
NIC
REBEL
EDITION

Sami Laiho

The Cybersecurity Turning Point:
How Today’s Shifts Will Redefine Trust, Identity, and Survival.

NIC REBEL EDITION

Sami Laiho

Chief Research Officer / MVP

- IT Admin since 1995 / MCT since 2001
- MVP in Windows OS since 2011, Security since 2024
- ”100 Most Influencial people in IT in Finland” – TiVi’2019→
- Specializes in and trains:
  - Troubleshooting
  - Windows Internals
  - Security, Social Engineering, Auditing
- Trophies:
  - Best Session at Advanced Threat Summit 2020
  - Best Speaker at NIC, Oslo 2016, 2017, 2019, 2020, 2022, 2023 and 2024
  - Ignite 2018 – Session #1 and #2 (out of 1708) !
  - TechEd Europe and North America 2014 - Best session, Best speaker
  - TechEd Australia 2013 - Best session, Best speaker
- Hobbies: Counting my kids, Geeking out

Geopolitics

BBC

BBC

EU cyber agency says airport software held to ransom by criminals

3 hours ago

Share Save

Joe Tidy Cyber correspondent and Tabby Wilson

Drones were observed overnight above Karup airbase (pictured), Denmark's largest military base

Sweden's power grid operator confirms data breach claimed by ransomware gang

Sweden's power grid operator is investigating a data breach after a ransomware group threatened to leak hundreds of gigabytes of purportedly stolen internal data.

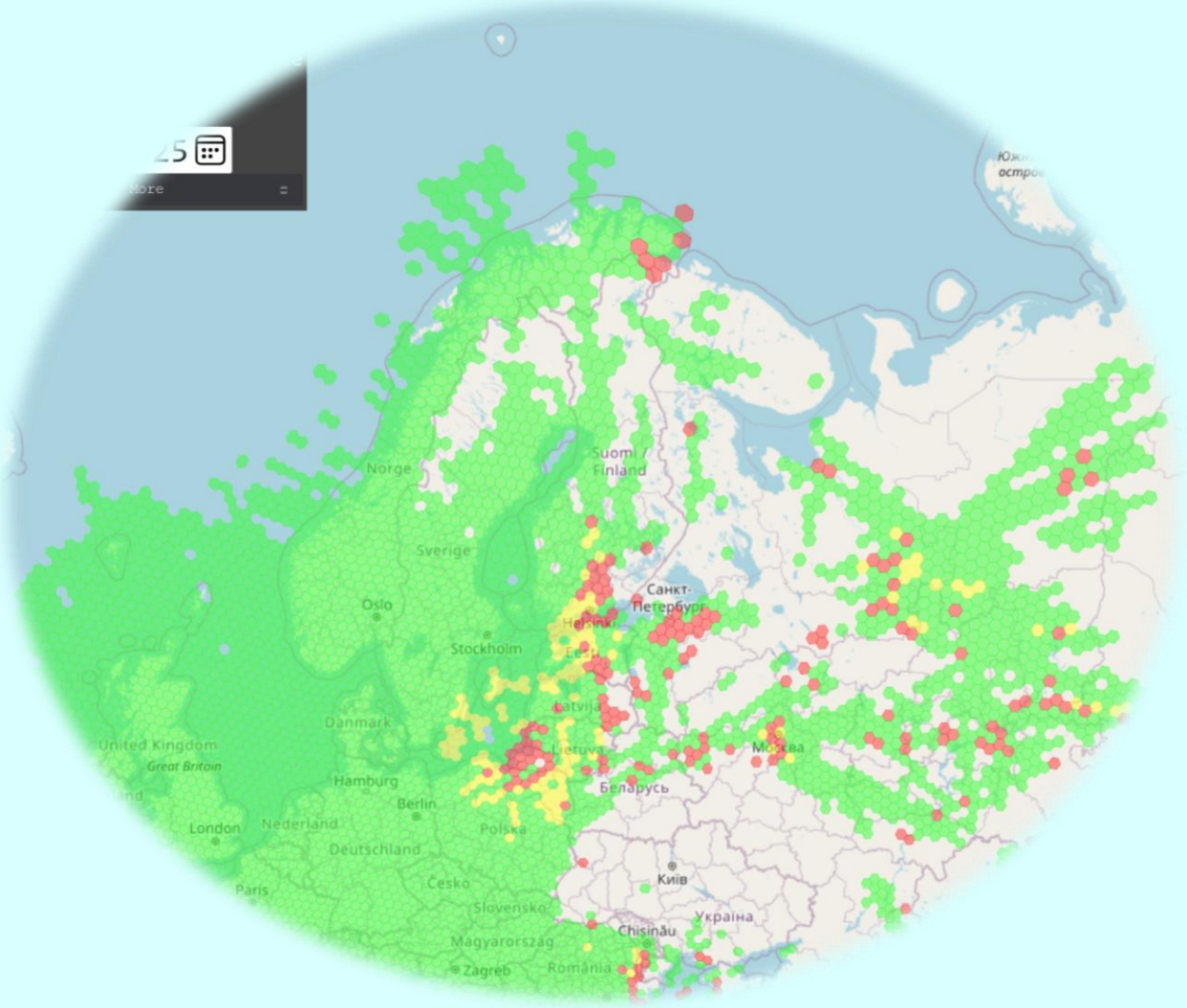
State-owned Svenska kraftnät, which operates the country's electricity transmission system, said the incident affected a "limited external file transfer solution" and did not disrupt Sweden's power supply.

"We take this breach very seriously and have taken immediate action," said Chief Information Security Officer Cem Göcgören in a statement. "We understand that this may cause concern, but the electricity supply has not been affected."

NIC REBEL EDITION

GPS / GNSS

- [GPSJAM GPS/GNSS Interference Map]



NIC REBEL EDITION

NIC REBEL EDITION

JLR Attack

- Estimated 2.1 B£ losses
- Tens of contractors bancrupt

Inside the Jaguar Land Rover hack: stalled smart factories, outsourced cybersecurity and supply chain woes

Being a carmaker where 'everything is connected' has left JLR unable to isolate its plants or functions, forcing a shutdown of most systems

By Jasper Jolly and Dan Milmo

NIC REBEL EDITION

Ransomware

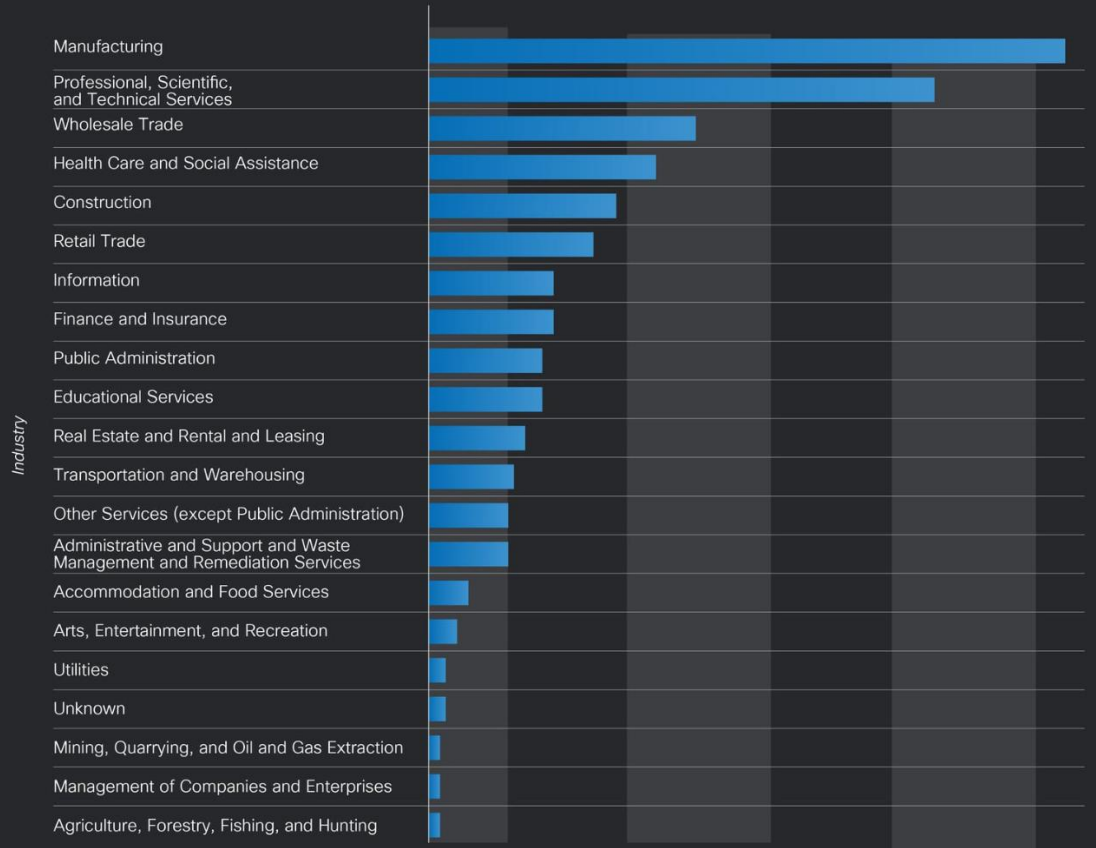
- “Ransomware attacks were up 50% in 2025 through October 21, according to Cyble data, rising to 5,010 from 3,335 in the same period of 2024. Cyble’s data is based on ransomware group claims on their dark web data leak sites.”
- https://cyble.com/blog/ransomware-attacks-surge-50-percent/

NIC REBEL EDITION

RANSOMWARE.LIVE

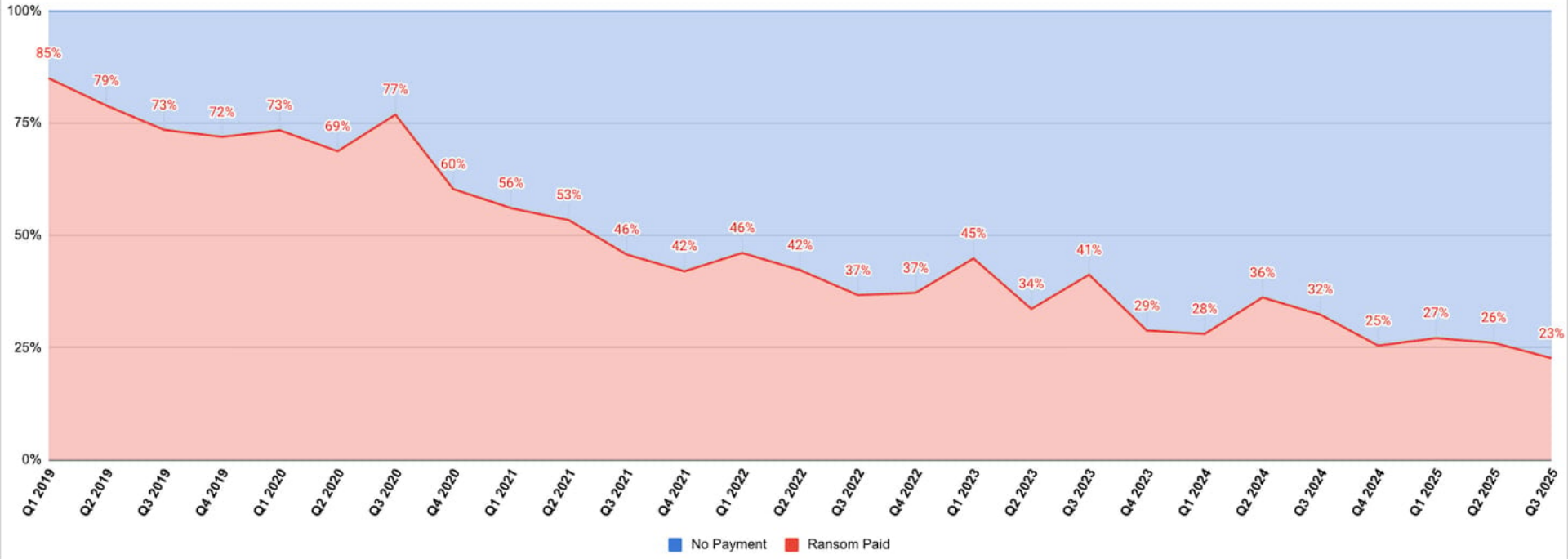
Sectors experiencing damage/impact

CISCO TALOS



NIC REBEL EDITION

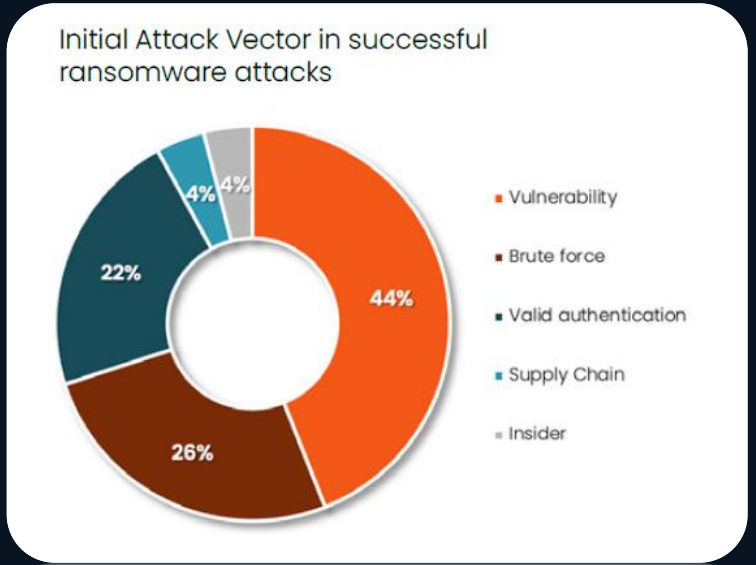
All Ransomware Payment Resolution Rates



NIC REBEL EDITION

2024

- Attack Vectors – How do they get in?



Source: Truesec

Average critical vulnerability remediation time (days)

Industry	2024	2025
Diversified financials	14	22
Software	24	13
Healthcare services	20	22
Professional services	29	21

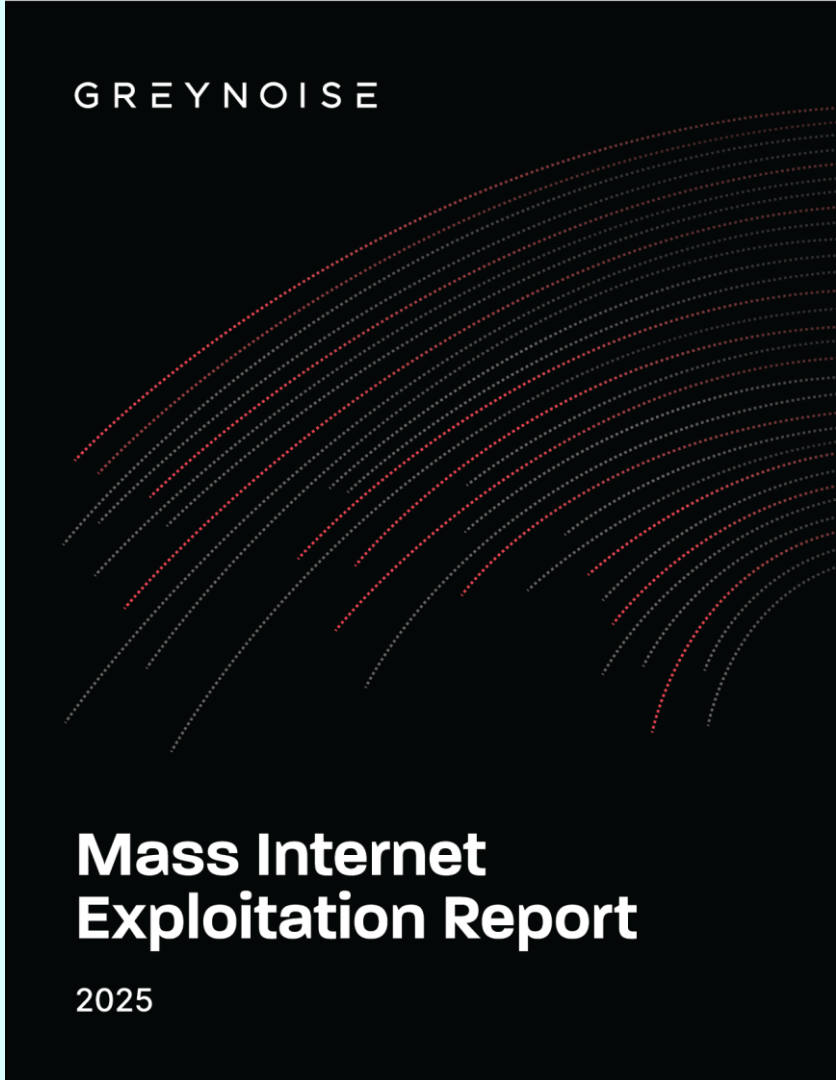
Intruder - 2025 Exposure Management Index

”For us two days was too slow”

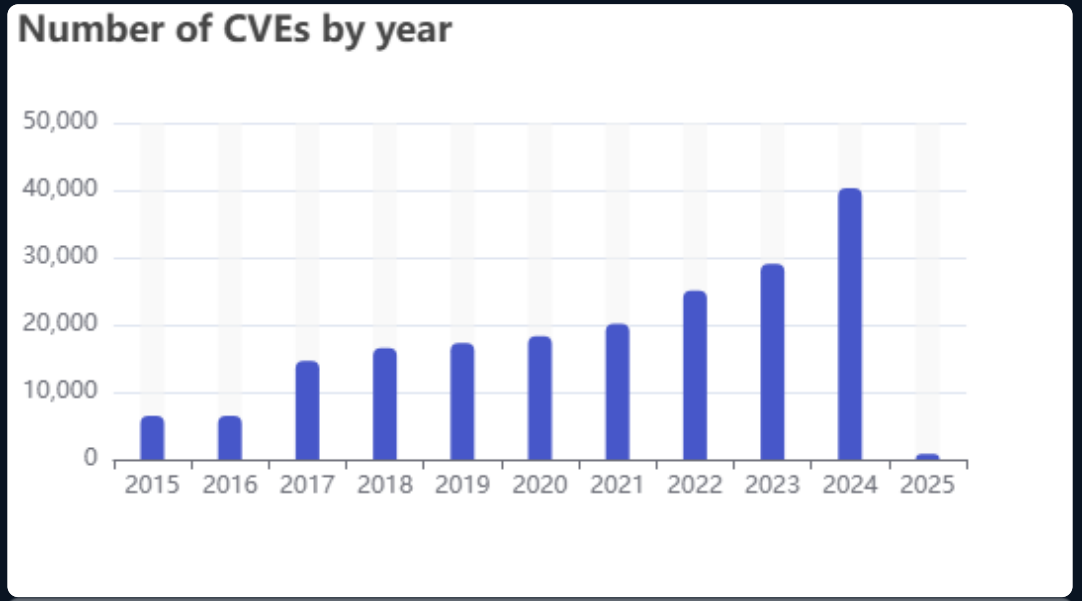
Google

GREYNOISE 2025 REPORT

- The most exploited vulnerability of 2024 targeted home internet routers, fueling massive botnets used in global cyberattacks.
- 40% of exploited vulnerabilities in 2024 were from 2020 or earlier — some dating back to the 1990s.
- Attackers are exploiting vulnerabilities within hours of disclosure
- A surge in May 2024 was traced to 12,000+ hacked Android devices, showing mobile threats are growing.
- D-Link and Ivanti devices were among the most heavily exploited in 2024, posing critical security risks for businesses and governments.



Cumulative Yearly CVE publication



NIC REBEL EDITION

Cyberpress

Supply Chain Attacks

"In fact, Gartner predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021."

Supply chain compromises mean you don't even need to be the target to become a victim

NIC REBEL EDITION

NPM


WIZ
Threat Update!
Shai-Hulud:
npm Supply Chain
Worm Delivering
Data-Stealing Malware

SBOM

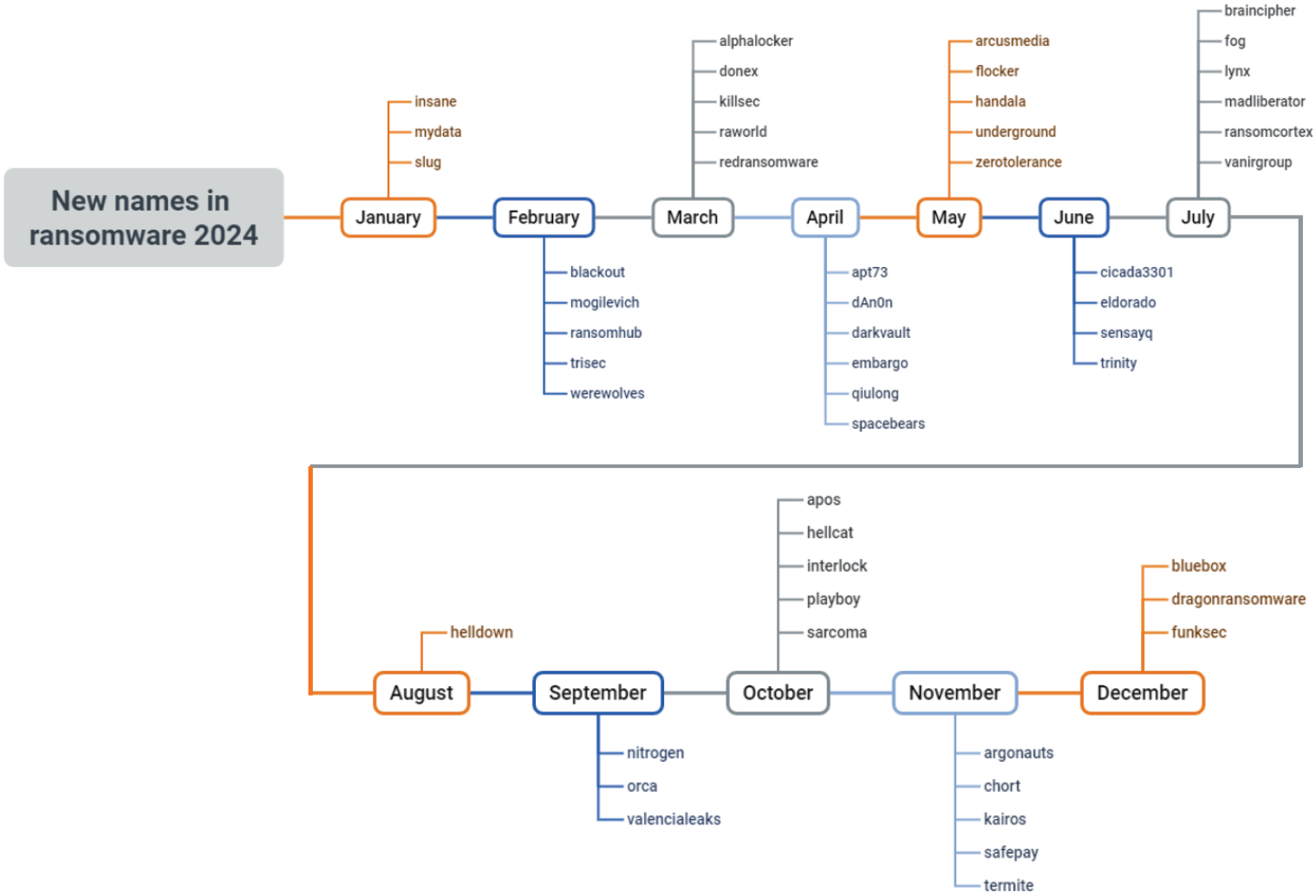
Identity is the most valuable/vulnerable asset

for the enemy as well

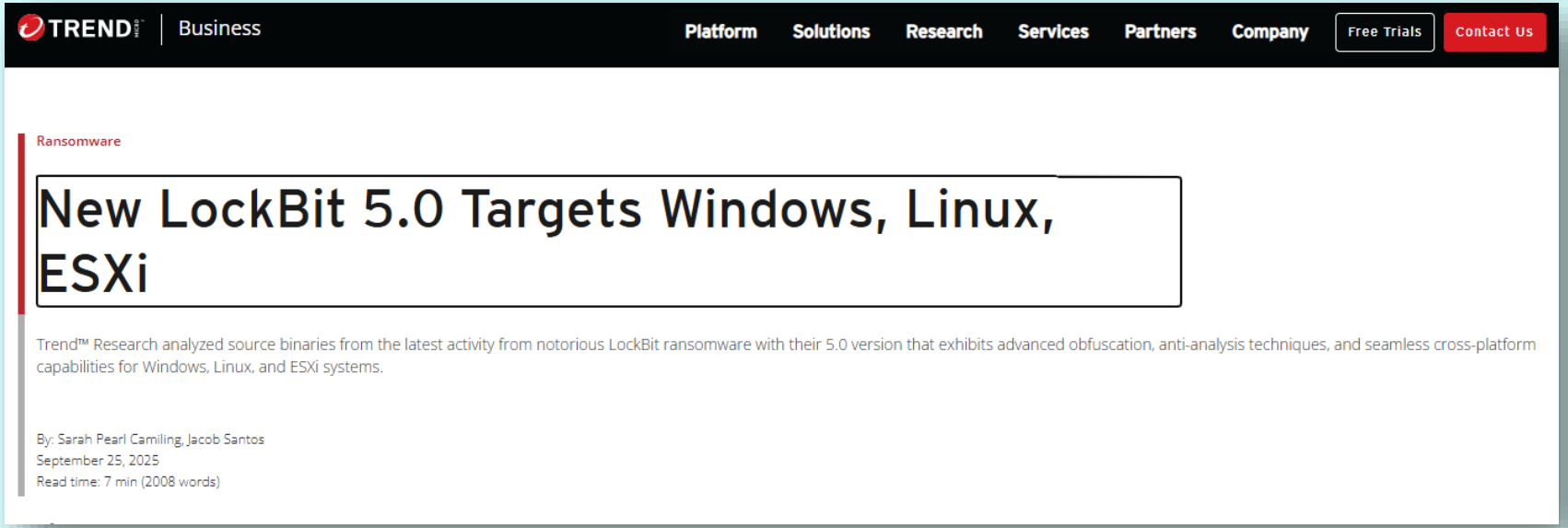
NIC REBEL EDITION

ContiGroup

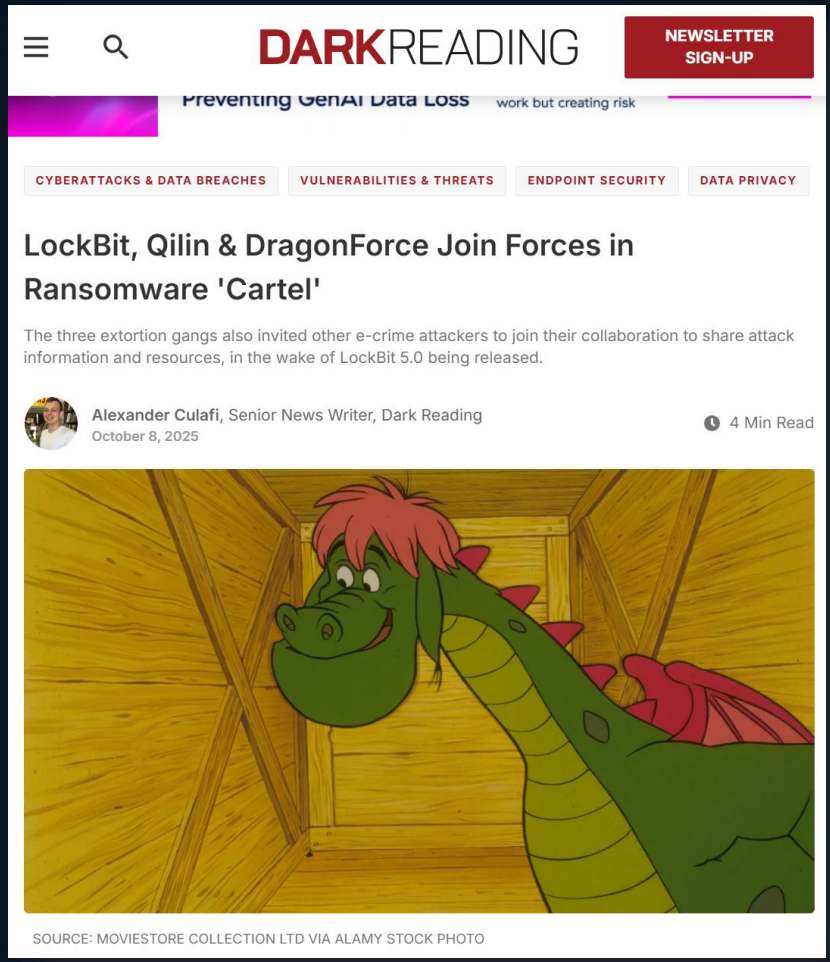
NIC REBEL EDITION


New names in ransomware 2024
January
insane
mydata
slug
February
blackout
mogilevich
ransomhub
trisec
werewolves
March
alphalocker
donex
killsec
raworld
redransomware
April
apt73
dAn0n
darkvault
embargo
qiulong
spacebears
May
arcusmedia
flocker
handala
underground
zerotolerance
June
cicada3301
eldorado
sensayq
trinity
July
braincipher
fog
lynx
madliberator
ransomcortex
vanirgroup
August
helldown
September
nitrogen
orca
valencialeaks
October
apos
hellcat
interlock
playboy
sarcoma
November
argonauts
chort
kairos
safepay
termite
December
bluebox
dragonransomware
funksec

News to anyone…



Cartels arrise



NIC REBEL EDITION

There are some limits – even for criminals

Except for mr. Kivimäki

Check out: [Most Wanted: Teen Hacker • HBO Max]

Hi Team,

Black Basta Ransomware group affiliates have been known to use Microsoft Teams to reach target users.

Threat actors use Microsoft Teams to send messages and make calls, pretending to be IT or help desk staff. Our rule is searching for specific strings in the related usernames within in the created OneonOne type Chats with external users.

Please confirm all participants in this Teams Chat/Meeting who are outside your organization are expected.

Ref.: https://arcticwolf.com/resources/blog/december-2024-uptick-in-social-engineering-campaign-deploying-black-basta-ransomware/

Incident name: Suspicious External Teams Chat Created

- Event type: chatcreated
- Application: MicrosoftTeams
- User who initiated chat: simone[redacted]
- Target user: sami@adminize.com

NIC REBEL EDITION

Identity: The Core Battlefield

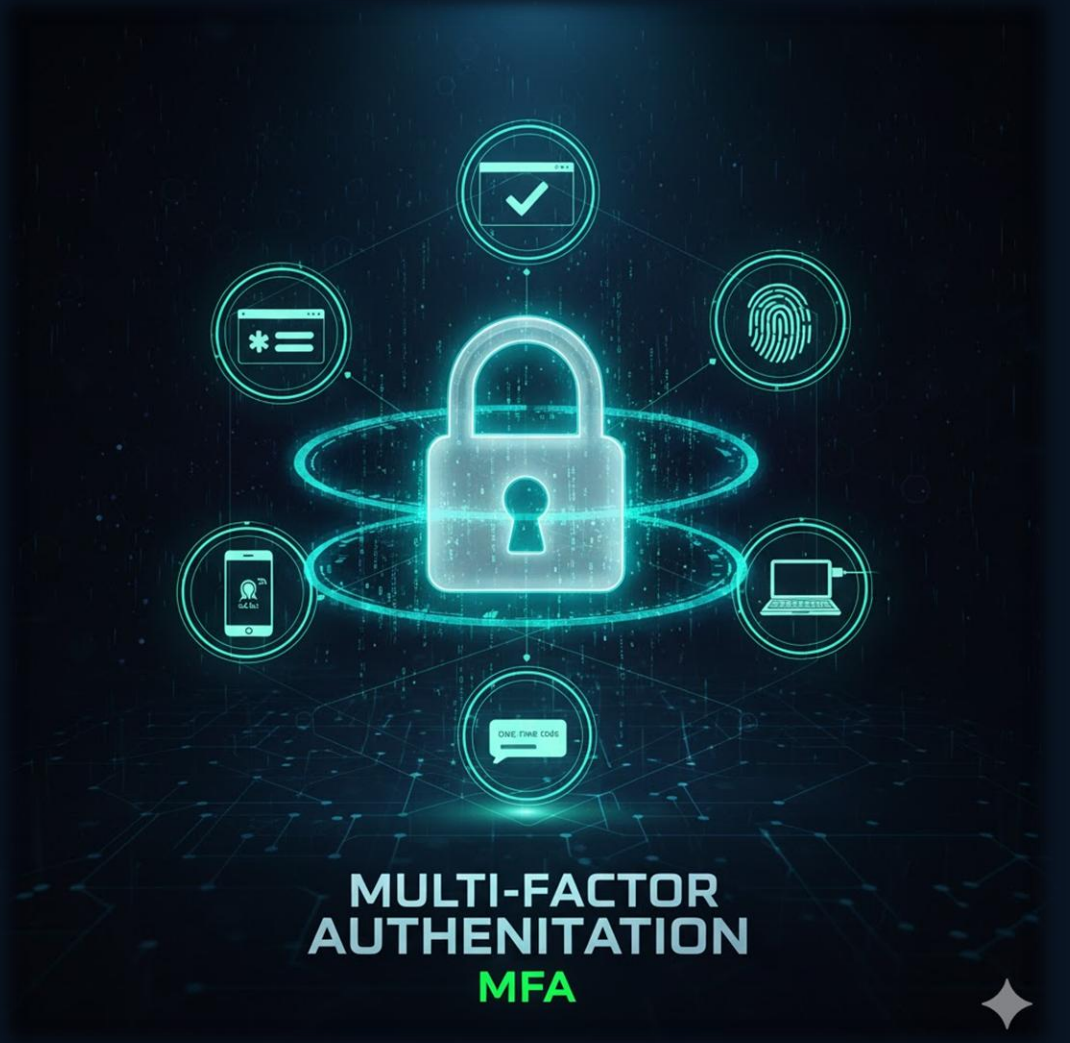
Identity has shifted from a control to a target.

“Most known attacks still start with a STAB – Steal, Try, Ask, Buy”
- The Grugg

NIC REBEL EDITION

MFA blocks 99% of Phishing

- Yes, still today…



NIC REBEL EDITION

SIM Swapping

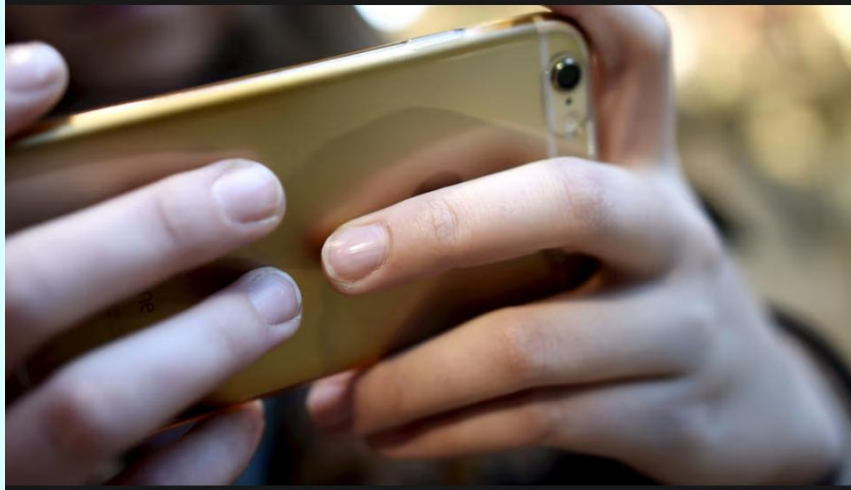
SMS is not a secure authenticator
- Although better than nothing…

TIETOTURVA

Tämä huijaustapa yleistyy Suomessa – uhri menettää puhelinnumeronsa

Poliisi varoittaa niin kutsutusta sim swapping -huijauksesta.

JAA TALLENNA KOMMENTIT



Hyökkäys voi vaarantaa rahat. KUVA: ANTTI AIMO-KOIVISTO / LEHTIKUVA

Kuuntele juttu

Tuomas Linnake
7.10. 10:52

AI affects both Identities and Geopolitics

AI isn’t just a defender’s tool — it’s an **attacker’s force multiplier**.

ChatGPT in Finland

NIC REBEL EDITION


BREAKING NEWS:
FINLAND INVADES NORWAY

NIC REBEL EDITION

”There were 105,120 deepfake attacks reported in 2024, which is about one attack every five minutes.”

Source: Barracuda Networks

Redefining Survival

- Accelerate detection and response with AI on the defender’s side.
- Security posture becomes an organizational survival strategy, not just IT.
- Geopolitics → cyberattacks as economic warfare.

NIC REBEL EDITION

Turning Point

- Resilience replaces prevention.
- Build trust layers that degrade gracefully — not brittle perimeters.
- Identity is no longer just your **login** — it's your **attack surface**.
- AI is both the **adversary's scalpel** and **the defender's shield**.
- Those who adapt **trust models** and **response capabilities** survive.

NIC REBEL EDITION

Homework

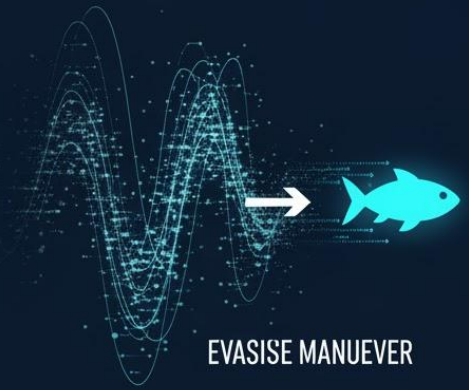
- Keeping your inventory up-to-date and prepare for SBOM
- Prioritizing vulnerabilities based on risk - Patch more, Test Less
- Protecting Internet-facing assets
- Tiering your directories both on-premise and cloud
- Managing (at least) your Tier 0 only from Privileged Access Workstations
- Deploying a PAM for external contractor access, if not all privileged access
- Segmenting networks and critical assets, preferably with SDNs that are identity-based
- Not trusting your internal networks more than external
- Hardening endpoints and infrastructure
- Strong access controls, allowing no more access than is required, with frequent verification
- A strong source of user identity and authentication, including Phishing Resistant MFA and biometrics, as well as machine authentication with device compliance and health checks
- Encryption of data at rest and in transit
- Ransomware-resistant backups that are immutable, air-gapped, and isolated as much as possible
- Honeypots that lure attackers to fake assets for early breach detection
- Proper configuration and protection of APIs and cloud service connections, and their secret keys
- Monitoring for unusual and anomalous activity with EDR/XDR/SIEM, Active Directory monitoring, endpoint security, and data loss prevention (DLP) tools
- Routinely assessing and confirming controls through audits, vulnerability scanning, and penetration tests
- Practicing recovery and crisis situation handling
- Deploying or outsourcing a SOC
- Automate faster than attackers.
- Don’t just secure systems — secure trust itself.

NIC REBEL EDITION

Your job is not to stop the enemy but to slow it down…

Your security controls force the enemy to behave abnormally, making it an anomaly, that your SOC can detect and stop…

COHESIVE STREAM



EVASISE MANUEVER

PATH COMPARISON: GROUP VS. INDIVIDUAL

NIC REBEL EDITION

Thank You!
Enjoy NIC!

NIC REBEL EDITION