K logix

BE CONFIDENT.

MARCH 2024 | THREAT INTEL NEWSLETTER

VPN Vulnerabilities: Ivanti and Fortinet

C-Suite level threat review by applicable business area addressing active threats.

Two widely used VPN appliances, Ivanti and Fortinet, recently disclosed several zero-day vulnerabilities, quickly catching the attention of federal agencies, cybersecurity personnel and threat actors. VPN vulnerabilities present an opportunity for threat actors to access sensitive parts of an organization. Moreover, these supply chain vulnerabilities enable adversaries to automate targeting multiple victims, compounding opportunities for financial gain and intelligence acquisition.

Ivanti Zero-Day Vulnerabilities:

In the span of a month, five (5) high and critical zero-day vulnerabilities surfaced with Ivanti Connect Secure (9.x, 22.x), Ivanti Policy Secure (9.x, 22.x) and ZTA gateways. The five vulnerabilities are CVE-2023-46805, CVE-2024-21887, CVE-2024-21893, CVE-2024-21888, and CVE-2024-22024. The vulnerabilities enable a threat actor to gain unauthenticated access to its target and elevate privileges. Many threat actors are currently exploiting these vulnerabilities. Notably, UTA0178 / UNC5221, a Chinese Advanced Persistent Threat (APT) actor, is thought to be one of them.

Fortinet Zero-Day Vulnerabilities:

Fortinet, a developer of security solutions, disclosed four (4) vulnerabilities affecting its VPN solution back in February. The four vulnerabilities are CVE-2024-21762, CVE-2024-23113, CVE-2023-44487, and CVE-2023-47537. Fortinet solutions are prevalent among government institutions and critical infrastructure which makes them a target, particularly among Chinese-backed APT groups.

UTA0178 / UNC5221

Threat Level: High

Attack:

Once UTA0178 gains access to its target's environment via the Ivanti vulnerabilities (MITRE T1190), threat analysts have observed the deployment of several different types of malwares to assist with compromise. One of which is a web shell tracked as BUSHWALK (MITRE T1505.003) that is able to execute arbitrary commands or write files to a server. Another is ZIPLINE which is used to communicate with the C2 server. This adversary also utilizes techniques to hinder forensic analysis and incident response. One such example is tampering with Ivanti's internal Integrity Checker Tool (ICT), which keeps a list of expected files on the system. UTA0178 may modify this list to prevent identification of new or mismatched files (MITRE T1070). Another evasion technique is clearing system logs (MITRE T1070). This adversary steals information from compromised environments for espionage.

Remediation:

- Patch Ivanti vulnerabilities. CISA provides mitigation recommendations for federal agencies under its jurisdiction in its emergency directive.
- Run the Ivanti external Integrity Checker Tool to identify signs of compromise.
- Investigate replacing legacy VPN models with a zero-trust network architecture (ZTNA).

Volt Typhoon

Threat Level: High

Attack:

Volt Typhoon is a Chinese APT actor that is known to utilize zero-day vulnerabilities in public-facing appliances, such as the ones discussed in this report, to gain initial access into a victim's network (MITRE T1190). Before gaining entry, this threat actor conducts extensive reconnaissance on its targets which includes gathering information on the organization, such as its network, business structure and people (MITRE T1590, T1591,T1593, and T1589). Once inside, Volt Typhoon tends to utilize living off the land techniques for execution, defense evasion and exploration. Such techniques include utilizing the command line (MITRE T1059), incorporating trusted binaries (MITRE T1218) and performing software packing (MITRE T1027.002). Volt Typhoon is politically motivated, exfiltrating information that can support crippling critical infrastructure in a conflict scenario with China.

Remediation:

- Patch Fortinet vulnerabilities.
- Ensure your organization has a comprehensive third-party risk program in place.
- Validate your security controls against common threat behaviors utilized by adversaries.

UTA0178 / UNC5221:

- **Overview of this threat actor's post-exploitation activity:** https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day
- **Additional insight into this threat actor's post-exploitation activity:** https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation

Volt Typhoon:

- **The Five Eyes released a joint advisory about Volt Typhoon:** https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
- **Volt Typhoon threat activity:** https://www.bleepingcomputer.com/news/security/chinese-hackers-hid-in-us-infrastructure-network-for-5-years/

How K logix Can Help

- Technology Advisory
  - Email Security
  - Endpoint Detection and Protection (EDR)
  - Identity and Access Management (IAM)
  - Managed Security Service Provider (MSSP)
  - Security Information and Event Management (SIEM)
  - Cloud Security Posture Management (CSPM)
  - SaaS Security Posture Management (SaaS)
- Programmatic Advisory
  - Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
  - Cloud Security Maturity
  - Identity and Access Management Program Maturity
- Threat Intelligence
  - Notification to customers of threats
  - On-demand briefings
  - Threat exposure workshops
  - User awareness training seminars
  - Monthly and quarterly threat intelligence reports

Volt Typhoon Example Attack Sequence

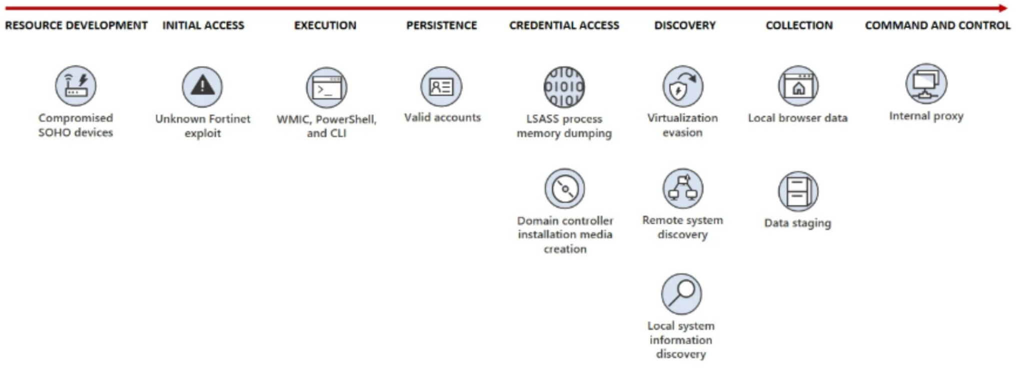

Figure 1. Volt Typhoon attack diagram

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

ABOUT K LOGIX

Cybersecurity Advisory and Consulting Services

Our white-glove approach empowers leaders to advance their security programs to strategically align with the business to reduce risk.