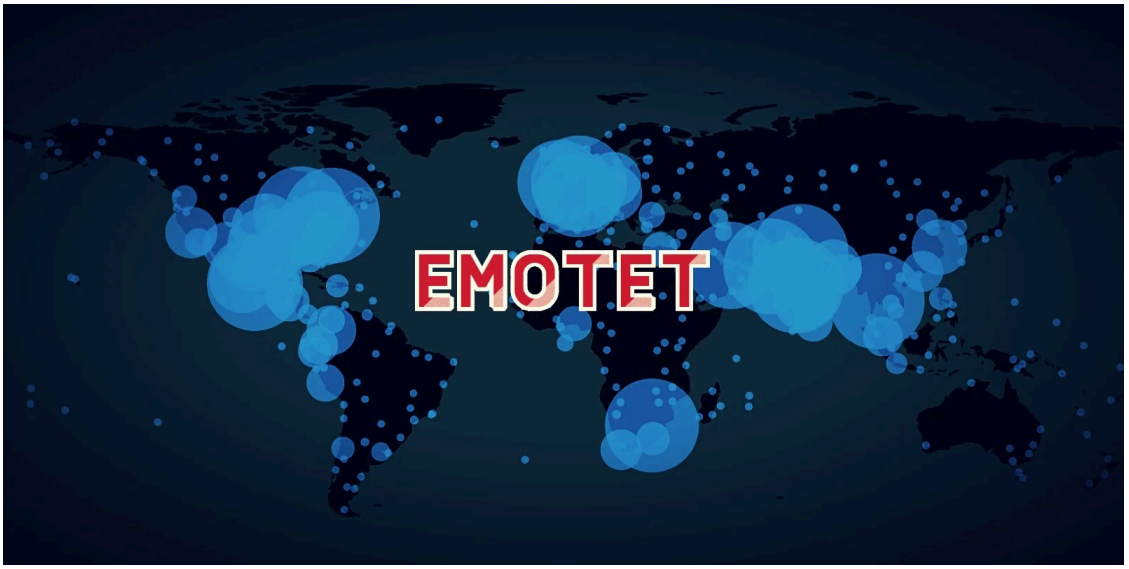
Emotet botnet starts blasting malware again after 4 month break

By Lawrence Abrams

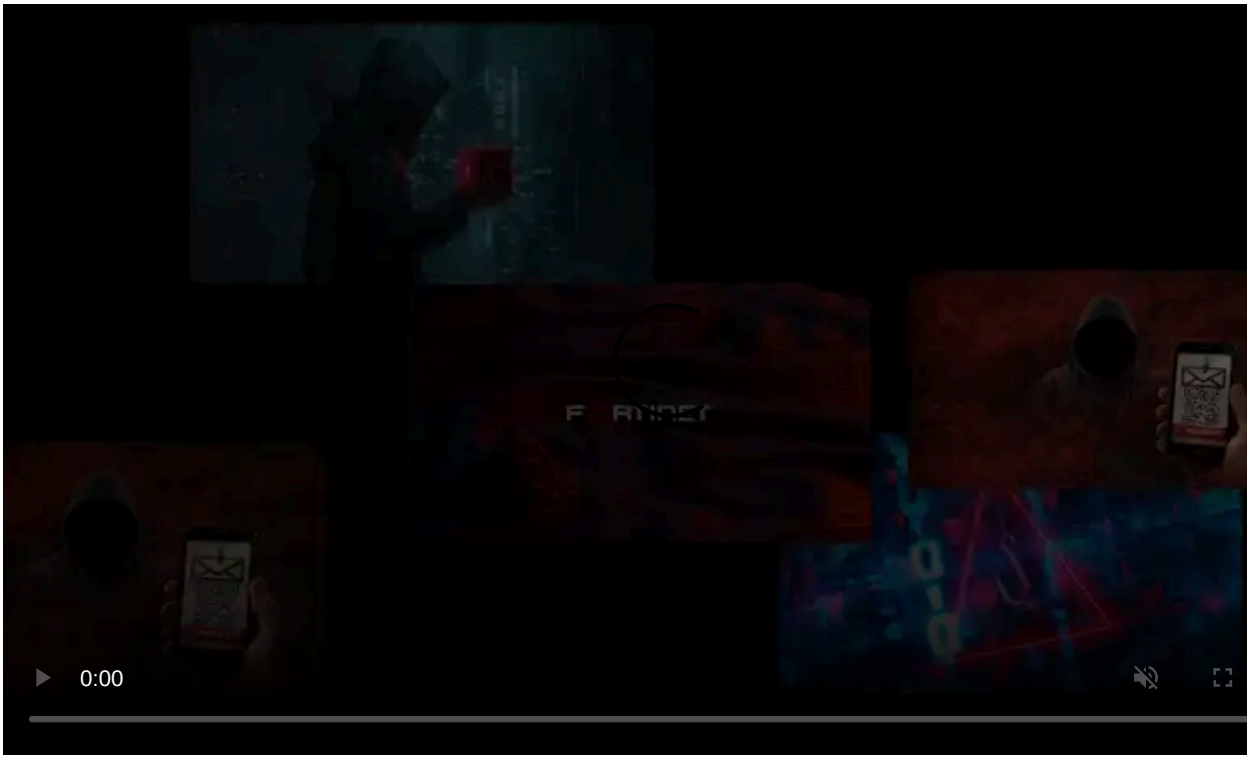
Published: 2022-11-02 · Archived: 2026-04-05 21:27:04 UTC

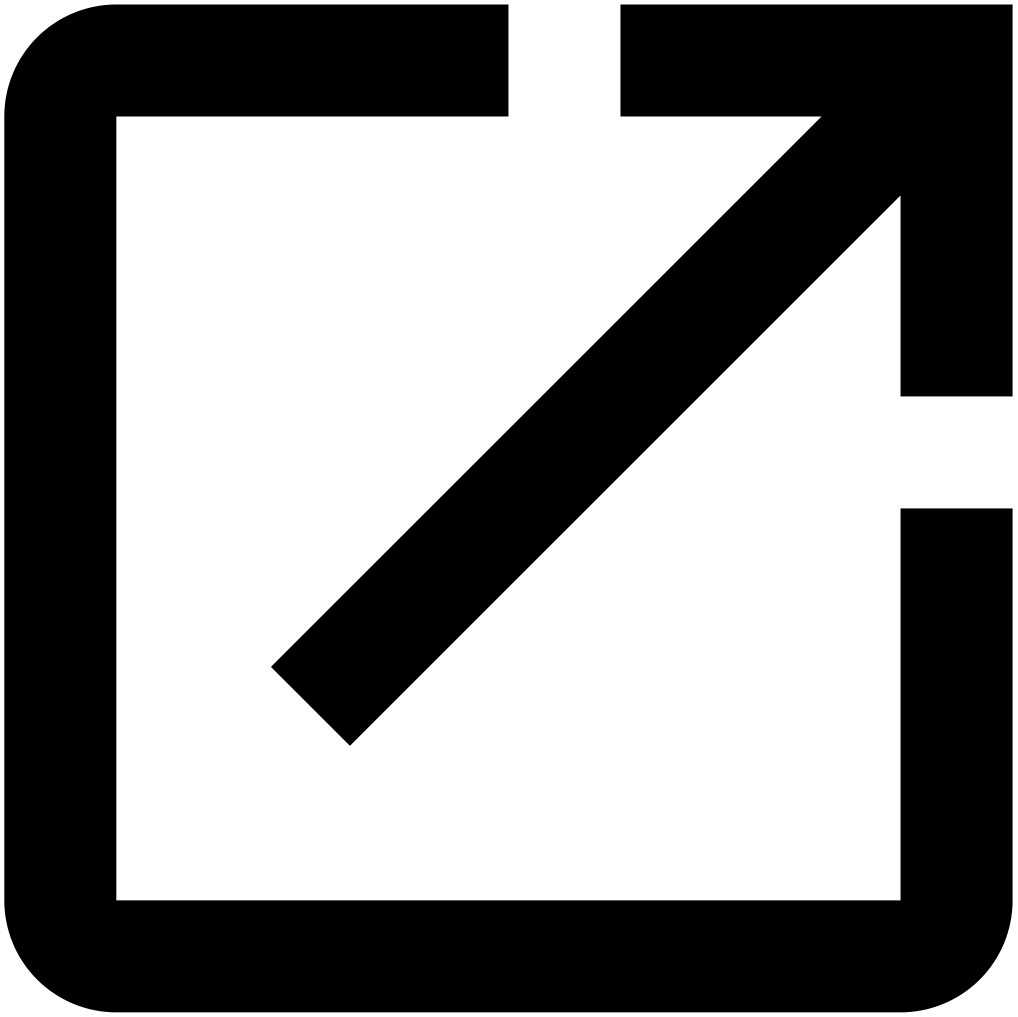


The Emotet malware operation is again spamming malicious emails after almost a four-month "vacation" that saw little activity from the notorious cybercrime operation.

Emotet is a malware infection distributed through phishing campaigns containing malicious Excel or Word documents. When users open these documents and enable macros, the Emotet DLL will be downloaded and loaded into memory.

Once loaded, the malware will search for and steal emails to use in future spam campaigns and drop additional payloads such as Cobalt Strike or other malware that commonly leads to ransomware attacks.


0:00



While Emotet was considered the most distributed malware in the past, it suddenly stopped spamming on July 13th, 2022.

Emotet returns

Researchers from the Emotet research group Cryptolaemus reported that at approximately 4:00 AM ET on November 2nd, the Emotet operation suddenly came alive again, spamming email addresses worldwide.

Proofpoint threat researcher, and Cryptolaemus member, Tommy Madjar, told BleepingComputer that today's Emotet email campaigns are using stolen email reply chains to distribute malicious Excel attachments.

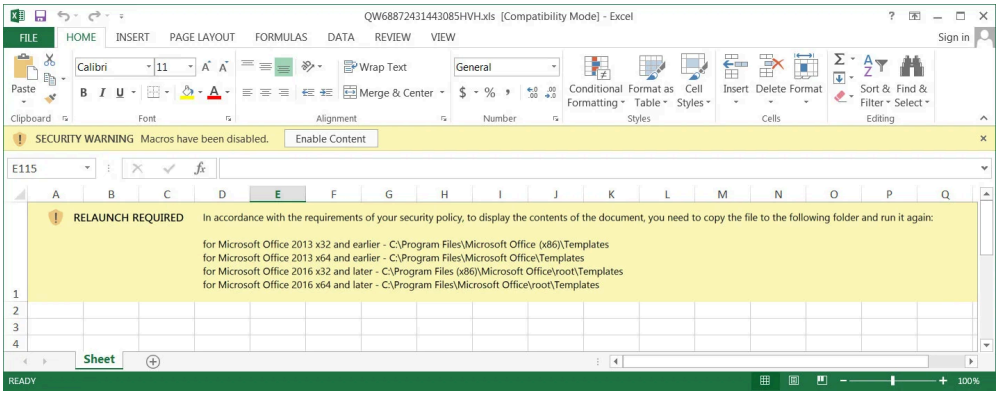
From samples uploaded to VirusTotal, BleepingComputer has seen attachments targeted at users worldwide under various languages and file names, pretending to be invoices, scans, electronic forms, and other lures.

A partial listing of example file names can be seen below:

```
 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
```

Today's Emotet campaign also introduces a new Excel attachment template that contains instructions to bypass Microsoft's Protected View.



Malicious Emotet Excel document

Source: BleepingComputer

When a file is downloaded from the Internet, including as an email attachment, Microsoft will add a special Mark-of-the-Web (MoTW) flag to the file.

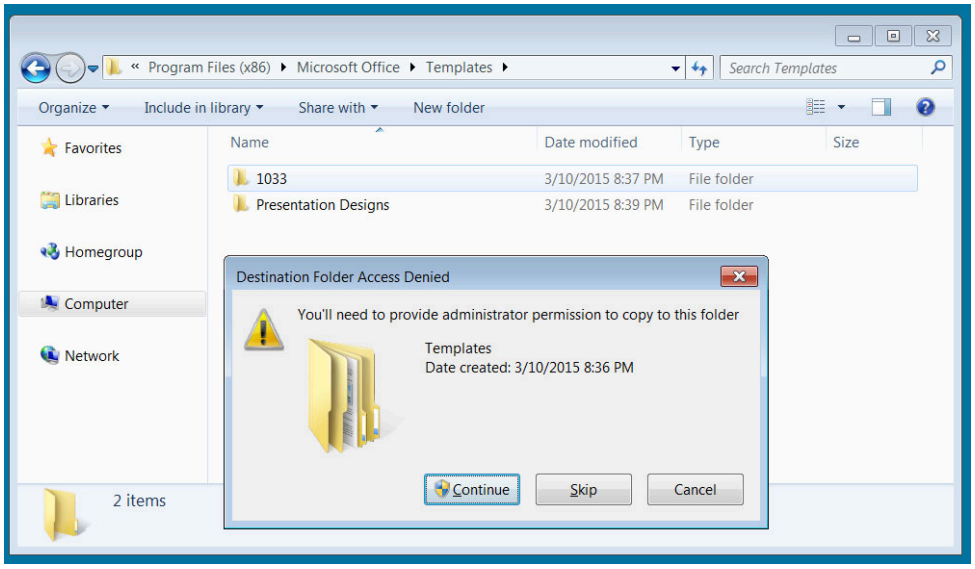
When a user opens a Microsoft Office document containing a MoTW flag, Microsoft Office will open it in Protected View, preventing macros that install malware from being executed.

However, in the new Emotet Excel attachment, you can see that the threat actors are instructing users to copy the file into the trusted 'Templates' folders, as doing this will bypass Microsoft Office's Protected View, even for files containing a MoTW flag.

```
 "RELAUNCH REQUIRED In accordance with the requirements of your security policy, to display the contents of the document,

for Microsoft Office 2013 x32 and earlier - C:\Program Files\Microsoft Office (x86)\Templates
for Microsoft Office 2013 x64 and earlier - C:\Program Files\Microsoft 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"
```

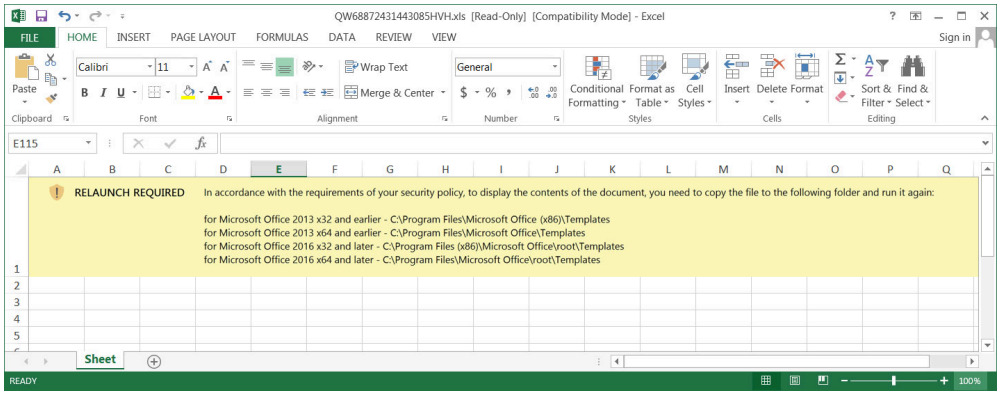
While Windows will warn users that copying a file into the 'Templates' folder requires 'administrators' permissions, the fact that a user is attempting to copy the file indicates that there is a good chance they will also press the 'Continue' button.



Requesting administrator permissions

Source: BleepingComputer

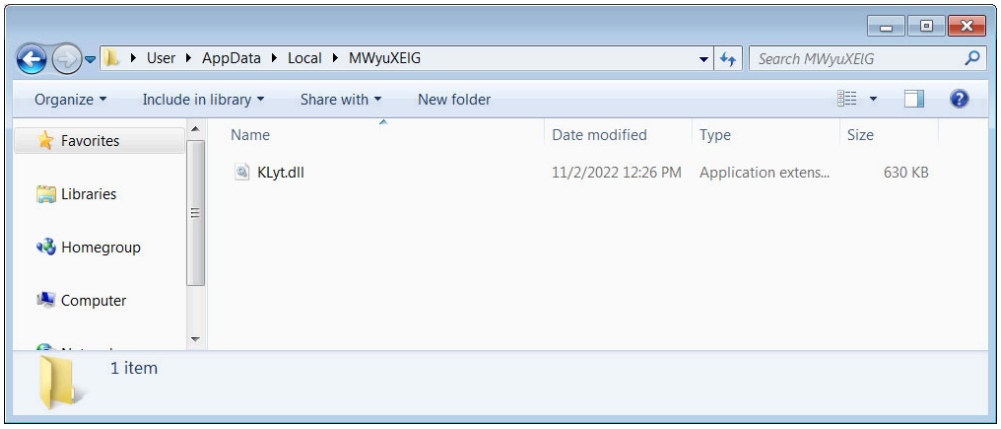
When the attachment is launched from the 'Templates' folder, it will simply open and immediately execute macros that download the Emotet malware.



Bypassing Microsoft Office Protected View

Source: BleepingComputer

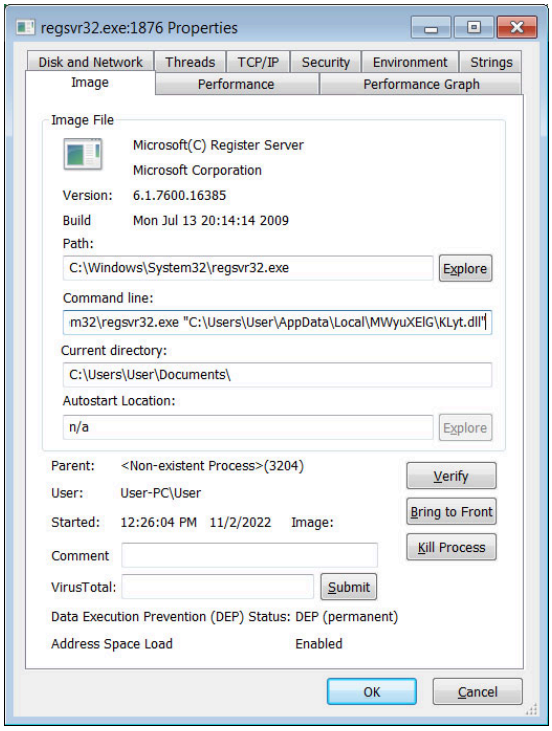
The Emotet malware is downloaded as a DLL into multiple random-named folders under %UserProfile%\AppData\Local, as shown below.



Emotet stored in a random folder in %LocalAppData%

Source: BleepingComputer

The macros will then launch the DLL using the legitimate regsvr32.exe command.



Emotet DLL running via Regsvr32.exe

Source: BleepingComputer

Once downloaded, the malware will quietly run in the background while connecting to the Command and Control server for further instructions or to install additional payloads.

Madjar told BleepingComputer that today's Emotet infections have not begun dropping additional malware payloads on infected devices.

However, in the past, Emotet was known for installing the TrickBot malware and, more recently, Cobalt Strike beacons.

These Cobalt Strike beacons are then used for initial access by ransomware gangs who spread laterally on the network, steal data, and ultimately encrypt devices.

Emotet infections were used in the past to give Ryuk and Conti ransomware gangs initial access to corporate networks.

Since Conti's shutdown in June, Emotet was seen partnering with the BlackCat and Quantum ransomware operations for initial access on already infected devices.

Update 11/3/22: This article originally said spamming stopped on June 13th. Correct date is July 13th.
