INTEL471

SAMPLE REPORT

CYBER GEOPOLITICAL INTELLIGENCE FINDINGS:

China Escalates Cyberattacks on Critical Infrastructure Amid Geopolitical Conflicts

Executive Summary

Intel 471 is a leading provider of cyber threat intelligence solutions. We've now extended this expertise to include a new Cyber Geopolitical Intelligence reporting offering that allows customers to make risk assessments, analyses, and forecasts for developing or emerging situations based on the geopolitics, foreign affairs and related cyber threats. This new curated intelligence and reporting provides customers with insights on key players and regions and their political, economic, and security situations.

The growing convergence of e-crime, nation state, and geopolitical events is an important yet difficult problem to understand. With these reports, we shine a light on the intersection of these events for our customers. Merging our current capabilities in human-led analysis of cybercrime with experts in geopolitical intelligence, Intel 471 brings a thoughtful approach for analysts that addresses key intelligence gaps through easily consumed Spot Reports, Intelligence Bulletins, Intelligence Summaries, and Threat Briefs.

The following report is an example of our Cyber Geopolitical Intelligence output, and details how we help empower the customer to develop proactive strategies to protect and mitigate against the cyber threats that have become part of the arsenal in geopolitical conflicts.

China Escalates Cyberattacks on Critical Infrastructure amid Geopolitical Conflicts

Summary

Governments worldwide have called for increased vigilance and tightened security to mitigate Chinese cyber threats targeting critical infrastructure in recent years. This report presents case studies on two Chinese state-linked threats — **APT31** and **Volt Typhoon** — and analyzes their recent cyber operations against vital sectors.

Key findings

- The **APT31** group primarily conducts attacks to exfiltrate valuable information and occasionally targets high-profile organizations to assert China's cyber power.
- The **Volt Typhoon** group prioritizes secrecy and often retargets the same entities over the years to ensure the group maintains access to their information technology (IT) networks with the aim of causing damage at an opportune time such as military clashes.
- Understanding how global geopolitical developments trigger Chinese state-affiliated cyber threat activity can help cybersecurity practitioners anticipate and defend against it.

Introduction

In April 2024, a key member of the U.S. Indo-Pacific Command cautioned the Chinese Communist Party (CCP) is building capacity to invade Taiwan by 2027 to mark the centennial founding of the People's Liberation Army (PLA). The PLA's modernization also is expected to be complete that year following years of heavy defense investments. Several top U.S. military officers made similar predictions in recent years, although the forecast attack schedule ranges from 2024 to 2027.[1]

In spite of the murky timeline, it is clear China is accelerating its targeting of critical infrastructures abroad, especially in the U.S. Beijing's offensive cyber operations against vital sectors are "both broad and unrelenting" as it pre-positions itself on IT networks for disruptive or destructive cyberattacks.[2]

Why US is Key Target

Ahead of the U.S. presidential elections in November 2024, U.S. politicians increasingly are arousing anti-China sentiments, calling for enhanced restrictions related to the export of U.S. cutting-edge and emerging technologies, among other things. Sensing a closing window of exploitation, the CCP is trying to seize economic growth under the wire by pilfering American trade secrets before security and trade measures are imposed.

Additionally, China is poised to become the aggressor regarding several flashpoint issues in Asia, including its territorial claims in the South China Sea and reunification with Taiwan. The U.S. has committed to coming to the defense of the Philippines and Taiwan if they were attacked. Crippling U.S. critical infrastructure almost certainly will guarantee widespread panic within the country, serving as a distraction to delay U.S. aid from reaching its allies and partners in the Indo-Pacific.

The following two case studies examine past campaigns of **APT31** and **Volt Typhoon**.

Case Study 1: APT31

Target Regions, Sectors

On March 25, 2024, the U.K. and the U.S. sanctioned Wuhan Xiaoruizhi Science and Technology Co. (Wuhan XRZ) for numerous malicious cyber campaigns that endangered their respective national securities. Seven Chinese nationals were indicted on charges stemming from their involvement in the company. Wuhan XRZ was established in Wuhan, China, in 2010 and is a Ministry of State Security (MSS) front company linked with **APT31**.[3]

The **APT31** group is a collection of Chinese intelligence officers, private information security contractors and administrative staff that carry out cyberattacks on behalf of the Hubei State Security Department. It primarily targets the U.S. but targets also have been reported in Southeast Asia, Hong Kong, Europe and the U.K.

The cyber threat group targeted the defense industrial base, IT, health care and energy sectors in the U.S. since 2017 and successfully compromised:

- A defense contractor that manufactured flight simulators for the U.S. military.
- A Tennessee-based aerospace and defense contractor.
- An Alabama-based aerospace and defense research corporation.
- A Texas-based energy company.

- A California-based managed service provider (MSP).
- Numerous machine learning (ML) laboratories.
- Multiple health care and medical research facilities.

Operations Targeting Critical Resources

In August 2023, cybersecurity researchers reported **APT31** has targeted industrial organizations in eastern Europe since at least April 2022 to steal data from air-gapped systems. The threat group used at least 15 distinct implants in each stage of the operations, as well as its signature FourteenHi malware family.[4]

The group's attacks often were timed to coincide with periods of heightened geopolitical tensions between China and the U.S. After the U.S. imposed trade tariffs on China steel imports, China's Ministry of Commerce promised a "major response." A day later, **APT31** started to register infrastructure that impersonated American Steel Co. and the International Steel Trade Forum to use as command-and-control (C2) servers to deploy malware in American Steel's network.

When Hong Kong pro-democracy activists were nominated for the Nobel Peace Prize, **APT31** targeted the Norwegian government and a major Norwegian MSP. The cyber threat group acquired administrator rights that gave it full access to centralized computer systems used by nationwide state administration offices.[5] In 2020, a top U.S. Department of State official called China's broad maritime claims in the South China Sea "completely unlawful," prompting a retaliatory spear-phishing campaign against the U.S. navy and related think tanks.

Case Study 2: Volt Typhoon

Target Regions, Sectors

The **Volt Typhoon** aka **Vanguard Panda**, **Bronze Silhouette**, **Dev-0391**, **UNC3236**, **Voltzite**, **Insidious Taurus** group first was discovered in mid-2021 and is a Chinese nation-state group that primarily targets the U.S. — particularly the manufacturing, utility, transportation, construction, maritime, government, IT and education industries. The media brought wider attention to the group's activity in May 2023 when Microsoft revealed its campaign against vital sectors in Guam and across the U.S. Apart from typical espionage, **Volt Typhoon** was pre-positioning itself on critical infrastructure networks with the intent to disrupt or destroy at Beijing's command.[6]

From July 2023 to August 2023, **Voltzite**, an alleged operation technology (OT)-focused unit within **Volt Typhoon**, targeted electric transmission and distribution providers in Africa by compromising industrial control systems (ICSs) and using tactics, techniques and procedures (TTPs) similar to its U.S. campaigns.[7]

Exploiting Operational Technology Security Flaws

Since 2021, **Volt Typhoon's** targets and patterns of behavior have strayed from traditional cyber espionage and intelligence gathering operations. The threat group focuses on gaining access to IT networks that will enable lateral movement to OT assets. OT underpins the operations of every critical infrastructure sector, but despite its importance, these systems are notoriously difficult to patch due to stability, accessibility and cost considerations. OT also has a decades-long lifecycle so it often lacks what would be considered as standard security features today such as encryption, which likely was not a priority at the time of build.

Operations Targeting Critical Resources

Common TTPs in **Volt Typhoon's** cyber operations that target critical infrastructure include conducting extensive pre-exploitation reconnaissance and tailoring tactics to the target environment, dedicating ongoing resources to maintain persistence — as long as five years in some cases. The group frequently tests access to domain-joined OT assets by using default OT vendor credentials or compromised credentials in some instances. The group also targets the same entities repeatedly over extended periods to validate and enhance its unauthorized access.

The group uses an array of techniques to ensure its concealment, which include:

- Avoids leaving malware artifacts that would trigger security alerts.
- Deletes logs in a targeted manner.
- Uses living-off-the-land (LOTL) techniques.
- Leverages a botnet of small office-home office (SOHO) routers as intermediate infrastructure to obscure its activity by having C2 traffic emanate from local internet service providers (ISPs) in the target's geographic area.
- Avoids exfiltrating substantial amounts of data. Instead, it typically steals OT-specific data such as supervisory control and data acquisition (SCADA)-related information and geographic information system (GIS) information that could be stored for future disruptive attacks.[8]

Gaining access to these assets gives **Volt Typhoon** the power to:

- Manipulate heating, ventilation and air conditioning systems in secured areas such as server rooms.
- Disrupt critical energy and water controls.
- Access and manipulate camera surveillance systems at critical infrastructure facilities.
- Move laterally to other control systems.

Assessment

The two case studies demonstrate how Chinese cyber threat groups with a political agenda can use network access for disruptive effects in the face of geopolitical tensions or military conflicts.

Objectives

The objective of **APT31's** attacks varies but includes stealing diplomatic intelligence and appropriate trade secrets or exfiltrating sensitive information of critical infrastructure personnel. On the other hand, **Volt Typhoon** often exhibits only minimal activity within the compromised environments and stays quietly burrowed deep within target networks for years.

Where **APT31** conducts high-profile proactive and reactive cyberattacks, such as theft or retaliating against anti-CCP entities, respectively, **Volt Typhoon** demonstrates deliberate, long-term cultivation of strategic entryways into foreign countries' most critical sectors that are stored for future use in the event the CCP's interests are threatened.

Targeting

The **APT31** group appears to be more inclined to abruptly pivot targets — from defense agencies to financial organizations — in response to global geopolitical fluctuations. These targets have included organizations outside critical infrastructure sectors and commonly are highly visible entities in the target country. In comparison, **Volt Typhoon** focuses on breaching entities of various sizes in specific industry verticals, such as utilities, that serve the horizontal market.

The **Volt Typhoon** group targeted small and medium-sized enterprises that provide critical services to large companies and key geographic locations. By compromising

vulnerable, smaller third-party vendors with limited cybersecurity capabilities, the threat group can exploit their trusted relationships to gain a foothold in larger partner organizations with robust security practices that otherwise would have been too onerous for **Volt Typhoon** to overcome. This modus operandi will enable **Volt Typhoon** to conduct supply chain attacks without a physical overseas presence.

Tactics, Techniques, Procedures

The **APT31** group exhibits typical Chinese state-sponsored cyber threat behavior that includes spear-phishing, vulnerability exploitation and the use of custom and off-the-shelf malware and tools. The **Volt Typhoon** group uses hands-on-keyboard, LOTL techniques and botnets to customize and masquerade its presence on breached networks, opting for long-term rather than immediate political gains.

By gauging the CCP's response toward an event, statement or measure, security teams can anticipate incoming waves of Chinese politically and ideologically motivated cyberattacks. Any move perceived to threaten the CCP regime highly likely will trigger a cyber response against foreign entities linked with the issue.

Detection Strategies

Threat Hunting

Proactively hunt for **APT31** behavior and identifiers with custom hunt packs via Cyborg's Hunter platform.

HUNT PACKAGE	LINK
Autorun or ASEP Registry Key Modification	https://hunter.cyborgsecurity.io/research/hunt-package/8289e2ad-bc74-4ae3-bfaa-cdeb4335135c
Scheduled Task Created	https://hunter.cyborgsecurity.io/research/hunt-package/aaa77f56-4a4c-4fdd-a6e3-156e1996d310
File Created in Startup Folder	https://hunter.cyborgsecurity.io/research/hunt-package/8fedb48c-396b-4cd5-9483-69d7fc3eecee
Common Abused Executables Launched Outside of System32	https://hunter.cyborgsecurity.io/research/hunt-package/50641742-9446-4418-a0fa-9ac0fdb9d7dc

HUNT PACKAGE	LINK
Excessive Windows Discovery CommandLine Arguments — Potential Malware Installation	https://hunter.cyborgsecurity.io /research / hunt-package /8bb5819f -06a4 -4e5d -9099 - e43115601999

Proactively hunt for **Volt Typhoon** behavior and identifiers with custom hunt packs via Cyborg's Hunter platform.

HUNT PACKAGE	LINK
Netsh Port Forwarding Command	https://hunter.cyborgsecurity.io/research/hunt-package/0eca36b6-57ef-42b2-bf74-6d0b7dd12aa1
Powershell Encoded Command Execution	https://hunter.cyborgsecurity.io/research/hunt-package/d2d3bbc2-6e57-4043-ab24-988a6a6c88db
Remote Process Instantiation via WMI	https://hunter.cyborgsecurity.io/research/hunt-package/dd0ca1e2-046f-4878-b7f8-32b790420ef2
Dump Active Directory Database with NTDSUtil — Potential Credential Dumping	https://hunter.cyborgsecurity.io/research/hunt-package/98846e7f-c90c-4156-8643-54a613286b66
WMIC Windows Internal Discovery and Enumeration	https://hunter.cyborgsecurity.io/research/hunt-package/bc0fd59c-4217-46a7-a167-764727118567
Potential Impacket wmiexec Module Command Execution	https://hunter.cyborgsecurity.io/research/hunt-package/5b4c793a-260a-4d43-bbc7-ad4547eeacda
Dump LSASS via comsvcs DLL	https://hunter.cyborgsecurity.io/research/hunt-package/f68b340c-0148-458f-913d-344a39509632
ShadowCopy Image Accessed	https://hunter.cyborgsecurity.io/research/hunt-package/812301b1-e7b2-4d58-928f-ccef60b48762
Potentially Injected Process Command Execution	https://hunter.cyborgsecurity.io/research/hunt-package/7daf20ca-9558-4b09-bb38-03a09e47746b

MITRE ATT&CK Techniques

This report uses the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) framework. **APT31's** TTPs include:

TECHNIQUE TITLE	ID	USE
Initial Access [TA0001]		
Phishing: Spearphishing Attachment	T1566.001	Threat actors used lure documents to deploy off-the-shelf spyware.
Execution [TA0002]		
User Execution: Malicious File	T1204.002	A system is compromised when the user runs the malware believing it to be a legitimate document.
Command and Scripting Interpreter: Windows Command Shell	T1059.003	Uses cmd.exe to execute multiple commands.
Native API	T1106	Uses CreateProcessW function to execute Windows Command Line
Scheduled Task/Job: Scheduled Task	T1053.005	Malware is executed via a Windows task created by the threat actor.
Persistence [TA0003]		
Registry Run Keys / Startup Folder	T1547.001	Malware achieves persistence by adding itself to the Registry as a startup program.
Create or Modify System Process: Windows Service	T1543.003	Installs itself as a service to achieve persistence.
Scheduled Task/Job: Scheduled Task	T1053.005	Malware is executed via a Windows task created by the threat actor.
Defense Evasion [TA0005]		
Deobfuscate/Decode Files or Information	T1140	Uses an RC4 key to decrypt the malware configuration as well as communication.
Process Injection: Portable Executable Injection	T1055.002	Malware injects itself into various legitimate processes upon execution (msiexec.exe, svchost.exe).

TECHNIQUE TITLE	ID	USE
System Checks	T1497.001	Employs various system checks to detect and avoid virtualization and analysis environments.
Time Based Evasion	T1497.003	Employs various time-based methods to detect and avoid virtualization and analysis environments.
Hijack Execution Flow: DLL Side-Loading	T1574.002	Threat actors abused a legitimate application binary to load a malicious DLL.
Discovery [TA0007]		
File and Directory Discovery	T1083	The malware attempts to discover files of various types (.doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .rtf, .eml).
System Network Configuration Discovery	T1016	Threat actors use the netstat and ipconfig utilities to get local network interface configuration and enumerate open ports.
System Owner/User Discovery	T1033	Threat actors use the systeminfo, whoami, and net utilities to get information about the user and the compromised system.
Process Discovery	T1057	Threat actors use tasklists to enumerate running processes.
Collection [TA0009]		
Data from Local System	T1005	The malware is designed to collect and exfiltrate arbitrary data, including from air-gapped systems, by abusing removable devices.
Data from Removable Media	T1025	The malware is designed store all data collected on a specific infected USB drive in order to exfiltrate it fromv an air-gapped network.

Volt Typhoon's TTPs include:

TECHNIQUE TITLE	ID	USE
Reconnaissance [TA0043]		
Gather Victim Host Information	T1592	Volt Typhoon conducts extensive pre-compromise reconnaissance. This includes web searches, including victim-owned sites, for victim host, identity, and network information, especially for information on key network and IT administrators.
Gather Victim Identity Information	T1589	Volt Typhoon conducts extensive pre-compromise reconnaissance to learn about the target organization's staff.
Gather Victim Identity Information: Email Addresses	T1589.002	Volt Typhoon targets the personal emails of key network and IT staff.
Gather Victim Network Information	T1590	Volt Typhoon conducts extensive pre-compromise reconnaissance to learn about the target organization's network.
Gather Victim Org Information	T1591	Volt Typhoon conducts extensive pre-compromise reconnaissance to learn about the target organization.
Search Open Websites/ Domains	T1593	Volt Typhoon conducts extensive pre-compromise reconnaissance. This includes web searches, including victim-owned sites, for victim host, identity, and network information, especially for information on key network and IT administrators.
Search Victim-Owned Websites	T1594	Volt Typhoon conducts extensive pre-compromise reconnaissance. This includes web searches, including victim-owned sites, for victim host, identity, and network information, especially for information on key network and IT administrators.
Resource Development [TA0042]		

TECHNIQUE TITLE	ID	USE
Acquire Infrastructure: Botnet	T1583.003	Volt Typhoon uses multi-hop proxies for command-and-control infrastructure. The proxy is typically composed of Virtual Private Servers (VPSs) or small office/home office (SOHO) routers.
Compromise Infrastructure: Botnet	T1584.005	Volt Typhoon used Cisco and NETGEAR end-of-life SOHO routers implanted with KV Botnet malware to support their operations.
Compromise Infrastructure: Server	T1584.004	Volt Typhoon has redirected specific port traffic to their proxy infrastructure, effectively converting the PRTG's Detection Guidance server into a proxy for their C2 traffic.
Develop Capabilities: Exploits	T1587.004	Volt Typhoon uses publicly available exploit code, but is also adept at discovering and exploiting vulnerabilities as zero days.
Obtain Capabilities: Exploits	T1588.005	Volt Typhoon uses publicly available exploit code, but is also adept at discovering and exploiting vulnerabilities as zero days.
Initial Access [TA0001]		
Exploit Public-Facing Application	T1190	Volt Typhoon commonly exploits vulnerabilities in networking appliances such as Fortinet, Ivanti (formerly Pulse Secure), NETGEAR, Citrix, and Cisco.
External Remote Services	T1133	Volt Typhoon often uses VPN sessions to securely connect to victim environments, enabling discrete follow-on intrusion activities.
Execution [TA0002]		
Command and Scripting Interpreter	T1059	Volt Typhoon uses hands-on-keyboard execution for their malicious activity via the command-line.
Command and Scripting Interpreter: PowerShell	T1059.001	Volt Typhoon has executed clients via PowerShell.

TECHNIQUE TITLE	ID	USE
Command and Scripting Interpreter: Unix Shell	T1059.004	Volt Typhoon has used Brightmetricagent.exe, which contains multiplexer libraries that can bi-directionally stream data over through NAT networks and contains a command-line interface (CLI) library that can leverage command shells such as PowerShell, Windows Management, Instrumentation (WMI), and Z Shell (zsh).
Windows Management Instrumentation	T1047	Volt Typhoon has used Windows Management Instrumentation Console (WMIC) commands.
Persistence [TA0003]		
Valid Accounts	T1078	Volt Typhoon primarily relies on valid credentials for persistence.
Privilege Escalation [TA0004]		
Exploitation for Privilege Escalation	T1068	Volt Typhoon first obtains credentials from public-facing appliances after gaining initial access by exploiting privilege escalation vulnerabilities in the operating system or network services.
Defense Evasion [TA0005]		
Direct Volume Access	T1006	Volt Typhoon has executed the Windows-native vssadmin command to create a volume shadow copy.
Indicator Removal: Clear Persistence	T1070.009	Volt Typhoon has selectively cleared Windows Event Logs, system logs, and other technical artifacts to remove evidence of their intrusion activity and masquerading file names.
Indicator Removal: Clear Windows Event Logs	T1070.001	Volt Typhoon has selectively cleared Windows Event Logs, system logs, and other technical artifacts to remove evidence of their intrusion activity and masquerading file names.

TECHNIQUE TITLE	ID	USE
Indicator Removal: File Deletion	T1070.004	Volt Typhoon created systeminfo.dat in C:\Users\Public\Documents, but subsequently deleted it.
Masquerading: Match Legitimate Name or Location	T1036.005	Volt Typhoon has selectively cleared Windows Event Logs, system logs, and other technical artifacts to remove evidence of their intrusion activity and masquerading file names.
Modify Registry	T1112	Volt Typhoon has used the netsh command, a legitimate Windows command, to create a PortProxy registry modification on the PRTG server.
Obfuscated Files or Information: Software Packing	T1027.002	Volt Typhoon has obfuscated FRP client files (BrightmetricAgent.exe and SMSvcService.exe) and the command-line port scanning utility ScanLine by packing the files with Ultimate Packer for Executables (UPX).
System Binary Proxy Execution	T1218	Volt Typhoon uses hands-on-keyboard activity via the command-line and use other native tools and processes on systems (often referred to as "LOLBins"), known as LOTL, to maintain and expand access to the victim networks.
Credential Access [TA0006]		
Brute Force: Password Cracking	T1110.002	Volt Typhoon has exfiltrated NTDS.dit and SYSTEM registry hive to crack passwords offline.
Credentials from Password Stores	T1555	Volt Typhoon has installed browser-saved passwords history, credit card details, and cookies.
Credentials from Password Stores: Credentials from Web Browsers	T1555.003	Volt Typhoon has strategically targeted network administrator web browser data, focusing on both browsing history and stored credentials.

TECHNIQUE TITLE	ID	USE
OS Credential Dumping: LSASS Memory	T1003.001	Volt Typhoon used a DLL with MiniDump and the process ID of Local Security Authority Subsystem Service (LSASS) to dump the LSASS process memory and obtain credentials.
OS Credential Dumping: NTDS	T1003.003	Volt Typhoon appears to prioritize obtaining valid credentials by extracting the Active Directory database file (NTDS.dit).
Unsecured Credentials	T1552	Volt Typhoon has obtained credentials insecurely stored on an appliance.
Unsecured Credentials: Private Keys	T1552.004	Volt Typhoon has accessed a Local State file that contains the Advanced Encryption Standard (AES) encryption key used to encrypt the passwords stored in the Chrome browser, which enables the actors to obtain plaintext passwords stored in the Login Data file in the Chrome browser.
Discovery [TA0007]		
Account Discovery: Local Account	T1087.001	Volt Typhoon executed net user and user for user account information.
Application Window Discovery	T1010	Volt Typhoon created and accessed a file named rult3uil.log on a Domain Controller in C:\Windows\System32\. The rult3uil.log file contained user activities on a compromised system, showcasing a combination of window title information and focus shifts, keypresses, and command executions across Google Chrome and Windows PowerShell, with corresponding timestamps.
Browser Information Discovery	T1217	Volt Typhoon has installed browser-saved passwords history, credit card details, and cookies.

TECHNIQUE TITLE	ID	USE
File and Directory Discovery	T1083	Volt Typhoon enumerated several directories , including directories containing vulnerability testing and cyber related content and facilities data, such as construction drawings.
Log Enumeration	T1654	Volt Typhoon has captured successful logon events.
Network Service Discovery	T1046	Volt Typhoon has used commercial tools, LOTL utilities, and appliances already present on the system for system information, network service, group, and user discovery.
Peripheral Device Discovery	T1120	Volt Typhoon has obtained the victim's system screen dimension and display devices information.
Permission Groups Discovery	T1069	Volt Typhoon has used commercial tools, LOTL utilities, and appliances already present on the system for system information, network service, group, and user discovery.
Process Discovery	T1057	Volt Typhoon executed tasklist /v to gather a detailed process listing.
Query Registry	T1012	Volt Typhoon has interacted with a PuTTY application by enumerating existing stored sessions.
Software Discovery	T1518	Volt Typhoon has obtained the victim's list of applications installed on the victim's system.
System Information Discovery	T1082	Volt Typhoon has used commercial tools, LOTL utilities, and appliances already present on the system for system information, network service, group, and user discovery.

TECHNIQUE TITLE	ID	USE
System Location Discovery	T1614	Volt Typhoon has obtained the victim's current system locale.
System Network Configuration Discovery: Internet Connection Discovery	T1016.001	Volt Typhoon employs ping with various IP addresses to check network connectivity and net start to list running services.
System Owner/User Discovery	T1033	Volt Typhoon has used commercial tools, LOTL utilities, and appliances already present on the system for system information, network service, group, and user discovery.
System Service Discovery	T1007	Volt Typhoon employs ping with various IP addresses to check network connectivity and net start to list running services.
System Time Discovery	T1124	Volt Typhoon has obtained the victim's system timezone.
Lateral Movement [TA0008]		
Remote Service Session Hijacking	T1563	Volt Typhoon potentially had access to a range of critical PuTTY profiles, including those for water treatment plants, water wells, an electrical substation, operational technology systems, and network security devices. This would enable them to access these critical systems.
Remote Services: Cloud Services	T1021.007	During the period of Volt Typhoon's known network presence, there were anomalous login attempts to an Azure tenant potentially using credentials previously compromised from theft of NTDS.dit.
Remote Services: Remote Desktop Protocol	T1021.001	Volt Typhoon has moved laterally to the Domain Controller via an interactive RDP session using a compromised account with domain administrator privileges.

TECHNIQUE TITLE	ID	USE
Use Alternate Authentication Material	T1550	Volt Typhoon may be capable of using other methods such as Pass the Hash or Pass the Ticket for lateral movement.
Valid Accounts: Cloud Accounts	T1078.004	During the period of Volt Typhoon's known network presence, there were anomalous login attempts to an Azure tenant potentially using credentials previously compromised from theft of NTDS.dit.
Collection [TA0009]		
Archive Collected Data	T1560	Volt Typhoon collected sensitive information obtained from a file server in multiple zipped files.
Archive Collected Data: Archive via Utility	T1560.001	Volt Typhoon has compressed and archived the extracted ntds.dit and accompanying registry files (by executing ronf.exe, which was likely a renamed version of rar.exe).
Data Staged	T1074	Volt Typhoon accessed the file C:\Users\{redacted}\Downloads\History.zip, which presumably contained data from the User Data directory of the user's Chrome browser, which the actors likely saved in the Downloads directory for exfiltration.
Screen Capture	T1113	Volt Typhoon has obtained a screenshot of the victim's system using two libraries (gdi32.dll and gdiplus.dll)
Command and Control [TA0011]		
Encrypted Channel	T1573	Volt Typhoon has set up FRP clients on a victim's corporate infrastructure to establish covert communications channels for command and control.

TECHNIQUE TITLE	ID	USE
Ingress Tool Transfer	T1105	Volt Typhoon uses legitimate, but outdated versions of network admin tools. For example, in one confirmed compromise, actors downloaded an outdated version of comsvcs.dll, on the DC in a non-standard folder.
Proxy	T1090	Volt Typhoon has setup FRP clients on a victim's corporate infrastructure to establish covert communications channels for command and control.
Proxy: Internal Proxy	T1090.001	Volt Typhoon has used the netsh command, a legitimate Windows command, to create a PortProxy registry modification on the PRTG server.
Proxy: Multi-hop Proxy	T1090.003	Volt Typhoon uses multi-hop proxies for command-and-control infrastructure.
Exfiltration [TA0010]		
Exfiltration Over Alternative Protocol	T1048	Volt Typhoon exfiltrated files via Server Message Block (SMB).

GIRs

6.1.8 Technology, media and telecommunications sector

6.1.5 Manufacturing sector

5.5.1 Espionage

6.2.6.5 United States

6.2.2.8 China

6.1.6.2 National government

6.1.6.6 Military and defense

Endnotes

1. 21Mar2024 The Japan Times article: China on track to be ready to invade Taiwan by 2027, U.S. commander says
   https://www.japantimes.co.jp/news/2024/03/21/asia-pacific/politics/taiwan-china-invasion-2027/
2. 18Apr2024 FBI article: Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure, FBI Director Says
   https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says
3. 25Mar2024 U.S. Department of the Treasury press release: Treasury Sanctions China-Linked Hackers for Targeting U.S. Critical Infrastructure
   https://home.treasury.gov/news/press-releases/jy2205
4. 31Jul2023 Kaspersky report: Common TTPs of attacks against industrial organizations. Implants for gathering data
   https://ics-cert.kaspersky.com/publications/reports/2023/07/31/common-ttps-of-attacks-against-industrial-organizations-implants-for-gathering-data/
5. 20Jun2021 Security Affairs article: Norway blames China-linked APT31 for 2018 government hack
   https://securityaffairs.com/119161/apt/norway-blames-china-apt31.html
6. 07Feb2024 CISA report: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure
   https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
7. 28Feb2024 Dragos report: VOLTZITE Espionage Operations Targeting U.S. Critical Systems
   https://hub.dragos.com/hubfs/116-Datasheets/Dragos_IntelBrief_VOLTZITE_FINAL.pdf?hsLang=en
8. 07Feb2024 CISA report: Identifying and Mitigating Living Off the Land Techniques
   https://www.cisa.gov/sites/default/files/2024-02/Joint-Guidance-Identifying-and-Mitigating-LOTL_V3508c.pdf

Notes

ABOUT INTEL 471

Intel 471 equips enterprises and government agencies with intelligence-driven security offerings powered by real-time insights into cyber adversaries, threat patterns, and potential attacks relevant to their operations. By integrating human-sourced intelligence with advanced automation and curation, the company's platform enhances security measures and enables teams to bolster their security posture by prioritizing controls and detections based on real-time cyber threats. Organizations are empowered to neutralize and mitigate digital risks across dozens of use cases across our solution portfolios: Cyber Threat Exposure, Cyber Threat Intelligence, and Cyber Threat Hunting. Learn more at www.intel471.com.

Our customers' eyes and ears outside the wire.

INTEL471

1209 N Orange St, Wilmington, DE 19801