Investigadores de seguridad de Microsoft publicaron detalles de una nueva campaña generalizada que distribuye una infame pieza de malware sin archivos que se encontró principalmente en usuarios europeos y brasileños a inicios de este año.

Apodado como Astaroth, el troyano de malware ha estado haciendo las rondas desde al menos 2017 y fue diseñado para robar información sensible de los usuarios, tal como credenciales, pulsaciones de teclas y otros datos, sin el uso de algún archivo ejecutable en el disco de la víctima o instalación de software.

Inicialmente descubierto por investigadores en Cybereason en febrero pasado, Astaroth ha vivido ejecutando la carga útil directamente en la memoria de una computadora específica o aprovechando herramientas legítimas del sistema, como WMIC, Certutil, Bitsadmin y Regsvr32, para ejecutar el código malicioso.

Andrea Lelli, investigadora del Equipo de Investigación ATP de Microsoft Defender, detectó un repentino aumento inusual en el uso de la herramienta de línea de comandos de Instrumentación de Gestión (WMIC), mientras revisaba los datos de telemetría de Windows, lo que sirvió como revelación de un ataque sin archivo.

Al hacer clic en el archivo de acceso directo, se ejecuta la herramienta WMIC incorporada de Windows que descarga y ejecuta un código JavaScript, lo que abusa aún más de la herramienta Bitsadmin para descargar todas las demás cargas maliciosas que realizan las tareas malintencionadas de robo y carga de los datos de la víctima mientras se disfraza como sistema proceso.

> *«Todas las cargas útiles están codificadas en Base64 y decodificadas con la herramienta Certuil. Dos de ellas dan como resultado archivos DLL simples. La herramienta Regsvr32 se usa para cargar una de las DLL decodificadas, que a su vez descifra otros archivos hasta que la carga útil final, Astaroth, se inyecta en el proceso Userinit»*, dijo el investigador el lunes.

Esto significa que el malware no se basa en ninguna vulnerabilidad o en el uso tradicional de troyanos. Distinto a eso, se basa completamente en las herramientas y comandos del sistema durante toda su cadena de ataques para disfrazarse como una actividad regular.

Esta técnica se denomina como *«living off the land»* o Vivir fuera de la tierra, y permite que el malware evite la detección de la mayoría de las soluciones de seguridad antivirus de punto final que se basan en el análisis de archivos estáticos.

Las etapas iniciales de acceso y ejecución para instalar silenciosamente el malware Astaroth en los dispositivos de destino se han demostrado en la cadena de ataque mostrada en la imagen.

Una vez en el sistema destino, Astaroth intenta robar la información confidencial, mencionada anteriormente, para luego enviarla a un servidor remoto controlado por los hackers.

El atacante puede utilizar esta información robada para tratar de *«moverse lateralmente a través de redes, realizar robos financieros o vender información de la víctima en la clandestinidad cibernética»,* dijo el investigador.

Microsoft dijo que las características de su protección de próxima generación Defender ATP, podrían detectar este tipo de ataques de malware sin archivos en cada etapa de infección, mientras que otras soluciones de seguridad centradas en archivos no protegen a sus clientes.

> *«Estar sin archivos no significa ser invisible; ciertamente no significa ser indetectable. No existe el ciberdelito perfecto, aún cuando el malware sin archivos deja un largo rastro de evidencia»*, dijo Andrea.