Cuáles son los archivos que llegan a los correos y redes sociales para robar datos

04/12/2022

Un informe de **HP Wolf Security** reveló que los formatos de archivos comprimidos, como .ZIP y .RAR, fueron los más usados para distribuir software malicioso entre julio y septiembre de este 2022, superando a los de Office, que durante tres años fueron la opción prioritaria de los ciberdelincuentes.

Según los resultados obtenidos a través de los dispositivos que ejecutan este sistema de ciberseguridad, el 44 % del software malicioso se entregó dentro de archivos comprimidos, teniendo un aumento del 11 % respecto al trimestre anterior en el año.

Mientras que el 32 % se distribuyó por medio de documentos de Office, como Microsoft Word, Excel y PowerPoint.

Nuevas formas de ataque

La utilización de este tipo de archivos comprimidos vino acompañada de una nueva forma de contrabando de HTML, en la que los ciberdelincuentes incrustan software malicioso en formatos HTML para eludir la seguridad de los correos electrónicos y plataformas, para luego realizar el ataque.

Un ejemplo es lo que sucedió con las campañas recientes de QakBot y IceID que utilizaron estos archivos para dirigir a los usuarios a visores de documentos en línea falsos, que se hacían pasar por **Adobe.**

Después le pedían a las personas abrir un archivo comprimido .ZIP, ingresar una contraseña y descomprimir más documentos que contenían el malware y atacar al computador.

Este tipo de ataques son difíciles de detectar para los programas de ciberseguridad y los correos electrónicos porque el malware dentro del archivo HTML original está codificado y encriptado. Así que el ciberdelincuente solo debe asegurarse de que el sitio web sea lo más parecido al original para engañar a las personas.

Una práctica que se ha visto implementada en otras aplicaciones como Drive. En octubre los atacantes crearon una plataforma similar a esta para hacer creer a los usuarios que era el servicio en la nube oficial de Google, pero allí se buscaba distribuir los archivos comprimidos .ZIP con malware.

“Estas campañas fueron más convincentes de las que habíamos visto anteriormente, dificultando a las personas distinguir los archivos en los que pueden confiar y en los que no”, explicó Alex Holland, analista senior de malware del equipo de investigación de amenazas de la empresa encargada del informe.

Otro tipo de ataque encontrado fue una cadena de infección modular que le daba la facultad a los delincuentes de cambiar

la carga útil, como spyware, ransomware o keylogger, a mitad de la campaña, o introducir nuevas características como el geofacing, que permite crear límites digitales.

Es decir que el ciberdelincuente iniciaba un ataque, pero si venía la necesidad de cambiar el tipo de la manera de hacerlo, según su objetivo, lo podía realizar con facilidad. Esto porque no se incluía un malware directamente en el archivo adjunto, lo que hace muy difícil para los sistemas de protección detectar los movimientos.

“Como se muestra, los atacantes están cambiando de técnica constantemente, dificultando así la detección”, señaló Ian Pratt, jefe global de seguridad de sistemas personales de la compañía.

Según datos de la empresa, los usuarios de sus dispositivos han hecho clic en más de 18 mil millones de archivos adjuntos de correos electrónicos, páginas web y documentos descargados sin denuncias de infracciones debido a los diferentes tácticas que tienen los delincuentes para eludir a los sistemas de seguridad.

Fuente: Infobae