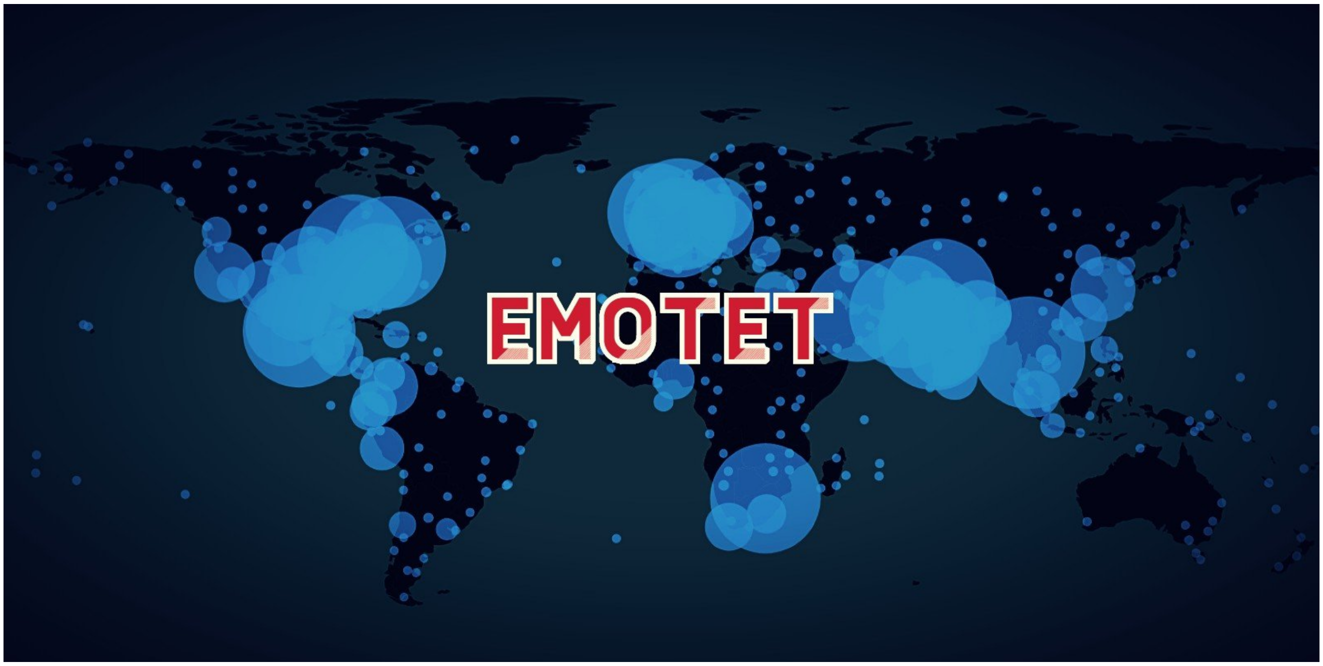
Emotet malware attacks return after three-month break

Lawrence Abrams

By
Lawrence Abrams

- March 7, 2023
- 04:10 PM
- 2



The Emotet malware operation is again spamming malicious emails as of Tuesday morning after a three-month break, rebuilding its network and infecting devices worldwide.

Emotet is a notorious malware distributed through email containing malicious Microsoft Word and Excel document attachments. When users open these documents and macros are enabled, the Emotet DLL will be downloaded and loaded into memory.

Once Emotet is loaded, the malware will sit quietly, waiting for instructions from a remote command and control server.

Eventually, the malware will steal victims' emails and contacts for use in future Emotet campaigns or download additional payloads such as Cobalt Strike or other malware that commonly leads to ransomware attacks.

While Emotet has been considered the most distributed malware in the past, it has gradually slowed down, with its last spam operation seen in November 2022. However, even then, the spamming only lasted two weeks.

Emotet returns in 2023

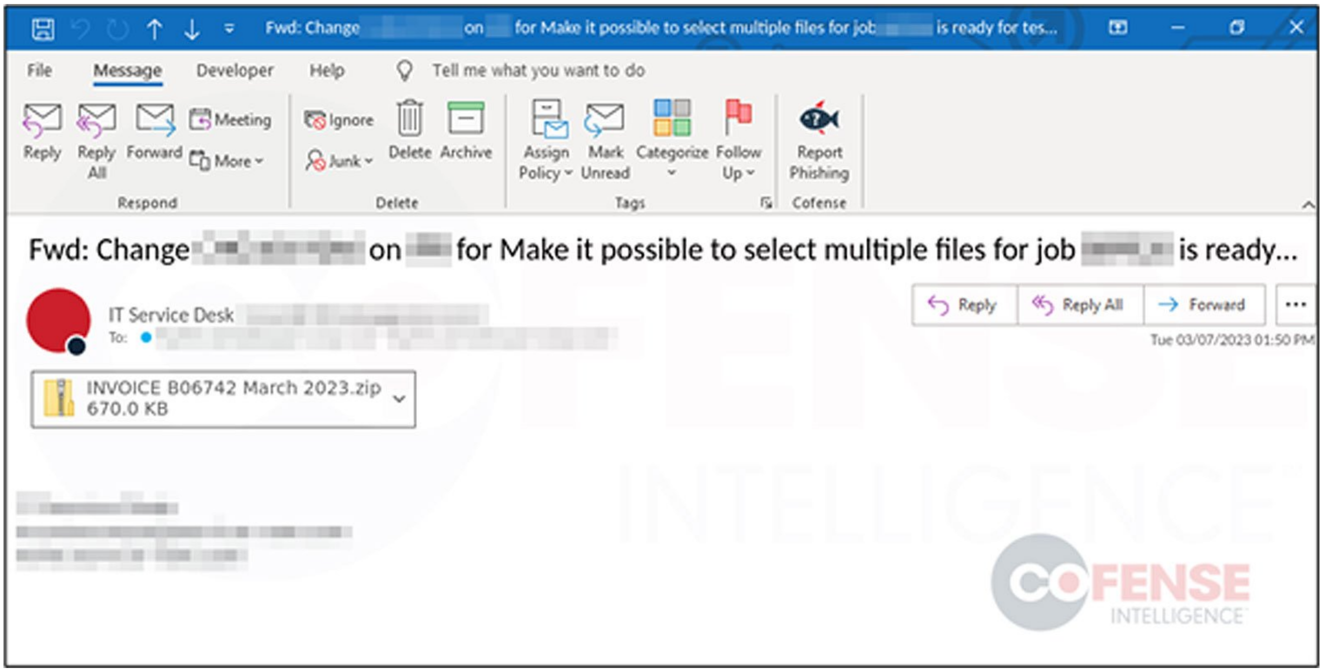
Today, cybersecurity firm Cofense and the Emotet-tracking group Cryptolaemus warned that the Emotet botnet had once again resumed sending emails.

"As of 1200UTC Ivan finally got E4 to send spam. We are seeing Red Dawn templates that are very large coming in at over 500MB. Currently seeing a decent flow of spam. Septet of payload URLs and ugly macros," tweeted Cryptolaemus.

Cofense also confirmed to BleepingComputer that the spam campaign began at 7:00 AM ET, with current volumes remaining low.

"The first email we saw was around 7am EST. Volume remains low at this time as they continue to rebuild and gather new credentials to leverage and address books to target," Cofense told BleepingComputer.

Instead of using reply-chain emails like in the previous campaign, the threat actors are utilizing emails that pretend to be invoices, as shown below.



Fwd: Change [redacted] on [redacted] for Make it possible to select multiple files for job [redacted] is ready...

IT Service Desk [redacted]
To: [redacted]

Tue 03/07/2023 01:50 PM

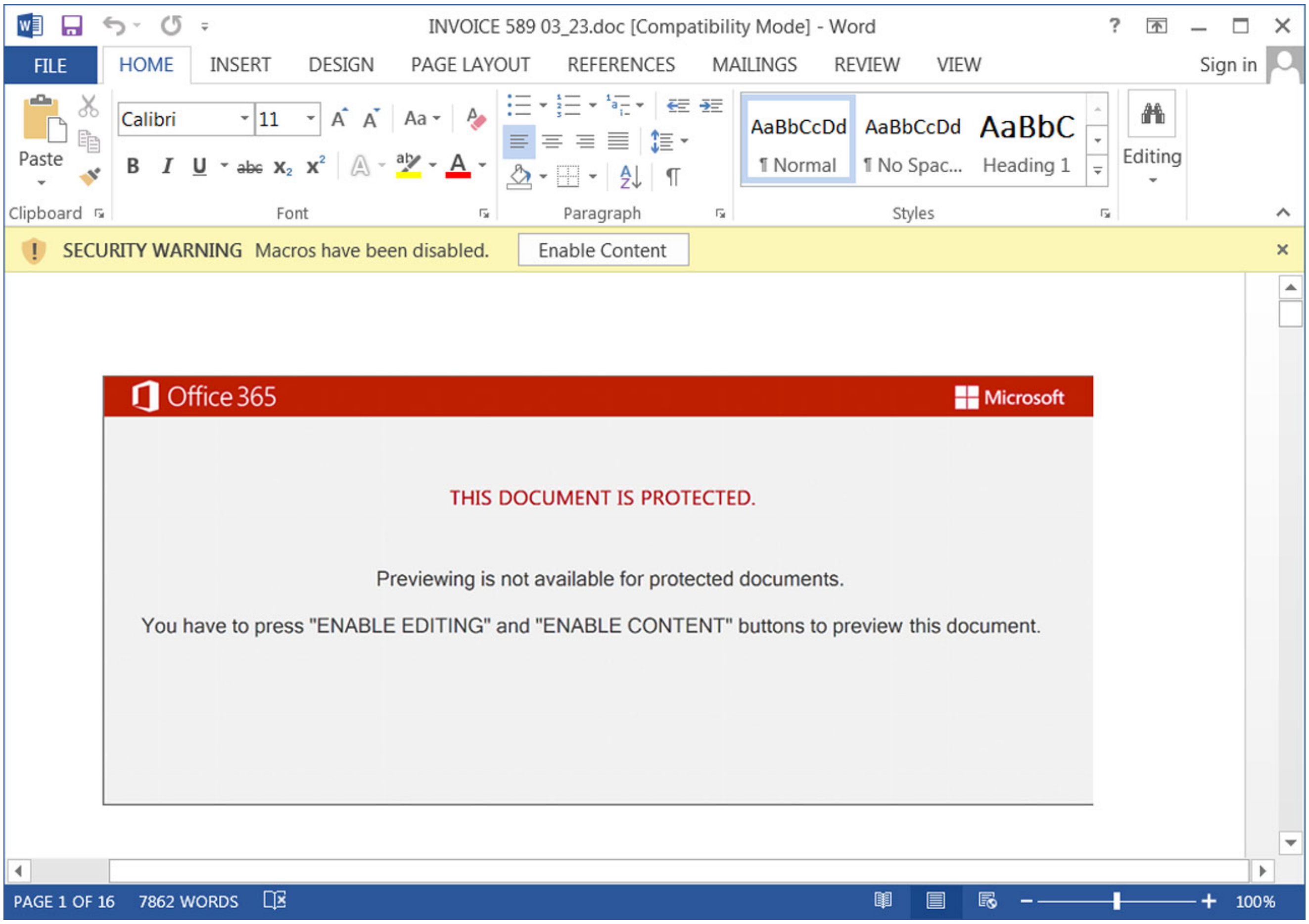
INVOICE B06742 March 2023.zip
670.0 KB

[redacted]

Emotet phishing email
Source: Cofense

Attached to these emails are ZIP archives containing inflated Word documents that are over 500 MB in size. They are padded with unused data to make the files larger and harder for antivirus solutions to scan and detect them as malicious.

These Microsoft Word documents use Emotet's 'Red Dawn' document template, prompting users to enable content on the document to see it correctly.



INVOICE 589 03_23.doc [Compatibility Mode] - Word

SECURITY WARNING Macros have been disabled.

THIS DOCUMENT IS PROTECTED.

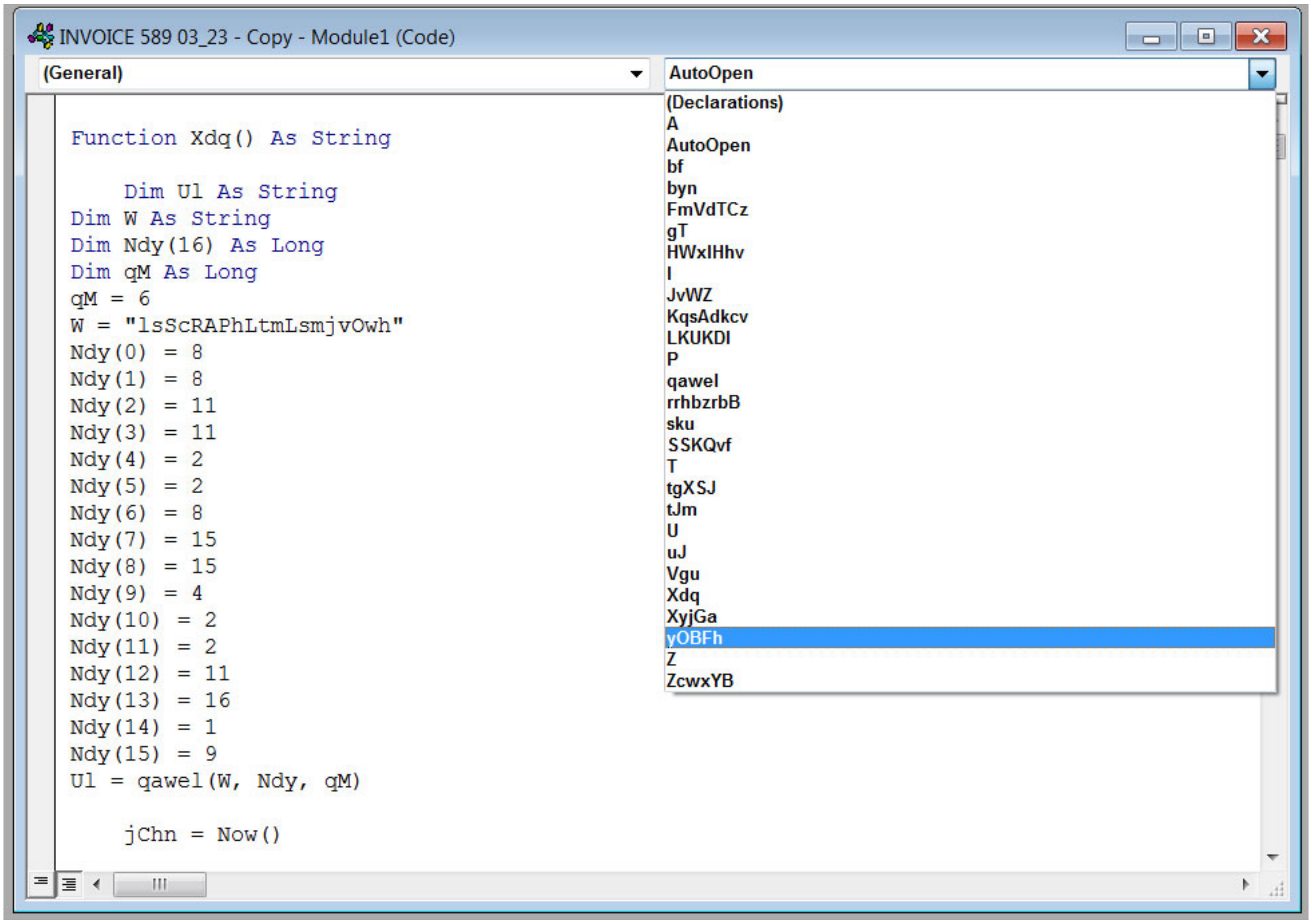
Previewing is not available for protected documents.

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

Malicious Microsoft Word document using the Red Dawn template

Source: BleepingComputer

These documents contain a mess of macros that will download the Emotet loader as a DLL from compromised sites, many of which are hacked WordPress blogs.



```
Function Xdq() As String

    Dim Ul As String
Dim W As String
Dim Ndy(16) As Long
Dim qM As Long
qM = 6
W = "lsScRAPhLtmLsmjvOwh"
Ndy(0) = 8
Ndy(1) = 8
Ndy(2) = 11
Ndy(3) = 11
Ndy(4) = 2
Ndy(5) = 2
Ndy(6) = 8
Ndy(7) = 15
Ndy(8) = 15
Ndy(9) = 4
Ndy(10) = 2
Ndy(11) = 2
Ndy(12) = 11
Ndy(13) = 16
Ndy(14) = 1
Ndy(15) = 9
Ul = qawel(W, Ndy, qM)

    jChn = Now()
```

A mess of malicious macros in an Emotet Word document

Source: BleepingComputer

When downloaded, Emotet will be saved to a random-named folder under %LocalAppData% and launched using regsvr32.exe.

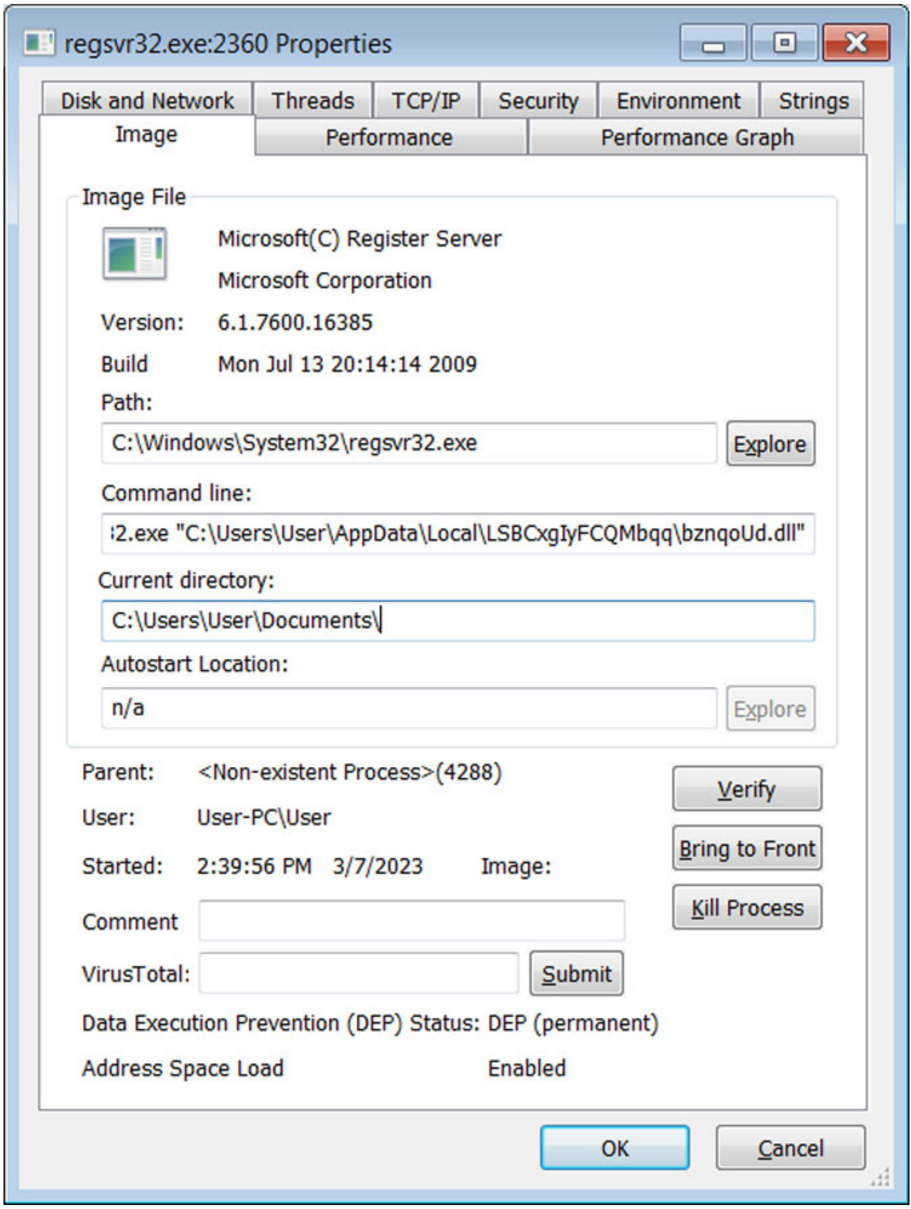


Image File

Microsoft(C) Register Server
Microsoft Corporation
Version: 6.1.7600.16385
Build Mon Jul 13 20:14:14 2009

Path:
C:\Windows\System32\regsvr32.exe

Command line:
2.exe "C:\Users\User\AppData\Local\LSBCxgIyFCQMbqq\bznqoUd.dll"

Current directory:
C:\Users\User\Documents\

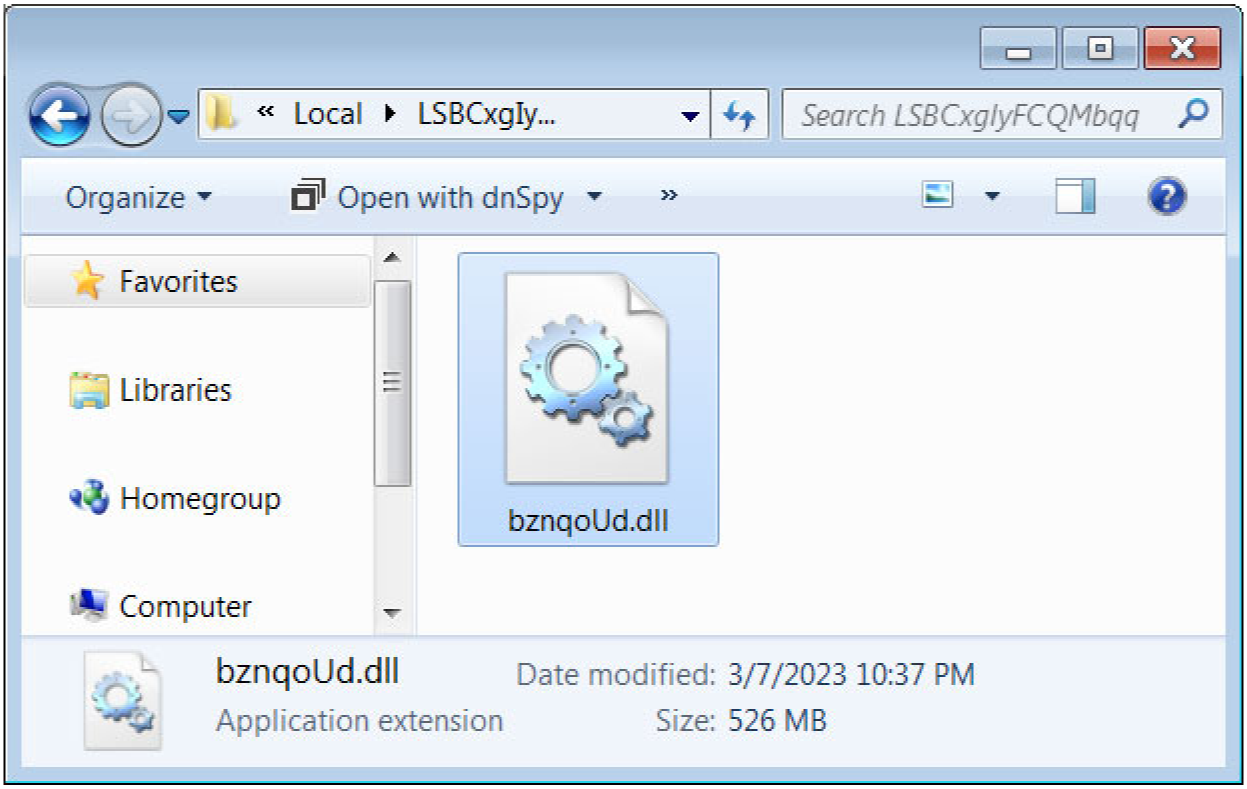
Autostart Location:
n/a

Parent: <Non-existent Process>(4288)
User: User-PC\User
Started: 2:39:56 PM 3/7/2023 Image:
Comment
VirusTotal:
Data Execution Prevention (DEP) Status: DEP (permanent)
Address Space Load Enabled

Emotet loader launched by Regsvr32.exe
Source: BleepingComputer

Like the Word document, the Emotet DLL has been also padded to be be 526MB to hinder the ability to detect it as malicious by antivirus software.

This evasion technique shows success, as illustrated in a VirusTotal scan where the malware is only detected by one security vendor out of 64 engines, with that vendor only detecting it as 'Malware.SwollenFile'.



bznqoUd.dll
Application extension
Date modified: 3/7/2023 10:37 PM
Size: 526 MB

Large Emotet DLL to evade detection
Source: BleepingComputer

Once running, the malware will run in the background, awaiting commands, which will likely install further payloads on the device

The payloads allow other threat actors to remotely access the device, which is then used to spread further in the compromised network.

These attacks commonly lead to data theft and full-blown ransomware attacks on breached networks.

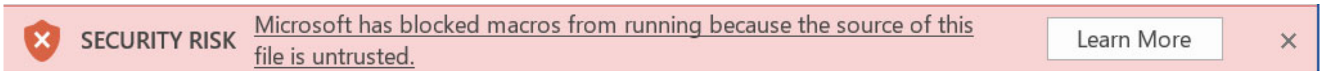
Cofense says that they have not seen any additional payloads being dropped now, and the malware is just collecting data for future spam campaigns.

Recent Microsoft changes save the day

While Emotet is rebuilding its network, the current method may not have much success after recent changes by Microsoft.

In July 2022, Microsoft finally disabled macros by default in Microsoft Office documents downloaded from the Internet.

Due to this change, users who open an Emotet document will be greeted with a message stating that the macros are disabled because the source of the file is not trusted.



SECURITY RISK Microsoft has blocked macros from running because the source of this file is untrusted.

Macros disabled by default in Microsoft Office
Source: BleepingComputer

ANALYGENCE senior vulnerability analyst, Will Dormann, told BleepingComputer that this change also affects attachments saved from emails.

For most users receiving Emotet emails, this feature will likely protect them from mistakenly enabling macros unless they make a concerted effort to enable them.

This change has led other threat actors to move away from Word and Excel documents and abuse other file formats, such as Microsoft OneNote, ISO images, and JS files.

It would not be surprising to see Emotet also move to different attachment types after this initial campaign does not go as intended.

Related Articles:

New IcedID variants shift from bank fraud to malware delivery

Emotet malware distributed as fake W-9 tax forms from the IRS

Microsoft OneNote will block 120 dangerous file extensions

Emotet malware now distributed in Microsoft OneNote files to evade defenses

FakeCalls Android malware returns with new ways to hide on phones

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.