Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

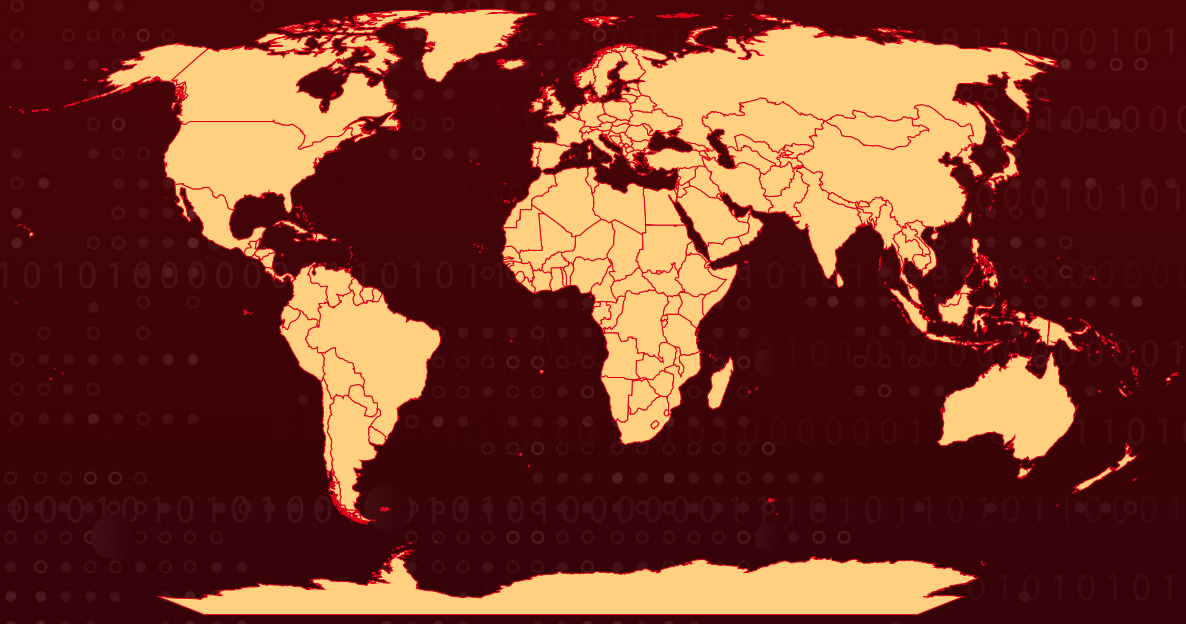
Nexcorium: IoT Botnet Campaign Exploiting TBK DVR Devices

Date of Publication	Admiralty Code	TA Number
April 21, 2026	A1	TA2026108

Summary

First Seen: 2026
Targeted Regions: Worldwide
Targeted Platforms: Linux (ARM, MIPS R3000, x86-64/AMD64)
Targeted Products: TBK DVR-4104, TBK DVR-4216, Huawei HG532
Malware: Nexcorium
Attack: Nexcorium is a multi-architecture Mirai variant deployed through exploitation of CVE-2024-3721, an OS command injection vulnerability in TBK DVR devices. Threat actors manipulate HTTP request parameters to deliver a downloader shell script that fetches architecture-specific payloads. Once established, the malware persists through multiple system-level mechanisms, brute-forces adjacent IoT devices via Telnet using default credentials, and launches large-scale distributed denial-of-service (DDoS) attacks via centralized command-and-control infrastructure.

Attack Regions



Targeted Non-Targeted

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-3721	TBK DVR OS Command Injection Vulnerability	TBK DVR-4104 / DVR-4216	✗	✗	EOL
CVE-2017-17215	Huawei HG532 Remote Code Execution Vulnerability	Huawei HG532	✓	✗	EOL

Attack Details

#1

Researchers have uncovered an active campaign in which threat actors are exploiting vulnerabilities in TBK DVR devices to propagate a new Mirai-based variant dubbed Nexcorium. The intrusion begins with the abuse of CVE-2024-3721, a critical OS command injection flaw affecting TBK DVR-4104 and DVR-4216 models. By targeting the /device.rsp?opt=sys&cmd= endpoint and manipulating the mdb/mdc parameters, attackers are able to remotely execute arbitrary system commands. Notably, the exploit traffic carries a custom HTTP header, "X-Hacked-By: Nexus Team – Exploited By Erratic", which serves as a potential attribution clue linking the activity to the Nexus Team. Once access is gained, a shell-based downloader named "dvr" is deployed, retrieving architecture-specific payloads (ARM, MIPS R3000, x86-64) labeled with the nexuscorp prefix, assigning full permissions, and executing them with device-specific arguments.

#2

Once executed, the Nexcorium payload announces its presence with the message "nexuscorp has taken control" before initiating its core routines. Its internal structure closely aligns with the traditional Mirai framework, comprising three primary components: a watchdog, a scanner, and an attack module. Configuration data, including command-and-control (C2) details, persistence instructions, embedded exploits, and a brute-force credential list, is obfuscated using XOR encoding with keys 0x13 and 0xFD. The watchdog module, identifiable by the marker "NXS_WD_CHILD," ensures process resilience by supervising child operations. To maintain integrity, the malware computes a hash of its binary using the FNV-1a algorithm; if discrepancies are detected, it regenerates itself under a new filename with restricted permissions, reinforcing operational continuity.

#3

For propagation, Nexcorium leverages a dual strategy. It includes a built-in exploit for CVE-2017-17215, targeting Huawei HG532 routers, which is decoded at runtime and delivered via crafted network packets. In parallel, it conducts Telnet-based brute-force attacks using an extensive hard-coded credential list featuring common and vendor-default usernames and passwords such as admin, 12345, hikvision, and default. Upon successful access, the malware validates the shell environment using commands like system, sh, and cat /bin/busybox, then identifies the device architecture to deploy the appropriate payload variant.

#4

After establishing a foothold, Nexcorium embeds itself deeply within the system to ensure persistence. It copies its binary to /usr/local/bin/sysd and implements four separate persistence mechanisms: modifying /etc/inittab for process respawning, adding execution commands to /etc/rc.local, creating a systemd service (/etc/systemd/system/persist.service), and scheduling execution through cron jobs. To complicate forensic analysis, the original binary is deleted post-installation. The botnet's primary objective is large-scale distributed denial-of-service (DDoS) operations, supporting a wide range of flood techniques including UDP, TCP SYN, ACK, PSH, URG, SMTP floods, and VSE query attacks. Communication with its C2 infrastructure hosted at r3brqw3d[.]b0ats[.]top, enables dynamic command execution, including directives to launch attacks, halt operations (killattk), or terminate the bot (botkill).

Recommendations

Isolate or Replace End-of-Life TBK DVR Devices: TBK DVR-4104 and DVR-4216 models are end-of-life products that no longer receive firmware updates or security patches from the vendor. Organizations still operating these devices should immediately disconnect them from internet-facing networks, restrict management access to trusted internal subnets only, and prioritize replacing them with actively supported alternatives that receive regular security updates.

Replace Default Credentials on IoT Devices: Change all factory-default usernames and passwords on DVRs, routers, IP cameras, and other IoT devices. Nexcorium carries an extensive hard-coded wordlist targeting common defaults such as "admin," "12345," "hikvision," and vendor-specific credentials.

Disable Telnet on IoT Devices: Disable Telnet services on all networked devices where SSH or other secure management protocols are available. Nexcorium's scanner module relies on Telnet-based brute-force attacks for lateral propagation.

Deploy IPS Signatures for CVE-2024-3721 and CVE-2017-17215: Enable intrusion prevention signatures that detect exploitation attempts against TBK DVR command injection (CVE-2024-3721) and Huawei HG532 remote code execution (CVE-2017-17215) flaws.

Monitor for Persistence Artifacts: Hunt for unauthorized modifications to /etc/inittab, /etc/rc.local, and /etc/systemd/system/persist.service, as well as unexpected cron job entries and binaries located at /usr/local/bin/sysd on Linux-based IoT devices.

Segment IoT Networks: Place all IoT and surveillance devices on dedicated VLANs with strict egress filtering. Prevent these segments from initiating outbound connections to the internet except through approved proxy or filtering gateways.

Implement DDoS Mitigation Controls: Deploy upstream DDoS mitigation services and rate-limiting rules to absorb or deflect volumetric flood attacks (UDP, TCP SYN, TCP ACK, SMTP) that Nexcorium-infected botnets may direct at organizational infrastructure.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Persistence	T1037: Boot or Logon Initialization Scripts	T1037.004: RC Scripts
	T1053: Scheduled Task/Job	T1053.003: Cron
	T1543: Create or Modify System Process	T1543.002: Systemd Service
Defense Evasion	T1140: Deobfuscate/Decode Files or Information	
	T1070: Indicator Removal	T1070.004: File Deletion

Tactic	Technique	Sub-technique
Credential Access	T1110: Brute Force	T1110.001: Password Guessing
Discovery	T1082: System Information Discovery	
Lateral Movement	T1021: Remote Services	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
Impact	T1498: Network Denial of Service	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	84[.]200[.]87[.]36, 176[.]65[.]148[.]186
Domain	r3brqw3d[.]b0ats[.]top
SHA256	696aeb6321313919f0a41a520e6fa715450bbfb271a9add1e54efe16484a9c35, 37132e804ccb3fc4ba1f72205da70c3d7a6e66b43178707a9d8ee1156d815c21, e4789416c35b345e75c023a8c07c207c79937c6a5444e1c29d85d18d2f660d8c, 0b510f93f47590791626d2fa74ddd62ba6eb8a5a5bb7b8476c0ceffc7be94ebe, 9b805585c457811d2c5c5664ede9ee869b53e3c9999100505d7ee8de7f855fdf, 95d1eb12d58206319c514c7240d058c512bb22b31f6ea22ed8be3ae44305c9f7, 7c01d5b53861cd34e10a79fdea16dcf08bce9c78ed72abd6d6f3e9ce75a24734, 838e35b62a6b38675e467301166cdcc54f98d528fe43d56936caeffec88ac696, 2ccf23b8165e8c05899aa7ba4755b896ebf1d20d3b701cffdc768482486b0a74,

TYPE	VALUE
SHA256	29404df12a7723ce46c8b199c88a808aa315dd8ff8fd1e06a34ccd3d16f4553b, b1274de00a7f3d7ab9792ec3456e9d5bf057738666f34183f1d72060e2d4f678, 721c7cb2109ec97c14413cb8b58ddce0ecf0c1f13f22ee4f72eed79b57592cf5, 89dae116c77b0035277d39dfe01043624427c119ddee8883a3ba54a42a6ae400

Patch Details

Both CVE-2024-3721 and CVE-2017-17215 affect end-of-life (EOL) devices, meaning no official security patches are available from the vendors, leaving affected systems exposed and requiring replacement or network-level mitigations.

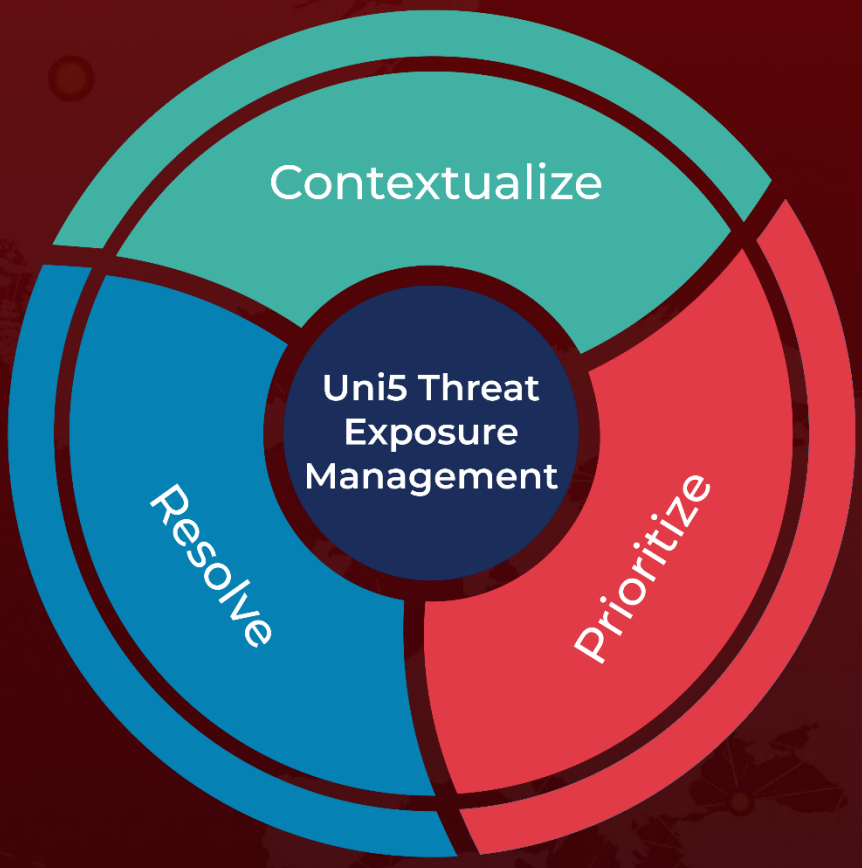
References

https://www.fortinet.com/blog/threat-research/tracking-mirai-variant-nexcorium-a-vulnerability-driven-iot-botnet-campaign

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

April 21, 2026 • 09:15 AM

More at www.hivepro.com