Grupo de ransomware Lynx Ransomware

Resumen ejecutivo

Desde su aparición a mediados de **2024, Lynx** se ha consolidado como uno de los **grupos de ransomware** más estructurados y sofisticados del panorama internacional, operando bajo un modelo de **ransomware-as-a-service (RaaS)** con **doble extorsión**. Considerado sucesor de INC Ransomware, reutiliza parte de su código y estructura, pero ha evolucionado hacia una plataforma más profesionalizada, con un sistema de afiliados y un portal en la Dark Web donde publica o subasta datos robados para presionar a las organizaciones afectadas.

Su cadena operativa combina tácticas **de acceso inicial** —mediante *phishing*, explotación de vulnerabilidades o uso de **credenciales comprometidas**— con **movimiento lateral, exfiltración de información y cifrado de sistemas**, aplicando la extensión **.lynx** a los archivos afectados.

Desde el punto de vista técnico, Lynx destaca por su **sofisticación criptográfica** (combinación de **AES-128 y Curve25519**), su **capacidad multiplataforma** (Windows, Linux y ESXi) y sus **técnicas avanzadas de evasión**, como la eliminación de copias de seguridad, la finalización de servicios críticos y la ofuscación de procesos.

Estas características, junto con su estructura RaaS organizada, le otorgan una alta capacidad de adaptación y expansión en entornos corporativos diversos.

Grupo de ransomware: Lynx

Lynx es un grupo de Ransomware-as-a-Service (RaaS) surgido en 2024 y considerado sucesor de INC Ransomware. Opera mediante afiliados a los que ofrece herramientas y soporte para ejecutar ataques de doble extorsión, combinando el cifrado de sistemas con la filtración de datos robados en una pagina web accesible desde la red TOR.

Su modelo permite personalizar campañas y adaptarlas a distintos entornos, lo que ha favorecido su rápida expansión.

Países y sectores afectados

El grupo ha mostrado una rápida expansión, con más de 300 víctimas confirmadas a nivel mundial, principalmente en **Estados Unidos, Reino Unido, Australia, Alemania y Canadá**.

En cuanto a **España**, se ha confirmado al menos un caso durante 2025: Lynx reclamó haber atacado **Ona Hotels**, una cadena hotelera española, con amenaza de filtración de datos.

En cuanto a los sectores afectados, Lynx ha apuntado principalmente a **manufactura, servicios profesionales, tecnología, energía, transporte, turismo, finanzas y construcción**, sin limitarse solo a grandes corporaciones. De hecho, un número considerable de víctimas son **pequeñas y medianas empresas (PYMEs)**, lo que demuestra que el grupo prioriza oportunidades de ataque basadas en vulnerabilidades y exposición, más que en el tamaño o relevancia pública de la organización.

Análisis técnico

Lynx opera bajo un modelo **RaaS** que facilita a sus afiliados lanzar ataques coordinados con alto grado de personalización. Emplea phishing, explotación de vulnerabilidades y credenciales comprometidas para el acceso inicial, seguido de **movimiento lateral, exfiltración y cifrado de datos**.

Opera con un **modelo de doble extorsión**, cifrando los sistemas y filtrando datos robados en su portal web si la víctima no paga.

Características técnicas principales:

- Lynx funciona como **Ransomware-as-a-Service (RaaS)**: operadores centrales junto a afiliados que personalizan y ejecutan ataques.
- Emplea **phishing, credenciales comprometidas, explotación de servicios remotos** (RDP/SSH) y **vulnerabilidades** en aplicaciones empresariales.
- Tiene variantes capaces de afectar **Windows, Linux** y entornos **ESXi**, ampliando su alcance sobre infraestructura crítica.
- **Cifra unidades locales y de red**, monta volúmenes ocultos, elimina instantáneas para bloquear la recuperación y utiliza la API del Administrador de reinicio de Windows para cifrar archivos en uso.
- Emplea criptografía, combinando **AES-128** en modo CTR junto con la implementación Donna de **Curve25519**, y añade la extensión .lynx a los archivos cifrados

Técnicas MITRE ATT&CK

Táctica	Técnica más usada
Initial Access	**T1566** — Phishing
Execution	**T1059** — Command and Scripting Interpreter **T1203** — Exploitation for Client Execution
Persistence	**T1053** — Scheduled Task/Job **T1547** — Boot or Logon Autostart Execution
Privilege Escalation	**T1134** — Access Token Manipulation **T1548** — Abuse Elevation Control Mechanism
Defense Evasion	**T1027** — Obfuscated Files or Information **T1070.001** — Clear Windows Event Logs **T1036** — Masquerading **T1140** — Deobfuscate/Decode Files or Information **T1562** — Impair Defenses
Discovery	**T1018** — Remote System Discovery **T1083** — File and Directory Discovery **T1082** — System Information Discovery **T1135** — Network Share Discovery
Lateral Movement	**T1021** — Remote services
Collection	**T1005** — Data Local System
Command and Control	**T1071** — Application Layer Protocol **T1573** — Encrypted Channel
Exfiltration	**T1041** — Exfiltration Over C2 Channel
Impact	**T1486** — Data Encrypted for Impact **T1489** — Service Stop **T1490** — Inhibit System Recovery

Medidas de mitigación

Proactivas

- ❑ Restringir ejecución de scripts y comandos no autorizados. (T1059 - Command and Scripting Interpreter)
- ❑ Auditar y restringir la creación de tareas programadas. (T1053.005 - Scheduled Task)
- ❑ Restringir privilegios, segmentar la red, controlar accesos remotos y auditar consultas y accesos a archivos. (T1018, T1082, T1083 - Discovery)
- ❑ Auditar y limitar usuarios RDP, deshabilitar el servicio si no es necesario, usar gateways y MFA. (T1021.001 - Remote Services: Remote Desktop Protocol)
- ❑ Realizar backups frecuentes, offline o segregados, y limitar accesos a datos críticos. (T1486 - Data Encrypted for Impact)

Reactivas

- ❑ Usar antivirus con AMSI, auditar registros y WMI, aplicar reglas ASR y formar a los usuarios para bloquear archivos ofuscados. (T1027 - Obfuscated Files or Information)
- ❑ Usar sandbox y microsegmentación, bloquear drivers vulnerables y aplicar protección contra exploits; mantener software actualizado y usar inteligencia de amenazas. (T1203 - Exploitation for Client Execution)

Conclusiones y recomendaciones

Lynx se ha consolidado como una **amenaza** dentro del panorama de ransomware, destacando por su **rápido crecimiento y su modelo RaaS**, que permite a afiliados ejecutar ataques altamente personalizados. Su combinación de **técnicas de evasión, movimiento lateral y doble extorsión** lo hace especialmente difícil de detectar y contener, mientras que su enfoque global evidencia su capacidad de adaptarse a distintos entornos corporativos.

Más allá de ser solo un malware, Lynx funciona como una plataforma criminal organizada, ofreciendo a terceros herramientas, soporte y estrategias que facilitan ataques sofisticados sin necesidad de desarrollar software propio. Esto refleja una tendencia creciente en el ransomware: **ataques más estructurados, automatizados y accesibles** a una mayor variedad de actores. Para protegerse de esta amenaza, las organizaciones deben priorizar el control de accesos, la monitorización constante, la implementación de los parches de actualización, backups inmutables y segmentación de red, combinados con inteligencia de amenazas para anticipar y mitigar incidentes.

