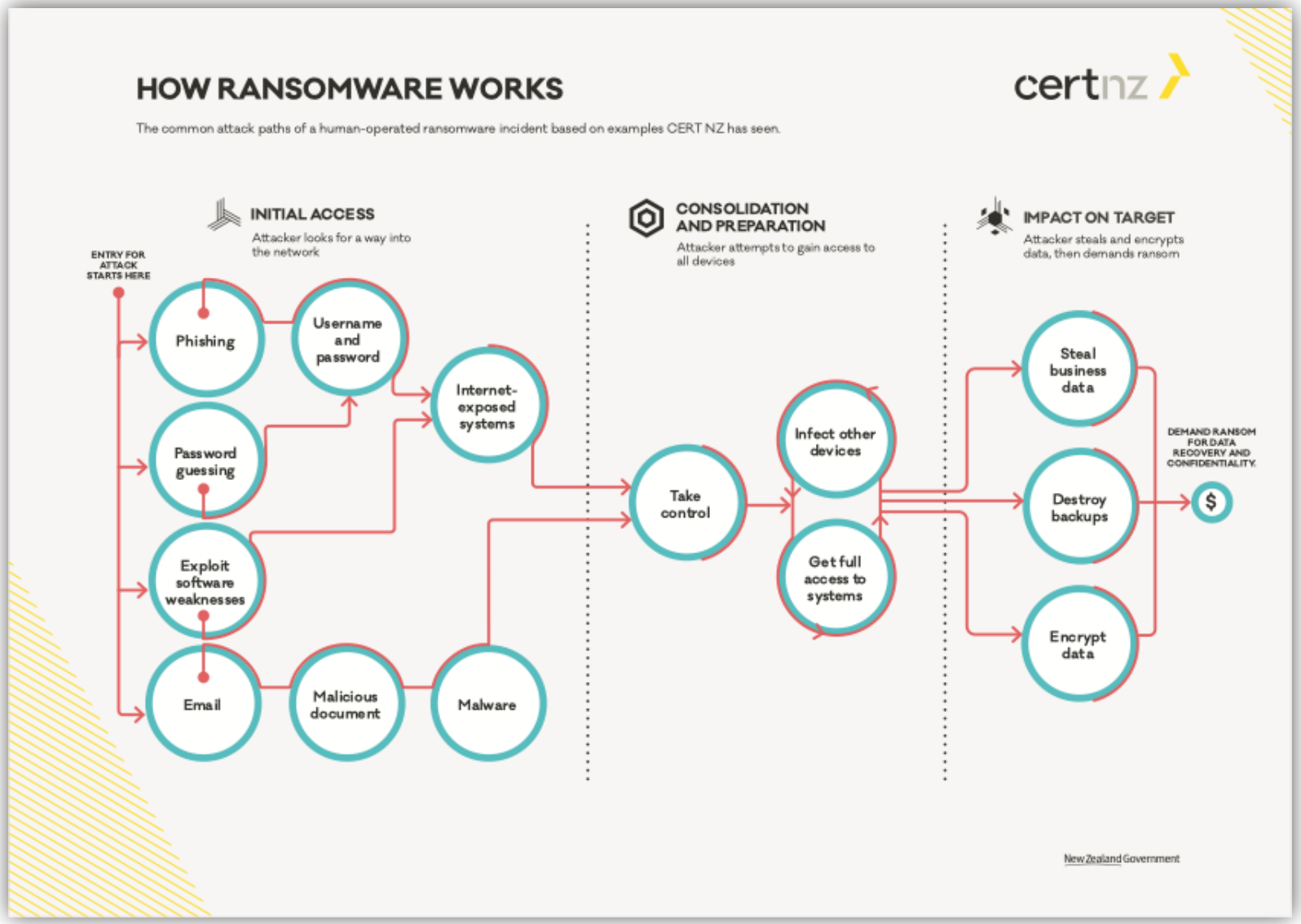
Ransomware, muito além de uma infecção por *malware*

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

Esquenta CTF – Programa *Hackers* do Bem
São Paulo, SP – 04 de abril de 2025

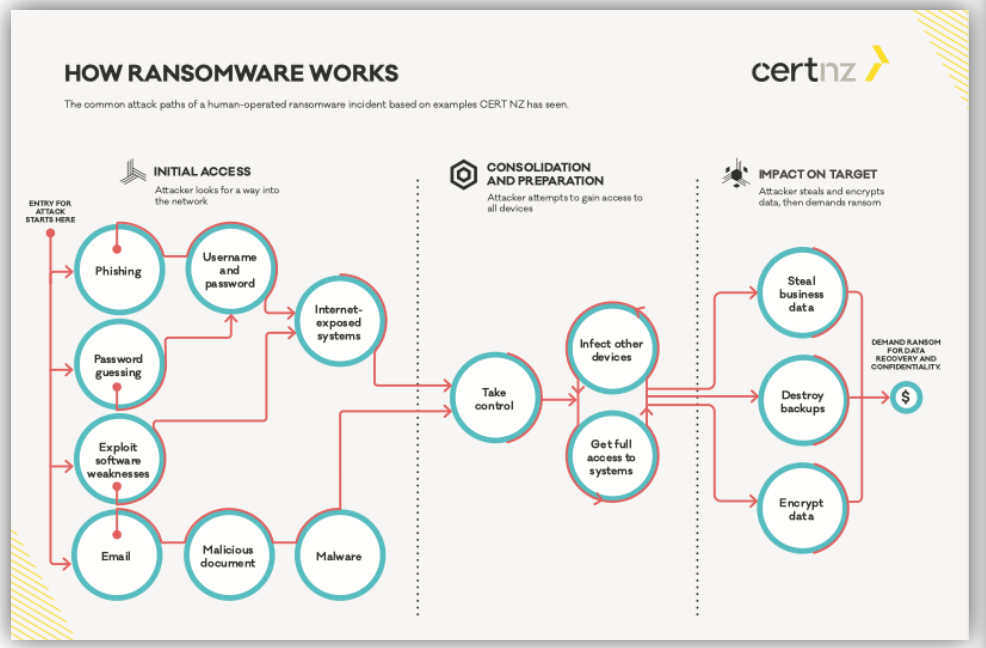
cert.br nic.br cgi.br

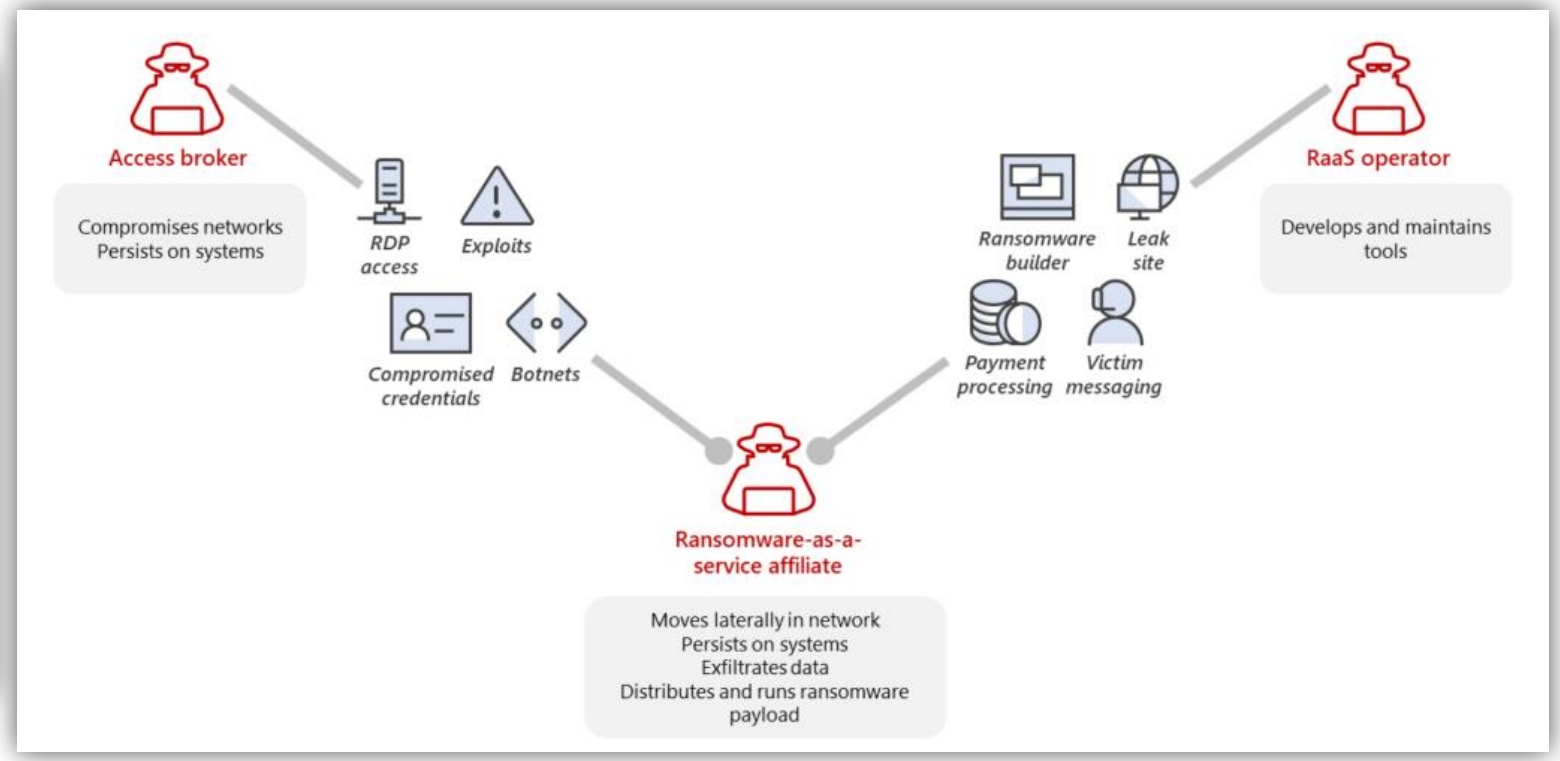
Human Operated Ransomware



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

Ransomware as a Service – RaaS

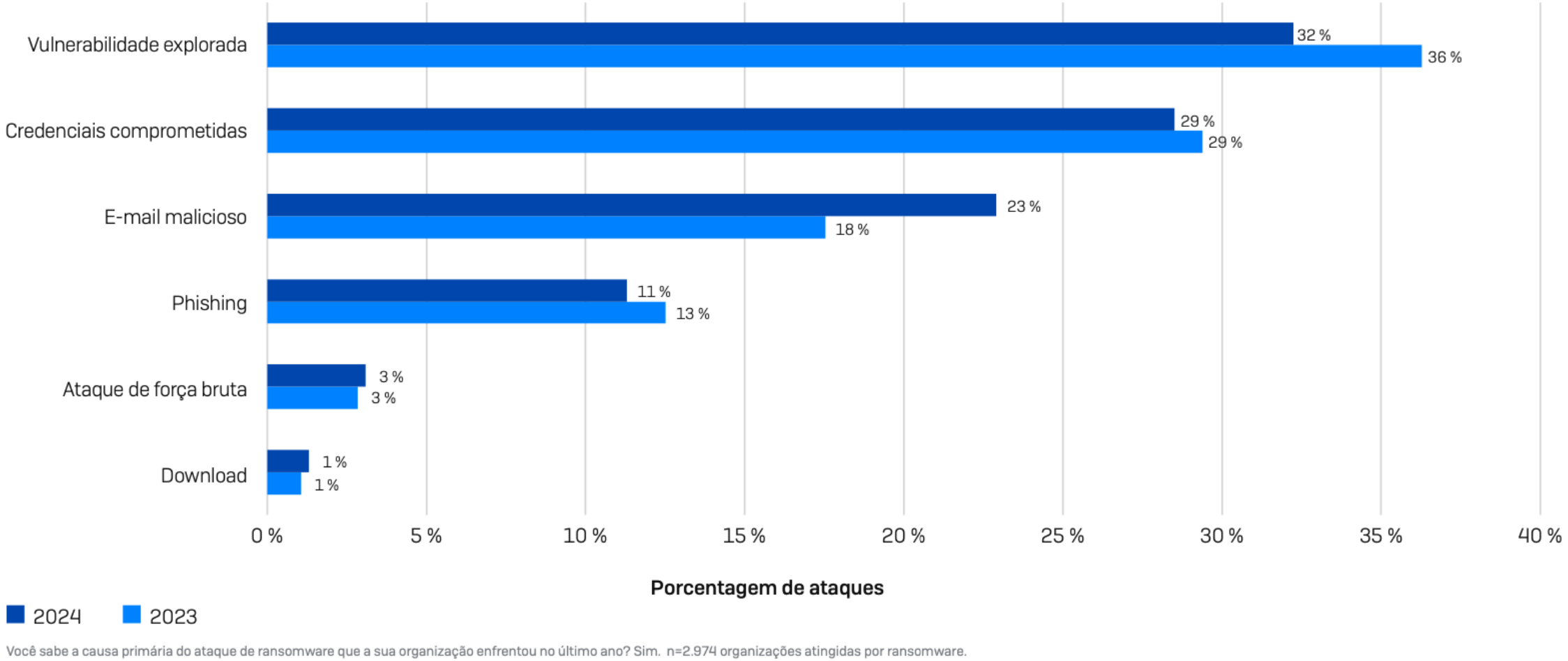




Fonte: https://www.cert.govt.nz/assets/ransomware/cert-lifecycle-of-a-ransomware-incident-business-version.pdf
https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

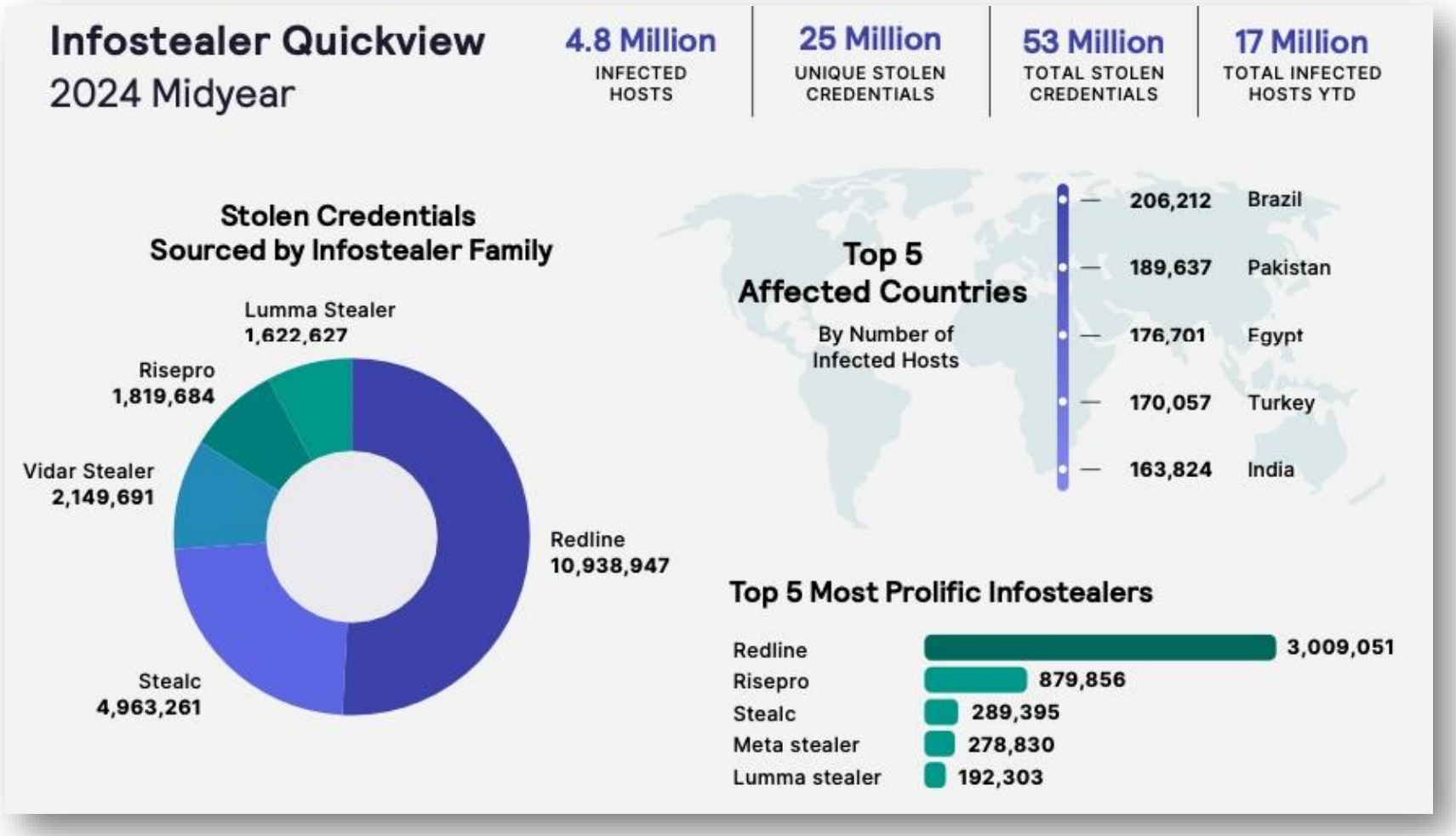
TLP:CLEAR

Causas primárias dos ataques de *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

TLP:CLEAR

CYBERSECURITY ADVISORY

#StopRansomware: RansomHub Ransomware

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

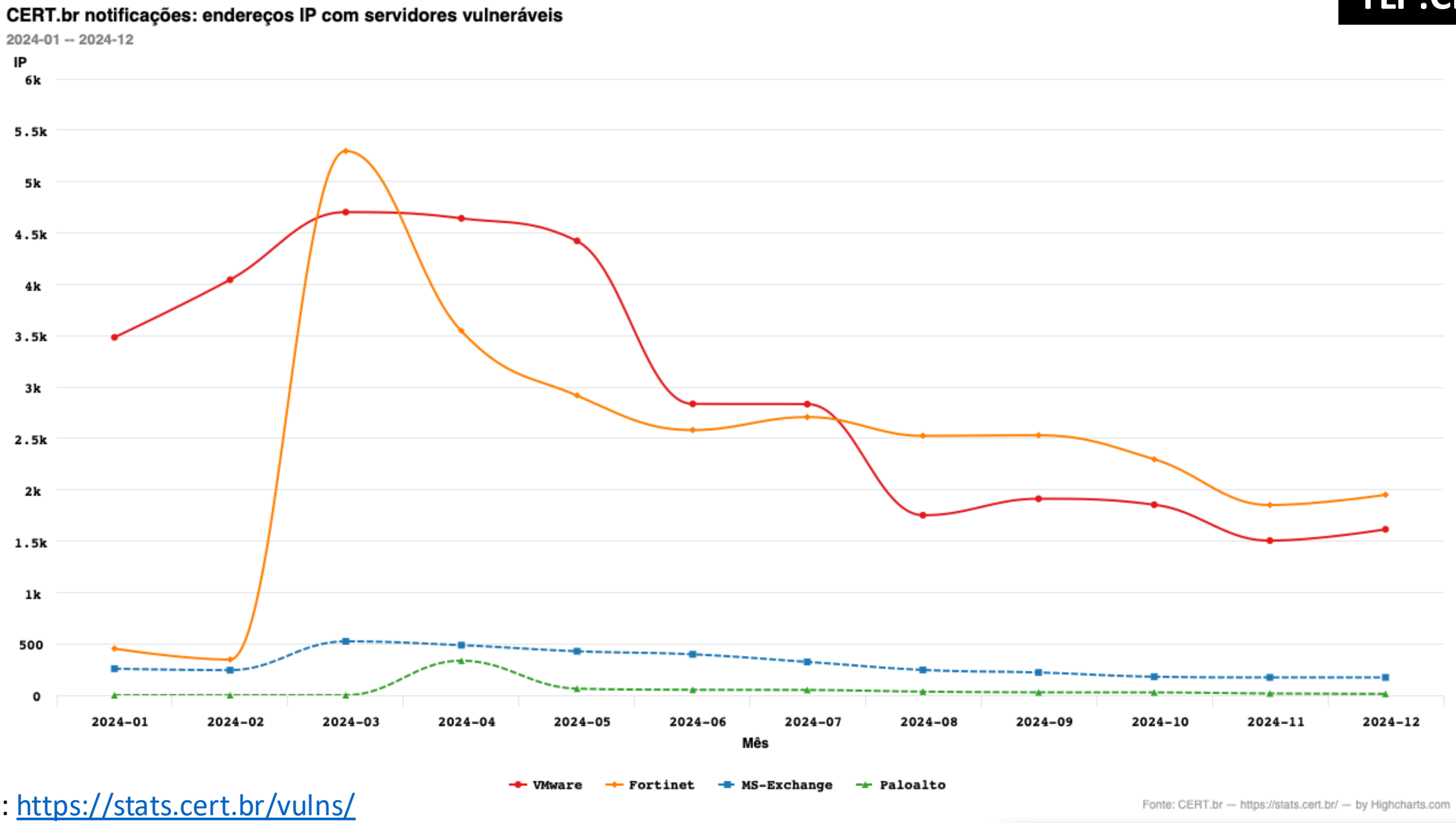
Initial Access

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



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

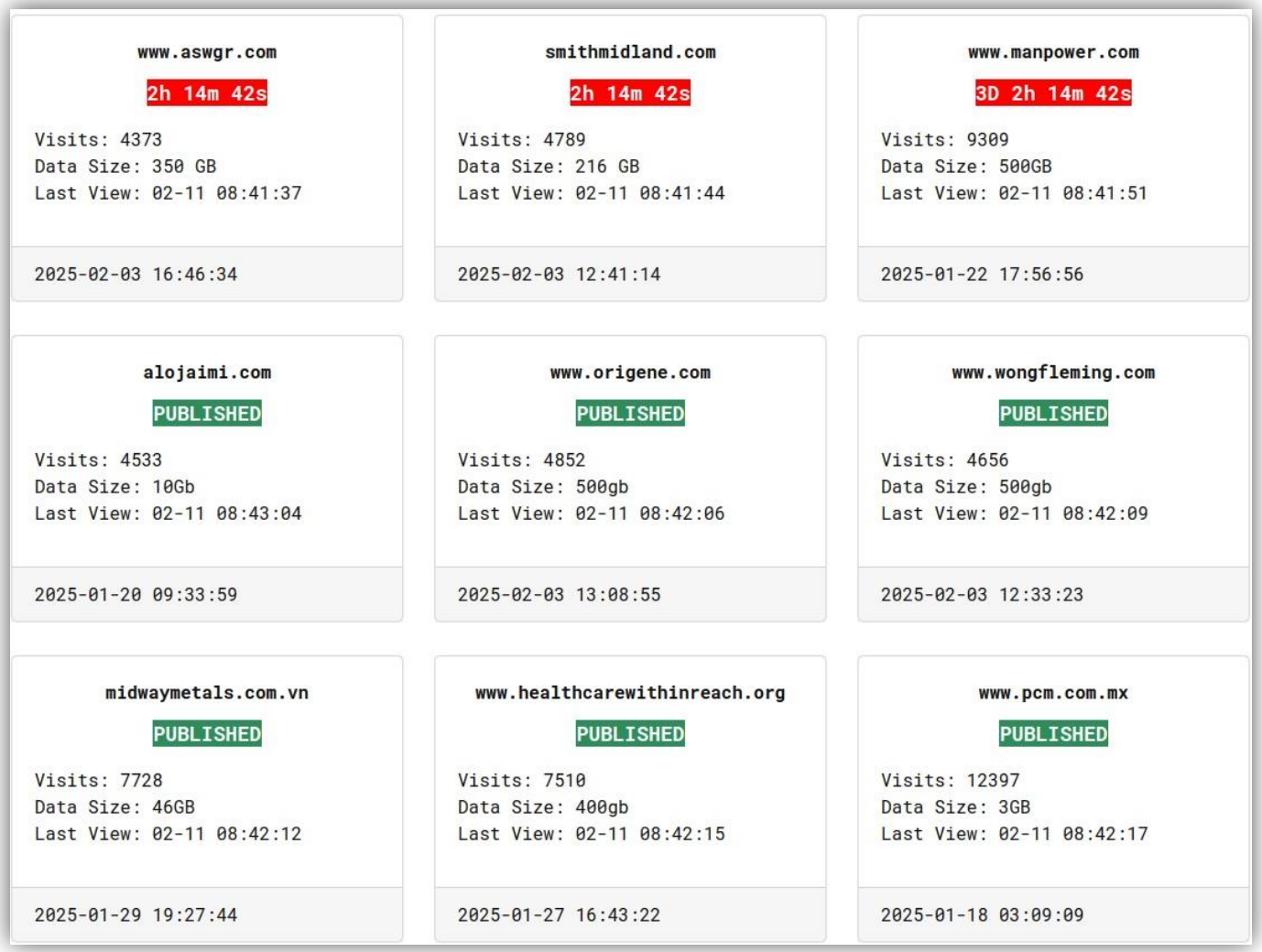
Following initial access, RansomHub affiliates created user accounts for persistence [T1136], reenabled disabled accounts [T1098], and used Mimikatz [S0002] on Windows systems to gather credentials [T1003] and escalate privileges to SYSTEM [T1068]. Affiliates then moved laterally inside the network through 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



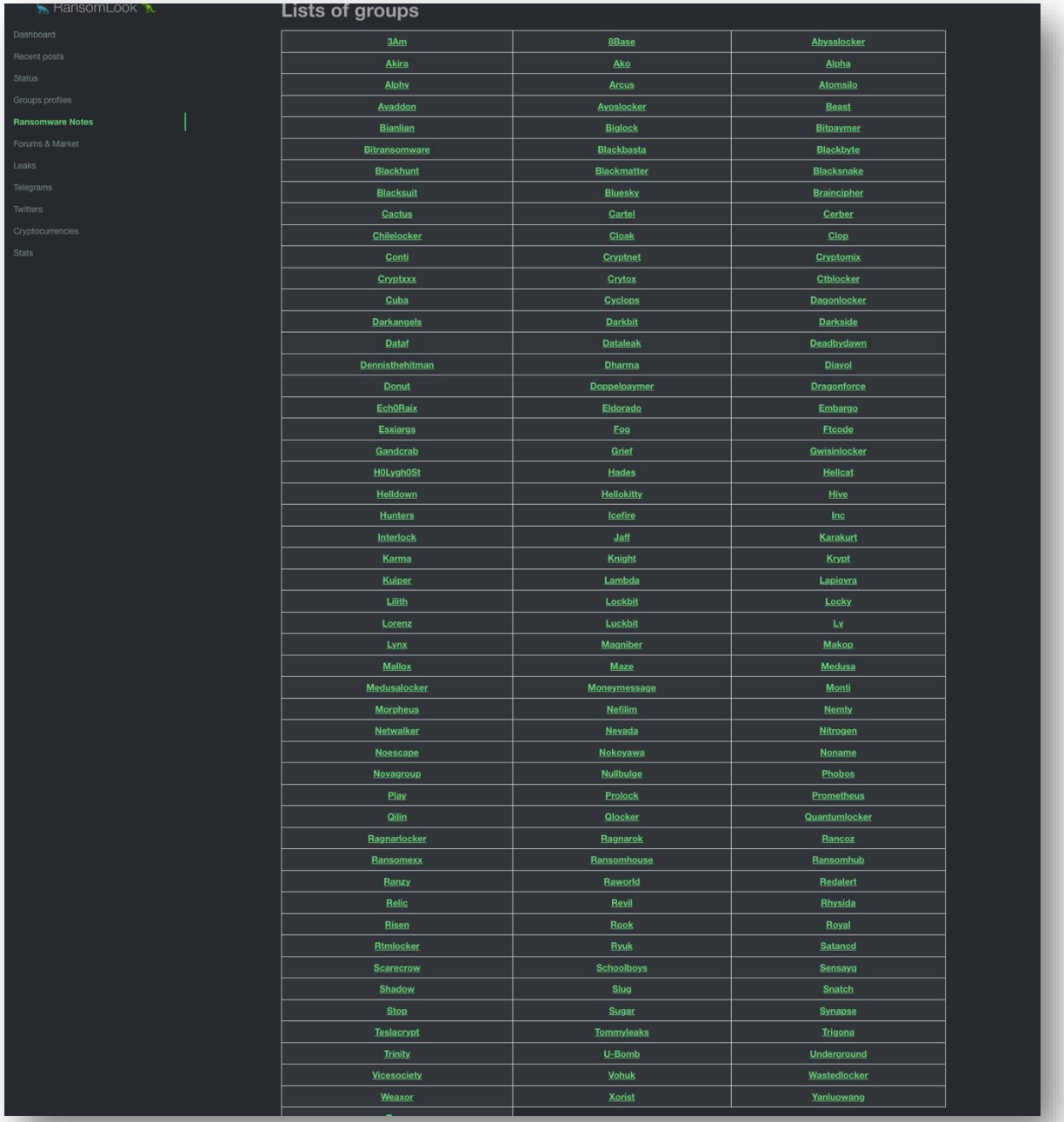
www.aswgr.com 2h 14m 42s Visits: 4373 Data Size: 350 GB Last View: 02-11 08:41:37 2025-02-03 16:46:34	**smithmidland.com** 2h 14m 42s Visits: 4789 Data Size: 216 GB Last View: 02-11 08:41:44 2025-02-03 12:41:14	**www.manpower.com** 3D 2h 14m 42s Visits: 9309 Data Size: 500GB Last View: 02-11 08:41:51 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.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

TLP:CLEAR

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
Backup	• **Fazer e testar *backups* periodicamente** • **Proteger** contra acesso e modificação não autorizada
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

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

Obrigada

lucimara@cert.br

notificações para: cert@cert.br

@certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br