Un grupo de hackers está utilizando un truco inteligente para crear archivos de Excel maliciosos que tienen bajas tasas de detección y una mayor probabilidad de eludir los sistemas de seguridad.

Descubierta por los investigadores de seguridad de NVISO Labs, la banda de malware, a la que nombraron Epic Manchego, ha estado activa desde junio y se dirige a empresas de todo el mundo, con correos electrónicos de phishing que contienen un documento de Excel malicioso.

Los investigadores aseguran que los archivos maliciosos de Excel pasaban por alto los escáneres de seguridad y tenían tasas bajas de detección. También mencionaron que los archivos maliciosos fueron compilados con EPPlus, una biblioteca .NET.

Los desarrolladores por lo general usan esta biblioteca como parte de sus aplicaciones para agregar la funciones *«Exportar como Excel» o «Guardar como hoja de cálculo».*

La biblioteca se puede utilizar para generar archivos en una gran variedad de formatos de hojas de cálculo e incluso es compatible con Excel 2019.

NVISO dijo que los hackers de Epic Manchego parecen estar usando EPPlus para generar archivos de hoja de cálculo en el formato Office Open XML (OOXML).

Los archivos OOXML generados por los piratas carecían de una sección de código VBA compilado, específico para los documentos de Exceln compilados en el software Office de Microsoft.

Algunos productos antivirus y escáneres de correo electrónico buscan específicamente esta parte del código VBA para buscar posibles signos de documentos de Excel maliciosos, lo que explicaría por qué las hojas de cálculo generadas por la banda Epic Manchego tenían tasas de detección más bajas que otros archivos maliciosos.

Los investigadores explicaron que los ciberdelincuentes simplemente almacenaron su código

malicioso en un formato de código VBA personalizado, que también estaba protegido con contraseña para evitar que los sistemas de seguridad e investigadores analizaran su contenido.

Pero a pesar de utilizar un método diferente para generar sus documentos de Excel maliciosos, los archivos de hoja de cálculo basados en EPPlus todavía funcionaban como cualquier otro documento de Excel.

Los documentos maliciosos todavía contenían un macro script malicioso. Si los usuarios que abrieron los archivos de Excel permitieron que se ejecutara la secuencia de comandos, los macros descargarían e instalarían malware en los sistemas de la víctima.

Las cargas útiles finales fueron troyanos de robo de información clásicos, como Azorult, AgentTesla, Formbook, Matiex y njRat, que descargaban contraseñas de los navegadores, correos electrónicos y clientes FTP del usuario y las enviaban a los servidores de Epic Manchego.

Aunque la decisión de usar EPPlus para generar sus archivos de Excel maliciosos podría haber tenido algunos beneficios, también perjudicó a los hackers, ya que permitió al equipo de NVISO detectar fácilmente sus operaciones pasadas mediante una búsqueda para documentos de Excel.

NVISO dijo que descubrió más de 200 archivos de Excel maliciosos vinculados a Epic Manchego, y el primero se remonta al 22 de junio de 2020.

Los investigadores aseguran que el grupo parece estar experimentado con esta técnica, y desde los primeros ataques, han aumentado tanto su actividad como la sofisticación de sus ataques, lo que sugiere que esto podría tener un uso más amplio en el futuro.

> *«Estamos familiarizados con esta biblioteca .NET, ya que la hemos estado usando desde hace un par de años para crear documentos maliciosos («maldocs») para*

> *nuestro equipo rojo y probadores de penetración»*, dijo la compañía.

Los indicadores de compromiso y un desglose técnico de los archivos de Excel maliciosos renderizados por EPPlus están disponibles en el informe Epic Manchego de NVISO Labs.