ORDR SECURITY BULLETIN

Volt Typhoon (State-Sponsored Cyber Actor)

By: Pandian Gnanaprakasam, Gowri Sunder Ravi, Srinivas Loke

Summary of Advisory from FBI/CISA

- Actors with malicious intentions, particularly the People's Republic of China-backed Volt Typhoon group, are manipulating small office/home office (SOHO) routers by exploiting software vulnerabilities that manufacturers need to address through secure software engineering.
- More specifically, the Volt Typhoon actors are utilizing security flaws in SOHO routers as springboards to further infiltrate U.S. critical infrastructure entities. The Cybersecurity & Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have issued this warning due to recent and ongoing threat activities.
- They are urging SOHO router manufacturers to incorporate security features into their products from the start and encouraging all SOHO router users to demand higher security standards from the outset.
- "China's hackers are targeting American civilian critical infrastructure, pre-positioning to cause real-world harm to American citizens and communities in the event of conflict," said FBI Director Christopher Wray. "*Volt Typhoon malware enabled China to hide as they targeted our communications, energy, transportation, and water sectors.*"
- These routers were used by the group to route their network traffic, enhancing the stealth of their operations, and lowering overhead costs for acquiring infrastructure.

Information about Volt Typhoon: (Also tracked as Insidious Taurus)

- Volt Typhoon is a state-sponsored actor based in China, known for its espionage and information-gathering activities. It has been active since mid-2021 and has targeted critical infrastructure organizations in the United States, **spanning various sectors, including communications, manufacturing, utility, transportation, construction, maritime, government, IT, and education.**

- Volt Typhoon employs a variety of tactics, techniques, and procedures (TTPs) to achieve its objectives. One of their primary strategies is the use of "living-off-the-land" techniques, which involve using built-in network administration tools to perform their objectives. This strategy allows the actor to evade detection by blending in with normal Windows system and network activities, avoiding alerts from endpoint detection and response (EDR) products, and limiting the amount of activity captured in default logging configurations.

- They also try to blend into normal network activity by routing traffic through compromised small office and home office (SOHO) network equipment, including routers, firewalls, and VPN hardware.

- Mitigation strategies against Volt Typhoon include identifying and examining the activity of compromised accounts, closing, or changing credentials for compromised accounts, and implementing behavioral monitoring to detect activity that uses normal sign-in channels and system binaries.

- Of importance is the "KV-Botnet," revealed in a report from Lumen's Black Lotus Labs, is designed to infect end of life small-office home-office (SOHO) network devices developed by at least not limited to four different vendors. It comes built with a series of stealth mechanisms and the ability to spread further into local area networks (LANs). Microsoft has confirmed that many of the devices, which include those manufactured by ASUS, Cisco, D-Link, NETGEAR, and Zyxel.

- Since at least February 2022, KV-Botnet has primarily infected SOHO routers like the Cisco RV320, DrayTek Vigor, and Netgear ProSafe product lines. As of mid-November, it expanded to exploit IP cameras developed by Axis Communications.

- Microsoft assesses the *"Volt Typhoon campaign is pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises."*

Prohibited Manufacturers -

Section 889 of the National Defense Authorization Act (NDAA) prohibits the use of federal funds to buy certain telecommunications equipment or services from specific manufacturers. These manufacturers include:

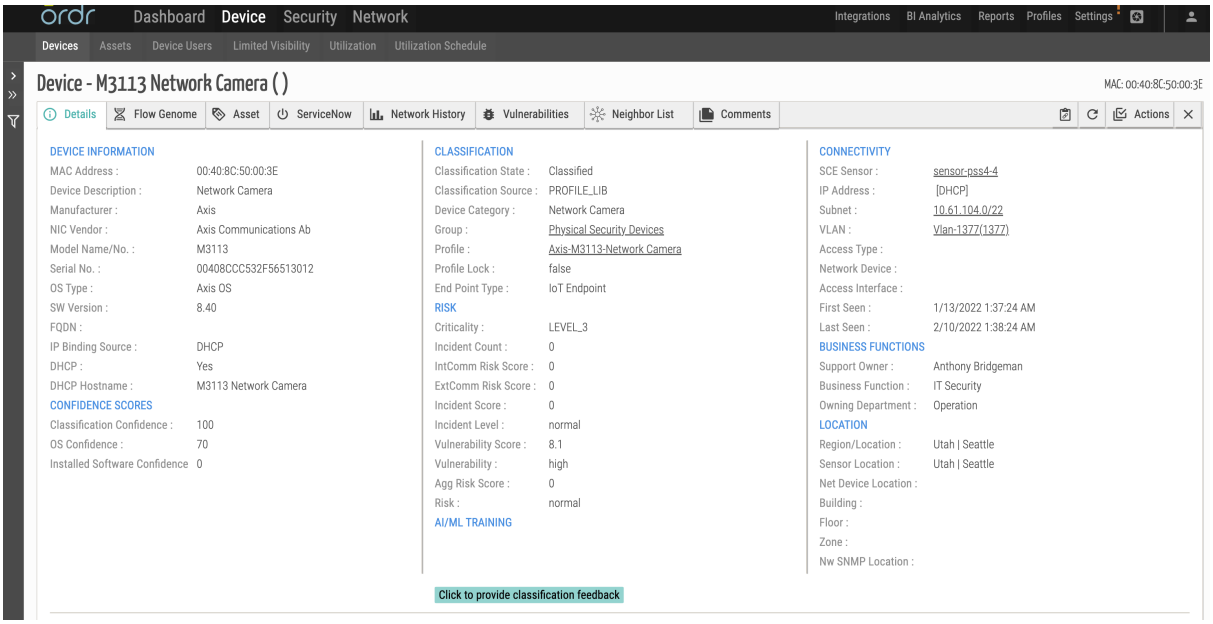
- Huawei Technologies Company
- Hytera Communications Corporation
- ZTE Corporation
- Hangzhou Hikvision Technology Company
- Dahua Technology Company
- Any subsidiary or affiliate of these companies

Section 889 also prohibits the government from contracting with any entity that uses certain telecommunications equipment or services produced by these manufacturers. This prohibition applies to all purchases, regardless of the size of the contract or order.

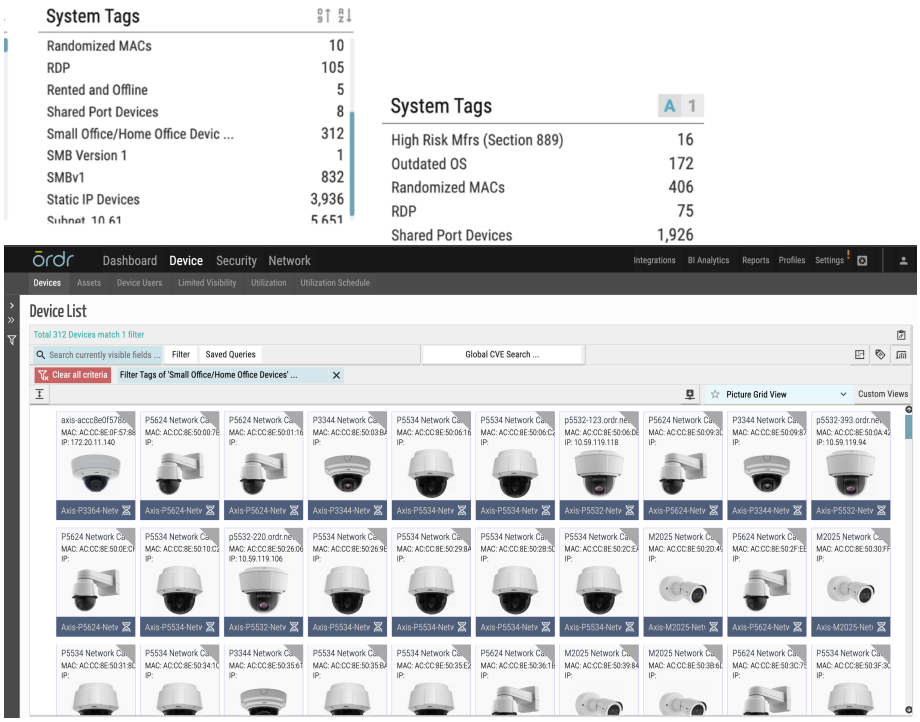
How Ordr Helps

See

- Ordr automatically discovers and classifies and profiles all devices based on the manufacturer, make, and model.



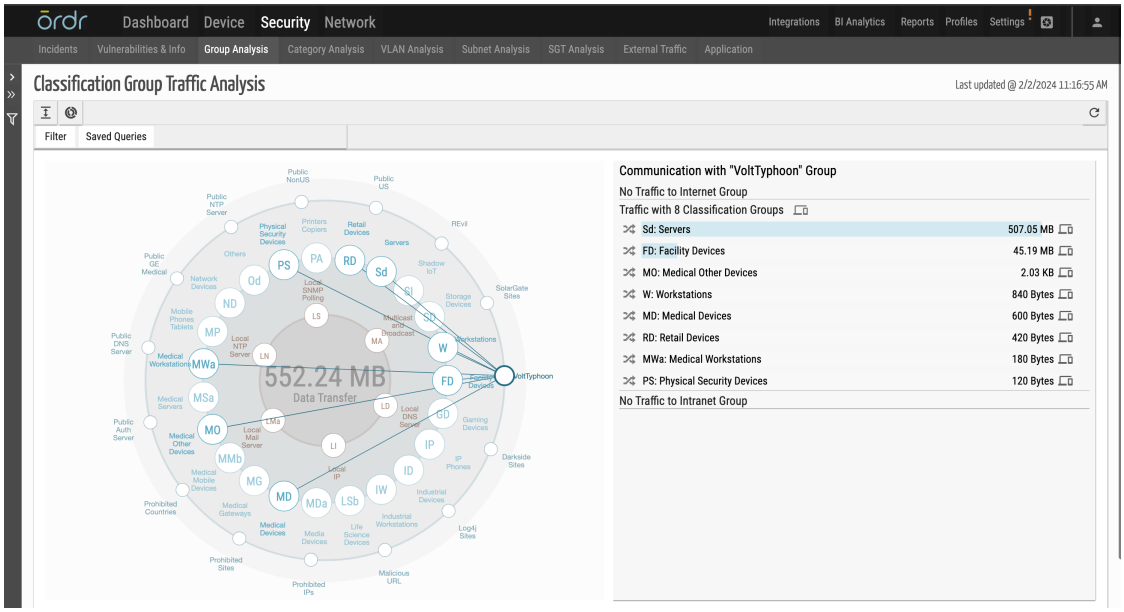
- For this attack Ordr discovers the devices known to be impacted, including the manufacturers like Axis, Netgear, Dray Tek, D-Link, Zyxel. These devices are automatically tagged and can be easily tracked in the system.



  - Ordr identifies and highlights Small Office / Home Offices devices in our customer environment mentioned in the advisories and produces a device download csv/xlsx report from the reports tab for customers to easily download in addition to the ability to lookup devices directly from the tag section.

Know

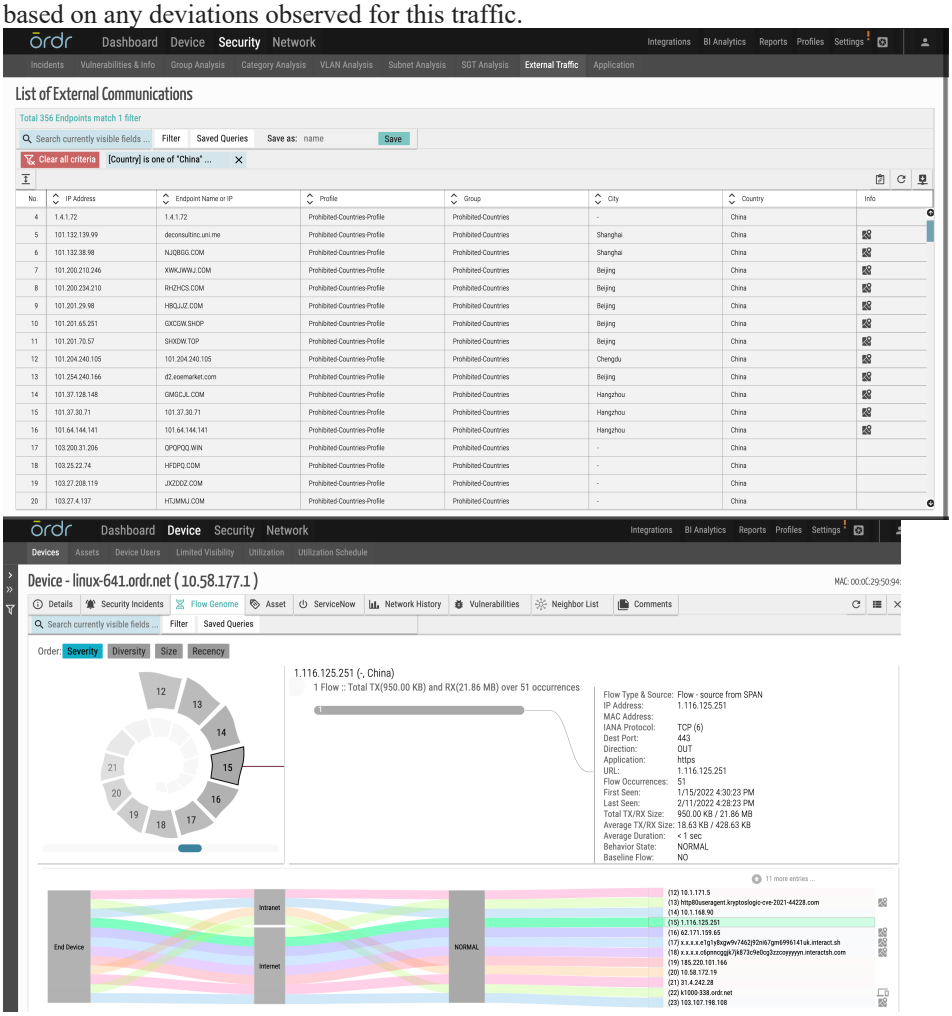
- In real-time, Ordr ‘s external IP/IOC tracks every communication to prohibited IP/URLs.
- Ordr provides in depth insights into category traffic analysis that highlights the communication patterns between devices and external entities, making it easier to see devices communicating to list of prohibited countries including China. All the call back addresses associated with the threat actor Volt Typhoon have been marked accordingly.



- Ordr uses a cloud-based threat intelligence platform where the list is continuously updated, and all communications are marked accordingly in the Ordr Security Threat Card.

- Ordr has an IDS engine that can detect attacks originating from Volt Typhoon and generate alerts based on analysis of packets transacting over the wire.
- IDS Rule: Ordr’s network data collectors process packets for Deep packet inspection and at the same time checks for signatures and this rule that detects presence of “Volt Typhoon User Agent” and generates a high severity alarm.

- Ordr also provides the capability to baseline all the communications based on profile, location, business function, or any customized entity using our AI/ML techniques. Ordr can trigger anomalies based on any deviations observed for this traffic.



Secure

- Ordr provides ability for segmentation of the impacted devices and control access to only must have communications based on zero trust policies.

Other helpful Links:

[1]https://www.crowdstrike.com/cybersecurity-101/living-off-the-land-attacks-lotl/
[2]https://www.cisa.gov/sites/default/files/2024-01/SbD-Alert-Security-Design-Improvements-for-SOHO-Device-Manufacturers.pdf
[3]https://www.darkreading.com/cloud-security/volt-typhoon-soho-botnet-infects-us-govt-entities
[4]https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/
[5] https://www.securityweek.com/wp-content/uploads/2024/01/Volt-Typhoon.pdf
[6]https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF
[7]https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/
[8]https://www.cisa.gov/news-events/news/opening-statement-cisa-director-jen-easterly
[9[https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a