Investigadores de seguridad cibernética descubrieron una muestra de PlugX, que emplea métodos engañosos para infectar dispositivos de medios USB extraíbles adjuntos con el fin de propagar el malware a sistemas adicionales.

> *«Esta variante de PlugX es compatible con gusanos e infecta dispositivos USB de tal forma que se oculta del sistema de archivos operativo de Windows. Un usuario no sabría que su dispositivo USB está infectado o posiblemente se utiliza para extraer datos de sus redes»,* dijeron Mike Harbison y Jen Miller-Osborn, investigadores de Unit42 de Palo Alto Networks.

La compañía de seguridad cibernética dijo que descubrió el artefacto durante un esfuerzo de respuesta a incidentes después de un ataque de ransomware Black Basta contra una víctima no identificada. Entre otras herramientas descubiertas en el entorno comprometido se incluyen el cargador de malware Gootkit y el marco del equipo rojo Brute Ratel C4.

Trend Micro destacó previamente el uso de Brute Ratel por parte del grupo Black Basta en octubre de 2022, con el software entregado como una carga útil de segunda etapa por medio de una campaña de phishing de Quakbot. Desde entonces, la cadena de ataque se ha utilizado contra un gran equipo de energía regional con sede en el sureste de Estados Unidos, según Quadrant Security.

Sin embargo, no hay evidencia que vincule a PlugX, una backdoor ampliamente compartida entre varios grupos de estados-naciones chinos, o Gootkit, con el grupo de ransomware Black Basta, lo que sugiere que puede haber sido implementado por otros atacantes.

La variante USB de PlugX se destaca por el hecho de que utiliza un caracter Unicode particular llamado espacio de no interrupción (U+00A0) para ocultar archivos en un dispositivo USB conectado a una estación de trabajo.

> *«El caracter de espacio en blanco evita que el sistema operativo Windows*

> *represente el nombre del directorio, ocultándolo en lugar de dejar una carpeta sin nombre en el Explorador»,* dijeron los investigadores.

Finalmente, se utiliza un archivo de acceso directo de Windows (.LNK) creado en la carpeta raíz de la unidad flash para ejecutar el malware desde el directorio oculto. La muestra de PlugX no solo tiene la tarea de implantar el malware en el host, sino también de copiarlo en cualquier dispositivo extraíble que pueda estar conectado camuflándolo dentro de una carpeta de papelera de reciclaje.

El archivo de acceso directo, por su parte, lleva el mismo nombre que el del dispositivo USB y aparece como un icono de unidad, con los archivos o directorios existentes en la raíz del dispositivo extraíble movidos a una carpeta oculta creada dentro de la carpeta *«acceso directo».*

> *«Cada vez que se hace clic en el archivo de acceso directo del dispositivo USB infectado, el malware PlugX inicia el Explorador de Windows y pasa la ruta del directorio como parámetro. Esto después muestra los archivos en el dispositivo USB desde dentro de los directorios ocultos y también infecta el host con el malware PlugX»*, dijo Unit42.

La técnica se basa en que el Explorador de archivos de Windows (antes Explorador de Windows) por defecto no mustra elementos ocultos. Pero el giro inteligente aquí es que los archivos maliciosos dentro de la llamada papelera de reciclaje no se muestran cuando la configuración está habilitada.

Esto significa que los archivos falsos solo se pueden ver en un sistema operativo similar a Unix como Ubuntu o montando el dispositivo USB en una herramienta forense.

> *«Una vez que se descubre e infecta un dispositivo USB, todos los archivos nuevos escritos en la carpeta raíz del dispositivo USB después de la infección se mueven a la carpeta oculta dentro del dispositivo USB. Debido a que el archivo de acceso directo de Windows se parece al de un dispositivo USB y el malware muestra los archivos de la víctima, sin saberlo, siguen propagando el malware PlugX»,* agregaron los investiadores.

Unit42 dijo que también descubrió una segunda variante de PlugX que, además de infectar dispositivos USB, copia todos los archivos Adobe PDF y Microsoft Word del host a otra carpeta oculta en el dispositivo USB creada por el malware.

El uso de unidades USB como medio para filtrar archivos específicos de interés de sus objetivos indica un intento por parte de los hackers de saltar sobre las redes abiertas.

Con el último desarrollo, PlugX se une a las filas de otras familias de malware como ANDROMEDA y Raspberry Robin, que han agregado la capacidad de propagarse por medio de unidades USB infectadas.

> *«El descubrimiento de estas muestras indica que el desarrollo de PlugX todavía está vivo y entre al menos algunos atacantes técnicamente capacitados, y sigue siendo una amenaza activa»,* concluyeron los investigadores.