Zagrożenia dla rynku cyberbezpieczeństwa rynku finansowego w okresie 01.08-31.08.2022

Ataki DDoS na podmioty z rynku finansowego w Sierpniu

W sierpniu zarejestrowaliśmy **15** istotnych ataków DDoS na podmioty z rynku finansowego.

Charakterystyka ataków:

- 10 ataków aplikacyjnych i 13 wolumetrycznych – coraz częściej zdarzają się jednoczesne ataki wolumetryczno-aplikacyjne – 5 istotnych przypadków w sierpniu.
- Największy atak wolumetryczny w tym Sierpniu dochodził do **141 Gbps.**
- W źródłach ataku są adresy IP TOR Node, IoT, Mikrotik, usługi chmurowe.

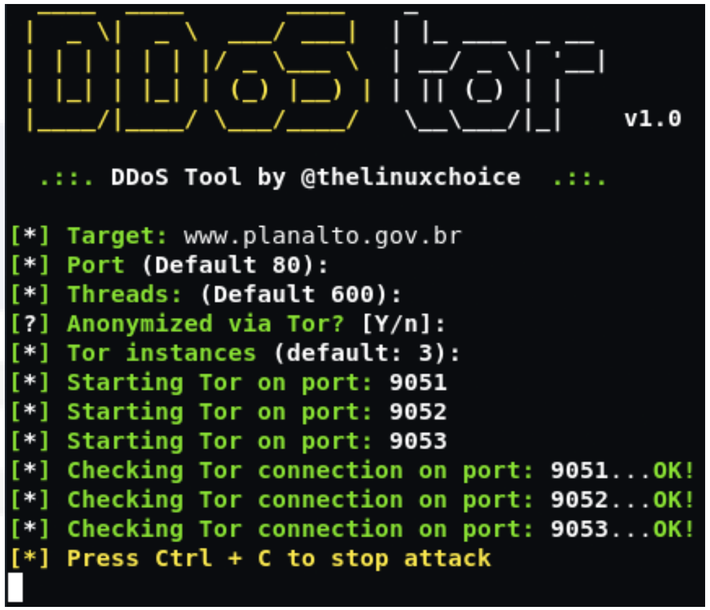
Ataki DDoS na podmioty z rynku finansowego w Sierpniu

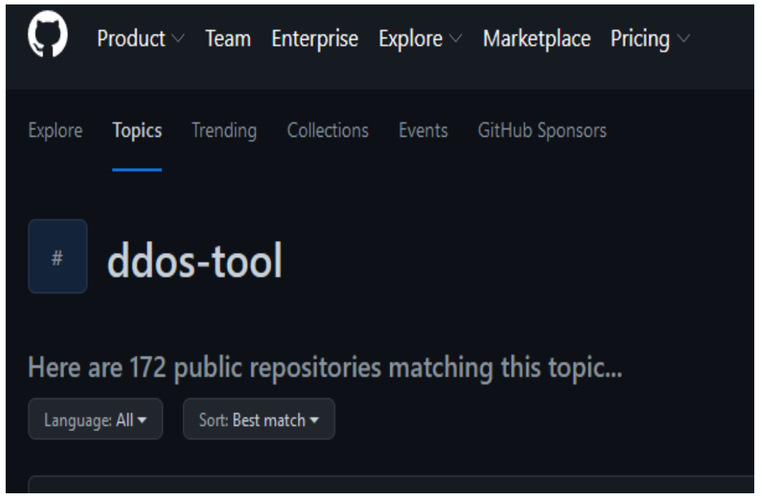
Część ataków realizowana była z wykorzystaniem technik amplifikacji – NTP; DNS; TCP/SYN ACK

W sierpniu łączny czas ataków wynosił – 630 minut

Cel ataków:

- Strony główne banków,
- bankowość mobilna,
- serwisy informacyjne,
- usługi DNS,
- usługi 3DSecure.





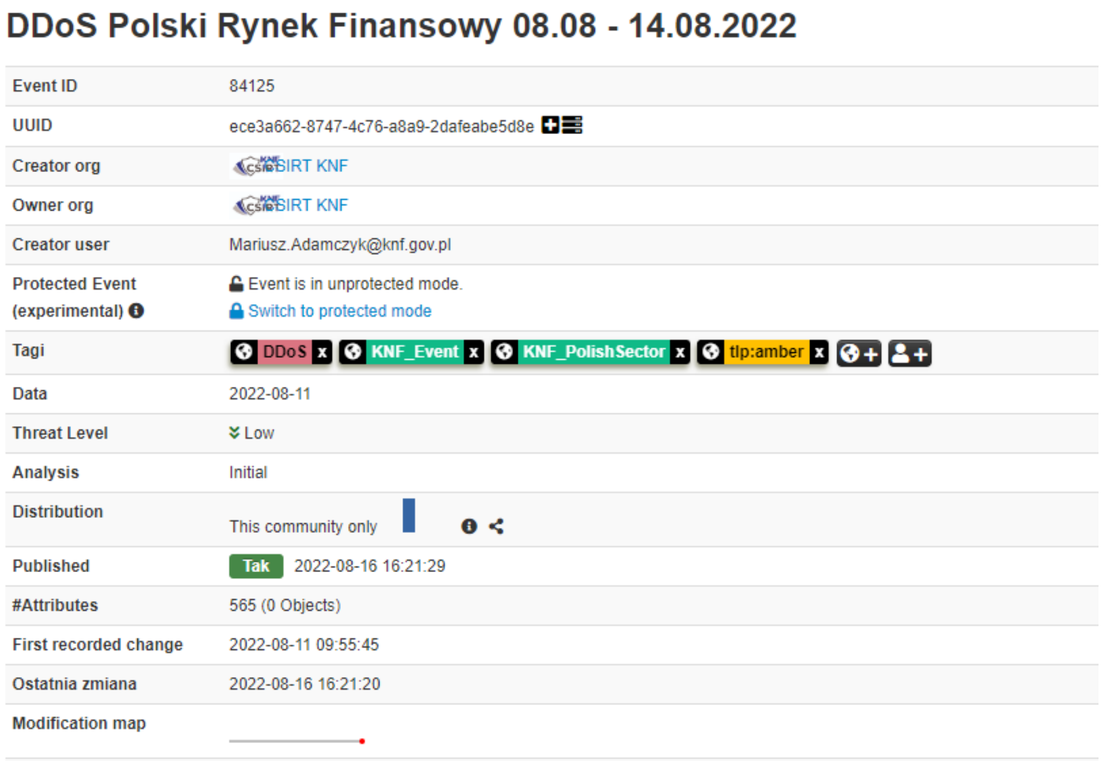
Ataki DDoS na podmioty z rynku finansowego w Sierpniu

TOP krajów atakujących na podstawie adresów IP:

- Rosja,
- USA,
- Indonezja,
- Tajlandia,
- Wietnam,
- Polska.

Więcej informacji o źródłach ataków można znaleźć w MISP

- https://mispouk.knf.gov.pl/events/view/84125
- https://misp.knf.gov.pl/events/view/83577



DDoS Polski Rynek Finansowy 08.08 - 14.08.2022

Event ID	84125
UUID	ece3a662-8747-4c76-a8a9-2dafeabe5d8e
Creator org	CSIRT KNF
Owner org	CSIRT KNF
Creator user	Mariusz.Adamczyk@knf.gov.pl
Protected Event (experimental)	Event is in unprotected mode. Switch to protected mode
Tagi	DDoS x KNF_Event x KNF_PolishSector x tlp:amber x
Data	2022-08-11
Threat Level	Low
Analysis	Initial
Distribution	This community only
Published	Tak 2022-08-16 16:21:29
#Attributes	565 (0 Objects)
First recorded change	2022-08-11 09:55:45
Ostatnia zmiana	2022-08-16 16:21:20
Modification map	

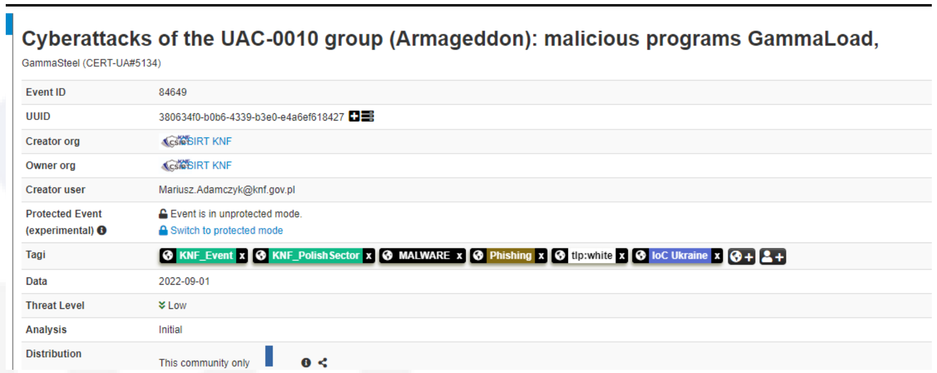
Armagedon APT

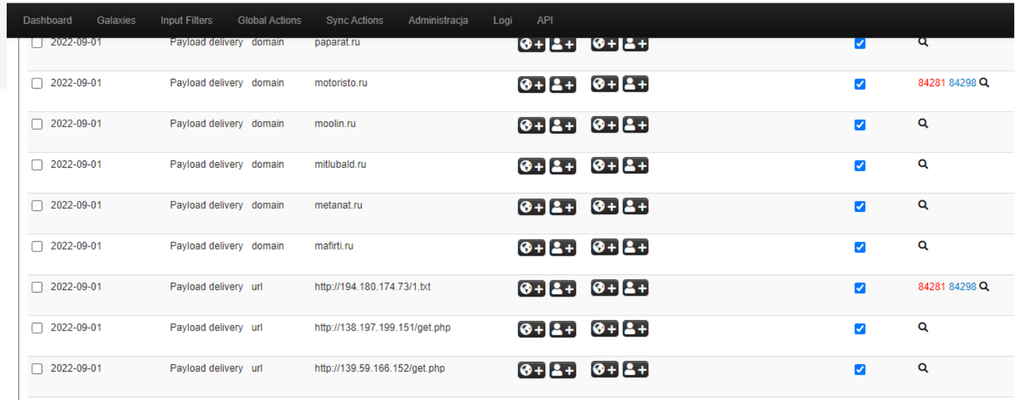
- Pierwsze wzmianki już w 2013/14 roku.
- Główny kierunek Ukraina.
- Phishing i spear phishing.
- Obsada powiązana ze służbami FSB.
- odpowiadają za GammLoad/GammaSteel i Shuckworm.

Armagedon APT

GammaLoad i GammaSteel Malware
https://mispouk.knf.gov.pl/events/view/84649
380634f0-b0b6-4339-b3e0-e4a6ef618427

Shuckworm
https://mispouk.knf.gov.pl/events/view/84281/1/84649
cb29af2f-6e7e-423e-baeb-2721eb4b6f52





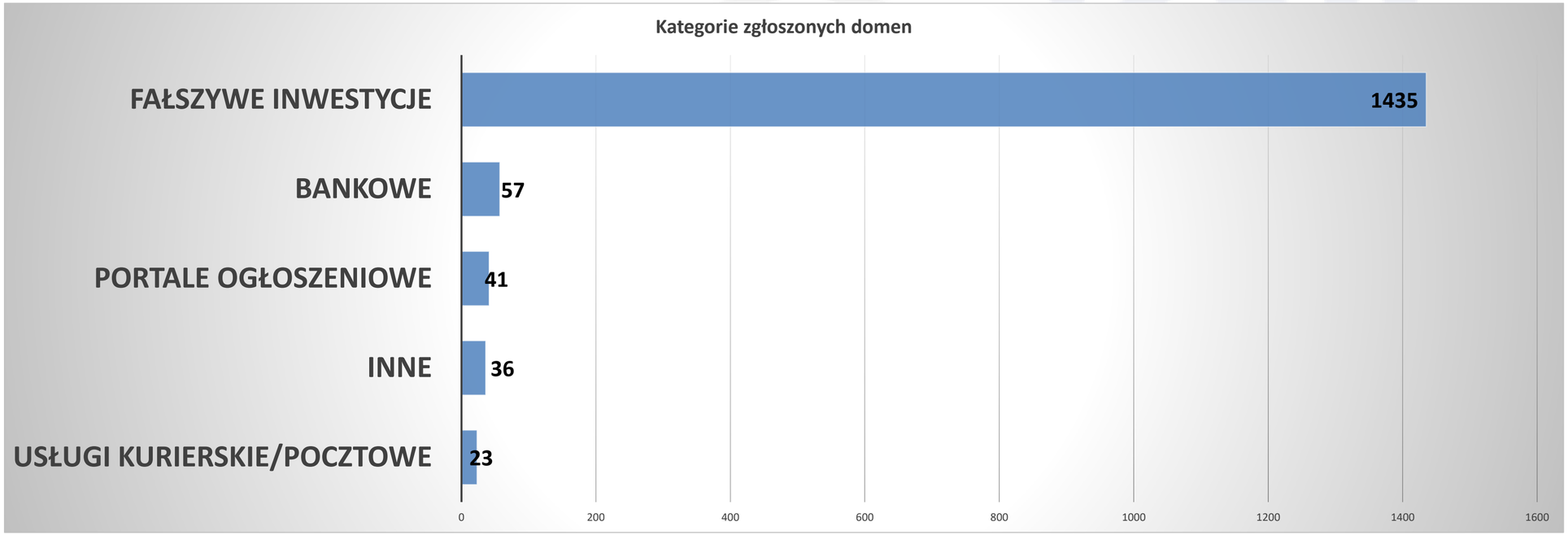
Przypominamy o zgłaszaniu ataków DDoS

W zgłoszeniu prosimy o uwzględnienie

- Czas ataku
- Skutki ataku
- Adresację biorąca udział w ataku
- Raporty z systemów AntyDDoS (np. Arbor)
- Wolumeny i metody ataku
- Na łączu jakiego operatora dochodziło do ataku

Ataki Phishingowe na klientów rynku finansowego

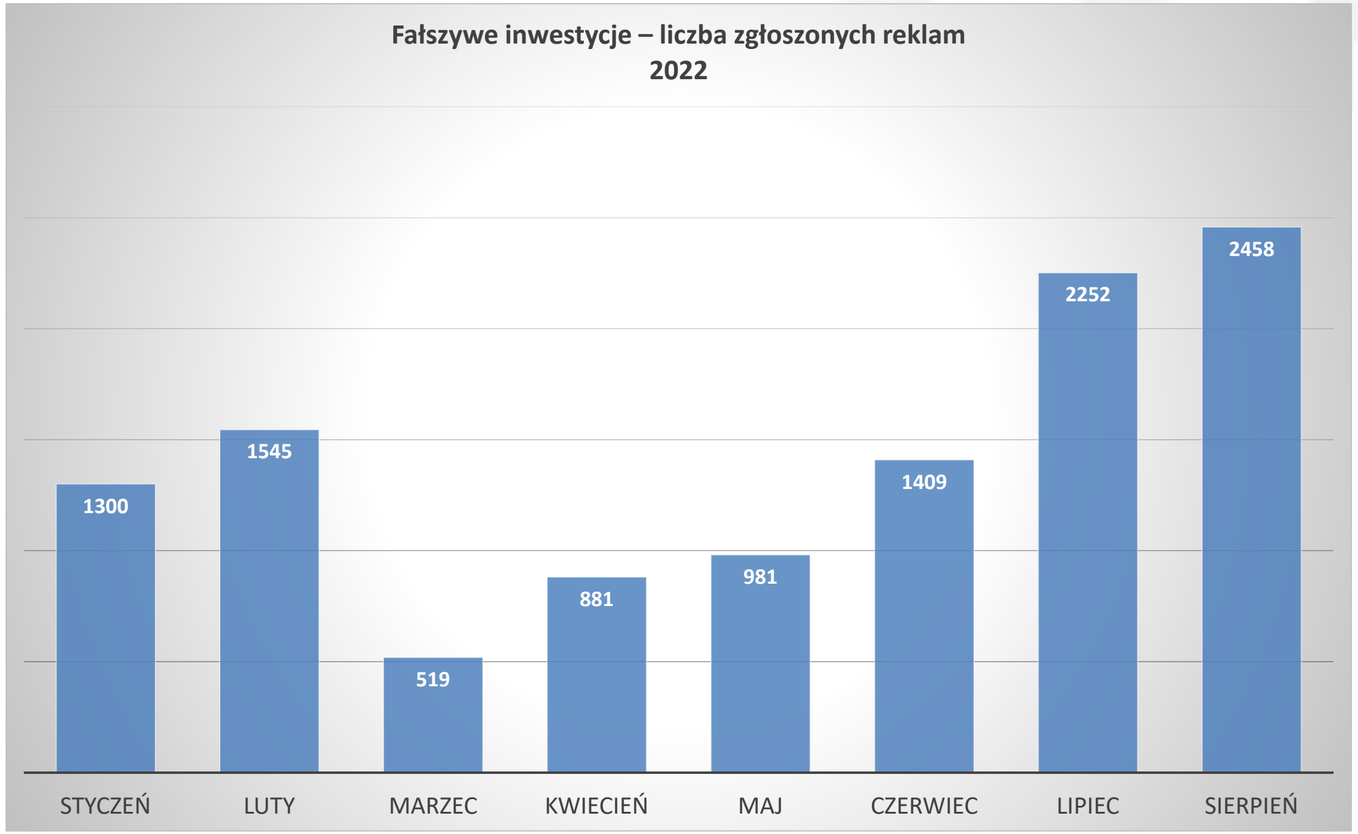
W sierpniu CSIRT KNF zgłosił do zablokowania 1593 domeny (1852 w lipcu).

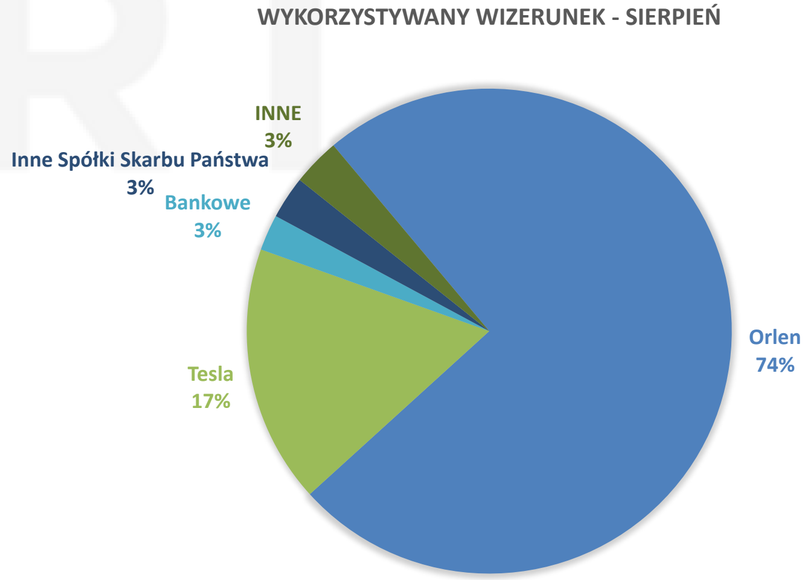


CERT Polska dodał na listę ostrzeżeń 4823 domeny (4395 w lipcu). Obecnie na liście znajduje się 69549 domen.

Ataki Phishingowe na klientów bankowości elektronicznej

Fałszywe reklamy na platformie Facebook

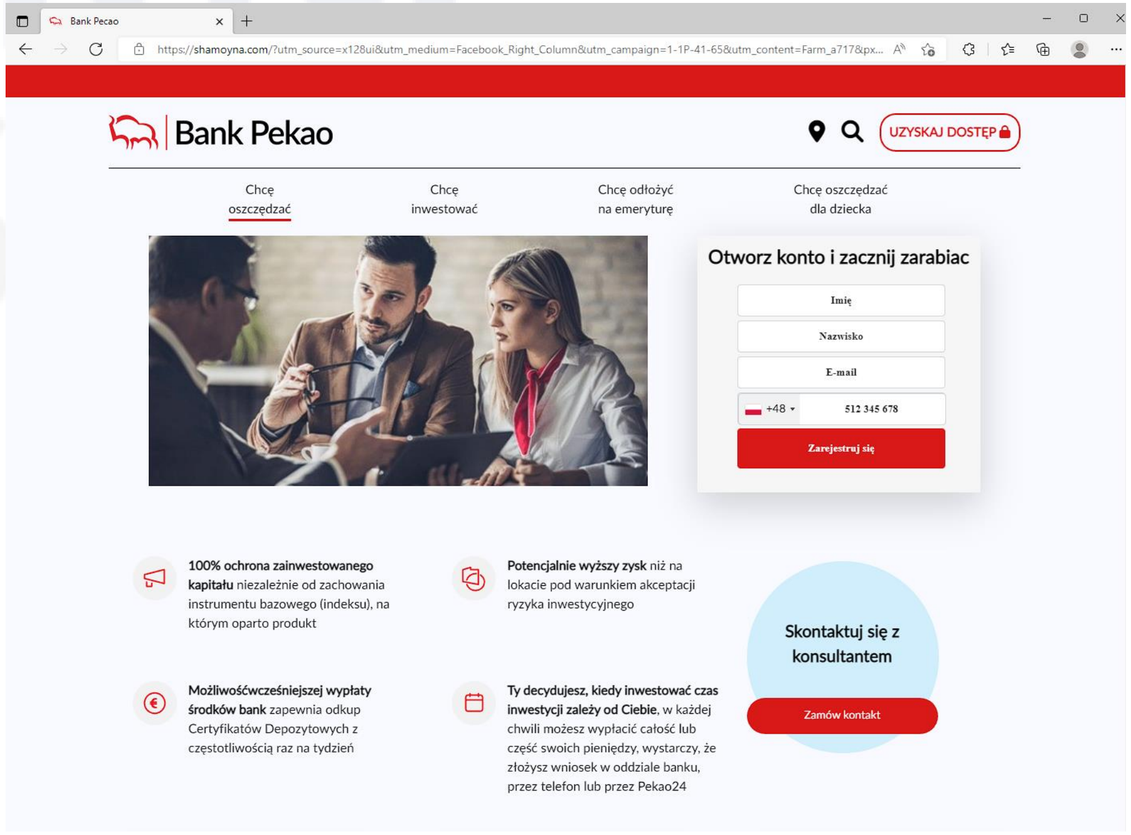




Ataki Phishingowe na klientów bankowości elektronicznej

Fałszywe reklamy na platformie Facebook.

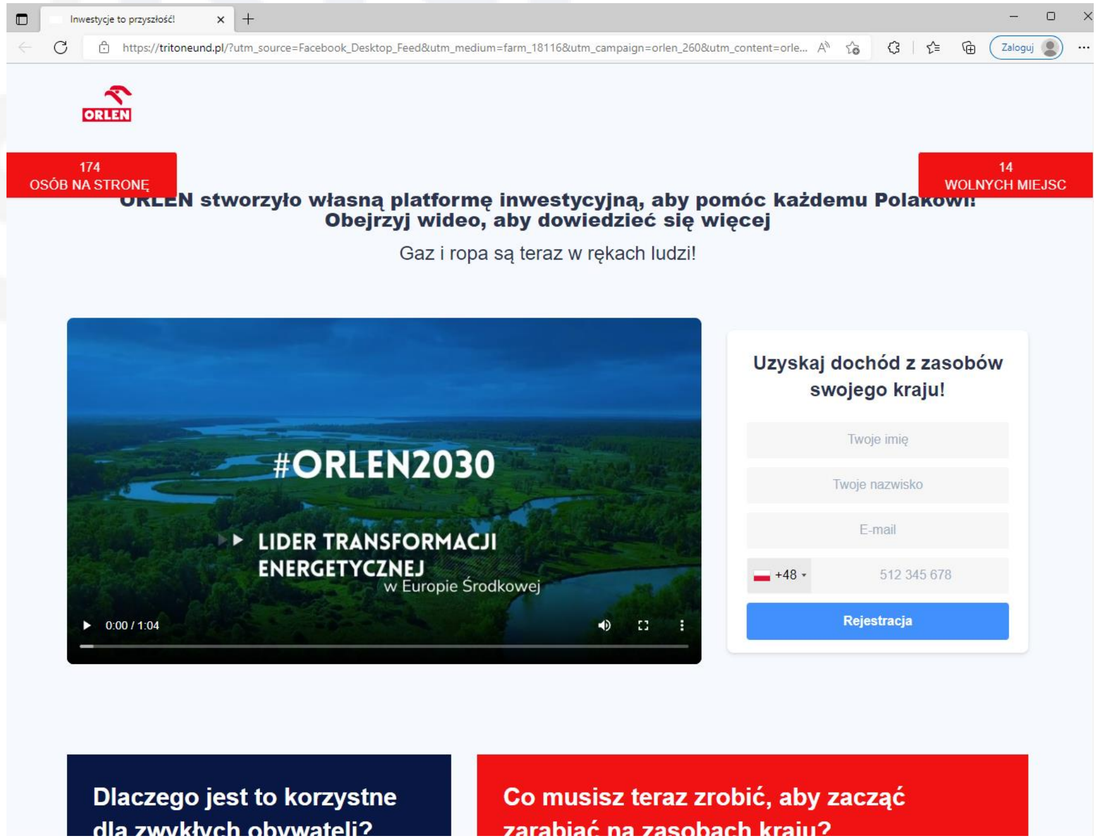
- Podszycie m.in. pod PEKAO – fałszywe inwestycje.



Ataki Phishingowe na klientów bankowości elektronicznej

Fałszywe reklamy na platformie Facebook.

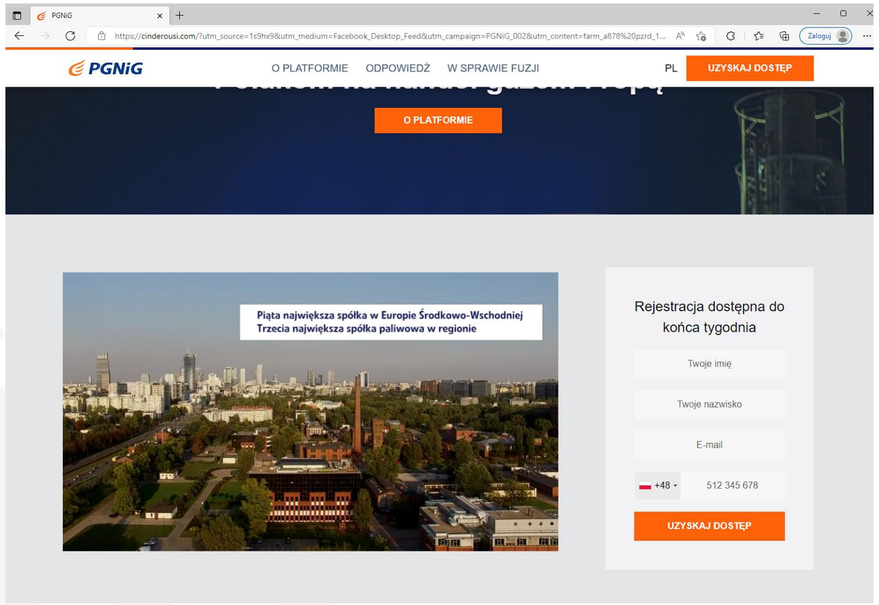
- Podszycia pod ORLEN



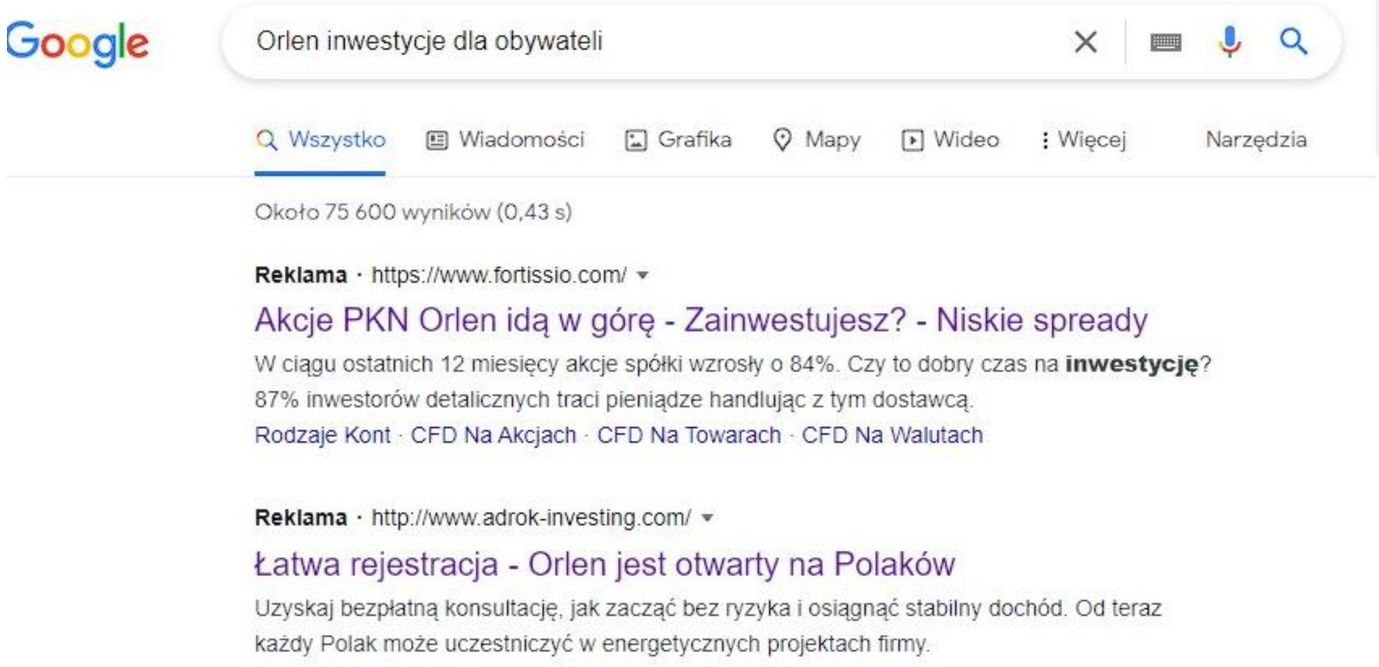
Ataki Phishingowe na klientów bankowości elektronicznej

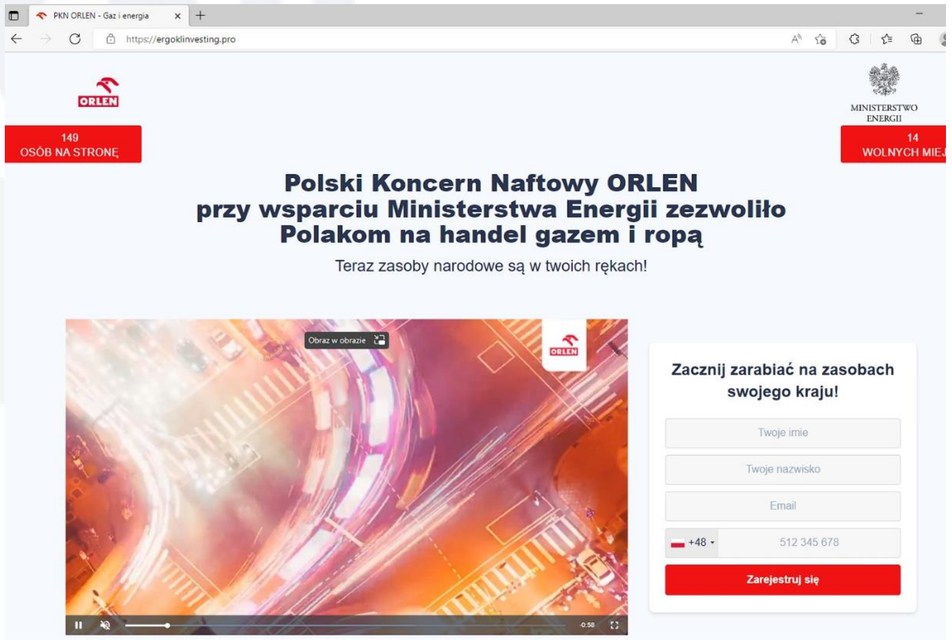
Fałszywe reklamy na platformie Facebook.

- Podszycia pod inne Spółki Skarbu Państwa

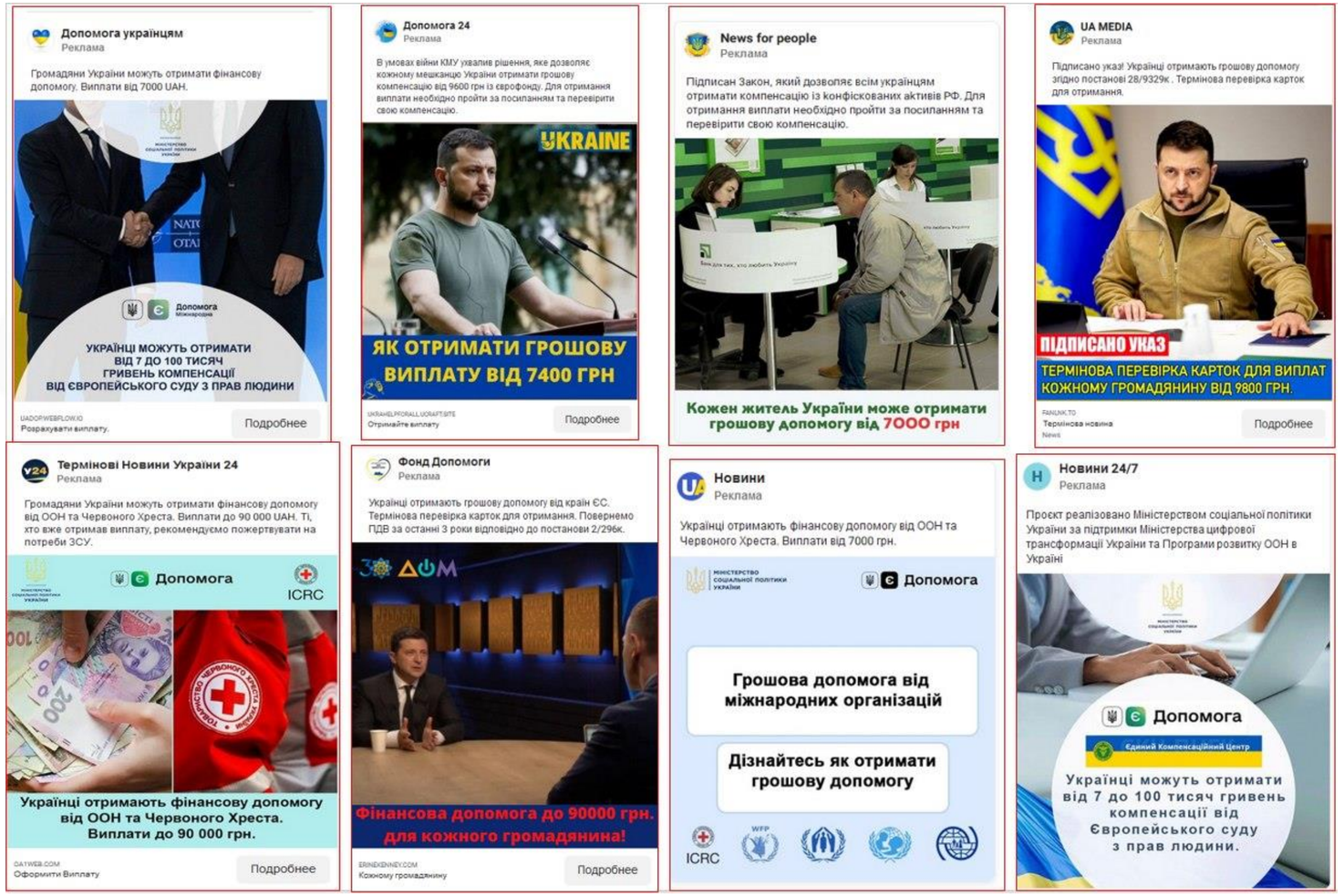


Ataki Phishingowe na klientów bankowości elektronicznej





Fałszywe reklamy inwestycyjne w serwisie Facebook – ukierunkowane na obywateli Ukrainy



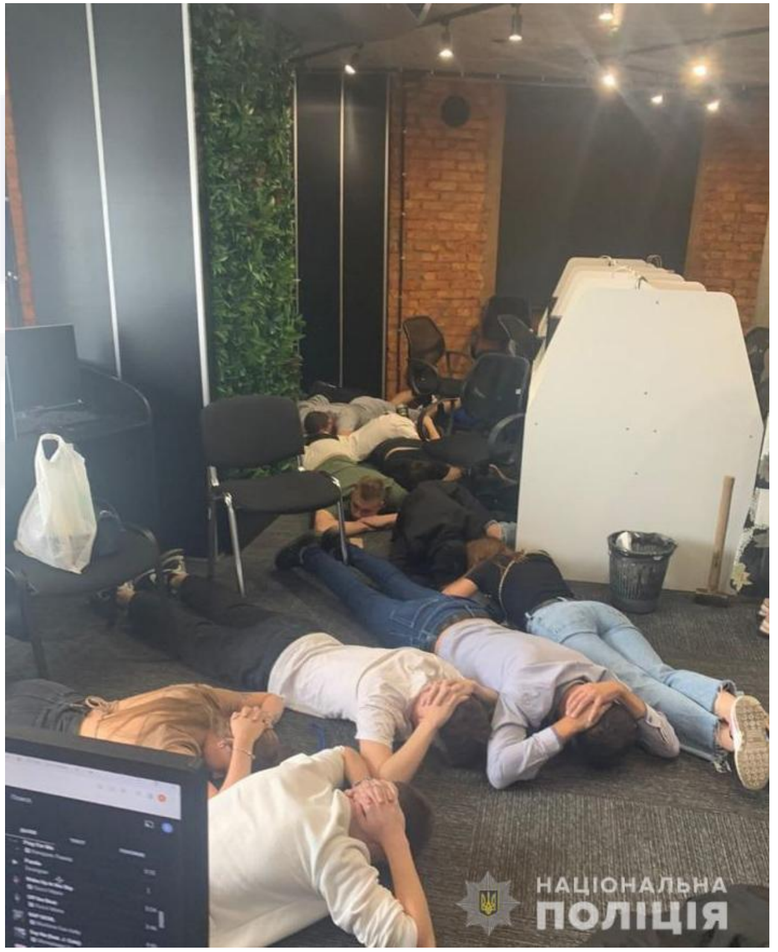
Zatrzymanie grupy przestępczej na Ukrainie

Ukraińska policja najechała call center podszywające się pod banki. Wrabiali ofiary na inwestycje w kryptowaluty, akcje, ropę, ...

31 SIERPNIA 2022, 13:08 | W BIEGU | KOMENTARZY 10

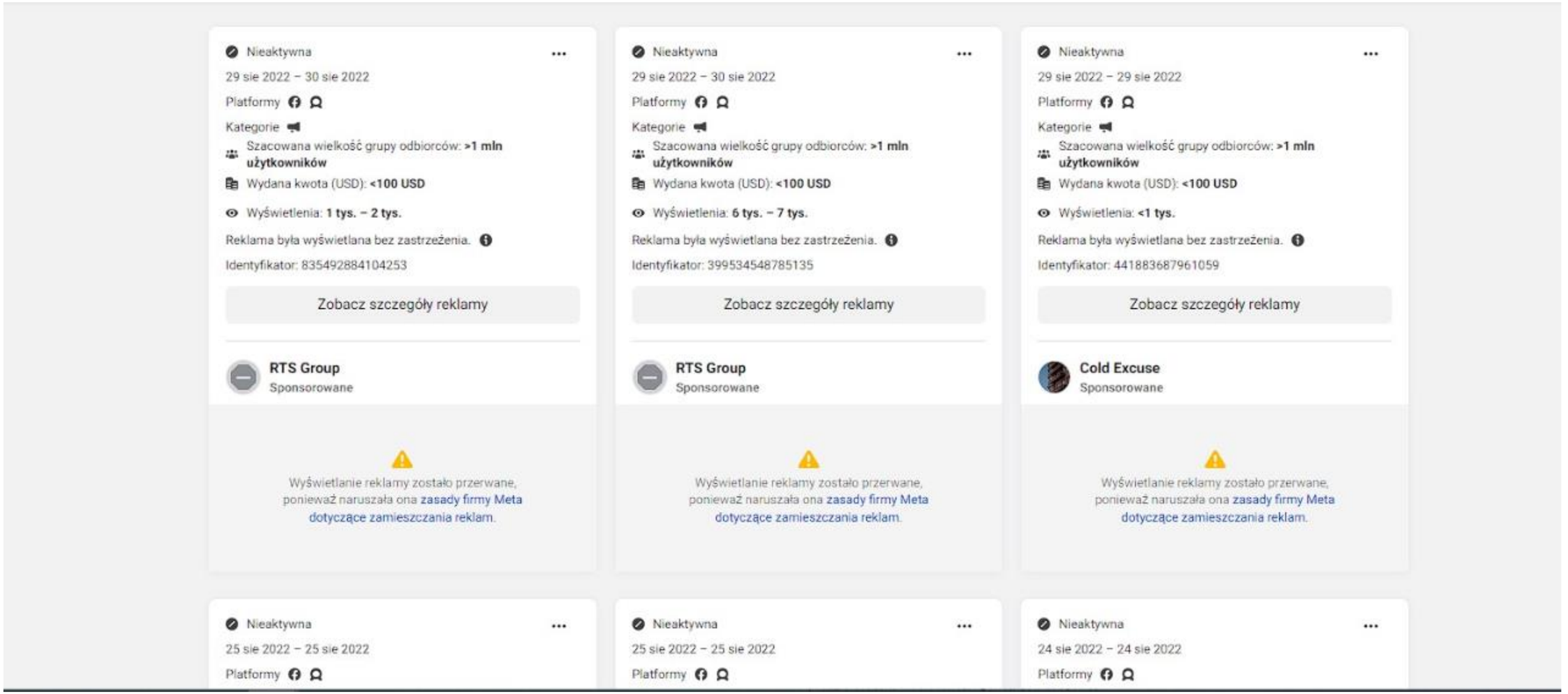
TAGI: AWARENESS, BANKI, SCAM, SPOOFING

Opis całej operacji policji możecie znaleźć tutaj (ciekawe jaką rolę pełni(ł) oznaczony przez nas strzałką rekwizyt):



Źródło: https://sekurak.pl/ukrainska-policja-najechala-call-center-podszywajace-sie-pod-banki-wrabiali-ofiary-na-inwestycje-w-kryptowaluty-akcje-rope/

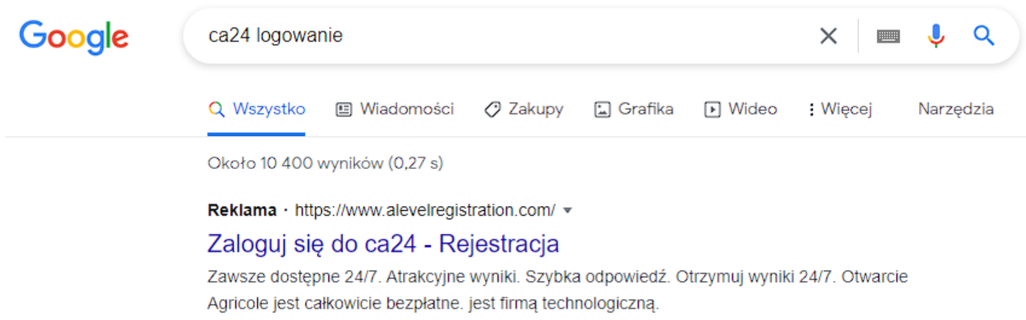
Ataki Phishingowe na klientów rynku finansowego (Facebook)

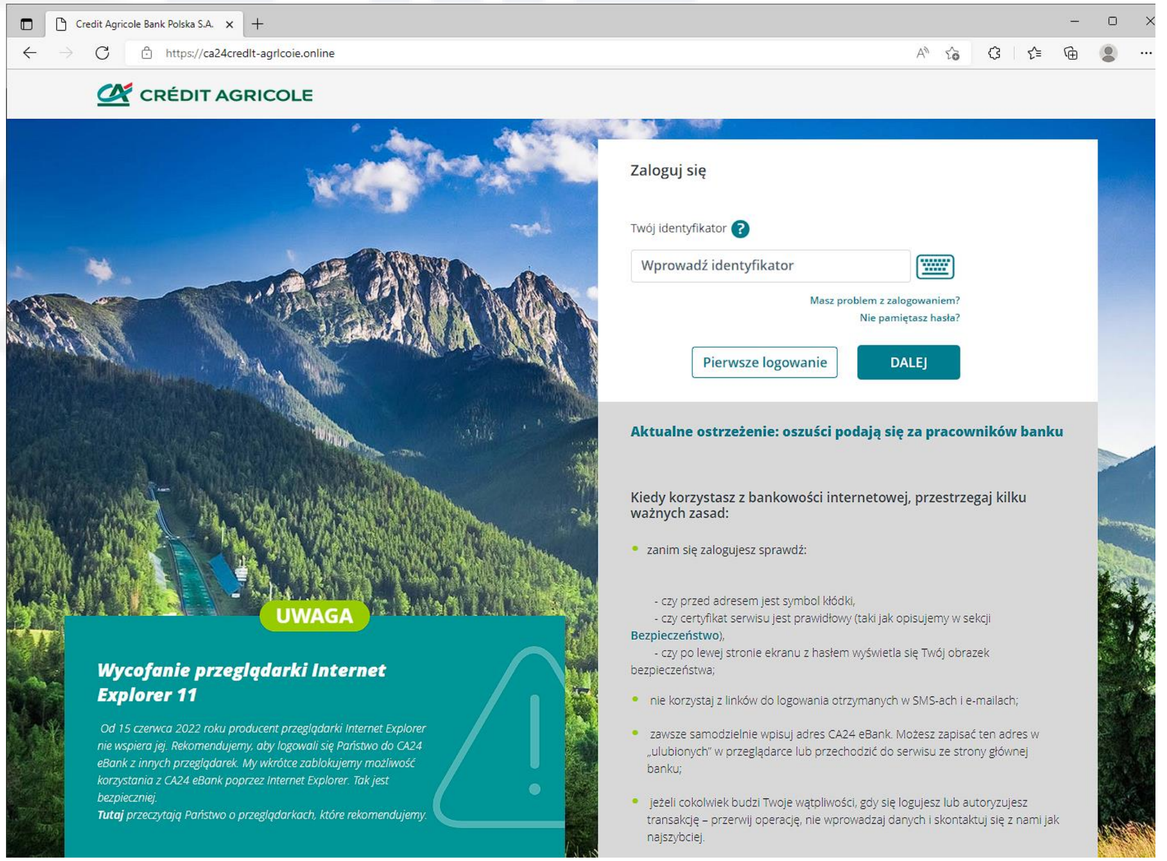


Ataki Phishingowe na klientów rynku finansowego

Fałszywe reklamy na platformie Google.

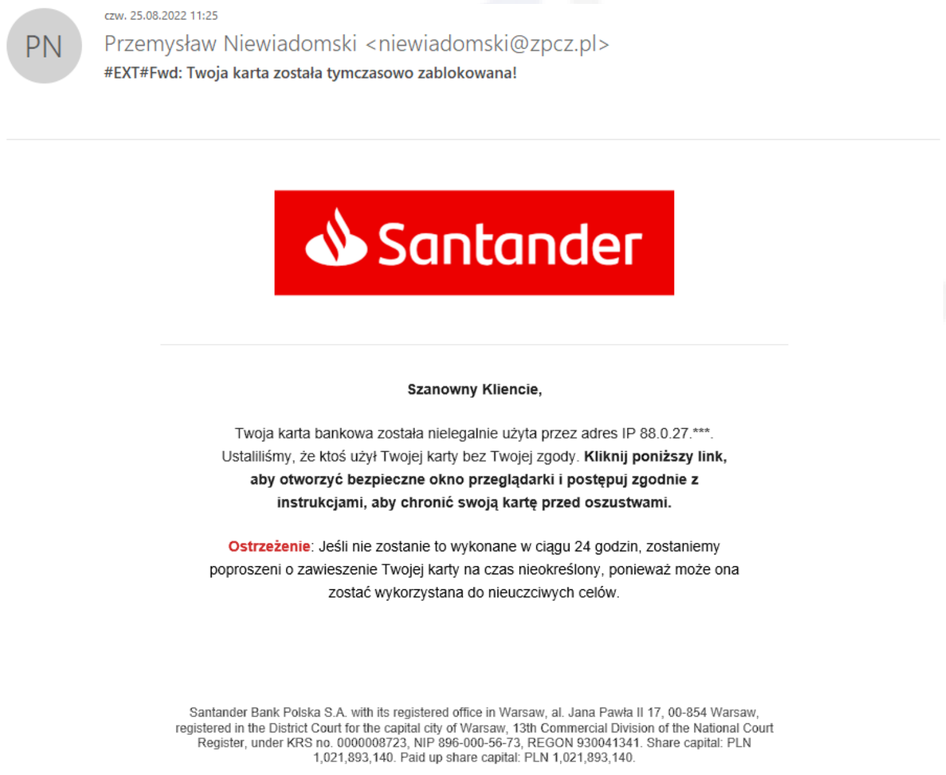
- Podszycie pod Credit Agricole.





Ataki Phishingowe na klientów rynku finansowego

Fałszywe maile poszywające się pod BANKI – „Twoja karta została tymaczasowo zablokowana”:



PN

czw. 25.08.2022 11:25

Przemysław Niewiadomski <niewiadomski@zpcz.pl>

#EXT#Fwd: Twoja karta została tymczasowo zablokowana!

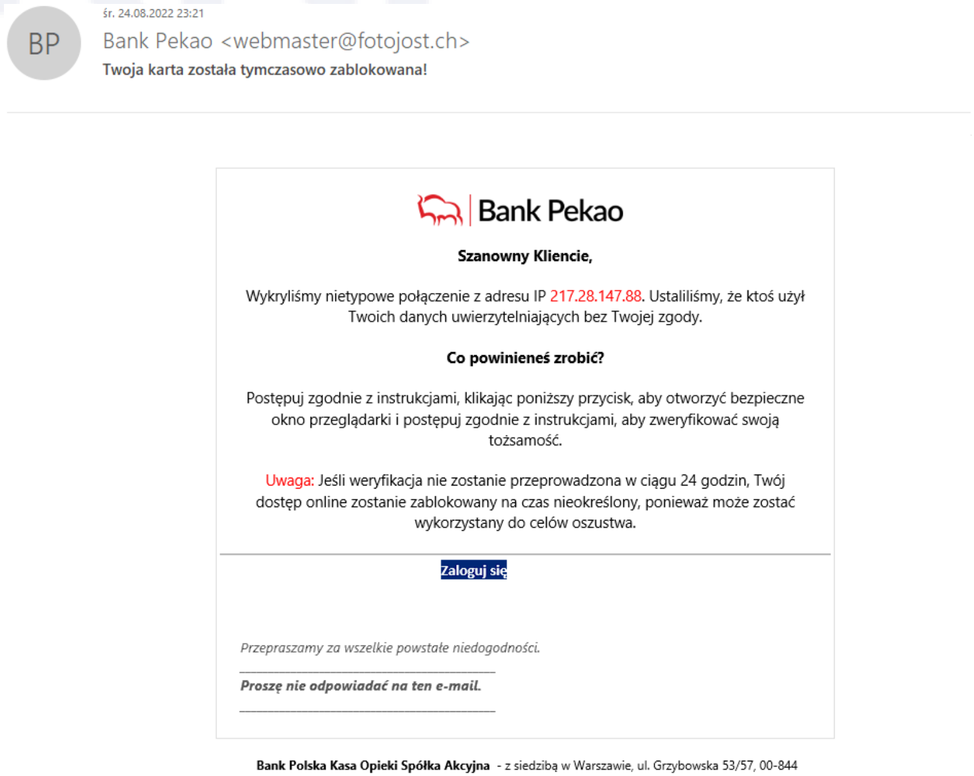
Santander

Szanowny Kliencie,

Twoja karta bankowa została nielegalnie użyta przez adres IP 88.0.27.***. Ustaliliśmy, że ktoś użył Twojej karty bez Twojej zgody. **Kliknij poniższy link, aby otworzyć bezpieczne okno przeglądarki i postępuj zgodnie z instrukcjami, aby chronić swoją kartę przed oszustwami.**

Ostrzeżenie: Jeśli nie zostanie to wykonane w ciągu 24 godzin, zostaniemy poproszeni o zawieszenie Twojej karty na czas nieokreślony, ponieważ może ona zostać wykorzystana do nieuczciwych celów.

Santander Bank Polska S.A. with its registered office in Warsaw, al. Jana Pawła II 17, 00-854 Warsaw, registered in the District Court for the capital city of Warsaw, 13th Commercial Division of the National Court Register, under KRS no. 0000008723, NIP 896-000-56-73, REGON 930041341. Share capital: PLN 1,021,893,140. Paid up share capital: PLN 1,021,893,140.



BP

śr. 24.08.2022 23:21

Bank Pekao <webmaster@fotojost.ch>

Twoja karta została tymczasowo zablokowana!

Bank Pekao

Szanowny Kliencie,

Wykryliśmy nietypowe połączenie z adresu IP 217.28.147.88. Ustaliliśmy, że ktoś użył Twoich danych uwierzytelniających bez Twojej zgody.

Co powinieneś zrobić?

Postępuj zgodnie z instrukcjami, klikając poniższy przycisk, aby otworzyć bezpieczne okno przeglądarki i postępuj zgodnie z instrukcjami, aby zweryfikować swoją tożsamość.

Uwaga: Jeśli weryfikacja nie zostanie przeprowadzona w ciągu 24 godzin, Twój dostęp online zostanie zablokowany na czas nieokreślony, ponieważ może zostać wykorzystany do celów oszustwa.

Zaloguj się

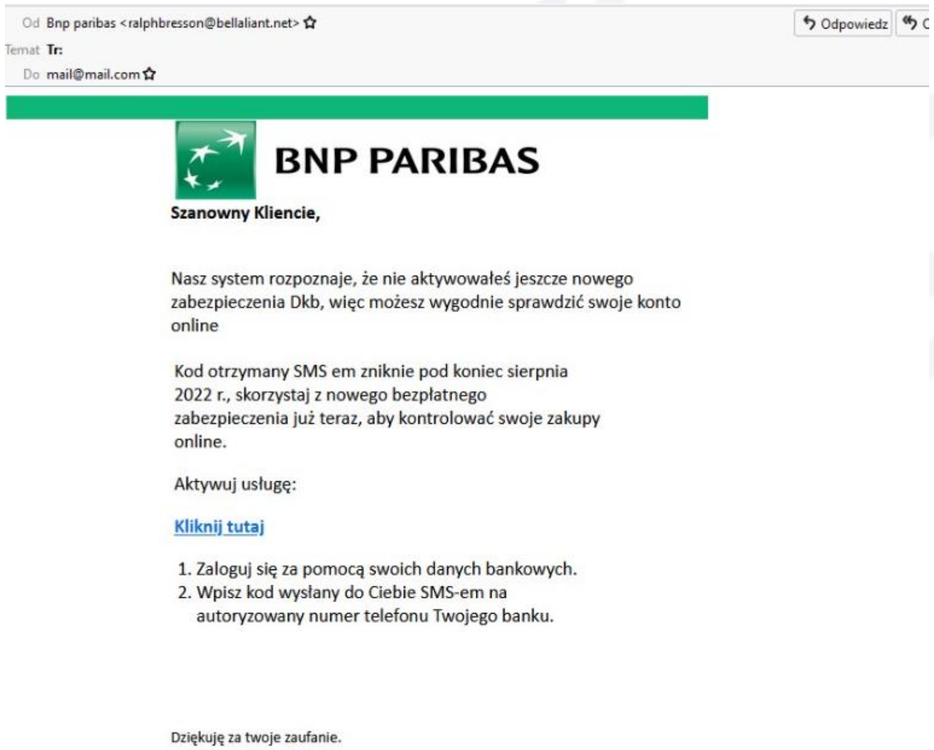
Przepraszamy za wszelkie powstałe niedogodności.

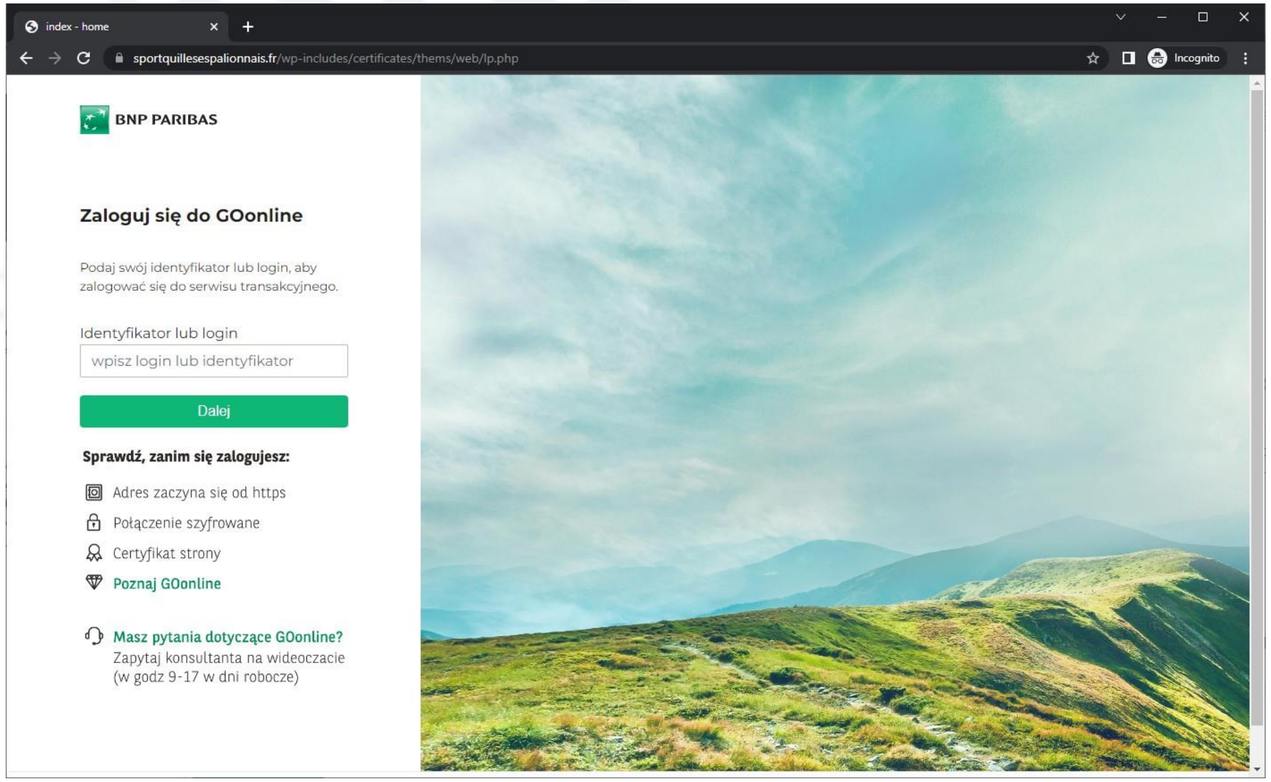
Proszę nie odpowiadać na ten e-mail.

Bank Polska Kasa Opieki Spółka Akcyjna - z siedzibą w Warszawie, ul. Grzybowska 53/57, 00-844

Ataki Phishingowe na klientów rynku finansowego

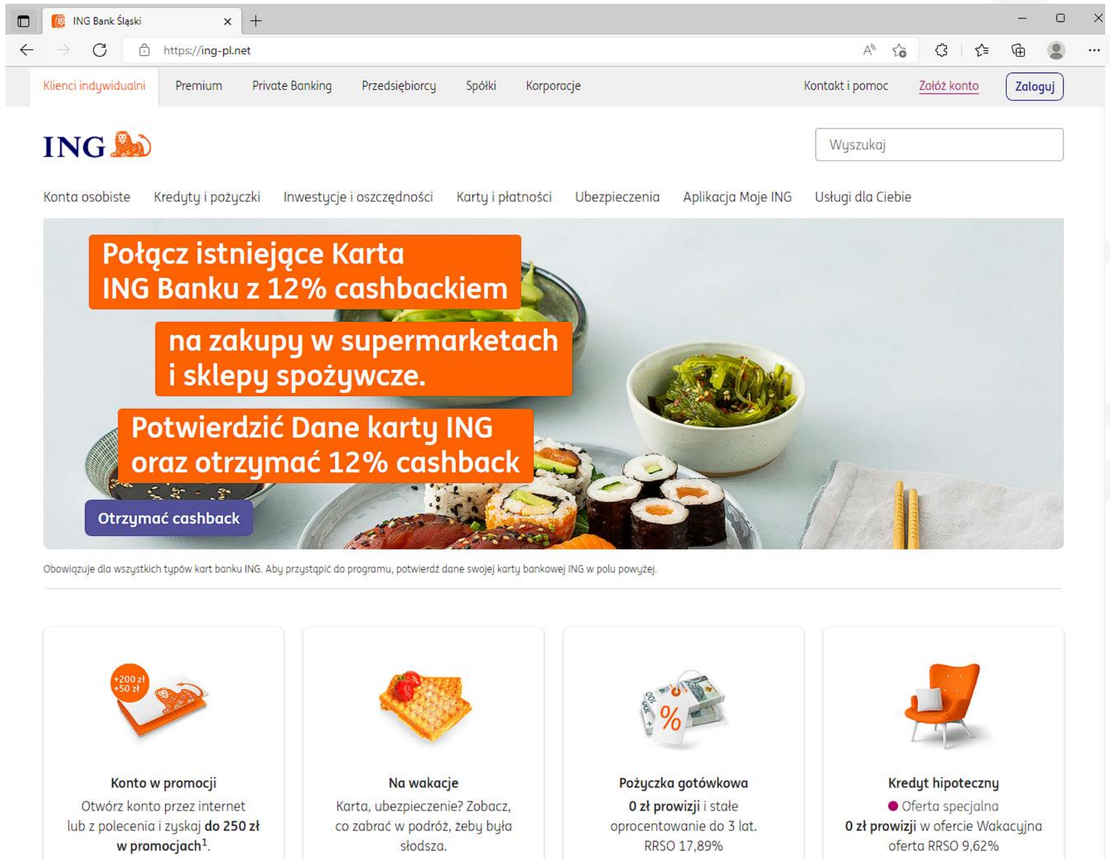
Fałszywe maile poszywające się pod Bank BNP Paribas – „Aktywacja konta”:

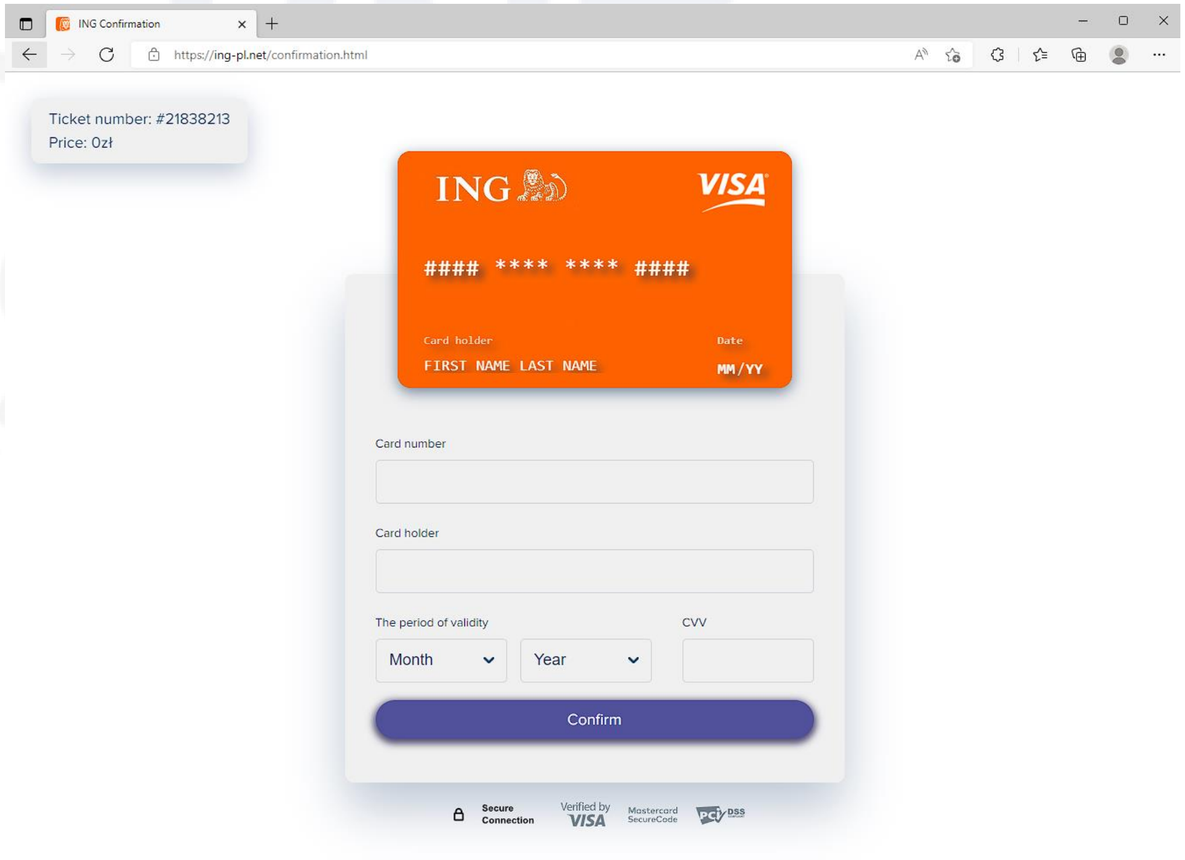




Ataki Phishingowe na klientów rynku finansowego

Podszycie pod Bank ING – „Cashback”.

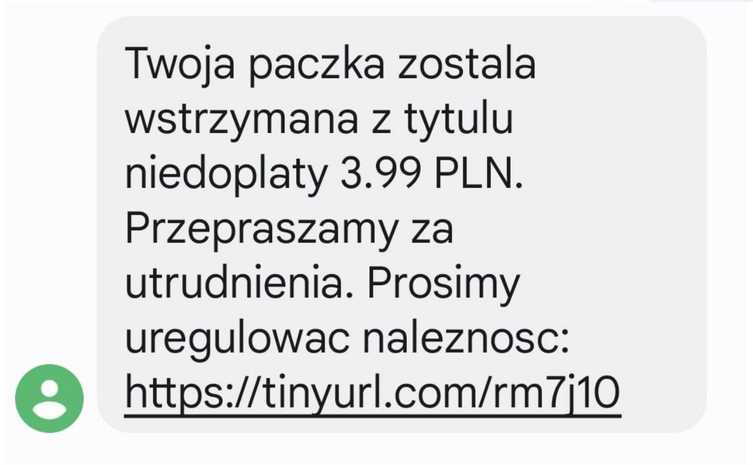


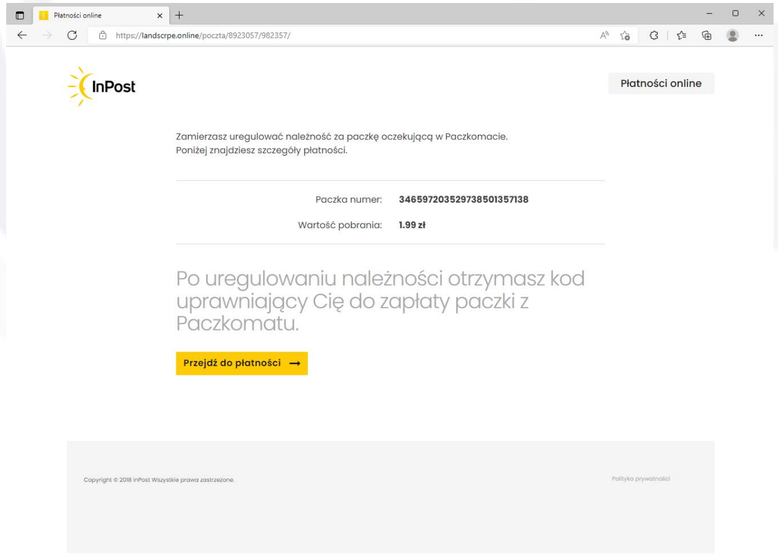


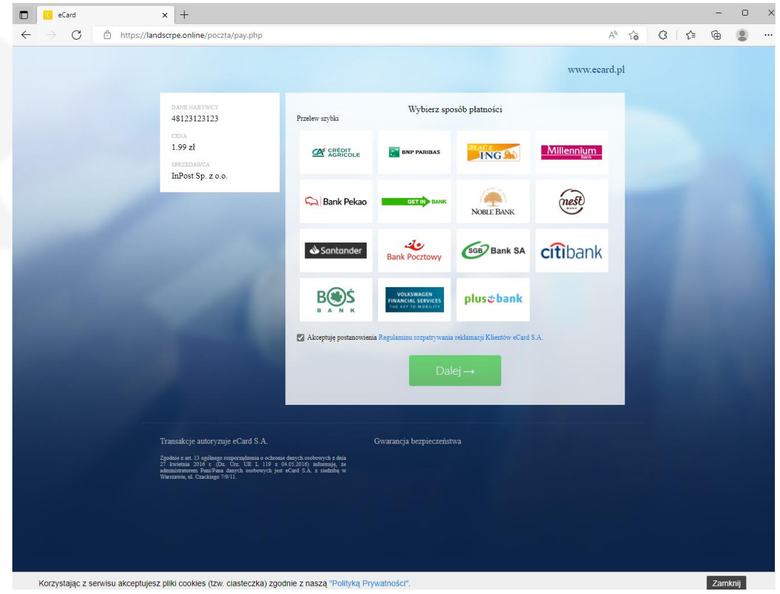
Ataki Phishingowe na klientów rynku finansowego

Inne

- Phishing Inpost







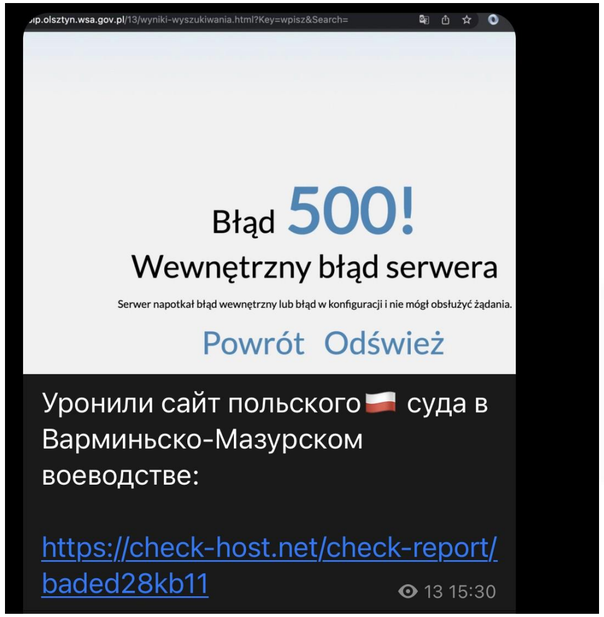
CTI – informacje o działalności grup przestępczych i haktywistów

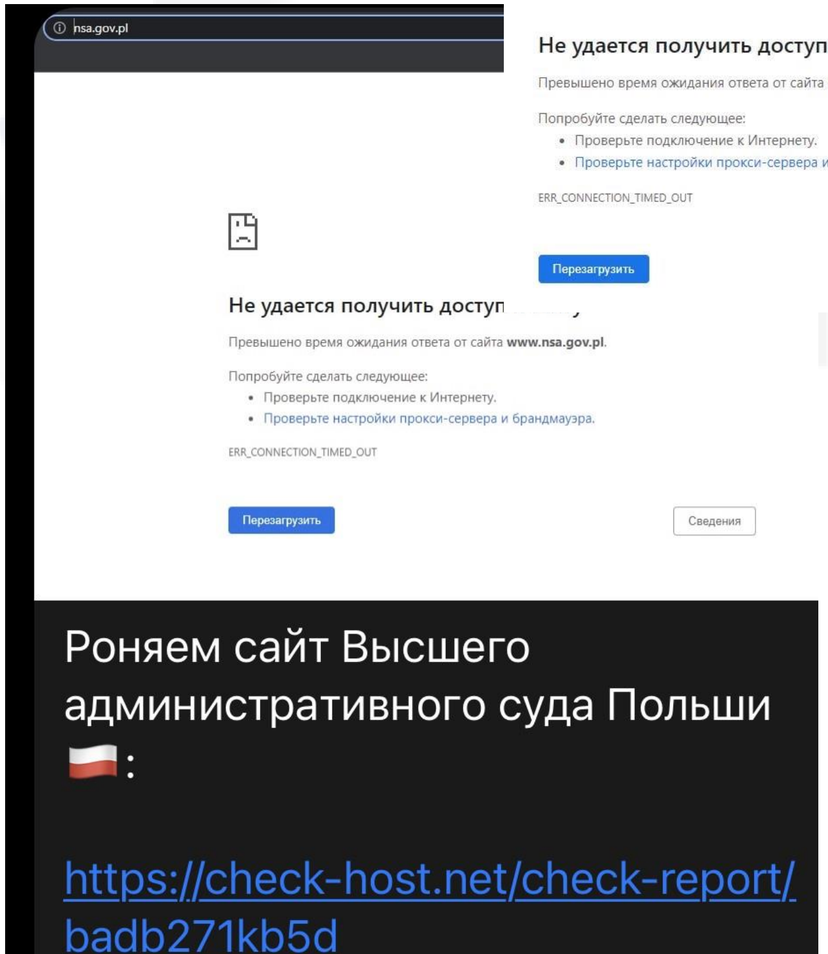
Ataki grup haktywistycznych w dalszym ciągu są bieżącym zagrożeniem dla sektora finansowego oraz infrastruktury krytycznej.

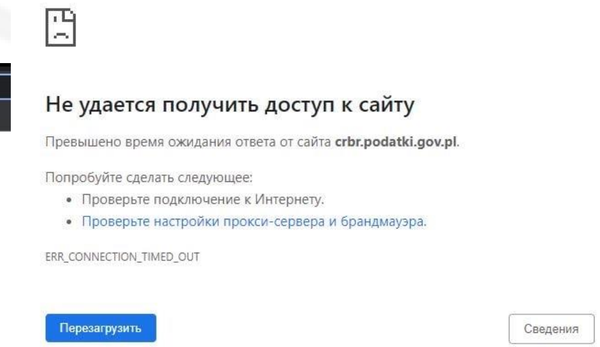
Sierpień – ataki w Polsce:

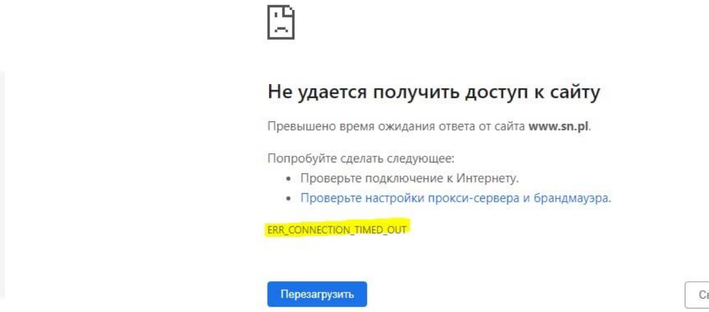
- Plb.pl,
- Bumar.Gliwice.pl,
- Poznanairport.pl,
- Airport.gdansk.pl,
- Gkpge.pl,
- Imim.pl,
- Elpak.com.pl,
- Lotnisko-chopina.pl,
- Wabrzezno.sr.gov.pl,
- Limanowa.sr.gov.pl,
- Slupsk.sr.gov.pl,
- Jawor.sr.gov.pl,
- Ilawa.sr.gov.pl,
- Gdansk-południe.sr.gov.pl,
- Elk.sr.gov.pl,
- slupsk.so.gov.pl,
- Trzcianka.sr.gov.pl,
- Polandhub.pl,
- Hrubieszow.sr.gov.pl,
- Lebork.sr.gov.pl,
- Zabrze.sr.gov.pl,
- Debica.sr.gov.pl,
- Mbank.pl,
- Otomoto.pl,
- Nsa.gov.pl,
- Lodz.wsa.gov.pl,
- Wbj.pl,
- Skycms.pl,
- Sn.pl,
- Nawa.gov.pl,
- Crbr.podatki.gov.pl

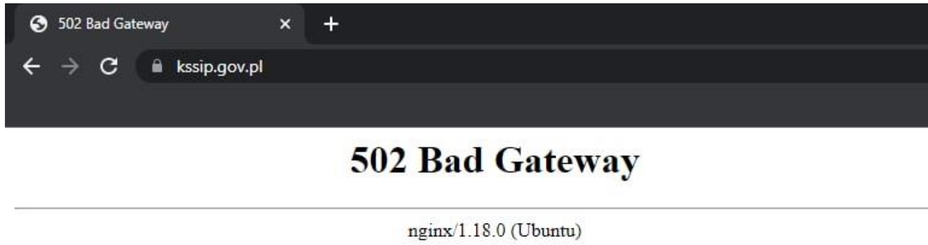
CTI – informacje o działalności grup przestępczych i haktywistów





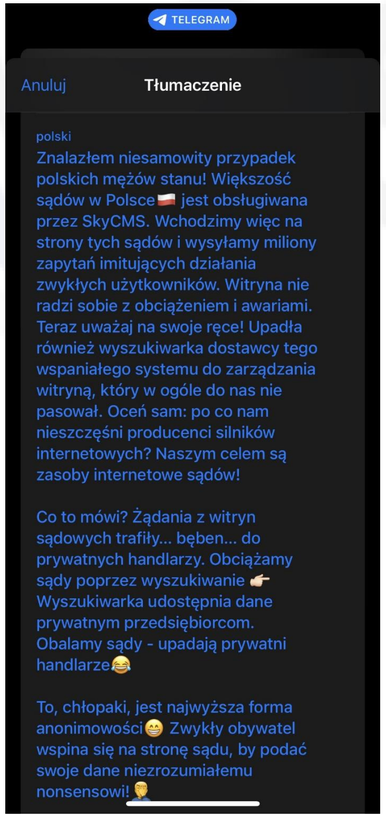


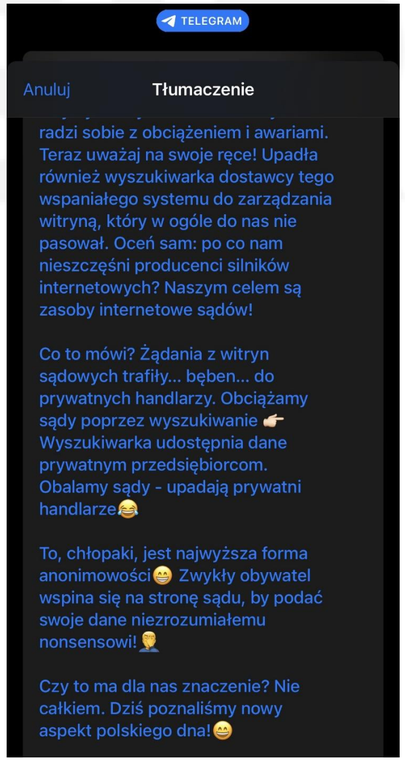




CTI – informacje o działalności grup przestępczych i haktywistów – pozostałe

Grupa NoName057(16) wykonuje ataki głównie na stronach korzystających z systemu zarządzania treścią jakim jest SkyCMS. NoName „ujawniło” sposób na ataki, które przeprowadza na polskie sądy.

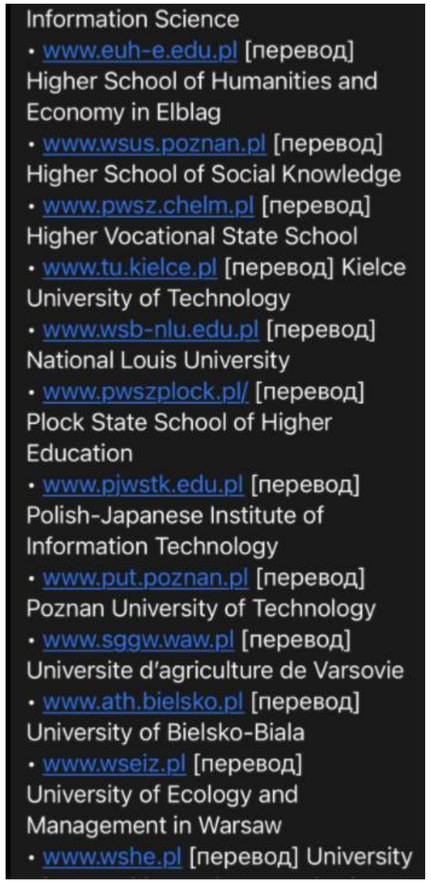


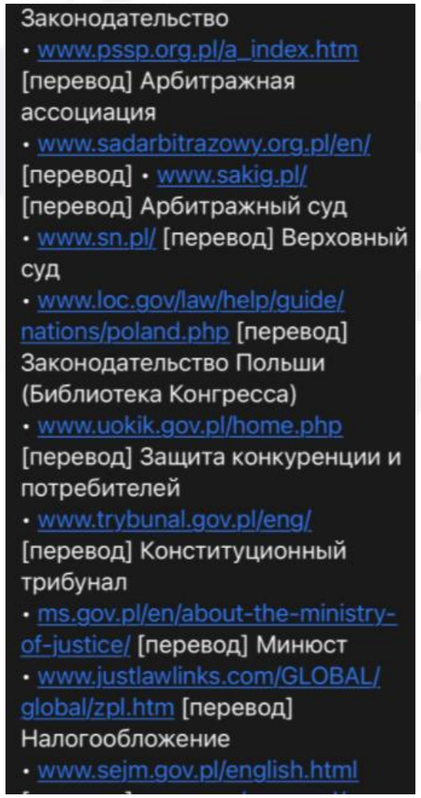


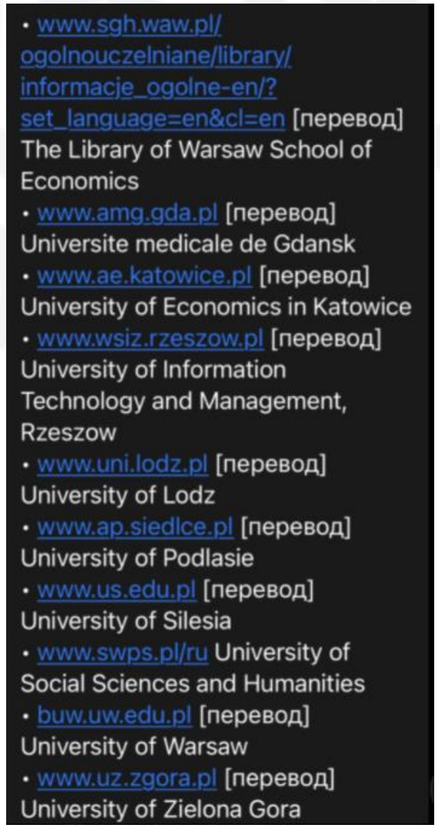
Nowa grupa haktywistyczna

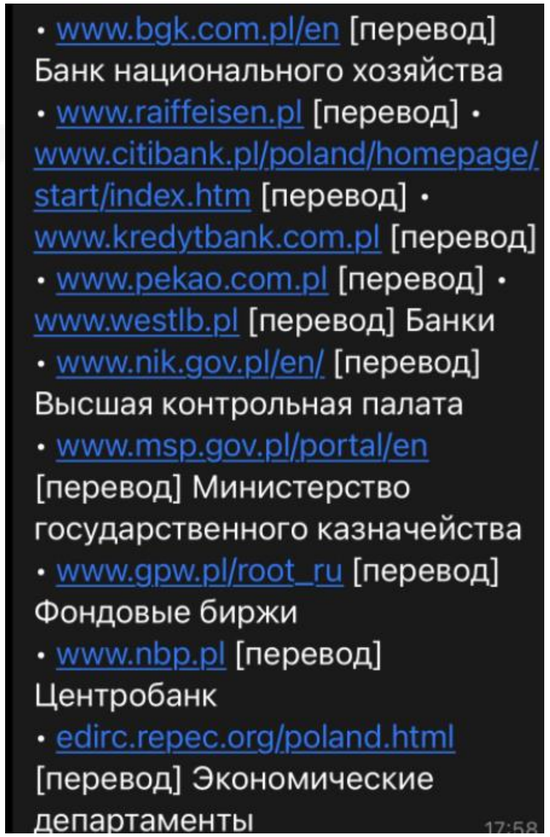
CTI – informacje o działalności grup przestępczych i haktywistów – pozostałe

Ddosia Project zebrała wszystkie potencjalne cele ataków na Polskę.


Information Science
• www.euh-e.edu.pl [перевод]
Higher School of Humanities and Economy in Elblag
• www.wsus.poznan.pl [перевод]
Higher School of Social Knowledge
• www.pwsz.chelm.pl [перевод]
Higher Vocational State School
• www.tu.kielce.pl [перевод] Kielce University of Technology
• www.wsb-nlu.edu.pl [перевод]
National Louis University
• www.pwszplock.pl/ [перевод]
Plock State School of Higher Education
• www.pjwstk.edu.pl [перевод]
Polish-Japanese Institute of Information Technology
• www.put.poznan.pl [перевод]
Poznan University of Technology
• www.sggw.waw.pl [перевод]
Universite d'agriculture de Varsovie
• www.ath.bielsko.pl [перевод]
University of Bielsko-Biala
• www.wseiz.pl [перевод]
University of Ecology and Management in Warsaw
• www.wshe.pl [перевод] University


Законодательство
• www.pssp.org.pl/a_index.htm [перевод] Арбитражная ассоциация
• www.sadarbitrazowy.org.pl/en/ [перевод] • www.sakig.pl/ [перевод] Арбитражный суд
• www.sn.pl/ [перевод] Верховный суд
• www.loc.gov/law/help/guide/nations/poland.php [перевод] Законодательство Польши (Библиотека Конгресса)
• www.uokik.gov.pl/home.php [перевод] Защита конкуренции и потребителей
• www.trybunal.gov.pl/eng/ [перевод] Конституционный трибунал
• ms.gov.pl/en/about-the-ministry-of-justice/ [перевод] Минюст
• www.justlawlinks.com/GLOBAL/global/zpl.htm [перевод] Налогообложение
• www.sejm.gov.pl/english.html


• www.sgh.waw.pl/ogolnouczelniane/library/informacje_ogolne-en/?set_language=en&cl=en [перевод] The Library of Warsaw School of Economics
• www.amg.gda.pl [перевод] Universite medicale de Gdansk
• www.ae.katowice.pl [перевод] University of Economics in Katowice
• www.wsiz.rzeszow.pl [перевод] University of Information Technology and Management, Rzeszow
• www.uni.lodz.pl [перевод] University of Lodz
• www.ap.siedlce.pl [перевод] University of Podlasie
• www.us.edu.pl [перевод] University of Silesia
• www.swps.pl/ru University of Social Sciences and Humanities
• buw.uw.edu.pl [перевод] University of Warsaw
• www.uz.zgora.pl [перевод] University of Zielona Gora


• www.bgk.com.pl/en [перевод] Банк национального хозяйства
• www.raiffeisen.pl [перевод] • www.citibank.pl/poland/homepage/start/index.htm [перевод] • www.kredytbank.com.pl [перевод]
• www.pekao.com.pl [перевод] • www.westlb.pl [перевод] Банки
• www.nik.gov.pl/en/ [перевод] Высшая контрольная палата
• www.msp.gov.pl/portal/en [перевод] Министерство государственного казначейства
• www.gpw.pl/root_ru [перевод] Фондовые биржи
• www.nbp.pl [перевод] Центробанк
• edirc.repec.org/poland.html [перевод] Экономические департаменты
17:58

CTI – informacje o działalności grup przestępczych i haktywistów – Lockbit i wyciek danych z firmy Entrust

Grupa Lockbit przyznała się do ataku oraz wycieku danych z firmy Entrust. Pliki są możliwe do pobrania.

- Victim : entrust.com
- Ransomware : **LockBit**
- Ransomware URL : http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion/post/xAOhe6J7pMnz22zj62fea209d0e74

CTI – informacje o działalności grup przestępczych i haktywistów - ransomware

Atak ransomware „Cuba” na rządowe strony Czarnogóry. Czarnogóra początkowo obwiniała stronę rosyjską o atak – możliwe, że Grupa Cuba jest powiązana i sponsorowana przez Rosję.

U.S. Embassy in Montenegro

Information: Ukrainians in Montenegro Seeking Travel to the U.S.A. Read More...

Visas | U.S. Citizen Services | Our Relationship | Business | Education & Culture | Embassy

Security Alert – Montenegro

Home | News & Events | Security Alert – Montenegro

12

Location: Montenegro, Countrywide

Event: A persistent and ongoing cyber-attack is in process in Montenegro. The attack may include disruptions to the public utility, transportation (including border crossings and airport), and telecommunication sectors.

Actions to Take:

- Be aware of your surroundings.
- Limit movement and travel to the necessities
- Review your personal security plans.
- Have travel documents up to date and easily accessible.
- Monitor local media for updates.

Cuba RANSOMWARE welcomes you

Skupstina

Parliament of Montenegro

Department for Public Relations performs tasks related to the following: informing the public on activities of the Parliament, the President, vice-presidents and the Secretary General, working bodies and MPs, preparing and issuing press releases in cooperation with the organisational units, organising of press conferences, planning, preparing and organising of communication with the public, as well as external communication, providing professional support for appearances in the media, issuing accreditations to the journalists and keeping records of the accredited journalists, as well as organising citizens' visits to the Parliament.

Date the files were received: 19 August 2022

website: https://www.skupstina.me

files: Financial documents, correspondence with bank employees, account movements, balance sheets, tax documents, compensation, source code.

Ransomware – rekomendacje CERT Polska i CISA

RANSOMWARE GUIDE

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.

Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion. The monetary value of ransom demands has also increased, with some demands exceeding US $1 million. Ransomware incidents have become more destructive and impactful in nature and scope. Malicious actors engage in lateral movement to target critical data and propagate ransomware across entire networks. These actors also increasingly use tactics, such as deleting system backups, that make restoration and recovery more difficult or infeasible for impacted organizations. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations large and small.

On September 30, 2020, a joint Ransomware Guide was released, which is a customer centered, one-stop resource with best practices and ways to prevent, protect and/or respond to a ransomware attack. CISA and MS-ISAC are distributing this guide to inform and enhance network defense and reduce exposure to a ransomware attack:

This Ransomware Guide includes two resources:

- **Part 1: Ransomware Prevention Best Practices**
- **Part 2: Ransomware Response Checklist**

CISA recommends that organizations take the following initial steps:

- Join an information sharing organization, such as one of the following:
  - Multi-State Information Sharing and Analysis Center (MS-ISAC): https://learn.cisecurity.org/ms-isac-registration
  - Election Infrastructure Information Sharing and Analysis Center (EI-ISAC): https://learn.cisecurity.org/ei-isac-registration
  - Sector-based ISACs - National Council of ISACs: MEMBER ISACS | natlcouncilofisacs (nationalisacs.org
  - Information Sharing and Analysis Organization (ISAO) Standards Organization: Information Sharing Groups – ISAO Standards Organization/
- Engage CISA to build a lasting partnership and collaborate on information sharing, best practices, assessments, exercises, and more:
  - SLTT organizations: CyberLiaison_SLTT@cisa.dhs.gov v
  - Private sector organizations: CyberLiaison_Industry@cisa.dhs.gov
- Engaging with your ISAC, ISAO, and with CISA will enable your organization to receive critical information and access to services to better manage the risk posed by ransomware and other cyber threats.

Ransomware Guide (Sept. 2020)

Expand All Sections

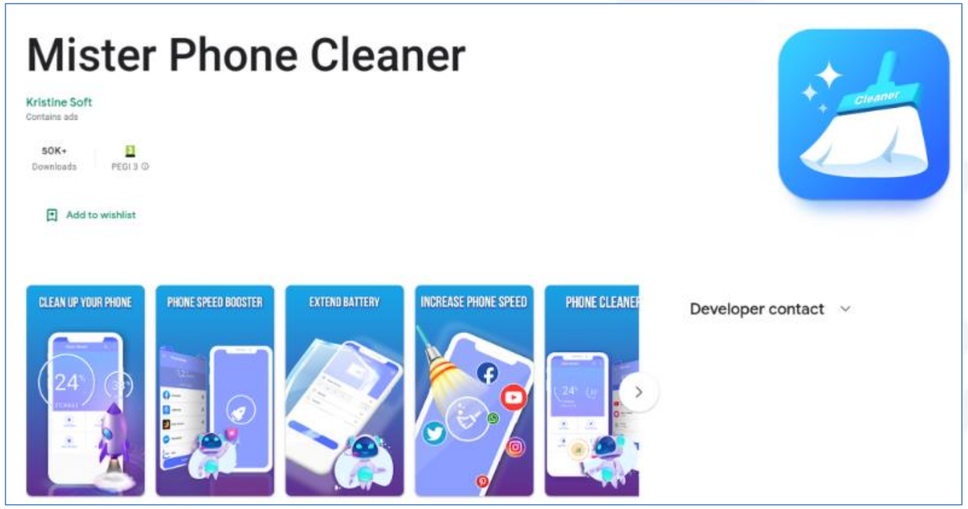
Part 1: Ransomware Prevention Best Practices +

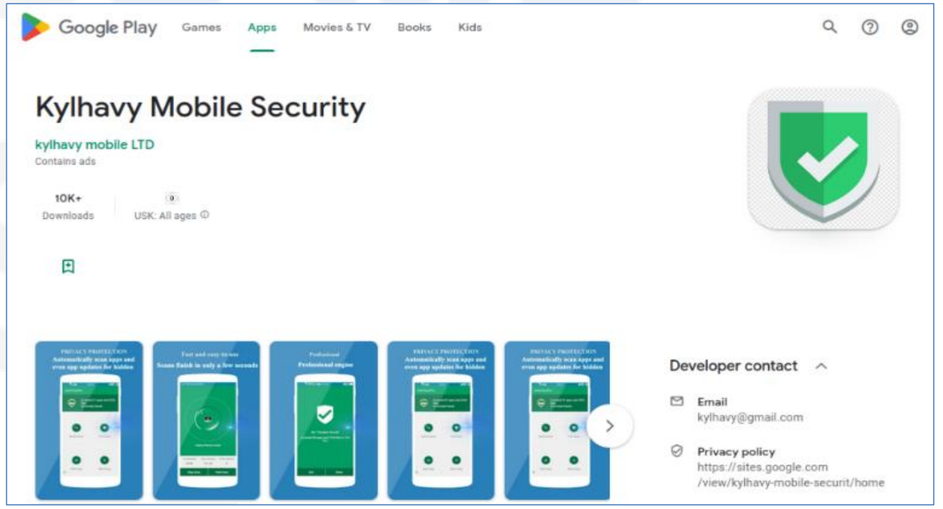
Part 2: Ransomware Response Checklist +

https://www.cisa.gov/stopransomware/ransomware-guide
https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf

Złośliwe oprogramowanie

Sharkbot w Google Play





Rys. 1 – Aplikacje biorące udział w infekcji Sharkbotem

Źródło: *https://blog.fox-it.com/2022/09/02/sharkbot-is-back-in-google-play/*

Złośliwe oprogramowanie

Sharkbot w Google Play

- Dropper został umieszczony w rozwiązaniach typu ***Phone Cleaner*** *oraz* ***Mobile Security***
- W celu ograniczenia wykrycia malware nie wykorzystuje ***Accessibility Services*** na początkowym etapie infekcji (użytkownik samodzielnie instaluje złośliwy moduł serwowany pod pozorem aktualizacji rozwiązania antywirusowego)
- Nowozaobserwowane serwery C2 dystrybuują listę celów obejmujących m.in. **Hiszpanię**, **Polskę**, **Australię**, **Niemcy**, **Austrię** i **USA** (dotychczas były to **Włochy** i **Wielka Brytania**)

Źródło: *https://blog.fox-it.com/2022/09/02/sharkbot-is-back-in-google-play/*

Złośliwe oprogramowanie

Sharkbot w Google Play

- Opisywana wersja droppera weryfikuje **kod kraju operatora karty SIM** (przejście do kolejnej fazy infekcji następuje w przypadku spełnienia warunków określających kraj i atakowaną aplikację zainstalowaną na urządzeniu)
- Aplikacja w sklepie Google jest dostępna do pobrania wyłącznie z **określonych geolokalizacji**
- Na dalszym etapie infekcji malware usiłuje uzyskać dostęp do ***Accessibility Services***

Źródło: *https://blog.fox-it.com/2022/09/02/sharkbot-is-back-in-google-play/*

Złośliwe oprogramowanie

Sharkbot w Google Play – wybrane funkcjonalności wersji 2.25-2.26

- **Injection** / **Overlay** – wyświetlanie nakładki po uruchomieniu atakowanej aplikacji
- **Keylogging** – przechwytywanie *Accessibility eventów (*np. rejestrowanie wciśniętych klawiszy, rejestrowanie zmian w polach tekstowych)
- **Przechwytywanie komunikacji SMS**
- **ATS i zdalna kontrola** (wywoływanie kliknięć, symulacja użycia fizycznych przycisków, podmiana zawartości pól tekstowych, etc.) – umożliwia wykonywanie transakcji bezpośrednio z zainfekowanego urządzenia
- **Wykradanie ciasteczek sesyjnych**
- **Próby wymuszenia logowania z pominięciem biometrii**

Źródło: *https://blog.fox-it.com/2022/09/02/sharkbot-is-back-in-google-play/*

Złośliwe oprogramowanie

BugDrop

- ThreatFabric odnajduje w sieci próbkę **droppera** w fazie deweloperskiej
- Dystrybucja próbki ma odbywać się pod pozorem rozwiązania typu **QR scanner**
- *ThreatFabric* wykazuje korelację badanej wersji ***BugDrop'a*** z grupą związaną ze złośliwym oprogramowaniem ***Xenomorph***
- Prawdopodobne próby wykorzystania ***BugDrop'a*** mogą być ukierunkowane na omijanie mechanizmów bezpieczeństwa implementowanych w systemie Android 13 (ochrona przed przydzieleniem uprawnień typu ***Accessibility*** aplikacjom instalowanym poprzez ***sideloading***)
- Zachęcamy do zapoznania się z artykułem:

https://www.threatfabric.com/blogs/bugdrop-new-dropper-bypassing-google-security-measures.html

Zidentyfikowane zagrożenia dla systemów informatycznych w sierpniu

- **VMware - Workspace ONE, vRealize, Cloud Foundation** szereg krytycznych podatności w produktach VMware. CVE-2022-31656, CVE-2022-31657, CVE-2022-31658, CVE-2022-31659, CVE-2022-31660, CVE-2022-31661, CVE-2022-31662, CVE-2022-31663, CVE-2022-31664, CVE-2022-31665. CVSS scoring określono od 4.7 do 9.8
- **Apache Spark ACL** - krytyczna podatność typu Shell Command Execution, opisana w (CVE-2022-33891 CVSS v3 8.8). Podatność ta dot. wersji Apache niższych od 3.1.3, 3.2.2, 3.3.0.
- **F5 BIG-IP –** Szereg krytycznych podatności dotyczących następujących komponentów: **iControl REST** (CVE-2022-35728 CVSS v3 8.1), **BIG-IP APM access policy** (CVE-2022-35245 CVSS v3 7.5), **TMM** (CVE-2022-34655 CVSS v3 7.5), (CVE-2022-32455 CVSS v3 7.5), (CVE-2022-34862 CVSS v3 7.5), **BIG-IP Message Routing MQTT** (CVE-2022-35240 CVSS v3 7.5), **HTTP2 profile** (CVE-2022-35236 CVSS v3 7.5), **BIG-IP TLS1.3 iRule** (CVE-2022-34651 CVSS v3 7.5), **BIG-IP APM and SSL Orchestrator** (CVE-2022-33203 CVSS v3 7.5), **BIG-IP HTTP MRF** (CVE-2022-35272 CVSS v3 7.5), **BIG-IP monitor configuration** (CVE-2022-35735 CVSS v3 7.2).
- **Dell Unity** – szereg krytycznych podatności w systemach pamięci masowych firmy Dell (Dell EMC Unity, Dell EMC Unity 300, Dell EMC Unity 300F, Dell EMC Unity 350F, Dell EMC Unity 400).

Zidentyfikowane zagrożenia dla systemów informatycznych w sierpniu

- **MS Windows Defender Credential Guard** – krytyczna podatność systemów Windows w tym "Windows Server 2022" w komponencie „Defender Credential Guard”, umożliwiająca eskalację uprawnień w systemie.
- **Splunk Enterprise 9.0.0** - krytyczna podatność komponentu Ingest Action Handler Slunk Enterprise opisana w (CVE-2022-37437 CVSS v3 7.4) polegająca na nieprawidłowej walidacji certyfikatów co negatywnie wpływa na bezpieczeństwo procesu autentykacji.
- **Google Chrome –** podatność typu 0-Day opisana w (CVE-2022-2856) określona jako „insufficient validation of untrusted input in Intents” co, do której nie opublikowano szczegółów z uwagi na trwający proces aktualizacji przeglądarek o poprawkę bezpieczeństwa.
- **Apple** – dwie krytycznych podatności typu Zero-Day
- **Zimbra Collaboration** –krytyczna podatnośc Zimbra Collaboration (ZCS) w wersji niższych niż 8.8.15 patch 33 oraz 9.0 patch 26 opisana w (CVE-2022-27925 CVSS v3 7.2)

Zidentyfikowane zagrożenia dla systemów informatycznych w sierpniu

- **Intel AEPIC Leak** – krytyczna podatność opisna w (CVE-2022-21233 CVSS v3 6.0) dotycząca komponentu APIC „Advanced Programmable Interrupt Controller” wchodzącego w skład architektury procesorów firmy Intel. Podatność prowadzi do wycieku wrażliwych danych bezpośrednio z pamięci cache procesora.
- **VMware** - szereg podatności w VMware vRealize (CVE-2022-31672 CVSS v3 7.2) – eskalacja uprawnień, (CVE-2022-31673 CVSS v3 6.5) – dot. poufności wrażliwych danych, (CVE-2022-31674 CVSS v3 6.5) - dot. poufności wrażliwych danych, (CVE-2022-31675 CVSS v3 5.6) – ominięcie autentykacji,
- **Palo Alto Networks PAN-OS –** podatność typu RDoS TCP, opisana w (CVE-2022-0028 CVSS v3 8.6). Pojawiła się również informacja o publicznie dostępnym **Exploicie** na inną podatność opisaną (CVE-2022-2038 CVSS v3 7.2) dotyczącą komponentu **PAN-OS Management Interface.**
- **Zoom Client for Meetings** – szereg krytycznych podatności w wersji niższej niż 5.11.0 klienta Zoom w tym krytyczna (CVE-2022-28755 CVSS v3 7.8) polegająca na niewłaściwym parsowaniu URL zamieszczanych w Czacie komunikatora, mogąca skutkować RCE po stronie użytkownika
- **Zimbra Collaboration** –krytyczna podatnośc Zimbra Collaboration (ZCS) w wersji niższych niż 8.8.15 patch 33 oraz 9.0 patch 26 opisana w (CVE-2022-27925 CVSS v3 7.2)

Zidentyfikowane zagrożenia dla systemów informatycznych

W dalszym ciągu w przeważającej liczbie ujawnianych ataków cybernetycznych wykorzystywane są, „stare” od dawna znane podatności komponentów systemów i infrastruktury celów ataków.

1) **Windows Runtime Remote Code Execution Vulnerability (CVE-2022-21971)** – krytyczna podatność ujawniona w systemach Windows aż do Windows Server 2022, opublikowana w lutym 2022 roku. Pozwala na zdalne wykonanie kodu po stronie systemu,
2) **Log4Shell (CVE-2021-44228)** – z uwagi na powszechność wykorzystania podatnej biblioteki Log4j.
3) **ProxyShell (CVE-2021-31207, CVE-2021-34473, CVE-2021-34523)** – podatność dot. Serwerów MS Exchange pozwalająca na zdalne wykonanie kodu i podniesienie uprawnień.
4) **ProxyLogon (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065)** – kolejna podatność serwerów MS Exchange 2013, 2016 oraz 2019. Aktywnie wykorzystywana przez chińskie grupy APT m. in. „Hafnium”.

Zidentyfikowane zagrożenia dla systemów informatycznych

W dalszym ciągu w przeważającej liczbie ujawnianych ataków cybernetycznych wykorzystywane są, „stare” od dawna znane podatności komponentów systemów i infrastruktury celów ataków.

5) **Atlassian Confluence Server & Data Center**. Trzy aktywnie wyszukiwane i exploitowane podatności w lipcu, z których dwie ze scorring CVSS v3 na poziomie Critical. **(CVE-2022-26138)** - podatność typu: Hard-Coded Password. Podatne wersje Confluence Server and Data Center 7.4.0, 7.13.0, 7.4.12, 7.16.0, 7.15.1, oraz 7.17.0. **(CVE-2022-26137)** – podatność typu RCE w komponencie „HTTP Request Handler” Atlassian Jira. Skuteczne exploitowanie pozwala na zdalne wykonanie kodu po stronie serwera.
6) **Apple iOS and macOS contain an out-of-bounds write vulnerability (CVE-2022-32893) oraz (CVE-2022-32894)** – podatność systemów operacyjnych i aplikacji w wersjach niższych niż iOS 15.6.1 oraz iPadOS 15.6.1, macOS Monterey 12.5.1 jak również Safari 15.6.1. Pozwalająca na zdalne wykonanie kodu po stronie systemu za pośrednictwem spreparowanego złośliwego kontentu strony www. W przypadku podatnej aplikacji, kod zostanie wykonany z uprawnieniami kernela.

Zidentyfikowane zagrożenia dla systemów informatycznych

W dalszym ciągu w przeważającej liczbie ujawnianych ataków cybernetycznych wykorzystywane są, „stare” od dawna znane podatności komponentów systemów i infrastruktury celów ataków.

.

7) **Palo Alto Networks PAN-OS (CVE-2022-028)** – podatność pozwalająca na wykonanie ataku typu RDoS TCP. W przypadku niestandardowej konfiguracji profilu komponentu „URL filtering” dla strefy z zewnętrzyn interfejsem sieciowym, podatność ta może zostać wykorzystana przez zdalnego atakującego z sieci zewnętrznej.
8) **SAP szereg produktów podatności typu „HTTP request smuggling” oraz „HTTP request concatenation” (CVE-2022-22536)** – podatności w produktach typu ERP (SAP NetWeaver Application Server ABAP, SAP NetWeaver Application Server Java, ABAP Platform, SAP Content Server 7.53, SAP Web Dispatcher) pozwalające nieautoryzowanemu użytkownikowi na spreparowanie requstów HTTP i dodanie do nich dodatkowych parametrów, które zostaną wykonane. Podatność ma wpływ na spójność i poufność danych.