

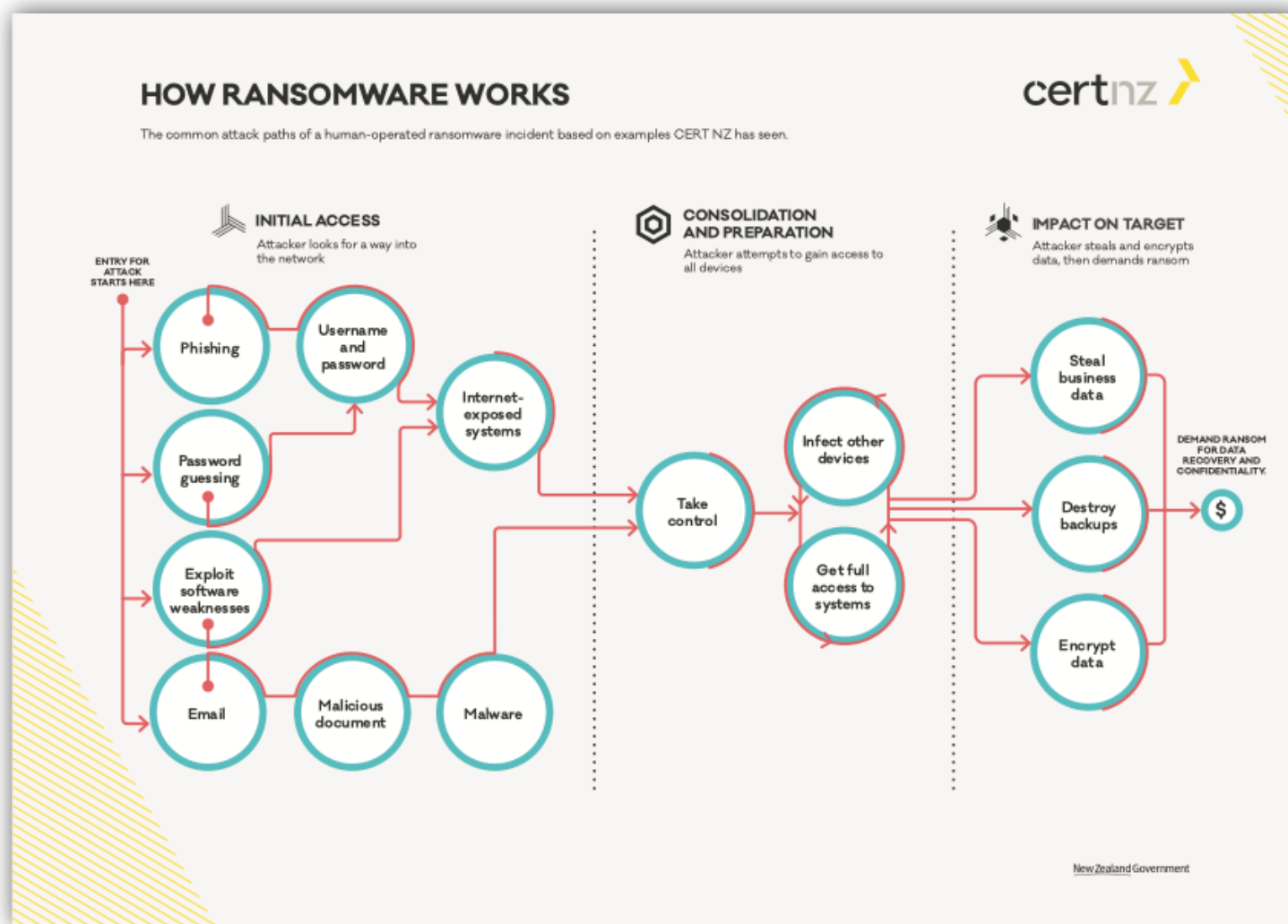
Ransomware, muito além de uma infecção por *malware*

Lucimara Desiderá, M.Sc. CISSP
Analista de Segurança, CERT.br/NIC.br

Ransomware Task Force Brazil
Brasília, DF – 23 e 24 de setembro de 2024

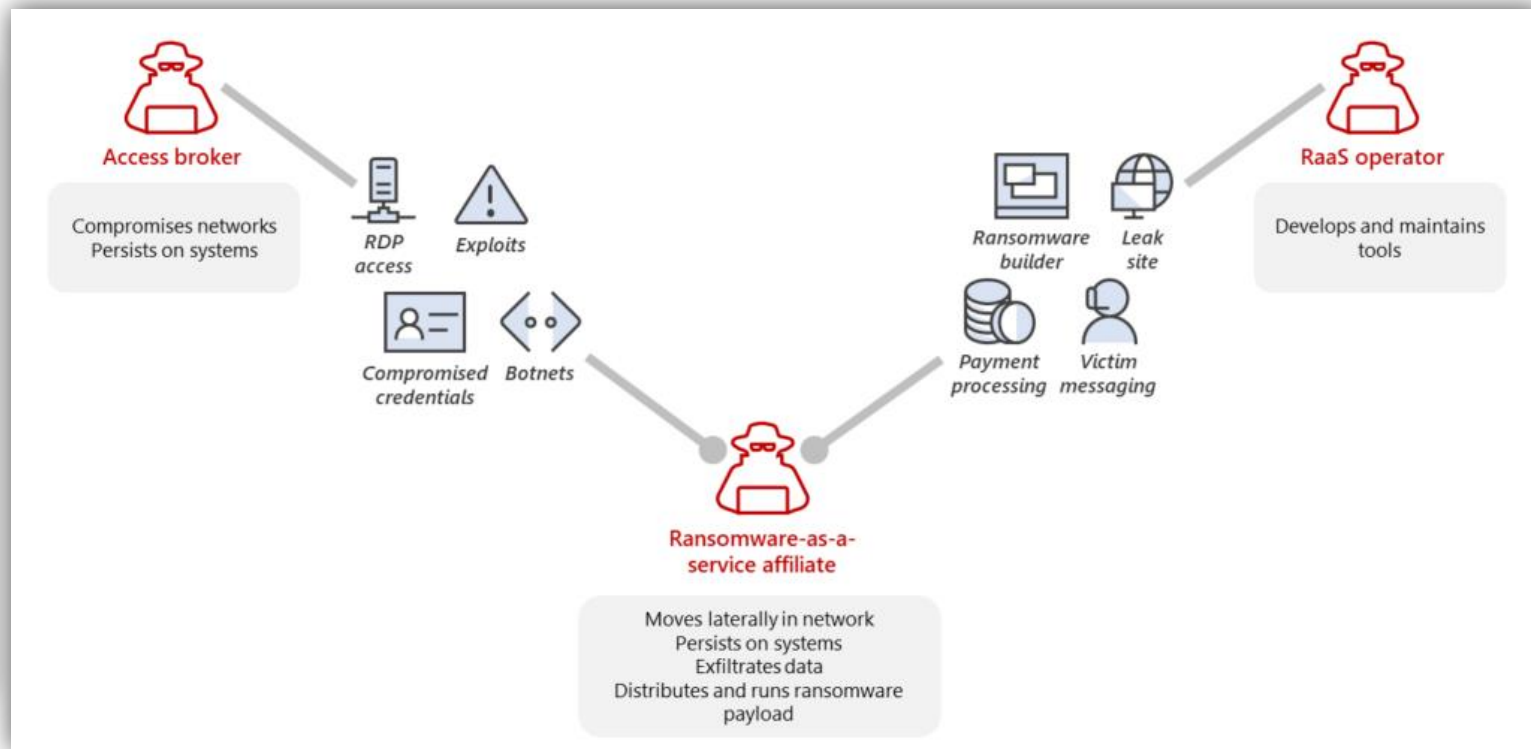
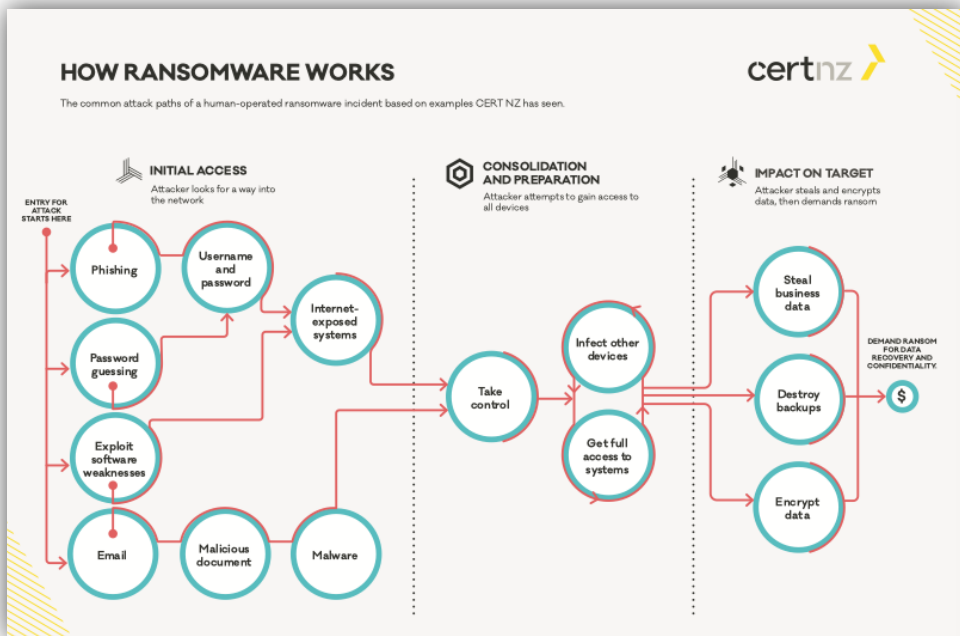
cert.br nic.br egi.br

Human Operated Ransomware



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

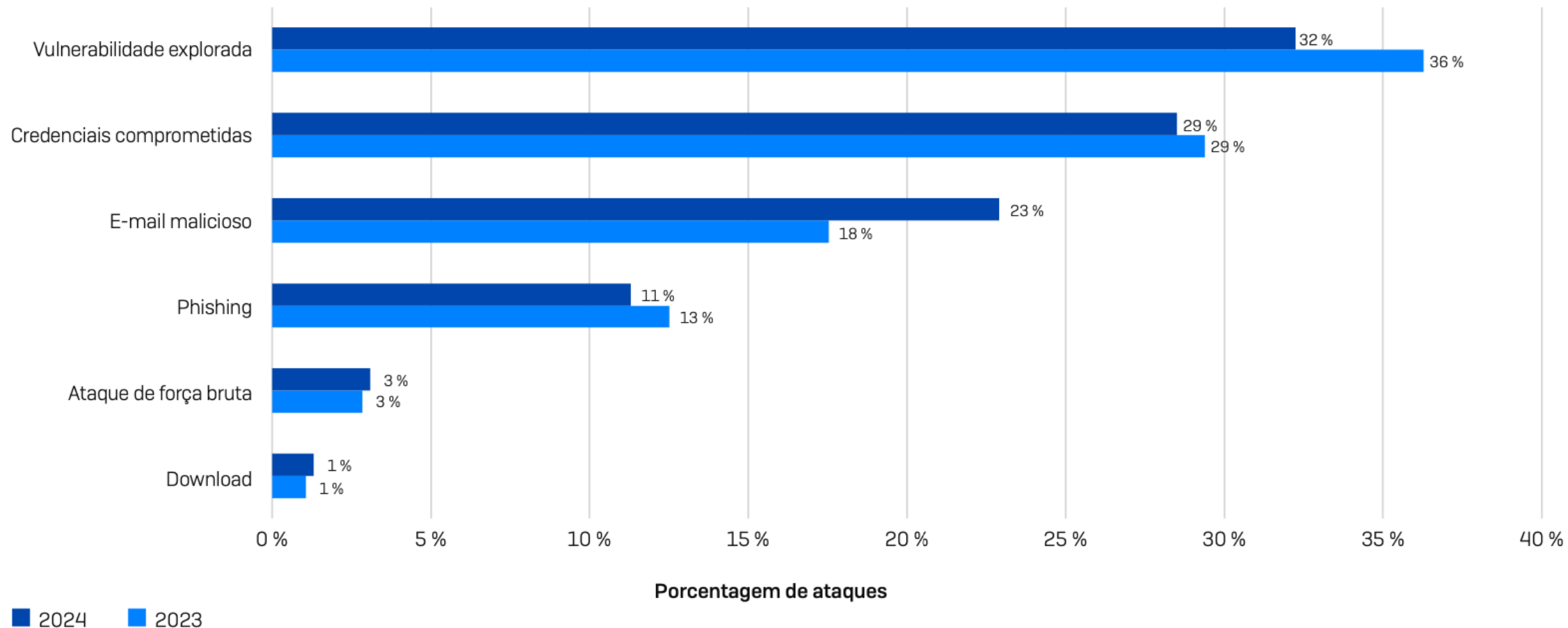
Ransomware as a Service – RaaS



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*



Você sabe a causa primária do ataque de ransomware que a sua organização enfrentou no último ano? Sim. n=2.974 organizações atingidas por ransomware.

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

#StopRansomware: RansomHub Ransomware

Release Date: August 29, 2024

Alert Code: AA24-242A

Initial Access

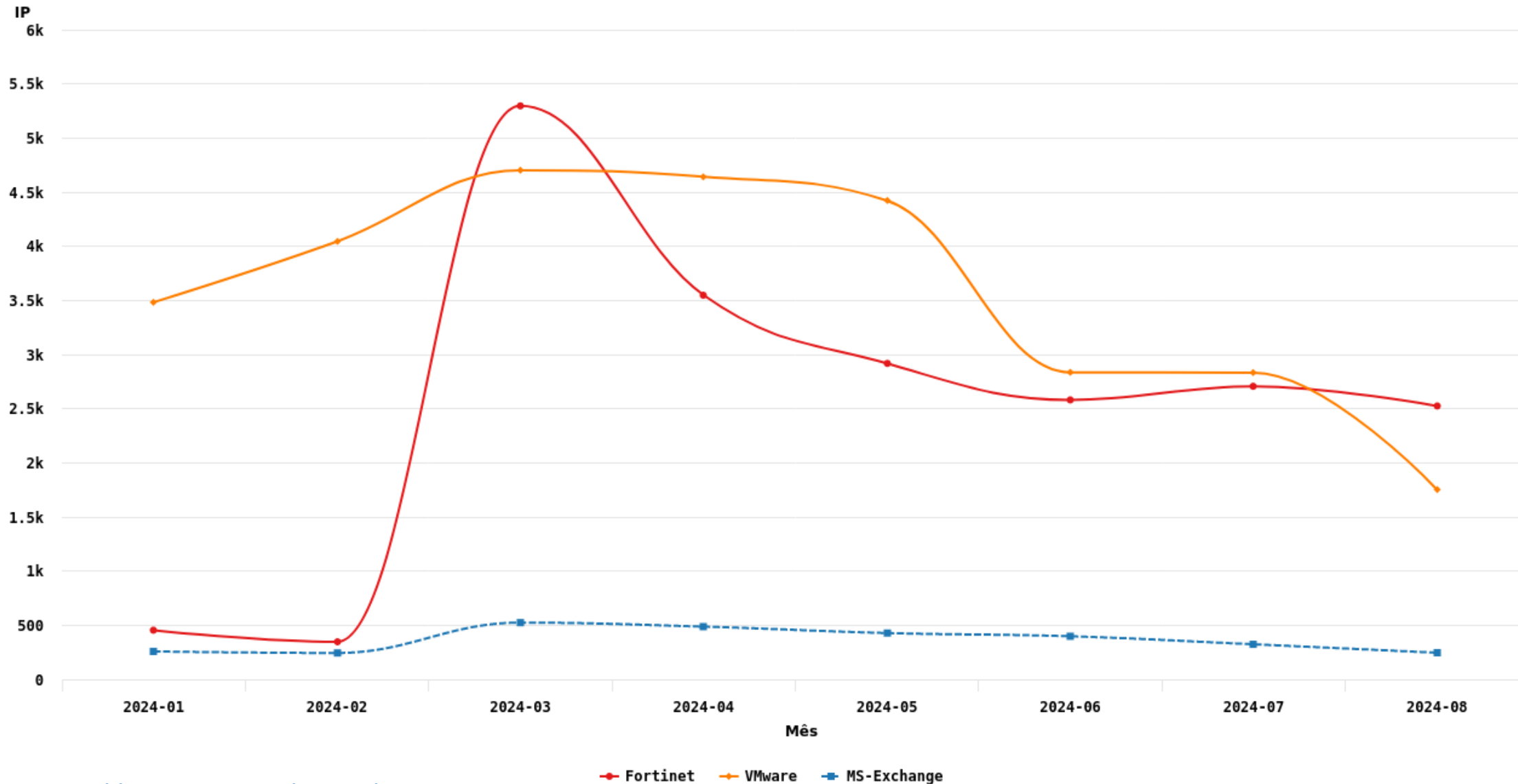
RansomHub affiliates typically compromise internet facing systems and user endpoints by using methods such as phishing emails [T1566^{cf}], exploitation of known vulnerabilities [T1190^{cf}], and password spraying [T1110.003^{cf}]. Password spraying targets accounts compromised through data breaches. Proof-of-concept exploits are obtained from sources such as ExploitDB and GitHub [T1588.005^{cf}]. Exploits based on the following CVEs have been observed:

- CVE-2023-48788^{cf} (CWE-89^{cf})
 - 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^{cf}
 - 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^{cf}].

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

CERT.br notificações: endereços IP com servidores vulneráveis

2024-01 -- 2024-08



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

Fonte: CERT.br — <https://stats.cert.br/> — by Highcharts.com

#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^{cf}], reenabled disabled accounts [T1098^{cf}], and used Mimikatz [S0002^{cf}] on Windows systems to gather credentials [T1003^{cf}] and escalate privileges to SYSTEM [T1068^{cf}]. Affiliates then moved laterally inside the network through methods including Remote Desktop Protocol (RDP) [T1021.001^{cf}], PsExec [S0029^{cf}], Anydesk [T1219^{cf}], Connectwise, N-Able, Cobalt Strike [S0154^{cf}], 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^{cf}], Amazon AWS S3 buckets/tools [T1537^{cf}], HTTP POST requests [T1048.003^{cf}], WinSCP, Rclone, Cobalt Strike, Metasploit, and other methods.

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

RansomHub – Exemplos de Vítimas

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

- 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>

Existem muitos outros grupos de RaaS

type to search

RansomLook

- Dashboard
- Recent posts
- Status
- Groups profiles
- Ransomware Notes**
- Forums & Market
- Leaks
- Telegrams
- Twitters
- Cryptocurrencies
- Stats

Lists of groups

3Am	8Base	Abysslocker
Akira	Ako	Alpha
Alphv	Atomsilo	Avaddon
Avoslocker	Beast	Bianlian
Biglock	Bitpaymer	Bitransomware
Blackbasta	Blackbyte	Blackhunt
Blackmatter	Blacksnake	Blacksuit
Bluesky	Braincipher	Cactus
Cartel	Cerber	Chillelocker
Cloak	Clop	Conti
Cryptinet	Cryptomix	Cryptxxx
Crylox	Clobberer	Cuba
Cyclops	Dagonlocker	Darkangels
Darkbit	Darkside	Dataf
Dataleak	Deadbydawn	Dharma
Diavol	Donut	Doppelpaymer
Dragonforce	Ech0Raix	Eldorado
Embargo	Esxlargs	Fog
Etcode	Gandcrab	Grief
Gwisinlocker	H0Llygh0St	Hades
Hellokitty	Hive	Hunters
Icefire	Inc	Jaff
Karakurt	Karma	Knight
Kuiper	Laplovrá	Lilith
Lockbit	Locky	Lorenz
Luckbit	Lv	Lynx
Magniber	Makop	Mallox
Maze	Medusa	Medusalocker
Moneymessage	Monti	Nefilim
Nemty	Netwalker	Nevada
Noescape	Nokoyawa	Noname
Novagroup	Nullbulge	Phobos
Play	Prometheus	Qilin
Qlocker	Quantumlocker	Ragnarlocker
Ragnarok	Rancoz	Ransomexx
Ransomhouse	Ransomhub	Ranzy
Raworld	Redalert	Relic
Revil	Rhysida	Risen
Rook	Royal	Rtmlocker
Ryuk	Scarecrow	Schoolboys
Sensayq	Shadow	Slug
Snatch	Stop	Sugar
Synapse	Teslacrypt	Trigona
U-Bomb	Underground	Vicesociety
Vohuk	Wastedlocker	Xorist
Yanluowang	Zeon	

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

Melhor Prevenir que Remediar

cert.br nic.br egi.br

Recomendações

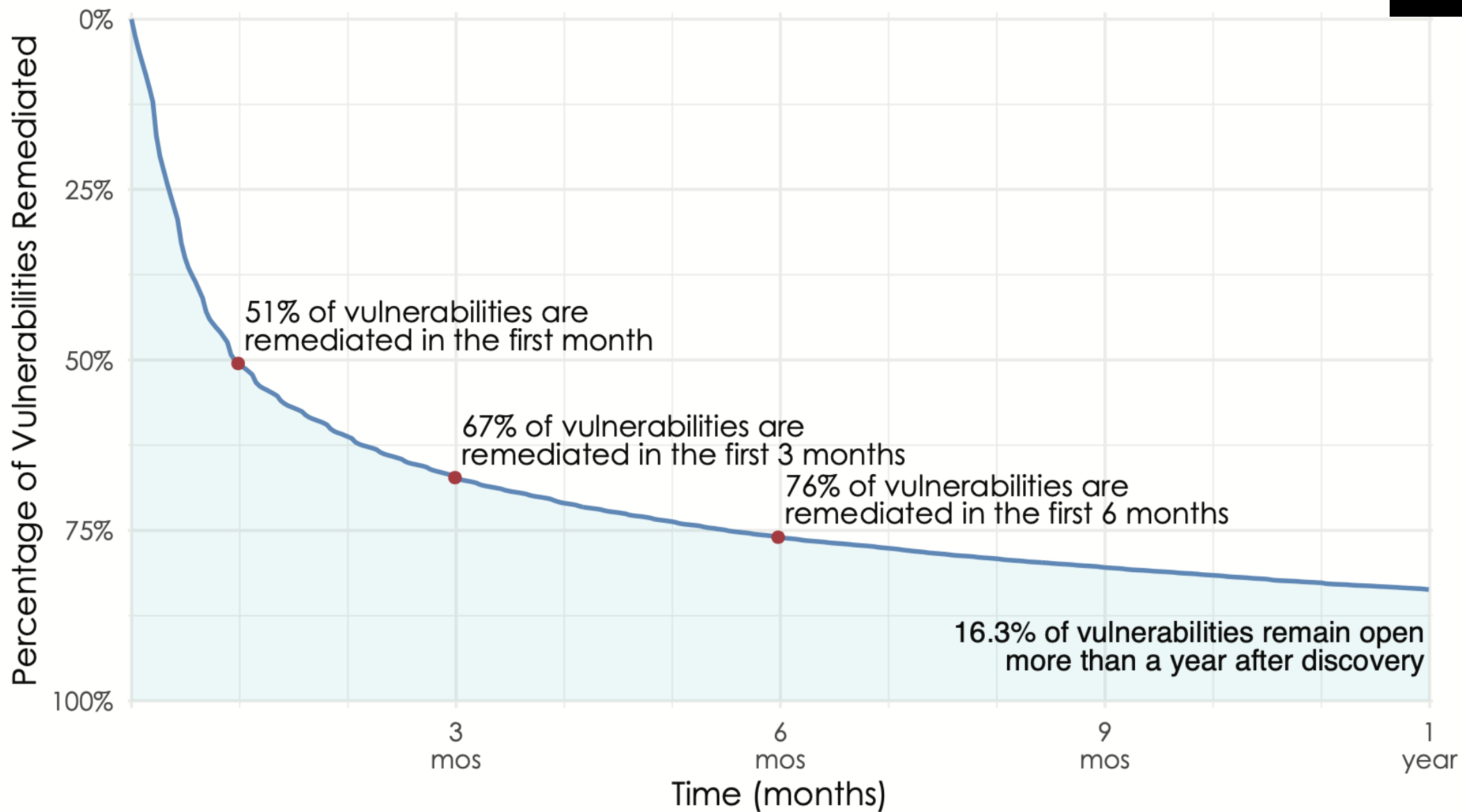
	Medida
Controle de Acesso e gestão de identidade	<ul style="list-style-type: none"> • Implementar autenticação com múltiplos fatores • Adequar permissões ao mínimo necessário (Privilégio Mínimo)
Reduzir superfície de ataque	<ul style="list-style-type: none"> • Manter equipamentos e sistemas atualizados • Segmentar a rede
<i>Backup</i>	<ul style="list-style-type: none"> • Fazer e testar <i>backups</i> periodicamente
Conhecer e monitorar o ambiente	<ul style="list-style-type: none"> • Conhecer o que é padrão no ambiente e monitorar: <ul style="list-style-type: none"> - <i>logins</i> em contas de acesso remoto - <i>logins</i> 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	<ul style="list-style-type: none"> • Treinar colaboradores para que saibam reconhecer e reportem: <ul style="list-style-type: none"> - <i>phishing</i> e outros potenciais ataques de engenharia social - infecção por <i>malware</i> - ataque <i>ransomware</i>
Processos e procedimentos	<ul style="list-style-type: none"> • Ter um plano de resposta a incidentes

Recomendações



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.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

Obrigada

@ lucimara@cert.br

@ Notificações para: cert@cert.br



Link para os slides
<https://cert.br/docs/palestras>

nic.br **cgi.br**

www.nic.br | www.cgi.br