Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

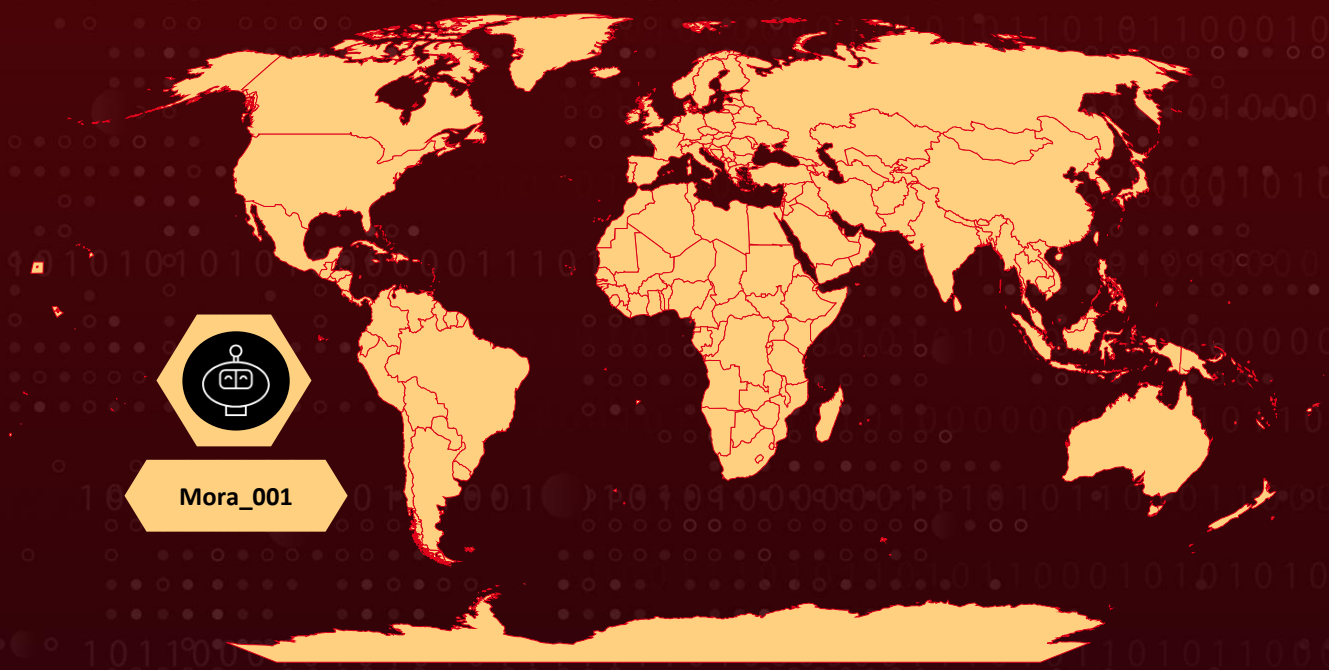
New SuperBlack Ransomware Strikes via Fortinet Authentication Bypass

Date of Publication	Admiralty Code	TA Number
March 14, 2025	A1	TA2025079

Summary

Attack Commenced: 2024
Targeted Countries: Worldwide
Malware: SuperBlack
Threat Actor: Mora_001
Targeted Products: FortiOS, FortiProxy
Attack: The SuperBlack ransomware, a modified LockBit 3.0 variant, is deployed by the Mora_001 threat actor using a double extortion strategy to steal and encrypt sensitive data. They exploit Fortinet vulnerabilities (CVE-2025-24472 & CVE-2024-55591) for initial access, escalating privileges by creating super_admin accounts. Persistence is maintained through HA configuration manipulation, while VPN brute-force attacks enable lateral movement. With FortiGate devices at risk globally, organizations must urgently patch vulnerabilities and enhance security measures.

Attack Regions



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

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-24472	Fortinet FortiOS Authorization Bypass Vulnerability	Fortinet FortiOS and FortiProxy Office	✗	✓	✓
CVE-2024-55591	Fortinet FortiOS Authorization Bypass Vulnerability	Fortinet FortiOS and FortiProxy	✓	✓	✓

Attack Details

#1

A new ransomware strain, SuperBlack, has been deployed by the threat actor Mora_001, targeting Fortinet devices by exploiting CVE-2025-24472 and CVE-2024-55591. By leveraging authentication bypass flaws in FortiOS and FortiProxy, the attackers infiltrate networks and establish control over critical firewall configurations. This initial access enables them to escalate privileges by creating a super_admin account using jsconsole and HTTPS methods, granting them full administrative rights.

#2

To maintain persistence, the attackers create multiple admin accounts and manipulate High Availability (HA) configurations to sync malicious access across backup firewalls. They then conduct network discovery to identify internal assets and expand their reach using VPN brute-force attacks. This lateral movement allows them to gather sensitive data, including firewall configurations, VPN databases, and network maps, which they exfiltrate through encrypted HTTPS connections.

#3

The attack culminates in ransomware deployment, where the SuperBlack ransomware is used. This ransomware, a modified version of LockBit 3.0, shares similarities with BlackMatte, BlackMatter, and BrainCipher, indicating connections to advanced cybercriminal networks. The attackers employ a double extortion strategy, stealing sensitive data before encrypting the victim's systems to maximize their leverage in ransom negotiations.

#4

Mora_001 operates as both an Initial Access Broker (IAB) and a Ransomware Operator, showcasing moderate to high sophistication. Their ability to exploit vulnerabilities, maintain long-term access, and execute ransomware-based extortion demonstrates a well-coordinated cybercrime operation. Organizations using Fortinet products must implement security patches and enhance monitoring to mitigate these risks.

Recommendations

Apply Security Patches: Immediately update Fortinet devices to the latest firmware versions to patch vulnerabilities CVE-2025-24472 and CVE-2024-55591.

Enhance Access Controls: Restrict administrative access to trusted IP addresses, enforce multi-factor authentication (MFA), and disable unnecessary remote access.

Monitor for Anomalies: Continuously monitor logs for unauthorized admin account creation, unexpected HA configuration changes, and unusual VPN activity.

Strengthen Endpoint Protection: Deploy advanced threat detection tools, regularly scan for malware, and enable automatic threat response for suspicious activities.

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, store them securely offline. Test restoration processes to ensure backup integrity and availability. In case of an SuperBlack ransomware attack, up-to-date backups enable recovery without paying the ransom.

Potential MITRE ATT&CK TTPs

TA0004 Privilege Escalation	TA0042 Resource Development	TA0040 Impact	TA0002 Execution
TA0008 Lateral Movement	TA0001 Initial Access	TA0005 Defense Evasion	TA0006 Credential Access
TA0011 Command and Control	TA0003 Persistence	TA0007 Discovery	T1047 Windows Management Instrumentation
T1190 Exploit Public-Facing Application	T1588.006 Vulnerabilities	T1059 Command and Scripting Interpreter	T1210 Exploitation of Remote Services

T1133 External Remote Services	T1556 Modify Authentication Process	T1136.001 Local Account	T1136 Create Account
T1602 Data from Configuration Repository	T1588 Obtain Capabilities	T1588.005 Exploits	T1053.005 Scheduled Task
T1053 Scheduled Task/Job	T1068 Exploitation for Privilege Escalation	T1098 Account Manipulation	T1486 Data Encrypted for Impact
T1489 Service Stop	T1020 Automated Exfiltration	T1556.001 Domain Controller Authentication	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	89[.]248[.]192[.]55, 94[.]154[.]35[.]208, 80[.]66[.]88[.]90, 185[.]147[.]124[.]31, 96[.]31[.]67[.]39, 94[.]156[.]177[.]187, 170[.]130[.]55[.]164, 185[.]147[.]124[.]10, 109[.]248[.]160[.]118, 213[.]176[.]64[.]114, 57[.]69[.]19[.]70, 185[.]147[.]124[.]34, 192[.]248[.]155[.]218, 185[.]147[.]124[.]55, 176[.]53[.]147[.]5, 80[.]64[.]30[.]237, 193[.]143[.]1[.]65, 185[.]224[.]0[.]201, 5[.]181[.]171[.]133, 94[.]156[.]227[.]208, 95[.]217[.]78[.]122,

TYPE	VALUE
IPv4	77[.]239[.]112[.]0, 192[.]248[.]155[.]218, 185[.]95[.]159[.]43, 95[.]179[.]234[.]4, 217[.]144[.]189[.]35, 45[.]15[.]17[.]67, 185[.]147[.]124[.]34
SHA256	c994b132b2a264b8cf1d47b2f432fe6bda631b994ec7dcddf5650113f4a5a404, f383bca7e763b9a76e64489f1e2e54c44e1fd24094e9f3a28d4b45b5ec88b513, 813ad8caa4dcbd814c1ee9ea28040d74338e79e76beae92bedc8a47b402dedc2, 782c3c463809cd818dadad736f076c36cdea01d8c4efed094d78661ba0a57045, d9938ac4346d03a07f8ce8b57436e75ba5e936372b9bfd0386f18f6d56902c88, 917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2
User names	adnimistrator, fortigate-firewall, admin_support, newadmin, forticloud-tech, newadminuser, newadminz, renewadmin, admin-vpn-access, admin-vpn-access-work, adminp0g, it_manager

Patch Link

https://fortiguard.fortinet.com/psirt/FG-IR-24-535

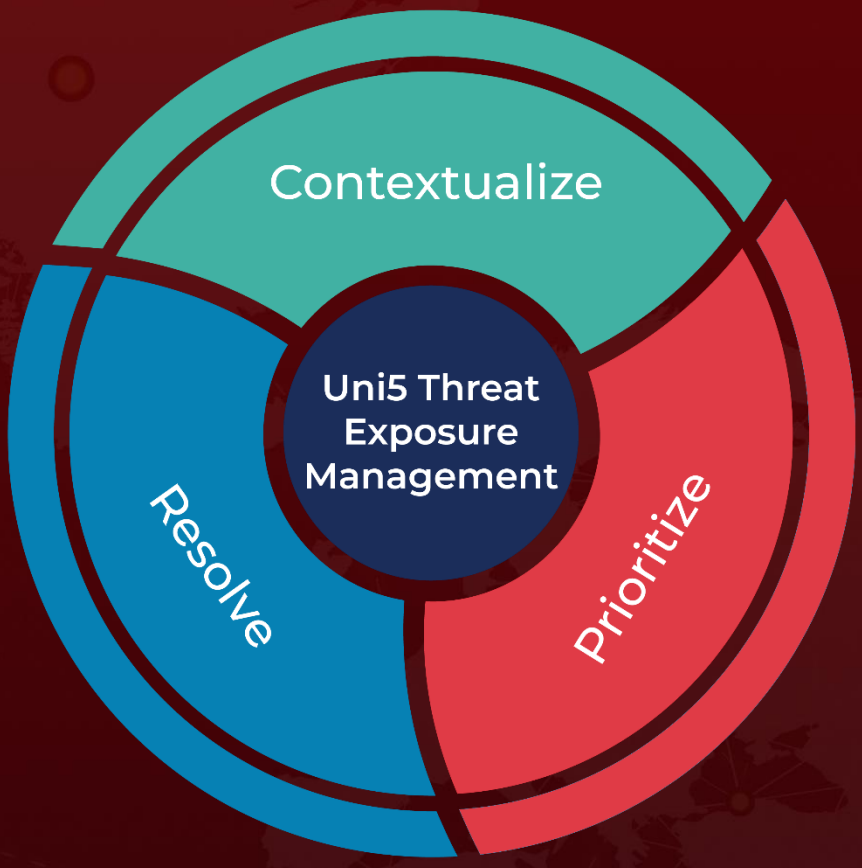
References

https://www.forescout.com/blog/new-ransomware-operator-exploits-fortinet-vulnerability-duo/

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

March 14, 2025 • 5:30 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com