THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

Cyber Threat Advisory

Volt Typhoon

Threat Actor Malware

CATEGORY

Malware

SEVERITY

High

Platforms

Windows

IMPACT

- **Espionage and Intelligence Gathering**
- **Infrastructure Disruption**
- **National Security Threat**
- **Economic and Operational Risks**
- **Broader Security Ecosystem Impact**

Description

Volt Typhoon

Volt Typhoon, a state-sponsored actor from China. Active since mid-2021, Volt Typhoon has targeted critical infrastructure organizations in the United States and has affected four countries. The targeted sectors include communications, manufacturing, utilities, transportation, construction, maritime, government, IT, and education, with a focus on espionage and long-term undetected access. Volt Typhoon's campaign is aimed at post-compromise credential access and network system discovery. Microsoft assesses with moderate confidence that the campaign's objective is to develop capabilities to disrupt critical communications infrastructure between the United States and Asia during future crises. The observed behavior of Volt Typhoon aligns with Secureworks' identification of BRONZE SILHOUETTE, which operates on behalf of the People’s Republic of China (PRC) and targets U.S. government and defense organizations for intelligence purposes, reflecting Chinese state-sponsored tradecraft. Given the significant potential impact on customers and the broader security ecosystem, Microsoft emphasizes the need for increased community awareness, thorough investigation, and the implementation of protective measures.

Indicator of compromise

SHA-256

eaef901b31b5835035b75302f94fee27288ce46971c6db6221ecbea9ba7ff9d0
99b80c5ac352081a64129772ed5e1543d94cad708ba2adc46dc4ab7a0bd563f1
baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c
b4f7c5e3f14fb57be8b5f020377b993618b6e3532a4e1eb1eae9976d4130cc74
4b0c4170601d6e922cf23b1caf096bba2fade3dfcf92f0ab895a5f0b9a310349
c0fc29a52ec3202f71f6378d9f7f9a8a3a10eb19acb8765152d758aded98c76d
d6ab36cb58c6c8c3527e788fc9239d8dcc97468b6999cf9ccd8a815c8b4a80af
9dd101caee49c692e5df193b236f8d52a07a2030eed9bd858ed3aaccb406401a
450437d49a7e5530c6fb04df2e56c3ab1553ada3712fab02bd1eeb1f1adbc267
93ce3b6d2a18829c0212542751b309dacbdc8c1d950611efe2319aa715f3a066
7939f67375e6b14dfa45ec70356e91823d12f28bbd84278992b99e0d2c12ace5
389a497f27e1dd7484325e8e02bbdf656d53d5cf2601514e9b8d8974befddf61
c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b
e453e6efc5a002709057d8648dbe9998a49b9a12291dee390bb61c98a58b6e95
6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff
cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984
8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2
d17317e1d5716b09cee904b8463a203dc6900d78ee2053276cc948e4f41c8295
472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d
3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642
eaef901b31b5835035b75302f94fee27288ce46971c6db6221ecbea9ba7ff9d0

17506c2246551d401c43726bdaec800f8d41595d01311cf38a19140ad32da2f4
8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2
d17317e1d5716b09cee904b8463a203dc6900d78ee2053276cc948e4f41c8295
472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d
3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642
baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c
b4f7c5e3f14fb57be8b5f020377b993618b6e3532a4e1eb1eae9976d4130cc74
4b0c4170601d6e922cf23b1caf096bba2fade3dfcf92f0ab895a5f0b9a310349
c0fc29a52ec3202f71f6378d9f7f9a8a3a10eb19acb8765152d758aded98c76d
d6ab36cb58c6c8c3527e788fc9239d8dcc97468b6999cf9ccd8a815c8b4a80af
9dd101caee49c692e5df193b236f8d52a07a2030eed9bd858ed3aaccb406401a
450437d49a7e5530c6fb04df2e56c3ab1553ada3712fab02bd1eeb1f1adbc267
93ce3b6d2a18829c0212542751b309dacbdc8c1d950611efe2319aa715f3a066
7939f67375e6b14dfa45ec70356e91823d12f28bbd84278992b99e0d2c12ace5
389a497f27e1dd7484325e8e02bbdf656d53d5cf2601514e9b8d8974befddf61
c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b
e453e6efc5a002709057d8648dbe9998a49b9a12291dee390bb61c98a58b6e95
6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff
cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984
17506c2246551d401c43726bdaec800f8d41595d01311cf38a19140ad32da2f4
17506c2246551d401c43726bdaec800f8d41595d01311cf38a19140ad32da2f4

SHA-1

04423659f175a6878b26ac7d6b6e47c6fd9194d1

ffb1d8ea3039d3d5eb7196d27f5450cac0ea4f34

ffdb3cc7ab5b01d276d23ac930eb21ffe3202d11

35b909b27f0c35f21f32b2a5a6d1a4e065494c9a

MD5

e37bf229890ac181bdef1ad8ee0c2

5c0061445ac2f8e6cadf694e54146914

7f8e8722da728b6e834260b5a314cbac

f9943591918adeeeee7da80e4d985a49

6ed4f5f04d62b18d96b26d6db7c18840

3a97d9b6f17754dcd38ca7fc89caab04

Remediation

- Enhanced Monitoring: Deploy advanced threat detection and continuous monitoring.
- Credential Security: Enforce multi-factor authentication and strong password policies.
- Network Segmentation: Implement network segmentation and strict access controls.
- Patch Management: Regularly update systems and conduct vulnerability assessments.
- Employee Training: Conduct cyber security awareness training.
- Incident Response: Develop and drill incident response plans.
- Block all IOCs on your XDR, EDR and other security tools.

THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

Cyber Threat Advisory

Secure your byte world

+1 (832) 27 2738

info@threatcure.net

https://threatcure.net