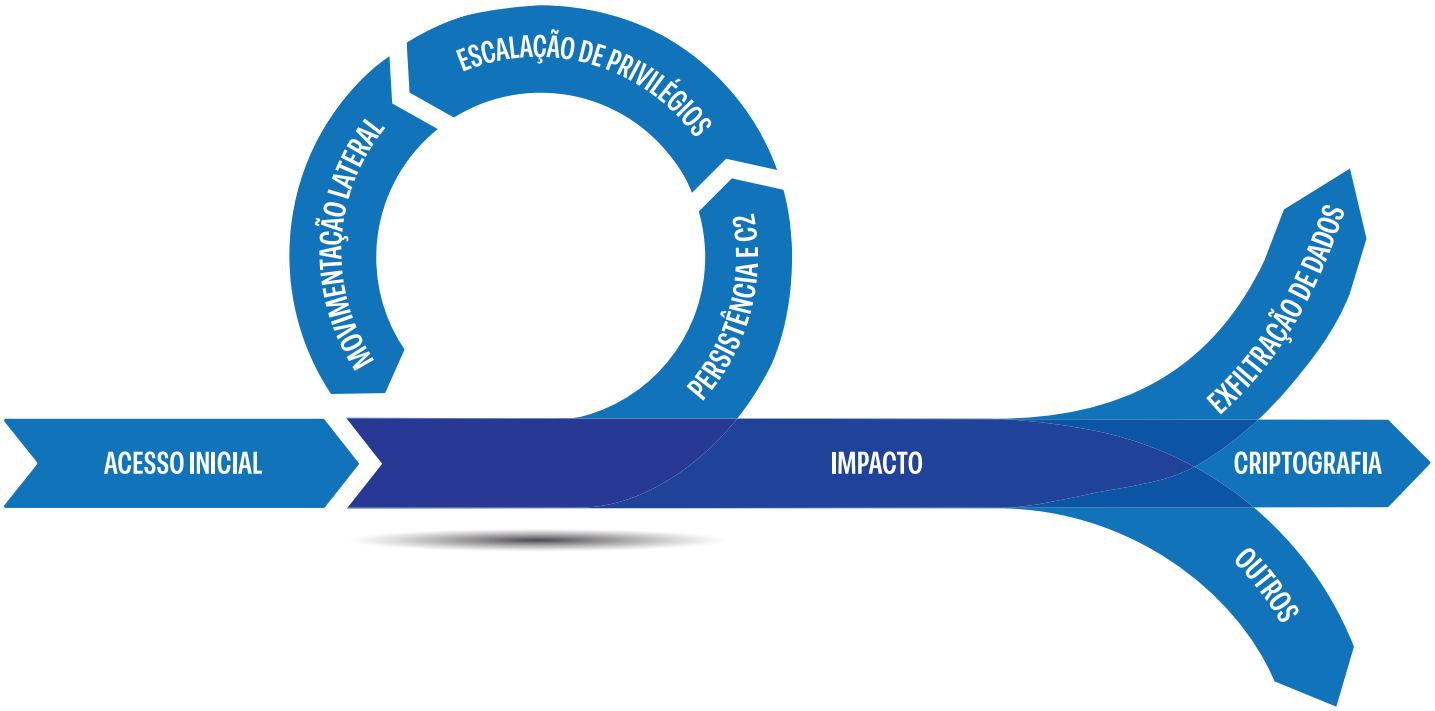
RANSOMWARE: COMO SE PROTEGER

Entenda como funciona o ataque, como proteger sua rede e instrumentá-la para detecção, e como responder caso seja vítima.

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

cert.br

RANSOMWARE: COMO ACONTECE



ACESSO INICIAL
O atacante invade a rede da empresa utilizando credenciais comprometidas, vulnerabilidades de *software*, engenharia social ou *malware*.

PERSISTÊNCIA E C2
O atacante estabelece um acesso persistente e mecanismos de comunicação entre o sistema invadido e a infraestrutura de Comando e Controle (C2).

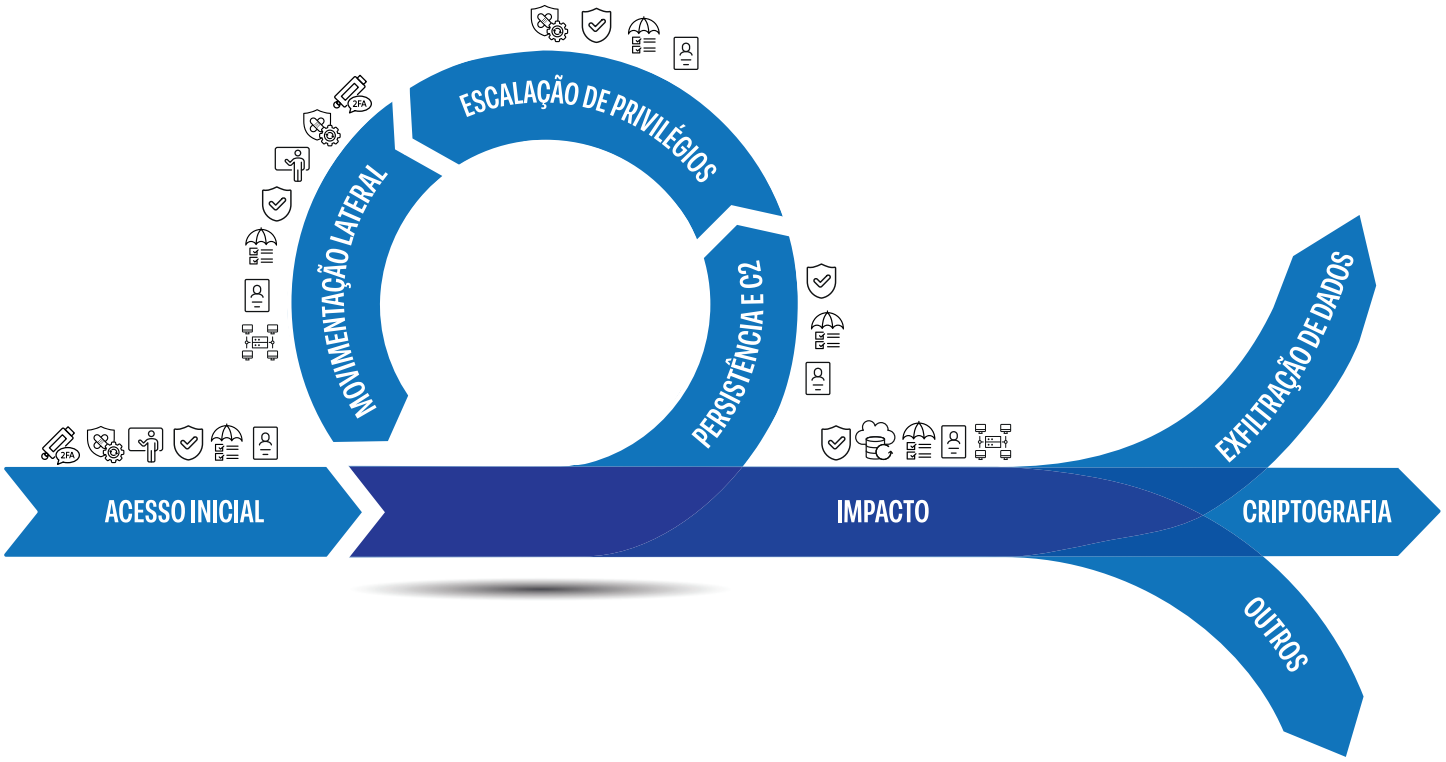
ESCALAÇÃO DE PRIVILÉGIOS
O atacante obtém permissões elevadas para realizar atividades de administrador, acessar dados sensíveis e movimentar-se lateralmente na rede.

MOVIMENTAÇÃO LATERAL
O atacante se move pela rede, ganha acesso a sistemas e dados críticos e propaga o *ransomware* (*malware*) pelo ambiente para realizar a criptografia na fase de Impacto.

IMPACTO
O atacante causa o máximo de impacto para pressionar a empresa a pagar o resgate. As técnicas mais comuns são a criptografia e a exfiltração de dados.

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

RANSOMWARE: COMO SE PROTEGER



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.

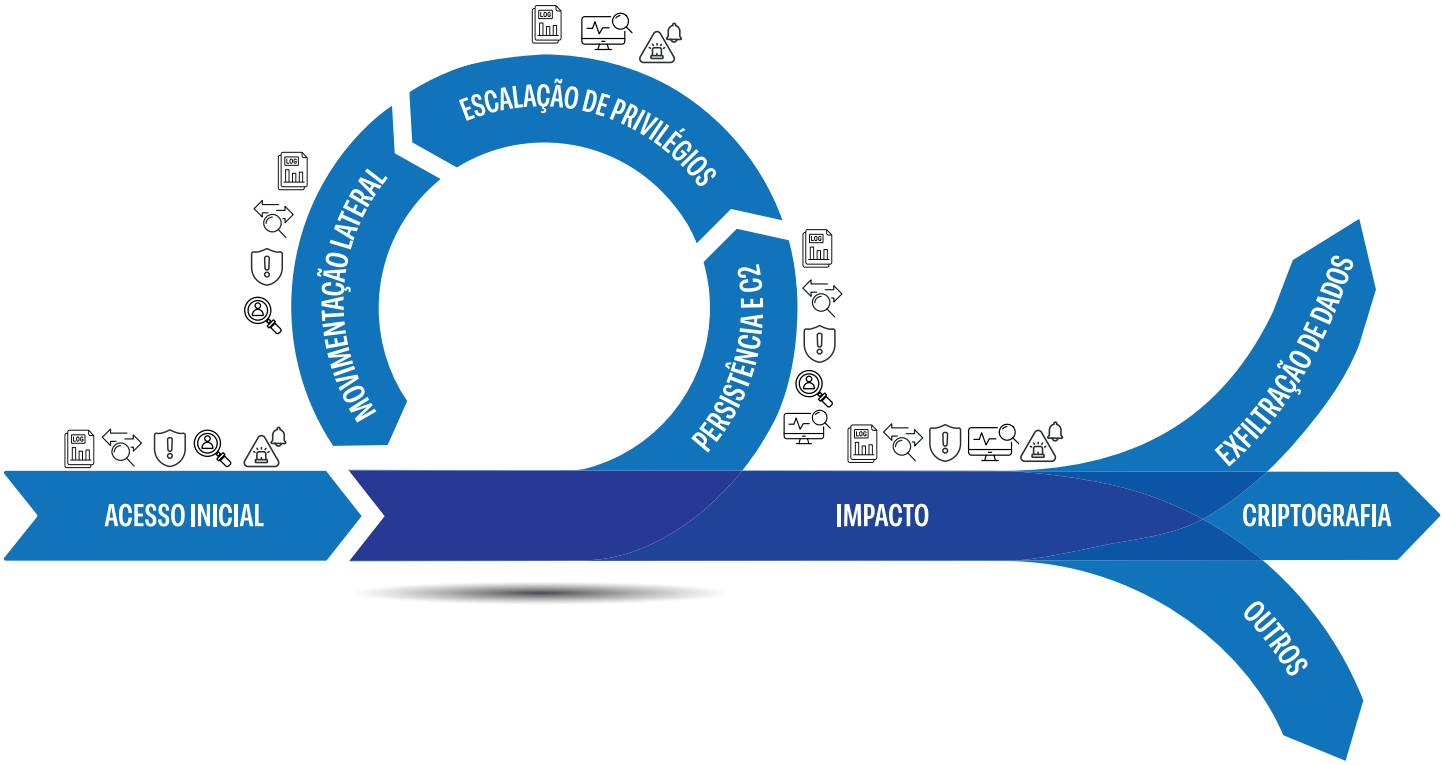
USAR FERRAMENTAS DE PROTEÇÃO
Implementar ferramentas de proteção e de monitoração de rede.

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.

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

RANSOMWARE: COMO DETECTAR



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.

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

RANSOMWARE: COMO RESPONDER

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.

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.

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

cert.br

O CERT.br **(https://cert.br/)** é um Grupo de Resposta a Incidentes de Segurança (CSIRT) de responsabilidade nacional de último recurso, mantido pelo NIC.br. Além da gestão de incidentes, também atua na conscientização sobre os problemas de segurança, na consciência situacional e transferência de conhecimento, sempre respaldado por forte integração com as comunidades nacional e internacional de CSIRTs.

nic.br

O Núcleo de Informação e Coordenação do Ponto BR – NIC.br **(https://nic.br/)** é uma entidade civil de direito privado e sem fins de lucro, encarregada da operação do domínio .br, bem como da distribuição de números IP e do registro de Sistemas Autônomos no País. Conduz ações e projetos que trazem benefícios à infraestrutura da Internet no Brasil.

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

julho / 2025