RAPORT ROCZNY Z DZIAŁALNOŚCI CERT POLSKA 2022

Krajobraz bezpieczeństwa polskiego internetu

CERT.PL
NASK

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 2022

Krajobraz bezpieczeństwa polskiego internetu

CERT.PL
NASK

SPIS TREŚCI

WSTĘP

Znane techniki, nowe okoliczności, wzrost świadomości dotyczącej cyberzagrożeń. Tymi hasłami można podsumować to, co w polskiej cyberprzestrzeni wydarzyło się w roku 2022.

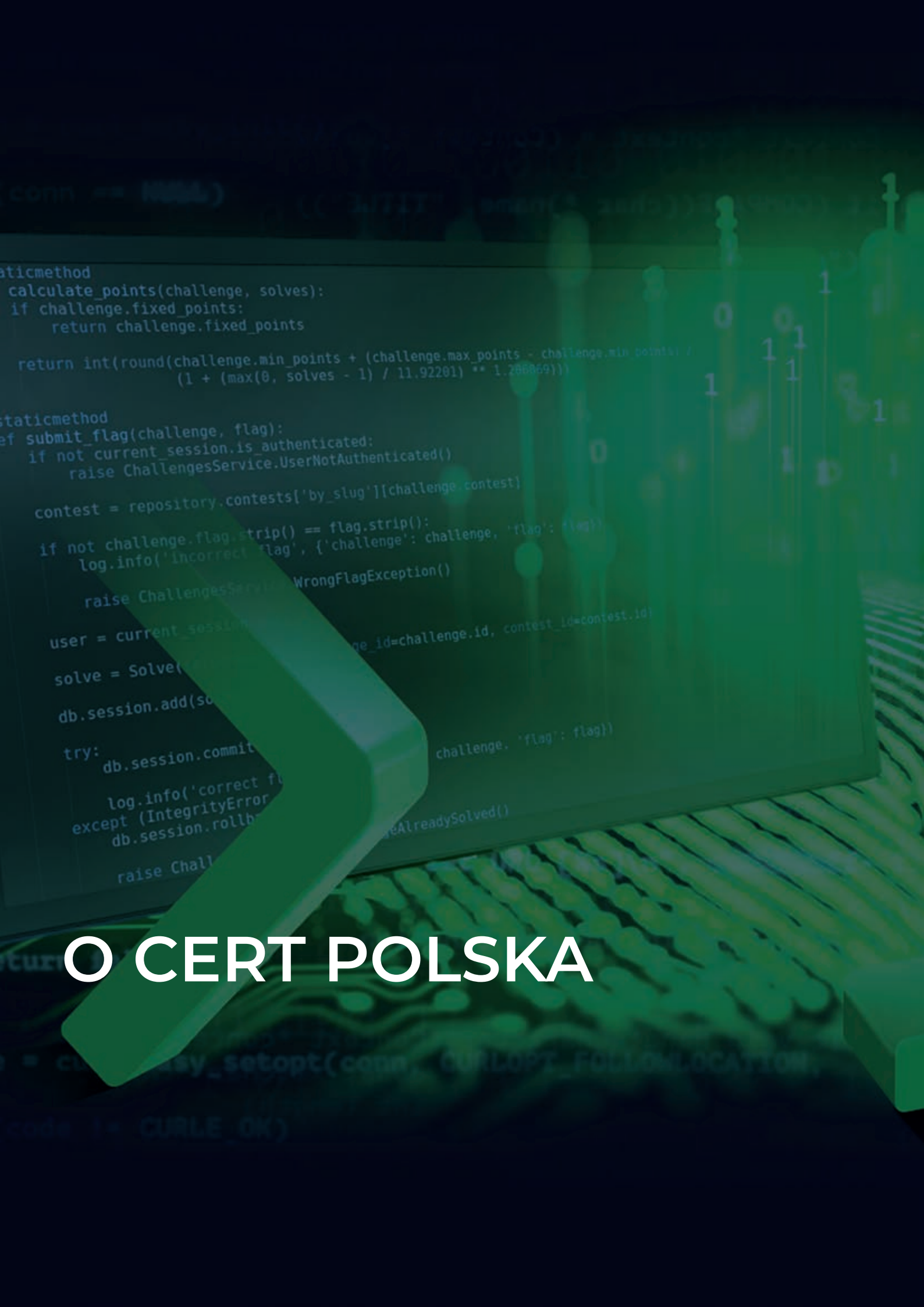
Wciąż obserwowaliśmy masowe kampanie phishingowe, ale także spoofing numeru telefonu czy przypadki kradzieży tożsamości. Te oparte na sztuczkach socjotechnicznych mechanizmy niezmiennie należały do najpowszechniej wykorzystywanych przez cyberprzestępców. Jednocześnie – dzięki licznym kampaniom edukacyjnym i ostrzeżeniom publikowanym w social mediach - rosła wiedza o zagrożeniach. Przełożyło się to na rekordową liczbę zgłoszeń. W całym 2022 r. otrzymaliśmy ich ponad 322 tysiące, co przełożyło się na ponad 39 tysięcy obsłużonych incydentów. 25 625 incydentów zaklasyfikowaliśmy jako phishing.

Oprócz przybliżenia najpopularniejszych kampanii cyberprzestępców 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. Swoje miejsce w raporcie mają także ataki typu ransomware oraz działania wykorzystujące motyw “fałszywych inwestycji”. Wspierane reklamami w wyszukiwarkach oraz mediach społecznościowych, bardzo dobrze przygotowane strony zachęcały do rzekomo bezpiecznego wykorzystania oszczędności. Pewnym novum były fałszywe inwestycje z wojennym motywem w tle.

Nie jest to jedyny przykład, który pokazuje, że sytuacja za naszą wschodnią granicą wpływała na krajowe cyberbezpieczeństwo. Zdarzenia, które bezpośrednio łączymy z wojną w Ukrainie, to też np. zmasowane ataki typu DDoS na portale istotnych krajowych podmiotów gospodarczych czy pojawienie się fałszywych sklepów z opałem. Tym działaniom zdecydowaliśmy się poświęcić w raporcie cały rozdział.

Nie da się ukryć, że sytuacja międzynarodowa wpływa na cyberprzestrzeń. Oprócz zagrożeń inicjuje jednak też szanse. Taką szansą jest współpraca, zwłaszcza na poziomie operacyjnym. Wierzymy, że kolejny rok przyniesie jej pogłębienie i wymierne efekty w postaci ograniczenia niekorzystnych zjawisk w Internecie. Tymczasem jednak zapraszamy do zapoznania się z naszą analizą.

Owocnej lektury!



O CERT POLSKA

Dbamy o bezpieczeństwo polskiego Internetu. To hasło, które najdokładniej oddaje sens i cel naszej pracy.

CERT Polska to historycznie pierwszy w Polsce zespół reagowania na incydenty. Dzięki skutecznej działalności od 1996 r. staliśmy się wiarygodnym i rozpoznawalnym partnerem w środowisku eksperckim i sektorze publicznym. Dziś rzetelną obsługą zgłoszeń oraz działalnością edukacyjną podobną pozycję budujemy wśród obywateli.

Zespół CERT Polska działa w strukturach NASK – Państwowego Instytutu Badawczego i realizuje część zadań zespołu CSIRT NASK zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa. Jesteśmy zespołem odpowiedzialnym za obsługę incydentów bezpieczeństwa i współpracę z podobnymi jednostkami na całym świecie, zarówno w działalności operacyjnej, jak i badawczo-wdrożeniowej.

Jako CSIRT NASK, zgodnie z art. 26 przywołanej ustawy, odpowiadamy m.in. za:

- monitorowanie zagrożeń i incydentów na poziomie krajowym,
- reagowanie na zgłoszone incydenty,
- koordynację obsługi incydentów,
- prowadzenie zaawansowanych analiz złośliwego oprogramowania oraz analizy podatności,
- rozwijanie narzędzi i metod do wykrywania i zwalczania zagrożeń cyberbezpieczeństwa,
- prowadzenie działań z zakresu budowania świadomości w obszarze cyberbezpieczeństwa.

Zajmujemy się także koordynacją 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 powyżej oraz ust. 5 i 7 ustawy o KSC,
- osoby fizyczne.

Ważnym aspektem naszej pracy jest też budowanie świadomości w obszarze cyberbezpieczeństwa oraz proaktywne poszukiwanie rozwiązań na wyzwania, które stoją przed instytucjami, o których mowa wyżej. Do każdego zgłoszenia podchodzimy indywidualnie. Oferujemy wsparcie i pomoc merytoryczną. Obserwujemy trendy w cyberprzestrzeni i prowadzimy statystyki. Skutecznie ostrzegamy i informujemy. Więcej o naszej codziennej pracy przeczytacie w Raporcie. Zapraszamy do lektury!

KALENDARIUM

STYCZEŃ

10.01 Baza wiedzy o hasłach
https://cert.pl/hasla/

28.01 Jak można było pozyskać dane na temat (nie)zaszczepionych Polaków?
https://niebezpiecznik.pl/post/jak-mozna-bylo-pozyskac-dane-na-temat-nie-zaszczepionych-polakow/

LUTY

20.02 Atak na Lotnicze Pogotwie Ratunkowe. Włamywacze zażądali 1,5 miliona złotych
https://niebezpiecznik.pl/post/atak-na-lotnicze-pogotwie-ratunkowe/

24.02 Rekomendacje w związku ze zwiększonym zagrożeniem w cyberprzestrzeni wywołanym sytuacją na Ukrainie
https://cert.pl/posts/2022/02/rekomendacje-cyberprzestrzen-ukraina/

MARZEC

03.03 Portal Money.pl zhackowany. Włamywacz życzył porażki Ukrainie
https://niebezpiecznik.pl/post/portal-money-pl-zhackowany-przez-sily-prorosyjskie/

17.03 Błąd w przetwarzaniu czasu sparaliżował dziś PKP. I koleje w innych krajach też
https://niebezpiecznik.pl/post/cyberatak-na-pkp-ktorego-nie-bylo/

31.03 Uwaga, krytyczna podatność w Spring Core. Spring4Shell. Można przejmować (bez uwierzytelnienia) aplikacje / systemy (RCE).
https://sekurak.pl/uwaga-krytyczna-podatnosc-w-spring-core-spring4shell-mozna-przejmowac-bez-uwierzytelnienia-aplikacje-systemy-rce/

KWIECIEŃ

01.04 Ataki z wykorzystaniem techniki Browser In The Browser

https://cert.pl/posts/2022/04/ataki-browser-in-the-browser/

04.04 Numery ksiąg wieczystych znów były widoczne w Geoportalu, ale to był błąd

https://niebezpiecznik.pl/post/numery-ksiag-wieczystych-znow-byly-widoczne-w-geoportalu-ale-to-byl-blad/

MAJ

07.05 Dziura w rządowym serwisie. Można było pobrać "dane niejawne" przedsiębiorców jednoosobowych

https://niebezpiecznik.pl/post/dziura-w-rzadowym-serwisie-mozna-bylo-pobrac-dane-niejawne-przedsiebiorcow-jednoosobowych/

31.05 Twitter ukarany. Zapłaci 150 milionów dolarów bo wykorzystał numery telefonów użytkowników do reklam

https://niebezpiecznik.pl/post/twitter-ukarany-zaplaci-150-milionow-dolarow-bo-wykorzystal-numery-telefonow-uzytkownikow-do-reklam/

CZERWIEC

18.06 Krytyczna podatność w Zimbra – w łatwy sposób można wykradać hasła do e-maili użytkowników

https://sekurak.pl/krytyczna-podatnosc-w-zimbra-w-latwy-sposob-mozna-wykradac-hasla-do-e-maili-uzytkownikow/

https://www.sonarsource.com/blog/zimbra-mail-stealing-clear-text-credentials-via-memcache-injection/

LIPIEC

19.07 Rozwój technik ataku grupy UNC1151/Ghostwriter

https://cert.pl/posts/2022/07/techniki-unc1151/

19.07

UOKiK idzie na wojnę z bankami. Bo ignorują klientów okradzionych przez Internet

https://niebezpiecznik.pl/post/uokik-idzie-na-wojne-z-bankami-bo-ignoruja-klientow-okradzionych-przez-internet/

SIERPIEŃ

10.08

Mass Exploitation of (Un)authenticated Zimbra RCE: CVE-2022-27925

https://www.volexity.com/blog/2022/08/10/mass-exploitation-of-unauthenticated-zimbra-rce-cve-2022-27925/

20.08

Bitomaty zhackowane przez trywialne błędy komunikacji

https://zaufanatrzeciastrona.pl/post/bitomaty-zhakowane-przez-trywialne-bledy-konfiguracji/

WRZESIEŃ

20.09

Rządowy serwis eFaktura.gov[.]pl zhackowany.

https://niebezpiecznik.pl/post/rzadowy-serwis-efaktura-gov-pl-zhackowany/

23.09

Wyciekły dane osobowe studentów SGH. Przez miesiąc pokazywała je wyszukiwarka Bing

https://niebezpiecznik.pl/post/wyciekly-dane-osobowe-studentow-sgh/

29.09

Wyciekły dane studentów z Uniwersytetu Medycznego w Łodzi. Już wiadomo kogo i jakie!

https://niebezpiecznik.pl/post/wyciekly-dane-studentow-z-uniwersytetu-medycznego-w-lodzi/

29.09

New Microsoft Exchange zero-days actively exploited in attacks

https://www.bleepingcomputer.com/news/security/new-microsoft-exchange-zero-days-actively-exploited-in-attacks/

PAŹDZIERNIK

14.10 New “Prestige” ransomware impacts organizations in Ukraine and Poland

https://assets.sophos.com/X24WTUEQ/at/b5n9ntjqmbkb8fg5rn25g4fc/sophos-2023-threat-report.pdf

26.10 Hubert zarejestrował domenę z “gmail” w nazwie, CERT Polska to zauważył i teraz Hubert ma zablokowane konto i wkurzonych klientów

https://niebezpiecznik.pl/post/hubert-zarejestrowal-domene-z-gmail-w-nazwie-cert-polska-to-zauwazyl-i-teraz-hubert-ma-zablokowane-konto-i-wkurzonych-klientow/

LISTOPAD

02.11 Cyberatak (możliwy ransomware) w Instytucie Centrum Zdrowia Matki Polki w Łodzi.

https://sekurak.pl/cyberatak-mozliwy-ransomware-w-instytucie-centrum-zdrowia-matki-polki-w-lodzi/

09.11 Kanał TVP Sport na Youtube shackowany

https://niebezpiecznik.pl/post/kanal-sportowy-tvp-zhackowany/

GRUDZIEŃ

13.12 Krytyczna podatność w Fortinet FortiOS SSL-VPN (CVE-2022-42475)

https://cert.pl/posts/2022/12/krytyczna-podatnosc-fortios/

22.12 Lastpass: atakujący uzyskali dostęp do zaszyfrowanych baz haseł użytkowników. Nie ma totalnej paniki, ale też nie jest dobrze (zostaje jeszcze ostatnia bariera do przełamania)

https://sekurak.pl/lastpass-atakujacy-uzyskali-dostep-do-zaszyfrowanych-baz-hasel-uzytkownikow-nie-ma-totalnej-paniki-ale-tez-nie-jest-dobrze-zostaje-jeszcze-ostatnia-bariera-do-przelamania/

https://cert.pl/posts/2022/12/lastpass-wyciek-bazy-danych/

DZIAŁANIA CERT POLSKA

LISTA OSTRZEŻEŃ

Zespół CERT Polska kontynuuje projekt Listy Ostrzeżeń, dzięki której możemy chronić polskich internautów przed zagrożeniami czyhającymi na nich każdego dnia. Za jej pomocą operatorzy telekomunikacyjni (oraz inne podmioty, które wdrożyły Listę) mogą uniemożliwiać dostęp do domen na niej zawartych, w rezultacie podnosząc bezpieczeństwo swoich użytkowników.

W roku 2022 Lista Ostrzeżeń CERT Polska obchodziła swoją drugą rocznicę powstania. Od początku do końca roku 2022 zostało umieszczone na niej 43283 domen, dzięki czemu powstrzymano prawie 21 milionów prób rozwiązań nazw mnemonicznych szkodliwych stron. Porównując te statystyki z rokiem 2021 były to wzrosty o odpowiednio: 28% oraz 34%. W naszej ocenie podane statystyki potwierdzają potrzebę istnienia oraz rozwoju Listy. Cieszącą nas informacją jest rosnąca liczba podmiotów i produktów korzystających z listy. Co za tym idzie, rośnie również liczba zapytań o zawartość Listy wysłanych do naszego serwera - porównując lata 2021 i 2022 przyrost wyniósł ponad 142%.

W podsumowaniu 2022 roku warto również wspomnieć o liczbie ponad 220 tysięcy zgłoszeń (dokonanych za pomocą opcji "zgłoszenie złośliwej domeny" na naszej stronie oraz systemów automatycznych, w tym zgłoszeń SMS) zawierających podejrzane domeny. To właśnie m. in. dzięki nim jesteśmy w stanie dokładniej monitorować pojawiające się zagrożenia.

Najczęściej obserwowaną kampanią, której domeny nasz zespół umieszczał na Liście Ostrzeżeń była fałszywa strona Facebook'a, z "sensacyjną" wiadomością, do której można uzyskać dostęp po zalogowaniu – w ten sposób atakujący wyłudzali od ofiar dane dostępowe do konta. Na temat tej kampanii można przeczytać więcej na naszej stronie[1].

Lista Ostrzeżeń prowadzona przez nasz zespół została również uwzględniona w projekcie ustawy o zwalczaniu nadużyć w komunikacji elektronicznej. Pozwoli to na objęcie ochroną jeszcze większej liczby użytkowników polskiego Internetu. Ponadto nawiązaliśmy współpracę z resolverem Quad9[2], dzięki czemu domeny na liście są również blokowane dla użytkowników tej usługi.

Niezmiennie zachęcamy do zgłaszania zaobserwowanych zagrożeń na stronie https://incydent.cert.pl/ oraz przekazywania podejrzanych wiadomości SMS pod numer +48 799 448 084, dzięki czemu nasz zespół może reagować jeszcze sprawniej na zaistniałe incydenty. W tym miejscu składamy również serdeczne podziękowania wszystkim, którzy w swoich zgłoszeniach dostarczają niezwykle cenne informacje, przyczyniając się do wzrostu bezpieczeństwa użytkowników polskiej (i nie tylko) części Internetu.

1 https://cert.pl/posts/2022/04/facebook-weryfikacja/
2 https://quad9.net/, adres resolvera: 9.9.9.9

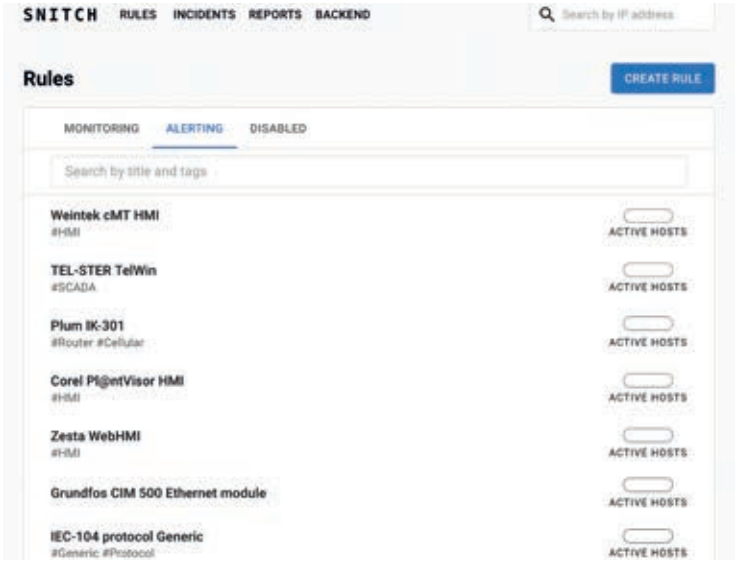
#BEZPIECZNYPRZEMYSŁ

Rok 2022 był kolejnym w którym kontynuowaliśmy akcję #BezpiecznyPrzemysł. W ramach projektu aktywnie działamy na rzecz podniesienia poziomu cyberbezpieczeństwa polskiej infrastruktury przemysłowej. Obszar naszych działań stale rośnie, ale nadal skupiamy się w dużej mierze na urządzeniach dostępnych z publicznego Internetu, takich jak sterowniki PLC czy panele operatorskie (HMI). W tym roku stworzyliśmy system, który automatyzuje naszą pracę, nazwaliśmy go Snitch.

SNITCH

Snitch to system monitorowania i raportowania o urządzeniach podłączonych do Internetu. Do modułu monitorowania są wykorzystywane wyszukiwarki umożliwiające przeszukiwanie banerów usług, takie jak Shodan[3], ZoomEye[4], czy Censys[5].

Snitch umożliwia tworzenie reguł w ramach których definiowane są frazy wyszukiwania tzw. dorki. Dorki są definiowane na podstawie bazy wiedzy tworzonej wewnętrznie przez CERT Polska. Skupiamy się na tym, aby pokrywały one jak najwięcej urządzeń powszechnie wykorzystywanych w zakładach przemysłowych Polsce. Przykładowa lista systemów, które monitoruje snitch została pokazana na rysunku 1.



Rys. 1 Zrzut ekranu panelu z listą reguł systemu Snitch

3 https://www.shodan.io/
4 https://www.zoomeye.org/
5 https://search.censys.io/

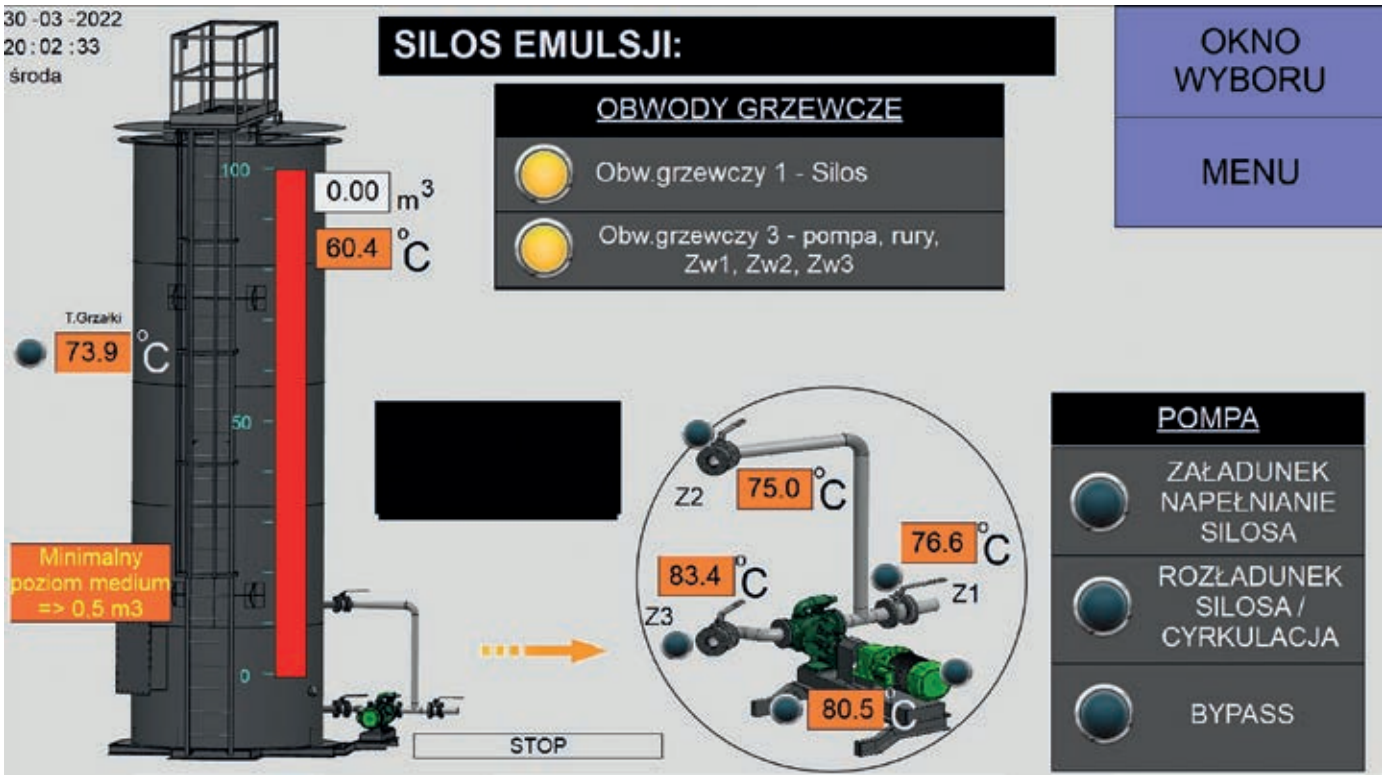
Snitch następnie cyklicznie odpytuje wyszukiwarki i zapisuje wykryte adresy IP. Kolejny moduł generuje raporty w formie wiadomości e-mail na podstawie wcześniej zdefiniowanego szablonu, wyszukuje adres kontaktowy (ang. abuse) dla danego adresu IP i wysyła wiadomość.

Drugim kanałem kontaktowym który będzie wykorzystywać Snitch to system n6. Z powodu trudności z dotarciem do faktycznego właściciela systemu, dodatkowy kanał zwiększy tę szansę.

Warto podkreślić, że skanowania odbywają się cyklicznie, co pozwala monitorować stan odłączania niepożądanych urządzeń od Internetu i eskalować do analizy ręcznej w przypadku braku działań ze strony adresata.

CIEKAWE ZNALEZISKA

W ciągu tego roku podjęliśmy działania względem licznych przypadków, w których można było zdalnie przejąć całkowitą kontrolę na procesem przemysłowym. Za każdym razem kontaktowaliśmy się i współpracowaliśmy z właścicielami celem rozwiązania problemu. Ciekawym przykładem może być znaleziony przez nas panel HMI pozwalający na zarządzanie silosem magazynującym emulsję asfaltową (rys 2).



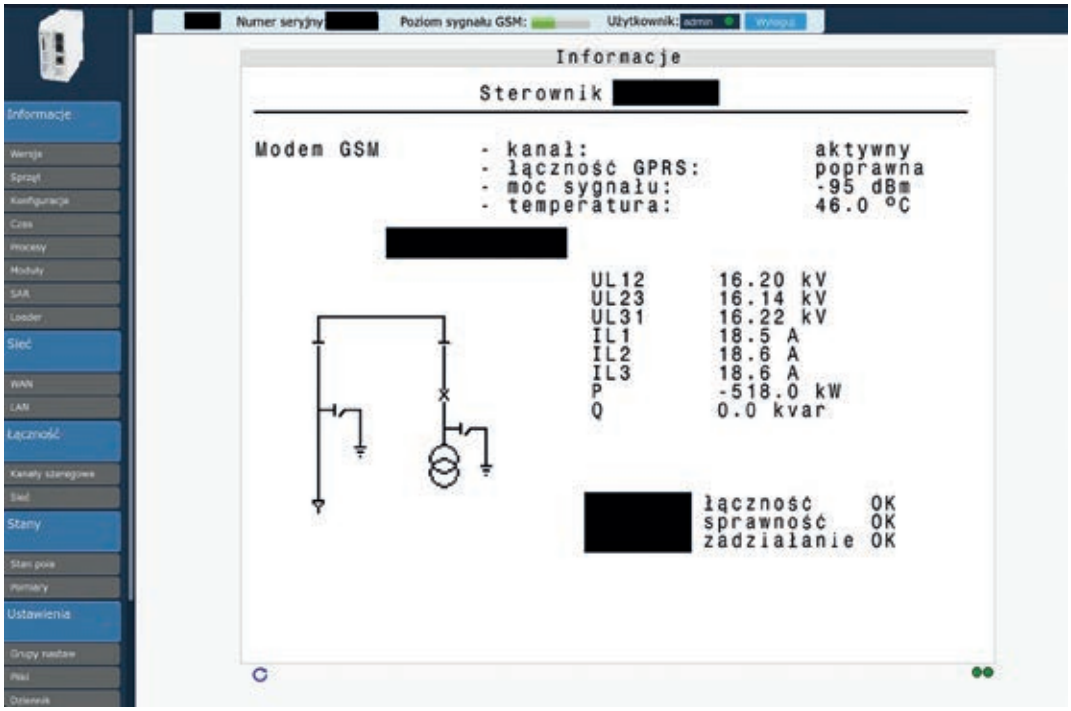
Rys. 2 panel HMI pozwalający na zarządzanie silosem magazynującym emulsję asfaltową

Trendem, który obserwujemy jest znaczny wzrost liczby instalacji OZE (Odnawialne Źródła Energii) podłączanych bezpośrednio do Internetu. Dotyczy to również dużych instalacji. Przykładowo udało nam się znaleźć sterownik oraz kamerę, dostępne zdalnie bez uwierzytelniania, na stacji elektroenergetycznej WN 110/20 kV odpowiedzialnej za przesył prądu z farmy wiatrowej 14MW (rys 3). W innym przypadku natrafiliśmy na podstację energetyczną należącą do farmy fotowoltaicznej (Rys. 4).

```
FWS/> db

Master devices: (9)
  dnpx(1001)  Alive                hmi(1004)   Dead
  dnpx(1002)  Alive                hmi(1005)   Dead
  dnpx(1003)  Dead                 hmi(1006)   Alive
  gps(90)     Alive                hmi(1009)   Dead
  hmi(1000)   Dead
Slave devices: (35)
  dnp(501)    Alive                mbus(305)   Alive
  iec(231)    Alive                mbus(306)   Alive
  iec(232)    Alive                mbus(11015) Alive
  iec(401)    Alive                mbus(11016) Alive
  iec(2001)   Alive                bi(11)      Alive
  iec(2002)   Alive                bo(12)      Alive
  iec(2003)   Alive                vd(100)     Alive
  iec(2004)   Alive                vd(101)     Alive
  iec(2005)   Alive                vd(102)     Alive
  iec(2006)   Alive                vd(103)     Alive
  iec(11011)  Alive                vd(104)     Alive
  iec(11012)  Alive                sqc(10)     Alive
  iec(11013)  Alive                sqc(11)     Alive
  iec(11014)  Alive                sqe(10)     Alive
  mbus(301)   Alive                sqe(11)     Alive
  mbus(302)   Alive                ctmr(0)     Alive
  mbus(303)   Alive                sys(1)      Alive
  mbus(304)   Alive
```

Rys. 3 sterownik stacji elektroenergetycznej odpowiedzialnej za przesył prądu z farmy wiatrowej



Rys. 4 sterownik stacji elektroenergetycznej odpowiedzialnej za przesył prądu z farmy fotowoltaicznej

Kolejnym obszarem naszej działalności jest poszukiwanie nieznanych wcześniej podatności ze szczególnym uwzględnieniem sprzętu używanego w Polsce. W tym roku udało się znaleźć podatność klasy Directory Traversal w web serwerze Payara, która dotyczyła również jego wersji dla urządzeń wbudowanych (Payara Embedded) – CVE-2022-37422[6]. Znaleźliśmy również podatność pozwalającą na zdalny odczyt plików systemowych bez uwierzytelniania w popularnym systemie SCADA polskiego producenta. Niestety w momencie pisania tego raportu, podatność nadal nie posiada łatki.

6 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37422

ĆWICZENIA I KONKURSY

Zespół CERT Polska regularnie uczestniczy w krajowych i międzynarodowych ćwiczeniach sprawdzających zarówno umiejętności technicznej analizy zagrożeń jak i testujących procedury reagowania na incydenty. Najważniejszymi z nich są coroczne ćwiczenia defensywne Locked Shields, organizowane raz na dwa lata Cyber Europe oraz europejskie zawody European Cyber Security Challenge dla młodzieży.

CYBER EUROPE

“Cyber Europe” to cykliczne ćwiczenia organizowane przez Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA). Polegają na symulacji ogólnoeuropejskiej sytuacji kryzysowej, podczas której sztaby krajowe mogą przetestować wypracowane procedury operacyjne i scenariusze przygotowane na wypadek wystąpienia dużych incydentów.

Celem ćwiczeń „Cyber Europe” jest testowanie procedur zarządzania kryzysowego w obliczu międzynarodowego kryzysu w cyberprzestrzeni (w sieciach i systemach komputerowych) – zarówno tych wewnętrznych (w poszczególnych organizacjach na poziomie państw członkowskich i w poszczególnych sektorach), jak również procedur na poziomie europejskim (tzw. SOP – Standard Operating Procedures).

W dziedzinie cyberbezpieczeństwa jest to szczególnie istotne, ponieważ kryzysy w cyberprzestrzeni mają potencjał przerodzenia się w realne zagrożenia fizyczne (np. brak prądu, problemy z łącznością). W takiej sytuacji konieczna jest sprawna współpraca zespołów reagowania na incydenty bezpieczeństwa komputerowego (CERT lub CSIRT) z zespołami i centrami zarządzania kryzysowego oraz zespołami medialnymi, a także z administracją publiczną i sektorem prywatnym (każda edycja dotyczy innego sektora gospodarki).

Pierwsza edycja ćwiczeń “Cyber Europe” odbyła się w 2010 r. Dwa lata później ćwiczenia dotyczyły sektora bankowego, w 2014 r. – sektora energetycznego i telekomunikacyjnego. Natomiast w 2016 roku w ćwiczeniu wzięli udział dostawcy Internetu i firmy z sektora bezpieczeństwa IT. Piąta edycja z czerwca 2018 r., dotyczyła sektora lotnictwa cywilnego. Tegoroczne Cyber Europe 2022 skupiło się na kryzysie w sektorze ochrony zdrowia.

Procedury wypracowane przez państwa członkowskie i ENISA w poprzednich edycjach stały się podstawą zaleceń Komisji Europejskiej w sprawie skoordynowanego reagowania na incydenty i kryzysy na dużą skalę. Zalecenia zawierają ramowe procedury i organizację współpracy europejskiej na poziomie strategicznym, a także operacyjnym.

Skalę ćwiczenia najlepiej opisują liczby. W szóstej edycji uczestniczyło 29 państw z Unii Europejskiej i Europejskiego Stowarzyszenia Wolnego Handlu oraz agencje unijne zajmujące się cyberbezpieczeństwem i działające w sektorze ochrony zdrowia, takie jak Komisja Europejska, CERT-EU, Europol, EMA, ENISA. Łącznie ćwiczyło 302 organizacji (164 z sektora publicznego) i 918 zespołów lub specjalistów cyberbezpieczeństwa, zarządzania kryzysowego i komunikacji.

Przedstawicielami Polski byli: NASK – Państwowy Instytut Badawczy z działającym w nim CSIRT NASK, w którym zespół CERT Polska wykonuje zadania techniczne, CSIRT GOV, administracja publiczna reprezentowana przez Rządowe Centrum Bezpieczeństwa, Kancelaria Prezesa Rady Ministrów, Ministerstwo Zdrowia, Centrum e-Zdrowia oraz dostawca sieci telekomunikacyjnej i podmioty szpitalne i laboratoryjne z sektora ochrony zdrowia. Łącznie 15 zespołów z 11 organizacji.

Podczas dwudniowego ćwiczenia polscy uczestnicy wymienili setki wiadomości mailowych. Podmioty działające w ramach Krajowego Systemu Cyberbezpieczeństwa dodatkowo wykorzystywały istniejące już kanały komunikacji adekwatnie do rozwijającego się przebiegu zdarzeń. W ten sposób przetestowano pozytywnie wypracowaną infrastrukturę. Podmioty z sektora ochrony zdrowia miały okazję zapoznać się z formularzem przeznaczonym do zgłaszania incydentów bezpieczeństwa komputerowego oraz procesem obsługi takiego zdarzenia.

W scenariuszu ćwiczenia znalazły się incydenty bezpieczeństwa w sieciach i systemach informatycznych związane z przełamaniem zabezpieczeń, utratą danych, czy nieautoryzowanym dostępem do danych oraz złamaniem RODO. Ponadto pojawiły się zdarzenia bezpośrednio wpływające na życie człowieka, takie jak atak na wszczepialne kardiowertery stymulujące pracę serca pacjenta oraz incydenty medialne związane z walką z dezinformacją, czy zarządzanie komunikacją kryzysową. Scenariusz także zawierał potencjalne zagrożenia dla pozostałych sektorów gospodarki, które mogły się rozprzestrzenić w związku z nieodpowiednią obsługą incydentu.

Całe ćwiczenie zostało przeprowadzone w specjalnie stworzonym do tego celu środowisku imitującym świat rzeczywisty. Stworzono kopie najczęściej wykorzystywanych źródeł pozyskiwania informacji o zdarzeniach: portali informacyjnych, platform społecznościowych, stron służących do dzielenia się fragmentami kodu i wiele innych. Całość była zarządzana wiadomościami mailowymi wysyłanymi przez komitet organizacyjny ulokowany w Agencji Unii Europejskiej ds. Cyberbezpieczeństwa. Organizatorzy byli wspierani przez lokalnych moderatorów czuwających nad płynnością ćwiczenia na poziomie krajowym.

Zdarzenia techniczne, sprawdzające doświadczenie wyspecjalizowanych zespołów reagowania na incydenty bezpieczeństwa komputerowego w przeprowadzaniu m.in. analiz powłamaniowych, zautomatyzowanych analiz informacji z otwartych źródeł, analiz próbek złośliwego oprogramowania, były kluczowym aspektem ćwiczenia. Zadania techniczne składały się na incydenty, a usuwanie ich skutków wpływało na skuteczność odpowiedzi na kryzys.

Wnioski i rekomendacje z ćwiczenia zostały opracowane na przełomie listopada i grudnia 2022 roku. Uzgodniona na poziomie europejskim treść raportu została przekazana koordynatorom krajowym i uczestnikom ćwiczenia. Publicznie dostępna część raportu z organizacji i przebiegu ćwiczenia, jest dostępna na stronie ENISA[7]. Na stronie dostępne są także raporty z poprzednich edycji Cyber Europe. Należy przy tym zaznaczyć, że większość obserwacji i wniosków nie jest publikowana. Stanowią one informację prawnie chronioną – informacje niejawne administracji publicznej oraz tajemnice handlowe przedsiębiorstw biorących udział w ćwiczeniu. Ćwiczenia dały możliwość przetrenowania działania punktów kontaktowych do spraw cyberbezpieczeństwa i ich współdziałania z centrami zarządzania kryzysowego. W zakresie procedur na poziomie krajowym, przetestowane zostało współdziałanie NASK i RCB w inicjowaniu Zespołu ds. incydentów krytycznych i jego relacji do Rządowego Zespołu Zarządzania Kryzysowego. Działanie to było jednym z celów krajowych ćwiczeń i pozwoliło na sprawdzenie jednego z zakładanych wariantów reagowania na incydenty i ich eskalowania z poziomu organizacji na poziom krajowy. Doświadczenia zostaną wykorzystane przy tworzeniu kolejnych aktualizacji planów zarządzania kryzysowego. Sprawdzono współdziałanie, na poziomie technicznym i proceduralnym, podmiotów cyberbezpieczeństwa oraz działających w sektorze ochrony zdrowia. Zweryfikowano czy współpraca jest wystarczająco dojrzała, aby pozwoliła na odparcie złożonego zagrożenia – przebiegającego w cyberprzestrzeni, ale mającego realny, fizyczny skutek dla podmiotów ochrony zdrowia. Zauważono braki i mankamenty, szczególnie w komunikacji i bieżącej wymianie informacji. Braki dotyczyły głównie zbyt wolnego przepływu informacji związanego z chęcią samodzielnego rozwiązania zadań po stronie atakowanego podmiotu.

7 https://www.enisa.europa.eu/publications/cyber-europe-2022-after-action-report

LOCKED SHIELDS

Locked Shields to największe i najbardziej zaawansowane ćwiczenia obrony bezpieczeństwa komputerowego na świecie. Organizowane są przez Centrum Doskonalenia Cyberobrony NATO (CCDCOE) z siedzibą w Estonii każdej wiosny już od 12 lat (z przerwą w 2020 r.). W ćwiczeniach uczestniczą kraje finansujące działanie Centrum, instytucje NATO i Unii Europejskiej oraz wybrane podmioty komercyjne i instytucje naukowe. W scenariuszu ćwiczenia każda z reprezentacji ćwiczących krajów pełni rolę zespołu "niebieskiego", czyli reagowania na incydenty bezpieczeństwa teleinformatycznego. Na prośbę fikcyjnego, sojuszniczego kraju Berylia każdy z zespołów "niebieskich" przez dwa dni ochrania symulowaną część jego infrastruktury informatycznej przed wrogimi działaniami zespołu "czerwonych". Do zadań zespołów "niebieskich" należą nie tylko działania defensywne - zabezpieczanie sieci, wykrywanie i zapobieganie atakom, ale także wymiana informacji w ramach sojuszniczej współpracy międzynarodowej. Wszystko dzieje się pod dużą presją czasu w nieznanym wcześniej środowisku. Działania "czerwonych" mają z kolei symulować zorganizowanego, wrogiego zespołu posługującego się taktyką, technikami i procedurami aktora APT ("advanced persistent threat") sponsorowanego przez obce państwo. W 2022 r. w ćwiczeniach wzięło udział ponad 2000 specjalistów z 32 krajów.

W ramach symulowanej bazy wojskowej każdy z zespołów "niebieskich" miał do obrony ponad 220 wirtualnych systemów informatycznych: od typowych systemów takich jak stacje robocze, serwery, urządzenia sieciowe, chmurę obliczeniową, po wyspecjalizowane takie jak system obrony przeciwlotniczej czy wydzielona sieć 5G oraz systemy infrastruktury przemysłowej produkcji i dystrybucji prądu oraz procesu uzdatniania wody. Nowością w tym roku był symulowany system finansowy państwa z instytucją banku centralnego i izby rozliczeniowej. Na systemy chronione przez 24 zespoły "niebieskich" przeprowadzono ponad 8 tysięcy ataków.

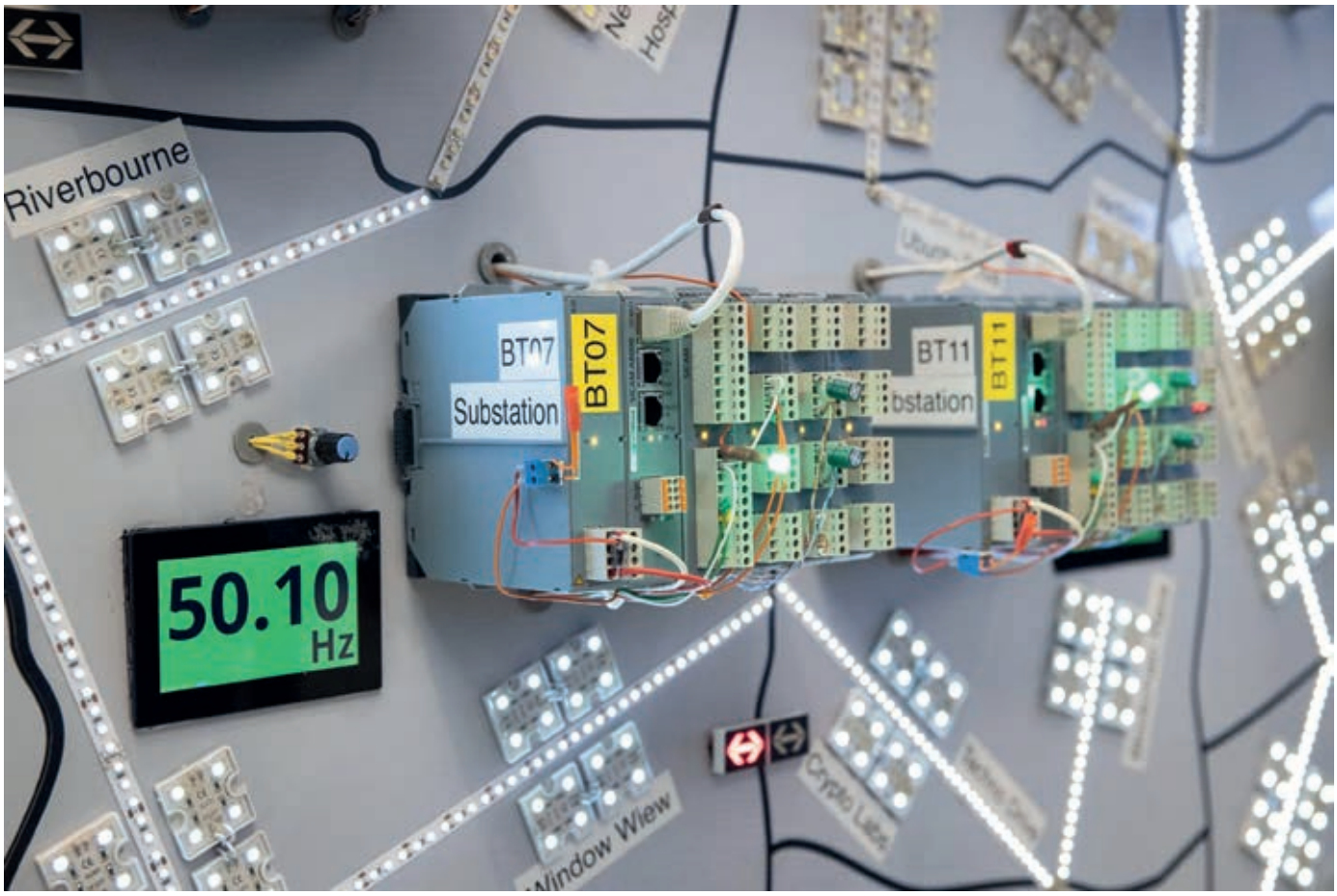
Struktura ćwiczenia wymaga od każdego z zespołów koordynacji w wielu aspektach zarządzania cyberbezpieczeństwem w obliczu konfliktu hybrydowego. Oprócz zabezpieczania systemów oraz odpierania ataków w ramach reagowania na incydenty, od zespołów "niebieskich" oczekuje się także wymiany informacji w ramach 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 w formule 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.

Łączona reprezentacja polsko-litewska, pod przewodnictwem polskiego oficera z Dowództwa Komponentu Wojsk Obrony 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 2022 r. drugie miejsce. Ćwiczenia wygrała reprezentacja Finlandii, a na podium znalazła się również reprezentacja estońsko-gruzińska.

W 2022 r. eksperci CERT Polska oraz NASK kierowali pracami aż czterech zespołów w polskiej reprezentacji:

- systemów specjalnych (w tym infrastruktury przemysłowej oraz sieci 5G),
- aplikacji Internetowych,
- infrastruktury sieciowej,
- prawnego.



Rys. 5. symulowany system dystrybucji prądu w ćwiczeniu Locked Shields, fot. CCDCOE

EUROPEAN CYBER SECURITY CHALLENGE

European Cyber Security Challenge to młodzieżowe mistrzostwa Europy w cyberbezpieczeństwie. Corocznie organizowane wydarzenie zapoczątkowane przez Komisję Europejską w 2013 r. ma na celu popularyzację zagadnień z zakresu cyberbezpieczeństwa oraz zachęcić młodzież do planowania kariery zawodowej w tym obszarze. Od 2016 r. za organizację wydarzenia odpowiedzialna jest ENISA. Polska po raz pierwszy wzięła udział w zawodach z cyklu 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 użycia i 5 osób w wieku od 21 do 25 lat. 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 finałach odpowiada zespół CERT Polska.

W indywidualnym konkursie kwalifikacyjnym w formule Capture The Flag przeprowadzonym w dniach 15-17 lipca na platformie hack.cert.pl wzięły udział 82 osoby, a 59 z nich 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. Pierwsze miejsce w kwalifikacjach zdobył Krzysztof Haładyn, a kapitanem wyłonionej reprezentacji został Grzegorz Uriasz. Każda chętna osoba może zmierzyć się z zadaniami konkursowymi z tych i ubiegłych kwalifikacji na stronie https://hack.cert.pl.

Finały odbyły się w dniach 13-16 września w Wiedniu. W 2022 r. udział wzięła rekordowa liczba reprezentacji narodowych - aż 28. W konkursie finałowym polska reprezentacja zajęła piąte miejsce. Na podium stanęły odpowiednio reprezentacje: Danii, Niemiec i Francji. Finały w 2023 r. odbędą się w Norwegii.

Rys. 6 Polska reprezentacja podczas finałów ECSC w Wiedniu, fot. NASK

SCENA CTF

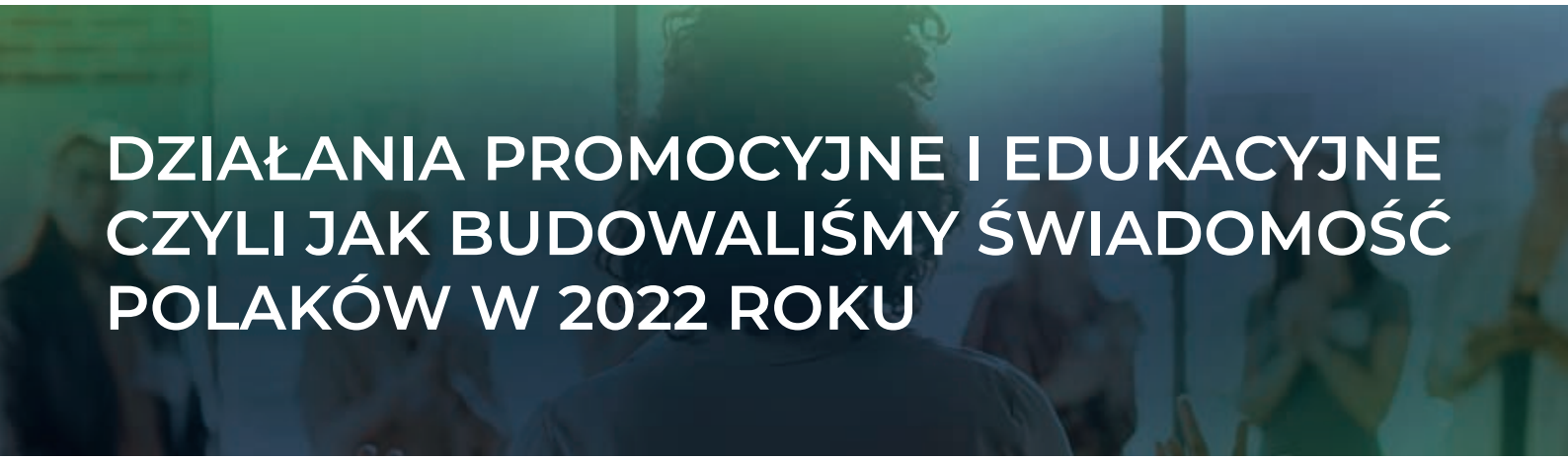
Konkursy Capture The Flag (CTF) są drużynowymi zawodami bezpieczeństwa komputerowego. Organizowane są niezależnie przez instytucje naukowe, rządy państw, organizacje pozarządowe oraz same zespoły CTF. Zawody podzielić można według formy i miejsca rozgrywki. Najpopularniejszą formułą zawodów jest "jeopardy", 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).

Najbardziej prestiżowe konkursy łączą obie formuły – kwalifikacje przeprowadzane przez Internet w formule "jeopardy" oraz finały w formule "attack/defence" organizowane offline. Te ostatnie najczęściej odbywają się przy okazji międzynarodowych konferencji cyberbezpieczeństwa. Panująca pandemia nadal sprawia, że część cyklicznych konferencji odbywa się on-line, co negatywnie wpływa na światową scenę CTF.

Pierwsze miejsce w światowym rankingu CTFTime w 2022 r. zdobył zespół "organizers" powstały z połączenia studenckich drużyn ze Szwajcarii, Niemiec i Wielkiej Brytanii. Drugie miejsce zdobył amerykańsko-koreański zespół "perfect r00t". Trzecie miejsce wywalczył chiński zespół "Never Stop Exploiting". Polskie zespoły "justCatTheFish", "p4" oraz "Dragon Sector" zajęły kolejno 7, 21 oraz 68 miejsca. W 2022 r. odbyły się również kolejne edycje konkursów organizowanych przez "justCatTheFish" oraz "p4". W obu zwyciężył rosyjski zespół "C4T BuT S4D".

W 2022 r. odbyła się również trzecia edycja konkursu bezpieczeństwa informatycznego w branży kosmicznej "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 poprzednich latach odbyły się w formule "jeopardy", wygrał ponownie polski zespół. 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" również zwyciężył poprawiając swój wynik sprzed roku (drugie miejsce). Zgodnie z zasadami konkursu, zwycięstwo w tym roku, oprócz nagrody finansowej w wysokości 60 tysięcy dolarów, zapewniło również polskiej ekipie udział w finałach w 2023 r., które odbędą się podczas konferencji Defcon w Las Vegas.

Rys. 7 Członkowie drużyny “Poland Can Into Space” podczas finałów Hack-a-sat w 2022 r.



DZIAŁANIA PROMOCYJNE I EDUKACYJNE CZYLI JAK BUDOWALIŚMY ŚWIADOMOŚĆ POLAKÓW W 2022 ROKU

Ostatnie miesiące 2022 roku przyniosły duże zmiany w liczbie przyjętych przez CERT Polska zgłoszeń. Jak znaczące były to zmiany? I z czego wynikały?

Do listopada zeszłego roku miesięczna liczba zgłoszeń przetwarzanych przez zespół CERT Polska wahała się od 10 do 36 tysięcy. Koniec roku zmienił tę dynamikę. Listopad to ponad 42 tysiące zgłoszeń, grudzień – już 85 tysięcy! Dało to na koniec roku liczbę 322 479, którą możemy zestawić z rezultatem ubiegłorocznym, który wyniósł „zaledwie" 116 071. Łatwo zatem policzyć, że średnia z roku 2021 to poniżej 10 tysięcy zgłoszeń miesięcznie. Co zatem wydarzyło się w polskiej cyberprzestrzeni w ostatnich miesiącach? I co zmieniło nastawienie Polaków do wysyłania zgłoszeń?

Prawdopodobnie nie ma na to pytanie jednoznacznej odpowiedzi. Faktem jest, że systematycznie zwiększa się aktywność cyberprzestępców. Że ich ataki są coraz śmielsze i coraz częściej mają charakter masowy jak np. opisywane w tym raporcie kampanie phishingowe. Niezaprzeczalnie na polską cyberprzestrzeń wpłynęła też wojna w Ukrainie. Jej skutki także przybliżamy w niniejszej publikacji. Ale tym co zmieniło się najbardziej jest świadomość użytkowników. Polacy coraz umiejętniej rozpoznają zagrożenia i coraz chętniej zgłaszają je do CSIRT NASK.

Rozpoznawalność CERT Polska nie jest tu bez znaczenia. Na rosnącą w oczach Polaków wiarygodność i „popularność" instytucji wpływ mają kampanie edukacyjne i promocyjne realizowane w 2022 roku. Mowa tu zarówno o spotach radiowych i telewizyjnych, jak i działaniach prowadzonych w kanałach social media CERT Polska.

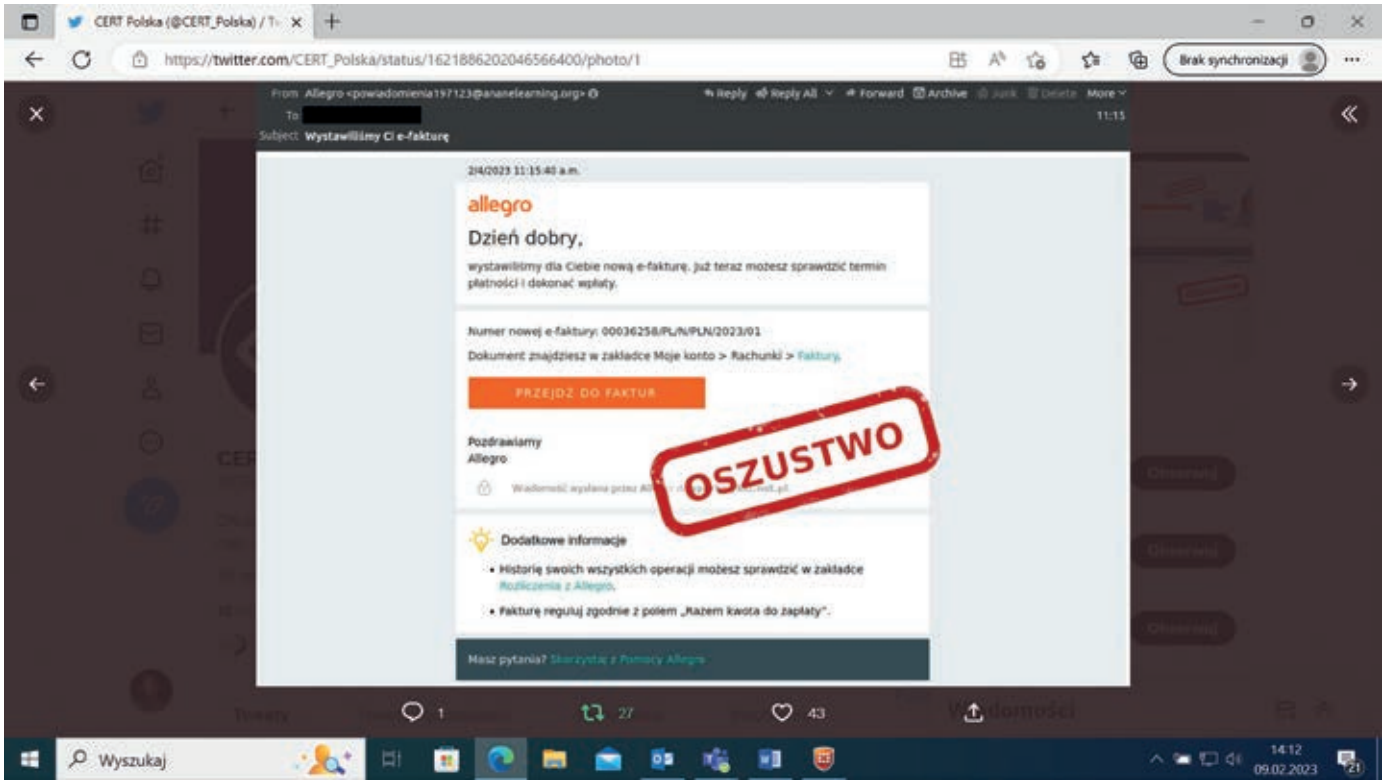
Emisję spotów, w których podkreślaliśmy wartość przesyłania do nas podejrzanych SMS-ów rozpoczęliśmy w połowie listopada. W sumie w telewizji oraz ogólnopolskich i regionalnych rozgłośniach radiowych reklamę wyemitowano ponad 500 razy, co pozwoliło osiągnąć zasięg na poziomie 30 milionów. Emisje miały miejsce także w czasie najwyższej oglądalności np. przed meczami Mistrzostw Świata w piłce nożnej. Ich wpływ był dla nas bardzo widoczny – każdorazowo podnosił liczbę zgłoszeń.

Rys. 8 Fragment spotu emitowanego podczas kampanii telewizyjnej

Działo się tak ponieważ w kampanii, oprócz pokazywania przykładów działania cyberoszustów, informowaliśmy jak i gdzie zgłaszać taką niepokojącą aktywność.

Rys. 9 Fragment spotu informujący o tym, gdzie należy wysyłać zgłoszenia

Oprócz tego prowadziliśmy działania edukacyjne na kanałach social media, które wspieraliśmy obecnością naszych ekspertów w wiodących stacjach radiowych i telewizyjnych. Na szczególną uwagę zasługują systematycznie wydawane ostrzeżenia. Ostrzeżenia dotyczą największych kampanii oszustów i są publikowane równolegle na Facebooku, Twitterze oraz LinkedInie CERT Polska. Regularność publikacji, aktualne kwestie i ważne społecznie zagadnienia powodują, że posty przygotowane przez ekspertów CERT docierają nawet do kilkuset tysięcy odbiorców.



Rys. 10 Przykładowe ostrzeżenie publikowane w social mediach

Oprócz ostrzeżeń, wydawanych ad hoc, w kanałach social media publikowane są także stałe cykle edukacyjne – w październiku i listopadzie był to zestaw grafik „CyberWiesz" dotyczący podstawowych zagadnień z obszaru cyberbezpieczeństwa takich jak: socjotechnika, spoofing czy instalowanie aplikacji z niezaufanych źródeł. W grudniu natomiast przybliżaliśmy pojęcia z zakresu bezpieczeństwa w sieci w formie „CyberKalendarza".

Rys.11 Przykładowa ilustracja, która powstała w ramach cyklu #CyberWiesz

Budowanie profesjonalnego wizerunku uzupełnialiśmy obecnością na kluczowych konferencjach branżowych takich jak np.: Confidence czy Oh my hack, biorąc udział w międzynarodowych konkursach i ćwiczeniach (które także w tym raporcie opisujemy), a także wspierając merytorycznie uczestników hackathonów.

Czy się opłaciło? Tutaj odpowiedź jest już jednoznaczna. Rosnąca rozpoznawalność i zaufanie, przekładają się na liczbę zgłoszeń. Zgłoszenia natomiast to pełniejszy obraz tego, co w polskiej cyberprzestrzeni się dzieje, możliwość skuteczniejszego działania i ostrzegania. A o to przecież zespołowi CERT Polska chodzi najbardziej.

INCYDENTY I ZAGROŻENIA

PODSUMOWANIE ROKU Z PERSPEKTYWY ZGŁASZANYCH INCYDENTÓW

Kolejny rok i kolejny rekordowy wynik zarejestrowanych oraz obsłużonych incydentów cyberbezpieczeństwa przez zespół CERT Polska, który od 2018 r. pełni obowiązki zespołu CSIRT NASK na podstawie Ustawy o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 roku. W 2022 r. odnotowano 322 479 zgłoszeń incydentów cyberbezpieczeństwa. Wśród nich występowały również takie, które nie zostały uznane za incydent. CERT Polska dokonał starannej klasyfikacji, na podstawie której wytypował 115 164 zgłoszeń, z których zarejestrował 39 683 incydentów cyberbezpieczeństwa.

W 2022 r. zespół CERT Polska zaobserwował ponad 34 proc. wzrost zarejestrowanych incydentów cyberbezpieczeństwa w porównaniu do roku poprzedniego. Ilość wszystkich zgłoszeń wzrosła o blisko 178 proc., a tych powiązanych z incydentami o ponad 75 proc. Wzrost zgłoszeń oraz incydentów cyberbezpieczeństwa z całą pewnością wynika z coraz większej świadomości istnienia zespołu CERT Polska. W 2022 r. rozpoczęła się kampania społeczna w telewizji oraz radio informująca o czyhających zagrożeniach i sposobie ich zgłaszenia do zespołu CERT Polska.

Zgłoszenia incydentów przyjmujemy:

Formularzem na stronie: https://incydent.cert.pl/ – Zgłoś incydent,

Formularzem na stronie: https://incydent.cert.pl/domena – Zgłoszenie złośliwej domeny,

SMS: +48 799 448 084,

Telefonicznie: +48 22 380 82 74,

E-mailem: cert@cert.pl,

Listownie na adres NASK PIB.

Najczęściej zgłaszanym typem incydentów zarejestrowanych w 2022 r. były incydenty związane z oszustwami komputerowymi, a szczególnie phishingu. CERT Polska zarejestrował 25 625 incydentów zaklasyfikowanych jako phishing, co stanowi 64 proc. wszystkich obsłużonych incydentów w 2022 r. Imponująca jest również liczba zgłoszeń, aż 82 830 zgłoszenia powiązane są z incydentami phishingu! Najpopularniejszym typem phishingu było wykorzystywanie wizerunku firmy kurierskiej InPost – 5 119 incydentów. Na podium znalazł się również serwis mediów społecznościowych Facebook - 4 370 incydentów oraz serwis ogłoszeniowy Vinted – 2 926 incydentów.

Kolejnym często zgłaszanym w ubiegłym roku rodzajem incydentu, było szkodliwe oprogramowanie. Na podstawie 15 433 zgłoszeń zarejestrowano 3 409 incydentów tego typu, co przekłada się na 8,59 proc. wszystkich incydentów. Wśród zarejestrowanych incydentów, aż 2 607 dotyczyły szkodliwego oprogramowania o nazwie Flubot.

Trzecim typem incydentów, który występował najczęściej w 2022 r., były włamania m.in. do systemów informatycznych oraz kont pocztowych. Tego typu incydentów zarejestrowano 354, co przekłada się na 0,89 proc. wszystkich incydentów. Tak niewielki procent wynika z faktu, iż wiele włamań jest zgłaszanych równocześnie z domeną phishingową. Finalnie takie zgłoszenia często klasyfikowane są jako phishing.

Ciekawostką jest, że incydenty zaklasyfikowane jako obraźliwe i nielegalne treści, w tym spam również nie pozostają daleko w tyle. Pomimo iż zarejestrowano ich „zaledwie" 308 - 0,78 proc. wszystkich incydentów, to dokonano tego na podstawie 5 257 zgłoszeń. Statystycznie przypada aż 17 zgłoszeń na 1 incydent cyberbezpieczeństwa w tej kategorii.

CSIRT NASK w ramach Ustawy o Krajowym Systemie Cyberbezpieczeństwa w 2022 r. obsłużył 30 incydentów, które zaklasyfikowano jako poważne. Incydenty tego typu to takie, których wystąpienie spowodowało lub mogłoby spowodować znaczne obniżenie jakości lub przerwanie ciągłości działania świadczonej usługi kluczowej. Zostało zarejestrowanych 21 incydentów poważnych w sektorze bankowym, 5 w sektorze energii, 3 w sektorze ochrony zdrowia oraz 1 w sektorze transportu.

W 2022 r. CSIRT NASK obsłużył 937 incydentów dotyczących podmiotów publicznych. Najczęściej rejestrowanymi incydentami zaklasyfikowanymi jako incydenty w podmiocie publicznym były incydenty z sektora administracji publicznej - 547 incydentów, sektora oświaty i wychowania - 134 incydentów oraz sektora infrastruktury cyfrowej - 81 incydentów.

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

Sektor gospodarki	Liczba incydentów	%
Energetyka	4 320	10,89%
Transport	111	0,28%
Bankowość	2 944	7,42%
Infrastruktura rynków finansowych	2 813	7,09%
Służba zdrowia	251	0,63%
Wodociągi	9	0,02%
Infrastruktura cyfrowa	1 821	4,59%
Inne	88	0,22%
Brak	0	0,00%
Administracja publiczna	757	1,91%
Budownictwo i gospodarka nieruchomościami	24	0,06%
Kultura i ochrona dziedzictwa narodowego	30	0,08%
Kultura fizyczna	8	0,02%
Oświata i wychowanie	167	0,42%
Rolnictwo	6	0,02%
Rybołówstwo	1	0,00%
Wyznania religijne i mniejszości narodowe	2	0,01%
Działalność ubezpieczeniowa	35	0,09%
Izby gospodarcze i handlowe	4	0,01%
Handel hurtowy i detaliczny	5 438	13,70%
Produkcja	2 650	6,68%
Logistyka i dystrybucja	15	0,04%
Poczta i usługi kurierskie	6 093	15,35%
Turystyka	10	0,03%
Gospodarka odpadami	3	0,01%
Hotele, restauracje, catering	44	0,11%
Media	7 329	18,47%
Usługi inne	496	1,25%
Osoby fizyczne	4 214	10,62%
TOTAL	39 683	100,00%

Tab. 1. Incydenty obsłużone przez CERT Polska w 2022 r. w podziale na sektor gospodarki.

Typy incydentów	Liczba incydentów	%
I. Obraźliwe i nielegalne treści	308	0,78%
Spam	239	0,60%
Dyskredytacja, obrażanie	6	0,02%
Pornografia dziecięca, przemoc	0	0,00%
Niesklasyfikowane	63	0,16%
II. Złośliwe oprogramowanie	3 409	8,59%
Wirus	0	0,00%
Robak sieciowy	0	0,00%
Koń trojański	20	0,05%
Oprogramowanie szpiegowskie	1	0,00%
Dialer	0	0,00%
Rootkit	0	0,00%
Niesklasyfikowane	3 388	8,54%
III. Gromadzenie informacji	31	0,08%
Skanowanie	19	0,05%
Podsłuch	0	0,00%
Inżynieria społeczna	1	0,00%
Niesklasyfikowane	11	0,03%
IV. Próby włamań	121	0,30%
Wykorzystanie znanych luk systemowych	7	0,02%
Próby nieuprawnionego logowania	31	0,08%
Wykorzystanie nieznanych luk systemowych	0	0,00%
Niesklasyfikowane	83	0,21%
V. Włamania	354	0,89%
Włamanie na konto uprzywilejowane	7	0,02%

Włamanie na konto zwykłe	147	0,37%
Włamanie do aplikacji	5	0,01%
Bot	1	0,00%
Niesklasyfikowane	194	0,49%
VI. Dostępność zasobów	175	0,44%
Atak blokujący serwis (DoS)	6	0,02%
Rozproszony atak blokujący serwis (DDoS)	97	0,24%
Sabotaż komputerowy	0	0,00%
Przerwa w działaniu usług (niezłośliwe)	49	0,12%
Niesklasyfikowane	23	0,06%
VII. Atak na bezpieczeństwo informacji	39	0,10%
Nieuprawniony dostęp do informacji	20	0,05%
Nieuprawniona zmiana informacji	3	0,01%
Niesklasyfikowane	16	0,04%
VIII. Oszustwa komputerowe	35 009	88,22%
Nieuprawnione wykorzystanie zasobów	1	0,00%
Naruszenie praw autorskich	2	0,01%
Kradzież tożsamości, podszycie się	28	0,07%
Phishing	25 625	64,57%
Niesklasyfikowane	9 353	23,57%
IX. Podatne usługi	188	0,47%
Otwarte serwisy podatne na nadużycia	72	0,18%
Niesklasyfikowane	116	0,29%
X. Inne	49	0,12%
Razem	39 683	100,00%

Tab 2. Incydenty obsłużone przez CERT Polska w 2022 r. w podziale na kategorie wg taksonomii eCSIRT.net mkVI1

ZGŁOSZENIA SMS

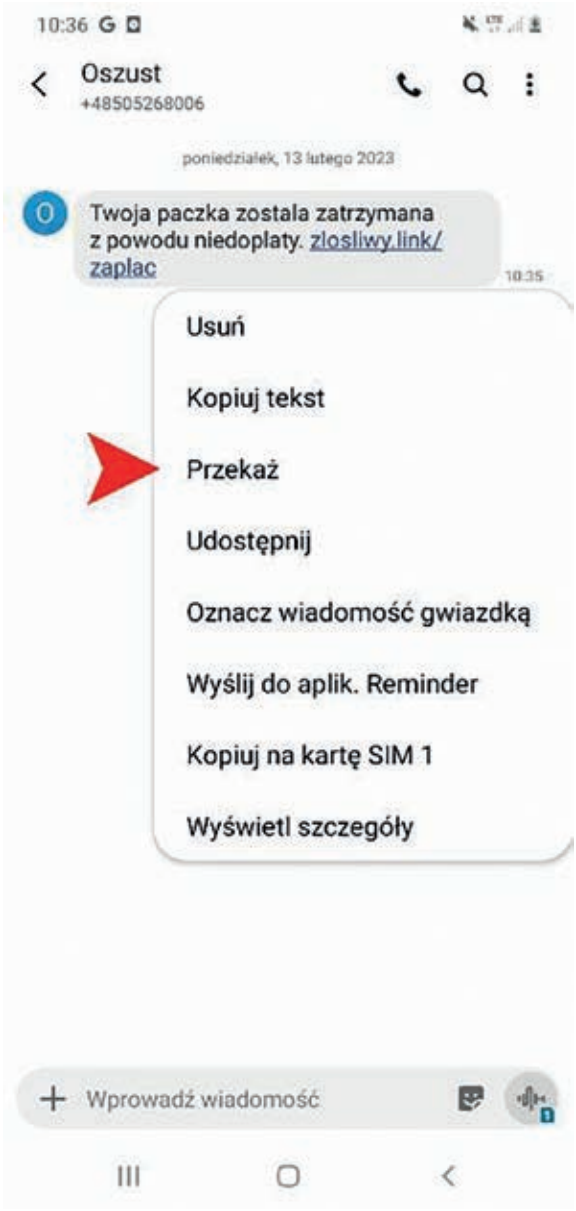
W maju 2021 r. uruchomiliśmy usługę przyjmowania zgłoszeń SMS zawierających adres URL (tzw. link), które wzbudzają podejrzenia. Pozwala to na szybkie i łatwe przesłanie nam wiadomości, która wzbudza wątpliwość. Ten kanał zgłoszeń jest w pełni zautomatyzowany, tzn. nie służy do interakcji z użytkownikiem. Po krótkiej analizie wstępnej, polegającej na sprawdzeniu znajdującego się w wiadomości linku, zgłaszający otrzymuje SMS-em jedną z następujących informacji zwrotnych:

- “W wiadomosci znajduje sie zlosliwa domena.” - domena z wykrytego adresu URL znajduje się na Liście ostrzeżeń,
- “Co najmniej jedna z domen jest zlosliwa.” - co najmniej jedna domena jednego z wykrytych adresów URL znajduje się na Liście ostrzeżeń,
- “Dziekujemy za przeslanie wiadomosci.” - rozpoznano nowy adres URL lub nie została podjęta decyzja, że jest on złośliwy,
- “Nie przyjeto zgloszenia, automatyczny system nie znalazl adresow URL w tresci wiadomosci SMS.” - wiadomość SMS nie zawiera adresu URL, ewentualne oszustwo z nią związane należy zgłosić przez formularz kontaktowy.

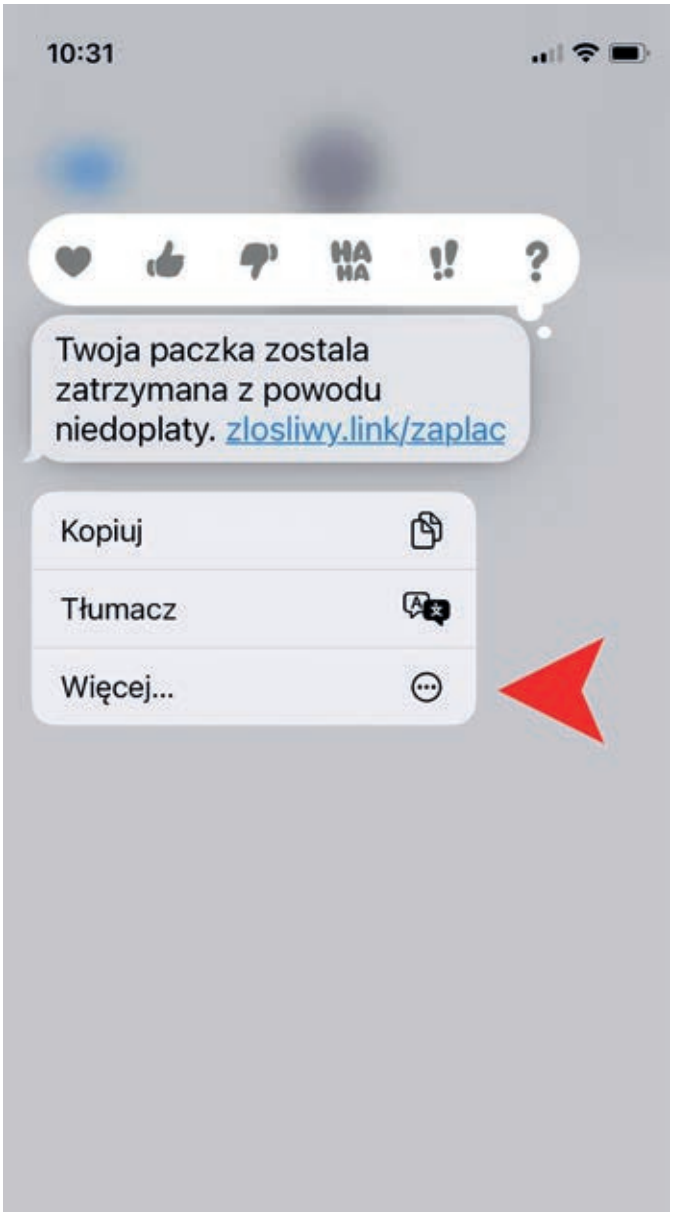
Warto podkreślić, że kanał zgłoszeń SMS, ze względu na swój automatyczny charakter, służy jedynie do rozpoznawania wiadomości z linkiem, które są elementem schematu phishingowego. Wszelkie inne incydenty należy zgłaszać w innej formie, najlepiej przy użyciu formularza na stronie https://incydent.cert.pl.

JAK ZGŁOSIĆ SMS-A?

Zgłoszenie wiadomości SMS jest bardzo proste, choć może się delikatnie różnić zależnie od dostawcy oprogramowania. Dla telefonów z systemem Android przesyłanie zgłoszenia może się dodatkowo minimalnie różnić wizualnie, ze względu na nakładkę producenta lub konkretną wersję aplikacji do obsługi SMS, ale wszystkie funkcjonalności nazywają się tak samo. Wystarczy przytrzymać zgłaszaną wiadomość, a następnie w rozwijanym menu wybrać opcję **Przekaż** (Rys. 12). W kolejnym kroku należy wpisać numer **799 448 084** lub - jeśli numer znajduje się już na liście kontaktów - wybrać go z listy i wysłać wiadomość.

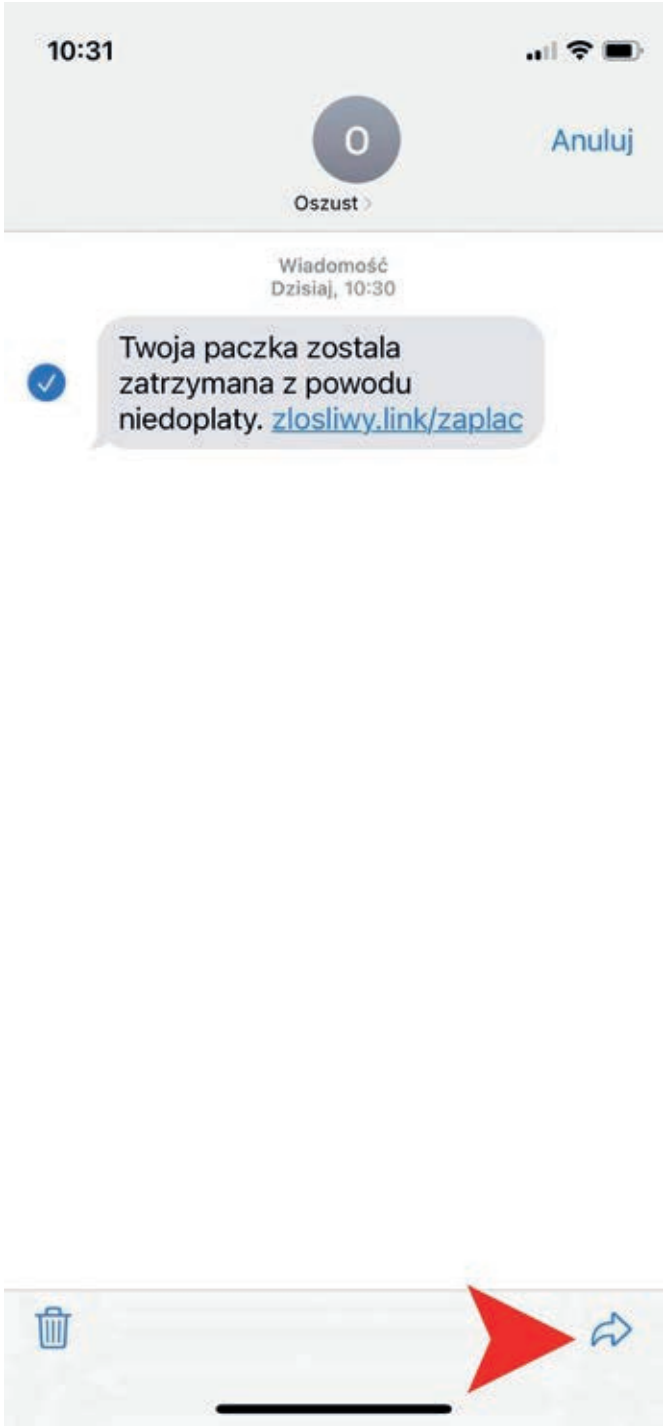


Rys. 12 Przekazywanie wiadomości z urządzenia z systemem Android.



Rys. 13 Przekazywanie wiadomości z Iphone - pierwszy widok.

Dla użytkowników iPhone ten proces różni się nieznacznie. Po przytrzymaniu wiadomości należy wybrać opcję **Więcej...** (Rys. 13), a w kolejnym kroku wcisnąć strzałkę w prawym dolnym rogu (Rys. 14).



Rys. 14 Przekazywanie wiadomości z Iphone – drugi widok.

STATYSTYKI ZGŁOSZEŃ SMS

W 2021 r., od momentu wprowadzenia omawianego systemu otrzymaliśmy 15 694 zgłoszenia SMS. Jest to duży sukces. Wśród zgłoszeń prawie połowa, bo aż 7 313 została uznana za złośliwe wiadomości phishingowe. 2022 r. przerósł nasze oczekiwania pod względem statystyk. Otrzymaliśmy aż 217 685 wiadomości SMS, czyli prawie 14 razy więcej! Aż 199 868 SMS-ów zawierało link, który został poddany dalszej analizie. Za próbę phishingu uznano 82 319 z tych wiadomości, a w konsekwencji wpisano 32 361 domen na Listę ostrzeżeń. Na ten nagły przyrost zgłoszeń wpływ ma nie tylko generalne większe wykorzystywanie SMS-ów przez oszustów, widoczne na przestrzeni całego roku, ale też nasza działalność społeczna i marketingowa opisana w innej sekcji tego artykułu. W samym listopadzie i grudniu przekroczyliśmy 100 000 otrzymanych SMS-ów, z czego 68 917 w ostatnim miesiącu roku. Na ten wynik na pewno ma wpływ większa aktywność oszustów związana z okresem świątecznym, ale jednocześnie pokazuje ona wartość prowadzonych przez nas działań społecznych.

DLACZEGO WARTO ZGŁASZAĆ SMS-Y DO CERT POLSKA?

Powinno się zgłaszać się podejrzane SMS-y do CERT Polska z kilku względów. Przesłany SMS może być pierwszym zgłoszeniem zawierającym nowy link do niebezpiecznej strony, dzięki czemu jej domena trafi na naszą Listę ostrzeżeń i tym samym uda się uchronić przed oszustwem więcej osób. Po drugie, każda informacja o cyberzagrożeniu jest dla nas kluczowa, świadomość skali na podstawie wielu powtarzających się zgłoszeń może przyczynić się do wydania ostrzeżenia lub podjęcia innych działań. Kolejną ważną kwestią jest powstająca ustawa o zwalczaniu nadużyć w komunikacji elektronicznej[8]. Zgodnie z jej projektem CSIRT NASK będzie tworzył wzorce złośliwych wiadomości, które będą blokowane przez operatorów telekomunikacyjnych. Aby ten mechanizm mógł w pełni sprawnie funkcjonować, potrzebujemy nie tylko wszystkich linków znajdujących się w złośliwych SMS-ach, ale też ich pełnej treści, dlatego tak istotne są przesyłane do nas zgłoszenia.

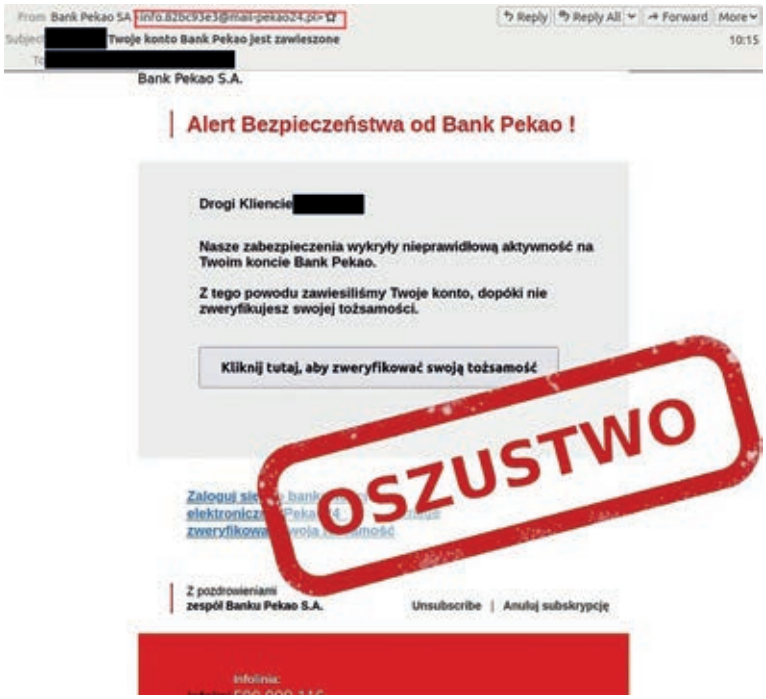
8 https://www.gov.pl/web/premier/projekt-ustawy-o-zwalczaniu-naduzyc-w-komunikacji-elektronicznej

ZNANE KAMPANIE PHISHINGOWE KONTYNUOWANE W 2022 R.

W tym roku pojawiło się wiele nowych pomysłów, jak oszukać polskich internautów. Jednak wiele oszustw wciąż opiera się na starych, znanych technikach, które nadal są skuteczne. W tym rozdziale chcielibyśmy wymienić największe kampanie, które były już znane i opisywane w poprzednich latach, ale nadal stanowiły duże zagrożenie dla użytkowników w 2022 r.

ALERTY BEZPIECZEŃSTWA NA KONTACH BANKOWYCH

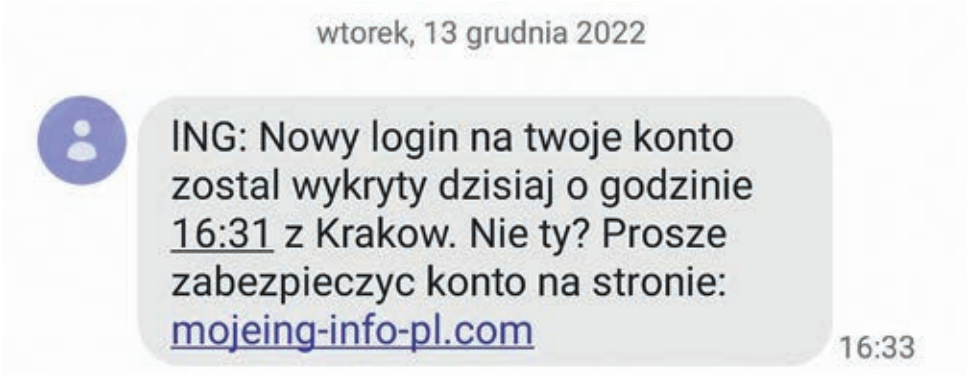
Jednymi z powtarzających się co roku oszustw, są phishingi wykorzystujące wizerunek banków. Przestępcy wykorzystują głównie schemat polegający na komunikowaniu potrzeby podjęcia działań względem nietypowej akcji na koncie bankowym. Wywierają presję czasu na potencjalnej ofierze i w ten sposób próbują ją nakłonić do wejścia na kontrolowaną przez nich fałszywą stronę.



Rys. 15 Nieprawdziwy e-mail mówiący o nieprawidłowej akcji na koncie.

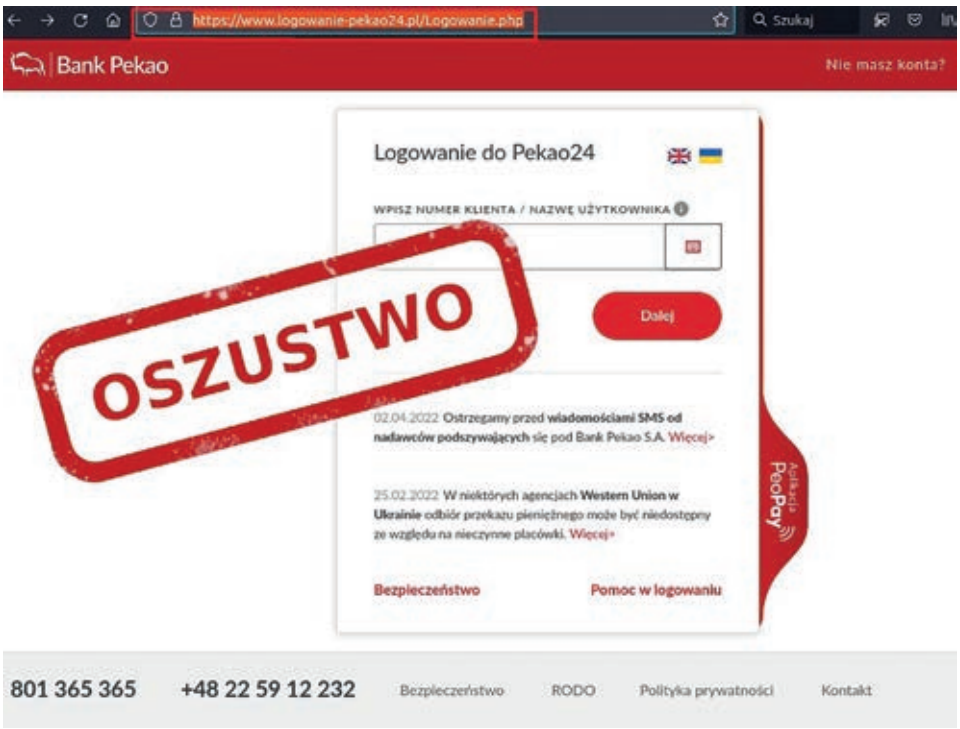
Do komunikacji z ofiarami oszuści wykorzystują między innymi wiadomości e-mail. Na losowe skrzynki pocztowe trafiają wiadomości podszywające się pod konkretny bank, które w treści zawierają link to fałszywego panelu logowania. W tych kampaniach oszuści przykładają dużą staranność do wyglądu stron, aby jak najlepiej odwzorowywały panele logowania do bankowości mobilnej danego banku.

W 2022 r. przestępcy podjęli się realizacji masowej kampanii SMS. Na telefony Polaków trafiały wiadomości o nowym loginie na konto oraz zachęcały do kliknięcia w podany link, w celu zabezpieczenia rachunku. Podobnie jak w kampaniach mailowych, przestępcy wiernie odtworzyli panel logowania do bankowości mobilnej.



Rys. 16 Fałszywy SMS dotyczący nieuprawnionego logowania na konto ING.

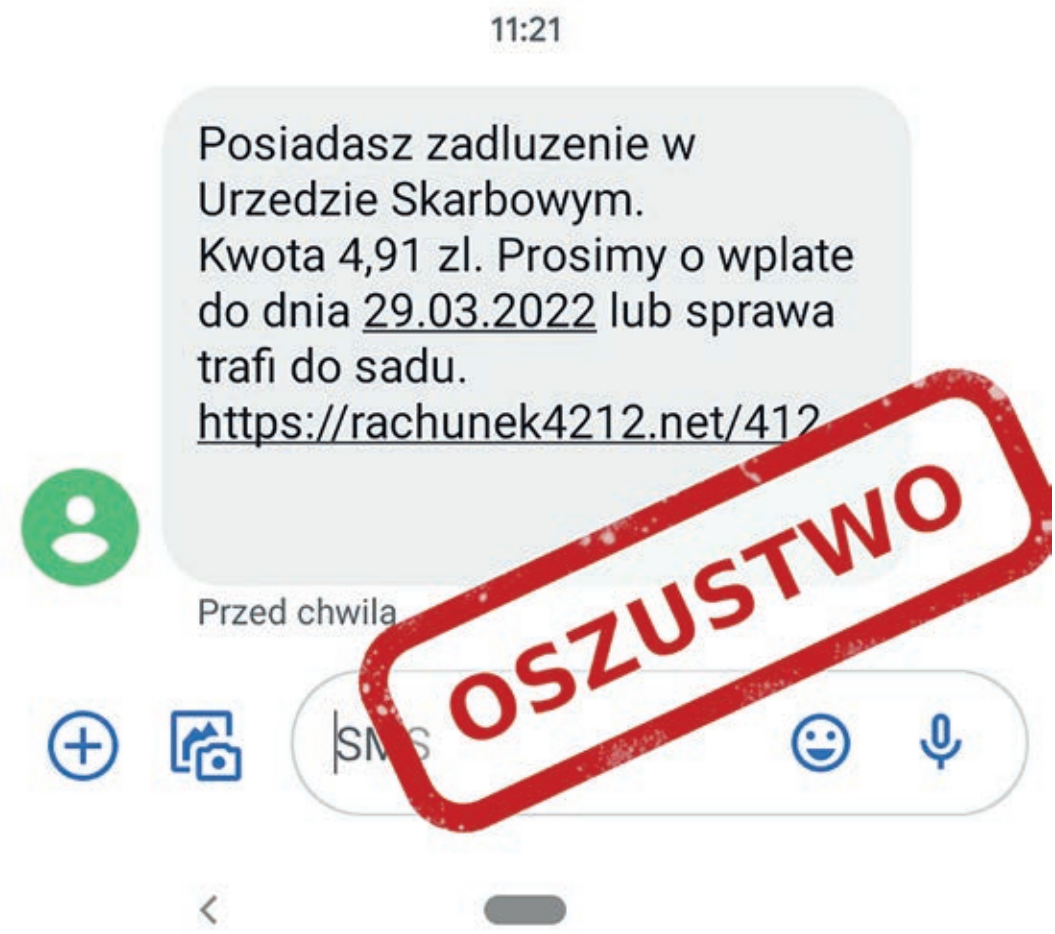
Wszystkie kampanie phishingowe miały na celu wyłudzanie danych logowania do konta bankowego potencjalnej ofiary oraz, co ważne, kodów autoryzacji do różnych czynności na koncie. Były to m.in. dodanie odbiorcy zaufanego czy przesłanie przelewu na konkretny numer. Efektem wpisania wszelkich danych, o które prosili przestępcy, była kradzież środków pieniężnych zgromadzonych na koncie.



Rys. 17 Fałszywy panel logowania w domenie logowanie-pekao24[.]pl

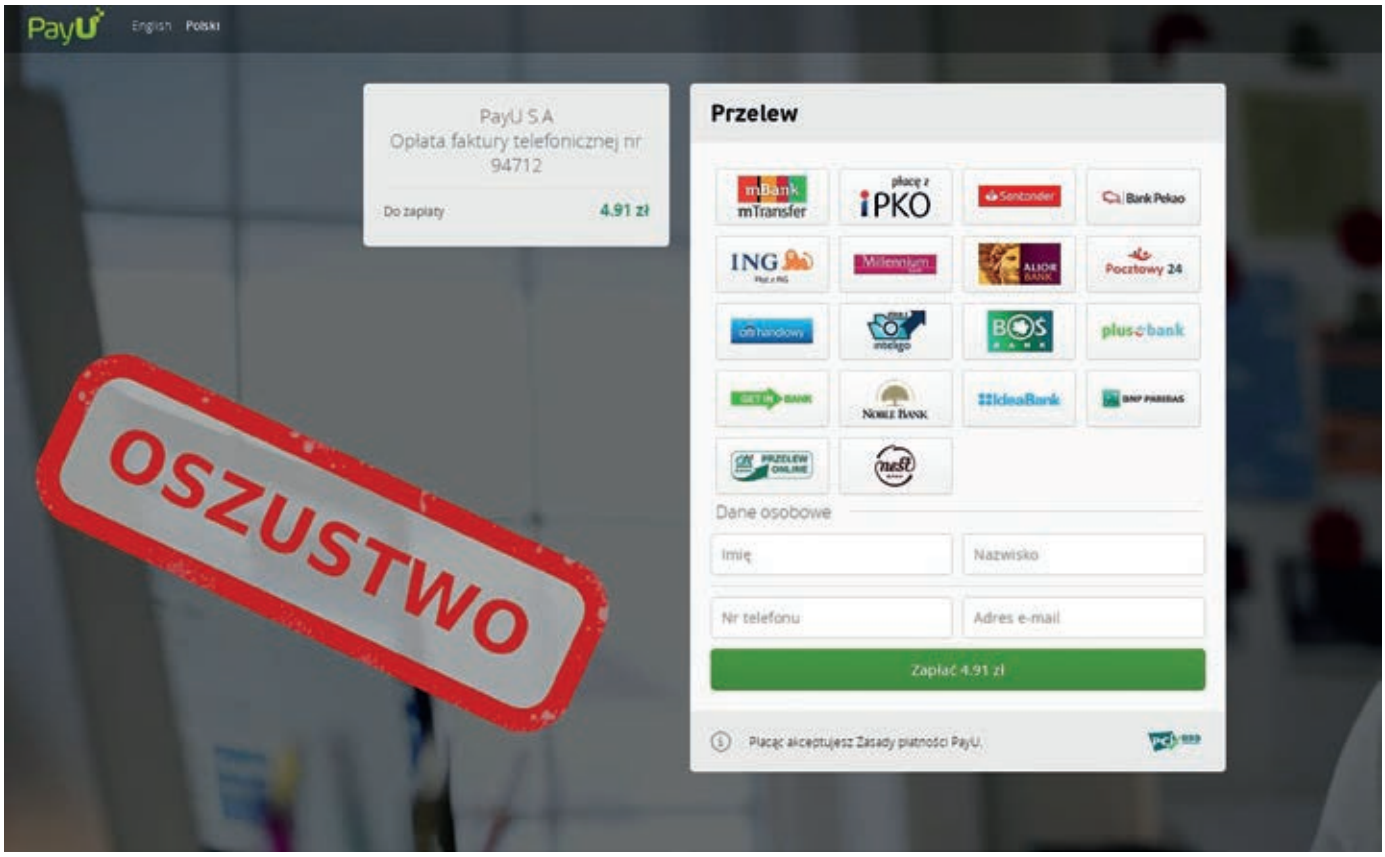
FAŁSZYWE BRAMKI PŁATNOŚCI

W poprzednich raportach często wspominaliśmy o kampaniach phishingowych, które wykorzystywały wizerunek znanych bramek płatności. W tych kampaniach oszuści również wywierali na ofierze presję czasu, często sugerując potencjalne negatywne konsekwencje.



Rys.18 Fałszywa wiadomość SMS

Charakterystyczną cechą tych kampanii jest metoda ich dystrybucji. W większości przypadków fałszywe linki trafiały na losowe numery telefonów poprzez SMS-y. W wiadomościach znajdował się albo bezpośredni link do bramki płatności albo skrócony link, który finalnie prowadził do fałszywego panelu płatności.



Rys. 19 Fałszywa bramka płatności PayU powiązana z SMS z Rys. 18.

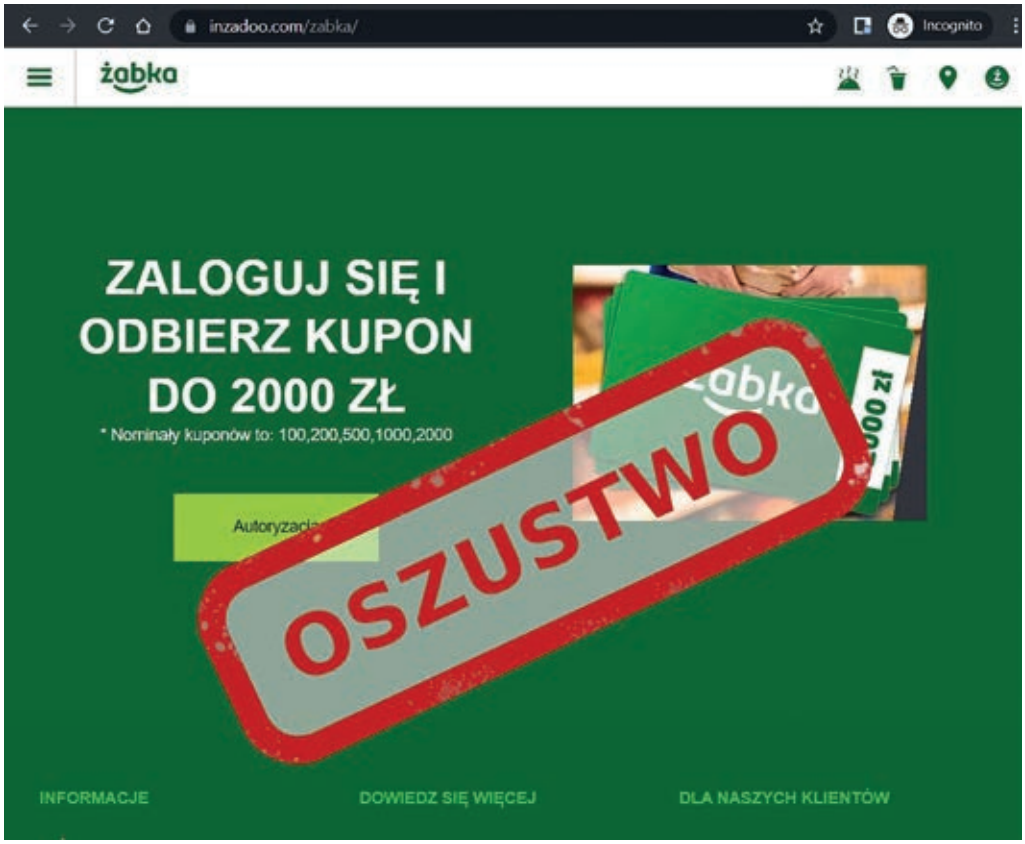
W 2021 r. najczęściej wykorzystywane były charakterystyczne skrócone linki w domenach .sv oraz .co. W tym roku oszuści zaczęli korzystać z bardziej rozpoznawalnych serwisów skracających linki, takich jak tinyurl.com.

Wśród znanych schematów tego oszustwa, kontynuowanego także w 2022 r., należy wymienić:

- fałszywe bramki PayU lub eCard, np. w okresie składania deklaracji PIT informacje o rzekomej spłacie zadłużenia w urzędzie skarbowym, ,
- wiadomości SMS, w których oszuści proszą o dopłatę do paczki lub opłacenie rachunku za energię elektryczną.

Rys.20 Fałszywy SMS informujący o kuponie na zakupy.

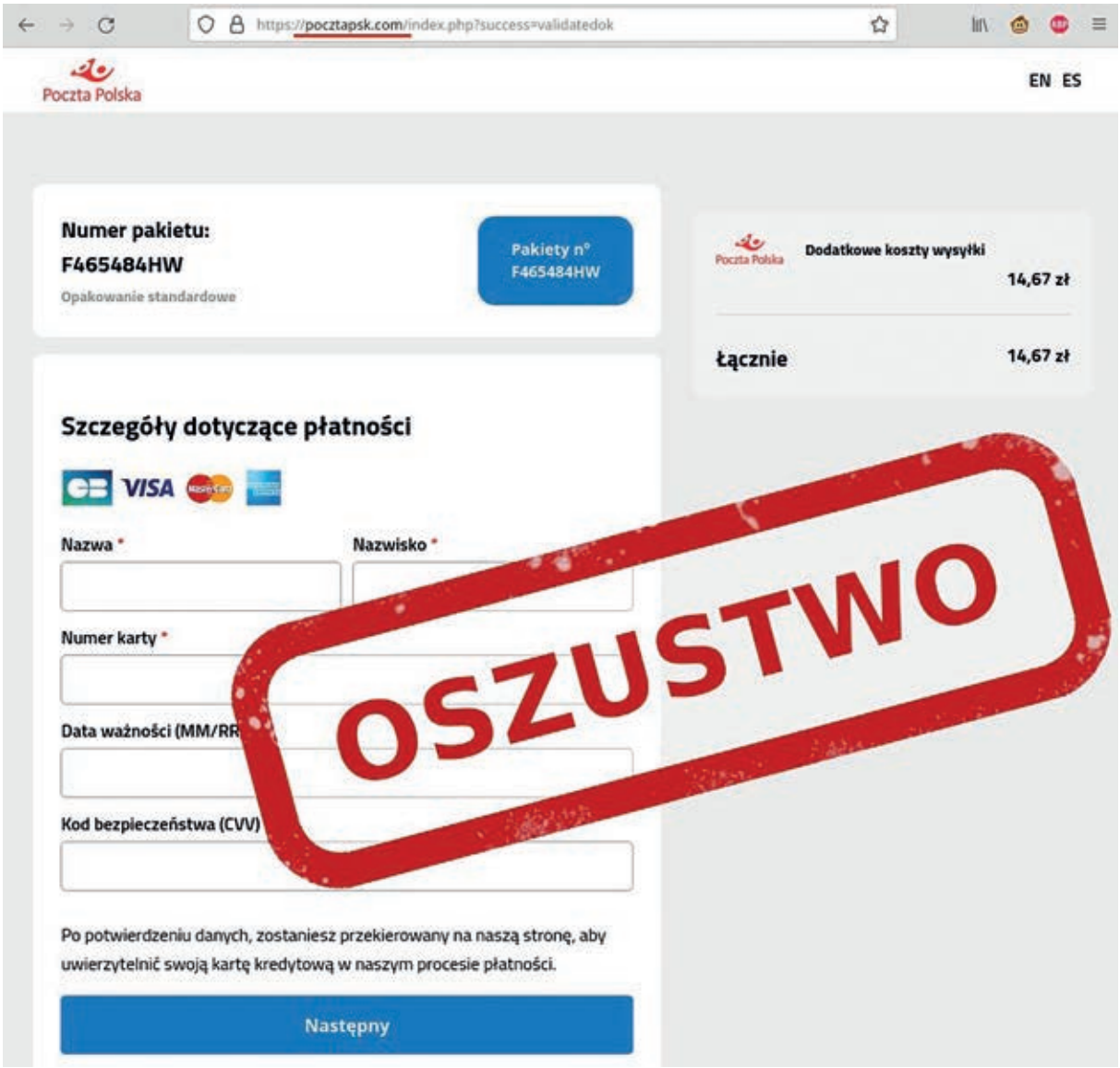
Na przestrzeni roku przestępcy wzbogacali swoje portfolio o kolejne podmioty. Pod koniec 2022 r. zaczęli wykorzystywać wizerunek sieci sklepów Żabka i rozsyłali SMS-y, które informowały o możliwości odbioru kuponu na zakupy. Załączony link prowadził do strony, która finalnie wyłudzała dane bankowości poprzez fałszywą bramkę płatności.



Rys. 21 Fałszywa strona wykorzystująca wizerunek sklepu Żabka, prowadząca do fałszywego panelu płatności.

Poza tymi dominującymi na przestrzeni roku schematami, warto zwrócić uwagę na pomniejsze kampanie wykorzystujące:

- wizerunek Poczty Polskiej, w którym oszuści przenosili ofiarę na fałszywy panel płatności w celu uregulowania rzekomej opłaty celnej,
- temat uregulowania opłaty za mandat karny poprzez załączony link, który prowadził do fałszywego panelu płatności PayU lub BlueMedia.

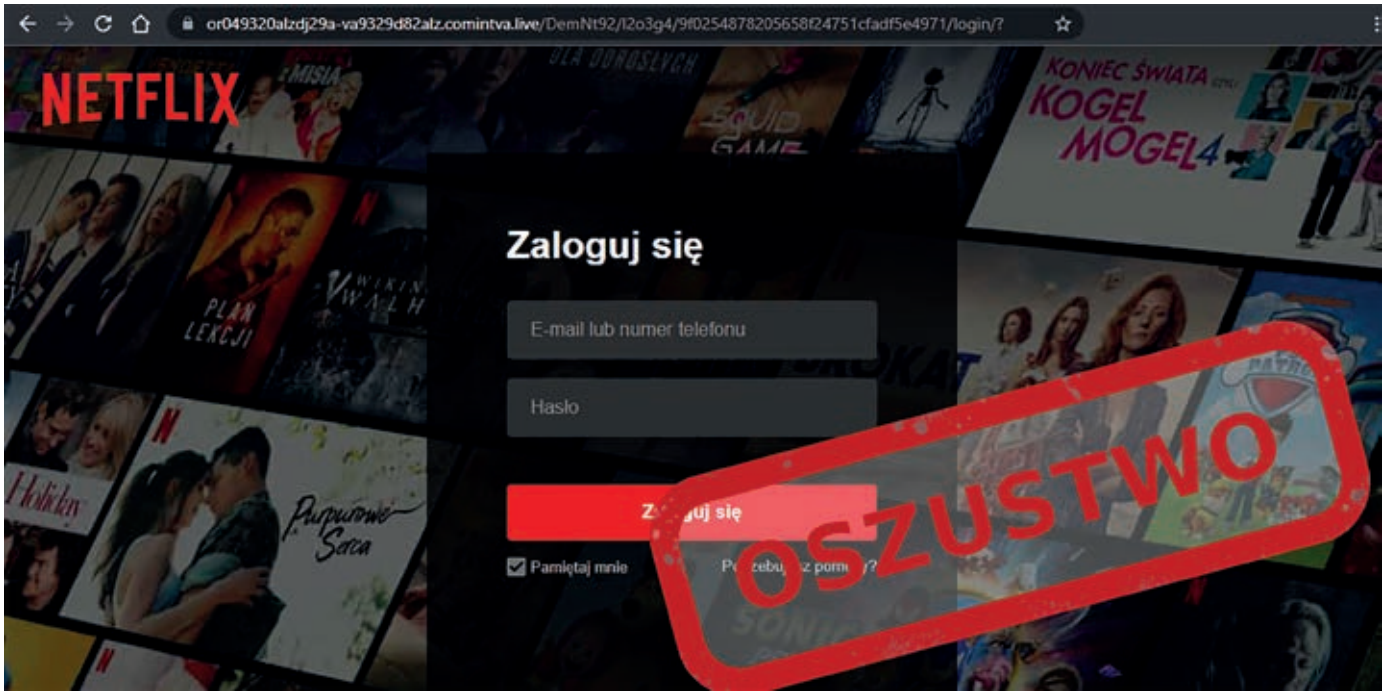


Rys. 22 Fałszywa bramka płatności wykorzystująca wizerunek Poczty Polskiej.

Kampanie te dystrybuowane są w sposób masowy, ale często w krótkich, maksymalnie 3 dniowych okresach.

KRADZIEŻ KONT UŻYTKOWNIKÓW NETFLIX

Netflix jest obecnie najpopularniejszą platformą streamingową w Polsce[9]. Ten fakt zachęca przestępców do kolejnych oszustw, których celem jest wyłudzanie danych logowania do konta na tym portalu.

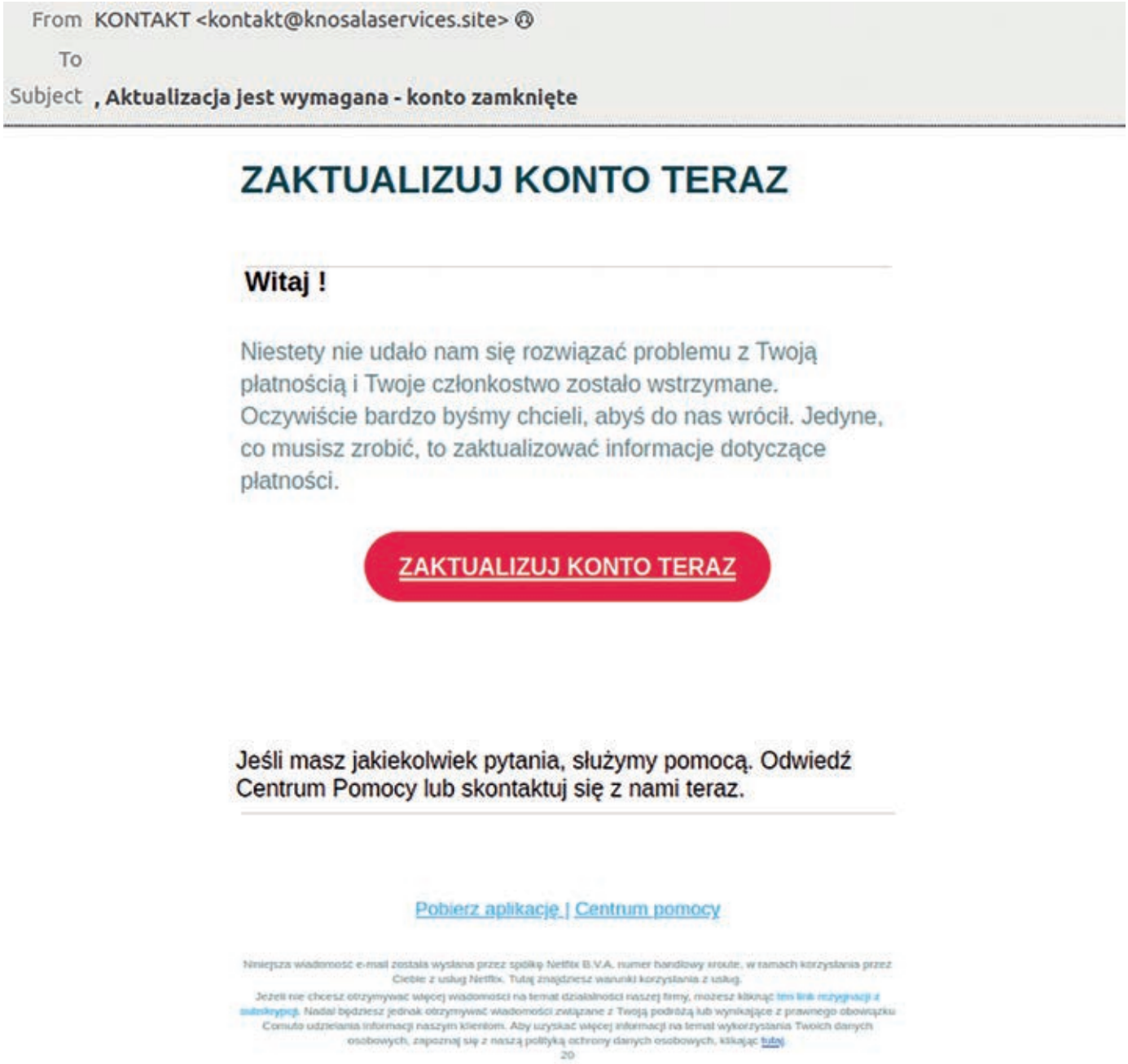


Rys. 23 Fałszywy panel logowania do Netflixa.

Do tej pory podstawowy schemat działania oszustów polegał na rozsyłaniu dużej liczby maili na losowe skrzynki pocztowe. Ich treść wskazywała na potrzebę zaktualizowania konta w związku z rzekomym problemem z płatnością za subskrypcję.

Po wejściu na stronę pojawiał się fałszywy panel logowania do konta. Podanie w nim swoich danych logowania skutkowało przekazaniem ich przestępcom. Konta te zazwyczaj były przejmowane, a później sprzedawane po zaniżonej cenie.

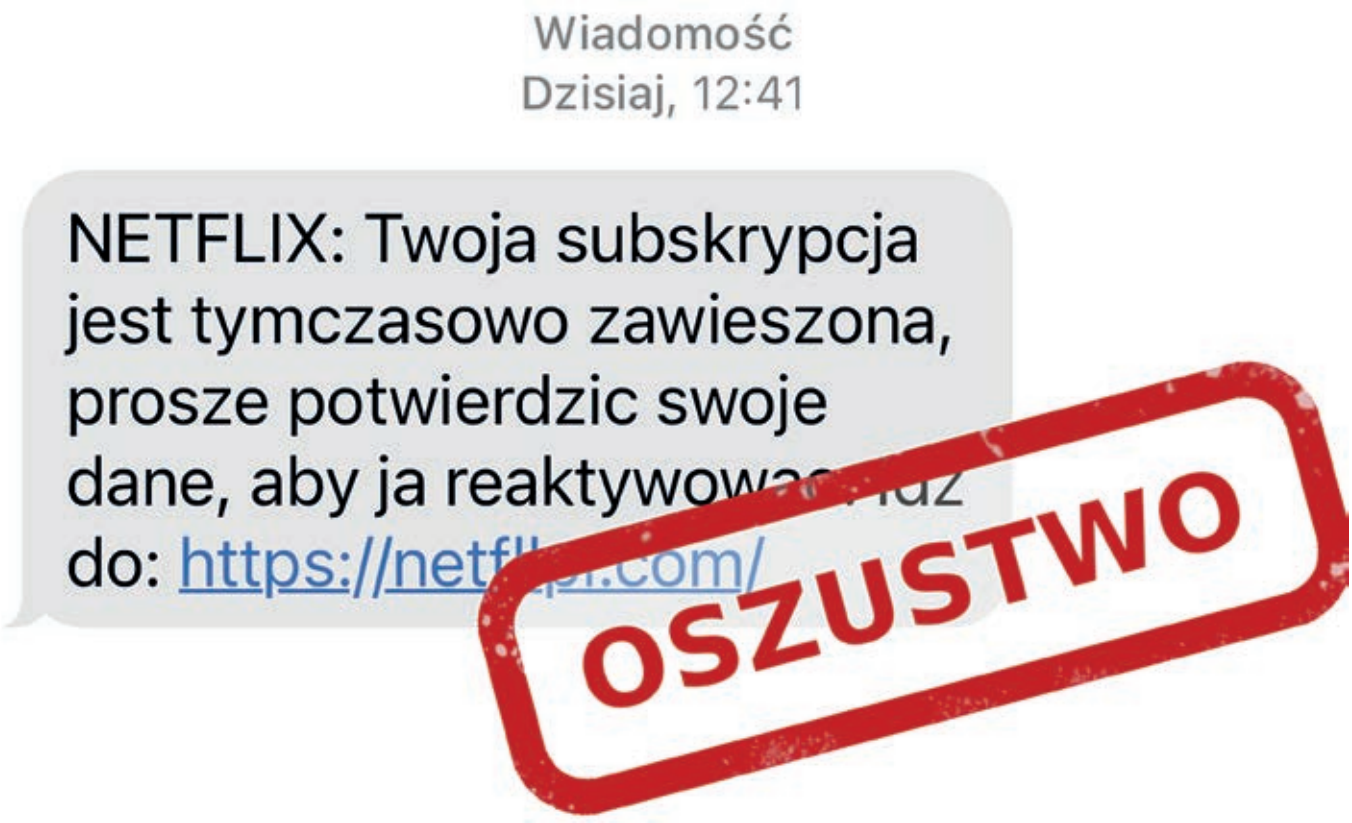
9 https://www.enisa.europa.eu/publications/cyber-europe-2022-after-action-report



Rys. 24 E-mail mówiący o potrzebie podjęcia akcji na koncie Netflix.

Kampania ta pojawiała się epizodycznie. Nie była prowadzona w sposób ciągły na na przestrzeni całego roku, a oszuści co jakiś czas rozpoczynali kolejną wysyłkę identycznych wiadomości. Inną cechą charakterystyczną tej kampanii były domeny, które nie pokrywały się z tematyką portalu Netflix. Większość z linków zawartych w wiadomościach prowadziła na domeny ze strefy PL, które następnie przekierowywały na jedną, wspólną domenę, gdzie znajdował się phishing.

W 2022 r. pojawiła się inna kampania phishingowa dotycząca użytkowników serwisu Netflix. W podobnym epizodycznym stylu, na losowe numery telefonów trafiały wiadomości SMS o rzekomo zawieszonej subskrypcji. W treści znajdowała się informacja o możliwości reaktywacji subskrypcji poprzez stronę pod przesłanym linkiem.



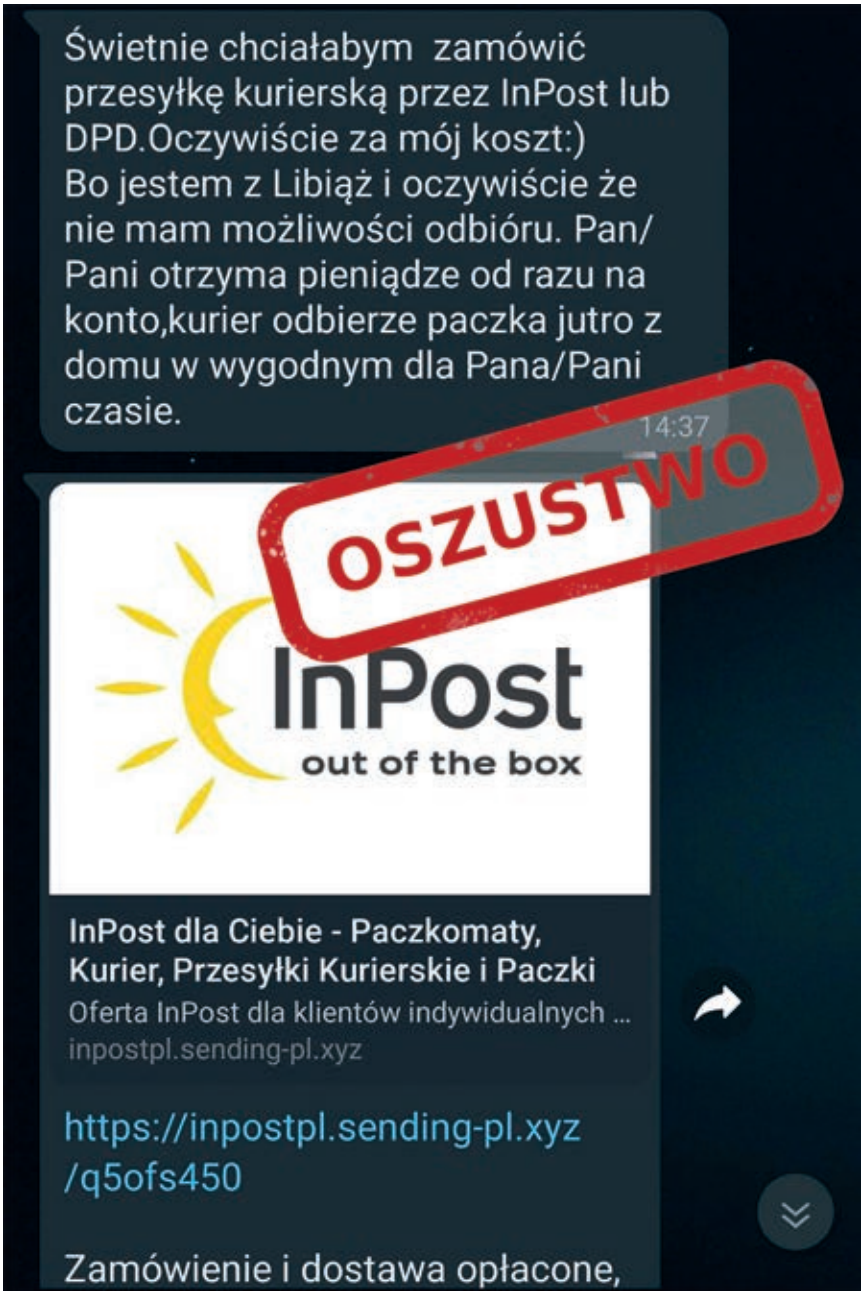
Rys. 25 SMS dotyczący rzekomej potrzeby reaktywacji subskrypcji Netflix.

Na stronie pojawiały się dwa panele. Jeden, znany z poprzedniej wersji oszustwa, panel logowania do konta Netflix. Podobnie, jak przy poprzednich kampaniach, podanie danych logowania skutkowało przekazaniem i potencjalną utratą dostępu do konta. W tym przypadku oszuści posunęli się o krok dalej i po rzekomym zalogowaniu się na konto, prosili o podanie danych karty płatniczej w celu reaktywacji konta.

W przeciwieństwie do mailowej kampanii phishingowej, wykorzystywane nazwy domen były bardzo zbliżone do nazwy faktycznego serwisu. Takie działanie miało uśpić czujność potencjalnej ofiary i w ten sposób zachęcić do otworzenia załączonego linku.

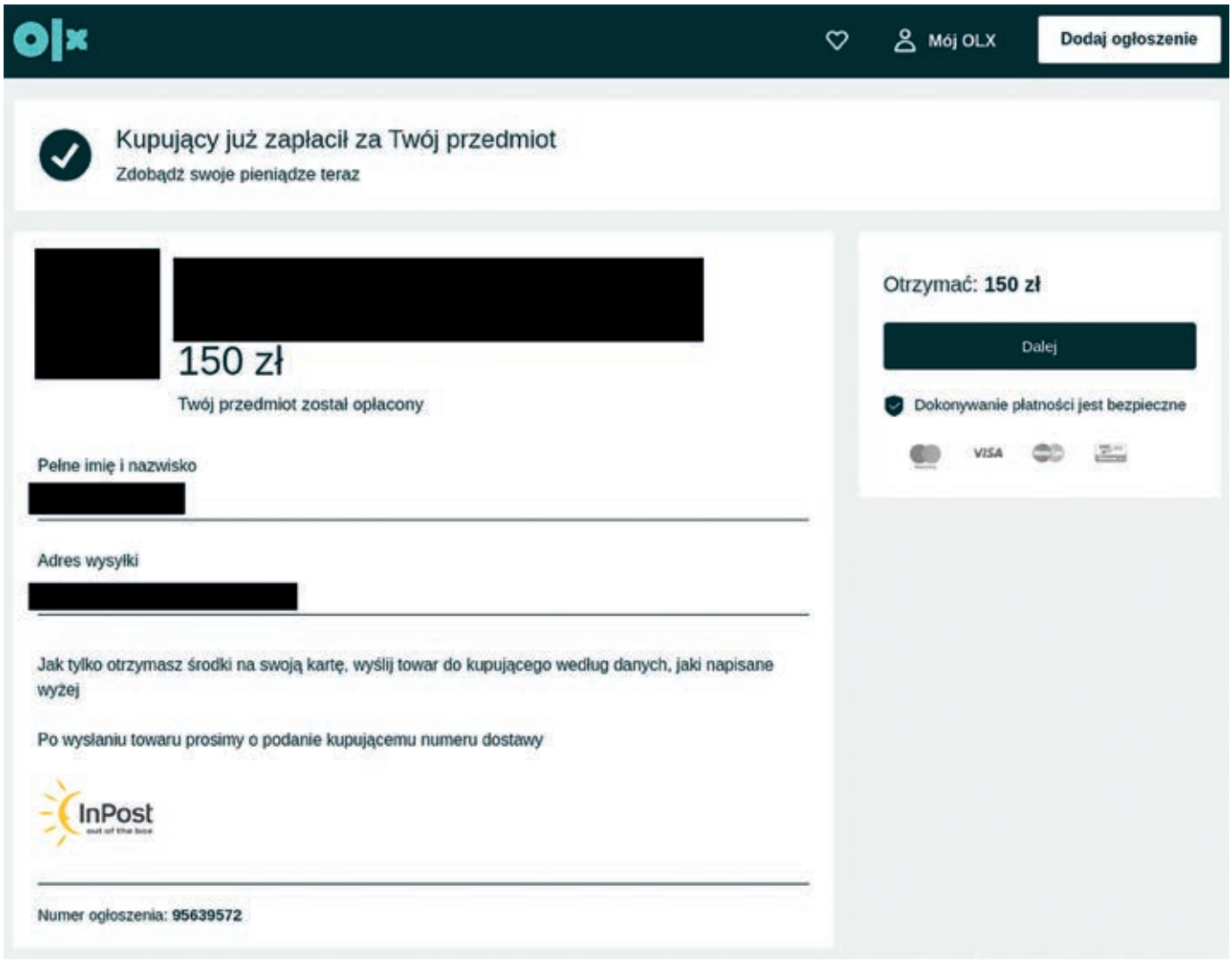
WYŁUDZANIE PIENIĘDZY OD SPRZEDAWCÓW NA PORTALACH OGŁOSZENIOWYCH

Od końca 2020 r. obserwujemy kampanie phishingowe, których celem są sprzedawcy działający na różnych portalach ogłoszeniowych. W 2021 r. była to jedna z częściej obserwowanych przez nasz zespół kampanii phishingowych. Przestępcy wykorzystali niską świadomość istnienia takiego oszustwa oraz chęć sprzedającego do szybkiej finalizacji transakcji. Wraz z upływem czasu wzrosła świadomość o tego rodzaju oszustwie wśród użytkowników Internetu i tym samym liczba zgłoszeń z nim związanych znacząco zmalała w 2022 r.



Rys. 26 Fragment konwersacji z oszustem na Whatsapp z linkiem do fałszywego panelu płatności.

Niezmiennie od kilku lat, oszuści kontaktują się poprzez komunikator WhatsApp ze sprzedawcami tworzącymi ogłoszenia na portalach takich jak OLX czy Vinted. W trakcie rozmowy przestępcy sugerowali duże zainteresowane wystawionym przedmiotem oraz deklarowali chęć szybkiego zakupu. W wiadomościach informowali sprzedającego o rzekomym nowym sposobie zapłaty za przedmiot. Oszuści w wiadomościach umieszczali link do strony podszywającej się pod portal OLX, która finalnie służyła do wyłudzania danych karty płatniczej. Charakterystyczną cechą tego oszustwa jest to, że pierwsza wyświetlona zawartość zawierała przekopiowane informacje dotyczące faktycznego ogłoszenia.



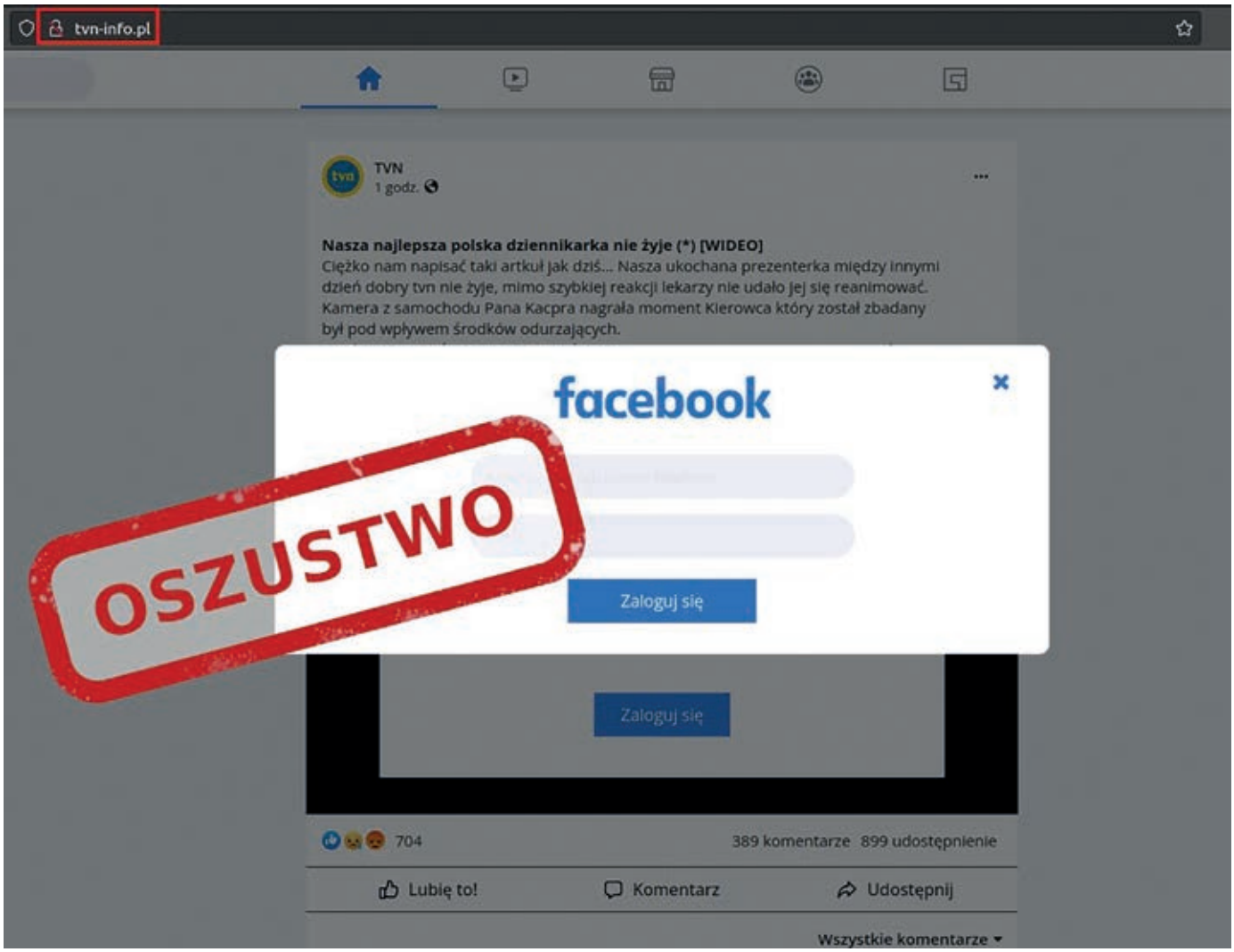
Rys. 27 Fałszywa strona OLX informująca o zapłaceniu za przedmiot.

Podobnie jak w poprzednich latach, pojawiały się warianty tej kampanii wycelowane w użytkowników serwisów Booking oraz BlaBlaCar. We wszystkich przypadkach metoda pozostawała niezmienna. Przestępcy informowali, że ktoś skorzystał z naszego ogłoszenia i zachęcali do kliknięcia w link, aby odebrać pieniądze.

NIEPRAWDZIWE POSTY ORAZ PRZEJMOWANIE KONT NA FACEBOOK

Oszustwa wymierzone w użytkowników Facebooka znane są od lat. Można wyróżnić dwie główne wersje prowadzonych kampanii. Mniej popularna ciągle bazuje na tym samym schemacie - z przejętych kont oszuści wysyłają masowo wiadomości do osób z listy znajomych przejętego konta, w których znajdują się linki do fałszywego panelu logowania do portalu Facebook. Zdarza się również, że przestępcy chcą spieniężyć dostęp do czyjegoś konta i rozsyłają wiadomości do znajomych danego użytkownika z prośbą o przelanie pieniędzy poprzez BLIK.

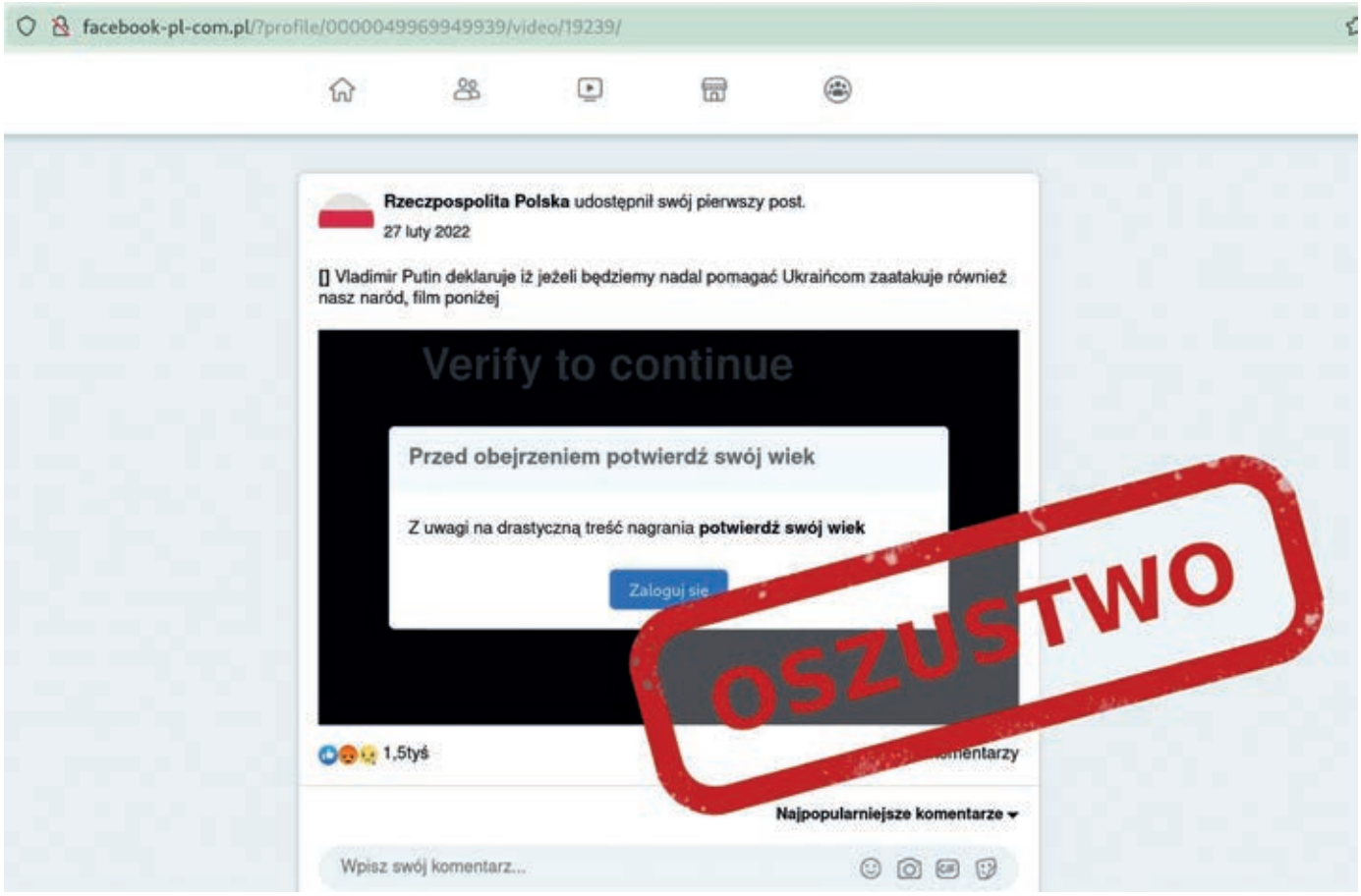
Jednak bardziej rozpoznawalnym i częściej obserwowanym wariantem tego oszustwa są fałszywe posty na licznych grupach. Bardzo często oszuści wykorzystują chwytliwe tematy, które w danym okresie wywołują dużo emocji lub po prostu są kontrowersyjne.



Rys. 28 Fałszywa strona prezentująca post na Facebook oraz panel logowania.

Najczęstszym miejscem publikacji fałszywych postów były grupy otwarte posiadające dużą liczbę członków, zazwyczaj lokalne (miejskie, gminne) lub handlowe typu "sprzedam/wymienię/oddam". Publikacja wykorzystywana do ataku ma prostą strukturę. Składa się z krótkiego opisu wywołującego silne emocje (strach, oburzenie, prośbę o pomoc) oraz linku do fałszywej strony.

Wpisy te zazwyczaj mówią o dramatycznym wydarzeniu: wypadku, porwaniu czy ataku na konkretną osobę. Bardzo często fabrykowano informacje o krzywdzie wyrządzonej znanej osobistości lub rzekomej osobie z okolicy. Wywołanie silnych emocji sprawia, że ludzie bez namysłu klikają w podany link, w podobny sposób działają clickbaity.



Rys. 29 Fałszywa strona prezentująca nieprawdziwy post o wojnie w Ukrainie.

W 2022 r. pojawiały się fałszywe wpisy dotyczące ważniejszych wydarzeń z tego roku. Na szczególną uwagę zasługują posty, które odnosiły się do dni przed oraz w trakcie wojny w Ukrainie. Oszuści tworzyli historie, które miały wzbudzać strach wśród Polaków. Bardzo często prezentowano fałszywe informacje o rzekomym ataku na Polskę, czy też "realnych groźbach Putina".

Należy jednak zwrócić uwagę, że w ubiegłym roku wykorzystywane były także inne wydarzenia, m.in. Koncert Finałowy Wielkiej Orkiestry Świątecznej Pomocy. W okresie przygotowań do 30. Finału WOŚP na różnych grupach zaczęły pojawiać się wpisy o rzekomym wypadku Jerzego Owsiaka.

Rys. 30 Post na grupie Facebook, prezentujący informacje o rzekomym wypadku Jerzego Owsiaka.

Niezależnie od prezentowanej historii, cały proces opiera się na imitacji mechanizmu logowania się do aplikacji poprzez powiązanie konta z kontem Facebookowym. Wpisane dane logowania w takim panelu trafiają prosto do przestępców.

Skuteczną metodą obrony przed tego typu atakami jest odpowiednie zabezpieczenie swojego konta. Zespół CERT Polska nie zaobserwował, żeby przestępcy wyłudzali od potencjalnych ofiar np. kody z aplikacji do dwuskładnikowego uwierzytelnienia. Dzięki dwuetapowej weryfikacji nasze konto jest zabezpieczone nawet w przypadku podania danych logowania na fałszywej stronie. Zachęcamy do zapoznania się z naszym poradnikiem, aby dowiedzieć się więcej na temat bezpiecznego korzystania z portali społecznościowych (https://cert.pl/uploads/docs/CERT_Polska_Bezpieczna_poczta_i_konta_spolecznosciowe.pdf).

NOWE KAMPANIE ZAOBSERWOWANE W 2022 ROKU

W ubiegłym roku przestępcy wykorzystywali rozwój technologii cyfrowych do przeprowadzenia zaawansowanych kampanii phishingowych i infekowania szkodliwym oprogramowaniem, które, tak jak w przypadku działań z wcześniejszych lat, miały na celu wyłudzenie danych uwierzytelniających do bankowości elektronicznej, ale również do kont pocztowych i społecznościowych.

KAMPANIE WYKORZYSTUJĄCE WIZERUNEK STRON I INSTYTUCJI RZĄDOWYCH

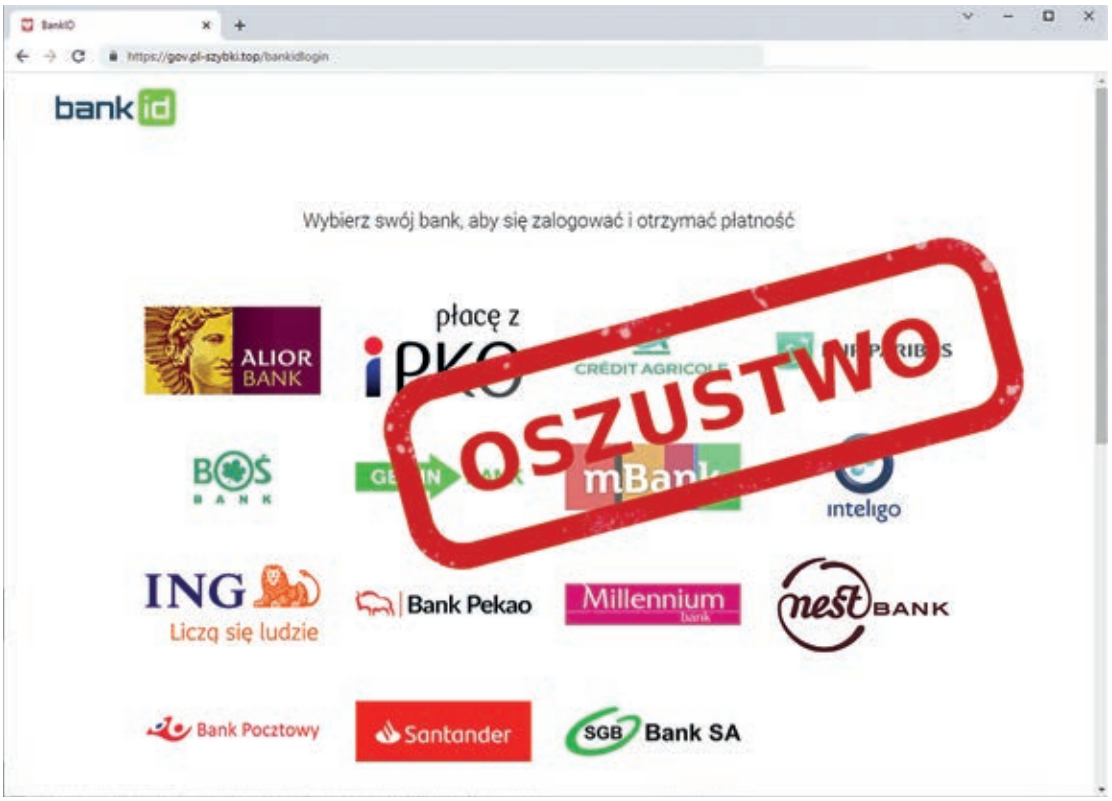
Na początku 2022 r. przestępcy dystrybuowali wiadomości informujące o dopłatach do szczepienia, SMS-y zawierały link do witryny podszywającej się pod portal "gov.pl".

Rys. 31 Fałszywa wiadomość SMS.

Na stronie, wykorzystującej logotyp rządowego portalu, znajdowała się informacja o wypłacie 300 zł za szczepienie w ramach programu “Wsparcie”. Pieniądze mieli otrzymać wszyscy Polacy, którzy przeszli pełny cykl szczepienia. Rzekomy odbiór środków miał być realizowany poprzez zalogowanie do bankowości Internetowej.

Rys. 32 Strona wykorzystująca wizerunek portalu gov.pl.

W rzeczywistości link prowadził do fałszywego panelu podszywającego się pod wybrany bank, którego celem było przechwycenie danych logowania potencjalnej ofiary. Podanie ich przestępcom mogło doprowadzić do utraty środków finansowych.

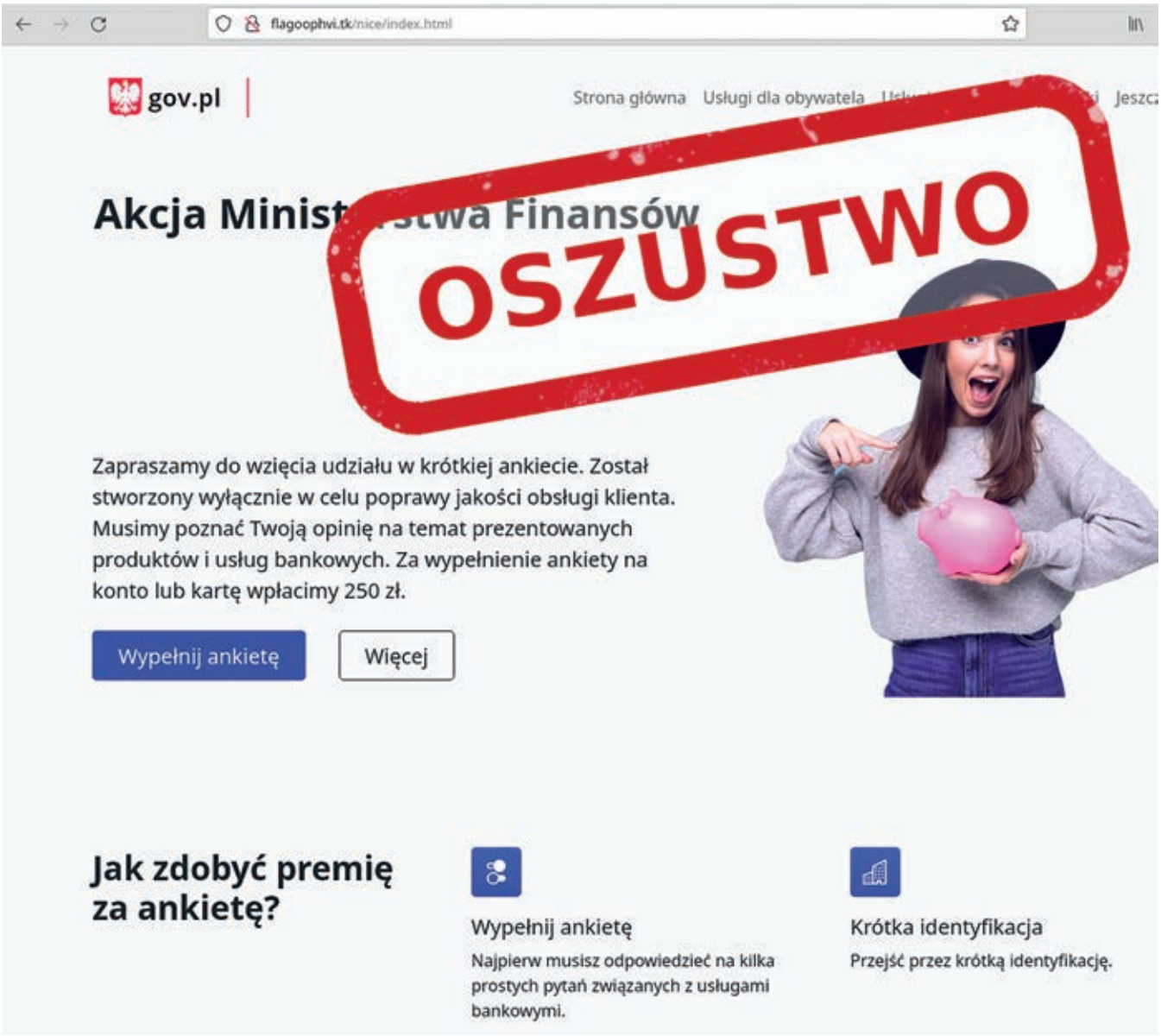


Rys. 33 Fałszywa bramka płatności.

W kolejnym wariancie kampanii oszuści, podszywając się pod Ministerstwo Finansów, wysyłali wiadomości SMS z zaproszeniem do wzięcia udziału w ankiecie. Aby zachęcić do kliknięcia w załączony link, oszuści oferowali 250 zł za wypełnienie formularza.

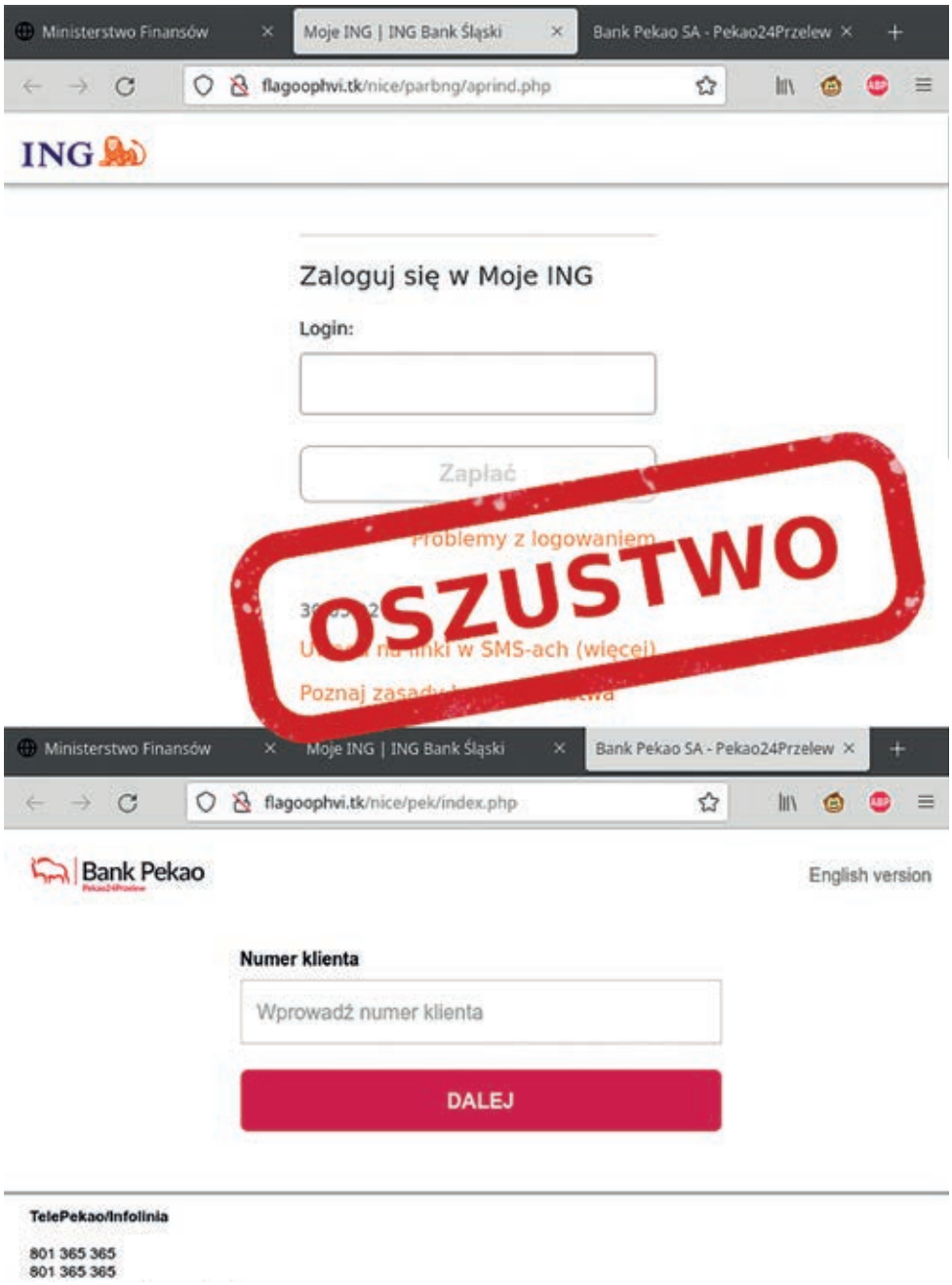
Rys. 34 SMS dotyczący rzekomej ankiety Ministerstwa Finansów.

Po wejściu na stronę ukazywał się portal, który wyglądem przypominał serwis gov.pl. Zamieszczona na nim była ankieta, która miała dotyczyć oceny jakości obsługi klienta przez jego bank.



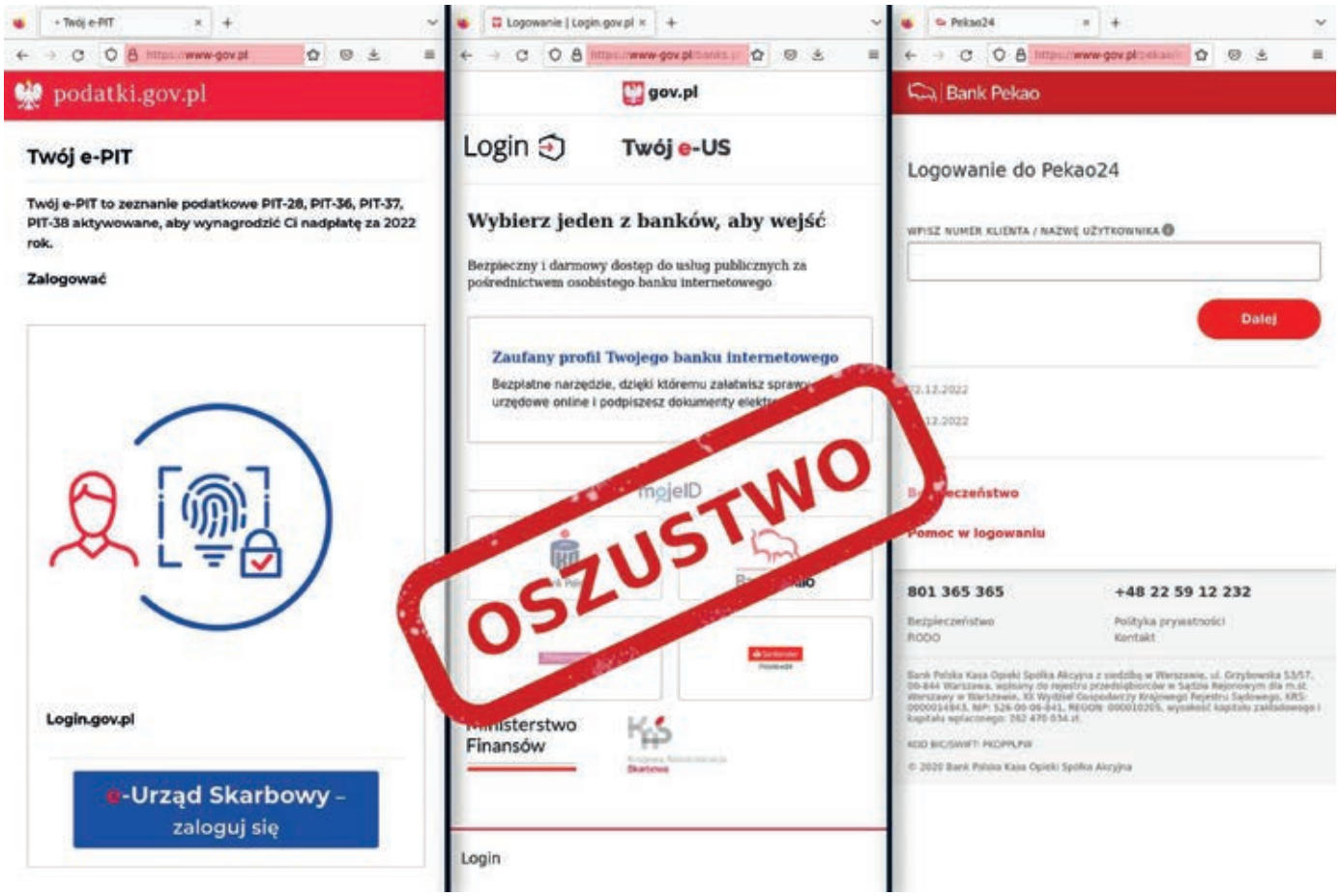
Rys. 35 Strona podszywająca się pod portal gov.pl

W ostatniej fazie oszustwa pojawiał się panel logowania do banku pod pretekstem powiązania z kontem, na które potencjalna ofiara miała otrzymać obiecaną nagrodę. W rzeczywistości dane logowania trafiały do przestępców.



Rys. 36 Fałszywe panele logowania do banków.

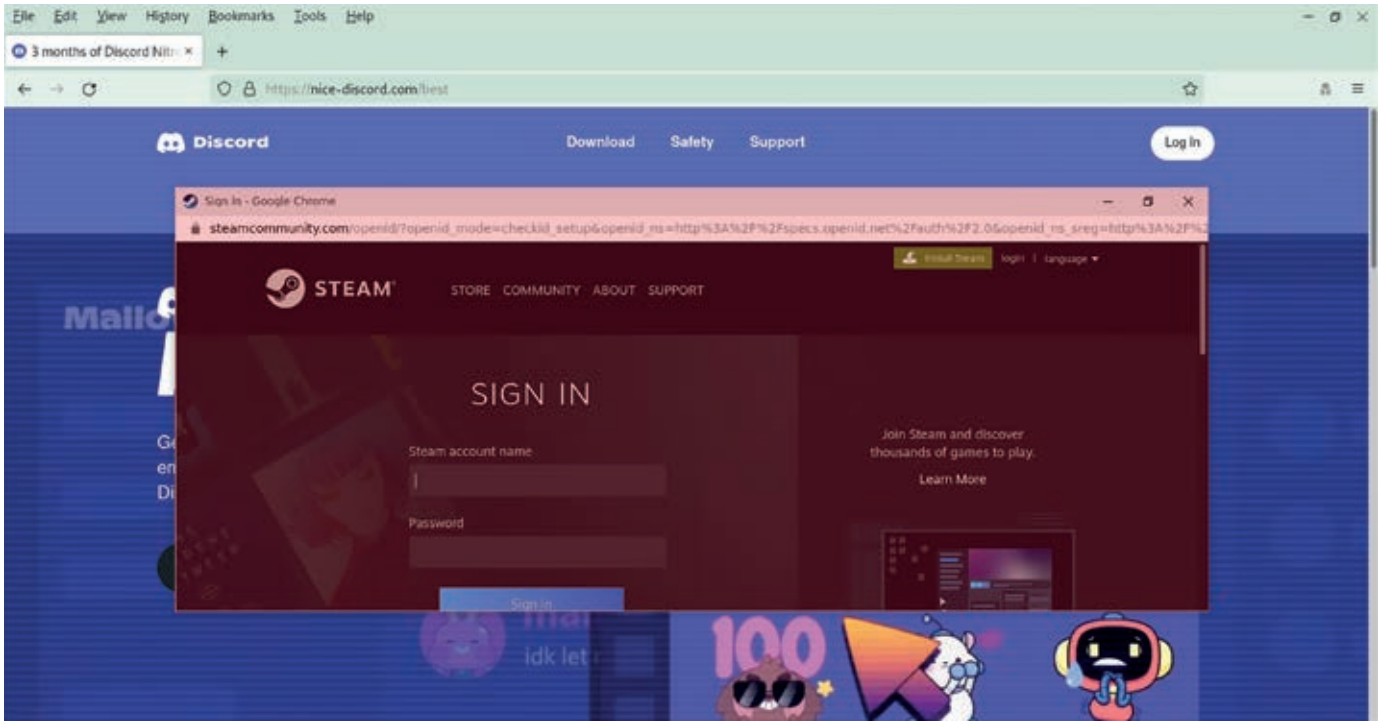
W nowej odsłonie kampanii oszuści znów podszywali się pod Ministerstwo Finansów i Krajową Administrację Skarbową. W tym przypadku informowali o możliwości uzyskania rekompensaty za nadpłatę podatku PIT. Po kliknięciu w znajdujący się w wiadomości link, użytkownik był przenoszony na nieprawdziwą stronę Twój e-PIT. Dalsza część oszustwa przebiegała tak jak we wcześniejszych wersjach kampanii: wyświetlany był panel wyboru banku, a następnie fałszywy panel logowania. Zdobyte w ten sposób dane uwierzytelniające do bankowości Internetowej służyły do kradzieży pieniędzy z konta.



Rys. 37 Strona podszywająca się pod serwis podatki.gov.pl.

ATAKI Z WYKORZYSTANIEM TECHNIKI BROWSER IN THE BROWSER

Większość stron Internetowych, które przestępcy wykorzystują w kampaniach phishingowych, nie różni się od siebie pod względem sposobu działania. Jednak w 2022 r. spopularyzowało się niestandardowe rozwiązanie w postaci techniki Browser In The Browser. Polega ona na wyświetlaniu w ramach odwiedzanej strony pozornie nowego okna przeglądarki, zawierającego fałszywy panel logowania. Okno stanowiło jedynie element strony, dobrze wykonany graficznie, przez co ofiara mogła je pomylić z faktycznym nowym oknem aplikacji. Dodatkowo, wyświetlany w nim fałszywy pasek adresu zawierał poprawną domenę strony logowania. Użytkownik, który sprawdził zawartą w nim domenę przed wpisaniem wrażliwych danych, mógł sądzić, że znajduje się na właściwej stronie.



Rys. 38 Przykładowy atak z zastosowaniem techniki Browser in The Browser.

Technika ta zazwyczaj imituje zachowanie strony podczas logowania za pomocą dostawcy tożsamości. Takie logowanie może przebiegać na dwa sposoby. Zazwyczaj strony, na których następuje próba logowania, przekierowują automatycznie do witryny logowania dostawcy tożsamości. Po zalogowaniu się użytkownik jest przekierowywany z powrotem na pierwotną stronę. Zdarza się jednak, że zamiast przekierowania, strona dostawcy tożsamości otwiera się w osobnym okienku przeglądarki. Samo automatyczne otwarcie osobnego okna przeglądarki z panelem logowania nie jest czymś szczególnie zaskakującym. Jednak w tym drugim przypadku może dojść do oszustwa, jeśli okno ze stroną logowania nie jest prawdziwe. Chcąc uchronić się przed tego typu atakiem warto zwrócić uwagę na jeden szczegół. W przypadku fałszywego okna nie jest możliwe jego wyświetlenie poza obszarem, który kontrolują przestępcy, czyli zawartości karty w przeglądarce. Warto spróbować przesunąć okno w bok lub w górę, w taki sposób, aby zasłoniło część okna przeglądarki. W przypadku fałszywego okna nie będzie to możliwe.

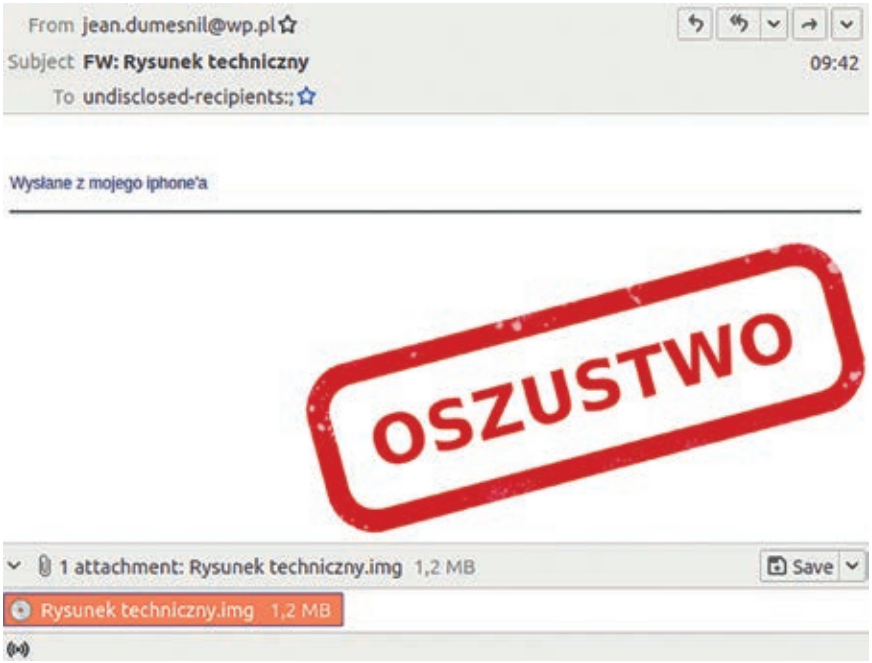
DYSTRYBUCJA OPROGRAMOWANIA INFORMATION STEALER POPRZEZ POCZTĘ E-MAIL

W 2022 r. przestępcy wielokrotnie wykorzystywali wektor ataku, jakim są skrzynki pocztowe, aby zainfekować komputer osoby, która otworzy szkodliwy załącznik. W części kampanii wykorzystywany był spoofing, czyli podszycie pod nadawcę wiadomości, które możliwe było dzięki błędnej konfiguracji mechanizmu SPF oraz DMARC przez właściciela domeny lub jej braku.

W jednej z kampanii wykorzystany został brak konfiguracji mechanizmu SPF dla domeny biznes.gov.pl. Przestępcy podszyli się pod nadawcę i przeprowadzili wysyłkę wiadomości, w których informowali o powiadomieniu, które miało rzekomo znajdować się w załączniku. W rzeczywistości załącznikiem było archiwum ze złośliwym skryptem, który po otwarciu infekował system szkodliwym oprogramowaniem.

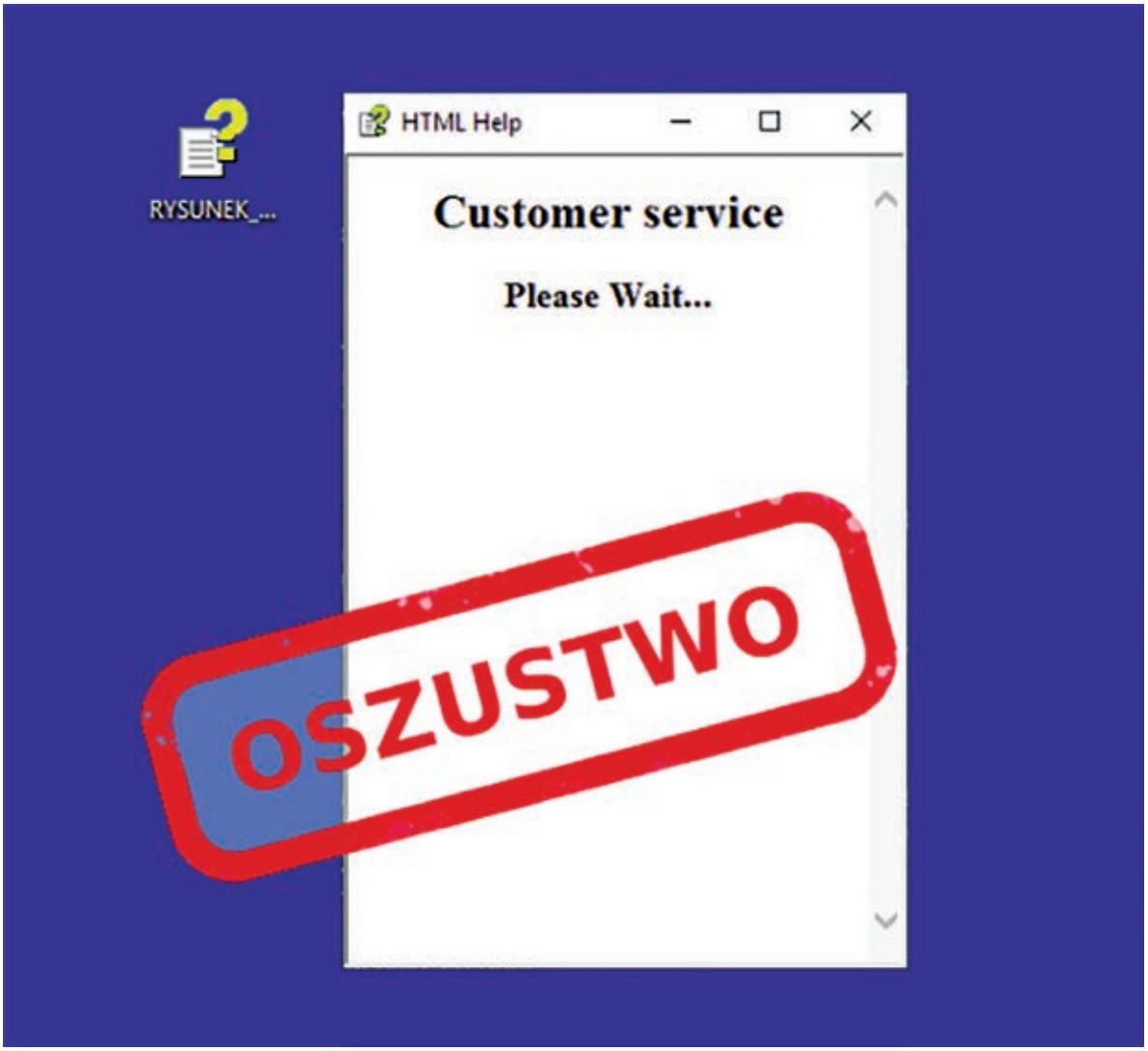
Rys. 39 Wiadomość e-mail podszywająca się pod domenę biznes.gov.pl.

Jednym z najczęściej spotykanych wariantów było szkodliwe oprogramowanie z rodziny Agent Tesla. W jednym ze sposobów dystrybucji tego szkodliwego oprogramowania cyberprzestępcy rozsyłali e-maile zawierające jedynie załączony plik IMG z rzekomym rysunkiem technicznym. W rzeczywistości było to archiwum, w którym znajdował się plik CHM.



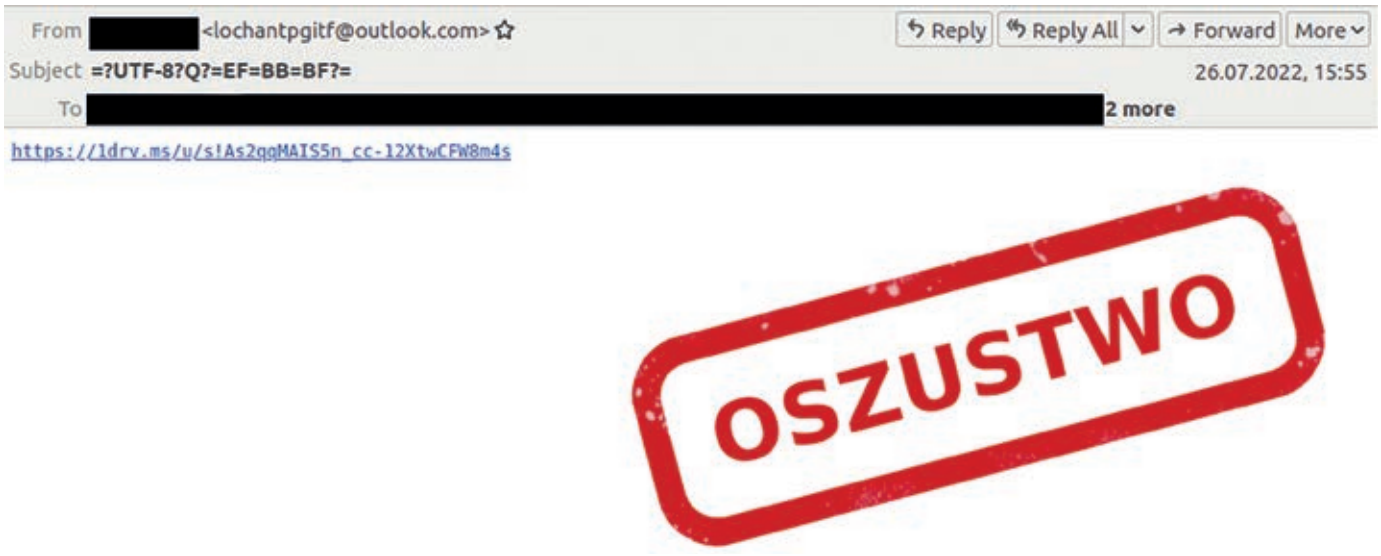
Rys. 40 Wiadomość e-mail ze złośliwym załącznikiem.

Po jego uruchomieniu wyświetlało się okienko (Rys. 41), a w tle instalowane było szkodliwe oprogramowanie z rodziny Agent Tesla. Jego główną funkcjonalnością jest kradzież wrażliwych informacji z komputera ofiary.

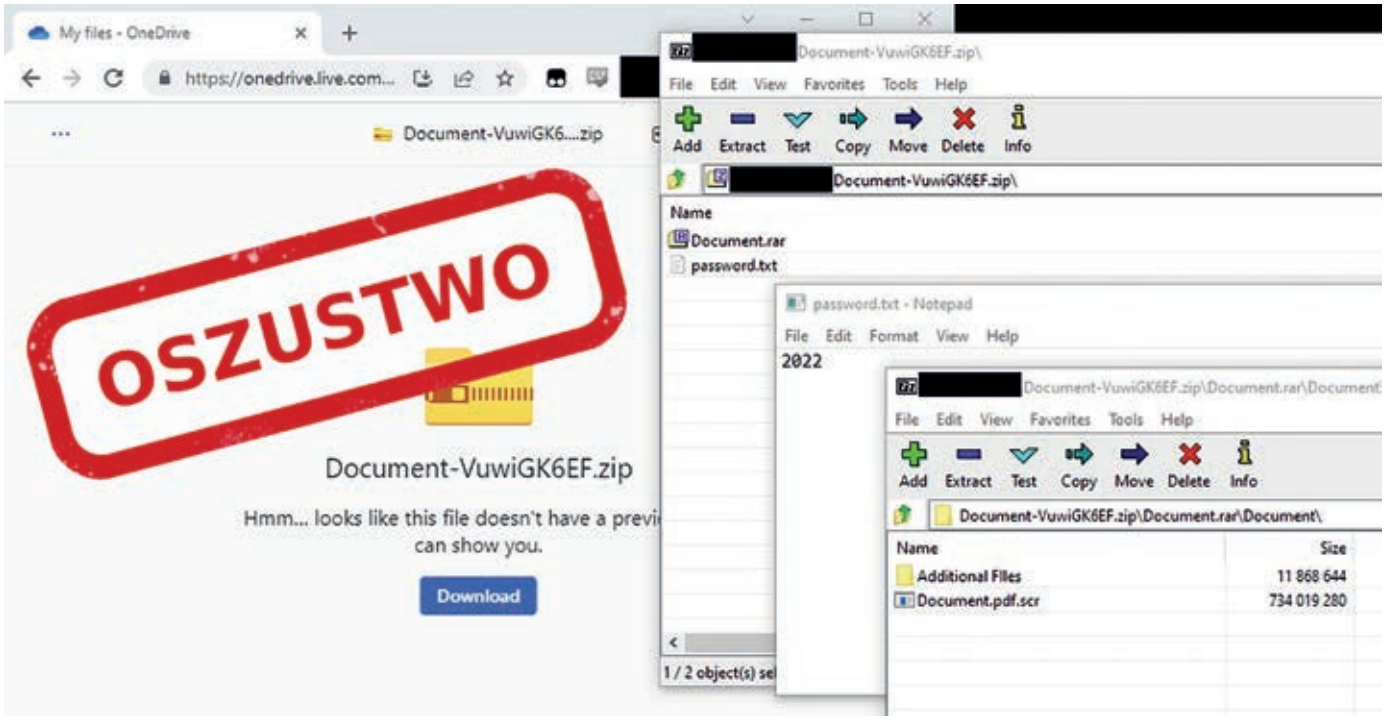


Rys. 41 Okno wyświetlane po uruchomieniu złośliwego załącznika.

Nie zawsze szkodliwe oprogramowanie znajdowało się bezpośrednio w załączniku wiadomości e-mail. W jednym z zaobserwowanych wariantów oszustwa na skrzynki pocztowe trafiały wiadomości, które w treści zawierały tylko link do platformy OneDrive, który służył do pobrania spakowanego archiwum. Znajdowało się w nim kolejne archiwum oraz plik z hasłem do jego odszyfrowania. Dopiero po rozpakowaniu drugiego archiwum, pośród rozpakowanych plików, znajdował się właściwy złośliwy plik wykonywalny .SCR. Jego uruchomienie powodowało zainstalowanie malware'u z rodziny Redline Stealer. Jej główną funkcjonalnością jest wysoce skuteczna kradzież danych uwierzytelniających zapisanych na komputerze.



Rys. 42 Wiadomość e-mail z linkiem do szkodliwego oprogramowania.



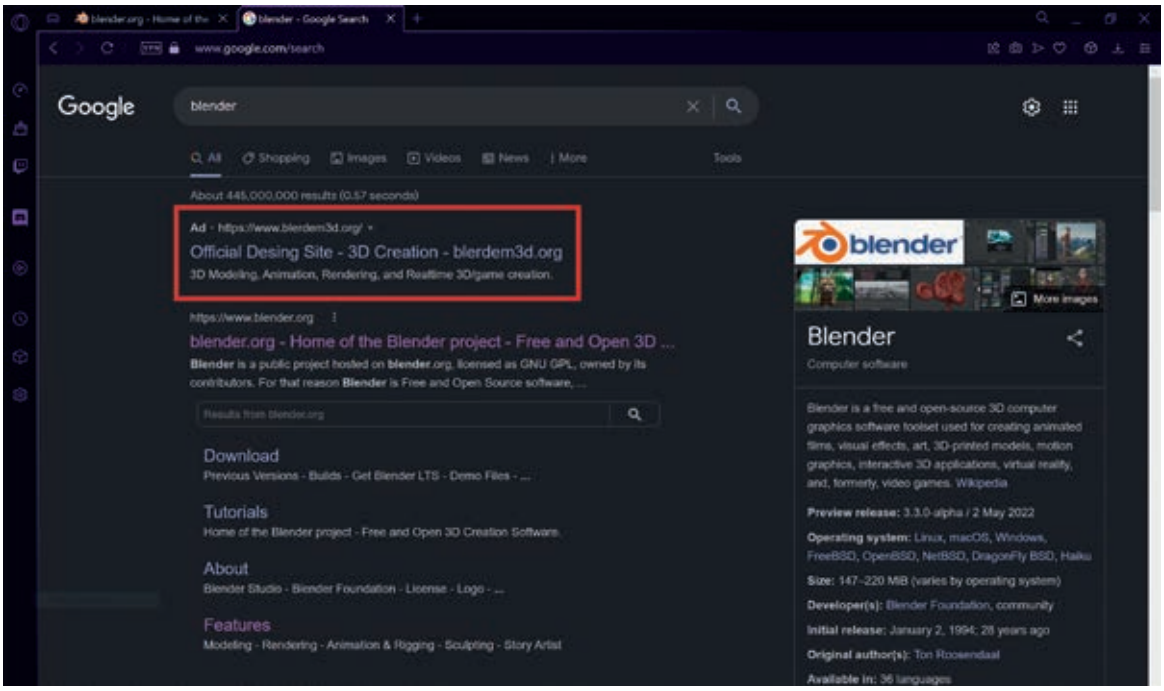
Rys. 43 Kolejne etapy ekstrakcji szkodliwego oprogramowania.

Oszuści w wiadomościach e-mail podszywali się również pod różne polskie firmy. Pod pretekstem rzekomej prośby o przekazanie oferty próbowali wielokrotnie nakłonić do otworzenia arkusza załączonego do wiadomości. W rzeczywistości załącznik o nazwie "specyfikacja.xlsx" doprowadzał do instalacji złośliwego trojana z rodziny Xloader / Formbook. Pozwalał on przestępcom na zdalny dostęp do komputera ofiary oraz na pozyskanie wrażliwych informacji, w tym zapisanych danych logowania do serwisów Internetowych.

Rys. 44 Wiadomość e-mail ze złośliwym załącznikiem .xlsx.

KAMPANIA REKLAMOWA "AD HIJACKING" ZA POŚREDNICTWEM GOOGLE ADS

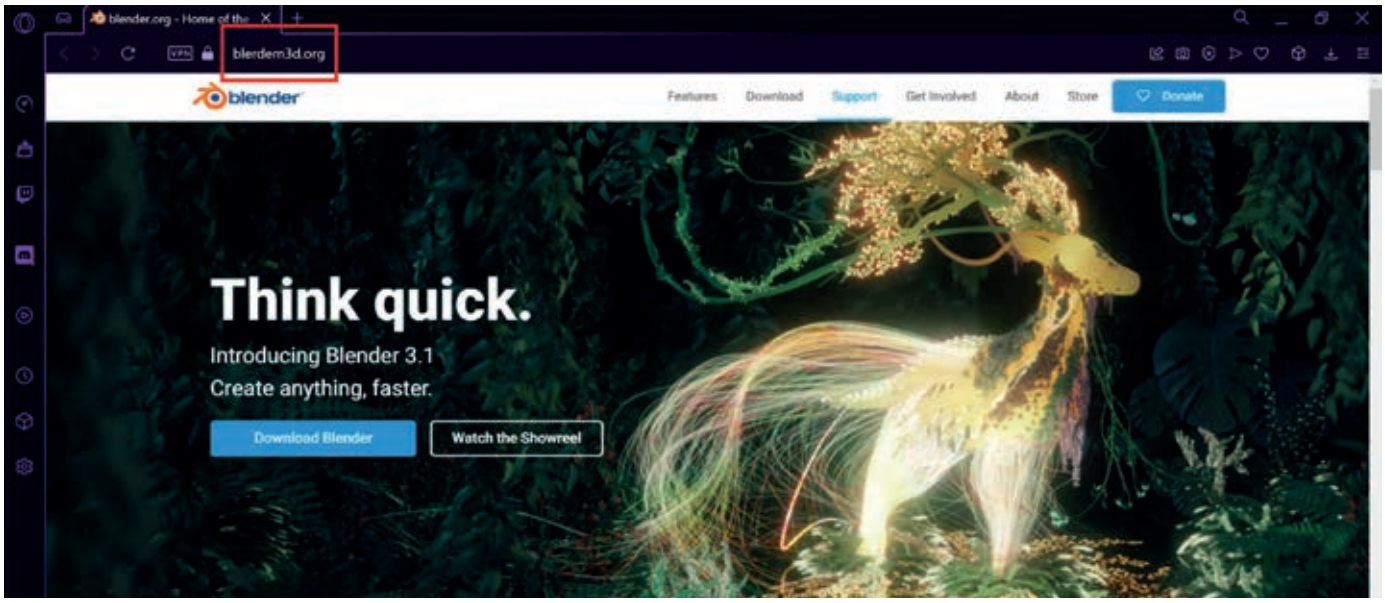
W drugiej połowie 2022 r. przestępcy zaczęli wykorzystywać system reklamowy Google Ads do wysokiego pozycjonowania w wyszukiwarce stron rozpowszechniających szkodliwe oprogramowanie. Przestępcy tworzyli strony Internetowe z nazwami domen podobnymi do nazw producentów oprogramowania. Strony te pojawiały się na pierwszych miejscach wyników wyszukiwania w Google, przez co nie wzbudzały podejrzeń.



Rys. 45 Przykładowa reklama Google Ads prowadząca do fałszywej strony.

Źródło: https://www.reddit.com/r/blender/comments/vvrxko/warning_fake_blender_website_paying_for_priority/.

Po kliknięciu w reklamę następowało przekierowanie na fałszywą stronę podszywającą się pod dostawcę wybranego oprogramowania, na której znajdował się odnośnik do pobrania pliku ze szkodliwym oprogramowaniem w formacie .exe lub .zip. Kampania była wykorzystywana do dystrybucji BatLoadera, złośliwego instalatora wykorzystywanego między innymi do infekowania komputerów ransomwarem Royal lub do infekcji oprogramowaniem z rodziny IcedID, które wykorzystywane było do dostarczania kolejnych niepożądanych programów lub skryptów, takich jak np. Cobalt Strike. Umożliwiało to cyberprzestępcom uzyskanie pełnego dostępu do systemu użytkownika, dzięki czemu mogli pozyskać dane uwierzytelniające do serwisów, z których korzystała ofiara.



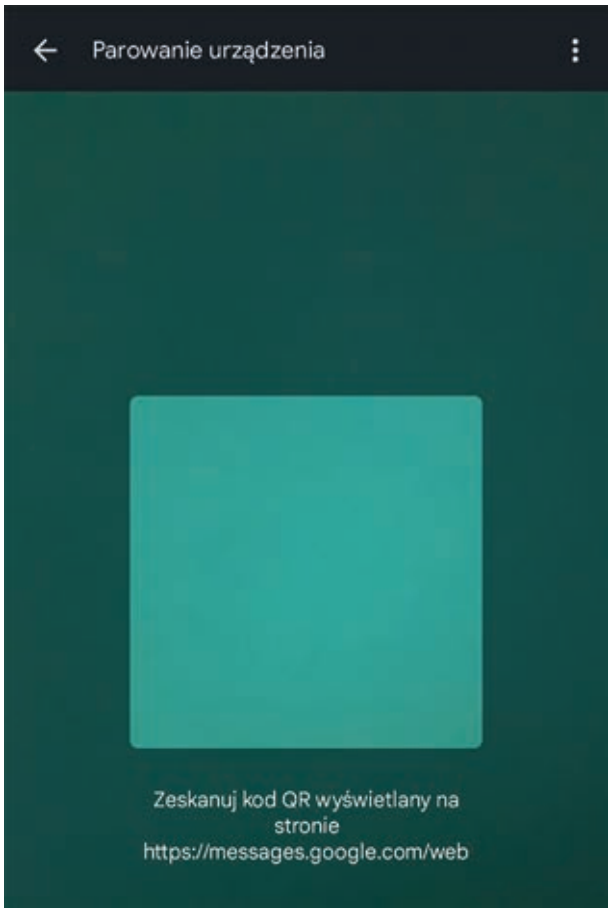
Rys. 46 Strona ze szkodliwym oprogramowaniem podszywająca się pod producenta oprogramowania Blender.

OSZUSTWA Z WYKORZYSTANIEM KODÓW QR

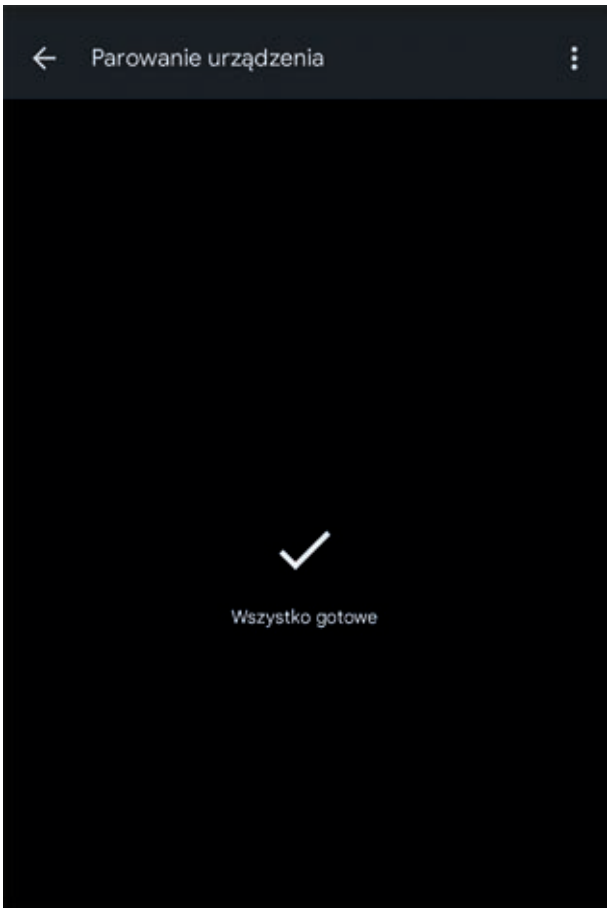
Jednym z celów ataków w 2022 r. stały się dzieci i młodzież korzystające z otwartych komunikatorów jak np. Discord, na których oszuści zbierali informacje, a następnie tworzyli profil ofiary, sprawdzając jej zainteresowania czy listę znajomych. Następnie przestępcy wykorzystując zdobytą wiedzę podejmowali próbę kontaktu, podając się za dalszego znajomego potrzebującego pomocy lub oferując płatne przedmioty w grach w zamian za wyświadczenie przysługi.

Już po nawiązaniu kontaktu oszuści nakłaniali ofiarę do zainstalowania i skonfigurowania aplikacji Wiadomości ze Sklepu Google Play. Kiedy potencjalna ofiara zainstalowała aplikację, otrzymywała od przestępców kod QR, który należało zeskanować. Kod służył do parowania urządzenia z aplikacją, do którego nie były potrzebne żadne dane uwierzytelniające. Ponadto w trakcie procesu konfigurowania ofiara nie była powiadamiana o następstwach czy też ostrzegana przed potencjalnymi zagrożeniami.

Rys. 47 Menu parowania urządzenia w aplikacji Wiadomości.



Rys. 48 Ekran parowania urządzenia.

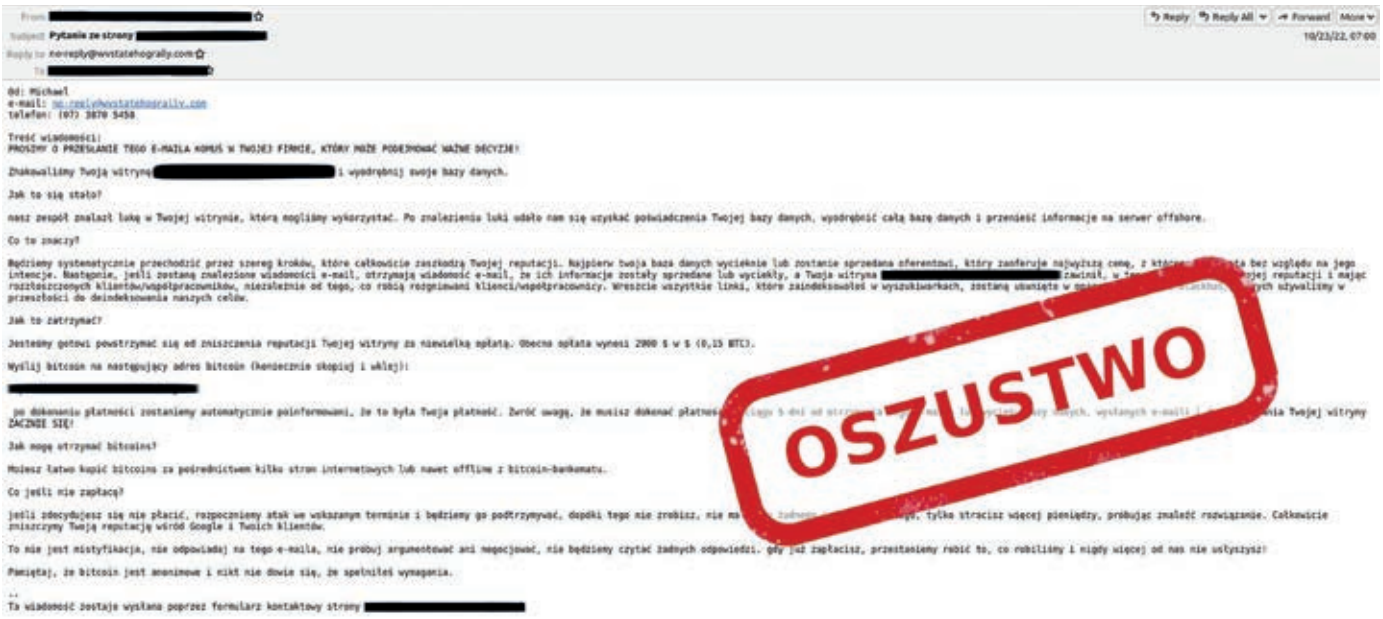


Rys. 49 Komunikat wyświetlany po pomyślnym sparowaniu urządzenia

Po zeskanowaniu kodu przez ofiarę, oszust uzyskiwał dostęp do zapisanych i przychodzących wiadomości, a także kontaktów oraz miał możliwość wysyłania wiadomości. Takie uprawnienia były wykorzystywane przez przestępców do obciążania rachunku ofiary poprzez wysyłkę wiadomości typu SMS Premium oraz do szantażu, dzięki informacjom zawartym w wiadomościach i liście kontaktów. Warto również zwrócić uwagę, że uzyskane dostępy mogą w przyszłości posłużyć do przejęcia drugiego składnika uwierzytelniania z wiadomości SMS, w przypadku jego stosowania przez ofiarę oraz do podjęcia prób oszustwa wobec znajomych ofiary z wykorzystaniem jej urządzenia.

SPERSONALIZOWANE SZANTAŻE NA WŁAŚCICIELI STRON INTERNETOWYCH

Przestępcy coraz częściej personalizują swoje kampanie pod potencjalne ofiary, czym chcą wzbudzić w nich większe zaniepokojenie, ale także urealistycznić atak. W jednej z odsłon kampanii w ubiegłym roku przestępcy kierowali swoje wiadomości do właścicieli stron Internetowych, w których zamieszczali informację o rzekomym włamaniu na stronę Internetową i wykradzeniu bazy danych, a także żądali okupu w postaci przelewu określonej sumy Bitcoinów na portfel kryptowalutowy. Dla uwiarygodnienia próby wyłudzenia środków pieniężnych zamieszczane było również hasło potencjalnej ofiary. W rzeczywistości takie hasło pochodziło z wycieków danych, natomiast wszelkie inne informacje przestępcy uzyskiwali poprzez web scrapping, czyli automatyczne zbieranie danych z publicznych serwisów.



Rys. 50 Przykładowy e-mail ze spersonalizowanym szantażem.

TROJAN BANKOWY HYDRA

W poprzednim roku przestępcy wykorzystywali wiadomości mailowe również jako wektor ataku na użytkowników urządzeń mobilnych. Potencjalne ofiary otrzymywały wiadomość z domeny zbliżonej do domeny banku ING, w treści której oszuści informowali o rzekomym braku instalacji aplikacji zabezpieczającej na telefonie. Miało to być powodem zablokowania konta, które zostałoby odblokowane dopiero po zrealizowaniu wskazanych działań.

Wiadomość zawierała link, który przenosił ofiarę na stronę podszywającą się pod bank. Przestępcy w pierwszej kolejności zachęcali ofiarę do wpisania danych uwierzytelniających do bankowości Internetowej.

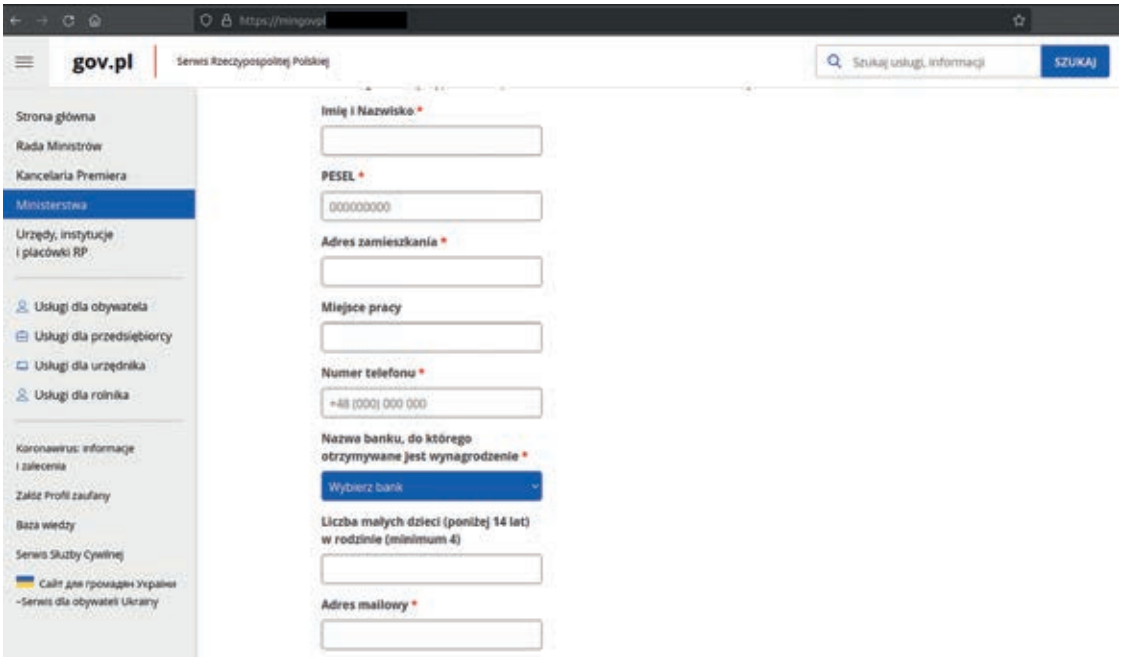
W dalszych krokach potencjalna ofiara, jeśli korzystała z urządzenia mobilnego, była proszona o zainstalowanie aplikacji, natomiast w przypadku kiedy korzystała z komputera - o zeskanowanie telefonem wyświetlonego kodu QR. Po pobraniu pliku, którym był trojan bankowy Hydra, użytkownik musiał nadać specjalne uprawnienia aplikacji, dzięki czemu mogła ona zainstalować złośliwe oprogramowanie, a następnie nawiązać komunikację z serwerem Command & Control. Atak miał na celu zbieranie danych uwierzytelniających wpisywanych przez ofiarę w wielu różnych aplikacjach mobilnych, a następnie przesłanie ich na serwer przestępców.

WYKORZYSTANIE WIZERUNKU MINISTERSTWA FINANSÓW

W 2022 r. przestępcy wykorzystywali wielokrotnie wizerunek różnych instytucji państwowych m.in. Ministerstwa Finansów. W jednym z wariantów oszuści na fałszywej stronie Internetowej informowali o rzekomym rozporządzeniu, według którego obywatelom RP, ze względu na rosnące bezrobocie i migracje związane z rosyjską agresją, miała przysługiwać jednorazowa wypłata świadczenia finansowego.

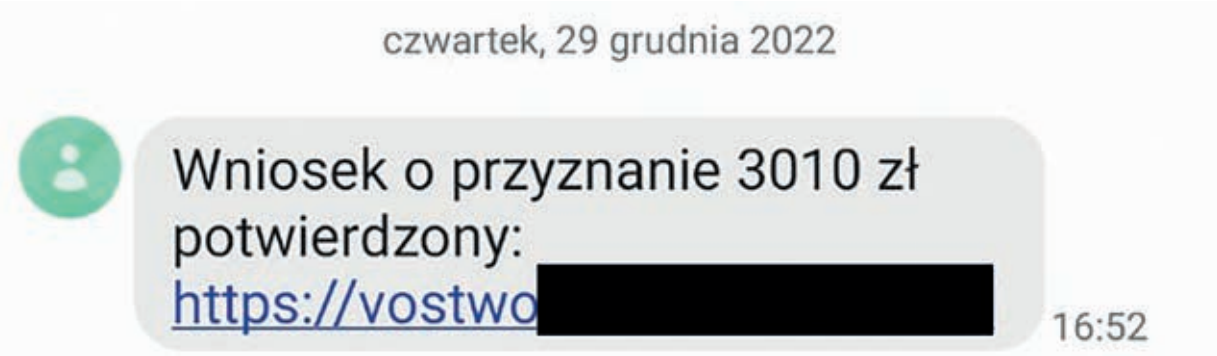
Rys. 51 Strona wykorzystująca wizerunek Ministerstwa Finansów.

Na stronie zamieszczone było fałszywe rozporządzenie, a poniżej znajdował się formularz do przesłania szczegółowych danych osobowych oraz kontaktowych i informacji o banku potencjalnej ofiary. Po przesłaniu wypełnionego formularza wyświetlany był komunikat o jego pomyślnym uzupełnieniu, a także prośba o oczekiwanie na dalsze instrukcje, które miały zostać dostarczone w wiadomości e-mail lub SMS.



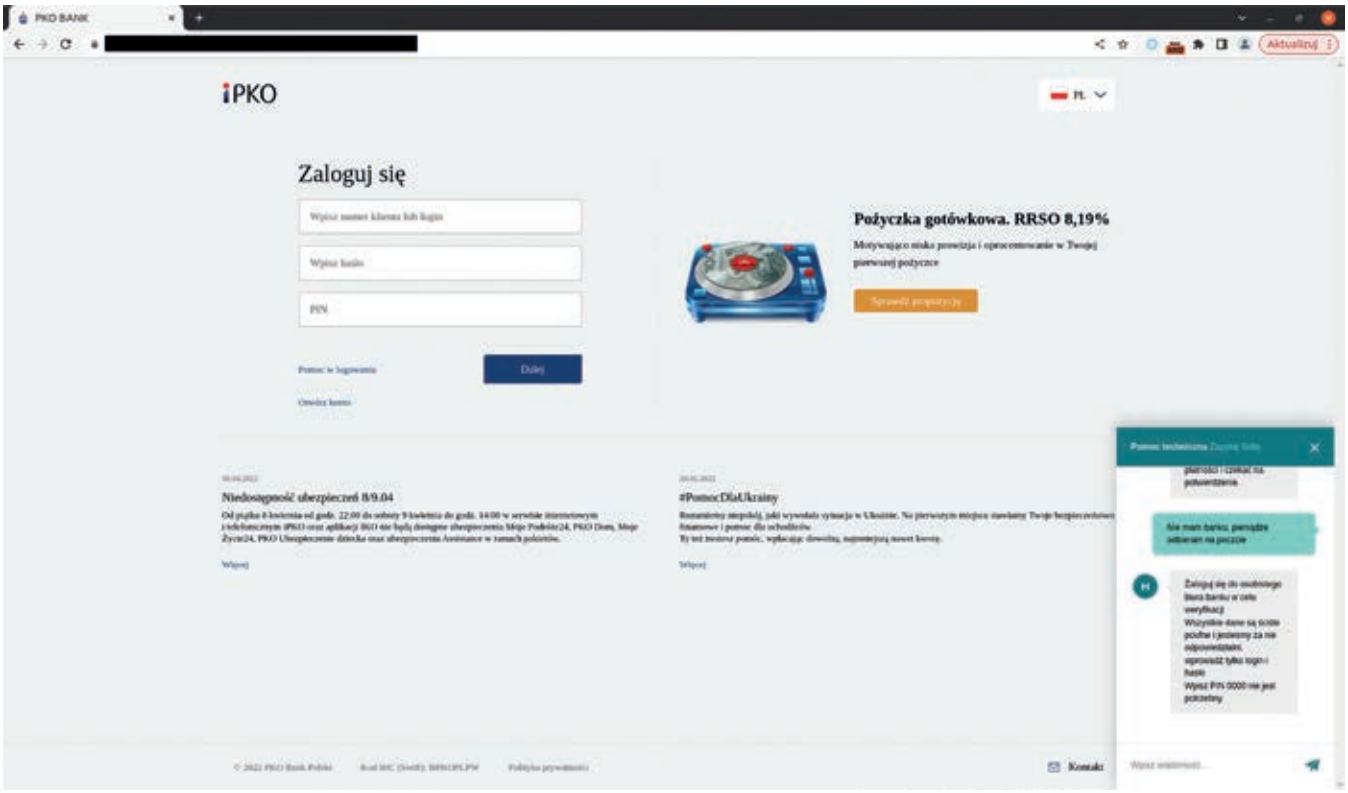
Rys. 52 Fałszywy formularz wyłudzający dane osobowe oraz kontaktowe.

W kolejnym etapie poszkodowany otrzymywał wiadomość SMS. Przestępcy, wykorzystując bramki SMS, podszywali się pod nadawcę wiadomości, którym rzekomo był bank wybrany podczas uzupełniania formularza. W treści wiadomości oszuści umieszczali informację o przyznanej kwocie świadczenia oraz link do strony podszywającej pod bank potencjalnej ofiary.



Rys. 53 SMS dotyczący przyznania rzekomej kwoty pieniędzy.

Po kliknięciu w link użytkownik przenoszony był do fałszywego panelu logowania, w którym przestępcy próbowali pozyskać informacje o danych uwierzytelniających i kodzie PIN ofiary. W przypadku podania prawidłowych danych poszkodowany był przenoszony na stronę, na której proszony był o podanie kodu autoryzacyjnego, który ofiara otrzymywała ze swojego banku w wiadomości SMS. Udostępnienie przez ofiarę danych uwierzytelniających oraz kodu autoryzacyjnego umożliwiało przestępcom uzyskanie pełnego dostępu do konta bankowego, w wyniku czego poszkodowany mógł stracić wszystkie zgromadzone na koncie środki.

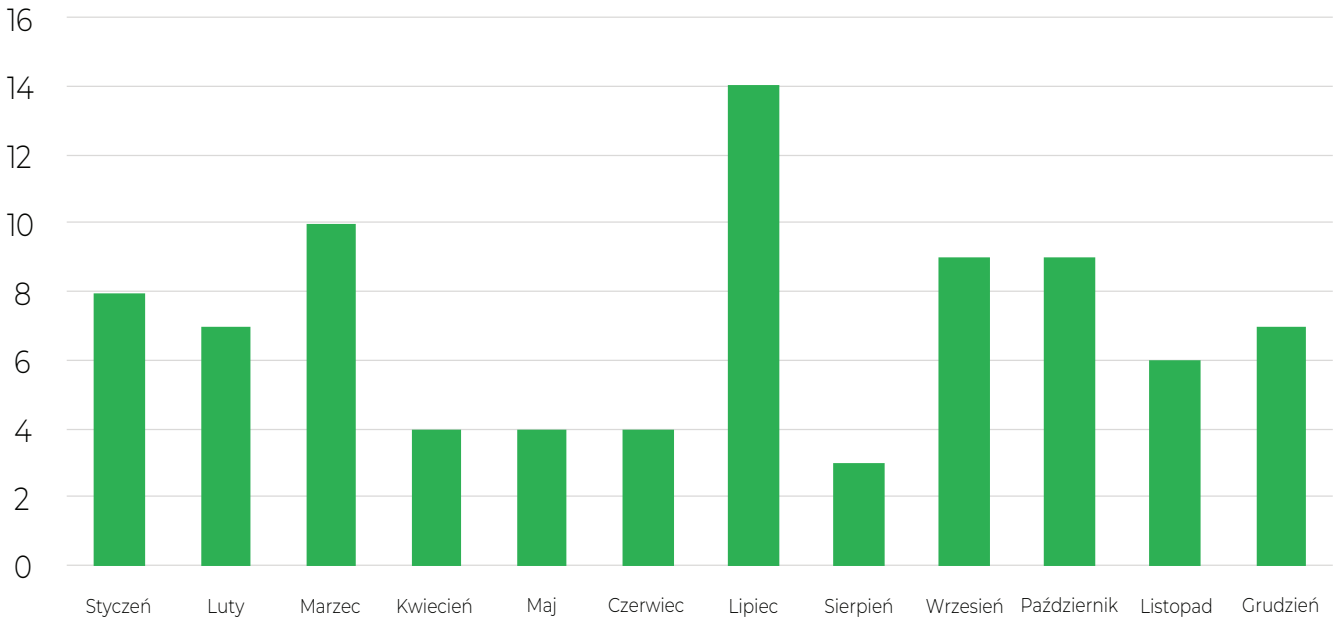


Rys. 54 Fałszywy panel logowania do banku PKO BP.

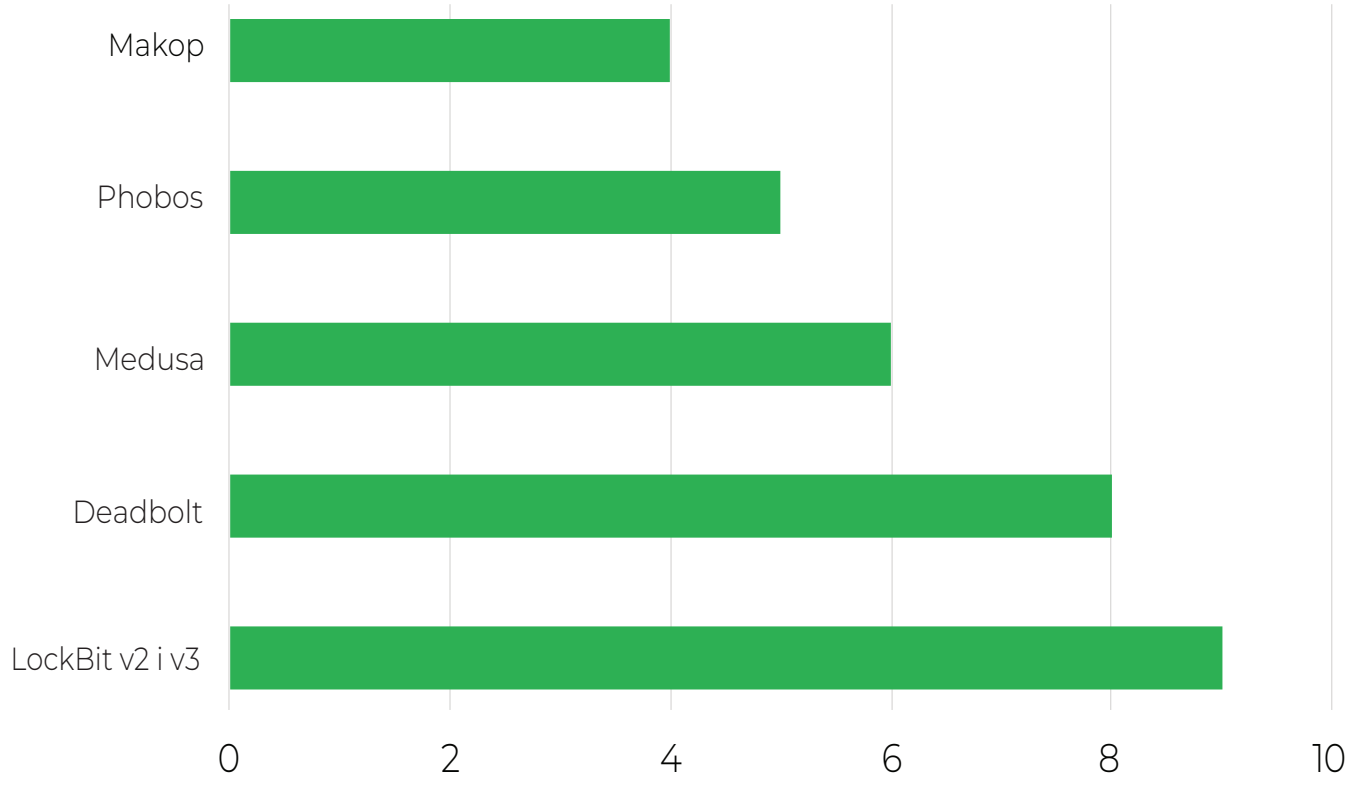
RANSOMWARE

W ubiegłorocznym raporcie za 2021 r. pisaliśmy, że wówczas jednym z największych zagrożeń dla cyberbezpieczeństwa było ransomware, czyli szkodliwe oprogramowanie, które wymusza zapłacenie okupu poprzez akcję, np. zaszyfrowania danych. Również i w 2022 r. ataki przy użyciu tego typu oprogramowania były jednymi z największych wyzwań dla naszego zespołu oraz prawdopodobnie większości zespołów zajmujących się bezpieczeństwem na poziomie krajowym i europejskim.

W 2022 r. CERT Polska zarejestrował 85 incydentów związanych z tym zagrożeniem. Jest to około 20 proc. mniej niż w roku 2021, w którym obsłużyliśmy 124 incydenty. Były one często jednak incydentami skierowanymi na większe firmy prywatne, instytucje państwowe czy podmioty w sektorze zdrowia. W przypadku ataków na tego typu podmioty wpływ na obywateli jest większy niż w przypadku ataku na komputer osoby prywatnej. W 2022 r. najwięcej incydentów, bo aż 56, zgłosiły firmy oraz osoby prywatne, a następnie instytucje publiczne, które poinformowały o w sumie 24 incydentach. Wśród nich znalazły się jednostki samorządu terytorialnego, takie jak urzędy gminy i miasta, instytucje systemu opieki zdrowotnej czy uczelnie wyższe. Najwięcej incydentów związanych z działaniem oprogramowania ransomware zgłoszono do zespołu CERT Polska w lipcu oraz marcu, było do odpowiednio 14 i 10 incydentów.



Wykres 1. Liczba incydentów ransomware w podziale na miesiące.

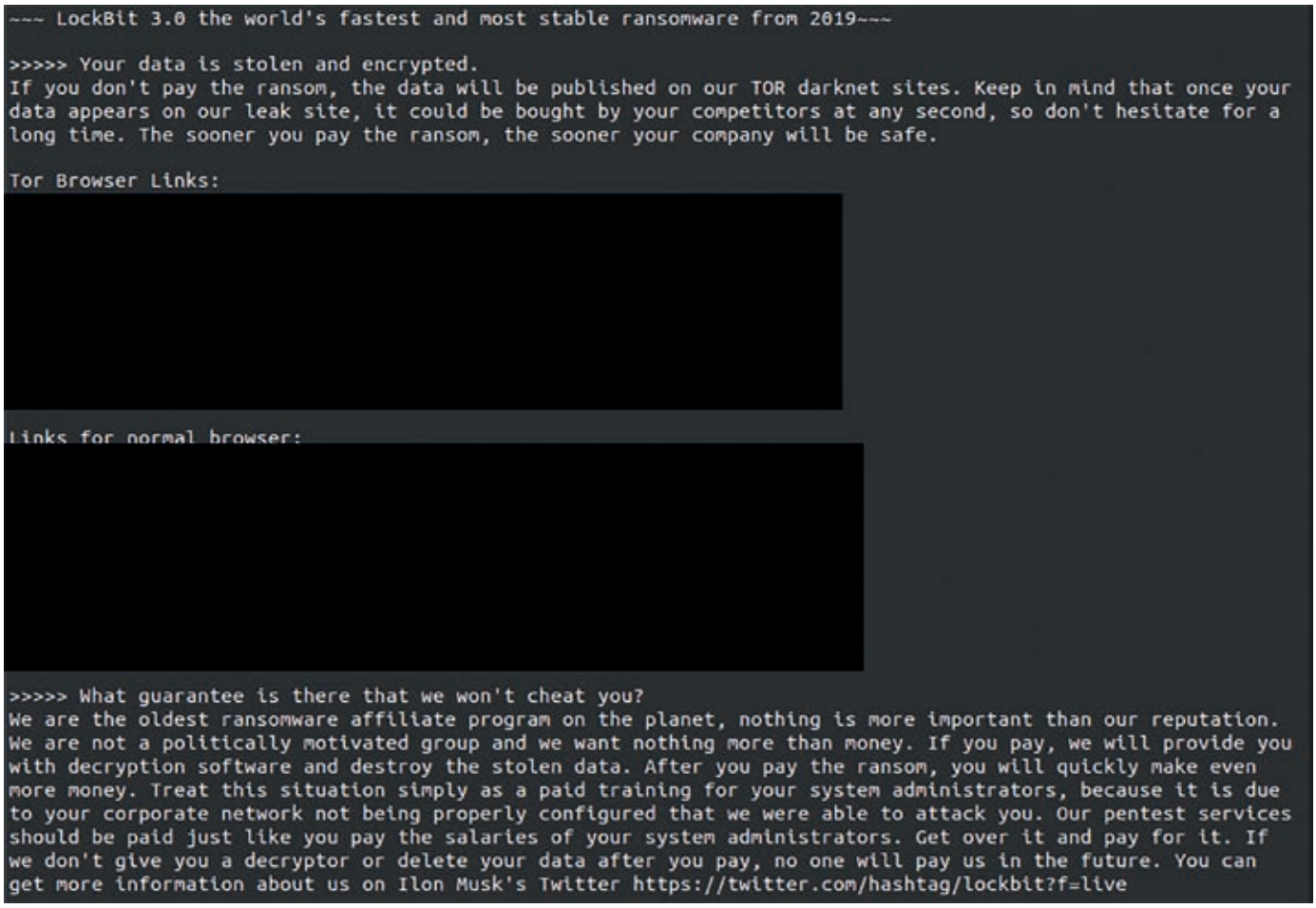


Wykres 2. 5 najpopularniejszych rodzin ransomware zaobserwowanych w Polsce.

RODZINY ZAOBSERWOWANE PRZEZ CERT POLSKA W 2022 ROKU

LOCKBIT

Jednym z częściej zarejestrowanych przez zespół CSIRT NASK rodzajów ransomware był ransomware LockBit. Oprogramowanie LockBit w wersji 1.0 zostało pierwszy raz zaobserwowane w 2019 r. [1], w 2022 r. została zidentyfikowana wersja 3.0. Oprogramowanie LockBit działa w trybie Ransomware as a Service (RaaS) i do tej pory ataki z wykorzystaniem tego oprogramowania zostały wykryte, m.in. w krajach Unii Europejskiej, USA, Rosji oraz Chin. Celami atakujących zazwyczaj są małe i średnie przedsiębiorstwa, jednak oprogramowanie LockBit zostało wykorzystane przy atakach na międzynarodowe firmy takie jak Continental [2], Entrust [3] oraz Thales [4]. W Polsce ten rodzaj ransomware został zaobserwowany m.in. w incydencie w Szpitalu Matki Polki w Łodzi [5].



Rys. 55 Zdjęcie ze zrzutem ekranu pliku z żądaniem okupu, który zostaje wygenerowany po zaszyfrowaniu danych.

PRESTIGE

Raport zespołu MSTC (Microsoft Threat Intelligence Center) opisujący ransomware Prestige odbił się szerokim echem w środowiskach związanych z cyberbezpieczeństwem w Polsce jak i w Ukrainie [6]. Prestige zaobserwowano w atakach na instytucje związane z transportem i infrastrukturą logistyczną we wspomnianych krajach. Ransomware został powiązany z rosyjską grupą IRIDIUM, łączoną z inną rosyjską grupą – Sandworm. Niezależnie od powiązań grupa ta była obserwowana w atakach na infrastrukturę teleinformatyczną Ukrainy od początku wojny rosyjsko-ukraińskiej. Przy infekcji wykorzystywane jest otwartoźrodłowe oprogramowanie Impacket [7]. Po infekcji oprogramowanie wyszukuje we wszystkich katalogach, oprócz C:\Windows\ oraz C:\ProgramData\Microsoft\, plików o wybranych rozszerzeniach, a następnie szyfruje je. Po etapie szyfrowania dodawane jest rozszerzenie .enc do każdego zaszyfrowanego pliku oraz notatka README.txt z żądaniem okupu. Niezależnie od wersji ransomware do szyfrowania danych wykorzystywany jest algorytm AES. Pierwszy raz oprogramowanie Prestige zostało zaobserwowane 11 października 2022 r. jednak specjaliści z MSTC wskazują, że ten rodzaj ransomware mógł być wykorzystywany już od marca 2022 r.

BLACKCAT

Raport grupy Sophos [8] dotyczący obrazu cyberbezpieczeństwa na świecie wskazał oprogramowanie BlackCat jako drugie najczęściej wykorzystywane w 2022 r. Zostało ono wykryte przy ok. 12 proc. wszystkich zaobserwowanych przez grupę atakach. W raporcie wydanym przez FBI, zawierającym IoC ransomware BlackCat [9], wskazano, że wykorzystywane są zdobyte wcześniej zabezpieczone dane logowania do maszyn z systemem Windows, żeby później eskalować dostępy do kont administratorów oraz użytkowników potencjalnego Active Directory środowiska ofiary. W późniejszych etapach wykorzystywane jest oprogramowanie

CobaltStrike oraz narzędzia Microsoft, takie jakie Microsoft Sysinternals. Oprogramowanie BlackCat oprócz szyfrowania danych również je wykrada. Narażone są nie tylko dane lokalne, ale również te znajdujące się w chmurach podłączonych do środowiska ofiary. Ransomware BlackCat został powiązany przez FBI z dwoma grupami – DarkSide oraz BlackMatter i został on pierwszy raz zaobserwowany pod koniec 2021 r.

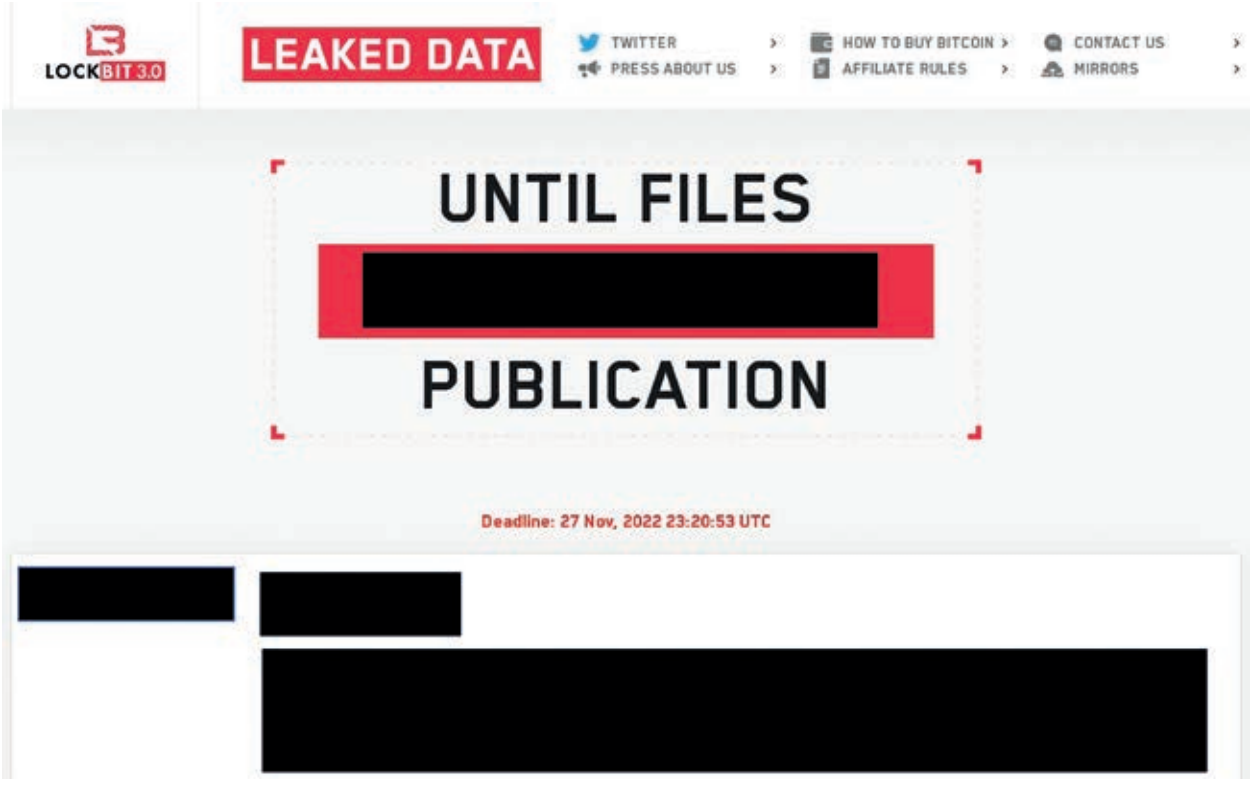
ZAOBSERWOWANE TRENDY

SZKODLIWE DZIAŁANIA AS A SERVICE

Specjaliści z grupy Sophos w swoim raporcie [8] wskazali również nowy trend wykształcający się wśród aktorów. Tym trendem jest udostępnianie różnego rodzaju usług w formie aaS (as a Service). Specjaliści w raporcie wyróżnili następujące usługi: dostępu - udostępnianie zestawów danych uwierzytelniających do systemów teleinformatycznych, dystrybucji malware, phishingu, technik OPSEC, szyfrowania, oszustw, wyłudzeń telefonicznych oraz skanowania. Jest to trend, który rozszerza znany już wcześniej tryb dystrybucji Ransomware as a Service. Przyczynami tego trendu, wskazywanymi przez specjalistów, jest dynamiczny rozwój natury działalności cyberprzestępczej oraz kwestia finansowania grup cyberprzestępczych. Cyberprzestępcy coraz częściej zostają wykorzystywani przez inne podmioty do wywarcia presji na swoich ofiarach, co pokazała trwająca wojna ukraińsko-rosyjska.

WZROST POPULARNOŚCI KRADZIEŻY DANYCH

W trakcie analizy zgłoszonych incydentów zespół CERT Polska zauważył, że przestępcy coraz częściej w trakcie ataku i szyfrowania danych wysyłają je również na swoje serwery. Ma to na celu zwiększenie szansy na zapłacenie okupu przez zaatakowaną firmę. Informacja o kradzieży danych jest często publikowana na stronie przestępców hostowanej w sieci TOR wraz z planowanym terminem opublikowania danych. Dochodzi nawet do sytuacji, że operatorzy szkodliwego oprogramowania są w stanie przełożyć termin publikacji danych, jeśli firma deklaruje chęć zapłacenia okupu. Oczywiście należy zawsze pamiętać, że cała transakcja to po prostu przekazanie środków finansowych grupie przestępczej, która nadal może zostawić sobie kopię danych, a dodatkowo zyskać w ten sposób motywację do prowadzenia kolejnych ataków.



Rys. 56 Zrzut ekranu ze strony grupy LockBit 3.0.

PORADNIK DOTYCZĄCY RANSOMWARE

Chronienie swojej firmy przed zaszyfrowaniem danych oraz coraz częściej spotykaną eksfiltracją ich poza infrastrukturę przedsiębiorstwa robi się z roku na rok coraz trudniejszym wyzwaniem . Wychodząc naprzeciw oczekiwaniom administratorów systemów zespół CERT Polska stworzył poradnik związany z zabezpieczaniem swojej infrastruktury przed atakiem, jak i po udanym ataku ransomware. Można się z nim zapoznać pod linkiem: https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf

Materiały dotyczące ataków tego rodzaju:

1. https://www.kaspersky.com/resource-center/threats/lockbit-ransomware
2. https://heimdalsecurity.com/blog/continental--lockbit-ransomware/
3. https://heimdalsecurity.com/blog/entrust-allegedly-hit-with-lockbit-ransomware/
4. https://heimdalsecurity.com/blog/thales-global-tech-company-data-released-by-lockbit--ransomware-gang/
5. https://sekurak.pl/szpital-matki-polki-w-lodzi--zainfekowany-ransomware-informuja-rowniez-o-mozliwym-wycieku/
6. https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware--impacts-organizations-in-ukraine-and-poland/ oraz https://github.com/fortra/impacket
7. https://assets.sophos.com/X24WTUEQ/at/b5n-9ntjqmbkb8fg5rn25g4fc/sophos-2023-threat--report.pdf
8. https://www.ic3.gov/Media/News/2022/220420.pdf
9. https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackcat

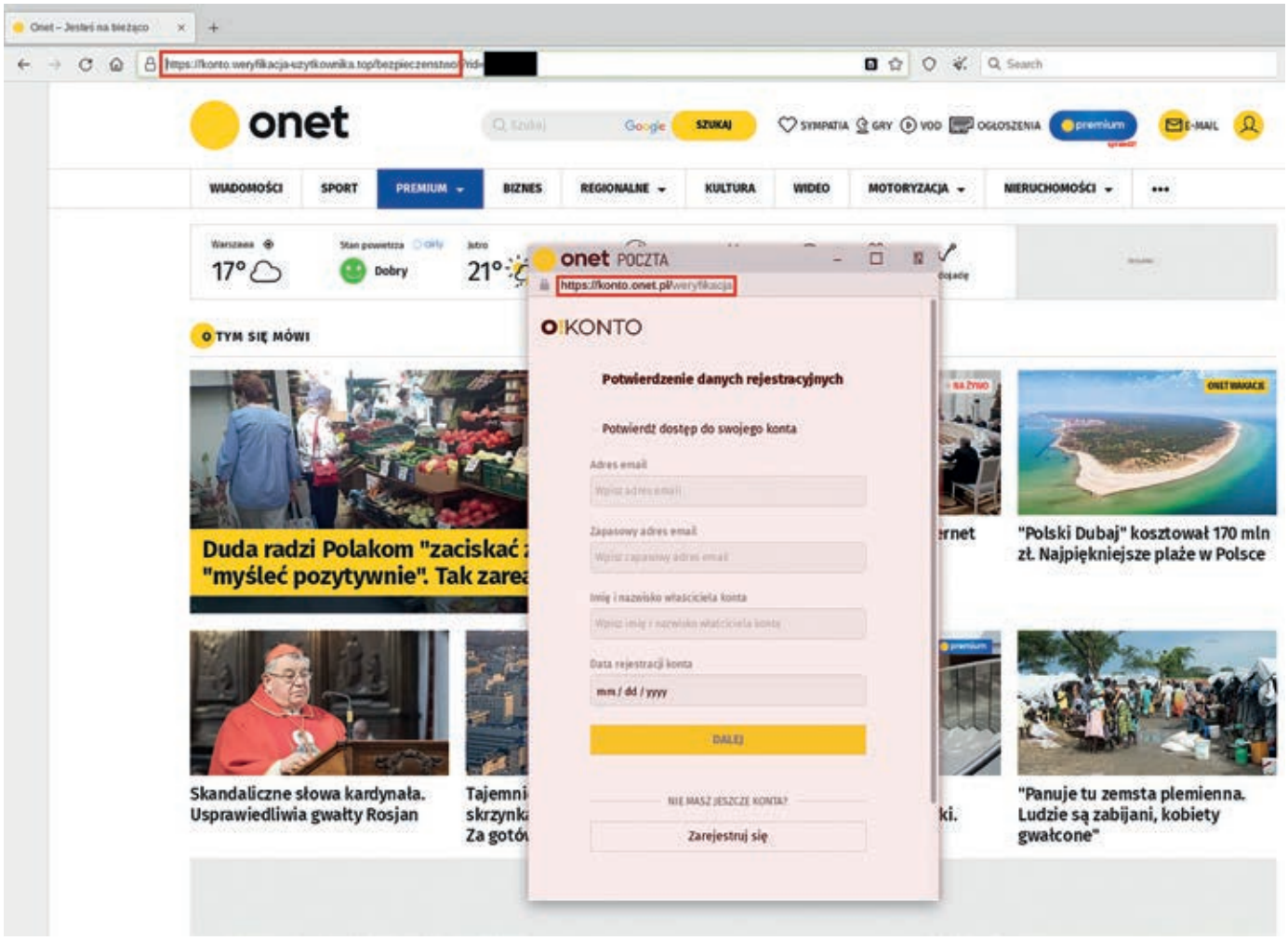
DZIAŁALNOŚĆ GRUPY UNC1151/GHOSTWRITER

Od dwóch lat obserwujemy kampanie phishingowe w wykonaniu grupy UNC1151/Ghostwriter na skrzynki w domenach polskich dostawców poczty (Interia, WP, Onet). Ataki te są ukierunkowane na osoby zajmujące eksponowane stanowiska lub mogące posiadać wiedzę na temat polityki prowadzonej względem Rosji i Białorusi.

Grupa UNC1151/Ghostwriter wykorzystuje głównie fałszywe maile informujące o rzekomym naruszeniu warunków użytkowania poczty i konieczności weryfikacji danych osobowych. Przykład takiego maila pokazano na Rys. 57

Rys. 57 Fałszywy e-mail phishingowy wysłany przez grupę UNC1151/Ghostwriter.

W atakach na przełomie roku 2021 i 2022 użytkownik był przekierowywany z fałszywego maila bezpośrednio na stronę udającą panel logowania. Natomiast w marcu 2022 r. zaczęto korzystać z techniki Browser-in-the-Browser, co opisaliśmy w naszym artykule: https://cert.pl/posts/2022/07/techniki-unc1151/. Technika ta może być wyjątkowo niebezpieczna i łatwa do przeoczenia. Polega ona na wyświetleniu w ramach odwiedzanej strony pozornie nowego okna przeglądarki, zawierającego fałszywy panel logowania. Okno to, będące elementem strony, jest na tyle dobrze wykonane, że ofiara może mieć trudności z odróżnieniem spreparowanego od prawdziwego nowego okna aplikacji. Przykład phishingu z wykorzystaniem tej techniki pokazano na rys 58.



Rys. 58 Przykład phishingu grupy UNC1151/Ghostwriter z wykorzystaniem techniki Browser-in-the-Browser.

Do października 2022 r. w atakach wykorzystywano dedykowane, nowo zakupione domeny, przygotowywane pod każdą kampanię phishingową. Użyto m.in. takie domeny jak: *poczta.walidacja-uzytkownika[.]space, usluga.kontrola-poczty[.]top, czy konto.weryfikacja-uzytkownika[.]top*. Domeny wskazywały na serwer ze skonfigurowanym narzędziem GoPhish. Warto zauważyć, że wymagało to od atakujących zakupienia zarówno serwera jak i domeny.

W październiku został zmieniony zarówno sposób wysyłki jak i hostowania phishingu. Od tego momentu grupa nie utrzymuje żadnej własnej infrastruktury dedykowanej dla kampanii. Maile są wysyłane bezpośrednio ze skrzynek założonych na serwisach, na które prowadzony jest atak, np. przy ataku na użytkowników serwisu Interia została wykorzystana skrzynka "*identyfikacja_uzytkownika@interia.pl*". Ataki są prowadzone z użyciem łańcucha przejętych stron, a poświadczenia wysyłane na

darmowe serwisy logujące zapytania HTTP. Przykładowy schemat wykorzystania przejętych stron wygląda następująco:

1. Link w mailu kieruje do pliku php na pierwszej przejętej stronie, np. https://przejęta_strona_1.pl/email.php.
2. Skrypt automatycznie przekierowuje na drgą przejętą stronę, np. https://przejęta_strona_1.pl/okonto.html. Znajduje się na niej phishing zrealizowany metodą Browser-in-the-Browser.
3. Druga strona posiada iframe, w którym ładowana jest zawartość z trzeciej przejętej strony udającej nowe okno przeglądarki.
4. W przypadku podania danych logowania są one wysyłane na darmowy serwis oferujący logowanie zapytań POST, który monitorują atakujący.

Od momentu rozpoczęcia użycia tej techniki zaobserwowaliśmy wykorzystanie dziesiątek przejętych polskich i zagranicznych stron. Prawdopodobnie jest ona stosowana w celu obejścia prób wykrycia maili phishingowych przez dostawców poczty. Wykorzystanie przejętej domeny z długą historią oraz łańcuch przekierowań utrudnia automatyczne rozpoznanie zawartości.

To co również zmieniło się w 2022 r. względem 2021 to dobór celów ataków. Obecnie rzadziej są to osoby bezpośrednio związane z polityką, a częściej takie, które mogą posiadać istotną wiedzę, choć nie jest to takie oczywiste. Przykładowo: tłumacze przysięgli języka rosyjskiego, prawnicy, księża prawosławni, emerytowani wojskowi, czy wykładowcy.

WYCIEKI DANYCH

Wycieki danych są problemem, z którym na przestrzeni ostatnich lat zetknęła się większość polskich użytkowników Internetu. Wraz ze wzrostem liczby podmiotów przetwarzających różnego rodzaju dane, w tym dane wrażliwe, rośnie również liczba chętnych, by te dane wykraść i wykorzystać.

JAK DOCHODZI DO WYCIEKÓW?

NIEZAMIERZONE DZIAŁANIE OSOBY PRZETWARZAJĄCEJ DANE

Często powodem wycieków jest brak wystarczającej uwagi i ostrożności w ich przetwarzaniu. Jednym z przykładów jest przytaczane wielokrotnie niewłaściwe korzystanie z funkcji "do wiadomości" (DW, ang. CC) przy wysyłaniu e-maila. Jeżeli nie chcemy, by każdy, kto otrzymał daną wiadomość poznał pozostałych adresatów, powinniśmy skorzystać z opcji "ukryte do wiadomości" (UDW, ang. BCC). Pamiętajmy również o szyfrowaniu nośników danych. Utrata laptopa, pendrive czy dysku będzie zdecydowanie mniej bolesna, jeżeli będziemy mieli pewność, że znalazca nie uzyska dostępu do jego zawartości. Obecnie stosowane urządzenia mają zazwyczaj wbudowane, proste w użyciu mechanizmy szyfrowania. Nie zapominajmy, że źródłem wycieku nie muszą być wcale dokumenty w formie elektronicznej, mogą być to też np. notatki i dokumenty w formie papierowej[10].

BŁĘDY W KONFIGURACJI SYSTEMÓW

Szerokiej skali wyciek dotknął Szkołę Główną Handlową, gdzie na skutek błędu programistycznego udostępniono publicznie dane osobowe części studentów[11]. Błędne zabezpieczenie interfejsu API w T-Mobile pozwoliło atakującemu w okresie od końca listopada do końca roku uzyskać dane osobowe 37 milionów klientów sieci[12]. Krążące w sieci od lipca prywatne informacje dotyczące kont Twittera miały swoje źródło w podatnym API, które zostało wykorzystane w roku 2021 do wydobycia danych dotyczących około 200 milionów kont[13]. Jak widać, nawet systemy tworzone przez doświadczonych inżynierów dla globalnych korporacji mogą posiadać błędy pozwalające na nieautoryzowany dostęp do informacji.

ŁAŃCUCH WYCIEKÓW

W niektórych przypadkach jeden wyciek to dopiero początek problemów - zwłaszcza jeżeli zawiera dane logowania użytkowników. Uzyskane informacje są często wykorzystywane do przeprowadzania prób logowania w innych serwisach w ramach ataków typu "credential stuffing". Niestety, przez skłonność użytkowników do częstego wykorzystywania takich samych lub zbliżonych haseł do wielu serwisów, ataki te kończą się powodzeniem. Celem takiego ataku na dużą skalę padli użytkownicy serwisu PayPal. Wykorzystując znalezione w wyciekach dane logowania przestępcy uzyskali dostęp do blisko 35 tys. kont[14]. Użycie podobnej techniki zaobserwowano też m. in. wobec Norton Password Manager, czyli jednego z dostępnych na rynku menedżerów haseł[15].

10 "Utracone" notatniki służbowe policjanta KMP w Łomży. Prokuratura prowadzi śledztwo!"
11 "Wyciekły dane osobowe studentów SGH. Przez miesiąc pokazywała je wyszukiwarka Bing..."
12 "T-Mobile hacked to steal data of 37 million accounts in API data breach"
13 "200 million Twitter users' email addresses allegedly leaked online"
14 "PayPal accounts breached in large-scale credential stuffing attack"
15 "NortonLifeLock warns that hackers breached Password Manager accounts"

DZIAŁANIA CYBERPRZESTĘPCÓW

Wszelkie informacje mogą stanowić łakomy kąsek dla cyberprzestępców. Poza ich sprzedażą mogą oni wykorzystać je do przygotowania kolejnych ataków.

W ostatnich latach powszechnym stało się rozbudowywanie szkodliwego oprogramowania typu ransomware o funkcje pozwalające na kradzież danych z zainfekowanych maszyn. Wcześniej głównym jego zadaniem było szyfrowanie danych i żądanie okupu za możliwość ich odzyskania. Kradzież danych daje więcej możliwości nacisku na ofiarę, np. poprzez groźby ich publicznego ujawnienia. Ponadto uzyskane dane mogą być wykorzystane w dalszych atakach na ten sam cel, jego klientów lub kontrahentów. Ofiarą ataku ransomware w tym roku padły m. in. Urząd Miasta Zambrów[16] czy Instytut Centrum Zdrowia Matki Polki w Łodzi[17]. W żadnym z tych przypadków nie potwierdzono dotychczas wycieku danych.

Czasami cyberprzestępcy uzyskują dostęp do danych, co do których bezpieczeństwa powinniśmy mieć pewność. Tak było w przypadku wycieku z LastPass, menedżera haseł z synchronizacją w chmurze. Na skutek uzyskania dostępu do danych uwierzytelniających jednego z pracowników, atakujący uzyskali dostęp do danych użytkowników, w tym zaszyfrowanych pełnych kopii baz zawierających zapisane przez nich dane logowania[18]. Bezpieczeństwo danych użytkowników zależy więc w dużej mierze od tego, jak mocne hasło wykorzystali do szyfrowania bazy. Należy również pamiętać, że nie wszystkie pola wpisów w bazach były szyfrowane.

W niektórych przypadkach atak nie musi być ukierunkowany bezpośrednio w daną organizację. Wystarczy, że zaatakowany zostanie jeden z jej kontrahentów. Tak było w przypadku wycieku danych z serwisu Uber. Na skutek uzyskania nieautoryzowanego dostępu do kopii zapasowych baz danych Teqtivity (świadczącej dla Ubera usługi z zakresu m. in. zarządzania kapitałem) doszło do wycieku danych 77 tysięcy kierowców i pojazdów Ubera[19].

JAK PRZYGOTOWAĆ SIĘ NA WYCIEK?

Mając świadomość, że wycieki danych są w dzisiejszych czasach na porządku dziennym, nie powinniśmy zakładać, że informacje, które podajemy, będą w pełni bezpieczne. Możemy natomiast postarać się, aby skutki potencjalnego wycieku były jak najmniej bolesne.

PODAWAJ MINIMUM WYMAGANYCH DANYCH

Im mniej danych przekażemy np. tworząc konto w serwisie lub robiąc zakupy w internecie, tym mniej informacji może ulec wyciekowi i będą one mniej użyteczne dla przestępców. Jeżeli możemy zamiennie podać różne rodzaje danych, np. adres e-mail lub numer telefonu jako dane kontaktowe, wybierzmy tę opcję, której upublicznienie na skutek wycieku będzie niosło za sobą mniejsze konsekwencje.

UŻYWAJ UNIKALNYCH, SILNYCH HASEŁ

Wielokrotne używanie tego samego hasła powoduje, że jesteśmy bardziej podatni na opisane wyżej ataki typu "credential stuffing", wykorzystujące hasła z wycieku w jednym serwisie do uzyskania dostępu do kont w innych serwisach. Nawet jeżeli hasła są różne, ale podobne lub tworzone z wykorzystaniem łatwej do odgadnięcia metody, to przestępcy są w stanie w krótkim czasie je odgadnąć. Pamiętajmy też, aby nie tworzyć haseł z informacji dostępnych o nas publicznie lub łatwych do uzyskania, takich jak data urodzenia. Ona również może znaleźć się w wyciekach i być wykorzystana razem z innymi informacjami takimi jak imię, nazwisko czy adres e-mail. Dobrą praktyką jest korzystanie z menedżerów haseł, które przy odpowiednio silnym haśle głównym zapewniają wysoki poziom bezpieczeństwa pozwalając na używanie losowych i unikalnych haseł. Zachęcamy do przeczytania kompendium wiedzy o hasłach, które znaleźć można na naszej stronie Internetowej. Poza korzystaniem z silnych haseł poziom bezpieczeństwa możemy podnieść konfigurując uwierzytelnianie dwuskładnikowe tam, gdzie to możliwe.

16 "Ransomware w kolejnym urzędzie w Polsce (w tle również wyciek danych). Zambrów"
17 "Zawiadomienie o naruszeniu ochrony danych osobowych"
18 "Lastpass: Hackers stole customer vault data in cloud storage breach"
19 "Uber suffers new data breach after attack on vendor, info leaked online"

REAGUJ NA POWIADOMIENIA O INCYDENTACH

W przypadku wykrycia wycieku danych przepisy ustawy o ochronie danych osobowych nakładają na ich administratora obowiązek poinformowania użytkowników. Komunikat musi zawierać zakres danych, które uległy wyciekowi. W wypadku otrzymania tego typu powiadomienia nie powinniśmy go ignorować. W pierwszej kolejności należy zweryfikować jego prawdziwość - obserwujemy bowiem wiadomości phishingowe wykorzystujące ten scenariusz do kradzieży danych (więcej informacji na temat tego czym jest phishing i jak się przed nim chronić znajdziesz na naszej stronie). Po zweryfikowaniu prawdziwości otrzymanego komunikatu postępujmy zgodnie z zaleceniami administratora. Sprawdźmy też, czy dane, które wyciekły, mogą być wykorzystane do prób uzyskania dostępu do innych kont.

STOSUJ SEPARACJĘ TOŻSAMOŚCI

Powszechnie stosowaną praktyką jest rozdzielenie adresów e-mail na te wykorzystywane prywatnie i służbowo. Nic nie stoi na przeszkodzie, aby podobną separację wprowadzić właśnie wśród swoich prywatnych adresów. Dobrym pomysłem jest używanie do korzystania z bankowości innego adresu e-mail niż ten, który widnieje na naszych kontach społecznościowych czy forach. Odrębne konta e-mail pozwalają na zachowanie większej prywatności, jak i ograniczenie szkód spowodowanych ewentualnym wyciekiem danych.

SPRAWDZAJ OBECNOŚĆ SWOICH DANYCH W WYCIEKACH

Serwis “Have I Been Pwned?”[20] pozwala na sprawdzenie, czy nasz adres e-mail lub numer telefonu występuje w znanych wyciekach danych. Umożliwia on również dodanie naszego adresu e-mail do stałego monitoringu nowych wycieków, dzięki czemu w razie wystąpienia incydentu obejmującego naszą cyfrową tożsamość, zostaniemy o tym poinformowani. Podobne funkcje często są również wbudowane w popularne menedżery haseł.

CO ZROBIĆ PO WYCIEKU?

Wiele zależy od zakresu danych, jakie uległy wyciekowi. Jeżeli wyciekło nasze hasło, należy zmienić je w każdym serwisie, w którym było wykorzystywane. Dobrym pomysłem będzie też włączenie weryfikacji dwuetapowej na każdym z kont. Jeżeli doszło do wycieku naszej osobowości prawnej: numeru PESEL, dowodu osobistego itp., warto rozważyć podjęcie dodatkowych kroków. Powszechną praktyką stosowaną przez przestępców, którzy weszli w posiadania tego typu danych, jest próba zaciągnięcia na nie pożyczki. Istnieje kilka serwisów, które mogą pomóc nam chronić się przed tego typu praktykami:

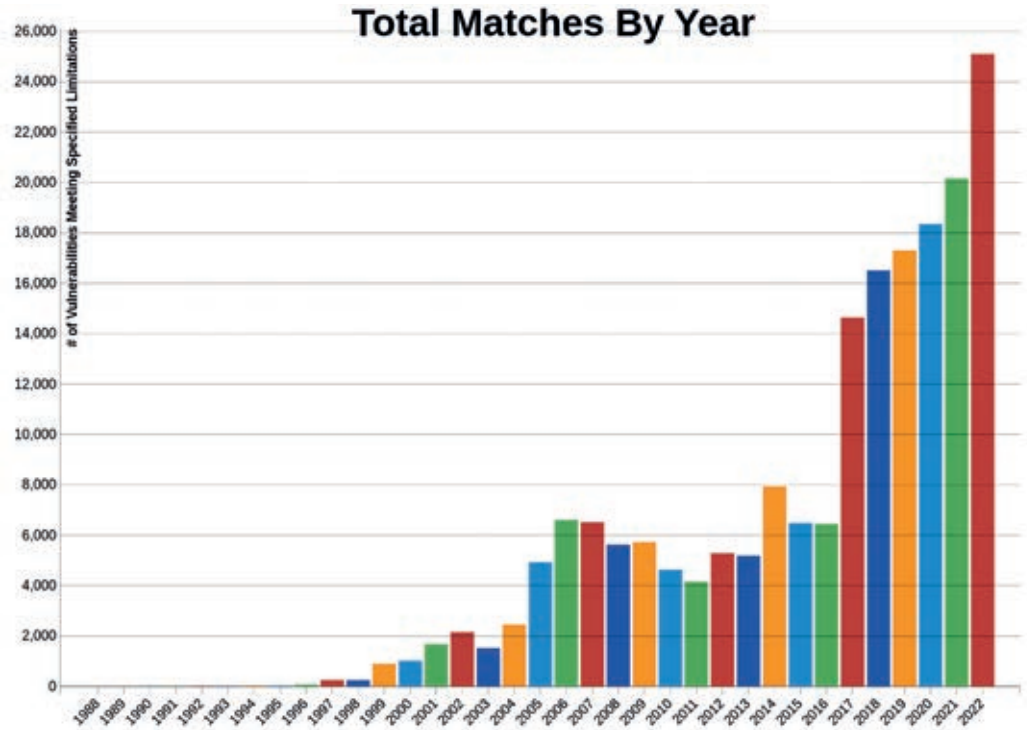
- Biuro Informacji Kredytowej (BIK) - oferujące m.in. powiadomienia o próbie uzyskania kredytu na nasze dane oraz raporty podsumowujące nasze zobowiązania kredytowe,
- Rejestr dłużników BIG – mający na celu gromadzenie i udostępnianie informacji dotyczących osób z nieuregulowanymi zobowiązaniami,
- Portal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

Zachęcamy również do śledzenia naszych mediów społecznościowych na portalu Facebook (https://fb.com/CERT.Polska) oraz Twitterze (@CERT_Polska), gdzie informujemy o obserwowanych przez nas bieżących scenariuszach oszustw i innych zagrożeniach wymierzonych w polskich internautów.

20 https://haveibeenpwned.com/

NAJWAŻNIEJSZE PODATNOŚCI W 2022 ROKU

Rok 2022 był rekordowy pod względem liczby nowych podatności. W bazie National Vulnerability Database (NVD) prowadzonej agencję NIST[21] w minionym roku pojawiło się ponad 25 tys. nowych podatności. Stanowi to znaczny wzrost względem roku 2021 i wpasowuje się w rosnący trend, który widzimy już od 6 lat (Wykres 3). Należy jednak pamiętać, że podatności zarejestrowane w bazie NVD nie stanowią idealnego odwzorowania aktualnego krajobrazu zagrożeń. Bardzo duża część podatności jest czysto teoretyczna i nigdy nie zostaje wykorzystana w praktyce. Bardzo dobrym dopełnieniem jest baza aktywnie wykorzystywanych podatności prowadzona przez agencję CISA[22]. Zawiera ona jedynie podatności, których wykorzystanie zostało zaobserwowane na szerszą skalę. Na stan z końca roku 2022 aktywnie wykorzystywanych było 868 różnych podatności, przy czym 93 zostało opublikowanych w tym samym roku.



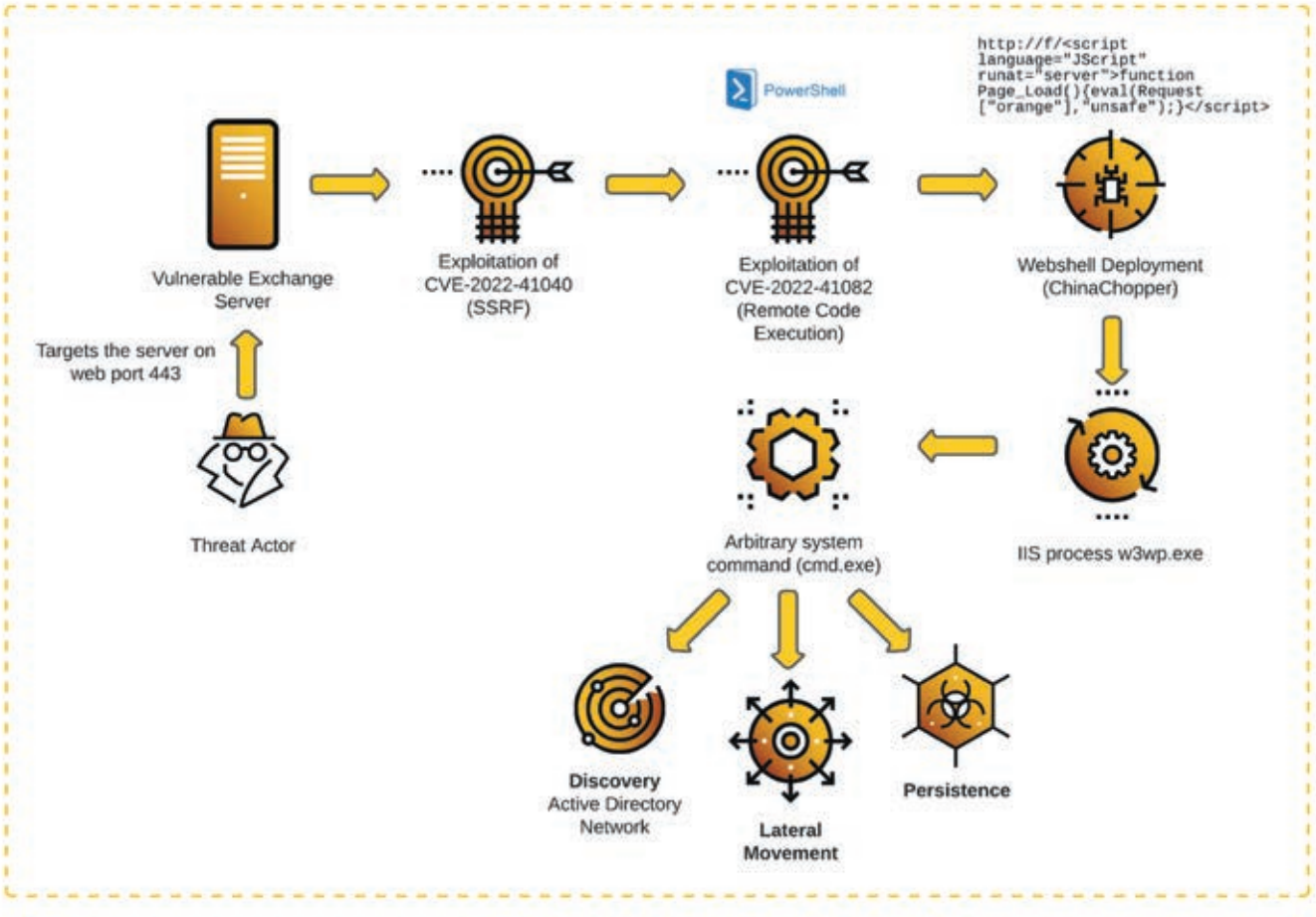
Wykres 3. Liczba nowych podatności zarejestrowanych w bazie NVD w ujęciu rocznym,

źródło: https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all&isCpeNameSearch=false

21 https://nvd.nist.gov/
22 https://www.cisa.gov/known-exploited-vulnerabilities-catalog

PROXYNOTSHELL (CVE-2022-41040 I CVE-2022-41082)

Podatność ProxyNotShell jest zbliżona do podatności ProxyShell, o której wspominaliśmy w raporcie z roku 2021[23]. Podobnie jak poprzednia podatność, ProxyNotShell nie wykorzystuje jednej luki, lecz łączy kilka słabości w jeden atak, który pozwala na przejęcie kontroli nad serwerem Exchange. Warto zaznaczyć, że w przypadku tej podatności atakujący musi posiadać przynajmniej jedno działające konto na serwerze pocztowym, ale nie musi ono posiadać uprawnień administracyjnych. W praktyce bardzo często atakujący wyszukują organizacje z podatnym serwerem Exchange, a następnie szukają działających poświadczeń w wyciekach lub starają się je zakupić od innych przestępców. Znajomość hasła do dowolnego konta pocztowego poprzez wykorzystanie podatności pozwala atakującemu na umieszczenie na serwerze skryptu webshell. Warto zaznaczyć, że uzyskanie kontroli nad serwerem Exchange bardzo często prowadzi również do uzyskania uprawnień administracyjnych w usłudze Active Directory. Daje to atakującemu kompletną kontrolę nad infrastrukturą organizacji.



Rys. 59 Przykładowy atak na serwer Exchange wykorzystując podatność ProxyNotShell,

źródło: https://www.cybereason.com/blog/threat-alert-proxynotshell-two-critical-vulnerabilities-affecting-ms-exchange*

23 https://cert.pl/uploads/docs/Raport_CP_2021.pdf#page=53

Podczas obsługi zgłoszeń kilkukrotnie natrafiliśmy na incydenty, w których znaczna część infrastruktury organizacji została zaszyfrowana i punktem wejściowym atakującego była właśnie podatność ProxyNotShell. W celu ograniczenia wpływu luki na polskie organizacje powiadomiliśmy właścicieli podatnych serwerów widocznych z Internetu mailowo oraz poprzez platformę współdzielenia informacji o incydentach bezpieczeństwa N6. O podatnościach informowaliśmy również za pomocą naszych kont w mediach społecznościowych (Rys. 60).

Statystyki z procesu informowania właścicieli podatnych serwerów:

- Liczba instancji MS Exchange w polskiej adresacji, które były podatne na ProxyNotShell: **208**
- Liczba powiadomień wysłana do organizacji: **86** (niektóre organizacje posiadały kilka serwerów).

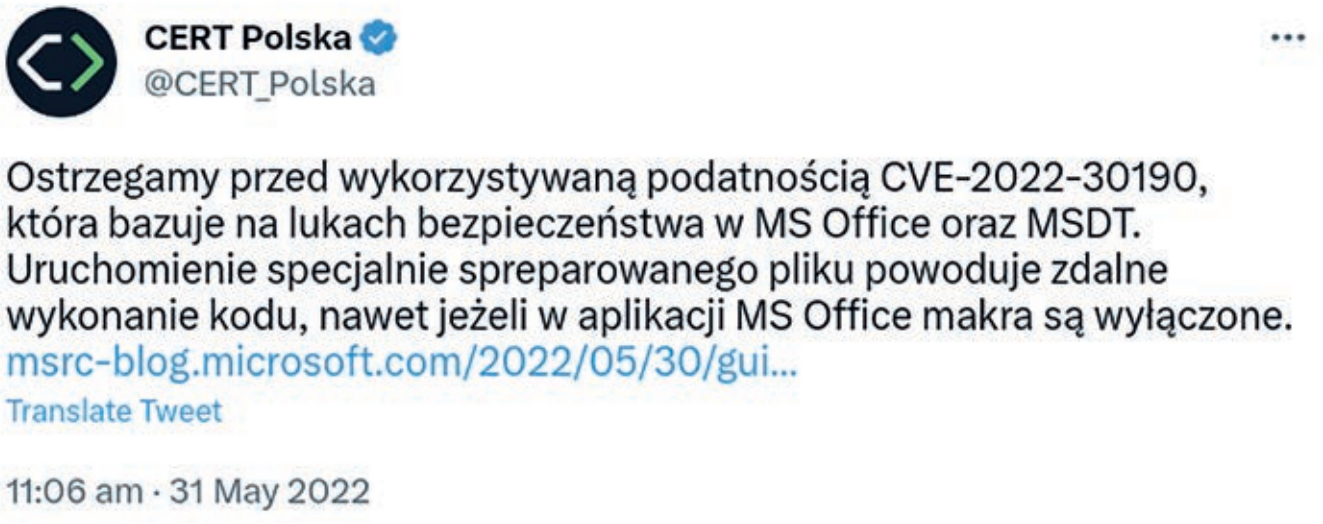
Rys. 60 Ostrzeżenie przed podatnością ProxyNotShell

https://twitter.com/CERT_Polska/status/1575810236958605312*

FOLLINA (CVE-2022-30190)

Wykorzystywanie tej podatności zostało zauważone i pierwszy raz publicznie opisane przez badaczy z zespołu nao_sec pod koniec maja 2022 r[24]. W momencie jej opisania podatność nie posiadała łatki. Dostrzeżona próbka była dokumentem Microsoft Word i wykorzystała lukę w narzędziu diagnostycznym pomocy technicznej Microsoft (MSDT). W przeciwieństwie do podobnych ataków za pomocą złośliwych dokumentów nie wymagała ona od użytkownika żadnej interakcji poza otwarciem dokumentu. Tak więc użytkownik jedynie otwierając złośliwy dokument umożliwiał atakującemu na wykonanie kodu i uruchomienie skryptu PowerShell, który następnie prowadził do infekcji złośliwym oprogramowaniem.

24 https://twitter.com/nao_sec/status/1530196847679401984



Rys. 61 Ostrzeżenie przed podatnością CVE-2022-30190

https://twitter.com/CERT_Polska/status/1531562851361599494*

Pomimo publikacji przez Microsoft poprawek usuwających lukę w MSDT niespełna trzy tygodnie po publicznej informacji o luce, podatność była bardzo chętnie wykorzystywana przez atakujących podobnie do CVE-2017-11882[25]. Podatność ta polegała na możliwości przepełnienia buforu, a co za tym idzie, wykonaniu dowolnego kodu w Edytorze równań firmy Microsoft. Mimo swojego wieku i dostępnej poprawki jest nadal jedną z najczęściej wykorzystywanych podatności przy próbie infekcji użytkowników za pomocą złośliwych dokumentów MS Office.

FORTIOS (CVE-2022-42475)

Jeśli w infrastrukturze organizacji można wyznaczyć jakiś element krytyczny, to z pewnością jest nim serwer VPN. Oddzielając wewnętrzną infrastrukturę od Internetu chroni bardziej wrażliwe systemy przed nieustannymi atakami z zewnątrz. Właśnie z tego powodu podatności w rozwiązaniach VPN są chętnie wykorzystywane przez różnego rodzaju atakujących – od grup przestępczych nastawionych na zysk, po grupy APT mające na celu wykradanie niejawnych dokumentów.

Przykładem takiej podatności było opublikowane pod koniec roku CVE-2022-42475. Podatność dotyczyła modułu SSL-VPN urządzeń korzystających z Fortinet FortiOS i pozwalała atakującemu na przejęcie kontroli nad urządzeniem bez potrzeby uwierzytelniania. Dodatkowo okazało się, że podatność była wykorzystywana jeszcze przed opublikowaniem o niej informacji i łatek poprawiających błąd.

W ramach obsługi incydentu i ograniczenia wpływu podatności na organizacje w Polsce powiadomiliśmy właścicieli wszystkich podatnych serwerów mailowo oraz poprzez platformę N6. Na naszej stronie opublikowaliśmy również artykuł[26] z opisem podatności, rekomendacjami oraz sposobem wykrycia ataku.

Oto statystyki z procesu informowania właścicieli podatnych serwerów:

- Liczba instancji MS Exchange w polskiej adresacji, które były podatne na CVE-2022-42475 (stan na 2022-10-10): **198**,
- Liczba powiadomień wysłana do organizacji: **91** (niektóre organizacje posiadały kilka serwerów).

25 https://nvd.nist.gov/vuln/detail/CVE-2017-11882
26 https://cert.pl/posts/2022/12/krytyczna-podatnosc-fortios/

Rys. 62 Artykuł opisujący podatność CVE-2022-42475, sposoby zmitygowania ryzyka oraz detekcji ataku. https://cert.pl/posts/2022/12/krytyczna-podatnosc-fortios/*

WOJNA W UKRAINIE

– WPŁYW NA CYBERBEZPIECZEŃSTWO

24 lutego 2022 r. rozpoczęła się pełnowymiarowa rosyjska inwazja na Ukrainę. Już w miesiącach poprzedzających wojnę Rosja prowadziła nasilone działania w cyberprzestrzeni, przygotowujące grunt pod to, co miało się wydarzyć. W styczniu rosyjscy hakerzy doprowadzili do paraliżu ukraińskie strony rządowe, a tuż przed rozpoczęciem inwazji przeprowadzono także cyberatak na sieć satelitarną KA-SAT. Celem działań było uniemożliwienie komunikacji między tysiącami użytkowników w Ukrainie, a także zerwanie łączności z szerokopasmowym Internetem dla dziesiątek tysięcy odbiorców w niektórych państwach członkowskich Unii Europejskiej. Dziś – ponad rok od wybuchu wojny – obserwujemy, jak Rosja próbuje wykorzystywać ataki cybernetyczne, aby destabilizować sytuację wewnętrzną w państwach wspierających Ukrainę. Ataki na instytucje publiczne i infrastrukturę krytyczną wzmogły się, co wpisuje się w realizację rosyjskiej strategii wojskowej. Czy ich wpływ jest jednak taki, jakiego się spodziewano?

W początkowych doniesieniach z Ukrainy pojawiał się często termin „wojna hybrydowa". Sugerowano także, że będzie to „wojna cyfrowa", ograniczająca się do cyberprzestrzeni. Z perspektywy czasu wiemy już, że mamy do czynienia z pełnoskalowym konfliktem, gdzie narzędzia konwencjonalne odgrywają kluczową rolę. Po raz pierwszy jednak możemy obserwować, jak tradycyjne działania wojenne wspierane są przez aktywności w cyberświecie. Mamy tu na myśli zarówno aktywność hakerów czy konkretnych grup haktywistycznych, jak również szerzenie dezinformacji.

Skala incydentów w 2022 r. jest zdecydowanie większa niż w latach poprzednich. Częściowo wpływ na to ma sytuacja za naszą wschodnią granicą. Zdarzenia w polskiej cyberprzestrzeni, które bezpośrednio łączymy z sytuacją w Ukrainie, to zmasowane ataki typu DDoS na strony rządowe i portale istotnych krajowych podmiotów gospodarczych. Mamy do czynienia także z kampaniami phishingowymi, które wykorzystują motyw wojny i pojawiają się głównie w mediach społecznościowych. Zmiany na rynku energii wywołane rosyjską agresją przyniosły też masowe pojawienie się fałszywych sklepów z opałem.

Właśnie te zjawiska chcielibyśmy przybliżyć w rozdziale dotyczącym wojny w Ukrainie. Zależy nam na pokazaniu jak bardzo cyberprzestrzeń zależna jest od wydarzeń w świecie rzeczywistym. Jak intensywnie geopolityka wpływa dziś na to, z czym mierzymy się w sieci i jak sojusze zawiązywane na gruncie militarnym czy politycznym znajdują odbicie w działaniach grup haktywistycznych. Należy podkreślić, że zjawiska tu opisane łączą kraje sprzymierzone z Ukrainą. Polska nie jest jedynym państwem, które mierzy się z wrogą aktywnością w sieci. Podobne mechanizmy działania czy nawet te same grupy haktywistów obserwujemy w pozostałych krajach naszego regionu i w USA.

Co ciekawe, działania, które miały służyć destabilizacji, skłaniają państwa do większej współpracy i wymiany doświadczeń, co pozwala wyciągać wnioski i skuteczniej odpowiadać na ataki. Pamiętajmy również, że zagrożenie w cyberprzestrzeni związane z wojną w Ukrainie jeszcze nie minęło.

ATAK NA SIEĆ INTERNETU SATELITARNEGO VIASAT

24 lutego 2022 r. sieć satelitarna KA-SAT należąca do firmy Viasat padła ofiarą ukierunkowanego ataku. Efektem działań aktora była niedostępność usług łączności satelitarnej przez dziesiątki tysięcy urządzeń końcowych, głównie w Europie Środkowo-Wschodniej.

PRZEBIEG ATAKU

We wczesnych godzinach porannych 24 lutego 2022 r. sieć KA-SAT odnotowała atak DoS na swoją infrastrukturę satelitarną pochodzący z urządzeń końcowych zlokalizowanych na terytorium Ukrainy. Atak ten rozpoczął się około godziny 03:02 UTC i skutkował niestabilnością połączenia urządzeń klienckich z siecią oraz brakiem możliwości dołączenia do sieci nowych urządzeń. Viasat oraz Skylogic rozpoczęli analizę incydentu obserwując spadającą liczbę urządzeń końcowych podłączonych do segmentu sieci dotkniętego atakiem, który wpłynął na licznych abonentów na terenie Europy Środkowo-Wschodniej. Jednym z największych ujawnionych komercyjnych podmiotów, który odczuł skutki ataku, była niemiecka firma z sektora energetycznego Enercon. Utraciła ona zdolność zdalnego monitorowania i sterowania 5 800 turbinami wiatrowymi. Nie zostały opublikowane informacje o wpływie tego ataku na sektor zbrojeniowy oraz na wojska obrony Ukrainy.

STRONA TECHNICZNA

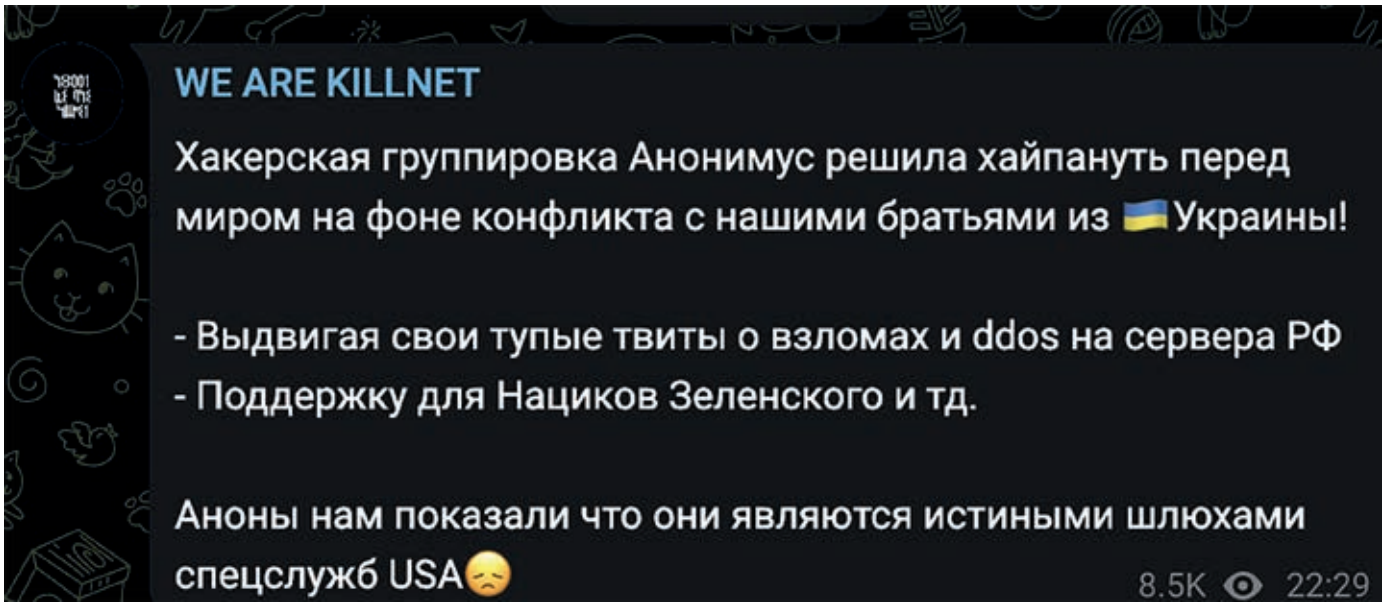
Późniejsza analiza incydentu wskazała, że wykorzystanym wektorem ataku była źle skonfigurowana brama VPN. Za jej pomocą atakujący uzyskali dostęp do sieci wewnętrznej Viasat, która była używana do zarządzania kliencką siecią KA-SAT. Przy użyciu tego dostępu atakujący wysłali na wpięte do sieci modemy klientów serię komend, które najprawdopodobniej doprowadziły do pobrania oraz uruchomienia złośliwego oprogramowania AcidRain. Jest to oprogramowaniem typu wiper, zaprojektowane pod architekturę MISP, szeroko wykorzystywaną w modemach. Jego głównym zadaniem jest zaburzenie funkcjonalności urządzeń przez nadpisanie plików reprezentujących urządzenia logiczne (/dev/...) w systemie operacyjnym oraz finalnie restart systemu. Zaatakowane w ten sposób urządzenia nie były w stanie poprawnie uruchomić się ponownie, co skutkowało niedostępnością usługi (DoS). Według informacji udzielonych przez producenta, reset do ustawień fabrycznych przywracał sprawność urządzenia, ponieważ w ramach ataku nie zostawał nadpisany firmware. Nie znaleziono też wskazań, aby atak miał wpływ na infrastrukturę służącą do aktualizacji urządzeń lub modyfikował obrazy oprogramowania przeznaczonego dla modemów. Ponadto nie znaleziono również śladów na jakiekolwiek inne złośliwe działanie oprogramowania, mające na celu eksfiltrację danych, bądź inne rodzaje niedestruktywnych działań.

ATRYBUCJA

Atak rozpoczął się niemal w tym samym momencie, co pełnowymiarowa inwazja Rosji na Ukrainę. W samej Ukrainie atak dotknął, zakłócając bądź zupełnie uniemożliwiając łączność satelitarną, tysiące klientów. Użyte do ataku złośliwe oprogramowanie AcidRain posiada pewne elementy wspólne z zaobserwowanym wcześniej modułem niszczącym, używanym przy dystrybucji złośliwego oprogramowania VPNFilter. Oprogramowanie VPNFilter zostało przypisane różnym aktorom powiązanym z rosyjską instytucją odpowiedzialną za wywiad wojskowy GRU. Jednak widoczne są znaczące różnice pomiędzy tymi próbkami złośliwego oprogramowania, w związku z czym atrybucja ataku nie jest do końca jasna.

ATAKI DDOS PRZEPROWADZANE PRZEZ ROSYJSKICH HAKTYWISTÓW

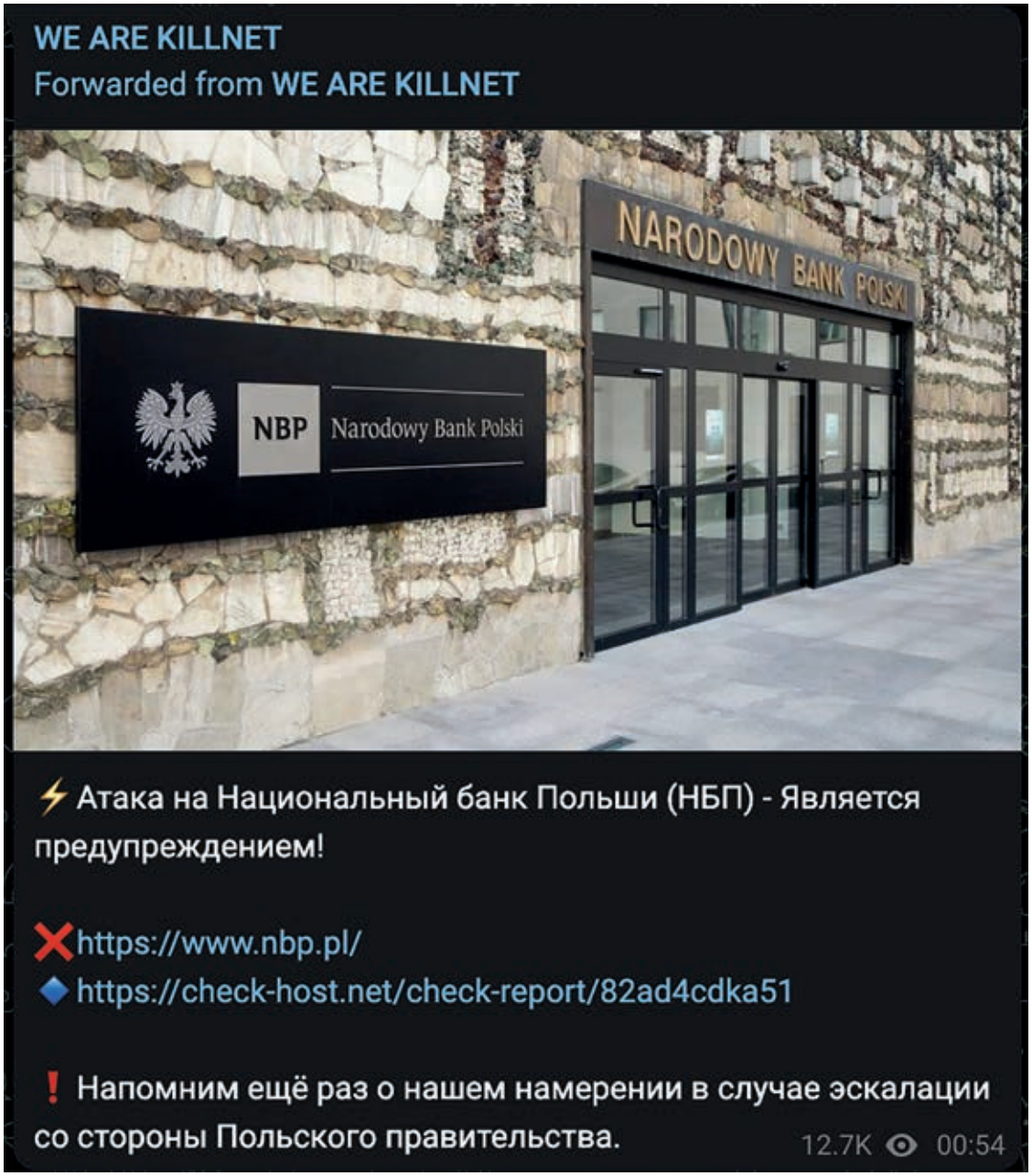
Wraz z rozpoczęciem wojny w Ukrainie wiele grup cyberprzestępczych i haktywistów rozpoczęło swoje działania przeciwko naszemu sąsiadowi, a następnie ten impakt przeniósł się na takie kraje jak Polska, kraje nadbałtyckie i skandynawskie. Jedną z takich grup jest grupa Killnet, która przed rozpoczęciem wojny specjalizowała się w atakach DDoS. W przeciwieństwie do innych wysoko wykwalifikowanych rosyjskich grup cyberprzestępczych (Sandworm i FancyBear), Killnet nie jest wyspecjalizowaną i dobrze zorganizowaną grupą. Jest częściowo ustrukturyzowana i składa się z mniejszych, mniej znanych grup, które również sympatyzują z Rosją. Killnet jest znany z szerzenia propagandy i dezinformacji. Do grup prorosyjskich powiązanych z Killnet należą Legion i Xaknet.



Rys. 63 Przykład wiadomości od grupy Killnet

Celem pierwszych ataków przeprowadzonych przez grupę Killnet były ukraińskie instytucje publiczne i firmy, takie jak ukraiński oddział Vodafone. Następnie grupa swoje ataki kierowała na kraje, które wspierały Ukrainę bądź nie popierały bezpośrednio inwazji Rosji na Ukrainę. Zgodnie z tą taktyką kolejnymi celami Killnetu były takie kraje jak Litwa, Łotwa, Estonia czy Polska. W późniejszym okresie atakowali także CyberPol, który oskarżali o włamanie na ich serwer i kradzież informacji o jednym z członków grupy. Zaatakowali również Centrum Doskonalenia Cyberobrony NATO (CCDCOE), które

jest odpowiedzialne za organizację największych na świecie ćwiczeń obrony bezpieczeństwa komputerowego “Locked Shields”. W sumie na liście celów Killnetu znajduje się wiele państwa z różnych kontynentów.Pod koniec marca 2022 r. Killnet przeprowadził atak DDoS na stronę Internetową Sądu Najwyższego, a następnie Narodowego Banku Polskiego. Od tego momentu Killnet regularnie przeprowadzał i informował o atakach DDoS na inne polskie podmioty rządowe i prywatne firmy. Przeprowadził również atak DDoS na strony Internetowe ośmiu polskich lotnisk. Trudno ustalić, w jaki sposób Killnet i podległe jemu grupy wybierają swoje cele. Wśród polskich celów są instytucje rządowe, takiej jak wspomniany wcześniej Sąd Najwyższy i Narodowy Bank Polski, Policja, ale również takie podmioty jak szpitale w mniejszych miejscowościach powiatowych oraz firmy, takiej jak np: Castorama, mBank czy Orange.



Rys.64 Przykład wiadomości o ataku na stronę NBP

Atakujący zamieszczają informacje o przeprowadzonym ataku za pośrednictwem swoich kanałów w serwisie Telegram. Początkowo przestępcy umieszczali wpis o planowanym działaniu, tuż przed jego przeprowadzeniem. Po pewnym czasie zmienili podejście i obecnie informują o ataku, który został już przeprowadzony i odniósł według nich zamierzony skutek.

Głównym celem przestępców padają najczęściej strony Internetowe różnych państwowych instytucji, ale też prywatnych firm. W serwisie Telegram atakujący publikują zrzut ekranu z serwisu https://check-host.net/, na którym pokazują chwilowy problem z dostępnością do strony głównej atakowanego podmiotu. Rezultat, który uzyskali atakujący, często jest iluzoryczny, strony najczęściej są niedostępne tylko przez kilka minut, bądź odrzucają połączenia z adresów IP innych niż polskie. Atakowane strony mają głównie charakter informacyjny, dlatego w większości przypadków nie dochodzi do zakłócenia funkcjonowania instytucji, która padła ofiarą cyberprzestępców. Głównym celem grupy Killnet jest szerzenie propagandy i dezinformacji.

Rys.65 Przykład wiadomości od grupy Killnet z listą atakowanych celów

Grupa Killnet została wpisana na listę Russian State-Sponsored za swoje ataki DDoS na infrastrukturę krytyczną USA i innych krajów anglosaskich.

Killnet wielokrotnie zmieniał swoją strukturę. Pojawił się Killnet 2.0, a następnie Legion Russia, który składał się z innych grup mających wspólnie przeprowadzać atak DDoS.

Zespół CSIRT KNF przygotował poradnik z dobrymi praktykami w zakresie przeciwdziałania atakom DDoS. Zalecamy zapoznanie się z tym poradnikiem.

https://cebrf.knf.gov.pl/images/Raporty/Dobre_praktyki_w_zakresie_przeciwdziaania_atakom_DDoS_77247.pdf

ZNANE KAMPANIE WYKORZYSTUJĄCE MOTYW WOJNY

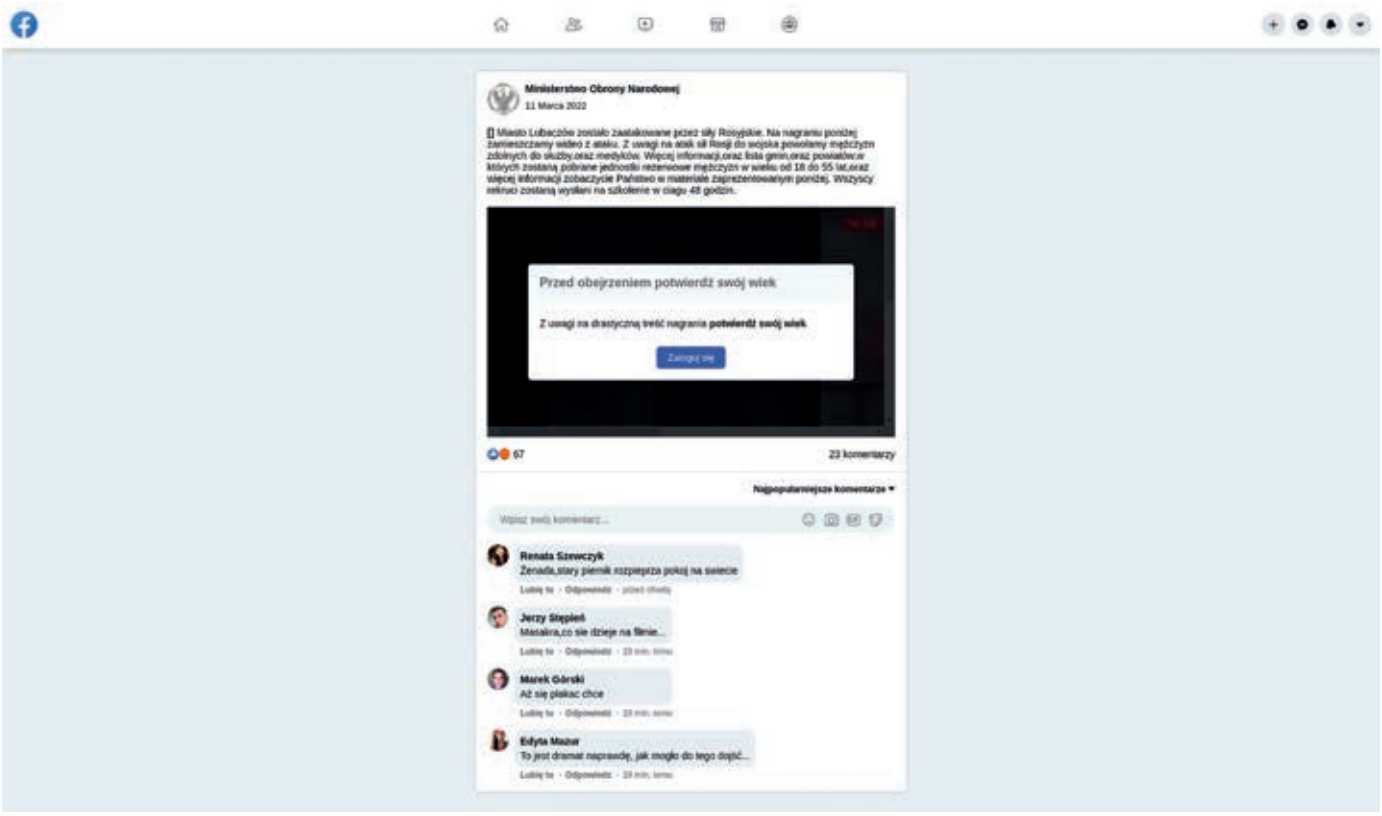
FAŁSZYWE PANELE LOGOWANIA DO FACEBOOKA

Najpowszechniejszym oszustwem w 2022 r. były fałszywe artykuły wyłudzające dane logowania do serwisu Facebook. Panel logowania do platformy poprzedzał artykuł z informacją, która miała wzbudzić w odbiorcy skrajne uczucia i zainteresowanie. Przykładowo pojawiały się nieprawdziwe informacje mówiące o ataku Białorusi na Ukrainę i bestialskim czynie dwóch białoruskich żołnierzy, pojmaniu prezydenta Ukrainy, a w innym przypadku o jego śmierci. Artykuły opisywały również ostrzał Lubaczowa, Przemyśla, Rzeszowa i Hrubieszowa rosyjskimi rakietami. Popularne były także informacje dotyczące naszego kraju, w których opisywano, jak obywatele Ukrainy zaatakowali młodą kobietę w centrum miasta. Według innych artykułów wojna mogła rzekomo zostać zakończona po spełnieniu kilku warunków przez polskich polityków. Nie były to jedyne poruszane tematy.

Wszystkie artykuły łączyło jedno - rzekomy materiał wideo przedstawiający kluczowe informacje. Dostęp do nagrań można było uzyskać jedynie po wcześniejszej weryfikacji, oczywiście za pomocą serwisu Facebook.

Przestępcy wykorzystywali wcześniej przejęte konta, za pomocą których rozpowszechniali specjalnie przygotowane domeny z sensacyjnymi informacjami i panelem logowania do serwisu Facebook. Szata graficzna fałszywych stron Internetowych do złudzenia przypominała znane portale społecznościowe lub portale z wiadomościami, co usypiało czujność czytelnika. Z każdym kolejnym przejętym kontem zwiększała się baza potencjalnych ofiar i zasięg propagacji oszustwa. Cyberprzestępcy wykorzystywali konta również do wyłudzania pieniędzy od znajomych ofiary, nieświadomych zaistniałej sytuacji. Oszust kontaktował się z potencjalną ofiarą prosząc o przelew pieniędzy i przesyłał fałszywą bramkę płatności. Częściej zdarzały się wyłudzenia kodu BLIK.

Rys. 66 Przykłady fałszywych artykułów poprzedzających panel logowania wyłudzający dane.

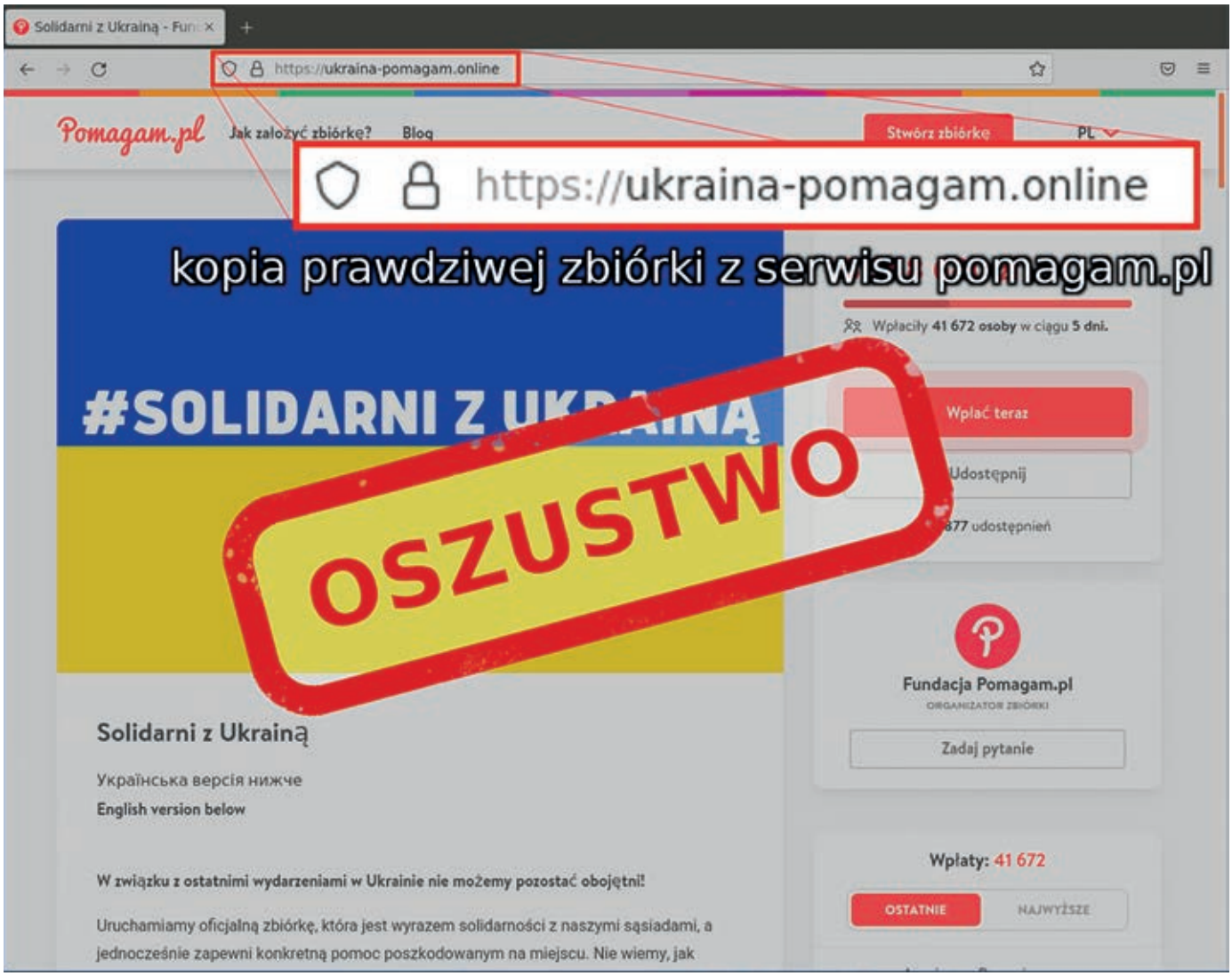


Rys. 67 Przykłady fałszywych artykułów poprzedzających panel logowania wyłudzający dane.

FAŁSZYWE ZBIÓRKI

W 2022 r. CERT Polska odnotował również próby wyłudzenia pieniędzy pod przykrywką prowadzenia działań pomocowych. W ostatnich dniach lutego minionego roku zaobserwowaliśmy fałszywą domenę łudząco podobną do Pomagam.pl, znanego serwisu do tworzenia zbiórek. Organizatorem tej zbiórki miała być sama Fundacja Pomagam, a zebrane środki sięgały ponad 3,5 mln złotych.

Dodatkowo pojawiały się próby wyłudzenia środków pieniężnych bezpośrednio na konta oszustów lub portfele kryptowalut. Informacje o fałszywych zbiórkach były rozpowszechniane w wiadomościach mailowych, SMS-ach, czy we wpisach w mediach społecznościowych.



Rys. 68 Fałszywa zbiórka pieniędzy.

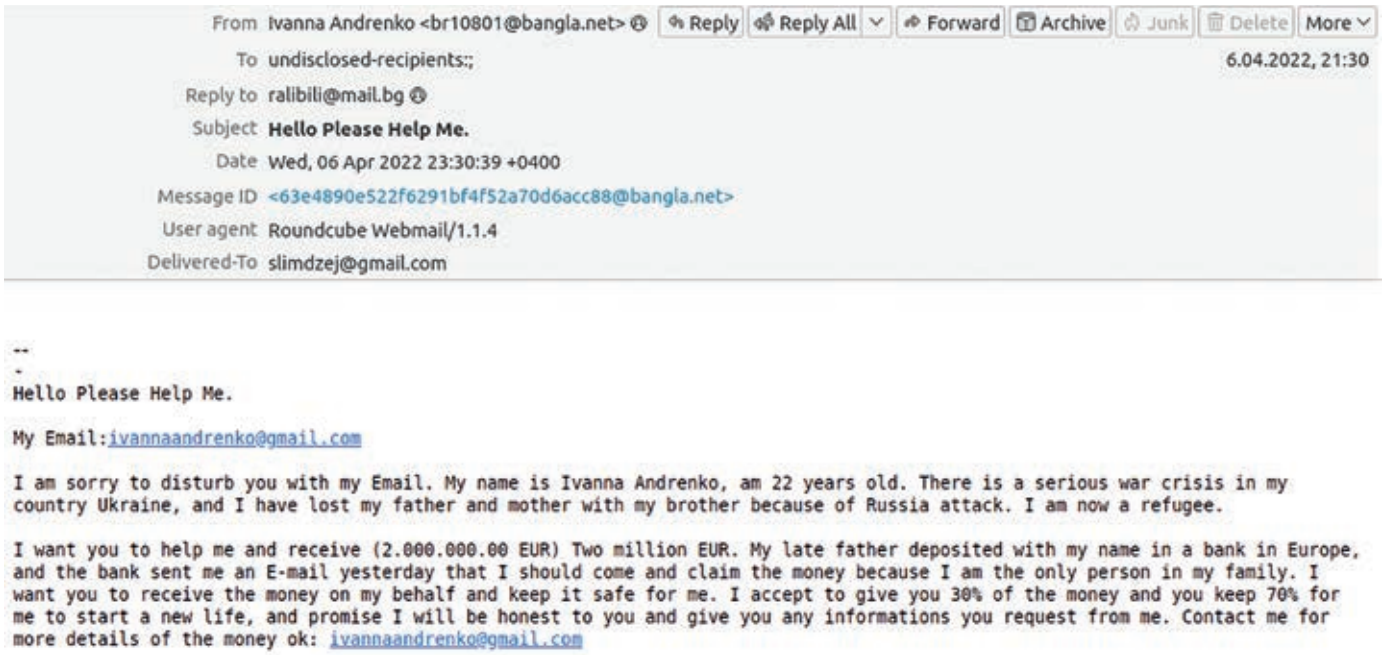
SPAM NIGERYJSKI

Jedno z najstarszych oszustw - spam nigeryjski również znalazł swoje odzwierciedlenie w czasie wojny. Oszuści stworzyli fałszywe postaci, takie jak:

- ukraińska wdowa, której mąż zginął na wojnie,
- strategiczny pracownik NATO mający związek z Ukrainą,
- inżynier okrętowy zaangażowany w wojnę,
- inżynier pracujący w Azovstal,
- 22-letnia Ukrainka, która straciła swoich rodziców na wojnie i potrzebuje pomocy w transferze ogromnej sumy pieniędzy w bezpieczne miejsce.

Chociaż skuteczność tego rodzaju oszustwa nie jest duża, nadal niektóre osoby, zachęcone łatwym zyskiem, tracą oszczędności swojego życia.

Schemat działania oszustów nie odbiega od wcześniej znanych przykładów nigeryjskiego spamu. Ofiara jest przekonywana o możliwości wzbogacenia się, jednak w celu sfinalizowania transakcji musi zapłacić niewielką kwotę. Wraz z zaangażowaniem w rozmowę z niewielkiej kwoty robi się znaczna suma pieniędzy.



From Ivanna Andrenko <br10801@bangla.net> Reply Reply All Forward Archive Junk Delete More
To undisclosed-recipients:; 6.04.2022, 21:30
Reply to ralibili@mail.bg
Subject **Hello Please Help Me.**
Date Wed, 06 Apr 2022 23:30:39 +0400
Message ID <63e4890e522f6291bf4f52a70d6acc88@bangla.net>
User agent Roundcube Webmail/1.1.4
Delivered-To slimdzej@gmail.com

--
-
Hello Please Help Me.

My Email:ivannaandrenko@gmail.com

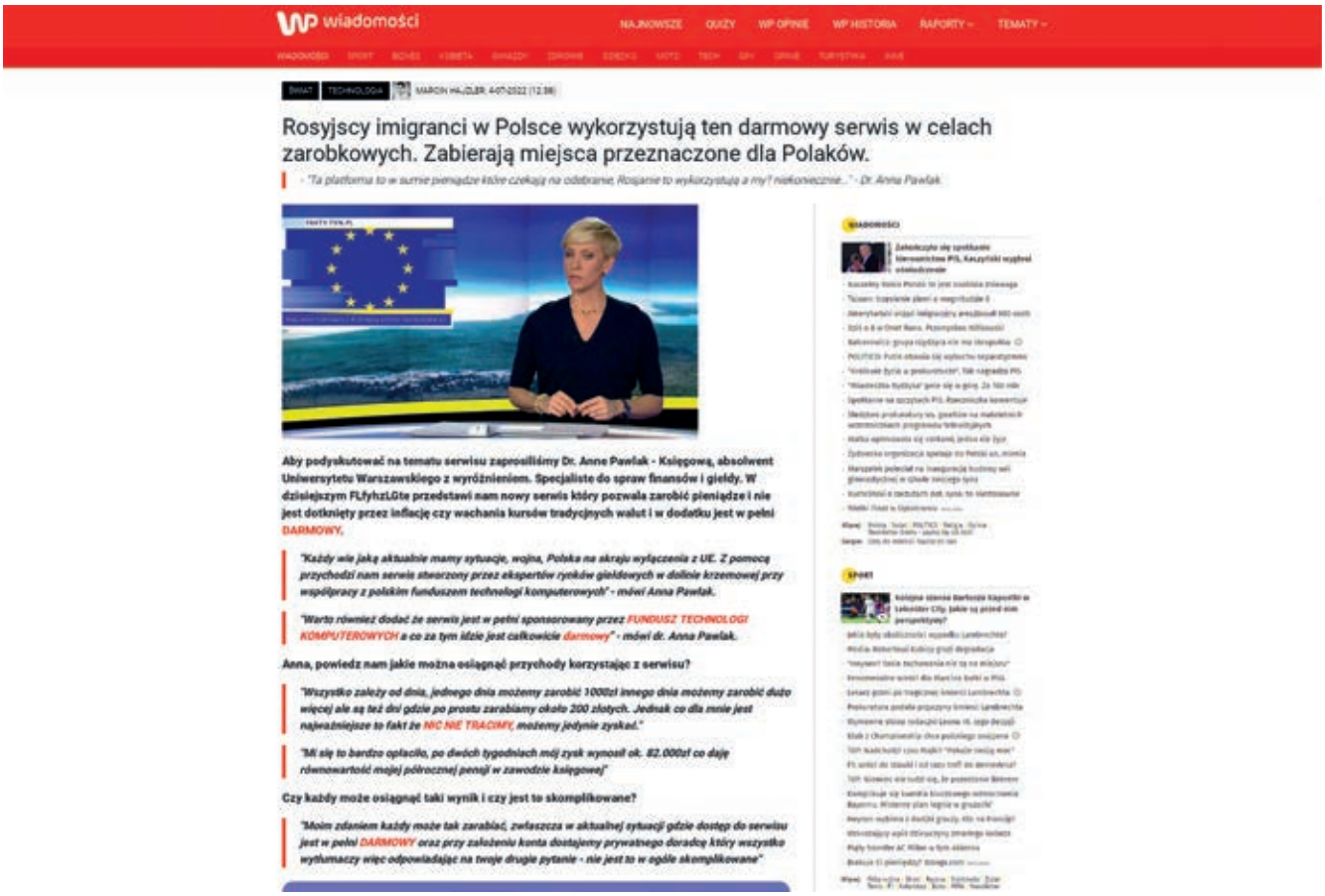
I am sorry to disturb you with my Email. My name is Ivanna Andrenko, am 22 years old. There is a serious war crisis in my country Ukraine, and I have lost my father and mother with my brother because of Russia attack. I am now a refugee.

I want you to help me and receive (2.000.000.00 EUR) Two million EUR. My late father deposited with my name in a bank in Europe, and the bank sent me an E-mail yesterday that I should come and claim the money because I am the only person in my family. I want you to receive the money on my behalf and keep it safe for me. I accept to give you 30% of the money and you keep 70% for me to start a new life, and promise I will be honest to you and give you any informations you request from me. Contact me for more details of the money ok: ivannaandrenko@gmail.com

Rys. 69 Spam nigeryjski wykorzystujący motyw Ukrainy.

FAŁSZYWE INWESTYCJE

Fałszywe inwestycje to kolejny typ oszustwa z wojennym motywem. Skierowana do Polaków kampania reklam opisujących platformy inwestycyjne, za pomocą których można rzekomo szybko wzbogacić się na inwestycjach w kryptowaluty lub akcje firm. Artykuł, który miał zachęcić do inwestowania, sugerował, że rosyjscy imigranci wykorzystują darmowe narzędzie w celu ominięcia sankcji i szybkiego zarobku. Na początku oszuści zachęcają do wpłaty małych kwot na ich platformę, która na początkowym etapie wprowadza błąd, sugerując, że przyrost pieniędzy jest duży. Użytkownik skuszony szybkim zyskiem, wpłaca swoje oszczędności z myślą o zwiększeniu rzekomego zarobku. Jednak przelane pieniądze trafiają finalnie na konta przestępców. Tego typu kampanie były masowo propagowane za pośrednictwem wiadomości mailowych o charakterze spamu.



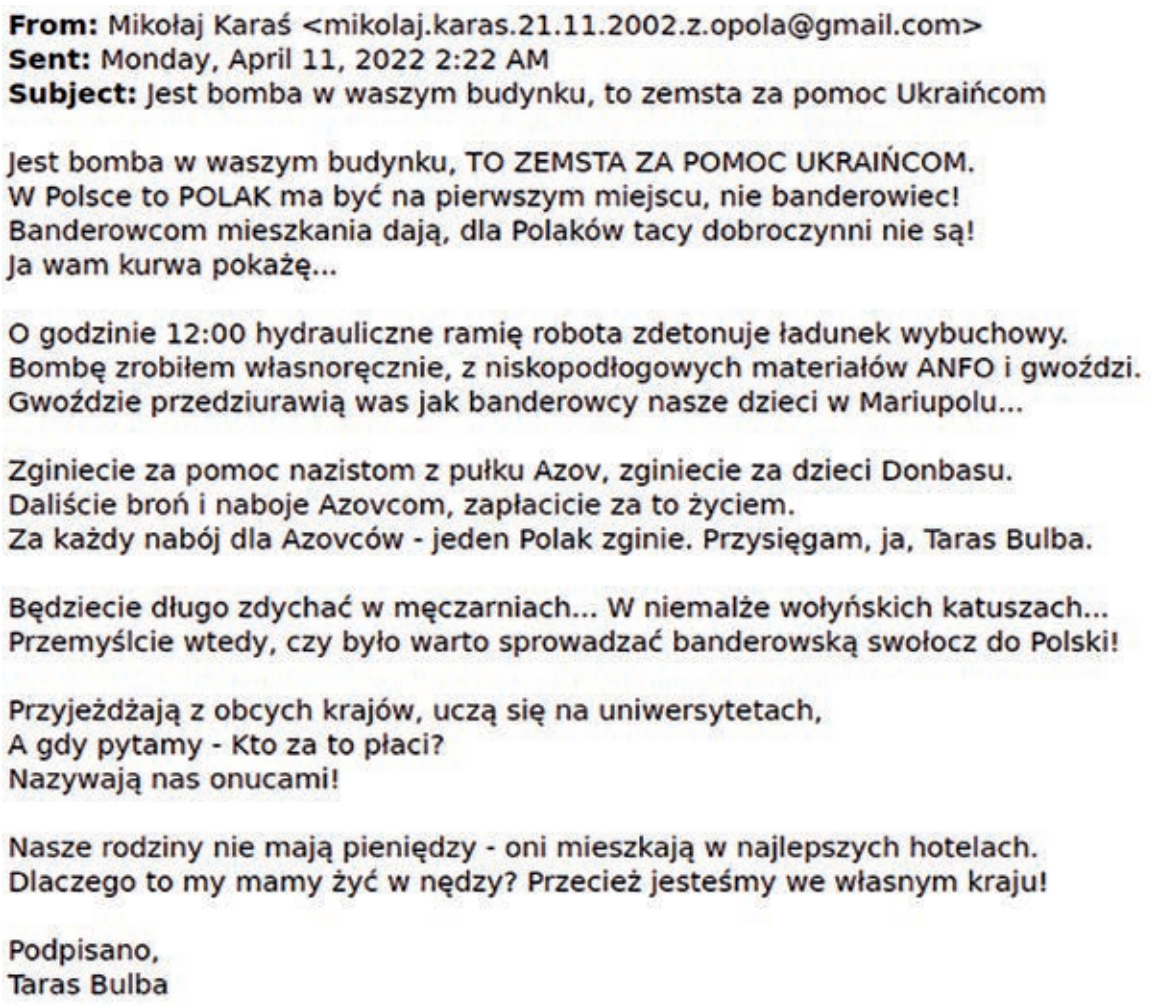
Rys.70 Reklama zachęcająca do inwestowania.

MAILE Z GROŹBAMI

Instytucje i osoby publiczne zmagały się z falą maili o charakterze kaskadowym. Wiadomości zawierały informacje o podłożeniu bomby, dozownika z niebezpiecznym gazem lub innych urządzeń mogących wyrządzić krzywdę osobom znajdującym się we wskazanym w mailu obiekcie. Początkowo zgłoszeniem zajmowały się odpowiednie służby, ale z czasem, z powodu coraz większej powszechności tego rodzaju zagrożenia, wiadomości mailowe z groźbami były klasyfikowane jako informacje o niskiej wiarygodności. Wśród motywów wspomnianych wiadomości można wymienić brak pomocy obywatelom Ukrainy, jak również nadmierną pomoc Ukraińcom. CERT Polska zarejestrował również groźby mailowe o charakterze propagandowym, które celowo miały wzbudzić w Polakach niechęć do Ukrainy i jej obywateli.

W kwietniu 2022 r. na skrzynki pocztowe publicznych szpitali masowo wpływały wiadomości informujące o podłożeniu bomby w ramach zemsty za działania podczas pandemii oraz pomoc ukraińskim uchodźcom.

```
Jestem Ukraiński i zaniosłem bomba do Was budynek.
Bomba wyjebat i zamorduję Lachy.
Bomba wyjebat Wtorek 12:00 godzina.
Śmierć jednego Lacha to metr wolnej Ukrainy.
Albo będzie wolna Ukraina albo lechicka krew po kolana.
Polaków w pień wyciąć.
```



From: Mikołaj Karaś <mikolaj.karas.21.11.2002.z.opola@gmail.com>
Sent: Monday, April 11, 2022 2:22 AM
Subject: Jest bomba w waszym budynku, to zemsta za pomoc Ukraińcom

Jest bomba w waszym budynku, TO ZEMSTA ZA POMOC UKRAIŃCOM.
W Polsce to POLAK ma być na pierwszym miejscu, nie banderowiec!
Banderowcom mieszkania dają, dla Polaków tacy dobroczynni nie są!
Ja wam kurwa pokażę...

O godzinie 12:00 hydrauliczne ramię robota zdetonuje ładunek wybuchowy.
Bombę zrobiłem własnoręcznie, z niskopodłogowych materiałów ANFO i gwoździ.
Gwoździe przedziurawią was jak banderowcy nasze dzieci w Mariupolu...

Zginiecie za pomoc nazistom z pułku Azov, zginiecie za dzieci Donbasu.
Daliście broń i naboje Azovcom, zapłacicie za to życiem.
Za każdy nabój dla Azovców - jeden Polak zginie. Przysięgam, ja, Taras Bulba.

Będziecie długo zdychać w męczarniach... W niemalże wołyńskich katuszach...
Przemyślcie wtedy, czy było warto sprowadzać banderowską swołocz do Polski!

Przyjeżdżają z obcych krajów, uczą się na uniwersytetach,
A gdy pytamy - Kto za to płaci?
Nazywają nas onucami!

Nasze rodziny nie mają pieniędzy - oni mieszkają w najlepszych hotelach.
Dlaczego to my mamy żyć w nędzy? Przecież jesteśmy we własnym kraju!

Podpisano,
Taras Bulba

Rys. 71 Spam o charakterze kaskadowym.

WIADOMOŚCI O CHARAKTERZE SPAMOWYM

Próby ataków na ofiary wycieków danych z różnych serwisów są obserwowane przez analityków nieustannie od lat. Najbardziej popularną kampanią spamową związaną z tematem wojny w Ukrainie, była kampania, w której oszuści podawali się za ukraińskich hakerów. Wiadomości były najczęściej wysyłane na adresy kontaktowe powiązane ze sklepami Internetowymi. Osoby nieuprawnione miały rzekomo przejąć kontrolę nad wspomnianą stroną. Atakujący chcąc wyłudzić pieniądze, sugerowali, że była to darowizna na rzecz Ukrainy. W rzeczywistości był to jednak prywatny portfel kryptowalut. W przypadku braku wpłaty, na przejętej stronie miała pojawić się informacja widoczna dla odwiedzających witrynę. Informacja również miała sugerować darowiznę na rzecz Ukrainy.

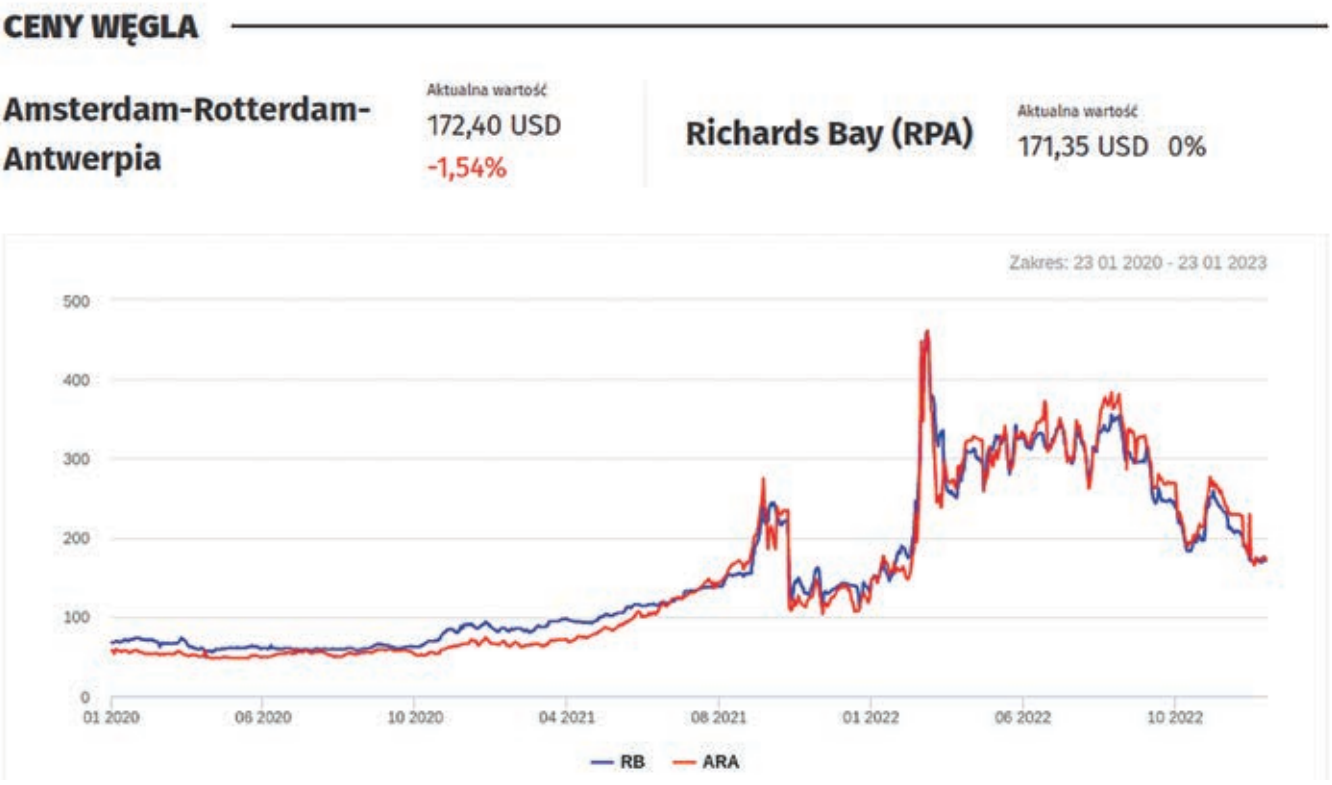
Takie próby wyłudzenia trafiały także na publicznie dostępne adresy e-mail.

Opisane kampanie nie są jedynymi oszustwami, które wykorzystywały motyw wojny w Ukrainie. W sieci można było odnaleźć ogłoszenia wynajęcia pokoju, mieszkania lub całego domu. Osoby z Ukrainy odpowiadały na ogłoszenie, przelewały na konto pieniądze, po czym okazywało się, że takiego lokum nie ma, a rozmowa z osobą kontaktową z ogłoszenia nagle się urywała.

CERT Polska odnotował również liczne wiadomości spamowe odnoszące się do naszych wschodnich sąsiadów. Najczęściej były to wiadomości o charakterze dezinformacyjnym i propagandowym. Dezinformacja pojawiała się również na przejętych stronach Internetowych.

FAŁSZYWE SKLEPY Z WĘGLEM – SKUTEK KRYZYSU ENERGETYCZNEGO ZWIĄZANEGO Z WOJNĄ

Pod koniec 2021 r. oraz od początku 2022 r. mieszkańcy Europy musieli się zmierzyć z rosnącymi cenami energii i surowców grzewczych. Było to spowodowane rozpoczęciem wojny w Ukrainie i faktem, że Rosja przez wiele lat była znaczącym eksporterem paliw na rynek europejski. Skutkiem wybuchu wojny było podpisanie przez prezydenta RP ustawy z 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego. Ustawa wprowadza zakaz przywozu do Polski i tranzytu przez terytorium naszego kraju węgla i koksu pochodzących z Rosji i Białorusi. Na rynkach europejskich ceny węgla gwałtownie rosły, napędzane strachem i masowymi zakupami surowca, które miały zabezpieczyć dostawy na zimę 2022/2023.



Wykres 4. Wykres rosnących cen węgla w kontekście inwazji Rosji na Ukrainę.
https://www.wnp.pl/gornictwo/notowania/ceny_wegla/

Według statystyk z rządowego serwisu dane.gov.pl węgiel kamienny stanowi podstawowe źródło ogrzewania dla 3,8 mln z 15 mln gospodarstw domowych w Polsce, a dodatkowe 800 tys. gospodarstw korzystało z węgla w celu grzewczym. Sprawiło to, że zaczęto masowo kupować dostępne na rynku paliwa stałe, żeby uchronić się przed potencjalnymi problemami w sezonie grzewczym.

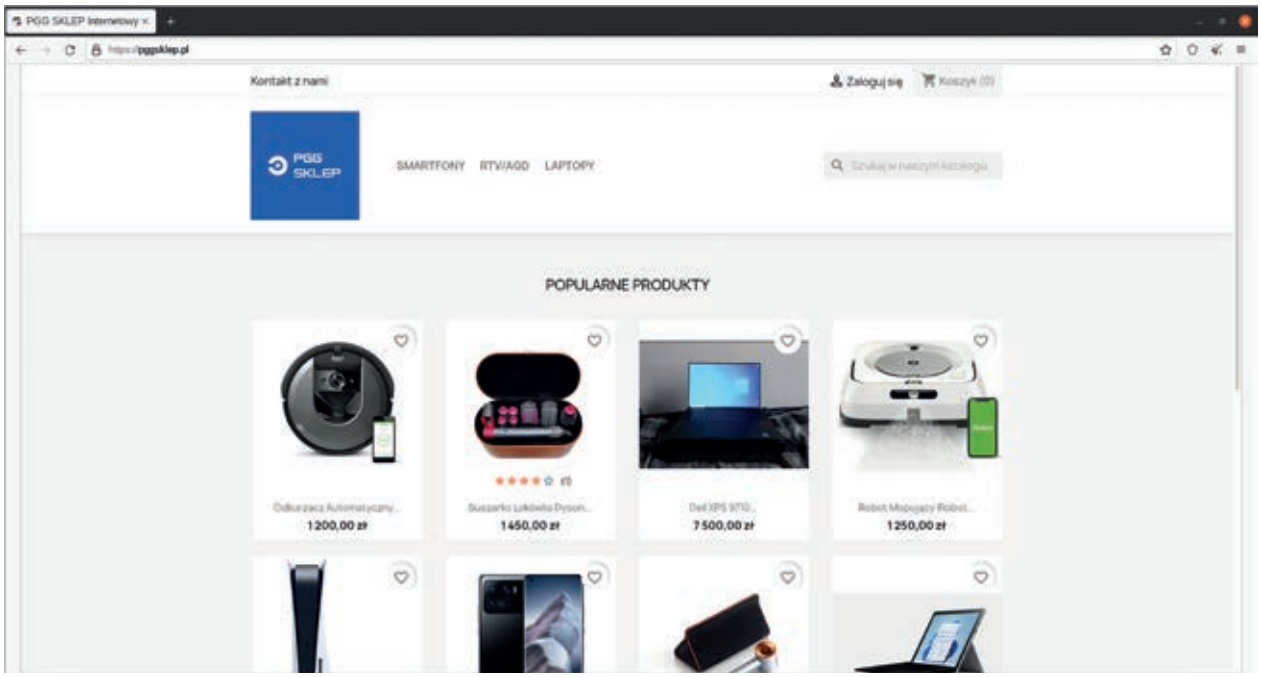
Zainteresowanie było tak duże, że u większości sprzedawców, w tym w sklepie Polskiej Grupy Górniczej, towar był niedostępny przez większość czasu, a sprzedaż prowadzona była tylko w konkretne dni tygodnia.

Źródło: https://dane.gov.pl/pl/dataset/2061,szacunki-danych-o-zuzyciu-energii-w-gospodarstwach/resource/38941

Rys. 72 Informacja o braku towaru na stronie sklep.pgg.pl.

Takie sytuacje są zawsze wykorzystywane przez cyberprzestępców. Na początku pandemii czy wybuchu wojny w Ukrainie praktycznie już od pierwszego dnia pojawiały się fałszywe artykuły, których celem było wyłudzenie danych logowania głównie do serwisu Facebook. Również w tym przypadku przestępcy postanowili wykorzystać medialny temat i desperacje użytkowników Internetu, którzy szukali sposobu na kupno węgla czy pelletu. Sprzyjała też temu niestabilna cena paliw stałych, która potrafiła się zmieniać z tygodnia na tydzień.

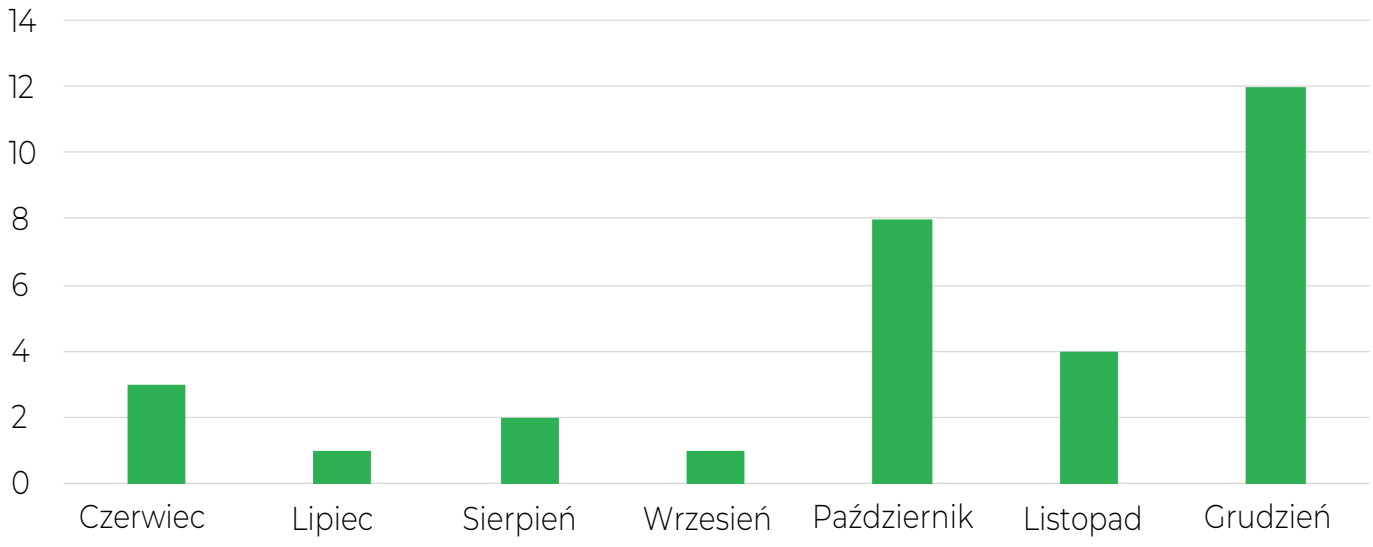
Pierwsze zgłoszenia fałszywych sklepów oferujących sprzedaż węgla czy pelletu trafiły do naszego zespołu w czerwcu 2022 r. Sklepy oferowały sprzedaż tych paliw w przedziale od 1200 do 1500 zł, co już wtedy było ceną kilkaset złotych niższą od średniej rynkowej, która zbliżała się wówczas do 2000 złotych.



Rys. 73 Zrzut strony głównej fałszywego sklepu.

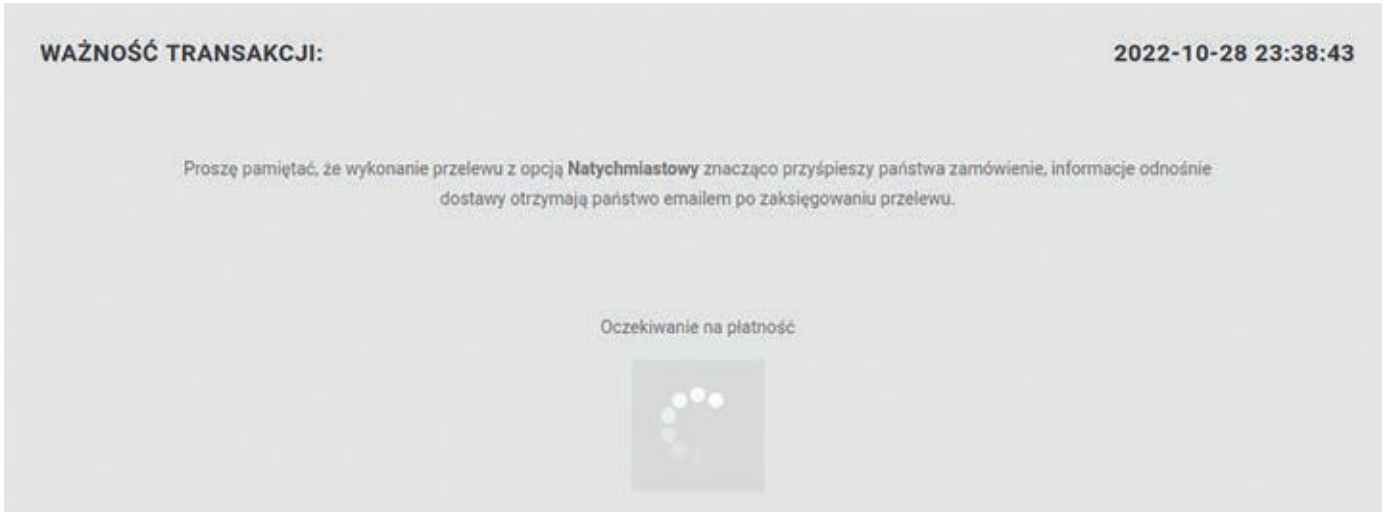
Najciekawszym przypadkiem zaobserwowanym przez CERT Polska był sklep podszywający się pod oficjalną platformę sprzedażową Polskiej Grupy Górniczej. Zgodnie ze zgłoszeniami użytkowników oraz analizą poczynioną przez nasz zespół przestępcy eksponowali na głównej stronie sklepu paliwa stałe synchronicznie z trwającymi sesjami sprzedażowymi na oficjalnej stronie sklep.pgg.pl, aby następnie wystawić zaślepkę w postaci sklepu oferującego sprzęt elektroniczny. Prawdopodobnym celem było utrudnienie weryfikacji zjawiska przez naszych analityków i przedłużenie okresu funkcjonowania fałszywego sklepu.

Zjawisko nasiliło się wraz ze zbliżającym się okresem grzewczym. Przestępcy najczęściej wykorzystywali markę Polskiej Grupy Górniczej. W grudniu nasz zespół zaobserwował aż 12 fałszywych sklepów, z których 7 wykorzystywało w domenie nazwę PGG.



Wykres 5. Liczba fałszywych sklepów oferujących sprzedaż węgla w 2022 roku.

Standardowo dla tego typu sklepów, płatność można było zrealizować jedynie przelewem bankowym. W takim przypadku odzyskanie przez ofiarę pieniędzy jest trudniejsze niż przy płatności kartą, która może oferować mechanizm chargeback. Fałszywe sklepy namawiają ofiarę do wykonania przelewu natychmiastowego, jako powód podając na przykład szybszą realizację usługi.



Rys. 74 Informacja zachęcająca do wykonania przelewu natychmiastowego.

Jak przeciwdziałać temu zjawisku?

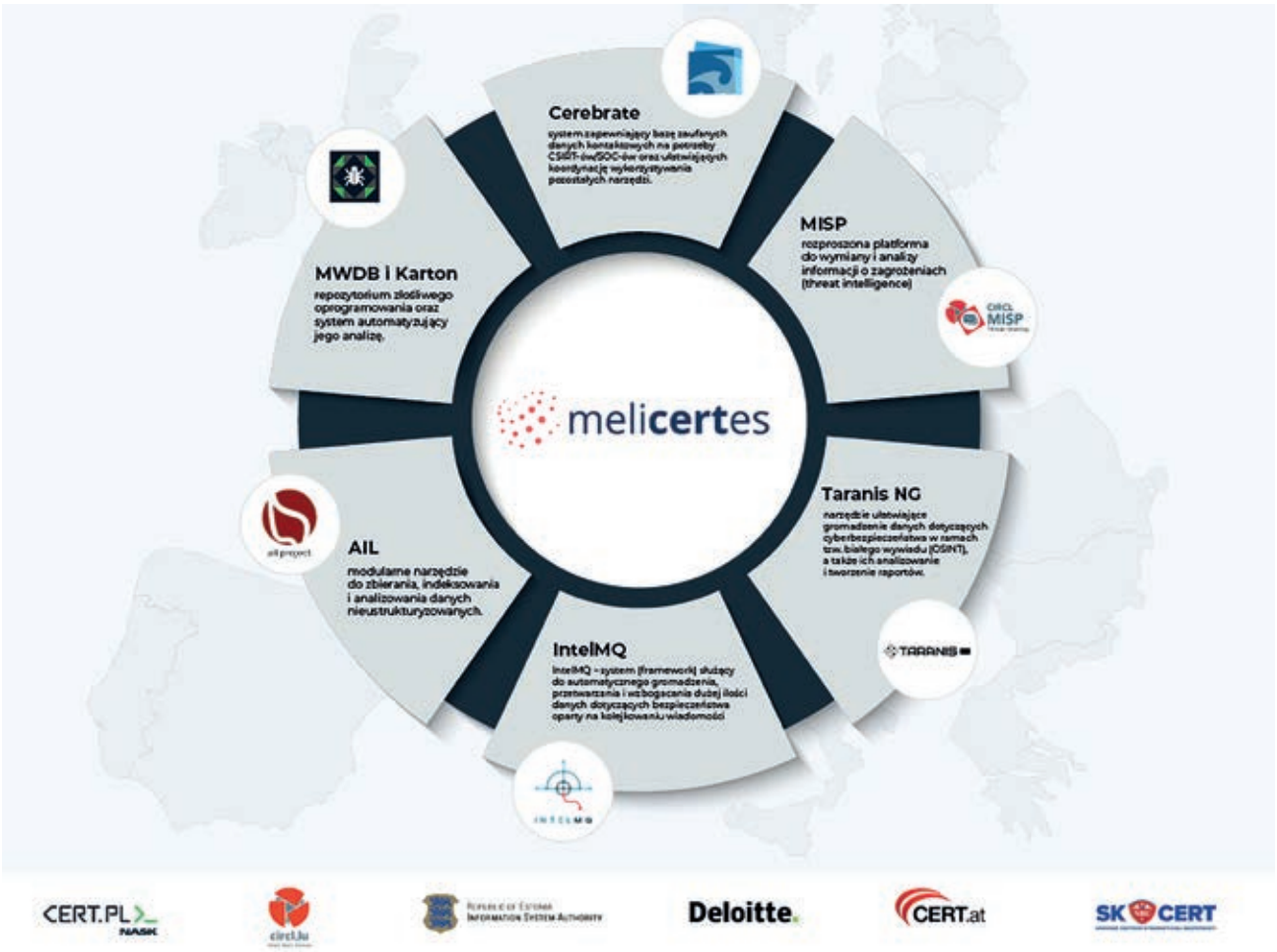
W celu zwalczania stron, które jawnie służą do wyłudzania środków finansowych od polskich użytkowników Internetu, prowadzimy listę ostrzeżeń przed niebezpiecznymi stronami. W przypadku fałszywych sklepów sprzedających węgiel również miała ona zastosowanie i dzięki wpisaniu domen na listę udało się zablokować aż 27 311 prób wejść.

Jeśli chcesz czuć się bezpieczniej robiąc zakupy przez Internet zachęcamy do zapoznania się ze stworzonym przez nas poradnikiem na temat bezpiecznych zakupów online. Poradnik dostępny jest na naszej stronie pod adresem: https://cert.pl/uploads/docs/CERT_poradnik_zakupowy.pdf

PROJEKTY CERT POLSKA

MELICERTES

Wraz z końcem roku 2022 sfinalizowaliśmy trwający trzy lata projekt MeliCERTes (kontrakt SMART 2018/1024), którego celem było stworzenie platformy wspierającej współpracę europejskich zespołów CSIRT oraz ich działania operacyjne.



Rys. 75 Narzędzia open source wchodzące w skład MeliCERTes.

Nasz zespół pełnił rolę głównego koordynatora projektu, a w prace nad platformą MeliCERTes zaangażowane były jeszcze cztery europejskie CSIRT-y: CERT.at (Austria), CERT-EE (Estonia), CIRCL (Luksemburg) oraz SK-CERT (Słowacja). W konsorcjum uczestniczyła również firma Deloitte (Belgia).

Podstawowym celem stworzenia platformy MeliCERTes jest wsparcie strategii Komisji Europejskiej w zakresie cyberbezpieczeństwa poprzez:

- umożliwienie efektywnej komunikacji w ramach Sieci CSIRT,
- rozwój i udostępnienie przydatnych narzędzi open source, używanych i utrzymywanych przez CSIRT-y.

Projekt ma też na celu wsparcie instytucji europejskich w realizacji długoterminowych działań, takich jak osiągnięcie suwerenności cyfrowej oraz promocja zaufanych i transgranicznych usług cyfrowych.

Główną rolą CERT Polska było opracowanie koncepcji całej platformy oraz koordynacja działań konsorcjum. Oprócz tego nasz zespół realizował również zadania techniczne związane z integracją finalnej platformy MeliCERTes.

REZULTATY PROJEKTU

Podstawowym osiągnięciem projektu jest stworzenie platformy MeliCERTes, która składa się z dwóch głównych części. Do pierwszej należy zestaw narzędzi open source[27], które są wykorzystywane przez zespoły CSIRT, SOC oraz inne komórki zajmujące się cyberbezpieczeństwem w sektorze publicznym i prywatnym. Drugą grupę tworzą natomiast narzędzia, które ENISA wdraża na potrzeby Sieci CSIRT (CSIRTs Network, ustanowiona dyrektywą NIS).

W ramach projektu powstało nowe narzędzie o nazwie Cerebrate, opracowane specjalnie na potrzeby platformy MeliCERTes. Ulepszone zostały również wszystkie pozostałe narzędzia open source.

NARZĘDZIA WCHODZĄCE W SKŁAD PLATFORMY

Cerebrate: system zapewniający bazę zaufanych danych kontaktowych na potrzeby CSIRT-ów/SOC-ów oraz ułatwiających koordynację wykorzystywania pozostałych narzędzi. https://cerebrate-project.org/

MISP: rozproszona platforma do wymiany i analizy informacji o zagrożeniach (threat intelligence). https://www.misp-project.org/

Taranis NG: narzędzie ułatwiające gromadzenie otwartych danych dotyczących cyberbezpieczeństwa (OSINT), a także ich analizowanie i tworzenie raportów. https://taranis.ng/

IntelMQ: system (framework) służący do automatycznego gromadzenia, przetwarzania i wzbogacania dużej ilości danych dotyczących bezpieczeństwa oparty na kolejkowaniu wiadomości. https://github.com/certtools/intelmq/

AIL: modularne narzędzie do zbierania, indeksowania i analizowania danych nieustrukturyzowanych. https://www.ail-project.org/

MWDB i Karton: repozytorium złośliwego oprogramowania oraz system automatyzujący jego analizę. https://github.com/CERT-Polska/mwdb-core

PRZYSZŁOŚĆ PROJEKTU

W listopadzie 2022 r. została zorganizowana w Brukseli konferencja, w której aktywny udział wzięli przedstawiciele Komisji Europejskiej, HaDEA (Europejska Agencja Wykonawcza ds. Zdrowia i Cyfryzacji) oraz beneficjenci projektów cyberbezpieczeństwa z krajów Unii Europejskiej. Uczestnicy podsumowali efekty finansowania cyberbezpieczeństwa z programu Connecting Europe Facility[28] oraz projektu MeliCERTes. Uzgodniono, że platforma będzie dalej utrzymywana i rozwijana, w celu zapewnienia otwartych narzędzi współpracy dla CSIRT-ów w ramach UE.

Projekt MeliCERTes jest przykładem udanej współpracy europejskich CSIRT-ów przy rozwoju narzędzi, które wspierają działania operacyjne. Formalnie projekt został zakończony, natomiast narzędzia open source wchodzące w jego skład będą dalej rozwijane przez CSIRT-y i społeczność użytkowników.

27 https://github.com/melicertes/docs
28 https://hadea.ec.europa.eu/programmes/cef-old/cef-telecom_en

W 2022 r. zakończył się projekt CyberExchange, który wspierał wymianę wiedzy i doświadczeń pomiędzy 11 europejskimi CSIRT-ami. Projekt rozpoczął się w 2018 r. i planowo miał zakończyć się w 2020 r., jednak pandemia COVID-19 spowodowała przedłużenie go o ponad rok. Oprócz CERT Polska udział w nim brały udział zespoły z Austrii, Chorwacji, Czech, Grecji, Łotwy, Luksemburga, Malty, Rumunii i Słowacji. Liderem konsorcjum było czeskie stowarzyszenie CZ.NIC, w ramach którego funkcjonuje CSIRT.CZ.

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

Nasz zespół gościł przedstawicieli CERT.at, CERT.LV i CERT.hr, SK-CERT, CSIRT Malta. Jednym z głównych tematów wspólnych prac i dyskusji były narzędzia wspierające działania operacyjne, takie jak analiza złośliwego oprogramowania.

Projekt był współfinansowany z funduszy Unii Europejskiej w ramach instrumentu „Łącząc Europę”, numer grantu 2017-EU-IA-0118.

JTAN

CERT Polska koordynuje projekt Joint Threat Analysis Network, w którym biorą udział europejskie CSIRT-y krajowe: CIRCL (Luksemburg), CERT.LV (Łotwa), CERT.at (Austria), SK-CERT (Słowacja), CERT-EE (Estonia), DNSC (Rumunia) oraz firma Corexalys (Francja).

Główny cel JTAN to rozwój narzędzi do pozyskiwania, analizy oraz wymiany informacji o zagrożeniach (Cyber Threat Intelligence). Projekt rozpoczął się w 2021 r. i prace będą trwać do 2024 r.

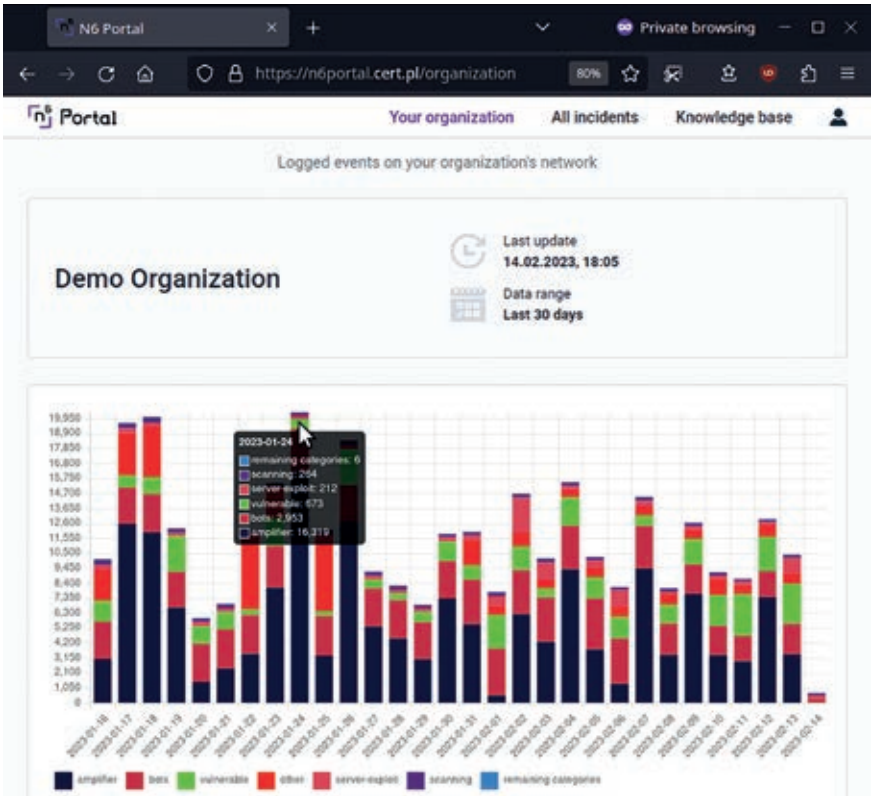
W ramach projektu rozwijane są narzędzia open source:

- AIL – system do zbierania, indeksowania i analizowania danych nieustrukturyzowanych związanych z bezpieczeństwem.
- Graphoscope – narzędzie wspomagające pracę analityków poprzez integrację i wizualizację danych z wielu źródeł.
- Taranis NG – system automatyzujący pozyskiwanie informacji z otwartych źródeł (OSINT) i ułatwiający ich analizę.
- n6 i MWDB tworzone przez CERT Polska, o których bardziej szczegółowo piszemy poniżej.

Projekt jest współfinansowany z funduszy Unii Europejskiej w ramach instrumentu „Łącząc Europę”, numer grantu 2020-EU-IA-0260.

W ramach projektu wprowadziliśmy szereg ulepszeń w systemie n6. Te najbardziej widoczne pojawiły się na stronie startowej w portalu n6[29]. Po zalogowaniu użytkownik ma dostępny wykres zdarzeń wewnątrz sieci organizacji na przestrzeni ostatnich 30 dni (Rys. 76). Kolejną zmianą widoczną dla użytkowników jest dodanie do portalu bazy wiedzy, w której zamieszczamy najważniejsze informacje dotyczące korzystania z systemu n6. W ubiegłym roku dodaliśmy również nowe źródła danych, przede wszystkim w kategoriach phishing oraz podatne urządzenia. Znaczącą integracją było dodanie danych z platformy Domain Trust utrzymywanej przez Global Cyber Alliance[30].

Ponadto wdrożyliśmy wiele poprawek w silniku n6 oraz rozbudowaliśmy funkcjonalność interfejsu administracyjnego. Kod źródłowy n6 jest dostępny w serwisie GitHub: https://github.com/CERT-Polska/n6



Rys. 76 Nowy widok zdarzeń w sieci uczestnika n6 (dane przykładowe).

29 https://n6portal.cert.pl/
30 https://www.nask.pl/pl/aktualnosci/4883,NASK-podpisal-umowe-o-wspolpracy-z-Global-Cyber-Alliance.html

W ubiegłym roku aktywnie rozwijaliśmy wersję open source MWDB[31].

Dodaliśmy wsparcie dla protokołu OpenID Connect umożliwiającego uwierzytelnianie poprzez zewnętrznych dostawców tożsamości. Ta funkcjonalność jest szczególnie przydatna przy bardziej złożonych wdrożeniach MWDB, w pierwszej kolejności będziemy jej używać dla uwierzytelniania użytkowników z europejskiej Sieci CSIRT-ów[32].

Pozostałe ulepszenia to m.in:

- dodanie ustrukturyzowanych atrybutów w formacie JSON;
- możliwość tworzenia własnych szablonów do niestandardowej prezentacji atrybutów w interfejsie webowym;
- poprawiona wydajność wyszukiwania;
- dodane wsparcie dla uwierzytelniania poprzez mechanizm AWS IAM, co pozwala na łatwiejszą integrację z usługą Amazon S3 do przechowywania próbek złośliwego oprogramowania.

Pracowaliśmy również nad poprawieniem jakości kodu, m.in. w obszarze autoryzacji i interfejsu użytkownika, który w MWDB oparliśmy na frameworku React.

31 https://github.com/CERT-Polska/mwdb-core
32 https://csirtsnetwork.eu/

STATYSTYKI

W tej części raportu prezentujemy statystyki dotyczące zdarzeń przetwarzanych automatycznie, przede wszystkim z wykorzystaniem platformy n6[33]. Dotyczą one podatnych systemów, prawdopodobnych infekcji lub skutecznych ataków w polskich sieciach, które zostały pozyskane z zewnętrznych źródeł, a następnie zaraportowane do CERT Polska. Dane takie są agregowane, normalizowane i udostępniane bezpłatnie właścicielom sieci oraz odpowiednim zespołom CSIRT.

OGRANICZENIA

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

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

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

BOTNETY

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

BOTNETY W POLSCE

Tabela 3 prezentuje liczbę zainfekowanych komputerów w polskich sieciach. W 2022 r. łącznie zgromadziliśmy informacje o 302 696 adresach IP wykazujących aktywność botów. Porównując z poprzednimi latami po raz kolejny odnotowaliśmy spadek – o około 140 tys. w porównaniu z 2021 r. i o około 340 tys. w porównaniu z 2020 r.

33 https://n6.cert.pl/

	Rodzina	Maksimum dzienne	Średnia dzienna	Odchylenie standardowe
1	Andromeda	2 127	1 244	379
2	Avalanche	1 444	587	135
3	Mirai	920	431	136
4	Conficker	668	349	104
5	QSnatch	651	508	97
6	Gamut	483	102	108
7	Sality	418	159	103
8	ISFB	396	71	94
9	Nymaim	371	53	27
10	Necurs	316	144	48

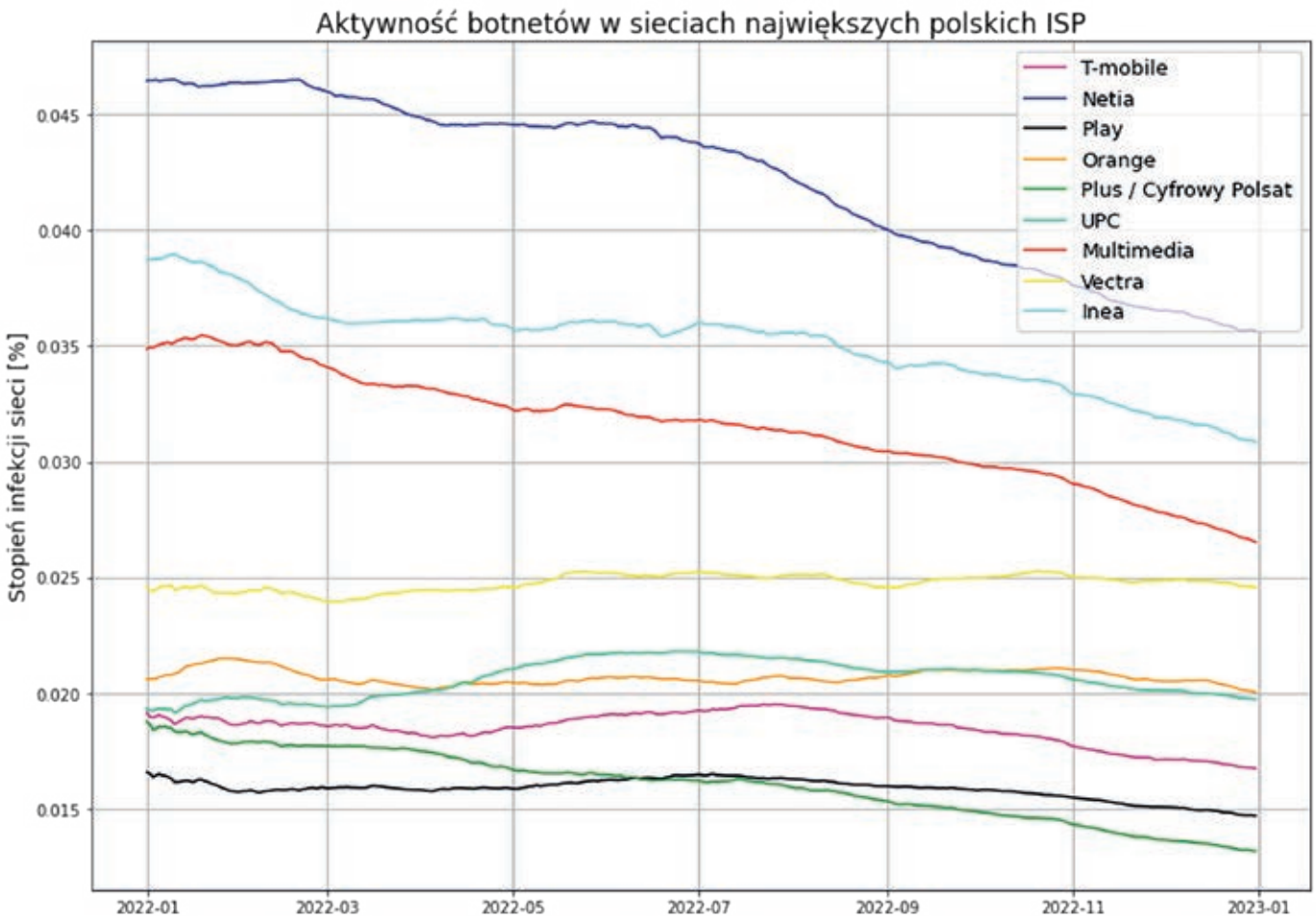
Tab. 3. Największe botnety w Polsce.

W polskich sieciach od lat obserwujemy aktywność botnetów, które już są sinkholowane. Przykładem jest botnet Andromeda, który po raz kolejny znalazł się na pierwszym miejscu powyższego zestawienia ze średnią dzienną liczbą zainfekowanych urządzeń na poziomie około 1,2 tys. Przypomnijmy, że w 2021 r. ta liczba wynosiła niemal 2 tys., więc widoczny jest znaczny spadek. Również w skali roku obserwujemy tendencję spadkową: na początku roku średnio notowaliśmy wartości bliskie 2 tys. adresów IP, natomiast w końcówce roku poziom ten zbliżył się do tysiąca adresów. Trend spadkowy zarejestrowaliśmy także w infekcjach urządzeń QNAP Systems botnetem QSnatch - spadek o około 200 adresów IP porównując wartości z początku i końca 2022 r. Tendencja spadkowa jest też widoczna w przypadku botnetu Necurs. Po raz kolejny w zestawieniu pojawia się rodzina botnetów IoT Mirai. Warto podkreślić jej wyższą pozycję w zestawieniu w porównaniu z ubiegłym rokiem. Średnio 431 urządzeń IoT z adresami IP wykazywało infekcję tą rodziną. Po spadku o około 200 adresów między 2020 r. i 2021 r. tym razem odnotowaliśmy wzrost o około 100 adresów.

INFEKCJE 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 2021 roku" wydanego przez Urząd Komunikacji Elektronicznej[34].

34 https://www.uke.gov.pl/download/gfx/uke/pl/defaultaktualnosci/36/431/13/raport_o_stanie_rynku_telekomunikacyjnego_w_polsce_w_2021_r..pdf



Wykres 6. Aktywność botnetów w sieciach największych ISP w 2022 r.

W 2022 r. średnia dzienna liczba zainfekowanych urządzeń w polskim internecie wynosiła 4 121. Na przestrzeni roku obserwujemy niewielką tendencję spadkową. W styczniu 2022 r. w polskich sieciach stopień infekcji wynosił około 4,5 tys. urządzeń. Wartość ta utrzymywała się na stałym poziomie do połowy roku. Następnie w drugiej połowie roku obserwowaliśmy spadek i w końcówce roku liczba ta zatrzymała się na około 3,5 tys. urządzeń.

Stopień infekcji sieci w przypadku żadnego z operatorów nie przekraczał pół promila. Podobnie jak w ubiegłych latach największy odsetek zainfekowanych użytkowników oszacowaliśmy w sieciach Netia. W przypadku tego operatora zachowany został malejący trend, szczególnie widoczny w drugiej połowie roku. Po raz kolejny na drugim i trzecim miejscu pod względem stopnia infekcji znaleźli się kolejno operatorzy INEA oraz Multimedia. W obu przypadkach obserwujemy tendencję spadkową, jednak spadek ten nie jest aż tak znaczny na przestrzeni roku jak w 2021 r. W przypadku pozostałych operatorów stopień infekcji sieci utrzymuje się na podobnym stałym poziomie w przeciągu roku. Wyjątkiem jest tu Plus / Cyfrowy Polsat gdzie widoczna jest tendencja spadkowa. Operatorzy Play oraz Plus / Cyfrowy Polsat wypadają w tym zestawieniu najkorzystniej, stopień infekcji jest u nich najniższy.

W przypadku botnetu Andromeda, podobnie jak w ubiegłym roku, największą liczbę zainfekowanych urządzeń obserwujemy w sieciach Orange oraz Plus / Cyfrowy Polsat. Dzienna liczba adresów IP utrzymuje się na poziomie powyżej 300 adresów w przypadku Orange oraz powyżej 200 w przypadku Plusa / Cyfrowego Polsatu. Infekcje botnetem Avalanche obserwowaliśmy najczęściej u operatorów Plus / Cyfrowy Polsat. Liczba ta utrzymywała się na poziomie 100 urządzeń. Najwięcej zainfekowanych urządzeń NAS mają użytkownicy w sieciach Orange (średnio 170 urządzeń) oraz UPC (średnio 60

urządzeń). W pozostałych sieciach problem infekcji botnetem QSnatch był marginalny. Podobnie jak w ubiegłym roku infekcje botnetem Mirai obserwowaliśmy głównie w sieciach Orange, a u pozostałych operatorów liczba ta była nieznaczna. Infekcje botnetem Conficker obserwowaliśmy najczęściej u operatorów Orange oraz Netia (średnio 50 urządzeń w obu przypadkach).

SERWERY C&C

C&C NA ŚWIECIE

W 2022 r. zebraliśmy informacje o 8 570 adresach IP prawdopodobnie używanych jako serwery do zarządzania botnetami (Command & Control, C&C). Jest to liczba zbliżona do tej, którą odnotowaliśmy w zeszłym roku (9 410 adresów), jednak znacznie mniejsza niż w 2020 r. (64 653 adresów). Wynika to m.in. z faktu, że część źródeł dostarczających nam tego rodzaju dane jest nieaktywna.

Z uwagi na charakter zagrożenia zdecydowaliśmy się na opisanie problemu uwzględniając 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. Spośród 131 krajów, w których odnotowaliśmy obecność serwerów C&C, najwięcej z nich było zlokalizowanych w Stanach Zjednoczonych (3 386).

Poz.	Kraj	Liczba adresów IP	Udział
1	Stany Zjednoczone	3 386	39,51%
2	Rumunia	550	6,42%
3	Holandia	358	4,18%
4	Niemcy	273	3,19%
5	Rosja	236	2,75%
6	Meksyk	208	2,43%
7	Zjednoczone Emiraty Arabskie	201	2,35%
8	Francja	194	2,26%
9	Kanada	191	2,23%
10	Wielka Brytania	190	2,22%
...	...	...	...
40	Polska	29	0,34%

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

Zaobserwowaliśmy 1 275 różnych systemów autonomicznych (AS), w których umiejscowione były serwery C&C. Dziesięć systemów autonomicznych zawierało około 26 proc. wszystkich złośliwych serwerów, a najpopularniejszym z nich był Cloudflare, który bardzo często jest wykorzystywany do ukrycia prawdziwego adresu serwera. Jak można zauważyć w tabeli 5, zgodnie z zestawieniem w tabeli 4, najwięcej systemów autonomicznych jest zarejestrowanych w Stanach Zjednoczonych.

Poz.	Numer AS	Nazwa	Kraj	Liczba IP	Udział
1	13335	Cloudflare	Stany Zjednoczone	356	4,15%
2	8708	RCS-RDS	Rumunia	311	3,63%
3	7922	COMCAST	Stany Zjednoczone	302	3,52%
4	211252	DELIS	Stany Zjednoczone	227	2,65%
5	14061	DigitalOcean	Stany Zjednoczone	202	2,36%
6	701	Verizon	Stany Zjednoczone	194	2,26%
7	5384	Emirates Telecommunications Corporation	Zjednoczone Emiraty Arabskie	190	2,22%
8	8151	Uninet	Meksyk	170	1,98%
9	16509	Amazon	Stany Zjednoczone	153	1,79%
10	209	CenturyLink Communications	Stany Zjednoczone	146	1,70%

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

Otrzymaliśmy również zgłoszenia o 2 815 pełnych nazwach domenowych (FQDN), które pełniły rolę serwerów zarządzających botnetami. Zostały one zarejestrowane w obrębie 155 domen najwyższego poziomu (TLD), z czego prawie 44 proc. w domenie .com. W tym roku nie odnotowaliśmy żadnych serwerów C&C wykorzystujących domenę .pl. Zestawienie najpowszechniejszych TLD przedstawiamy w tabeli 6. Jak można zauważyć, ponad 62 proc. wszystkich domen zarejestrowanych jest na najpopularniejszych TLD (.com, .net i .org), jednak widać też udział mniej popularnych domen takich jak .xyz, .top czy .online. Co ciekawe, wśród 10 najpopularniejszych TLD zaobserwowaliśmy tylko 2 domeny krajowe (ccTLD): .ru (domena Rosji) oraz .cf (domena Republiki Środkowoafrykańskiej).

Poz.	TLD	Liczba domen	Udział
1	com	1 238	43,98%
2	net	260	9,24%
3	org	256	9,09%
4	xyz	173	6,15%
5	top	68	2,42%
6	ru	56	1,99%
7	online	52	1,85%
8	info	48	1,71%
9	cf	31	1,10%
10	site	27	0,96%

Tab. 6. Najpowszechniejsze domeny najwyższego poziomu, pod którymi znajdowały się serwery zarządzające botnetami.

C&C W POLSCE

W Polsce serwery C&C były aktywne pod 29 różnymi adresami IP (30 miejsce na świecie) w 19 systemach autonomicznych. Jest to mniej niż w 2021 r., kiedy zebraliśmy informacje o 59 polskich adresach IP w 34 systemach autonomicznych, jednak nie możemy wyciągać wniosków na tej podstawie, ze względu na mniejszą liczbę źródeł danych niż rok temu.

Systemami autonomicznymi, w których znajdowało się najwięcej polskich adresów IP są: Orange (AS5617, 8 adresów), GHOST (AS202422, 2 adresy), GigaHostingServices (AS213010, 2 adresy) oraz Google (AS396982, 2 adresy).

PHISHING

PHISHING HOSTOWANY W POLSKICH SIECIACH

W tym podrozdziale uwzględniamy wyłącznie statystyki dotyczące phishingu w tradycyjnym rozumieniu tego słowa, czyli jedynie podszywania się pod pod znane marki w celu wyłudzenia wrażliwych danych z wykorzystaniem poczty elektronicznej i stron WWW. Przykładowo, nie uwzględniamy w tej kategorii podszywania się pod dostawców faktur w celu dystrybucji złośliwego oprogramowania.

W 2022 r. otrzymaliśmy łącznie 29578 zgłoszeń phishingu w polskich sieciach. Są to wszystkie zgłoszenia, niezależnie od tego czy celem ataku byli polscy użytkownicy. Dotyczyły one 18618 adresów URL z 16086 domenami, które rozwiązywały się na 1962 adresy IP. Oznacza to bardzo duży wzrost w porównaniu z zeszłym rokiem. Ta zmiana wynika m.in. z faktu wykorzystania nowego źródła danych – od sierpnia zapisujemy informacje na temat zagrożeń pozyskanych od Global Cyber Alliance. W tabeli 7 wymieniliśmy 10 systemów autonomicznych, w których znajdowało się najwięcej stron phishingowych. Tak jak w poprzednich latach, można zauważyć znaczący udział home.pl w porównaniu z innymi systemami autonomicznymi, co może wynikać z taniej oferty handlowej tej firmy.

Poz.	Numer AS	Nazwa	Liczba adresów IP	Liczba domen
1	12824	home.pl	482	2 078
2	20940	Akamai Technologies	180	88
3	15967	Nazwa.pl	162	2 670
4	41079	H88	107	1 426
5	16276	OVH	91	623
6	197226	Sprint	66	195
7	29522	KEI	58	166
8	203417	LH.pl	51	1 110
9	198414	H88	40	236
10	57367	Atman	39	290

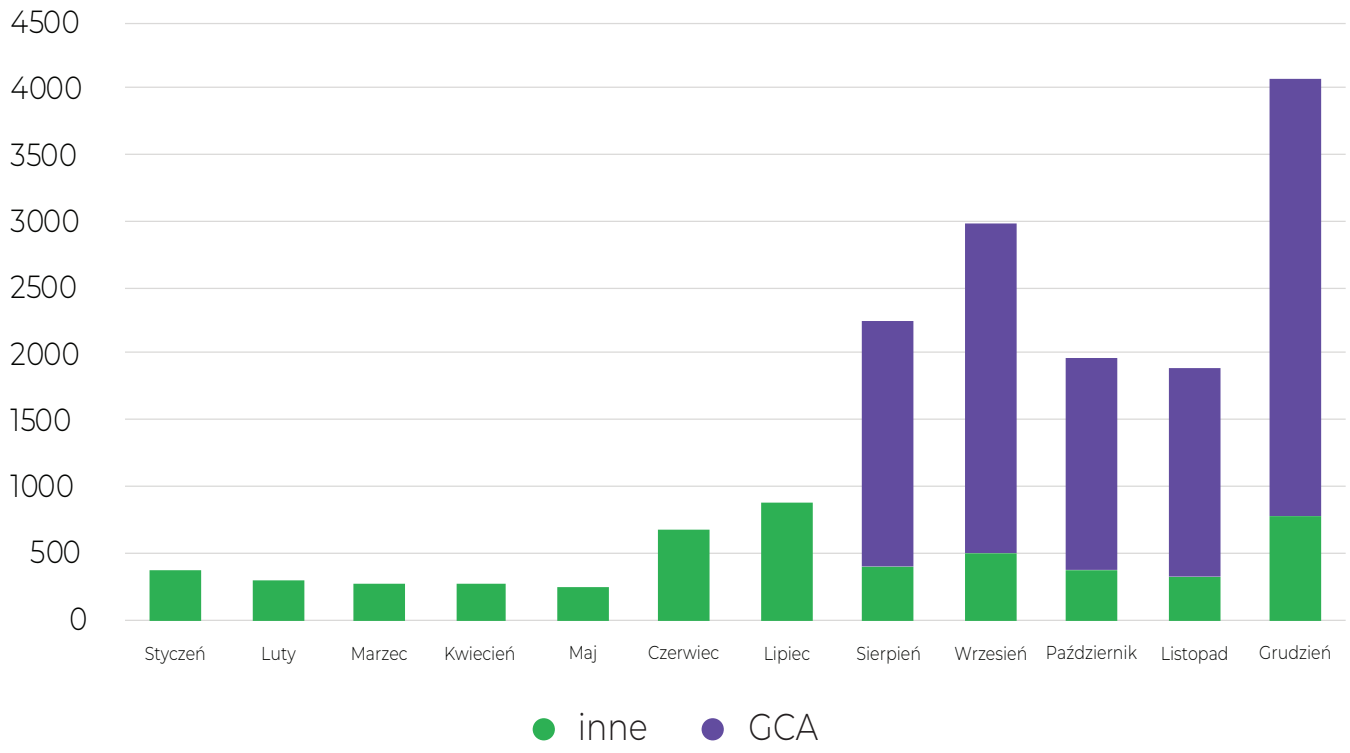
Tab. 7. Polskie systemy autonomiczne, w których znajdowało się najwięcej stron phishingowych.

Wśród zaobserwowanych przez nas nazw domenowych znajdowało się 235 różnych TLD (ang. Top-Level Domain). Dwie najpopularniejsze z nich, czyli .com oraz .pl stanowiły ponad 65 proc. wszystkich zgłoszonych nazw domenowych. Ich popularność może wynikać m.in. z większego zaufania użytkowników do tych domen. Przestępcy mogą decydować się na nie ze względu na niższą cenę rejestracji domeny lub ze względu na większą dostępność nazw.

Poz.	TLD	Liczba domen	Udział
1	com	6 690	41,59%
2	pl	3 775	23,47%
3	online	592	3,68%
4	net	509	3,16%
5	dev	485	3,02%
6	info	435	2,70%
7	eu	425	2,64%
8	org	416	2,59%
9	cfd	397	2,47%
10	site	342	2,13%

Tab. 8. Najpowszechniejsze domeny najwyższego poziomu w Polsce, pod którymi znajdowało się najwięcej stron phishingowych.

Na wykresie 7 przedstawiliśmy liczbę domen phishingowych rozwiązujących się na adresy IP w polskich sieciach w podziale na miesiące. Dane otrzymane od Global Cyber Alliance istotnie wpłynęły na statystykę w ostatnich miesiącach, dlatego oznaczyliśmy je innym kolorem. Jak można zauważyć na wykresie, przez większość roku liczba domen phishingowych utrzymywała się na w miarę stałym poziomie i oscylowała na poziomie blisko 500 domen miesięcznie. Natomiast jeśli uwzględnić dane od GCA, można zauważyć bardzo duży wzrost liczby domen phishingowych w grudniu, który prawdopodobnie wyniknął ze zwiększonego zainteresowania zakupami w internecie w tym okresie, co zwiększyło także aktywność przestępców.



Wykres 7. Liczba domen phishingowych, których adresy IP należały do polskich sieci z podziałem na miesiące. Kolorem fioletowym oznaczono domeny phishingowe pochodzące od Global Cyber Alliance, a zielonym domeny pochodzące z innych źródeł.

PHISHING, KTÓRY TRAFIŁ NA LISTĘ OSTRZEŻEŃ CERT POLSKA

Domeny, które trafiły w 2022 r. na listę ostrzeżeń CERT Polska[35] rozwiązywały się na 14 799 adresów IP. Przestępcy atakujący polskich użytkowników wykorzystywali usługi Cloudflare do ukrycia prawdziwej lokalizacji serwera, aż 11 196 adresów IP należało do tego dostawcy. Pomijając amerykańskie firmy oraz home.pl preferowanymi lokalizacjami wybieranymi przez przestępców są Hostinger (Cypr) oraz VPS-UA i Hosting Ukraine (Ukraina). Szczegółowe informacje znajdują się w tabeli 9.

Najpopularniejszymi firmami, pod które podszywali się przestępcy atakujący Polaków były Facebook, InPost, Orlen oraz Vinted. Fałszywy Facebook był hostowany najczęściej na serwerach home.pl - prawie 25 proc. wszystkich domen. Co ciekawe, Amazon oraz Cloudflare miały bardzo mały udział w hostowaniu phishingów wymierzonych w Facebooka, co może świadczyć o blokowaniu przez nich tego typu ataków. Phishing wykorzystujący wizerunek InPost był najchętniej hostowany za usługami Cloudflare oraz w rosyjskim systemie autonomicznym Selectel (AS50340). Również podszywanie się pod Orlen było w dużej części związane z Cloudflare, natomiast najpopularniejszym systemem autonomicznym wybieranym do hostingu był ukraiński AS56851. Strony phishingowe podszywające się pod Vinted były w ponad 90 proc. hostowane za usługami Cloudflare.

35 https://www.cert.pl/posts/2020/03/ostrzezenia_phishing/

Poz.	Numer AS	Nazwa AS	Liczba IP
1	13335	Cloudflare	11 196
2	47583	Hostinger	490
3	12824	home.pl	350
4	56851	VPS-UA	221
5	16509	Amazon	202
6	200000	Hosting Ukraine	178
7	14061	DigitalOcean	148
8	14618	Amazon	134
9	16276	OVH	109
10	22612	Namecheap	95

Tab. 9. Systemy autonomiczne z największą liczbą adresów IP, które rozwiązywały się z domen znajdujących się na liście ostrzeżeń.

Najpopularniejszymi domenami najwyższego poziomu były com, pl i xyz. Popularność polskiej TLD oraz com wynika ze zwiększonej skuteczności podszywania się pod oryginalną domenę, natomiast xyz jest spowodowane najprawdopodobniej niską ceną tej domeny.

Poz.	Liczba Domen	TLD
1	14654	com
2	9415	pl
3	8519	xyz
4	3529	info
5	2434	site
6	2250	space
7	2079	net
8	1996	top
9	1574	eu
10	1049	online

Tab. 10. Najczęściej występujące domeny najwyższego poziomu (TLD), które znalazły się na liście ostrzeżeń.

Poz.	Numer AS	Nazwa AS	Liczba IP
1	12824	home.pl	350
2	41079	Cyber_Folks	23
3	29522	Cyber_Folks	20
4	15967	Nazwa.pl	19
5	203417	LH.pl	15
6	16276	OVH	10
7	198414	Cyber_Folks	10
8	197226	Sprint	8
9	200088	Artnet	6
10	5617	Orange	5

Tab. 11. Systemy autonomiczne zlokalizowane w Polsce z największą liczbą adresów IP, które rozwiązywały się z domen znajdujących się na liście ostrzeżeń.

STRONY ZWIĄZANE ZE ZŁOŚLIWYM OPROGRAMOWANIEM

W ubiegłym roku zebraliśmy informacje o 7 903 498 adresach URL, związanych z działalnością złośliwego oprogramowania. Wśród nich 47 014 znajdowało się w domenie .pl, a 46 632 rozwiązywały się na polskie adresy IP.

Analogiczne podsumowanie przeprowadziliśmy dla nazw domenowych związanych z działalnością złośliwego oprogramowania, których w ubiegłym roku odnotowaliśmy 589 219. Wśród nich 5 204 należało do domeny .pl, a 5 386 rozwiązywało się na polskie adresy IP. Listę adresów IP, na które wskazywało najwięcej domen .pl, umieściliśmy w tabeli 12. Adresy w zestawieniu należą do dostawców usług hostingu oraz do Cloudflare. Najczęściej występujący adres (217.97.216.17) jest związany z usługą Orange Office, na przestrzeni lat był używany do hostingu tysięcy stron WWW, a część z nich najprawdopodobniej została przejęta przez przestępców i wykorzystana do ataków na użytkowników.

Zestawienie systemów autonomicznych, w których znajdowało się najwięcej adresów IP związanych ze złośliwym oprogramowaniem, umieściliśmy w tabeli 13. Łatwo zauważyć, że zdecydowanie największy udział należy do chińskich systemów autonomicznych.

Poz.	Liczba domen .pl	Adres IP	Numer AS	Nazwa
1	131	217.97.216.17	5617	Orange
2	94	94.154.117.92	203417	LH.pl
3	65	37.59.49.187	16276	OVH
4	61	176.31.124.7	16276	OVH
5	55	94.154.117.156	203417	LH.pl
6	52	91.212.150.245	43350	nForce
7	49	188.114.96.13	13335	Cloudflare
8	49	188.114.97.13	13335	Cloudflare
9	45	62.122.190.126	203417	LH.pl
10	44	62.122.190.67	203417	LH.pl

Tab. 12. Adresy IP, na których utrzymywano najwięcej domen .pl związanych ze złośliwym oprogramowaniem.

Poz.	Liczba IP	Numer AS	Nazwa	Odsetek wszystkich adresów w AS	Udział
1	108 383	4837	China Unicom	0,19%	27,34%
2	43 307	13335	Cloudflare	2,64%	10,92%
3	40 976	9829	National Internet Backbone	0,76%	10,34%
4	35 466	4134	Chinanet	0,03%	8,95%
5	17 891	17816	China Unicom	0,46%	4,51%
6	9 511	46606	Unified Layer	0,97%	2,40%
7	6 690	16509	Amazon	0,02%	1,69%
8	3 942	14061	Digital Ocean	0,15%	0,99%
9	3 722	8075	Microsoft	0,01%	0,94%
10	3 586	3462	HINET	0,03%	0,90%

Tab. 13. Systemy autonomiczne, w których znajdowało się najwięcej adresów IP związanych ze złośliwym oprogramowaniem.

USŁUGI POZWALAJĄCE NA PROWADZENIE ATAKÓW DRDoS

W 2022 r. otrzymaliśmy informacje o 485 067 adresach IP, pod którymi znajdowały się usługi umożliwiające przeprowadzenie rozproszonych ataków odmowy usługi ze wzmocnieniem (Distributed Reflection Denial of Service - DRDoS), spośród których 464 513 znajdowało się w Polsce. 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.

W poniższym zestawieniu znalazła się większa liczba pozycji niż w ubiegłym roku. Wynika to z faktu dodania przez nas nowych źródeł danych, które dostarczają informacje o nowych rodzajach usług, których nie śledziliśmy poprzednio. W przypadku Ubiquiti i DVR-DHCPDiscover czas obserwacji jest zauważalnie krótszy niż w pozostałych przypadkach. Dane dotyczące tych usług zaczęły napływać w trakcie roku.

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 2022 r.

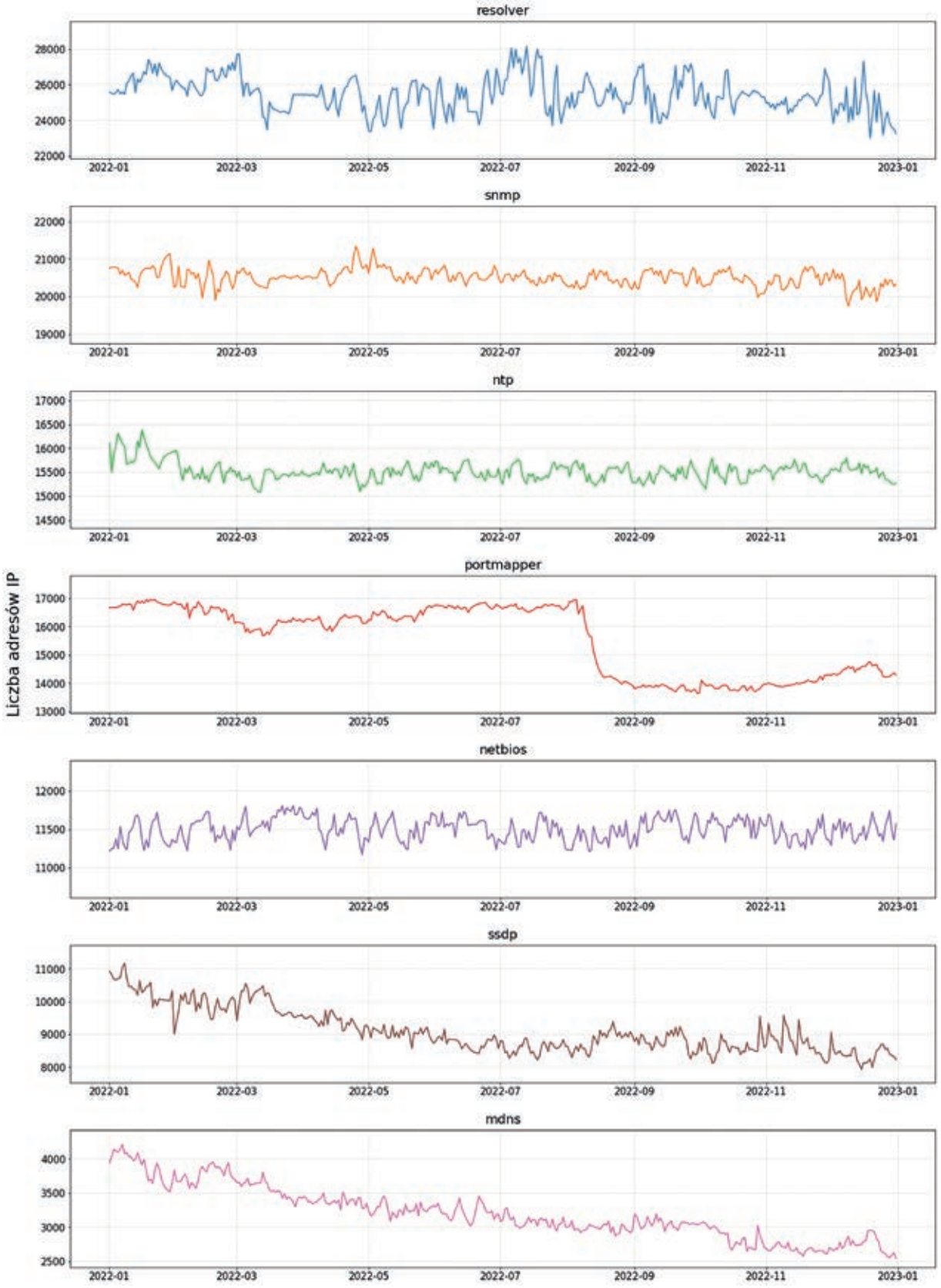
Poz.	Nazwa podatności / otwartej usługi	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odchylenie standardowe	Czas obserwacji
1	resolver	25 338	29 901	1 862	90,41%
2	SNMP	20 472	21 750	308	88,76%
3	NTP	15 516	16 931	873	90,68%
4	portmapper	15 504	17 197	1 250	88,21%
5	NetBIOS	11 464	11 996	636	89,31%
6	SSDP	9 021	11 512	950	89,86%
7	mDNS	3 165	4 307	472	90,95%
8	mssql	1 725	2 849	324	88,49%
9	ubiquiti	1 711	1 969	331	48,21%
10	dvr-dhcpdiscover	1 405	3 232	715	73,15%
11	chargen	147	264	14	90,13%
12	CoAP	33	41	3	92,54%
13	qotd	33	46	7	89,31%
14	xdmcp	23	34	3	90,13%
15	ard	19	32	3	91,78%
16	rdpeudp	10	30	4	90,41%

Tab. 14. 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 zastosowaliśmy podobną metodykę jak ta, która została wprowadzona po raz pierwszy w raporcie z 2020 r. Także w 2022 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: https://www.shadowserver.org/what-we-do/). Problem dotyczy wszystkich analizowanych usług i w związku z tym, że AS5617 w wielu przypadkach ma wysoki udział w całkowitej liczbie adresów IP dla danej usługi, wpływa on w znacznym stopniu na zbiorcze statystyki. Zdecydowaliśmy się na odpowiednie skorygowanie danych przy użyciu metody opisanej dokładnie w raporcie z 2020 r. Zainteresowanych zachęcamy do sięgnięcia po edycję raportu sprzed dwóch lat w celu zapoznania się ze szczegółami. Następnie na podstawie skorygowanych danych powstały tabele i wykresy umieszczone w raporcie.

Na wykresie 8 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 siedmiu najczęściej zgłaszanych usług.

W przypadku usług resolver, SNMP, NTP i NetBIOS liczba adresów IP utrzymuje się na podobnym poziomie w skali roku. Pozytywnym trendem jest stopniowy spadek liczby urządzeń związanych z usługą SSDP oraz mDNS na przestrzeni całego roku. W przypadku usługi portmapper widoczny jest gwałtowny spadek liczby adresów w drugiej połowie roku. Takie sytuacje mogą wynikać np. z aktualizacji konfiguracji maszyn u niektórych dostawców usług lub wprowadzenia odpowiednich reguł filtrowania ruchu.



Wykres 8. Najpowszechniejsze źle skonfigurowane usługi mogące brać udział w atakach DRDoS. Wykres ukazuje zmiany liczebności podatnych adresów IP w Polsce w 2022 r.

OTWARTE SERWERY DNS

Najpopularniejszą obserwowaną w 2022 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 2022 r. otrzymaliśmy 6 152 112 zgłoszeń o 147 391 adresach IP z uruchomionym otwartym resolverem – to spadek o około 17 tys. adresów w porównaniu z rokiem 2021, co świadczy o niewielkiej poprawie. Dzienna średnia liczba adresów wynosi obecnie 25 338. Na przestrzeni 2022 r. dzienna liczby adresów IP z tą usługą utrzymywała się na podobnym stałym poziomie. Podobnie jak w ubiegłych latach, w zestawieniu systemów autonomicznych z liczbą adresów dominował AS5617, czyli sieć Orange. Także w przypadku tego systemu autonomicznego widać, że średnia dzienna liczby adresów IP utrzymuje się na podobnym poziomie i wpływa to w największym stopniu na trend ogólny. W pozostałych systemach autonomicznych z tabeli dzienna liczba adresów IP utrzymuje się na stałym poziomie w skali roku lub zmiany są niewielkie. Nowością w poniższym zestawieniu w porównaniu z ubiegłym rokiem jest AS34859, w którego przypadku niepokoić może bardzo wysoki odsetek adresów (34 proc.), które mogą zostać wykorzystane do ataku DRDoS.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	15 253	18 913	0,27%
2	12741	Netia	1 123	2 273	0,07%
3	6830	UPC	605	930	0,02%
4	34859	Zyn Line	604	987	33,70%
5	12912	T-Mobile	546	839	0,05%
6	13110	INEA	471	510	0,28%
7	29314	Vectra	393	471	0,07%
8	8374	Plus / Cyfrowy Polsat	291	320	0,02%
9	31242	TKPSA	260	284	0,23%
10	5588	T-Mobile	224	239	0,13%

Tab. 15. 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 2022 r. otrzymaliśmy 5 984 839 zgłoszeń o 125 159 adresach z uruchomionym SNMP, co oznacza spadek o około 30 tys. w liczbie adresów w porównaniu do 2021 r. Natomiast najistotniejszy wskaźnik, czyli dzienna średnia liczba wystąpień, wyniosła 20 472 adresy, co stanowi redukcję o około 5 tys. względem poprzedniego roku. Ponownie na pierwszym miejscu znalazł się AS12741 należący do Netii.

W przypadku tego systemu autonomicznego pod koniec 2021 r. zanotowaliśmy gwałtowny spadek średniej dziennej liczby adresów IP, który mógł wynikać np. ze zmian w konfiguracji urządzeń w systemie autonomicznym tego operatora. W 2022 r. liczba ta utrzymuje się na mniej więcej stałym poziomie podobnym do tego z końca 2021 r. Stąd porównując średnie z całego 2021 r. i 2022 r. obserwujemy znaczny spadek o około 6 tys. adresów (22 proc.). Podobnie jak w 2021 r. odnotowaliśmy wysoki odsetek wszystkich adresów w AS w przypadku Net Center (AS60920) oraz Digicom (AS57978) - w obu przypadkach powyżej 20 proc. adresów IP rozgłaszanych przez te systemy autonomiczne miało instancję SNMP otwartą na dostęp z Internetu.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	12741	Netia	2 403	2 749	0,15%
2	5617	Orange	2 041	2 735	0,04%
3	20804	TELENERGO	849	916	0,35%
4	60920	NETCENTER	663	762	21,58%
5	56515	OXYNET	592	616	4,45%
6	199390	ALFAKS	488	508	15,89%
7	57978	DIGICOM	422	459	20,61%
8	41809	Enterpol	299	330	2,21%
9	6830	UPC	290	463	0,01%
10	199234	Komputerowe Studio Grafiki	253	276	8,24%

Tab. 16. Dzienna liczba adresów IP, na których wykryto działającą usługę SNMP 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 2022 r. otrzymaliśmy łącznie 4 958 992 zgłoszenia o 26 824 adresach IP, co stanowi spadek o około 4 tys. w porównaniu z rokiem poprzednim. Dzienna średnia liczba wystąpień wyniosła 15 516 adresów, co jest wartością porównywalną z ubiegłym rokiem.

W przypadku tej usługi dzienna liczba adresów IP oscylowała w skali roku względem mniej więcej tego samego poziomu. Jedynym systemem autonomicznym z poniższej tabeli, w którym zanotowaliśmy niewielki malejący trend w przeciągu roku był system autonomiczny należący do Netii (AS12741). Podobnie jak rok wcześniej uwagę zwraca AS48956, w którym po raz kolejny odnotowaliśmy wysoki odsetek adresów, które mogą zostać wykorzystywane w atakach DDoS - blisko 10 procent.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	1 732	2 533	0,03%
2	12741	Netia	1 170	1 429	0,07%
3	5588	T-Mobile	971	1 047	0,58%
4	12912	T-Mobile	816	1 049	0,07%
5	48956	HYPERNET	445	515	9,66%
6	199715	MSITELEKOM	386	396	2,47%
7	20960	TKTELEKOM	300	328	0,12%
8	6830	UPC	281	419	0,01%
9	9085	SUPERMEDIA	258	270	0,61%
10	15694	ATMAN	215	230	0,29%

Tab. 17. Dzienna liczba adresów, na których wykryto działającą usługę NTP 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 2022 r. otrzymaliśmy 4 811 561 zgłoszeń o 47 343 adresach z usługą portmapper dostępną na publicznym interfejsie. Dzienna średnia wynosiła 15 504 adresy, co oznacza spadek o około 2 tys. względem roku 2021. Przez pierwszą połowę roku dzienna średnia liczba adresów utrzymywała się na stałym poziomie. W sierpniu 2022 r. zaobserwowaliśmy nagły spadek z poziomu mniej więcej 16 tys. adresów do poziomu 14 tys. Liczba ta utrzymywała się w dalszej części roku. Gwałtowny spadek był spowodowany przez AS50599 oraz AS20804. 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. Podobnie jak w 2021 r. wysoko w zestawieniu znajdują się ATMAN (AS57367) ze zbliżoną średnią liczbą adresów IP w porównaniu do roku ubiegłego. Drugi rok z rzędu w zestawieniu pojawia się także Data Space (AS57367), gdzie widzimy wysoki odsetek zainfekowanych adresów IP (ponad 5 proc.).

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	57367	ATMAN	1 321	1 388	8,46%
2	16276	OVH	1 319	2 178	0,03%
3	50599	Data Space	662	1 097	5,28%
4	20804	TELENERGO	644	1700	0,27%
5	47329	WDM	405	422	4,16%
6	59491	LIVENET	373	619	5,20%
7	12741	Netia	312	370	0,02%
8	197155	ARTNET	296	422	2,63%
9	50840	HITME	258	317	5,60%
10	35787	Internet Cafe	239	254	6,67%

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

NETBIOS

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

W 2022 r. otrzymaliśmy 2 456 368 zgłoszeń o 46 787 adresach IP, co stanowi wzrost o około 2 tys. w porównaniu z 2021 r. Dzienna średnia liczba wystąpień wyniosła 11 464 adresy i jest to wartość porównywalna z rokiem poprzednim. Przez większość roku obserwowaliśmy utrzymującą się na stałym poziomie liczbę adresów IP z uruchomioną usługą NetBIOS. W przypadku żadnego z systemów autonomicznych znajdujących się w pierwszej dziesiątce zestawienia zawartego w tabeli nie odnotowaliśmy tendencji spadkowej ani wzrostowej. Podobnie jak w roku 2021 na dwóch pierwszych miejscach zestawienia znalazły się systemy autonomiczne należące do Orange i Netii z porównywalną z rokiem ubiegłym średnią liczbą adresów IP. W przypadku każdego z systemów autonomicznych zawartych w tabeli odsetek adresów z usługą NetBIOS dostępną publicznie był na bardzo niskim poziomie.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	6 471	7 989	0,08%
2	12741	Netia	581	646	0,04%
3	13110	INEA	136	152	0,08%
4	12824	home.pl	119	128	0,06%
5	8374	Plus / Cyfrowy Polsat	110	129	0,01%
6	12912	T-Mobile	106	159	0,01%
7	8970	WASK WROCMAN	105	153	0,16%
8	8267	CYFRONET	94	120	0,12%
9	5588	T-Mobile	77	87	0,05%
10	12423	TORMAN	77	137	0,23%

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 tym samym na przykład nieograniczony dostęp z Internetu wbrew dobrym praktykom bezpieczeństwa lub dostęp do aplikacji bez uwierzytelnienia. W 2022 r. odnotowaliśmy 53 188 458 takich obserwacji dotyczących 967 503 adresów IP z Polski. Na kolejnych stronach zostały przedstawione szczegółowe informacje o zagrożeniach, które występują w polskich sieciach najczęściej. Przedstawione statystyki zostały obliczone analogicznie jak w podrozdziale dotyczącym usług pozwalających na prowadzenie ataków DRDoS. W przypadku podatnych usług wystąpił ten sam problem z mało wiarygodnymi danymi dotyczącymi AS5617 (Orange), została więc użyta ta sama metoda szacowania.

W poniższym zestawieniu znalazło się więcej pozycji niż w ubiegłym roku. Wynika to z tego, że dodaliśmy nowe źródła danych, które dostarczają informacje o nowych rodzajach usług, których nie śledziliśmy poprzednio.

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

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

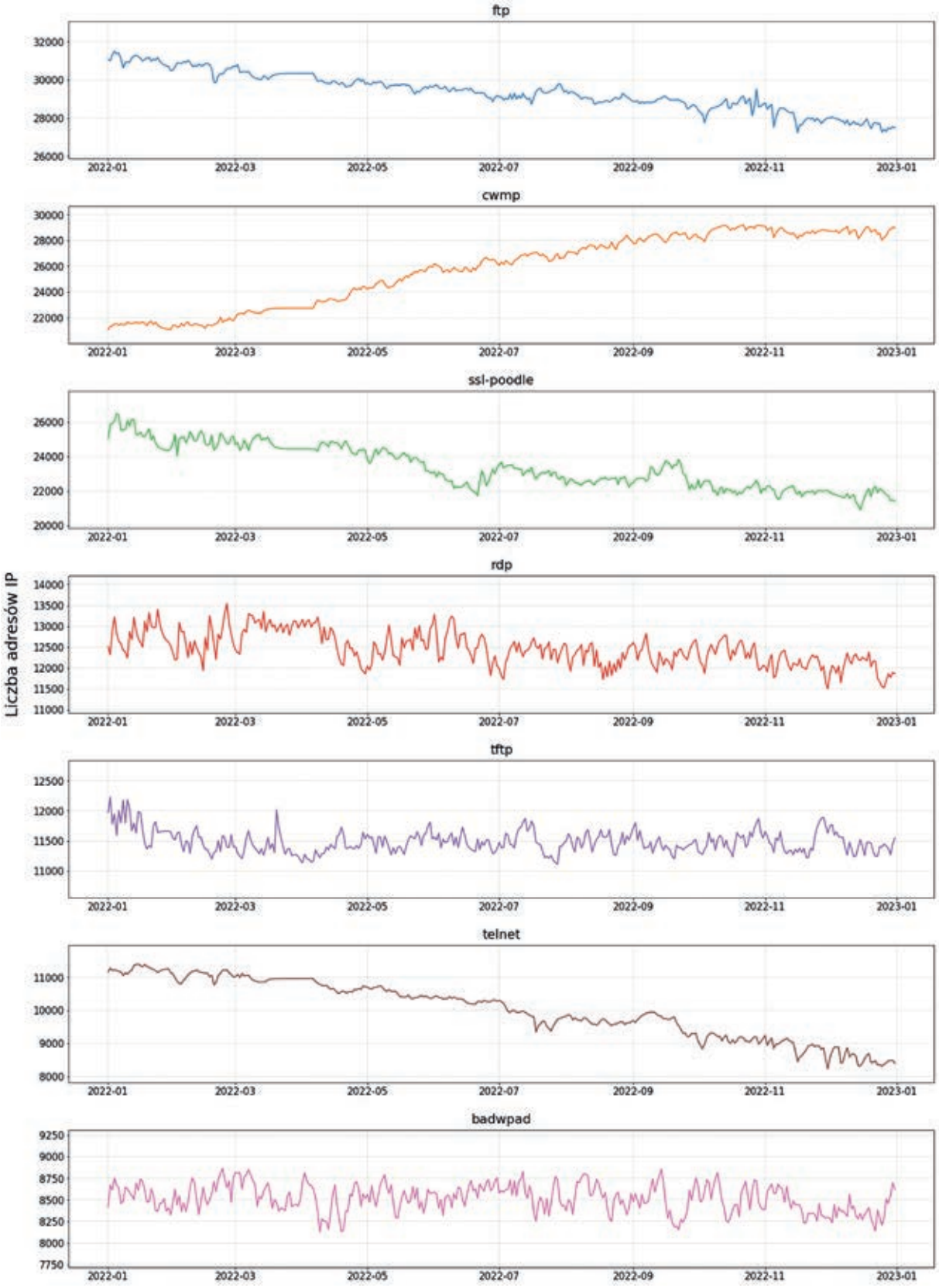
Poz.	Nazwa podatności / otwartej usługi	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odchylenie standardowe	Czas obserwacji
1	FTP (dane uwierzytelniające w postaci jawnej)	28 963	31 720	2 841	91,50%
2	CWMP	25 728	29 493	2 748	91,23%
3	SSL-POODLE	23 239	27 040	1 783	90,95%
4	RDP	12 444	14 475	635	91,78%
5	TFTP	11 483	13 085	321	89,58%
6	Telnet	9 917	11 573	1 202	91,50%
7	BadWPAD	8 516	9 189	288	100%
8	ISAKMP	5 097	6 569	993	89,58%
9	SMB	4 803	6 538	1 313	88,21%
10	VNC	3 314	4 803	327	90,68%
11	SSL-FREAK	3 140	3 960	495	90,68%
12	RSYNC	2 254	2 730	167	92,32%
13	NAT-PMP	1 265	1 662	225	89,86%
14	AFP	984	1 179	75	92,32%
15	MQTT	753	861	26	92,32%
16	AMQP	654	705	26	92,05%
17	IPMI	631	757	80	91,78%
18	MongoDB	586	658	33	91,23%
19	IPP	579	729	53	92,32%
20	LDAP	336	386	13	92,32%
21	Radmin	182	247	14	92,32%
22	Memcached	163	180	6	90,68%
23	Cisco Smart Install	111	123	6	92,32%
24	Elasticsearch	59	72	4	90,95%
25	Redis	56	79	7	89,86%
26	ADB	10	18	3	92,32%

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.

Na wykresie 9 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, ze średnią liczbą obserwowanych IP większą niż 8 tys.

Porównując rok 2022 z 2021 nie zauważamy dużych zmian w czołówce zestawienia. Wciąż podobne usługi są w Polsce zagrożone atakiem. Nie odnotowaliśmy także gwałtownych spadków lub wzrostów liczby adresów IP w trakcie roku. Patrząc na wykres możemy zauważyć pozytywny trend w zakresie stopniowego spadku liczby urządzeń związanych z podatnością Poodle i usługami FTP, RDP oraz Telnet na przestrzeni całego roku. W przypadku BadWPAD oraz TFTP dzienna liczba adresów IP utrzymuje się na stałym poziomie. Jedynie w przypadku usługi CWMP widzimy stopniowy wzrost w skali roku. Wynika to prawdopodobnie z podłączenia nowych urządzeń pozwalających na zdalną konfigurację u operatora Netia.



Wykres 9. Najpowszechniejsze zagrożone usługi. Wykres ukazuje zmiany liczebności podatnych adresów IP w Polsce w 2022 r.

W ramach omawiania podatnych usług zdecydowaliśmy się wydzielić podrozdziały dotyczące serwerów Exchange, systemów przemysłowych (ICS/OT) oraz usługi HTTP. Dane zostały zaprezentowane poniżej w osobnych tabelach.

EXCHANGE

W poniższej sekcji znalazły się informacje dotyczące podatnych serwerów Microsoft Exchange. Wszystkie podatności wymienione w tabeli są podatnościami Remote Code Execution, umożliwiającymi zdalne wykonanie kodu na zaatakowanym systemie.

Poz.	Nazwa podatności	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odchylenie standardowe	Czas obserwacji
1	CVE-2022-41082	347	408	29	3,01%
2	CVE-2021-27065	28	58	4	34,24%
3	CVE-2020-0688	23	56	5	62,19%
4	CVE-2021-26855	14	28	5	92,32%

Tab. 21. Zestawienie najliczniej występujących w Polsce serwerów Exchange 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.

PRZEMYSŁOWE SYSTEMY STEROWANIA

W poniższej sekcji znalazły się informacje dotyczące systemów ICS/OT, które są dostępne publicznie. Podczas skanowań nie sprawdzano konkretnych podatności. Tego typu urządzenia nie powinny być jednak dostępne z Internetu. Zestawienie uwzględnia zarówno adresy IP, na których faktycznie dostępne są poniższe usługi, jak również te, które są dostępne intencjonalnie jak systemy honeypot, ponieważ ich odróżnienie na podstawie danych ze skanowania Internetu jest trudne, a ich łączna liczba niewielka.

Poz.	Nazwa podatności / otwartej usługi	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odchylenie standardowe	Czas obserwacji
1	S7	196	214	8	76,71%
2	Codesys	152	194	5	73,69%
3	Modbus	72	105	32	77,26%
4	EtherNet/IP	62	74	2	73,97%
5	BACnet	51	75	7	73,97%
6	Fox	24	30	2	76,71%
7	DNP3	18	53	5	75,34%
8	OPC UA Binary	15	30	8	71,78%
9	Omron FINS	12	18	1	73,12%
10	GE SRTP	10	14	1	70,13%
11	PC Worx	6	8	1	73,69%
12	MELSEC-Q	4	7	1	73,97%
13	ICCP	2	6	1	62,73%
14	EtherCAT	2	5	1	61,63%
15	IEC 60870-5-104	1	5	1	60,54%

Tab. 22. Zestawienie najliczniej występujących w Polsce systemów ICS/OT 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.

HTTP

W poniższej sekcji znalazły się informacje dotyczące systemów z działającą usługą HTTP, które mogą być narażone na ataki. Podane w tabeli podatności oznaczają:

- Basic auth - serwery HTTP, które używają Basic Authentication. Dane uwierzytelniające są transmitowane w postaci jawnej bez szyfrowania.
- Basic auth (IoT) - jak wyżej. Dotyczy urządzeń IoT.
- Zimbra CVE-2022-37042 - podatność pozwalająca na zdalne wykonanie kodu.
- Folder .git - dostępny publicznie folder .git.

Poz.	Nazwa	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odchylenie standardowe	Czas obserwacji
1	Basic auth	11 141	16 004	1 669	92,05%
2	Basic auth (IoT)	3 530	7 541	1 043	92,05%
3	Zimbra CVE-2022-37042	548	624	106	38,63%
4	Folder .git	537	588	12	16,43%

Tab. 23. Zestawienie najliczniej występujących w Polsce serwerów HTTP 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.

FTP

FTP (ang. File Transfer Protocol) jest protokołem transferu plików. FTP nie zapewnia szyfrowania (jeśli nie jest użyte FTPS) i może ujawniać wrażliwe informacje i dane uwierzytelniające. Opisywane zestawienie zawiera dostępne publicznie serwery, do których dane uwierzytelniające są przesyłane w postaci jawnej.

W 2022 r. otrzymaliśmy 9 584 306 zgłoszeń o 85 947 adresach IP z dostępną publicznie usługą FTP. Dzienna średnia liczba adresów wynosiła 28 963. Na przestrzeni 2022 r. widoczna jest tendencja spadkowa. Różnica między początkiem i końcem roku wynosi około 3 tys. adresów. Trend spadkowy jest widoczny w większości wymienionych w tabeli systemach autonomicznych. Wyjątkiem jest AS31242 gdzie odnotowaliśmy nieznaczny wzrost w trakcie roku. Niepokoi bardzo wysoki odsetek adresów w AS48727, w którym podatnych jest ponad 40 proc. wszystkich adresów.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	12741	Netia	1 963	2 266	0,12%
2	16276	OVH	1 427	1 622	0,03%
3	6830	UPC	1 085	1 259	0,03%
4	12912	T-Mobile	988	1 116	0,09%
5	9085	SUPERMEDIA	715	755	1,68%
6	8374	Plus / Cyfrowy Polsat	590	662	0,04%
7	31242	TKPSA	585	678	0,51%
8	29314	Vectra	537	619	0,10%
9	13110	INEA	468	520	0,28%
10	48727	ADAMEK	413	660	40,33%

Tab. 24. Dzienna liczba adresów, na których wykryto usługę FTP dostępną na publicznym interfejsie, z którą można było nawiązać połączenie kanałem nieszyfrowanym, w podziale na systemy autonomiczne.

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 2022 r. otrzymaliśmy 8 513 629 zgłoszeń o 289 906 adresach IP z dostępną publicznie usługą CWMP. Jest to spadek o około 300 tys. adresów w porównaniu do 2021 r. Dzienna średnia liczba adresów wynosiła 25 728, co jest spadkiem o około 10 tys. w porównaniu do poprzedniego roku. Należy zwrócić jednak uwagę, że w pierwszym kwartale ubiegłego roku dzienna liczba adresów utrzymywała się na znacznie wyższym poziomie, co podnosi wartość średnią. Następnie w lutym nastąpił gwałtowny spadek. Stąd porównując dane począwszy od drugiego kwartału 2021 r. z 2022 r. stwierdzamy, że dzienna liczba adresów utrzymywała się na podobnym poziomie. Na przestrzeni 2022 r. widoczna jest tendencja wzrostowa w większości systemów autonomicznych. Wzrost na przestrzeni roku wyniósł około 7 tys. adresów. Znaczny udział w całkowitej liczbie adresów IP dla usługi CWMP miała Netia, gdzie odnotowaliśmy wzrost w trakcie roku, co wpływa w znaczący sposób na ogólny trend. Niepokoi wysoki odsetek podatnych adresów w AS198766 oraz AS200125 – podatnych jest odpowiednio około 32 proc. oraz 17 proc. wszystkich adresów w tych systemach autonomicznych.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	12741	Netia	12 142	14 634	0,67%
2	44124	RYBNET	1 439	1 615	10,04%
3	198766	NETSYSTEM BRZESKO	1 377	1 511	31,64%
4	21021	Multimedia	1 001	1 196	0,16%
5	44692	DOMTEL	731	795	3,32%
6	197227	PSM WINOGRADY	703	954	3,81%
7	50231	SYRION	690	1 277	2,75%
8	12912	T-Mobile	675	863	0,06%
9	51337	DEBACOM	666	707	10,84%
10	200125	INTERTOR	524	621	17,06%

Tab. 25. 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 7 882 346 zgłoszeń o 163 247 adresach IP. Jest to spadek o około 50 tys. adresów w porównaniu z 2021 r. Średnia dzienna liczba adresów wynosiła 23 239, co jest spadkiem o około 3 tys. w porównaniu do poprzedniego roku. Podobnie jak w 2021 r. w większości systemów autonomicznych obserwujemy stopniowy spadek w przeciągu roku lub też dzienna liczba adresów utrzymuje się na stałym poziomie. Na uwagę zasługuje AS206417, w którym odnotowaliśmy wysoki odsetek podatnych adresów. W tym przypadku wartość ta wynosi ponad 20 proc. Podobnie jak rok wcześniej w czołówce zestawienia znalazł się AS59958 z odsetkiem podatnych adresów na poziomie prawie 6 proc.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	12741	Netia	4 379	5 454	0,26%
2	59958	P.H.U MMJ	1 151	1 254	5,84%
3	43939	InternetIA	687	844	0,26%
4	6830	UPC	559	727	0,01%
5	31242	TKPSA	526	631	0,46%
6	12912	T-Mobile	472	648	0,04%
7	5588	T-Mobile	427	490	0,26%
8	206417	FRESHMAIL	412	459	20,12%
9	29007	PETROTEL	399	461	2,44%
10	29314	Vectra	395	577	0,08%

Tab. 26. Dzienna liczba adresów, na których wykryto działającą usługę SSL z podatnością POODLE, w podziale na systemy autonomiczne.

RDP

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

W 2022 r. otrzymaliśmy 4 085 489 zgłoszeń o 55 376 adresach IP (spadek o około 40 tys. w porównaniu z 2021 r.), na których wykryto usługę RDP dostępną na publicznym interfejsie. Średnia dzienna liczba adresów wynosiła 12 444 (spadek o około 2 tys. w porównaniu z 2021 r.). W przypadku RDP widzimy niewielką ogólną tendencję spadkową, co ma też swoje odzwierciedlenie w większości systemów autonomicznych. Spadek ten jest jednak niewielki i zdecydowanie mniej zauważalny niż w ubiegłym roku. Uwagę zwraca AS201814, w którego przypadku sytuacja wygląda odmiennie. Tutaj obserwujemy wzrost liczby adresów na przestrzeni roku. W tym przypadku niepokoi też wysoki w porównaniu do innych odsetek podatnych adresów, który wynosi prawie 5 proc.

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	12741	Netia	860	1 102	0,05%
2	6830	UPC	578	716	0,01%
3	16276	OVH	535	681	0,01%
4	12912	T-Mobile	487	602	0,04%
5	201814	SKYTECH	364	791	3,95%
6	9112	POZMAN	326	635	0,44%
7	13110	INEA	280	331	0,17%
8	8374	Plus / Cyfrowy Polsat	262	330	0,02%
9	8970	WASK WROCMAN	253	362	0,39%
10	42927	S-NET	253	278	1,65%

Tab. 27. Dzienna liczba adresów, na których wykryto usługę RDP 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 2 640 900 zgłoszeń o 66 260 adresach IP z dostępnym TFTP. Jest to spadek o około 20 tys. w porównaniu z 2021 r. Średnia dzienna liczba adresów wyniosła 11 483 i jest to wartość porównywalna z ubiegłym rokiem. W przeciągu roku liczba adresów IP utrzymuje się na podobnym, stałym poziomie. Nie dostrzegamy tendencji wzrostowej ani spadkowej. Dotyczy to wszystkich systemów autonomicznych zawartych w tabeli. Analogicznie jak w poprzednich latach szczególną uwagę zwracają wysokie odsetki adresów w systemach autonomicznych Spółdzielnia Mieszkaniowa „Północ" w Częstochowie (AS198000) oraz WIFIMAX (AS199510) - kolejno 18 proc. i 12 proc.

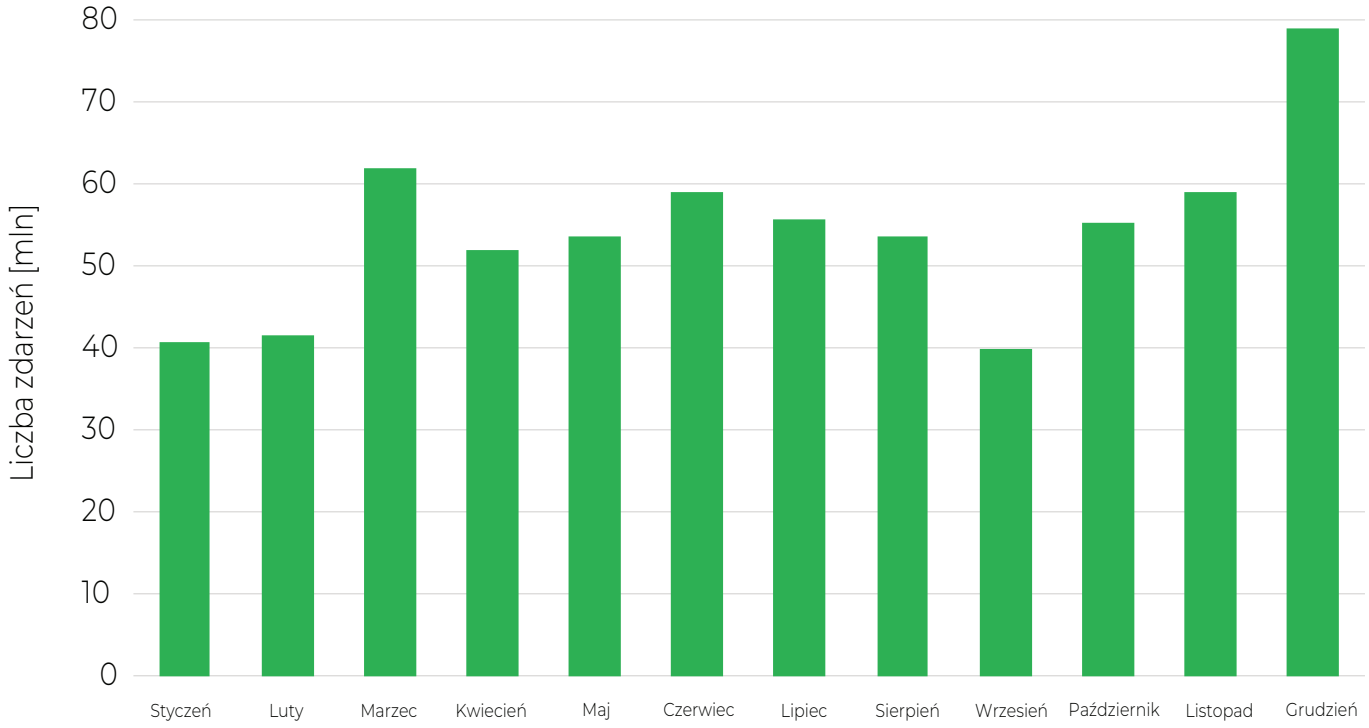
Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	4 909	7 549	0,05%
2	198000	SMPOLNOC	1 667	1 931	18,09%
3	12741	Netia	469	531	0,03%
4	21021	Multimedia	264	314	0,04%
5	39507	IPIVISION	128	168	0,34%
6	12912	T-Mobile	116	149	0,01%
7	196927	RTK	113	953	1,38%
8	200125	INTERTOR	105	129	3,42%
9	5588	T-Mobile	102	112	0,06%
10	199510	WIFIMAX	94	97	12,24%

Tab. 28. Dzienna liczba adresów, na których wykryto usługę TFTP dostępną na publicznym interfejsie, w podziale na systemy autonomiczne.

DANE Z SYSTEMÓW HONEYPOT

W 2022 r. przeanalizowaliśmy dane z sieci sensorów SISSDEN/Caprica (więcej informacji o projekcie SISSDEN znajduje się m.in. w raporcie rocznym za rok 2019), na którą składa się kilka rodzajów honeypotów o różnych poziomach interakcji. W ten sposób monitorowane są m.in. próby logowania, ataki na usługi SSH, Telnet oraz Elasticsearch, ataki na systemy ICS/SCADA oraz próby rozsyłania spamu. W ten sposób odnotowaliśmy 652 410 184 zdarzenia pochodzące z 11 172 091 różnych adresów IP należących do 31 225 systemów autonomicznych. Liczba zarejestrowanych zdarzeń z podziałem na miesiące znajduje się na wykresie 10.

Dla grudnia, czyli miesiąca, w którym odnotowaliśmy największą liczbę zdarzeń, średnio dziennie obserwowaliśmy prawie 117 tysięcy adresów IP, z których łączono się do systemów honeypot. Natomiast największa liczba adresów IP zarejestrowanych w ciągu jednego dnia wyniosła ponad 143 tysiące. Można zakładać, że większość z urządzeń odpowiedzialnych za tego rodzaju oportunistyczne ataki była zainfekowana złośliwym oprogramowaniem.



Wykres 10. Liczba odnotowanych zdarzeń z podziałem na miesiące.

Spośród wszystkich zdarzeń odnotowanych przez honeypoty, wyróżniliśmy te, które pochodziły z polskich sieci. W 2022 r. otrzymaliśmy ich 3 005 754, a pochodziły one z 37 438 adresów IP należących do 1 043 systemów autonomicznych.

Najpopularniejsze porty, co do których zebraliśmy informacje o próbach ataków na usługi, prezentujemy w tabeli 29. Popularność większości z wymienionych portów wynika przede wszystkim z powszechnie przyjętego przypisania ich do określonych usług sieciowych. Dlatego też na podstawie portu z dużą dozą pewności jesteśmy w stanie ustalić, na jaką usługę był skierowany atak. Duża ilość rejestrowanych prób ataku na porty 37215 oraz 5555 może wynikać z podatności znalezionych na urządzeniach Huawei oraz na urządzeniach z systemem Android.

Podobną analizę przeprowadziliśmy dla ataków pochodzących z polskich sieci - szczegółowe informacje przedstawione są w tabeli 30. Jak można zauważyć, większość portów docelowych jest wspólna dla obu analiz, jednak pojawiły się trzy nowe. Wystąpienie portu 6881 w naszej analizie jest prawdopodobnie spowodowane wykorzystywaniem go przez protokół Bittorrent. Natomiast porty 2323 i 81 są ściśle powiązane z próbami ataku - port 2323 jest czasami wykorzystywany jako alternatywny port dla protokołu Telnet, z kolei port 81 był wykorzystywany m.in. do prób wykorzystania podatności w kamerach Internetowych.

Poz.	Port docelowy	Opis portu / usługa	Liczba zdarzeń
1	23	Telnet	16 358 592
2	445	Microsoft-DS (Directory Services)	15 576 205
3	22	SSH	12 697 467
4	80	HTTP	5 578 471
5	443	HTTPS	2 913 857
6	8080	HTTP (alternatywny)	2 536 565
7	1433	Microsoft-SQL-Server	2 112 687
8	37215	Huawei Home Gateway	2 057 253
9	8443	PCsync HTTPS	1 909 283
10	5555	m.in. Android Debug Bridge	1 642 476

Tab 29. 10 najczęściej atakowanych portów.

Poz.	Port docelowy	Opis portu / usługa	Liczba zdarzeń
1	23	Telnet	8 567
2	80	HTTP	4 810
3	22	SSH	4 021
4	8080	HTTP (alternatywny)	2 838
5	445	Microsoft-DS (Directory Services)	2 674
6	6881	BitTorrent	1 453
7	2323	rockwell-csp2	1 046
8	443	HTTPS	964
9	81	HTTP (alternatywny)	950
10	5555	Personal-agent	871

Tab 30. 10 najczęściej atakowanych portów z adresów IP z polskich sieci.

MWDB

W 2022 r. w ramach serwisu mwdb.cert.pl:

- przeanalizowano łącznie ponad 373 tys. próbek złośliwego oprogramowania,
- pozyskano 14,5 tys. statycznych konfiguracji,
- zarejestrowano 334 kont dla zewnętrznych analityków złośliwego oprogramowania, w sumie w platformie zarejestrowanych jest 1176 użytkowników.

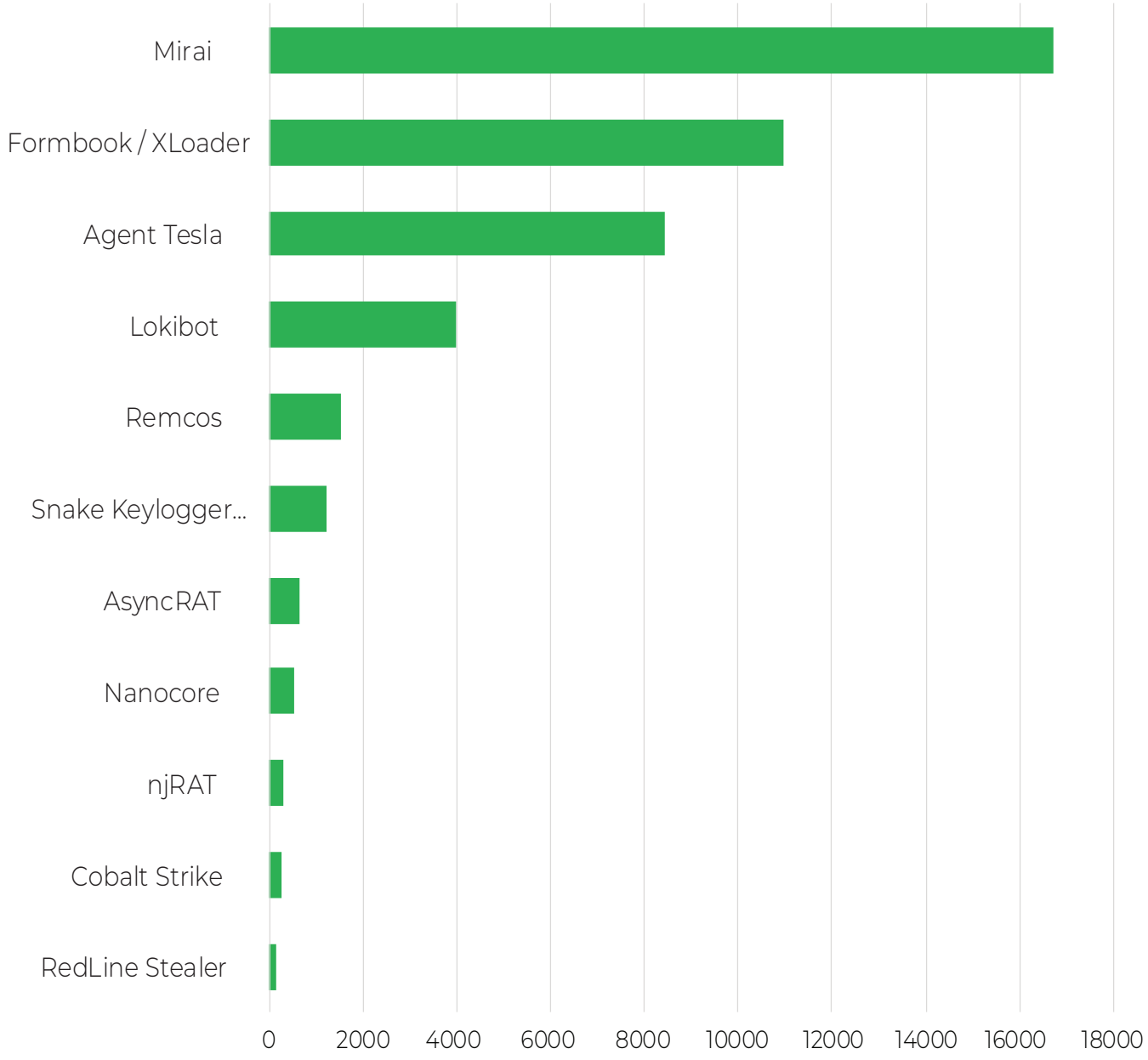
Tabela 31 przedstawia zestawienie rodzin złośliwego oprogramowania, które zostały rozpoznane przez MWDB. Najczęściej wykrywaliśmy Mirai, botnet IoT, którego liczne warianty i konfiguracje pojawiające się w 2022 r. mają znaczący udział w repozytorium. Kolejne miejsca zajmuje złośliwe oprogramowanie na platformę Windows, gdzie podobnie jak w poprzednich latach, rok 2022 minął pod znakiem tzw. infostealerów, czyli złośliwego oprogramowania służącego do wykradania danych (a w szczególności haseł) z komputerów użytkowników. Innym obserwowanym typem oprogramowania, które przeważało w 2022 r., są tzw. Remote Access Trojans (RAT), pozwalające na przejmowanie kontroli nad zainfekowanymi komputerami i wykonywanie na nich dowolnych działań.

Wśród analiz przeprowadzonych w ramach serwisu MWDB, wyróżniały się takie rodziny jak XLoader (będący następcą rodziny Formbook), Agent Tesla, Lokibot czy Remcos. Znaczny udział ma również Snake Keylogger, znany również pod nazwą 404 Keylogger, który zadebiutował na przełomie 2020 i 2021 roku[36]. Ta stosunkowo nowa rodzina oprogramowania jest aktywnie rozwijana przez twórców.

Poz.	Nazwa rodziny	Liczba plików wykonywalnych	Liczba unikalnych konfiguracji
1	Mirai	16 720	3 083
2	Formbook / XLoader	10 951	1 589
3	Agent Tesla	8 438	2 239
4	Lokibot	3 968	942
5	Remcos	1 536	756
6	Snake Keylogger (404 Keylogger)	1 231	384
7	AsyncRAT	637	468
8	Nanocore	525	299
9	njRAT	321	229
10	Cobalt Strike	278	183

Tab. 31. Dziesięć rodzin złośliwego oprogramowania z największą liczbą próbek rozpoznanych przez serwis MWDB w 2022 r.

36 https://www.fortinet.com/blog/threat-research/deep-dive-into-a-fresh-variant-of-snake-keylogger-malware



Wykres 11. Dziesięć rodzin złośliwego oprogramowania z największą liczbą próbek rozpoznanych przez serwis MWDB w 2022 r.

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