Word Count: 1502, excluding this note, section titles, footnotes and the References section

Introduction

On the 24th May 2023, Microsoft announced that they had uncovered malicious activity by Volt Typhoon, a People's Republic of China (PRC) state-sponsored actor [3]. Based on the targeting of the IT systems of organisations responsible for critical infrastructure in the US and allied territories, the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) assessed that *"People's Republic of China (PRC) state-sponsored cyber actors are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States."* [9]

The attack is particularly concerning due to the effectiveness of the techniques used to evade detection and the geopolitical tensions between the USA and PRC. This case study provides an overview of the incident (including the methods used), associated security failures and potential mitigation techniques.

Incident Overview

Though initially reported in May 2023, it is believed that Volt Typhoon's infiltration dates back to 2021 [3]. Below is an estimated timeline:

- **Mid-2021:** Volt Typhoon is active on US and allied cyberspace [1]
- **February 2023:** The FBI is deployed to, and CISA begins defence engagement with, Guam [1], a US territory of strategic importance in the Indo-Pacific [11].
- **May 2023:** Microsoft release blog post detailing Volt Typhoon's activities [1]
- **September 2023:** CISA and FBI identify potential victims, and CISA confirms compromises of critical infrastructure. [1]
- **January to February 2024:** US government disrupts the "KV Botnet" used by Volt Typhoon and release a Joint Cybersecurity Advisory (JCSA) document. [1]
- **April 2024:** US president Biden signs a new national security memorandum in an effort to protect critical infrastructure [12].
- **November 2024:** Cybersecurity ratings platform SecurityScorecard reports a "resurgence of Volt Typhoon" [13].

The CISA observed that Volt Typhoon tailored their tactics, techniques, and procedures (TTPs) according to the victim, but that attacks tended to follow a particular pattern [9]:

1. **Reconnaissance:** information is gathered on the target to identify vulnerabilities.

2. **Initial access:** access to the target system is gained, typically through the exploitation of known or zero-day vulnerabilities[1] of network appliances.
3. **Privilege Escalation:** after access is gained, the actor uses privilege escalation attacks[2] to obtain administrator-level credentials. (In some cases, credentials were accessed on public-facing appliances)
4. **Lateral Movement:** the credentials are used to move across the network and gain access to the domain controller[3].
5. **Discovery:** the actor uses living off the land (LOTL)[4] techniques to gather intelligence on the system.
6. **Full Compromise:** the Active Directory Database[5] is extracted from the domain controller.
7. **Deciphering of hashes:** the actor uses a variety of methods to 'break' the hashes stored on the Active Directory Database, gaining higher-level access.
8. **Additional infiltration and discovery:** Higher-level access is used for additional infiltration and discovery, often targeting systems that are used to control utilities.

The TTPs employed by Volt Typhoon underscore some of the weaknesses of cyber infrastructure system, as discussed below.

Security Failures and Preventative Measures

The success of Volt Typhoon's activities highlighted some critical weaknesses in the cyber defence systems of the affected organisations. However, many of these weaknesses could have been mitigated by preventative measures.

Arguably, the key issue exploited by Volt Typhoon, allowing them initial access to systems, was the inadequate security of public-facing network security appliances. Sometimes this was due to issues not identified by the vendor, as in the case of Versa Director (see [5]), but could often be attributed to poor patch management. In the case of Fortinet FortiGuard devices, Volt Typhoon appeared to take advantage of a known issue, which could have been prevented if the device owners had applied the relevant

[1] "A zero-day vulnerability is an undiscovered flaw in an application or operating system, a gap in security for which there is no defence or patch because the software maker does not know it exists—they've had "zero days" to prepare an effective response." [14]
[2] "A privilege escalation attack is a cyberattack to gain illicit access of elevated rights, permissions, entitlements, or privileges beyond what is assigned for an identity, account, user, or machine." [15]
[3] Server responsible for user authentication and validation on a network. [16]
[4] Living Off the Land techniques use existing tools of the target system. This helps the attacker evade detection [17]
[5] Database that resides on a domain controller and contains sensitive information such as hashed passwords.

patches [8]. Indeed, the CISA include the applying of patches in their "Actions to take today to mitigate Volt Typhoon activity" [9].

Once initial access was gained, compromised small office/home office (SOHO) routers were used as proxies, enabling Volt Typhoon to carry out further discovery. The use of such devices aided the group's efforts to avoid detection [3]. Again, there was fault both on the side of vendors and that of users. Companies, such as Cisco, stopped providing updates for so-called End-of-life hardware, leaving them open to more recently discovered vulnerabilities [18]. Additionally, routers were often configured sub-optimally by users [7]. To mitigate this risk in future, actions should be taken by both vendors and users. Vendors should implement secure default configurations for their devices such as the requirement for the user to change or set the password during the initial setup. Users should adhere to security best practices, such as regularly updating firmware.

Regarding network architecture, affected organisations often failed to isolate critical components. The lack of network segmentation allowed attackers to move laterally across compromised networks to target specific components like domain controllers or Operational Technology.

Another significant weakness exploited by Volt Typhoon was the insufficient monitoring and detection capabilities of many organisations. By their very nature, LOTL techniques allow attackers' activities to blend in with normal network behaviour as only tools already on the affected system are utilised. Many organisations lack effective security against such techniques [10]. High quality, machine learning powered Security Information and Event Management (SIEM) platforms could help organisations identify the more subtle anomalies displayed by the LOTL techniques of APTs [4].

Finally, inadequate logging and auditing practices exacerbated vulnerabilities exposed by Volt Typhoon. By leveraging LOTL techniques, such as PowerShell[6] queries on Windows event logs[7], attackers were able to extract information and aid with their reconnaissance of networks post compromise [3].

These security failures illustrate the multi-faceted nature of Volt Typhoon's operations and the need for organisations to be proactive and thorough in implementing their security measures.

[6] PowerShell is a tool developed by Microsoft for system management and automation through the use of a command-line shell and scripting language [6].
[7] Windows event logs are records of the activity on a Windows operating system. Logs tend to be categorised by type: system, application, setup or security [19].

Critical Analysis and Reflection

The Volt Typhoon attack has brought into focus the complex web of responsibilities between governments, organisations, hardware and software providers, and individuals, in defending against cyber security threats.

As discussed previously, the exploitation of public-facing network security appliances and SOHO routers was vital to Volt Typhoon's success. Manufacturers have an ethical responsibility to take action to ensure the security of their devices is maintained, even if they are no longer in production. Vulnerabilities should be patched, especially for devices still in widespread use. Given the technical nature of cyber security, manufacturers should enforce secure practices by design, such as requiring the changing of default credentials during initial setup or disabling insecure features like publicly exposed management interfaces by default.

While hardware and software providers bear a significant share of responsibility, target organisations also play a crucial role. Implementing robust network segmentation, timely patch management, and intrusion detection systems could have limited Volt Typhoon's ability to move laterally or evade detection. A more proactive approach, including regular vulnerability assessments and penetration testing, is essential to identifying risks before they can be exploited.

At an individual level, citizens and employees must take responsibility for securing their personal and work-related networks. While they may not have specialised knowledge, adhering to basic cybersecurity principles, such as using strong, unique passwords and enabling multi-factor authentication, can significantly reduce vulnerabilities. For more complex measures, education becomes critical. Governments have a duty to foster cybersecurity among their citizens. This could be through measures such as integrating cybersecurity into school curricula and public awareness campaigns that inform on emerging threats and best practices for mitigation.

Governments also have a duty to ensure significant investment is made to keep cyber borders as well defended as physical borders. In his testimony before a House committee hearing, FBI Director Christopher A. Wray said that "If you took every single one of the FBI cyber agents, intelligence analysts and focused them exclusively on the China threat, China's hackers would still outnumber FBI cyber personnel by at least 50 to 1," [2]. If a nation as rich and powerful as the US has insufficient resources devoted to cybersecurity it could have severe repercussions internationally.

The Volt Typhoon attack is massive in scope. The CISA Executive director was quoted as saying that any number "is likely an underestimate" when asked about the total number of victims [20]. Given the magnitude and potential seriousness of the consequences of the operation, it highlights the need for international collaboration to aid with the detection and mitigation both of this current threat and future APTs.

Conclusion

Although Volt Typhoon has caused minimal explicit damage to date, their choice of targets—critical infrastructure systems—highlights both their strategic intent and the significant potential for disruption. Their sophisticated tactics demonstrate a capability that, if fully realised, could result in severe consequences. The chair of the House committee hearing previously discussed described the Volt Typhoon operation as "… the cyberspace equivalent of placing bombs on American bridges, water treatment facilities and power plants. There is no economic benefit for these actions. There's no pure intelligence-gathering rationale. The sole purpose is to be ready to destroy American infrastructure," [2].

While actions have been taken to disrupt their operations, Volt Typhoon remains a significant and evolving threat, and the actions of governments, organisations and individuals are pivotal to mitigating the risk they cause, and future campaign of APTs.

References

[1] **Adamski, M., Scott, A. and DeGrippo, S.** 2024. *Hiding in Plain Sight: Hunting Volt Typhoon Cyber Actors.* Presented at the RSA Conference 2024, San Francisco, CA, USA, May 6, 2024. Retrieved December 4, 2024 from https://static.rainfocus.com/rsac/us24/sess/1697229699824001SGq7/finalwebsite/2024_USA24_CID-M06_01_Hiding-In-Plain-Sight-Hunting-Volt-Typhoon-Cyber-Actors_1714497536483001iMLx.pdf.

[2] **Cadell, C., Menn, J.** 2024. *FBI says it's shut down sources of recent Chinese infrastructure hacks.* The Washington Post. Retrieved December 4, 2024 from https://www.washingtonpost.com/national-security/2024/01/31/china-volt-typhoon-hack-fbi/

[3] **Microsoft Threat Intelligence.** 2023. *Volt Typhoon targets US critical infrastructure with living-off-the-land techniques.* Microsoft Security Blog. Retrieved December 4, 2024 from https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

[4] **Nayyar, S.** 2021. *Achieving Advanced Threat Detection With Intelligent SIEM.* Forbes. Retrieved December 4, 2024 from https://www.forbes.com/councils/forbestechcouncil/2021/02/22/achieving-advanced-threat-detection-with-intelligent-siem/

[5] **Lakshmanan, S.** 2024. *Chinese Volt Typhoon Exploits Versa Director Flaw, Targets U.S. and Global IT Sectors.* The Hacker News. Retrieved December 4, 2024 from https://thehackernews.com/2024/08/chinese-volt-typhoon-exploits-versa.html

[6] **Wheeler, S., Buck, A., Koon, S., Mando, C. and Jacobson, H.** 2024. *What is PowerShell?*. Retrieved December 4, 2024 from https://learn.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.4

[7] **Unit 42.** 2024. *Threat Brief: Attacks on Critical Infrastructure Attributed to Insidious Taurus (Volt Typhoon).* Retrieved December 4, 2024 from https://unit42.paloaltonetworks.com/volt-typhoon-threat-brief/

[8] **Windsor, C.** 2023. *Analysis of CVE-2023-27997 and Clarifications on Volt Typhoon Campaign.* Fortinet PSIRT Blogs. Retrieved December 4, 2024 from https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign

[9] **Cybersecurity and Infrastructure Security Agency (CISA).** 2024. *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure.* Retrieved December 4, 2024, from https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[10] **Cybersecurity and Infrastructure Security Agency (CISA).** 2024. *Identifying and Mitigating Living Off the Land Techniques.* Retrieved December 4, 2024, from https://www.cisa.gov/resources-tools/resources/identifying-and-mitigating-living-land-techniques

[11] **Fong, C and Roy, D.** 2024. *Guam's Strategic Importance in the Indo-Pacific*. Council on Foreign Relations. Retrieved December 4, 2024 from https://www.cfr.org/in-brief/guams-strategic-importance-indo-pacific

[12] **Shepardson, D.** 2024. *Biden signs new memo to boost security of US critical infrastructure*. Reuters. Retrieved December 4, 2024 from https://www.reuters.com/world/us/biden-signs-new-memo-boost-security-us-critical-infrastructure-2024-04-30/

[13] **Sherstobitoff, R.** 2024. *The Botnet is Back: SSC STRIKE Team Uncovers a Renewed Cyber Threat*. SecurityScorecard Blog. Retrieved December 4, 2024 from https://securityscorecard.com/blog/botnet-is-back-ssc-strike-team-uncovers-a-renewed-cyber-threat/

[14] **Hewlett Packard Enterprise.** *Zero-Day Vulnerability*. HPE Glossary. Retrieved December 4, 2024 from https://www.hpe.com/uk/en/what-is/zero-day-vulnerability.html

[15] **Haber, M.J.** 2023. *Privilege Escalation Attack & Defense Explained*. BeyondTrust Blog. Retrieved December 4, 2024 from https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained

[16] **SolarWinds.** *What Is a Domain Controller?*. SolarWinds IT Glossary. Retrieved December 4, from https://www.solarwinds.com/resources/it-glossary/domain-controller

[17] **National Security Agency (NSA).** 2024. *Combatting Cyber Threat Actors Perpetrating Living Off the Land Intrusions*. Retrieved December 4, 2024 from https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3669159/combatting-cyber-threat-actors-perpetrating-living-off-the-land-intrusions/.

[18] **Greig, J.** 2024. *End-of-life Cisco routers targeted by China's Volt Typhoon group*. The Record. Retrieved December 4, 2024 from https://therecord.media/cisco-routers-end-of-life-china-espionage-volt-typhoon

[19] **SolarWinds.** *What Is a Windows Event Log?*. SolarWinds IT Glossary. Retrieved December 4, 2024 from https://www.solarwinds.com/resources/it-glossary/windows-event-log

[20] **Greig, J. and Matishak, M.** 2024. *Any number given of Volt Typhoon victims 'likely an underestimate,' CISA says*. The Record. Retrieved December 4, 2024 from https://therecord.media/volt-typhoon-targets-underestimated-cisa-says