

Resumen ejecutivo

Sinobi es un ransomware, que actúa como servicio (RaaS), identificado entre mediados de 2025 y que ha emergido como un grupo de doble extorsión en el panorama del ransomware. Este malware roba información sensible de sus víctimas y la publica en portales de la dark web para presionar el pago de un rescate y evitar su filtración. Sus campañas han sido asociadas con **accesos iniciales mediante credenciales comprometidas de VPN** (se han documentado casos con credenciales de SonicWall), **explotación de vectores de acceso remoto y uso de herramientas legítimas** (*living-off-the-land*) para la exfiltración de información.

A **nivel técnico**, el malware cifra los archivos de las unidades de red locales y compartidas, dejando notas de rescate y archivos marcados con la **extensión .SINOBI**. Utiliza Curve-25519 Donna junto a AES-128-CTR para el cifrado, lo que hace imposible la recuperación sin la clave privada Curve-25519 del atacante. Esta técnica es idéntica a la de otras variantes de ransomware como Babuk.

Operativamente, Sinobi parece comportarse como una entidad que **reutiliza código y metodología** de familias previas; se observan similitudes significativas con la familia Lynx (a nivel de código, técnicas criptográficas similares y sitios de filtración parecidos). Esto facilita su rápida escalada y adaptación en campañas corporativas.

Desde una perspectiva del negocio delictivo, Sinobi actúa como un intermediario de datos y operador de doble extorsión. Para ello mantiene un portal en la red Tor donde publica listas y fragmentos de datos de víctimas, empleando plazos de presión e intimidación para forzar el pago del rescate.

Grupo de ransomware: Sinobi

Sinobi es un grupo de ransomware identificado en 2025 y considerado una posible evolución de **Lynx**, dada la gran coincidencia en código, estructuras de sitios de filtración y modus operandi. Opera bajo un modelo de **Ransomware-as-a-Service** (RaaS), ofreciendo a sus afiliados herramientas y soporte para ejecutar ataques de **doble extorsión**, que combinan el cifrado de sistemas con la filtración de datos en portales de la *dark web*. En los ataques confirmados, el ransomware asigna la extensión “.SINOBI” a los archivos cifrados y genera la nota de rescate con el nombre “README.txt”.

Países y sectores afectados

Aunque Sinobi es un grupo relativamente reciente, su actividad ha comenzado a expandirse de forma sostenida desde **mediados de 2025**, hasta alcanzar un número considerable de objetivos (87 víctimas confirmadas). Estas víctimas se concentran principalmente en **Estados Unidos**, seguido de Reino Unido, Canadá y Francia.

En **España**, se ha confirmado al menos un ataque a la empresa LASER AUTOMOTIVE VALENCIA SL, que opera en el sector industrial y manufactura. Un ataque que fue reivindicado por el grupo en su **leaksite** a fecha de 1 de octubre de 2025.






En cuanto a los sectores más atacados por Sinobi, los datos públicos muestran que se han centrado en **manufactura, construcción, energía, salud, educación y servicios financieros** como algunos de los sectores más recurrentes.

Análisis técnico

Sinobi es un ransomware tipo RaaS que inicia ataques mediante credenciales comprometidas (por ejemplo, credenciales de SonicWall SSL VPN) o vulnerabilidades, realiza movimientos laterales, escalada de privilegios y exfiltración de datos. También elimina copias de seguridad y detiene servicios críticos para dificultar la recuperación.

El proceso de cifrado de Sinobi aplica criptografía moderna, cifrando archivos a través de los algoritmos AES y Curve25519 y añadiendo la extensión .sinobi.

Características técnicas principales:

-  Funciona como **Ransomware-as-a-Service** (RaaS): operadores centrales junto a afiliados que coordinan y personalizan ataques.
-  **Vectores de acceso inicial:** credenciales comprometidas, VPNs expuestas, explotación de servicios remotos y vulnerabilidades en aplicaciones empresariales.
-  **Cifrado de archivos:** combina AES y Curve25519 y añade la extensión .sinobi a los ficheros cifrados.
-  **Técnicas de evasión:** eliminación de copias de seguridad, terminación de servicios críticos y uso de herramientas legítimas para exfiltración de datos.
-  **Exfiltración:** uso de Rclone para copiar ficheros de unidades mapeadas o compartidas hacia servidores externos controlados por el atacante.

Técnicas MITRE ATT&CK

Táctica	Técnica más usada
Initial Access	T1190 – Exploitation of Public-Facing Application T1133 – External Remote Services
Execution	T1059.001 – Command and Scripting Interpreter: PowerShell T1203 – Exploitation for Client Execution T1059.003 – Command and Scripting Interpreter: Windows Command Shell
Persistence	T1136.001 – Create Account: Local Account T1543.003 – Create or Modify System Process: Windows Service
Privilege Escalation	T1055.001 – Process Injection: Dynamic-link Library Injection T1543.003 – Create or Modify System Process: Windows Service T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1548 – Abuse Elevation Control Mechanism
Defense Evasion	T1070 – Indicator Removal on Host T1027 – Obfuscated Files or Information T1140 – Deobfuscate/Decode Files or Information T1036.005 – Masquerading: Match Legitimate Name or Location T1222 – File and Directory Permissions Modification T1562.001 – Impair Defenses: Disable or Modify Tools
Discovery	T1007 – System Service Discovery T1012 – Query Registry T1057 – Process Discovery T1016 – System Network Configuration Discovery T1083 – File and Directory Discovery
Lateral Movement	T1021 – Remote Services T1091 – Replication Through Removable Media
Command and Control	T1071.001 – Application Layer Protocol: Web Protocols T1090.002 – Proxy: External Proxy T1095 – Non-Application Layer Protocol T1572 – Protocol Tunneling
Impact	T1486 – Data Encrypted for Impact T1485 – Data Destruction T1489 – Service Stop

Medidas de mitigación

Proactivas

- ❑ Mantener software actualizado y aplicar parches de seguridad. (T1190 – Exploitation of Public-Facing Application)
- ❑ Restringir accesos remotos y aplicar autenticación multifactor. (T1133 / T1021 – External Remote Services / Remote Services)
- ❑ Restringir ejecución de scripts no firmados y registrar uso de intérpretes. (T1059.001 / T1059.003 – PowerShell / Windows Command Shell)
- ❑ Usar EDR y proteger integridad de procesos privilegiados. (T1055.001 – Process Injection)
- ❑ Auditar y restringir la creación de cuentas y servicios. (T1136.001 / T1543.003 – Create Account / Create or Modify System Process)
- ❑ Monitorizar y proteger claves de inicio automático. (T1547.001 – Registry Run Keys / Startup Folder)
- ❑ Proteger logs y monitorizar procesos ofuscados o renombrados. (T1070 / T1027 / T1140 / T1036.005 – Indicator Removal / Obfuscation / Masquerading)

Reactivas

- ❑ Bloquear o controlar uso de dispositivos USB. (T1091 – Replication Through Removable Media)
- ❑ Utilizar aplicaciones de seguridad (EMET o WDEG) que detectan el comportamiento anómalo durante la fase de explotación. (T1203 – Exploitation for Client Execution)

Conclusiones y recomendaciones

Sinobi surgió a mediados de 2025 y rápidamente se ha posicionado entre las principales **amenazas de ransomware del año**, destacando por su expansión acelerada y el alcance de sus ataques. En apenas dos meses ha comprometido a decenas de organizaciones, la mayoría en Estados Unidos, lo que demuestra una operación bien **organizada y de impacto global**.

Aunque al principio se pensó que Sinobi podía ser una reaparición de Lynx, por las similitudes en su código y plataformas de filtración, los análisis actuales indican que se trata de grupos distintos pero vinculados, posiblemente compartiendo recursos o infraestructura. Lynx, junto con INC Ransom, continúa activo, lo que sugiere la existencia de un **ecosistema criminal interconectado que colabora o intercambia herramientas**.

Para **reducir el riesgo frente a Sinobi**, se recomienda **proteger los accesos remotos con MFA, mantener copias de seguridad seguras, segmentar la red y limitar los privilegios de usuario**. Además, es clave **usar herramientas de detección avanzada y monitorizar amenazas activas** para responder con rapidez ante posibles ataques.

