CERT.PL
NASK

RAPORT ROCZNY
Z DZIAŁALNOŚCI CERT POLSKA

2021

Krajobraz bezpieczeństwa polskiego internetu

NASK-PIB/CERT Polska

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

mail: info@cert.pl

www.cert.pl

RAPORT ROCZNY
Z DZIAŁALNOŚCI
CERT POLSKA

2021

Krajobraz bezpieczeństwa
polskiego internetu

SPIS TREŚCI

WSTĘP

Nowy raport, stare techniki – tak w skrócie można ująć kluczowe obserwacje z 2021 r. Przestępcy udoskonalili znane sposoby oszustw i częściej zaczęli sięgać po metody wcześniej rzadko używane. Zaobserwowaliśmy wiele prób podszycia się pod kogoś, w których wykorzystywana jest już nie tylko fałszywa strona instytucji, ale także spoofing numeru telefonu lub kradzież tożsamości. Do realizacji ataku przestępcy wykorzystują narzędzia do zdalnego zarządzania urządzeniem użytkownika oraz stosują wyrafinowane sztuczki socjotechniczne. To wszystko przełożyło się na rekordową liczbę zgłoszeń w kategorii oszustw komputerowych, których łączny udział w całości obsłużonych przez nas incydentów wyniósł blisko 90 proc. Dlatego również w 2021 r. nie ustawaliśmy w wysiłkach związanych z popularyzacją inicjatyw takich jak Lista ostrzeżeń CERT Polska. Publikując porady w mediach społecznościowych wspieraliśmy również samych użytkowników wskazując, jak rozpoznać i przeciwdziałać atakom socjotechnicznym.

Rok 2021 przyniósł ze sobą także bardzo liczne próby ataków wykorzystujących różne nawyki i słabości użytkowników sieci. Pierwszym z nich jest posiadanie jednego hasła do różnych serwisów, dzięki czemu przestępcy uzyskują dostęp do kilku kont jednocześnie. Zwiększa to znacząco ich możliwości przy przeprowadzaniu zaplanowanej przez siebie akcji. Drugą ludzką słabością, poprzez którą oszuści osiągają swoje cele, jest wiara w istnienie łatwych i szybkich sposobów zarabiania pieniędzy. Przez cały rok obserwowaliśmy bardzo liczne kampanie promujące osiągnięcie zysku poprzez rzekome inwestycje w kryptowaluty lub walory krajowych spółek skarbu państwa. Ten scenariusz nie posiadał liniowego przebiegu, natomiast skutek dla ofiary zawsze był taki sam – kończył się utratą zaoszczędzonych albo nawet pożyczonych pieniędzy.

Na polu bardziej technicznych aspektów cyberbezpieczeństwa na wyróżnienie zasługują dwie istotne podatności: Log4Shell i podatności dotyczące Microsoft Exchange, których próby wykorzystania zanotowaliśmy także w Polsce. Za ich sprawą można było dostrzec, jak istotne jest prawidłowe obchodzenie się z procesem zarządzania podatnościami we współczesnych organizacjach, a także jak ważna jest współpraca z właściwym zespołem odpowiedzialnym za bezpieczeństwo.

W raporcie można znaleźć także opisy realizowanych przez nas projektów badawczo-rozwojowych, w tym narzędzi open-source. Warte uwagi są również statystyki dotyczące zgłaszanych incydentów oraz zagrożeń w sieciach polskich operatorów, zebrane na podstawie danych z platformy 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;
- 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 2021 ROKU

1. CERT Polska zarejestrował łącznie 29 483 unikalne incydenty cyberbezpieczeństwa. Odnotowaliśmy wzrost obsłużonych incydentów o 182 proc. w porównaniu do roku 2020. Najczęstszym typem był phishing – stanowiący aż 76,57 proc. wszystkich obsłużonych incydentów. Jest to wzrost o 196 proc. w porównaniu do poprzedniego roku. Sektory gospodarki, których najczęściej dotyczyły incydenty to: media, handel hurtowy i detaliczny oraz poczta i usługi kurierskie.
2. W 2021 r. na naszą Listę Ostrzeżeń przed niebezpiecznymi stronami trafiło 33 tys. domen. Najczęściej obserwowanym przez nas schematem kampanii phishingowej było wyłudzenie danych logowania do portalu Facebook. Był to trzykrotny wzrost w stosunku do 2020 r.
3. W ramach akcji #BezpiecznyPrzemysł aktywnie działamy na rzecz podniesienia poziomu cyberbezpieczeństwa polskiej infrastruktury przemysłowej. Dzięki poszukiwaniu nowych podatności w sprzęcie popularnym w Polsce, pięciu z nich przydzielono numer CVE, w tym dwóm z wysokim poziomem zagrożenia CVSS 10.0.
4. Zaobserwowaliśmy 13 proc. wzrost liczby incydentów dotyczących ransomware'u. Największą aktywność odnotowaliśmy w podmiotach infrastruktury cyfrowej i wśród osób fizycznych oraz w administracji publicznej. Najczęściej atakującymi rodzinami były: REvil/Sodinokibi oraz Phobos, a następnie Lockbit 2.0, STOP/DJVU, Makop, QLocker oraz Avaddon.
5. Model Ransomware as a Service stał się de facto standardem. Przestępcy starają się zmaksymalizować swój zysk pochodzący z pojedynczego ataku, żądając okupu nie tylko za odzyskanie zaszyfrowanych danych, ale też za nieujawnienie lub nieinformowanie o ataku.
6. Wykryto krytyczne luki bezpieczeństwa w popularnym oprogramowaniu takim jak: VMware vCenter, Microsoft Exchange oraz bibliotece Apache Log4j. W każdym z przypadków staraliśmy się ustalić liczbę podatnych urządzeń w Polsce i skontaktować się z dotkniętymi podmiotami w celu poinformowania o problemie i sposobach jego naprawienia.
7. Przestępcy skupili się na udoskonalaniu znanych scenariuszy phishingowych: przejęciu kont na Facebooku, fałszywych bramkach płatności oraz wyłudzaniu pieniędzy od sprzedających na portalach ogłoszeniowych.
8. Zaobserwowaliśmy użycie trzech nowych rodzin trojanów na platformę Android: Flubot, BlackRock oraz ERMAC. Najczęściej były one dystrybuowane za pomocą fałszywych wiadomości SMS oraz e-maili, które posiadały odnośniki do odpowiednio spreparowanych stron internetowych.
9. Ze względu na wzrost częstości wykorzystania wiadomości SMS jako sposobu na dystrybucję złośliwych linków, uruchomiliśmy specjalny numer odbiorczy: +48 799 448 084, na który można zgłosić incydent przez przekazanie otrzymanej wiadomości SMS zawierającej podejrzany link.
10. Przestępcy zaczęli wykorzystywać nowy schemat oszustw dotyczących fałszywych inwestycji w kryptowaluty. Najpopularniejsze były dwa scenariusze. W jednym wykonywane były połączenia telefoniczne z informacją o rzekomo zainwestowanych wcześniej środkach. W drugim na portalach społecznościowych promowano strony, które oferowały fałszywe inwestycje.
11. 21 lipca 2021 r. zespół CERT Polska zaobserwował napływ zgłoszeń i publikacje informacji medialnych o niepokojących wiadomościach e-mail, otrzymywanych przez użytkowników Profilu Zaufanego. Ustaliliśmy, że miał miejsce atak typu credential stuffing, polegający

na masowych próbach logowania na konta użytkowników platformy ePUAP przy użyciu haseł pochodzących z wcześniejszych wycieków. Na początku sierpnia 2021 r. funkcjonariusze z Komendy Stołecznej Policji zatrzymali w Woli Krzywieckiej podejrzanego o przeprowadzenie ataków.

12. Łącznie zgromadziliśmy informacje o 439 077 adresach IP wykazujących aktywność zombie, co stanowi spadek o ok. 31 proc. w stosunku do 2020 r. Wśród najczęściej występujących, podobnie jak w zeszłym roku, znajdują się Andromeda, Avalanche i Conficker. Na 4. miejscu znalazł się Flubot atakujący system Android, a za nim QSnatch infekujący urządzenia QNAP.
13. Na przestrzeni całego roku widoczny był stopniowy spadek liczby urządzeń umożliwiających wykonanie ataku DRDoS przy użyciu usług takich jak otwarte resolvery DNS, SNMP, portmapper oraz SSDP. W przypadku usług NTP, Netbios i mDNS liczba adresów IP utrzymuje się na podobnym poziomie w skali roku.
14. Podobnie jak rok wcześniej, najczęstszymi podatnymi usługami były: CWMP, SSL-POODLE, RDP, Telnet i TFTP. Możemy zauważyć pozytywny trend w zakresie stopniowego spadku liczby urządzeń związanych z podatnością Poodle i usługami RDP oraz Telnet na przestrzeni całego roku. Jest to kontynuacja trendu spadkowego z 2020 r. Do dużego spadku podatnych urządzeń doszło w usłudze CWMP.

KALENDARIUM NAJWAŻNIEJSZYCH WYDARZEŃ

STYCZEŃ

28.01 Krytyczna podatność CVE-2021-3156 w Sudo.
https://cert.pl/posts/2021/01/krytyczna-podatnosc-cve-2021-3156-w-sudo/

28.01 Atak ransomware na sieć klinik kardiologicznych American Heart of Poland.
https://zaufanatrzeciastrona.pl/post/atak-ransoware-na-najwieksza-siec-klinik-kardiologicznych-w-polsce/

LUTY

4.02 Policja rozbiła grupę przestępców odpowiedzialną za tworzenie fałszywych sklepów internetowych.
https://zaufanatrzeciastrona.pl/post/nastepna-banda-internetowych-oszustow-w-rekach-policji/

9.02 CD Projekt informuje o ataku ransomware na swoją sieć.
https://niebezpiecznik.pl/post/cd-projekt-informuje-o-ataku-ransomware-na-swoja-siec/

18.02 UODO nałożył 100 tysięcy złotych kary na KSSIP w związku z wyciekiem danych z 2020 r.
https://niebezpiecznik.pl/post/100-tys-zl-kary-za-wyciek-danych-sedziow-i-prokuratorow/

MARZEC

2.03 Krytyczne podatności w serwerze pocztowym Microsoft Exchange.
https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901

10.03 Niedostępność wielu serwisów w Europie spowodowana pożarem serwerowni OVH
https://niebezpiecznik.pl/post/splonela-serwerownia-ovh/

17.03 Włamanie na stronę Państwowej Agencji Atomistyki i portal zdrowie.gov.pl.
https://niebezpiecznik.pl/post/panstwowa-agencja-atomistyki-zhackowana-wrzucono-falszywy-komunikat-o-wzroscie-promieniowania/

KWIECIEŃ

3.04 Upublicznienie paczki z danymi 533 milionów użytkowników Facebooka.
https://niebezpiecznik.pl/post/facebook-wyciek-dane-533-milionow-uzytkownikow/

20.04 Wyciek danych osobowych ponad 20 000 policjantów, strażaków, celników i pograniczników.
https://niebezpiecznik.pl/post/wyciek-20000-danych-policjantow-funkcjonariuszy/

MAJ

18.05 Rozesłanie fałszywych maili o "powołaniu do cyberwojska" podszywających się pod gen. bryg. Karola Molendę.
https://niebezpiecznik.pl/post/nie-nie-zostales-powolany-do-cyberwojska/

CZERWIEC

1.06 Firma Uniqa opublikowała adresy email kilku tysięcy klientów przez wysyłanie maili bez użycia "Ukryte Do Wiadomości".
https://niebezpiecznik.pl/post/wpadka-uniqa/

8.06 Włamanie na skrzynkę pocztową ministra Michała Dworczyka.
https://niebezpiecznik.pl/post/michal-dworczyk-wyciek-telegram/

LIPIEC

18.07 Amnesty International opublikowało raport z analizy działania oprogramowania szpiegowskiego Pegasus.
https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

31.07 Wyciek danych klientów firmy Tauron.
https://niebezpiecznik.pl/post/wykradziono-dane-osobowe-klientow-taurona-w-tym-nagrania-rozmow/

SIERPIEŃ

13.08 Policja zatrzymała osobę odpowiedzialną za atak credential stuffing na Profil Zaufany.
https://niebezpiecznik.pl/post/wlamywal-sie-na-profile-zaufane-zostal-aresztowany-na-2-miesiace-ale-grozi-mu-8-lat/

15.08 Krytyczne błędy w modułach Wi-Fi firmy Realtek.
https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2021-35392_35395.pdf

16.08 Wyciek danych klientów a2mobile, Premium Mobile i NAU Mobile.
https://niebezpiecznik.pl/post/dane-klientow-a2mobile-premium-mobile-i-nau-mobile-byly-dostepne-dla-wlamywaczy/

WRZESIEŃ

11.09 Wyciek danych klientów Centrum Medyczne Luxmed Lublin sp. z o. o.
https://niebezpiecznik.pl/post/luxmed-informuje-o-incydencie-otwarty-dostep-do-danych-osobowych-pacjentow/

30.09 Atak ransomware na firmę Totolotek.
https://niebezpiecznik.pl/post/totolotek-zhackowany-dane-uzytkownikow-mogly-wyciec/

PAŹDZIERNIK

4.10 Awaria doprowadziła do kilkugodzinnej niedostępności serwisów firmy Meta.
https://niebezpiecznik.pl/post/facebook-whatsapp-i-instagram-nie-dzialaja/

8.10 Fałszywe certyfikaty szczepień przeciw COVID.
https://niebezpiecznik.pl/post/falszowanie-certyfikat-covid-paszport/

LISTOPAD

4.11 Zatrzymanie części członków grupy ransomware REvil.
https://www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged

8.11 List otwarty pracowników CERT Polska.
https://cert.pl/posts/2021/11/list-otwarty/

8.11 Atak ransomware na europejskie oddziały Media Markt.
https://www.bleepingcomputer.com/news/security/mediamarkt-hit-by-hive-ransomware-initial-240-million-ransom/

16.11 Firma Mandiant opublikowała raport związany z działalnością UNC1151.
https://www.mandiant.com/resources/unc1151-linked-to-belarus-government

GRUDZIEŃ

10.12 Krytyczna podatność w bibliotece Apache Log4j.
https://cert.pl/posts/2021/12/krytyczna-podatnosc-w-bibliotece-apache-log4j/

OCHRONA CYBERPRZESTRZENI RP I DZIAŁANIA CERT POLSKA

Podsumowanie roku z perspektywy zgłaszanych incydentów

Sukcesywnie każdego roku CERT Polska rejestruje coraz większą liczbę zgłoszeń oraz incydentów cyberbezpieczeństwa. W 2021 r. CERT Polska zarejestrował 116 071 zgłoszeń. Spośród wszystkich zgłoszeń nasi specjaliści wytypowali 65 586, na podstawie których zarejestrowano łącznie **29 483 unikalnych incydentów cyberbezpieczeństwa.**

Zgłoszenia incydentów trafiają do nas 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,
- listownie korzystając z formularza dostępnego na stronie bip.nask.pl

CERT Polska odnotował **wzrost obsłużonych incydentów na poziomie 182 proc. w porównaniu do roku ubiegłego.** Przypomnijmy, że w 2020 r. CERT Polska obsłużył 10 420 unikalnych incydentów cyberbezpieczeństwa.

Najpopularniejszym typem incydentów w 2021 r. był phishing – stanowiący aż 76,57 proc. wszystkich obsłużonych incydentów. **Liczba incydentów zaklasyfikowanych jako phishing w porównaniu do roku poprzedniego wzrosła o 196 proc.** i osiągnęła wartość 22 575 incydentów. Tak samo jak w roku poprzednim, fundamentalny wpływ na zwiększenie liczby zarejestrowanych incydentów phishingowych miała wprowadzona w marcu 2020 r. Lista Ostrzeżeń przed stronami niebezpiecznymi. Najpopularniejszym phishingiem w 2021 r. było podszywanie się pod serwis społecznościowy Facebook – 4852 incydentów.

Drugim typem incydentów pod względem popularności jakie CERT Polska zarejestrował i obsłużył było szkodliwe oprogramowanie. Tego typu incydentów w 2021 r. zarejestrowano 2847, co stanowi 9,66 proc. wszystkich obsłużonych incydentów. Liczba ta w porównaniu do roku ubiegłego wzrosła o 281 proc.

Trzecie miejsce w rankingu liczby zarejestrowanych incydentów w ubiegłym roku przypada kategorii obraźliwych i nielegalnych treści, w tym spamu. Odsetek tego typu incydentów wyniósł 1,05 proc. Tak niewielki procent wynika z faktu, iż do jednego incydentu zespół CERT Polska często przypisuje wiele zgłoszeń. Jest to szczególnie zauważalne dla tej kategorii incydentów, gdzie za 311 incydentów odpowiadało aż 21 522 zgłoszeń. Dodatkowo incydenty z kategorii obraźliwych i nielegalnych treści są obsługiwane przez dedykowany do tego celu zespół Dyżurnet.pl, który również działa w strukturach NASK. Popularnymi obsługiwanymi tego typu incydentami były ataki tzw. sextortion scam, polegające na masowym rozsyłaniu wiadomości mailowych informujących o rzekomym przejęciu kontroli nad urządzeniami ofiary oraz posiadaniu przez nadawcę materiałów prezentujących ofiarę w kontekście erotycznym. W zamian za zapłacenie żądanego okupu, atakujący oferuje wykasowanie kompromitujących materiałów.

CERT Polska rejestrując incydenty klasyfikuje i przypisuje je do odpowiednich sektorów, których dotyczyły. Specjaliści zespołu CERT Polska w 2021 r. zarejestrowali łącznie 8339 incydentów, które wystąpiły w sektorze media. Taka liczba daje około 28,28 proc. wszystkich zarejestrowanych incydentów. Sektor ten obejmuje między innymi incydenty występujące w mediach społecznościowych, prasie czy telewizji. Wśród wszystkich incydentów zaklasyfikowanych w sektorze media, znaczna część czyli 91,73 proc. to incydenty typu phishing.

Kolejnym sektorem pod względem ilości zarejestrowanych incydentów był sektor handlu hurtowego i detalicznego. W sektorze tym zarejestrowano ogółem 17,38 proc. wszystkich incydentów, co daje liczbę 5125 incydentów. Sektor ten obejmuje między innymi incydenty w serwisach aukcyjnych oraz sklepach internetowych. Podobnie jak w sektorze media, w tym przypadku również incydenty typu phishing stanowią znaczącą przewagę wszystkich incydentów – 89,17 proc.

Trzecim sektorem z wynikiem 4338 incydentów jest sektor poczta i usługi kurierskie. W tym sektorze zarejestrowano 4338 incydentów cyberbezpieczeństwa, 84,14 proc. z nich również dotyczą phishingu. Ten sektor obejmuje między innymi incydenty dotyczące firm spedycyjnych czy operatorów poczty elektronicznej.

CSIRT NASK w ramach Ustawy o Krajowym Systemie Cyberbezpieczeństwa w 2021 r. obsłużył **36 incydentów, które zaklasyfikowano jako poważne,** czyli takie, których wystąpienie ma istotny skutek zakłócający świadczenie usługi kluczowej. Zostało zarejestrowanych 31 incydentów poważnych z sektora bankowego, 3 z sektora energii oraz 2 z sektora ochrony zdrowia. CERT Polska zarejestrował o 4 incydenty poważne więcej niż w roku 2020.

W 2021 r. CSIRT NASK obsłużył 512 incydentów dotyczących podmiotów publicznych. To wzrost o 11 proc. względem roku ubiegłego. Najczęstsze zarejestrowane incydenty zaklasyfikowane jako incydenty w podmiocie publicznym należały do sektora administracja publiczna – 288 przypadków. Kolejnym sektorem była oświata i wychowanie – 81 incydentów oraz sektor infrastruktura cyfrowa – 43 incydenty.

Dokładne statystyki incydentów z podziałem na sektory gospodarki i rodzaje incydentów zawarte są w tabelach nr 1 i 2.

W połowie kwietnia 2021 r. odnotowaliśmy w Polsce pierwsze sygnały pojawienia się złośliwego oprogramowania o nazwie Flubot. Ze względu na jego charakterystykę polegającą na rozprzestrzenianiu się z wykorzystaniem wiadomości SMS, uruchomiliśmy specjalny numer odbiorczy. Od 24 kwietnia na numer +48 799 448 084 można zgłosić do CERT Polska incydent, poprzez przekazanie otrzymanej wiadomości SMS zawierającej podejrzany link.

Do końca roku **na dedykowany numer telefonu otrzymaliśmy 23 308 zgłoszeń,** w których treści znalazł się adres URL. 11 852 z nich, a więc 50,8 proc., znajdowało się w domenie umieszczonej na liście ostrzeżeń. **Dzięki zgłoszeniom kanałem SMS zablokowanych zostało 3 588 złośliwych domen. Stanowi to 10,6 proc. wszystkich blokad z 2021 roku.** Jest to zaskakująca liczba, biorąc pod uwagę, że większość z nich trafiło na nią w listopadzie i grudniu.

Uruchomienie kanału zgłoszeń SMS pozwoliło nam również uzyskać lepszy pogląd na to, które oszustwa najczęściej rozprzestrzeniają się tą drogą. Bezapelacyjnie najwięcej, bo aż 10 693 złośliwych linków dotyczyło dystrybucji Flubota, który był przyczyną utworzenia numeru odbiorczego. Drugi w kolejności był phishing wykorzystujący wizerunek firm PGE oraz InPost. Zgłoszeń wpisujących się w schemat tej kampanii było 863. Podium zamykają oszustwa wycelowane w osoby sprzedające przedmioty na portalach aukcyjnych, takich było 403. Kampanie te zostały szczegółowo opisane w dalszych rozdziałach.

Sektor gospodarki	Liczba incydentów	%
Energetyka	4 084	13,85%
Transport	220	0,75%
Bankowość	947	3,21%
Infrastruktura rynków finansowych	563	1,91%
Służba zdrowia	150	0,51%
Wodociągi	18	0,06%
Infrastruktura cyfrowa	1 606	5,45%
Inne	68	0,23%
Brak	0	0,00%
Administracja publiczna	429	1,46%
Budownictwo i gospodarka nieruchomościami	89	0,30%
Kultura i ochrona dziedzictwa narodowego	11	0,04%
Kultura fizyczna	2	0,01%
Oświata i wychowanie	142	0,48%
Rolnictwo	2	0,01%
Rybołówstwo	0	0,00%
Wyznania religijne i mniejszości narodowe	6	0,02%
Działalność ubezpieczeniowa	3	0,01%
Izby gospodarcze i handlowe	4	0,01%
Handel hurtowy i detaliczny	5 125	17,38%
Produkcja	421	1,43%
Logistyka i dystrybucja	18	0,06%
Poczta i usługi kurierskie	4 338	14,71%
Turystyka	15	0,05%
Gospodarka odpadami	6	0,02%
Hotele, restauracje, catering	295	1,00%
Media	8 339	28,28%
Usługi inne	118	0,40%
Osoby fizyczne	2 464	8,36%
Razem	29 483	100,00%

Tab. 1. Incydenty obsłużone przez CERT Polska w 2021 r. w podziale na sektor gospodarki.

Typy incydentu	Liczba incydentów	%
I. Obraźliwe i nielegalne treści	**311**	**1,05%**
Spam	262	0,89%
Dyskredytacja, obrażanie	9	0,03%
Pornografia dziecięca, przemoc	4	0,01%
Niesklasyfikowane	36	0,12%
II. Złośliwe oprogramowanie	**2 847**	**9,66%**
Wirus	1	0,00%
Robak sieciowy	0	0,00%
Koń trojański	9	0,03%
Oprogramowanie szpiegowskie	0	0,00%
Dialer	0	0,00%
Rootkit	1	0,00%
Niesklasyfikowane	2 836	9,62%
III. Gromadzenie informacji	**27**	**0,09%**
Skanowanie	19	0,06%
Podsłuch	0	0,00%
Inżynieria społeczna	3	0,01%
Niesklasyfikowane	5	0,02%
IV. Próby włamań	**127**	**0,43%**
Wykorzystanie znanych luk systemowych	2	0,01%
Próby nieuprawnionego logowania	15	0,05%
Wykorzystanie nieznanych luk systemowych	0	0,00%
Niesklasyfikowane	110	0,37%
V. Włamania	**247**	**0,84%**
Włamanie na konto uprzywilejowane	6	0,02%

Włamanie na konto zwykłe	118	0,40%
Włamanie do aplikacji	6	0,02%
Bot	2	0,01%
Niesklasyfikowane	115	0,39%
VI. Dostępność zasobów	**148**	**0,50%**
Atak odmowy usługi (DoS)	6	0,02%
Rozproszony atak odmowy usługi (DDoS)	74	0,25%
Sabotaż komputerowy	1	0,00%
Przerwa w działaniu usług (niezłośliwe)	53	0,18%
Niesklasyfikowane	14	0,05%
VII. Atak na bezpieczeństwo informacji	**55**	**0,19%**
Nieuprawniony dostęp do informacji	33	0,11%
Nieuprawniona zmiana informacji	3	0,01%
Niesklasyfikowane	19	0,06%
VIII. Oszustwa komputerowe	**25 472**	**86,40%**
Nieuprawnione wykorzystanie zasobów	3	0,01%
Naruszenie praw autorskich	1	0,00%
Kradzież tożsamości, podszycie się	12	0,04%
Phishing	22 575	76,57%
Niesklasyfikowane	2 881	9,77%
IX. Podatne usługi	**216**	**0,73%**
Otwarte serwisy podatne na nadużycia	53	0,18%
Niesklasyfikowane	163	0,55%
X. Inne	**33**	**0,11%**
Razem	**29 483**	**100,00%**

Tab 2. Incydenty obsłużone przez CERT Polska w 2021 r. w podziale na kategorie wg taksonomii eCSIRT.net mkVI[1].

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

Lista ostrzeżeń przed niebezpiecznymi stronami

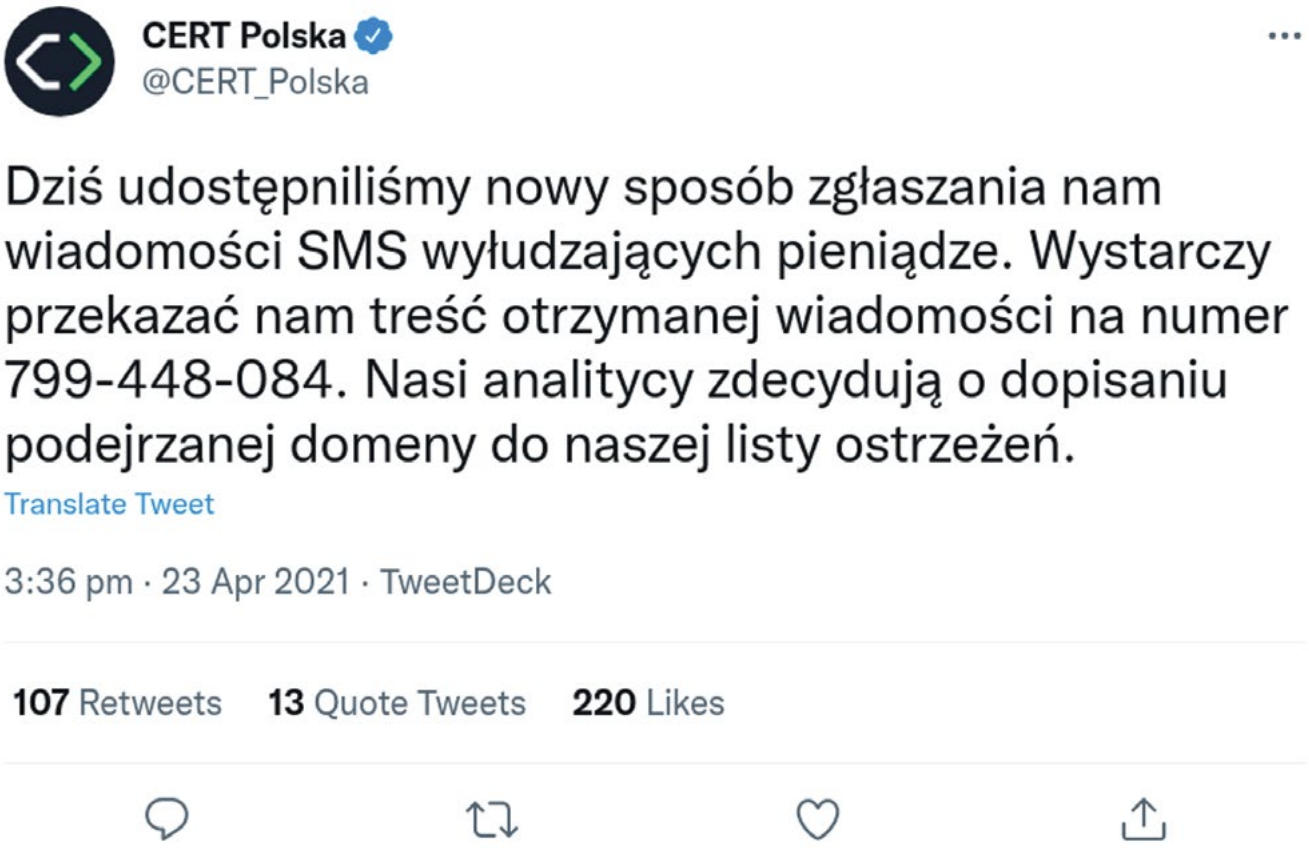
W marcu 2021 r. prowadzona przez CERT Polska Lista ostrzeżeń przed niebezpiecznymi stronami obchodziła swoje pierwsze urodziny. Nieodpłatnie udostępniany przez nas spis domen jest wykorzystywany zarówno przez operatorów telekomunikacyjnych, administratorów oraz użytkowników indywidualnych do poprawy bezpieczeństwa w sieci poprzez blokowanie znanych domen używanych do wyłudzeń danych oraz kradzieży środków finansowych.

Rys. 1. Plansza informacyjna o zablokowaniu strony przez Listę Ostrzeżeń. Wygląd strony może różnić się w zależności od operatora telekomunikacyjnego.

Najprostszym sposobem, aby zacząć korzystać z Listy jest dodanie jej w formacie adblock[2] do rozszerzenia uBlock Origin w zainstalowanej przeglądarce. Więcej informacji na temat integracji znajduje się na podstronie poświęconej Liście[3].

W odpowiedzi na nasilające się kampanie złośliwego oprogramowania Flubot, w kwietniu uruchomiliśmy nowy sposób zgłaszania podejrzanych domen – poprzez wiadomości SMS[4]. Dzięki niemu, w przypadku otrzymania wiadomości SMS zawierającej złośliwy adres URL, użytkownik może bardzo szybko nam ją zgłosić poprzez "podanie dalej" całej wiadomości na specjalny numer telefonu: **+48 799 448 084**. Wiadomości zgłoszone w ten sposób są przez nas analizowane, następnie załączone domeny są wpisywane na Listę ostrzeżeń jeśli faktycznie są wykorzystywane do oszustw.

2. https://hole.cert.pl/domains/domains_adblock.txt
3. https://cert.pl/posts/2020/03/ostrzezenia_phishing/
4. https://twitter.com/CERT_Polska/status/1385588498883874817



Rys. 2. Informacja o uruchomieniu usługi zgłaszania podejrzanych wiadomości za pomocą wiadomości SMS.

Do końca roku na Listę trafiło blisko 42 tys. złośliwych domen, z czego aż 33 tys. w 2021 r. Każda z zablokowanych domen była dokładnie weryfikowana przez naszych pracowników przed uznaniem za złośliwą, dzięki czemu stworzyliśmy jedno z najbardziej wiarygodnych źródeł tego typu danych, które może być przetwarzane w sposób automatyczny.

W wyniku rosnącego poziomu wdrożenia Listy w różnych systemach filtrowania treści, **tylko w 2021 r. udało się powstrzymać blisko 4 miliony prób wejścia na strony oznaczone jako wyłudzające dane.**

Najczęściej obserwowaliśmy kampanie phishingowe wyłudzające dane logowania do portalu Facebook (7785 domen). Była to najpopularniejsza forma phishingu w roku 2020, jednak w roku 2021 ich liczba wzrosła ponad trzykrotnie. Najczęściej wykorzystywany był schemat wyłudzenia danych logowania celem rzekomej weryfikacji wieku, wymaganego do obejrzenia filmu z drastycznego bądź szokującego wydarzenia. Niektóre z przykładów tego typu ataków pokazywaliśmy w ostrzeżeniach z 10 maja[5] i 11 października 2021 r[6].

5. https://twitter.com/CERT_Polska/status/1391757158551805955
6. https://twitter.com/CERT_Polska/status/1447547559245930497

Rys. 3. Strona z fałszywą informacją dotyczącą szczepień. Aby wyświetlić załączony film użytkownik musi najpierw podać dane logowania do swojego konta w celu weryfikacji wieku. Tak pozyskane dane przestępcy wykorzystują do dalszych wyłudzeń.

Cieszymy się, że coraz więcej firm i użytkowników korzysta z Listy ostrzeżeń przed niebezpiecznymi stronami. Widoczny jest stały, wzrastający trend. W związku z tym mamy nadzieję, że w następnym roku uda nam się jeszcze bardziej poszerzyć zasięg Listy i ochronić większą liczbę polskich użytkowników.

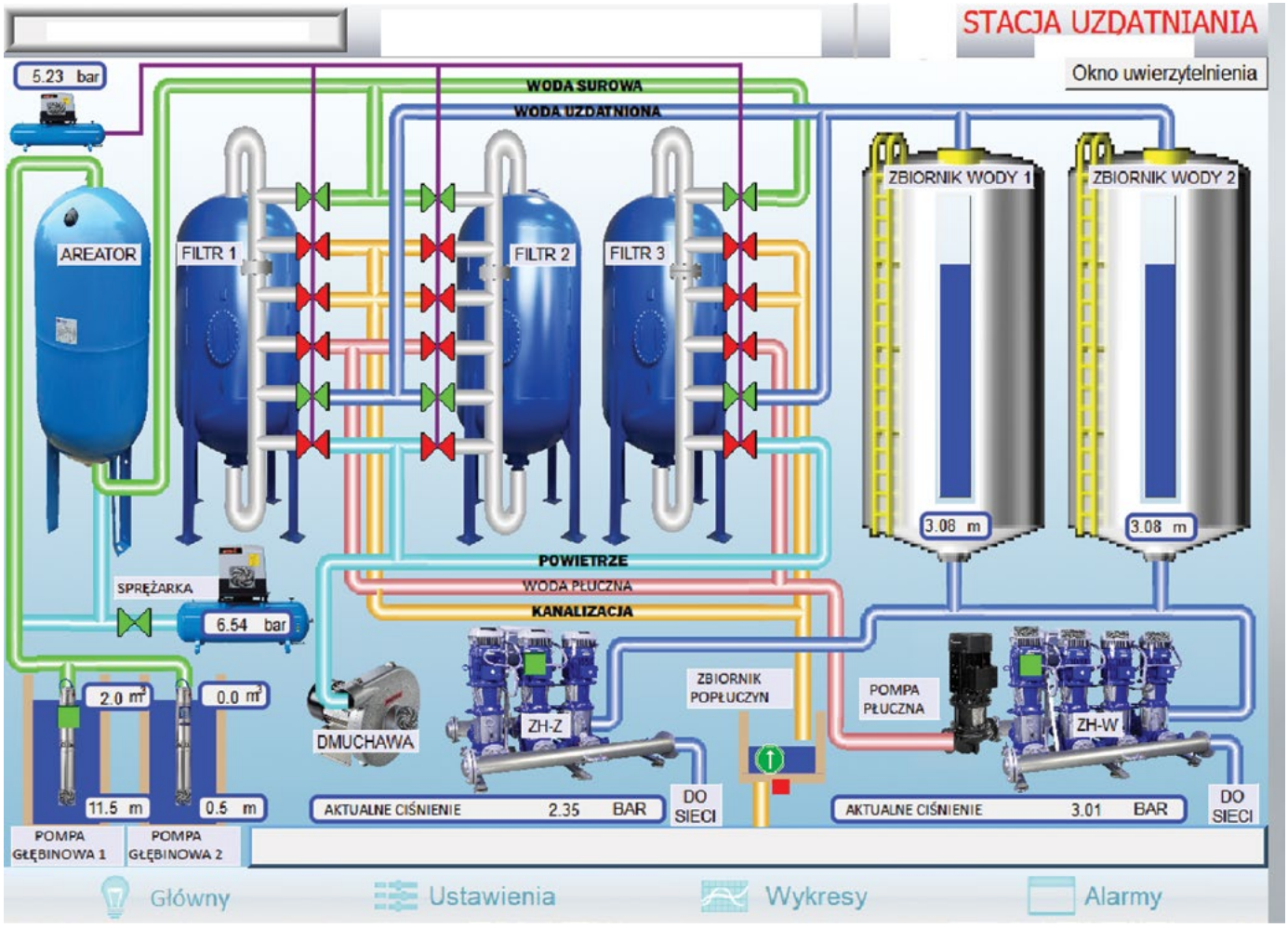
Zachęcamy do zgłaszania incydentów pod adresem: https://incydent.cert.pl/ i przekazywania złośliwych wiadomości SMS na numer **+48 799 448 084**, ponieważ głównie dzięki zgłoszeniom użytkowników możemy skutecznie działać.

#BezpiecznyPrzemysł

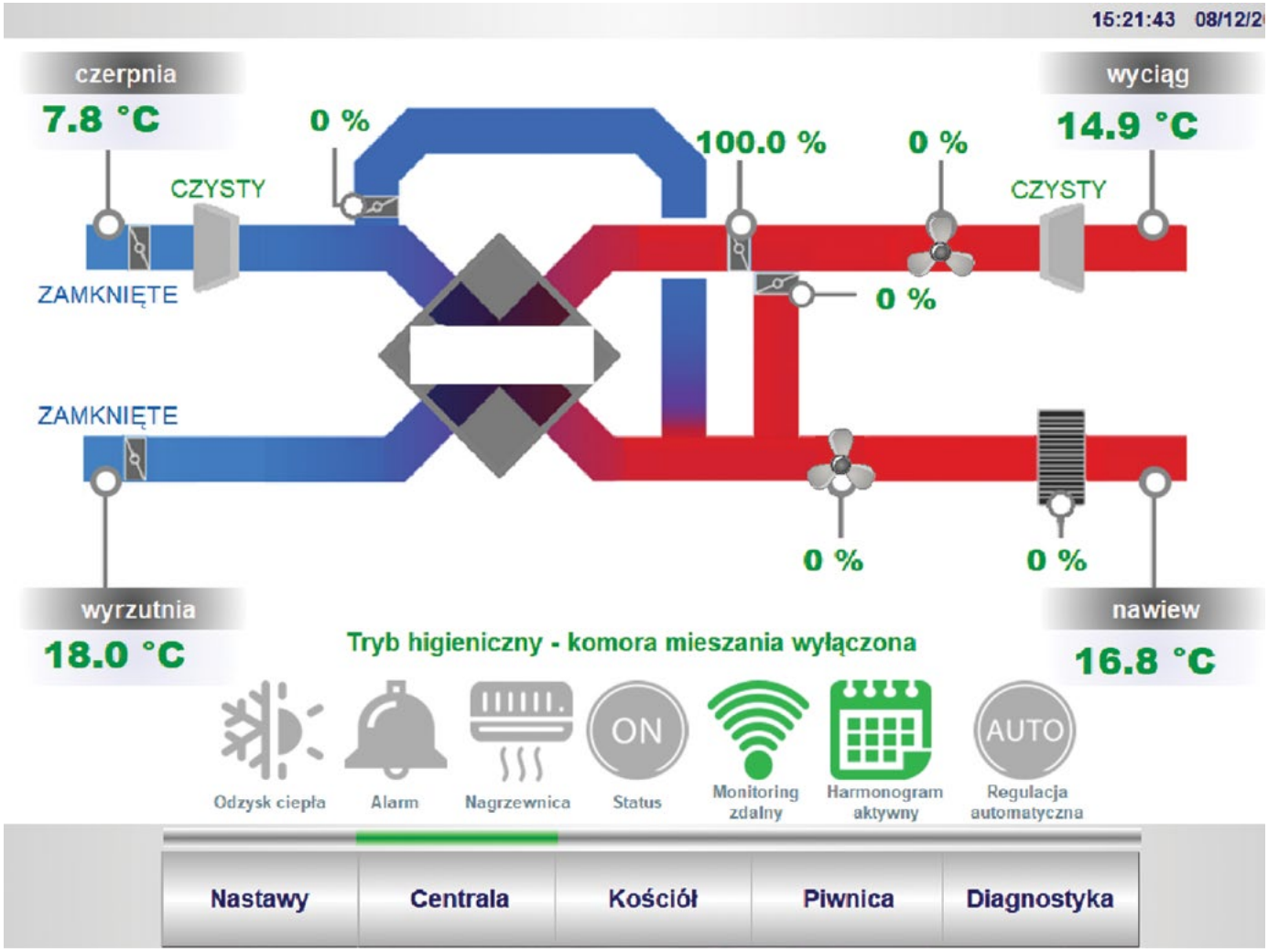
W 2021 r. kontynuowaliśmy akcję #BezpiecznyPrzemysł, w ramach której aktywnie działamy na rzecz podniesienia poziomu cyberbezpieczeństwa polskiej infrastruktury przemysłowej. W tym celu szukamy dostępnych z publicznego internetu urządzeń, takich jak sterowniki PLC czy panele operatorskie (HMI). Następnie kontaktujemy się z ich właścicielami i doradzamy, jak je zabezpieczyć. W tym roku skupiliśmy się głównie na rozwoju wewnętrznych narzędzi automatyzujących oraz na poszukiwaniu nowych podatności w sprzęcie popularnym w Polsce.

W ciągu tego roku podjęliśmy działania względem licznych przypadków, w których można było zdalnie przejąć całkowitą kontrolę na procesem przemysłowym. Do najciekawszych należą:

- 6 oczyszczalni ścieków;
- 4 stacje uzdatniania wody (przykład na rys. 4);
- przepompownia ścieków;
- mała elektrownia wodna;
- system centralnego ogrzewania w wieży kontroli lotów;
- liczne systemy automatyki budynkowej w centrach handlowych;
- system HVAC w kościele (rys. 5).



Rys. 4. Panel operatorski stacji uzdatniania wody dostępny z internetu.



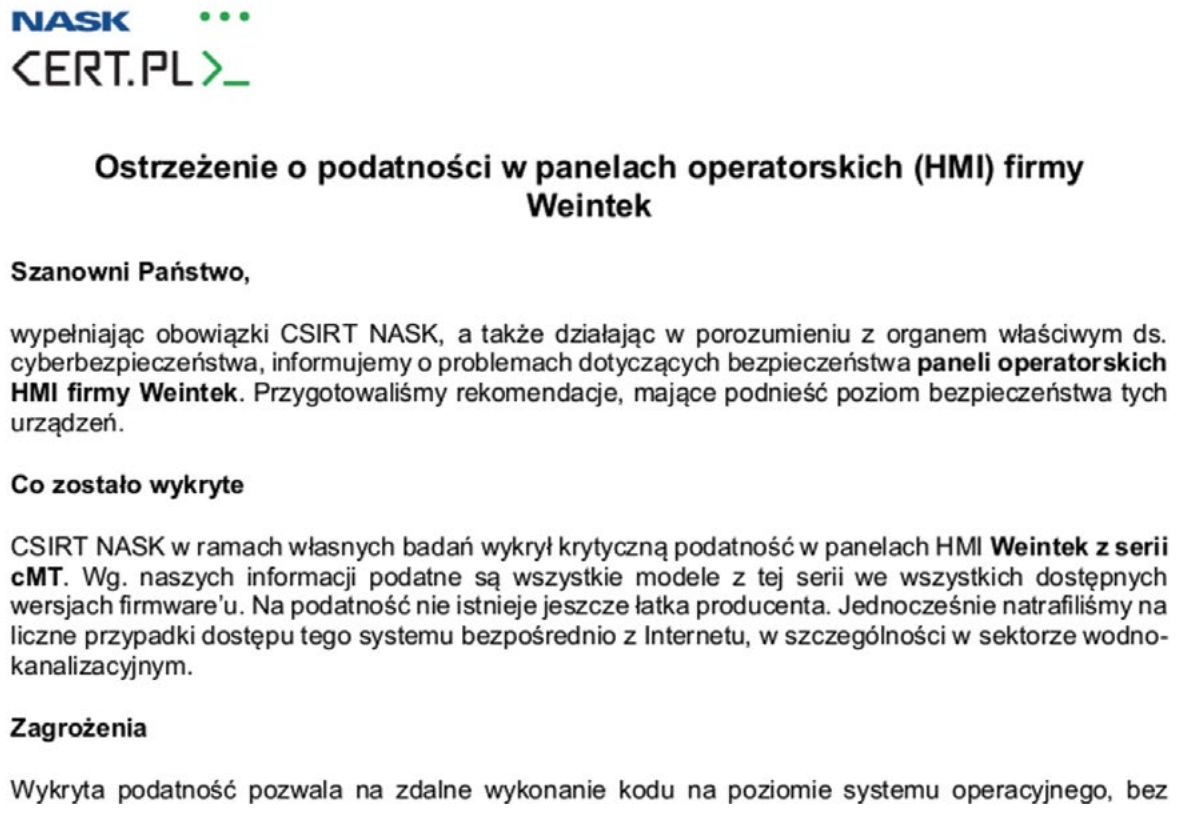
Rys. 5. Panel sterowania systemem HVAC w kościele dostępny z internetu.

W wyniku poszukiwania nowych podatności uzyskaliśmy możliwość zdalnego wykonania kodu aż na dwóch urządzeniach pełniących rolę centralnego HMI dla małych zakładów.

- 3 CVE (CVE-2021-27446, CVE-2021-27444, CVE-2021-27442) w oprogramowaniu **Weintek EasyWeb cMT**, w tym krytyczna podatność (**CVSS 10.0**) pozwalająca na zdalne wykonanie kodu bez uwierzytelniania[7];
- 2 CVE (CVE-2021-43931, CVE-2021-43936) w oprogramowaniu **Distributed Data Systems WebHMI**, w tym krytyczna podatność (**CVSS 10.0**) pozwalająca na zdalne wykonanie kodu bez uwierzytelniania[8].

Wszystkie podatności zostały zgłoszone w ramach procedury odpowiedzialnego ujawniania błędów, we współpracy z producentami. W każdym przypadku wysyłaliśmy też ostrzeżenia i rekomendacje poprzez organy właściwe ds. cyberbezpieczeństwa dla danych sektorów, natychmiast po wykryciu problemu. Przykład takiego ostrzeżenia można zobaczyć na rys. 6.

7. https://www.cisa.gov/uscert/ics/advisories/icsa-21-082-01
8. https://www.cisa.gov/uscert/ics/advisories/icsa-21-336-03



NASK
CERT.PL

Ostrzeżenie o podatności w panelach operatorskich (HMI) firmy Weintek

Szanowni Państwo,

wypełniając obowiązki CSIRT NASK, a także działając w porozumieniu z organem właściwym ds. cyberbezpieczeństwa, informujemy o problemach dotyczących bezpieczeństwa **paneli operatorskich HMI firmy Weintek**. Przygotowaliśmy rekomendacje, mające podnieść poziom bezpieczeństwa tych urządzeń.

Co zostało wykryte

CSIRT NASK w ramach własnych badań wykrył krytyczną podatność w panelach HMI **Weintek z serii cMT**. Wg. naszych informacji podatne są wszystkie modele z tej serii we wszystkich dostępnych wersjach firmware'u. Na podatność nie istnieje jeszcze łatka producenta. Jednocześnie natrafiliśmy na liczne przypadki dostępu tego systemu bezpośrednio z Internetu, w szczególności w sektorze wodno-kanalizacyjnym.

Zagrożenia

Wykryta podatność pozwala na zdalne wykonanie kodu na poziomie systemu operacyjnego, bez

Rys. 6. Fragment ostrzeżenia rozesłanego do sektorów po znalezieniu nowej podatności w panelach firmy Weintek.

Konferencja SECURE

W roku 2021 obchodziliśmy dwa ważne jubileusze. Świętowaliśmy 25-lecie powstania zespołu CERT Polska oraz 25. edycję konferencji SECURE. Od ćwierć wieku wspólnie budujemy społeczność działającą na rzecz bezpieczeństwa ICT, a podczas konferencji SECURE mamy niepowtarzalną okazję podzielić się wiedzą i doświadczeniem w tym zakresie.

15 czerwca odbyła się już czwarta edycja konferencji SECURE Early Bird. Gościem specjalnym był Stewart Garrick z fundacji Shadowserver, który opowiadał o współpracy z CERT Polska mającej na celu poprawę bezpieczeństwa użytkowników na poziomie krajowym. Z kolei specjaliści zespołu CERT Polska przedstawili zagadnienia, nad którymi pracują na co dzień. Wśród omawianych tematów znalazła się publikowana przez nas lista złośliwych domen (Mateusz Szymaniec), napotykane problemy ze zgłaszaniem błędów w systemach przemysłowych (Marcin Dudek) i wykorzystanie przejętych stron i kont społecznościowych do dezinformacji (Przemek Jaroszewski).

Główna konferencja SECURE odbyła się w dniach 19-20 października. Tak jak w poprzednim roku, konferencja została podzielona 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 rozpoczął się od panelu dyskusyjnego podsumowującego 25 lat działalności naszego zespołu. Wzięli w nim udział, oprócz Przemka Jaroszewskiego, także poprzedni kierownicy CERT Polska: Krzysztof Silicki, Mirosław Maj oraz Piotr Kijewski.

Jak zawsze można było liczyć na wysoki poziom merytoryczny prezentacji. Wśród prelegentów znaleźli się m.in. Adam Haertle z prezentacją o wpadkach przestępców, Alexandre Dulaunoy i Jean-Louis Huynen z CIRCL opowiadający o sposobie śledzenia botnetów kopiących kryptowaluty, a także minister Janusz Cieszyński, który omówił nowelizację Ustawy o Krajowym Systemie Cyber-

bezpieczeństwa. Gościliśmy również Piotra Borkowskiego, który opisał sposób budowania i działania zespołów typu Red Team, Kamila Dudka z prezentacją dotyczącą sposobów obejścia mechanizmu Secure Boot i Grzegorza Tworka o metodach oszukiwania podpisów cyfrowych w systemach Windows.

Nagrania z konferencji są dostępne na naszym kanale YouTube[9]. Aktualności można śledzić na stronie konferencji SECURE[10], a także na kontach społecznościowych w serwisie Twitter[11], Facebook[12] oraz LinkedIn[13].

Ćwiczenia i konkursy

CERT Polska regularnie uczestniczy w krajowych i międzynarodowych ćwiczeniach sprawdzających zarówno umiejętności technicznej analizy zagrożeń jak i testujących procedury reagowania na incydenty. Rok 2021 w kontekście międzynarodowych ćwiczeń dla światowej branży cyberbezpieczeństwa był próbą odnalezienia się w nowej rzeczywistości. Po rocznej przerwie spowodowanej pandemią koronawirusa odbyły się konkursy z serii Locked Shields i European Cyber Security Challenge. Pod koniec roku mogliśmy również zauważyć powrót niektórych cyklicznych, międzynarodowych konferencji cyberbezpieczeństwa, co z kolei umożliwia organizatorom konkursów Capture The Flag powrót do organizacji konkursów finałowych.

Locked Shields

Locked Shields to największe i najbardziej zaawansowane ćwiczenia obrony bezpieczeństwa komputerowego na świecie. Organizowane są przez certyfikowane przez NATO Centrum Doskonalenia Cyberobrony (CCDCOE) z siedzibą w Estonii każdej wiosny już od 11 lat (z przerwą w 2020 r.). W ćwiczeniach uczestniczą rządy krajów finansujących działanie Centrum, podmioty komercyjne oraz instytucje naukowe. Krajowe reprezentacje (oraz zespoły bezpieczeństwa zaproszonych organizacji międzynarodowych) w ćwiczeniu wcielają się w rolę zespołów "niebieskich". Pełnią rolę zespołów szybkiego reagowania na incydenty komputerowe, które przez dwa dni ćwiczeń na prośbę fikcyjnego kraju "Berylia" należącego do NATO, muszą ochraniać symulowaną infrastrukturę informatyczną przed atakami zespołu "czerwonego". W 2021 r. w ćwiczeniach udział wzięło ponad 2000 specjalistów z 30 krajów.

W ramach symulowanej bazy wojskowej każdy z zespołów "niebieskich" miał do obrony ponad 150 systemów informatycznych: od typowych systemów takich jak stacje robocze, serwery, urządzenia sieciowe, chmurę obliczeniową, po wyspecjalizowane takie jak system obrony przeciwlotniczej, sieć LTE oraz systemy infrastruktury przemysłowej: elektrownię wraz z systemem dystrybucji prądu, stację uzdatniania wody, oraz, co było nowością, system naziemnej obsługi satelity obserwacyjnego. Na systemy chronione przez 22 zespoły "niebieskich" przeprowadzono ponad 4 tysiące ataków.

Struktura ćwiczenia wymaga od każdego z zespołów koordynacji w wielu aspektach zarządzania cyberbezpieczeństwem w obliczu konfliktu hybrydowego. Oprócz zabezpieczenia systemów oraz odpierania ataków w ramach reagowania na incydenty, od zespołów "niebieskich" oczekuje się także wymiany informacji w ramach współpracy międzynarodowej, a także udziału w przeplatających się ze sobą, równoległych ścieżkach ćwiczenia polegających na:

- analizie informatyki śledczej, w której zespoły w ramach dedykowanego konkursu Capture The Flag muszą przeanalizować otrzymane obrazy nośników i odtworzyć przebieg incydentu,
- analizie medialnej, w której m.in. sprawdzana jest skuteczność reagowania na działania dezinformacyjne w symulowanym środowisku mediów tradycyjnych i społecznościowych,
- analizie prawnej, podczas której zespoły muszą przygotować szereg analiz prawnych z zakresu prawa międzynarodowego,
- działaniach strategicznych, w których testowane są procesy zarządzania kryzysowego.

Polska reprezentacja, pod przewodnictwem woj-

9. https://www.youtube.com/user/CERTPolska
10. https://secure.edu.pl
11. https://twitter.com/securepl
12. https://www.facebook.com/Konferencja.SECURE
13. https://www.linkedin.com/showcase/10852603/

skowego Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni, składająca się zarówno z wojskowych jak i cywilnych ekspertów: zespołów CSIRT, instytucji państwowych, podmiotów infrastruktury krytycznej oraz firm z sektora m.in. bankowego i telekomunikacyjnego zajęła w 2021 r. wysokie, 4. miejsce. Na podium znalazły się kolejno: Szwecja, Finlandia i Czechy.

W 2021 r. eksperci CERT Polska oraz NASK kierowali pracami aż czterech zespołów w polskiej reprezentacji:

- systemów specjalnych (w tym infrastruktury przemysłowej),
- aplikacji internetowych,
- infrastruktury sieciowej,
- prawnego.

Rys. 7. Część systemów przemysłowych używanych w ćwiczeniu, fot. NATO CCDCOE.

European Cyber Security Challenge

Po rocznej przerwie spowodowanej walką z pandemią powróciły młodzieżowe mistrzostwa Europy w cyberbezpieczeństwie, czyli zawody European Cyber Security Challenge. Organizowany corocznie konkurs zapoczątkowany przez Komisję Europejską w 2013 r. ma na celu popularyzację zagadnień z zakresu cyberbezpieczeństwa oraz zachęcenie młodzieży do planowania kariery zawodowej w tym obszarze. Od 2016 r. za organizację wydarzenia odpowiedzialna jest ENISA. Polska po raz pierwszy wzięła udział w zawodach ECSC w 2018 r.

Przed finałem konkursu każdy z krajów musi wyłonić 10-osobową reprezentację składającą się z 5 osób w wieku od 14. do 20. roku życia i 5 osób w wieku od 21 do 25 lat. W tej edycji konkursu, ze względu na odwołane wydarzenie przed rokiem, wyjątkowo zdecydowano się na podniesienie limitu wieku o jeden rok.

Podobnie jak w innych krajach, również w Polsce w celu wyłonienia reprezentacji organizowane są krajowe kwalifikacje. Od samego początku za jego organizację, opiekę nad reprezentacją i jej udział w europejskich finałach odpowiada zespół CERT Polska.

W indywidualnym konkursie kwalifikacyjnym w formule Capture The Flag przeprowadzonym w dniach 2–4 lipca na platformie hack.cert.pl udział wzięło 108 osób, z których 59 wykonało choć jedno zadanie. Uczestnicy zmagali się z zadaniami w kategoriach: bezpieczeństwa aplikacji internetowych, inżynierii wstecznej oprogramowania, wykorzystywania podatności bezpieczeństwa, kryptografii, informatyki śledczej i elektroniki.

Skład wyłonionej reprezentacji to:

- Jakub Kądziołka (kapitan),
- Kacper Kluk,
- Kajetan Grzybowski,
- Jakub Wasilewski,
- Szymon Borecki,
- Krzysztof Haładyn,
- Jakub Nowak,
- Patryk Balicki,
- Grzegorz Uriasz,
- Karol Baryła.

Każda chętna osoba może sama zmierzyć się z zadaniami konkursowymi z tych i ubiegłych kwalifikacji odwiedzając stronę https://hack.cert.pl.

Finały odbyły się w dniach 28 września – 1 października w czeskiej Pradze. Pomimo panującej pandemii koronawirusa w zawodach udział wzięło 19 reprezentacji narodowych. W konkursie finałowym polska reprezentacja po raz pierwszy stanęła na podium zajmując drugie miejsce. Pierwsze i trzecie miejsce zajęli odpowiednio: Niemcy oraz Włosi. Finały w 2022 r. odbędą się w Wiedniu.

Rys. 8. Finały ECSC 2021 w Pradze, fot. NASK.

Scena CTF

Konkursy Capture The Flag (CTF) są drużynowymi zawodami bezpieczeństwa komputerowego. Organizowane są niezależnie przez instytucje naukowe, rządy państw, organizacje pozarządowe oraz same zespoły CTF.

Zawody podzielić można według formy i miejsca rozgrywki. Najpopularniejszą formułą zawodów jest "jeopardy", w której drużyny rozwiązują od kilkunastu do kilkudziesięciu zadań o różnym poziomie trudności w kilku kategoriach: bezpieczeństwa aplikacji internetowych, inżynierii wstecznej i wykorzystywania znalezionych podatności, kryptografii czy analiz informatyki śledczej. Rozwiązanie zadania kończy się zdobyciem ukrytej "flagi" – kawałka tekstu, który zespoły na platformie konkursowej wymieniają na punkty. Wygrywa zespół, który zdobędzie najwięcej punktów. W tej formule organizowane są m.in. finały zawodów European Cyber Security Challenge oraz kwalifikacje do polskiej reprezentacji.

Inna formuła zawodów CTF to "attack/defence", w której każdy z zespołów otrzymuje identyczną kopię infrastruktury informatycznej, na której działają zadania-aplikacje przygotowane przez organizatorów. Zawody dzielą się na kilkuminutowe rundy, w których każdy z zespołów stara się wykraść flagi z systemów pozostałych zespołów. Wygrywa 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).

Przed pandemią koronawirusa najbardziej prestiżowe konkursy łączyły obie formuły – kwalifikacje przeprowadzane przez internet w formule "jeopardy" oraz finały w formule "attack/defence" organizowane offline. Te ostatnie najczęściej odbywały się przy okazji międzynarodowych konferencji cyberbezpieczeństwa. Pandemia sprawiła, że większość cyklicznych konferencji została zawieszona lub odbyła się on-line, co negatywnie wpłynęło na światową scenę CTF. Jednocześnie okazało się to szansą dla młodszych zespołów. Podobnie jak w poprzednim roku zdominowały one podium światowego rankingu CTFTime. Drugi raz z rzędu pierwsze miejsce zajął amerykański zespół "perfect blue". Drugie miejsce zdobył nowy zespół "organizers" powstały z połączenia studenckich drużyn ze Szwajcarii, Niemiec i Wielkiej Brytanii. Trzecie miejsce wywalczył zespół Super Guesser wywodzący się z Korei Południowej. W najlepszej światowej dwudziestce znalazły się trzy polskie zespoły: Dragon Sector, justCatTheFish oraz p4. Odbyły się również kolejne edycje konkursów organizowanych przez Dragon Sector oraz p4. Konkurs "Dragon CTF" wygrał tajwański zespół Balsn, a zwycięzcą konkursu organizowanego przez p4 okazał się paneuropejski zespół hxp.

W 2021 r. odbyła się również druga edycja konkursu bezpieczeństwa informatycznego w branży kosmicznej pt. "Hack-a-Sat" organizowanego przez amerykańskie wojsko. Ponownie wystąpił w nim zespół "Poland Can Into Space" złożony z członków zespołów p4 oraz Dragon Sector. W kwalifikacjach, które podobnie jak w poprzednim roku odbyły się w formule "jeopardy", wygrał polski zespół poprawiając swój wynik sprzed roku (drugie miejsce). Umożliwiło to ekipie z Polski udział w finałach, które były konkursem w formule "attack/defense", a zatem zespoły musiały nie tylko kontrolować swojego satelitę, ale również bronić go przed atakami innych zespołów oraz wykradać flagi z systemów zainstalowanych na symulowanych satelitach pozostałych drużyn. W finałowej klasyfikacji zespół "Poland Can Into Space", podobnie jak w ubiegłym roku, zajął drugie miejsce.

Rys. 9. Członkowie zespołu "Poland Can Into Space" (Dragon Sector / p4), drugiego najlepszego zespołu w konkursie Hack-A-Sat 2, fot. p4.

Projekty

MWDB i Karton

Projekt MWDB jest jedną z inicjatyw prowadzonych przez CERT Polska, której celem jest dostarczenie repozytorium pozwalającego na sprawną wymianę informacji na temat złośliwego oprogramowania. Prace nad projektem są kontynuowane nieustannie od 2018 r., kiedy publicznie udostępniony został serwis mwdb.cert.pl. Obecnie wśród komponentów dostępnych dla analityków złośliwego oprogramowania można znaleźć również:

- **MWDB Core**[14], czyli otwartoźródłowe oprogramowanie stanowiące rdzeń serwisu mwdb.cert.pl. Umożliwia uruchomienie podobnego repozytorium złośliwego oprogramowania w ramach własnej infrastruktury,
- **Karton**[15] – projekt stanowiący otwartoźródłowy framework do budowania i integracji mikroserwisów, składających się na środowisko służące do automatycznej analizy złośliwego oprogramowania,

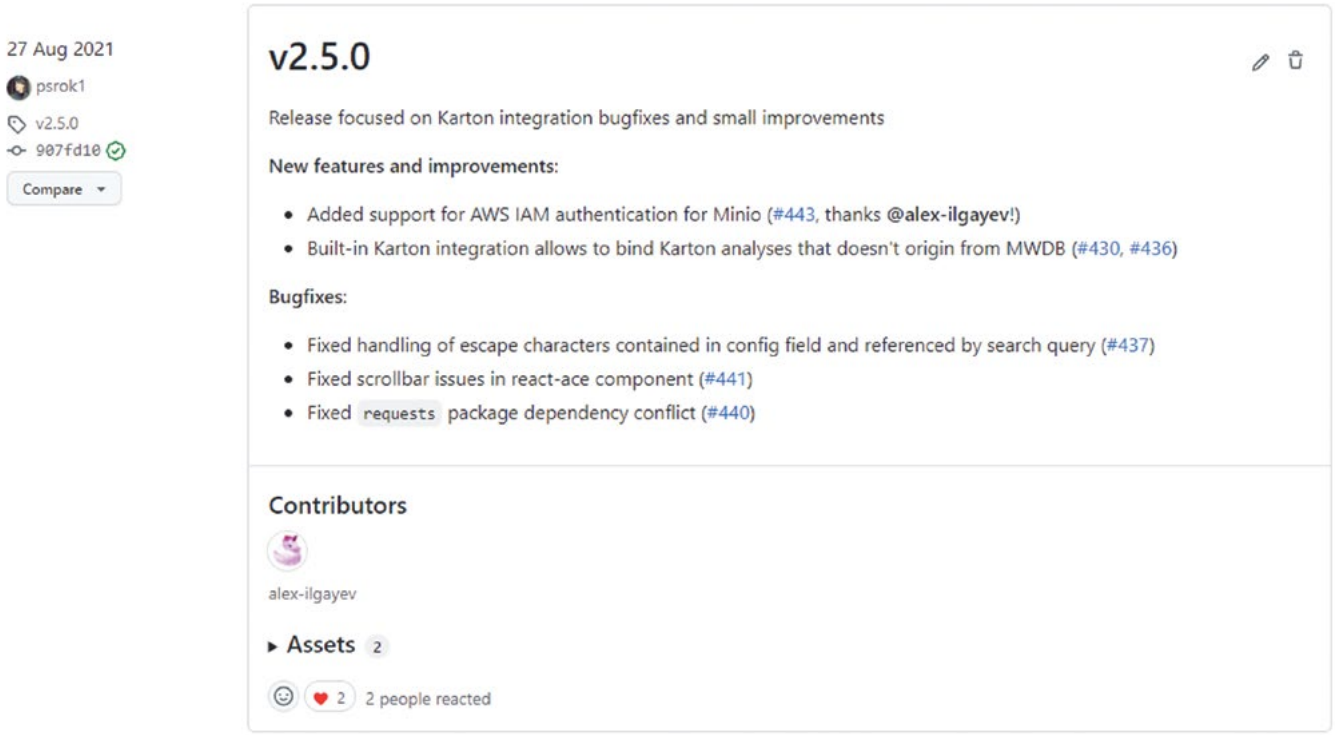
inne projekty wspomagające, takie jak **mquery**[16] (akcelerator wyszukiwania próbek za pomocą reguł Yara), **malduck**[17] (biblioteka do budowania modułów do ekstrakcji statycznej konfiguracji z próbek) czy **DRAKVUF Sandbox**[18] opisany w osobnym artykule na stronie 40.

Rozwój projektu MWDB Core

W ciągu 2021 r. prowadzono intensywne prace nad wzbogaceniem projektu MWDB Core o dodatkowe funkcje. Jedną z nich było eksperymentalne wprowadzenie możliwości łatwego zintegrowania zewnętrznego serwisu MWDB Core z serwisem mwdb.cert.pl. Integracja umożliwia przeszukiwanie repozytorium i pobieranie obiektów ze zdalnego serwisu mwdb.cert.pl z poziomu interfejsu własnej instancji MWDB Core.

W kolejnych wersjach wprowadzono wbudowaną integrację MWDB Core z projektem Karton, dzięki czemu nie trzeba instalować dodatkowych rozszerzeń, aby automatycznie zlecać analizy dla dodawanych próbek. Ponadto znacząco ułatwiono administrowanie własną instancją, a także umożliwiono usuwanie dowolnych obiektów z poziomu interfejsu. Kompletny wykaz zmian, jakie wprowadzono w MWDB Core, wraz z podziałem na poszczególne wersje można znaleźć w zakładce Releases na stronie Github projektu MWDB Core: https://github.com/CERT-Polska/mwdb-core/releases. Wiele z tych usprawnień wprowadzono dzięki sugestiom i poprawkom zewnętrznych kontrybutorów.

14. https://github.com/CERT-Polska/mwdb-core
15. https://github.com/CERT-Polska/karton
16. https://github.com/CERT-Polska/mquery
17. https://github.com/CERT-Polska/malduck
18. https://github.com/CERT-Polska/drakvuf-sandbox



Rys. 10. Opis wydania v2.5.0 oprogramowania MWDB Core.

Aby wspomóc analityków w efektywnym korzystaniu z projektu MWDB, w 2021 r. przeprowadziliśmy cykl prezentacji i warsztatów. Jeden z nich, zatytułowany "Build Your Own Malware Analysis Pipeline Using New Open Source Tools", odbył się 15 kwietnia w ramach FIRST Workshop Series[19] i jest dostępny na kanale YouTube organizacji FIRST: https://www.youtube.com/watch?v=dPwzF_hsCow. Na potrzeby tego typu warsztatów stworzyliśmy środowisko **karton-playground**, w ramach którego można w prosty sposób postawić podstawowe projekty składające się na MWDB i spróbować dodać do niego własne integracje.

Rozwój platformy MWDB odbywał się w ramach projektów AMCE i JTAN, tworzonych w ramach programu Unii Europejskiej „Łącząc Europę" (Connecting Europe Facility).

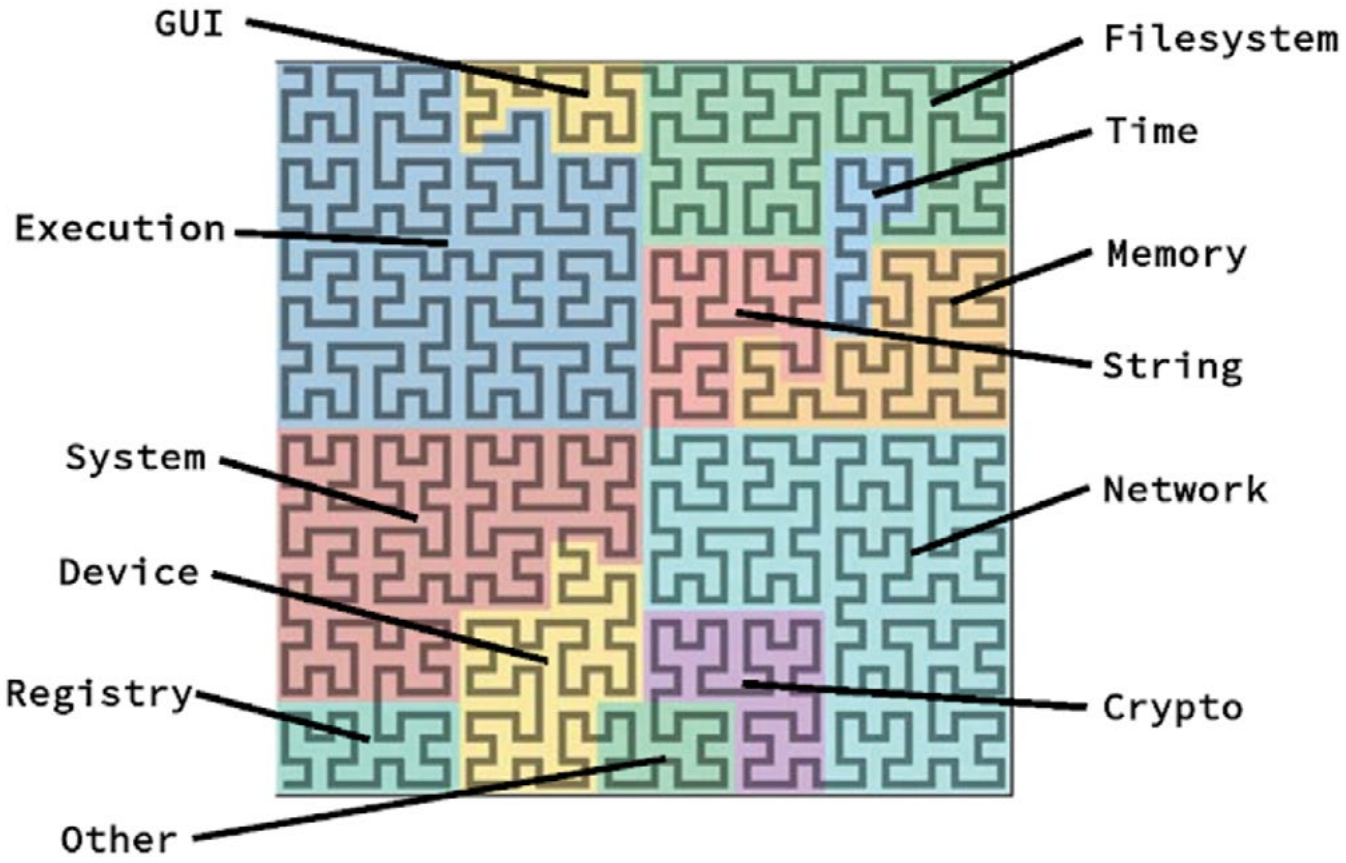
Automatyczna klasyfikacja próbek złośliwego oprogramowania na podstawie ApiVectorów

W raporcie za rok 2020 na str. 65[20] opisywaliśmy rozpoczęty przez nas eksperymentalny projekt związany z klasyfikacją próbek złośliwego oprogramowania na podstawie wykorzystywanych przez nie API systemowych.

Pierwszym etapem analizy próbki jest jej uruchomienie w naszym narzędziu DRAKVUF Sandbox[21], z którego otrzymujemy od kilku do kilkuset (a w skrajnych przypadkach nawet kilku tysięcy) zrzutów pamięci. Następnie zrzuty te poddawane są statycznemu wykrywaniu wywołań funkcji Windows API w kodzie binarnym badanej aplikacji, który się w nich znajduje. Wykorzystujemy do tego celu narzędzie ApiScout[22] stworzone przez Daniela Plohmanna.

Jednym z bardziej kompaktowych wyników dostarczanych przez ApiScout są wektory binarne o długości 1024, w 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 11.

19. https://www.first.org/events/training/ws-mar-apr2021/
20. https://cert.pl/uploads/docs/Raport_CP_2020.pdf#page=65
21. https://github.com/CERT-Polska/drakvuf-sandbox
22. https://github.com/danielplohmann/apiscout



Rys. 11. Graficzna reprezentacja ApiVectora (ApiQR) z użyciem krzywej Hilberta z podziałem bitów na kategorie semantyczne[23].

Następnie otrzymane ApiVectory używane są do przypisywania próbek do znanych nam rodzin złośliwego oprogramowania.

W 2021 r. projekt był dalej rozwijany. Punktem wyjściowym był dla nas wniosek z poprzedniego roku dotyczący przewagi metody klasyfikacji na poziomie pojedynczych zrzutów pamięci (czyli z pominięciem agregacji ApiVectorów) nad klasyfikacją na poziomie próbek.

Zmieniona została metoda klasyfikacji. Wcześniej każdy ApiVector otrzymany ze zrzutu pamięci był przyrównywany do ApiVectorów uwzględnionych wcześniej w wyuczonym modelu, które mają przypisane nazwy rodzin szkodliwego oprogramowania, i dopasowywany do wszystkich, które znalazły się ponad pewnym ustalonym progiem podobieństwa (stopień podobieństwa jest obliczany na podstawie indeksu Jaccarda[24]). Po zmianie wybierany jest tylko jeden, najbardziej podobny ApiVector z modelu (lub ew. kilka ApiVectorów w przypadku remisu). Struktura i sposób tworzenia modelu pozostały niezmienione. Oprócz tego wraz z klasyfikacją zrzutu zapisywana jest również odpowiadająca jej wartość podobieństwa. W tym momencie próg podobieństwa przestał być konieczny i zdecydowaliśmy się z niego w ogóle zrezygnować, żeby zachować jak najwięcej informacji, ponieważ proces selekcji tych najistotniejszych i wybór odpowiedniego progu może być dokonany przez analityka na późniejszym etapie.

Do mechanizmu automatycznych klasyfikacji zostało również doimplementowane uwzględnianie dodatkowego, tworzonego ręcznie modelu. Dzięki temu można łatwiej zarządzać elementami modeli, które nie zostały dodane automatycznie.

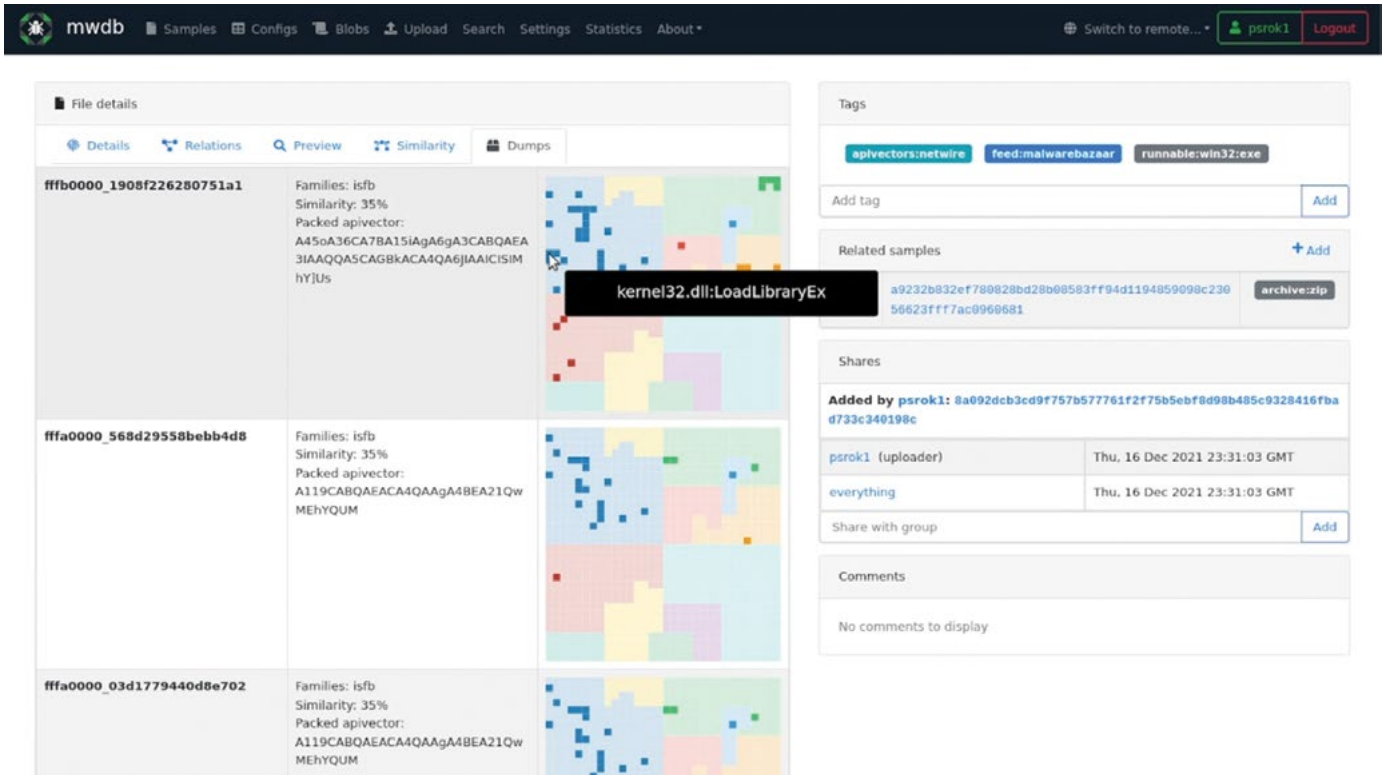
Do działania narzędzia ApiScout potrzebna jest baza danych offsetów funkcji eksportowanych przez biblioteki z Windows API, jak również adresy w pamięci, pod które same biblioteki są ładowane. Taką bazę generujemy tylko raz dla danego obrazu maszyny wirtualnej gościa. Nazwaliśmy ją profilem statycznym. Ponieważ profil taki jest generowany na uruchomionym systemie, to uwzględnia on wpływ mechanizmu ASLR, ale niestety

23. http://byte-atlas.blogspot.com/2018/04/apivectors.html
24. https://pl.wikipedia.org/wiki/Indeks_Jaccarda

nie w pełni, gdyż niektóre biblioteki mogą być ładowane pod różne adresy dla każdego uruchamianego procesu. Przez to niektóre offsety ASLR w profilu statycznym stają się nieprawidłowe, co uniemożliwia ApiScoutowi wyznaczenie prawdziwych adresów funkcji z odpowiadających tym offsetom bibliotek i w konsekwencji również wykrycie wywołań takich funkcji w zrzucie pamięci. W związku z tym pojawiła się potrzeba zbierania adresów załadowania bibliotek dla każdego procesu oddzielnie jeszcze w trakcie uruchomienia próbki w DRAKVUF Sandboxie. Następnie adresy te miałyby być łączone z profilem statycznym i w ten sposób tworzyć profile dedykowane poszczególnym procesom. Takie profile nazwaliśmy profilami dynamicznymi. W 2021 r. składanie ich zostało zaimplementowane w naszym projekcie klasyfikatora, dzięki czemu możliwe stało się wykrywanie wywołań funkcji Windows API, które wcześniej nie dawały się wykrywać.

Przy okazji powyższego usprawnienia została również zrobiona automatyzacja zbierania profilu statycznego z maszyny wirtualnej gościa – wcześniej bowiem profil generowało się ręcznie za pomocą dodatkowego narzędzia dostarczanego razem z ApiScoutem[25]. Implementacja oparta na tym narzędziu została wbudowana w DRAKVUF Sandboxa. Obsługa nowego sposobu dostarczania profilu statycznego nie została jeszcze w pełni ukończona po stronie projektu klasyfikatora – zostało to przewidziane na rok 2022.

Powstał również nowy, bardziej zaawansowany interfejs użytkownika prezentujący wyniki klasyfikacji. Został on zrealizowany jako plugin do MWDB, który zostanie wdrożony produkcyjnie w 2022 r.



Rys. 12. Przykładowy widok nowego interfejsu użytkownika.

System klasyfikacji powstał na bazie komponentów stworzonych przez CERT Polska, które udostępniamy na otwartych licencjach, w skład których wchodzą: system zarządzania zadaniami **Karton**, biblioteka kliencka MWDB – **mwdblib**[26] oraz biblioteka do wspomagania analizy złośliwego oprogramowania **Malduck**. Projekt klasyfikatora jest rozwijany w ramach projektu badawczego SPARTA, a dokładniej w ramach podprogramu T-SHARK, w obszarze analizy złośliwego oprogramowania na dużą skalę.

25. https://github.com/danielplohmann/apiscout/tree/master/apiscout/db_builder
26. https://github.com/CERT-Polska/mwdblib

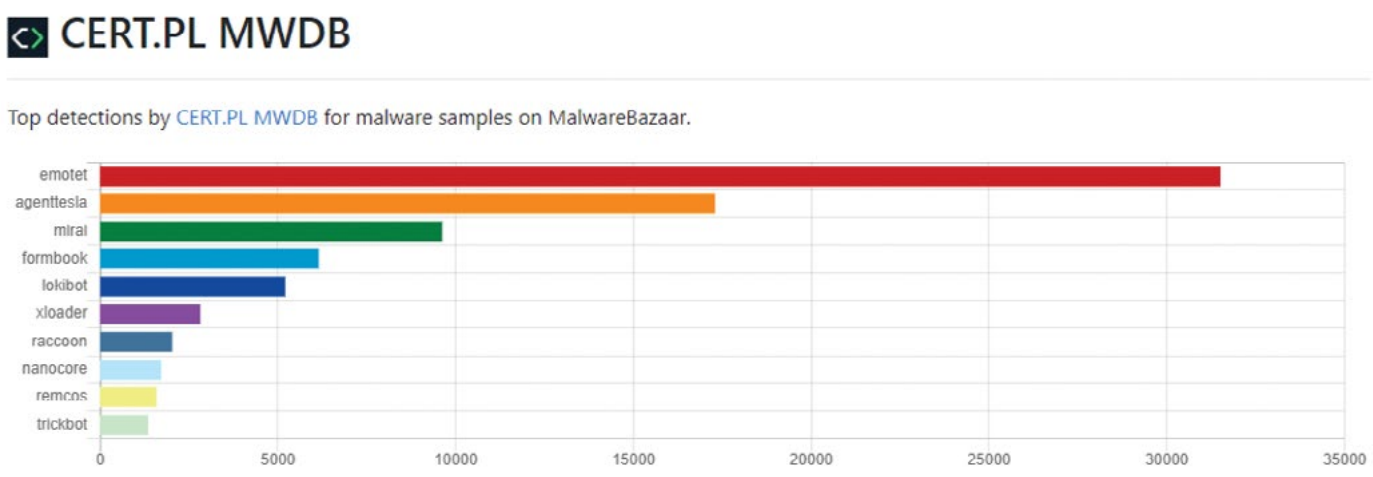
Statystyki z platformy mwdb.cert.pl

W 2021 r. w ramach serwisu mwdb.cert.pl:

- przeanalizowano łącznie ponad 368 tys. próbek złośliwego oprogramowania
- pozyskano 19 tys. statycznych konfiguracji
- zarejestrowano 188 kont dla zewnętrznych analityków złośliwego oprogramowania. W sumie z platformy mwdb.cert.pl korzysta już 842 użytkowników.

Nazwa rodziny	Liczba plików wykonywalnych	Liczba unikalnych konfiguracji
Mirai	14 315	3 087
Agent Tesla	11 540	4 311
Formbook (XLoader)	9 191	1 380
Lokibot	3 409	1 227
Sodinokibi	2 763	1 947
Raccoon	2 314	352
Qbot	2 212	70
Cobalt Strike	1 656	531
Emotet	1 627	27
Alien RAT	1 502	894

Tab. 3. Dziesięć najpopularniejszych rodzin pod względem liczby rozpoznanych próbek przez serwis mwdb.cert.pl w 2021 r.



Rys. 13. Całościowe statystyki wykrytych rodzin przez serwis mwdb.cert.pl na podstawie próbek dodanych do serwisu MalwareBazaar[27].

Powyższe rezultaty zostały uzyskane dzięki znacznemu udziałowi społeczności analityków złośliwego oprogramowania, zarówno tych, którzy zasilają serwis mwdb.cert.pl próbkami jak i użytkowników platformy MWDB Core, którzy dzielą się cennymi sugestiami i usprawnieniami.

27 https://bazaar.abuse.ch/statistics/

DRAKVUF Sandbox

DRAKVUF Sandbox[28] został upubliczniony na początku 2020 r. Projekt ma na celu zbudowanie systemu do analizy złośliwego oprogramowania, który oparty jest na monitorze DRAKVUF[29]. Więcej informacji na temat samego projektu i jego rozwoju w 2020 r. można znaleźć na str. 71 w raporcie za rok 2020[30].

W 2021 r. sandbox był nadal rozwijany. Składało się na to 197 pull requestów włączonych do repozytorium, z czego przeważającą część stanowiły usprawnienia istniejących możliwości sandboxa i dokumentacji. Spośród nowych funkcji należy wymienić:

- wyciąganie kluczy TLS z maszyny wirtualnej gościa, które można załadować do Wiresharka, aby odszyfrować ruch sieciowy[31],
- *drakplayground*[32] – środowisko do szybkiego stawiania testowej maszyny wirtualnej i interakcji z nią, użyteczne również do modyfikowania docelowego snapshota[33],
- generowanie profilu Windows API dla narzędzia ApiScout[34] (więcej na ten temat można znaleźć na str. 37–38),
- wdrożenie infrastruktury do testów, w tym w szczególności do testów regresyjnych, co przełoży się na większą stabilność kolejnych wydań[35].

Rozwój projektu DRAKVUF w 2021 r.

Tak jak w poprzednich latach w ramach rozwoju sandboxa nasz zespół wspierał również rozwój samego projektu bazowego, czyli DRAKVUF-a. Naprawiliśmy wiele błędów i dokonaliśmy usprawnień[36], w tym m.in. zaimplementowanie ochrony przeciwko wykorzystaniu przez złośliwe oprogramowanie techniki zwanej api-hammeringiem[37].

Jednak największe zmiany w projekcie DRAKVUF z udziałem specjalistów CERT Polska zostały wprowadzone przy okazji uczestnictwa w programie Google Summer of Code.

Google Summer of Code

Google Summer of Code (GSoC)[38] jest programem skupionym na pozyskiwaniu nowych kontrybutorów do społeczności otwartego oprogramowania. Uczestnicy programu mają za zadanie pracować nad kilkumiesięcznym projektem pod przewodnictwem mentorów z wybranej organizacji open source.

Potencjalni uczestnicy kontaktują się z organizacjami mentorującymi, z którymi chcą pracować. Następnie na podstawie pomysłu opublikowanego przez organizację przygotowują propozycję projektu. Po akceptacji spędzają kilka tygodni na zapoznawaniu się ze społecznością i istniejącym kodem, a także we współpracy z mentorami definiują kamienie milowe. Następnie przez kolejnych 12 tygodni piszą kod do projektu.

Od 2005 r. program Google Summer of Code połączył ponad 18 tys. nowych kontrybutorów otwartego oprogramowania ze 112 krajów z ponad 17 tys. mentorów ze 118 krajów. Napisano przy tym ponad 40 milionów linii kodu dla 746 organizacji open source.

Udział CERT Polska w GSoC

W 2021 r. zespół CERT Polska wziął udział w programie za pośrednictwem organizacji The Honeynet Project[39] [40], w wyniku czego nawiązaliśmy współpracę z dwoma studentami.

Efektem współpracy było wykonanie dwóch ulepszeń w projekcie DRAKVUF, opisanych w gościnnych artykułach na naszej stronie internetowej.

Linux Injector for automated malware analysis[41]

Kontrybutor: Manorit Chawdhry

28. https://github.com/CERT-Polska/drakvuf-sandbox
29. https://github.com/tklengyel/drakvuf
30. https://cert.pl/uploads/docs/Raport_CP_2020.pdf#page=71
31. https://github.com/CERT-Polska/drakvuf-sandbox/pull/392
32. https://github.com/CERT-Polska/drakvuf-sandbox/pull/435
33. https://drakvuf-sandbox.readthedocs.io/en/latest/usage/managing_snapshots.html#snapshot-modification
34. https://github.com/danielplohmann/apiscout
35. https://drakvuf-sandbox.readthedocs.io/en/v0.18.1/regression_testing.html
36. https://github.com/CERT-Polska/drakvuf-sandbox/releases/tag/v0.15.0-p2
37. https://github.com/tklengyel/drakvuf/pull/1114
38. https://summerofcode.withgoogle.com
39. https://www.honeynet.org/gsoc/gsoc-2021/
40. https://twitter.com/CERT_Polska_en/status/1369593756643647491
41. https://cert.pl/en/posts/2021/08/gsoc-linux-injector/

Celem projektu było stworzenie dla DRAKVUF-a linuksowego iniektora, czyli narzędzia, które potrafi wstrzykiwać shellcode oraz pisać i czytać pliki z linuksowego systemu z wirtualnej maszyny gościa. Takie możliwości pozwalają na wstrzyknięcie próbki złośliwego oprogramowania na maszynę gościa, uruchomienie tej próbki oraz pozyskanie wszystkich plików, które w wyniku tego uruchomienia zostały zapisane na dysku.

Dla systemu Windows w DRAKVUF-ie był już zaimplementowany stabilny iniektor. Istniał również jego linuksowy odpowiednik, ale był on niestabilny i polegał na stałych offsetach wewnątrz biblioteki glibc, które w rzeczywistości zmieniają się pomiędzy jej wersjami. W nowym podejściu autor zdecydował się na bezpośrednie wykorzystanie linuksowego interfejsu wywołań systemowych, co było możliwe dzięki temu, że interfejs ten jest stabilny pomiędzy wersjami jądra Linuksa.

W trakcie trwania GSoC-a w linuksowym iniektorze zostały zaimplementowane trzy metody:

1. **shellcode** – wstrzykuje podany kod maszynowy do wybranego procesu i uruchamia go.
2. **writefile** – kopiuje plik z hosta na maszynę wirtualną gościa. Z perspektywy zautomatyzowanej analizy złośliwego oprogramowania służy głównie do wstrzykiwania próbki.
3. **readfile** – kopiuje plik z maszyny wirtualnej gościa na hosta. Jest to szczególnie przydatne, gdy złośliwe oprogramowanie działa wieloetapowo – tą metodą możemy pozyskać plik, który został przez nie zapisany na dysku.

Po zakończeniu GSoC-a linuksowy iniektor został uzupełniony o metodę *execproc*, która uruchamia znajdujący się na maszynie wirtualnej gościa program, używając wywołań systemowych *vfork* oraz *execve*. Od tego momentu iniektor był już gotowy do wykorzystania przy automatycznej analizie linuksowego złośliwego oprogramowania.

Cały kod linuksowego iniektora jest dostępny w repozytorium DRAKVUF-a na GitHubie[42].

HID simulation for DRAKVUF[43]

Kontrybutor: Jan Gruber

Celem projektu było stworzenie w DRAKVUF-ie mechanizmu symulacji interakcji człowieka z systemem, której sztuczność byłaby niewykrywalna. Ma to służyć oszukaniu złośliwego oprogramowania i nakłonieniu go do ujawnienia swojego prawdziwego zachowania.

Zostało to zaimplementowane jako plugin do DRAKVUF-a o nazwie hidsim (z ang. *Human Interface Device simulator*, w skrócie *HID simulator*).

Plugin ten dostarcza trzy funkcjonalności:

1. Odtwarzanie nagranych wcześniej zdarzeń HID.
2. Wykonywanie losowych, naśladujących ludzkie, ruchów myszą.
3. Autonomiczne klikanie przycisków w pojawiających się na ekranie oknach (tylko na Windows 7).

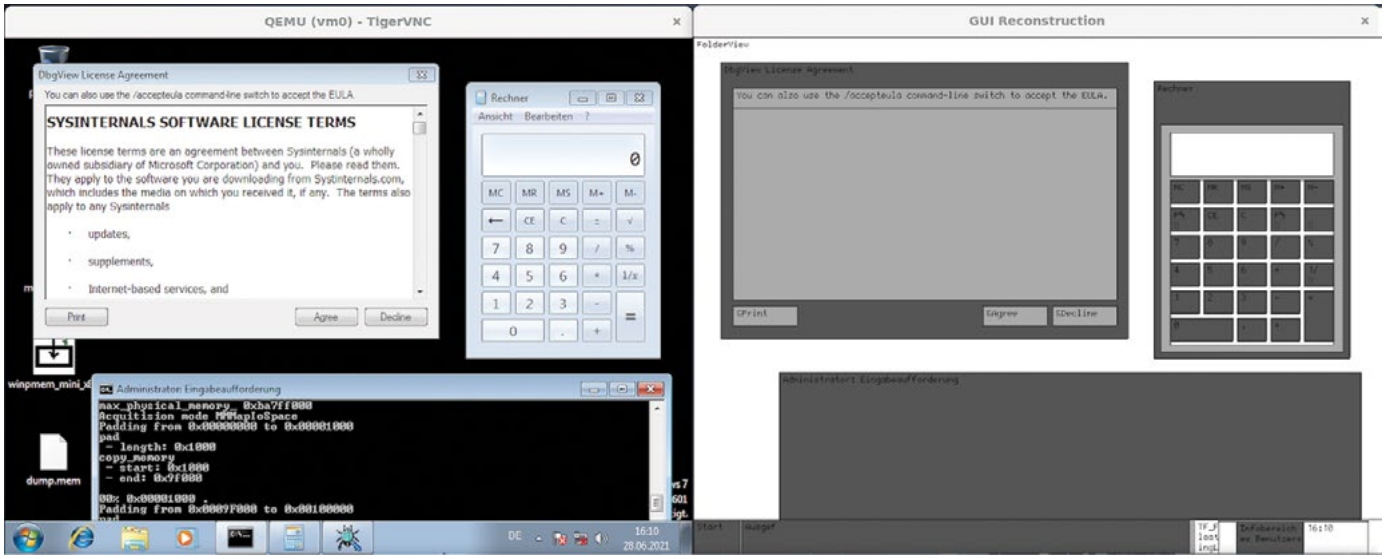
Do nagrywania szablonów sekwencji zdarzeń zostało zaimplementowane dodatkowe narzędzie o nazwie *hiddump*. Służy ono do przechwytywania zdarzeń HID w systemie Linux, a następnie umieszczania względnych i znormalizowanych wersji tych zdarzeń w pliku binarnym.

W trakcie projektu do repozytorium DRAKVUF-a zostało dodane około 3200 linii kodu oraz 700 linii komentarzy w dziesięciu pull requestach.

Oprócz powyższego wkładu w rozwój projektu DRAKVUF stworzone zostały dwa projekty pomocnicze:

- *ansible-drakvuf*[44] – automatyzacja w Ansible dla wdrożenia DRAKVUF-a na wybranym hoście,
- *vmi-reconstruct-gui*[45] – narzędzie do rekonstrukcji GUI systemu Windows 7 uruchomionego na maszynie wirtualnej pod Xenem.

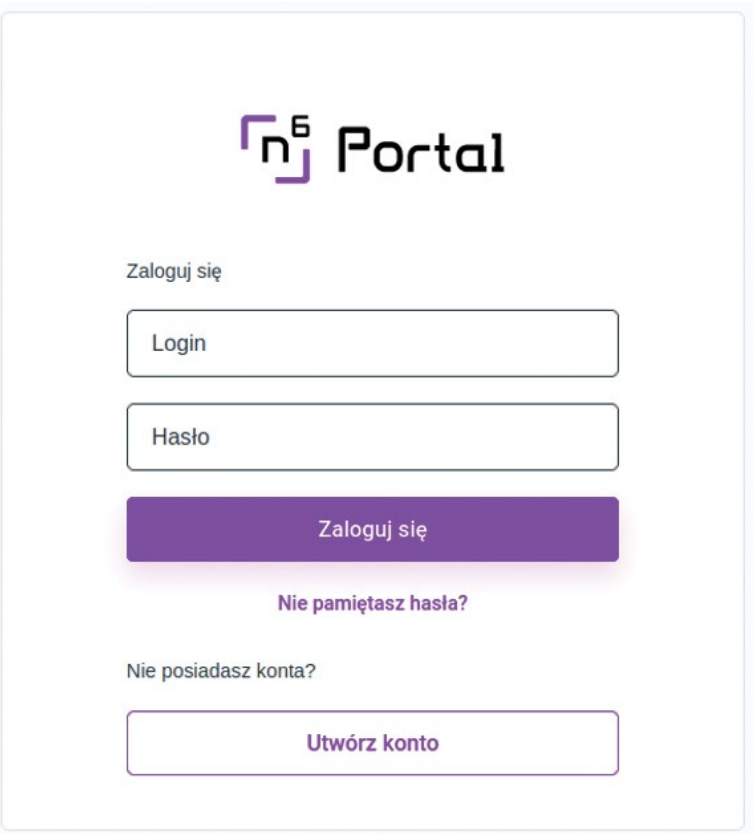
42. https://github.com/tklengyel/drakvuf/tree/master/src/libinjector/linux
43. https://cert.pl/en/posts/2021/08/hid-simulation-for-drakvuf/
44. https://github.com/jgru/ansible-drakvuf
45. https://github.com/jgru/vmi-gui-reconstruction



Rys. 14. Przykład rekonstrukcji GUI systemu Windows 7 z użyciem narzędzia vmi-reconstruct-gui[46].

n6 3.0 – nowe wydanie

W 2021 r. na licencji open source wydaliśmy dużą aktualizację systemu n6. Największą zmianą było zmigrowanie istniejącego kodu do najnowszej wersji języka Python 3. Towarzyszyły temu liczne drobne poprawki oraz porządkowanie kodu zgodnie z najnowszymi standardami. Wraz z podniesieniem wersji języka programowania, do głównej gałęzi kodu została dołączona nowa część związana z integracją podobnego do n6 narzędzia – IntelMQ. Od tej pory jest możliwe łączenie elementów obu systemów w sposób elastyczny, dopasowany do potrzeb.



Rys. 15. Ekran logowania do nowego interfejsu użytkownika.

46. https://cert.pl/uploads/2021/08/hid-simulation-for-drakvuf/vmi-gui-reconstruction.png

Kolejną dużą zmianą jest kompletnie nowy graficzny interfejs użytkownika – n6 Portal. Dodaliśmy uwierzytelnianie po haśle wraz z drugim składnikiem, interaktywny formularz zgłoszeniowy oraz pełne wsparcie dla powiadomień. Portal zyskał również swój dashboard, gdzie automatycznie prezentowane są informacje związane z incydentami w sieci organizacji.

Od tej pory ustawienia w Portalu są możliwe przez formularz do zmian konfiguracji organizacji, jak również ustawienia personalne użytkownika. Na Portalu użytkownik może zresetować swój klucz API czy zmienić drugi składnik logowania. Nowa wersja n6 zapewnia teraz wsparcie dla TOTP wraz kodami QR. n6 REST API doczekał się uwierzytelniania przy użyciu klucza API oraz drobnych optymalizacji wydajnościowych. Kod źródłowy wraz z dokumentacją można znaleźć na https://github.com/CERT-Polska/n6

Prace nad n6 były współfinansowane przez instrument Unii Europejskiej „Łącząc Europę".

MeliCERTes

Kontynuujemy rozpoczęty w 2020 r. trzyletni projekt MeliCERTes (SMART 2018/1024), czyli rozwój platformy do efektywnej wymiany informacji operacyjnych między zespołami CSIRT w celu wykrywania i zapobiegania incydentom oraz koordynowania reakcji na poziomie europejskim. Platforma jest tworzona na potrzeby europejskiej Sieci CSIRT (CSIRTs Network), w skład której wchodzą CSIRT-y krajowe wszystkich państw członkowskich UE oraz CERT-EU.

Projekt tworzony jest na zlecenie Komisji Europejskiej przez konsorcjum, które koordynujemy. Oprócz CERT Polska, w projekcie uczestniczy CERT.at, CERT-EE, CIRCL, SK-CERT oraz Deloitte.

MeliCERTes opiera się na trzech głównych filarach:

- usługi centralne dla Sieci CSIRT, gdzie kluczową rolę pełni w nim ENISA, która odpowiada za ich utrzymanie;
- narzędzia open source, które mogą być wykorzystywane lokalnie przez CSIRT-y oraz inne podmioty zajmujące się bezpieczeństwem (więcej informacji: https://github.com/melicertes/docs);
- usługi, które europejskie CSIRT-y dobrowolnie udostępniają społeczności w celu efektywniejszej walki z zagrożeniami (np. MWDB utrzymywane przez nasz zespół).

Projekty AMCE i JTAN

W grudniu 2021 r. zakończyliśmy projekt Advanced Threat Monitoring and Cooperation on the European and National Levels (AMCE), który realizowaliśmy dzięki grantowi nr 2018-PL-IA-0168 w ramach programu Unii Europejskiej „Łącząc Europę" (Connecting Europe Facility). W ramach projektu rozwinęliśmy wiele z systemów, które wykorzystujemy operacyjnie, w tym m.in.:

- platformę n6;
- platformę wymiany informacji o szkodliwym oprogramowaniu MWDB;
- system śledzenia botnetów mtracker;
- narzędzia wspomagające utrzymanie listy ostrzeżeń przed szkodliwymi stronami;
- wspólnie z fundacją Shadowserver: sieć honeypotów stworzoną w projekcie SISSDEN (https://sissden.eu/).

Duża część kodu, który powstał w efekcie tych prac, jest dostępna na otwartych licencjach na naszym koncie w serwisie GitHub: https://github.com/CERT-Polska/.

AMCE obejmowało również inne działania, takie jak organizacja Europejskiego Miesiąca Cyberbezpieczeństwa (European Cybersecurity Month, https://bezpiecznymiesiac.pl/) w Polsce, czy kwalifikacje i uczestnictwo w młodzieżowych mistrzostwach Europy w cyberbezpieczeństwie (European Cyber Security Challenge, więcej na stronie 32).

Udało nam się również zdobyć kolejny grant z programu „Łącząc Europę" i w drugiej połowie roku rozpocząć projekt Joint Threat Analysis Network (JTAN, nr grantu 2020-EU-IA-0260). W odróżnieniu od AMCE, który realizowaliśmy samodzielnie, w tym przypadku jesteśmy liderem konsorcjum europejskich CSIRT-ów.

Główny cel JTAN to rozwój narzędzi do pozyskiwania informacji (Cyber Threat Intelligence) oraz stworzenie mechanizmów, które pozwolą na sprawniejszą wymianę danych między systemami wykorzystywanymi przez CSIRT-y. Większość prac jest zaplanowana na lata 2022 – 2023, a o efektach będziemy informować na naszej stronie (http://cert.pl/) oraz w kolejnych raportach rocznych.

CyberExchange

W 2021 r. mogliśmy wznowić działania w projekcie CyberExchange, który wspiera wymianę wiedzy i doświadczeń pomiędzy europejskimi zespołami typu CERT. Oprócz CERT Polska w tej inicjatywie biorą udział zespoły z Austrii, Chorwacji, Czech, Grecji, Łotwy, Luksemburga, Malty, Rumunii i Słowacji. Liderem konsorcjum jest czeskie stowarzyszenie CZ.NIC, w ramach którego funkcjonuje CSIRT.CZ.

Projekt opiera się na krótkich stażach zagranicznych, które pozwalają specjalistom z krajowych, rządowych i akademickich zespołów reagowania na poznanie specyfiki pracy analogicznych instytucjach w innych krajach oraz nawiązanie bezpośrednich kontaktów, które są kluczowym elementem sprawnej współpracy międzynarodowej.

Pandemia COVID-19 i związane z nią ograniczenia spowodowały zablokowanie możliwości wyjazdów od pierwszego kwartału 2020 r. Wykorzystując lepszą sytuację w drugiej połowie 2021 r. udało nam się przyjąć przedstawicieli CERT.LV i CERT.hr. Głównym tematem wspólnych prac były narzędzia wspierające działania operacyjne CSIRT oraz analiza szkodliwego oprogramowania.

INCYDENTY I ZAGROŻENIA

Ransomware

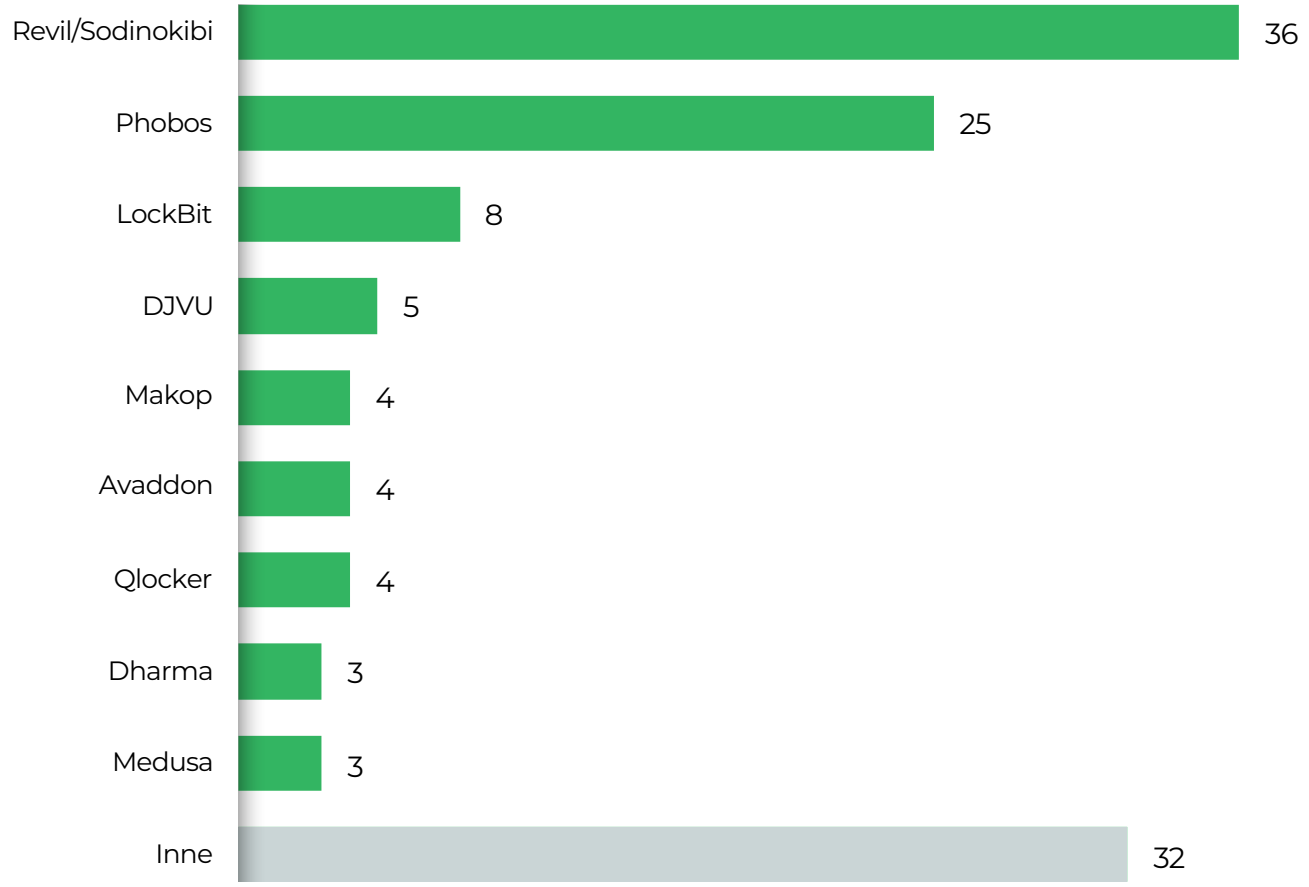
Jednym z największych zagrożeń dla cyberbezpieczeństwa w 2021 r. było ransomware, czyli szkodliwe oprogramowanie wykorzystywane do szyfrowania danych w celu wymuszenia okupu za ich odzyskanie. CERT Polska zarejestrował **124 incydenty** związane z tym zagrożeniem. Jest to niespełna **13 proc. więcej niż w roku 2020**, w którym obsłużyliśmy 110 incydentów. Biorąc pod uwagę poszczególne sektory, **największą aktywność zaobserwowano w podmiotach infrastruktury cyfrowej i wśród osób fizycznych** (po 27 incydentów) **oraz w administracji publicznej** (18 incydentów). We wszystkich sektorach **zarejestrowano 32 incydenty dotyczące podmiotów publicznych**. Wśród nich znalazły się **jednostki samorządu terytorialnego**, takie jak urzędy gminy i miasta czy **instytucje systemu opieki zdrowotnej. W sektorze prywatnym ofiarą stał się m.in. CDProjekt**, który na początku roku został zaatakowany oprogramowaniem z rodziny HelloKitty. Firma wystosowała oświadczenie, w którym poinformowała, że **zaszyfrowane dane udało się przywrócić dzięki utrzymywanym kopiom zapasowym.**

Wykres 1. Liczba zarejestrowanych incydentów w podziale na sektory.

Główne zagrożenia

Za zdecydowaną większość zaobserwowanych przez nas incydentów związanych z ransomware odpowiadają dwie rodziny szkodliwego oprogramowania: **REvil/Sodinokibi** oraz **Phobos** (odpowiednio 36 i 25 zarejestrowanych incydentów). Wśród pozostałych najczęściej występujących rodzin znalazły się: **Lockbit 2.0, STOP/DJVU, Makop, QLocker** oraz **Avaddon**.

Liczba zarejestrowanych incydentów w podziale na rodziny ransomware



Wykres 2. Liczba zarejestrowanych incydentów w podziale na rodziny ransomware.

Zaobserwowane trendy

Rozwój modelu Ransomware as a Service

Model RaaS stał się de facto standardem i przewiduje się, że w kolejnych latach nadal będzie dominował na rynku ransomware[47]. Dzięki niemu autorzy szkodliwego oprogramowania szyfrującego są w stanie poświęcić więcej uwagi jego rozwojowi, delegując wykonanie ataków do klientów. Pozwala to na wdrażanie bardziej zaawansowanych rozwiązań i usług, takich jak serwisy pozwalające na negocjacje okupów, upublicznianie wykradzionych danych czy świadczenie całodobowej pomocy atakującym.

Wielokrotne wymuszenia

Przestępcy starają się zmaksymalizować swój zysk pochodzący z pojedynczego ataku, żądając okupu nie tylko za odzyskanie zaszyfrowanych danych[48,49]. Przedmiotem negocjacji jest też możliwość ich ujawnienia lub poinformowania innych podmiotów o ataku, np. partnerów, udziałowców, organów nadzorczych czy opinii publicznej. Co więcej, jeśli atakującym udało się uzyskać dane wrażliwe klientów lub partnerów danej organizacji, oni również mogą stać się ofiarami szantażu, a uzyskane informacje mogą posłużyć do przygotowania ataku na ich urządzenia.

47. Sophos 2022 Threat Report https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2022-threat-report.pdf
48. 2021 Trends Show Increased Globalized Threat of Ransomware https://www.cisa.gov/uscert/ncas/alerts/aa22-040a
49. ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Wzrost szkód spowodowanych atakami

Ankieta przeprowadzona przez firmę Sophos[50] na początku roku wykazała, że średnia kwota strat spowodowanych atakiem ransomware wzrosła niemal dwukrotnie (z niecałych 800 tys. USD w roku 2020, do nieco ponad 1,8 miliona USD w roku 2021). Co więcej, dwie trzecie firm, które padły ofiarą ataku, odnotowały związany z nim znaczny spadek przychodów[51]. Nie bez powodu zaobserwowano też ograniczenie usług ubezpieczeniowych w zakresie cyberbezpieczeństwa, a zwłaszcza tych dotyczących ransomware[52].

Intensyfikacja działań organów ścigania

Wzrost szkód, kradzież informacji i obieranie za cele dużych korporacji spowodowały zintensyfikowanie działań organów ścigania wymierzonych w grupy cyberprzestępcze posługujące się ransomware. W niektórych przypadkach powstały międzynarodowe zespoły śledcze mające na celu identyfikację i ujęcie sprawców. Doprowadziło to do licznych aresztowań, podjęcia decyzji o zakończeniu działalności przez niektóre grupy[53] i częściowego odejścia pozostałych od przyciągających uwagę ataków[54].

Istotne rodziny ransomware

REvil/Sodinokibi

Jednym z głównych zagrożeń, zarówno w Polsce jak i na świecie[55], było oprogramowanie REvil znane również jako Sodinokibi. Zostało ono stworzone przez grupę odpowiedzialną za inną rodzinę ransomware – GandCrab. REvil był udostępniany w modelu RaaS wraz z całą infrastrukturą służącą do przygotowywania ataków, prowadzenia negocjacji z ofiarami i publikowania wykradzionych danych. Przed zaszyfrowaniem dane zidentyfikowane jako wartościowe były wykradane i wykorzystywane do podwójnego szantażu. Wśród ofiar znalazły się między innymi Acer[56] i Quanta Computer współpracująca z Apple[57]. Najpoważniejszym w skutkach był atak na firmę Kaseya, której oprogramowanie Kaseya VSA posłużyło do zainfekowania korzystających z niego niemal 1500 klientów[58]. Dokonano tego za pomocą ataku typu supply chain, w którym złośliwy kod był dystrybuowany wraz z aktualizacją oprogramowania. Dzięki współpracy 17 państw, Europolu, Eurojust i agencji INTERPOL aresztowano siedem osób powiązanych z grupą odpowiedzialną za REvil[59]. Udało się również stworzyć uniwersalne dekryptory, które pozwoliły na odzyskanie danych ponad 50 000 ofiar REvil/Sodinokibi i GandCrab. Narzędzie jest dostępne na stronie projektu No More Ransom[60].

Conti

Conti jest dystrybuowane przy wykorzystaniu spear-phishingu, wykradzionych lub słabych danych uwierzytelniających do RDP czy podatnych usług. W pierwszej kolejności wykorzystywane są takie narzędzia jak TrickBot czy Cobalt Strike, a sam ransomware używany jest już po uzyskaniu dostępu do większej liczby maszyn i transferze informacji zidentyfikowanych jako wrażliwe[61]. Dane zebrane na stronie projektu Ransomwhere[62] wskazują, że Conti przyniosło cyberprzestępcom największe zyski spośród wszystkich rodzin ransomware. Tylko w 2021 r. było to kilkanaście milionów USD. W 2022 r. doszło do znacznego wycieku informacji na temat grupy odpowiedzialnej za Conti, obejmującego kilkuletnią korespondencję i inne wrażliwe dane[63].

50. The State of Ransomware 2021 https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf
51. Ransomware: the true cost to business, https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf
52. Insurers run from ransomware cover as losses mount https://www.reuters.com/markets/europe/insurers-run-ransomware-cover-losses-mount-2021-11-19/
53. ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
54. 2021 Trends Show Increased Globalized Threat of Ransomware https://www.cisa.gov/uscert/ncas/alerts/aa22-040a
55. IBM X-Force Threat Intelligence Index 2022 https://www.ibm.com/security/data-breach/threat-intelligence/
56. Computer giant Acer hit by $50 million ransomware attack https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by--50-million-ransomware-attack/
57. REvil gang tries to extort Apple, threatens to sell stolen blueprints https://www.bleepingcomputer.com/news/security/revil-gang-tries-to-extort-apple-threatens-to-sell-stolen-blueprints/
58. Kaseya: Roughly 1,500 businesses hit by REvil ransomware attack https://www.bleepingcomputer.com/news/security/kaseya-roughly-1-500-businesses-hit-by-revil-ransomware-attack/
59. Five affiliates to Sodinokibi/REvil unplugged https://www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil--unplugged
60. The No More Ransom Project https://www.nomoreransom.org
61. Conti Ransomware https://www.cisa.gov/uscert/ncas/alerts/aa21-265a
62. Ransomwhere Project https://ransomwhe.re/
63. Conti Ransomware Group Diaries, Part I: Evasion https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/

Hive

Ransomware Hive odpowiada za jedną z najwyższych kwot okupu w historii cyberprzestępczości. W listopadzie 2021 r. jego ofiarą padła międzynarodowa sieć sklepów Media Markt, a żądania opiewały na kwotę 240 milionów USD. Hive działa w modelu RaaS, a wykradzione dane publikowane są w przygotowanym przez twórców serwisie, na który trafiło już kilkadziesiąt firm. Badaczom z Group-IB udało się uzyskać dostęp do panelu administratora wykorzystywanego przez przestępców, dzięki czemu upublicznione zostały liczne informacje dotyczące działań grupy[64]. Mimo, że Hive stał się aktywny dopiero w drugiej połowie roku, do połowy października jego ofiarami padło co najmniej 355 organizacji.

Poradnik dotyczący ransomware

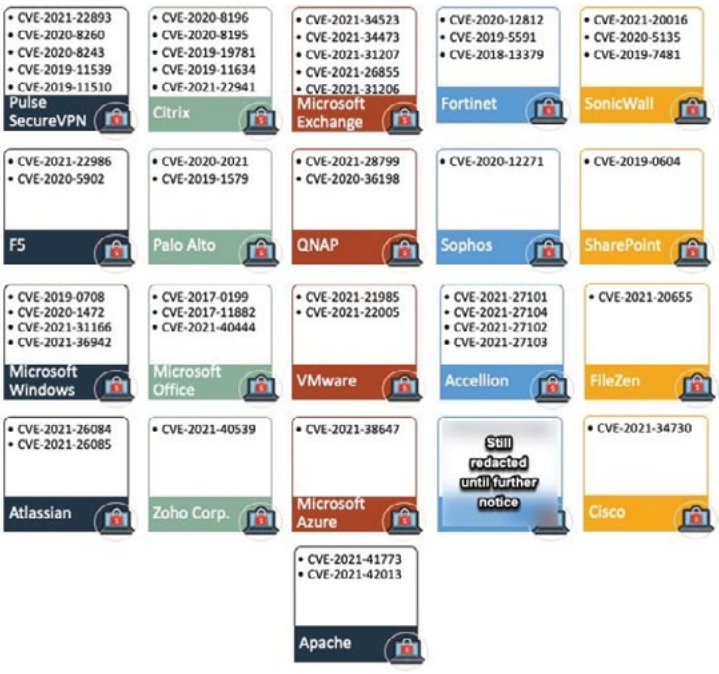
Zachęcamy do zapoznania się z przygotowanym przez nasz zespół poradnikiem dotyczącym ransomware. Opisujemy w nim działania, które można podjąć w celu przygotowania się na ten rodzaj zagrożenia, jak i czynności, które należy wykonać po stwierdzeniu infekcji. Poradnik dostępny jest na stronie CERT Polska: https://www.cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf.

Najważniejsze podatności w 2021 roku

Rok 2021 był wypełniony poważnymi podatnościami, które bardzo szybko były adaptowane i wykorzystywane przez cyberprzestępców, w szczególności przez grupy ransomware. Obserwujemy wyraźny trend wzrostu wykorzystania podatności w oprogramowaniu używanym przez firmy np. Microsoft Exchange czy VMware vCenter, względem tych w oprogramowaniu wykorzystywanym przez użytkownika końcowego, takich jak pakiet Office czy przeglądarka.

W 2021 r. w bazie NVD prowadzonej przez NIST zostało opublikowanych 21 957 podatności. Jest to znaczny wzrost względem roku 2020 (3,5 tys. więcej). Należy jednak zaznaczyć, że mimo tak dużej liczby zgłoszonych podatności, na dzień pisania raportu aktywnie wykorzystywanych wg. CISA[65] było tylko 326.

Grupy przestępcze nie ograniczają się tylko do podatności ujawnionych w danym roku. Na rysunku nr 16 pokazano luki najczęściej wykorzystywane przez grupy ransomware (stan na październik 2021 r.). Polecamy również zapoznać się z listą podatności obecnie aktywnie wykorzystywanych w atakach, na bieżąco aktualizowaną przez CISA: https://www.cisa.gov/known-exploited-vulnerabilities-catalog



Rys. 16. Podatności najczęściej wykorzystywane przez ransomware w 2021 roku[66].

64. Inside the Hive https://blog.group-ib.com/hive
65. Known exploited vulnerabilities catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog
66. https://twitter.com/pancak3lullz/status/1447644282614161412/photo/1

Zdecydowanie najgłośniejszą podatnością 2021 r. była podatność w bibliotece Log4j, znana jako Log4Shell. Mimo to z naszych obserwacji wynika, że najwięcej udanych ataków spowodowały podatności w Microsoft Exchange, znane pod nazwami ProxyLogon i ProxyShell, których skutki obserwujemy do tej pory. Często takie ataki są obserwowane z opóźnieniem. Wynika to z tego, że grupy przestępcze odsprzedają uzyskane dostępy, a incydent zostaje zauważony i zgłoszony, dopiero gdy uzyska go grupa, która spieniężа uzyskany dostęp, np. instalując ransomware.

Log4Shell

Pod koniec 2021 r. świat obiegła informacja o krytycznej podatności w jednej z najczęściej używanych bibliotek do logowania zdarzeń, wykorzystywanej przez aplikacje napisane w języku Java – Apache Log4j. Niedługo po wydaniu poprawki pojawiały się informacje o kolejnych problemach, co ostatecznie doprowadziło do publikacji czterech CVE opisanych w tabeli 4.

CVE	Podatne wersje Log4j	Opis
CVE-2021-44228	2.0-beta9 do 2.14.1. Z wyłączeniem 2.12.2-2.12.*	Pierwsza podatność, znana jako "Log4shell". Pozwala na zdalne wykonanie kodu.
CVE-2021-45046	2.0-beta9 do 2.15.0. Z wyłączeniem 2.12.2-2.12.*	Podatność będąca obejściem poprawki wdrożonej w wersji 2.15.0. Pozwala na zdalne wykonanie kodu.
CVE-2021-45105	2.0-alpha1 do 2.16.0 Z wyłączeniem 2.3.1 i 2.12.3-2.12.*	Podatność pozwala na atak odmowy dostępu.
CVE-2021-44832	2.0-beta7 do 2.17.0 Z wyłączeniem 2.3.2 i 2.12.4-2.12.*	Podatność pozwala na zdalne wykonanie kodu w przypadku możliwości edycji konfiguracji logowania. Takie zagrożenie występuje bardzo rzadko.

Tab. 4. Podatności w bibliotece Log4j ujawnione w 2021 r.

Głównym zagrożeniem związanym z Log4Shell jest możliwość zdalnego wykonania kodu, którego wykorzystanie (zależnie od konfiguracji) może być bardzo proste. Zdecydowanie jest to podatność, która w 2021 roku zyskała największy rozgłos i spowodowała łatanie systemów na niespotykaną nigdy wcześniej skalę.

W ramach działań zapobiegających skutkom wykorzystania tej podatności:

- Na stronie zamieściliśmy codziennie aktualizowane rekomendowane działania w związku z podatnością. Można się z nimi zapoznać pod adresem. https://cert.pl/posts/2021/12/krytyczna-podatnosc-w-bibliotece-apache-log4j/
- Rozesłaliśmy ostrzeżenie do właściwych sektorów poprzez organy właściwe, CSIRT-y poziomu krajowego, KRPM oraz RCB z prośbą o dalszą dystrybucję.
- W ramach dostępnej listy osób kontaktowych zgłoszonych w ramach ustawy o KSC rozesłaliśmy ostrzeżenia do **2976** podmiotów. Zostało wysłanych łącznie **6463** indywidualnych powiadomień.
- Opublikowaliśmy ostrzeżenie w ramach systemu S46.

VMware vCenter

Oprogramowanie VMware vCenter wykorzystywane jest do scentralizowanego zarządzania platformą wirtualizacyjną vSphere. Jest to produkt bardzo często wykorzystywany przez większe organizacje, które posiadają własne serwerownie. Uzyskanie do niego dostępu często oznacza przejęcie większości infrastruktury firmy.

W 2021 r. pojawiły się aż trzy poprawki na krytyczne podatności w VMware vCenter (CVE-2021-21972, CVE-2021-21985, CVE-2021-22005), które były potem wykorzystywane w masowych atakach. Każda z nich pozwalała na zdalne wykonanie kodu bez uwierzytelniania.

Są to dobre przykłady jak szybko takie poprawki są analizowane przez atakujących. W przypadku dwóch podatności (CVE-2021-21985, CVE-2021-22005) od momentu publikacji ostrzeżenia przez VMware do wykorzystania ich w atakach minęło zaledwie kilka dni. Również bardzo szybko publicznie pojawiły się gotowe do wykorzystania exploity.

Mimo że dostęp do vCenter powinien być ograniczony tylko do sieci administracyjnej, w internecie można znaleźć znaczną liczbę instancji dostępnych publicznie. **W Polsce było to ponad 300 przypadków.** W kwestii obu podatności informowaliśmy właścicieli takich serwerów o konieczności natychmiastowej aktualizacji i przekazaliśmy rekomendacje, że nie powinny być one dostępne z poziomu internetu.

Microsoft Exchange

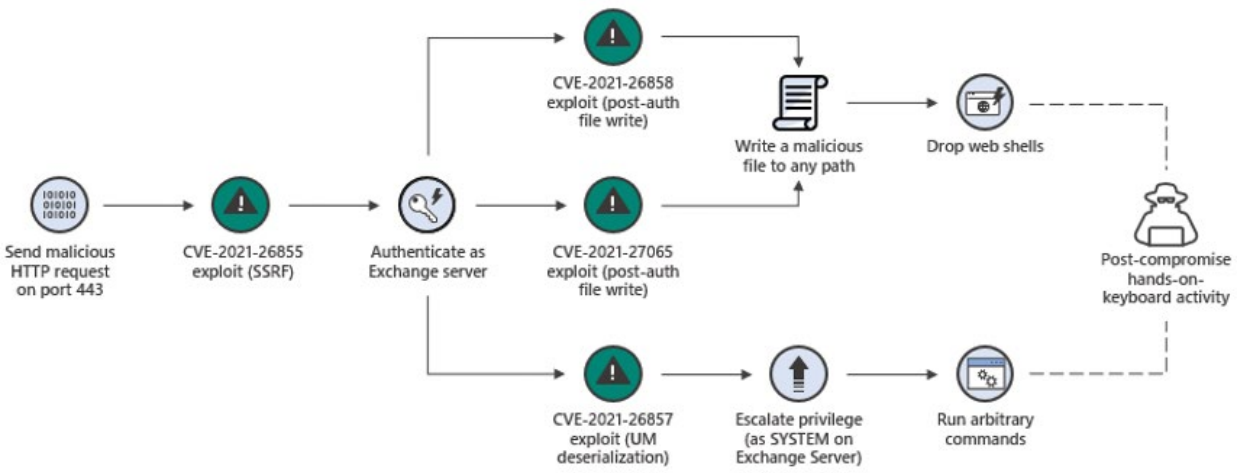
Microsoft Exchange jest najpopularniejszym korporacyjnym serwerem pocztowym, używanym przez największe firmy na świecie. Przejmując nad nim kontrolę, atakujący nie tylko uzyskuje dostęp do wiadomości mailowych całej organizacji, ale też często ma możliwość przejęcia kontrolera domeny.

W 2021 r. zostały opublikowano aż dwie grupy krytycznych podatności pozwalających na zdalne wykonanie kodu: ProxyLogon i ProxyShell.

ProxyLogon

Główna podatność znana pod nazwą ProxyLogon to CVE-2021-26855. Pozwala ona na ominięcie uwierzytelniania i wykonywanie poleceń jako administrator w MS Exchange. Razem z nią ujawnione zostały trzy podatności prowadzące do zdalnego wykonania kodu na poziomie systemu operacyjnego, korzystając z wcześniej zdobytego dostępu administracyjnego (CVE-2021-26857, CVE-2021-26858, CVE-2021-27065).

Ciekawostką jest, że wg. zespołu DEVCORE, który odkrył tę podatność, zostały one zgłoszone do Microsoftu już w styczniu 2021 r., ale nie zostały załatane przez kolejne 3 miesiące[67]. Okazało się, że w międzyczasie, kiedy jeszcze nie było wydanej poprawki, luki zaczęły być wykorzystywane przez jedną z grup APT – HAFNIUM. Od tego momentu sprawy bardzo przyspieszyły. Microsoft wydał w trybie natychmiastowym poprawki, a w ciągu kilku dni pojawiły się publicznie dostępne przykłady jak wykorzystać podatność do ataków. Bardzo krótki czas pomiędzy wydaniem poprawki a pojawieniem się publicznych exploitów na tak ważny komponent wielu firm jakim jest serwer pocztowy, spowodował lawinę ataków zarówno przez grupy APT, jak i ransomware. Na rys. 17 pokazano w jaki sposób wspomniane podatności były łączone i wykorzystywane podczas ataków.



Rys. 17. Sposób wykorzystania podatności ProxyLogon przez atakujących[68].

67. https://proxylogon.com/
68. https://www.microsoft.com/security/blog/2021/03/25/analyzing-attacks-taking-advantage-of-the-exchange-server-vulnerabilities/

Według dobrych praktyk, bezpośredni dostęp do panelu logowania MS Exchange z internetu nie powinien być możliwy, ale niestety jest to częsta, zła praktyka. W ramach naszych działań, widząc powagę problemu, od momentu ujawnienia podatności codziennie skanowaliśmy polską adresację IP w poszukiwaniu podatnych serwerów. W kolejnych dniach szukaliśmy również webshselli pozostawionych przez atakujących pod znanymi ścieżkami. Przedstawiamy kilka statystyk z tego okresu:

- Liczba instancji MS Exchange w polskiej adresacji, które były przynajmniej raz potwierdzone jako podatne: **1784**.
- Liczba instancji MS Exchange w polskiej adresacji, które były nadal podatne w momencie masowego wykorzystywania podatności: **453** – z bardzo dużym prawdopodobieństwem doszło w nich do włamania.
- Liczba instancji MS Exchange z zainstalowanym backdoorem (webshellem): **159** – są to potwierdzone włamania. Liczba jest znacznie zaniżona, bo skanowanie opierało się tylko na znanych ścieżkach webshelli.
- Liczba powiadomień wysłana do organizacji: **975** (niektóre organizacje posiadały kilka serwerów).
- Eskalacja bezpośrednia (włącznie z telefonicznym ustalaniem odpowiedzialnego administratora): około **100**.

ProxyShell

W sierpniu 2021 r. badacz bezpieczeństwa Orange Tsai z zespołu DEVCORE opublikował kolejny zestaw podatności w MS Exchang[69]. Główna podatność CVE-2021-34473 pozwalała na ominięcie uwierzytelniania, a następnie za pomocą podatności CVE-2021-34523 i CVE-2021-31207 podnoszone były uprawnienia i wgrywany webshell. Na szczęście tym razem podatność została załatana przez Microsoft z 3-miesięcznym wyprzedzeniem przed publikacją, co dało wielu organizacjom czas potrzebny na jej załatanie. Skutki tej luki zmniejszyło również to, że po doświadczeniach z *ProxyLogon* wiele firm ograniczyło dostęp do poczty tylko po zalogowaniu się do VPN-a. W polskiej adresacji również wykryliśmy znacznie mniej podatnych serwerów:

- Liczba instancji MS Exchange w polskiej adresacji, które były przynajmniej raz potwierdzone jako podatne: **240**.
- Liczba powiadomień wysłana do organizacji: **83** (niektóre organizacje posiadały kilka serwerów).

Ze skutkami tych podatności i liczbą zaatakowanych wtedy serwerów mierzymy się do tej pory. Często zdarza się, że po otrzymaniu zgłoszenia o zaszyfrowaniu przez ransomware, okazuje się, że kilka miesięcy wcześniej organizacja była powiadamiana o podatnej instancji MS Exchange, czy nawet o wykryciu przez nas webshella, ale podjęła niewystarczające działania, aby usunąć wszystkie tylne furtki pozostawione przez atakującego.

Ewolucja znanych kampanii phishingowych

Ubiegły rok upłynął dla przestępców zajmujących się phishingiem pod znakiem doskonalenia dobrze działających schematów. Znacząca część odnotowanych incydentów dotyczyła wariantów kampanii, które pojawiły się w latach poprzednich.

Przejmowanie kont na Facebooku

W 2021 r. ataki phishingowe na użytkowników Facebooka funkcjonowały głównie w dwóch wariantach. Najpopularniejszy z nich rozprzestrzeniał się za pomocą postów w grupach tematycznych. Najczęstszym celem były grupy otwarte posiadające dużą liczbę członków, zazwyczaj lokalne (miejskie, gminne) lub handlowe typu "sprzedam/wymienię/oddam".

Ogłoszenie wykorzystywane do ataku ma prostą strukturę. Składa się z krótkiego wyrażenia opisującego emocje (strach, oburzenie, prośbę o pomoc) oraz linku do fałszywej strony. W całym procesie ważną rolę odgrywa mechanizm tagów Open Graph, dzięki któremu pojawia się w poście odpowiednia miniaturka, domena oraz tytuł strony. Twórcy niektórych wersji phishingu zauważyli nieścisłość w interpretacji mechanizmu OGTags[70] ze strony Facebooka, co pozwala na sfałszowanie wyświetlanej nazwy domenowej. Efekt tego błędu można zauważyć na rys. 18.

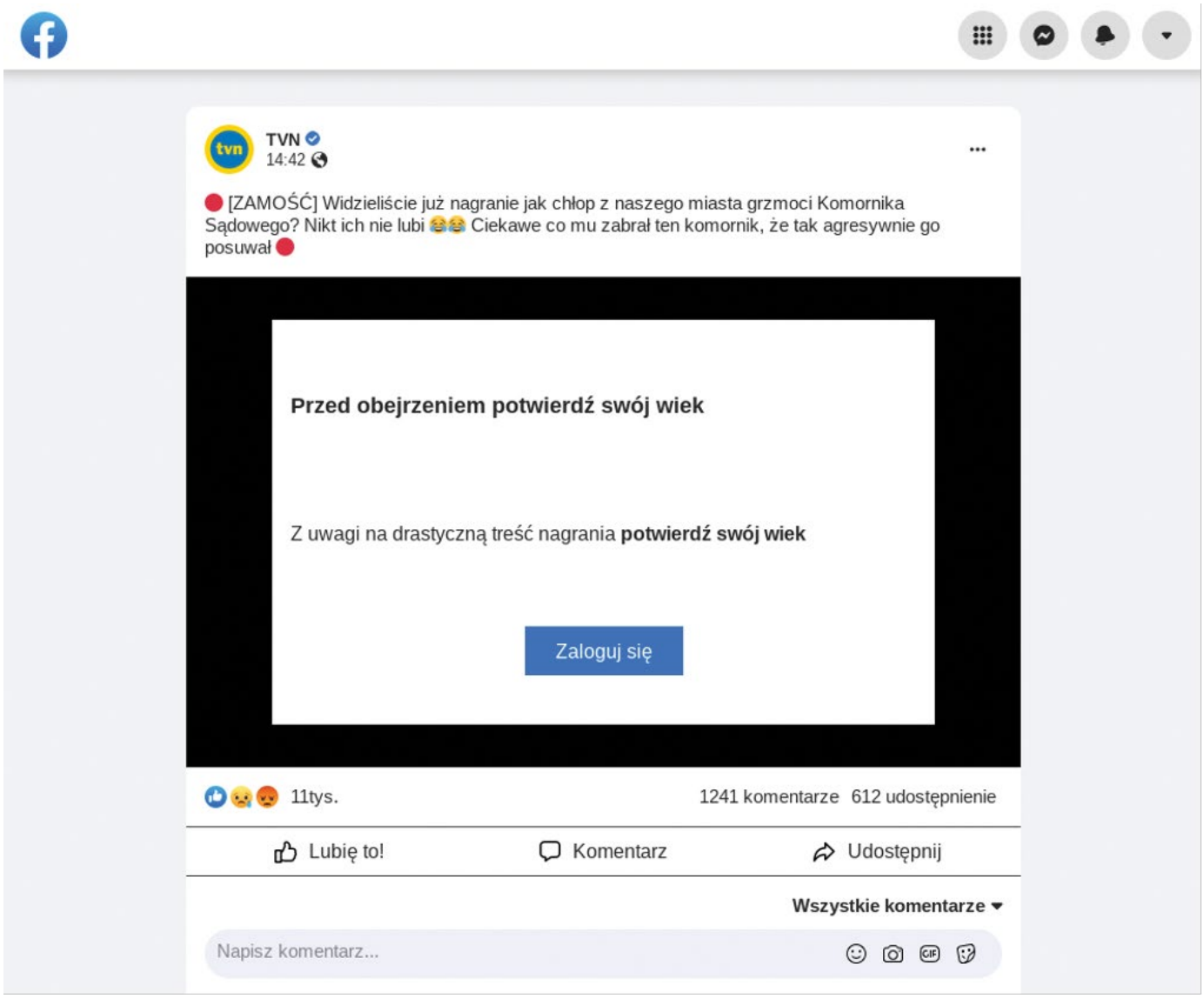
69. https://www.zerodayinitiative.com/blog/2021/8/17/from-pwn2own-2021-a-new-attack-surface-on-microsoft-exchange-proxyshell
70. The Open Graph Protocol https://ogp.me/

Rys. 18. Post phishingowy sugerujący, że link prowadzi na stronę wiadomosci.wp.pl.

Tematyka posta dotyczy sensacyjnej wiadomości. Najczęściej jest to porwanie, morderstwo, pobicie lub gwałt. Warto zwrócić uwagę na dostosowanie wyświetlanego tytułu strony do nazwy grupy lokalnej. W przykładowej grupie "Mieszkańcy Raszyn" tytuł na miniaturce brzmiałby "3-latek z Raszyn zaginął. Rodzice błagają o pomoc". Poza wymienionymi wyżej kategoriami informacji, zauważyliśmy bardzo szybką adaptację do aktualnej sytuacji społecznej, np. informacje o zmianach w programie 500+ czy rzekome komplikacje po przyjęciu szczepionki firmy Johnson&Johnson.

Rys. 19. Fałszywy post dopasowany do nazwy grupy.

Spreparowane strony składają się z 2 elementów: części informacyjnej mającej zawierać drastyczny film, który można obejrzeć po potwierdzeniu wieku, oraz fałszywego panelu logowania do Facebooka – rzekomej metody weryfikacji. Początkowo pierwszy etap wyłudzenia starał się wyglądem imitować znany portal z newsami, lecz na przestrzeni roku wyewoluował – przez postać bliżej nieokreślonego portalu społecznościowego, do ostatecznej formy przypominającej widok pojedynczego postu na Facebooku. Cały proces opiera się na imitacji mechanizmu logowania się do aplikacji poprzez powiązanie konta z kontem Facebookowym.



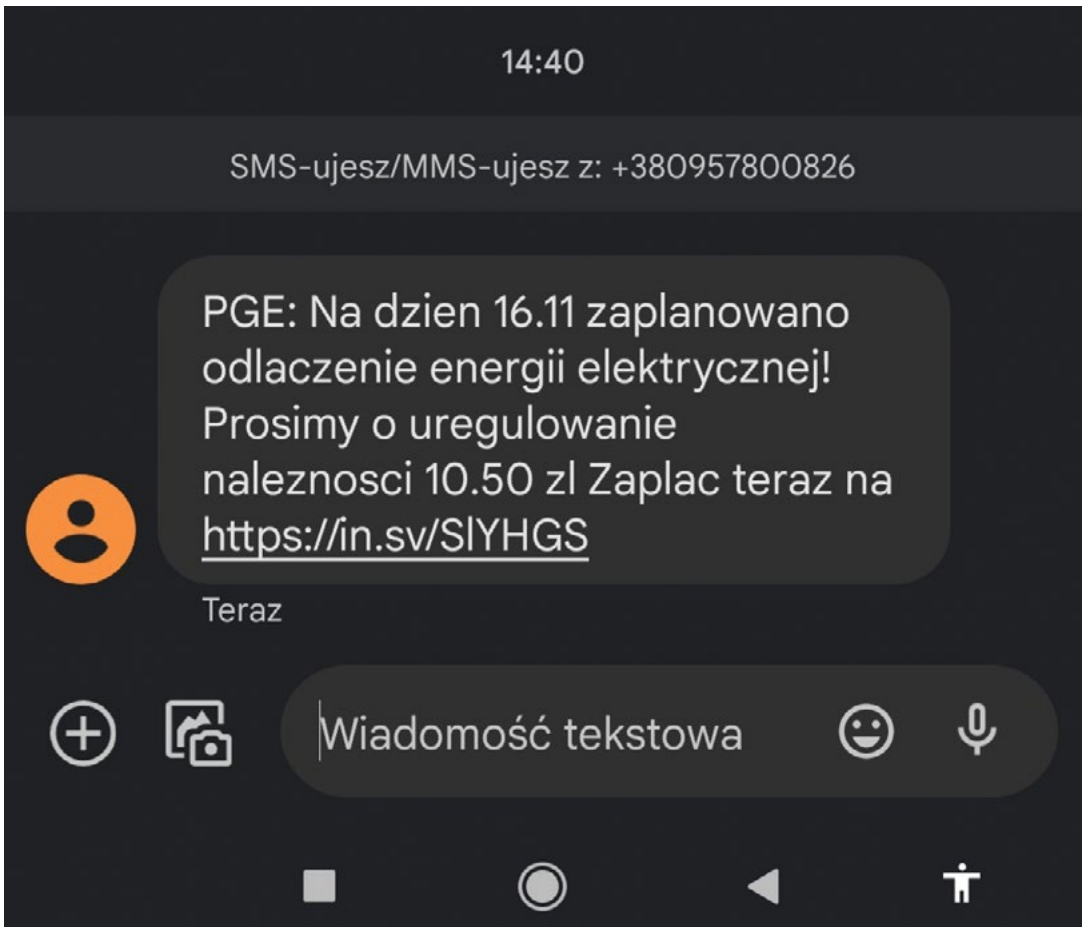
Rys. 20. Fałszywa strona z drastycznym filmem przypominająca post na Facebooku.

Drugą zauważalną grupą ataków phishingowych ukierunkowanych na przejęcie kont platformy Facebook były rzekome głosowania i konkursy. Schemat jest prostszy od opisanego powyżej. Polega on na wysłaniu wiadomości do znajomych z przejętego już konta z prośbą o udział w loterii pod załączonym linkiem. Oczywiście przesłany URL prowadzi do fałszywego panelu logowania. Ciekawym aspektem tej kampanii jest to, że phishing można zobaczyć tylko z mobilnych urządzeń.

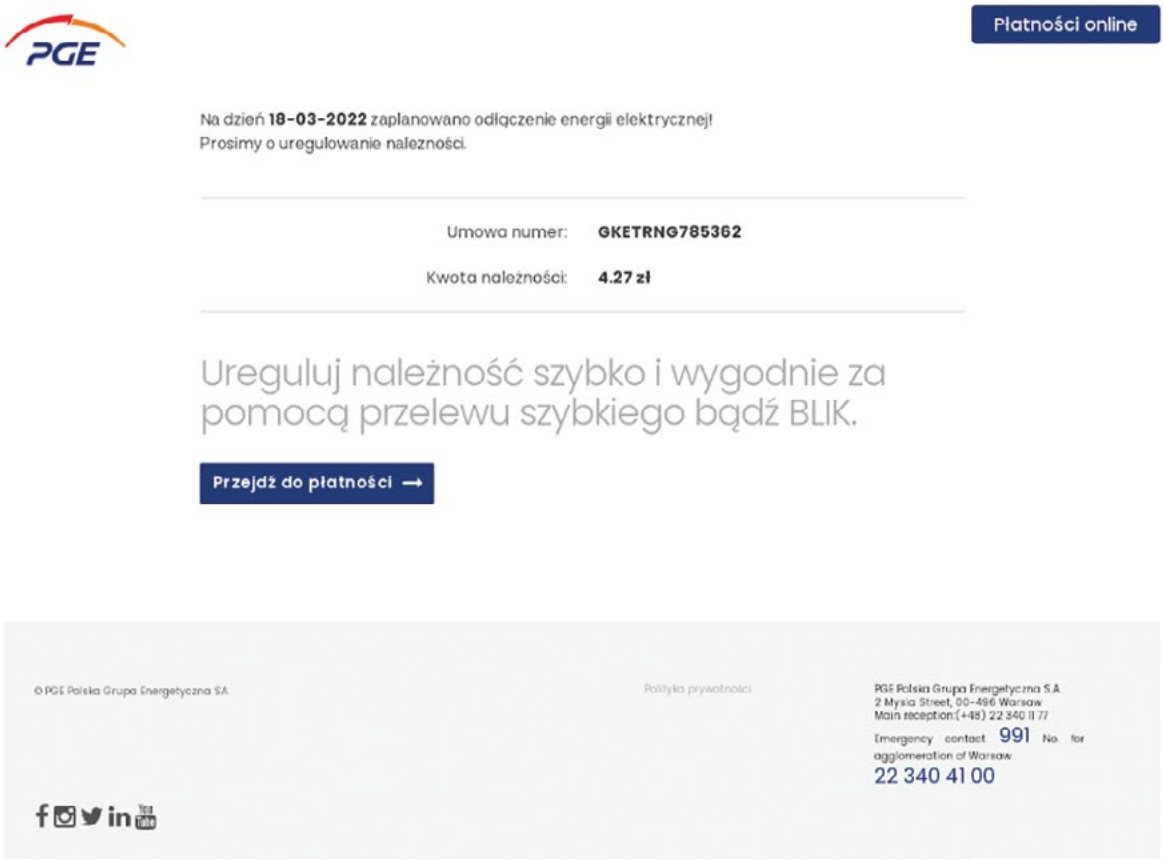
Mimo że obserwujemy rosnącą liczbę phishingów gromadzących dane kont Facebook, to nie ma jasnego motywu korzyści finansowych z prowadzonych kampanii. Jest to zmiana w stosunku do lat poprzednich, kiedy dochodziło do np. wyłudzania kodu BLIK od znajomych przejętego konta. Niektóre z wariantów opisywanego schematu wydają się być powiązane z oszustwami inwestycyjnymi, które zostały opisane w rozdziale "Oszustwa i fałszywe inwestycje". Pozyskane w ten sposób profile służą także do dalszego rozprzestrzeniania wiadomości phishingowych.

Fałszywe bramki płatności

W 2021 r. wzrosła liczba ataków phishingowych wykorzystujących motyw fałszywych bramek płatności, choć procentowy udział tego scenariusza wśród wszystkich wyłudzeń zmalał. Nasz zespół zarejestrował najwięcej incydentów realizowanych według schematu, który zaobserwowano pod koniec 2020 r. W jego skład wchodzi SMS, panel informujący o potrzebie dopłaty oraz fałszywa bramka płatności wykorzystująca wizerunek firmy eCard. Wiadomość phishingowa zawiera informację o potrzebie dopłaty za wskazaną usługę oraz link do rzekomej płatności. Na przestrzeni roku przestępcy przeszli od bezpośredniego przesyłania docelowej domeny do korzystania z charakterystycznych skracaczy linków w domenach .sv i .co. W tej kampanii zauważyliśmy wykorzystanie 3 motywów: dopłata do przesyłki firmy InPost, opłata za energię elektryczną od PGE oraz opłata za gaz od PGNiG. W kwietniu fałszywy panel eCard, który do tej pory wyłudzał tylko dane do kont bankowych, został poszerzony o możliwość "płatności" BLIKIEM.



Rys. 21. Wiadomość SMS sugerująca konieczność dopłaty za prąd.



Rys. 22. Fałszywa strona z komunikatem o konieczności dopłaty za prąd prowadząca do bramki płatności.

Poza tym dominującym na przestrzeni roku schematem, zauważalne były także pomniejsze kampanie, które wykorzystywały wizerunek bramki płatności PayU. Scenariusz jest niezmienny od kilku lat, polega na rozesłaniu za pomocą SMS-a linku do fałszywej strony. Dołączana jest do tego treść wykorzystująca różne motywy mające całość uwiarygodnić. W tym roku wśród najczęściej pojawiających się tematów tych wiadomości znalazły się:

- opłacenie mandatu,
- dopłata ze względu na złe rozliczenie podatku,
- loteria szczepień.

Ta kampania, w przeciwieństwie do opisanej powyżej, nie działała na przestrzeni całego roku, tylko bazowała na krótkich okresach 2–3-dniowych, podczas których masowo rozsyłano SMS-y.

Wyłudzanie pieniędzy od sprzedawców na portalach ogłoszeniowych

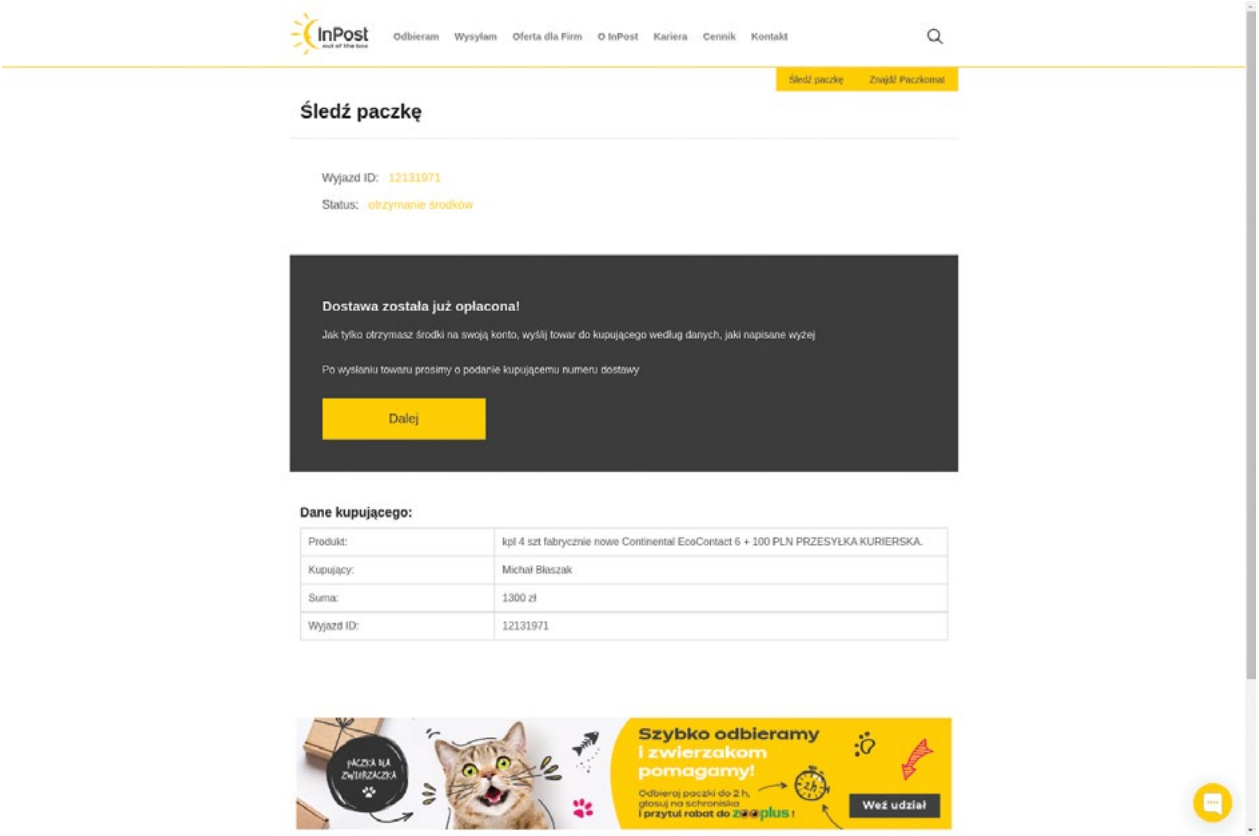
Zdecydowanym liderem wśród schematów phishingowych jest ten skierowany nie na klienta, a na sprzedawcę. Tego typu atak po raz pierwszy pojawił się pod koniec 2020 r. i od tego czasu prężnie się rozwijał. Prawdopodobnie największym czynnikiem wpływającym na jego sukces jest poszukiwanie ofiar wśród sprzedawców, co dodaje całemu przedsięwzięciu wiarygodności. Atakowana osoba rzeczywiście sprzedaje przedmiot będący celem rozmowy i spodziewa się kontaktu ze strony nieznajomego. Dodatkowo na rozwój tego schematu wpłynęła również pandemiczna rzeczywistość oraz wspieranie możliwości zdalnych zakupów przez portale ukierunkowane na handel lokalny z odbiorem własnym.

Początkowo potencjalnymi ofiarami były osoby sprzedające przedmioty na portalu OLX. Dostawały one link do fałszywej strony, na której widniał komunikat o zakupie sprzedawanego przedmiotu oraz przycisk do odebrania przelanych pieniędzy. Kierował on do strony wyłudzającej dane karty kredytowej. Z upływem czasu zaczęły pojawiać się dodatkowe elementy wyłudzenia tj. fałszywe panele logowania do bankowości online (niektóre banki wymagają zalogowania w celu potwierdzenia transakcji kartą) czy czat z pracownikiem przeprowadzającym użytkownika przez proces oszustwa.

W pierwszych miesiącach 2021 r., poza wykorzystywaniem wizerunku firmy OLX, zaczęły pojawiać się fałszywe strony podszywające się pod firmę kurierską InPost oraz Pocztę Polską, na których wyświetlane były informacje o wybranym sposobie dostawy przez rzekomego kupującego. Następnie celem przestępców stali się ogłoszeniodawcy korzystający z innych platform:

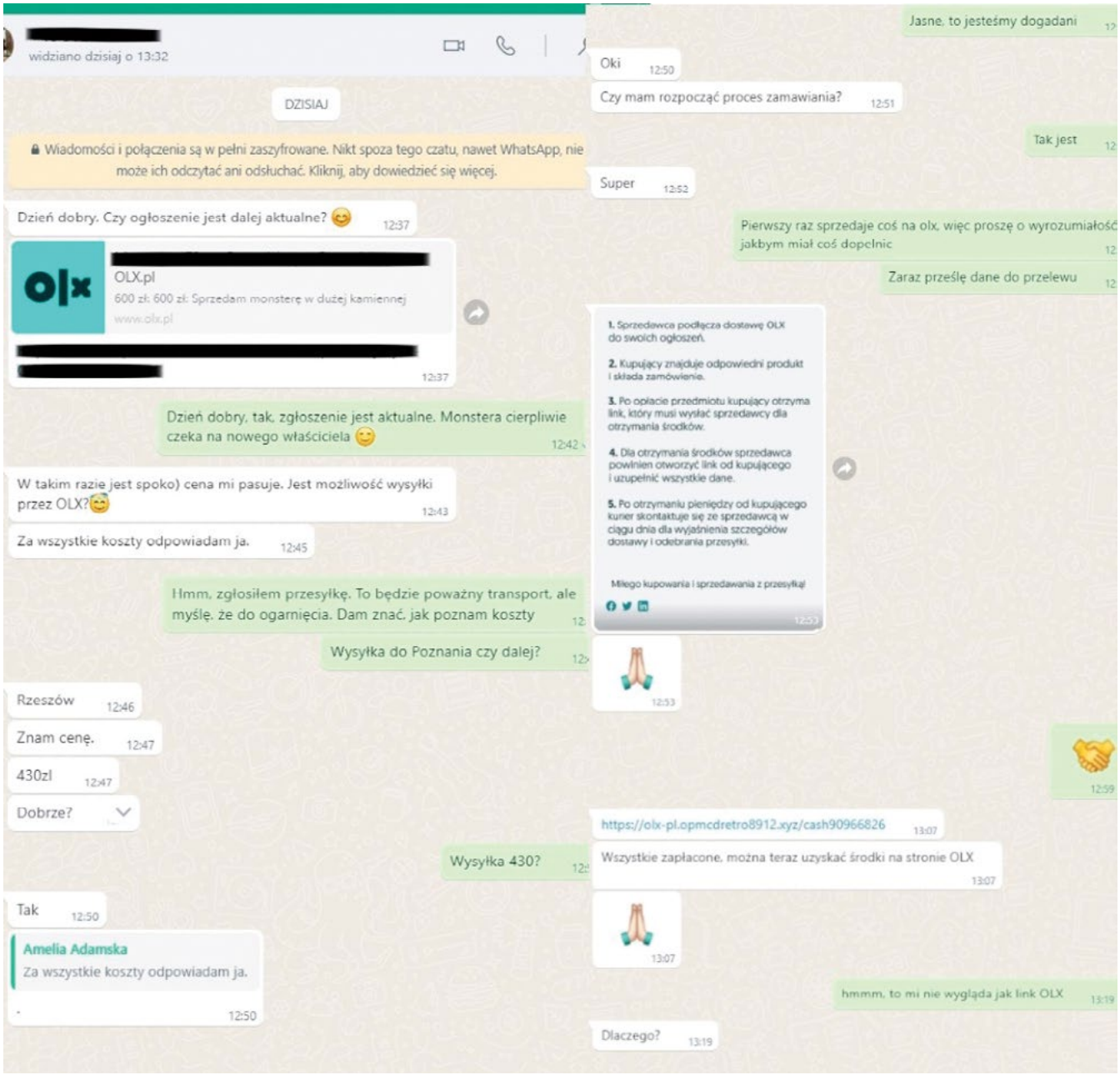
- Vinted – handel używaną odzieżą,
- Blablacar – odpłatne przewozy osób w trakcie prywatnych podróży,
- Booking – wynajem krótkoterminowy.

We wszystkich przypadkach metoda pozostawała niezmienna. Przestępcy informowali, że ktoś skorzystał z naszego ogłoszenia i zachęcali do kliknięcia w link, aby odebrać pieniądze.



Rys. 23. Przykładowa fałszywa strona wykorzystująca wizerunek InPost.

Do dystrybucji złośliwych linków początkowo wykorzystywano aplikację WhatsApp. Najpierw osoba kontaktująca się przesyłała odnośnik do prawdziwej oferty z zapytaniem czy jest nadal aktualna. Po zaangażowaniu ofiary w rozmowę symulującą chęć zakupu przedmiotu, oszust wysyłał link do strony phishingowej. Z czasem zaczęły pojawiać się inne sposoby, takie jak powiadomienie e-mail czy zwykły SMS. Większość fałszywych stron dotyczyła ofert przedmiotów, które mogą sugerować, że sprzedawcy zależy na szybkiej sprzedaży przedmiotu. Najpopularniejszymi kategoriami były ubrania, akcesoria dziecięce, elektronika oraz biżuteria.



Rys. 24. Rozmowa z osobą rzekomo zainteresowaną zakupem.

Trojany mobilne w Polsce

Rynek urządzeń mobilnych z roku na rok powiększa się i ten trend w 2021 r. również został zachowany. Według raportu Digital 2021[71] między styczniem 2020 r. a styczniem 2021 roku liczba użytkowników urządzeń mobilnych na świecie zwiększyła się o 93 miliony, co oznacza wzrost o 1,8 proc. Z raportu wynika, że rynek urządzeń mobilnych został zdominowany przez dwa systemy operacyjne – Android, który w grudniu 2020 r. wykorzystywany był przez 72,5 proc. urządzeń, oraz iOS, używany w 26,9 proc. smartfonów.

Według badania zleconego przez UKE, w roku 2021[72] 96,9 proc. ankietowanych korzystało z telefonu komórkowego, z czego 80,4 proc. ze smartfona. Warto też odnotować, że blisko 74 proc. użytkowników spotkało się z usługą automatycznych SMS-ów. Zdecydowanie najwięcej respondentów (ponad 90 proc.) otrzymywało automatyczne powiadomienia dotyczące alertów RCB, zaś nieco ponad 50 proc. otrzymywało wiadomości systemowe od operatora (o aktywacji usługi czy płatności). Na trzecim miejscu (49,3 proc.) respondenci wskazali powiadomienia kurierskie i pocztowe.

71. Digital 2021 https://datareportal.com/reports/digital-2021-global-overview-report
72. https://www.uke.gov.pl/download/gfx/uke/pl/defaultaktualnosci/36/410/1/2021_raport_uke_klienci_indywidualni.pdf

Popularność smartfonów i automatycznych SMS-ów dostrzegli również przestępcy. Coraz częściej przygotowują kampanie phishingowe nakierowane na ich użytkowników oraz złośliwe oprogramowanie na platformy mobilne.

Rok 2021 cechował się znacznym wzrostem liczby zgłoszeń związanych z tym zagrożeniem. W tym okresie do zespołu zespołu CERT Polska trafiło ponad 17,5 tys. zgłoszeń dotyczących szkodliwych aplikacji na systemy operacyjne Android.

Przegląd zaobserwowanych nowych trojanów

Flubot

Po raz pierwszy Flubot, inaczej Cabassous, został zaobserwowany pod koniec 2020 r. w Finlandii i Hiszpanii[73] [74], gdzie prowadzone były kampanie phishingowe wykorzystujące logotypy firm FedEx, DHL oraz Correos. Kampanie Flubota były przeprowadzane w kilkudziesięciu krajach, w tym w Polsce. CERT Orange Polska podczas analizy próbki Flubota w wersji 4.9[75] wyszczególnił 28 krajów do których były wysyłane SMSy.

Podstawową funkcją Flubota jest wstrzykiwanie podstawionych stron logowania do konkretnych aplikacji. Wpisane do takiego panelu login i hasło są wysyłane do serwera C&C.

Nazwa Flubot wywodzi się od sposobu propagowania tego złośliwego oprogramowania (od ang. flu oznaczającego grypę) i wynika ona z jego funkcji. Flubot wykorzystuje zainfekowany telefon do dalszego rozsyłania wiadomości phishingowych. Oznacza to, że wraz z każdą infekcją rośnie liczba botów wysyłających wiadomości phishingowe na losowe numery telefonów.

Warto zwrócić uwagę na fakt, że baza numerów telefonów, do których były wysyłane wiadomości, jest zasilana między innymi poprzez listę kontaktów z zainfekowanych telefonów.

Wraz z kolejnymi kampaniami realizowanymi w wielu krajach, funkcje Flubota rozwijały się. Między innymi utrudniano przechwytywanie komunikacji między botem a serwerem C&C, wprowadzając mechanizmy tunelowania ruchu DNS over HTTPS.

BlackRock

W drugim kwartale 2020 r. pojawiło się nowe szkodliwe oprogramowanie BlackRock[76], które w dużym stopniu opierało się na zapożyczeniu kodu oraz funkcji z rodziny Xerxes oraz LokiBot. Poza wspomnianym niżej incydentem, zespół CERT Polska w 2020 r. nie zaobserwował żadnej kampanii związanej z tą konkretną rodziną. W 2021 r. kampania była aktywna przez bardzo krótki okres.

Wśród możliwości BlackRocka można wyróżnić:

- logowanie wpisywanych danych,
- listowanie, przekazywanie oraz wysyłanie SMS-ów,
- blokowanie ekranu,
- zbieranie informacji na temat urządzenia oraz powiadomień,
- ukrywanie ikony aplikacji,
- umożliwienie usunięcia aplikacji,
- wstrzykiwanie fałszywych paneli logowania do konkretnych aplikacji.

ERMAC

We wrześniu 2021 r. CERT Polska zaobserwował nowy wariant opisywanego w 2020 r. trojana Cerberus – ERMAC. W porównaniu z poprzednimi wariantami, zmieniony został wykorzystywany do tej pory algorytm szyfrowania. Zaimplementowana została też funkcja raportowania listy kont dodanych w systemie. Podobnie jak w przypadku pierwszej wersji Cerberusa, kilka miesięcy wcześniej także pojawiła się oferta jego sprzedaży. ERMAC był prawdopodobnie wykorzystywany przez tego samego aktora, który stał za kampanią BlackRock.

Kampanie złośliwego oprogramowania androidowego zaobserwowane w 2021 roku

Wzorem lat ubiegłych, w 2021 r. szkodliwe oprogramowanie na urządzenia mobilne było najczęściej dystrybuowane za pomocą fałszywych wiadomości SMS oraz e-maili, które posiadały odnośniki do odpowiednio spreparowanych stron interne-

73. *INCIBE-CERT Flubot Analysis Study 2021* https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe-cert_flubot_analysis_study_2021_v1.pdf
74. *New Massive Mobile Malware Ring Targeting Europe* https://www.prodaft.com/resource/detail/flubot-new-masssive-mobile-malware-ring-targeting-europe
75. *Flubot 4.9* - szybka analiza https://cert.orange.pl/aktualnosci/flubot-4-9-szybka-analiza
76. *BlackRock* - The trojan that wanted to get them all https://www.threatfabric.com/blogs/blackrock_the_trojan_that_wanted_to_get_them_all.html

towych. Chociaż witryny te prezentowały różne zawartości, wszystkie miały jeden cel: zachęcenie potencjalnej ofiary do pobrania szkodliwego pliku ze wskazanego zasobu.

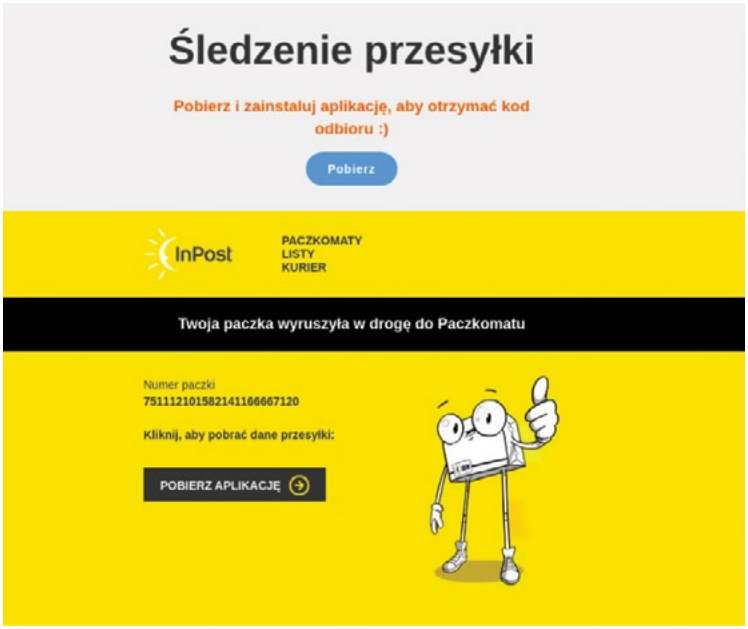
Poniżej, w kolejności chronologicznej, przedstawiony został przegląd najciekawszych kampanii, zaobserwowanych przez CERT Polska w 2021 r.

Odbiór paczki Inpost

W pierwszej połowie stycznia zespół CERT Polska zaobserwował kontynuację schematu dystrybucji szkodliwego oprogramowania z rodziny Alien, z wykorzystaniem logotypów firmy InPost. Sposób dystrybucji nie zmienił się w 2021 r., dalej na losowe numery wysyłane były SMS-y, które zawierały w swojej treści link do strony przypominającej portal wcześniej wspomnianego podmiotu. Wiadomości były tak skonstruowane, aby zachęcić użytkownika do pobrania aplikacji ze wskazanego zasobu. W tym celu przestępcy powoływali się na konieczność podjęcia działań względem wspomnianej sytuacji.

Uznaje się, że w drugiej połowie stycznia, kampania została zakończona. Nasz zespół nie zaobserwował w 2021 r. kolejnych zgłoszeń związanych z Alienem.

Rys. 25. Przykład wiadomości nakłaniającej do pobrania oraz zainstalowania szkodliwej aplikacji.



Rys. 26. Fałszywa stronia nakłaniająca do instalacji szkodliwej aplikacji.

Aktualizacja regulaminu oraz Polityka antyspamowa

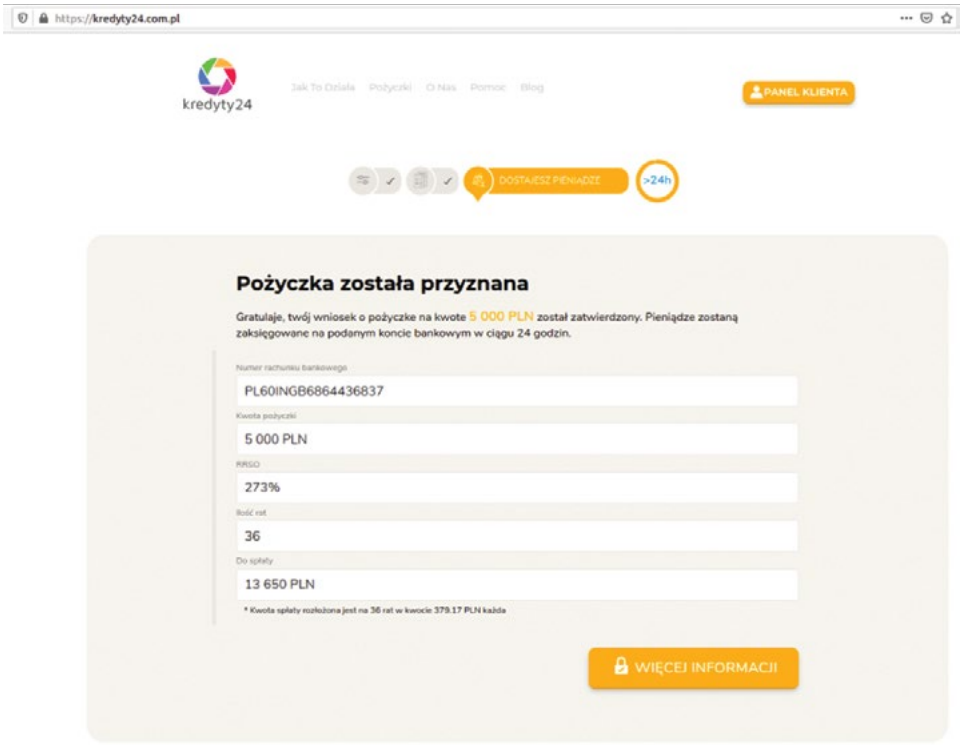
W pierwszej połowie 2021 r. CERT Polska zaobserwował kontynuację kampanii dystrybucji szkodliwego oprogramowania z rodziny Hydra, w których wykorzystano logotypy dostawców usługi poczty elektronicznej, takich jak WP, o2, Onet czy Interia. Losowi adresaci na swoje skrzynki pocztowe otrzymywali wiadomości od rzekomego administratora skrzynki. Zależnie od wariantu oszustwa, w treści e-maila znajdowały się informacje o konieczności zatwierdzenia zaktualizowanego regulaminu lub fałszywe powiadomienie o blokadzie konta, spowodowanej rzekomym spamem wychodzącym ze skrzynki. Cel oszustów, niezależnie od schematu, pozostawał ten sam – zachęcenie ofiary do pobrania i zainstalowania szkodliwej aplikacji. Ostatni raz ten schemat został użyty w maju 2021 r.

Rys. 27. Fałszywa wiadomość mailowa informująca o rzekomej aktualizacji regulaminu oraz potrzebie podjęcia działań przed blokadą konta.

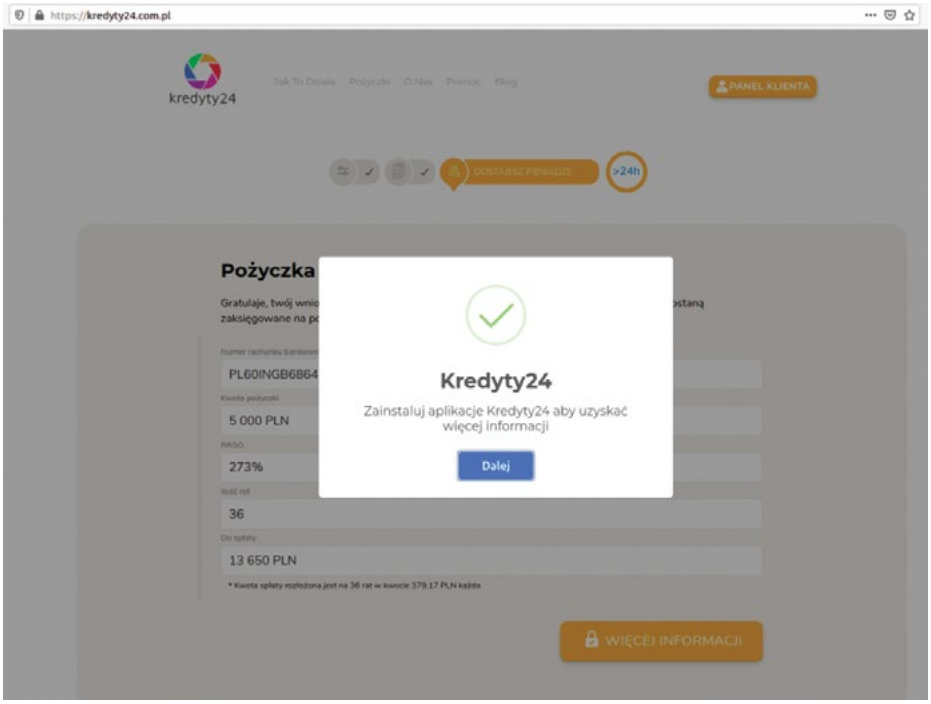
Rys. 28. Strona podszywająca się pod serwis Onet Poczta, zachęcająca do pobrania szkodliwej aplikacji.

Udzielenie pożyczki

W lutym 2021 r. zespół CERT Polska zaobserwował rozwinięcie kampanii dystrybuujących szkodliwe aplikacje z rodziny Hydra. W tym przypadku stworzono oraz wykorzystano logotyp nieistniejącego podmiotu finansowego. Oszuści wysyłali wiadomości mailowe, w których informowali o pozytywnym rozpatrzeniu wniosku kredytowego, rzekomo złożonego przez adresata. W treści znajdował się link do portalu, umożliwiającego przekierowanie pożyczonych pieniędzy na konto bankowe. Po wejściu na stronę ukazywał się widok ponownie informujący odwiedzającego o przyznanej pożyczce. Po kliknięciu w dowolny przycisk na stronie pojawiała się informacja o konieczności pobrania aplikacji.



Rys. 29. Fałszywa strona przedstawiająca widok rzekomo przyznanej pożyczki.



Rys. 30. Monit wyświetlający się na stronie, zachęcający do pobrania szkodliwej aplikacji.

STOP COVID

W styczniu 2021 r. miała miejsce pierwsza i jedyna masowa kampania dystrybucji szkodliwego oprogramowania z rodziny BlackRock. Wykorzystywała ona w tym czasie popularny temat aplikacji informujących o kontakcie z osobą chorą na COVID-19. Oszuści wysłali na losowe numery telefonów wiadomości SMS, w których nakłaniano do instalacji oprogramowania. Po wejściu na załączony link pojawiał się portal, który zachęcał do pobrania aplikacji ze wskazanego zasobu. Pobranie aplikacji było poprzedzone instrukcją instalacji, która faktycznie informowała, jak obejść systemowe zabezpieczenia ograniczające instalację aplikacji pochodzących z nieznanego źródła.

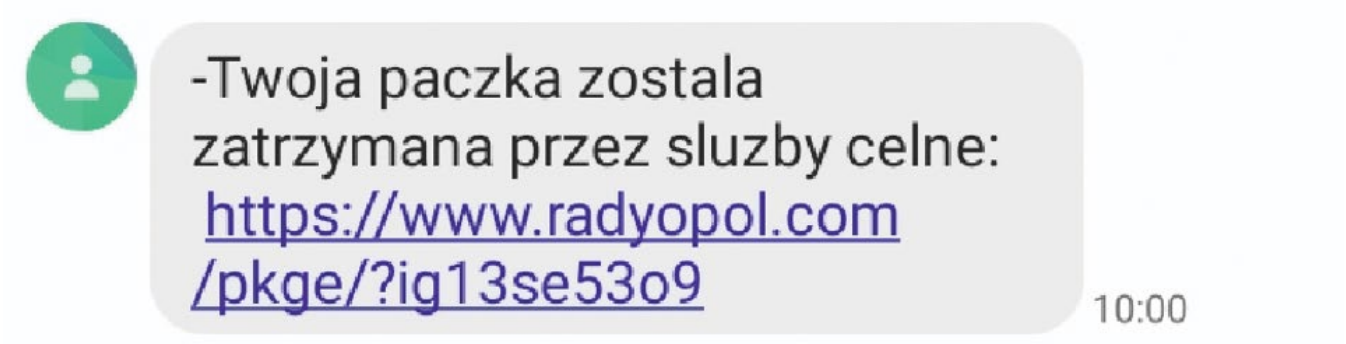
Rys. 31. Strona prezentująca fałszywą aplikację do śledzenia zakażeń COVID-19.

Rys. 32. Instrukcja informująca jak ominąć zabezpieczenia instalacji aplikacji z nieznanego źródła.

Dostarczane paczki

W połowie kwietnia 2021 r. pojawiła się pierwsza z trzech faz nowej kampanii, która skalą dystrybucji zdominowała pozostałe schematy. Użytkownicy telefonów komórkowych masowo otrzymywali wiadomości informujące o rzekomym zatrzymaniu paczki przez służby celne lub innych problemach z jej dostarczeniem. Powiadomienia zawierały również link do strony używającej logotypu firmy kurierskiej DHL i zachęcającej do instalacji aplikacji do zarządzania oraz śledzenia rzekomej przesyłki. W rzeczywistości był to trojan bankowy z rodziny Flubot.

Należy podkreślić skalę tego oszustwa. W tym schemacie wykorzystano domeny, które najprawdopodobniej zostały wcześniej przejęte. Świadczy o tym fakt wykorzystania ogromnej liczby unikalnych nazw (ponad 400), które w żaden sposób nie pokrywały się z wykorzystywaną tematyką kurierską. Co więcej, w przypadku pierwszej fali, która trwała od 15 do 27 kwietnia 2021 r., nasz zespół przyjął ponad 3500 zgłoszeń powiązanych z Flubotem. Stanowiło to około 50 proc. wszystkich zgłoszeń obsłużonych w tym przedziale czasowym.



Rys. 33. Fałszywy SMS dotyczący rzekomo zatrzymanej paczki.

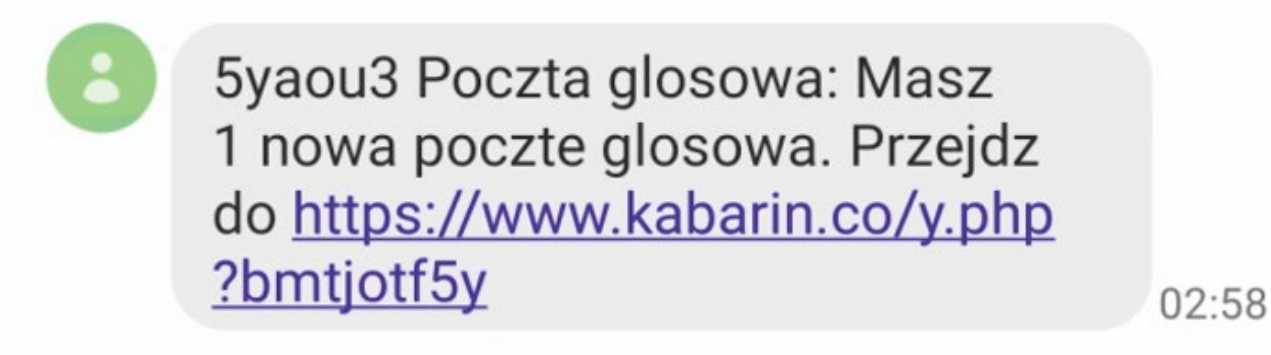
Rys. 34. Strona wykorzystująca logotyp DHL, zachęcająca do pobrania aplikacji, która ma rzekomo umożliwić śledzenie przesyłki.

Poczta głosowa

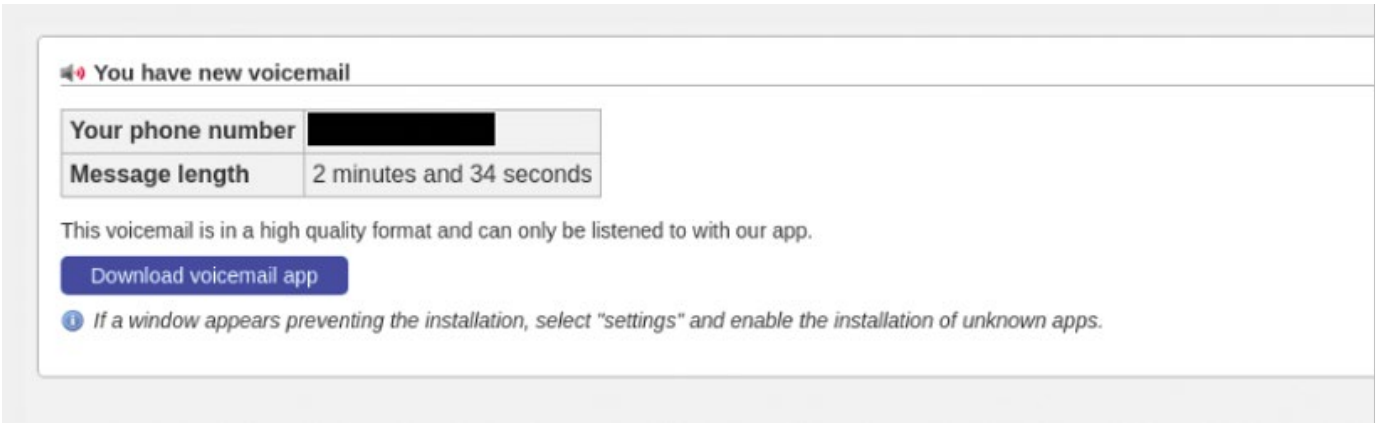
Po prawie 4 miesiącach braku aktywności operatorów Flubota, 12 sierpnia pojawiła się nowa kampania tego szkodliwego oprogramowania. Tym razem oszuści wykorzystywali znaki firmowe operatorów telekomunikacyjnych i informowali o rzekomej wiadomości na poczcie głosowej odbiorcy. Podobnie jak w poprzednim przypadku, w treści wiadomości znajdował się link, który przekierowywał na stronę umożliwiającą pobranie aplikacji. Cechą charakterystyczną strony był minimalistyczny wygląd, prezentujący proste dane na temat rzekomej wiadomości głosowej.

Kluczowym wyróżnikiem tej kampanii była podobna formuła konstruowania kolejnych schematów wiadomości. Wraz z rozwojem kampanii, pojawiały się kolejne mechanizmy, które miały ograniczyć możliwości wykrywania potencjalnego spamu przez filtry antyspamowe systemu operacyjnego Android. W tym celu dodano losowe ciągi znaków na początku wiadomości.

W ciągu 16 dni aktywności tej konkretnej fali (w okresie 12–28 sierpnia 2021 r.), nasz zespół obsłużył ponad 2 tysiące zgłoszeń.



Rys. 35. Wiadomość SMS informująca o rzekomej wiadomości głosowej.



Rys. 36. Fałszywa strona zachęcająca do pobrania aplikacji, która ma umożliwić odtworzenie wiadomości głosowej.

mObywatel

W połowie sierpnia 2021 r. pojawiła się kampania związana z ERMAC, nową rodziną trojana bankowego wywodzącego się od Cerberusa. Tym razem przestępcy wykorzystali wizerunek aplikacji mObywatel. Do losowych odbiorców trafiały wiadomości SMS od nadawcy "M0BYWATEL", które informowały o rzekomym wyznaczeniu terminu kolejnej dawki szczepienia lub o wygranej w "loterii narodowej". W SMS-ie również znajdował się link do aplikacji, dzięki której adresat wiadomości miałby uzyskać więcej informacji. Wejście na stronę prowadziło do spreparowanego widoku aplikacji Google Play, który miał umożliwić pobranie aplikacji mObywatel.

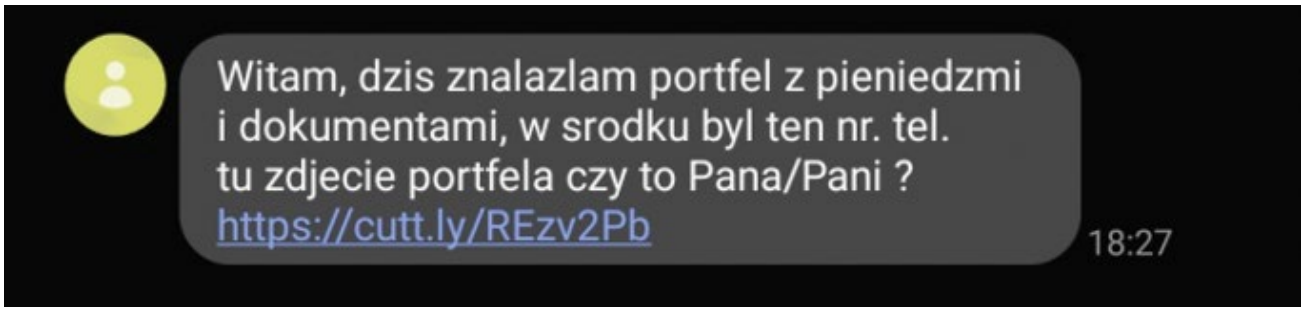
Oszuści coraz chętniej wykorzystują wizerunek sklepu Google Play w celu uwiarygodnienia źródła pobieranej aplikacji. Użytkownik może nie zauważyć, że znajduje się na stronie, która jedynie przypomina sklep Google Play. Dlatego tak ważne jest, aby wszystkie aplikacje pobierać z poziomu aplikacji danego sklepu (a nie przez stronę internetową), a także zwracać uwagę na wyświetlane komunikaty podczas instalacji.

Rys. 37. Fałszywa wiadomość SMS o rzekomej wygranej w "loterii narodowej".

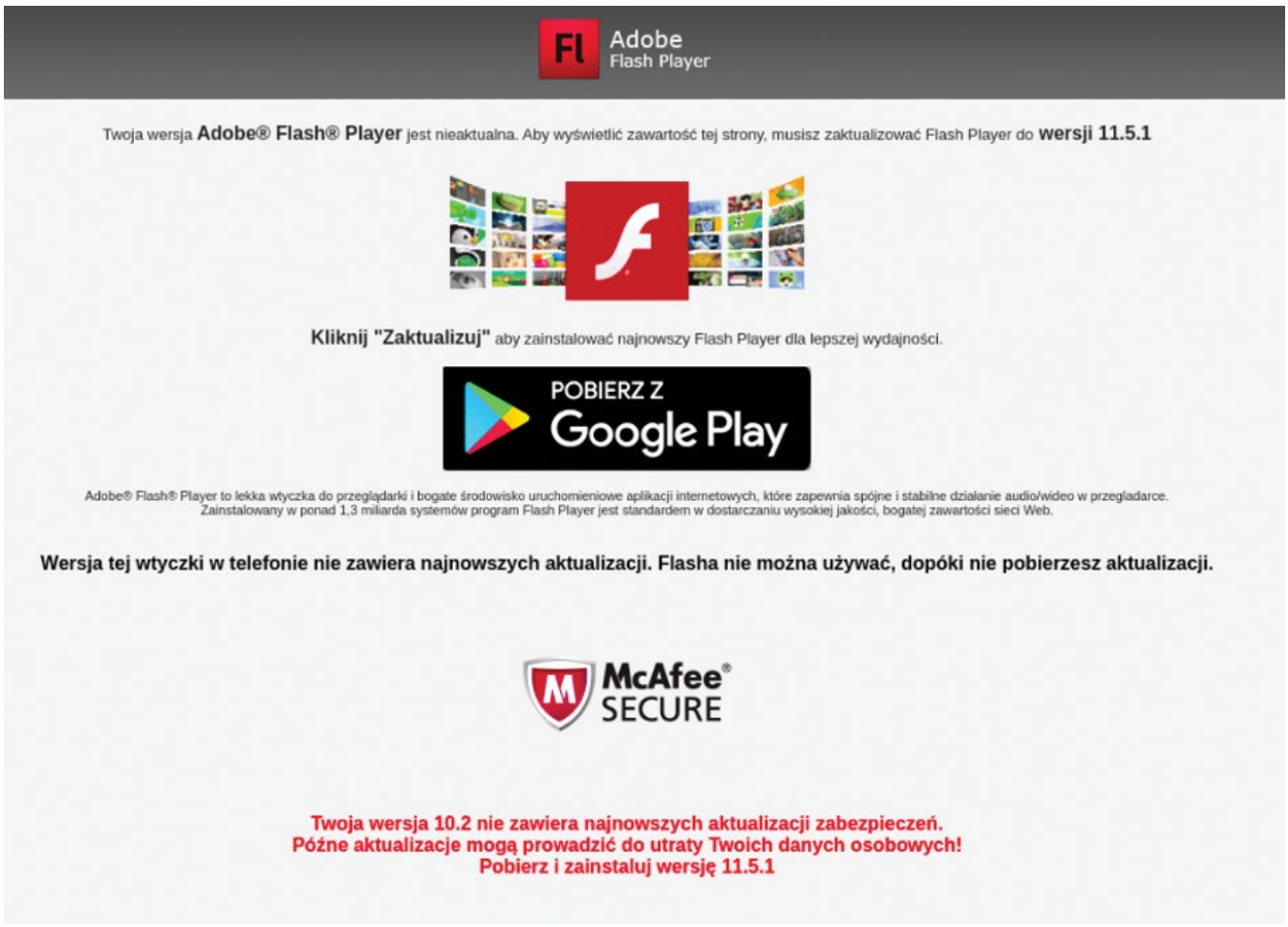
Rys. 38. Podrobiony widok sklepu Google Play, który ma rzekomo umożliwić pobranie aplikacji mObywatel.

Aktualizacja Adobe Flash, otrzymane zdjęcia

Kampania z wykorzystaniem wizerunku mObywatela nie była jedynym schematem rozpowszechnianym przez aktora związanego z ERMAC. W tym samym okresie, na losowe numery telefonów, przychodziły SMS-y informujące o rzekomym odnalezieniu portfela z dokumentami adresata. W treści znajdował się link do strony, która wykorzystywała logo firmy Adobe oraz zachęcała do pobrania wymaganej aktualizacji do Adobe Flash Playera. Podobnie jak w przypadku mObywatela, wskazany zasób udostępniał plik APK, będący tak naprawdę szkodliwym oprogramowaniem z rodziny ERMAC.



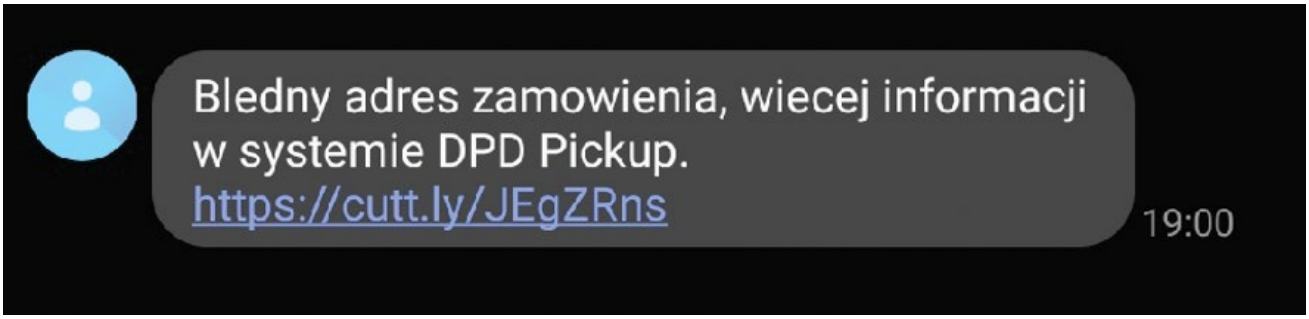
Rys. 39. SMS informujący o zgubionym portfelu z dokumentami.



Rys. 40. Strona z rzekomą aktualizacją Adobe Flash Playera.

Błędny adres zamówienia DPD Pickup

Ostatnią kampanią przeprowadzoną przez aktora odpowiedzialnego za ERMAC była kolejna masowa wysyłka wiadomości SMS. Tym razem informowano o rzekomym błędzie w adresie zamówienia, który miał być przekazany do firmy kurierskiej DPD. Treść wiadomości sugerowała, że adresat może uzyskać więcej informacji korzystając z systemu DPD Pickup, do którego link został załączony w treści wiadomości. Podobnie jak w poprzednich kampaniach tego aktora, strona, wykorzystując wizerunek konkretnego podmiotu, zachęcała do pobrania i zainstalowania szkodliwej aplikacji.



Rys. 41. Fałszywa wiadomość dotycząca rzekomo błędnego adresu zamówienia.

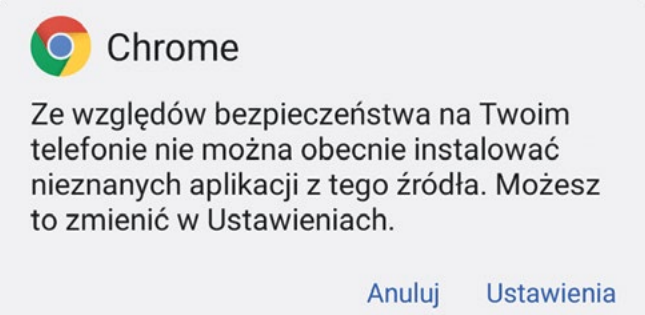
Dostarczane paczki, poczta głosowa oraz aktualizacja Adobe Flash

Od drugiej połowy listopada 2021 do końca roku, CERT Polska odnotowywał rosnącą liczbę zgłoszeń związanych z masową kampanią dystrybucji szkodliwego oprogramowania z rodziny Flubot. W trakcie trwania tej kampanii nasz zespół obsłużył ponad **11,5 tysiąca** powiązanych z nią zgłoszeń. W trakcie tej fali wykorzystywane były naprzemiennie dwa schematy użyte w poprzednich falach.

Jak uniknąć infekcji?

Przede wszystkim należy unikać instalowania aplikacji pochodzących z nieznanych źródeł. W przypadku jakichkolwiek wątpliwości najlepiej jest zweryfikować czy otrzymana wiadomość zachęcająca do instalacji aplikacji jest prawdziwa. Jednocześnie warto pamiętać, że samo kliknięcie w link przesłany w wiadomości SMS czy w e-mailu i wejście na niebezpieczną stronę, nie spowoduje samoczynnej instalacji złośliwej aplikacji.

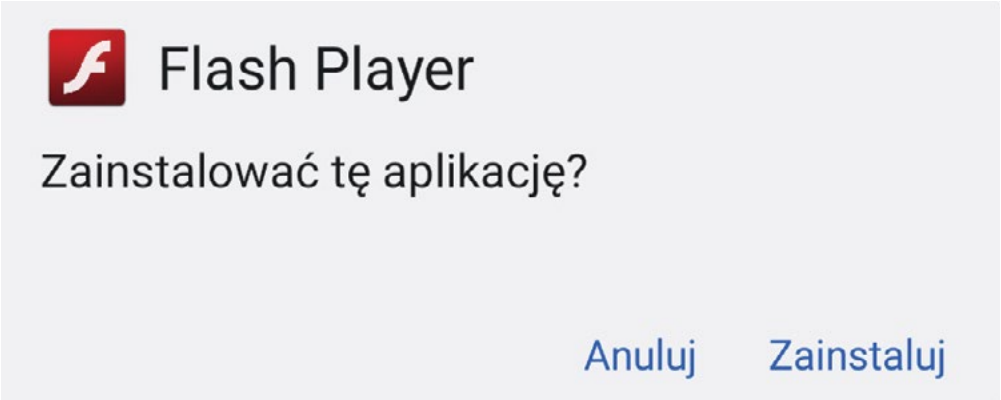
Przed instalacją aplikacji z innych źródeł niż sklep z aplikacjami preinstalowany na urządzeniu, pojawia się komunikat systemowy z pytaniem czy chcemy zezwolić na instalowanie aplikacji z tego źródła[77].



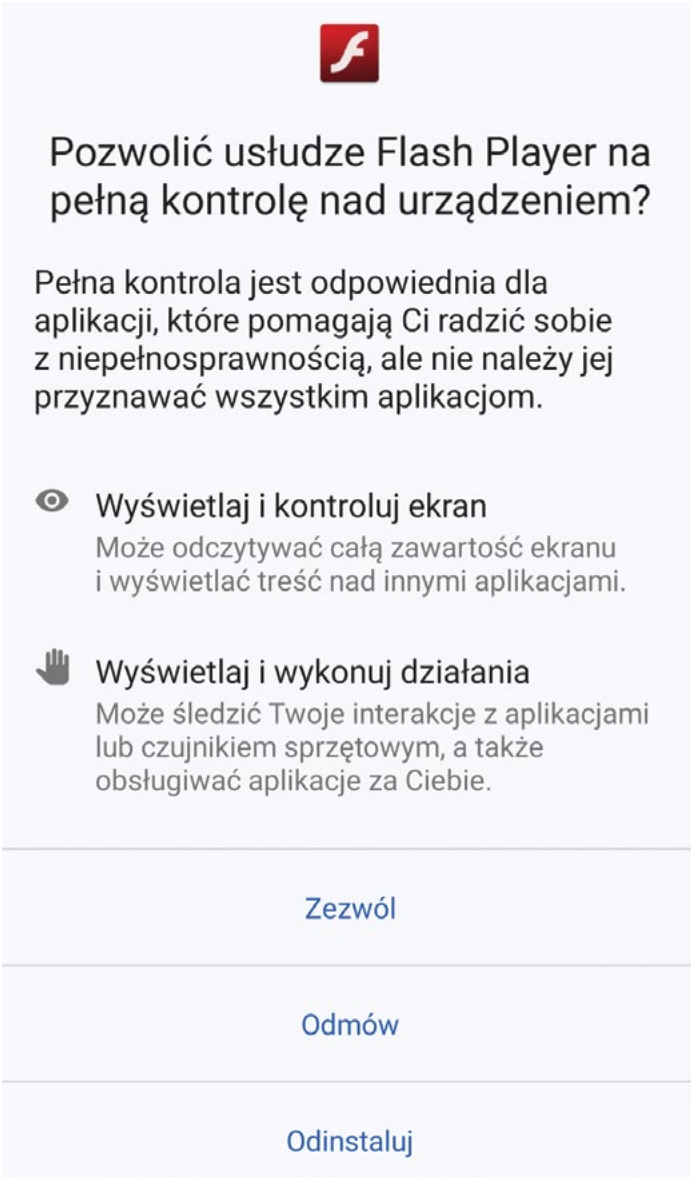
Rys. 42. Przykład komunikatu pytającego o zezwolenie na instalację aplikacji poprzez przeglądarkę Google Chrome.

Rys. 43. Strona w ustawieniach, na której można zezwolić na instalację aplikacji z danego źródła.

77. Funkcjonalność dostępna od Androida 8 Oreo: https://developer.android.com/studio/publish#publishing-unknown



Rys. 44. Przykład komunikatu przed instalacją fałszywej aplikacji Flash Player.



Rys. 45. Przykład komunikatu, w którym fałszywa aplikacja Flash Player prosi o udzielenie uprawnienia do kontroli nad urządzeniem.

78. https://www.facebook.com/CERT.Polska/posts/4774454839241535

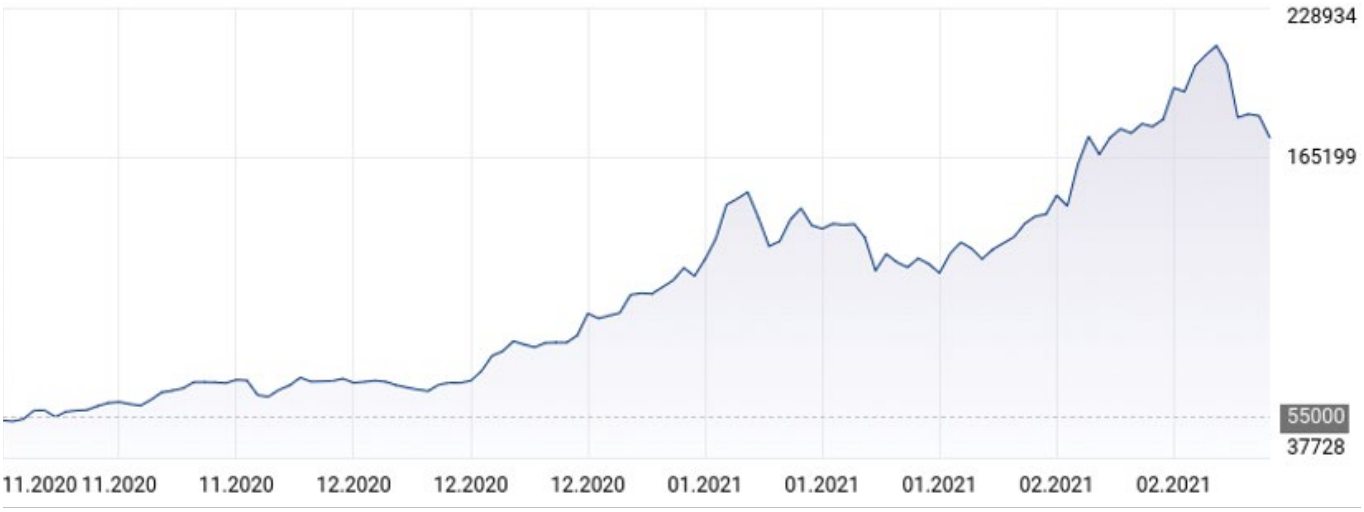
Jeśli aplikacja zostanie zainstalowana, jej usunięcie może okazać się bardzo trudne — opisane rodziny potrafią się dobrze przed tym chronić. Jeżeli jednak zorientujemy się, że nasze urządzenie zostało zainfekowane, zawsze warto zwrócić się o pomoc do specjalisty, np. zgłaszając incydent za pośrednictwem formularza kontaktowego na stronie CERT Polska.

Zachęcamy do śledzenia naszych profili społecznościowych, gdzie na bieżąco umieszczamy ostrzeżenia przed podobnymi kampaniami oraz rekomendacje działań w związku z zagrożeniem.

Mając na uwadze trzecią falę Flubota, opublikowaliśmy także krótki poradnik jakie działania należy podjąć w przypadku odebrania podejrzanej wiadomości[78].

Oszustwa i fałszywe inwestycje

Pierwsze miesiące 2021 r. charakteryzowały się rosnącą popularnością kryptowalut, w szczególności Bitcoina. Potwierdza to m.in. liczba wyszukiwań słowa "bitcoin" w Google. W tym okresie wzrosła również gwałtownie wartość Bitcoina, co ilustruje poniższy wykres.



Wykres 3. Wykres ceny Bitcoin w analizowanym okresie[79].

Trend ten został zauważony przez przestępców, którzy wykorzystali go w nowym schemacie oszustw. Praktycznie wszystkie analizowane przez CERT Polska przypadki fałszywych inwestycji dotyczyły kryptowalut. Najczęściej mowa była o Bitcoinie zapewne dlatego, że jest to najbardziej znana kryptowaluta. Zachęcanie do "inwestycji" odbywało się przy użyciu kilku mechanizmów, z których dwa były wykorzystywane najczęściej.

Najwięcej zgłoszeń dotyczyło otrzymanego połączenia telefonicznego z informacją o rzekomo zainwestowanych wcześniej środkach. Osoba dzwoniąca oferowała pomoc w wypłacie tych środków. W tym celu należało zainstalować program do zdalnego dostępu (zdalnego pulpitu) np. AnyDesk. Choć sam program jest w pełni legalny i powszechnie wykorzystywany, to w tym przypadku pozwala oszustom na uzyskanie dostępu do urządzenia.

O wiele bardziej skomplikowany był drugi schemat, masowo wykorzystywany przez przestępców. Polegał on na promocji stron, które oferowały fałszywe inwestycje w kryptowalutę z wykorzystaniem specjalnie stworzonego algorytmu, który miał decydować o szczególnie korzystnym kupnie i sprzedaży aktywów.

79. Źródło: https://www.google.com/finance/quote/BTC-PLN

Puls Biznesu

Aktualności Moda Celebryci Rozrywka

RAPORT SPECJALNY: Eksperci są pełni podziwu dla Tomasz Biernacki jego ostatniej inwestycji, co wywołało przerażenie wśród dużych banków."

Korzystając z tej „luki fortuny", polscy obywatele zgarniają już miliony złotych bez wychodzenia z domu – ale czy to jest legalne?

Jak widać w

na:Temat | GAZETA POLSKA | Fakt | PARKIET | Newsweek POLSKA

Tomasz Biernacki ujawnia nową, tajną inwestycję, która sprawia, że setki Polaków stają się bardzo bogaci.

(Puls Biznesu) - polski przedsiębiorca, menedżer, założyciel i współwłaściciel sieci handlowej Dino Polska Tomasz Biernacki, zdobył sławę jako zuchwała osoba mówiąca wprost, która nie ma oporów, by mówić szczerze o tym, jak zarabia pieniądze.

W zeszłym tygodniu Tomasz był gościem programu „Kuba Wojewódzki Show", w którym ujawnił nową „lukę fortuny". Taka „luka", wg jego słów, może zamienić każdą osobę w **milionera w ciągu 3-4 miesięcy**. Biernacki przekonywał wszystkich ludzi w Polsce, by skorzystali z tej świetnej okazji, zanim wielkie banki ostatecznie tego zabronią.

WYNIKI CZYTELNIKÓW

Wygrana: 7 521 zł

"Korzystałem z Bitcoin Up dopiero od 2 tygodni a już wykupiłam dzięki niemu urlop w Europie."

Anna Tomaszewska
z Gdańska

Wygrana: 5 552 zł

"Korzystam z Bitcoin Up od ponad dwóch tygodni a mój początkowy wkład 1100 zł wzrósł do 5 802 złotych. To o wiele więcej niż mogę zarobić w pracy."

Marik Majewski
Łódź

Wygrana: 9 200 zł

Rys. 46. Przykładowa strona wykorzystująca wizerunek celebrytów do promowania fałszywych inwestycji

Platformy do rzekomych inwestycji często reklamowane były na Facebooku za pośrednictwem przejętych kont, co miało uwiarygodnić przekaz wśród znajomych. Po kliknięciu w link użytkownik zazwyczaj był przenoszony do strony przypominającej wyglądem znane portale informacyjne. Znajdował się tam artykuł często wykorzystujący wizerunki celebrytów, który informował o nowym, bardzo skutecznym serwisie umożliwiającym inwestowanie bez potrzeby posiadania eksperckiej wiedzy. Po zarejestrowaniu się na takiej stronie ofiara często zachęcana była do inwestowania początkowo relatywnie niedużej kwoty, zazwyczaj równowartości około 200 euro. Następnie na platformie można było obserwować jak wartość portfela inwestycyjnego rzekomo rosła. Prezentowany wzrost nie miał jednak nic wspólnego z rzeczywistością. Dzięki zbudowanemu w ten sposób zaufaniu, przestępcy mogli przekonać ofiary do zwiększenia inwestycji.

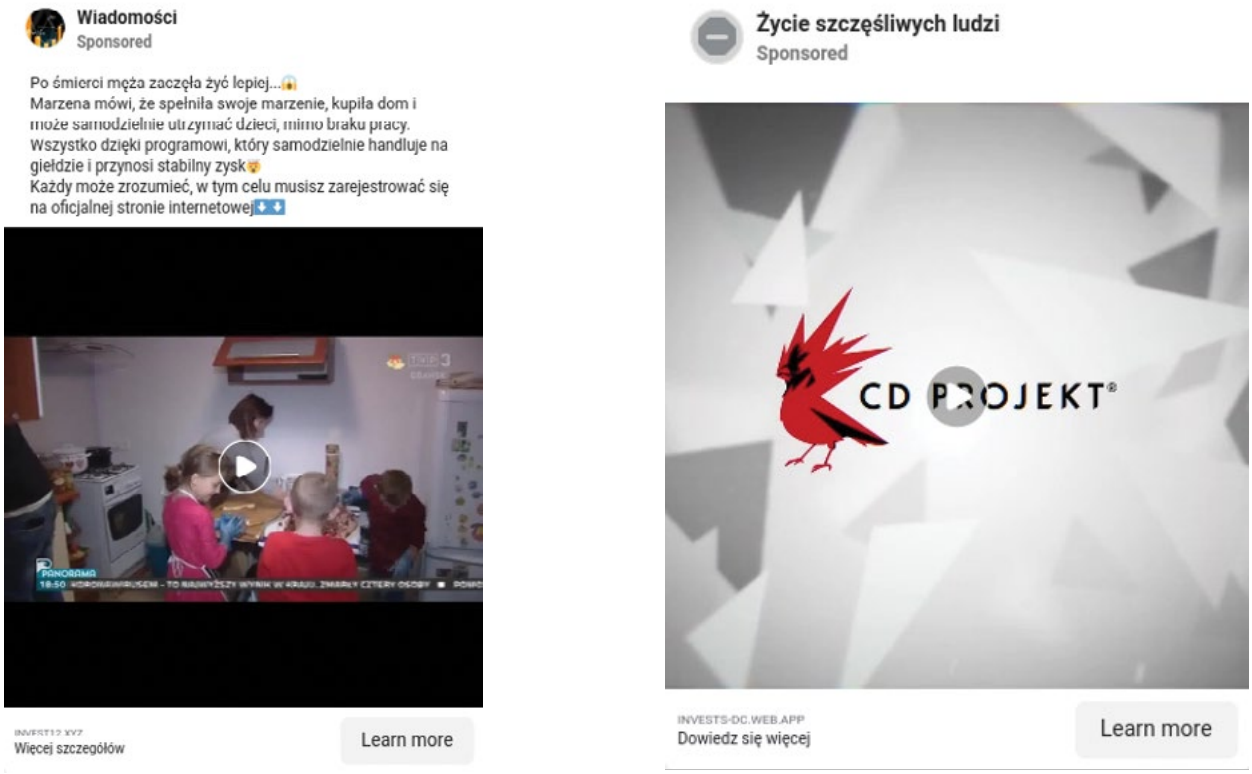
Kolejna metoda wyłudzenia pieniędzy polegała na wysyłaniu informacji o konieczności opłacenia podatku lub uiszczenia dodatkowych opłat. W tym celu oszuści podszywali się pod różne instytucje. Ostatnim etapem tego oszustwa było nakłonienie ofiary do zainstalowania programu do zdalnego dostępu do komputera. Podobnie jak we wcześniej opisanym mechanizmie, pozornym celem miała być pomoc w wypłacie środków. Umożliwienie zdalnego dostępu do komputera i konta ban-

kowego otwartego w przeglądarce często skutkowało także zaciągnięciem kredytu przez oszustów w imieniu nieostrożnych użytkowników.

W drugiej połowie 2021 r. do CERT Polska zaczęły napływać zgłoszenia dotyczące kolejnego schematu oszustw. Tym razem, zamiast inwestycji w kryptowaluty, przestępcy reklamowali serwisy umożliwiające rzekomy zakup akcji różnych znanych spółek. Początkowo oszuści często wykorzystywali firmy z sektora energetycznego. Zmiana schematu działania pokrywa się czasowo z dużymi spadkami cen większości kryptowalut. Dostępne w mediach informacje o niepewności rynku kryptowalut mogły zniechęcić potencjalne ofiary do tego typu inwestycji. Podobnie jak w poprzednim schemacie, na różnych serwisach społecznościowych, np. na Facebooku lub YouTubie, można było znaleźć reklamy, które w sposób nieuprawniony wykorzystywały logotypy powszechnie znanych firm, wizerunki celebrytów, a nawet polityków zajmujących najważniejsze stanowiska w państwie. Warto podkreślić, że przestępcy wykorzystywali również zewnętrzne mechanizmy reklamowe do wyświetlania treści promujących szkodliwe strony na znanych portalach informacyjnych.

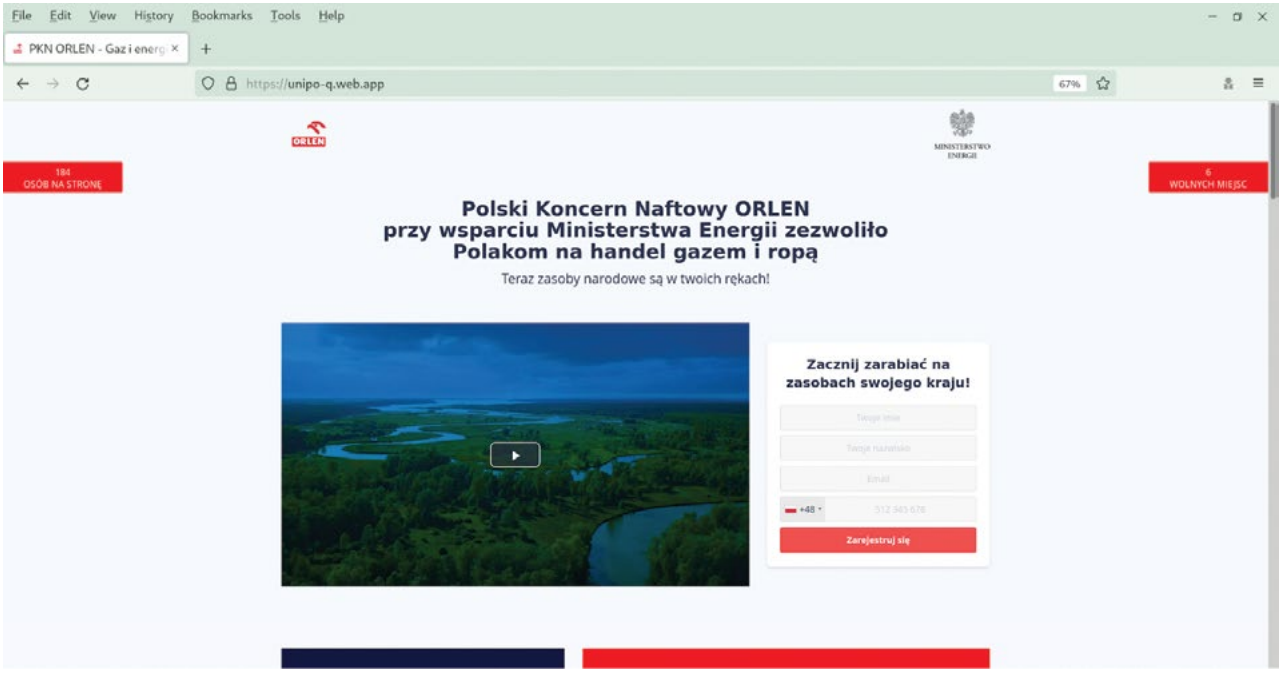
Rys. 47. Reklamy wykorzystujące wizerunek firm PGE i Orlen do promowania fałszywych inwestycji.

Po pewnym czasie przestępcy zaczęli nawet tworzyć zmanipulowane materiały wideo, które wykorzystywały obraz z programów telewizyjnych. Do gotowego obrazu podkładane było nagranie nakłaniające do dokonania inwestycji na promowanych stronach. Co więcej, pod koniec roku pojawiły się również kolejne podmioty, których wizerunek był wykorzystywany przez oszustów. Były to m.in. firmy takie jak CD Projekt RED oraz Volkswagen.



Rys. 48. Reklamy wykorzystujące spreparowane materiały wideo do promowania fałszywych inwestycji.

Najczęściej w takiej reklamie zamieszczony był link do strony z formularzem kontaktowym, za pośrednictwem którego zainteresowana inwestycjami osoba mogła przesłać swoje dane kontaktowe. Prawie w każdym przypadku strony wyglądały podobnie, a przestępcy zmieniali tylko logotypy lub zdjęcia.

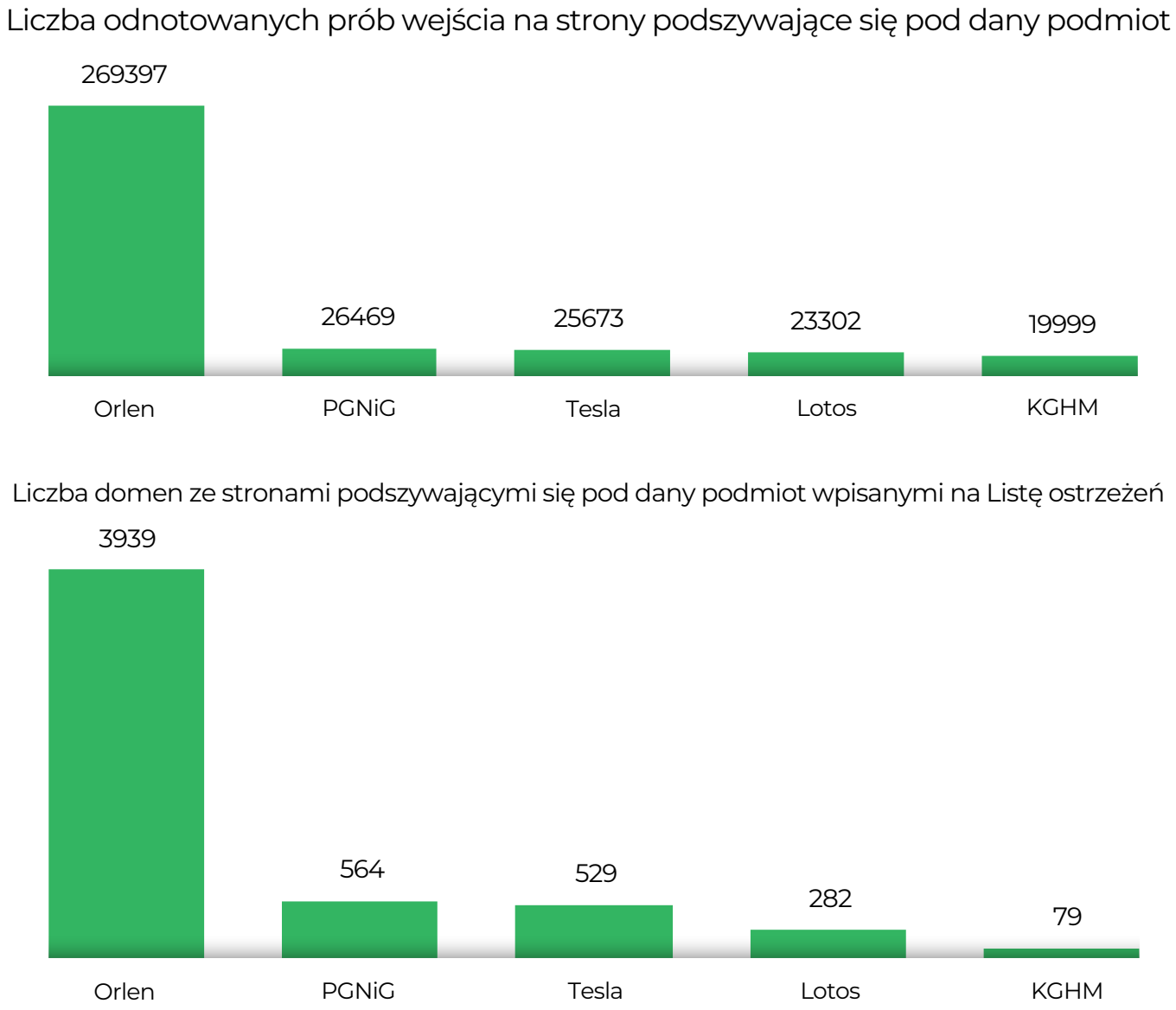


Rys. 49. Szkodliwa strona wykorzystująca wizerunek firmy Orlen do promowania fałszywych inwestycji.

Po podaniu wymaganych danych kontaktowych przedstawiciel firmy oferującej rzekomo bezpieczne i bardzo lukratywne inwestycje, kontaktował się telefonicznie z zainteresowanym i nakłaniał go do przelewu środków. Podobnie jak w przypadku oszustwa wykorzystującego zainteresowanie kryptowalutami, inwestowana początkowo kwota była relatywnie niska, jednak rosła w trakcie rozmowy. Czasami, aby zwiększyć zaufanie, oszukane osoby otrzymywały informacje o zyskach. Kolejnym etapem było uzyskanie przez oszustów dostępu do rachunku bankowego osoby zainteresowanej szybkim zarobkiem. W tym celu, podobnie jak we wcześniej opisanych schematach, przedstawiciel nakłaniał do zainstalowania aplikacji do zdalnego pulpitu.

W niektórych przypadkach przedstawiciel firmy oferującej fałszywe inwestycje prosił inwestora, by ten poddał się procesowi rzekomej weryfikacji. W tym celu inwestor otrzymywał link do strony, na której należało zamieścić skan dowodu osobistego lub podać swoje dokładne dane.

Wszystkie domeny, które wykorzystywane były w tych dwóch schematach oszustw, były wpisywane na Listę ostrzeżeń przed niebezpiecznymi stronami. W całym 2021 r. nasz zespół przeanalizował 5719 takich domen, na które odnotowaliśmy 378 tysięcy prób wejścia.



Wykres 5. Wykresy przedstawiające pięć podmiotów z największą liczbą prób wejść na domeny wpisane na Listę ostrzeżeń.

Wycieki danych

Wraz z ciągłym wzrostem ilości przetwarzanych danych w systemach informatycznych, obserwujemy większą liczbę przypadków ich wycieków. Dotyczy to zarówno wielkich korporacji, jak i małych przedsiębiorstw lub osób fizycznych. Za bezpieczeństwo danych odpowiadają wszystkie osoby, które na każdym szczeblu przepływu muszą ściśle przestrzegać procedur bezpieczeństwa. Równie ważnym aspektem są same systemy teleinformatyczne, wymagające zabezpieczeń na poziomie projektu, konfiguracji i utrzymania.

Jak wyciekają dane?

Nie wszystkie wycieki mają związek z włamaniami hakerów. Częstym źródłem wycieku danych jest niezamierzone działanie osoby, która je przetwarza. Stale popełnianym błędem jest używanie funkcji "Do Wiadomości" (DW, ang. CC)[80] przy wysyłaniu wiadomości e-mail do wielu odbiorców jednocześnie. W takim przypadku każdy z adresatów pozna adresy pozostałych korespondentów.

Powszechnym zjawiskiem są również błędnie skonfigurowane systemy, np. umożliwiające dostęp do bazy danych bez znajomości hasła. Z takim przypadkiem spotkali się analitycy firmy Comparitech, którzy w marcu 2021 r. upublicznili[81] informację o dostępnej w internecie bez żadnych ograniczeń bazie, zawierającej dane osobowe 35 milionów rezydentów Stanów Zjednoczonych.

Wyciekiem nazywamy również przypadki, w których doszło do zgubienia lub kradzieży niezaszyfrowanego nośnika danych (laptop, dysk twardy, pendrive). Podobna sytuacja zachodzi, gdy mamy do czynienia z kradzieżą, zgubieniem lub utylizacją niezniszczonych dokumentów. W lipcu internauci z Piły odkryli[82] kontener pełen dokumentów, znajdujący się w publicznie dostępnym miejscu. Najprawdopodobniej miało to związek z zamknięciem i likwidacją placówki pobliskiego banku.

Rys. 50. Kontener z dokumentami niepoddanymi zniszczeniu[83].

80. (ang. *carbon copy*) polecenie wysłania kopii do dodatkowych odbiorców. Bezpieczną alternatywą jest BCC
81. Źródło: https://www.comparitech.com/blog/information-security/35-million-us-residents-exposed/
82. Źródło: https://www.rmf.fm/magazyn/news,40086,bank-wyrzucil-dokumenty-klientow-na-smietnik-tysiace-danych-osobowych-znalazlo-sie-na-ulicy.html
83. Źródło: https://www.wykop.pl/wpis/59209573/aktualizacja-sytuacji-pod-santanderem-w-pile-dawni/

Na szczęście nie każdy otwarty dostęp do danych kończy się wyciekiem. Wiele niezabezpieczonych baz danych lub porzuconych dokumentów nigdy nie wpadnie w niepowołane ręce. Nie jest to jednak argument za tym, by bagatelizować problem. W każdym przypadku starajmy się działać z najwyższą ostrożnością.

Działania cyberprzestępców

Oczywiście poważnym zagrożeniem dla bezpieczeństwa danych są również działania przestępców. Wykradzione informacje mogą zostać odsprzedane lub wykorzystane jako punkt wyjścia do popełniania kolejnych oszustw. Tego typu dane są więc popularnym towarem na czarnym rynku i są chętnie wykradane.

Cyberprzestępcy często swoją uwagę kierują na serwisy internetowe, które umożliwiają użytkownikom zarejestrowanie w nim konta. Celem ataku staje się kradzież bazy danych z danymi do logowania – najczęściej adresem e-mail i (zabezpieczonym) hasłem. Jako że częstym błędem internautów jest używanie jednego hasła (lub jego wariacji) do wielu serwisów, przestępcy w ten sposób mogą zdobyć dostęp do innych zasobów użytkowników. Przykładowo wykradając hasło danej osoby z forum dyskusyjnego poświęconego wędkarstwu, próbują następnie zalogować się nim do jej skrzynki pocztowej. W przypadku uzyskania dostępu do poczty, mogą wykonać procedurę resetu hasła do innych serwisów – np. Facebooka, co w następnym kroku zostanie wykorzystane do przeprowadzenia kolejnych oszustw, np. kradzieży „na Blika".

Standardową praktyką jest przechowywanie w bazie danych haseł w formie niejawnej (kryptograficzna funkcja skrótu – ang. hash). Istnieją jednak skuteczne metody odzyskiwania formy jawnej tak przechowywanego hasła. Skuteczność tych metod zależy od użytej funkcji skrótu, a także od złożoności hasła. Jednak nawet zestaw danych osobowych pozbawionych haseł również jest cennym towarem, pozwalając m.in. na wykonywanie celowanych ataków. Zdarza się również, że w procesie uwierzytelniania stosowany jest PESEL. 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), jednak nie należy go traktować jak sekretu.

Bardzo poważnym zagrożeniem, którego rozkwit obserwujemy w ostatnich latach, jest również ransomware. Jest to typ złośliwego oprogramowania szyfrującego pliki na zainfekowanym komputerze. Ofierze wyświetlane jest żądanie okupu, w którym przestępcy domagają się przekazania pieniędzy w zamian za klucz umożliwiający odszyfrowanie plików. W ostatnim czasie, coraz częściej oprócz operacji szyfrowania, dane są wysyłane na serwery sprawców. Grupy przestępcze trudniące się atakami tego typu za cel obierają z reguły duże korporacje. Jednak dane, które stamtąd wyciekają, dotyczą również podmiotów spoza tych organizacji, np. kontrahentów lub użytkowników świadczonych przez nie usług. Informacje o zjawisku ransomware znajdują się na stronie 46.

Jak możemy zadbać o swoje bezpieczeństwo?

Niestety, jako bezpośredni lub pośredni użytkownicy różnych systemów informatycznych nie mamy możliwości realnej oceny 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 minimum wymaganych danych osobowych

Im mniej informacji na nasz temat będzie przetwarzanych, tym mniej atrakcyjne będą dla atakujących, bądź trudniej będzie ich użyć do przeprowadzenia ataku lub kradzieży tożsamości. W wielu wypadkach podawanie prawdziwych lub kompletnych danych osobowych nie jest potrzebne, np. na stronie z darmowymi treściami rozrywkowymi.

Stosuj separację tożsamości

Powszechną dobrą praktyką jest oddzielanie komputerowej przestrzeni służbowej od prywatnej. Możemy tę zasadę rozszerzyć dzieląc kolejno te przestrzenie, zakładając osobną skrzynkę mailową do „spraw urzędowych", zakupów online, serwisów rozrywkowych, etc. Taki zabieg samoczynnie zwiększa prywatność, a w razie wycieku zmniejsza ilość czynności, które trzeba wykonać (np. zmiana numerów telefonów, adresów e-mail).

Używaj unikalnych, silnych haseł

Silne hasło w dużym stopniu utrudnia ataki siłowe/słownikowe, a używanie innych haseł do różnych serwisów niweluje problemy opisane w „działania cyberprzestępców". Haseł nie trzeba pamiętać – dobrą praktyką jest korzystanie z menedżerów haseł. Zachęcamy do przeczytania materiału CERT Polska o tworzeniu i używaniu haseł w bezpieczny sposób, który znaleźć można na naszej stronie internetowej[84].

Reaguj na ostrzeżenia o incydentach

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 zostają zresetowane. Nie ignorujmy takich ostrzeżeń i odpowiednio reagujmy na nie. Przeczytajmy je uważnie i po upewnieniu się, że dotyczy naszego konta, postępujmy zgodnie z zaleceniami administratora. Ocena prawdziwości wiadomości jest tutaj kluczowa – jeżeli mamy podejrzenie, że wiadomość może być fałszywa – powinniśmy skontaktować się z administratorem danego serwisu. Jako CERT Polska obserwujemy bowiem wiadomości phishingowe, których scenariusz opiera się na rzekomej informacji od administratora z prośbą o zmianę hasła lub wykonanie innej operacji, wymagającej zalogowania się.

Co robić w przypadku wycieku?

Czynności, które należy podjąć, zależą od kontekstu wycieku i typu danych, które zostały ujawnione. W dużej części przypadków zbiór ten będzie zawierał nasze hasło, które bezzwłocznie powinniśmy zmienić. Ponadto, jeżeli w jakimkolwiek innym systemie korzystamy z tego samego hasła, tam również wymagana jest jego zmiana.

Jeżeli wyciekowi uległy dane dotyczące nie tylko naszej wirtualnej tożsamości, ale także osobowości prawnej (numer PESEL, numer dowodu osobistego) warto rozważyć podjęcie kroków w celu zmniejszenia ryzyka oszustw związanych z kradzieżą tożsamości. Popularnym 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. Te rozwiązania 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 zapobiegnięcia zaciągania pożyczek na nasze dane osobowe.

Oprócz powyższych, w przypadku kiedy upublicznione zostały dane z naszego dowodu tożsamości, 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 jesteśmy klientami. Przestępcy potrafią w krótkim czasie wyrobić falsyfikat dowodu osobistego, co może mieć wiele poważnych konsekwencji.

Ponadto należy sobie uświadomić, że wycieki danych są idealną pożywką dla przestępców i nieustannie zasilają ich możliwości zarówno masowych, jak i tych bardziej spersonalizowanych ataków. Im więcej aktualnych danych na nasz temat przestępcy pozyskają, tym bardziej wiary-

84. https://cert.pl/posts/2022/01/kompleksowo-o-haslach/

godne oszustwa 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.

Serwis "Have I been pwned?" (https://haveibeenpwned.com/) pozwala na sprawdzenie, czy nasz adres e-mail występuje w znanych wyciekach danych. Umożliwia on również dodanie naszego adresu do stałego monitoringu nowych wycieków, dzięki czemu w razie wystąpienia incydentu obejmującego naszą cyfrową tożsamość, zostaniemy o tym poinformowani.

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 scenariuszach oszustw i innych zagrożeniach wymierzonych w polskich internautów.

Atak na Profil Zaufany

21 lipca 2021 r. zespół CERT Polska zaobserwował zgłoszenia i informacje medialne o niepokojących wiadomościach e-mail, otrzymywanych przez użytkowników Profilu Zaufanego. Wiadomości informowały o nieudanej próbie logowania. Osoby zgłaszające powyższe incydenty twierdziły, że nie dokonywały w ostatnim czasie prób logowania do Profilu Zaufanego, a w szczególności nie dokonały nieudanych prób logowania na swój profil. Sprawą szybko zainteresował się Sekretarz Stanu ds. Cyfryzacji w Kancelarii Premiera Rady Ministrów Janusz Cieszyński. W wyniku rozmów z ministrem Cieszyńskim, zespół CERT Polska, pełniący rolę krajowego zespołu reagowania na incydenty bezpieczeństwa informatycznego CSIRT NASK, podjął się koordynacji i pomocy w ustaleniu przyczyn występowania niepokojących wiadomości we współpracy z dostawcą platformy ePUAP – Centralnym Ośrodkiem Informatyki (COI).

Rys. 51. Informacja o zgłoszeniach nieudanych prób logowania do Profilu Zaufanego[85].

85. Źródło: https://twitter.com/niebezpiecznik

Analiza incydentu

Z informacji opublikowanej na Twitterze przez branżowy portal Niebezpiecznik.pl można wyczytać, że pierwsze podejrzenia wskazywały na masowe próby logowania dokonywane przez nieznanego aktora lub na awarię rządowego systemu. Awaria została jednak wykluczona. W trakcie obsługi incydentu CERT Polska ustalił, że miał miejsce atak polegający na masowych próbach logowania na konta użytkowników platformy ePUAP przy użyciu Profilu Zaufanego. Ten rodzaj ataku wykorzystuje tendencję użytkowników do ponownego używania tych samych haseł w kilku miejscach. Dane do logowania pozyskiwane są najczęściej z upublicznionych wycieków danych i przy ich użyciu dochodzi do próby zalogowania się na konta w innych usługach. Atak taki określa się pod angielską nazwa: credential stuffing.W ramach obsługi incydentu CERT Polska zebrał istotne informacje, które zostały przekazane organom właściwym w celu wykonania dalszych czynności śledczych oraz podjęcia kroków prawnych.

Zatrzymanie sprawcy

Już na początku sierpnia 2021 r. funkcjonariusze z Komendy Stołecznej Policji zatrzymali w Woli Krzywieckiej podejrzanego o przeprowadzenie ataków. W trakcje zatrzymania zabezpieczono również sprzęt komputerowy i różne nośniki danych. W trakcie analizy zebranych materiałów ujawniono, że mężczyzna zdobył dostęp do kont co najmniej 239 osób poprzez nieuprawnione zalogowanie się. Odkryto również ślady wskazujące na udostępnianie pozyskanych w ten sposób danych osobom trzecim. Podejrzany 27-latek przyznał się do przeprowadzenia ataków na użytkowników Profilu Zaufanego. W związku z powyższym, został na niego nałożony 2-miesięczny areszt tymczasowy. Za popełnione przestępstwa grozi mu kara do 8 lat pozbawienia wolności.

Rys. 52. Zatrzymanie osoby podejrzanej o przeprowadzanie ataków. Źródło: policja.pl.

Podszywanie się, groźby i fałszywe alarmy bombowe

W 2021 r. odnotowano liczne incydenty związane z fałszywymi alarmami bombowymi i groźbami skierowanymi wobec różnych instytucji i osób publicznych. Tego typu ataki występowały również w poprzednich latach i zazwyczaj miały postać anonimowych e-maili wysyłanych na skrzynki pocztowe, zmuszając pracowników instytucji do podjęcia ewakuacji. Fałszywe alarmy bombowe określa się często mianem ataków kaskadowych, gdyż jeden sprawca w jednym czasie rozsyła pogróżki do wielu instytucji naraz, co zwiększa szansę na reakcję ze strony ofiar i stanowi znaczne obciążenie dla służb ratunkowych.

Podczas dystrybucji tego typu korespondencji wykorzystywane są zazwyczaj skrzynki mailowe, które rejestrowane są jednorazowo dla danej wysyłki. Dodatkowo przestępcy rejestrują się w danym serwisie mailowym i rozsyłają pogróżki przy użyciu anonimizującej sieci Tor, co utrudnia namierzenie sprawcy. Ze względu na rozgłos medialny, jaki jest efektem tych działań, metoda wciąż znajduje naśladowców.

W 2021 r. przestępcy zaczęli dodatkowo podszywać się pod znane osoby publiczne, polityków, dziennikarzy, a także pracowników instytucji zajmujących się cyberbezpieczeństwem. Przestępcy zakładali skrzynki do rozsyłania gróźb, zawierając w loginie imię i nazwisko danej osoby. Dane osobowe zawarte były również w treści wiadomości. Charakter wykorzystania skrzynek i treść wiadomości odpowiadała dotychczasowym schematom, jednak wykorzystanie danych osobowych budziło dodatkowy rozgłos i prowokowało adresatów do prób kontaktu z osobą, pod którą się podszywano np. celem zweryfikowania pochodzenia wiadomości.

Pod koniec roku kampania została rozszerzona o telefony z pogróżkami, w których podstawiano fałszywy numer dzwoniącego, czyli stosowano tzw. Caller ID spoofing. Jest to możliwe dzięki specjalnym bramkom internetowym VoIP, z których można wykonywać połączenia z wykorzystaniem dowolnego numeru telefonu. Co ważne, technika ta nie wymaga przejęcia kontroli nad telefonem ofiary. Bramki tego typu wykorzystują słabości protokołów używanych w sieciach komórkowych. Oznacza to, że operatorzy sieci komórkowych często nie są w stanie zweryfikować, czy połączenie w ramach którego jest prezentowany numer faktycznie pochodzi z karty SIM, która jest zarejestrowana dla danego numeru. Warto mieć na uwadze, że Caller ID Spoofing nie jest nową techniką i jest powszechnie wykorzystywany również w atakach phishingowych, gdzie przestępcy podszywają się pod bank lub lokalny komisariat policji. Podobny spoofing można zastosować również w przypadku wiadomości SMS, by podstawić dowolny numer lub nazwę w polu nadawcy.

Aby dodatkowo uwiarygodnić groźby, w kampaniach telefonicznych wykorzystywano informacje zebrane z publicznie dostępnych źródeł takich jak profile społecznościowe czy wycieki baz danych ze sklepów internetowych. Źródła były wykorzystywane do pozyskania numerów telefonów (zarówno ofiar podszycia się, jak i adresatów gróźb), a także innych danych osobowych. Połączenia wykonywane były z wykorzystaniem syntezatora głosu, który czytał tekst wiadomości.

W przypadku gdy nie mamy pewności, że połączenie telefoniczne, które otrzymaliśmy faktycznie pochodzi z wyświetlanego numeru telefonu – najlepiej rozłączyć się i oddzwonić. Warto mieć na uwadze, że spoofing jest wykorzystywany również w klasycznych oszustwach. W przypadku gdy otrzymujemy telefon z banku i nie mamy pewności co do tożsamości rozmówcy, często banki udostępniają możliwość uwierzytelnienia ze strony pracownika banku za pośrednictwem osobnego kanału, np. wyświetlając powiadomienie w aplikacji zainstalowanej na telefonie lub w ramach serwisu internetowego.

Kampanie złośliwego oprogramowania Formbook/XLoader

W 2021 r. zauważyliśmy wzrostowy trend wykorzystania złośliwego oprogramowania z rodziny Formbook/Xloader. Na podstawie danych z systemu MWDB, w tym roku dodanych zostało 6205 próbek należących do tej rodziny, z których udało się uzyskać 1342 unikalnych konfiguracji tego trojana.

Formbook jest wielofunkcyjnym trojanem dzia-

łającym na systemach Windows, pozwalającym między innymi na wykradanie danych logowania z formularzy, zarówno w przeglądarkach jak i programach pocztowych. Wśród funkcji można również znaleźć monitorowanie wciśnięć klawiszy, schowka oraz zdalne tworzenia zrzutów ekranu zainfekowanego urządzenia.

Po raz pierwszy został zaobserwowany na początku 2016 r.[86] i był dostępny do kupienia w formie „malware-as-a-service" (MaaS), co pozwalało na uzyskanie dostępu do skompilowanego oprogramowania oraz do panelu C&C działającego na serwerze autora. Dodatkowo możliwe było wykupienie kodu źródłowego samego panelu C&C oraz uruchomienie go na własnym serwerze. Po pierwszym roku działania Formbooka, autor nagle zakończył sprzedaż złośliwego oprogramowania, jako powód podając wykorzystanie programu w złośliwych kampaniach. Nie przeszkodziło to jednak przestępcom z dostępem do kodu źródłowego panelu C&C w dalszym korzystania z wykupionego narzędzia, a sam Formbook stał się jedną z najpopularniejszych rodzin złośliwego oprogramowania[87].

Rys. 53. Oferta sprzedaży Formbooka[88].

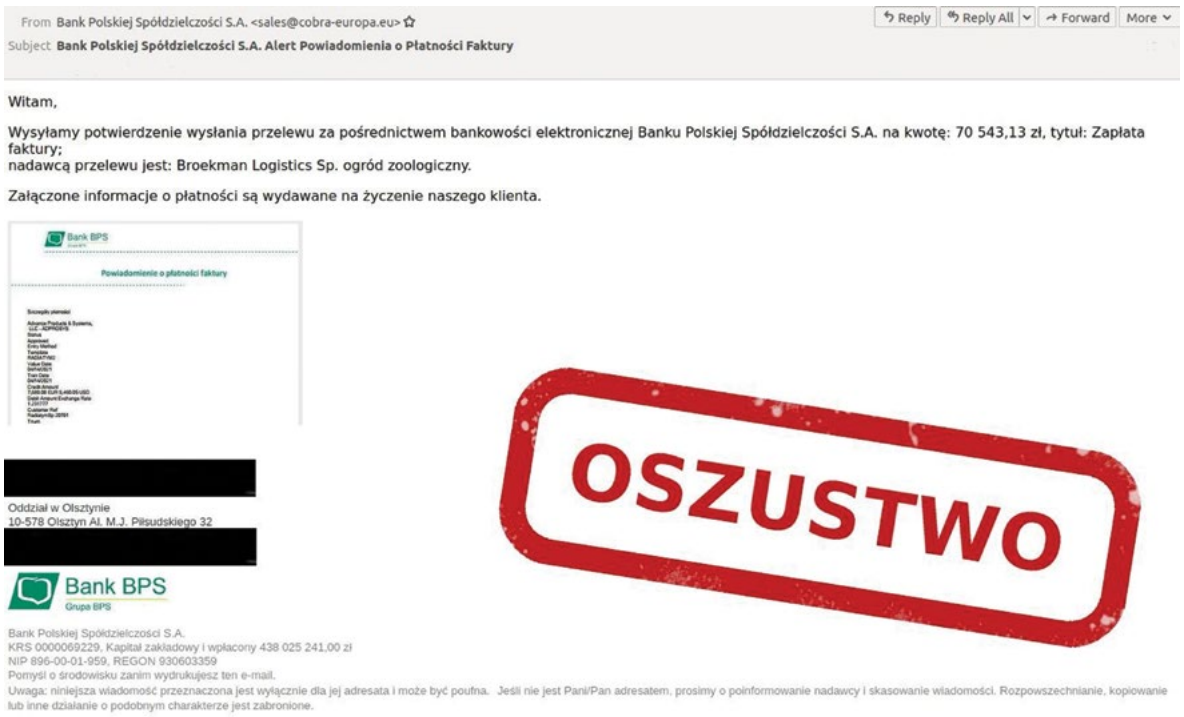
86. https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Nicolao.pdf
87. https://any.run/malware-trends/
88. https://www.mandiant.com/resources/formbook-malware-distribution-campaigns

Po czterech latach, w 2020 r. , na forum pojawiło się ogłoszenie reklamujące sprzedaż nowego trojana o nazwie Xloader, którego analiza szybko wykazała duże podobieństwo z wcześniej sprzedawanych Formbookiem. Inaczej niż w poprzednim przypadku, trojan został opublikowany w dwóch wersjach – na urządzenia z systemem Windows oraz MacOS. Dodatkowo sprzedawca zrezygnował ze sprzedaży kodu źródłowego panelu oraz zezwolił jedynie na ograniczony czasowo dostęp do narzędzia. Od tego momentu nazwy Formbook oraz Xloader stosowane są zamiennie.

Rys. 54. Oferta sprzedaży XLoadera[90].

Najczęstszym wektorem infekcji tą rodziną złośliwego oprogramowania są załączniki w e-mailach phishingowych, często podszywających się pod istniejące przedsiębiorstwa. Wiadomości te nakłaniają do opłacenia zaległych faktur lub opłat za wysyłkę zamówionego towaru. Coraz częściej zamiast załącznika dodawane jest hiperłącze kierujące do pobrania złośliwego pliku. Na rysunku 55. widoczna jest wiadomość z kampanii podszywającej się pod bank BPS, w której po kliknięciu w obrazek będący jednocześnie hiperłączem, pobierane było archiwum w formacie ISO. Jego odpakowanie oraz uruchomienie zawartego w nim pliku wykonywalnego kończyło się infekcją oprogramowaniem z rodziny Formbook/Xloader.

90. https://research.checkpoint.com/2021/top-prevalent-malware-with-a-thousand-campaigns-migrates-to-macos/



Rys. 55. Przykład wiadomości podszywającej się pod wizerunek banku BPS[91].

91. https://twitter.com/CERT_Polska/status/1433359784569364483/photo/1

STATYSTYKI

W tej części raportu prezentujemy statystyki dotyczące zdarzeń przetwarzanych automatycznie, przede wszystkim z wykorzystaniem platformy n6[92]. 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.

Dokładność i ograniczenia przedstawionych statystyk

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 5. prezentuje liczbę zainfekowanych komputerów w polskich sieciach. W 2021 r. łącznie zgromadziliśmy informacje o 439 077 adresach IP wykazujących aktywność zombie. Jest to spadek o około 200 tys. w porównaniu z 2020 r.

92. https://n6.cert.pl/

	Rodzina	Maksimum dzienne	Średnia dzienna	Odchylenie standardowe
1	Andromeda	3 139	1 927	498
2	Avalanche	2 028	867	296
3	Conficker	1 962	832	360
4	Flubot	1 638	122	218
5	QSnatch	1 192	939	170
6	Nymaim	1 044	90	178
7	Hummer	833	391	177
8	ISFB	816	438	180
9	Mirai	752	334	144
10	Necurs	558	309	103

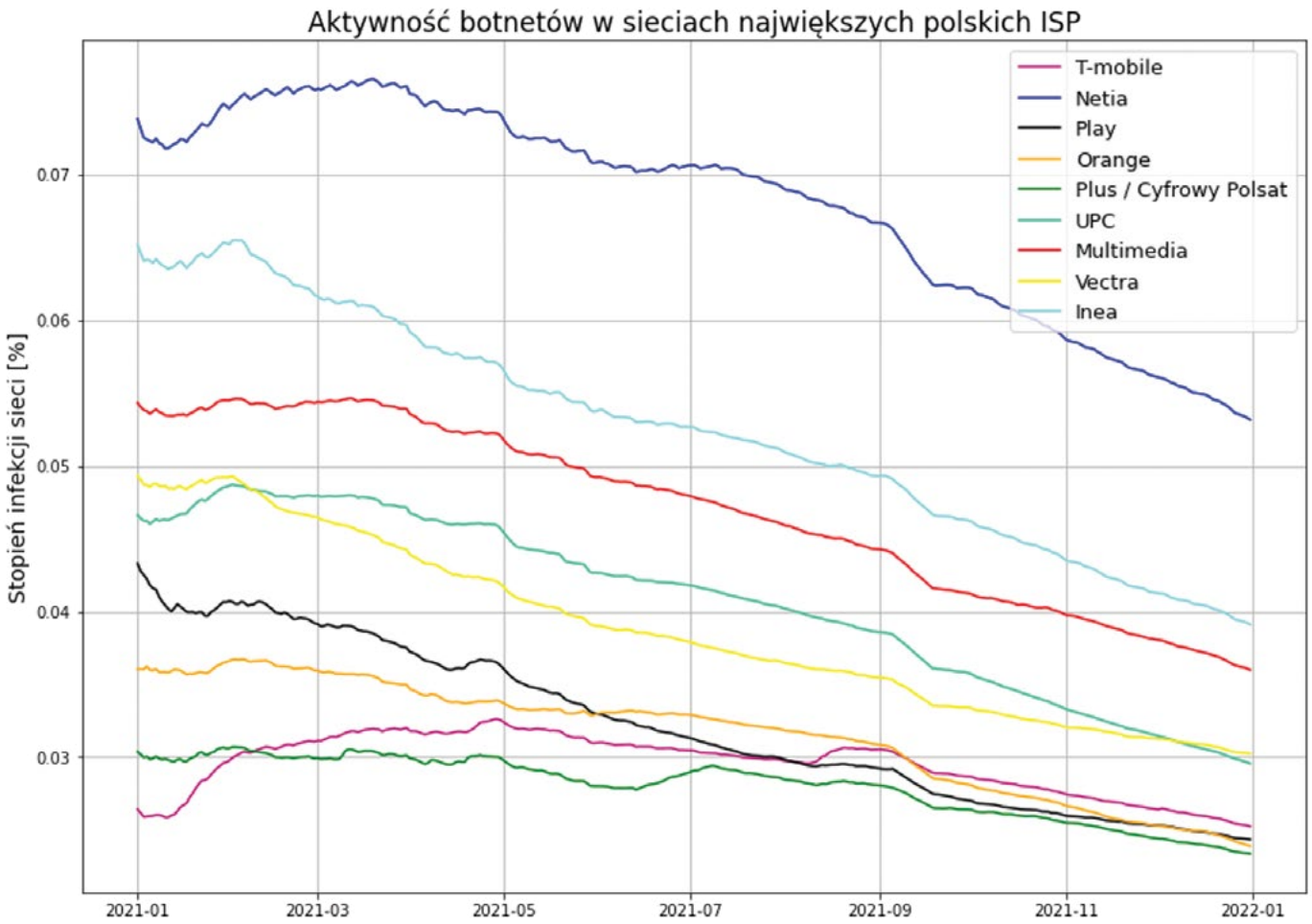
Tab. 5. Największe botnety w Polsce.

W polskich sieciach od lat obserwujemy aktywność botnetów, które są już sinkholowane. Przykładem takiego botnetu jest Andromeda, który po raz kolejny znalazł się na pierwszym miejscu powyższego zestawienia ze średnią dzienną liczbą zainfekowanych urządzeń na poziomie dochodzącym prawie do 2 tys. W przypadku tego botnetu, podobnie jak w 2020 r., widzimy dalszy stopniowy spadek w skali roku. Na początku roku notowaliśmy średnio wartości bliskie 2500 adresów IP, natomiast w końcówce roku poziom ten zbliżył się do 1500 adresów. Trend spadkowy zarejestrowaliśmy także w infekcjach urządzeń QNAP Systems botnetem QSnatch. Był to spadek o około 500 adresów IP, porównując wartości ze stycznia i grudnia 2021 r. Tendencję spadkową widzimy też w przypadku botnetów Avalanche i Conficker. Po raz kolejny w zestawieniu pojawia się botnet IoT Mirai. W ujęciu miesięcznym średnio 334 urządzenia IoT z adresami IP wykazywało infekcję tą rodziną. Jest to poprawa o około 200 urządzeń w porównaniu z 2020 r.

Aktywność botnetów z podziałem na operatorów telekomunikacyjnych

Na wykresie 6. 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 2020 r." wydanego przez Urząd Komunikacji Elektronicznej[93].

93. https://www.uke.gov.pl/download/gfx/uke/pl/defaultaktualnosci/36/391/10/raport_o_stanie_rynku_telekomunikacyjnego_w_polsce_w_2020_roku_.pdf



Wykres 6. Aktywność botnetów w sieciach największych ISP w 2021 r.

W 2021 r. średnia dzienna liczba zainfekowanych urządzeń w polskim internecie wynosiła 6621. Na przestrzeni roku obserwujemy konsekwentną tendencję spadkową. W styczniu 2021 r. w polskich sieciach stopień infekcji wynosił około 9 tys. urządzeń. W połowie roku liczba zainfekowanych urządzeń osiągnęła poziom około 7 tys., natomiast w końcówce roku liczba ta zatrzymała się na poziomie 4 tys.

Podobnie jak w ubiegłych latach największy odsetek zainfekowanych użytkowników oszacowaliśmy w sieciach dostawcy Netia. W przypadku tego operatora zachowany został malejący trend. Znaczny spadek stopnia infekcji sieci na przestrzeni roku dotyczy także pozostałych polskich dostawców, co jest korzystną zmianą, ponieważ tendencja spadkowa w ubiegłym roku nie była aż tak wyraźna. W przypadku każdego z operatorów stopień infekcji nie przekraczał jednego promila.

W przypadku botnetu Andromeda największą liczbę zainfekowanych urządzeń obserwujemy w sieciach Orange oraz Plus i Cyfrowy Polsat. Dzienna liczba adresów IP utrzymuje się na poziomie powyżej 300 adresów. Najwięcej zainfekowanych urządzeń NAS mają użytkownicy w sieciach Orange (średnio 250 urządzeń) oraz UPC (średnio 150 urządzeń). Infekcje botnetem Conficker obserwowaliśmy najczęściej u operatorów Orange oraz Netia (średnio 100 urządzeń w obu przypadkach). Podobnie jak w ubiegłym roku infekcje botnetem Mirai obserwowaliśmy głównie w sieciach Orange. W pozostałych sieciach problem infekcji Miraiem był marginalny.

Serwery C&C

W 2021 r. zebraliśmy informacje o 9410 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. Podobnie jak w poprzednich latach najwięcej złośliwych serwerów było zlokalizowanych w Stanach Zjednoczonych (33 proc.). 68 proc. spośród wszystkich serwerów C&C utrzymywanych było w 10 krajach przedstawionych w tabeli 6. Zaobserwowaliśmy serwery w 136 krajach na całym świecie.

Poz.	Kraj	Liczba adresów IP	Udział
1	USA	3 089	32,83%
2	Holandia	694	7,38%
3	Niemcy	566	6,01%
4	Rosja	465	4,94%
5	Tajlandia	412	4,38%
6	Chiny	326	3,46%
7	Wielka Brytania	225	2,39%
8	Francja	212	2,25%
9	Indie	183	1,94%
10	Hongkong	182	1,93%
...	...	...	...
30	Polska	59	0,63%

Tab. 6. Kraje z największą liczbą serwerów C&C.

Zaobserwowaliśmy 1580 różnych systemów autonomicznych (AS), w których umiejscowione były serwery C&C. Dziesięć systemów autonomicznych zawierało ponad 28 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	727	7,73%
2	14061	DigitalOcean	353	3,75%
3	45629	JasTel	314	3,34%
4	16509	Amazon	271	2,88%
5	36352	ColoCrossing	203	2,16%
6	15169	Google	181	1,92%
7	16276	OVH	172	1,83%
8	9009	M247	158	1,68%
9	213035	Des Capital	154	1,64%
10	46606	Unified Layer	143	1,52%

Tab. 7. Systemy autonomiczne z największą liczbą serwerów C&C.

W Polsce serwery C&C były aktywne pod 59 różnymi adresami IP (30. miejsce na świecie, z udziałem 0,63 proc.) w 34 systemach autonomicznych. W tabeli 8. prezentujemy zestawienie systemów autonomicznych, w których znajdowało się najwięcej złośliwych serwerów zarządzających botnetami. W sumie zawierały one prawie 60 proc. wszystkich serwerów C&C w Polsce.

Poz.	Numer AS	Nazwa	Liczba adresów IP	Udział
1	204957	Green Floid	7	11,86%
2	20940	Akamai	7	11,86%
3	51290	Hosteam	3	5,08%
4	16625	Akamai	3	5,08%
5	21021	Multimedia	3	5,08%
6	57509	L&L	2	3,39%
7	12824	home.pl	2	3,39%
8	197226	Sprint	2	3,39%
9	12912	T-Mobile	2	3,39%
10	35787	Internet Cafe	2	3,39%
11	201814	Meverywhere	2	3,39%

Tab. 8. Systemy autonomiczne, w których hostowanych jest najwięcej serwerów C&C w Polsce.

Otrzymaliśmy również zgłoszenia o 6291 pełnych nazwach domenowych (FQDN), które pełniły rolę serwerów zarządzających botnetami. Zostały one zarejestrowane w obrębie 222 domen najwyższego poziomu (TLD), z czego prawie 58 proc. w *.com*.

Zestawienie najpowszechniejszych TLD przedstawiamy w tabeli 9. Jako serwery C&C było wykorzystywanych 6 domen *.pl*.

Poz.	TLD	Liczba domen	Udział
1	.com	3 645	57,94%
2	.net	321	5,10%
3	.xyz	313	4,98%
4	.org	277	4,40%
5	.ru	169	2,68%
6	.id	140	2,22%
7	.info	58	0,92%
8	.club	54	0,86%
9	.online	52	0,83%
10	.top	44	0,70%
...	...	...	...
54	.pl	6	0,10%

Tab. 9. 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 ani do wyłudzania danych przy pomocy złośliwego oprogramowania, ani do podszywania się pod dostawców faktur, np. w celu dystrybucji złośliwego oprogramowania.

W 2021 r. otrzymaliśmy łącznie 18 852 zgłoszenia phishingu w polskich sieciach. Dotyczyły one 7508 adresów URL z 4076 domenami prowadzącymi do stron, które rozwiązywały się na 1002 adresy IP. Oznacza to, że liczba systemów umiejscowionych w polskich adresach jako infrastruktura phishingowa w porównaniu z poprzednim rokiem jest na zbliżonym poziomie. Obserwując wyniki poszczególnych systemów autonomicznych, znaczna przewaga firmy home.pl wynika prawdopodobnie z jej oferty handlowej, która jest atrakcyjna również dla przestępców .

Poz.	Numer AS	Nazwa AS	Liczba adresów IP	Liczba domen
1	12824	home.pl	293	902
2	15967	Nazwa.pl	164	346
3	20940	Akamai Technologies	73	ZX34
4	16625	Akamai Technologies	57	115
5	41079	H88	39	795
6	16276	OVH	26	54
7	203417	LH.pl	25	196
8	29522	KEI.PL	24	45
9	57367	Atman	21	36
10	43641	Sollutium	21	31

Tab. 10. Polskie systemy autonomiczne, w których znajdowało się najwięcej stron phishingowych.

Złośliwe strony

W ubiegłym roku zebraliśmy informacje o 2 915 585 adresach URL związanych z działalnością szkodliwego oprogramowania, z czego 47 742 adresy były w domenie *.pl*, a 43 125 rozwiązywało się na polskie adresy IP.

Najpopularniejszą domeną drugiego poziomu w domenie *.pl* wśród adresów URL było home.pl (5328 wystąpień).

Analogicznie zebraliśmy informacje o 266 748 nazwach domenowych, z czego 3754 nazwy były w domenie *.pl*, a 3154 rozwiązywało się na polskie adresy IP. Najpopularniejsze adresy IP, w których znajdowały się te domeny, przedstawiono w tabeli 11.

Najczęściej występującymi domenami drugiego poziomu w domenie *.pl*, wśród nazw domenowych były *com.pl* (237 wystąpień), *home.pl* (177 wystąpień) oraz *neostrada.pl* (131 wystąpień).

Poz.	Liczba domen .pl	Adres IP	ASN	Nazwa
1	141	217.97.216.17	5617	Orange
2	103	3.121.154.182	16509	Amazon
3	89	91.212.150.245	43350	nForce
4	71	172.67.169.11	13335	Cloudflare
5	71	104.21.27.72	13335	Cloudflare
6	57	37.59.49.187	16276	OVH
7	56	176.31.124.7	16276	OVH
8	21	212.180.187.186	9085	Supermedia
9	18	195.78.67.35	41079	Cyber Folks
10	17	5.252.231.39	203417	LH.pl

Tab. 11. Adresy IP, na których utrzymywano najwięcej domen .pl związanych ze złośliwym oprogramowaniem.

Poz.	Liczba IP	ASN	Nazwa	Odsetek wszystkich adresów w AS	Udział
1	211 824	4837	China Unicom	0,36%	36,78%
2	67 017	9829	National Internet Backbone	1,24%	11,64%
3	43 327	4134	Chinanet	0,04%	7,52%
4	29 681	17816	China Unicom	0,76%	5,15%
5	28 262	8661	Telekomi i Kosoves	67,32%	4,91%
6	24 406	13335	Cloudflare	1,53%	4,24%
7	18 708	17622	China Unicom	2,66%	3,25%
8	15 241	17488	Hathway	1,52%	2,65%
9	7 518	17623	China Unicom	1,15%	1,31%
10	6 836	46606	Unified Layer	0,53%	1,19%

Tab. 12. Systemy autonomiczne, w których znajdowało się najwięcej adresów IP związanych ze złośliwym oprogramowaniem.

Usługi pozwalające na prowadzenie ataków DRDoS

W 2021 r. otrzymaliśmy informacje o 614 404 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 2021 r.

Poz.	Nazwa podatności / otwartej usługi	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odchylenie standardowe	Czas obserwacji
1	resolver	31 920	43 039	4 862	97,80%
2	SNMP	26 291	31 352	2 619	97,53%
3	portmapper	17 453	23 045	1 428	95,34%
4	SSDP	15 659	18 817	1 422	96,43%
5	NTP	15 646	17 787	618	97,26%
6	NetBIOS	11 613	13 437	763	96,43%
7	mDNS	4 127	5 117	398	95,34%
8	mssql	2 512	3 311	515	95,89%
9	chargen	181	292	54	97,26%
10	qotd	40	61	9	95,06%
11	xdmcp	11	33	7	97,26%

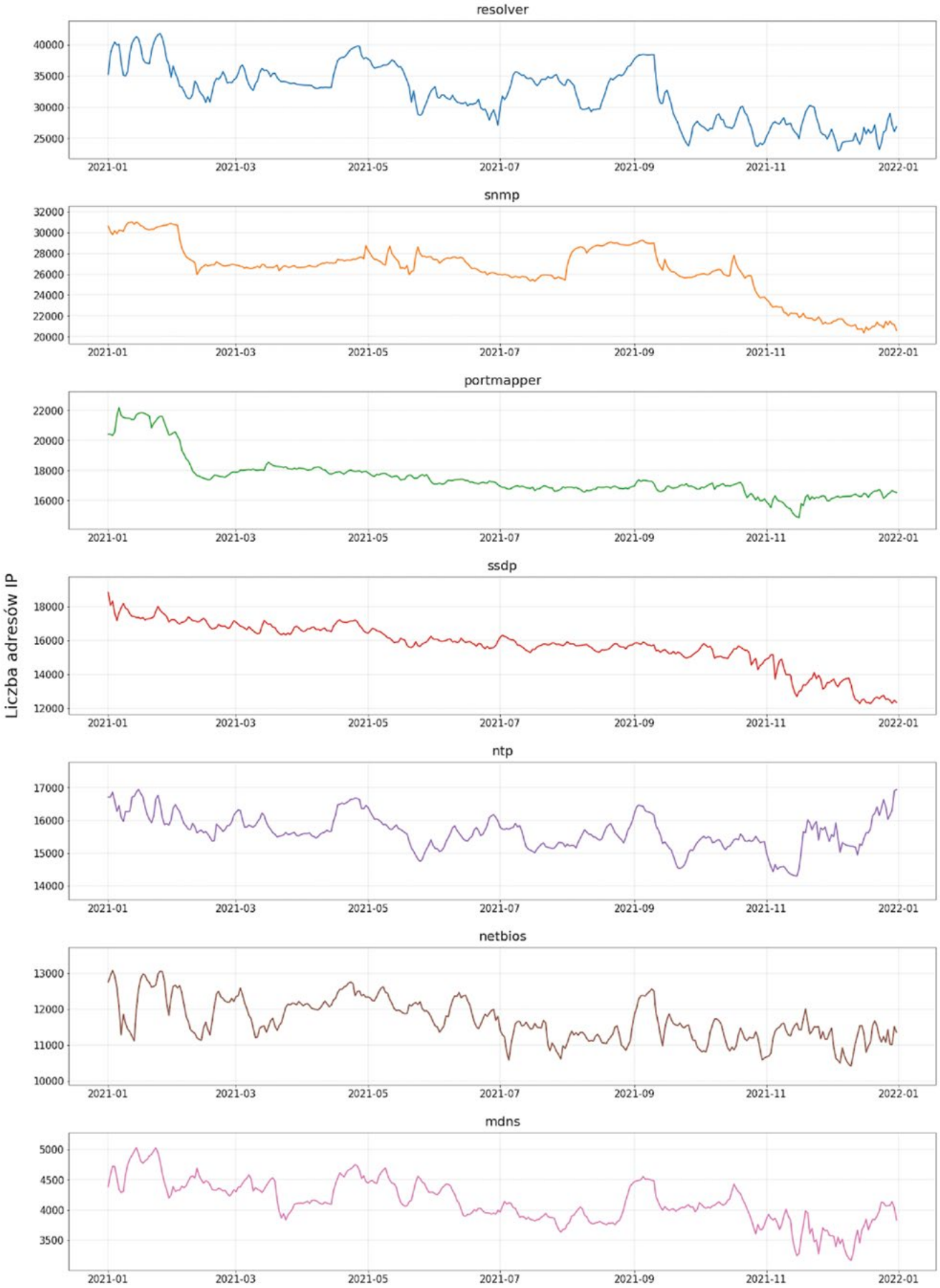
Tab. 13. Zestawienie najczęściej występujących niepoprawnie skonfigurowanych usług możliwych do wykorzystania w atakach DRDoS. Odchylenie standardowe dotyczy zmienności w dziennej liczbie adresów IP obserwowanych na przestrzeni roku, łączny czas obserwacji odpowiada części roku, dla której mieliśmy informacje o danej usłudze.

Przy analizie danych o usługach pozwalających na prowadzenie ataków DRDoS oraz usługach ze znanymi podatnościami w 2021 r. zastosowaliśmy podobną metodykę jak ta, która została wprowadzona po raz pierwszy w raporcie z 2020 r. Także w 2021 r. dysponowaliśmy niekompletnymi danymi pochodzącymi z niektórych systemów autonomicznych w pewnych okresach czasu. Problem dotyczył głównie jednego z systemów autonomicznych należących do Orange (AS5617). 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 Shadowserver jest dostępnych na stronie organizacji[94]). 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 dokładnie w raporcie z 2020 r. Zainteresowanych zachęcamy do lektury raportu z 2020 r. w celu zapoznania się ze szczegółami. Następnie na podstawie skorygowanych danych powstały tabele i wykresy umieszczone w raporcie.

Na wykresie 7. 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, SNMP, portmapper oraz SSDP na przestrzeni całego roku. W przypadku usług NTP, Netbios i mDNS liczba adresów IP utrzymuje się na podobnym poziomie w skali roku.

94. https://www.shadowserver.org/what-we-do/



Wykres 7. Najpowszechniejsze źle skonfigurowane usługi mogące brać udział w atakach DRDoS. Wykres ukazuje zmiany liczebności podatnych adresów IP w Polsce w 2021 r.

Otwarte serwery DNS

Najpopularniejszą obserwowaną w 2021 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 2021 r. otrzymaliśmy 11 250 637 zgłoszeń o 164 009 adresach IP z uruchomionym otwartym resolverem – to spadek o niecałe 10 proc. adresów w porównaniu z rokiem 2020, co świadczy o niewielkiej poprawie. Dzienna średnia liczba adresów wynosi obecnie 31 920. Na przestrzeni 2021 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. 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 zmiany są niewielkie. W przypadku AS15969 niepokoić może wysoki odsetek adresów (10 proc.), które mogą zostać wykorzystane do ataku DRDoS. Jeszcze gorzej sytuacja wygląda w przypadku AS200889, gdzie ponad 50 proc. adresów IP jest podatnych. W porównaniu z 2020 r. ponownie obserwujemy spadek liczby otwartych resolverów w sieci Netia (AS12741) – średnia dzienna liczba zmalała o 124 w stosunku do poprzedniego roku.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	19241	28949	0,35%
2	12741	Netia	1215	1480	0,07%
3	6830	UPC	461	518	0,01%
4	13110	Inea	409	470	0,24%
5	29314	Vectra	321	387	0,06%
6	15969	SYSTEMIA	301	347	9,80%
7	5588	T-Mobile	283	339	0,02%
8	12912	T-Mobile	283	372	0,04%
9	8374	Plus / Cyfrowy Polsat	280	317	0,02%
10	200889	MARIANWITEK	276	320	53,91%

Tab. 14. 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 2021 r. otrzymaliśmy 9 094 972 zgłoszenia o 155 046 adresach z uruchomionym SNMP, co oznacza spadek o około 23 proc. w liczbie adresów w porównaniu do 2020 r. Natomiast najistotniejszy wskaźnik, czyli dzienna średnia liczba wystąpień, wyniosła 26 291 adresów, co stanowi wzrost o około 12 proc. względem poprzedniego roku. Ponownie na pierwszym miejscu znalazł się AS12741 należący do Netii. Patrząc na dane tylko z 2021 r. można zauważyć tendencję spadkową, widoczną szczególnie w końcówce roku. Jest to spowodowane przede wszystkim gwałtownym spadkiem w należącym do Netii AS12741, który mógł wynikać np. ze zmian w konfiguracji urządzeń w systemie autonomicznym tego operatora. W 2021 r. po raz pierwszy na liście pojawił się Digicom (AS57978) z wysokim odsetkiem adresów w AS. Jedynie w przypadku tego dostawcy obserwowaliśmy niewielki wzrost w ciągu roku. Niepokoić może po raz kolejny wysoki odsetek adresów w systemie autonomicznym Net Center (AS60920) – ponad 22 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	8 630	10 955	0,52%
2	5617	Orange	2 857	3 476	0,02%
3	20804	TELENERGO	875	960	0,36%
4	60920	NETCENTER	691	763	22,49%
5	56515	OXYNET	505	659	3,79%
6	202281	C3	422	888	8,24%
7	199390	ALFAKS	400	998	13,02%
8	4	ISI	358	419	0,55%
9	8374	Plus / Cyfrowy Polsat	329	381	0,02%
10	57978	DIGICOM	324	452	15,82%

Tab. 15. 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 2021 r. otrzymaliśmy 5 954 751 zgłoszeń o 64 713 adresach IP z usługą portmapper dostępną na publicznym interfejsie. Dzienna średnia wynosiła 17 453 adresy, co oznacza spadek o prawie 7 proc. względem roku 2020. W drugiej połowie lutego 2021 r. zaobserwowaliśmy spadek z poziomu mniej więcej 21 tys. adresów do poziomu 18 tys. Liczba ta utrzymywała się w dalszej części roku z niewielką tendencją spadkową, by w grudniu ostatecznie osiągnąć poziom około 16 tys. adresów IP. Gwałtowny spadek jest spowodowany przez AS61317, który jest liderem naszego zestawienia. Takie sytuacje mogą wynikać np. z aktualizacji konfiguracji maszyn u tych dostawców usług lub wprowadzenia odpowiednich reguł filtrowania ruchu. W pozostałych systemach autonomicznych sytuacja była dość stabilna z niewielką tendencją spadkową. Podobnie jak w 2020 r. wysoko w zestawieniu znajdują się ATMAN (AS57367) oraz OVH (AS16276) ze zbliżoną średnią liczbą adresów IP w porównaniu do roku ubiegłego. Nowością w zestawieniu jest Data Space (AS57367), gdzie widzimy wysoki odsetek zainfekowanych adresów IP (prawie 7 proc.).

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	61317	ASDETUK	2559	5864	0,24%
2	57367	ATMAN	1330	1400	8,12%
3	50599	Data Space	841	1049	6,70%
4	16276	OVH	825	1085	0,02%
5	5617	Orange	712	1147	0,01%
6	20804	TELENERGO	604	885	0,25%
7	59491	LIVENET	414	689	5,78%
8	47329	WDM	406	422	4,17%
9	12741	Netia	391	453	0,02%
10	197155	ARTNET	339	418	3,01%

Tab. 16. Dzienna liczba adresów, na których wykryto działającą usługę Portmapper 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 2021 r. otrzymaliśmy 5 311 285 zgłoszeń o 170 969 adresach IP związanych z usługą SSDP. Jeśli chodzi o liczbę adresów IP to ponownie zanotowaliśmy spadek o prawie 7 proc. w porównaniu z 2020 r. Spadek nie jest jednak aż tak znaczny jak w porównaniu między 2020 i 2019 r., gdy wynosił ponad 50 proc. Dzienna średnia liczba wystąpień wyniosła 15 659 adresów, co stanowi wzrost o ponad 20 proc. w porównaniu z rokiem poprzednim. Natomiast w przeciągu roku notowaliśmy systematyczny spadek liczby adresów IP. AS5617 należący do Orange kolejny rok znalazł się na pierwszej pozycji w zestawieniu. W przypadku tego systemu autonomicznego zanotowaliśmy skokowy spadek liczby adresów IP w połowie listopada 2021 r. z poziomu 2 tys. na poziom 500 adresów. Na uwagę zasługuje ponownie wysoki odsetek adresów w systemie autonomicznym należącym do DERKOM (AS197697) – w 2021 r. wynosi on 20 proc. Jest to znaczący wzrost w porównaniu z rokiem ubiegłym, gdy wynosił on około 12 proc.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	1912	3016	0,03%
2	197697	DERKOM	1732	2051	21,14%
3	29314	Vectra	1119	1638	0,21%
4	12741	Netia	762	941	0,05%
5	8374	Plus / Cyfrowy Polsat	529	615	0,04%
6	41023	ARREKS	458	497	12,78%
7	50231	SYRION	221	325	0,88%
8	31242	TKPSA	213	370	0,19%
9	199201	SPI-NET	213	291	6,93%
10	12912	T-Mobile	206	239	0,03%

Tab. 17. Dzienna liczba adresów, na których wykryto działającą usługę SSDP 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 2021 r. otrzymaliśmy łącznie 5 385 816 zgłoszeń o 30 730 adresach IP, co stanowi spadek o niecałe 8 proc. w porównaniu z rokiem poprzednim. Przypomnijmy, że poprzednio spadek ten był dużo większy, bo wynosił około 85 proc. adresów. Dzienna średnia liczba wystąpień wyniosła 15 646 adresów. W przypadku tej usługi dzienna liczba adresów IP oscylowała względem mniej więcej tego samego poziomu w skali roku. W porównaniu z poprzednim rokiem zmalała liczba adresów obsługujących ten protokół w systemie autonomicznym Orange (AS5617) – spadek o około 700 adresów. W przypadku Netii i T-Mobile (znajdujących się na drugim i trzecim miejscu w zestawieniu) liczba ta utrzymywała się na podobnym poziomie.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	1434	2595	0,03%
2	12741	Netia	1430	1651	0,09%
3	5588	T-Mobile	1056	1203	0,08%
4	48956	HYPERNET	358	505	7,77%
5	199715	MSITELEKOM	350	394	2,24%
6	20960	TKTELEKOM	320	352	0,13%
7	20804	TELENERGO	257	379	0,11%
8	8798	PAGI	253	394	2,82%
9	9085	SUPERMEDIA	243	274	0,57%
10	31242	TKPSA	242	312	0,21%

Tab. 18. Dzienna liczba adresów, na których wykryto działającą usługę NTP 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 i nie jest to związane wyłącznie z możliwością wykorzystania usługi w atakach DDoS.

W 2021 r. trzymaliśmy 3 934 411 zgłoszeń o 44 254 adresach IP, co stanowi spadek o ponad 10 proc. w porównaniu z 2020 r. Dzienna średnia liczba wystąpień wyniosła 11 613 adresów i jest to wartość o ponad 8 proc. mniejsza niż w roku poprzednim. Przez większość roku obserwowaliśmy utrzymującą się na stałym poziomie liczbę adresów IP z uruchomioną usługą NetBIOS. Wszystkie systemy autonomiczne z poniższej tabeli wykazywały podobny przebieg do wykresu ogólnego. Podobnie jak w 2020 r., na dwóch pierwszych miejscach zestawienia znalazły się systemy autonomiczne należące do Orange i Netii z porównywalną z rokiem ubiegłym średnią liczbą adresów IP.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	7162	9007	0,13%
2	12741	Netia	612	722	0,04%
3	13110	Inea	127	151	0,08%
4	12824	home.pl	122	141	0,06%
5	8267	CYFRONET	105	136	0,14%
6	8374	Plus / Cyfrowy Polsat	94	124	0,01%
7	5588	T-Mobile	77	95	0,01%
8	8970	WASK WROCMAN	76	152	0,12%
9	31242	TKPSA	76	91	0,07%
10	197226	SPRINT	66	84	0,46%

Tab. 19. Dzienna liczba adresów, na których wykryto działającą usługę NetBIOS 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 2021 r. odnotowaliśmy 45 199 753 takie obserwacje, dotyczące 1 250 311 adresów IP z Polski.

Na kolejnych stronach raportu przedstawiamy szczegółowe informacje o zagrożeniach, które najczęściej występują w polskich sieciach. Zaprezentowane 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). Z tego powodu użyliśmy tej samej metody szacowania.

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. 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	35 829	167 047	50 592	96,71%
2	SSL-POODLE	26 167	37 277	3 634	96,71%
3	RDP	14 178	22 656	2 205	96,98%
4	Telnet	13 269	20 344	2 236	96,34%
5	TFTP	11 599	17 958	2 593	95,06%
6	BadWPAD	9 109	13 030	1 465	99,17%
7	ISAKMP	5 698	7 563	560	95,89%
8	VNC	3 993	7 857	976	96,43%
9	SSL-FREAK	3 518	5 750	911	97,26%
10	SMB	3 162	4 532	472	97,26%
11	NAT-PMP	1 861	2 520	370	95,34%
12	IPMI	712	974	168	96,43%
13	MongoDB	563	607	26	96,16%
14	Memcached	173	198	19	96,71%
15	LDAP	83	110	10	96,43%
16	Elasticsearch	56	70	7	96,98%
17	Redis	38	61	8	96,43%

Tab. 20. 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.

Porównując rok 2021 z 2020 zauważamy brak zmian na pierwszych siedmiu miejscach zestawienia. Wciąż na pierwszym miejscu znajduje się protokół CWMP. Należy jednak zauważyć znaczną zmianę średniej dziennej liczby adresów IP w tym przypadku. Zanotowaliśmy spadek o około 60 tys.

Na wykresie 8. 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 siedmiu najczęściej zgłaszanych usług.

Patrząc na wykres możemy zauważyć pozytywny trend w zakresie stopniowego spadku liczby urządzeń związanych z podatnością Poodle i usługami RDP oraz Telnet na przestrzeni całego roku. Jest to kontynuacja trendu spadkowego z ubiegłego roku. Szczególną uwagę zwraca wykres dla usługi CWMP. W jej przypadku liczba adresów IP utrzymywała się na stabilnym poziomie (podobnym do poziomu z drugiej połowy 2020 r.) aż do połowy lutego 2021 r. Następnie od tego momentu zanotowaliśmy duży spadek z poziomu około 160 tys. na poziom 15 tys. Miał na to wpływ AS6830 należący do UPC. W 2020 r. mieliśmy do czynienia z sytuacją odwrotną, gdy zanotowaliśmy gwałtowny wzrost dziennej liczby adresów IP w połowie roku i także było to spowodowane danymi pochodzącymi ze wspomnianego systemu autonomicznego.

Wykres 8. Najpowszechniejsze zagrożone usługi. Wykres ukazuje zmiany liczebności podatnych adresów IP w Polsce w 2021 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 2021 r. otrzymaliśmy 12 238 412 zgłoszeń o 597 642 adresach IP z dostępną publicznie usługą CWMP. Jest to spadek o około 45 proc. adresów w porównaniu do 2020 r. i spadek o ponad 60 proc. w porównaniu z 2019 r. Dzienna średnia liczba adresów wynosiła 35 829, co jest prawie trzykrotnym spadkiem w porównaniu do poprzedniego roku. Najbardziej znaczący wpływ na ten spadek miał system autonomiczny UPC (AS6830). W 2021 r. średnia dzienna liczba adresów w jego przypadku wynosiła ponad 20 tys., podczas gdy rok wcześniej aż około 58 tys. Do zmiany doszło w połowie lutego, gdy z poziomu około 160 tysięcy adresów wartości zaczęły w krótkim czasie spadać by osiągnąć pułap około 15 tys., który utrzymywał się już do końca roku. Znaczny udział AS6830 w całkowitej liczbie adresów IP dla usługi CWMP determinuje kształt wykresu ogólnego. W większości z pozostałych systemów autonomicznych z tabeli zauważamy trend wzrostowy w ciągu roku. Warto także zwrócić uwagę na AS5588 należący do T-Mobile, gdzie liczba adresów IP utrzymywała się na stałym poziomie w 2021 r. po tym jak odnotowaliśmy gwałtowny spadek na początku grudnia 2020 r. do poziomu kilkuset, co mogło świadczyć o zmianie w konfiguracji urządzeń w systemie autonomicznym tego operatora. Niepokoi wysoki odsetek podatnych adresów w sieci INTERTOR (AS200125) – podatnych jest ponad 10 proc. wszystkich adresów w tym systemie autonomicznym.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	6830	UPC	20 217	151 247	0,51%
2	12741	Netia	5 256	5 895	0,32%
3	5617	Orange	3 192	4 826	0,02%
4	21021	Multimedia	1 109	1 238	0,18%
5	5588	T-Mobile	525	713	0,04%
6	44124	RYBNET	521	1 066	3,63%
7	50231	SYRION	452	970	1,80%
8	51337	DEBACOM	420	641	6,84%
9	29314	Vectra	386	527	0,07%
10	200125	INTERTOR	326	442	10,61%

Tab. 21. 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 9 081 181 zgłoszeń o 215 368 adresach IP. Jest to spadek o prawie 19 proc. adresów w porównaniu z 2020 r. Średnia dzienna liczba adresów wynosiła 26 167, co jest spadkiem o ponad 16 proc. w porównaniu do poprzedniego roku. W większości systemów autonomicznych obserwujemy stopniowy spadek w ciągu 2021 r. z niewielkim wzrostem w grudniu. Wyjątkiem jest AS59958 (P.H.U MMJ), w którym podobnie jak w 2020 r. liczba adresów stale rosła. W przypadku UPC (AS6830) zanotowaliśmy skokowy spadek na początku sierpnia, który może wskazywać na zmiany w konfiguracji urządzeń w systemie autonomicznym tego operatora. W 2020 r. w przypadku tego systemu autonomicznego mieliśmy do czynienia ze skokowym wzrostem w trakcie roku.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	12741	Netia	4 940	6 534	0,30%
2	5617	Orange	3 712	5 442	0,01%
3	6830	UPC	1 517	2 540	0,04%
4	59958	P.H.U MMJ	863	1 239	4,38%
5	43939	INTERNETIA	678	890	0,26%
6	31242	TKPSA	459	588	0,40%
7	5588	T-Mobile	446	658	0,04%
8	13110	Inea	354	479	0,21%
9	29314	Vectra	352	501	0,07%
10	29007	PETROTEL	338	450	2,06%

Tab. 22. 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 ten gwarantuje wygodny dostęp do systemów, zalecamy zamknięcie dostępu do portu 3389 na interfejsach zewnętrznych.

W 2021 r. otrzymaliśmy 4 978 071 zgłoszeń o 96 335 adresach IP (spadek o niecałe 24 proc. w porównaniu z 2020 r.), na których wykryto usługę RDP dostępną na publicznym interfejsie. Średnia dzienna liczba adresów wynosiła 14 178 (spadek o około 40 proc. w porównaniu z 2020 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 obserwujemy niewielki wzrost liczby adresów na przestrzeni roku.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	5 042	7 826	0,02%
2	12741	Netia	1 090	1 382	0,07%
3	6830	UPC	711	860	0,02%
4	12912	T-Mobile	339	401	0,05%
5	8970	WASK WROCMAN	329	402	0,50%
6	13110	Inea	328	404	0,20%
7	8374	Plus / Cyfrowy Polsat	324	395	0,02%
8	16276	OVH	278	356	0,01%
9	204957	GREENFLOID	261	442	2,08%
10	21021	Multimedia	260	355	0,04%

Tab. 23. Dzienna liczba adresów, na których wykryto usługę RDP 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 2021 r. zebraliśmy 4 640 545 zgłoszeń dotyczących 115 656 adresów IP. Jest to spadek o ponad 31 proc. w porównaniu z ubiegłym rokiem. Średnia dzienna liczba adresów wynosiła 13 269. Stanowi to spadek o ponad 37 proc. adresów w porównaniu z poprzednim rokiem. W przypadku tego protokołu średnia dzienna liczba adresów malała lub utrzymywała się na tym samym poziomie w większości systemów autonomicznych. Wyjątkiem jest jedynie AS35191, gdzie notowaliśmy niewielki wzrost w pierwszej połowie roku, a następnie liczba adresów IP utrzymywała się na względnie stałym poziomie. Wśród systemów autonomicznych z tabeli 24. negatywnie po raz kolejny wyróżnia się system autonomiczny C3 NET (AS202281), gdzie około 13 proc. wszystkich rozgłaszanych adresów posiada dostępną usługę Telnet.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	4 919	6 795	0,02%
2	12741	Netia	2 662	3 331	0,16%
3	202281	C3-NET	688	797	13,44%
4	35191	ASTA-NET	406	612	0,70%
5	8374	Plus / Cyfrowy Polsat	370	435	0,03%
6	12912	T-Mobile	370	418	0,05%
7	21021	Multimedia	310	402	0,05%
8	6830	UPC	269	315	0,01%
9	13110	Inea	238	261	0,14%
10	5588	T-Mobile	222	270	0,02%

Tab. 24. Dzienna liczba adresów, na których wykryto usługę Telnet 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 3 909 428 zgłoszeń o 85 977 adresach IP z dostępnym TFTP. Jest to spadek o około 19 proc. w porównaniu z 2020 r. i o ponad 60 proc. w porównaniu z 2019 r. Średnia dzienna liczba adresów wyniosła 11 599 i jest to spadek o około 26 proc. Patrząc na wykres ogólny nie dostrzegamy tendencji wzrostowej ani spadkowej w skali całego roku. Liczba adresów IP utrzymuje się na podobnym, stałym poziomie. Dotyczy to wszystkich systemów autonomicznych zawartych w tabeli. Podobnie jak w poprzednim roku, na pierwszym miejscu zestawienia znalazł się AS5617 należący do Orange. W szczególności zwracają na siebie uwagę wysokie odsetki adresów w systemach autonomicznych Spółdzielni Mieszkaniowej „Północ" w Częstochowie (AS198000) oraz WIFIMAX (AS199510). Podobną sytuację mieliśmy także w roku ubiegłym.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	6 178	9 300	0,08%
2	198000	SMPOLNOC	1 685	1 970	18,28%
3	12741	Netia	520	618	0,03%
4	196927	RTK	400	790	4,88%
5	21021	Multimedia	300	336	0,05%
6	199201	SPI-NET	285	617	9,28%
7	39507	IPIVISION	194	243	0,52%
8	199510	WIFIMAX	138	161	17,97%
9	42673	SKYWARE	137	263	0,96%
10	200125	INTERTOR	130	159	4,23%

Tab. 25. 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 2021 r. otrzymaliśmy 3 296 647 zgłoszeń o 358 400 adresach IP, pod którymi dostępne były urządzenia podatne na ten atak. Jest to spadek o około 30 proc. w porównaniu z 2020 r. Dzienna, średnia liczba adresów IP wyniosła 9109 co stanowi spadek o około 23 proc. Patrząc na wykres ogólny, widzimy niewielką tendencję spadkową w skali roku, co jest także widoczne w przypadku wszystkich systemów autonomicznych znajdujących się w tabeli 26.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	21021	Multimedia	4 417	6 101	0,72%
2	35191	ASTA-NET	468	676	0,80%
3	35378	SATFILM	411	577	1,38%
4	12741	Netia	349	507	0,02%
5	5617	Orange	293	539	0,01%
6	44061	SMSNET	239	350	1,11%
7	43118	EAW	203	275	0,27%
8	29314	Vectra	199	4 454	0,04%
9	30975	TKK	174	243	0,71%
10	6830	UPC	174	289	0,01%

Tab. 26. Dzienna liczba adresów urządzeń podatnych na atak BadWPAD, w podziale na systemy autonomiczne.

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