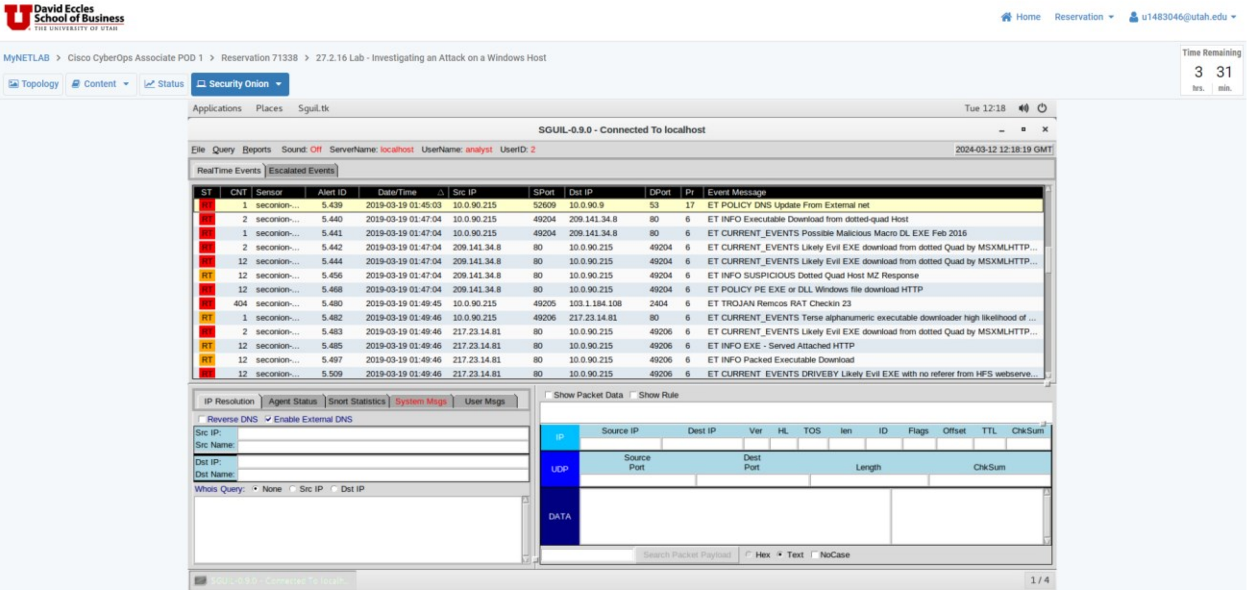
Vu Nguyen

UID: u1483046

Assignment 30 - Investigating an Attack on a Windows Host (Lab, Q&A and Quiz)

1. Part 1, Step 1c



Sound: Off ServerName: localhost UserName: analyst UserID: 2

2024-03-12 12:18:19 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	seconion-...	5.439	2019-03-19 01:45:03	10.0.90.215	52609	10.0.90.9	53	17	ET POLICY DNS Update From External net
RT	2	seconion-...	5.440	2019-03-19 01:47:04	10.0.90.215	49204	209.141.34.8	80	6	ET INFO Executable Download from dotted-quad Host
RT	1	seconion-...	5.441	2019-03-19 01:47:04	10.0.90.215	49204	209.141.34.8	80	6	ET CURRENT_EVENTS Possible Malicious Macro DL EXE Feb 2016
RT	2	seconion-...	5.442	2019-03-19 01:47:04	209.141.34.8	80	10.0.90.215	49204	6	ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP...
RT	12	seconion-...	5.444	2019-03-19 01:47:04	209.141.34.8	80	10.0.90.215	49204	6	ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP...
RT	12	seconion-...	5.456	2019-03-19 01:47:04	209.141.34.8	80	10.0.90.215	49204	6	ET INFO SUSPICIOUS Dotted Quad Host MZ Response
RT	12	seconion-...	5.468	2019-03-19 01:47:04	209.141.34.8	80	10.0.90.215	49204	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	404	seconion-...	5.480	2019-03-19 01:49:45	10.0.90.215	49205	103.1.184.108	2404	6	ET TROJAN Remcos RAT Checkin 23
RT	1	seconion-...	5.482	2019-03-19 01:49:46	10.0.90.215	49206	217.23.14.81	80	6	ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of ...
RT	2	seconion-...	5.483	2019-03-19 01:49:46	217.23.14.81	80	10.0.90.215	49206	6	ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP...
RT	12	seconion-...	5.485	2019-03-19 01:49:46	217.23.14.81	80	10.0.90.215	49206	6	ET INFO EXE - Served Attached HTTP
RT	12	seconion-...	5.497	2019-03-19 01:49:46	217.23.14.81	80	10.0.90.215	49206	6	ET INFO Packed Executable Download
RT	12	seconion-...	5.509	2019-03-19 01:49:46	217.23.14.81	80	10.0.90.215	49206	6	ET CURRENT_EVENTS DRIVEBY Likely Evil EXE with no referer from HFS webserve...

□ Reverse DNS ☑ Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:

Whois Query: ● None ○ Src IP ○ Dst IP

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum

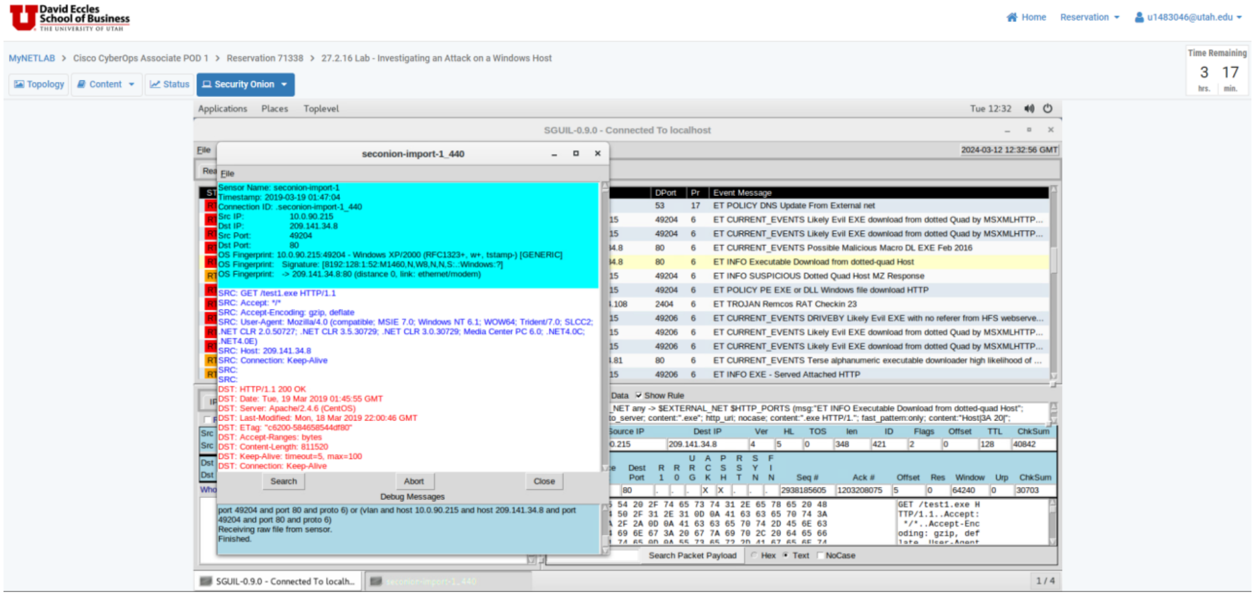
UDP	Source Port	Dest Port	Length	ChkSum

DATA

SGUIL-0.9.0 - Connected To localh...

1 / 4

2. Part 1, Step 2b



```
Sensor Name: seconion-import-1
Timestamp: 2019-03-19 01:47:04
Connection ID: .seconion-import-1_440
Src IP:          10.0.90.215
Dst IP:          209.141.34.8
Src Port:        49204
Dst Port:        80
OS Fingerprint: 10.0.90.215:49204 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint:   Signature: [8192:128:1:52:M1460,N,W8,N,N,S::Windows:?]
OS Fingerprint:   -> 209.141.34.8:80 (distance 0, link: ethernet/modem)

SRC: GET /test1.exe HTTP/1.1
SRC: Accept: */*
SRC: Accept-Encoding: gzip, deflate
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2;
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C;
.NET4.0E)
SRC: Host: 209.141.34.8
SRC: Connection: Keep-Alive
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Tue, 19 Mar 2019 01:45:55 GMT
DST: Server: Apache/2.4.6 (CentOS)
DST: Last-Modified: Mon, 18 Mar 2019 22:00:46 GMT
DST: ETag: "c6200-584658544df80"
DST: Accept-Ranges: bytes
DST: Content-Length: 811520
DST: Keep-Alive: timeout=5, max=100
DST: Connection: Keep-Alive
```

```
port 49204 and port 80 and proto 6) or (vlan and host 10.0.90.215 and host 209.141.34.8 and port
49204 and port 80 and proto 6)
Receiving raw file from sensor.
Finished.
```

	DPort	Pr	Event Message
	53	17	ET POLICY DNS Update From External net
15	49204	6	ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP...
15	49204	6	ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP...
4.8	80	6	ET CURRENT_EVENTS Possible Malicious Macro DL EXE Feb 2016
4.8	80	6	ET INFO Executable Download from dotted-quad Host
15	49204	6	ET INFO SUSPICIOUS Dotted Quad Host MZ Response
15	49204	6	ET POLICY PE EXE or DLL Windows file download HTTP
.108	2404	6	ET TROJAN Remcos RAT Checkin 23
15	49206	6	ET CURRENT_EVENTS DRIVEBY Likely Evil EXE with no referer from HFS webserve...
15	49206	6	ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP...
15	49206	6	ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP...
.81	80	6	ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of ...
15	49206	6	ET INFO EXE - Served Attached HTTP

Data ☑ Show Rule

```
_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET INFO Executable Download from dotted-quad Host";
to_server; content:".exe"; http_uri; nocase; content:".exe HTTP/1."; fast_pattern:only; content:"Host|3A 20|";
```

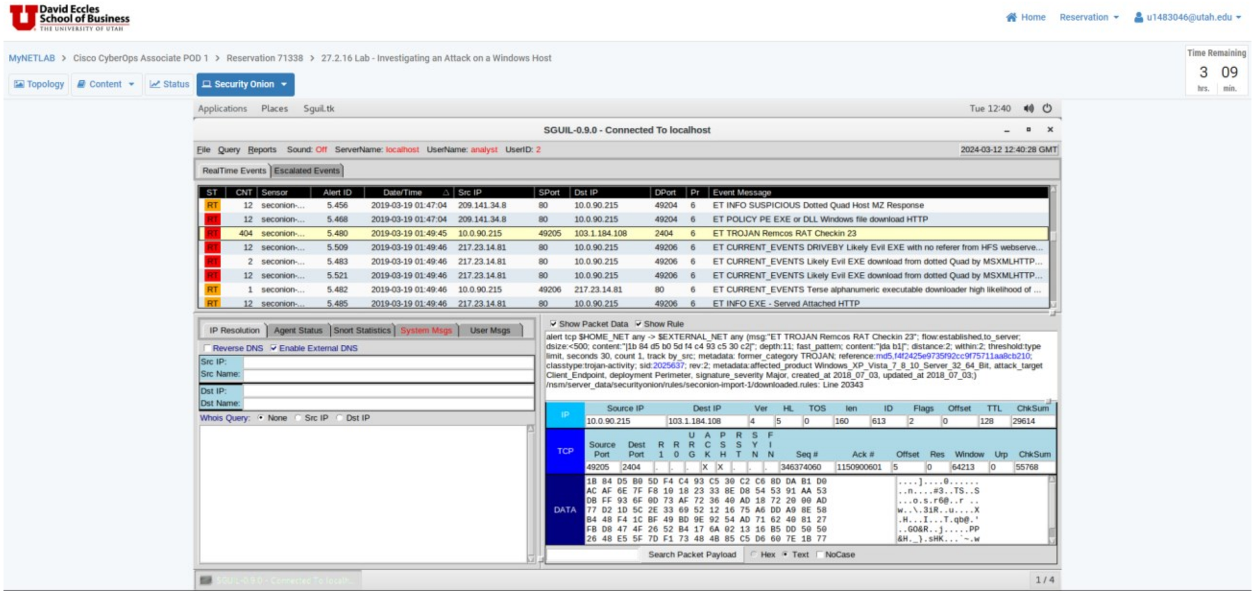
Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
0.215	209.141.34.8	4	5	0	348	421	2	0	128	40842

Dest Port	R 1	R 0	URG	ACK	PSH	RST	SYN	FIN	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
80	.	.	.	X	X	.	.	.	2938185605	1203208075	5	0	64240	0	30703

```
5 54 20 2F 74 65 73 74 31 2E 65 78 65 20 48      GET /test1.exe H
4 50 2F 31 2E 31 0D 0A 41 63 63 65 70 74 3A      TTP/1.1..Accept:
A 2F 2A 0D 0A 41 63 63 65 70 74 2D 45 6E 63       */*..Accept-Enc
4 69 6E 67 3A 20 67 7A 69 70 2C 20 64 65 66      oding: gzip, def
```

Search Packet Payload ○ Hex ● Text □ NoCase

3. Part 1, Step 2f



Sound: Off ServerName: localhost UserName: analyst UserID: 2

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	12	seconion-...	5.456	2019-03-19 01:47:04	209.141.34.8	80	10.0.90.215	49204	6	ET INFO SUSPICIOUS Dotted Quad Host MZ Response
RT	12	seconion-...	5.468	2019-03-19 01:47:04	209.141.34.8	80	10.0.90.215	49204	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	404	seconion-...	5.480	2019-03-19 01:49:45	10.0.90.215	49205	103.1.184.108	2404	6	ET TROJAN Remcos RAT Checkin 23
RT	12	seconion-...	5.509	2019-03-19 01:49:46	217.23.14.81	80	10.0.90.215	49206	6	ET CURRENT_EVENTS DRIVEBY Likely Evil EXE with no referer from HFS webserve...
RT	2	seconion-...	5.483	2019-03-19 01:49:46	217.23.14.81	80	10.0.90.215	49206	6	ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP...
RT	12	seconion-...	5.521	2019-03-19 01:49:46	217.23.14.81	80	10.0.90.215	49206	6	ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP...
RT	1	seconion-...	5.482	2019-03-19 01:49:46	10.0.90.215	49206	217.23.14.81	80	6	ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of ...
RT	12	seconion-...	5.485	2019-03-19 01:49:46	217.23.14.81	80	10.0.90.215	49206	6	ET INFO EXE - Served Attached HTTP

□ Reverse DNS ☑ Enable External DNS

Src IP:	
Src Name:	
Dst IP:	
Dst Name:	

Whois Query: ● None ○ Src IP ○ Dst IP

☑ Show Packet Data ☑ Show Rule

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Remcos RAT Checkin 23"; flow:established,to_server;
dsize:<500; content:"|1b 84 d5 b0 5d f4 c4 93 c5 30 c2|"; depth:11; fast_pattern; content:"|da b1|"; distance:2; within:2; threshold:type
limit, seconds 30, count 1, track by_src; metadata: former_category TROJAN; reference:md5,f4f2425e9735f92cc9f75711aa8cb210;
classtype:trojan-activity; sid:2025637; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target
Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_07_03, updated_at 2018_07_03;)
/nsm/server_data/securityonion/rules/seconion-import-1/downloaded.rules: Line 20343
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	10.0.90.215	103.1.184.108	4	5	0	160	613	2	0	128	29614

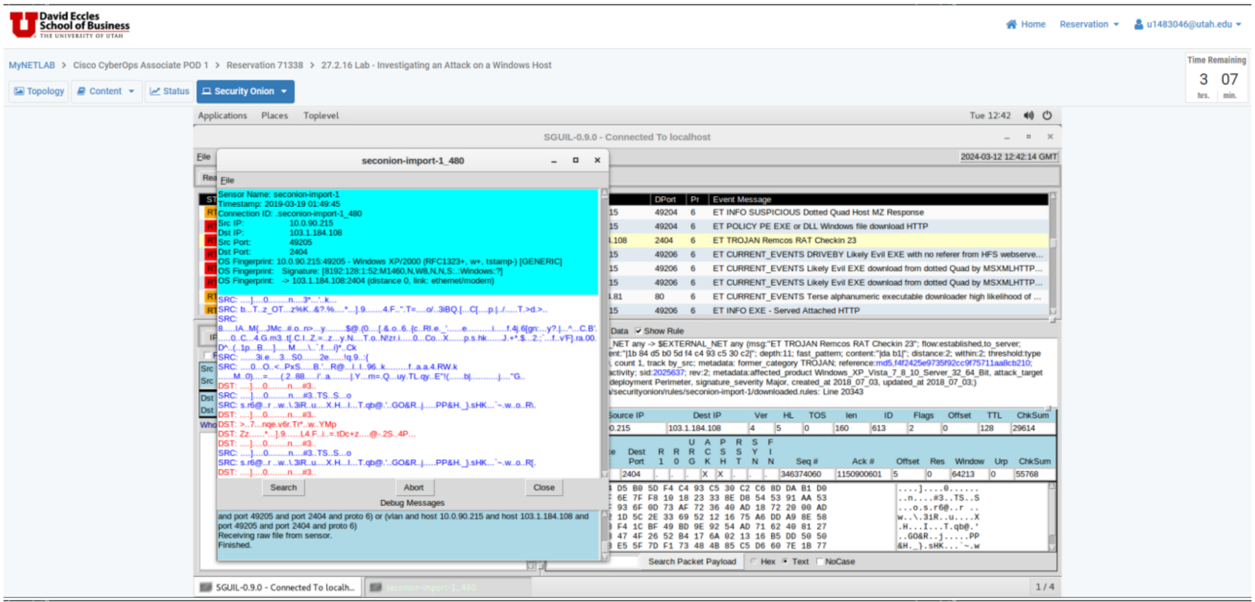
TCP	Source Port	Dest Port	R 1	R 0	URG	ACK	PSH	RST	SYN	FIN	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	49205	2404	.	.	.	X	X	.	.	.	346374060	1150900601	5	0	64213	0	55768

DATA

```
1B 84 D5 B0 5D F4 C4 93 C5 30 C2 C6 8D DA B1 D0      ....]....0......
AC AF 6E 7F F8 10 18 23 33 8E D8 54 53 91 AA 53      ..n....#3..TS..S
DB FF 93 6F 0D 73 AF 72 36 40 AD 18 72 20 00 AD      ...o.s.r6@..r ..
77 D2 1D 5C 2E 33 69 52 12 16 75 A6 DD A9 8E 58      w..\.3iR..u....X
B4 48 F4 1C BF 49 BD 9E 92 54 AD 71 62 40 81 27      .H...I...T.qb@.'
FB D8 47 4F 26 52 B4 17 6A 02 13 16 B5 DD 50 50      ..GO&R..j.....PP
26 48 E5 5F 7D F1 73 48 4B 85 C5 D6 60 7E 1B 77      &H._}.sHK...`~.w
```

Search Packet Payload ○ Hex ● Text □ NoCase

4. Part 1, Step 2g



2024-03-12 12:42:14 GMT

```
Sensor Name: seconion-import-1
Timestamp: 2019-03-19 01:49:45
Connection ID: .seconion-import-1_480
Src IP:            10.0.90.215
Dst IP:            103.1.184.108
Src Port:          49205
Dst Port:          2404
OS Fingerprint: 10.0.90.215:49205 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint:   Signature: [8192:128:1:52:M1460,N,W8,N,N,S::Windows:?]
OS Fingerprint:   -> 103.1.184.108:2404 (distance 0, link: ethernet/modem)

SRC: ....]....0.........n....3*....'..k....
SRC: b...T..z_OT....z%K..&?.%.....*....].9........4.F..".T=.....o/..3iBQ.[....C[.....p.|../......T.>d.>..
SRC:
8......IA...M{....JMc...#.o...n>....y..........$@.(0.....[.&.o..6..{c..Rl.e._'.......e............i......f.4j.6[gn:....y?.|....^....C.B'.
......0...C....4.G.m3..t[.C.I..Z.=...z....y.N.....T.o..N!zr.i......0....Co....X........p.s.hk........J.+*.$....2.;`.....f...v'F].ra.00.
D^..(..1p....B.....].......M......\..`.f.....i)*..Ck
SRC: ........3i.e.....3....S0.........2e........!q.9..:{
SRC: .....0....O..<...PxS......B.'....R@....I...I...96...k...........f...a.a.4.RW.k
........M...0)....=.......(.2...88.......i'...a..........|.Y....m=.Q....uy.TL.qy...E"!(........b|.............j....."G..
DST: ....]....0.........n....#3..
SRC: ....]....0.........n....#3..TS...S....o
SRC: s.r6@...r ..w..\.3iR...u.....X.H....I....T.qb@.'..GO&R..j.......PP&H._}.sHK....`~.w...o..R\.
DST: ....]....0.........n....#3..
DST: >...7....nqe.v6r.Tr*...w...YMp
DST: Zz.......*....].9.......L4.F...i...=.tDc+z.....@-.2S...4P....
DST: ....]....0.........n....#3..
SRC: ....]....0.........n....#3..TS...S....o
SRC: s.r6@...r ..w..\.3iR...u.....X.H....I....T.qb@.'..GO&R..j.......PP&H._}.sHK....`~.w...o..R[.
DST: ....]....0.........n....#3..
```

Debug Messages

```
and port 49205 and port 2404 and proto 6) or (vlan and host 10.0.90.215 and host 103.1.184.108 and
port 49205 and port 2404 and proto 6)
Receiving raw file from sensor.
Finished.
```

	DPort	Pr	Event Message
15	49204	6	ET INFO SUSPICIOUS Dotted Quad Host MZ Response
15	49204	6	ET POLICY PE EXE or DLL Windows file download HTTP
.108	2404	6	ET TROJAN Remcos RAT Checkin 23
15	49206	6	ET CURRENT_EVENTS DRIVEBY Likely Evil EXE with no referer from HFS webserve...
15	49206	6	ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP...
15	49206	6	ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP...
.81	80	6	ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of ...
15	49206	6	ET INFO EXE - Served Attached HTTP

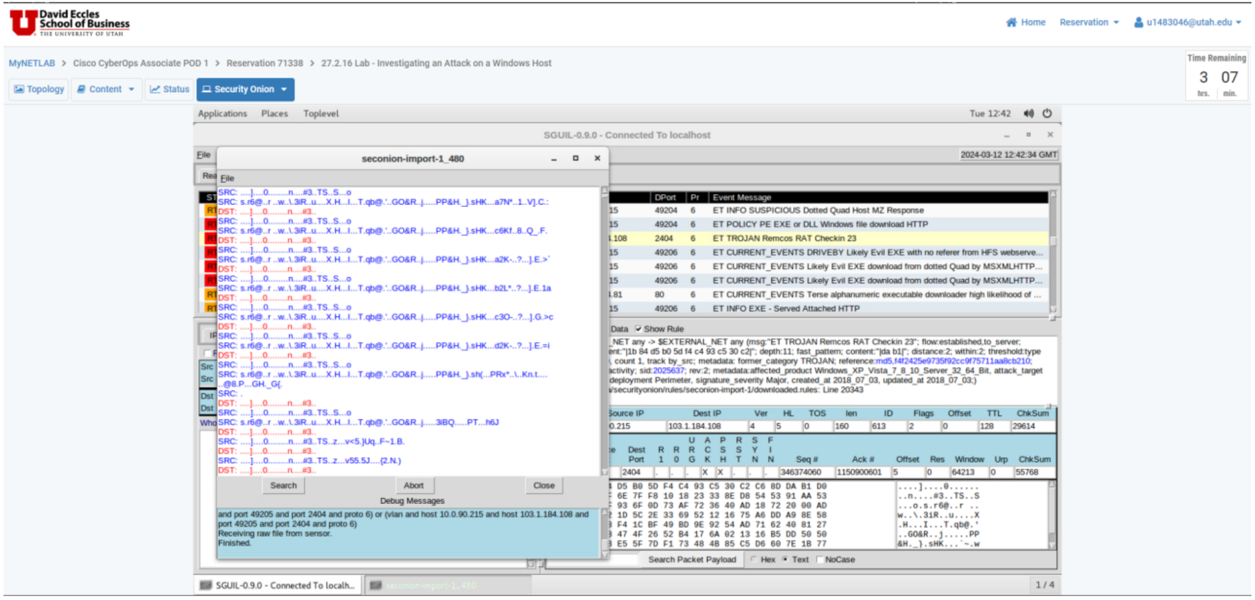
Data ☑ Show Rule

```
_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Remcos RAT Checkin 23"; flow:established,to_server;
ent:"|1b 84 d5 b0 5d f4 c4 93 c5 30 c2|"; depth:11; fast_pattern; content:"|da b1|"; distance:2; within:2; threshold:type
, count 1, track by_src; metadata: former_category TROJAN; reference:md5,f4f2425e9735f92cc9f75711aa8cb210;
activity; sid:2025637; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target
deployment Perimeter, signature_severity Major, created_at 2018_07_03, updated_at 2018_07_03;)
/securityonion/rules/seconion-import-1/downloaded.rules: Line 20343
```

Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
0.215	103.1.184.108	4	5	0	160	613	2	0	128	29614

Dest Port	R 1	R 0	URG	ACK	PSH	RST	SYN	FIN	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
2404	.	.	.	X	X	.	.	.	346374060	1150900601	5	0	64213	0	55768

```
 D5 B0 5D F4 C4 93 C5 30 C2 C6 8D DA B1 D0      ....]....0......
 6E 7F F8 10 18 23 33 8E D8 54 53 91 AA 53      ..n....#3..TS..S
 93 6F 0D 73 AF 72 36 40 AD 18 72 20 00 AD      ...o.s.r6@..r ..
 1D 5C 2E 33 69 52 12 16 75 A6 DD A9 8E 58      w..\.3iR..u....X
 F4 1C BF 49 BD 9E 92 54 AD 71 62 40 81 27      .H...I...T.qb@.'
 47 4F 26 52 B4 17 6A 02 13 16 B5 DD 50 50      ..GO&R..j.....PP
 E5 5F 7D F1 73 48 4B 85 C5 D6 60 7E 1B 77      &H._}.sHK...`~.w
```



2024-03-12 12:42:34 GMT

```
SRC: ....]....0.........n....#3..TS...S....o
SRC: s.r6@...r ..w..\.3iR...u.....X.H....I....T.qb@.'..GO&R..j.......PP&H._}.sHK....a7N*...1...V].C.:
DST: ....]....0.........n....#3..
SRC: ....]....0.........n....#3..TS...S....o
SRC: s.r6@...r ..w..\.3iR...u.....X.H....I....T.qb@.'..GO&R..j.......PP&H._}.sHK....c6Kf...8...Q_.F.
DST: ....]....0.........n....#3..
SRC: ....]....0.........n....#3..TS...S....o
SRC: s.r6@...r ..w..\.3iR...u.....X.H....I....T.qb@.'..GO&R..j.......PP&H._}.sHK....a2K-...?....].E.>`
DST: ....]....0.........n....#3..
SRC: ....]....0.........n....#3..TS...S....o
SRC: s.r6@...r ..w..\.3iR...u.....X.H....I....T.qb@.'..GO&R..j.......PP&H._}.sHK....b2L*...?....].E.1a
DST: ....]....0.........n....#3..
SRC: ....]....0.........n....#3..TS...S....o
SRC: s.r6@...r ..w..\.3iR...u.....X.H....I....T.qb@.'..GO&R..j.......PP&H._}.sHK....c3O-...?....].G.>c
DST: ....]....0.........n....#3..
SRC: ....]....0.........n....#3..TS...S....o
SRC: s.r6@...r ..w..\.3iR...u.....X.H....I....T.qb@.'..GO&R..j.......PP&H._}.sHK....d2K-...?....].E.=i
DST: ....]....0.........n....#3..
SRC: ....]....0.........n....#3..TS...S....o
SRC: s.r6@...r ..w..\.3iR...u.....X.H....I....T.qb@.'..GO&R..j.......PP&H._}.sh(....PRx*...\...Kn.t.....
..@8.P....GH._G[.
SRC: .
DST: ....]....0.........n....#3..
SRC: ....]....0.........n....#3..TS...S....o
SRC: s.r6@...r ..w..\.3iR...u.....X.H....I....T.qb@.'..GO&R..j.......3iBQ......PT....h6J
DST: ....]....0.........n....#3..
SRC: ....]....0.........n....#3..TS...z....v<5.}Uq...F~1.B.
DST: ....]....0.........n....#3..
SRC: ....]....0.........n....#3..TS...z....v55.5J.....{2.N.)
DST: ....]....0.........n....#3..
```

Debug Messages

```
and port 49205 and port 2404 and proto 6) or (vlan and host 10.0.90.215 and host 103.1.184.108 and
port 49205 and port 2404 and proto 6)
Receiving raw file from sensor.
Finished.
```

	DPort	Pr	Event Message
15	49204	6	ET INFO SUSPICIOUS Dotted Quad Host MZ Response
15	49204	6	ET POLICY PE EXE or DLL Windows file download HTTP
.108	2404	6	ET TROJAN Remcos RAT Checkin 23
15	49206	6	ET CURRENT_EVENTS DRIVEBY Likely Evil EXE with no referer from HFS webserve...
15	49206	6	ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP...
15	49206	6	ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP...
.81	80	6	ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of ...
15	49206	6	ET INFO EXE - Served Attached HTTP

Data ☑ Show Rule

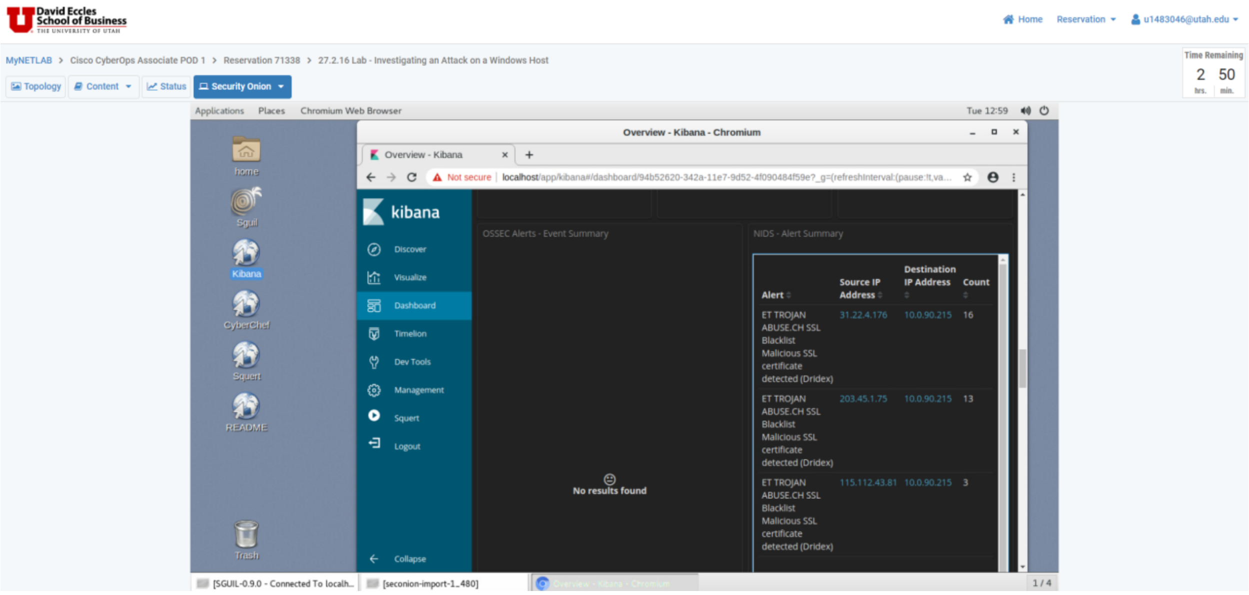
```
_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Remcos RAT Checkin 23"; flow:established,to_server;
ent:"|1b 84 d5 b0 5d f4 c4 93 c5 30 c2|"; depth:11; fast_pattern; content:"|da b1|"; distance:2; within:2; threshold:type
, count 1, track by_src; metadata: former_category TROJAN; reference:md5,f4f2425e9735f92cc9f75711aa8cb210;
activity; sid:2025637; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target
deployment Perimeter, signature_severity Major, created_at 2018_07_03, updated_at 2018_07_03;)
/securityonion/rules/seconion-import-1/downloaded.rules: Line 20343
```

Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
0.215	103.1.184.108	4	5	0	160	613	2	0	128	29614

Dest Port	R 1	R 0	URG	ACK	PSH	RST	SYN	FIN	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
2404	.	.	.	X	X	.	.	.	346374060	1150900601	5	0	64213	0	55768

```
 D5 B0 5D F4 C4 93 C5 30 C2 C6 8D DA B1 D0      ....]....0......
 6E 7F F8 10 18 23 33 8E D8 54 53 91 AA 53      ..n....#3..TS..S
 93 6F 0D 73 AF 72 36 40 AD 18 72 20 00 AD      ...o.s.r6@..r ..
 1D 5C 2E 33 69 52 12 16 75 A6 DD A9 8E 58      w..\.3iR..u....X
 F4 1C BF 49 BD 9E 92 54 AD 71 62 40 81 27      .H...I...T.qb@.'
 47 4F 26 52 B4 17 6A 02 13 16 B5 DD 50 50      ..GO&R..j.....PP
 E5 5F 7D F1 73 48 4B 85 C5 D6 60 7E 1B 77      &H._}.sHK...`~.w
```

5. Part 2, Step 2b



localhost/app/kibana#/dashboard/94b52620-342a-11e7-9d52-4f090484f59e?_g=(refreshInterval:(pause:!t,va...

OSSEC Alerts - Event Summary

No results found

NIDS - Alert Summary

Alert	Source IP Address	Destination IP Address	Count
ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	31.22.4.176	10.0.90.215	16
ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	203.45.1.75	10.0.90.215	13
ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	115.112.43.81	10.0.90.215	3