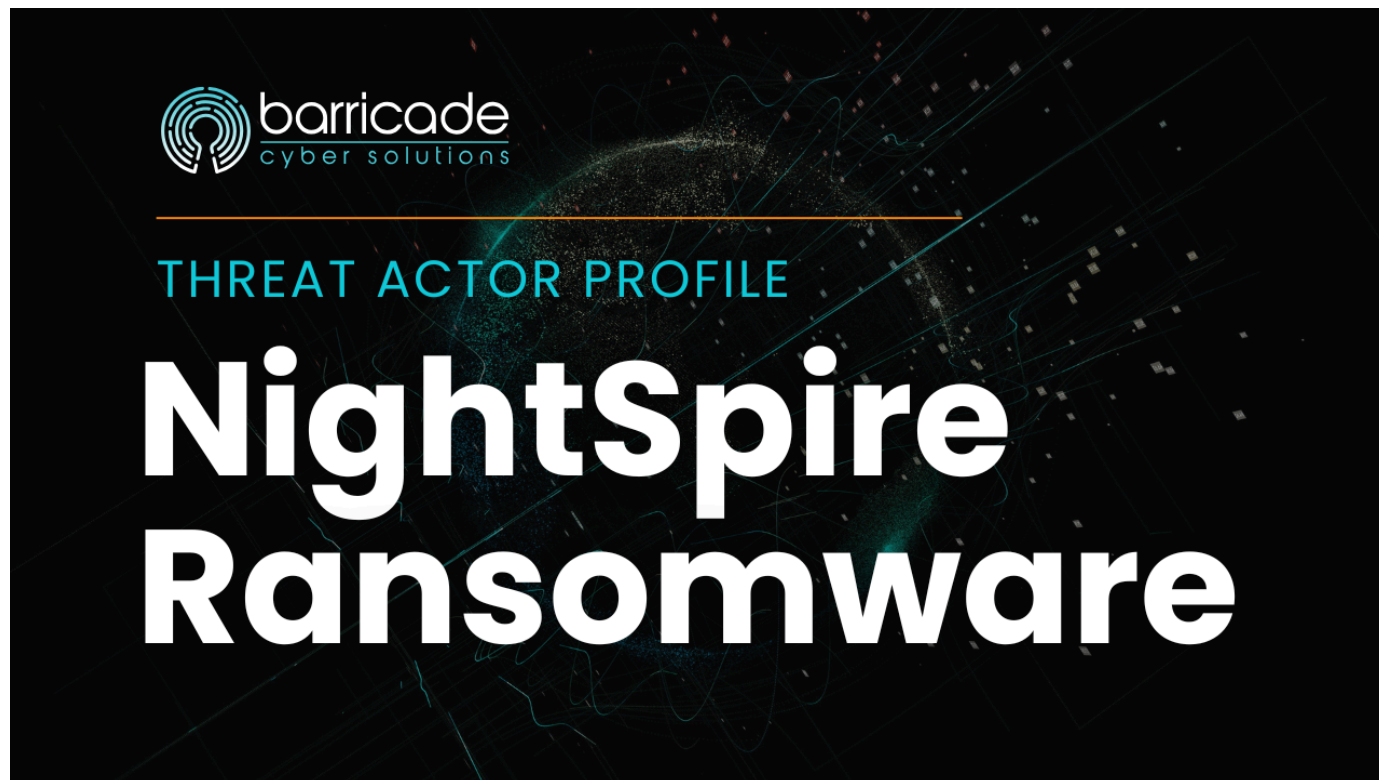


NightSpire Ransomware: Threat Actor Profile

 barricadecyber.com/nightspire-ransomware

Eric J. Taylor

September 16, 2026



In this profile

- [Executive Summary](#)
- [NightSpire at a Glance](#)
- [Who Is Behind It](#)
- [How They Get In](#)
- [What They Do Once Inside](#)
- [Who They Hit: Eighteen Months of Leak-Site Data](#)
- [The Leak Site and the Negotiation Portal](#)
- [What the Ransom Note Looks Like](#)
- [Infrastructure History](#)
- [How Barricade Hunts and Disrupts NightSpire](#)
- [Your Clear Battle Plan](#)
- [MITRE ATT&CK Mapping](#)
- [Indicators of Compromise](#)
- [Sources and Confidence](#)

[Back to top](#)

A field guide for business and IT leaders who would rather read this than meet NightSpire in person.

NightSpire is the kind of group that does not need to be sophisticated to hurt you. It gets in through an exposed firewall or an open remote-desktop session, quietly copies your files to cloud storage, encrypts what remains, and then squeezes you twice: once on a public leak site where your name is posted with a countdown, and again in a private chat where an operator negotiates the price. This profile is drawn from Barricade's direct review of the group's live leak site and negotiation portal, the threat-actor record we maintain in Barricade's threat intelligence platform, and reporting from Huntress, Picus Security, S-RM, eCrime.ch, and RansomLook.

Updated 21 September 2026. This revision adds eighteen months of leak-site victim data, the group's full infrastructure and contact history, the current ransom-note text and demand structure, and the status of the clearnet mirror Barricade reported for takedown in July 2026. The 21

September update names the specific tools and the FortiOS vulnerability described in vendor reporting, extends the technique mapping, and brings the victim count current. The original profile was published on 4 August 2026.

Executive Summary

NightSpire is a financially motivated ransomware and data-extortion group first seen in February and March 2025. It runs a double-extortion model: it encrypts victim data, appending the **.nspire** extension, and threatens to publish stolen files on its Tor leak site and sell them to the victim's named competitors. Its leak site has posted 359 victims between 13 March 2025 and 20 September 2026, with a sharp peak in February and March 2026 and a marked slowdown since June.

Access typically comes through the perimeter. Reporting attributes intrusions to exploitation of internet-facing firewalls and VPNs, including the FortiOS authentication bypass CVE-2024-55591, and to remote-desktop access. Once inside, the group leans on ordinary administrative and file-transfer tools to find, stage, and exfiltrate data before encryption. Victims are overwhelmingly small and mid-sized businesses. Manufacturing, healthcare, professional services, and construction lead, and the United States is the most affected country by a wide margin.

Bottom line: NightSpire is opportunistic and noisy, not stealthy, but it is effective against organizations that leave a perimeter service unpatched or a remote-desktop port exposed. A patched edge, enforced multi-factor authentication, and offline backups remove most of its leverage.

Confidence: High for the leak site, negotiation behavior, hosting, contact indicators, and ransom-note content, which Barricade reviewed directly or holds in its threat intelligence platform. High for victim counts and cadence, which come from eCrime.ch leak-site monitoring, though leak-site postings undercount real victims because paying victims are never posted. Medium for the intrusion tradecraft, tooling, file hashes, and the FortiOS access vector, which are attributed to external reporting and are cited inline. Attribution to a specific individual or origin remains unconfirmed. Indicators tied to a particular sample or date are version-specific and are marked as such.

NightSpire at a Glance

Attribute	Detail
Group	NightSpire (self-branded). Handles seen in reporting include xdragon128 and cuteliyuan
First seen	February and March 2025. First leak-site posting 13 March 2025 (eCrime.ch)
Type	Ransomware and data extortion. Encryptor reported as a Go-based portable executable (Picus)
Encrypted extension	.nspire
Extortion model	Double extortion. Encryption plus threat to publish on the Tor leak site and sell to competitors. Recent notes also threaten to open-source stolen source code
Initial access	Perimeter exploitation (firewalls and VPNs, including FortiOS CVE-2024-55591 as reported by S-RM) and remote-desktop access (Huntress, Picus Security)
Victims posted	359 leak-site postings, 13 March 2025 to 20 September 2026 (eCrime.ch via Barricade's threat intelligence platform)
Victimology	Small and mid-sized businesses. Manufacturing, healthcare, professional services, and construction lead. United States most affected
Opening demand	30,000 US dollars in Bitcoin in the current ransom-note template, with a 72-hour deadline and time-based discounts. Negotiations Barricade reviewed opened far higher
Contact	OnionMail, ProtonMail, qTox, Session, and Telegram. Contact channels have rotated at least three times

Who Is Behind It

NightSpire runs under its own brand, so it is tracked by name rather than as an unknown cluster. Beyond that, attribution is unsettled. S-RM has assessed the operation as low in experience, pointing to reused hostnames, a non-privacy Gmail address, and erratic negotiation behavior, and has raised the possibility that NightSpire is a rebrand of an earlier group tracked as Rbfs. The eCrime.ch tracker notes the absence of victims in Commonwealth of Independent States countries and the style of the portal as consistent with an Eastern European or Russian-speaking crew, while stressing that concrete attribution is still pending and that it sees no evidence of a predecessor group. There is a tension worth naming. The group makes basic operational-security mistakes, yet reporting also ties its intrusions to the exploitation of a perimeter vulnerability. Low discipline and a real ability to get through the front door can live in the same group, and both should shape how you defend against it. Whether NightSpire is

a true ransomware-as-a-service operation is contested. Some vendors describe a closed shop with no public affiliate program, others describe an active service, and the group's own portal presents itself as a service. The leak site now lists six named affiliates (Phantom, Reaper, Volt, Blaze, Shadow, Blade) according to RansomLook monitoring. Those are self-reported labels on a criminal site and cannot be verified, but the group is at minimum advertising itself as a service. Its newest ransom note describes the operation as a structured syndicate with support desks, recruiters, and analysts. Our read is that NightSpire is still maturing and that the affiliate branding is as much marketing as fact.

How They Get In

Two access paths appear across the reporting, and they are not mutually exclusive. The first is the network perimeter: exploitation of internet-facing firewalls and VPNs. S-RM reported in March 2025 that the group used CVE-2024-55591, a FortiOS flaw that lets an unauthenticated attacker gain super-admin access to an unpatched FortiGate firewall without valid credentials. The second is remote desktop, either an exposed service or one reached with valid credentials. Huntress and Picus Security both describe a March 2026 intrusion that began with an RDP session to a single endpoint. In one negotiation Barricade reviewed, the operator offered to explain the exact vulnerability used as part of the deal, which is consistent with an access-driven intrusion rather than a phishing lure.

What They Do Once Inside

NightSpire's playbook after access is deliberately ordinary, which is what makes it hard to catch on tools alone. In the March 2026 intrusion documented by Huntress, the operator installed Chrome Remote Desktop to hold access, ran Everything (a free file-search utility from voidtools) to locate data quickly, used 7-Zip to archive selected folders, and ran MEGAsync to move those archives to MEGA cloud storage. Huntress also saw VMware Workstation and WPS Office installed on the same endpoint, and AnyDesk activity alongside Chrome Remote Desktop. S-RM's earlier casework from 2025 adds WinSCP and MEGAcmd as exfiltration tools. Picus Security notes two details that are easy to hunt for: the Chrome Remote Desktop install registers a Windows service named "Chrome Remote Desktop Service", and AnyDesk adds its own service plus a shortcut in the Startup folder. None of these programs is malicious on its own. The signal is seeing them appear together on a server, outside your normal software baseline. Only after data is staged and exfiltrated does the encryptor run, appending the .nspire extension and dropping a ransom note that points the victim to the negotiation portal. One ransom-note variant, addressed to a hotel, states that the group also encrypted files held in OneDrive and deliberately left those file extensions unchanged. If that claim is accurate, it means synced cloud storage is inside the blast radius and a clean-looking OneDrive folder is not proof that data survived. Treat cloud-synced shares as encrypted until verified. Huntress has made an important point about this group: its indicators are not fixed. Between two incidents a few months apart, the encryptor and the ransom-note filename changed. Barricade's threat intelligence platform now holds four distinct ransom-note templates and four note filenames for this group. A hash or a note name is useful for a specific intrusion but should not be treated as a durable signature. Behavior and infrastructure age better than file hashes here.

Who They Hit: Eighteen Months of Leak-Site Data

Barricade's threat intelligence platform ingests every NightSpire leak-site posting tracked by eCrime.ch. As of 21 September 2026 that is 359 victims. Leak-site data has a known bias: it only shows victims who did not pay, or had not paid by the deadline, so real victim counts are higher. Within that limit, the cadence tells a clear story.

Quarter	Victims posted
2025 Q1	18
2025 Q2	56
2025 Q3	7
2025 Q4	29
2026 Q1	147
2026 Q2	72
2026 Q3	29

Activity built steadily through 2025 and then exploded in the first quarter of 2026, when the group posted 147 victims in three months, more than in all of 2025 combined. February and March 2026 each saw more than sixty postings. Since then the pace has fallen every month: 22 in June, 16 in July, 8 in August, and 6 in the first three weeks of September. That slowdown coincides with the period after Barricade's July takedown request against the group's clearnet mirror, but we do not claim the two are connected. A drop in postings can also mean affiliates left, the group is negotiating more quietly, or it is preparing a rebrand. Geography is broad but United States-heavy. Of the 239 postings with a known country, the United States accounts for 70 (29 percent). No other country reaches six percent.

Country	Victims	Share of known
United States	70	29%
India	13	5%
Turkey	12	5%
France	11	5%
Spain	9	4%
Taiwan	8	3%
Italy	8	3%
Egypt	7	3%
Thailand	7	3%
Brazil	7	3%

By sector, manufacturing leads, but healthcare is a clear second, which was not visible in the early vendor snapshots. Technology firms, which early reporting placed near the top, account for only a small share of the full record.

Sector group	Victims	Share of known
Manufacturing	46	19%
Healthcare and medical	30	13%
Professional services (legal, accounting, consulting)	23	10%
Construction and engineering	21	9%
Retail and wholesale	20	8%
Transport and logistics	14	6%
Government and education	11	5%
IT and technology	9	4%
Financial services	8	3%
Hospitality and travel	4	2%
Other or unclassified	53	22%

Size confirms the small-business focus. Of the 205 postings with a known headcount, 71 percent are organizations of 200 employees or fewer, and 37 percent have between 11 and 50 staff. Only 4 postings involve organizations above 5,000 employees. A few incidents have been confirmed publicly by the victims themselves or by local reporting, which eCrime.ch links to the corresponding leak-site postings. Nippon Ceramic (Nicera) in Japan disclosed unauthorized access to its servers in April 2025 and later reported roughly 35,650 individuals and 950 companies affected. ChangShen Hospital in Taiwan suspended new-patient registration during a system outage that eCrime.ch ties to a NightSpire posting. The Ingonyama Trust Board in South Africa was reported by TechCentral as the target of a ransomware attack. These are cited for context and carry medium confidence for attribution, since the public statements do not always name the group.

The Leak Site and the Negotiation Portal

Barricade reviewed NightSpire's live leak site and its negotiation portal directly in July 2026. The site is a straightforward web application that lists victims with a countdown timer for each, and a separate section preserves past negotiations. The negotiations reveal how the group operates when a victim engages. In one complete exchange, the group opened at 150,000 dollars and, over a series of deadlines and threats to publish and to sell data to competitors, settled toward a floor near 100,000 dollars. The operators offer to decrypt a small non-sensitive test file as proof, and they deliver stolen data samples and decryption tools through public file-sharing services. The ransom note the group is currently dropping reads very differently from those negotiations. It opens with a demand of 30,000 US dollars in Bitcoin, a 72-hour deadline, and a discount

schedule: 30 percent off for a response within 48 hours and 50 percent off within 24 hours, under the slogan that the faster you pay, the lower the ransom. It then spends most of its length on pressure: warnings not to involve cyber-insurance carriers, an invitation to secretly disclose policy limits so the group can price to them, a claim that recovery and negotiation firms are middlemen who steal from victims, a list of regulatory and legal consequences, and a made-up statistic that two in three breached companies close within six months. The note describes NightSpire as a structured syndicate with support desks, recruiters, and analysts, and offers a security audit report as a bonus for paying. Older note variants are shorter and plainer. The shift toward long, persuasive, insurer-hostile text is consistent with a group that has learned where its negotiations stall. The leak board was actively maintained at the time of our July review, with new victims and fresh countdowns appearing through the day. The negotiation section, by contrast, reads as an archive of concluded cases used as social proof to pressure current victims.

What the Ransom Note Looks Like

Barricade's threat intelligence platform holds the full text of four NightSpire ransom-note variants. The excerpts below are reproduced so responders can recognise a note on sight. Onion addresses and email addresses are defanged, and victim-specific identifiers and portal passwords were removed before the notes were catalogued. Spelling errors are the group's own. The full notes are held in Barricade's records and can be provided to incident responders on request.

Variant 1: "NightSpire Encryption Notice" (current template, dropped as [NSPIRE_MSG].txt). Opening demand and discount schedule:

NightSpire Encryption Notice

Your internal servers and backup & virtual infrastructure have been fully compromised.
All your files encrypted by NIGHTSPIRE Ransomware.
You have 72 hours to respond.
The initial payment for decryption and file deletion is 30000 USD in Bitcoin.
This amount is based on your annual revenue, and this is notably less amount than all of your past hard work and effort to develop all of your products.

However, the amount can be renegotiated depending on the circumstances.

Our Discount Service Includes:

- If you respond within 48 hours, we will provide you 30% discount as service.
- If you respond within 24 hours, we will provide you 50% discount as service.

"The faster you pay, the lower the ransom." That's our motto.

Variant 1, continued. The insurance and negotiator section that sets this group apart:

>>> IMPORTANT – INSURANCE NOTICE

Do NOT involve your cyber insurance company directly.

They will sabotage negotiations to avoid paying the full policy amount.

If your coverage is \$10M, they will offer us \$100K.
We will reject it.
They will refuse to increase.
Result: no payment, full data leak, total damage – for you.

If you anonymously inform us of your insurance limits and terms,
we will NOT exceed that amount in negotiations.

This guarantees:

- Fast resolution
- Data deletion
- Full decryption
- No public leak

Variant 2: "Dear Management" (earlier long-form note, references the original leak-site onion):

Dear Management,

If you are reading this message, it means that:

- your network infrastructure has been compromised,
- sensitive data was leaked,
- files are encrypted

The best and only thing you can do is to contact us
to settle the matter before any losses occurs.

Onion Site:

[http://nspireymvapgigtuoynlafqvlz7ey6himgn5bdvdcowfyto3yryd\[.\]onion](http://nspireymvapgigtuoynlafqvlz7ey6himgn5bdvdcowfyto3yryd[.]onion)

Proton Mail:

night.spire.team@proton[.]me

Variant 3: short note (nightspire_readme.txt era; typos in the original):

-Your sensetive data are stolen and encrypted!
If you pay within 3 days, we will decrypt it and also, we will not public your data.
After that we will public this situation and all data.

-DO NOT MODIFY FILES YOURSELF.
-DO NOT USE THIRd PARTY SOFTWARE TO RESTORE YOUR DATA.
-YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.
-YOUR DATA IS STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT OUR HELP.

CONTACT US:
Onion Mail : nightspireteam.receiver@onionmail[.]org
qTox ID: 3B61CFD6E12D789A439816E1DE08CFDA58D76EB0B26585AA34CDA617C41D5943CDD15DB0B7E6
http://a2lyiiaq4n74tlgz4fk3ft4akolapfrzk772dk24iq32cznjsmzpanqd[.]onion
http://nspiremkiq44zcxjbgvab4mdedyh2pzj5kzbmvtfcugq3mczx3dqogid[.]onion

Variant 4: hotel-specific note, including the claim that OneDrive files were encrypted without changing extensions:

Hi, Your hotel is hacked!
Your servers and files are locked and copied.
=====

REMEMBER!
We also locked files in OneDrive.
And we did not change the extensions of files in OneDrive.
=====

You cannot decrypt yourself without our key, even you're using third party software or from help of security companies.
Please do not waste your time.
Your files will be easily decrypted with pay. Never worry.

Two things stand out across the variants. The contact channels change from note to note, which is why the indicators section lists every address the group has ever used. And the tone escalates over time, from a plain three-day ultimatum in the short note to several pages of persuasion in the current template. If you receive a note that matches none of these, it does not rule NightSpire out; it more likely means the template has been revised again.

Infrastructure History

NightSpire has cycled through at least six Tor addresses since March 2025, plus a separate Tor file server for leaked data and a distinct negotiation portal referenced in the ransom note. Barricade's threat intelligence platform tracks each with its role and last-seen date. The current canonical leak site was observed online by eCrime.ch on 21 September 2026. Ransom notes and the leak site both direct victims to onion addresses. Barricade has not observed the group using a clearnet domain; its only clearnet presence to date was the raw IP mirror described below.

Tor address	Role and status
nspireyzmvapgiwgtuoznlafqvlz7ey6himtgn5bdvdcowfyo3yryd[.]onion	Tor leak site. Earliest site (ransom-note era, last seen April 2025)
a2lyiiaq4n74tlgz4fk3ft4akolapfrzk772dk24iq32cznjsmzpanqd[.]onion	Tor leak site
nspiremkiq44zcxjbgvab4mdedyh2pzj5kzbmvtfcugq3mczx3dqogid[.]onion	Tor leak site. Last seen January 2026
nspirebcv4sy3yydaerccut34hwc4fsxqqv4b4ye4xmo6qp3vxhulqd[.]onion	Tor leak site
nspirep7orjq73k2x2fwh2mxgh74vm2now6cdbnnxjk2f5wn34bmdxad[.]onion	Tor leak site. Current canonical site, seen online by eCrime.ch on 21 September 2026
p3reixfwlpjtein4yta3kiwyijxdktypcipz6jjq4wgybi73e3fsmeyd[.]onion	Tor file server used to stage leaked data
nspire7lugml7ybqyjaaxtsgrs4qn3fcon3lrbih6wamttvdm5ke4qd[.]onion	Tor negotiation portal, referenced in the ransom note

Contact channels have rotated at least three times. The group began in early 2025 with a Gmail address and ProtonMail, moved its receiving address to OnionMail in May 2025, announced a further change of address in February 2026, and added a second Telegram channel in March 2026. Each rotation has been announced on the leak site rather than hidden, which is typical of a group more interested in being reachable than in

staying quiet. Every address the group has ever published is listed in the indicators section, because dormant addresses still turn up in older ransom notes on victim systems.

How Barricade Hunts and Disrupts NightSpire

Two principles guide how Barricade approaches groups like this.

Always be hunting evil. We go looking for these operations rather than waiting for one to reach a client. Profiling NightSpire, mapping its infrastructure, and reading its negotiation history are all part of that work.

Protect our clients at all costs. Everything we learn about an active group feeds straight back into protecting the organizations we defend, from detection content to takedown action that shortens the time a group can operate.

When we find a group's infrastructure, we record a durable fingerprint of it. For NightSpire that fingerprint includes the structure of the leak site, the assets it serves, its Tor addresses, and the contact channels it reuses across incidents. That work matters because attackers move. When NightSpire changes hosting provider or rotates to a new address, the fingerprint lets us re-identify the same operation quickly instead of losing the trail, so a server move does not shake our tracking. We also act on what we find. The clearnet mirror described in the original profile was hosted by Tier.net Technologies LLC in the United States, inside the 154.29.64.0/20 range. On 28 July 2026 at 13:34 UTC, Barricade submitted takedown requests to that hosting provider and to the upstream internet service provider. **Update, 13 September 2026:** the mirror at 154.29.74[.]158 and its sibling host at 154.29.75[.]158 no longer respond on any port we checked. The group's Tor leak site remains online, so the operation itself has not been disrupted, but its only clearnet presence has gone dark. We have not received formal confirmation from the provider and do not claim the takedown request was the cause. We will keep watching the range for a re-home and will update this profile if the mirror returns. Everything in this profile also lives as a structured threat-actor record in Barricade's threat intelligence platform, where it is linked to every leak-site posting, ransom note, and contact indicator the group has used. That record is what lets us answer, within minutes, whether a client's incident matches NightSpire.

Your Clear Battle Plan

- 1. Close the perimeter first.** Patch internet-facing firewalls and VPNs on a priority schedule, with particular attention to FortiOS and FortiGate advisories. Retire any edge device that is out of support. This is the single control that most directly removes NightSpire's preferred way in.
- 2. Lock down remote access.** Do not expose remote desktop to the internet. Require multi-factor authentication on every remote entry point, including VPNs and administrative portals, and alert on new remote-management software such as AnyDesk or Chrome Remote Desktop appearing on servers.
- 3. Hunt the pre-encryption behavior.** The louder, earlier signal is data being gathered and moved. Watch for a file-search utility running on servers, bulk archiving, and outbound transfers to cloud storage or file-transfer services that your business does not normally use.
- 4. Keep backups the malware cannot reach.** Maintain at least one offline or immutable backup copy and test that you can restore from it. Do not count synced cloud folders such as OneDrive as a backup; NightSpire claims to encrypt those too. This is what turns encryption from a crisis into an inconvenience.
- 5. Detect on behavior, not just hashes.** Because this group changes its encryptor and note names, alert on the .nspire extension and on the recovery-destruction and exfiltration behavior rather than relying on a single file hash.
- 6. Decide your insurer and counsel posture before the note arrives.** The current ransom note is written to split you from your insurer and your negotiator. Agree in advance who speaks for the company, loop in breach counsel and your carrier on day one, and treat any instruction in the note about who not to call as the attacker's preference, not yours.

MITRE ATT&CK Mapping

The techniques below reflect Barricade's collection and are corroborated by external reporting where noted. Additional techniques cited by S-RM are being verified against the source appendix and are not listed here until confirmed.

Tactic	Technique	ID
Initial Access	Exploit Public-Facing Application	T1190
Initial Access	External Remote Services	T1133
Persistence	Create or Modify System Process: Windows Service	T1543.003
Discovery	File and Directory Discovery	T1083
Collection	Data Staged: Local Data Staging	T1074.001
Collection	Archive Collected Data: Archive via Utility	T1560.001

Tactic	Technique	ID
Command and Control	Remote Access Software	T1219
Exfiltration	Exfiltration to Cloud Storage	T1567.002
Impact	Data Encrypted for Impact	T1486
Impact	Financial Theft	T1657

Indicators of Compromise

Barricade collected the network, contact, and host indicators below directly from the group's infrastructure and maintains them in its threat intelligence platform. File hashes and note filenames are attributed to external reporting and are version-specific, so treat them as tied to a particular sample rather than as durable signatures. Contact addresses are listed in full, including retired ones, because old ransom notes on victim systems still carry them.

Network and infrastructure (Barricade, high confidence)

Indicator	Context
154.29.74[.]158	Cleartext leak-site and negotiation-portal mirror (Tier.net). Unresponsive as of 13 September 2026
154.29.75[.]158	Sibling host in the same range. Unresponsive at every check
nspireymvapgwtuoznlafqvlz7ey6himtgn5bdvdcowfyo3yryd[.]onion	Tor leak site. Earliest site (ransom-note era, last seen April 2025)
a2lyiaq4n74tlgz4fk3ft4akolapfrzk772dk24iq32cznjsmzpanqd[.]onion	Tor leak site
nspiremkiq44zcxjbgvab4mdedyh2pzj5kzbmvftcugq3mczx3dqogid[.]onion	Tor leak site. Last seen January 2026
nspirebcv4sy3yydtaercuut34hwc4fsxqqv4b4ye4xmo6qp3vxhulqd[.]onion	Tor leak site
nspirep7orjq73k2x2fwh2mxgh74vm2now6cdbnnxjk2f5wn34bmdxad[.]onion	Tor leak site. Current canonical site, seen online by eCrime.ch on 21 September 2026
p3reixfwlpjtein4yta3kiwyijxdktypcipz6jjq4wgybyi73e3fsmeyd[.]onion	Tor file server used to stage leaked data
nspire7lugml7ybqyjaaxtsgrs4qn3fcon3lrjbih6wamttdm5ke4qd[.]onion	Tor negotiation portal, referenced in the ransom note

Contact indicators (Barricade threat intelligence platform, high confidence)

Type	
Email (current)	nightspire.team2026@onionmail[.]org, nightspireteam.receiver@onionmail[.]org
Email (retired)	night.spire.team@gmail[.]com, night.spire.team@onionmail[.]org, night.spire.team@proton[.]me, nightspire.team2026@proton[.]me, nightspire.team2026@proton[.]me
Telegram	night_spire_team, nightspire_breach, nightspireteam2025
qTox IDs	038F61A270B8094E713E4815C4FA5086E4AD3A021575C6F90EE65A0C123D3E3BF6926C3B59EA3B61CFD6E12D789A439816E1DE0
Session	057d49830799b1fb3f73d7c611f67a82322efedd8a04ff08011a38ade05459a02

Host and malware (external reporting, version-specific)

Indicator	Context and source
.nspire	Encrypted-file extension (Barricade, Picus, Huntress)

Indicator	Context and source
[NSPIRE_MSG].txt, nightspire_readme.txt, readme.txt, readme_2.txt, _nightspire_readme.txt	Ransom-note filenames across four note variants (Barricade threat intelligence platform, Huntress)
bde50a42efc079edde1a314243ad339db2d42e343fbbcd39117803b0f5960355	Encryptor enc.exe, December 2025 (Huntress)
ad67031e2ca68764fe1a7d6632c02b02a299d59efb920710011a9a2ccf4399b7	Encryptor enc.exe, March 2026 (Huntress)
35cefe4bc4a98ad73dda4444c700aac9f749efde8f9de6a643a57a5b605bd4e7	Everything.exe, the voidtools file-search utility, as seen in 2025 intrusions (S-RM). Legitimate software: use as context alongside other indicators, not as a standalone block
prince1990905@gmail[.]com	Tied to Chrome Remote Desktop deployment (Picus, Huntress)
14.139.185[.]60	WinSCP remote server used for transfer (S-RM)

Sources and Confidence

This profile combines Barricade's direct review of NightSpire's live leak site and negotiation portal in July 2026, the structured threat-actor record in Barricade's threat intelligence platform, published reporting from Huntress, Picus Security, and S-RM, and leak-site monitoring data from eCrime.ch and RansomLook. Findings about the leak site, negotiation behavior, hosting, contact indicators, and ransom-note content are high confidence and were observed directly or hold primary-source text. Victim counts and cadence are high confidence as a record of leak-site postings but understate true victim numbers. Findings about intrusion tradecraft, tooling, file hashes, and the FortiOS access vector are medium confidence and are attributed to the cited external sources. Attribution to a specific person or country is not established. Where sources disagree, for example on ransomware-as-a-service status and on the primary access vector, the disagreement is stated rather than resolved. Only information cleared for public release is included here.

Need help responding to a threat like this? Book time with Barricade:

This brief is provided by Barricade Cyber Solutions for informational purposes. IOCs and findings are sourced as cited; confidence levels are noted inline.