# Emotet is back

hornetsecurity.com/en/security-information/emotet-is-back/

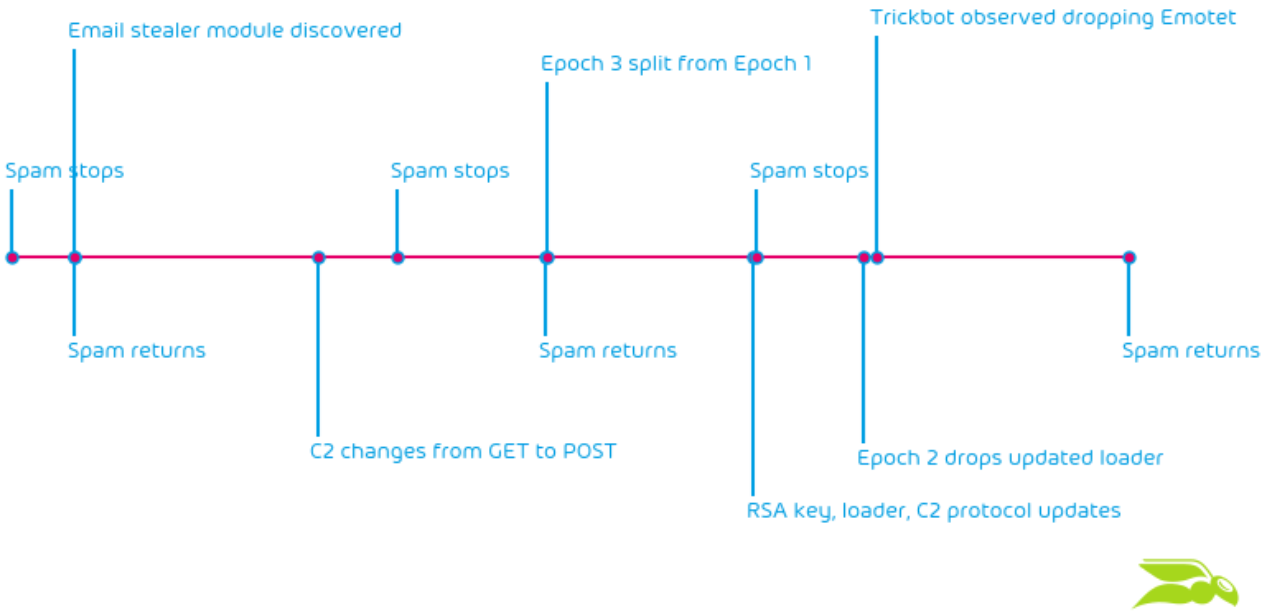
Security Lab July 20, 2020


## Summary

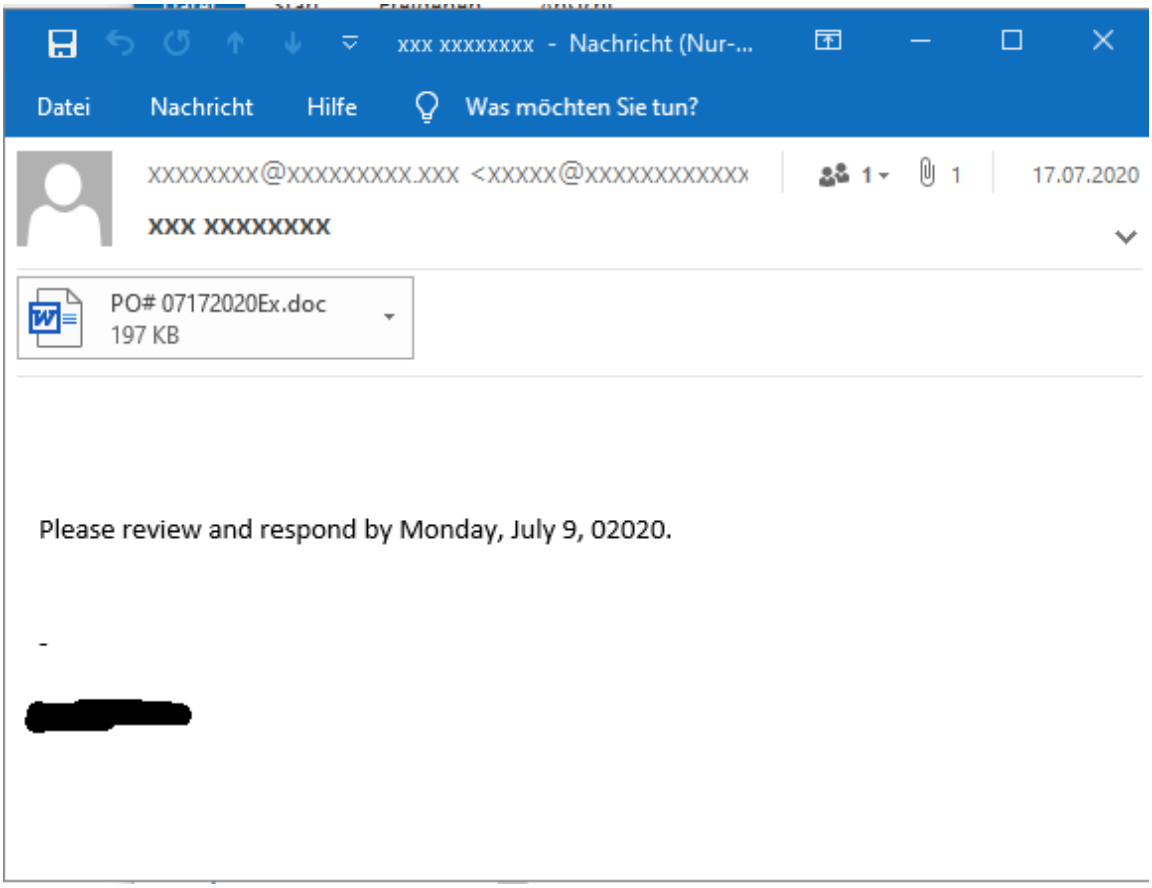
On 2020-07-17 the Hornetsecurity Security Lab detected the return of Emotet malspam. The reemerging Emotet malspam was already blocked by existing detection rules. The current Emotet malspam wave again uses malicious macro documents spread either via attachments or via malicious download links. As usual, the VBA macros in the document download the Emotet loader that the Hornetsecurity Security Lab has previously analyzed [EmotetLoader].

## Background

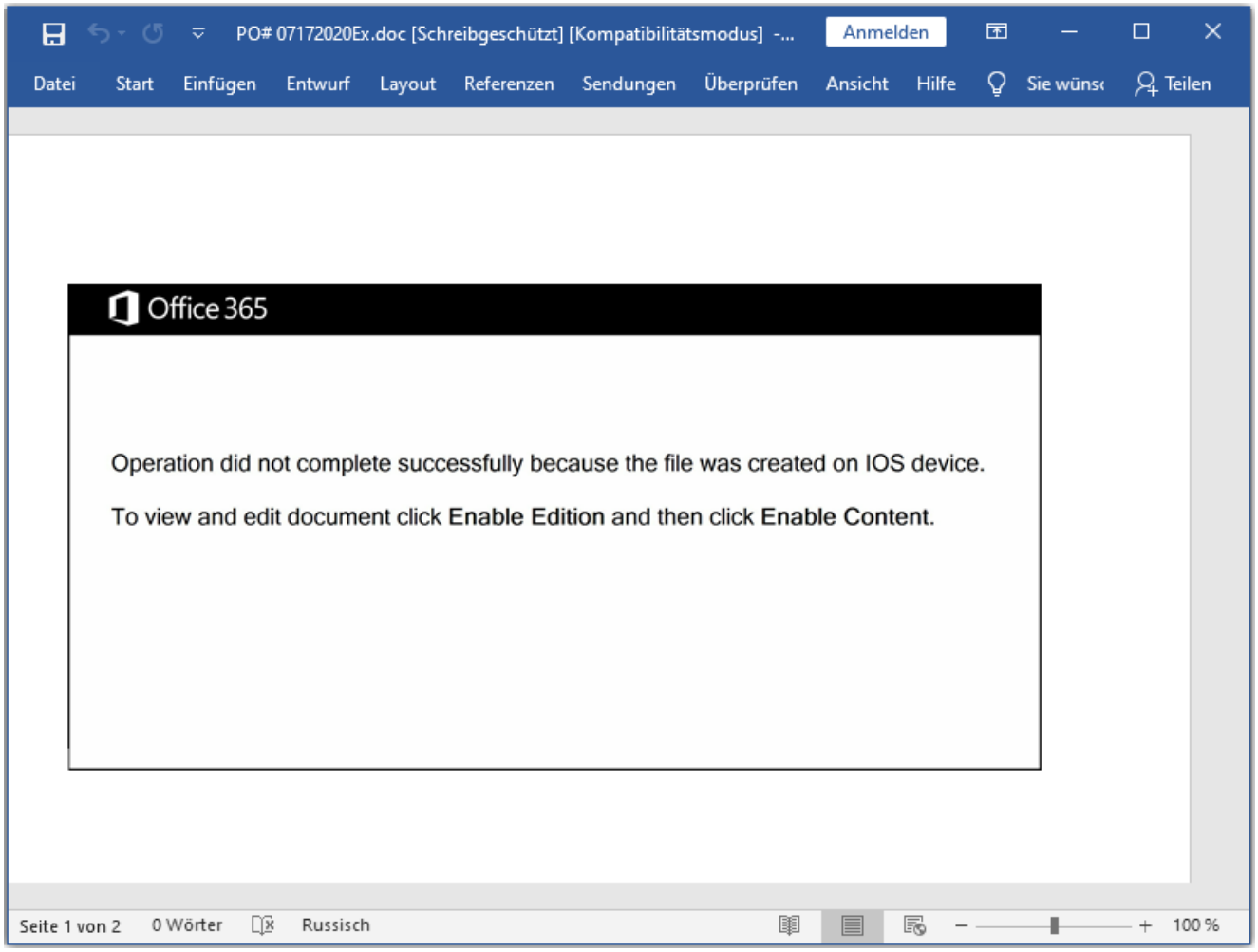
As previous reported the return of Emotet was inevitable. The Emotet botnet did not send malspam since 2020-02-07. While there were other activities on the botnet, as can be seen in the following timeline, no malspam was observed by the Hornetsecurity Security Lab since 2020-02-07.




On 2020-07-17 new Emotet malspam emails were blocked by Hornetsecurity's email filtering systems. One of such emails looks as follows:



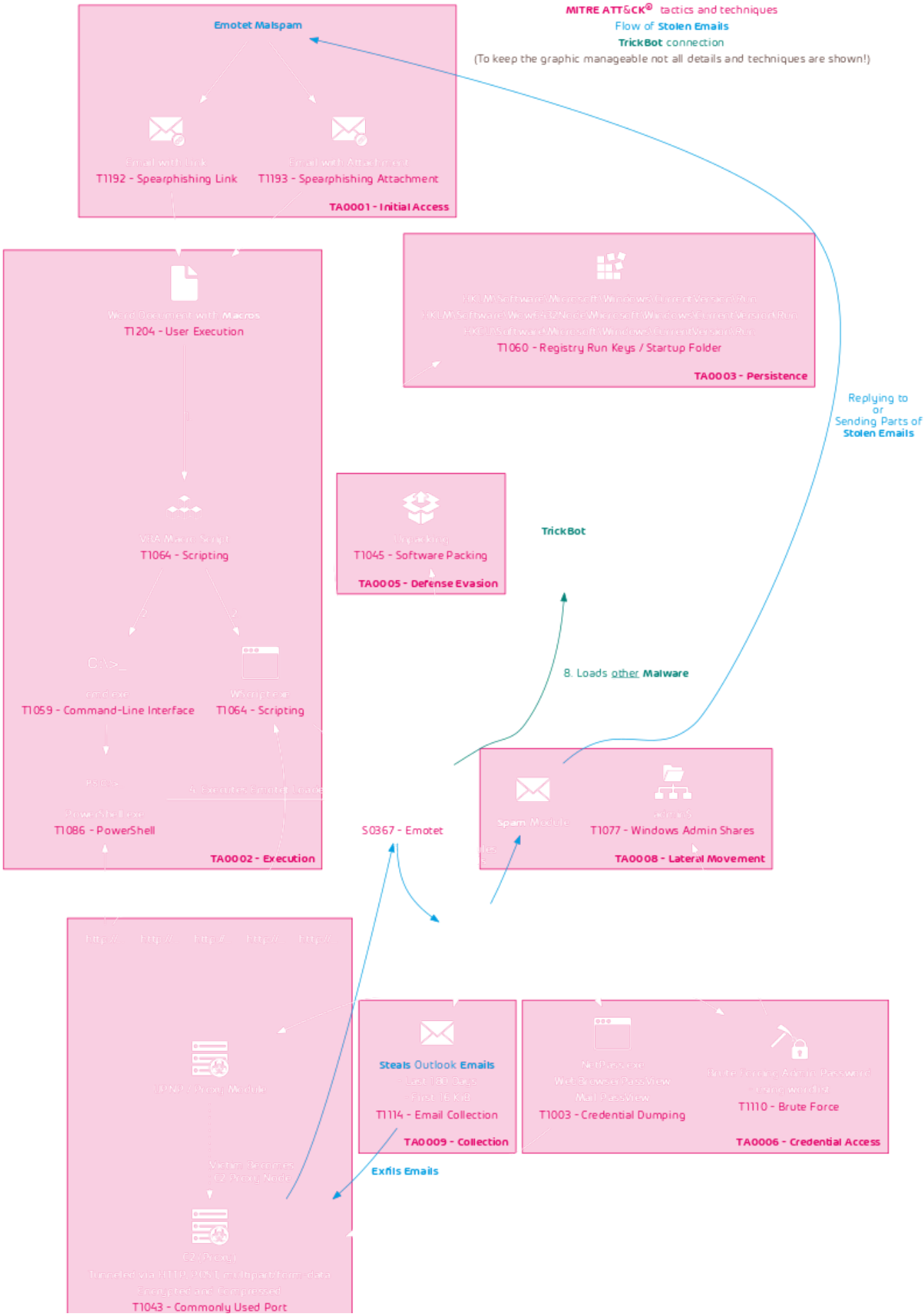
The email has a Word document attached, however, other emails with malicious download links to the malicious Word documents exist as well. When opening the document it instructs the user to click the “Enable Editing” (or as the Emotet authors put it “Enable Edition”) and click the “Enable Content” banner buttons:




If a user does so, they become a victim to Emotet.

## Technical Analysis

As previously reported the typical Emotet infection chain is as follows:

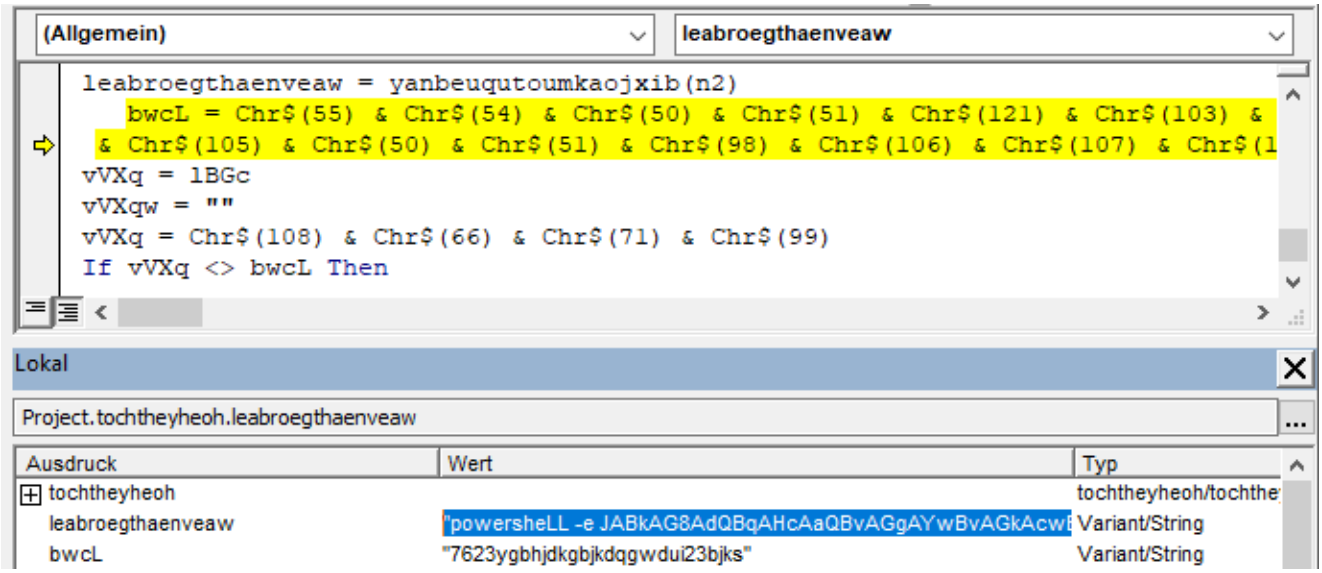

MITRE ATT&CK® tactics and techniques
Flow of Stolen Emails
TrickBot connection
(To keep the graphic manageable not all details and techniques are shown!)
Emotet Malspam
Email with Link
T1192 - Spearphishing Link
Email with Attachment
T1193 - Spearphishing Attachment
TA0001 - Initial Access
Word Document with Macros
T1204 - User Execution
VBA Macro Script
T1064 - Scripting
C:\>_
cmd.exe
T1059 - Command-Line Interface
Wscript.exe
T1064 - Scripting
PS C:\>
Powershell.exe
T1086 - PowerShell
4. Executes Emotet Loader
TA0002 - Execution
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
T1060 - Registry Run Keys / Startup Folder
TA0003 - Persistence
Unpacking
T1045 - Software Packing
TA0005 - Defense Evasion
TrickBot
8. Loads other Malware
Replying to
or
Sending Parts of
Stolen Emails
Spam Module
admin$
T1077 - Windows Admin Shares
TA0008 - Lateral Movement
S0367 - Emotet
http://
TOR? / Proxy Module
Victim Becomes
C2 Proxy Node
C2 (Proxy)
Tunneled via HTTP POST multipart/form-data
Encrypted and Compressed
T1043 - Commonly Used Port
Steals Outlook Emails
- Last 180 Days
- First 16 KiB
T1114 - Email Collection
TA0009 - Collection
NetPass.exe
WebBrowserPassView
MailPassView
T1003 - Credential Dumping
Brute Forcing Admin Password
using wordlist
T1110 - Brute Force
TA0006 - Credential Access
Exfils Emails

T1065 - Uncommonly Used Port
T1094 - Custom Command and Control Protocol
T1032 - Standard Cryptographic Protocol

TA0011 - Command and Control

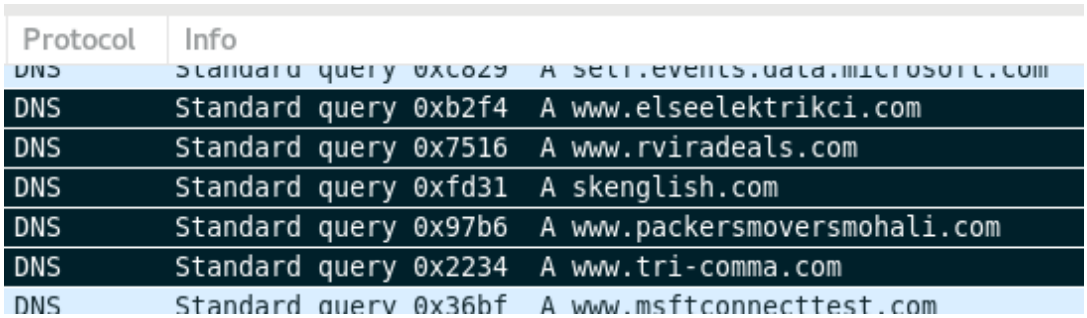
We already reported on the Emotet loader as part of an analysis regarding its updates. Because at that time Emotet did not send malspam we could not outline the malicious documents typically used in Emotet infections.

The VBA macros are obfuscated. The macro will construct a Powershell command from obfuscated strings embedded in the VBA macro:




Decoding the Base64-encoded command reveals the 5 Emotet loader download URLs:


The document will try to download the Emotet loader from each of these 5 URLs:




In case one of the 5 downlods is successful, it executes the Emotet loader, which we previously analyzed in a different article [EmotetLoader].

## Conclusion and Countermeasure

Unlike previously speculated Emotet has no new tricks – at least not when it comes to the malspam.

To protect against Emotet the US CERT recommends to “implement filters at the email gateway to filter out emails with known malspam indicators” [USCERT].

Hornetsecurity’s Spam Filter and Malware Protection, with the highest detection rates on the market, already detected and blocked the reemerged Emotet malspam. Hornetsecurity’s Advanced Threat Protection extends this protection by also detecting yet unknown threats.

Beyond blocking the incoming Emotet emails defenders can use public available information by the Cryptolaemus team, a voluntary group of IT security people banding together to fight Emotet. They provide new information daily via their website [CryptolaemusWeb]. There you can obtain the latest C2 IP list for finding and/or blocking C2 traffic. For real-time updates you can follow their Twitter account [CryptolaemusTwitter].

## References


- [EmotetLoader] https://www.hornetsecurity.com/en/security-information/awaiting-the-inevitable-return-of-emotet/
- [USCERT] https://www.us-cert.gov/ncas/alerts/TA18-201A
- [Cryptolaemus] https://paste.cryptolaemus.com/
- [CryptolaemusTwitter] https://twitter.com/Cryptolaemus1


## Indicators of Compromise (IOCs)

### Hashes

| SHA256 | Description |
|---|---|
| `99d8438c947cac7ca363037f1436ecab4e7fa4609c9c59f6fd5006a050d361aa` | Malicious document |
| `5d2c6110f2ea87a6b7fe9256affbac0eebdeee18081d59e05df4b4a17417492b` | Malicious document |
| `c5949244e5d529848c2323545a75eec34e6ba33c6519d46359b004d6717a68a5` | Malicious document |

### URLs

- `hxxps[:]//www.elseelektrikci[.]com/wp-content/hedk3/`
- `hxxps[:]//www.rviradeals[.]com/wp-includes/LeDR/`
- `hxxps[:]//skenglish[.]com/wp-admin/o0gf/`
- `hxxps[:]//www.packersmoversmohali[.]com/wp-includes/pgmt4x/`
- `hxxps[:]//www.tri-comma[.]com/wp-admin/MmD/`

### DNSs

- `www.elseelektrikci[.]com`
- `www.rviradeals[.]com`
- `skenglish[.]com`
- `www.packersmoversmohali[.]com`
- `www.tri-comma[.]com`