

Resumen ejecutivo

Warlock es un **grupo cibercriminal** que opera bajo el modelo de **ransomware-as-a-service (RaaS)**, dificultando de este modo la atribución directa de sus ataques y amplificando el alcance y la velocidad de propagación del malware. Desde su aparición pública en junio de 2025, el grupo lanzó en pocas semanas múltiples campañas de compromiso a **escala global**, explotando **vulnerabilidades de Microsoft SharePoint ("ToolShell")**, con especial impacto en **infraestructuras críticas, sector tecnológico y sector de las telecomunicaciones**. Además, la actividad ha sido vinculada por varios analistas a Storm-2603 (grupo con base en China), consolidando de esta forma un modelo híbrido crimen-estado.

Su cadena operativa suele incluir el acceso inicial mediante vulnerabilidades conocidas (**CVE-2025-49704, CVE-2025-49706, CVE-2025-53770 y CVE-2025-53771**), despliegue de webshells, movimiento lateral con herramientas legítimas y exfiltración de información sensible. A diferencia de otros grupos RaaS, Warlock ha incorporado la **subasta privada de datos robados** como alternativa al clásico portal en la dark web donde se venden los datos, elevando el riesgo reputacional y de cumplimiento más allá del cifrado.

En consecuencia, Warlock supone un **riesgo alto** para organizaciones con SharePoint on-premise expuestos. Además, la **probabilidad de ataque** es **alta**, debido a su carácter **oportunista y modular**, ya que Warlock es capaz de capitalizar ventanas de exposición para lograr rápidamente el acceso, persistencia y control de la organización, maximizando el impacto operativo y la presión de extorsión mediante robo y monetización de datos.

Grupo de ransomware: Warlock

Warlock surgió en **junio de 2025**, a partir de una **campana de captación de afiliados** publicada en el foro ruso **RAMP**. Desde sus primeras campañas, el grupo destacó por incorporar la **subasta privada de datos exfiltrados**, maximizando el beneficio económico y reduciendo la exposición pública de sus operaciones.

Las investigaciones actuales apuntan a una **colaboración técnica** con **Storm-2603**, una entidad maliciosa de origen chino que habría facilitado la cadena de vulnerabilidades "ToolShell" para la explotación de Microsoft SharePoint. Este modelo refuerza la hipótesis de una **alianza táctica entre proveedores de exploits y operadores de ransomware**, más que una relación directa de autoría.

En el ecosistema RaaS, Warlock actúa como **operador principal y coordinador de afiliados**, ofreciendo infraestructura, cifradores y servicios de gestión de pagos, mientras que los afiliados ejecutan la intrusión inicial y la exfiltración de datos.

Países y sectores afectados

Las intrusiones confirmadas, y atribuidas a este grupo durante los últimos meses, abarcan **al menos 61 organizaciones en 21 países diferentes**. Se han detectado compromisos en **Norteamérica, Europa, Asia y África**, con prevalencia en **Estados Unidos, Reino Unido, Japón, India y Francia**. Los sectores más afectados incluyen **tecnología, telecomunicaciones, servicios financieros, manufactura, agricultura**, así como **organismos gubernamentales y servicios esenciales**.





A día de hoy solo se ha detectado una organización comprometida por Warlock en España, aunque es previsible que aumente este número en los próximos meses.

Análisis técnico

Warlock compromete organizaciones explotando la cadena de vulnerabilidades **ToolShell** en Microsoft SharePoint on-premises expuestos a Internet. Una vez accedido a los sistemas, establece **persistencia**, **desactiva los controles de seguridad** mediante listas preconfiguradas de procesos y servicios, **eleva privilegios** y realiza **movimientos laterales** a través de herramientas living-off-the-land. A continuación, inicia comunicaciones con su **servidor de mando y control** (C2) y realiza la **exfiltración** de información hacia servicios de almacenamiento en la nube.

Por último, el cifrador de Warlock **cifra ficheros a gran escala**, deja notas de rescate (How_to_decrypt_my_data.txt) y aplica la extensión .x2anylock a los ficheros.

Características técnicas principales:

-  Explotación de **Microsoft SharePoint** on-premise mediante **CVE-2025-49704** y **CVE-2025-49706** y bypasses **CVE-2025-53770** **CVE-2025-53771** (ToolShell).
-  Realiza **movimientos laterales** a través de **herramientas living-off-the-land** (PsExec, Impacket y WMI) y hace un abuso de **GPO** para el despliegue masivo del payload.
-  **Exfiltración de datos** a través de la herramienta Rclone hacia servicios de almacenamiento en nube.
-  Aplica la **extensión .x2anylock** a los ficheros cifrados y envía notas de rescate con el nombre **"How_to_decrypt_my_data.txt"** y **"How to decrypt my data.log"**.

Técnicas MITRE ATT&CK

Táctica	Técnica más usada
Initial Access	T1190 – Exploit Public-Facing Application T1203 – Exploitation for Client Execution
Execution	T1059.001 – Command and Scripting Interpreter: PowerShell
Persistence	T1505.003 – Server Software Component: Web Shell T1543.003 – Create or Modify System Process: Windows Service T1053 – Scheduled Task/Job
Defense Evasion	T1112 – Modify Registry T1036 – Masquerading T1562 – Impair Defenses T1497 – Virtualization/Sandbox Evasion
Credential Access	T1003.001 – OS Credential Dumping: LSASS Memory
Discovery	T1082 – System Information Discovery T1057 – Process Discovery T1007 – System Service Discovery T1135 – Network Share Discovery T1083 – File and Directory Discovery
Lateral Movement	T1021.006 – Remote Services: Windows Remote Management T1021.002 – Remote Services: SMB/Windows Admin Shares
Command and Control	T1105 – Ingress Tool Transfer
Exfiltration	T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage T1041 – Exfiltration Over C2 Channel
Impact	T1486 – Data Encrypted for Impact

Medidas de mitigación

Proactivas

- ❑ Escanear periódicamente los sistemas en busca de vulnerabilidades y establecer procedimientos para subsanar las vulnerabilidades detectadas. (T1190 - Exploit Public-Facing Application)
- ❑ Utilizar el control de aplicaciones cuando sea apropiado y eliminar herramientas desactualizadas o que no sean imprescindibles. (T1562.001 - Impair Defenses)
- ❑ Habilitar ASR y Credential Guard, restringir NTLM y WDigest, y usar contraseñas únicas. (T1003.001 - OS Credential Dumping: LSASS Memory)
- ❑ Restringir privilegios, segmentar la red, controlar accesos remotos y auditar consultas y accesos a archivos. (T1082 - System Information Discovery)

Reactivas

- ❑ Utilizar aplicaciones de seguridad (EMET o WDEG) que detectan el comportamiento anómalo durante la fase de explotación. (T1203 - Exploitation for Client Execution)
- ❑ Utilizar un antivirus para poner en cuarentena automáticamente archivos sospechosos y desactivar PowerShell cuando no sea necesario. (T1059.001 - Command and Scripting Interpreter: PowerShell)
- ❑ Restringir la navegación de red a través de servidores proxy que impidan el uso de servicios externos no autorizados. (T1567.002 - Exfiltration to Cloud Storage)

Conclusiones y recomendaciones

Warlock representa una amenaza sofisticada, modular y oportunista, orientada a explotar vulnerabilidades conocidas y a maximizar el beneficio mediante el robo, la extorsión y la subasta de datos.

Recomendaciones prioritarias:

- ❑ Implementar políticas ágiles de parcheo y verificación continua de exposición de servicios.
- ❑ Restringir el acceso remoto y segmentar la red para limitar movimientos laterales.
- ❑ Mantener copias de seguridad offline y probar su restauración.
- ❑ Desplegar mecanismos de detección (EDR/XDR) capaces de identificar actividad living-off-the-land y transferencias sospechosas.
- ❑ Monitorizar foros underground y fuentes OSINT para detectar subastas privadas o filtraciones vinculadas a Warlock.

La aplicación de estas medidas, combinada con un enfoque proactivo y coordinado de ciberseguridad, permitirá reducir la superficie de ataque, detectar actividad anómala en fases tempranas y mitigar el impacto operativo de posibles incidentes.

