Hive Pro®

Threat Level

Red

✓ CISA: AA23-270A

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

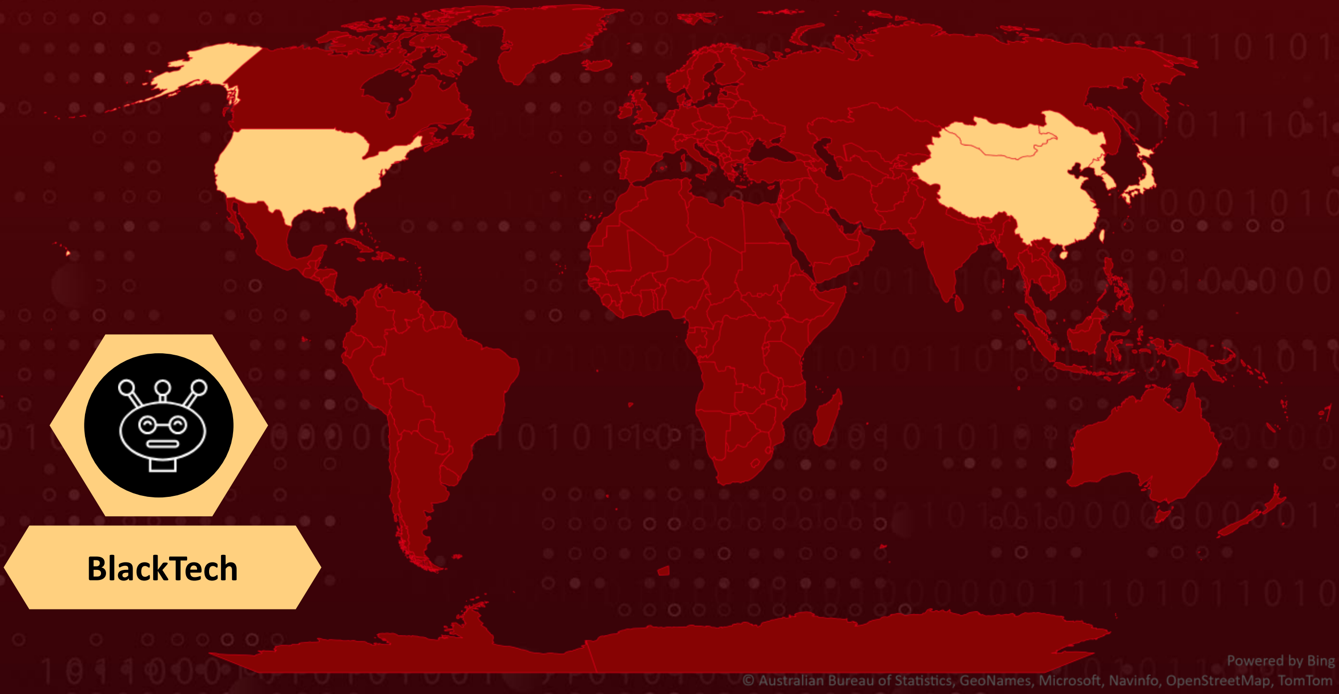
BlackTech: China-Linked Cyber Actors Exploit Router Firmware

Date of Publication	Admiralty code	TA Number
September 29, 2023	A1	TA2023393

Summary

First Appearance: 2010
Actor Name: BlackTech (a.k.a. Palmerworm, Temp.Overboard, Circuit Panda, and Radio Panda)
Target Region: U.S. and East Asia
Affected Platforms: Windows, Linux, and FreeBSD
Target Sectors: Government, industrial, technology, media, electronics, telecommunication, military

Actor Map


BlackTech
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Actor Details

#1 BlackTech is a cyber actor group that has been active since 2010, targeting a wide range of organizations and industries in the United States and East Asia. They are known for their ability to modify router firmware without being detected and for exploiting trusted network relationships between routers.

#2 The group targets various sectors, including government, industrial, technology, media, electronics, and telecommunications. They have also shown interest in entities supporting the military efforts of both the U.S. and Japan.

#3 BlackTech employs custom malware and dual-use tools to conduct their cyber operations. They constantly update their tools to evade detection by security software. Additionally, they use stolen code-signing certificates to make their malicious payloads appear legitimate.

#4 To avoid detection, BlackTech uses "living off the land" tactics, which means they blend in with normal operating system and network activities. This includes disabling logging on routers and employing various techniques for persistence on compromised hosts.

#5 One of BlackTech's notable tactics involves pivoting from international subsidiaries of U.S. and Japanese companies to expand their access within target networks. They abuse trusted network relationships between subsidiaries and headquarters, allowing them to move freely within corporate networks.

#6 The group has also demonstrated expertise in targeting and compromising router devices. They manipulate router firmware to hide their activities, disable logging, and conceal commands. In some cases, they replace legitimate firmware with malicious versions to establish persistent backdoor access.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
BlackTech (a.k.a. Palmerworm, Temp.Overboard, Circuit Panda, and Radio Panda)	China	U.S. and East Asia	Government, industrial, technology, media, electronics, telecommunication, military
	MOTIVE		
	Information theft and espionage		

Recommendations

Keep router firmware up to date: Router manufacturers regularly release firmware updates that address security vulnerabilities. By keeping your router firmware up to date, you can help to protect your network from known vulnerabilities that BlackTech may be exploiting.

Network Segmentation: Implement strong network segmentation to limit lateral movement within your network. This can help prevent cyber actors from easily pivoting between different parts of your organization.

Monitor your network for suspicious activity: There are a number of tools and services that can help you to monitor your network for suspicious activity. By monitoring your network regularly, you can detect any attempts by BlackTech to compromise your devices.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0008 Lateral Movement	TA0011 Command and Control
T1588 Obtain Capabilities	T1588.003 Code Signing Certificates	T1199 Trusted Relationship	T1205 Traffic Signaling
T1542.004 ROMMONkit	T1112 Modify Registry	T1562 Impair Defenses	T1562.003 Impair Command History Logging
T1601.001 Patch System Image	T1021.001 Remote Desktop Protocol	T1021.004 SSH	T1071.002 File Transfer Protocols
T1090 Proxy			

References

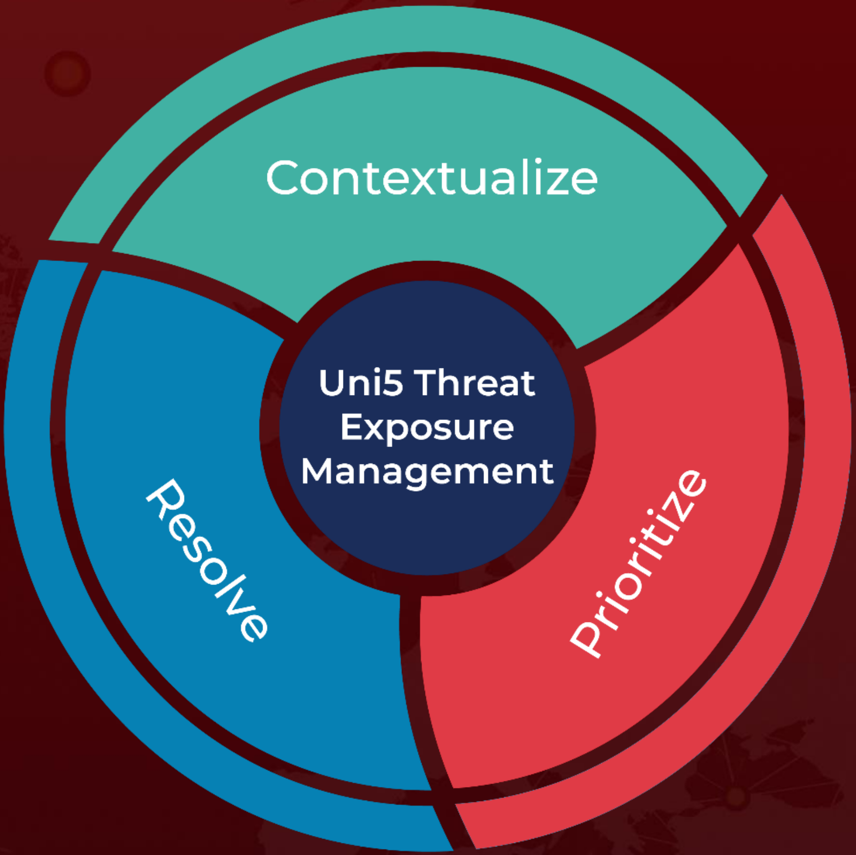
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-270a

https://attack.mitre.org/groups/G0098/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 29, 2023. 7:30 AM

More at www.hivepro.com