Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

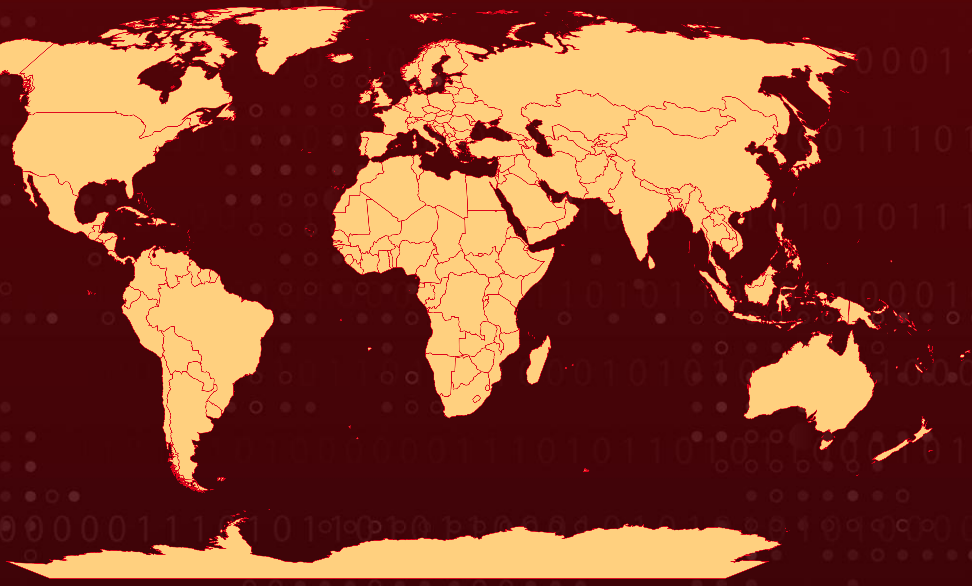
RondoDox Botnet Campaign Targets TBK DVRs and Four-Faith Routers

Date of Publication	Admiralty Code	TA Number
July 9, 2025	A1	TA2025211

Summary

First Seen: September 2024
Malware: RondoDox botnet
Targeted Architectures: ARM, MIPS, Intel 80386, MC68000, MIPS R3000, PowerPC, SuperH, ARCompact, x86-64, AArch64
Targeted Region: Worldwide
Attack: A newly identified botnet campaign, RondoDox, is actively exploiting critical vulnerabilities in TBK DVRs and Four-Faith devices, enabling attackers to covertly compromise systems and repurpose them for malicious operations. This sophisticated malware employs evasion and persistence techniques, transforming overlooked network devices into stealth proxies for coordinated, large-scale DDoS campaigns. The campaign underscores the growing operational risks posed by unpatched, poorly secured infrastructure in enterprise and industrial environments.

Targeted Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-3721	TBK DVR OS Command Injection Vulnerability	TBK DVR-4104 and DVR-4216 devices	✗	✗	✗
CVE-2024-12856	Four-Faith OS Command Injection Vulnerability	Four-Faith F3x24 and F3x36	✓	✗	✗

Attack Details

#1

A new wave of cyberattacks has emerged with the discovery of a RondoDox botnet campaign exploiting two critical vulnerabilities, CVE-2024-3721 and CVE-2024-12856. Both flaws have been publicly disclosed and are currently under active exploitation, posing severe threats to device security and overall network integrity.

#2

The first vulnerability, CVE-2024-3721, affects TBK DVR-4104 and DVR-4216. This flaw allows remote attackers to execute arbitrary commands on affected devices without requiring any authentication. In essence, it hands over full control of security surveillance systems to malicious actors. Recently, CVE-2024-3721 has been actively exploited in attempts to deploy a variant of the Mirai botnet.

#3

The second vulnerability, CVE-2024-12856, targets Four-Faith F3x24 and F3x36. This exploit technically demands authentication, but the widespread use of default credentials renders most of these devices effectively defenseless. Once compromised, attackers gain deep access to network infrastructure and any connected systems, which can lead to broader compromises.

#4

RondoDox is a particularly stealthy strain of malware, originally crafted for Linux-based systems running on ARM and MIPS architectures. However, its capabilities have since expanded to include a wide array of architectures, significantly broadening its reach. RondoDox employs advanced persistence techniques.

#5

Its shell script downloader probes for writable directories with execution permissions to plant its payload. After gaining a foothold, it establishes multiple redundant mechanisms to maintain control. These include modifying system startup scripts, creating hidden services, and even renaming critical security utilities to evade detection and removal attempts.

#6

RondoDox actively seeks out and disables security monitoring tools running on the infected system. It cleverly disguises its malicious traffic as legitimate network activity, mimicking data from gaming services, VPN clients, and messaging apps to slip past intrusion detection systems unnoticed.

#7

What makes this threat campaign especially concerning is the environment in which these vulnerable devices operate. Many are deployed in retail outlets, warehouses, and small business office's locations where such equipment is often neglected for years, left running outdated firmware and exposed to the internet through misconfigured ports. This makes them prime targets as it is easy to breach, difficult to monitor, and seldom secured.

Recommendations

Isolate Vulnerable Devices: Immediately segment TBK DVR-4104/4216 systems and Four-Faith F3x24/F3x36 routers from the primary corporate network. Place these devices in dedicated, restricted network zones or VLANs without unnecessary internet exposure.

Change All Default Credentials: Immediately replace any factory-default usernames and passwords on Four-Faith routers and other connected devices. Enforce unique, strong passwords aligned with organizational password policies. Disable unused user accounts and restrict administrative privileges to essential personnel only.

Enhance Network Monitoring: Enhance continuous network monitoring to detect anomalous activity involving affected devices across both internal and external connections. Prioritize detection of unusual outbound traffic, especially to known malicious IP addresses listed in the Indicators of Compromise section. Additionally, actively monitor for potential signs of compromise, including unexpected system processes or services, unauthorized modifications to startup files, suspicious files in temporary directories, and unexplained traffic to gaming, VPN, or messaging service domains.

Conduct Immediate Asset Inventory: Identify and document all instances of affected TBK DVR and Four-Faith router models within your infrastructure. Record current firmware versions, configurations, operational dependencies, and network placement for each device.

Remove Persistence and Restore System Integrity: Perform deep forensic reviews on potentially compromised hosts to uncover RondoDox's persistence mechanisms. Focus on init script modifications, unauthorized crontab entries, and symlinks in directories such as /etc/init.d/, /etc/rcS, or /etc/inittab. Identify and remove malicious artifacts and renamed binaries, including tampered versions of iptables, shutdown, and passwd. Deploy file integrity monitoring tools to track critical system binaries and startup configurations for unauthorized changes.

Detect Anti-Forensics Behavior: Deploy behavioral detection mechanisms to catch attempts by RondoDox to erase traces of its activity. This includes monitoring for deleted shell histories, abrupt termination of forensic tools (e.g., Wireshark, tcpdump), and execution of unfamiliar scripts in memory-based directories such as /dev/shm and /tmp.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	TA0042 Resource Development	T1584 Compromise Infrastructure
T1584.005 Botnet	T1059 Command and Scripting Interpreter	T1037 Boot or Logon Initialization Scripts	T1543 Create or Modify System Process
T1027 Obfuscated Files or Information	T1036 Masquerading	T1070 Indicator Removal	T1562 Impair Defenses
T1562.001 Disable or Modify Tools	T1071 Application Layer Protocol	T1071.004 DNS	T1105 Ingress Tool Transfer
T1082 System Information Discovery	T1057 Process Discovery	T1588 Obtain Capabilities	T1588.005 Exploits
T1588.006 Vulnerabilities	T1078 Valid Accounts	T1078.001 Default Accounts	T1569 System Services

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	45[.]135[.]194[.]34, 83[.]150[.]218[.]93, 14[.]103[.]145[.]202, 14[.]103[.]145[.]211,

TYPE	VALUE
IPv4	154[.]91[.]254[.]95, 78[.]153[.]149[.]90, 178[.]215[.]238[.]91, 116[.]203[.]104[.]203, 130[.]61[.]64[.]122, 161[.]97[.]219[.]84, 130[.]61[.]69[.]123, 185[.]84[.]81[.]194, 54[.]36[.]111[.]116, 192[.]3[.]165[.]37, 162[.]243[.]19[.]47, 63[.]231[.]92[.]27, 80[.]152[.]203[.]134, 42[.]112[.]26[.]36
SHA256	c88f60dbae08519f2f81bb8efa7e6016c6770e66e58d77ab6384069a515e451c, eb3e2a6a50f029fc646e2c3483157ab112f4f017406c3aabedaae0c94e0969f6, f4cd7ab04b1744babef19d147124bfc0e9e90d557408cc2d652d7192df61bda9, e3c080e322862d065649c468d20f620c3670d841c30c3fe5385e37f4f10172e7, e62df17150fcb7fea32ff459ef47cdd452a21269efe9252bde70377fd2717c10, 53e2c2d83813d1284ddb8c68b1572b17cca95cfc36a55a7517bf45ff40828be5, 43d4847bf237c445ed2e846a106e1f55abefef5c3a8545bd5e4cad20f5deb9a4, 4c2429fc8b8ec61da41cbba1b8184ec45fa93a9841b4ca48094bba7741b826b8, 694d729d67f1b0c06702490bfab1df3a96fe040fe5d07efa5c92356c329757be, edae3b75deb8013bd48ac4534cca345b90938a2abb91672467c2bf9ae81ff683, 0814a0781ab30fca069a085dba201d6fd0f414498fafa4bb42859786d91d4781, 59b4deee977e9e27b60e7e179d54a1ce8e56624e73b799523416eee828bfaf76, 9f916a552efc6775367a31357a633dc0be01879830d3fddccdf3c40b26e50afd, 0a9ebbecc8ec58c253039520304ca373cfb8d1674d67993e6485e244a77d6ec9, 6c81fd73b4bef6fef379cbefdcce7f374ea7e6bf1bf0917cf4ca7b72d4cee788,

TYPE	VALUE
SHA256	a55a3859a203ca2bae7399295f92aeae61d845ffa173c1938f938f5c148eef99, 57573779f9a62eecb80737d41d42165af8bb9884579c50736766abb63d2835ba, 3daa53204978b7797bd53f5c964eed7a73d971517a764785ce3ab65a9423c2e7, 8bf8928bc255e73e0b5b0ce13747c64d82d5f2647da129f189138773733ac21f, 20a24b179bdbbdcc0053838c0484ea25eff6976f2b8cb5630ab4efb28b0f06b5, 42aa715573c7d2fca01914504cb7336db715d73d1e20d23e4bd37f2e4f4fe389, c9278ce988343606350a94156ca28ee28bd605d1d95c810a16866eee1f997598, a197f60d5f5641f2c56576b4c867d141612c6e00db29c512f266835510b8a62d, 8250d289c5ec87752cec1af31eed0347cf2dd54dc0fbeea645319c4dae238ee2, d02414a54e97ad26748812002610f1491a2a746e9ba0f9d05de3d47d7bab4f5e, c123a91fdacd9a4c0bcf800d6b7db5162cfd11cb71e260647ef0f2c60978ebfc, ef708fec1afbea4fb32b586e0dacf0d228c375a532008d81453c367256afea5a, 305507f34c14c72cab35715b7f7b25b32352a8e19b8a283003aaf539d12ca517, 937e6ab0dfcedfa23eced7b52d3899b0847df3fcb7a9c326b71027a7ab5f5b93
MD5	011a406e89e603e93640b10325ebbdc8, 24fd043f9175680d0c061b28a2801dfc, 29b83f0aae7ed38d27ea37d26f3c9117, 2e9920b21df472b4dd1e8db4863720bf, 3120a5920f8ff70ec6c5a45d7bf2acc8, 3c2f6175894bee698c61c6ce76ff9674, 45a41ce9f4d8bb2592e8450a1de95dcc, 524a57c8c595d9d4cd364612fe2f057c, 74dee23eaa98e2e8a7fc355f06a11d97, 761909a234ee4f1d856267abe30a3935, 7eb3d72fa7d730d3dbca4df34fe26274, 8a3e1176cb160fb42357fa3f46f0cbde, 8d92e79b7940f0ac5b01bbb77737ca6c, 95eaa3fa47a609ceefa24e8c7787bd99, 96ee8cc2edc8227a640cef77d4a24e83, aaf34c27edfc3531cf1cf2f2e9a9c45b, ba32f4eef7de6bae9507a63bde1a43aa

Patch Details

As of July 2025, security patches addressing CVE-2024-3721 and CVE-2024-12856 have not yet been released by the respective vendors. We recognize this may raise concerns for organizations managing these devices and are committed to providing clear, timely information as the situation evolves. In the absence of formal patches, standard security best practices remain in effect. This typically includes network segmentation, password hardening, disabling unnecessary services, and proactive monitoring. For actionable risk mitigation, please refer to the Recommendations section of this advisory.

References

https://www.fortinet.com/blog/threat-research/rondobox-unveiled-breaking-down-a-botnet-threat

https://vulncheck.com/blog/four-faith-cve-2024-12856

https://securelist.com/mirai-botnet-variant-targets-dvr-devices-with-cve-2024-3721/116742/

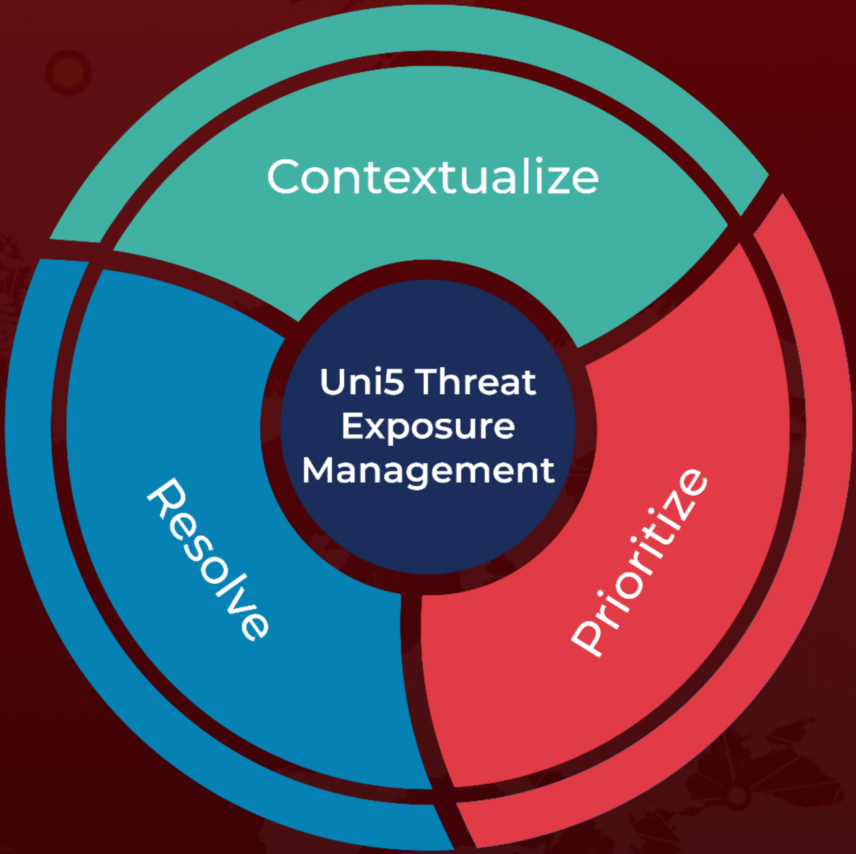
https://hivepro.com/threat-advisory/gayfemboy-botnet-evolution-of-a-potent-threat/

https://github.com/nu113d/CVE-2024-12856

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

July 9, 2025 • 10:30 PM

More at www.hivepro.com