Threat Feed Report – Nspire

Author: Hitesh Said **Date:** 19/07/2025

1. Executive Summary:-

Nspire is a new type of ransomware that attacks finance and logistics companies. It encrypts files, adds the .nspire extension, and leaves a ransom note asking for Bitcoin payment through a TOR site. It spreads through phishing emails and unsecured connections, and works similarly to other known ransomware.

2. Threat Metadata:-

Field	Details
Threat Name	NightSpire Virus
Type	Ransomware , Fileslocker , Stealer , Spyware
First Seen	2025-05-18
Last Seen	2025-07-07
Source	VirusTotal,Malware Bazaar , OSINT
Threat Group (If Known)	NA

3. Technical Indicators (IoCs)

IOC Type	Value
SHA256 Hash	32e10dc9fe935d7c835530be214142041b6aa25ee32c62648dea124401137ea5
MD5 Hash	2bf543faf679a374af5fc4848eea5a98
File Name	32e10dc9fe935d7c835530be214142041b6aa25ee32c62648dea124401137ea5
File Size	4.2MB
Extension	.nspire
File Path	C:\ProgramData\System\nspire_payload.exe
Ransom Note	Nspire_ReadMe.txt
C2 Server IP/Domain	213.156.145.22 / nsp1relk6xsxbxi4.onion
BTC Address	NA
Contact Information	nightspireteam.receiver@onionmail.org

4. Attribution and Group Association

Attribute	Information
Threat Actor	Nspire Ransomware Group
Known Victims	Raja Ferry Port Public Company Limited, M-POWER Information ,Al Tadawi Specialty Hospital 60+ other unnamed victims
Location	Thailand ,Taiwan ,UAE
Possible Relation	May be a rebrand of a LockBit affiliate group
Sector Targeted	Finance, Logistics, Healthcare , Transportation / Logistics ,Technology Healthcare

5. Impact Assessment

- **Risk Level**: High
- **Data Loss Potential**: Confirmed
- **Spread**: Not self-replicating
- **Data Exfiltration**: Probable before encryption
- **Leak Site**: On .onion domain

6. Mitigation & Recommendations

Recommended detection, prevention, and response steps.

- Add known file hashes to antivirus and EDR blocklists
- Audit for suspicious scheduled tasks and PowerShell usage
- Isolate infected systems immediately upon detection
- Train staff on phishing and document-based malware
- Regularly backup critical systems and store them offline

7. Attachments & Reference Links:-

Details regarding the Nspire payload, based on analysis from VirusTotal:

Attribute	Information
VirusTotal File Report	**Link to Report**
SHA256 Hash	`32e10dc9fe935d7c835530be214142041b6aa25ee32c62648dea124401137ea5`
File Name	`32e10dc9fe935d7c835530be214142041b6aa25ee32c62648dea124401137ea5.exe`
File Type	PE Executable (64-bit)
File Size	4.21 MB
Last Analysis Date	11 days ago (from report generation)
Popular Threat Labels	trojan.encoder/nightspire
Threat Categories	trojan, ransomware
Family Labels	encoder, gornsm, nightsnire
Selected Vendor Detections	• AhnLab-V3: Ransomware/Win.Nightspire.C5769860 • Alibaba: Ransom:Win32/Filecoder.ab2caf63 • Avast: Win64:Malware-gen • CrowdStrike Falcon: Win/malicious_confidence_100% (W) • DrWeb: Trojan.Encoder.42410

Additional reference links as per document outline:

- Ransom Note Sample:
- MITRE ATT&CK Mapping:

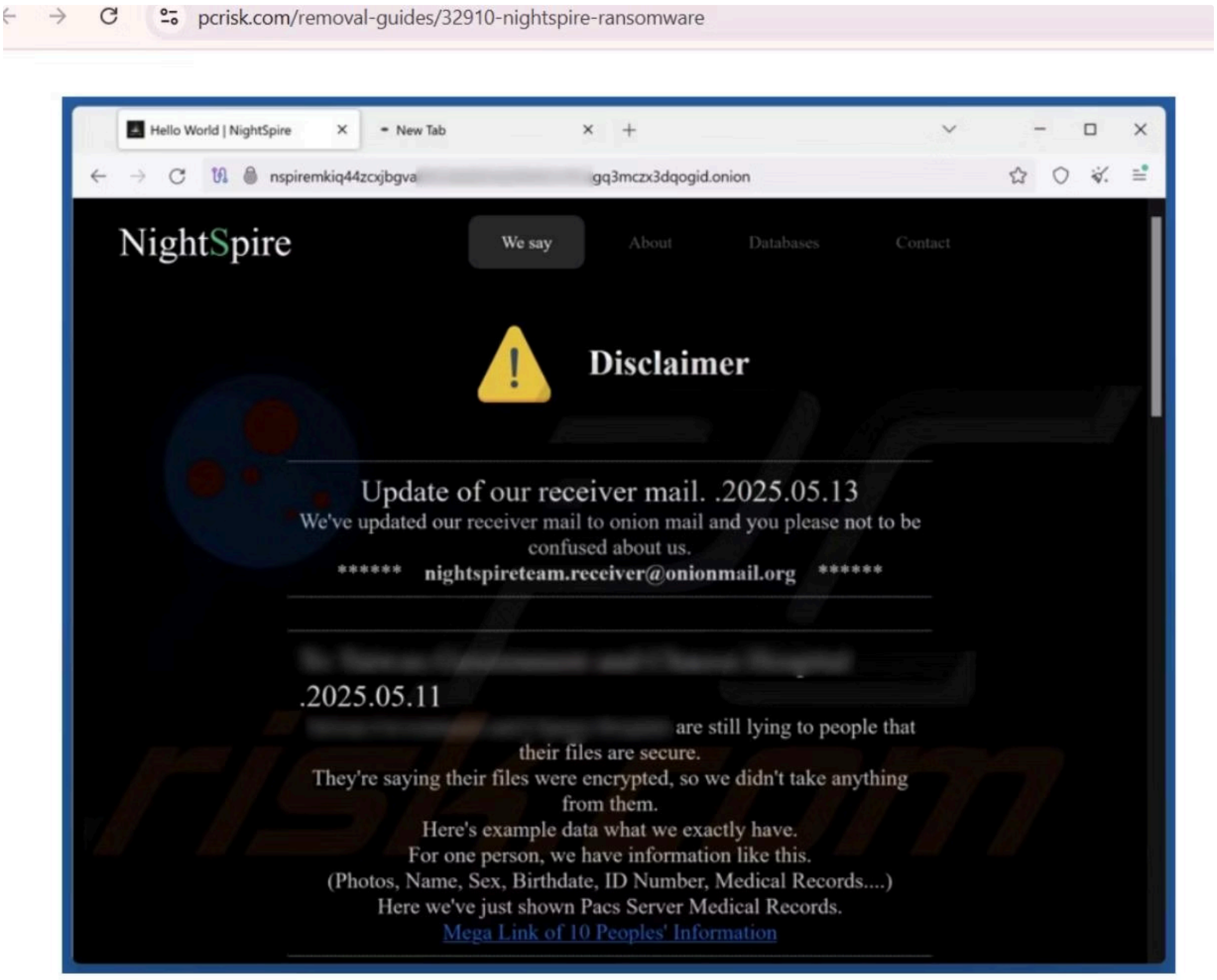
● Ransom Note Sample:

Below is a sample of the ransom note left by the Nspire ransomware:

> 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. We're waiting here with UUID
> nkobsv9jxmwvt26ad335g56e3ipt37etvfrt6chp
> 3B61CFD6E12D789A439816E1DE08CFDA58D76EB0B26585AA34CDA617C41D5943CDD15DB0B7E6
>
> We're waiting here with UUID nkobsv9jxmwvt26ad335g56e3ipt37etvfrt6chp
>
> Method * : **nightspireteam.receiver@onionmail.org**
>
> Method 1 : Our gTox ID
>
> Method 2 : Browse our Onion Site with Tor Browser
>
> **http://nspiremkiq44zcxj**
>
> **http://a2lyiiaq4n74tlgz**
>
> 100% Windows (CRLF) 3mczx3dqogid.onion cznjsmzpangd.onion $UTF-8$

● Tor Website Visual:

Screenshots of the Nspire ransomware's Tor payment website are provided below:



● MITRE ATT&CK Mapping

-T1486	Data Encrypted for Impact
-T1005	Data from Local System
-T1555	Credentials from Password Stores
-T1573	Encrypted Channel (Tor usage)
-T1190	Exploit Public-Facing Application
-T1573	Command and Control over Encrypted Channels

8. Comment

The Nspire ransomware appears to be operated by a money-driven hacker group, possibly connected to the LockBit gang. They use common hacking tools like to take control of systems and steal data before locking files. Because of this, it's a serious threat. The included indicators and sandbox analysis will help SOC teams detect and respond to the attack quickly.