Investigadores de ciberseguridad revelaron cómo actores maliciosos aprovecharon una vulnerabilidad ya corregida en Microsoft Windows para desplegar el malware PipeMagic en ataques vinculados al ransomware RansomExx.

Los incidentes giran en torno al abuso de CVE-2025-29824, una falla de escalamiento de privilegios que afecta al Windows Common Log File System (CLFS) y que Microsoft solucionó en abril de 2025, según un informe conjunto publicado hoy por Kaspersky y BI.ZONE.

PipeMagic fue identificado por primera vez en 2022 como parte de las campañas de RansomExx contra compañías industriales en el sudeste asiático. El malware actúa como una puerta trasera completa, capaz de otorgar acceso remoto y ejecutar una amplia variedad de comandos en los sistemas comprometidos.

En aquellas campañas iniciales, los atacantes explotaron CVE-2017-0144, una vulnerabilidad de ejecución remota en Windows SMB, para penetrar en las infraestructuras de las víctimas. Posteriormente, en octubre de 2024, se observaron cadenas de infección en Arabia Saudita que usaban como señuelo una aplicación falsa de OpenAI ChatGPT para propagar el malware.

En abril de este año, Microsoft atribuyó la explotación de CVE-2025-29824 y el uso de PipeMagic a un grupo de amenazas identificado como Storm-2460.

"Una característica particular de PipeMagic es que genera un arreglo aleatorio de 16 bytes utilizado para crear una tubería nombrada con el formato: \\.*pipe**1.*"*, explicaron los investigadores Sergey Lozhkin, Leonid Bezvershenko, Kirill Korchemny e Ilya Savelyev. *"Después de ello, se lanza un hilo que de manera continua crea esta tubería, intenta leer datos de ella y luego la elimina. Este método de comunicación es esencial para que la puerta trasera transfiera cargas útiles cifradas y notificaciones."*

PipeMagic es un malware modular basado en complementos que utiliza un dominio alojado en la nube de Microsoft Azure para descargar componentes adicionales. En los ataques de 2025 dirigidos a Arabia Saudita y Brasil, se apoyó en un archivo de índice de ayuda de Microsoft (*"metafile.mshi"*) como cargador. Dicho cargador descomprime código C# que

descifra y ejecuta *shellcode* incrustado.

"El shellcode inyectado corresponde a código ejecutable para sistemas Windows de 32 bits", detallaron los analistas. *"Este carga un ejecutable sin cifrar embebido dentro del propio shellcode."*

Kaspersky también descubrió en 2025 nuevos rastros de cargadores de PipeMagic que se hacían pasar por un cliente de ChatGPT, muy similares a los observados en octubre de 2024. Estas muestras empleaban técnicas de secuestro de DLL para ejecutar una librería maliciosa disfrazada como archivo de actualización de Google Chrome (*"googleupdate.dll"*).

Independientemente del método de carga utilizado, todos los caminos conducen a la instalación del *backdoor* PipeMagic, que soporta diversos módulos:

- Módulo de comunicación asíncrona con cinco comandos para finalizar el plugin, leer/escribir archivos, detener una operación de archivo o cancelar todas las operaciones.
- Módulo cargador para inyectar cargas adicionales en memoria y ejecutarlas.
- Módulo inyector para lanzar ejecutables en C#.

"La detección constante de PipeMagic en ataques contra organizaciones en Arabia Saudita y su reciente aparición en Brasil demuestran que el malware sigue activo y que sus desarrolladores continúan ampliando sus capacidades", afirmaron los expertos.

"Las versiones descubiertas en 2025 presentan mejoras respecto a las de 2024, diseñadas para mantenerse en los sistemas de las víctimas y moverse lateralmente dentro de las redes internas. En las intrusiones más recientes, los atacantes emplearon la herramienta ProcDump, renombrada como dllhost.exe, para extraer memoria del proceso LSASS."