Threat Intelligence Brief: PRC Cyber Threats and Volt Typhoon Operations Targeting American Infrastructure

Cyber threats from the People's Republic of China (PRC) remain an active threat to American businesses and infrastructure. Specifically, Volt Typhoon poses a consistent threat to small-to-medium size business service providers and vendors further affecting their ability to provide essential services (i.e. water, energy, and aviation). Compromising such businesses serves as a direct downstream effect on the general public. Preventing issues at this level is critical to ensuring secure business transactions, trust in customers and the public as well as national security risk.

Diamond model:

1. Adversary - Volt Typhoon (Chinese sponsored actor)
2. Capability - living off the land (LOTL) techniques, exploitation of known vulnerabilities, stolen credentials and valid account theft
3. Victim - American Infrastructure sectors and small businesses (water, energy, aviation, and etc.)
4. Infrastructure - reliant on network edge devices (compromised VPNs, routers, firewalls), remote access tools, and obfuscate their malware

MITRE ATT&CK Mapping

- Initial access (T1190): expose weakness in internet-facing host (firewalls, routers, VPN)
- Execution (T1059): command-line abuse utilizing Windows capabilities and scripting for implementation
- Persistence (T1078): using valid accounts to gain access for remote systems or external services like VPN and other network devices
- Defense (T1562): disable defensive mechanisms such as auditing and firewalls

Impact

The Volt Typhoon group showcases the ability to obstruct American infrastructure networks with long-term, furtive access. Through its use of stolen credentials, compromised VPNs and obfuscated malware, the group was seemingly unbeknownst while continued unruly mechanisms were implemented. Their mechanisms of initial access network edge devices creates established relations with internal infrastructure that poses serious concern to national security, trust from the public and continuity of business operations.

Recommendations

1. Monitor valid accounts - Regularly auditing behavior of users and access will validate legitimate usage

2. Secure edge devices - continually monitoring and hardening connections of network edge devices will ensure safety
3. Implement Authentication - Utilizing Multi-Factor Authentication (MFA) for all remote access and privileged accounts
4. Secure Vulnerabilities - Patching internet facing devices like firewalls or VPNs for known vulnerabilities will sharpen vulnerability management

Sources

- CISA. *Under the Digital Radar: Defending Against the People's Republic of China's Nation-State Cyber Threats to America's Small Businesses*. https://www.cisa.gov/news-events/news/under-digital-radar-defending-against-peoples-republic-chinas-nation-state-cyber-threats-americas
- CISA. *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection*. Advisory AA24-038A. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a