Initial Access

Spearphishing:

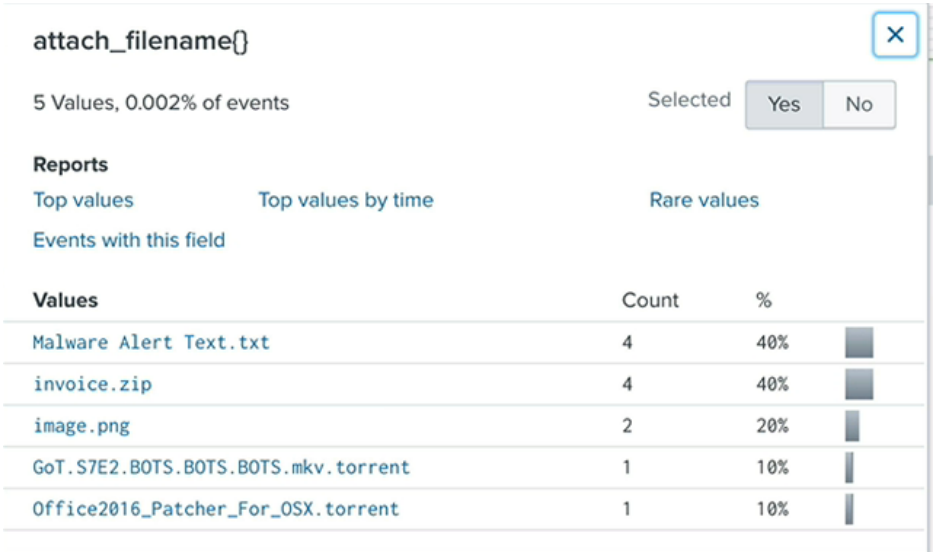
Hypothesis:
ATT&CK - Phishing: Spearphishing Attachment

Adversaries will attempt to establish a foothold within froth.ly using a spearphishing attachment.

Here are some questions to think about that may help as we conduct our hunt:

- What data sources (sourcetypes) should we look for mail traffic in?
- Do we have visibility into what email attachments are being received?
- Are there specific kinds of attachments that we should be hunting for?
- If we have attachments of interest, what attributes are associated with it? Sender, recipient, subject, message and more
- Do we see those attributes in other emails?
- Are there prior spearphishing attempts that perhaps were unsuccessful that can be leveraged in our hunt?

- We can brainstorm sources from where mail attachments can be found, or the protocols used in mail exchange. We can find that source is *smtp* and the sourcetype is *attach_filename.* Upon further hunting we can see the top 2 attachments seem malicious. Let's search for events related to invoice.zip.



- After narrowing down to only one attachment "*invoice.zip*", and analyzing the we could find the attributes mentioned in the hypothesis.

- We know that the adversary has used VPN services to hide his location. Upon investigation, those 4 IP addresses are Microsoft Servers showing up in Redmond, Washington.

src_ip

4 Values, 100% of events

Selected Yes No

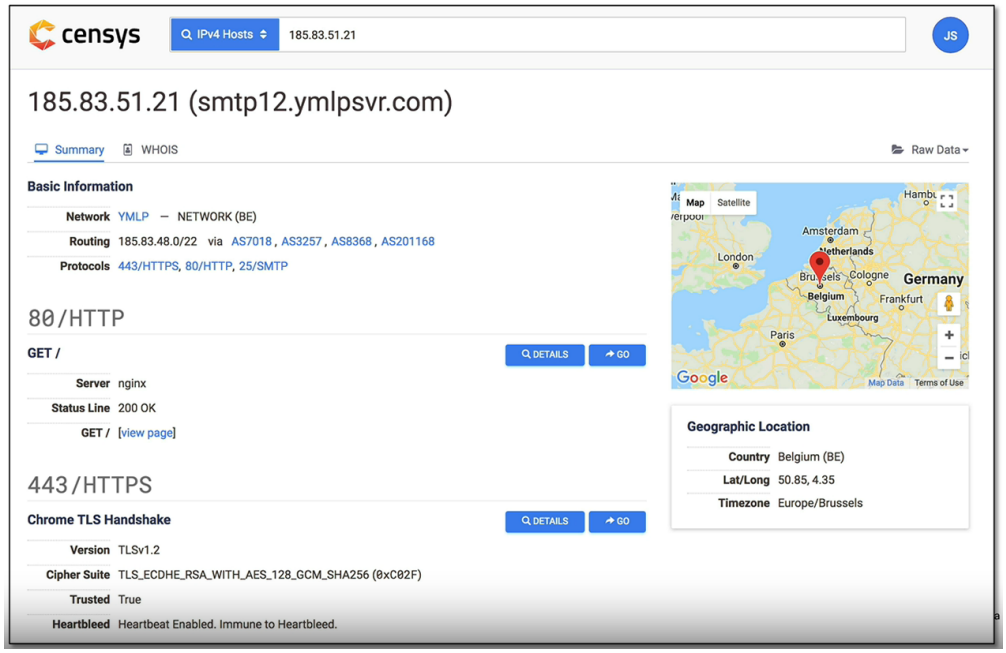
Reports

Top values Top values by time Rare values

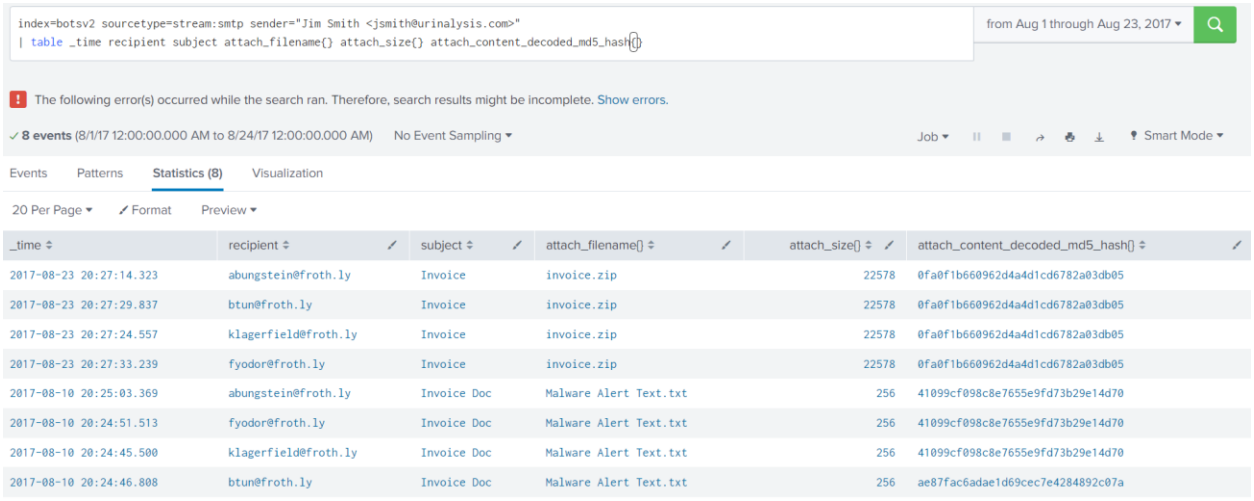
Events with this field

Values	Count	%
104.47.37.62	1	25%
104.47.38.87	1	25%
104.47.41.43	1	25%
104.47.42.76	1	25%

- However, the source from which the mail was sent, can be observed, and also the originating IP address by examining the content header of the mail, which was located in Belgium. 185.83.51.21 (smtp12.ymlpsvr.com)



- Now we search if Jim Smith has previously sent any mails to any of our employees. We can see that Jim has already tried to send a document which was automatically removed because it was identified as malicious. So he modified his attachment and sent mails again. Performing a OSINT on the file hash was a dead end.



```
index=botsv2 sourcetype=stream:smtp sender="Jim Smith <jsmith@urinalysis.com>"
| table _time recipient subject attach_filename{} attach_size{} attach_content_decoded_md5_hash{}
```

from Aug 1 through Aug 23, 2017

The following error(s) occurred while the search ran. Therefore, search results might be incomplete. Show errors.

✓ 8 events (8/1/17 12:00:00.000 AM to 8/24/17 12:00:00.000 AM) No Event Sampling Job Smart Mode

Events Patterns Statistics (8) Visualization

20 Per Page Format Preview

_time	recipient	subject	attach_filename{}	attach_size{}	attach_content_decoded_md5_hash{}
2017-08-23 20:27:14.323	abungstein@froth.ly	Invoice	invoice.zip	22578	0fa0f1b660962d4a4d1cd6782a03db05
2017-08-23 20:27:29.837	btun@froth.ly	Invoice	invoice.zip	22578	0fa0f1b660962d4a4d1cd6782a03db05
2017-08-23 20:27:24.557	klagerfield@froth.ly	Invoice	invoice.zip	22578	0fa0f1b660962d4a4d1cd6782a03db05
2017-08-23 20:27:33.239	fyodor@froth.ly	Invoice	invoice.zip	22578	0fa0f1b660962d4a4d1cd6782a03db05
2017-08-10 20:25:03.369	abungstein@froth.ly	Invoice Doc	Malware Alert Text.txt	256	41099cf098c8e7655e9fd73b29e14d70
2017-08-10 20:24:51.513	fyodor@froth.ly	Invoice Doc	Malware Alert Text.txt	256	41099cf098c8e7655e9fd73b29e14d70
2017-08-10 20:24:45.500	klagerfield@froth.ly	Invoice Doc	Malware Alert Text.txt	256	41099cf098c8e7655e9fd73b29e14d70
2017-08-10 20:24:46.808	btun@froth.ly	Invoice Doc	Malware Alert Text.txt	256	ae87fac6adae1d69cec7e4284892c07a

What have we learned?

- Originating Sender: 185.83.51.21
- Sender Name: Jim Smith <jsmith@urianalysis.com>
- Recipient(s): fyodor@froth.ly
- Attachment Name: Invoice.zip
- Size: 22578
- Date/Time: 8/23/17 8:27:33.239 PM
- Body : Mail containing details of invoice.
- Subject : Invoice

User Execution: Malicious File

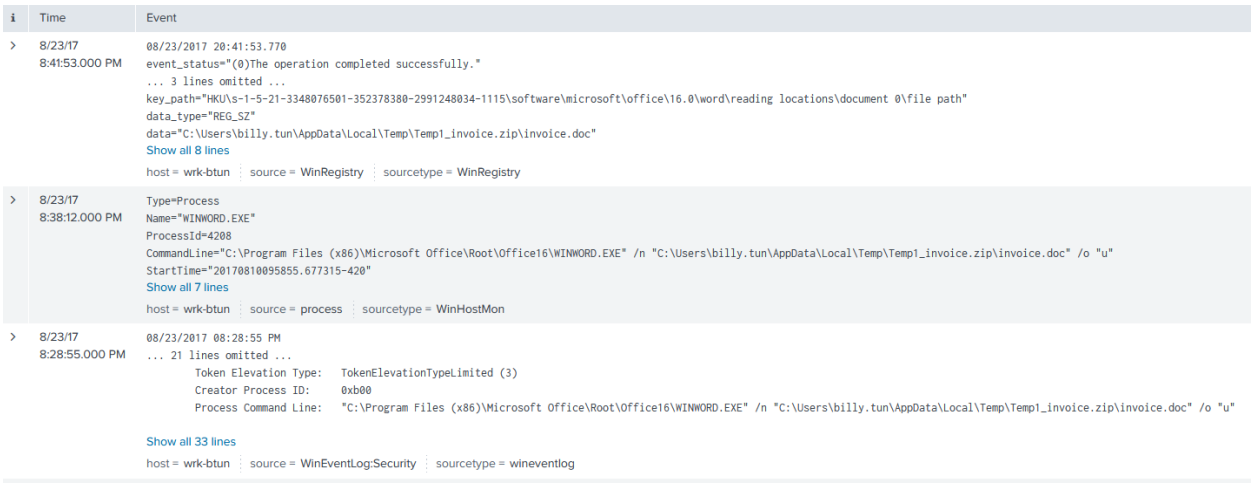
Hypothesis:
ATT&CK - User Execution: Malicious File

With confirmation of the spearphishing hypothesis, adversaries will attempt to establish a foothold within frothly by enticing a user to execute a malicious file.

Here are some questions to think about that may help as we conduct our hunt:

- What data sources (sourcetypes) should execution of files be seen in?
- Should we be looking for file executions before or after spearphishing attachments may have been received?
- What kind of supporting information is found in events when a file execution occurs?
- What other indicators do we have to start looking for user execution?
- In this case, we know that a spearphishing attachment called invoice.zip was received
- What system did the execution occur on?
- What user name executed the file?
- What happened upon execution of a file?

- Now, we search for other instances where invoice.zip was seen. We can notice that in source '*process'* and sourcetype '*WinHostMon'* we can find the attachment. It is also possible that after the delivery of the malicious file, a malicious process could've started. So we search for processes linked with invoice.zip.
- If we look at the Windows Event Logs and Registry, we can see winword.exe starting and opening invoice.doc from within temp_invoice.zip.



i	Time	Event
>	8/23/17 8:41:53.000 PM	08/23/2017 20:41:53.770 event_status="(0)The operation completed successfully." ... 3 lines omitted ... key_path="HKU\s-1-5-21-3348076501-352378380-2991248034-1115\software\microsoft\office\16.0\word\reading locations\document 0\file path" data_type="REG_SZ" data="C:\Users\billy.tun\AppData\Local\Temp\Temp1_invoice.zip\invoice.doc" Show all 8 lines host = wrk-btun source = WinRegistry sourcetype = WinRegistry
>	8/23/17 8:38:12.000 PM	Type=Process Name="WINWORD.EXE" ProcessId=4208 CommandLine="C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:\Users\billy.tun\AppData\Local\Temp\Temp1_invoice.zip\invoice.doc" /o "u" StartTime="20170810095855.677315-420" Show all 7 lines host = wrk-btun source = process sourcetype = WinHostMon
>	8/23/17 8:28:55.000 PM	08/23/2017 08:28:55 PM ... 21 lines omitted ... Token Elevation Type: TokenElevationTypeLimited (3) Creator Process ID: 0xb00 Process Command Line: "C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:\Users\billy.tun\AppData\Local\Temp\Temp1_invoice.zip\invoice.doc" /o "u" Show all 33 lines host = wrk-btun source = WinEventLog:Security sourcetype = wineventlog

- If we turn our attention to Sysmon, we see two events referencing invoice.zip, around the same time as the process creation Windows event but before the Windows registry event.
- If we look at the process creation Sysmon event, we can see here that winword.exe was executed and invoice.doc, extracted from invoice.zip was opened. Based upon this and the absence of a VirusTotal hit, we may have a macro execution creating havoc.
- Let's use our time picker and narrow our time range down to the first Sysmon event that occurred on August 23 at 20:28:55 and then let's look for activity in the next minute or so after this first Sysmon event occurs.

- As we scroll through the list of Sysmon events, we see this event shortly after the winword.exe execution. A quick glance at the CommandLine shows encoded PowerShell. Let's grab the encoded PowerShell. It is mentioned that it is encoded in base64. So using an online base64 decoder, we find the following output.

What have we learned?

- Billy Tun appears to have executed the attachment invoice.doc.
- Invoice.doc was extracted from invoice.zip that was found in the spearphishing email
- PowerShell was executed after the documented was opened.
- The PowerShell found after the document was opened is identical to PowerShell found in a previous hunt for PowerShell Empire that was conducted.