

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

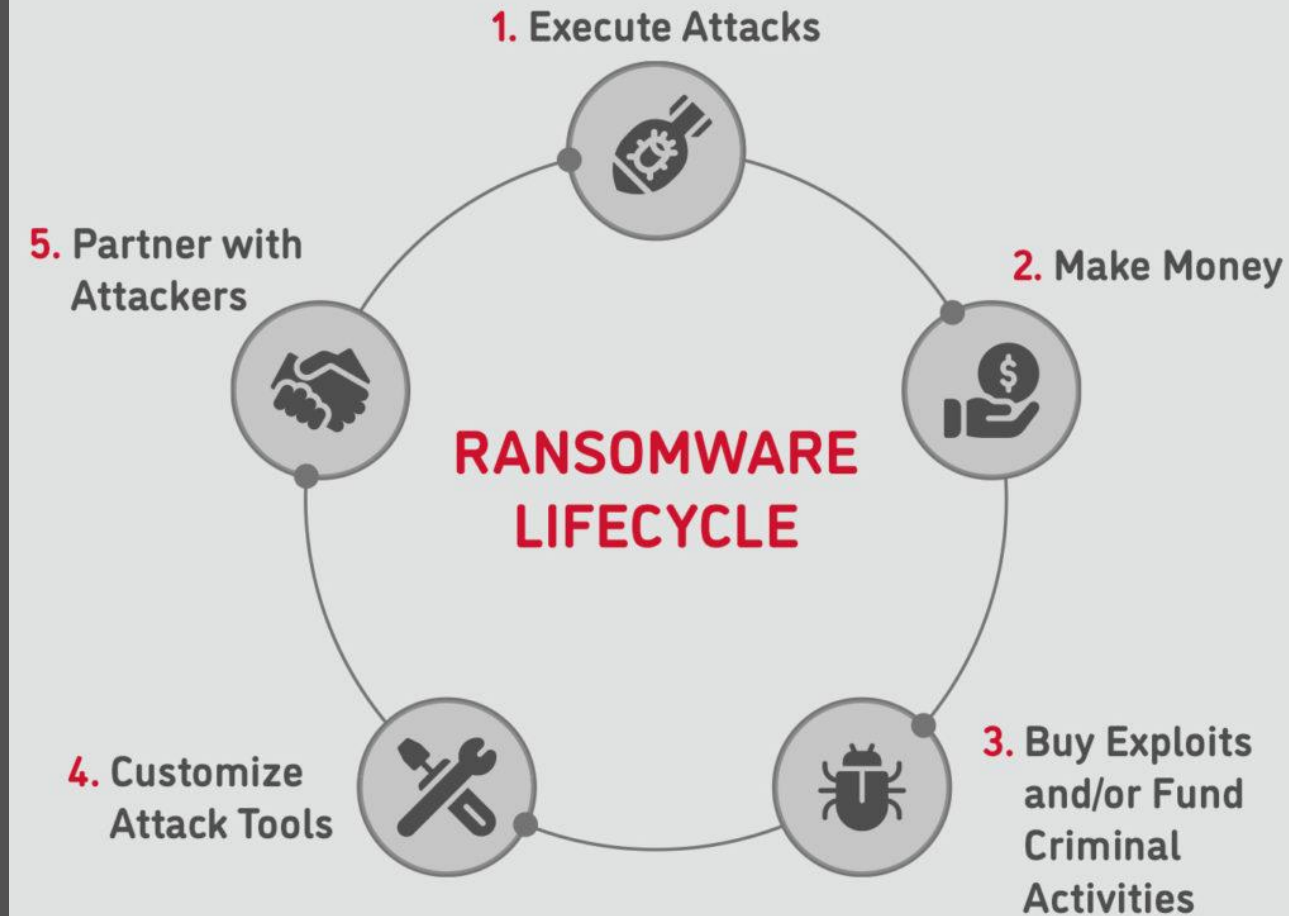
- Databázy
- Citlivé dáta
- Informácie o používateľoch
- Duševné vlastníctvo



3. RANSOMWARE

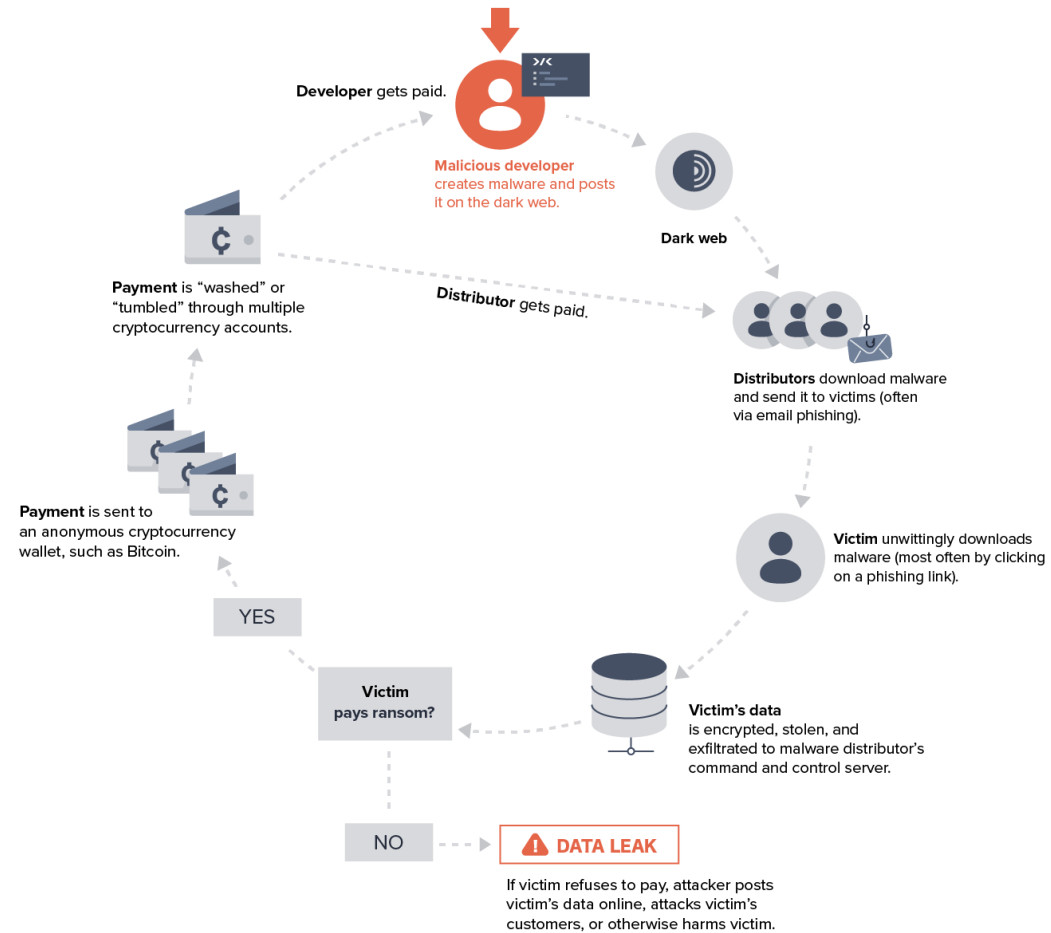
- Pracovné stanice
- Servery
- Sieťové úložiská
- Cloudové systémy
- Zálohovacie systémy

RANSOMWARE Z POHL'ADU EKONOMIKY



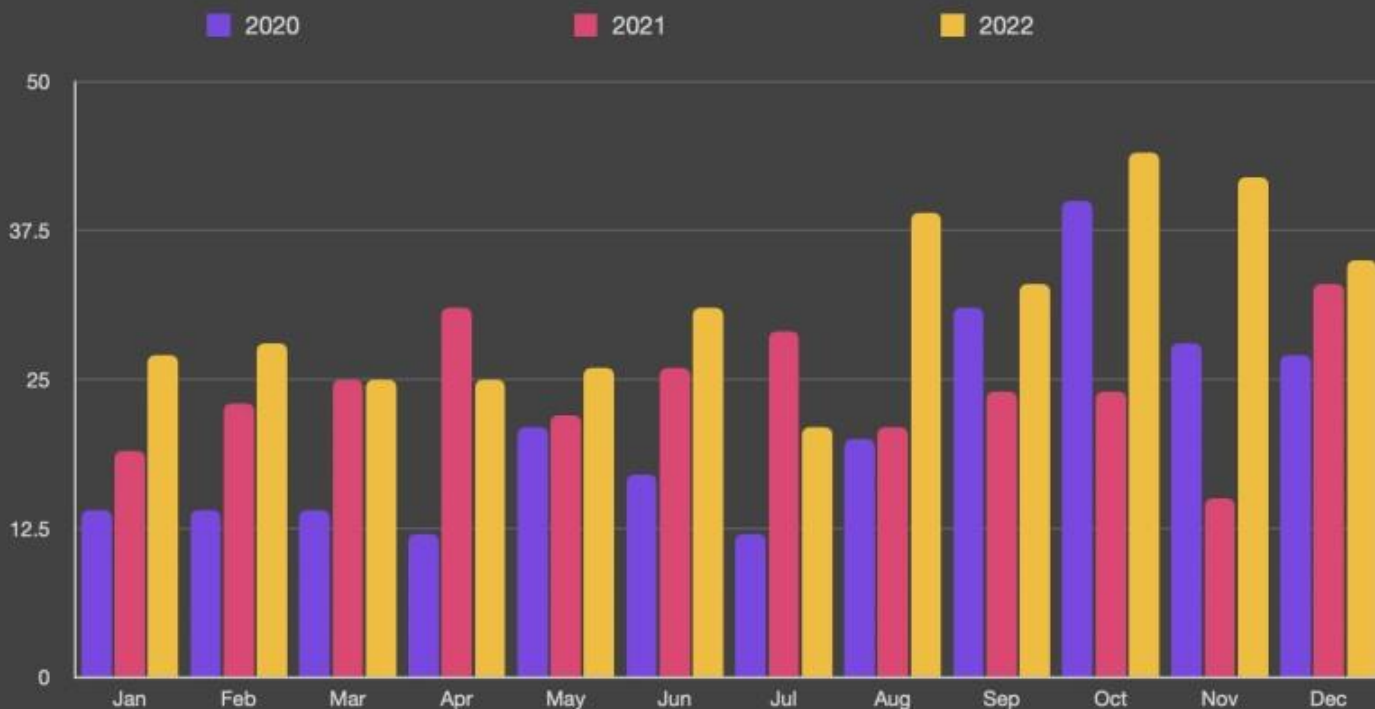
RANSOMWARE EKOSYSTÉM

The Ransomware Ecosystem



RANSOWMARE TRENDS

Ransomware Trend by Month



Key Trends



87% of all attacks use PowerShell



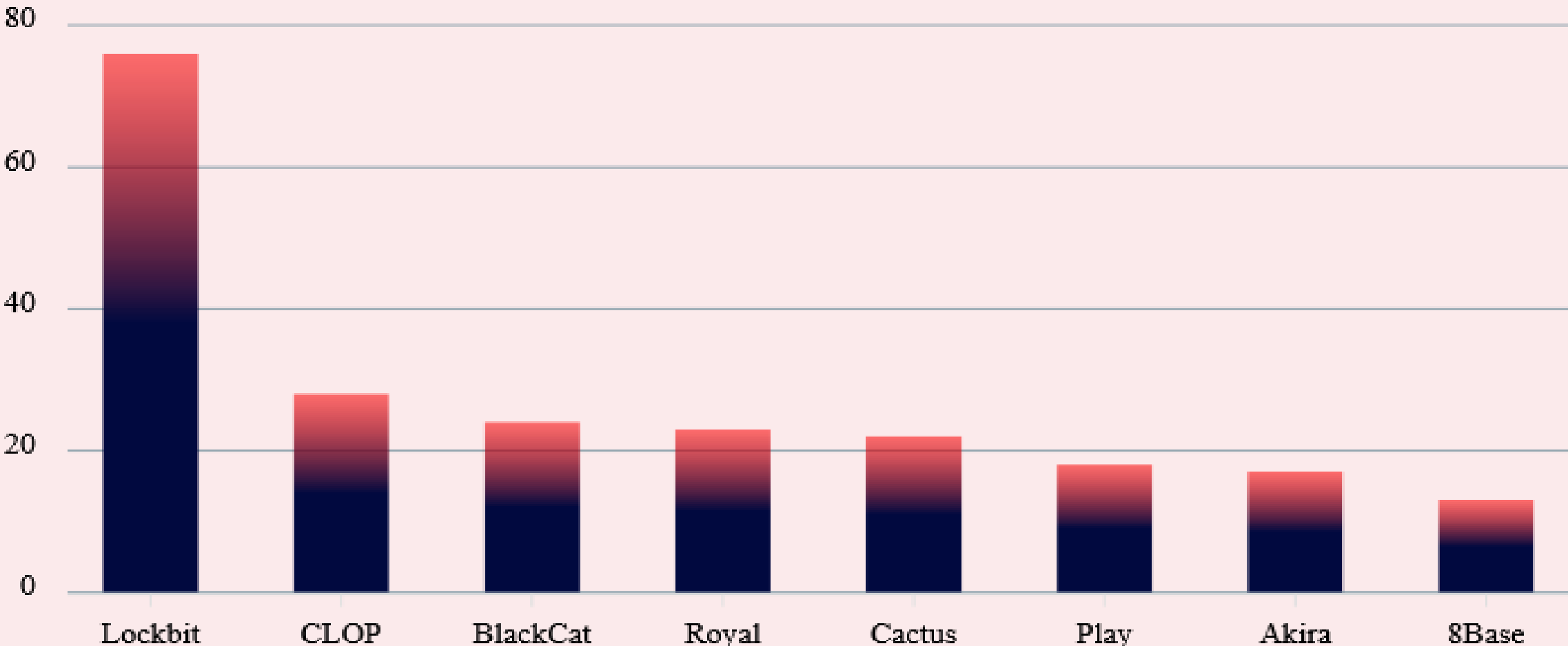
89% of attacks exfiltrate data



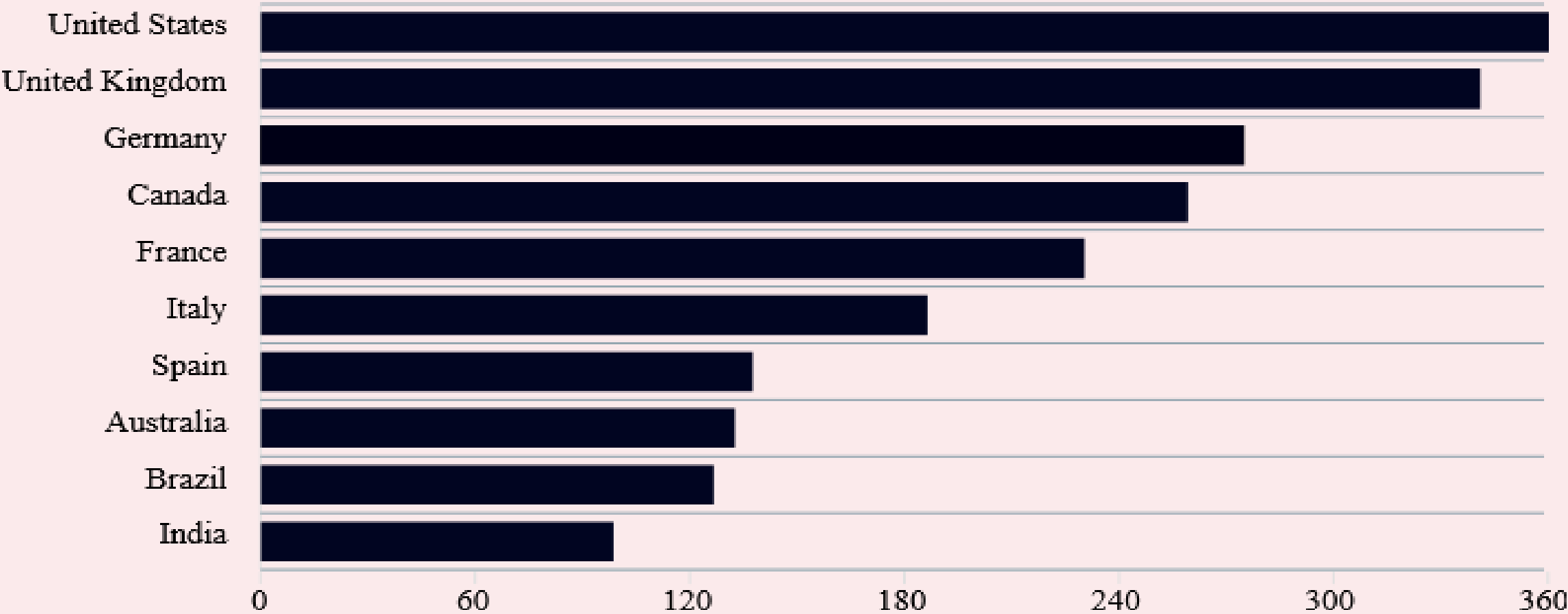
Average payout
US \$258,143k
+13.2% from Q2/22

Copyright © 2022 BlackFog, Inc. Key statistics compiled and collected by BlackFog from various sources including BlackFog Enterprise. May only be used with attribution link to blackfog.com

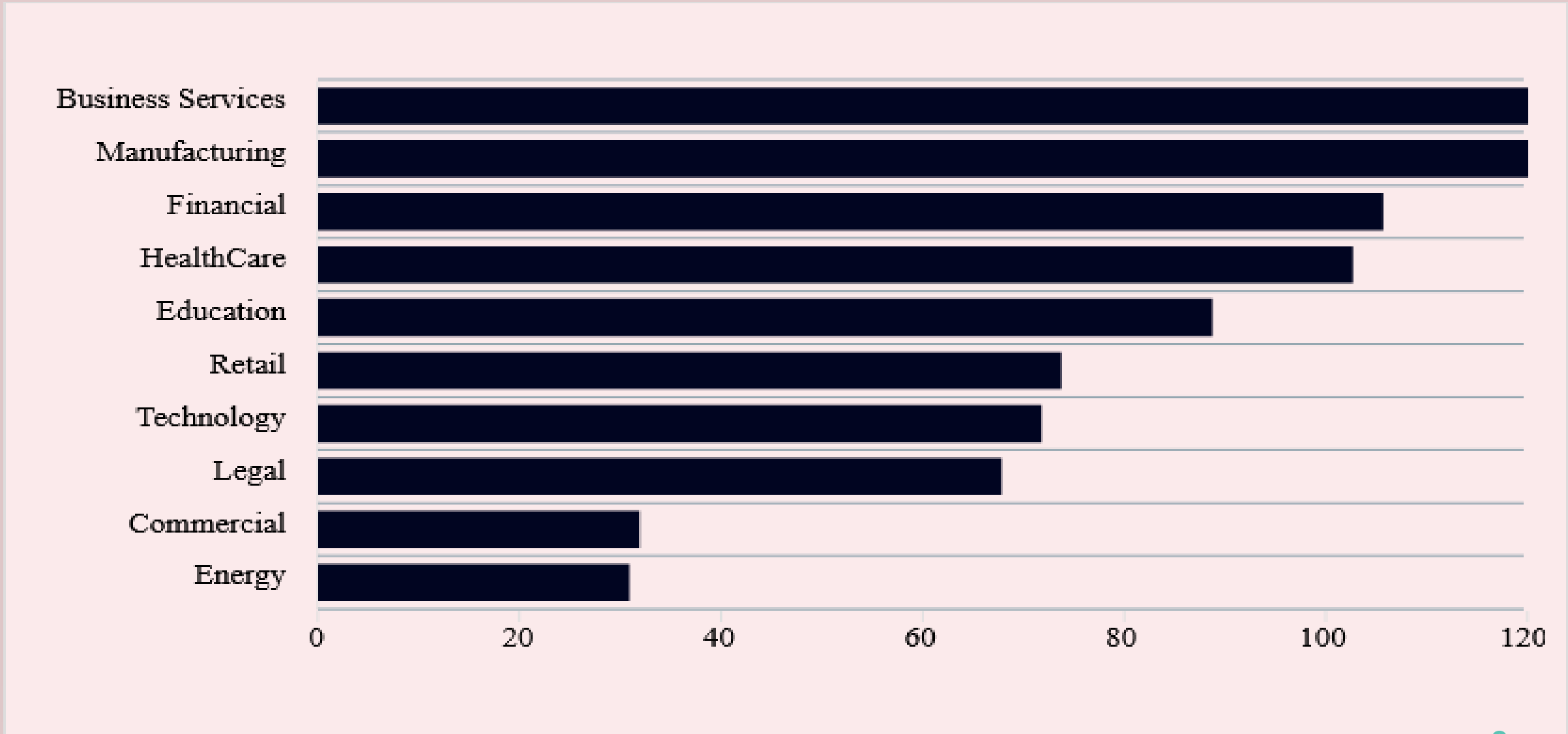
Top Group VPM - Average Victims Per Month



Top Targeted Countries



Top Targeted Sectors



TOP TRENDY ZA 2023



Primárny focus na exfiltráciu dát



Pomer príjmu z monetizácie dát voči sume za dešifrovanie rastie



Cielené útoky na cloudové systémy



Útoky na virtualizačné platformy

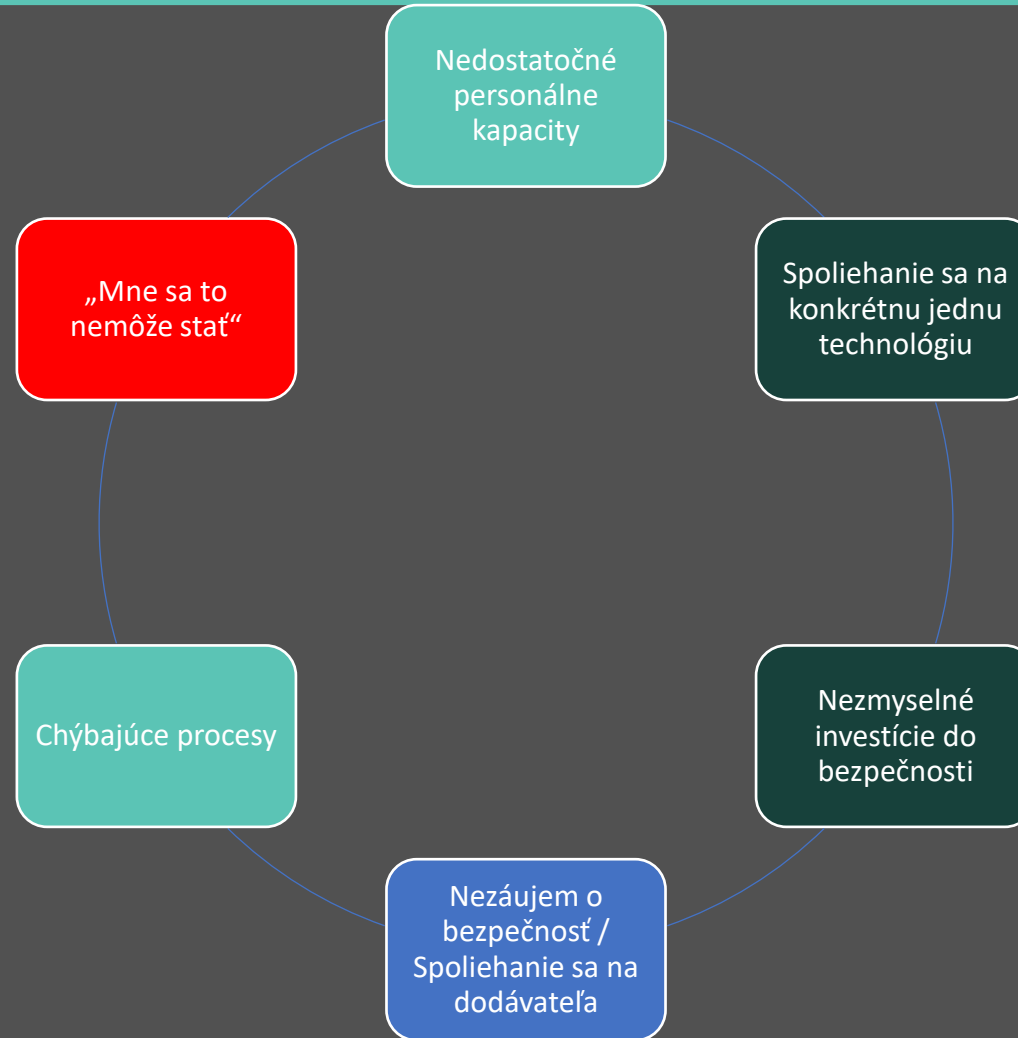


Automatizácia útokov



Exploitácia 0-day a 1-day zraniteľností

ČO ROBIA ORGANIZÁCIE ZLE



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/