Emotet Returns, Now Adopts Binary Padding for Evasion

trendmicro.com/en_no/research/23/c/emotet-returns-now-adopts-binary-padding-for-evasion.html

March 13, 2023

Overview

Following a three-month hiatus, Emotet spam activities resumed in March 2023, when a botnet known as Epoch 4 began delivering malicious documents embedded in Zip files that were attached to the emails.

We have been tracking the threat actor’s efforts to deploy new command-and-control (C&C) infrastructure, where we detected activity spikes in January and February.

Date (2023)	Count
January 25	2
January 26	9
January 27	10
February 6	6
February 7	24
February 28	1
March 1	37
March 6	6
March 7	9

Table 1. Emotet C&C Server Infrastructure deployments during the early parts of 2023

Infection chain

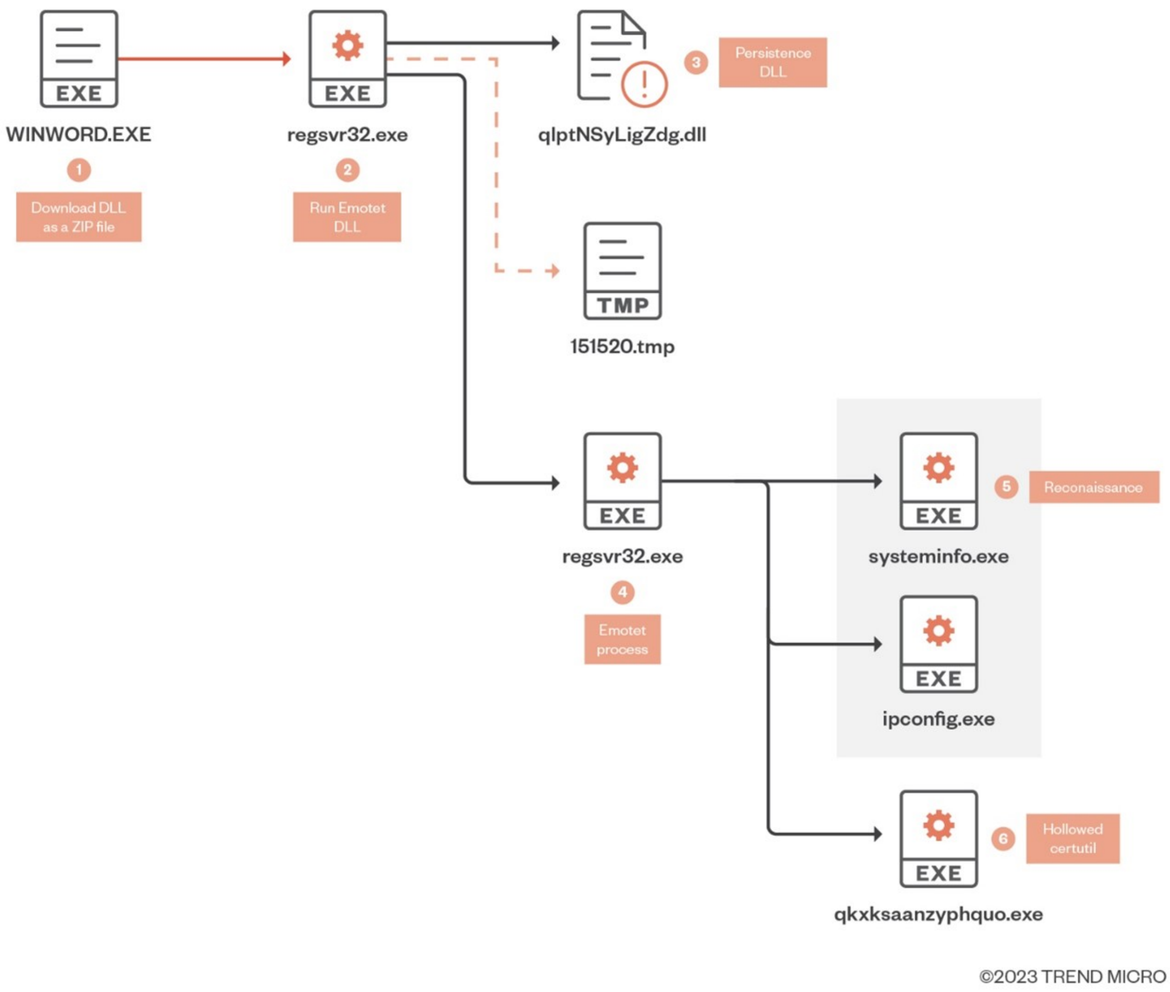
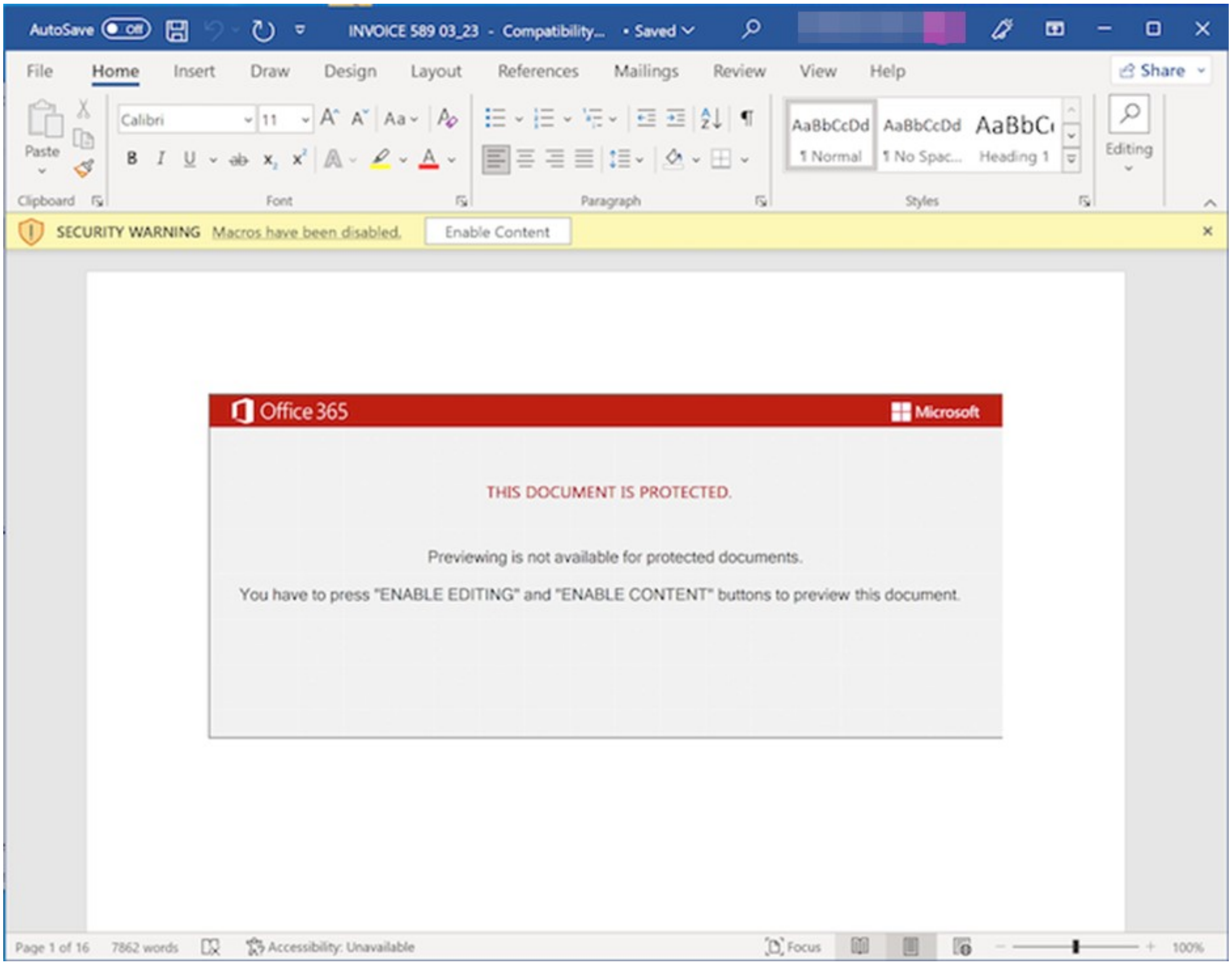


Figure 1. Sample infection chain

The threat actors behind Emotet continue to use malicious documents containing macros to deliver the malicious payload. Note that while Microsoft disabled macros from the internet by default in 2022, the document template employs social engineering techniques to trick users into enabling macros to allow the attack to proceed as intended.

The threat actors behind these emails have adopted the use of binary padding as an evasion technique, where both the dropper document and the Emotet DLL files are inflated to 500+ megabytes to avoid security solutions. Other similar defense evasion techniques have previously been observed being used by other malicious actors.



SECURITY WARNING Macros have been disabled. Enable Content

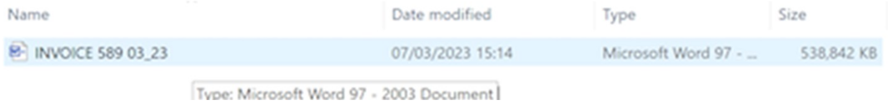
Office 365 Microsoft

THIS DOCUMENT IS PROTECTED.

Previewing is not available for protected documents.

You have to press "ENABLE EDITING" and "ENABLE CONTENT" buttons to preview this document.

Figure 2. Malicious document prompting the user to enable macros



Name	Date modified	Type	Size
INVOICE 589 03_23	07/03/2023 15:14	Microsoft Word 97 - ...	538,842 KB

Type: Microsoft Word 97 - 2003 Document

Figure 3. Malicious document with a file size of approximately 500MB

Once a user enables macros for the malicious document, it will download a ZIP file will from one of seven hardcoded and obfuscated URLs (which will be iterated through until the file is successfully retrieved):

- hxxps://midcoastsupplies.com[.]au/configNQS/Es2oE4GEH7fbZ/
- hxxp://mtp.evotek[.]vn/wp-content/L/
- hxxp://www.189dom[.]com/xue80/C0aJr5tfI5Pvi8m/
- hxxps://esentai-gourmet[.]kz/404/EDt0f/
- hxxp://139.219.4[.]166/wp-includes/XXrRaJtiutdHn7N13/
- hxxps://www.snaptikt[.]com/wp-includes/aM4Cz6wp2K4sfQ/
- hxxps://diasgallery[.]com:443/about/R/

The macro will then check if the response is 200 (indicating a success retrieval of the file). If so, it will then check if that file is either a PE File or a Zip file, suggesting that the threat actors may adopt alternative file formats to Zip files containing binary padded PE files.

The macro uses a function that checks the file type of the downloaded payload by examining the first two bytes of the file. It first checks if the first two bytes are equal to the ASCII values of "M" and "Z" (77 and 90, respectively). If so, it returns a value of 1, indicating that the file is a PE file. On the other hand, if the first two bytes are not equal to "M" and "Z," the function checks if they are equal to the ASCII values of "P" and "K" (80 and 75, respectively). If so, it returns a value of 2, indicating that the file is a Zip file.

The CopyHere() method of the Shell32.FolderItems object is then used to extract the contents of the Zip file to the destination folder, after which the macro deletes the temporary folder files.

Finally, regsvr32.exe is invoked and the DLL is loaded with the /s switch to silently execute the Emotet payload to infect the endpoint.

Stealer and spam routines

For its stealer and spam routines, Emotet will make a copy of certutil.exe (a legitimate command-line tool) in the temporary directory that starts in a suspended state and then hollowed out.

The malware will then load one of several modules such as NirSoft's Web Browser PassView and Mail PassView tools, an Outlook stealer, and a spam module before resuming execution. Note that we have not observed any second stage payloads outside of Emotet’s stealer and the spam modules. However, it is possible that payloads (such as backdoors and/or other information stealers) might be dropped in the future to enable access for other threat actors.

Evasion techniques

Binary padding is used to inflate file sizes so that they exceed the size limitations imposed by anti-malware solutions such as sandboxes and scan engines. In this example, the Emotet DLL is padded with 00 bytes in the overlay, inflating the PE file from 616KB to 548.1MB.

For Emotet, both the dropper document and the PE files use the 00-byte padding technique to inflate the file size. Malicious actors use Zip compression to transport the relatively small files via email and HTTP, before decompression is used to inflate the files to evade security solutions.

Finally, reconnaissance activities are performed either via IP configs or through the affected machine’s system information.

Conclusion and recommendations

Emotet has been a prolific and resilient threat, even surviving a takedown of its infrastructure in 2021. Given what we've seen of Emotet over the years, it would not be surprising to see it evolve further in future attacks, employing alternative malware delivery methods, adopting new evasion techniques, and integrating additional second and even third-stage payloads into its routines.

To avoid getting infected by malicious spam emails, users should be cautious of emails from unknown senders or with suspicious subject lines. These types of emails are often paired with social engineering techniques that are designed to get recipients to click on a link or download an attachment containing malware. Users should also ensure that macros are disabled in Microsoft Office applications and avoid enabling them even when even prompted. Using spam filters can also help automatically filter out suspicious or unwanted emails before they reach the user's inbox. By following these precautions, both individual users and organizations can greatly reduce the risk of getting infected by malicious spam emails.

Endpoint solutions like Trend Micro's Smart Protection Suites and Worry-Free Business Security solutions offer protection for both users and businesses against threats like Emotet. These solutions come equipped with behavior-monitoring capabilities that enable them to detect malicious files, scripts, and messages. They can also block all related malicious URLs. Additionally, the Trend Micro™ Deep Discovery™ solution includes an email inspection layer that can identify and protect enterprises from malicious attachments and URLs. By leveraging these powerful tools, users and businesses can effectively defend themselves against the damaging effects of Emotet and other similar threats.

Indicators of compromise

The indicators of compromise for this entry can be found here.