Nro. Alerta:	AL-2025-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	14-Jul-2025	Ransomware NightSpire	Pág.: **1** of **5**

I. DATOS GENERALES:

Clase de alerta: Incidente
Tipo de Incidente: Ransomware
Nivel de riesgo: Alta

II. ALERTA

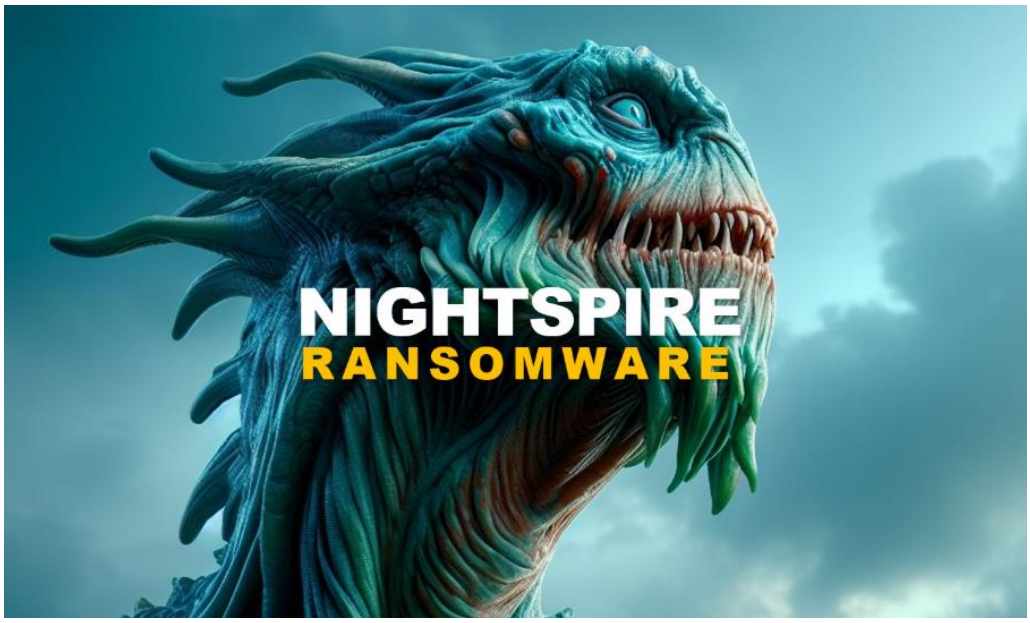

Figura 1.- Ransomware NightSpire - figura referencial

Ransomware NightSpire es una cepa maliciosa perteneciente a la familia Snatch, que ha comprometido diversas organizaciones públicas y privadas en América Latina. Emplea técnicas de cifrado avanzadas combinadas con amenazas de filtración de datos para ejercer presión sobre las víctimas y exigir altos pagos de rescate. Se recomienda implementar medidas inmediatas de contención, monitoreo y protección.

III. INTRODUCCIÓN

Su propagación se lleva a cabo mediante Phishing y tácticas engañosas, los emails son un método de envío común con archivos adjuntos (zip, exe o scripts) o enlaces infectados que instala el Ransomware NightSpire al hacer clic, aunque también puede distribuirse a través de sitios web comprometidos, anuncios maliciosos (malvertising), actualizaciones de software falsos y redes P2P.

En algunos casos puede usar troyanos o explotar vulnerabilidades del sistema para obtener acceso, como la explotación de CVE-2024-55591, un zero-day en FortiOS que permite acceso super-admin no autorizado, dando control total sobre el firewall. Una vez dentro del sistema, puede incluso propagarse a través de redes locales o unidades extraíbles para ampliar su alcance.

Ransomware NightSpire combina un cifrado agresivo con una estrategia de doble extorsión, consolidándose como una amenaza crítica en el panorama actual de la ciberseguridad. Al igual que otras cepas de su linaje, está diseñado específicamente para bloquear archivos en los sistemas comprometidos y exigir un pago a cambio de la clave de descifrado. Tras lograr la infección, añade la extensión **.nspire** a todos los archivos cifrados, por ejemplo, un archivo como “document.pdf” se convierte en “document.pdf**.nspire”**. Al finalizar el proceso, se genera una nota de rescate llamada **readme.txt**, en la que se informa del ataque y se amenaza con la pérdida definitiva de los archivos cifrados tanto locales, como en los almacenados en la nube y se advierte sobre la posible filtración de estos datos robados en caso de no realizar el pago.

La comunicación con las víctimas se lleva a cabo sobre plataformas relativamente seguras como ProtonMail, Telegram o DLS (Sitio de filtraciones en la Dark Web). Se adjunta la nota de rescate de ransomware NightSpire:

```
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 -
Method * : nightspireteam.receiver@onionmail.org
Method 1 : Our qTox ID
3B61CFD6E12D789A439816E1DE08CFDA58D76EB0B26585AA34CDA617C41D5943CDD15DB
0B7E6
Method 2 : Browse our Onion Site with Tor Browser
-
We're waiting here with UUID -
```

Figura 2.- Contenido de archivo readme.txt (nota de rescate) - Ransomware NightSpire

IV. VECTOR DE ATAQUE

Se detallan las técnicas de ataque MITRE asociadas al Ransomware NightSpire:

Táctica (Objetivo)	Técnica MITRE (ID)	Descripción aplicada a NightSpire
Acceso Inicial	T1190 – Explotación de aplicaciones públicas	NightSpire explotó CVE-2024-55591 en FortiOS para obtener acceso no autorizado a firewalls expuestos a Internet.
Ejecución	T1059.001 – PowerShell	Utilizó PowerShell para ejecutar herramientas internas o scripts durante el movimiento lateral, aprovechando funciones nativas de Windows (LOLBins).
Escalada de privilegios	T1068 – Explotación y escalada de privilegios	Mediante la misma CVE explotada, el grupo obtuvo acceso con privilegios de súper administrador en los dispositivos FortiGate.
Evasión de defensas	T1036 – Enmascaramiento	Se usaron herramientas legítimas para disfrazar la actividad maliciosa como procesos del sistema.
	T1218 – Proxy de binarios del sistema	Uso de programas como WinSCP, MEGACmd, y otros binarios legítimos para ejecutar comandos sin ser detectados por soluciones de seguridad (LOLBins).
Reconocimiento	T1046 – Descubrimiento de servicios de red	Se utilizaron escáneres de red para detectar puertos abiertos, servicios activos e infraestructura interna antes del cifrado.
	T1083 – Descubrimiento de archivos y directorios	Herramienta Everything.exe utilizada para listar y localizar archivos importantes dentro del sistema comprometido.
Movimiento Lateral	T1021 – Servicios remotos	El grupo se movió lateralmente en la red utilizando FTP y otras herramientas remotas.
	T1021.001 – Protocolo de Escritorio Remoto (RDP)	Se sospecha que utilizaron RDP junto con cuentas protegidas mediante ProtonMail y OnionMail para comunicación y comando y control.
Uso de Infraestructura	T1585.002 – Cuentas de correo electrónico	Creación de cuentas anónimas (como ProtonMail) para phishing, negociación de rescates y ocultación de identidad.
Adquisición de Herramientas	T1588.002 – Herramientas disponibles públicamente	Uso de herramientas legítimas y accesibles como WinSCP, 7-Zip, Everything.exe y MEGACmd para sus fines maliciosos.

Tabla 1. Técnicas, Tácticas y Procesos de ataque – Ransomware NightSpire

V. IMPACTO

Algunos de los programas en que el Ransomware NightSpire tiene su impacto usándolo para su persistencia y movimiento lateral.

- El uso de protocolos RDP y VPN para acceso inicial.
- Para movimiento lateral emplea el uso de LOLBins (archivos ejecutables legítimos del sistema operativo) con herramientas como PsExec, WMIC y PowerShell.

- Para exfiltracion de informacion WinSCP, MEGACmd o rclone aprovechando protocolos asimétricos no C2 cifrados para evitar activar los sistemas de detección de intrusiones.
- Everything.exe para indexar archivos valiosos del sistema

VI. INDICADORES DE COMPROMISO

Tablas referenciales a Hashes y canales de comunicación usados para la negociación de rescate como Dark Web, cuentas de emails y grupo de telegram.

Hashes
0170601e27117e9639851a969240b959
7a4aee1910b84c6715c465277229740dfc73fa39
35cefe4bc4a98ad73dda4444c700aac9f749efde8f9de6a643a57a5b605bd4e7

Tabla 2. Hashes – Ransomware NightSpire

DLS
a2lyiiaq4n74tlgz4fk3ft4akolapfrzk772dk24iq32cznjsmzpanqd[.]onion
nspireyzmvapgiwgtuoznlafqvlyz7ey6himtgn5bdvdcowfyto3yryd[.]onion

Tabla 3. Sitios de filtraciones de la Dark Web – Ransomware NightSpire

Mails
night.spire.team[@]gmail[.]com
night.spire.team[@]onionmail[.]org
night.spire.team[@]proton[.]me

Tabla 4. Direcciones de emails de negociación – Ransomware NightSpire

Telegram
hxxps://t[.]me/night_spire_team

Tabla 5. Canal de comunicación de negociación – Ransomware NightSpire

VII. RECOMENDACIONES:

- Activa MFA en accesos administrativos, RDP, VPN y paneles web para dificultar accesos no autorizados con credenciales robadas.
- Limita el uso de RDP, FTP y PsExec. Aplica listas blancas de IP, desactiva servicios no necesarios y revisa logs de conexión fuera de horario laboral.
- Monitorea la ejecución de programas como powershell.exe, cmd.exe, WinSCP.exe, MEGAcmd.exe, Everything.exe, entre otros, ya que suelen usarse para moverse lateralmente o exfiltrar datos.
- Divide la red por zonas (usuarios, servidores, backups), bloquea tráfico SMB y RDP innecesario y aplica control de acceso interno con firewalls y ACLs.

- Mantén backups offline o en nubes seguras, con control de acceso, protección contra sobrescritura y validación periódica de integridad.
- Configura detecciones para borrado de copias de seguridad (vssadmin), escaneos de red, cambios de privilegios y creación de archivos .nspire.
- Bloquea adjuntos peligrosos, enlaces maliciosos y fomenta la capacitación para reconocer intentos de phishing o correos con ingeniería social.
- Establece protocolos para aislar sistemas afectados, recopilar evidencias, contactar a expertos y comunicar el incidente. Evita pagar el rescate.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

RANSOMWARE NIGHTSPIRE: UN DEPREDADOR SILENCIOSO EN LAS SOMBRAS DIGITALES (2025) https://www.cyclonis.com/es/ransomware-nightspire-un-depredador-silencioso-en-las-sombras-digitales/

THREAT ACTOR PROFILE: NIGHTSPIRE RANSOMWARE GROUP (2025) https://cyble.com/threat-actor-profiles/nightspire-ransomware-group/?utm_source=chatgpt.com

DARK WEB PROFILE: NIGHTSPIRE RANSOMWARE(2025) https://socradar.io/dark-web-profile-nightspire-ransomware/

NIGHTSPIRE RANSOMWARE (2025) https://www.broadcom.com/support/security-center/protection-bulletin/nightspire-ransomware

RANSOMWARE – NIGHTSPIRE(2025) https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/nightspire