DCO COBRA and SOSSEC - CYBER TALK

Feb 1st, 2024

Presenter:
Mandiant, now part of Google Cloud

Program Title: **Volt Typhoon Threat Actor Group Targeting US Critical Infrastructure!**

Presentation Speakers:

Mr. Andy DiFazio, ***Mandiant – DoD & IC***
Mr. Aaron Cherrington, ***Mandiant – Sr. Principal Threat Intelligence Analyst***

Volt Typhoon Overview

China is capable of launching cyber-attacks that could disrupt critical infrastructure services within the U.S. and allied nations, including against:

- Oil and gas pipelines
- Rail systems
- Aviation
- Ports
- Electric
- Maritime
- Water
- Electronic component manufacturers
- Defense Industrial Base

Chinese Advanced Persistent Threat (APT) Actors have been observed gaining credentialed access into U.S. Critical Infrastructure entities to likely slow or stop a U.S. Military response effort in a Taiwan invasion scenario.

Background

- Tracked internally as UNC3236 and a number of other designators
- Initially observed by Mandiant in 2021 targeting ADSelfService Plus authentication bypass vulnerability in Zoho ManageEngine ServiceDesk Plus
    - Technical evidence points to efforts since 2020.
- ~~It's unclear the true intent of the intent of the activity~~
    - The extent of the activity against critical infrastructure and the highly targeted nature is concerning.
    - Strong emphasis on concealment

Motivation

At the House Select Committee on CCP, witnesses stated:

- *Chinese hackers are positioning on American infrastructure* ***in preparation to wreak havoc and cause real world harm****.... if and when China decides to strike.* --FBI Director Wray

At the House Select Committee on CCP on 31 January 2024, witnesses included:

- **General Paul Nakasone, Commander, United States Cyber Command**
- **Ms. Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency**
- **Mr. Christopher Wray, Director, Federal Bureau of Investigation**
- **Mr. Harry Coker, Jr., Director, Office of the National Cyber Director**

Motivation

At the House Select Committee on CCP, witnesses stated:

- *In recent years, we have seen a deeply concerning evolution in chinese targeting of US critical infrastructure. In particular, we have seen Chinese actors, including Volt Typhoon, burrowing deep into our critical infrastructure to enable destructive attacks in the event of a major crisis or conflict. - -CISA Director Easterly*
    - *Through the disruption of our pipelines, the severing of our telecommunications, the pollution of our water facilities, the crippling of our transportation modes* ***all to ensure that they can incite societal panic and chaos and to deter our ability to marshall military might, and civilian will.***

Initial Access

- Exploits edge devices
- Known vulnerabilities leveraged:
  - CVE-2021-40539 – Zoho ManageEngine AD Self-Service Plus
  - CVE-2021-27860 – FatPipe WARP/IPVPN/MPVPN
- Deliver a custom webshell
  - CISA and Secureworks report that it is likely derived from Awen Webshell
- Crowdstrike identified custom webshells

Challenge: Short bursts of activity. It's not always clear how the threat actor achieves access to the edge device.

Post-Compromise Activity

- Relies on living-off-the-land-techniques
  - Rarely uses malware
- Hands-on-keyboard activities
  - Uses command line, WMIC, and attempts to gain credentials via NTDS.dit through various means
- Known user agents used by the threat actor:
  - `Mozilla/5.0 (Windows NT 6.1; WOW64; rv:68.0) Gecko/20100101 Firefox/68.0`
  - `Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36`
- Selective deletion of Windows and System logs to remove evidence of intrusion and compromise.

Actor's Goal: Maintain persistent access

Challenge: Stealthy efforts to blend make detection more difficult

Command and Control

- Leverage compromised credentials to maintain persistent access and blend
- Route traffic through compromised SOHO edge devices (obfuscation networks)
- Less often:
  - Port forwarding proxies
  - Custom versions of fast reverse proxies (FRP)
  - Possibly derived from the publicly available
  - fatedier FRP or the EarthWorm tunneler

```
wmic  /node:[redacted] /user:[redacted] /password:
[redacted] process call create "cmd.exe /c netsh interface portproxy
add v4tov4 listenport=50100 listenaddress=0.0.0.0
connectport=[redacted] connectaddress=[redacted]"

wmic  /node:[redacted] /user:[redacted] /password:
[redacted] process call create "cmd.exe /c netsh interface portproxy
delete v4to4v listenport=50100 listenaddress=0.0.0.0"
```

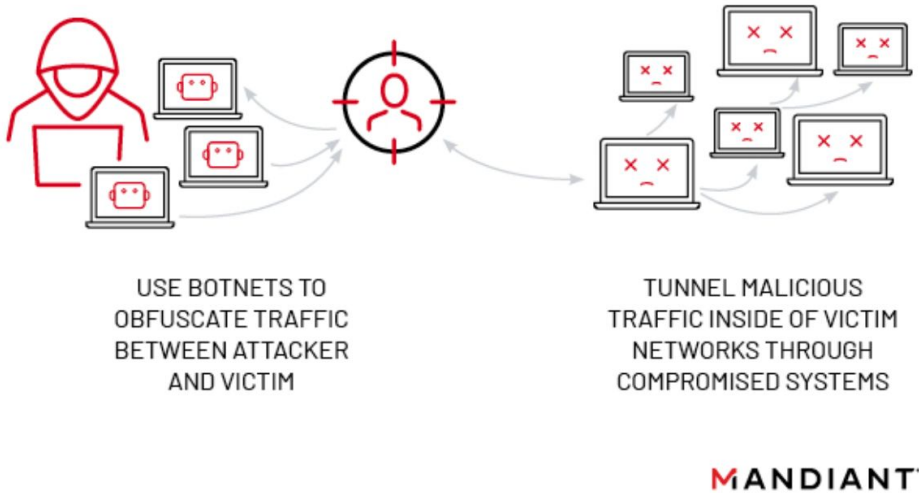
Figure 6. Volt Typhoon commands creating and later deleting a port proxy on a compromised system

Microsoft reported port forwarding proxy activity

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

Challenge: After initial access is achieved the C2 communications can be difficult to detect. The volume of C2 traffic may be minimal with persistent access the primary goal.

PRC Obfuscation Infrastructure



Challenge: Traditional Indicator of Compromise (IOC) blocking techniques will not be as effective to stop or detect actor reconnaissance or initial access.

KV-Botnet and ORBs

The KV-botnet is a network of compromised routers and firewall devices (primarily small office/home office or SOHO models) that are controlled by malicious actors.

- The botnet serves as a hidden network to transfer data and carry out attacks.
- KV-botnet focuses on vulnerable routers, firewalls, and VPN devices from manufacturers like Cisco, DrayTek, Fortinet, and NETGEAR (possibly others). It often targets outdated or end-of-life devices with readily available exploits.
    - Compromises devices through known vulnerabilities or weak login credentials.
    - Employs sophisticated techniques to stay hidden and blend in with legitimate network traffic.
    - Can be used to launch attacks against higher-value targets.
- Volt Typhoon has been identified operating on this infrastructure, but other Chinese threat actors have been leveraging it as well.

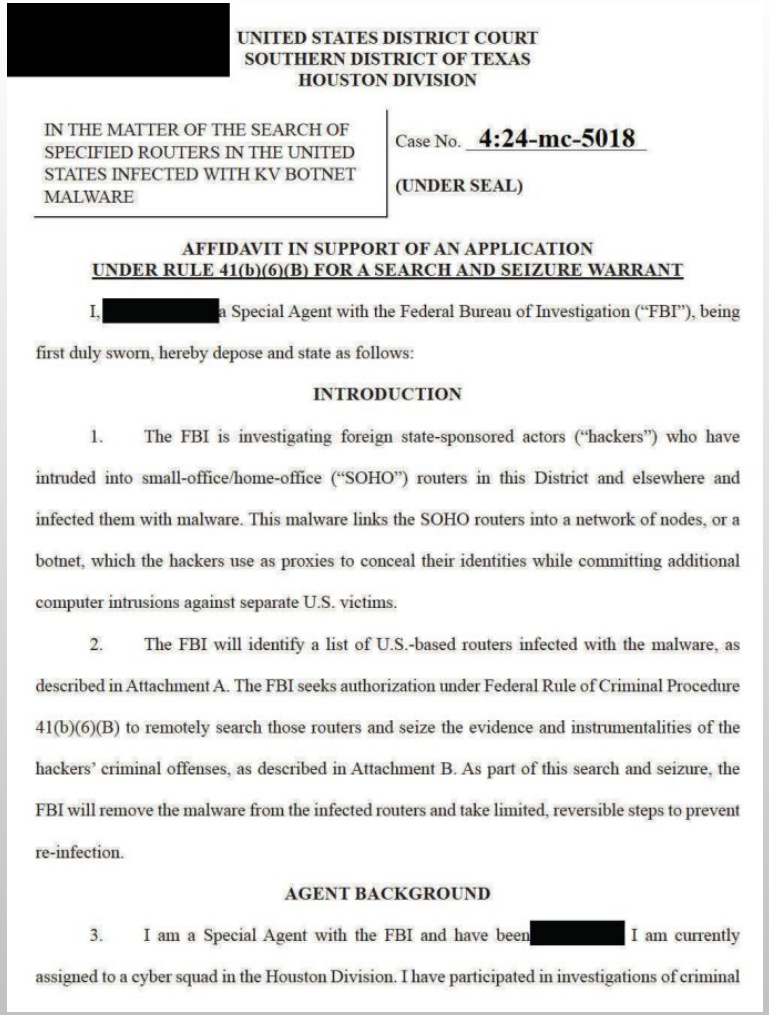
Numerous Chinese APT groups appear to be using Operational Relay Boxes (ORBs), leveraging abused SOHO routers, and placing a higher emphasis on tradecraft

DoJ KV-Botnet Take Down

Four different warrants for CONUS purposes

- Search and Seizure Warrants Signed 06 December 2023 - 09 January 2024.
- Conduct remote search
  - Some sort of tool to gather IP addresses of infected.
  - Limited to US based routers
- Conduct seizure
  - Seizure of data as evidence of the crime
    - Copy then Delete KV-Botnet Malware
  - Prevent reinfection
  - Point remaining malware to only talk to itself
  - Prevent communications between device and other KV-Botnet nodes
  - Stopping KV-Botnet VPN process.

Similar to Cyclops Blink takedown in April 2022



[redacted]

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

IN THE MATTER OF THE SEARCH OF SPECIFIED ROUTERS IN THE UNITED STATES INFECTED WITH KV BOTNET MALWARE

Case No. 4:24-mc-5018

(UNDER SEAL)

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41(b)(6)(B) FOR A SEARCH AND SEIZURE WARRANT

I, [redacted] a Special Agent with the Federal Bureau of Investigation ("FBI"), being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. The FBI is investigating foreign state-sponsored actors ("hackers") who have intruded into small-office/home-office ("SOHO") routers in this District and elsewhere and infected them with malware. This malware links the SOHO routers into a network of nodes, or a botnet, which the hackers use as proxies to conceal their identities while committing additional computer intrusions against separate U.S. victims.

2. The FBI will identify a list of U.S.-based routers infected with the malware, as described in Attachment A. The FBI seeks authorization under Federal Rule of Criminal Procedure 41(b)(6)(B) to remotely search those routers and seize the evidence and instrumentalities of the hackers' criminal offenses, as described in Attachment B. As part of this search and seizure, the FBI will remove the malware from the infected routers and take limited, reversible steps to prevent re-infection.

AGENT BACKGROUND

3. I am a Special Agent with the FBI and have been [redacted] I am currently assigned to a cyber squad in the Houston Division. I have participated in investigations of criminal

Related Activity

Numerous reports have surfaced over the past several years that have styles and techniques that appear to be related in this evolved style of tradecraft. Some of these are Volt Typhoon while others are likely other groups

- Palmerworm (AKA Temp.Overboard)
- HiatusRAT
- KV-Botnet
- ZuoRAT
- Plead Malware
- BlackTech (AKA Temp.Overboard)
- Bronze Silhoutte (AKA Volt Typhoon)
- Various governmental reports

Numerous Chinese APT groups appear to be using Operational Relay Boxes (ORBs), leveraging abused SOHO routers, and placing a higher emphasis on tradecraft

Blacktech / TEMP.Overboard

BlackTech actors use a variety of techniques to evade detection, including:

- Use custom malware, dual-use tools, and living off the land tactics
- Disable logging on routers, to conceal their operations
- Modifying the victim's registry.
- Using stolen code-signing certificates to sign their malware.
- Configuring their tools to evade detection by security software and EDR.
- Patching the system image to modify router firmware.
- Hiding their presence and obfuscating changes made to compromised Cisco routers by hiding Embedded Event Manager (EEM) policies.
- Using a modified bootloader on routers to allow the modified firmware to continue evading detection.

BlackTech (a.k.a. Palmerworm, Temp.Overboard, Circuit Panda, and Radio Panda) actors have targeted government, industrial, technology, media, electronics, and telecommunication sectors, including entities that support the militaries of the U.S. and Japan.

HiatusRAT

Another family of publicly disclosed router malware is HiatusRAT:

- HiatusRAT is a type of malware that infects business-grade routers.
- It uses two malicious files to steal data and turn infected routers into covert proxies.
- The malware can also capture traffic on ports commonly used for email and file transfer.
- Researchers believe the attackers behind HiatusRAT are targeting businesses.
- The article was published in March 2023, but the researchers believe the malware campaign started in July 2022.

US Military: 2023 campaigns showed a shift toward targeting US military procurement systems for reconnaissance purposes.

Taiwan-based Organizations: HiatusRAT has been used in attacks against various Taiwanese organizations, including semiconductor and chemical manufacturers, as well as a municipal government.

Sourcing and further reading

https://blog.lumen.com/new-hiatusrat-router-malware-covertly-spies-on-victims/
https://blog.lumen.com/hiatusrat-takes-little-time-off-in-a-return-to-action/
https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/
https://www.microsoft.com/en-us/security/blog/2023/11/09/microsoft-shares-threat-intelligence-at-cyberwarcon-2023/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a
https://www.secureworks.com/blog/chinese-cyberespionage-group-bronze-silhouette-targets-us-government-and-defense-organizations
https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/
https://www.ithome.com.tw/news/160289
https://www.ic3.gov/Media/News/2023/230927.pdf
https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt
https://www.trendmicro.com/en_us/research/17/f/following-trail-blacktech-cyber-espionage-campaigns.html
https://documents.trendmicro.com/assets/appendix-following-the-trail-of-blacktechs-cyber-espionage-campaigns.pdf
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_8_yi-chin_yu-tung_en.pdf
https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical
https://www.youtube.com/watch?v=MJOX3cpHfUI

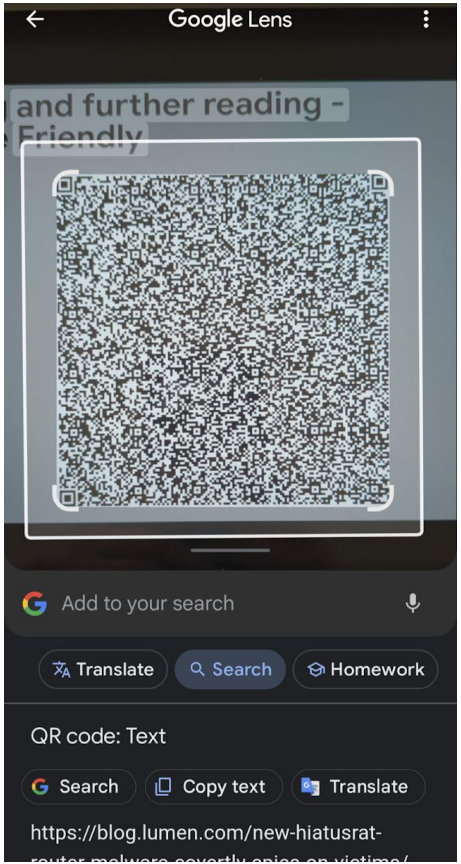
Sourcing and further reading - QR Code Friendly

Ensure that you are using a QR code reader that can read text.

All the links are in there.

Example is Google Lens on the left which isc scanning it, then allows you to copy text at the bottom.

If it doesn't work right now, at least take a picture to play with it later.



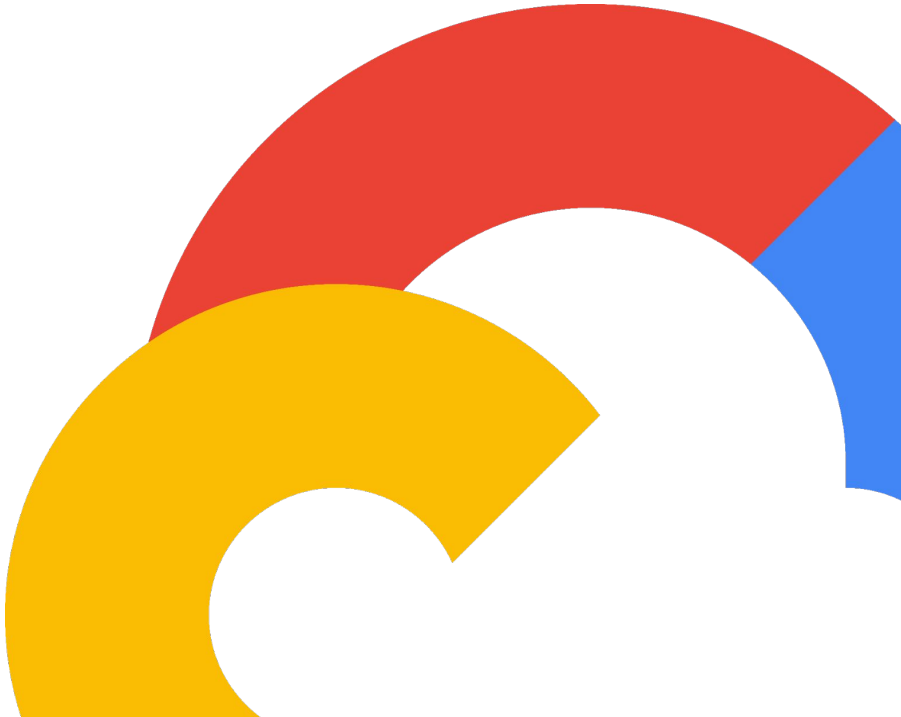
Thank you

For further information please reach out to

Andy DiFazio - DoD + IC
andrewdifazio@google.com
(m) 571.213.7406

MANDIANT
NOW PART OF Google Cloud

Google Cloud



SOSSEC Membership is Required for Award on PEO EIS, DCO Cyberspace Operations Broad Responsive Agreement (COBRA) Other Transaction Agreement (OTA)

Benefits of Joining the SOSSEC Consortium

- ✓ Opportunity to perform work under seven (9) OTAs for the Air Force, Army and National Geospatial-Intelligence Agency
- ✓ Opportunity to build members' business base by applying their technologies/expertise to meeting urgent DoD requirements
- ✓ Simple, streamlined process to compete for DoD work
- ✓ Average 60 days from requirements definition to award
- ✓ Flexible treatment of intellectual property
- ✓ OTA access to any DoD user with approval of OTA customer
- ✓ Transition from Prototype to Production without further competition

Go to **www.sossecinc.com** and click on the **JOIN** Tab to access the membership application. The process is simple and rapid. There is no joining fee, and the membership fee is $500 per year. Membership is open to Industry (traditional, nontraditional, small business), not for profit and academic institutions that share the values of the SOSSEC Consortium.

For questions about SOSSEC COBRA OTA, contact Gene Del Coco at edelcoco@sossecinc.com or Ed Aguirre at eaguirre@sossecinc.com.