Strategie útočníků v roce 2025 a na co se připravit v roce 2026

Ing. Lubomír Ošmera

Microsoft Security trainer, consultant and red teamer

(MCT, MCSE, CEI, CEH, CND, CARTE, CRTE)

https://www.linkedin.com/in/lubomirosmera/

lubomir@osmera.tech

Lubomirosmera.cz

Hybridlcloudprotection.com

Gopas.cz

Old sins

No only 2025 – unfortunately ☹

Skeleton in the wardrobe

Encryption

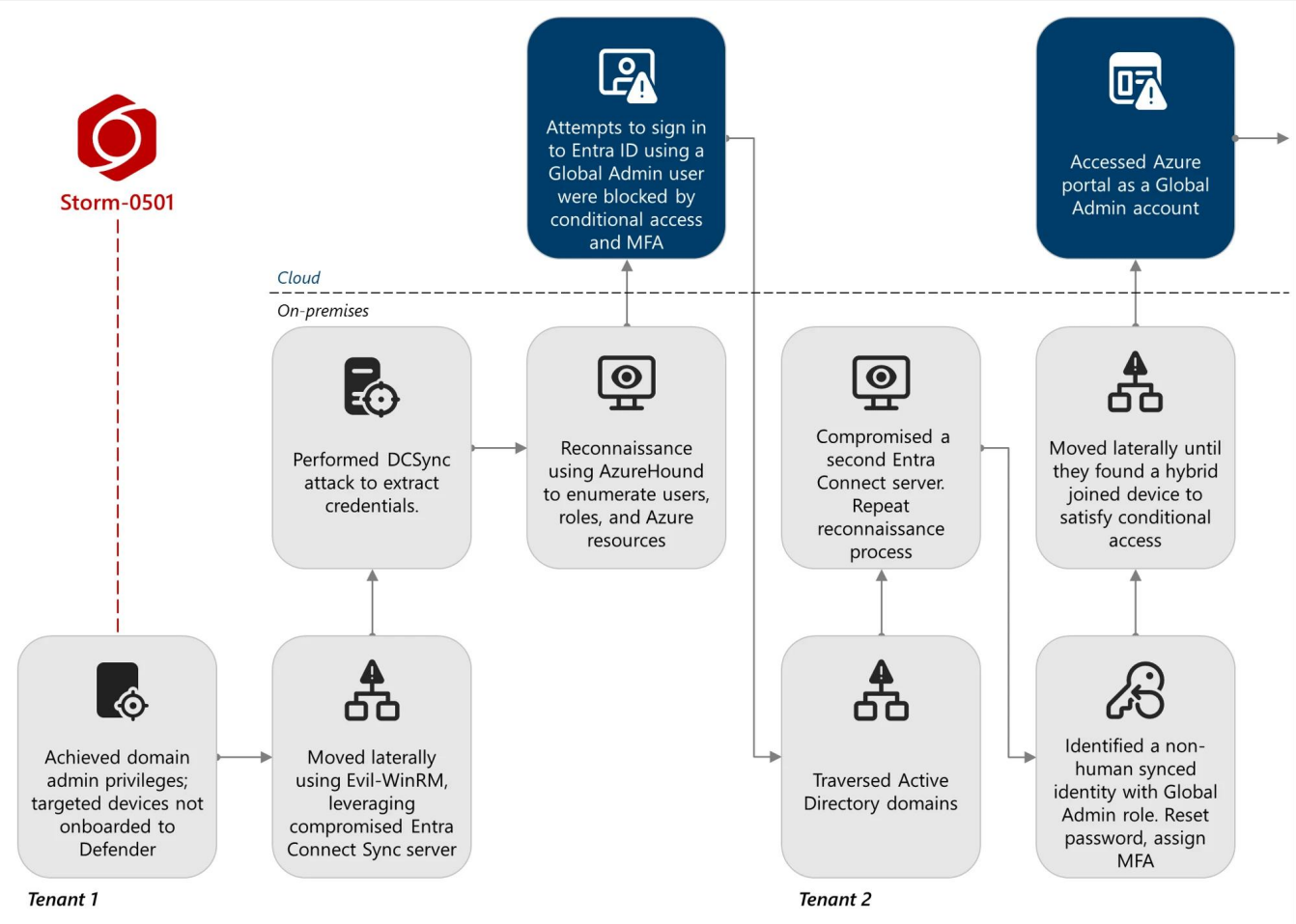
In 42.9% of infrastructures I've assessed, **endpoint drives aren't encrypted.**

Yes — no BitLocker, even in environments with roaming laptops, remote workers, and sensitive data.

I still hear it from admins:
"We're not using BitLocker."
"Never really needed it."
"It's just a laptop."

Horizon Secured research

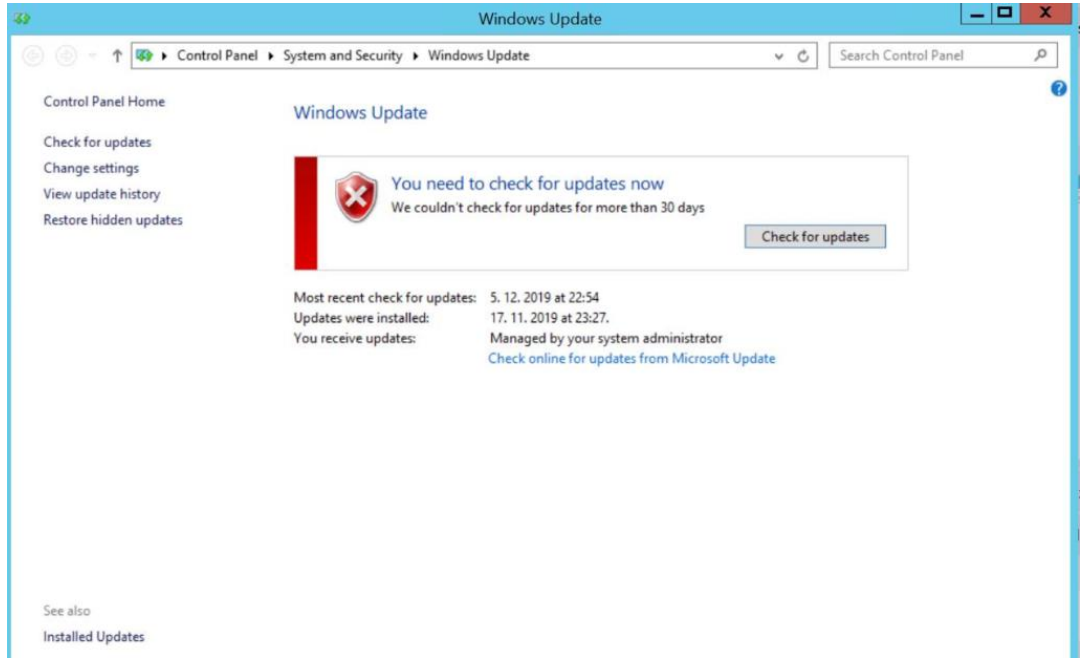
Strong security technologies – only somewhere



Storm-0501's evolving techniques lead to cloud-based ransomware | Microsoft Security Blog

Vulnerabilities

- In the first half of 2025, **23,667 CVEs** were disclosed, representing a significant increase compared to 2024.
- Attackers **actively exploited 161 of these vulnerabilities**, with **42% having publicly available exploit code**.
- Critical servers must have AV, nice to have - EDR, strong hardening



https://www.recordedfuture.com/research/h1-2025-malware-and-vulnerability-trends

ShadowIT, ShadowAI

The State of Shadow AI - Trends, Insights & Statistics | UpGuard

UpGuard

increasing within workplaces. Organisations are aware of the threat, but the traditional security playbook is proving inadequate, leaving leaders uncertain about how to address the problem.

Our definitive report built on survey responses from 500 security leaders and 1,000 employees across the globe, reveals the human nature driving this invisible, systemic threat:

- **Usage is widespread**: 81% of employees and 88% of security leaders report using unapproved AI tools, indicating that the issue is systemic across the enterprise.
- **Blocking fails**: 45% of workers find workarounds to access blocked applications, showing that the restriction only compromises visibility.
- **Knowledge increases risk**: Even with 40% of employees recalling AI training, 40% still use unapproved tools on a daily basis. Our study found that training fails to prevent high-frequency risks and may instead be fueling overconfidence in AI, leading to an increase in employees sidestepping controls.
- **Trust is eroding**: 24% of employees trust AI tools more than their managers or colleagues, indicating a shift in trust from human relationships to technology.

Our data highlights the necessity for a new approach focused on visibility, strategic guardrails, and user empowerment. Read the report to understand why your current security playbook is failing and what strategic imperatives must guide your shift.

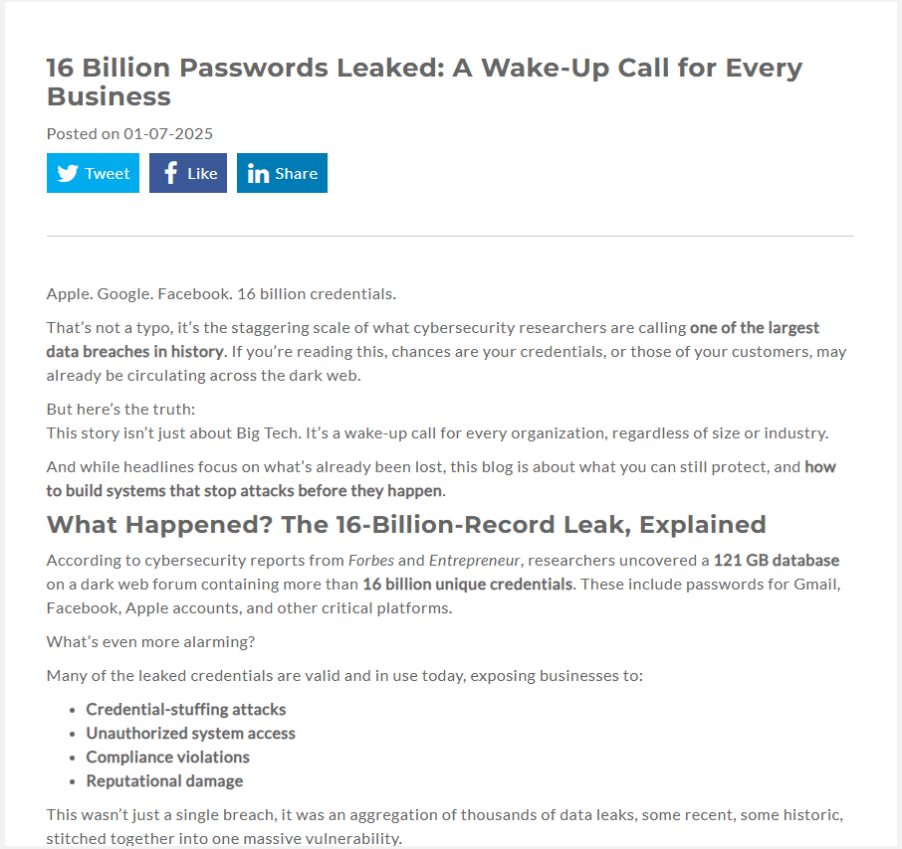
Iot, OT

Incident / Metric	Description / Outcome	Notes / Source
Global number of IoT devices	~18 billion connected IoT devices worldwide	Estimated number of IoT devices in operation
BadBox 2.0 botnet – infected devices	Over 10,000,000 IoT devices (smart TVs, projectors, infotainment systems, etc.)	Largest known IoT botnet identified in July
BadBox 2.0 attack types	Click fraud, account hijacking, residential proxy services, DDoS attacks	Broad impact on network performance and online services
Matrix botnet – scale	Global botnet composed of compromised IoT devices	Exploited known vulnerabilities (Mirai-based) to launch DDoS attacks
Raptor Train botnet – compromised devices	More than 200,000 devices worldwide	Historical incident included for IoT threat landscape context
Mars Hydro exposure incident	Exposure of 2.7 billion IoT-related records due to misconfiguration	Demonstrates systemic weaknesses in IoT data security
Roku account compromises	576,000 compromised user accounts (second incident)	Highlights growing attacks against consumer IoT ecosystems
Overall IoT risk trend	IoT devices increasingly targeted due to weak security controls	Threats continue to escalate as IoT adoption expands

https://asimily.com/blog/the-top-internet-of-things-iot-cybersecurity-breaches-in-2025/

Passwords

Leaked passwords, duplicates



16 Billion Passwords Leaked: A Wake-Up Call for Every Business

Posted on 01-07-2025

Tweet Like Share

Apple. Google. Facebook. 16 billion credentials.

That's not a typo, it's the staggering scale of what cybersecurity researchers are calling **one of the largest data breaches in history**. If you're reading this, chances are your credentials, or those of your customers, may already be circulating across the dark web.

But here's the truth:
This story isn't just about Big Tech. It's a wake-up call for every organization, regardless of size or industry.

And while headlines focus on what's already been lost, this blog is about what you can still protect, and **how to build systems that stop attacks before they happen**.

What Happened? The 16-Billion-Record Leak, Explained

According to cybersecurity reports from *Forbes* and *Entrepreneur*, researchers uncovered a **121 GB database** on a dark web forum containing more than **16 billion unique credentials**. These include passwords for Gmail, Facebook, Apple accounts, and other critical platforms.

What's even more alarming?

Many of the leaked credentials are valid and in use today, exposing businesses to:

- **Credential-stuffing attacks**
- **Unauthorized system access**
- **Compliance violations**
- **Reputational damage**

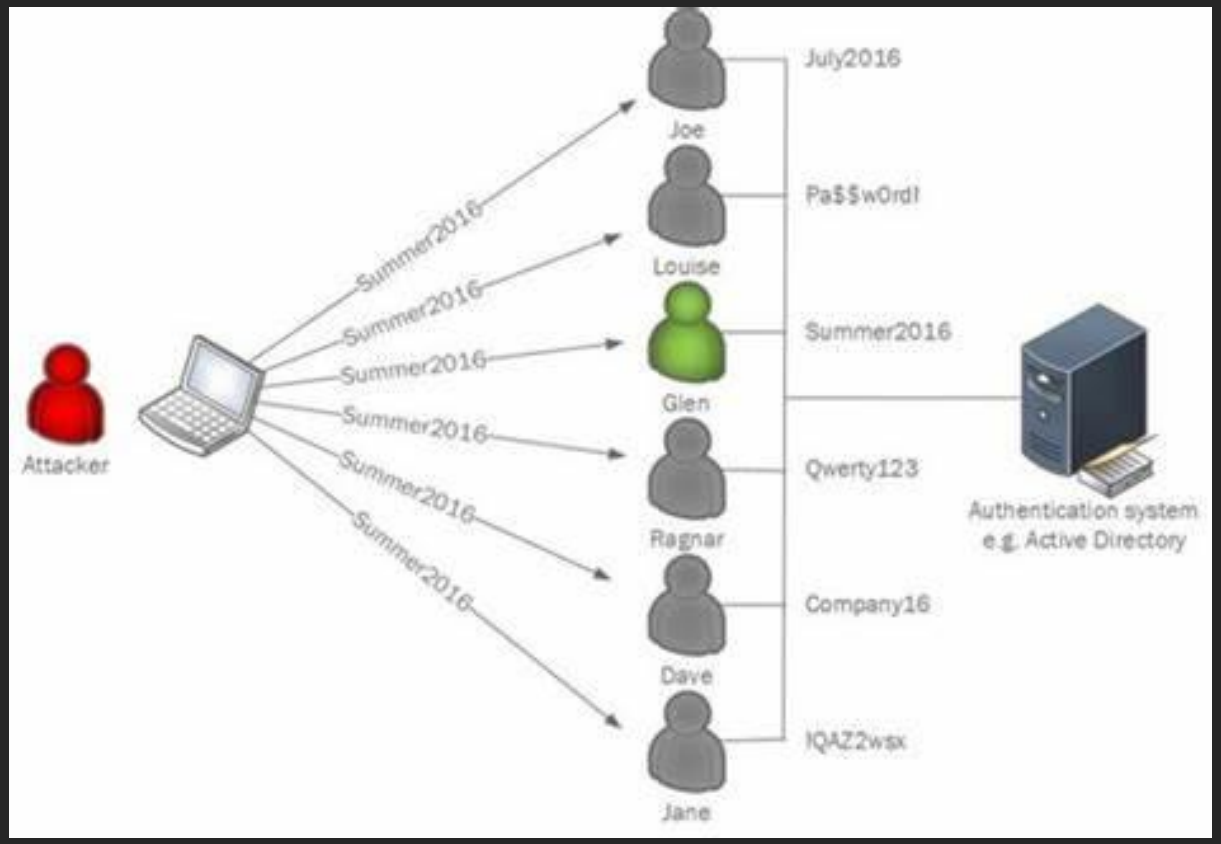
This wasn't just a single breach, it was an aggregation of thousands of data leaks, some recent, some historic, stitched together into one massive vulnerability.

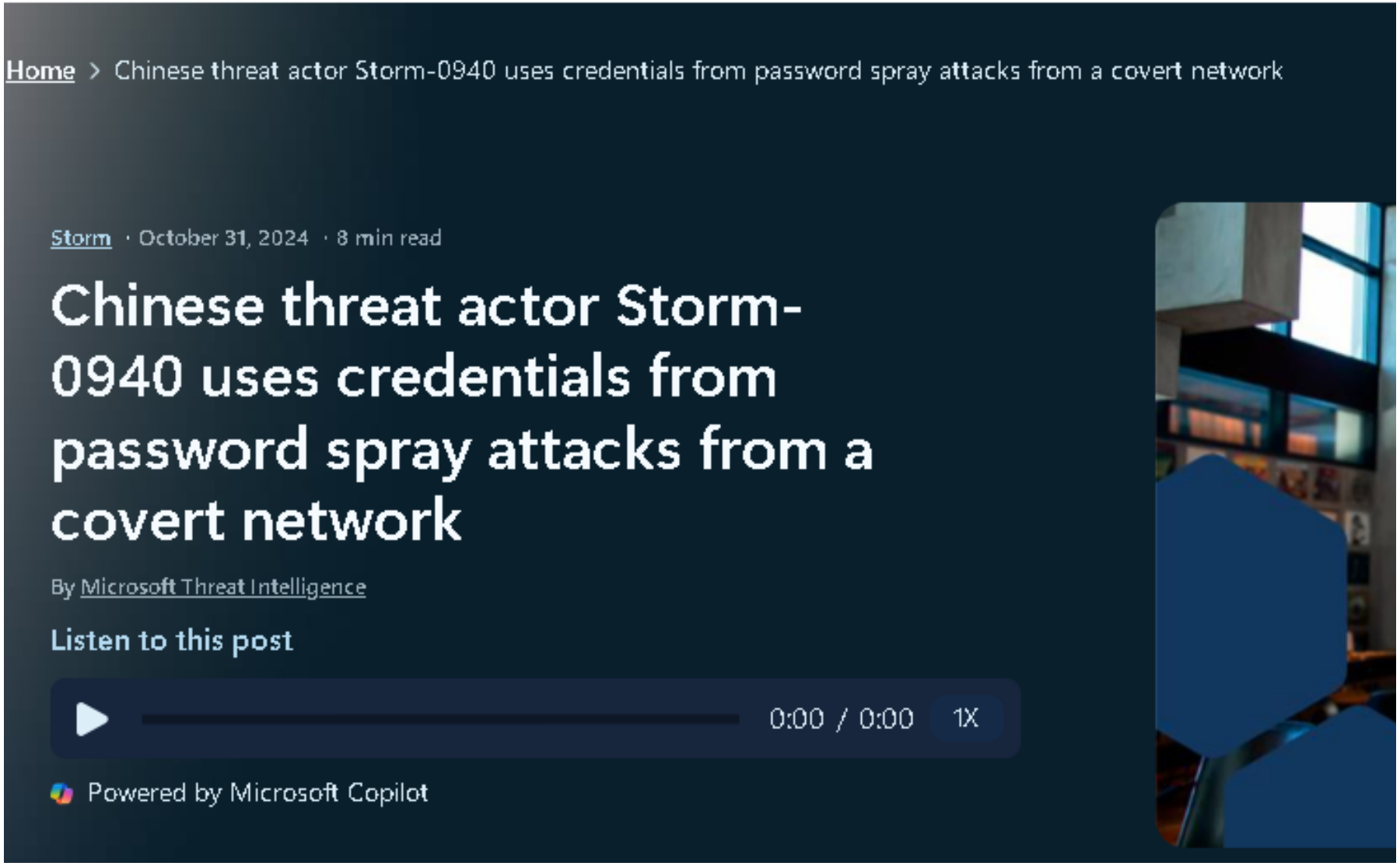
16 Billion Passwords Leaked: A Wake-Up Call for Every Business - VigiTrust

Passwords interesting examples

- Jak jedno špatné heslo položilo 158 let starou firmu | SecurityCast 300
- Jak to opravdu bylo s heslem ke kamerám v Louvre? | SecurityCast 304

Initial access – password spray





https://www.microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/

Forbes

INNOVATION › CYBERSECURITY

Microsoft Password Spray And Pray Attack Targets Accounts Without 2FA

By Davey Winder, Senior Contributor. Davey Win... Follow Autl

Published Feb 25, 2025, 06:18am EST, Updated Feb 26, 2025, 10:20pm EST

https://www.forbes.com/sites/daveywinder/2025/02/25/microsoft-password-spray-and-pray-attack-targets-accounts-without-2fa/?utm_source=chatgpt.com

https://www.portnox.com/blog/cyber-attacks/spray-and-pray-botnet-takes-aim-at-microsoft-365/

DIVE BRIEF

Attackers wield password-spray attacks to zero-in on targets, research finds

The highly effective brute-force attack method requires little effort, Trellix said. Organizations with weak password policies or no MFA are especially at risk.

https://www.cybersecuritydive.com/news/password-spray-attacks-targeted/733460/?utm_source=chatgpt.com

Published Nov. 20, 2024

MFA?

- **Attacker know what is the correct password!**
- Probably MFA is not everywhere – consider RD gateway, VPN, onprem AD, Citrix, ERP systems

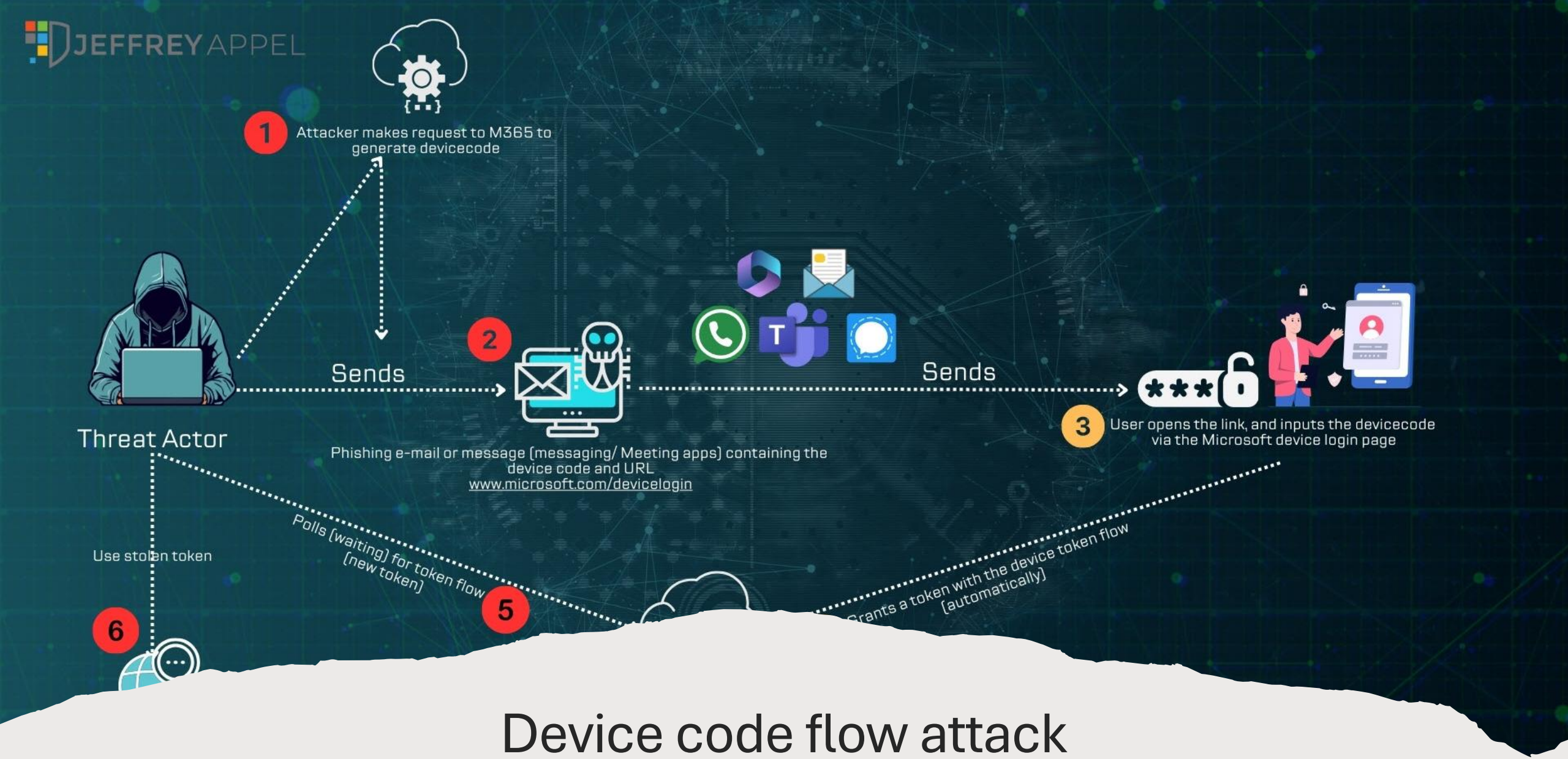
Passwordless – invincible?

Strong authentication – phishing resistant authentication

Phishing resistant – weakness?

Do you know common examples?

https://trickbd.com/tricks/813565



Device code flow attack

Reference: https://jeffreyappel.nl/wp-content/uploads/2025/02/Device-Phishing-Flow-MS-1.jpg

As threats evolve, Microsoft might update these policies to use new features, functionality, or improve their effectiveness

- Block all high risk agents from accessing all resources (Preview)
- Block legacy authentication
- Block device code flow
- Multifactor authentication for admins accessing Microsoft Admin portals
- Multifactor authentication for all users
- Multifactor authentication for per-user multifactor authentication users
- Multifactor authentication and reauthentication for risky sign-ins

2025 – tenant wide policies rollout from MS

https://learn.microsoft.com/en-us/entra/identity/conditional-access/managed-policies

Social engineering

Všeobecná zdravotní pojišťovna ČR

Důležité: Platba nebyla úspěšná

Vážený zákazníku,

Během pokusu o zpracování Vaší poslední platby jsme narazili na problém. Vaše platební metoda byla odmítnuta naším systémem.

Aktualizujte prosím své platební údaje, abychom mohli pokračovat v poskytování služeb bez přerušení.

Aktualizovat platební údaje

Upozornění: Ujistěte se, že Vaše bankovní údaje jsou aktuální a správné. V opačném případě může dojít k dalšímu zpoždění plateb.

S pozdravem,
Všeobecná zdravotní pojišťovna ČR

https://www.vzp.cz/o-nas/aktuality/nova-vlna-podvodu-kybersmejdi-opet-utoci-pres-e-maily#:~:text=%E2%80%9ETento%20podvod%20je%20velmi%20dob%C5%99e,%C5%99editel%20Odboru%20bezpe%C4%8Dnosti%20VZP%20%C4%8CR

Upomínka: Neuhrazená daň za rok 2024 – výzva k úhradě do 5 dnů

FS Finanční Správa <info@financni-zprava.cz>
Komu [redacted]

Odpovědět | Odpovědět všem | Přeposlat | ...

st 18.06.2025 9:42

Vážený poplatníku,
evidujeme u Vás **neuhrazenou daňovou povinnost za zdaňovací období roku 2024** ve výši **720 Kč**.

Podle § 251 daňového řádu jste povinen/povinna provést úhradu nejpozději do **5 pracovních dnů** od doručení této výzvy. V opačném případě bude částka navýšena o zákonný úrok z prodlení.

Detaily k platbě a možnosti úhrady naleznete na následujícím odkazu:
Zobrazit detail daňové povinnosti a zaplatit online

S pozdravem,
Finanční správa České republiky
Odbor daňové správy
Tento e-mail byl generován automaticky. Na tuto zprávu neodpovídejte.

F. FINANČNÍ SPRÁVA

https://financnisprava.gov.cz/cs/financni-sprava/media-a-verejnost/tiskove-zpravy-gfr/tiskove-zpravy-2025/financni-sprava-upozornuje-na-dalsi-vlnu-podvodnych-zprav#:~:text=v%C3%BDzvy%20k%C2%A0%C3%BAhrad%C4%9B%20dan%C4%9B%20a%C2%A0zneu%C5%BE%C3%ADvaj%C3%AD%20jm%C3%A9no,i%C2%A0logo%20finan%C4%8Dn%C3%AD%20spr%C3%A1vy

Od: **Česká Pošta Sledování Zásilek <cpost@ceskaposta.net>**
Předmět: Naléhavě NETservis s.r.o., Informace o Vaší zásilce
Datum: 8. srpna 2013 13:49:06 GMT+02:00
Komu: NETservis s.r.o.
Odpověď na: Česká Pošta Sledování Zásilek <cpost@ceskaposta.net>

NETservis s.r.o.,

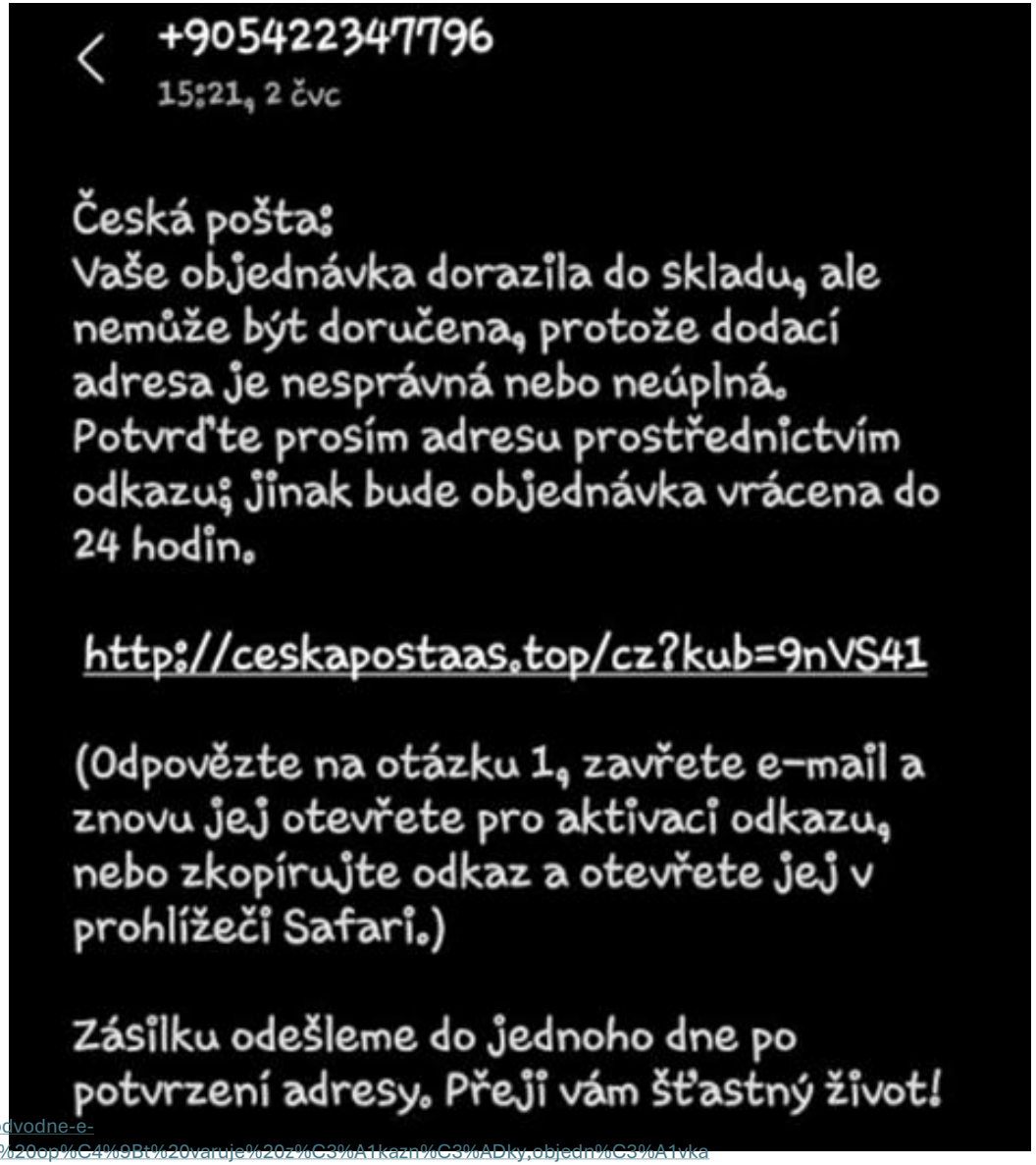
Kurýr nevydal zásilku s podacím číslem **DR6878456545C**, na Vaši adresu 05.8.2013, protože nikdo nebyl na adrese v tomto okamžiku. Prosím, podívejte se na informace o zásilku , vytisknout a jít na poštu dostávat balíček.

http://www.ceskaposta.cz/cz/nastroje/sledovani-zasilky.php

Pozor

Pokud je zásilku nedostali do 30 pracovních dnů Česká pošta bude mít právo nárokovat odškodnění od tebe jde o to udržet ve výši 45 Kč za každý den udržet. Zde najdete informace o postupu a podmínkách parcely vedení v nejbližší pobočce. Děkujeme, že využíváte naše doručovací služby. S přáním příjemného dne Vaše Česká pošta

Telefonicky : 840 111 244



https://www.ceskaposta.cz/o-ceske-poste/aktualni-podvodne-e-maily#:~:text=%C4%8Cesk%C3%A1%20po%C5%A1ta%20op%C4%9Bt%20varuje%20z%C3%A1kazn%C3%ADky,objedn%C3%A1vka%20vr%C3%A1cena%20do%2024%20hodin

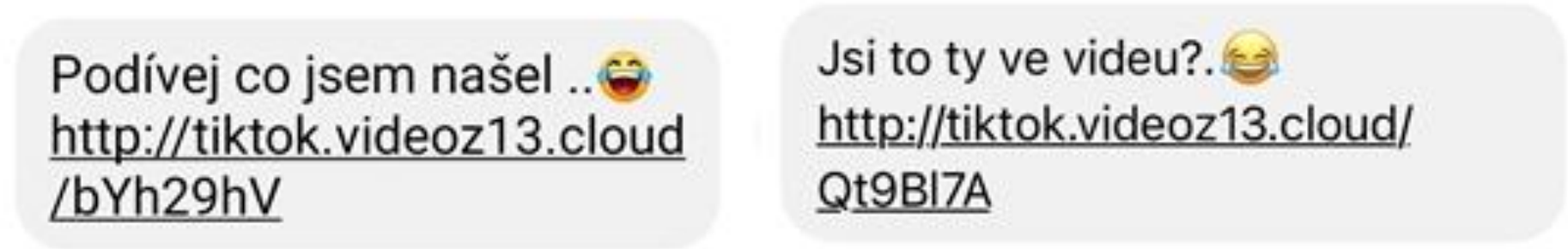
TELEFONÁTY OD POLICISTŮ NEBO FALEŠNÝCH BANKÉŘŮ

Nejinak tomu bylo i tentokrát v jednom případu na Nymbursku.
Poškozenou 56letou ženu koncem února telefonicky kontaktovalo neznámé číslo, kdy se do telefonu ozvala neznámá žena, která poškozenou informovala o tom, že si pod její identitou chtěla vzít neznámá žena na její osobu úvěr ve výši 250 tisíc korun na pobočce v Pardubicích. Vzhledem k tomu, že toto jednání bylo podezřelé, měla následně poškozenou přepojit na pracovníka bezpečnosti. Ten údajně zjistil, že někdo nahlížel do osobního účtu poškozené a připojil k němu nové telefonní číslo a zřejmě tedy poškozené ukradl bankovní identitu. Aby žena o své peníze nepřišla, měla bankéři sdělit, jakými bankovními účty disponuje, aby bylo možné finanční prostředky na těchto účtech zachránit. Tímto způsobem pak podvodník zjistil, že žena disponuje nejen vlastním bankovním účtem, ale i účtem firemním, jelikož pracuje jako účetní na jedné ze škol na Nymbursku.

Žena se pak podle pokynů měla přihlásit na internetové stránky, kde se měla přihlásit ke zmíněným účtům a peníze převést na zabezpečený rezervní účet, což žena ze strachu o své i firemní peníze udělala. Dle pokynů pak začala posílat peníze na „zabezpečené účty" a takto přeposílala platby ve vyšších částkách.
Jak je již bohužel v těchto případech obvyklé, podvodníci využívají různé taktiky, aby svou oběť znejistili a vyvolali v ní pocit, že jsou její peníze v nebezpečí a pak nabízejí pomoc s převodem na bezpečný účet nebo vybraní finanční hotovosti, kterou pak poškození mají odevzdat pracovníkovi banky, který jí odveze přímo do banky a uloží na bezpečný účet.

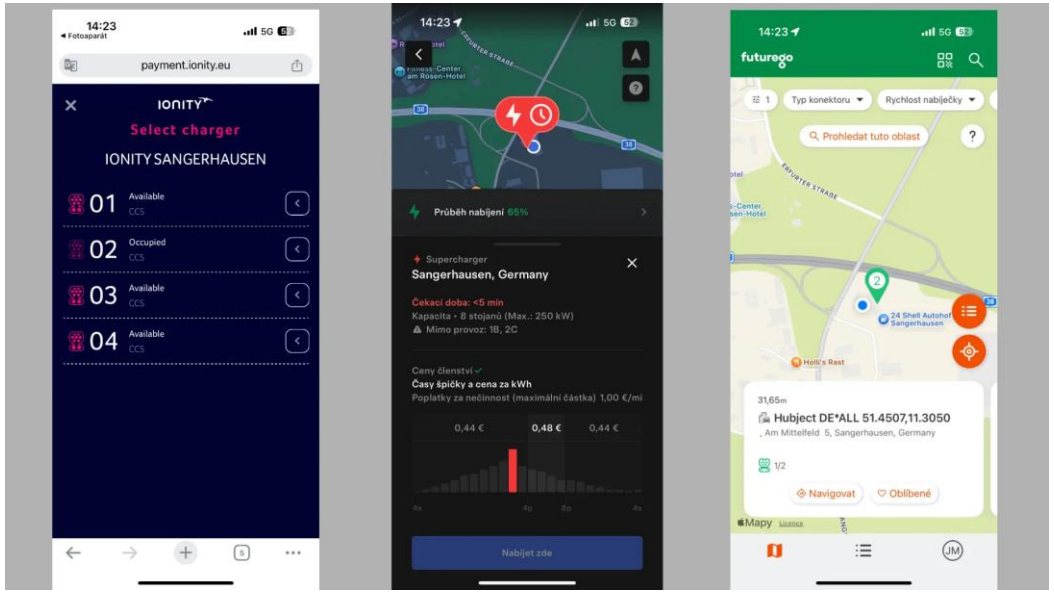
https://policie.gov.cz/clanek/or-nymburk-zpravodajstvi-falesny-banker-opet-na-scene.aspx#:~:text=Po%C5%A1kozenou%2056letou%20%C5%BEenu%20koncem%20%C3%BAnora,T%C3%ADmto%20zp%C5%AFsobem

https://publico.cz/cesko/babis-podvod-kryptomena-nova#:~:text=Pro%C4%8D%20je%20to%20d%C5%AFle%C5%BEit%C3%A9%3A%20Technologie%2C,brzy%20nemus%C3%AD%20sta%C4%8Dit%20ani%20to



PODVODNÁ ZPRÁVA NA MESSENGERU: „JSI TO TY VE VIDEU?“

https://mobilmania.zive.cz/clanky/jsi-to-ty-ve-videu-podvodne-zpravy-se-siri-v-messengeru-chteji-z-vas-vylakat-penize-na-odkazy-neklikejte/sc-3-a-1356911/default.aspx#:~:text=,videu%3F%E2%80%9C%20nebo%C2%A0%E2%80%9EPod%C3%ADvej%2C%20co%20jsem%20na%C5%A1el%E2%80%9C

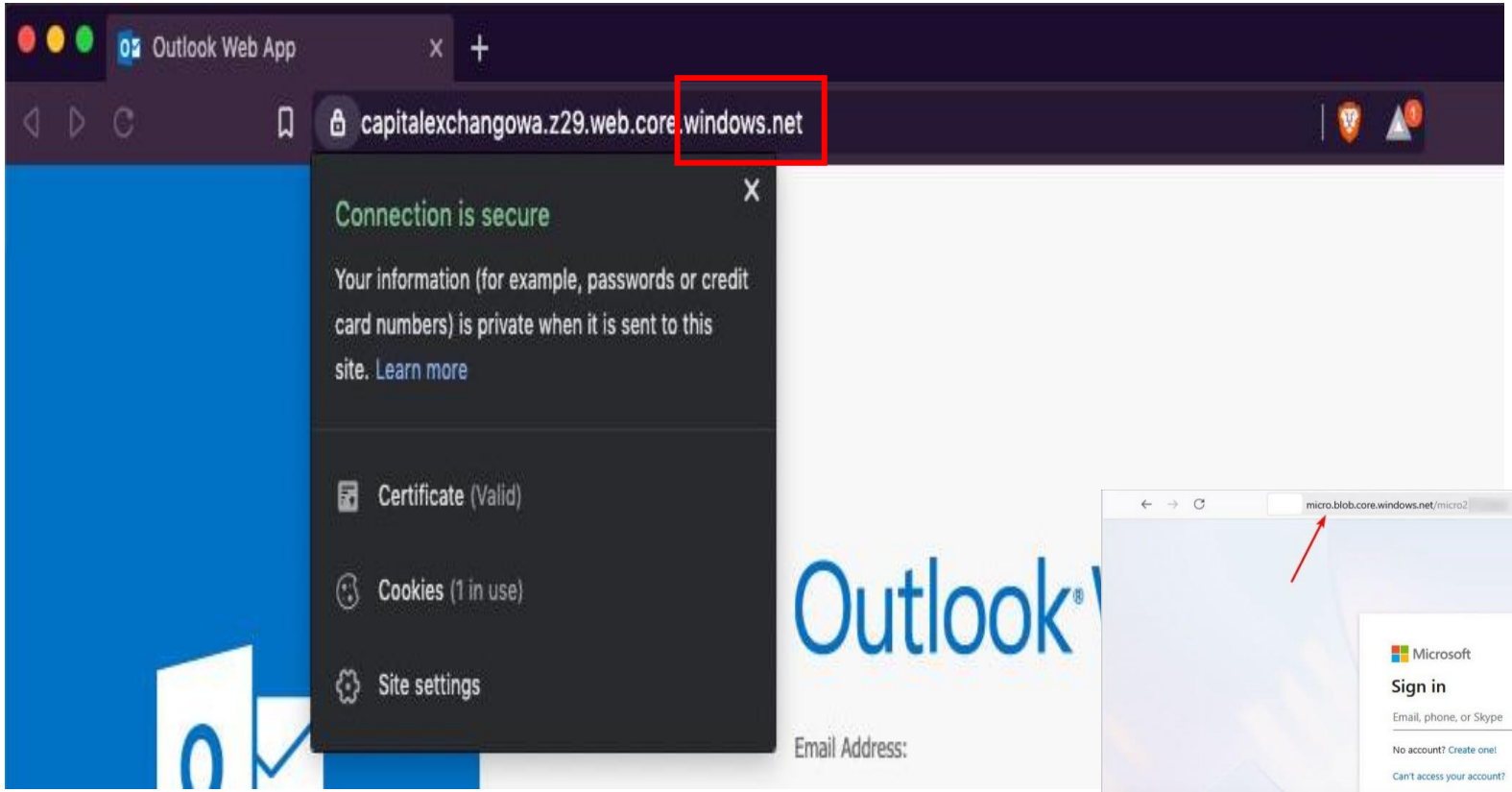


Falešné QR kody

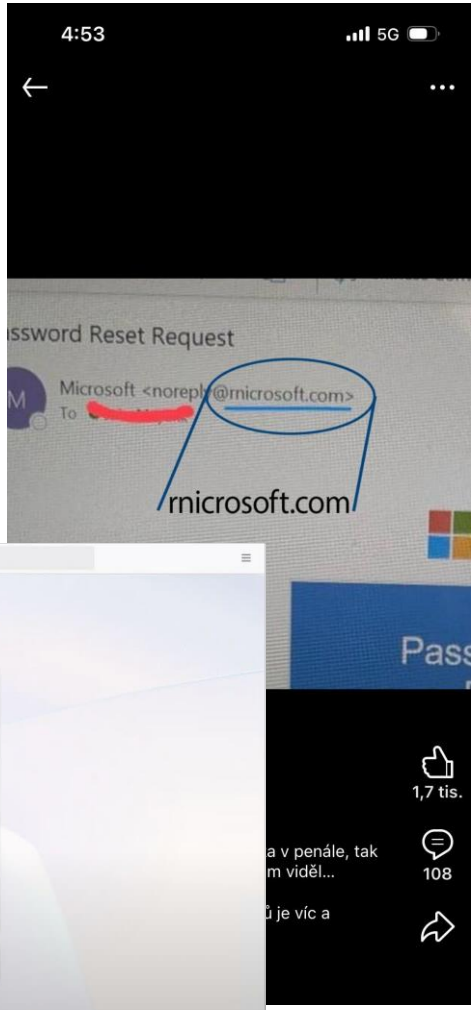
https://www.garaz.cz/clanek/reportaze-je-tady-novy-podvod-jenz-se-zameruje-na-ridice-zejmena-na-ty-kteri-jsou-v-nouzi-nebo-neznali-21015017

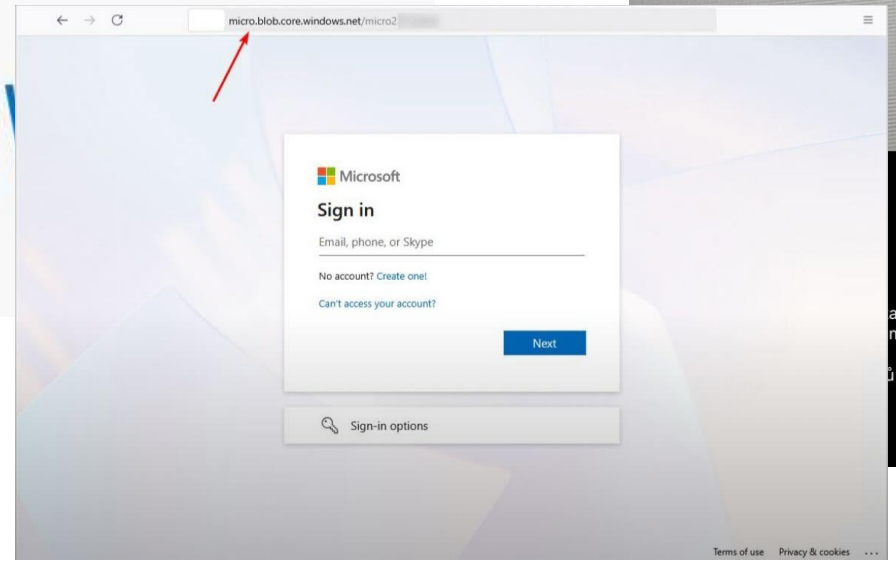
„Correct“ domains

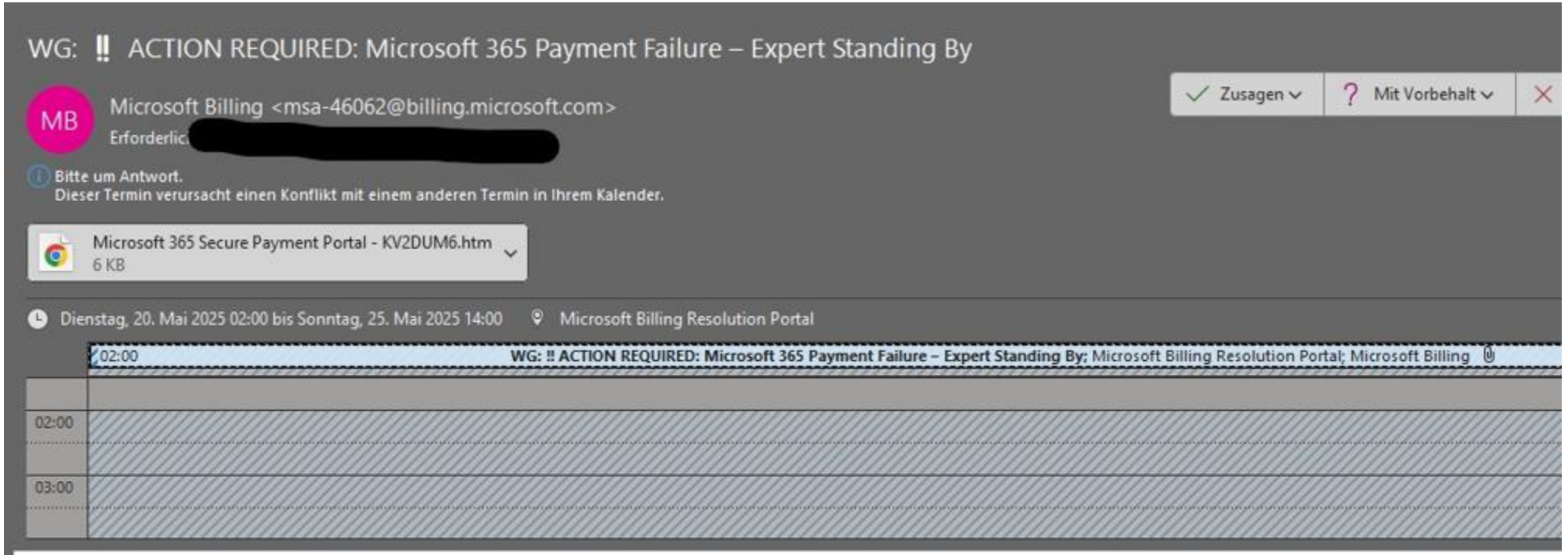
https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide



https://medium.com/proferosec-osm/simple-rules-to-protect-against-spoofed-windows-net-phishing-attacks-714a2e52dd3c







-----Ursprünglicher Termin-----
Von: Microsoft Billing <msa-46062@billing.microsoft.com>
Gesendet: Mittwoch, 21. Mai 2025 14:00
An: Microsoft Billing ; info; Payment Resolution Team
Betreff: ‼ ACTION REQUIRED: Microsoft 365 Payment Failure – Expert Standing By
Zeit: Dienstag, 20. Mai 2025 02:00 bis Sonntag, 25. Mai 2025 14:00 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien.
Ort: Microsoft Billing Resolution Portal

https://borncity.com/win/2025/05/31/phishing-with-appointment-invitations-targets-office-365-accounts/#:~:text=Victims%20are%20asked%20to%20enter,company%20details%20or%20email%20credentials

Vishing

Vishing v roce 2025: Nahrávky jsou minulost, dnes letí klonování reálných hlasů | cdr.cz

AI

AI fully driven malware

https://www.infosecurity-magazine.com/news/chinese-hackers-cyberattacks-ai/

AI attacks, AI stealing

Mladý vývojář v rychle rostoucím fintechovém start-upu se snažil stihnout termín spuštění, a tak zkopíroval API klíč k využívanému jazykovému modelu (LLM) do veřejného repozitáře GitHub.

Během několika hodin ale někdo tento klíč zkopíroval, přidal k dalším a následně na Discordu i prodal kyberzločincům.

Než si technický ředitel zmíněné společnosti všiml podezřelých okolností ohledně využití LLM, vznikla už obrovská škoda: tisíce dolarů v nákladech na navýšený výpočetní výkon jazykového modelu a ztráta důvěrných obchodních dat.

Nejde o žádnou hypotetickou událost – je to souhrn toho, co se opakovaně dělo v první polovině letošního roku.

V lednu 2025 otřásly světem AI úniky dat, které se nepodobaly oněm starým „někdo nechal otevřenou databázi", ale spíše novému druhu kyberútoků. DeepSeek, nový populární jazykový model z Číny, přišel o své klíče a dvě miliardy tokenů zmizely v éteru, kde je útočníci použili ke kdovíčemu.

O několik týdnů později zaznamenal OmniGPT, široce používaný agregátor chatbotů AI, který propojuje uživatele s více jazykovými modely, závažné narušení bezpečnosti, při kterém na veřejnost uniklo více než 34 milionů zpráv uživatelů a tisíce klíčů API.

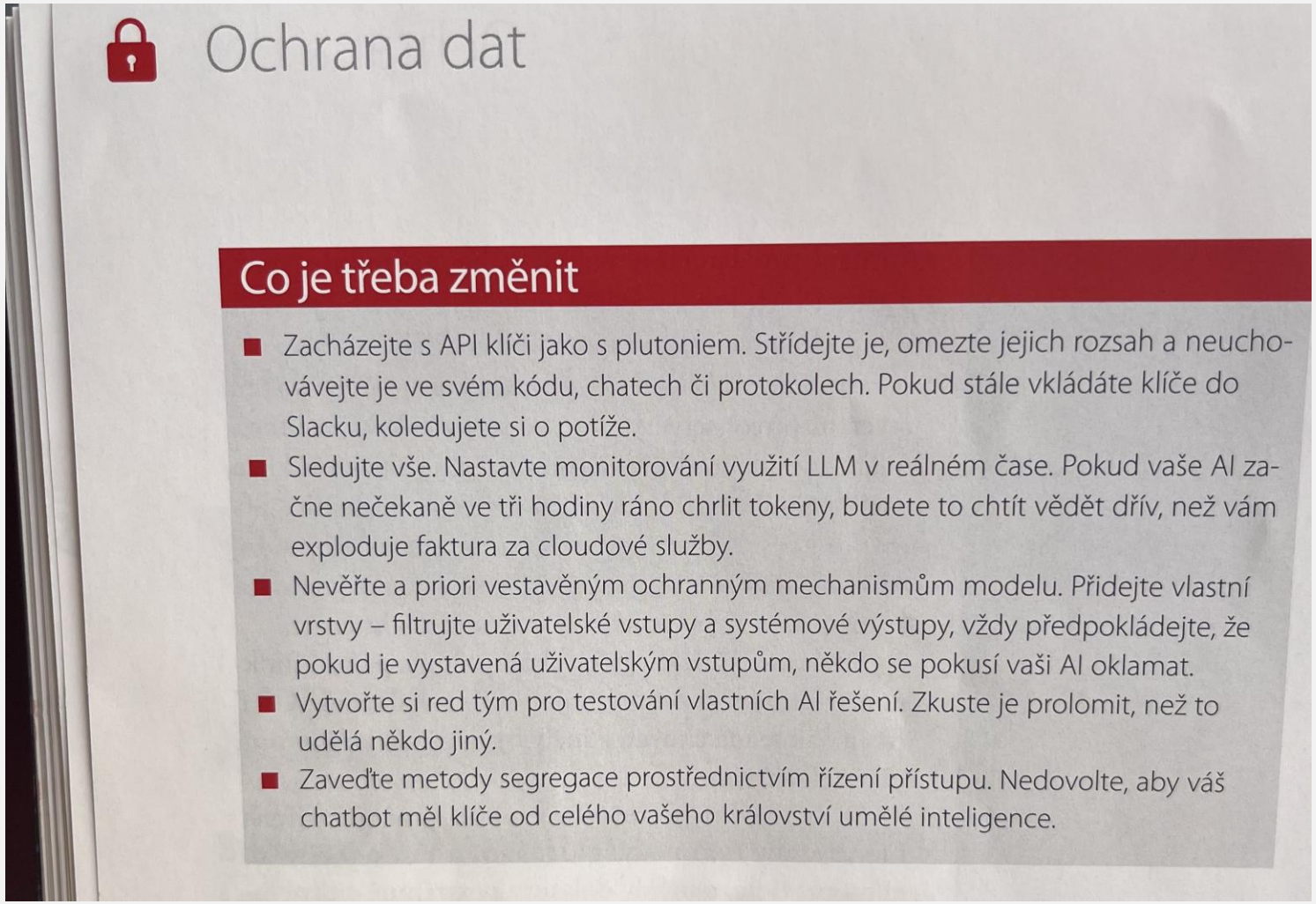
Pokud těmto strojům svěřujete svá data, nyní můžete v reálném čase sledovat, jak tuto důvěru zrazují.

[Se správným promptem mohou útočníci přimět jazykové modely, aby odkryly logiku a pravidla svého fungování a někdy i extrémně citlivé informace.]

Vkrást mysl, ne data

...o léta se firmy obávaly hackerů, kteří kradou soubory ...bo drží získaná data jako rukojmí. Ale únos LLM ...edstavuje něco úplně jiného – něco podivnějšího ...ákeřnějšího. Útočníci jdou p... ...ých „moz-...", které pohánějí va... ...ikat... ...kum, vaše ...lnikání.

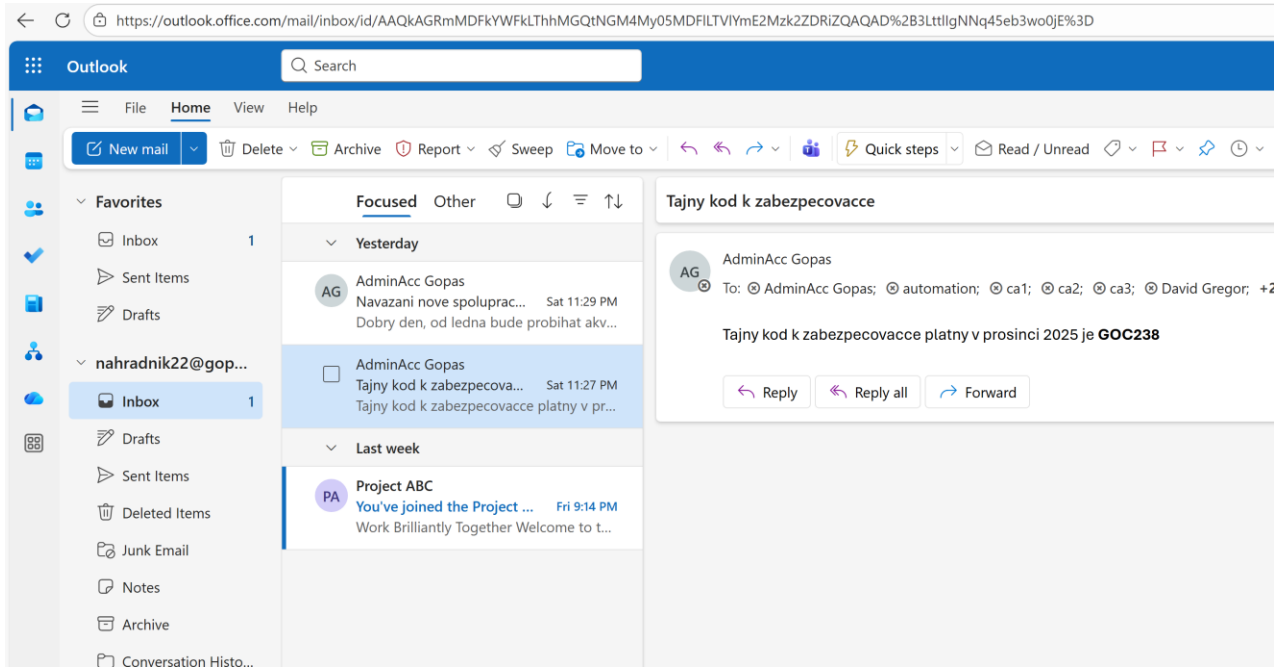
...Prohledávají GitHub, skenují konfigurace cloudu, ...once prohledávají kanály



COMPUTERWORLD 10/2025

AI and spear phishing

Cílení na konkrétní skupinové projekty
•Např. **Project ABC** nebo **Designers** – cílení na spolupráci.
•Phishing email:
•*„Tady je nový návrh projektu ABC, připomínky prosím do konce dne.“*
• 🎯 **Cíl:** Získání přístupu k OneDrive / SharePoint projektům nebo vložení malwaru do projektových souborů.



🧠 **Co útočník z této obrazovky zjistí:**

1. Jméno odesílatele a název účtu:

- **Odesílatel:** `AdminAcc Gopas` – vypadá jako **administrativní nebo technický účet** (pravděpodobně autorita v organizaci).
- To budí důvěru → ideální identita pro spear phishing.

2. Příjemci zprávy:

- Zpráva byla poslána více lidem (ca1, ca2, ca3, ...), což indikuje, že šlo o **hromadné sdělení důvěrného charakteru**.

3. Obsah zprávy:

- „Tajný kód k zabezpečovačce platný v prosinci 2025 je **GOC238**“
- Tohle působí jako **citlivá informace** (např. PIN, přístupový kód, nebo token k zařízení / aplikaci).

4. Jméno příjemce:

- `nahradnik22@...` – dočasný nebo náhradní účet. Útočník může tušit, že jde o méně privilegovaného nebo méně zkušeného uživatele → **snazší cíl**.

🎯 Jak to může být zneužito útočníkem:

✅ 1. Vytvoření důvěryhodného phishing emailu

Útočník může napsat:

> *"Ahoj, posílám ti nový kód k zabezpečovačce, předchozí verze GOC238 expirovala. Nový je přiložen v PDF."*

→ Uživatel otevře PDF → dropper nebo odkaz na phishing web.

✅ 2. Zneužití názvu „AdminAcc Gopas“

Útočník může spoofnout nebo kompromitovat účet a napsat jménem AdminAcc:

> *"V systému jsme zaznamenali nesprávné použití kódu GOC238, klikněte pro reset: [link]."*

→ Cíl klikne a zadá přihlašovací údaje → účet kompromitován.

✅ 3. Zjištění interních zvyklostí

Z emailu lze odvodit:

- Organizace používá "zabezpečovačky" (možná fyzické zařízení nebo bezpečnostní aplikace)
- Hesla/kódy jsou rozesílány e-mailem (!)
- Název kódu má formát (např. GOC + číslo) → útočník může generovat falešné

✅ 4. Vytváření falešného kontextu pro další útok

Například:

> *"Byl vydán nový firmware k zabezpečovačce, je třeba jej nainstalovat a zadat kód GOC238 pro aktivaci."*
> *"Klikni zde pro stažení bezpečnostního asistenta."*

→ Přílohou může být malware s názvem např. `SecureUpdate_GOC238.exe`

LOLBAS TREND

LOLBAS

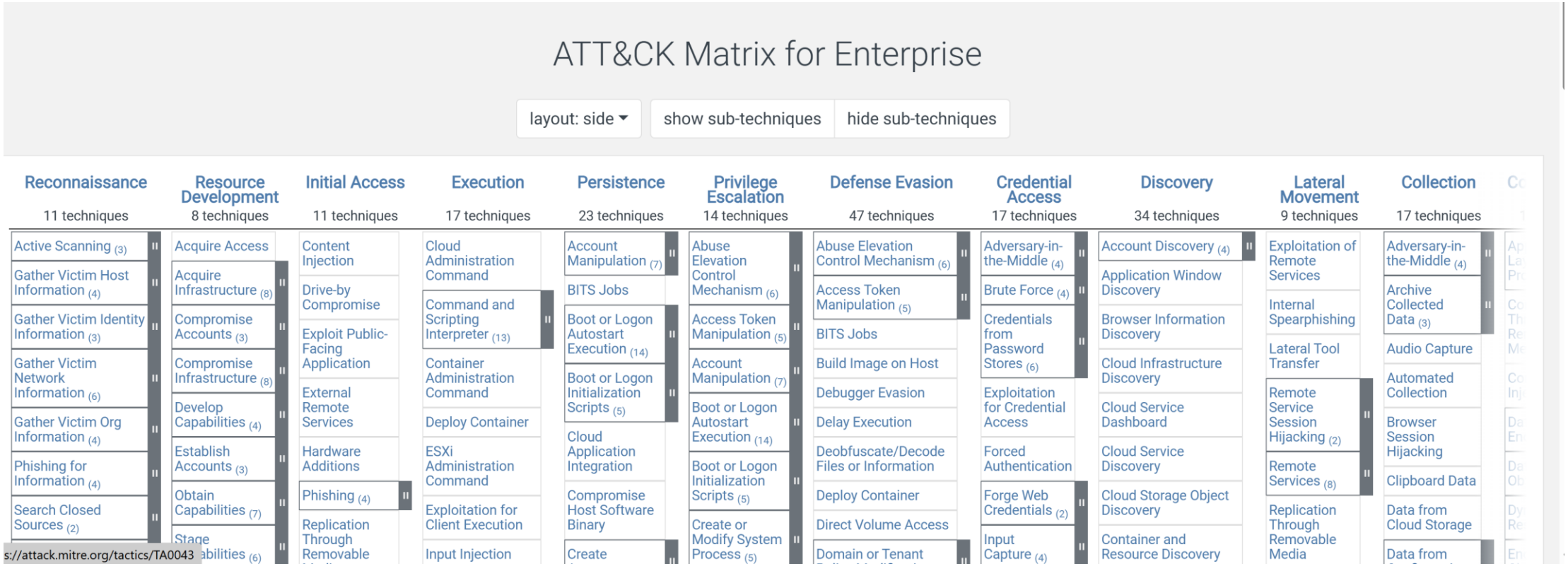
It takes two: The 2025 Sophos Active Adversary Report | SOPHOS

Bitlocker ransomware

https://www.seqrite.com/blog/bitlocker-ransomware-attack-defense/

Detection

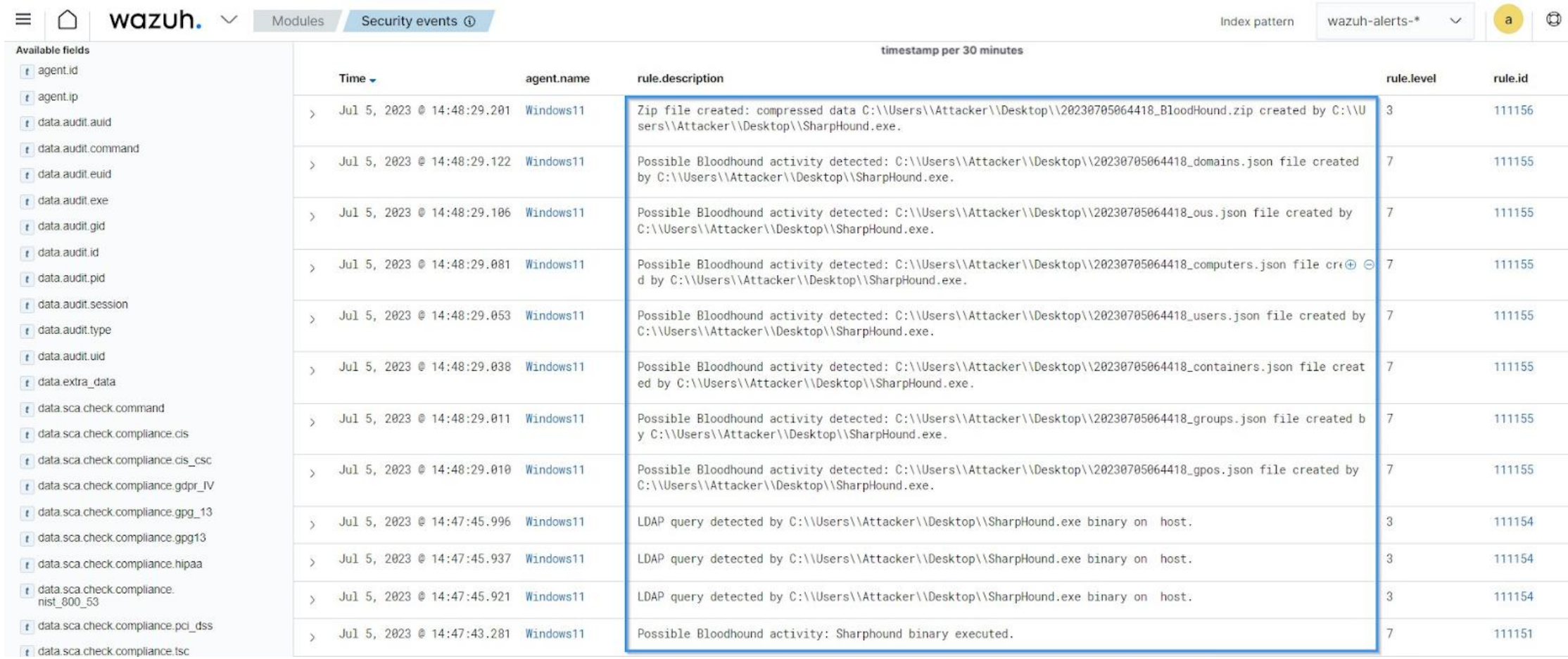
Where detection needs to be strengthened?



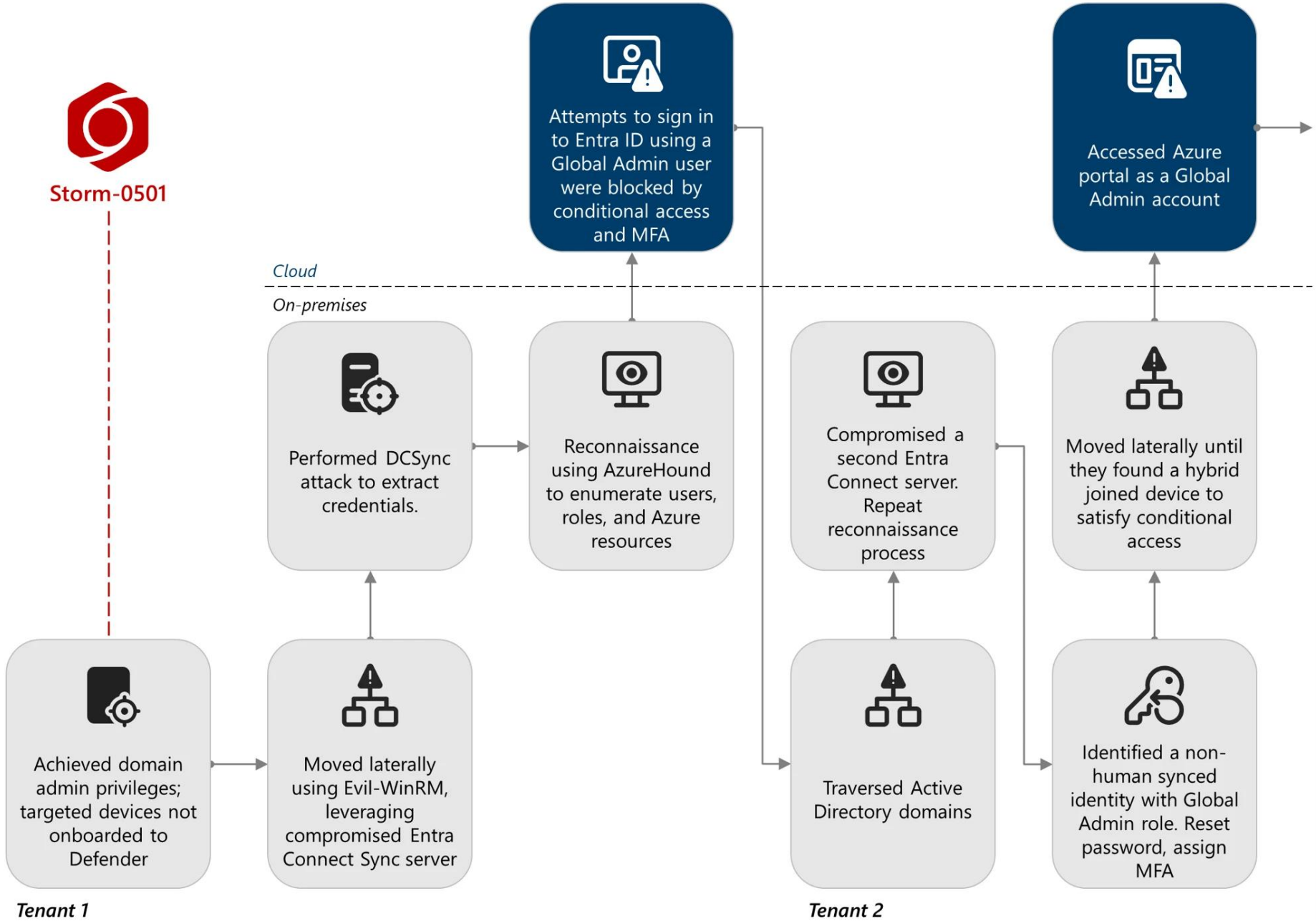
https://attack.mitre.org

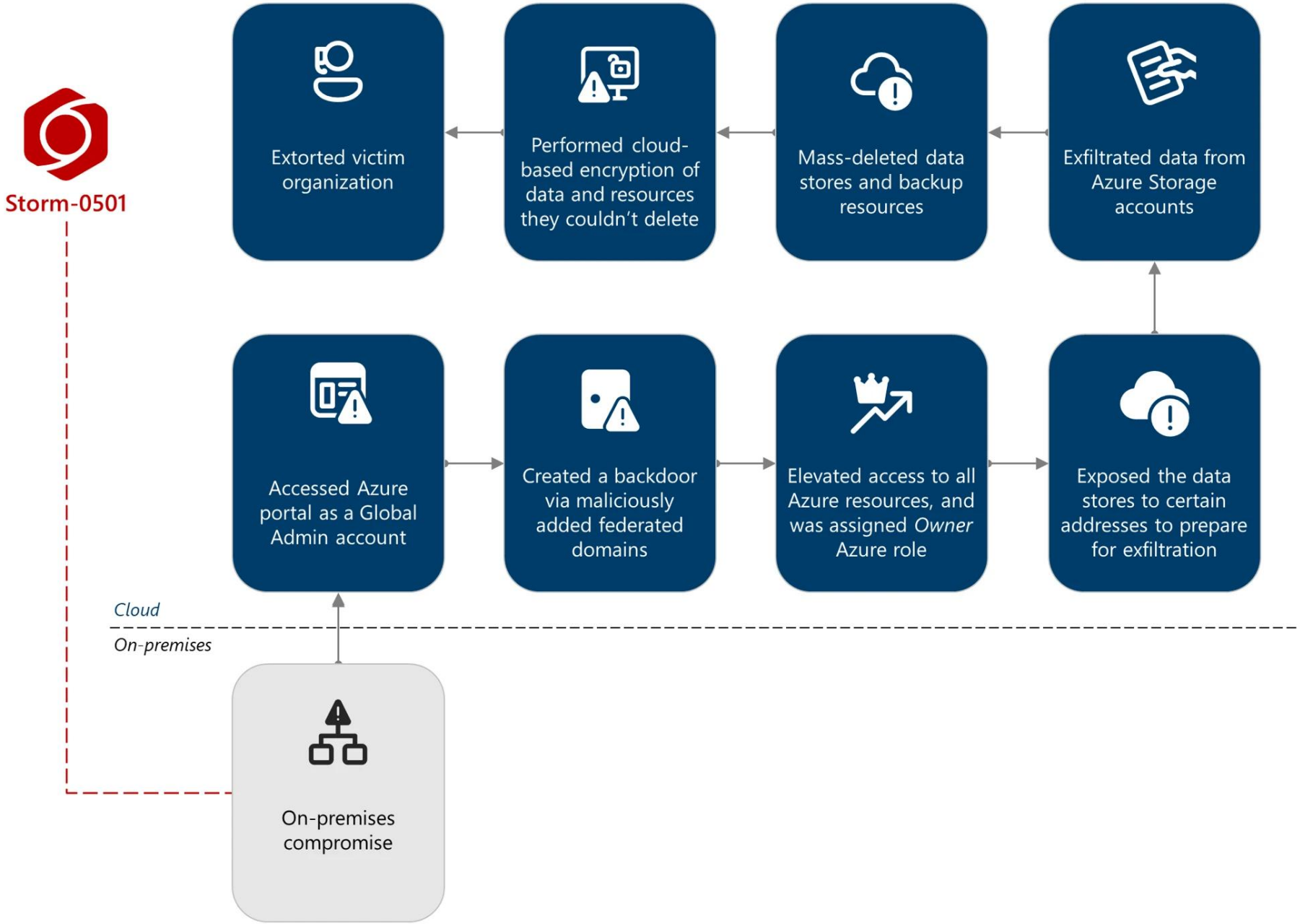
Reconnaisance

Example: AD reconnaissance – AD recon
https://github.com/sense-of-security/ADRecon/blob/master/ADRecon.ps1


wazuh.
Modules
Security events
Index pattern
wazuh-alerts-*
a
Available fields
agent.id
agent.ip
data.audit.auid
data.audit.command
data.audit.euid
data.audit.exe
data.audit.gid
data.audit.id
data.audit.pid
data.audit.session
data.audit.type
data.audit.uid
data.extra_data
data.sca.check.command
data.sca.check.compliance.cis
data.sca.check.compliance.cis_csc
data.sca.check.compliance.gdpr_IV
data.sca.check.compliance.gpg_13
data.sca.check.compliance.gpg13
data.sca.check.compliance.hipaa
data.sca.check.compliance.nist_800_53
data.sca.check.compliance.pci_dss
data.sca.check.compliance.tsc
timestamp per 30 minutes
Time
agent.name
rule.description
rule.level
rule.id
Jul 5, 2023 @ 14:48:29.201 Windows11 Zip file created: compressed data C:\\Users\\Attacker\\Desktop\\20230705064418_BloodHound.zip created by C:\\Users\\Attacker\\Desktop\\SharpHound.exe. 3 111156
Jul 5, 2023 @ 14:48:29.122 Windows11 Possible Bloodhound activity detected: C:\\Users\\Attacker\\Desktop\\20230705064418_domains.json file created by C:\\Users\\Attacker\\Desktop\\SharpHound.exe. 7 111155
Jul 5, 2023 @ 14:48:29.106 Windows11 Possible Bloodhound activity detected: C:\\Users\\Attacker\\Desktop\\20230705064418_ous.json file created by C:\\Users\\Attacker\\Desktop\\SharpHound.exe. 7 111155
Jul 5, 2023 @ 14:48:29.081 Windows11 Possible Bloodhound activity detected: C:\\Users\\Attacker\\Desktop\\20230705064418_computers.json file cr d by C:\\Users\\Attacker\\Desktop\\SharpHound.exe. 7 111155
Jul 5, 2023 @ 14:48:29.053 Windows11 Possible Bloodhound activity detected: C:\\Users\\Attacker\\Desktop\\20230705064418_users.json file created by C:\\Users\\Attacker\\Desktop\\SharpHound.exe. 7 111155
Jul 5, 2023 @ 14:48:29.038 Windows11 Possible Bloodhound activity detected: C:\\Users\\Attacker\\Desktop\\20230705064418_containers.json file created by C:\\Users\\Attacker\\Desktop\\SharpHound.exe. 7 111155
Jul 5, 2023 @ 14:48:29.011 Windows11 Possible Bloodhound activity detected: C:\\Users\\Attacker\\Desktop\\20230705064418_groups.json file created by C:\\Users\\Attacker\\Desktop\\SharpHound.exe. 7 111155
Jul 5, 2023 @ 14:48:29.010 Windows11 Possible Bloodhound activity detected: C:\\Users\\Attacker\\Desktop\\20230705064418_gpos.json file created by C:\\Users\\Attacker\\Desktop\\SharpHound.exe. 7 111155
Jul 5, 2023 @ 14:47:45.996 Windows11 LDAP query detected by C:\\Users\\Attacker\\Desktop\\SharpHound.exe binary on host. 3 111154
Jul 5, 2023 @ 14:47:45.937 Windows11 LDAP query detected by C:\\Users\\Attacker\\Desktop\\SharpHound.exe binary on host. 3 111154
Jul 5, 2023 @ 14:47:45.921 Windows11 LDAP query detected by C:\\Users\\Attacker\\Desktop\\SharpHound.exe binary on host. 3 111154
Jul 5, 2023 @ 14:47:43.281 Windows11 Possible Bloodhound activity: Sharphound binary executed. 7 111151

Case study example


Storm-0501
Attempts to sign in to Entra ID using a Global Admin user were blocked by conditional access and MFA
Accessed Azure portal as a Global Admin account
Cloud
On-premises
Performed DCSync attack to extract credentials.
Reconnaissance using AzureHound to enumerate users, roles, and Azure resources
Compromised a second Entra Connect server. Repeat reconnaissance process
Moved laterally until they found a hybrid joined device to satisfy conditional access
Achieved domain admin privileges; targeted devices not onboarded to Defender
Moved laterally using Evil-WinRM, leveraging compromised Entra Connect Sync server
Traversed Active Directory domains
Identified a non-human synced identity with Global Admin role. Reset password, assign MFA
Tenant 1
Tenant 2


Storm-0501
Extorted victim organization
Performed cloud-based encryption of data and resources they couldn't delete
Mass-deleted data stores and backup resources
Exfiltrated data from Azure Storage accounts
Accessed Azure portal as a Global Admin account
Created a backdoor via maliciously added federated domains
Elevated access to all Azure resources, and was assigned *Owner* Azure role
Exposed the data stores to certain addresses to prepare for exfiltration
Cloud
On-premises
On-premises compromise

Important notes

- More tenants, more Active Directory domains
- Of the multiple compromised domains, only one domain had significant Defender for Endpoint deployment, leaving portions of the network unmonitored.
- ***LOLBINS*** *- systeminfo.exe, net.exe, nltest.exe, tasklist.exe, quser.exe*
- *Remote management –* ***Anydesk, winrm***
- ***Where is MDE?*** *sc query sense, sc query windefend* *(*effort to avoid detection by targeting non-onboarded systems.)
- AD reconnaissance – AD recon https://github.com/sense-of-security/ADRecon/blob/master/ADRecon.ps1
- **Entra Connect Sync server that was not onboarded to Defender for Endpoint**.
- Impersonating a domain controller - This technique is often used to extract credentials without triggering traditional authentication-based alerts.
- **MFA and Conditional access!** - they traversed between Active Directory domains and eventually moved laterally to compromise a second Entra Connect server associated with different Entra ID tenant and Active Directory domain. Discovered non-human synced identity that was assigned with the Global Administrator role
- **Conditional access: MFA and Entra hybrid joined device:**
  - Attacker reset the user's on-premises password, simply register a new MFA method under their control
  - The threat actor had to move laterally between different devices in the network


2026?

Next steps

Healtchecky, konzultace, pentesty, red teaming, security tuning:

Emailem: lubomir@osmera.tech

Web: https://lubomirosmera.cz/securitytuning/

HeroHero: https://herohero.co/laudablekrxyalcmnrybe

Gopas kurzy:

GOC213 - Windows Server - hacking and pentesting Active Directory

GOC215 - Microsoft 365 - bezpečnost hybridního prostředí

GOC238 - Microsoft Azure - hacking a penetrační testování