2024-03-20

HUNTER

EMERGING THREATS

VOLT TYPHOON THREAT GROUP

UPDATE 3/20/24: On Tuesday (3/19/24), an advisory from President Biden's administration was released to state governors, detailing the threat of foreign entities including the Volt Typhoon group targeting critical drinking water and wastewater infrastructure - with the potential to "disrupt the critical lifeline of clean and safe drinking water". With Volt Typhoon in particular, it was revealed that last month the threat group was discovered infiltrating networks of a number of critical infrastructure organizations such as communications, energy, transportation, and water and wastewater. They have been identified as "pre-positioned" within these environments, enabling the threat of carrying out disruption across the critical infrastructure sectors. It was recommended that these water facilities adopt basic security measures, such as resetting default passwords and updating software, and provided a list of additional actions and resources; which can be found here: [Top Cyber Actions for Securing Water Systems](https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems)

CYBORG SECURITY

THREAT SUMMARY

UPDATE 3/20/24: On Tuesday (3/19/24), an advisory from President Biden's administration was released to state governors, detailing the threat of foreign entities including the Volt Typhoon group targeting critical drinking water and wastewater infrastructure - with the potential to "disrupt the critical lifeline of clean and safe drinking water". With Volt Typhoon in particular, it was revealed that last month the threat group was discovered infiltrating networks of a number of critical infrastructure organizations such as communications, energy, transportation, and water and wastewater. They have been identified as "pre-positioned" within these environments, enabling the threat of carrying out disruption across the critical infrastructure sectors. It was recommended that these water facilities adopt basic security measures, such as resetting default passwords and updating software, and provided a list of additional actions and resources; which can be found here: [Top Cyber Actions for Securing Water Systems](https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems)

Volt Typhoon is a state-sponsored cyber espionage group that has been observed to be active since 2021. The threat actor has had operations targeting several different countries, but have had a presence conducting campaigns against the United States and Guam - with the apparent goal being to disrupt communication infrastructure between the United States and Asia region. Additionally, organizations that have been targeted by the group include communications, manufacturing, utility, transportation, construction, education, government, and information technology. Volt Typhoon has been known to gather intelligence and conduct surveillance operations on nations, specializing in their stealth and persistence. In recent events (January 2024), the United States Department of Justice and the FBI (Federal Bureau of Investigation) released a statement regarding a Volt Typhoon led operation attempting to target US critical infrastructure via KV botnet - to which was shut down and disrupted by mimicking an attacker's C2 network to send a remote kill command. With Volt Typhoon's continued efforts and persistence to conduct malicious campaigns against U.S. and critical infrastructure (combined with warnings from the Department of Justice of upcoming threats), it is important to assess, understand and prepare for the actor's capabilities and operations.

SYNOPSIS

The Volt Typhoon threat group, believed to be state-sponsored by the Chinese government, has been associated with numerous attacks targeting critical infrastructure in the United States since 2021. They have recently been affiliated with a botnet (KV Botnet) malware campaign that was comprised of hundreds of United States based small office/home office routers being compromised - and was neutralized by FBI and DOJ related entities in January 2024. Known for gathering intelligence and executing surveillance operations stealthily, the threat actors relied on living-off-the-land techniques to stay hidden and blended in with normal network activity by abusing these vulnerable routers.

Volt Typhoon utilizes a range of tactics, techniques, and procedures (TTPs), including spear-phishing campaigns, exploitation of vulnerabilities in public-facing applications, and the use of customized toolkits/malware to infiltrate target networks. An actor that utilizes living-off-the-land techniques and tools, such as WMIC (Windows Management Instrumentation Command line) for local command execution, PsExec for remote executions, and native discovery utilities (such as netstat, systeminfo) for example - their method of operation is to compromise, gather/steal information, and disrupt services covertly.

HUNT PACKAGES

SHADOWCOPY IMAGE ACCESSED
https://hunter.cyborgsecurity.io/research/hunt-package/812301b1-e7b2-4d58-928f-ccef60b48762

NETSH PORT FORWARDING COMMAND
https://hunter.cyborgsecurity.io/research/hunt-package/0eca36b6-57ef-42b2-bf74-6d0b7dd12aa1

WMIC WINDOWS INTERNAL DISCOVERY AND ENUMERATION
https://hunter.cyborgsecurity.io/research/hunt-package/bc0fd59c-4217-46a7-a167-764727118567

POTENTIALLY INJECTED PROCESS COMMAND EXECUTION
https://hunter.cyborgsecurity.io/research/hunt-package/7daf20ca-9558-4b09-bb38-03a09e47746b

DUMP LSASS VIA COMSVCS DLL
https://hunter.cyborgsecurity.io/research/hunt-package/f68b340c-0148-458f-913d-344a39509632

POTENTIAL IMPACKET WMIEXEC MODULE COMMAND EXECUTION
https://hunter.cyborgsecurity.io/research/hunt-package/5b4c793a-260a-4d43-bbc7-ad4547eeacda

DUMP ACTIVE DIRECTORY DATABASE WITH NTDSUTIL - POTENTIAL CREDENTIAL DUMPING
https://hunter.cyborgsecurity.io/research/hunt-package/98846e7f-c90c-4156-8643-54a613286b66

EXCESSIVE WINDOWS DISCOVERY COMMANDLINE ARGUMENTS - POTENTIAL MALWARE INSTALLATION
https://hunter.cyborgsecurity.io/research/hunt-package/8bb5819f-06a4-4e5d-9099-e43115601999

REMOTE PROCESS INSTANTIATION VIA WMI
https://hunter.cyborgsecurity.io/research/hunt-package/dd0ca1e2-046f-4878-b7f8-32b790420ef2

POWERSHELL ENCODED COMMAND EXECUTION
https://hunter.cyborgsecurity.io/research/hunt-package/d2d3bbc2-6e57-4043-ab24-988a6a6c88db

RELATED LINKS
Sign up for free HUNTER access
Volt Typhoon Threat Group Emerging Threat Collection

MITRE CONTEXT

- Tactic Names:
  - Privilege Escalation
  - Discovery
  - Defense Evasion
  - Execution
  - Command and Control
  - Credential Access
  - Lateral Movement
- Technique Names:
  - Obfuscated Files or Information
  - PowerShell
  - OS Credential Dumping
  - System Information Discovery
  - NTDS
  - Proxy
  - Windows Management Instrumentation
  - SMB/Windows Admin Shares
  - Remote System Discovery
  - System Network Configuration Discovery
  - Process Injection
- Threat Names:

REFERENCES

1. https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/
2. https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/
3. https://www.darkreading.com/cybersecurity-operations/us-govt-reportedly-trying-to-disrupt-volt-typhoon-attack-infrastructure
4. https://www.justice.gov/usao-sdtx/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical