Investigadores en ciberseguridad han identificado una nueva cepa de ransomware llamada HybridPetya, que recuerda al famoso malware Petya/NotPetya, pero que además incorpora la capacidad de eludir el mecanismo Secure Boot en sistemas UEFI (Unified Extensible Firmware Interface) aprovechando una vulnerabilidad que fue corregida y divulgada a inicios de este año.

La firma eslovaca de ciberseguridad ESET indicó que las muestras fueron subidas a la plataforma VirusTotal en febrero de 2025.

"HybridPetya cifra la Master File Table, que contiene la metainformación de todos los archivos en particiones con formato NTFS," afirmó el investigador de seguridad Martin Smolár. *"A diferencia del Petya/NotPetya original, HybridPetya puede comprometer sistemas modernos basados en UEFI al instalar una aplicación EFI maliciosa en la partición del sistema EFI."*

En otras palabras, la aplicación UEFI desplegada es el componente central encargado de cifrar el archivo MFT (Master File Table), que reúne los metadatos de todos los archivos en la partición NTFS.

HybridPetya se compone de dos módulos principales: un bootkit y un instalador; el bootkit, a su vez, existe en dos variantes distintas. El bootkit que instala el instalador es el responsable principal de cargar su configuración y comprobar el estado del cifrado. Puede almacenar tres valores distintos:

0 — listo para cifrar
1 — ya cifrado
2 — rescate pagado, disco descifrado

Si el valor está en 0, lo cambia a 1 y procede a cifrar el archivo `\EFI\Microsoft\Boot\verify` usando el algoritmo Salsa20 con la clave y el nonce especificados en la configuración. Además, crea en la partición del sistema EFI un archivo llamado `\EFI\Microsoft\Boot\counter` antes de iniciar el proceso de cifrado de todos

los volúmenes con formato NTFS. Ese archivo sirve para llevar el conteo de los clústeres de disco que ya han sido cifrados.

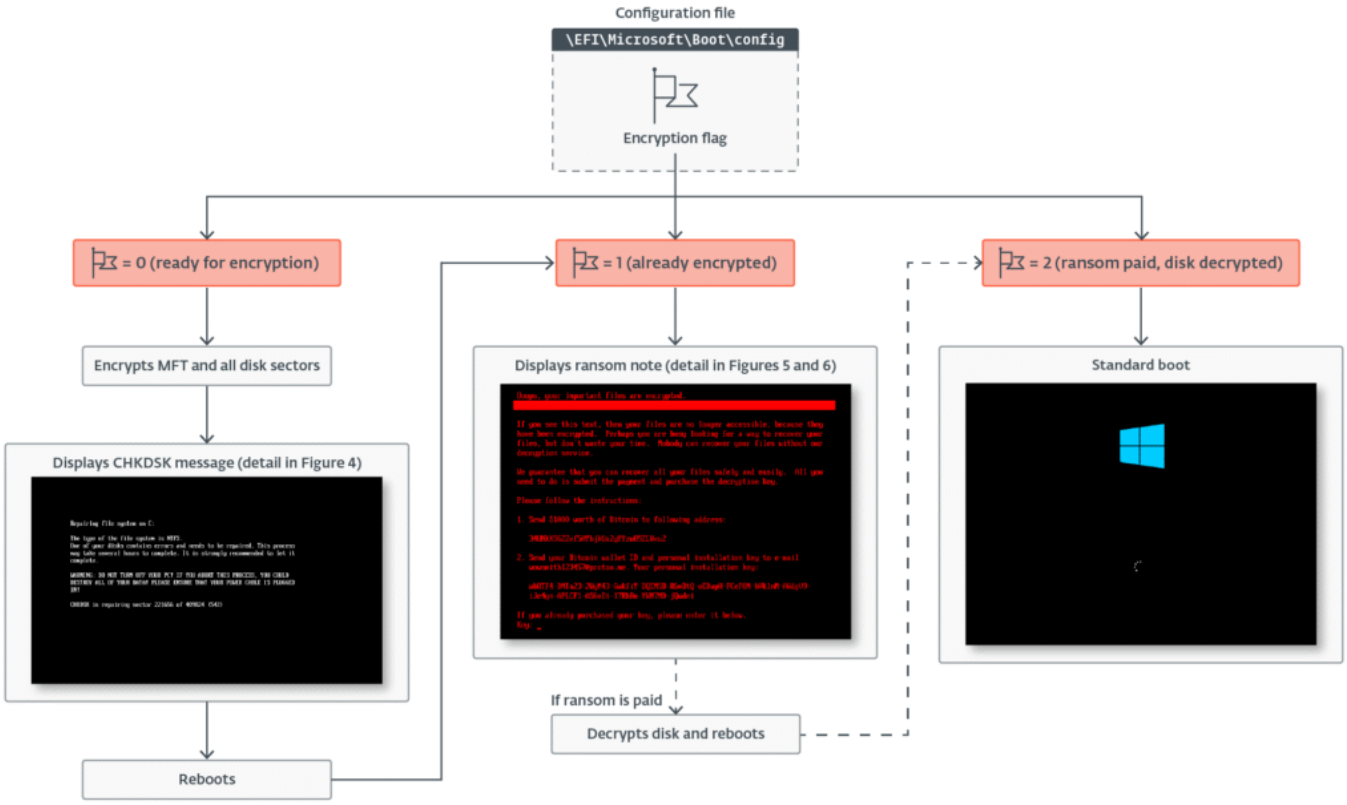
El bootkit también actualiza el mensaje falso de CHKDSK que aparece en pantalla para mostrar el estado actual del cifrado, mientras que la víctima es engañada creyendo que el sistema está reparando errores de disco.

Si el bootkit detecta que el disco ya está cifrado (es decir, el indicador está en 1), muestra una nota de rescate exigiendo que la víctima envíe $1,000 en Bitcoin a la dirección especificada (`34UNkKSGZZvf5AYbjkUa2yYYzw89ZLWxu2`). La billetera está vacía actualmente, aunque ha recibido $183.32 entre febrero y mayo de 2025.

La pantalla con la nota de rescate también ofrece una opción para que la víctima ingrese la clave de "desbloqueo" que habría comprado al operador tras realizar el pago; el bootkit verifica esa clave y trata de descifrar el archivo `EFI\Microsoft\Boot\verify`. Si se introduce la clave correcta, el indicador pasa a 2 y se inicia la fase de descifrado leyendo el contenido del archivo `\EFI\Microsoft\Boot\counter`.

"La descifrado se detiene cuando el número de clústeres descifrados es igual al valor del archivo counter," explicó Smolár. *"Durante la recuperación del MFT, el bootkit muestra el progreso actual del proceso de descifrado."*

La fase de descifrado también incluye que el bootkit restaura los cargadores de arranque legítimos —`\EFI\Boot\bootx64.efi` y `\EFI\Microsoft\Boot\bootmgfw.efi`— a partir de las copias de seguridad creadas durante la instalación. Completado ese paso, se solicita a la víctima reiniciar su equipo con Windows.



Conviene destacar que los cambios en el cargador de arranque realizados por el instalador al desplegar el componente bootkit UEFI provocan un fallo del sistema (conocido como pantalla azul o BSoD) y garantizan que el binario del bootkit se ejecute cuando el dispositivo arranque.

ESET agregó que ciertas variantes de HybridPetya han sido detectadas explotando CVE-2024-7344 (puntuación CVSS: 6.7), una vulnerabilidad de ejecución remota en la aplicación UEFI Howyar Reloader (`reloader.efi`, renombrada en el artefacto como `\EFI\Microsoft\Boot\bootmgfw.efi`) que podría permitir eludir Secure Boot.

El ejemplar también incluye un archivo especialmente creado llamado `cloak.dat`, que puede ser cargado por `reloader.efi` y contiene el binario del bootkit en XOR. Microsoft revocó desde entonces el binario antiguo y vulnerable como parte de su actualización de

Patch Tuesday de enero de 2025.

"Cuando el binario reloader.efi (desplegado como bootmgfw.efi) se ejecuta durante el arranque, busca la presencia del archivo cloak.dat en la partición del sistema EFI y carga la aplicación UEFI embebida desde ese archivo de una forma muy insegura, ignorando por completo cualquier verificación de integridad, con lo que se evade UEFI Secure Boot," afirmó ESET.

Otra diferencia entre HybridPetya y NotPetya es que, a diferencia de las capacidades destructivas de aquel, el nuevo artefacto permite a los atacantes reconstruir la clave de descifrado a partir de las claves de instalación personales de la víctima.

Los datos de telemetría de ESET no muestran evidencia de que HybridPetya se haya utilizado ampliamente en ataques reales. La compañía también señaló el reciente hallazgo por parte de la investigadora Aleksandra "Hasherezade" Doniec de una prueba de concepto (PoC) de Petya para UEFI, por lo que podría existir "alguna relación entre ambos casos." No obstante, ESET no descarta que HybridPetya pudiera ser también una PoC.

"HybridPetya es al menos el cuarto ejemplo público conocido de un bootkit UEFI real o de prueba de concepto con capacidad para eludir UEFI Secure Boot, uniéndose a BlackLotus (explotando CVE-2022-21894), BootKitty (explotando LogoFail) y al PoC Hyper-V Backdoor (explotando CVE-2020-26200)," dijo ESET.

"Esto demuestra que los bypass de Secure Boot no solo son posibles —se están volviendo más comunes y atractivos tanto para investigadores como para atacantes."

UEFI, sucesor del BIOS (Basic Input/Output System), es un objetivo valioso para los atacantes. Como UEFI se ejecuta antes del sistema operativo en el arranque, el malware capaz de infectar el proceso de arranque puede evadir el software de seguridad tradicional, ejecutar código con privilegios elevados y resultar extremadamente sigiloso y difícil de eliminar.

El descubrimiento de HybridPetya coincide con que el investigador Kazuki Matsuo de FFRI

Security describió una técnica llamada Shade BIOS que permite al malware operar totalmente ajeno a las medidas de seguridad a nivel de sistema operativo y realizar acciones maliciosas sin depender del hardware en tiempo de ejecución.

Se ha descrito como un malware "puro-BIOS" que permanece en memoria incluso después del arranque del SO, preservando funcionalidades UEFI y pudiendo usar drivers en tiempo de ejecución —lo que le da la capacidad de subvertir todo tipo de protecciones de ciberseguridad.

Shade BIOS *"separa el malware UEFI de la seguridad a nivel de sistema operativo,"* dijo Matsuo en una ponencia en Black Hat 2025 el mes pasado, y añadió que no necesita conocer el dispositivo objetivo ni implementar toda la pila de drivers o acceder directamente a I/O.