El actor de amenazas conocido como Silver Fox ha sido vinculado al uso indebido de un controlador vulnerable previamente desconocido asociado con WatchDog Anti-malware, como parte de un ataque de tipo *Bring Your Own Vulnerable Driver* (BYOVD), con el propósito de desactivar soluciones de seguridad instaladas en equipos comprometidos.

El controlador vulnerable en cuestión es "amsdk.sys" (versión 1.0.600), un driver de kernel de Windows de 64 bits, firmado de manera legítima, que se considera desarrollado a partir del SDK de Zemana Anti-Malware.

"Este controlador, creado sobre el SDK de Zemana Anti-Malware, estaba firmado por Microsoft, no figuraba en la lista de controladores vulnerables bloqueados por Microsoft y tampoco fue identificado por proyectos comunitarios como LOLDrivers", explicó Check Point en su análisis.

El ataque se caracteriza por una estrategia de doble controlador, donde un driver vulnerable conocido de Zemana ("zam.exe") se emplea en equipos con Windows 7, mientras que el controlador no detectado de WatchDog se utiliza en sistemas que operan con Windows 10 o 11.

El driver de WatchDog Anti-malware contiene varias fallas, siendo la principal su capacidad de finalizar procesos arbitrarios sin comprobar si estos están protegidos (PP/PPL). También es susceptible a escaladas de privilegios locales, lo que permite al atacante obtener acceso sin restricciones al dispositivo del controlador.

El objetivo final de la campaña, identificada por primera vez por Check Point a finales de mayo de 2025, es aprovechar estos controladores vulnerables para neutralizar las soluciones de protección en los endpoints, despejando el camino para la instalación y persistencia de malware sin activar defensas basadas en firmas.

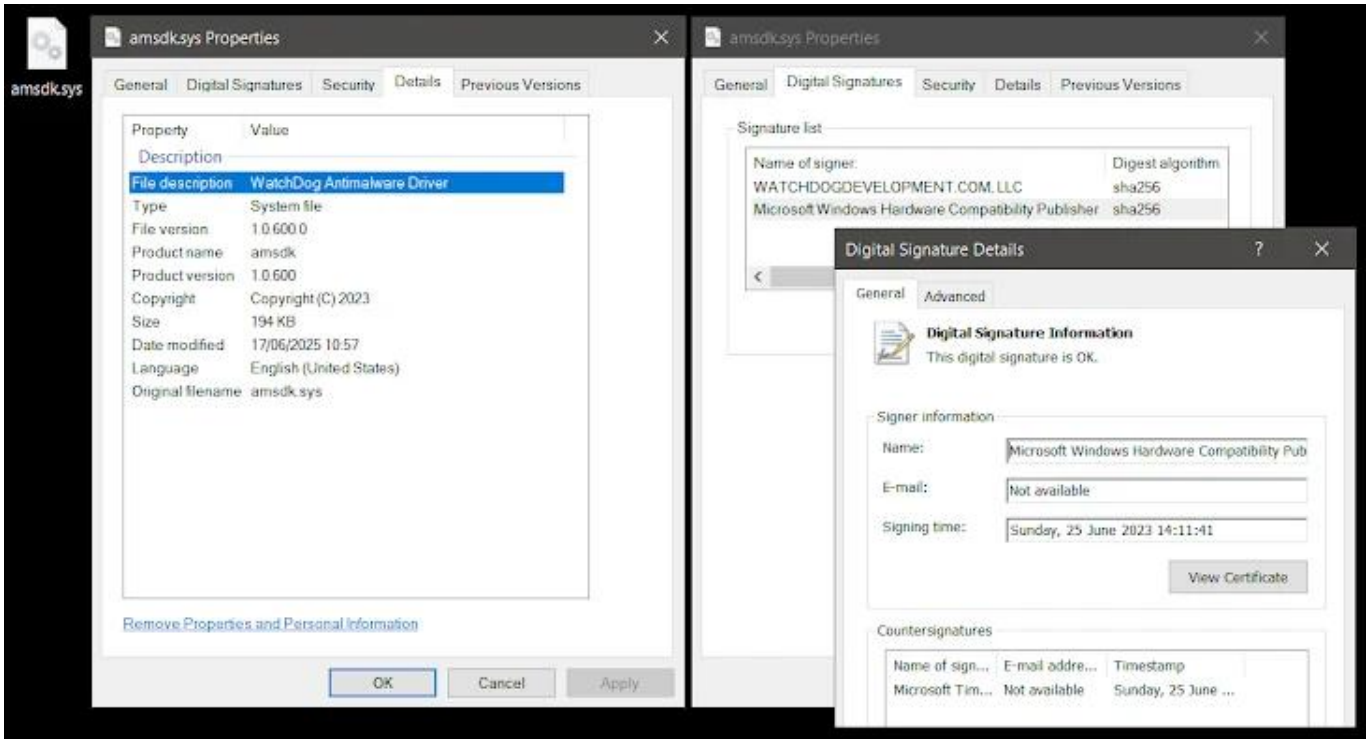
Como se ha observado previamente, la campaña está diseñada para desplegar ValleyRAT (también llamado Winos 4.0) como carga final, otorgando al actor de amenazas capacidades de control y acceso remoto. La compañía de ciberseguridad señaló que los ataques utilizan

un *loader* todo en uno, que integra funciones anti-análisis, dos drivers embebidos, lógica para deshabilitar antivirus y el *downloader* de la DLL de ValleyRAT en un único binario.

"Al ejecutarse, la muestra realiza varias comprobaciones comunes de anti-análisis, como Anti-VM (detección de entornos virtuales), Anti-Sandbox (detección de ejecución en un sandbox), detección de hipervisores, entre otras", indicó Check Point. *"Si alguna de estas comprobaciones falla, la ejecución se detiene y se muestra un falso mensaje de error del sistema"*.

El *downloader* está diseñado para comunicarse con un servidor de comando y control (C2) con el fin de descargar el *backdoor* modular ValleyRAT en la máquina infectada.

Tras una divulgación responsable, WatchDog liberó un parche (versión 1.1.100) para mitigar el riesgo de LPE mediante la aplicación de una DACL robusta, aunque sin solucionar la vulnerabilidad de finalización arbitraria de procesos. Como consecuencia, los atacantes se adaptaron rápidamente e incorporaron la versión modificada alterando un solo byte, sin invalidar la firma de Microsoft.



"Con solo cambiar un byte en el campo de marca de tiempo no autenticado, conservaron la firma válida de Microsoft mientras generaban un nuevo hash de archivo, evadiendo de manera efectiva las listas de bloqueo basadas en hash", destacó Check Point. *"Esta técnica de evasión, sutil pero efectiva, refleja patrones observados en campañas anteriores"*.

"Esta campaña demuestra cómo los actores de amenazas están superando debilidades conocidas para convertir en armas controladores firmados pero vulnerables y previamente no clasificados —un punto ciego para muchos mecanismos de defensa. La explotación de un controlador firmado por Microsoft y combinado con técnicas de evasión como la manipulación de firmas representa una amenaza sofisticada y en evolución".

Silver Fox, también llamado SwimSnake, The Great Thief of Valley (o Valley Thief), UTG-Q-1000 y Void Arachne, ha estado muy activo desde principios del año pasado, enfocándose principalmente en víctimas de habla china mediante sitios falsos que simulan ser Google Chrome, Telegram y herramientas con inteligencia artificial (IA) como DeepSeek, para

distribuir troyanos de acceso remoto como ValleyRAT.

Según el proveedor chino de ciberseguridad Antiy, se cree que este grupo existe desde la segunda mitad de 2022, con el objetivo de atacar a usuarios y empresas locales para robar información y cometer fraudes.

"El grupo criminal difunde principalmente archivos maliciosos a través de programas de mensajería instantánea (WeChat, Enterprise WeChat, etc.), promoción SEO en buscadores, correos de phishing, entre otros", señaló la empresa. *"El grupo cibercriminal 'SwimSnake' continúa actualizando con frecuencia tanto el malware como los métodos de evasión frente a antivirus"*.

Los ataques hacen uso de versiones troyanizadas de software de código abierto, programas maliciosos creados con el framework Qt o instaladores MSI disfrazados de Youdao, Sogou AI, WPS Office y DeepSeek para distribuir ValleyRAT, incluyendo su módulo en línea capaz de capturar pantallazos de WeChat y de bancos en línea.

Paralelamente, QiAnXin detalló otra campaña llevada a cabo por el *"Finance Group"*, una subdivisión de Silver Fox, que apunta a personal financiero y directivos de empresas e instituciones con el fin de robar información sensible o beneficiarse directamente mediante fraudes.

Estos ataques aprovechan señuelos de phishing relacionados con auditorías fiscales, facturas electrónicas, anuncios de subsidios y transferencias de personal, para engañar a los usuarios y que ejecuten troyanos de acceso remoto, mientras alojan las cargas maliciosas en servicios legítimos en la nube como Alibaba Cloud OSS y Youdao Cloud Notes para intentar evadir la detección.

El *Finance Group* es uno de los cuatro subgrupos que forman parte de Silver Fox; los otros tres son el *News and Romance Group*, el *Design and Manufacturing Group* y el *Black Watering Hole Group*.

De manera particular, tras tomar control de un equipo mediante ataques de tipo *watering hole* y phishing, el *Finance Group* accede a las cuentas de redes sociales de la víctima y las utiliza para enviar códigos QR de phishing a distintos grupos de WeChat, con la finalidad de recolectar números de cuentas bancarias y contraseñas, drenando finalmente los fondos para obtener ganancias.

"UTG-Q-1000 es uno de los grupos de ciberdelincuencia más activos y agresivos en China en los últimos años. Sus operaciones están altamente organizadas, son técnicamente sofisticadas y motivadas por fines financieros", aseguró QiAnXin. *"Han establecido una cadena de beneficios en el mercado negro que incluye: espionaje (robo de datos), control remoto mediante malware y fraude financiero con phishing"*.