

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:

SecurityOnion

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>

COMMENTS ATTACHMENTS OBSERVABLES EVENTS HISTORY

Imported pcap file:

- https://www.malware-traffic-analysis.net/2022/02/08/epoch-00003_infection_smb_1_capt_and_overbat.tlfs_vnc4_28
- https://www.malware-traffic-analysis.net/2022/02/08/epoch-00003_infection_smb_2_vnc5_Cobalt_Strip4_smb_06

Analyzed as a defender would analyze live network traffic:

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

Severity: High
Priority: 0
TLP: Green
MFP: Red
Category: general
Tags: [create](#) [edit tags](#)

Case ID: 886288979cc3e640
Author: dsuggs@sample.com
Created: Feb 14, 2022 8:28 PM
Updated: Feb 14, 2022 8:28 PM

SecurityOnion

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>

COMMENTS ATTACHMENTS OBSERVABLES EVENTS HISTORY

Filter Results

Action	Created	Updated	Filename
Message-88-48-5223-861 (system)	Feb 14, 2022 8:23 PM	Feb 14, 2022 8:28 PM	Message-88...
Message-88-48-5223-861 (system)	Feb 14, 2022 8:23 PM	Feb 14, 2022 8:28 PM	Message-88...

Severity: High
Priority: 0
TLP: Green
MFP: Red
Category: general
Tags: [create](#) [edit tags](#)

Case ID: 886288979cc3e640
Author: dsuggs@sample.com
Created: Feb 14, 2022 8:28 PM
Updated: Feb 14, 2022 8:28 PM

SecurityOnion

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>

COMMENTS ATTACHMENTS OBSERVABLES EVENTS HISTORY

Filter Results

Action	Created	Updated	Type	Value
Message-88-48-5223-861 (system)	Feb 14, 2022 8:23 PM	Feb 14, 2022 8:28 PM	other	reflex.program.WORLDWIDEORAMA.COM
Message-88-48-5223-861 (system)	Feb 14, 2022 8:23 PM	Feb 14, 2022 8:28 PM	domain	mldevcorp.com
Message-88-48-5223-861 (system)	Feb 14, 2022 8:23 PM	Feb 14, 2022 8:28 PM	domain	gmscalvus.com
Message-88-48-5223-861 (system)	Feb 14, 2022 8:23 PM	Feb 14, 2022 8:23 PM	domain	hustlell.com
Message-88-48-5223-861 (system)	Feb 14, 2022 8:23 PM	Feb 14, 2022 8:23 PM	domain	diyallip.com
Message-88-48-5223-861 (system)	Feb 14, 2022 8:28 PM	Feb 14, 2022 8:28 PM	ip	93.208.208.37
Message-88-48-5223-861 (system)	Feb 14, 2022 8:28 PM	Feb 14, 2022 8:28 PM	ip	93.208.208.37
Message-88-48-5223-861 (system)	Feb 14, 2022 8:28 PM	Feb 14, 2022 8:28 PM	ip	44.175.86.9
Message-88-48-5223-861 (system)	Feb 14, 2022 8:27 PM	Feb 14, 2022 8:27 PM	ip	45.71.885.120
Message-88-48-5223-861 (system)	Feb 14, 2022 8:27 PM	Feb 14, 2022 8:27 PM	ip	45.127.342.89

Value Search, Filename, etc.:

```
45.127.342.89
```

Severity: High
Priority: 0
TLP: Green
MFP: Red
Category: general
Tags: [create](#) [edit tags](#)

Case ID: 886288979cc3e640
Author: dsuggs@sample.com
Created: Feb 14, 2022 8:28 PM
Updated: Feb 14, 2022 8:28 PM

The screenshot shows the SecurityOnion interface with the 'EVENTS' tab selected. The main content area displays a table of network events. The table has columns for Action, Timestamp, ID, Category, Module, and Detail. The events listed are:

Action	Timestamp	ID	Category	Module	Detail
>	2022-02-08 20:26:50.359 +00:00	JIRKASBBYFMC0001T	network	cmk	rd
>	2022-02-08 20:26:50.767 +00:00	JVRLASBBYFMC0001T	network	cmk	rd
>	2022-02-08 20:43:17.489 +00:00	WRKASBBYFMC0001G	network	cmk	notice
>	2022-02-08 20:57:37.235 +00:00	OBKASBBYFMC0001G	network	cmk	barbosa
>	2022-02-08 20:43:12.490 +00:00	JFKASBBYFMC0001G	network	cmk	rip
>	2022-02-08 20:43:03.404 +00:00	JVRLASBBYFMC0001G	network	cmk	rip
>	2022-02-08 20:43:28.797 +00:00	BRKASBBYFMC0001G	network	cmk	ahit
>	2022-02-08 20:43:13.023 +00:00	CVKASBBYFMC0001G	network	cmk	ahit
>	2022-02-08 20:43:08.497 +00:00	JFKASBBYFMC0001G	network	cmk	ahit
>	2022-02-08 20:43:13.023 +00:00	ORNASBBYFMC0001G	network	cmk	ahit

Below the table, there is a metadata section with key-value pairs:

- @timestamp: 2022-02-08T16:43:13.023Z
- @version: 10.2.6.181
- @type: _type
- @version: 1.12.0
- event.category: network
- event.module: cmk
- event.type: ahit
- event.severity: 3

The right sidebar contains a 'Summary' section with the following information:

- Assignee: doug@example.com
- Status: In progress
- Severity: High
- Priority: 0
- TLP: Green
- MAP: Red
- Category: network
- Tags: cmk, cmk-ahit
- Case ID: JIRKASBBYFMC0001G
- Author: doug@example.com
- Created: Feb 08, 2022 5:28 PM
- Updated: Feb 08, 2022 5:44 PM

The screenshot shows the SecurityOnion interface with the 'SYSTEM' tab selected. The main content area displays a table of system events. The table has columns for Action, User, Time, and Detail. The events listed are:

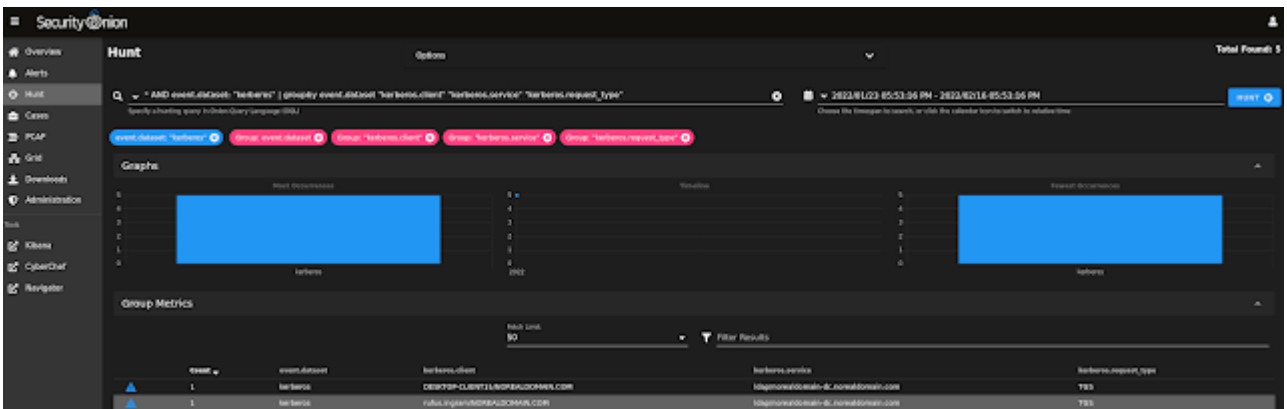
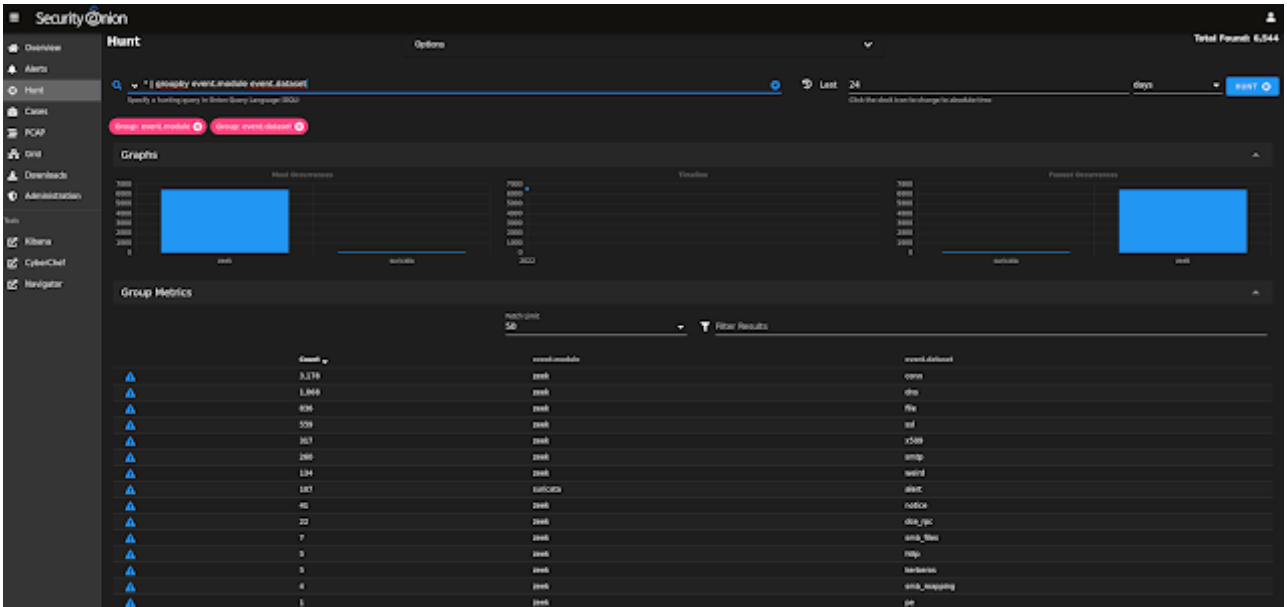
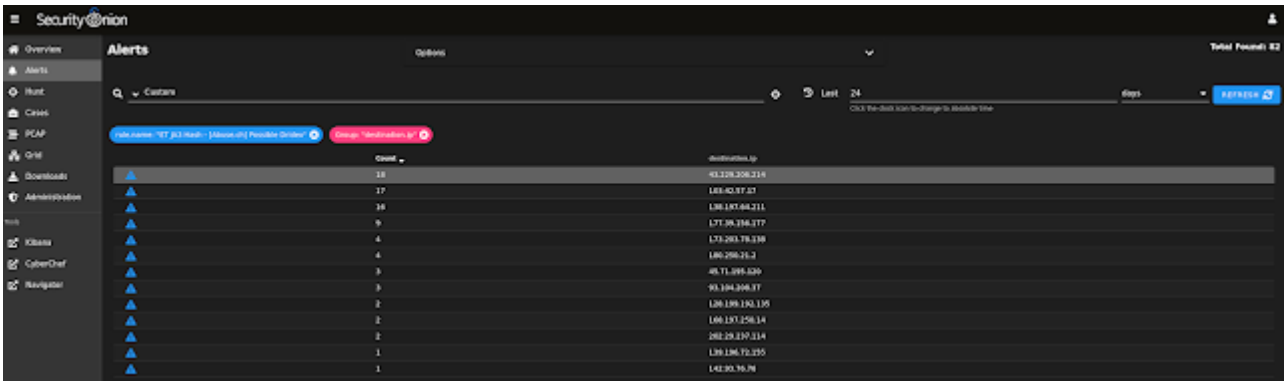
Action	User	Time	Detail
>	doug@example.com	Feb 16, 2022 5:04 PM	Events + Create
>	doug@example.com	Feb 16, 2022 5:04 PM	Events + Create
>	doug@example.com	Feb 16, 2022 5:04 PM	Events + Create
>	doug@example.com	Feb 16, 2022 5:04 PM	Events + Create
>	doug@example.com	Feb 16, 2022 5:04 PM	Events + Create
>	doug@example.com	Feb 16, 2022 5:05 PM	Observables + Create
>	doug@example.com	Feb 16, 2022 5:05 PM	Observables + Create
>	doug@example.com	Feb 16, 2022 5:05 PM	Observables + Create
>	doug@example.com	Feb 16, 2022 5:05 PM	Observables + Create
>	doug@example.com	Feb 16, 2022 5:05 PM	Observables + Create
>	doug@example.com	Feb 16, 2022 5:05 PM	Observables + Create

Below the table, there is a metadata section with key-value pairs:

- ID: JIRKASBBYFMC0001G
- Kind: Observables
- Operation: Create
- Created: Feb 16, 2022 5:25 PM
- Updated: Feb 16, 2022 5:35 PM
- Group Type: evidence
- Group ID: 0
- Type: 0
- Value: 183-42.17.1.1
- Description: dmz-vlan-10

The right sidebar contains a 'Summary' section with the following information:

- Assignee: doug@example.com
- Status: In progress
- Severity: High
- Priority: 0
- TLP: Green
- MAP: Red
- Category: network
- Tags: cmk, cmk-ahit
- Case ID: JIRKASBBYFMC0001G
- Author: doug@example.com
- Created: Feb 08, 2022 5:28 PM
- Updated: Feb 08, 2022 5:44 PM



The screenshot shows the Security Onion interface. At the top, there is a search bar with the query: `* AND event.database: "dfs" | groupby event.module event.dataset "dfs.query.name"`. Below the search bar, there are several filters: `event.dataset: "dfs"`, `Group: event.module`, `Group: event.dataset`, and `Group: "dfs.query.name"`. The main content area is titled "Group Metrics" and displays a table with columns: `Count`, `event.module`, `event.dataset`, and `dfs.query.name`. The table lists various domains and their corresponding counts. The first row is highlighted.

Count	event.module	event.dataset	dfs.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.alestrane.net.mx
7	zeek	dns	imap.secureserver.net
7	zeek	dns	smtp.office365.com
7	zeek	dns	smtp.pec.it
6	zeek	dns	pop.ecn.ne.jp
6	zeek	dns	secas.emalltrn.com
6	zeek	dns	vi0.events.data.microsoft.com
6	zeek	dns	vgad.localdomain
6	zeek	dns	vgad.noreldomain.com
5	zeek	dns	imaggio.zoho.com
5	zeek	dns	mail.aruba.it
5	zeek	dns	mail.carryexpress.com.co
5	zeek	dns	mail.semaseoluciones.com
5	zeek	dns	mail.vietacn.com.vn
5	zeek	dns	mail78.camlerzone.com
5	zeek	dns	pop.gmail.com
5	zeek	dns	pop.secureserver.net
4	zeek	dns	lizmail.one.th
4	zeek	dns	ecs.office.com
4	zeek	dns	mail.blancolae.co.za

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