RAPORT O STANIE BEZPIECZEŃSTWA CYBERPRZESTRZENI RP W 2021 ROKU

RAPORT O STANIE BEZPIECZEŃSTWA CYBERPRZESTRZENI RP W 2021 ROKU

WARSZAWA, LIPIEC 2022

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

1. STATYSTYKI INCYDENTÓW KOORDYNOWANYCH PRZEZ ZESPÓŁ CSIRT GOV....8
2. ZAGROŻENIA ZIDENTYFIKOWANE W 2021 ROKU....18
3. ZAGROŻENIA - OPROGRAMOWANIE ZŁOŚLIWE....31
4. ARAKIS GOV....37
5. OCENA BEZPIECZEŃSTWA SYSTEMÓW TI....43
6. PROAKTYWNE DZIAŁANIA ZESPOŁU CSIRT GOV....53
7. ZAGROŻENIA DLA OBSZARU INFRASTRUKTURY KRYTYCZNEJ....57
8. PODSUMOWANIE....63

WSTĘP

Raport o stanie bezpieczeństwa cyberprzestrzeni RP wydawany jest corocznie przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV w celu przedstawienia zagrożeń i incydentów w cyberprzestrzeni RP dotyczących organów państwa, administracji państwowej oraz infrastruktury krytycznej. W Raporcie prezentowane są dane statystyczne dotyczące incydentów obsłużonych przez Zespół CSIRT GOV wraz z ich krótką charakterystyką.

Informacje zawarte w Raporcie służą przedstawieniu głównych rodzajów zagrożeń rozpoznawanych przez Zespół CSIRT GOV, co tym samym powinno przyczyniać się do podnoszenia poziomu bezpieczeństwa systemów teleinformatycznych w instytucjach państwowych, administracji publicznej czy infrastruktury krytycznej.

Przedmiotowy Raport powstał na podstawie danych 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 GOV, jak również ustaleń własnych.

W 2021 roku Zespół CSIRT GOV odnotował 762 175 zgłoszeń dotyczących potencjalnego wystąpienia incydentu teleinformatycznego, z czego 26 899 okazało się faktycznym incydentem. Wzrost liczby zgłoszeń w stosunku do 2020 roku jest ponad trzykrotny i wynika w głównej mierze z zagrożeń wykrywanych przez system ARAKIS GOV.

Szczegóły dotyczące analizy statystyk incydentów w poszczególnych kwartałach 2021 roku, opis najważniejszych zagrożeń cyberbezpieczeństwa i podatności, a także informacja na temat dystrybucji ostrzeżeń przez Zespół CSIRT GOV zostały umieszczone w rozdziale pierwszym Raportu.

W rozdziale drugim Raportu znajdują się informacje dotyczące zagrożeń bezpieczeństwa systemów teleinformatycznych, które wystąpiły w 2021 roku zarówno na świecie, jak i w Polsce. Znalazły się tam między innymi opisy podatności Apache Log4J w bibliotece języka Java, ProxyLogon i Proxyshell dotyczące

oprogramowania Microsoft Exchange, jak również przedstawiono ataki wykorzystujące socjotechnikę. Opisane zostały kampanie phishingowe - ataki wykorzystujące inżynierię społeczną, których narastający trend jest obserwowany już od 2019 roku i stanowi jeden z głównych wektorów ataków stosowanych przez cyberprzestępców. Znalazły się tam także informacje na temat długofalowych kampanii APT, których działania monitorowane są na bieżąco przez CSIRT GOV.

W rozdziale trzecim Raportu przedstawione zostały wyniki analizy ponad 7 tysięcy plików zgłoszonych przez podmioty do Zespołu CSIRT GOV. Wymieniono wykorzystywane w niniejszych plikach złośliwe oprogramowanie, przedstawiono charakterystykę ich działania i omówiono cechy badanych próbek.

Raport zawiera również statystyki pochodzące z ARAKIS GOV - systemu 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 2021 roku w sieciach teleinformatycznych podmiotów uczestniczących w projekcie ARAKIS GOV zanotowano łącznie 1 758 708 908 przepływów, co przełożyło się na 3 366 360 wygenerowanych przez system alarmów.

W Raporcie zawarto 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. Mają one na celu identyfikację istotnych podatności wpływających na bezpieczeństwo infrastruktury teleinformatycznej podmiotów.

Dodatkowo, opublikowano informacje o udziale przedstawicieli CSIRT GOV w ćwiczeniach dot. cyberbezpieczeństwa, udziale w konsultacjach dotyczących wypracowania rekomendacji wzmacniających cyberbezpieczeństwo w sektorze energii oraz stosownych wytycznych sektorowych dotyczących zgłaszania incydentów TI.

Przedstawione zostały także aspekty cyberbezpieczeństwa infrastruktury przemysłowej OT, na które należy zwrócić uwagę w ramach zarządzania jej cyberbezpieczeństwem.

Reasumując, coroczny Raport Zespołu CSIRT GOV o stanie bezpieczeń-

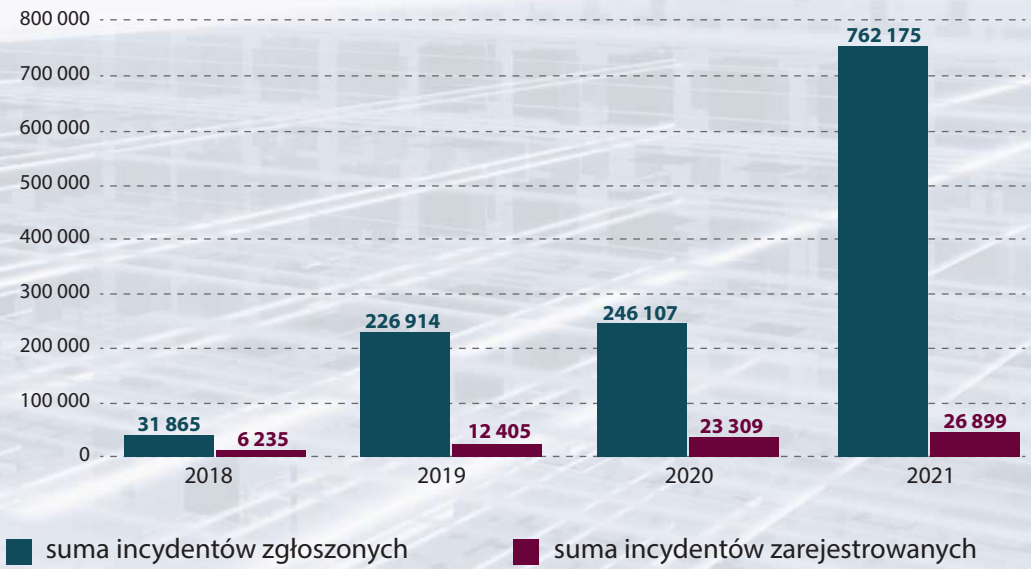
stwa cyberprzestrzeni RP ma przede wszystkim na celu podnoszenie świadomości użytkowników na temat zagrożeń i podatności występujących w systemach teleinformatycznych. Ukierunkowany jest na podwyższanie poziomu bezpieczeństwa systemów oraz na wdrożenie odpowiednich działań ograniczających możliwość eskalacji wystąpienia potencjalnego zagrożenia.

1. STATYSTYKI INCYDENTÓW KOORDYNOWANYCH PRZEZ ZESPÓŁ CSIRT GOV

1.1 STATYSTYKA ROCZNA

W 2021 roku Zespół CSIRT GOV zarejestrował w sumie 762 175 zgłoszeń o potencjalnym wystąpieniu incydentu teleinformatycznego, spośród których 26 899 zostało uznanych za incydenty. Poniżej przedstawione i omówione zostały statystyki dotyczące liczby zgłoszeń w porównaniu do lat poprzednich wraz z podziałem na kategorie incydentów oraz rodzaj instytucji.

W 2021 roku zarejestrowano ponad trzykrotnie więcej zgłoszeń w stosunku do roku poprzedniego, gdzie w sumie zarejestrowano 246 107 zgłoszeń. Wzrost zarejestrowanych zgłoszeń wynika przede wszystkim z liczby alarmów generowanych przez system ARAKIS GOV. System ARAKIS GOV umożliwia identyfikowanie zagrożeń m.in. na podstawie dedykowanych sygnatur bezpieczeństwa. Stałe zasilanie systemu ARAKIS w nowe sygnatury, jak również zwiększająca się liczba zainstalowanych sond, skutkują większą detekcją, a co za tym



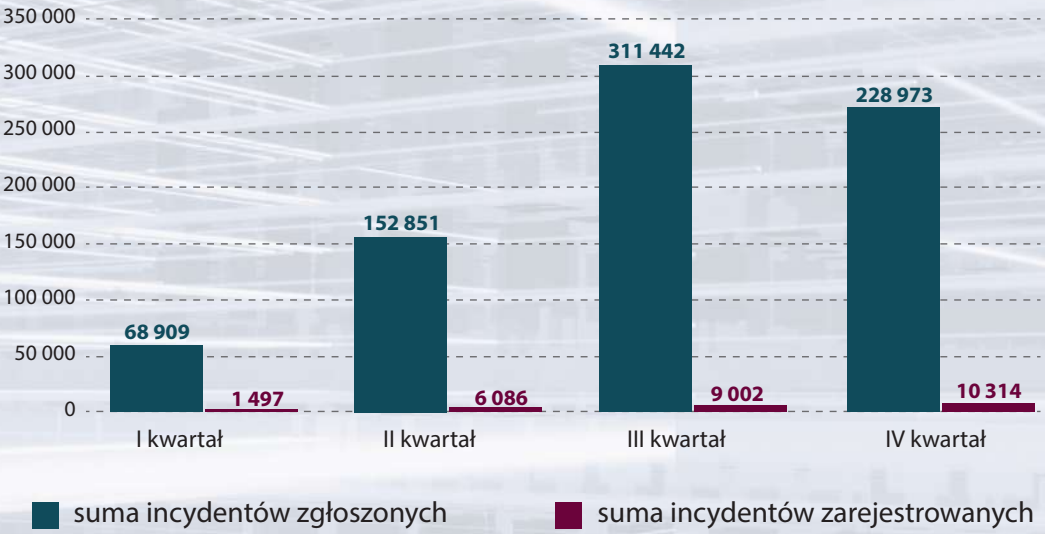
Wykres 1. Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych latach

idzie - większą liczbą generowanych zgłoszeń. Z analizą zagrożeń rozpoznawanych przez system ARAKIS GOV można zapoznać się w rozdziale nr 4.

Spośród ponad 760 tys. zgłoszeń w 2021 roku zarejestrowano 26 899 incydentów. Stanowi to wzrost o około 15% w porównaniu do poprzedniego roku, gdzie zidentyfikowano 23 309 incydentów. Zebrane statystyki wskazują na utrzymującą się tendencję wzrostową zarówno wpływających zgłoszeń, jak również zarejestrowanych incydentów. Wśród stałych czynników mających wpływ na obserwowany poziom cyberzagrożeń jest, z jednej strony, szerokie wykorzystanie cyberprzestrzeni do utrzymywania ciągłości działania różnego rodzaju usług elektronicznych, zapewnienia ciągłości działania procesów biznesowych, wykorzystania cyberprzestrzeni do komunikacji i działalności statutowej instytucji i podmiotów. Z drugiej strony natomiast czynnikiem kształtującym wskazaną tendencję jest postępujący rozwój taktyk i technik wykorzystywanych przez cyberprzestępców starających się wykorzystywać nowe oraz znane już podatności, a także stosujących zaawansowane wektory ataku. Wśród okoliczności, które w 2021 roku nie pozostawały bez wpływu na liczbę incydentów, był także utrzymujący się stan pandemii wirusa SARS-CoV-2, a powiązane z nią motywy wykorzystywane były do przeprowadzania ataków phishingowych. W 2021 roku odnotowano różnego rodzaju incydenty socjotechniczne z wykorzystaniem tematyki szczepień, certyfikatów szczepień, a także testów epidemicznych. Zostały także zidentyfikowane incydenty takie jak ransomware, vishing czy spoofing telefoniczny.

1.2 ANALIZA POSZCZEGÓLNYCH KWARTAŁÓW

Spośród analizowanych kwartałów należy wskazać, iż w III kwartale zarejestrowanych zostało najwięcej zgłoszeń, tj. 311 442. Liczba ta była w głównej mierze wynikiem zwiększonej liczby alarmów systemu ARAKIS GOV.



Wykres 2. Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych kwartałach 2021 r.

Jeśli chodzi o zarejestrowane incydenty, to zauważalny jest wzrost liczby rejestrowanych incydentów wraz z kolejnymi kwartałami. Najwyższy wzrost odnotowano pomiędzy I a II kwartałem 2021 roku, natomiast najwięcej incydentów (10 314), zarejestrowano w IV kwartale 2021 roku.

Zespół CSIRT GOV w 2021 roku zarejestrował także zwiększoną liczbę incydentów, które związane były z ujawnianymi podatnościami, wskazywanymi jako szczególnie istotne dla bezpieczeństwa infrastruktury teleinformatycznej z uwagi na ogólnie szerokie wykorzystanie podatnego oprogramowania wśród podmiotów wchodzących w zakres obszaru instytucjonalnego odpowiedzialności Zespołu CSIRT GOV.

Charakteryzując zwłaszcza kwestię ujawnianych podatności należy zauważyć, że na początku I kwartału 2021 roku, w dalszym ciągu identyfikowane były zagrożenia związane z naruszeniem bezpieczeństwa oprogramowania SolarWinds Orion. Zagrożenie to zostało nagłośnione w grudniu 2020 roku. Oprogramowanie to przeznaczone jest do zarządzania i monitorowania pracy infra-

struktury serwerowej. Atak przeprowadzany był za pomocą aplikacji SolarWinds Orion, gdzie zidentyfikowano kod złośliwy. W cyfrowo podpisanej bibliotece SolarWinds.Orion.Core.BusinessLayer.dll, znajdował się kod zawierający backdoor, który za pomocą protokołu HTTP kontaktował się z serwerami C2. Aktualizacje do oprogramowania SolarWinds Orion z zaimplementowanym złośliwym kodem pojawiały się na oficjalnej stronie SolarWinds od marca do maja 2020. Przeprowadzone przez CSIRT GOV działania pozwoliły ustalić, iż nie wykryto skutecznego wykorzystania przedmiotowej podatności w obszarze będącym we właściwości Zespołu.

Kolejnym zagrożeniem wykrytym w 2021 roku, które pojawiło się na przełomie II i III kwartału, była krytyczna podatność Proxy Logon w MS Exchange Server (wersje 2013, 2016, 2019). Podatność dotyczyła możliwości umieszczenia na serwerze webowym (będącym częścią Exchange'a) spreparowanego pliku aspx, działającego jako webshell. Przekazywane parametry w wysyłanym żądaniu używane były do wykonywania kodu po stronie serwera. Ataki związane były z czterema lukami w zabezpieczeniach oznaczonymi poniższymi sygnaturami:

- CVE-2021-26855;
- CVE-2021-26857;
- CVE-2021-26858 i CVE-2021-27065.

Incydenty dotyczące wskazanej podatności identyfikowane były także w obszarze właściwości CSIRT GOV. Analiza przeprowadzona odnośnie podatnych serwerów MS Exchange pozwoliła ustalić, iż w żadnej z instytucji będącej we właściwości CSIRT GOV nie doszło do przełamania zabezpieczeń. W jednym z incydentów zaobserwowano próby połączeń, gdzie ruch sieciowy odbywał się za pośrednictwem protokołu HTTP wraz z TLSv1.2. W innym przypadku zidentyfikowano rekonesans infrastruktury pod kątem możliwości wykorzystania przedmiotowej podatności.

We wrześniu 2021 roku pojawiła się kolejna informacja dotycząca podatności w MS Exchange Server. Zagrożenie dotyczyło masowego skanowania serwerów poczty elektronicznej Microsoft Exchange w poszukiwaniu łańcucha podatności, które zbiorczo zostały określone jako ProxyShell. ProxyShell dotyczyło w zasadzie trzech podatności, które umożliwiały między innymi zdalne wykonanie nieuwierzytelnionego kodu na serwerach Microsoft Exchange, tj.:

- CVE-2021-34473;
- CVE-2021-34523;
- CVE-2021-31207.

Zespół CSIRT GOV w toku przeprowadzonych działań prowadził czynności mające na celu wsparcie podmiotów w obsłudze incydentu celem identyfikacji podatności i przeprowadzenia kroków pozwalających na wdrożenie środków mitygujących.

W grudniu 2021 roku wykryta została podatność w bibliotece Apache Log4j, w wersjach od 2.0-alpha1 do 2.17.0 włącznie, z wyłączeniem wersji 2.12.4. Podatności pozwalały m.in. na zdalne wykonanie kodu z uprawnieniami danej aplikacji, np. webserwera wykorzystującego Log4j. Pierwotnie rozpoznana została tylko jedna z podatności Log4Shell o sygnaturze CVE-2021-44228, po czym odnotowywano kolejne, które nadal stanowiły zagrożenie w kontekście eksploitacji. W sumie zarejestrowano kilka podatności:

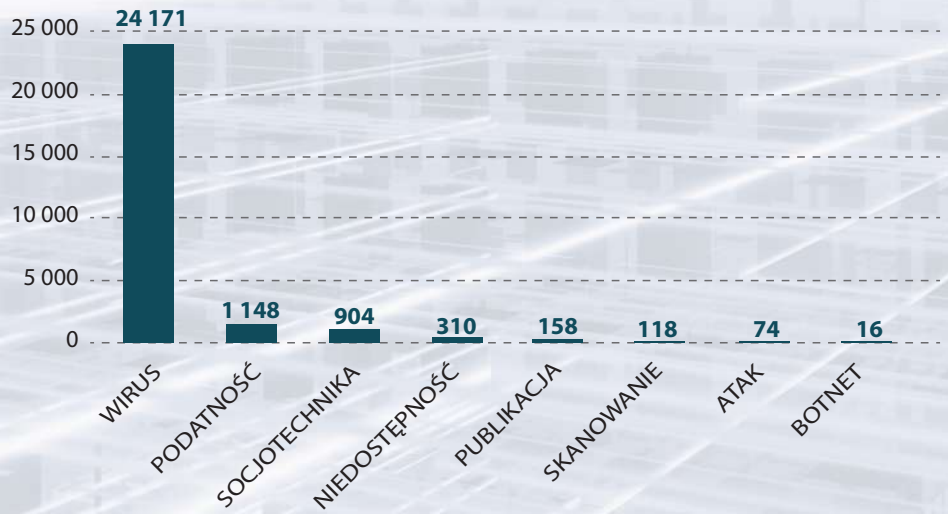
- CVE-2021-44228;
- CVE-2021-45046;
- CVE-2021-45105;
- CVE-2021-44832.

W związku z tym, iż przedmiotowa podatność została uznana za jedną z najbardziej krytycznych podatności dla infrastruktury serwerowej, zwłaszcza dostępnej w sieci Internet, i dotyczyła wielu usług, miała miejsce koordynacja incydentu w ramach Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego poziomu krajowego, tj. CSIRT GOV, CSIRT MON oraz CSIRT NASK. Podatność ta uznana została jako potencjalnie szeroko odziaływująca na cyberbezpieczeństwo o potencjalnie dużym zasięgu.

W IV kwartale 2021 w okresie od 5 grudnia 2021 r. do 10 grudnia 2021 r., Zespół CSIRT GOV wykonywał także zadania związane z wprowadzeniem stopnia alarmowego ALFA-CRP. Stopień alarmowy został wprowadzony w związku z organizacją Szczytu Cyfrowego ONZ – IGF 2021 (the UN Internet Governance Forum).

1.3 STATYSTYKA INCYDENTÓW POD WZGLĘDEM KATEGORII INCYDENTÓW

Poniżej przedstawiono statystykę dotyczącą rodzajów kategorii zarejestrowanych incydentów przez Zespół CSIRT GOV w roku 2021. W ubiegłym roku najwięcej incydentów sklasyfikowano jako WIRUS, PODATNOŚĆ oraz SOCJOTECHNIKA. W ramach kategorii WIRUS zidentyfikowano 24 171 incydentów. Wiąże się to z alarmami pochodzącymi z systemu wczesnego ostrzegania o zagrożeniach pochodzących z sieci Internet ARAKIS GOV. Przedmiotowe alarmy mogą świadczyć o infekcji stacji roboczych, jak również serwerów w instytucjach administracji państwowej lub u operatorów infrastruktury krytycznej. Wzrastająca liczba incydentów zawartych w tej kategorii spowodowana jest aktualizowaną bazą IoC (ang. Indicators of Compromise) o najnowsze wskaźniki kompromitacji. Baza ta wzbogacana jest o IoC pochodzące zarówno z własnych ustaleń jak również źródeł zewnętrznych o znanej reputacji. Na ilość incydentów typu WIRUS wpływ ma także rozwój systemu ARAKIS GOV obejmujący nowe instancje w instytucjach.



Wykres 3. Statystyka incydentów w 2021 roku z podziałem na kategorie

Druga najliczniejsza kategoria to PODATNOŚĆ, w ramach której zidentyfikowano 1 148 incydentów w zasobach IT rozumianych jako słabość systemu teleinformatycznego, błędy konfiguracyjne oraz brak odpowiedniej polityki bezpieczeństwa, związanej z aktualizacją oraz weryfikacją poprawnie wdrożonych

rozwiązań teleinformatycznych. Ta kategoria objęła m.in. incydenty związane z podatnościami MS Exchange oraz Log4j.

Trzecią najliczniejszą kategorią jest SOCJOTECHNIKA obejmująca 904 incydenty. Zagrożenia te dotyczą kampanii phishingowych, podszywania się oraz ataków z zakresu inżynierii społecznej wymierzonych przeciwko użytkownikom systemów teleinformatycznych, które mają na celu wyłudzenie poufnych informacji, zainfekowanie komputera złośliwym oprogramowaniem, bądź nakłonienie użytkownika do określonych działań. W tej kategorii najwięcej incydentów dotyczyło podszywania się pod witryny internetowe wykorzystujące wizerunek podmiotu, często mających na celu wyłudzenie środków finansowych bądź danych logowania.

Następną kategorią jest NIEDOSTĘPNOŚĆ (310 zarejestrowanych incydentów). Tę kategorię obejmują zdarzenia dotyczące niedostępności witryn internetowych, awarii technicznych oraz prac technicznych.

W kategorii PUBLIKACJA zarejestrowano 158 incydentów obejmujących zgłoszenia dotyczące wycieków, publikacji w sieci wykradzionych informacji, dezinformacji, zniesławienia czy naruszenia praw autorskich.

Kolejna kategoria SKANOWANIE objęła 118 incydentów dotyczących rekonesansu infrastruktury teleinformatycznej administracji rządowej oraz infrastruktury krytycznej.

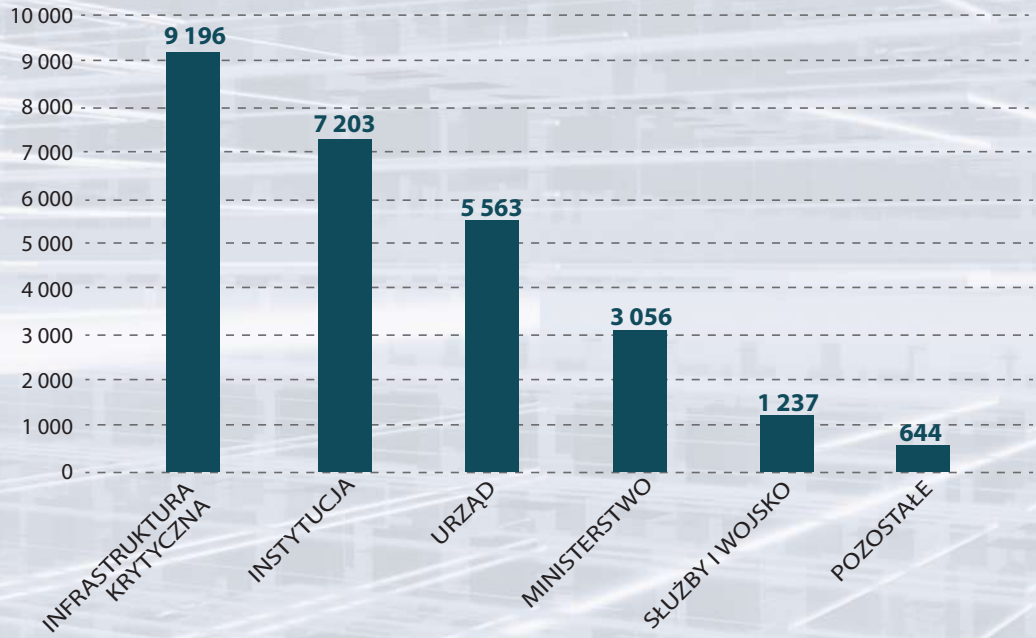
W kategorii ATAK zgłoszone zostały 74 incydenty związane z wszelkiego rodzaju przeprowadzanymi atakami na systemy teleinformatyczne np. DDoS, DoS, przełamanie zabezpieczeń.

W ramach ostatniej kategorii BOTNET zarejestrowano w sumie 16 incydentów, czyli zagrożeń dotyczących identyfikacji komputerów należących do sieci przejętych komputerów.

Poza wyżej wymienionymi kategoriami, które ujęte są jako kategorie dotyczące stricte faktycznych incydentów obsługiwanych przez CSIRT GOV, odnotowano również 846 incydentów nie będących we właściwości Zespołu CSIRT GOV. Zostały one przekazane zgodnie z ustawą z dnia 5 lipca o krajowym systemie cyberbezpieczeństwa do odpowiednich CSIRT-ów poziomu krajowego. Zespół CSIRT GOV otrzymywał również wiadomości dotyczące wyznaczenia osób do kontaktów, zawierające formularze zgłoszenia osób do kontaktów z CSIRT GOV. W ubiegłym roku otrzymano 117 wiadomości, w których zgłoszono lub zaktualizowano osoby wskazane do kontaktu.

1.4 STATYSTYKA INCYDENTÓW POD WZGLĘDEM SEKTORÓW

Patrząc na statystykę zgłaszania incydentów z podziałem na poszczególne sektory, zaobserwować można, że w 2021 roku najwięcej zgłoszeń dotyczyło operatorów infrastruktury krytycznej – 9196 zarejestrowanych incydentów. Jest to znaczący wzrost w stosunku do poprzedniego roku, gdzie incydentów dotyczących infrastruktury krytycznej odnotowano w sumie 2626.

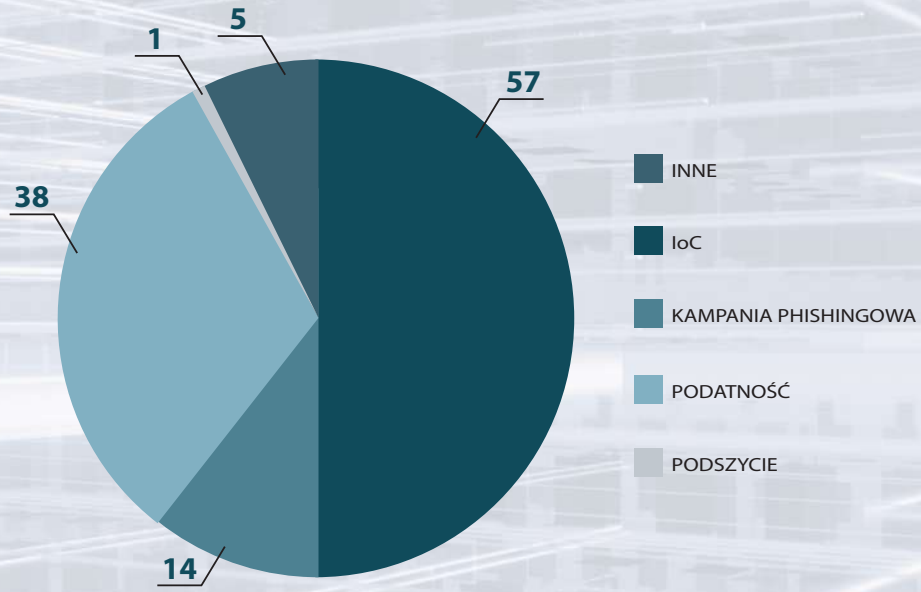


Wykres 4. Liczba incydentów wg sektorów

Kolejnymi sektorami pod względem liczby zarejestrowanych zgłoszeń były instytucje (7203 zgłoszenia) oraz urzędy, gdzie zidentyfikowano 5563 incydenty.

1.5 OSTRZEŻENIA DYSTRYBUOWANE PRZEZ CSIRT GOV W 2021 ROKU

Zespół CSIRT GOV w ramach działań mitygujących zagrożenia przesyła ostrzeżenia do organów państwowych oraz operatorów infrastruktury krytycznej zawierające informacje dotyczące zidentyfikowanych zagrożeń wraz ze wskaźnikami kompromitacji. W 2021 roku zostało rozdystrybuowanych w sumie 115 takich ostrzeżeń.



Wykres 5. Ostrzeżenia wysłane przez Zespół CSIRT GOV

Najwięcej ostrzeżeń – 57, dotyczyło informacji o IoC, czyli o wskaźnikach kompromitacji zidentyfikowanych zagrożeń, np. IoC dotyczących złośliwego ruchu sieciowego czy podejrzanych domen. Kolejną grupą ostrzeżeń były informacje na temat podatności, między innymi informacje na temat wykrytych podatności w różnego rodzaju oprogramowaniach i systemach. W tej kategorii znajdowały się ostrzeżenia o podatnościach związanych z oprogramowaniem SolarWinds (na początku roku rozdystrybuowano dwa ostrzeżenia), podatności ProxyLogon oraz ProxyShell w Microsoft Exchange Server (rozdystrybuowano 7 ostrzeżeń), a także krytycznej podatności w bibliotece Apache Log4j (przesłano 11 ostrzeżeń). Ostrzeżeń o zidentyfikowanych kampaniach phishingowych rozesłano w sumie 14. Rozdysponowano także 5 ostrzeżeń zawierających się w kategorii Inne, które informowały, np. o wprowadzeniu stopnia alarmowego ALFA-CRP. Wystosowano także jedno ostrzeżenie o zagrożeniu dotyczącym podszycia.

2. ZAGROŻENIA ZIDENTYFIKOWANE W 2021 ROKU

2.1 OGÓLNA CHARAKTERYSTYKA ZAGROŻEŃ ORAZ ATAKÓW, JAKIE WYSTĘPOWAŁY NA ŚWIECIE W 2021 ROKU

W roku 2021 na świecie odnotowano kilka krytycznych podatności, które dotyczyły niekiedy także bardzo popularnego i szeroko stosowanego, również w administracji publicznej, oprogramowania.

W pierwszej kolejności można tutaj wymienić podatność o nazwie ProxyLogon, dotyczącą oprogramowania Microsoft Exchange, która wystąpiła na początku 2021 roku. Należy także zaznaczyć, że na przestrzeni kilku miesięcy po jej ujawnieniu wskazana podatność była wykorzystywana przez różnych aktorów oraz grupy cyberprzestępcze. Pomimo wydania stosownej aktualizacji w marcu 2021 roku, już we wrześniu opublikowany został kolejny łańcuch podatności, który dotyczył oprogramowania MS Exchange nazwany tym razem Proxyshell. Przedmiotowa podatność umożliwiała wykonanie na podatnym serwerze zdalnego kodu z uprawnieniami systemowymi.

Ponadto, 2021 rok na świecie charakteryzował się licznymi atakami typu ransomware. Spośród znanych infekcji, w szczególności odnotowano atak na infrastrukturę sieci Colonial Pipeline – jednego z największych amerykańskich rurociągów naftowych. Z informacji udostępnionych w źródłach otwartych wynikało, że w wyniku powyższego ataku doszło do czasowego wstrzymania przesyłu paliw oraz wycieku danych z zaatakowanego przedsiębiorstwa.

Pod koniec 2021 roku miało także miejsce ujawnienia podatności w szeroko stosowanej bibliotece języka Java o nazwie Apache Log4J, która również stała się krytyczną z uwagi na powszechne jej wykorzystanie w aplikacjach sieciowych dostępnych w sieci Internet, jak również w wielu produktach komercyjnych.

Poza grupą powyższych, relatywnie nowych zagrożeń i ataków, występowały także stałe zagrożenia atakami socjotechnicznymi, w szczególności mającymi na celu kradzież danych uwierzytelniających, bądź infekcję szkodliwym oprogramowaniem.

2.2 GŁÓWNE ZAGROŻENIA I PODATNOŚCI, JAKIE WYSTĄPIŁY W 2021 ROKU W OBSZARZE DZIAŁANIA CSIRT GOV

Ze swojej strony Zespół CSIRT GOV prowadził szereg działań, związanych ze zidentyfikowanymi podatnościami. Działania te polegały na obsłudze incydentów, publikacji ostrzeżeń, biuletynów, jak również wydawania rekomendacji.

Proxylogon

Po uzyskaniu informacji o wystąpieniu nowej podatności, sklasyfikowanej, jako krytyczna, dotyczącej serwera poczty elektronicznej Microsoft Exchange, Zespół CSIRT rozdysponował ostrzeżenie do wszystkich, będących we właściwości CSIRT GOV podmiotów. Powyższa podatność pozwalała na nieuprawniony odczyt zawartości kont email oraz zdalne wykonanie kodu na podatnym serwerze.

W wyniku własnych ustaleń Zespół CSIRT GOV zidentyfikował, określoną liczbę, pozostających we właściwości Zespołu CSIRT GOV serwerów, które zostały uznane jako podatne, co mogło skutkować przełamaniem ich zabezpieczeń. Podjęte działania pozwoliły na przeprowadzenie właściwych aktualizacji przez wytypowane instytucje i podmioty, tym samym ograniczyły możliwość eksploitacji ich serwerów. W ramach działań mitygujących ustalono próby połączeń na serwer Microsoft Exchange jednej z instytucji. Zarejestrowane próby szkodliwych połączeń odbywały się z adresów IP, przypisanych m.in. do Chin oraz Indii. Dodatkowo, zidentyfikowano jeden podmiot, który odnotował liczne próby rekonesansu, jednakże skutecznie zablokowane na systemach zaporowych.

Proxyshell

We wrześniu 2021 roku światło dzienne ujrzał kolejny łańcuch podatności dotyczący środowiska Microsoft Exchange, zbiorczo określony jako Proxyshell. Wskazana luka pozwalała atakującemu na zdalne wykonanie kodu na podatnym serwerze bez konieczności przeprowadzenia procesu uwierzytelnienia, tym samym podatność ta została sklasyfikowana jako krytyczna. Zespół CSIRT GOV z początkiem września 2021 roku rozesłał pomiędzy organy państwowe oraz podmioty infrastruktury krytycznej szereg ostrzeżeń, zawierających opis wspomnianych podatności, jak również listę adresów IP, które zgodnie z posiadaną wiedzą były wykorzystywane w zakresie rekonesansu. Lista adresów IP była suk-

cesywnie poszerzana o nowe adresacje wykryte jako uczestniczące w rekonesansie lub eksploitacji podatności.

W sumie opublikowano 5 ostrzeżeń, w wyniku których otrzymano odpowiedź od kilkudziesięciu podmiotów. Dziewięć podmiotów zidentyfikowało połączenia do swoich serwerów ze wskazanych w ostrzeżeniach Zespołu CSIRT GOV złośliwych adresów IP. Dalsza analiza, w szczególności otrzymanych danych logowania, wykazała, że doszło do próby kompromitacji serwera Microsoft Exchange w jednej z instytucji. W związku z powyższym, Zespół CSIRT GOV niezwłocznie przeprowadził stosowną analizę powłamaniową, w wyniku której instytucja przeprowadziła, z uwzględnieniem rekomendacji CSIRT GOV, implementację nowej instancji serwera MS Exchange.

Apache Log4J

W związku z publikacją w dniu 10 grudnia 2021 roku informacji o krytycznej podatności w bardzo popularnej i szeroko stosowanej w sieci Internet bibliotece Log4J, która umożliwiała zdalne wykonanie kodu, zostały przeprowadzone w ramach zespołów reagowania na incydenty bezpieczeństwa komputerowego szczebla krajowego działania mające na celu koordynację obsługi incydentu na poziomie krajowym.

W związku z powyższym, w ramach prowadzonych działań Zespół CSIRT GOV przekazał w sumie ponad 11 różnych kategorii ostrzeżeń, skierowanych bezpośrednio do organów administracji państwowej, jak również rozesłanych do podmiotów infrastruktury krytycznej za pośrednictwem Rządowego Centrum Bezpieczeństwa. Powyższe ostrzeżenia zawierały informacje o przedmiotowym zagrożeniu, w tym m.in. wskaźniki, umożliwiające weryfikację posiadanych w instytucjach systemów pod kątem występowania przedmiotowej podatności, dane na temat wytycznych producentów podatnego oprogramowania oraz rekomendacje dotyczące wdrożenia dalszych czynności zapobiegawczych.

W toku podjętych działań zidentyfikowano wiele podatnych wersji oprogramowania, w tym dotyczących takich środowisk, jak np.: Vmware, F-Secure, CyberArk, ZOHO ManageEngine, ElasticSearch, Logstash, Graylog, szeregu produktów marki CISCO oraz różnych platform internetowych. Ponadto, wykonana przez CSIRT GOV analiza otrzymanych od instytucji danych na temat połączeń wykazała, że od momentu publikacji w sieci Internet informacji o przedmiotowej podatności, systemy brzegowe instytucji odnotowywały masowe skanowania w poszukiwa-

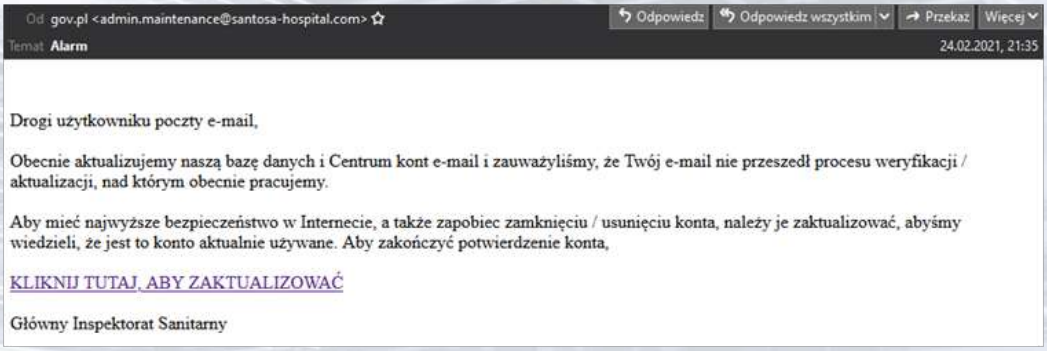
niu przedmiotowego błędu. Spośród prób eksploitacji zidentyfikowano aktywność adresu IP, który był przypisany do terenu Federacji Rosyjskiej, natomiast zakodowany w Base64 przepływ zawierał próbę instalacji na podatnej maszynie jednej z popularnych koparek kryptowalut.

Reasumując, należy podkreślić, iż w toku podjętych działań nie zarejestrowano w okresie obsługi zagrożenia Log4J, incydentów czy naruszeń bezpieczeństwa, które mogły skutkować przełamaniem zabezpieczeń w obszarze administracji publicznej czy infrastruktury krytycznej.

2.3 ODNOTOWANE ATAKI SOCJOTECHNICZNE

W 2021 roku Zespół CSIRT GOV odnotował 882 zgłoszenia w kategorii SOCJOTECHNIKA. W tej grupie incydentów znalazły się m.in. kampanie phishingowe oraz podszycia. Inżynieria społeczna obejmuje różne techniki, metody manipulacji, które służą do osiągnięcia konkretnego celu w postaci nakłonienia osób do działań zgodnych z zamierzeniami atakujących. Stosowana jest m.in. manipulacja psychologiczna, np. wykorzystywanie panujących nastrojów (np. strachu związanego z COVID-19), po to by przekonać użytkownika np. do pobrania i otworzenia załącznika czy podania danych logowania na specjalnie spreparowanej witrynie internetowej. Jednym z najczęściej stosowanych rodzajów inżynierii społecznej jest phishing. W roku ubiegłym najwięcej kampanii phishingowych dotyczyło wyłudzenia danych logowania oraz środków finansowych. Poniżej zostały zaprezentowane przykłady wybranych kampanii.

W lutym 2021 roku pojawiła się kampania podszywająca się pod Główny Inspektorat Sanitarny, której celem było pozyskanie danych logowania poczty elektronicznej. Wiadomości o tytule *Alarm* wysyłane były z adresu admin.maintenance@santosa-hospital.com. Treść wiadomości informowała o potrzebie aktualizacji baz danych i weryfikacji adresów e-mail, której można było dokonać pod linkiem *https[:]//postadzz[.]000webhostapp[.]com/pis[.]html.*



Od: gov.pl <admin.maintenance@santosa-hospital.com>
Odpowiedz | Odpowiedz wszystkim | Przekaz | Więcej
Temat: **Alarm**
24.02.2021, 21:35

Drogi użytkowniku poczty e-mail,

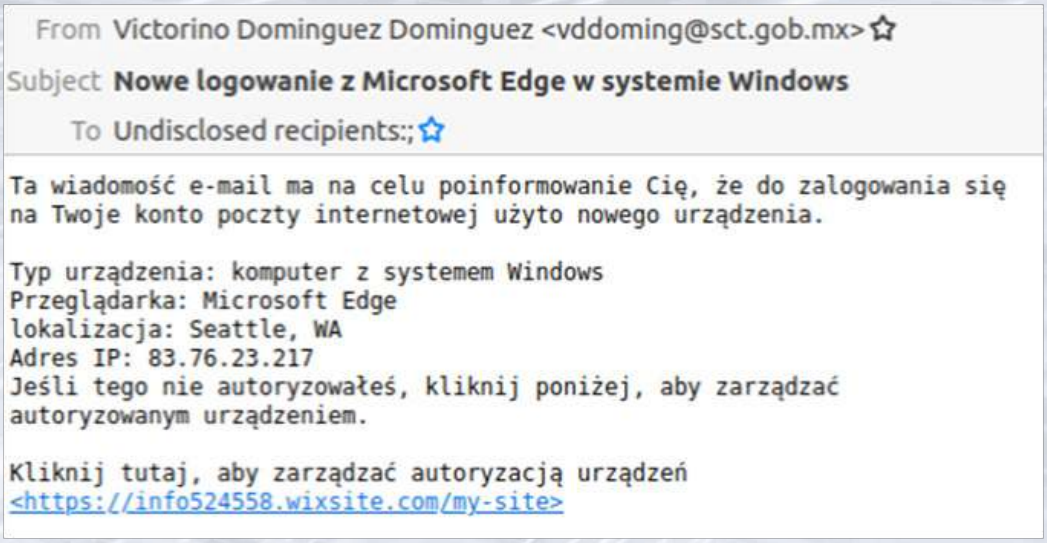
Obecnie aktualizujemy naszą bazę danych i Centrum kont e-mail i zauważyliśmy, że Twój e-mail nie przeszedł procesu weryfikacji / aktualizacji, nad którym obecnie pracujemy.

Aby mieć najwyższe bezpieczeństwo w Internecie, a także zapobiec zamknięciu / usunięciu konta, należy je zaktualizować, abyśmy wiedzieli, że jest to konto aktualnie używane. Aby zakończyć potwierdzenie konta,

KLIKNIJ TUTAJ, ABY ZAKTUALIZOWAĆ

Główny Inspektorat Sanitarny

Kolejną zarejestrowaną kampanią była kampania phishingowa polegająca na rozsyłaniu wiadomość pomiędzy organy administracji publicznej oraz operatorów infrastruktury krytycznej, pochodząca z adresu vddoming@sct.gob.mx. Wiadomość zatytułowana była *Nowe Logowanie z Microsoft Edge w systemie Windows*. Treść wiadomości informowała o rzekomym zalogowaniu się na pocztę e-mail z komputera w lokalizacji *Seattle,WA*. W treści wiadomości zawarty był odnośnik *https[:]//info524558[.]wixsite[.]com/my-site*, który kierował do spreparowanego panelu logowania OWA Exchange firmy Microsoft, w którym należało podać dane logowania do skrzynki e-mail. Poniżej przedstawiono przykład tego typu wiadomości e-mail.



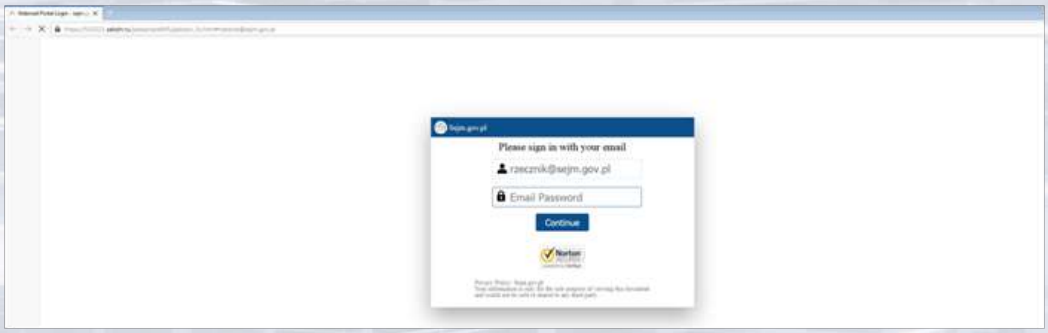
From Victorino Dominguez Dominguez <vddoming@sct.gob.mx>
Subject **Nowe logowanie z Microsoft Edge w systemie Windows**
To Undisclosed recipients:;

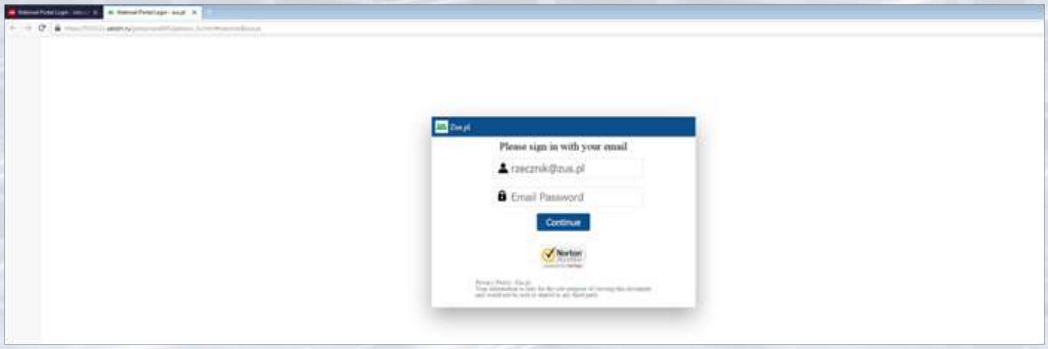
Ta wiadomość e-mail ma na celu poinformowanie Cię, że do zalogowania się na Twoje konto poczty internetowej użyto nowego urządzenia.

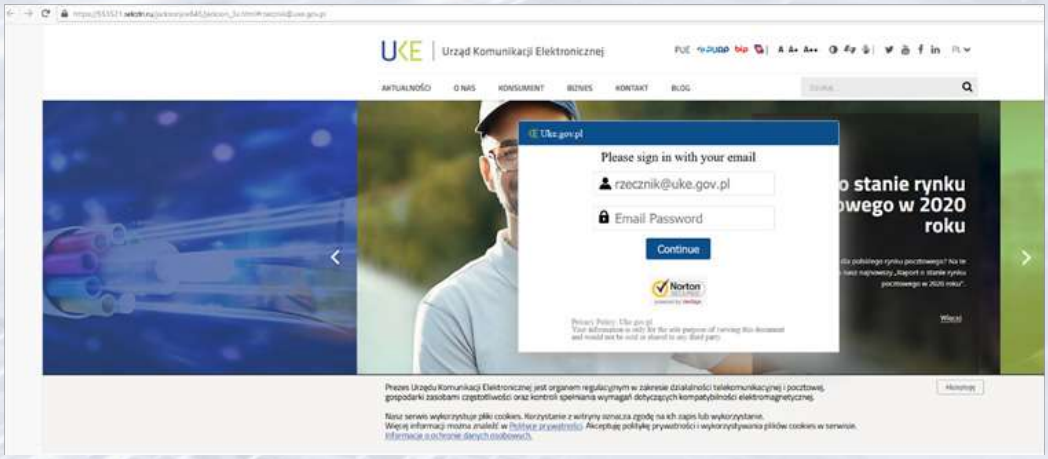
Typ urządzenia: komputer z systemem Windows
Przeglądarka: Microsoft Edge
lokalizacja: Seattle, WA
Adres IP: 83.76.23.217
Jeśli tego nie autoryzowałeś, kliknij poniżej, aby zarządzać autoryzowanym urządzeniem.

Kliknij tutaj, aby zarządzać autoryzacją urządzeń
<https://info524558.wixsite.com/my-site>

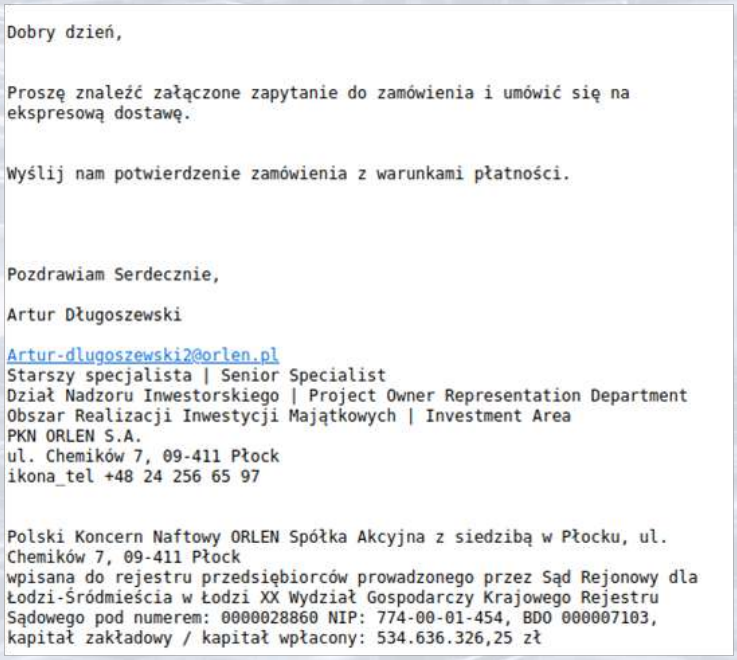
Dość popularne były też kampanie phishingowe, w których informowano o np. zawieszeniu skrzynki pocztowej z powodu błędu systemu na serwerze pocztowym, przepełnieniu skrzynki pocztowej lub niedostarczeniu wiadomości e-mail z jakichś innych powodów. Celem usunięcia wskazanych problemów należało kliknąć w link podany w wiadomości. Najczęściej link przekierowywał do witryny wyłudzającej dane uwierzytelniające. W niektórych przypadkach po otwarciu wskazanego odnośnika pojawiał się panel logowania, gdzie wyświetlało się m.in. logo danej instytucji, które zmieniało się w zależności od domeny wpisanej w odpowiednim miejscu w adresie URL, np.:
https[:]//553521[.]selcdn[.]ru/jacksonjoe845/jackson_3x[.]html#[_adres_email_osoby_]







Jedna z kampanii phishingowych w sieci Internet podszywała się m.in. pod firmę Orlen S.A. Wiadomości e-mail pochodziły z domeny bitmagest.es powiązanej z adresem IP: 217.160.131.123. z tytułem wiadomości *Zapytanie o zamówienie*, zaś treść informowała o zapoznaniu się z zapytaniem do zamówienia. Do wiadomości załączony był załącznik w formacie .rar. W wiadomościach użytkownik nakłaniany był do otwarcia złośliwego załącznika, gdzie umieszczono GuLoader - narzędzie do pobierania malware, które wykorzystywane jest do rozprzestrzeniania różnych trojanów zdalnego dostępu (RAT) lub innego złośliwego oprogramowania. Przykład tego typu email-a przedstawiono poniżej.



Dobry dzień,

Proszę znaleźć załączone zapytanie do zamówienia i umówić się na ekspresową dostawę.

Wyślij nam potwierdzenie zamówienia z warunkami płatności.

Pozdrawiam Serdecznie,

Artur Długoszewski

Artur-dlugoszewski2@orlen.pl
Starszy specjalista | Senior Specialist
Dział Nadzoru Inwestorskiego | Project Owner Representation Department
Obszar Realizacji Inwestycji Majątkowych | Investment Area
PKN ORLEN S.A.
ul. Chemików 7, 09-411 Płock
ikona_tel +48 24 256 65 97

Polski Koncern Naftowy ORLEN Spółka Akcyjna z siedzibą w Płocku, ul. Chemików 7, 09-411 Płock
wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi-Śródmieścia w Łodzi XX Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem: 0000028860 NIP: 774-00-01-454, BDO 000007103, kapitał zakładowy / kapitał wpłacony: 534.636.326,25 zł

Załączniki zawierały pliki wykonywalne, których IoC przedstawiono poniżej:
Nazwa pliku: Zapytanie o zam#U00f3wienie (02182021-00260).exe
MD5: 1d9144162489992075312 95c80c030b3

Nazwa pliku: Zapytanie o zam#U00f3wienie (02182021).exe
MD5: b4a36eac087bc9ec64964b5d41d9f95a

Nazwa pliku: Zapytanie o zam#U00f3wienie (02172021-00260).exe
MD5: 6b7a97e67c48068d7f77d1262489ed33

W 2021 roku w dalszym ciągu były obserwowane kampanie wykorzystujące motyw Faktury Play, gdzie podany w treści wiadomości link *https[:]//logowanie-play-pl[.]selfip[.]net/kl/* powiązany z adresem IP 68.68.98[.]110 prowadził do strony phishingowej, na której ofiara została proszona o podanie danych uwierzytelniających do konta Play. Następnie na kolejnych podstronach należało podać numer karty kredytowej, na którą miał nastąpić rzekomy zwrot funduszy z nadpłaty. W kampanii posługiwano się m.in. domeną *wizardly-heisenberg.68-68-98-95.plesk.page.*


PLAY

TWOJA FAKTURA JEST ONLINE

Hello ,

Z przykrością informujemy, że ostatnie rozliczenie Twojej faktury za styczeń 2021 zostało zapłacone dwukrotnie.

Zapraszamy do złożenia wniosku o zwrot pieniędzy, klikając poniższy link:

Zażądać zwrotu

Uwaga: jeśli problem nie zostanie rozwiązany w ciągu najbliższych 12 godzin, zwrot środków nie będzie możliwy.

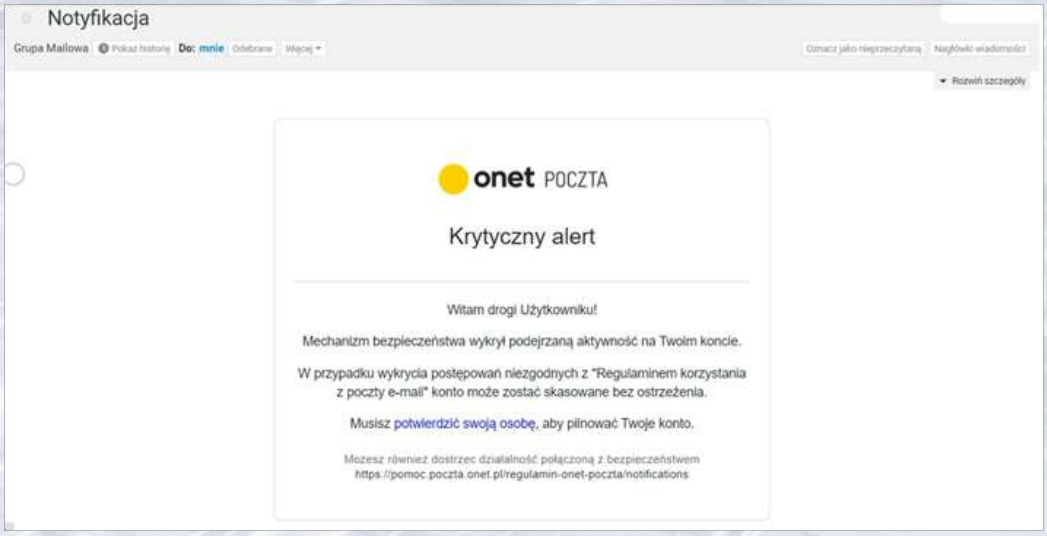
Przepraszamy za wszelkie niedogodności

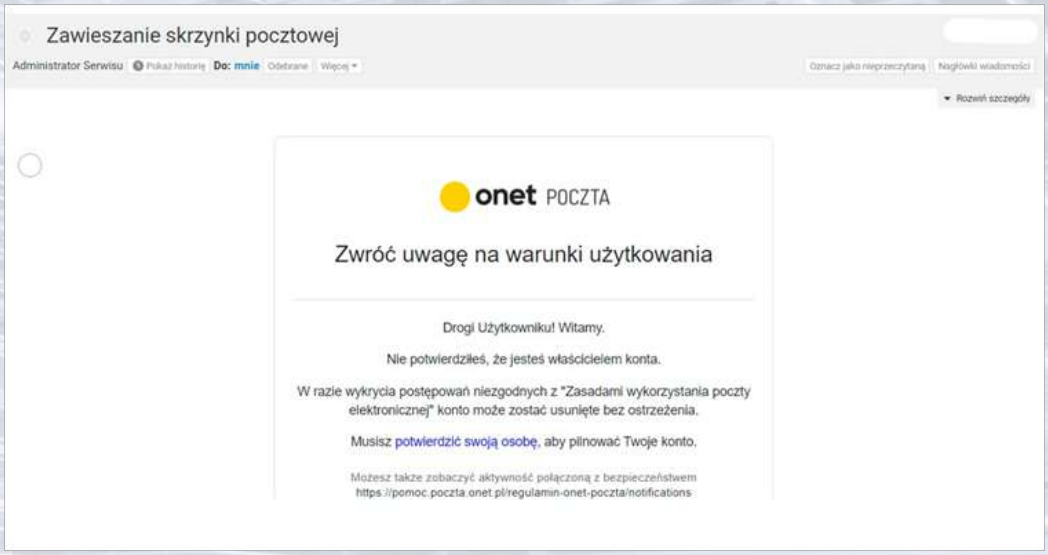
2.3 ODNOTOWANE PRZEZ ZESPÓŁ CSIRT GOV AKTYWNOŚCI GRUP APT

Jednym z obserwowanych w roku 2021 zagrożeń, które można przypisać działaniom grup APT, były ataki socjotechniczne typu spearphishing, których celem było wyłudzenie danych uwierzytelniających do kont usług elektronicznych różnych ofiar. Częstym celem takich działań było przejęcie przez atakującego nie tylko danych logowania do konta samej poczty email, ale także uzyskanie dostępu do kolejnych usług wirtualnych (w szczególności kont portali społecznościowych) powiązanych ze skompromitowanymi kontami email. Ataki typu spearphising były i są często stosowane przez grupy cyberprzestępcze, jak również grupy typu state-sponsored. Cyberprzestępcy motywowani są przede wszystkim chęcią pozyskania i utrzymania dostępu do danych użytkownika w celu przeprowadzania kolejnych ataków lub szerzenia dezinformacji.

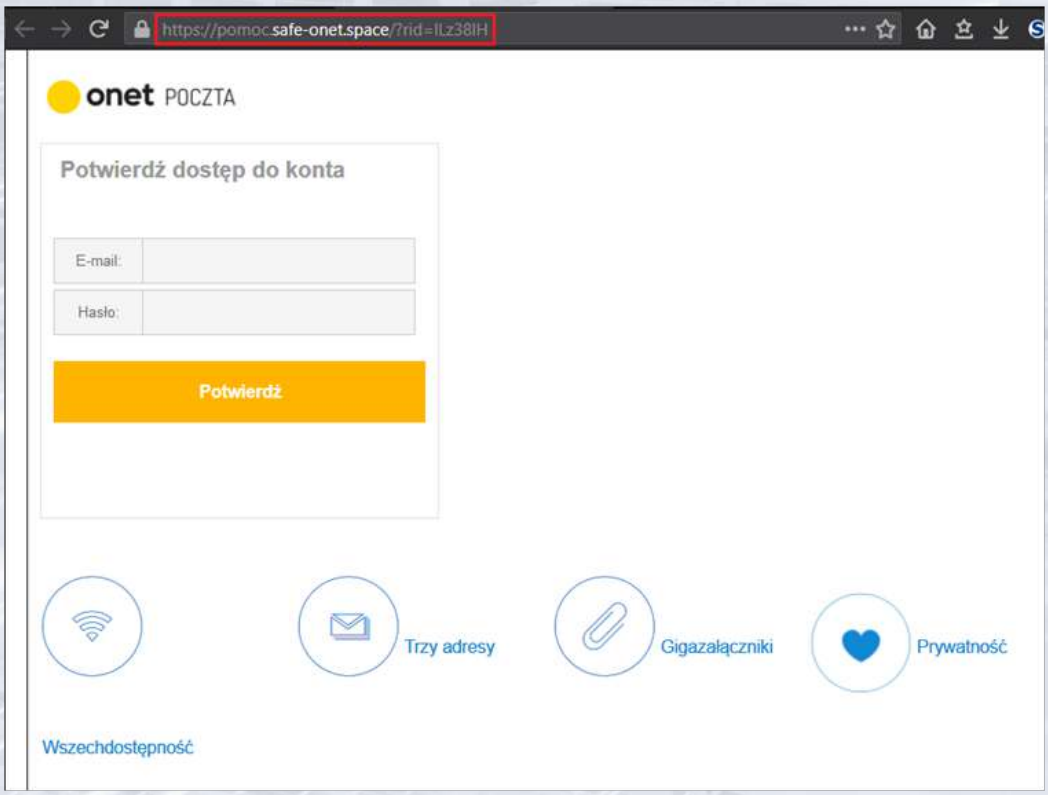
Jednym z przykładów powyższego zagrożenia w 2021 roku była także szeroko komentowana w przestrzeni medialnej operacja o nazwie Ghostwriter, której sprawstwo przypisuje się grupie UNC1151. Badając wykorzystywane przez UNC1151 tzw. TTP's, (ang. tactics, techniques, and procedures) można przypisać jej ataki socjotechniczne, których celem mogło być w sumie kilka tysięcy adresów email należących m.in. do polskich dostawców poczty elektronicznej.

Poniżej kilka przykładów powyższych szkodliwych działań, które przypisano do grupy UNC1151, m.in. fałszywy email, który miał skłonić ofiarę do odwiedzenia złośliwego odnośnika:

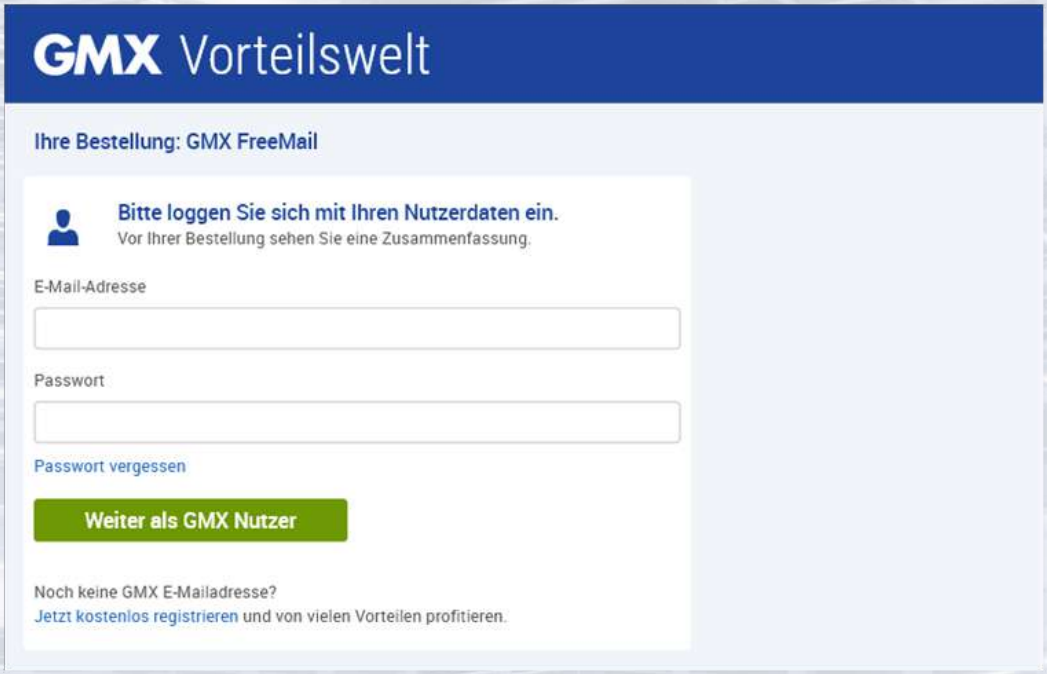




Po odwiedzeniu przez ofiarę załączonego do fałszywej wiadomości odnośnika ukazywała się przygotowana przez napastników fałszywa strona, zawierająca formularz:



Wśród celów znajdowali się użytkownicy wielu operatorów poczty elektronicznej, zarówno polskich jak i zagranicznych:



Często również atakujący po otrzymaniu za pośrednictwem fałszywego formularza danych ofiary był nawet skłonny wyrazić jej swoją wdzięczność za przesłane informacje poprzez wysłanie kolejnej, fałszywej wiadomości o poprawnej weryfikacji konta.

Ponadto, spośród odnotowywanych w 2021 roku przez Zespól CSIRT GOV zagrożeń kilkukrotnie zidentyfikowano wrogą aktywność cybeprzestępczą, którą można przypisać działaniom w ramach długofalowych kampanii prowadzonych przez grupy APT. Do najczęściej identyfikowanych w 2021 roku przez Zespół CSIRT GOV grup tego typu można zaliczyć przede wszystkim grupę APT29 oraz APT31. Grupie ATP29 w 2021 roku przypisano m.in. szereg ataków socjotechnicznych, natomiast w przypadku grupy APT31 można wskazać na próbę przełamania zabezpieczeń jednej z instytucji polskiej administracji publicznej.

Ponadto, do powyższej kategorii zaliczyć można także szkodliwe działania, przypisywane grupie o nazwie Snake/Turla. Jednakże, aktywność tej grupy dotyczyła głownie ośrodków akademickich oraz osób, związanych z szeroko pojętym obszarem think-tanków i NGO.

Reasumując, zgodnie z posiadaną wiedzą wrogie działania grup APT w obszarze CRP w 2021 roku objawiały się przede wszystkim wykorzystaniem ataków socjotechnicznych. W niektórych przypadkach przeciwnik stosował także metody służące eksploitacji podatności w usługach serwerowych. Dodatkowo odnotowano, że cechą wspólną wielu z powyższych ataków było użycie przez napastnika oprogramowania o nazwie Cobalt Strike.

Cobalt Strike to multiplatformowe oprogramowanie, będące zbiorem narzędzi służących do prowadzenia testów penetracyjnych oraz operacji typu Red Team. Ponadto, jego elastyczność, stabilność oraz szeroka gama funkcjonalności sprawiła, że stało się bardzo popularne wśród wielu grup APT.

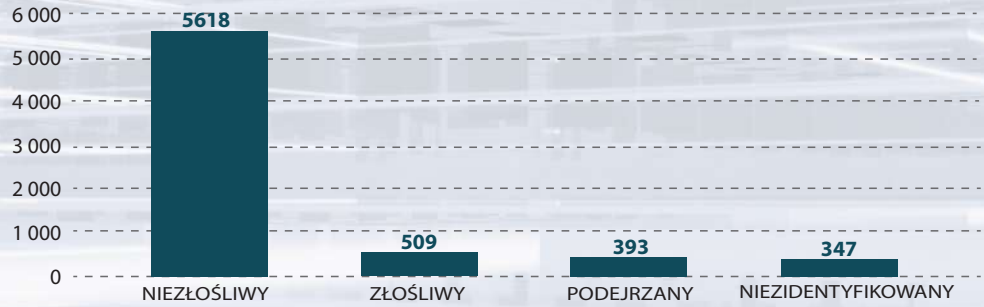
3. ZAGROŻENIA - OPROGRAMOWANIE ZŁOŚLIWE

3.1 OPROGRAMOWANIE ZŁOŚLIWE - STATYSTYKA

Statystyka zgłoszeń zawierających pliki lub zasoby internetowe podlegające sprawdzeniu m.in. w systemach typu Sandbox

W 2021 roku Zespół CSIRT GOV przeprowadził analizę prawie 7 tysięcy plików zgłoszonych przez podmioty, spośród których ponad 500 zostało rozpoznanych jako złośliwe.

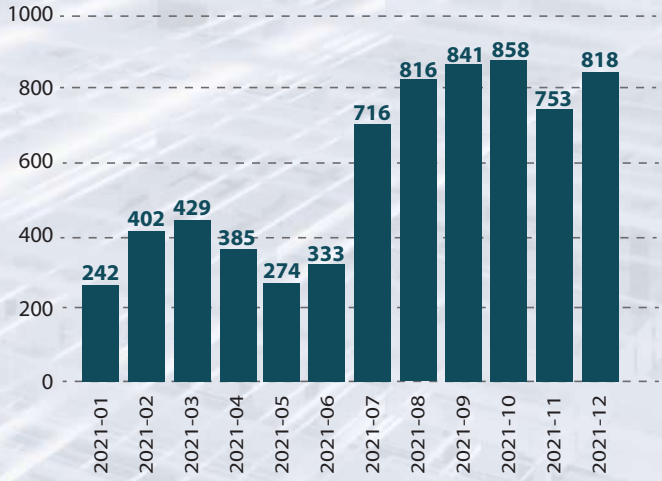
Poniżej przedstawiono wykres z podziałem na wynik przeprowadzonych analiz wszystkich zgłoszonych plików.



Wykres 6. Wyniki analizy zgłoszonych plików

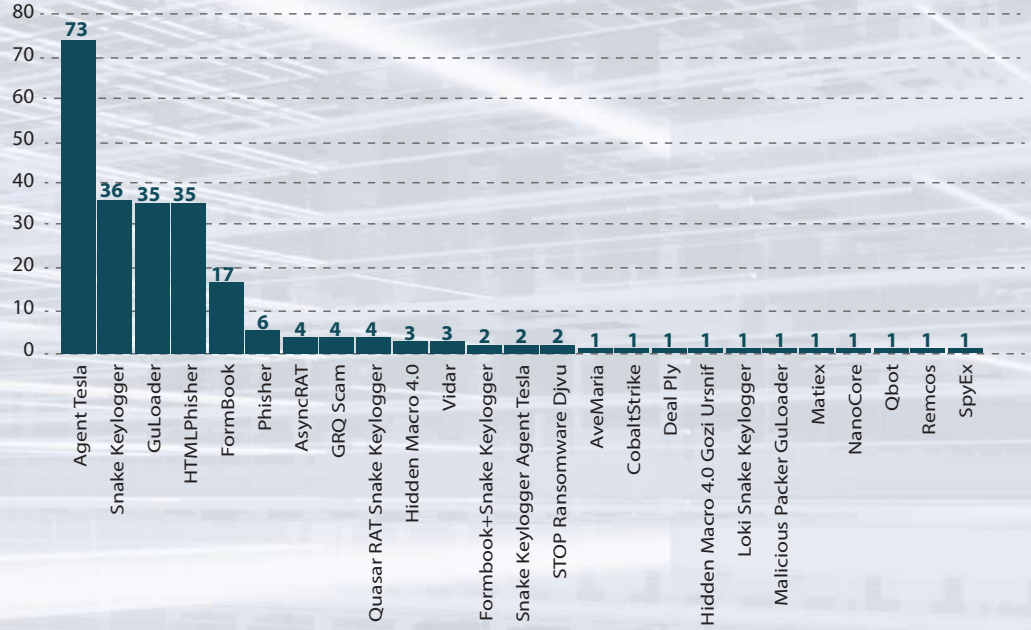
Analiza w środowiskach badawczych wykazała, iż 5 618 plików nie wykazywało żadnych cech złośliwych, 509 zostało rozpoznanych jako złośliwe, 393 jako podejrzane oraz 347 ze statusem nieoznaczonym (np. ze względu na brak poprawnego uruchomienia).

Poniżej przedstawiono miesięczny rozkład analizowanych plików.



Wykres 7. Statystyka miesięczna analizowanych plików

Spośród 509 zidentyfikowanych złośliwych plików, 237 zostało sklasyfikowanych m.in. za pomocą reguł YARA oraz Sigma do poniższych typów oprogramowania złośliwego.



Wykres 8. Klasyfikacja oprogramowania złośliwego

Najwięcej próbek oprogramowania złośliwego w 2021 roku zostało rozpoznanych jako Agent Tesla, Snake Keylogger, GuLoader oraz HTML Phisher.

Agent Tesla jest trojanem umożliwiającym uzyskanie zdalnego dostępu do stacji roboczej (Remote Access Trojan), którego głównym celem jest pozyskanie danych uwierzytelniających użytkownika tj. ekstrakcja zapisanych loginów i haseł z przeglądarek internetowych, klientów pocztowych, oprogramowania VPN i innych aplikacji użytkowych. Dodatkowo, oprogramowanie złośliwe posiada funkcjonalność zapisu treści wpisywanych za pomocą klawiatury (keylogger), przechwytywania zrzutów ekranu oraz danych z przesyłanych formularzy (form-grabbing). Agent Tesla eksflitruje zebrane dane ze stacji roboczej z wykorzystaniem protokołu SMTP.

Snake Keylogger podobnie jak Agent Tesla należy do oprogramowania złośliwego skupiającego się na kradzieży poufnych informacji z urządzenia ofiary, w tym przede wszystkim treści wpisywanych za pomocą klawiatury, wykonywania zrzutów ekranu oraz wykradania danych ze schowka.

GuLoader jest oprogramowaniem złośliwym napisanym w języku Visual

Basic, który pełni funkcję downloadera – pobiera faktyczny zaszyfrowany kod złośliwy z zewnętrznych zasobów (np. zasoby dysku Google lub OneDrive), a następnie uruchamia go w pamięci. GuLoader w 2021 roku najczęściej dystrybuowany był z wykorzystaniem spreparowanych dokumentów DOC/DOCX/XLS/XLSX zawierających makra z skryptem VBA lub osadzonymi obiektami OLE.

Oprogramowanie rozpoznane, jako HTML Phisher związane było najczęściej z przesłanym załącznikiem do korespondencji e-mail w formacie „HTML" lub „HTM", zawierającym formularz logowania do rzekomego serwera poczty elektronicznej ze statycznie umieszczonymi zdjęciami w kodzie źródłowym (zakodowanymi w base64). Wprowadzenie danych uwierzytelniających do spreparowanego formularza powodowało przesłanie danych do zewnętrznego serwera z wykorzystaniem metod HTTP typu GET (przykładowo funkcja XMLHttpRequest).

Ponadto, klasyfikacja oprogramowania bazująca na analizie behawioralnej wykazała następujący podział zachowań analizowanych plików lub zasobów internetowych.

L.p.	WYKRYTE ZACHOWANIE	LICZBA WYSTĄPIEŃ
1	Evader	124
2	Trojan/Bot, Spyware, Evader	92
3	Phishing	69
4	Trojan/Bot, Evader	64
5	Exploiter, Evader	30
6	Exploiter	28
7	Trojan/Bot, Adware, Spyware, Evader	15
8	Trojan/Bot	12
9	Ransomware	5
10	Trojan/Bot, Spyware, Exploiter, Evader	5

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;

Miner – wykorzystanie zasobów CPU/GPU do wydobycia kryptowalut;

Ransomware – szyfrowanie danych użytkownika; identyfikacja blokady stacji roboczej; identyfikacja instrukcji deszyfracji danych (ransom-note);

Spreading – rozprzestrzenianie się oprogramowania złośliwego z wykorzystaniem różnych mediów (pamięci USB, zasoby sieciowe);
Phishing – wykrycie nakłaniania użytkownika do wykonania określonego działania; udostępnienia poufnych informacji tj. hasła dostępowego, danych logowania oraz danych kart płatniczych;
Banker – identyfikacja prób modyfikacji transakcji bankowych;
Trojan/Bot – identyfikacja zmiany stacji roboczej w klienta sieci botnet; umożliwienie zdalnego dostępu do stacji roboczej (RAT);
Adware – identyfikacja wstrzyknięcia niepożądanych reklam do wyników wyszukiwania w przeglądarce internetowej;
Spyware – identyfikacja kradzieży danych wrażliwych tj. danych z przeglądarek internetowych, danych logowania;
Exploiter – identyfikacja wykorzystania podatności w oprogramowaniu lub systemie operacyjnym.

Poniżej przedstawiono 10 najczęściej identyfikowanych reguł spośród wszystkich przeprowadzonych analiz w środowisku sandbox, które m.in. wpływały na końcową ocenę badanego pliku lub zasobu internetowego.

L.p.	WYKRYTA REGUŁA	LICZBA IDENTYFIKACJI
1	Podejrzane wywołania interpretera PowerShell	476
2	Rozpoznanie pliku przez silniki antywirusowe	207
3	Identyfikacja zaszyfrowanych danych w dokumencie (ochrona hasłem)	186
4	Modyfikacja kontekstu wątku w innym procesie (thread injection)	138
5	Próba detekcji narzędzi do analizy dynamicznej oraz systemów typu sandbox	138
6	Próba kradzieży danych uwierzytelniających do skrzynki pocztowej (poprzez dostęp do plików)	110
7	Wstrzyknięcie pliku PE do obcych procesów	104
8	Rozpoznanie domeny / adresu URL przez silniki antywirusowe	104
9	Próba kradzieży danych wrażliwych z przeglądarki (historia, hasła, ciasteczka)	97
10	Podejrzane uruchomienie skryptu PowerShell	94

Tabela 2. 10 najczęściej identyfikowanych reguł

Poniżej przedstawiono statystyczne ujęcie głównych typów plików poddanych analizie w 2021 roku w systemach automatycznych.

L.p.	TYP PLIKU
1	Adobe Portable Document Format
2	Word Microsoft Office Open XML Format document
3	Generic OLE2 / Multistream Compound File
4	Microsoft Word document
5	Win32 Executable (generic) Net Framework
6	7-Zip compressed archive
7	Exel Microsoft Office Open XML Format document
8	ZIP compressed archive

Tabela 3. Główne typy plików poddawane analizie malware

Wśród głównych typów plików poddanych analizie w systemach automatycznych przechodziły pliki w formacie PDF przesłane wraz z załącznikami w wiadomościach e-mail oraz dokumenty i arkusze kalkulacyjne pakietów biurowych.

4. ARAKIS GOV

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 2021 roku w sieciach teleinformatycznych podmiotów uczestniczących w projekcie ARAKIS GOV zanotowano łącznie 1 758 708 908 przepływów, co przełożyło się na 3 366 360 wygenerowanych przez system alarmów[1]. Wśród zanotowanych alarmów:

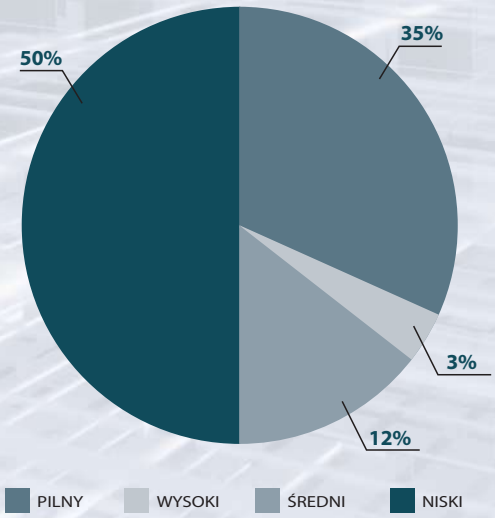
• 1 170 136 alarmów miało priorytet pilny, tzn. wymagało niezwłocznej reakcji na zagrożenie ze strony administratorów, z uwagi naduże ryzyko przełamania zabezpieczeń;

• 99 207 alarmów miało priorytet wysoki, tzn. wymagało wzmożonej uwagi w kontekście zagrożenia wskazanego w alarmie, z uwagi na średnie ryzyko przełamania zabezpieczeń;

• 416 987 alarmów miało priorytet średni, tzn. były to alarmy informujące o dobrze znanym zagrożeniu, które niosły małe ryzyko przełamania zabezpieczeń;

• 1 680 030 alarmów miało priorytet niski, tzn. były to alarmy informacyjne dot. aktualnej sytuacji na styku sieci wewnętrznej z siecią Internet.

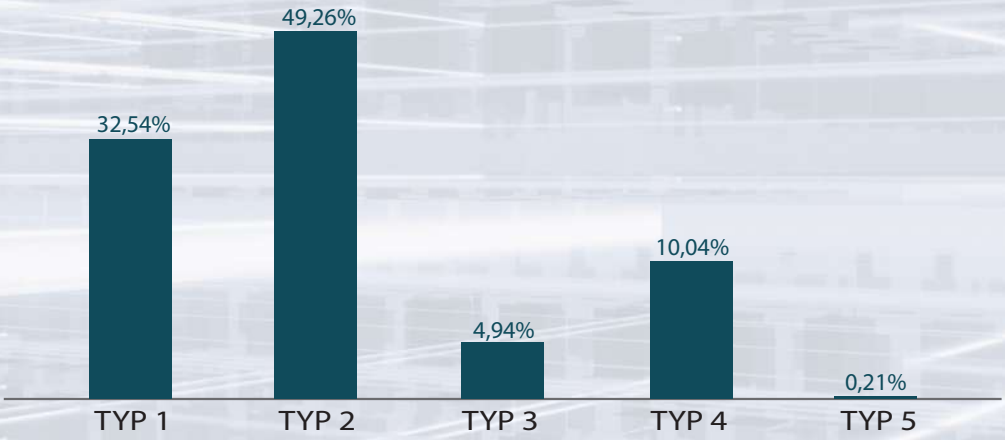
Poniżej przedstawiono podział zarejestrowanych przez ARAKIS GOV alarmów.



Wykres 9. 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:

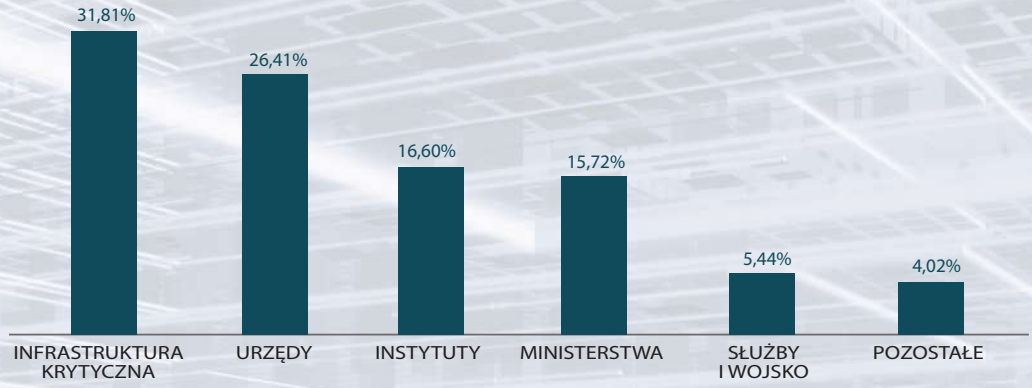
- Typ 1 – komunikacja do złośliwych adresów;
- Typ 2 – skanowania;
- Typ 3 – wykryte znane ataki;
- Typ 4 – wykryte nieopisane ataki;
- Typ 5 – infekcje wewnętrzne.



Wykres 10. Procentowy podział alarmów systemu ARAKIS GOV ze względu na typ

W 2021 roku **alarmy Systemu ARAKIS GOV typu 1** (komunikacja do złośliwych adresów) stanowiły 32,54%. 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 2021 roku najwięcej przepływów zostało zanotowanych w instytucjach skategoryzowanych jako Infrastruktura Krytyczna (31,81%), co wynika po części z ilości elementów systemu ARAKIS GOV rozlokowanych w poszczególnych instytucjach. Wygenerowane alarmy pozwalają określić kierunki zainteresowań osób przeprowadzających skanowania.



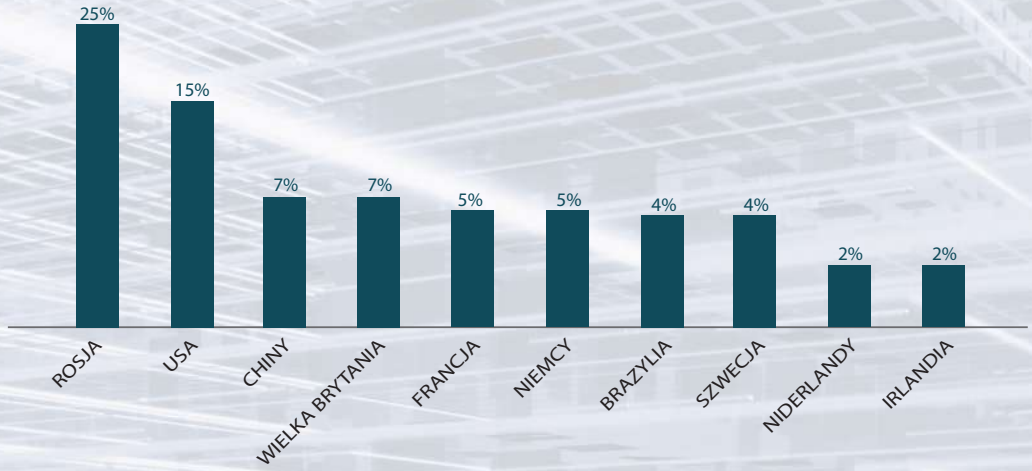
Wykres 11. Procentowy podział przepływów alarmów typu 2 w instytucjach

Alarmy typu 3 i 4 (wykryte znane ataki, wykryte nieopisane ataki) stanowiły odpowiednio 4,94% oraz 13,04% ze wszystkich przepływów, co wprost wynika z wygenerowania sygnatury IDS w oparciu o obserwowane komunikacje lub dopasowania do sygnatury IDS nie widzianej 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 GOV.

Do najbardziej aktywnych krajów pod kątem liczby generowanych przepływów w 2021 roku należały Rosja (25% przepływów) oraz Stany Zjednoczone (15% przepływów).

Warto też zaznaczyć, iż liczba przepływów z poszczególnych krajów należących do grupy TOP 10 stanowi 76% wszystkich wygenerowanych przepływów zanotowanych przez System ARAKIS GOV w 2021 roku co stanowi wzrost o 3 pp. względem roku 2020.



Wykres 12. Rozkład źródeł ataków na sieci monitorowane przez system ARAKIS GOV pod kątem liczby generowanych przepływów

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	-	495 923 051	ICMP Echo Reply / Request
2	21	134 732 316	FTP
3	22	45 627 979	SSH
4	445	22 775 188	SMB
5	23	26 480 955	Telnet
6	80	20 212 805	HTTP
7	1900	12 876 443	SSDP
8	443	12 102 185	HTTPS
9	1443	10 931 137	MSSQL
10	6379	10 120 524	Redis

Tabela 4. Zidentyfikowane w 2021 roku skanowania i próby eksploitacji usług na podstawie danych z systemu ARAKIS GOV

W roku 2021 najczęściej wykorzystywanym elementem rekonesansu był protokół ICMP. Warto odnotować duży wzrost zainteresowania usługą FTP i SSH powiązaną z portami 21 i 22. Zmalało zainteresowanie usługą MSSQL (port 1443) oraz SMB (port 445).

L.p.	LICZBA PRZEPŁYWÓW	Reguła SNORT
1	9905745	ET SCAN Suspicious inbound to MSSQL 1433
2	6927430	ET SCAN Potential SSH Scan OUTBOUND
3	3578862	ET SCAN Sipvicious Use-Agent Detected (friendly-scanner)
4	2350178	ET SCAN Sipvicious Scan
5	1353556	ET INFO Session Traversal Utilities for NAT (STUN Binding Request)
6	1135346	ET SCAN Suspicious inbound to mySQL port 3306
7	986389	ET SCAN Suspicious inbound to PostgreSQL port 5432
8	486775	ET SCAN Suspicious inbound to Oracle SQL port 1521
9	349455	GPL NETBIOS SMB-DS IPC$ unicode share access
10	293613	ET INFO Potentially unsafe SMBv1 protocol in use

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

W 2021 roku zidentyfikowano 9 905 745 dopasowań reguł SNORT do obserwowanego ruchu sieciowego związanego z portem 1433, co jest znaczącym spadkiem względem roku 2020. Warte odnotowania jest zwiększone zainteresowanie usługami baz danych mySQL, PostgeSQL i Oracle SQL (odpowiednio porty: 3306, 5432, 1521), które nie były w takim stopniu rozpoznawane w roku 2020.

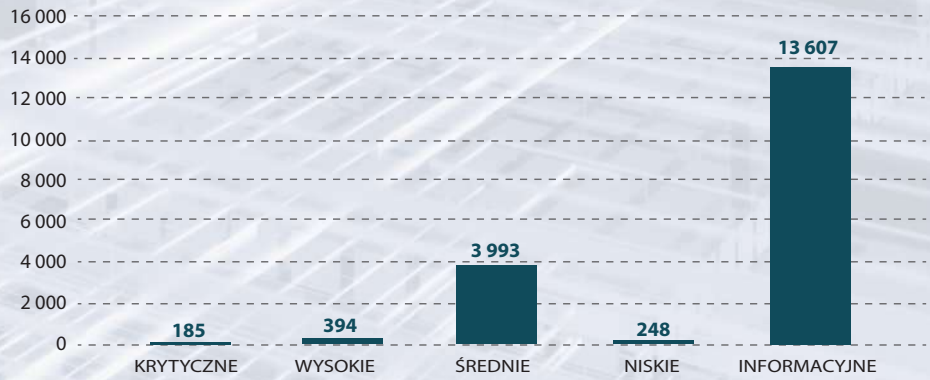
5. OCENA BEZPIECZEŃSTWA SYSTEMÓW TI

W 2021 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 91 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 23 września 2020 r. w sprawie przeprowadzania przez Agencję Bezpieczeństwa Wewnętrznego ocen bezpieczeństwa systemów teleinformatycznych na 2021 r., Zespół CSIRT GOV przeprowadził przedmiotowe czynności w siedemnastu instytucjach administracji rządowej oraz infrastruktury krytycznej, w których przebadał (w sumie) 149 segmentów sieci / systemów teleinformatycznych oraz 36 domen / subdomen internetowych.

W ramach oceny bezpieczeństwa Zespół CSIRT GOV przeprowadził szereg testów mających na celu identyfikację istotnych podatności wpływających na bezpieczeństwo infrastruktur teleinformatycznych poszczególnych 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 począwszy 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 13. Zestawienie zidentyfikowanych podatności z podziałem na priorytet

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

- Nieaktualne wersje oprogramowania
    a) Microsoft Windows
    b) Microsoft SQL Server
    c) Microsoft Exchange Server
    d) IBM WebSphere Application Server
    e) VMWare ESXi
    f) Apache Tomcat
    g) OpenSSL
    h) Oracle Database
    i) Pulse Connect Secure
    j) PHP
    k) Python

- Niewspierane wersje oprogramowania
    a) PHP
    b) HP Data Protector
    c) Python

- 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) Lightweight Directory Access Protocol (LDAP)
    f) Network Level Authentication (NLA)
    g) Online Certificate Status Protocol (OCSP)
    h) Remote Executions Of Command (rexecd)
    i) Network File System (NFS)
    j) Simple Network Management Protocol (SNMP)
    k) Microsoft Server Message Block 1.0 (SMBv1)
    l) Secure Shell (SSH)

• Dostęp anonimowy, bez wymaganego uwierzytelnienia lub na podstawie domyślnych haseł:

a) Serwery bazodanowe Elasticsearch

b) Serwery z dostępną usługą SAP

c) Serwery SMTP

d) Serwery FTP

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

f) IBM Tivoli Monitoring

g) HP OfficeJet Pro

Przykłady wykrytych podatności opisano poniżej:

a) Wykorzystanie serwera SMTP działającego na adresie publicznym (dostępny z sieci Internet) celem wysłania wiadomości na istniejące konto e-mail w domenie przy jednoczesnym podszyciu się pod inną osobę;

```
root@kali4-machine:/home/pentester# telnet [redacted] 25
Trying [redacted] ...
Connected to [redacted].
Escape character is '^]'.
220 poczta.[redacted].pl ESMTP Postfix
HELO csirt.gov.pl
250 poczta.[redacted].pl
MAIL FROM: marek.[redacted]@[redacted].pl
250 2.1.0 Ok
RCPT TO: katarzyna.[redacted]@[redacted].pl
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: Marek [redacted]
To: katarzyna.[redacted]@[redacted].pl
Subject: Wiadomosc od Marka
Mime-Version: 1.0
Content-Type: text/plain; charset=UTF-8

Dzien dobry,

Wiadomosc wyslana z wykorzystaniem hosta stojacego na publicznym adresie.

Pozdrawiam
[redacted]
.
250 2.0.0 Ok: queued as A066980104
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
root@kali4-machine:/home/pentester#
```

b) Przełamanie słabego hasła, umożliwiającego dostęp do platformy - Intelligent Platform Management Interface (IPMI);

```
[*] Sending IPMI requests to 172.20.15.73->172.20.15.73 (1
hosts)
[+] 172.20.15.73:623 - IPMI - IPMI-2.0 UserAuth(auth_msg,
auth_user, non_null_user) PassAuth(password, md5) Level(1.5,
2.0)
[*] Scanned 1 of 1 hosts (100% complete)
```

```
[+] 172.20.15.73:623 - IPMI - Hashfound:
USERID:b9f6afd600130003cc61d3f4e7367e06d8c268cc94e22bccbb6de5307
b734e7536b4e76a1b4339864a012b519d48e211b0186cae8b6319f2140655534
5524944:3e0d0b61e54424e558274048bdf67fa05d7d338f
[*] Scanned 1 of 1 hosts (100% complete)
```

```
ID  Name    Callin  Link Auth  IPMI Msg   Channel Priv Limit
1                true    false      false      NO ACCESS
2   USERID      true    truetrue       ADMINISTRATOR
3                true    false      false      NO ACCESS
4                true    false      false      NO ACCESS
5                true    false      false      NO ACCESS
```

c) Wykorzystanie podatności serwera IIS, a w konsekwencji uzyskanie tzw. ”bluescreen” hosta;

```
10.1.1.50 (443/tcp)
-------------------------------------------------
  Product                 : Microsoft IIS 7.5
  Server response header  : Microsoft-IIS/7.5
  Support ended           : 2020-01-14
  Supported versions      : Microsoft IIS 8.5 / 8.0
```

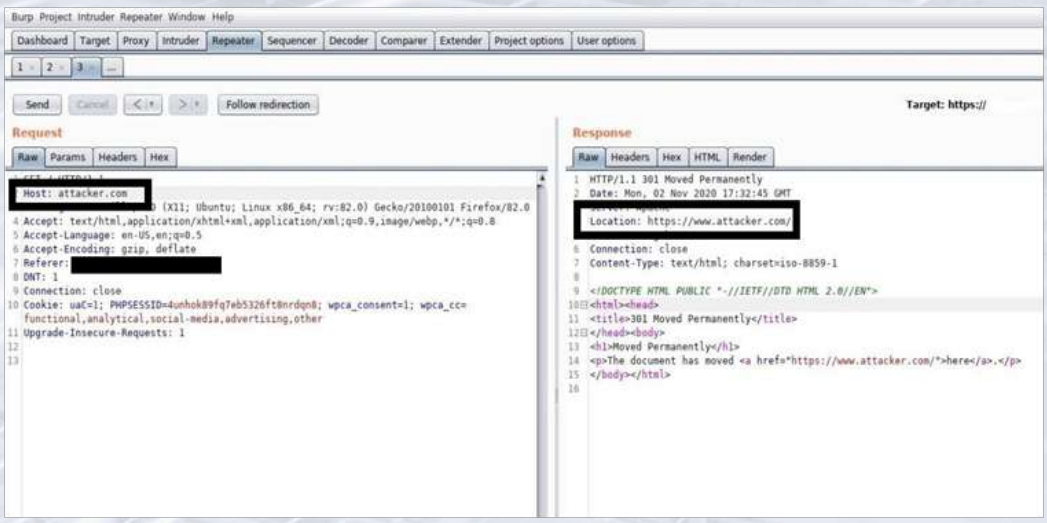
```
┌──(root㉿kali)-[/home/pentester]
└─# wget --header="Range: bytes=18-18446744073709551615" http://10.1.1.50/welcome.png --no-check-certificate
--2021-04-20 11:44:50--  http://10.1.1.50/welcome.png
Łączenie się z 10.1.1.50:80... połączono.
Żądanie HTTP wysłano, oczekiwanie na odpowiedź... Błąd odczytu (Połączenie zerwane przez drugą stronę) w nagłówkach.
Ponawianie próby.

--2021-04-20 11:44:55--  (próba: 2) http://10.1.1.50/welcome.png
Łączenie się z 10.1.1.50:80... połączono.
Żądanie HTTP wysłano, oczekiwanie na odpowiedź... Błąd odczytu (Połączenie zerwane przez drugą stronę) w nagłówkach.
Ponawianie próby.
```

d) Host Header Injection;

Badana aplikacja nieprawidłowo walidowała otrzymany w żądaniu nagłówek „Host". Po podmianie nagłówka „Host" aplikacja przekierowywała użytkownika do domeny podanej w zmienionym nagłówku.

Potencjalny napastnik może wykorzystać przedmiotową podatność w ataku Web Cache Poisoning, polegającym na zmanipulowaniu pamięci cache serwera proxy, który może znajdować się przed aplikacją, w taki sposób, iż zwykli użytkownicy po wysłaniu żądania do aplikacji zostaną przeniesieni na potencjalnie złośliwą stronę, będącą pod kontrolą atakującego.

Innym, potencjalnym wykorzystaniem podatności Host Header Injection jest atak na formularz zmiany hasła do aplikacji. Jeżeli atakujący poda w formularzu adres mailowy ofiary, a w żądaniu do serwera aplikacji zmieni nagłówek „Host", ofiara może otrzymać w wiadomości email link do zmiany hasła, który będzie prowadził do strony kontrolowanej przez atakującego, łudząco podobnej do prawdziwej strony aplikacji. Aplikacja powinna posiadać listę zaufanych domen i odrzucać wszystkie żądania, w których domena znajdująca się w nagłówku „Host" nie znajduje się na przedmiotowej liście.



e) Server-Side Request Forgery;

Podatność polegała na wysłaniu przez serwer testowanej aplikacji żądania do dowolnego zasobu wybranego przez atakującego. Błąd polegał na tym, iż aplikacja pobierała wartość nagłówka żądania „Referer", będącego pod kontrolą atakującego i wysyłała żądanie do zasobu wyspecyfikowanego we wspomnianym nagłówku. Podatność mogła umożliwić adwersarzowi interakcję z wewnętrznymi zasobami sieciowymi.

Poniżej widać żądanie do serwera wraz ze zmanipulowanym nagłówkiem „Referer" z wartością wskazującą na serwer atakującego:

Serwer atakującego, nasłuchujący połączenia klienta.

Aplikacja powinna posiadać listę dopuszczonych domen, do których może wysyłać żądania.

f) SQL Injection typu Blind;

SQL Injection jest podatnością pozwalająca atakującemu wstrzyknąć do zapytania SQL (kierowanego do produkcyjnej bazy danych, z której korzysta witryna WWW) własny fragment kodu SQL. Podatność SQL Injection typu Blind nie pozwala w bezpośredni sposób uzyskać informacje z bazy danych, jednakże metodą prób i błędów, wysyłając znaczną ilość żądań przy pomocy automatycznych narzędzi/skryptów, można pozyskać dane z całej bazy danych lub interesujących napastnika tabel.

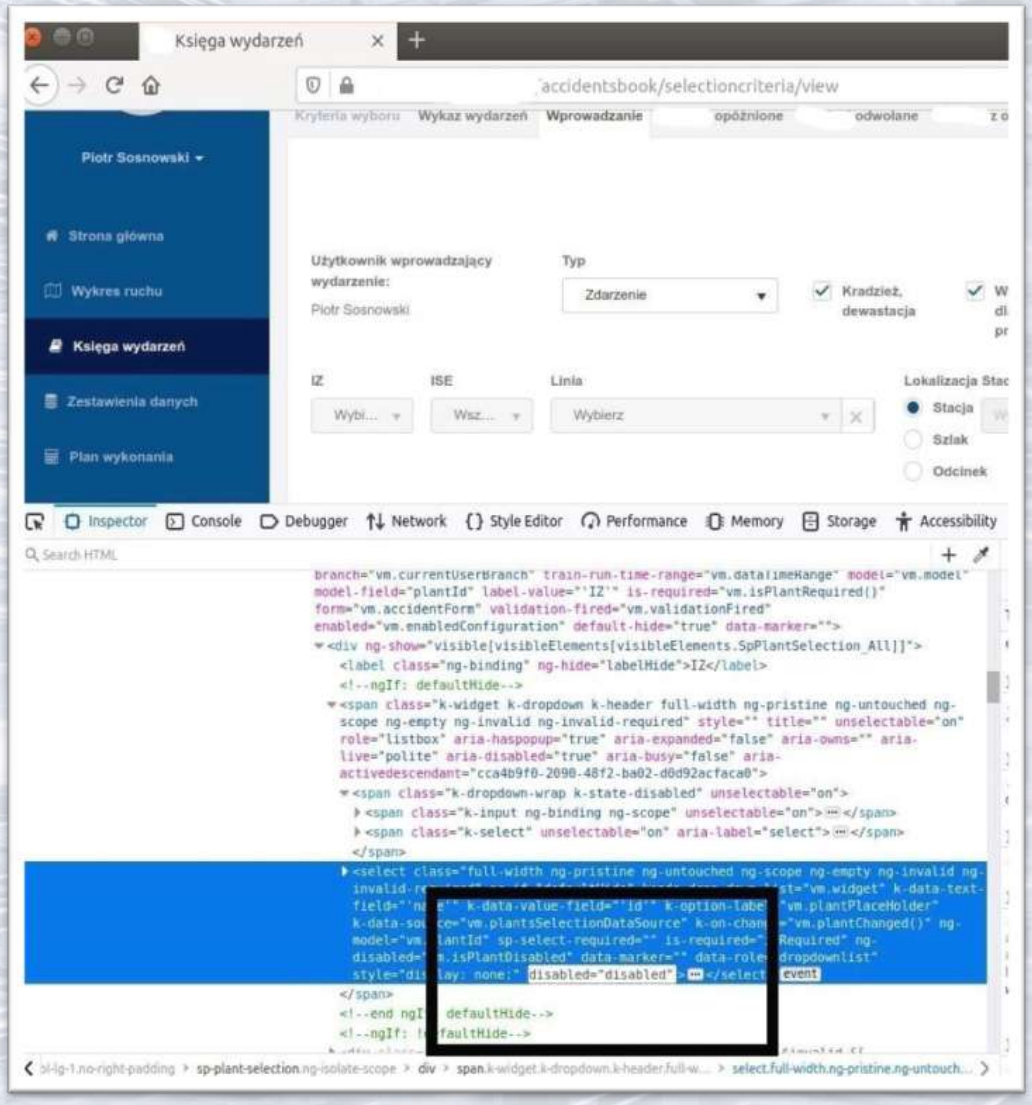
W testowanej aplikacji błąd występował w parametrze żądania GET „searchFilter".

Poniżej przykład wstrzyknięcia funkcji SQL – Sleep.

Aplikacja nie powinna dołączać danych pochodzących od użytkownika bezpośrednio do zapytania SQL. Zamiast tego dane użytkownika powinny być dostarczone w zapytaniu jako parametr (tzw. Prepared Statement). Ponadto wszelkie znaki specjalne pochodzące od użytkownika powinny być enkodowane lub usunięte.

g) Niewłaściwa kontrola dostępu;

Przykładem niewłaściwej kontroli uprawnień był jeden z formularzy dostępnych w badanej aplikacji webowej. Testowy użytkownik o nazwie „Piotr Sosnowski" miał odebrane uprawnienia do dostępu i teoretycznie nie miał możliwości wypełnienia formularza jak również jego wysłania. Zabezpieczenie odbierające mu tę możliwość opierało się wyłącznie na dodaniu atrybutu „disabled" w tagach „select", co widać na poniższym zrzucie z ekranu.



Usunięcie atrybutu „disabled" spowodowało, iż formularz stał się całkowicie dostępny i umożliwił przesłanie zgłoszenia. Takie zachowanie aplikacji mogło świadczyć, iż kontrola dostępu miała miejsce po stronie klienta i mogła spowodować wyciek lub modyfikację potencjalnie wrażliwych danych przez nieuprawnionego użytkownika. Prawidłowa kontrola dostępu powinna odbywać się zarówno po stronie klienta jak i po stronie serwera.

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

a) Akceptowanie połączeń z wykorzystaniem szyfrowania SSL 2.0, 3.0, TLS 1.0;

b) Wsparcie dla słabych algorytmów szyfrowania SSL (długość klucza od 64 do 112 bit-ów);

c) Wykorzystywanie algorytmów hashowania podatnych na kolizję tj. m.in. MD2, MD4, MD5 lub SHA1;

d) Podatność DROWN w SSLv2 – możliwa deszyfracja przechwyconego ruchu TLS;

e) Podatność POODLE w SSLv3 – możliwe przeprowadzenie ataku typu Man-in-the-Middle;

f) Stosowanie certyfikatów typu „self-signed" - certyfikat X.509 serwerów podpisany przez nieznane centrum autoryzacyjne (CA);

g) Internet Key Exchange (IKEv1) – stosowanie trybu Aggressive Mode;

h) Serwery Apache podane na ataki typu Slow HTTP DoS;

i) Brak skonfigurowanego Network Level Authentication (NLA) dla serwerów RDP;

j) Stosowanie usługi Telnet.

W ramach prowadzonych ocen bezpieczeństwa Zespół CSIRT GOV przeprowadził również analizę źródeł otwartych, tzw. OSINT. Czynności te pozwoliły na określenie publicznie dostępnych danych zawartych m.in. jako metadane w dokumentach publikowanych w ramach serwerów WWW oraz portali społecznościowych, na których pracownicy poszczególnych instytucji posiadali aktywne konta. Dane te mogą posłużyć do przeprowadzenia ataków socjotechnicznych na pracowników instytucji.

6. PROAKTYWNE DZIAŁANIA ZESPOŁU CSIRT GOV

W 2021 roku Zespół CSIRT GOV wziął udział w kolejnej edycji ćwiczeń CYBER CONFLICT EXERCISES.

CCE2021

W 2021 roku po raz kolejny Zespół CSIRT GOV uczestniczył w ćwiczeniach Cyber Conflict Exercise (CCE2021), których organizatorem była południowo-koreańska instytucja CSTEC-Cyber Security Training and Exercise Center. Ćwiczenia zostały przeprowadzone w formie zdalnej za pośrednictwem sieci Internet. Zadania postawione przez organizatorów dotyczyły szeroko pojętej teleinformatyki oraz cyberbezpieczeństwa i miały w dużej mierze charakter zawodów typu CTF (Capture The Flag). Zadania z którymi zmierzyli się uczestnicy dotyczyły m.in.:

- obrony infrastruktury przed aktywnymi atakami;
- informatyki śledczej;
- przełamania zabezpieczeń aplikacji oraz serwerów www;
- programowania;
- analizy ruchu sieciowego;
- analizy złośliwego oprogramowania;
- analizy baz danych;

Zadania postawione przed uczestnikami w dużej mierze odzwierciedlały wyzwania, z którymi spotkać się można na co dzień w obszarze cyberbezpieczeństwa właściwym dla zespołów reagowania na incydenty bezpieczeństwa komputerowego.

LOCKED SCHIELDS

W dniach 13-16 kwietnia 2021 roku odbyły się ćwiczenia o kryptonimie „Locked-Shields 2021" do udziału w których zaproszeni zostali członkowie zespołu CSIRT GOV. Ćwiczenia „LockedShields" to największe na świecie ćwiczenia z zakresu cyberobrony, które organizowane są cyklicznie przez NATO CooperativeCyber-Defence of Excellence (CCDCOE). Ćwiczenia LS w 2021 roku to 22 zespoły Blue Team z różnych krajów, około 5 tysięcy elementów wirtualnego środowiska, które zgodnie ze scenariuszem są celem ponad 4 tysięcy ataków realizowanych w czasie rzeczywistym. Oprócz zabezpieczenia złożonych systemów IT/OT, zespoły Blue Team miały za zadanie skutecznie rozwiązywać incydenty, podejmować strategiczne decyzje oraz rozwiązywać zadania z zakresu informatyki śledczej, prawa oraz mediów. Polski zespół Blue Team współtworzyli eksperci m.in. z Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni, krajowych Zespołów CSIRT, instytucji finansowych, energetycznych oraz sektora prywatnego i uczelni wyższych. Polski Zespół w klasyfikacji finalnej zajął wysokie 4 miejsce, zdobywając łącznie 58 166 punktów, przy średniej dla wszystkich drużyn wynoszącej 40 443 punktów. Zwycięska drużyna Szwecji zdobyła ok. 62 000 punktów.

W 2021 roku Zespół CSIRT GOV brał także udział w konsultacjach dotyczących wypracowania rekomendacji wzmacniających cyberbezpieczeństwo w sektorze energii oraz stosownych wytycznych sektorowych dotyczących zgłaszania incydentów. Konsultacje te były nadzorowane przez organ właściwy ds. cyberbezpieczeństwa w sektorze energii, tj. Ministerstwo Klimatu i Środowiska. W wyniku zakończenia prac powstał dokument „Rekomendacje dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa w sektorze energii oraz wytyczne sektorowe dotyczące zgłaszania incydentów", który został opublikowany na stronach rządowych we wrześniu 2021 roku. W ramach przedmiotowego dokumentu zostało uwzględnione szereg obszarów cyberbezpieczeństwa istotnych z punktu widzenia sektora energii, jak również przydatnych dla innych obszarów usług kluczowych. Wartym zapoznania w dokumencie jest formularz weryfikacji dojrzałości cyberbezpieczeństwa organizacji pozwalający przede wszystkim

na określenie pozycji danego podmiotu z punktu widzenia wdrożenia środków dla określonych w formularzu obszarów kontroli bezpieczeństwa obejmujących identyfikację, ochronę, wykrywanie, reagowanie oraz odtwarzanie.

Jednocześnie w rekomendacjach przedstawiono zadania leżące po stronie operatorów usług kluczowych związane z zarządzaniem incydentem cyberbezpieczeństwa zgodnie z przepisami ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa, w tym sposobu zgłaszania incydentów do CSIRT GOV.

7. ZAGROŻENIA DLA OBSZARU INFRASTRUKTURY KRYTYCZNEJ

W rozdziale zostały przybliżone wybrane aspekty zagrożeń dotyczące kwestii cyberbezpieczeństwa systemów OT oraz IT, które dotyczą infrastruktury krytycznej jak również operatorów usług kluczowych, na które należy zwrócić uwagę w ramach zapewnienia ciągłości działania procesów przemysłowych czy kluczowych.

W ramach swoich ustawowych obowiązków Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV realizuje zadania ukierunkowane na rozpoznawanie i wykrywanie zagrożeń godzących w bezpieczeństwo istotnych z punktu widzenia ciągłości funkcjonowania Rzeczpospolitej Polskiej systemów teleinformatycznych organów administracji publicznej, jak również systemów i sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej czy operatorów usług kluczowych (IK i OUK). Zadania CSIRT GOV na rzecz obszaru IK i OUK obejmują przede wszystkim obsługę incydentów cyberbezpieczeństwa, wydawanie rekomendacji i ostrzeżeń o zagrożeniach w cyberprzestrzeni, wdrażanie systemu wczesnego ostrzegania ARAKIS GOV, jak również prowadzenie ocen bezpieczeństwa systemów teleinformatycznych znajdujących się w podmiotach należących do IK i OUK. Szereg wskazanych zadań ukierunkowany na obszar IK i OUK realizowany jest w ramach statutowych kompetencji Zespołu CSIRT GOV, uwzględniając znaczenia sektora infrastruktury krytycznej jak i usług kluczowych w systemie bezpieczeństwa państwa.

Analizując kwestie cyberbezpieczeństwa dotyczące infrastruktury krytycznej i operatorów usług kluczowych można wyróżnić określonego rodzaju zagrożenia, które w szczególności należy uwzględnić przy nadzorze cyberbezpieczeństwa infrastruktury OT oraz IT.

Cyberbezpieczeństwo systemów wspierających usługi kluczowe czy krytyczne nabiera szczególnego znaczenia z uwagi na postępującą integrację/konwergencję systemów OT z obszarem IT. Proces ten podyktowany jest przede wszystkim kwestiami biznesowymi, w tym możliwością integracji środowiska OT w ramach zarządzania usługami przedsiębiorstw, które przebiegają w obszarze IT.

Zjawisko to, poza uwarunkowaniami rynkowymi, niesie za sobą ryzyko materializacji określonego rodzaju cyberzagrożeń, które jako właściwe dla IT staje się także istotnym elementem kształtującym bezpieczeństwo infrastruktury

OT. Na poziom tego typu ryzyk IT w obszarze OT mają wpływ przede wszystkim uwarunkowania takie jak: uproszczone przenoszenie praktyk właściwych dla cyberbezpieczeństwa IT na obszar OT czy niedostrzeganie aspektów zarządzania bezpieczeństwem OT w postaci wykorzystywania kadry zajmującej się tylko infrastrukturą/posiadającą tylko doświadczenie w obszarze IT.

Jednym z filarów bezpieczeństwa usług kluczowych jak również krytycznych jest bezpieczeństwo sieci i systemów wykorzystujących technologie teleinformatyczne do zapewnienia ciągłości działania właściwych usług wytwórczych. Wśród najistotniejszych aspektów znacząco wpływających na bezpieczeństwo realizowanej usługi jest świadomość osób realizujących zadania związane z procesem technologicznym. Wobec rozwijającej się digitalizacji nieuniknione jest inwestowanie w **podnoszenie kwalifikacji pracowników** odpowiedzialnych za cyberbezpieczeństwo infrastruktury, w tym w obszarze OT. Brak merytorycznego przygotowania do realizacji zadań z tego obszaru obniża poziom odporności systemów IT i OT na cyberzagrożenia.

Konsekwencją braku podnoszenia kwalifikacji pracowników w zakresie kompetencji cyberbezpieczeństwa OT są możliwości materializacji zdarzeń, które prowadzą do incydentów naruszających bezpieczeństwo procesów przemysłowych. Przykładem sytuacji niewłaściwego podejścia personelu zajmującego się cyberbezpieczeństwem może być np. aktywne skanowanie systemów sterowania procesem technologicznym infrastruktury przemysłowej przez służby stricte związane z IT, w ramach audytu bezpieczeństwa. Zastosowanie narzędzi IT do użycia w środowisku przemysłowym bez właściwej konfiguracji skanera oraz uwzględnienia szczególnych cech środowiska OT może doprowadzić do istotnego zakłócenia pracy segmentu przemysłowego powodując jego awaryjne odstawienie. Innym przykładowo niewłaściwym podejściem jest umożliwienie prowadzenia prac serwisowych przez niewykwalifikowany zespół wykonawcy zewnętrznego, lekceważąc tym samym podstawowe wymagania w zakresie zapewnienia bezpieczeństwa systemów teleinformatycznych wspierających pracę infrastruktury przemysłowej.

Opisane ryzyka mogą być także wynikiem łączenia urządzeń informatycznych oraz usług im towarzyszących ze sprzętem i oprogramowaniem wykorzystywanym do sterowania i nadzoru nad procesami technologicznymi i produkcyjnymi.

W celu uniknięcia podobnych zdarzeń należy przede wszystkim zaprojektować, wdrożyć a następnie utrzymywać systemy IT/OT wg zasad segmentacji tychże systemów. **Prawidłowe odseparowanie środowiska IT od OT** znacząco podnosi bezpieczeństwo świadczenia usługi kluczowej poprzez ograniczenie dostępu do krytycznych danych i systemów. Tym samym, tego typu scenariusze pokazują, że brak właściwej konfiguracji oraz nieuwzględnienie szczególnych cech środowiska OT może doprowadzić do ograniczenia świadczenia danej usługi bądź jej awaryjnego wyłączenia.

Wśród elementów mających istotne znaczenie jest także kwestia punktów wejścia do infrastruktury OT. Użytkowanie rozległej infrastruktury OT zwiększa ryzyko zakłócenia jej działania i prób nieuprawnionego dostępu. Dotyczy to zwłaszcza dostępu opartego o dostęp bezprzewodowy, np. WiFi, jak również dostęp oparty o urządzenia sieciowe funkcjonujące w sieci Internet. Tego typu dostępy narażone są na ciągłe skanowania oraz próby eksploitacji, jak również ataki naruszające dostępność usług. Eksploatacja tych punktów musi uwzględniać restrykcyjne ustawienia bezpieczeństwa (m.in. redundację), stosowanie rozwiązań typu firewall oraz monitorowanie dostępu w ramach systemów alertowych.

Kolejnym aspektem bezpieczeństwa obszaru IK i OUK jest kwestia zwiększenia się znaczenia pracy zdalnej przez personel lub firmy świadczące usługi utrzymaniowo-wdrożeniowe. Upowszechnienie pracy zdalnej wymogło na IK i OUK potrzebę zapewnienia bezpiecznej komunikacji dla tych obiektów. W tym celu w komunikacji przy użyciu należy stosować odpowiednie protokoły szyfrujące, np. TLS (Transport Layer Security) czy zalecane uwierzytelnianie wieloskładnikowe MFA (MultifactorAuthentication), które mają na celu zapewnienie dodatkowej ochrony i weryfikacji użytkownika w czasie logowania. Z uwagi na aspekt pracy zdalnej większość pracodawców wprowadziło korzystanie z wirtualnych sieci prywatnych tzw. VPN (Virtual Private Network) pozwalających na bezpieczny dostęp do zasobów danego przedsiębiorstwa. Warunkiem świadczenia pracy na zasadach tzw. homeoffice jest posiadanie przez pracodawcę właściwej architektury brzegowej wyposażonej w systemy monitorowania sesji czy odpowiednie tzw. stacje przesiadkowe. Istotne dla bezpieczeństwa danego środowiska przemysłowego jest również **wprowadzenie rozwiązań dla zarządzania dostępem zdalnym** przez operatorów ze środowiska OT,a nie IT.

Osobnym zagadnieniem jest procedura udzielenia zdalnego dostępu pod-

miotom zewnętrznym bądź kontraktorom do zasobów operatora usługi kluczowej czy infrastruktury krytycznej. Nie rekomenduje się, żeby pracownicy podmiotów implementujących systemy teleinformatyczne na obiektach IK/OUK korzystali z możliwości zdalnego dostępu do środowiska komputerowego klienta na swoich zasadach. W każdym przypadku opisana sytuacja powinna być ściśle monitorowana, w tym, tak jak dla pracowników, możliwość pracy zdalnej powinna być kontrolowana w oparciu o tzw. stacje przesiadkowe. Dodatkowo, w celu zwiększenia bezpieczeństwa styku sieci przemysłowej ze stacją przesiadkową, rekomendowane jest **wdrożenie polityki tzw. whitelisting-u** wyłącznie wymaganych aplikacji na stacjach przesiadkowych. Ponadto, w kontekście zdalnego dostępu do systemów teleinformatycznych należy zapewnić odpowiedni poziom wsparcia technicznego za pośrednictwem personelu przeszkolonego z właściwych procedur i instrukcji związanych z pracą zdalną. Jednocześnie należy unikać sytuacji, w których dostawca sprzętu lub oprogramowania posiada stałe podłączenie do sieci przemysłowych. Dodatkową warstwą ochrony połączeń zdalnych może być wykorzystanie reguł dopuszczających połączenia wyłącznie z zaufanych adresów IP lub ograniczających do konkretnego obszaru geograficznego (np. kraju).

Ważnym zadaniem stawianym osobom zapewniającym wsparcie dla wszystkich pracowników realizujących swoje obowiązki służbowe jest również obsługa incydentów, która musi być realizowana przez **dedykowane zespoły cyberbezpieczeństwa w ramach Security Operation Center**, czy ewentualnie w ramach zespołu reagowania na incydenty, z dostępem do systemów monitoringu i alertowania klasy SIEM lub SOAR. W tym zakresie powinny zostać utworzone i przetestowane procedury obsługi zdarzeń w tym reagowanie na zagrożenia równolegle zarówno w sieciach IT oraz OT.

Wśród ryzyk, które należy dostrzegać jako następstwo niewłaściwego podejścia do bezpieczeństwa OT, należy wskazać zagrożenia typu ransomware. Czynnikiem zwiększającym skalę potencjalnego ataku, co jeszcze raz warto podkreślić, jest brak separacji OT od infrastruktury IT, tym samym może to naruszyć ciągłość działania infrastruktury przemysłowej. Zagrożenia ransomware utrzymują się globalnie stale na wysokim poziomie. W 2021 roku incydenty z użyciem ransomware dotknęły wiele przedsiębiorstw na świecie, szczególnie w branżach o krytycznym znaczeniu. W centrum zainteresowania grup wykorzystujących ransomware do wymuszania okupów w zamian za udostępnienie

możliwości dekrypcji plików był przede wszystkim sektor energetyczny. Niewątpliwie, motywacja merkantylna grup haktywistycznych ukierunkowuje ich zainteresowanie na „większe przedsiębiorstwa". Przykładem tego typu ataków w 2021 roku, był atak na amerykański koncern Colonial Pipeline, mający znaczny udział w przesyle paliw znad Zatoki Meksykańskiej na zachodnie wybrzeże USA. Problem „szantażu komputerowego" (uniemożliwienie korzystania z własnych zasobów oraz sieci, eksfiltracja w celu późniejszego ujawnienia danych) dotyczy również polskich podmiotów. Należy podkreślić, że skutki materializacji skutecznych ataków ransomware w ramach OK czy OUK mogą prowadzić do naruszenia świadczenia usługi krytycznej czy kluczowej. Wskazywanymi praktycznymi metodami ochrony przed atakami typu ransomware są **stałe aktualizacje podatnych komponentów infrastruktury, silna segmentacja sieci, wprowadzanie rozwiązań na zasadzie „security by design", tworzenie kopii zapasowych danych kluczowych**. Elementem, który należy uwzględnić przy mitygacji tego typów ataków jest także polityka bezpieczeństwa aktualizacji komponentów sprzętowych czy programowych infrastruktury IK oraz OUK, jak również procedury bezpieczeństwa dotyczące dostawców, w tym dotyczące zapewnienia bezpiecznego łańcucha dostaw.

Kolejnym ryzykiem związanym z cyberbezpieczeństwem w sieciach OT jest brak identyfikacji poszczególnych zagrożeń ukierunkowanych na dany typ organizacji oraz brak pełnej inwentaryzacji wykorzystywanych zasobów sprzętowych, oprogramowania oraz wykorzystywanych technologii.

Reasumując, dla zapewnienia niezakłóconej ciągłości działania podmiotów IK i OUK ważne jest niepowielanie schematów działania dotyczących stricte infrastruktury IT, a ich odpowiednie wykorzystanie w ramach procesów przemysłowych funkcjonujących w oparciu o całą gamę urządzeń automatyki przemysłowej, sterowników czy systemów sterowania.

8. PODSUMOWANIE

W 2021 roku Zespół CSIRT GOV zarejestrował ponad trzykrotny wzrost zgłoszeń o potencjalnym wystąpieniu incydentu bezpieczeństwa teleinformatycznego w stosunku do roku poprzedniego. Wynika to w głównej mierze ze wzrostu liczby alarmów generowanych przez system ARAKIS GOV, który na przestrzeni minionego roku był sukcesywnie rozwijany m.in. o nowe sygnatury ataków oraz nowe instalacje sond. Niemniej jednak wzrost liczby zgłoszeń przełożył się również na wzrost faktycznych incydentów, których odnotowano 26 899, co było rekordowym wynikiem w ramach prowadzonych statystyk Zespołu CSIRT GOV.

Biorąc pod uwagę klasyfikację incydentów, w dalszym ciągu palmę pierwszeństwa dzierży kategoria WIRUS, obejmująca detekcję aktywności szkodliwego oprogramowania. Na specjalną uwagę może zasługiwać fakt, iż drugie miejsce zajęła kategoria PODATNOŚĆ, dotycząca całego szeregu ujawnionych w 2021 roku błędów w popularnie wykorzystywanym oprogramowaniu. Można dla przykładu wymienić tutaj chociażby głośne medialnie podatności ProxyLogon, ProxyShell, czy Apache Log4J. Ponadto, tradycyjnie już wysokie miejsce wśród odnotowanych zagrożeń zajęła SOCJOTECHNIKA, która na przestrzeni ostatnich lat niezmiennie jest jednym z najpopularniejszych, o ile nie najpopularniejszym wektorem ataku.

Rok 2021 to także odnotowana przez Zespół CSIRT GOV aktywność grup sponsorowanych, popularnie określanych mianem grup APT - Advanced Persistent Threat. Jest to szczególnie widoczne w kontekście administracji publicznej oraz infrastruktury krytycznej. Wśród zidentyfikowanych przez Zespół CSIRT GOV zagrożeń tego typu można wyróżnić takie jak np. APT29, APT31, czy Snake/Turla. Podsumowując miniony rok, nie sposób nie wspomnieć o zagrożeniu, którego sprawstwo przypisuje się grupie UNC1151 i kampanii o nazwie Ghostwriter. Jej działania łączyły w sobie wektor ataku oparty o techniki socjotechniczne z długofalowym przygotowaniem i koordynacją, wpisującą się w techniki, taktyki i procedury tradycyjnych grup APT.

Kolejnym, odnotowanym w 2021 roku i wartym uwagi elementem jest rodzaj identyfikowanego przez Zespół CSIRT GOV złośliwego oprogramowania. Zdecydowanie najczęściej wykorzystywanym w roku ubiegłym złośliwym oprogramowaniem był malware Agent Tesla, a na dalszych miejscach znalazły się m.in. Snake Keylogger i GuLoader. W dalszym ciągu najpopularniejszą metodą

propagacji jest tutaj masowa wysyłka wiadomości email z załącznikiem, często w postaci plików archiwum z hasłem. Powyższe pozwala napastnikowi na ominięcie silników antywirusowych. Dodatkowo, przeanalizowane przez Zespół CSIRT GOV próbki złośliwego oprogramowania wskazują, że najczęściej posiadanymi przez malware funkcjami są te, które pozwolają na ominięcie zabezpieczeń systemu operacyjnego, jak np.: anty-debugging czy obfuskacja.

Jednym z istotnych systemów cyberbezpieczeństwa wspierającym pracę Zespołu CSIRT GOV w zakresie wykrywania i ostrzegania przed zagrożeniami w sieci Internet jest system ARAKIS GOV. W 2021 roku przedmiotowy system wygenerował przeszło trzy miliony alarmów, co przełożyło się na 1 170 136 alarmów o priorytecie pilnym, tzn. wymagało niezwłocznej reakcji ze strony administratorów. Każdy z zanotowanych przez system ARAKIS GOV alarmów posiada dokładne dane techniczne, pozwalające na jego weryfikację oraz jest szczegółowo klasyfikowany do poszczególnego typu. Wśród odnotowanych w 2021 roku typów zdecydowanie przodowały Typ 1 - komunikacja do złośliwych adresów IP/domen oraz Typ 2 - skanowanie.

W 2021 roku Zespół CSIRT GOV przeprowadził ocenę bezpieczeństwa 149 segmentów sieci/systemów teleinformatycznych oraz 36 domen/subdomen internetowych w 17 instytucjach administracji publicznej oraz infrastruktury krytycznej. W wyniku powyższego Zespół CSIRT GOV zidentyfikował 185 krytycznych błędów, co stanowi blisko dwukrotny wzrost w porównaniu do roku poprzedniego, a także 394 błędów o stopniu wysokim, które mogły skutkować przełamaniem zabezpieczeń przez adwersarza i tym samym prowadzić do eskalacji zagrożenia.

W roku 2021, Zespół CSIRT GOV wziął udział także w międzynarodowych ćwiczeniach oraz warsztatach Locked Schields oraz Cyber Conflict Excercise.

Spis tabel:

Tabela 1. Zachowania analizowanych plików/zasobów internetowych.....34
Tabela 2. 10 najczęściej identyfikowanych reguł.....35
Tabela 3. Główne typy plików poddawane analizie malware.....36
Tabela 4. Zidentyfikowane w 2021 roku skanowania i próby eksploitacji usług na podstawie danych z systemu ARAKIS GOV.....41
Tabela 5. Najczęściej dopasowane reguły do ruchu sieciowego widzianego przez system ARAKIS GOV.....42

Spis wykresów:

Wykres 1. Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych latach.....9
Wykres 2. Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych kwartałach 2021 r.....11
Wykres 3. Statystyka incydentów w 2021 roku z podziałem na kategorie.....14
Wykres 4. Liczba incydentów wg sektorów.....16
Wykres 5. Ostrzeżenia wysłane przez Zespół CSIRT GOV.....17
Wykres 6. Wyniki analizy zgłoszonych plików.....32
Wykres 7. Statystyka miesięczna analizowanych plików.....32
Wykres 8. Klasyfikacja oprogramowania złośliwego.....33
Wykres 9. Procentowy rozkład alarmów systemu ARAKIS GOV ze względu na priorytet.....38
Wykres 10. Procentowy podział alarmów systemu ARAKIS GOV ze względu na typ.....39
Wykres 11. Procentowy podział przepływów alarmów typu 2 w instytucjach.....40
Wykres 12. Rozkład źródeł ataków na sieci monitorowane przez system ARAKIS GOV pod kątem liczby generowanych przepływów.....41
Wykres 13. Zestawienie zidentyfikowanych podatności z podziałem na priorytet.....44

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

praca@csirt.gov.pl