



**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 incyduentu;
- 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**

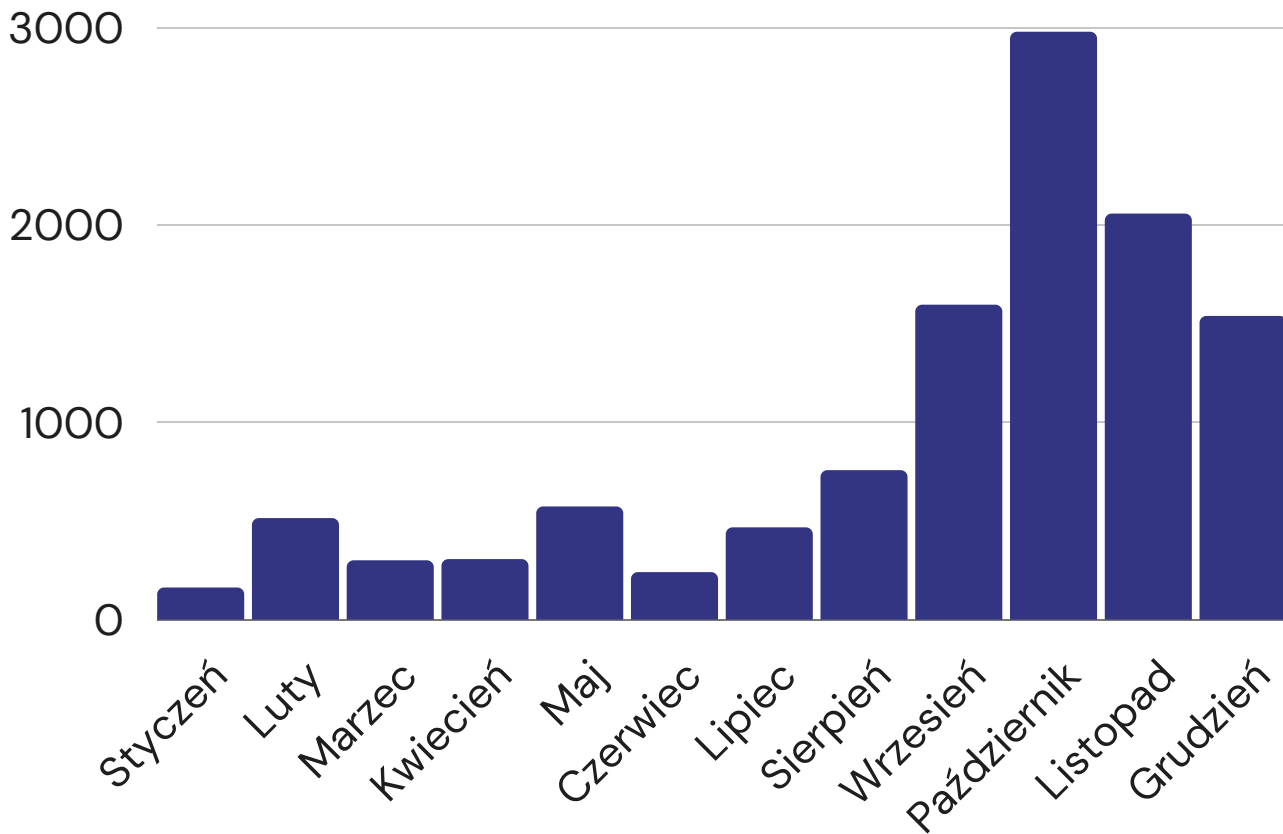
INNE

**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.

## STATYSTYKI

# 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 podstawić 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.



The image shows a screenshot of a tweet from CSIRT KNF (@CSIRT\_KNF) dated February 5, 2021, at 8:59 AM. The tweet contains a warning about a malicious application that impersonates the official 'Kwarantanna Domowa' app. The application is described as being able to steal data from online banking by using a fake login panel. A screenshot of the app's permissions is also shown, listing various Android permissions such as BIND\_ACCESSIBILITY\_SERVICE, READ\_SMS, RECEIVE\_SMS, SEND\_SMS, INTERNET, CALL\_PHONE, READ\_CONTACTS, and READ\_PHONE\_STATE. The tweet includes a URL: kwarantannadomowa[.]com.

CSIRT KNF  
@CSIRT\_KNF

Ostrzegamy przed fałszywą aplikacją podszywającą się pod "Kwarantanna domowa" od @CyfryzacjaKPRM.

Ww. Aplikacja to złośliwe oprogramowanie, które wykrada dane do bankowości internetowej za pomocą fałszywego panelu logowania do banku.

Niebezpieczny URL:  
kwarantannadomowa[.]com

8:59 AM · 5 Feb, 2021



# 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.](#)

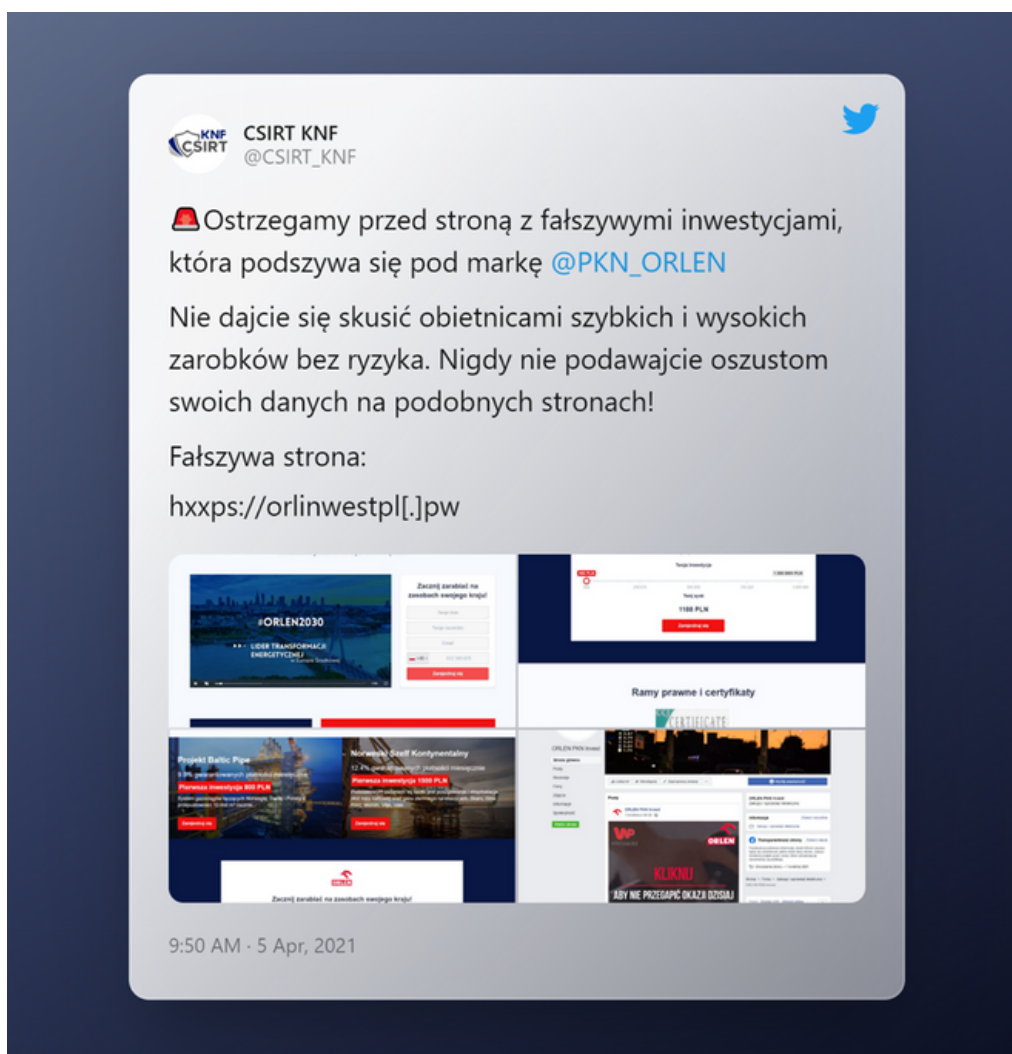


# Kwiecień

## 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.



The image shows a screenshot of a tweet from CSIRT KNF (@CSIRT\_KNF) dated 9:50 AM on April 5, 2021. The tweet contains a warning about a fraudulent investment website. The text of the tweet is as follows:

**⚠️ Ostrzegamy przed stroną z fałszywymi inwestycjami, która podszywa się pod markę @PKN\_ORLEN**

Nie dajcie się skusić obietnicami szybkich i wysokich zarobków bez ryzyka. Nigdy nie podawajcie oszustom swoich danych na podobnych stronach!

Fałszywa strona:  
[hxxps://orlinwestpl\[.\]pw](https://orlinwestpl[.]pw)

The tweet includes four screenshots of the fraudulent website. The first screenshot shows a landing page with the text "#ORLEN2030" and "LEADER TRANSFORMACJI ENERGETYCZNEJ". The second screenshot shows a "Twoje inwestycje" section with a "Nawet 12% zysk" and "1000 PLN" investment amount. The third screenshot shows a "Ramy prawne i certyfikaty" section with a "CERTIFICATE" logo. The fourth screenshot shows a "Projekt Baltic Pipe" section with "12% zysk" and "1000 PLN" investment amount. The tweet also features the CSIRT KNF logo and a Twitter bird icon.

# 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.

**CSIRT KNF**  
@CSIRT\_KNF

⚠️ Ostrzegamy przed podszywaniem się pod portal @Airbnb!

Oszuści publikują ogłoszenia wynajmu na podrobionych wersjach serwisu, gdzie proponują atrakcyjne ceny. Ofiara po akceptacji rezerwacji otrzymuje FAŁSZYWĄ fakturę celem jej opłacenia.

Zawsze zwracaj uwagę na adres [www](http://www.airbnb.com)!

**FALSZYWA FAKTURA DO OPŁACENIA**

**FALSZYWY MAIL REZERWACYJNY**

9:07 AM · 21 May, 2021

# 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.

The image shows a screenshot of a tweet from the account CSIRT KNF (@CSIRT\_KNF). The tweet contains a warning about a phishing website that impersonates the Polish Bank Association (Związek Banków Polskich). The tweet includes a warning icon, the text of the warning, the address of the phishing site, and two screenshots of the website's interface. The first screenshot shows a promotional banner for the bank association, and the second screenshot shows a page with various offers and a 'Zaloguj się' (Log in) button. The tweet is dated 4:57 PM on June 21, 2021.

**KNF CSIRT KNF @CSIRT\_KNF**

**⚠ Uwaga! Ostrzegamy przed fałszywą stroną podszywającą się pod Związek Banków Polskich. Oszuści wyłudniają od użytkowników dane kontaktowe pod pretekstem fałszywej promocji.**

Adres fałszywej strony:  
[hxxps://zwiazekbankowpolskich\[.\]com](https://zwiazekbankowpolskich[.]com)

**Związek Banków Polskich**  
28 marca Związek Banków Polskich ogłosił konkurs i konkurs nagrody gwarantowanej.  
Promocja od Związku Banków Polskich 2021 Więcej informacji

**Promocja od Związku Banków Polskich**  
Zaloguj się

**SGB Mobile**  
Aktualny kurs wymiany  
Przebieg z karty

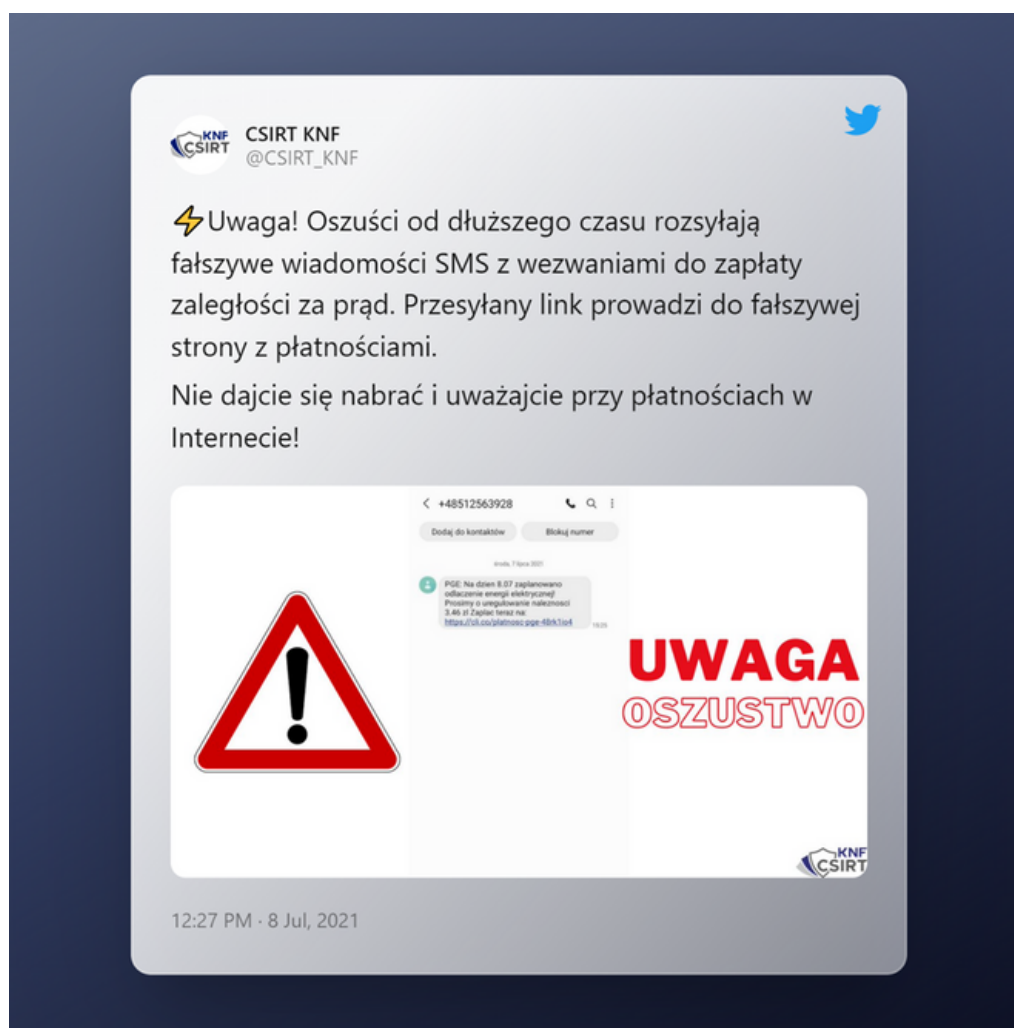
Zaloguj się na Związek Banków Polskich  
100

4:57 PM · 21 Jun, 2021

# Lipiec

## FALSZYWE 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.



The image shows a screenshot of a Twitter post from the account CSIRT KNF (@CSIRT\_KNF). The tweet contains a warning in Polish about fraudulent SMS messages. The text of the tweet is as follows:

⚡ Uwaga! Oszuści od dłuższego czasu rozsyłają fałszywe wiadomości SMS z wezwaniem do zapłaty zaległości za prąd. Przesyłany link prowadzi do fałszywej strony z płatnościami.

Nie dajcie się nabrać i uważajcie przy płatnościach w Internecie!

The tweet includes a screenshot of a text message from the number +48512563928. The message text is: "PGE: Na dzień 8.07 zaplanowano odłączenie energii elektrycznej. Prosimy o uregulowanie należności 3.49.07. Dopuszczalne nr: https://ul.co.pl/platecno-pge-488.11e8". To the left of the message screenshot is a red triangular warning sign with a black exclamation mark. To the right of the message screenshot, the words "UWAGA" and "OSZUSTWO" are written in large, bold, red letters. The tweet is timestamped "12:27 PM · 8 Jul, 2021" and features the CSIRT KNF logo in the bottom right corner.

# 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 sposobie oszustwa możecie przeczytać w naszym artykule.](#)



The image is a screenshot of a tweet from CSIRT KNF (@CSIRT\_KNF) dated August 16, 2021. The tweet contains a warning about a scam on Facebook Marketplace. The scam involves a seller on Facebook Marketplace who, after a brief exchange of information, asks the buyer to send a payment link to a WhatsApp account. The tweet includes a screenshot of a Facebook Marketplace listing for a phone and a screenshot of a WhatsApp chat where the scammer asks for payment. The tweet also includes the CSIRT KNF logo and a Twitter logo.

**Uwaga!**

Oszuści okradający użytkowników OLX grasują od niedawna na Facebook Marketplace!

Udają zainteresowanie kupnem, po czym przenoszą konwersację na inny komunikator. Tam informują o dokonanej płatności i przesyłają link po "odbior" środków, aby wyłudzić dane do naszej karty.

**OSZUSTWO "NA KUPUJĄCEGO" NA PLATFORMIE:**

ze sprzedażą telefonu na platformie FACEBOOK MARKETPLACE kontaktuje się z nami oszust.

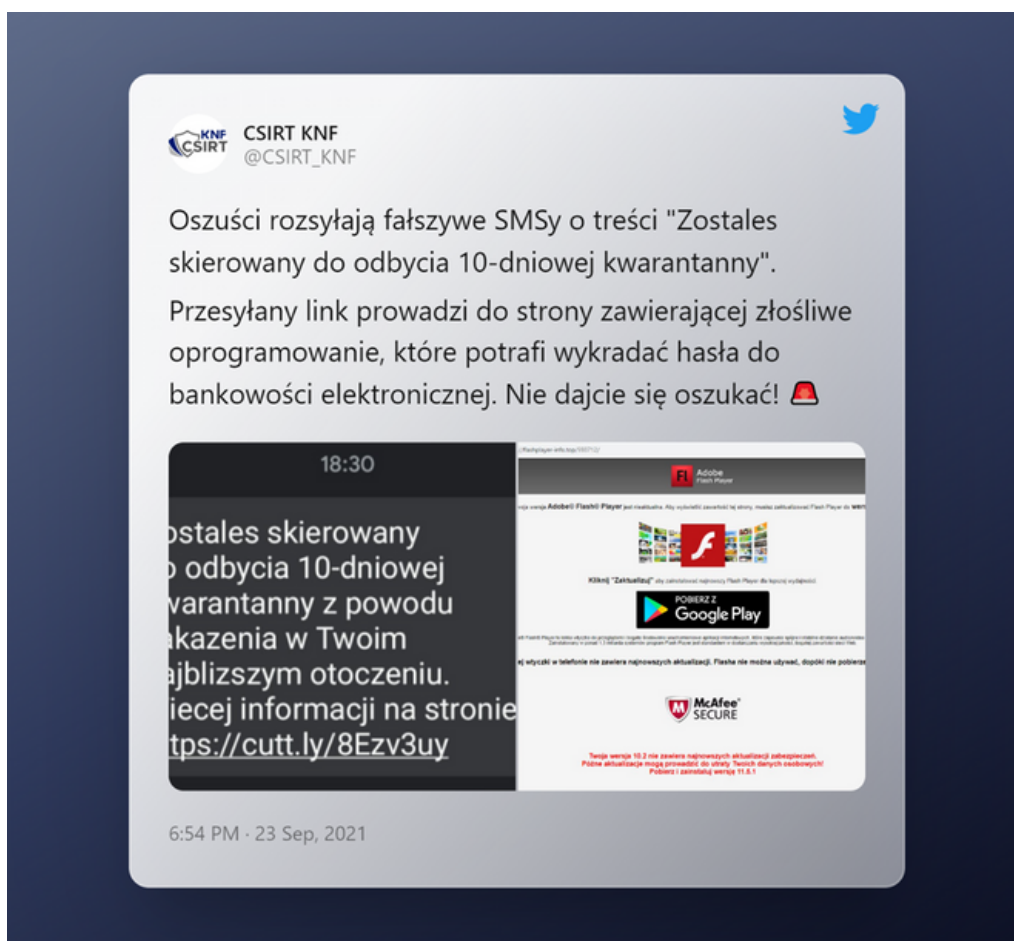
Po krótkiej wymianie informacji o przesyłce i sposobie realizacji otrzymujemy link gdzie "odbieramy" swoje

2:52 PM · 16 Aug, 2021

# 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.



The image shows a screenshot of a Twitter post from the account CSIRT KNF (@CSIRT\_KNF). The post contains a warning about a phishing attack. It includes a yellow warning icon and text in Polish. Below the text are two side-by-side screenshots of a web browser. The left screenshot shows the legitimate mBank.pl website with a login form. The right screenshot shows a phishing page with a URL bar displaying 'online.mbank.com/pl/Login'. The tweet is timestamped '12:01 PM · 29 Nov, 2021'.

**CSIRT KNF**  
@CSIRT\_KNF

**⚠ Uwaga!**

Ostrzegamy przed fałszywą stroną podszywającą się pod [@mBankpl](#).

Przestępcy wykorzystują do oszustwa specjalne kodowanie znaków "ą" zamiast "a", przez co fałszywa domena łudząco przypomina prawdziwą.

Bądźcie czujni!

12:01 PM · 29 Nov, 2021

# Grudzień

## DOPLATA DO PACZKI

Falszywe 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.



The image shows a screenshot of a Twitter post from the account CSIRT KNF (@CSIRT\_KNF). The post is in Polish and contains a warning about a phishing scam. The text of the tweet is as follows:

**Uwaga!**  
W związku z okresem przedświątecznym, przestępcy nasilają swoje ataki na portfele internautów.  
Oszuści wysyłają fałszywe SMS z prośbą o dopłacenie do paczki, podszywając się pod @PaczkomatyPL.  
Nie dajcie się oszukać!

The tweet includes four screenshots of the phishing scam:

- The first screenshot shows an SMS message from Inpost: "Inpost; Prosimy uregulowac nalezność;" with a link: <https://link.sv/inpost-d0s65z>.
- The second screenshot shows a webpage with a form for payment, with a yellow button labeled "Przejdź do płatności".
- The third screenshot shows a webpage with a form for payment, with a yellow button labeled "Przejdź do płatności".
- The fourth screenshot shows a payment gateway interface with various payment methods like Visa, Mastercard, and others.

The tweet is timestamped "9:24 AM · 1 Dec, 2021".

# 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

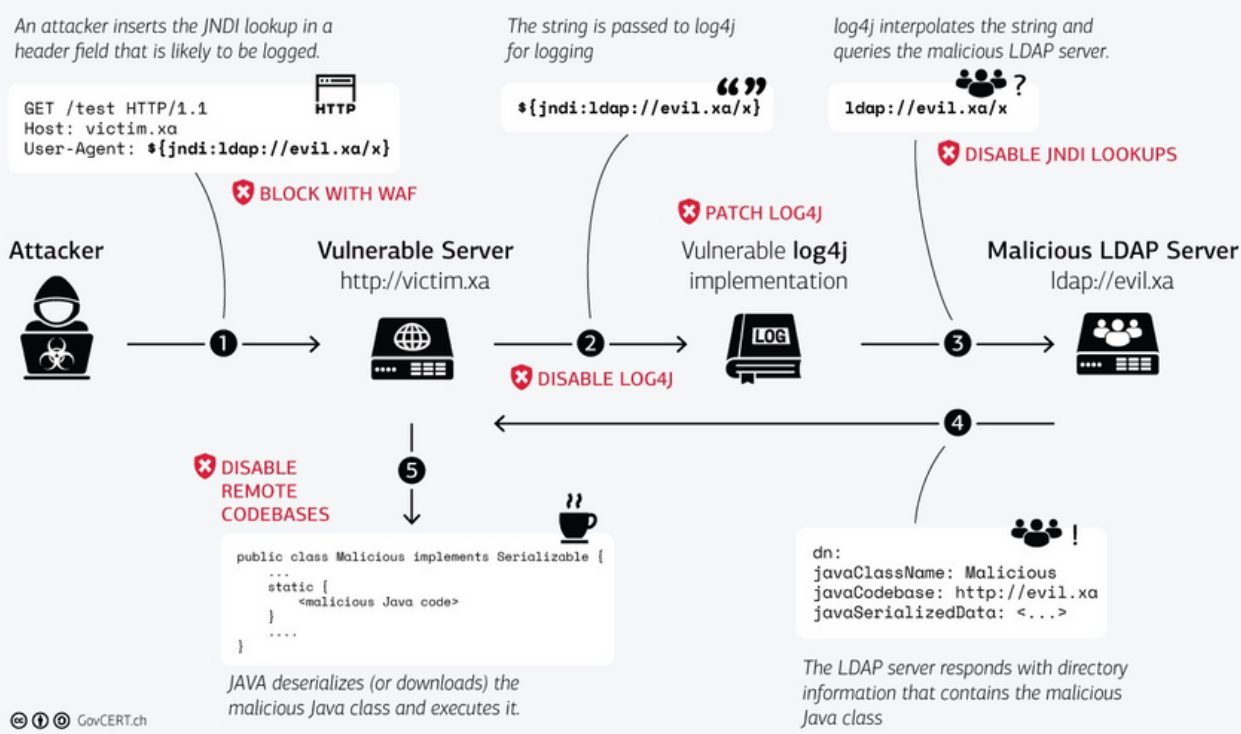
# Zagrożenia globalne

## 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.

### The log4j JNDI Attack

and how to prevent it



ŹRÓDŁO: GOVCERT.CH