La decisión de Microsoft de bloquear las macros de Visual Basic para aplicaciones (VBA) de forma predeterminada para los archivos de Office descargados de Internet, llevó a muchos atacantes a improvisar sus cadenas de ataque en los últimos meses.

Ahora, según Cisco Talos, los actores persistentes avanzados (APT) y las familias de malware de productos básicos usan cada vez más archivos de complemento de Excel (.XLL) como vector de intrusión inicial.

Los documentos de Office armados entregados por medio de correos electrónicos de phishing y otros ataques de ingeniería social se han mantenido como uno de los puntos de entrada más usados por los grupos criminales que buscan ejecutar código malicioso.

Estos documentos tradicionalmente solicitan a las víctimas que habiliten macros para ver contenido aparente inocuo, solo para activar la ejecución de malware de forma sigilosa en segundo plano.

Para contrarrestar este mal uso, el fabricante de Windows promulgó un cambio crucial a partir de julio de 2022 que bloquea las macros en los archivos de Office adjuntos a los mensajes de correo electrónico, cortando de forma efectiva un vector de ataque crucial.

Aunque este bloqueo solo se aplica a las nuevas versiones de Access, Excel, PowerPoint, Visio y Word, los malos actores han estado experimentando con rutas de infección alternativas para implementar malware.

Uno de esos métodos resultan ser los archivos XLL, que Microsoft describe como un *«tipo de archivo de biblioteca de vínculos dinámicos (DLL) que solo puede abrir Excel».*

> *«Los archivos XLL se pueden enviar por correo electrónico, e incluso con las medidas habituales de escaneo antimalware, los usuarios pueden abrirlos sin saber que pueden contener código malicioso»,* dijo el investigador de Cisco Talos, Vanja Svajcer.

La compañía de seguridad cibernética dijo que los hackers están empleando una combinación de complementos nativos escritos en C++, así como aquellos desarrollados con una herramienta gratuita llamada Excel-DNA, un fenómeno que ha experimentado un aumento significativo desde mediados de 2021 y siguió hasta este año.

Se dice que el primer uso malicioso documentado públicamente de XLL ocurrió en 2017 cuando el atacante APT10 (también conocido como Stone Panda) vinculado a China, utilizó la técnica para inyectar su carga útil de puerta trasera en la memoria a través del vaciado de procesos.

Desde entonces, varios otros colectivos adversarios siguieron sus pasos, incluyendo TA410 (un actor con enlaces a APT10), DoNot Team, FIN7, así como familias de malware de productos básicos como Agent Tesla, Arkei, Buer, Dridex, Ducktail, Ekipa, .RAT, FormBook, IceID, Vidar Stealer y Warzone RAT.

El abuso del formato de archivo XLL para distribuir Agent Tesla y Dridex fue destacado previamente por Unit 42 de Palo Alto Networks, y dijo que *«puede indicar una nueva tendencia en el panorama de amenazas».*

> *«A medida que más y más usuarios adopten nuevas versiones de Microsoft Office, es probable que los atacantes se alejen de los documentos maliciosos basados en VBA a otros formatos como XLL o confíen en la explotación de vulnerabilidades recién descubiertas para lanzar código malicioso en el espacio de proceso de aplicaciones de oficina»,* dijo Svajcer.

Las macros maliciosas de Microsoft Publisher empujan a Ekipa RAT

Ekipa RAT, además de incorporar complementos XLL Excel, también recibió una actualización en noviembre de 2022 que le permite aprovechar las macros de Microsoft Publisher para

soltar el troyano de acceso remoto y robar información sensible.

> *«Al igual que con otros productos de oficina de Microsoft, como Excel o Word, los archivos de Publisher pueden contener macros que se ejecutarán al abrir o cerrar el archivo, lo que los convierte en vectores de ataque iniciales interesantes desde el punto de vista del actor de amenazas»*, dijo Trustwave.

Cabe mencionar que las restricciones de Microsoft para impedir que las macros se ejecuten en archivos descargados de Internet no se extienden a los archivos de Publisher, lo que permite a los adversarios explotar esta vía para campañas de phishing.

> *«El Ekipa RAT es un gran ejemplo de cómo los atacantes cambian continuamente sus técnicas para adelantarse a los defensores. Los creadores de este malware están rastreando los cambios en la industria de la seguridad, como el bloqueo de macros de Internet por parte de Microsoft, y cambiando sus tácticas en consecuencia»*, dijo el investigador de Trustwave, Wojciech Cieslak.