Un nuevo estudio sobre herramientas destinadas a desactivar sistemas de detección y respuesta en endpoints (EDR) ha revelado que 54 de ellas emplean una técnica conocida como “bring your own vulnerable driver” (BYOVD), aprovechándose de un total de 34 controladores con vulnerabilidades.

Los programas diseñados para eliminar EDR han sido frecuentes en intrusiones de ransomware, ya que brindan a los afiliados una forma de neutralizar el software de seguridad antes de desplegar malware que cifra archivos. Esto se hace con el objetivo de evitar ser detectados.

«Las bandas de ransomware, especialmente aquellas que operan bajo el modelo de ransomware como servicio (RaaS), suelen generar nuevas versiones de sus cifradores con frecuencia, y lograr que cada una pase desapercibida puede ser un proceso largo,» explicó el investigador de ESET, Jakub Souček, en un informe compartido con The Hacker News.

«Más importante aún, los cifradores son intrínsecamente muy ruidosos (ya que necesitan modificar una gran cantidad de archivos en poco tiempo); por lo tanto, hacer que este tipo de malware no sea detectado resulta bastante complicado.»

Los EDR killers funcionan como un componente externo especializado que se ejecuta para deshabilitar los controles de seguridad antes de activar los cifradores, lo que permite que estos últimos se mantengan simples, estables y fáciles de reconstruir. Sin embargo, esto no significa que no existan casos donde la finalización de EDR y el módulo de ransomware estén integrados en un solo binario. El ransomware Reynolds es un ejemplo de ello.

La mayoría de estas herramientas dependen de controladores legítimos pero vulnerables para obtener privilegios elevados y cumplir sus objetivos. De cerca de 90 herramientas identificadas por la empresa eslovaca de ciberseguridad, más de la mitad utilizan la conocida técnica BYOVD debido a su fiabilidad.

«El objetivo de un ataque BYOVD es obtener privilegios en modo kernel, también conocidos como Ring 0,» explica Bitdefender. *«En este nivel, el código tiene acceso total a la memoria*

del sistema y al hardware. Dado que un atacante no puede cargar un controlador malicioso sin firma, 'introduce' uno firmado por un proveedor confiable (como un fabricante de hardware o una versión antigua de antivirus) que contiene una vulnerabilidad conocida.»

Con acceso al kernel, los actores maliciosos pueden finalizar procesos EDR, desactivar herramientas de seguridad, manipular callbacks del kernel y debilitar las protecciones del endpoint. El resultado es un abuso del modelo de confianza de controladores de Microsoft para evadir defensas, aprovechando que el controlador vulnerable es legítimo y está firmado.

Los EDR killers basados en BYOVD son desarrollados principalmente por tres tipos de actores:

- Grupos cerrados de ransomware como DeadLock y Warlock, que no dependen de afiliados
- Atacantes que reutilizan y modifican código de prueba de concepto existente (por ejemplo, SmilingKiller y TfSysMon-Killer)
- Ciberdelincuentes que comercializan estas herramientas en mercados clandestinos como servicio (por ejemplo, DemoKiller, también conocido como Бафомет, ABYSSWORKER y CardSpaceKiller)

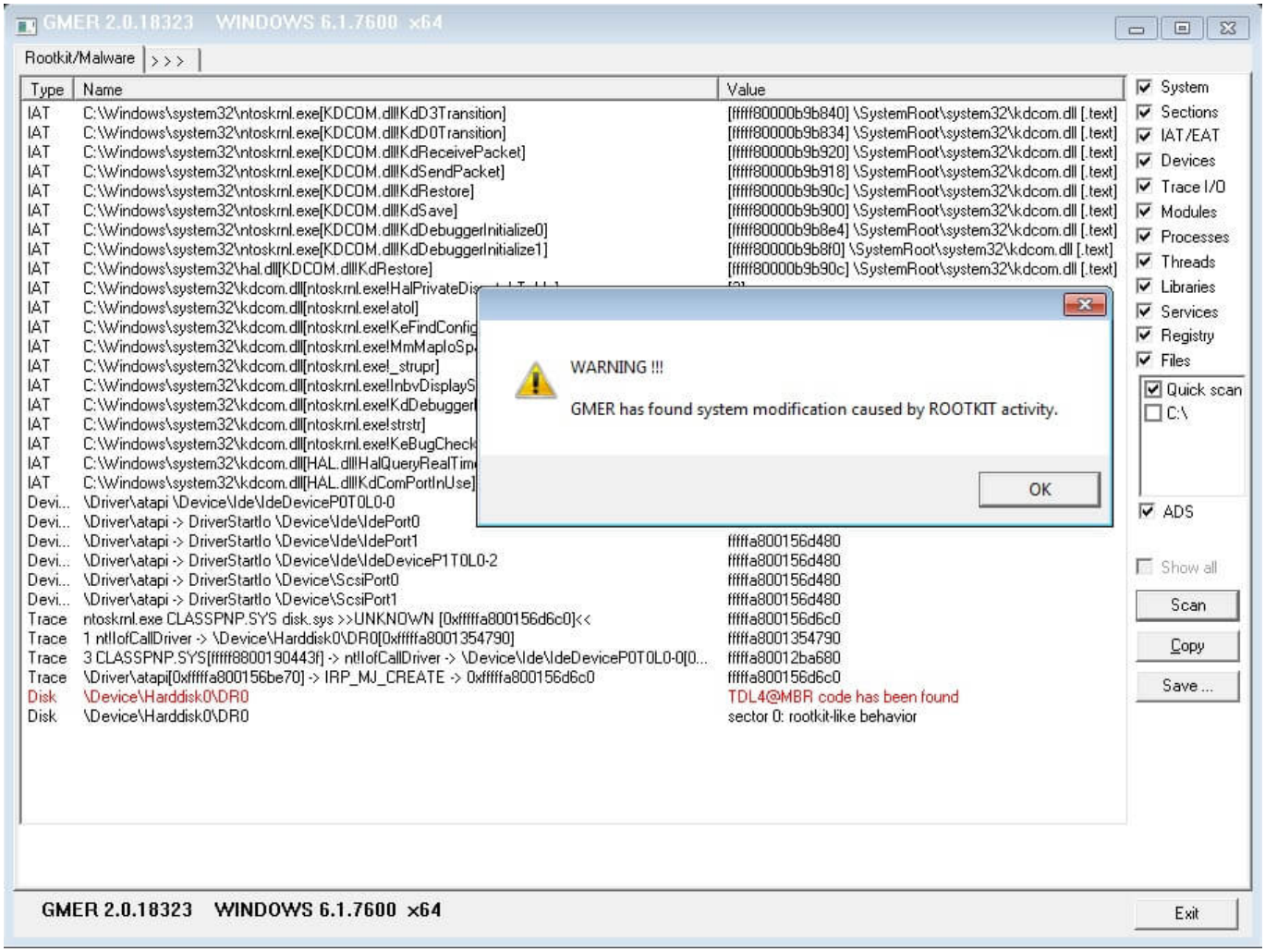
ESET también indicó que identificó herramientas basadas en scripts que utilizan comandos administrativos integrados como taskkill, net stop o sc delete para interferir con el funcionamiento normal de procesos y servicios de seguridad. Algunas variantes combinan scripting con el Modo Seguro de Windows.

«Dado que el Modo Seguro solo carga un subconjunto mínimo del sistema operativo, y normalmente no incluye soluciones de seguridad, el malware tiene más probabilidades de desactivar la protección,» señaló la compañía. *«Al mismo tiempo, esta actividad es muy evidente, ya que requiere reiniciar el sistema, lo cual es arriesgado y poco confiable en entornos desconocidos. Por ello, se observa con poca frecuencia en ataques reales.»*

Una tercera categoría de EDR killers corresponde a herramientas anti-rootkit, que incluyen utilidades legítimas como GMER, HRSword y PC Hunter, las cuales ofrecen interfaces

intuitivas para finalizar procesos o servicios protegidos. Una cuarta categoría emergente está formada por herramientas sin controlador, como EDRSilencer y EDR-Freeze, que bloquean el tráfico saliente de las soluciones EDR y provocan que estos programas entren en un estado similar a un “coma”.

«Los atacantes ya no invierten tanto esfuerzo en hacer que sus cifradores pasen desapercibidos,» indicó ESET. *«En cambio, las técnicas sofisticadas para evadir defensas se han trasladado a los componentes en modo usuario de los EDR killers. Esta tendencia es especialmente visible en herramientas comerciales, que a menudo incorporan capacidades avanzadas de anti-análisis y anti-detección.»*



Para combatir el ransomware y estas herramientas, bloquear la carga de controladores comúnmente explotados es un mecanismo de defensa esencial. No obstante, dado que los EDR killers se ejecutan en la fase final, justo antes de lanzar el cifrador, un fallo en este punto permite al atacante cambiar fácilmente a otra herramienta para lograr el mismo objetivo.

Esto implica que las organizaciones deben implementar defensas en capas y estrategias de detección que permitan monitorear, identificar, contener y mitigar amenazas de forma proactiva en cada etapa del ciclo de ataque.

«Los EDR killers persisten porque son económicos, consistentes y están desacoplados del cifrador — una combinación ideal tanto para los desarrolladores, que no necesitan centrarse en ocultar sus cifradores, como para los afiliados, que disponen de una herramienta potente y fácil de usar para desactivar defensas antes del cifrado,» concluyó ESET.