Se han dirigido campañas hacia entidades gubernamentales, organizaciones militares y usuarios civiles en Ucrania y Polonia como parte de una serie de ataques diseñados para sustraer información confidencial y obtener acceso remoto persistente a los sistemas infectados.

Durante el periodo comprendido entre abril de 2022 y julio de 2023, un grupo de intrusiones ha utilizado señuelos de phishing y documentos falsos para implementar un malware descargador conocido como PicassoLoader, el cual actúa como un conducto para lanzar el malware Cobalt Strike Beacon y njRAT.

> *«Los ataques emplearon una cadena de infección en varias etapas que se inició con documentos maliciosos de Microsoft Office, siendo los formatos de archivo de Microsoft Excel y PowerPoint los más utilizados. Esto fue seguido por un descargador ejecutable y una carga útil oculta en un archivo de imagen, presumiblemente para dificultar su detección»,* declaró el investigador de Cisco Talos, Vanja Svajcer, en un informe reciente.

Algunas de estas actividades han sido atribuidas a un grupo de amenazas conocido como GhostWriter (también conocido como UAC-0057 o UNC1151), cuyos objetivos se cree que están alineados con el gobierno de Bielorrusia.

Cabe destacar que un subconjunto de estos ataques ya ha sido documentado en el último año por el Equipo de Respuesta a Emergencias Informáticas de Ucrania (CERT-UA) y por Fortinet FortiGuard Labs, uno de los cuales utilizó documentos de PowerPoint con macros para distribuir el malware Agent Tesla en julio de 2022.

Las cadenas de infección buscan persuadir a las víctimas para que habiliten las macros, siendo la macro de VBA diseñada para descargar un descargador de DLL conocido como PicassoLoader, el cual se comunica posteriormente con un sitio controlado por los atacantes para obtener la carga útil de la siguiente etapa, que consiste en un archivo de imagen legítimo que contiene el malware final.

Esta revelación coincide con el informe detallado del CERT-UA sobre una serie de operaciones de phishing que distribuyen el malware SmokeLoader, así como un ataque de smishing diseñado para obtener control no autorizado de las cuentas de Telegram de los objetivos.

El mes pasado, el CERT-UA reveló una campaña de ciberespionaje dirigida a organizaciones estatales y representantes de medios en Ucrania, en la que se utilizan correos electrónicos y mensajes instantáneos para distribuir archivos que, al ejecutarse, activan un script de PowerShell denominado LONEPAGE para obtener las cargas útiles de robo de navegadores (THUMBCHOP) y keylogger (CLOGFLAG) en la siguiente etapa.

GhostWriter es uno de los múltiples actores de amenazas que han fijado su atención en Ucrania. Esto incluye al grupo estatal ruso APT28, el cual se ha observado utilizando adjuntos HTML en correos electrónicos de phishing que instan a los destinatarios a cambiar sus contraseñas de UKR.NET y Yahoo! debido a actividad sospechosa detectada en sus cuentas, redirigiéndolos a páginas falsas que finalmente roban sus credenciales.

Este desarrollo también sigue a la implementación de un *«manual de cinco fases estándar»* por parte de los hackers relacionados con la inteligencia militar rusa (GRU) en sus operaciones disruptivas contra Ucrania, en un *«esfuerzo deliberado por aumentar la velocidad, escala e intensidad»* de sus ataques.

Esto implica aprovechar infraestructuras al límite para obtener acceso inicial, utilizar técnicas de *«vivir de la tierra»* para llevar a cabo reconocimiento, movimiento lateral y robo de información con el fin de limitar su presencia de malware y evadir la detección, establecer acceso persistente y privilegiado a través de objetos de directiva de grupo (GPO), desplegar borradores y transmitir sus acciones a través de identidades de hacktivistas en Telegram.

> *«Los beneficios que el manual ofrece son particularmente adecuados para un entorno operativo acelerado y altamente disputado, lo que indica que los objetivos de guerra de Rusia probablemente hayan guiado las tácticas elegidas por el GRU»,* afirmó Mandiant, una subsidiaria de Google.