

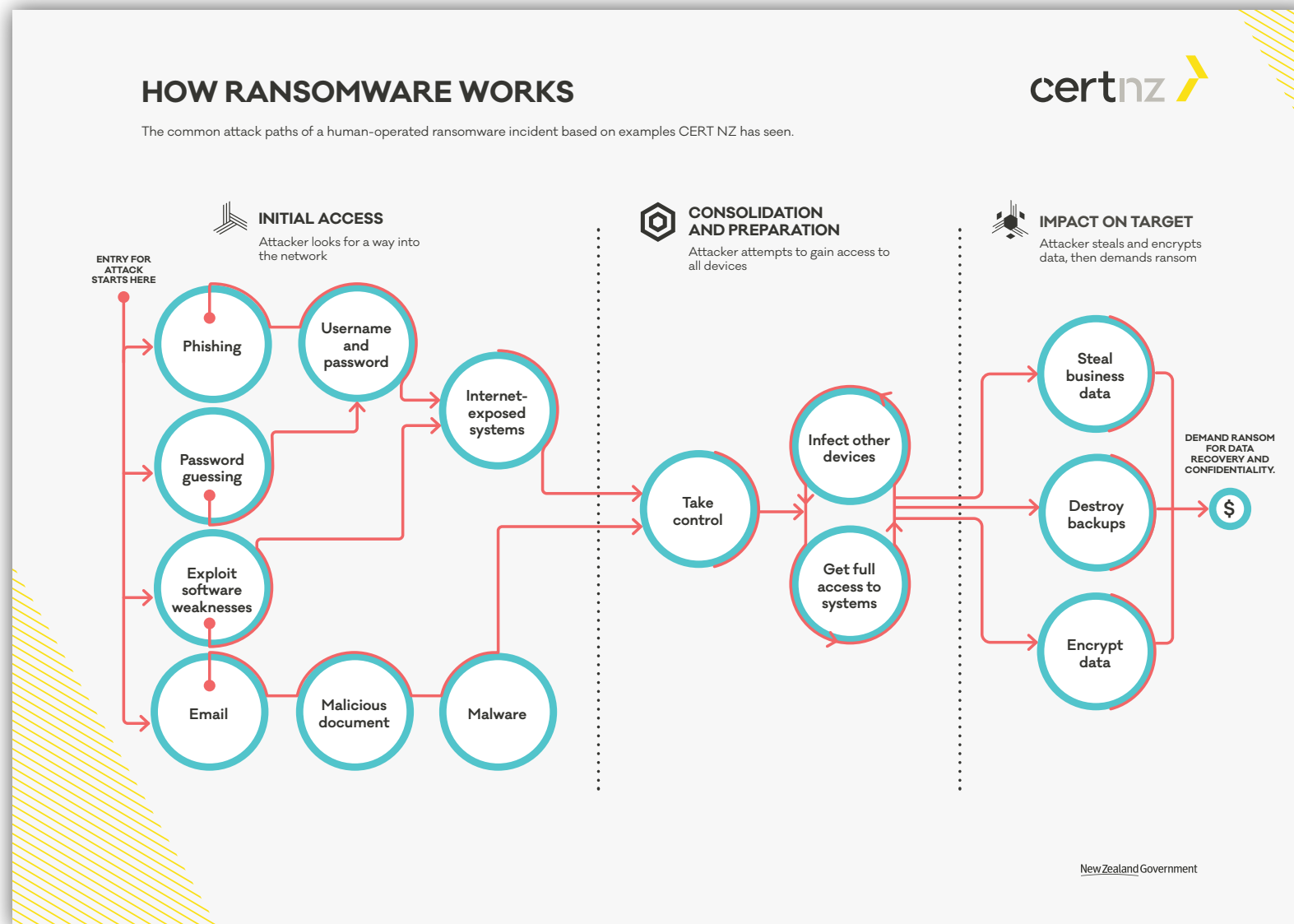
Ransomware, muito além de uma infecção por *malware*

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

Fórum Temático 1: Defesa e Segurança Cibernética
Brasília, DF – 23 de junho de 2025

cert.br nic.br cgi.br

Human Operated Ransomware



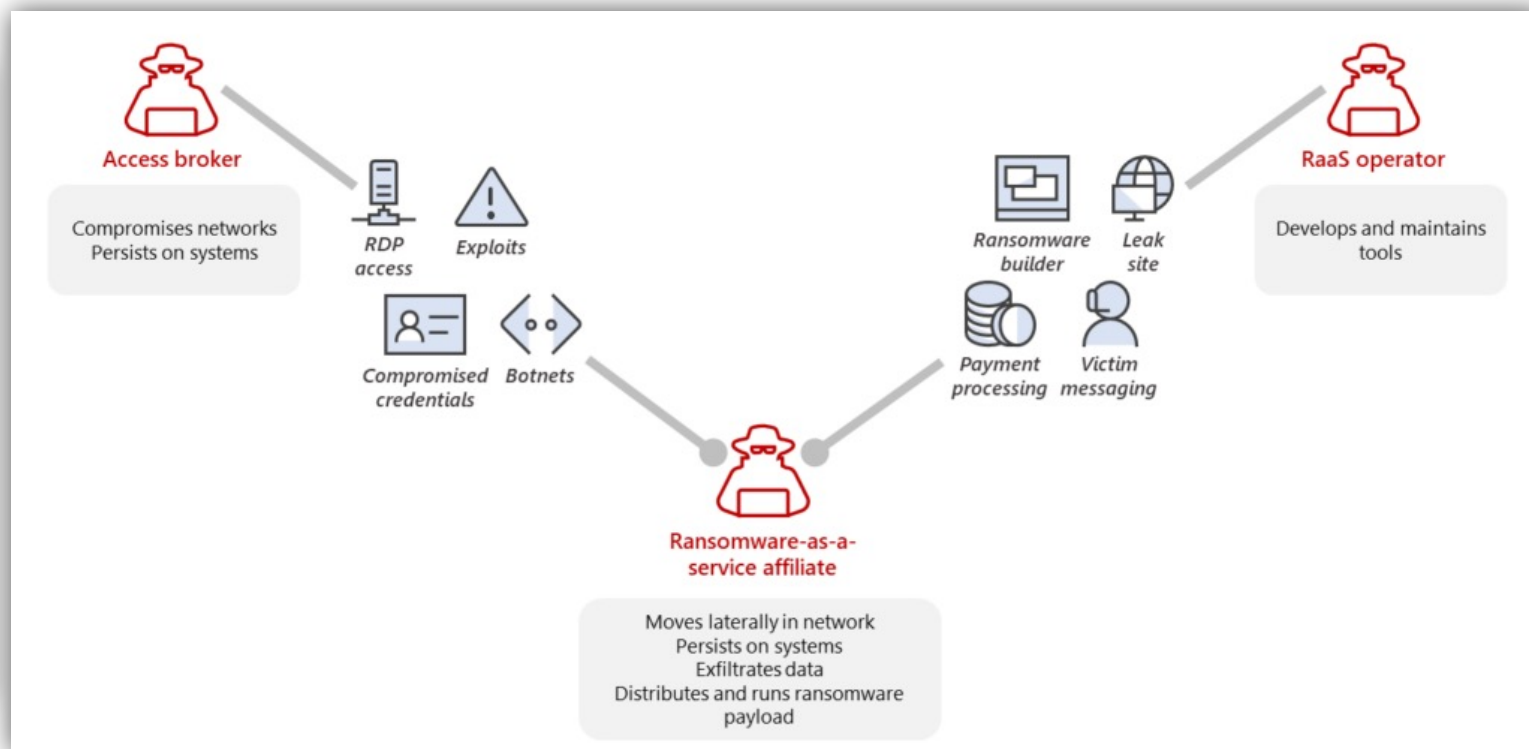
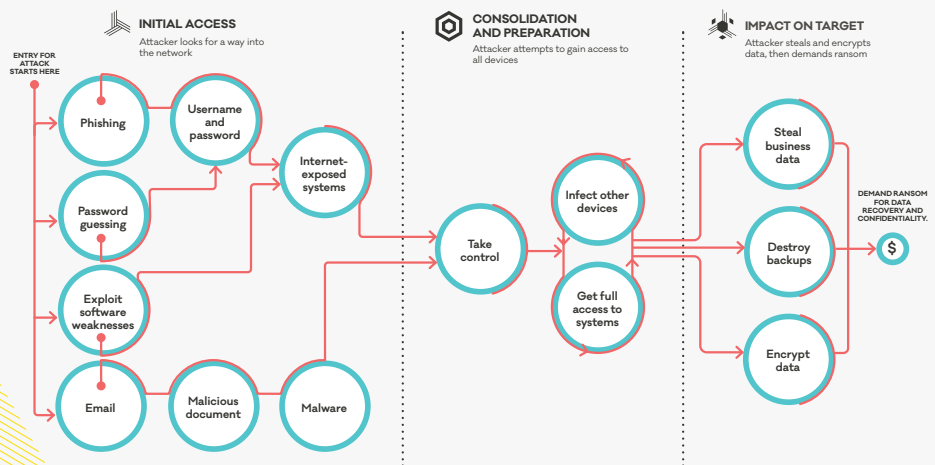
Fonte: <https://www.cert.govt.nz/assets/ransomware/cert-lifecycle-of-a-ransomware-incident-business-version.pdf>

Ransomware as a Service – RaaS

HOW RANSOMWARE WORKS

The common attack paths of a human-operated ransomware incident based on examples CERT NZ has seen.

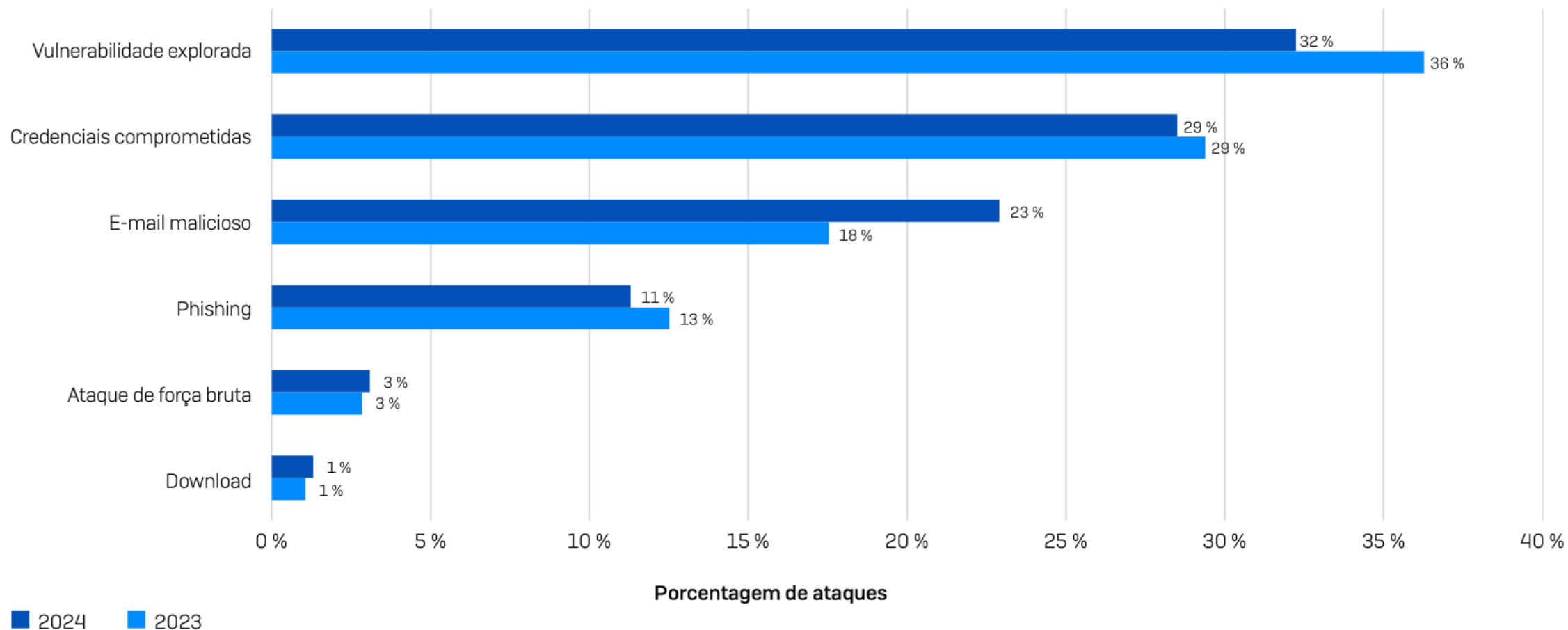
certnz



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/>

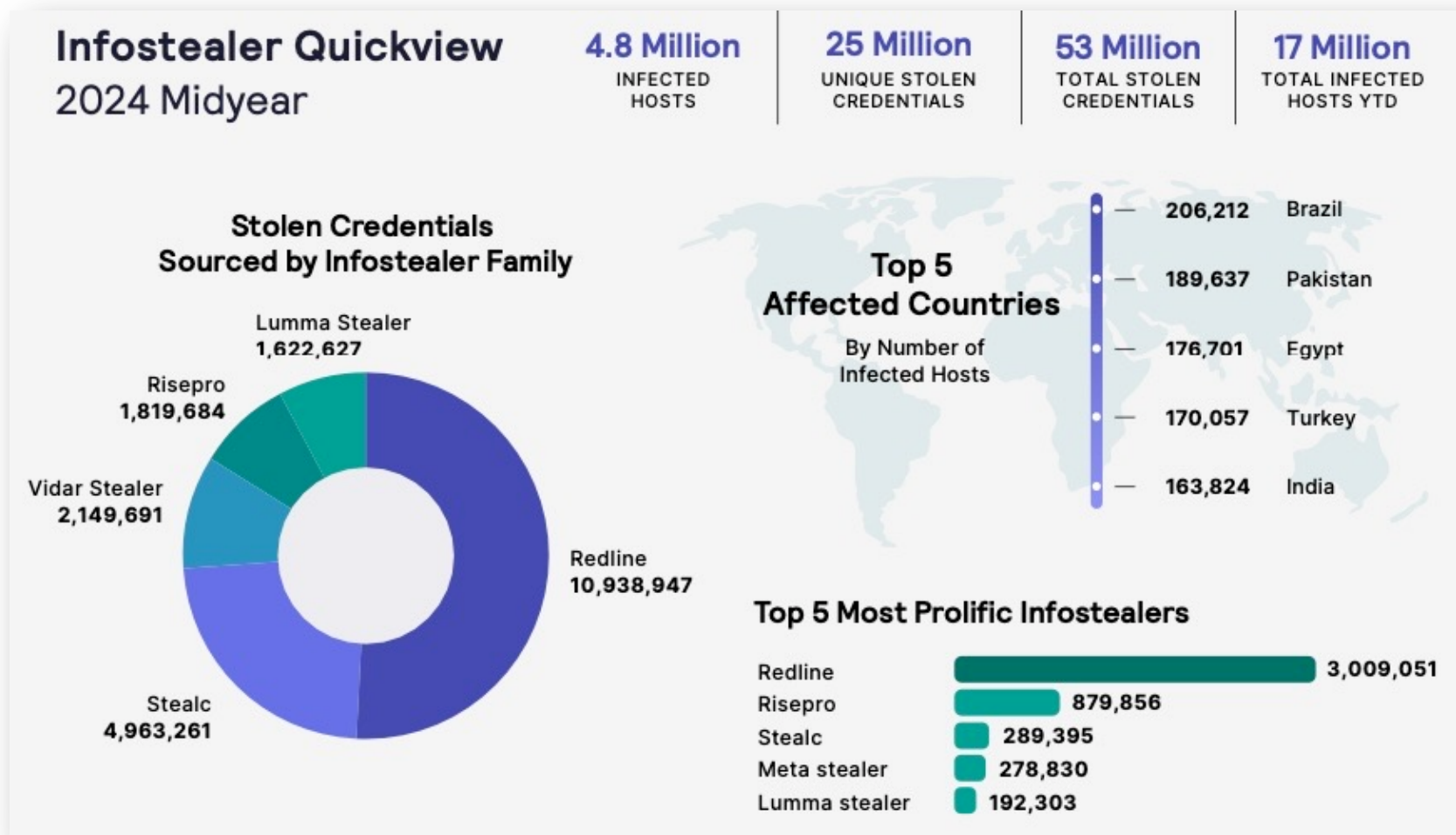
Causas primárias dos ataques de *ransomware*



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>

Causas primárias dos ataques de *ransomware*



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

#StopRansomware: RansomHub Ransomware

Release Date: August 29, 2024

Alert Code: AA24-242A

Initial Access

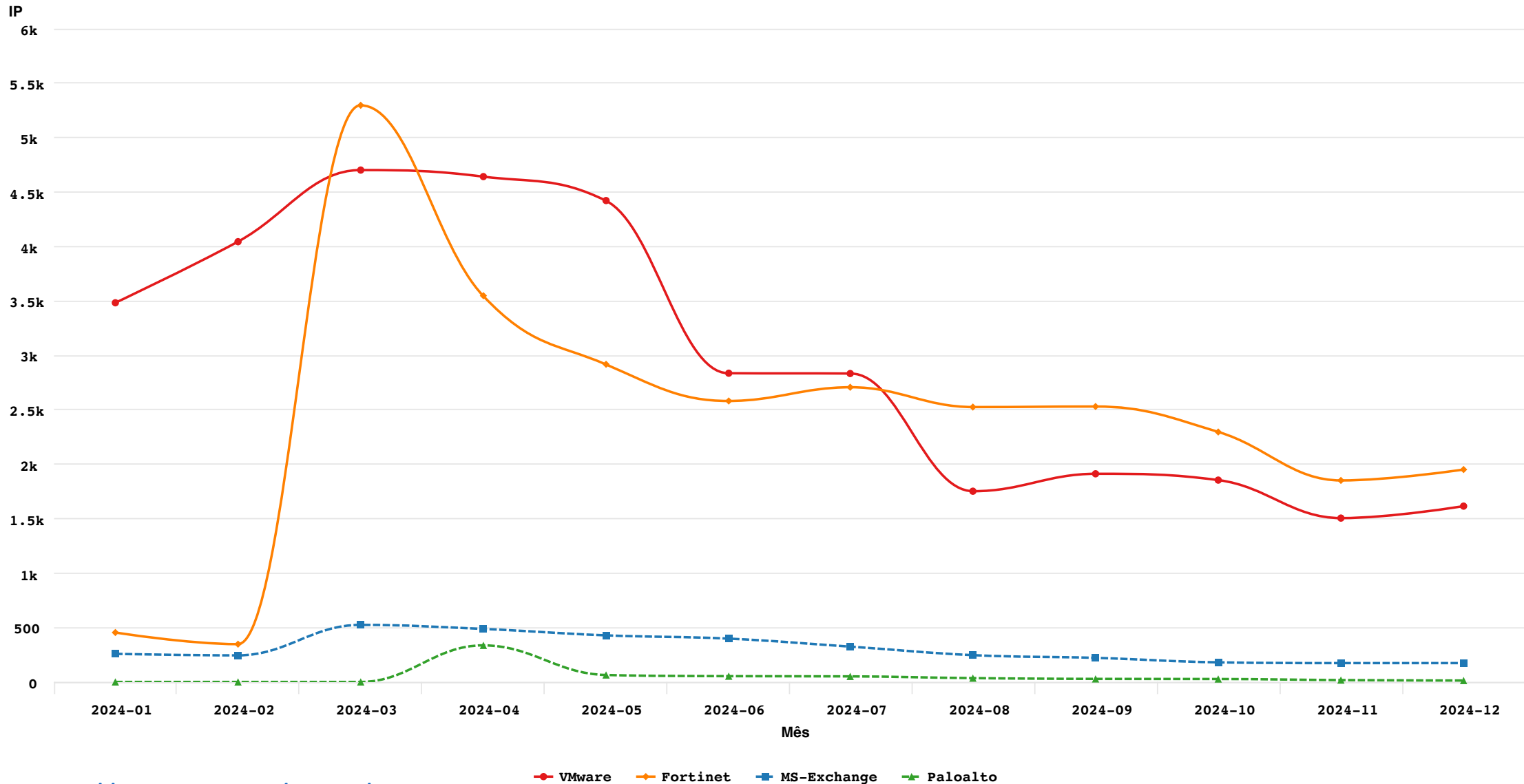
RansomHub affiliates typically compromise internet facing systems and user endpoints by using methods such as phishing emails [T1566^{cf}], exploitation of known vulnerabilities [T1190^{cf}], and password spraying [T1110.003^{cf}]. Password spraying targets accounts compromised through data breaches. 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 -- 2024-12



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](#)], 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

www.aswgr.com 2h 14m 42s Visits: 4373 Data Size: 350 GB Last View: 02-11 08:41:37 2025-02-03 16:46:34	smithmidland.com 2h 14m 42s Visits: 4789 Data Size: 216 GB Last View: 02-11 08:41:44 2025-02-03 12:41:14	www.manpower.com 3D 2h 14m 42s Visits: 9309 Data Size: 500GB Last View: 02-11 08:41:51 2025-01-22 17:56:56
alojaimi.com PUBLISHED Visits: 4533 Data Size: 10Gb Last View: 02-11 08:43:04 2025-01-20 09:33:59	www.origene.com PUBLISHED Visits: 4852 Data Size: 500gb Last View: 02-11 08:42:06 2025-02-03 13:08:55	www.wongfleming.com PUBLISHED Visits: 4656 Data Size: 500gb Last View: 02-11 08:42:09 2025-02-03 12:33:23
midwaymetals.com.vn PUBLISHED Visits: 7728 Data Size: 46GB Last View: 02-11 08:42:12 2025-01-29 19:27:44	www.healthcarewithinreach.org PUBLISHED Visits: 7510 Data Size: 400gb Last View: 02-11 08:42:15 2025-01-27 16:43:22	www.pcm.com.mx PUBLISHED Visits: 12397 Data Size: 3GB Last View: 02-11 08:42:17 2025-01-18 03:09:09

imobesidade.com.br
 oficina.oficinasdasfinancas.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

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

RansomLook				Lists of groups		
Dashboard				3Am	8Base	Abyssalocker
Recent posts				Akira	Ako	Alpha
Status				Alphv	Arcus	Atomsilo
Groups profiles				Avaddon	Avoslocker	Beast
Ransomware Notes				Blamian	Biglock	Bitpaymer
Forums & Market				Bitransomware	Blackbaata	Blackbyte
Leaks				Blackhunt	Blackmatter	Blacksnake
Telegram				Blacksuit	Bluesky	Braincipher
Twitter				Cactus	Cartel	Cerber
Cryptocurrencies				Chilelocker	Cloak	Clop
Stats				Conti	Crypnet	Cryptomix
				Crypboxx	Crytox	Citblocker
				Cuba	Cyclops	Dagonlocker
				Darkangels	Darkbit	Darkside
				Dataf	Dataleak	Deadbydawn
				DennisTheHitman	Dharma	Diavol
				Donut	Doppelpaymer	Dragonforce
				Ech0Raix	Eldorado	Embargo
				Esxiargs	Fog	Ftcode
				Gandcrab	Grief	Gwainlocker
				HOLyph0St	Hades	Helicat
				Helldown	Hellockitty	Hive
				Hunters	Icefire	Inc
				Interlock	Jaff	Karakurt
				Karma	Knight	Krypt
				Kulper	Lambda	Lapiovr
				Lilith	Lockbit	Locky
				Lorenz	Luckbit	Lv
				Lynx	Magniber	Makop
				Mallox	Maze	Medusa
				Medusalocker	Moneymessage	Monti
				Morpheus	Nefilim	Nemty
				Netwalker	Nevada	Nitrogen
				Noescape	Nokoyawa	Noname
				Novagroup	Nullbulge	Phobos
				Play	Prolock	Prometheus
				Qilin	Qlocker	Quantumlocker
				Ragnarlocker	Ragnarok	Rancoz
				Ransomexx	Ransomhouse	Ransomhub
				Ranzy	Raworld	Redalert
				Relic	Revil	Rhysida
				Risen	Rook	Royal
				Rtmlocker	Ryuk	Satanod
				Scarecrow	Schoolboys	Sensaya
				Shadow	Slug	Snatch
				Stop	Sugar	Synapse
				Teslacrypt	Tommyleaks	Trigona
				Trinity	U-Bomb	Underground
				Vicesociety	Vohuk	Wastedlocker
				Weaxor	Xorist	Yanluowang

TLP:CLEAR

Melhor Prevenir que Remediar

cert.br nic.br cgi.br

Recomendações

	Medida
Controle de Acesso e gestão de identidade	• Implementar autenticação com múltiplos fatores • Adequar permissões ao mínimo necessário (Privilégio Mínimo)
Gestão de Vulnerabilidades	• Manter equipamentos e sistemas atualizados - priorizar sistemas expostos e vulnerabilidades ativamente exploradas
Reduzir superfície de ataque	• Segmentar a rede • Desativar serviços que não são usados • Não expor serviços e dados desnecessariamente na Internet
<i>Backup</i>	• Fazer e testar <i>backups</i> periodicamente • Proteger contra acesso e modificação não autorizada
Conhecer e monitorar o ambiente	• Conhecer o que é padrão no ambiente e monitorar: - <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	• Treinar colaboradores para que saibam reconhecer e reportar: - <i>phishing</i> e outros potenciais ataques de engenharia social - infecção por <i>malware</i>
Processos e procedimentos	• Ter um plano de resposta a incidentes

O básico faz diferença



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>

Obrigada

© lucimara@cert.br

© notificações para: cert@cert.br X @certbr

<https://cert.br/>

nic.br cgi.br

www.nic.br | www.cgi.br