K logix
Be confident.

AUGUST 2024 | THREAT INTEL NEWSLETTER

Chinese Advanced Persistent Threat (APT) Actors: APT40 and Volt Typhoon

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

The People's Republic of China (PCR) is linked to sophisticated threat actors such as APT40 and Volt Typhoon, the two APTs outlined in this report. According to the 2024 Threat Assessment Report from the Office of the Director of National Intelligence "China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks." Thus, it is important for organizations to test their defenses against the tactics and techniques employed by Chinese APT groups.

APT40:

APT40 is a politically motivated threat actor; its actions align with the interests of the PCR. APT40 targets both private and public organizations predominantly in the following industries: defense, maritime, consulting, high-tech, healthcare, media, and publishing. As a highly sophisticated threat actor, APT40 can exploit newly identified vulnerabilities within hours and days of public release.

Volt Typhoon:

Volt Typhoon, also known as UNC3236 and Bronze Silhouette, is a state-sponsored threat actor from China. This threat group targets critical infrastructure sectors such as telecommunications, energy, transportation, and water/wastewater. Volt Typhoon's activity indicates it is positioning itself to disrupt critical functions in the case of a conflict between China and one of its target countries which includes, but is not limited to, the United States (US), Australia, Canada, New Zealand, and United Kingdom (UK).

APT40

Threat Level: High

Attack:

For initial access, APT40 prefers to exploit vulnerabilities in public-facing infrastructure (MITRE T1190). This threat actor then seeks to maintain its foothold in its target environment by deploying web shells (MITRE T1505.003) and obtaining valid credentials (MITRE T1078) for persistence. APT40 may then utilize valid accounts to interact with remote services and move laterally on the victim's network (MITRE T1021.002). To blend in with legitimate traffic, APT40 leverages compromised small-office / home-office (SOHO) devices to orchestrate its malicious activity and communicate with its victim's environment (MITRE T1584.008). It further obfuscates its malicious activity by clearing event logs (MITRE T1070.001). The objective of this threat actor's malicious activity is espionage; much of its action concentrates on uncovering and extracting sensitive information. This threat actor has been observed employing numerous exfiltration techniques including MITRE T1041, T1048, and T1567.002.

Remediation:

- Establish a network segmentation strategy to hinder lateral movement.
- Keep internet-exposed devices and services patched and up to date.
- Perform penetration testing to validate the strength of your organization's cyber defense strategy.

Volt Typhoon

Threat Level: High

Attack:

Before compromise, Volt Typhoon conducts extensive reconnaissance on its target environments. This includes gathering information on key personnel, user behavior and its victim's network architecture (MITRE T1589 and T1590). When ready to infiltrate a network, Volt Typhoon commonly gains initial access by exploiting vulnerabilities in network appliances (MITRE T1190). Once inside, Volt Typhoon focuses on establishing persistence. In a breach of a US Water and Wastewater system, Volt Typhoon utilized compromised admin credentials to establish persistence via VPN and RDP sessions (MITRE T1133). This threat actor then spent over nine (9) months hidden in its victim's environment, gathering data such as domain credentials and other pertinent information (MITRE T1078.002). In its attacks, Volt Typhoon favors living-off-the-land (LOTL) techniques for defense evasion. Similar to APT40, Volt Typhoon compromises SOHO devices with malware, creating a botnet (MITRE T1584.005). Volt Typhoon then utilizes the compromised devices to disguise its malicious activity.

Remediation:

- Review VPN logins for duration, frequency, and location to discover any abnormalities.
- Ensure your organization has end-of-life support for systems which may include isolation, configuration changes, and additional scanning.
- Implement the security principle of least privilege when utilizing remote desktop services.

APT40:

- **Examines the tactics and techniques employed by APT40 in two previous attacks:** https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/apt40-advisory-prc-mss-tradecraft-in-action
- **Details recent APT40 activity:** https://www.bleepingcomputer.com/news/security/chinese-apt40-hackers-hijack-soho-routers-to-launch-attacks/

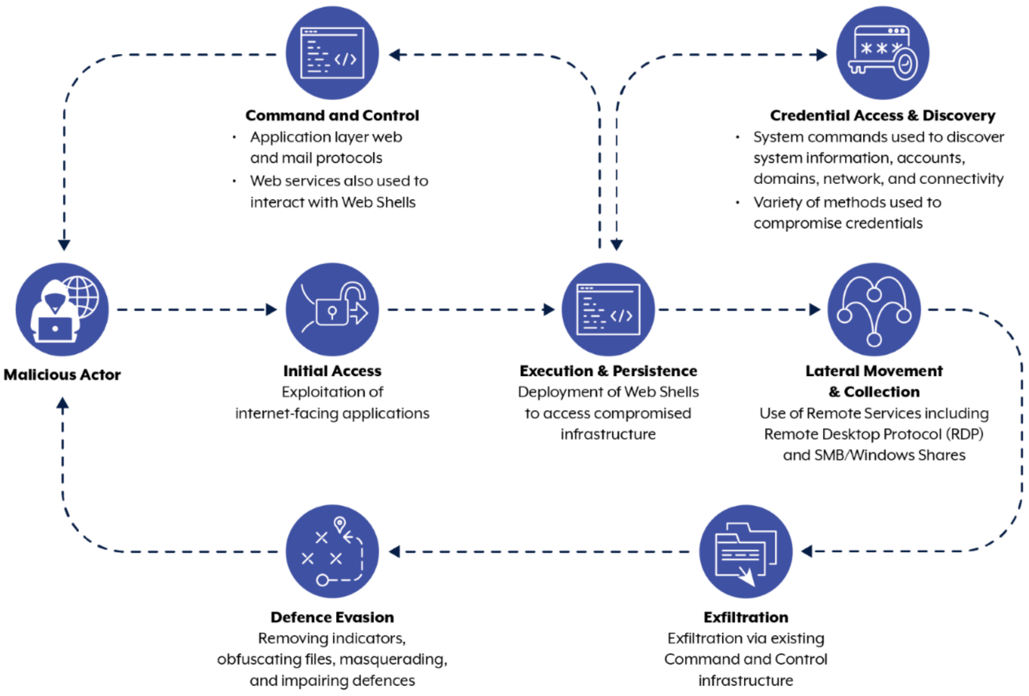
Volt Typhoon:

- **Technical Review of Volt Typhoon:** https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
- **Overview of the U.S. disrupting Volt Typhoons KV Botnet:** https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical

How K logix Can Help

- Technology Advisory
  - Email Security
  - Endpoint Detection and Response (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

APT40 Attack Sequence



Command and Control
- Application layer web and mail protocols
- Web services also used to interact with Web Shells

Credential Access & Discovery
- System commands used to discover system information, accounts, domains, network, and connectivity
- Variety of methods used to compromise credentials

Malicious Actor

Initial Access
Exploitation of internet-facing applications

Execution & Persistence
Deployment of Web Shells to access compromised infrastructure

Lateral Movement & Collection
Use of Remote Services including Remote Desktop Protocol (RDP) and SMB/Windows Shares

Defence Evasion
Removing indicators, obfuscating files, masquerading, and impairing defences

Exfiltration
Exfiltration via existing Command and Control infrastructure

Source: https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/apt40-advisory-prc-mss-tradecraft-in-action

ABOUT K LOGIX

Cybersecurity Advisory and Consulting Services

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