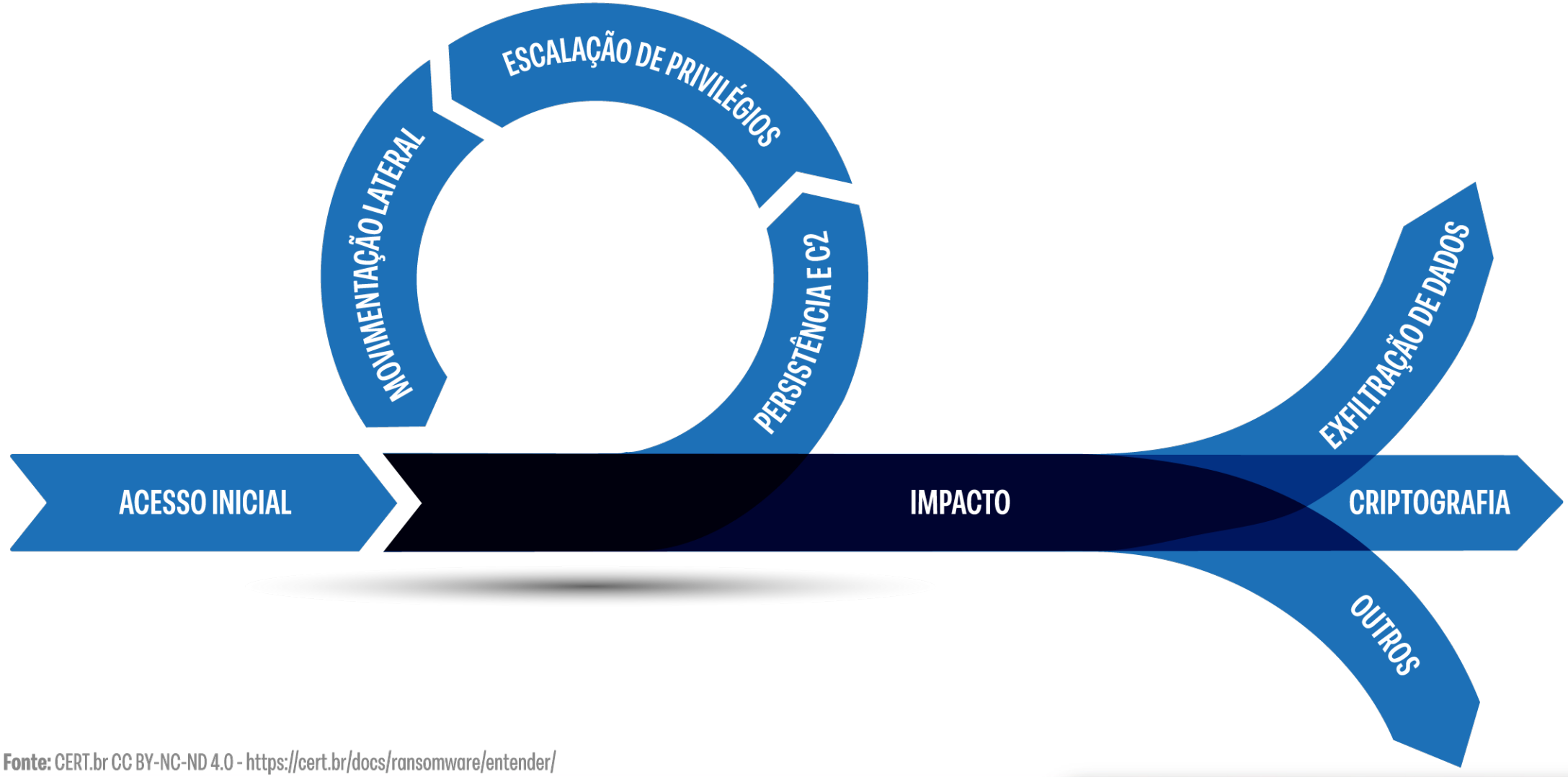
Prevenção e Detecção de *Ransomware*: Onde as Grandes Vítimas estão Errando?

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

Mês da Cibersegurança – Petrobras
04 de novembro de 2025

cert.br nic.br cgi.br

Ciclo de Vida de um Ataque de *Ransomware*



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

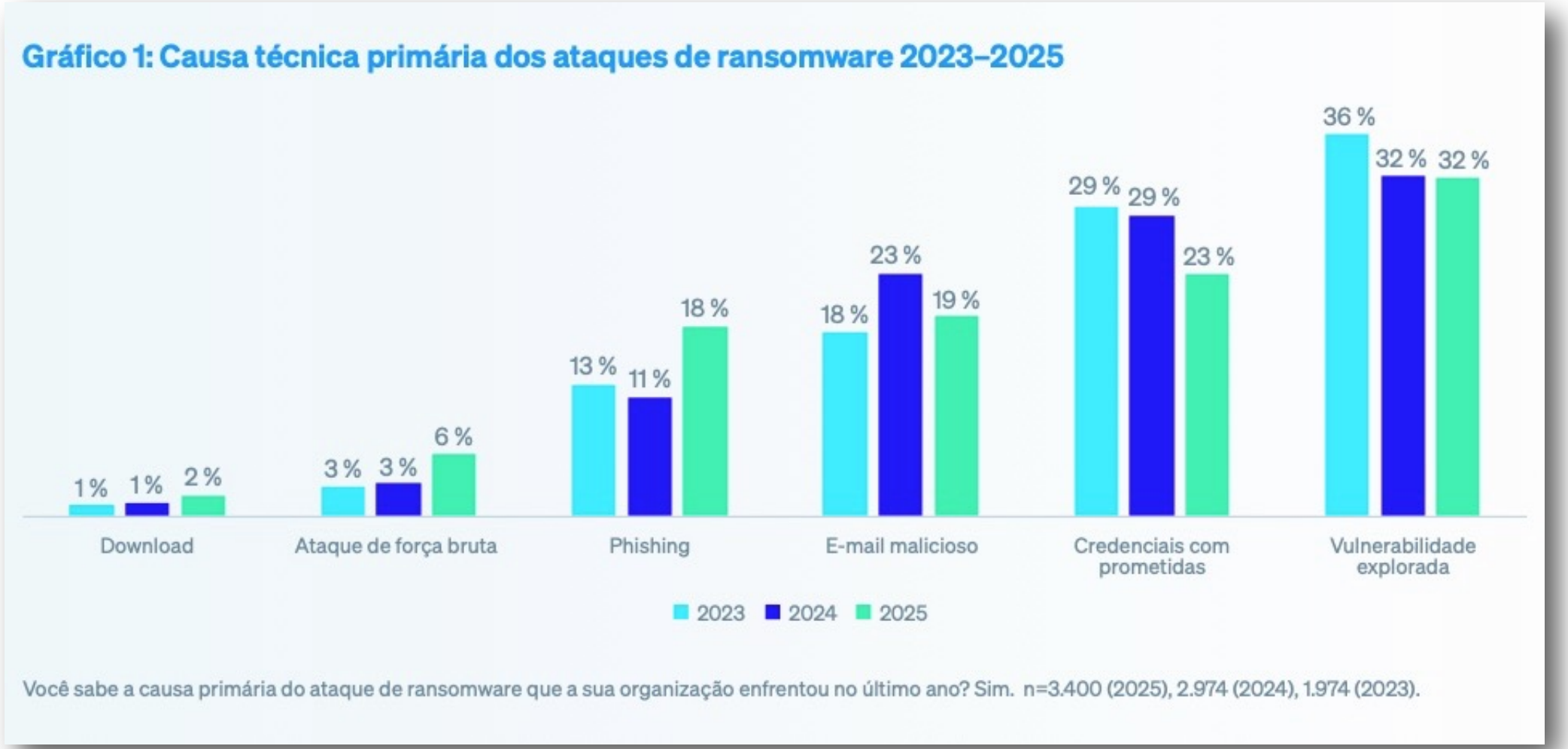
- ACESSO INICIAL
- PERSISTÊNCIA E C2
- ESCALAÇÃO DE PRIVILÉGIOS
- MOVIMENTAÇÃO LATERAL
- **IMPACTO**

  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



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

A Princípio, nada de novo...

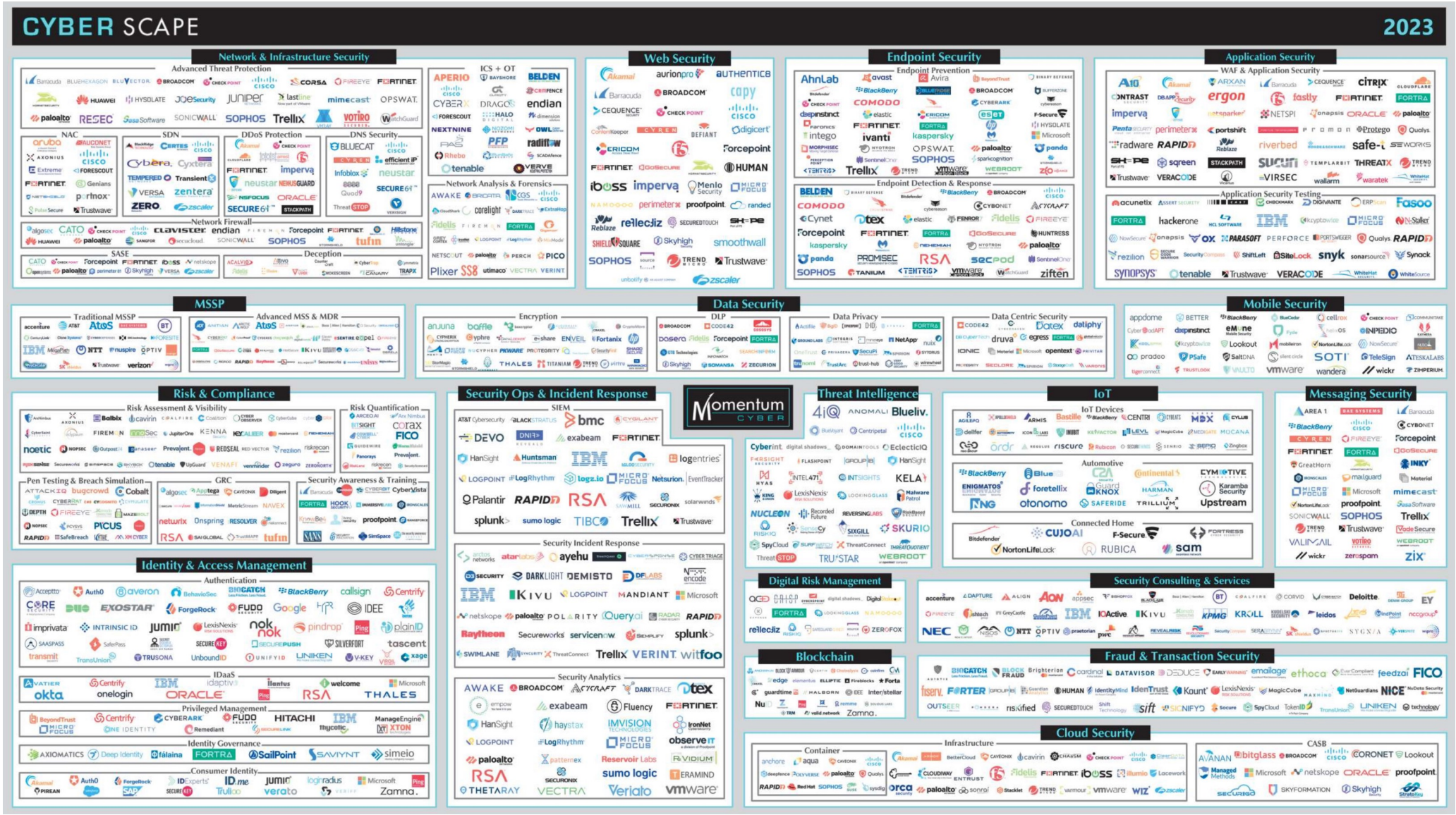
Por que, então, tantos incidentes com vítimas de grande porte?

As empresas não tem ferramentas e investem em proteção e detecção?

Não seria possível prevenir ou detectar nas fases iniciais?

Temos Abundância de Ferramentas e Provedores de Soluções

TLP:CLEAR



Fonte: https://www.shteinsolutions.com/cyberscape/index.html

TLP:CLEAR

Industrial Cyber

Search | Register | Login

Channels | Features | News | Vendor Directory | Resources | Webinars & Events | Team

Home · Attacks and Vulnerabilities · Half of 2025 ransomware attacks hit critical sectors as manufacturing, healthcare, and energy top global targets

The manufacturing sector experienced the sharpest growth, with attacks surging 61% compared with the previous year. High-profile incidents included Jaguar Land Rover's global shutdown and Bridgestone's production disruptions, illustrating how ransomware can paralyze supply chains and economies. Together, these high-profile

Among 103 active ransomware groups, just five, including Qilin, Clop, Akira, Play, and SafePay, were responsible for nearly 25% of all incidents, highlighting the growing professionalization and consolidation within cybercriminal ecosystems.

Attacks And

SOC & Incident Response Threat Landscape

Half of 2025 ransomware attacks hit critical sectors as manufacturing, healthcare, and energy top global targets

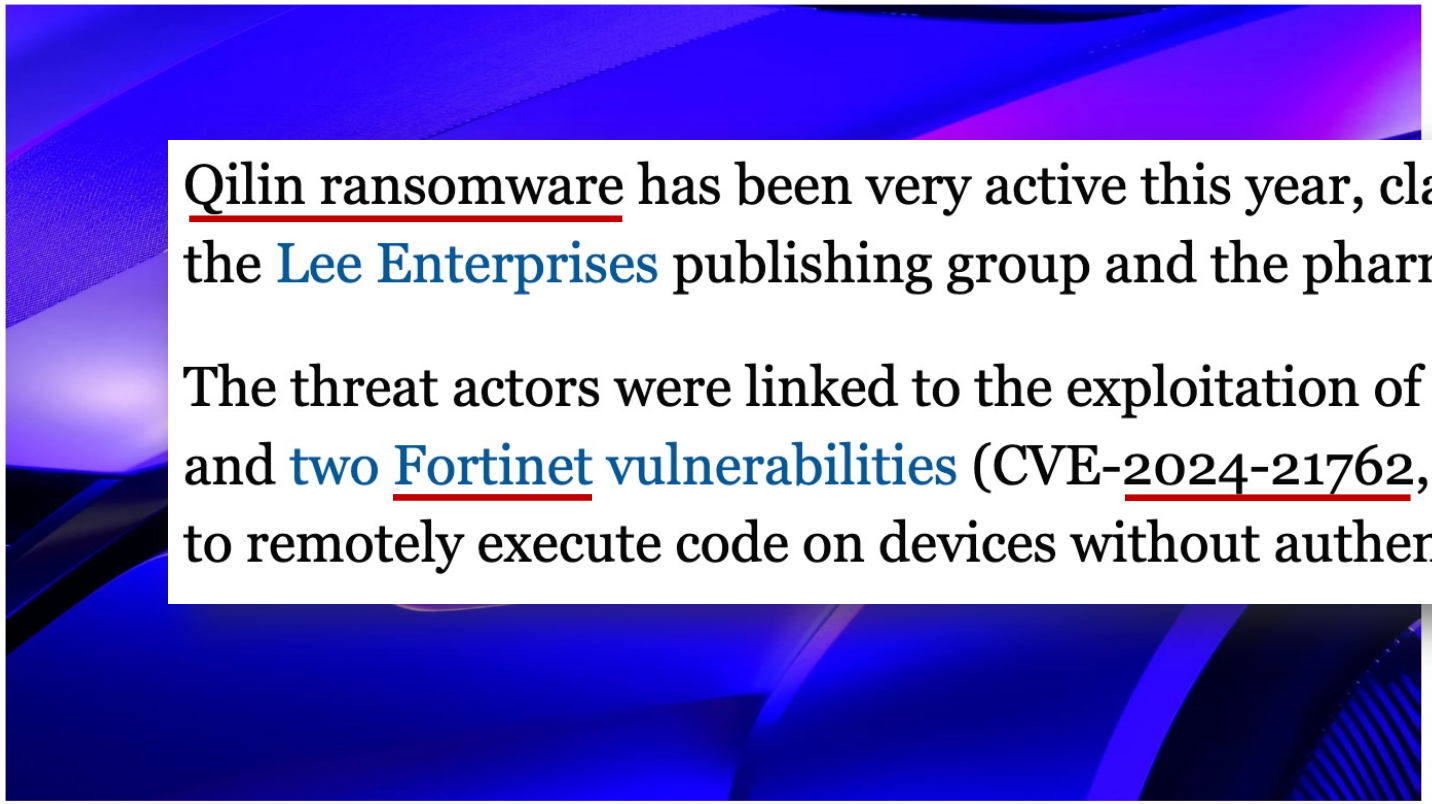
OCTOBER 22, 2025

Fonte: https://industrialcyber.co/reports/half-of-2025-ransomware-attacks-hit-critical-sectors-as-manufacturing-healthcare-and-energy-top-global-targets/

TLP:CLEAR

Nissan confirms design studio data breach claimed by Qilin ransomware

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



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.

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).

Fonte: https://www.bleepingcomputer.com/news/security/nissan-confirms-design-studio-data-breach-claimed-by-qilin-ransomware/

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

TLP:CLEAR

Estatísticas do CERT.br

Servidores e Dispositivos de Borda Vulneráveis Notificados Mensalmente

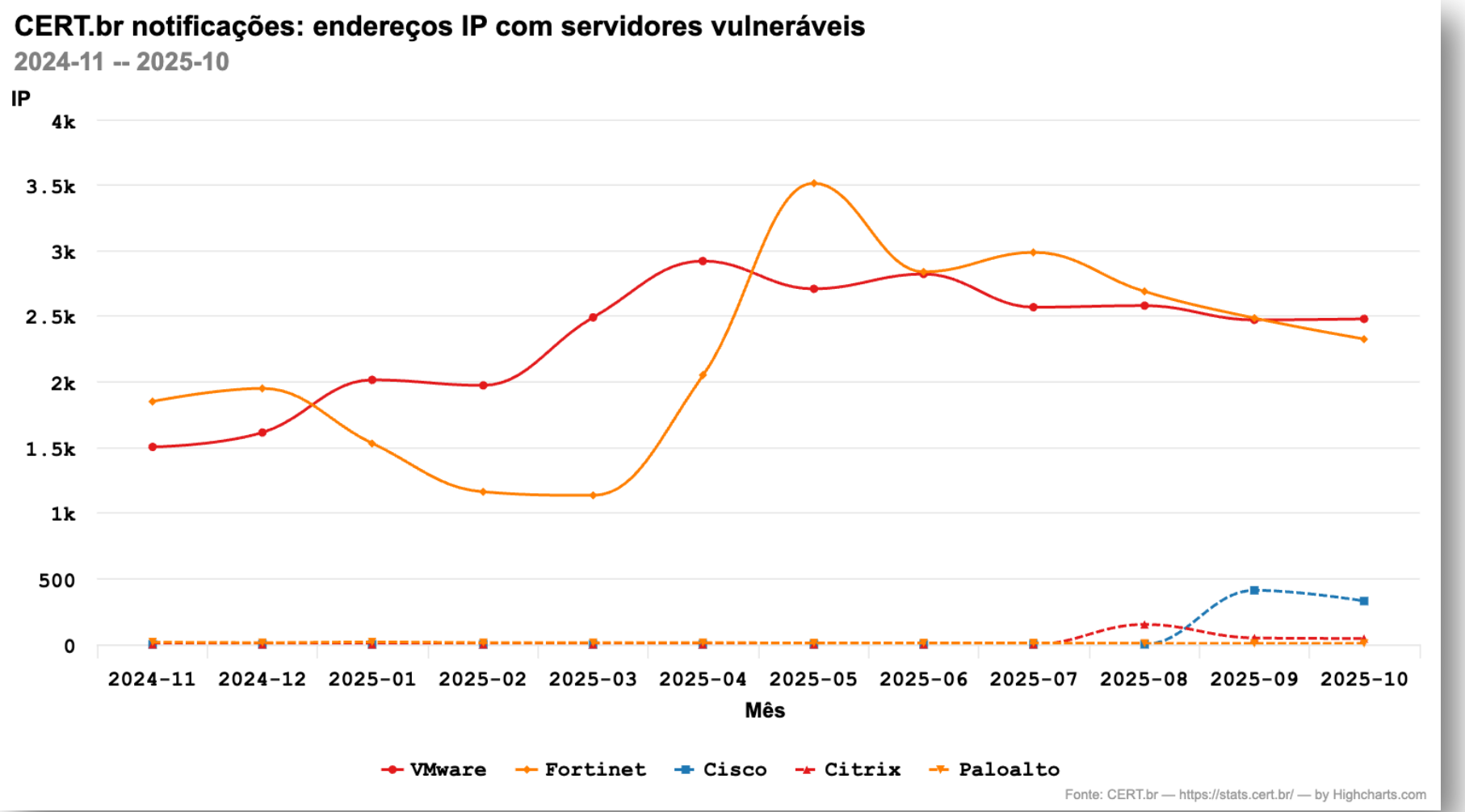
VMware
- CVEs: 14
- CISA KEV: 7
- Usado em *ransomware*: 4

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

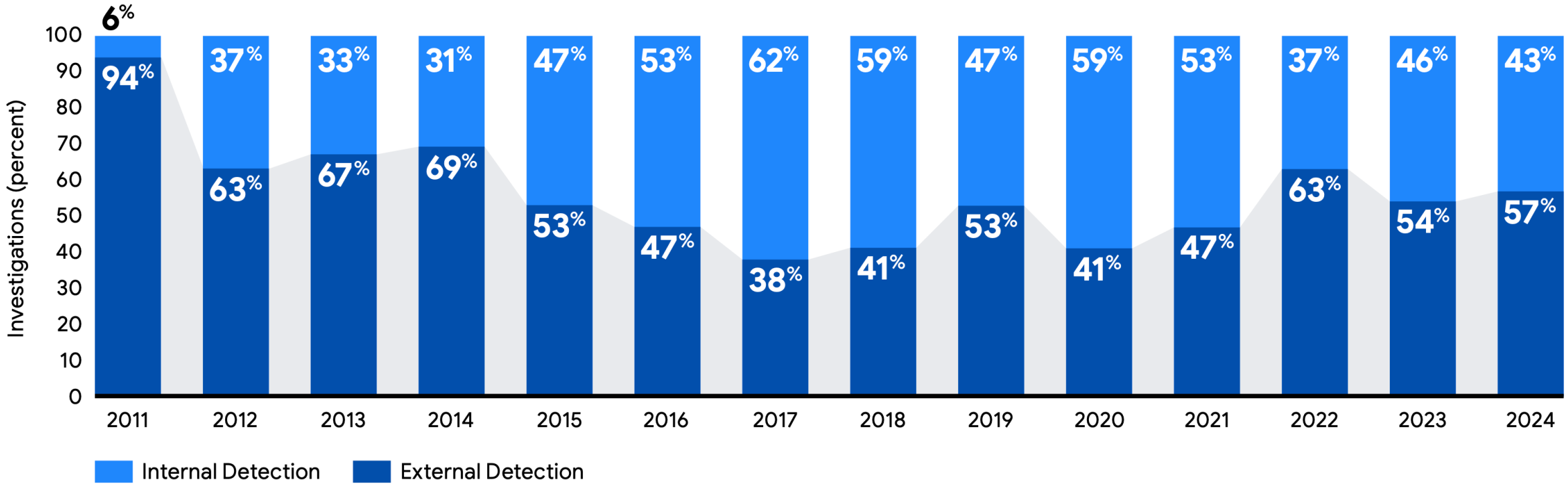
Paloalto
- CVEs: 1
- CISA KEV: 1
- Usado em *ransomware*: 1



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

Mandiant M-Trends 2025

Incidentes Detectados Internamente vs. Notificados por Fontes Externas



Fonte: https://services.google.com/fh/files/misc/m-trends-2025-en.pdf

Algo está faltando…

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.

Mesmo que não impeçam todas as fases, podem **retardar o ataque, limitar o impacto** e **aumentar a resiliência** operacional da empresa.

1. Usar Autenticação Multifator (MFA)

2. Fazer Gestão de Vulnerabilidades

3. Conscientizar Funcionários

4. Usar Ferramentas de Proteção

5. Fazer e Proteger *Backups*

6. Reduzir a Superfície de Ataque

7. Gerenciar Identidades e Acessos

8. Segmentar a Rede

Aplicar Correções não é Trivial

- **Mais da metade** das organizações só conseguem **aplicar patches em 15.5%** dos CVEs/mês
  - ¼ corrige menos de 6.6% dos CVEs
- **Mas apenas de 5%** dos CVEs são ativamente **explorados**
  - boa parte com CVSS < 7
- 32% das top 100 vulnerabilidades exploradas na lista do ShadowServer são "*vintage vulnerabilities*"
- CISA KEV (*Known Exploited Vulnerabilities*) tem 46% de "*vintage vulnerabilities*"

Fontes: https://arxiv.org/pdf/2302.14172 | https://www.first.org/resources/papers/vulncon2024/VulnCon-Why-Can-t-We-All-Just-Get-Along.pdf

Priorização de *Patches* com Base em Risco

Queremos responder essa pergunta:

Qual o risco de uma vulnerabilidade
ser ativamente explorada **e** causar um impacto negativo?

Ou seja, **quais patches** eu preciso **aplicar agora e quais podem esperar** a próxima janela de manutenção?

Conhece-te a ti mesmo...

Para poder priorizar é necessário ter um mapeamento completo

- Análise de risco, aka, “Joias da Coroa”
  - tanto de dados, quanto de sistemas
- Determinar todas as versões de *software*
  - não é suficiente depender de banner de aplicação
  - precisa mapear os pacotes e as dependências
- Não esquecer daquilo que é desenvolvido localmente
  - bancos de dados, personalizações, APIs, aplicativos, etc, etc
  - também é necessário mapear os *frameworks*, os pacotes e as dependências utilizadas
  - DevSecOps precisa gerar e consumir: SBOM (SPDX ou CycloneDX), VEX e CSAF
- Não esquecer da nuvem!

Ecossistema de Identificação de *Software*

Padrões para Identificação Unívoca de *Software e suas* Dependências

- **CPE** – Common Platform Enumeration
  - was designed for operating systems, applications, and hardware devices. CPE is maintained by the NVD.
  - `cpe:<cpe_version>:<part>:<vendor>:<product>:<version>:<update>:<edition>:<language>:<sw_edition>:<target_sw>:<target_hw>:<other>`
- **PURL** – Package URL
  - standardizes how software package metadata is represented so they can universally be identified and located
  - ex: `pkg:pypi/django@3.2.5. ; pkg:maven/org.apache.commons/commons-lang3@3.12.0 ; pkg:generic/libpng@1.6.37?download_url=https://sourceforge.net/projects/libpng/`
- **OmniBOR**
  - capable of identifying every source code file incorporated into each built artifact
    - Artifact ID – a SHA256 hash of the artifact
    - Input Manifest – a text file which records information about the inputs used to build a software artifacts. By "inputs" we mean anything provided to a build tool in order to produce the artifact.

Fontes: https://nvd.nist.gov/products/cpe | https://github.com/package-url/purl-spec | https://omnibor.io/

Risco de Ser Explorado e Causar Impacto Significativo

Padrões para Severidade, Probabilidade de Exploração e Impacto

Vulnerabilidade + **Prob. Exploração** + **Impacto**

CVSS COMMON VULNERABILITY SCORING SYSTEM + **CISA KEV e EPSS** Exploit Prediction Scoring System + **SSVC**

O CVSS dá uma nota para a vulnerabilidade sozinha, “no vácuo”. Não leva em conta o contexto:

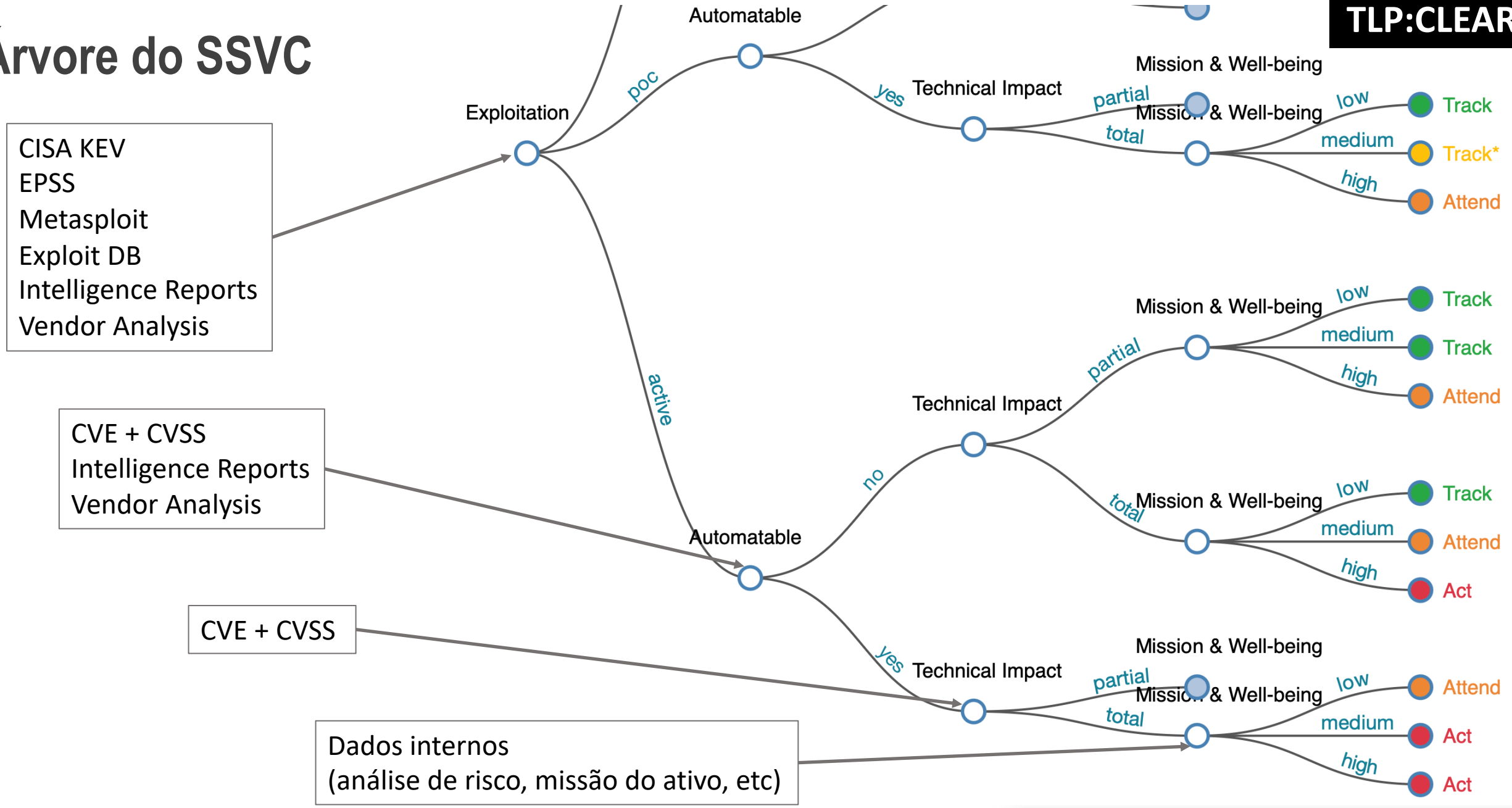
- É explorável no contexto onde é usada?
- Tem mecanismos de proteção ou defesas no ambiente?
- Qual o impacto para mim?

CISA KEV: “ground thruth”, mas limitado ao contexto do ambiente do público alvo do CISA.

EPSS: é uma previsão, como a do tempo, e podem ocorrer tempestades quando a previsão era de sol!

Requer conhecer em detalhes seu parque e ter um bom **mapeamento de ativos**, **versões**, **configurações** e uma boa **análise de risco**. **Você sabe**, mesmo, **todas as dependências** dos *softwares* que usa?

Árvore do SSVC

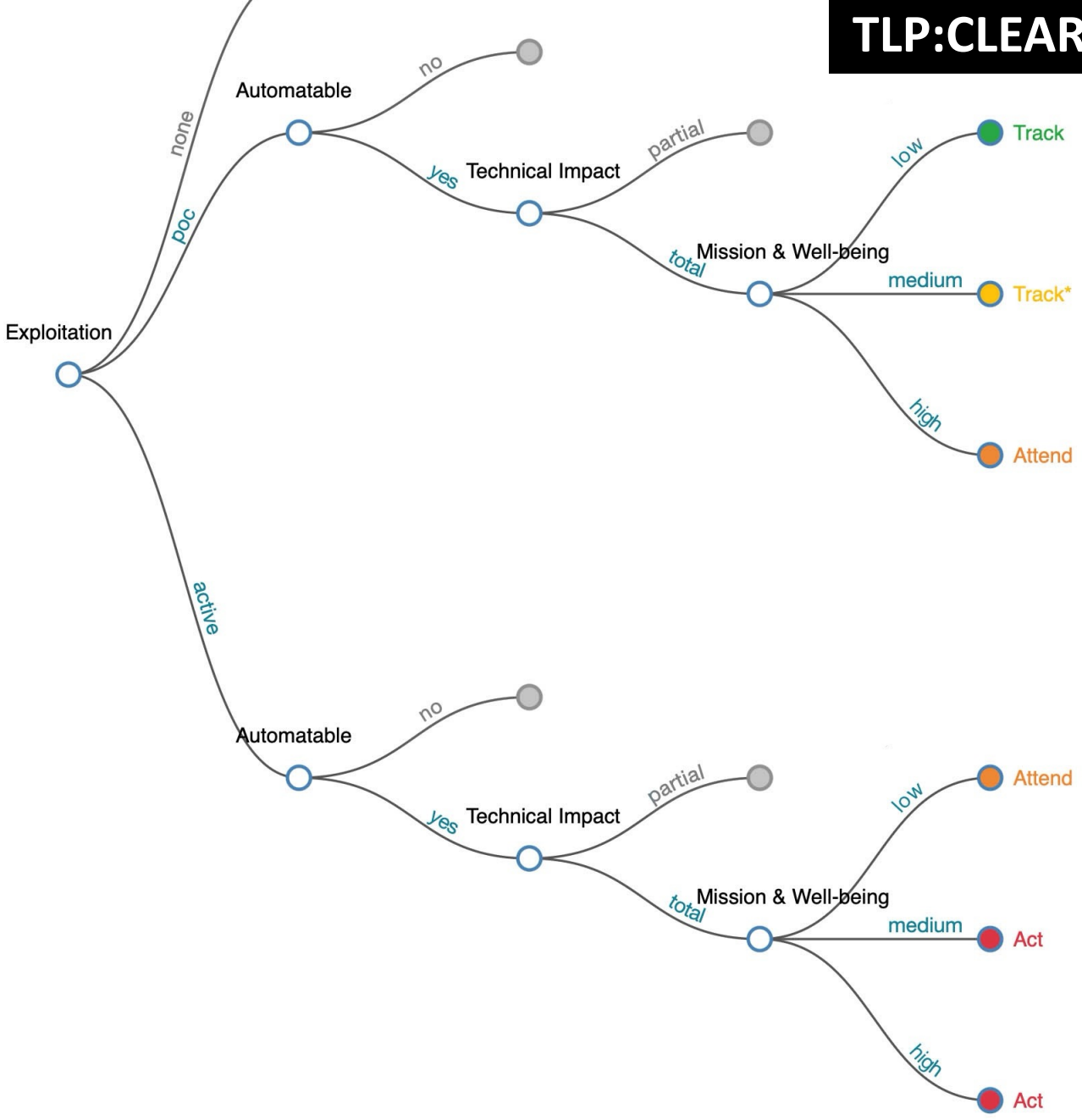


TLP:CLEAR

Making SSVC Easier: **CISA *Vulnrichment***

- Agrupamento, em um único local, de informações sobre vulnerabilidades que preencham uma destas condições:
  - **`"Exploitation": ”yes”`**
  - **`"Exploitation": "poc”`**
  - **`"Automatable": "yes”`**
  - **`"Technical Impact": "total”`**

- Para cada CVE, o seu **`json`** passa a incluir os detalhes de:
  - CWE e CVSS



Fontes: https://github.com/cisagov/vulnrichment

Assuma o Controle da Priorização da Aplicação de Patches

É URGENTE conseguir identificar os patches imprescindíveis

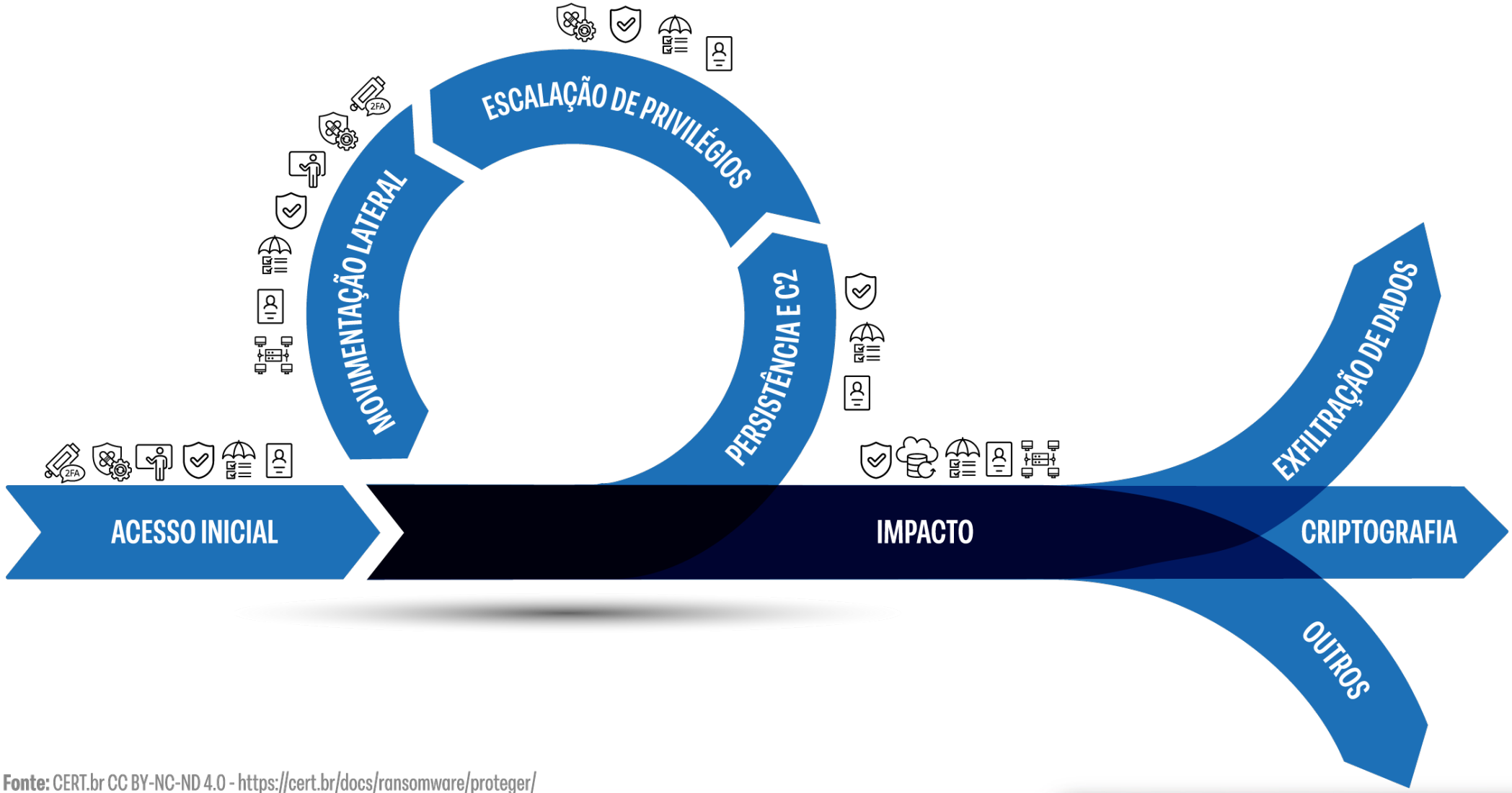
- "É pra ontem"
  - Se o CERT.br notificar (https://stats.cert.br/vulns/)
  - Se estiver no CISA KEV (https://cisa.gov/kev/)
- Aplicar assim que possível
  - Se for em um ativo que se parar, impede sua organização de funcionar
  - Se atingir os critérios do CISA Vulnrichment (https://github.com/cisagov/vulnrichment)
  - Se o percentil do EPSS for muito alto (https://www.first.org/epss/)

- Sim, é difícil instalar todos os patches
  - entre outras coisas, faltam tempo e pessoal capacitado

Quem assume o risco, em última instância, é você e sua organização

- Não use apenas CVSS como critério, ele não foi feito para priorização!
- Cobre seu fornecedor de ferramentas de gestão de vulnerabilidades
  - Desconfie se a resposta for muito simplista
  - É OK ter uma métrica própria, mas é necessário saber algo sobre quais métricas são usadas
  - Verifique se ele já não integra EPSS e/ou SSVC
  - Cobre que consuma o VEX do fabricante
- Complemente com sua própria avaliação
  - Os dados são todos públicos

Proteção
Um único Mecanismo Pode ser Usado para Múltiplas Defesas



Detecção

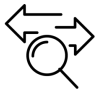
Detectar o Quanto Antes para Minimizar ou até Evitar o Impacto

A **detecção** pode ocorrer nas **diferentes fases** e ***de* distintas formas.**

Quanto antes detectar, **menores** serão os **impactos**.

É necessário **preparar o ambiente** para **monitorar** e **detectar** as atividades dos atacantes.

1. Habilitar e Analisar *Logs*



2. Monitorar o Tráfego de Rede

3. Observar Alertas de Ferramentas de Proteção

4. Monitorar Contas de Usuários e Administradores

5. Monitorar o Uso dos Sistemas

6. Estabelecer um Canal para Receber Notificações de Segurança

Detecção

Toda a Detecção Decorre da Análise de Dados em um Espectro

Ataques conhecidos

- São o foco das ferramentas e times de segurança
  - SOC, SOAR, SIEM, *DR, Segurança de perímetro, etc, etc
- Todos atuam com base no que já foi determinado como ataque
- Mesmo sistemas com IA
  - ele precisam ser treinados com ataque vs. legítimo
  - vantagem é que identificam variantes
  - não detectam algo realmente novo

Comportamentos e ataques desconhecidos

Comportamentos legítimos e erros de sistema

- Podem ser ignorados por sistemas de SOC
- Mas são importantes para detecção de incidentes no escopo ITIL, mas sem impacto direto em integridade e confidencialidade, como por exemplo
  - falhas de *hardware*
  - erros de configuração
  - erros de processo

Detecção
Toda a Detecção Decorre da Análise de Dados em um Espectro

Ataques conhecidos

- São o foco das ferramentas e times de segurança
  - SOC, SOAR, SIEM, *DR, Segurança de perímetro, etc, etc
- Todos atuam com base no que já foi determinado como ataque
- Mesmo sistemas com IA
  - ele precisam ser treinados com ataque vs. legítimo
  - vantagem é que identificam variantes
  - não detectam algo realmente novo

Comportamentos e ataques desconhecidos

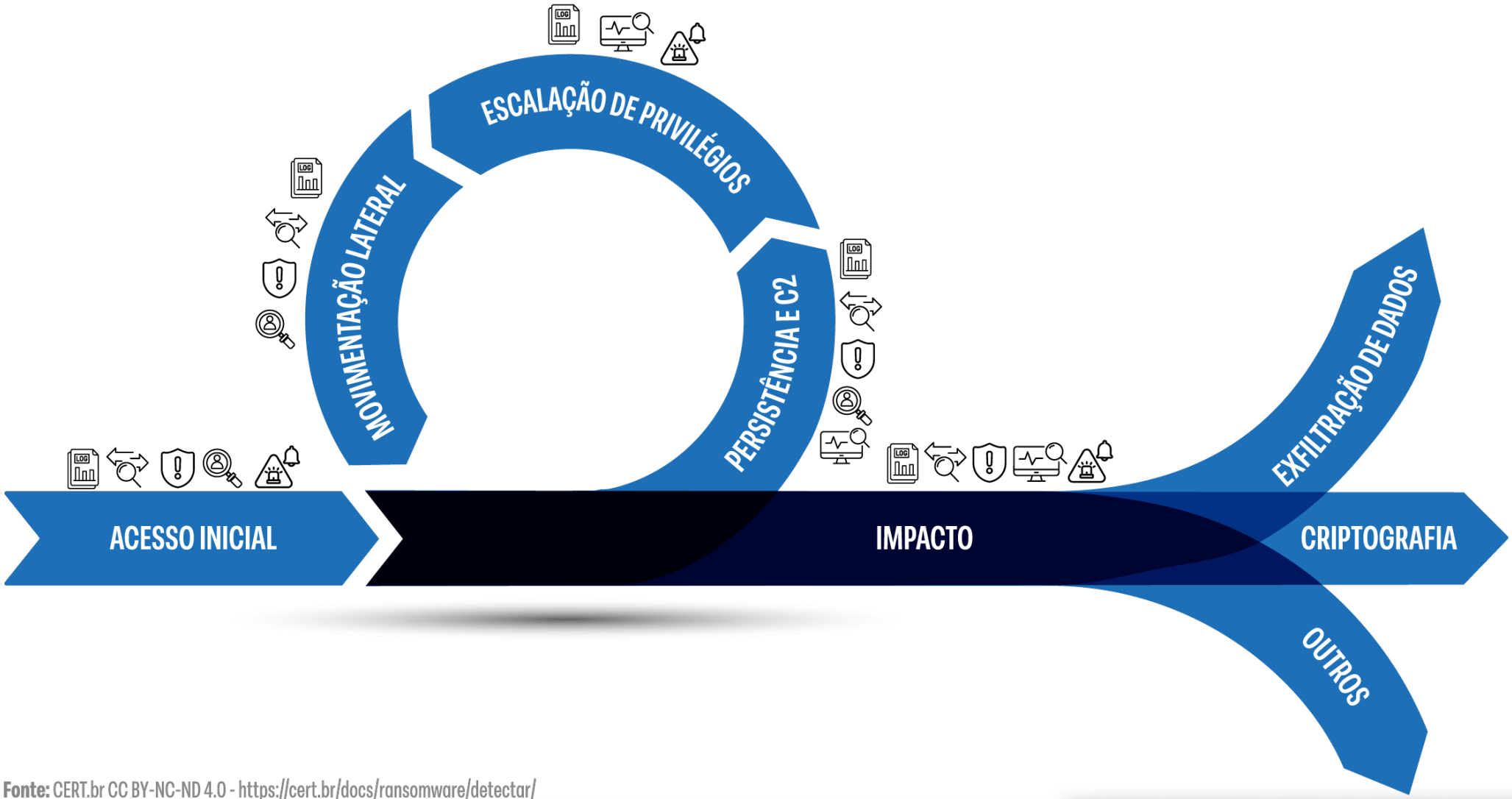
- Ambiente instrumentado
  - telemetria de rede (netflow) é essencial
- Analistas
  - pessoas fazem a real detecção
  - ferramentas lidam com o conhecido
  - não precisa ser um time de *threat hunting*
- Estabeleça canais para receber notificações externas
  - e-mails do SOC, abuse ou CSIRT
  - RFC 9116
    `https://[xxx]/.well-known/security.txt`

Comportamentos legítimos e erros de sistema

- Podem ser ignorados por sistemas de SOC
- Mas são importantes para detecção de incidentes no escopo ITIL, mas sem impacto direto em integridade e confidencialidade, como por exemplo
  - falhas de *hardware*
  - erros de configuração
  - erros de processo

Detecção

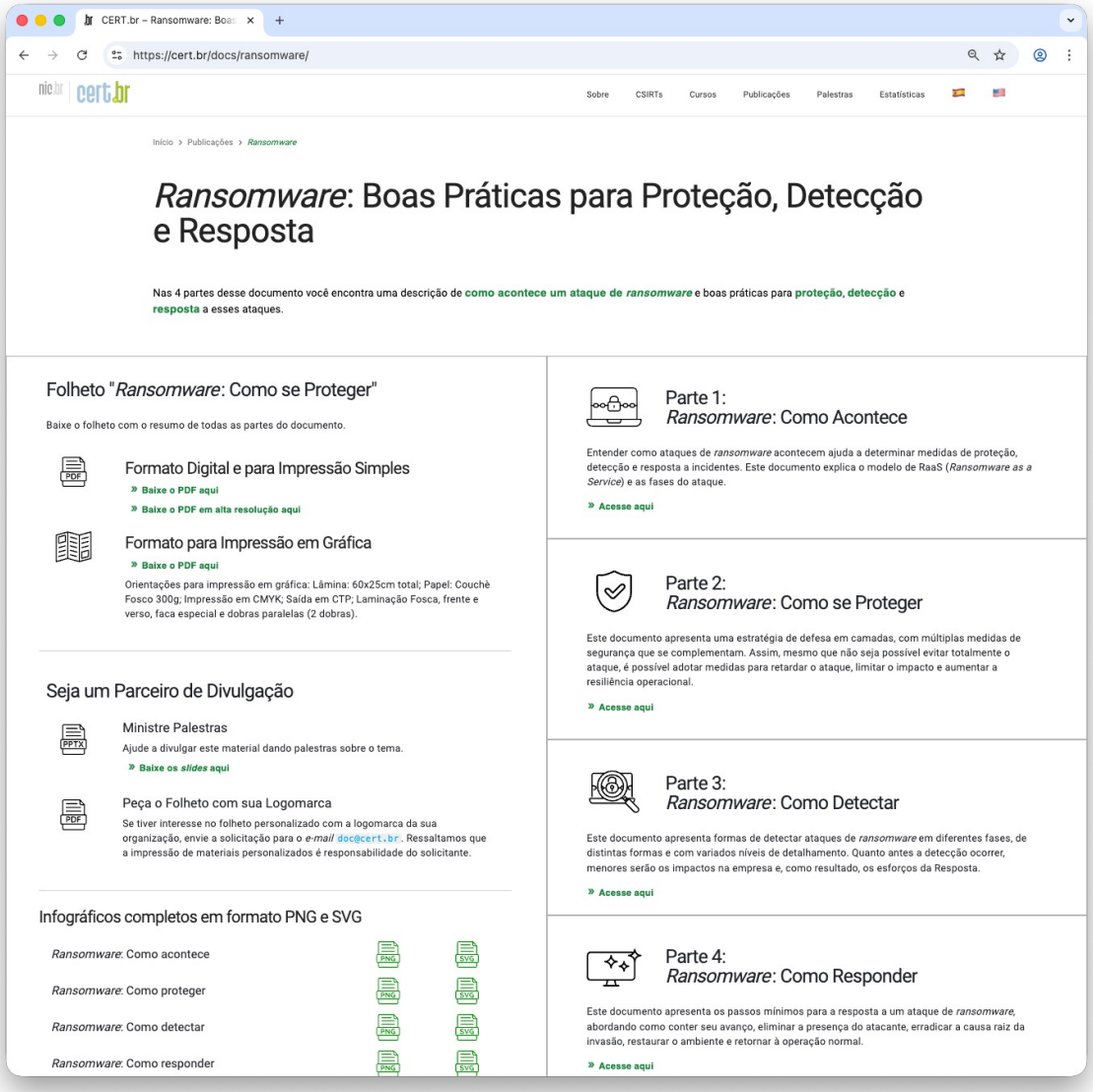
Detectar o Quanto Antes para Minimizar ou até Evitar o Impacto



Leitura Recomendada

Documento Completo e Folheto Resumido

TLP:CLEAR



CERT.br – Ransomware: Boas

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

nic.br | cert.br

Sobre CSIRTs Cursos Publicações Palestras Estatísticas

Início › Publicações › *Ransomware*

Ransomware: Boas Práticas para Proteção, Detecção e Resposta

Nas 4 partes desse documento você encontra uma descrição de **como acontece um ataque de *ransomware*** e boas práticas para **proteção**, **detecção** e **resposta** a esses ataques.

Folheto "*Ransomware*: Como se Proteger"

Baixe o folheto com o resumo de todas as partes do documento.

Formato Digital e para Impressão Simples

» Baixe o PDF aqui

» Baixe o PDF em alta resolução aqui

Formato para Impressão em Gráfica

» Baixe o PDF aqui

Orientações para impressão em gráfica: Lâmina: 60x25cm total; Papel: Couchè Fosco 300g; Impressão em CMYK; Saída em CTP; Laminação Fosca, frente e verso, faca especial e dobras paralelas (2 dobras).

Seja um Parceiro de Divulgação

Ministre Palestras

Ajude a divulgar este material dando palestras sobre o tema.

» Baixe os *slides* aqui

Peça o Folheto com sua Logomarca

Se tiver interesse no folheto personalizado com a logomarca da sua organização, envie a solicitação para o *e-mail* doc@cert.br. Ressaltamos que a impressão de materiais personalizados é responsabilidade do solicitante.

Infográficos completos em formato PNG e SVG

Ransomware: Como acontece

Ransomware: Como proteger

Ransomware: Como detectar

Ransomware: Como responder

Parte 1: *Ransomware*: Como Acontece

Entender como ataques de *ransomware* acontecem ajuda a determinar medidas de proteção, detecção e resposta a incidentes. Este documento explica o modelo de RaaS (*Ransomware as a Service*) e as fases do ataque.

» Acesse aqui

Parte 2: *Ransomware*: Como se Proteger

Este documento apresenta uma estratégia de defesa em camadas, com múltiplas medidas de segurança que se complementam. Assim, mesmo que não seja possível evitar totalmente o ataque, é possível adotar medidas para retardar o ataque, limitar o impacto e aumentar a resiliência operacional.

» Acesse aqui

Parte 3: *Ransomware*: Como Detectar

Este documento apresenta formas de detectar ataques de *ransomware* em diferentes fases, de distintas formas e com variados níveis de detalhamento. Quanto antes a detecção ocorrer, menores serão os impactos na empresa e, como resultado, os esforços da Resposta.

» Acesse aqui

Parte 4: *Ransomware*: Como Responder

Este documento apresenta os passos mínimos para a resposta a um ataque de *ransomware*, abordando como conter seu avanço, eliminar a presença do atacante, erradicar a causa raiz da invasão, restaurar o ambiente e retornar à operação normal.

» Acesse aqui

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