Sitios web fraudulentos que promocionan Google Chrome han sido utilizados como señuelo para distribuir instaladores maliciosos que instalan un troyano de acceso remoto conocido como ValleyRAT.

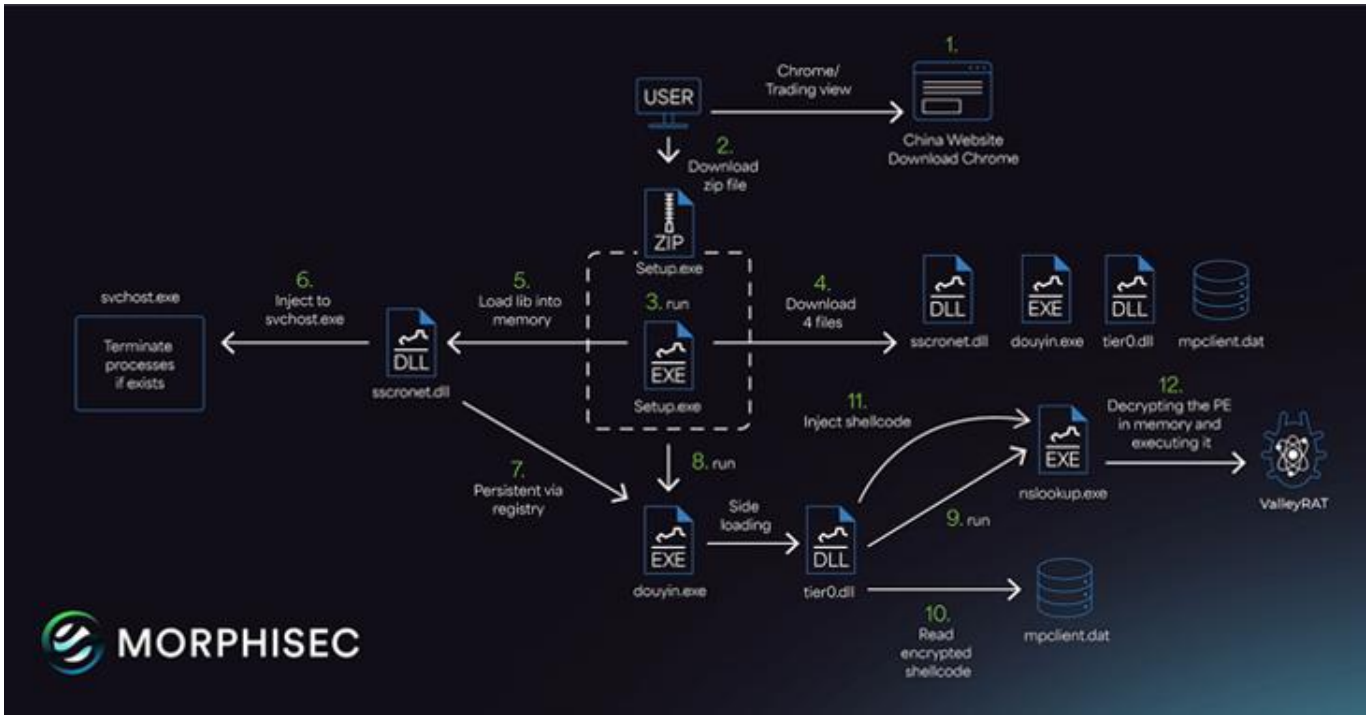
Este software malicioso, detectado inicialmente en 2023, ha sido atribuido a un grupo de amenazas identificado como Silver Fox, cuyas operaciones previas han tenido como objetivo principal regiones de habla china, incluyendo Hong Kong, Taiwán y China continental.

> *«Este grupo ha centrado su atención en roles estratégicos dentro de las empresas, particularmente en áreas como finanzas, contabilidad y ventas, lo que indica un enfoque en posiciones clave con acceso a información y sistemas sensibles»,* explicó Shmuel Uzan, investigador de Morphisec, en un informe reciente.

Las primeras fases de estos ataques han incluido la entrega de ValleyRAT junto con otros tipos de malware, como Purple Fox y Gh0st RAT, este último ampliamente empleado por diversos grupos de cibercriminales chinos.

Hasta el mes pasado, instaladores fraudulentos de programas legítimos han servido como método de distribución del troyano mediante el uso de un cargador de DLL denominado PNGPlug.

Es importante señalar que en el pasado se utilizó una táctica similar dirigida a usuarios de Windows de habla china, en la que Gh0st RAT se propagaba a través de paquetes de instalación alterados del navegador Chrome.



Siguiendo un patrón similar, el ataque más reciente vinculado a ValleyRAT involucra un sitio web falso de Google Chrome que persuade a las víctimas para que descarguen un archivo ZIP con un ejecutable denominado «Setup.exe».

Al ejecutarse, este archivo verifica si cuenta con privilegios administrativos y, de ser así, procede a descargar cuatro componentes adicionales, entre ellos, un ejecutable legítimo de Douyin («Douyin.exe»), la versión china de TikTok, el cual se utiliza para cargar de manera encubierta una DLL maliciosa («tier0.dll») que inicia el troyano ValleyRAT.

Otro archivo DLL («sscronet.dll») también se descarga, cuya función es finalizar procesos en ejecución que figuren en una lista de exclusión.

Desarrollado en C++ y con instrucciones en chino, ValleyRAT está diseñado para registrar lo que aparece en pantalla, capturar las pulsaciones del teclado y mantenerse activo en el sistema comprometido. Además, puede establecer comunicación con un servidor remoto para recibir órdenes adicionales, lo que le permite inspeccionar procesos activos, descargar y

ejecutar archivos DLL o binarios arbitrarios, entre otras acciones maliciosas.

> *«Para introducir sus cargas maliciosas, los atacantes aprovecharon ejecutables legítimos con firmas digitales válidas, pero vulnerables a la manipulación del orden de búsqueda de DLLs»,* indicó Uzan.

Este hallazgo coincide con el informe de Sophos sobre ataques de phishing que utilizan archivos en formato Scalable Vector Graphics (SVG) para evitar ser detectados y distribuir registradores de teclas basados en AutoIt, como Nymeria, o redirigir a los usuarios a sitios fraudulentos diseñados para robar credenciales.