Trends in the Recent Emotet Maldoc Outbreak

fortinet.com/blog/threat-research/Trends-in-the-recent-emotet-maldoc-outbreak

April 18, 2022

Emotet is a malware family that steals sensitive and private information from victims' computers. The malware has infected more than a million devices and is considered one of the most dangerous threats of the decade.

In addition to analyzing threats, FortiGuard Labs also focuses on how malware spreads. We have observed that the recent Emotet outbreak is being spread through a variety of malicious Microsoft Office files, or maldocs, attached to phishing emails. Once a victim opens the attached document, a VBA Macro or Excel 4.0 Macro is used to execute malicious code that downloads and runs the Emotet malware.

In this blog, we will focus on what these malicious documents look like and how they drop Emotet malware onto a victim's local disk. We will first look at the samples captured in this campaign and then examine their propagation trends.

Affected Platforms: Microsoft Windows
Impacted Users: Windows users
Impact: Controls victim's device and collects sensitive information
Severity Level: Critical

Phishing Emails with Malicious Attachment

The recent Emotet outbreak uses phishing emails combined with social engineering to trick victims into loading the malware onto their devices. These emails often include "Re:" or "Fw:" in the subject line, as shown in Figure 1 and 2, to disguise the email as a reply or forwarded message to help convince the target that the email is legitimate.

Figure 1: Reply email with an attachment

Figure 2: Forwarded email with .xls file attachment

Figure 3 showcases another technique, where the malicious document is packed into a ZIP archive with a password that is attached to an email, with the password included in the body of the text.

Figure 3: Email with a password-protected ZIP archive attachment

Examining the Malicious Excel Files and Word Documents

The attached Excel files and Word documents contain malicious macros. Once opened, they display an image requesting the victim to click the "Enable Content" button in the security warning bar. This enables the malicious macro to be executed.

The images below show the techniques used to trick victims into clicking the "Enable Content" button in the Excel files and Word documents used in this campaign. Figure 4 shows screenshots of an opened Word document and Figure 5 is of the opened Excel file.

Figure 4: Word document content when opened

Figure 5: Excel file content when opened

Analyzing the Malicious Macros and their Behaviors

Macros in Microsoft Office files are usually written in VBA (Visual Basic for Applications). In this case, the Word documents contain malicious VBA code while the Excel files use Excel 4.0 Macro in addition to VBA Macro.

We captured five different samples connected with this Emotet campaign that contain differences in the macro code and execution flow. For identification purposes, we have given each sample a tag name, which is from when the sample first appeared. The tag name

consists of two parts, the year prefix and a suffix with the week of the month, connected by an underscore.

The first sample appeared in the third week of November 2021 and its tag name is "2021_NovW3". It is an Excel file or Word document with VBA Macro. The second is an Excel file using Excel 4.0 Macro. It appeared in the fourth week of November 2021 with the tag name "2021_NovW4". The third sample is a Word document with a VBA Macro with the tag name of "2021_DecW2". The fourth sample is an Excel file with an Excel 4.0 Macro. It's tag name is "2021_DecW4". The fifth sample is an Excel file with a VBA Macro and the tag name of "2022_FebW2".

Tag Name	File Type	Macro Type
2021_NovW3	Excel/Word	VBA Macro
2021_NovW4	Excel	Excel 4.0 Macro
2021_DecW2	Word	VBA Macro
2021_DecW4	Excel	Excel 4.0 Macro
2022_FebW2	Excel	VBA Macro

Below is an analysis of the malicious macro component of each captured sample.

2021_NovW3:

This sample has a VBA function called "Workbook_Open()" or "Document_Open()" that is executed automatically when the file is opened. It then calls another function to write script data to a VBS file and save it in the "C:\ProgramData\" folder. Next, it uses "Wscript.exe" to execute the VBS file.

Figure 6: VBA code used to execute the dropped VBS file

In the VBS file it generates a PowerShell code snippet to download the Emotet malware dll into the "C:\ProgramData\" folder and then execute it using "regsvr32.exe".

Figure 7: Script code in the dropped VBS file

2021_NovW4:

This is an Excel file that uses formulas on an Excel 4.0 Macro sheet instead of a VBA Macro to execute malicious code. As shown in Figure 8, some sheets are hidden, including the one that contains the malicious formulas. Cell A1 in sheet "FEGFL" is named "Auto_Open" and includes a built-in macro that automatically runs the formula from that cell once the file is opened.

This macro sheet includes formulas that call the API "URLDownloadToFileA" to download the Emotet malware from different URLs. It attempts to download the Emotet malware from the URL in each formula until a download is successful. The Emotet malware is a dll file saved with an .ocx file extension and executed using "regsvr32.exe".

Figure 8: The Macro Sheet is hidden and cell A1 is named "Auto_Open"

2021_DecW2:

This VBA code includes a function called "AutoOpen()" that automatically runs a macro when the document is opened. In this function, it saves itself as an HTA (HTML Application) file in text format, as shown in Figure 9. At the same time, script data is displayed in the content text area below the picture that is hidden with a minimum font size and white font color (the font color has been changed to red in Figure 9 for easier viewing). Since the HTA file is in text format, the script data in the content text area is the only part included in the file. To execute the HTA file, "explorer.exe" on Windows system is used in the VBA Macro.

Figure 9: VBA code to save ActiveDocument as HTA file

Figure 10: VBA code to execute the dropped HTA file

Script code in the HTA file extracts JavaScript code to download the Emotet malware. The Emotet malware is saved to the "C:\Users\Public" folder as a JPG file, but it is actually a dll file. In the end, the Emotet malware dll is executed with "rundll32.exe".

Figure 11: Script code in the HTA file

2021_DecW4:

In the hidden macro sheet "Macro1", cell F1 is named "Auto_Open" to automatically run the formula when the file is opened. There is normal text in the cells below cell F1 until cell F18, which contains the formula to execute. The simple formula, shown in Figure 12, uses "mshta.exe" to execute an HTML URL. The web page of HTML URL is protected by HTML Guardian, a tool that encrypts source code.

Figure 12: Formula and "Auto_Open" in macro sheet

After decrypting the HTML source code, there is a VBScript code snippet obfuscated by the string "{GOOGLE}", as shown in Figure 13. It runs a PowerShell code snippet to download and execute script from a PNG URL. The PNG URL is not an image file but a PowerShell

script file that contains multiple URLs to download Emotet malware. Finally, the Emotet malware is saved as a dll file in the "C:\Users\Public\Documents\" folder and executed using "rundll32.exe".

Figure 13: VBScript code used to run a PowerShell script

2022_FebW2:

This sample has the same code and execution flow as "2021_DecW4". But instead of using an Excel 4.0 Macro, it uses a VBA Macro to execute its malicious behaviors. Figure 14 shows the content in the autorun function "AutoOpen()". Although there are lots of comments, the VBA code is very simple, using "mshta.exe" to execute an HTML URL. As the script code and subsequent process in the HTML URL is identical to the contents in "2021_DecW4", we can look at it for more details.

Figure 14: VBA code that an HTML URL is executed

Attack Trends in the Latest Emotet Campaign

Emotet was first discovered in 2014 and continues to attack victims. The latest Emotet campaign broke out in mid-November of 2021 and is spread using malicious documents attached to phishing emails. FortiGuard Labs has been tracking these malicious documents as well as the number of variants used to evade detection in this campaign. Figure 15 shows the daily timestamps for Emotet maldocs used from mid-November 2021 to March 2022. All the samples mentioned in the previous section emerged during this period.

The first attack appeared on November 16, 2021. After that, it spread different types of malicious documents every week until the Christmas break. Once the break ended on January 12, it surged with more frequent and consistent attacks, releasing a large number and variety of malicious documents. From the end of February through the end of March, it turned to using the same type of malicious document (2021_NovW4) with different phishing picture templates. After February 28th, new malicious documents appeared every day except for weekends, with only one or two days off.

Figure 15: Timeline of the latest Emotet Maldoc campaign

Conclusion

In the previous section, we showed that some types of malicious documents have more timestamps on the timeline than others. The pie chart in Figure 16 is based on the occurrence frequency of timestamps, showing the usage rate of each malicious document in this campaign. According to this chart, "2021_NovW4" has been the most active, involving more than 50% of the malicious documents discovered. The second most is "2021_NovW3", consisting of 27% Excel files and 6% Word documents. It is worth mentioning that Excel files

accounted for 93% of all malicious documents, much higher than Word documents at only 7%. One of the possible reasons is that the Excel 4.0 Macro only works with Excel files. Because if this, users should be especially cautious about suspicious emails with an attached Excel file from an unknown sender.

Figure 16: Types of malicious documents in the campaign

FortiGuard Labs also collected the Emotet malware payloads during this period. Figure 17 shows the weekly counts of Emotet malware, with timestamps for each Emotet maldoc in the timeline displayed below the bar chart. Weeks with high counts match when malicious documents appeared, while those without malicious documents were almost silent.

Figure 17: Count of Emotet malware per week

The graph also shows that all malicious documents detected after Christmas were Excel files. Using an Excel file is more flexible because its macro type can be VBA Macro, Excel 4.0 Macro, or both. One of the benefits is that Excel 4.0 Macro, an older technique, bypasses antivirus detection more easily than a VBA Macro.

As shown in the timeline, Emotet malware has primarily been spread since March 2022 through the malicious Excel file "2021_NovW4", which uses the Excel 4.0 Macro. We believe that the authors prefer to use Excel files with Excel 4.0 Macro for malicious documents to reduce detection by antivirus engines.

Fortinet Protections

Fortinet customers are protected from this malware by FortiGuard's Web Filtering, AntiVirus, FortiMail, FortiClient, FortiEDR, and CDR (content disarm and reconstruction) services:

The malicious macros inside the Excel sample can be disarmed by the FortiGuard CDR (content disarm and reconstruction) service.

FortiEDR detects the Word and Excel files and Emotet dll file as malicious based on their behavior.

Fortinet customers are protected from these malicious documents and malware by FortiGuard AntiVirus, which is included in FortiMail. It detects all malicious macro file types, including Excel 4.0 Macro samples.

All malicious documents described in this report are detected by FortiGuard AntiVirus as follows:

VBA/Agent.8095!tr.dldr
VBA/Agent.5A47!tr
VBA/Bomber.46B3!tr.dldr

XF/Agent.NN!tr.dldr
XF/CoinMiner.Z!tr
MSExcel/Agent.DVP!tr.dldr
HTML/Sabsik.FL!tr

The Emotet malware payloads are detected by FortiGuard AntiVirus as follows:

W32/Emotet.EHR!tr
W32/GenKryptik.FSPR!tr
W32/Emotet.1156!tr
W32/Agent.FSUQ!tr
W32/Kryptik.HNXJ!tr
W32/Emotet.1143!tr
W32/Emote.CQ!tr

In addition, Fortinet has multiple solutions designed to train users on how to understand and detect phishing threats:

The FortiPhish Phishing Simulation Service uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and to train and reinforce proper practices when users encounter targeted phishing attacks.

We also suggest that organizations have their end users go through our FREE NSE training: NSE 1 – Information Security Awareness. It includes a module on Internet threats to train end users on how to identify and protect themselves from phishing attacks.

IOCs

Malicious documents (SHA256):

3e97f09fc53890ba2d5ae2539b5c8df372ed2506ed217d05ff2cf8899d15b8e6
2ecc2a48fa4eadb80367f69799277c54a0fe6dd2220a6a2dd7b81cfba328ed19
ed180371dfec2186148bbcab99102ce45fb1fcc3764b384c2abcaceba2fa65b6
719900e330cecd87250ac1f6c31f2d6f42f226294fb011cf47c442f8d2b7455b
3ccb809cd97cc08ff380600dcaa5244ef2abd7afd9e7a9f2df7c4e28fee637f0
e167804a6f36dc99e96909bcededa8a733dd8633037b8b52e8d7881d20446c16
bd9b8fe173935ad51f14abc16ed6a5bf6ee92ec4f45fd2ae1154dd2f727fb245
57fcbb058fc0dfe0cce29676569f2e30d1f8a59345ab161d8183d0769428f4e2

Emotet malware (SHA256):

4900d1e66cef8507b265c0eec3ff94cb5f774847d969e044dc8ccd72334181f5
2dcfcaaf3ccd8e06043e651cd5b761ae50f3463c6420d067b661969e0500dce2
52f6fce27184b61ceb3c02d360e04dc1489c4136a0ffcbb39c50d27474e4283b
ccbefa930edc4d5b5b34a5dea16c73c9d3f3b4167406c3ae841bc71fce45c68e
cd105196cbf17f11dbff2b623f5bfaf9ef8d91f2598fe3bc2a7da192c2cee457
9535c3f02ee8a47ad1392f36a1ff44a3d5cb067ecef748e63e1628bc489c9d90
ca2b7c0f2a2a42ce586d63ccfcf131f8b99d73521742cc15d6255e76f9278fbc
d5f4292d4f5661ce12dd8384cfbb22a3d17908290ba80d9de3a1697064d248a7

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.