Videos de YouTube que promocionan trampas para videojuegos están siendo utilizados para distribuir un malware de robo de información previamente desconocido llamado Arcane, el cual parece estar dirigido a usuarios de habla rusa.

Según un análisis de Kaspersky, *«lo intrigante de este malware es la cantidad de información que recopila».* Arcane extrae credenciales de cuentas de clientes de VPN y plataformas de juegos, así como datos de diversas herramientas de red como ngrok, Playit, Cyberduck, FileZilla y DynDNS.

El ataque se ejecuta a través de enlaces compartidos en videos de YouTube, que dirigen a los usuarios a un archivo comprimido protegido con contraseña. Al abrirlo, este descomprime un archivo por lotes (start.bat) que, mediante PowerShell, descarga otro archivo comprimido.

El script por lotes utiliza PowerShell para ejecutar dos archivos incrustados en el nuevo archivo descargado. Además, desactiva la protección de Windows SmartScreen y excluye las carpetas raíz de cada unidad del filtro de SmartScreen.

De los dos archivos ejecutables, uno es un minero de criptomonedas y el otro es un malware de robo de datos conocido como VGS, una variante de Phemedrone Stealer. Desde noviembre de 2024, los ataques han comenzado a reemplazar VGS con Arcane.

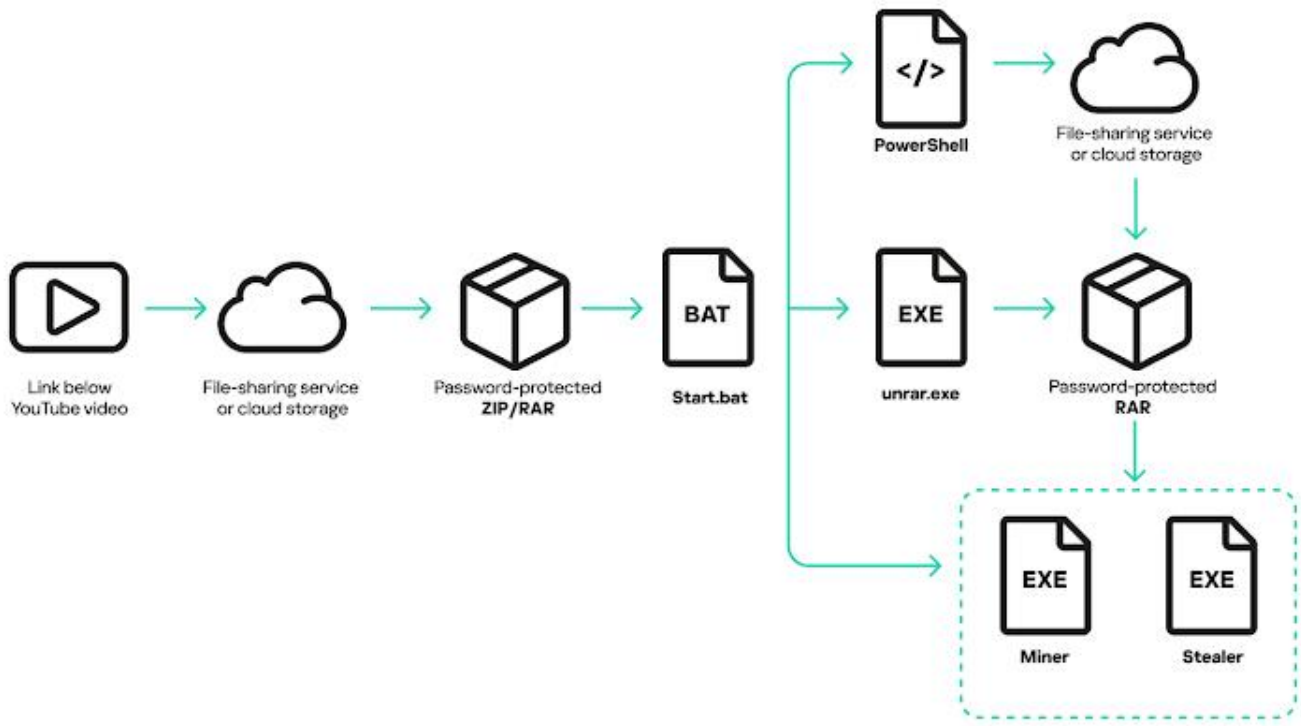
A pesar de que Arcane incorpora código de otros malware, los investigadores de Kaspersky no lograron vincularlo directamente con ninguna familia de malware conocida.

Información robada por Arcane

Arcane está diseñado para extraer credenciales, contraseñas, datos de tarjetas de crédito y cookies de navegadores basados en Chromium y Gecko. Además, recopila información del sistema y archivos de configuración de diversas aplicaciones, incluyendo:

- Clientes VPN: OpenVPN, Mullvad, NordVPN, IPVanish, Surfshark, Proton, hidemy.name, PIA, CyberGhost y ExpressVPN.

- Herramientas de red: ngrok, Playit, Cyberduck, FileZilla y DynDNS.
- Aplicaciones de mensajería: ICQ, Tox, Skype, Pidgin, Signal, Element, Discord, Telegram, Jabber y Viber.
- Clientes de correo: Microsoft Outlook.
- Plataformas de juegos: Riot Client, Epic Games, Steam, Ubisoft Connect (antes Uplay), Roblox, Battle.net y diversos clientes de Minecraft.
- Monederos de criptomonedas: Zcash, Armory, Bytecoin, Jaxx, Exodus, Ethereum, Electrum, Atomic, Guarda y Coinomi.



Métodos avanzados de extracción de datos

Arcane también es capaz de:

- Tomar capturas de pantalla del dispositivo infectado.
- Enumerar procesos en ejecución.
- Extraer información de redes Wi-Fi guardadas, incluyendo contraseñas.

Kaspersky destaca que los navegadores generan claves únicas para cifrar datos sensibles como contraseñas y cookies. Arcane utiliza la API de Protección de Datos (DPAPI) para obtener estas claves. Sin embargo, lo que lo hace más peligroso es que incorpora un archivo ejecutable de la herramienta Xaitax, diseñada para descifrar claves del navegador. Esta utilidad se ejecuta de manera oculta para extraer las claves necesarias.

Además, Arcane cuenta con un método específico para robar cookies en navegadores basados en Chromium, abriendo una copia del navegador a través de un puerto de depuración para obtener los datos.

Expansión de la campaña maliciosa

Los actores detrás de este malware han extendido sus ataques mediante un cargador denominado ArcanaLoader, el cual se promociona falsamente como una herramienta para descargar trampas en videojuegos, pero en realidad instala Arcane. Los principales países afectados por esta campaña son Rusia, Bielorrusia y Kazajistán.

Kaspersky concluye que esta operación demuestra la capacidad de adaptación de los ciberdelincuentes, quienes constantemente actualizan sus herramientas y métodos de distribución. *«Arcane es particularmente interesante debido a la gran cantidad de datos que recopila y las técnicas que emplea para extraer la información deseada por los atacantes»*, señala la compañía de ciberseguridad.