El nuevo malware bancario que está robando información en varios países

19/12/2022

Prometiendo una autorización de acceso a Internet a través de redes wifi, los delincuentes están engañando a usuarios para robar información para entrar a sus aplicaciones bancarias y tomar el dinero de las cuentas.

Esta modalidad se repite constantemente y recientemente surgió un nuevo malware llamado **Zombinder**, que fue encontrado por los investigadores de **Threat Fabric**, y ya ha afectado a más 1.300 personas en países como **Canadá, España y Portugal.**

Así es Zombiender, nuevo virus bancario

Los ciberdelincuentes detrás de esta amenaza usan aplicaciones de autorización de conexión wifi, como las que aparecen en hoteles o redes públicas, para invitar a las víctimas a descargar una supuesta plataforma oficial que permita establecer la conexión.

Al instalar la app en el celular, el malware tiene la capacidad de realizar diferentes ataques como robar correos electrónicos, códigos de verificación, credenciales y las frases que protegen los monederos de las criptomonedas.

El virus viene escondido en aplicaciones ‘zombie’, de ahí su nombre. Estas plataformas no tienen ningún tipo de utilidad para el usuario, pero sí se encargan de infectar el dispositivo, incluso con malwares de terceros.

“**Zombinder** deja caer y lanza el troyano **Xenomorph,** mientras que la aplicación original permanece completamente operativa, por lo que la víctima permanece desprevenida. Cabe señalar que los autores de **Xenomorph** (conocido como HadokenSecurity) continúan desarrollando el troyano”, informó la empresa que detectó el virus.

Los principales objetivos de los ciberdelincuentes son cuentas bancarias de entidades como **N26, CaixaBank, Santander, ING, Abanca, Targobank, Kutxa, Pibank, Unicaja, BBVA, Bankinter u Openbank**, entre otras.

Para evitar que más personas caigan víctimas de este malware, los investigadores publicaron un listado de las aplicaciones que contienen el virus, que ataca a usuarios de Android:

– WiFi Auto Authenticator (com.woosh.wifiautoauth)

– Football live stream (com.aufait.footballlivestream)

– OG (com.much.dizzy)

– Wi Fi Authorization (com.welomuxitononu.voretije)

– Live Football Stream 1.9 (com.busafobawori.zuvo)

– OGInsta+ Mod (com.fuyocelasisi.woyopu)

– VidMate (com.focus.equip)

Así que en caso de tener una de estas plataformas instaladas, será mejor eliminarla, además de cambiar las contraseñas de acceso a los bancos, porque la expansión de este tipo de malware puede propagarse en diferentes partes del sistema operativo.

Archivos ZIP, una opción para los

ciberdelincuentes

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.

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 este formato para eludir la seguridad de los correos electrónicos y plataformas y, de este modo, 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.

Fuente: Infobae