Unit 42 de Palo Alto Networks detalló el funcionamiento interno de un malware llamado OriginLogger, que ha sido promocionado como el sucesor del ampliamente usado ladrón de información y troyano de acceso remoto (RAT) Agent Tesla.

Agent Tesla es un registrador de teclas y acceso remoto basado en .NET, que ha tenido una presencia desde hace tiempo en el panorama de amenazas, lo que permite a los hackers obtener acceso remoto a los sistemas específicos y enviar información confidencial a un dominio controlado por el atacante.

Se sabe que se utiliza en la naturaleza desde 2014, se anuncia para la venta en foros de la dark web y generalmente se distribuye a través de correos electrónicos no deseados maliciosos como un archivo adjunto.

En febrero de 2021, la compañía de seguridad cibernética Sophos, reveló dos nuevas variantes del malware básico (versión 2 y 3), que presentaban capacidades para robar credenciales de navegadores web, aplicaciones de correo electrónico y clientes VPN, además de usar la API de Telegram para comando y control.

Ahora, según el investigador de Uint 42, Jeff White, lo que se ha etiquetado como Agent Tesla versión 3 es en realidad OriginLogger, que surgió para llenar el vacío dejado por el primero después de que sus operadores cerraron la tienda el 4 de marzo de 2019, después de problemas legales.

El punto de partida de la investigación de la firma de seguridad cibernética fue un video de YouTube que se publicó en noviembre de 2018 y que detalla sus características, lo que condujo al descubrimiento de una muestra de malware («OriginLogger.exe«) que se cargó en la base de datos de malware VirusTotal el 17 de mayo de 2022.

El ejecutable es un binario generador que permite que un cliente comprado especifique los tipos de datos que se capturarán, incluyendo el portapapeles, las capturas de pantalla y la lista de aplicaciones y servicios (por ejemplo, navegadores, clientes de correo electrónico, etc.) desde los cuales se obtendrán las credenciales.

La autenticación del usuario se logra mediante el envío de una solicitud a un servidor OriginLogger, que se resuelve en los nombres de dominio *0xfd3[.]com y su contraparte más reciente originpro[.]me* en función de dos artefactos compilador el 6 de septiembre de 2020 y el 29 de junio de 2022.

Unit 42 dijo que pudo identificar un perfil de GitHub con el nombre de usuario 0xfd3 que alojaba dos repositorios de código fuente para robar contraseñas de Google Chrome y Microsoft Outlook, los cuales se utilizan en OrionLogger.

OrionLogger, como Agent Tesla, se entrega por medio de un documento de Microosft Word señuelo, que al abrirlo, está diseñado para mostrar una imagen de un pasaporte para un ciudadano alemán y una tarjeta de crédito, junto con una serie de hojas de cálculo de Excel incrustadas en él.

Las hojas de trabajo, a su vez, contienen una macro de VBA que usa MSHTA para invocar una página HTML alojada en un servidor remoto que, por su parte, incluye un código JavaScript ofuscado para obtener dos archivos binarios codificados alojados en Bitbucket.

La primera de las dos piezas de malware es un cargador que usa la técnica de vaciado de procesos para inyectar el segundo ejecutable, la carga útil OrionLogger, en el proceso aspnet_compiler.exe, una utilidad legítima para precompilar aplicaciones ASP.NET.

> *«El malware utiliza métodos probados y verdaderos e incluye la capacidad de registrar teclas, robar credenciales, tomar capturas de pantalla, descargar cargas útiles adicionales, cargar los datos en una miríada de formas e intentar evitar la detección»,* dijo White.

Además, un análisis de un corpus de más de 1900 muestras indica que los mecanismos de exfiltración más comunes para enviar los datos al atacante son a través de SMTP, FTP, cargas web al panel OrionLogger y Telegram con la ayuda de 181 bots únicos.

> *«Los keyloggers comerciales históricamente atendieron a atacantes menos avanzados, pero como se ilustra en el documento de señuelo inicial analizado aquí, esto no hace que los atacantes sean menos capaces de usar múltiples herramientas y servicios para ofuscar y hacer que el análisis sea más complicado»,* dijo White.