Investigadores de ciberseguridad han revelado detalles sobre una nueva campaña de cryptojacking que emplea paquetes de software pirateado como señuelo para desplegar una versión personalizada del minero XMRig en equipos comprometidos.

«El análisis del dropper recuperado, los mecanismos de persistencia y la carga de minería pone de manifiesto una infección sofisticada y de múltiples etapas que prioriza la máxima tasa de hash para la minería de criptomonedas, a menudo desestabilizando el sistema de la víctima», señaló el investigador de Trellix, Aswath A, en un informe técnico publicado la semana pasada.

«Además, el malware presenta capacidades similares a las de un gusano, propagándose a través de dispositivos de almacenamiento externos, lo que facilita el movimiento lateral incluso en entornos aislados (air-gapped).»

El punto de entrada del ataque radica en el uso de señuelos de ingeniería social que promocionan software premium gratuito en forma de paquetes pirateados, como instaladores de suites de ofimática, con el fin de engañar a usuarios desprevenidos para que descarguen ejecutables infectados con malware.

El binario funciona como el sistema nervioso central de la infección, desempeñando distintos papeles como instalador, vigilante, gestor de cargas útiles y limpiador, supervisando las diferentes fases del ciclo de vida del ataque. Presenta un diseño modular que separa las funciones de monitoreo de las cargas principales responsables de la minería de criptomonedas, la escalada de privilegios y la persistencia en caso de que el proceso sea interrumpido.

Esta flexibilidad, o cambio de modo, se logra mediante argumentos de línea de comandos –

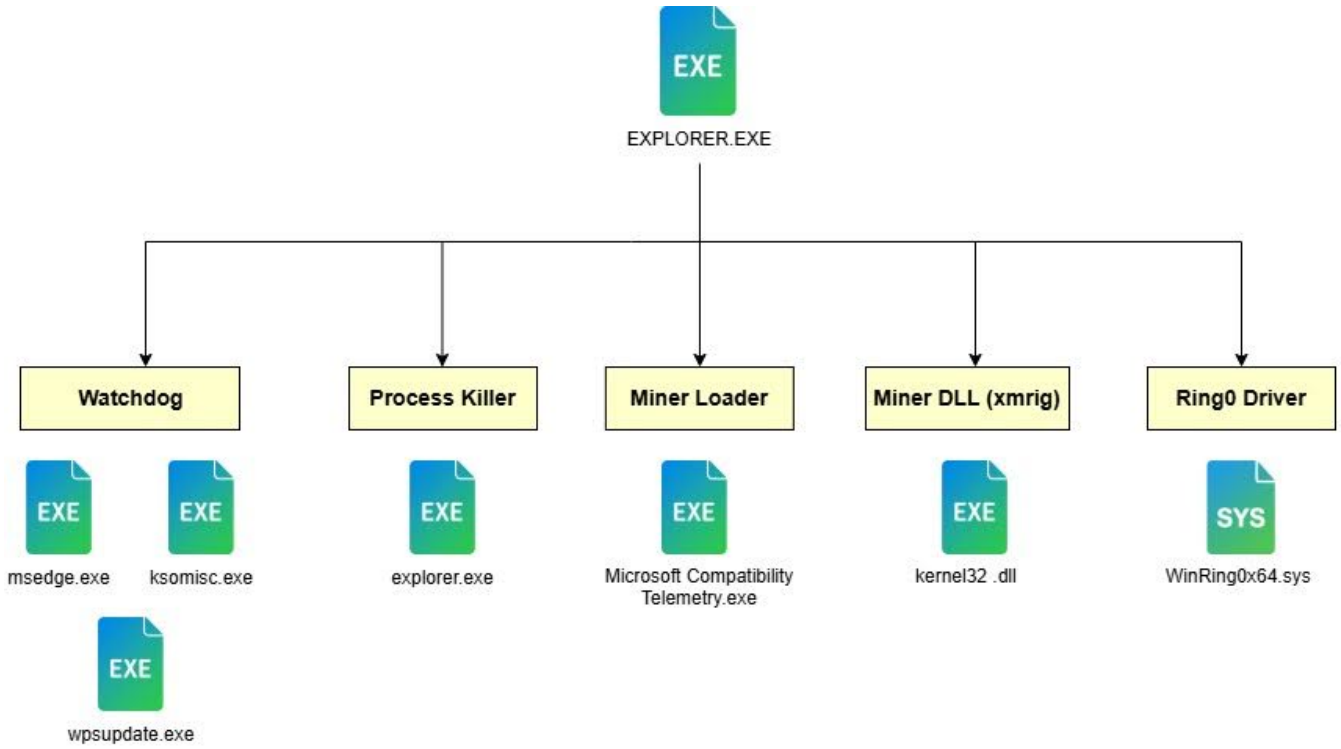
Sin parámetros, para validar el entorno y realizar la migración durante la fase inicial de instalación.
002 Re:0, para desplegar las cargas principales, iniciar el minero y entrar en un bucle de supervisión.

016, para reiniciar el proceso del minero si es finalizado.
barusu, para activar una secuencia de autodestrucción que finaliza todos los componentes maliciosos y elimina los archivos.

El malware incorpora una bomba lógica que funciona obteniendo la hora local del sistema y comparándola con una marca temporal predefinida –

Si la fecha es anterior al 23 de diciembre de 2025, el malware continúa con la instalación de los módulos de persistencia y lanza el minero.
Si la fecha es posterior al 23 de diciembre de 2025, el binario se ejecuta con el argumento «barusu», lo que provoca un «desmantelamiento controlado» de la infección.

Según Trellix, la fecha límite estricta del 23 de diciembre de 2025 sugiere que la campaña fue concebida para operar indefinidamente en los sistemas comprometidos, y que dicha fecha podría marcar la expiración de una infraestructura de comando y control (C2) alquilada, un cambio previsto en el mercado de criptomonedas o la transición planificada hacia una nueva variante de malware.



En la rutina estándar de infección, el binario —que actúa como un «portador autónomo» de todas las cargas maliciosas— escribe en el disco los distintos componentes, incluido un ejecutable legítimo del servicio de Telemetría de Windows que se utiliza para cargar de forma lateral la DLL del minero.

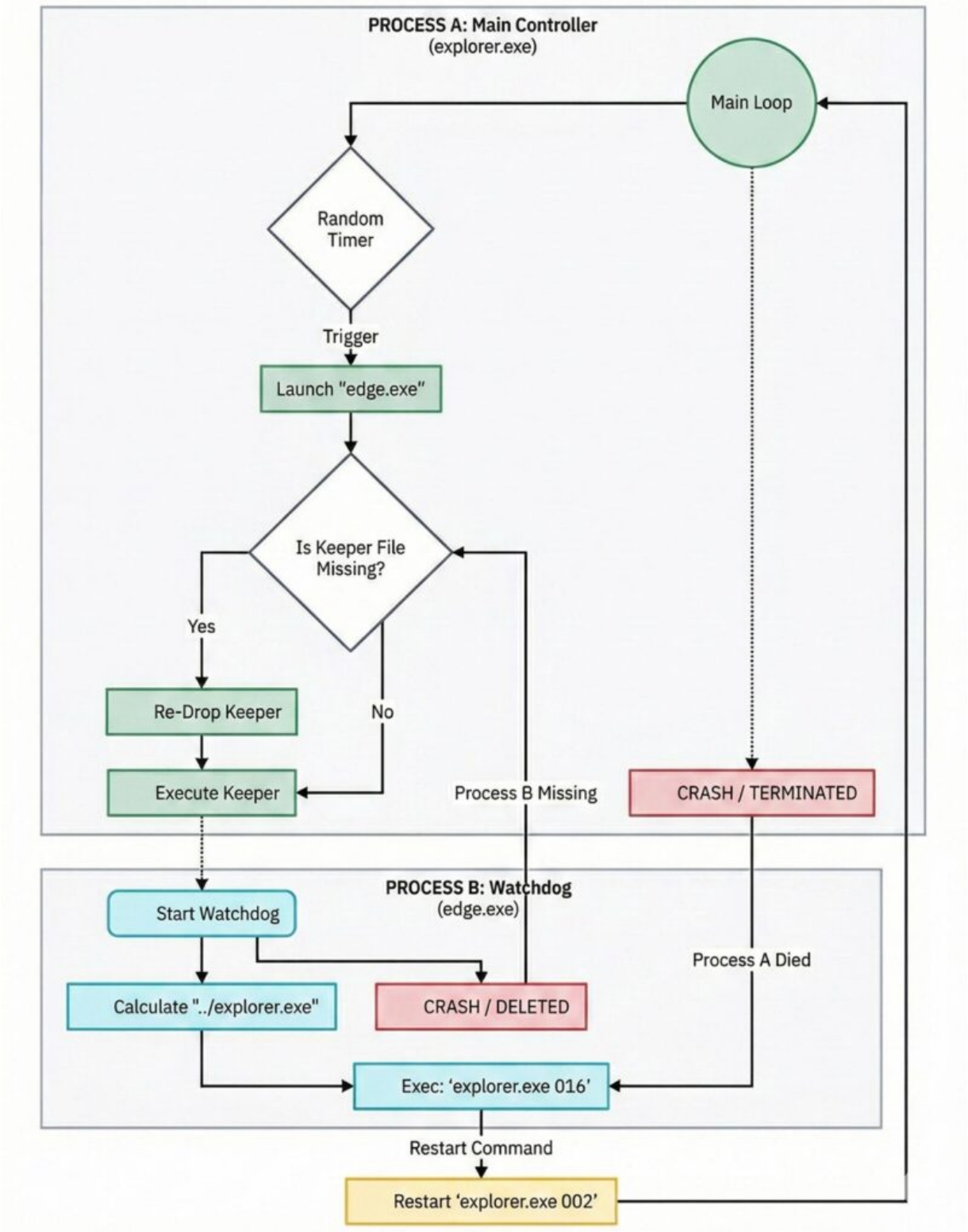
También se depositan archivos destinados a garantizar la persistencia, desactivar herramientas de seguridad y ejecutar el minero con privilegios elevados mediante el uso de un controlador legítimo pero vulnerable («WinRing0x64.sys»), como parte de la técnica conocida como bring your own vulnerable driver (BYOVD). Este controlador es vulnerable a la falla registrada como CVE-2020-14979 (puntuación CVSS: 7.8), que permite la escalada de privilegios.

La integración de este exploit en el minero XMRig tiene como objetivo obtener un mayor control sobre la configuración de bajo nivel del CPU y aumentar el rendimiento de la minería (es decir, la tasa de hash de RandomX) entre un 15% y un 50%.

«Una característica distintiva de esta variante de XMRig es su agresiva capacidad de propagación», indicó Trellix. *«No depende únicamente de que el usuario descargue el dropper; intenta activamente extenderse a otros sistemas mediante medios extraíbles. Esto transforma al malware de un simple troyano en un gusano.»*

Las evidencias muestran que la actividad de minería se produjo, aunque de manera intermitente, a lo largo de noviembre de 2025, antes de incrementarse notablemente el 8 de diciembre de 2025.

«Esta campaña es un claro recordatorio de que el malware de tipo commodity sigue evolucionando», concluyó la compañía de ciberseguridad. *«Al encadenar ingeniería social, suplantación de software legítimo, propagación tipo gusano y explotación a nivel de kernel, los atacantes han construido una botnet resistente y altamente eficiente.»*


PROCESS A: Main Controller
(explorer.exe)
Main Loop
Random Timer
Trigger
Launch "edge.exe"
Is Keeper File Missing?
Yes
No
Re-Drop Keeper
Execute Keeper
Process B Missing
CRASH / TERMINATED
PROCESS B: Watchdog
(edge.exe)
Start Watchdog
Calculate "../explorer.exe"
CRASH / DELETED
Process A Died
Exec: 'explorer.exe 016'
Restart Command
Restart 'explorer.exe 002'

La revelación se produce después de que Darktrace informara haber identificado un artefacto malicioso probablemente generado con un modelo de lenguaje de gran tamaño (LLM), que explota la vulnerabilidad React2Shell (CVE-2025-55182, puntuación CVSS: 10.0) para descargar un kit de herramientas en Python, el cual aprovecha el acceso obtenido para desplegar un minero XMRig mediante la ejecución de un comando de shell.

«Aunque la cantidad de dinero generada por el atacante en este caso es relativamente baja, y la criptominería no es una técnica nueva, esta campaña demuestra que los LLM basados en IA han hecho que el cibercrimen sea más accesible que nunca», señalaron los investigadores Nathaniel Bill y Nathaniel Jones.

«Una sola sesión de prompting con un modelo fue suficiente para que este atacante generara un marco de explotación funcional y comprometiera más de noventa equipos, lo que demuestra que el valor operativo de la IA para los adversarios no debe subestimarse.»

Según WhoisXML API, los atacantes también han estado utilizando un kit denominado ILOVEPOOP para escanear sistemas expuestos que siguen siendo vulnerables a React2Shell, aparentemente con el objetivo de preparar el terreno para futuras ofensivas. La actividad de sondeo se ha dirigido especialmente a organizaciones gubernamentales, de defensa, financieras e industriales en Estados Unidos.

«Lo que hace inusual a ILOVEPOOP es la discrepancia entre cómo fue desarrollado y cómo se utilizó», afirmó Alex Ronquillo, vicepresidente de producto en WhoisXML API. *«El código en sí demuestra un conocimiento de nivel experto sobre los componentes internos de React Server Components y emplea técnicas de ataque que no aparecen en ningún otro kit documentado de React2Shell.»*

«Sin embargo, quienes lo desplegaron cometieron errores operativos básicos al interactuar con los sistemas honeypot de monitoreo de WhoisXML API, fallos que un atacante sofisticado normalmente evitaría. En términos prácticos, esta brecha apunta a una división del trabajo.»

«Podríamos estar ante dos grupos distintos: uno que desarrolló la herramienta y otro que la

está utilizando. Este patrón se observa en operaciones patrocinadas por Estados: un equipo capacitado crea las herramientas y luego las entrega a operadores que ejecutan campañas masivas de escaneo. Los operadores no necesitan comprender cómo funciona la herramienta; solo deben ejecutarla.»