UMBRELLA STAND MALWARE TARGETS FORTINET FIREWALLS

Vairav Security News Report

Date: June 23, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

UMBRELLA STAND is a sophisticated, modular malware framework uncovered by the UK National Cyber Security Centre (NCSC), designed to stealthily compromise **Fortinet FortiGate 100D firewalls**. Likely deployed through exploitation of security vulnerabilities, UMBRELLA STAND enables long-term persistence, remote shell access, and covert command-and-control (C2) communication via **fake TLS beacons** on **port 443**.

Key characteristics of the malware include:

1. Fake TLS communications that impersonate encrypted HTTPS traffic without performing legitimate handshakes
2. AES-CBC encrypted C2 messages using a fixed IV
3. Advanced persistence via reboot hooking and dynamic linker (ld.so.preload) hijacking
4. Remote shell functionality and file exfiltration in 6000-byte chunks
5. Masquerading of processes as /bin/httpsd and use of hidden directories (e.g., /data2/.ztls/)
6. Deployment of open-source reconnaissance tools such as BusyBox, nbtscan, tcpdump, and openLDAP

CAMPAIGN DETAILS

Campaign Name	UMBRELLA STAND
Targeted Devices	Fortinet FortiGate 100D
Initial Access Vector	Post-exploitation of vulnerable FortiGate firewalls (exact CVE not disclosed)
Infection Timeline	Active as of early 2025, likely ongoing
Target Sectors	Critical infrastructure, enterprise firewalls, and embedded network environments
Attribution	Unknown threat actor (potential overlap with COATHANGER toolchain)
Geographic Focus	UK visibility confirmed; global implications expected
Purpose	Covert surveillance, C2 persistence, shell access, and data exfiltration

The malware is believed to be deployed through the exploitation of unknown or unpatched vulnerabilities and is designed to facilitate long-term espionage or remote access by advanced threat actors. Its modular architecture includes components for:

- **Networking and task management** (blghtd)
- **Persistence watchdogs** (jvnlpe)
- **Startup loaders** (cisz)
- **Dynamic injection mechanisms** (libguic.so, reboot_hooker)
- **File encryption/decryption** (a)

UMBRELLA STAND's sophisticated design intends to evade, persist, and exfiltrate data from critical infrastructure firewalls. Its modular nature and deceptive C2 techniques suggest an espionage-oriented campaign, possibly linked to the same actors behind COATHANGER. Organizations relying on FortiGate 100D firewalls should take immediate action to identify compromises, strengthen network perimeter visibility, and eliminate backdoor footholds.

INDICATORS OF COMPROMISE (IOCs)

File Hashes
8bacd5df99476328321a7e8e2fc0124c20f7a7ebf3e8f151c050387038515b70
591d60c1d356da827a26f4141fa431d3663af91746d5371014695b1c89bac2b2
6a3abc19f324a475d4ce01fcc69797fc90e1a47970ed90e9cb01f540f3000b4e
190293440fce95f45eb8bf5d40334b41dd68c79578d06fe9b34670298daea7f3
a64b41e98e3e1066f41fbff5d4f99f6d34b792d35fe2be7e5d9fa8f3f8b93739
d1d5f502e2039b20269b562bbc1e5622a73bbecad54cb25ae5eaa7a91504e70e
d3b88b7f640e478d8d875e12b4561e8c794909e4954aebbc6fd1f5e79f381648
65f1e17f7fa2e2fd9c57265f390484a7428c192f59ee41fc7c0d8386ea3b811a
38801caae26916367dd6cf6e8c55e50ed62526fe242cd0343dfe80a70564c28a
881998c9864d2c7fe35f9b8071dbcf84386cb15da77e6f6a086cf605a4dd7823
C2
89.44.194.32

MITRE ATT&CK TECHNIQUES

Tactics	Techniques (ID)
Execution	Command and Scripting Interpreter (T1059) • Unix Shell (T1059.004)
Defense Evasion	Deobfuscate/Decode Files or Information (T1140) Process Injection (T1055) Indicator Removal (T1070) • File Deletion (T1070.004) Hide Artifacts (T1564) • Process Argument Spoofing (T1564.010) • Hidden Files and Directories (T1564.001)
Persistence	Boot or Logon Autostart Execution (T1547) • Kernel Modules and Extensions (T1547.006) Hijack Execution Flow (T1574) • Dynamic Linker Hijacking (T1574.006)
Discovery	Process Discovery (T1057) Network Service Discovery (T1046) Network Sniffing (T1040)
Command and control	Data Obfuscation (T1001) • Protocol or Service Impersonation (T1001.003)

RECOMMENDATIONS

1. **Patch Fortinet Devices**: Apply all critical updates for FortiGate firewalls, especially FortiOS 100D series.
2. **Hunt for Anomalous Traffic:** Investigate TLS connections on port 443 without valid handshakes. Look for traffic to/from C2 IP: 89.44.194.32.
3. **Monitor for Persistence Techniques:** Check for LD_PRELOAD modifications and presence of /data2/.ztls/.
4. **Detect Masquerading:** Scan for processes using false names (e.g., /bin/httpsd) or injected into PID 1.
5. **Use YARA Rules from NCSC:** Deploy provided signatures to detect both encrypted and plaintext variants of UMBRELLA STAND.
6. **Restrict Tool Usage:** Block unauthorized use of BusyBox, nbtscan, and tcpdump on security appliances.

REFERENCES

https://securityonline.info/ncsc-uncovers-umbrella-stand-malware-stealthy-backdoor-targets-fortinet-fortigate-firewalls/

https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/umbrella-stand/ncsc-mar-umbrella_stand.pdf

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com