Alerta Id	0017
Fecha del reporte	08/20/2025
Entidad	Todas las entidades del ecosistema digital
Título	Hackers explotan vulnerabilidad de Windows para desplegar el malware PipeMagic en ataques de ransomware RansomExx
Herramienta de detección	Fortirecon
Activo involucrado	Microsoft Windows – versiones vulnerables al exploit de CLFS (CVE-2025-29824)
Tipo de alerta	Explotación activa de vulnerabilidad / Distribución de malware modular
Nivel de riesgo	Crítico

Objetivo

Informar a las entidades del ecosistema digital sobre la explotación activa de la vulnerabilidad **CVE-2025-29824** en Microsoft Windows, utilizada por el grupo de ransomware RansomExx (Storm-2460) para desplegar el malware modular **PipeMagic**, el cual permite la ejecución remota de código, persistencia en sistemas comprometidos y la exfiltración de información sensible a través de comunicaciones cifradas.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Descripción

Investigadores de ciberseguridad de Kaspersky y BI.ZONE identificaron que actores de amenazas están explotando la vulnerabilidad **CVE-2025-29824**, un fallo de escalación de privilegios en el subsistema Windows Common Log File System (CLFS) parcheado por Microsoft en abril de 2025.

Los ataques recientes atribuidos al grupo Storm-2460 involucran la distribución del malware PipeMagic, un backdoor modular que facilita la ejecución de payloads adicionales y la comunicación cifrada con servidores de comando y control (C2).

La amenaza ha sido identificada y clasificada dentro de la plataforma FortiRecon (Adversary Centric Intelligence - OSINT Cyber Threats), específicamente en la categoría Early Warning, con la entrada publicada el 18 de agosto de 2025 bajo el título:

“Microsoft Windows Vulnerability Exploited to Deploy PipeMagic RansomExx Malware”.

Esto confirma la relevancia del incidente y su visibilidad dentro de ecosistemas de inteligencia de amenazas de nivel empresarial.

Principales hallazgos:

- PipeMagic establece tuberías con nombre (\\.\pipe\1.<cadena hex>) para comunicaciones internas y transmisión de payloads cifrados.

- El malware ha sido distribuido mediante diferentes vectores:

    - Archivos de ayuda de Microsoft (.msi) como cargadores.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Aplicaciones falsas de ChatGPT, desarrolladas en Rust, que muestran una ventana en blanco mientras instalan el malware en segundo plano.

- Técnicas de DLL hijacking, usando archivos maliciosos disfrazados como googleupdate.dll.

- En 2025, se han identificado campañas dirigidas a organizaciones en Arabia Saudí, Brasil, Venezuela y Estados Unidos, especialmente en los sectores financiero, bienes raíces, TI y retail.

- En ataques recientes, se detectó el uso de ProcDump renombrado como dllhost.exe para extraer credenciales desde LSASS.

La Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA) agregó **CVE-2025-29824** a su catálogo de vulnerabilidades explotadas conocidas, reforzando la urgencia de aplicar medidas de mitigación.

Impacto

- **Compromiso total del sistema operativo Windows vulnerable** mediante escalación de privilegios.

- **Despliegue de ransomware RansomExx**, con impacto en la continuidad operativa, cifrado de archivos y riesgo de filtración de datos.

- **Riesgo elevado de persistencia y movimiento lateral** en redes corporativas.

- **Sectores más afectados**: TI, financiero, bienes raíces, retail y salud (potencialmente).

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Recomendaciones de mitigación

1. Aplicar inmediatamente los parches de seguridad liberados por Microsoft en abril y agosto de 2025 que corrigen CVE-2025-29824 y otras vulnerabilidades críticas.

2. Monitorear intentos de carga de archivos sospechosos (.msi, googleupdate.dll, aplicaciones no oficiales de ChatGPT).

3. Revisar procesos relacionados con dllhost.exe y verificar si corresponden a instancias legítimas.

4. Implementar políticas de mínimo privilegio y segmentación de red para limitar el movimiento lateral.

5. Mantener respaldos cifrados y probados, aislados de la red de producción.

6. Capacitar a los usuarios sobre la descarga segura de aplicaciones y los riesgos de software falso.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Fuentes

- https://gbhackers.com/cisa-alerts-on-trend-micro-apex-one-vulnerability/#google_vignette
- https://thehackernews.com/2025/08/microsoft-windows-vulnerability.html
- https://www.perplexity.ai/discover/tech/microsoft-patches-critical-win-hGgDfFTHQy.5GajGiUk3cA

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el **CSIRT Salud** a través de las líneas telefónicas **(+57) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570