Emotet Again! The First Malspam Wave of 2023 | Deep Instinct

By Simon KeninThreat Intelligence ResearcherDeep Instinct Threat Lab

Published: 2023-03-10 · Archived: 2026-04-05 20:00:21 UTC

Earlier this week, on Tuesday, March 7th, Emotet was observed for the first time this year sending new malspam to infect victims. This is significant because the last time Emotet was seen sending malicious spam was in November of 2022. This current wave is different from the one in November, though, including new evasion techniques that we will detail in this blog.

Deep Instinct's Threat Research team has been tracking Emotet over the last year and has written about its periods of silence and reemergence with new tactics. We will continue to track the malware and alert the community to any changes or activity.

- November 17, 2022: Emotet Vacation Is Over: No Rest For The Wicked
- June 9, 2022: Emotet Malware Returns in 2022

The first to observe and tweet about Emotet's return was @ilbaroni_:

Figure 1: First public observation of Emotet's return

Delivery via Thread Hijacking Emails

The delivery method that Emotet used is the same as in November, however, this time the attached zip files are not password protected.

Deep Instinct's Threat Research team observed thread-hijacked emails sent to companies around the globe, including in Japan:

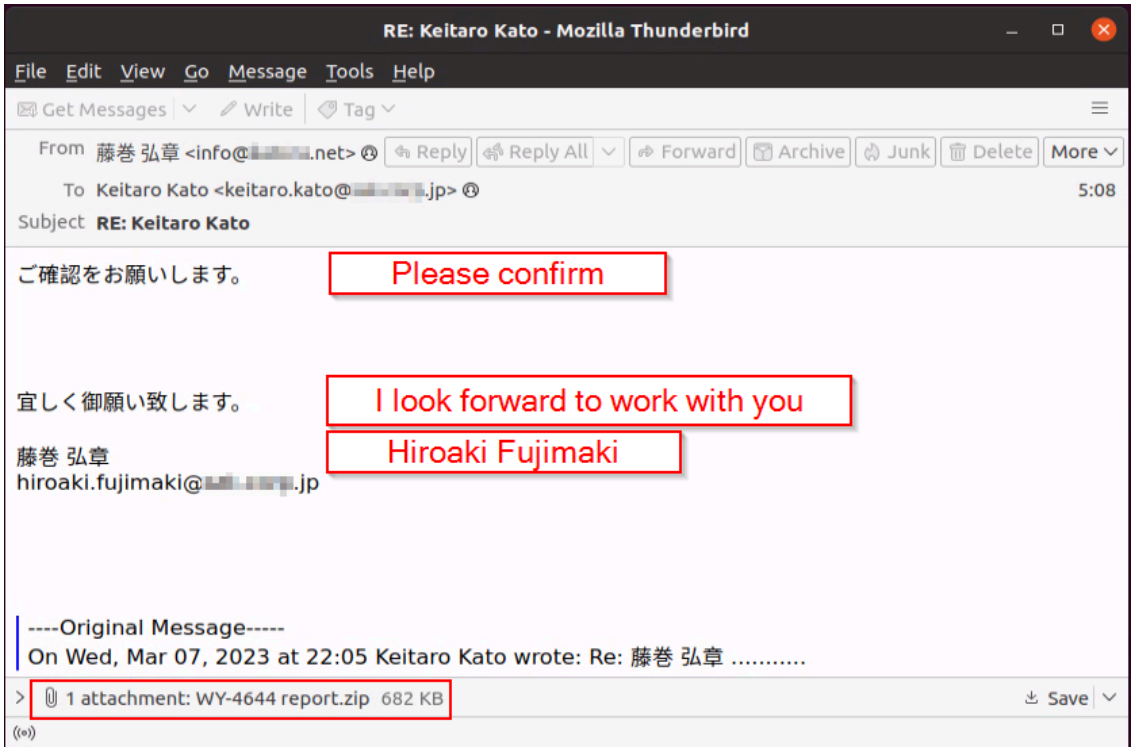

Figure 2: Thread-hijacked mail in Japanese

Changes to Emotet Malspam

In November, Emotet was sending malicious Excel files in the archives. Now Emotet is sending archives with malicious Word files.

The Word files include macros that, if enabled, start the infection chain.

The first page contains an image that tries to lure the receiver to enable macros:

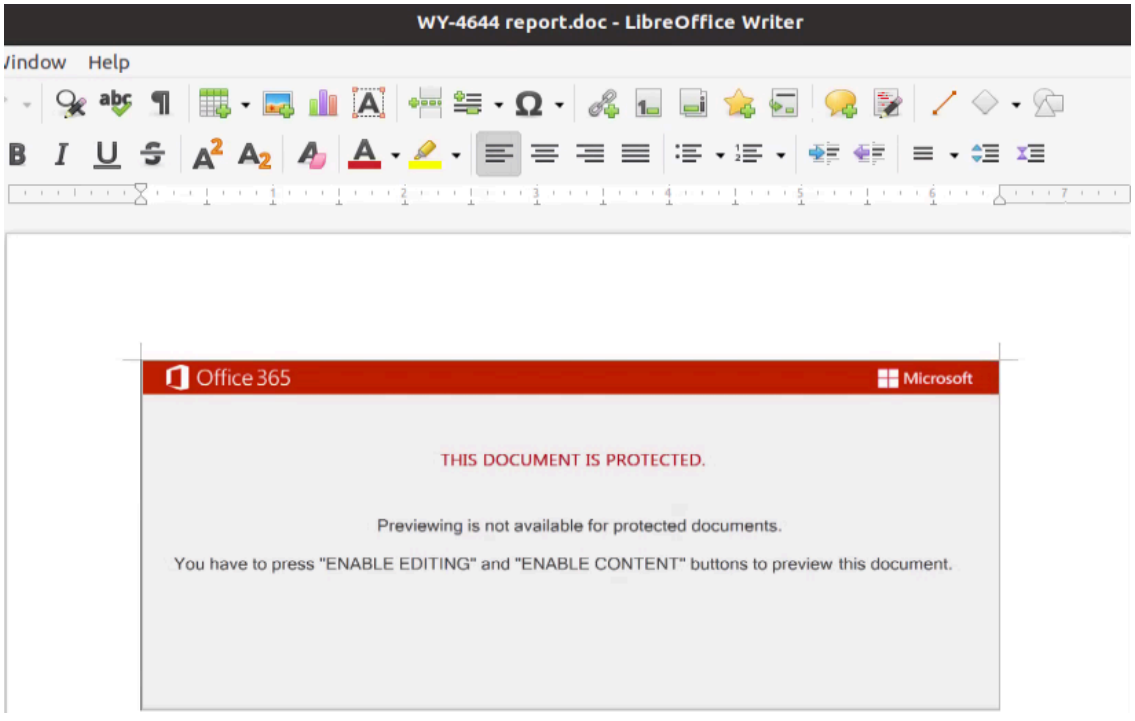

Figure 3: Social engineering lure on first page

The second page is blank, while pages 3-7 are excerpts from the novel "Moby-Dick" which are written in white font to make the pages appear blank.

The whole document has 14,801 characters and 2,587 words; the text is added as part of an evasion technique. Many security tools will classify a Word document with just an image and a macro as malicious, which is true in most cases.

Some people still use macros for legitimate reasons, despite there being little reason to do so with the advances we have made in technology in the 21st century.

Adding textual context to a file with macros might fool some security tools into thinking that the file is benign:

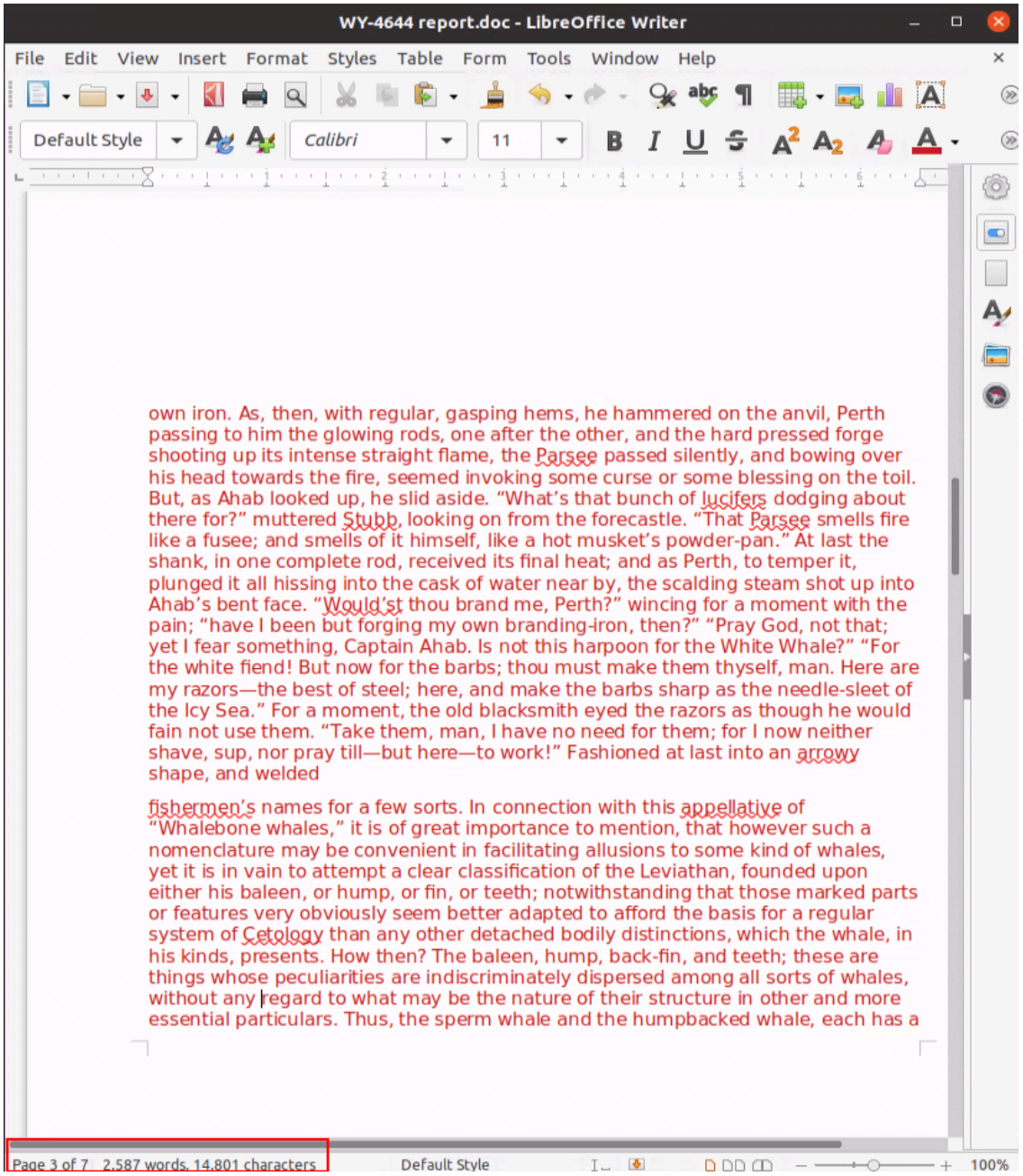

Figure 4: Changing the font color reveals the hidden text

The Word document in the example contains several long and obfuscated macros which download and execute a ZIP file containing the Emotet DLL from one of several compromised websites.

If that's not enough, the most interesting change made by Emotet that it now artificially inflates the size of the Word document to over 500mb:

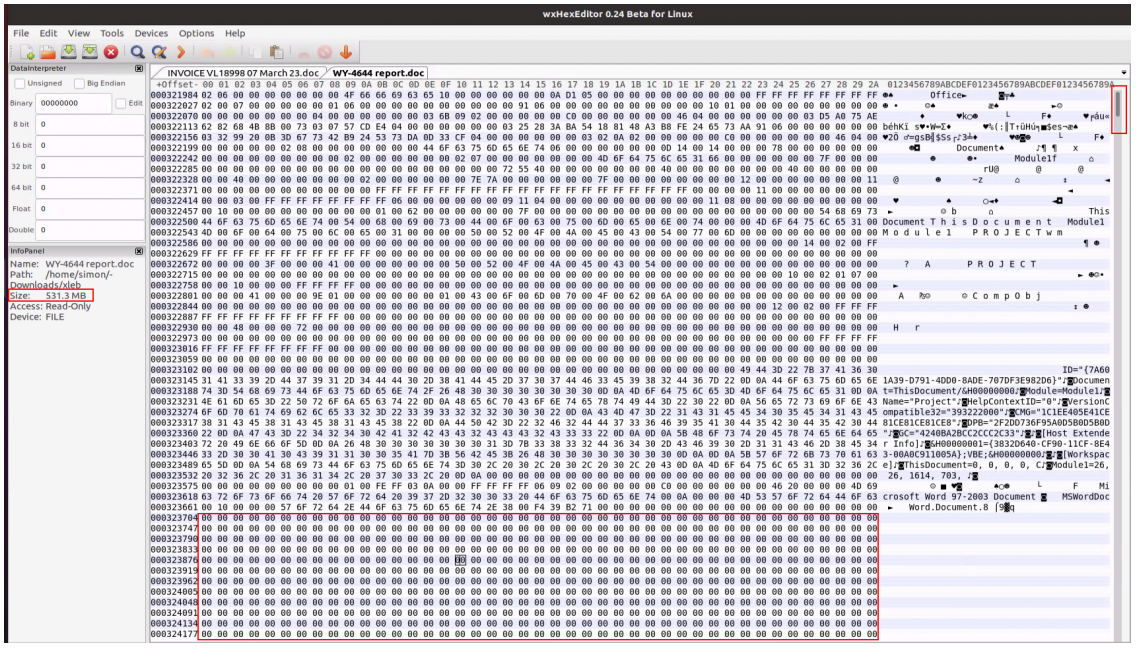

Figure 5: Zero bytes are added to the end of the document.

This is done by simply adding zero bytes at the end of the document. Deep Instinct researchers have seen this technique previously used to inflate the final payloads, such as executables or DLL files.

The result is like the one before, and because the files are so big, many security products and sandboxes don't scan them, which breaks the automatic analysis and IOC extraction.

As mentioned earlier, the macros download a ZIP file from compromised hosts which contain a DLL file which is the Emotet loader. This DLL is also inflated with zero bytes to a file size of over 500mb.

The combination of both the initial attack vector and the payload being artificially inflated might completely blind products that solely rely on static analysis.

Despite these changes the behavior of the loader appears the same.

In the past Emotet used to copy a local version of the certutil.exe; this time Emotet drops a specific version of renamed certutil into "<AppData>\Local\Temp."

The hash of the observed version is: 4224312da8c3a37b95dd78236fca5ca316021c5de6e517d0ddc753ee26932e6a

Emotet is still using process injection, therefore, security products that do not rely solely on static detection have a better chance at stopping the current wave.

IOC

DOC: a13b394e4017c0c77faf4fab6c3aea4de3443f11610cc85a1d677249b9b2bc3a

DLL: efcf59f4423df8fdacbfa8c3d23b6a3e4722bab65c31ea8a7f32daadddfa7adc

For the full list of IOCs (278) visit our GitHub page.
