The Four Horses of Evil: Threat Actors & Malware, May – June 2023

Brad E. Rhodes

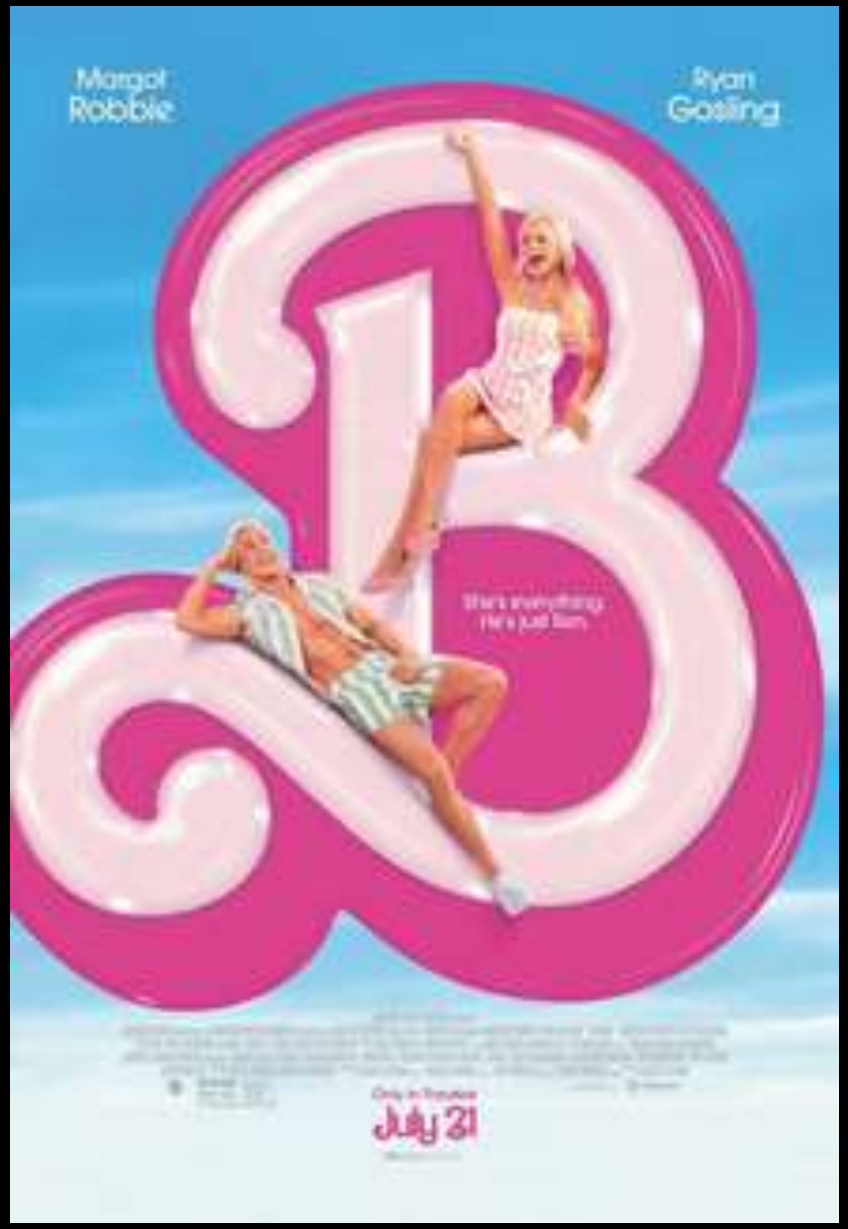
Outline

- WHOIS: Brad E. Rhodes
- How's your summer been?
- Snakes, Pandas, Extortion, and Zero Days
- Snake Malware (APT 29)
- Volt Typhoon (Vanguard Panda)
- CL0P Ransomware/Extortion
- UNC4841
- Summary / Q&A?

WHOIS:Brad Rhodes

- TLDR:
  - Senior Manager, Accenture Federal Services
  - COL, Cyber (17A), 63rd Readiness Division, G6/CIO
  - Military Cyber Professionals Association, HammerCon Co-Lead
  - Speaker, Author, Professor, Coach
  - #toomany Pro-Certs, highlights: CISSP-ISSEP, CISM, CDPSE, PMP, CEH, GMON, GCIH, Cloud+, CySA+
  - Extra Class Amateur Radio (HAM): KG4COS
- Feel free to view/listen/grab my previous presentation/articles here: https://github.com/cyberguy514

How’s your summer been?



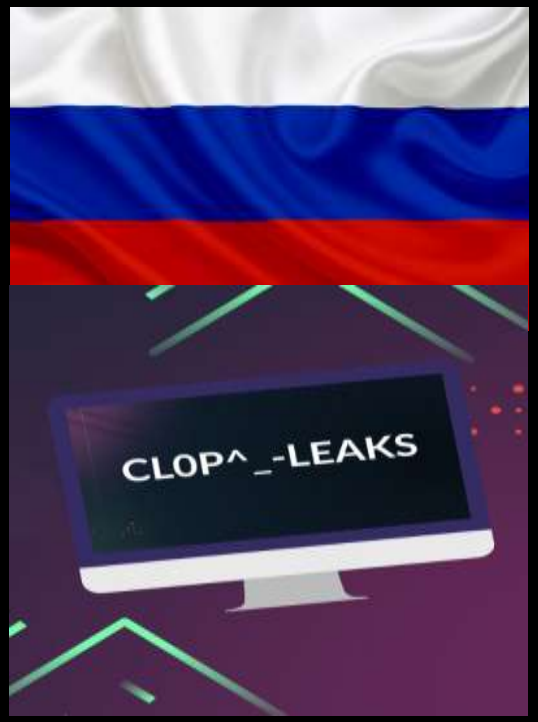
Copyright Warner Brothers

Copyright Universal & Syncopy

Snakes, Pandas, Extortion, and Zero Days

https://www.cisa.gov/sites/default/files/2023-05/aa23-129a_snake_malware_2.pdf

https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/



https://www.progress.com/security/moveit-transfer-and-moveit-cloud-vulnerability

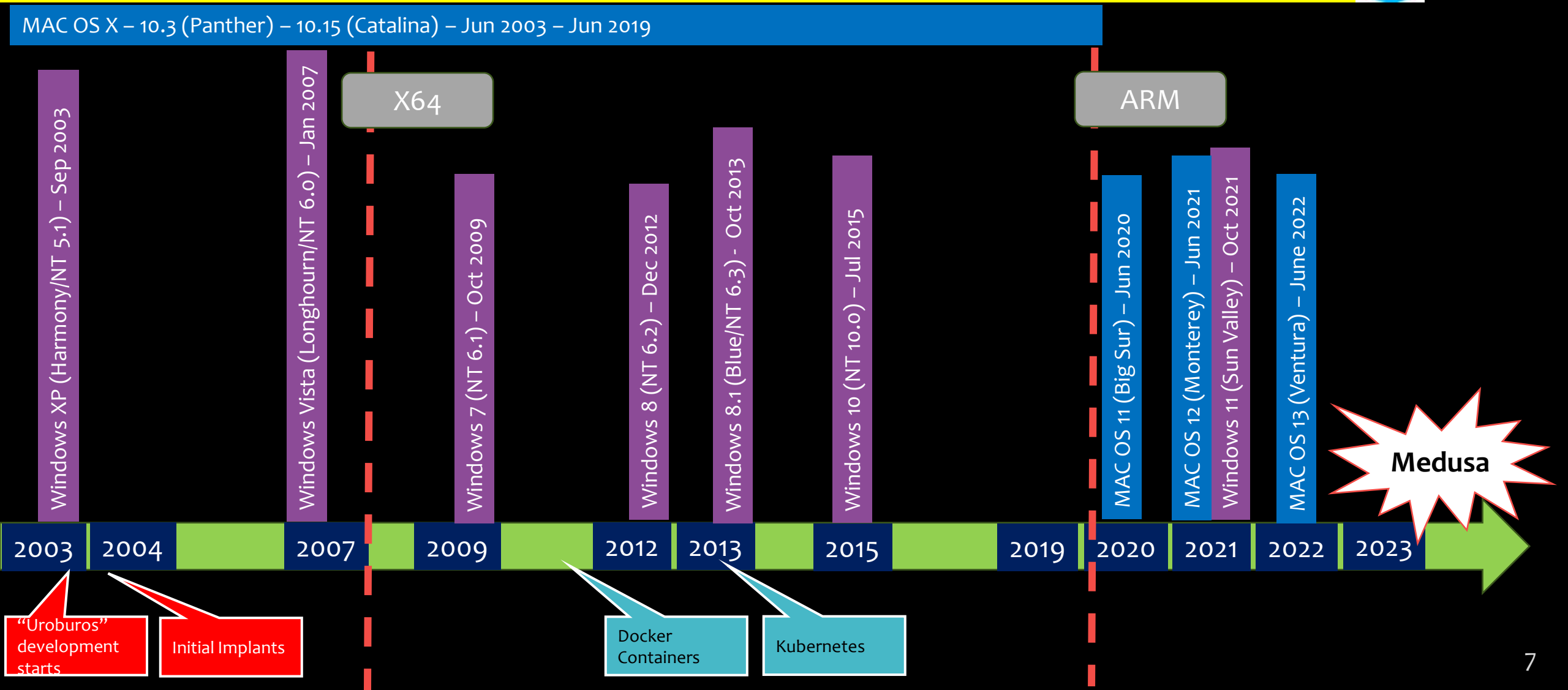
https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

Snake Malware (APT 29): “Cozy Bear”

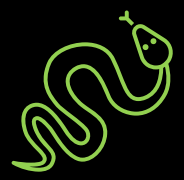
https://www.bankinfosecurity.com/russian-backed-apt-groups-compete-each-other-report-a-13149

Snake Malware (APT 29): Timeline

So may Linux variants…

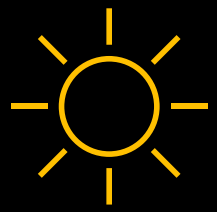


Snake Malware (APT 29): – We've seen this before…



Snake Malware

- Mission: Espionage
- Threat Actor: APT29 (Russian FSB)
- Vector: Supply Chain (Long Term)
- Use of Readily Available Components: Yes
  - Examples: OpenSSL, AES, Containers
- Interactive Access Capable: Yes
- Unique-ish Encoding: Base62
- Impact: Unknown



Sunburst Malware (SolarWinds)

- Mission: Espionage
- Threat Actor: APT29 (Russian FSB)
- Vector: Supply Chain (Short Term)
- Use of Readily Available Components: Yes
  - Examples: Cobalt Strike
- Interactive Access Capable: Yes
- Unique-ish Encoding: Base32, XOR'd
- Impact: Unknown

No need for threat actors in the same family to re-invent the wheel when the same TTPs continue to work!

Snake Malware (APT 29): Operation Medusa

PRESS RELEASE

Justice Department Announces Court-Authorized Disruption of Snake Malware Network Controlled by Russia's Federal Security Service

Tuesday, May 9, 2023

Share

FBI-created tool named *PERSEUS*, which issued commands that caused the Snake malware to overwrite its own vital components!

Through Operation MEDUSA, the FBI, and the U.S. Attorney's Office for the Eastern District of New York Neutralized the FSB's Premier Cyberespionage Malware Implant in Coordination with Multiple Foreign Governments

The Justice Department today announced the completion of a court-authorized operation, code-named MEDUSA, to disrupt a global peer-to-peer network of computers compromised by sophisticated malware, called "Snake", that the U.S. Government attributes to a unit within Center 16 of the Federal Security Service of the Russian Federation (FSB). For nearly 20 years,

TOP

https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-snake-malware-network-controlled

JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA23-129A

May 9, 2023

Communications Security Establishment | Centre de la sécurité des télécommunications

Canadian Centre for Cyber Security | Centre canadien pour la cybersécurité

National Cyber Security Centre | Australian Government Australian Signals Directorate | ACSC Australian Cyber Security Centre | National Cyber Security Centre

Hunting Russian Intelligence "Snake" Malware

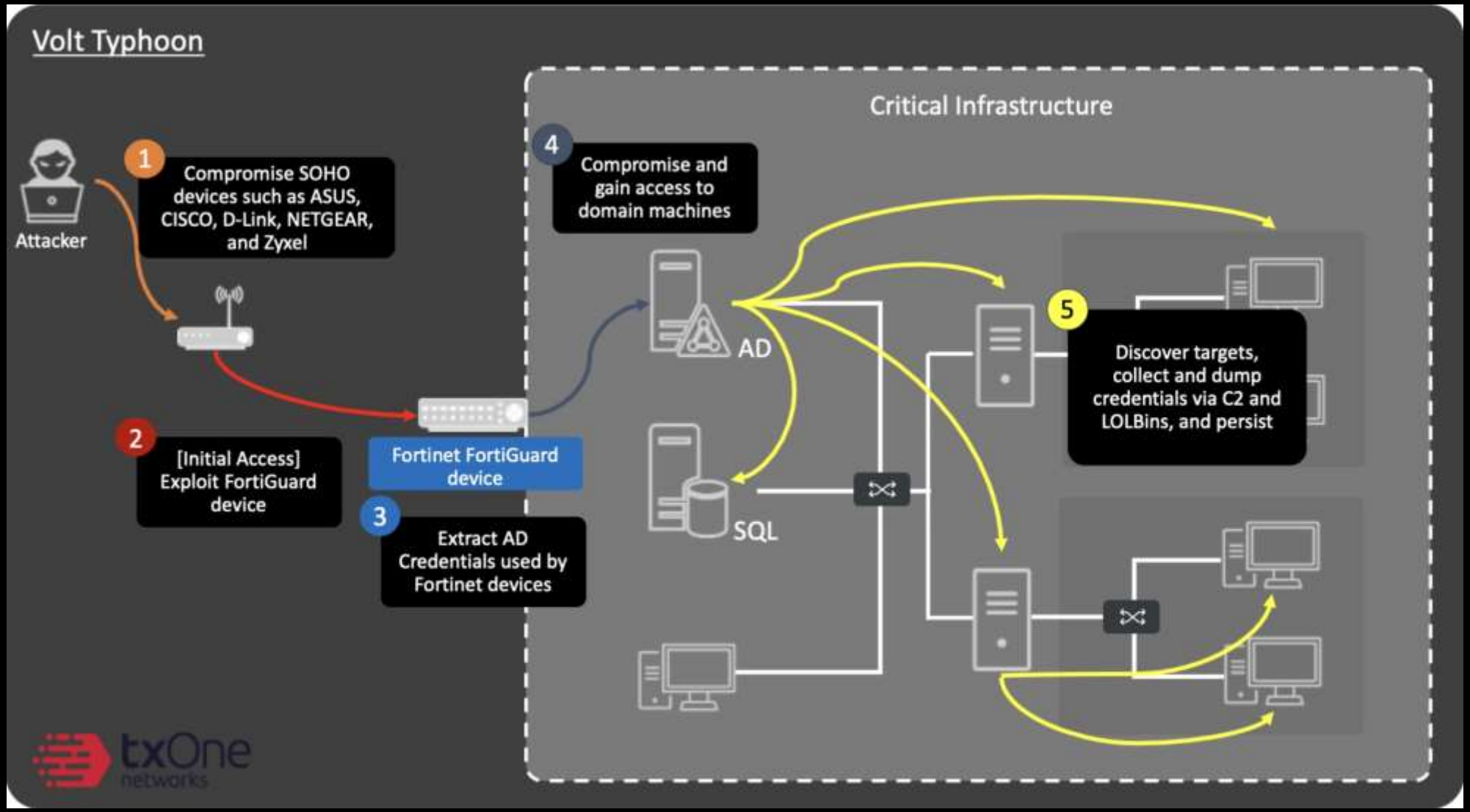
SUMMARY

The Snake implant is considered the most sophisticated cyber espionage tool designed and used by Center 16 of Russia's Federal Security Service (FSB) for long-term intelligence collection on sensitive targets. To conduct operations using this tool, the FSB created a covert peer-to-peer (P2P) network of numerous Snake-infected computers worldwide. Many systems in this P2P network serve as relay nodes which route disguised operational traffic to and from Snake implants on the FSB's ultimate targets. Snake's custom communications protocols employ encryption and fragmentation for confidentiality and are designed to hamper detection and collection efforts.

https://www.cisa.gov/sites/default/files/2023-05/aa23-129a_snake_malware_2.pdf

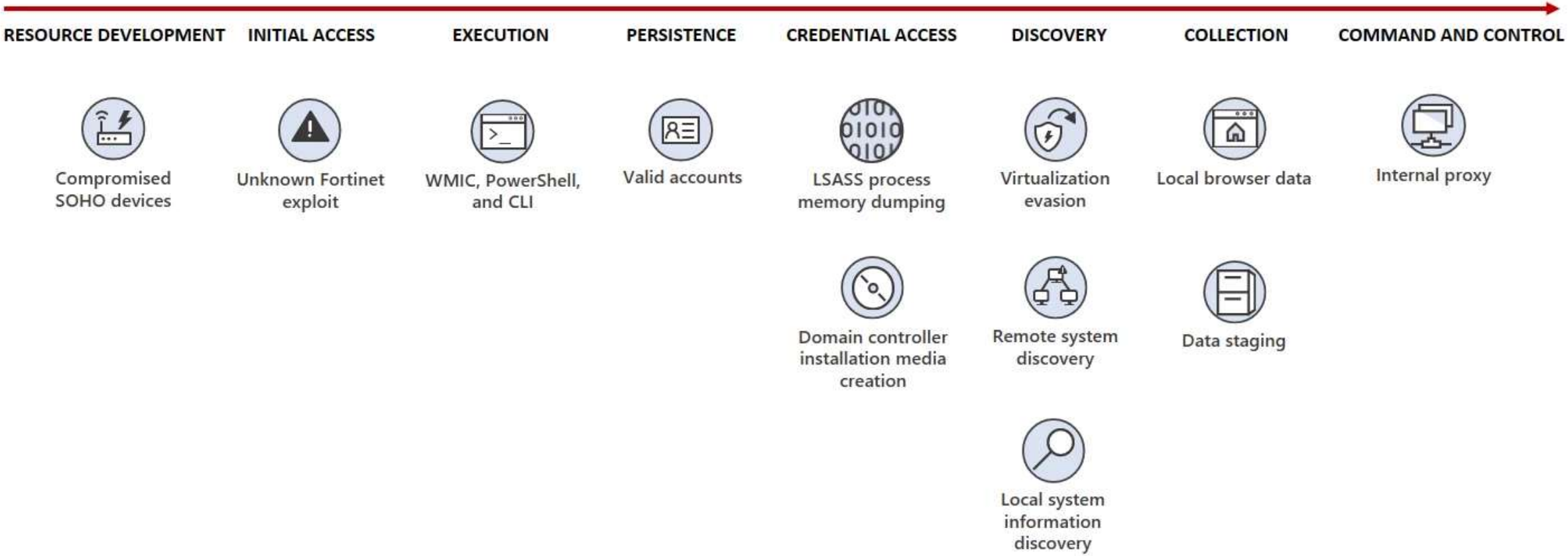
Snake was "caught" because of human-errors! In some cases, apparent rushed deployments occurred with operators leaving function names, cleartext strings, and developer comments in plain sight.

Volt Typhoon (Vanguard Panda): Critical Infrax



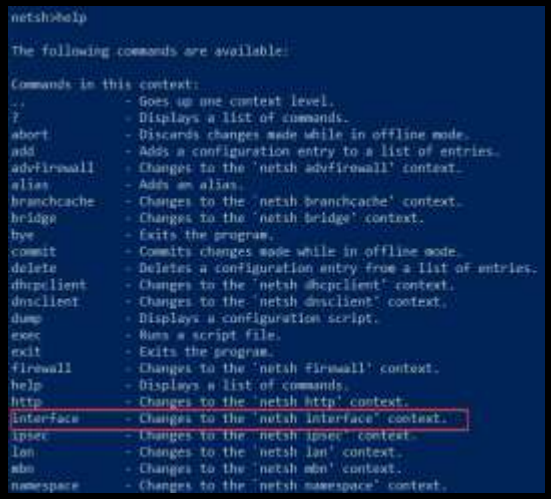
https://www.txone.com/blog/volt-typhoons-cyberattack/

Volt Typhoon (Vanguard Panda): TTPs



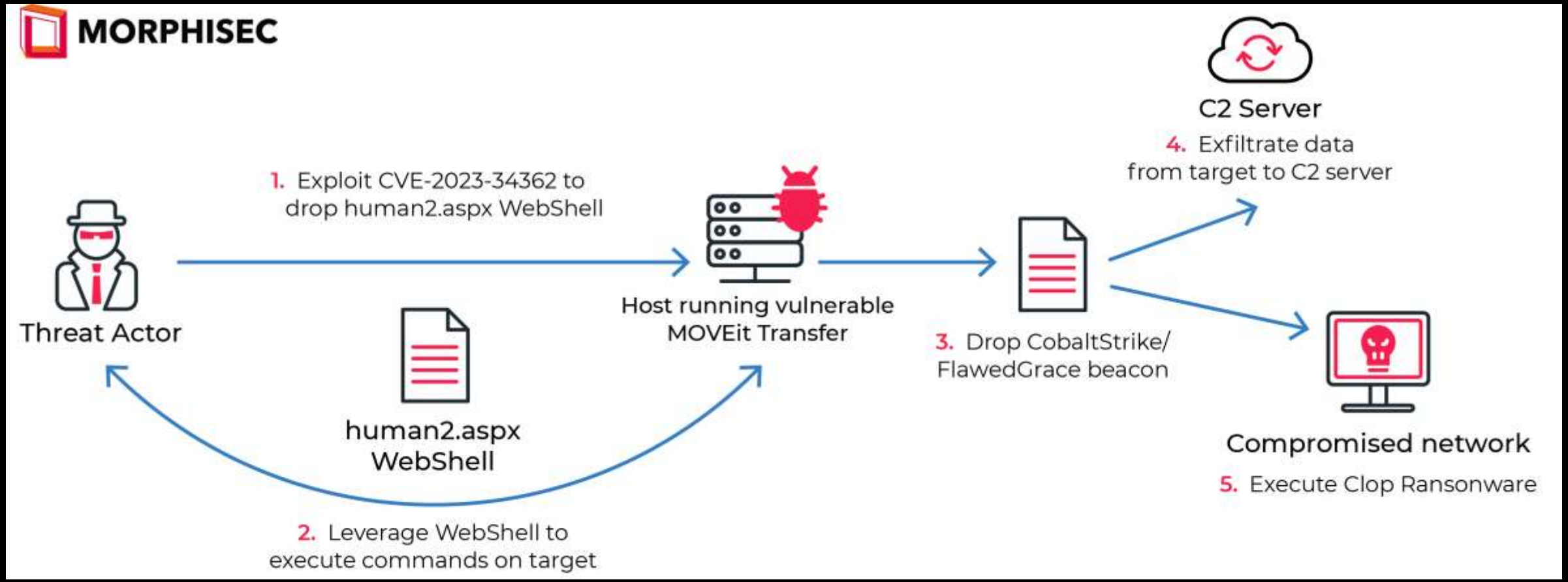
https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

Volt Typhoon (Vanguard Panda): Living-off-the-Land



https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF

CL0P Ransomware/Extortion: SQL Injection



https://blog.morphisec.com/how-to-protect-against-the-moveit-transfer-exploit

CL0P Ransomware/Extortion: Multiple Versions

Affected Version	Fixed Version	Documentation	Comments
MOVEit Transfer 2023.0.0 (15.0)	MOVEit Transfer 2023.0.2 (15.0.2)	MOVEit 2023 Upgrade Documentation	Patches were updated to include fixes for the Jun 9 CVE.
MOVEit Transfer 2022.1.x (14.1)	MOVEit Transfer 2022.1.6 (14.1.6)	MOVEit 2022 Upgrade Documentation	Patches were updated to include fixes for the Jun 9 CVE.
MOVEit Transfer 2022.0.x (14.0)	MOVEit Transfer 2022.0.5 (14.0.5)		
MOVEit Transfer 2021.1.x (13.1)	MOVEit Transfer 2021.1.5 (13.1.5)	MOVEit 2021 Upgrade Documentation	Patches were updated to include fixes for the Jun 9 CVE.
MOVEit Transfer 2021.0.x (13.0)	MOVEit Transfer 2021.0.7 (13.0.7)		
MOVEit Transfer 2020.1.x (12.1)	Special Patch Available	See KB Vulnerability (May 2023) Fix for MOVEit Transfer 2020.1 (12.1)	Patches were updated to include fixes for the Jun 9 CVE.
MOVEit Transfer 2020.0.x (12.0) or older	MUST upgrade to a supported version	See MOVEit Transfer Upgrade and Migration Guide	Patches were updated to include fixes for the Jun 9 CVE.
MOVEit Cloud	Prod: 14.1.6.97 or 14.0.5.45 Test: 15.0.2.39	All MOVEit Cloud systems are fully patched at this time. Cloud Status Page	Patches were updated to include fixes for the Jun 9 CVE.

https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023

CL0P Ransomware/Extortion: Extortion

DEAR COMPANIES

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

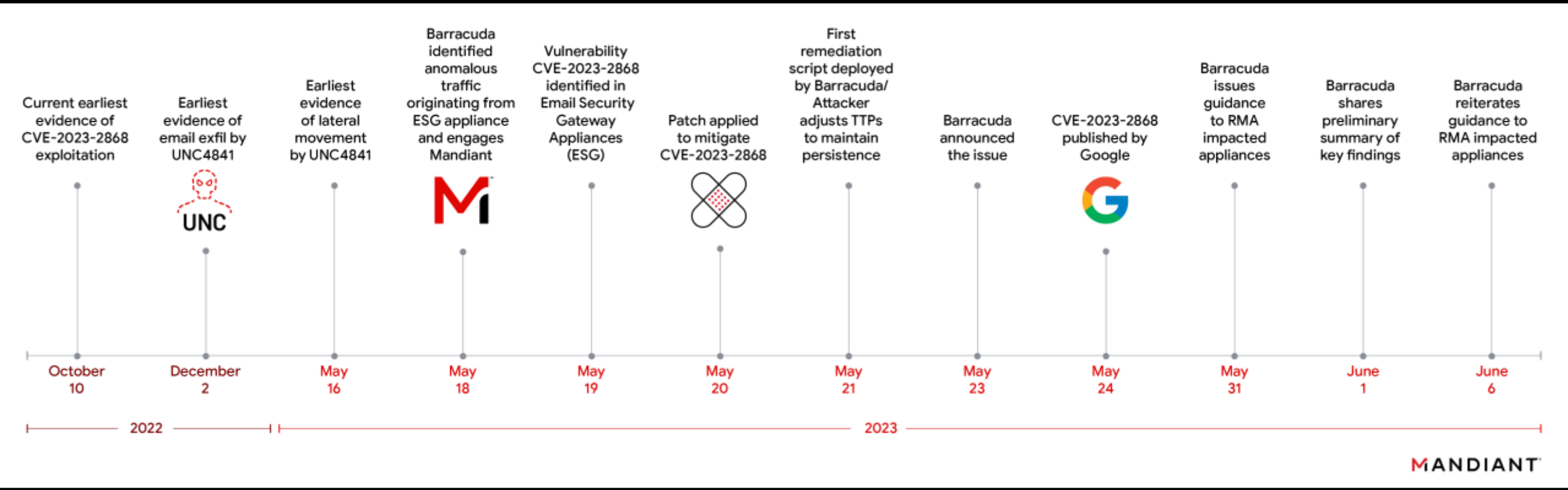
STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

https://cybernews.com/editorial/moveit-clop-ransomware-explained/

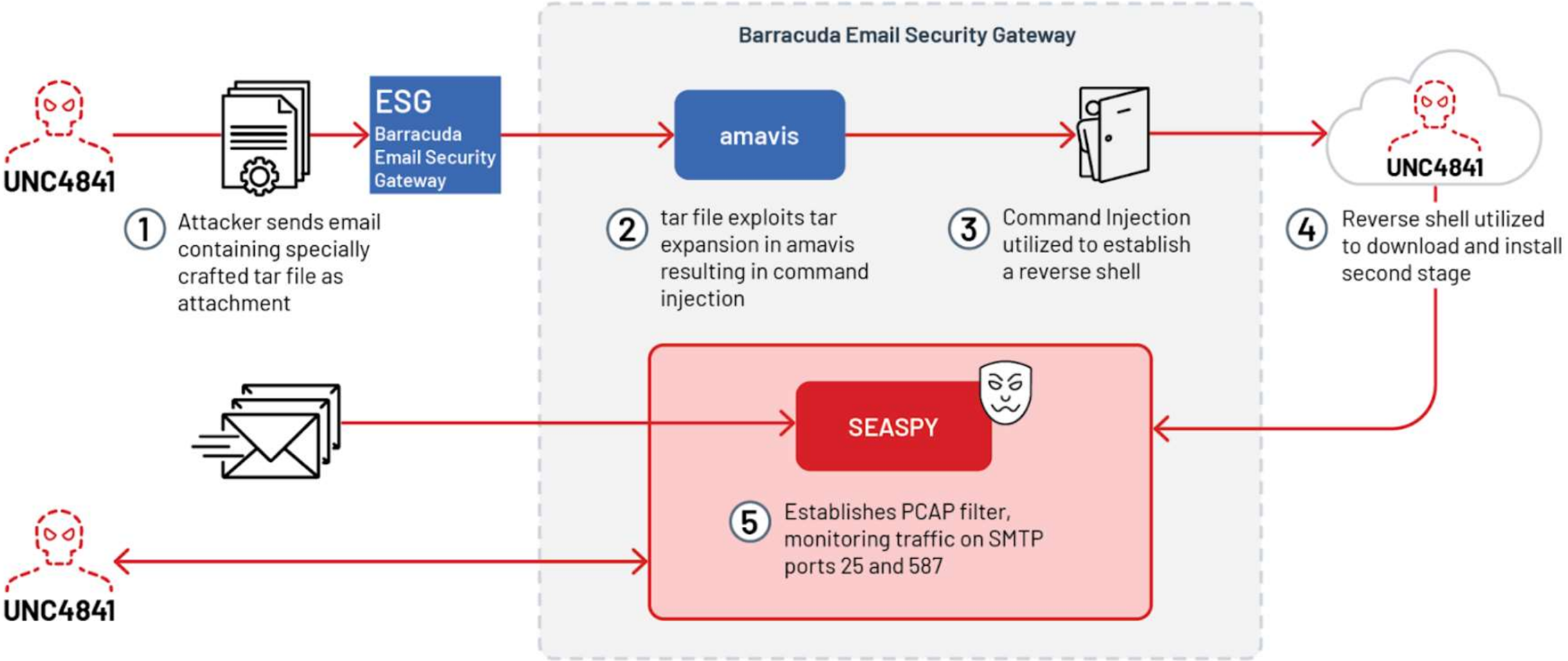
https://www.darkreading.com/attacks-breaches/shell-latest-clop-moveit-victim

UNC4841: Barracuda ESG Attack Timeline



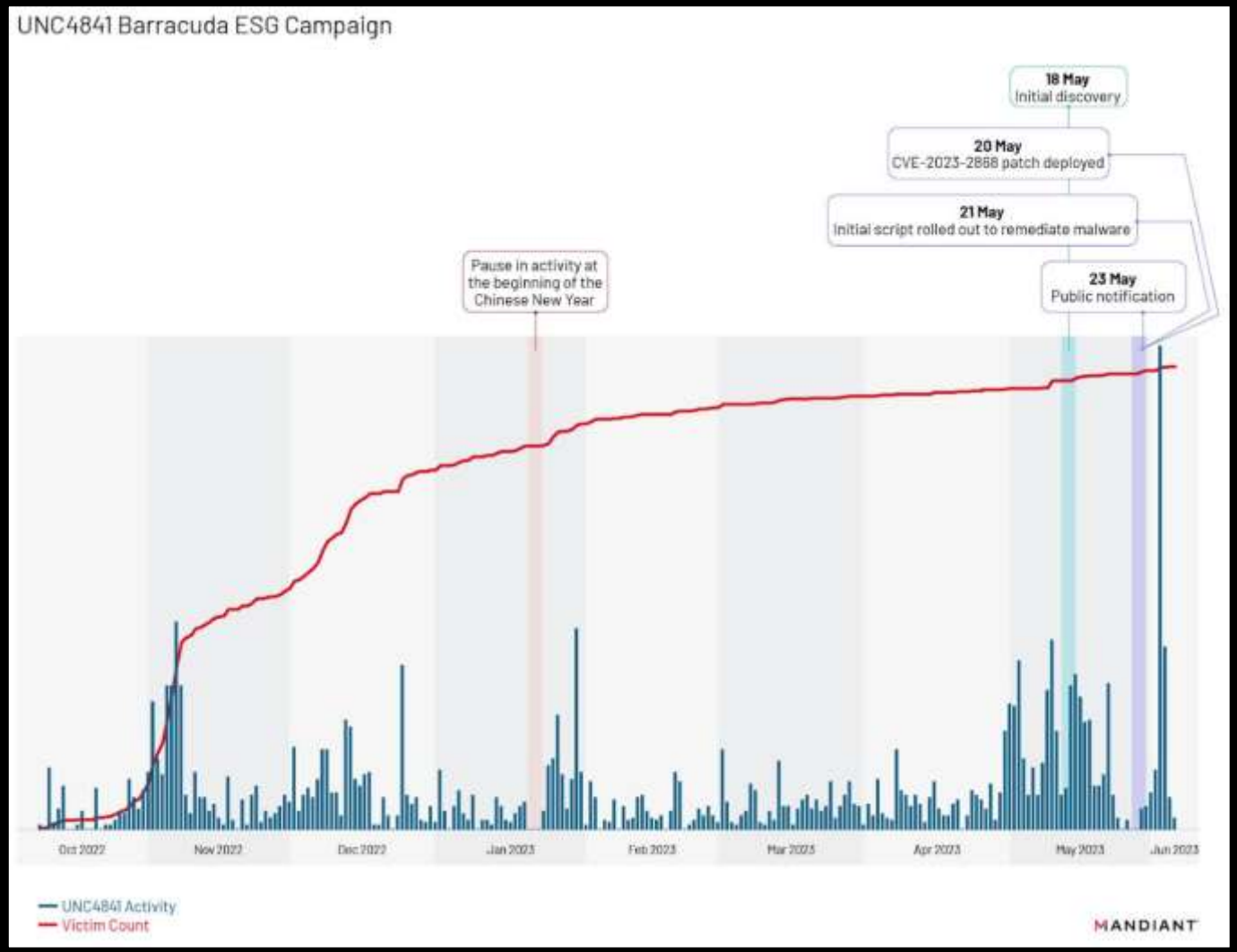
https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

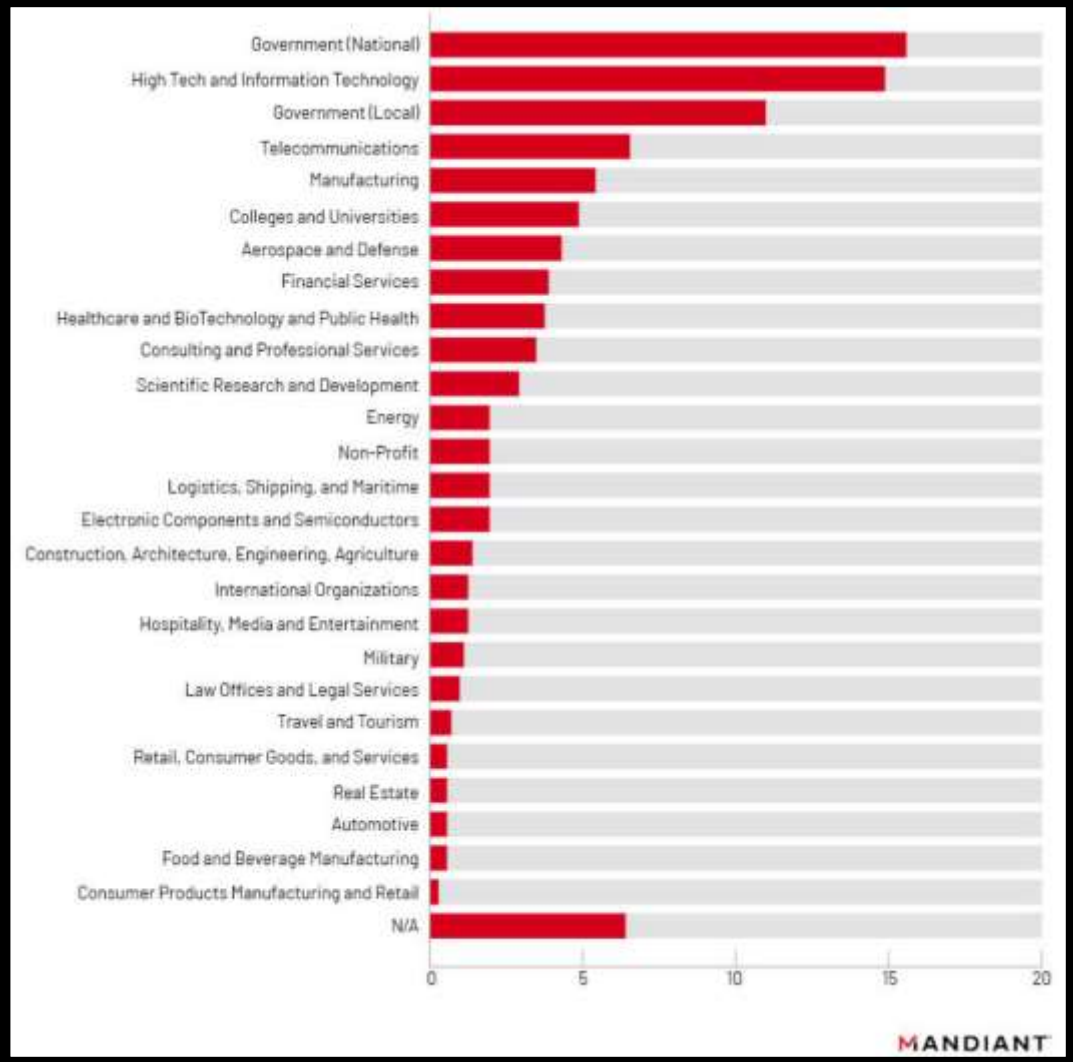
UNC4841: No User Interaction Needed!



https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

UNC4841: A True APT Campaign



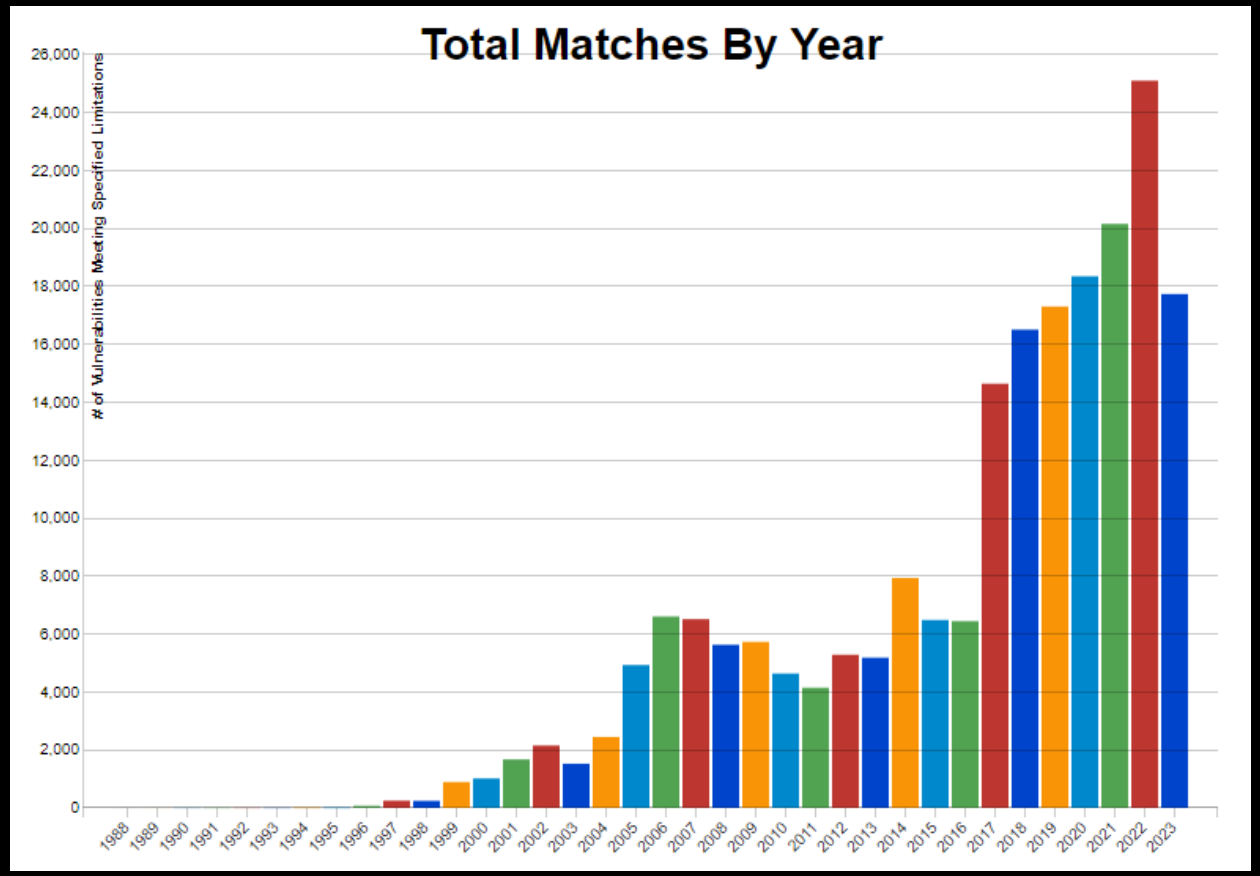


https://www.mandiant.com/resources/blog/unc4841-post-barracuda-zero-day-remediation

Summary

- It has been a crazy summer!
- APT29's Snake malware in operations since 2003
- Vanguard Panda was (likely is) testing US cyber defenses
- CL0P did not have to work very hard
- UNC4841 likely purchased Barracuda ESGs
- Living-off-the-Land and why we need detailed logs (https://www.malwarearchaeology.com/cheat-sheets)

BONUS – CISA KEV Catalog



https://www.cisa.gov/known-exploited-vulnerabilities-catalog

https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all&isCpeNameSearch=false

Thanks Peak Cyber!

Happy to Connect!: https://www.linkedin.com/in/brad-e-rhodes-the-terminal-colonel/