Computer Emergency Response Team of Mauritius

A Department of the Ministry of Information Technology, Communication and Innovation

CERT-MU Security Alert

Date of Issue: 25 June 2025

Dual Malware Threats: UMBRELLA STAND and SHOE RACK Targeting FortiGate Firewalls

Severity: High

Description

Two advanced malware strains - UMBRELLA STAND and SHOE RACK are targeting FortiGate 100D series firewalls. UMBRELLA STAND is a multi-component malware enabling remote shell access, file manipulation, and network exfiltration, while SHOE RACK serves as a post-exploitation tool, using reverse SSH tunneling and DNS-over-HTTPS for secure communication and remote access.

CERT-MU advises organisations to be cautious and follow the recommendations below.

Technical Details:

1. Initial Compromise:

UMBRELLA STAND exploits vulnerabilities in FortiGate 100D series firewalls, gaining access and deploying various tools for persistence and control.

SHOE RACK, once deployed after the initial compromise, establishes a reverse SSH connection using a non-standard version of SSH, allowing attackers to bypass traditional network security measures.

2. Persistence Mechanism:

UMBRELLA STAND uses a combination of reboot hooks, ldpreload techniques, and file manipulation to ensure the malware survives reboots and remains undetected.

SHOE RACK ensures persistence by modifying SSH configurations and creating reverse SSH tunnels, allowing attackers to maintain remote access to the compromised device without detection.

3. C2 Communication:

UMBRELLA STAND communicates with its C2 server over fake TLS traffic on port 443, masking its true intent by mimicking legitimate encrypted communications.

SHOE RACK uses DNS-over-HTTPS (DOH) to resolve the C2 server's IP, then establishes a TCP/TLS connection for SSH communication. It uses non-standard SSH channels, making detection difficult.

4. Data Exfiltration and Command Execution:

UMBRELLA STAND facilitates file exfiltration, remote shell commands, and manipulation of system settings.

SHOE RACK, via reverse SSH tunnels, allows the attacker to interact with the compromised device and tunnel traffic from other networked systems, enabling deep network pivoting

Indicators of Compromise

Type	Indicator
FileHash-MD5	8535eb46a621f806a21fb9c1f4f79ab2
FileHash-MD5	fa2a49f137a622c20ab078c0f7028cf2
FileHash-SHA1	a11e33292d6fe1eb27860c70276fcae118bcf274
FileHash-SHA1	d47d8c42556fe5081a94483eb47be4c59a515861
FileHash-SHA256	5c5843ae833cab1417a0ac992b5007fce40158fc3afec4c6e4fd0e932de07177
FileHash-SHA256	d86d360f51550feccfd92f0e04891591ab9b0c049eacd07d49460f6b3d7764bf
IPv4	65.20.73.163
URL	http://gopkg.in/ini%2ev1.

URL	http://phcia.duckdns.org:443
domain	gopkg.in
hostname	phcia.duckdns.org

Recommendations

1. Ensure all FortiGate devices, including the 100D series, are regularly updated with the latest security patches provided by Fortinet.
2. Review and tighten control over reboot functionality in Fortinet devices to prevent unauthorized hooks like those used by UMBRELLA STAND.
3. Deploy file integrity monitoring (FIM) and rootkit detection tools to detect unauthorized file changes or the injection of malicious binaries (e.g., blghtd, cisz, libguic.so).
4. Set up network monitoring systems to detect anomalies in network traffic patterns, especially fake TLS communications or unusual beaconing on port 443.
5. Block the IOCs at their respective controls.

Report Cyber Incidents

Report cyber security incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS - http://maucors.govmu.org/)**

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)
Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu
MAUCORS: http://maucors.govmu.org