Threat Brief: Attacks on Critical Infrastructure Attributed to Insidious Taurus (Volt Typhoon)

By Unit 42

Published: 2024-02-14 · Archived: 2026-04-02 10:44:43 UTC

Executive Summary

Insidious Taurus (aka Volt Typhoon) is identified by U.S. government agencies and international government partners as People's Republic of China (PRC) state-sponsored cyber actors. This group focuses on pre-positioning themselves within U.S. critical infrastructure IT networks, likely in preparation for disruptive or destructive cyberattacks in the event of a major crisis or conflict with the United States. During a hearing on Jan. 31, 2024, FBI director Christopher Wray told the U.S. House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party that Volt Typhoon was "the defining threat of our generation."

The U.S. government, in collaboration with international government allies, has published two Joint Cybersecurity Advisories (CSA) about this activity. They published the first Joint CSA on May 24, 2023. They published the second Joint CSA on Feb. 7, 2024.

The first CSA discusses the group's use of small office/home office (SOHO) network devices as intermediate infrastructure to obscure their activity. It also describes the use of living-off-the-land techniques and the use of built-in network administration tools to perform objectives, as means of hiding their activity. Palo Alto Networks was credited for providing input on the activity as part of the first CSA.

The second CSA discussed a wider set of techniques used by this group. These techniques include performing extensive pre-compromise reconnaissance, the exploitation of known or zero-day vulnerabilities in public-facing network appliances to gain initial access, and a focus on gaining administrator credentials within a victim environment.

The U.S. Department of Justice published a press release on Jan. 31 stating that a court-authorized operation has disrupted a botnet of hundreds of U.S.-based SOHO devices infected with the KV-botnet. The KV-botnet has been used by multiple different threat actors, including Insidious Taurus.

The vast majority of the devices included in the botnet were routers that were vulnerable because they were no longer supported through their manufacturer's security patches or other software updates. Threat actor groups chain together compromised devices within this botnet to form a covert data transfer network.

Despite the disruption of the KV-botnet, Insidious Taurus remains an ongoing threat and cyberattacks targeting critical infrastructure warrant special attention. Unit 42 will continue to update this threat brief as more information becomes available.

Palo Alto Networks customers are better protected from Insidious Taurus through the following:

- Next-Generation Firewall with the Advanced Threat Prevention security subscription can help block the attacks with Threat Prevention signatures.
- Advanced Threat Prevention has an inbuilt machine learning-based detection that can detect exploits in real time.
- Advanced URL Filtering and DNS Security identify known IPs and domains associated with this group as malicious.
- Cortex XSOAR can automate workflows for data enrichment, indicators of compromise (IoC) hunting and remediation actions to reduce manual work and speed up the patching process.
- Cortex XDR and XSIAM agent helps protect against the techniques executed by this threat actor using Behavioral Threat Protection and its multiple security modules. Cortex Analytics has multiple detection models covering the techniques, with additional relevant coverage by the Identity Analytics module.
- Cortex Xpanse is able to detect a wide range of internet-exposed SOHO devices.
- Prisma Cloud agents have detection for all known Insidious Taurus malware samples listed within WildFire.
- Prisma Access has detection for all known Insidious Taurus malware samples within WildFire and all related threat signatures will be detectable at services turnup.

Organizations can engage the Unit 42 Incident Response team for specific assistance with this threat and others.

Adversary Attack Methodology

In late 2021, Unit 42 observed a threat actor (now identified as Insidious Taurus) using a then-undisclosed Zoho ManageEngine ADSelfService Plus vulnerability (CVE-2021-40539) for initial access. While performing incident response activities, Unit 42 identified a connection to a network-attached storage (NAS) server with FTP running. We found a sample of SockDetour in the trash of that NAS.

SockDetour is a custom backdoor used to maintain persistence, designed to serve as a backup backdoor in case a threat actor's primary one is removed. The tactics and techniques used during this event aligned with what Microsoft then called DEV-0391, which is now known as Volt Typhoon.

Insidious Taurus also uses one rarely used malware family, EarthWorm, as well as custom versions of open-source tools Impacket and Fast Reverse Proxy. Employment of these tools further underscores our assessment of the attackers' technical skill and their focus on remaining undetected.

Exploiting vulnerabilities in internet-facing devices is a known initial access vector for Insidious Taurus. They are believed to have the capability to identify and develop their own zero-day exploits while also taking advantage or publically disclosed vulnerabilities and exploits.

Once initial access has been achieved, a common attribute of attacks is the need to generate as little malicious activity as possible to evade detection and blocking by protection software. Getting caught at all, let alone quickly, precludes operational success.

Insidious Taurus actors take multiple steps to avoid detection, showing an overall technical ability only seen with advanced attackers. One of the ways they do this is by using compromised SOHO devices. Originating attacks from households or small businesses aids attackers because many do not have significant security protections in place.

In addition to requiring manual software updates, SOHO devices are also rarely configured according to best practices by users and they have network management interfaces exposed directly online. Because of these things, many attackers of all motivations – including botnets – also recognize and use SOHO devices for malicious activity. This was true for the case Unit 42 worked in late 2021 where a connection led to the identification of the compromised NAS server.

Another common technique Insidious Taurus has used to remain undetected, formerly the sole realm of advanced attackers but now more widely used, is a technique known as living off the land. This is when attackers abuse legitimate tools – often those used by system administrators for legitimate purposes – for malicious use.

If captured in logs, this activity often looks similar to legitimate network administration use. This includes network enumeration, determining account permissions and even password recovery tools. Because of their widespread legitimate use, these tools are often on allow lists for download and can be difficult to detect when used for malicious activity.

Another way actors can hide their activity when interacting with victim networks, is to carry out their work using direct hands-on keyboard activity vs using scripts to automate activity. By doing so, the attackers can hamper detection efforts again because their activity appears to be expected, human activity rather than a barrage of scripted commands to detect and interdict. For now, this technique remains one only used effectively by advanced attackers due to the required knowledge and skill.

Interim Guidance

Unit 42 recommends following the guidance provided by CISA in their latest CSA. This includes the following:

- Hardening the attack surface
- Securing credentials and accounts
- Securing and limiting the use of remote access services
- Implementing network segmentation
- Securing cloud assets
- Being prepared through logging, threat modeling and training

Additionally, Unit 42 recommends increasing detection opportunities to identify living off the land attacks.

Unit 42 Managed Threat Hunting Queries

The queries below represent a few ways organizations can hunt for activity that could be related to Insidious Taurus. However, the techniques and IoCs being hunted for here may not be unique to Insidious Taurus and any results should be considered in the context of other identified activity.

```
// Description: Looks for the netsh PortProxy command being used to enable port forwarding

// Ref: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

config case_sensitive = false

|filter action_process_image_name in ("netsh.exe","cmd.exe")

|filter action_process_image_command_line contains "netsh interface portproxy add v4tov4"
```

|fields _time, agent_hostname, actor_effective_username, actor_process_image_path, action_process_image_command_line

// Description: Looks for the creation of a PortProxy registry key

// Ref: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

config case_sensitive = false

|dataset = xdr_data

|filter event_type = ENUM.REGISTRY AND (event_sub_type in (ENUM.REGISTRY_CREATE_KEY, ENUM.REGISTRY_SET_VALUE))

|filter action_registry_key_name = "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\PortProxy\v4tov4\tcp"

|fields _time, agent_hostname, actor_effective_username, actor_process_image_name, actor_process_command_line, event_type, event_sub_type, action_registry_key_name, action_registry_data

// Description: Looks for WMIC information gathering command observed being used by Volt Typhoon

// Ref: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

config case_sensitive = false

|dataset = xdr_data

|filter event_type = ENUM.PROCESS and event_sub_type = ENUM.PROCESS_START

|filter action_process_image_name = "wmic.exe" and actor_process_image_name = "cmd.exe" and action_process_image_command_line contains "path win32_logicaldisk get caption,filesystem,freespace,size,volumename"

|fields _time,agent_hostname,actor_effective_username,actor_process_image_name,actor_process_command_line,action_process_image_command_line

// Description: Look for attempts to dump NTDS.dit to disk via Ntdsutil IFM command

// Ref: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

config case_sensitive = false

|dataset = xdr_data

|filter action_process_image_name = "ntdsutil.exe" AND (action_process_image_command_line contains "ac i ntds" or action_process_image_command_line contains "activate instance ntds") and action_process_image_command_line contains "create full"

|fields _time,agent_hostname,actor_effective_username,actor_process_image_path,action_process_image_command_line

// Description: Look for instances of cmd.exe being spawned with arguments consistent with the usage of Impacket's Wmiexec

// Ref: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

config case_sensitive = false

|dataset = xdr_data

|filter event_type = ENUM.PROCESS AND event_sub_type = ENUM.PROCESS_START

|filter os_actor_process_image_name = "wmiprvse.exe" AND action_process_image_name = "cmd.exe" AND action_process_image_command_line contains """/Q /c * \\\\127.0.0.1\\ADMIN$__* 2>&1"""

|fields _time, agent_hostname, actor_effective_username, os_actor_process_image_name, action_process_image_command_line

```
// Description: Looks for the execution of binaries matching the Indicators of compromise (IoCs) in the Volt Typhoon CSA report

// Ref: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

config case_sensitive = false

|dataset = xdr_data

|filter event_type = ENUM.PROCESS AND event_sub_type = ENUM.PROCESS_START

|filter action_process_image_sha256 in
("f4dd44bc19c19056794d29151a5b1bb76afd502388622e24c863a8494af147dd","ef09b8ff86c276e9b475a6ae6b54f08ed77e09e169f7fc0872eb1d42

|fields _time,agent_hostname,actor_effective_username,actor_process_image_path,action_process_image_path,action_process_image_command_li
```

```
// Description: Looks for file writes matching the Indicators of compromise (IoCs) in the Volt Typhoon CSA report

// Ref: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

config case_sensitive = false

|dataset = xdr_data

|filter event_type = ENUM.FILE and event_sub_type = ENUM.FILE_WRITE

|filter action_file_sha256 in
("f4dd44bc19c19056794d29151a5b1bb76afd502388622e24c863a8494af147dd","ef09b8ff86c276e9b475a6ae6b54f08ed77e09e169f7fc0872eb1d42

|fields _time, agent_hostname, actor_effective_username, actor_process_image_path, actor_process_command_line, action_file_path, action_file_sh
```

```
// Description: Looks for the execution of known Volt Typhoon Fast Reverse Proxy (frp) binaries

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

config case_sensitive = false

|dataset = xdr_data

|filter event_type = ENUM.PROCESS AND event_sub_type = ENUM.PROCESS_START

|filter action_process_image_sha256 in
("baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c","b4f7c5e3f14fb57be8b5f020377b993618b6e3532a4e1eb1eae9976d41

|fields _time,agent_hostname,actor_effective_username,actor_process_image_path,action_process_image_path,action_process_image_command_li
```

Conclusion

Based on the available public information, Unit 42 assesses Insidious Taurus as a top tier, sophisticated APT. We concur with the attribution made in both Joint Cyber Security Advisories that this activity is associated with a PRC state-sponsored actor.

As activity from Insidious Taurus is challenging to detect, we agree with the CSA's recommendations to focus on a few key areas. This includes mitigation activities such as updating any internet facing device like SOHO equipment or virtual private networks (VPNs), as threat actors use these devices as part of a botnet or as an initial access vector.

These recommendations also include strengthening the use of multifactor authentication. And finally, it includes prioritizing sufficient logging, which can be especially important for detecting activity within an environment that could be indicative of living off the land techniques. Additional detailed guidance on actions to take can be found in the latest Joint CSA.

Palo Alto Networks customers are better protected through our products, as listed below. We will update this threat brief as more relevant information becomes available.

Palo Alto Networks Product Protections for Insidious Taurus

Palo Alto Networks customers can leverage a variety of product protections and updates designed to identify and defend against this threat.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks is offering a no-cost, no-obligation emergency bundle for organizations to help identify and mitigate any exposure to Insidious Taurus's use of exploits that target vulnerabilities in various networking gear, including an Attack Surface Assessment and a Prisma Access 90-day license.

This offer is promotional and subject to availability. Due to the rapidly changing nature of this vulnerability, Palo Alto Networks reserves the right to update this offer.

Next-Generation Firewalls and Prisma Access With Advanced Threat Prevention

The Next-Generation Firewall with the Advanced Threat Prevention security subscription can help block the attacks via the following Threat Prevention signatures: 91676, 92734, 91362, 90829, 91363, 86360, 90926, 90952, 90972, 90851, 83202, 85739.

Advanced Threat Prevention provides inline machine learning that can help detect vulnerability exploits in real time.

Prisma Access

All known Insidious Taurus malware samples within WildFire and all related threat signatures will be detectable by Prisma Access at services turnup.

Prisma Access is a centralized cloud-delivered security service that uses a Zero Trust Strategy. It enforces the principles of least privilege and continuous trust verification to not only limit access to users based on need, but also to continually monitor changes in application workloads. It also monitors user behavior using cutting-edge machine learning and artificial intelligence to deliver best in breed alerts and mitigation. This establishes protection beyond initial access and can help limit or prevent impact to operations in the case of attempted compromise.

The environment is automatically updated and protected with the latest inline machine learning-powered threat prevention technologies, such as WildFire, Advanced URL Filtering, Advanced Threat Prevention and more. Prisma Access provides a continuous and dynamic security inspection ecosystem that can stop even zero-day threats.

By using machine learning-based detection, Prisma Access is able to provide detection and response to zero-day threats in real time, preventing even some of the most complex attacks that exist in the security landscape today.

Prisma Access also offers advanced DLP protection to protect access and data integrity to all applications and data-based workloads across a customer organization.

Cortex XSOAR

Cortex XSOAR can automate workflows for data enrichment, IoC hunting and remediation actions to reduce manual work and speed up the patching process.

Cortex XDR and XSIAM

Cortex XDR and XSIAM agent helps protect against the techniques executed by this threat actor using Behavioral Threat Protection and its multiple security modules.

Cortex Analytics has multiple detection models covering the techniques, with additional relevant coverage by the Identity Analytics module.

Cortex Xpanse

Cortex Xpanse is able to detect a wide range of internet-exposed SOHO devices including those manufactured by Cisco, NETGEAR, D-Link, ASUS, H3C, Xiaomi, MikroTik, and more with over 20 different individual rules available.

Cloud-Delivered Security Services for Next-Generation Firewall

Advanced URL Filtering and DNS Security identify known IPs and domains associated with this group as malicious.

Prisma Cloud

All known Insidious Taurus malware samples listed within WildFire will be detectable by Prisma Cloud agents.

Prisma Cloud continuously monitors for malicious traffic. By integrating the threat intelligence data from WildFire, Prisma Cloud agents are able to detect and protect cloud virtual machines, container and serverless runtime environments from the execution of malicious runtime operations originating from our customers' cloud environments.

Additional Resources

- Joint Cybersecurity Advisory: People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection [PDF] – Cybersecurity and Infrastructure Security Agency (CISA)
- Volt Typhoon targets US critical infrastructure with living-off-the-land techniques – Microsoft Threat Intelligence
- PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure – Cybersecurity and Infrastructure Security Agency (CISA)
- Identifying and Mitigating Living Off the Land Techniques [PDF] – Cybersecurity and Infrastructure Security Agency (CISA)
- U.S. government disrupts botnet People's Republic of China used to conceal hacking of critical infrastructure – U.S. Attorney's Office, Southern District of Texas
- KV-Botnet: Don't Call It A Comeback – Black Lotus Labs, Lumen
- Secure by Design Alert: Security Design Improvements for SOHO Device Manufacturers – Resources, Cybersecurity and Infrastructure Security Agency (CISA)
- Routers Roasting On An Open Firewall: The KV-Botnet Investigation – Black Lotus Labs, Lumen
- MAR-10448362-1.v1 Volt Typhoon – Analysis Report, Cybersecurity and Infrastructure Security Agency (CISA)
- Volt Typhoon Compromises 30% of Cisco RV320/325 Devices in 37 Days – SecurityScorecard

Updated May 26, 2023, at 3:27 p.m. PT.

Updated Feb. 14, 2024, at 2:25 p.m. PT.

Updated Feb. 20, 2024, at 11:27 a.m. PT to add promotional offer.

Table of Contents

Related Articles

- Phantom Taurus: A New Chinese Nexus APT and the Discovery of the NET-STAR Malware Suite
- Threat Actor Groups Tracked by Palo Alto Networks Unit 42 (Updated Aug. 1, 2025)
- Squidoor: Suspected Chinese Threat Actor's Backdoor Targets Global Organizations

Enlarged Image
