Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Nitrogen Ransomware Is Breaking In Without Triggering Any Alarms

Date of Publication

May 22, 2025

Admiralty Code

A1

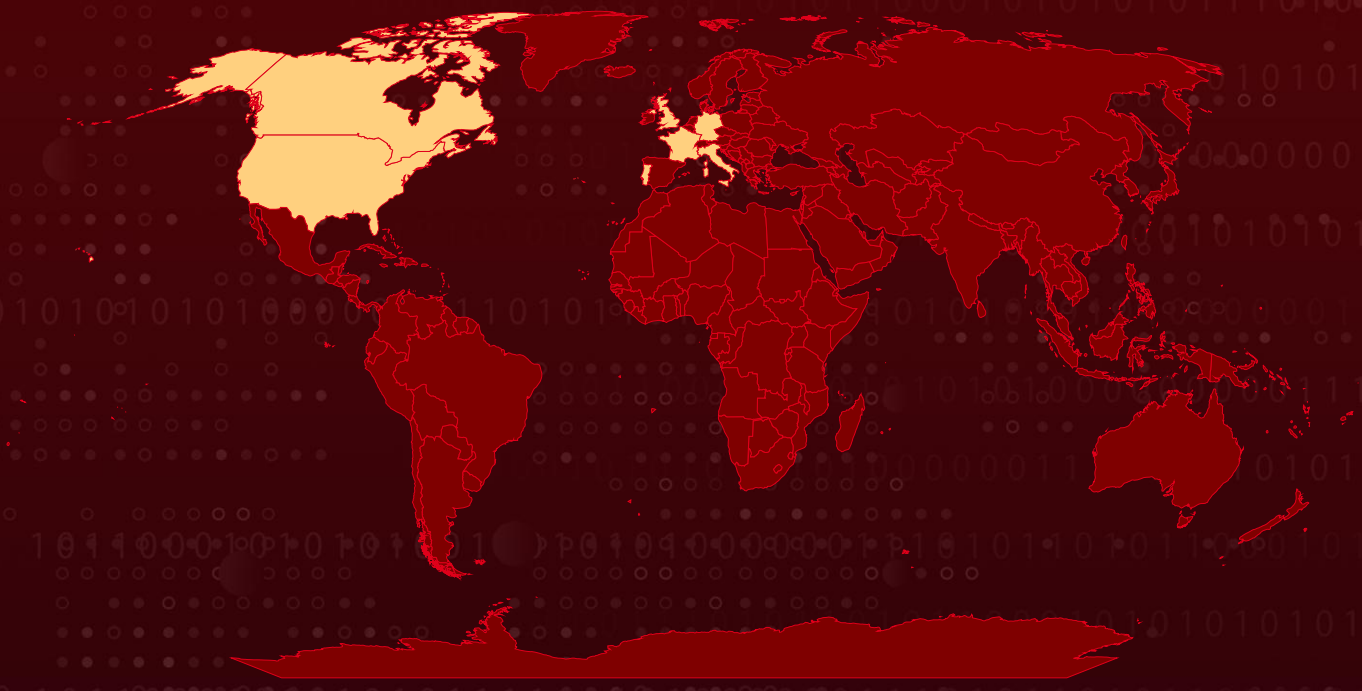
TA Number

TA2025159

Summary

Active Since: September 2024
Malware: Nitrogen Ransomware (aka NitroBlog)
Targeted Countries: United States, Canada, United Kingdom, Portugal, Germany, France, Italy
Targeted Industries: Automotive, Banking, Business Services & Consulting, Casino & Gambling, Construction, Education, Electronics, Energy, Engineering, Finance, Gaming, Hospitality, Investment firms, IT, Manufacturing, Media, Retail, Technology, Utilities
Affected Product: Windows
Ransom: $1,000,000
Attack: Since its emergence in September 2024, Nitrogen ransomware has quickly built a reputation as a serious threat in the cyber landscape, targeting organizations across industries with alarming precision. Its danger lies not only in its ability to encrypt critical data but also in its use of legitimate system tools to bypass defenses, often evading detection while leaving behind encrypted files and ransom notes.

Attack Regions



Attack Details

#1 A formidable ransomware strain known as Nitrogen has rapidly emerged as a significant threat, particularly targeting the financial sector. First detected in September 2024, Nitrogen has swiftly built a notorious reputation for its sophisticated attack techniques and the severe damage it inflicts on victim organizations.

#2 Over the past four months, the Nitrogen ransomware group has maintained a highly active and aggressive campaign. While financial services remain a primary target, their operations have extended across a broad spectrum of industries, including construction, manufacturing, and technology. These attacks have spanned multiple regions, with a marked concentration in the United States, Canada, and the United Kingdom.

#3 Notably, Nitrogen bears several similarities to the earlier LukaLocker ransomware. Like its predecessor, Nitrogen follows the double-extortion model, encrypting sensitive data and demanding a ransom for its release while threatening to publicly leak stolen information. What sets Nitrogen apart, however, is the complexity of its attack chain and the deceptive strategies it employs to evade detection.

#4 The infection process often begins with malvertising campaigns on popular search engines such as Google and Bing. Once the malicious payload is executed, the ransomware enumerates all active processes on the compromised machine, storing this information for subsequent use.

#5 It then searches specifically for truesight.sys, a legitimate driver associated with RogueKiller AntiRootkit. This driver, cataloged in LOLDrivers, a list of living-off-the-land (LOTL) binaries, is exploited to terminate antivirus and endpoint detection processes. Because the driver itself is not inherently malicious, it bypasses standard security defenses without raising immediate alarms.

#6 In addition, Nitrogen disables Safe Boot, a critical Windows recovery feature, effectively cutting off one of the primary avenues for restoring infected systems. Once these defensive layers have been neutralized, the attackers deploy their ransomware payload.

#7 The malware attempts to terminate various processes, encrypt files across the system, appending a .NBA extension to each, and leaves behind a ransom note titled readme.txt in multiple directories, detailing payment demands and instructions for data recovery.

Recommendations

Avoid Interacting with Unverified Ads and Links: Malvertising campaigns often disguise malicious payloads within seemingly legitimate advertisements on popular search engines and websites. Avoid clicking on sponsored results or banner ads from unknown or untrusted sources. Always access official vendor sites directly by typing the URL and be cautious with downloads or promotions that seem too good to be true they are often bait for delivering malware.

Backup & Recovery Preparedness: Maintain offline, immutable, and regularly tested backups. Ensure recovery time objectives (RTOs) and recovery point objectives (RPOs) meet business continuity requirements in the event of ransomware deployment.

Network Segmentation & Zero Trust Implementation: Segment critical infrastructure to isolate sensitive data and limit lateral movement. Implement Zero Trust Network Access (ZTNA) by enforcing identity-based policies rather than traditional perimeter security.

Implement the 3-2-1 Backup Rule: Maintain three total copies of your data, with two backups stored on different devices and one backup kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

Establish a Ransomware-Specific Incident Response Plan: Develop a clear, actionable incident response strategy tailored to ransomware attacks, with predefined roles, communication protocols, and decision trees.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0007 Discovery	TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration
TA0040 Impact	T1204 User Execution	T1204.002 Malicious File	T1057 Process Discovery

T1562 Impair Defenses	T1562.001 Disable or Modify Tools	T1562.009 Safe Mode Boot	T1037 Boot or Logon Initialization Scripts
T1486 Data Encrypted for Impact	T1490 Inhibit System Recovery	T1071.001 Web Protocols	T1005 Data from Local System
T1082 System Information Discovery	T1583 Acquire Infrastructure	T1583.008 Malvertising	T1189 Drive-by Compromise
T1211 Exploitation for Defense Evasion	T1007 System Service Discovery		

Indicators of Compromise (IOCs)

TYPE	VALUE
TOR Address	nitrogenczslprh3xyw6lh5xyjvmsz7ciljoqxxknd7uymkfetfhgvqd[.]onion, bf7dw4n6zne6rbgjlpcsidphpk753nkyubipkym5t4pntgfyb6clw2qd[.]onion, xqsdbtrtmufdyiqnkrkvosec4gqappf2egcptzqppjtqdevsoadakyqd[.]onion
Tox ID	46CA5EEC55A16767B7F8293DB18F753D1BF60C536747EFD115035DDA40948427E1DDFD107F03, 088B7708F2C1557B6023B1102FFC5C36C023FF4883CB073F26A33B73832C9268993ED58B817E, C1DD64D0994AEAA297225CD94D1A6842819C74319A85350913AB9A82678C001EB09B71214D66, 620C7A54EC212FB482A684BA74381C3623CCE4D0E27FAE348688F65E0F0F6B6A149790D1AE7D
Mutex	nvxkjcv7yxctvgsdfjhv6esdvsx
SHA256	5dc8b08c7e1b11abf2b6b311cd7e411db16a7c3827879c6f93bd0dac7a71d321, 9514035fea8000a664799e369ae6d3af6abfe8e5cda23cdafbede83051692e63, ab366a7c4a343a798490c4451d1d8e42aea2b894cb3162b5c59e08d8507ffe2c, c94b70dff50e69639b0ef1e828621c5fddcf144fea93e27520f48264ddd33273, 0db5c55ef52e89401a668f59bf4f69391f4632447c51483bb64749d7f2123916,

TYPE	VALUE
SHA256	779576719a9c400a7a4abed0386e2111eb331160572c91a2fd8eaa1a7d6e6c63, e6a498b89aa04d7c25cbfa96599a4cd9bdcc79e73bf7b09906e5ca85bda2bff6, 55f3725ebe01ea19ca14ab14d747a6975f9a6064ca71345219a14c47c18c88be, fa3eca4d53a1b7c4cfcd14f642ed5f8a8a864f56a8a47acbf5cf11a6c5d2afa2, bfc2ef3b404294fe2fa05a8b71c7f786b58519175b7202a69fe30f45e607ff1c

Recent Breaches

https://mardearhotels.com/en/
https://www.stadtwerke-schwerte.de/
https://www.globalmediagroup.pt/
https://senecagames.com/
https://www.akto.fr/
https://www.sirius.to.it/
https://reiusa.net/
https://srpfcu.org/

References

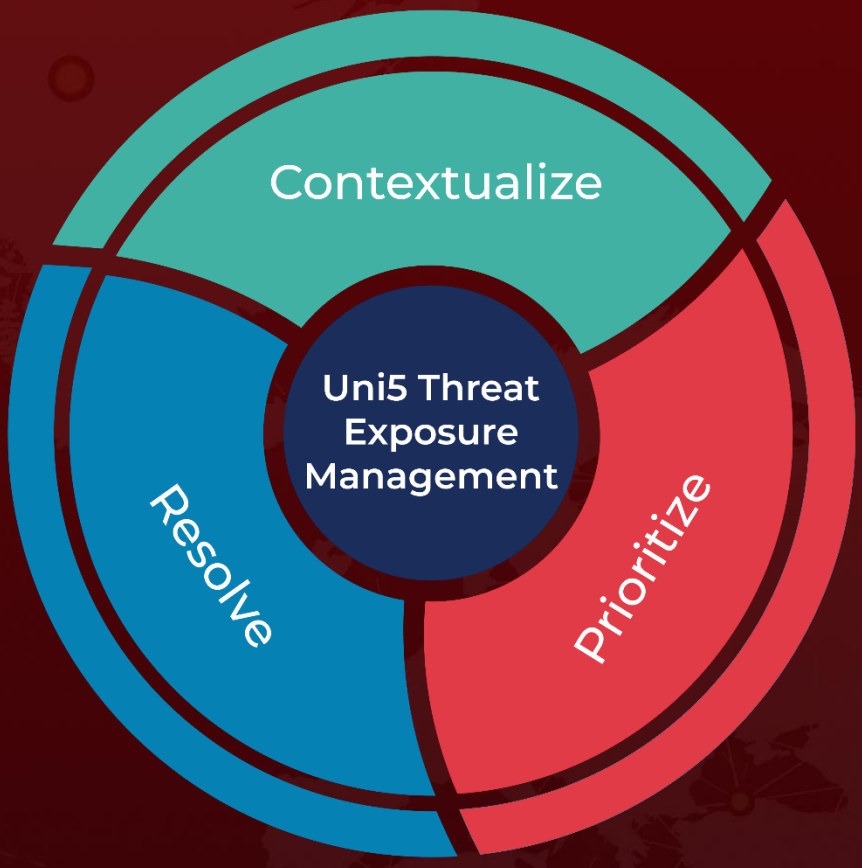
https://any.run/cybersecurity-blog/nitrogen-ransomware-report/

https://thedfirreport.com/2024/09/30/nitrogen-campaign-drops-sliver-and-ends-with-blackcat-ransomware/

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 22, 2025 • 3:30 AM

More at www.hivepro.com