SANS ISC: InfoSec Handlers Diary Blog - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training InfoSec Handlers Diary Blog

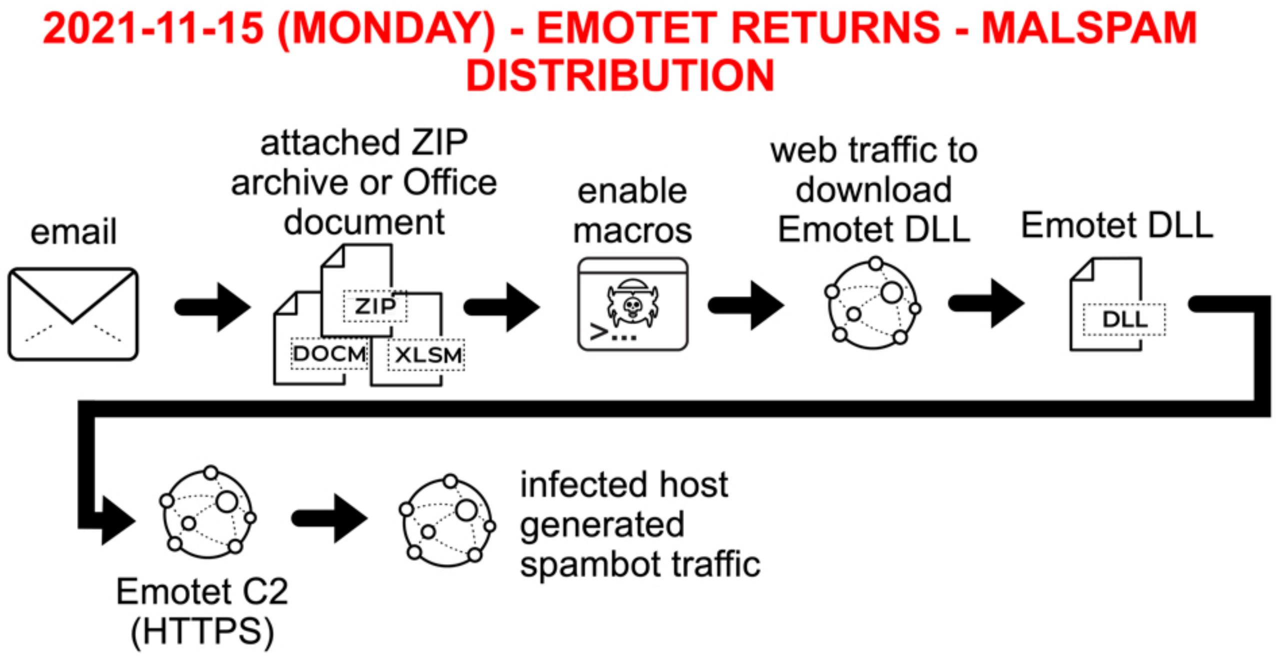
isc.sans.edu/diary/28044

Emotet Returns

Published: 2021-11-16
Last Updated: 2021-11-16 06:18:35 UTC
by Brad Duncan (Version: 1)
2 comment(s)
Introduction

Back in January 2021, law enforcement and judicial authorities worldwide took down the Emotet botnet. Although some Emotet emails still went out in the weeks after that, those were remnants from the inactive botnet infrastructure. We hadn't seen any *new* Emotet since then.

But on Monday 2021-11-15, we saw indicators that Emotet has returned. This diary reviews activity from a recent Emotet infection.


2021-11-15 (MONDAY) - EMOTET RETURNS - MALSPAM DISTRIBUTION
email
attached ZIP archive or Office document
ZIP
DOCM
XLSM
enable macros
>...
web traffic to download Emotet DLL
Emotet DLL
DLL
Emotet C2 (HTTPS)
infected host generated spambot traffic

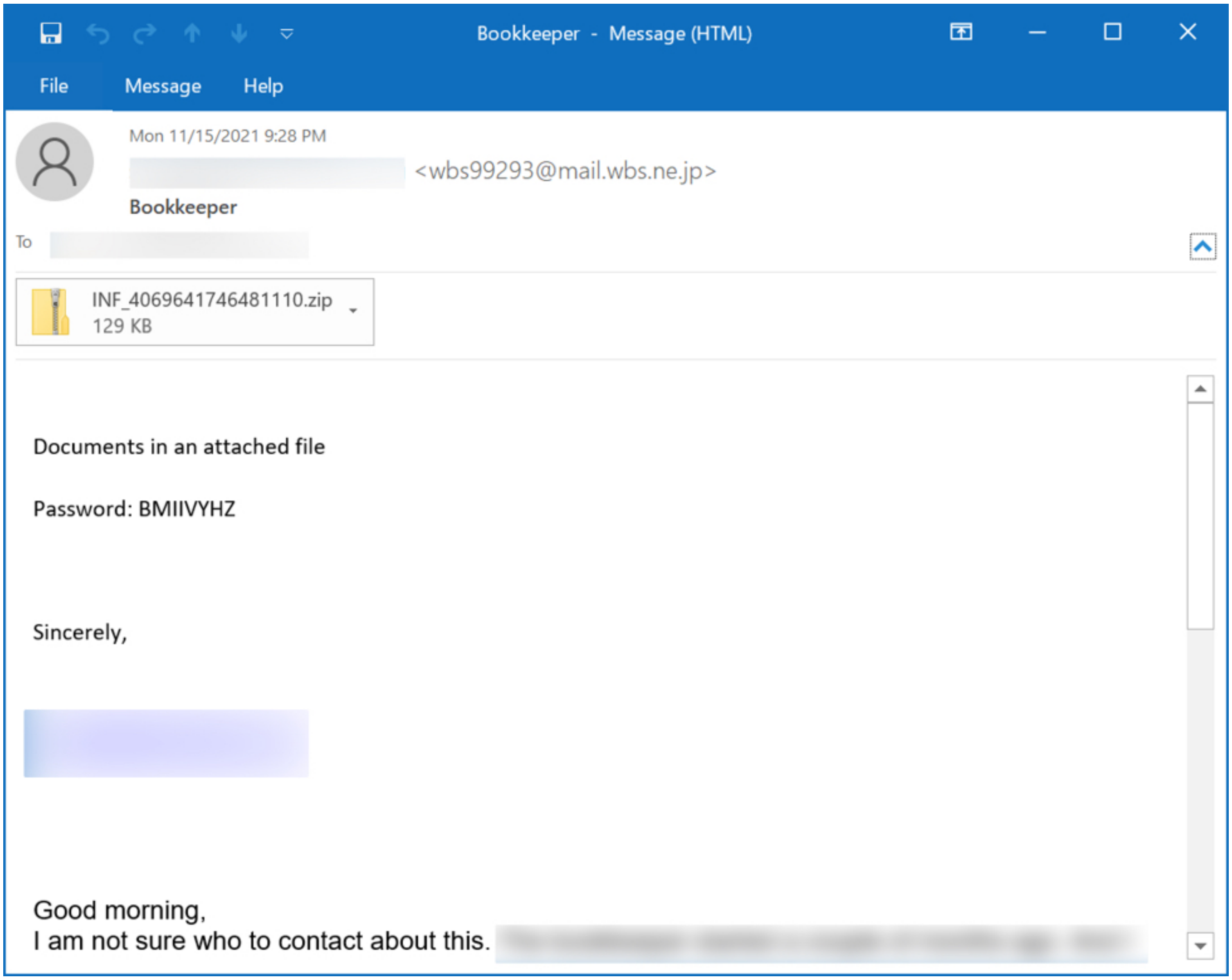
Shown above: Chain of events for Emotet infection on Monday 2021-11-15.

Emails

We found some emails from a newly-revived Emotet botnet on Monday 2021-11-15 that have one of three types of attachments:

- Microsoft Excel spreadsheet
- Microsoft Word document
- Password-protected zip archive (password: BMIIVYHZ) containing a Word document

These emails were all spoofed replies that used data from stolen email chains, presumably gathered from previously infected Windows hosts.



Mon 11/15/2021 9:28 PM

[redacted] <wbs99293@mail.wbs.ne.jp>

Bookkeeper

To [redacted]

INF_4069641746481110.zip
129 KB

Documents in an attached file

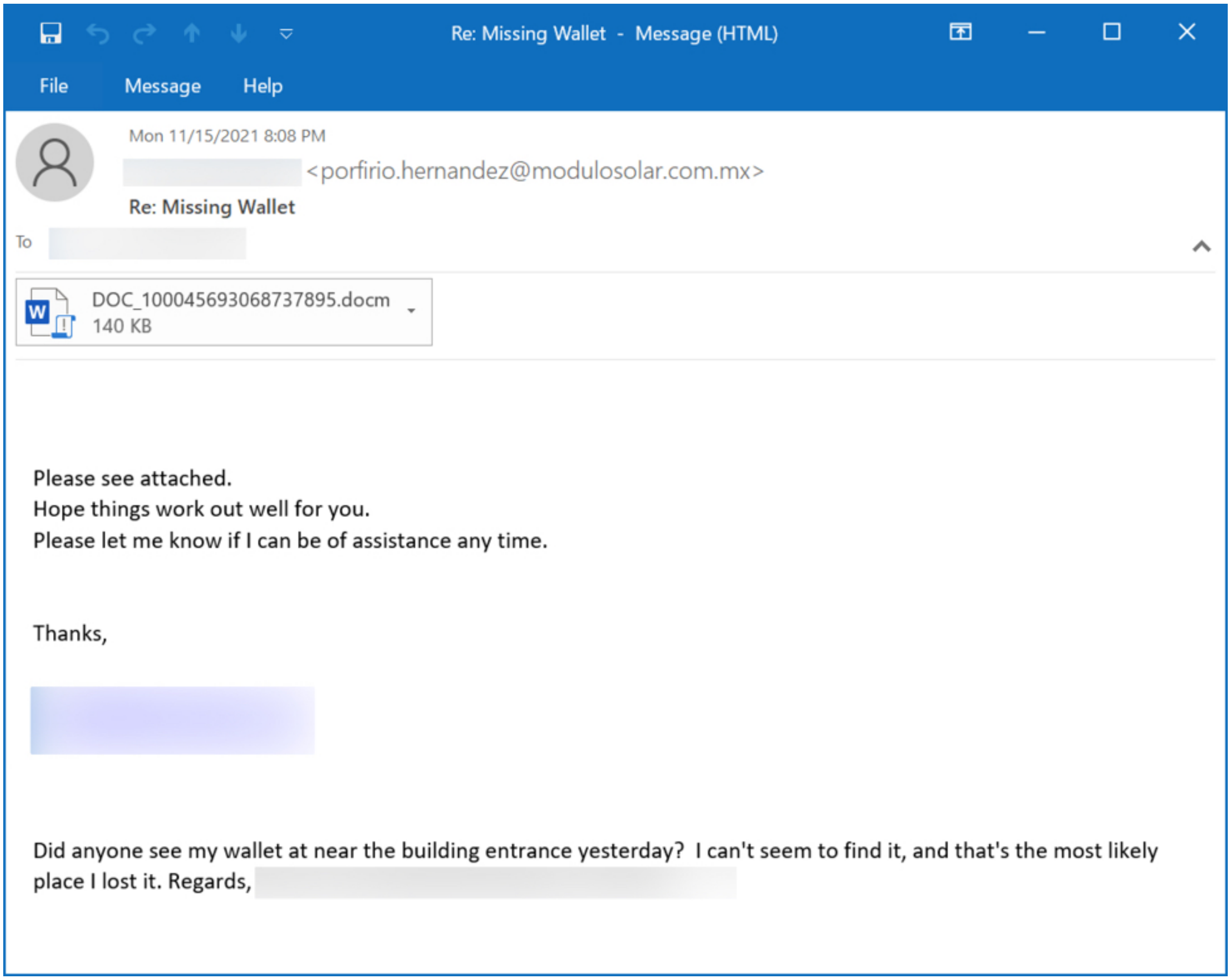
Password: BMIIVYHZ

Sincerely,

[redacted]

Good morning,
I am not sure who to contact about this. [redacted]

Shown above: Example of Emotet malspam with password protected zip attachment.



Mon 11/15/2021 8:08 PM

[redacted] <porfirio.hernandez@modulosolar.com.mx>

Re: Missing Wallet

To [redacted]

DOC_100045693068737895.docm
140 KB

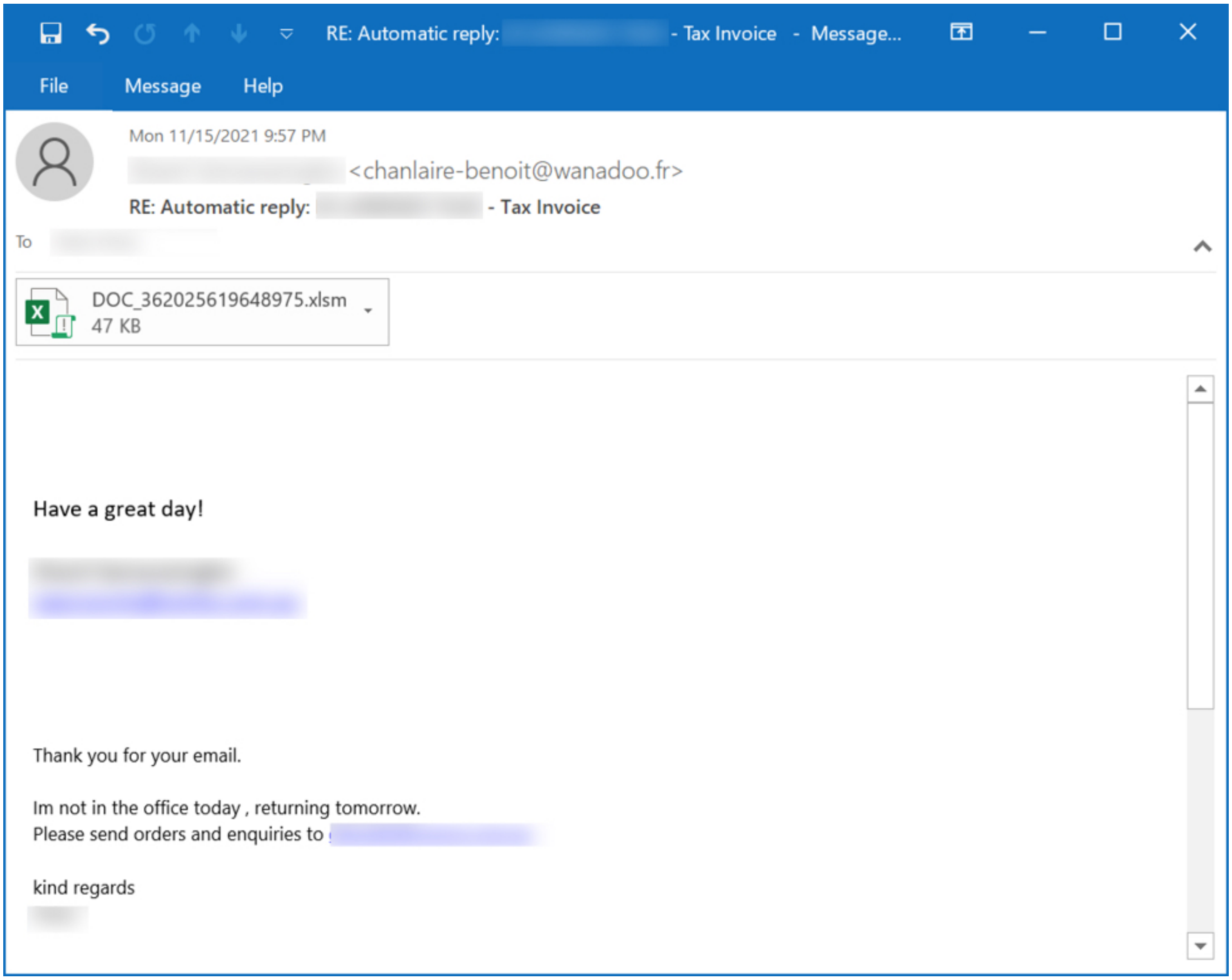
Please see attached.
Hope things work out well for you.
Please let me know if I can be of assistance any time.

Thanks,

[redacted]

Did anyone see my wallet at near the building entrance yesterday? I can't seem to find it, and that's the most likely place I lost it. Regards, [redacted]

Shown above: Example of Emotet malspam with attached Word document.



Mon 11/15/2021 9:57 PM

[redacted] <chanlaire-benoit@wanadoo.fr>

RE: Automatic reply: [redacted] - Tax Invoice

To [redacted]

DOC_362025619648975.xlsm
47 KB

Have a great day!

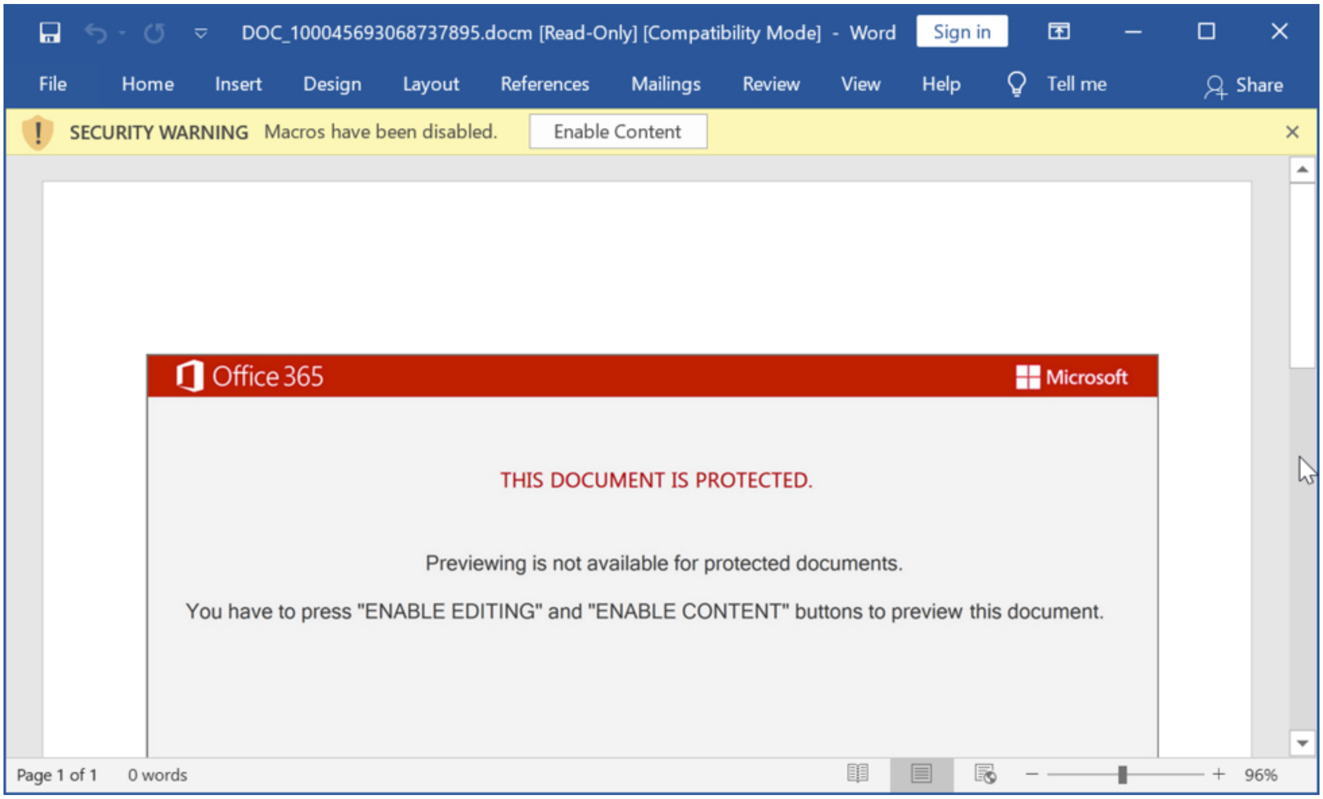
[redacted]

Thank you for your email.

Im not in the office today , returning tomorrow.
Please send orders and enquiries to [redacted]

kind regards
[redacted]

Shown above: Example of Emotet malspam with attached Excel file.



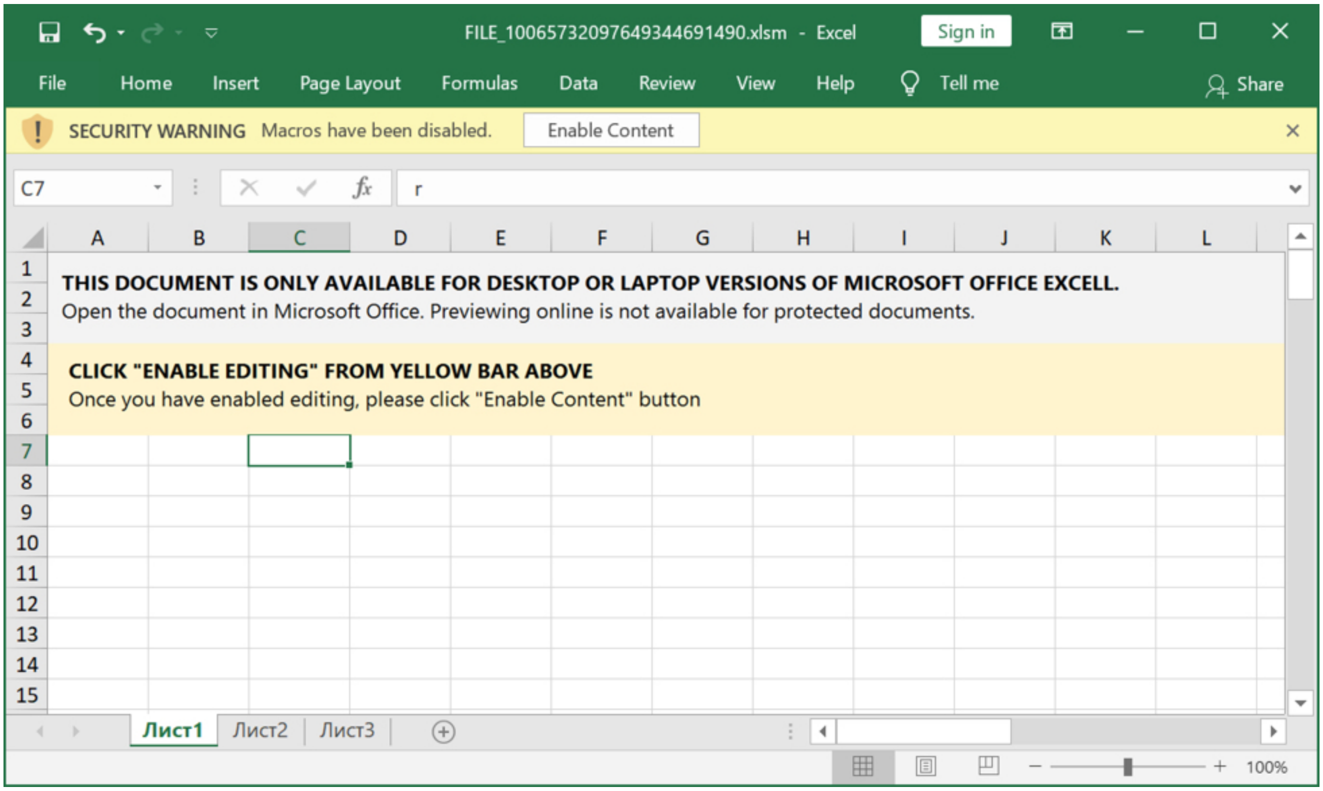
SECURITY WARNING Macros have been disabled.

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.

Shown above: Screenshot of Word document for Emotet.



SECURITY WARNING Macros have been disabled.

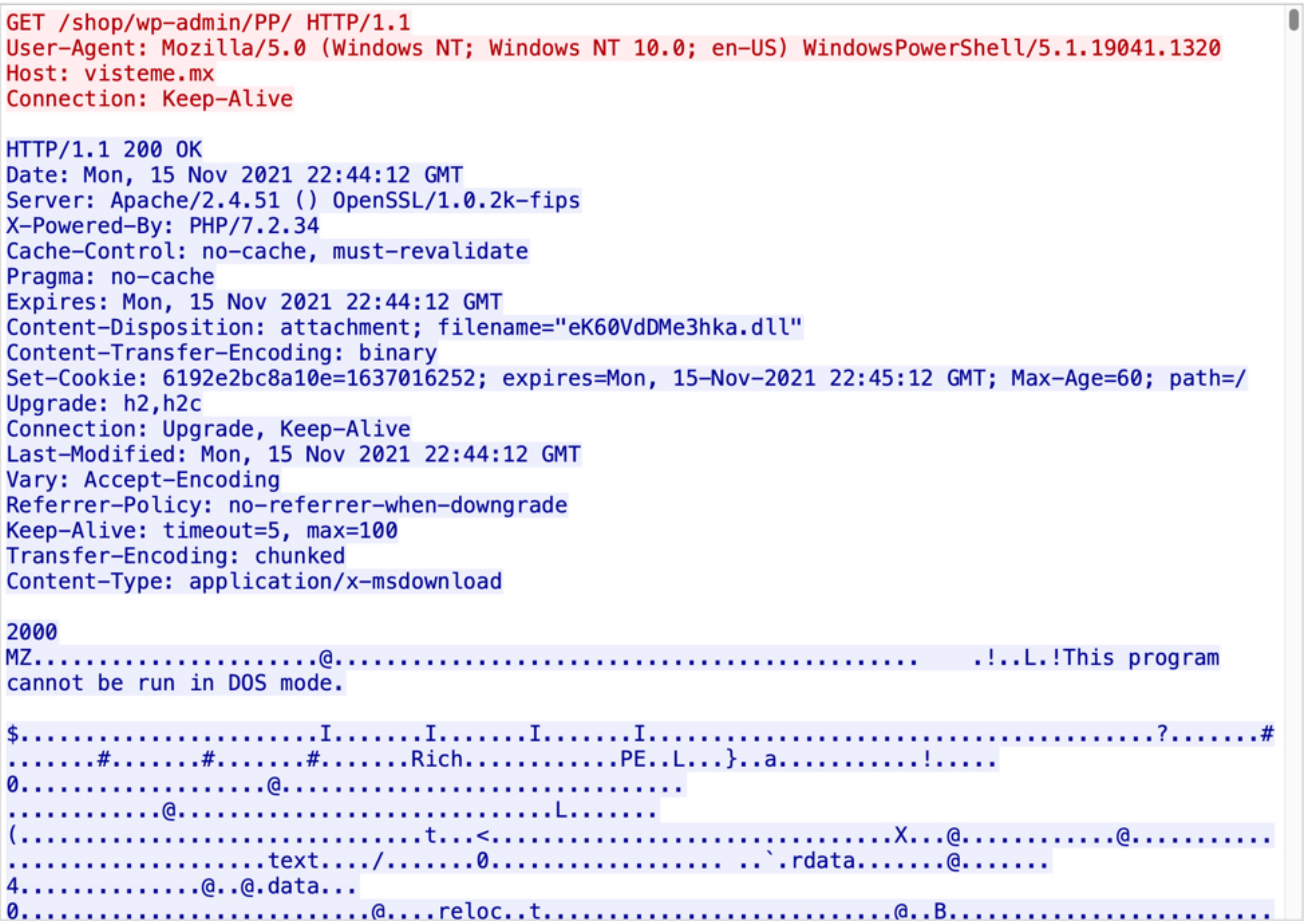
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCELL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.

CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button

Shown above: Screenshot of Excel spreadsheet for Emotet.

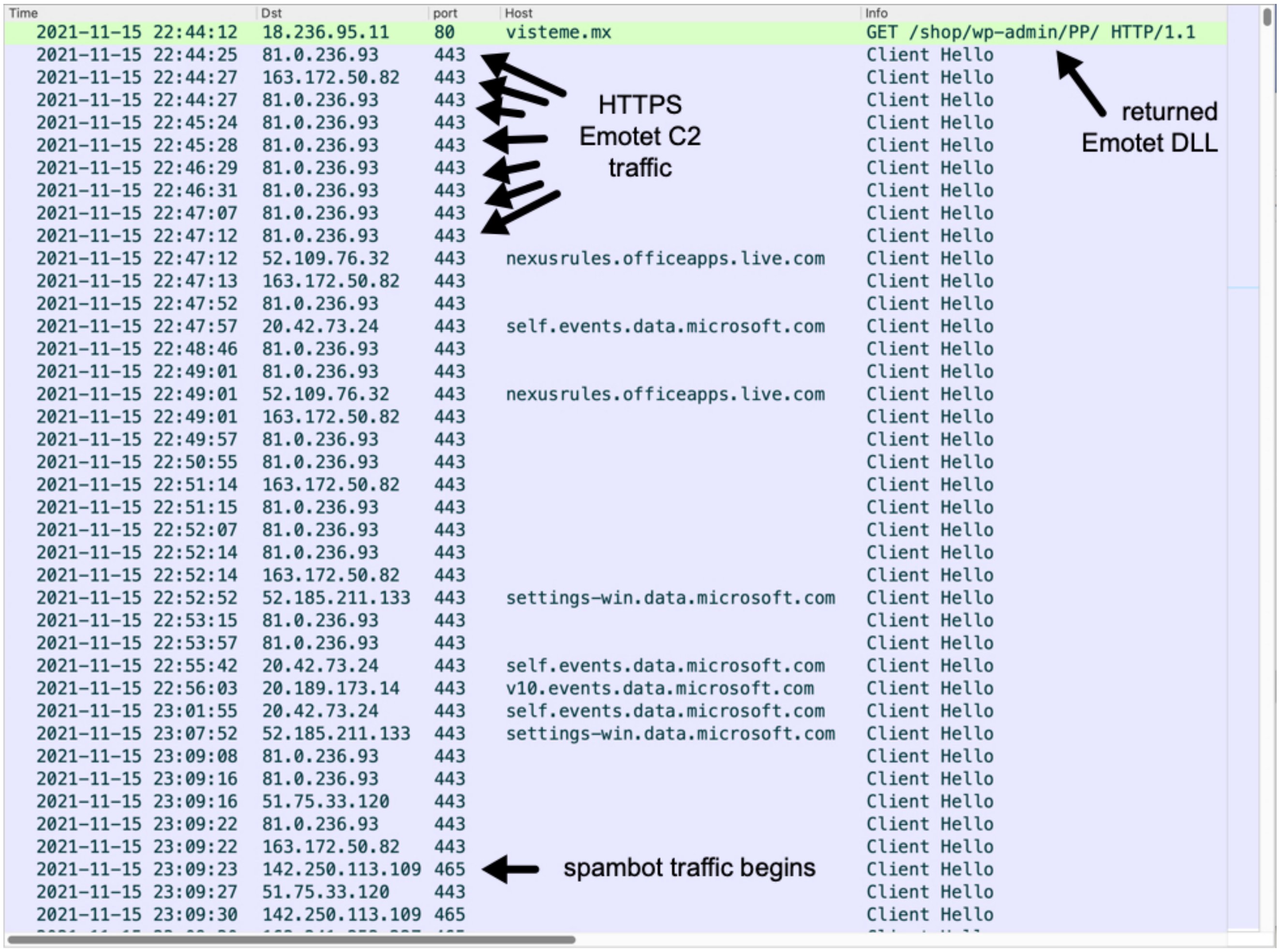
Infection traffic

Infection traffic for Emotet is similar to what we saw before the takedown in January 2021. The only real difference is Emotet post-infection C2 is now encrypted HTTPS instead of unencrypted HTTP. My infected lab host turned into a spambot trying to push out more Emotet malspam.



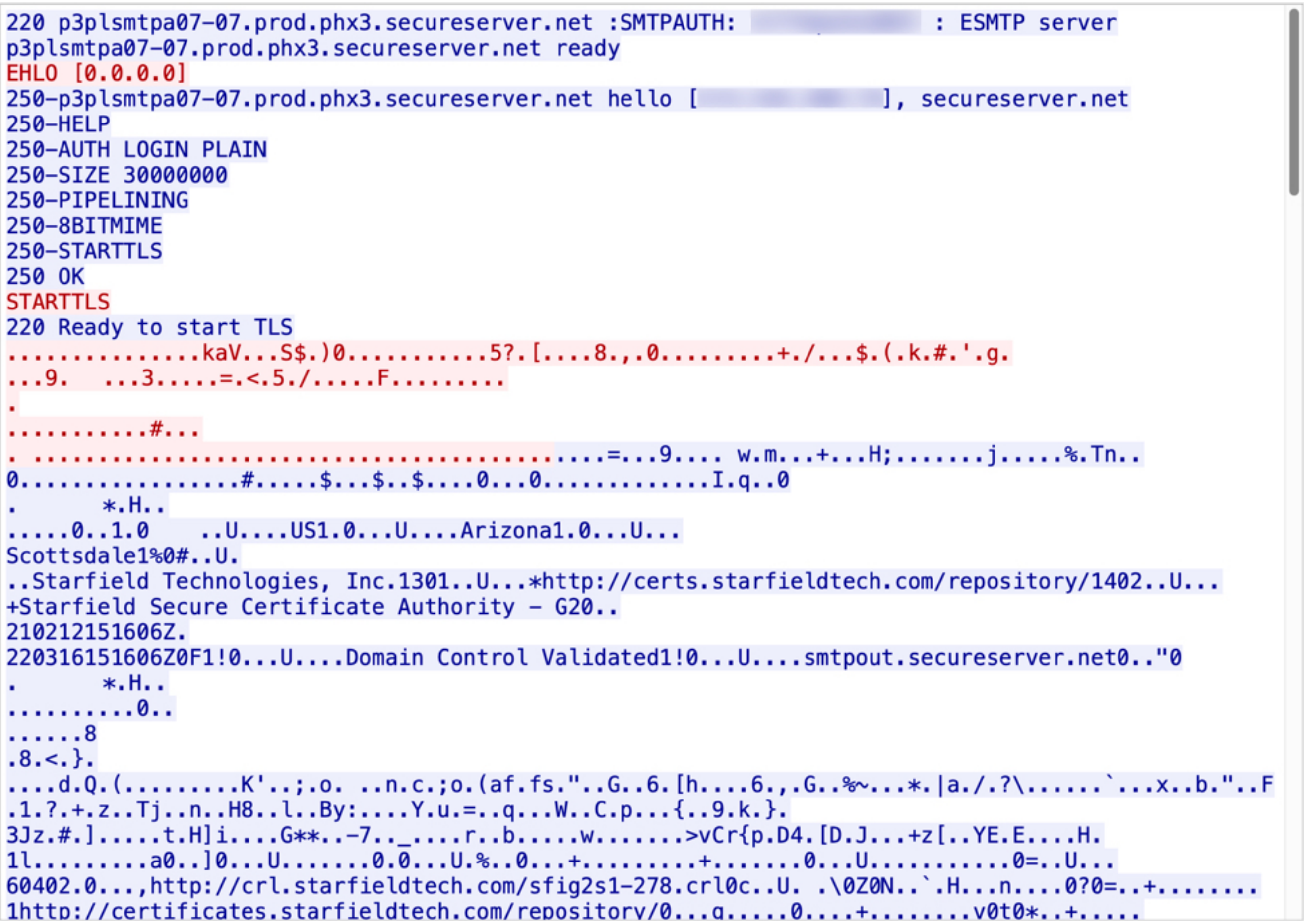
```
GET /shop/wp-admin/PP/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.1320
Host: visteme.mx
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 15 Nov 2021 22:44:12 GMT
Server: Apache/2.4.51 () OpenSSL/1.0.2k-fips
X-Powered-By: PHP/7.2.34
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Mon, 15 Nov 2021 22:44:12 GMT
Content-Disposition: attachment; filename="eK60VdDMe3hka.dll"
Content-Transfer-Encoding: binary
Set-Cookie: 6192e2bc8a10e=1637016252; expires=Mon, 15-Nov-2021 22:45:12 GMT; Max-Age=60; path=/
Upgrade: h2,h2c
Connection: Upgrade, Keep-Alive
Last-Modified: Mon, 15 Nov 2021 22:44:12 GMT
Vary: Accept-Encoding
Referrer-Policy: no-referrer-when-downgrade
Keep-Alive: timeout=5, max=100
Transfer-Encoding: chunked
Content-Type: application/x-msdownload

2000
MZ......................@.............................................    .!..L.!This program
cannot be run in DOS mode.

$.......................I.......I.......I.......I........................................?.......#
.......#.......#.......#.......Rich............PE..L...}..a...........!.....
0...................@...............................
............@.............................L.......
(...............................t...<...............................X...@............@...........
....................text..../.......0.................. ..`.rdata.......@.......
4..............@..@.data...
0...........................@....reloc..t...........................@..B..........................
```

Shown above: Example of traffic generated by Excel or Word macros for an Emotet DLL.



Time	Dst	port	Host	Info
2021-11-15 22:44:12	18.236.95.11	80	visteme.mx	GET /shop/wp-admin/PP/ HTTP/1.1
2021-11-15 22:44:25	81.0.236.93	443		Client Hello
2021-11-15 22:44:27	163.172.50.82	443		Client Hello
2021-11-15 22:44:27	81.0.236.93	443		Client Hello
2021-11-15 22:45:24	81.0.236.93	443		Client Hello
2021-11-15 22:45:28	81.0.236.93	443		Client Hello
2021-11-15 22:46:29	81.0.236.93	443		Client Hello
2021-11-15 22:46:31	81.0.236.93	443		Client Hello
2021-11-15 22:47:07	81.0.236.93	443		Client Hello
2021-11-15 22:47:12	81.0.236.93	443		Client Hello
2021-11-15 22:47:12	52.109.76.32	443	nexusrules.officeapps.live.com	Client Hello
2021-11-15 22:47:13	163.172.50.82	443		Client Hello
2021-11-15 22:47:52	81.0.236.93	443		Client Hello
2021-11-15 22:47:57	20.42.73.24	443	self.events.data.microsoft.com	Client Hello
2021-11-15 22:48:46	81.0.236.93	443		Client Hello
2021-11-15 22:49:01	81.0.236.93	443		Client Hello
2021-11-15 22:49:01	52.109.76.32	443	nexusrules.officeapps.live.com	Client Hello
2021-11-15 22:49:01	163.172.50.82	443		Client Hello
2021-11-15 22:49:57	81.0.236.93	443		Client Hello
2021-11-15 22:50:55	81.0.236.93	443		Client Hello
2021-11-15 22:51:14	163.172.50.82	443		Client Hello
2021-11-15 22:51:15	81.0.236.93	443		Client Hello
2021-11-15 22:52:07	81.0.236.93	443		Client Hello
2021-11-15 22:52:14	81.0.236.93	443		Client Hello
2021-11-15 22:52:14	163.172.50.82	443		Client Hello
2021-11-15 22:52:52	52.185.211.133	443	settings-win.data.microsoft.com	Client Hello
2021-11-15 22:53:15	81.0.236.93	443		Client Hello
2021-11-15 22:53:57	81.0.236.93	443		Client Hello
2021-11-15 22:55:42	20.42.73.24	443	self.events.data.microsoft.com	Client Hello
2021-11-15 22:56:03	20.189.173.14	443	v10.events.data.microsoft.com	Client Hello
2021-11-15 23:01:55	20.42.73.24	443	self.events.data.microsoft.com	Client Hello
2021-11-15 23:07:52	52.185.211.133	443	settings-win.data.microsoft.com	Client Hello
2021-11-15 23:09:08	81.0.236.93	443		Client Hello
2021-11-15 23:09:16	81.0.236.93	443		Client Hello
2021-11-15 23:09:16	51.75.33.120	443		Client Hello
2021-11-15 23:09:22	81.0.236.93	443		Client Hello
2021-11-15 23:09:22	163.172.50.82	443		Client Hello
2021-11-15 23:09:23	142.250.113.109	465		Client Hello
2021-11-15 23:09:27	51.75.33.120	443		Client Hello
2021-11-15 23:09:30	142.250.113.109	465		Client Hello

Shown above: Traffic from an infection filtered in Wireshark.



```
220 p3plsmtpa07-07.prod.phx3.secureserver.net :SMTPAUTH: [redacted] : ESMTP server
p3plsmtpa07-07.prod.phx3.secureserver.net ready
EHLO [0.0.0.0]
250-p3plsmtpa07-07.prod.phx3.secureserver.net hello [[redacted]], secureserver.net
250-HELP
250-AUTH LOGIN PLAIN
250-SIZE 30000000
250-PIPELINING
250-8BITMIME
250-STARTTLS
250 OK
STARTTLS
220 Ready to start TLS
...............kaV...S$.)0...........5?.[....8.,.0.........+./...$.(.k.#.'.g.
...9.   ...3.....=.<.5./.....F.........
.
...........#...
. .........................................=...9.... w.m...+...H;.......j.....%.Tn..
0..................#.....$...$..$....0...0.............I.q..0
.      *.H..
.....0..1.0    ..U....US1.0...U....Arizona1.0...U...
Scottsdale1%0#..U.
..Starfield Technologies, Inc.1301..U...*http://certs.starfieldtech.com/repository/1402..U...
+Starfield Secure Certificate Authority - G20..
210212151606Z.
220316151606Z0F1!0...U....Domain Control Validated1!0...U....smtpout.secureserver.net0.."0
.      *.H..
..........0..
......8
.8.<.}.
....d.Q.(.........K'..;.o. ..n.c.;o.(af.fs."..G..6.[h....6.,.G..%~...*.|a./.?\......`...x..b."..F
.1.?.+.z..Tj..n..H8..l..By:....Y.u.=..q...W..C.p...{..9.k.}.
3Jz.#.].....t.H]i....G**..-7.._.....r..b.....w.......>vCr{p.D4.[D.J...+z[..YE.E....H.
1l.........a0..]0...U.......0.0...U.%..0...+.........+.......0...U...........0=..U...
60402.0...,http://crl.starfieldtech.com/sfig2s1-278.crl0c..U. .\0Z0N..`.H...n....0?0=..+........
1http://certificates.starfieldtech.com/repository/0...q.....0....+........v0t0*..+.....
```

Shown above: TCP stream of encrypted SMTP traffic from my infected Windows host.

Indicators of Compromise (IOCs)

The following are Word documents, Excel files, and a password-protected zip archive I saw from Emotet on Monday 2021-11-15.

SHA256 hash: 7c5690577a49105db766faa999354e0e4128e902dd4b5337741e00e1305ced24

- File size: 143,401 bytes
- File name: DOC_100045693068737895.docm
- File name: DOC_10010148844855817699830.docm
- File name: INF_10043023764772507433030.docm

SHA256 hash: bd9b8fe173935ad51f14abc16ed6a5bf6ee92ec4f45fd2ae1154dd2f727fb245

- File size: 143,121 bytes
- File name: FILE_24561806179285605525.docm

SHA256 hash: f7a4da96129e9c9708a005ee28e4a46af092275af36e3afd63ff201633c70285

- File size: 132,317 bytes
- File name: INF_4069641746481110.zip

SHA256 hash: d95125b9b82df0734b6bc27c426d42dea895c642f2f6516132c80f896be6cf32

- File size: 143,108 bytes
- File name: INF_4069641746481110.docm

SHA256 hash: 88b225f9e803e2509cc2b83c57ccd6ca8b6660448a75b125e02f0ac32f6aadb9

- File size: 47,664 bytes
- File name: FILE_10065732097649344691490.xlsm

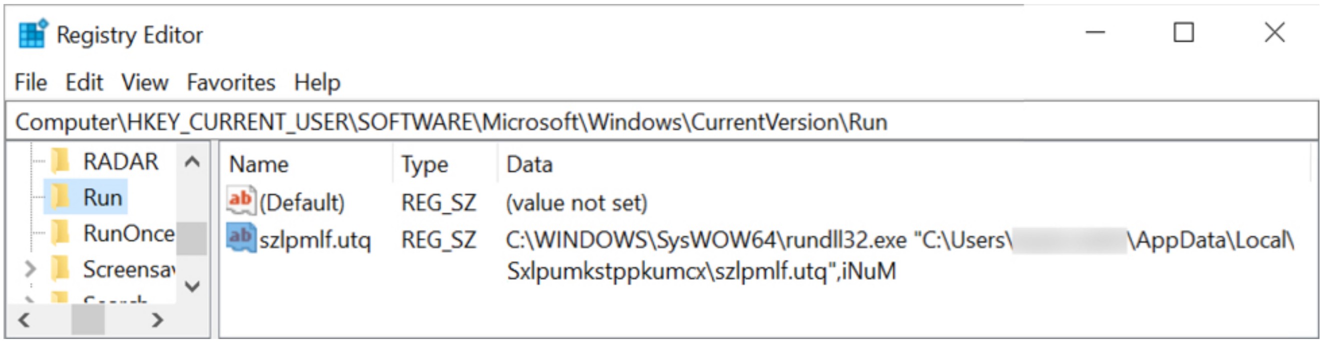
SHA256 hash:
1abd14d498605654e20feb59b5927aa835e5c021cada80e8614e9438ac323601

- File size: 47,660 bytes
- File name: SCAN_1002996108727260055496.xlsm

The following are URLs generated by macros from the above files for an Emotet DLL file:

- hxxp://av-quiz[.]tk/wp-content/k6K/
- hxxp://devanture[.]com[.]sg/wp-includes/XBByNUNWvIEvawb68/
- hxxp://ranvipclub[.]net/pvhko/a/
- hxxp://visteme[.]mx/shop/wp-admin/PP/
- hxxps://goodtech.cetxlabs[.]com/content/5MfZPgP06/
- hxxps://newsmag.danielolayinkas[.]com/content/nVgyRFrTE68Yd9s6/
- hxxps://team.stagingapps[.]xyz/wp-content/aPIm2GsjA/

The Emotet DLL was first stored as a random file name with a .dll extension under the ***C:\ProgramData*** directory. Then it was moved to a randomly-named directory under the infected user's ***AppData\Local*** folder. The DLL is then made persistent through a Windows registry update as shown below.



Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
szlpmlf.utq	REG_SZ	C:\WINDOWS\SysWOW64\rundll32.exe "C:\Users\[redacted]\AppData\Local\Sxlpumkstppkumcx\szlpmlf.utq",iNuM

Shown above: Example of registry update to keep Emotet persistent.

SHA256 hashes for 7 examples of Emotet DLL files:

- 0b132c7214b87082ed1fc2427ba078c3b97cbbf217ca258e21638cab28824bfa
- 373398e4ae50ecb20840e6f8a458501437cfa8f7b75ad8a62a84d5c0d14d3e59
- 29de2e527f736d4be12b272fd8b246c96290c7379b6bc2d62c7c86ebf7f33cd4

- 632447a94c590b3733e2e6ed135a516428b0bd1e57a7d254d5357b52668b41f1
- 69efec4196d8a903de785ed404300b0bf9fce67b87746c0f3fc44a2bb9a638fc
- 9c345ee65032ec38e1a29bf6b645cde468e3ded2e87b0c9c4a93c517d465e70d
- b95a6218777e110578fa017ac14b33bf968ca9c57af7e99bd5843b78813f46e0

HTTPS Emotet C2 traffic:

- 51.75.33[.]120 port 443
- 51.159.35[.]157 port 443
- 81.0.236[.]93 port 443
- 94.177.248[.]64 port 443
- 92.207.181[.]106 port 8080
- 109.75.64[.]100 port 8080
- 163.172.50[.]82 port 443

Final words

The emails examples and malware samples from Monday's Emotet activity on 2021-11-15 can be found here.

Brad Duncan
brad [at] malware-traffic-analysis.net

Keywords: DLL Emotet malspam spambot

2 comment(s)

DEV522
Defending Web Application Security Essentials
LEARN MORE
Learn to defend your apps before they're hacked

Top of page

×

Diary Archives