Investigadores de ciberseguridad han identificado un nuevo malware llamado PLAYFULGHOST, que posee múltiples capacidades de recolección de información, como el registro de teclas, captura de pantalla y audio, acceso remoto a la línea de comandos, transferencia de archivos y ejecución de comandos.

El equipo de Google Managed Defense señaló que este backdoor comparte varias características con Gh0st RAT, una herramienta de administración remota cuyo código fuente fue filtrado públicamente en 2008.

PLAYFULGHOST puede infectar sistemas a través de diferentes métodos iniciales, incluyendo correos electrónicos de phishing con temas relacionados con códigos de conducta o el uso de técnicas de manipulación de resultados de motores de búsqueda (SEO) para distribuir versiones alteradas de aplicaciones VPN legítimas como LetsVPN.

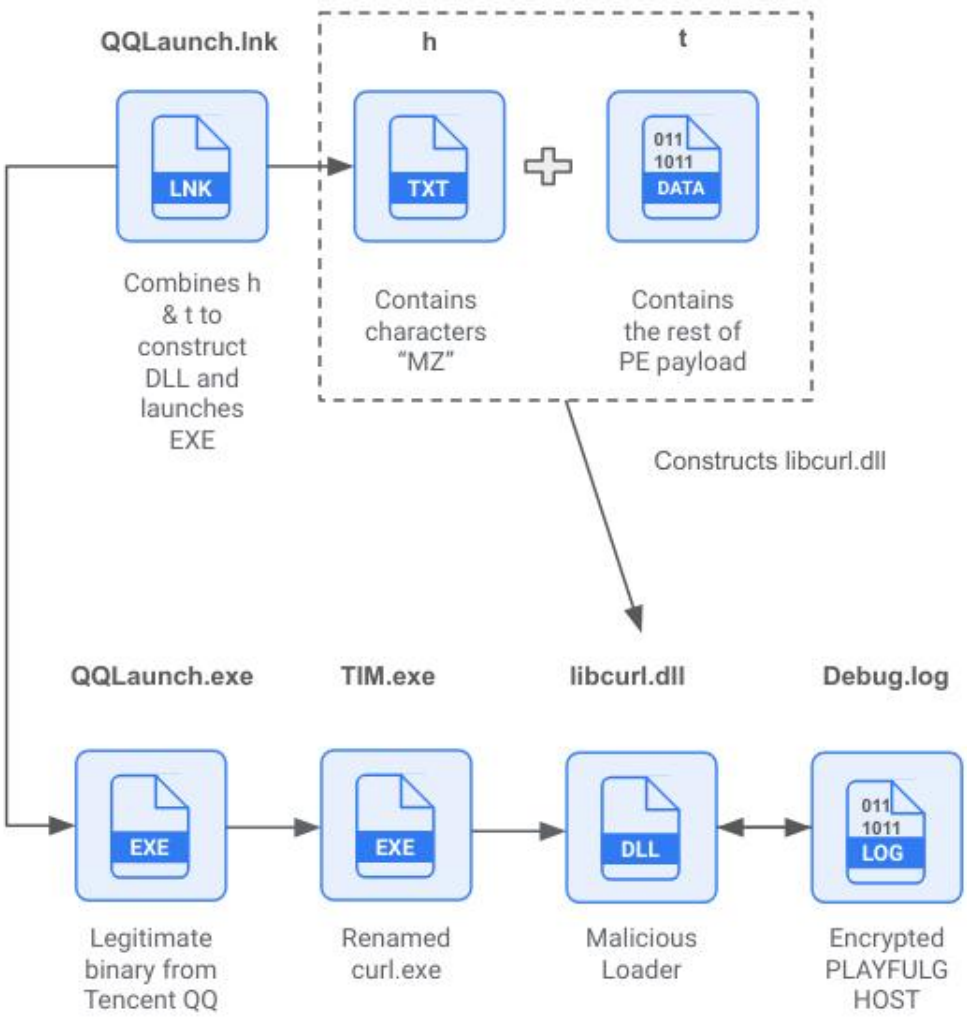
> *«En un caso de phishing, el ataque comienza al engañar a la víctima para que abra un archivo RAR malicioso disfrazado como una imagen con la extensión .jpg. Cuando se extrae y ejecuta, el archivo deja caer un ejecutable malicioso de Windows que finalmente descarga y ejecuta PLAYFULGHOST desde un servidor remoto»*, explicó la compañía.

En los ataques que utilizan envenenamiento SEO, el objetivo es persuadir a los usuarios para que descarguen instaladores infectados de LetsVPN. Una vez ejecutados, estos instaladores despliegan un payload intermedio encargado de recuperar los archivos necesarios para el backdoor.

Lo que hace única a esta infección es el uso de técnicas avanzadas como el secuestro del orden de búsqueda de DLL y la carga lateral de archivos maliciosos, los cuales descifran y cargan PLAYFULGHOST directamente en la memoria del sistema.

Además, Mandiant observó un método más complejo de ejecución en el que un archivo de acceso directo de Windows (QQLaunch.lnk) combina información de otros archivos

denominados «h» y «t» para generar una DLL maliciosa que luego se carga utilizando una versión renombrada de «curl.exe».



El malware es capaz de mantener persistencia en el sistema mediante cuatro estrategias principales: claves de registro Run, tareas programadas, la carpeta de inicio de Windows y la creación de servicios. Entre sus funciones avanzadas, destaca su capacidad para recopilar datos como pulsaciones de teclado, capturas de pantalla, grabaciones de audio, información de cuentas de QQ, programas de seguridad instalados, contenido del portapapeles y detalles

del sistema.

Además, puede desplegar más cargas maliciosas, bloquear la entrada de dispositivos periféricos, borrar registros de eventos de Windows, eliminar datos del portapapeles, manipular archivos, y eliminar perfiles y cachés de navegadores como Sogou, QQ, 360 Safety, Firefox y Google Chrome. También puede eliminar perfiles y datos locales de aplicaciones de mensajería como Skype, Telegram y QQ.

El malware también incluye herramientas adicionales como Mimikatz y un rootkit diseñado para ocultar registros, archivos y procesos especificados por los atacantes. Junto con los componentes de PLAYFULGHOST, se distribuye una herramienta de código abierto llamada Terminator, que puede deshabilitar procesos de seguridad mediante un ataque de tipo Bring Your Own Vulnerable Driver (BYOVD).

> *«En una ocasión, Mandiant detectó un payload de PLAYFULGHOST integrado en BOOSTWAVE. BOOSTWAVE es un shellcode que funciona como un cargador en memoria para una carga ejecutable portátil (PE) adjunta»,* añadió la empresa.

El uso de aplicaciones como Sogou, QQ y 360 Safety, junto con los señuelos relacionados con LetsVPN, sugiere que estas campañas de malware están dirigidas principalmente a usuarios de habla china que utilizan sistemas Windows. En julio de 2024, la empresa canadiense de ciberseguridad eSentire reportó una campaña similar que usaba instaladores falsos de Google Chrome para distribuir Gh0st RAT mediante un dropper llamado Gh0stGambit.