TIR-20250326 SuperBlack Ransomware – A LockBit Variant Exploiting Fortinet Vulnerabilities

3/26/2025

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

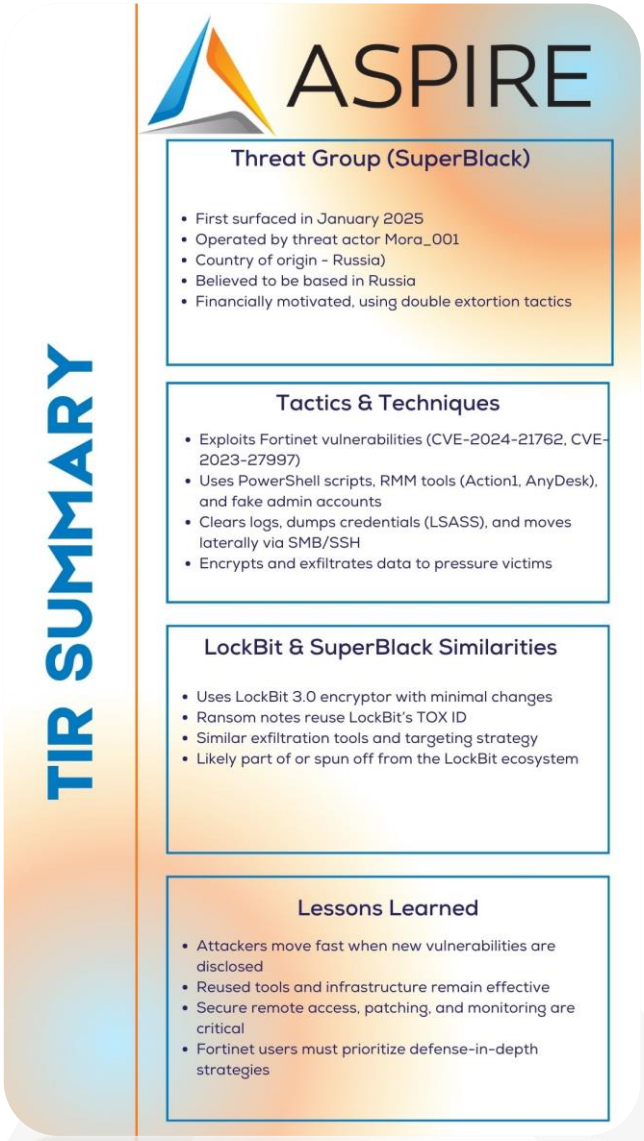
EXECUTIVE SUMMARY

SuperBlack ransomware surfaced in early 2025 and quickly drew attention from security researchers due to its similarities with LockBit 3.0. Operated by a threat actor known as ***Mora_001***, SuperBlack combines LockBit's leaked code with new infrastructure, updated ransom notes, and a data exfiltration tool.

The group was first observed exploiting critical Fortinet vulnerabilities to gain access to victim environments, then pivoting quickly to lateral movement, encryption, and extortion.

SuperBlack appears to be operated out of Russia and has already impacted organizations in the United States, India, and Brazil. Targeted industries include healthcare, manufacturing, technology, and critical infrastructure - sectors that commonly rely on Fortinet's network appliances.

Let’s unpack the technical and operational aspects of SuperBlack, and the vulnerabilities being exploited.



SUPERBLACK RANSOMWARE

Researchers at Forescout's Vedere Labs first spotted SuperBlack in January 2025. What stood out wasn't just the use of LockBit code, but how quickly the actor moved to exploit Fortinet firewalls using recently disclosed vulnerabilities.

SuperBlack doesn't appear to be a fork of LockBit in the traditional sense. Instead, it uses LockBit 3.0's encryptor almost unchanged. The biggest differences lie in the ransom note and the addition of a custom data exfiltration tool. This reuse of infrastructure and tooling—combined with slight rebranding—suggests either a LockBit affiliate or a former operator repackaging the toolset under a new name.

Fortinet Vulnerabilities Being Exploited

Two Fortinet CVEs are at the heart of the initial access technique used by Mora_001:

- **CVE-2024-21762** – A heap-based buffer overflow in FortiOS and FortiProxy that allows unauthenticated attackers to execute arbitrary code using specially crafted HTTP requests.
- **CVE-2023-27997** – Known as XORTIGATE, this pre-authentication remote code execution vulnerability in FortiOS SSL VPN enables attackers to take over affected systems.

Once Mora_001 exploits these bugs, they typically create a privileged account with names like "forticloud-tech" or "fortigate-firewall" to blend in with legitimate admin accounts. From there, they deploy additional tooling, exfiltrate data, and launch the encryption payload.

TIES TO LOCKBIT 3.0

The ransomware payload used by SuperBlack matches the LockBit 3.0 encryptor with very minor modifications. This includes nearly identical encryption methods, file extension behavior, and code structure. What's more telling is that the ransom note includes a TOX ID that had been previously tied to LockBit operations, something rarely reused outside tightly linked groups.

TOX, a peer-to-peer encrypted messaging protocol, is often used by ransomware groups to communicate securely with victims. Because it doesn't rely on centralized infrastructure, TOX is nearly impossible to trace or block without insider access. In this case, the TOX ID found in SuperBlack's ransom note was identical to one used in earlier LockBit campaigns. This kind of reuse - especially of secure, private communication channels - strongly implies a shared operator or overlapping team structure. TOX IDs are rarely recycled unless there's a direct relationship between actors.

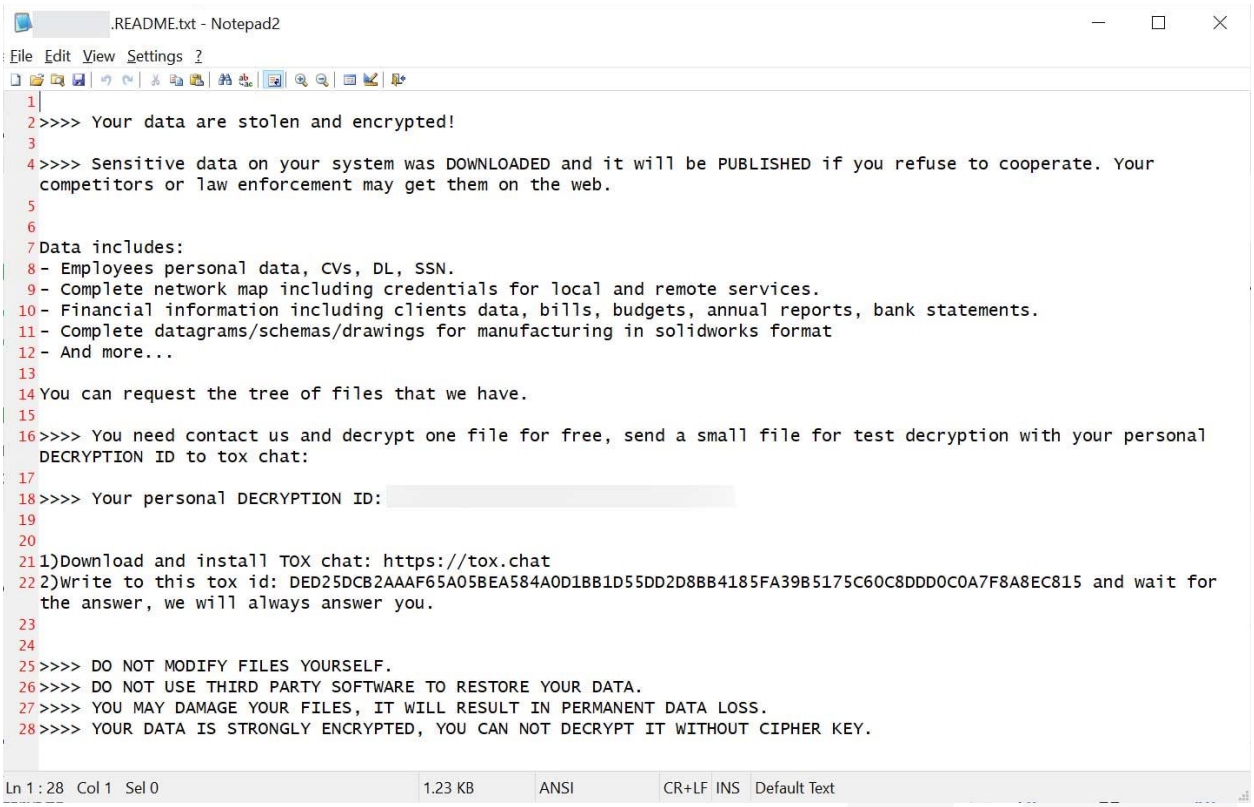
Researchers also identified similarities in SuperBlack's approach to exfiltration and system targeting. The custom data theft tool used by SuperBlack closely mirrors utilities once seen in LockBit incidents, suggesting that ***Mora_001*** may have access to the same internal toolset or developers. This level of consistency, paired with infrastructure reuse, points to more than a casual relationship.

This kind of reuse could mean:

- Mora_001 was a LockBit affiliate who broke off and started their own campaign.
- The encryptor and tools leaked (intentionally or not), and Mora_001 repurposed them quickly.
- SuperBlack is a rebrand or shadow operation being run by someone still aligned with LockBit.

Given the Russian language found in some artifacts, time zone patterns, and longstanding overlaps with LockBit behavior, researchers strongly believe the group is operating out of Russia and is part of the broader LockBit ecosystem - whether officially or unofficially.

SuperBlack Ransomware Note



Source: Forescout

Industries and Regions Being Targeted

SuperBlack is targeting sectors that rely on Fortinet appliances, including:

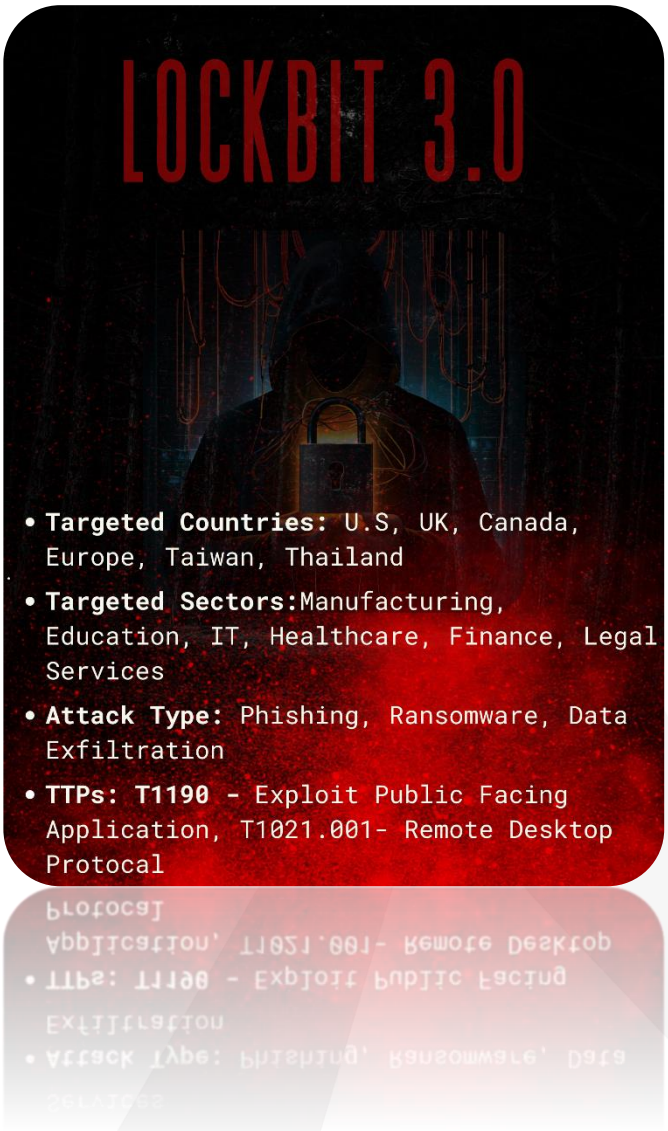
- Healthcare
- Manufacturing
- Government and public sector
- Technology and managed services

Geographically, the top three countries affected so far are:

- United States (with over 7,000 exposed FortiGate firewalls)
- India
- Brazil

Background on LockBit

LockBit is one of the most prolific ransomware operations of the past several years, known for pioneering the double extortion model and running a Ransomware-as-a-Service (RaaS) program that recruited affiliates worldwide. Since its emergence in 2019, LockBit has been linked to thousands of attacks globally, targeting industries across government, healthcare, finance, and manufacturing.



In early 2024, international law enforcement agencies carried out a major disruption of LockBit infrastructure under Operation Cronos. This included the takedown of leak sites, arrests of suspected affiliates, and the seizure of servers. While the core group was temporarily disrupted, many researchers warned that LockBit's affiliates and leaked code would continue to fuel ransomware activity under new names.

SuperBlack is potentially one such case. Whether it's a splinter group, a rogue affiliate, or a deliberate rebrand, the overlap in tooling, tactics, and even communication methods makes it clear that LockBit's playbook is still active - even if the name has changed.

TACTICS & TECHNIQUES

SuperBlack demonstrates a disciplined approach to compromising networks. Their tactics follow a well-defined structure aligned with the MITRE ATT&CK framework but are executed in a way that suggests familiarity with real-world enterprise environments.

Initial Access

The operation often begins with the exploitation of public-facing Fortinet appliances. Specifically, ***Mora_001*** has been observed using CVE-2024-21762 and CVE-2023-27997 to bypass authentication on FortiGate firewalls and gain administrative access. This is a textbook example of Initial Access (T1190 – Exploit Public-Facing Application), using known vulnerabilities as a springboard into the network.

Execution

Once inside, the attacker shifts quickly to Execution (T1059.001 – PowerShell), leveraging script-based commands to disable defenses and prepare for lateral movement. PowerShell is a favored tool because it's already built into Windows and often allowed by default.

Persistence

To stay in the environment without being detected, SuperBlack establishes Persistence through two main methods: creating new privileged user accounts (T1136.001) and deploying remote monitoring tools like Action1 and AnyDesk (T1219). These tools help maintain access over time, especially if the original exploit vector is closed.

Privilege Escalation

SuperBlack also elevates privileges using T1548.002 – Abuse Elevation Control Mechanism, often granting admin rights to the newly created accounts. These accounts blend in by mimicking legitimate Fortinet or IT administrator names.

Defense Evasion

Next, the threat actor attempts to cover their tracks through Defense Evasion techniques like clearing Windows event logs (T1070.001) and using encoded scripts or binaries to bypass detection (T1027 – Obfuscated Files or Information).

Credential Access

Credential harvesting is a vital part of the campaign. The group uses T1003.001 – OS Credential Dumping: LSASS Memory to extract usernames and passwords from memory, which helps them move laterally within the network. Once they have credentials, Lateral Movement (T1021 – Remote Services: SMB/SSH) and Discovery (T1018 – Remote System Discovery) follow, targeting file servers, domain controllers, and other high-value systems.

Lateral Movement and Discovery

Before encryption, SuperBlack quietly exfiltrates sensitive data using a custom-built tool. This step falls under Exfiltration Over C2 Channel (T1041) and is typically done quietly to avoid tipping off defenders. Finally, the operation culminates in Impact (T1486 – Data Encrypted for Impact), where data across multiple systems is encrypted, and a ransom note is dropped with instructions to communicate via TOX.– Systems are encrypted, and ransom notes are dropped.

Recent Attacks

So far, public reporting hasn't confirmed specific victim names, but incident response teams have seen signs of:

- Admin accounts being renamed and reused
- Fortinet firewall logs showing signs of CVE-2024-21762 exploitation
- Use of SSH and RMM tools to maintain access for days or weeks before encryption

Ransom notes instruct victims not to contact law enforcement or recovery companies, claiming that any such attempt will trigger a full data leak. This pressure tactic mimics LockBit's double extortion model.

Conclusion

SuperBlack shows us that the ransomware world doesn't always need something brand new to do real damage. A little bit of recycled code, a known set of vulnerabilities, and some infrastructure tweaks are enough to cause chaos when timing and targeting are right.

This threat actor is quick-moving and has shown that they know how to exploit unpatched Fortinet firewalls effectively. For organizations still running vulnerable versions of FortiOS or FortiProxy, the risk is great.

Ultimately, this is about money. SuperBlack's entire operation is built around financial gain. The group combines encryption with data theft to increase pressure on victims and maximize payouts. Their use of TOX and tailored ransom notes shows a clear intent to maintain control of negotiations and push victims toward payment. Everything about their tactics - from the initial access to the final demand - is focused on profit, not ideology.

Aspire's Recommendations

SuperBlack actively exploits known Fortinet vulnerabilities to gain access to corporate networks. Aspire Technology Partners recommends the following to help keep your organization safe:

Patch Fortinet Devices Immediately

- Make sure CVE-2024-21762 and CVE-2023-27997 are addressed.
- Remove any outdated firmware or end-of-life appliances.

Lock Down Admin Access

- Disable remote management from the internet.
- Use access controls and enforce MFA for all admin accounts.

Look for Suspicious Admin Accounts

- If you see new usernames like "forticloud-tech," investigate immediately.

- Audit for changes to privileged groups.

Segment Your Network

- Don’t let one compromised system become many.
- Use VLANs and firewall rules to separate high-value systems.

Deploy EDR and Monitor Logs

- Look for PowerShell abuse, credential dumping, and lateral movement.
- Set alerts for unexpected logins and account creations.

Educate and Prepare

- Make sure your team knows how ransomware attacks unfold.
- Run table-top exercises so everyone knows what to do when it hits.

MITRE MAP

Initial Access	T1190 – Exploit Public Facing Application
Execution	T1059.001 – Command and Scripting Interpreter: PowerShell
Persistence	T1219 – Remote Access Software
Privilege Escalation	T1548.002 – Abuse Elevation Control Mechanism: Bypass Use Access Control
Defense Evasion	T1070.001 – Clear Windows Event Logs T1027 – Obfuscated Files or Information
Credential Access	T1003.001 – OS Credential Dumping: LSASS Memory
Lateral Movement	T1021.002 - Remote Services: SMB/Windows Admin Shares
Exfiltration	T1041 – Exfiltration Over C2 Channel
Impact	T1486 – Data Encrypted for Impact

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.
  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

INDICATORS OF COMPROMISE (IOCS)

Below is a sample of IoCs for SuperBlack ransomware. Please see a complete list of IoCs here.

IP Addresses

- 109[.]248[.]160[.]118
- 192[.]248[.]155[.]218
- 80[.]66[.]88[.]90
- 185[.]147[.]124[.]31
- 213[.]176[.]64[.]114
- 217[.]144[.]189[.]35
- 5[.]181[.]171[.]133
- 57[.]69[.]19[.]70
- 89[.]248[.]192[.]55
- 94[.]154[.]35[.]208
- 94[.]156[.]177[.]187
- 95[.]179[.]234[.]4
- 95[.]217[.]78[.]122
- 96[.]31[.]67[.]39

SHA256

- 782c3c463809cd818dadad736f076c36cdea01d8c4efed094d78661ba0a57045
- 813ad8caa4dcbd814c1ee9ea28040d74338e79e76beae92bedc8a47b402dedc2
- 917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2
- c994b132b2a264b8cf1d47b2f432fe6bda631b994ec7dcddf5650113f4a5a404
- d9938ac4346d03a07f8ce8b57436e75ba5e936372b9bfd0386f18f6d56902c88
- f383bca7e763b9a76e64489f1e2e54c44e1fd24094e9f3a28d4b45b5ec88b513
- fa3f3f12cee3c18aa50ea8b8e38708cad06875e617164baca8f8ee7156459249

SHA1

- 97b148c27f3da29ba7b18d6aee8a0db9102f47c9

MD5

- 294e9f64cb1642dd89229fff0592856b
- 914685b69f2ac2ff61b6b0f1883a054d

Domains

- Lockbitaptxxx[.]onion
- User[.]group

SUPPORTING DOCUMENTATION

SuperBlack ransomware used to exploit Fortinet vulnerabilities | Cybersecurity Dive

New Ransomware Operator Exploits Fortinet Vulnerability Duo

SuperBlack - a new Lockbit ransomware variant

Police arrest suspected LockBit operator as the ransomware gang spills new data | TechCrunch

Forescout details SuperBlack ransomware exploiting critical Fortinet vulnerabilities - Industrial Cyber

New Ransomware Operator Exploits Fortinet Vulnerability Duo - LevelBlue - Open Threat Exchange

#StopRansomware Guide | CISA

Cyble - Lockbit 3.0 - Ransomware Group Launches New Version

Ransomware Prevention and Response for CISOs — FBI

Lockbit 3.0 Ransomware Group Target Multiple Sectors

Ransomware in 2022: Evolving threats, slow progress | TechTarget

PSIRT | FortiGuard Labs

Analysis of CVE-2023-27997 and Clarifications on Volt Typhoon Campaign | Fortinet Blog

Leaked LockBit 3.0 builder used by 'Bl00dy' ransomware gang in attacks

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.