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

Archived: 2026-04-05 23:43:21 UTC

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.

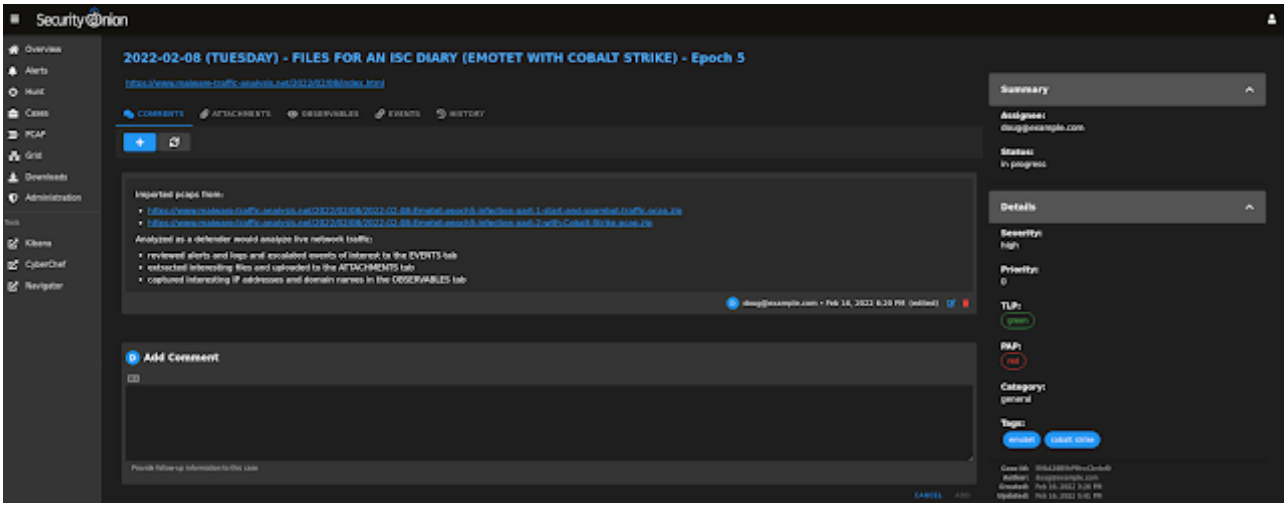
To learn more about Security Onion, please see:
https://securityonion.net
https://securityonion.net/docs

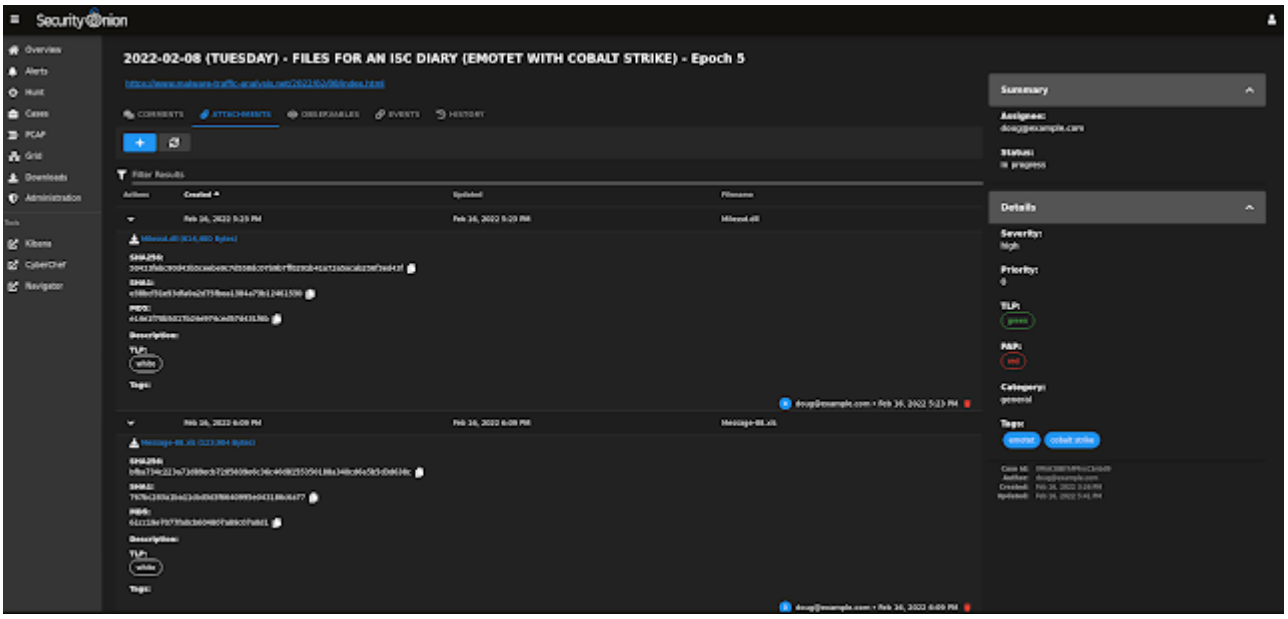
More Samples

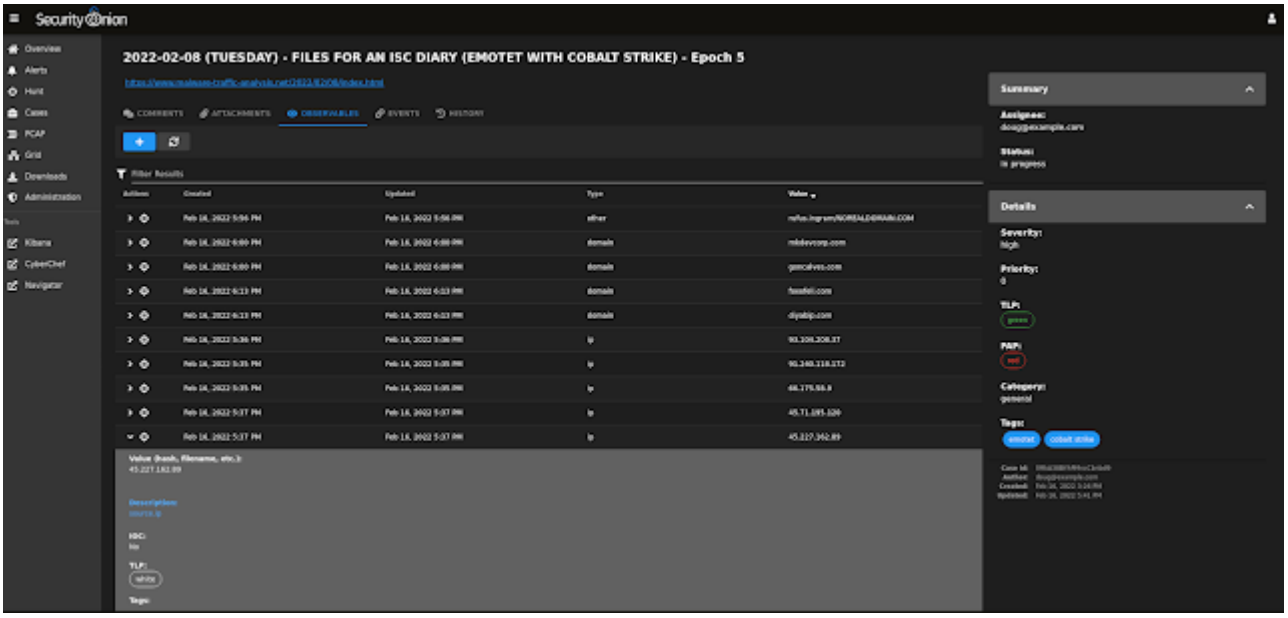
Find all of our Quick Malware posts at:
https://blog.securityonion.net/search/label/quick%20malware%20analysis

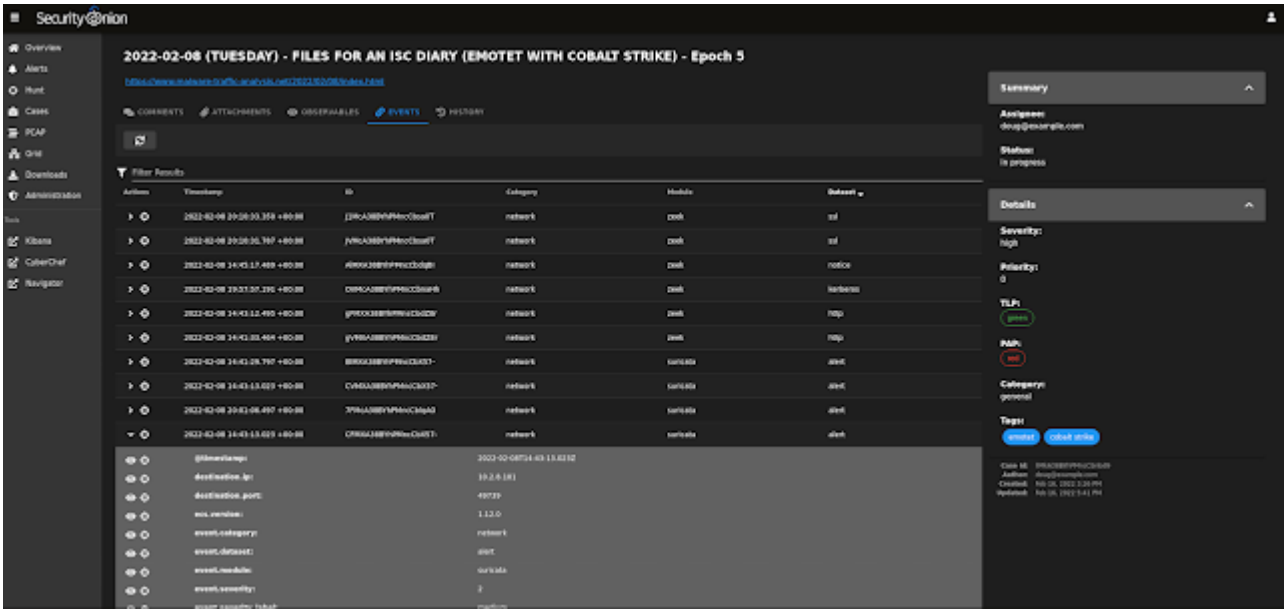
Screenshots

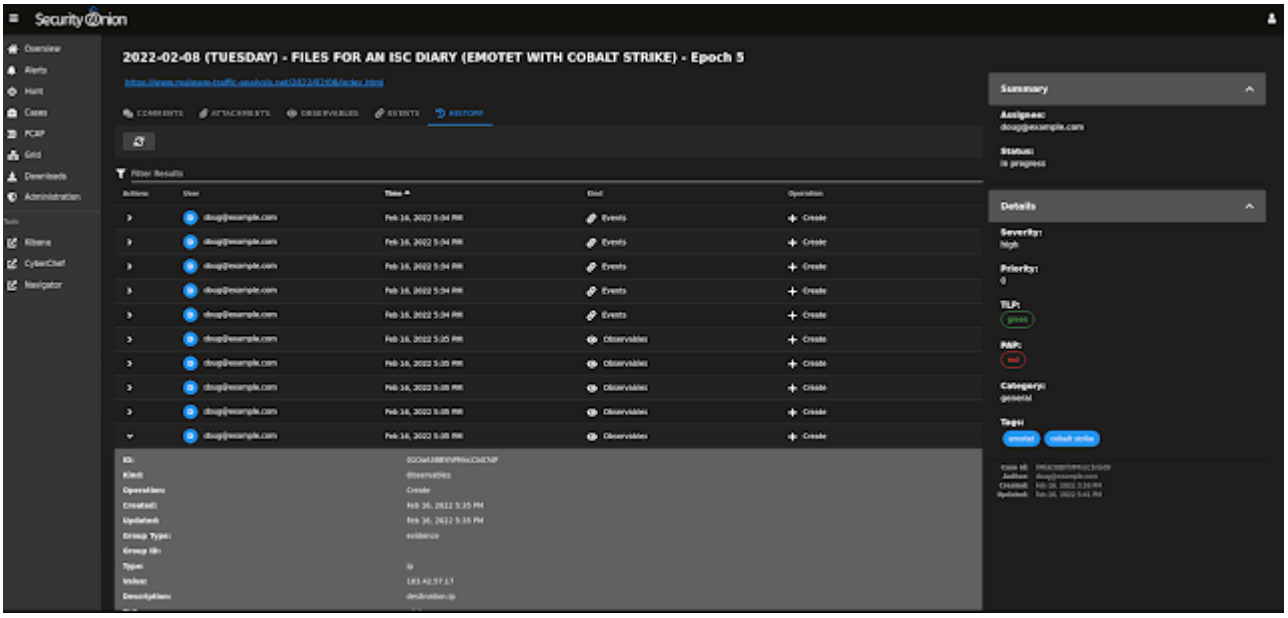
Click the first image to start the screenshot tour:

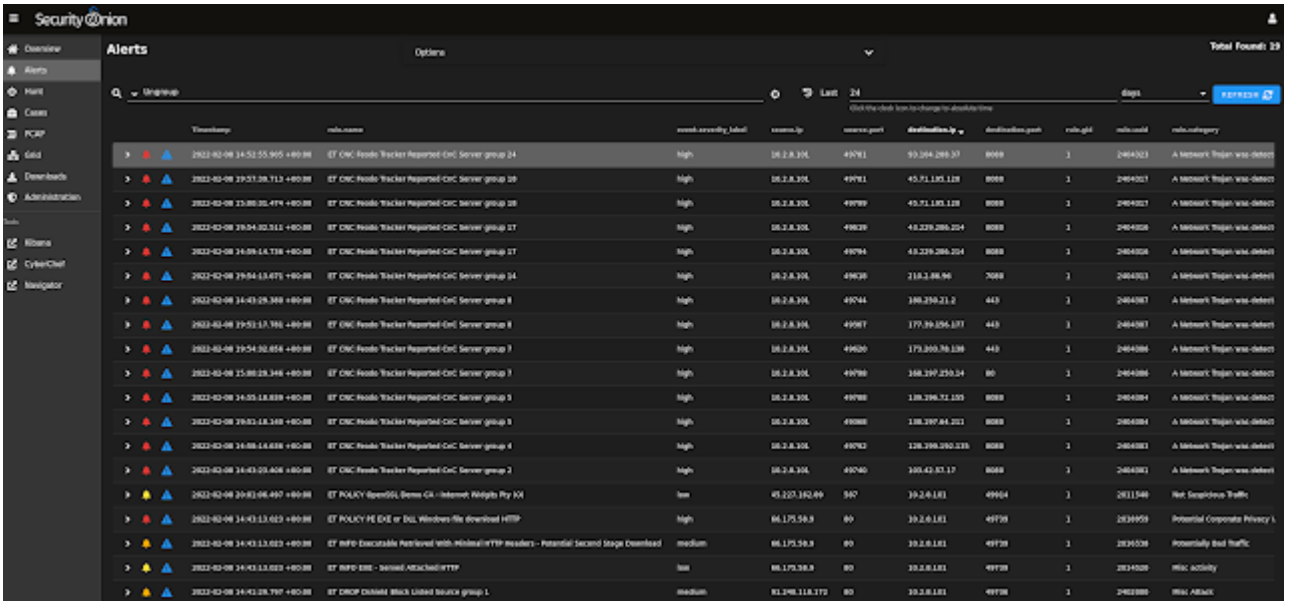

Security Onion
2022-02-08 (TUESDAY) - FILES FOR AN ISC DIARY (EMOTET WITH COBALT STRIKE) - Epoch 5
Summary
Details
Add Comment

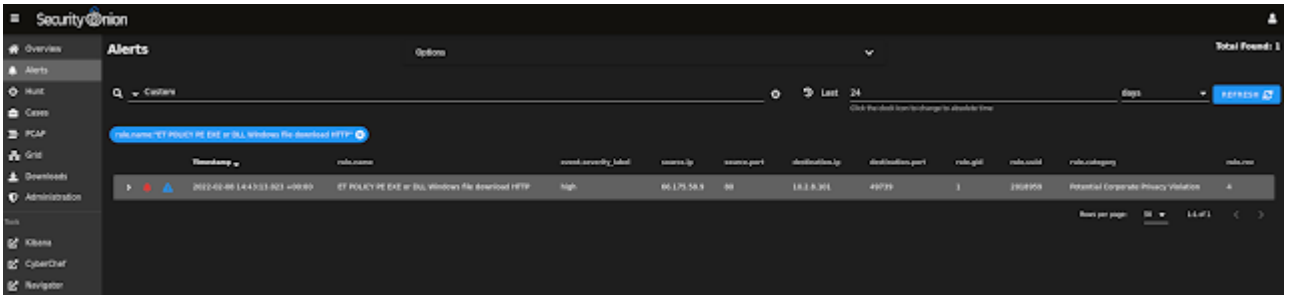

Security Onion
2022-02-08 (TUESDAY) - FILES FOR AN ISC DIARY (EMOTET WITH COBALT STRIKE) - Epoch 5
Summary
Details

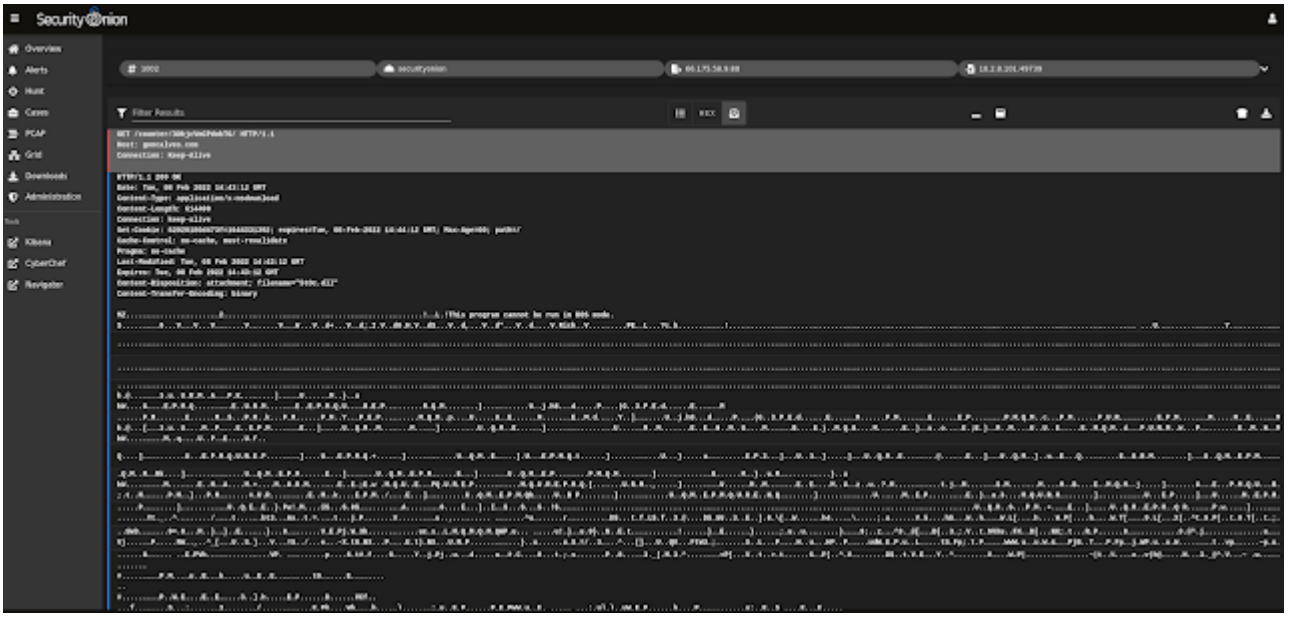

Security Onion
2022-02-08 (TUESDAY) - FILES FOR AN ISC DIARY (EMOTET WITH COBALT STRIKE) - Epoch 5
Summary
Details

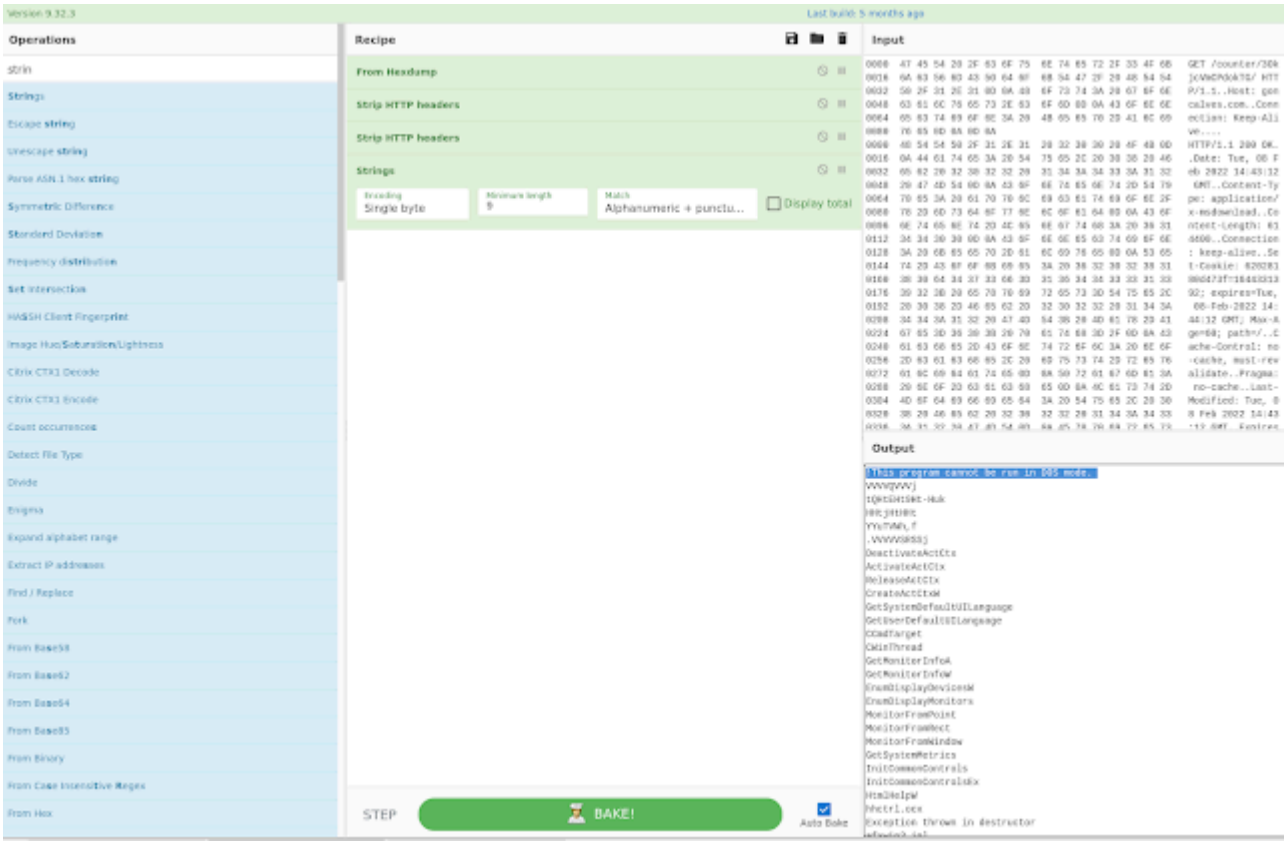

Security Onion
2022-02-08 (TUESDAY) - FILES FOR AN ISC DIARY (EMOTET WITH COBALT STRIKE) - Epoch 5
Summary
Details

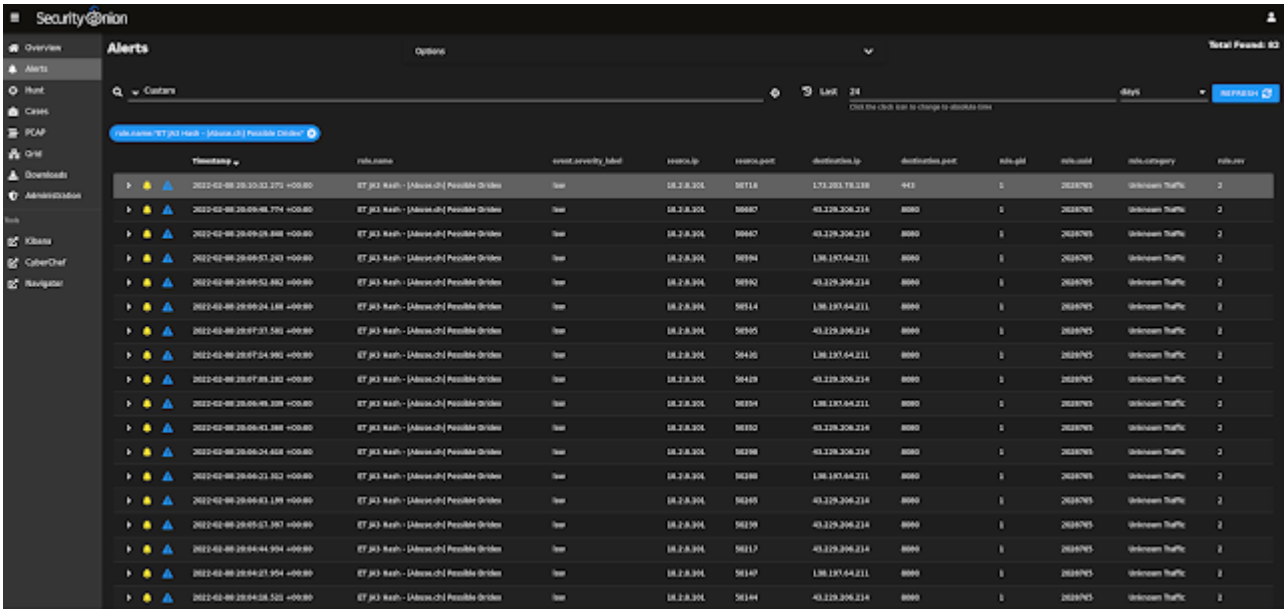

Security Onion
2022-02-08 (TUESDAY) - FILES FOR AN ISC DIARY (EMOTET WITH COBALT STRIKE) - Epoch 5
Summary
Details

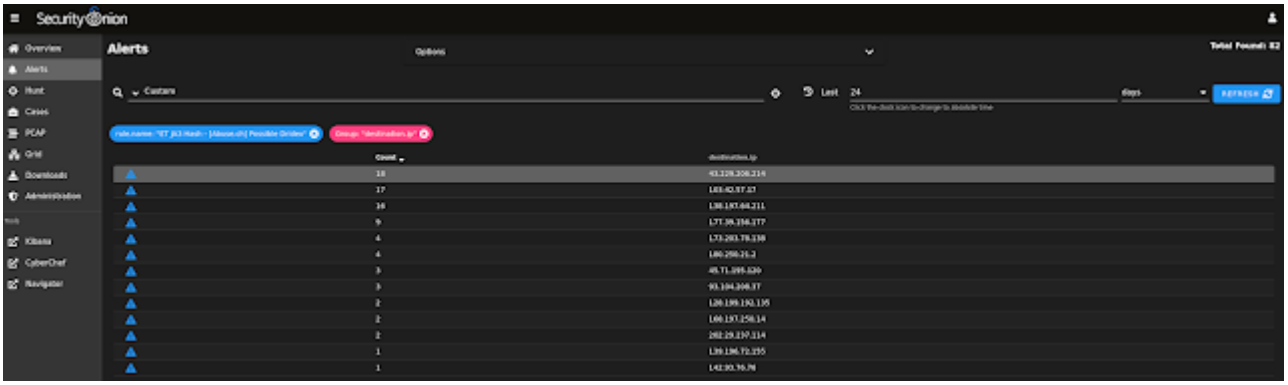

Security Onion
Alerts
Options
Total Found: 19
Overview
Alerts
Hunt
Cases
PCAP
Grid
Downloads
Administration
Kibana
CyberChef
Navigator

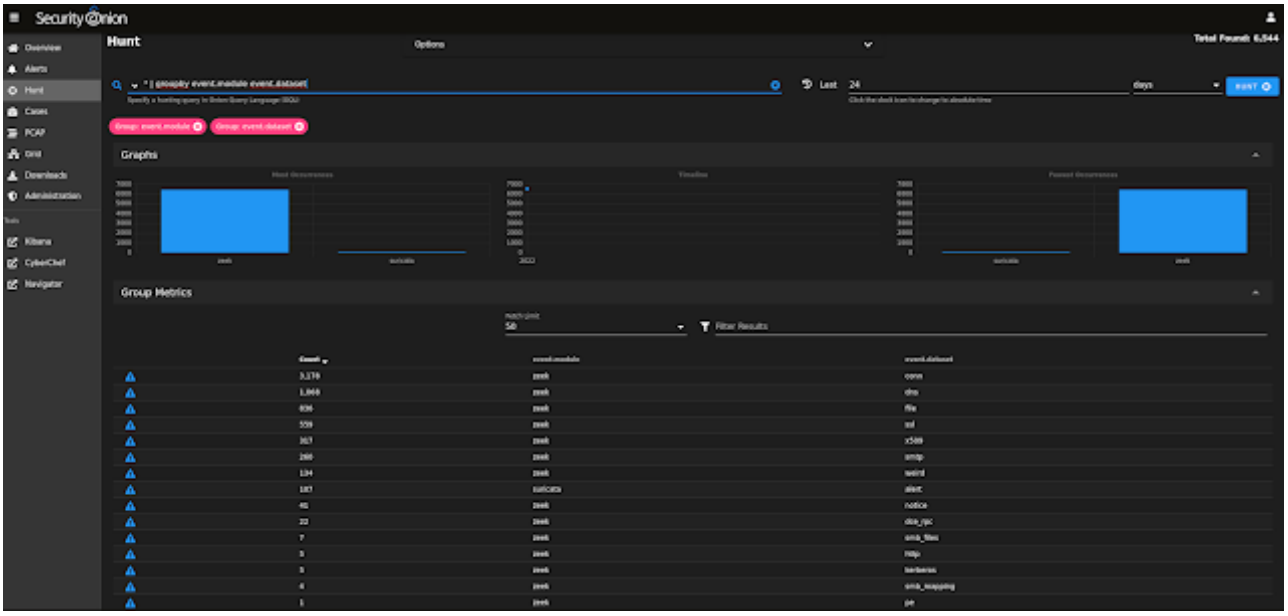

Security Onion
Alerts
Options
Total Found: 1
rule.name:"ET POLICY PE EXE or DLL Windows file download HTTP"
Overview
Alerts
Hunt
Cases
PCAP
Grid
Downloads
Administration
Kibana
CyberChef
Navigator

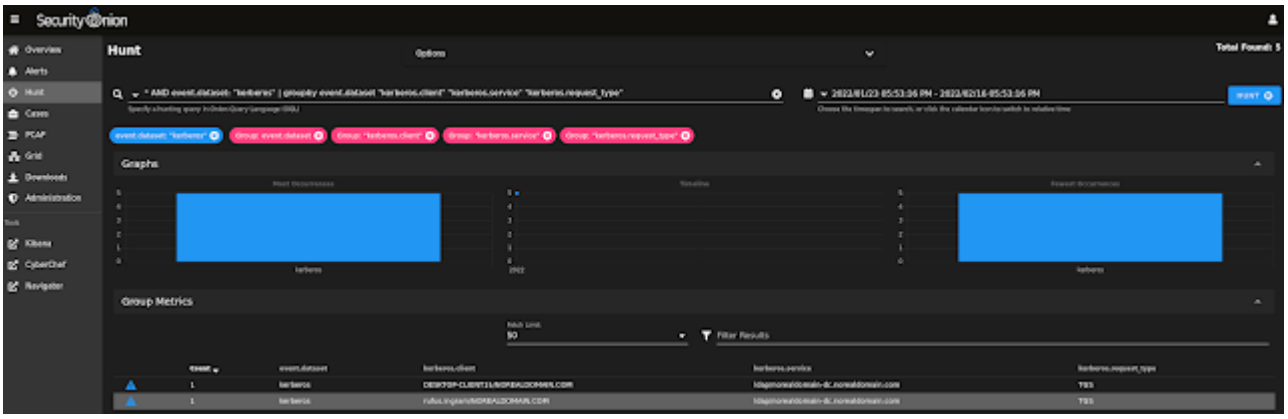

Security Onion
Overview
Alerts
Hunt
Cases
PCAP
Grid
Downloads
Administration
Kibana
CyberChef
Navigator

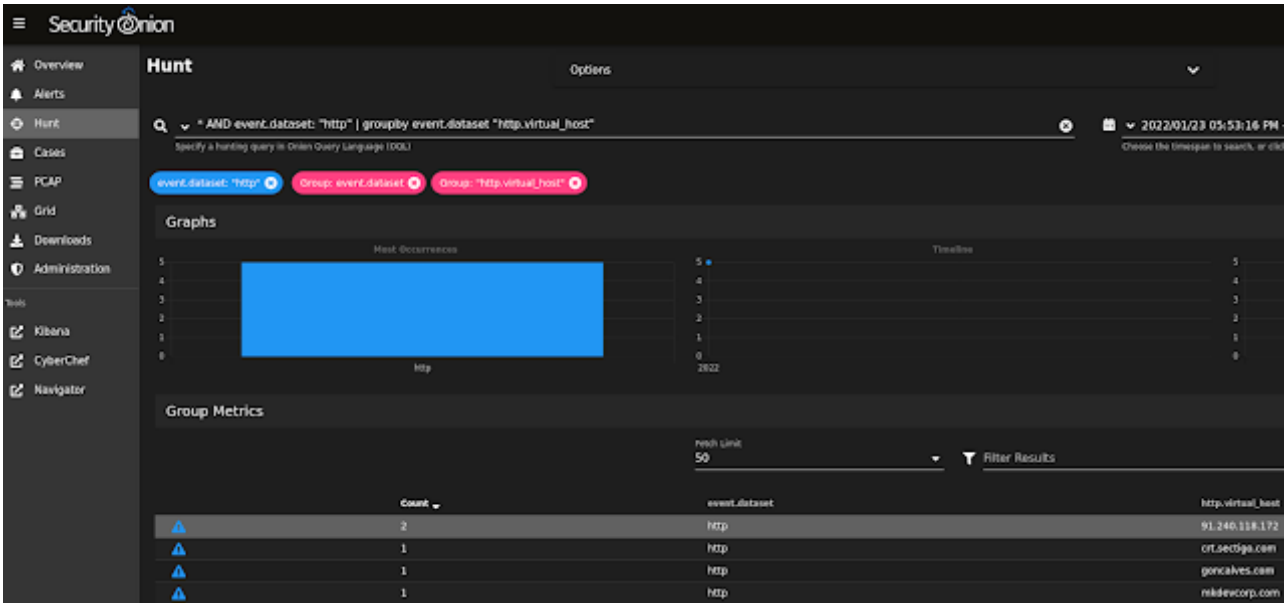

Operations
Recipe
Input
Output
From Hexdump
Strip HTTP headers
Strip HTTP headers
Strings
STEP
BAKE!
Auto Bake

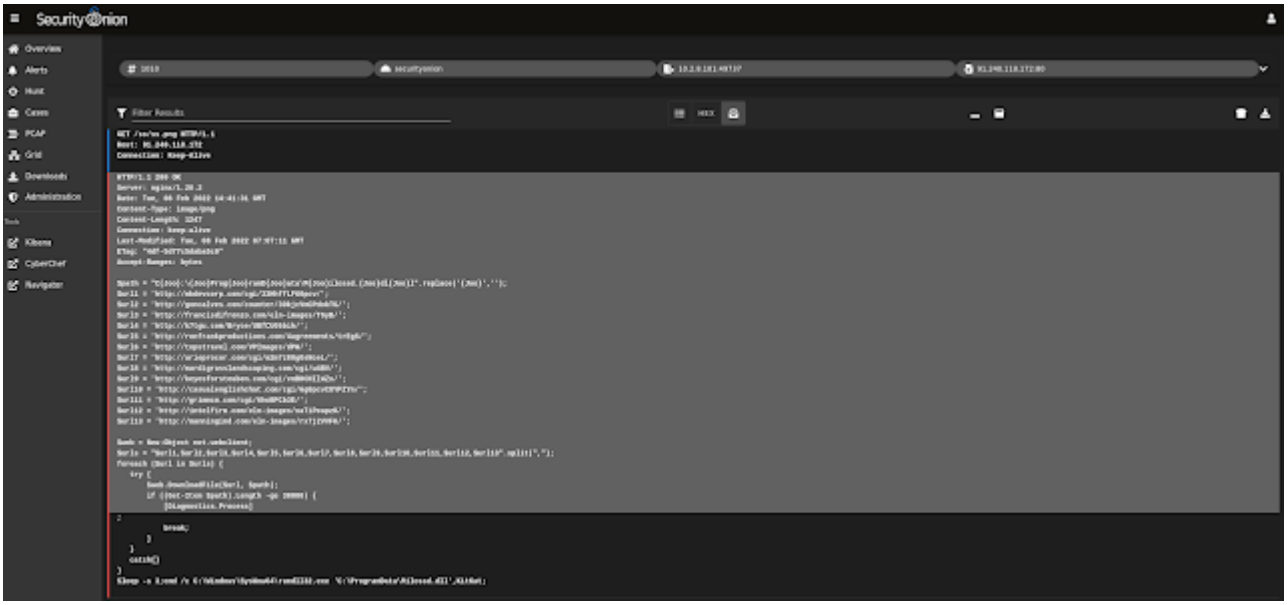

Security Onion
Alerts
Overview
Hunt
Cases
PCAP
Grid
Downloads
Kibana
CyberChef
Navigator
REFRESH

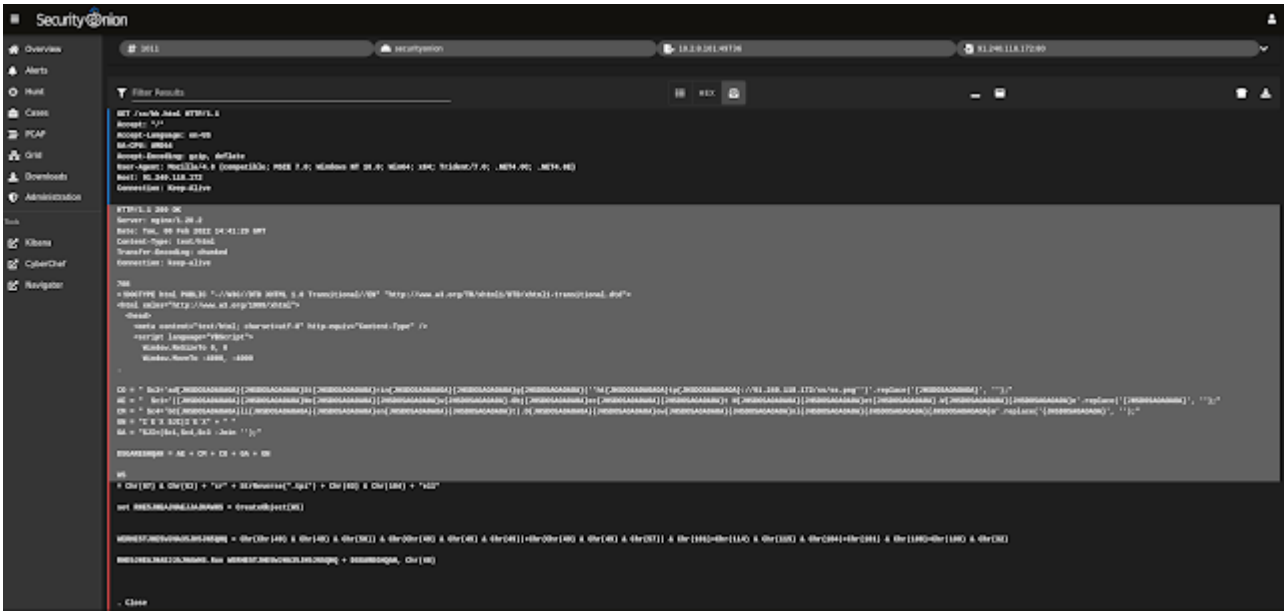

Security Onion
Alerts
Overview
Alerts
Hunt
Cases
PCAP
Grid
Downloads
Administration
Kibana
CyberChef
Navigator

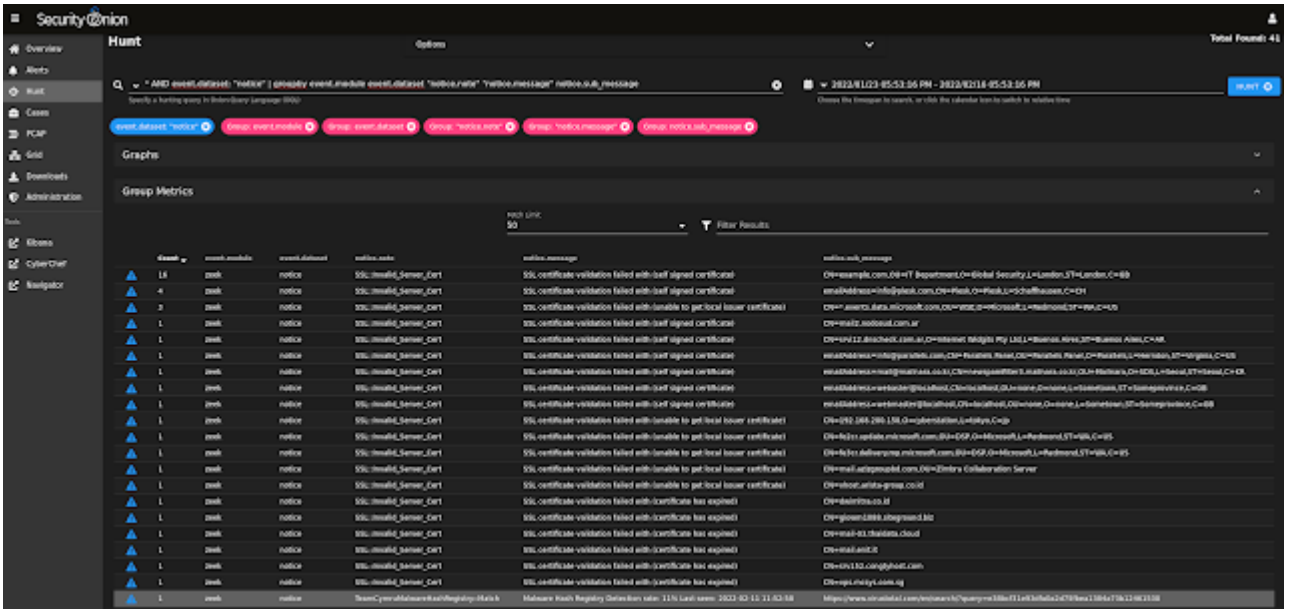

Security Onion
Hunt
Overview
Alerts
Hunt
Cases
PCAP
Grid
Downloads
Administration
Kibana
CyberChef
Navigator
Graphs
Group Metrics

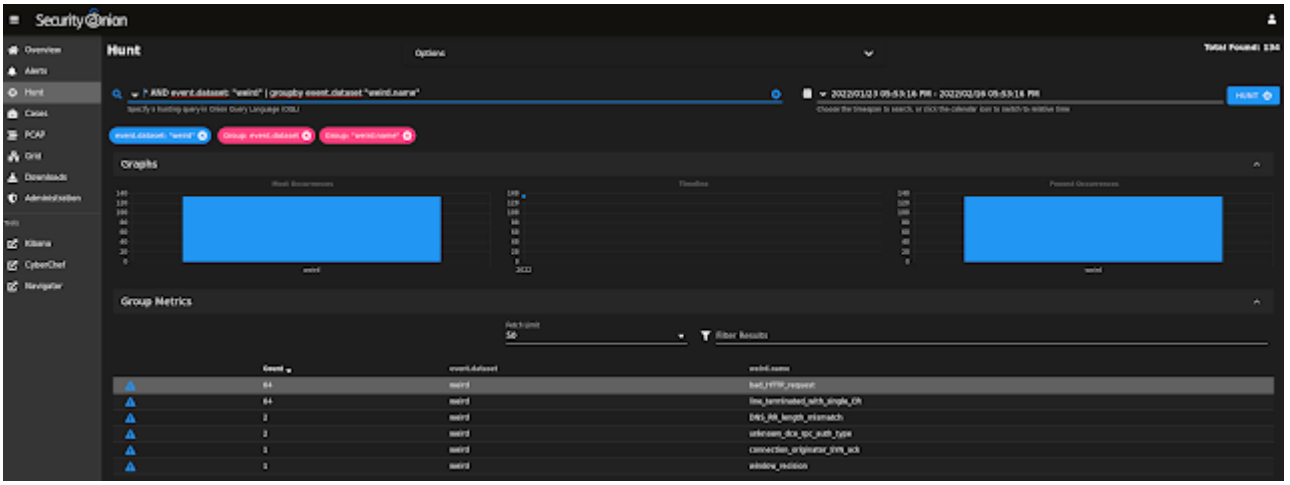

Security Onion
Hunt
Overview
Alerts
Hunt
Cases
PCAP
Grid
Downloads
Administration
Kibana
CyberChef
Navigator
Graphs
Group Metrics

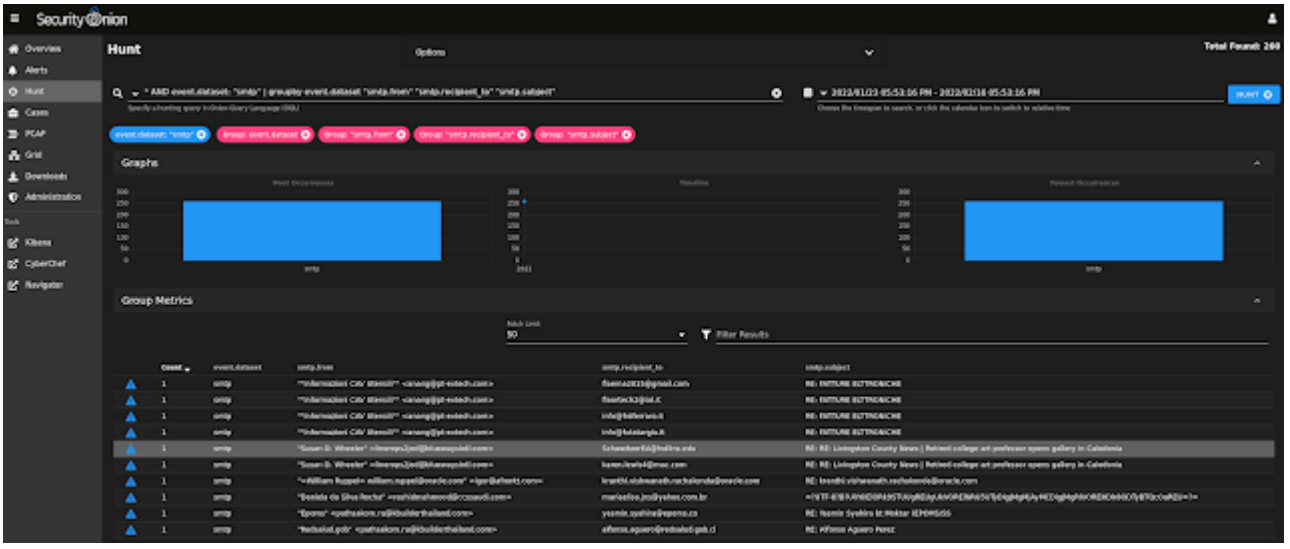

Security Onion
Overview
Alerts
Hunt
Cases
PCAP
Grid
Downloads
Administration
Kibana
CyberChef
Navigator
Hunt
Options
* AND event.dataset: "http" | groupby event.dataset "http.virtual_host"
2022/01/23 05:53:16 PM
event.dataset: "http"
Group: event.dataset
Group: "http.virtual_host"
Graphs
Host Occurrences
Timeline
http
2022
Group Metrics
Filter Results
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

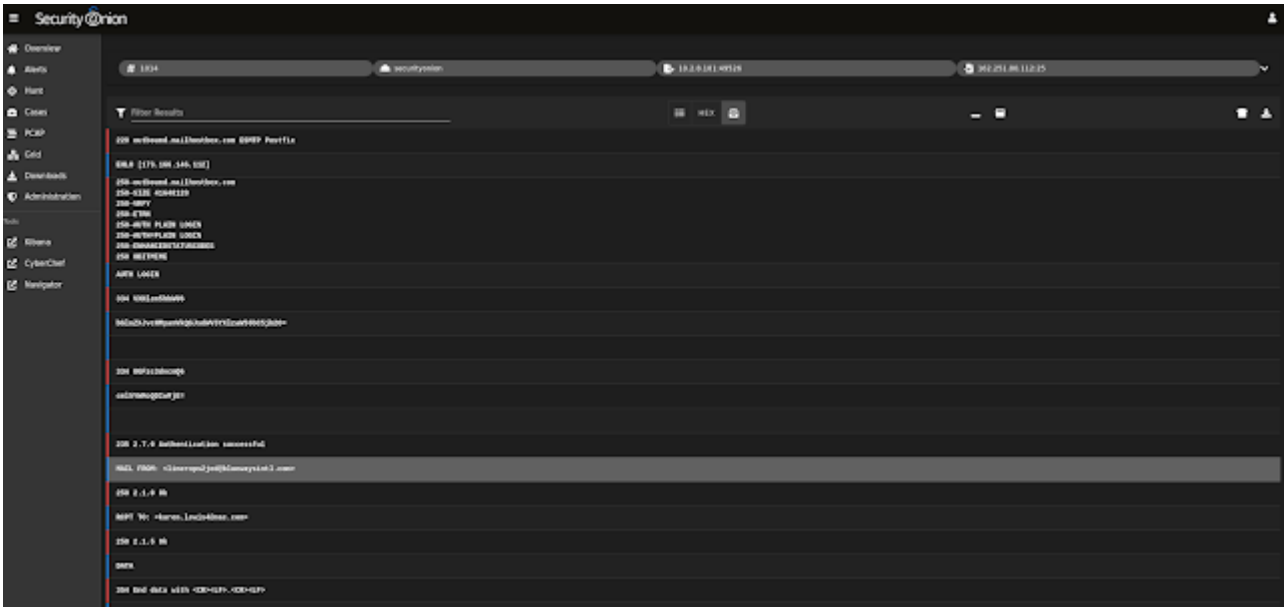

Security Onion
Filter Results

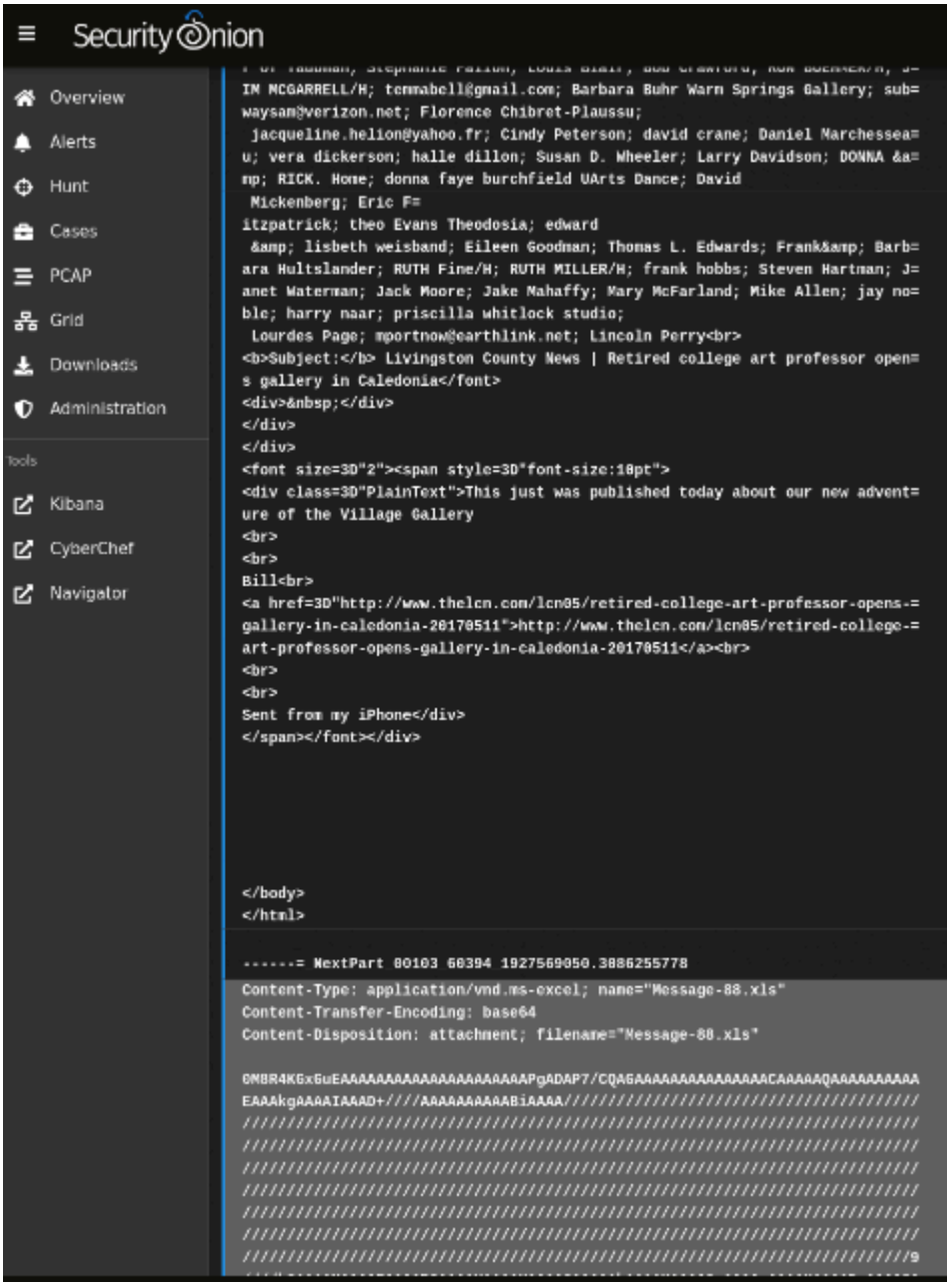

Security Onion
Filter Results


Security Onion
Hunt
Graphs
Group Metrics


Security Onion
Hunt
Graphs
Group Metrics


Security Onion
Hunt
Graphs
Group Metrics


Security Onion
Overview
Alerts
Hunt
Cases
PCAP
Grid
Downloads
Administration
Kibana
CyberChef
Navigator
Filter Results
HEX

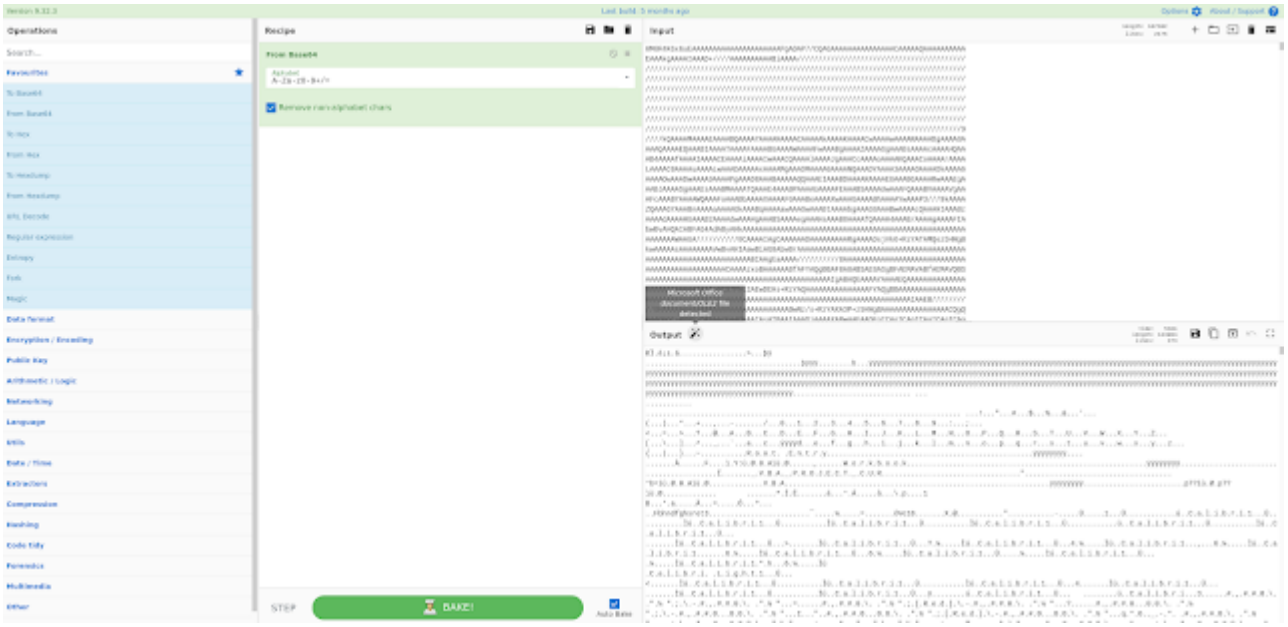

Security Onion
Overview
Alerts
Hunt
Cases
PCAP
Grid
Downloads
Administration
Tools
Kibana
CyberChef
Navigator
IM MCGARRELL/H; tenmabell@gmail.com; Barbara Buhr Warn Springs Gallery; sub=
waysam@verizon.net; Florence Chibret-Plaussu;
jacqueline.helion@yahoo.fr; Cindy Peterson; david crane; Daniel Marchessea=
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
& lisbeth weisband; Eileen Goodman; Thomas L. Edwards; Frank& 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=
blc; harry naar; priscilla whitlock studio;
Lourdes Page; mportnow@earthlink.net; Lincoln Perry
Subject: Livingston County News | Retired college art professor open=
s gallery in Caledonia

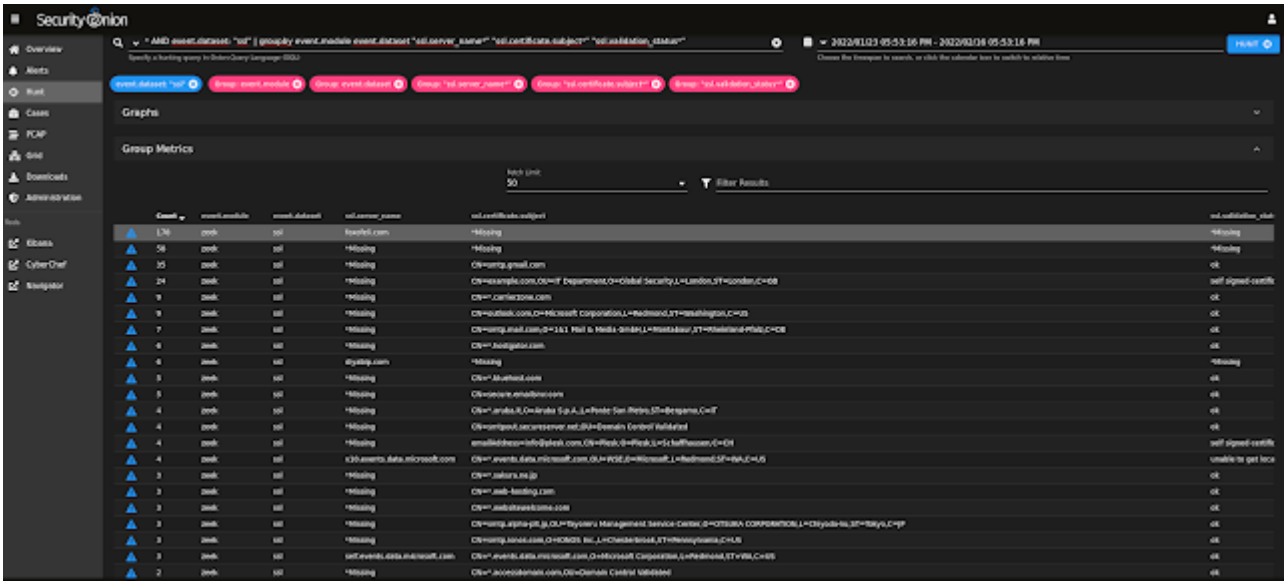
<span style=3D"font-size:10pt">
<div class=3D"PlainText">This just was published today about our new advent=
ure of the Village Gallery

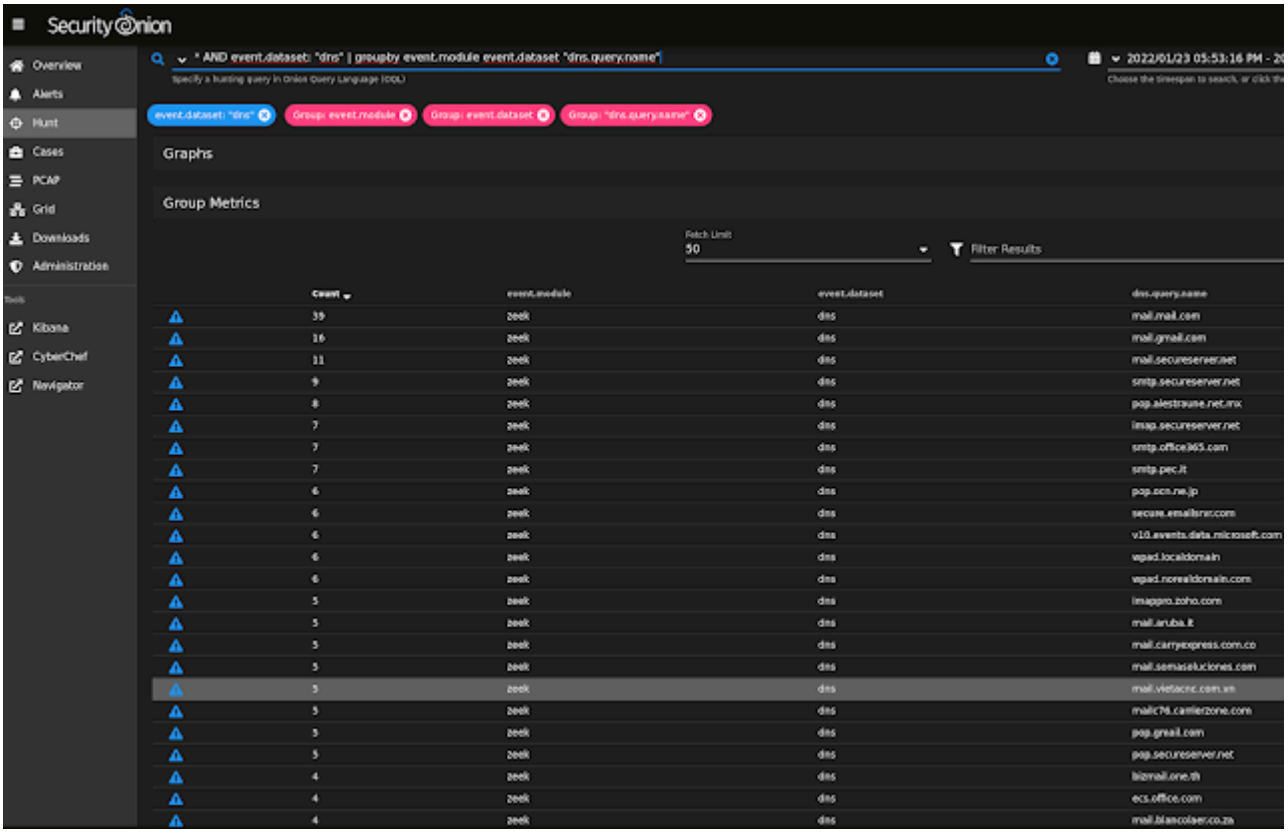
Bill
<a href=3D"http://www.thelcn.com/lcn05/retired-college-art-professor-opens-=
gallery-in-caledonia-20170511">http://www.thelcn.com/lcn05/retired-college-=
art-professor-opens-gallery-in-caledonia-20170511

Sent from my iPhone

</body>
</html>
------= NextPart 80103 60394 1927569050.3886255778
Content-Type: application/vnd.ms-excel; name="Message-88.xls"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="Message-88.xls"
0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAAAAAAAACAAAAAQAAAAAAAAAA
EAAAkgAAAAIAAAD+////AAAAAAAAAABiAAAA/////////////////////////////////////
//
//
//
//
//
//
//9


Operations
Recipe
From Base64
Input
Output
STEP
BAKE!


Security Onion
Overview
Alerts
Hunt
Cases
PCAP
Grid
Downloads
Administration
Kibana
CyberChef
Navigator
Graphs
Group Metrics



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