Ransomware Attack Prevention, Detection, and Response: The Essentials That Can Make a Difference

Lucimara Desiderá, M.Sc. CISSP
Security Analyst
CERT.br/NIC.br

2025 FIRST Regional Symposium Latin America & Caribbean
San Salvador, El Salvador - October 8-9, 2025

cert.br nic.br cgi.br

Ransomware Evolution

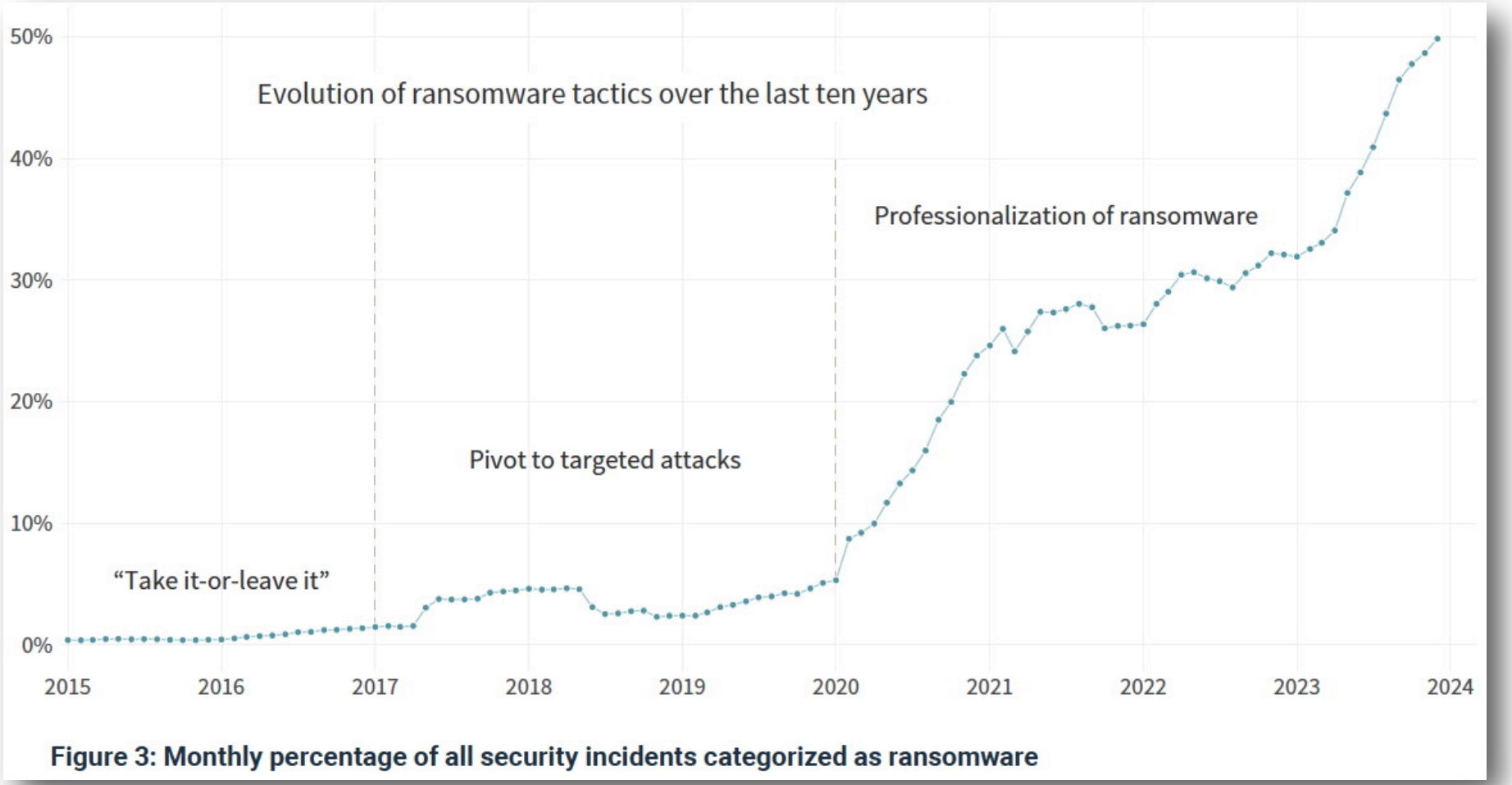
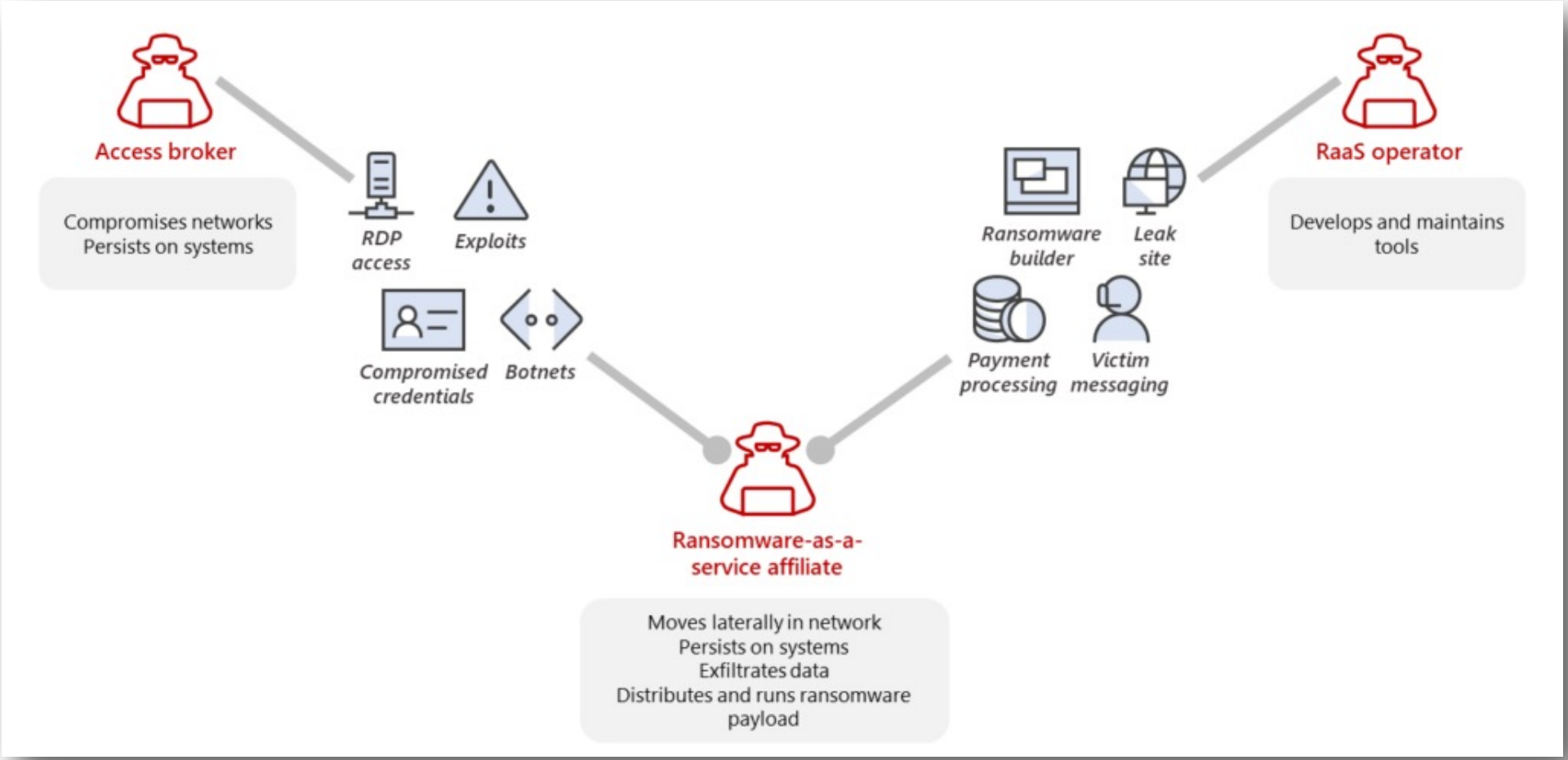


Figure 3: Monthly percentage of all security incidents categorized as ransomware

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

Ransomware as a Service – RaaS

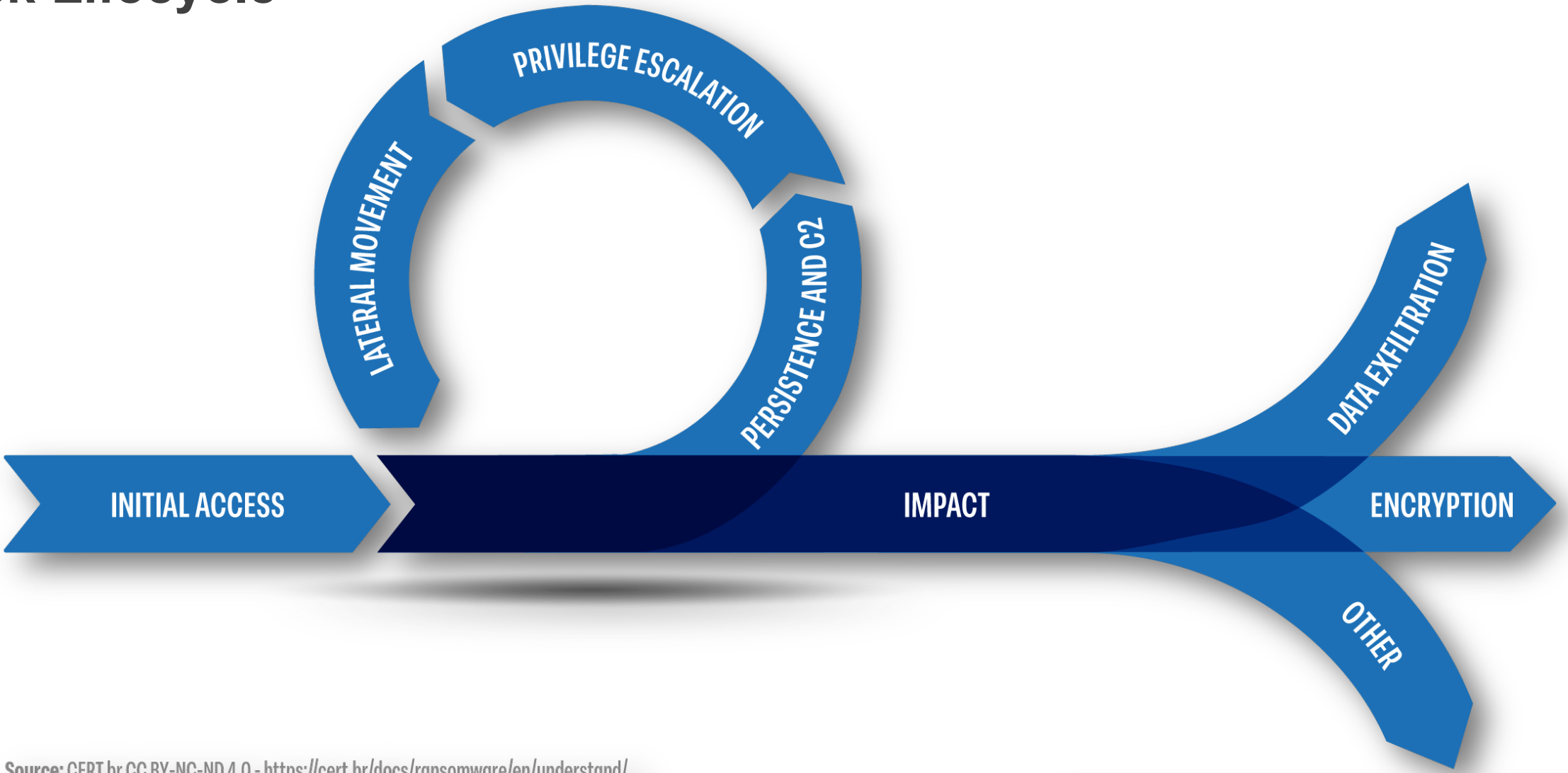


Fonte: https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

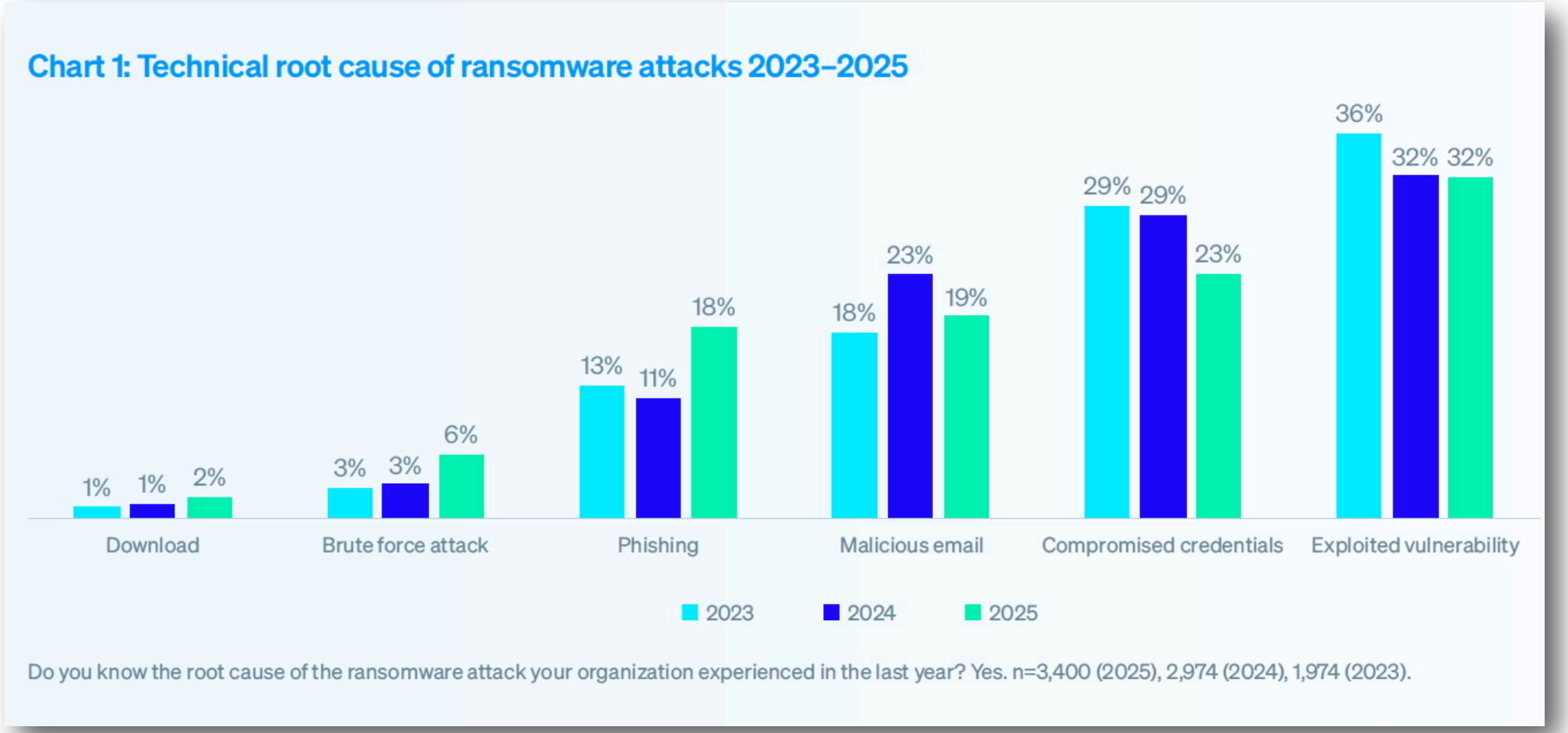
TLP:CLEAR

Ransomware: How it Happens

Attack Lifecycle



Root Cause



Fonte: https://www. sophos.com/pt-br/content/state-of-ransomware

TLP:CLEAR

CYBERSECURITY ADVISORY

#StopRansomware: RansomHub Ransomware

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

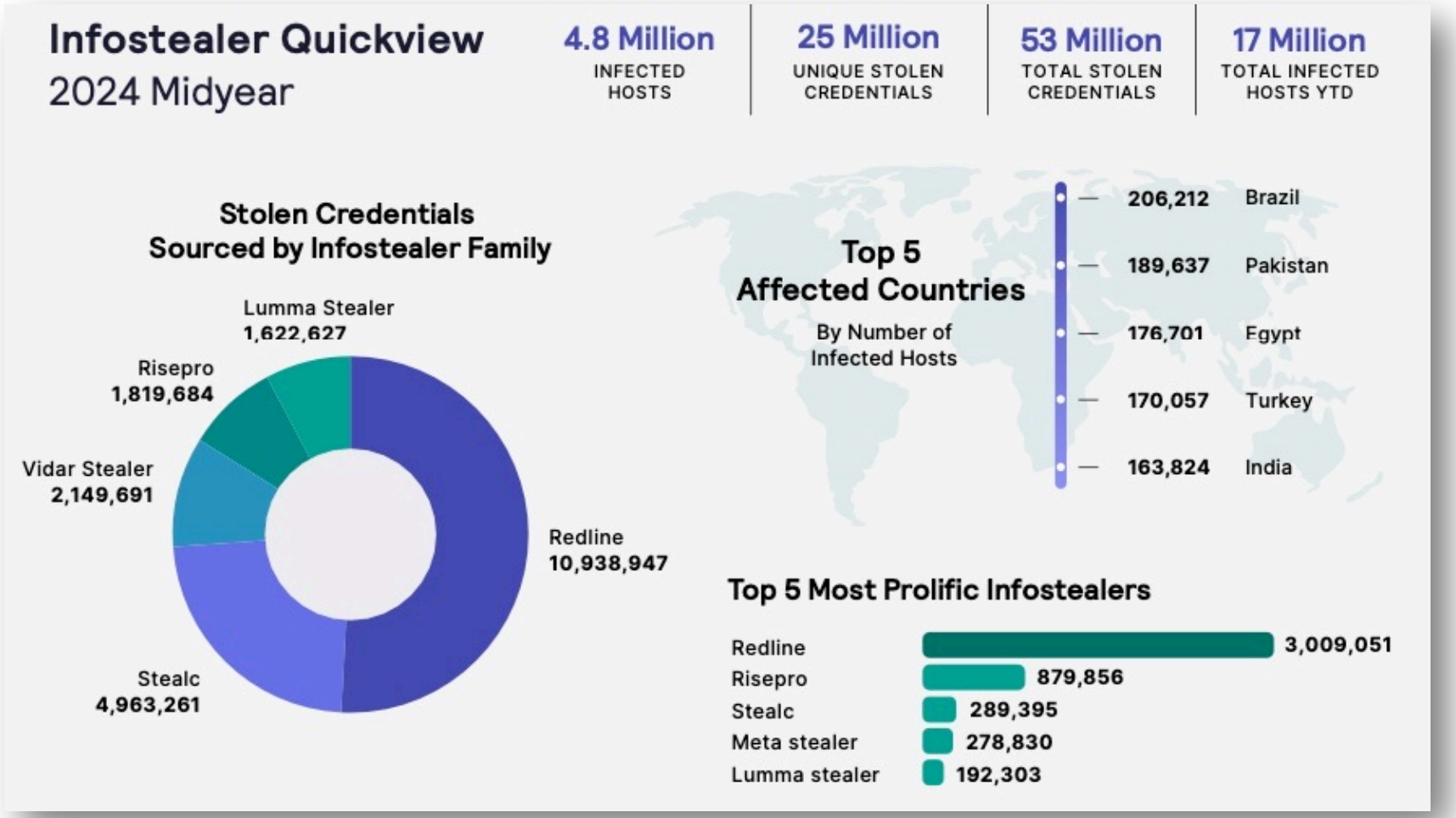
Initial Access

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].

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

Root Cause



Fonte: https://go.flashpoint.io/ransomware_survival_guide

What are The Essentials That Can Make a Difference

cert.br nic.br cgi.br

TLP:CLEAR

Complete Document and Leaflet

Home > Publications > Ransomware (EN)

Ransomware: Best Practices for Protection, Detection, and Response

In the 4 parts of this document, you will find a description of **how a ransomware attack occurs** and best practices for **protecting** against, **detecting**, and **responding** to these attacks.

"Ransomware: How to Protect" Brochure

Find here a brochure summarizing all parts of the document as well as all the infographics in PNG and SVG formats.

Digital Format in Low and High Resolutions

- » Download the low resolution PDF here
- » Download the high resolution PDF here

Format for Printing in Printing Shops

- » Download the PDF here

Infographics in PNG format

- » Infographic "Ransomware: How It Happens"
- » Infographic "Ransomware: How to Protect"
- » Infographic "Ransomware: How to Detect"
- » Infographic "Ransomware: How to Respond"

Infographics in SVG format

- » Infographic "Ransomware: How It Happens"
- » Infographic "Ransomware: How to Protect"
- » Infographic "Ransomware: How to Detect"
- » Infographic "Ransomware: How to Respond"

Part 1: Ransomware: How It Happens

Understanding how ransomware attacks occur helps determine protection, detection, and incident response measures. This document explains the RaaS (Ransomware as a Service) model and the attack phases.

» Read it here

Part 2: Ransomware: How to Protect

This document presents a layered defense strategy, with multiple, complementary security measures. Thus, even if it's not possible to completely prevent an attack, it's possible to take steps to slow it down, limit its impact, and increase operational resilience.

» Read it here

Part 3: Ransomware: How to Detect

This document presents ways to detect ransomware attacks at different stages, in different ways, and with varying levels of detail. The earlier the detection occurs, the less impact it will have on the organization and, consequently, less effort is required for response.

» Read it here

Part 4: Ransomware: How to Respond

This document outlines the minimum steps for responding to a ransomware attack, covering how to contain its spread, eliminate the attacker's presence, eradicate the root cause of the intrusion, restore the environment, and return to normal operation.

» Read it here

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

Also Available in Spanish!

nic.br | cert.br

Sobre CSIRTs Cursos Publicações Palestras Estatísticas

Início > Publicações > *Ransomware* (ES)

Ransomware: mejores prácticas para protección, detección y respuesta

En las cuatro partes de este documento encontrará una descripción de **cómo se producen los ataques de *ransomware***, así como mejores prácticas para **protegernos**, **detectarlos** y **responder** ante estos ataques.

Apoyo de difusión: lacnic csirt

Folleto "*Ransomware*: cómo protegernos"

Encuentre aquí un folleto que resume todas las partes del documento, así como las infografías en formatos PNG y SVG.

Formato digital y para imprimir

- Descargue el PDF en línea aquí
- Descargue el PDF alta resolución aquí

Formato para imprenta

- Descargue el PDF aquí

Infografías en formato PNG

- Infografía *Ransomware*: cómo se produce
- Infografía *Ransomware*: cómo protegernos
- Infografía *Ransomware*: cómo detectarlo
- Infografía *Ransomware*: cómo responder

Infografías en formato SVG

- Infografía *Ransomware*: cómo se produce
- Infografía *Ransomware*: cómo protegernos
- Infografía *Ransomware*: cómo detectarlo
- Infografía *Ransomware*: cómo responder

Parte 1: *Ransomware*: cómo se produce

Comprender cómo se producen los ataques de *ransomware* ayuda a definir medidas de protección, detección y respuesta ante estos incidentes. Este documento explica el modelo RaaS (*Ransomware as a Service*) y las fases de un ataque.

» Consultar el documento

Parte 2: *Ransomware*: cómo protegernos

Este documento presenta una estrategia de defensa por capas que incluye numerosas medidas de seguridad complementarias. De este modo, si bien no siempre es posible prevenir completamente un ataque, sí podemos tomar medidas para ralentizarlo, limitar su impacto y aumentar la resiliencia operativa.

» Consultar el documento

Parte 3: *Ransomware*: cómo detectarlo

Este documento presenta métodos para detectar ataques de *ransomware* en diferentes fases, de distintas formas y con diversos niveles de detalle. Cuanto antes se detecte, menor será el impacto en la empresa y, por lo tanto, en los esfuerzos de respuesta.

» Consultar el documento

Parte 4: *Ransomware*: cómo responder

Este documento detalla los pasos mínimos para responder a un ataque de *ransomware* y describe cómo contener su propagación, eliminar la presencia del atacante, erradicar la causa raíz de la intrusión, restaurar el entorno y reanudar la operación normal.

» Consultar el documento

RANSOMWARE: CÓMO PROTEGERNOS

Descubra cómo funcionan los ataques, cómo proteger su red y prepararla para detectarlos, y cómo responder en caso de convertirse en víctima.

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

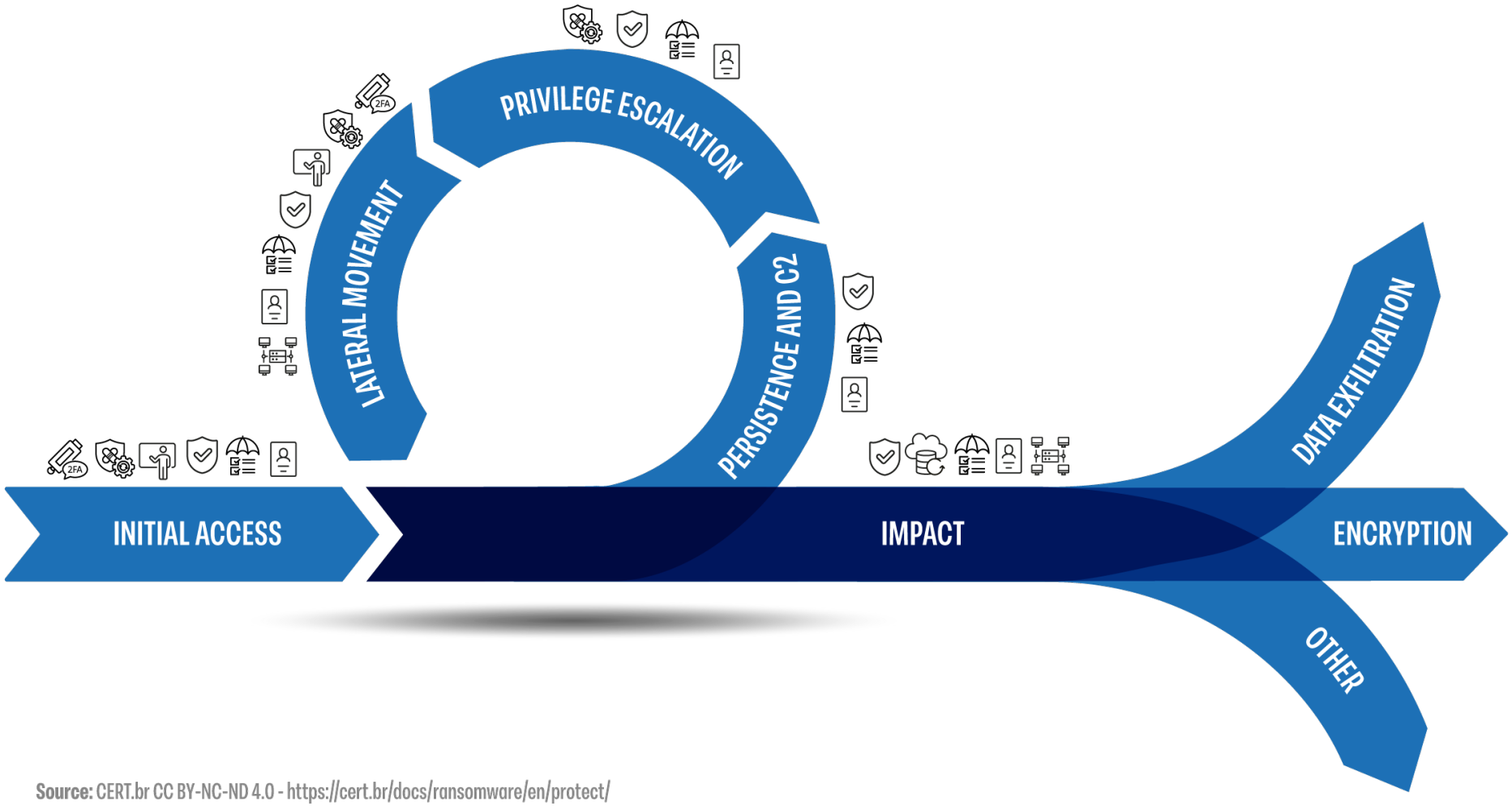
Apoyo de difusión: lacnic csirt

Producción: cert.br

Better Safe Than Sorry

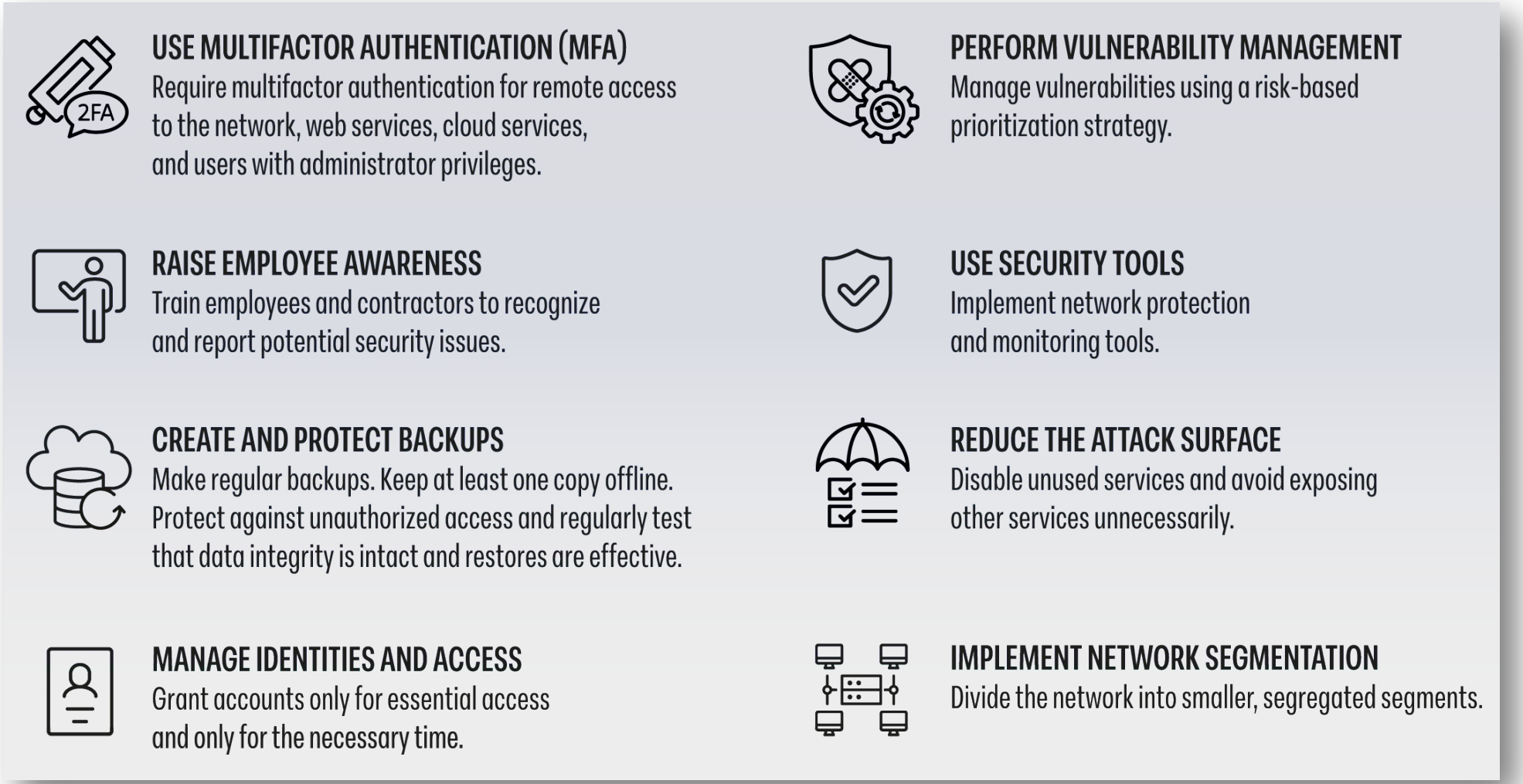
cert.br nic.br cgi.br

Prevention: The Essentials That Can Make a Difference



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

Prevention: The Essentials That Can Make a Difference



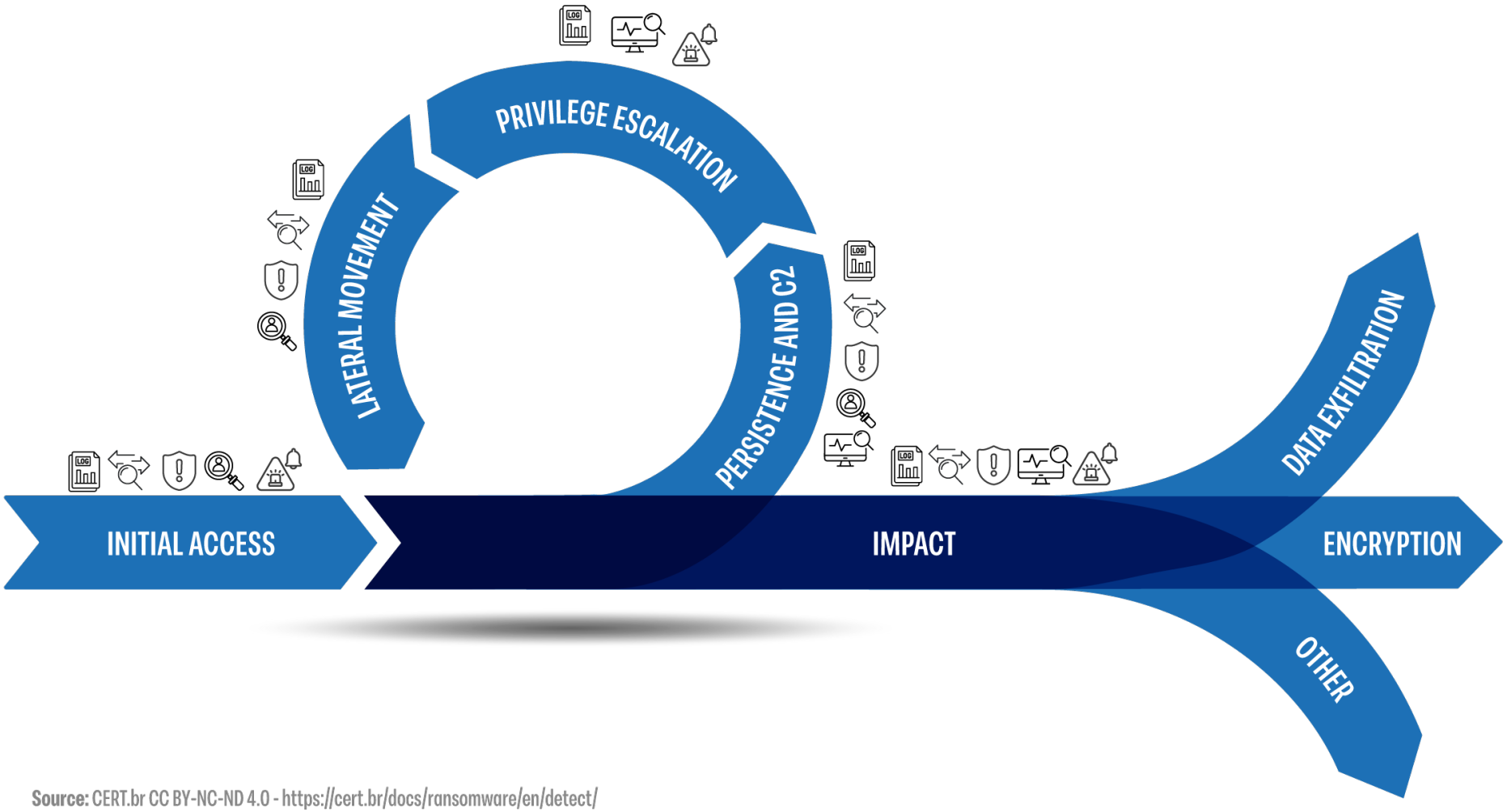
Fonte: CERT.br CC BY-NC-ND 4.0 - https://cert.br/docs/ransomware/en/protect/

What If Initial Access Cannot Be Prevented?

cert.br nic.br cgi.br

Detection – The Essentials That Can Make a Difference
Layered Defense

TLP:CLEAR



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

TLP:CLEAR

Detection – The Essentials That Can Make a Difference

The earlier the detection, the quicker the response

ENABLE AND ANALYZE LOGS

Enable and analyze logs generated on equipment and systems.
Enable Netflows on network devices and firewalls.

MONITOR NETWORK TRAFFIC

Monitor incoming and outgoing Internet traffic, and internal traffic between organization networks.

WATCH FOR ALERTS COMING FROM SECURITY TOOLS

Monitor security tool alerts to detect suspicious activity and, if possible, block it.

MONITOR USER AND ADMINISTRATOR ACCOUNTS

Monitoring the creation of user and administrator accounts, and any unauthorized access to them.

MONITOR THE USE OF SYSTEMS

Monitor the use of systems to detect changes in configurations, data transfer and encryption, and the installation of malware and remote access tools.

ESTABLISH A CHANNEL TO RECEIVE SECURITY NOTIFICATIONS

Have a public contact to receive security notifications from people both external and internal to the organization.

TLP:CLEAR

Response: It's Necessary to be Prepared

The faster the response, the lesser the impact

1. 

FOLLOW THE INCIDENT RESPONSE PLAN
Define roles and train contacts to be involved in the response.
Document the actions taken and the information collected.

2. 

CONTAIN THE ATTACK
Protect uncompromised systems. Isolate affected systems.
Preserve evidence.

3. 

IDENTIFY THE RANSOMWARE
Determine the ransomware involved in the attack and understand its behavior.

4. 

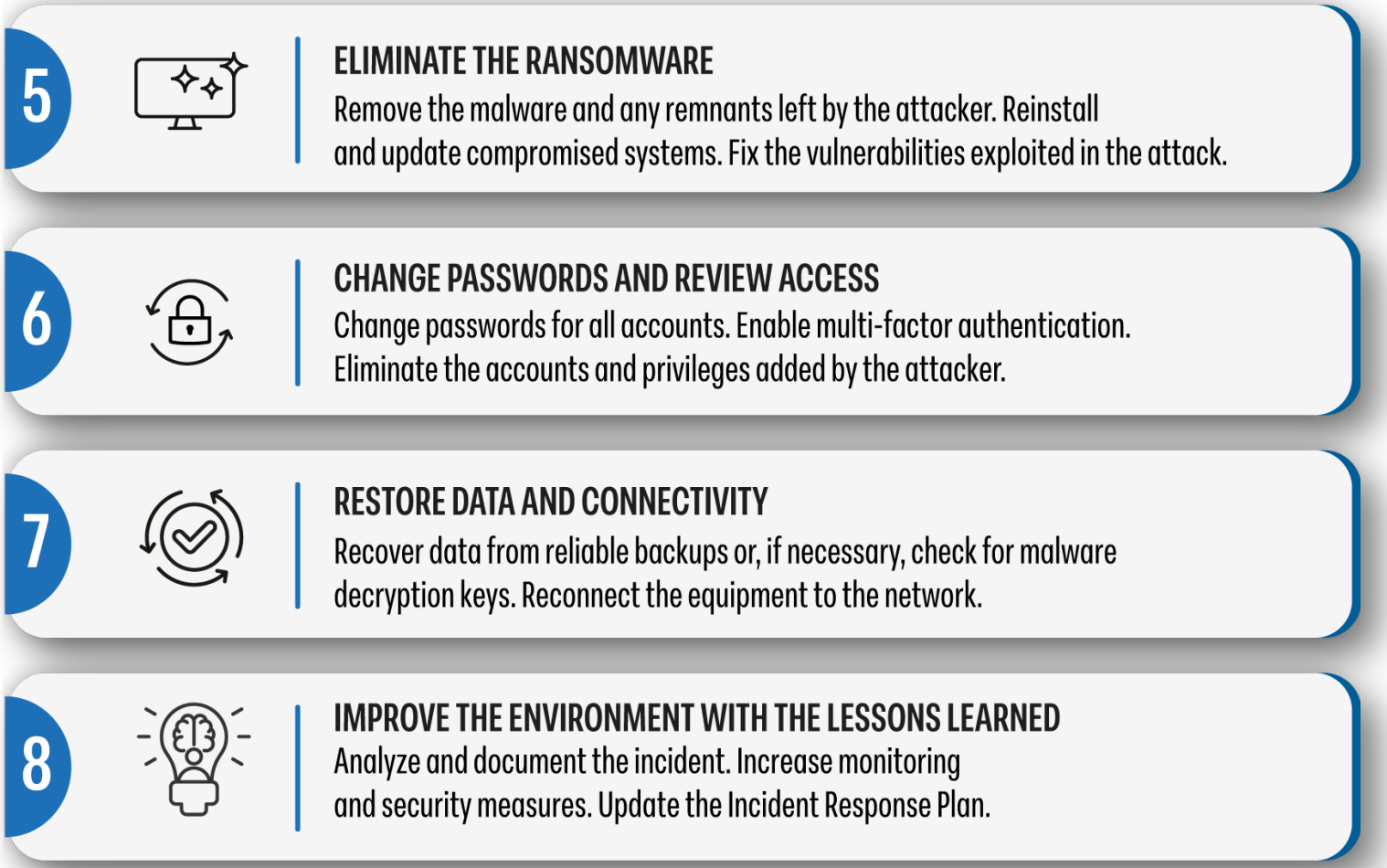
ANALYZE THE COLLECTED INFORMATION
Cross-reference the logs and evidence with the ransomware information.
Determine the root cause and extent of the attack.

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

TLP:CLEAR

Response: It's Necessary to be Prepared

The faster the response, the lesser the impact



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

Thank you!

Incident reports to : cert@cert.br @certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br