Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

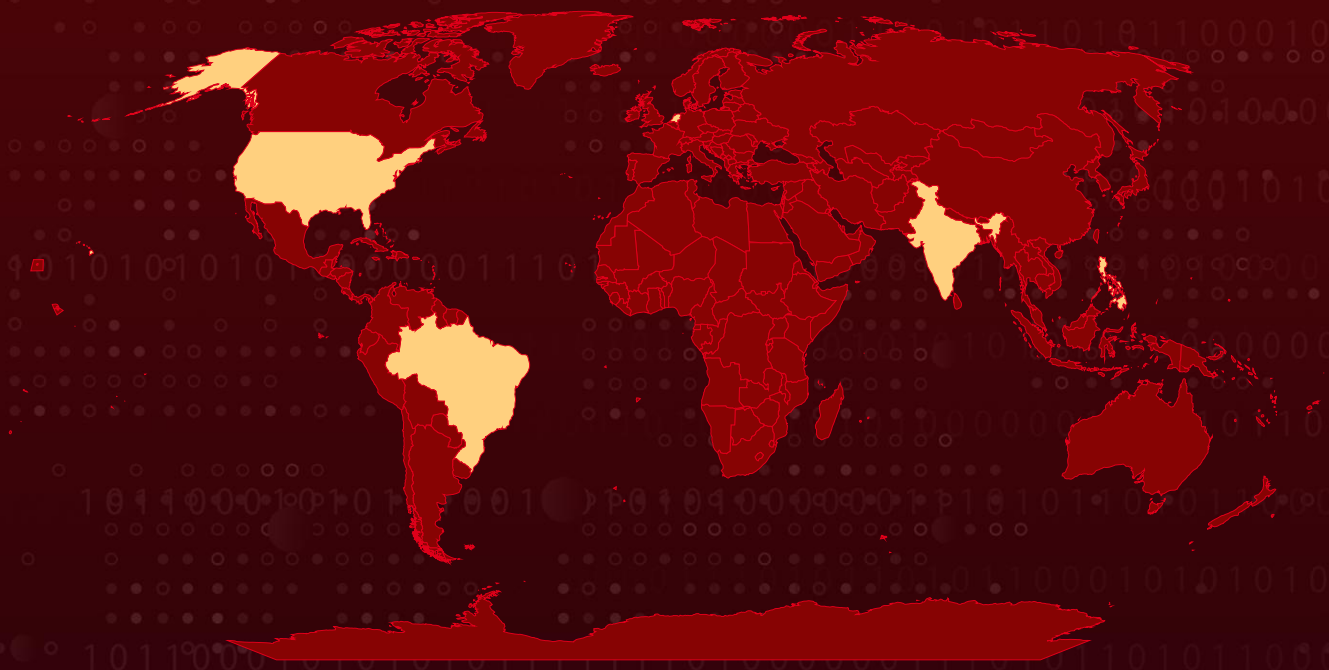
Agenda Ransomware Group Escalates Attacks with New Multi-Stage Loaders

Date of Publication	Admiralty Code	TA Number
May 9, 2025	A1	TA2025143

Summary

First Seen: November 2024
Targeted Countries: India, United States, Netherlands, Brazil, Philippines
Malware: Agenda Ransomware (aka Qilin, Water Galura), SmokeLoader, NETXLOADER
Targeted Platforms: Windows
Targeted Industries: Healthcare, Technology, Financial Services, Telecommunications
Attack: The Agenda (Qilin) ransomware group has evolved its attacks by using NETXLOADER and SmokeLoader to launch stealthy, multi-stage campaigns. NETXLOADER leverages heavy obfuscation to inject malware directly into memory, evading detection. SmokeLoader follows by downloading additional malicious payloads before deploying the Agenda ransomware to encrypt critical systems. This campaign has targeted the healthcare, technology, financial, and telecom sectors across the U.S., Netherlands, Brazil, India, and the Philippines, posing a severe threat to organizations.

Attack Regions



Attack Details

#1

The Agenda ransomware group (also known as Qilin) is a Russian-speaking cybercriminal group first identified around July 2022. It has quickly become a major threat by continually evolving its malware arsenal. Initially written in Go and later rewritten in Rust, Agenda's ransomware gained features such as remote code execution and advanced evasion techniques. The group targets a broad range of critical systems including domain networks, storage infrastructure, and virtual environments like VCenter ESXi making them a serious concern for cybersecurity teams worldwide.

#2

In late 2024, Agenda launched a more advanced attack campaign, signaling a tactical shift through the use of two powerful tools: SmokeLoader, a known malware downloader, and NETXLOADER, a newly discovered .NET-based loader. This combination allowed them to carry out multi-stage attacks with greater stealth and sophistication, increasing the overall risk to targeted organizations.

#3

The attack typically begins with NETXLOADER, which is heavily obfuscated using .NET Reactor 6 to prevent analysis. It employs advanced techniques like JIT hooking and control flow obfuscation to avoid detection. Once executed, it fetches and injects additional payloads from benign-looking, disposable domains directly into system memory bypassing standard security controls.

#4

After this initial stage, SmokeLoader is deployed to deepen the compromise. Known for its versatility, SmokeLoader can retrieve more malware, establish system persistence, and escalate privileges. It also uses dynamic API resolution and evasion techniques to remain undetected. The final payload is the Agenda ransomware itself, which encrypts critical files and systems, often halting business operations entirely.

#5

This campaign has primarily affected organizations in healthcare, technology, finance, and telecommunications across the U.S., Netherlands, Brazil, India, and the Philippines. The combined use of NETXLOADER and SmokeLoader has substantially increased Agenda's threat level, enabling more evasive, coordinated, and damaging attacks that are harder to detect and mitigate.

Recommendations

Restrict access and patch systems: Grant administrative privileges sparingly and keep all security software up to date. Regularly scan for vulnerabilities and ensure endpoint protection can identify or block unknown malware.

Email and web hygiene: Train all staff to be wary of unsolicited emails, attachments, or links. Implement filtering on email and web traffic to block known malicious sites and content. This helps prevent loaders like SmokeLoader or NETXLOADER from reaching user machines in the first place.

Layered security and monitoring: Use a combination of endpoint protection, email security, and network defenses. Employ tools like sandboxing (to safely analyze suspicious files) and SIEM or logging systems to spot unusual activity (e.g. unexpected file creations or outbound connections). Continuous monitoring can help detect abnormal behavior early, before ransomware spreads.

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 Agenda ransomware attack, up-to-date backups enable recovery without paying the ransom.

Potential MITRE ATT&CK TTPs

TA0010 Exfiltration	TA0005 Defense Evasion	TA0002 Execution	TA0004 Privilege Escalation
TA0003 Persistence	TA0011 Command and Control	TA0007 Discovery	TA0040 Impact
T1566 Phishing	T1059 Command and Scripting Interpreter	T1078 Valid Accounts	T1078.001 Default Accounts
T1071.001 Web Protocols	T1071 Application Layer Protocol	T1027.007 Dynamic API Resolution	T1048 Exfiltration Over Alternative Protocol

T1134.002 Create Process with Token	T1027 Obfuscated Files or Information	T1134 Access Token Manipulation	T1622 Debugger Evasion
T1497.001 System Checks	T1036 Masquerading	T1070 Indicator Removal	T1055 Process Injection
T1057 Process Discovery	T1010 Application Window Discovery	T1573 Encrypted Channel	T1573.001 Symmetric Cryptography
T1486 Data Encrypted for Impact	T1490 Inhibit System Recovery	T1480 Execution Guardrails	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	4684aa8ab09a70d0e25139286e1178c02b15920b, f995ec5d88afab30f9efb62ea3b30e1e1b62cdc3, 05bf016c137230bfdc6eaae95b75a56aff76799d, Bdf33e2ba85f35ea86fb016620371fe80855fe68, 16b776ff80f08105b362f9bc76c73a21c51664c2, 1399e63d4662076eeed3b4498c2f958c611a4387
URLs	hxxp[://]serverlogs295[.]xyz/statweb255/index[.]php, hxxp[://]servblog475[.]cfd/statweb255/index[.]php, hxxp[://]demblog797[.]xyz/statweb255/index[.]php, hxxp[://]admlogs457[.]cfd/statweb255/index[.]php, hxxp[://]blogmstat599[.]xyz/statweb255/index[.]php, hxxp[://]bloglogs757[.]cfd/statweb255/index[.]php, hxxp[://]pzh1966[.]com/statweb255/index[.]php, hxxp[://]mxblog77.cfd/777/

Recent Breaches

https://mdgny.com
https://gates-cooper.com
https://jbanksdesign.com
https://clinpath.com
https://gslelectric.com
https://nssjpn.co.jp
https://hcsheriff.gov
https://shraderlaw.com
https://hci66.fr
https://ancc.org
https://newseason.com
https://www.malaysiaairports.com.my
https://www.matrixneworld.com
https://nuovadfl.it
https://dlcid.com
https://www.rfsd13.org
https://bostonconveyorandautomation.com
https://mossyoak.com
https://www.solovue.com
https://rcmanubhai.com.fj
https://www.megachem.com

References

https://www.trendmicro.com/en_us/research/25/e/agenda-ransomware-group-adds-smokeloader-and-netxloader-to-their.html

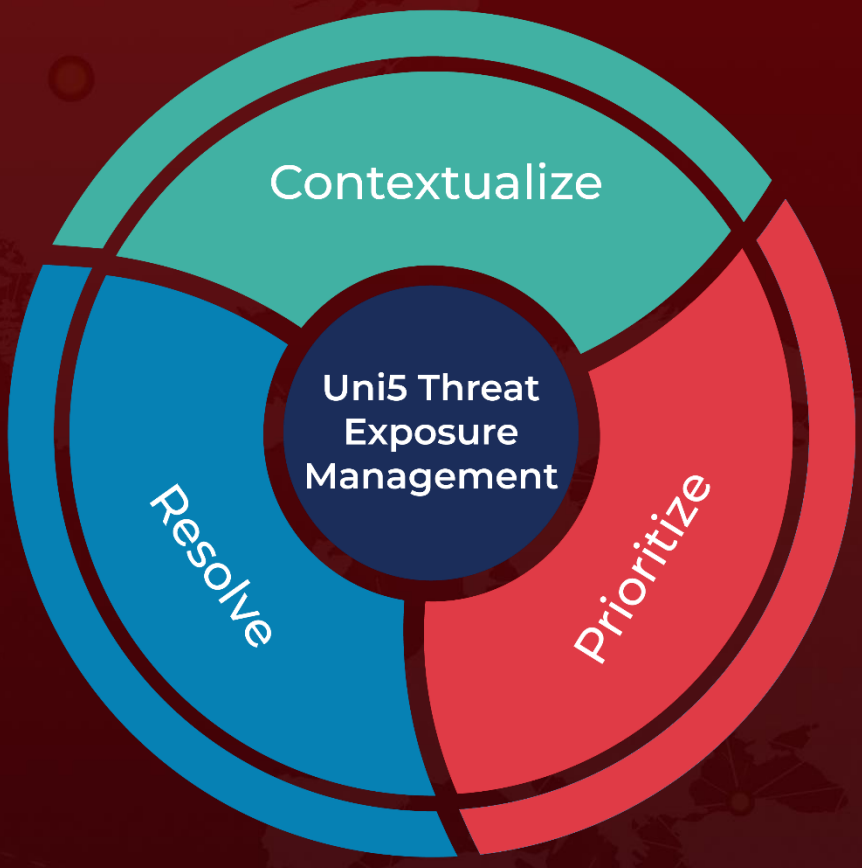
https://documents.trendmicro.com/assets/txt/NETXLOADER-IOCsy4h6Kis.txt

https://www.hivepro.com/threat-advisory/agenda-ransomware-targets-vmware-vcenter-esxi-servers-globally/

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

May 9, 2025 • 6:30 AM

More at www.hivepro.com