Volt Typhoon Threat Profile

By Will Seligman

2024

Overview

Volt Typhoon is a sophisticated state sponsored Chinese APT group operating under the People's Republic of China. The group has gained significant attention in recent years for its advanced tactics and techniques aimed at compromising critical infrastructure in the United States and other countries, in-depth reconnaissance, and extensive post-exploitation data collection.

Motivations

Volt Typhoon's primary motivation appears to be preparing for potential future conflicts or crises involving the United States. The group's activities suggest they are:

- Pre-positioning themselves on IT networks of critical infrastructure organizations.
- Maintaining long term persistence to carry out objectives.
- Gaining access to operational technology (OT) systems.
- Developing capabilities to disrupt or destroy critical infrastructure in the event of a major crisis or escalated geopolitical tensions or military conflicts.

This approach differs from traditional cyber espionage operations, indicating a more aggressive intent. (1)

Attribution

Volt Typhoon has been linked to sponsorship by the People's Republic of China (PRC) due to a combination of TTPs consistently observed in their operations, with indicators linked back 5 years effectively to 2019. (1) Multiple cybersecurity firms and intelligence agencies have linked the group under various aliases, Vanguard Panda, Dev-0391, UNC3236, BRONZE SILHOUETTE, Voltzite, to the Chinese state through the following factors:

- **Operational Patterns:** The group’s operations align with the strategic interests of the PRC, particularly in targeting U.S. critical infrastructure, indicating state sponsorship. (5)

- **China's Denial vs. Continued Operations:** Despite consistently denying involvement, China has been repeatedly accused of cyber espionage and interference, as seen in the 2021 New Zealand hacking incident linked to APT40. These denials have done little to stop their state-sponsored groups from being tied to ongoing malicious cyber activity targeting critical infrastructure and democratic institutions globally.(8)
- **Consistent Targeting of U.S. and Allied Critical Infrastructure:** The group's focus on pre-positioning in critical systems mirrors other Chinese cyber espionage campaigns, suggesting preparation for future disruptive or destructive operations during a potential geopolitical conflict.(7)

Summary of Recent Activity (2022 to current)

Volt Typhoon has been actively compromising IT networks of critical infrastructure organizations in the United States and its territories. Key points include:

- Compromises detected in Communications, Energy, Transportation Systems, and Water and Wastewater Systems sectors. (1)
- Successful infiltration of networks in both continental and non-continental United States, including Guam. (4)
- Exploitation of CVE-2024-39717, in Versa Director servers, with the deployment of a sophisticated "VersaMem" web shell for credential harvesting and in-memory code execution, observed from June 12, 2024.(5)
- Exploitation of CVE-2022-42475 in an FortiGate 300D firewall. (1)
- Use of a sophisticated SOHO router botnet (KV-botnet) as covert data transfer infrastructure, with observed activity against ISPs, telecommunications firms, and a U.S. territorial government entity in Guam from August 2022 through May 2023. (4)
- Focus on maintaining long-term, undiscovered persistence by using Living Off the Land techniques, avoiding malware, and relying on native tools including downloading outdated comsvcs.dll for credential dumps, or Magnet RAM Capture for memory dumps. (1)

Notable Tactics, Techniques, and Procedures

1. Extensive reconnaissance (TA0043):
    - Web searches for victim (T1591), network (T1590), and staff information (T1589)
    - Targeted queries on exposed infrastructure (T1592, T1594, T1592)
    - Identification of key network and IT staff (T1589.002)
2. Initial Access (TA0001):
    - Exploitation of both publicly available vulnerabilities (T1588.005) and zero-day vulnerabilities (T1587.004)
    - Focus on publicly exposed services, networking appliances, and remote services (T1190)
3. Execution and Stealthy Operational Security (TA0002):
    - Minimal activity within compromised environments, and little to no malware
    - Selective log deletion and artifact removal to conceal actions (T1070)
    - Using legitimate tools (T1105), to prevent suspicious detections
    - Extensive use of Living Off the Land (LOTL/LOL) techniques and native tools (TA0005)
4. Persistence and Defense Evasion (TA0003, TA0005):
    - Minimal malware usage and activity within compromised environments
    - Use of valid credentials, usually extracted from the compromised public facing applications (T1068, T1552), or through the credential access phase
    - Use of Fast Reverse Proxy (FRP) clients on victim infrastructure for covert channels (T1090, T1573)
5. Credential Access and Discovery (TA0006, TA0007):
    - Commonly extracting security logs to .dat files and analysis for further user reconnaissance
    - Avoidance of data exfiltration, instead focusing on persistence, dumping NTDS.dit (T1003.003) via volume shadow copies (T1006)
    - Regular extraction of domain credentials, repeated exfiltration of NTDS.dit files from domain controllers (T1003.003)
    - Credentials from public facing applications after initial access from zero-days or CVEs (T1068, T1552)
    - Exploitation of web browser data for stored credentials
6. Command and Control (TA0011):
    - Typically composed of Virtual Private Servers (VPSs) or small office/home office (SOHO) routers (T1090.002, T1584.005)
    - Compromised routers and IoT devices

Conclusion

Volt Typhoon represents a significant threat to global critical infrastructure. Its sophisticated tactics, long-term planning, and focus on high operational security for evasion, set it apart from other APT groups. As tensions between nations continue to rise, the potential for Volt Typhoon to play a role in future conflicts remains a pressing concern for national security agencies worldwide.

References

- https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
- https://blog.lumen.com/taking-the-crossroads-the-versa-director-zero-day-exploitation/
- https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/
- https://unit42.paloaltonetworks.com/volt-typhoon-threat-brief/
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a
- https://www.cisa.gov/resources-tools/resources/prc-state-sponsored-cyber-activity-actions-critical-infrastructure-leaders
- https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques
- http://web.archive.org/web/20240407094745/https://www.scmp.com/news/asia/australasia/article/3256736/new-zealand-accuses-china-hacking-parliament-following-us-uk-allegations