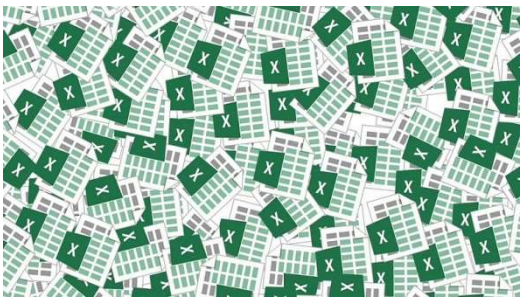
ALERTA: Complementos maliciosos de Excel XLL infectan con Malware RedLine (07/DICIEMBRE/2021)

Ciberdelincuentes envían spam, a formularios de contacto de sitios web y foros de discusión para distribuir archivos de Excel XLL, los mismos que descargan e instalan el malware RedLine para robar información y contraseñas.



Introducción

Los archivos tipo XLL, son bibliotecas de macros de Excel y se clasifican como complementos de Excel.

En algunos señuelos de phishing, analizados por el equipo de BleepingComputer, se evidenció que los actores de amenazas han creado sitios web falsos para alojar los archivos maliciosos Excel XLL, utilizados para instalar el malware RedLine.

RedLine es un caballo de Troya que recopila credenciales FTP y archivos de sistemas infectados, así como cookies, nombres de usuario y contraseñas, e información de tarjetas de crédito almacenada en navegadores web.

Además de robar datos, RedLine tiene la capacidad de ejecutar comandos, descargar y lanzar otro malware y tomar fotografías de las pantallas activas de Windows.

Toda esta información se recopila y se devuelve a los atacantes para su venta en el mercado criminal o para otros fines destructivos y fraudulentos.

Vector de ataque: Malware, Phishing

Los archivos de tipo XLL, son archivos ejecutables con bibliotecas de vínculos dinámicos (DLL). Muchas personas saben que no deben descargar/ejecutar archivos de dudosa procedencia de tipo “.exe”, lo mismo ocurre con los archivos XLL.

Al ejecutar archivos XLL, se conectan inmediatamente e inician Microsoft Excel, solicitando permiso para ejecutar el complemento relevante y, por lo tanto, el código que contiene, como se evidencia en la Figura 1.

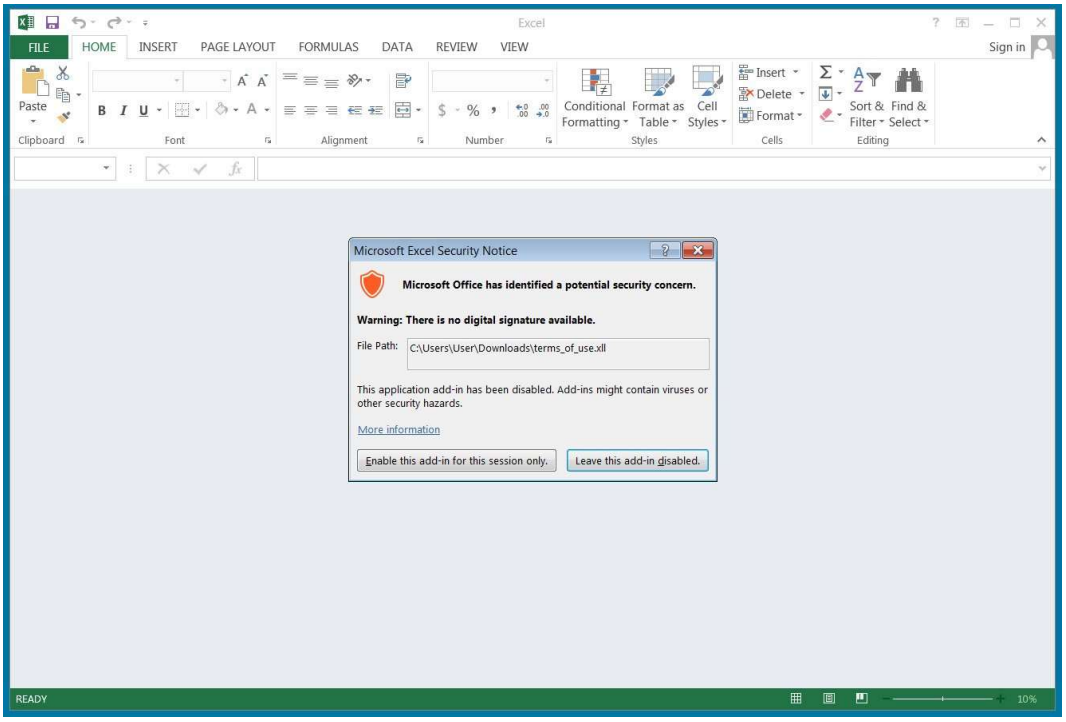


Figura 1.- Ejemplo de ejecución de archivo de Excel tipo XLL. **Fuente:** Bleeping Computer

Impacto:

Al ser una víctima de esta campaña de distribución de malware a través de documentos tipo XLL, se debe asumir que sus contraseñas almacenadas están comprometidas, al igual que sus tarjetas de crédito almacenadas en los distintos navegadores de internet.

Como los archivos XLL son ejecutables, los actores de amenazas pueden usarlos para realizar una variedad de comportamientos maliciosos en un dispositivo.

Estos archivos generalmente no se envían como archivos adjuntos, sino que se instalan a través de otro programa o mediante su administrador de Windows.

Recomendaciones:

El Centro de Respuesta a Incidentes Informáticos EcuCERT recomienda:

- Evitar descargar y ejecutar archivos de tipo XLL de Excel que se adjunten en correos electrónicos no solicitados,

- No abrir, manipular, o interactuar con correos electrónicos altamente sospechosos recibidos en las respectivas bandejas de correo ya sea personales o Institucionales.
- Instalar software antivirus de confianza, ya sea en versión libre o de paga
- Escanear archivos de tipo XLL de Excel en un software antivirus, en el caso de necesitar ejecutar el mismo.
- Mantener actualizado la suite de Microsoft Office, aplicando las últimas actualizaciones de seguridad disponibles.
- Mantener actualizado el OS de Microsoft Windows, aplicando las últimas actualizaciones de seguridad disponibles.

Referencias:

Lawrence Abrams (2021, diciembre 5). Malicious Excel XLL add-ins push RedLine password-stealing malware. Recuperado 7 de diciembre de 2021. Obtenido de https://www.bleepingcomputer.com/news/security/malicious-excel-xll-add-ins-push-redline-password-stealing-malware/

Mia ausente (2021, diciembre 6), Malicious Excel XLL Add-ons Launch Redline Malware. Recuperado 7 de diciembre de 2021 de https://en.secnews.gr/375936/kakovoula-prostheta-excel-xll-prowthoun-kakovoulo-logismiko-redlibe/

Shaunwade (2021, diciembre 7), Some Excel XLL add-ins are pushing password-stealing malware. Recuperado 7 de diciembre de 2021. Obtenido de https://www.jioforme.com/some-excel-xll-add-ins-are-pushing-password-stealing-malware/980406/