| Nro. Alerta: | AL-2025-052 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert<br>V 1.1 |
|---|---|---|---|
| TLP: | TLP:CLEAR | | |
| Fecha: | 29-sep-2025 | Warlock Ransomware | Pág.: **1** of **6** |

## I. DATOS GENERALES:

**Clase de alerta:** Incidente
**Tipo de Incidente:** Ransomware
**Nivel de riesgo:** Alta
**Sector Afectado:** Desarrollo de software

## II. ALERTA

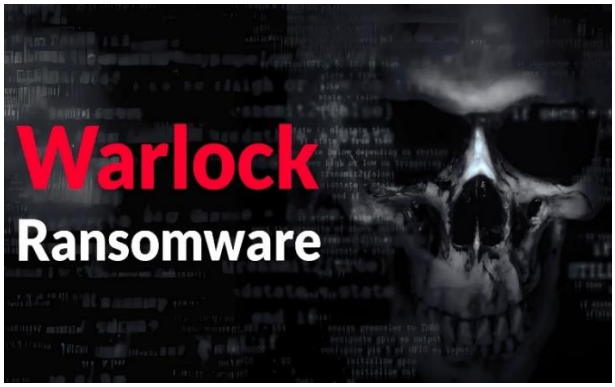


***Figura 1.-*** Warlock Ransomware - figura referencial

En el EcuCERT, se recepta la notificación de una campaña maliciosa atribuida a un actor de amenaza con sede en china llamado Storm-2603, la que explota un grupo de vulnerabilidades críticas conocidas como ToolShell en Microsoft SharePoint para desplegar el Warlock Ransomware. Esta amenaza presenta un riesgo elevado debido a su uso de técnicas avanzadas de evasión y cifrado, incluyendo la desactivación de defensas como Microsoft Defender antes del despliegue del malware.

## III. INTRODUCCIÓN

Warlock Ransomware es una operación de ransomware como servicio (RaaS) observada por primera vez en junio de 2025, estrechamente relacionada con el actor de amenazas Storm-2603. Este grupo ha sido vinculado a ataques dirigidos contra organizaciones de alto perfil mediante el uso de vulnerabilidades de día cero en Microsoft SharePoint. La primera aparición pública de Warlock Ransomware se dio en foros de ciberdelincuencia como RAMP, promocionado con mensajes llamativos como: “Si quieres un Lamborghini, llámame”.

Microsoft ha confirmado que Storm-2603 ha utilizado CVE-2025-49706 como punto inicial de compromiso, seguido de la implementación de web shells y herramientas como Mimikatz e Impacket para el robo de credenciales y movimiento lateral.

Posteriormente, los entornos comprometidos son cifrados con Warlock Ransomware, empleando un modelo de doble extorsión.

Si bien Storm-2603 tiene origen chino, no se le ha atribuido directamente vínculos con otros actores estatales como Linen Typhoon o Violet Typhoon, también involucrados en campañas similares. Hasta la fecha, se estima que al menos 11 organizaciones han sido afectadas, convirtiendo esta operación en una de las más relevantes del segundo semestre de 2025.

## IV. VECTOR DE ATAQUE

### Acceso inicial

Warlock Ransomware aprovecha los servidores SharePoint locales sin parches mediante solicitudes HTTP POST para cargar shells web, eludiendo la autenticación y estableciendo un punto de apoyo dentro de las redes objetivo.

### Escalada de privilegios y compromiso del dominio

Una vez dentro, los atacantes manipulan los objetos de política de grupo (GPO), activan cuentas de invitado y escalan privilegios para obtener el control de todo el dominio.

### Ejecución y evasion

Mediante scripts por lotes personalizados, Warlock despliega cargas útiles de ransomware mientras desactiva las defensas. Una herramienta conocida, identificada como Trojan.Win64.KILLLAV.I, se dirige específicamente a los productos de seguridad de los puntos finales y los desactiva.

### Robo de credenciales y movimiento lateral

El grupo emplea Mimikatz y la extracción del subárbol del registro para recopilar credenciales, al tiempo que mapea las relaciones de confianza del dominio para el movimiento lateral a través de SMB y RDP.

### Cifrado y exfiltración

Los archivos se cifran con la extensión .x2anylock y se dejan notas de rescate en todos los sistemas. Los datos se exfiltran utilizando RClone, a menudo disfrazados bajo nombres de archivo legítimos como «TrendSecurity.exe».

Se muestra proceso TTPs:

| Táctica | Técnica/Subtécnica | Evidencia en el caso |
|---|---|---|
| Acceso inicial | Exploitation for Client Execution (T1203) | Explotación CVE-2025-49704 para RCE |
| | Exploitation of Public-Facing Application (T1190) | Explotación de CVE-2025-49706, 53770, 53771 en SharePoint |
| Persistencia | Web Shell (T1505.003) | Instalación de spinstall0.aspx, spinstall.aspx, etc. |
| | Modify Existing Service (T1543.003) | Alojado en proceso w3wp.exe de IIS |
| | Scheduled Task/Job (T1053) | Uso de tareas programadas para persistencia |
| Evasión defensiva | Modify Registry (T1112) | Modificación del registro para deshabilitar Microsoft Defender |
| | Masquerading (T1036) | Shells y DLL maliciosos ocultos como archivos legítimos |
| | Impair Defenses (T1562) | Deshabilitación de protecciones de endpoint |
| Credenciales | Credential Dumping: LSASS Memory (T1003.001) | Robo de credenciales con Mimikatz desde LSASS |
| Movimiento lateral | Remote Services: SMB/Windows Admin Shares (T1021.002) | Uso de PsExec para movimiento lateral |
| | Remote Services: Remote Management (T1021.006) | Uso de Impacket para movimiento lateral |
| Ejecución | Command and Scripting Interpreter: PowerShell (T1059.001) | Descarga/ejecución de payloads en PowerShell |
| Impacto | Data Encrypted for Impact (T1486) | Cifrado de datos (ransomware) |
| | Exfiltration Over C2 Channel (T1041) | Publicación de datos robados (doble extorsión) |
| Exfiltración | Exfiltration Over Web Services (T1567.002) | Exfiltración vía túneles web / C2 |

***Tabla 1.-*** TTPs - Warlock Ransomware

## V. IMPACTO

Aplicativos empleados para persistencia y movimiento lateral:

- Mimikatz
- SMB
- RDP
- RClone

## VI. INDICADORES DE COMPROMISO

| Nombre de archivo | Tipo | Ruta (si aplica) |
|---|---|---|
| spinstall0.aspx | Shell web | |
| spinstall.aspx | Shell web | |
| spinstall1.aspx | Shell web | |

| Nombre de archivo | Tipo | Ruta (si aplica) |
|---|---|---|
| spinstall2.aspx | Shell web | |
| IIS_Server_dll.dll | Puerta trasera IIS Storm-2603 | |
| SharpHostInfo.x64.exe | Herramienta de recopilación | |
| xd.exe | Proxy inverso | |
| debug_dev.js | Exfiltración de configuración web | \1[5-6]\TEMPLATE\LAYOUTS\debug_dev.js |

***Tabla 2.-*** Shells web y puertas traseras – Warlock Ransomware

| Hash SHA-256 | Asociado a |
|---|---|
| 92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514 | spinstall0.aspx (shell web) |
| 24480dbe306597da1ba393b6e30d542673066f98826cc07ac4b9033137f37dbf | Shell web (C2) |
| b5a78616f709859a0d9f830d28ff2f9dbbb2387df1753739407917e96dadf6b0 | Shell web (C2) |

***Tabla 3.-*** Hashes de archivos (SHA-256) – Warlock Ransomware

| Dominio/URL | Uso |
|---|---|
| c34718cbb4c6.ngrok-free[.]app/file.ps1 | Entrega de PowerShell vía Ngrok |
| msupdate[.]updatemicfosoft[.]com | Dominio C2 Storm-2603 |
| update[.]updatemicfosoft[.]com | Dominio C2 Storm-2603 |

***Tabla 4.-*** Dominios y URL – Warlock Ransomware

| Dirección IP | Uso |
|---|---|
| 131.226.2[.]6 | C2 post-explotación |
| 134.199.202[.]205 | Fuente de explotación |
| 104.238.159[.]149 | Fuente de explotación |
| 188.130.206[.]168 | Fuente de explotación |
| 65.38.121[.]198 | C2 post-explotación Storm-2603 |
| 192.168.10.5 | IP privada (inofensiva) |

***Tabla 5.-*** Direcciones IP – Warlock Ransomware

## VII. RECOMENDACIONES:

- Actualizar inmediatamente los servidores SharePoint con los parches proporcionados por Microsoft para las vulnerabilidades mencionadas.
- Activar la Interfaz de Escaneo Antimalware (AMSI) y utilizar soluciones antivirus actualizados.
- Después de aplicar los parches, rotar las claves criptográficas para prevenir accesos no autorizados.
- Reiniciar los servicios de Internet Information Services para aplicar completamente las actualizaciones.

- Utilizar herramientas de detección y respuesta en endpoints para monitorear y mitigar actividades sospechosas.
- Revisar regularmente los sistemas en busca de los indicadores mencionados y cualquier actividad inusual.

## 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:

**ECUCERT (2025).** Alerta 2025-037: Vulnerabilidades críticas en Microsoft SharePoint Server (CVE-2025-53770 y CVE-2025-53771). https://www.ecucert.gob.ec/wp-content/uploads/2025/07/Al-2025-037-Vulnerabilidades-criticas-en-Microsoft-SharePoint-Server-CVE-2025-53770-y-CVE-2025-53771.pdf

**ECUCERT (2025)**. Alerta 2025-041: Actualización sobre la vulnerabilidad ToolShell en SharePoint. https://www.ecucert.gob.ec/wp-content/uploads/2025/08/Al-2025-041-Actualizacion-vulnerabilidad-ToolShell-SharePoint.pdf

**TREND MICRO (2025).** Warlock Ransomware: Análisis de la amenaza emergente. https://www.trendmicro.com/es_es/research/25/h/warlock-ransomware.html

**ATTACKIQ (2025).** Emulación del ransomware Warlock. https://www.attackiq.com/2025/08/27/emulating-warlock-ransomware/

**FORTRA (2025).** Warlock Ransomware: Lo que necesitas saber. https://www.fortra.com/blog/warlock-ransomware-what-you-need-know

**THE RECORD (2025).** Microsoft informa sobre el despliegue del ransomware Warlock en ataques a SharePoint. https://therecord.media/microsoft-says-warlock-ransomware-deployed-in-sharepoint-attacks

**UNIT42 (2025).** Explotación activa de vulnerabilidades en Microsoft SharePoint (CVE-2025-49704, CVE-2025-49706, CVE-2025-53770). https://unit42.paloaltonetworks.com/microsoft-sharepoint-cve-2025-49704-cve-2025-49706-cve-2025-53770/

**HALCYON (2025).** Warlock Ransomware: Actor de amenaza emergente. https://www.halcyon.ai/blog/emerging-threat-actor-warlock-ransomware

**PROTOSLABS (2025).** Warlock Ransomware-as-a-Service (RaaS): Resumen actualizado y victimología. https://www.protoslabs.io/resources/warlock-ransomware-as-a-service-raas-group-updated-summary-victimology