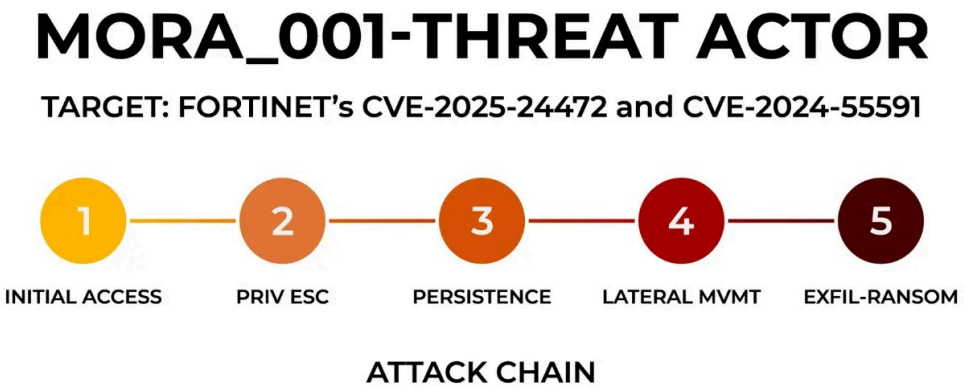
SuperBlack Actors Exploiting Two Fortinet Vulnerabilities to Deploy Ransomware

By Kaaviya

Published: 2025-03-14 · Archived: 2026-04-05 13:03:39 UTC



Between late January and early March 2025, cybersecurity researchers at Forescout's Vedere Labs uncovered a series of sophisticated intrusions leveraging critical Fortinet vulnerabilities.

The attacks, attributed to a newly identified threat actor tracked as "Mora_001," culminated in the deployment of a custom ransomware strain dubbed "SuperBlack."

Mora_001 has demonstrated a systematic approach to compromising networks, beginning with the exploitation of two critical Fortinet vulnerabilities: CVE-2024-55591 and CVE-2025-24472.

These flaws affect FortiOS versions prior to 7.0.16 and allow unauthenticated attackers to gain super_admin privileges on vulnerable devices with exposed management interfaces.

Researchers observed two distinct exploitation methods in the wild, beginning just 96 hours after the public release of a proof-of-concept exploit on January 27, 2025.

The first method utilized the jsconsole interface, exploiting the WebSocket vulnerability with spoofed IP addresses (often 127.0.0.1, 8.8.8.8, or other recognizable addresses).

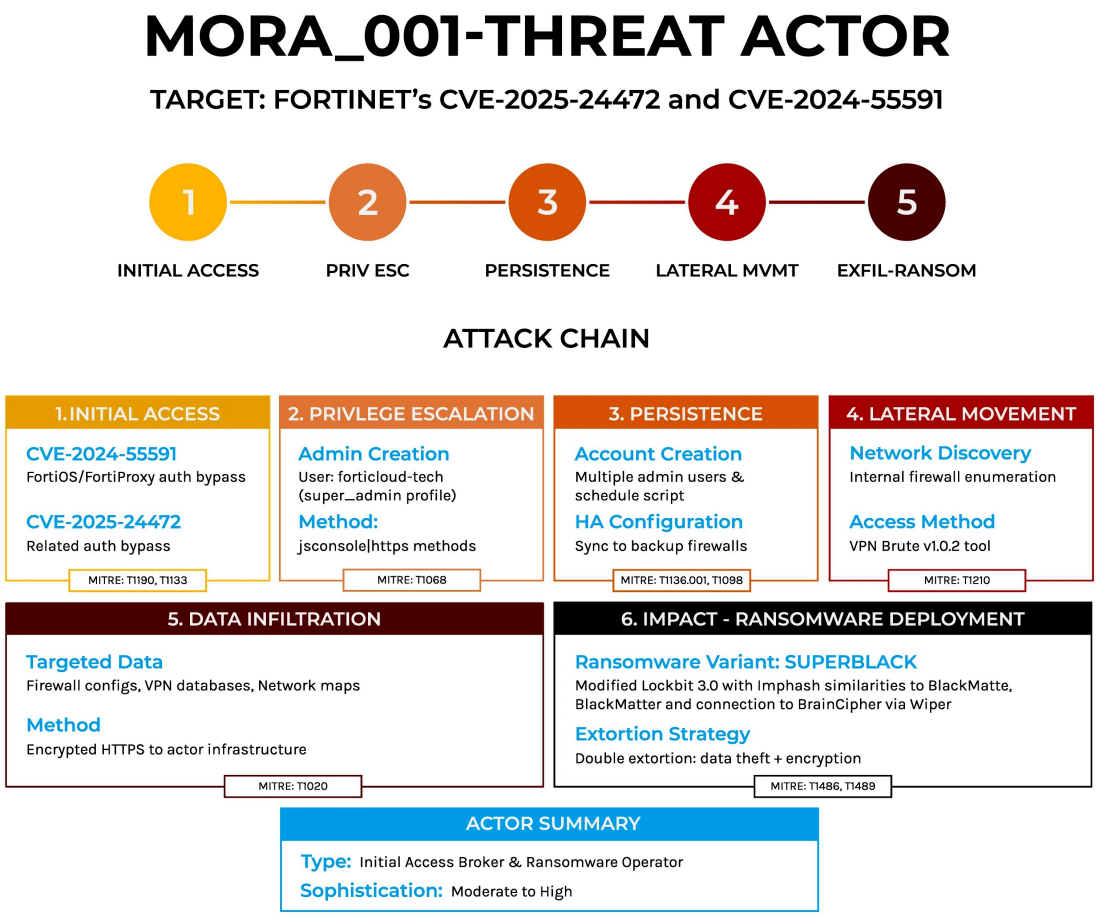
The second method employed direct HTTPS requests targeting the same underlying vulnerability.

Persistence Techniques

After gaining initial access, Mora_001 established persistence through several sophisticated mechanisms.

The attackers consistently created local system administrator accounts with names designed to blend in with legitimate services, including “forticloud-tech,” “fortigate-firewall,” and “adnimistrator” (a deliberate misspelling of “administrator”).

A particularly insidious technique involved creating automated tasks to ensure persistence even after remediation attempts.



Attack Chain & methods

For example, the attackers configured daily scripted automation tasks that would automatically recreate administrator accounts if they were removed.

One such script included the command to recreate a “forticloud-sync” user with super_admin privileges and a predetermined password.

In environments with High Availability (HA) configurations, Mora_001 forced synchronization to propagate the compromised configuration to additional firewalls within the same cluster, effectively spreading their backdoor accounts across multiple devices.

After establishing persistence, Mora_001 conducted extensive reconnaissance using the FortiGate dashboards to gather environmental intelligence.

The attackers accessed the Status, Security, Network, and Users & Devices dashboards to identify potential paths for lateral movement.

In environments with VPN capabilities, the threat actor created additional VPN user accounts with names resembling legitimate accounts but with subtle modifications, such as adding a digit at the end (e.g., “xxx1”).

These accounts were then added to VPN user groups, enabling future network access while evading casual administrative review.

Network Traversal Methods

For lateral movement, Mora_001 leveraged multiple techniques:

1. Using stolen VPN credentials to access internal networks.
2. Exploiting High Availability (HA) configuration propagation to compromise additional firewalls.
3. Abusing authentication infrastructure via TACACS+ or RADIUS when configured to synchronize with Active Directory.
4. Employing Windows Management Instrumentation (WMIC) for remote system discovery and execution.
5. Utilizing SSH to access additional servers and network devices.

The attackers prioritized high-value targets, particularly file servers, authentication servers, domain controllers, and database servers.

Rather than indiscriminately encrypting entire networks, Mora_001 selectively targeted systems containing sensitive data, focusing first on data exfiltration before initiating encryption.

The ransomware deployed by Mora_001, designated “SuperBlack” by researchers, closely resembles LockBit 3.0 (also known as LockBit Black) but with specific modifications.

The primary differences lie in the ransom note structure and the inclusion of a custom data exfiltration executable.

Despite the cosmetic changes, the ransomware maintains strong connections to the LockBit ecosystem.

The ransom note includes a Tox chat ID (DED25DCB2AAAF65A05BEA584A0D1BB1D55DD2D8BB4185FA39B5175C60C8DDD0C0A7F8A8EC815) that has been previously linked to LockBit 3.0 operations.

The note retains LockBit's HTML template structure but removes explicit branding elements, such as the header, that would typically identify it as LockBit ransomware.

Researchers identified additional samples on VirusTotal with similar ransom notes, connecting SuperBlack to import hashes previously associated with BlackMatter, LockBit, and BlackMatte ransomware.

This evidence suggests Mora_001 is either a current or former LockBit affiliate leveraging their leaked builder or an independent threat actor repurposing LockBit's infrastructure and tools.

Infrastructure & Patterns

The primary SuperBlack executable handles the encryption process and downloads additional components, including a wiper module designated "WipeBlack."

This component has been observed in previous ransomware incidents tied to LockBit and BrainCipher, which in turn has connections to SenSayQ, EstateRansomware, and RebornRansomware.

The wiper employs sophisticated anti-forensic techniques, including dynamic resolution of Windows APIs to obstruct static analysis and the use of named pipes for command execution.

After encryption is complete, it overwrites the ransomware executable with random data using a 1MB buffer and a decryption key of 0x3105DFDE, effectively erasing evidence of the initial infection.

Mora_001's operations have been linked to specific infrastructure, including IP address 185.147.124.34, which was observed performing brute force attempts against multiple edge devices.

This IP address hosts a tool identified as "VPN Brute v1.0.2," a Russian-language utility designed to brute force credentials for various VPN services and edge devices.

The VPN Brute tool targets multiple platforms, including:

- Remote Desktop Web Access (RDWeb)
- PulseSecure (referred to as "Dana" in the tool)
- Outlook Web Access (OWA)
- Palo Alto Networks GlobalProtect
- Fortinet
- Cisco
- F5 Networks BIG-IP
- Citrix

Researchers identified 15 additional IP addresses running versions of VPN Brute, with newer variants offering enhanced functionality such as continued brute forcing after successful credential discovery, custom username and password combinations, and honeypot detection capabilities.

The Mora_001 campaign underscores the increasing trend of exploiting perimeter security appliances for initial access, with attackers rapidly weaponizing disclosed vulnerabilities.

As of the report's writing, the United States (7,677), India (5,536), and Brazil (3,201) host the highest numbers of exposed FortiGate firewalls, making them particularly vulnerable to these attacks.

Mitigations

To protect against Mora_001 and similar threats, organizations should implement the following measures:

1. Patch vulnerable systems immediately by applying FortiOS updates addressing CVE-2024-55591 and CVE-2025-24472.
2. Restrict management access by disabling external management interfaces whenever possible.
3. Conduct regular audits of administrator accounts to identify and remove unauthorized users.
4. Examine automation settings for suspicious tasks, particularly those scheduled to run daily or during off-hours.
5. Review VPN users and groups for slight variations of legitimate usernames or recently created accounts.
6. Enable comprehensive logging, including CLI audit logs, HTTP/S traffic logs, Network Policy Server auditing, and authentication system auditing.

The Mora_001 campaign represents a sophisticated evolution in the ransomware landscape, blending opportunistic exploitation with targeted data theft and selective encryption.

While maintaining operational connections to established ransomware ecosystems like LockBit, Mora_001 has developed distinct tactics and tools that set it apart as a unique threat actor.

Organizations with Fortinet deployments should prioritize patching vulnerable devices and implementing the recommended mitigations to protect against this emerging threat.

The rapid exploitation of newly disclosed vulnerabilities highlights the critical importance of timely security updates and comprehensive network monitoring to detect and respond to sophisticated attacks before they can achieve their objectives.

Source: https://cybersecuritynews.com/superblack-actors-exploiting-two-fortinet-vulnerabilities/