Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

La botnet Emotet comienza a lanzar malware nuevamente después de un descanso de 4 meses .

04/Noviembre/2022

Contenido

INTRODUCCIÓN

La operación de malware Emotet vuelve a enviar correos electrónicos no deseados después de unas "vacaciones" de casi cuatro meses en las que hubo poca actividad de la notoria operación de ciberdelincuencia.

EMOTET ATACA NUEVAMENTE

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2022_11_04_2
Clasificación de alerta:	Amenaza
Tipo de Impacto:	Alto
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	11/04/2022
Es día cero (0 day):	No

RESUMEN

Emotet es una infección de malware distribuida a través de campañas de phishing que contienen documentos maliciosos de Excel o Word. Cuando los usuarios abren estos documentos y habilitan las macros, la DLL de Emotet se descargará y cargará en la memoria.

Una vez cargado, el malware buscará y robará correos electrónicos para usarlos en futuras campañas de spam y soltará cargas útiles adicionales como Cobalt Strike u otro malware que comúnmente conduce a ataques de ransomware.

Si bien Emotet se consideraba el malware más distribuido en el pasado, de repente dejó de enviar spam el 13 de julio de 2022.

EMOTET REGRESA

Investigadores del grupo de investigación de Emotet, Cryptolaemus , informaron que aproximadamente a las 4:00 a. m. ET del 2 de noviembre, la operación de Emotet volvió a cobrar vida repentinamente, enviando spam a direcciones de correo electrónico en todo el mundo.

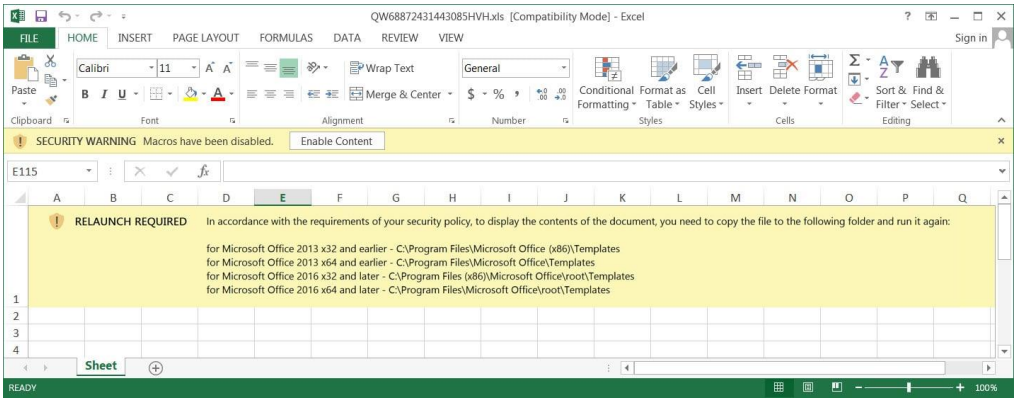
El investigador de amenazas de Proofpoint y miembro de Cryptolaemus, Tommy Madjar , dijo que las campañas de correo electrónico de Emotet de hoy utilizan cadenas de respuesta de correo electrónico robadas para distribuir archivos adjuntos de Excel maliciosos.

A partir de muestras cargadas en VirusTotal , se ha visto archivos adjuntos dirigidos a usuarios de todo el mundo en varios idiomas y nombres de archivo, que fingen ser facturas, escaneos, formularios electrónicos y otros señuelos.

A continuación, se puede ver una lista parcial de ejemplos de nombres de archivos:

```
Scan_20220211_77219.xls
fattura novembre 2022.xls
BFE-011122 XNIZ-021122.xls
FH-1612 report.xls
2022-11-02_1739.xls
Fattura 2022 - IT 00225.xls
RHU-011122 OOON-021122.xls
Electronic form.xls
Rechnungs-Details.xls
Gmail_2022-02-11_1621.xls
gescanntes-Dokument 2022.02.11_1028.xls
Rechnungs-Details.xls
DETALLES-0211.xls
Dokumente-vom-Notar 02.11.2022.xls
INVOICE0000004678.xls
SCAN594_00088.xls
Copia Fattura.xls
Form.xls
Form - 02 Nov, 2022.xls
Nuovo documento 2022.11.02.xls
Invoice Copies 2022-11-02_1008, USA.xls
payments 2022-11-02_1011, USA.xls
```

La campaña de Emotet de hoy también presenta una nueva plantilla de archivos adjuntos de Excel que contiene instrucciones para evitar la vista protegida de Microsoft.



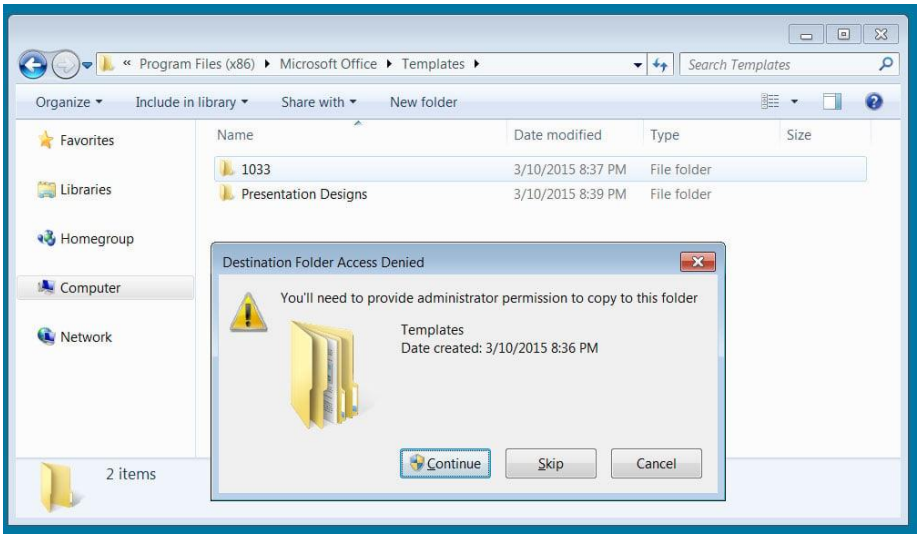
Cuando se descarga un archivo de Internet, incluso como un archivo adjunto de correo electrónico, Microsoft agregará un indicador especial Mark-of-the-Web (MoTW) al archivo.

Cuando un usuario abre un documento de Microsoft Office que contiene un indicador de MoTW, Microsoft Office lo abrirá en Vista protegida, lo que evitará que se ejecuten macros que instalen malware.

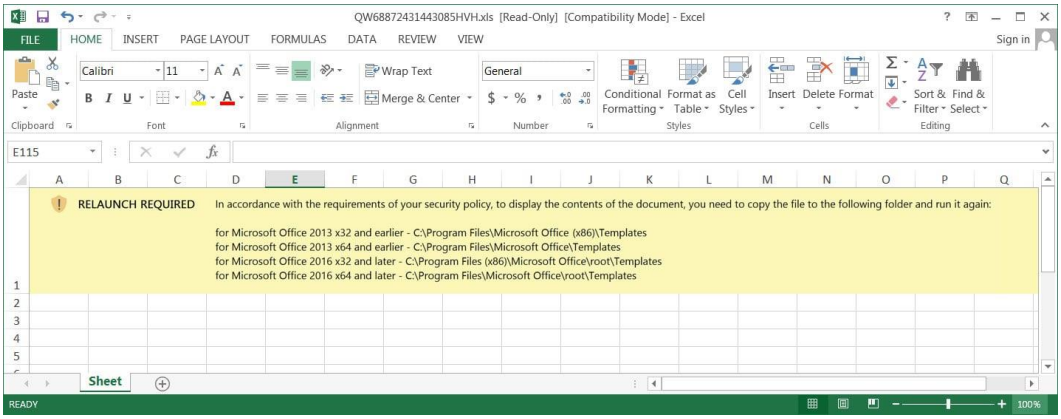
Sin embargo, en el nuevo archivo adjunto de Emotet Excel, puede ver que los actores de amenazas están instruyendo a los usuarios para que copien el archivo en las carpetas de 'Plantillas' de confianza, ya que al hacer esto se omitirá la Vista protegida de Microsoft Office, incluso para los archivos que contienen una bandera MoTW.

```
"RELAUNCH REQUIRED In accordance with the requirements of your
security policy, to display the contents of the document, you n
eed to copy the file to the following folder and run it again:


for Microsoft Office 2013 x32 and earlier - C:\Program Files\Mi
crosoft Office (x86)\Templates

for Microsoft Office 2013 x64 and earlier - C:\Program Files\Mi
crosoft Office\Templates

for Microsoft Office 2016 x32 and later - C:\Program Files (x86
)\Microsoft Office\root\Templates

for Microsoft Office 2016 x64 and later - C:\Program
Files\Microsoft Office\root\Templates"
```

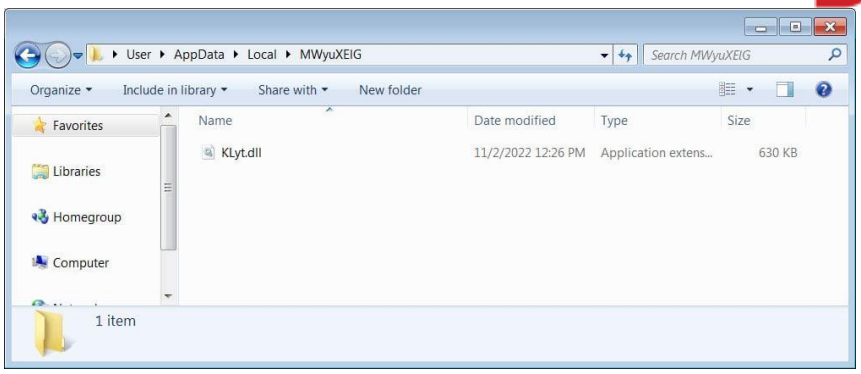
Si bien Windows advertirá a los usuarios que copiar un archivo en la carpeta 'Plantillas' requiere permisos de 'administrador', el hecho de que un usuario intente copiar el archivo indica que existe una buena posibilidad de que también presione el botón 'Continuar'.



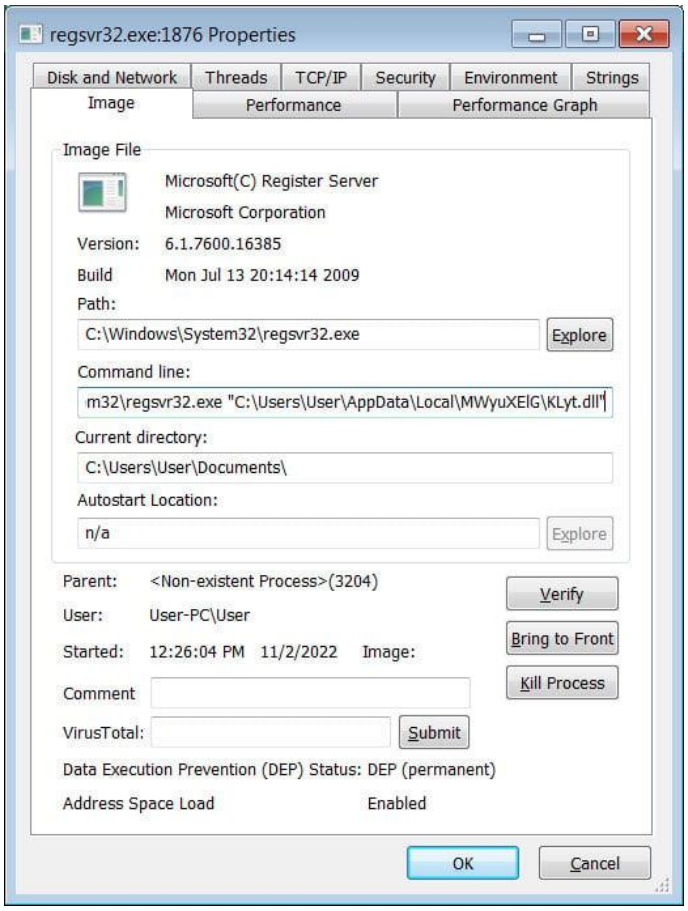
Cuando se inicia el archivo adjunto desde la carpeta 'Plantillas', simplemente se abrirá y ejecutará de inmediato las macros que descargan el malware Emotet.



El malware Emotet se descarga como DLL en varias carpetas con nombres aleatorios en %UserProfile%\AppData\Local, como se muestra a continuación.



Las macros luego iniciarán la DLL usando el comando legítimo regsvr32.exe.



Una vez descargado, el malware se ejecutará silenciosamente en segundo plano mientras se conecta al servidor de Comando y Control para obtener más instrucciones o para instalar cargas útiles adicionales.

Madjar dijo que las infecciones de Emotet de hoy no han comenzado a arrojar cargas útiles de malware adicionales en los dispositivos infectados.

Sin embargo, en el pasado, Emotet era conocido por instalar el malware TrickBot y, más recientemente, las balizas Cobalt Strike .

Estas balizas Cobalt Strike se utilizan luego para el acceso inicial de las bandas de ransomware que se propagan lateralmente en la red, roban datos y, en última instancia, cifran los dispositivos.

Las infecciones de Emotet se utilizaron en el pasado para dar a las bandas de ransomware Ryuk y Conti acceso inicial a las redes corporativas.

Desde el cierre de Conti en junio , se vio a Emotet asociándose con las operaciones de ransomware BlackCat y Quantum para el acceso inicial en dispositivos ya infectados.

RECOMENDACIONES

- Agregar los Indicadores de compromiso en sus consolas AV, Firewall, Proxy. Para garantizar una cobertura adecuada ante esta amenaza.

- Validar que solo las cuentas con nivel de administrador en dominio puedan instalar software en sus equipos.

- Se recomienda de forma periódica hacer un escaneo profundo con su Antivirus a todos sus equipos.

- Capacite a sus usuarios en la detección de Phishing y recuerde que debe reportar al área de informática todo correo que les parezca sospechoso.

Indicadores de Compromiso

https://github.com/develgroup/SOC_IOCs/tree/main/20220506_06_EmotetRansomware

Noticia Completa

https://devel.group/blog/romcom-se-distribuye-mediante-aplicaciones-popularmente-conocidas/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757
El Salvador: +(503) 2249 4252
Honduras: +(504) 2283 5904
República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente