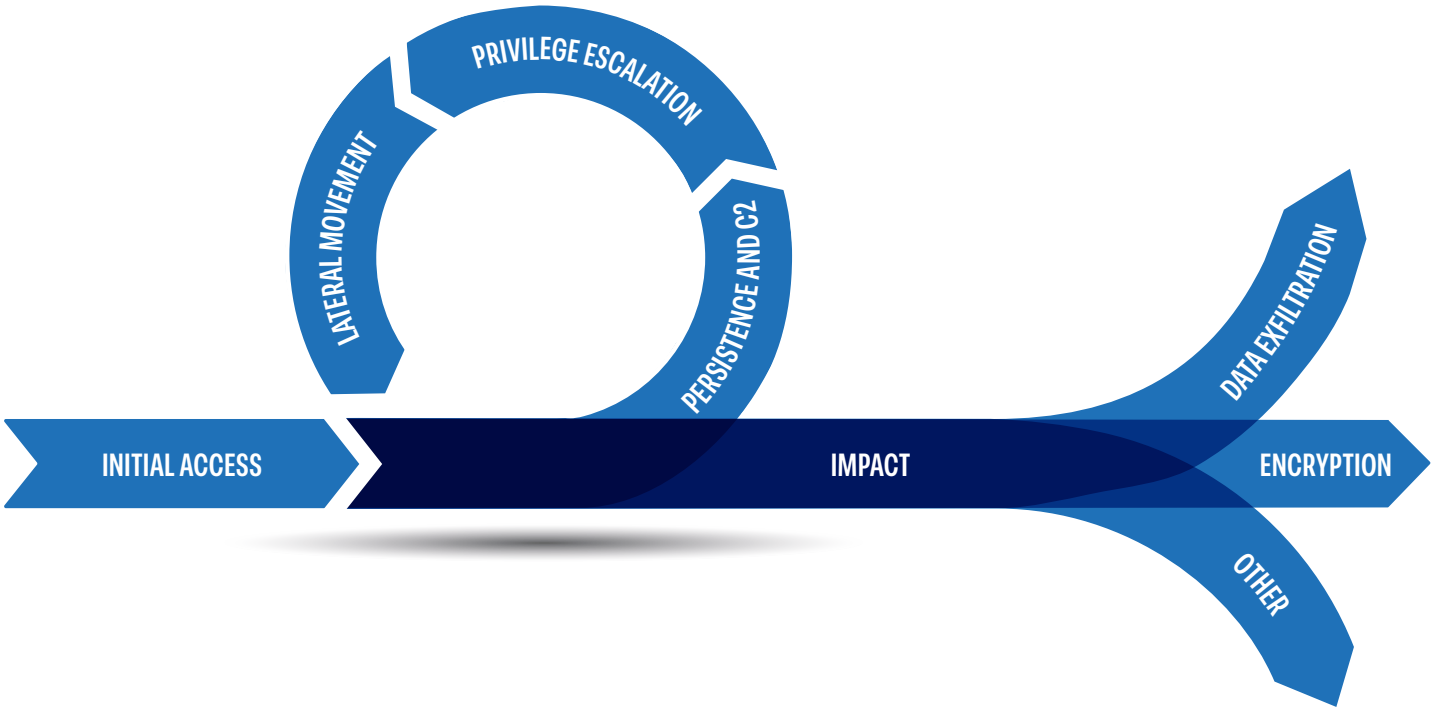
RANSOMWARE:
HOW TO PROTECT

Understand how it happens, how to protect your network and prepare the environment for detection, and how to respond if you become a victim.

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

cert.br

RANSOMWARE: HOW IT HAPPENS



INITIAL ACCESS
The attacker breaches the organization's network using compromised credentials, exploiting software vulnerabilities, using social engineering, or installing malware.

PERSISTENCE AND C2
The attacker establishes persistent access and communication mechanisms between the compromised system and the Command and Control (C2) infrastructure.

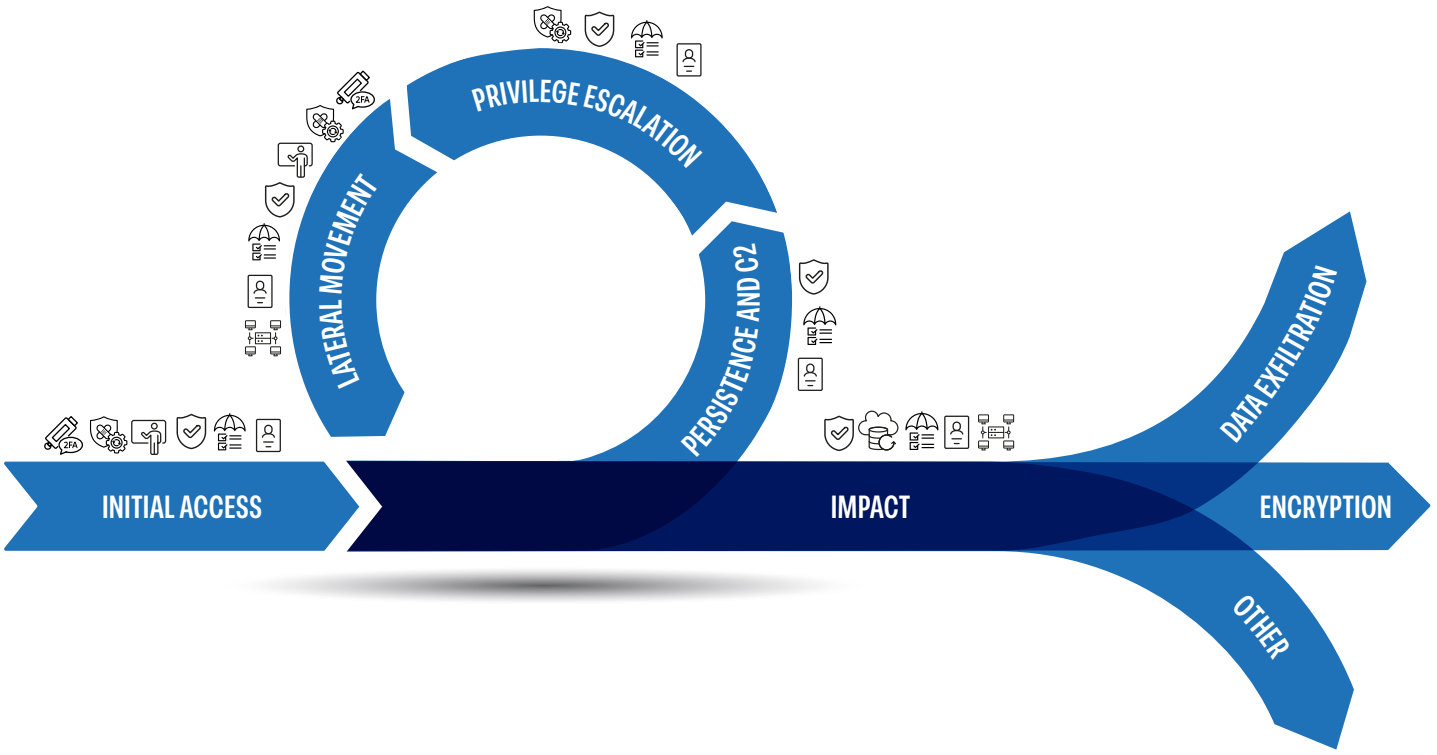
PRIVILEGE ESCALATION
The attacker obtains elevated permissions to perform administrator activities, access sensitive data, and move laterally within the network.

LATERAL MOVEMENT
The attacker moves through the network, gains access to critical systems and data, and propagates the ransomware (malware) throughout the environment to encrypt assets in the Impact phase.

IMPACT
The attacker causes maximum impact to pressure the organization into paying the ransom. The most common techniques are encryption and data exfiltration.

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

RANSOMWARE: HOW TO PROTECT



USE MULTIFACTOR AUTHENTICATION (MFA)
Require multifactor authentication for remote access to the network, web services, cloud services, and users with administrator privileges.

RAISE EMPLOYEE AWARENESS
Train employees and contractors to recognize and report potential security issues.

CREATE AND PROTECT BACKUPS
Make regular backups. Keep at least one copy offline. Protect against unauthorized access and regularly test that data integrity is intact and restores are effective.

MANAGE IDENTITIES AND ACCESS
Grant accounts only for essential access and only for the necessary time.

PERFORM VULNERABILITY MANAGEMENT
Manage vulnerabilities using a risk-based prioritization strategy.

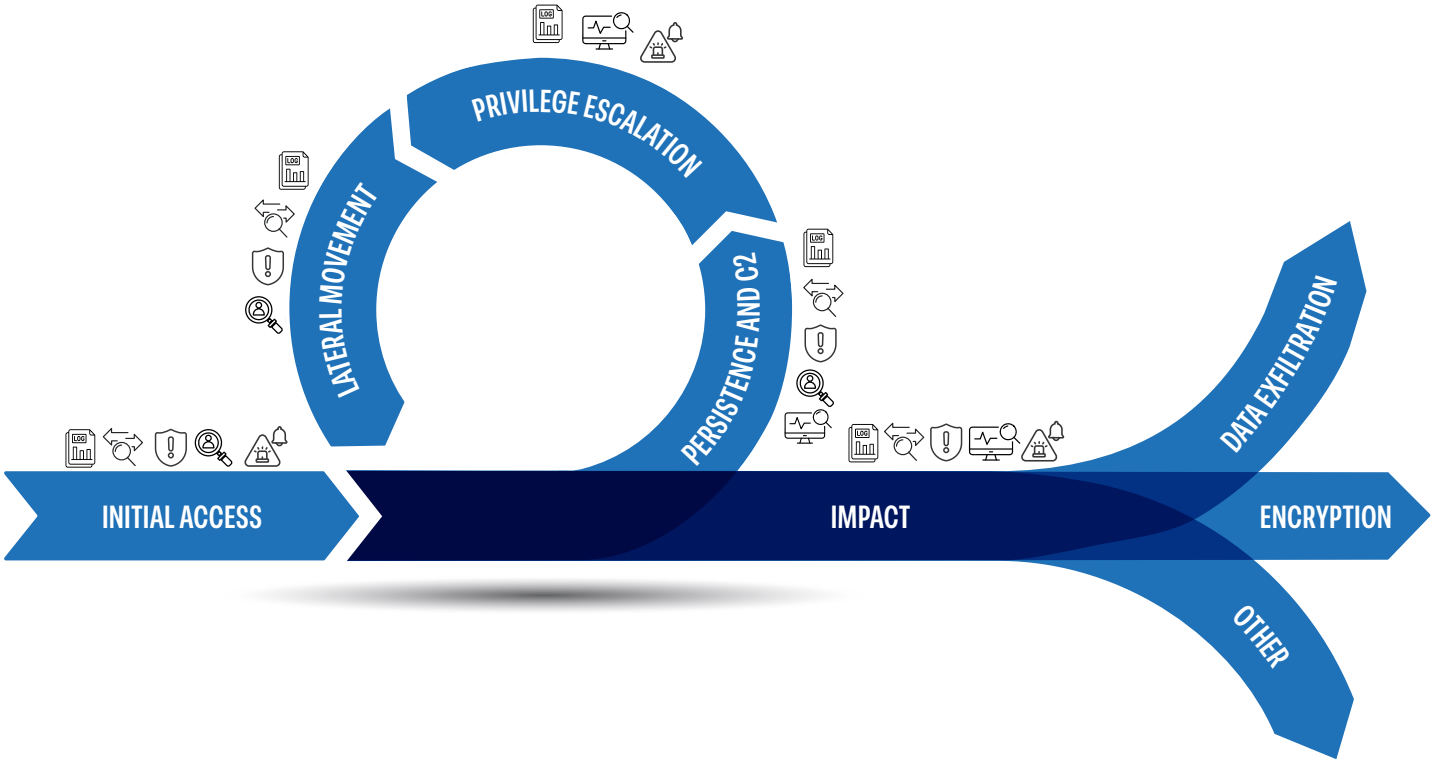
USE SECURITY TOOLS
Implement network protection and monitoring tools.

REDUCE THE ATTACK SURFACE
Disable unused services and avoid exposing other services unnecessarily.

IMPLEMENT NETWORK SEGMENTATION
Divide the network into smaller, segregated segments.

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

RANSOMWARE: HOW TO DETECT



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.

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

RANSOMWARE: HOW TO RESPOND

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.

5

ELIMINATE THE RANSOMWARE

Remove the malware and any remnants left by the attacker. Reinstall
and update compromised systems. Fix the vulnerabilities exploited in the attack.

6

CHANGE PASSWORDS AND REVIEW ACCESS

Change passwords for all accounts. Enable multi-factor authentication.
Eliminate the accounts and privileges added by the attacker.

7

RESTORE DATA AND CONNECTIVITY

Recover data from reliable backups or, if necessary, check for malware
decryption keys. Reconnect the equipment to the network.

8

IMPROVE THE ENVIRONMENT WITH THE LESSONS LEARNED

Analyze and document the incident. Increase monitoring
and security measures. Update the Incident Response Plan.

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

cert.br

CERT.br (**https://cert.br/**) is the Brazilian National Computer Emergency Response Team of Last Resort, maintained by NIC.br. In addition to incident management, it also works on raising awareness about security issues, situational awareness, and knowledge transfer, always backed by strong integration with the national and international CSIRT communities.

nic.br

The Brazilian Network Information Center – NIC.br (**https://nic.br/**) is a nonprofit entity that is in charge of the operations related to the .br domain, as well as the allocation of IP numbers and the registration of autonomous systems in the country. It takes actions and conducts projects that are of benefit to the infrastructure of the Internet in Brazil.

English translation technical review: Merike Käo, DoubleShot Security.

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

september / 2025