Los expertos en ciberseguridad han detectado un nuevo ladrón de información *«sofisticado»* basado en Java que utiliza un bot de Discord para extraer datos delicados de sistemas comprometidos.

El malware, denominado NS-STEALER, se propaga a través de archivos ZIP que simulan ser software crackeado, según el análisis publicado la semana pasada por Gurumoorthi Ramanathan, investigador de seguridad de Trellix.

Dentro del archivo ZIP se encuentra un archivo de acceso directo de Windows fraudulento («Loader GAYve»), que actúa como un conducto para desplegar un archivo JAR malicioso. Este JAR, a su vez, crea inicialmente una carpeta llamada «NS-» para almacenar los datos recopilados.

En dicha carpeta, el malware almacena capturas de pantalla, cookies, credenciales y datos de autocompletado sustraídos de más de dos docenas de navegadores web, información del sistema, una lista de programas instalados, tokens de Discord y datos de sesión de Steam y Telegram. La información recopilada se transfiere luego a un canal de bot de Discord.

> *«Considerando la función altamente avanzada de recopilación de información sensible y el uso de X509Certificate para respaldar la autenticación, este malware puede extraer rápidamente información de los sistemas de la víctima con [Java Runtime Environment]»,* afirmó Ramanathan.
>
> *«El uso del canal de bot de Discord como EventListener para recibir datos exfiltrados también es eficiente desde el punto de vista de los costos».*

Este descubrimiento coincide con la actualización (versión 4.1) realizada por los actores de amenazas responsables del malware Chaes (también conocido como Chae$) para el ladrón de información, mejorando su módulo Chronod, encargado de robar credenciales de inicio de sesión introducidas en navegadores web e interceptar transacciones de criptomonedas.

Las cadenas de infección que distribuyen el malware, según Morphisec, utilizan señuelos de correo electrónico con temáticas legales escritos en portugués para engañar a los destinatarios y hacer clic en enlaces falsos que despliegan un instalador malicioso para activar el Chaes$ 4.1.

En un giro interesante, los desarrolladores también dejaron mensajes de agradecimiento dirigidos al investigador de seguridad Arnold Osipov, quien ha analizado exhaustivamente Chaes en el pasado, expresando su gratitud por contribuir a mejorar su «software», mensaje incorporado directamente en el código fuente.