

RANSOMWARE

AKTUÁLNE TRENDY, STRATÉGIE
ÚTOČNÍKOV A DNEŠNÁ REALITA

LUKÁŠ HLAVIČKA

MODUS OPERANDI



1. PRIENIK DO IS ČI INFRAŠTRUKTÚRY

- Webové aplikácie
- Emaily
- Infraštruktúry



2. ÚNIKY DÁT

- Databázy
- Citlivé dáta
- Informácie o používateľoch
- Duševné vlastníctvo



3. RANSOMWARE

- Pracovné stanice
- Servery
- Sieťové úložiská
- Cloudové systémy
- Zálohovacie systémy

KYBERNETICKÝ ÚTOK - TYPY

Shotgun útok

- Útočníci rozošlú infikované emaily na získaný adresár (najčastejšie z nejakého leaku alebo webscrape-u) s infikovanou linkou alebo prílohou
- Útočníci exploitujú zraniteľnosti dostupné zo siete Internet (napr. identifikované prostredníctvom Shodan.io alebo Censys.io)
- Žiadna až minimálna aktivita útočníka v napadnutej infraštruktúre
- Nízka až stredná pravdepodobnosť exfiltrácie údajov
- Útok je primárne cielený na nízko zabezpečené organizácie
 - Útočníci exfiltrujú dáta ku ktorým sa dostanú
 - Útočníci spustia ransomware s právami, ktoré majú k dispozícii
- Zálohy a cloudové úložiská väčšinou zostávajú nedotknuté

KYBERNETICKÝ ÚTOK - TYPY

Shotgun kompromitácia - pokročilá „práca“ na kompromitovanej org.

- Útočníci rozošlú infikované emaily na získaný adresár (najčastejšie z nejakého leaku alebo webscrape-u) s infikovanou linkou alebo prílohou
- Útočníci exploitujú zraniteľnosti dostupné o sieti Internet (napr. identifikované prostredníctvom Shodan.io alebo Censys.io)
- Útočníci kompromitujú subdodávateľa (Kaseya)

SHOTGUN KOMPROMITÁCIA

Stredná až vysoká aktivita útočníka v napadnutej infraštruktúre

- Obchádzanie bezpečnostných opatrení
- Vyhľadávanie a príprava na likvidáciu záloh
- Vytváranie predmostí v infraštruktúre
- Vyhľadávanie „crown jewels“ a ich exfiltrácia
- Snaha o kompromitáciu čo najväčšej časti organizácie
- Vytváranie sekundárnych backdoorov
- Koordinované spustenie ransomware

SHOTGUN KOMPROMITÁCIA

Vysoká pravdepodobnosť exfiltrácie údajov

- Zálohy a cloudové úložiská sú väčšinou kompromitované
- Útočník sa snaží „vydierať 2 až 3-krát“
 - V prípade nezaplatenia, organizácia nedostane prístup k dátam
 - V prípade nezaplatenia, budú dáta organizácie zverejnené
 - V niektorých prípadoch, budú kontaktovaní klienti (v prípade nezaplatenia, budú dáta klientov zverejnené)

KYBERNETICKÝ ÚTOK - TYPY

Cielený útok na organizáciu

- Útočníci vyhľadávajú zraniteľnosti a spôsoby ako sa dostať do organizácie
 - Zraniteľné systémy na perimetri organizácie
 - Spear-phishingové emaily
 - Watering hole útoky
 - Útoky na subdodávateľov
 - Nespokojní zamestnanci

CIELENÝ ÚTOK NA ORGANIZÁCIU

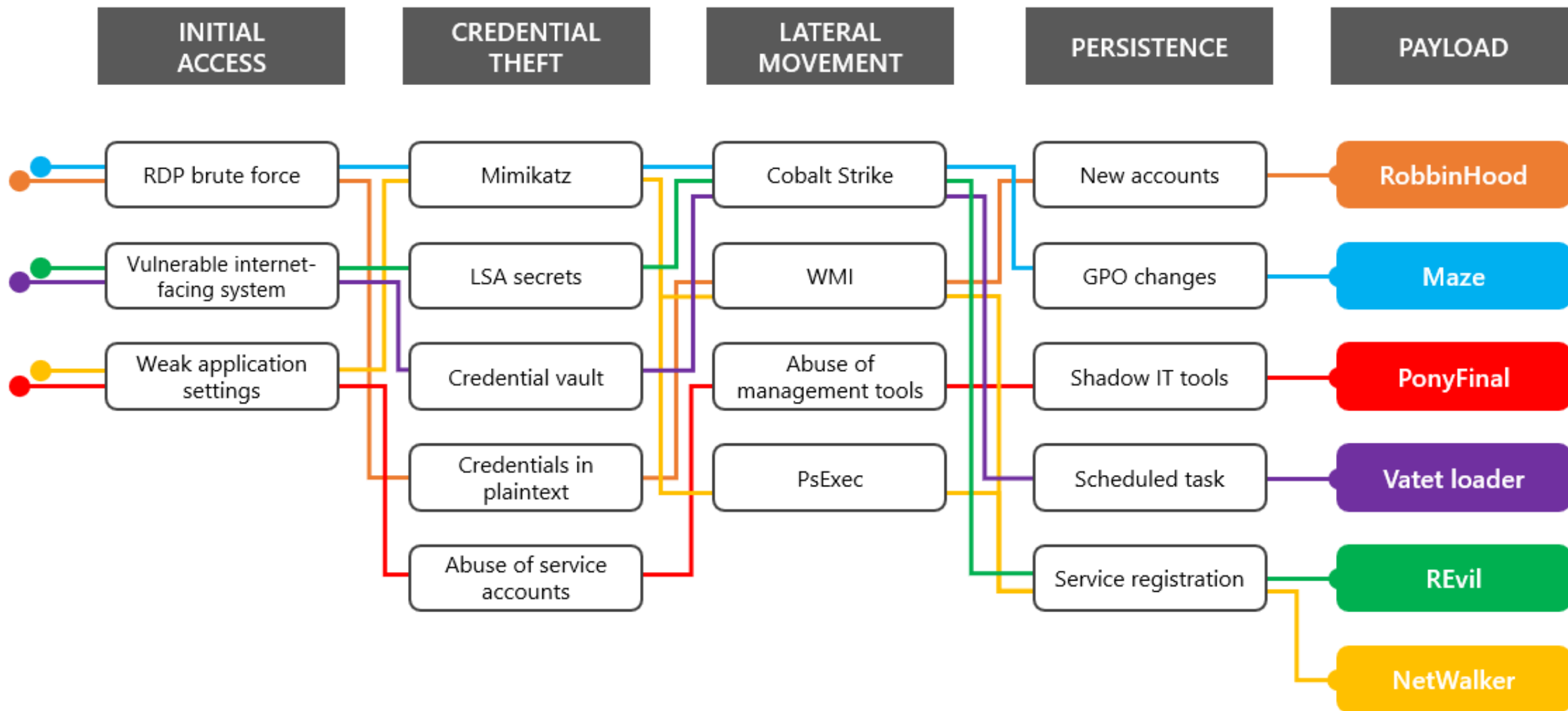
Vysoká aktivita útočníka v napadnutej infraštruktúre

- Obchádzanie bezpečnostných opatrení
- Vyhľadávanie a príprava na likvidáciu záloh
- Vytváranie predmostí v infraštruktúre
- Vyhľadávanie „crown jewels“ a ich exfiltrácia
- Snaha o kompromitáciu čo najväčšej časti organizácie
- Vytváranie sekundárnych backdoorov
- Koordinované spustenie ransomware

CIELENÝ ÚTOK NA ORGANIZÁCIU

Vysoká pravdepodobnosť exfiltrácie údajov

- Cieľom sú bohaté spoločnosti
- Zálohy a cloudové úložiská väčšinou sú kompromitované.
- Útočník sa snaží „vydierať 2 až 3-krát“
 - V prípade nezaplatenia, organizácia nedostane prístup k dátam
 - V prípade nezaplatenia, budú dáta zverejnené
 - V niektorých prípadoch, budú kontaktovaní klienti (v prípade nezaplatenia budú dáta klientov zverejnené)
 - **Novinka:** V prípade nezaplatenia sú kontaktovaní akcionári spoločnosti s hrozbou zverejnenia údajov s cieľom znížiť hodnotu akcií spoločnosti



AKTÍVNE SKUPINY ... NIEKTORÉ

Group Name	Onion V.	Link
Arvin Club	v3	Open
Babuk	v3	Open
BlackByte	v3	Open
Bl4ckt0r	v3	Open
CL0P	v3	Open
CONTI	v3	Open
CRYP70N1C0D3	v3	Open
Cuba	v3	Open
Grief	v3	Open
Hive	v3	Open
HolyGhost	v3	Open
LockBit 2.0	v3	Open
LockData Auction	v3	Open
Lorenz	v3	Open
IV BLOG	v3	Open Open
Medusa	v3	Open
Midas	v3	Open
Moses Staff	v2	Open DEEP-WEB
Pay2Key	v3	Open
Quantum	v3	Open
Ragnar_Locker	v3	Open
RAMP	v3	Open
Ransom Cartel	v3	Open
RansomEXX	v3	Open
Snatch	v3	Open
x001xs	v3	Open

NEAKTÍVNE SKUPINY... NIEKTORÉ

Site Name	Onion V.	Link
? "Leaks from darknet..."	v3	Open
? NONAME	v3	Open Open
54bb47h	v3	Open
AlphaVM	v3	Open
Astro Team	v3	Open
AtomSilo	v3	Open
AvosLocker	v3	Open
Avaddon	v2	Open
BlackMatter	v3	Open
Black Shadow	v2	Open
Bonaci Group	v3	Open
CoomingProject	v3	Open Open [CLEARWEB]
Darkside	v3	Open
DoppelPaymer	v3	Open
Entropy	v3	Open
Everest	v3	Open
Groove	v3	Open
Haron	v3	Open Login: Chaddadgroup:Chaddadgroup
Hitler	v3	Open
Hotarus	v3	Open
Karma Leaks	v3	Open
LockBit	v2	Open
MBC	v3	Open
Mount Locker	v2	Open
N3tw0rm	v3	Open
Nefilim	v2	Open
Payload.bin	v3	Open
Prometheus	v2	Open
Pysa	v3	Open
RAGNAROK	v3	Open
Ranzy/AKO	v3	Open
REvil	v3	Open
Rook	v3	Open

RANSOMWARE GROUP WEBSITE

[Home](#) [PGP KEY](#) [About](#)

bedfordshire.police.uk

Bedfordshire Police Data Leak Leaked data includes emails,names,and phone numbers

March 12, 2022
leak
[MORE](#)

elitemate.com

Leaked dating site information This data includes name, lastname, address, phone,ip and etc DOWNLOAD

January 31, 2022
leak
[MORE](#)

afcx.co

This is just a small part of this site's database.

November 28, 2021
leak
[MORE](#)

Arvin Club

آزادی برای اتصال



Recent Posts

 [bedfordshire.police.uk](#)

 [elitemate.com](#)

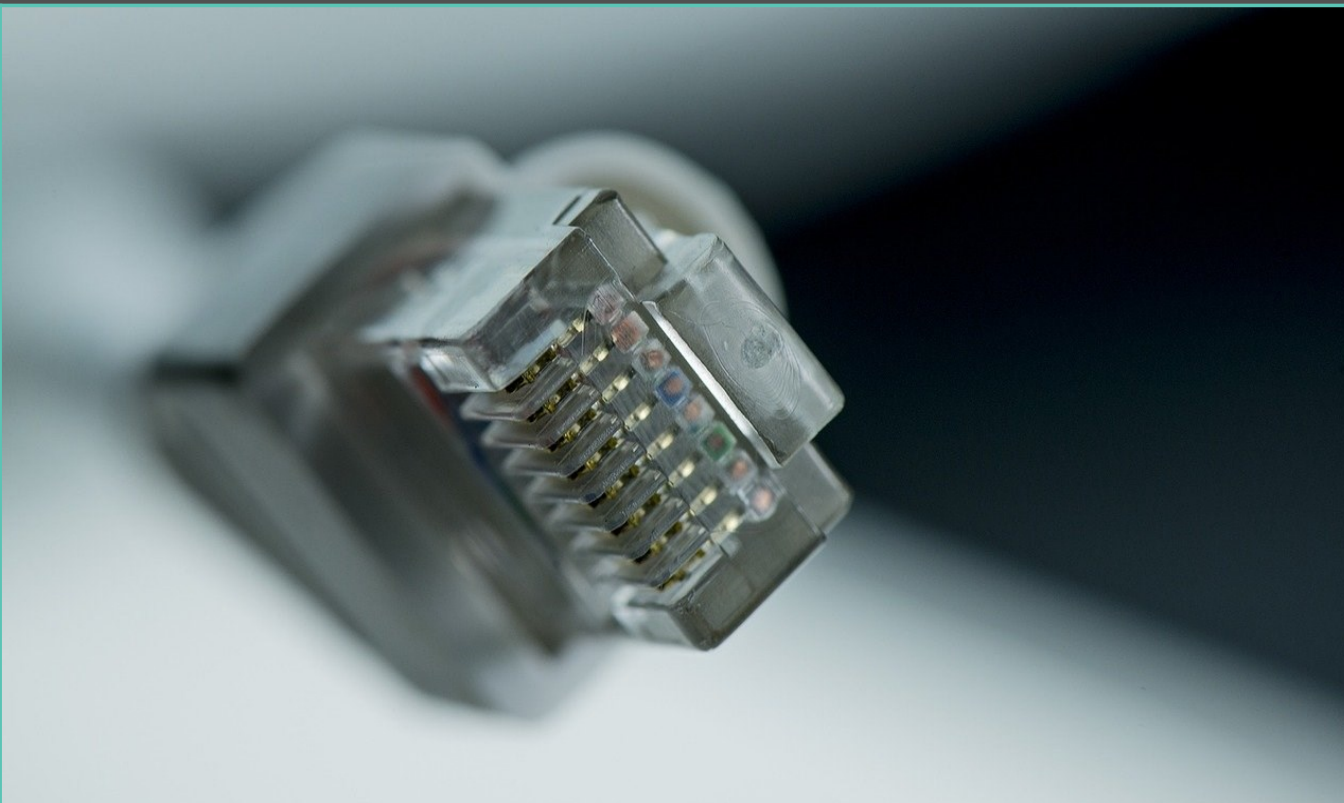
 [afcx.co](#)

RIEŠENIE BEZPEČNOSTNÉHO INCIDENTU



PRVÉ KROKY PO IDENTIFIKÁCIÍ ÚTOKU (RANSOMWARE) DO 2 HODÍN

- Odpojenie zálohovacích technológií !!!!!
- Odpojenie najmenej časti siete ktorá obsahuje všetky kompromitované zariadenia
 - Sieťový segment
 - Lokalitu
 - Celú infraštruktúru (odporúčané)
- Zablokovanie cloudových technológií
 - AWS
 - O365 / Azure
 - GCP



PRVÉ KROKY PO IDENTIFIKÁCIÍ ÚTOKU (RANSOMWARE) DO 6 HODÍN

- Kontrola integrity záloh
- Spustenie procesu riešenia bezpečnostných incidentov
 - Vymenovanie veliteľa incidentu
 - Zostaviť IR team
 - Interný tím
 - Externá podpora
- Triáž bezpečnostného incidentu
- Zaistenie digitálnych stôp
- Spustenie vytvárania IR plánu (prípadne overenie existujúceho)
- Identifikácia spôsobu šírenia



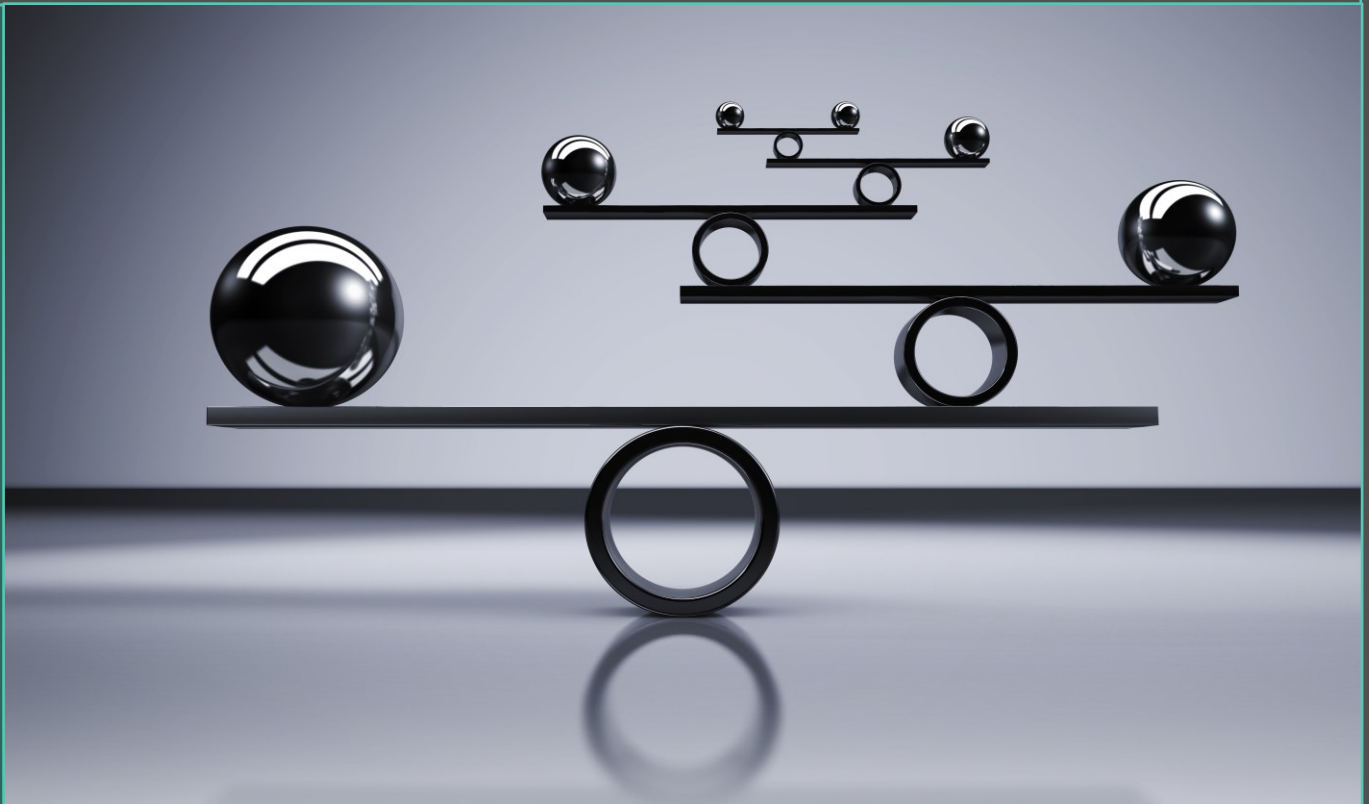
PRVÉ KROKY PO IDENTIFIKÁCIÍ ÚTOKU (RANSOMWARE) DO 24-48 HODÍN

- Spustenie implementácie IR plánu
- Obnova infraštruktúry zo záloh ?
- Reinštalácia infraštruktúry ?
- Identifikácia chýbajúcich technológií
- Spustenie inštalácie chýbajúcich technológií
- Kroky
 - Zaistenie digitálnych stôp
 - Analýza bezpečnostného incidentu
 - Eradikácia / obnovenie
 - Bezpečnostný dohľad



ZABEZPEČENIE INFRAŠTRUKTÚRY PRED ĎALŠÍM PRIENIKOM

- Quick wins
 - Zmena hesiel/privátnych kľúčov (vrátane technických)
 - Odstránenie sekundárnych infekcií/backdoorov
 - Reštriktívne pravidlá firewallu (whitelisting)
 - Základný hardening systémov prístupných z internetu
 - Základný hardening pracovných staníc, Active Directory a Cloud
- Monitoring infraštruktúry + kontinuálny compromise assessment
- Incident readiness assessment a implementácia opatrení



KROKY PO VYRIEŠENÍ BEZPEČNOSTNÉHO INCIDENTU

- Forenzná analýza
 - Aktivita útočníka v systéme
 - Iniciálny bod kompromitácie
 - Identifikácia sekundárnych infekcií
- Vykonanie kompletného bezpečnostného auditu
- Identifikácia:
 - Root cause kompromitácie systému
 - Problémov pri riešení bezpečnostného incidentu
 - Procesy
 - Technológie ľudia



NÁŠ TÍM



ÚSPECHY

- Nájdenie viacerých zraniteľností v operačných systémoch, IT a OT systémoch (6 pridelených CVE, ďalších 15 v procese)
- Súčasť víťazného tímu NATO Locked Shields (4 členovia tímu)
- Autori a spoluautori viacerých výskumných tém prezentovaných na najlepších svetových konferenciách (vrátane DefCon, CyberCrimeCon, Black Hat, TF CSIRT atď.)
- Autori a spoluautori viacerých nástrojov kybernetickej bezpečnosti (Gargamel, vakcína proti ransomvéru, IOC checker, ESET Log parser atď.)



SKÚSENOSTI

- Reakcie na incidenty a operácie kybernetickej obrany vo vládných inštitúciách, globálnych finančných, fintech, technologických a neziskových organizáciách
- Vykonali sme viac ako 290 reakcií na incidenty, forenzných činností a kybernetickej obrany proti 13 aktérom hrozieb typu APT
- Penetračné testovanie a red teaming v spoločnostiach patriacich do Fortune 500, vládných inštitúciách a neziskových organizáciách
- Vykonali sme viac ako 240 red teamingov a stovky penetračných testov

NAŠE SLUŽBY



Incident Response

Rapid on-site deployment and remote response and mitigation of computer security incidents



Digital Forensics

Acquisition of digital evidence, investigation, and reconstruction of security incidents



Malware Analysis

Analysis of properties, functionality, origin and potential impacts of malicious code



Threat Hunting

Active hunting for threats in infrastructure based on TTPs and searching for indicators of compromise



CSIRT Services

Full array of CSIRT services, including 24/7 DFIR and proactive security



Incident Preparedness

Assessment of adequacy of processes and technology for swift and effective reaction.



Offensive Security

Vulnerability Assessment, Penetration Testing, Red Team and Purple Team Engagements



Attack Simulations

Phishing, Spearphishing, Whaling. Custom Scenarios incl. Custom "Malware"



Managed Defense

SOC Level 3 + Level 4. Network and Endpoints. EDR, SIEM, SOAR.



Defensive Intelligence

Data Leaks Searches and Analysis, ClearWeb, DeepWeb, DarkWeb



Advisory Services

Audits and Implementations of Security Frameworks, vCISO. Technical Audits and Hardening



Trainings and Exercises

Trainings for personnel, IT professionals and management. Tabletop exercises and drills

NAŠE CERTIFIKÁCIE



ĎAKUJEM ZA POZORNOST

OTÁZKY?

KONTAKTUJE NÁS



INFO@ISTROSEC.COM



+421 917 699 002



WWW.ISTROSEC.COM



WWW.ISTROSEC.COM/BLOG/