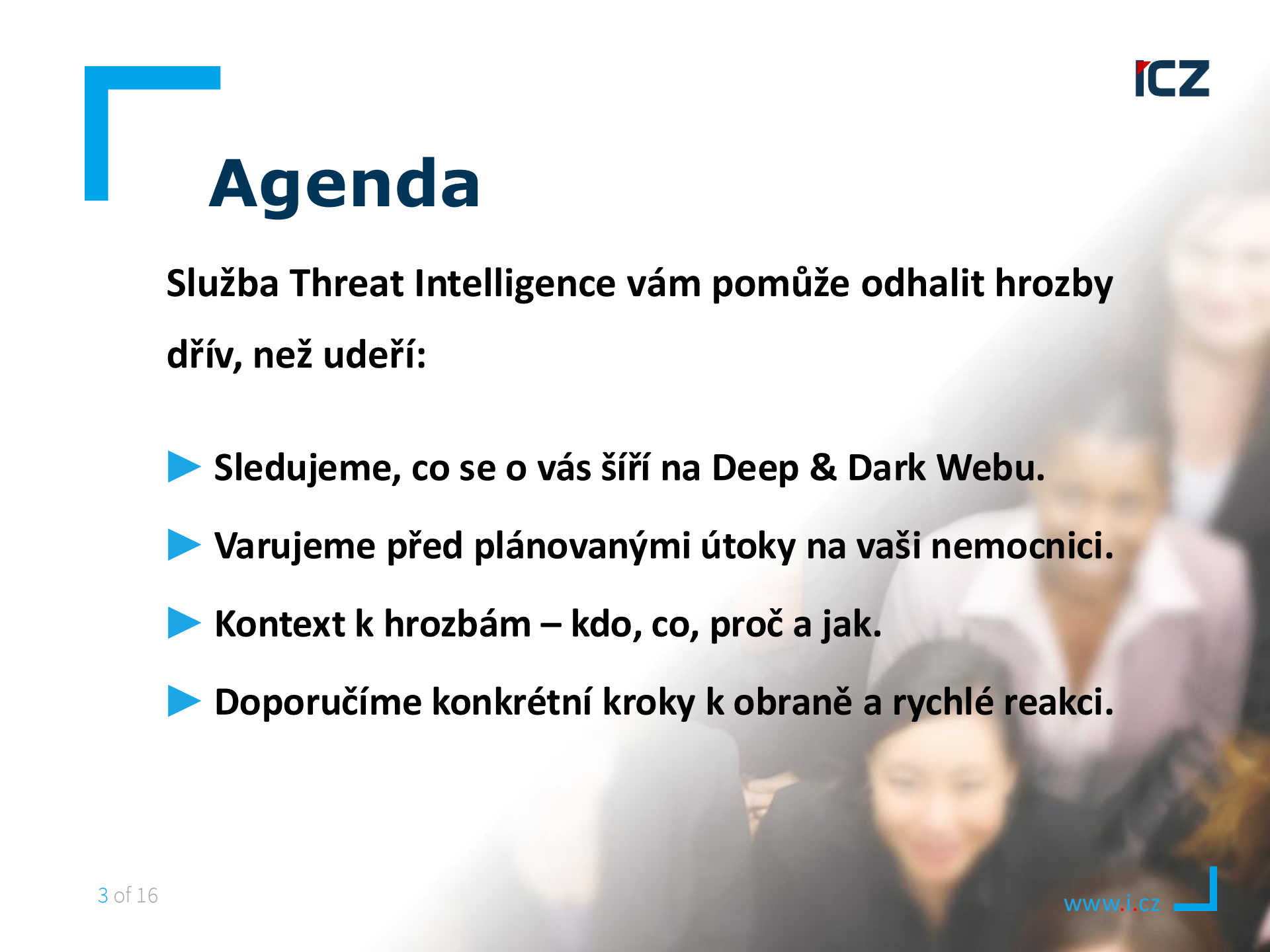
Získejte náskok před útočníky - Threat Intelligence

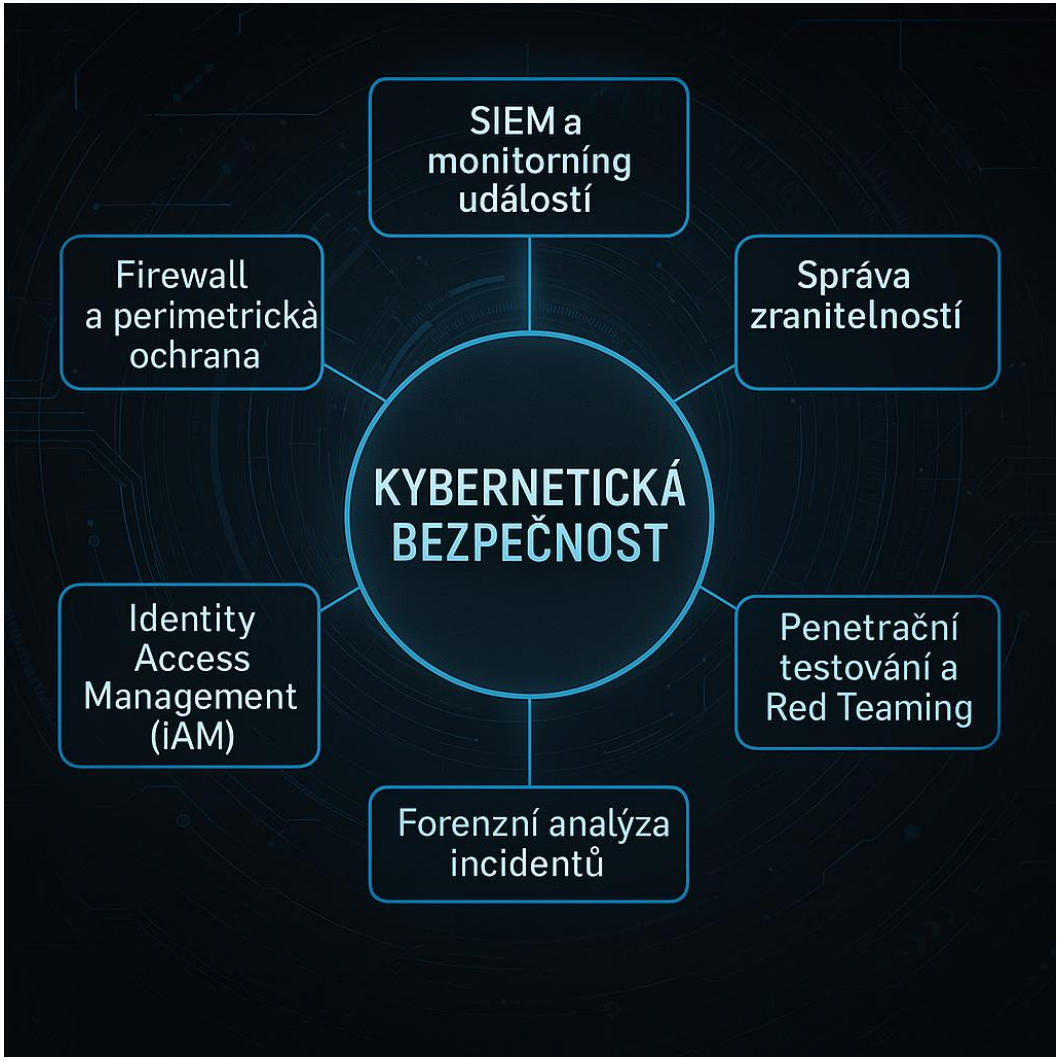
Agenda

Služba Threat Intelligence vám pomůže odhalit hrozby dřív, než udeří:

- **Sledujeme, co se o vás šíří na Deep & Dark Webu.**
- **Varujeme před plánovanými útoky na vaši nemocnici.**
- **Kontext k hrozbám – kdo, co, proč a jak.**
- **Doporučíme konkrétní kroky k obraně a rychlé reakci.**



Kybernetická Bezpečnost



Proč je zdravotnictví terčem?

- Kyberútoky narůstají, i na nemocnice
- Citlivá data, nepřetržitý provoz, omezené IT zdroje
- Pro útočníky je to 'měkký cíl‘ a zajímavý cíl

Nebezpečí, které nevidíme . . .

Co o vás ví útočník dřív,

než vůbec uvidíme náznaky útoku?

- Data mohou být prodávána na dark webu
- Útoky nezačínají útokem, ale výzvědnou činností
- Příprava útoku trvá týdny

Threat Intelligence

1. Včasné varování před hrozbami

Platforma sbírá obrovské množství dat z otevřených zdrojů (OSINT), dark webu, fór hackerů, sociálních sítí a interních bezpečnostních kanálů.

Díky tomu firma dostane **upozornění na nové zranitelnosti, útoky nebo úniky dat** ještě dřív, než se stihnou rozšířit.

2. Prevence proti kyberútokům

Pomáhá **identifikovat, které konkrétní hrozby jsou pro vaši firmu nejrelevantnější**.

Umožňuje zaměřit obranu na nejkritičtější oblasti a zranitelnosti.

Threat Intelligence

3. Analýza úniků a kompromitovaných dat

Platforma monitoruje, jestli **neunikly přihlašovací údaje nebo firemní data** na dark webu nebo v úložištích úniků.

Může tak pomoci odhalit například **úniky e-mailových adres, hesel nebo citlivých dokumentů**.

4. Zrychlení reakce na incidenty

Integruje se s nástroji pro správu incidentů (např. SIEM, SOAR) a pomáhá **automatizovat reakce na bezpečnostní incidenty**.

Bezpečnostní tým tak může rychleji zjistit, co se děje, a správně zareagovat.

Threat Intelligence

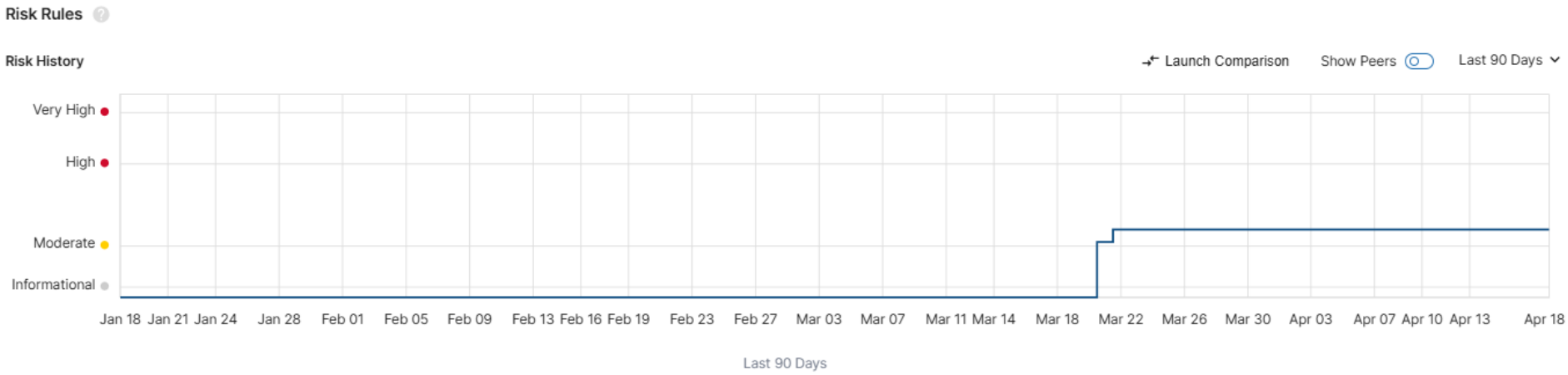
5. Podpora rozhodování vedení

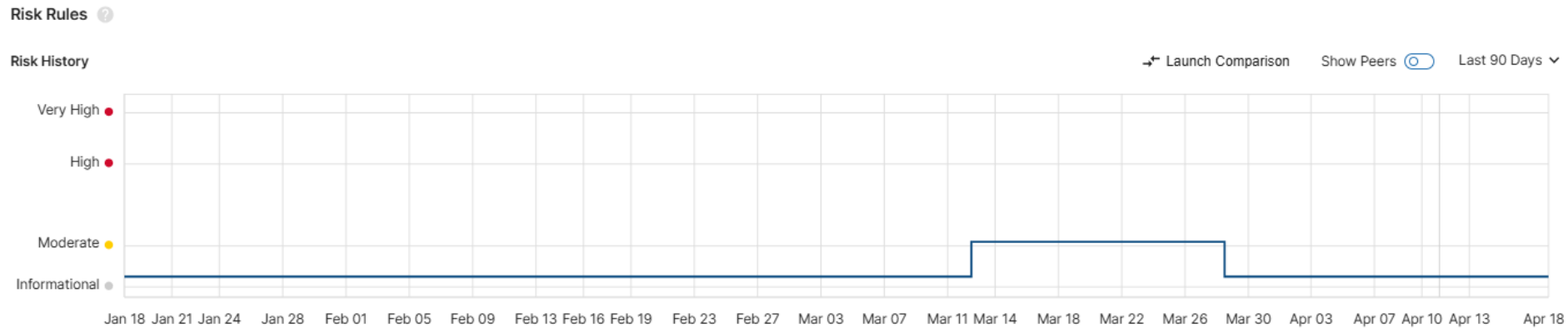
Poskytuje **strategické reporty a analýzy**, které pomáhají vedení firmy pochopit aktuální rizika a správně investovat do kybernetické ochrany.

6. Soulad s předpisy a compliance

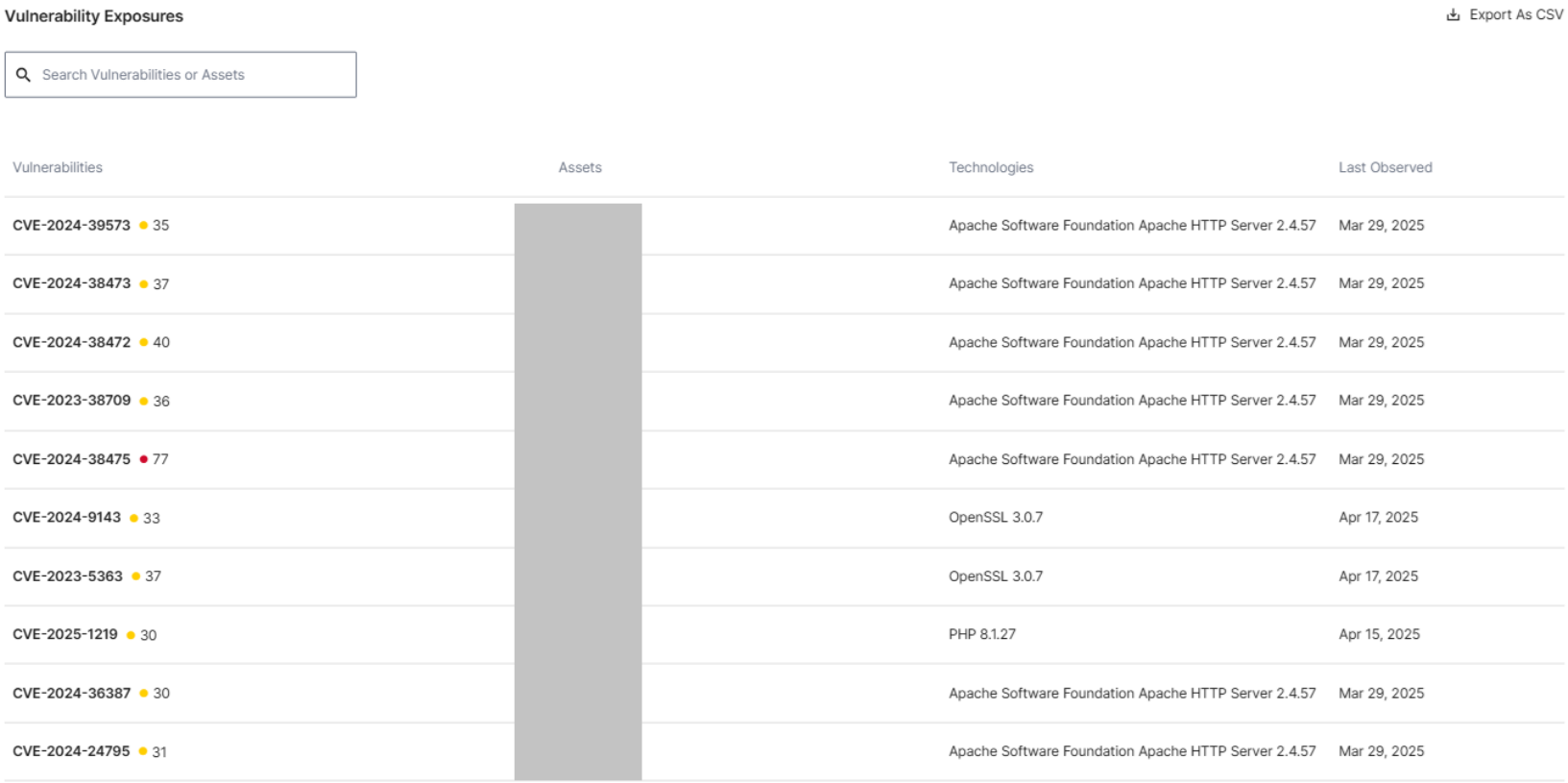
Pomáhá splnit bezpečnostní požadavky regulací (např. NIS2, GDPR), protože umožňuje efektivní sledování a dokumentaci hrozeb.

Vulnerability Exposures





Vulnerability Exposures



Přihlašovací údaje na Dark webu

email	password	documentTitle	documentPublishDate
vasakj@nemocnice.cz	Ad**********	Malware Logs 7236-7257 | Part 1	2025-04-09T11:00:26.000Z
lekarna@nemocnice.cz	PDH**********	April 2025 Combo Lists | Part 39	2025-04-06T00:00:00.000Z
slavicekl@nemocnice.cz	582**********	April 2025 Combo Lists | Part 39	2025-04-06T00:00:00.000Z
bratrankovav@nemocnice.cz	175**********	February 2025 Combo Lists | Part 2	2025-03-19T00:00:00.000Z
vanekm@nemocnice.cz	YF**********	Malware Logs 4561	2025-02-23T16:03:25.000Z
kucerovao@nemocnice.cz	Sl**********	Malware Logs 671	2025-1-13T15:58:57.109Z

Phishing Detections

Recorded Future Phishing Detections

Infrastructure Analysis

APR 11 2025

Recorded Future Phishing Detection analysis of https://illegaladboosters-pi.vercel.app/zL20vMDFjcjl4entry=ttu&g_ep=EgoyMDI1MDM on April 11, 2025

"**https://illegaladboosters-pi.vercel.app/zL20vMDFjcjl4entry=ttu&g_ep=EgoyMDI1MDM** was reported as phishing impersonating **facebook** on April 11, 2025."

Source Recorded Future Phishing Detection on Apr 11, 2025, 02:451+ reference

Infrastructure Analysis

APR 8 2025

Recorded Future Phishing Detection analysis of https://trackinfringementfunnelboost.vercel.app/get_help on April 08, 2025

"**https://trackinfringementfunnelboost.vercel.app/get_help** was reported as phishing impersonating **meta** on April 08, 2025."

Source Recorded Future Phishing Detection on Apr 8, 2025, 03:521+ reference

Infrastructure Analysis

APR 6 2025

Recorded Future Phishing Detection analysis of https://northern-stitch-coelurus.glitch.me/ks8s.html on April 06, 2025

"**https://northern-stitch-coelurus.glitch.me/ks8s.html** was reported as high confidence phishing impersonating **deutsche telekom** on April 06, 2025."

Source Recorded Future Phishing Detection on Apr 6, 2025, 04:041+ reference

Infrastructure Analysis

APR 5 2025

Recorded Future Phishing Detection analysis of https://mangokl.com/ on April 05, 2025

"**https://mangokl.com/**, which was indicated as phishing, is no longer live as of April 05, 2025."

Source Recorded Future Phishing Detection on Apr 5, 2025, 02:001+ reference

Infrastructure Analysis

APR 3 2025

Recorded Future Phishing Detection analysis of https://apply-for-page-terms-review-here.vercel.app/index.html on April 03, 2025

"**https://apply-for-page-terms-review-here.vercel.app/index.html** was reported as high confidence phishing impersonating **facebook** on April 03, 2025."

Source Recorded Future Phishing Detection on Apr 3, 2025, 03:551+ reference

výzva k akci

- Útok je otázka 'kdy', ne 'jestli‘
- Útok je otázka JAK?
- Threat Intelligence vám dává možnost mít náskok
- Bez informací bojujeme poslepu
    - Každý kdo bojoval s hrozbou to ví
- S informacemi máme šanci něco udělat.

www.i.cz

Erik Mikuš
erik.mikus@i.cz

Music: http://www.bensound.com