Netskope Threat Coverage: The Return of Emotet

By Gustavo Palazolo

Published: 2021-11-18 · Archived: 2026-04-06 00:21:02 UTC

Co-authored by Gustavo Palazolo and Ghanashyam Satpathy

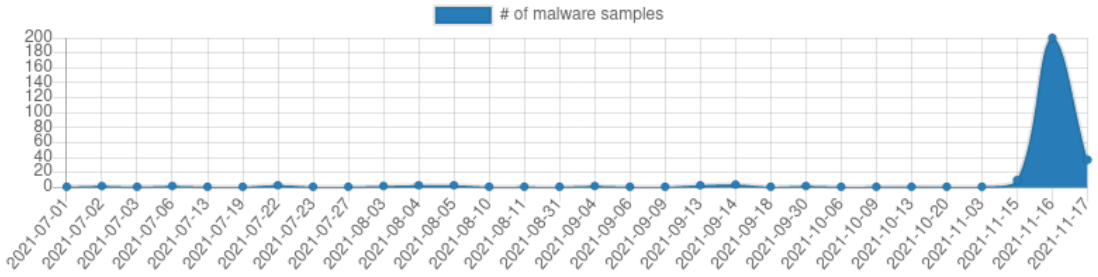
Summary

At the beginning of 2021, Emotet was considered to be the world's most dangerous malware by Europol. The threat was first discovered in 2014 when it was acting as a banking trojan. Over the years, the malware evolved into one of the most relevant botnets in the threat landscape, often used to deliver other threats, such as Trickbot and Ryuk ransomware. Netskope detected Emotet during Oct 2020, using PowerShell and WMI to download and execute its payload.

After massive collaboration between law enforcement agencies around the world, Emotet was taken down in January 2021, where the malware's infrastructure was disrupted from the inside. This was extremely important, as infected machines were redirected towards law enforcement-controlled infrastructure, preventing further actions from Emotet's threat actors.

After almost a year, Emotet (a.k.a. Geodo, Heodo) was spotted again in the wild, being delivered by Trickbot. This new campaign is being tracked by MalwareBazaar / Feodo Tracker, where we can see an increase since November 15, 2021.

Tag:	Emotet Alert
Firstseen:	2020-03-19 18:51:04 UTC
Lastseen:	2021-11-17 14:12:32 UTC
Sightings:	69'953
Malpedia:	https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet

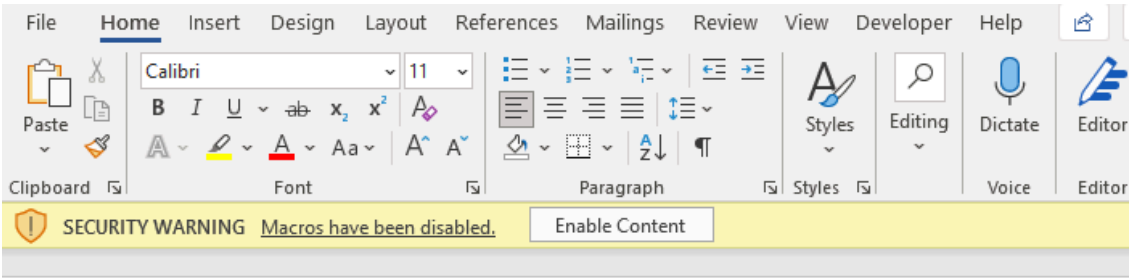


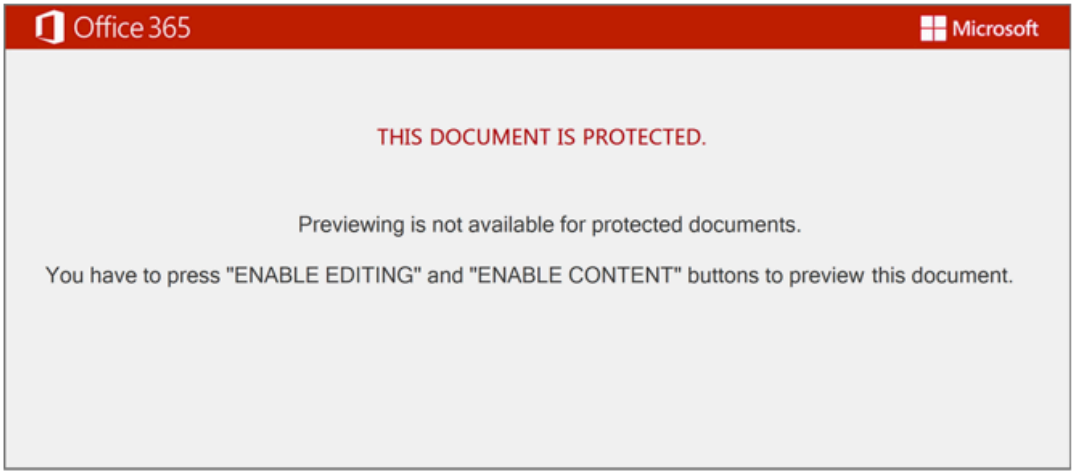
Screenshot of Emotet tracker from MalwareBazaar.

In this threat coverage, we will analyze a malicious Microsoft Office document from a set of files that are delivering the new Emotet payload.

Analysis

Once we open the document, we can see a fake message that lures the victim into enabling the macros, by clicking the “Enable Editing” and “Enable Content” buttons.





Malicious document that delivers Emotet.

The threat actors protected the VBA project with a password to prevent viewing the macro in the VBA editor, likely to slow down analysis.

Protected VBA project.

After bypassing this protection, we can see that the document contains an obfuscated macro code.

Macro code executed by the document.

There are a few functions that are not used at all, possibly added as decoys. The main code is triggered by the “ `Document_Open()` ” function.

Function triggered once the document is opened.

By looking at the function called by this entry point, we can see the threat actors attempt to hide a PowerShell script by using string concatenation and replace, which can all be easily removed.

The VBA code goal is to execute a PowerShell script, that basically iterates over a URL list, and tries to download the content into “ `C:\ProgramData\` ”.

Prettyfied PowerShell script executed by the malicious document.

Once an online URL is found, Emotet's DLL is written into the disk with a random name, for example: "`C:\ProgramData\1856230245.dll`".

At the time of our analysis, three of the URLs were offline.

Online and Offline URLs from Emotet's document.

The downloaded file is a 32-bit DLL, and although this information is not 100% reliable, it looks like the file was compiled on November 16, 2021.

Emotet’s payload downloaded by the malicious document.

The final payload is another DLL, which is unpacked and executed in memory by the downloaded file.

Emotet being unpacked in memory.

Once running, Emotet starts the communication with its C2 servers.

Emotet C2 communication.

At the moment of this analysis, there are 19 online servers linked to Emotet.

Protection

Netskope Threat Labs is actively monitoring this campaign and has ensured coverage for all known threat indicators and payloads.

- **Netskope Threat Protection**
  - `Document-Word.Trojan.Emotet`
  - `Win32.Trojan.Emotet`
- **Netskope Advanced Threat Protection** provides proactive coverage against this threat.
  - `Gen.Malware.Detect.By.StHeur` indicates a sample that was detected using static analysis
  - `Gen.Malware.Detect.By.Sandbox` indicates a sample that was detected by our cloud sandbox

IOCs

Emotet Document Hashes

SHA256

4938ef80579abd3efdb5caa81ccd37648e771dfcd8eb6fb59789faf5c29002d9

fcdc52a70e95e9e1979db1a9145ca43135ad7b1497a6c62b606989734680cd5d

eeabaea8e1a978fb94bbb03a4dd20c9259c9a65bdaee42ab5a777ca1ccba27a0

7ba276ef23853e8a1bc1b32b8fa67ff845d9fa78c2820aa68c4907aead76fd06

MD5

97b18705eb20d678681e39cc877b3d2a

93288048b2d674437e5d8adcf13d1169

7d987aac2dba9450640fb15d860be5dc

356252e7a07ec1a807795cfb77629ea7

The full list of IOCs analyzed in this campaign can be found in our Git repository.
