China-linked Threats to Operational Technology

⋮ 3/21/2024

Table of contents

Key Points

- This report examines the threat posed by Chinese advanced persistent threat (APT) groups on operational technology (OT) by analyzing four key cyber attacks from the past 12 months conducted by threat actors with a China nexus (“APT27,” “APT31,” “BlackTech,” and “Volt Typhoon”). Network defenders may find the detection rules and key recommendations detailed throughout this report useful.
- Recommended mitigations against the tactics, techniques, and procedures (TTPs) involved in these attacks include preventing execution of processes created remotely through WMI/PSExec in Windows Defender and implementing tighter access control to critical assets that require Remote Desktop Protocol (RDP).
- We expect that Chinese APT activity will almost certainly retain its distinct qualities—such as frequent zero-day exploitations and sophisticated social-engineering tactics—over the next year.
- Chinese threat actors are also likely to target OT and network devices more during this period to exfiltrate valuable information and disrupt critical infrastructure.

In keeping with the other Threat Spotlight Reports in our series on operational technology (OT), this report examines the threat posed by Chinese APT groups to OT. We analyze four key Chinese cyber attacks with an OT element—targeting companies that are major users of OT or using TTPs that align with the MITRE Industrial Control Systems (ICS) Matrix—from the past 12 months. We review the common TTPs used in these cyber incidents and provide key detection and mitigation advice. This report will be particularly useful for organizations that have, or that are planning to incorporate, OT in their infrastructure.

Introduction

China's strategic interests—the "Belt and Road" and "Made in China 2025" initiatives—along with strained geopolitical relations on multiple fronts (including South China Sea territorial disputes, Taiwan's sovereignty, and repeated clashes with the US) have escalated its need for information. The ability to access, control, manipulate, and destroy information will provide Beijing with a significant advantage, growing commercial success for Chinese companies, and—in the event of war—informing its military strategies.

APT groups have become essential to the Chinese Communist Party (CCP)'s extensive cyber campaigns. While some of these threat groups conduct a mix of financially and politically motivated attacks, many of them primarily carry out cyber espionage and intelligence-gathering operations at the behest of Chinese security bureaus. ReliaQuest recently published a report on the Chinese hacking ecosystem that shows the business relationship between Chinese APT groups and private security contractors.

The following incidents are indicative of how China is relying on APT groups to disrupt OT environments. One of the objectives of such operations is likely to, in the event of conflict with the US or US allies, possibly disrupt or damage critical infrastructure to slow down the US' military and political responses.

Key OT Cyber Incidents

In the past 12 months, Chinese threat groups including APT27, APT31, BlackTech, and Volt Typhoon have targeted organizations that use OT. Below, we take a closer look at each incident.

Volt Typhoon Targets US Critical Infrastructure with Botnet

In January 2024, the US government disclosed that it had disrupted the botnet that the Volt Typhoon group used to conceal the origin of its activities, which included the targeting of critical infrastructure organizations in the US and other countries. The botnet mainly consisted of Cisco and NetGear routers that had reached their end-of-life status, which meant they were no longer receiving security patches or updates from the manufacturers. Volt Typhoon used multi-hop proxies—typically composed of virtual private servers (VPSs) or small office/home office (SOHO) routers—for command-and-control (C2) infrastructure. US security agencies asserted with high confidence that Volt Typhoon was pre-positioning itself on critical IT networks, with the aim of disrupting OT functions across various sectors.

PT27 Leverages ChargeWeapon Backdoor in OT Targeting

In October 2023, APT27 targeted semiconductor companies in Hong Kong, Singapore, and Taiwan in a cyber-espionage campaign, impersonating the Taiwan Semiconductor Manufacturing Company to deliver Cobalt Strike beacons. The threat group leveraged the "HyperBro" loader and a new malware downloader to deliver additional malware. A compromised Cobra DocGuard web server was also used to host second-stage binaries, including a Go-based backdoor, "ChargeWeapon." ChargeWeapon is typically used to get remote access and send device and network information from a compromised host to APT27's C2 server.

BlackTech Maintains Persistence via Router Backdoors

In September 2023, US and Japanese authorities warned that BlackTech was modifying branch router firmware without detection to pivot from certain organizations' international subsidiaries to their corresponding headquarters in Japan and the US. BlackTech targeted several sectors that heavily depend on OT, including

wholesale trade; information; and professional, scientific, and technical services. BlackTech attacks typically begin with spearphishing emails that contain backdoor-laden attachments that deploy malware to harvest sensitive data.

APT31 Uses Multiple Backdoors in Attacks on Air-Gapped Systems

In August 2023, cybersecurity researchers reported that APT31 had compromised numerous industrial organizations in Eastern Europe to siphon data from air-gapped systems in 2022. The threat group used multiple malware variants to establish persistent remote access and gather sensitive information, which they then sent to infrastructure controlled by the group. Its toolkit included the "FourteenHi" malware family and the first-stage backdoor "MeatBall." APT31 used Yandex Cloud for C2.

Common TTPs

The Volt Typhoon attack stands out from the other three incidents—it was the only attack whose goal was specifically to disrupt OT systems. During the attack, Volt Typhoon attempted to gain access to OT assets by using default OT vendor credentials (T0812). Some credentials—those previously compromised via NTDS.dit theft (T0859) —proved fruitful. Once the group gained access, it had multiple options for disruption: it could have manipulated heating, ventilation, and air conditioning (HVAC) systems in server rooms (T0831, T0847); disabled critical energy and water controls (T0880); and accessed camera surveillance systems at OT facilities. Because its botnet was taken down, it's unclear what its specific action plan was. It is clear, though, that the ability to impact these sectors would provide China with a significant opportunity.

The other three incidents also had an OT element, but were primarily conducted for espionage—their use of multiple backdoors throughout the different stages of the attacks indicated that data exfiltration was key.

Despite their differences, all four attacks had TTPs in common. Below, we'll show how these TTPs were used in each case study and provide recommendations for each.

Remote Services: Remote Desktop Protocol (T1021.001)

Examples

- Volt Typhoon has been known to move laterally to the domain controller (DC) via an interactive Remote Desktop Protocol (RDP) session using a compromised account with domain administrator privileges.
- BlackTech has used RDP to move laterally across a compromised entity's network.

Recommendations

- Disable remote interactive logon of service accounts to prevent them from being used for RDP.
- Configure and enable multifactor authentication (MFA) for RDP sessions, helping to prevent lateral RDP and RDP brute-forcing.
- Adhere to the principle of least privilege and minimize RDP to only the required accounts.
- Configure access to critical assets that require RDP to use designated jump boxes, allowing tighter access control and improved auditing.

Exploit Public-Facing Application (T1190)

Examples

- Volt Typhoon commonly exploits vulnerabilities in networking appliances such as Fortinet, Ivanti, NETGEAR, Citrix, and Cisco.
- APT27 has historically used a malware downloader to fetch malicious binaries from a compromised Cobra DocGuard server.

Recommendations

- Utilize security tools, such as a web application firewall (WAF), to protect public-facing applications and provide logging visibility into access and requests to and from the application.
- Properly segment all public-facing applications from the intranet to minimize risk of exploitation compromising sensitive infrastructure.
- Adhere to a robust and frequent vulnerability assessment and patching cycle for all public-facing appliances.
- Develop an emergency patch and mitigation plan to be used for widespread zero-day exploitation.

Ingress Tool Transfer (T1105)

Examples

- Volt Typhoon uses legitimate but outdated versions of network admin tools. For example, in one confirmed compromise, the threat group downloaded an outdated version of comsvcs.dll on the DC in a nonstandard folder.
- APT27 uses a malware downloader to download more malware, such as ChargeWeapon, onto the compromised host.

Recommendations

- Utilize application control solutions to help prevent threat actors from attempting to evade defenses. This can be achieved by using less-common methods of resource retrieval, such as via “certutil.”
- Maintain an up-to-date block list of known hosting sites and actively monitor outbound request attempts through your forward proxy.
- If an endpoint detection and response (EDR) solution is not available, leverage Sysmon Event ID 3 to log and monitor process executions generating network connections.

Command and Scripting Interpreter: PowerShell (T1059.001)

Examples

- Volt Typhoon has implanted the FRP clients with filename SMSvcService.exe on a Shortel Enterprise Contact Center (ECC) server, and a second FRP client with filename Brightmetricagent.exe on another server. These clients, when executed via PowerShell, open reverse proxies between the compromised system and Volt Typhoon C2 servers.
- APT27 uses base64-encoded PowerShell to download malware artifacts and drops them under c:\programdata of the compromised device.

Recommendations

- Leverage application control solutions to explicitly allow a list of expected PowerShell scripts or applications that should be executing PowerShell.

- If utilizing Windows Defender, enable the Attack Surface Reduction (ASR) rule “Block Execution of Potentially Obfuscated Scripts” to help prevent execution of obfuscated PowerShell payloads.
- While not applicable for many organizations, consider disabling remote PowerShell via the WinRM (Windows Remote Management) service to prevent lateral PowerShell execution.
- If utilizing Windows Defender, enable the ASR rule “Block process creations originating from PSExec and WMI commands” to help prevent execution of processes created remotely through Windows Management Instrumentation (WMI) or PSExec.

Window Management Instrumentation (T1047)

Examples

- Volt Typhoon has used Windows Management Instrumentation Console (WMIC) commands to execute ntdsutil to copy NTDS.dit and SYSTEM registry hive from the volume shadow copy.
- APT27 uses ChargeWeapon, which has WMI execution capabilities, to collect information (hostname, IP address, and process tree) from compromised hosts to identify high-value targets.

Recommendations

- Implement the principle of least privilege by configuring the WMI namespace security to allow access only to the necessary users and groups.
- Consider enabling WMI auditing through Group Policy Object (GPO) to provide visibility into WMI access and usage events, as this activity is often not logged or monitored. Please note that WMI logging can be high volume.
- If utilizing Windows Defender, enable the ASR rule “Block process creations originating from PSExec and WMI commands” to help prevent execution of processes created remotely through WMI.

Gather Victim Host Information (T1592)

Examples

- Volt Typhoon conducts extensive pre-compromise reconnaissance. This includes web searches, including searches of sites owned by the compromised user or organization, to gather host, identity, and network information, especially for information on key network and IT administrators.
- APT27 used the ChargeWeapon backdoor to send host and network information from the compromised host to its C2 server.

Recommendations

- Conduct frequent scanning and audits of public-facing infrastructure, including validation of any networking devices after configuration or rule changes, to assess service exposures or exposed information useful for profiling.
- Minimize information exposed through job listings, such as for network engineers or developers, that might expose what technologies are being used internally or behind public-facing applications.

Masquerading: Match Legitimate Name or Location (T1036.005)

Examples

- Volt Typhoon has selected cleared Windows Event Logs, system logs, and other technical artifacts to remove evidence of their intrusion activity and masquerading file names.
- APT27 used a Malleable C2 profile to disguise itself as jQuery CDN to evade traditional firewall

Recommendations

- Leverage application control solutions to create path-based rules to prevent execution of files from non-standard paths and folders such as “Downloads,” “Music,” “Public,” or “debug.”
- Leverage application control solutions to create policies for allowed execution of commonly abused binaries and scripts based off hash and location to prevent Bring Your Own Vulnerable Driver (BYOVD) attacks.
- Utilize file integrity monitoring solutions for critical systems to alert and protect against unauthorized changes to specific directories or commonly abused binaries and scripts.

Deobfuscate/Decode Files or Information (T1140)

Examples

- APT31 uses RC4 key to decrypt the malware configuration, as well as to protect communication.
- APT27 has used a one-byte-length key (0x01) to decrypt an XOR-encrypted Cobalt Strike payload to evade signature-based malware detection.

Recommendations

- If utilizing Windows Defender, enable the (ASR rule “Block Execution of Potentially Obfuscated Scripts” to help prevent execution of obfuscated PowerShell payloads.

Threat Forecast

Collaborations between Chinese APT groups have resulted in frequent overlapping of TTPs and toolsets, making attributing Chinese APT activity challenging. This longstanding cooperation (e.g., pooled resources) is almost certainly going to continue, with cyber operations remaining aligned with the CCP’s broader strategic interests. Chinese APT activity will almost certainly retain its distinct qualities: frequent zero-day exploitations, scrupulous attention to maintaining persistence and remaining undetected, and sophisticated social engineering tactics.

As geopolitical events concerning China continue to develop around the world, Chinese threat actors are likely to increasingly turn to targeting OT devices and network to exfiltrate valuable information and potentially to cause disruption or gain control of a country’s critical infrastructures in the long-term future. OT assets are highly likely to continue to lag in security patching, providing cyber perpetrators an extended window of opportunity for exploitation.

The ReliaQuest Threat Research team will continue to monitor these groups and their TTPs, providing detections to our customers and recommendations to the broader public to protect against the associated threats.