Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 roku

CSIRT GOV

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 roku

Warszawa, sierpień 2021

ZESPÓŁ CSIRT GOV

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego, pełni rolę Zespołu CSIRT poziomu krajowego. Odpowiada on 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

dane kontaktowe
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 za rok 2020 publikowany jest przez Zespół CSIRT GOV w celu udostępnienia informacji w zakresie przede wszystkim danych statystycznych wraz z ich charakterystyką, dotyczących incydentów koordynowanych przez Zespół CSIRT GOV. Informacje zawarte w raporcie mają zwrócić uwagę jego odbiorcom na główne rodzaje zagrożeń rozpoznawanych corocznie przez Zespół CSIRT GOV, co tym samym powinno przyczyniać się do wsparcia procesów podnoszących poziom bezpieczeństwa systemów teleinformatycznych w instytucjach państwowych, administracji państwowej czy infrastrukturze krytycznej, jak również być przydatne dla szerokiego grona odbiorców.

Przedmiotowy raport powstał na podstawie danych, które zostały zanonimizowane, pochodzących m.in. ze zgłoszeń otrzymanych od podmiotów i osób zewnętrznych, zgłoszeń z systemów autonomicznych wykorzystywanych przez Zespół CSIRT GOV oraz systemu wczesnego ostrzegania o zagrożeniach teleinformatycznych ARAKIS 3.0 GOV, jak również ustaleń własnych.

W roku 2020 Zespół CSIRT GOV odnotował 246 107 zgłoszeń dotyczących potencjalnego wystąpienia incydentu teleinformatycznego, z czego 23 309 okazało się faktycznym incydentem. Obie, wskazane ilości są najwyższe w historii działania Zespołu i stanowią zauważalny wzrost w stosunku do roku poprzedniego.

W raporcie uwzględniono także informacje o kampaniach phishingowych - atakach wykorzystujących inżynierię społeczną, które znacznie nasiliły się w 2020 roku. Powyższy, narastający trend jest obserwowany już od 2019 roku i obecnie stanowi jeden z głównych wektorów ataków stosowanych przez cyberprzestępców.

Niniejszy raport zawiera ponadto syntetyczne informacje o prowadzonych, na mocy art. 32a ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu oraz Rozporządzenia Rady Ministrów z dnia 19 lipca 2016 r. w sprawie przeprowadzania oceny bezpieczeństwa związanej z zapobieganiem zdarzeniom o charakterze terrorystycznym, ocenach bezpieczeństwa systemów teleinformatycznych instytucji administracji rządowej oraz infrastruktury krytycznej, mających na celu identyfikację istotnych podatności wpływających na bezpieczeństwo infrastruktury teleinformatycznej wskazanych powyżej podmiotów.

Dodatkowo, w raporcie zostały opublikowane informacje o udziale przedstawicieli CSIRT GOV w ćwiczeniach dot. cyberbezpieczeństwa, które z uwagi na sytuację pandemiczną były organizowane w 2020 roku w znacznie mniejszym zakresie, przede wszystkim w formie ćwiczeń zdalnych. Pomimo tych okoliczności CSIRT GOV debiutował w organizowanych przez południowokoreański instytut badawczy National Security Research Institute ćwiczeniach Cyber Conflict Exercises 2020 oraz pierwszych Międzysektorowych Ćwiczeniach Cyberbezpieczeństwa KSC-EXE 2020.

Przedmiotowy raport zawiera również krótką statystykę z realizowanego przez operatorów usług kluczowych oraz podmiotów publicznych obowiązku, zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa, wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, co umożliwia sprawną obsługę zgłoszeń dotyczących incydentów, jak i pozwala na otrzymywanie stosownych ostrzeżeń o zagrożeniach.

Ponadto, w niniejszym raporcie przedstawiono rekomendacje dotyczące bezpieczeństwa pracy zdalnej. Biorąc pod uwagę panującą w 2020 roku sytuację pandemiczną i wynikające z niej restrykcje, wiele podmiotów i instytucji rozpoczęło działania w trybie pracy zdalnej, co stworzyło szerokie pole do prowadzenia szkodliwych działań przez cyberprzestępców.

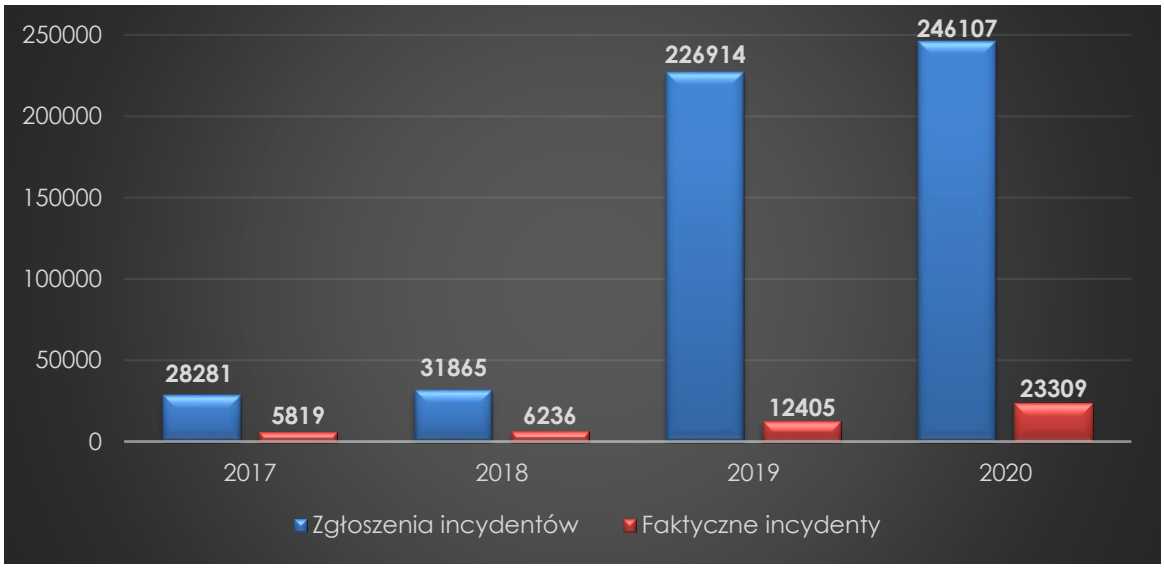
Reasumując, coroczna publikacja raportu o stanie bezpieczeństwa cyberprzestrzeni RP, ma przede wszystkim na celu podnoszenie świadomości użytkowników o zagrożeniach i podatnościach ukierunkowanych na osiągnięcie minimalnego, akceptowalnego poziomu bezpieczeństwa systemów teleinformatycznych oraz na podjęcie decyzji o wdrożeniu odpowiednich działań ograniczających możliwość eskalacji wystąpienia ewentualnego zagrożenia.

1. STATYSTYKI INCYDENTÓW KOORDYNOWANYCH PRZEZ ZESPÓŁ CSIRT GOV

1.1. Dane w ujęciu całościowym

Zgodnie z art. 26 ust. 7 ustawy o krajowym systemie cyberbezpieczeństwa do zadań Zespołu CSIRT GOV należy koordynacja obsługi incydentów zgłaszanych przez zobowiązanych w tym zakresie uczestników krajowego systemu cyberbezpieczeństwa, do których należą m.in. administracja rządowa oraz operatorzy infrastruktury krytycznej.

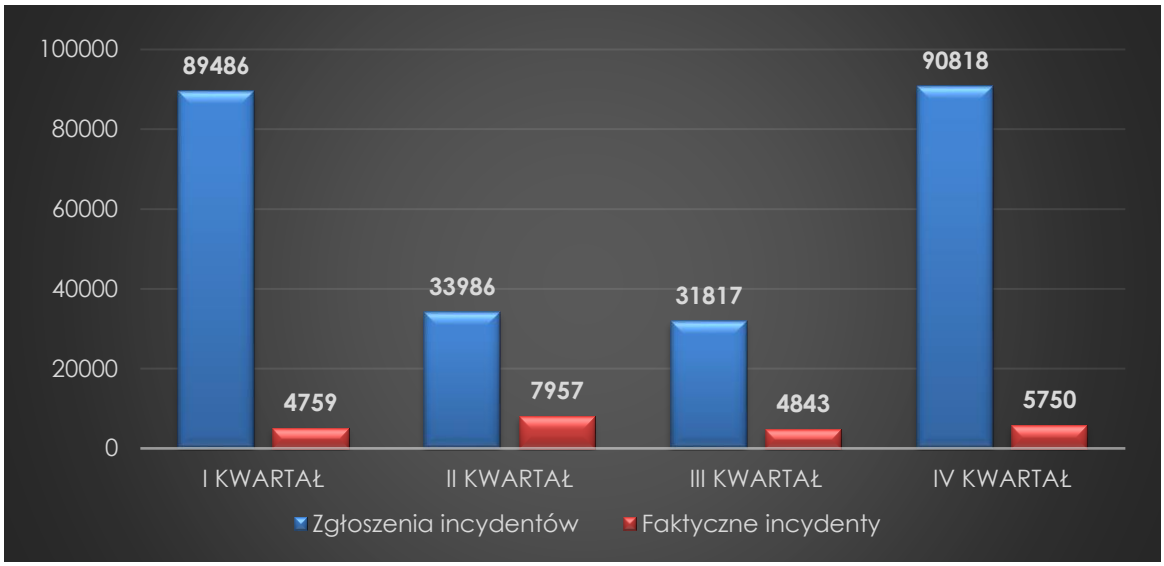
W roku 2020 Zespół CSIRT GOV odnotował 246 107 zgłoszeń, które zostały zakwalifikowane jako zdarzenia dotyczące potencjalnego wystąpienia incydentu teleinformatycznego w ramach obszaru kompetencyjnego Zespołu. Obserwowana wysoka ilość zgłoszeń jest wynikiem przede wszystkim wejścia w życie przepisów ustawy o krajowym systemie cyberbezpieczeństwa, tym samym w latach 2019 - 2020 nastąpił zauważalny wzrost ilości zgłoszeń przesyłanych do CSIRT GOV w stosunku do wcześniejszych okresów sprawozdawczych. Jednocześnie, czynnikiem oddziaływującym na wskazaną tendencję, był wzrost ilości zgłoszeń rejestrowanych przez systemy wykrywania oraz ostrzegania przed zagrożeniami dotyczącymi systemów teleinformatycznych instytucji, podmiotów czy organów państwa znajdujących się w kompetencji Zespołu CSIRT GOV, co było podyktowane skalą cyberzagrożeń obecnych w cyberprzestrzeni RP.



Wykres 1 - Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych latach

Liczba zdarzeń, które zostały zarejestrowane w roku 2020 jako faktyczny incydent, wyniosła w sumie 23 309, co stanowi wzrost o około 88% w stosunku do roku 2019 przy wzroście ilości zgłoszeń tylko na poziomie około 8%. W perspektywie lat 2019–2020 został utrzymany trend wskazujący na podwajanie ilości incydentów w relacji rok do roku (Wykres 1).

Analiza poszczególnych kwartałów roku 2020 wskazuje natomiast, że najwięcej zgłoszeń, oscylujących wokół liczby 90 tysięcy, przypadło na kwartały I oraz IV, stanowiąc prawie trzykrotny wzrost ilości zgłoszeń w porównaniu do pozostałych kwartałów 2020 roku. Zależność ta wynika przede wszystkim z alarmów systemu ARAKIS GOV, których liczba we wskazanych okresach wzrosła ze względu na wykryte aktywne skanowania adresacji sieciowych należących do instytucji administracji państwowej i operatorów infrastruktury krytycznej. Dodatkowym czynnikiem kształtującym wskazaną statystykę w IV kwartale 2020 roku był zwiększony poziom detekcji zagrożeń związany z rozwojem możliwości systemu wczesnego ostrzegania, działającego w infrastrukturze podmiotów krajowego systemu cyberbezpieczeństwa.

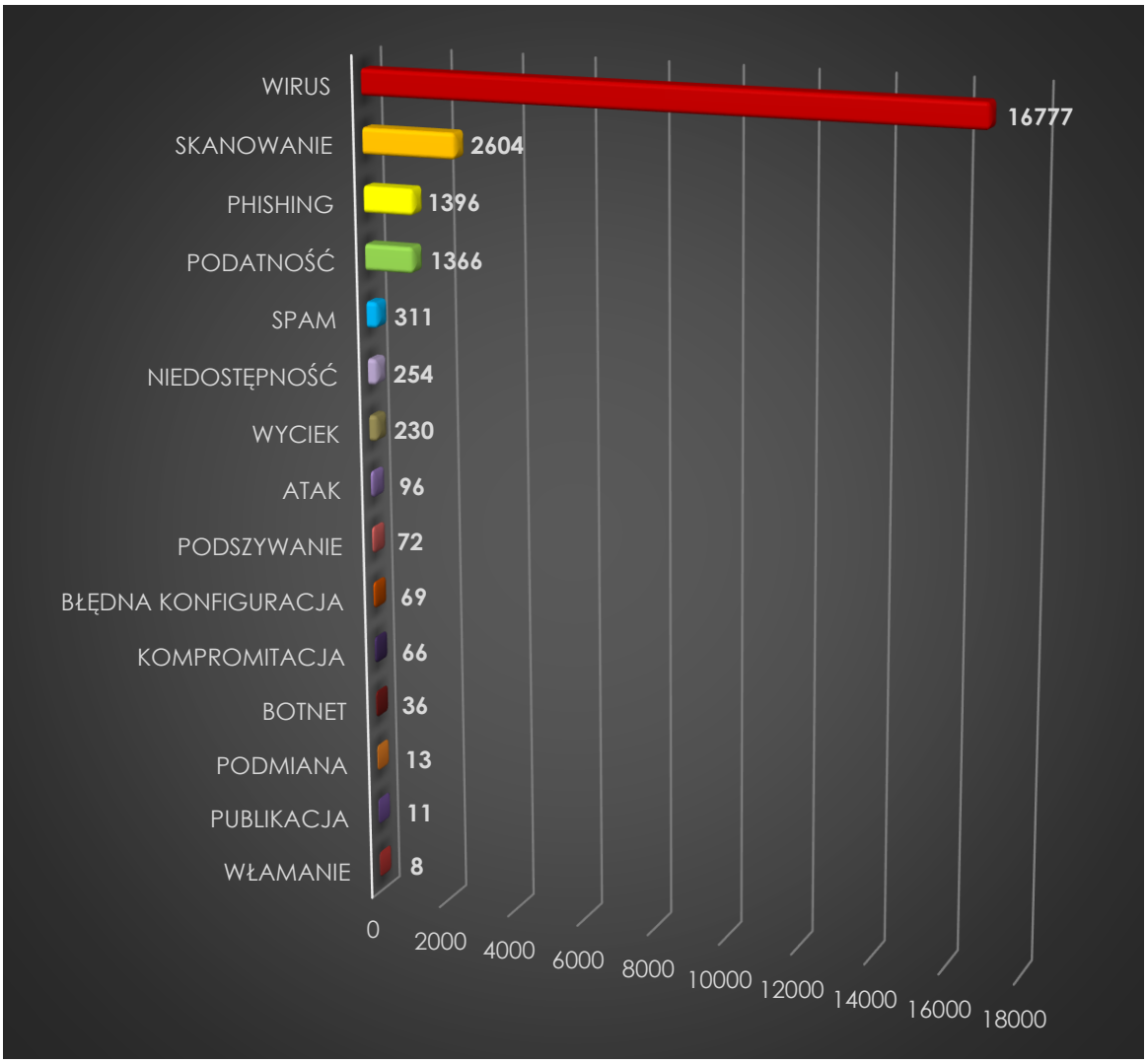


Wykres 2 - Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych kwartałach 2020 roku

Największa liczba faktycznych incydentów została zarejestrowana w II kwartale 2020 roku, przy relatywnie małej ilości zgłoszeń. Wzrost ilości faktycznych incydentów w tym kwartale był prawdopodobnie spowodowany efektem tzw. lockdown-u w związku z epidemią COVID-19.

Różnica pomiędzy liczbą zarejestrowanych zgłoszeń a faktyczną liczbą incydentów wynika z faktu, iż część ze zgłoszeń stanowią tzw. false-positive, czyli błędnie wskazujące na wystąpienie zagrożenia. Są to najczęściej przypadki niewłaściwej interpretacji przez zgłaszającego prawidłowego ruchu sieciowego. Kolejną przyczyną powodującą różnice odnośnie przedmiotowych danych są wielokrotne zgłoszenia dotyczące tych samych incydentów. Jest to zauważalne przede wszystkim w przypadku korzystania z systemów zautomatyzowanych, takich jak N6 czy ARAKIS 3.0 GOV. Ponadto zgłoszenia pochodzące z systemów automatycznych zostają poddane późniejszej weryfikacji przez Zespół CSIRT GOV, który wskazuje, czy zgłoszenia można zaklasyfikować jako faktyczne incydenty.

Mając na względzie rodzaje zarejestrowanych incydentów przez Zespół CSIRT GOV w roku 2020, w dalszej części niniejszego raportu zaprezentowany został wykres przedstawiający podział incydentów według zidentyfikowanych kategorii.



Wykres 3 - Statystyka incydentów w roku 2020 z podziałem na kategorie (skala liniowa)

W roku 2020, podobnie jak i w 2019, najwięcej incydentów zostało sklasyfikowanych wśród trzech następujących kategorii: WIRUS, SKANOWANIE, PHISHING.

Kategoria WIRUS, jako najliczniejsza, stanowiła prawie 72% ogółu wszystkich incydentów. Ilość incydentów w tej kategorii związana jest przede wszystkim ze zwiększeniem się skuteczności identyfikacji oprogramowania złośliwego w oparciu o systemy detekcji, sygnatury oraz przepływy sieciowe. W tym zakresie należy wskazać na powiadomienia systemu ARAKIS 3.0 GOV. Dotyczą one alarmów, które mogą świadczyć o infekcji stacji roboczej w instytucji administracji państwowej lub u operatora infrastruktury krytycznej. Liczba incydentów typu WIRUS rośnie gwałtownie na przestrzeni ostatnich lat. W stosunku do roku 2019 można zaobserwować wzrost o ponad 132%[1].

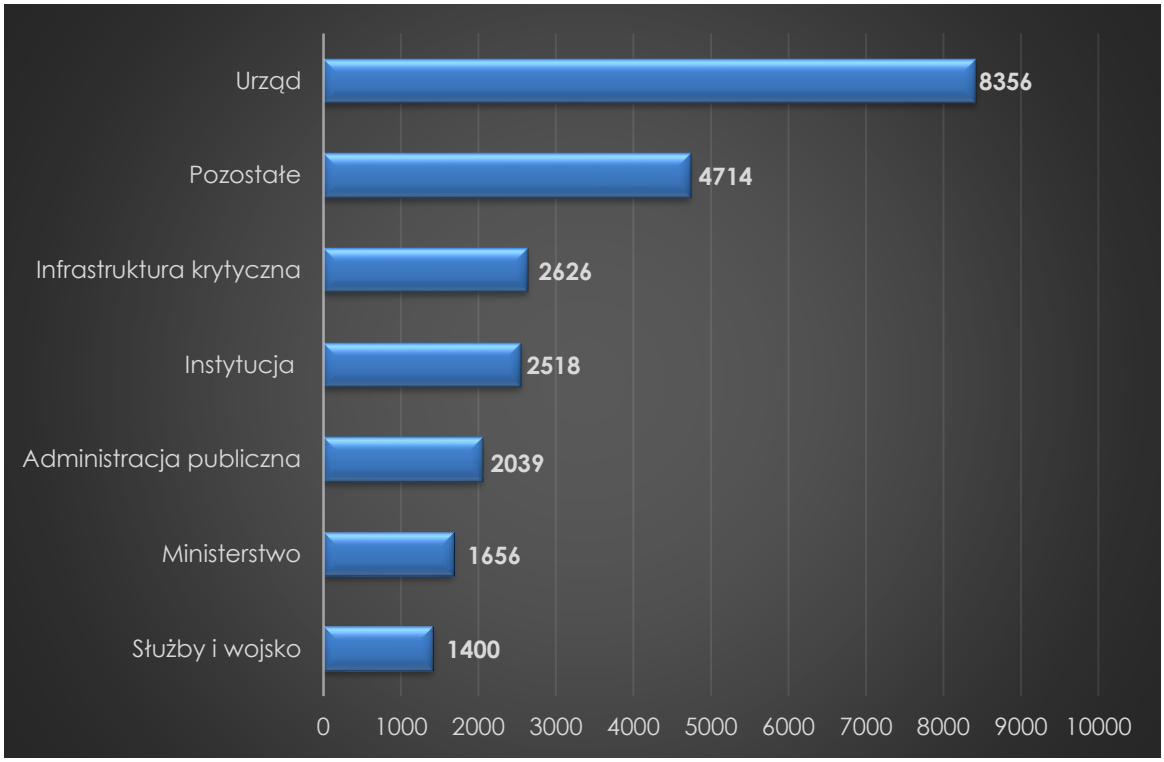
Drugą pod względem liczności grupą są incydenty zaklasyfikowane jako SKANOWANIE. Wynikają one także z alarmów ARAKIS 3.0 GOV i dotyczą złośliwego lub podejrzanego ruchu skierowanego na adresację podmiotów podległych CSIRT GOV. W przypadku kategorii SKANOWANIE utrzymuje się wyraźna tendencja wzrostowa, przy czym w ubiegłym roku tego typu incydentów było prawie 39% więcej niż w roku 2019[2].

Jednym z istotniejszych rodzajów zagrożeń są także kampanie phishingowe. Pomimo tego, że opierają się one na stosowaniu metod socjotechniki, stanowią realne zagrożenie dla bezpieczeństwa systemów teleinformatycznych i mogą również stanowić fazę inicjującą bardziej rozległy atak, pozwalający na uzyskanie dostępu do infrastruktury teleinformatycznej danego podmiotu. Wzrost zarejestrowanych incydentów dotyczących kategorii PHISHING wynosi prawie 19% w porównaniu z rokiem 2019[3].

Kolejnym zagrożeniem, które godzi w bezpieczeństwo teleinformatyczne, są podatności w zasobach IT rozumianych jako słabość systemu teleinformatycznego, wynikająca z błędów konfiguracyjnych lub braku odpowiedniej polityki bezpieczeństwa, związanej z aktualizacją oraz weryfikacją poprawnie wdrożonych rozwiązań teleinformatycznych.

[1]W kategorii WIRUS w 2019 r. zarejestrowano 7 219 incydentów, podczas gdy w 2020 r. odnotowano 16 777 incydentów.
[2]W kategorii SKANOWANIE w 2019 r. zarejestrowano 1 878 incydentów, podczas gdy w 2020 r. odnotowano 2 604 incydentów.
[3]W kategorii PHISHING w 2019 r. zarejestrowano 1 178 incydentów, podczas gdy w 2020 r. odnotowano 1 396 incydentów.

Również w tym wypadku można zaobserwować wzrost liczby incydentów w kategorii PODATNOŚĆ o ponad 34% w stosunku do roku 2019[4].

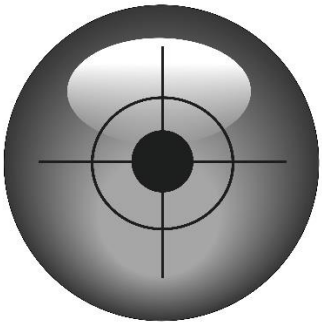


Wykres 4 - Statystyka wybranych incydentów w 2020 roku z podziałem na instytucje

Biorąc pod uwagę rozkład incydentów na poszczególne sektory, największą grupę w 2020 roku stanowiły incydenty dotyczące urzędów państwowych – 8 356 incydentów. Istotne kierunki zagrożeń zostały także wykryte w ramach infrastruktury krytycznej oraz instytucji publicznych. W roku 2020 zaobserwować również można istotny przyrost w stosunku do roku 2019 liczby incydentów dotyczących urzędów państwowych (prawie 118%)[5], infrastruktury krytycznej (około 283%)[6] oraz służb i wojska (prawie 311%)[7].

[4]W kategorii PODATNOŚĆ w 2019 r. zarejestrowano 1 016 incydentów, podczas gdy w 2020 r. odnotowano 1366 incydentów.
[5]W zakresie urzędów państwowych, w 2019 r. zarejestrowano 3 837 incydentów, podczas gdy w 2020 r. odnotowano 8 356 incydentów.
[6]W zakresie infrastruktury krytycznej, w 2019 r. zarejestrowano 685 incydentów, podczas gdy w 2020 r. odnotowano 2 626 incydentów.
[7]W zakresie służb i wojska, w 2019 r. zarejestrowano 341 incydentów, podczas gdy w 2020 r. odnotowano 1 400 incydentów.

2.CHARAKTERYSTYKA WYBRANYCH ZAGROŻEŃ



2.1 Zagrożenie SOLAR WINDS

W grudniu 2020 roku, Zespół CSIRT GOV uzyskał informacje o kompromitacji łańcucha dostaw oprogramowania SolarWinds Orion Platform, który w wersjach produktu od 2019.4 HF 5 do 2020.2.1 HF 1 posiadał zaimplementowany złośliwy kod - backdoor SUNBURST, który umożliwiał m.in. nieautoryzowane przesyłanie i wykonywanie dowolnych plików, zbieranie informacji o systemie, ponowne uruchamianie stacji roboczej, wyłączanie usług systemowych, jak również dostęp do zasobów sieci zaatakowanej organizacji. Oprogramowanie złośliwe wykorzystywało m.in. protokół komunikacyjny *Orion Improvement Program* (OIP), w celu ukrycia ruchu wśród normalnej aktywności sieciowej oprogramowania SolarWinds. Ryzyko płynące z tego typu zagrożenia dotyczyło wielu tysięcy przedsiębiorstw wykorzystujących ww. produkt na całym świecie. Skuteczność kampanii związana była z kompromitacją łańcucha dostaw aktualizacji pobieranych z serwerów producenta platformy SolarWinds Orion, które zawierały nieznany wcześniej backdoor. Implant posiadał mechanizm oczekiwania w trybie uśpienia, trwającym nawet do dwóch tygodni, po którym próbował m.in. rozwiązywać subdomeny „avsvmcloud[.]com" z wykorzystaniem algorytmu generowania domen (DGA). Dodatkowo, w ataku wykorzystywane było oprogramowanie złośliwe typu dropper „TEARDROP", które to natomiast korzystało z biblioteki znajdującej się pod ścieżką:

'C:\WINDOWS\SysWOW64\netsetupsvc[.]dll'.

W ramach działań mitygujących powyższe zagrożenia, Zespół CSIRT GOV przesłał ostrzeżenia do podmiotów wchodzących w zakres kompetencyjny CSIRT GOV dot. zidentyfikowanego zagrożenia wraz ze wskaźnikami kompromitacji, jak również wersjami oprogramowania, które zostały skompromitowane.

2.2 Zidentyfikowane grupy APT w 2020 roku

APT Kimsuky- VelvetChollima

Kampania Kimsuky została wykryta jako ataki ukierunkowane na polskie instytucje rządowe oraz podmioty prowadzące działania w ramach Organizacji Narodów Zjednoczonych. W atakach wykorzystywano „spearphishing", a wiadomości zawierające pliki ze złośliwym oprogramowaniem kierowane były do ściśle określonych osób, np. pracujących w departamentach związanych z kontaktami międzynarodowymi. Grupa typowała odbiorców na podstawie wpisów ze stron WWW, LinkedIn, GoldenLine, Facebook i innych portali. Ataki miały na celu pozyskanie informacji powszechnie niedostępnych, jak również uzyskanie dostępu do skrzynek poczty elektronicznej.

APT Gamaredon (Primitive Bear)

APT Gamaredon dotyczyła polskich placówek dyplomatycznych oraz innych polskich instytucji funkcjonujących na terenie Ukrainy. Ataki były poprzedzone rozpoznaniem, a końcowe złośliwe oprogramowanie przesyłano jedynie na wybrane hosty. Na podstawie analiz przeprowadzonych ataków zaobserwowano wykorzystanie wyspecjalizowanego złośliwego oprogramowania.

APT 41 (Wicked Panda) - ZOHO CVE-2020-10189

Zidentyfikowano ataki z wykorzystaniem podatności typu 0-day, pozwalającej na zdalne wykonanie kodu w oprogramowaniu „ZohoManageEngineDesktopCentral". Podatność została sklasyfikowana pod numerem CVE-2020-10189.

APT 36 (Mythic Leopard)

Zarejestrowano ataki wymierzone w polskie ministerstwa z wykorzystaniem przejętej wcześniej przez grupę APT 36 infrastruktury rządowej innych państw. Zidentyfikowano złośliwe oprogramowanie, które było zmodyfikowaną wersją oprogramowania RAT o nazwie Quasar.

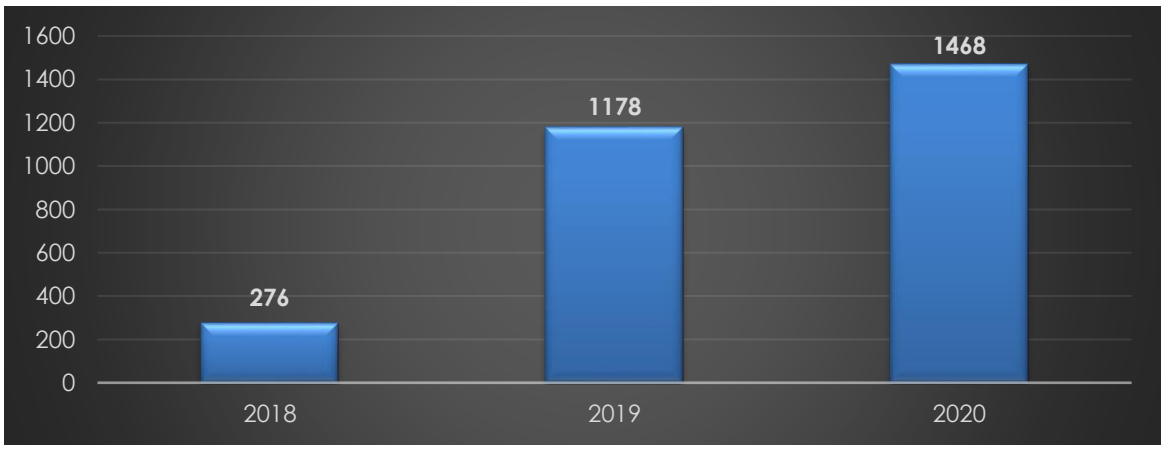
APT Turla (Venomous Bear)

Zidentyfikowano zaawansowane ataki wymierzone w instytucje rządowe z wykorzystaniem autorskiego oprogramowania oraz mało popularnych exploitów. Podejmowane przez grupę działania ukierunkowane były na pozyskanie informacji powszechnie niedostępnych.

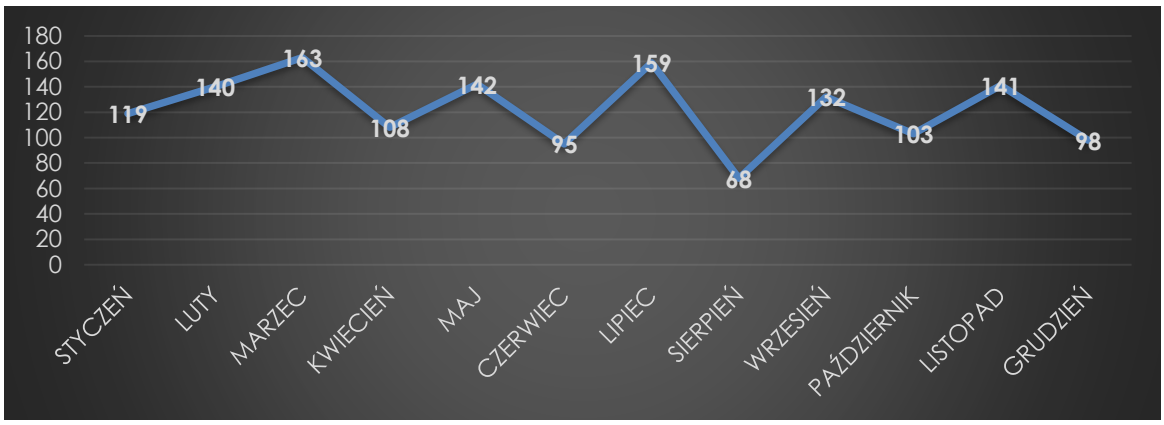
3. PHISHING

3.1 Inżynieria społeczna – trend ogólny

W 2020 roku Zespół CSIRT GOV zarejestrował 1468 incydentów typu inżynieria społeczna, w tym 1396 z kategorii PHISHING i 72 z kategorii PODSZYWANIE. Tym samym odnotowany został wzrost liczby incydentów o około 24% względem roku poprzedniego. Poniżej przedstawiony został wykres porównujący sumę incydentów typu inżynieria społeczna w ostatnich 3 latach, a także wykres zarejestrowanych w 2020 roku zgłoszeń w ujęciu miesięcznym.



Wykres 5 - Liczba zgłoszeń z kategorii PHISHING oraz PODSZYWANIE



Wykres 6 - Liczba zgłoszeń z kategorii PHISHING oraz PODSZYWANIE z podziałem na miesiące

Zaprezentowane dane wskazują, iż w 2020 roku nastąpił wzrost liczby kampanii phishingowych względem 2019 roku. W ujęciu miesięcznym największa aktywność kampanii phishingowych przypadła na marzec oraz lipiec 2020 roku. Jednocześnie zauważalna była prawidłowość comiesięcznego naprzemiennego wzrostu i spadku aktywności.

W okresie objętym raportem najczęściej występującą kampanią phishingową były wiadomości e-mail podszywające się pod dział helpdesk lub administratorów oraz wykorzystujące logo i emblematy instytucji administracji publicznej lub operatorów infrastruktury krytycznej, aby dodatkowo uwiarygodnić korespondencję. Treść wiadomości miała zachęcić odbiorcę do otworzenia zawartego w niej odnośnika i wprowadzenia danych logowania do poczty elektronicznej. Można zatem słusznie wnioskować, że głównym celem tych kampanii było pozyskanie danych uwierzytelniających do skrzynek administracji publicznej i przejęcie zawartych w nich informacji.

Administracja publiczna stała się również celem kampanii phishingowych zakrojonych na szeroką skalę w sieci Internet, w których wykorzystywano wizerunek m.in. firm kurierskich takich jak Poczta Polska, InPost, a także operatorów telekomunikacyjnych Orange i Play. Celem tych ataków najczęściej była próba infekcji złośliwym oprogramowaniem lub pozyskanie danych autoryzacyjnych do serwisów bankowości elektronicznej i wykradanie środków finansowych. Wiadomości tego typu zawierały informacje dotyczące rzekomych przesyłek pocztowych oraz link, pod którym można było uiścić dopłatę do przesyłki. W innych przypadkach treść korespondencji nawiązywała do konieczności opłacenia faktury za usługi telekomunikacyjne. W tej formie wiadomość zawierała zwykle załącznik imitujący plik PDF z fakturą, która okazywała się najczęściej formatem XLS oraz XLSM zawierającym złośliwe makro.

Dodać należy, iż w 2020 roku sytuacja epidemiczna na świecie i w kraju miała swoje przełożenie w cyberprzestrzeni, co widać m.in. na przykładzie stosownych kampanii phishingowych. Duży wzrost kampanii przypadający na marzec może mieć właśnie związek z pandemią COVID-19, gdyż to w tym miesiącu przyszło się zmierzyć z nową sytuacją epidemiczną w Polsce, co równocześnie pozwoliło atakującym na wykorzystanie motywu podszywania się pod instytucje, np. Światową Organizację Zdrowia, jak również wykorzystywania scenariuszy wskazujących na sprzedaż maseczek i środków do dezynfekcji, czy pobierania opłat za dezynfekcję paczki.

3.2 Kampanie phishingowe w 2020 roku

Helpdesk/administrator poczty

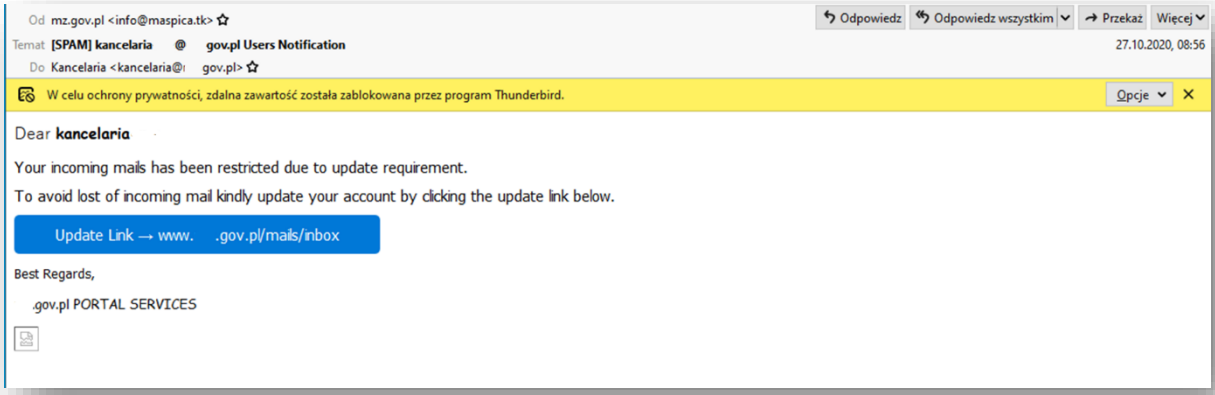
Jednym z najczęściej wykorzystywanych motywów kampanii phishingowych były wiadomości e-mail podszywające się pod helpdesk lub administratorów poczty, których celem było nakłonienie odbiorcy do otworzenia linku zawartego w treści i wprowadzenie danych logowania do skrzynki pocztowej. Nadawca wiadomości sugerował konieczność potwierdzenia danych pod pretekstem unieważnienia dostępu do poczty elektronicznej. W rzeczywistości dochodziło do kompromitacji skrzynki, a potencjalnie nawet do całkowitej utraty dostępu. Najczęstszymi tematami wiadomości były następujące sformułowania: „Actionrequired", „Users Notification" czy „OSTRZEŻENIE ADMINISTRATORA!!!" (pisownia oryginalna).

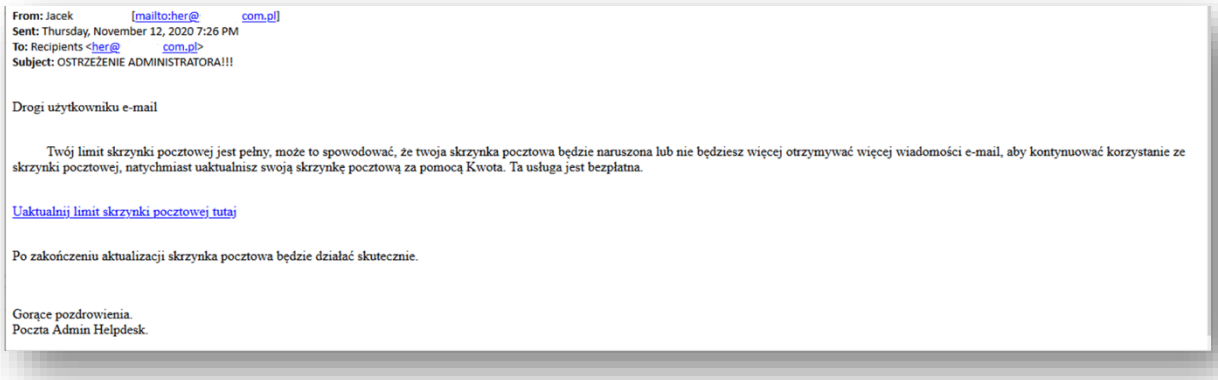
W treści wiadomości znajdował się komunikat w języku angielskim lub polskim informujący o zapełnieniu limitu skrzynki pocztowej i konieczności jej aktualizacji, ponieważ w przeciwnym wypadku użytkownik straci możliwość dostępu do poczty oraz odbierania i wysyłania wiadomości. Ze względu na treść i formę ułożenia zdań, a także brak polskich znaków można wyciągnąć wniosek, iż wiadomości wysyłane w języku polskim były tłumaczone z innego języka, co wskazuje na aspekt międzynarodowy kampanii. W niektórych wiadomościach znajdował się formularz, który należało uzupełnić o takie wartości jak nazwa użytkownika, hasło, adres e-mail czy numer telefonu. W niektórych kampaniach odnośniki przenosiły do strony, gdzie dla uwiarygodnienia prawdziwości korespondencji wyświetlane były logo i emblematy danej instytucji. Skrypt strony był przygotowany w taki sposób, aby w zależności od domeny instytucji zaszytej w adresie URL zmieniać grafikę na odpowiednią dla każdego podmiotu.

Wiadomości były wysyłane m.in. z adresów w domenach:

- servicebuero-wismar.de;
- nchbd.com;
- bata.co.id;
- cupid.or.jp.

Poniżej przedstawione zostały przykładowe wiadomości:





From: Jacek [mailto:her@ com.pl]
Sent: Thursday, November 12, 2020 7:26 PM
To: Recipients <her@ com.pl>
Subject: OSTRZEŻENIE ADMINISTRATORA!!!

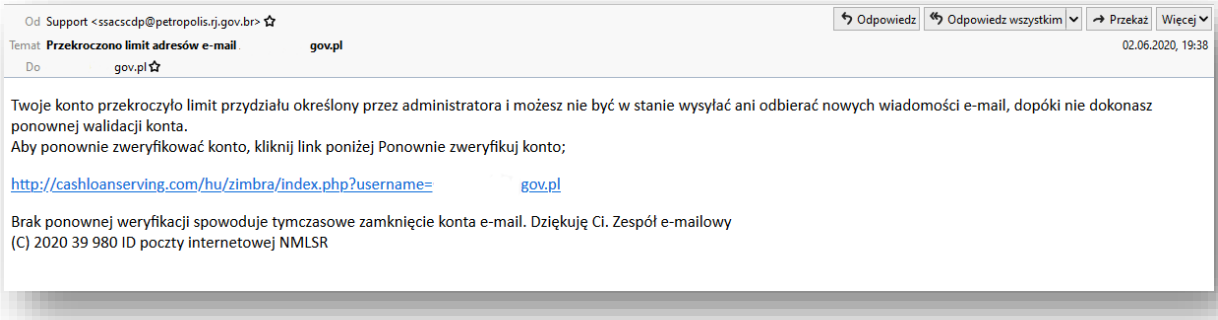
Drogi użytkowniku e-mail

Twój limit skrzynki pocztowej jest pełny, może to spowodować, że twoja skrzynka pocztowa będzie naruszona lub nie będziesz więcej otrzymywać więcej wiadomości e-mail, aby kontynuować korzystanie ze skrzynki pocztowej, natychmiast uaktualnisz swoją skrzynkę pocztową za pomocą Kwota. Ta usługa jest bezpłatna.

Uaktualnij limit skrzynki pocztowej tutaj

Po zakończeniu aktualizacji skrzynka pocztowa będzie działać skutecznie.

Gorące pozdrowienia.
Poczta Admin Helpdesk.



Od Support <ssacscdp@petropolis.rj.gov.br>
Temat **Przekroczono limit adresów e-mail** **gov.pl**
Do gov.pl

Odpowiedz | Odpowiedz wszystkim | Przekaż | Więcej
02.06.2020, 19:38

Twoje konto przekroczyło limit przydziału określony przez administratora i możesz nie być w stanie wysyłać ani odbierać nowych wiadomości e-mail, dopóki nie dokonasz ponownej walidacji konta.
Aby ponownie zweryfikować konto, kliknij link poniżej Ponownie zweryfikuj konto;

http://cashloanserving.com/hu/zimbra/index.php?username= gov.pl

Brak ponownej weryfikacji spowoduje tymczasowe zamknięcie konta e-mail. Dziękuję Ci. Zespół e-mailowy
(C) 2020 39 980 ID poczty internetowej NMLSR

Na podstawie powyższych informacji można wskazać, iż zaprezentowany typ ataku wykorzystujący motyw zablokowania poczty/wykorzystania wolnej przestrzeni na dysku był jedną z najczęstszych kampanii ukierunkowanych na administrację publiczną w 2020 roku. Panel logowania z oficjalną grafiką instytucji wskazuje, że była to kampania przygotowana z myślą o konkretnych podmiotach, do których została wysłana wiadomość, a nie kolejna ogólna akcja zakrojona na szeroką skalę w sieci Internet. Warto jednak nadmienić, że przygotowana kampania nie została dopracowana ze szczegółami, o czym świadczą wykorzystane adresy e-mail. W niektórych przypadkach wyświetlana była nazwa konta „postmaster" lub „backoffice" oraz „info", co mogłoby sugerować kontakt ze strony administratorów czy helpdesku, jednak prawie wszystkie adresy były w charakterystycznych domenach zagranicznych, które mogły budzić wątpliwość u odbiorców co do prawdziwości wiadomości.

Faktury

Motyw nieopłaconych faktur rozsyłanych w wiadomościach elektronicznych stanowi trend aktualny od kilku lat i jest często wykorzystywany z uwagi na powszechność tego typu korespondencji elektronicznej. Regularnie pojawiają się kampanie, w których atakujący podszywają się pod operatorów telekomunikacyjnych znanych sieci komórkowych takich jak Orange czy Play i pod pretekstem wystawienia nowej faktury za usługi próbują dokonać infekcji komputera użytkownika, który otworzy plik z fakturą.

Tytuły przesyłanych wiadomości miały nie wzbudzać podejrzeń i odnosić się bezpośrednio do przyczyny kontaktu, dlatego atakujący używali takich sformułowań jak (pisownia oryginalna):

- E-faktura Orange;
- E-faktura 05.2020;
- e-faktura Play24;
- Play faktura do pobrania.

Wyświetlana nazwa nadawcy nawiązywała do treści wiadomości, dlatego odbiorca mógł przeczytać, że wiadomość została wysłana przez operatora Orange lub Play, jednak rzeczywistymi nadawcami korespondencji były m.in. adresy z domen:

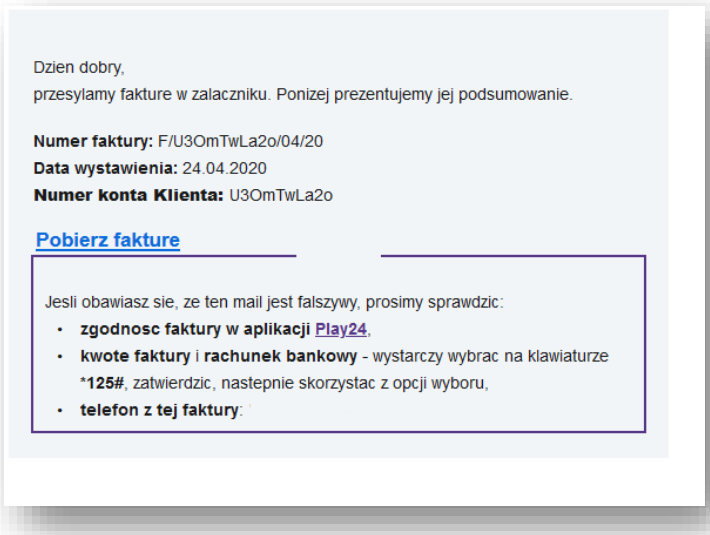
- gmx.com;
- o2.pl;
- onet.eu;
- wp.pl;
- interia.pl;
- mail.com.

Wykorzystanie adresów poczty elektronicznej w polskich serwisach może świadczyć o kompromitacji skrzynek albo o polskim pochodzeniu atakujących.

W związku z tym, iż treść wiadomości odwzorowywała rzeczywisty wygląd

prawdziwej korespondencji z wystawionymi fakturami wysyłanymi przez operatorów, a jednocześnie w fałszywej korespondencji brakowało polskich znaków, można sformułować wniosek, że kampania prowadzona była z wykorzystaniem przejętych skrzynek pocztowych.

Poniżej przedstawione zostały przykładowe wiadomości z opisanej kampanii:

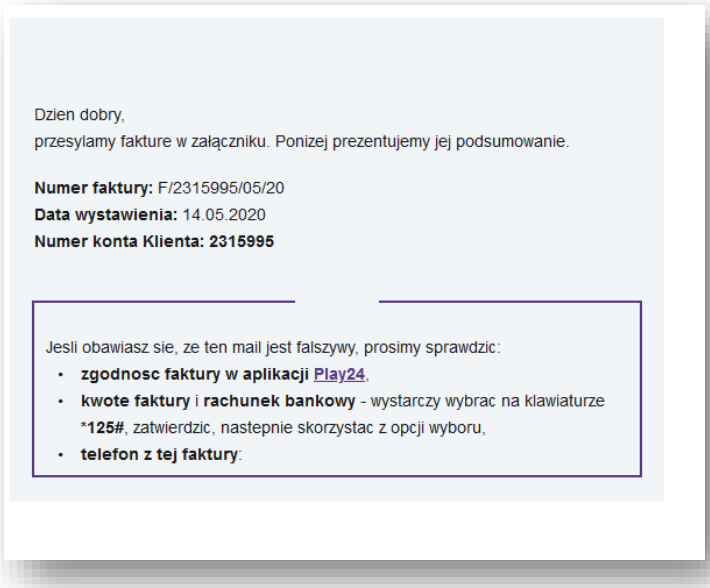


Dzien dobry,
przesylamy fakture w zalaczniku. Ponizej prezentujemy jej podsumowanie.

Numer faktury: F/U3OmTwLa2o/04/20
Data wystawienia: 24.04.2020
Numer konta Klienta: U3OmTwLa2o

Pobierz fakture

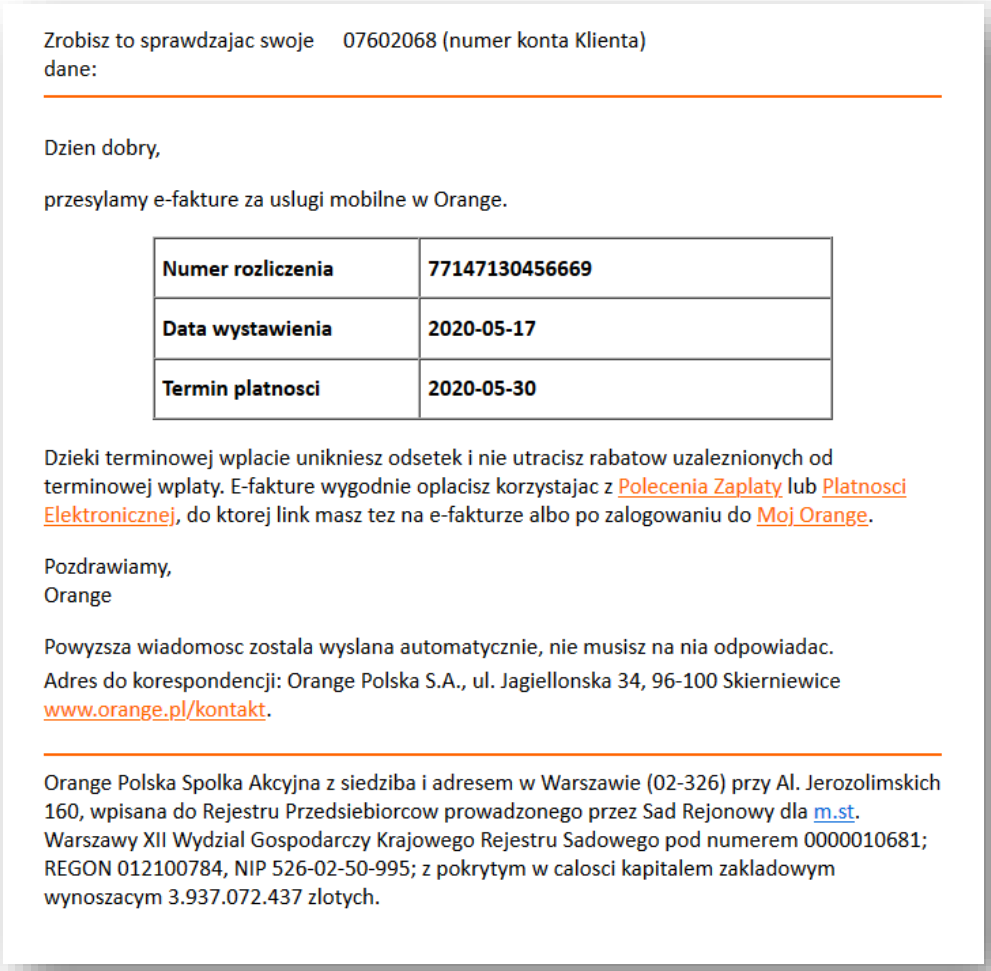
Jesli obawiasz sie, ze ten mail jest falszywy, prosimy sprawdzic:
- **zgodnosc faktury w aplikacji Play24**,
- **kwote faktury** i **rachunek bankowy** - wystarczy wybrac na klawiaturze *125#, zatwierdzic, nastepnie skorzystac z opcji wyboru,
- **telefon z tej faktury**:



Dzien dobry,
przesylamy fakture w załączniku. Ponizej prezentujemy jej podsumowanie.

Numer faktury: F/2315995/05/20
Data wystawienia: 14.05.2020
Numer konta Klienta: 2315995

Jesli obawiasz sie, ze ten mail jest falszywy, prosimy sprawdzic:
- **zgodnosc faktury w aplikacji Play24**,
- **kwote faktury** i **rachunek bankowy** - wystarczy wybrac na klawiaturze *125#, zatwierdzic, nastepnie skorzystac z opcji wyboru,
- **telefon z tej faktury**:



Zrobisz to sprawdzajac swoje dane: 07602068 (numer konta Klienta)

Dzien dobry,

przesylamy e-fakture za uslugi mobilne w Orange.

Numer rozliczenia	**77147130456669**
Data wystawienia	**2020-05-17**
Termin platnosci	**2020-05-30**

Dzieki terminowej wplacie unikniesz odsetek i nie utracisz rabatow uzaleznionych od terminowej wplaty. E-fakture wygodnie oplacisz korzystajac z Polecenia Zaplaty lub Platnosci Elektronicznej, do ktorej link masz tez na e-fakturze albo po zalogowaniu do Moj Orange.

Pozdrawiamy,
Orange

Powyzsza wiadomosc zostala wyslana automatycznie, nie musisz na nia odpowiadac.
Adres do korespondencji: Orange Polska S.A., ul. Jagiellonska 34, 96-100 Skierniewice www.orange.pl/kontakt.

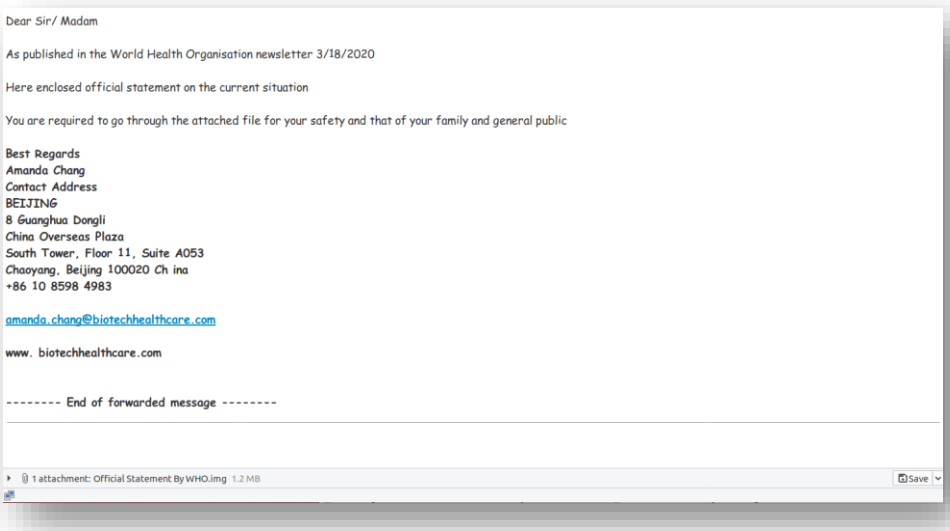
Orange Polska Spolka Akcyjna z siedziba i adresem w Warszawie (02-326) przy Al. Jerozolimskich 160, wpisana do Rejestru Przedsiebiorcow prowadzonego przez Sad Rejonowy dla m.st. Warszawy XII Wydzial Gospodarczy Krajowego Rejestru Sadowego pod numerem 0000010681; REGON 012100784, NIP 526-02-50-995; z pokrytym w calosci kapitalem zakladowym wynoszacym 3.937.072.437 zlotych.

Cechą charakterystyczną dla powyższych kampanii phishingowych były załączniki z rzekomą fakturą, wysyłane w formacie XLS lub .tar. W opisanych kampaniach atakujący wykorzystywali złośliwe oprogramowanie Zloader (w przypadku faktur Play) oraz DanaBot (w przypadku faktur Orange), których celem była kradzież danych logowania do banku oraz środków finansowych ulokowanych na kontach zainfekowanych osób. Dzięki wykorzystaniu złośliwego oprogramowania atakujący uwiarygadniali fałszywe strony internetowe (np. podmieniając certyfikaty stron) lub wstrzykując złośliwy kod do oryginalnych stron, tym samym skutecznie wprowadzając użytkowników w przeświadczenie, że korzystają z prawdziwych, niezmodyfikowanych stron.

SARS-CoV-2

W związku z panującą na świecie w roku 2020 sytuacją epidemiczną, pojawiło się też wiele kampanii phishingowych próbujących wykorzystać pandemię do propagacji zagrożeń. Poniżej przedstawionych zostało kilka kampanii phishingowych, zidentyfikowanych przez Zespół CSIRT GOV, które wykorzystywały motyw epidemii koronawirusa:

- podszywanie się pod stronę łudząco przypominającą mapę rozprzestrzeniania się koronawirusa, zawierającą plik .exe ze złośliwym oprogramowaniem o nazwie AZORult. Jest to malware, który wykradał takie informacje jak hasła, pliki cookies (tzw. ciasteczka) czy historię przeglądania. Ponadto miał możliwość pobierania dodatkowych modułów na zainfekowane maszyny. Fałszywa strona różniła się tym, że po zainstalowaniu złośliwych plików otwierała się za pomocą aplikacji, gdzie oryginalna strona uruchamiała się w przeglądarce;
- kampania phishingowa rozsyłająca wiadomości e-mail, których motyw opierał się na rzekomo oficjalnym komunikacie wystosowanym przez WHO - Światową Organizację Zdrowia. Wiadomość zawierała złośliwy załącznik o nazwie "official statement by who.img", który w rzeczywistości okazywał się plikiem wykonywalnym "OfficialStatement By WHO.exe". Poniżej przykładowa treść wiadomości:


Dear Sir/ Madam

As published in the World Health Organisation newsletter 3/18/2020

Here enclosed official statement on the current situation

You are required to go through the attached file for your safety and that of your family and general public

Best Regards
Amanda Chang
Contact Address
BEIJING
8 Guanghua Dongli
China Overseas Plaza
South Tower, Floor 11, Suite A053
Chaoyang, Beijing 100020 Ch ina
+86 10 8598 4983

amanda.chang@biotechhealthcare.com

www. biotechhealthcare.com

-------- End of forwarded message --------

1 attachment: Official Statement By WHO.img 1.2 MB Save

- kampania polegająca na rozsyłaniu wiadomości, w których atakujący przedstawiali się jako firma oferująca sprzęt oraz środki ochronne (maski, płyny dezynfekujące itp.), pomagające chronić przed koronawirusem. W wiadomości znajdował się załącznik o nazwie „COVID 19 info_pdf.exe", który był plikiem wykonywalnym zawierającym złośliwe oprogramowanie AgentTesla;
- ujawniono kampanię mającą na celu wyłudzenie środków finansowych. Rozsyłana z adresu justicenwamaka@gmail.com dotyczyła przekazania środków pieniężnych (400 000, 00 USD) jako wsparcia finansowego ze względu na panującą pandemię COVID-19. Dodatkowym wskaźnikiem, który umożliwiał identyfikację przedmiotowej wiadomości, był adres e-mail uunicef1@outlook.com, który znajdował się w polu „odpowiedz do" oraz w samej treści wiadomości.

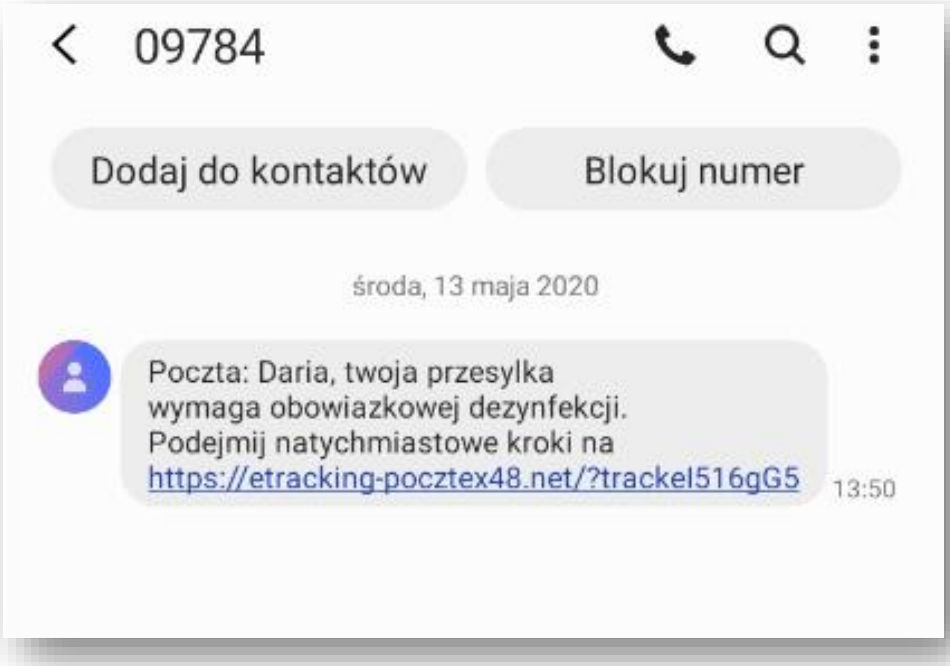
Przytoczone przykłady kampanii pokazują, iż cyberprzestępcy próbowali wykorzystać niepewną i nową sytuację związaną z wirusem SARS-CoV-2. Wykorzystując ten motyw próbowano uzyskać różnego typu informacje, np. na temat danych osobowych, czy dokonać infekcji systemów teleinformatycznych. Najbardziej popularne mechanizmy kompromitacji to np. włamanie do biznesowej poczty e-mail, przełamywanie zabezpieczeń, oprogramowanie szyfrujące ransomware czy złośliwe oprogramowanie.

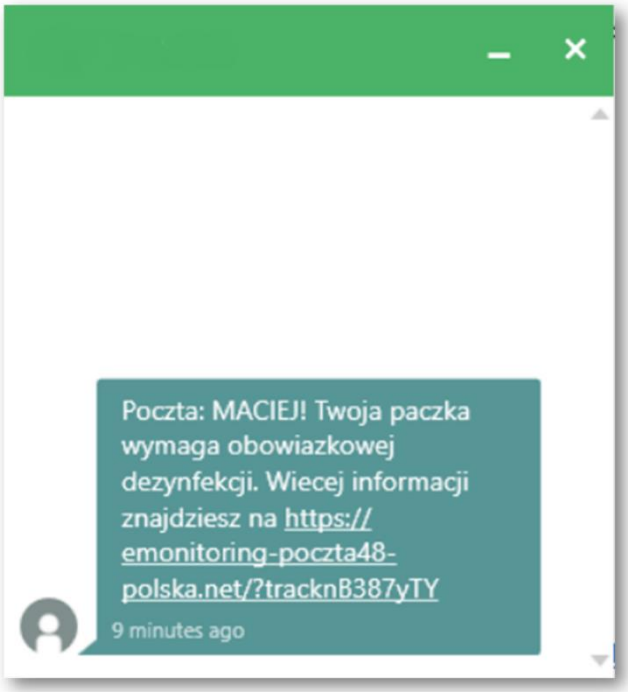
Poczta Polska

W roku 2020 zaobserwowano także zwiększoną ilość incydentów związanych z wykorzystywaniem wizerunku Poczty Polskiej. Incydenty pojawiały się cyklicznie, choć najbardziej wzmożoną aktywność można było zaobserwować w okresie nadchodzących wyborów na urząd Prezydenta RP, które miały odbyć się korespondencyjnie. Były to zarówno wiadomości elektroniczne jak i wiadomości SMS, które zawierały złośliwy załącznik lub odnośnik przekierowujący do złośliwego oprogramowania. Odnotowano dużą liczbę zrejestrowanych domen podszywających się pod Pocztę Polską. Poniżej przedstawiono przykładowe domeny:

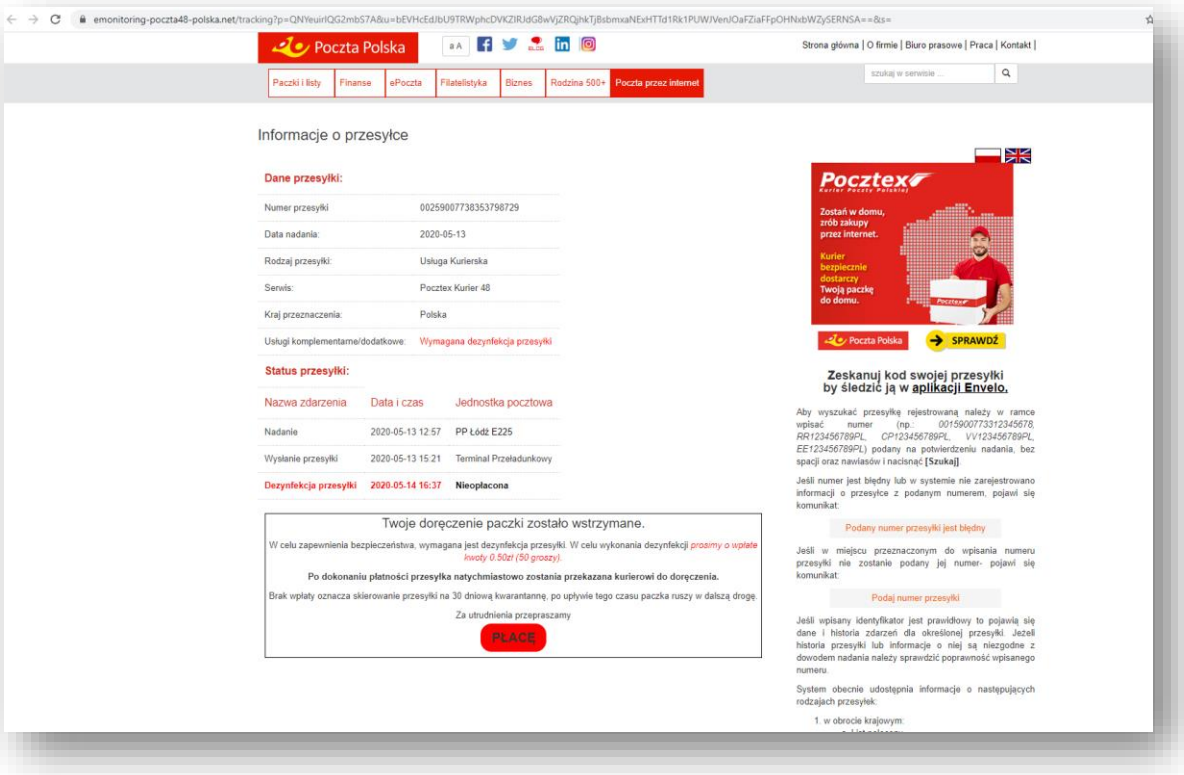
- poczta-polska24.net;
- pocztapolska24.net;
- pocztexpolska.eu;
- poczta-polska24.eu;
- pocztapolska.eu;
- pocztapolska24.eu;
- dotpay.opocztapolska.net;
- ipocztexpolska.net;
- rpocztapolska.net;
- monitor-ipocztapolska.net;
- etracking-ppocztapolska.com;
- uppocztapolska.net;
- emonitoring-epoczta-polska.net;
- spocztapolska.net.

Jedną z kampanii wykorzystującą wizerunek Poczty Polskiej i związanej z pandemią koronawirusa, były spreparowane wiadomości SMS, w których umieszczany był link z odnośnikiem do śledzenia przesyłek Poczty Polskiej, na której dodano zdarzenia związane z przekazaniem przesyłki do dezynfekcji. Poniżej przedstawiono przykładowe treści takich wiadomości SMS.


09784
Dodaj do kontaktów
Blokuj numer
środa, 13 maja 2020
Poczta: Daria, twoja przesylka wymaga obowiazkowej dezynfekcji. Podejmij natychmiastowe kroki na https://etracking-pocztex48.net/?trackel516gG5
13:50


Poczta: MACIEJ! Twoja paczka wymaga obowiazkowej dezynfekcji. Wiecej informacji znajdziesz na https://emonitoring-poczta48-polska.net/?tracknB387yTY
9 minutes ago

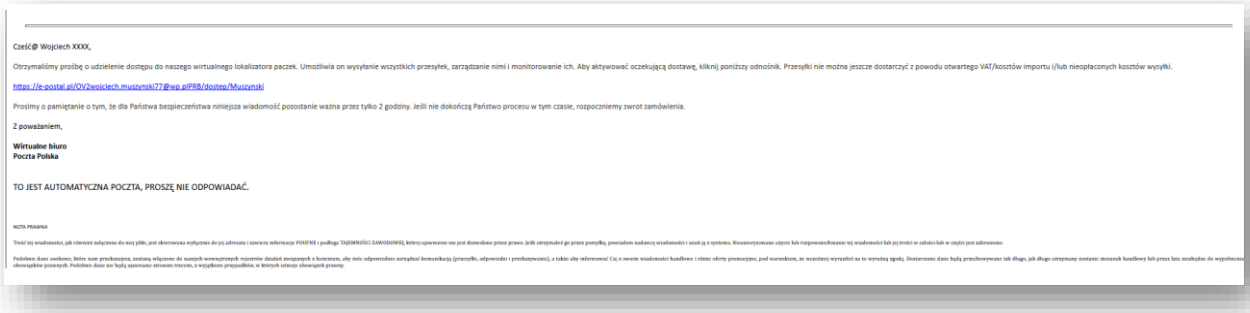
Po kliknięciu w link w treści wiadomości przekierowywano użytkownika na stronę banku, gdzie proszono o zapłatę 50gr za dezynfekcję paczki. Po zalogowaniu na konto użytkownik dostawał wiadomość SMS z kodem autoryzacyjnym, który powodował zlecenie przelewu na kwotę 2200 zł.



Klienci Poczty Polskiej dostawali również wiadomości działające w podobny sposób, lecz o innej treści, np. o przekroczeniu wagi przesyłanej paczki:

Poczta Polska S.A.: Zatrzymalismyprzesylke w sortowni ze wzgledu na przekroczenie zadeklarowanej wagi. Prosimy o doplate 0,82 zl na ipocztapolska.pl/?ID_784596412254 . Brak platnosciskutkowalbedzie zwrotem przesylki do nadawcy zgodnie z cennikiem Poczty Polskiej. Wiadomosc wygenerowana automatycznie

Rozsyłane były także fałszywe wiadomości e-mail:



Cześć@ Wojciech XXXX,

Otrzymaliśmy prośbę o udzielenie dostępu do naszego wirtualnego lokalizatora paczek. Umożliwia on wysyłanie wszystkich przesyłek, zarządzanie nimi i monitorowanie ich. Aby aktywować oczekującą dostawę, kliknij poniższy odnośnik. Przesyłki nie można jeszcze dostarczyć z powodu otwartego VAT/kosztów importu i/lub nieopłaconych kosztów wysyłki.

https://e-postal.pl/OV2wojciech.muszynski77@wp.plPR8/dostep/Muszynski

Prosimy o pamiętanie o tym, że dla Państwa bezpieczeństwa niniejsza wiadomość pozostanie ważna przez tylko 2 godziny. Jeśli nie dokończą Państwo procesu w tym czasie, rozpoczniemy zwrot zamówienia.

Z poważaniem,

Wirtualne biuro
Poczta Polska

TO JEST AUTOMATYCZNA POCZTA, PROSZĘ NIE ODPOWIADAĆ.

NOTA PRAWNA

Treść tej wiadomości, jak również załączone do niej pliki, jest skierowana wyłącznie do jej adresata i zawiera informacje POUFNE i podlega TAJEMNICY ZAWODOWEJ, której ujawnienie nie jest dozwolone przez prawo. Jeśli otrzymałeś go przez pomyłkę, powiadom nadawcę wiadomości i usuń ją z systemu. Niezatrzymywanie ujęcia lub rozpowszechnianie tej wiadomości lub jej treści w całości lub w części jest zabronione.

Podobne dane osobowe, które nam przekazujesz, zostaną włączone do naszych wewnętrznych rejestrów działań związanych z leczeniem, aby móc odpowiednio zarządzać komunikacją (przesyłki, odpowiedzi i przekazywanie), a także aby informować Cię o swoim wiadomości handlowe i różne oferty promocyjne, pod warunkiem, że wcześniej wyraziłeś na to wyraźną zgodę. Dostarczone dane będą przechowywane tak długo, jak długo otrzymany zostanie stosunek handlowy lub przez lata niezbędne do wypełnienia obowiązków prawnych. Podobne dane nie będą ujawniane stronom trzecim, z wyjątkiem przypadków, w których istnieje obowiązek prawny.

Po kliknięciu w link w wiadomości powyżej ukazywała się poniższa strona:

W zdecydowanej większości opisane powyżej kampanie miały na celu wyłudzenie środków finansowych od użytkowników Poczty Polskiej. Dodatkowo można zauważyć, iż nawet w niektórych z przykładów próbowano wykorzystać sytuację związaną z panującą wówczas pandemią.

Kampanie phishingowe wyłudzające kryptowalutę Bitcoin

W 2020 roku regularnie obserwowano zmasowaną wysyłkę wiadomości e-mail, w której użytkownik dostaje informacje o przejęciu komputera i zainfekowaniu go złośliwym oprogramowaniem, dzięki któremu przestępca uzyskuje prywatne informacje na temat ofiary. Kampania ta ma na celu wyłudzenie środków finansowych w postaci kryptowaluty Bitcoin. Poniżej lista domen z jakich m.in. wysyłane były wyłudzające wiadomości:

- ksmith@colodnyfass.com;
- sybil.peckmy@dc.com.pl;
- peter@anonymousgang.com;
- szuszkiewiczw@pocztex.pl;
- ruponu@soneramail.nl;
- biuro90@itpartner24.pl;
- mail@furniturefile.nl;
- hmmm@alzet.nl;
- thisisjusttestmessageatall@brito.nl;
- karen@karenwoodruff.com;
- noone@hjotmail.com;
- mbarrett@ustankalliance.com;
- mvial@mi-mail.cl;
- hiro@wakatakeya.com;
- winnie@inns.com.cn.

Najczęściej używano następujących tytułów wiadomości phishingowej:

- Oferta handlowa;
- Interes Handlowy;
- Z0stałeś zhak0wany.

Treść wiadomości, jeśli się zmieniała, to dość nieznacznie. Poniżej przykład jednej z odsłon przedmiotowej kampanii:

> *„Cześć! Niestety, mam dla Ciebie złe wiadomości. Parę miesięcy temu zdobyłem dostęp do urządzenia, którego używasz do przeglądania internet. Od tego czasu monitorowałem Twoją aktywność internetową.[…] Prześlij równowartość 1200 EUR na mój portfel Bitcoin, a zapomnę o całej sprawie. Usunę również wszystkie dane i filmy na zawsze.[…] Mój portfel Bitcoin (BTC): 1EyAadxvFqjvG9swUeexQLFhTvdV6jBTbi.*
> *Masz 48 godzin na odpowiedź […]"*

Wskazana kampania phishingowa powracała regularnie i była zakrojona na szeroką skalę w sieci Internet. Kampania wykazywała się pewną skutecznością, o czym świadczył portfel bitcoinowy umieszczony do płatności w treści wiadomości.

Adres	***1EyAadxFqjvG9swUeexQLFhTvdV6jBTbi***
Liczba raportów	264
Ostatni raport	12 Paź 2020 14:33:51 +0000
Liczba otrzymanych Bitcoinów	**0.94593813 BTC**
Liczba otrzymanych transakcji	9

Tabela 1- Dane ze strony blockchain.info

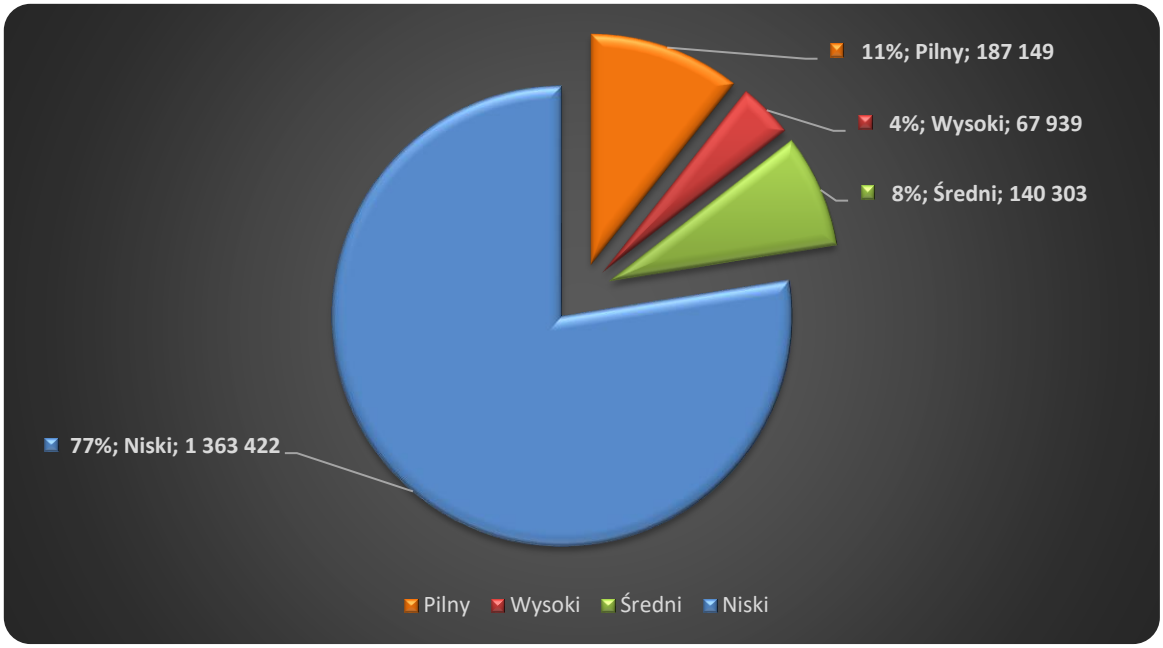
4. ARAKIS

System ARAKIS 3.0 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 2020 roku, w sieciach teleinformatycznych podmiotów uczestniczących w projekcie ARAKIS 3.0 GOV, zanotowano łącznie **1 813 243 995** przepływów, co przełożyło się na **1 758 813** wygenerowanych przez system alarmów[8]. Wśród zanotowanych alarmów:

- **187 149** alarmów miało priorytet pilny, tzn. wymagało natychmiastowej reakcji na zagrożenie ze strony administratorów, niosło duże ryzyko przełamania zabezpieczeń;
- **67 939** alarmów miało priorytet wysoki, tzn. wymagało wzmożonej uwagi w kontekście zagrożenia wskazanego w alarmie, niosło średnie ryzyko przełamania zabezpieczeń;
- **140 303** alarmy miały priorytet średni, tzn. były to alarmy informujące o dobrze znanym zagrożeniu, które niosły małe ryzyko przełamania zabezpieczeń;
- **1 363 422** alarmy miały priorytet niski, tzn. były to alarmy czysto informacyjne dot. aktualnej sytuacji na styku sieci wewnętrznej z siecią Internet.

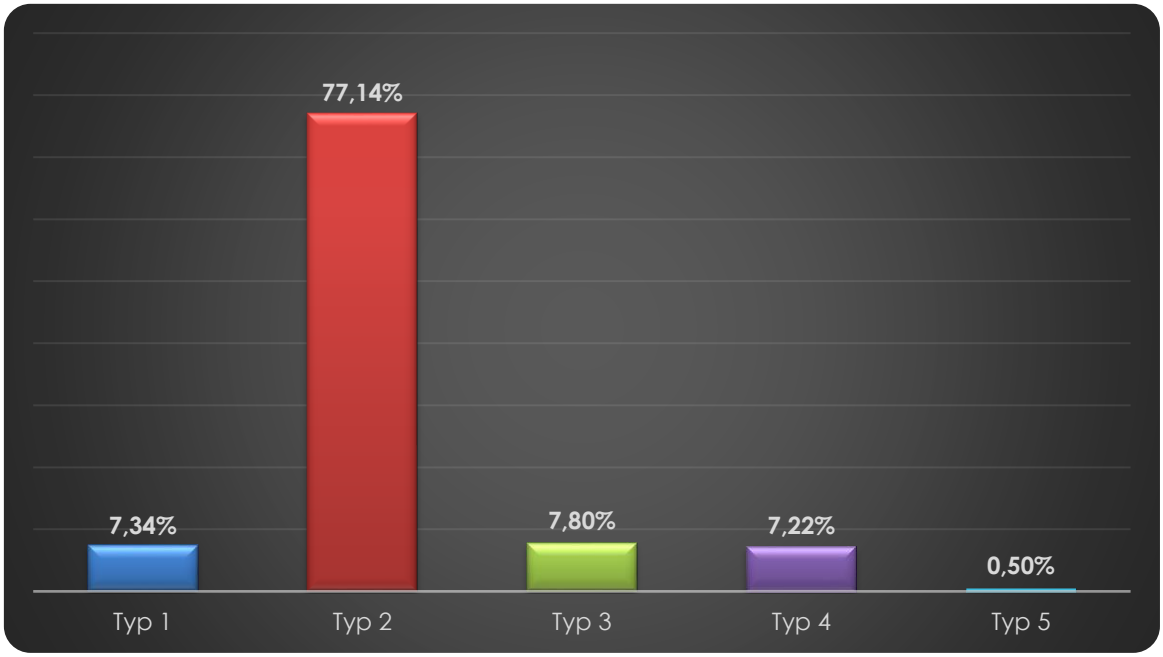
[8] Pojedynczy alarm może składać się z wielu przepływów.



Wykres 7 - Procentowy rozkład alarmów systemu ARAKIS 3.0 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:

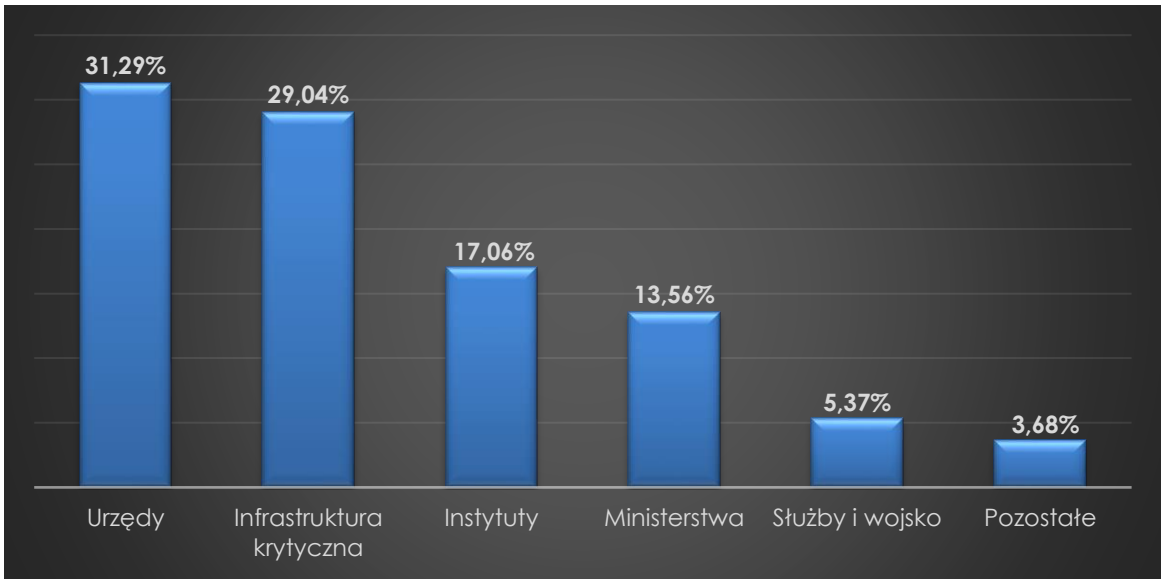
- Typ 1 – komunikacja do złośliwych adresów;
- Typ 2 – skanowania;
- Typ 3 – wykryte znane ataki;
- Typ 4 – wykryte nieopisane ataki;
- Typ 5 – infekcje wewnętrzne.



Wykres 8 - Procentowy podział alarmów systemu ARAKIS 3.0 GOV ze względu na typ

W 2020 roku alarmy Systemu ARAKIS 3.0 GOV typu 1 (komunikacja ze złośliwych adresów) stanowiły 7,34% 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 (skanowania)w 2020 roku najwięcej przepływów zostało zanotowanych w instytucjach skategoryzowanych jako *Urzędy* (31,29%), co wynika po części z ilości elementów systemu ARAKIS 3.0 GOV rozlokowanych w poszczególnych instytucjach. Wygenerowane alarmy pozwalają określić kierunki zainteresowań osób przeprowadzających skanowania.



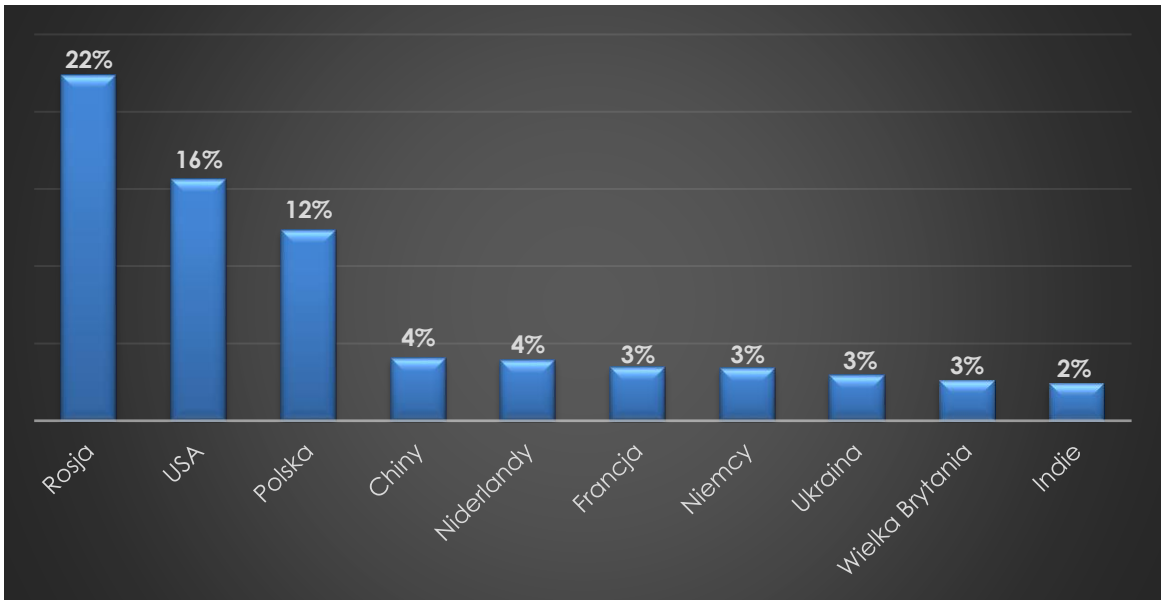
Wykres 9 - Procentowy podział przepływów alarmów typu 2 w instytucjach

Alarmy typu 3 i 4 (wykryte znane ataki i wykryte nieopisane ataki) stanowiły odpowiednio 7,80% oraz 7,22% 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 (infekcje wewnętrzne) są to infekcje wewnętrzne identyfikowane na podstawie niepożądanej komunikacji z elementami sieci objętymi systemem ARAKIS 3.0 GOV.

Do najbardziej aktywnych krajów pod kątem liczby generowanych przepływów w 2020 roku należały Rosja (22% przepływów) oraz Stany Zjednoczone (16% przepływów). Należy zwrócić uwagę na duży stosunek przepływów pochodzących z adresów należących do Polski (12% przepływów). W stosunku do poprzedniego roku wzrost aktywności adresów należących do polskiej puli adresowej wzrósł o 2 p.p.

Warto też zaznaczyć, iż liczba przepływów z poszczególnych krajów należących do grupy TOP 10 stanowi 73% wszystkich wygenerowanych przepływów zanotowanych przez System ARAKIS 3.0 GOV w 2020 roku.



Wykres 10 - Rozkład źródeł ataków na sieci monitorowane przez system ARAKIS 3.0 GOV pod kątem liczby generowanych przepływów

Biorąc pod uwagę specyfikę sieci Internet (tzw. *brak granic*), infrastruktura teleinformatyczna podmiotów generujących przepływy w stronę systemu ARAKIS 3.0 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	471 328 186	ICMP Echo Reply
4	1433	262 952 317	MSSQL
3	445	133 408 731	SMB
4	23	33 012 305	Telnet
5	21	27 271 263	FTP
6	22	22 930 057	SSH
7	111	18 441 881	RPC
8	80	10 406 209	HTTP
9	443	10 114 738	HTTPS
10	8291	8 758 628	Urządzenie MikroTik

Tabela 2 - Zidentyfikowane w 2020 roku skanowania i próby eksploitacji usług na podstawie danych z systemu ARAKIS 3.0 GOV

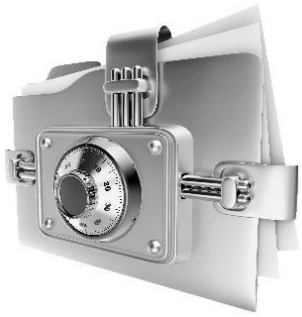
W roku 2020 najczęściej wykorzystywanym elementem rekonesansu był protokół ICMP Echo Reply. Warto odnotować po raz kolejny duże zainteresowanie usługą MSSQL powiązaną z portem 1433 oraz port 445 powiązany z usługą SMB, posiadającą wiele znanych podatności. W przypadku pozostałych protokołów odnotowano mniejsze ilości przepływów niż w roku poprzednim.

L.p.	Liczba przepływów	Reguła SNORT
1	35653275	ET SCAN Suspicious inbound to MSSQL port 1433
2	5736998	ET INFO Potentially unsafe SMBv1 protocol in use
3	3036033	GPL NETBIOS SMB-DS IPC$ unicodeshareaccess
4	2999576	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)
5	2762758	ET SCAN Potential SSH Scan OUTBOUND
6	2134202	GPL NETBIOS SMB-DS IPC$ shareaccess
7	1704970	ET SCAN Sipvicious Scan
8	1249421	ET SCAN Behavioral Unusual Port 1433 traffic, Potential Scan orInfection
9	795211	ET SCAN Suspicious inbound to mySQL port 3306
10	678260	ET SCAN SSH BruteForceTool with fake PUTTY version

Tabela 3 - Najczęściej dopasowane reguły do ruchu sieciowego widzianego przez system ARAKIS 3.0 GOV

W 2020 roku zidentyfikowano 35 653 275 dopasowań reguł SNORT do obserwowanego ruchu sieciowego związanego z portem 1433. Przedmiotowe dopasowania mają odzwierciedlenie m.in. w ruchu zaprezentowanym w poprzedniej tabeli na poszczególne porty docelowe – najczęściej wykrywane są reguły dotyczące prób nieuprawnionego wykorzystania usług MSSQL i SMB, co mogło wiązać się z próbami uzyskania dostępu do baz danych lub wykorzystaniem znanych podatności.

5. Ocena bezpieczeństwa systemów TI



W 2020 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 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.

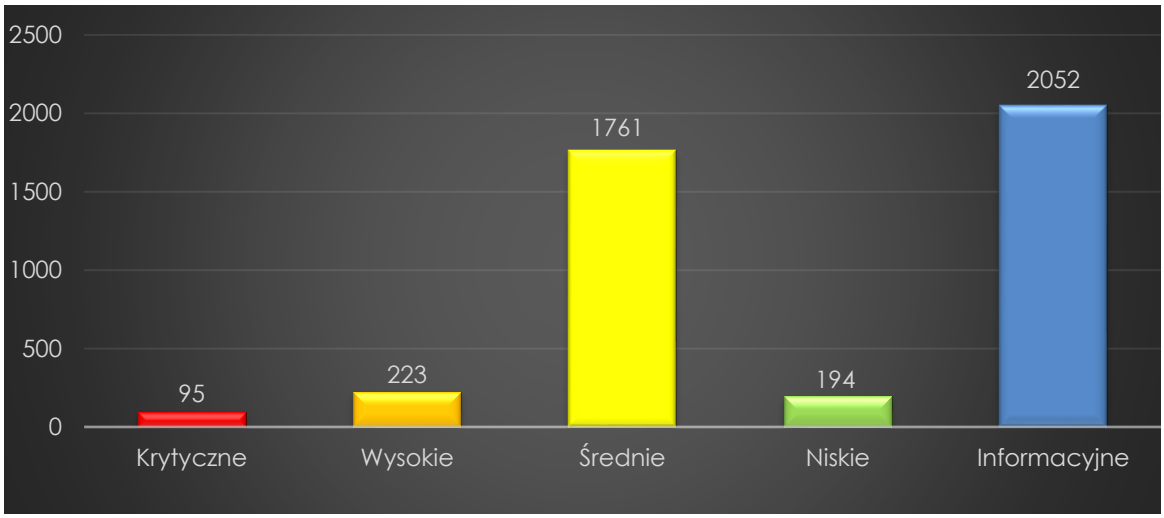
Zgodnie z Decyzją nr 90 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 25 września 2019 r. w sprawie przeprowadzenia przez Agencję Bezpieczeństwa Wewnętrznego ocen bezpieczeństwa systemów teleinformatycznych na 2020 r., Zespół CSIRT GOV przeprowadził przedmiotowe czynności w czternastu instytucjach administracji rządowej oraz infrastruktury krytycznej, w których przebadał 82 systemy teleinformatyczne.

Nazwa instytucji	Liczba przebadanych systemów teleinformatycznych
Naczelny Sąd Administracyjny	2
PGE Polska Grupa Energetyczna S.A.	12
Grupa LOTOS S.A.	10
Krajowe Biuro Wyborcze	4
Poczta Polska S.A.	5
PKP Polskie Linie Kolejowe S.A.	8
Ministerstwo Finansów – Krajowa Administracja Skarbowa	7
Polska Agencja Żeglugi Powietrznej	4
Lubelski Urząd Wojewódzki z Lublinie	6
Górnośląskie Towarzystwo Lotnicze S.A. – Port Lotniczy Katowice Pyrzowice	6
Urząd Morski w Gdyni	2
AQUANET S.A.	5
Dolnośląski Urząd Wojewódzki we Wrocławiu	5
Warmińsko-Mazurski Urząd Wojewódzki w Olsztynie	6

Tabela 4 - Wykaz przebadanych systemów teleinformatycznych

W ramach przeprowadzonych ocen bezpieczeństwa Zespół CSIRT GOV zrealizował szereg testów mających na celu identyfikację istotnych podatności wpływających na bezpieczeństwo infrastruktur teleinformatycznych instytucji. Do rzeczowych testów należało pasywne, półpasywne oraz aktywne zbieranie informacji, identyfikacja podatności architektury systemów i usług sieciowych, wykorzystywanie podatności oraz analiza wpływu wykorzystania czynników inżynierii społecznej.

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



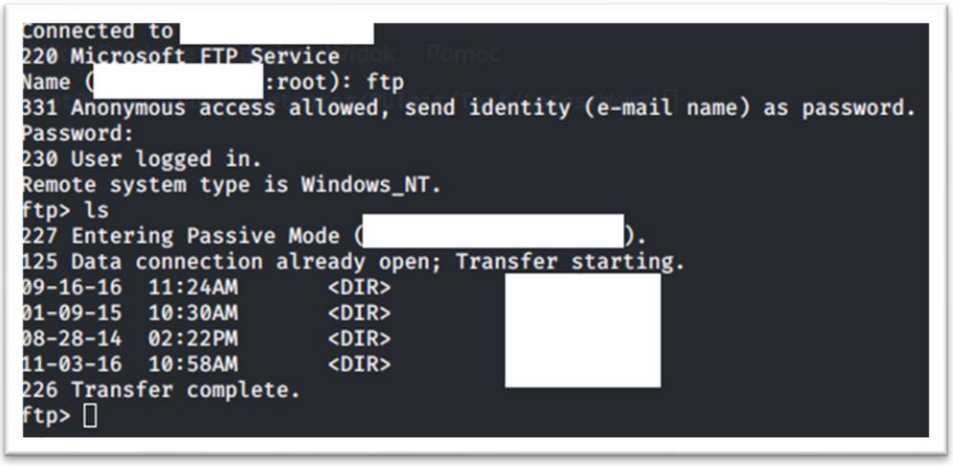
Wykres 11 - Zestawienie zidentyfikowanych podatności z podziałem na priorytet

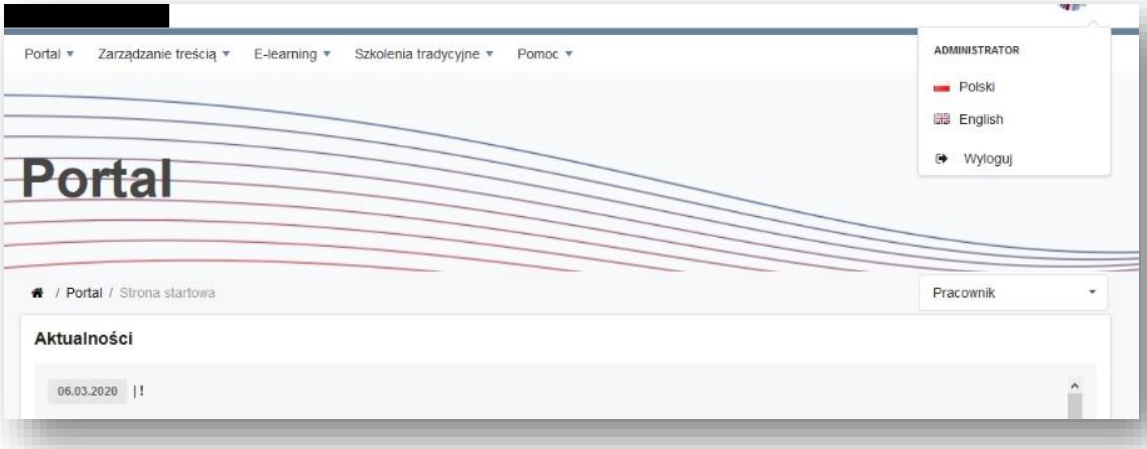
Do najistotniejszych (krytycznych oraz wysokich) podatności zidentyfikowanych w ramach przeprowadzonych ocen bezpieczeństwa systemów teleinformatycznych należały:

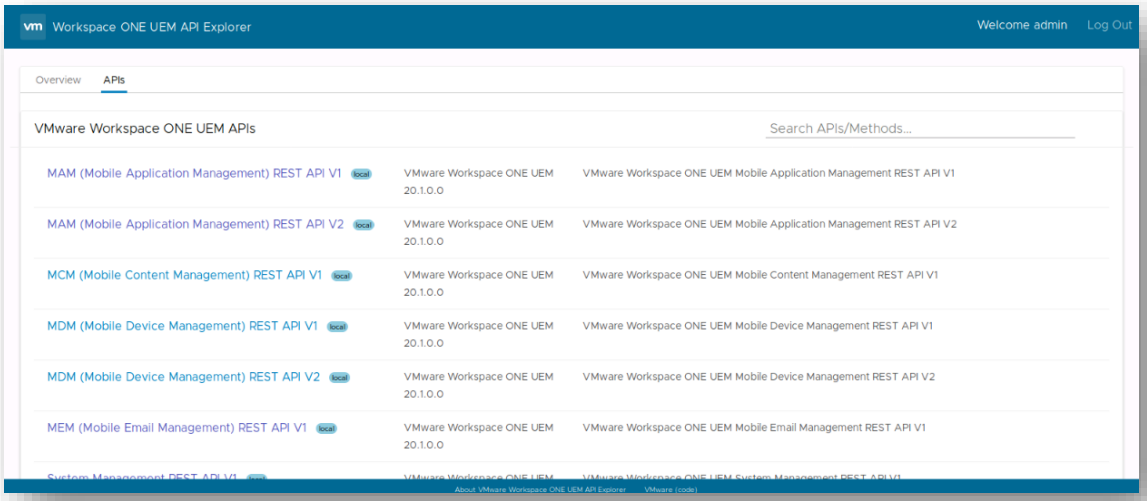
- Wersje oprogramowania zwierające podatności:
  a) OpenSSL;
  b) Apache;

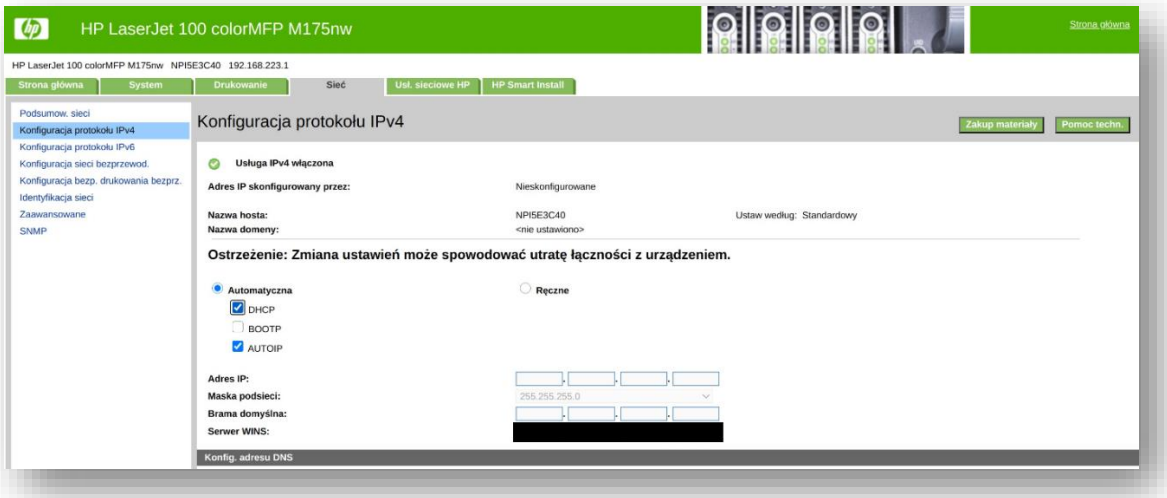
c) IBM Spectrum Protect;
d) Oracle WebLogic;
e) HP Data Protector;
f) TYPO3;
g) PostgreSQL;
h) HP IntegratedLights-Out;
i) Vmware ESXi.

- Nieaktualne wersje oprogramowania:
  a) Apache;
  b) PHP;
  c) Kibana;
  d) phpMyAdmin;
  e) OpenSSL;
  f) NGINX.
- Niewspierane wersje oprogramowania i systemów operacyjnych:
  a) Apache;
  b) Microsoft Windows Server;
  c) OpenSSL;
  d) CentOS.
- Nieprawidłowo zabezpieczone dostępy do urządzeń sieciowych, serwerów, usług, portali – dostęp do paneli administracyjnych urządzeń zabezpieczony poprzez domyślne hasła producenta i/lub hasła o nieodpowiedniej długości i złożoności – przykłady poniżej:

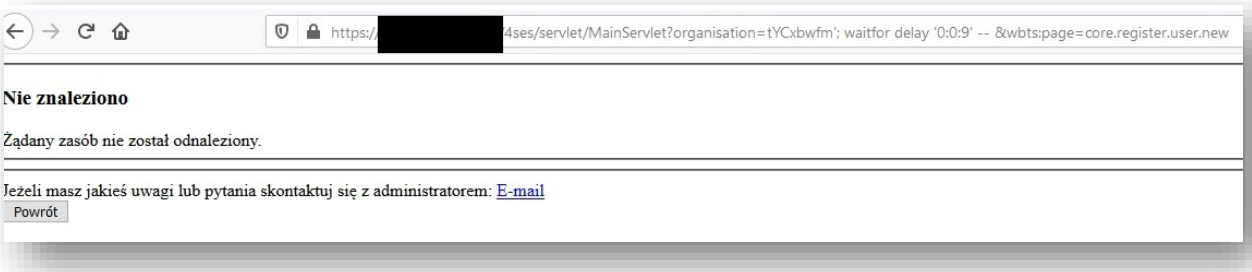

Connected to
220 Microsoft FTP Service
Name (:root): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
227 Entering Passive Mode ( ).
125 Data connection already open; Transfer starting.
09-16-16 11:24AM <DIR>
01-09-15 10:30AM <DIR>
08-28-14 02:22PM <DIR>
11-03-16 10:58AM <DIR>
226 Transfer complete.
ftp>


Portal
Zarządzanie treścią
E-learning
Szkolenia tradycyjne
Pomoc
ADMINISTRATOR
Polski
English
Wyloguj
Portal
/ Portal / Strona startowa
Pracownik
Aktualności
06.03.2020

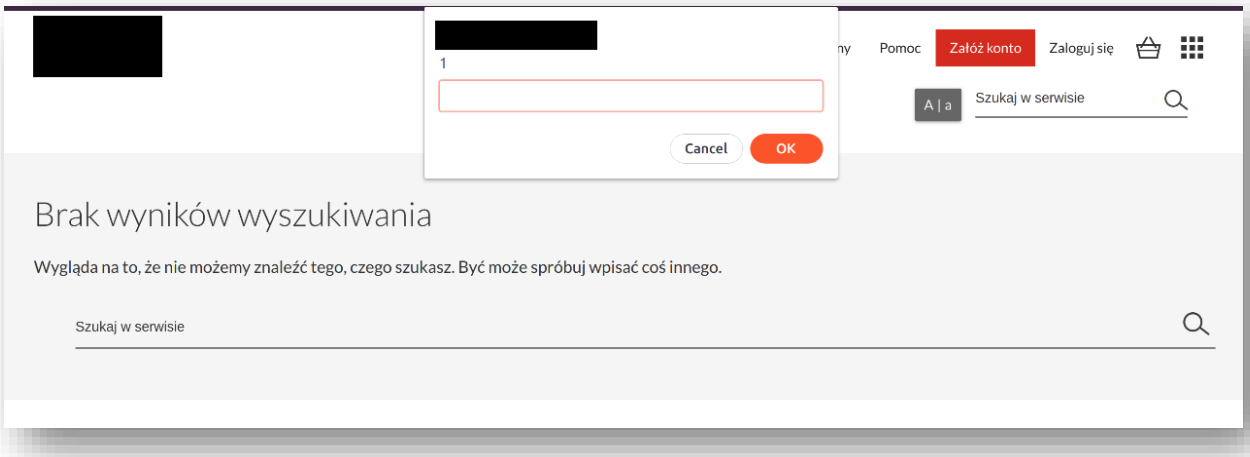

Workspace ONE UEM API Explorer
Welcome admin
Log Out
Overview
APIs
VMware Workspace ONE UEM APIs
Search APIs/Methods...
MAM (Mobile Application Management) REST API V1
MAM (Mobile Application Management) REST API V2
MCM (Mobile Content Management) REST API V1
MDM (Mobile Device Management) REST API V1
MDM (Mobile Device Management) REST API V2
MEM (Mobile Email Management) REST API V1
VMware Workspace ONE UEM 20.1.0.0



- Stosowanie protokołu IPMI v2.0 zawierającego podatności;
- Hasło do panelu administratora do aplikacji zaszyte w kodzie strony w formie komentarza;
- Stosowanie protokołu RDP zawierającego podatności;
- Akceptacja połączeń z wykorzystaniem szyfrowania SSL 2.0 i/lub 3.0 pozwalających na przeprowadzenie ataków typu man-in-the-midle;
- Występowanie podatności typu SQL Injection pozwalającej na podmianę struktury logicznej zapytania SQL kierowanego do produkcyjnej bazy danych;



- Podatność typu Blind SQL Injection;
- Podatność typu HTML Injection;
- Podatność typu XSS;



- Brak ochrony przed atakami CSRF;
- Hasła użytkowników podatne na atak „brute-force" i dostęp do panelu logowania dla wszystkich użytkowników sieci Internet, w tym sieci anonimizującej TOR;

- Możliwość uzyskania domyślnej nazwy zdalnego serwera SNMP.

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

- Wsparcie dla słabych algorytmów szyfrowania SSL (długość klucza od 64 do 112 bit-ów);
- Certyfikat X.509 serwera jest podpisany przez nieznane centrum autoryzacyjne (CA) – podpis typu „self-signed”;
- Usługa zdalna wykorzystuje łańcuch certyfikatów SSL, który zawiera główny certyfikat wydany przez niezaufany urząd certyfikacyjny;
- Ważność certyfikatu SSL wygasła;
- Wykorzystywanie algorytmów hashowania podatnych na kolizję tj. m.in. MD2, MD4, MD5 lub SHA1;
- Podatność pozwalająca na wymuszenie słabszego szyfrowania Diffie-Hellman z kluczem <=1024 bitów (Logjam);
- Stosowanie usługi Telnet;
- Błędy w konfiguracji Apache JServ umożliwiające czytanie plików aplikacji z podatnego serwera;
- Wsparcie dla szyfrowania SSLv3 pozwalającego na przeprowadzenie ataku Man-in-the-middle;
- Możliwość uzyskania listy plików znajdujących się na serwerze www;
- Podatność na ataki typu Breach;
- Możliwość wstrzyknięcia dowolnego nagłówka HTTP typu HOST;
- Serwer WWW nieposiadający ustawionego nagłówka „X-Frame-Options” lub „Content-Security-Policy”;
- Podatność na ataki typu „Clickjacking”;
- Serwer NTP odpowiada na zapytania w trybie 6;
- Włączona metoda HTTP TRACE;
- Podatność pozwalająca na wymuszenie słabszego szyfrowania;
- Możliwość zalogowania się do systemu przy użyciu sesji NULL.

W ramach prowadzonych ocen bezpieczeństwa Zespół CSIRT GOV przeprowadził również analizę źródeł otwartych, tzw. 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 aktywne konta.

6. ĆWICZENIA

W roku 2020 sytuacja pandemiczna wpłynęła na ograniczenia w zakresie organizacji ćwiczeń dot. cyberbezpieczeństwa. Część z ćwiczeń została przełożona na kolejny rok, podczas gdy w niektórych przypadkach organizatorzy wybrali scenariusze ćwiczenia tylko poprzez opcję zdalną.

Niemniej jednak, pomimo wskazanych okoliczności Zespół CSIRT GOV zaangażowany był w realizację ćwiczeń zarówno zespołów międzynarodowych jak i na szczeblu krajowym.

CCE2020

W dniu 29 października 2020 roku Zespół CSIRT GOV wziął udział w ćwiczeniach (CCE2020), które zostały przeprowadzone w formie zdalnej. Był to pierwszy udział przedstawicieli CSIRT GOV w ćwiczeniach CCE organizowanych przez południowokoreański instytut badawczy National Security Research Institute. Ćwiczenia Cyber Conflict Exercises odbywają się w Korei Południowej i dotyczą cyberbezpieczeństwa administracji publicznej. W edycji 2020 wzięło udział 30 zespołów z Korei Południowej oraz 5 zaproszonych drużyn zagranicznych, w tym Zespół CSIRT GOV.

Celem przewodnim ćwiczeń było zwiększenie odporności administracji rządowej, agencji państwowych, a także instytucji cywilnych wobec zagrożeń cyberbezpieczeństwa. Zadania, z którymi musiały się zmierzyć poszczególne zespoły cyberbezpieczeństwa, w dużej mierze miały charakter wyzwań typu *Capture the Flag*. W ramach scenariuszy ćwiczenia przewidziano możliwość sprawdzenia zdolności do obrony przed cyberatakami w czasie rzeczywistym, a także umiejętności prowadzenia analizy incydentów.

Ćwiczenia stały się okazją do poznania metod i sposobu działania drużyn azjatyckich zajmujących się reagowaniem na incydenty w cyberprzestrzeni. Zadania realizowane przez poszczególne zespoły wymagały umiejętności m.in. dotyczących informatyki śledczej, programowania, analizy ruchu sieciowego,

analizy przełamywania zabezpieczeń aplikacji i serwerów WWW, a także w zakresie złośliwego oprogramowania.

KSC-EXE 2020

W dniach 22-23 września 2020 roku odbyły się pierwsze Międzysektorowe Ćwiczenia Cyberbezpieczeństwa KSC-EXE 2020, do udziału w których został zaproszony Zespół CSIRT GOV. Organizacja ćwiczeń na poziomie krajowym jest realizacją przepisów ustawy o krajowym systemie cyberbezpieczeństwa, nałożonych na Pełnomocnika Rządu ds. Cyberbezpieczeństwa. Tegoroczne ćwiczenia, z uwagi na stan zagrożenia epidemicznego, odbyły się w formule zdalnej wykorzystując wspólne środowisko chmurowe do komunikacji, wymiany dokumentów oraz wideokonferencji.

Wśród głównych celów stawianych w ćwiczeniach zaplanowano weryfikację zdolności podmiotów Krajowego Systemu Cyberbezpieczeństwa do reagowania w sytuacjach kryzysowych spowodowanych cyberatakami, jak również wzmocnienie możliwości działania w sytuacji kryzysowej w oparciu o organy wchodzące w skład Zespołu ds. Incydentów Krytycznych oraz Rządowego Zespołu Zarządzania Kryzysowego.

W ćwiczeniach wzięły udział m.in. podmioty z sektorów finansowego, telekomunikacyjnego, energetycznego i pozostałych zespołów CSIRT poziomu krajowego, tj. CSIRT MON i CSIRT NASK.

W ćwiczeniach wykorzystano scenariusze ataków na sektor finansowy oraz energetyczny. Zakładane sytuacje kryzysowe obejmowały m.in. przerwanie lub zakłócenie świadczenia usług kluczowych.

Planowane są kolejne tego typu ćwiczenia zgodnie z kompetencjami Pełnomocnika Rządu ds. Cyberbezpieczeństwa.

7. USTAWA O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA, REALIZACJA OBOWIĄZKU ZGŁOSZENIA OSÓB DO KONTAKTU Z CSIRT GOV

Wprowadzając ustawę z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa, ustawodawca nałożył na operatorów usług kluczowych oraz na podmioty publiczne obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Stanowi o tym art. 9, który brzmi, iż operator usługi kluczowej wyznacza osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz przekazuje organowi właściwemu do spraw cyberbezpieczeństwa dane, o których mowa w art. 7 ust. 2 pkt. 8 i 9, nie później niż w terminie 3 miesięcy od zmiany tych danych. Natomiast art. 22 ust. 1 pkt. 5 omawianej ustawy stanowi, iż podmiot publiczny, o którym mowa w art. 4 pkt. 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego, ma obowiązek przekazania do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV dane osoby, o której mowa w art. 21, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia jej wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

W związku z powyższym, Zespół CSIRT GOV prowadzi zestawienie podmiotów oraz operatorów, które zgłosiły osoby odpowiedzialne za utrzymywanie kontaktów z Zespołem CSIRT GOV. Od wejścia ustawy w życie (sierpień 2018) do końca roku 2020 prawie 400 podmiotów i operatorów przesłało formularz zgłoszenia osób do kontaktów z CSIRT GOV, w tym 193 we właściwości CSIRT GOV.

Poniżej roczna statystyka przesłanych formularzy:

ROK	Liczba przesłanych formularzy ogółem	Właściwość Zespołu CSIRT GOV
2018	45	23
2019	209	91
2020	140	79

Tabela 5 - Roczna statystyka przesłanych formularzy kontaktowych

Należy zauważyć, że realizacja obowiązków ustawowych w zakresie przekazywania do Zespołu CSIRT GOV danych osób wyznaczonych do kontaktów w zakresie cyberbezpieczeństwa umożliwia zarówno operatorom usług kluczowych, jak i podmiotom publicznym sprawną obsługę zgłoszeń dotyczących incydentów oraz pozwala na otrzymywanie stosownych ostrzeżeń o zagrożeniach.

Wskazane jest, aby realizacja obowiązków informacyjnych w zakresie przekazywania danych osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, w tym z właściwym zespołem CSIRT poziomu krajowego, była uwzględniona w procedurach w ramach polityki bezpieczeństwa informacji zarówno u operatorów usług kluczowych jak i podmiotów publicznych.

8. REKOMENDACJE DOTYCZĄCE BEZPIECZEŃSTWA PRACY ZDALNEJ

Rok 2020 najpewniej będzie kojarzony z pandemią koronawirusa, w wyniku której zostało wprowadzonych wiele restrykcji i obostrzeń, które jednocześnie oddziaływały na funkcjonowanie instytucji państwowych.

W obliczu zagrożenia epidemicznego wprowadzano w wielu instytucjach określone rozwiązania teleinformatyczne umożliwiające świadczenie pracy w systemie pracy zdalnej. Spowodowało to tym samym, że zdecydowanie większa część zadań administracji państwowej oraz organów państwa przeszła na aktywność w sieci Internet, wykorzystując stosowne środki komunikacji i pracy przeznaczone dla pracy zdalnej. Wielu pracodawców umożliwiło swoim pracownikom tego rodzaju pracę, dzięki której można było zapewnić ciągłość działania danej instytucji czy organu państwa, tym samym minimalizując ryzyko epidemiczne.

Umożliwienie pracy zdalnej stworzyło określonego rodzaju wyzwania bezpieczeństwa teleinformatycznego dla jednostek państwowych w postaci konieczności zapewnienia stałego dostępu do zasobów teleinformatycznych, przy zachowaniu bezpieczeństwa przetwarzanych w systemach informacji, standardowo polegającego na uwzględnieniu takich atrybutów ochrony informacji jak poufność, dostępności oraz ich integralność.

Należy także zwrócić uwagę na jeden aspekt wskazanej sytuacji. Mianowicie decyzja dotycząca zapewnienia pracy zdalnej w większej jak dotychczas skali była bardzo często podyktowana potrzebą dostarczenia w krótkim czasie stosownych rozwiązań teleinformatycznych, umożliwiających dostęp zdalny dla całego grona pracowników do poczty służbowej, zasobów lokalnych, systemów intranetowych czy też umożliwienia prowadzenia telekonferencji.

Podmioty, które nie posiadały odpowiednio rozwiniętego w tym kierunku zaplecza IT były bardziej podatne na ataki ukierunkowane na administrowane przez nich systemy.

Zagrożenia te mogły przyczyniać się zarówno do strat wizerunkowych jak i ewentualnie utraty danych wrażliwych.

Biorąc pod uwagę konieczność zapewnienia usług teleinformatycznych w systemie pracy zdalnej dla pracowników podmiotów, można zwrócić uwagę na dwa najbardziej wykorzystywane rozwiązania teleinformatyczne w tym zakresie, tj. systemy klasy VPN oraz systemy do telekonferencji.

Dostęp do infrastruktury lokalnej poprzez wirtualną sieć prywatną VPN oznacza konieczność ustanowienia określonych środków bezpieczeństwa uniemożliwiających osobom postronnym próbę uzyskania dostępu do chronionych zasobów.

Błędna konfiguracja zabezpieczeń połączenia VPN stwarza problem nieupoważnionego zdalnego dostępu. VPN działają zarówno jako drzwi wejściowe do infrastruktury, jak również jako tylne do krytycznych danych i aplikacji, co jest także przedmiotem zainteresowania atakujących. VPN są równolegle punktami wejścia do wewnętrznych zasobów, a także administracyjnego backend-u różnych systemów, dając osobom nieuprawnionym możliwość wprowadzenia zmian, wyłączenia, zniszczenia, kradzieży danych lub uzyskania nieautoryzowanego dostępu, jak również spowodowania wielorakiego rodzaju zakłóceń w infrastrukturze. Dla zespołów bezpieczeństwa IT zabezpieczenie VPN stanowi nieustające wyzwanie. Wiele z najbardziej znanych naruszeń bezpieczeństwa można powiązać bezpośrednio z błędną konfiguracją sieci VPN lub wprowadzaniem polityk bezpieczeństwa, stwarzających wyjątki w dostępie z pominięciem właściwych zabezpieczeń.

W przypadku telekonferencji, podobnie jak w połączeniach VPN, głównym zagrożeniem jest wykorzystanie błędów w istniejących platformach do obsługi telekonferencji.

Odnosząc się do pracy zdalnej należy zaznaczyć, że po stronie pracownika leży przestrzeganie zasad dotyczących stosownego postępowania z danymi firmowymi, a po stronie pracodawcy spoczywa zapewnienie bezpiecznego do nich dostępu oraz zapewnienie odpowiedniego bezpieczeństwa danych od strony technicznej.

Biorąc pod uwagę powyższe, w celu minimalizacji ryzyka związanego z naruszeniem bezpieczeństwa danych firmowych, można sformułować pewne zalecenia pozwalające na zapewnienie większego bezpieczeństwa pracy zdalnej dla personelu, przy kontroli ryzyka związanego z tego rodzajami usług teleinformatycznych, świadczonych dla pracowników przez instytucje. Wśród zaleceń wartych uwzględnienia można wskazać następujące:

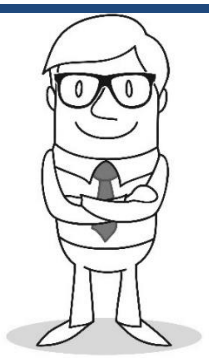
- należy udostępnić pracownikowi służbowy sprzęt przygotowany do pracy zdalnej oraz wdrożyć mechanizmy mające na celu ograniczenie użytkowania służbowych stacji roboczych do celów prywatnych, a w szczególności korzystania z prywatnej poczty e-mail, portali społecznościowych, z wyjątkiem uzasadnionych przypadków, np. „public relations";
- należy upewnić się, że system operacyjny jest poprawnie zaktualizowany, a ochrona antywirusowa włączona (należy pamiętać o aktywnej ochronie i włączonej aktualizacji sygnatur);
- rekomendowane jest, aby konto użytkownika nie posiadało uprawnień administracyjnych, oraz nie pozwalało na instalowanie żadnego oprogramowania niezatwierdzonego przez dany podmiot;
- należy stosować rozwiązania pozwalające na kryptograficzną ochronę danych na dyskach służbowych, np. w przypadku komputerów opartych o system Microsoft można stosować wbudowane w system operacyjny narzędzie BitLocker lub korzystać z innych rozwiązań kryptograficznych;
- należy zapewnić pracownikom dostęp do danych firmowych za pośrednictwem wirtualnej sieci prywatnej VPN administrowanej

przez instytucję. Wybierając VPN należy zwrócić uwagę, które z rozwiązań pozwalają na zapewnienie wysokiego poziomu bezpieczeństwa uwzględniając m.in. kwestie uwierzytelnienia pomiędzy klientem a serwerem, autoryzacji dostępu danego klienta do zasobów, szyfrowania zapewniającego poufność przesyłanych informacji, a także rozliczalności pracy klientów w dostępie do VPN;

- należy zapewnić ciągłą aktualizację środowiska VPN i śledzić na bieżąco ujawniane podatności wykorzystywanych rozwiązań, zwłaszcza umożliwiające naruszenie procesów uwierzytelnienia pomiędzy serwerem a klientem;
- w sytuacji, gdy służbowy komputer jest również wykorzystywany m.in. do wideokonferencji, kursów czy szkoleń można utworzyć osobne konto w systemie z maksymalnie ograniczonymi uprawnieniami. Powyższe ma na celu uniemożliwienie dostępu do zasobów konta związanego bezpośrednio z pracą zdalną, szczególnie gdy np. charakter „e-szkolenia" może uwzględniać udostępnianie pulpitu pomiędzy uczestnikami a prowadzącym;
- wykorzystywanie popularnych platform do spotkań online instalowanych w systemie operacyjnym powinno opierać się o aktualne wersje oraz konfigurację zgodną z zaleceniami producenta. W przypadku platform do wideokonferencji uruchamianych z poziomu przeglądarki, tzw. WEB'owych, należy zwrócić uwagę nie tylko na aktualizację samej przeglądarki, ale także na zainstalowane wtyczki/rozszerzenia, które mogą dawać nieuprawniony dostęp do zawartości strony;
- najważniejszym aspektem jest ochrona strumieni przesyłanych danych. Bezpieczeństwo wideokonferencji powinno być zabezpieczone protokołem HTTPS z zaufanym certyfikatem lub ewentualnie wykorzystany tunel VPN w przypadku środowiska serwerowego pod pełną kontrolą organizatora;

- adres URL do wideokonferencji powinien być unikatowy i trudny do odgadnięcia oraz niedostępny publicznie;
- oprócz logowania poprzez adres e-mail i unikatowe hasło (hasło powinno być przede wszystkim długie oraz niesłownikowe), rekomendowane jest również uwierzytelnienie dwuskładnikowe (2FA) np. kod wysłany poprzez SMS czy sprzętowy token lub aplikację.

9. PODSUMOWANIE



W 2020 roku, Zespół CSIRT GOV po raz kolejny zarejestrował najwyższą liczbę zgłoszeń klasyfikowanych jako podejrzenie wystąpienia incydentów bezpieczeństwa teleinformatycznego, co przełożyło się również na najwyższą liczbę samych incydentów. W konsekwencji zarejestrowano 246 107 zgłoszeń o potencjalnym wystąpieniu incydentu teleinformatycznego w instytucjach administracji publicznej oraz operatorów infrastruktury krytycznej. Jest to znaczny wzrost, szczególnie biorąc pod uwagę sytuację pandemiczną w 2020 roku i związane z nią restrykcje oraz obostrzenia dotyczące zarówno wielu obszarów gospodarki jak i samej administracji publicznej. Liczba zdarzeń, która została zakwalifikowana jako faktyczny incydent bezpieczeństwa wyniosła 23 309, co stanowi prawie dwukrotny wzrost względem roku 2019, kiedy to odnotowano 12 405 przypadków naruszenia bezpieczeństwa teleinformatycznego. Zgodnie z klasyfikacją incydentów, tak jak w latach poprzednich, najwyższe miejsce w ramach zarejestrowanych incydentów przypadło zdarzeniom w kategorii WIRUS związanym z wykryciem działania szeroko pojętego szkodliwego oprogramowania. W 2020 roku zarejestrowanych zostało aż 16 777 incydentów tego typu. W ciągu ostatniego roku Zespół CSIRT GOV odnotował także znacznie zwiększoną liczbę incydentów skategoryzowanych jako PHISHING, gdzie ilość ta w 2020 roku była wyższa o blisko 19% w stosunku do roku 2019. Dodatkowo, Zespół CSIRT GOV w 2020 roku odnotował wzrostową tendencję incydentów typu SKANOWANIE. Wynika to w dużej mierze z alarmów systemu ARAKIS 3.0 GOV i dotyczy złośliwego lub podejrzanego ruchu skierowanego na adresację podmiotów podległych CSIRT GOV.

W 2020 roku zidentyfikowano także zagrożenia o charakterze międzynarodowym, które wystąpiły w polskiej cyberprzestrzeni. Wśród nich na uwagę zasługuje m.in. aktywność tzw. grup APT – Advanced Persistent Threat. Przeprowadzone czynności analityczne wykazały, że część z nich prowadziła swoje wrogie działania także wobec podmiotów, będących

we właściwości Zespołu CSIRT GOV, np. APT Kimsuky, APT Gamaredon, APT36, czy APT 41. Miniony rok to również znaczny wzrost incydentów typu PHISHING ujawnianych w podmiotach państwowych jak i infrastrukturze krytycznej. Organy państwa stały się celem wielu ataków tego typu zagrożeń, które występowały na szeroką skalę w sieci Internet, gdzie wykorzystywano wizerunek popularnych dostawców telekomunikacyjnych, bądź przewozów kurierskich. Na uwagę zasługuje także fakt, iż występująca sytuacja pandemiczna i związane z nią doniesienia medialne, były często wykorzystywane jako motywy w atakach socjotechnicznych ukierunkowanych na użytkowników polskiej cyberprzestrzeni.

W roku 2020 system wczesnego ostrzegania o zagrożeniach teleinformatycznych ARAKIS 3.0 GOV odnotował 1 813 243 995 przepływów, co przełożyło się na 1 758 813 wygenerowanych przez system alarmów. Ponownie, powyższe dane stanowią znaczny wzrost w porównaniu do roku ubiegłego. Jednakże należy zaznaczyć, iż ponad dwukrotny wzrost w liczbie wygenerowanych alarmów dotyczył alarmów o priorytecie niskim oraz średnim, na co miał wpływ dużo większy udział alarmów typu 2 – skanowanie. Dodatkowo, w stosunku do roku ubiegłego, dostrzec można znaczne zmniejszenie ilości wygenerowanych alarmów typu 1 - komunikacji do złośliwych serwerów oraz typu 3 – wykrytych znanych ataków. Ponownie, jak w roku ubiegłym, do państw, które wygenerowały największą ilość przepływów, można zaliczyć Rosję oraz USA.

W wyniku przeprowadzonych w 2020 roku ocen bezpieczeństwa systemów teleinformatycznych instytucji administracji rządowej oraz infrastruktury krytycznej, Zespół CSIRT GOV dokonał identyfikacji szeregu podatności w systemach podlegających ocenie, począwszy od błędów informacyjnych aż do podatności posiadających status krytycznych. W roku 2020 Zespół CSIRT GOV przeprowadził ocenę bezpieczeństwa 82 systemów

teleinformatycznych, należących do 14 instytucji administracji rządowej oraz infrastruktury krytycznej.

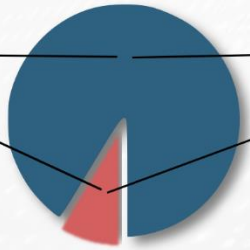
W wyniku przeprowadzonych testów bezpieczeństwa zidentyfikowano łącznie 4 325 podatności, w tym 95 podatności o stopniu krytycznym oraz 223 o stopniu wysokim, co mogło skutkować przełamaniem zabezpieczeń przez atakujących i tym samym prowadzić do eskalacji ataku. Ponownie, do najistotniejszych (krytycznych oraz wysokich) podatności zidentyfikowanych w ramach przeprowadzonych ocen bezpieczeństwa systemów teleinformatycznych należały wersje oprogramowania zawierające podatności, których ujawnienie często było spowodowane wykorzystywaniem ich nieaktualnych wersji.

Spis tabel:

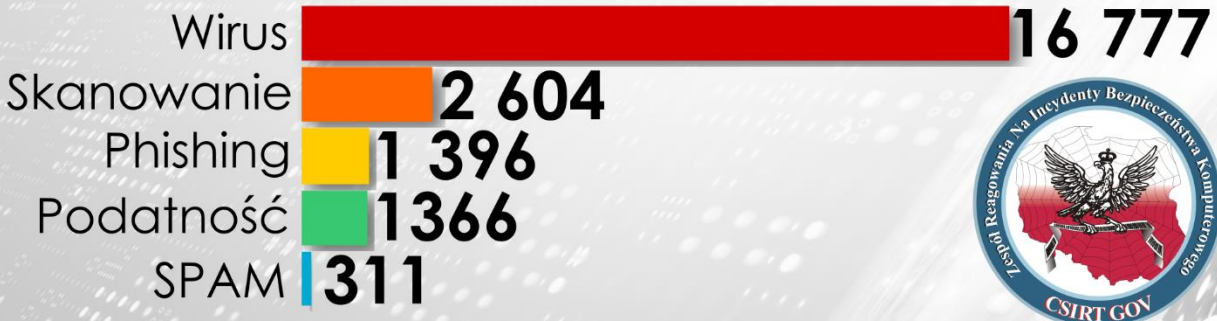
Spis wykresów:

Zgłoszone incydenty: **246 107**

Faktyczne incydenty: **23 309**



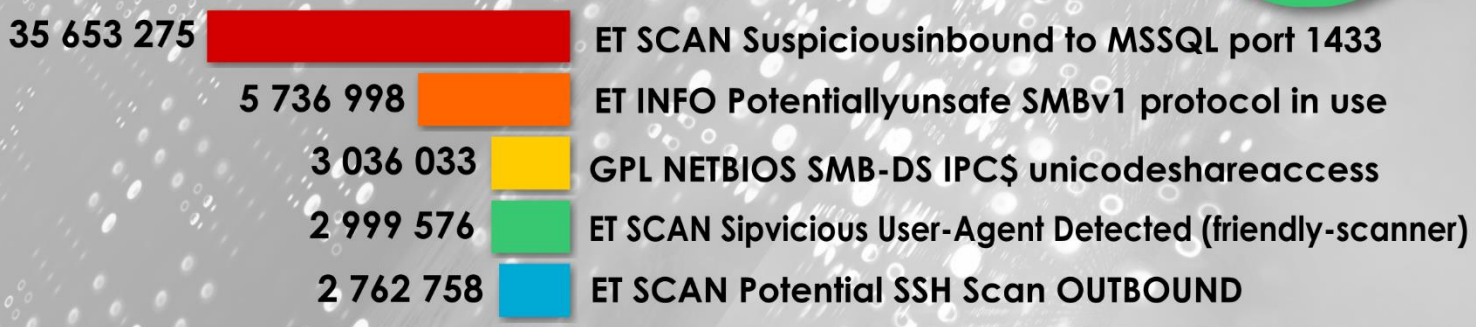
TOP 5 incydentów



Zespół Reagowania Na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV

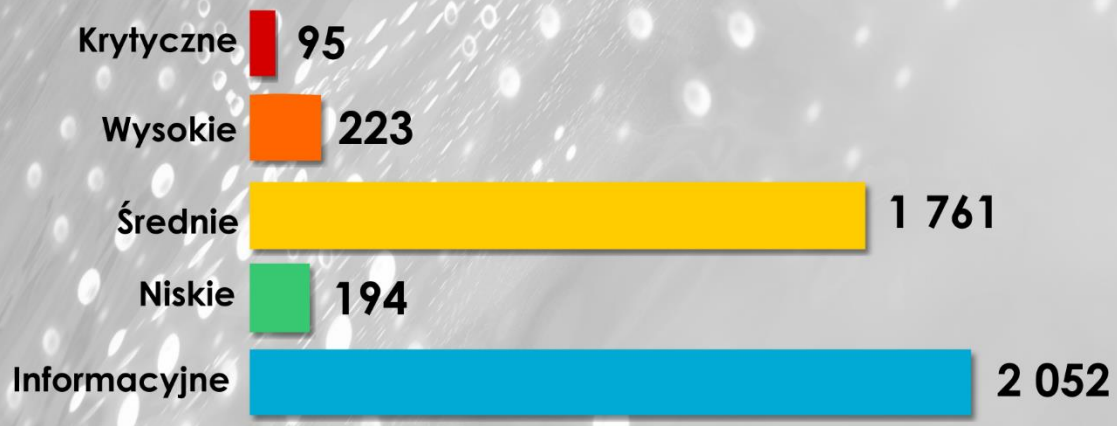
arakis GOV

TOP 5 dopasowań reguł do obserwowanego ruchu sieciowego



Ocena bezpieczeństwa systemów TI

Zestawienie zidentyfikowanych podatności z podziałem na priorytet



Zainteresowanych służbą lub pracą
w Zespole Reagowania Na Incydenty
Bezpieczeństwa Komputerowego
CSIRT GOV prosimy o kontakt:

praca@csirt.gov.pl

Dodatkowe informacje:

Wymagania:

- Wykształcenie techniczne (informatyka, elektronika, telekomunikacja) lub studenci ostatnich lat studiów
- Znajomość systemów operacyjnych rodziny Windows, Unix i Linux na poziomie administracyjnym
- Bardzo dobra znajomość działania protokołów sieci TCP/IP
- Bardzo dobra znajomość tematyki zagrożeń dla bezpieczeństwa teleinformatycznego oraz metod ich neutralizowania
- Znajomość języka angielskiego na poziomie komunikatywnym