Hive Pro

Threat Level

Red

CISA:AA23-144a

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

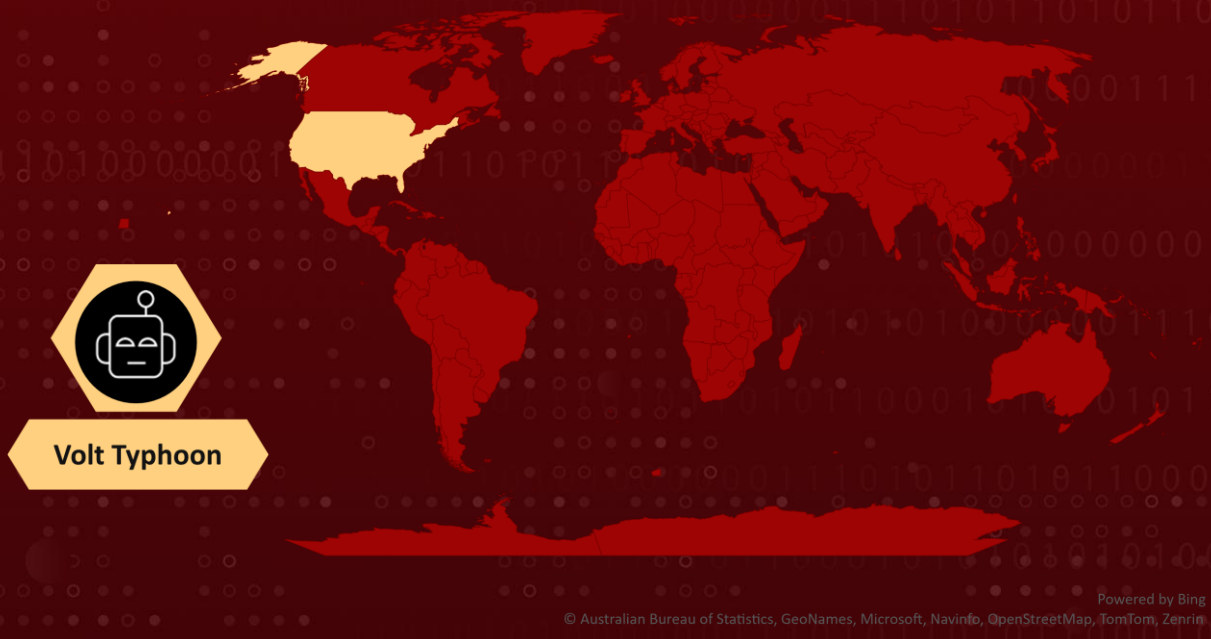
Volt Typhoon Chinese Espionage Group Targets U.S. Government

Date of Publication	Admiralty code	TA Number
June 6, 2023	A1	TA2023252

Summary

First Appearance: 2021
Actor Name: Volt Typhoon (aka BRONZE SILHOUETTE)
Target Industries: Communications, Manufacturing, Utility, Transportation, Construction, Maritime, Government, Information Technology, and Education.
Target Region: United States and the U.S. island territory of Guam.

Actor Map



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2021-40539	Zoho ManageEngine ADSelfService Plus Authentication Bypass Vulnerability	Zoho ManageEngine	✓	✓	✓
CVE-2021-27860	FatPipe WARP, IPVPN, and MPVPN Configuration Upload exploit	FatPipe WARP, IPVPN, and MPVPN software	✗	✓	✓

Actor Details

#1

A significant surge of operations has been detected and attributed to an orchestrated threat group sponsored by the People's Republic of China (PRC). This activity is specifically linked to a threat actor, Volt Typhoon (aka BRONZE SILHOUETTE), a state-sponsored entity operating from China. Since 2021, this threat group has been actively engaged in conducting network intrusion operations against various government and defense organizations within the United States.

#2

Volt Typhoon's focus primarily revolves around espionage and acquiring information through targeted and covert methods, including obtaining post-compromise credential access and systematically exploring network systems. The Volt Typhoon campaign places a strong emphasis on stealth, relying predominantly on living-off-the-land (LOTL) techniques and direct engagement by skilled operators.

#3

To gain initial access to targeted organizations, Volt Typhoon exploits internet-facing Fortinet FortiGuard devices. Moreover, they attempt to blend in with regular network activity by routing traffic through the compromised small office and home office (SOHO) network equipment, such as routers, firewalls, and VPN hardware.

#4

Additionally, they have been observed utilizing customized versions of open-source tools to establish a command and control (C2) channel via a proxy, enabling them to remain undetected. In a September 2021 attack against a U.S. organization, Volt Typhoon resurfaced, exploiting a vulnerability in an internet-facing ManageEngine ADSelfService Plus server (CVE-2021-40539) to gain initial access.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Volt Typhoon (aka BRONZE SILHOUETTE)	China **MOTIVE** Information theft and espionage	United States and the U.S. island territory of Guam.	Communications, Manufacturing, Utility, Transportation, Construction, Maritime, Government, Information Technology, and Education.

Recommendations

Strengthen Authentication and Account Security: Implement robust multi-factor authentication (MFA) policies using hardware security keys or Microsoft Authenticator to mitigate the risk of compromised valid accounts. Consider adopting passwordless sign-in and enforcing password expiration rules. Deactivate unused accounts to reduce the potential attack surface and mitigate risks associated with this access method.

Enhance Domain Controller Security and Monitoring: Harden domain controllers and closely monitor event logs for process creations related to ntdsutil.exe and similar processes. Stay vigilant for malicious file names that follow a specific pattern, such as C:\Windows[a-zA-Z]{8}.exe. Regularly audit and validate the use of administrator privileges to ensure the legitimacy of executed commands.

Investigate Unusual Network Activity: Conduct thorough investigations of command lines, registry entries, and firewall logs to identify any unusual **IP addresses** and ports. Pay particular attention to any hosts that appear to be involved in suspicious actor actions. Apply security **patches** and updates to address vulnerabilities promptly and proactively mitigate potential risks.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0011** Command and Control	**T1003** OS Credential Dumping
T1003.001 LSASS Memory	**T1003.003** NTDS	**T1016** System Network Configuration Discovery	**T1033** System Owner/User Discovery
T1047 Windows Management Instrumentation	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell	**T1059.003** Windows Command Shell
T1069 Permission Groups Discovery	**T1069.001** Local Groups	**T1069.002** Domain Groups	**T1070** Indicator Removal
T1070.001 Clear Windows Event Logs	**T1082** System Information Discovery	**T1090** Proxy	**T1090.002** External Proxy
T1110 Brute Force	**T1110.003** Password Spraying	**T1190** Exploit Public-Facing Application	**T1505** Server Software Component
T1505.003 Web Shell	**T1555** Credentials from Password Stores		

Indicator of Compromise (IOCs)

TYPE	VALUE
File paths	C:\Users\Public\Appfile C:\Perflogs C:\Windows\Temp

TYPE	VALUE
File Names	backup.bat cl64.exe update.bat Win.exe billagent.exe nc.exe update.exe WmiPrvSE.exe billaudit.exe rar.exe vm3dservice.exe WmiPreSV.exe cisco_up.exe SMSvcService.exe watchdogd.exe
User-agent	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:68.0) Gecko/20100101 Firefox/68.0
MD5	006c4a5950f75c2c9049cda1a62c09a0 af3a81605aa8e29c8be9e91d2ce19fc1 670545a24a2ce2ac7a0e863790bfe2e1
SHA1	4d3572cfc8460fe0299377f6bc05d865a987529f a9e32e2bd499c1070f4e0b5a6d85119f1aa0a778 4ba6b043313c8d163f2ab7c4505c8b9b8cd68061
IPV4	109.166.39[.]139 23.227.198[.]247 104.161.54[.]203
SHA256	17506c2246551d401c43726bdaec800f8d41595d01311cf38a19140ad32da2f4 389a497f27e1dd7484325e8e02bbdf656d53d5cf2601514e9b8d8974beffddf61 3a9d8bb85fbcfe92bae79d5ab18e4bca9eaf36cea70086e8d1ab85336c83945f 3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71 3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642 41e5181b9553bbe33d91ee204fe1d2ca321ac123f9147bb475c0ed32f9488597 450437d49a7e5530c6fb04df2e56c3ab1553ada3712fab02bd1eeb1f1adbc267 472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d

TYPE	VALUE
SHA256	4b0c4170601d6e922cf23b1caf096bba2fade3dfcf92f0ab895a5f0b9a310349 6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff 66a19f7d2547a8a85cee7a62d0b6114fd31afdee090bd43f36b89470238393d7 7939f67375e6b14dfa45ec70356e91823d12f28bbd84278992b99e0d2c12ace5 8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2 93ce3b6d2a18829c0212542751b309dacbdc8c1d950611efe2319aa715f3a066 9dd101caee49c692e5df193b236f8d52a07a2030eed9bd858ed3aaccb406401a b4f7c5e3f14fb57be8b5f020377b993618b6e3532a4e1eb1eae9976d4130cc74 baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c c0fc29a52ec3202f71f6378d9f7f9a8a3a10eb19acb8765152d758aded98c76d c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b c7fee7a3ffaf0732f42d89c4399cbff219459ae04a81fc6eff7050d53bd69b99 cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984 d17317e1d5716b09cee904b8463a203dc6900d78ee2053276cc948e4f41c8295 d6ab36cb58c6c8c3527e788fc9239d8dcc97468b6999cf9ccd8a815c8b4a80af d6ebde42457fe4b2a927ce53fc36f465f0000da931cfab9b79a36083e914ceca e453e6efc5a002709057d8648dbe9998a49b9a12291dee390bb61c98a58b6e95 ee8df354503a56c62719656fae71b3502acf9f87951c55ffd955feec90a11484 ef09b8ff86c276e9b475a6ae6b54f08ed77e09e169f7fc0872eb1d427ee27d31 f4dd44bc19c19056794d29151a5b1bb76afd502388622e24c863a8494af147dd Fe95a382b4f879830e2666473d662a24b34fccf34b6b3505ee1b62b32adafa15

Patch Links

https://www.manageengine.com/products/self-service-password/advisory/CVE-2021-40539.html

https://www.fatpipeinc.com/support/cve-list.php

References

https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_PRC_State_Sponsored_Cyber_Living_off_the_Land_v1.1.PDF

https://www.tenable.com/blog/volt-typhoon-cybersecurity-advisory

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

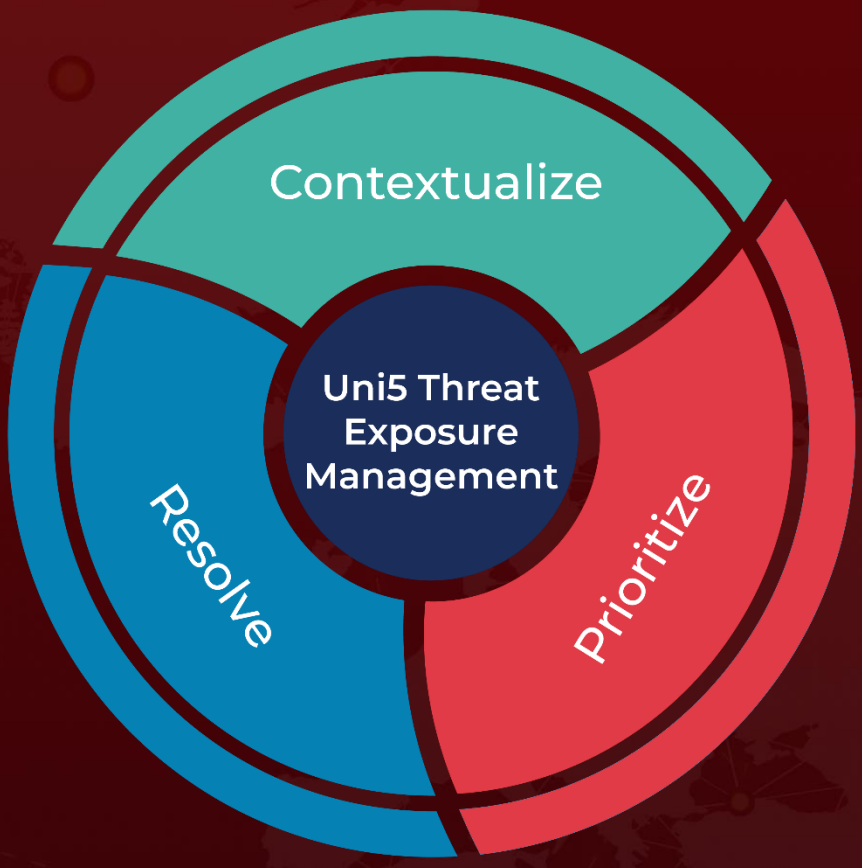
https://www.secureworks.com/blog/chinese-cyberespionage-group-bronze-silhouette-targets-us-government-and-defense-organizations

https://www.ic3.gov/Media/News/2021/211117-2.pdf

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

June 6, 2023 . 7:19 AM

© 2023 All Rights are Reserved by HivePro

More at www.hivepro.com