Ransomware Best Practices: When the Best is the Enemy of the Good

Cristine Hoepers, Ph.D.
General Manager, CERT.br/NIC.br
cristine@cert.br

NatCSIRT 2026
June 13th, 2026 – Denver, CO, USA

cert.br nic.br cgi.br

TLP:CLEAR

cert.br

Computer Emergency Response Team Brazil

National CSIRT of Last Resort

Services Provided to the Community

Incident Management

- Coordination
- Technical Analysis
- Mitigation and Recovery Support

Situational Awareness

- Data Acquisition
  - Distributed Honeypots
  - SpamPots
  - Threat feeds
- Information Sharing

Knowledge Transfer

- Awareness
  - Development of Best Practices
  - Outreach
- Training
- Technical and Policy Advisory

Affiliations and Partnerships:

FIRST MEMBER

M3AAWG Messaging Malware Mobile Anti-Abuse Working Group

Carnegie Mellon University Software Engineering Institute — SEI Partner Network

APWG

Accredited by Trusted Introducer

Mission

To increase the level of security and incident handling capacity of the networks connected to the Internet in Brazil.

Constituency

Any network that uses Internet Resources allocated by NIC.br

- IP addresses or ASNs allocated to Brazil
- domains under the ccTLD .br

Governance

Maintained by **NIC.br** – The National Internet Registry (NIR)

- not for profit
- all activities are funded by .br domain registration

NIC.br is the **executive branch of CGI.br** – The Brazilian Internet Steering Committee

- a multistakeholder organization
- with the purpose of coordinating and integrating all Internet service initiatives in Brazil

https://cert.br/about/
https://cert.br/sobre/filiacoes/
https://cert.br/about/rfc2350/

Agenda and Motivation

TLP:CLEAR

Our objective:
Simplify the message

What will be discussed in this presentation

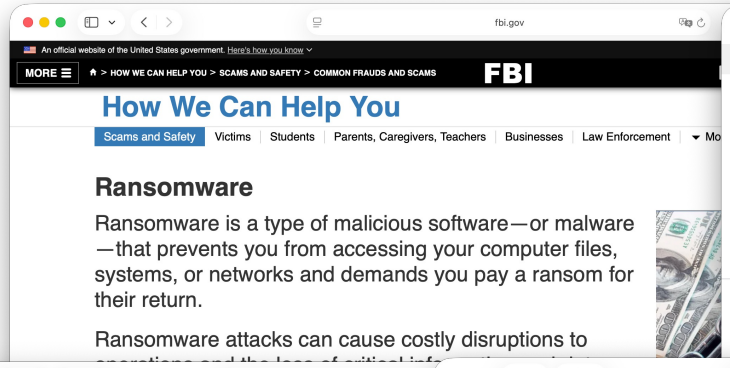
- Why we decided to write yet another best practices document about ransomware
- Challenges we identified
  - specially for Small and Medium Enterprises (SMEs)
- The choices we made along the way

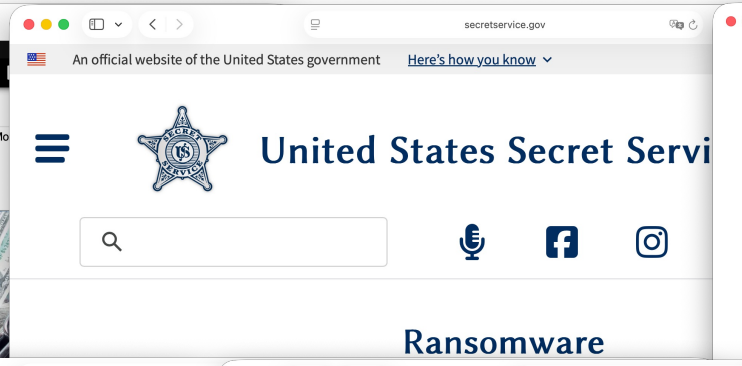
What we have created:
Ransomware: How to Protect

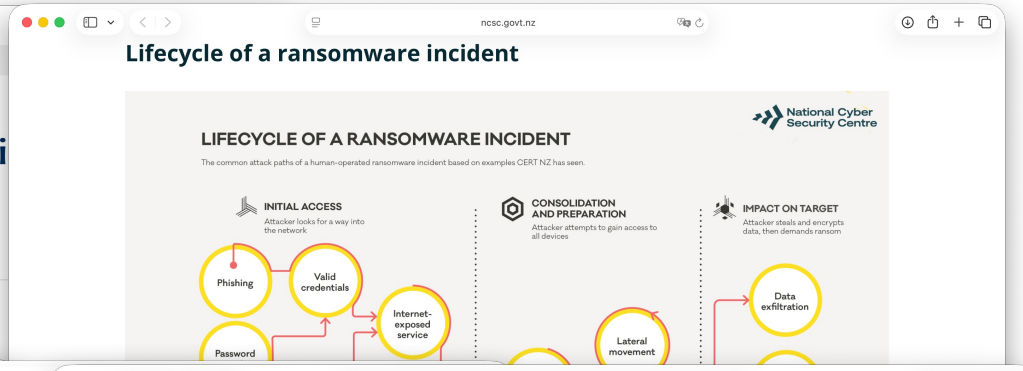
- In 3 languages:
  PT-BR, ES, EN

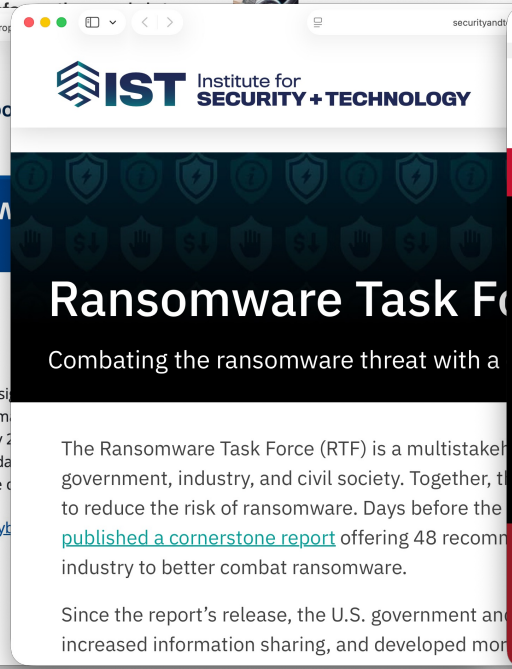
Ransomware Prevention, Detection and Response:
Several really good recommendations already exist

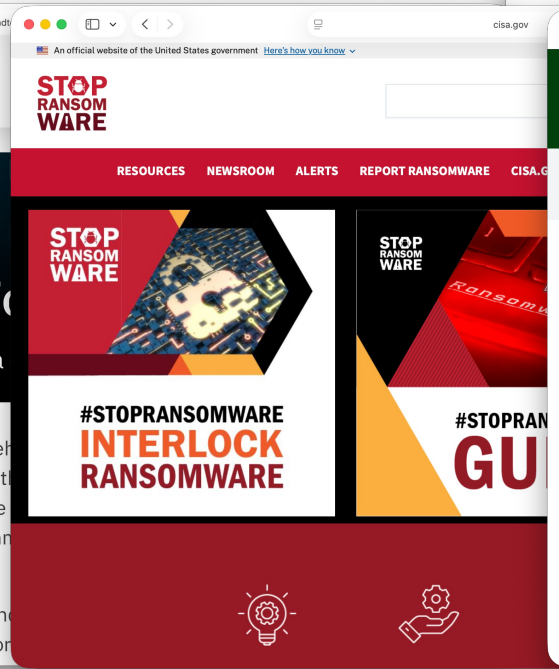
TLP:CLEAR











https://www.fbi.gov/ransomware | https://www.secretservice.gov/investigations/ransomware | https://www.ncsc.govt.nz/protect-your-organisation/protect-your-organisation-against-ransomware/
https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks | https://securityandtechnology.org/ransomwaretaskforce/ | https://www.cisa.gov/stopransomware | https://www.first.org/global/sigs/msr/

TLP:CLEAR

But attacks and victims continue to grow:
Professionalization and number of victims go hand in hand

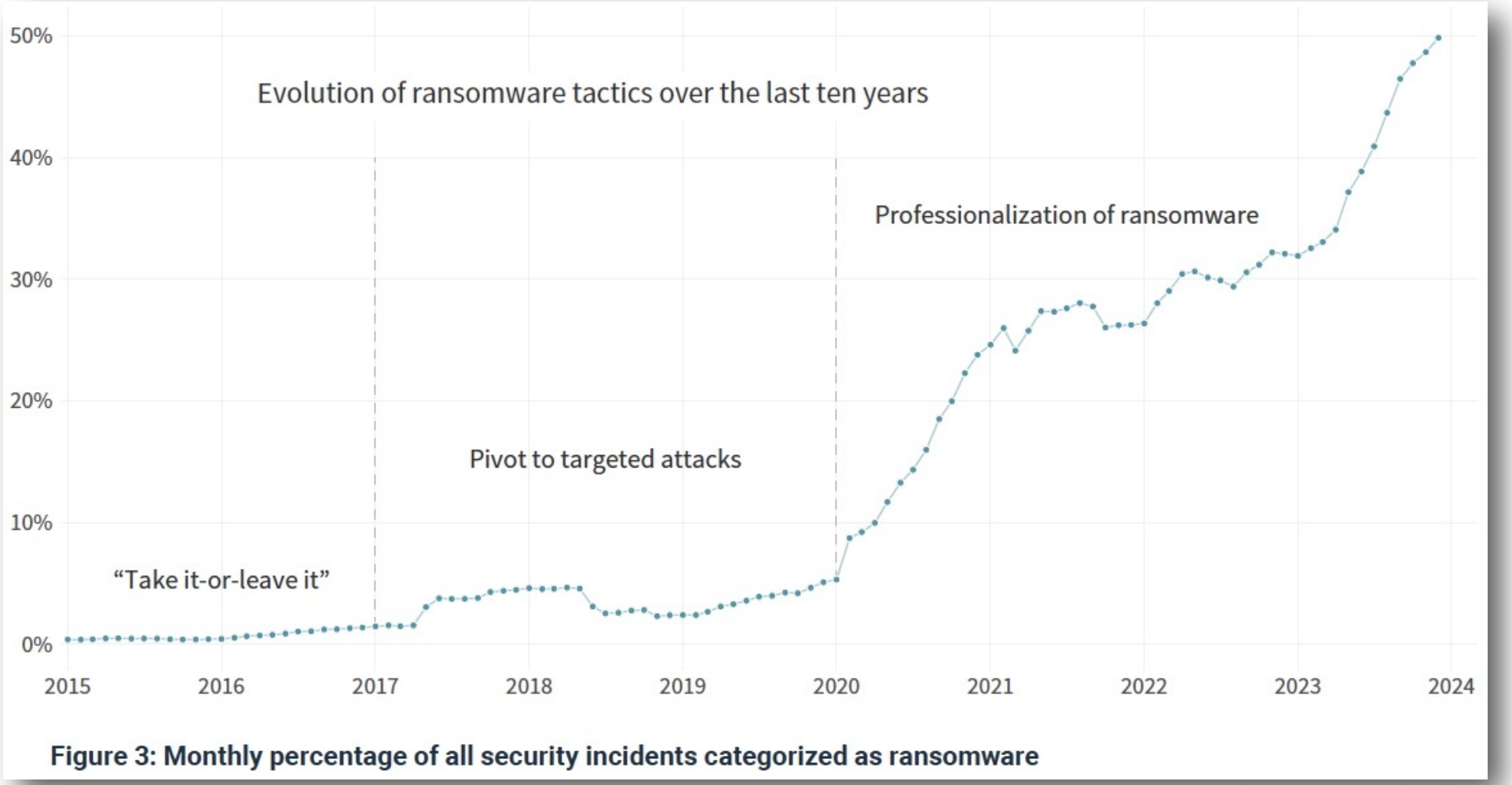


Figure 3: Monthly percentage of all security incidents categorized as ransomware

Source: https://www.cyentia.com/iris-ransomware/

We set ourselves to identify how to improve the situation

SMEs perspective

- What's missing?
  - understanding?
  - prioritization?
  - money?
  - tools?
  - people?
  - something else?
- How to motivate business owners?
- How to empower contractors to "sell" the need for investment and change?

Technical perspective

- Grasp the ransomware business model
  - Where are the weakest links?
  - How to detect early and minimize impact?
- Lessons from victims and incident responders
  - How to detect early?
  - What are the biggest mistakes in prevention and detection?
  - If you had to pick, what are the top 2 measures people are failing to implement?
    - defense
    - detection

What we found out

SME Owner Perspective

"*All or nothing*" mentality prevails

- "*It is impossible to implement all recommendations*"
- "*I am going to be compromised and fined by the regulators anyway*"
  - so, why invest so much in prevention and detection if it is doomed to fail?

Plus

- Security measures "get in the way" of daily work

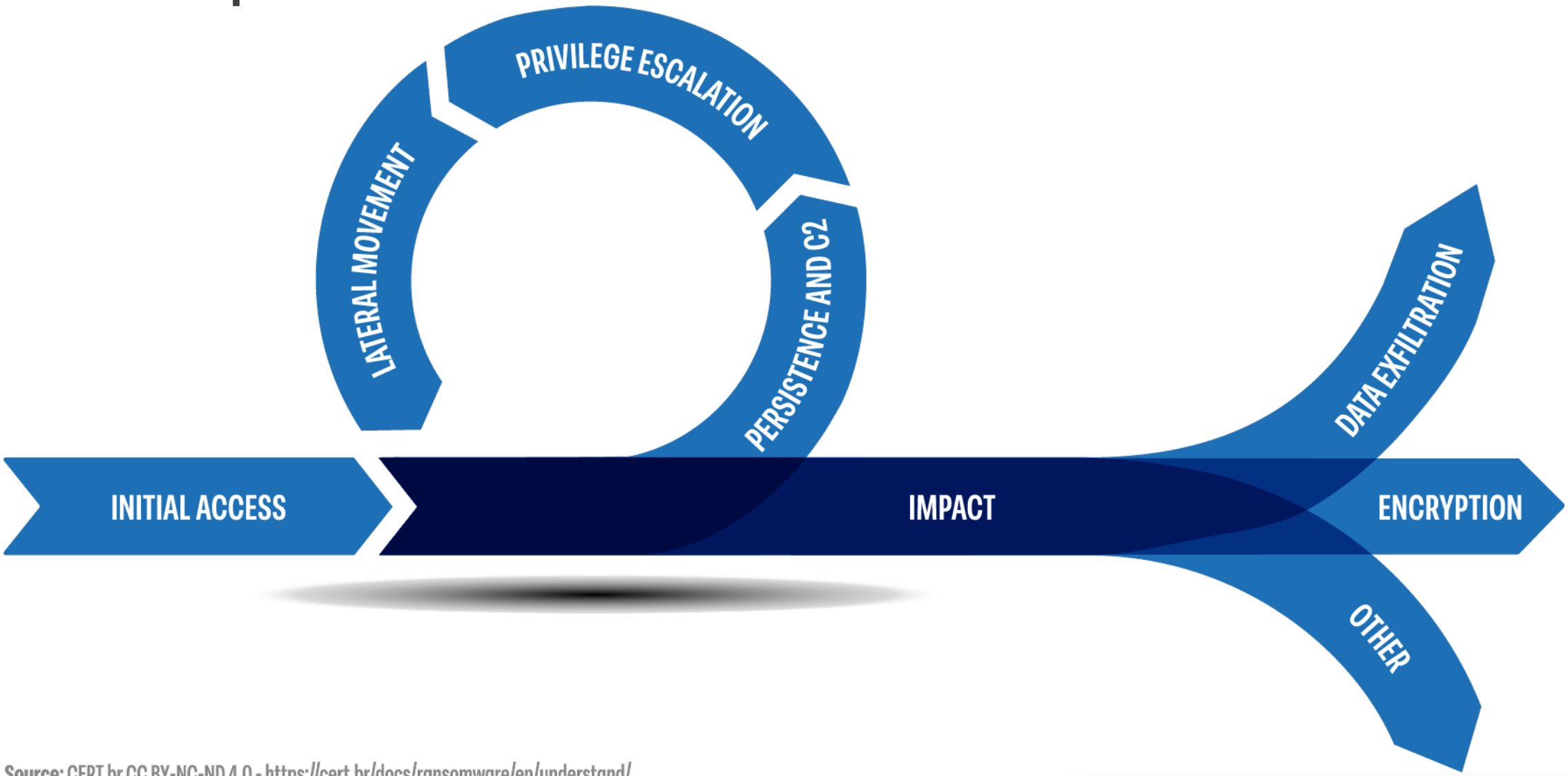
MSS / Security Contractor Perspective

"*I can't convince them on the importance of the measures*" sums up the overall feeling

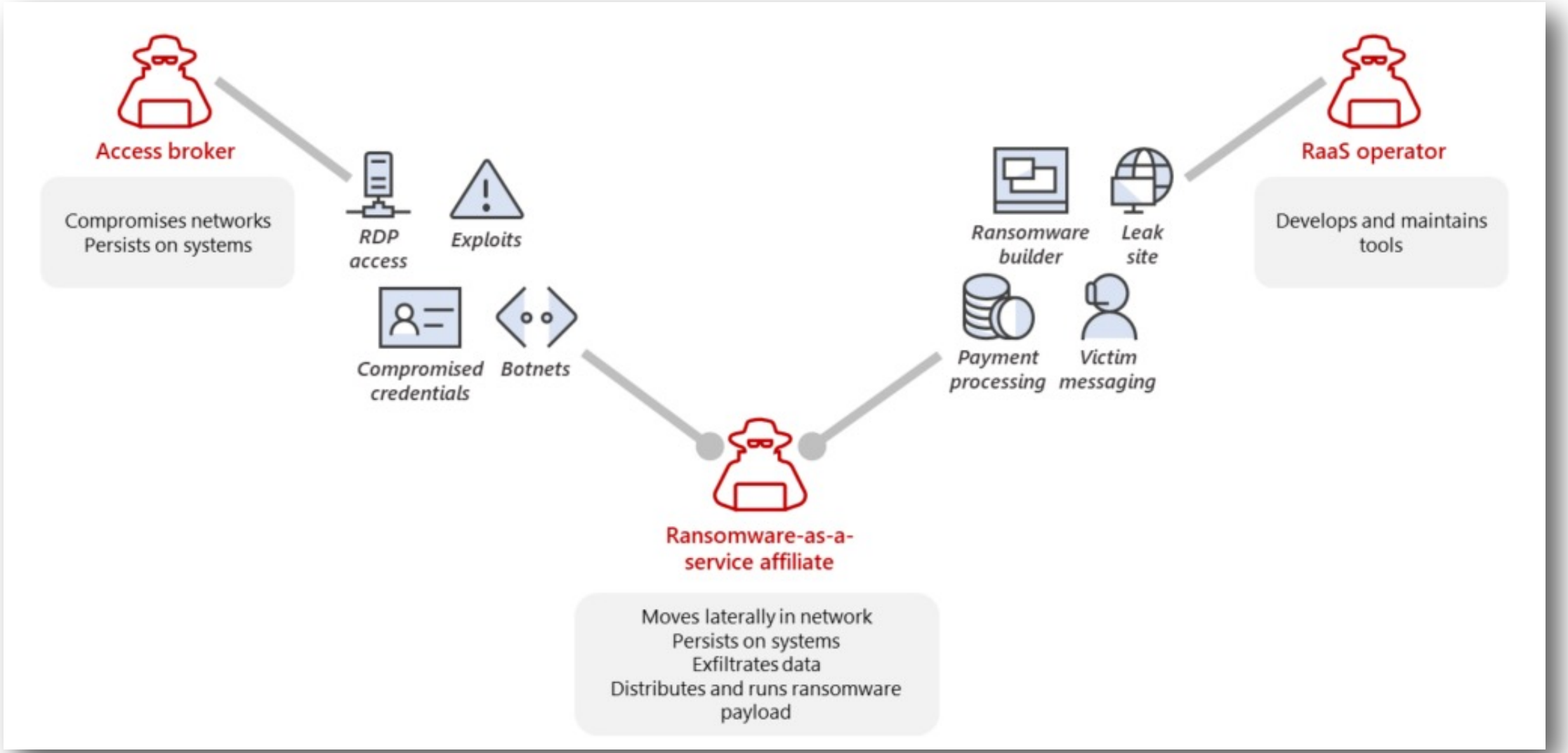
- It is hard to convince the owners about the importance of the measures
- Tools are expensive
- Most SME executives don't see business value in security measures

TLP:CLEAR

Ransomware Life Cycle
Victims' Perspective



Ransomware Business Model:
Ransomware as a Service



Source: https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

TLP:CLEAR

CYBERSECURITY ADVISORY

#StopRansomware: RansomHub Ransomware

Release Date: August 29, 2024 **Alert Code:** AA24-242A

Initial Access

RansomHub affiliates typically compromise internet facing systems and user endpoints by using methods such as phishing emails [T1566], exploitation of known vulnerabilities [T1190], and password spraying [T1110.003]. Password spraying targets accounts compromised through data breaches. Proof-of-concept exploits are obtained from sources such as ExploitDB and GitHub [T1588.005]. Exploits based on the following CVEs have been observed:

- CVE-2023-48788 (CWE-89)
  - An improper neutralization of special elements used in an SQL command (SQL injection') in Fortinet FortiClientEMS version 7.2.0 through 7.2.2 and FortiClientEMS 7.0.1 through 7.0.10 allows attacker to execute unauthorized code or commands via specially crafted packets.
- CVE-2017-0144
  - The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, also known as "Windows SMB Remote Code Execution Vulnerability" [T1210].

Source: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a

TLP:CLEAR

Industrial Cyber

Search | Register | Login

Channels | Features | News | Vendor Directory | Resources | Webinars & Events | Team

Home · Attacks and Vulnerabilities · Half of 2025 ransomware attacks hit critical sectors as manufacturing, healthcare, and energy top global targets

The manufacturing sector experienced the sharpest growth, with attacks surging 61% compared with the previous year. High-profile incidents included Jaguar Land Rover's global shutdown and Bridgestone's production disruptions, illustrating how ransomware can paralyze supply chains and economies. Together, these high-profile

Among 103 active ransomware groups, just five, including Qilin, Clop, Akira, Play, and SafePay, were responsible for nearly 25% of all incidents, highlighting the growing professionalization and consolidation within cybercriminal ecosystems.

Attacks And

SOC & Incident Response Threat Landscape

Half of 2025 ransomware attacks hit critical sectors as manufacturing, healthcare, and energy top global targets

OCTOBER 22, 2025

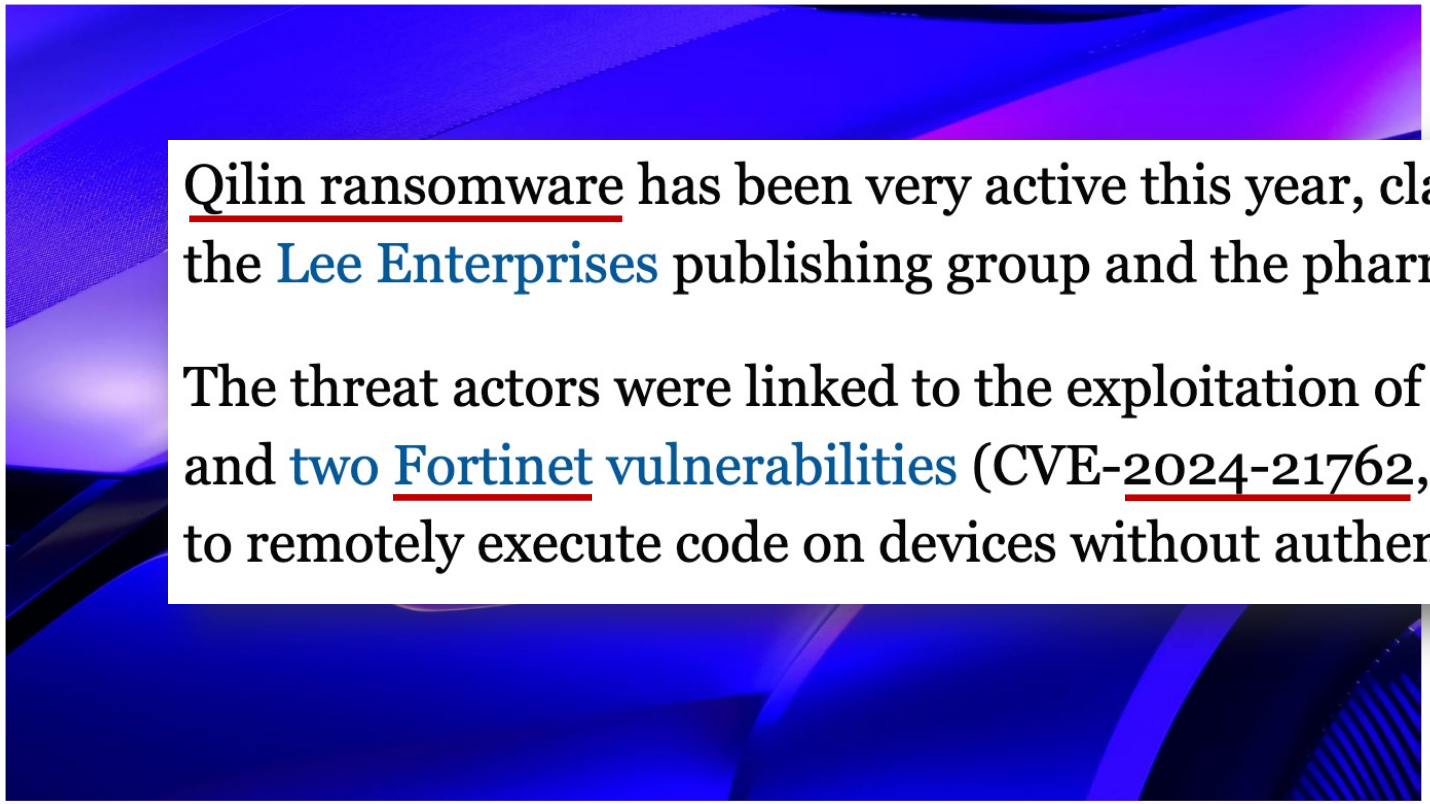
Source: https://industrialcyber.co/reports/half-of-2025-ransomware-attacks-hit-critical-sectors-as-manufacturing-healthcare-and-energy-top-global-targets/

TLP:CLEAR

Nissan confirms design studio data breach claimed by Qilin ransomware

By Bill Toulas

August 26, 2025 09:48 AM 0



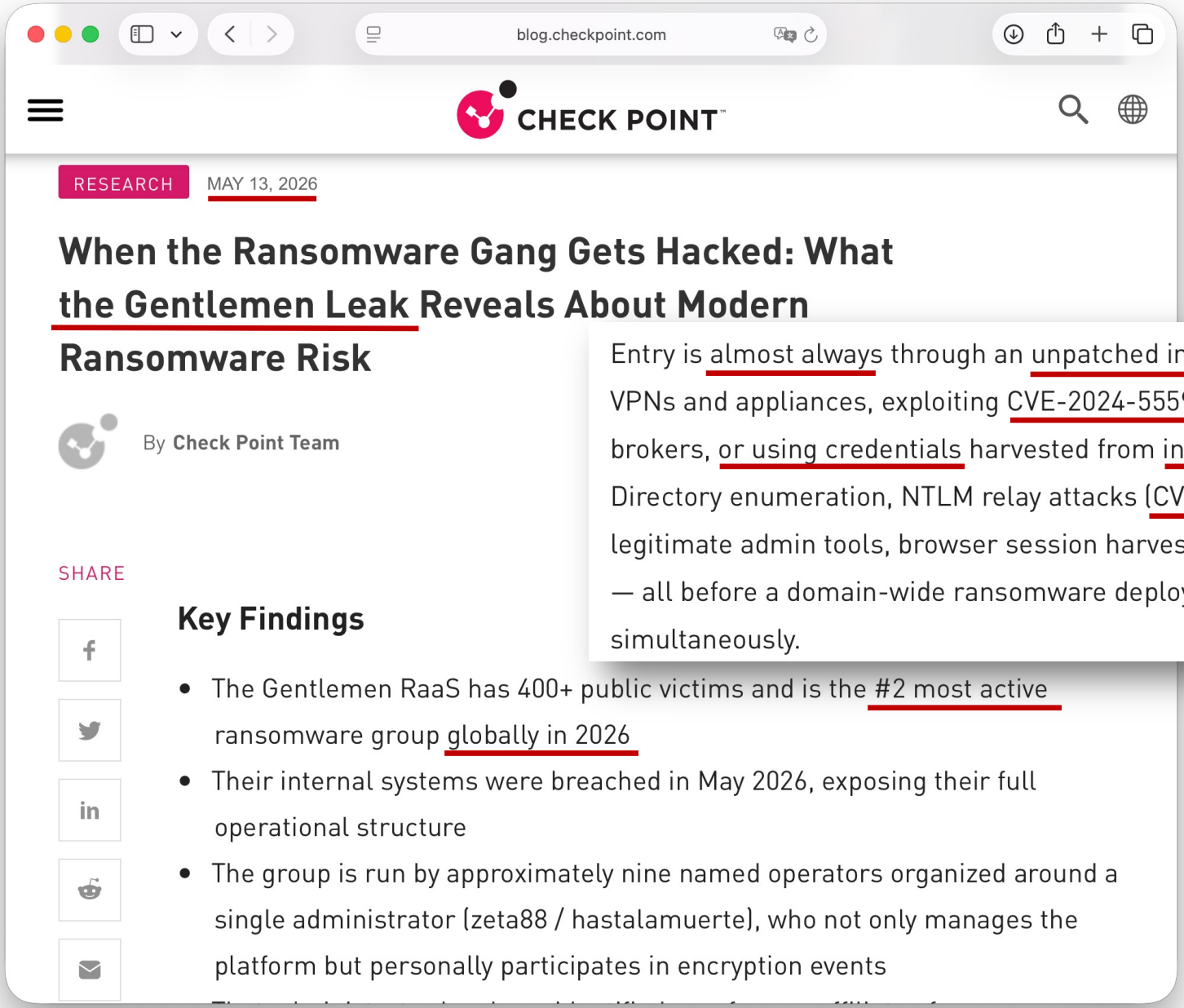
Nissan Japan has confirmed to BleepingComputer that it suffered a data breach following unauthorized access to a server of one of its subsidiaries, Creative Box Inc. (CBI).

Qilin ransomware has been very active this year, claiming high-profile victims such as the Lee Enterprises publishing group and the pharmaceutical firm Inotiv.

The threat actors were linked to the exploitation of the Kickidler employee monitoring tool and two Fortinet vulnerabilities (CVE-2024-21762, CVE-2024-55591), which enabled them to remotely execute code on devices without authentication.

Source: https://www.bleepingcomputer.com/news/security/nissan-confirms-design-studio-data-breach-claimed-by-qilin-ransomware/

TLP:CLEAR



Entry is almost always through an unpatched internet-facing device. The Gentlemen specifically target VPNs and appliances, exploiting CVE-2024-55591 and CVE-2025-32433, buying access from third-party brokers, or using credentials harvested from infostealer log markets. Once inside, they move fast: Active Directory enumeration, NTLM relay attacks (CVE-2025-33073), EDR disablement, lateral movement via legitimate admin tools, browser session harvesting for Microsoft 365 and Okta access, and data exfiltration — all before a domain-wide ransomware deployment via Group Policy that hits every connected endpoint simultaneously.

Source: https://blog.checkpoint.com/research/when-the-ransomware-gang-gets-hacked-what-the-gentlemen-leak-reveals-about-modern-ransomware-risk/

The lessons learned along the way…

- Most business owners don't understand
  - why security controls are important
  - what each control protects
- Focus on prioritization based on risk
  - if everything is a priority, nothing is a priority
- Early detection is the key
  - perfect security is not the goal
  - the goal should be to minimize impact
- Most people get lost with big, lengthy and detailed recommendations
  - once you are convinced you need them, then they are a good guidance on how to implement a control/detection

- Top **protection** measures mentioned by specialists
  - Multifactor Authentication (MFA)
  - Patches, specially in edge devices
  - Network segmentation
  - Identity Management
    - too many privileges
    - abandoned accounts
- Top **detection** measures mentioned by specialists
  - Monitor edge devices and identity
    - identity on premises and on the cloud
  - Detect exfiltration early
    - Outgoing network monitoring (NetFlows)
      - data leak is becoming #1 extortion
      - exfiltration occurs in almost all cases

Protection

Most attacks could be avoided with basic security controls

The same control **could be use** to prevent **distinct phases** of the attack.

Even if it is not possible to avoid Initial Access, **measures** exist **to delay the attack**, **limit the impact** and **increase** the operational **resilience**.

1. Use Multifactor Authentication (MFA)

2. Perform Vulnerability Management
(Prioritize edge devices + CISA KEV)

3. Raise employee awareness
(especially to report potential problems)

4. Use security tools

5. Create and protect backups

6. Reduce the attack surface

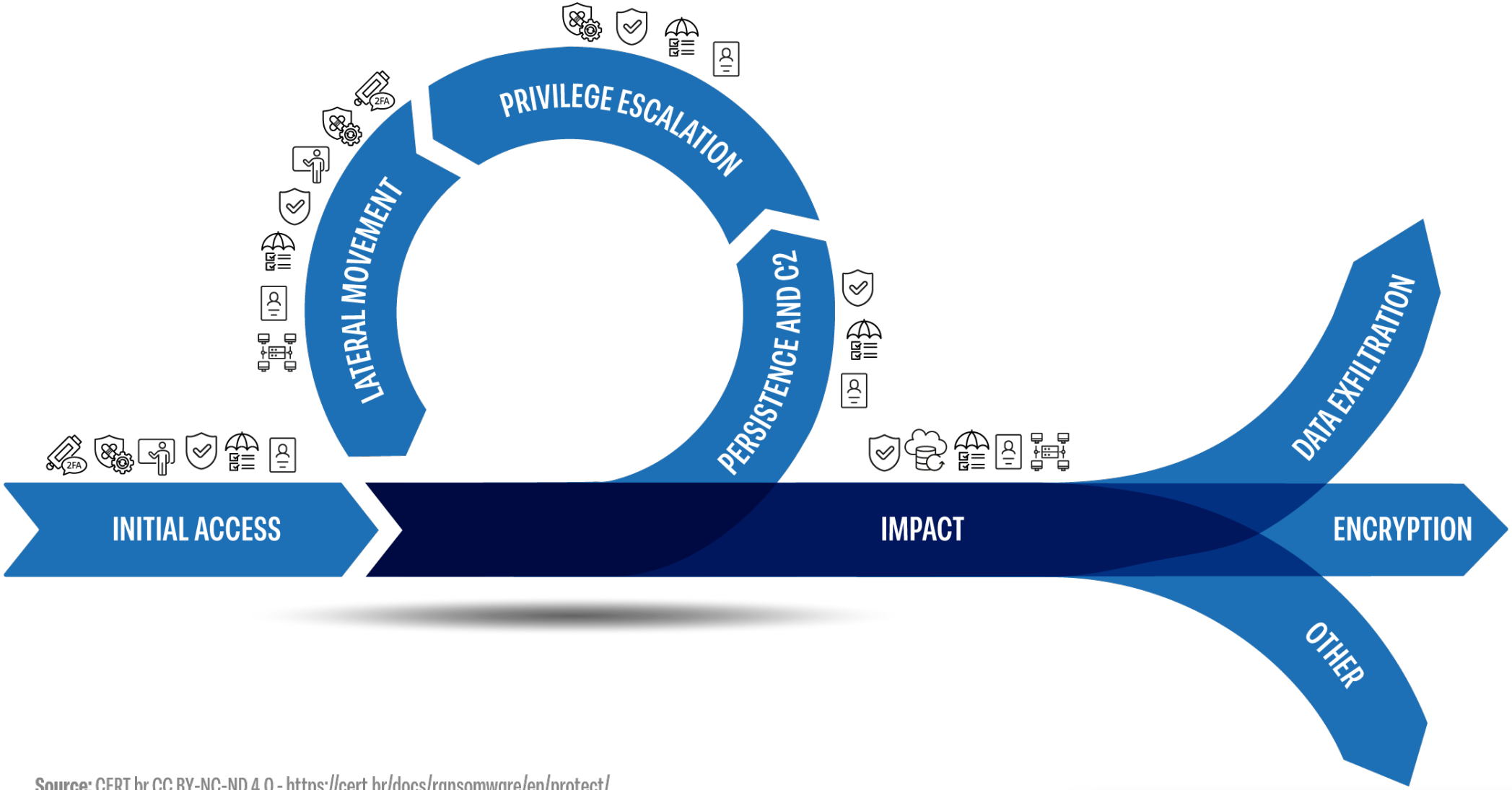
7. Manage identities and access

8. Implement network segmentation

TLP:CLEAR

Protection

A Single Measure can be Used to Defend from Multiple Attacks



Source: CERT.br CC BY-NC-ND 4.0 - https://cert.br/docs/ransomware/en/protect/

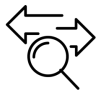
Detection

The sooner the detection occurs, the smaller the impact

Ransomware attacks can be **detected in different phases**, in **different ways** and with **varying levels of detail**.

It is essential to **previously prepare** the environment **to monitor and detect** the activities.

1. Enable and analyze logs



2. Monitor network traffic

3. Watch for alerts coming from security tools

4. Monitor user and administrator accounts

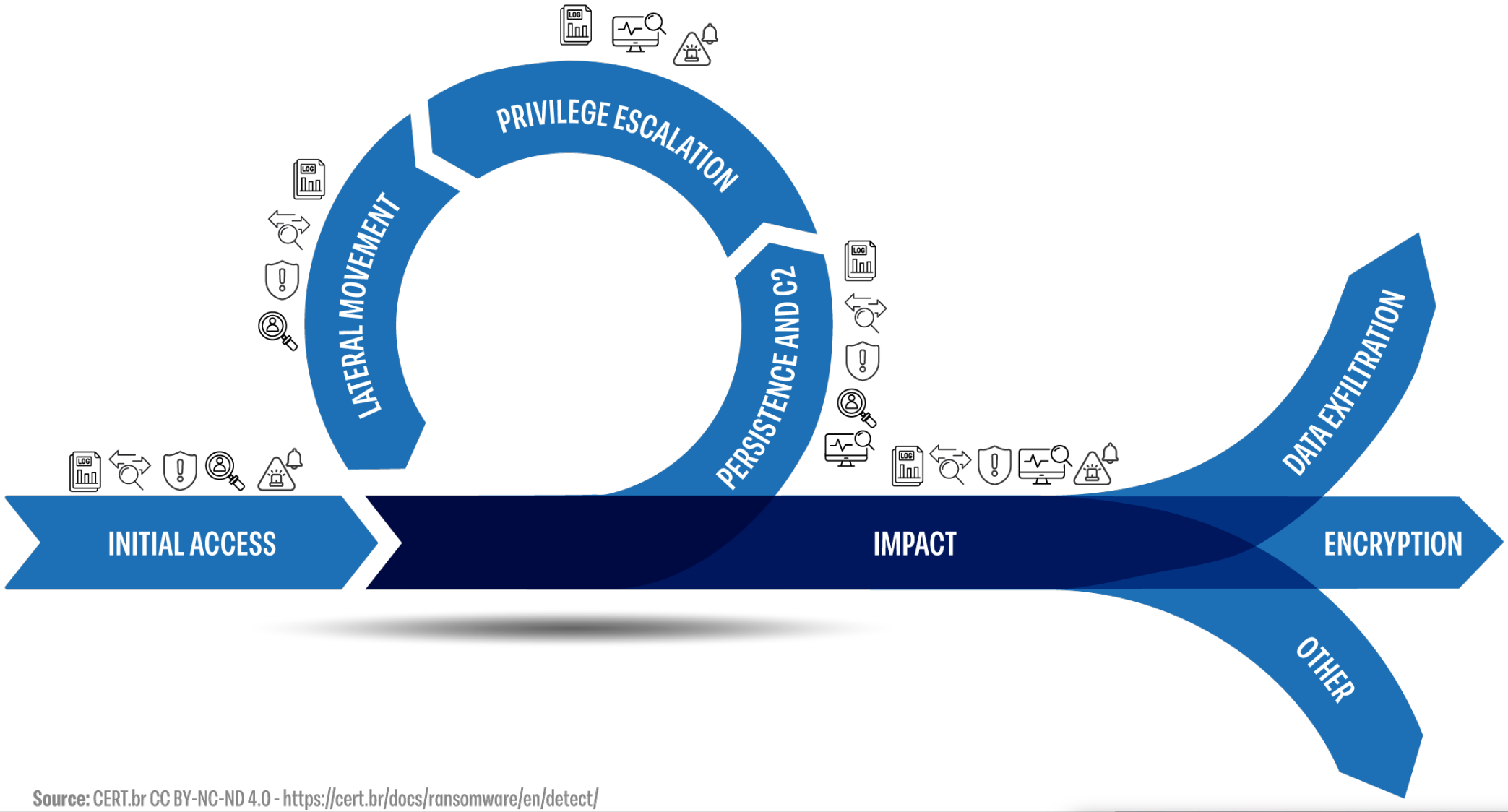
5. Monitor the use of systems

6. Establish a channel to receive security notifications

TLP:CLEAR

Detection

Each phase offers opportunities to detect and stop the attacker



Final thoughts

A simple message matters

Impressions from direct contact with business owners after presenting at an Industry Federation event

- complex words, jargon and too many details shut them down
- simple metaphors help with the “why” message
  - e.g. comparing digital security measures, with those at “brick and mortar” facilities

Bonus:

- Check the new CISA BOD 26-04: “Prioritizing Security Updates Based on Risk”

Dissemination partners are key

- Federal Government
  - CTIR Gov-BR
  - GOV.br Security Awareness Portal
  - Federal Police
- State Governments
  - IT Coordinators for Tocantins and Paraíba
  - Mato Grosso State Police
- Industry organizations
  - Sescon, Fenacon, Fieto
- Health insurance provider Unimed
- LACNIC CSIRT (Spanish translation)

Patch Smarter, Not Harder: https://www.cisa.gov/news-events/news/patch-smarter-not-harder
CISA BOD 26-04: https://www.cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk

Feel Free to Use our Materials!

TLP:CLEAR

Thank You!

@ Incident reports to: cert@cert.br 𝕏 @certbr

https://cert.br/

https://cert.br/docs/ransomware/

nic.br cgi.br

www.nic.br | www.cgi.br