Un kit de arranque sigiloso de interfaz de firmware extensible unificada (UEFI), llamado BlackLotus, se ha convertido en el primer malware conocido públicamente capaz de eludir las defensas de arranque seguro, lo que lo convierte en una amenaza potente en el panorama cibernético.

> *«Este bootkit puede ejecutarse incluso en sistemas Windows 11 completamente actualizados con UEFI Secure Boot habilitado»,* dijo la compañía ESET en un informe.

Los bootkits UEFI se implementan en el firmware del sistema y permiten un control total sobre el proceso de inicio del sistema operativo (SO), lo que hace posible deshabilitar los mecanismos de seguridad a nivel del sistema operativo e implementar cargas útiles arbitrarias durante el inicio de sesión con privilegios elevados.

Ofrecido a la venta por $5,000 dólares (y $200 dólares por cada nueva versión posterior), el potente y persistente juego de herramientas está programado en ensamblador y C, y tiene un tamaño de 80 kilobytes. También tiene capacidades de geofencing para evitar infectar computadoras en Armenia, Belorrusia, Kazakstán, Moldavia, Rumania, Rusia y Ucrania.

Los detalles sobre BlackLotus surgieron por primera vez en octubre de 2022, y el investigador de seguridad de Kaspersky, Sergey Lozhkin, lo descubrió como una solución sofisticada de software delictivo.

> *«Esto representa un pequeño salto hacia adelante, en términos de facilidad de uso, escalabilidad, accesibilidad y, lo que es más importante, el potencial de un impacto mucho mayor en las formas de persistencia y evasión y/o destrucción»,* dijo Scott Scheferman, de Eclypsium.

En otras palabras, BlackLotus explota una vulnerabilidad de seguridad rastreada como

CVE-2022-21894 (también conocida como Baton Drop) para eludir las protecciones de arranque seguro de UEFI y configurar la persistencia. Microsoft abordó la vulnerabilidad como parte de su actualización del martes de parches de enero de 2022.

Una explotación exitosa de la vulnerabilidad, según ESET, permite la ejecución de código arbitrario durante las primeras fases de arranque, lo que permite que un atacante realice acciones maliciosas en un sistema con UEFI Secure Boot habilitado sin tener acceso físico a él.

> *«Este es el primer abuso conocido públicamente de esta vulnerabilidad. Su explotación aún es posible ya que los binarios afectados y firmados válidamente aún no se han agregado a la lista de revocación de UEFI«,* dijo Martin Smolár, investigador de ESET.

«BlackLotus aprovecha esto, trayendo sus propias copias de binarios legítimos, pero vulnerables, al sistema para explotar la vulnerabilidad», allanando efectivamente el camino para los ataques BYOVD (Bring Your Own Vulnerable Driver).

Además de estar equipado para desactivar mecanismos de seguridad como BitLokcker, Hypervisor-protected Code Integrity (HVCI) y Windows Defender, también está diseñado para colocar un controlador de kernel y un descargador HTTP que se comunica con un servidor de comando y control (C2) para recuperar malware adicional en modo usuario o modo kernel.

El modus operandi exacto utilizado para implementar el kit de arranque aún se desconoce, pero comienza con un componente de instalación que es responsable de escribir los archivos en la partición del sistema EFI, deshabilitar HVCI y BitLocker, y después reiniciar el host.

El reinicio es seguido por la activación de CVE-2022-21894 para lograr la persistencia e instalar el kit de arranque, después de lo cual se ejecuta automáticamente en cada inicio del sistema para implementar el controlador del kernel.

Aunque el controlador tiene la tarea de iniciar el descargador HTTP en modo de usuario y ejecutar las cargas útiles en modo kernel de la próxima etapa, este último es capaz de ejecutar comandos recibidos del servidor C2 por medio de HTTPS.

Esto incluye descargar y ejecutar un controlador de kernel, DLL o un ejecutable regular, obteniendo actualizaciones de bootkit e incluso desinstalando el bootkit del sistema infectado.

> *«En los últimos años se han descubierto muchas vulnerabilidades críticas que afectan la seguridad de los sistemas UEFI. Desafortunadamente, debido a la complejidad de todo el ecosistema UEFI y los problemas relacionados con la cadena de suministro, muchas de estas vulnerabilidades han dejado a muchos sistemas vulnerables incluso mucho tiempo después de que se hayan solucionado las vulnerabilidades, o al menos después de que nos dijeron que se habían solucionado»,* dijo Smolár.

> *«Era solo cuestión de tiempo antes de que alguien aprovechara estas fallas y creara un kit de arranque UEFI capaz de operar en sistemas con UEFI Secure Boot habilitado».*