US Coast Guard Cyber Command
Maritime Cyber Alert 01-23

May 26, 2023

Information Sharing Protocol: TLP: CLEAR (https://www.us-cert.gov/tlp)

Threat from People's Republic of China State-Sponsored Cyber Actor VOLT TYPHOON

Summary:

The Coast Guard would like to amplify the recently released Joint Cybersecurity Advisory (CSA) and Microsoft Blogpost that highlight recent People's Republic of China (PRC) sponsored cyber activity seen across U.S. critical infrastructure, including the Marine Transportation System (MTS). Known affected organizations have included communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors. Volt Typhoon's primary tactics, techniques, and procedures (TTPs) is "living off the land", which uses built-in network administration tools to perform their objectives. This TTP allows the actor to evade detection by blending in with normal Windows system and network activities, avoid endpoint detection and response (EDR) products that would alert on the introduction of third-party applications to the host, and limit the amount of activity that is captured in default logging configurations.

Volt Typhoon Activity:

Observed behavior indicates the threat actor intends to perform espionage and maintain access without being detected for as long as possible. Microsoft has observed Volt Typhoon achieve initial access through internet facing Fortinet FortiGuard devices. Both the Microsoft Blogpost and the Joint CSA include numerous Indicators of Compromise and examples of techniques Volt Typhoon has used to conduct their activities while remaining undetected. The following is an overview of the process they follow:

- Issuing commands via the command line to:
  - Collect data, including credentials from local and network systems;
  - Stage it for exfiltration; and
  - Use the stolen valid credentials to maintain persistence.
- Blending into normal network activity by:
  - Routing traffic through compromised small office and home office (SOHO) network equipment, including routers, firewalls, and VPN hardware. This includes SOHO network edge devices manufactured by ASUS, Cisco, D-Link, NETGEAR, and Zyxel.
  - Using custom versions of open-source tools to establish a command and control (C2) channel over proxy to further stay under the radar.

Mitigation Measures:

The Coast Guard strongly encourages every company to review the advisory and harden their cyberspace terrain by searching for and mitigating any instances of the highlighted Indicators of Compromise within their own networks and systems. More detailed mitigation instructions can be found within the Joint CSA.

If malicious activity is discovered, companies should follow normal reporting procedures in accordance with their Incident Response Plans, which includes reporting such discoveries to the National Response Center (NRC) or local Coast Guard unit. Companies unable to take discovery actions highlighted in the advisory, or those who would like additional assistance, should contact their local USCG Cyber Specialist or email the Maritime Cyber Readiness Branch at maritimecyber@uscg.mil. The Coast Guard has subject matter experts standing by to answer questions and provide information about Coast Guard Cyber Protection Team services, or for immediate assistance call the Coast Guard Cyber Command 24x7 Watch at (202) 372-2904.

References:

Cybersecurity & Infrastructure Security Agency (2023, May 24). *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection.* Retrieved May 24, 2023, from https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF

Microsoft Security Blog. (2023, May 24). *Volt Typhoon targets US critical infrastructure with living-off-the-land techniques.* Retrieved May 14, 2023, from https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

The information contained in this cyber alert is provided for **informational purposes only**. This information is based on common standards and best practices, and the implementation of which does not relieve any domestic, international safety, operational, or material requirements. The USCG does not provide any warranties of any kind regarding this information and shall not be held liable for any damages of any kind that arose out of the results of, or reliance upon this information.