Investigadores de seguridad cibernética descubrieron este martes nuevas técnicas de entrega y evasión adoptadas por el troyano de acceso remoto (RAT) de Agent Tesla, para sortear las barreras de defensa y monitorear a sus víctimas.

Generalmente, el software espía de Windows se propaga a través de señuelos de ingeniería social y ahora no solo se dirige a la Interfaz de Escaneo Antimalware (AMSI) de Microsoft en un intento de derrotar al software de protección de endpoints, sino que además, emplea un proceso de instalación de varias etapas y utiliza la API de mensajería Tor y Telegram para comunicarse con un servidor de comando y control (C2).

La compañía de seguridad cibernética Sophos, que observó dos versiones de Agent Tesla, la versión 2 y la versión 3, actualmente en estado activo, dijo que los cambios son otra señal más de la evolución constante de Agent Tesla diseñada para dificultar el análisis estático y la sandbox.

> *«Las diferencias que vemos entre la v2 y la v3 de Agent Tesla parecen estar enfocadas en mejorar la tasa de éxito del malware contra las defensas sandbox y los escáneres de malware, y en brindar más opciones C2 a sus clientes atacantes»,* dijeron los investigadores de Sophos.

con un keylogger y un ladrón de información basado en .NET, Agent Tesla se ha implementado en una serie de ataques desde finales de 2014, con características adicionales incorporadas a lo largo del tiempo que le permiten monitorear y recopilar la entrada del teclado de la víctima, tomar capturas de pantalla y exfiltrar las credenciales que pertenecen a una variedad de software como clientes VPN, clientes de correo electrónico y FTP y navegadores web.

En mayo pasado, durante el apogeo de la pandemia, se descubrió que una variante del malware se propagaba a través de campañas de spam con temática COVID para robar contraseñas WiFi junto con más información, como las credenciales de correo electrónico de Outlook de los sistemas de destino.

Después, en agosto de 2020, la segunda versión de Agent Tesla aumentó a 55 la cantidad de aplicaciones destinadas al robo de credenciales, cuyos resultados se transmitieron a un servidor controlado por el atacante a través de SMTP o FTP.

Aunque el uso de SMTP para enviar información a un servidor de correo electrónico controlado por el atacante se detectó en 2018, también se descubrió que una de las nuevas versiones identificadas por Sophos aprovechaba el proxy Tor para las comunicaciones HTTP y la API de la aplicación de mensajería instantánea Telegram para transmitir la información a una sala de chat privada.

Además, Agent Tesla ahora intenta modificar el código en AMSI en un intento de omitir los escaneos de cargas útiles maliciosas obtenidas por el descargador de la primera etapa, que luego toma el código ofuscado codificado en base64 de Pastebin que actúa como cargador para el malware.

AMSI es un estándar de interfaz que permite que las aplicaciones y los servicios se integren con cualquier producto antimalware existente que esté presente en una máquina con Windows.

Además, para lograr la persistencia, el malware se copia a sí mismo en una carpeta y establece los atributos de la carpeta en «oculto» y «sistema» para ocultarlo en el Explorador de Windows, dijeron los investigadores.

> *«El método de entrega más extendido para Agent Tesla es el spam malicioso. Las cuentas de correo electrónico que se utilizan para difundir Agent Tesla son por lo general cuentas legítimas que se han visto comprometidas. Las organizaciones y las personas deben, como siempre, tratar los archivos adjuntos de correo electrónico de remitentes desconocidos con precaución y verificar los archivos adjuntos antes de abrirlos»,* dijeron los investigadores Sean Gallagher y Markel Picado.