Threat Hunting with a SIEM

Mustafa Ranapurwala | Ross Barber | Carina Martinez-Lopez | Zoe Medina | Randall Seymore
20 November 2023
CYBR 512

For issues with embedded content, please use the Google Doc
https://docs.google.com/document/d/142IdinbUHd0MH5nbc5ZSvv0IzKlf3YdhLef0vkH5KMk/edit?usp=sharing

Table of Contents

Statement of Objective

This lab is intended to review the results of searches in Splunk performed in the context of detecting an Advanced Persistent Threat (APT) spear phishing attack by a fictional nation-state actor. The team seeks to combine various searches into a dashboard, correlating malicious activity to facilitate incident response and contain the attack.

Theory

Testers expect to effectively identify "suspicious email attachments" through analysis of various Splunk searches centered around files observed during a given timeframe. Spear phishing attempts often involve emails with attachments sent to an unusually small number of recipients within an organization, or in some cases to a single individual. By setting thresholds for what constitutes a typical versus atypical number of recipients, then correlating this with attachment types, sizes, and additional data points, searches should be able to flag potential spear phishing activities.

Description of Experimental Setup

A Splunk Server was made available by Boss of the SOC (BOTS) leveraging the publicly-available BOTS dataset across various Splunk apps and threat hunting queries. Testers logged into https://apthunting.splunk.show using credentials provided on the “Hunting an APT with Splunk - Initial Access” Scenario Resources page.

Procedure

Initial searches will aggregate the number of emails received by each individual in the BOTS dataset, focusing on those who receive more than 10 emails in a month-long period to identify potential targets of interest. This list will then be leveraged in a new search to filter emails sharing identical attachment filenames to identify similarities in file names. A new field, “Attachment,” will be created to combine filename and size for unique identification, followed by a count of these unique values. Subsequently, the number of unique recipients per attachment type will be calculated to pinpoint targeted spear phishing attacks. Results will be visually represented through a bar chart with a set Y-Axis interval, enhancing the interpretability of the data. Finally, a comprehensive dashboard will be crafted, integrating results from all searches and making them usable for ongoing monitoring and rapid response to suspicious email attachment activities.

Data

Setup

Login to BOTS Splunk instance

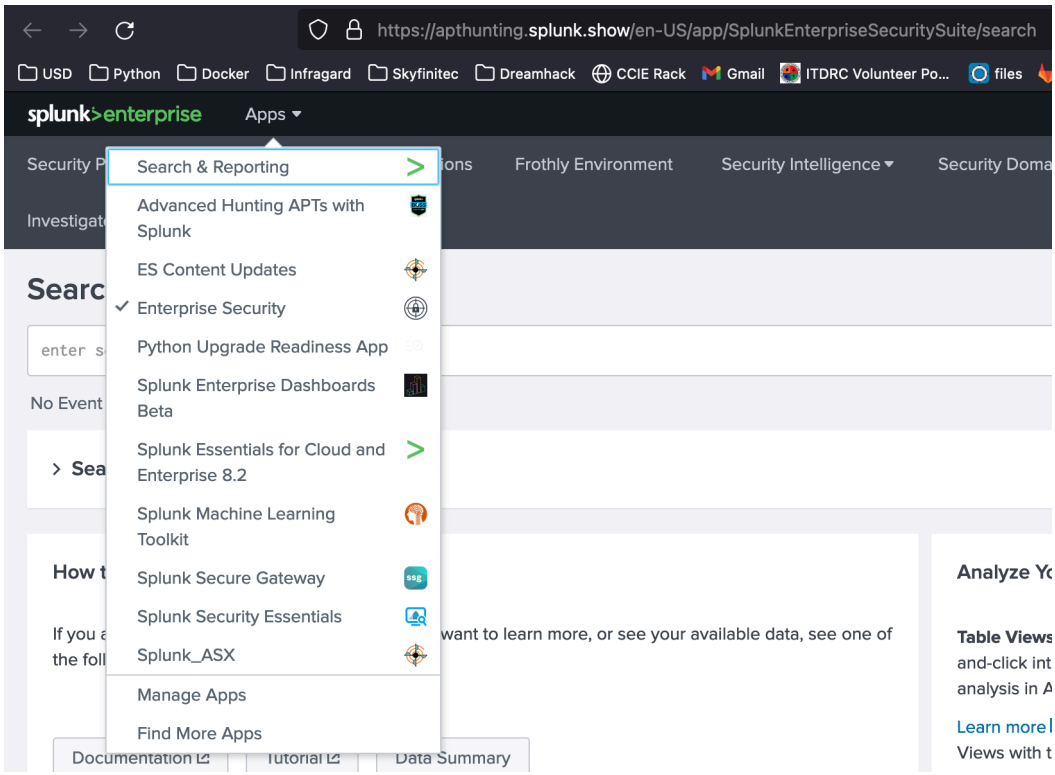
SUMMARY RESOURCES

Access the Splunk Server to answer questions throughout this workshop, using the below shown server and credentials:

SplunkServer: https://apthunting.splunk.show

User ID: user001-splk

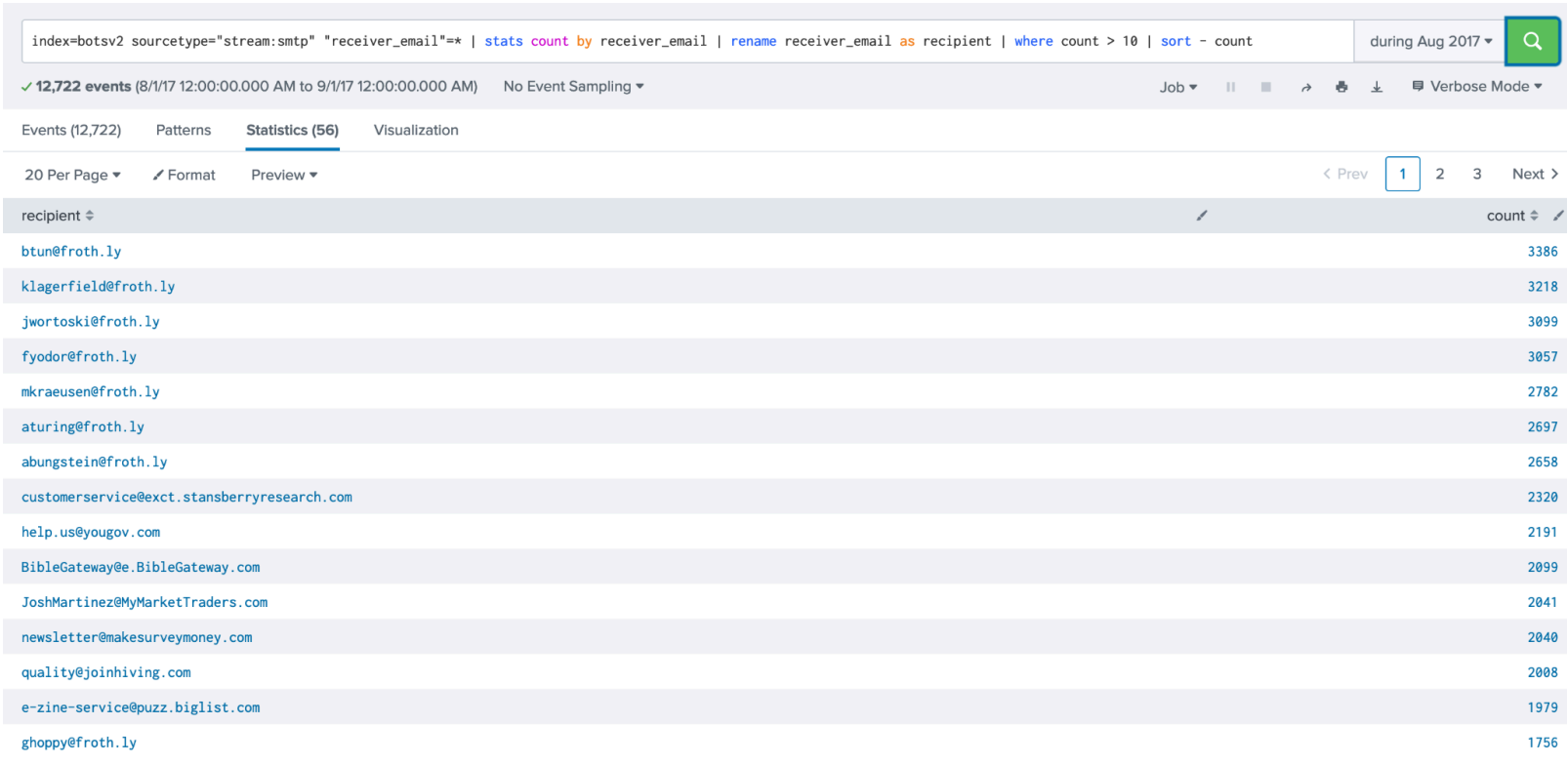
Password: Splunk.5



Initial Searches

Search and results displaying number of emails received by recipient during August 2017, filtered on addresses that received more than ten emails throughout the month

Search String	Explanation
index=botsv2 sourcetype=”stream:smtp” “receiver_email”=* | stats count by receiver_email | rename receiver_email as recipient | where count > 10 | sort - count	This search works by filtering only for events that contain a “receiver_email” field and counts the number of events for each unique email address. Then, the search only displays email addresses with a count of over 10 and sorts the emails by count in descending order.

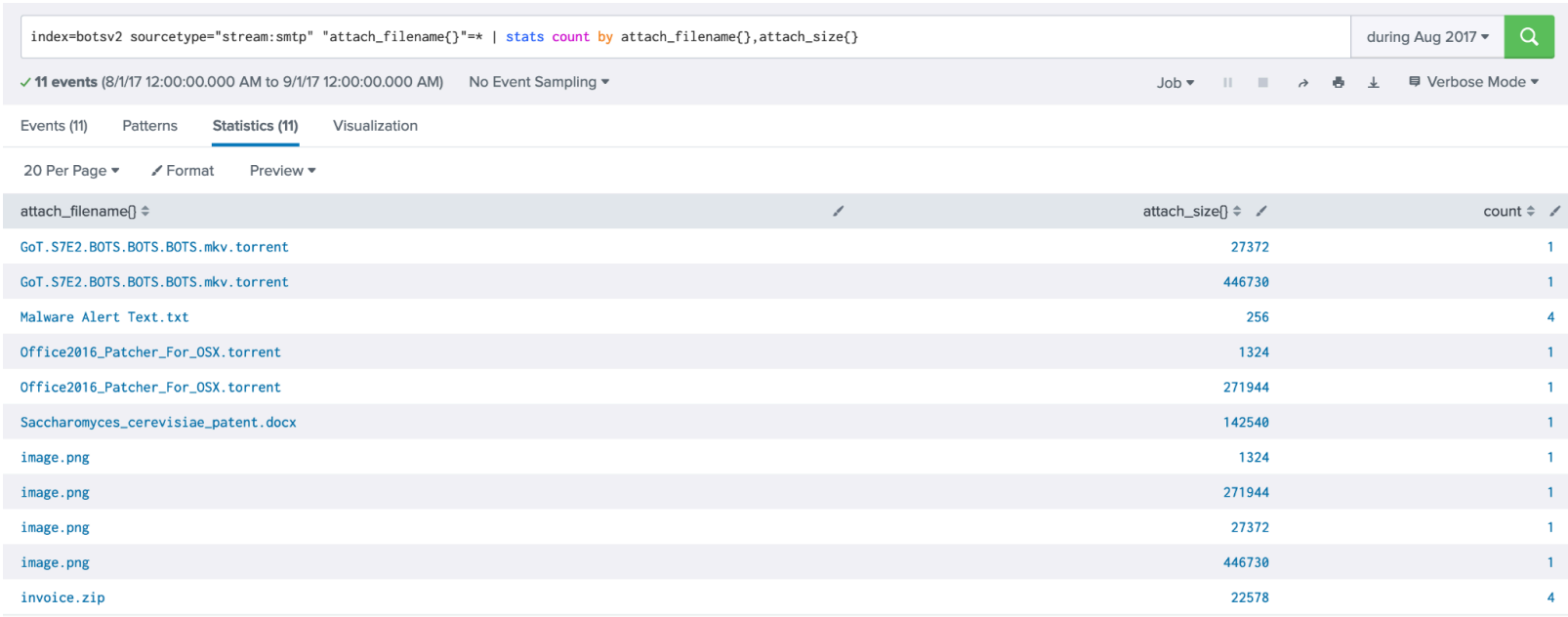


Search and results displaying number of emails with similar attachment filename

Search String	Explanation
index=botsv2 sourcetype=”stream:smtp” “attach_filename{}”=* | stats count by attach_filename{} | sort count	This search works by filtering only for events that contain an “attach_filename” field and counts the number of events for each unique file name. Then, the search sorts the count value in increasing order.

Search and results displaying number of email attachments with same unique combination of file name and size

Search String	Explanation
index=botsv2 sourcetype=”stream:smtp” “attach_filename{}”=* | stats count by attach_filename{},attach_size{}	This search works by filtering only for events that contain an “attach_filename” field and counts the number of events for each unique attachment file name and attachment file size. Then, the search displays the attachment size for each file name.



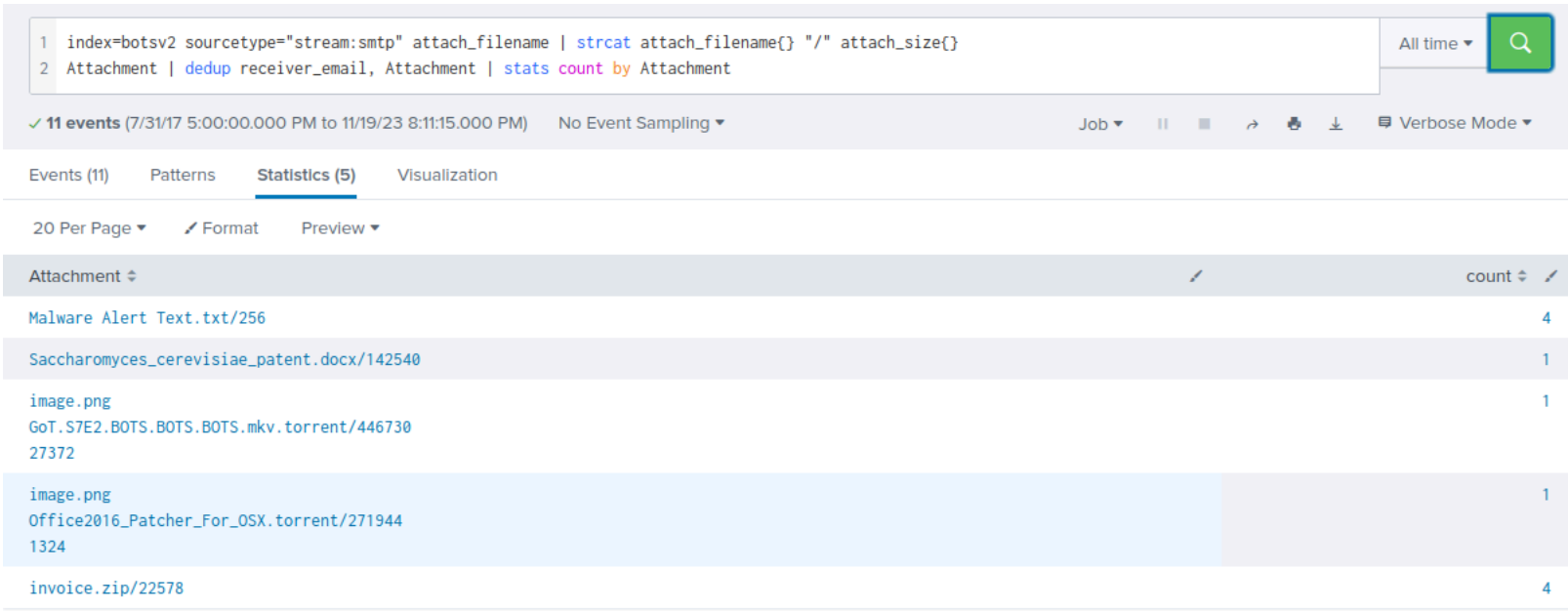
attach_filename{}	attach_size{}	count
GoT.S7E2.BOTS.BOTS.BOTS.mkv.torrent	27372	1
GoT.S7E2.BOTS.BOTS.BOTS.mkv.torrent	446730	1
Malware Alert Text.txt	256	4
Office2016_Patcher_For_OSX.torrent	1324	1
Office2016_Patcher_For_OSX.torrent	271944	1
Saccharomyces_cerevisiae_patent.docx	142540	1
image.png	1324	1
image.png	271944	1
image.png	27372	1
image.png	446730	1
invoice.zip	22578	4

Search and results displaying file attachments along with the attachment size, and the count of unique filenames.

Search String	Explanation
index=botsv2 sourcetype=”stream:smtp” “attach_filename{}”=* “attach_size{}”=* | strcat attach_filename{} “/” attach_size{} Attachment | stats count by Attachment	This search works by filtering only for events that contain an “attach_filename” field and an “attach_size” field. Then, It concatenates the “attach_filename” field and the “attach_size” field with a “/” in between and presents the new string under the field “Attachment.” Finally, the search counts the number of events for each unique “Attachment” string and displays the results.

Search and results displaying the number of unique recipients for each type of unique attachment.

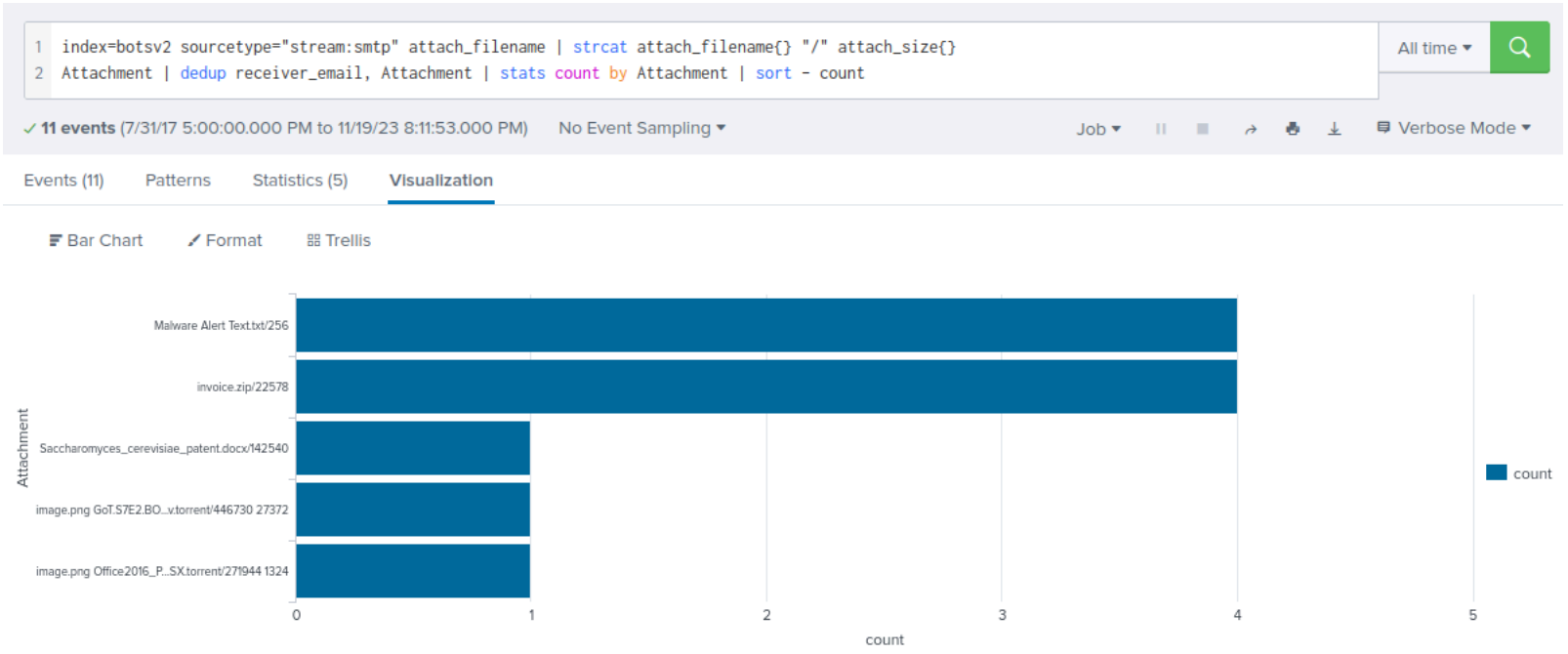
Search String	Explanation
index=botsv2 sourcetype=”stream:smtp” attach_filename | strcat attach_filename{} “/” attach_size{} Attachment | dedup receiver_email, Attachment | stats count by Attachment	This search works by filtering only for events that contain an “attach_filename” field. Then, It concatenates the “attach_filename” field and the “attach_size” field with a “/” in between and presents the new string under the field “Attachment.” Next, it removes any duplicate events where the “receiver_email” field and “Attachment” string are the same. Finally, the search counts the number of events for each unique “Attachment” string and displays the results.



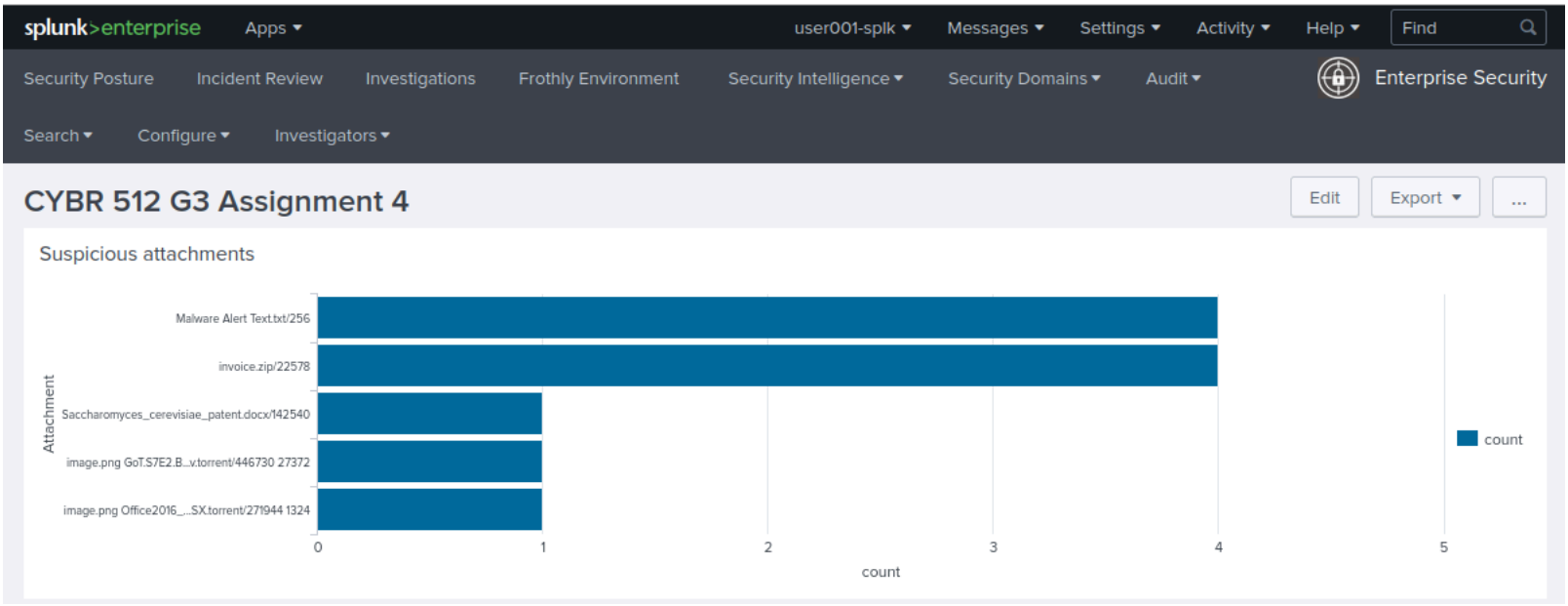
Data Visualization

Bar Chart Conversion

Search String	Explanation
index=botsv2 sourcetype=”stream:smtp” attach_filename | strcat attach_filename{} “/” attach_size{} Attachment | dedup receiver_email, Attachment | stats count by Attachment | sort - count	This search works by filtering only for events that contain an “attach_filename” field. Then, It concatenates the “attach_filename” field and the “attach_size” field with a “/” in between and presents the new string under the field “Attachment.” Next, it removes any duplicate events where the “receiver_email” field and “Attachment” string are the same. Finally, the search counts the number of events for each unique “Attachment” string, sorts the count in decreasing order, and displays the results in a bar chart with an Y-Axis interval of 1.



Dashboard Conversion



Analysis of Data

By ultimately creating a unique representation of each attachment based on filename and size, we were able to quantify the distribution of attachments based on specific time frame and evidence of specifically targeted users. Calculating the number of unique recipients per attachment type revealed patterns indicative of spear phishing, with certain attachments sent to a conspicuously limited number of recipients.

Discussion of Results

Output from Splunk searches offers significant insight into phishing-related behaviors. The team's initial theory that spear phishing attempts might correlate with emails sent to a small number of recipients was substantiated. A discernible pattern was identified where certain attachments were distributed to fewer individuals, aligning with the characteristics of spear phishing attacks. The data also provided visibility into repeated attachment file names across multiple emails, which were correlated with additional data points such as file size to narrow down suspicious email activity.

Conclusion

Overall, the team determined targeted Splunk searches can effectively highlight suspicious email attachments indicative of spear phishing activities. By establishing thresholds for normal and abnormal recipient counts, attachment file names, and sizes, searches could successfully pinpoint potential security breaches. The analysis strategy outlined in this lab demonstrates that a similar dataset can be combined with appropriate correlation techniques and become a robust method for identifying sophisticated cyber threats. Finally, creating a comprehensive but digestible dashboard from these results is an important step to aid ongoing surveillance and proactive threat mitigation.