**Splunk BOTSv3 - Level 300 Questions**

**Question 300**

|  |  |
| --- | --- |
| **Question** | What is the full user agent string that uploaded the malicious link file to OneDrive? |
| **Working** | Link files have an extension of “.lnk” and to search for activity related to one drive, search the “ms:o365:management” sourcetype. This gives a few events which reference the same file:  BRUCE BIRTHDAY HAPPY HOUR PICS.lnk  Going down the fields, you can find the operation field which presents the option of “FileUploaded”    This gives us one event with the User Agent String we need. Interestingly Naenara is a North Korean web browser.  Note for later: users IP is 104.207.83.63 and their user id = bgist@froth.ly |
| **Commands** | index=botsv3 sourcetype="ms:o365:management" "\*.lnk" Operation=FileUploaded |
| **Answer** | Mozilla/5.0 (X11; U; Linux i686; ko-KP; rv: 19.1br) Gecko/20130508 Fedora/1.9.1-2.5.rs3.0 NaenaraBrowser/3.5b4 |

**Question 301**

|  |  |
| --- | --- |
| **Question** | What external client IP address is able to initiate successful logins to Frothly using an expired user account? |
| **Working** | Going to the sourcetype of “ms:aad:signin” and searching for “\*expire\*” gives us one event where the user appears to have entered an expired password:    Searching for the userPrincipleName leads us to us 11 events where it appears that after 3 attempts the users logged in and all events have the same IP address. |
| **Commands** | 1. index=botsv3 sourcetype="ms:aad:signin" "\*expire\*" 2. index=botsv3 sourcetype="ms:aad:signin" userPrincipalName="klagerfield@froth.ly" |
| **Answer** | 199.66.91.253 |

**Question 302**

|  |  |
| --- | --- |
| **Question** | According to Symantec's website, what is the discovery date of the malware identified in the macro-enabled file? Answer guidance: Provide the US date format MM/DD/YY. (Example: January 1, 2019 should be provided as 01/01/19) |
| **Working** | The hint says to search the wineventlog:application sourcetype but for whatever reason it has become a source category and the sourcetype is wineventlog. Further filtering on the SourceName field for “Symantec AntiVirus” gives a couple of events with the one below being a macro enabled Excel file.    Searching Google for W97M.Empstage leads us to Broadcom’s website where it claims the definition was created on 11/12/2016 which the scoreboard says is wrong. Going to the Wayback Machine, in the desperate hope that its catalogued Symantec’s old website, thankfully we have the answer in the below picture |
| **Commands** | index="botsv3" sourcetype="wineventlog" source="wineventlog:application" SourceName="Symantec AntiVirus"  | table Message |
| **Answer** | 11/11/16 |

**Question 303**

|  |  |
| --- | --- |
| **Question** | What is the password for the user that was successfully created by the user "root" on the on-premises Linux system? |
| **Working** | This took a while to obtain. I first went to the linux\_secure and linux\_audit source types where you can find evidence that root has created a couple of users  ec2-user looks interesting but searching on this across linux\_audit, bash\_history or even unix:useraccounts doesn’t lead to anything promising. Unix:useraccounts sourcetype actually has a password field that’s set to X but is wrong. Turning to the hints, it suggests using “osquery:results”. Looking into osquery it shows that the root account created the account tomcat7 and shows the command that it used to create that user. This command contains the password with the string after the -p argument. |
| **Commands** | 1. index=botsv3 sourcetype=linux\_audit user\_id=0 command=useradd 2. index=botsv3 sourcetype="osquery:results" columns.cmdline="\*useradd\*" "decorations.username"=root |
| **Answer** | ilovedavidverve |

**Question 304**

|  |  |
| --- | --- |
| **Question** | What is the name of the user that was created after the endpoint was compromised? |
| **Working** | I feel like I should know more about this question. Which compromise is it talking about and what kind of endpoint are we talking about? Is it the AWS account, a Linux server or a windows server?  Anyway the hint suggests to go look at WinEventLog:Security. Looking into the events stored, there’s a “User Account Management” category and created action which gives us 1 event. In the message of this event, it says a new account was created with the name of “svcvnc” which suspiciously has the naming of a windows service (e.g. svchost) |
| **Commands** | index="botsv3" sourcetype="wineventlog" source="WinEventLog:Security" category="User Account Management" action=created |
| **Answer** | svcvnc |

**Question 305**

|  |  |
| --- | --- |
| **Question** | What is the process ID of the process listening on a "leet" port? |
| **Working** | Leet is also written as 1337 and searching for this reveals a couple of source types but the most useful looking is “Unix:ListeningPorts”. Narrowing it down further to src and dest ports that are assigned to 1337 we get 1 event where the process of netcat is running. The answer can be found within the pid field. |
| **Commands** | index=botsv3 (src\_port=1337 OR dest\_port=1337) sourcetype="Unix:ListeningPorts" |
| **Answer** | 14356 |

**Question 306**

|  |  |
| --- | --- |
| **Question** | A search query originating from an external IP address of Frothly's mail server yields some interesting search terms. What is the search string? |
| **Working** | It seems from the stream:smtp events that the organisation is using outlook for their emails which means they probably have an exchange server. Doing a general search for exchange led to the ms:o365:management sourcetype. And looking at the workloads we see Exchange among the options:    Searching through the fields, there is one called operation which shows an option for “New-MailboxSearch” and adding this to our search we get the following event with a suspect search:    Just to determine whether this is frothly’s normal naming convention for their mail servers I searched across the Exchange events and deduped the Originating servers and got the below results:    Thus, our search above seems legitimate. |
| **Commands** | 1. index=botsv3 sourcetype="ms:o365:management" Workload=Exchange Operation="New-MailboxSearch" 2. index=botsv3 sourcetype="ms:o365:management" Workload=Exchange | dedup OriginatingServer | table OrganizationName, OriginatingServer |
| **Answer** | cromdale OR beer OR financial OR secret |

**Question 307**

|  |  |
| --- | --- |
| **Question** | What is the MD5 value of the file downloaded to Fyodor's endpoint system and used to scan Frothly's network? |
| **Working** | The hint says to go look at the symon sourcetype. Narrowing the search to Fyodor’s computer we see a number of events with some event codes. Searching for Sysmon event codes I came across Microsoft’s guide to their codes: <https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>  Since it’s scanning the network, that suggests the process would be doing a lot of network connections so we’ll narrow it down to event code 3. Looking at some of the files that have been loaded we see the following:    Searching for hdoor, the first result on google is a MITRE ATT&CK page saying its malware. Next searching on this file and searching for event code 1 where the process/file was created allows us to see the MD5 Hash that was generated. |
| **Commands** | 1. index=botsv3 sourcetype="xmlwineventlog" Computer="FYODOR-L.froth.ly" EventID=3 2. index=botsv3 sourcetype="xmlwineventlog" Computer="FYODOR-L.froth.ly" Image="C:\\Windows\\Temp\\hdoor.exe" EventCode=1 |
| **Answer** | 586EF56F4D8963DD546163AC31C865D7 |

**Question 308**

|  |  |
| --- | --- |
| **Question** | Based on the information gathered for question 304, what groups was this user assigned to after the endpoint was compromised? Answer guidance: Comma separated without spaces, in alphabetical order. |
| **Working** | The user svcvnc was created 20/8/2018 8:08:17 PM. Searching for that user after this time leads to the “wineventlog:security” sourcetype. Looking at the fields there’s a signature field with the following values:    User’s being added to local groups looks like a suitable signature to search against. Looking into the 2 events we see the account was added to the Administrators and Users groups. |
| **Commands** | index="botsv3" sourcetype="wineventlog" signature="A member was added to a security-enabled local group" "svcvnc" |
| **Answer** | administrators,users |

**Question 309**

|  |  |
| --- | --- |
| **Question** | At some point during the attack, a user's domain account is disabled. What is the email address of the user whose account gets disabled and what is the email address of the user who disabled their account? Answer guidance: Comma separated without spaces, in alphabetical order. (Example: [jdoe@mycompany.com](mailto:jdoe@mycompany.com),tmiller@mycompany.com) |
| **Working** | Originally, I went looking through the wineventlog events and thought I may have found the answer as I saw there was a signature that was “User logon to account was disabled by administrator”    As the event it just about a login failing, I tried to search for the event where the user may have been disabled but to no avail. Looking at the hint it says to go look at the ms:aad:audit sourcetype which is for data to do with Azure Active Directory. Here we quickly find the “Disable account activity” which provides both the user who was disabled and the culprit |
| **Commands** | * index="botsv3" sourcetype="wineventlog" source="WinEventLog:Security" signature="User logon to account disabled by administrator" |
| **Answer** | bgist@froth.ly,fyodor@froth.ly |

**Question 310**

|  |  |
| --- | --- |
| **Question** | Another set of phishing emails were sent to Frothly employees after the adversary gained a foothold on a Frothly computer. This malicious content was detected and left behind a digital artifact. What is the name of this file? Answer guidance: Include the file extension. (Example: badfile.docx) |
| **Working** | Looking at the stream:smtp sourcetype and filtering to emails that have attachments we find    Now pwned does look dodgy but first let’s look at Malware Alert Text. According to this site: <https://www.law.upenn.edu/its/docs/office/office-365-ATP.php> it seems to be part of a feature of Exchange email servers where if malware is detected, it removes the attachment and replaces it with this text file.  Note to self this email got sent around (2018-08-20T09:55:14.433322Z)  Looking into this email attachment, its encoded in base64    Decoding it leads to: |
| **Commands** | 1. index="botsv3" sourcetype="stream:smtp"  | stats values("attach\_filename{}") 2. index="botsv3" sourcetype="stream:smtp" "attach\_filename{}"=\* "attach\_filename{}"="Malware Alert Text.txt" |
| **Answer** | Frothly-Brewery-Financial-Planning-FY2019-Draft.xlsm |

**Question 311**

|  |  |
| --- | --- |
| **Question** | Based on the answer to question 310, what is the name of the executable that was embedded in the malware? Answer guidance: Include the file extension. (Example: explorer.exe) |
| **Working** | Searching for all events where the filename in above question gives us 2 events, 1 of which mentions a HxTsr.exe file. Searching online for this suggests that it’s clean and that is part of Office but apparently this is our answer. |
| **Commands** | index="botsv3" "Frothly-Brewery-Financial-Planning-FY2019-Draft\*" |
| **Answer** | [HxTsr.exe](./sourcetype%3Dxmlwineventlog&display.page.search.mode=verbose&dispatch.sample_ratio=1&workload_pool=&earliest=0&latest=now&sid=1728632770.1952) |

**Question 312**

|  |  |
| --- | --- |
| **Question** | How many unique IP addresses "used" the malicious link file that was sent? |
| **Working** | Going back to the question 300, doing a general search for the lnk file there’s a value of “Anonymous Link Used” for the Operation field. Then just distinct count the src\_ip addresses in the events to get the answer |
| **Commands** | index="botsv3" "BRUCE BIRTHDAY HAPPY HOUR PICS.lnk" sourcetype="ms:o365:management" Operation=AnonymousLinkUsed  | stats dc(src\_ip) |
| **Answer** | 7 |

**Question 314**

|  |  |
| --- | --- |
| **Question** | What port number did the adversary use to download their attack tools? |
| **Working** | Unsure how to approach this question, will try again later. |
| **Commands** |  |
| **Answer** |  |

**Question 315**

|  |  |
| --- | --- |
| **Question** | During the attack, two files are remotely streamed to the /tmp directory of the on-premises Linux server by the adversary. What are the names of these files? Answer guidance: Comma separated without spaces, in alphabetical order, include the file extension where applicable. |
| **Working** | The hints say to go check “osquery:results”. The category column seems to be the field that holds the folder being used for folders. Next looking at the target\_path there’s a super suspect looking file called “definitelydontinvestigatethisfile.sh”. Checking out the colonel files on the events before and after leads to the answer. |
| **Commands** | index=botsv3 sourcetype="osquery:results" "columns.action"=CREATED "columns.category"=tmp  | table \_time, decorations.username, columns.target\_path |
| **Answer** | colonel,definitelydontinvestigatethisfile.sh |

**Question 317**

|  |  |
| --- | --- |
| **Question** | What is the first executable uploaded to the domain admin account's compromised endpoint system? Answer guidance: Include the file extension. |
| **Working** | Going back to Sysmon and restricting the TargetFilename to “exe” files we eventually see the file hdoor.exe again. |
| **Commands** | index=botsv3 sourcetype="XmlWinEventLog" TargetFilename="\*.exe" (EventCode=11 OR EventCode=15)  | table host, Image, TargetFilename, EventData\_Xml | reverse |
| **Answer** | hdoor.exe |

**Question 318**

|  |  |
| --- | --- |
| **Question** | From what country is a small brute force or password spray attack occurring against the Frothly web servers? |
| **Working** | Hint says to go look at Linux\_Secure. Upon looking at the events it seems there’s a lot of IP addresses but the one’s that show up in failure events are from the US or Canada. So, this might not be from a single IP address but rather from a block of them. Using the iplocation command and then counting the events by country we get Russia as our second highest source of events. |
| **Commands** | index=botsv3 sourcetype="linux\_secure" action!=created | iplocation source\_ip | stats count by Country | sort -count |
| **Answer** | Russia |

**Question 319**

|  |  |
| --- | --- |
| **Question** | The adversary created a BCC rule to forward Frothly's email to his personal account. What is the value of the "Name" parameter set to? |
| **Working** | Searching for how outlook rules would be defined in Splunk source types this site can be found: <https://research.splunk.com/cloud/289ed0a1-4c78-4a43-9321-44ea2e089c14/> Which suggests to look at the o365\_management source type and find an operation called “New-TransportRule”. Upon searching for these constraints, 1 event is found with with the following information:    Interestingly, Naver seems to belong to a South Korean company. Looking up SOX also gives results for the Sarbanes-Oxley act which is to do with compliance. This may have been an attempt to appear legitimate. |
| **Commands** | index=botsv3 sourcetype="ms:o365:management" Workload=Exchange Operation="New-TransportRule" |
| **Answer** | SOX |

**Question 320**

|  |  |
| --- | --- |
| **Question** | What is the password for the user that was created on the compromised endpoint? |
| **Working** | In question 304 it was identified that the attackers created the user account “svcvnc”. Searching for this user and the string “pass\*” in the Windows Event Logs gives 5 events. And in one of the events the net command can be seen being used to add the user and create their password. |
| **Commands** | index=botsv3 "svcvnc" "pass\*" sourcetype=wineventlog |
| **Answer** | Password123! |

**Question 321**

|  |  |
| --- | --- |
| **Question** | The Taedonggang adversary sent Grace Hoppy an email bragging about the successful exfiltration of customer data. How many Frothly customer emails were exposed or revealed? |
| **Working** | Searching the emails for Grace Hoppy, you’ll see the first event has an email from Grace to everybody else about how she received an email from someone claiming “All your datas belong to us” with a Pastebin link  If you find the original version of this email. The attacker encoded it in Base64, so it’s nice we don’t have to go through the effort of decryption here. The link has expired but thankfully archive.md (a Wayback Machine alternative) has stored an old copy.    Then you just need to count the email addresses present in the text dump. |
| **Commands** | index=botsv3 sourcetype="stream:smtp" "ghoppy@froth.ly" |
| **Answer** | 8 |

**Question 322**

|  |  |
| --- | --- |
| **Question** | What is the path of the URL being accessed by the command and control server? Answer guidance: Provide the full path. (Example: The full path for the URL https://imgur.com/a/mAqgt4S/lasd3.jpg is /a/mAqgt4S/lasd3.jpg) |
| **Working** | Going back to 317, when viewing the context around “hdoor.exe” there is definitely shenanigans happening with the surrounding PowerShell commands as it has been encoded in Base64. The hint too, says to go look at the PowerShell logs. The PowerShell logs conveniently give the commands in plain text but it’s still obfuscated. There is however a section towards the end of the code that mentions the path. Extracting these paths and counting the occurrences gives the answer: |
| **Commands** | index=botsv3 sourcetype="wineventlog" source="WinEventLog:Microsoft-Windows-PowerShell/Operational" | rex field=Message "(?<urlpath>\;\$t\=\'[a-zA-Z0-9\/\.]+\'\;)" | stats count by urlpath |
| **Answer** | /admin/get.php |

**Question 323**

|  |  |
| --- | --- |
| **Question** | At least two Frothly endpoints contact the adversary's command and control infrastructure. What are their short hostnames? Answer guidance: Comma separated without spaces, in alphabetical order. |
| **Working** | Changing the last question to count by host as well as the url path gives the answer. |
| **Commands** | index=botsv3 sourcetype="wineventlog" source="WinEventLog:Microsoft-Windows-PowerShell/Operational" | rex field=Message "(?<urlpath>\;\$t\=\'[a-zA-Z0-9\/\.]+\'\;)" | stats count by urlpath, host |
| **Answer** | ABUNGST-L,FYODOR-L |

**Question 324**

|  |  |
| --- | --- |
| **Question** | Who is Al Bungstein's cell phone provider/carrier? Answer guidance: Two words. |
| **Working** | Doing a general search for “ABUNGST” and looking at the source types, there’s one that looks promising; “Script:GetEndpointInfo”. Using this provides 1 event with Verizon Wireless in the event data. My guess is this employee has company MFA or Data Loss Prevention software on their phone and it’s recording the phone metadata. |
| **Commands** | index=botsv3 "ABUNGST" sourcetype="Script:GetEndpointInfo" |
| **Answer** | Verizon Wireless |

**Question 325**

|  |  |
| --- | --- |
| **Question** | Microsoft cloud services often have a delay or lag between "index time" and "event creation time". For the entire day, what is the max lag, in minutes, for the sourcetype: ms:aad:signin? Answer guidance: Round to the nearest minute without the unit of measure. |
| **Working** | Nice simple question; Get the difference between the index and event creation times, find the max and then round. |
| **Commands** | index=botsv3 sourcetype="ms:aad:signin" | eval drift=\_indextime-\_time | stats max(drift) as MaxDrift | eval MaxDrift=Round((MaxDrift/60)) |
| **Answer** | 51 |

**Question 326**

|  |  |
| --- | --- |
| **Question** | According to Mallory's advertising research, how is beer meant to be enjoyed? Answer guidance: One word. |
| **Working** | This took forever to get because I thought I was meant to view the file contents inside Splunk.  The hint says to go look at the code42:security sourcetype. Narrowing this further by Mallory as the process owner, you can then look at the file names available:    Since it was downloaded via chrome, searching for the this file online leads to this website that hosts it: <https://www.brewersassociation.org/wp-content/uploads/2017/04/BA_Advertising_Code_Overview.pdf>  Reading through it, it’s filled with obvious tagline that the alcohol is meant to be enjoyed responsibly. |
| **Commands** | index=botsv3 sourcetype="code42:security" processOwner=MalloryKraeusen | stats values("files{}.fileName") |
| **Answer** | responsibly |

**Question 328**

|  |  |
| --- | --- |
| **Question** | What text is displayed on line 2 of the file used to escalate tomcat8's permissions to root? Answer guidance: Provide contents of the entire line. |
| **Working** | Searching for tomcat8 we find a few results and sourcetypes. Viewing some of the osquery:result events, shows files that have been previously marked as suspicious    Searching for definitelydontinvestigatethisfile.sh in the wineventlog sourcetype shows data being streamed into it as base64 but further examination of the base64 string makes it appear to be an image file. The colonel file also has base64 contents and decoding this gives you a human readable file where the second line includes the words “priv esc” short for privilege escalation! |
| **Commands** | 1. index=botsv3 "tomcat8" sourcetype="osquery:results" "columns.action"=UPDATED | stats values("columns.target\_path") 2. index=botsv3 "/tmp/colonel" sourcetype=wineventlog |
| **Answer** | \* Ubuntu 16.04.4 kernel priv esc |

**Question 329**

|  |  |
| --- | --- |
| **Question** | One of the files uploaded by Taedonggang contains a word that is a much larger in font size than any other in the file. What is that word? |
| **Working** | The hint says to go view the WinEventLogs or osquery:results. Looking at osquery for files that have been created and we come across the files mentioned in a previous question that the user tomcat8 created    We’ve already investigated the base64 for colonel, so we shall investigate the base64 for definitelydontinvestigatethisfile.sh. Decoding it using CyberChef from base64, the site claims it’s an image format and transforming it into an image we get the following:    Splunk is a piece of text in the background and apparently our answer. |
| **Commands** | 1. index=botsv3 sourcetype="osquery:results" ("columns.action"=CREATED OR "columns.action"=UPDATED) | stats values("columns.target\_path") by "decorations.username" 2. index=botsv3 "definitelydontinvestigatethisfile" | table CommandLine, ParentCommandLine |
| **Answer** | Splunk |

**Question 330**

|  |  |
| --- | --- |
| **Question** | What Frothly VPN user generated the most traffic? Answer guidance: Provide the VPN user name. |
| **Working** | From the previous questions I’ve seen mention of the Cisco ASA and AnyConnect and I thought some of the software might be shenanigans scanning the network or creating backdoors but looks like its genuine software allowing employees to work from home. Going into the cisco:asa source type there are quite a few events. Narrowing the events down by the signatures of SVC, AnyConnect and WebVPN and getting the top Cisco\_ASA\_user presents the answer |
| **Commands** | index=botsv3 sourcetype="cisco:asa" Cisco\_ASA\_user=\* (signature=SVC OR signature=AnyConnect OR signature=WebVPN) | top Cisco\_ASA\_user limit=1 |
| **Answer** | mkraeusen |

**Question 331**

|  |  |
| --- | --- |
| **Question** | Using Splunk commands only, what is the upper fence (UF) value of the interquartile range (IQR) of the count of event code 4688 by Windows hosts over the entire day? Use a 1.5 multiplier. Answer guidance: UF = Q3 + 1.5 x IQR |
| **Working** | What on earth? Searching for “Splunk” and “interquartile range” leads to a community post which in turn leads to this Splunk Article - <https://docs.splunk.com/Documentation/Splunk/latest/Search/Findingandremovingoutliers>  The article states the formula for the IQR is 75th Percentile - 25th Percentile and to do this you need to use the eventstats and p<Integer> commands. |
| **Commands** | index=botsv3 sourcetype="WinEventLog" EventCode=4688 | stats count as hostcount by host | eventstats p25(hostcount) as Q1, p75(hostcount) as Q3 | eval IQR=Q3-Q1 | eval UF=Q3+(1.5\*IQR) |
| **Answer** | 1368 |

**Question 332**

|  |  |
| --- | --- |
| **Question** | What is the CVE of the vulnerability that escalated permissions on Linux host hoth? Answer guidance: Submit in normal CVE format. (Example: cve-2018-9805) |
| **Working** | In the answer for question 328, you can see that the start of the Base64 string mentioned an Ubuntu privilege escalation and the author who made it. Searching google for this, leads to this site: <https://vulners.com/exploitdb/EDB-ID:45058>  And this site gives us the CVE number. |
| **Commands** |  |
| **Answer** | CVE-2017-16995 |

**Question 333**

|  |  |
| --- | --- |
| **Question** | What is the CVE of the vulnerability that was exploited to run commands on Linux host hoth? Answer guidance: Submit in normal CVE format. (Example: cve-2018-9805) |
| **Working** | The last hint suggests that there’s strange code being put into a web form so we shall look into the “stream:http” sourcetype and narrow the search to the hoth host and the POST method.    The form\_data has a lot of strange code but the uri\_path has saveGangster.action which doesn’t appear legitimate. Searching for this on google leads to an exploit-db page about a remote code execution vulnerability: https://www.exploit-db.com/exploits/42324 |
| **Commands** | index=botsv3 sourcetype="stream:http" host=hoth http\_method=POST |
| **Answer** | CVE-2017-9791 |