CERT.PL
NASK

20

RAPORT ROCZNY
z działalności CERT POLSKA 2023

23

CERT.PL
NASK

2023

RAPORT ROCZNY
z działalności CERT POLSKA

2023

Wstęp

Nowoczesne technologie w obszarze cyberbezpieczeństwa są dla nas tylko narzędziem wspierającym nasze codzienne działania. To ludzie, którzy ich używają naprawdę dokonują zmian. W CERT Polska mamy takich ludzi, a 2023 rok przyniósł nam wiele istotnych zmian, o których opowiadamy w tej publikacji.

W mijających miesiącach przede wszystkim doskonaliliśmy nasze narzędzia, takie jak Artemis, Snitch, n6 czy MWDB. Lepsze narzędzia, to lepszy ogląd na to, co dzieje się w cyberprzestrzeni, a co za tym idzie możliwość skuteczniejszego reagowania. Sieć nie zna granic, dlatego zależy nam na tym, by dzielić się wiedzą z innymi podmiotami odpowiedzialnymi za cyberbezpieczeństwo. Z tą myślą udostępniamy większość kodu narzędzi w formule open source. O tym, że warto ich używać mogą świadczyć dane, które znajdziecie Państwo w raporcie.

W ubiegłym roku wciąż rozwijaliśmy także ten fragment naszej działalności, który odnosi się do badania cyberprzestrzeni, analizowania działań cyberprzestępców. Podsumowanie tych obserwacji znajduje się w części dotyczącej incydentów i zagrożeń. W zeszłorocznej edycji zamieściliśmy rozdział poświęcony wojnie w Ukrainie – opisywaliśmy m.in. ataki typu DDoS na strony rządowe i portale podmiotów gospodarczych, a także pojawienie się fałszywych sklepów z opałem. Chcieliśmy pokazać, jak bardzo cyberprzestrzeń zależna jest od wydarzeń w świecie rzeczywistym. Dlatego i w tym raporcie znajdują się liczne odniesienia do bieżących wydarzeń, a rozdział o grupach APT jest tego doskonałym przykładem. Pokazuje on m.in. jak jesienne wybory do polskiego parlamentu wpływały na cyberprzestrzeń.

W raporcie opisujemy również liczne, bardzo ważne dla nas współprace, które owocowały projektami, ćwiczeniami i warsztatami. Pochylamy się nad tematem ustawy o zwalczaniu nadużyć w komunikacji elektronicznej, która niesie dla naszego zespołu szereg istotnych zmian i obowiązków, a dla użytkowników – szansę na ograniczenie ilości phishingu, z którym mają do czynienia na co dzień. Informacje o tych inicjatywach znajdą Państwo w rozdziale podsumowującym działania CERT Polska.

Wreszcie – last but not least – omawiamy skalę i rodzaje incydentów. Już same statystyki pozwalają uznać poprzedni rok za rekordowy. Na pierwszy rzut oka obraz, który się na ich bazie rysuje wydaje się mocno niepokojący. Jednak już pobieżna lektura pozwala zorientować się, że olbrzymia skala zgłoszeń, to także efekt działań promocyjnych i uruchomienia nowego, bezpłatnego numeru 8080 do zgłaszania podejrzanych wiadomości SMS. Wierzymy, że nasze działania przekładają się na wzrost świadomości dotyczącej cyberzagrożeń, a co za tym idzie wzrost liczby zgłoszeń. Rozwój wiedzy w obszarze cyberbezpieczeństwa to przecież najlepsza broń w walce z cyberoszustami.

Zapraszamy do lektury, bo ten raport to potężny zastrzyk wiedzy o tym, z jakimi zagrożeniami mamy do czynienia i jak skuteczniej możemy się przed nimi bronić.

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!

CERT Polska nadaje numery CVE

Nowe zadanie: koordynowane ujawnianie podatności

> **CERT Polska od sierpnia 2023 r. ma status CNA (CVE Numbering Authority), co pozwala na nadawanie identyfikatorów i publikowanie informacji o podatnościach w programie CVE. Wypracowanie zasad dla skoordynowanego ujawniania podatności było ważnym punktem na mapie obowiązków wynikających z przyjmowania Dyrektywy NIS 2.**

CVE (Common Vulnerabilities and Exposures) to międzynarodowy program wspierający ujawnianie luk bezpieczeństwa w oprogramowaniu lub sprzęcie komputerowym. Od 1999 r. program ten kataloguje podatności i oznacza je unikalnymi identyfikatorami w postaci „CVE-RRRR-XXXX", które stały się międzynarodowym standardem. Baza CVE jest publiczna i dostępna za darmo dla każdego. Obecnie jest ona podstawą dla organizacji z całego świata w identyfikacji i śledzeniu informacji o nowych lukach bezpieczeństwa. Lista CVE zasila również amerykańską Narodową Bazę Danych Podatności (NVD), gdzie można przeglądać rekordy CVE w wygodny sposób.

Każda osoba, która znajdzie podatność, może zgłosić ją do organizacji będącej CNA, czyli CVE Numbering Authority. Są to organizacje, które oceniają zasadność zgłoszenia, koordynują kontakt pomiędzy zaangażowanymi stronami, nadają podatnościom numery i dbają o jakość bazy. Każde CNA ma przydzielony zakres odpowiedzialności (scope), wewnątrz którego powinno katalogować podatności. Od 1 sierpnia 2023 r. CERT Polska jako jedyna instytucja w kraju i jeden z 7 CERT-ów w Europie może nadawać numery CVE, które służą identyfikacji i katalogowaniu publicznie ujawnionych podatności.

Zespół CERT Polska został wdrożony do Programu CVE przez MITRE, jego organizację założycielską. Zakresem odpowiedzialności CERT.PL są podatności odkryte przez Zespół lub zgłoszone do Zespołu w celu koordynowanego ujawnienia, które nie leżą w zakresie innych organizacji CNA[1].

Identyfikator CVE mogą otrzymać luki w oprogramowaniu, które zostało udostępnione publicznie (to kryterium spełniają również programy komercyjne). Oprogramowanie tworzone na jednostkowe zamówienie, które nie jest szerzej dystrybuowane, nie powinno więc mieć wpisu CVE. Ponadto błędom w usługach online (np. hosting, dostawca poczty) nie przypisuje się identyfikatorów CVE, ponieważ ich mitygacja nie wymaga podjęcia działań przez użytkowników. Co ważne, swój identyfikator otrzymuje każdy niezależnie występujący błąd w kodzie programu, stąd często w wyniku jednego zgłoszenia tworzonych jest wiele wpisów CVE.

Rola CERT Polska w procesie ujawniania błędów w oprogramowaniu

Proces koordynowanego ujawniania podatności (CVD, ang. Coordinated Vulnerability Disclosure) został wprowadzony do porządku prawnego poprzez zapisy dyrektywy NIS 2 i opisany szczególnie w motywach 58-63 oraz w artykule 12. Od daty wejścia w życie, czyli 16 stycznia 2023 r., państwa członkowskie mają 21 miesięcy na wdrożenie Dyrektywy do prawa krajowego. Jej postanowienia powinny być stosowane we wszystkich krajach Unii Europejskiej od 18 października 2024 r.

Zgodnie z NIS 2 każde państwo członkowskie powinno wyznaczyć jeden ze swoich CSIRT-ów do pełnienia roli koordynatora, występującego w razie potrzeby w charakterze Zaufanego Pośrednika między osobami zgłaszającymi a producentami lub dostawcami produktów lub usług ICT.

1 Lista organizacji CNA jest dostępna pod adresem cve.org/ProgramOrganization/CNAs

Rysunek 1: Diagram ról w procesie CVD

(źródło: CyberPolicy NASK, Poradnik „Skoordynowane ujawnianie podatności", 2022)

Niezamówione przez właściciela systemu testy bezpieczeństwa mogą stawiać obie kluczowe strony procesu CVD, czyli Zgłaszającego i Organizację, której dotyczy podatność, „po przeciwnych stronach barykady". Aby osiągnąć porozumienie obu stron i maksymalne korzyści potrzebna jest skoordynowana współpraca. Coraz więcej producentów oprogramowania otwiera się na zgłoszenia błędów od badaczy ogłaszając politykę CVD. Część z nich idzie o krok dalej, proponując wynagrodzenie za znalezienie błędów w ramach programów „bug bounty". Jednak nawet w przypadku, gdy brakuje polityki CVD, znalazca błędu ma obowiązek poinformować Organizację o znalezionej podatności. Może on poprosić o pomoc zespół CERT Polska jako Zaufanego Pośrednika, którego zadaniem jest pomoc w dotarciu do Organizacji w celu weryfikacji i usunięcia podatności, a także negocjowanie terminu opublikowania informacji.

Rysunek 2: Schemat procesu obsługi podatności

Proces zgłaszania podatności do zespołu CERT Polska został zilustrowany na powyższym rysunku. Zachęcamy, aby w pierwszej kolejności zgłaszający spróbował zgłosić lukę bezpieczeństwa bezpośrednio do producenta, co ma umożliwić usunięcie podatności w jak najkrótszym czasie. W następnym kroku, po otrzymaniu informacji o błędzie, jako Zaufany Pośrednik próbujemy niezależnie nawiązać kontakt z Organizacją i przekazać jej otrzymane informacje w celu weryfikacji istnienia podatności i ustalenia szczegółów ich dotyczących. Jeżeli okazuje się to niemożliwe (np. nie otrzymujemy odpowiedzi na wysłane wiadomości; oprogramowanie nie jest dalej wspierane) przystępujemy

do publikacji informacji o podatności na podstawie zgłoszenia. Równolegle także sprawdzamy, czy luka może otrzymać identyfikator zgodnie z zasadami Programu CVE. Jeżeli kryteria Programu nie są spełnione, zazwyczaj odstępujemy od publikacji informacji, natomiast w dalszym ciągu dążymy do usunięcia problemu.

Treść upublicznionego wpisu zawiera krótki opis problemu, miejsca jego występowania i potencjalnych skutków wykorzystania podatności. Nie publikujemy szczegółów pozwalających na przeprowadzenie ataku. Wpis możliwie precyzyjnie określa oprogramowanie z dokładnością do jego wersji zawierających omawiane zagrożenie.

Podatności ujawnione w 2023 przez CERT.PL

Koordynowane ujawnianie podatności zazwyczaj jest złożonym i długim procesem, na który składają się: nawiązywanie bezpiecznego kontaktu z właściwym adresatem, usuwanie podatności i dystrybucja poprawionego oprogramowania wśród klientów. Zdarza się, że od zgłoszenia do publikacji informacji mija kilka miesięcy.

> **W okresie od 1 sierpnia (moment uzyskania statusu CNA) do końca roku 2023 otrzymaliśmy 26 zgłoszeń o podatnościach, z czego 12 spełniało kryteria otrzymania identyfikatorów CVE. Na ich podstawie zarezerwowaliśmy 32 identyfikatory CVE i opublikowaliśmy informacje dotyczące sześciu z nich. Warto zaznaczyć, że trzy opublikowane podatności zostały odkryte w ramach badań własnych CERT Polska oraz NASK.**

Artykuły zawierające informacje o podatnościach ujawnionych przez Zespół CERT Polska są publikowane na stronie cert.pl/cve.

Więcej informacji o obsłudze zgłoszeń podatności przez nasz Zespół jest dostępne na stronie cert.pl/cvd.

Kalendarium

Styczeń

10.01

W ciągu 24h wpisaliśmy na listę ostrzeżeń aż 1032 domeny
https://www.facebook.com/CERT.Polska/posts/pfbid0LNYECRR1FmStw2WQKMG7E2ZpJbvwTYBw9sftE9aYG8dWh5FJmJfXBijzztCrqzSol

25.01

Inauguracja projektu Artemis
https://cert.pl/posts/2023/01/artemis

Luty

06.02

Zaobserwowaliśmy kampanie typu Ad Hijacking
https://cert.pl/posts/2023/02/ad-hijacking-google-ads

Marzec

09.03

Kampania phishingowa informująca o zwrocie pieniędzy za oszustwo na Olx lub Vinted
https://www.facebook.com/CERT.Polska/posts/pfbid0Q9BGaAPorSYCajW323jT2LAjfv5iyjDRAJiJNBKPscxWfsoXKxBLMTghYnR8P5jxl

14.03

Microsoft opublikował informację o krytycznej podatności CVE-2023-23397 w aplikacji Outlook na systemie Windows.
https://cert.pl/posts/2023/03/outlook-cve-2023-23397

27.03

Sezon na kampanie phishingowe informujące o zwrocie podatku
https://www.facebook.com/CERT.Polska/posts/pfbid0ea47ZyHg7AbXkLKvB7TwJH3AdLG4yDkEkTGGLWLoabvh89ghy6Zz3GTNnmxeeXutl

Kwiecień

18-19.04

Konferencja Secure 2023
https://cert.pl/posts/2023/04/secure-2023

13.04

Ujawnienie kampanii szpiegowskiej związanej z rosyjskimi służbami specjalnymi
https://www.gov.pl/web/baza-wiedzy/kampania-szpiegowska-wiazana-z-rosyjskimi-sluzbami

21.04

3. miejsce CERT Polska w LockedShields
https://www.facebook.com/CERT.Polska/posts/pfbid034uvQzqbte39jWFWQPFjtuTYu2U4KzV27yhJdLjWZS8YGBEdF23QRzJKEJcm9NjWAl

Maj

09.05

Start naszej kampanii medialnej promującej 2FA
https://www.facebook.com/CERT.Polska/posts/pfbid02QihnBvZMbFybF2SbZLe7KwECBw4fELCMKv8Dzhrz31M4i54QtmD3yHcZTFhQLdTpl

10.05

Publikacja Rocznego Raport z działalności CERT Polska w 2022
https://cert.pl/posts/2023/05/krajobraz-bezpieczenstwa-polskiego-internetu-w-2022-roku

31.05

Upublicznienie dużego zbioru wykradzionych danych logowania polskich użytkowników Internetu
https://cert.pl/posts/2023/05/wyciek-stealer-2023

Czerwiec

12.06

Krytyczna podatność CVE-2023-27997 w urządzeniach FortiGate SSL VPN
https://twitter.com/CERT_Polska/status/1668177568976052225

23.06

Start wakacyjnego cyklu Cyberparawan
https://www.facebook.com/CERT.Polska/posts/pfbid0E3A2SeVADg7CJpMnEmWJ941PUnKZKqaCNeRuSCMLVLNcH9D712VQq5L6QeeSiUykl

27.06

Atak hackerski na systemy IT w Olsztynie
https://sekurak.pl/atak-hackerski-na-systemy-it-olsztyna-jednostka-zdzit-nie-dzialaja-systemy-sterowania-ruchem-biletomaty

Lipiec

21.07

Krajowe kwalifikacje do EuropeanCyberSecurityChallenge 2023
https://hack.cert.pl

Sierpień

1.08

Zostaliśmy CNA - CERT Polska będzie współtworzył bazę podatności CVE
https://cert.pl/posts/2023/08/cna

Wrzesień

01.09

CERT Polska udaremnił szeroko zakrojoną kampanię phishingową
https://twitter.com/CERT_Polska/status/1697186759019209199

15.09

Udostępnienie narzędzia Bezpieczna poczta
https://bezpiecznapoczta.cert.pl

25.09

Wejście w życie Ustawy o zwalczaniu nadużyć w komunikacji elektronicznej (UZNKE)
https://cert.pl/posts/2023/09/uznke

Październik

1.10

Kulminacja nasilenia kampanii phishingowych i dezinformacyjnych prowadzonych przez grupę UNC1151 w związku z nadchodzącymi wyborami parlamentarnymi
Więcej w rodziale o aktywności grup APT

03.10

Uwaga na fałszywe sklepy internetowe oferujące tani węgiel
https://www.facebook.com/CERT.Polska/posts/pfbid02JwYBoAv8GHc3M44y7vxyMK6ze8rAYbRgh8uY2CaZTbSK25SjA6548aE1VJ563of8l

10.10

10 tysięcy domen sprawdzonych w serwisie bezpiecznapoczta.cert.pl
https://www.facebook.com/CERT.Polska/posts/pfbid0e1BXLy7WfefMgighRPHejKjBTccaTM3QrFkQeLMLHaxgq658i2c5drMxZKhXq3PHl

20.10

Firma Cisco opublikowała informację o krytycznej podatności CVE-2023-20198 w funkcjonalności Web User Interface oprogramowania Cisco IOS XE.
https://cert.pl/posts/2023/10/cisco-cve-2023-20198

Listopad

13.11

Przeglądarka Google Chrome rezygnuje z ikony kłódki na pasku adresu
https://blog.chromium.org/2023/05/an-update-on-lock-icon.html

22.11

Uruchomiliśmy nowy numer (8080) do zgłoszeń SMS
https://twitter.com/NASK_pl/status/1727255424519557460

27.11

Wyciek danych z laboratoriów Alab
https://zaufanatrzeciastrona.pl/post/wyniki-badan-medycznych-kilkudziesieciu-tysiecy-polakow--ujawnione-przez-wlamywaczy

Grudzień

05.12

CERT Polska na OhMyHack
https://omhconf.pl/#agenda

13.12

Artemis ma rok
https://cert.pl/posts/2023/12/artemis-podsumowanie

Incydenty i zagrożenia w 2023

Przegląd nowych kampanii i ewolucja już znanych

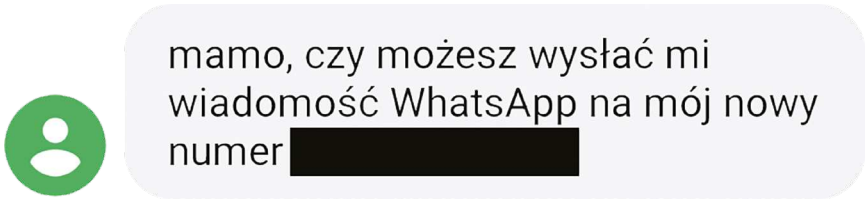
Celem cyberprzestępców zazwyczaj są nasze pieniądze i dane. I chociaż od lat pozostaje on taki sam, to zmieniają się techniki wykorzystywane w atakach.

Nowe kampanie

Wakacyjne oszustwo

W okresie wakacyjnym zaobserwowaliśmy nową metodę stosowaną przez cyberprzestępców - wakacyjne oszustwo. Nasilenie tej kampanii miało miejsce w lipcu i sierpniu, czyli w czasie, kiedy dzieci i młodzież często przebywali poza domem.

Przestępcy wysyłali wiadomości takie jak poniżej:



Rysunek 3: Przykład wiadomości wysyłanej przez przestępców

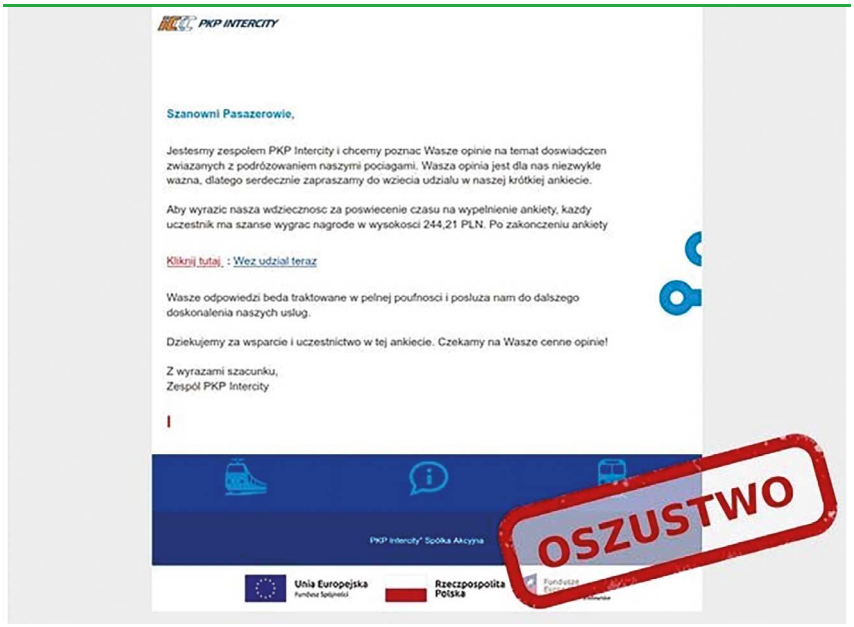
Krótka wymiana zdań na WhatsApp prowadziła do wyłudzenia pieniędzy od niczego nieświadomych rodziców. Podczas konwersacji oszuści wyjaśniali, dlaczego kontaktują się z nieznanego numeru (utrata telefonu) oraz próbowali zdobyć podstawowe informacje o dziecku, co miało umożliwić skuteczniejsze podszywanie się w dalszej rozmowie.

Jeśli oszust dowiadywał się, że rodzic nie ma bankowości elektronicznej, to prosił o dane z karty płatniczej i kod SMS autoryzujący operację, aby w ten sposób uzyskać dostęp do pieniędzy rodzica. Kiedy natomiast okazywało się, że rodzic nie miał na swoim koncie żądanej kwoty, oszust proponował zakup tańszego telefonu.

Ankiety

Fałszywe ankiety nie są wyszukanym oszustwem, jednak według naszych obserwacji mogą być skuteczne. Chęć zysku przy niskim nakładzie pracy zachęca ludzi do wzięcia w nich udziału. Nie u wszystkich wzbudza podejrzenie konieczność podania danych personalnych, często poufnych.

W okresie wakacyjnym zaobserwowaliśmy kampanię, w której oszuści podszywali się pod PKP Intercity. Po wypełnieniu ankiety badania satysfakcji z usług przewoźnika, użytkownik mógł otrzymać nagrodę pieniężną. W celu jej odebrania należało wpisać dane karty płatniczej na fałszywej stronie.



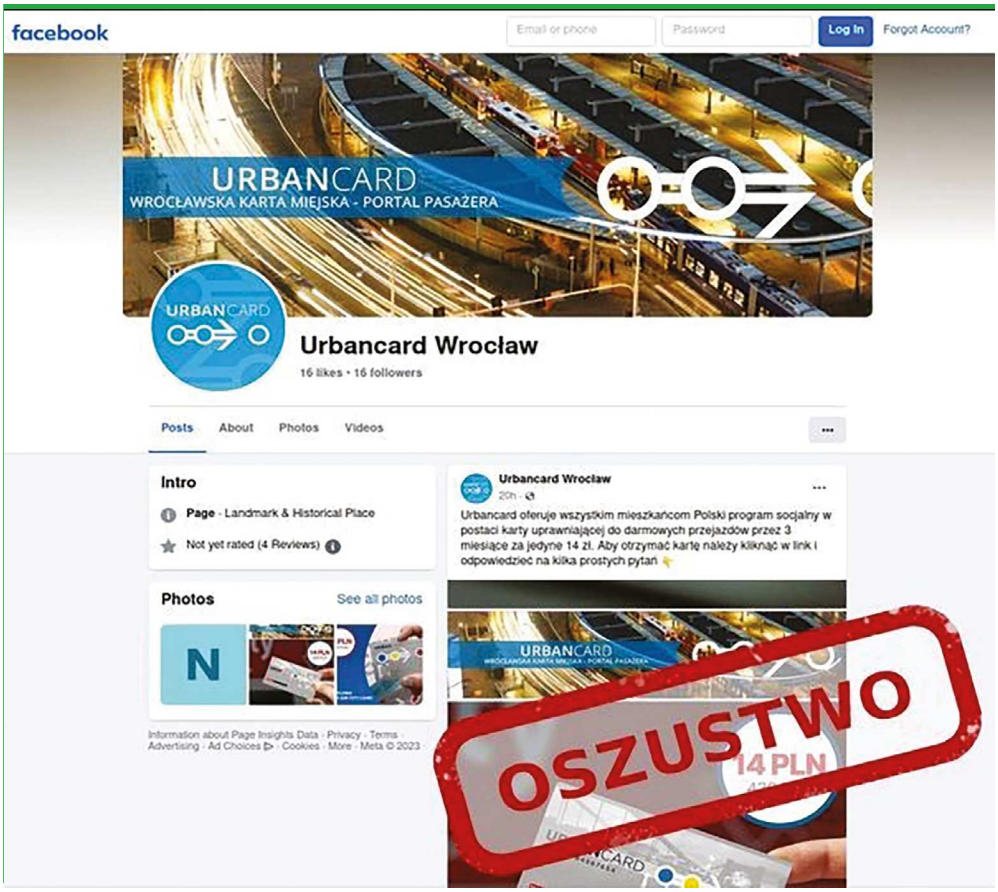
Rysunek 4: Fałszywe ankiety podszywające się pod PKP Intercity

W październiku zaczęliśmy rejestrować domeny zawierające fałszywe ankiety, w których nagrodami miały być darmowe bilety długookresowe w największych polskich aglomeracjach. Bilety miały być udostępnione zainteresowanym jako wygrana loterii po wypełnieniu ankiety i dokonaniu niewielkiej płatności na fałszywej stronie. Oczywiście wszystkie potencjalne ofiary wygrywały loterię, a dane karty płatniczej trafiały w ręce oszustów.

Rysunek 5: Domena z nieprawdziwą ankietą

Ogromna zniżka na bilety komunikacji miejskiej była wykorzystywana także w kolejnej odsłonie tej kampanii z innym wektorem. Nowy wariant oszustwa polegał na stworzeniu fałszywych profili na Facebooku. Za ich pośrednictwem udostępniane były posty informujące o możliwym zdobyciu

Wrocławskiej lub Warszawskiej Karty Miejskiej w atrakcyjnej cenie. Link zawarty w poście prowadził do strony wyłudzającej dane osobowe. Następnym etapem tego oszustwa był panel wyłudzający dane karty płatniczej.



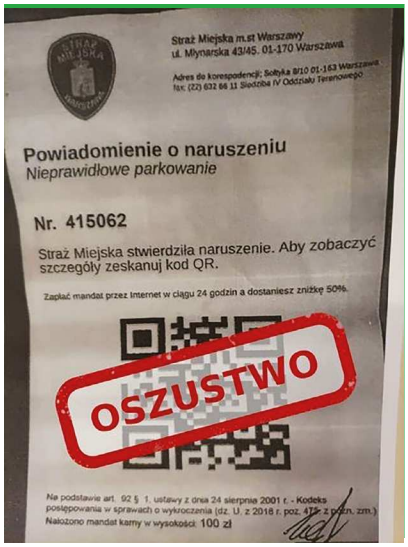
Rysunek 6: Fałszywy profil na Facebooku oferujący kartę miejską w niższej cenie

Wykorzystanie kodu QR

Wektorem ataku nie zawsze muszą być SMS-y czy e-maile. Czasami ataki zaczynały się od naklejek.

W lipcu zaczęliśmy otrzymywać zgłoszenia informujące o kodach QR naklejonych na miejskich parkometrach. Kierowcy chcący uiścić opłatę za parking, po zeskanowaniu kodu byli przenoszeni na stronę zawierającą logo miasta Krakowa. Strona miała na celu wyłudzenie danych karty płatniczej. W ten sposób nieświadomi mieszkańcy Krakowa i turyści mogli przekazać dane karty w ręce przestępców.

Za to w październiku kierowcy parkujący w centrum Warszawy mogli znaleźć za wycieraczkami samochodu nieprawdziwe powiadomienie o nieprawidłowym parkowaniu. Dokument miał być rzekomo wystawiony przez Straż Miejską i zawierał kod QR, którego zeskanowanie miało umożliwić kierowcy zweryfikowanie szczegółów wystawionego mandatu. Dodatkową zachętą do wykonania działań miało być zredukowanie kwoty mandatu o 50 procent, jeśli zostanie on opłacony w przeciągu 24 godzin. Strona, do której był przenoszony kierowca po zeskanowaniu kodu, podszywała się pod Policję i wyłudzała dane uwierzytelniające do bankowości online.



Rysunek 7: Fałszywe powiadomienie o naruszeniu za nieprawidłowe parkowanie

Kampania GuLoader

Nie samymi phishingami przestępcy żyją. We wrześniu wystartowała kampania mailowa, w której oszuści podszywali się pod Urząd Zamówień Publicznych. Treść wiadomości informowała o przetargu w związku z kontraktami rządowymi. Warto jednak zauważyć, że była ona napisana łamaną polszczyzną, bez zachowania zasad interpunkcji. W załączniku wiadomości znajdował się skompresowany plik, który po rozpakowaniu i uruchomieniu infekował komputer ofiary złośliwym oprogramowaniem GuLoader. To wyspecjalizowane i jedno z najbardziej znanych szkodliwych oprogramowań, którego zadaniem jest pobranie i uruchomienie kolejnych złośliwych modułów. Te z kolei mają wykonać konkretne działania - kradzież danych lub umożliwienie zdalnego dostępu do urządzenia.

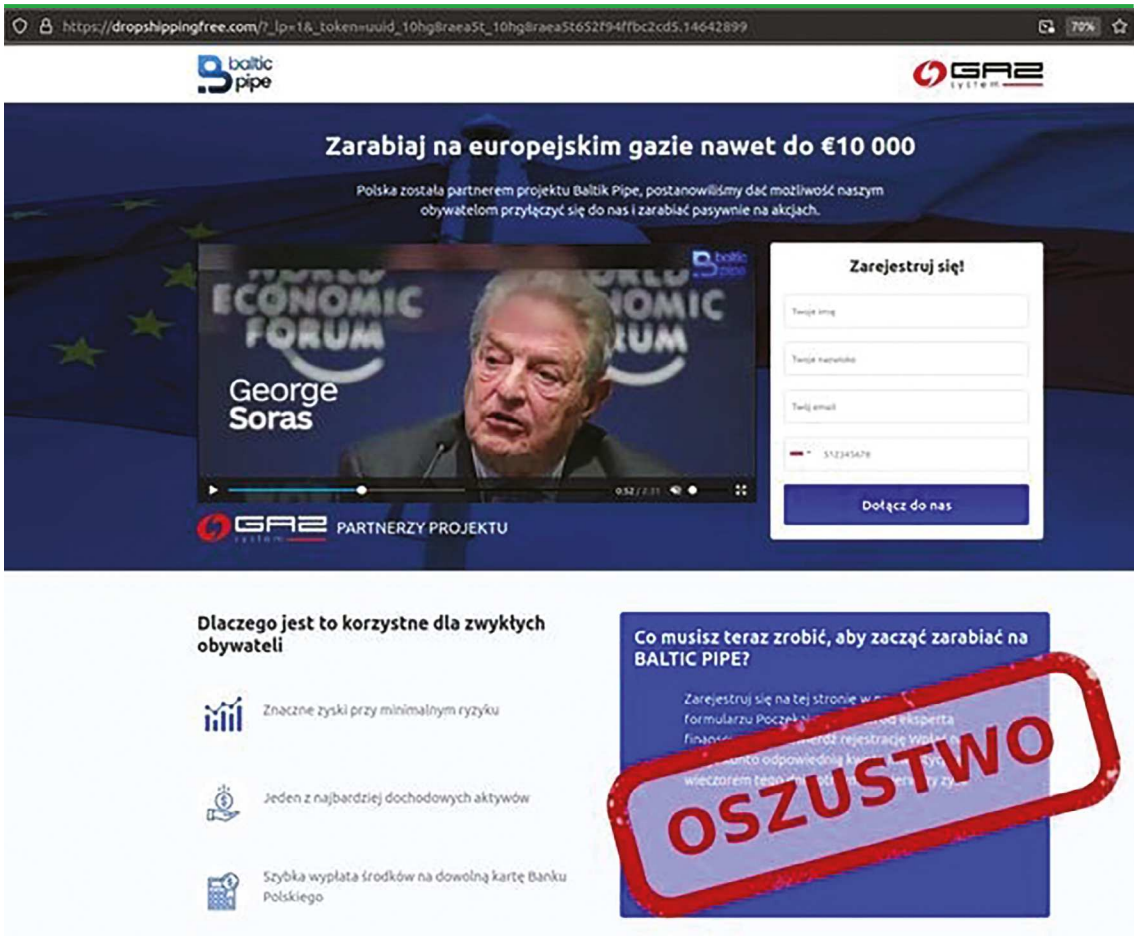
Rysunek 8: Wiadomość e-mail rozpowszechniająca GuLoader

Kontynuacja kampanii z poprzednich lat

Najwięcej obserwowanych przez nas kampanii opiera się na znanych technikach wykorzystywanych przez lata. Niektóre z kampanii nie zmieniają się, w niektórych zauważamy nieznaczne modyfikacje i udoskonalenia.

Fałszywe reklamy inwestycyjne

Jedna z większych kampanii to fałszywe reklamy zachęcające do inwestowania na giełdzie lub w kryptowaluty. Tego typu domeny są najczęściej wpisywanymi przez nas na listę ostrzeżeń. Schemat działania oszustów pozostaje od początku taki sam. Użytkownik jest zachęcany do bardzo opłacalnej inwestycji. Reklamowane są platformy inwestycyjne, za pomocą których można inwestować w kryptowaluty lub akcje firm. Do rozpoczęcia inwestycji niezbędne jest podanie na stronie danych kontaktowych. W dalszym etapie przedstawiciel firmy oferującej fałszywe inwestycje kontaktuje się z zainteresowanym telefonicznie i nakłania do ulokowania finansów i wykonanie przelewu. Platformy zawsze obiecują duży zysk z zainwestowanych pieniędzy. W rzeczywistości „zainwestowane" pieniądze trafiają na konta oszustów, a jakiekolwiek wzrosty i możliwość wzbogacenia się to jedynie socjotechniczny wabik.



Rysunek 9: Przykład reklamy nakłaniającej do inwestycji

Fałszywe panele logowania do Facebooka

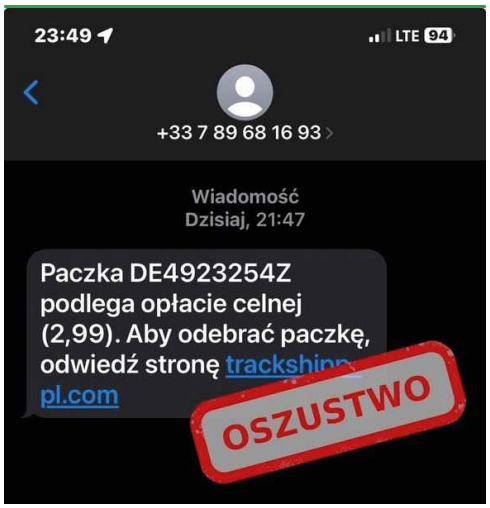
Cały czas obserwujemy nowe odsłony fałszywych paneli logowania do Facebooka. Posty z odnośnikiem były publikowane na grupach na Facebooku, wykorzystując zazwyczaj głośne w danym czasie sprawy. Często pojawiają się również wzbudzające emocje nieprawdziwe artykuły. Zazwyczaj w artykule jest link do rzekomego nagrania. Dostęp do niego mogą mieć jedynie osoby pełnoletnie, dlatego konieczna jest weryfikacja wieku. Ta weryfikacja ma się odbyć przez ponowne logowanie do Facebooka. Użytkownik jest przenoszony na stronę łudząco przypominającą panel logowania platformy. Oczywiście wykorzystywane domeny nie mają nic wspólnego z portalem społecznościowym i są phishingiem wyłudzającym dane logowania.

Rysunek 10: Fałszywy artykuł udostępniany na Facebooku

Dopłaty do paczek

Niewiele się zmieniło także w kampanii dopłat do paczek. Cały czas obserwujemy masowe akcje tego typu. Oszuści wykorzystują wizerunek niemal wszystkich operatorów logistycznych. Rzekomymi nadawcami wiadomości SMS bywają firmy takie jak Inpost, Poczta Polska, DPD czy DHL. Wektorem oszustwa najczęściej są SMS-y. Mniej popularne są wiadomości e-mailowe.

W masowo wysyłanych wiadomościach zawarta jest informacja o konieczności dopłaty za paczkę. Takie działanie ma być konieczne z powodu przekroczonej wagi przesyłki, dodatkowej opłaty za cło, nieobecności odbiorcy w domu lub niepełnego adresu odbiorcy. Zazwyczaj opłata jest niewielka, aby uśpić czujność potencjalnej ofiary.

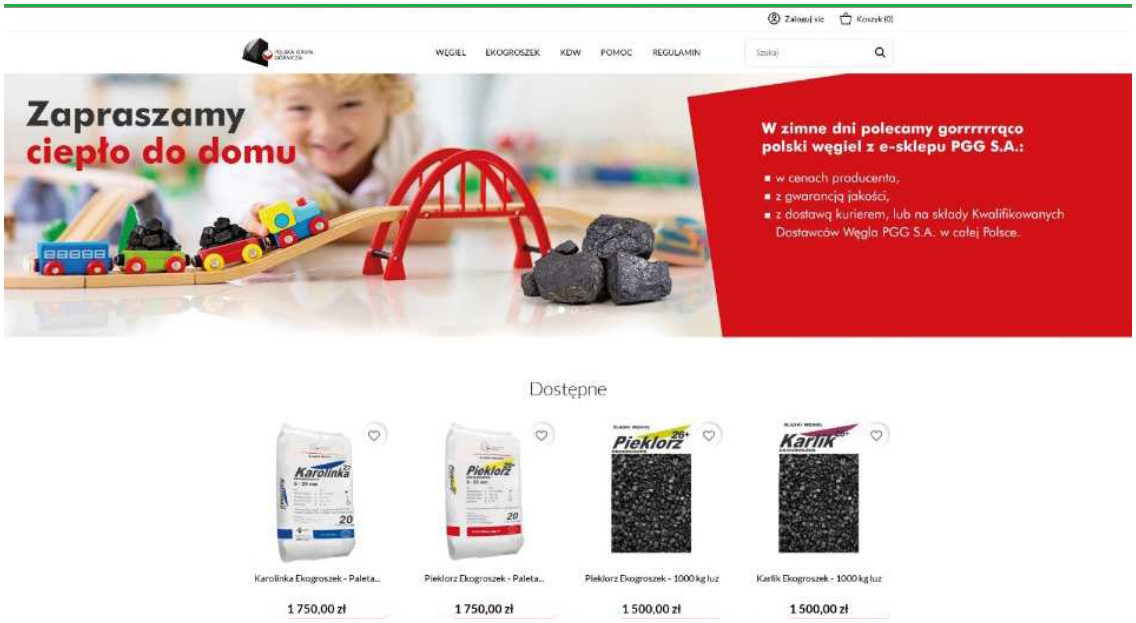


Rysunek 11: Przykład wiadomości SMS informującej o rzekomej opłacie celnej

Wiadomości zawierają link, który przekierowuje, w zależności od wariantu, na fałszywą stronę bramki płatności lub stronę wyłudzającą dane karty płatniczej.

Fałszywe sklepy z węglem

W 2022 roku zaobserwowaliśmy nowy typ oszustwa - fałszywe sklepu z węglem. Kampania wykorzystywała kryzys energetyczny związany z wojną w Ukrainie. W 2023 roku na początku października, czyli wraz z rozpoczęciem sezonu grzewczego, schemat ten powrócił. Skala była mniejsza niż rok wcześniej, jednak działanie oszustów było identyczne. Oferowali oni węgiel z polskich kopalni w wyjątkowo korzystnej cenie. Płatność można było zrealizować jedynie przelewem bankowym, co zamykało oszukanym użytkownikom możliwość odzyskania pieniędzy.

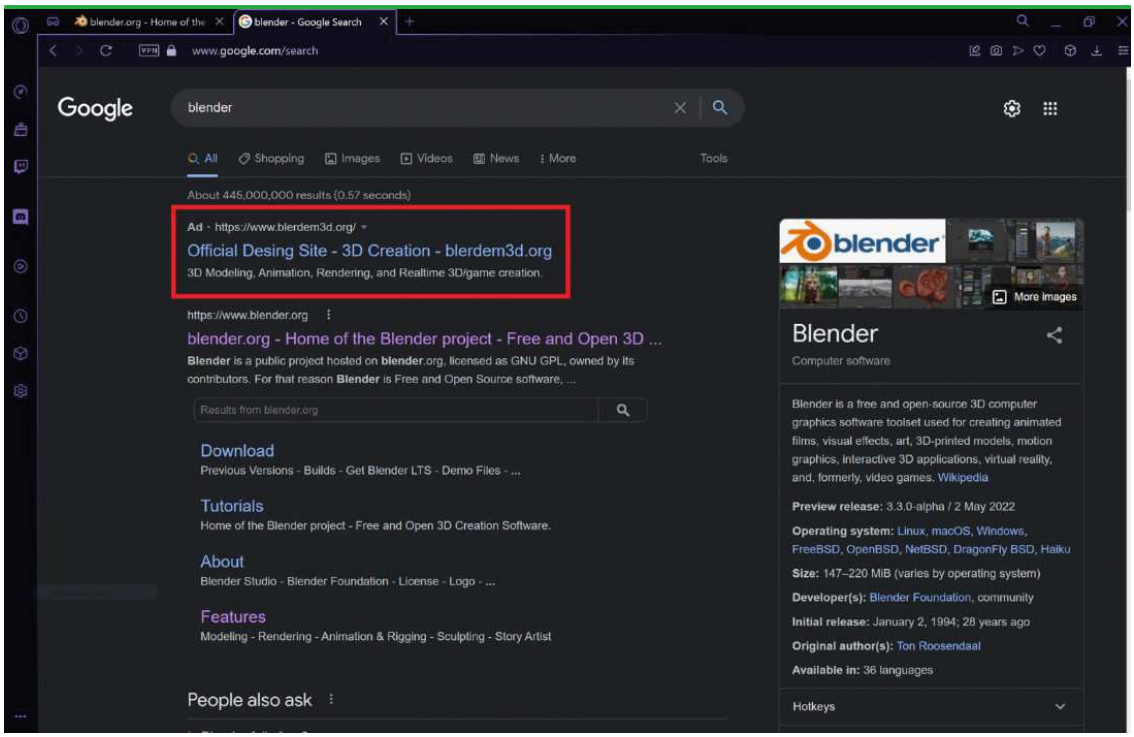


Rysunek 12: Sklep podszywający się pod oficjalny sklep PGG

Kampania szkodliwych reklam

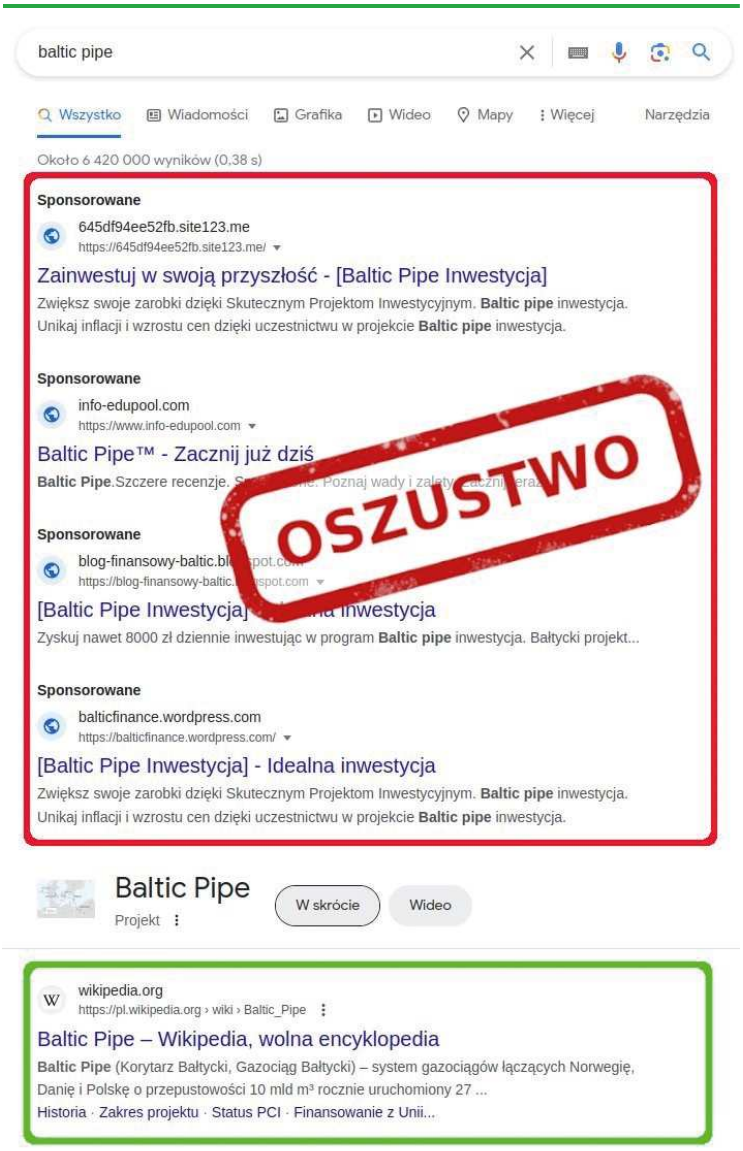
W połowie 2022 roku przestępcy zaczęli wykorzystywać wysokie pozycjonowanie w wyszukiwarce Google w celu rozpowszechniania szkodliwego oprogramowania. Ten typ oszustwa jest przez nas obserwowany cały czas. Strony pojawiają się na pierwszych miejscach w wyszukiwarce i są oznaczone jako reklamy. Te reklamy odnoszą do stron podszywających się pod producentów oprogramowania. Zazwyczaj już na głównej stronie użytkownik ma możliwość pobrania złośliwego oprogramowania. Strona przypomina witrynę z legalnym programem, a dodatkowo użytkownik dostaje się na nią z wyszukiwarki. To skutecznie usypia czujność.

Za pomocą tego oszustwa dystrybuowany był instalator BiTLoader wykorzystywany do infekowania komputerów ransomwarem Royal. Innym wariantem był IcedID, który dostarczał kolejne niepożądane programy lub skrypty np. Cobalt Strike. Uruchomienie pobranego pliku prowadzi najczęściej do zainfekowania systemu szkodliwym oprogramowaniem, które wykrada dane z urządzenia i przesyła je do przestępców. W ten sposób atakujący uzyskują m.in. dostęp do danych uwierzytelniających do serwisów, z których korzysta ofiara.



Rysunek 13: Przykład szkodliwej reklamy

Oszuści za pomocą wysokiego pozycjonowania rozpowszechniali również fałszywe inwestycje, które zostały opisane wcześniej.

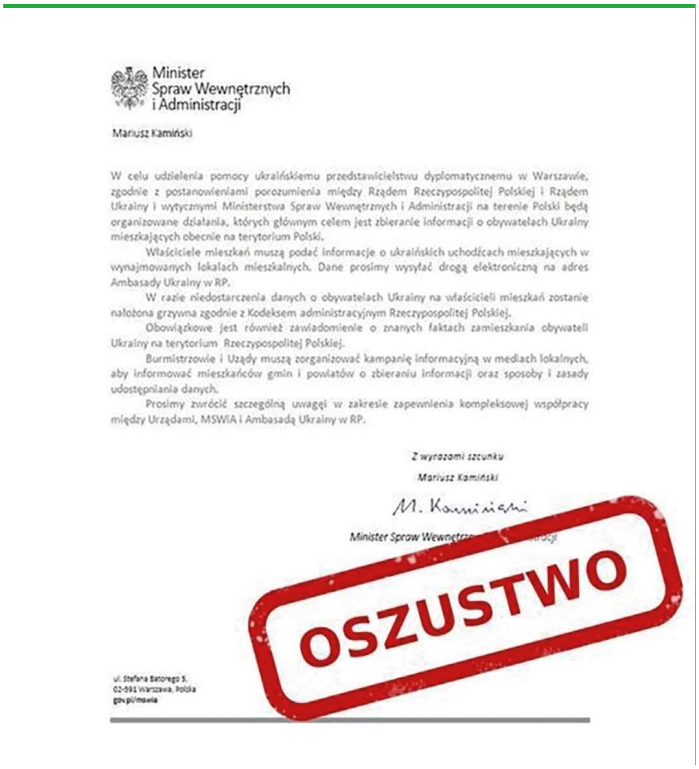


Rysunek 14: Wysoko pozycjonowane reklamy fałszywych inwestycji

Podszycia pod strony rządowe

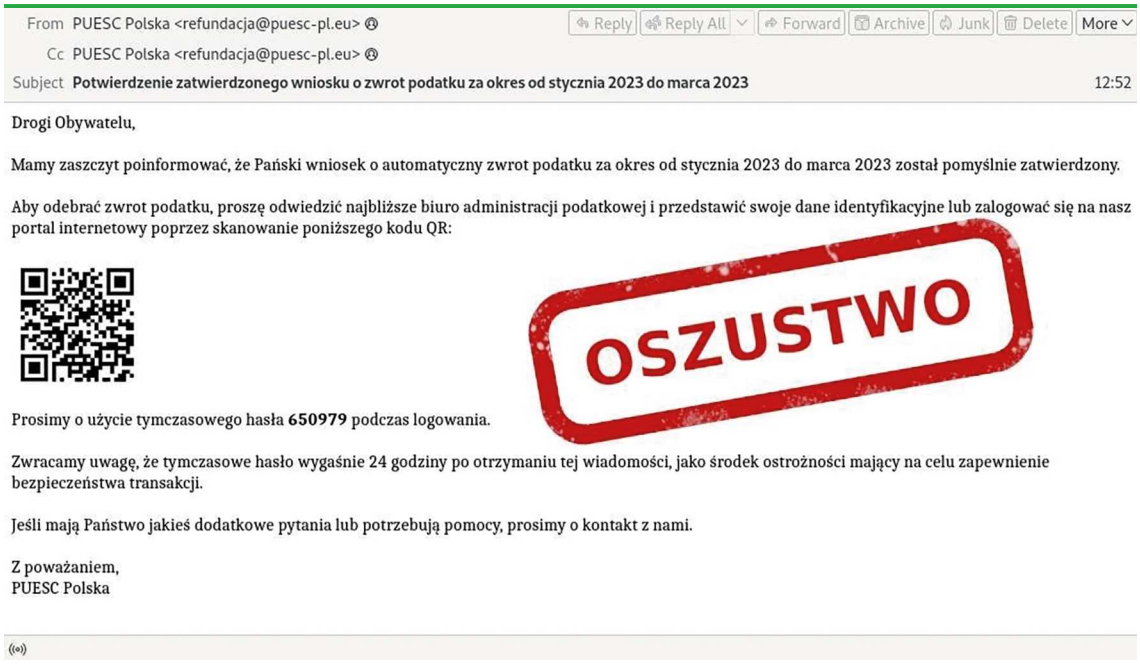
Już w 2022 roku zaobserwowaliśmy nasilenie oszustw wykorzystujących wizerunek stron i instytucji rządowych. W 2023 roku kampanie tego typu również były częste. A schematy w nich wykorzystywane były ciekawe i warte opisania.

W styczniu odnotowaliśmy kampanię phishingową podszywającą się pod Krajową Administrację Skarbową. Podobne oszustwa obserwujemy od lat głownie w okresach rozliczania podatku, ale, co ciekawe, także w miesiącach niezwiązanych z działalnością organów podatkowych. Wiadomości mailowe informowały o pozytywnym rozpatrzeniu wniosku o automatyczny zwrot podatku. Zwrot pieniędzy miał być możliwy poprzez przelew bankowy, który miał zostać wypłacony po zalogowaniu na konto bankowe. Oczywiście logowanie na fałszywej stronie skutkowało utratą pieniędzy, a nie ich zdobyciem.



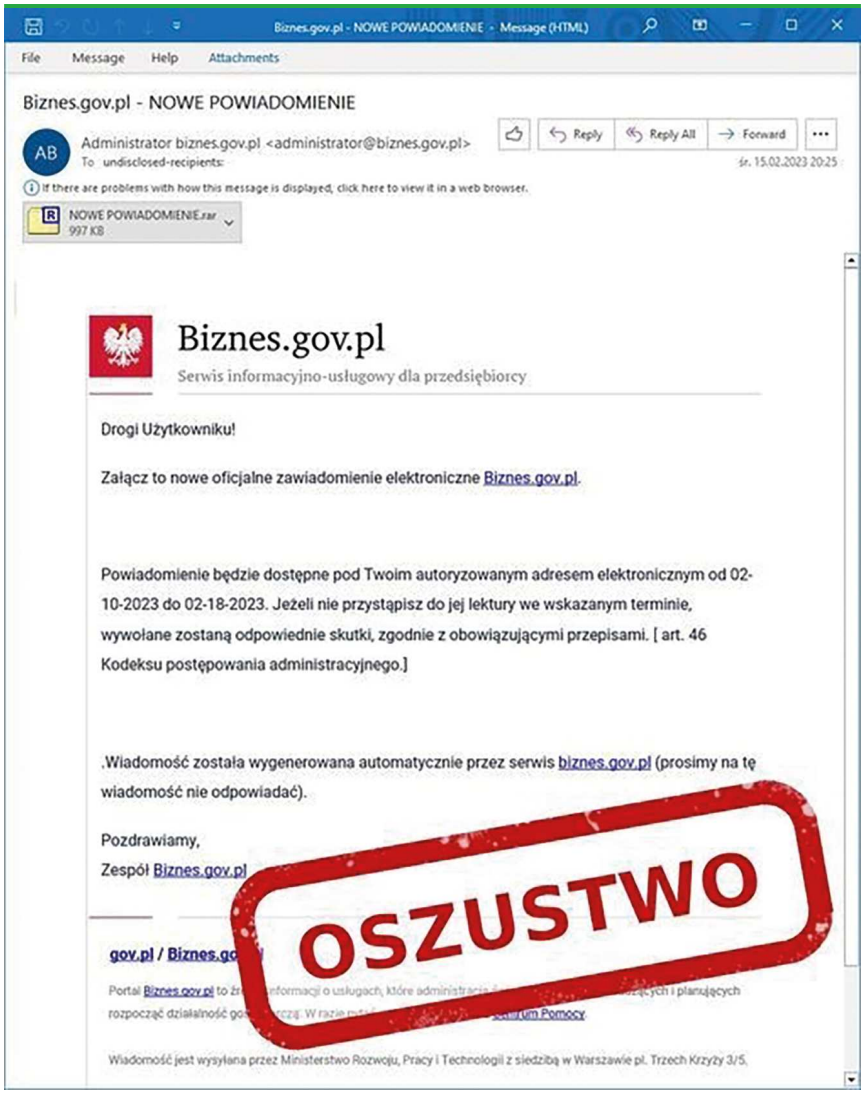
Rysunek 15: Rzekomy zwrot podatku. Podszycie pod Krajową Administrację Skarbową

Kolejna odsłona tej kampanii miała miejsce pod koniec marca. Tym razem wektorem były SMS-y. W wiadomości znajdowała się informacja o rzekomym zatwierdzeniu zwrotu podatku, a link przenosił do strony wyłudzającej dane logowania do bankowości on-line. W innym wariancie w wiadomościach e-mailowych znajdował się kod QR, który również przenosił na stronę wyłudzającą dane logowania do bankowości.



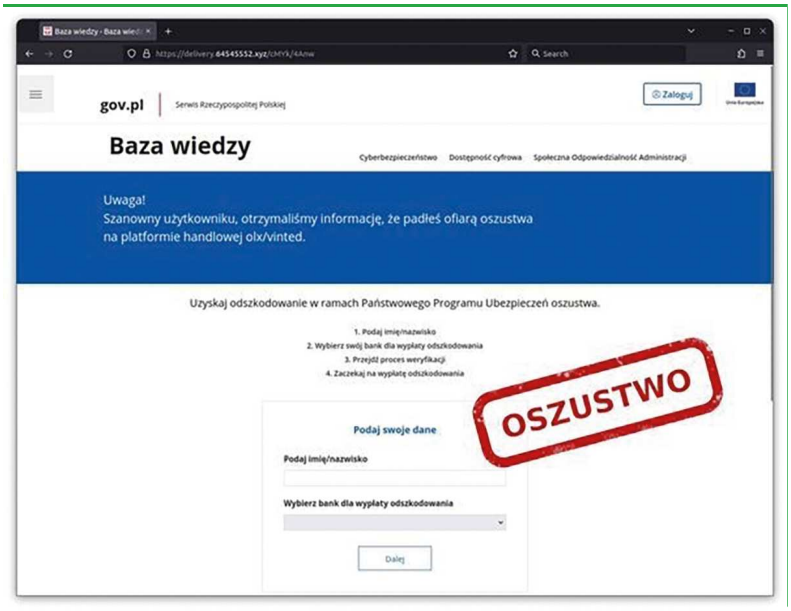
Rysunek 16: Wiadomość e-mail z kodem QR przenoszącym do strony phishingowej

W lutym zaobserwowaliśmy powrót kampanii e-mailowej wykorzystującej wizerunek Ministerstwa Rozwoju i Technologii. W wiadomościach znajdowała się informacja o rzekomym zawiadomieniu z portalu biznes.gov.pl. Załącznik zawierał złośliwe oprogramowanie. Był to trojan, który wykradał dane z zainfekowanego systemu.



Rysunek 17: Wiadomość e-mail rozpowszechniająca szkodliwe oprogramowanie

Kreatywność oszustów dała o sobie znać na początku marca, kiedy zaczęły spływać do nas zgłoszenia obrazujące kampanię SMS-ową. Było to połączenie dwóch znanych schematów. Masowo wysyłane SMS-y były zaproszeniem do odebrania rekompensaty za oszustwo na platformie OLX lub Vinted. Odnośnik w wiadomości przenosił do strony wykorzystującej wizerunek serwisu Rzeczypospolitej Polskiej. Użytkownik był informowany o możliwości uzyskania odszkodowania w ramach rzekomego Państwowego Programu Ubezpieczeń od oszustwa. Na dalszym etapie ofiara zachęcana była do zalogowania się na swoje konto bankowe. Oczywiście strona, na której należało to zrobić, była fałszywa. W ten sposób po podaniu danych logowania do bankowości, trafiały one w ręce oszustów, co skutkowało jak zawsze w takich sytuacjach - utratą pieniędzy z konta.

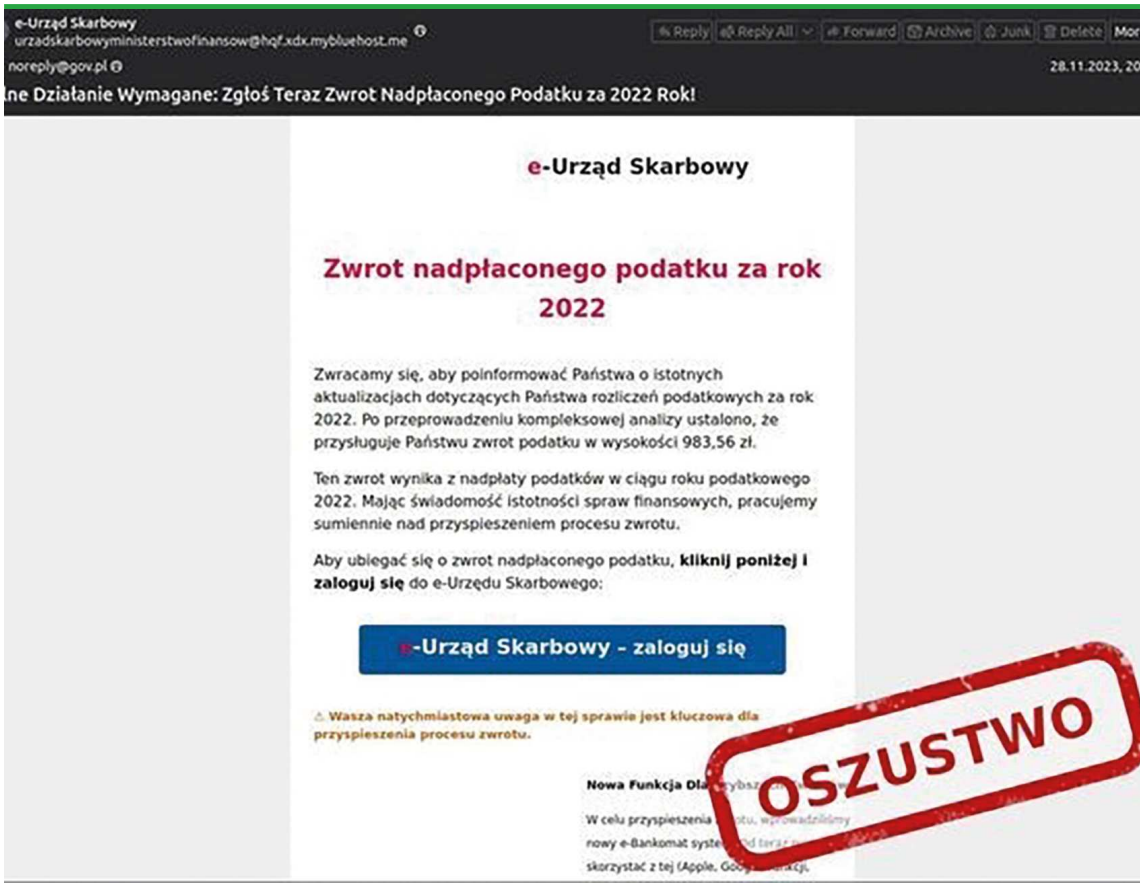


Rysunek 18: Strona podszywająca się pod gov.pl

Maj upłynął pod znakiem kampanii wyłudzającej dane osobowe i dane karty płatniczej. Do potencjalnych ofiar docierała wiadomość zachęcająca do odebrania świadczenia przyznanego przez ZUS. Link prowadził do strony phishingowej podszywającej się pod Ministerstwo Rodziny i Polityki Społecznej.

Rysunek 19: Strona podszywająca się pod Ministerstwo Rodziny i Polityki Społecznej

W sierpniu oraz na przełomie listopada i grudnia zaobserwowaliśmy niedużą kampanię fałszywych maili, które informowały o zwrocie nadpłaconego podatku za rok 2022. Wiadomość zawierała odnośnik do rzekomego e-Urzędu Skarbowego. Link przekierowywał na fałszywą stronę wykorzystującą wizerunek Urzędu Skarbowego i Ministerstwa Finansów. Dzięki tej stronie miał nastąpić zwrot środków finansowych. W rzeczywistości strona wyłudzała dane osobowe oraz dane uwierzytelniające do bankowości on-line.



Rysunek 20: Fałszywa informacja o zwrocie nadpłaconego podatku

Obserwowane działania grup APT

Od czasu rozpoczęcia wojny w Ukrainie obserwujemy znaczne nasilenie aktywności grup APT, często wiązanych z obcymi państwami. Większość tych działań ma na celu pozyskanie informacji, ale w 2023 r. zdarzały się również ataki – wymierzone w szczególności w sektor transportu i w logistykę – których celem było zakłócenie ciągłości działania.

Warto też zaznaczyć, że przypadki opisywane w tym raporcie są tylko fragmentem działalności grup APT, obserwowanym przez CERT Polska/CSIRT NASK i nie oddają w pełni skali znanych ataków tych grup na polskie podmioty.

Obserwowana przez nas aktywność grup APT w 2023 r. została zaprezentowana w Tabeli 1. Można zauważyć, że znaczna część grup jest wiązana z Federacją Rosyjską i niektóre z nich przejawiają stałą aktywność.

	Styczeń	Luty	Marzec	Kwiecień	Maj	Czerwiec	Lipiec	Sierpień	Wrzesień	Październik	Listopad	Grudzień
UNC1151 | Ghostwriter (Rosja/Białoruś)	X	X	X	X	X	X		X	X	X	X	
APT28 | Fancy Bear | Forest Blizzard (Rosja)			X		X		X		X	X	X	X
APT29 | Cozy Bear | Midnight Blizzard (Rosja)	X	X	X	X	X	X	X				X	X
Callisto | Star Blizzard | Coldriver (Rosja)						X		X	X	X		
Sandworm | Voodo Bear | Seashell Blizzard (Rosja)		X										
Gamaredon | Primitive Bear | Aqua Blizzard (Rosja)	X	X										
Turla | Venomous Bear | Secret Blizzard (Rosja)		X	X									X
Winter Vivern (Rosja)		X								X		
Mustang Panda (Chiny)	X	X										
APT-UNK1		X						X				
APT-UNK2									X	X		

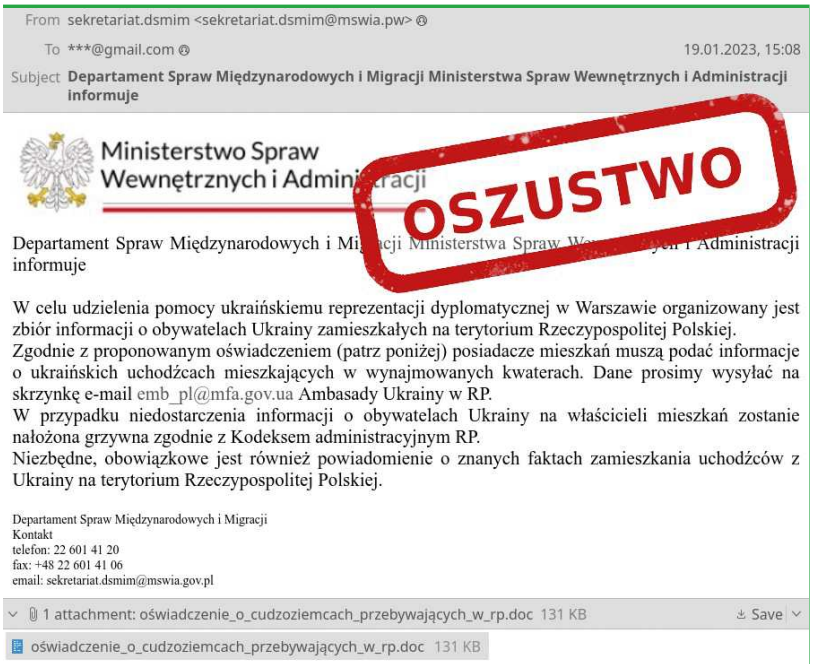
Tabela 1: Aktywność grup APT obserwowanych przez CERT Polska/CSIRT NASK w 2023 r

Wybrane kampanie

UNC1151/Ghostwriter

W 2023 r. najbardziej aktywna była grupa UNC1151, powiązana z operacją Ghostwriter. Firmy Mandiant[2] i Google[3], w swoich publikacjach wskazały, że grupa ta z dużym prawdopodobieństwem jest powiązana z rządem Białorusi, ale według innych publikacji ma również związek z rosyjskimi służbami specjalnymi[4]. Celami ataków są głównie osoby związane z polityką i wojskowością oraz mogące mieć pośredni związek z Rosją i Białorusią, np. tłumacze przysięgli języka rosyjskiego, prawnicy, pracownicy organizacji pozarządowych, księża prawosławni czy dziennikarze. Atakowano nie tylko polskich obywateli, podobne ataki obserwowano również w Ukrainie, Litwie, Łotwie, czy w Niemczech. Motywacją była najczęściej kradzież informacji w celach wywiadowczych oraz prowadzenia kampanii dezinformacyjnych.

W przeszłości grupa ta specjalizowała się w atakach phishingowych na prywatne skrzynki pocztowe, o czym pisaliśmy w roku 2022[5]. Natomiast w 2023 r. większość obserwowanej aktywności była związana z dystrybucją szkodliwego oprogramowania oraz dezinformacją. W pierwszym kwartale 2023 roku zaobserwowaliśmy duże kampanie dezinformacyjne w Polsce, Litwie i Łotwie, związane z rzekomymi ćwiczeniami przy granicy z Ukrainą, brakiem jodku potasu w aptekach, zagrożeniem terrorystycznym na terenie Polski, rekrutacją do wojska, czy zbieraniem informacji o uchodźcach (rys. 21). W naszej ocenie głównym celem prowadzonych kampanii było wprowadzanie niepewności i pogłębienie podziałów w społeczeństwie.



Rysunek 21: Przykładowa wiadomość będąca częścią kampanii deziformacyjnej dot. zbierania informacji o uchodźcach

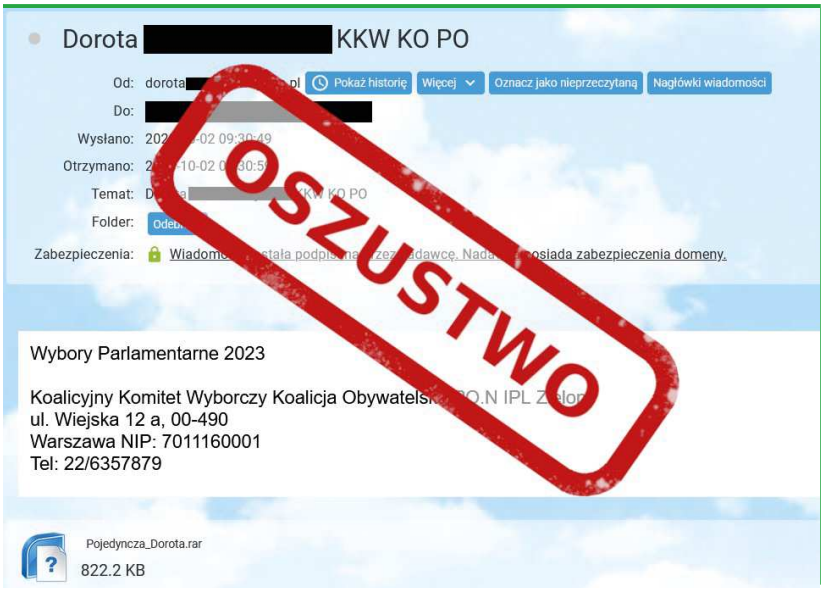
2 https://www.mandiant.com/resources/unc1151-linked-to-belarus-government

3 https://blog.google/threat-analysis-group/update-threat-landscape-ukraine

4 https://www.gov.pl/web/sluzby-specjalne/ustalenia-abw-i-skw-dot-atakow-hakerskich

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

W kolejnych kwartałach obserwowaliśmy głównie kampanie dystrybucji złośliwego oprogramowania w formie spakowanych plików .chm, przesyłanych jako załącznik do wiadomości e-mail. Przeważała tematyka związana z nadchodzącymi wyborami parlamentarnymi. Docelowo na komputerze ofiary było najczęściej instalowane oprogramowanie COBALT STRIKE, dające atakującym pełny dostęp do zainfekowanej maszyny.



Rysunek 22: Wiadomość phishingowa podszywająca się pod jeden z komitetów wyborczych, zawierająca szkodliwy załącznik

Działania dezinformacyjne, w tym także te z wykorzystaniem materiałów wykradzionych z przejętych skrzynek pocztowych i zainfekowanych komputerów, trwały do czasu wyborów. Zaobserwowaliśmy m.in. ciekawy atak na systemy informacji w wybranych centrach handlowych, gdzie wyświetlono plansze z fałszywymi wiadomościami. Prawdopodobnym wektorem ataku był system firmy zewnętrznej (dostępny z internetu), służący do zarządzania treścią na wyświetlaczach.

Rysunek 23: Fałszywa informacja wyświetlona na przejętym systemie w centrum handlowym

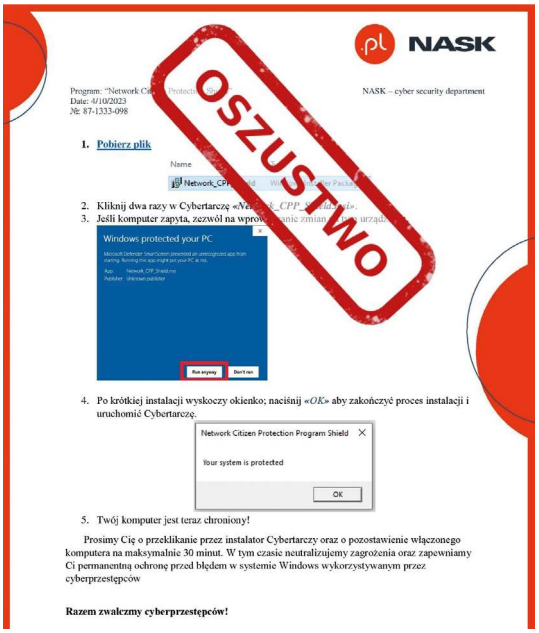
Po wyborach parlamentarnych aktywność grupy UNC1151 znacznie zmalała.

APT28 / Fancy Bear / Forest Blizzard

Główną informacją związaną z grupą APT28 w roku 2023 było ujawnienie wykorzystywania przez nią podatności typu 0day w Microsoft Outlook (CVE-2023-23397) co najmniej od sierpnia 2022 r. Tuż po tym, jak uzyskaliśmy informację o podatności, opublikowaliśmy artykuł z rekomendacjami[6]. Podatność pozwalała atakującemu na zdalne przejęcie skrótu hasła domenowego po otrzymaniu przez ofiarę spreparowanej wiadomości e-mail. Nie wymagało to żadnej interakcji ze strony użytkownika. Z przechwyconego skrótu atakujący był w stanie odzyskać hasło, jeśli nie było ono wystarczająco złożone. Ustalono, że celami ataków były polskie firmy z sektorów transportu, energetyki i zbrojeniowego. W kolejnych miesiącach obserwowaliśmy powtarzające się stosunkowo proste kampanie phishingowe (ukierunkowane na przejęcie haseł do kont pocztowych) oraz dystrybuujące złośliwe oprogramowanie. Większość tych kampanii była wysyłana do szerokiego grona odbiorców z sektorów będących w obszarze zainteresowania grupy.

APT-UNK2

Oprócz grup, których działalność jest dobrze poznana i odpowiednio zakwalifikowana, śledzimy również aktorów, których w danej chwili nie jesteśmy w stanie powiązać z żadną z nich. Jedną z takich grup jest aktor, który przeprowadził kampanię polegającą na podszywaniu się pod NASK. W załączniku do rozesłanego e-maila znajdowała się instrukcja instalacji rzekomego sieciowego programu ochrony obywateli. W trakcie analizy stwierdziliśmy, że podczas uruchomienia pliku z linku podanego w instrukcji dochodziło do infekcji złośliwym oprogramowaniem Lumma Stealer. Oprogramowanie to jest wykorzystywane głównie w atakach motywowanych finansowo, jednak w tym przypadku na podstawie celów oraz powiązanych kampanii oceniamy, że motywacją aktora było pozyskiwanie potencjalnie użytecznych informacji. Ta sama grupa korzystała wcześniej z domen podszywających się pod strony prezentujące treści związane z cyberbezpieczeństwem w Polsce, szczytem NATO w Wilnie, czy organizacjami działającymi na rzecz wolności prasy



Rysunek 24: Kampania, w której podszyto się pod NASK z instrukcją instalacji rzekomego „sieciowego programu ochrony obywateli”

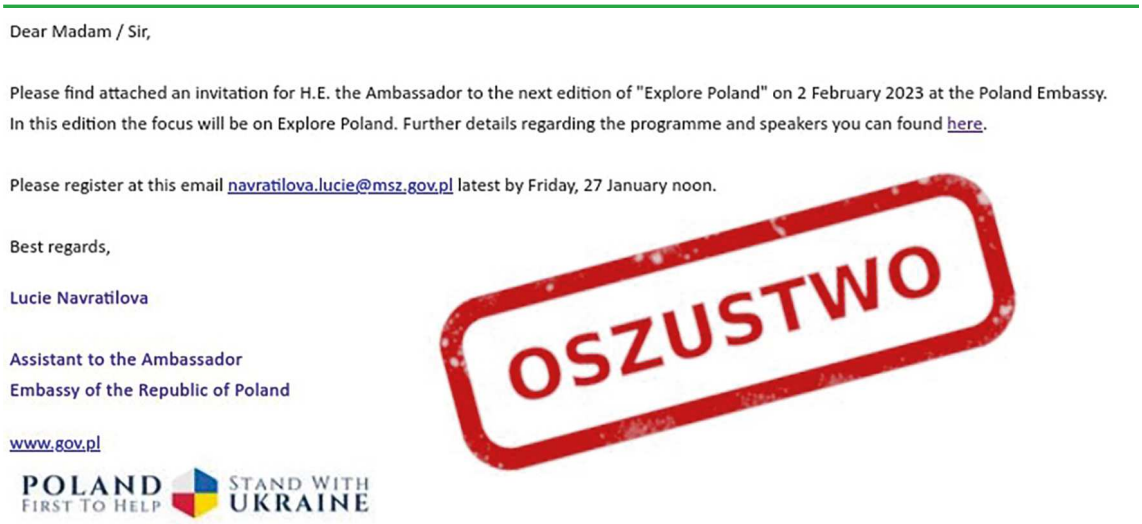
6 https://cert.pl/posts/2023/03/outlook-cve-2023-23397

Współpraca krajowa i międzynarodowa

W ramach codziennej pracy nad aktywnością grup APT blisko współpracujemy z CSIRT-ami poziomu krajowego (CSIRT GOV i CSIRT MON) oraz z zespołami polskich służb specjalnych. Bardzo wartościowa jest również współpraca międzynarodowa w ramach CSIRTs Network oraz z partnerami komercyjnymi. Często prawie identyczne ataki prowadzone są w wielu krajach jednocześnie.

W 2023 r. razem z partnerami dwukrotnie opisywaliśmy obserwowaną aktywność grupy APT29/ Midnight Blizzard, powiązanej z Rosyjską Służbą Wywiadu Zagranicznego (SVR).

Pierwszy raport[7] w tej sprawie wydaliśmy w kwietniu 2023 r. wspólnie ze Służbą Kontrwywiadu Wojskowego. Dotyczył on kampanii szpiegowskiej, której celem było pozyskiwanie informacji z ministerstw spraw zagranicznych oraz placówek dyplomatycznych, w większości znajdujących się w państwach należących do NATO i Unii Europejskiej. Udało się osiągnąć zakładany cel, którym było zakłócenie tej kampanii.


Dear Madam / Sir,

Please find attached an invitation for H.E. the Ambassador to the next edition of "Explore Poland" on 2 February 2023 at the Poland Embassy.
In this edition the focus will be on Explore Poland. Further details regarding the programme and speakers you can found here.

Please register at this email navratilova.lucie@msz.gov.pl latest by Friday, 27 January noon.

Best regards,

Lucie Navratilova

Assistant to the Ambassador
Embassy of the Republic of Poland

www.gov.pl

POLAND FIRST TO HELP STAND WITH UKRAINE

Rysunek 25: Przykładowa wiadomość email wysłana przez grupę APT29, podszywająca się pod polską ambasadę i nakłaniająca do kliknięcia w złośliwy link

Drugi raport[8] dotyczący tej samej grupy opublikowaliśmy w grudniu 2023 r. W operacji opisywanej w raporcie brały udział także Federalne Biuro Śledcze (FBI), Amerykańska Agencja ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury (CISA), Narodowa Agencja Bezpieczeństwa (NSA), Brytyjskie Narodowe Centrum Bezpieczeństwa Cybernetycznego (UK NCSC), oraz polska Służba Kontrwywiadu Wojskowego (SKW). Prowadzone działania dotyczyły przeciwdziałania kampanii, w której wykorzystywana była podatność CVE-2023-42793 w oprogramowaniu JetBrains TeamCity.

Oprogramowanie to jest używane do zarządzania i automatyzacji procesu kompilacji, budowania, testowania i wydawania oprogramowania. Dostęp do serwera TeamCity może prowadzić do dostępu do kodów źródłowych, certyfikatów kryptograficznych oraz może być wykorzystany do wpłynięcia na proces wytwarzania oprogramowania – co z kolei może pozwolić na manipulowanie

7 https://cert.pl/posts/2023/04/kampania-szpiegowska-apt29

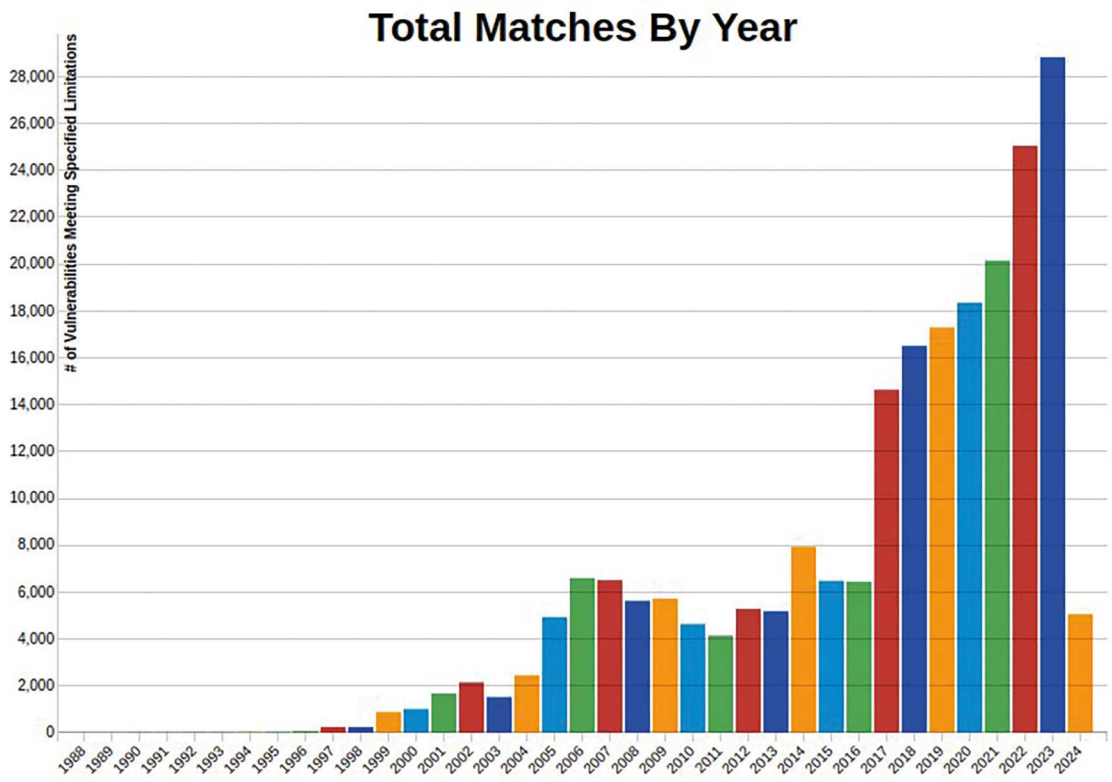
8 https://cert.pl/posts/2023/12/apt29-teamcity

łańcuchem dostaw oprogramowania. Dzięki podjętym działaniom udało się zatrzymać tę kampanię i poinformować ofiary.

Rok 2023 był pierwszym, w którym zdecydowaliśmy się publicznie opisać obserwowane aktywności grup APT. Skłoniła nas do tego sytuacja za wschodnią granicą i związana z tym znacznie zwiększona liczba incydentów dotyczących działań wymierzonych w polskie podmioty. Dlatego też z dumą dzielimy się powyższym podsumowaniem, mając nadzieję, że będzie stanowiło ciekawą lekturę, dla tych, którzy chcą lub potrzebują orientować się w krajobrazie zagrożeń w cyberprzestrzeni.

Najważniejsze podatności w 2023 roku

W 2023 roku po raz siódmy z rzędu nastąpił wzrost liczby nowych podatności (Wykres 1). W bazie National Vulnerability Database, która prowadzona jest przez amerykańską agencję NIST [1], opublikowanych zostało ponad 29 tysięcy nowych podatności. Szczególną uwagę należy również zwrócić na statystyki agencji CISA z bazy znanych i wykorzystywanych podatności [2], które umożliwiają dokładniejszą ocenę aktualnego krajobrazu zagrożeń. Na koniec 2023 roku aktywnie wykorzystywanych było 1074 różnych podatności, z czego 137 stanowiły podatności opublikowane w tym samym roku. Dla porównania, w roku 2022 było to odpowiednio 868 i 92 podatności. Zespół CERT Polska aktywnie monitorował podatności w produktach, które są szeroko wykorzystywane w Polsce. W przypadku uzyskania w ramach działań własnych lub od partnera informacji o podatnej instancji produktu Zespół nawiązywał komunikację z narażonymi podmiotami w celach wdrożenia koniecznych aktualizacji oraz ograniczenia potencjalnego ryzyka.



Wykres 1: 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

[1] https://nvd.nist.gov/

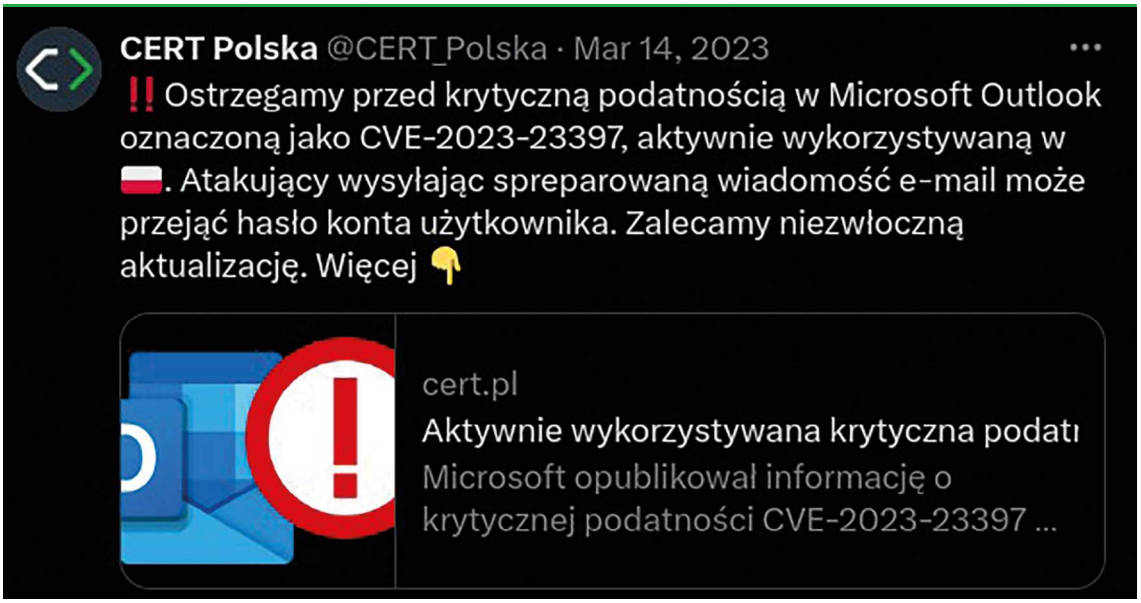
[2] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Microsoft Outlook (CVE-2023-23397)

Krytyczna podatność w aplikacji Outlook w systemie Windows mogła prowadzić do zdalnego przejęcia hasła domenowego bez interakcji użytkownika. Do ataku wystarczało otrzymanie przez ofiarę wiadomości e-mail zawierającej odpowiednio spreparowane wydarzenie kalendarza albo zadanie, które powodowało odwołanie do ścieżki UNC kontrolowanej przez atakującego.

Podatność pozwalała na przechwycenie skrótu NTLMv2 i późniejszą próbę odzyskania hasła domenowego poprzez atak siłowy. W sytuacji, gdy atakujący posiadał dostęp do sieci ofiary, możliwym było również bezpośrednie wykorzystanie skrótu NTLMv2 do zalogowania w innych usługach bez potrzeby łamania, tzw. NTLM relay.

W związku z tą podatnością zespół CERT Polska wysłał 4075 ostrzeżeń do różnych organizacji.

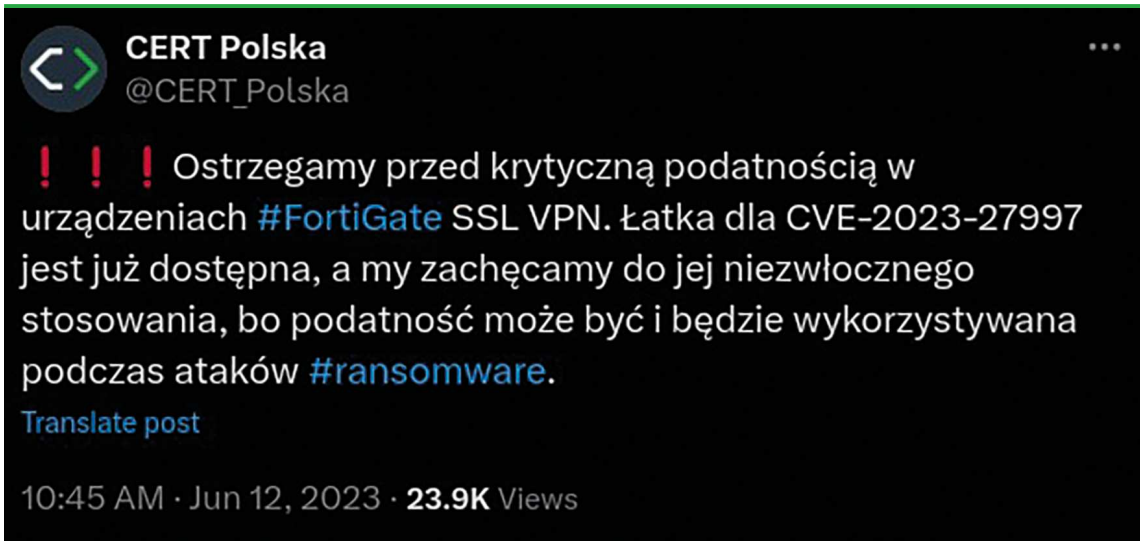


Rysunek 26: Ostrzeżenie przed podatnością CVE-2023-23397

Fortigate SSL-VPN (CVE-2023-27997)

Podatność w urządzeniach Fortigate z systemem FortiOS to luka związana z przepełnieniem bufora sterty w module wstępnego uwierzytelniania usługi SSL-VPN. J ej wykorzystanie pozwalało na przepełnienie nadmiaru danych z zaalokowanego bloku pamięci do sąsiednich bloków na stercie, tym samym umożliwiając wykonanie dowolnego złośliwego kodu, nawet w przypadku, kiedy włączone było uwierzytelnianie dwuskładnikowe. Choć podatność CVE-2023-27997 została opublikowana 12 czerwca, to już 14 czerwca publicznie dostępne były exploity pozwalające na jej wykorzystanie, co zwiększało ryzyko wzmożonych ataków ransomware.

Zespół CERT Polska wykrył 218 instancji usług SSL-VPN urządzeń Fortigate z systemem FortiOS w polskiej adresacji, które były podatne na CVE-2023-27997. W związku z tym wysłaliśmy 128 powiadomień do różnych organizacji (niektóre z nich posiadały po kilka instancji).

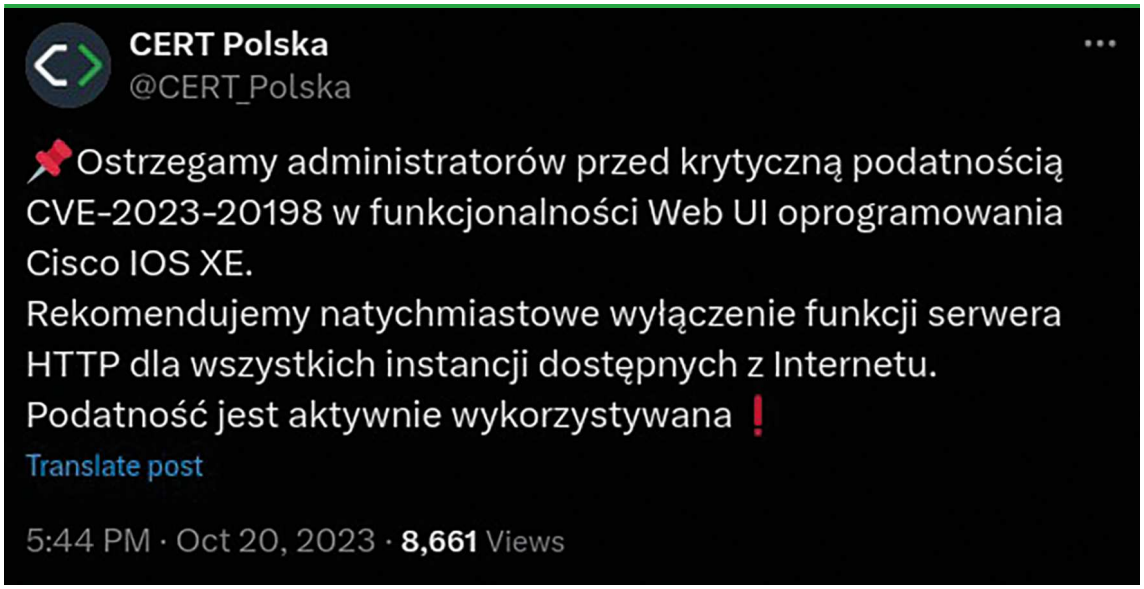


Rysunek 27: Ostrzeżenie przed podatnością CVE-2023-27997

Cisco IOS XE (CVE-2023-20198)

Krytyczna podatność dotyczyła funkcjonalności Web User Interface w oprogramowaniu Cisco IOS XE, która stosowana jest do zarządzania systemem, opartym na graficznym interfejsie użytkownika. Podatność była aktywnie wykorzystywana w atakach od 18 września 2023 roku. Atakujący miał możliwość utworzenia nowego konta administratora z poziomu interfejsu użytkownika, bez konieczności autoryzacji. Konto te w dalszych krokach służyło do utworzenia implantu zawierającego plik konfiguracyjny **cisco_service.conf**. Plik ten definiował nowy punkt końcowy serwera WWW, używany do interakcji z implantem. Aby implant stał się aktywny, serwer sieciowy musiał zostać ponownie uruchomiony. Sam punkt końcowy przyjmował określone parametry, które umożliwiały atakującemu wykonanie dowolnych poleceń na poziomie systemu.

Zespół CERT Polska znalazł 492 instancje Cisco IOS XE w polskiej adresacji, które były podatne na CVE-2023-20198. W związku z tym wysłaliśmy 106 powiadomień do różnych organizacji (niektóre z nich posiadały po kilka instancji).



Rysunek 28: Ostrzeżenie przed podatnością CVE-2023-20198

Zespół CERT Polska zaleca szczególnie administratorom sieci i kierownikom jednostek ciągłe śledzenie komunikatów bezpieczeństwa, które publikowane są przez producentów posiadanego oprogramowania oraz urządzeń, a także priorytetowe wykonywanie aktualizacji podatnych systemów w celu zapewnienia bezpieczeństwa organizacji. Ważnym również jest bezustanne monitorowanie infrastruktury pod względem występujących anomalii, które mogłyby świadczyć o tym, że jest ona przedmiotem ataku.

Ignorowanie zagrożeń związanych z krytycznymi podatnościami może skutkować incydentami bezpieczeństwa, takimi jak ataki ransomware lub wycieki danych wrażliwych.

Wycieki danych i strona bezpiecznedane.gov.pl

Od momentu, gdy internet stał się integralną częścią naszego życia, zyskaliśmy dostęp do niezliczonej ilości informacji i usług na wyciągnięcie ręki. Jednakże, wraz z tą wygodą, pojawia się również ryzyko, które często jest niedoceniane: wyciek danych. To zagrożenie może dotknąć każdego z nas, a jego skutki mogą być bardzo poważne. Nasze dane finansowe, medyczne, a nawet te najbardziej osobiste, mogą w jednej chwili trafić do cyberprzestępców i prowadzić do poważnych konsekwencji.

Wyciek z Morele po 6 latach

Pierwszym istotnym wydarzeniem związanym z wyciekiem danych w 2023 roku był wyrok Naczelnego Sądu Administracyjnego z dnia 9 lutego w sprawie wycieku z serwisu morele.net z 2018 roku. We wrześniu 2019 r. Prezes Urzędu Ochrony Danych Osobowych nałożył na sklep internetowy Morele.net karę 2,8 mln zł za nienależytą ochronę danych osobowych. Sklep złożył skargę kasacyjną do Naczelnego Sądu Administracyjnego, a wyrok zapadł 9 lutego 2023 r. NSA uznał, że skarga kasacyjna ma usprawiedliwione podstawy, choć nie we wszystkich kwestiach zgodził się z argumentacją spółki Morele.net. W ocenie NSA sam skutek, czyli włamanie i kradzież bazy z danymi klientów, nie jest dowodem na to, że administrator danych nie dochował odpowiednich standardów. NSA zwrócił też uwagę, że Wojewódzki Sąd Administracyjny (WSA) nie zlecił sporządzenia opinii biegłego, wbrew sugestiom ukaranego podmiotu.

Na początku 2024 roku Urząd Ochrony Danych Osobowych poinformował, że zakończył kolejne postępowanie administracyjne w sprawie wycieku i postanowił nałożyć na spółkę kolejną karę w wysokości 3.8 miliona złotych.

Wyciek danych z oprogramowania wykradającego dane

Pod koniec maja 2023 roku większość mainstreamowych mediów publikowała informacje na temat „największego wycieku danych polskich użytkowników w historii". W rzeczywistości sytuacja wyglądała inaczej, niż przedstawiały ją media, a sam wyciek znacząco różnił się chociażby od tego ze sklepu Morele. Zbiór danych pochodził najprawdopodobniej od operatorów kilku różnych programów typu data stealer. Dane te zostały następnie połączone w jedną listę. Zaobserwować to można to było m.in. po dużej ilości danych powiązanych z grami online, a co można połączyć z pobieraniem przez wielu graczy oprogramowania mającego pozwolić uzyskać niesprawiedliwą przewagę nad innymi. Tego typu programy są często trojanami, które zawierają moduły wykradania danych.

Opublikowane dane, w ilości około miliona unikalnych rekordów, nie były w żaden sposób ustrukturyzowane, a adresy e-mail wielokrotnie powtarzały się w kontekście tego samego serwisu. Wynikało to np. z podania kilkukrotnie hasła podczas procesu rejestracji, jeśli wprowadzone hasło nie spełniło minimalnych wymagań postawionych przez serwis. Sprawiało to, że dane te nie były gotowe do wykorzystania przez przestępców. Użycie ich wymagałoby wcześniejszego ich opracowania.

W trakcie analizy danych z wycieku i w ramach obsługi incydentu Zespół CERT Polska prowadził działania informacyjne m.in. za pomocą serwisu n6 oraz powiadomień mailowych do wielu instytucji, w szczególności administratorów rozpoznawalnych skrzynek pocztowych. Dodatkowo Centralny Ośrodek Informatyki uruchomił serwis bezpiecznedane.gov.pl, za pomocą którego można było sprawdzić, czy nasze dane pojawiły się w wycieku.

Rysunek 29: Strona bezpiecznedane.gov.pl

Wyciek danych medycznych z sieci laboratoriów ALAB

Serwis Bezpieczne Dane uruchomiony został w maju, ale jego największa wartość ujawniła się w grudniu przy okazji dużego wycieku danych medycznych. Przestępcy w listopadzie 2023 uzyskali nieuprawniony dostęp do infrastruktury informatycznej firmy ALAB Laboratoria, w tym do bazy, gdzie przechowywane były dane medyczne klientów. Najistotniejsze były tutaj dane osobowe, takie jak numery pesel czy adresy zamieszkania oraz wyniki przeprowadzonych badań. Wykradzione pliki opublikowane zostały w dwóch partiach w grudniu. Ujawnione dane zostały wgrane do serwisu bezpiecznedane.gov.pl, gdzie każdy zainteresowany mógł zalogować się za pomocą Profilu Zaufanego i na podstawie swojego numeru pesel sprawdzić, czy jego dane znajdowały się w wycieku.

Rysunek 30: Informacje o wycieku z ALAB Laboratoria opublikowane na stronie gov.pl

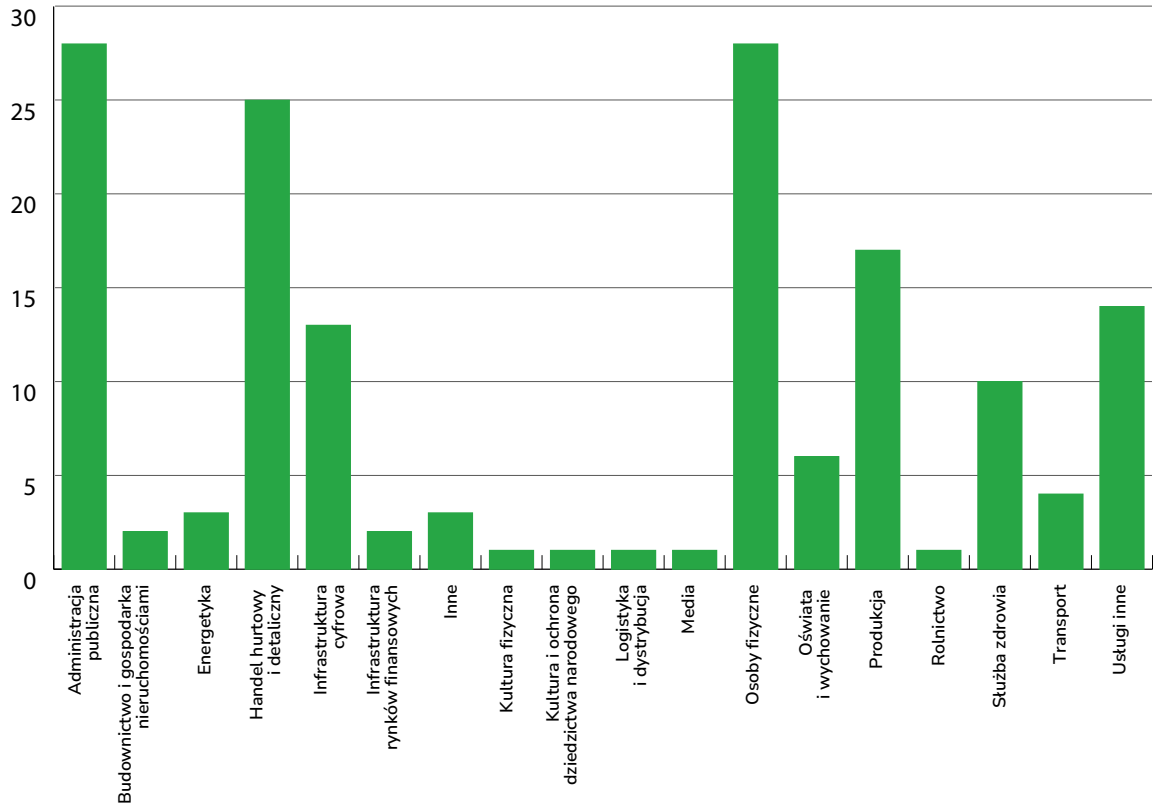
Zastrzeganie numeru PESEL

Od 17 listopada 2023 pojawiła się możliwość zastrzegania swojego numeru PESEL. Jest to działanie, które, w przypadku wycieku naszych danych osobistych czy nawet logowania do bankowości internetowej, mają uniemożliwić zaciągnięciu w naszym imieniu jakichkolwiek zobowiązań finansowych, bądź uzyskanie duplikatu karty SIM. PESEL można zastrzec w aplikacji mObywatel lub poprzez wizytę w banku, na poczcie czy w urzędzie gminy. Instytucje finansowe, takie jak banki, zostały zobowiązane do weryfikowania, czy podany numer PESEL nie jest zastrzeżony przy każdej próbie zaciągnięcia zobowiązania finansowego. Niestety obowiązek ten wejdzie w życie dopiero od 1 czerwca 2024. Za pomocą aplikacji mObywatel możliwe jest również sprawdzenie statusu naszego numeru PESEL oraz historii zapytań od różnych instytucji. Dzięki temu można sprawdzić, czy ktoś próbował wykorzystać nasze dane w sposób nieuprawniony.

Ransomware

Ransomware to szkodliwe oprogramowanie wykorzystywane do szyfrowania danych na zainfekowanych systemach w celu wymuszenia okupu za udostępnienie klucza pozwalającego na odzyskanie plików. Ataki z jego wykorzystaniem pozostają jednym z największych zagrożeń cyberbezpieczeństwa, które dotyczy zarówno dużych podmiotów jak i osób prywatnych. Jak wskazują doniesienia medialne[9], liczba organizacji dotkniętych atakami z wykorzystaniem ransomware rośnie z roku na rok.

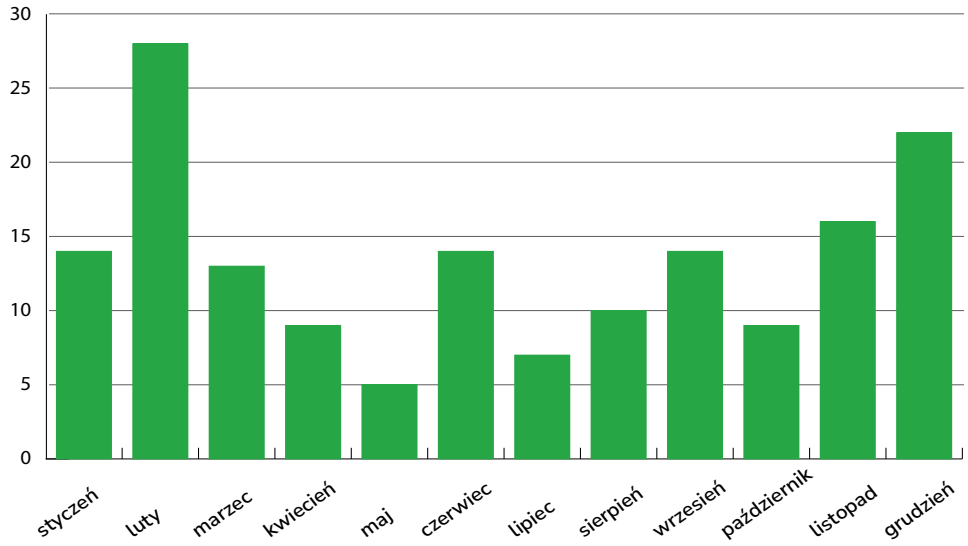
Trend ten był widoczny także w naszym kraju. W 2023 roku CERT Polska zarejestrował 161 incydentów związanych z atakami ransomware. Jest to niemal dwa razy więcej niż rok wcześniej, kiedy obsłużyliśmy 85 incydentów. Zdecydowana większość z nich została zgłoszona przez podmioty biznesowe (81), następnie administrację publiczną (31) i osoby prywatne (30).



Wykres 2: Liczba incydentów ransomware w podziale na sektory gospodarki

W tej statystyce nie może zabraknąć wskazania podziału zarejestrowanych incydentów zgodnie z kategoriami zawartymi w ustawie o Krajowym Systemie Cyberbezpieczeństwa (uKSC). Zarejestrowaliśmy 37 incydentów w podmiotach publicznych oraz dwa incydenty, które dotyczyły operatorów usług kluczowych i spełniły progi klasyfikujące je jako incydenty poważne.

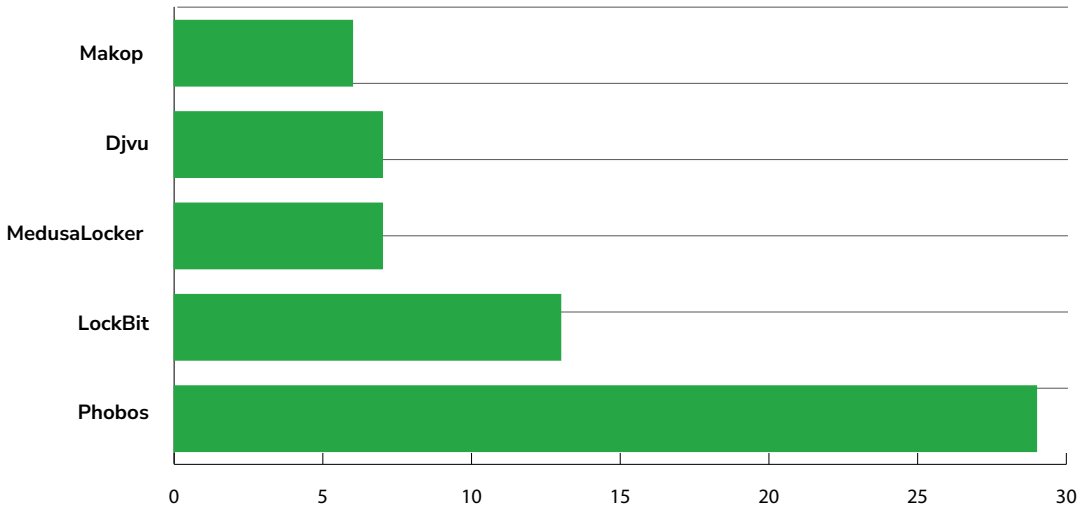
9 https://securityaffairs.com/157759/reports/ransomware-attacks-2023-report.html



Wykres 3: Liczba incydentów ransomware zarejestrowanych w poszczególnych miesiącach

Główne zagrożenia

W 2023 roku najczęściej zgłaszano nam incydenty związane z rodziną ransomware Phobos, która pojawiała się wyraźnie częściej niż inne. Zarejestrowaliśmy 29 incydentów z nią związanych. Drugą najczęściej pojawiającą się rodziną było szkodliwe oprogramowanie Lockbit (13 incydentów, w zdecydowanej większości w wersji Black tj. Lockbit 3.0). Wśród pozostałych najczęściej występujących rodzin znalazły się: MedusaLocker oraz Djvu (po 7 incydentów), a także Makop (6 incydentów). W 44 przypadkach nie udało się ustalić rodzaju szkodliwego oprogramowania odpowiedzialnego za incydent. Wynikało to na ogół z niewystarczających informacji przekazanych przez zgłaszający podmiot.



Wykres 4: Liczba incydentów zaobserwowanych w 2023 w podziale na rodziny ransomware

Rodziny zaobserwowane przez CERT Polska w 2023

Phobos

Ransomware Phobos został odnotowany po raz pierwszy w grudniu 2018 roku i od tamtej pory pozostaje aktywnym zagrożeniem. Liczba infekcji z jego użyciem utrzymuje się na stosunkowo wysokim poziomie. W kolejnych latach pojawiły się też liczne warianty tego oprogramowania, takie jak Eking czy Faust. Z uwagi na podobieństwo taktyk wykorzystywanych przez ich operatorów są one łączone z grupą odpowiedzialną za oryginalnego Phobosa. Co ciekawe, techniki wykorzystywane przez operatorów ransomware w celu uzyskania dostępu do infrastruktury organizacji pozostają niezmienione. Bazują oni najczęściej na wiadomościach phishingowych z załącznikami zawierającymi szkodliwe oprogramowanie lub niezabezpieczonych serwerach RDP (usługa zdalnego pulpitu), do których logują się przy użyciu przechwyconych poświadczeń lub poprzez skuteczny atak brute force. W 2023 ta rodzina ransomware atakowała zarówno podmioty publiczne jak i prywatne, w tym związane z sektorem zdrowia.

Lockbit

Tak samo jak w 2022 roku[10], w 2023 ransomware Lockbit pozostał najbardziej rozpowszechnionym zagrożeniem w swojej kategorii. W skali globalnej – operatorzy ransomware umieścili na swojej stronie internetowej informacje o ponad tysiącu ofiar swoich działań[11]. Grupa odpowiedzialna za rozwój tej rodziny szkodliwego oprogramowania udostępnia je stowarzyszonym grupom przestępczym lub samotnym operatorom w modelu Ransomware as a Service (RaaS), pobierając procent od okupu wyłudzonego od zaatakowanego podmiotu. Skutkuje to ogromnym zróżnicowaniem technik używanych podczas ataków. Zazwyczaj jednak ataki z wykorzystaniem oprogramowania Lockbit wykorzystują technikę double extortion – przestępcy przed zaszyfrowaniem transferują dane na kontrolowane przez siebie serwery. Na początku 2024 roku organy ścigania przejęły infrastrukturę grupy, dzięki czemu udało się przechwycić część kluczy deszyfrujących, co pozwoliło na stworzenie dekryptora (dostępnego na stronie www.nomoreransom.com).

MedusaLocker

Jest to kolejna rodzina ransomware operująca w modelu RaaS. Podobnie jak w przypadku Phobosa, operatorzy tego szkodliwego oprogramowania uzyskują dostęp do infrastruktury atakowanej organizacji poprzez usługę RDP, niezałataną podatność lub pozyskując dane uwierzytelniające w wyniku ataku brute force. Alternatywnym wektorem są wiadomości phishingowe zawierające w załączniku szkodliwe oprogramowanie. MedusaLocker także dokonuje eksfiltracji danych z zaatakowanej organizacji przed ich zaszyfrowaniem. Cechą charakterystyczną tej rodziny są liczne odmiany ransomware, różniące się zarówno pozostawianą notką jak i rozszerzeniem dopisywanym do nazwy zaszyfrowanych plików. W 2023 roku odnotowaliśmy incydenty związane tym ransomware głównie w małych i średnich przedsiębiorstwach, w jednym przypadku atak dotknął podmiotu z sektora medycznego.

Djvu

Infekcje ransomware Djvu są obserwowane od 2018 roku, kiedy to wkroczył on na scenę jako wariant szkodliwego oprogramowania STOP. Jego cechą charakterystyczną było korzystanie ze strategii

10 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

11 https://securityaffairs.com/157759/reports/ransomware-attacks-2023-report.html

klasycznych trojanów – pozorowanie nieszkodliwych plików multimedialnych lub podszywanie się pod znane aplikacje i sterowniki, w efekcie czego użytkownicy sami pobierali ransomware na swoje komputery. Djvu kontynuuje tę strategię – prawie wszystkie zarejestrowane przez nasz zespół w 2023 roku incydenty związane z tą rodziną szkodliwego oprogramowania pochodziły od osób prywatnych. Dodatkowo atakom ransomware Djvu często towarzyszą infekcje oprogramowaniem typu „stealer", które przed szyfrowaniem wykrada z hosta wrażliwe informacje (zwłaszcza dane dostępowe i klucze kryptograficzne).

Zaobserwowane Trendy

Wielokrotne wymuszenia

Większość obserwowanych przez nasz zespół ataków ransomware jest motywowanych finansowo – sprawcy liczą na to, że atak obejmie dane krytyczne dla działania danego podmiotu. W efekcie będzie on zmuszony do zapłacenia okupu, aby móc dalej normalnie funkcjonować. Dlatego w trakcie ataku operatorzy ransomware aktywnie poszukują i niszczą kopie zapasowe.

Trendem, który był już raportowany w poprzednich latach, jest rosnąca liczba incydentów, w których sprawcy przed rozpoczęciem procesu szyfrowania starają się wytransferować dane, do których mają dostęp. Zyskują w ten sposób dodatkowy środek nacisku na zaatakowany podmiot na wypadek, gdyby ten nie był zainteresowany płaceniem okupu, ponieważ odzyskał swoje dane z kopii zapasowej. Warto przy tym zwrócić uwagę na fakt, że pozostawiane przez atakujących notatki z żądaniem okupu niekiedy wprowadzają ofiary w błąd, informując o rzekomej kradzieży danych i grożąc ich opublikowaniem, podczas gdy atak obejmował jedynie szyfrowanie. Zazwyczaj w przypadku udanej eksfiltracji danych sprawcy zamieszczają na swojej stronie hostowanej w sieci TOR informację o włamaniu do danego podmiotu, próbkę wykradzionych plików oraz termin, w którym zostanie opublikowana całość, jeżeli nie otrzymają okupu (jest to wówczas tzw. double extortion). Z uwagi na stosunkowo niską przepływność sieci TOR, całość materiałów często jest też publikowana na stronach hostujących pliki dostępnych w internecie. W trakcie analiz incydentów zespół CERT Polska zaobserwował, że przestępcy starają się transferować przede wszystkim potencjalnie najbardziej wartościowe pliki, takie jak bazy danych i katalogi użytkowników, pomijając np. obrazy maszyn wirtualnych.

„Ciche" ataki

W przypadku ataku ransomware jednym z kluczowych wyzwań jest ustalenie wektora infekcji – w przeciwnym razie istnieje ryzyko, że po odtworzeniu infrastruktury atakujący ponownie rozpoczną proces szyfrowania. Z analiz incydentów przeprowadzonych przez CERT Polska wynika, że nierzadko włamywacze mają dostęp do sieci atakowanego podmiotu na długo przed rozpoczęciem procesu szyfrowania. W wielu przypadkach logi nie pozwalają na ustalenie dokładnej daty i sposobu uzyskania przez adwersarzy dostępu do infrastruktury, jednak pozwalają na odtworzenie przebiegu ich aktywności. Chociaż najczęściej obserwowane przez nas wektory pozostają takie same – niezabezpieczone serwery pulpitu zdalnego lub dostęp z wykorzystaniem przejętych danych autoryzacyjnych użytkownika – to coraz częściej obserwujemy incydenty, w których atakujący umieszczają szkodliwe oprogramowanie w sieci zaatakowanego podmiotu dopiero, gdy są już gotowi na rozpoczęcie procesu szyfrowania. Etap penetracji w głąb zaatakowanej sieci oraz eksfiltracja danych są natomiast realizowane z wykorzystaniem standardowych narzędzi wykorzystywanych przez administratorów (np. skrypty powershell, narzędzia z pakietu PsTools), przez co nie generują alertów oprogramowania antywirusowego i/lub EDR.

Poradnik dotyczący ransomware

W związku z tym, że, jak wspomnieliśmy na początku, ataki z użyciem ransomware są bardzo powszechne - dotykają organizacji publicznych, przedsiębiorstw, ale także osób prywatnych - zachęcamy do zapoznania się z przygotowanym przez nasz zespół poradnikiem dotyczącym ransomware. Opisujemy w nim działania, które można podjąć w celu przygotowania się na ten rodzaj zagrożenia, jak i czynności, które należy wykonać po stwierdzeniu infekcji. Poradnik dostępny jest na stronie CERT Polska: https://www.cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf

Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej

Przez ostatnie 2 lata pracownicy CERT Polska brali udział w pracach nad projektem legislacji dotyczącej rozwiązań przeciwdziałających cyberzagrożeniom. W zespole roboczym znaleźli się również przedstawiciele Ministerstwa Cyfryzacji, Urzędu Komunikacji Elektronicznej oraz przedsiębiorców telekomunikacyjnych. Owocem tych działań jest ustawa z 28 lipca 2023 roku (Dz. U. poz. 1703) o zwalczaniu nadużyć w komunikacji elektronicznej[12]. Prace zespołu skupiały się na realnych rozwiązaniach, które mają szanse zostać wprowadzone w życie i odnieść oczekiwany skutek. Ostatecznie regulacja zajmuje się walką z phishingiem, smishingiem, spoofingiem e-mail oraz telefonicznym. Ustawa weszła w życie 24 września 2023 roku, ale nie wszystkie regulacje zaczęły obowiązywać już w tym terminie.

Phishing

Do walki z phishingiem zostało wykorzystane sprawdzone autorskie rozwiązanie CERT Polska, czyli Lista ostrzeżeń. To dojrzały projekt funkcjonujący od 2020 roku, który powstał dzięki porozumieniu zawartemu pomiędzy Ministerstwem Cyfryzacji, Orange Polska, Polkomtelem, P4 i T-Mobile Polska. Wymienienie listy w ustawie sprawia, że także pozostali przedsiębiorcy telekomunikacyjni mogą być chronieni przed skutkami blokowania połączeń ze złośliwymi domenami. Wszelkie skargi, czy to pochodzące od użytkowników, czy właścicieli blokowanych domen rozpatrywane są bez udziału dostawców usług telekomunikacyjnych. Warunkiem uzyskania takiego prawa jest dołączenie do porozumienia[13]. Usankcjonowanie naszego projektu sprawia, że właściciele domen również są chronieni przed nieuprawnionym blokowaniem ruchu do ich serwisu. Od decyzji o wpisanie domeny na Listę ostrzeżeń można odwołać się do Prezesa Urzędu Komunikacji Elektronicznej.

12 https://www.gov.pl/web/baza-wiedzy/porozumienie-w-sprawie-listy-ostrzezen

13 https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20230001703/O/D20231703.pdf

Smishing

Za smishing uznano każdą wiadomość, która ma na celu nakłonienie odbiorcy do konkretnego działania m.in. niekorzystnego rozporządzenia mieniem czy udostępnienia danych osobowych. W ramach walki z tym zagrożeniem powstało unikalne rozwiązanie. CERT Polska tworzy wzorce wiadomości smishingowych, a przedsiębiorcy telekomunikacyjni obowiązani są blokować wszystkie wiadomości, które wpisują się w jakikolwiek z otrzymanych wzorców. Same wzorce są oparte o wyrażenia regularne, a system działa od 16 kwietnia 2024 r. Ze względu na transparentność procesu ustalono, że każdy wzorzec musi być upubliczniony w terminie od 14 do 21 dni od wprowadzenia go do systemu.

Do tworzenia wzorców wiadomości potrzebne jest monitorowanie zjawiska smishingu. Robimy to od kwietnia 2021 roku, ale żeby zwiększyć ilość otrzymywanych danych, otrzymaliśmy prawo do darmowego numeru 8080.

Dodatkowym rozwiązaniem jest ochrona nadpisów wiadomości SMS (wyświetlana nazwa nadawcy) należących do podmiotów publicznych. Będziemy prowadzić rejestr nadpisów wykorzystywanych przez podmioty publiczne. Te z kolei będą mogły wysyłać SMS-y tylko ze zgłoszonym do nas nadpisem. Celem regulacji jest, aby obywatel otrzymując SMS-a o treści sugerującej związek ze sprawą administracyjną mógł sprawdzić w naszym wykazie, czy na pewno podchodzi on od zaufanego podmiotu.

Spoofing e-mail

Do walki ze spoofingiem e-mail, ale też pozostałym spamem, wykorzystano znane i sprawdzone rozwiązania. Podmioty publiczne mają obowiązek korzystania z mechanizmów SPF, DMARC oraz DKIM. Wszystkie razem znacznie ułatwiają, wykrywanie spoofingu w mailach przychodzących, jak i uniemożliwiają podszycie się pod konkretną firmę. Regulacja ta dotyczy na razie tylko sektora publicznego. Opisane mechanizmy stanowią zaś system naczyń połączonych, który

działa w pełni, gdy obie strony komunikacji z niego korzystają. Aby sprawnie funkcjonował, należy zachęcić do korzystania z tych rozwiązań także podmioty prywatne. Z tego powodu stworzyliśmy narzędzie https://bezpiecznapoczta.cert.pl/, któremu poświęciliśmy osobny rozdział.

Drugim aspektem jest ograniczenie możliwości przejęcie skrzynek pocztowych pracowników sektora publicznego. W związku z tym na dostawcę poczty dla podmiotu publicznego został nałożony obowiązek wprowadzenia do oferty możliwości skonfigurowania uwierzytelnienia wieloskładnikowego. Przymus ten wszedł w życie 24 marca 2024.

Oba obowiązki dotyczą również dostawców poczty, którzy posiadają co najmniej 500 tys. użytkowników.

CLI spoofing

W ramach walki ze spoofingiem telefonicznym powstaje rozwiązanie, które ma na celu blokowanie połączenia, a przynajmniej usuwanie zmodyfikowanej etykiety dzwoniącego, w przypadku wykrycia takiego oszustwa. Pełnoprawna walka z tym zjawiskiem ma się zacząć najpóźniej do 24 września 2024 roku. Natomiast już od 24 marca 2024 roku funkcjonuje lista numerów, z których nie można wykonywać połączeń. Lista DNO (ang. Do Not Originate) zawiera zgłoszone numery, z których właściciel nie zamierza wykonywać połączeń. Do takiej kategorii należą m.in. numery infolinii. W momencie otrzymania połączenia z takiego numeru operator telefoniczny będzie wiedział, że należy zablokować połączenie.

Sukces?

Wszystkie powyższe rozwiązania mają potencjał i szanse, by okazać się skutecznymi. Ich wspólnym mianownikiem jest zmniejszenie częstotliwości występowania zwalczanych zagrożeń, poprzez zwiększenie kosztu (czasowego, pieniężnego) ich wytworzenia.

Działania CERT Polska

Lista Ostrzeżeń

Rok 2023 to kolejny rok funkcjonowania Listy Ostrzeżeń. Był on szczególny z kilku względów.

W trzecim kwartale 2023 roku w życie weszły zapisy ustawy o zwalczaniu nadużyć w komunikacji elektronicznej, dzięki którym Lista znalazła umocowanie prawne. Została również wskazana formalna ścieżka odwołania od decyzji o umieszczeniu domeny na Liście.

Drugie znaczące wydarzenie to uruchomienie łatwiejszego do zapamiętania numeru 8080, obok działającego do tej pory 799 448 084. Na oba numery można przekazywać podejrzane wiadomości SMS zawierające linki, w celu ich weryfikacji przez nasz zespół. Jeśli odnośnik prowadzi do szkodliwej strony, zostanie ona dodana na Listę Ostrzeżeń.

Kolejną nowością jest druga wersja formatu Listy. O zmianach, które wprowadza można przeczytać na naszej stronie[14]. Zachęcamy do zmiany używanej wersji na wersję drugą!

Niezmiennie zachęcamy też do zgłaszania zagrożeń za pomocą formularza dostępnego na stronie https://incydent.cert.pl/ oraz przekazywania podejrzanych wiadomości SMS, tym razem już na numer 8080. Cieszy nas rosnąca świadomość społeczna dotycząca istnienia takiej możliwości. Na koniec pragniemy podziękować wszystkim Zgłaszającym, dzięki którym nasz zespół może skuteczniej chronić innych użytkowników.

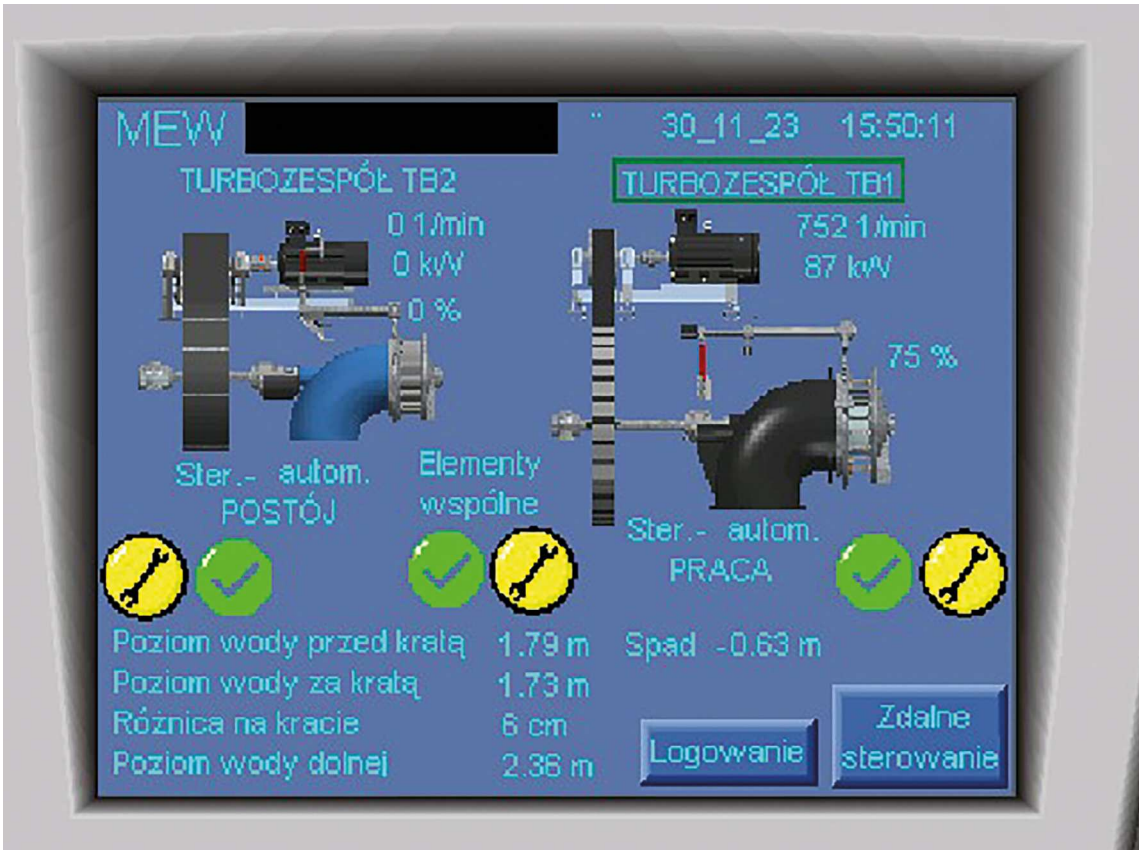
14 https://cert.pl/lista-ostrzezen

#BezpiecznyPrzemysł

W 2023 roku kontynuowaliśmy akcję #BezpiecznyPrzemysł, w ramach której aktywnie działamy na rzecz podniesienia poziomu cyberbezpieczeństwa polskiej infrastruktury przemysłowej. Skupiamy się na poszukiwaniu urządzeń przemysłowych dostępnych z publicznego internetu, takich jak sterowniki PLC czy panele operatorskie (HMI) oraz informowaniu właścicieli o zagrożeniu związanym z ich błędną konfiguracją. W 2022 r. stworzyliśmy do tego celu autorski system Snitch (więcej o nim w dalszej części raportu), który automatyzuje dużą część naszej pracy. W 2023 r. mocno rozbudowaliśmy to narzędzie.

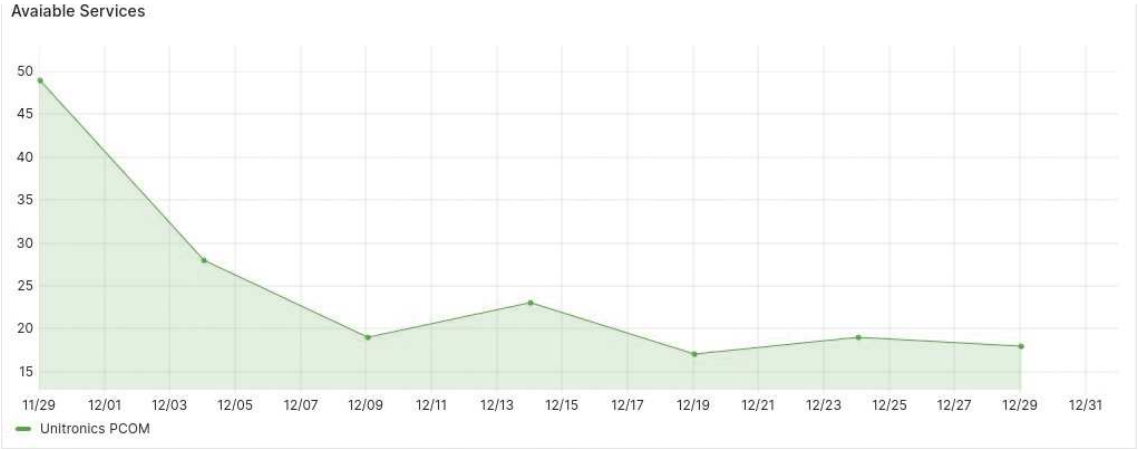
W ciągu 2023 roku podjęliśmy działania względem licznych przypadków, w których można było zdalnie przejąć całkowitą kontrolę nad procesem przemysłowym. Za każdym razem kontaktowaliśmy się i współpracowaliśmy z właścicielami celem rozwiązania problemu.

Przykładowo, w listopadzie 2023 r. CISA opublikowała informację o ataku na stację uzdatniania wody w USA z wykorzystaniem sterownika Unitronics dostępnego z internetu[15]. Po uzyskaniu informacji o zagrożeniu wykorzystaliśmy system Snitch, aby znaleźć podobne przypadki w Polsce. Udało nam się odszukać i powiadomić właścicieli 43 urządzeń skonfigurowanych w sposób umożliwiający potencjalny atak. Jednym z takich urządzeń był sterownik z wbudowanym panelem HMI zarządzający małą elektrownią wodną (rys. 31), możliwe było jego zdalne przeprogramowanie. W ciągu miesiąca udało nam się zmniejszyć liczbę dostępnych z internetu sterowników do 18 (wyk. 5).



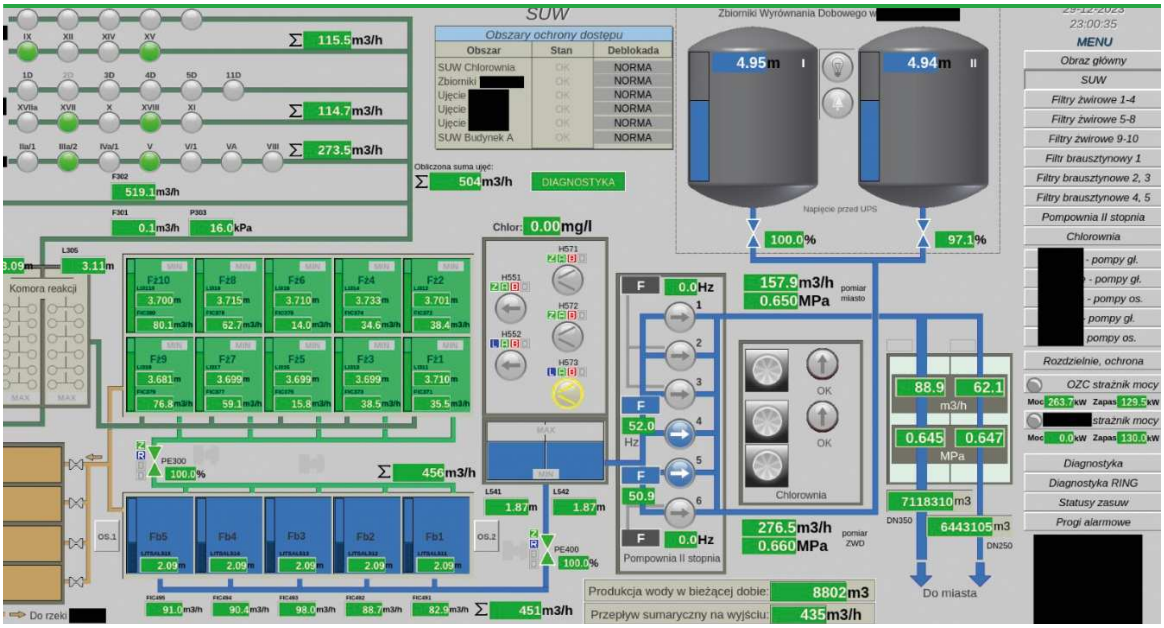
Rysunek 31: Panel HMI małej elektrowni wodnej

15 https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems



Wykres 5: Widoczność sterowników Unitronics

Jednym z najpoważniejszych zdarzeń znalezionych przy pomocy Snitcha w 2023 r. był dostępny z internetu panel systemu SCADA oczyszczalni ścieków, sieci kanalizacyjnej i stacji uzdatniania wody w dużym mieście powyżej 50 tys. mieszkańców. Za jego pomocą można było nie tylko odczytywać stan parametrów, ale również zmieniać nastawy dozowania podchlorynu sodu (rys 32), co mogłoby prowadzić do poważnych konsekwencji.



Rysunek 32: Stacja uzdatniania wody dużego miasta dostępna z internetu

Zgłoszenia SMS

W maju 2021 roku uruchomiliśmy usługę przyjmowania zgłoszeń wiadomości SMS zawierających adres URL (tzw. link). Pozwala ona na szybkie i łatwe przesłanie nam wiadomości, która wzbudza podejrzenia. Każda wiadomość poddawana jest krótkiej analizie wstępnej, polegającej na sprawdzeniu znajdującego się w niej linku. Jeśli strona, do której prowadzi link, jest nam już znana jako szkodliwa, zgłaszający otrzymuje stosowną informację. W przeciwnym wypadku wysyłamy podziękowanie za przekazanie nam potencjalnie szkodliwej wiadomości.

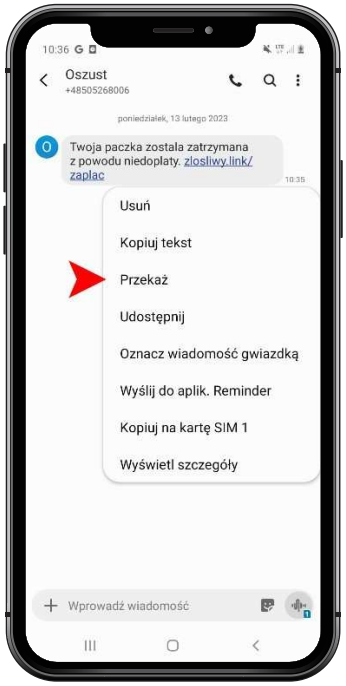
Ustawa o zwalczaniu nadużyć

Wprowadzenie w 2023 roku ustawy o zwalczaniu nadużyć w komunikacji elektronicznej spowodowało zmianę w naszym podejściu. Od początku grudnia przyjmujemy również zgłoszenia, które nie zawierają linku. Wiąże się to z faktem, że definicja ustawowa nie łączy smishingu z obecnością linku w wiadomości. Musimy więc dopuszczać możliwość istnienia kampanii SMS-owych bez adresu URL, które mimo to należałoby zablokować. Więcej o samym procesie blokowania można przeczytać w innym rozdziale.

Drugą kluczową zmianą wprowadzoną przez ustawę jest zagwarantowanie bezpłatnego wysyłania zgłoszeń SMS na łatwy do zapamiętania numer **8080**.

Jak zgłosić SMS?

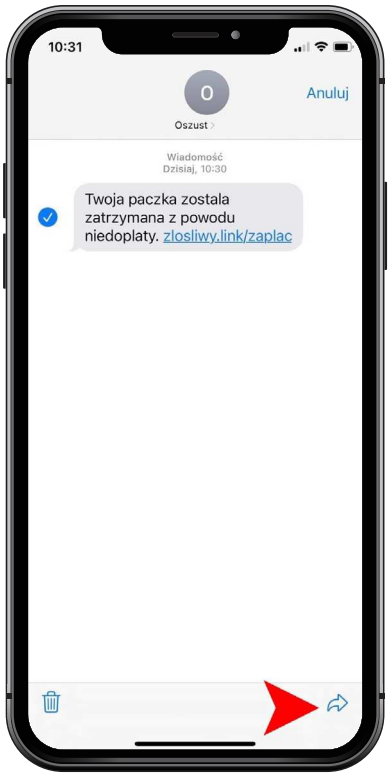
Zgłoszenie wiadomości SMS jest bardzo proste, choć może się nieco różnić zależnie od posiadanego urządzenia. Dla telefonów z systemem Android przesyłanie zgłoszenia może się dodatkowo minimalnie różnić wizualnie, ze względu na nakładkę producenta lub konkretną wersję aplikacji do obsługi SMS, ale wszystkie funkcje nazywają się tak samo. Wystarczy przytrzymać zgłaszaną wiadomość, a następnie w rozwijanym menu wybrać opcję Przekaż (rys. 33). W kolejnym kroku należy wpisać numer 8080 (lub wybrać go z listy zapisanych kontaktów) i wysłać wiadomość.



Rysunek 33:
Przekazywanie wiadomości z urządzenia z systemem Android. Strzałką oznaczono opcję Przekaż

Dla użytkowników iPhone ten proces różni się tylko nieznacznie. Po przytrzymaniu wiadomości należy wybrać opcję Więcej... (rys. 34), a w kolejnym kroku wcisnąć strzałkę w prawym dolnym rogu (rys. 35).

Rysunek 34:
Przekazywanie wiadomości z iPhone – pierwszy krok. Strzałką oznaczono opcję Więcej...



Rysunek 35:
Przekazywanie wiadomości z iPhone – drugi krok. Strzałką oznaczono guzik przesłania dalej

Statystyki zgłoszeń SMS

W 2023 roku zanotowaliśmy podobną liczbę zgłoszeń (221 880) wiadomości co rok wcześniej (217 685). Warty uwagi jest fakt, że ponad 1/3 zgłoszeń (84 880) została zanotowana w grudniu, po ogłoszeniu bezpłatnego numeru **8080**. 2023 rok był lepszy pod względem jakości zgłoszeń. Aż 119 752 z nich było powiązanych z próbami wyłudzenia (wzrost o ok. 37 tys. r/r). W konsekwencji na Listę ostrzeżeń wpisano **8346** domen. Czy podobna liczba zgłoszeń co w 2022 r. oznacza, że osiągnęliśmy maksymalną rozpoznawalność i powyższe statystyki (zwłaszcza liczba wykorzystywanych domen) realnie obrazują sytuację smishingu w Polsce? Trudno ocenić. Natomiast na przestrzeni ostatnich lat zauważamy, że okres od Black Friday do Nowego Roku dostarcza najwięcej zgłoszeń w ciągu roku. Sugeruje to, że wszelkie scenariusze związane z dostawami kurierskimi są nadal bardzo skuteczne.

Edukacja i promocja - czyli czy nr 8080 podniósł świadomość Polaków w obszarze cyberbezpieczeństwa?

Ostatnie miesiące 2023 roku przyniosły duże zmiany w liczbie przyjętych przez CERT Polska zgłoszeń. Przyczyny tego zjawiska omawiamy w tym Raporcie w wielu miejscach, tu spojrzymy na to zagadnienie także w kontekście działań promocyjnych i edukacyjnych, które realizowaliśmy.

Do listopada zeszłego roku średnia miesięczna liczba zgłoszeń przetwarzanych przez zespół CERT Polska wynosiła ok. 30 tys. Koniec roku zmienił tę dynamikę. Listopad to blisko 42 tys. zgłoszeń, grudzień – ponad 100 tys.! Dało to na koniec roku niemal 400 tys. zgłoszeń. To rekord, ale taki, który długo się nie utrzyma, ponieważ styczeń 2024 pokazał, że tendencja jest zdecydowanie wzrostowa. Co zatem działo się w polskiej cyberprzestrzeni w ostatnich miesiącach? I jak zdarzenia te wpłynęły na nastawienie Polaków do wysyłania zgłoszeń?

Poszukujący jednoznacznej odpowiedzi na powyższe pytania mogą poczuć się rozczarowani. Uważamy, że na taką sytuację złożyło się wiele elementów. W tym rozdziale chcemy się im przyjrzeć.

Aktywność cyberprzestępców się zwiększa – to fakt, który potwierdzają opisywane w tym raporcie kampanie phishingowe i dane statystyczne. Koniec roku to czas wzmożonej aktywności przestępców, ale jednocześnie Polacy coraz umiejętniej rozpoznają zagrożenia i coraz chętniej je do nas zgłaszają.

Dzieje się tak również dlatego, że rozpoznawalność CERT Polska rośnie, na co wpływ mają bez wątpienia kampanie edukacyjne i promocyjne. 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 2022 roku. Pod koniec roku 2023 wznowiliśmy kampanię, wzbogacając ją o informację o nowym, bezpłatnym numerze 8080, na który można w prosty sposób przesłać podejrzaną wiadomość.

Rysunek 36: Fragment spotu z numerem 8080

Od połowy czerwca do połowy grudnia trwała także inna ogólnopolska kampanii edukacyjno-informacyjna. Jej celem było podniesienie świadomości Polaków na temat zagrożeń ze strony cyberprzestępców. Kampania organizowana przez Ministerstwo Cyfryzacji oraz NASK-PIB i CERT Polska, była współfinansowana ze środków Unii Europejskiej. Realizowaliśmy ją m.in. w internecie, telewizji, radiu i prasie. Miała ona formę 5-odcinkowego serialu. W każdym spocie przedstawione zostało jedno cyberzagrożenie i kilka praktycznych wskazówek dla osób, których może dotknąć podobna sytuacja.

Rysunek 37: Spot telewizyjny dot. bezpiecznych zakupów

Aby ułatwić dotarcie do zagadnień poruszanych w spotach, na stronie internetowej CERT Polska utworzyliśmy specjalne zakładki. Każda z nich zawierała informacje i rady związane z tematyką emitowanych odcinków.

Kraków

1941
w tym roku wyprodukowano wagon typu K, który już w niedzielę, 16 lipca, będzie kursował na Krakowskiej Linii Muzealnej

UTRUDNIENIA
Jak poinformował wykonawca Trasy Wolbromskiej (zachodniej obwodnicy Zielonek), od 19 lipca, od godz. 6 zajęty na potrzeby robót budowlanych zostanie fragment jednego z pasów ruchu na ulicy Glogera (przy granicy z gminą Zielonki). Na tym odcinku zostanie wprowadzony ruch wahadłowy. Nowa droga będzie się łączyć z północną obwodnicą Krakowa, realizowaną obecnie przez Generalną Dyrekcję Dróg Krajowych i Autostrad.

KRAKÓW
TELEFON
dziennikarza dyżurnego
697 730 318
E-MAIL
redakcja@gk.pl

Musimy podzielić się miastem z dzikimi zwierzętami

Aleksandra Łabędź

Centrum Krakowa, place zabaw, blokowiska czy też miejskie parki - właśnie w tych miejscach coraz częściej pojawiają się dzikie zwierzęta.

Począwszy od gryzoni, po dzikie ptaki, mniejsze ssaki, czy też pokaźnych rozmiarów dziki, a nawet łosie. Nowe pokolenia dzików czy saren wcale nie migrują do miasta, ale rodzą się w nim. Coraz częściej dzikie tereny są im obce, a miejskie warunki to jedyne, które znają. - To nie dzikie zwierzęta mają problem z nami, ale my z nimi. To my musimy się nauczyć gospodarować przestrzenią miejską i współżyć z tymi zwierzętami - wyjaśnia dr hab. inż. Marek Wajdzik, prof. URK.

- Obecnie na terenie Krakowa mamy przynajmniej 30 stanowisk, gdzie żyje ok. 4-5 bobrów - dodaje Marek Wajdzik, prof. URK.

Z korytarzy ekologicznych korzystają także większe zwierzęta, m.in. dziki, sarny, łosie a także średniej wielkości ssaki: lisy, jenoty czy borsuki. W Krakowie pojawił się też szop pracz.

- Obecnie miasta mają formę „rozlaną" powstałą w wyniku włączenia terenów zabudowanych wraz z polami i lasami, w których zwierzęta już występowały. Z drugiej strony osoby, które zamieszkują miasta, widząc te zwierzęta zimą, spieszą, by je czymś nakarmić. Tak sami doprowadzamy do tego, że zwierzęta widząc, że o pokarm nie trzeba walczyć, same zbliżają się do osiedli, na których mieszkamy. Później to generuje liczne problemy - dodaje prof. Wajdzik.

Dziki na razie opanowują peryferia miasta, ale jak można przypuszczać, niebawem wybiorą się do centrum

Jednym z przykładów, gdzie widok dzika już nikogo nie dziwi, to osiedle Podwawelskie. Wystawienie tam śmieci powoduje, że zaraz pojawia się wataha dzików, która do tych koszy się dobiera.

- W miastach łatwiej się dzikim zwierzętom żyje. Oczywiście jest część gatunków, które nie zaaklimatyzowały się w bliskości człowieka i te najczęściej w dzisiejszych czasach giną - kuraki leśne, czyli głuszec i cietrzew. Jednak są również gatunki, które świetnie się w miastach czują. Jeszcze przed 50 laty nam się nie śniło, że w miastach będą mieszkały dziki, że w Tyńcu będą odbywały się jelenie gody (tzw. rykowisko) - mówi prof. URK.

Należy podkreślić, że dzikie zwierzęta niekoniecznie muszą migrować, ale po prostu rodzą się już w Krakowie i doskonale potrafią tutaj żyć.

- Powinniśmy się nauczyć z tymi zwierzętami żyć. Jednak moim zdaniem część gatunków musi podlegać użytkowaniu choćby myśliwskiemu, ponieważ gdyby nie one - doprowadziłbyśmy do takiej skrajnej sytuacji, że np. dziki byłyby na Plantach, na ul. Floriańskiej czy krakowskim Rynku Głównym - dodaje prof. Wajdzik.

Jak podkreśla ekspert z URK miasto powinno się rozbudować w taki sposób, by zapewnić dzikim zwierzętom swobodne przemieszczanie się za pośrednictwem zielonych enklaw. Konieczne jest również, by miasto miało „zielone służby", które będą się zajmować zarządzaniem populacjami zwierząt.

Wbrew coraz bardziej powszechnemu obyciu się mieszkańców miasta z dzikimi zwierzętami i odwrotnie, cały czas chociaż niewielkie, istnieje ryzyko ataków bezpośrednich.

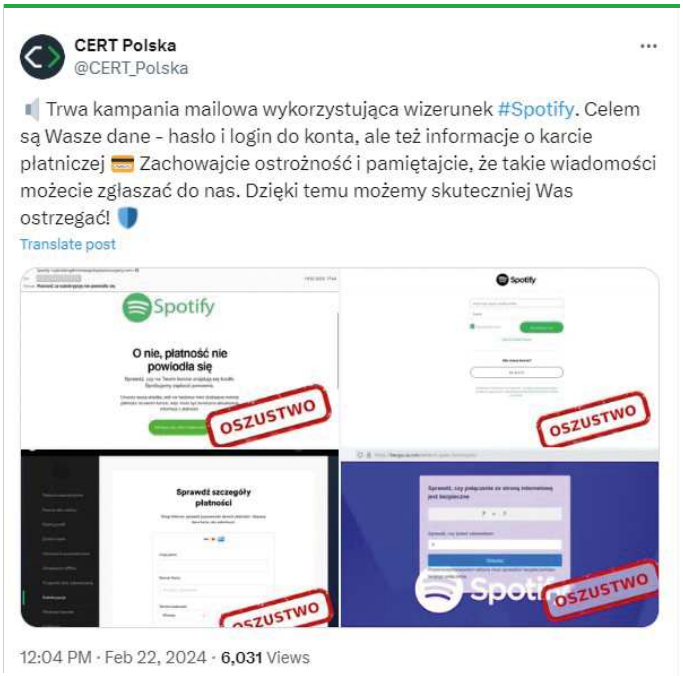
- Przestańmy się podpierać informacjami z horrorów! Tylko osób w skali roku ginie w wyniku ataków rekinów. Najwięcej osób zabijają... hipopotamy! To liczba ok. 2,7 tys. osób rocznie.

Na razie inwazja hipopotamów nam nie grozi.

Rysunek 38: Materiał prasowy przygotowany podczas kampanii edukacyjnej

Oprócz tego prowadziliśmy działania edukacyjne w social mediach, które wspieraliśmy obecnością naszych ekspertów w wiodących stacjach radiowych i telewizyjnych, a także w prasie.

Na szczególną uwagę zasługują systematycznie wydawane ostrzeżenia. Dotyczą one największych kampanii oszustów i są publikowane równolegle na profilach CERT Polska na Facebooku, X (dawniej Twitter) oraz LinkedInie. Regularność publikacji, aktualne kwestie i ważne społecznie zagadnienia powodują, że posty przygotowane przez ekspertów CERT Polska docierają nawet do kilkuset tysięcy odbiorców.



Rysunek 39: Przykład ostrzeżenia opublikowanego na portalu X

Oprócz ostrzeżeń, wydawanych w miarę konieczności, w kanałach social media publikowane są także stałe cykle edukacyjne – w okresie letnim była to seria #CyberParawan, w której przypominaliśmy o popularnych zagrożeniach oraz sposobach radzenia sobie z nimi.

Rysunek 40: Przykład postu w serii #CyberParawan

W grudniu był to natomiast zestaw animacji „CyberBombka" dotyczący kluczowych mitów z obszaru cyberbezpieczeństwa, takich jak: publiczne sieci WiFi czy popularna zielona kłódka. Cykl zakończył się dłuższym podsumowaniem zamieszczonym na stronie internetowej naszego zespołu.

Rysunek 41: Przykładowy post w ramach cyklu #CyberBOMBKA

Wymienione powyżej działania edukacyjne 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.

W ten sposób budowaliśmy świadomość, ale też zaufanie. Nasza rosnąca rozpoznawalność, nowy łatwy do zapamiętania numer i przekonanie, że CERT Polska to zespół ekspertów w obszarze zagrożeń, przełożyły się na liczbę zgłoszeń. A większa pula zgłoszeń to pełniejszy obraz tego, co dzieje się w polskiej cyberprzestrzeni. Na razie daje to możliwość skuteczniejszego działania i ostrzegania, ale już wkrótce – dzięki rozwiązaniom przewidzianym w ustawie o zwalczaniu nadużyć w komunikacji elektronicznej, dostaniemy do rąk dużo skuteczniejsze narzędzie. UZNKE daje możliwość blokowania phishingu zanim dotrze do użytkownika końcowego. Dlatego rosnąca liczba zgłoszeń jest dla nas nie tylko źródłem satysfakcji, ale także daje nam narzędzia – pozwalające nam lepiej rozumieć cyberkrajobraz i działać jeszcze efektywniej. A to jest w interesie wszystkich użytkowników internetu w Polsce.

Dwudziesta szósta edycja Secure

„Bezpieczeństwo w dobie zmian" to hasło przewodne konferencji Secure w 2023 r. To wiodące wydarzenie z obszaru cyberbezpieczeństwa zgromadziło w Warszawie ponad 300 uczestników, którzy dyskutowali m.in. o konieczności wspólnego działania w obliczu cyberzagrożeń.

Cyberbezpieczeństwo to nie jest opcja, tylko must have dla każdej firmy i organizacji – mówił podczas pierwszego panelu dotyczącego europejskiego krajobrazu cyberbezpieczeństwa minister cyfryzacji Janusz Cieszyński. Debatę moderował Krzysztof Silicki, a udział w niej wzięli także Uroš Svete oraz Juhan Lepassaar – dyrektor zarządzający Europejskiej Agencji Cyberbezpieczeństwa, który zauważył, że – bardziej widoczne od czasu inwazji na Ukrainę działania haktywistów, nie powinny przesłaniać rosnącego poziomu mniej zgłaszanych i mniej widocznych, ale wciąż pozostających poważnym zagrożeniem, ataków ransomware i cyberszpiegostwa w UE

Rysunek 42: Zdjęcie z dyskusji panelowej podczas inauguracji Secure

Debata o europejskim wymiarze cyberbezpieczeństwa stanowiła wprowadzenie do tego, co działo się później. Uzupełnieniem do perspektywy międzynarodowej było spojrzenie na grunt polski, a wyjściem do dalszej dyskusji wystąpienie kierownika zespołu CERT Polska Sebastiana Kondraszuka, w którym podsumował obserwacje z roku 2022. Kondraszuk zauważył, że liczba zgłoszeń odebranych przez CERT Polska wzrosła o 178%. – **To efekt rozwoju świadomości, ale i postępujących ułatwień dotyczących metod zgłaszania takich zjawisk** – mówił. Przedstawił też najpowszechniejsze zagrożenia i wyzwania, które następnie rozwijane były w ramach dwóch ścieżek tematycznych.

Blisko 50 prelegentów omawiało w kolejnych godzinach projekty, wyzwania i zmiany w prawie związane z cyberbezpieczeństwem. Krzysztof Zając z zespołu CERT Polska przybliżał efekty

skanowania polskiego internetu narzędziem Artemis i mówił o najczęściej znajdowanych podatnościach. Paweł Piekutowski z KNF opowiadał o skutkach ataków typu DDoS zaznaczając, że - nie jest dziś pytaniem czy będziemy mieli do czynienia z atakiem DDoS ale kiedy do niego dojdzie. Bartosz Trybus – także z zespołu CERT Polska – brał natomiast udział w dyskusji o skutkach ataków ransomware.

> **Wydarzeniem towarzyszącym Secure były odbywające się 18 kwietnia warsztaty. Ponad 100 uczestników z podmiotów, które zgodnie z KSC, leżą w zakresie zainteresowania CSIRT NASK szkoliło się m.in. z zapobiegania atakom DNS czy systemu S46. Mówiliśmy też o narzędziu N6, które jest szczególnie rekomendowane przez zespół CERT Polska. – Zachęcamy do dzielenia się wiedzą i do korzystania z doświadczeń innych – mówił o projekcie prowadzący szkolenie Krzysztof Rydz. Kolejna edycja konferencji odbędzie się w kwietniu 2024 r.**

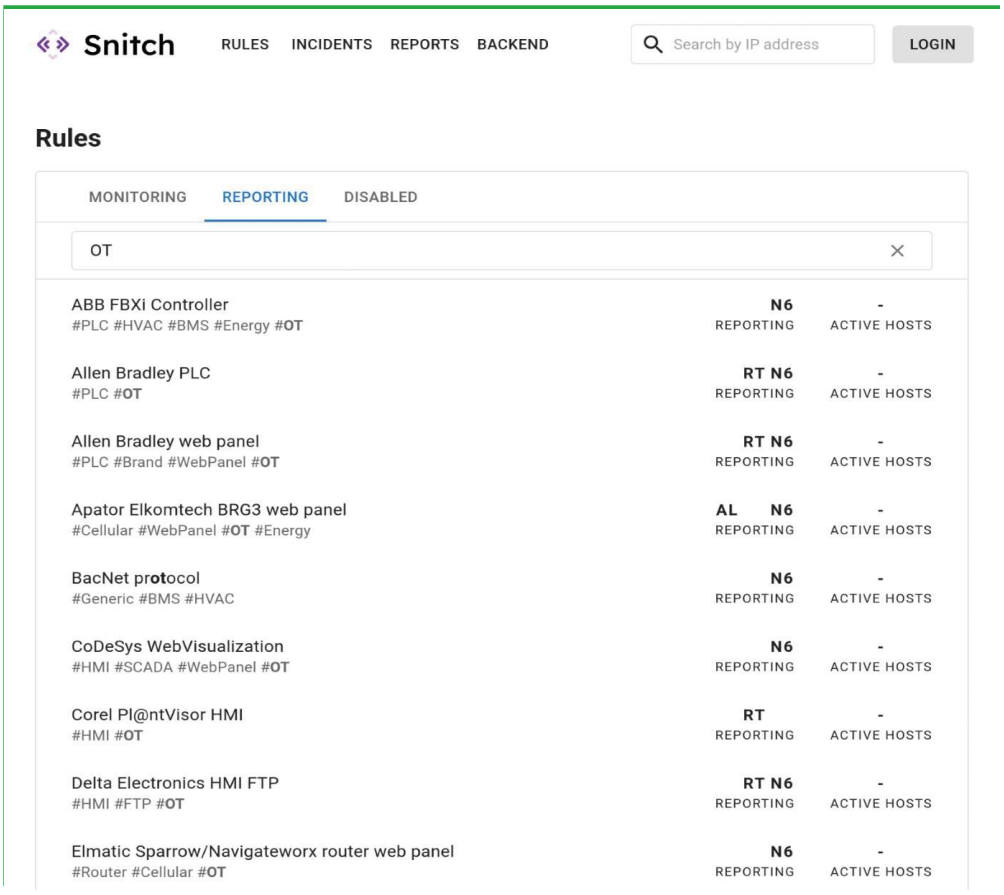
Projekty R&D

Snitch

Rysunek 43: Logo Snitch

Dostępność w internecie urządzeń OT/IoT może rodzić poważne konsekwencje dla cyberbezpieczeństwa instytucji, których dotyczy. Snitch pozwala automatycznie monitorować taką ekspozycję z wykorzystaniem serwisów Shodan i Zoomeye.

Umożliwia on ustalanie reguł, w ramach których tworzone są frazy wyszukiwania tzw. dorki. Dorki są definiowane na podstawie wewnętrznej bazy wiedzy zarządzanej przez CERT Polska. Skupiamy się na tym, aby pokrywały one jak najwięcej urządzeń powszechnie wykorzystywanych w zakładach przemysłowych Polsce. Przykładowa lista wybranych systemów, które monitoruje Snitch została pokazana na rysunku 44.



Rysunek 44: Zrzut ekranu części listy reguł OT systemu Snitch

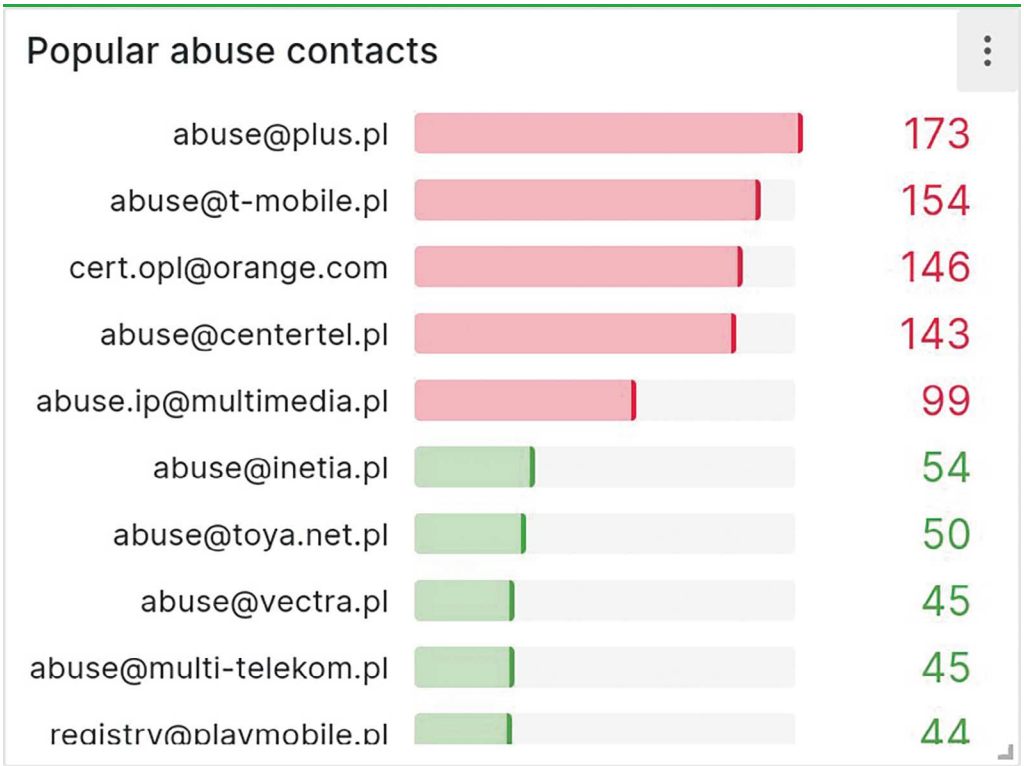
Snitch, korzystając z tych reguł, cyklicznie odpytuje wyszukiwarki i zapisuje wykryte adresy IP. Kolejny moduł generuje raporty w formie wiadomości e-mail, wyszukuje adres kontaktowy (ang. abuse contact) dla danego adresu IP i wysyła wiadomość.

Drugim kanałem kontaktowym jest system n6. Dodatkowa możliwość komunikacji zwiększa szanse na dotarcie do faktycznego właściciela systemu w przypadku problemów.

Warto podkreślić, że skanowania odbywają się cyklicznie, co pozwala monitorować stan odłączania niepożądanych urządzeń od internetu i podejmować dodatkowe działania w przypadku długotrwałego braku reakcji ze strony adresata.

Trudności

Dużym wyzwaniem, z jakim się mierzymy, jest docieranie do faktycznych administratorów systemów, którzy mogą podjąć działania zabezpieczające. Naszym głównym źródłem kontaktów jest baza RIPE, gdzie niestety dane nie zawsze są aktualne lub wskazują na operatora, który co prawda jest właścicielem adresu IP, ale nie jest administratorem urządzenia z niego korzystającego. Dodatkowo, często dla danego adresu IP można pozyskać kilka kontaktowych adresów e-mail, a wybór właściwego nie zawsze jest oczywisty, zwłaszcza przy przetwarzaniu przez automatyczne systemy. Najczęściej systemy przemysłowe są podłączane do internetu z wykorzystaniem kart SIM. W takim przypadku adresem kontaktowym będzie operator telefonii komórkowej, który to dopiero może przekazać nasze powiadomienie do właściwego adresata. Najliczniejszych odbiorców powiadomień pokazano na rysunku 45.



Rysunek 45: Najliczniejsi odbiorcy powiadomień z systemu Snitch

Kolejny problem pojawia się już po nawiązaniu kontaktu. Właściciele prywatni nie mają obowiązku podjęcia działań w celu usunięcia zagrożenia i nie zawsze udaje się ich do tego przekonać. Zdarzają się też przypadki, gdzie wsparcie dostawcy systemu nie zostało przedłużone, a właściciel nie potrafi sam zmienić jego konfiguracji.

Obie te trudności udaje się najczęściej rozwiązać, ale nierzadko zajmuje to dużo czasu, podczas którego niezabezpieczone urządzenie może być wykorzystane do ataku. Dlatego też w przypadku poważnego zaniedbania bezpieczeństwa systemów mogących mieć znaczny wpływ na bezpieczeństwo obywateli, np. panel sterowania oczyszczalnią ścieków, incydenty są odpowiednio eskalowane w celu przyspieszenia ich obsługi.

Nowości

W najbliższych planach chcemy dodać nowe źródło danych w postaci systemu n6. Do tej pory dane były jedynie wysyłane do n6 w celu dystrybucji do podłączonych do tego systemu podmiotów. Zauważaliśmy jednak potencjał poszerzenia naszego monitoringu i raportowania poprzez zbieranie danych z n6 pochodzących ze źródeł zewnętrznych jak np. Shadowserver, a następnie rozsyłanie powiadomień drogą mailową.

Od nowego roku Snitch to nie tylko OT, ale również IT. W ramach części zadań nowo powołany podzespół zajmuje się agregowaniem dorków i rozsyłaniem powiadomień o podatnościach w systemach IT. W większości przypadków nie ma możliwości jednoznacznej weryfikacji, czy konkretna usługa jest podatna. Z tego powodu powiadomienie o podatności otrzymują wszyscy właściciele usług widocznych w dniu pojawienia się podatności z prośbą o weryfikację.

Statystyki raportowania OT

Pierwsze powiadomienia wypłynęły z aplikacji z dniem 26 maja 2023. Od tego czasu aż do końca roku zostało wysłanych 1748 powiadomień mailowych. Dotyczyły one 5564 usług, z czego 968 były unikalne i dotyczyły 813 unikalnych hostów. Obecnie w systemie działa 39 reguł monitorowania.

Z naszych obserwacji wynika, że pomimo naszych działań ostrzegawczych w ogólnym trendzie nie widać znaczących zmian w widoczności systemów przemysłowych. Jednak w 2023 roku system był mocno rozbudowywany, a reguły modyfikowane. Pełny obraz spodziewamy się zobaczyć dopiero w 2024 roku, kiedy system będzie funkcjonował ze znacznie większą liczbą reguł przez pełny rok.

Bezpieczna Poczta

W 2023 roku CERT Polska stworzył serwis bezpiecznapoczta.cert.pl, którego celem jest ochrona użytkowników poczty elektronicznej i ułatwienie instytucjom sprawdzenia poprawności konfiguracji mechanizmów podnoszących jej bezpieczeństwo.

Główne funkcjonujące dziś instrumenty weryfikacji nadawcy poczty to: SPF, DMARC i DKIM. Niepoprawna ich konfiguracja naraża instytucję na znaczące ryzyko. Daje bowiem cyberprzestępcom możliwość wysyłania fałszywych wiadomości, w których mogą podszyć się pod dowolnego nadawcę z domeny tego podmiotu. Właśnie dlatego niektórzy dostawcy poczty traktują e-maile przychodzące z domen niewykorzystujących tych mechanizmów jako spam. Warto zaznaczyć, że używanie mechanizmów SPF, DKIM i DMARC nie wymaga dodatkowej pracy od użytkownika poczty – jeśli administrator je skonfiguruje, wiadomości są weryfikowane automatycznie.

25 sierpnia została opublikowana ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (pełny tekst ustawy znajduje się pod adresem https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20230001703/T/D20231703L.pdf). Wśród innych istotnych rozwiązań, znajdziemy w niej obowiązek stosowania mechanizmów umożliwiających weryfikację nadawcy wiadomości e-mail. Zapisy te dotyczą dostawców poczty, którzy świadczą usługi dla co najmniej 500 000 użytkowników lub dla podmiotu publicznego.

Serwis bezpiecznapoczta.cert.pl jest dostępny publicznie od połowy sierpnia 2023 roku. Od tego czasu użytkownicy sprawdzili za jego pomocą prawie 19 tys. domen, a prawie 8 tys. zostało sprawdzonych więcej niż raz. Z serwisu korzystają nie tylko instytucje publiczne, ale też podmioty prywatne, np. firmy.

Kod źródłowy systemu został opublikowany na platformie Github (https://github.com/CERT-Polska/mailgoose), aby umożliwić uruchamianie podobnych serwisów zagranicznym zespołom CERT.

Projekt JTAN

Joint Threat Analysis Network (JTAN) to europejski projekt koordynowany przez CERT Polska, który ma na celu rozwój narzędzi do pozyskiwania, analizy oraz wymiany informacji o zagrożeniach (Cyber Threat Intelligence). Oprócz naszego zespołu w skład konsorcjum wchodzą europejskie CSIRT-y krajowe: CIRCL (Luksemburg), CERT.LV (Łotwa), CERT.at (Austria), SK-CERT (Słowacja), CERT-EE (Estonia), DNSC (Rumunia) oraz firma Corexalys (Francja).

Narzędzia udostępniane na otwartych licencjach rozwijane w ramach projektu to:

- AIL - system do zbierania, indeksowania i analizowania danych nieustrukturyzowanych związanych z bezpieczeństwem. https://www.ail-project.org/
- Graphoscope - narzędzie wspomagające pracę analityków poprzez integrację i wizualizację danych z wielu źródeł. https://github.com/cert-lv/graphoscope
- Taranis NG - system automatyzujący pozyskiwanie informacji z otwartych źródeł (OSINT) i ułatwiający ich analizę. https://github.com/SK-CERT/Taranis-NG
- n6 - platforma do automatycznej dystrybucji informacji o zagrożeniach. https://github.com/CERT-Polska/n6
- MWDB - repozytorium danych o złośliwym oprogramowaniu. https://github.com/CERT-Polska/mwdb-core
- CocktailParty - narzędzie do udostępniania strumieni danych, w szczególności pochodzących z sensorów. https://github.com/flowintel/cocktailparty

W ubiegłym roku rozpoczęliśmy prace nad integracją wybranych narzędzi, aby ułatwić analizę zróżnicowanych zbiorów danych, do których dostęp mają CSIRT-y oraz inne podmioty monitorujące zagrożenia.

Realizacja projektu rozpoczęła się w 2021, a zakończy w 2024 roku. Jest on współfinansowany z funduszy Unii Europejskiej w ramach instrumentu „Łącząc Europę”, numer grantu 2020-EU-IA-0260.

Współfinansowane przez instrument Unii Europejskiej „Łącząc Europę”

DNS4EU

DNS4EU to element opublikowanej przez Komisję Europejską strategii cyberbezpieczeństwa , który ma na celu wprowadzenie prywatnego i bezpiecznego publicznego resolvera DNS w ramach Unii Europejskiej. Będzie on stanowił alternatywę dla obecnie dominujących na rynku usług, kontrolowanych przez podmioty spoza UE, budując niezależność w obszarze usług cyfrowych. Projekt realizuje międzynarodowe konsorcjum tworzone przez Whalebone (Czechy, lider), CZ.NIC (Czechy), CVUT (Czechy), Time.lex (Belgia), deSEC (Niemcy), HUN-REN Sztaki (Węgry), ABILAB (Włochy), DNSC (Rumunia) oraz NASK-PIB.

Wykorzystanie resolvera DNS4EU będzie w pełni dobrowolne, a użytkownicy zawsze będą mieć możliwość korzystania z usługi innego dostawcy. Jednakże jedną z przewag DNS4EU będzie skuteczna ochrona przed zagrożeniami wymierzonymi w obywateli UE poprzez szybkie blokowanie niebezpiecznych stron na poziomie DNS.

Po stronie NASK-PIB projekt realizuje CERT Polska wspólnie z Centrum Badań i Rozwoju. Nasze prace skupiają się na wczesnym wykrywaniu domen wykorzystywanych do phishingu, a efekty będą również służyły do ulepszenia prowadzonej przez nas Listy Ostrzeżeń przed niebezpiecznymi stronami (https://cert.pl/lista-ostrzezen/).

Projekt oficjalnie rozpoczął się w styczniu 2023 roku, a wsparcie finansowe UE będzie trwać trzy lata. Przez ten czas zostanie opracowany model biznesowy, który zapewni długofalowe utrzymanie usługi. Należy jednak zaznaczyć, że publiczny resolver pozostanie bezpłatny dla użytkowników końcowych. Więcej informacji znajduje się na oficjalnej stronie projektu: https://www.joindns4.eu/

Numer grantu: 101095329 21-EU-DIG-EU-DNS,

pełna nazwa projektu: **DNS4EU and European DNS Shield.**

DNS4EU

Dofinansowane przez Unię Europejską

Artemis

Rysunek 46: Logo narzędzia Artemis

W roku 2023 CERT Polska inaugurował kolejne działania poprawiające bezpieczeństwo polskiego internetu. Jednym z zainicjowanych w tym czasie projektów był Artemis. Dwanaście miesięcy działania dało imponujące efekty - przeskanowaliśmy ponad 50 tys. domen i adresów IP, odkrywając ponad 180 tys. podatności lub błędnych konfiguracji.

Artemis to narzędzie rozwijane przez zespół CERT Polska, a zapoczątkowane przez członków koła Politechniki Warszawskiej KN Cyber. Przy jego pomocy badamy strony udostępnione w internecie w poszukiwaniu podatności bezpieczeństwa i błędów konfiguracyjnych. Regularne skanowanie systemów pozwala monitorować i podnosić ich poziom bezpieczeństwa. Uzyskane wyniki nie są w żaden sposób upubliczniane, a jedynie niezwłocznie przekazywane administratorom, dzięki czemu zyskują oni cenną wiedzę na temat wykrytych podatności i mogą wykorzystać ją w celu poprawy bezpieczeństwa zarządzanych przez siebie systemów. Warto też dodać, że w ramach ponownych testów zespół CERT Polska sprawdza, czy niezbędne poprawki zostały wdrożone.

Istotną cechą przygotowanego przez nas narzędzia jest to, że proces skanowania pozwala administratorom zidentyfikować obserwowane działania jako prowadzone przez CERT Polska. Pozwala to ograniczyć do minimum ewentualny stres i zagrożenia związane z pochopnym reagowaniem. Wszystkie istotne dla administratorów informacje zostały opisane na dedykowanej podstronie: https://cert.pl/skanowanie/

Rezultaty licznych skanowań, poza podnoszeniem poziomu bezpieczeństwa danego podmiotu, pozwalają też budować szerszy obraz cyberbezpieczeństwa Polski i kierować zasoby CERT Polska tam, gdzie są one najbardziej potrzebne, np. poprzez tworzenie poradników, czy prowadzenie akcji informacyjnych i edukacyjnych.

W 2023 roku łącznie przeskanowano ok. 50.6 tys. domen i adresów IP i ok. 251.7 tys. subdomen, w tym:

- ok. 36.9 tys. domen oraz ok. 25.7 tys. subdomen szkół i placówek oświatowych - skanowane były m.in. strony szkół podstawowych, ponadpodstawowych oraz policealnych, jak również domeny młodzieżowych domów kultury, przedszkoli czy poradni psychologiczno-pedagogicznych,
- ok. 5.4 tys. domen i adresów IP oraz ok. 95.5 tys. subdomen jednostek samorządu terytorialnego - skanowane były także np. strony spółek odpowiedzialnych za wywóz śmieci, jak również archiwalne domeny czy systemy obsługujące pocztę, jeśli znajdowały się w subdomenie danej gminy,
- ok. 2.3 tys. domen i adresów IP oraz ok. 3.8 tys. subdomen - badanie na zlecenie CSIRT MON,
- ok. 1.9 tys. domen oraz ok. 7 tys. subdomen firm i instytucji, które same zgłosiły się do skanowania,
- ok. 1.7 tys. domen oraz ok. 14.9 tys. subdomen w domenie gov.pl,
- ok. 1.1 tys. domen oraz ok. 2.9 tys. subdomen - badanie na zlecenie Organu Właściwego ds. cyberbezpieczeństwa w sektorze zdrowia,
- 890 domen i adresów IP oraz ok. 84.4 tys. subdomen uczelni - były to np. strony wydziałów, ale też domeny związane z konferencjami czy projektami naukowymi,
- 521 domen oraz ok. 2.3 tys. subdomen banków,
- 397 domen oraz ok. 1.1 tys. subdomen stron m.in. posłów, senatorów, prezydentów miast i partii politycznych w kontekście wyborów parlamentarnych w 2023 i samorządowych w 2024,

- 373 domeny i adresy IP oraz 537 subdomen - badanie na zlecenie Ministerstwa Infrastruktury,
- 343 domeny oraz ok. 1.8 tys. subdomen gazet i portali lokalnych,
- 289 domen i adresów IP oraz 551 subdomen - inne,
- 267 domen oraz ok. 34.1 tys. subdomen operatorów usług kluczowych,
- 70 domen oraz ok. 1 tys. subdomen producentów automatyki przemysłowej.

Domeny z prefiksem www zostały wyłączone z powyższego zestawienia. Oznacza to, że strona dostępna zarówno pod adresem www.strona.pl, jak i strona.pl zostanie uwzględniona raz. Niektóre domeny mogą występować w więcej niż jednej kategorii, np. uczelnie wojskowe.

Łącznie zgłoszono ok. 184.8 tys. podatności lub błędnych konfiguracji, w tym ok. 11.6 tys. wiążących się z wysokim, ok. 106.8 tys. - średnim i ok. 66.3 tys. - niskim zagrożeniem. Przynajmniej jedną podatność/błędną konfigurację wykryto w ok. 65.8 tys. przeskanowanych domenach/subdomenach.

Znaleziono:

- ok. 78.7 tys. przypadków korzystania z nieaktualnego oprogramowania - stwarza to ryzyko ataku przy użyciu znanych podatności - niektóre z nich mogą skutkować tym, że ze strony można pobrać dane, inne pozwalają zmieniać treść strony lub np. uzyskać uprawnienia administratora,
- ok. 44.2 tys. przypadków problemów z konfiguracją SSL/TLS - stwarza to ryzyko przechwycenia komunikacji użytkownika ze stroną - jeżeli dane zostaną przechwycone i pojawił się tam login i hasło, to przestępca może je poznać i zalogować się do serwisu jako uprawniony użytkownik,
- ok. 27 tys. przypadków błędnie skonfigurowanych mechanizmów weryfikacji nadawcy poczty e-mail - stwarza to ryzyko wysyłania fałszywych e-maili z danej domeny,
- ok. 16 tys. przypadków, gdy zasób taki, jak np. panel administracyjny czy panel logowania (np. do bazy danych czy usługi zdalnego pulpitu) był dostępny publicznie - atak jest możliwy np. jeśli jedno z kont ma słabe hasło albo jeśli w usłudze występują podatności,
- ok. 11.2 tys. przypadków, gdy informacje o konfiguracji serwera, lista subdomen lub listy plików w folderach na serwerze były dostępne publicznie - może to atakującemu ułatwić rekonesans, poznanie używanego oprogramowania lub nazw plików, które nie powinny być dostępne publicznie, a w konsekwencji także umożliwić ich pobranie,
- ok. 4.5 tys. przypadków konkretnych krytycznych lub poważnych podatności umożliwiających np. przejęcie strony lub pobranie danych z bazy danych,
- ok. 3.4 tys. przypadków, gdy wrażliwe dane, takie jak: kopie zapasowe, kod źródłowy, zrzuty bazy danych czy dziennik zdarzeń serwera były dostępne publicznie,
- 20 przypadków, gdy domena zbliżała się do wygaśnięcia - odpowiednio wczesne powiadomienie instytucji zmniejsza ryzyko niedostępności usługi lub przejęcia domeny przez atakującego.

Administratorzy systemów otrzymują na bieżąco informacje o wykrytych podatnościach.

Skanowanie jest automatycznie, dlatego też powyższe liczby mogą zawierać duplikaty lub odnosić się do sytuacji, w których w rzeczywistości podatność nie występuje, ponieważ np. wykryto niepoprawnie skonfigurowane SSL/TLS w domenie, która w praktyce nie jest używana.

Kod źródłowy systemu Artemis jest publiczny (https://github.com/CERT-Polska/Artemis) i wykorzystywany m.in. przez zagraniczne zespoły CERT - dzięki temu CERT Polska ma istotny wpływ na poprawę bezpieczeństwa również systemów niepozostających w jego obszarze odpowiedzialności.

Platforma MWDB

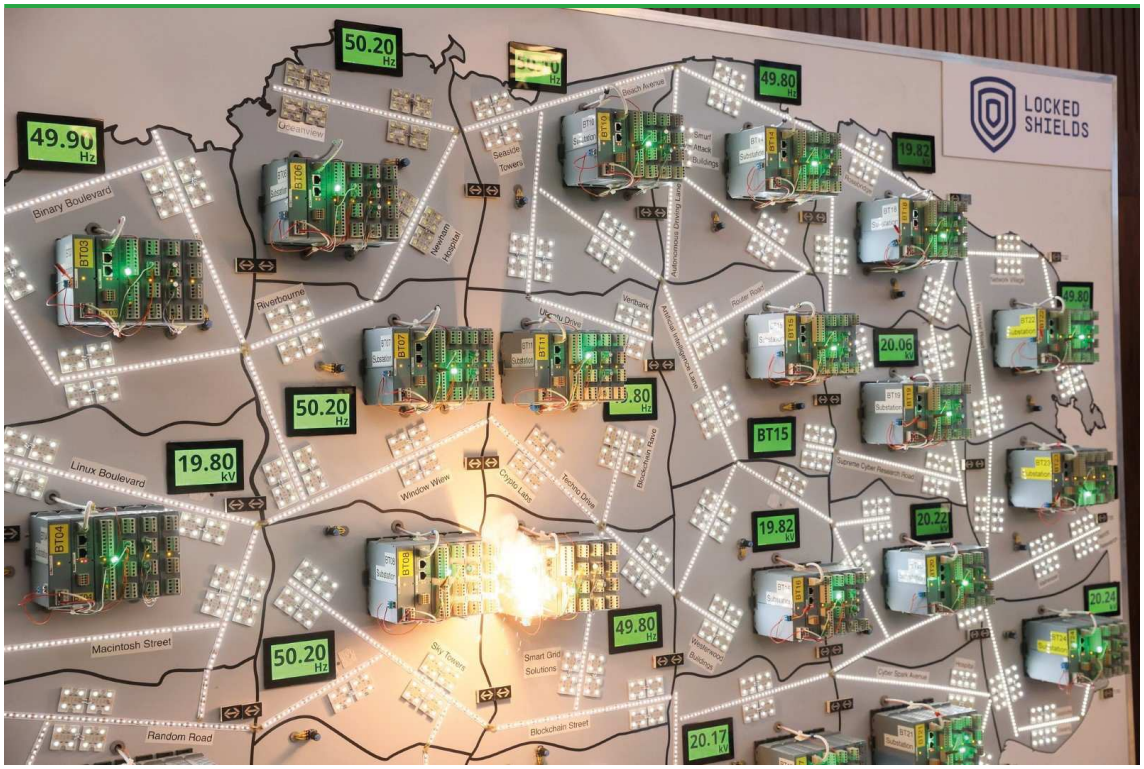
MWDB to repozytorium informacji na temat złośliwego oprogramowania prowadzone i rozwijane przez CERT Polska. Próbki złośliwego oprogramowania są automatycznie wzbogacane dodatkowymi metadanymi pochodzącymi z wewnętrznych systemów analitycznych. Kod MWDB jest udostępniany na otwartej licencji: https://github.com/CERT-Polska/mwdb-core. W 2023 roku dodano do repozytorium ponad 300 tys. próbek złośliwego oprogramowania. W ramach wykonanych automatycznych analiz dla 40 tys. z nich została określona rodzina złośliwego oprogramowania. Uzyskano również 13 tys. nowych unikalnych konfiguracji, czyli informacji, które służą szkodliwemu oprogramowaniu do komunikowania się z serwerami przestępców. Uzyskane dane pozwalają specjalistom CERT Polska na śledzenie aktywności poszczególnych rodzin złośliwego oprogramowania.

Wykres 6: Wykres przedstawiający 10 najczęściej obserwowanych rodzin złośliwego oprogramowania w 2023 roku

Baza wiedzy MWDB zasilana jest również dzięki danym przesyłanym przez specjalistów z całego świata. W 2023 roku do projektu MWDB dołączyło 263 analityków, a pod koniec roku liczba aktywnych kont wyniosła niemal 1,5 tysiąca. Samo oprogramowanie również doczekało się licznych ulepszeń m.in. dzięki sugestiom i poprawkom od użytkowników, przesłanym w serwisie GitHub.

Ćwiczenia i konkursy

Locked Shields 2023



Rysunek 47: fot. CCDCOE

Locked Shields to organizowane przez NATO największe ćwiczenia obrony bezpieczeństwa komputerowego na świecie. Od 12 lat co roku (z przerwą w 2020) specjaliści z uczestniczących w ćwiczeniu krajów biorą udział we wspólnych zmaganiach. W 2023 roku w wydarzeniu uczestniczyło ponad 3000 specjalistów z 38 krajów.

Podczas ćwiczeń zadaniem ekspertów jest obrona infrastruktury „Berylii" - fikcyjnego kraju należącego do NATO. Nie jest to łatwe zadanie - już od początku ćwiczenia sieć kraju jest atakowana przez hakerów wrogiej „Krymsonii". Aby wyjść z tego zmagania obronną ręką, obrońcy Berylii muszą zabezpieczyć się na każdym poziomie - stacji roboczych pracowników, serwerów usługowych, sieci, routerów, a nawet systemów przemysłowych i infrastruktury krytycznej. A to nie wszystko - poza aspektami technicznymi, w ćwiczeniu oceniane są też bardziej miękkie aspekty, jak poprawna interpretacja prawa w zakresie cyberbezpieczeństwa, oraz reakcja medialna na pojawiające się fałszywe informacje. Liczą się także działania strategiczne, w których testowane są procesy zarządzania kryzysowego. Ostatecznie, brana jest pod uwagę również ciągłość działania i czy użytkownicy (symulowani przez organizatora ćwiczenia) mogą skutecznie wykonywać swoją pracę mimo trwających działań w cyberprzestrzeni.

Największy wpływ na zwycięstwo ma oczywiście skuteczna obrona przed wrogimi atakami, ale nie jest to jedyna rzecz, na którą kładzie się nacisk. Ważne jest również dzielenie się z sojusznikami (innymi krajami biorącymi udział w ćwiczeniu) zdobytymi w trakcie analiz informacjami, jak np. próbki złośliwego oprogramowania albo adresy używane do ataków. Jest to logiczne - ostatecznie jednym z głównych celów ćwiczenia jest poprawianie kooperacji między krajami sojuszu północnoatlantyckiego. W przypadku, gdyby scenariusz ćwiczeń stał się kiedyś rzeczywistością, kluczowa będzie skuteczna wymiana informacji między współpracującymi w NATO krajami.

Polska reprezentacja, pod przewodnictwem wojskowego 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 2023 roku 3 miejsce (na 24 startujące zespoły). Na podium LS 2023 stanęły również łączone zespoły szwedzko-islandzki (pierwsze miejsce) oraz zespół łączący specjalistów z Estonii i USA (drugie miejsce).

W 2023 roku eksperci z CERT Polska oraz NASK aktywnie brali udział w ćwiczeniach, pomagając m.in. w obronie:

- systemów specjalnych (w tym infrastruktury przemysłowej),
- aplikacji internetowych,
- systemów Linux,
- infrastruktury sieciowej,
- a także pracowali w zespołach od analiz prawnych oraz informatyki śledczej.

European Cyber Security Challenge 2023

Rysunek 48: Polska reprezentacja na zawodach ECSC 2023, fot. CERT Polska

European Cyber Security Challenge (ECSC) to międzynarodowe zawody cyberbezpieczeństwa, w których biorą udział drużyny złożone z młodzieży z krajów z całego świata. Celem projektu jest popularyzacja wiedzy o cyberbezpieczeństwie wśród starszej młodzieży i młodych dorosłych, oraz zachęcanie do wyboru kariery w tym obszarze. Drużyna z każdego kraju składa się z 5 osób w wieku od 14 do 20 roku życia oraz 5 osób w wieku od 21 do 25 lat.

W Polsce w celu wyłonienia reprezentacji organizowane są krajowe kwalifikacje, za które od początku odpowiada CERT Polska. W 2023 roku frekwencja była rekordowa, w zawodach wzięło udział 156 osób, z czego 106 ukończyło przynajmniej jedno zadanie. Specjaliści CERT Polska i NASK-PIB opiekują się reprezentacją również podczas finałów oraz pilnują przebiegu zawodów - w 2023 roku sprawowali role trenerów, członka komitetu sterującego oraz sędziego.

Finały odbyły się w dniach 25-27 października w Hamar w Norwegii. Podczas nich nie obyło się bez problemów technicznych - cały drugi dzień zawodów został unieważniony, a gracze narzekali również na problemy z dostępami do platformy konkursu oraz nieoryginalnymi zadaniami (wykorzystanymi wcześniej na innych zawodach). Po zaciekłej walce, Polska zajęła 9 miejsce na 28 zespołów - na podium stanęły zespoły z Niemiec, Szwajcarii i Danii.

HackASat

Rysunek 49: Zdjęcie sceny konkursu z wynikami na koniec drugirgo dnia, fot. Can Info Space

W sierpniu 2023 r. odbyła się czwarta i, jak do tej pory, największa edycja konkursu „Hack-A-Sat" organizowanego przez amerykańskie wojsko. Reklamowany przez slogan „World's first CTF in space" („Pierwszy konkurs Capture the Flag w kosmosie"), to największy dotychczas konkurs bezpieczeństwa informatycznego w branży kosmicznej.

W tym roku finały odbyły się stacjonarnie w Las Vegas w ramach konferencji DEFCON. Do celów konkursu wystrzelony został w kosmos prawdziwy satelita, na którym zawodnicy uruchamiali swoje programy oraz - oczywiście - próbowali wykorzystać błędy w jego zabezpieczeniach i przejąć nad nim kontrolę. Mimo że podatności oraz środowisko zostały specjalnie przygotowane do zawodów tak, żeby gracze nie byli w stanie zaburzyć dostępności platformy, nie wszystko poszło gładko. Największym problemem okazała się fizyka - z uwagi na orbitę, po której poruszał się satelita (a która była całkowicie poza kontrolą organizatorów), polecenia można było wysyłać jedynie w krótkich oknach czasowych, które dodatkowo musiały zostać równo podzielone między wszystkich graczy.

Mimo tych trudności polski zespół „Poland Can Into Space", w skład którego weszli także pracownicy CERT Polska, zajął drugie miejsce. Zawody wygrał włoski zespół „mhackeroni".

Statystyki

n6

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

Metodyka

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 są rejestrowane przez nasze systemy monitorujące i rzadko zostają 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.

Kolejna uwaga dotyczy wersji protokołu IP: wszystkie podane statystyki odnoszą się do wersji czwartej tego protokołu. Wynika to z niewielkiego wciąż stopnia wdrożenia IPv6 w naszym n6

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.

Kolejna uwaga dotyczy wersji protokołu IP: wszystkie podane statystyki odnoszą się do wersji czwartej tego protokołu. Wynika to z niewielkiego wciąż stopnia wdrożenia IPv6 w naszym kraju oraz, co się z tym wiąże, z pomijalnie małej liczby zgłoszeń jakie otrzymujemy odnośnie tego rodzaju adresów.

Ostatnia uwaga dotyczy rozmiarów systemów autonomicznych (AS). Ustaliliśmy je na podstawie danych pochodzących z RIPE z 1 lipca 2023 r.

Botnety

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

Boty w Polsce

W 2023 r. łącznie zgromadziliśmy informacje o 277 936 adresach IP wykazujących aktywność botów. Porównując z 2022 r., jest to spadek o około 25 tys. Średnia dzienna liczba zainfekowanych urządzeń w polskim internecie wynosiła 3 838. Na przestrzeni roku obserwujemy niewielką tendencję spadkową z około 4 tys. na początku roku do 3 tys. we wrześniu. Od tego momentu zanotowaliśmy znaczny wzrost co ma związek z pojawieniem się nowych zagrożeń, których wcześniej nie obserwowaliśmy. Liczba zainfekowanych urządzeń pod koniec roku osiągnęła wartość około 7 tys. Tabela 2 prezentuje liczbę zainfekowanych komputerów w polskich sieciach.

	Rodzina	Maksimum dzienne	Średnia dzienna	Odchylenie standardowe	Czas obserwacji
1	Socks5System	2 825	1 832	1 077	13,97%
2	Andromeda	1 469	992	216	100%
3	Mirai	1 000	339	181	100%
4	Avalanche	866	460	129	99,72%
5	AdLoad	733	590	138	36,16%
6	Lumma Stealer	525	155	163	12,32%
7	PseudoMa-nuscrypt	516	276	213	35,34%
8	Hummer	474	118	29	97,80%
9	QSnatch	466	343	57	97,26%
10	Conficker	455	278	70	98,35%

Tabela 2: Największe botnety w Polsce.

W polskich sieciach od lat obserwujemy aktywność botnetów, które już są sinkholowane. Przykładem takiego botnetu jest Andromeda, który po raz kolejny znalazł się w czołówce powyższego zestawienia ze średnią dzienną liczbą zainfekowanych urządzeń na poziomie prawie 1 tys. W przypadku botnetów Andromeda, Avalanche, Hummer oraz Conficker obserwujemy utrzymującą się w skali roku liczbę zainfekowanych urządzeń. Trend spadkowy zanotowaliśmy natomiast w przypadku botnetów Mirai oraz QSnatch. Niektóre z zagrożeń znajdujących się w tabeli zaczęliśmy obserwować dopiero pod koniec roku. Są to Socks5Systemz, AdLoad, Lumma Stealer i PseudoManuscrypt. Szczególną uwagę warto zwrócić na Socks5Systemz, który znalazł się na pierwszym miejscu w tabeli ze średnią liczbą zainfekowanych urządzeń przekraczającą 1,8 tys.

Serwery C&C w Polsce

Serwery C&C były aktywne w Polsce pod 26 różnymi adresami IP w 16 systemach autonomicznych. Jest to mniej niż w 2022 r., kiedy zebraliśmy informacje o 29 adresach IP w 19 systemach autonomicznych. Systemami autonomicznymi, w których znajdowało się najwięcej polskich adresów IP są AS201814, AS210228, AS20940 oraz AS21021. W każdym z nich obserwowaliśmy 3 adresy. W 2023 r. otrzymaliśmy 1 zgłoszenie o pełnej nazwie domenowej (FQDN), która pełniła rolę serwera C&C, wykorzystując domenę .pl.

Phishing

W tym rozdziale uwzględniamy wyłącznie statystyki dotyczące phishingu w tradycyjnym rozumieniu tego słowa, czyli jedynie podszywania się 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.

Phishing hostowany w polskich sieciach

W 2023 r. otrzymaliśmy łącznie 95 696 zgłoszeń phishingu w polskich sieciach. Dotyczyły one 51 374 adresów URL z 49 039 domenami, które rozwiązywały się na 3 097 adresów IP. W tabeli 3 wymieniliśmy 10 dostawców, u których w polskich sieciach znajdowało się najwięcej stron phishingowych. Analogicznie jak w poprzednich latach, można zauważyć znaczący udział home.pl w porównaniu z innymi systemami autonomicznymi.

Poz.	Nazwa	Numery AS	Liczba adresów IP	Liczba domen	Liczba IP na liście ostrzeżeń	Liczba domen na liście ostrzeżeń
1	home.pl	12824	478	1268	276	590
2	Akamai Technologies	20940, 16625	434	454	4	3
3	Nazwa.pl	15967	316	6080	10	14
4	Cyber Folks	41079, 29522, 43758	275	9262	35	149
5	Artnet	200088, 197155	192	1610	60	794
6	OVH	16276	129	2841	11	22
7	Atman	57367, 15694, 24723	95	2746	6	22
8	LH.pl	203417	72	1022	16	460
9	Beyond.pl	31229	69	447	1	2
10	Sprint	197226	60	406	3	10

Tabela 3: Dostawcy, u których w polskich systemach autonomicznych znajdowało się najwięcej stron phishingowych

Phishing, który trafił na listę ostrzeżeń CERT Polska

W 2023 r. na listę ostrzeżeń CERT Polska trafiło 79 267 domen, które udało się rozwiązać na 24 595 adresów IP. W praktyce oznacza to zablokowanie około 54 milionów prób rozwiązań nazw mnemonicznych (w uproszeniu: prób wejścia) stron uznanych za stanowiące zagrożenie. Liczba zapytań o zawartość listy ostrzeżeń wysłanych do naszych serwerów wyniosła w 2023 r. około 191 milionów. Podobnie jak w ubiegłym roku przestępcy atakujący użytkowników wykorzystywali usługi Cloudflare do ukrycia prawdziwej lokalizacji serwera, aż 81% adresów IP należało do tego dostawcy. Pomijając amerykańskie firmy oraz home.pl przestępcy chętnie wykorzystują infrastrukturę na Cyprze, w Chinach oraz w Rosji.

W tabeli 4 umieściliśmy najczęściej występujące domeny najwyższego poziomu, które znalazły się na liście ostrzeżeń. Najpopularniejszymi TLD 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.	TLD	Liczba domen
1	com	22799
2	pl	16735
3	xyz	6646
4	site	5587
5	top	3051
6	online	2432
7	info	1764
8	space	1239
9	live	1224
10	click	1187

Tabela 4: Najczęściej występujące domeny najwyższego poziomu (TLD), które znalazły się na liście ostrzeżeń

W tabeli 5 znajdują się najpopularniejsze cele, pod które podszywali się przestępcy. W 2023 r. najczęściej występującym celem phishingu były oszustwa inwestycyjne. W tym przypadku oraz w przypadku oszustw na Allegro, Baltic Pipe, OLX oraz PGNiG odnotowaliśmy znaczny wzrost liczby domen. W przypadku oszustw związanych z firmami Facebook oraz InPost widoczny jest spadek. Jak w przypadku większości obserwowanych przez nasz zespół kampanii, więcej szczegółów można znaleźć w artykule zamieszczonym na naszej stronie.

Poz.	Cel phishingu	Liczba domen 2023 r.	Liczba domen 2022 r.
1	Inwestycje	20609	2443
2	Allegro	11015	643
3	Baltic Pipe	6971	583
4	Facebook	6638	7186
5	OLX	4564	1656
6	InPost	2770	6728
7	PGNiG	2764	309
8	Tesla	2758	2647
9	Netflix	1495	1231
10	Webmail	1325	562

Tabela 5: Najczęściej występujące cele phishingu, które znalazły się na liście ostrzeżeń

Usługi pozwalające na prowadzenie ataków DRDoS

W 2023 r. otrzymaliśmy 28 616 864 zgłoszenia o 639 075 adresach IP w Polsce, pod którymi znajdowały się usługi umożliwiające przeprowadzenie rozproszonych ataków odmowy usługi ze wzmocnieniem (Distributed Reflection Denial of Service - DRDoS). 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.

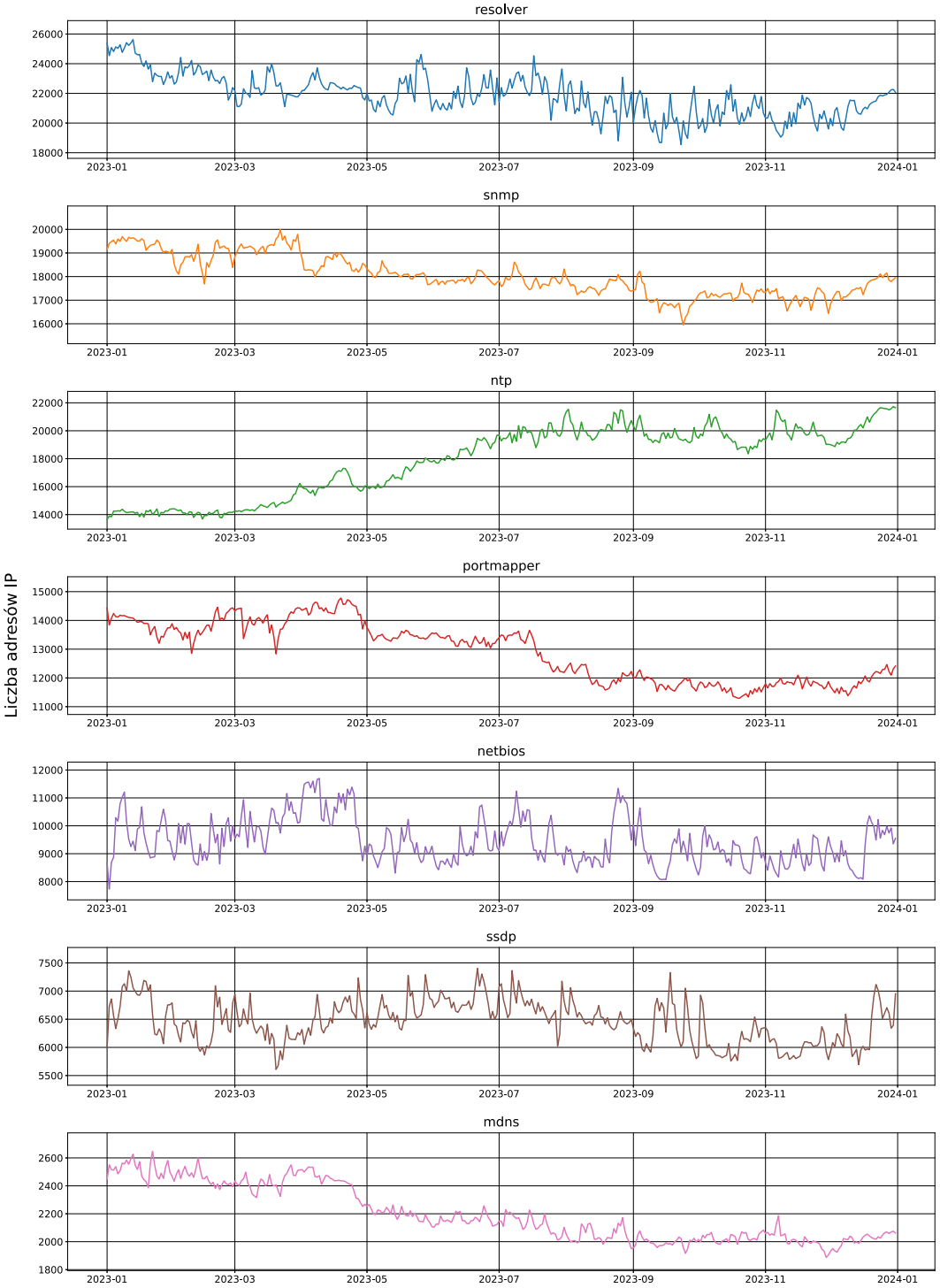
Poniżej przedstawiamy zestawienie usług, które mogły być wykorzystane do ataków i były najliczniej reprezentowane w polskim internecie. Wybrane usługi zostały omówione w dalszej części raportu.

Poz.	Nazwa podatności / otwartej usługi	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odchylenie standardowe	Czas obserwacji
1	Open resolver	21811	25849	2472	98,08%
2	SNMP	17991	19938	1249	98,63%
3	NTP	17866	21857	2592	98,08%
4	Portmapper	12797	14970	1226	97,80%
5	NetBIOS	9458	11893	1356	98,63%
6	SSDP	6447	7495	620	98,35%
7	mDNS	2195	2626	213	98,63%
8	mssql	1324	1945	176	98,08%
9	Ubiquiti	1281	1650	139	97,80%
10	DVR DHCPDiscover	1245	1842	310	98,35%
11	CHARGEN	116	182	16	98,90%
12	CoAP	35	45	4	98,63%
13	QOTD	25	49	4	98,35%
14	XDMCP	17	22	1	98,08%
15	ARD	12	19	2	98,35%
16	RDPEUDP	6	23	3	97,53%

Tabela 6: 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.

Na wykresie 7 został pokazany przebieg zaobserwowanej przez nas liczby urządzeń, które mogą zostać wykorzystane do przeprowadzenia ataków DRDoS w skali roku. Wykresy zostały sporządzone dla 7 najczęściej zgłaszanych usług. W przypadku usług NetBIOS oraz SSDP liczba adresów IP utrzymuje się na podobnym poziomie w skali roku. Pozytywnym trendem jest stopniowy spadek liczby urządzeń związanych z usługą resolver, SNMP, portmapper oraz mDNS na przestrzeni całego roku, natomiast w przypadku usługi NTP widzimy stopniowy wzrost.



Wykres 7: Najpowszechniejsze źle skonfigurowane usługi mogące brać udział w atakach DRDoS. Wykres ukazuje zmiany liczebności podatnych adresów IP w Polsce w 2023 r.

Otwarte serwery DNS

Najpopularniejszą obserwowaną w 2023 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.

Liczba zgłoszeń w ciągu roku: 5 816 393

Liczba unikalnych adresów IP, których dotyczyły zgłoszenia: 334 211

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	14780	18280	0,27%
2	12741	Netia	1900	3141	0,11%
3	51986	PHU IT	995	1024	97,17%
4	12912	T-Mobile	698	829	0,06%
5	50599	Data Space	533	986	4,43%
6	6830	UPC	492	541	0,01%
7	13110	Inea	405	456	0,24%
8	29314	Vectra	366	405	0,07%
9	8374	Plus / Cyfrowy Polsat	271	315	0,02%
10	31242	TKPSA	239	264	0,21%

Tabela 7: 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.

Liczba zgłoszeń w ciągu roku: 5 825 610

Liczba unikalnych adresów IP, których dotyczyły zgłoszenia: 91 801

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	12741	Netia	1966	2161	0,12%
2	5617	Orange	1778	2170	0,03%
3	20804	TELENERGO	819	888	0,34%
4	60920	NETCENTER	516	641	16,80%
5	199390	ALFAKS	495	508	16,11%
6	12912	T-Mobile	320	576	0,03%
7	57978	DIGICOM	311	399	15,19%
8	41809	ENTERPOL	254	282	2,07%
9	6830	UPC	254	290	0,01%
10	200594	SOFT-PARTNER	218	308	10,64%

Tabela 8: 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.

Liczba zgłoszeń w ciągu roku: 6 500 451

Liczba unikalnych adresów IP, których dotyczyły zgłoszenia: 105 973

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	1794	2786	0,03%
2	12741	Netia	1248	1461	0,07%
3	12912	T-Mobile	920	985	0,08%
4	57608	DGNET	898	1554	13,49%
5	6830	UPC	824	1072	0,02%
6	48956	HYPERNET	477	634	9,81%
7	199715	MSITELEKOM	387	398	2,48%
8	9085	SUPERMEDIA	276	285	0,65%
9	198525	CLIMAX	238	253	18,59%
10	29314	Vectra	226	324	0,04%

Tabela 9: 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.

Liczba zgłoszeń w ciągu roku: 4 567 380

Liczba unikalnych adresów IP, których dotyczyły zgłoszenia: 48 692

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	16276	OVH	2245	3111	0,05%
2	57367	ECO-ATMAN	627	1357	4,54%
3	50599	Data Space	502	1158	4,17%
4	47329	WDM	403	421	4,14%
5	12741	Netia	290	321	0,02%
6	59491	LIVENET	266	342	3,71%
7	35787	Internet Cafe	245	254	6,84%
8	197155	ARTNET,	220	379	1,91%
9	31242	TKPSA	217	231	0,19%
10	50840	HITME	211	271	4,58%

Tabela 10: 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.

Liczba zgłoszeń w ciągu roku: 1 850 901

Liczba unikalnych adresów IP, których dotyczyły zgłoszenia: 37 794

Poz.	Numer AS	Nazwa AS	Średnia	Maksimum	Odsetek wszystkich adresów w AS
1	5617	Orange	6146	7357	0,11%
2	12741	Netia	446	539	0,03%
3	12912	T-Mobile	134	165	0,01%
4	13110	Inea	128	147	0,08%
5	8374	Plus / Cyfrowy Polsat	88	110	0,01%
6	16276	OVH	88	138	0,00%
7	8970	WASK	78	163	0,12%
8	8267	CYFRONET	66	105	0,09%
9	12824	home.pl	59	101	0,03%
10	12423	TORMAN	58	143	0,18%

Tabela 11: 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 2023 r. odnotowaliśmy 49 423 317 takich obserwacji dotyczących 773 720 adresów IP z Polski.

Poniżej przedstawiamy zestawienie usług, które mogły być zagrożone atakiem i były najliczniej reprezentowane w polskim internecie.

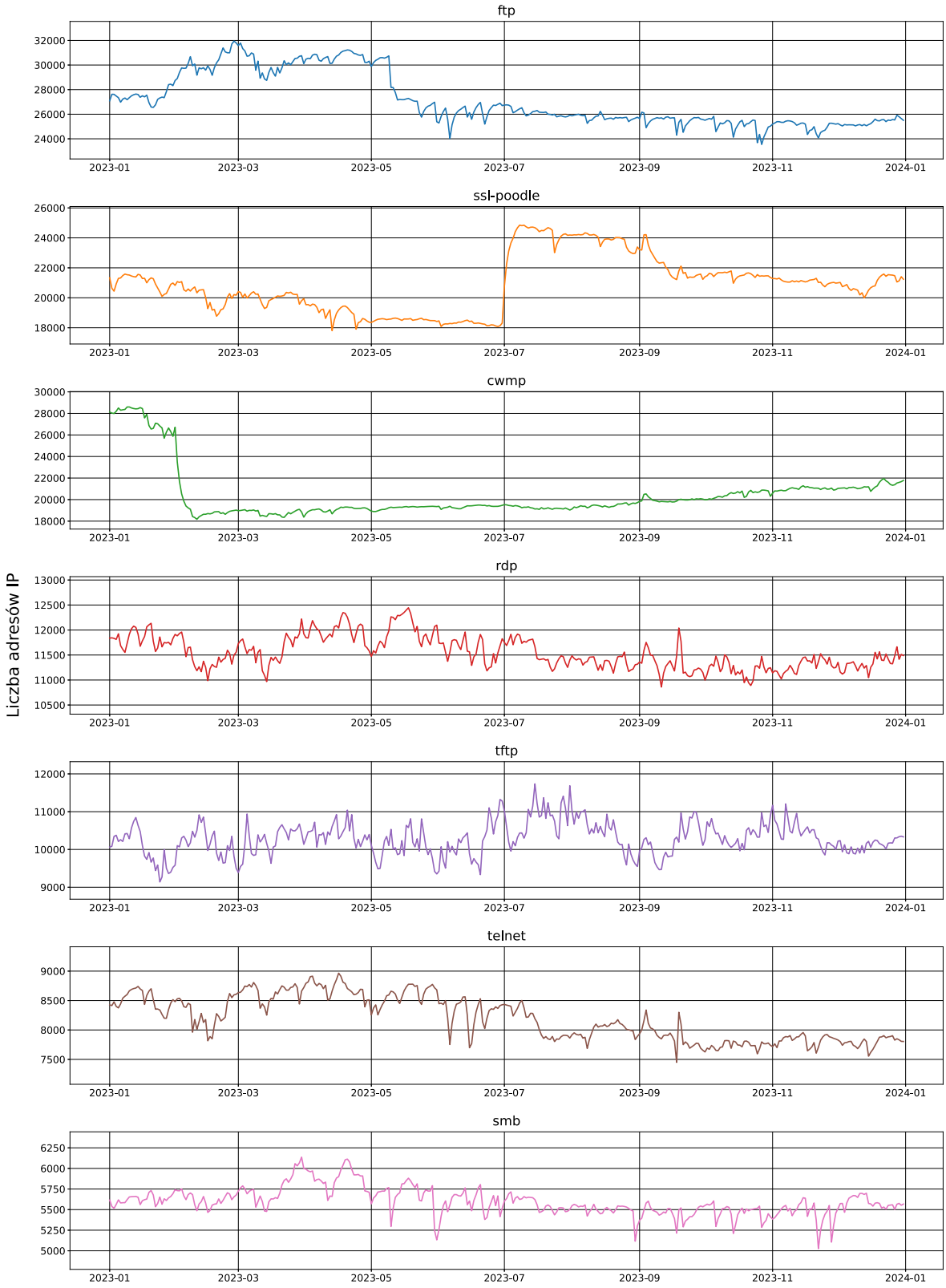
Poz.	Nazwa podatności / otwartej usługi	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odchylenie standardowe	Czas obserwacji
1	FTP (dane uwierzytelniające w postaci jawnej)	26831	31967	2591	98,35%
2	SSL-POODLE	20697	24926	2075	98,35%
3	CWMP	20170	28831	2674	98,08%
4	RDP	11521	12473	474	98,90%
5	TFTP	10290	11770	718	97,53%
6	Telnet	8126	8977	544	98,35%
7	SMB	5512	6129	557	98,63%
8	ISAKMP	4825	5416	282	29,86%
9	BadWPAD	4494	17214	5548	52,32%
10	VNC	3223	5044	441	98,63%
11	SSL-FREAK	2421	3069	450	98,63%
12	RSYNC	2109	2477	264	98,63%
13	NAT-PMP	916	1063	96	98,35%

14	MQTT	853	1091	104	98,35%
15	AFP	785	1074	106	98,63%
16	MongoDB	694	798	92	99,45%
17	AMQP	663	762	77	98,63%
18	IPMI	523	609	34	98,35%
19	IPP	470	628	61	98,90%
20	LDAP	323	400	36	98,90%
21	Memcached	185	217	22	98,63%
22	Radmin	164	256	24	98,63%
23	Cisco Smart Install	93	169	17	98,90%
24	Redis	89	130	17	98,63%
25	Elasticsearch	62	82	7	98,63%
26	ADB	13	25	4	98,63%

Tabela 12: 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 8 został pokazany przebieg zaobserwowanej przez nas liczby urządzeń, na których znajdują się podatne usługi w skali roku. Wykresy zostały sporządzone dla 7 najczęściej zgłaszanych usług. Porównując rok 2023 z 2022, nie zauważamy dużych zmian w czołówce zestawienia. Wciąż podobne usługi są w Polsce zagrożone atakiem. Na uwagę zasługują wykresy dla FTP, SSL-POODLE oraz CWMP. Kształt wykresu dla usługi FTP zdeterminowała sytuacja w AS20853. W przypadku SSL-POODLE zanotowaliśmy skokowy wzrost liczby adresów IP, na który wpływ miały AS35191 oraz AS198766. Sytuację odwrotną zanotowaliśmy dla usługi CWMP gdzie widzimy gwałtowny spadek, na który wpływ miał AS12741 należący do Netii. W przypadku RDP, TFTP, Telnet oraz SMB dzienna liczba adresów IP utrzymuje się w skali roku na podobnym poziomie.



Wykres 8: Najpowszechniejsze zagrożone usługi. Wykres ukazuje zmiany liczebności podatnych adresów IP w Polsce w 2023 r.

W ramach omawiania podatnych usług zdecydowaliśmy się wydzielić podrozdziały dotyczące serwerów Exchange, usługi HTTP oraz systemów przemysłowych (ICS/OT). 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 podatnym systemie.

Poz.	Nazwa podatności	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odchylenie standardowe	Czas obserwacji
1	CVE-2023-36439	148	375	64	12,32%
2	CVE-2023-21529	135	457	77	86,84%
3	CVE-2022-41082	97	345	56	98,63%
4	CVE-2023-36745	88	126	21	17,80%
5	CVE-2021-27065	14	34	6	98,63%
6	CVE-2020-0688	14	32	5	98,63%
7	CVE-2021-26855	9	21	3	98,35%

Tabela 13: 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.

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.
- **Folder .git** - dostępny publicznie folder .git.

Poz.	Nazwa	Średnia dzienna liczba adresów IP	Dzienne maksimum adresów IP	Odchylenie standardowe	Czas obserwacji
1	Basic auth	8590	15913	1372	98,63%
2	Basic auth (IoT)	6574	9653	1031	96,98%
3	Roundcube CVE-2023-5631	538	759	79	17,80%
4	Folder .git	476	564	47	98,90%
5	Zimbra CVE-2022-37042	248	339	42	98,90%
6	VMware CVE-2019-5544	96	125	17	89,58%
7	Fortinet CVE-2022-42475	61	176	45	98,90%
8	Citrix CVE-2023-27898	54	111	23	80,82%
9	GeoServer CVE-2022-24816	48	66	8	84,65%
10	Fortinet CVE-2023-27997	37	143	22	55,06%
11	VMware CVE-2020-3992	15	24	2	87,12%
12	Joomla CVE-2023-23752	8	46	3	84,38%
13	Citrix CVE-2022-27510	6	15	3	54,52%
14	Citrix CVE-2023-4966	5	35	5	22,19%
15	VMware CVE-2021-21974	5	146	21	66,30%

Tabela 14: 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.

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. Zestawienia 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	191	259	21	98,63%
2	Codesys	151	227	20	98,90%
3	BACnet	88	121	11	98,90%
4	Modbus	81	117	11	98,90%
5	EtherNet/IP	59	73	8	98,90%
6	Fox	27	33	3	98,90%
7	OPC UA Binary	22	33	3	98,90%
8	Unitronics	19	28	6	8,21%
9	DNP3	11	26	3	98,90%
10	GE SRTP	8	14	1	98,35%
11	Omron FINS	8	15	2	98,35%
12	PC Worx	6	8	1	98,08%
13	IEC 60870-5-104	4	10	1	97,53%
14	MELSEC-Q	4	6	1	98,35%
15	ICCP	3	7	1	97,80%

Tabela 15: 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.

Szerokie statystyki

Obsługa zgłoszeń, incydentów i reagowanie na zagrożenia

W 2023 roku do CERT Polska wpłynęło 371 089 zgłoszeń. Po dokładnej weryfikacji, 210 360 z nich uznano za zgłoszenia dotyczące incydentów cyberbezpieczeństwa. Na ich podstawie zarejestrowano łącznie 80 267 unikalnych incydentów. Rok do roku CERT Polska rejestruje coraz większą liczbę incydentów, a w stosunku do roku ubiegłego odnotowano ponad stuprocentowy przyrost! (Tab. 16). Wzrost liczby zgłoszeń oraz rejestrowanych incydentów cyberbezpieczeństwa wynika m.in. z nieustannie zwiększającej się świadomości społeczeństwa na temat zagrożeń i roli zespołu CERT Polska. Od 2022 r. w telewizji, radiu i kinach emitowane są spoty w ramach kampanii społecznych informujących o potencjalnych zagrożeniach i sposobie ich zgłaszania do zespołu CERT Polska.

Zgłoszenia trafiają do nas poprzez:

- **Formularz na stronie** https://incydent.cert.pl/ – Zgłoś incydent,
- **Formularz na stronie** https://incydent.cert.pl/domena – Zgłoszenie złośliwej domeny,
- **SMS na numer 8080** - zgłoszenie szkodliwej wiadomości SMS,
- **Telefon na numer** +48 22 380 82 74,
- **E-mail:** cert@cert.pl,
- **Tradycyjną pocztę** na adres NASK-PIB.

Najczęstsze typy incydentów w 2023 r.

Phishing

Najpopularniejszym typem incydentów zarejestrowanych w 2023 r. były, tak jak niezmiennie od wielu lat, strony phishingowe. Zarejestrowano 41 423 tego typu incydenty, co stanowi aż 51,61 proc. wszystkich obsłużonych incydentów. To wzrost o ponad 61 pkt. proc. w porównaniu do roku ubiegłego. Najpopularniejszymi kampaniami phishingowymi były m.in. wykorzystujące wizerunek serwisu aukcyjnego Allegro – 11 161 przypadków, serwisu społecznościowego Facebook – 5 308 przypadków i serwisu sprzedażowego OLX – 4 753 przypadki.

Oszustwa komputerowe

Kolejnym popularnym typem incydentów były oszustwa komputerowe. Zarejestrowano ich 34 304, co stanowi ponad 42 proc. wszystkich zarejestrowanych incydentów. Wśród nich znajdą się m.in. fałszywe sklepy internetowe oraz popularne w ubiegłym roku oszustwa finansowe, podszywające się pod różnego rodzaju koncerny paliwowo-energetyczne, firmy oraz instytucje. Oszuści reklamując nieistniejący program dla akcjonariuszy indywidualnych, próbują wyłudzić od ofiar środki finansowe.

Szkodliwe oprogramowanie

Trzecim typem incydentów, które występowały najczęściej w 2023 r., było szkodliwe oprogramowanie. Zarejestrowano 1 650 przypadków, czyli o połowę mniej niż w poprzednim roku Obserwowane przez nas incydenty obejmowały zarówno infekcje oprogramowaniem ransomware, jak i kampanie spamowe dystrybuujące oprogramowanie Remcos i Agent Tesla. Przypomnijmy, że w 2022 r. incydentów szkodliwego oprogramowania zarejestrowano ponad 2 razy więcej - 3 409 przypadków.

Incydenty objęte krajową ustawą o systemie cyberbezpieczeństwa

CSIRT NASK w ramach ustawy o krajowym systemie cyberbezpieczeństwa w 2023 r. obsłużył 40 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 31 incydentów poważnych w sektorze bankowym oraz 9 w sektorze ochrony zdrowia

W 2023 r. CSIRT NASK obsłużył 2 184 incydenty dotyczące podmiotów publicznych. Najczęściej rejestrowanymi incydentami zaklasyfikowanymi jako incydenty w podmiocie publicznym były incydenty z sektora administracji publicznej – 1 206 incydentów, sektora oświaty i wychowania - 282 incydenty oraz sektora ochrony zdrowia - 231 incydentów.

Dokładne statystyki incydentów z podziałem na sektory gospodarki i rodzaje incydentów zawarte są w tabelach nr 17 i 18.

Historyczne porównanie liczby incydentów	Liczba incydentów
2023	80 267
2022	39 683
2021	29 483
2020	10 420
2019	6 484
2018	3 739
2017	3 182
2016	1 926
2015	1 456
2014	1 282
2013	1 219
2012	1 082
2011	605
2010	674
2009	1 292
2008	1 796
2007	2 108
2006	2 427
2005	2 516
2004	1 222
2003	1 196
2002	1 013
2001	741
2000	126
1999	105
1998	100
1997	75
1996	50

Tabela 16: Historyczne zestawienie liczby obsłużonych incydentów przez CERT Polska w latach 1996 – 2023.

Sektor gospodarki	Liczba incydentów	Procent wszystkich
Handel hurtowy i detaliczny	19 253	23,99%
Infrastruktura rynków finansowych	18 943	23,61%
Media	10 191	12,70%
Energetyka	9 196	11,46%
Poczta i usługi kurierskie	5 319	6,63%
Infrastruktura cyfrowa	5 101	6,35%
Bankowość	2 481	3,09%
Produkcja	2 353	2,93%
Administracja publiczna	2 234	2,78%
Osoby fizyczne	2 105	2,62%
Usługi inne	902	1,12%
Transport	492	0,61%
Inne	451	0,56%
Ochrona zdrowia	405	0,50%
Oświata i wychowanie	354	0,44%
Hotele, restauracje, catering	153	0,19%
Logistyka i dystrybucja	64	0,08%
Kultura i ochrona dziedzictwa narodowego	62	0,08%
Budownictwo i gospodarka nieruchomościami	61	0,08%
Działalność ubezpieczeniowa	47	0,06%
Rolnictwo	27	0,03%
Izby gospodarcze i handlowe	20	0,02%
Wodociągi	13	0,02%
Turystyka	13	0,02%
Gospodarka odpadami	10	0,01%
Kultura fizyczna	9	0,01%
Wyznania religijne i mniejszości narodowe	8	0,01%
Rybołówstwo	0	0,00%
Razem	80 278	100,00%

Tabela 17: Incydenty obsłużone przez CERT Polska w 2023 r. w podziale na sektor gospodarki

Typy incydentów	Liczba incydentów	Procent wszystkich
Oszustwa komputerowe	75 917	94,58%
Szkodliwe oprogramowanie	1 650	2,06%
Podatne usługi	964	1,20%
Obraźliwe i nielegalne treści	584	0,73%
Włamania	418	0,52%
Dostępność zasobów	385	0,48%
Próby włamań	205	0,26%
Atak na bezpieczeństwo informacji	59	0,07%
Inne	56	0,07%
Gromadzenie informacji	29	0,04%
Razem	80 267	100,00%

Tabela 18: Incydenty obsłużone przez CERT Polska w 2023 r. w podziale na kategorie wg taksonomii eCSIRT.net mkVI.

Spis rysunków

Spis tabel

Spis wykresów

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