Se ha detectado una brecha en la política de Microsoft Windows que está siendo aprovechada principalmente por actores de amenazas que hablan chino nativo para falsificar firmas en controladores de modo kernel.

Según un informe exhaustivo en dos partes por Cisco Talos, los actores están utilizando múltiples herramientas de código abierto que modifican la fecha de firma de los controladores de modo kernel para cargar controladores maliciosos y no verificados que están firmados con certificados caducados. Esta es una amenaza importante, ya que el acceso al kernel proporciona acceso completo a un sistema y, por lo tanto, compromete por completo el sistema.

Después de una divulgación responsable, Microsoft informó que ha tomado medidas para bloquear todos los certificados y mitigar la amenaza. Además, afirmó que su investigación reveló que *«la actividad se limitaba al abuso de varias cuentas de programas de desarrollo y no se ha identificado ninguna violación de cuentas de Microsoft».*

Además de suspender las cuentas de programas de desarrollo involucradas en el incidente, la empresa tecnológica destacó que los actores de amenazas ya habían obtenido privilegios administrativos en los sistemas comprometidos antes de utilizar los controladores.

Es importante señalar que el fabricante de Windows ya había implementado protecciones similares en diciembre de 2022 para evitar que los atacantes de ransomware utilicen controladores firmados por Microsoft para actividades posteriores a la explotación.

La aplicación de la firma del controlador, que requiere que los controladores de modo kernel estén firmados digitalmente con un certificado del Portal de Desarrollo de Microsoft, es una línea de defensa crucial contra controladores maliciosos que podrían potencialmente evadir soluciones de seguridad, alterar los procesos del sistema y mantener la persistencia.

La nueva vulnerabilidad descubierta por Cisco Talos permite falsificar firmas en controladores de modo kernel, lo que permite eludir las políticas de certificados de Windows.

Esto es posible gracias a una excepción establecida por Microsoft para mantener la compatibilidad, que permite controladores con firma cruzada si están *«firmados con un certificado de entidad final emitido antes del 29 de julio de 2015 que esté encadenado a una autoridad de certificación cruzada compatible»*.

> *«La tercera excepción crea una laguna que permite que un controlador recién compilado se firme con certificados no revocados emitidos antes o que hayan caducado antes del 29 de julio de 2015, siempre que la cadena de certificados esté encadenada a una autoridad de certificación cruzada compatible»,* explicó la empresa de ciberseguridad.

Como resultado, un controlador firmado de esta manera no se impedirá su carga en un dispositivo con Windows, lo que permite a los actores de amenazas aprovechar la cláusula de escape para implementar miles de controladores maliciosos firmados sin someterlos a la verificación de Microsoft.

Estos controladores maliciosos se implementan utilizando software de falsificación de marcas de tiempo de firma, como HookSignTool y FuckCertVerifyTimeValidity, que han estado disponibles públicamente desde 2019 y 2018, respectivamente.

HookSignTool ha estado accesible a través de GitHub desde el 7 de enero de 2020, mientras que FuckCertVerifyTimeValidity fue añadido por primera vez al servicio de alojamiento de código el 14 de diciembre de 2018.

> *«HookSignTool es una herramienta de falsificación de firmas de controladores que modifica la fecha de firma de un controlador durante el proceso de firmado mediante una combinación de interceptación de la API de Windows y la alteración manual de la tabla de importación de una herramienta legítima de firmado de código»*, explicó Cisco Talos.

Específicamente, implica la intercepción de la función CertVerifyTimeValidity, que verifica la validez temporal de un certificado, para cambiar la marca de tiempo de firmado durante la ejecución.

> *«Este pequeño proyecto evita que el signtool verifique la validez temporal del certificado y te permite firmar tu archivo binario con un certificado desactualizado sin tener que modificar manualmente la hora del sistema»,* se lee en la página de GitHub de FuckCertVerifyTimeValidity.

> *«HookSignTool instala un gancho en crypt32!CertVerifyTimeValidity y hace que siempre devuelva 0, y hace que kernel32!GetLocalTime devuelva lo que quieras, ya que puedes agregar '-fuckyear 2011' a la línea de comando de signtool para firmar un certificado del año 2011».*

> *«HookSignTool es una herramienta de falsificación de firmas de controladores que modifica la fecha de firma de un controlador durante el proceso de firma al interceptar la función de verificación de validez temporal del certificado (CertVerifyTimeValidity) de crypt32. Esto se logra mediante la combinación de técnicas de enganche en la API de Windows y la alteración manual de la tabla de importación de una herramienta legítima de firmado de código»,* explicó Cisco Talos.

Específicamente, la herramienta realiza un enganche en la función CertVerifyTimeValidity, encargada de verificar la validez temporal de un certificado, para cambiar la marca de tiempo de firma durante la ejecución.

Dicho esto, llevar a cabo una falsificación exitosa requiere contar con un certificado de firma de código no revocado que haya sido emitido antes del 29 de julio de 2015, junto con la clave

privada y la frase de contraseña del certificado.

Cisco Talos informó haber descubierto más de una docena de certificados de firma de código con claves y contraseñas contenidas en un archivo PFX alojado en GitHub, en un repositorio bifurcado de FuckCertVerifyTimeValidity. No está claro de inmediato cómo se obtuvieron estos certificados.

Además, se ha observado que HookSignTool se ha utilizado para volver a firmar controladores crackeados con el objetivo de eludir las comprobaciones de integridad de la administración de derechos digitales (DRM). Por ejemplo, el actor llamado «Juno_Jr» publicó una versión crackeada de PrimoCache, una solución legítima de almacenamiento en caché de software, en un foro chino de cracking de software el 9 de noviembre de 2022.

En esta versión crackeada, el controlador parcheado se volvió a firmar con un certificado originalmente emitido a *'Shenzhen Luyoudashi Technology Co., Ltd.'*, el cual se encontraba en el archivo PFX alojado en GitHub. Esta capacidad de volver a firmar un controlador crackeado elimina un obstáculo significativo al intentar eludir las comprobaciones de DRM en un controlador firmado.

Pero eso no es todo. También se utiliza HookSignTool en un controlador previamente no documentado llamado RedDriver, el cual falsifica la marca de tiempo de su firma. Activo desde al menos 2021, RedDriver funciona como un secuestrador de navegador basado en controladores, que aprovecha la Plataforma de Filtrado de Windows (WFP) para interceptar el tráfico del navegador y redirigirlo a localhost (127.0.0.1).

El navegador objetivo se elige al azar de una lista codificada que contiene los nombres de proceso de muchos navegadores populares en idioma chino, como Liebao, QQ Browser, Sogou y UC Browser, así como Google Chrome, Microsoft Edge y Mozilla Firefox.

> *«Inicialmente encontré RedDriver mientras investigaba la falsificación de marcas de tiempo de certificados en controladores de Windows. Fue una de las primeras*

> *muestras que me pareció sospechosa de inmediato. Lo que llamó mi atención fue la lista de navegadores web almacenada en el archivo de RedDriver»,* comentó Chris Neal, investigador de divulgación de Cisco Talos

El objetivo final de esta redirección del tráfico del navegador no está claro, aunque es evidente que esta capacidad podría ser abusada para manipular el tráfico del navegador a nivel de paquetes.

Las cadenas de infección de RedDriver comienzan con la ejecución de un archivo binario llamado «DnfClientShell32.exe», el cual establece comunicaciones cifradas con un servidor de comando y control (C2) para descargar el controlador malicioso.

> *«No observamos la entrega del archivo inicial, pero es muy probable que el archivo se haya empaquetado para hacerse pasar por un archivo de juego, y que se haya alojado en un enlace de descarga malicioso. Es probable que la víctima haya pensado que estaba descargando un archivo de una fuente legítima y haya ejecutado el archivo. 'DNFClient' es el nombre de un archivo que pertenece a 'Dungeon Fighter Online', que es un juego extremadamente popular en China y comúnmente conocido como 'DNF'»,* mencionó Neal.

> *«Es probable que RedDriver haya sido desarrollado por actores de amenazas altamente capacitados, ya que el proceso de desarrollo de controladores maliciosos requiere un alto nivel de conocimiento y experiencia. Si bien la amenaza parece dirigirse a hablantes nativos de chino, es probable que los autores también sean hablantes de chino».*

> *«Los autores también demostraron un conocimiento o experiencia en los ciclos de vida del desarrollo de software, lo cual implica que han tenido experiencia previa en*

> *el desarrollo de software».*