Todos podem ser Alvo de *Ransomware*: Medidas Básicas Podem Fazer a Diferença para Reduzir o Impacto

Miriam von Zuben
Analista de Segurança
miriam@cert.br

Fórum da Internet no Brasil – FIB16
Belém, PA – 29 de maio de 2026

cert.br nic.br cgi.br

cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CERT Nacional de Último Recurso

Serviços Prestados à Comunidade

Gestão de Incidentes

- Coordenação
- Análise Técnica
- Suporte à Mitigação e Recuperação

Consciência Situacional

- Aquisição de Dados
  - *Honeypots* Distribuídos
  - SpamPots
  - *Threat feeds*
- Compartilhamento das Informações

Transferência de Conhecimento

- Conscientização
  - Desenvolvimento de Boas Práticas
  - Cooperação, Eventos e Reuniões (*Outreach*)
- Treinamento
- Aconselhamento Técnico e de Políticas

Filiações e Parcerias:

FIRST MEMBER

M3AAWG Messaging Malware Mobile Anti-Abuse Working Group

Carnegie Mellon University Software Engineering Institute — SEI Partner Network

APWG

Accredited by TI Trusted Introducer 5

https://cert.br/sobre/ | https://cert.br/sobre/filiacoes/ | https://cert.br/about/rfc2350/

Missão

Aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

Público Alvo (*Constituency*)

Redes que utilizam recursos administrados pelo NIC.br

- endereços IP ou ASNs alocados ao Brasil
- domínios sob o ccTLD .br

Principais Atividades

- Facilitar a coordenação do tratamento de incidentes entre as partes
  - Ponto de contato nacional de último recurso
  - Trabalho colaborativo com outras entidades
  - Auxílio na análise técnica e compreensão de ataques e ameaças
- Aumentar a detecção, correlação de eventos e determinação de tendências
- Transferir o conhecimento através de cursos, boas práticas e conscientização

Agenda

– O que é o *ransomware*
– Como acontece
– Como se proteger
– Como detectar
– Como responder

Ransomware

cert.br nic.br cgi.br

Ransomware
Originalmente

- *Ransomware* era apenas um tipo de *malware*
- Desenvolvido para deixar dados e sistemas inacessíveis até o pagamento do resgate
- Geralmente:
  - criptografava dados ou partes dos sistemas
  - exigia pagamento pela chave de criptografia

Ransomware
Nos Dias Atuais

- Evoluiu para um ataque elaborado
- Realizado por grupos de múltiplos indivíduos que:
  - dividem tarefas
  - coordenam as diversas fases do ataque
- Atacantes:
  - invadem redes das empresas
  - **comprometem sistemas críticos**
  - **exfiltram dados**
  - destroem *backups*
  - criptografam dados
  - **fazem múltiplas extorsões**

Ransomware	Double Extortion	Triple Extortion	Quadruple Extortion
Abyss Locker	⚠		
Black Basta	⚠		
FunkSec	⚠		
HellCat	⚠		
Interlock	⚠		
Lynx	⚠		
Morpheus	⚠		
Nnice	⚠		
RansomHub	⚠		
XELERA	⚠		
Akira	⚠	⚠	
Medusa	⚠	⚠	
ALPHV/BlackCat	⚠	⚠	⚠
CL0P	⚠	⚠	⚠
LockBit 3.0	⚠	⚠	⚠

Fig. 4: Akamai researchers have observed these ransomware groups employing various extortion tactics

Fonte: https://www.akamai.com/lp/soti/ransomware-trends-2025

Ransomware
Evolução

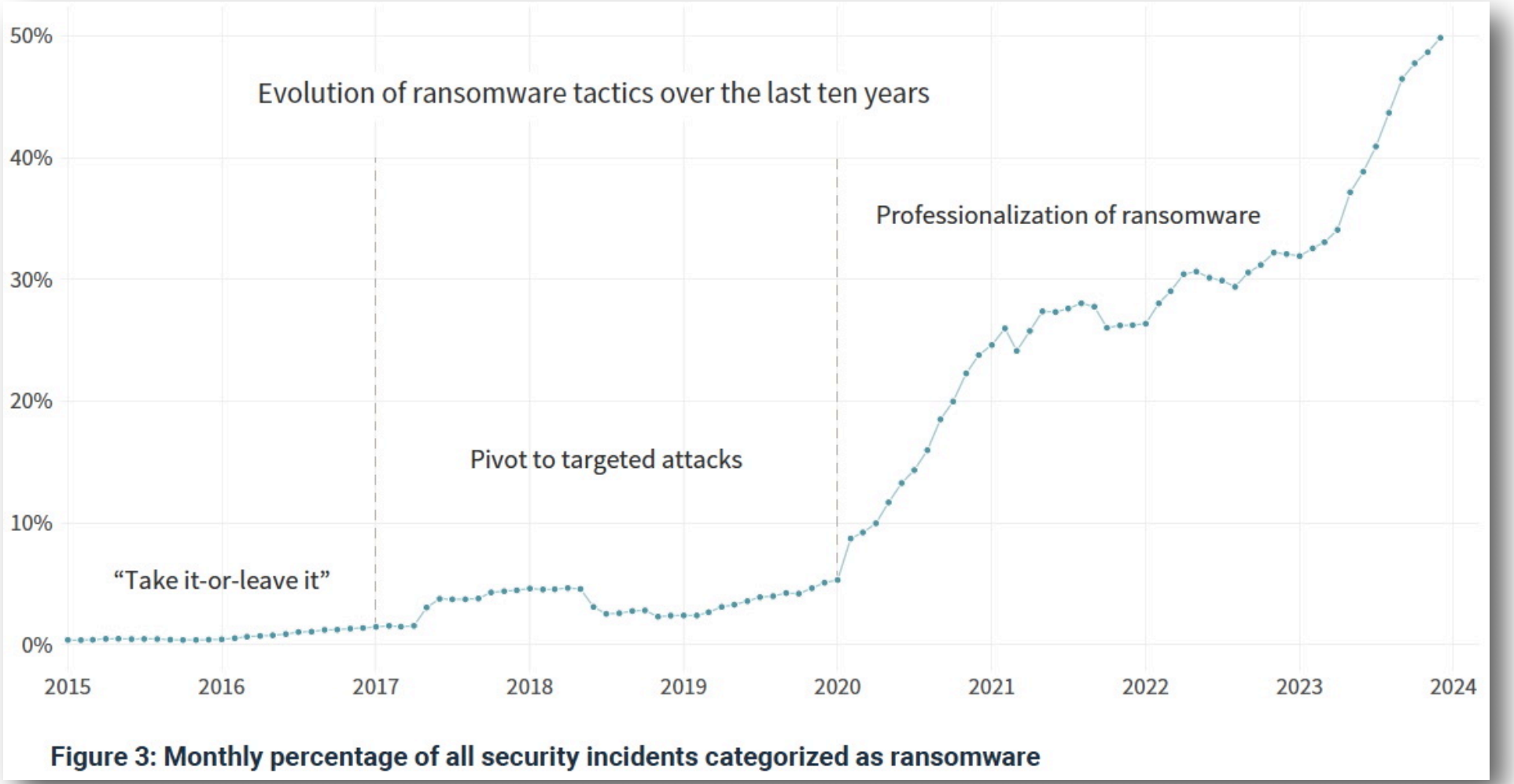
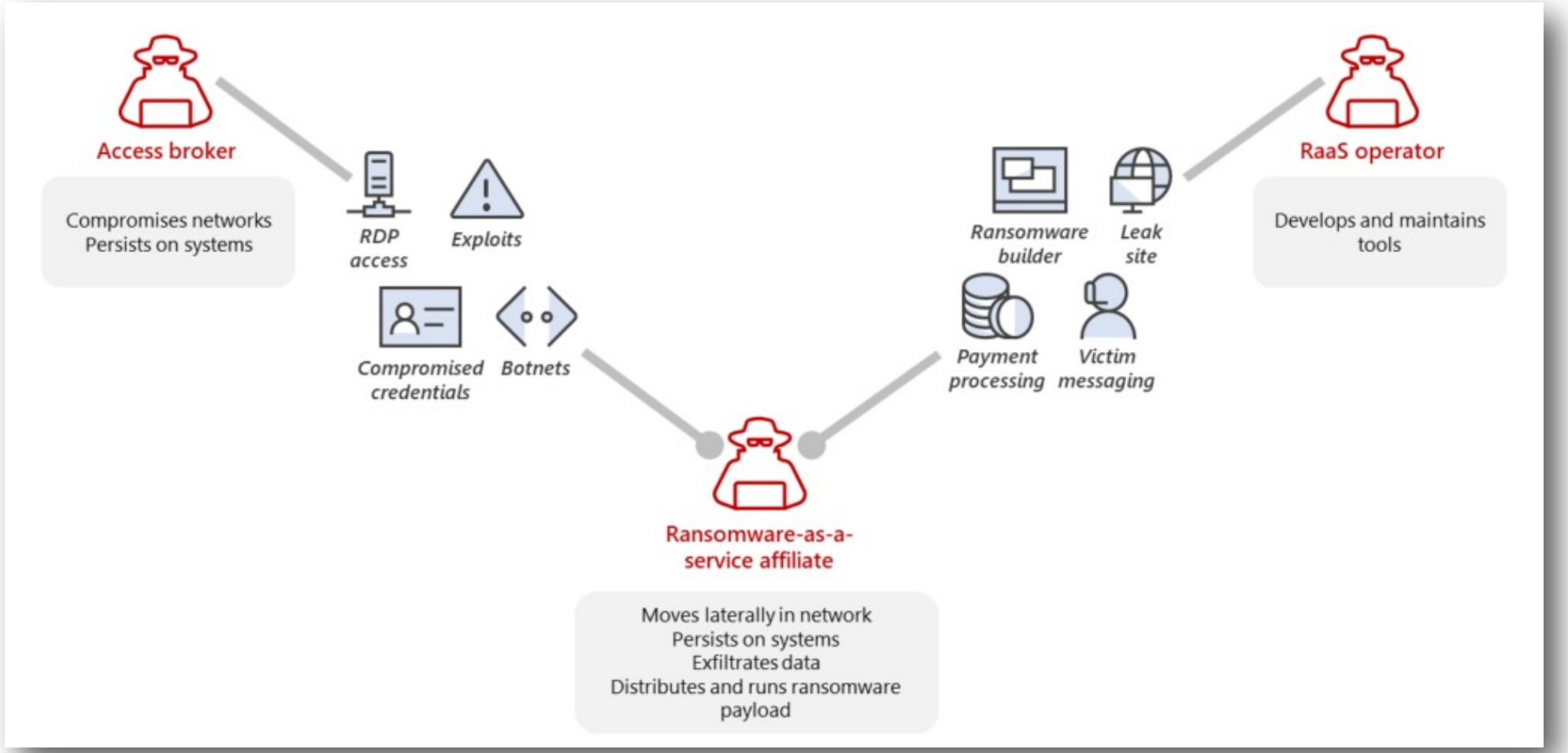


Figure 3: Monthly percentage of all security incidents categorized as ransomware

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

Ransomware
Ransomware as a Service

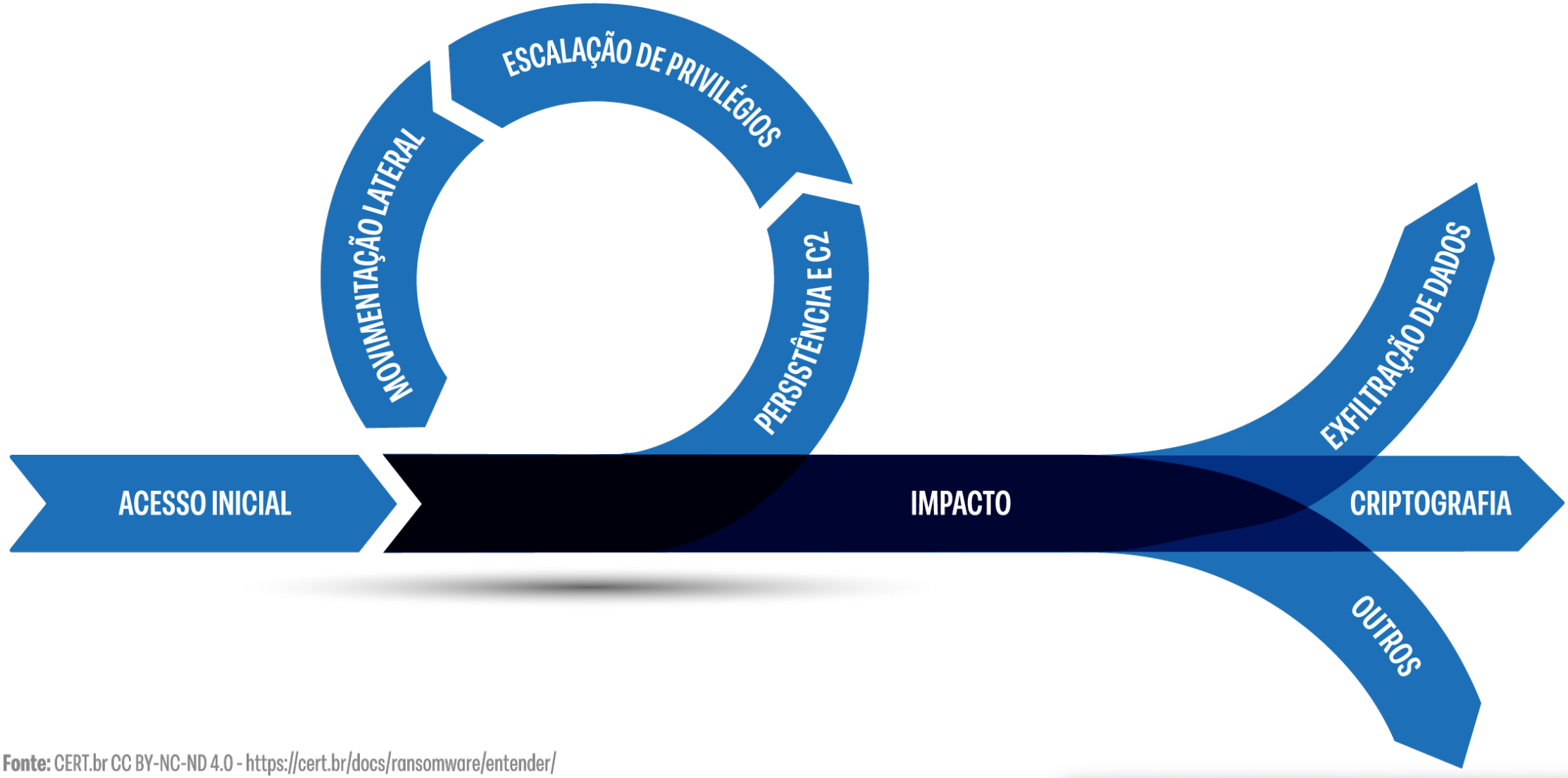


Fonte: https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

Ransomware: Como Acontece

cert.br nic.br cgi.br

Como Acontece
Ciclo de Vida do Ataque



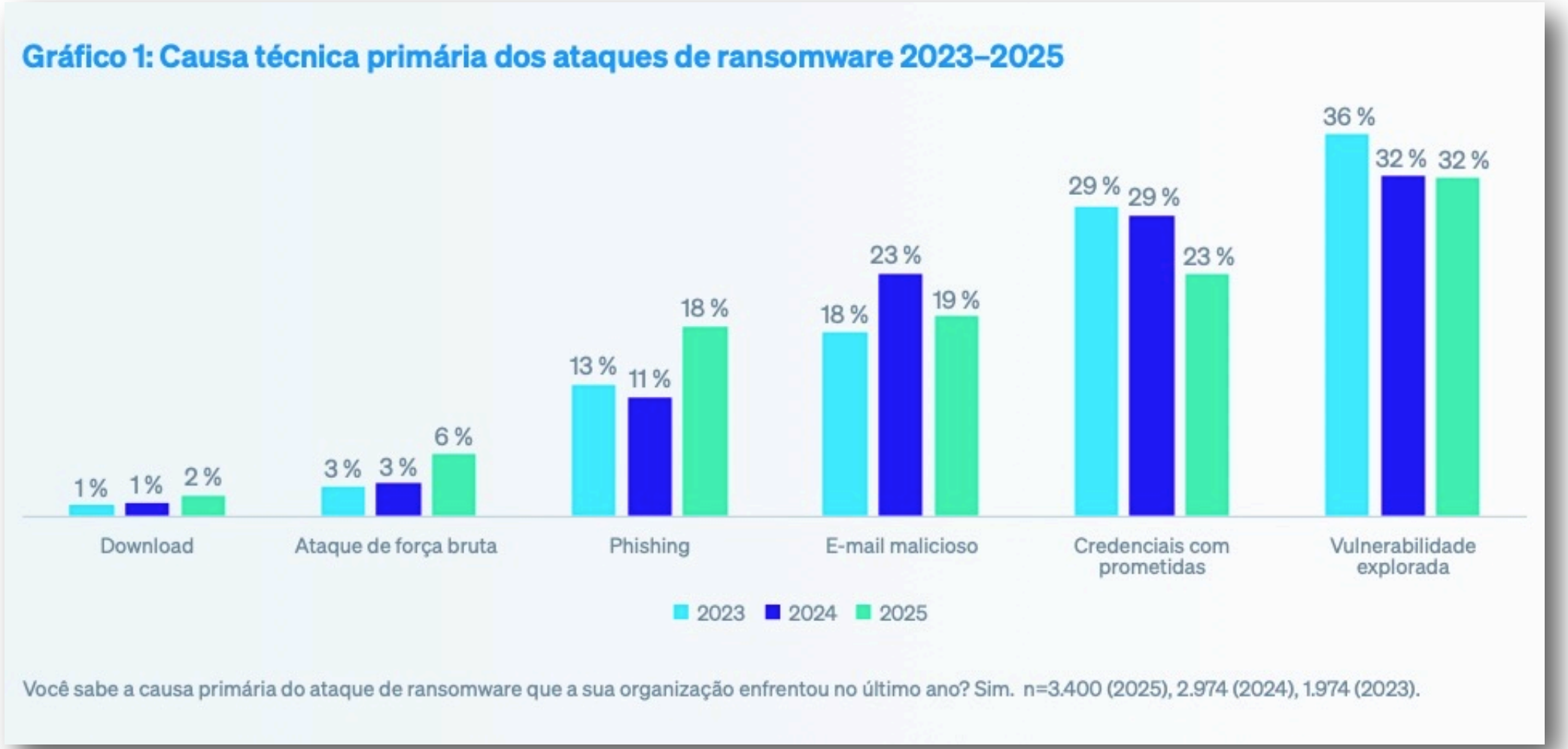
Como Acontece
Acesso Inicial

- **ACESSO INICIAL**
  Atacante tenta invadir a rede da empresa.
- PERSISTÊNCIA E C2
- ESCALAÇÃO DE PRIVILÉGIOS
- MOVIMENTAÇÃO LATERAL
- IMPACTO

Principais vetores de invasão:

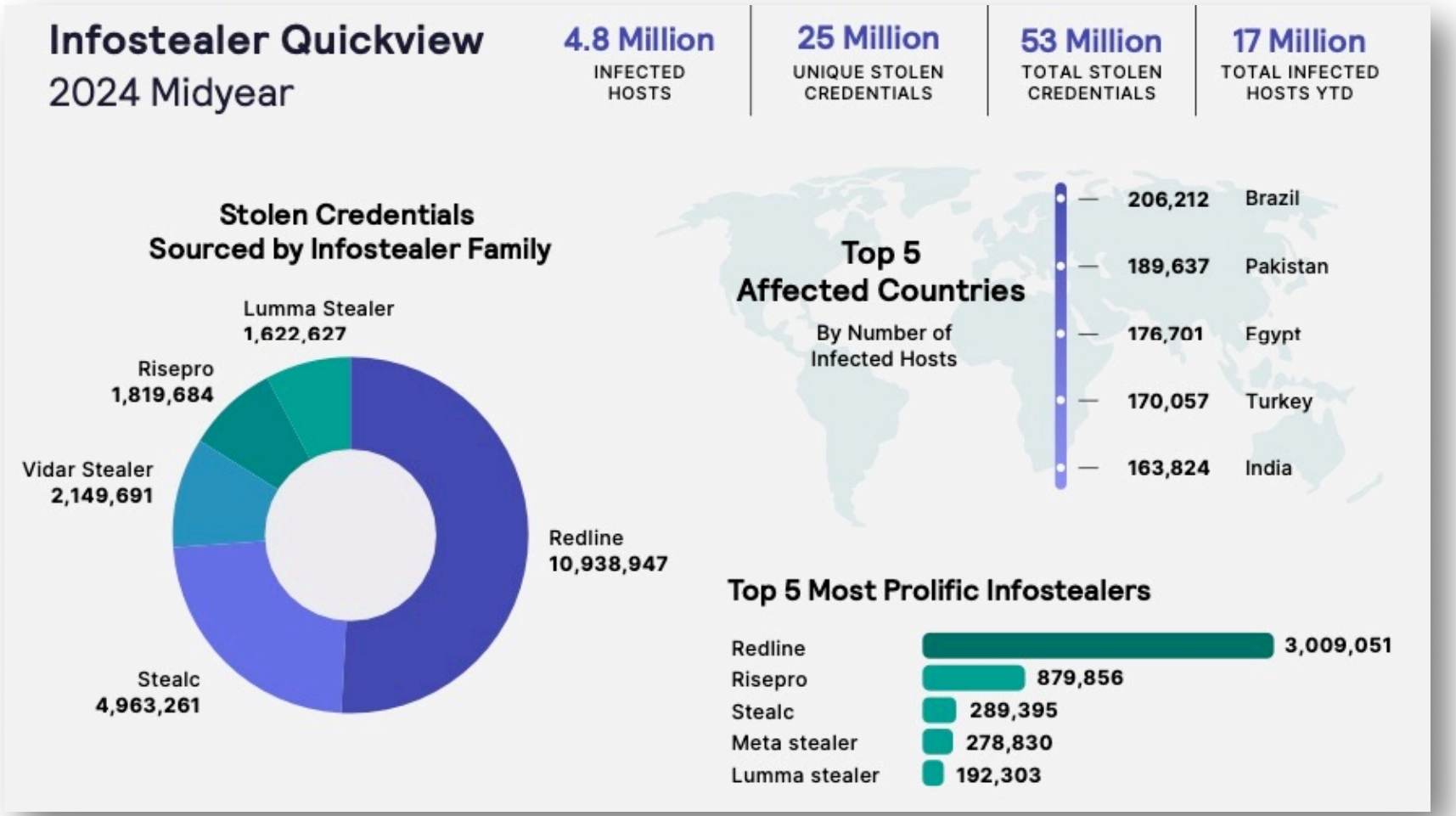
- Credenciais de acesso remoto comprometidas
  - ex: de VPN e RDP
- Vulnerabilidades de *software*
  - ex: em equipamentos de borda
- *Phishing*
  - ex: por *e-mail* ou mensagem de texto
- *Malware*
  - ex: via anexo de *e-mail* ou *link* patrocinado
- Engenharia social
  - ex: ligação telefônica fingindo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

Como Acontece
Causas Primárias dos Ataques de *Ransomware*



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

Como Acontece
Causas Primárias dos Ataques de *Ransomware*



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

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

Como Acontece
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

Como Acontece
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

Como Acontece
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

Como Acontece
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*

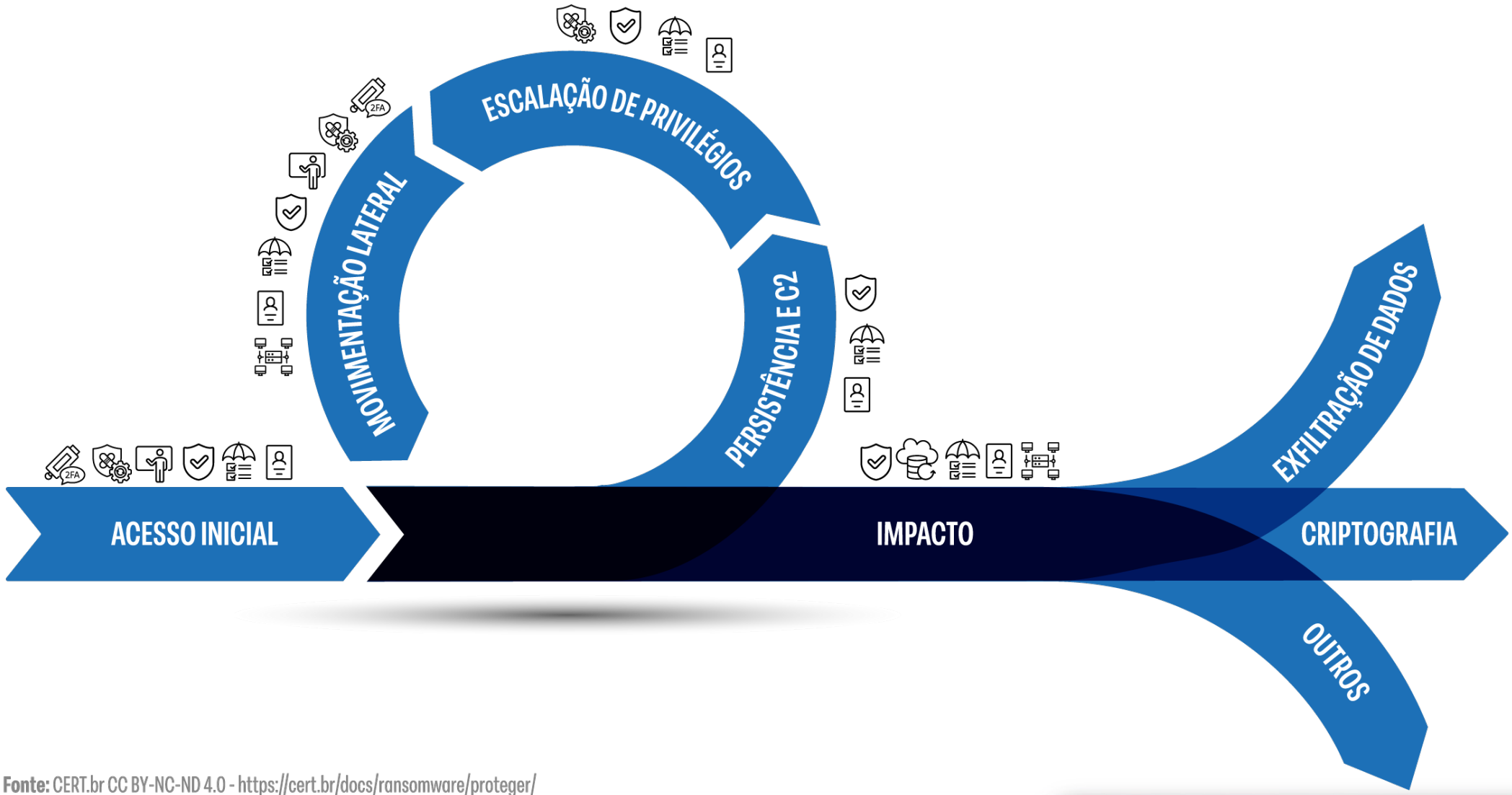
Ransomware: Como se Proteger

cert.br nic.br cgi.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
Um Único Mecanismo Pode ser Usado para Múltiplas Defesas



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

1. Usar Autenticação Multifator (MFA)

Evita o acesso via **credenciais comprometidas**.

Dificulta **Acesso Inicial** e **Movimentação Lateral**.

Priorize:

- Acesso remoto
- Serviços via Web
- Serviços em nuvem
- Usuários com privilégios de administrador

Prefira mecanismos MFA resistentes a *phishing*

2. Fazer Gestão de Vulnerabilidades

Previne a exploração de vulnerabilidades.

Dificulta **Acesso Inicial, Escalação de Privilégios** e **Movimentação Lateral**.

Priorize a correção de:

- Sistemas **expostos** na Internet
- Vulnerabilidades **ativamente exploradas**
  - ex: catálogo CISA *Known Exploited Vulnerabilities* (KEV)

Se não for possível corrigir:

- Isole o sistema
- Aplique controles mais restritivos
- Implemente soluções de contorno

3. Conscientizar Funcionários

Mitiga ataques que exploram o **"fator humano"**, como **engenharia social**.

Dificulta **Acesso Inicial** e **Movimentação Lateral**.

Treine funcionários e terceiros para que:

- Conheçam os **canais oficiais**
  - suporte técnico
  - segurança
- Reconheçam **comunicações suspeitas**
  - ex: *phishing*
- **Reportem problemas** de segurança
  - ex: alertas, acesso indevido, computador "estranho"
- Saibam **o que fazer** em caso de *ransomware*

4. Usar Ferramentas de Proteção

Ajuda a **prevenir, detectar e conter** diversas atividades maliciosas**.**

Atua em todas as fases do ataque.

Adote:

- Proteção para ***endpoints***
  - com capacidade de **detecção e resposta**
- Filtros ***antispam***
- **Monitoração** de tráfego de rede
  - use ***netflow,*** se possível

5. Fazer e Proteger *Backups*

Permite a **recuperação** de dados e sistemas críticos.

Essencial na fase de **Resposta**.

Faça *backups* **regularmente**

Proteja **contra acesso e modificação** não autorizados

Mantenha ao menos uma cópia ***offline***

Verifique os *backups* frequentemente

- **Integridade** dos dados
- Eficácia da restauração

6. Reduzir a Superfície de Ataque

Diminui a quantidade de elementos passíveis de exploração.

Previne **Acesso Inicial**, **Escalação de Privilégios, Movimentação Lateral e Impacto.**

Desative serviços não usados
- Na **Internet** e na **rede interna**

Não exponha serviços e dados
- *Desktop* remoto (ex: RDP)
- *Backups*
- Compartilhamentos de rede (ex: SMB)
- Armazenamentos em nuvem (ex: *buckets*)
- Servidores críticos (ex: AD)
- Impressoras e outros dispositivos em rede

7. Gerenciar Identidades e Acessos

Reduz o risco de **acessos indevidos** e o **abuso de privilégios** em caso de invasão.

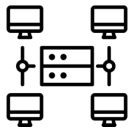
É relevante em todas as fases do ataque.

Use o princípio do **privilégio mínimo**

- Conceda **permissões necessárias à função**
- **Limite** contas com **acessos privilegiados**
- Forneça **acesso remoto** só a quem **precisa**
- **Restrinja** acessos a recursos
  - ex: compartilhamentos de rede e *backups*

Revise acessos regularmente

- **Desabilite** contas inativas
- **Revogue permissões** desnecessárias



8. Segmentar a Rede

Ajuda a **conter** o ataque e a **exfiltração** de dados.

Limita **Movimentação Lateral** e **propagação de *malware*.**

Separe, por exemplo:

- Serviços críticos
- Equipamentos de usuários
- Sistemas legados

Isole os segmentos

- Libere apenas os acessos necessários

Ransomware: Como Detectar

cert.br nic.br cgi.br

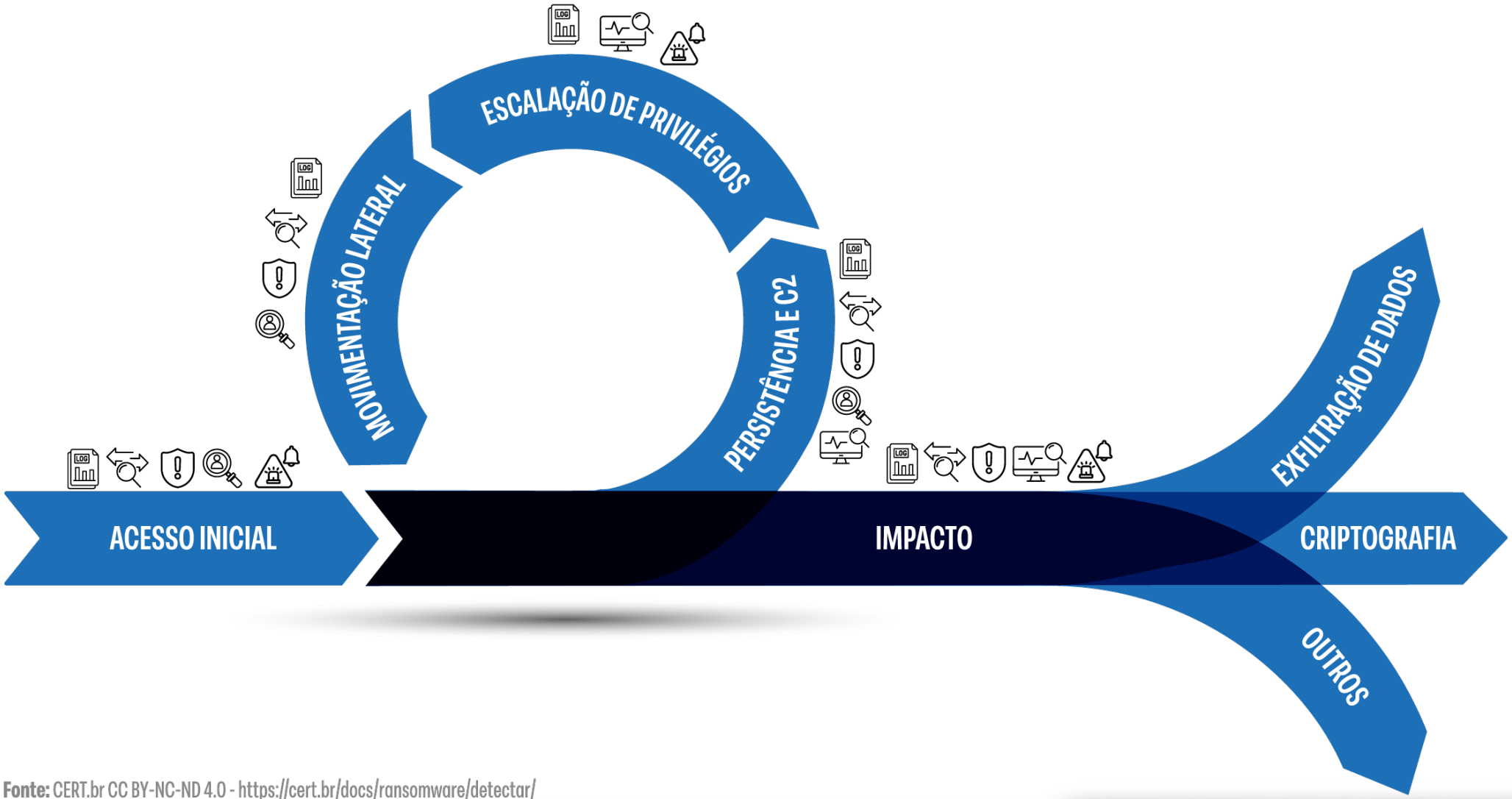
Detecção

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



1. Habilitar e Analisar *Logs*

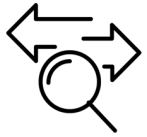
Permite **identificar e rastrear** atividades maliciosas**.**

Essencial para **Detecção** e **Resposta**.

Ative a geração de *logs*
- Dispositivos de rede
- Servidores
- Ferramentas de segurança
- Aplicações
- Serviços de nuvem

Centralize o armazenamento
- Proteja contra acesso indevido e adulteração

Mantenha:
- *Logs* no mesmo fuso horário (ex: UTC)
- Horário de todos dispositivos sincronizados **(**ex: via NTP**)**
  - use uma **fonte confiável de tempo** (ex: NTP.br**)**



2. Monitorar o Tráfego de Rede – Entrada

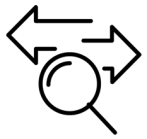
Ajuda a identificar tentativas de **Acesso Inicial**, acessos já efetivados e **Movimentação Lateral.**

Conheça as comunicações legítimas

- tanto da Internet como de redes internas

Monitore:

- **Conexões remotas indevidas**
- **Tentativas sucessivas** de acesso a serviço específico
- **Varreduras** de redes e portas



2. Monitorar o Tráfego de Rede – Saída

Permite identificar ataque em andamento, em especial **exfiltração** de dados e **comunicação com C2**.

Conheça o padrão de tráfego de saída

Monitore:

- **Aumentos atípicos**
  - volume de dados transmitidos
  - tráfego em compartilhamentos de rede
- **Conexões** para endereços **IP ou *links* maliciosos**
- **Consultas DNS**
  - **C2** conhecidos
  - domínios envolvidos com *ransomware*
- Requisições **Tor**
- **Sessões** muito **longas**

3. Observar Alertas de Ferramentas de Proteção

Facilita a **identificação de atividades suspeitas**.

Monitore:

- ***Logs* e alertas**
- As próprias ferramentas
  - desativação
  - alteração de configurações

Bloqueie instalação e execução de *software* não original

4. Monitorar Contas de Usuários e Administradores

Ajuda a detectar **invasão e criação** de contas.

Monitore:

- **Acessos remotos** bem-sucedidos
- Acessos a contas com **privilégios de administrador**
- Acessos a **contas inativas** ou fora do padrão de uso
- **Criação ou alteração** de contas
  - em especial de administrador
- Ataques de **força bruta de credencial**
  - sobretudo autenticação bem-sucedida após várias falhas

5. Monitorar o Uso dos Sistemas

Ajuda a detectar **alterações** no **comportamento** dos sistemas.

Entenda o que é uso “normal”

Monitore:

- **Alterações**
  - **no padrão** de uso de CPU, disco e rede
  - **em configurações** de sistemas
  - em **arquivos críticos**
- **Instalações** de *software*
- Execuções de **processos desconhecidos**
- Acesso a arquivos *decoy* (isca)

6. Estabelecer um Canal para Receber Notificações de Segurança

Ajuda a **identificar vazamentos** de dados, sistemas **infectados**, contas **invadidas** e **vulnerabilidades**.

Crie e monitore canais de comunicação

- Caixas padrão de *e-mail*
  - ex: abuse@dominio e security@dominio
- Arquivo security.txt no *site*

Mantenha **atualizado** o **contato técnico** de WHOIS

Incentive a notificação de problemas de segurança

- Por funcionários e terceiros

Use as notificações:

- Para **treinar ferramentas** de proteção
- Como **alerta** de ataques

Estatísticas do CERT.br

Servidores e Dispositivos de Borda Vulneráveis Notificados Mensalmente

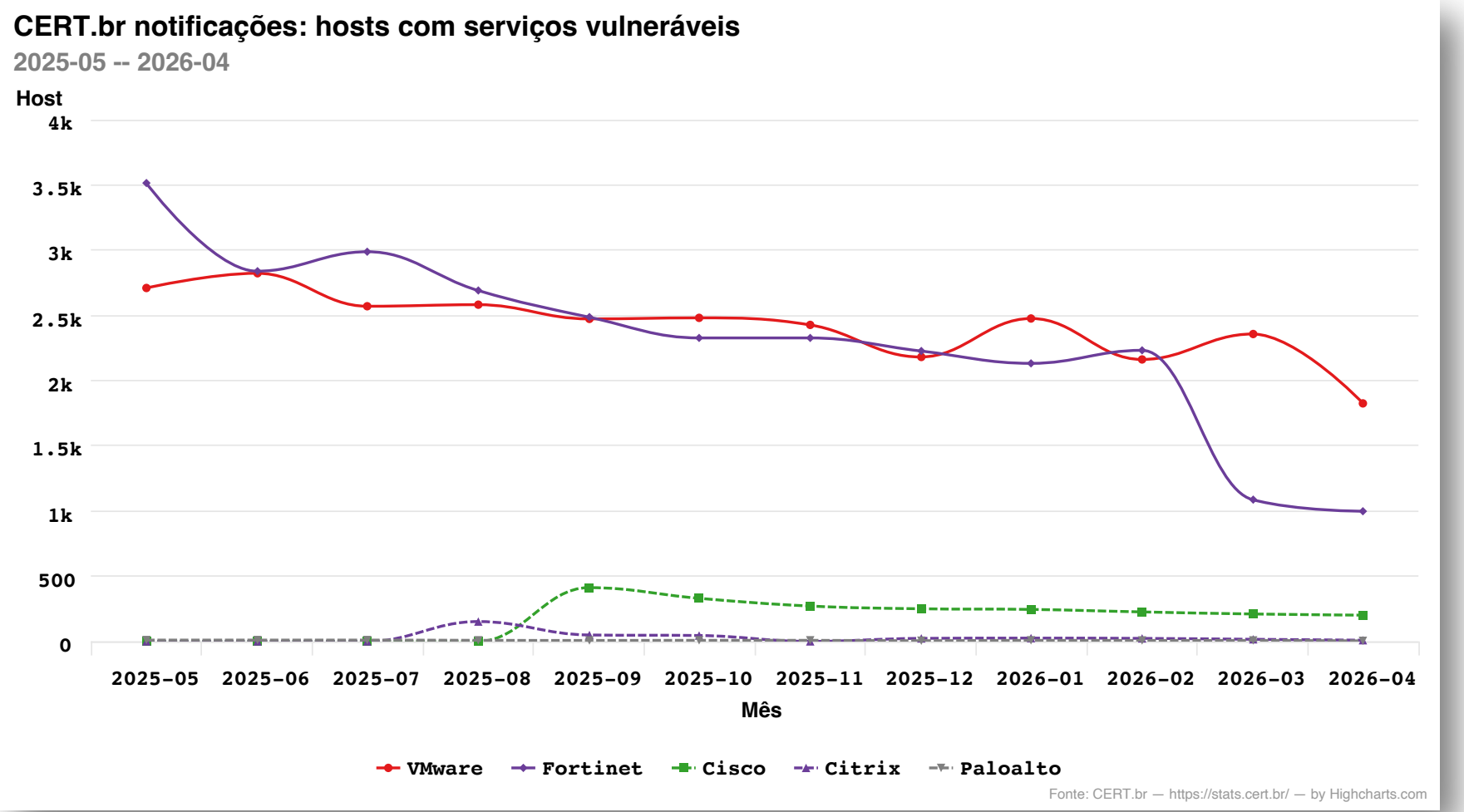
VMware
- CVEs: 14
- CISA KEV: 7
- Usado em *ransomware*: 4

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/

Ransomware: Como Responder

cert.br nic.br cgi.br

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

1. Seguir o Plano de Resposta a Incidentes

Ajuda a **acelerar decisões**, conter o ataque, **reduzir os prejuízos e os esforços** de recuperação.

Tenha um Plano de Resposta a Incidentes que inclua:

- Contatos que devem ser envolvidos
- Funções que devem ser exercidas
- Requisitos e prazos de notificação a órgão regulador
- Passos de resposta a incidente

Treine o plano

- Para que todos saibam desempenhar suas tarefas

Documente

- Decisões, ações tomadas e informações coletadas

2. Conter o Ataque – Proteger Sistemas não Comprometidos

Evita que **mais** sistemas sejam **afetados, limita a perda** de dados e **facilita o retorno** das atividades.

Priorize o isolamento de **sistemas e dados críticos**

- ex: *backups*

Desligue ou desconecte equipamentos **não afetados**

Desligue ou bloqueie a escrita em sistemas de armazenamento e compartilhamento

- ex: NAS, SMB, nuvem

2. Conter o Ataque – Isolar Sistemas Comprometidos

Interrompe a **cadeia de ataque**, a **exfiltração** de dados e a **propagação** do *malware*.

Desconecte:

- Sistemas da rede
  - todos os tipos de conexões
- Dispositivos externos
  - ex: discos e *pen-drives*

Bloqueie conexões maliciosas

- ex: para servidores de C2

Preserve as evidências

- *Dump* de memória
- *Snapshots* de máquinas virtuais e volumes em nuvem

Colete os dados antes de alterar os sistemas

3. Identificar o *Ransomware*

Ajuda a **identificar** sistemas **afetados e vulnerabilidades** exploradas, e avaliar **opções de recuperação**.

Analise:

- Informações da **nota de resgate**
- **Extensão dos arquivos** criptografados
- *Dump* de memória

Busque **decifradores**

- **Alternativa** em caso de *backups* corrompidos
  - use fontes confiáveis

4. Analisar as Informações Coletadas

Ajuda a identificar a **causa raiz** do incidente e dimensionar a **extensão** do incidente.

Pesquise sobre o *ransomware*

- IoC, técnicas e ferramentas usadas

Relacione os dados e determine:

- Ponto de entrada na rede
- Credenciais comprometidas
- Vulnerabilidades exploradas
- Data de início do incidente
- Dados exfiltrados
- Conexões feitas pelo atacante
- Sistemas afetados pelo *malware*

Isole novos sistemas comprometidos identificados

5. Eliminar o *Ransomware*

Visa **erradicar os vestígios** do ataque.

Não basta apenas **deletar** o *malware*.

Reinstale os sistemas comprometidos
- Use **fontes confiáveis**

Aplique todas as **atualizações**
- Em especial as de segurança

Corrija a falha que permitiu o Acesso Inicial
- Mitigue se não for possível corrigir

6. Trocar Senhas e Revisar Acessos

Elimina **acessos e privilégios** obtidos pelo atacante.

Evita que ele **retorne** usando **credenciais comprometidas**.

Altere senhas de **todas** as contas
- Assuma que foram comprometidas e **não são confiáveis**
- Priorize contas com acessos privilegiados

Elimine privilégios desnecessários ou adicionados

Bloqueie ou exclua contas criadas ou reativadas

Habilite a **autenticação multifator** (MFA)

7. Restaurar os Dados e a Conectividade

Visa o **retorno das operações** paralisadas, **sem reinfectar** o ambiente.

Recupere os dados de ***backups* confiáveis**

- De preferência de cópias ***offline***

Na ausência de *backups* confiáveis, tente:

- Usar decifradores
- Recriar usando os recursos disponíveis

Exclua medidas de contenção

Refaça as conexões de rede

8. Melhorar o Ambiente com as Lições Aprendidas

Procura garantir a resolução dos problemas e **evitar** a ocorrência de **novos incidentes**.

Reforce a monitoração e os controles de detecção

Faça um relatório do incidente

Atualize o Plano de Resposta a Incidentes

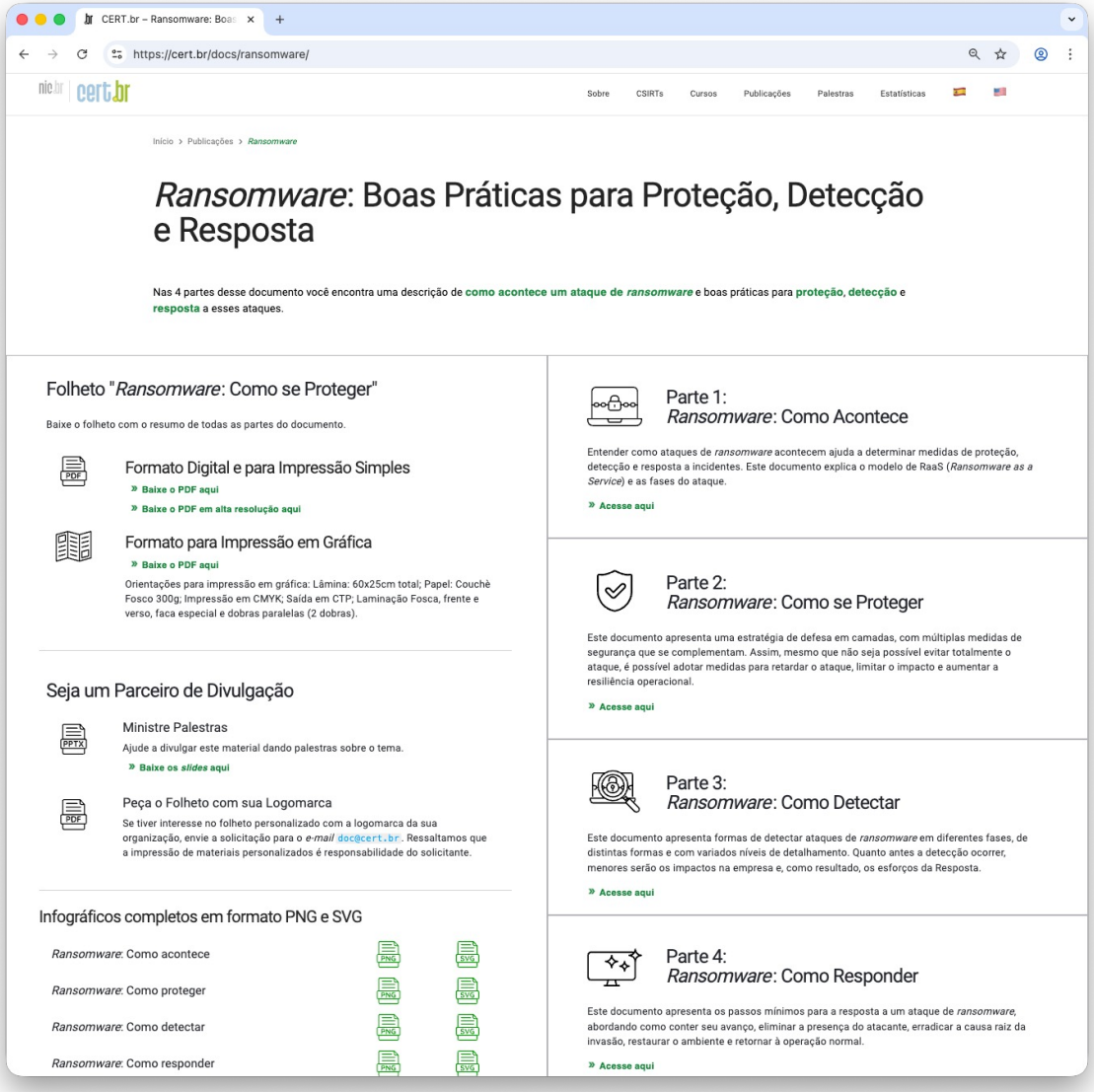
- O que **funcionou**, mas precisa ser ajustado
- O que **não funcionou** e precisa ser corrigido
- O que **faltou** e precisa ser incluído

Reforce as **medidas preventivas**

- Atualize sistemas
- Melhore controles
- Invista em treinamento e conscientização

Leitura Recomendada

Documento Completo e Folheto Resumido



Materiais de Conscientização

cert.br nic.br cgi.br

Cartilha de Segurança para Internet
Fascículos – Versões Digital e Impressão

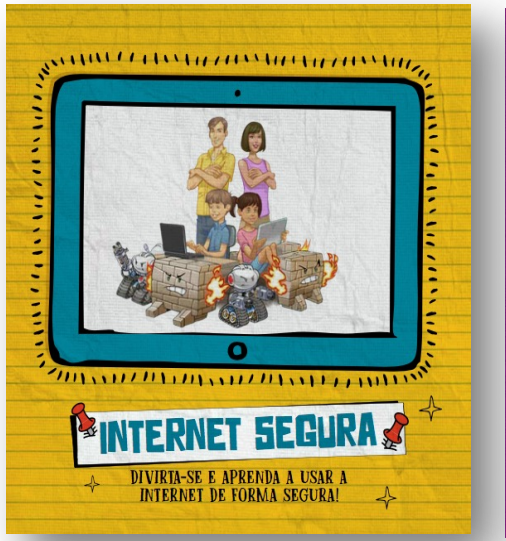
Cartilha de Segurança para Internet

https://cartilha.cert.br/

GOLPES: DESCONFIE. INFORME-SE. VERIFIQUE. CAIU? AJA RÁPIDO.

https://cartilha.cert.br/fasciculos

Portal Internet Segura
Materiais para Diferentes Públicos



https://internetsegura.br/

Projeto Cidadão na Rede
Vídeos Curtos de Diversos Temas

Cidadão na REDE

Cyberbullying: e se fosse com você?

Senhas seguras

Não clique em tudo que receber

Tome cuidado com as informações que você compartilha

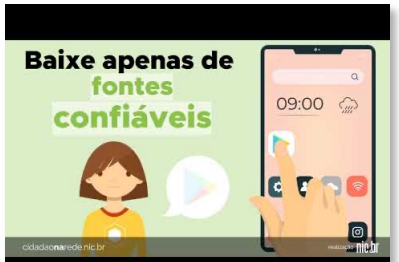
Vazamento de dados

Verificação em dois Fatores

Comprei on-line e me arrependi! O que fazer?

Controle Parental

Compras seguras: use cartão virtual!



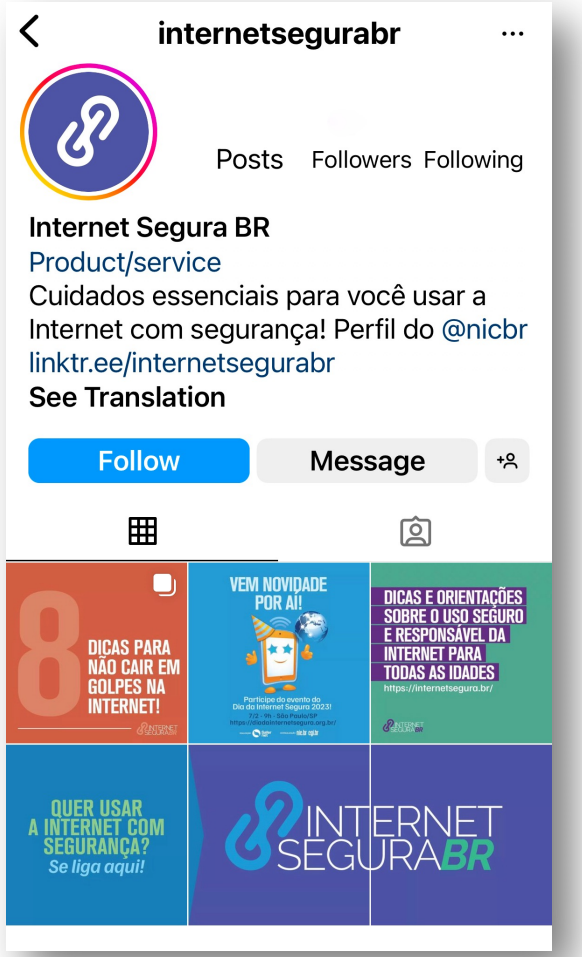
Cuidado com Aplicativos Falsos

Boatos

Não confie em estranhos na Internet!

https://cidadaonarede.nic.br/

Redes Sociais
Perfil @InternetSeguraBR



https://instagram.com/InternetSeguraBR/

Quer Receber ou Personalizar Nossos Materiais?

Guias, Jogos e Fascículos do CERT.br:

– doc@cert.br

Guias #InternetComResponsa

– info@nic.br

Vídeos do Cidadão na Rede

– https://cidadaonarede.nic.br/apoiadores/acesse/

Obrigada

@ miriam@cert.br

@ Notificações para: cert@cert.br 𝕏 @certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br