QILIN RANSOMWARE EXPLOITS FORTINET FLAWS TO TARGET GLOBAL NETWORKS

Vairav Security News Report

Date: June 09, 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

The **Qilin ransomware group** (also known as **Phantom Mantis**) has launched a new wave of targeted attacks exploiting multiple **Fortinet vulnerabilities** to gain unauthorized access and deploy ransomware across corporate environments.

Active since August 2022 under the "Agenda" name, Qilin has claimed responsibility for over **310 victims** to date, including major entities such as **Yangfeng Automotive**, **Lee Enterprises**, **Court Services Victoria**, and **Synnovis**, the latter causing severe disruption to London NHS hospitals.

According to a **private flash alert by PRODAFT**, Qilin's latest intrusion campaign, spanning **May to June 2025**, leverages both **CVE-2024-21762** and the recently exposed **CVE-2024-55591** to bypass authentication and execute malicious code remotely on **FortiGate devices**.

Although their current focus is on Spanish-speaking countries, the campaign is **opportunistic and globally scalable**. The activity highlights a growing trend of ransomware groups exploiting **network edge vulnerabilities** to gain persistent access.

Threat Actor Group Summary

Aliases: Agenda (initial name upon emergence), Phantom Mantis (as tracked by PRODAFT), Qilin (current public identifier in threat landscape)

Origin & Attribution: While precise attribution remains unconfirmed, operational behavior, infrastructure, and language usage suggest links to Russian-speaking cybercrime communities.

First Observed: August 2022

Attack Timeline: May – June 2025

Initial Access Vector: Exploitation of Fortinet FortiGate vulnerabilities

Target Profile

- **Industries:** Government, healthcare, publishing, legal, and logistics
- **Geographic Focus:** Spanish-speaking regions prioritized initially; global expansion likely
- **Notable Victims:** NHS hospitals (via Synnovis), Lee Enterprises, Court Services Victoria, Yangfeng Automotive.

Vulnerability Exploitation Details

CVE-2024-21762

- **Description:** FortiOS and FortiProxy SSL VPN, Improper access control that leads to remote code execution (RCE)
- **Impact:** Allows unauthenticated remote attackers to execute arbitrary code
- **CVSS Score:** 9.6 (Critical)
- **Vulnerable Devices Identified:** 150,000+ (as of March 2025 by Shadowserver)

CVE-2024-55591

- **Description:** FortiGate RCE, previously exploited as a zero-day
- **Impact:** Privilege Escalation
- **CVSS Score:** 9.6 (Critical)
- **First Known Exploitation:** November 2024
- **Notable Use:** Used by **Mora_001** operator to deploy **SuperBlack** ransomware linked to **LockBit**
- **Status:** Active exploitation in the wild

Recommendations

1. **Patch Immediately**
   - Update FortiOS and FortiProxy to the latest versions addressing **CVE-2024-21762** and **CVE-2024-55591**.
   - Verify compliance with CISA's BOD mandates.
2. **Audit Exposed Infrastructure**
   - Use external scanners to identify public-facing SSL VPNs and FortiGate appliances.
   - Monitor for anomalous access and admin activity via VPN logs.
3. **Harden VPN and Firewall Access**
   - Disable unused VPN services and enforce MFA for all remote access points.
   - Review admin account permissions and rotate credentials.
4. **Threat Hunting**
   - Search for indicators of compromise associated with Qilin/Agenda operations.
   - Look for suspicious lateral movement originating from network appliances.

5. **Backup and Segmentation Strategy**
    - Ensure off-site, immutable backups.
    - Segment critical infrastructure away from publicly accessible services.

Qilin's exploitation of Fortinet zero-day vulnerabilities for rapid ransomware deployment signals a continuing evolution in ransomware tradecraft, from phishing and maldocs to device-level access. Organizations must prioritize patching, network hardening, and identity controls to prevent attackers from leveraging infrastructure weaknesses into full-scale breaches.

References

https://www.bleepingcomputer.com/news/security/critical-fortinet-flaws-now-exploited-in-qilin-ransomware-attacks/

https://catalyst.prodaft.com/public/report/phantom-mantis-using-fortigate-vulnerabilities-to-deploy-qilin-ransomware/overview

https://www.cve.org/CVERecord?id=CVE-2024-55591

https://www.cve.org/CVERecord?id=CVE-2024-21762

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