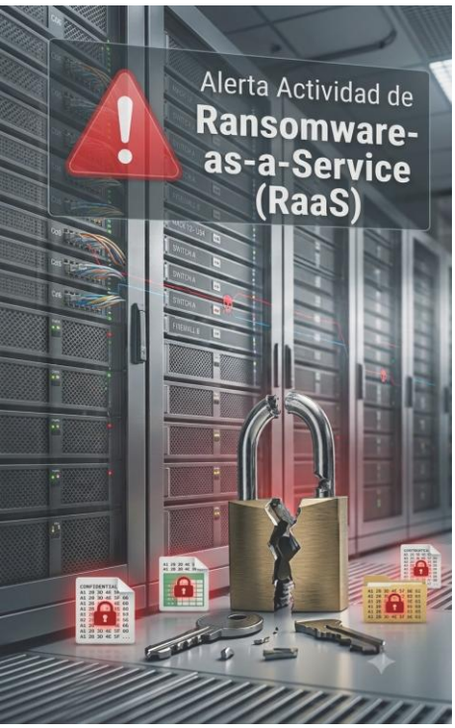
Alerta

Actividad de Ransomware-as-a-Service (RaaS)

COLCERT AL – 20260809 - 111

TLP:CLEAR

Resumen Ejecutivo



Se identificó actividad atribuible a una operación de Ransomware-as-a-Service (RaaS) orientada a la interrupción operativa. La amenaza ejecutó fases de post-explotación que incluyeron movimiento lateral en la red, despliegue de un kit de minería de criptomonedas (cryptojacking), recolección de información sensible mediante el historial de comandos de PowerShell en múltiples sistemas y, como fase final, el cifrado masivo de archivos.

Durante el análisis se observaron indicadores de compromiso (IoC) y patrones de comportamiento consistentes con la familia de Ransomware LockBit. No obstante, el artefacto utilizado en la fase de cifrado presenta características híbridas que evidencian el empleo de técnicas asociadas a múltiples familias de ransomware, entre ellas LockBit, BlackMatter y EnigmaLocker, lo que evidencia el uso de un builder modificado o la integración de componentes de diversas familias maliciosas.

El análisis técnico del binario de cifrado permitió identificar capacidades avanzadas de evasión y ejecución, entre las que destacan el empaquetado (packing) y la ofuscación del código para dificultar su análisis, la inyección de código en un proceso legítimo del sistema operativo (WerFault.exe) con el fin de ocultar la ejecución maliciosa, mecanismos de anti-análisis basados en la validación de la fecha del sistema y la configuración regional (idioma) del equipo comprometido, así como rutinas destinadas al cifrado selectivo o masivo de archivos.

El principal riesgo radica en la reutilización de una misma cadena de herramientas (toolset) por parte del actor de amenazas, lo que incrementa la probabilidad de compromisos adicionales en otras organizaciones. Entre las herramientas y técnicas observadas se encuentran el uso de PsExec empleando credenciales con privilegios de administrador para facilitar el movimiento lateral y la ejecución remota; cargadores (loaders) camuflados como procesos legítimos del sistema operativo; mineros de criptomonedas camuflados como componentes de Windows Media Player para evadir mecanismos de detección; y el abuso del binario legítimo WmiPrvSE.exe mediante la técnica de DLL Side-Loading, utilizada para cargar bibliotecas dinámicas maliciosas aprovechando la confianza del sistema operativo.

Contexto de la Amenaza

Como resultado de la investigación y de la correlación de los artefactos recopilados, el análisis se enfoco en dos líneas técnicas principales que permitieron identificar la cadena de ataque y caracterizar la metodología empleada por el actor de amenazas. La primera línea de análisis se centró en un conjunto de cuatro ejecutables estrechamente relacionados, los cuales conforman un kit de minería de criptomonedas diseñado para su despliegue en etapas posteriores al compromiso inicial. El análisis de estos componentes evidenció la implementación de múltiples mecanismos de persistencia, evasión de defensas y ejecución encubierta, orientados a mantener la permanencia del atacante dentro de la infraestructura comprometida y maximizar el aprovechamiento ilícito de los recursos computacionales de los sistemas afectados.

La segunda línea de análisis se enfocó en el estudio del binario legítimo de Microsoft WmiPrvSE.exe, identificado de forma recurrente dentro de más de una decena de archivos comprimidos junto con bibliotecas dinámicas (DLL) y otros artefactos maliciosos. La presencia sistemática de este ejecutable, acompañada de DLL maliciosas, constituye un patrón consistente con la técnica DLL Side-Loading (MITRE ATT&CK T1574.002), mediante la cual un ejecutable legítimo y firmado digitalmente es utilizado para cargar una biblioteca maliciosa desde un directorio controlado por el atacante.

Esta técnica permite ejecutar código arbitrario bajo la apariencia de un proceso confiable, incrementar el nivel de sigilo y reducir la probabilidad de detección por parte de las soluciones de seguridad. La correlación de ambas líneas de análisis, complementada con los indicadores de compromiso (IoC), y la secuencia temporal de los eventos, permitió confirmar la existencia de una campaña coordinada de distribución masiva de componentes maliciosos. La reconstrucción de la cadena de ataque evidencia una secuencia operacional claramente definida, que inicia con actividades de movimiento lateral y propagación interna, continúa con el despliegue de herramientas de post-explotación (incluyendo el kit de minería de criptomonedas y mecanismos de persistencia basados en el abuso de binarios legítimos) y culmina con la ejecución del ransomware, el cifrado de los sistemas comprometidos. En conjunto, los hallazgos demuestran que el actor de amenazas emplea una estrategia modular basada en la reutilización de herramientas legítimas del sistema operativo (Living-off-the-Land), combinada con técnicas avanzadas de evasión y persistencia para dificultar la detección, ampliar el alcance de la propagación dentro de la infraestructura y asegurar la ejecución de las fases finales del ataque antes de activar el proceso de cifrado.

Modelo de Negocio: Ransomware-as-a-Service

La familia con la que se asocia por similitud el componente de cifrado (LockBit) opera bajo un modelo de franquicia criminal (Ransomware-as-a-Service) desde 2019. Un equipo central desarrolla y mantiene el malware, provee infraestructura de comando y control sobre la red Tor, un portal de filtración de datos y un sistema de negociación con pasarelas de pago en criptomonedas; los afiliados (operadores independientes, técnicamente diversos) ejecutan la intrusión y el despliegue a cambio de entre el 70 % y el 80 % del rescate cobrado, mientras el equipo central retiene entre el 20 % y el 30 % restante. Este modelo explica por qué las TTP observadas en distintos incidentes atribuidos a la misma marca RaaS pueden variar sustancialmente: no existe un único operador, sino decenas de afiliados con sus propios flujos de trabajo.

La versión más reciente de esta familia (identificada por la plataforma de inteligencia como “5.0”, activa desde finales de 2025) elimina las restricciones previas que excluían del programa de afiliados a hospitales, infraestructura crítica y sector petrolero, e incorpora soporte multiplataforma (Windows, Linux y el hipervisor VMware ESXi), inyección reflectiva en memoria para evitar dejar el motor de cifrado en disco, y cifrado intermitente no lineal para dificultar la recuperación forense parcial. El programa de recompensas por errores que el grupo mantuvo hasta 2024 fue descontinuado después de que canales de comunicación fueran infiltrados por investigadores y fuerzas del orden.

NIVEL DE RIESGO

ALTO

Actores de amenaza asociados

Los siguientes actores han sido públicamente vinculados por la industria de inteligencia de amenazas al programa de afiliados de Ransomware as a Service.

Actor	Descripción
UNC2165 (Evil Corp / INDRIK SPIDER)	Organización cibercriminal con sede en Rusia, sancionada por la OFAC desde 2019. Un miembro sancionado de alto rango operó como afiliado de LockBit para evadir las restricciones de pago derivadas de las sanciones, generando más de 60 variantes personalizadas del ransomware.
UNC3944 (Scattered Spider / Octo Tempest)	Grupo de habla inglesa especializado en ingeniería social, SIM swapping y bypass de MFA. Actúa como afiliado multi-ransomware, desplegando tanto BlackCat/ALPHV como LockBit según el acceso obtenido.
UNC5174 (Xiaoqiying)	Actor de nivel estatal/mercenario especializado en explotación rápida de vulnerabilidades día cero o día uno en dispositivos perimetrales (VPN, firewalls). Actúa como corredor de accesos hacia afiliados de esta familia de ransomware.
UNC2758	Clúster enfocado en sector financiero y manufacturero en Europa y Norteamérica; se especializa en movimiento lateral silencioso en Active Directory mediante herramientas comerciales de administración de TI.
UNC3313	Actor enfocado en gobiernos locales y entidades educativas mediante credenciales RDP comprometidas.
Otros actores reportados de esta familia	FIN12, UNC2465, UNC2727, UNC3753, UNC4120, UNC4273

Motivación

Lo observado en la investigación es consistente con una motivación exclusivamente financiera, sin indicios de espionaje, sabotaje dirigido o agenda política. El actor combinó dos vías de monetización dentro de la misma intrusión: minería no autorizada de criptomonedas (monetización directa e inmediata, proporcional al tiempo de cómputo robado) y cifrado de archivos con nota de rescate (monetización diferida y de mayor cuantía potencial, sujeta a negociación con la víctima).

El ciclo de ataque reconstruido sigue el patrón típico de “Big Game Hunting” que caracteriza a las operaciones RaaS más activas: obtención de acceso privilegiado, reconocimiento interno y recolección de credenciales (incluyendo un intento deliberado de llegar a la infraestructura de copias de seguridad, paso habitual para maximizar la presión de pago al eliminar la posibilidad de restauración), distribución masiva de herramientas mediante mecanismos administrativos legítimos, y finalmente impacto simultáneo en múltiples sistemas para minimizar la ventana de reacción del equipo defensor.

Sectores objetivo

El patrón de selección de víctimas es consistente con el perfil de objetivos documentado públicamente para el ecosistema RaaS al que se asocia por similitud el componente de cifrado, que históricamente prioriza organizaciones con alta necesidad de continuidad operativa y baja tolerancia al tiempo de inactividad:

- Infraestructura crítica y manufactura de alto volumen.
- Hospitales, redes de salud y educación superior.
- Agencias gubernamentales territoriales y nacionales.
- Instituciones financieras y aseguradoras.

Las versiones más recientes de esta familia de ransomware ha eliminado las restricciones previamente impuestas por el operador del programa Ransomware-as-a-Service (RaaS), las cuales excluían como objetivos a organizaciones pertenecientes al sector salud y a infraestructuras críticas. Como consecuencia, la superficie potencial de ataque se ha ampliado significativamente, permitiendo que cualquier organización pública o privada, especialmente aquellas de tamaño mediano o grande, pueda convertirse en un objetivo de estas operaciones. En el contexto colombiano, este cambio incrementa el nivel de exposición de entidades de múltiples sectores económicos y gubernamentales, independientemente de la naturaleza de los servicios que prestan.

Técnicas y Tácticas — MITRE ATT&CK

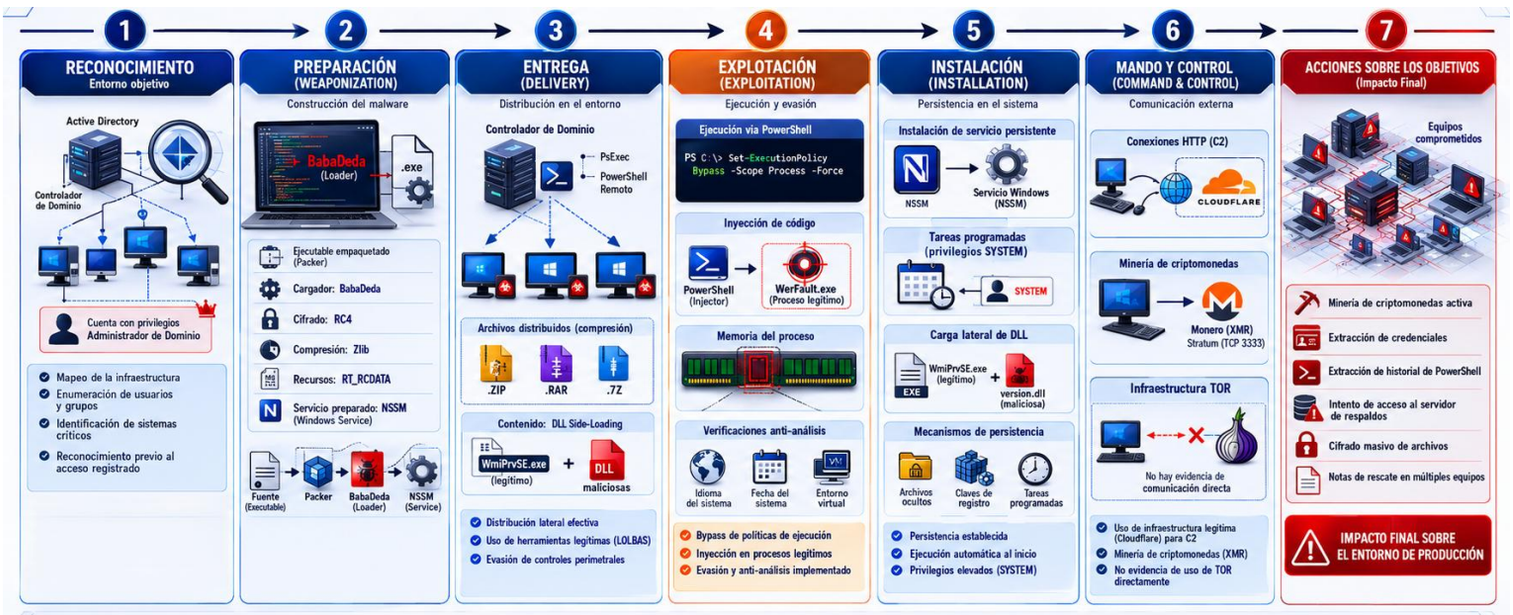
A continuación se detalla el ciclo de ataque documentado, organizado por fases.

Táctica	Técnica	ID	Observación
Reconocimiento (TA0043)	Búsqueda de información de víctimas / compra de acceso inicial	T1591 / T1589 (inferido)	Credenciales comprometidas o acceso comprado a un corredor de accesos (Initial Access Broker).
Acceso inicial (TA0001)	Cuentas válidas	T1078	El movimiento lateral se origina desde una cuenta de integridad “alta” ya en posesión del actor.
Ejecución (TA0002)	Intérprete de comandos y scripts (PowerShell)	T1059.001	Ejecución remota de powershell.exe -ExecutionPolicy Bypass -File Script.ps1 en hosts vía PsExec.
Ejecución (TA0002)	Ejecución de servicios remotos	T1569.002	PsExec.exe utilizado para lanzar procesos remotos desde los controladores de dominio.
Ejecución (TA0002)	Ejecución por el usuario / archivo malicioso	T1204 / T1105	Eventos de transferencia y ejecución de archivo detectados como parte de la distribución masiva del kit de minería.
Persistencia (TA0003)	Crear o modificar proceso del sistema (servicio)	T1543.003	Instalación del minero como servicio de Windows mediante el gestor NSSM (servicio “WMPUpdate”).
Persistencia (TA0003)	Tarea programada	T1053.005	Creación de tareas programadas con privilegios de SYSTEM para relanzar los componentes del minero tras reinicio.

Táctica	Técnica	ID	Evidencia en este incidente
Persistencia (TA0003)	Ejecución en el arranque / claves de registro (autorun)	T1547.001 / T1546.012	Eventos de creación o modificación de claves de registro y servicios en los hosts comprometidos.
Persistencia (TA0003)	Carga lateral de DLL (DLL sideloading)	T1574.002	Depósito de version.dll en ruta de usuario no estándar; adicionalmente, un binario legítimo de Microsoft (WmiPrvSE.exe) empaquetado junto a cargas maliciosas en más de 15 archivos comprimidos distintos.
Escalada de privilegios (TA0004)	Inyección de proceso	T1055	El cargador principal inyecta un payload de 4.449 bytes en el proceso legítimo WerFault.exe (manejador de errores de Windows), confirmado por firmas de comportamiento.
Evasión de defensas (TA0005)	Empaquetado de software / archivos ofuscados	T1027 / T1027.002	Punto de entrada anómalo (stub de packer), nombre de sección no estándar y alta entropía en el binario principal; cadena de desencriptación RC4 + descompresión Zlib en el cargador BabaDeda.
Evasión de defensas (TA0005)	Evasión de virtualización / sandbox	T1497	Verificación de fecha del sistema con salida anticipada tras superar un umbral; comprobación adicional de depuradores y entornos virtualizados en el cargador BabaDeda.
Evasión de defensas (TA0005)	Descubrimiento del sistema / salvaguarda de idioma (geofencing)	T1480 / T1082	Lectura de claves de registro NLS CustomLocale/ExtendedLocale para verificar el idioma configurado, patrón de exclusión de sistemas en ruso o de países de la CEI.
Evasión de defensas (TA0005)	Abuso de proceso firmado y de confianza	T1036 / T1055	Uso de WerFault.exe (binario legítimo firmado por Microsoft) como contenedor de la inyección, y de WmiPrvSE.exe (también firmado por Microsoft) como señuelo de reputación dentro de archivos comprimidos maliciosos.
Evasión de defensas (TA0005)	Deshabilitar o modificar herramientas / detener servicios	T1562.001 / T1489	Eventos de bloqueo de ejecución (Execution Blocked), detección de antivirus/EDR o servicios de respaldo; deshabilitación del servicio de Windows Update (wuauserv) por parte del kit de minería.
Evasión de defensas (TA0005)	Alteración de firewall / reglas de red	T1562.004	Eventos de intento de modificación de reglas de firewall.
Evasión de defensas (TA0005)	Ocultar artefactos (atributo oculto)	T1564.001	Los archivos del kit de minería (config.json, binarios y el controlador vulnerable) se marcan con el atributo “oculto” (attrib +h).
Evasión de defensas (TA0005)	Bloqueo del Administrador de Tareas (IFEO)	T1112 / T1562	Entrada en Opciones de Ejecución de Archivos de Imagen (IFEO) que asocia taskmgr.exe con un depurador ficticio para impedir su apertura.
Acceso a credenciales (TA0006)	Acceso a LSASS	T1003.001	Eventos de intento de acceso a memoria de LSASS, bloqueados por protección de integridad de procesos del sistema.

Táctica	Técnica	ID	Evidencia en este incidente
Acceso a credenciales (TA0006)	Credenciales en archivos / historial de comandos	T1552.003	Lectura del archivo ConsoleHost_history.txt de cuentas de servicio y administrador en hosts.
Descubrimiento (TA0007)	Descubrimiento de procesos, servicios, cuentas y ventanas	T1057 / T1007 / T1087 / T1010	Reconocimiento exhaustivo del host mediante el componente de persistencia del minero: enumeración de procesos, servicios instalados, cuentas y sesiones activas, y ventanas de aplicaciones abiertas.
Descubrimiento (TA0007)	Descubrimiento de información y ubicación del sistema	T1082 / T1083	Consulta de configuración local, versión de sistema operativo, parches instalados y estructura de archivos/directorios.
Movimiento lateral (TA0008)	Servicios remotos / recursos administrativos compartidos	T1021.002	PsExec dirigido a hosts.
Recolección (TA0009)	Preparación / puesta en escena de datos	T1074 / T1685	Eventos de actividad de preparación de datos.
Comando y control (TA0011)	Protocolo de aplicación estándar (HTTP)	T1071.001	Tráfico HTTP saliente confirmado desde el cargador principal; conexiones del minero hacia el dominio del pool de minería sobre el puerto 3333 (protocolo Stratum).
Impacto (TA0040)	Datos cifrados por impacto (ransomware)	T1486	Detecciones de comportamiento de cifrado (firma “LockBit Ransomware”); creación de nota de rescate.
Impacto (TA0040)	Secuestro de recursos (cripto-minería)	T1496	Despliegue de un minero XMRig disfrazado de componente de Windows Media Player en hosts, con importación de funciones de red para conectarse a pools públicos de Monero.
Impacto (TA0040)	Inhibición de la recuperación del sistema	T1490	Técnica descrita en el perfil operacional de referencia de esta familia de ransomware (eliminación de copias de seguridad)

Cyber kill chain



Indicadores de Compromiso (IoCs)

Cargador / componente de cifrado (enigma_pass.exe)

Archivo	Rol	MD5 / SHA-1 / SHA-256
enigma_pass.exe	Cargador / inyector — componente de cifrado	MD5: 103264597248e156a7dd13a873e7a269 SHA-1: 7a824ec8e6abda20e2cec3754633a0b8217cf74d SHA-256: ed0e1b21064c01ffdf5e0843c9dd78d65266d4272e440158a72f9bcac011301f
(payload inyectado en WerFault.exe)	Shellcode inyectado, 4.449 bytes	MD5: b4dce545325898fe296eb26c59b556dd SHA-1: 67abf4d30fcaec0a754412f233c7038644a4a19d SHA-256: 7f938fe6779ded1fbb9426fe09d90f22f408a9f24c1f0fb63279e56ae1af3df5

Otros artefactos relacionados (SHA-256)

SHA-256	Relación con el artefacto principal
2b0ac44dcc47da7de131e8d0a9e6feea39c8b10193d89aa1202b70480c614317	Archivo agrupado (Bundled) relacionado con el artefacto principal.
39548bd8ea6b244e1a7664a10aabd6714a0630e458a62ffcb06906b3a88f4405	Archivo agrupado (Bundled) relacionado con el artefacto principal.
5c001e235fdd0125aa7d2473bf3725a275951322a112e16c218e22db5a1879bf	Archivo agrupado (Bundled) relacionado con el artefacto principal.
5f8f6e8fbf6a80d1bc3f9acd19372dca3bcd9f8c8c60f359c2107a45c7e63402	Archivo agrupado (Bundled) relacionado con el artefacto principal.
ed21ffc5b65b71c1bbdf922794acfdd440fdbad8310f9a09ac3f402d21a06bb9	Archivo agrupado (Bundled) relacionado con el artefacto principal.

Otros indicadores del cargador

Indicador	Valor / Evidencia	Observación
Proceso destino de la inyección	C:\Windows\SysWOW64\WerFault.exe	Proceso legítimo utilizado para Process Injection.
Línea de comandos	WerFault.exe -u -p <PID> -s 268	El PID cambia en cada ejecución. Se recomienda buscar el patrón de la línea de comandos junto con el hash del proceso padre.
Mutex	Local\SM0:\<PID>:168\:WilStaging_02Local\SM0:\<PID>:64\:WilError_03	Mutexes generados por la librería WIL. No son exclusivos del malware; deben correlacionarse con otros IoC.
Claves de registro consultadas	HKLM\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-USHKLM\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US	Utilizadas para verificar el idioma del sistema como mecanismo de anti-análisis.

Kit de minería de criptomonedas (familia Xm1.exe)

Archivo	Rol	MD5 / SHA-1 / SHA-256	Clasificación
Xm1.exe	Ejecutable inicial de la cadena — descarga/orquesta el resto de componentes	MD5: 65682c6fc40a0740f9d4f7d1c3932f2b SHA-1: 5f479c02644c58450c85c5ad33efe9199cba0dae SHA-256: 738f81da7c22f3c9c692d54f66a041d694699fb7f2d28d75400ca37ba1a1d421	Malicioso — trojan.doina/stealer
wmplaunch.exe	Cargador/crypter (familia BabaDeda) — desempaqueta y ejecuta la carga en memoria	MD5: 3c1a6521aa9221bc5cde44c5f69941f4 SHA-1: 8974582e5fd94d996346771d55f5718d859e89fa SHA-256: 009e0eda2f5d51bd969bddcb23615bdaabf4b975942e0a3534f5b6eb0c2bf86e	Malicioso — BabaDeda (loader/crypter), 19 motores AV
wmpsere.exe / wmpshere.exe / 8z9dsr0.exe	Instalador de persistencia — abusa del gestor de servicios NSSM	MD5: 10264a9149f4c25f281ef4e92a849294 SHA-1: 065faaa2c1f10bb3d413a46c5a436e52fbca0db4 SHA-256: 2c09e0b47015ae02b4919d1e7e3d2baf32788acde5030da404c24422c58423ee	Malicioso — trojan.reincarnation/nssm, 25/76 motores AV
wmplay.exe	Minero XMRig (64 bits) disfrazado de componente de Windows Media Player	MD5: f3d46b0471c59850be74cde4e4dbe9a8 SHA-1: 295b95ce7b844fc42e2a82b94861c653cf303114 SHA-256: 186646d84125fc993ffdb7c71ac5b10db5b18ecc4b7a0e7465372fb97b0d1930	Malicioso — miner.bitminer/disguisedxmrigminer, 52/71 motores AV
wmprphe.exe	Carga útil extraída / módulo auxiliar	MD5: 1703b2074a22307e941e521b6ffd5c76 SHA-1: 21c3f4e7fd4b7ff3657771634e9db3e82620614a SHA-256: 21c35cc59e4971980c0d7a05687424ceade5c08953522216303253bc062f7973	Malicioso — Trojan.Ulise
wmprphe.exe (variante)	Archivo dropper	MD5: 9abde6bfa586b6956d3a59ef927a658f SHA-1: d421a2983eef1da187d11abab6a86146076d610f SHA-256: 0f380859ee7aeceaaba2f43ece220398c32a1e7f13894109e1acc251c265c0b3	Malicioso — W32.EvogenTrj
C:\Windows\zl6p25ab.exe	Carga útil extraída — minero adicional	SHA-256: 295dc7913560f9077fd4f78d29ded8043f39f4494de53b5c5fc19cd508cebaca	Malicioso — trojan.alien / minero
WinRing0.sys / WinRing0x64.sys	Controlador vulnerable (BYOVD) — permite acceso a MSR desde espacio de usuario	MD5: 0c0195c48b6b8582fa6f6373032118da SHA-1: d25340ae8e92a6d29f599fef426a2bc1b5217299 SHA-256: 11bd2c9f9e2397c9a16e0990e4ed2cf0679498fe0fd418a3dfdac60b5c160ee5	Hacktool — controlador vulnerable conocido (vulndriver)
4FCE.bat	Script de monitoreo — reinicia el servicio si el minero es finalizado	MD5: e94a116c3be8c637175602949e754628 SHA-1: 7c3a8d20c5e4091021a5bdd9a57c84f84470b43e SHA-256: 6badb7ed64ebeeddb91dc6866fc87009ff921b96c3b7800bf07d3dae93417867	No detectado por motores — ejecuta a Xm1.exe
del.bat	Script de limpieza de artefactos	MD5: e7e5c0bbe968e5c24610ff4204197feb SHA-1: 37a872e1d42573662640f0ee1f438fa955574289 SHA-256: 8aac0bbefb2f4ac67e760a60886969d590c5d3bb510cfa7b8bae5cec52ae0849	No detectado por motores — ejecuta a Xm1.exe
D7D4.bat	Script auxiliar de despliegue	MD5: 3ae79d467fe4118d9bd4216c2ca0ebd0 SHA-1: 268bc307ecee32683fca91b488113f09b5b23c78 SHA-256: f3f03cf48eeaac4ae50e95397818ea3f26ff75ca07d996bc40be178d829cdfe3	No detectado por motores — ejecuta a Xm1.exe
config.json	Archivo de configuración del minero XMRig	SHA-256: 7ca8242bcace1b7a441e88aff2ed5d33607bb1d90c829c7ae9b6dbc84db0544d	No detectado — artefacto de configuración
wmplay.zip	Archivo comprimido padre del minero	MD5: 7147f546cc3f334c0021c3e080423014 SHA-1: 9644041fec10fd3e7697537dae29172668df23b3 SHA-256: 23e00e3a256fb37e637c2d3e1a1b89c0e51197e30591c67e496e2de8fa424ef2	Malicioso — miner.bitminer/unwantedx

Dominios

Dominio	Contexto	Estado
goldyminer[.]space	Pool de minería contactado por el componente XMRig (puerto 3333, protocolo Stratum)	Malicioso
xmrig[.]com	Dominio del proyecto XMRig, incrustado en el binario del minero	Sospechoso
randomx[.]xmrig[.]com	Subdominio de documentación del algoritmo RandomX, incrustado en el binario del minero	Sospechoso

Direcciones IP

Dirección IP	Contexto	Estado
103[.]195[.]103[.]171	Contactada por Xm1.exe	Sospechosa
172[.]93[.]105[.]51	Contactada por Xm1.exe	Sospechosa

Recomendaciones Técnicas

Contención y aislamiento

- ❑ Aislar de inmediato cualquier equipo donde se detecten los hashes, nombres de archivo o patrones de comando listados, sin apagarlo. Desconectar de la red preserva la memoria volátil y evita exfiltración o propagación lateral adicional.
- ❑ Si el equipo permanece encendido, priorizar la captura de memoria antes de cualquier apagado, en particular del proceso WerFault.exe.

Erradicación y remediación

- ❑ Restablecer las contraseñas de todas las cuentas de dominio con privilegios administrativos, en particular cualquier cuenta que haya ejecutado PsExec o scripts remotos durante la ventana temporal del incidente.
- ❑ Auditar los servicios instalados con NSSM (comandos nssm list y nssm dump <nombre_del_servicio>) y eliminar cualquier servicio no autorizado que apunte a rutas de usuario (AppData, Temp, ProgramData).
- ❑ Revisar las entradas de Opciones de Ejecución de Archivos de Imagen (IFEO) bajo HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options en busca de asociaciones no autorizadas con herramientas del sistema como taskmgr.exe.
- ❑ Aplicar la lista de bloqueo de controladores vulnerables de Microsoft para impedir la carga del controlador identificado (WinRing0.sys / WinRing0x64.sys).

Medidas de protección y mitigación

Gestión de acceso e identidad

- ❑ Exigir autenticación multifactor (MFA) en todos los servicios expuestos a internet, en particular RDP, VPN y portales administrativos.
- ❑ Aplicar el principio de menor privilegio: restringir qué cuentas pueden ejecutar PsExec, WMI remoto o PowerShell remoto entre segmentos de red, y limitar el uso de cuentas de administrador de dominio a estaciones de administración dedicadas (privileged access workstations).
- ❑ Restringir el acceso al protocolo SMB mediante el bloqueo del puerto TCP 445 en segmentos donde no sea requerido.
- ❑ Realizar auditorias periódicas de las cuentas con privilegios administrativos para validar su vigencia, propietario y nivel de acceso.

Detección y respuesta (EDR/SIEM)

- ❑ Configurar alertas de alta prioridad para inyección o escritura de memoria remota hacia procesos legítimos del sistema (WerFault.exe y equivalentes) iniciada por procesos de usuario final.
- ❑ Habilitar registro extendido de creación de procesos (Sysmon Event ID 1/8/10) para correlacionar de forma fiable crashes legítimos de procesos del sistema frente a inyecciones dirigidas.
- ❑ Configurar alertas cuando WmiPrvSE.exe se ejecute desde una ruta distinta a C:\Windows\System32\wbem\, o cuando su proceso padre sea distinto de svchost.exe.
- ❑ Configurar umbrales de uso sostenido de CPU superior al 80 % como indicador de minería de criptomonedas no autorizada.
- ❑ Forzar el Modo de Lenguaje Restringido (CLM) en PowerShell y habilitar el registro de bloques de script (Event ID 4104).

Control de aplicaciones y filtrado de red

- ❑ Implementar AppLocker o Windows Defender Application Control (WDAC) para bloquear la ejecución de binarios no firmados desde directorios de escritura del usuario (AppData, Temp, Downloads).
- ❑ Restringir el tráfico saliente hacia puertos habitualmente usados por protocolos de minería (3333, 4444, 14444).

Resiliencia y recuperación

- ❑ Mantener copias de seguridad fuera de línea o inmutables, aisladas del dominio principal, siguiendo el modelo 3-2-1 (tres copias, dos medios distintos, una fuera del sitio).
- ❑ Probar de forma regular los procedimientos de recuperación ante desastres para validar la integridad de las copias de seguridad y el tiempo real de restauración.

Fuentes

- ❑ ColCERT. (2026). Informe de análisis dinámico en sandbox (CAPE) del cargador/inyector principal: Mapeo a MITRE ATT&CK e indicadores de compromiso [Informe técnico de análisis de malware].
- ❑ ColCERT. (2026). Informe de análisis del kit de minería de criptomonedas y sus componentes asociados: Cuatro ejecutables relacionados, scripts de despliegue y mecanismos de persistencia [Informe técnico de análisis de malware].
- ❑ ColCERT. (2026). Informe de análisis del binario WmiPrvSE.exe y archivos contenedores asociados: Identificación de técnicas de DLL Side-Loading y artefactos maliciosos relacionados [Informe técnico de análisis de malware].
- ❑ ColCERT. (2026). Reportes de análisis dinámico multi-motor en plataforma de sandbox para muestras del cargador principal, el binario WmiPrvSE.exe y archivo de historial de PowerShell asociado [Informe técnico de análisis de malware].
- ❑ ColCERT. (2026). Perfil operacional de la familia de ransomware asociada por similitud al componente de cifrado: Programa de afiliados, evolución técnica, actores asociados e infraestructura Tor [Informe de inteligencia de amenazas].
- ❑ ColCERT. (2026). Grafo de relaciones del artefacto principal del incidente mediante plataforma de inteligencia de amenazas (Google Threat Intelligence / VirusTotal Graph) [Informe técnico de análisis de relaciones de malware].