Assignment 4.1: Threat Hunting with a SIEM

Julia Andersen, Kayvon Karimi, Jacob Napierskie and Dale Whitehead

Shiley-Marcos School of Engineering, University of San Diego

CYBR-512: Incident Detection and Handling

Professor Mark Heckman, Ph.D.

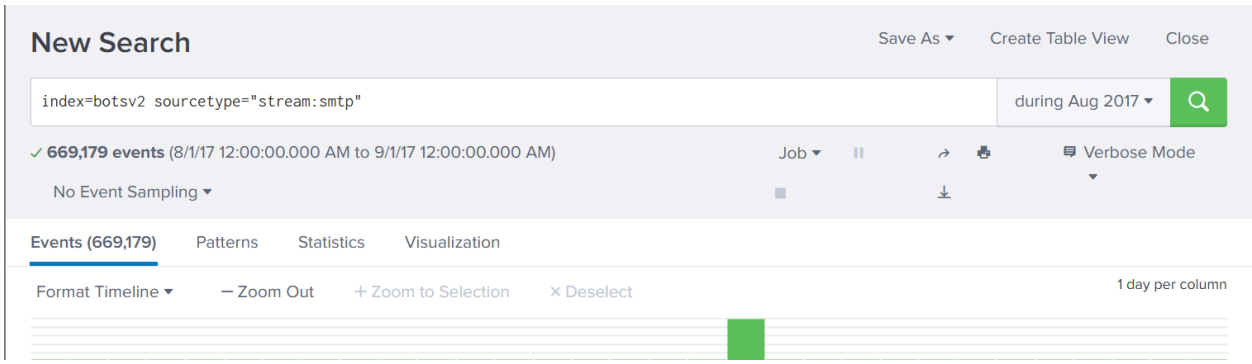
November 18, 2024

First search of smtp events for the month of August, 2017.
Search string used:
index=botsv2 sourcetype="stream:smtp"

How the search works:

- index=botsv2: Limits the search to the botsv2 index, a dataset commonly used for cybersecurity training with simulated attack data.
- sourcetype="stream:smtp": Filters events to only those related to SMTP (email) traffic, such as sender, recipient, and attachment details.
- Purpose: Retrieves email-related events from a cybersecurity dataset, typically used to analyze email activity for threats like phishing or suspicious attachments.

Search string and result:



1. Count the number of emails each person receives, but only for people who receive more than 10 emails. Sort the results in decreasing order so the people who get the most email are at the top of the list.

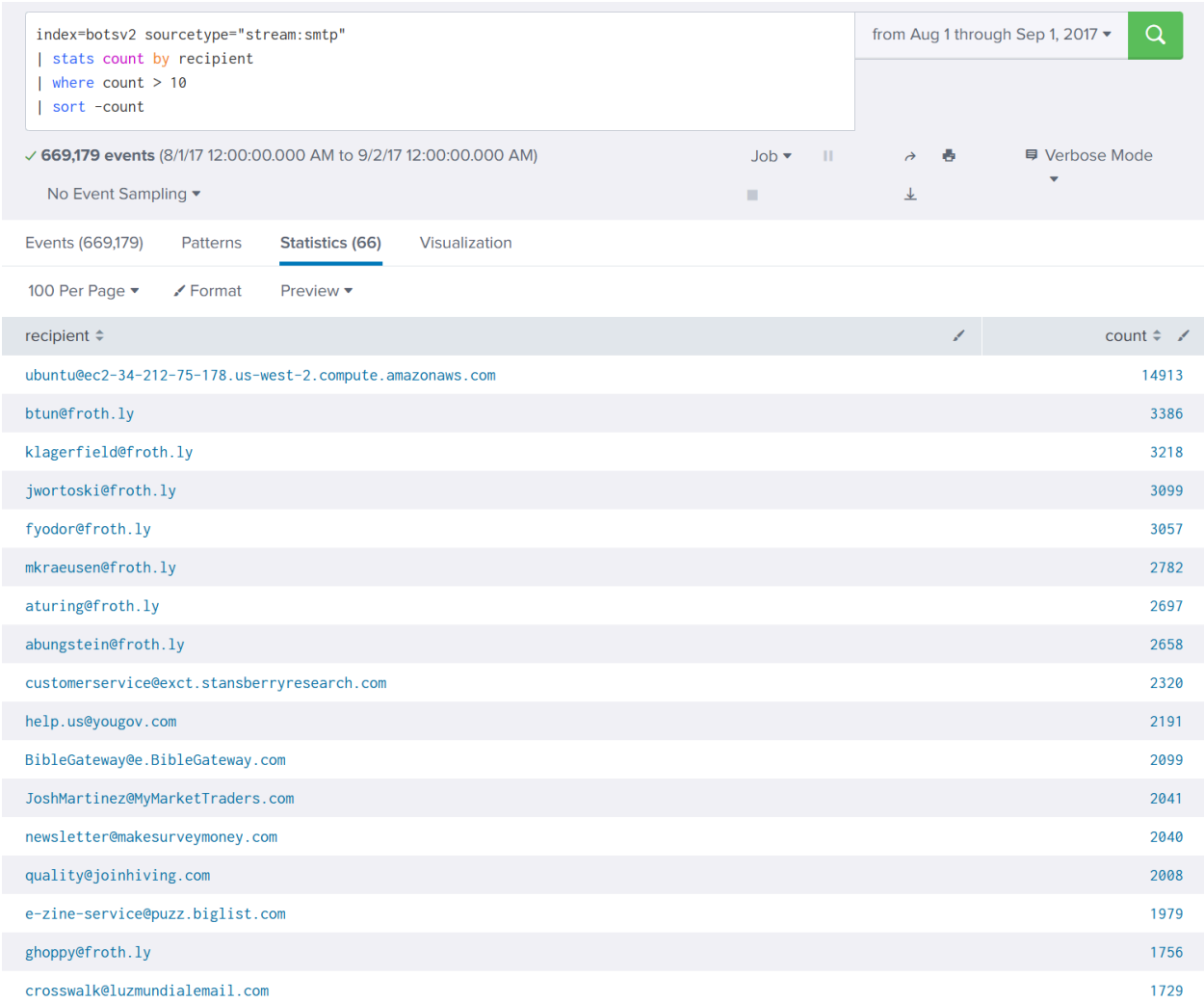
Search string used:
index=botsv2 sourcetype="stream:smtp"
stats count by recipient
where count > 10
sort -count

How the search works:

- index=botsv2 sourcetype="stream:smtp": Searches the botsv2 index for SMTP (email) events, focusing on email traffic data.
- stats count by recipient: Counts the number of emails received by each unique recipient.
- where count > 10: Filters the results to show only recipients who received more than 10 emails.

- sort -count: Sorts the results in descending order by the count, with recipients who received the most emails appearing at the top.

Search string and result:



recipient	count
ubuntu@ec2-34-212-75-178.us-west-2.compute.amazonaws.com	14913
btun@froth.ly	3386
klagerfield@froth.ly	3218
jwortoski@froth.ly	3099
fyodor@froth.ly	3057
mkraeusen@froth.ly	2782
aturing@froth.ly	2697
abungstein@froth.ly	2658
customerservice@exct.stansberryresearch.com	2320
help.us@yougov.com	2191
BibleGateway@e.BibleGateway.com	2099
JoshMartinez@MyMarketTraders.com	2041
newsletter@makesurveymoney.com	2040
quality@joinhiving.com	2008
e-zine-service@puzz.biglist.com	1979
ghoppy@froth.ly	1756
crosswalk@luzmundialemail.com	1729

2. Count the number of emails that have the same attachment filename. Display the results in increasing order.

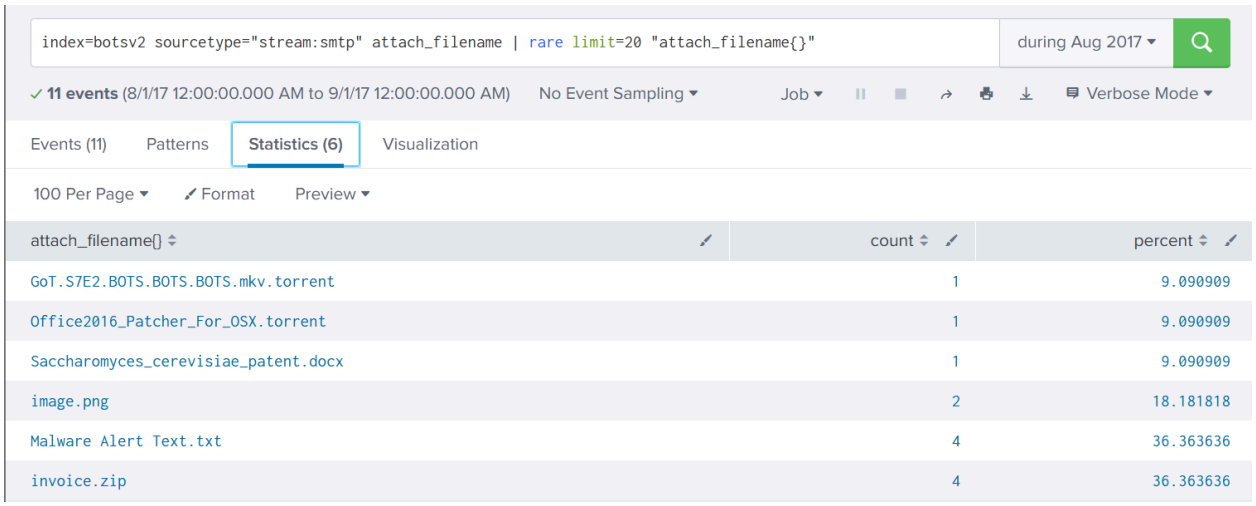
Search string used:
index=botsv2 sourcetype="stream:smtp" attach_filename
| rare limit=20 "attach_filename{}"

How the search works:

- index=botsv2 sourcetype="stream:smtp" attach_filename: Searches within the botsv2 index for SMTP (email) events that include an attachment filename.

- rare limit=20 "attach_filename{}": Finds the 20 least common (rarest) values in the attach_filename field.
- Purpose: Shows the filenames of attachments that appear least frequently in the email data, limited to the 20 rarest.

Search string and result:



attach_filename{}	count	percent
GoT.S7E2.BOTS.BOTS.BOTS.mkv.torrent	1	9.090909
Office2016_Patcher_For_OSX.torrent	1	9.090909
Saccharomyces_cerevisiae_patent.docx	1	9.090909
image.png	2	18.181818
Malware Alert Text.txt	4	36.363636
invoice.zip	4	36.363636

Count the number of email attachments that have the same unique combination of file name and size, using the search

Search string used:
index=botsv2 sourcetype="stream:smtp" attach_filename | stats count by attach_filename{},attach_size{}

How the search works:

- stats count by attach_filename{},attach_size{}: Counts the number of emails for each unique combination of attach_filename and attach_size.
- Purpose: Provides a breakdown of how many times each specific filename/size pair appears in the data.

Search string and result:

```
index=botsv2 sourcetype="stream:smtp" attach_filename | stats count by
attach_filename{},attach_size{}
```

during Aug 2017

✓ **11 events** (8/1/17 12:00:00.000 AM to 9/1/17 12:00:00.000 AM) No Event Sampling Job Verbose Mode

Events (11) Patterns **Statistics (11)** Visualization

100 Per Page Format Preview

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

3. Create a new field called "Attachment" that combines the attachment filename and size with a "/" in between, and count the unique values. Then count by Attachment.

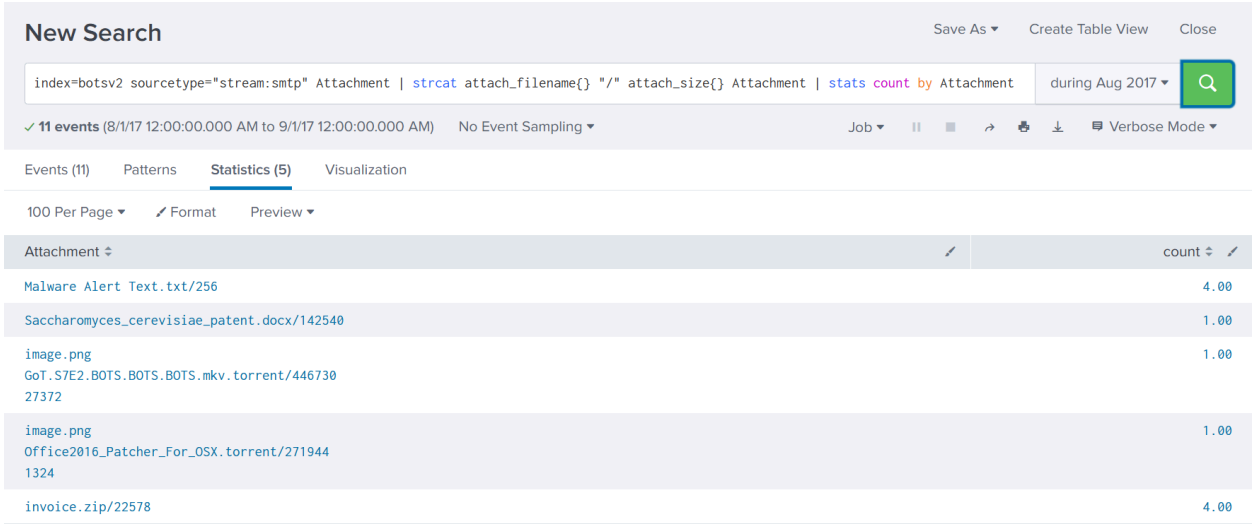
Search string used:

index=botsv2 sourcetype="stream:smtp" Attachment
| strcat attach_filename{} "/" attach_size{} Attachment
| stats count by Attachment

How the search works:

- index=botsv2 sourcetype="stream:smtp" Attachment: Searches in the botsv2 index for SMTP (email) events that include an "Attachment" field.
- strcat attach_filename{} "/" attach_size{} Attachment: Combines the attach_filename and attach_size fields with a / separator to create a new field called "Attachment" that shows the filename and size together.
- stats count by Attachment: Counts the occurrences of each unique "Attachment" combination (filename/size pair).

Search string and result:



4. Now count the number of unique recipients of each type of unique attachment. But remember, the same user could receive the same attachment in multiple emails. We don't want to count more than one of those events. Use the "dedup" command for that.

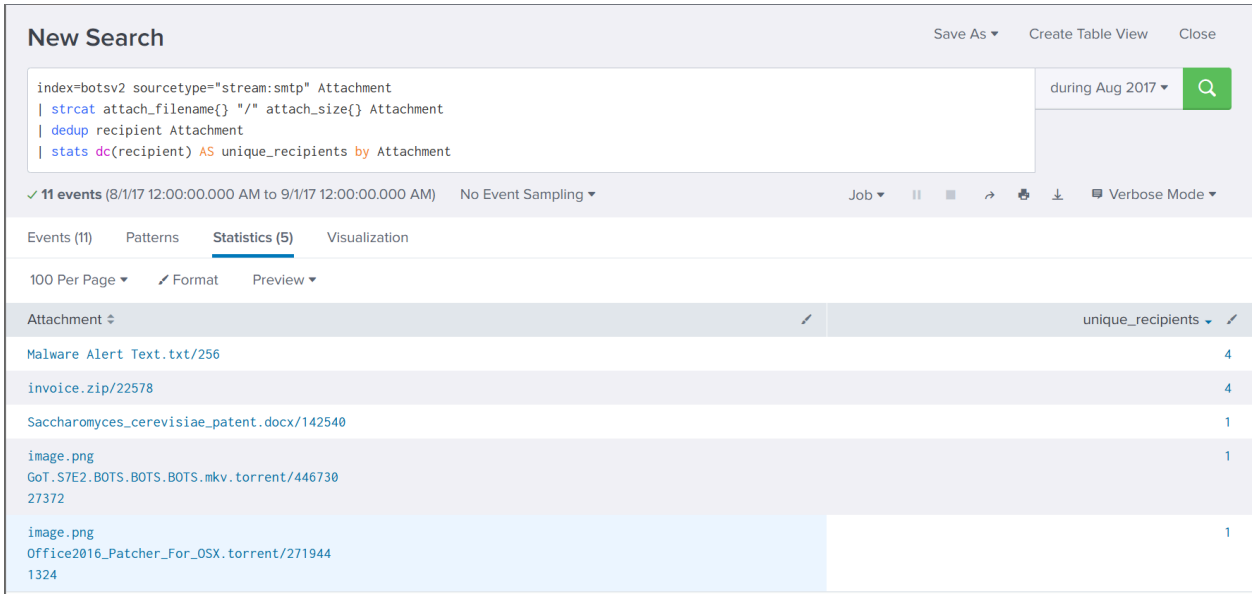
Search string used:

index=botsv2 sourcetype="stream:smtp" Attachment
| strcat attach_filename{} "/" attach_size{} Attachment
| dedup recipient Attachment
| stats dc(recipient) AS unique_recipients by Attachment

How the search works:

- **dedup recipient Attachment**: Removes duplicate events where the same recipient received the same attachment more than once, ensuring each recipient-attachment pair is unique.
- **stats dc(recipient) AS unique_recipients by Attachment**: Counts the distinct (dc) recipients for each unique attachment and labels the count as unique_recipients

Search string and result:



5. Convert the last search into a bar chart. Format the Y-Axis to have an interval of 1.

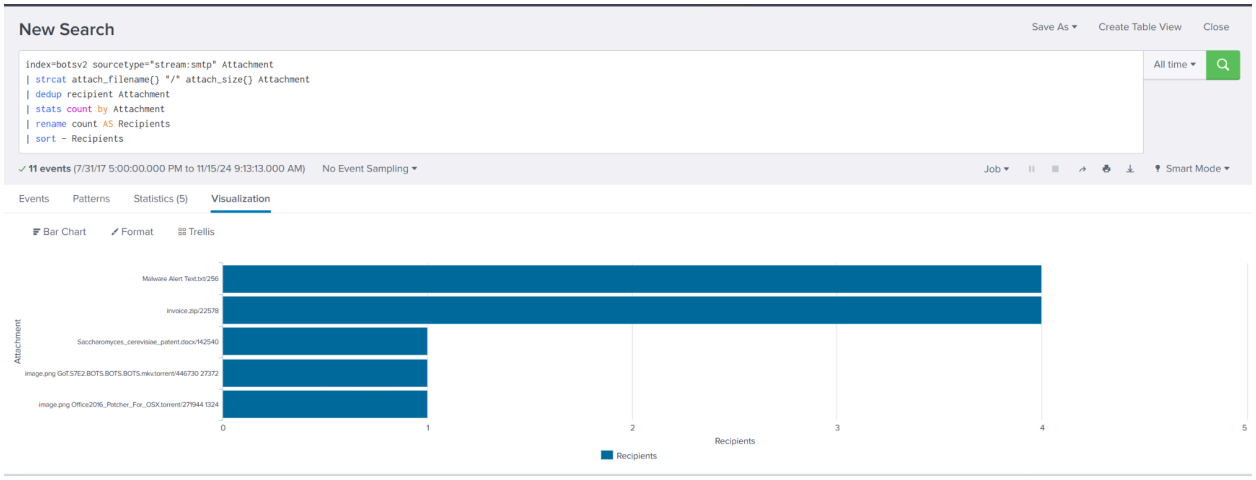
Search string used:

```
index=botsv2 sourcetype="stream:smtp" Attachment
| strcat attach_filename{} "/" attach_size{} Attachment
| dedup recipient Attachment
| stats count by Attachment
| rename count AS Recipients
| sort - Recipients
```

How the search works:

- **stats count by Attachment**: Counts the occurrences of each unique "Attachment" combination.
- **rename count AS Recipients**: Renames the count field to Recipients to make the label more descriptive.
- **sort - Recipients**: Sorts the results in descending order by the Recipients field, showing the attachments with the highest number of recipients first.

Search string and result:



6. The crafted display in the virtual console doesn't have the type of dashboard that we learned about before, so we have to go create one. Click on "Save As" and choose "New Dashboard". I've used the "Classic Dashboards", but you can try "Dashboard Studio" if you want to.

Save Panel to New Dashboard

Dashboard Title: CYBR 512 Assignment 4

cybr_512_assignment_4 Edit ID

Description: Optional

How do you want to build your dashboard? What's this?

Classic Dashboards
The traditional Splunk dashboard builder

Dashboard Studio NEW
A new builder to create visually-rich, customizable dashboards

Panel Title: Suspicious attachments

Visualization Type: Bar Chart | Statistics Table

Advanced Panel Settings

Panel Powered By: Inline Search

Drilldown: No action

Cancel | Save to Dashboard

CYBR512 Assignment 4

Suspicious attachments