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

unit42.paloaltonetworks.com/volt-typhoon-threat-brief/

Unit 42 May 26, 2023

By Unit 42

May 26, 2023 at 2:30 PM

Category: Threat Briefs and Assessments

Tags: China, Cloud-Delivered Security Services, Cortex XDR, Cortex XSIAM, Cortex XSOAR, Insidious Taurus, next-generation firewall, Prisma Access, Prisma Cloud, threat prevention, Volt Typhoon

This post is also available in: 日本語 (Japanese)

Executive Summary

On May 24, 2023, a Joint Cybersecurity Advisory was published by multiple intelligence agencies, working with private sector partners, disclosing several cyberattacks from nation-state threat actors. The group associated with this attack, known as Volt Typhoon (tracked by Unit 42 as Insidious Taurus), has been attributed to the People's Republic of China (PRC) and was conducting operations for espionage purposes.

Unit 42 is tracking Volt Typhoon activity and will continue to update this threat brief as more information becomes available. Palo Alto Networks was credited in the Joint Cybersecurity Advisory for providing input on the activity.

Cyberattacks targeting critical infrastructure warrant special attention in the current geopolitical climate. This activity is additionally noteworthy in that the attackers put significant focus on remaining undetected. They did so by abusing compromised small office and home office (SOHO) devices, using living off the land techniques, and only interacting manually with compromised devices.

Palo Alto Networks customers receive a variety of protections from Volt Typhoon including the following:

- Next-Generation Firewall with the Advanced Threat Prevention security subscription can help block the attacks.
- Advanced Threat Prevention has an inbuilt machine learning-based detection that can detect exploits in real time.
- 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 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.
- Prisma Cloud agents have detection for all known Volt Typhoon malware samples listed within WildFire.
- Prisma Access has detection for all known Volt Typhoon 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.

Additionally, Palo Alto Networks recommends updating any SOHO devices that are forward-facing to the internet. We also recommend for organizations to study activity within their environment to look for unusual behavioral activity associated with a chain of non-malicious binaries running together.

Threat Group Discussed	**Volt Typhoon, Insidious Taurus**

Table of Contents

Current Scope of the Attack

A common attribute of espionage-motivated 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.

The attackers in this case took multiple steps to avoid detection, showing an overall technical ability only seen with advanced attackers. First, the use of compromised SOHO devices aids attackers by causing their activity to originate from households or small businesses. This is an area not commonly accounted for in network security postures by default.

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.

Microsoft Threat Intelligence also published research documenting their insight into this activity. Volt Typhoon reportedly focused on critical infrastructure organizations located in the U.S. and Guam in “the communications, manufacturing, utility, transportation, construction, maritime, government, information technology and education sectors.”

Another common technique Volt Typhoon 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 being used for malicious activity.

Finally, when interacting with victim networks, the attackers also did not make use of scripts to automate activity, instead carrying out this work in direct hands-on keyboard 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 required knowledge and skill.

The use of one rarely used malware family, EarthWorm, as well as custom versions of open source tools Impacket and Fast Resource Proxy, further underscores the Unit 42 team’s assessment of the attackers’ technical skill and their focus on remaining undetected.

Interim Guidance

Unit 42 recommends any person or small business to update any SOHO devices that are forward-facing to the internet. We also recommend for organizations to study activity within their environment to look for unusual behavioral activity associated with a chain of non-malicious binaries running together.

Unit 42 Managed Threat Hunting Queries

```
// 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 co
"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_comma
```

```
// 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","ef09b8ff86c276e9b475a6ae6b54f08ed77e09e169f7fc0872e
|fields _time,agent_hostname,actor_effective_username,actor_process_image_path,action_process_image_path,action_process_image_com
```

```
// 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","ef09b8ff86c276e9b475a6ae6b54f08ed77e09e169f7fc0872e
|fields _time, agent_hostname, actor_effective_username, actor_process_image_path, actor_process_command_line, action_file_path, action
```

```
// 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-techniqu

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","b4f7c5e3f14fb57be8b5f020377b993618b6e3532a4e1eb1eae9
|fields _time,agent_hostname,actor_effective_username,actor_process_image_path,action_process_image_path,action_process_image_com
```

Conclusion

Based on the available public information, Unit 42 assesses Volt Typhoon as a top tier, sophisticated APT focused on espionage. We concur with the Joint Cybersecurity Advisory attribution that this activity is associated with a PRC state-sponsored actor.

As they are challenging to detect, we recommend any person or small business first update any SOHO devices that are forward-facing to the internet. We also recommend scrutinizing activity within their environment to look for unusual behavioral activity associated with a chain of non-malicious binaries running together.

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

Palo Alto Networks Product Protections for Volt Typhoon

Palo Alto Networks customers can leverage a variety of product protections and updates 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

Next-Generation Firewalls and Prisma Access With Advanced Threat Prevention

1. 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.
2. Advanced Threat Prevention provides inline machine learning that can detect vulnerability exploits in real time.

Prisma Access

All known Volt Typhoon 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.

Prisma Cloud

All known Volt Typhoon 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

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