People's Republic of China-Linked Cyber Actors Hide in Router Firmware

Executive summary

The United States National Security Agency (NSA), the U.S. Federal Bureau of Investigation (FBI), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Japan National Police Agency (NPA), and the Japan National Center of Incident Readiness and Strategy for Cybersecurity (NISC) (hereafter referred to as the "authoring agencies") are releasing this joint cybersecurity advisory (CSA) to detail activity of the People's Republic of China (PRC)-linked cyber actors known as BlackTech. BlackTech has demonstrated capabilities in modifying router firmware without detection and exploiting routers' domain-trust relationships for pivoting from international subsidiaries to headquarters in Japan and the U.S. — the primary targets. The authoring agencies recommend implementing the mitigations described to detect this activity and protect devices from the backdoors the BlackTech actors are leaving behind.

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. BlackTech actors use custom malware, dual-use tools, and living off the land tactics, such as disabling logging on routers, to conceal their operations. This CSA details BlackTech's tactics, techniques, and procedures (TTPs), which highlights the need for multinational corporations to review all subsidiary connections, verify access, and consider implementing Zero Trust models to limit the extent of a potential BlackTech compromise.

For more information on the risks posed by this deep level of unauthorized access, see the CSA People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices. [1]

Technical details

This advisory uses the MITRE® ATT&CK® for Enterprise framework, version 13.1. See the Appendix: MITRE ATT&CK Techniques for all referenced TTPs.

Background

Active since 2010, BlackTech actors have historically targeted a wide range of U.S. and East Asia public organizations and private industries. BlackTech actors' TTPs include developing customized malware and tailored persistence mechanisms for compromising routers. These TTPs allow the actors to disable logging [T1562] and abuse trusted domain relationships [T1199] to pivot between international subsidiaries and domestic headquarters' networks.

Observable TTPs

BlackTech cyber actors use custom malware payloads and remote access tools (RATs) to target victims' operating systems. The actors have used a range of custom malware families targeting Windows®, Linux®, and FreeBSD® operating systems. Custom malware families employed by BlackTech include:

- BendyBear [S0574]
- Bifrose
- BTSDoor
- FakeDead (a.k.a. TSCookie) [S0436]
- FlagPro [S0696]
- FrontShell (FakeDead's downloader module)
- IconDown
- PLEAD [S0435]
- SpiderPig
- SpiderSpring
- SpiderStack
- WaterBear [S0579]

BlackTech actors continuously update these tools to evade detection [TA0005] by security software. The actors also use stolen code-signing certificates [T1588.003] to

sign the malicious payloads, which make them appear legitimate and therefore more difficult for security software to detect [T1553.002].

BlackTech actors use living off the land TTPs to blend in with normal operating system and network activities, allowing them to evade detection by endpoint detection and response (EDR) products. Common methods of persistence on a host include NetCat shells, modifying the victim registry [T1112] to enable the remote desktop protocol (RDP) [T1021.001], and secure shell (SSH) [T1021.004]. The actors have also used SNScan for enumeration [TA0007], and a local file transfer protocol (FTP) server [T1071.002] to move data through the victim network. For additional examples of malicious cyber actors living off the land, see People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection. [2]

Pivoting from international subsidiaries

The PRC-linked BlackTech actors target international subsidiaries of U.S. and Japanese companies. After gaining access [TA0001] to the subsidiaries' internal networks, BlackTech actors are able to pivot from the trusted internal routers to other subsidiaries of the companies and the headquarters' networks. BlackTech actors exploit trusted network relationships between an established victim and other entities to expand their access in target networks.

Specifically, upon gaining an initial foothold into a target network and gaining administrator access to network edge devices, BlackTech cyber actors often modify the firmware to hide their activity across the edge devices to further maintain persistence in the network. To extend their foothold across an organization, BlackTech actors target branch routers—typically smaller appliances used at remote branch offices to connect to a corporate headquarters—and then abuse the trusted relationship [T1199] of the branch routers within the corporate network being targeted. BlackTech actors then use the compromised public-facing branch routers as part of their infrastructure for proxying traffic [TA0011], blending in with corporate network traffic, and pivoting to other victims on the same corporate network [T1090.002].

Maintaining access via stealthy router backdoors

BlackTech has targeted and exploited various brands and versions of router devices. TTPs against routers enable the actors to conceal configuration changes, hide commands, and disable logging while BlackTech actors conduct operations. BlackTech

actors have compromised several Cisco® routers using variations of a customized firmware backdoor [T1542.004]. The backdoor functionality is enabled and disabled through specially crafted TCP or UDP packets [T1205]. This TTP is not solely limited to Cisco routers, and similar techniques could be used to enable backdoors in other network equipment.

In some cases, BlackTech actors replace the firmware for certain Cisco IOS®-based routers with malicious firmware. Although BlackTech actors already had elevated privileges [TA0004] on the router to replace the firmware via command-line execution, the malicious firmware is used to establish persistent backdoor access [TA0003] and obfuscate future malicious activity. The modified firmware uses a built-in SSH backdoor [T1556.004], allowing BlackTech actors to maintain access to the compromised router without BlackTech connections being logged [T1562.003]. BlackTech actors bypass the router's built-in security features by first installing older legitimate firmware [T1601.002] that they then modify in memory to allow the installation of a modified, unsigned bootloader and modified, unsigned firmware [T1601.001]. The modified bootloader enables the modified firmware to continue evading detection [T1553.006], however, it is not always necessary.

BlackTech actors may also hide their presence and obfuscate changes made to compromised Cisco routers by hiding Embedded Event Manager (EEM) policies—a feature usually used in Cisco IOS to automate tasks that execute upon specified events—that manipulate Cisco IOS Command-Line Interface (CLI) command results. On a compromised router, the BlackTech-created EEM policy waits for specific commands to execute obfuscation measures or deny execution of specified legitimate commands. This policy has two functions: (1) to remove lines containing certain strings in the output of specified, legitimate Cisco IOS CLI commands [T1562.006], and (2) prevent the execution of other legitimate CLI commands, such as hindering forensic analysis by blocking copy, rename, and move commands for the associated EEM policy [T1562.001].

Firmware replacement process

BlackTech actors utilize the following file types to compromise the router. These files are downloaded to the router via FTP or SSH.

Table 1: File types to compromise the router

File Type	Description
Old Legitimate Firmware	The IOS image firmware is modified in memory to allow installation of the Modified Firmware and Modified Bootloader.
Modified Firmware	The firmware has a built-in SSH backdoor, allowing operators to have unlogged interaction with the router.
Modified Bootloader	The bootloader allows Modified Firmware to continue evading the router's security features for persistence across reboots. In some cases, only modified firmware is used.

BlackTech actors use the Cisco router's CLI to replace the router's IOS image firmware. The process begins with the firmware being modified in memory—also called hot patching—to allow the installation of a modified bootloader and modified firmware capable of bypassing the router's security features. Then, a specifically constructed packet triggers the router to enable the backdoor that bypasses logging and the access control list (ACL). The steps are as follows:

1. Download old legitimate firmware.
2. Set the router to load the old legitimate firmware and reboot with the following command(s):

```
config t
no boot system usbflash0 [filename]
boot system usbflash0 [filename]
end
write
reload
```

3. Download the modified bootloader and modified firmware.
4. Set the router to load the modified firmware with the following command(s):

```
conf t
no boot system usbflash0 [filename]
boot system usbflash0 [filename]
end
write
```

5. Load the modified bootloader (the router reboots automatically) with the following command:

```
upgrade rom file bootloader
```

6. Enable access by sending a trigger packet that has specific values within the UDP data or TCP Sequence Number field and the Maximum Segment Size (MSS) parameter within the TCP Options field.

Modified bootloader

To allow the modified bootloader and firmware to be installed on Cisco IOS without detection, the cyber actors install an old, legitimate firmware and then modify that running firmware in memory to bypass firmware signature checks in the Cisco ROM Monitor (ROMMON) signature validation functions. The modified version's instructions allow the actors to bypass functions of the IOS Image Load test and the Field Upgradeable ROMMON Integrity test.

Modified firmware

BlackTech actors install modified IOS image firmware that allows backdoor access via SSH to bypass the router's normal logging functions. The firmware consists of a Cisco IOS loader that will load an embedded IOS image.

BlackTech actors hook several functions in the embedded Cisco IOS image to jump to their own code. They overwrite existing code to handle magic packet checking, implement an SSH backdoor, and bypass logging functionality on the compromised router. The modified instructions bypass command logging, IP address ACLs, and error logging.

To enable the backdoor functions, the firmware checks for incoming trigger packets and enables or disables the backdoor functionality. When the backdoor is enabled, associated logging functions on the router are bypassed. The source IP address is stored and used to bypass ACL handling for matching packets. The SSH backdoor includes a special username that does not require additional authentication.

Detection and mitigation techniques

In order to detect and mitigate this BlackTech malicious activity, the authoring agencies strongly recommend the following detection and mitigation techniques. It would be trivial for the BlackTech actors to modify values in their backdoors that would render specific signatures of this router backdoor obsolete. For more robust detection, network defenders should monitor network devices for unauthorized downloads of bootloaders

and firmware images and reboots. Network defenders should also monitor for unusual traffic destined to the router, including SSH.

The following are the best mitigation practices to defend against this type of malicious activity:

- Disable outbound connections by applying the "transport output none" configuration command to the virtual teletype (VTY) lines. This command will prevent some copy commands from successfully connecting to external systems. **Note:** An adversary with unauthorized privileged level access to a network device could revert this configuration change. [3]

- Monitor both inbound and outbound connections from network devices to both external and internal systems. In general, network devices should only be connecting to nearby devices for exchanging routing or network topology information or with administrative systems for time synchronization, logging, authentication, monitoring, etc. If feasible, block unauthorized outbound connections from network devices by applying access lists or rule sets to other nearby network devices. Additionally, place administrative systems in separate virtual local area networks (VLANs) and block all unauthorized traffic from network devices destined for non-administrative VLANs. [4]

- Limit access to administration services and only permit IP addresses used by network administrators by applying access lists to the VTY lines or specific services. Monitor logs for successful and unsuccessful login attempts with the "login on-failure log" and "login on-success log" configuration commands, or by reviewing centralized Authentication, Authorization, and Accounting (AAA) events. [3]

- Upgrade devices to ones that have secure boot capabilities with better integrity and authenticity checks for bootloaders and firmware. In particular, highly prioritize replacing all end-of-life and unsupported equipment as soon as possible. [3] [5]

- When there is a concern that a single password has been compromised, change all passwords and keys. [3]

- Review logs generated by network devices and monitor for unauthorized reboots, operating system version changes, changes to the configuration, or attempts to update the firmware. Compare against expected configuration changes and patching plans to verify that the changes are authorized. [3]
- Periodically perform both file and memory verification described in the Network Device Integrity (NDI) Methodology documents to detect unauthorized changes to the software stored and running on network devices. [3]
- Monitor for changes to firmware. Periodically take snapshots of boot records and firmware and compare against known good images. [3]

Works cited

[1] Joint CSA, People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices, https://media.defense.gov/2022/Jun/07/2003013376/-1/-1/0/CSA_PRC_SPONSORED_CYBER_ACTORS_EXPLOIT_NETWORK_PROVIDERS_DEVICES_TLPWHITE.PDF
[2] Joint CSA, People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection, https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_PRC_State_Sponsored_Cyber_Living_off_the_Land_v1.1.PDF
[3] NSA, Network Infrastructure Security Guide, https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF
[4] NSA, Performing Out-of-Band Network Management, https://media.defense.gov/2020/Sep/17/2002499616/-1/-1/0/PERFORMING_OUT_OF_BAND_NETWORK_MANAGEMENT20200911.PDF
[5] Cisco, Attackers Continue to Target Legacy Devices, https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government or Japan, and this guidance shall not be used for advertising or product endorsement purposes.

Trademark recognition

Cisco and Cisco IOS are registered trademarks of Cisco Technology, Inc.
FreeBSD is a registered trademark of The FreeBSD Foundation.
Linux is a registered trademark of Linus Torvalds.
MITRE and MITRE ATT&CK are registered trademarks of The MITRE Corporation.
Windows is a registered trademark of Microsoft Corporation.

Purpose

This document was developed in furtherance of the authoring agencies' cybersecurity missions, including their responsibilities to identify and disseminate cyber threats, and to develop and issue cybersecurity specifications and mitigations.

Contact

NSA Cybersecurity Report Questions and Feedback: CybersecurityReports@nsa.gov
NSA's Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
NSA Media Inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov

U.S. organizations: Report incidents and anomalous activity to CISA 24/7 Operations Center at Report@cisa.dhs.gov, cisa.gov/report, or (888) 282-0870 and/or to the FBI via your local FBI field office.

Appendix: MITRE ATT&CK Techniques

See Tables 1-8 for all referenced BlackTech tactics and techniques in this advisory.

Table 1: BlackTech ATT&CK Techniques for Enterprise – Resource Development

Technique Title	ID	Use
Obtain Capabilities: Code Signing Certificates	T1588.003	BlackTech actors use stolen code-signing certificates to sign payloads and evade defenses.

Table 2: BlackTech ATT&CK Techniques for Enterprise – Initial Access

Technique Title	ID	Use
Initial Access	TA0001	BlackTech actors gain access to victim networks by exploiting routers.
Trusted Relationship	T1199	BlackTech actors exploit trusted domain relationships of routers to gain access to victim networks.

Table 3: BlackTech ATT&CK Techniques for Enterprise – Persistence

Technique Title	ID	Use
Persistence	TA0003	BlackTech actors gain persistent access to victims' networks.
Traffic Signaling	T1205	BlackTech actors send specially crafted packets to enable or disable backdoor functionality on a compromised router.
Pre-OS Boot: ROMMONkit	T1542.004	BlackTech actors modify router firmware to maintain persistence.

Table 4: BlackTech ATT&CK Techniques for Enterprise – Privilege Escalation

Technique Title	ID	Use
Privilege Escalation	TA0004	BlackTech actors gain elevated privileges on a victim's network.

Table 5: BlackTech ATT&CK Techniques for Enterprise – Defense Evasion

Technique Title	ID	Use
Defense Evasion	TA0005	BlackTech actors configure their tools to evade detection by security software and EDR.
Modify Registry	T1112	BlackTech actors modify the victim's registry.
Impair Defenses	T1562	BlackTech actors disable logging on compromised routers to avoid detection and evade defenses.
Impair Defenses: Impair Command History Logging	T1562.003	BlackTech actors disable logging on the compromised routers to prevent logging of any commands issued.
Modify System Image: Patch System Image	T1601.001	BlackTech actors modify router firmware to evade detection.

Table 6: BlackTech ATT&CK Techniques for Enterprise – Discovery

Technique Title	ID	Use
Discovery	TA0007	BlackTech actors use SNScan to enumerate victims' networks and obtain further network information.

Table 7: BlackTech ATT&CK Techniques for Enterprise – Lateral Movement

Technique Title	ID	Use
Remote Services: Remote Desktop Protocol	T1021.001	BlackTech actors use RDP to move laterally across a victim's network.

Remote Services: SSH	T1021.004	BlackTech actors use SSH to move laterally across a victim's network.

Table 8: BlackTech ATT&CK Techniques for Enterprise – Command and Control

Technique Title	ID	Use
Command and Control	TA0011	BlackTech actors compromise and control a victim's network infrastructure.
Application Layer Protocol: File Transfer Protocols	T1071.002	BlackTech actors use FTP to move data through a victim's network or to deliver scripts for compromising routers.
Proxy	T1090	BlackTech actors use compromised routers to proxy traffic.