Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

NailaoLocker Ransomware: Basic Design, Deadly Reach

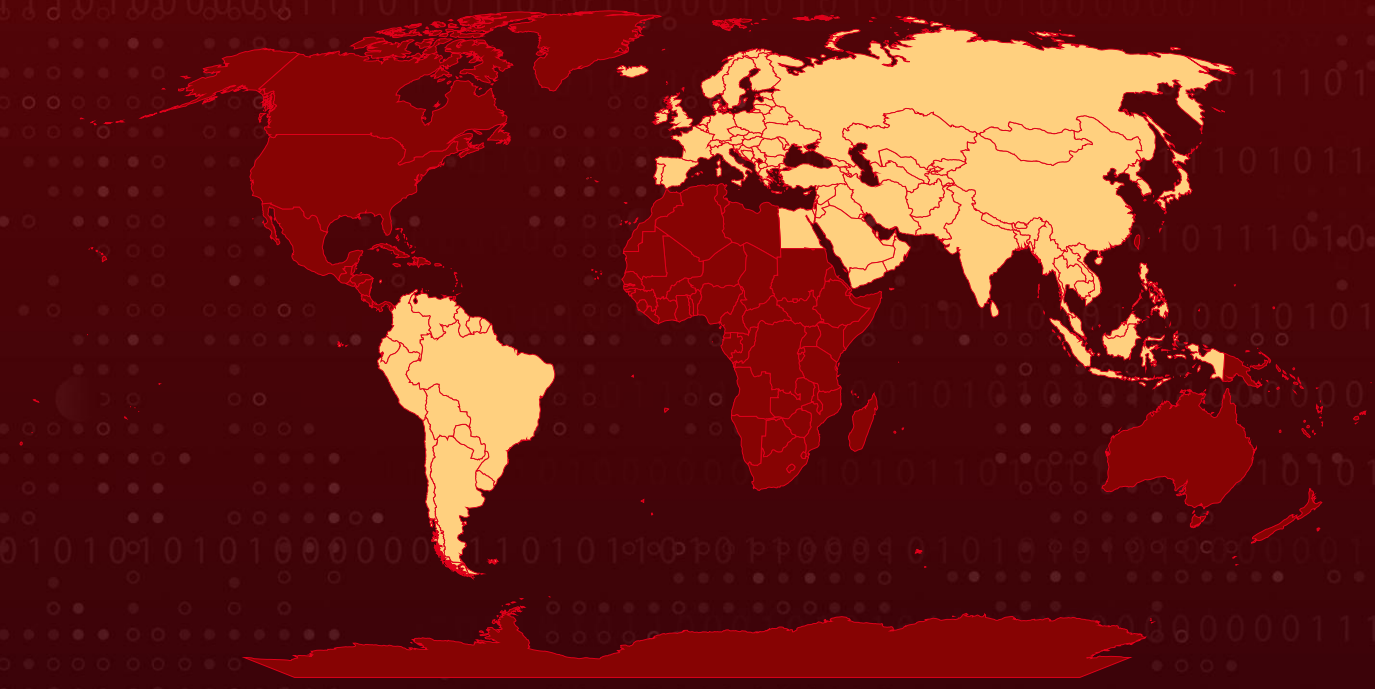
Date of Publication	Admiralty Code	TA Number
February 21, 2025	A1	TA2025054

Summary

Attack Commenced: November 2024
Malware: NailaoLocker Ransomware, Shadowpad, PlugX
Targeted Industries: Manufacturing, Transportation, Publishing, Energy, Pharmacy, Banking, Mining, Education, Entertainment
Targeted Regions: Europe, Middle East, Asia, South America

Attack: A new ransomware threat NailaoLocker has surfaced making waves in the cyber world with its unexpected simplicity and dangerous associations. Exploiting a Check Point Security Gateway vulnerability, this basic yet effective malware infiltrates networks, teaming up with notorious tools like ShadowPad and PlugX, often linked to Chinese state-sponsored hackers.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-24919	Check Point Security Gateway Information Disclosure Vulnerability	Check Point Security Gateway	✓	✓	✓

Attack Details

#1 A newly discovered ransomware strain NailaoLocker has emerged in recent cyberattacks, exploiting CVE-2024-24919 a vulnerability in Check Point Security Gateway to infiltrate targeted networks. Once inside, attackers deploy ShadowPad and PlugX, two notorious malware families long associated with Chinese state-sponsored threat groups.

#2 Despite its malicious intent, NailaoLocker is relatively rudimentary. Written in C++, it lacks the sophisticated features often seen in modern ransomware. It doesn't terminate security processes, evade sandbox environments, or scan for network shares. This simplistic design suggests that full encryption wasn't its primary goal.

#3 The infection process begins with DLL sideloading, where the ransomware piggybacks on a legitimate, signed executable. This executable acts as a loader dubbed NailaoLoader which first validates the environment through memory address checks. Once verified, it decrypts the main payload and injects it into memory.

#4 NailaoLocker then activates its encryption routine, using AES-256-CTR to lock files and append the ".locked" extension. After completing the encryption, it drops an HTML ransom note notably with an unusually long filename demanding payment for decryption.

#5 What makes this campaign particularly concerning is the integration of ShadowPad, a modular backdoor that has been in exclusive use by Chinese espionage actors since at least 2015. In this case, ShadowPad was used post-exploitation to bypass weak passwords and multi-factor authentication, paving the way for NailaoLocker's deployment.

#6 The scope of the attack is significant. Threat actors have reportedly targeted 21 companies across 15 countries, spanning nine industries. This wide-reaching campaign highlights the evolving tactics of state-linked cyber groups and the growing risks posed by even unsophisticated ransomware.

Recommendations

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.

Regularly Test Backup Restores: Conduct frequent tests to verify the integrity of backup data and ensure that restoration processes work as intended. This practice helps identify any issues before an actual data recovery scenario arises.

Patch Known Vulnerabilities Immediately: NailaoLocker exploits CVE-2024-24919, a known vulnerability in Check Point Security Gateway, to gain initial access. Organizations must prioritize timely patch management, especially for critical infrastructure and security devices.

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.

Conduct Ransomware Simulation Drills: Test the organization's resilience against ransomware attacks by conducting simulated scenarios to identify gaps in preparedness.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0040 Impact	TA0006 Credential Access	TA0009 Collection
TA0010 Exfiltration	TA0011 Command and Control	T1190 Exploit Public-Facing Application	T1574.002 DLL Side-Loading

T1574 Hijack Execution Flow	**T1204** User Execution	**T1204.002** Malicious File	**T1055.012** Process Hollowing
T1140 Deobfuscate/Decode Files or Information	**T1083** File and Directory Discovery	**T1486** Data Encrypted for Impact	**T1555** Credentials from Password Stores
T1560 Archive Collected Data	**T1560.001** Archive via Utility	**T1041** Exfiltration Over C2 Channel	**T1055** Process Injection
T1059 Command and Scripting Interpreter	**T1027** Obfuscated Files or Information	**T1212** Exploitation for Credential Access	**T1105** Ingress Tool Transfer

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	updata[.]dsqurey[.]com, time[.]dsqurey[.]com, dscriy[.]chtq[.]net, system[.]chtq[.]net, updata[.]chtq[.]net, network[.]oossafe[.]com, notes[.]oossafe[.]com, caba[.]superdasqe[.]me, ccs[.]superdasqe[.]me, czs[.]superdasqe[.]me, kzb[.]superdasqe[.]me
SHA256	8d44f2f442ca8f2fbbf75086a6f8d518c300ca93fe9957a9716076919b475865, 83c1a668ab06f55e6879593ca24eed9f78832be97ac90bb74ef5828067f2d900, c19be7a006bd2ba8deb56dcc6127a76f9624c6f1392a1794870dbed6f1a81bd5, c4db25ab55af2e943a297a5ecf7a62acc3ad8897ec8ba4ab3226a138da237b82, 28e6362ecf033b2a26c7457dcbd7ad2ab34e253fb08666d39073391a1254ea41, 7416f6b69b34b3a36a86e50808e1dc47f4dc665bfd6f394cef65e0ba5eaf961b, bc490047fe6e0b0000c6cd147d3cf483105c92cf00450bfe35ac70f276a9e5c8,

TYPE	VALUE
SHA256	c5f8a256d0969e253633160b9728b6c2bc044f536e92af178a05a598aaa09c1f, a2bb321d41b2300e80f9400950fa2125470d5b3927933ab4d6397f0cbf81532a, d74b6b2129936377aaccc619bcfd4df4ffbe2f35f960a4b043b23ae78a31ec35, 366ea3377eaefa28b655b530710c03fb2ace67bb531b1820e916cb02023892ba, f8915c5be0649642dac22572355f1462972f5087471f66f6a243f2374b208eb8, b38dab1ee402f731313d697d5d79372ae97fcab5704077771b5b82e705e0cd6d, 625ed0e0ad7d3fbf2738349c767a7990c9f0d388de66104e11df3e0c4632033c, 431a630983cd327fc70ea49b3a5497a179dbde19d8f13d2cfceef4e47613024b, e1d72b0cfc3342b8a6436e3047c3cc54246c346ac179e459d07620d192ba6e01, fa7f2ddf91980d639a87465bd2a38eaa44d6079b11ace3b2b3dff03caed66de5, b28bc39e569aa0cfe984c341830cb037c5305877ba22a940c3bdaeb43ca87878, 571607c7f55c3616e4c58db15e3d55317da10294dbc10e0cd1ed24879b8fc051, bc5b2ef81593095696433877cccb0ab75ef942258ef4795de5538df842d952f4, fa3a3351cd55089d40a7311e4bfaf15e4247416f78383d94ad58809467429b3e, 2df4c7bfa608ca88d9d659358894226910850ac0d7e566c6c10ec2727361d47b, b66660dfe1ce69f706aaa412fcd3ff18554d604df59c09adc2a8117417967ce9, 7b8ea6b1e2a29190cb28fc98ef837bf4a7a0b71b84177ce9395a5113a843c4d3, de4bb30e400f081601d4091206ba6c04ac502f50e0dbac879db8c0202bff8108, 5dc36e687a7fa3cfbf845e8a53173f37ac38559b6b87f9dcf609a72b3f284035, 37039a761114251f4556e4fe41c3ec01b7206a483c4698ffe5a0f1617a8bc26b, fcb8bf42d852526214578ab4b477b29f2412a7a931c6353db4fa6c221661edf4, ceac8b67f19d596b2c2f34d682f88c717d11dd4c1144e2e7439b6bb78adb1736, 9df4624f815d9b04d31d9b156f7debfd450718336eb0b75100d02cb45d47bd9a,

TYPE	VALUE
SHA256	28d78e52420906794e4059a603fa9f22d5d6e4479d91e9046a97318c83998679, bdf019bc6cfb239f0beae4275246216cd8ae8116695657a324497ec96e538aac, 41128b82fa12379034b3c42bdecf8e3b435089f19a5d57726a2a784c25e9d91f, c8268641aecad7bd32d20432da49bb8bfc9fe7391b92b5b06352e7f4c93bc19e, e06710652fa3c8b45fd0fece3b59e7614ad59a9bc0c570f4721aee3293ecd2d1, f4e8841a14aaa38352692340729c3ed6909d7521dd777518f12b8bd2d15ea00c5, Aa1233393dded792b74e334c50849c477c4b86838b32ef45d6ab0dc36b4511e3

Patch Link

https://support.checkpoint.com/results/sk/sk182336

References

https://www.trendmicro.com/en_us/research/25/b/updated-shadowpad-malware-leads-to-ransomware-deployment.html

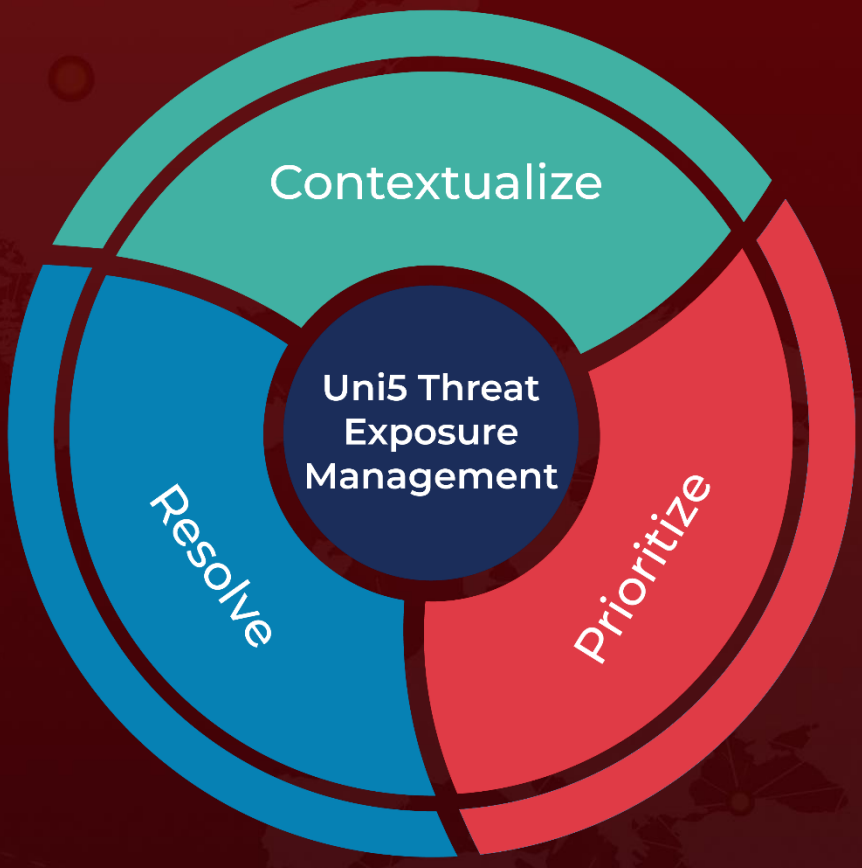
https://www.orangecyberdefense.com/global/blog/cert-news/meet-nailaolocker-a-ransomware-distributed-in-europe-by-shadowpad-and-plugx-backdoors

https://hivepro.com/threat-advisory/check-point-fixes-zero-day-cve-2024-24919-exploited-in-the-wild/

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

February 21, 2025 • 5:30 AM

More at www.hivepro.com