

Prevenção, Detecção e Resposta a Ataques de *Ransomware*: O Básico que Pode Fazer a Diferença?

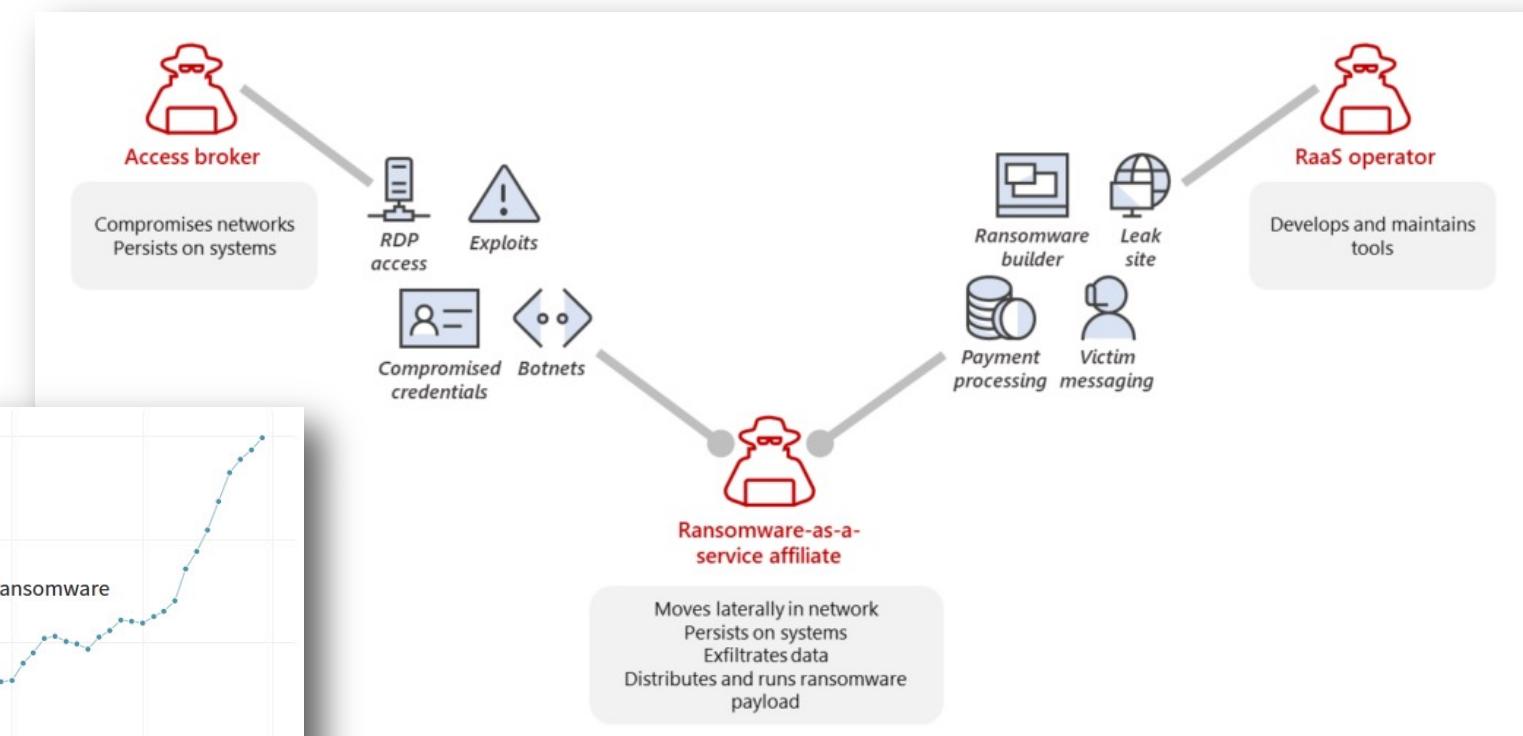
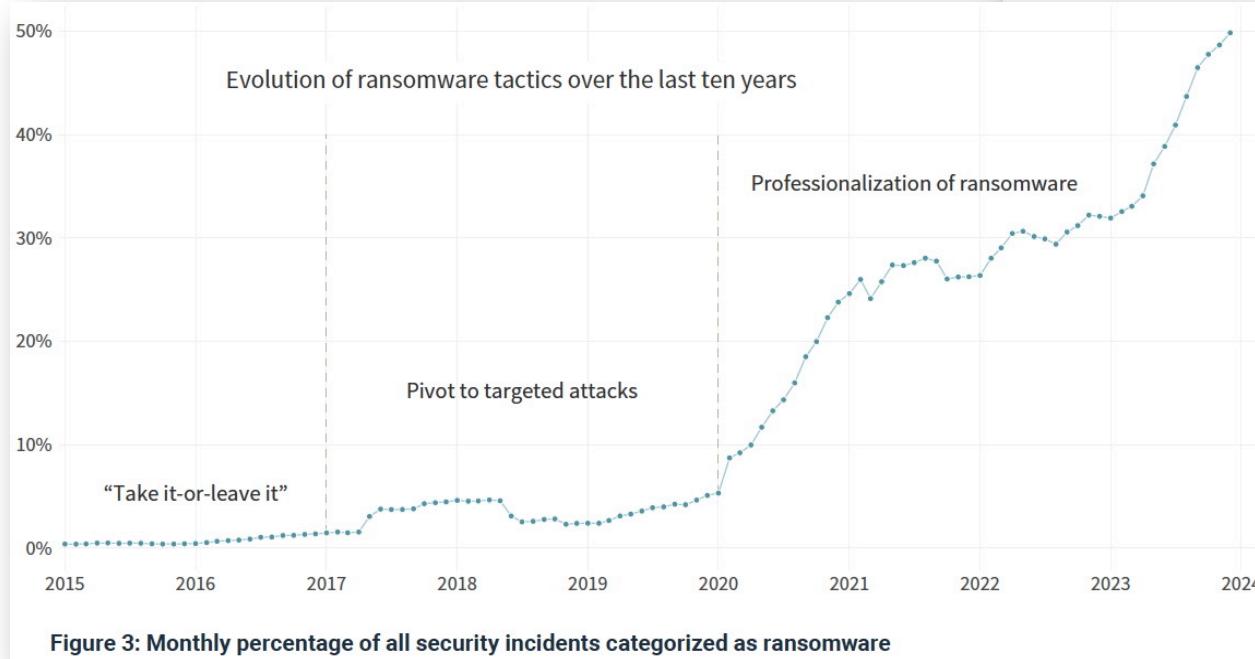
Lucimara Desiderá
Analista de Segurança
CERT.br/NIC.br

Miriam von Zuben
Analista de Segurança
CERT.br/NIC.br

GTS 40 - 15 de dezembro de 2025
São Paulo - SP

cert.br **nic**.br **egi**.br

Evolução do Ransomware

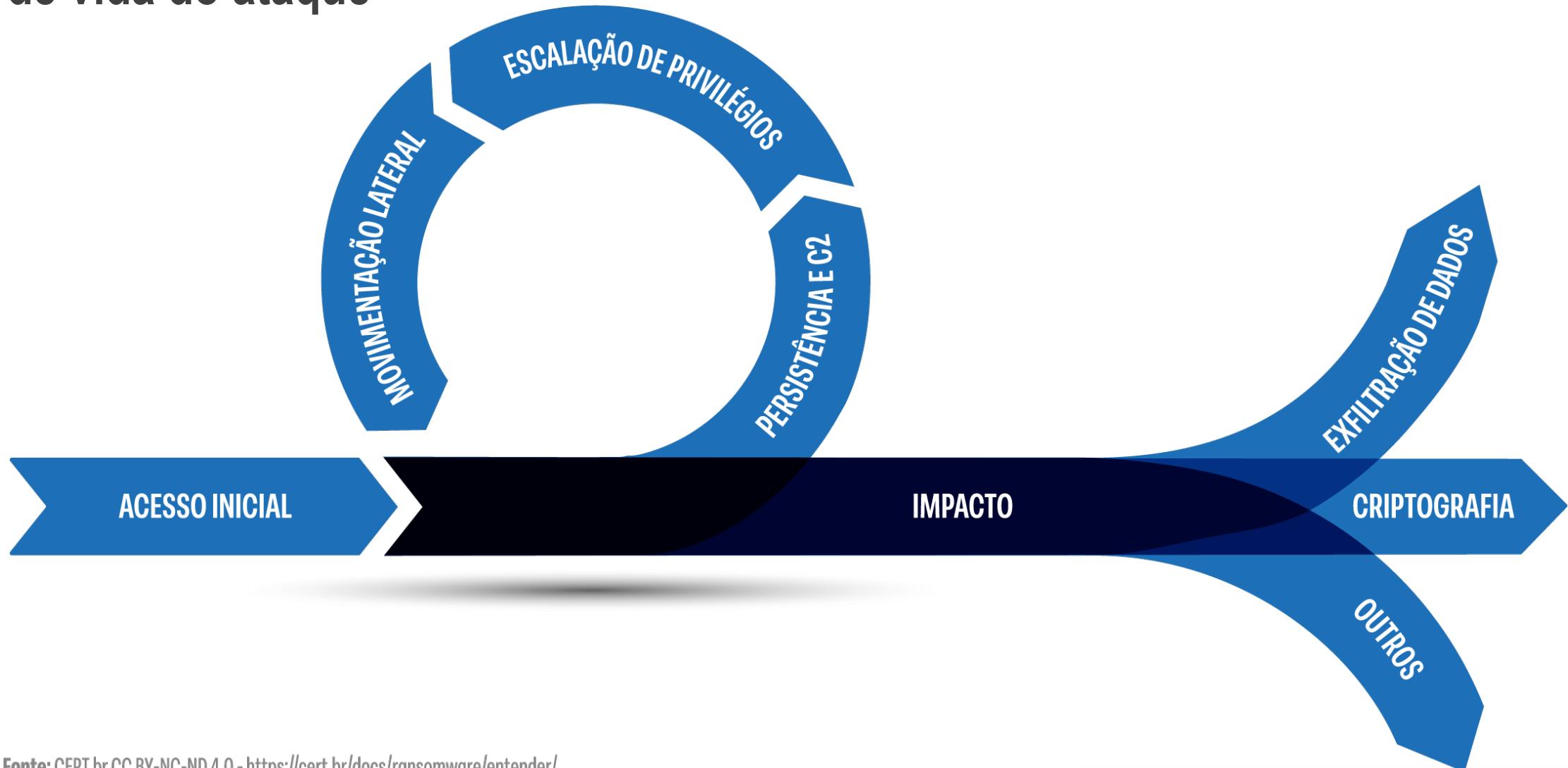


Fonte: <https://www.cyentia.com/iris-ransomware/>

<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/>

Ransomware: Como Acontece

Ciclo de vida do ataque



Fonte: CERT.br CC BY-NC-ND 4.0 - <https://cert.br/docs/ransomware/entender/>



Acesso Inicial

● ACESSO INICIAL

Atacante tenta invadir a rede da empresa.

- PERSISTÊNCIA E C2
- ESCALAÇÃO DE PRIVILÉGIOS
- MOVIMENTAÇÃO LATERAL
- IMPACTO

Principais vetores de invasão:

- Credenciais de acesso remoto comprometidas
 - ex: de VPN e RDP
- Vulnerabilidades de *software*
 - ex: em equipamentos de borda
- *Phishing*
 - ex: por *e-mail* ou mensagem de texto
- *Malware*
 - ex: via anexo de *e-mail* ou *link* patrocinado
- Engenharia social
 - ex: ligação telefônica fingindo ser suporte técnico

Persistência e C2

- ACESSO INICIAL

● PERSISTÊNCIA E C2

Atacante busca estabelecer acesso persistente e mecanismo de comunicação entre o sistema invadido e a infraestrutura de C2.

- ESCALAÇÃO DE PRIVILÉGIOS
- MOVIMENTAÇÃO LATERAL
- IMPACTO

Principais técnicas utilizadas:

- Criação de novas contas
- Modificação de contas existentes
- Instalação de *malware*
 - ex: *backdoor*
- Agendamento de tarefas e *scripts* de inicialização
- Abuso de ferramentas legítimas
 - ex: RDP e SSH

Escalação de Privilégios

- ACESSO INICIAL
- PERSISTÊNCIA E C2

● ESCALAÇÃO DE PRIVILÉGIOS

Atacante tenta obter permissões elevadas.

- MOVIMENTAÇÃO LATERAL
- IMPACTO

Principais técnicas utilizadas:

- Exploração de vulnerabilidades
- Invasão de contas privilegiadas
- Alteração de contas

Movimentação Lateral

- ACESSO INICIAL
- PERSISTÊNCIA E C2
- ESCALAÇÃO DE PRIVILÉGIOS

● MOVIMENTAÇÃO LATERAL

Atacante visa conhecer o ambiente, acessar sistemas críticos e propagar o *ransomware (malware)*.

- IMPACTO

Normalmente utiliza:

- Varreduras de rede
- Credenciais comprometidas
- Vulnerabilidades de *software*
- Ferramentas de acesso remoto
 - ex: RDP e SSH

Impacto

- ACESSO INICIAL
- PERSISTÊNCIA E C2
- ESCALAÇÃO DE PRIVILÉGIOS
- MOVIMENTAÇÃO LATERAL

● IMPACTO

Atacante busca causar danos, para pressionar o pagamento de resgate.

Técnicas mais comuns:

- Exfiltração de dados
- Criptografia de dados
- Destruição de backups

Survey da Sophos

Causas Primárias

Gráfico 1: Causa técnica primária dos ataques de ransomware 2023–2025



Você sabe a causa primária do ataque de ransomware que a sua organização enfrentou no último ano? Sim. n=3.400 (2025), 2.974 (2024), 1.974 (2023).

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

#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>

Melhor Prevenir que Remendar

cert.br **nic**.br **egi**.br

Proteção

Controles Básicos Que Podem Fazer a Diferença

- A maior parte dos ataques poderia ser evitada com **controles básicos**
- Um **mesmo controle** pode ser usado em **fases distintas** do ataque
- Necessidade de adotar estratégia de **defesa em camadas**
 - se não for possível impedir o Acesso Inicial, permite:
 - **retardar** o ataque
 - **limitar** o impacto
 - **aumentar a resiliência** operacional

Proteção Controles Básicos Que Podem Fazer a Diferença



USAR AUTENTICAÇÃO MULTIFATOR (MFA)

Exigir a autenticação multifator, para acesso remoto à rede, serviços web, serviços em nuvem e usuários com privilégios de administrador.



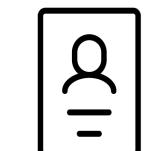
CONSCIENTIZAR FUNCIONÁRIOS

Treinar funcionários e terceiros para reconhecer e reportar potenciais problemas de segurança.



FAZER E PROTEGER BACKUPS

Fazer backups regulares, manter ao menos uma cópia *offline*. Proteger contra acesso indevido e testar regularmente se os dados estão íntegros e a restauração é eficaz.



GERENCIAR IDENTIDADES E ACESSOS

Conceder às contas apenas os acessos essenciais e pelo tempo necessário.



FAZER GESTÃO DE VULNERABILIDADES

Fazer gestão de vulnerabilidades usando estratégia de priorização baseada em risco.



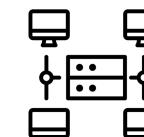
USAR FERRAMENTAS DE PROTEÇÃO

Implementar ferramentas de proteção e de monitoração de rede.



REDUZIR A SUPERFÍCIE DE ATAQUE

Desativar serviços sem uso e não expor os demais desnecessariamente.

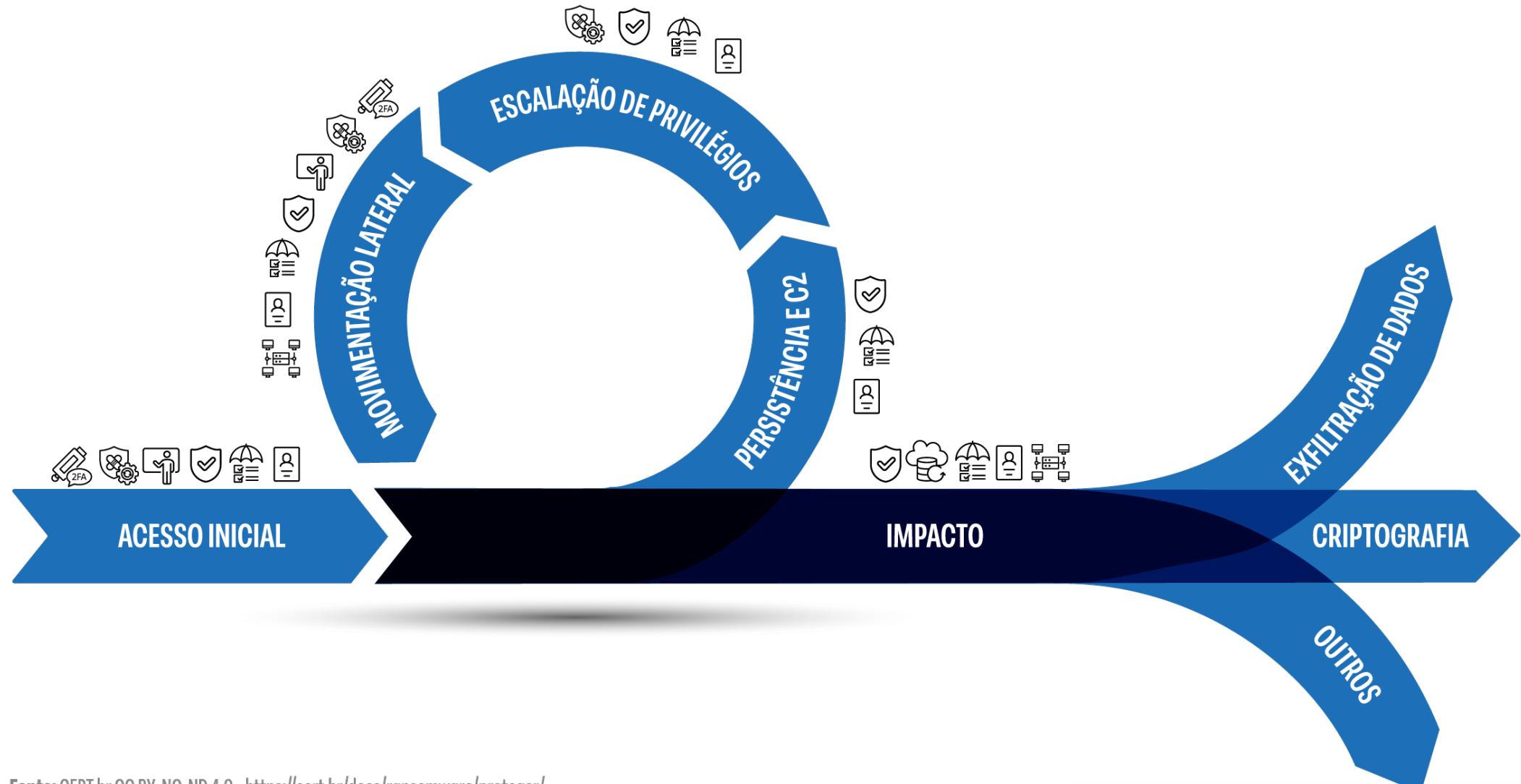


SEGMENTAR A REDE

Dividir a rede em segmentos menores e segregados.

Proteção

Um único Mecanismo Pode ser Usado para Múltiplas Defesas



Fonte: CERT.br CC BY-NC-ND 4.0 - <https://cert.br/docs/ransomware/proteger/>

Estatísticas do CERT.br

Servidores e Dispositivos de Borda Vulneráveis Notificados Mensalmente

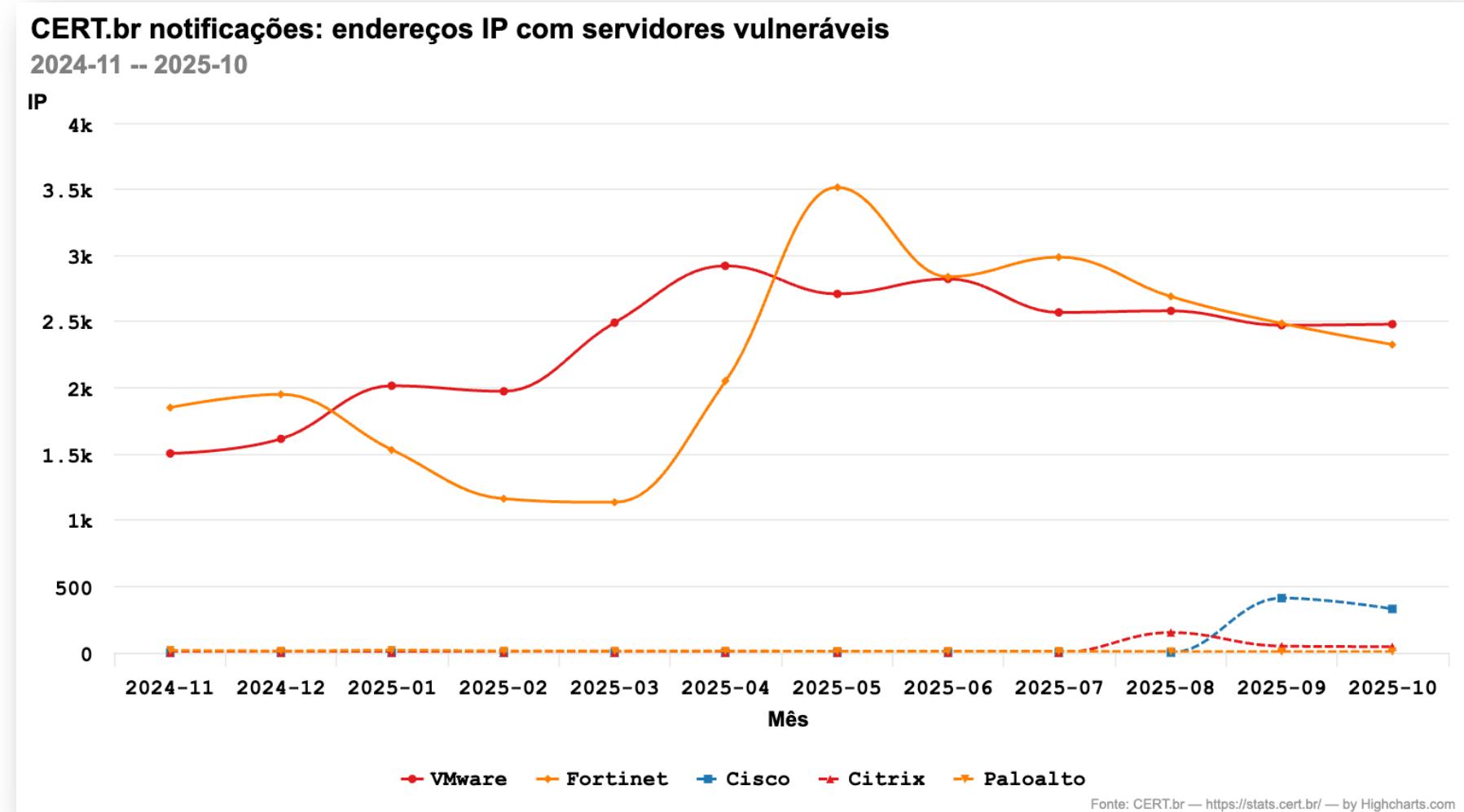
VMware
 - CVEs: 14
 - CISA KEV: 7
 - Usado em ransomware: 4

Fortinet
 - CVEs: 6
 - CISA KEV: 5
 - Usado em ransomware: 4

Cisco
 - CVEs: 3
 - CISA KEV: 2
 - Usado em ransomware: 0

Citrix
 - CVEs: 7
 - CISA KEV: 5
 - Usado em ransomware: 2

Paloalto
 - CVEs: 1
 - CISA KEV: 1
 - Usado em ransomware: 1



Fonte: <https://stats.cert.br/vulns/>

E SE Não For Possível Impedir o Acesso Inicial?

cert.br **nic**.br **egi**.br

Detecção

Detectar o Quanto Antes para Minimizar ou até Evitar o Impacto

- A detecção pode ocorrer:
 - nas diferentes fases
 - de distintas formas
- **Quanto antes detectar, menores serão os impactos**
- É necessário **preparar** o ambiente **para monitorar e detectar** as atividades dos atacantes

Detecção

Detectar o Quanto Antes para Minimizar ou até Evitar o Impacto



HABILITAR E ANALISAR LOGS

Habilitar e analisar os *logs* gerados nos equipamentos e sistemas Em dispositivos de rede e *firewalls*, habilitar também *netflows*.



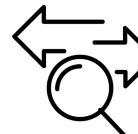
OBSERVAR ALERTAS DE FERRAMENTAS DE PROTEÇÃO

Observar os alertas das ferramentas de proteção, a fim de detectar atividades suspeitas e, se possível, já bloqueá-las.



MONITORAR O USO DE SISTEMAS

Monitorar o uso dos sistemas, a fim de detectar mudança em configurações, transferência e criptografia de dados, e instalação de *malware* e ferramentas de acesso remoto.



MONITORAR O TRÁFEGO DE REDE

Monitorar o tráfego de entrada e de saída da Internet, e o interno entre as redes da própria empresa.



MONITORAR CONTAS DE USUÁRIOS E ADMINISTRADORES

Monitorar a criação e o acesso indevido a contas de usuários e administradores.

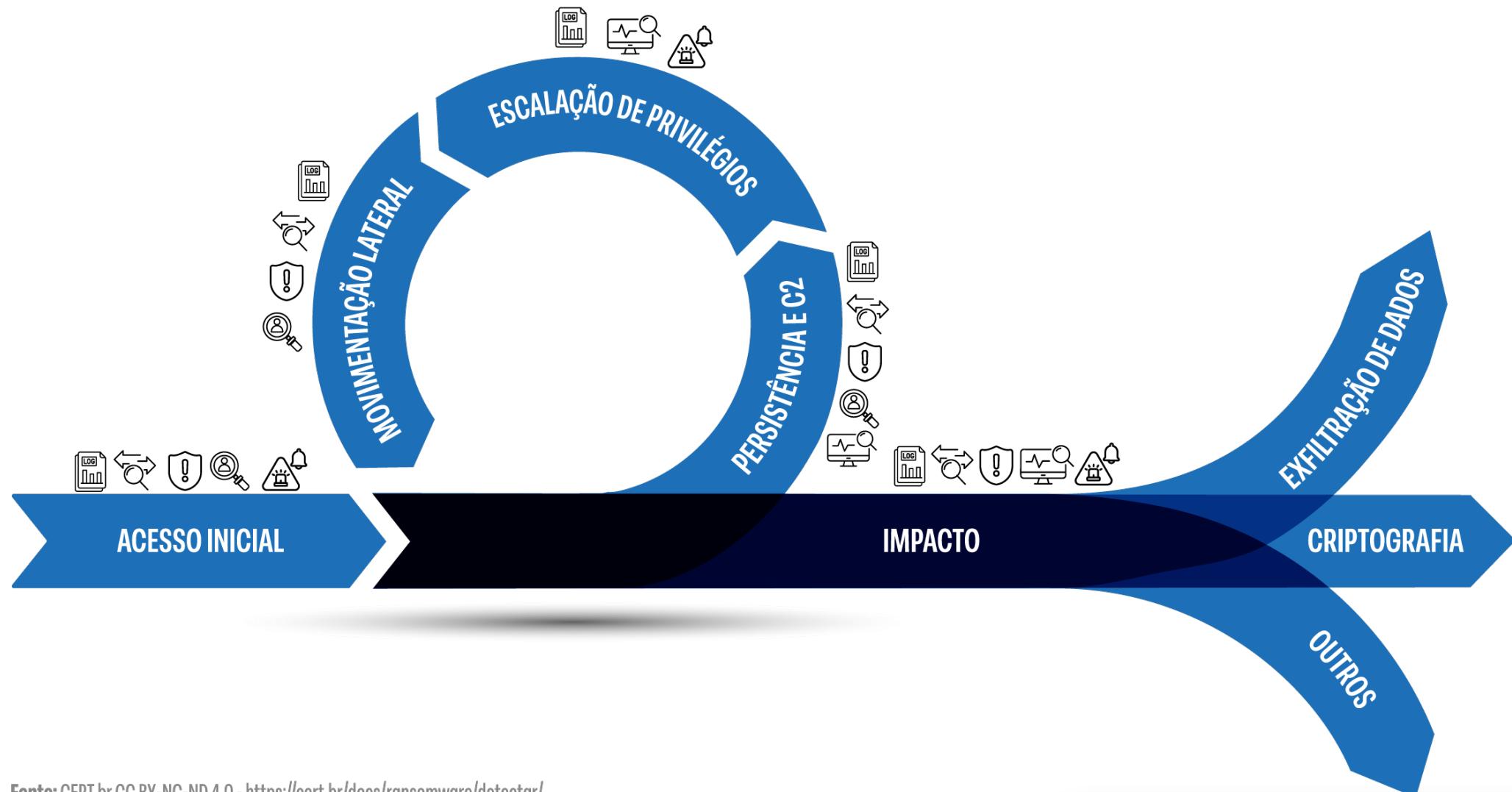


ESTABELECER UM CANAL PARA RECEBER NOTIFICAÇÕES DE SEGURANÇA

Ter um contato divulgado para receber notificações de segurança, de pessoas externas e internas à empresa.

Detecção

Detectar o Quanto Antes para Minimizar ou até Evitar o Impacto



Fonte: CERT.br CC BY-NC-ND 4.0 - <https://cert.br/docs/ransomware/detectar/>

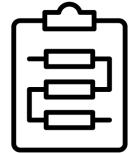
Resposta

É Necessário Agir Rapidamente para Conter o Avanço do Ataque

- Se detectados **indícios** de **qualquer fase** do ataque, é preciso:
 - **conter** o avanço
 - **eliminar** a presença do **atacante**
- É essencial **identificar e erradicar a causa raiz**
- **Falhas:**
 - na **remoção** de *malware*
 - na **eliminação** de vetores de acesso, ou
 - na **correção** de falhas exploradas
- **podem levar a novos ataques** e mais prejuízos

Resposta

É Necessário Agir Rapidamente para Conter o Avanço do Ataque



1. SEGUIR O PLANO DE RESPOSTA A INCIDENTES

Definir funções e treinar os contatos a serem envolvidos na resposta.
Documentar as ações tomadas e as informações coletadas.



2. CONTER O ATAQUE

Proteger os sistemas não comprometidos.
Isolar os sistemas afetados.
Preservar as evidências.



3. IDENTIFICAR O RANSOMWARE

Determinar o *ransomware* envolvido no ataque e entender seu comportamento.

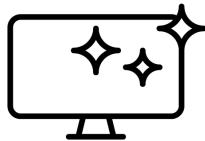
Resposta

É Necessário Agir Rapidamente para Conter o Avanço do Ataque



4. ANALISAR AS INFORMAÇÕES COLETADAS

- Cruzar os logs e as evidências com as informações do *ransomware*.
- Determinar a causa raiz e a extensão do ataque.



5. ELIMINAR O RANSOMWARE

- Remover o *malware* e os vestígios deixados pelo atacante.
- Reinstalar e atualizar os sistemas comprometidos.
- Corrigir as falhas exploradas no ataque.



6. TROCAR SENHAS E REVISAR ACESSOS

- Trocar as senhas de todas as contas.
- Habilitar autenticação multifator.
- Eliminar as contas e os privilégios adicionados pelo atacante.

Resposta

É Necessário Agir Rapidamente para Conter o Avanço do Ataque



7. RESTAURAR OS DADOS E A CONECTIVIDADE

Recuperar os dados de *backups* confiáveis ou, se necessário, verificar se há decifradores para o *malware*.

Reconectar os equipamentos à rede.



8. MELHORAR O AMBIENTE COM AS LIÇÕES APRENDIDAS

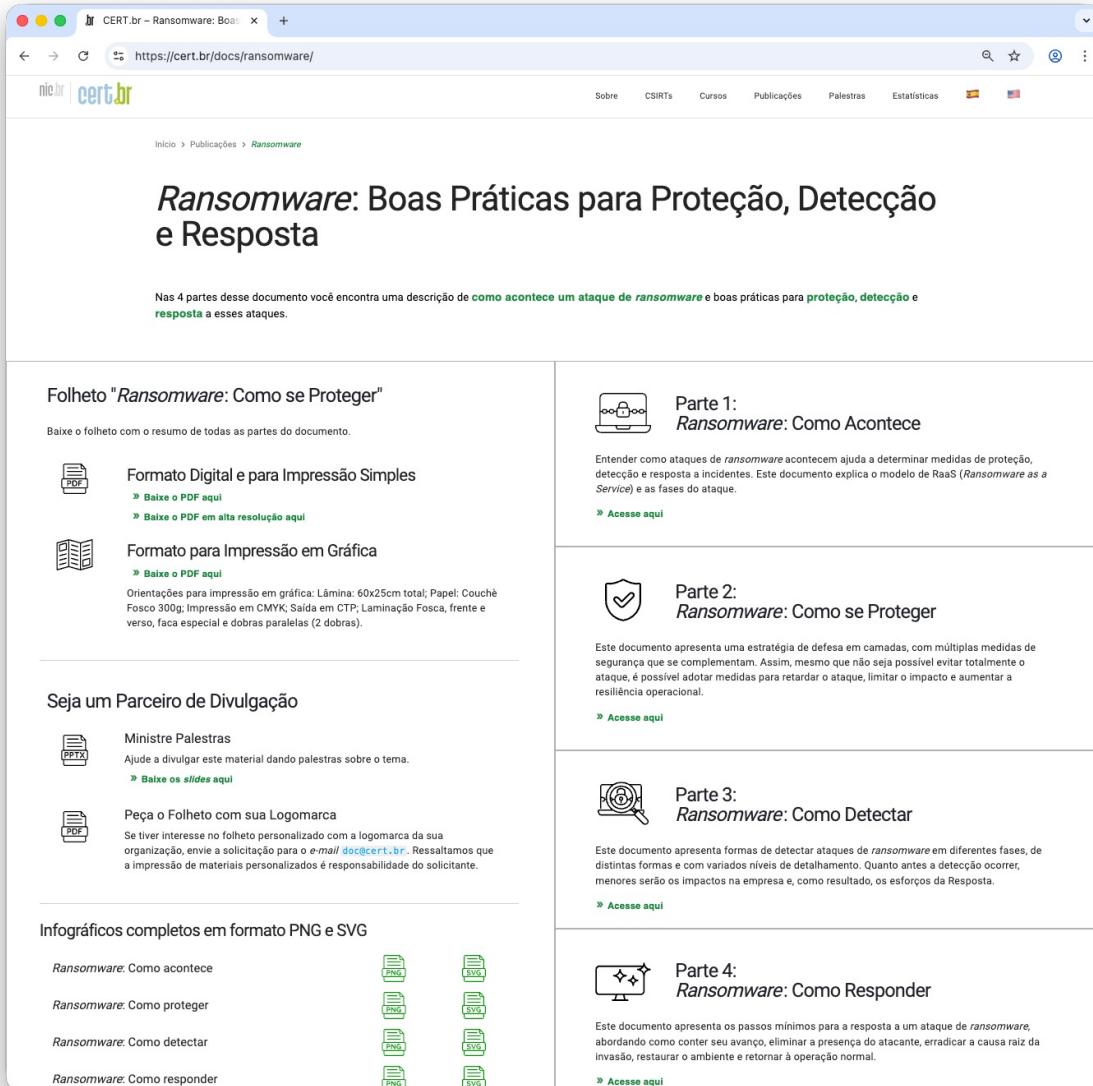
Analisar e documentar o incidente.

Intensificar a vigilância e as medidas de segurança.

Atualizar o Plano de Resposta a Incidentes.

Leitura Recomendada

Documento Completo e Folheto Resumido

A screenshot of a web browser displaying the CERT.br website at https://cert.br/docs/ransomware/. The page title is "Ransomware: Boas Práticas para Proteção, Detecção e Resposta". Below the title, a sub-section titled "Folheto 'Ransomware: Como se Proteger'" is shown. It includes a PDF icon and a link to download the digital version. A section for "Seja um Parceiro de Divulgação" shows options to download PPTX slides and PDF versions of the summary sheet. At the bottom, there's a section for "Infográficos completos em formato PNG e SVG" with links to four different infographics.

A summary sheet titled "RANSOMWARE: COMO SE PROTEGER". It features a large title "RANSOMWARE: COMO SE PROTEGER" in bold white letters. Below it, a sub-section titled "Entenda como funciona o ataque, como proteger sua rede e instrumentá-la para detecção, e como responder caso seja vítima." is described. A QR code is located in the bottom right corner.

cert.br

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

Obrigada!

✉️ para materiais de conscientização: doc@cert.br

✉️ notificações para: cert@cert.br ✖️ @certbr

<https://cert.br/>

nic.br cgi.br

www.nic.br | www.cgi.br