2021 Podsumowanie Roku w CSIRT KNF

OPIS WYBRANYCH ATAKÓW

CSIRT KNF

GENEZA POWSTANIA

Zespół CSIRT KNF realizujący zadania Sektorowego Zespołu Cyberbezpieczeństwa, we współpracy z podmiotami krajowego systemu cyberbezpieczeństwa, a w szczególności zespołami CSIRT poziomu krajowego, wspiera Operatorów Usług Kluczowych w obsłudze incydentów poważnych występujących w tych podmiotach, a także prowadzi działania mające na celu analizę pozostałych incydentów, trendów i zagrożeń w obszarze cyberbezpieczeństwa.

CELE

Głównym celem działań Sektorowego Zespołu Cyberbezpieczeństwa jest realizacja zadań określonych w Art. 44 Ustawy k.s.c. obejmujących m.in.:

- przyjmowanie zgłoszeń o incydentach poważnych oraz wsparcie w obsłudze tych incydentów;
- wspieranie OUK w wykonywaniu obowiązków określonych w Ustawie;
- analizowanie incydentów poważnych, wyszukiwanie powiązań pomiędzy incydentami oraz opracowywanie wniosków z obsługi incydentu;
- współpracę z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie koordynowania obsługi incydentów poważnych.

Rok 2021 w liczbach

CSIRT KNF

W ROKU 2021 ZGŁOSIŁ DO BLOKADY:

11,468 niebezpiecznych domen

PODZIAŁ FAŁSZYWYCH STRON NA KATEGORIE

3,986 PORTALE OGŁOSZENIOWE

3,033 USŁUGI KURIERSKIE/POCZTOWE

2,203 FAŁSZYWE INWESTYCJE

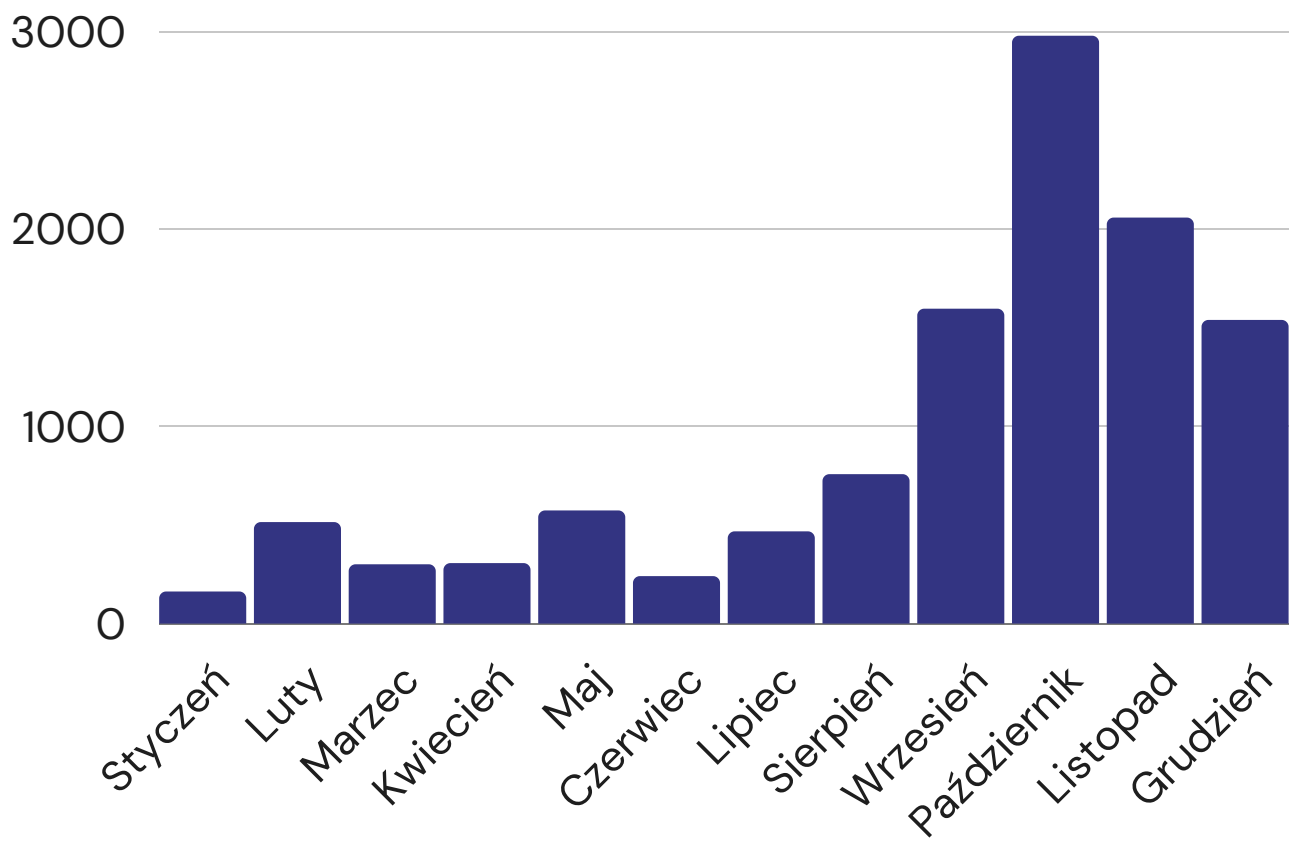
1,016 BANKI

906 INNE

324 FAŁSZYWE BRAMKI PŁATNOŚCI

Statystyki

LICZBA ZGŁOSZONYCH NIEBEZPIECZNYCH STRON.



Media

Na podstawie wiadomości pochodzących z publikacji CSIRT KNF w 2021 roku powstały **1102** artykuły w portalach branżowych oraz informacyjnych.

STATYSTKI

10

OPRACOWAŃ DOTYCZĄCYCH CYBERBEZPIECZEŃSTWA

5

ARTYKUŁÓW W PRASIE TRADYCYJNEJ O SKALI OGÓLNOPOLSKIEJ

159

OSTRZEŻEŃ OPUBLIKOWANYCH W SOCIAL MEDIA

ZASIĘG

1,087,000

REKORDOWA ILOŚĆ OSÓB, KTÓRA ZOBACZYŁA OSTRZEŻENIE

Zagrożenia w 2021 roku

Omówienie

FINANSOWE CYBERBEZPIECZEŃSTWO

Wraz ze wzrostem intensywności korzystania z usług internetowych, zwiększyła się aktywność cyberprzestępców. Najpopularniejszym sposobem ataku jest przesłanie linku zawierającego fałszywą domenę, która różni się od prawdziwej jedną literką lub słowem. Wprowadzenie danych na takiej stronie może spowodować, że trafią one do oszustów, którzy wykorzystają je do kradzieży naszych środków finansowych. Najwięcej zgłoszonych przez nas domen podszywało się pod portale ogłoszeniowe oraz firmy kurierskie, które w większości są używane do oszustwa „na kupującego". W ostatnim kwartale ubiegłego roku zaobserwowaliśmy wzmożoną aktywność wykorzystywania stron używanych do oszustwa na „fałszywe inwestycje", które posługiwały się wizerunkiem zaufanych podmiotów. Dużą popularnością wśród przestępców cieszą się również podszycia pod banki oraz bramki płatności. Inne zgłoszone przez nas domeny wyłudzały dane logowania do różnych portali internetowych. Przestępcy wykazują się dużą kreatywnością, śledzą globalne trendy oraz kierunki zachowań użytkowników, wykorzystując je aby oszustwa były bardziej wiarygodne. Poniżej prezentujemy wybrane zagrożenia z każdego miesiąca 2021 roku.

Styczeń

PODSZYCIE POD APLIKACJĘ PROTEGO SAFE

Fałszywa aplikacja mobilna rzekomo wykrywała COVID-19 za pomocą nagrania kaszlu. W rzeczywistości było to złośliwe oprogramowanie BlackRock, które po instalacji na urządzeniu było w stanie podstawiać overlay'e (nakładki) np. w aplikacjach bankowych. Dzięki temu zabiegowi wszelkie dane wprowadzone na ekranie telefonu trafiały bezpośrednio do przestępców.

Więcej możecie przeczytać w naszym artykule.

Luty

PODSZYCIE POD APLIKACJĘ „KWARANTANNA DOMOWA”

Strona przypominająca oficjalny sklep Google Play, na której umieszczono instalator oprogramowania Anubis. Złośliwa aplikacja korzystając z uprawnień związanych z ułatwieniami dostępu na telefonie, podstawia użytkownikom fałszywy panel do logowania w bankowości internetowej.

Marzec

FLUBOT

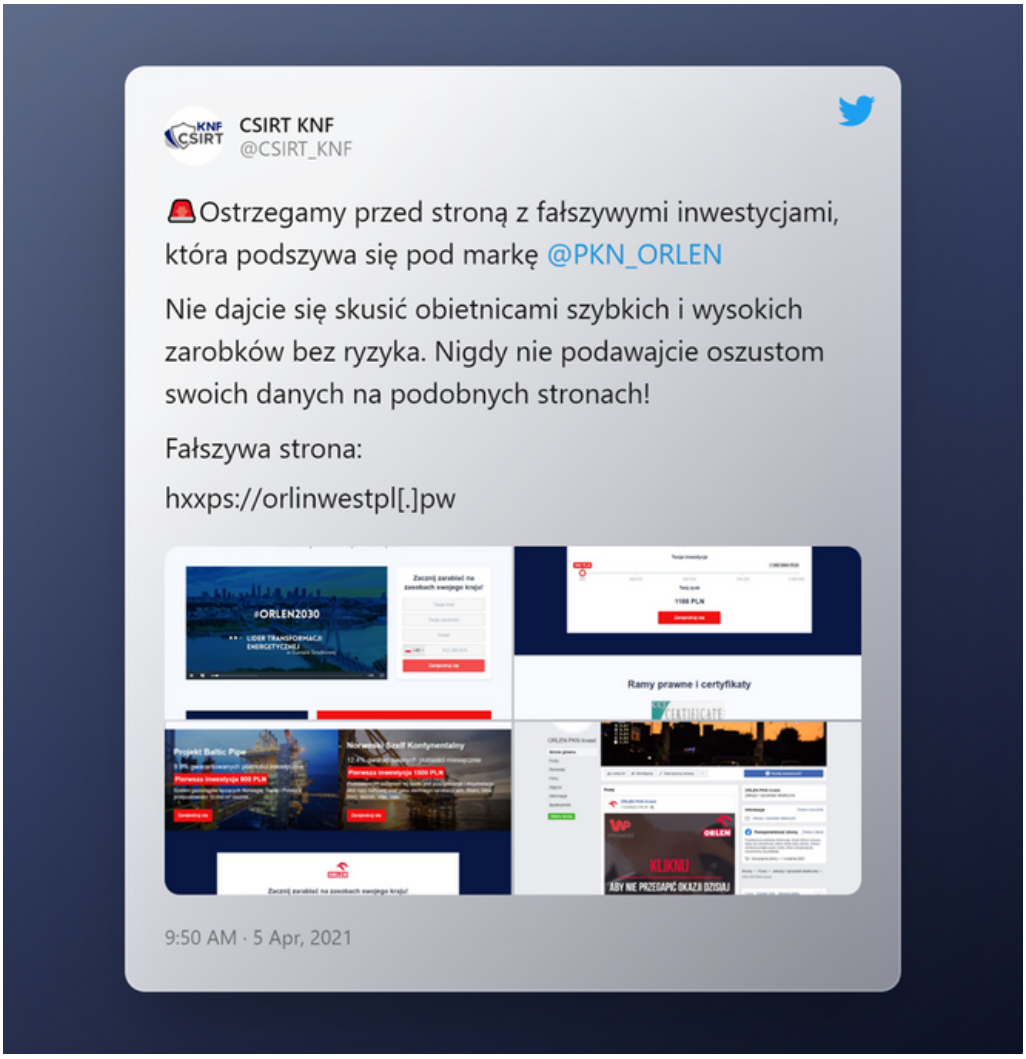
Złośliwe oprogramowanie FluBot, dystrybuowane za pomocą kampani SMS. Aplikacja po zainstalowaniu mogła wykraść dane bankowe oraz wykorzystać numery telefonów z listy kontaktów, aby następnie wysłać wiadomość sms ze szkodliwym linkiem do kolejnych osób. Treści zawarte w przesyłanych SMS-ach miały na celu nakłonienie użytkownika do kliknięcia w złośliwy link.

Więcej o Flubocie możecie przeczytać w naszym artykule.

Kwiecień

FAŁSZYWE INWESTYCJE

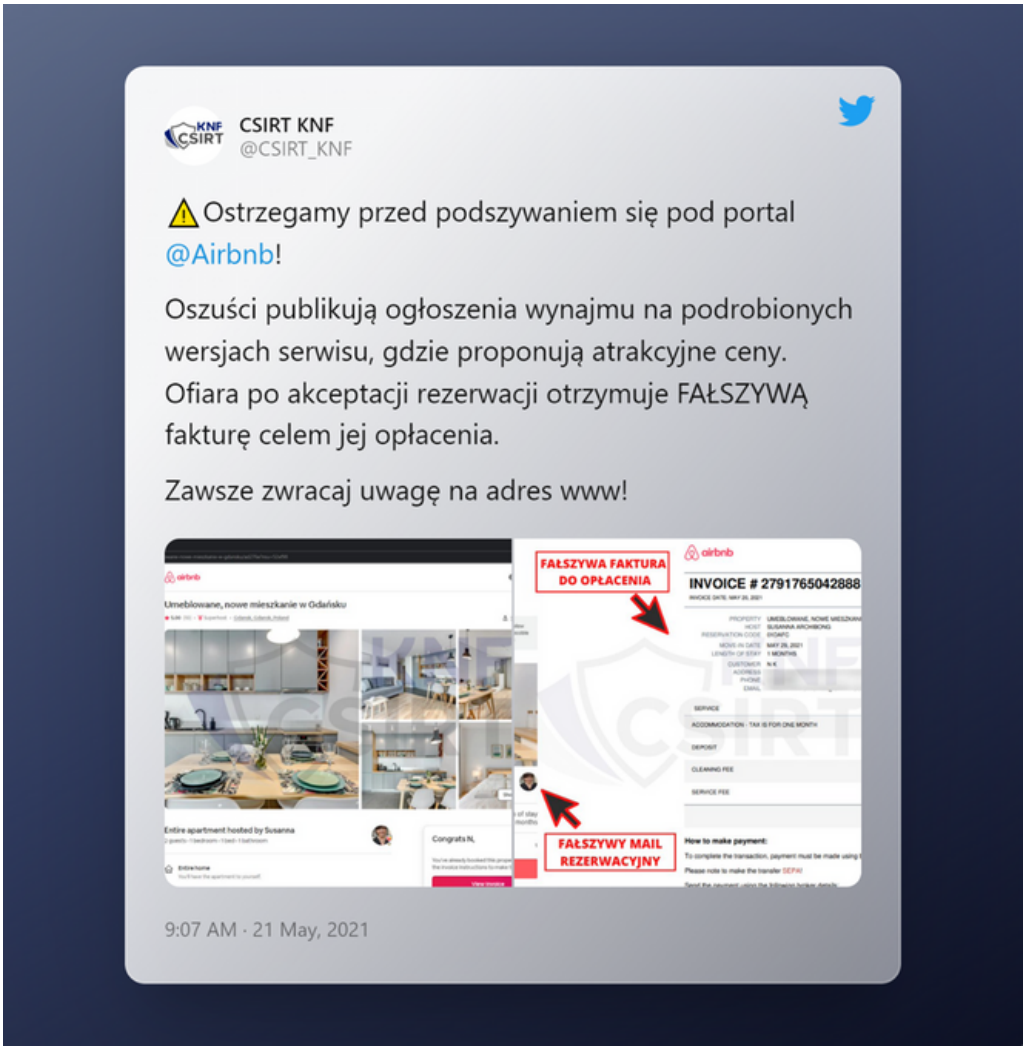
Spreparowane reklamy w mediach społecznościowych, oferujące duże zyski w krótkim czasie. Do uwiarygodnienia wykorzystywany jest wizerunek znanych osób lub zaufanych podmiotów.
Po kliknięciu w ogłoszenie następuje przekierowanie na fałszywą stronę, gdzie widnieje prośba o wypełnienie formularza kontaktowego. Po wprowadzeniu danych oszuści kontaktują się z nami przedstawiając się jako makler lub broker giełdowy. Następnie często pod presją szybkiego działania próbują nas nakłonić do zainwestowania pieniędzy, które tak naprawdę trafią do przestępców.



Maj

PODSZYWANIE SIĘ POD PORTALE OFERUJĄCE WYNAJEM KRÓTKOTERMINOWY

Strona podszywająca się pod portal oferujący wynajem miejsc noclegowych. Po dokonaniu rezerwacji za jego pomocą, otrzymywano do zapłaty fałszywą fakturę. Podobne oszustwa mogły również kierować do fałszywego panelu płatności w celu wyłudzenia poświadczeń bankowych.



Czerwiec

PODSZYWANIE SIĘ POD ZWIĄZEK BANKÓW POLSKICH

Reklama w mediach społecznościowych kierująca na fałszywą stronę wyłudzającą dane kontaktowe pod pretekstem fałszywych promocji. Pozyskane w ten sposób informacje mogły posłużyć do kolejnych oszustw lub kradzieży tożsamości.

Lipiec

FAŁSZYWY SMS O ZALEGŁOŚCIACH PŁATNOŚCI

Spreparowane wiadomości SMS z linkiem prowadzącym do opłaty za prąd. W treści zawarto informację o konieczności dopłaty za energię elektryczną, a nieuregulowanie wskazanej kwoty może spowodować jej odłączenie. Przesłany link prowadzi do fałszywej bramki płatności, która przechwytuje dane kart płatniczych podczas wykonywania transakcji.

Sierpień

PODSZYWANIE SIĘ POD PORTALE OGŁOSZENIOWE ORAZ FIRMY KURIERSKIE

Wykorzystywane głównie do oszustwa „na kupującego”. Nawiązywano kontakt ze sprzedającym, najczęściej za pomocą aplikacji Whatsapp, wysyłając link do rzekomego odbioru płatności. W rzeczywistości była to spreparowana strona, przez którą można było szybko stracić pieniądze.

Więcej o tym sposobnie oszustwa możecie przeczytać w naszym artykule.

Wrzesień

FAŁSZYWA KAMPANIA SMS Z INFORMACJĄ O SKIEROWANIU NA KWARANTANNĘ

Wiadomość zawierająca link do strony z komunikatem o nieaktualnej wersji oprogramowania Flash Player. Instalacja oprogramowania oraz nadanie jej odpowiednich uprawnień prowadziła do zainfekowania urządzenia trojanem bankowym Cerberus. W skutek tego podszywający mogli uzyskać pełen dostęp do urządzenia.

Październik

WYŁUDZENIE NA PIT

Wiadomości SMS z informacją o zwrocie podatku z rozliczenia PIT-37. Po wejściu w link zostaliśmy przekierowani na fałszywą stronę, która wyłudza dane uwierzytelniające do bankowości elektronicznej.

Listopad

PODSZYWANIE SIĘ POD STRONY BANKOWE

Specjalnie przygotowane serwisy bankowe, które pozornie mogą wyglądać jak autentyczne strony Banku. Poprzez specjalne kodowanie znaków, wykorzystano litery rozszerzonego alfabetu łacińskiego powstałe przez połączenie pojedynczej litery z kropką. Nazwy domen mogą łudząco przypominać te prawdziwe. Ataki mają na celu pozyskanie poświadczeń uwierzytelniających do bankowości elektronicznej.

Grudzień

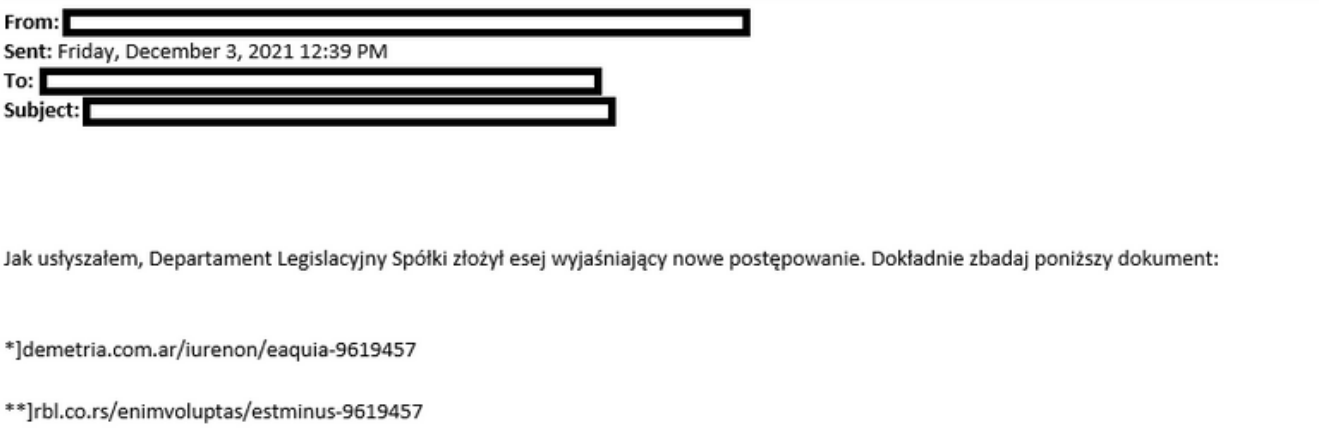
DOPŁATA DO PACZKI

Fałszywe wiadomości SMS zawierające prośbę o dopłatę do zamówionej paczki. Oszustwa te mają na celu wyłudzenie danych lub pieniędzy. Po kliknięciu w link jesteśmy przekierowani do fałszywego panelu płatności.

Zagrożenia globalne

QAKBOT

W pierwszej połowie grudnia ostrzegaliśmy przed kampanią malware, w ramach której rozsyłanie szkodliwych wiadomości odbywało się przy użyciu przejętych serwerów pocztowych. Charakterystyczną cechą kampanii było wykorzystanie przejętych serwerów w kontekście techniki reply-chain. Polega ona na rozsyłaniu wiadomości z historią konwersacji w treści, co sprawia wrażenie, że jest to kontynuacja korespondencji. W rezultacie niczego nieświadomy odbiorca może otrzymać np. wiadomość dystrybuującą złośliwe oprogramowanie, pochodzącą (jak mu się wydaje) od zaufanego nadawcy. Potencjalnymi wektorami ataku, umożliwiającymi nieautoryzowany dostęp do serwera mogą być podatności np. ProxyShell, czy ProxyLogon. Sama dystrybucja złośliwego archiwum prowadzącego do pobrania QakBota może odbywać się na kilka sposobów. Wśród nich znajdziemy wiadomość zawierającą złośliwy link, e-mail z niebezpiecznym załącznikiem, jak również umieszczony w wiadomości element graficzny wyświetlający szkodliwy adres URL.



From: [redacted]
Sent: Friday, December 3, 2021 12:39 PM
To: [redacted]
Subject: [redacted]

Jak usłyszałem, Departament Legislacyjny Spółki złożył esej wyjaśniający nowe postępowanie. Dokładnie zbadaj poniższy dokument:

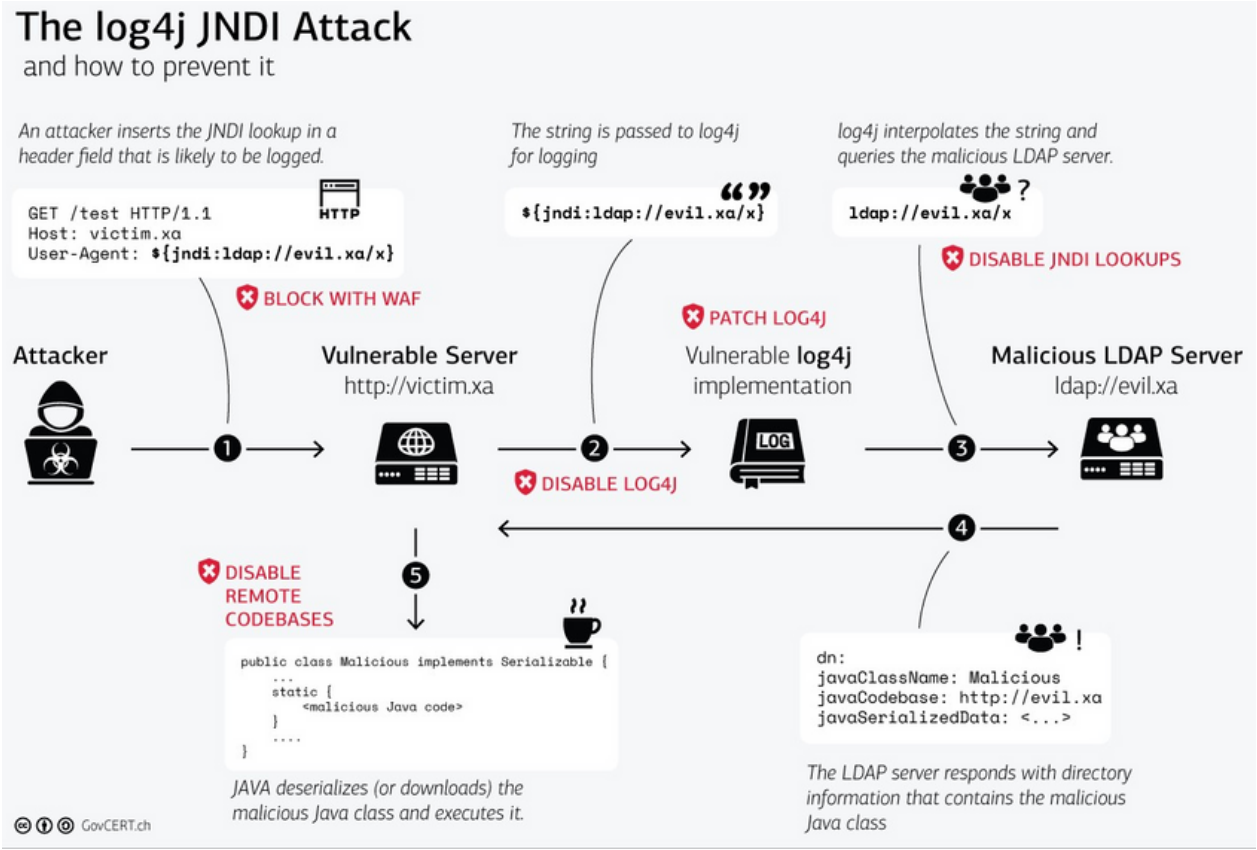
*]demetria.com.ar/iurenon/eaquia-9619457

**]rbl.co.rs/enimvoluptas/estminus-9619457

Zagrożenia globalne

LOG4SHELL

Podatność dotyczy popularnej biblioteki Java „log4j" a jej wykorzystanie daje możliwość zdalnego wykonania kodu po stronie serwera. Podatność jest aktualnie wykorzystywana przez atakujących, którzy aktywnie wyszukują podatnych elementów infrastruktury. Biblioteka ta jest jedną z najczęściej używanych bibliotek do logowania zdarzeń, wykorzystywanych przez aplikacje napisane w języku Java. Należy dodać, że z ww. biblioteki korzysta bardzo wiele komercyjnych aplikacji.



ŹRÓDŁO: GOVCERT.CH