Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

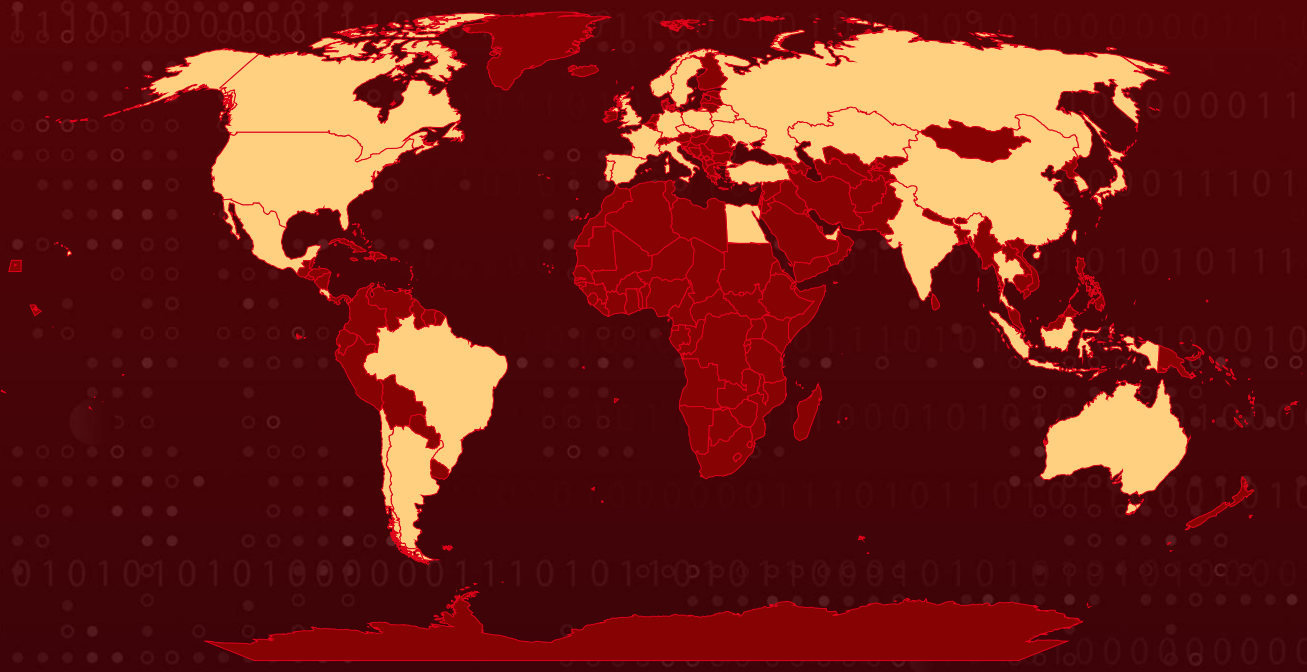
NightSpire Ransomware Expands Reach with Aggressive Extortion Deadlines

Date of Publication	Admiralty Code	TA Number
September 3, 2025	A1	TA2025266

Summary

First Seen: February 2025
Targeted Countries: United States, Japan, Thailand, United Kingdom, China, Poland, Hong Kong, Taiwan, Russia, Belarus, Kazakhstan, Ukraine, Brazil, Turkey, Mexico, Spain, Egypt, Canada, Australia, Italy, Portugal, India, Norway, United Arab Emirates, France, Argentina, South Korea
Targeted Platforms: Windows
Targeted Industries: Retail, Wholesale businesses, Chemical, Healthcare, Maritime, Accounting services, Manufacturing, Business services, Construction, Technology, Financial services, Insurance, Real estate, Agriculture, Transportation, Legal, Education, Hospitality
Malware: NightSpire ransomware
Attack: NightSpire is a Ransomware-as-a-Service group active since early 2025, gaining access through vulnerabilities like CVE-2024-55591 in FortiOS. It moves laterally with LOLBins, dumps credentials, and exfiltrates sensitive data before encrypting files with the ".nspire" extension using a hybrid AES/RSA routine. Victims face double-extortion through ransom notes and a leak site with aggressive deadlines as short as two days.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-55591	Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability	Fortinet FortiOS and FortiProxy	✓	✓	✓

Attack Details

#1

The NightSpire ransomware group, first identified in February 2025, operates under a Ransomware-as-a-Service (RaaS) model and leverages a dedicated leak site (DLS) with countdown timers to pressure victims. It has already targeted a wide range of industries worldwide, including retail, manufacturing, chemicals, maritime, and finance, by adopting a double-extortion model that combines data theft with file encryption. Victims face ransom demands alongside threats of public disclosure, with short deadlines that can be as brief as two days.

#2

NightSpire typically gains initial access by exploiting vulnerabilities in exposed services. Notably, the group has weaponized a FortiOS zero-day (CVE-2024-55591), as well as using opportunistic RDP brute force attacks on cloud hosts and phishing campaigns. Once inside, the attackers conduct lateral movement and privilege escalation using “living-off-the-land” techniques with tools like PowerShell, PsExec, WinSCP, and WMI. They frequently dump credentials with Mimikatz, while the ransomware payload, written in Go, employs obfuscation methods such as AES, RC4, and XOR to evade detection.

#3

Before deploying encryption, NightSpire actors perform data exfiltration to strengthen extortion leverage. Legitimate file transfer tools such as WinSCP and MEGACmd are used to steal sensitive information and upload it to attacker-controlled infrastructure. Once data theft is complete, the ransomware encrypts files, appends the “.nspire” extension, and drops ransom notes (e.g., readme.txt) in each affected directory. The encryption scheme uses a hybrid routine: block encryption (1 MB chunks) for file types like .iso, .vhdx, and .zip to accelerate the process, and full encryption for other files.

#4

Unlike some ransomware families, NightSpire does not alter the desktop background or remove volume shadow copies, though recovery remains difficult. Its growing victim list and cross-sector impact highlight both its effectiveness and reach.

Recommendations

Patch and Secure Remote Access: Apply security updates promptly, especially for firewalls, VPNs, and other services exposed to the internet. Limit RDP exposure, enforce multi-factor authentication (MFA) on all remote access, and monitor for unusual login attempts.

Endpoint and Server Hardening: Use advanced EDR/XDR solutions to detect behaviors linked to NightSpire, such as process tampering, disabling of logging services, or termination of backup processes. Configure application controls (e.g., AppLocker or WDAC) to block unauthorized executables. Monitor for encryption indicators like the creation of .nspire file extensions and rapid deletion of shadow copies.

Network Segmentation and Traffic Control: Segment the internal network to limit lateral movement between endpoints, especially for privileged and critical systems. Apply strict firewall rules and network policies to restrict outbound traffic, particularly to known malicious domains, Tor exit nodes, and suspected command-and-control (C2) infrastructure.

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

Potential MITRE ATT&CK TTPs

TA0010 Exfiltration	TA0040 Impact	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access

T1190 Exploit Public-Facing Application	T1059.001 PowerShell	T1059 Command and Scripting Interpreter	T1068 Exploitation for Privilege Escalation
T1036 Masquerading	T1218 System Binary Proxy Execution	T1486 Data Encrypted for Impact	T1485 Data Destruction
T1046 Network Service Discovery	T1083 File and Directory Discovery	T1021 Remote Services	T1021.001 Remote Desktop Protocol
T1585.002 Email Accounts	T1585 Establish Accounts	T1588.002 Tool	T1588 Obtain Capabilities
T1003.001 LSASS Memory	T1003 OS Credential Dumping	T1482 Domain Trust Discovery	T1041 Exfiltration Over C2 Channel
T1573 Encrypted Channel	T1583.006 Web Services	T1583 Acquire Infrastructure	T1078 Valid Accounts
T1110 Brute Force	T1021.002 SMB/Windows Admin Shares	T1027 Obfuscated Files or Information	T1567 Exfiltration Over Web Service
T1567.002 Exfiltration to Cloud Storage			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	2bf543faf679a374af5fc4848eea5a98, e2d7d65a347b3638f81939192294eb13, 35cefe4bc4a98ad73dda4444c700aac9, f749efde8f9de6a643a57a5b605bd4e7, 0170601e27117e9639851a969240b959

TYPE	VALUE
SHA1	7a4aee1910b84c6715c465277229740dfc73fa39
SHA256	35cefe4bc4a98ad73dda4444c700aac9f749efde8f9de6a643a57a5b605bd4e7, 32e10dc9fe935d7c835530be214142041b6aa25ee32c62648dea124401137ea5, d5f9595abb54947a6b0f8a55428ca95e6402d2aeb72cbc109beca457555a99a6
TOR Address	hxxp[://]nspireyzmvapgiwgtuoznlafqvlyz7ey6himtgn5bdvdcowfyto3yryd[.]onion/, hxxp[://]nspireyzmvapgiwgtuoznlafqvlyz7ey6himtgn5bdvdcowfyto3yryd[.]onion/datas[.]php, hxxp[://]a2lyiiaq4n74tlgz4fk3ft4akolapfrzk772dk24iq32cznjsmzpanqd[.]onion/, hxxp[://]nspiremkiq44zcxjbgvab4mdedyh2pzj5kzbmvftcugq3mczx3dqogid[.]onion/, hxxp[://]nspirebcv4sy3yydtaercuut34hwc4fsxqqv4b4ye4xmo6qp3vxhulqd[.]onion/, hxxp[://]nspirebcv4sy3yydtaercuut34hwc4fsxqqv4b4ye4xmo6qp3vxhulqd[.]onion/database
IPv4	14[.]139[.]185[.]60
Email	night[.]spire[.]team[@]gmail[.]com, night[.]spire[.]team[@]proton[.]me, night[.]spire[.]team[@]onionmail[.]org, nightspireteam[.]receiver[@]proton[.]me, nightspireteam[.]receiver[@]onionmail[.]org
File Names	7z2408-x64.exe, 7zG.exe, 7z.exe
Hostname	WINDOWS-DTX-8GB, XDRAGON-SERVER1
TOX ID	3B61CFD6E12D789A439816E1DE08CFDA58D76EB0B26585AA34CDA617C41D5943CDD15DB0B7E6

Patch Link

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

Recent Breaches

https://botaspistolero.com
https://juliaevansaccountants.co.uk
https://fam-eg.site123.me
https://www.csspv.cz
https://sisnet.co.cr
https://www.w8textil.com.br
https://sg268305-melco-capital-pte-ltd.contact.page
https://www.mfr.fr
https://www.mpinfo.com.tw
https://ardon45.fr
https://www.dplaw.com
https://www.chansn.com.tw
https://www.promenadevillagedental.com
https://www.compliancecg.com
https://pupk-indonesia.com
https://emotrans-chile.cl
https://zaphirauniformes.com.ar
https://www.nicera.co.jp
https://sistel-connections.com
https://www.poolrenovation.com
https://a3t.lu
https://stort.nu
https://stort.nu

References

https://asec.ahnlab.com/en/89913/

https://cyble.com/threat-actor-profiles/nightspire-ransomware-group/

https://www.s-rminform.com/latest-thinking/ransomware-in-focus-meet-nightspire

https://socradar.io/dark-web-profile-nightspire-ransomware/

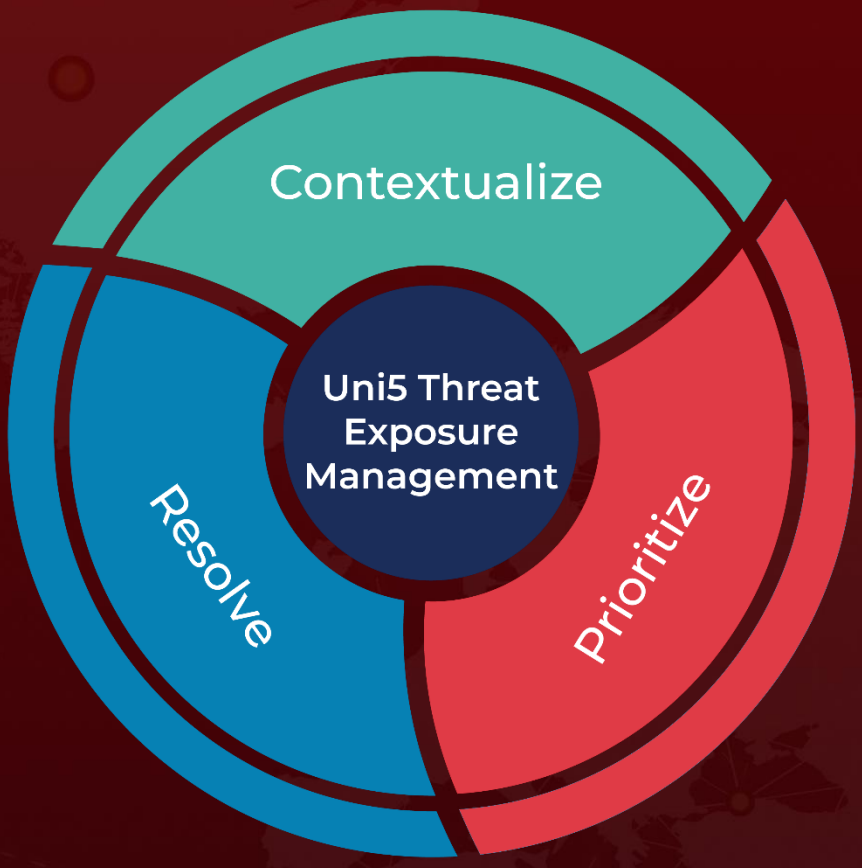
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/nightspire

https://hivepro.com/threat-advisory/fortinet-firewalls-under-siege-exploitation-of-critical-zero-day-cve-2024-55591/

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

September 3, 2025 • 11:40 PM

More at www.hivepro.com