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

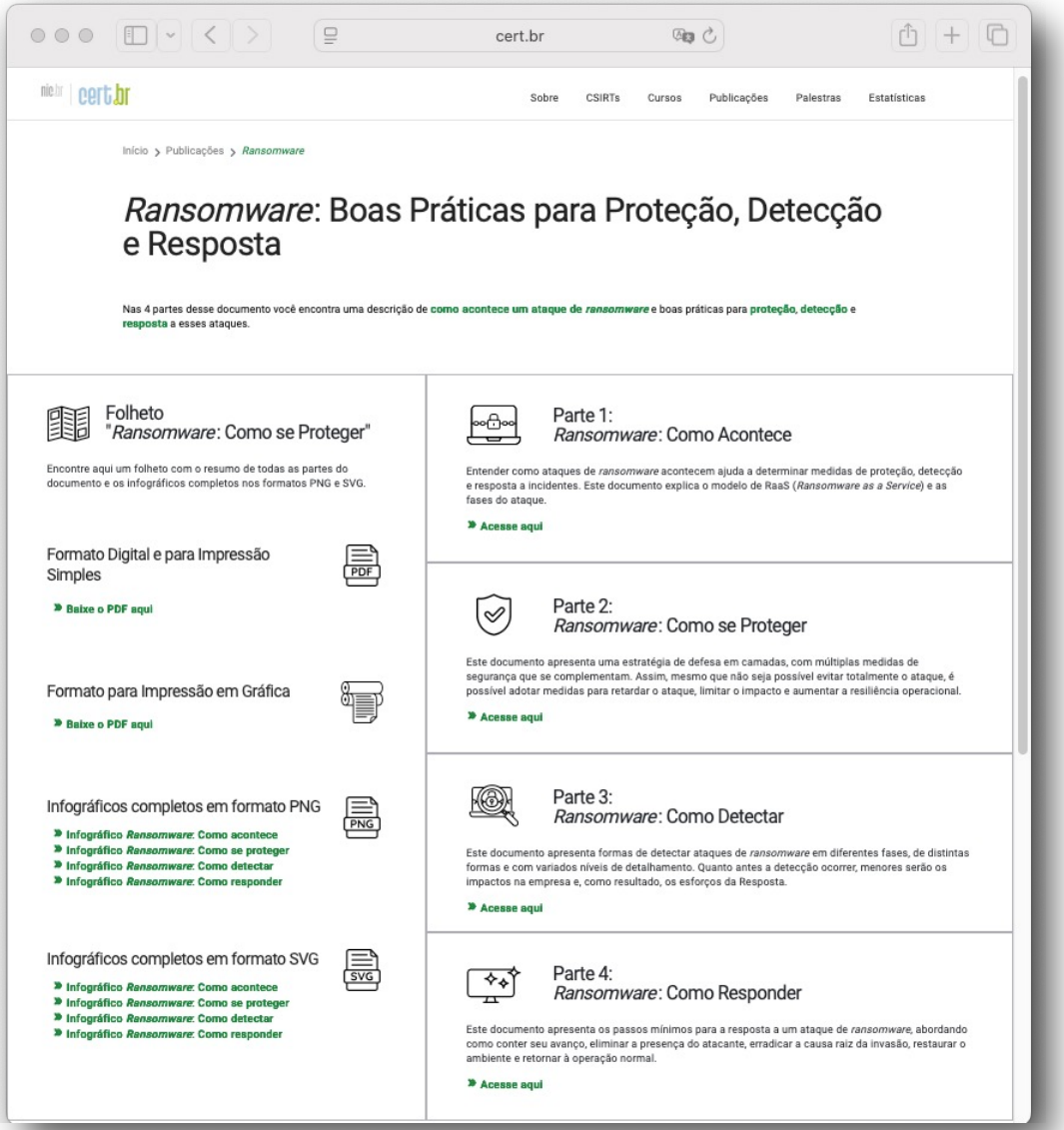
Cristine Hoepers, Ph.D.
Gerente Geral, CERT.br/NIC.br
cristine@cert.br

Reunião DESEG/FIESP
***Online* – 29 de agosto de 2025**

cert.br nic.br cgi.br

Documento Completo e Folheto

TLP:CLEAR



TLP:CLEAR

Nissan confirms design studio data breach claimed by Qilin ransomware

By **Bill Toulas** August 26, 2025 09:48 AM 0

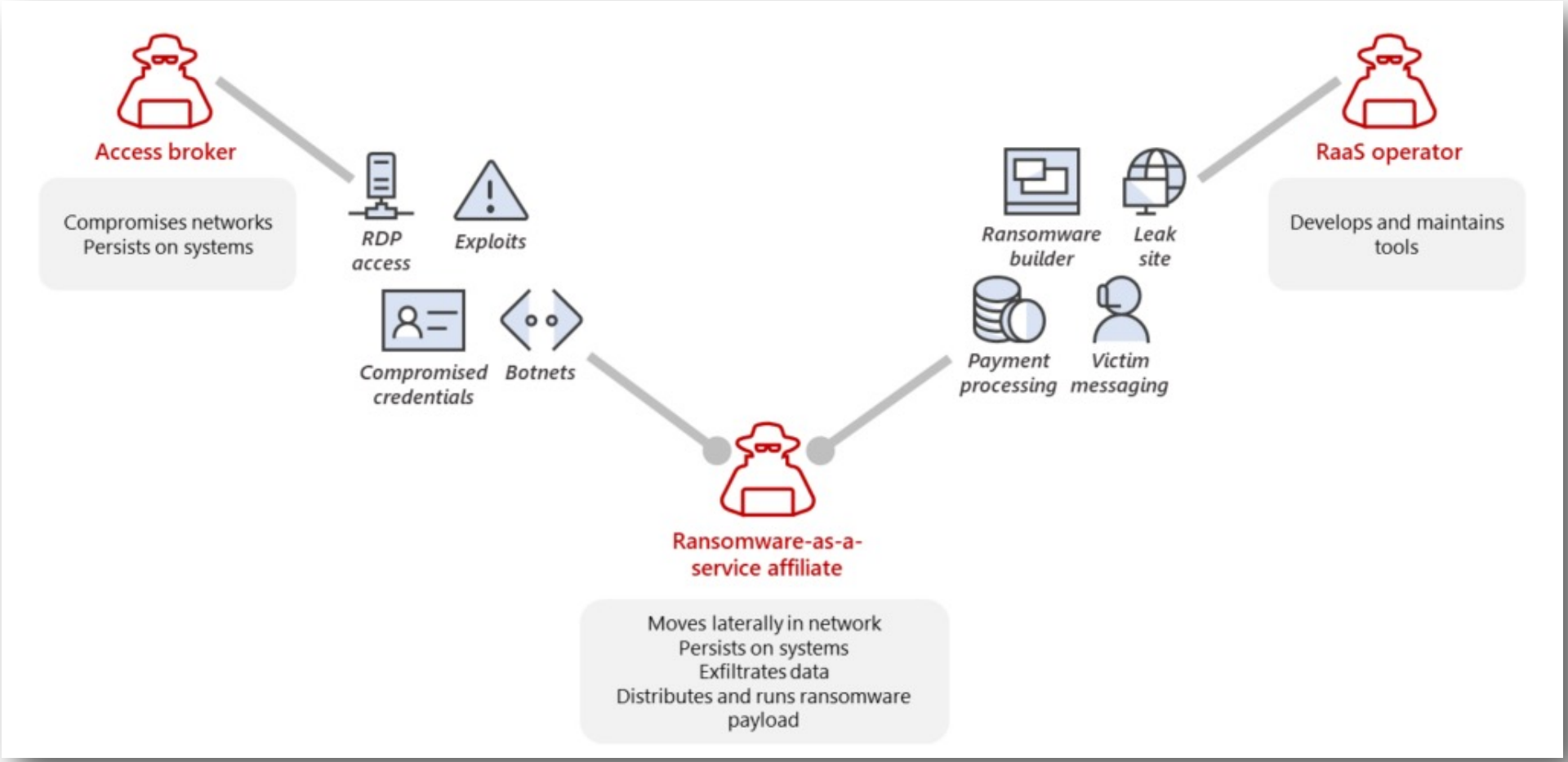
Nissan Japan has confirmed to BleepingComputer that it suffered a data breach following unauthorized access to a server of one of its subsidiaries, Creative Box Inc. (CBI).

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.

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

Além de uma infeção por *malware*
Ransomware as a Service – RaaS

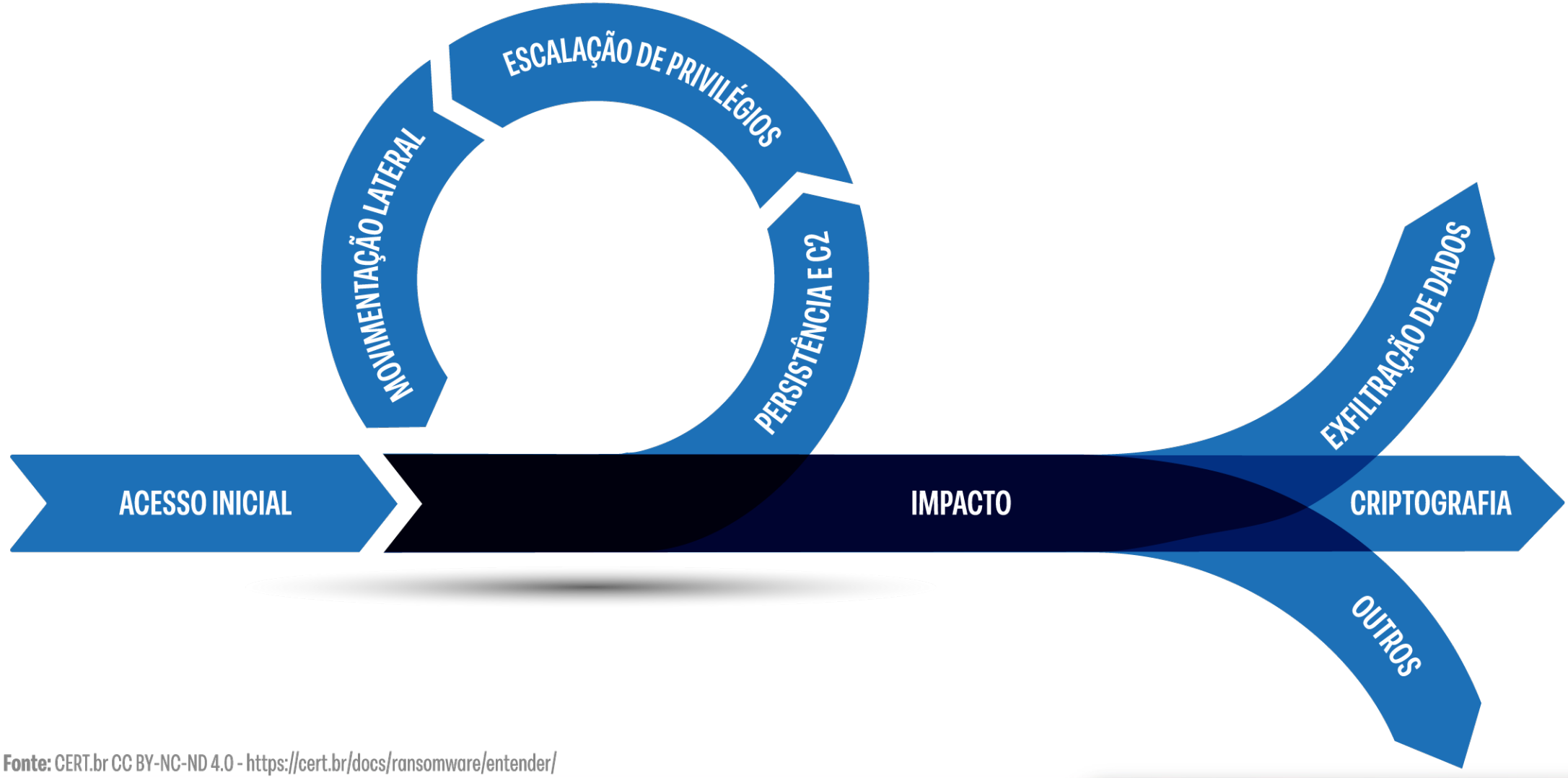


Fonte: https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

TLP:CLEAR

Ransomware: Como Acontece

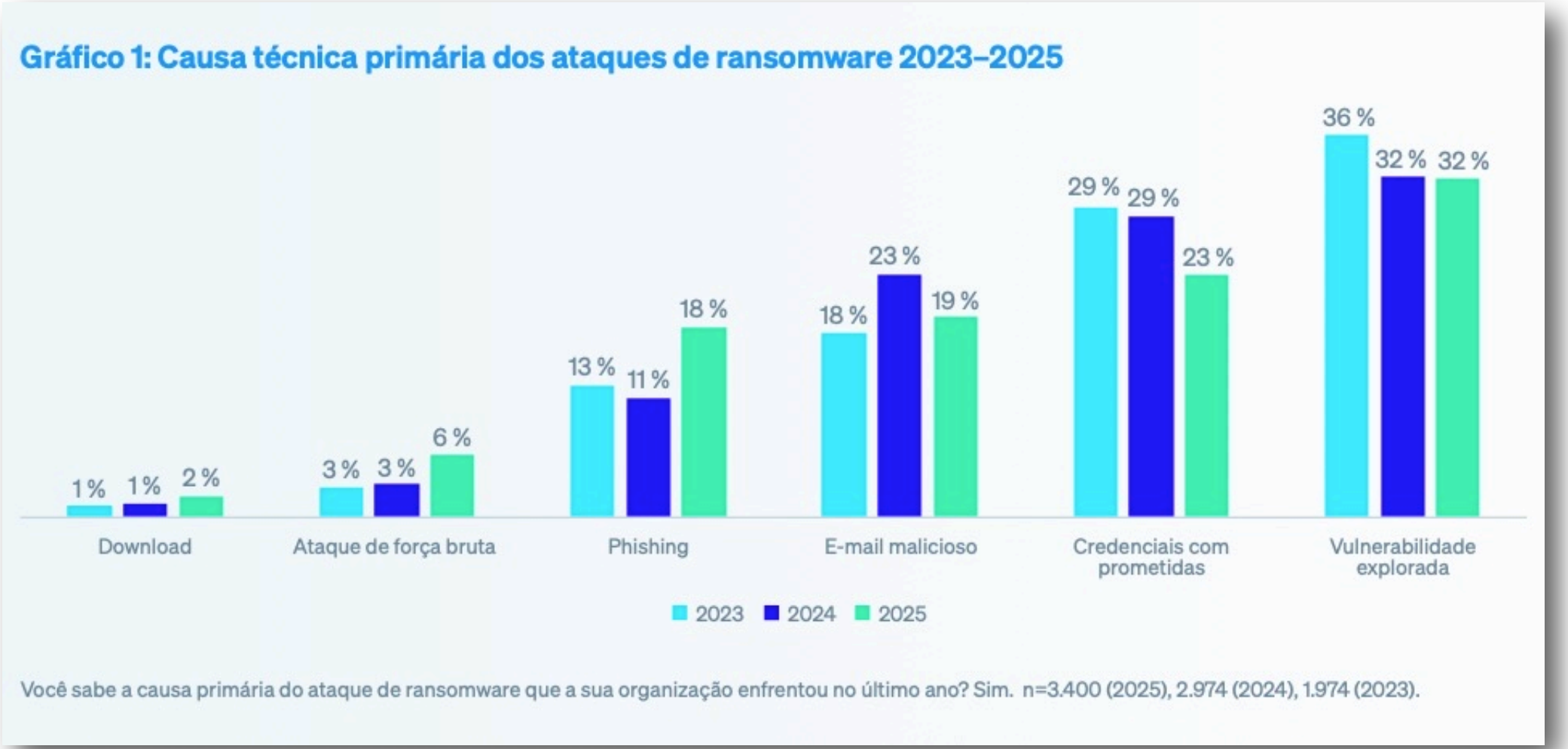
Ciclo de vida do ataque



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

Causas Primárias

TLP:CLEAR



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

Proteção: O Básico que Pode Fazer a Diferença

TLP:CLEAR

USAR AUTENTICAÇÃO MULTIFATOR (MFA)

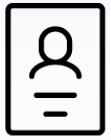
Exigir a autenticação multifator, para acesso remoto à rede, serviços web, serviços em nuvem e usuários com privilégios de administrador.

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

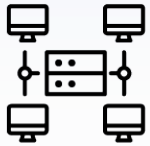
Fazer gestão de vulnerabilidades usando estratégia de priorização baseada em risco.

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.



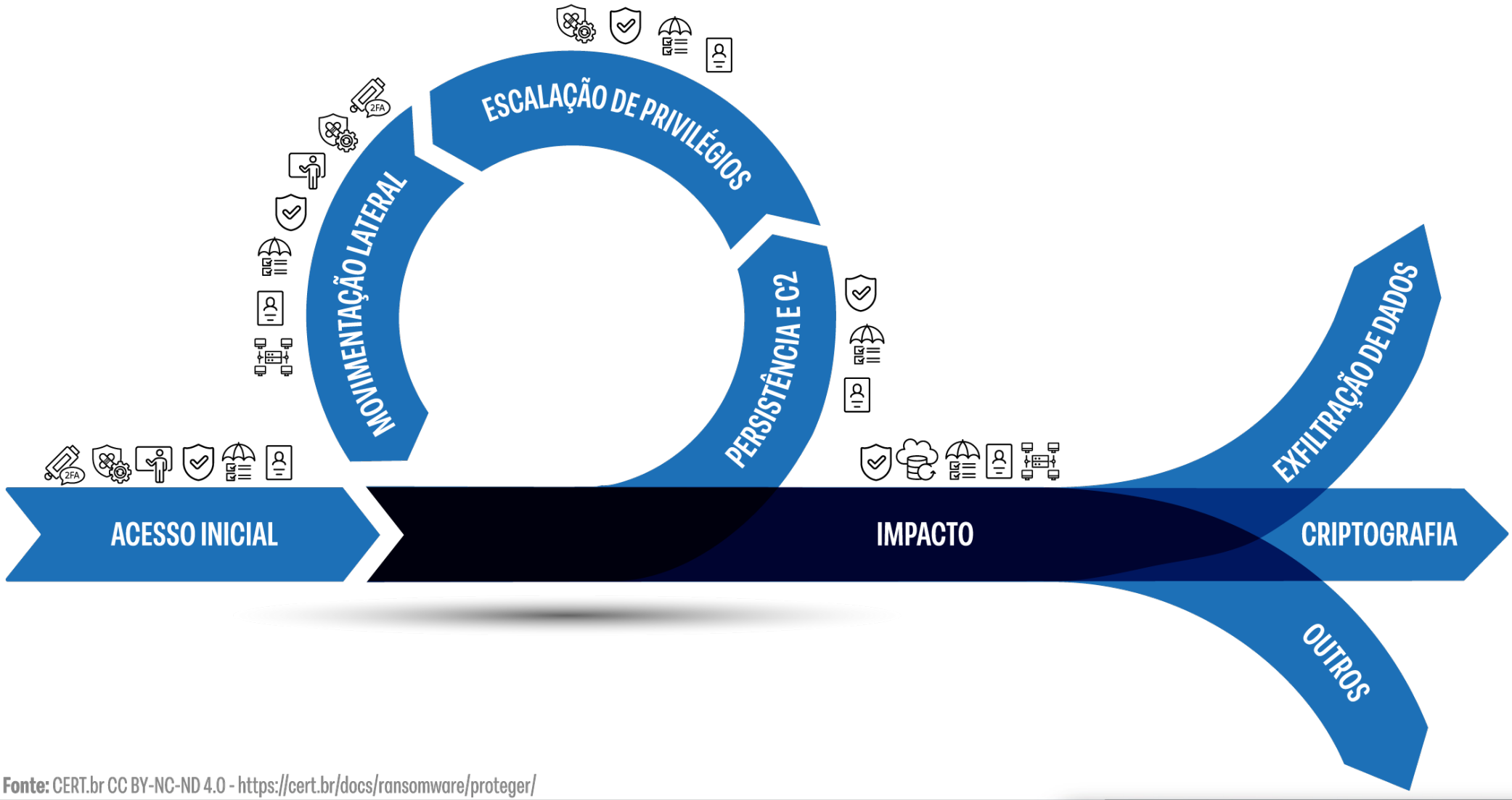
SEGMENTAR A REDE

Dividir a rede em segmentos menores e segregados.

TLP:CLEAR

Proteção: O Básico que Pode Fazer a Diferença

Defesa em Camadas



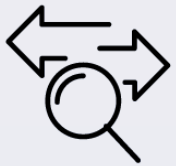
Fonte: CERT.br CC BY-NC-ND 4.0 - https://cert.br/docs/ransomware/proteger/

Detecção – O Básico que Pode Fazer a Diferença

TLP:CLEAR

HABILITAR E ANALISAR *LOGS*

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



MONITORAR O TRÁFEGO DE REDE

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

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 CONTAS DE USUÁRIOS E ADMINISTRADORES

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

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.

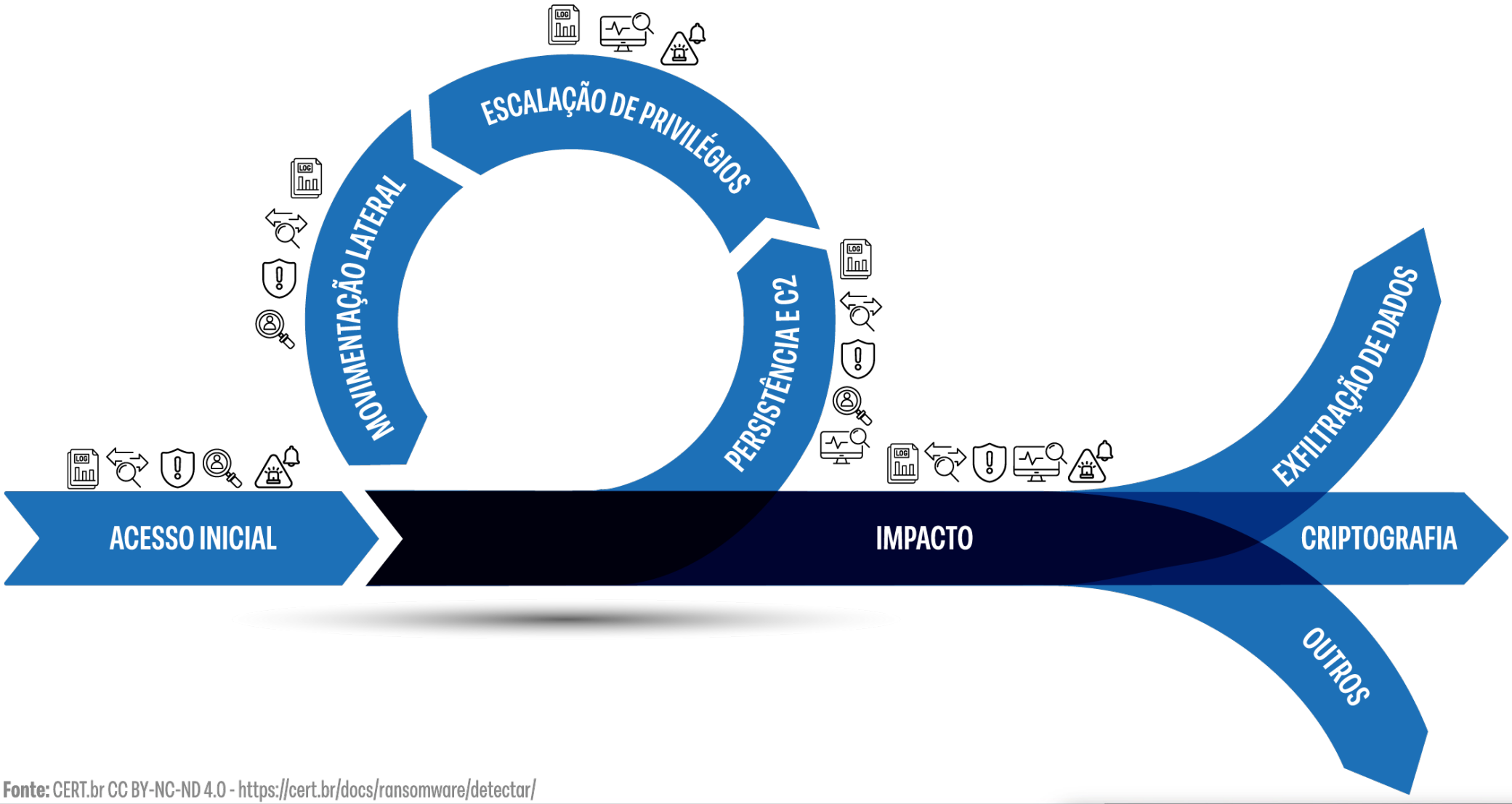
ESTABELECER UM CANAL PARA RECEBER NOTIFICAÇÕES DE SEGURANÇA

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

TLP:CLEAR

Detecção – O Básico que Pode Fazer a Diferença

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/

TLP:CLEAR

Resposta: É Preciso Estar Preparado

Quanto mais rápida a resposta, menor o impacto e o custo de recuperação

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.

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.

TLP:CLEAR

Resposta: É Preciso Estar Preparado
Quanto mais rápida a resposta, menor o impacto e o custo de recuperação

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.

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.

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