Los actores de amenazas asociados con el ransomware Black Basta podrían haber explotado una reciente vulnerabilidad de escalada de privilegios en el Servicio de Informes de Errores de Windows de Microsoft como un zero-day, según nuevos descubrimientos de Symantec.

La vulnerabilidad en cuestión es CVE-2024-26169 (puntuación CVSS: 7.8), un fallo de elevación de privilegios en el Servicio de Informes de Errores de Windows que podría ser explotado para obtener privilegios de SISTEMA. Microsoft corrigió esta vulnerabilidad en marzo de 2024.

> *«El análisis de una herramienta de exploit desplegada en ataques recientes reveló evidencia de que podría haber sido compilada antes del parche, lo que indica que al menos un grupo podría haber estado explotando la vulnerabilidad como zero-day»,* dijo el Equipo de Cazadores de Amenazas de Symantec, parte de Broadcom.

El grupo de amenazas con motivaciones financieras está siendo rastreado por la empresa bajo el nombre Cardinal, también conocido como Storm-1811 y UNC4393.

Se sabe que monetiza el acceso desplegando el ransomware Black Basta, generalmente aprovechando el acceso inicial obtenido por otros atacantes, inicialmente QakBot y posteriormente DarkGate, para infiltrarse en los entornos objetivo.

En los últimos meses, se ha observado que este actor de amenazas utiliza productos legítimos de Microsoft como Quick Assist y Microsoft Teams como vectores de ataque para infectar a los usuarios.

> *«El actor de amenazas utiliza Teams para enviar mensajes e iniciar llamadas en un intento de hacerse pasar por personal de TI o de soporte técnico. Esta actividad lleva al uso indebido de Quick Assist, seguido por el robo de credenciales utilizando EvilProxy, la ejecución de scripts por lotes y el uso de SystemBC para persistencia y comando y control»*, dijo Microsoft.

Symantec señaló que observó el uso de la herramienta de exploit como parte de un intento fallido de ataque de ransomware.

La herramienta *«aprovecha el hecho de que el archivo Windows werkernel.sys utiliza un descriptor de seguridad nulo al crear claves del registro»,* explicó.

> *«El exploit usa esto para crear una clave de registro 'HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WerFault.exe' donde establece el valor 'Debugger' como la ruta ejecutable propia. Esto permite al exploit iniciar una shell con privilegios administrativos.»*

El análisis de los metadatos del artefacto muestra que fue compilado el 27 de febrero de 2024, varias semanas antes de que Microsoft abordara la vulnerabilidad, mientras que otra muestra descubierta en VirusTotal tenía una marca temporal de compilación del 18 de diciembre de 2023.

Aunque los actores de amenazas suelen alterar las marcas temporales de archivos y directorios en un sistema comprometido para ocultar sus acciones o dificultar las investigaciones —una técnica conocida como timestomping— Symantec indicó que probablemente hay muy pocas razones para hacerlo en este caso.

Este desarrollo se produce en medio del surgimiento de una nueva familia de ransomware llamada DORRA, una variante del malware Makop, ya que los ataques de ransomware han vuelto a resurgir después de una disminución en 2022.

Según Mandiant, propiedad de Google, la epidemia de ransomware ha visto un aumento del 75% en publicaciones en sitios web de filtración de datos, con más de $1.1 mil millones pagados a los atacantes en 2023, en comparación con $567 millones en 2022 y $983 millones en 2021.

> *«Esto ilustra que la ligera disminución en la actividad de extorsión observada en 2022 fue una anomalía, potencialmente debido a factores como la invasión de Ucrania y las conversaciones filtradas de Conti»*, dijo la compañía.
>
> *«El actual resurgimiento en la actividad de extorsión probablemente se debe a varios factores, incluida la reubicación del ecosistema ciberdelincuente tras un año tumultuoso en 2022, nuevos participantes y nuevas asociaciones, y la oferta de servicios de ransomware por actores previamente asociados con grupos prolíficos que habían sido interrumpidos.»*