Hive Pro®

Threat Level

Red

CISA: AA24-038A

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

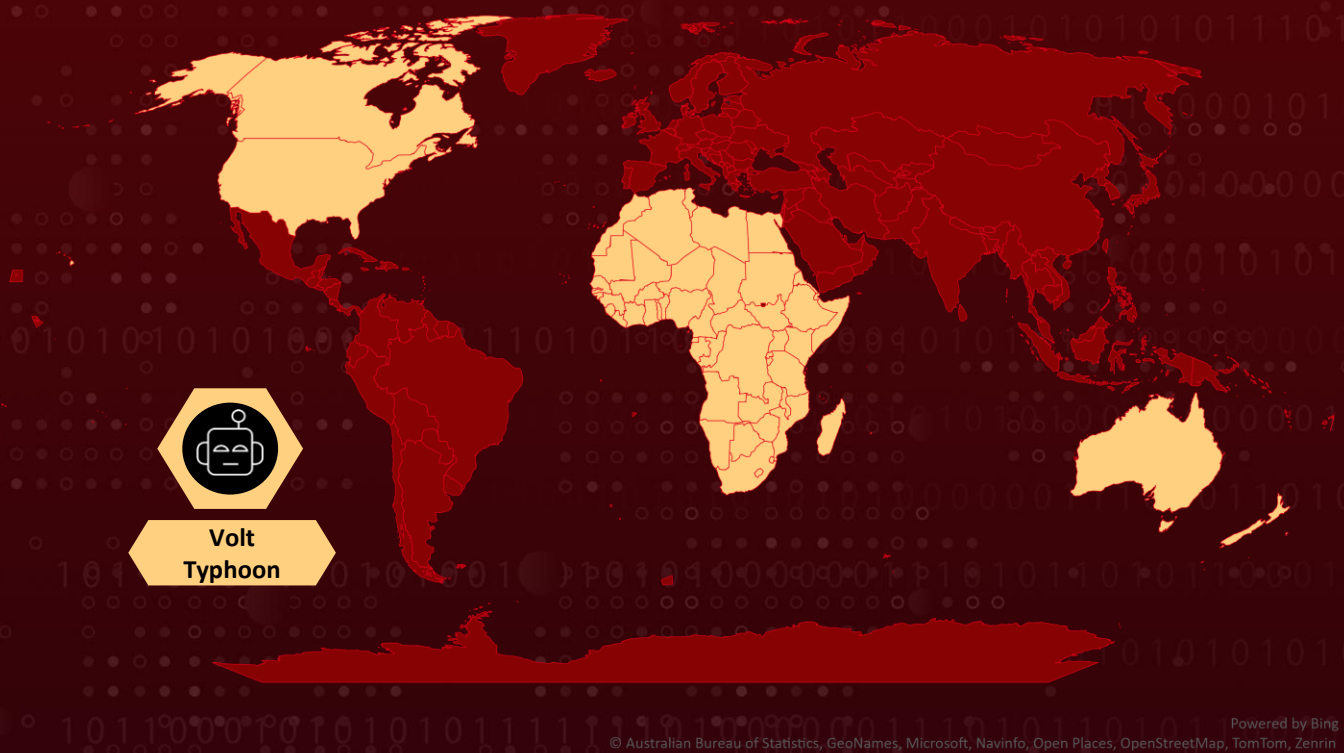
Volt Typhoon: A Cyber Threat to U.S. Critical Infrastructure

Date of Publication	Last updated date	Admiralty Code	TA Number
February 9, 2024	February 16, 2024	A1	TA2024050

Summary

Attack Began: May 2023
Targeted Countries: United States, Canada, Australia, New Zealand, and African countries
Threat Actor: Volt Typhoon (also known as Vanguard Panda, BRONZE SILHOUETTE, Dev-0391, UNC3236, Voltzite, and Insidious Taurus)
Targeted Industries: Communications, Energy, Transportation Systems, Water and Wastewater Systems, Emergency management services, Telecommunications, Satellite services, and Defense
Attack: State-sponsored cyber actors from the People's Republic of China, known as Volt Typhoon, are actively targeting critical infrastructure in the United States, employing sophisticated tactics like pre-compromise reconnaissance and living off the land (LOTL) techniques.

Attack Regions



Attack Details

#1 The People's Republic of China (PRC) has state-sponsored cyber actors, identified as Volt Typhoon, actively targeting U.S. and African critical infrastructure networks since early 2023. These actors aim to pre-position themselves for potential disruptive or destructive cyberattacks in the event of a major crisis or conflict with the United States.

#2 Volt Typhoon's primary techniques include slow and steady reconnaissance, living off the land (LOTL), web shells, compromised SOHO equipment, open-source tools, and credential theft. The targeted sectors include Communications, Energy, Transportation Systems, Water and Wastewater Systems, Emergency management services, Telecommunications, Satellite services, and Defense.

#3 Initially, Volt Typhoon employs meticulous pre-compromise reconnaissance to understand target networks and exploits vulnerabilities in public-facing network appliances for initial access. They prioritize obtaining administrator credentials through privilege escalation and use them to move laterally within the network, often via Remote Desktop Protocol. The group conducts discreet discovery operations and achieves full domain compromise by extracting the Active Directory database (NTDS.dit) from the DC.

#4 Additionally, they use offline password cracking techniques to decipher extracted hashes. Volt Typhoon strategically focuses on accessing Operational Technology (OT) assets using elevated credentials for further infiltration and discovery within networks.

#5 The group strategically targets key infrastructure assets and conducts activities like credential dumping, discovery, lateral movement, and collection of sensitive information. They leverage compromised credentials and stealthy techniques to evade detection and maintain long-term access. Additionally, they employ techniques such as selective log deletion and obfuscation of malware to cover their tracks.

#6 Overall, Volt Typhoon represents a significant cyber threat to critical infrastructure in the United States and African countries, even potentially other countries like Canada, Australia, New Zealand, which are also vulnerable. Mitigating these threats requires proactive measures, collaboration, and vigilance from both public and private sectors.

Recommendations

Apply Patches for Internet-Facing Systems: Prioritize patching critical vulnerabilities in appliances known to be frequently exploited by threat actors like Volt Typhoon. Regularly update and apply patches to ensure that internet-facing systems are protected against known vulnerabilities.

Implement Multi-Factor Authentication (MFA): Deploy MFA solutions that are resilient to phishing attacks, such as hardware tokens or biometric authentication. These methods provide an additional layer of security beyond passwords and help prevent unauthorized access, even if credentials are compromised.

Least Privilege Access: Restrict user permissions and privileges to only what is necessary for their roles. This reduces the potential impact of compromised accounts and limits the lateral movement of attackers.

Enable Logging and Centralized Log Management: Ensure that logging is enabled for application, access, and security logs on all systems. Store logs in a centralized system for easier monitoring, analysis, and incident response. Centralized log management facilitates the detection of suspicious activities and provides valuable insights into potential security incidents.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0010 Exfiltration	T1591 Gather Victim Org Information	T1593 Search Open Websites/Domains	T1594 Search Victim-Owned Websites
T1190 Exploit Public-Facing Application	T1583.003 Virtual Private Server	T1584.005 Botnet	T1584.004 Server

T1047 Windows Management Instrumentation	T1078 Valid Accounts	T1068 Exploitation for Privilege Escalation	T1006 Direct Volume Access
T1070.009 Clear Persistence	T1070.001 Clear Windows Event Logs	T1070.004 File Deletion	T1036.005 Match Legitimate Name or Location
T1112 Modify Registry	T1027 Obfuscated Files or Information	T1027.002 Software Packing	T1218 System Binary Proxy Execution
T1110.002 Password Cracking	T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers	T1003.001 LSASS Memory
T1003.003 NTDS	T1552 Unsecured Credentials	T1552.004 Private Keys	T1087.001 Local Account
T1010 Application Window Discovery	T1217 Browser Information Discovery	T1083 File and Directory Discovery	T1654 Log Enumeration
T1046 Network Service Discovery	T1120 Peripheral Device Discovery	T1069 Permission Groups Discovery	T1057 Process Discovery
T1012 Query Registry	T1518 Software Discovery	T1082 System Information Discovery	T1614 System Location Discovery
T1016.001 Internet Connection Discovery	T1033 System Owner/User Discovery	T1007 System Service Discovery	T1124 System Time Discovery
T1563 Remote Service Session Hijacking	T1021.001 Remote Desktop Protocol	T1550 Use Alternate Authentication Material	T1078.004 Cloud Accounts
T1560 Archive Collected Data	T1560.001 Archive via Utility	T1074 Data Staged	T1113 Screen Capture
T1573 Encrypted Channel	T1105 Ingress Tool Transfer	T1090 Proxy	T1090.001 Internal Proxy
T1090.003 Multi-hop Proxy	T1048 Exfiltration Over Alternative Protocol	T1590 Gather Victim Network Information	T1589.002 Email Addresses

T1059 Command and Scripting Interpreter	T1592 Gather Victim Host Information	T1589 Gather Victim Identity Information	T1021 Remote Services
T1584 Compromise Infrastructure	T1587.004 Exploits	T1587 Develop Capabilities	T1588.005 Exploits
T1588 Obtain Capabilities	T1133 External Remote Services	T1059.001 PowerShell	T1059.004 Unix Shell

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	99b80c5ac352081a64129772ed5e1543d94cad708ba2adc46dc4ab7a0bd563f1, eaef901b31b5835035b75302f94fee27288ce46971c6db6221ecbea9ba7ff9d0, edc0c63065e88ec96197c8d7a40662a15a812a9583dc6c82b18ecd7e43b13b70
MD5	3a97d9b6f17754dcd38ca7fc89caab04, 5c0061445ac2f8e6cadf694e54146914, 6ed4f5f04d62b18d96b26d6db7c18840, 7f8e8722da728b6e834260b5a314cbac, b1de37bf229890ac181bdef1ad8ee0c2, f9943591918adeeeee7da80e4d985a49, fd41134e8ead1c18ccad27c62a260aa6
IPv4	203.95.8[.]98, 203.95.9[.]54
Domain	Pdsguam[.]biz
SHA1	04423659f175a6878b26ac7d6b6e47c6fd9194d1, ffb1d8ea3039d3d5eb7196d27f5450cac0ea4f34, ffdb3cc7ab5b01d276d23ac930eb21ffe3202d11

References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

https://www.cisa.gov/news-events/analysis-reports/ar24-038a

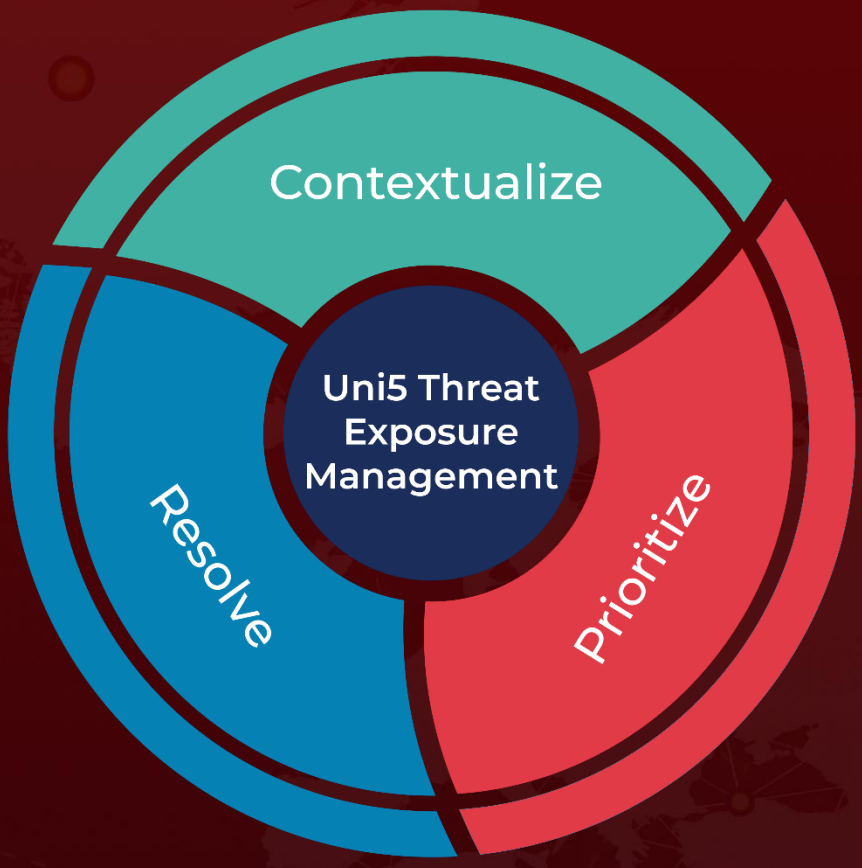
https://www.hivepro.com/threat-advisory/volt-typhoon-chinese-espionage-group-targets-u-s-government/

https://hub.dragos.com/hubfs/116-Datasheets/Dragos_IntelBrief_VOLTZITE_FINAL.pdf?hsLang=en

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 9, 2024 • 3:30 AM

More at www.hivepro.com