Ransomware, muito além de uma infecção por *malware*

Dra. Cristine Hoepers
Gerente, CERT.br/NIC.br
cristine@cert.br

Dr. Klaus Steding-Jessen
Gerente Técnico, CERT.br/NIC.br
jessen@cert.br

Reunião de Estudos Técnicos, ANPD – 08 de novembro de 2024

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: Membro pleno desde 2002 **TF-CSIRT Trusted Introducer:** *Accredited* desde 2020

APWG: *Research partner* desde 2004 **SEI/CMU:** Cursos autorizados desde 2003

***Honeynet Project*:** Mantém o capítulo do Brasil desde 2003

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

Foco do CERT.br nestes 27 anos:
Aumentar a Capacidade Nacional de Tratamento de Incidentes

Nenhum time ou estrutura única conseguirá fazer sozinho a segurança ou a resposta a incidentes

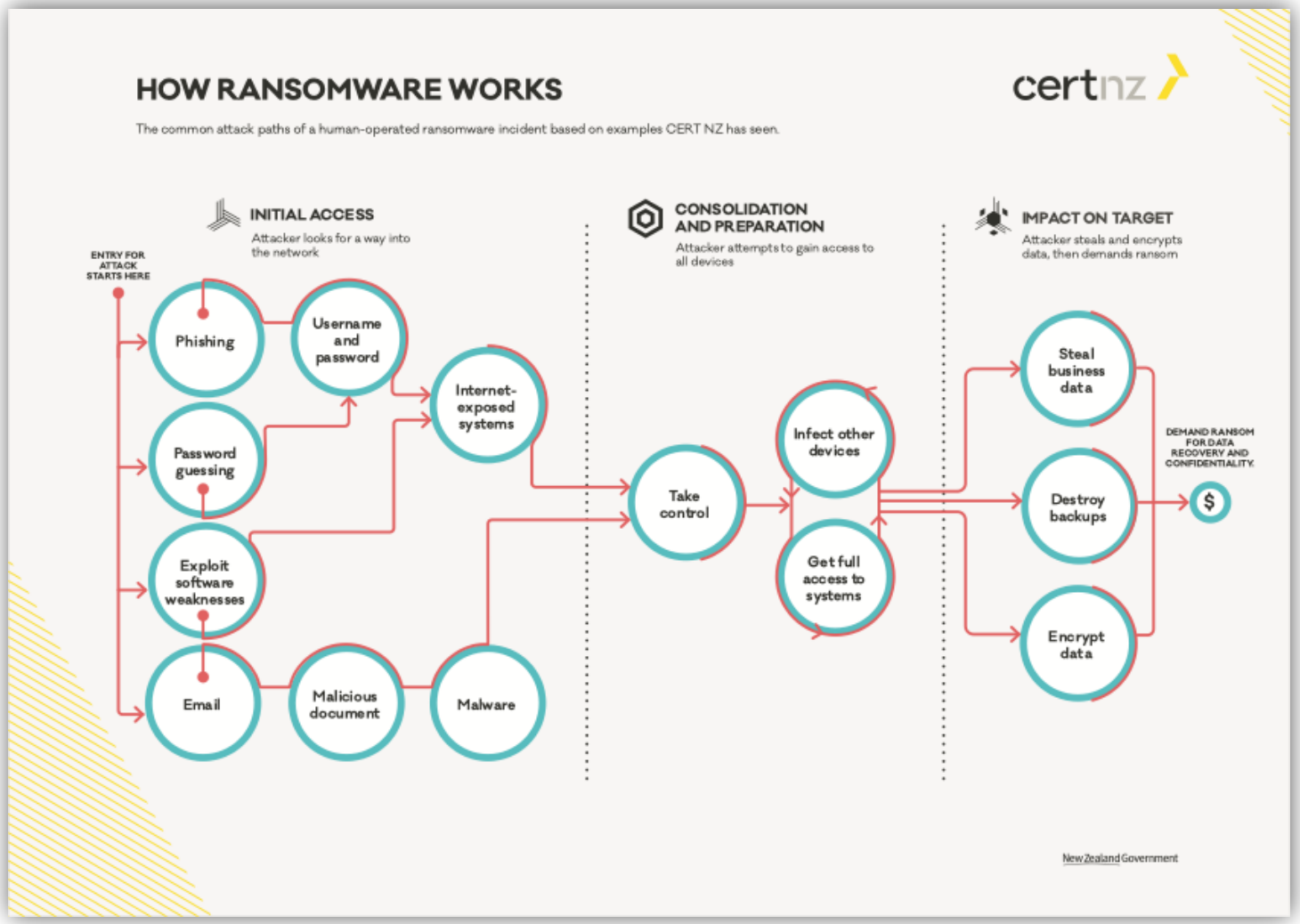
Fomentar e Fortalecer a Comunidade Nacional

- Ações junto a setores chave, para **criação e treinamento de Times** de Tratamento de Incidentes de Segurança (CSIRTs)
- **Auxiliar na análise** técnica e **facilitar** o tratamento de incidentes por outros CSIRTs
- Gerar massa crítica para possibilitar a **cooperação** e melhora na segurança das redes
- Ter uma visão sobre as principais **tendências** de ataques no Brasil

Participar da Comunidade Internacional

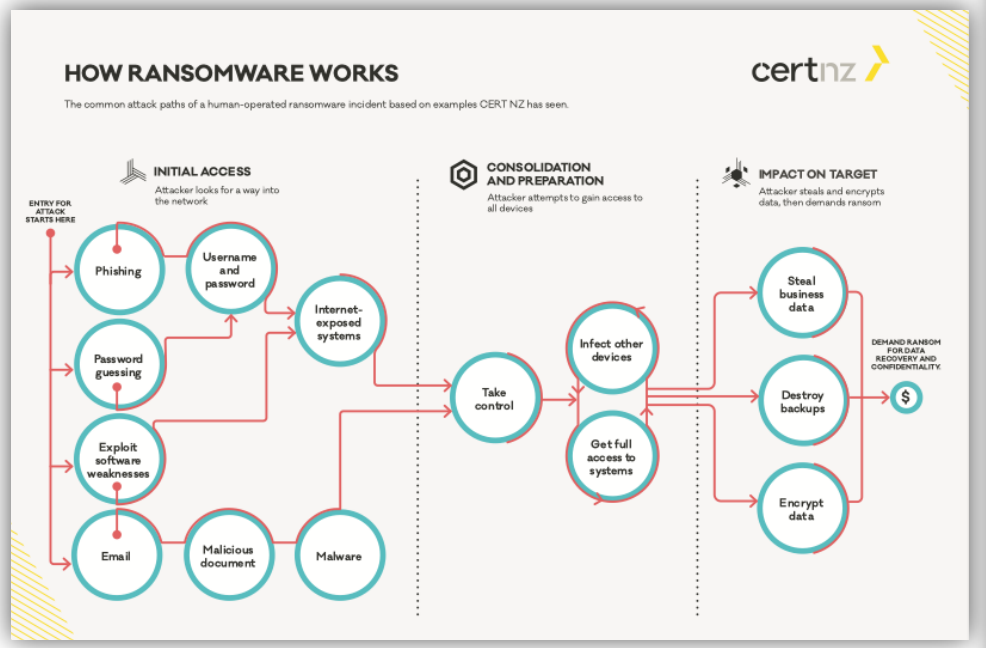
- Estabelecer **relações de confiança**
  - facilitar a comunicação em casos de incidentes
  - dar acesso a informações que ajudem a comunidade local
- **Influenciar** os padrões e certificações sendo construídos para CSIRTs
- Levar a **visão nacional** aos fóruns pertinentes

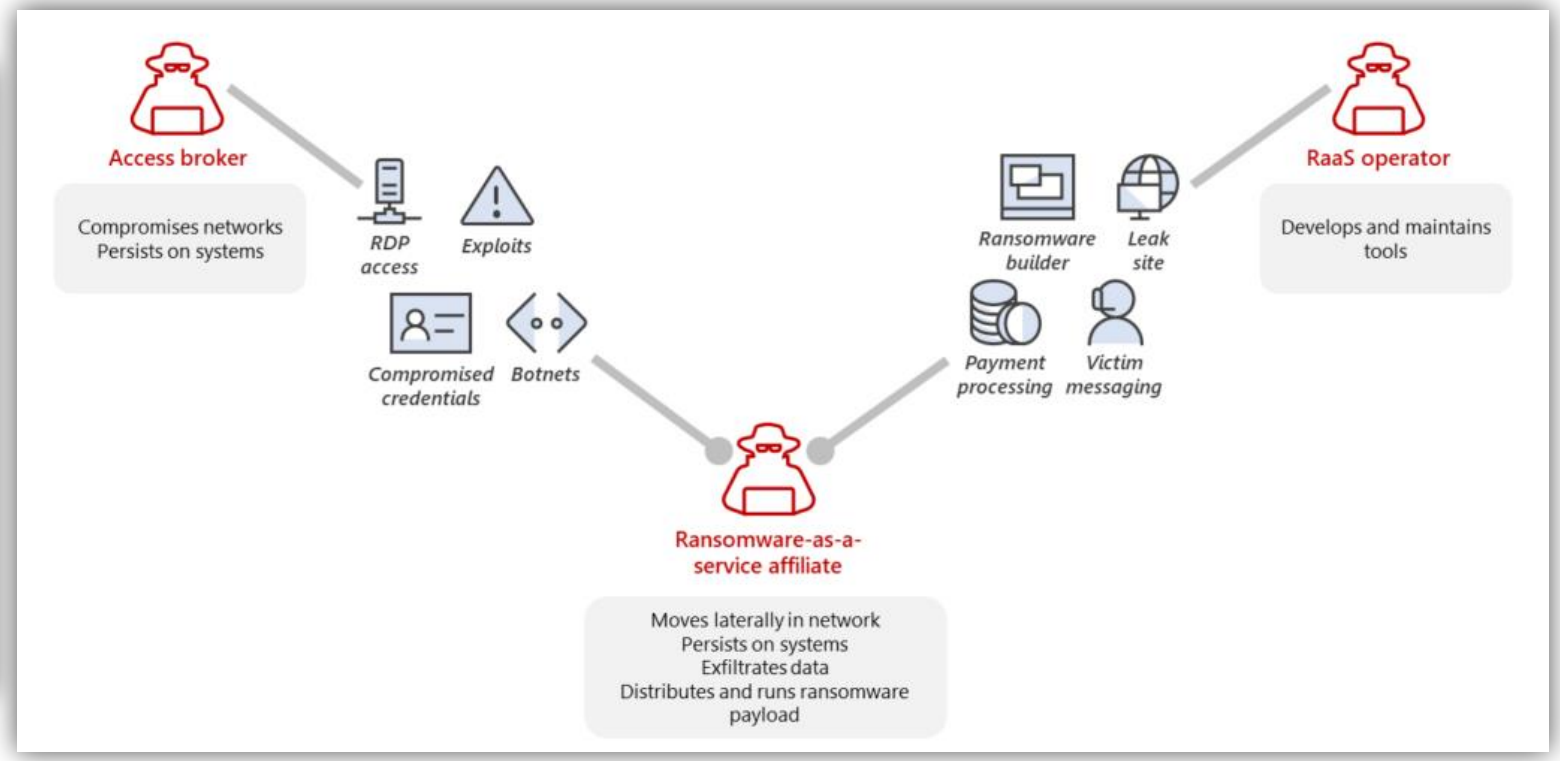
Human Operated Ransomware



Fonte: https://www.cert.govt.nz/assets/ransomware/cert-lifecycle-of-a-ransomware-incident-business-version.pdf

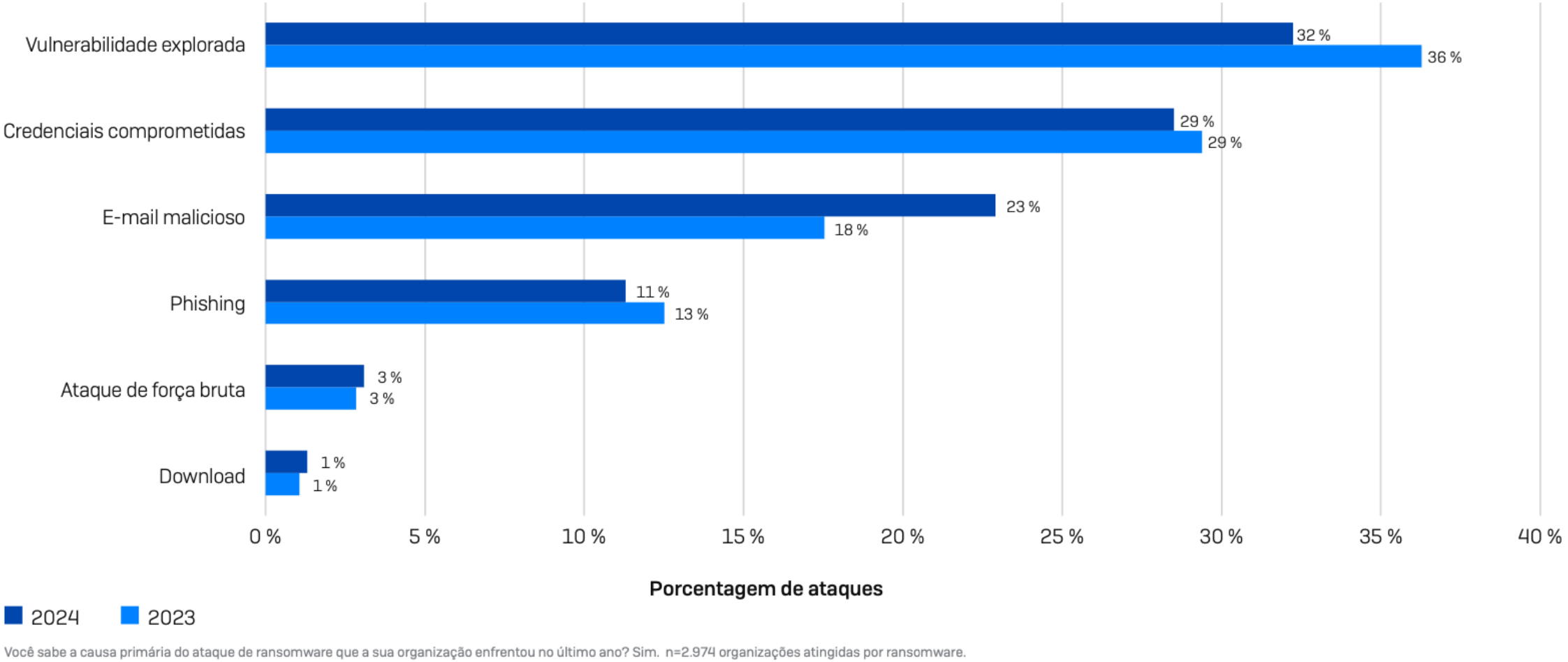
Ransomware as a Service – RaaS





Fonte: https://www.cert.govt.nz/assets/ransomware/cert-lifecycle-of-a-ransomware-incident-business-version.pdf
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/

Causas primárias dos ataques de *ransomware*



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

TLP:CLEAR

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:

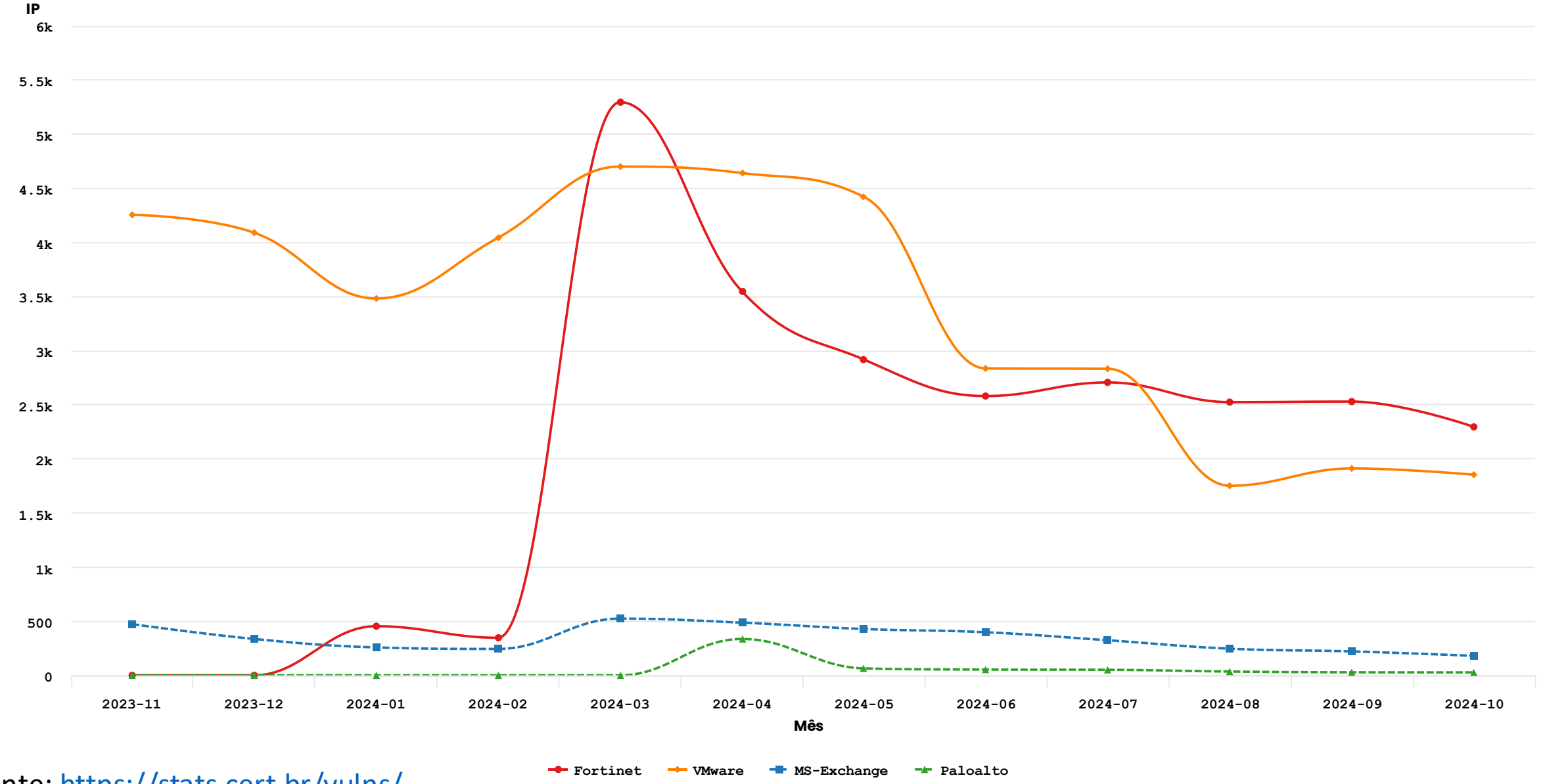
- CVE-2023-48788 (CWE-89)
  - An improper neutralization of special elements used in an SQL command (SQL injection') in Fortinet FortiClientEMS version 7.2.0 through 7.2.2 and FortiClientEMS 7.0.1 through 7.0.10 allows attacker to execute unauthorized code or commands via specially crafted packets.
- 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

CERT.br notificações: endereços IP com servidores vulneráveis

2023-11 -- 2024-10



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

TLP:CLEAR

CYBERSECURITY ADVISORY

#StopRansomware: RansomHub Ransomware

Release Date: August 29, 2024 **Alert Code:** AA24-242A

Privilege Escalation and Lateral Movement

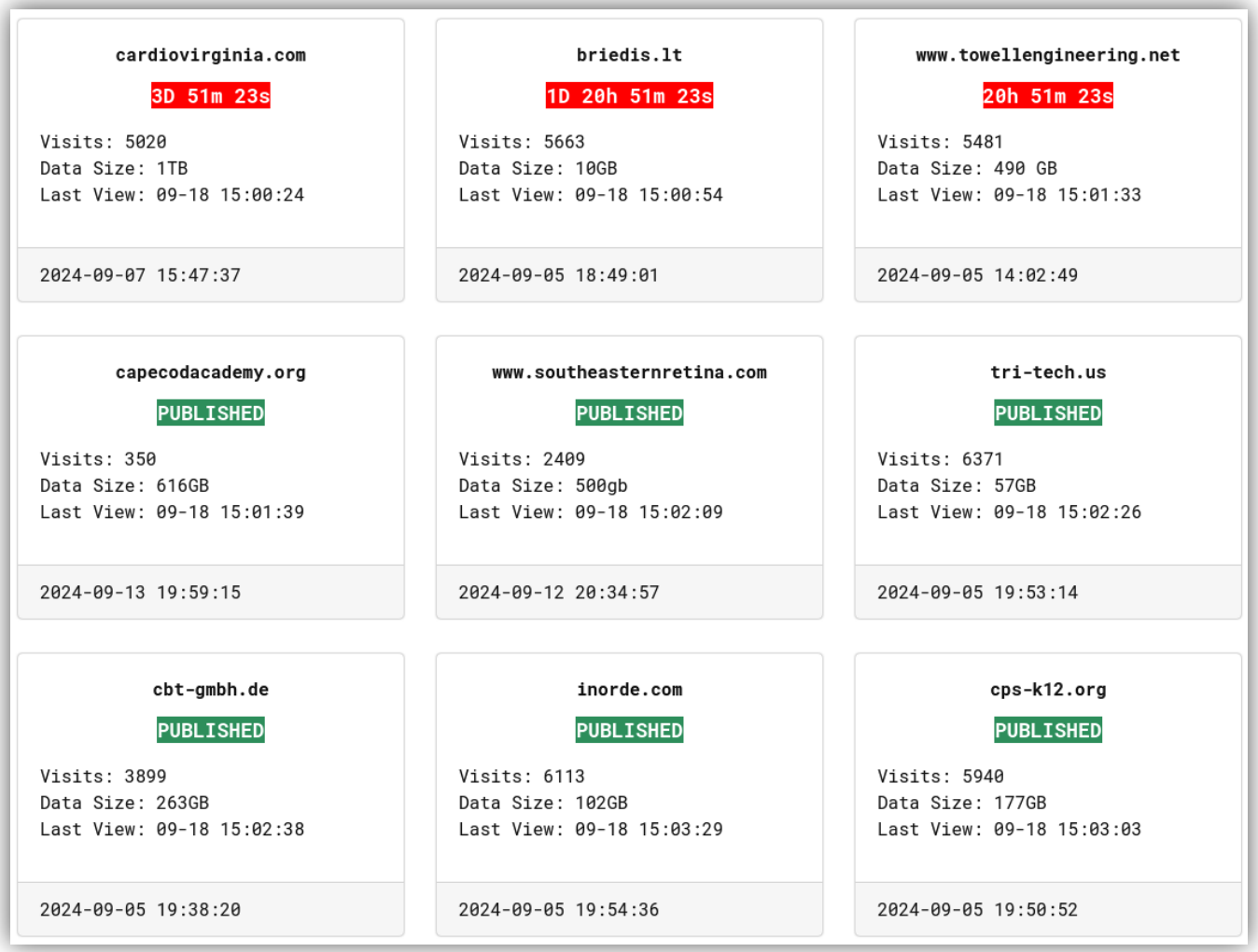
Following initial access, RansomHub affiliates created user accounts for persistence [T1136], reenabled disabled accounts [T1098], and used Mimikatz [S0002] on Windows systems to gather credentials [T1003] and escalate privileges to SYSTEM [T1068]. Affiliates then moved laterally inside the network through methods including Remote Desktop Protocol (RDP) [T1021.001], PsExec [S0029], Anydesk [T1219], Connectwise, N-Able, Cobalt Strike [S0154], Metasploit, or other widely used command-and-control (C2) methods.

Data Exfiltration

Data exfiltration methods depend heavily on the affiliate conducting the network compromise. The ransomware binary does not normally include any mechanism for data exfiltration. Data exfiltration has been observed through the usage of tools such as PuTTY [T1048.002], Amazon AWS S3 buckets/tools [T1537], HTTP POST requests [T1048.003], WinSCP, Rclone, Cobalt Strike, Metasploit, and other methods.

Fonte: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a

RansomHub – Exemplos de Vítimas



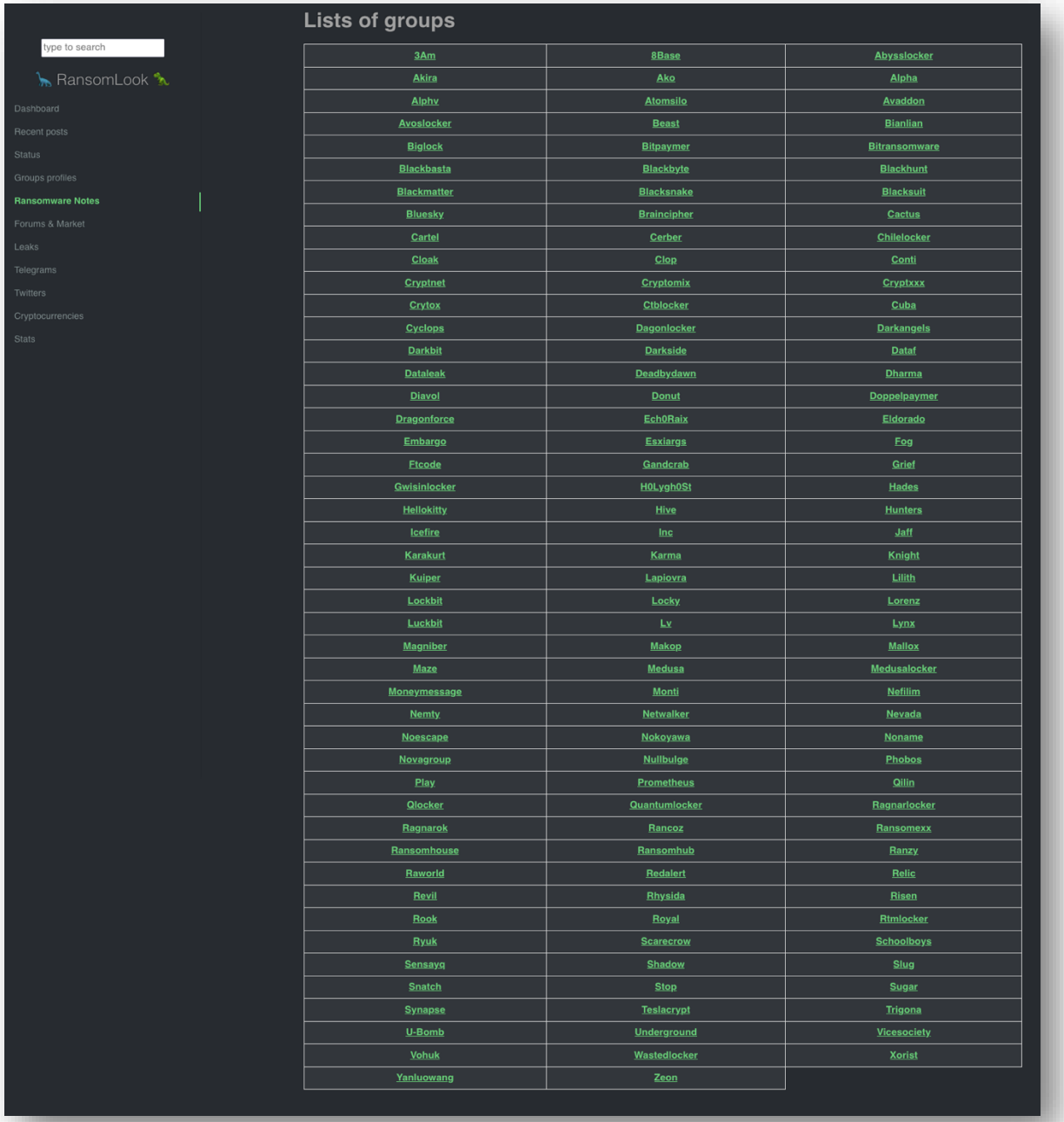
cardiovirginia.com 3D 51m 23s Visits: 5020 Data Size: 1TB Last View: 09-18 15:00:24 2024-09-07 15:47:37	**briedis.lt** 1D 20h 51m 23s Visits: 5663 Data Size: 10GB Last View: 09-18 15:00:54 2024-09-05 18:49:01	**www.towellengineering.net** 20h 51m 23s Visits: 5481 Data Size: 490 GB Last View: 09-18 15:01:33 2024-09-05 14:02:49
capecodacademy.org PUBLISHED Visits: 350 Data Size: 616GB Last View: 09-18 15:01:39 2024-09-13 19:59:15	**www.southeasternretina.com** PUBLISHED Visits: 2409 Data Size: 500gb Last View: 09-18 15:02:09 2024-09-12 20:34:57	**tri-tech.us** PUBLISHED Visits: 6371 Data Size: 57GB Last View: 09-18 15:02:26 2024-09-05 19:53:14
cbt-gmbh.de PUBLISHED Visits: 3899 Data Size: 263GB Last View: 09-18 15:02:38 2024-09-05 19:38:20	**inorde.com** PUBLISHED Visits: 6113 Data Size: 102GB Last View: 09-18 15:03:29 2024-09-05 19:54:36	**cps-k12.org** PUBLISHED Visits: 5940 Data Size: 177GB Last View: 09-18 15:03:03 2024-09-05 19:50:52

paciente.sempremedico.com.br
appweb.usinacoruripe.com.br
www.vbrlogistica.com.br
imobesidade.com.br
oficina.oficinadasfinancas.com.br
metalfrio.com.br
ceopag.com.br / ceofood.com.br
www.sicoob.com.br
equinocioplay.com.br
bitzsoftwares.com.br
www.sicoob.com.br
www.ham.org.br
www.ykp.com.br
www.shootinghouse.com.br
www.spmundi.com.br
www.portosaofrancisco.com.br
www.confins.com.br
www.lapastina.com
eucatex.com.br
...

Fonte: https://www.ransomlook.io/group/ransomhub

TLP:CLEAR

Existem muitos outros grupos de RaaS



Fonte: https://www.ransomlook.io/notes

Melhor Prevenir que Remediar

cert.br nic.br cgi.br

Recomendações do CERT.br

	Medida
Controle de Acesso e gestão de identidade	• **Implementar autenticação com múltiplos fatores** • Adequar permissões ao mínimo necessário (Privilégio Mínimo)
Reduzir superfície de ataque	• **Manter equipamentos e sistemas atualizados** • Segmentar a rede
Backup	• **Fazer e testar *backups* periodicamente**
Conhecer e monitorar o ambiente	• **Conhecer o que é padrão no ambiente e monitorar:** - *logins* em contas de acesso remoto - *logins* em contas com privilégios de administração - criação de contas de usuário - tráfego de saída - grandes quantidade de dados ou conexões muito longas
Pessoas – Treinamento e conscientização	• **Treinar colaboradores para que saibam reconhecer e reportem:** - *phishing* e outros potenciais ataques de engenharia social - infecção por *malware*
Processos e procedimentos	• **Ter um plano de resposta a incidentes**

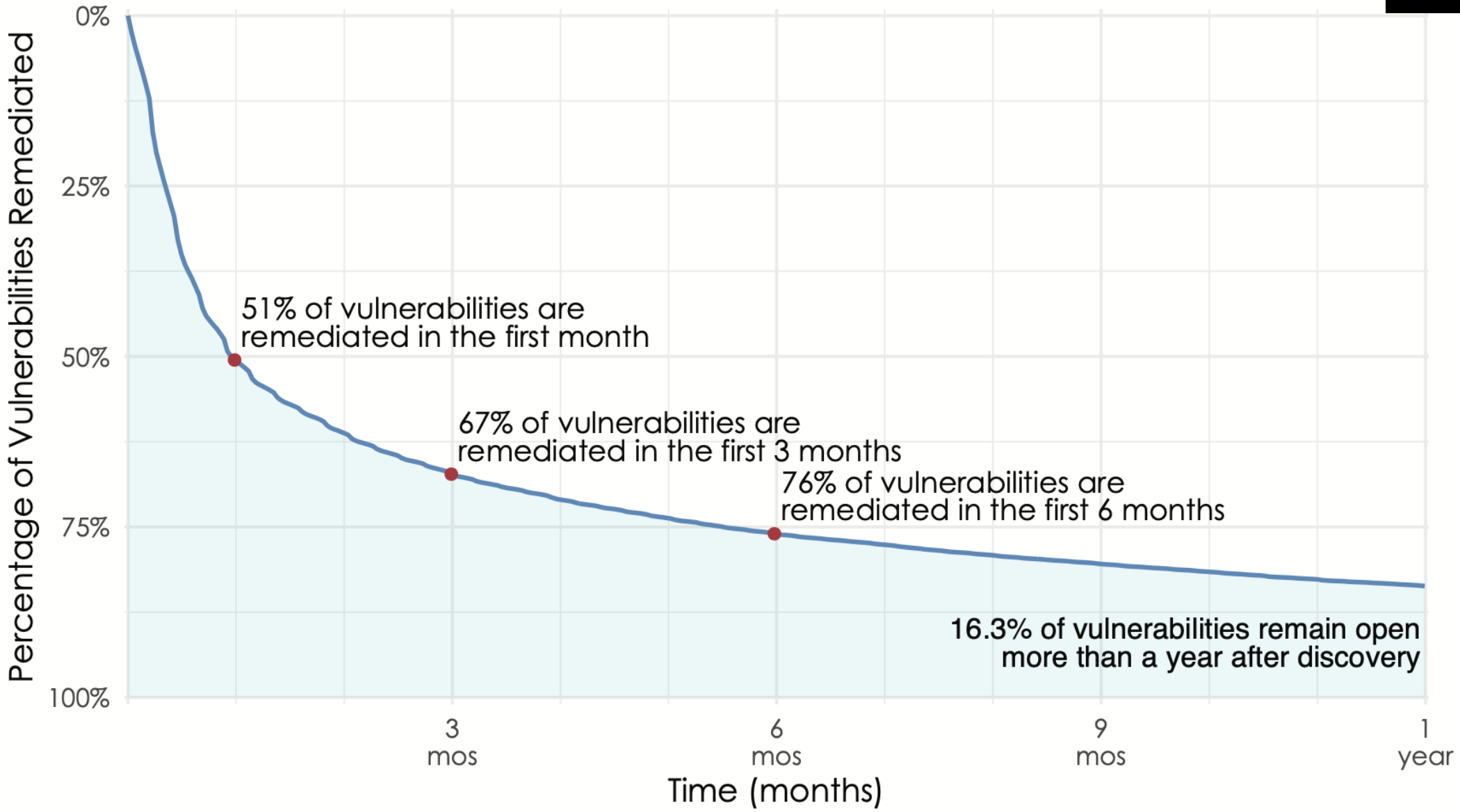
Recomendações do CISA

ACTIONS TO TAKE TODAY TO MITIGATE CYBER THREATS FROM RANSOMWARE:

1. Install updates for operating systems, software, and firmware as soon as they are released.
2. Require phishing-resistant MFA (i.e., non-SMS text based) for as many services as possible.
3. Train users to recognize and report phishing attempts.

Fonte: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a

TLP:CLEAR



Fonte: https://www.cyentia.com/patching-fast-and-slow/ | https://www.cyentia.com/why-your-mttr-is-probably-bogus/

Algumas Estatísticas Globais

- **Mais da metade** das organizações só conseguem **aplicar *patches* em 15.5%** dos CVEs/mês
  - ¼ corrige menos de 6.6% dos CVEs
- 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

Por que?

- Falta de priorização e compreensão de riscos
  - “Precisa atualizar? Está funcionando...”
  - “Mas está na rede interna, está seguro...”
  - “MFA é inconveniente e custa caro”
- Falta de pessoal capacitado
- Sistemas legados
  - Impedem atualização de SO e aplicações
- Falta de verba e planejamento
  - Licenças que expiram e não permitem *update* para correção de vulnerabilidades

Obrigado

@ Notificações para: cert@cert.br @certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br