

Analýza krizového řízení kybernetického útoku

Lukáš Březina, CEH/PCNSE
CTO Security - Taktik a.s.



Úvod do incidentu



Datum útoku

11/2024, víkend



Typ útoku

INC Ransom / INC Ransomware



Počáteční dopad

Exfiltrace 2TB dat / zašifrovaná server VLAN

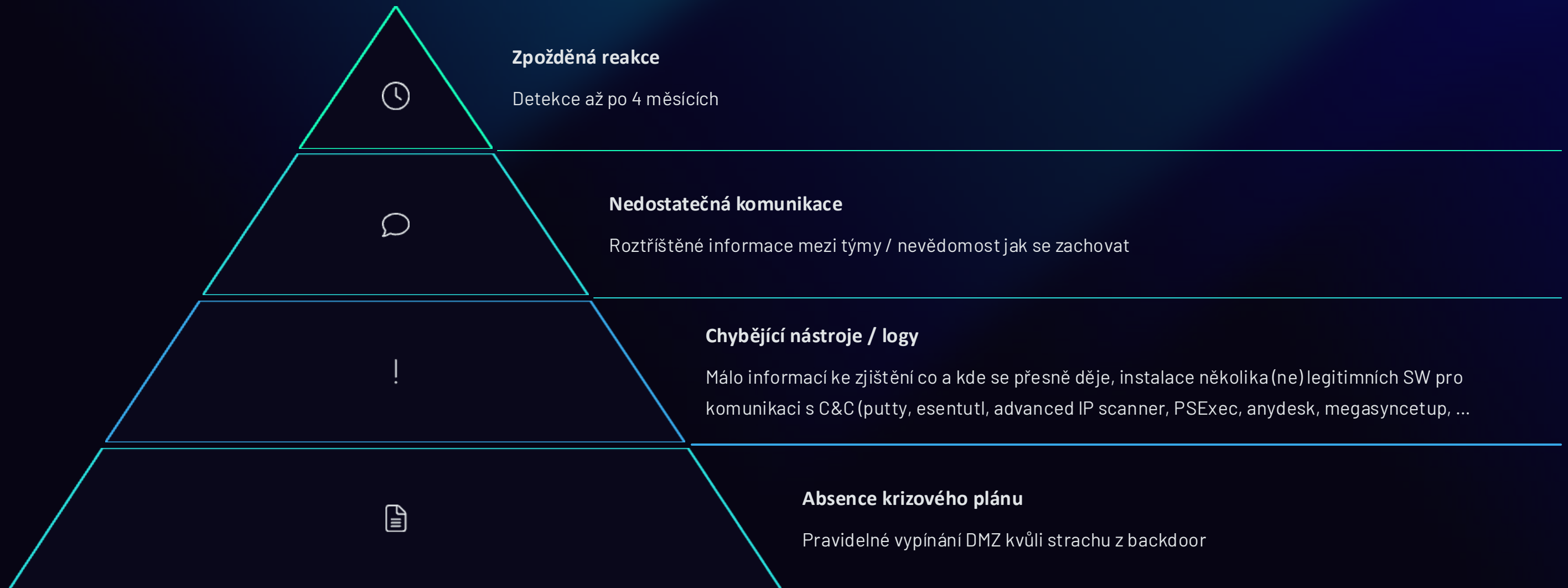


Ohrožené systémy / data

Servery, databáze, firemní data / know-how



Počáteční Reakce a Selhání



Průběh kybernetického útoku



1

Vstupní bod

Zranitelnost ve FortiClient EMS - CVE-2024-47575 / 2023-48788

2

Laterální pohyb

Zneužití síťových oprávnění pro šíření - vlastní AD účet s pravidelnou rotací hesel, hlučné přístupy na RDP / SMB,...

3

Šifrování dat

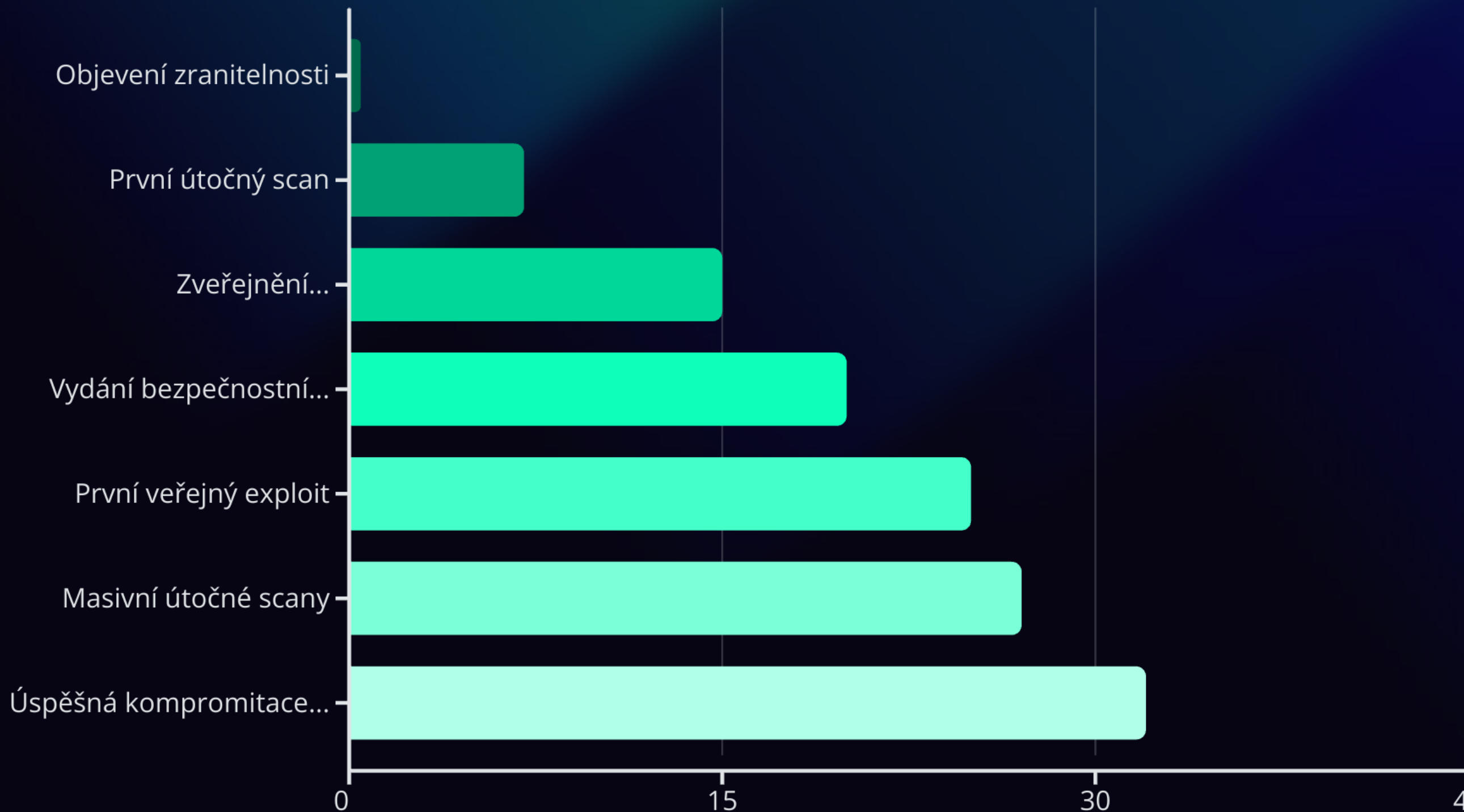
Postupné napadení a zašifrování celé DMZ a exfiltrace dat

4

Požadavek výkupného

30 BTC za dešifrovací klíč

Životní cyklus zranitelností



Životní cyklus skupiny INC Ransom a jejich INC ransomwaru

Analýza evoluce a operačních postupů útočnické skupiny

Průzkumná fáze

Skenování zranitelností a identifikace potenciálních cílů. Skupina INC Ransom typicky využívá automatizované nástroje k vyhledávání nezabezpečených systémů a zastaralého software.

Laterální pohyb

Pohyb napříč sítí, eskalace oprávnění a vytvoření persistentního přístupu. Tato fáze často trvá několik týdnů, během kterých útočníci mapují síť a aktiva.

Nasazení ransomwaru

Šifrování dat pomocí INC Ransomware, který využívá silné šifrovací algoritmy a distribuované šifrování pro maximální dopad. Typicky útočí mimo pracovní hodiny.

Vývoj taktik

Neustálá adaptace na nové bezpečnostní opatření. Skupina pravidelně aktualizuje svůj malware a mění taktiky pro obcházení detekce.



Počáteční průnik

Využití zranitelností v zabezpečení nebo phishingových kampaních k získání přístupu do systému. INC Ransom často používá zranitelnosti ve VPN branách a vzdálených přístupech.

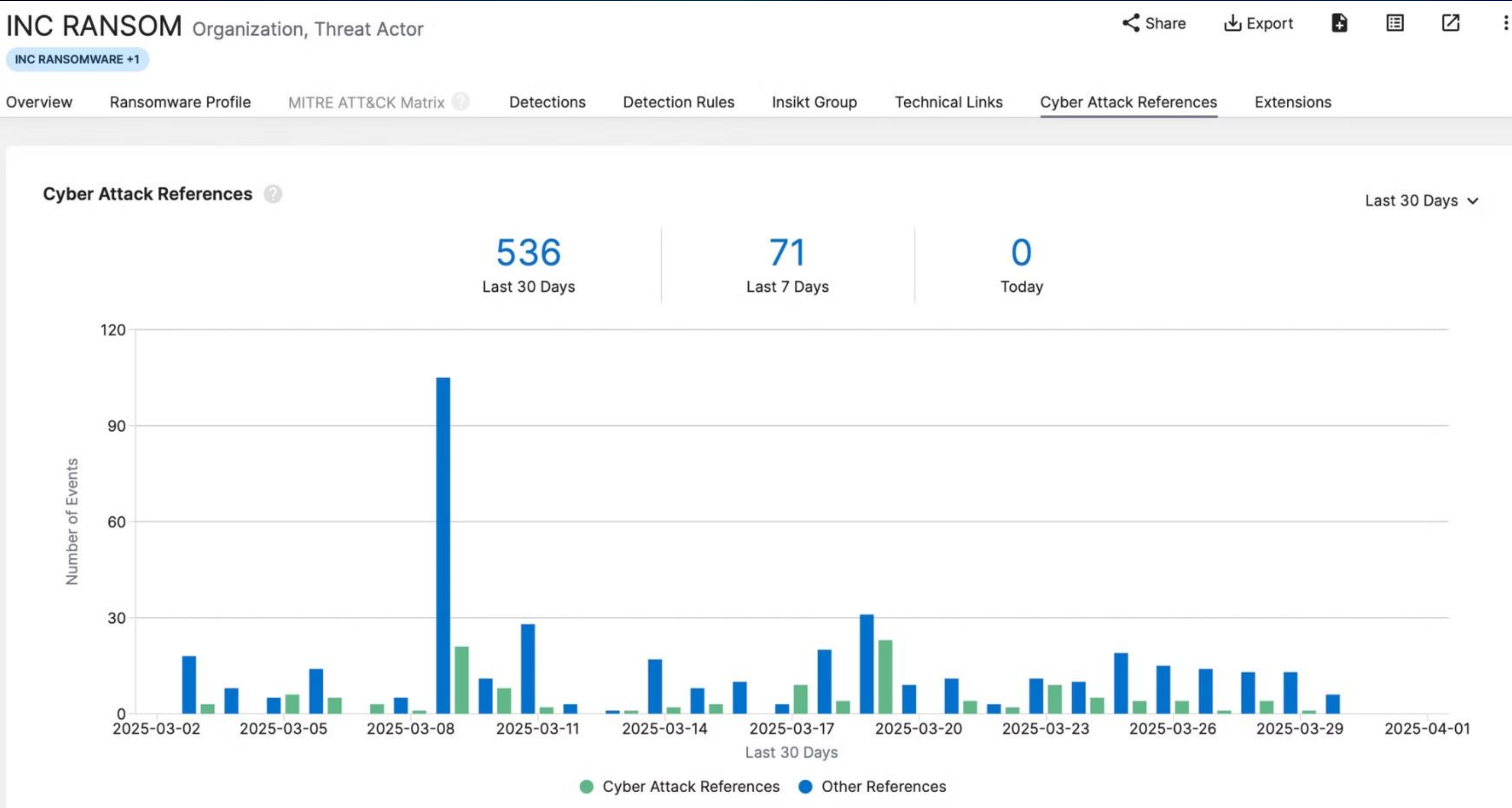
Exfiltrace dat

Krádež citlivých dat před zahájením šifrování. INC Ransom je známý tím, že ukradená data používá pro dvojí vydírání - hrozba zveřejnění a zašifrování.

Vydírání a vyjednávání

Požadavek výkupného (obvykle 10-50 BTC) a komunikace přes šifrované kanály. INC Ransom je známý svou "profesionální" komunikací a poskytováním důkazů dešifrování.

INC Ransomware se vyznačuje modulární architekturou, která umožňuje přizpůsobení útoku konkrétnímu cíli a efektivní obcházení bezpečnostních řešení specifických pro danou organizaci.



LIST of data for sell [REDACTED]



I would like to inform you that this company [REDACTED] does not worry about the security of its data does not want to pay for its mistakes in the field of cyber security.

We have about 2TB of this company's data in our hands. Including data on the production

[REDACTED] The full list of files is in the attachment.

We are announcing the sale of files of this company to one person. The starting price is \$1,000,000.

For purchase, write to TOX chat.

<https://tox.chat>

Contact TOX ID:

[REDACTED] 1C777AB1494514526595CA77F17A0271096D41AE41F65B9

Klíčové chyby v krizovém řízení



Koordinační chaos

Absence znalostí, komunikace, vnitřních policy, zkušeností jak se chovat pod útokem.



Opožděná izolace

Útočník měl 4 měsíce na vytvoření několika backdoor, nevěnována pozornost i hlučným upozorněním (brute force na RDP, SMB, nmap,...)



Ztráta know-how

Soubory jsou částečně obnoveny ze záloh, ale ztráta know-how / duševního vlastnictví je značná



Ohrožení třetích stran

Spolupracující dodavatelé hlásí ransomware útoky v následujících dnech / týdnech



Očekávaná přijatá nápravná opatření

Bezpečnostní rekonstrukce

Implementace Zero Trust architektury, mikrosegmentace, MFA, ochrana AD, viditelnost

Posílené monitorování

Implementace pokročilé EDR / XDR technologie, log management, centrální konzole správy



Nové krizové protokoly

Jasně postupy s definovanými rolami

Vzdělávací programy

Pravidelná školení pro všechny zaměstnance

Reálná přijatá nápravná opatření

Bezpečnostní rekonstrukce

Změna hesel, četnost, komplexita
Audit AD, mikrosegmentace,
viditelnost

Posílené monitorování

Implementace DLP,
Implementace 3 různých EDR
systémů (signature based, endpoint
vs. server,...)



Nové krizové protokoly

Patch management, penetrační
testy

Vzdělávací programy

Pravidelná školení pro všechny
zaměstnance



Poučení a doporučení

Pravidelná školení

Pravidelná školení zaměřená na rozpoznávání phishingu a bezpečnostních hrozeb.

Školení a analýza postupů pro různé typy kybernetických útoků.

Krizový plán a analýza

- *Start from the bottom*
- Zero Trust
- Jednoduchost, centralizace, detekce
- Vnitřní předpisy (práva, identity, klasifikace dat,...)

Eskalační procedury

Jasně definovaný komunikační řetězec při detekci incidentu.

Automatizované alertovací a exekuční systémy pro okamžitou notifikaci.

Závěr: Budoucnost kybernetické bezpečnosti



Klíčové poznatky

Připravenost je základem úspěšné obrany, ďábel je ukryt v základech / detailech. Incident response plán musí být pravidelně aktualizován a testován – backup umí provést každý, ale recovery? Klasifikace dat ?



Preventivní strategie

Implementace Zero Trust architektury, mikrosegmentace a plného logování minimalizuje dopad průniku. Proaktivní monitoring a detekce hrozeb jsou klíčové. Decentralizace a složitost unavuje obsluhu.



Kontinuální vzdělávání

Pravidelná školení pro zaměstnance o phishingu, sociálním inženýrství a bezpečném chování online. Simulace útoků zvyšují povědomí.



Investice do bezpečnosti

Nasazení pokročilých EDR/XDR detekčních a automatizačních systémů pro detekci a reakci na hrozby v reálném čase. Automatizace bezpečnostních procesů šetří čas, zdroje a pomáhá vyšetřovat. Integrujte!

Lukáš Březina

Chief Technical Officer - Security

TAKTIK, a.s.

TAKTIK, a.s.

Ohradské náměstí 2826/6, 155 00 Praha 5

Czech Republic

M: +420 739 433 600

E: lukas.brezina@taktik.cz

www.taktik.cz