Los actores de amenazas detrás de la operación de ransomware como servicio (RaaS) Medusa han sido detectados utilizando un controlador malicioso denominado ABYSSWORKER como parte de un ataque «Bring Your Own Vulnerable Driver» (BYOVD), diseñado para deshabilitar herramientas antimalware.

Según Elastic Security Labs, en un ataque de ransomware de Medusa se utilizó un cargador empaquetado con un servicio de empaquetado (PaaS) llamado HeartCrypt para entregar el cifrador.

> *«Este cargador se desplegó junto con un controlador firmado con un certificado revocado de un proveedor chino, al que llamamos ABYSSWORKER. Este controlador se instala en la máquina víctima y luego se usa para atacar y deshabilitar diferentes soluciones de detección y respuesta de endpoints (EDR)»,* indicó la empresa en un informe.

El controlador identificado, «smuol.sys», imita al legítimo controlador CrowdStrike Falcon («CSAgent.sys»). Se han detectado decenas de archivos relacionados con ABYSSWORKER en la plataforma VirusTotal, con registros que van desde el 8 de agosto de 2024 hasta el 25 de febrero de 2025. Todas las muestras encontradas están firmadas con certificados probablemente robados y posteriormente revocados de empresas chinas.

El hecho de que el malware esté firmado le otorga una apariencia de legitimidad, lo que le permite evadir los sistemas de seguridad sin levantar sospechas. Cabe destacar que este controlador diseñado para deshabilitar soluciones EDR ya había sido documentado previamente por ConnectWise en enero de 2025 bajo el nombre «nbwdv.sys».

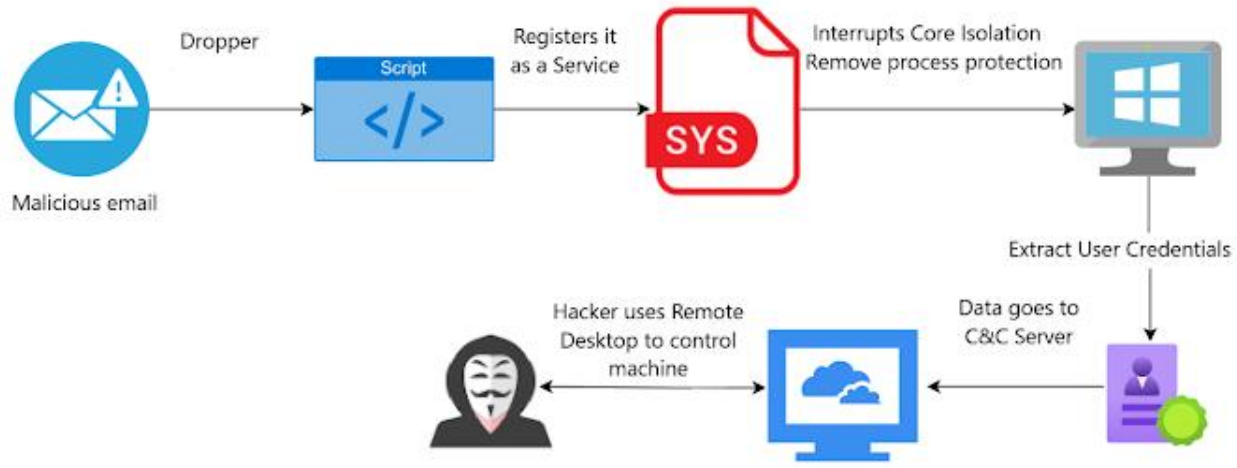
Una vez activado, ABYSSWORKER agrega el ID del proceso a una lista de procesos protegidos a nivel global y monitorea las solicitudes de control de entrada/salida (I/O) de dispositivos, redirigiéndolas a los controladores correspondientes según el código de control de I/O.

> *«Estos controladores abarcan una amplia gama de funciones, desde la manipulación de archivos hasta la terminación de procesos y controladores, proporcionando un conjunto de herramientas que permite deshabilitar de manera temporal o permanente los sistemas EDR»,* explicó Elastic.

Entre los códigos de control de I/O detectados, destaca el 0x222400, que puede usarse para desactivar productos de seguridad al buscar y eliminar todas las devoluciones de llamada de notificación registradas. Este mismo método ha sido adoptado por otras herramientas especializadas en desactivar soluciones EDR, como EDRSandBlast y RealBlindingEDR.

La lista de algunos códigos I/O es la siguiente:

- 0x222080 – Enable the driver by sending a password «7N6bCAoECbItsUR5-h4Rp2nkQxybfKb0F-wgbJGHGh20pWUuN1-ZxfXdiOYps6HTp0X»
- 0x2220c0 – Load necessary kernel APIs
- 0x222184 – Copy file
- 0x222180 – Delete file
- 0x222408 – Kill system threads by module name
- 0x222400 – Remove notification callbacks by module name
- 0x2220c0 – Load API
- 0x222144 – Terminate process by their process ID
- 0x222140 – Terminate thread by their thread ID
- 0x222084 – Disable malware
- 0x222664 – Reboot the machine



Los hallazgos siguen a un informe de Venak Security sobre cómo actores malintencionados están explotando un controlador de kernel legítimo pero vulnerable asociado con el antivirus ZoneAlarm de Check Point. Esta vulnerabilidad se utiliza en un ataque del tipo BYOVD (Bring Your Own Vulnerable Driver) para obtener privilegios elevados y desactivar funciones de seguridad de Windows, como la Integridad de Memoria.

Los atacantes aprovecharon estos privilegios para establecer una conexión mediante el Protocolo de Escritorio Remoto (RDP) en los sistemas infectados, lo que les permitió mantener un acceso persistente. Sin embargo, Check Point ya ha corregido esta vulnerabilidad.

> *«Como el controlador vsdatant.sys opera con altos privilegios en el kernel, los atacantes pudieron explotarlo para evadir las protecciones de seguridad y el software antivirus, obteniendo así control total sobre las máquinas infectadas»,* explicó la empresa.

Una vez superadas estas defensas, los atacantes lograron acceder al sistema, lo que les permitió obtener información sensible, como contraseñas de usuario y otras credenciales almacenadas. Estos datos fueron extraídos y podrían ser utilizados en futuros ataques.

Este incidente coincide con la atribución de la operación de ransomware RansomHub (también conocida como Greenbottle y Cyclops) al uso de una puerta trasera multifuncional previamente no documentada, denominada Betruger, por parte de al menos uno de sus afiliados.

Este malware incluye funciones avanzadas que suelen emplearse en las etapas previas a un ataque de ransomware, como la captura de pantalla, registro de pulsaciones de teclas (keylogging), análisis de la red, escalamiento de privilegios, extracción de credenciales y exfiltración de datos a un servidor remoto.

> *«Las capacidades de Betruger sugieren que fue desarrollado para reducir la cantidad de herramientas adicionales que deben ser introducidas en una red objetivo durante la preparación de un ataque de ransomware»*, señaló Symantec, una empresa propiedad de Broadcom.

El informe también destaca que el uso de malware personalizado más allá de las cargas útiles de cifrado es poco común en ataques de ransomware. Generalmente, los atacantes recurren a herramientas legítimas, técnicas de «living off the land» y malware de acceso público como Mimikatz y Cobalt Strike.