Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

SILVER FOX EXPLOTA CONTROLADORES FIRMADOS PARA DISTRIBUIR EL MALWARE VALLEYRAT

01/ 09 / 2025

CONTENIDO

INTRODUCCIÓN

El grupo Silver Fox APT, también conocido como Void Arachne, ha lanzado una campaña sofisticada que explota un controlador legítimo firmado por Microsoft para deshabilitar herramientas de seguridad internas y desplegar el RAT ValleyRAT en sistemas Windows modernos.

SILVER FOX EXPLOTA CONTROLADORES FIRMADOS PARA DISTRIBUIR EL MALWARE VALLEYRAT

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_09_01_3
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	01/09/2025
Es día cero (0 day):	No

RESUMEN

El grupo Silver Fox APT, también conocido como Void Arachne, ha lanzado una campaña sofisticada que explota un controlador legítimo firmado por Microsoft para deshabilitar herramientas de seguridad internas y desplegar el RAT ValleyRAT en sistemas Windows modernos.

Contexto estratégico

Silver Fox es un grupo de ciberespionaje con vínculos a China, activo desde 2024. Se especializa en ataques dirigidos y se le atribuye la distribución de ValleyRAT a través de:

- Instaladores troyanizados (por ejemplo, visores DICOM de Philips o herramientas comunes).
- Vectores como phishing dirigido, envenenamiento de SEO y aplicaciones engañosas.

¿Cómo funciona el ataque?

El ataque se basa en el controlador amsdk.sys (WatchDog Antimalware, versión 1.0.600). Aunque está firmado por Microsoft y no estaba en las listas de bloqueo de vulnerabilidades conocidas, los atacantes lo utilizaron para evadir la protección de Windows Defender y otras soluciones de seguridad avanzadas.

1. Enfoque de doble driver: Para asegurar la compatibilidad tanto en Windows 7 como en Windows 10/11, Silver Fox dividió la carga útil en dos drivers: uno conocido y bloqueado en sistemas antiguos, y el otro (amsdk.sys) para entornos modernos, que no era detectado. Ambos fueron empaquetados en un loader único con técnicas anti-análisis.
2. Evasión de firmas: El proveedor lanzó un parche (wamsdk.sys v1.1.100), pero Silver Fox lo evadió utilizando una versión modificada del driver con un solo byte cambiado en el campo de marca de tiempo no autenticado. Esto mantuvo la firma como válida y eludió los mecanismos de detección basados en hash.
3. Despliegue de ValleyRAT: Una vez que las defensas fueron desactivadas, el loader desplegó ValleyRAT, una puerta trasera modular que permite la vigilancia remota, la ejecución de comandos y la exfiltración de datos, con una infraestructura vinculada directamente a Silver Fox.

Esta campaña de driver firmado representa una nueva fase en su arsenal ofensivo, elevando significativamente su capacidad de sigilo y evasión.

RECOMENDACIONES

- Añade amsdk.sys v1.0.600 a la lista de bloqueo local de tu sistema, incluso si parece un archivo legítimo.
- Utiliza soluciones que detecten comportamiento anómalo, como la inyección en memoria o el lanzamiento de ValleyRAT.
- Activa alertas que te notifiquen sobre cambios en servicios o procesos deshabilitados por los drivers.
- Aísla los endpoints sensibles para reducir el impacto de posibles infecciones.
- Usa plataformas de emulación para probar las tácticas de Silver Fox y evaluar la efectividad de tus controles de seguridad.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/5232d870038483453b117417e07157d825287f6a/20250901_01_Silverfox

NOTICIA COMPLETA

https://devel.group/blog/silver-fox-explota-controladores-firmados-para-distribuir-el-malware-valleyrat/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group