THREAT BULLETIN

AR20240209-003 [Advisory Report] PRC-Linked Threat Actor Volt Typhoon Targets US Critical Infrastructure

TLP Clear

DESCRIPTION

TLP:CLEAR = Disclosure is not limited.

Key Details

Threat Actor Category: PRC State-Sponsored
Confirmed Threat Target(s): US Federal Government, Critical Infrastructure
Potential Threat Target(s): SLTT*
Targeted Technologies: End-of-Life (EOL) Routers (Cisco, Netgear. It is unknown to the MD-ISAC as of this writing if others have been or will be targeted in addition.)

*It is not explicitly known whether Volt Typhoon targets State, Local, Tribal, and Territorial (SLTT) governments in the US or just the Federal government. The focus of Volt Typhoon's attacks is stated as U.S. critical infrastructure, including operational technology systems in sectors such as communications, energy, transportation, and water. However, it is possible that SLTT governments could be affected if their critical infrastructure falls within these targeted sectors.

Summary

Volt Typhoon (Aliases: BRONZE SILHOUETTE, Insidious Taurus, TAG-87, VANGUARD PANDA, Dev-0391, UNC3236, and Voltzite) is a PRC-linked Advanced Persistent Threat (APT) group that has been involved in targeting government entities and critical infrastructure in the US. They have been active since mid-2021 and have been confirmed to compromise multiple critical infrastructure organizations including communications, energy, transportation and water and wastewater systems. While the United States government, in collaboration with the Federal Bureau of Investigation (FBI) and other agencies, has recently completed an operation in order to disrupt and dismantle the Volt Typhoon botnet, this group remains a significant threat to US government and critical infrastructure organizations.

Tactics, Techniques, & Procedures (TTPs)

The group has been known to exploit known vulnerabilities and compromise network devices such as routers to gain access to networks and further conduct reconnaissance and exploitation activities. Notably, the group has recently been exploiting two critical vulnerabilities in Cisco RV320 and RV325 models, tracked as CVE-2019-1653 and CVE-2019-1652. They have also employed living-off-the-land techniques, such as using legitimate tools and techniques to hide their activities and reduce detection. Additionally, Volt Typhoon has been known to use botnets to conceal the origin of their hacking activities. On Jan 31, 2024, the FBI reported that it had disrupted the KV-Botnet, which was utilized by Volt Typhoon and was composed largely of SOHO (small home/home office) routers that had reached EOL (end of life) and were no longer patchable.
On February 07, 2024, CISA, NSA, FBI, and other Federal partners released an advisory, warning that Volt Typhoon is likely preparing itself for further attacks, first by focusing on initial access and then later to turn to lateral movement across victim networks. As stated in the report, “the U.S. authoring agencies have recently observed indications of Volt Typhoon actors maintaining access and footholds within some victim IT environments for at least five years.” Because of their use of valid accounts and LOTL techniques, it is possible for the group to retain persistent access and remain undiscovered.

Mitre Att&ck TTPs:

T1003.001 (LSASS Memory)
T1003.003 (NTDS)
T1005 (Data from Local System)
T1036.005 (Match Legitimate Name or Location)
T1059 (Command and Scripting Interpreter)
T1071 (Application Layer Protocol)
T1078.001 (Default Accounts)
T1090 (Proxy)
T1105 (Ingress Tool Transfer)

T1119 (Automated Collection)
T1187 (Forced Authentication)
T1190 (Exploit Public-Facing Application)
T1505 (Server Software Component)
T1505.003 (Web Shell)
T1556.001 (Domain Controller Authentication)
T1583 (Acquire Infrastructure)

Known Leveraged CVEs:

CVE-2019-1653
CVE-2019-1652

Indicators of Compromise (IOCs)

04423659f175a6878b26ac7d6b6e47c6fd9194d1
17506c2246551d401c43726bdaec800f8d41595d01311cf38a19140ad32da2f4
36c63d0c2a78497ccf555e84f0233a514943faeff38281d99d00baf5df23f184
3a97d9b6f17754dcd38ca7fc89caab04
4b0c4170601d6e922cf23b1caf096bba2fade3dfcf92f0ab895a5f0b9a310349
5c0061445ac2f8e6cadf694e54146914
6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff
7043ffd9ce3fe48c9fb948ae958a2e9966d29afe380d6b61d5efb826b70334f5
7f8e8722da728b6e834260b5a314cbac
93ce3b6d2a18829c0212542751b309dacbdc8c1d950611efe2319aa715f3a066
99b80c5ac352081a64129772ed5e1543d94cad708ba2adc46dc4ab7a0bd563f1
9dd101caee49c692e5df193b236f8d52a07a2030eed9bd858ed3aaccb406401a
b1de37bf229890ac181bdef1ad8ee0c2
b4f7c5e3f14fb57be8b5f020377b993618b6e3532a4e1eb1eae9976d4130cc74
baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c
c0fc29a52ec3202f71f6378d9f7f9a8a3a10eb19acb8765152d758aded98c76d
c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b
cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984
d17317e1d5716b09cee904b8463a203dc6900d78ee2053276cc948e4f41c8295
d6ab36cb58c6c8c3527e788fc9239d8dcc97468b6999cf9ccd8a815c8b4a80af
d99941e4445efed5d4e407f91a9e5bba08d1be3f0dab065d1bfb4e70ab48d6526a730233d6889ba58de449f622e6a14e99dab853d40fc30a508627fd2735c973
df55591e730884470afba688e17c83fafb157ecf94c9f10a20e21f229434ea58b59f8eb771f8f9e29993f43f4969fe66dd913128822b534c9b1a677453dbb93c
e41df636a36ac0cce38e7db5c2ce4d04a1a7f9bc274bdf808912d14067dc1ef478268035521d0d4b7bcf96facce7f515560b38a7ebe47995d861b9c482e07e25
e453e6efc5a002709057d8648dbe9998a49b9a12291dee390bb61c98a58b6e95
eaef901b31b5835035b75302f94fee27288ce46971c6db6221ecbea9ba7ff9d0
edc0c63065e88ec96197c8d7a40662a15a812a9583dc6c82b18ecd7e43b13b70
f9943591918adeeeee7da80e4d985a49
fd41134e8ead1c18ccad27c62a260aa6
ffb1d8ea3039d3d5eb7196d27f5450cac0ea4f34
ffdb3cc7ab5b01d276d23ac930eb21ffe3202d11
114.143.222[.]242
117.211.166[.]22
117.239.157[.]74
118.99.13[.]45
118.99.13[.]78
118.99.13[.]8
140.82.30[.]126
149.248.38[.]177
154.216.191[.]249
154.39.152[.]240
154.39.244[.]169

154.39.245[.]89
154.55.138[.]106
176.102.35[.]175
183.82.110[.]178
184.67.141[.]110
185.126.119[.]162
194.50.159[.]3
202.22.227[.]179
203.95.8[.]98
203.95.9[.]54
206.233.131[.]201
206.233.133[.]147
206.233.133[.]221
207.246.97[.]32
208.83.234[.]97
208.97.106[.]10
210.212.224[.]124
24.212.225[.]54
38.48.120[.]107
38.48.120[.]160
38.48.120[.]217
38.48.120[.]77
38.48.120[.]93
38.48.120[.]96
38.48.121[.]205
45.11.92[.]176
45.144.243[.]75
45.146.120[.]29
45.146.120[.]55
45.146.120[.]62
45.200.14[.]225
45.32.174[.]131
45.63.60[.]39
45.85.0[.]253
46.10.197[.]206
49.204.65[.]90
49.204.73[.]250
49.204.75[.]90
49.204.75[.]92
5.180.79[.]140
5.183.101[.]116
5.252.197[.]80
61.2.141[.]161
70.60.30[.]222
80.64.80[.]169
82.117.159[.]158
89.203.140[.]246
91.220.202[.]150
91.220.202[.]165
93.62.0[.]77
94.125.218[.]19

References

https://www.cyber.nj.gov/alerts-advisories/volt-typhoon-targets-legacy-cisco-routers-in-new-campaign
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
https://www.cisa.gov/news-events/analysis-reports/ar24-038a
https://www.cisa.gov/sites/default/files/2024-02/Joint-Guidance-Identifying-and-Mitigating-LOTL_V3508c.pdf
https://www.darkreading.com/endpoint-security/feds-confirm-remote-killing-volt-typhoon-soho-botnet

Analysis from Recorded Future's Insikt Group was referenced in the creation of this report.

Incident Response

If administrators discover signs of attack or system compromise, the MD-ISAC recommends they:

- Immediately isolate affected systems.
- Collect and review relevant logs, data, and artifacts.
- Consider soliciting support from a third-party incident response organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.
- Report incidents to MD-ISAC via Maryland's 24/7 Operations Center (md-isac@maryland.gov or (410) 697-9700 - option #5).

Reporting and Contact Information

In the case of a cybersecurity incident related to information found in this threat bulletin, Md. Code, Public Safety Article § 14-104.1 (c)(2) and Md. Code, State Finance & Procurement Article § 3.5-406(b)(2)) mandate that you report this via the Maryland Incident Reporting System. It is also recommended that you submit any shareable cyber threat intelligence to the MD-ISAC via the MD-ISAC Threat Intelligence Platform (TIP).