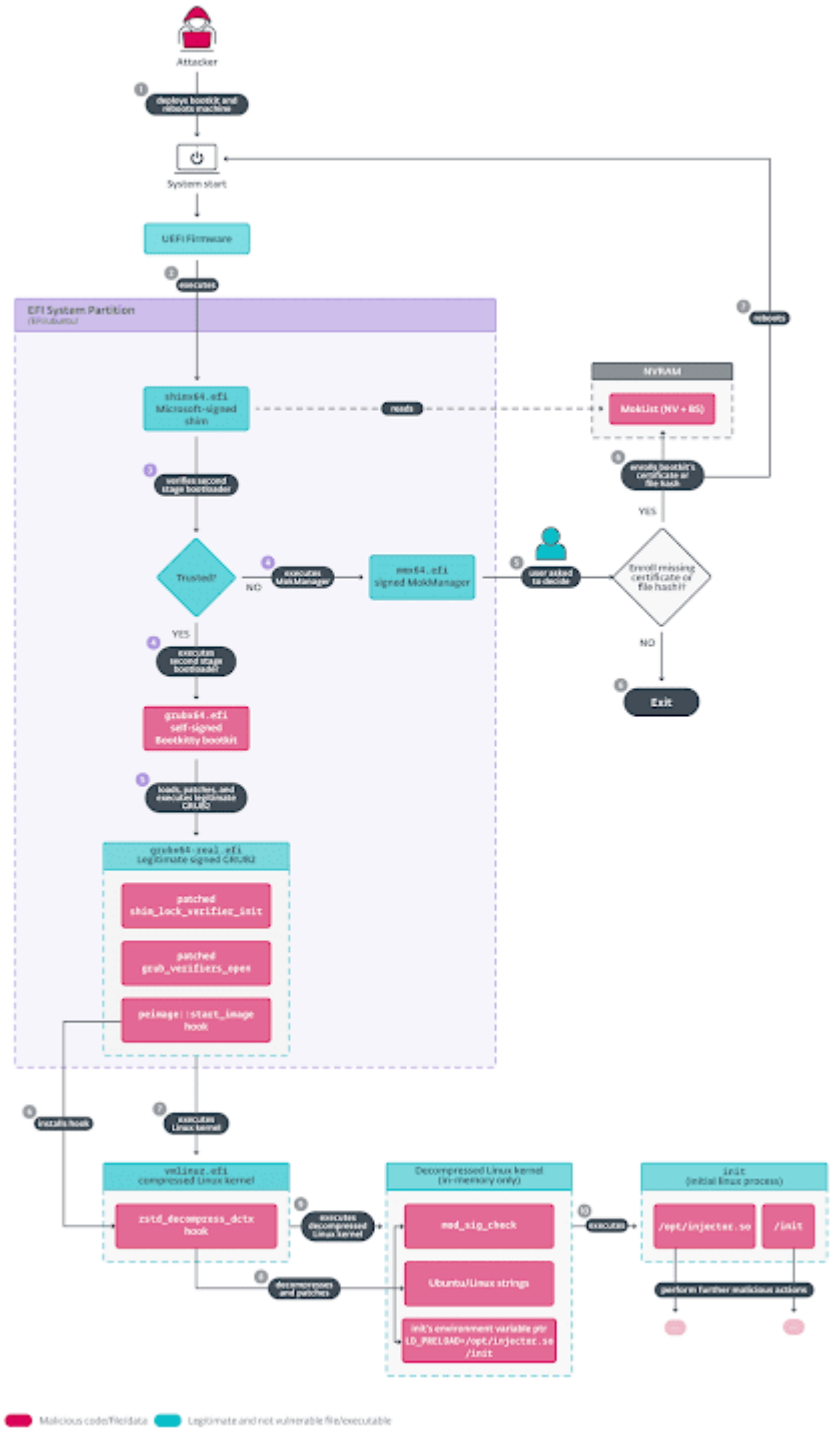
Investigadores en ciberseguridad han revelado detalles sobre lo que se considera el primer *bootkit* basado en la Interfaz Unificada Extensible de Firmware (UEFI) diseñado específicamente para sistemas Linux.

Conocido como Bootkitty, nombre dado por sus creadores identificados como BlackCat, este *bootkit* se considera un prototipo (*proof-of-concept*, PoC) y no existen indicios de que haya sido utilizado en ataques reales. También llamado IranuKit, fue subido a la plataforma VirusTotal el 5 de noviembre de 2024.

> *"El propósito principal del bootkit es desactivar la función de verificación de firmas del kernel y precargar dos binarios ELF desconocidos a través del proceso de inicialización de Linux (el primer proceso que ejecuta el kernel durante el arranque)",* explicaron Martin Smolár y Peter Stýrček, investigadores de ESET.

Este desarrollo es relevante porque representa un cambio en el panorama de amenazas cibernéticas, demostrando que los *bootkits* UEFI no se limitan exclusivamente a sistemas Windows.

Cabe destacar que Bootkitty utiliza un certificado autofirmado, lo que significa que no puede ejecutarse en sistemas con UEFI Secure Boot activado, salvo que previamente se haya instalado un certificado manipulado por un atacante.


Attacker
deploys bootkit and reboots machine
System start
UEFI Firmware
executes
EFI System Partition
shim64.efi
Microsoft-signed shim
reads
NVRAM
MokList (MV + BS)
verifies second stage bootloader
Trusted?
NO
executes MokManager
mm64.efi
signed MokManager
user asked to decide
Enroll missing certificate or file hash!?
YES
NO
Exit
executes second stage bootloader
grubx64.efi
self-signed
Bootkitty bootkit
loads, patches, and executes legitimate GRUB2
grubx64.real.efi
Legitimate signed GRUB2
patched shim_lock_verifier_init
patched grub_verifiers_open
peimage::start_image hook
installs hook
executes Linux kernel
vmlinuz.efi
compressed Linux kernel
zstd_decompress_dctx hook
executes decompressed Linux kernel
decompresses and patches
Decompressed Linux kernel
(in-memory only)
mod_sig_check
Ubuntu/Linux strings
init's environment variable ptr LD_PRELOAD=/opt/injector.so /init
executes
init
(initial linux process)
/opt/injector.so
/init
perform further malicious actions
Malicious code/file/data
Legitimate and not vulnerable file/executable

Con independencia del estado de UEFI Secure Boot, el diseño del *bootkit* permite arrancar el kernel de Linux y modificar en memoria las respuestas de las funciones de verificación de integridad antes de que se ejecute el gestor de arranque GRUB (*GNU GRand Unified Bootloader*).

En particular, si Secure Boot está habilitado, el *bootkit* interviene dos funciones de los protocolos de autenticación de UEFI para sortear las comprobaciones de integridad. Después, también modifica tres funciones del cargador GRUB legítimo para evitar otras verificaciones de seguridad.

La empresa eslovaca de ciberseguridad ESET informó que, durante la investigación del *bootkit*, se descubrió un módulo de kernel sin firmar que podría estar relacionado. Este módulo es capaz de desplegar un binario ELF llamado BCDropper, que carga un segundo módulo de kernel aún desconocido tras el inicio del sistema.

El módulo de kernel, que también utiliza BlackCat como autor, incluye funciones típicas de un *rootkit*, como ocultar archivos, procesos y habilitar la apertura de puertos. Hasta ahora, no se ha encontrado evidencia de vínculos con el grupo de ransomware ALPHV/BlackCat.

> *"Aunque se trate de un prototipo, Bootkitty supone un avance notable en las amenazas UEFI, desafiando la idea de que los bootkits modernos de UEFI son exclusivos de Windows",* destacaron los investigadores. Además, subrayaron la importancia de estar preparados para posibles amenazas futuras.