Personal y líderes políticos de la Unión Europea involucrados en proyectos de igualdad de género han sido objeto de una nueva campaña que emplea una versión actualizada del troyano RomCom RAT denominada PEAPOD.

La firma de ciberseguridad Trend Micro ha atribuido estos ataques a un grupo de amenazas que rastrea bajo el nombre de Void Rabisu, también conocido como Storm-0978, Tropical Scorpius y UNC2596, y se cree que está vinculado al ransomware Cuba.

Este colectivo adversario es algo inusual ya que lleva a cabo tanto ataques con motivaciones financieras como de espionaje, difuminando la distinción entre sus modos de operación. También está exclusivamente relacionado con el uso de RomCom RAT.

Los ataques que involucran esta puerta trasera han dirigido su atención a Ucrania y a países que apoyan a Ucrania en su conflicto con Rusia en el último año.

A principios de julio, Microsoft acusó a Void Rabisu de explotar la vulnerabilidad CVE-2023-36884, un fallo de ejecución de código remoto en Office y HTML de Windows, mediante documentos de Microsoft Office especialmente diseñados relacionados con el Congreso Mundial Ucraniano.

RomCom RAT tiene la capacidad de interactuar con un servidor de comando y control (C&C) para recibir órdenes y ejecutarlas en la máquina de la víctima, además de incorporar técnicas de evasión de la seguridad, lo que representa una constante evolución en su sofisticación.

Por lo general, el malware se distribuye a través de correos electrónicos de spear-phishing altamente dirigidos y anuncios falsos en motores de búsqueda como Google y Bing para engañar a los usuarios y hacer que visiten sitios de señuelo que alojan versiones troyanizadas de aplicaciones legítimas.

> *«Void Rabisu es uno de los ejemplos más claros donde vemos una mezcla de las tácticas, técnicas y procedimientos (TTP) típicamente utilizados por actores de*

> *amenazas cibernéticas delincuentes y TTP utilizados por actores de amenazas patrocinados por estados nacionales motivados principalmente por objetivos de espionaje»,* afirmó Trend Micro.

El conjunto más reciente de ataques detectados por la empresa en agosto de 2023 también entrega RomCom RAT, aunque se trata de una versión actualizada y más ligera del malware que se distribuye a través de un sitio web llamado wplsummit[.]com, que es una réplica del legítimo dominio wplsummit[.]org.

En el sitio web se encuentra un enlace a una carpeta de Microsoft OneDrive que alberga un archivo ejecutable llamado *«Unpublished Pictures 1-20230802T122531-002-sfx.exe»,* un archivo de 21,6 MB que pretende parecer una carpeta que contiene fotos del Women Political Leaders (WPL) Summit que tuvo lugar en junio de 2023.

El archivo binario es un descargador que coloca 56 imágenes en el sistema objetivo como señuelo, mientras que recupera un archivo DLL desde un servidor remoto. Se dice que estas imágenes fueron obtenidas por el actor malicioso a partir de publicaciones individuales en diversas plataformas de redes sociales como LinkedIn, X (anteriormente conocido como Twitter) e Instagram.

El archivo DLL, por su parte, establece contacto con otro dominio para obtener el artefacto PEAPOD de la tercera etapa, que admite un total de 10 comandos, en comparación con los 42 comandos admitidos por su predecesor.

La versión revisada está equipada para ejecutar comandos arbitrarios, descargar y cargar archivos, obtener información del sistema e incluso desinstalarse del host comprometido. Al reducir el malware a las características esenciales, se pretende limitar su presencia digital y complicar los esfuerzos de detección.

> *«Aunque no tenemos evidencia de que Void Rabisu esté respaldado por un estado, es posible que sea uno de los actores de amenazas motivados financieramente del*

> *ámbito del cibercrimen que se vio involucrado en actividades de ciberespionaje debido a las circunstancias geopolíticas extraordinarias provocadas por la guerra en Ucrania»,* concluyó Trend Micro.