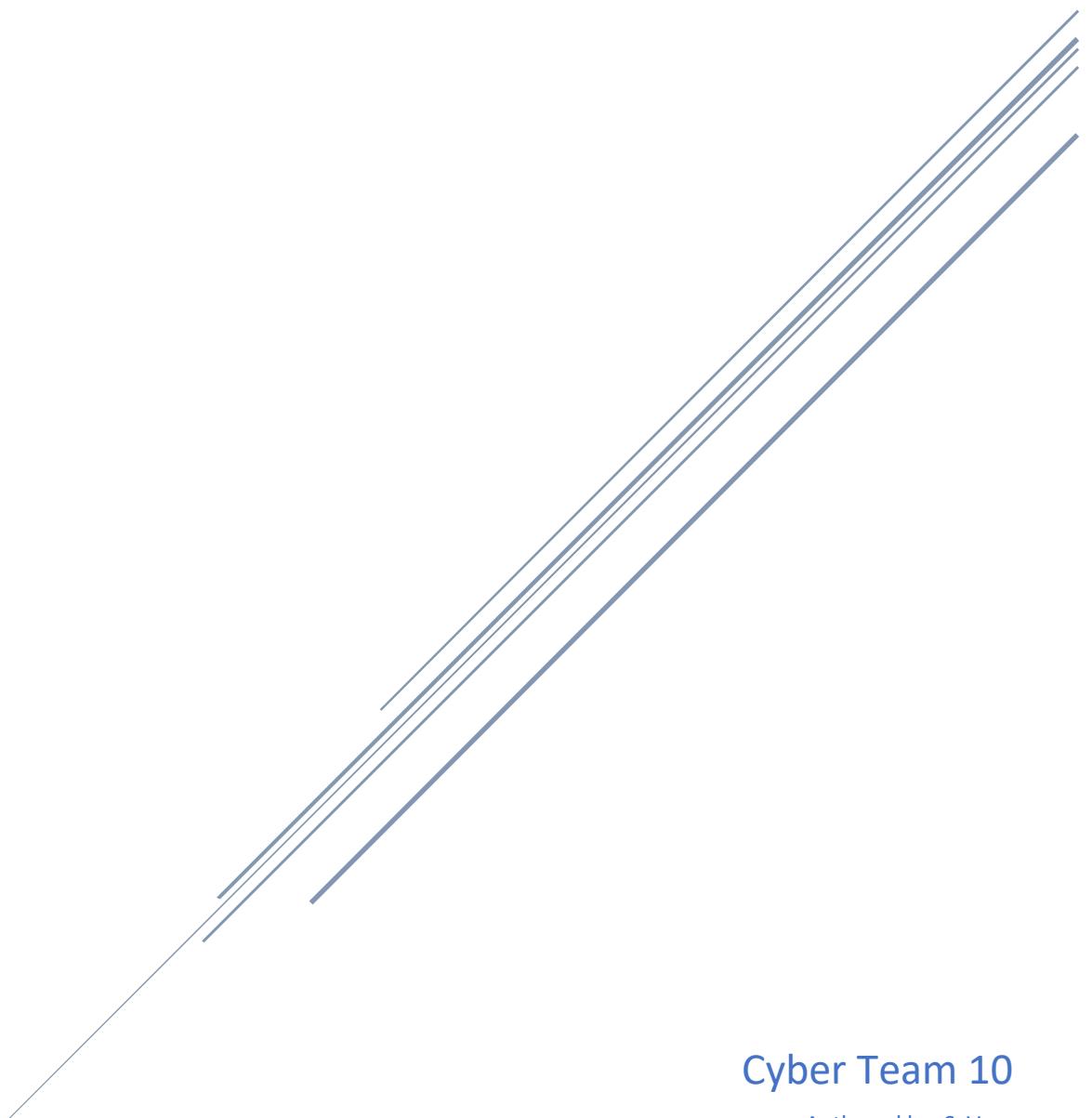


TASK 6 - TECHNICAL APPENDIX

Rev D



Cyber Team 10

Authored by: S. Voss

TABLE OF CONTENTS

1 - SEARCH AND DISCOVERY	2
2 - IDENTIFYING EMAILS WITH TIMESTAMP	18
3 - EVENT ID 11: FILE CREATE.....	19
4 - TIME RANGES	24
5 - EVENT ID 1 – PROCESS CREATION	28
6 - C2 TRAFFIC	36
7 - IDENTIFYING FIRST EXECUTION OF THE MALWARE BINARY	42
8 - REGISTRY EVENTS.....	44
9 - EK COMPROMISE VERIFICATION & MALWARE SUCCESS / FAILURE	48
10 – MEMORY	53
11 – EXECUTION TREE PROCESS.....	60

1 - SEARCH AND DISCOVERY

Option to set the time format to 2400

Change US to GB in address line...

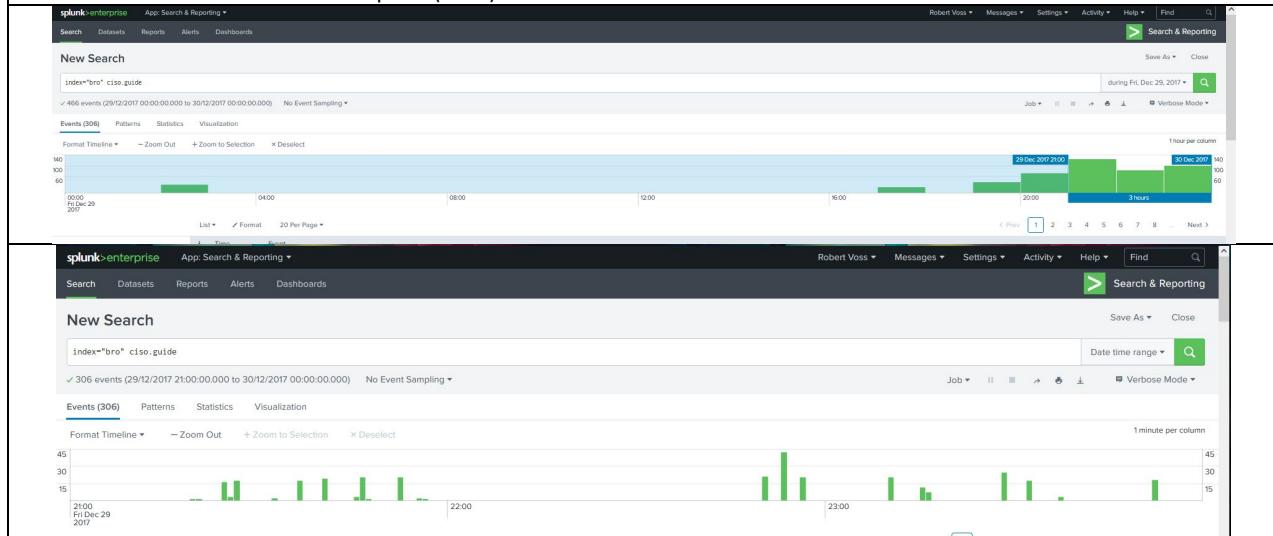
al:8000/en-US/app/search/ to :8000/en-GB/app/search/

Start with the day of the email...29-12-2017 (this format because of the 2400 clock change – dd-mm-yyyy)



The email arrived at 15:58 EST (converted to UCT makes it 20:58)

Set the search from the time it took place (2100) onward and zoom the selection.



Analyzing the suspicious email shows it aimed to convince recipients to visit ciso[.]guide.

The exploration led us to consider the possibility of a drive-by compromise as an initial access method. Simply browsing a compromised site could introduce malware to a system.

With this knowledge, we dove into our SIEM logs, focusing on network traffic connected to ciso[.]guide—the potentially compromised site.

While navigating the logs, we came across the `http_referer` field, a useful indicator of origin and redirection in web traffic.

We then asked, where was traffic from ciso[.]guide being referred to?

Our search for traffic originating from ciso[.]guide but being referred elsewhere unveiled anomalies: unresolved domain names and excessively complex URIs.

Digging deeper, we pinpointed the IP address associated with these anomalies and conducted further investigations online. Our findings confirmed our suspicions: the logs indicated encounters with a Rig EK landing page by four AT-USA devices.

When we first got into the SIEM, we had no idea what kind of information would be contained in each of the available log sources. We had to profile each log source, which meant manually exploring each index and literally just start clicking on stuff. There was no other way to go about it. As we were going through this process, we stumbled upon the `http_referrer` field.

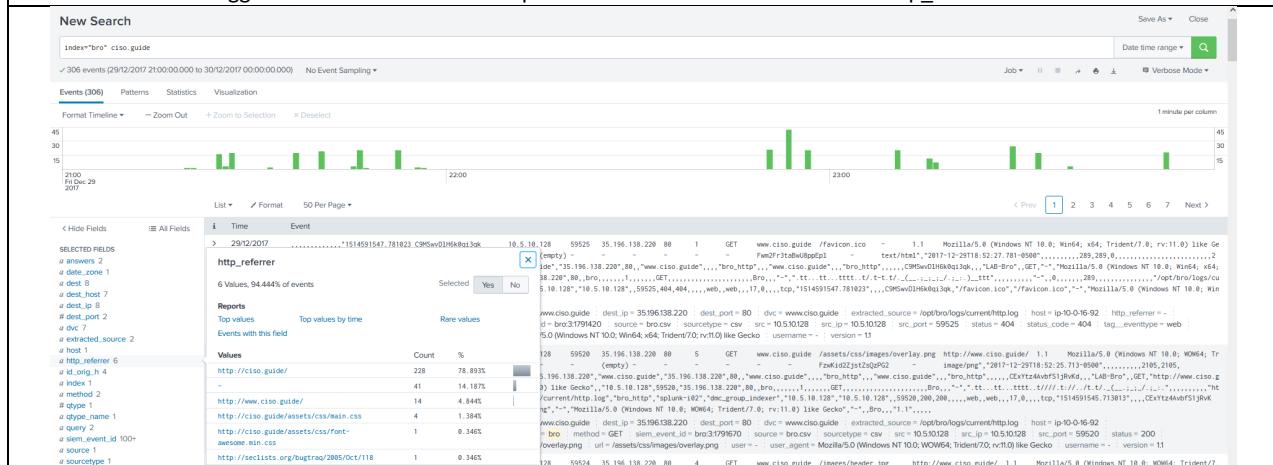
Interpreting the field name:

"http" relates to web traffic.

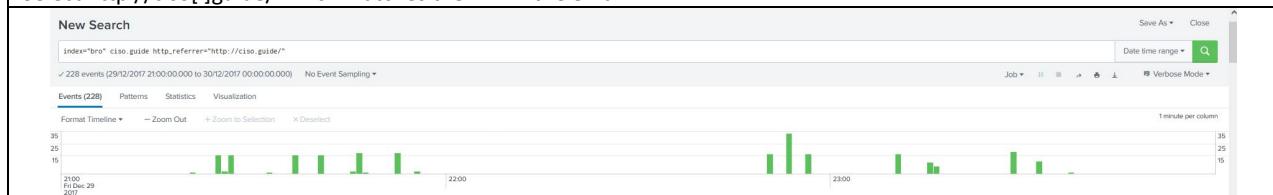
"referrer" indicated the referral or redirection of traffic.

We selected that field and conducted some searches with it until we stumbled upon the weird stuff.

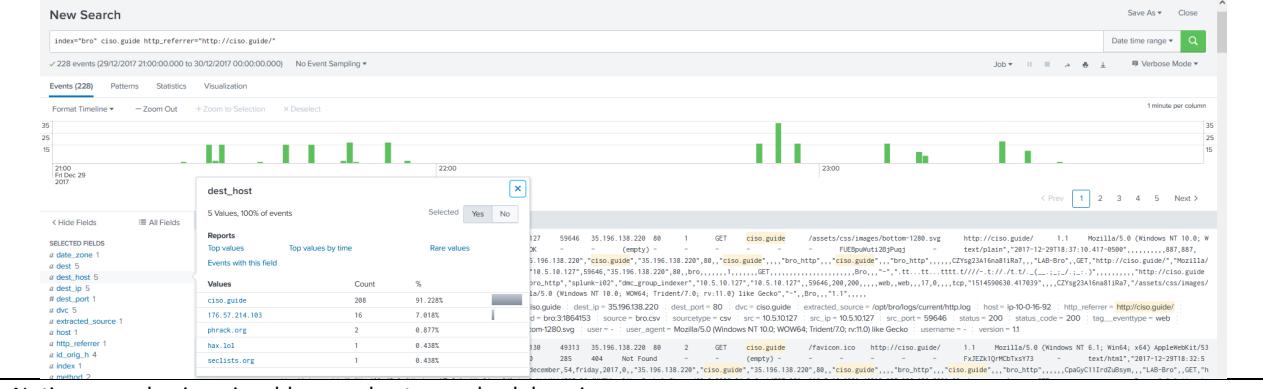
Because the email suggested to visit a website an option in the search was to select the http_referrer field.



Select [http://ciso\[.\]guide/](http://ciso[.]guide/) which matches the link in the email



Continuing to investigate the various fields
Select dest_host and examine for differences



Notice one value is an ip address and not a resolved domain name.

176.57.214.103 (this is not correct and a sign of a possible problem)

Continuing to investigate the various fields

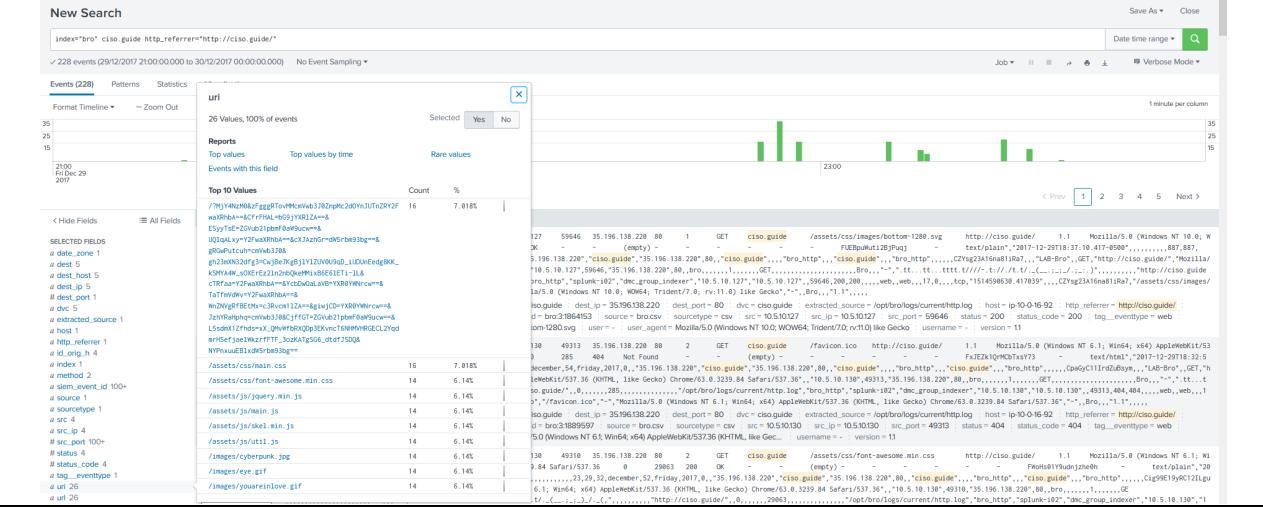
Select dest_ip and examine.

Inspect dest_ip

ip 176.57.214.103 is seen again

Continuing to investigate the various fields

Select uri field and examine.



Notice the obvious strange link

uri

26 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
/?MjY4NzM0&zFgggRTovMMcmVwb3J0ZnpMc2d0YnJUTnZRY2F	16	7.018%
waXRhbA==&CfrFHAL=bG9jYXR1ZA==&		
ESyyTsE=ZGVub21pbmF0aW9ucw==&		
UQ1qALxy=Y2FwaXRhbA==&cXJAzhGr=dW5rbm93bg==&		
gRGwPutcuh=cmVwb3J0&		
gh23mXN32dfg3=CwjBeJKgBj1Y1ZUV0U9qD_iUDUnEedg8KK_		
KSMYA4W_sOXErEz2ln2nbQkeMMixB6E61ETi-1L&		
cTRfaa=Y2FwaXRhbA==&YcbDwOaLaVB=YXR0YWNrcw==&		
TaTfmVdWv=Y2FwaXRhbA==&		
WnZNVgRfBEtMx=c3Rvcml1ZA==&giwjCD=YXR0YWNrcw==&		
JzhYRaPhpq=cmVwb3J0&CjffGT=ZGVub21pbmF0aW9ucw==&		
L5sdmX1Zfhds=xX_QMvWfbRXQDp3EKvncT6NHMVHRGECL2Yqd		
mrHSejaelWkzrfFTF_3ozKATgSG6_dtdfJSQ&		
NYPnxuuEB1xdW5rbm93bg==		
/assets/css/main.css	16	7.018%
/assets/css/font-awesome.min.css	14	6.14%
/assets/js/jquery.min.js	14	6.14%
/assets/js/main.js	14	6.14%
/assets/js/skel.min.js	14	6.14%
/assets/js/util.js	14	6.14%
/images/cyberpunk.jpg	14	6.14%
/images/eye.gif	14	6.14%
/images/youareinlove.gif	14	6.14%

Click on the strange link to add to the search

New Search

Save As ▾ Close

Index*bro* ciso_guide http://ciso_guide/* url*/?MjY4NzM0&zFgggRTovMMcmVwb3J0ZnpMc2d0YnJUTnZRY2F

Date time range ▾

✓ 16 events (29/12/2017 21:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling ▾

Events (16) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection X Deselect

1 minute per column

2
1
0

21:00 21 Dec 29 2017

With the uri in the search...select dest_ip and you see the same questionable ip address ip 176.57.214.103

New Search

```
index=*bro* ciso_guide http.referred="http://ciso_guide/*" uri="/?YjYwZmBzLggfTowMcmw3176zrpq230Yn1zNzY2wxXrbA=&CfFHAL+6g9jYXR1ZA+=E5SyyTtE=ZoVab21pbmf8a9uucw=8UQ1qAly=Y2fxXrbA=&cJAzGr=dW5tbe93bg=&gGePutcuwcnvib328agb23eXN3d2fg3
=&wzbkxgj1112wvnb0_1UD0neq8KX_KSM4W_0DXFr21n0qekh5i0DE61ET1-1L8cTRFa+&Y3DwOuLav0-YX89Wrc+c=St7Tm7dr+&wzNgrfbtth+&3rvca12A+&g1qjC+YX89Wrc+c=8JzhVrphqcnwE3838CjffG=ZoVab21pbmf8a9uucw=8L5sdX12fhds
=xz_QuHrftkQp3ExncTNNWHRGECL2yamrnfjeat1kzrFF7_3oXkATg56_ottf30Q0ANPvxxuE31x95tbe93bg*"
```

16 events (29/12/2017 21:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling ▾

Events (16) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection X Deselect

1 minute per column

dest_ip

1 Value, 100% of events Selected Yes No

Reports Top values Top values by time Events with this field

Values 176.57.214.103 Count % 16 100%

dest_ip 59148 176.57.214.103 88 1 GET /?YjYwZmBzLggfTowMcmw3176zrpq230Yn1zNzY2wxXrbA=&CfFHAL+6g9jYXR1ZA+=E5SyyTtE=ZoVab21pbmf8a9uucw=8UQ1qAly=Y2fxXrbA=&cJAzGr=dW5tbe93bg=&gGePutcuwcnvib328agb23eXN3d2fg3
=&wzbkxgj1112wvnb0_1UD0neq8KX_KSM4W_0DXFr21n0qekh5i0DE61ET1-1L8cTRFa+&Y3DwOuLav0-YX89Wrc+c=St7Tm7dr+&wzNgrfbtth+&3rvca12A+&g1qjC+YX89Wrc+c=8JzhVrphqcnwE3838CjffG=ZoVab21pbmf8a9uucw=8L5sdX12fhds
=xz_QuHrftkQp3ExncTNNWHRGECL2yamrnfjeat1kzrFF7_3oXkATg56_ottf30Q0ANPvxxuE31x95tbe93bg*"

23:00

Now pivot from current search to just bro logs and the questionable ip 176.57.214.103 by clicking on the ip and trimming up the search.

New Search

```
index=*bro* ciso_guide http.referred="http://ciso_guide/*" uri="/?YjYwZmBzLggfTowMcmw3176zrpq230Yn1zNzY2wxXrbA=&CfFHAL+6g9jYXR1ZA+=E5SyyTtE=ZoVab21pbmf8a9uucw=8UQ1qAly=Y2fxXrbA=&cJAzGr=dW5tbe93bg=&gGePutcuwcnvib328agb23eXN3d2fg3
=&wzbkxgj1112wvnb0_1UD0neq8KX_KSM4W_0DXFr21n0qekh5i0DE61ET1-1L8cTRFa+&Y3DwOuLav0-YX89Wrc+c=St7Tm7dr+&wzNgrfbtth+&3rvca12A+&g1qjC+YX89Wrc+c=8JzhVrphqcnwE3838CjffG=ZoVab21pbmf8a9uucw=8L5sdX12fhds
=xz_QuHrftkQp3ExncTNNWHRGECL2yamrnfjeat1kzrFF7_3oXkATg56_ottf30Q0ANPvxxuE31x95tbe93bg*"
```

16 events (29/12/2017 21:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling ▾

Events (16) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection X Deselect

1 minute per column

dest_ip 176.57.214.103

dest_ip 59148 176.57.214.103 88 1 GET /?YjYwZmBzLggfTowMcmw3176zrpq230Yn1zNzY2wxXrbA=&CfFHAL+6g9jYXR1ZA+=E5SyyTtE=ZoVab21pbmf8a9uucw=8UQ1qAly=Y2fxXrbA=&cJAzGr=dW5tbe93bg=&gGePutcuwcnvib328agb23eXN3d2fg3
=&wzbkxgj1112wvnb0_1UD0neq8KX_KSM4W_0DXFr21n0qekh5i0DE61ET1-1L8cTRFa+&Y3DwOuLav0-YX89Wrc+c=St7Tm7dr+&wzNgrfbtth+&3rvca12A+&g1qjC+YX89Wrc+c=8JzhVrphqcnwE3838CjffG=ZoVab21pbmf8a9uucw=8L5sdX12fhds
=xz_QuHrftkQp3ExncTNNWHRGECL2yamrnfjeat1kzrFF7_3oXkATg56_ottf30Q0ANPvxxuE31x95tbe93bg*"

23:00

New Search

index=*bro* dest_ip=176.57.214.103*

16 events (29/12/2017 21:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling ▾

Events (16) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection X Deselect

1 minute per column

dest_ip 176.57.214.103

dest_ip 59148 176.57.214.103 88 1 GET /?YjYwZmBzLggfTowMcmw3176zrpq230Yn1zNzY2wxXrbA=&CfFHAL+6g9jYXR1ZA+=E5SyyTtE=ZoVab21pbmf8a9uucw=8UQ1qAly=Y2fxXrbA=&cJAzGr=dW5tbe93bg=&gGePutcuwcnvib328agb23eXN3d2fg3
=&wzbkxgj1112wvnb0_1UD0neq8KX_KSM4W_0DXFr21n0qekh5i0DE61ET1-1L8cTRFa+&Y3DwOuLav0-YX89Wrc+c=St7Tm7dr+&wzNgrfbtth+&3rvca12A+&g1qjC+YX89Wrc+c=8JzhVrphqcnwE3838CjffG=ZoVab21pbmf8a9uucw=8L5sdX12fhds
=xz_QuHrftkQp3ExncTNNWHRGECL2yamrnfjeat1kzrFF7_3oXkATg56_ottf30Q0ANPvxxuE31x95tbe93bg*"

23:00

Now see who's talking to who...

Select src_ip

New Search

```
index=*bro* dest_ip=176.57.214.103*
```

16 events (29/12/2017 21:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling ▾

Events (16) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection X Deselect

1 minute per column

src_ip

4 Values, 100% of events Selected Yes No

Reports Top values Top values by time Events with this field

Values 176.57.214.103 Count % 1 100%

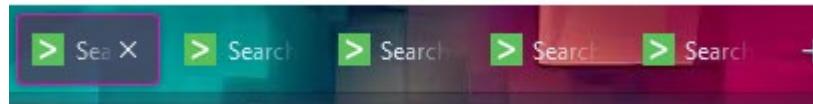
src_ip 59148 176.57.214.103 88 1 GET /?YjYwZmBzLggfTowMcmw3176zrpq230Yn1zNzY2wxXrbA=&CfFHAL+6g9jYXR1ZA+=E5SyyTtE=ZoVab21pbmf8a9uucw=8UQ1qAly=Y2fxXrbA=&cJAzGr=dW5tbe93bg=&gGePutcuwcnvib328agb23eXN3d2fg3
=&wzbkxgj1112wvnb0_1UD0neq8KX_KSM4W_0DXFr21n0qekh5i0DE61ET1-1L8cTRFa+&Y3DwOuLav0-YX89Wrc+c=St7Tm7dr+&wzNgrfbtth+&3rvca12A+&g1qjC+YX89Wrc+c=8JzhVrphqcnwE3838CjffG=ZoVab21pbmf8a9uucw=8L5sdX12fhds
=xz_QuHrftkQp3ExncTNNWHRGECL2yamrnfjeat1kzrFF7_3oXkATg56_ottf30Q0ANPvxxuE31x95tbe93bg*"

23:00

There are 4 ip addresses that are being referred over to ip 176.57.214.103

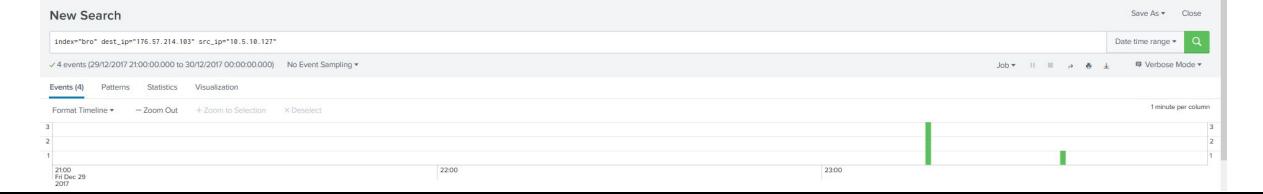
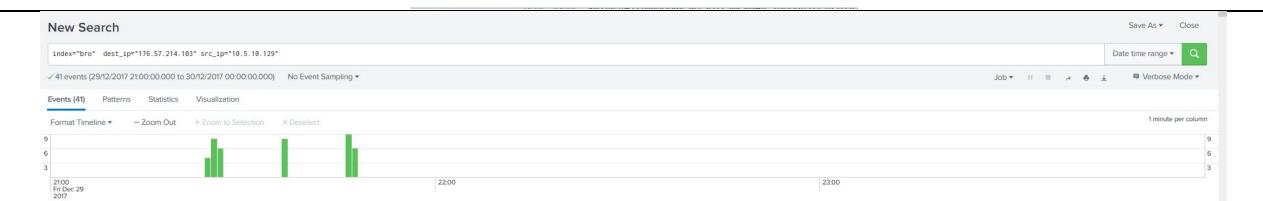
Now that the 4 devices have been identified you want to look deeper into each device...

Create (duplicate) 4 tabs...one for each device and rename the tabs for ease of identification and use



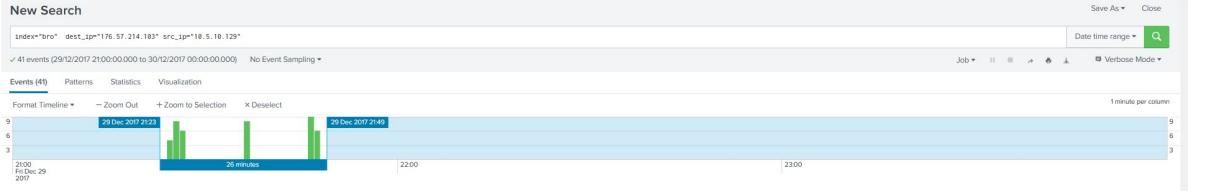
Now go into each device on each identified tab by clicking on each correlating ip address shown

src_ip	Count	%
10.5.10.129	41	55.40%
10.5.10.130	20	27.02%
10.5.10.128	9	12.16%
10.5.10.127	4	5.40%

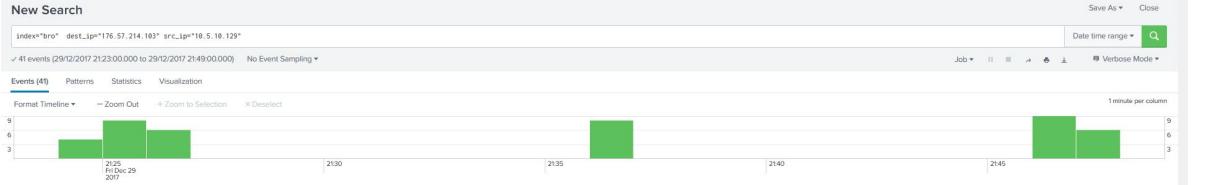


Now investigate each device separately...

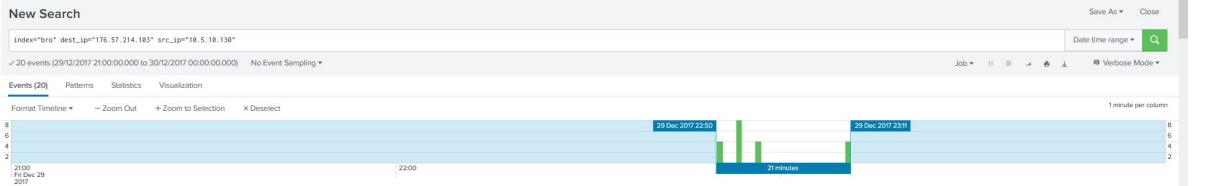
129



+ Zoom to selection



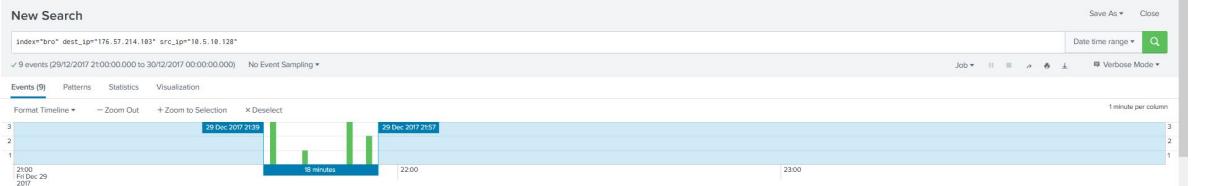
130



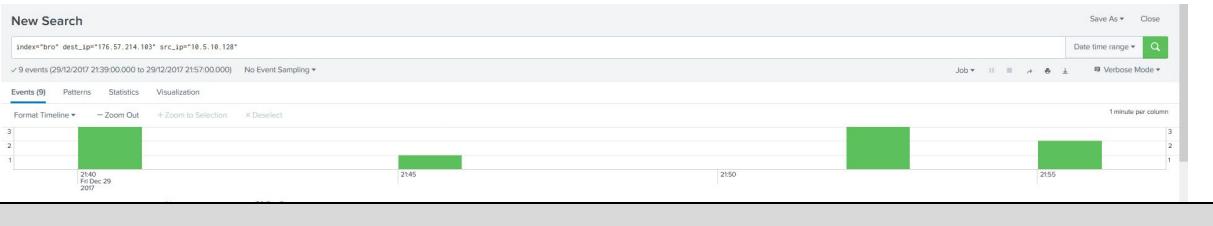
+ Zoom to selection

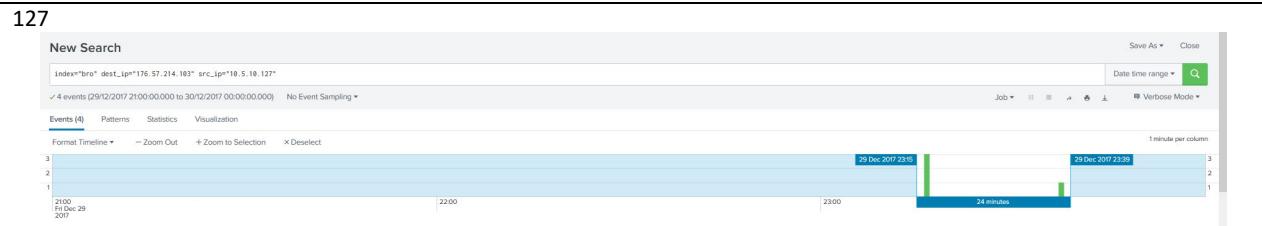


128

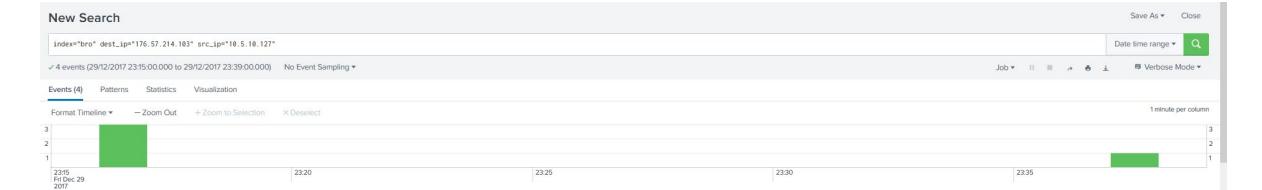


+ Zoom to selection

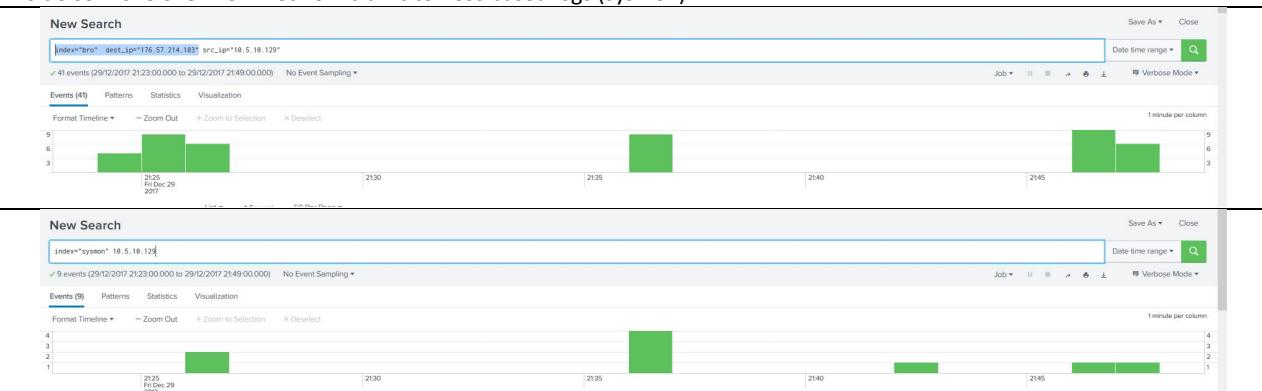




+ Zoom to selection



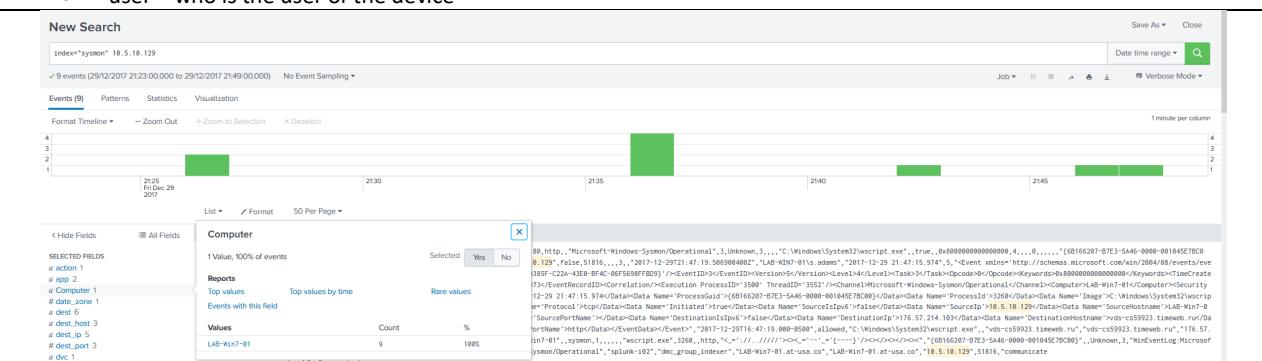
Now pivot from network traffic to host-based logs for each device by eliminating the bro from each of the searches... To do so move over from network traffic to host-based logs (sysmon).



Once in host-based logs there are 9 events for 129.

Various fields to check:

- Computer - Computer gives us the computer name which should be the main source used from now on, as ip addresses can change for each device as it logs into the network. The device name should almost ALWAYS remain the same.
 - scr_ip – gives us the current operating ip address the device is using
 - user – who is the user of the device



Computer gives us LAB-Win07-01 as the device name.

Scr_ip identifies the ip address as 10.5.10.129

The screenshot shows a Microsoft Power BI Data Studio interface with the following details:

- Top Bar:** Shows "Index='syomon' 10.5.10.129" and "Date time range".
- Event Log View:** Displays 9 events from 29/12/2017 21:23:00.000 to 29/12/2017 21:49:00.000. The first event is "No Event Sampling".
- Event Details:** A large green bar spans from 21:25 to 21:35, representing event ID 2.
- Event Timeline:** A timeline from 21:25 to 21:45 showing event IDs 1, 2, 3, 4, and 5.
- Event Fields:** A table showing fields like Action, App, Computer, Date, Dest, Dir, EventCode, EventDescription, EventID, ExtractedSource, Host, Image, Index, Process, ProcName, ProcThread, ProcType, ProcUser, Source, SourceType, Tag, and User.
- User Section:** Shows a user named "LAB-WIN-01\syomon" with a password hash of "488100...".
- Reports:** A section for "Top values" and "Events with this field".
- Values:** A table showing counts and percentages for various values like "LAB-WIN-01\syomon", "NT AUTHORITY\LOCAL SERVICE", and "NT AUTHORITY\NETWORK SERVICE".

User shows LAB-Win7-01\s.adams with s.adams as the user

You can see it's

Computer: LAB-Win07-1

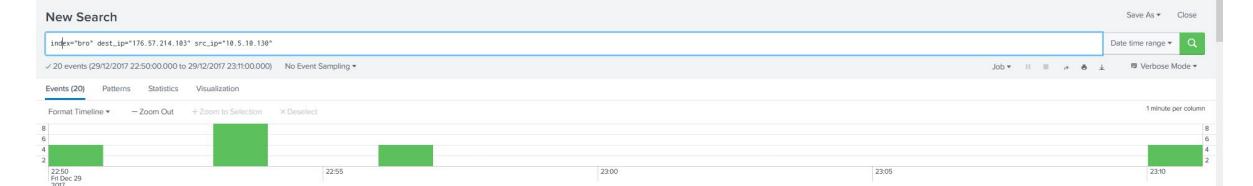
ip address: matches, 10

user: s. adams

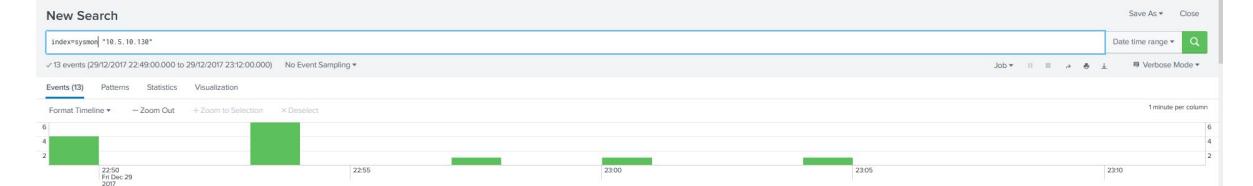
Do the same steps on all the remaining tabs

130

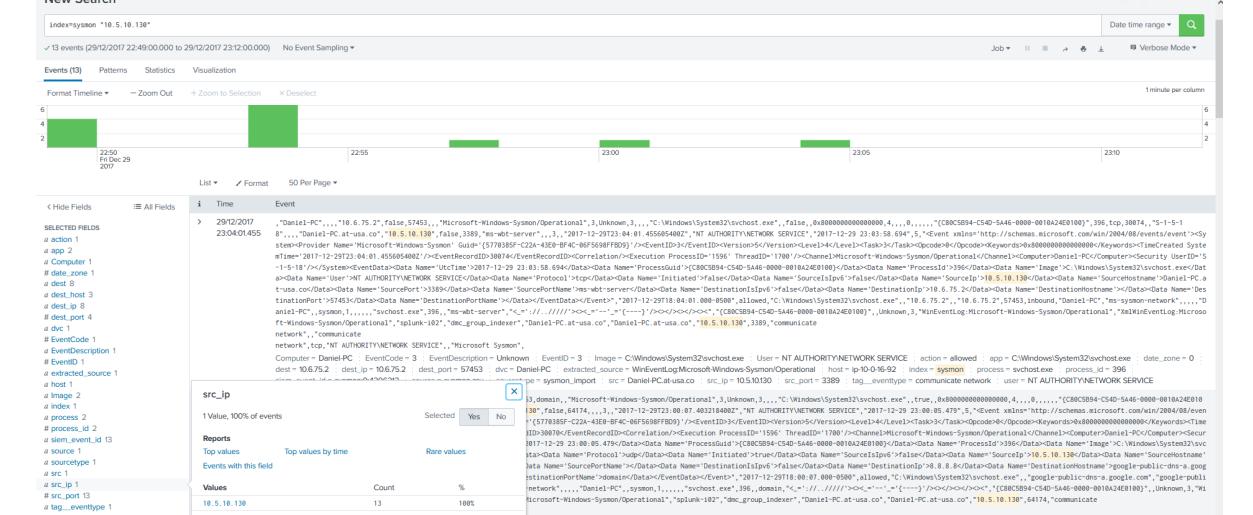
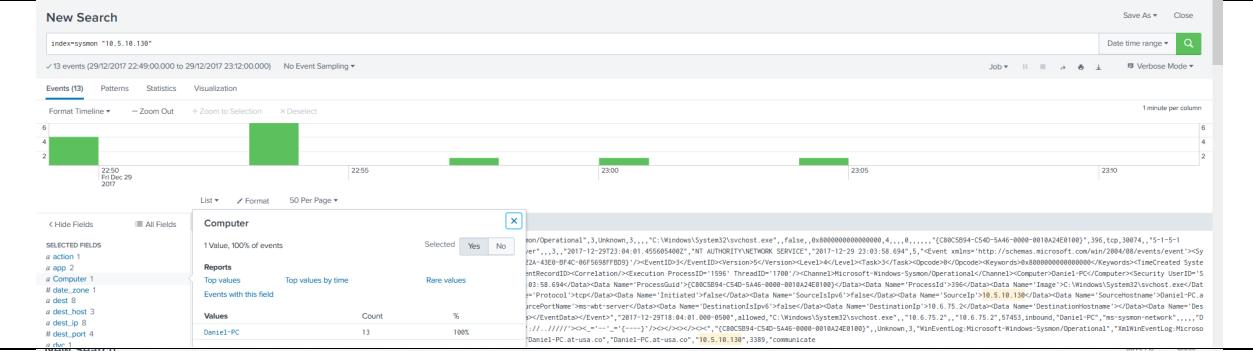
From

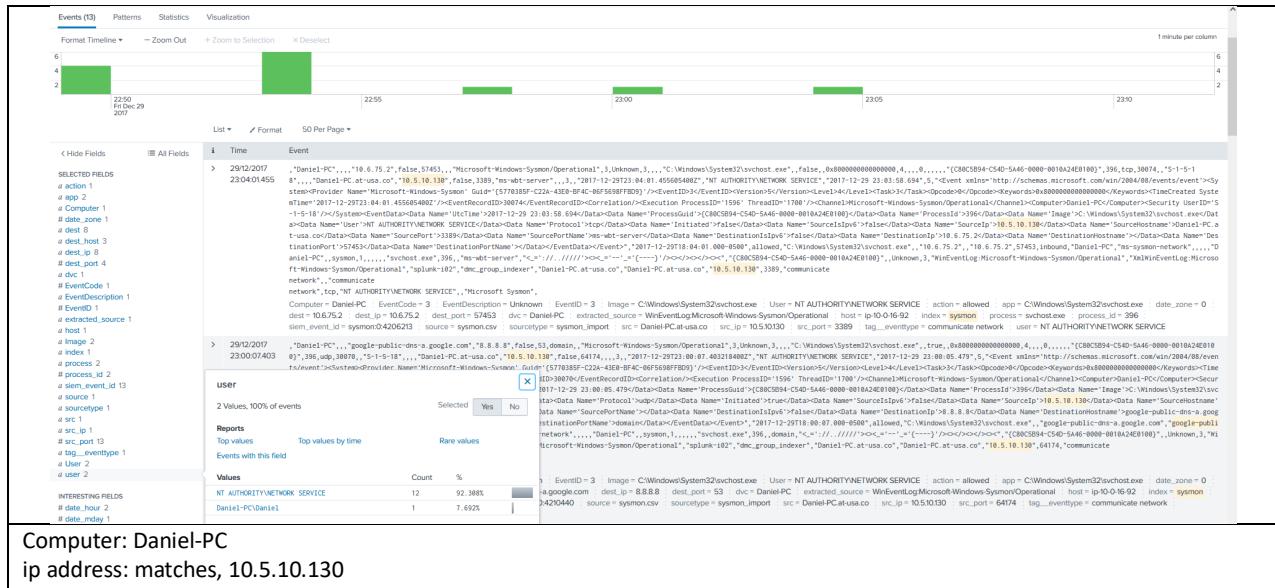


to



Investigate the three fields and identify the computer





Computer: Daniel-PC

ip address: matches, 10.5.10.130

user: Daniel-PC\Daniel

128

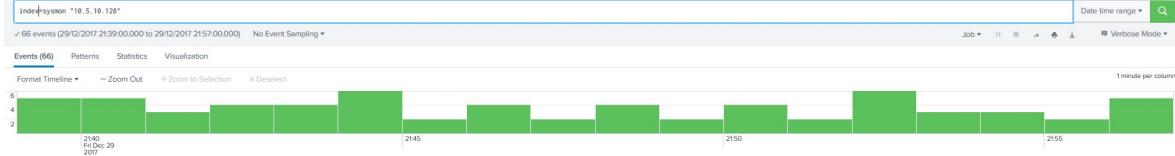
From

New Search



To

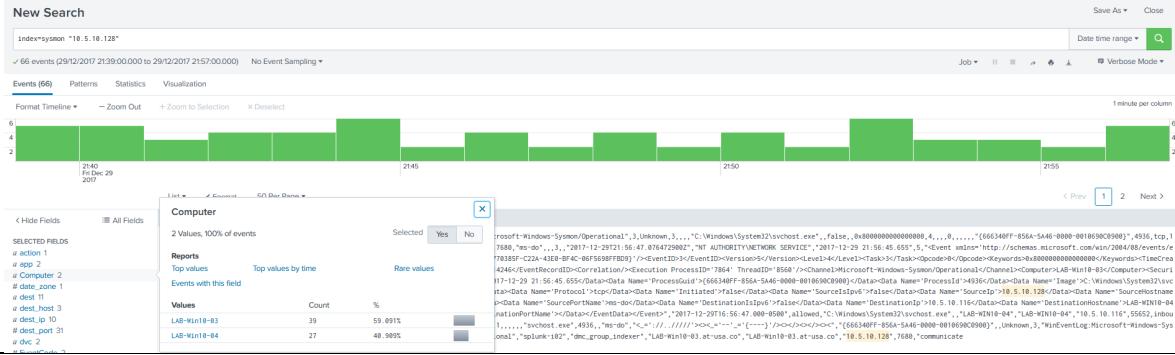
New Search



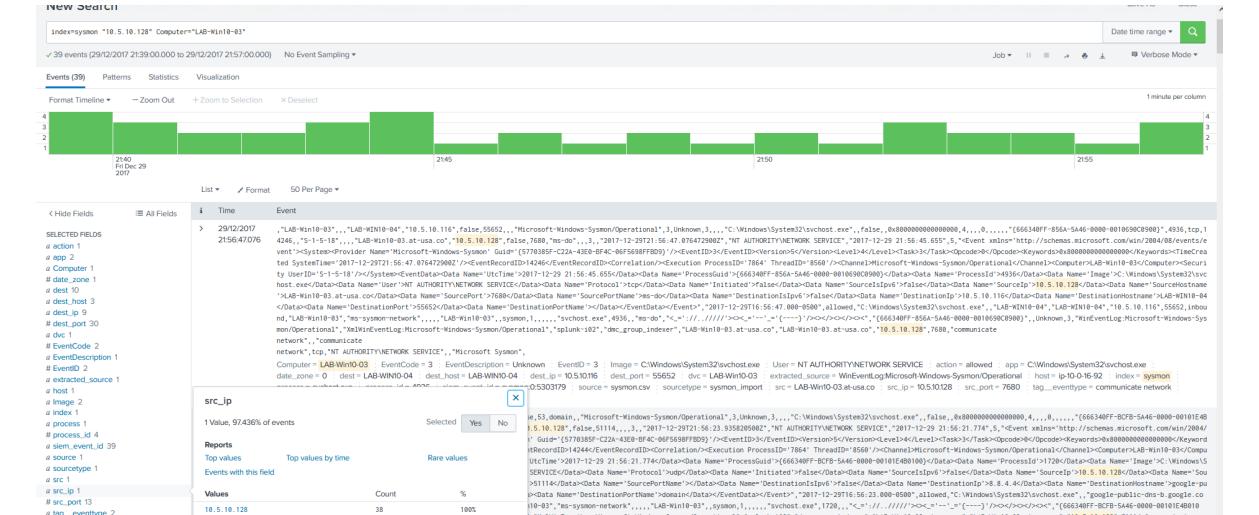
Investigate the three fields and identify the computer

Investigating 128...there are two possible computers...

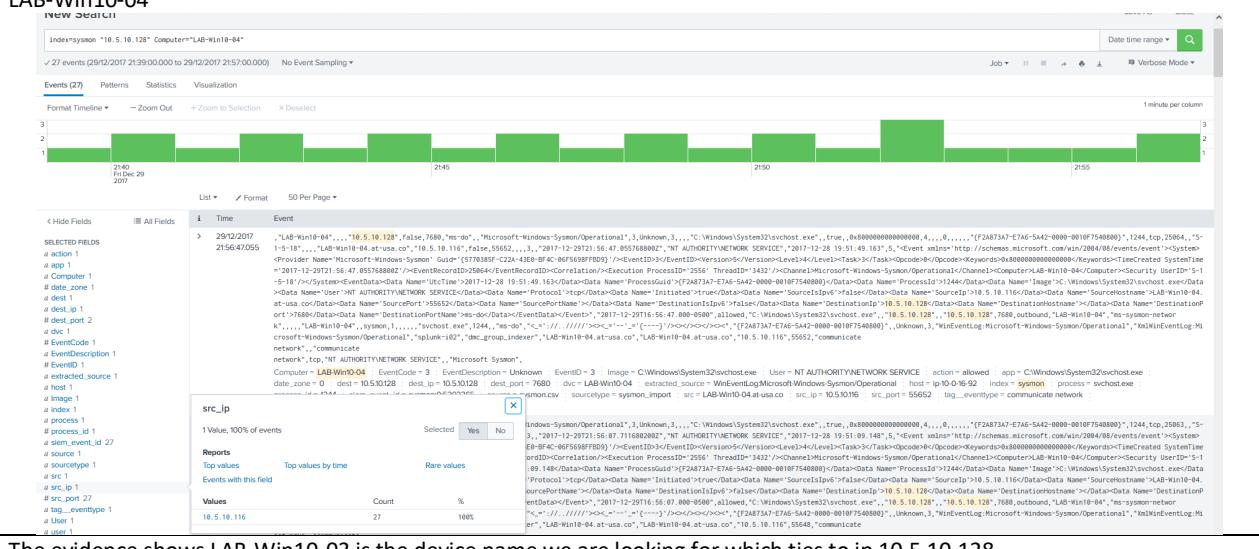
Click on each computer and then select scr_ip to see which computer identifies to which and then come back and select the one we're investigating.



LAB-Win10-03

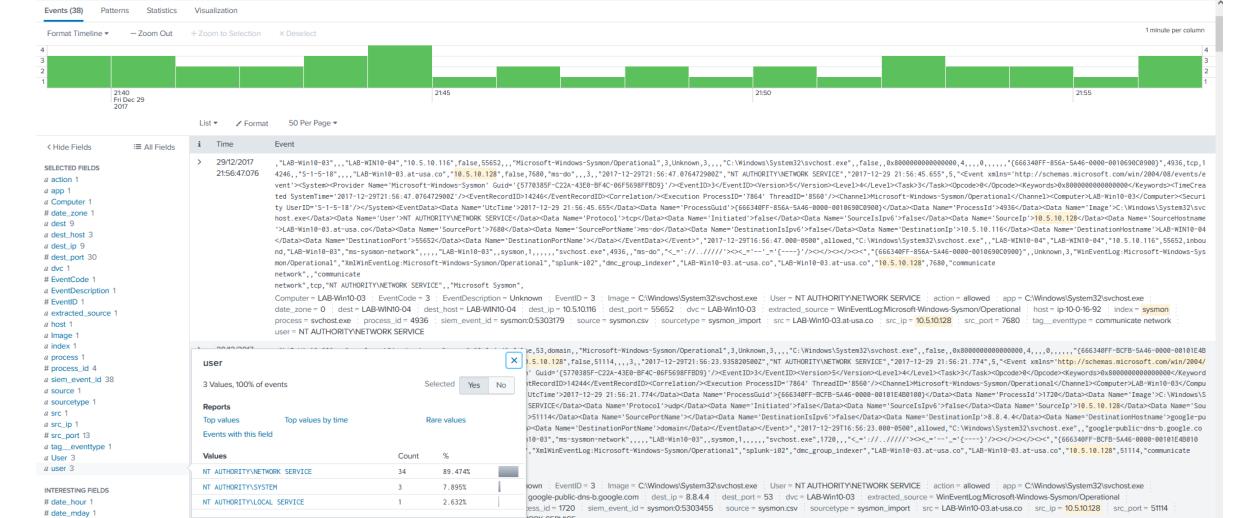


LAB-Win10-04



The evidence shows LAB-Win10-03 is the device name we are looking for which ties to ip 10.5.10.128.

User presents a problem which we will resolve later.

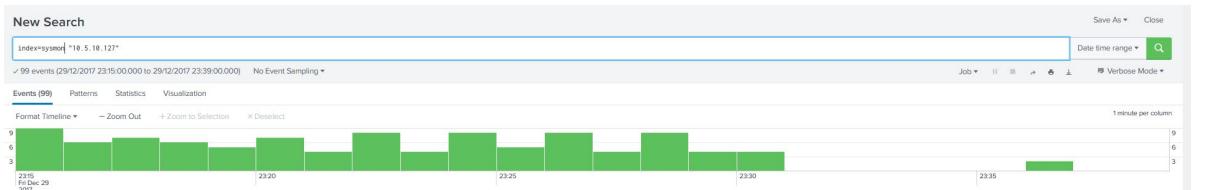


127

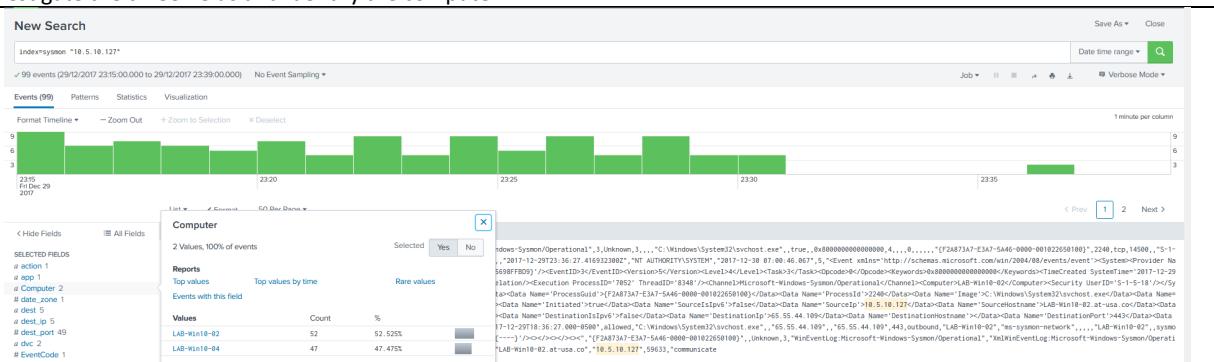
From



To

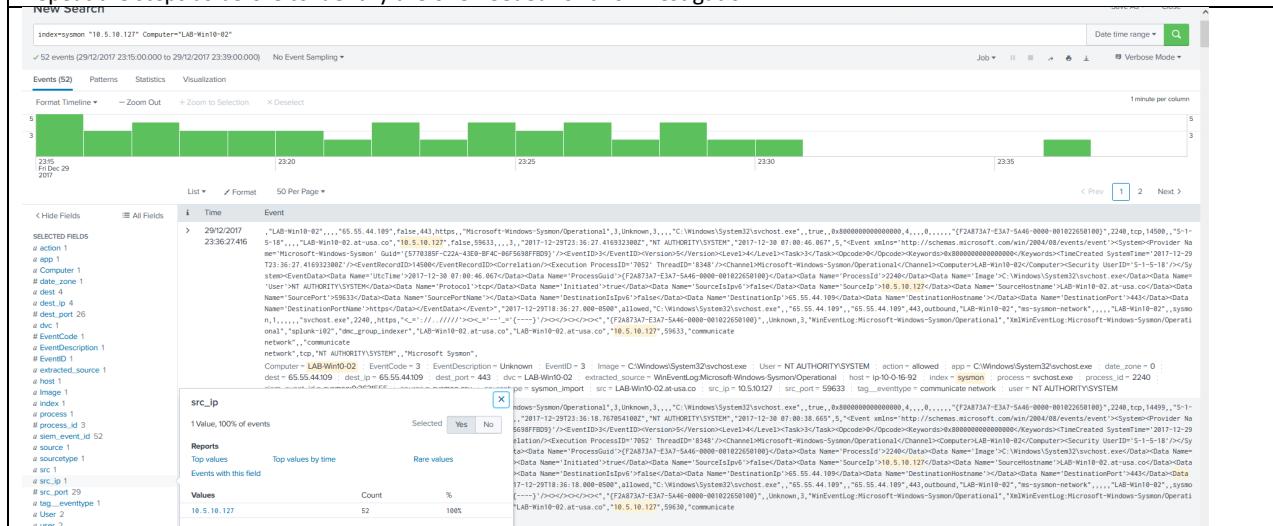


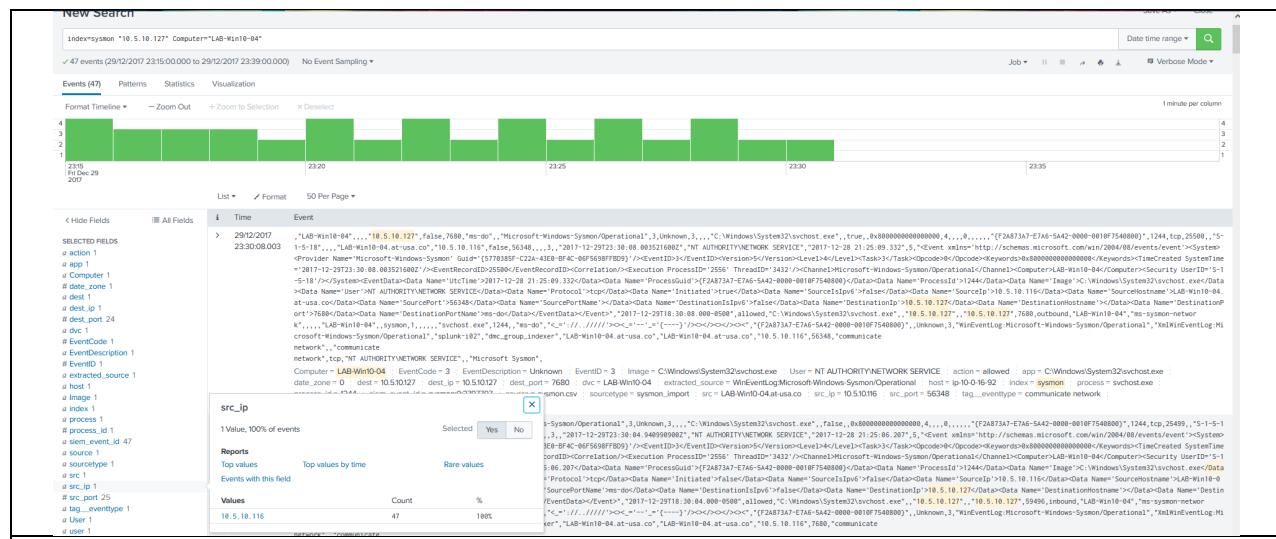
Investigate the three fields and identify the computer



As before this computer has two possibilities..

Repeat the steps as before to identify the one needed for this investigation





The evidence shows LAB-Win10-02 is the device name we are looking for which ties to ip 10.5.10.127.

User presents a problem which we will resolve later

With all four devices identified you need to use the computer Id and not the ip address to see all the proper Events. (This is not a network issue now but a host log search...)

10.5.10.129 - LAB-Win7-01 - S. Adams - 8 times

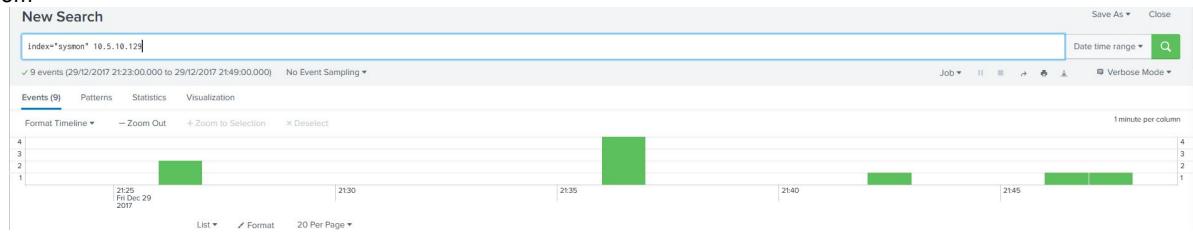
10.5.10.130 - Daniel-PC – Daniel - 5 times

10.5.10.128 - LAB-Win10-03 – M. Land - 2 times

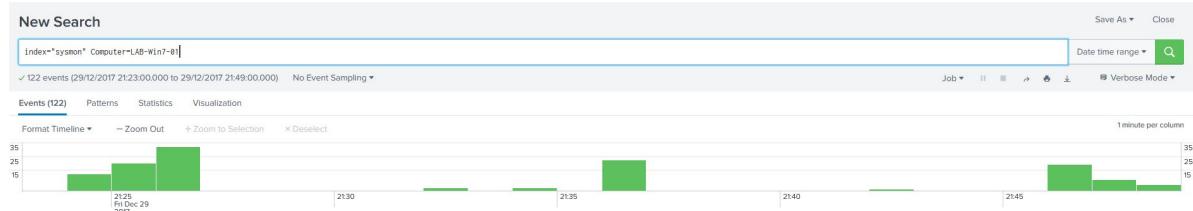
10.5.10.127 - LAB-Win10-02 – D. Walker - 1 time

Search 10.5.10.129 / LAB-Win7-01

From



To

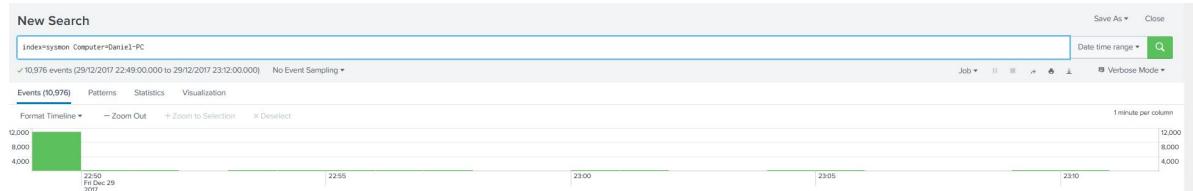


Search 10.5.10.130 / Daniel-PC

From



To

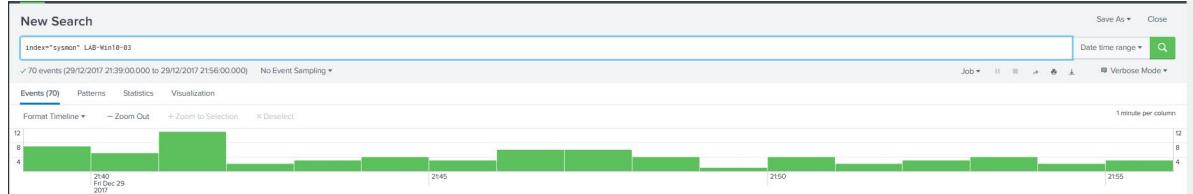


Search 10.5.10.128 / LAB-Win10-03

From

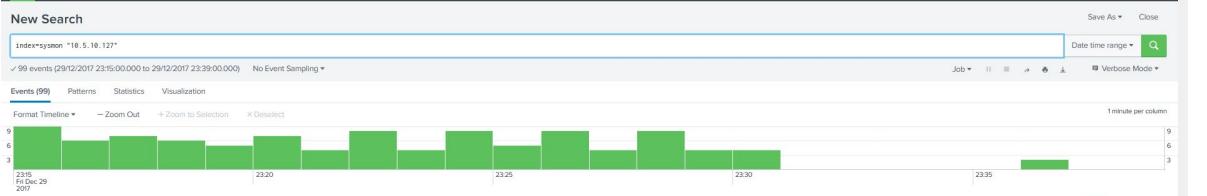


To

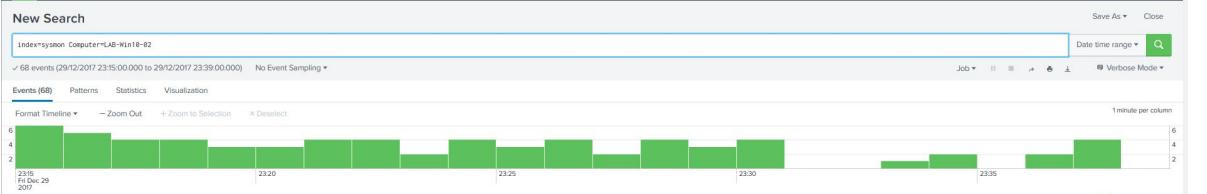


Search 10.5.10.127 / LAB-Win10-02

From



To



2 - IDENTIFYING EMAILS WITH TIMESTAMP

Investigate initial email recipient P. Brand

New Search

index="email" p.brand

✓ 32 events (29/12/2017 00:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling ▾

Events (32) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection × Deselect

1 hour per column

25
15
10
0

00:00 Fri Dec 29 2017 | 04:00 | 08:00 | 12:00 | 16:00 | 20:00

List ▾ Format 20 Per Page ▾

It is known that the email arrived at 15:58

```
> 29/12/2017 15:58:29 mail amavis[19130]: (19130-01) Passed CLEAN {RelayedInbound}, [127.0.0.1] <daniel@mail.at-usa.co> -> <p.brand@mail.at-usa.co>, Message-ID: <20171229205823.0FD25100231@mail.at-usa.co>, mail_id: f2f6g_UW6ar5I, Hits: 0.25, size: 804, queued_as: 4D013100242, 6217 ms, Tests: [HEADER_FROM_DIFFERENT_DOMAINS=0.25,NO_RELAYS=0.001,URIBL_BLOCKED=0.001]
date_zone = local | host = mail | index = email | process = amavis | siem_event_id = email:17383 | source = email.log | sourcetype = postfix_syslog

> 29/12/2017 15:58:29 mail postfix/smtpd[21122]: 0FD25100231: to=<p.brand@mail.usa.co>, relay=127.0.0.1[127.0.0.1]:10024, delay=6.3, delays=0.03/0.02/0.01/6.2, dsn=2.0.0, status=sent (250 2.0.0 from MTA(smt
p:[127.0.0.1]:10025): 250 2.0.0 Ok: queued as 4D013100242
date_zone = local | host = mail | index = email | process = postfix/amavis/smtp | siem_event_id = email:17373 | source = email.log | sourcetype = postfix_syslog | status = sent

> 29/12/2017 15:58:29 mail postfix/pipe[21140]: 4D013100242: to=<p.brand@mail.usa.co>, relay=dovecot, delay=0.04, delays=0.01/0.01/0.02, dsn=2.0.0, status=sent (delivered via dovecot service)
```

Notice the message ID

New Search

index="email" 20171229205823.0FD25100231@mail.at-usa.co

✓ 9 events (29/12/2017 00:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling ▾

Events (9) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection × Deselect

1 hour per column

25
15
10
0

00:00 Fri Dec 29 2017 | 04:00 | 08:00 | 12:00 | 16:00 | 20:00

List ▾ Format 20 Per Page ▾

Search the message ID to see which other devices it included

New Search

index="email" 20171229205823.0FD25100231@mail.at-usa.co

✓ 9 events (29/12/2017 00:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling ▾

Events (9) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection × Deselect

1 hour per column

25
15
10
0

00:00 Fri Dec 29 2017 | 04:00 | 08:00 | 12:00 | 16:00 | 20:00

List ▾ Format 50 Per Page ▾

It shows up in 9 events

i	Time	Event
>	29/12/2017 15:58:31	mail postfix/cleanup[21116]: D266910023F: message_id=<20171229205823.0FD25100231@mail.at-usa.co> date_zone = local host = mail index = email process = postfix/cleanup siem_event_id = email:17279 source = email.log sourcetype = postfix_syslog
>	29/12/2017 15:58:31	Dec 29 15:58:31 mail amavis[19129]: (19129-02) Passed CLEAN {RelayedInbound}, [127.0.0.1] <daniel@mail.at-usa.co> -> <s.adams@mail.usa.co>, Message-ID: <20171229205823.0FD25100231@mail.at-usa.co>, mail_id: kSpktxJbluW, Hits: 0.25, size: 804, queued_as: 4D6910023F, 8754 ms, Tests: [HEADER_FROM_DIFFERENT_DOMAINS=0.25,NO_RELAYS=0.001,URIBL_BLOCKED=0.001] date_zone = local host = mail index = email process = amavis siem_event_id = email:17255 source = email.log sourcetype = postfix_syslog
>	29/12/2017 15:58:30	Dec 29 15:58:30 mail postfix/cleanup[21116]: 4F7F110023F: message_id=<20171229205823.0FD25100231@mail.at-usa.co> date_zone = local host = mail index = email process = postfix/cleanup siem_event_id = email:17337 source = email.log sourcetype = postfix_syslog
>	29/12/2017 15:58:30	Dec 29 15:58:30 mail amavis[19131]: (19131-01) Passed CLEAN {RelayedInbound}, [127.0.0.1] <daniel@mail.at-usa.co> -> <d.walker@mail.usa.co>, Message-ID: <20171229205823.0FD25100231@mail.at-usa.co>, mail_id: NAHbfrsKzbGc, Hits: 0.25, size: 804, queued_as: 4F7F110023F, 7241 ms, Tests: [HEADER_FROM_DIFFERENT_DOMAINS=0.25,NO_RELAYS=0.001,URIBL_BLOCKED=0.001] date_zone = local host = mail index = email process = amavis siem_event_id = email:17373 source = email.log sourcetype = postfix_syslog
>	29/12/2017 15:58:29	Dec 29 15:58:29 mail postfix/cleanup[21116]: 45BA210023F: message_id=<20171229205823.0FD25100231@mail.at-usa.co> date_zone = local host = mail index = email process = postfix/cleanup siem_event_id = email:17454 source = email.log sourcetype = postfix_syslog
>	29/12/2017 15:58:29	Dec 29 15:58:29 mail amavis[19132]: (19132-01) Passed CLEAN {RelayedInbound}, [127.0.0.1] <daniel@mail.at-usa.co> -> <m.land@mail.usa.co>, Message-ID: <20171229205823.0FD25100231@mail.at-usa.co>, mail_id: z_r0DwxDqXU, Hits: 0.25, size: 804, queued_as: 45BA210023F, 6199 ms, Tests: [HEADER_FROM_DIFFERENT_DOMAINS=0.25,NO_RELAYS=0.001,URIBL_BLOCKED=0.001] date_zone = local host = mail index = email process = amavis siem_event_id = email:17430 source = email.log sourcetype = postfix_syslog
>	29/12/2017 15:58:29	Dec 29 15:58:29 mail postfix/cleanup[21116]: 4D013100242: message_id=<20171229205823.0FD25100231@mail.at-usa.co> date_zone = local host = mail index = email process = postfix/cleanup siem_event_id = email:17407 source = email.log sourcetype = postfix_syslog
>	29/12/2017 15:58:29	Dec 29 15:58:29 mail amavis[19130]: (19130-01) Passed CLEAN {RelayedInbound}, [127.0.0.1] <daniel@mail.at-usa.co> -> <p.brand@mail.usa.co>, Message-ID: <20171229205823.0FD25100231@mail.at-usa.co>, mail_id: f2fg_UW6ar5I, Hits: 0.25, size: 804, queued_as: 4D013100242, 6217 ms, Tests: [HEADER_FROM_DIFFERENT_DOMAINS=0.25,NO_RELAYS=0.001,URIBL_BLOCKED=0.001] date_zone = local host = mail index = email process = amavis siem_event_id = email:17383 source = email.log sourcetype = postfix_syslog
>	29/12/2017 15:58:23	Dec 29 15:58:23 mail postfix/cleanup[21116]: 0FD25100231: message_id=<20171229205823.0FD25100231@mail.at-usa.co> date_zone = local host = mail index = email process = postfix/cleanup siem_event_id = email:17473 source = email.log sourcetype = postfix_syslog

It appears to be a spoof email from daniel@mail.at-usa.co and fired off to other colleagues.

s.adams@mail.usa.co

d.walker@mail.usa.co

m.land@mail.usa.co

p.brand@mail.usa.co

It shows there were 4 recipients...it was derived by using the message id

3 - EVENT ID 11: FILE CREATE

An EK (Exploit Kit) is to distribute Malware (delivering a payload, creating a file) on a device.
Investigate Sysmon ID's

We're looking for something that creates files

Event ID 11: FileCreate

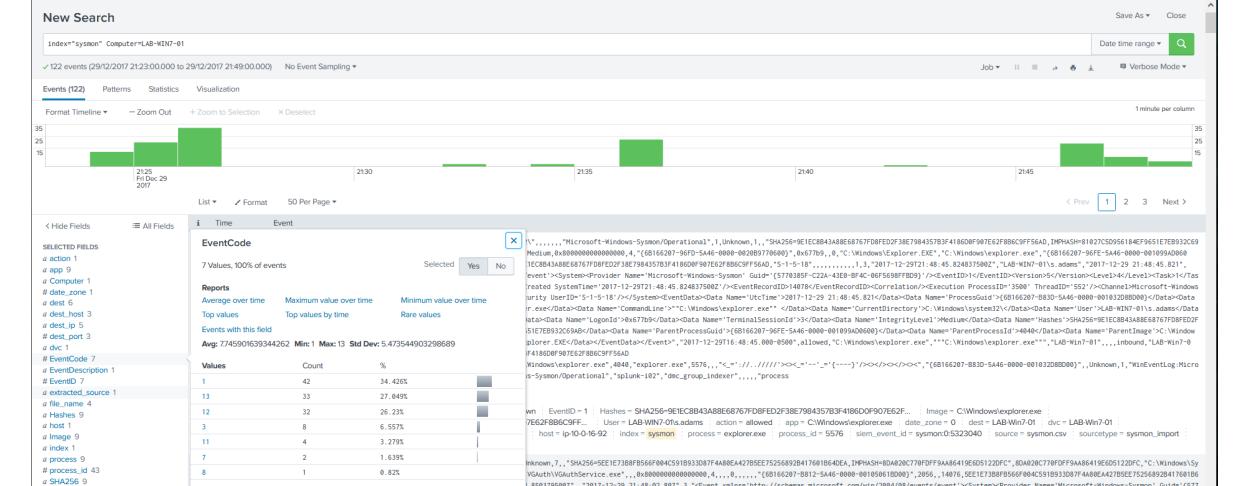
File create operations are logged when a file is created or overwritten. This event is useful for monitoring autostart locations, like the Startup folder, as well as temporary and download directories, which are common places malware drops during initial infection.

Investigate EventCode or EventID (they represent the same thing).

Select Event Code / ID 11 (File Create)

File create operations are logged when a file is created or overwritten. This event is useful for monitoring AutoStart locations, like the Startup folder, as well as temporary and download directories, which are common places malware drops during initial infection.

LAB-Win7-01



Select Event ID 11



With the Event ID 11 there are now a total of 4 events

Investigate the individual logs

Select the drop-down arrow for each log and investigate findings / fields listed

Event Log 1 21:46:21.166

A suspicious file name is evident (Bilo467.exe)

This is hidden data...this is the type of spurious location to look for when hunting a EK file

Event Log 2

A suspicious file name is evident (Bilo161.exe)

Event Log 3

Event Actions ▾		Actions ▾
Type	Field	Value
Selected ✓	Computer	LAB-Win7-01
✓	EventCode	11
✓	EventDescription	Unknown
✓	EventID	11
✓	Image	C:\Windows\system32\wscript.exe
✓	action	allowed
✓	app	C:\Windows\system32\wscript.exe
✓	date_zone	0
✓	dest	LAB-Win7-01
✓	dvc	LAB-Win7-01
✓	extracted_source	WinEventLog:Microsoft-Windows-Sysmon/Operational
✓	file_name	bld0494.exe
✓	host	ip-10-0-16-92
✓	index	sysmon
endpoint		"Microsoft Sysmon",

A suspicious file name is evident (Bilo439.exe)

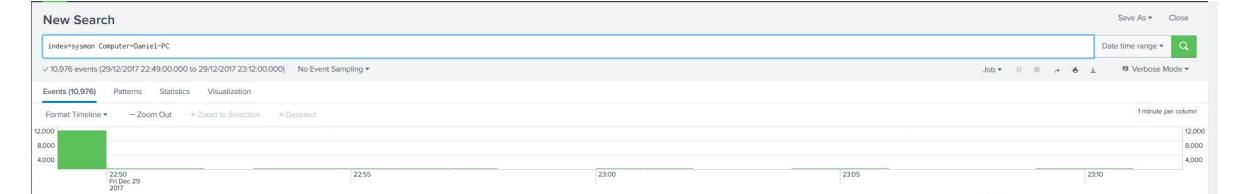
Now investigate the remaining computers for similar file names

10.5.10.130 - Daniel-PC – Daniel

10.5.10.128 - LAB-Win10-03 – M. Land

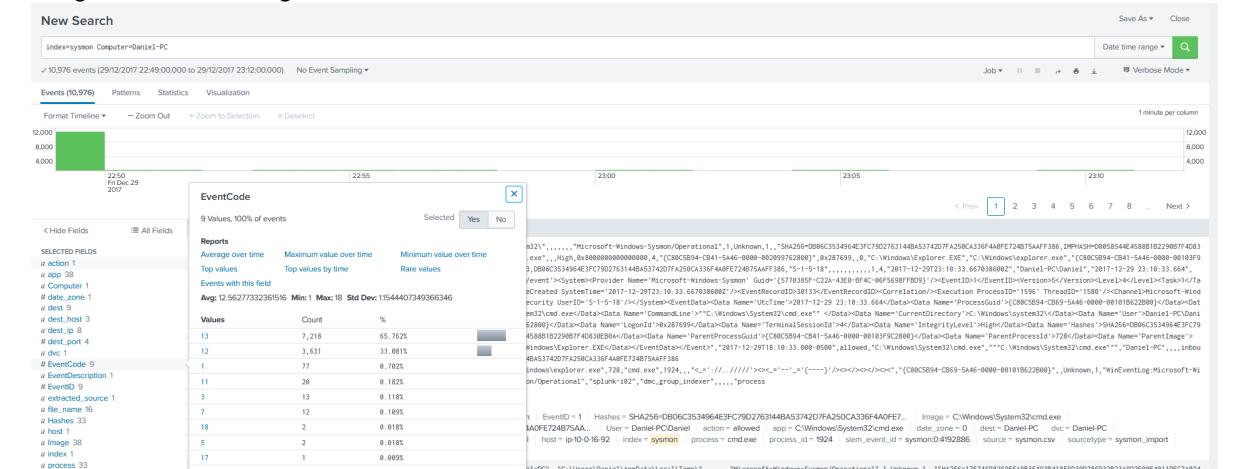
10.5.10.127 - LAB-Win10-02 – D. Walker

Daniel-PC



Event Code 11 has a total of 20 events

Investigate the individual logs



Select the Code and investigate each drop-down Event Log as before drop-down arrow for each log and investigate findings / fields listed



Investigate each event log for anything suspicious. (see below as examples)

Event Logs 1 and 2 show nothing suspicious

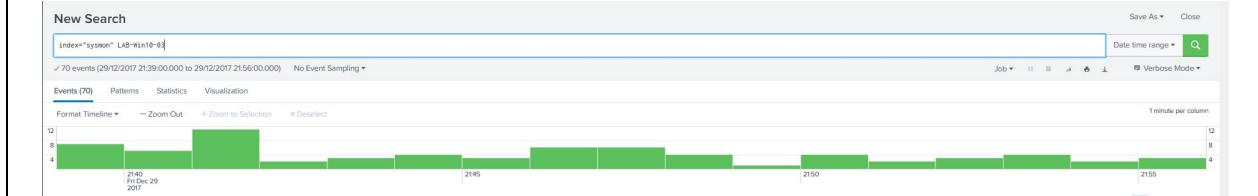
Event Log 3 has a suspicious file name



Event Log 4 has a suspicious file name

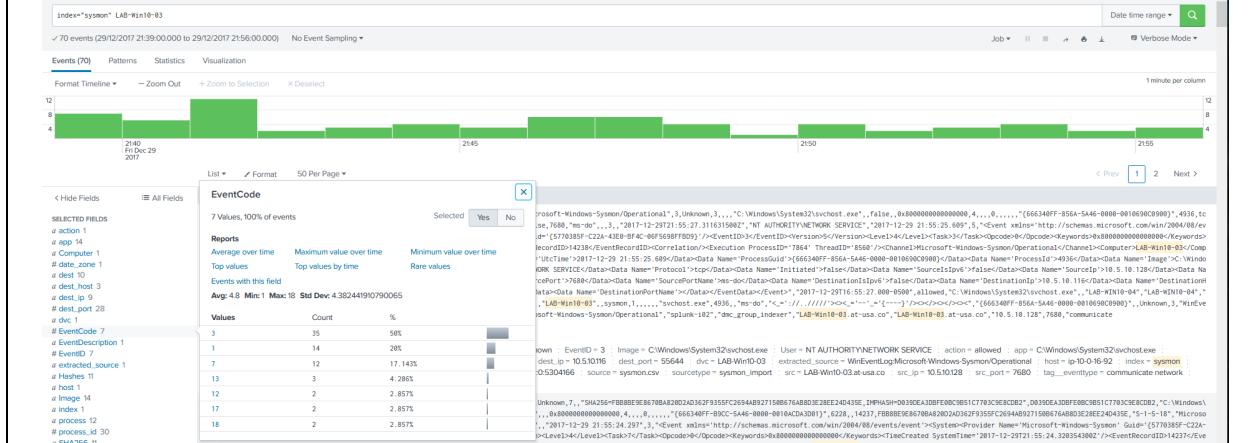


LAB-Win10-03



Event Code

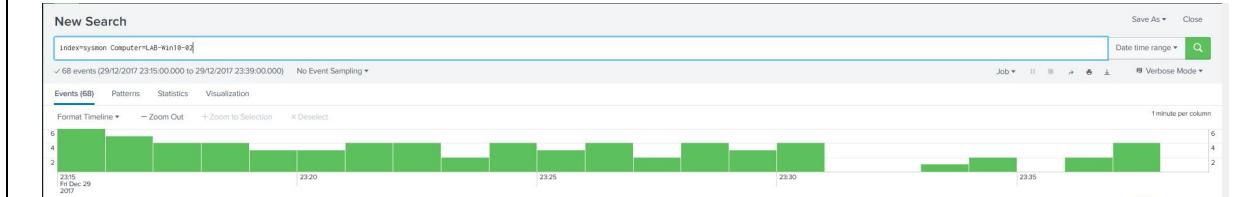
[New search](#)



There isn't an Event Code 11 on this device...

There were no files created on this device...

LAB-Win10-02



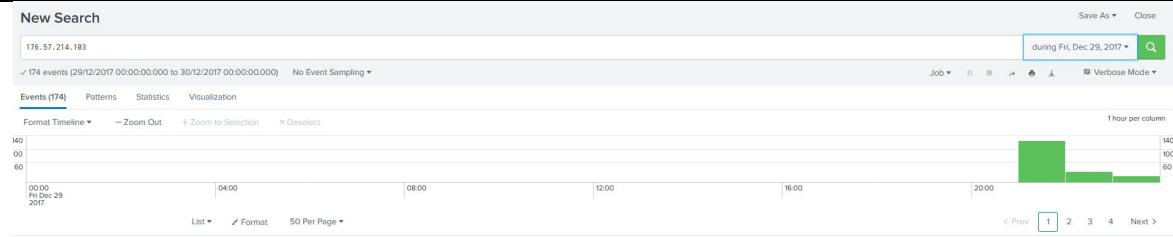
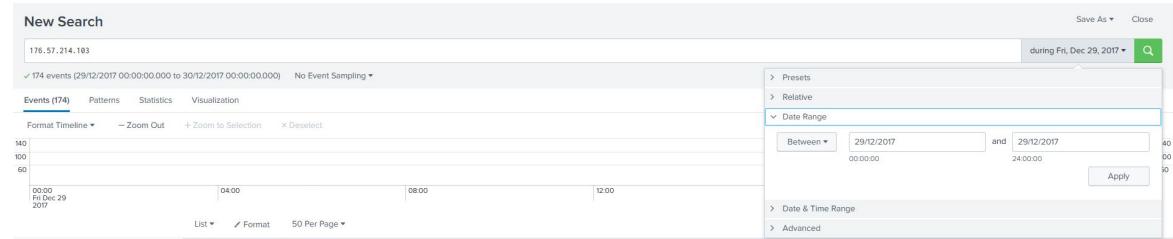
Event Code

There isn't an Event Code 11 on this device...
There were no files created on this device...

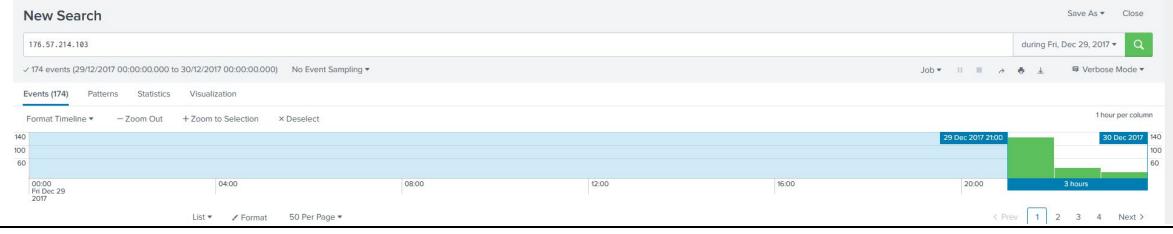
4 - TIME RANGES

The time range during which any AT-USA devices were exposed to the threat associated with ciso[.]guide (the EK landing page)

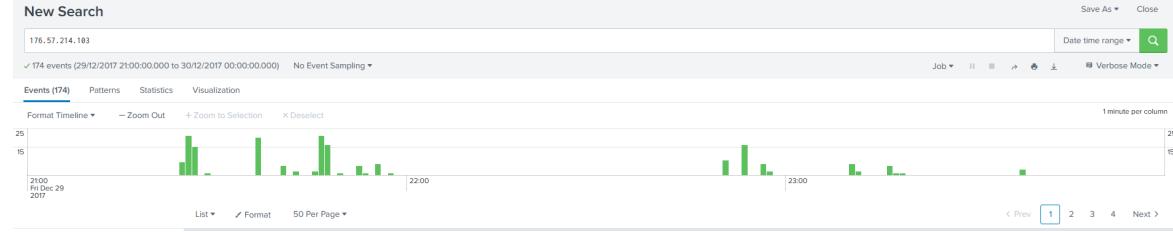
Set the time range set to the day of the attack and the ip address of the EK server



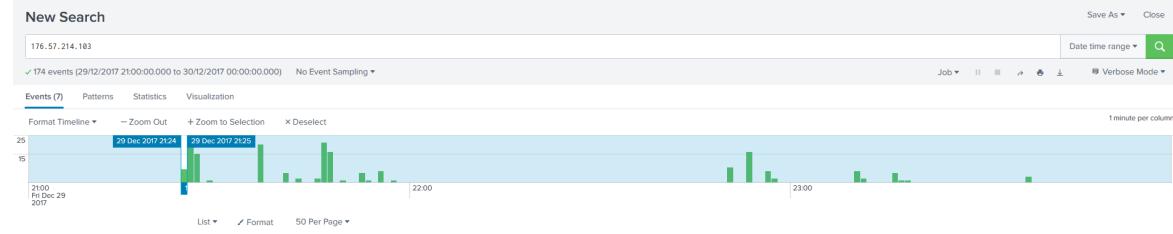
Zoom into the events shown to see all the traffic that any AT-USA device interacted with the EK server



You now have a broad time range when all the activity took place



Zoom into the first and last events shown to get your full-time range of the EK events, then you can single out each device to establish each own time stamps.



New Search

176.57.214.183

✓ 7 events (29/12/2017 21:24:00.000 to 29/12/2017 21:25:00.000) No Event Sampling

Events (4) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection X Deselect

29 Dec 2017 21:24:23 29 Dec 2017 21:24:24

1 second per column

4
3
2
1

21:24:00 21:24:10 21:24:20 21:24:30 21:24:40 21:24:50

List ▾ Format 50 Per Page ▾

Hide Fields All Fields Time Event

First event took place at 21:24:23.000

Repeat the process with the last event shown...

New Search

176.57.214.183

✓ 174 events (29/12/2017 21:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling

Events (3) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection X Deselect

29 Dec 2017 23:37:25 29 Dec 2017 23:38:00

1 minute per column

25
15

21:00 Fri Dec 29 2017

List ▾ Format 50 Per Page ▾

Search Datasets Reports Alerts Dashboards

Search & Reporting

New Search

176.57.214.183

✓ 3 events (29/12/2017 23:37:00.000 to 29/12/2017 23:38:00.000) No Event Sampling

Events (1) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection X Deselect

29 Dec 2017 23:37:11 29 Dec 2017 23:37:18

1 second per column

2
1

23:37:00 23:37:10 23:37:20 23:37:30 23:37:40 23:37:50

List ▾ Format 50 Per Page ▾

Selected Fields

a action 1
a app 1

> 23/12/2017 23:37:17 10.6.98.1 Dec 29 2017 18:37:17: ASA-6-382014: Teardown TCP connection 246315 for outside:176.57.214.183/88 to LAB-Workstations:10.5.10.127/59648 duration 0:00:13 bytes 0 TCP FINs
action = teardown app = AAA date_zone = 300 dest = 10.5.10.127 dest_ip = 10.5.10.127 dest_port = 59648 dvc = 10.6.90.1 host = ip-10-6-92 index = cisco siem_event_id = cisco01423523 source = cisco.fog sourcetype = cisco029a src = 176.57.214.103 src_ip = 176.57.214.103 src_port = 80

The last EK event took place at 23:37:17.000

Now search each device's interactions with the EK server

ip=10.5.10.129

New Search

176.57.214.183 10.5.10.129

✓ 85 events (29/12/2017 21:00:00.000 to 29/12/2017 22:00:00.000) No Event Sampling

Events (85) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection X Deselect

21:00 21:10 21:20 21:30 21:40 21:50

1 minute per column

18
12
6

21:00 Fri Dec 29 2017

New Search

176.57.214.183 10.5.10.129

✓ 85 events (29/12/2017 21:00:00.000 to 29/12/2017 22:00:00.000) No Event Sampling

Events (7) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection X Deselect

29 Dec 2017 21:24 29 Dec 2017 21:25

1 minute per column

18
12
6

21:00 Fri Dec 29 2017

New Search

176.57.214.183 10.5.10.129

✓ 85 events (29/12/2017 21:00:00.000 to 29/12/2017 22:00:00.000) No Event Sampling

Events (1) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection X Deselect

29 Dec 2017 21:49 29 Dec 2017 21:50

1 minute per column

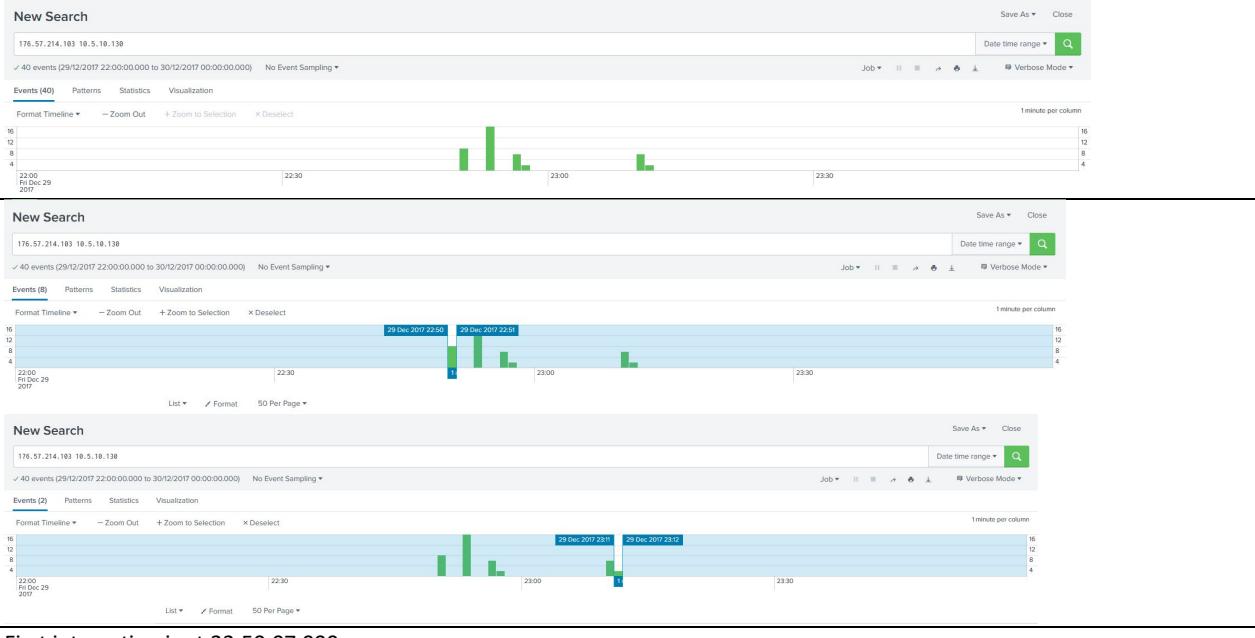
18
12
6

21:00 Fri Dec 29 2017

First interaction is at 21:24:23.000

Last interaction is at 21:49:14.000

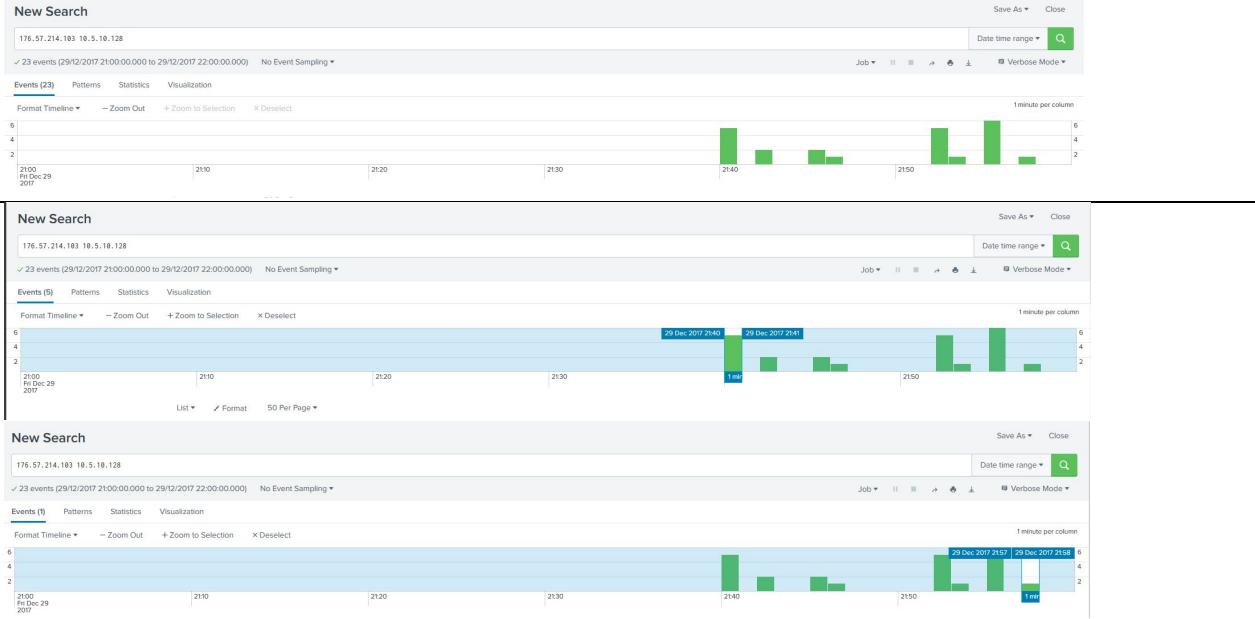
ip=10.5.10.130



First interaction is at 22:50:07.000

Last interaction is at 23:11:16.000

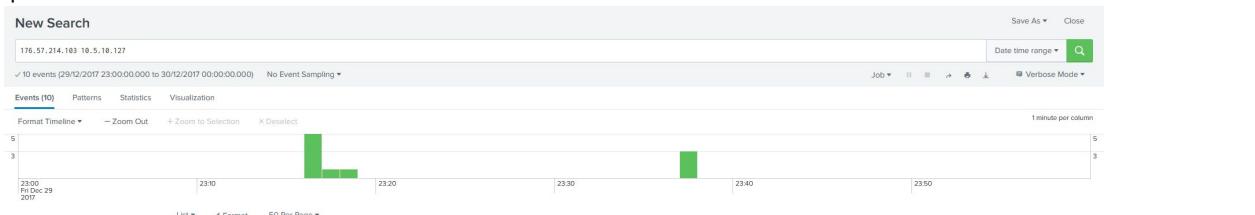
ip=10.5.10.128

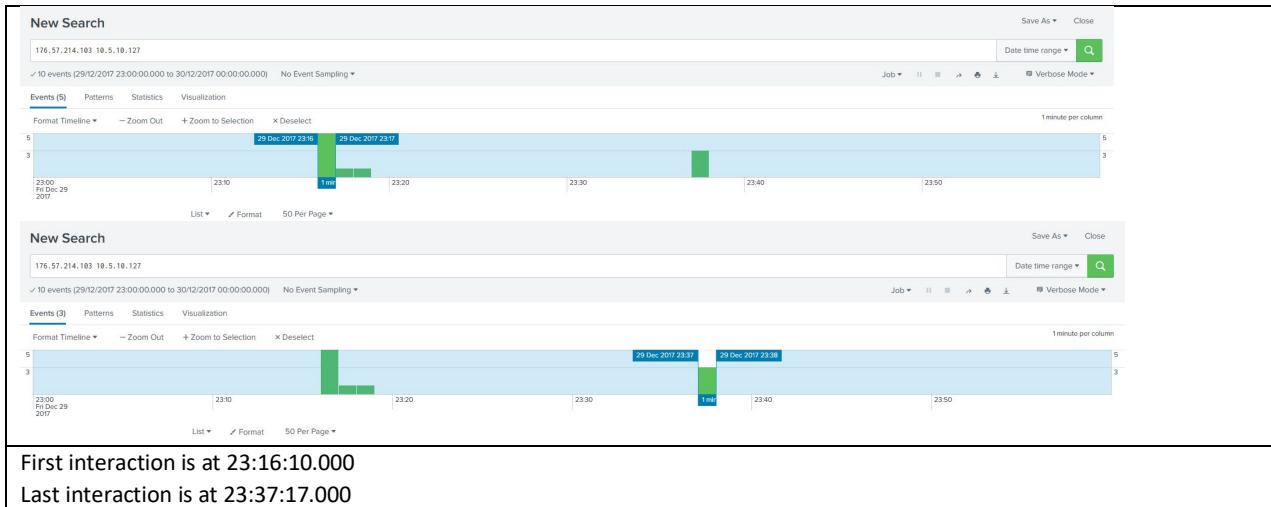


First interaction is at 21:40:33.000

Last interaction is at 21:57:06.000

ip=10.5.10.127



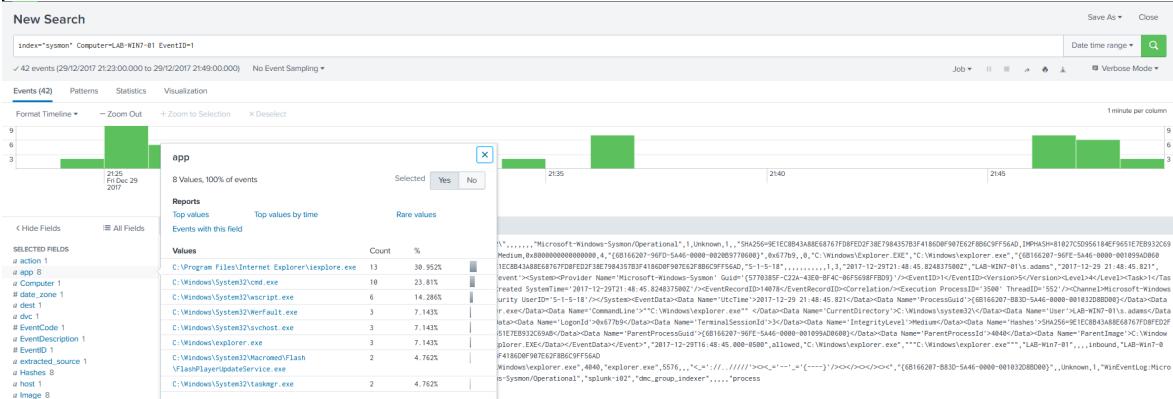
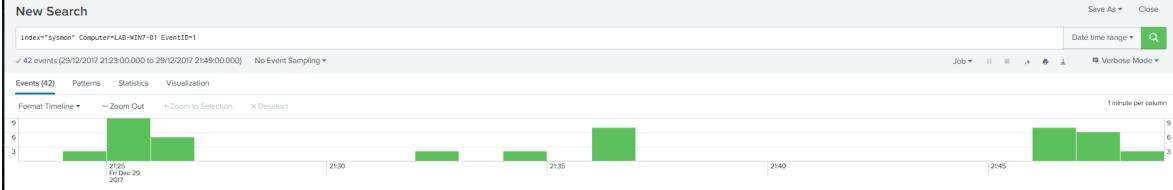
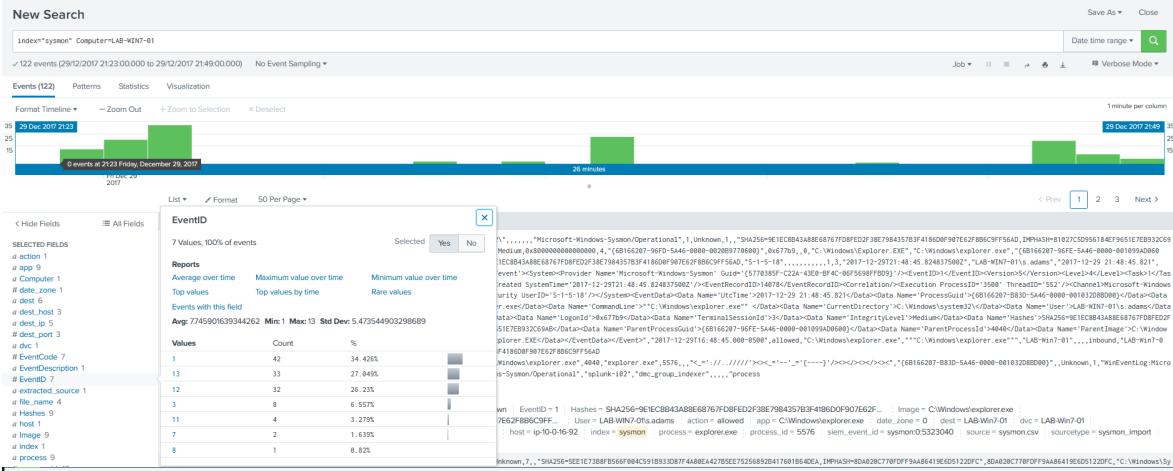
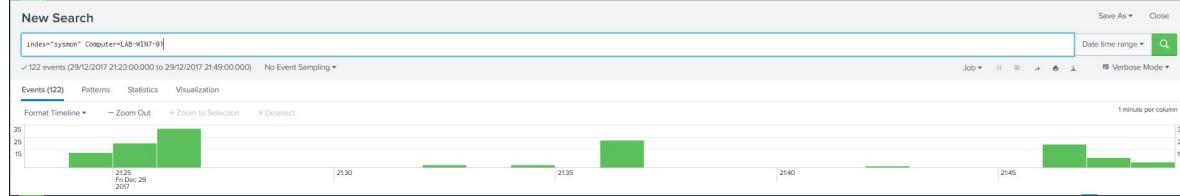


5 - EVENT ID 1 – PROCESS CREATION

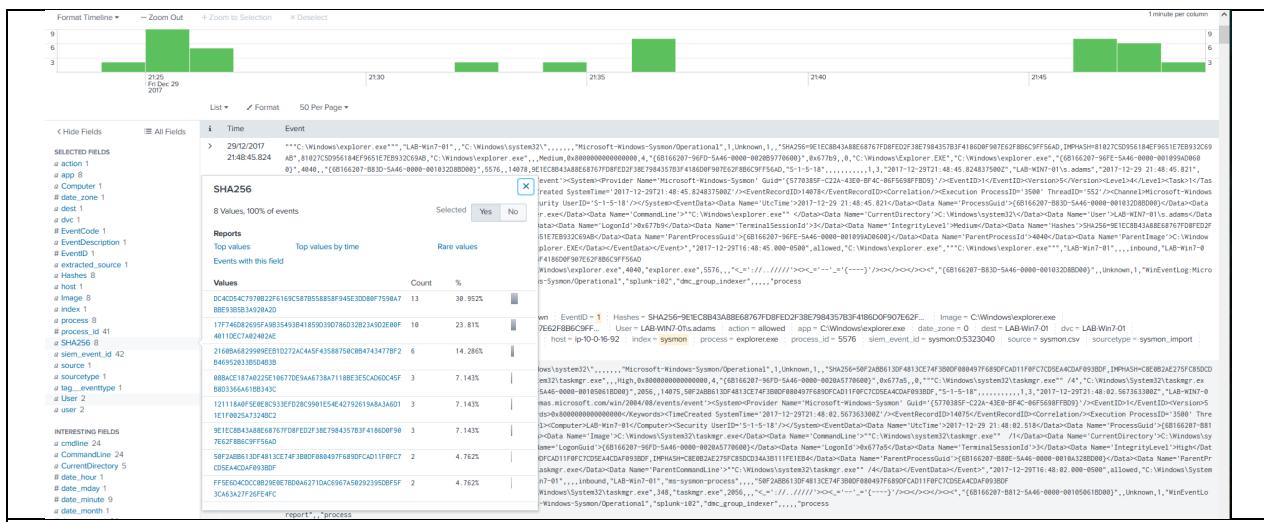
Event ID 1: Process creation

The process creation event provides extended information about a newly created process. The full command line provides context on the process execution. The `ProcessGUID` field is a unique value for this process across a domain to make event correlation easier. The hash is a full hash of the file with the algorithms in the `HashType` field.

LAB-Win7-01



There are no bilo files in the app field, so it appears that no bilo files were executed on this device...but not definitive yet... To help confirm there is a SHA256 / Hashes that can be searched...



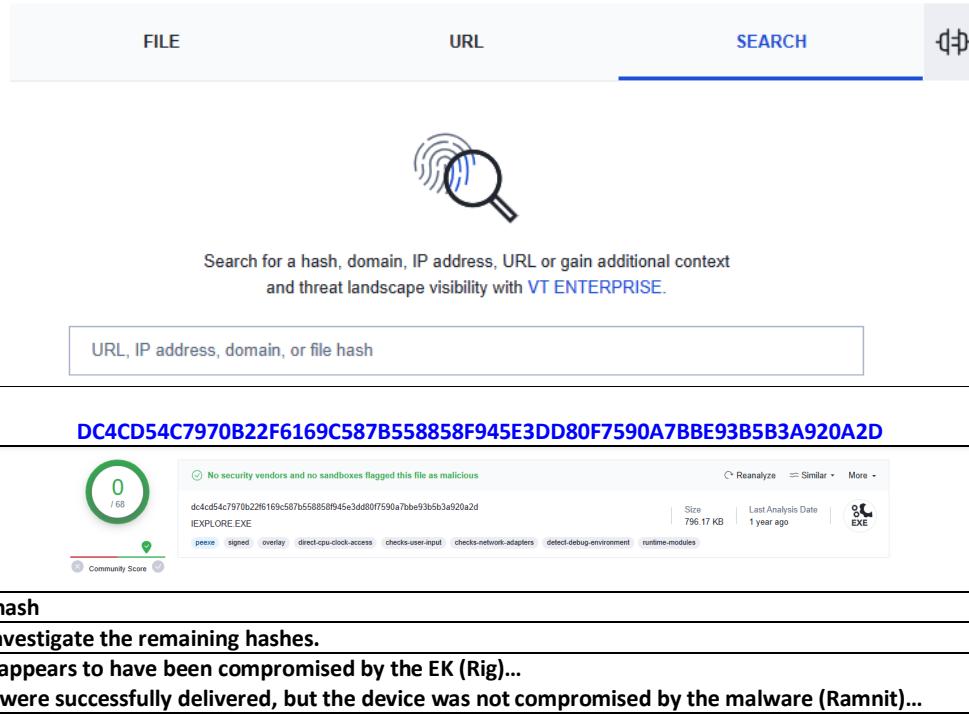
DC4CD54C7970B22F6169C587B558858F945E3DD80F7590A7BBE93B5B3A920A2D

Go to Virus Total and search the different SHA256's / Hashes



VIRUSTOTAL

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.



When trying to search in the current timeline on Daniel-PC there doesn't appear to be any events associated with bilo...so expand the search to the whole day and to all event 1 with bilo...

The screenshot displays four separate screenshots of the Microsoft Windows Event Viewer interface, showing different search results for the term "bilo".

- Top Screenshot:** Shows a search for "index=ssys Computer=Daniel-PC EventID=1". It finds 77 events between 22:49:00.0000 to 29/12/2017 23:12:00.0000. The visualization shows a histogram with a single bar at 22:50 on Dec 29, 2017, with a count of 2250. The details pane shows a list of events, with the first few entries being:
 - C:\Windows\System32\cmd.exe
 - C:\Windows\System32\wscript.exe
 - C:\Windows\System32\cmd.exe
 - C:\Windows\System32\cmd.exe
 - C:\Windows\System32\cmd.exe
- Second Screenshot:** Shows a search for "index=ssys Computer=Daniel-PC EventID=1" expanded to the entire day (29/12/2017). It finds 397 events between 00:00:00.0000 to 30/12/2017 00:00:00.0000. The visualization shows a histogram with bars at 00:00, 04:00, 08:00, 12:00, 16:00, and 20:00, with counts of approximately 300, 200, 100, 100, 100, and 100 respectively.
- Third Screenshot:** Shows a search for "index=ssys EventID=1 bilo>". It finds 17 events between 29/12/2017 00:00:00.0000 to 30/12/2017 00:00:00.0000. The visualization shows a histogram with a single bar at 00:00 on Dec 29, 2017, with a count of 16. The details pane shows a list of events, with the first few entries being:
 - C:\Windows\System32\cmd.exe
 - C:\Windows\System32\wscript.exe
 - C:\Windows\System32\cmd.exe
 - C:\Windows\System32\cmd.exe
- Bottom Screenshot:** Shows a search for "index=ssys EventID=1 bilo+app". It finds 17 events between 29/12/2017 00:00:00.0000 to 30/12/2017 00:00:00.0000. The visualization shows a histogram with a single bar at 00:00 on Dec 29, 2017, with a count of 16. The details pane shows a list of events, with the first few entries being:
 - C:\Windows\System32\cmd.exe
 - C:\Windows\System32\wscript.exe
 - C:\Windows\System32\cmd.exe

Select the appropriate app and add to search

app

3 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
C:\Windows\System32\cmd.exe	10	58.824%
C:\Windows\System32\wscript.exe	6	35.294%
C:\Users\Daniel\AppData\Local\Temp\bilo400.exe	1	5.882%

New Search

Index=system EventID=1 bilo app="C:\Users\Daniel\AppData\Local\Temp\bilo400.exe"

1 event (29/12/2017 00:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection X Deselect

00:00 Fri Dec 29 2017 04:00 08:00 12:00 16:00 20:00

Now investigate the SHA256 / Hashes

New Search

Index=system EventID=1 bilo app="C:\Users\Daniel\AppData\Local\Temp\bilo400.exe"

1 event (29/12/2017 00:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection X Deselect

00:00 Fri Dec 29 2017 04:00 08:00 12:00 16:00 20:00

List ▾ Format 50 Per Page ▾

< Hide Fields All Fields

SLECTED FIELDS

- action 1
- app 1
- computer 1
- date_zone 1
- dest 1
- dvc 1
- eventCode 1
- EventIDDescription 1
- EventID 1
- extracted_source 1
- Hashes 1
- Image 1
- index 1
- process 1
- process_id 1
- process_name 1
- siem_event_id 1
- source 1
- sourceType 1
- tag_eventtype 1
- user 1

SHA256

1 Value, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
8875F1B2F8CDA139402559067160B493C8F9440ECB19343FB24	1	100%
A58011F		

EventID = 1 Hashes = SHA256-0875FB2F8CDA139402559067160B493C8F9440ECB19343FB24 – Image = C:\Users\Daniel\AppData\Local\Temp\bilo400.exe
9343FB24A5B – User = Daniel-PC\Daniel – action = allowed – app = C:\Users\Daniel\AppData\Local\Temp\bilo400.exe – date_zone = 0 – dvc = Daniel-PC – host = ip-10-0-16-92 – index = symon – process = bilo400.exe – process_id = 2148 – siem_event_id = symon:0:4196569 – source = symon.csv – sourcetype = symon_import

VIRUSTOTAL

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE URL SEARCH 

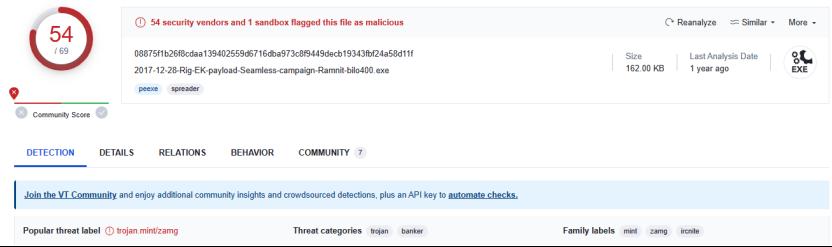


Search for a hash, domain, IP address, URL or gain additional context and threat landscape visibility with [VT ENTERPRISE](#).

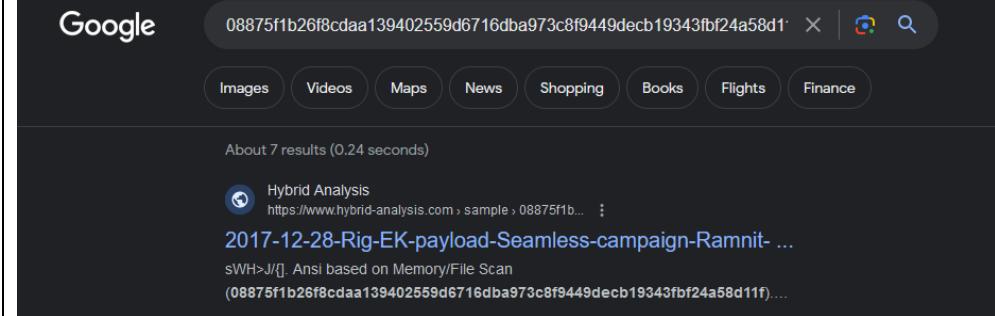
08875f1b26f8cdAA139402559d6716dba973c8f9449decb19343fb24a58d11f

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#).

Want to automate submissions? [Check our API](#), or access your [API key](#).


 A detailed analysis card for the file hash 08875f1b26f8cdAA139402559d6716dba973c8f9449decb19343fb24a58d11f. It shows a red circular 'Community Score' of 54/69. Below it, a message says "54 security vendors and 1 sandbox flagged this file as malicious". The file name is 2017-12-28-Rig-EK-payload-Seamless-campaign-Ramnit-bilo400.exe. It has a size of 162.00 KB and was last analyzed 1 year ago. The file type is EXE. Below the card are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. The COMMUNITY tab is active, showing a link to "Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks." Below the tabs are labels: Popular threat label: trojan/mal/zang, Threat categories: trojan/banker, Family labels: mal/zang/ircbot.

The bilo files are payloads
The threat cagatories are trojan and banker
Perform a google search for the hash...
08875f1b26f8cdAA139402559d6716dba973c8f9449decb19343fb24a58d11f


 A screenshot of a Google search results page for the hash 08875f1b26f8cdAA139402559d6716dba973c8f9449decb19343fb24a58d11f. The search bar shows the query. Below the search bar are links for Images, Videos, Maps, News, Shopping, Books, Flights, and Finance. The main search results area shows a hybrid analysis result from https://www.hybrid-analysis.com with the title "2017-12-28-Rig-EK-payload-Seamless-campaign-Ramnit-...". Below this, there is a note about memory/file scan results: "sWH>J[. Ansi based on Memory/File Scan (08875f1b26f8cdAA139402559d6716dba973c8f9449decb19343fb24a58d11f)...".

HYBRID ANALYSIS

2017-12-28-Rig-EK-payload-Seamless-campaign-Ramnit-bilo400.exe

This report is generated from a file or URL submitted to this webservice on December 29th 2017 05:58:56 (UTC). Report generated by Falcon Sandbox v7.20 © Hybrid Analysis

Additional Context

OSINT

External References: <http://www.malware-traffic-analysis.net/2017/12/28/index.html>
External User Tags: #ramnit #trojan

Indicators

Not all malicious and suspicious indicators are displayed. Get your own cloud service or the full version to view all details.

Malicious Indicators

External Systems

malicious Threat Score: 86/100 AV Detection: 84% Labeled as: F-Secure 2017-12-28-124143

File Details

Extracted Strings
Extracted File (0)
Notifications
Community (0)

Back to top

Latest News

Welcome to the Adversary Universe
Podcast: Unmasking the Threat Actors
Targeting Your Organization
Recent News - May 16, 2018

How CrowdStrike Uses Similarity-Based Mapping to Understand Cybersecurity Data and Prevent Adversaries

Leveraging the Dark Side How CrowdStrike Boosts Machine Learning Efficacy Against Adversaries

Denis Rozenboim - May 16, 2018

See More

Google Ramnit

About 311,000 results (0.32 seconds)

F-Secure https://www.f-secure.com/v-descs/virus-w32-ramnit

Ramnit | F-Secure Labs

The Ramnit family of harmful programs has numerous variants, which may individually be categorized as trojans, viruses or worms. The first Ramnit variants ...

Check Point Software https://www.checkpoint.com/.../What is Malware? Ramnit Malware

Ramnit is a banking trojan that was first discovered in 2010. It is one of the top 5 banking trojans worldwide but is especially prevalent in the APAC ...

How the Malware Works

Ramnit is a banking trojan, meaning that it is primarily intended to steal account credentials for online banking. However, like many banking trojans, Ramnit is designed to be highly modular, enabling it to collect additional types of credentials such as those for social media, email, and other accounts or to download and deploy other malware.

Ramnit is often spread via phishing campaigns that may deploy multi-stage malware. Once the target falls for the initial phishing campaign and runs the malware, it downloads and executes additional malware that eventually launches the Ramnit trojan. Ramnit will then attempt to collect banking credentials and may download additional Ramnit modules or other malware to achieve the attacker's goals.

One of the distinguishing features of the Ramnit malware is the use of both hardcoded domains and a domain generation algorithm (DGA) for command and control. Malware using a DGA generates a sequence of random-looking domains to which it sends command and control traffic. The attacker's command and control server runs the same DGA and registers these domains, directing the traffic to the attacker-controlled system. By using a DGA, the malware can avoid DNS blocklists because it is constantly using new, unblocked domains for its traffic.

The Threat

Since Ramnit is a modular banking trojan, the primary threat of the malware is the loss of an individual's login credentials for online banking, which may result in the theft of funds or the user's identity.

However, the Ramnit malware also can deploy additional modules or be used as a delivery vector for other malware variants. This means that the impact of a Ramnit infection depends on the details of the attack campaign and the malicious functionality that is successfully executed on the infected device.

Target Industries

Ramnit is primarily a banking trojan, meaning that its purpose is to steal login credentials for online banking, which cybercriminals can sell or use in future attacks. For this reason, Ramnit primarily targets individuals rather than focusing on particular industries.

Ramnit campaigns have been observed to target organizations in particular industries. For example, a 2019 campaign targeted financial organizations in the United Kingdom, Italy, and Canada.



How to Protect Against Ramnit Malware

Some best practices for protecting against the Ramnit banking trojan include:

- **Anti-Phishing Protection:** Ramnit malware is usually delivered as a malicious attachment to a phishing email, often via a downloader. Anti-phishing protections can help to identify and block or sanitize this malicious content, preventing the malware from reaching the user's device.
- **Endpoint Security Solutions:** Ramnit is an established malware variant with well-known behaviors and features. An endpoint security solution provides an organization or individual with the ability to detect Ramnit infections and prevent them from stealing credentials or deploying additional malware.
- **Cybersecurity Awareness Training:** Ramnit is commonly deployed via phishing emails, relying on deception to trick the user into executing the malicious functionality. Training employees to recognize and properly respond to phishing attacks can help prevent Ramnit infections.
- **DNS Traffic Analysis:** Ramnit malware often uses a DGA, which generates a series of random domains for command and control communications. Analysis of domain name lookups on a DNS server can enable an organization to identify the suspicious domain names that may indicate a Ramnit infection.
- **Multi-Factor Authentication (MFA):** Implementing MFA makes it more difficult for an attacker to make use of these stolen credentials by requiring access to an additional authentication factor.
- **Zero Trust Security:** While Ramnit primarily is designed to steal online banking credentials, it can also steal other credentials. By implementing a zero trust security policy and limiting the access and permissions of user accounts, an organization can decrease the potential impact and damage caused by a compromised account.



Ramnit Malware Detection and Protection with Check Point

Ramnit is one of the leading banking trojans and a common malware variant, especially in the APAC region. However, it is only one of several cybersecurity threats that companies face. For more information about the leading malware threats and the current cyber threat landscape, check out Check Point's [2023 Cyber Security Report](#).

[Check Point Harmony Endpoint](#) offers comprehensive threat prevention and detection for Ramnit, other malware, and various threats to the security of an organization's endpoints. For more information about Harmony Endpoint and to learn how it can help to enhance your organization's malware threat prevention capabilities, [sign up for a free demo today](#).

Sumation of Event 1 on the 4 devices:

1. LAB-Win10-02 shows no signs of the EK (Rig) or any payloads for the Malware Ramnit.
2. LAB-Win10-03 shows no signs of the EK (Rig) or any payloads for the Malware Ramnit.
3. LAB-Win7-01 - appears to have been compromised by the EK (Rig)...The Payloads were successfully delivered, but the device was not compromised by the malware Ramnit.
4. Daniel-PC has been compromised by the EK (Rig)...The Payloads were successfully delivered, and the device was infected by the malware Ramnit.

6 - C2 TRAFFIC

Set the date range out to an additional week.

New Search

index="sysmon" Computer="Daniel-PC"

70,935 events (12/29/2017 12:00:00.000 AM to 1/8/18 12:00:00.000 AM) No Event Sampling ▾

Events (70,935) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

18,000
14,000
10,000
6,000

Fri Dec 29 2017 Sun Dec 31 Tue Jan 2 2018 Thu Jan 4

List ▾ Format 20 Per Page ▾

Hide Fields All Fields Time Event

Save As ▾ Close

Date Range

Between ▾ 12/29/2017 and 01/07/2018 00:00:00 24:00:00 Apply

Presets Relative Date & Time Range Advanced

from Dec 29, 2017 through Jan 7, 2018 ▾

New Search

index="sysmon" Computer="Daniel-PC"

70,935 events (29/12/2017 00:00:00.000 to 08/01/2018 00:00:00.000) No Event Sampling ▾

Events (70,935) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

18,000
14,000
10,000
6,000

Fri Dec 29 2017 Sun Dec 31 Tue Jan 2 2018 Thu Jan 4 Sat Jan 6

List ▾ Format 1 hour per column

Hide Fields All Fields Time Event

Save As ▾ Close

from Dec 29, 2017 through Jan 7, 2018 ▾

Check for source ip addresses that could be used by Daniel-PC.

Event

02/01/2018 05:40:06.204

EventID = 13

EventDescription = Unknown

EventCode = 13

Image = C:\Windows\SysWOW64\svchost.exe

Action = allowed

App = C:\Windows\SysWOW64\svchost.exe

Data Zone = 0

User = Daniel-PC

Source = symon

Process = svchost.exe

Process ID = 2612

Siem_Event_ID = symon0163

Source Type = symon

Event Type = change endpoint

EventID = 13

EventCode = 13

Image = C:\Windows\SysWOW64\svchost.exe

Action = allowed

App = C:\Windows\SysWOW64\svchost.exe

Data Zone = 0

User = Daniel-PC

Source = WinEventLog\Microsoft\Windows\System\Operational

Process = svchost.exe

Process ID = 2612

Siem_Event_ID = symon0163

Source Type = symon

Event Type = change endpoint

EventID = 13

EventCode = 13

Image = C:\Windows\SysWOW64\svchost.exe

Action = allowed

App = C:\Windows\SysWOW64\svchost.exe

Data Zone = 0

User = Daniel-PC

Source = WinEventLog\Microsoft\Windows\System\Operational

Process = svchost.exe

Process ID = 2612

Siem_Event_ID = symon0163

Source Type = symon

Event Type = change endpoint

src_ip

5 Values, 0127% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Value	Count	%
10.5.10.138	56	62.22%
10.5.10.132	19	21.11%
10.5.10.131	7	7.78%
0.0.0.0	6	6.66%
10.5.10.125	2	2.22%

INTERESTING FIELDS

If date_hour 7

If date_mday 4

If date_minap 60

Conduct a Boolean search with the ip addresses

New Search

Daniel-PC OR 10.5.10.130 OR 10.5.10.131 OR 10.5.10.132 OR 10.5.10.125

94,245 events (29/12/2017 22:00:00.000 to 08/01/2018 00:00:00.000) No Event Sampling ▾

Events (94,245) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

20,000
14,000
8,000

Sun Dec 31 2017 Tue Jan 2 2018 Thu Jan 4 Sat Jan 6

List ▾ Format 20 Per Page ▾

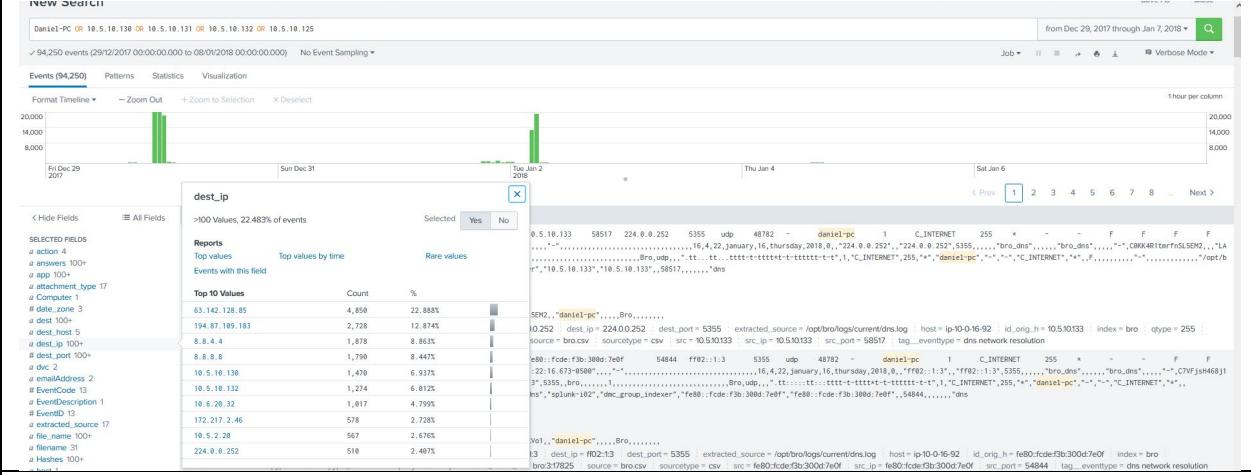
Save As ▾ Close

Date time range ▾

Job ▾ Verbose Mode ▾

1 hour per column

Investigate destination ip addresses



Conduct a Google search of unknown addresses

Investigate identified address



Investigate index

```
a app 3
a date_zone 3
a dest 5
a dest_ip 5
# dest_port 100+
a dvc 1
a extracted_source 3
a host 1
a id_orig_h 4
a index 3
# qtype 2
a qtype_name 2
a query 2
a service 2
a siem_event_id 100+
a source 3
a sourcetype 3
a src 4
a src_ip 4
```

index

3 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
snort	2,161	66.045%
cisco	558	17.054%
bro	553	16.901%

16:39:41.669 1366 28 1880 (empty) - - 00:0c:29:da:95:cb
nation."...16.4.39.january,41,thursday,2018,0,"194.87.109.183","194

Index shows there are Snort alerts, add snort to search

New Search

194.87.109.183 index=snort

✓ 2,361 events (29/12/2017 22:00:00.000 to 04/01/2018 17:00:00.000) No Event Sampling ▾

Events (2,161) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection × Deselect

1 hour per column

Sat Dec 30 2017 Sun Dec 31 Mon Jan 1 2018 Tue Jan 2 Wed Jan 3 Thu Jan 4

List ▾ Format 20 Per Page ▾

< Hide Fields ▾ All Fields i Time Event

02/01/2018 01/02-09:55:187994 [**] [1:33600:1] <ens192> MALWARE-CNC Win.Trojan.Ramnit variant outbound detected [**] [Classification: A Network Trojan was Detected] [Priority: 1] (TCP) 10.5.10.132:49864 -> 194.87.109.183
a_date_zone_1
a_dest_ip 1
dest_port 1
a_host 1
a_index 1
02/01/2018 01/02-09:54:759320 [**] [1:33600:1] <ens192> MALWARE-CNC Win.Trojan.Ramnit variant outbound detected [**] [Classification: A Network Trojan was Detected] [Priority: 1] (TCP) 10.5.10.132:49864 -> 194.87.109.183
date_zone = local dest_ip = 194.87.109.183 dest_port = 443 host = ip-10-0-16-92 index = snort siem_event_id = snort:0:8 source = snortlog sourcetype = snort src_ip = 10.5.10.132 src_port = 49864
date_zone = local dest_ip = 194.87.109.183 dest_port = 443 host = ip-10-0-16-92 index = snort siem_event_id = snort:0:8 source = snortlog sourcetype = snort src_ip = 10.5.10.132 src_port = 49864

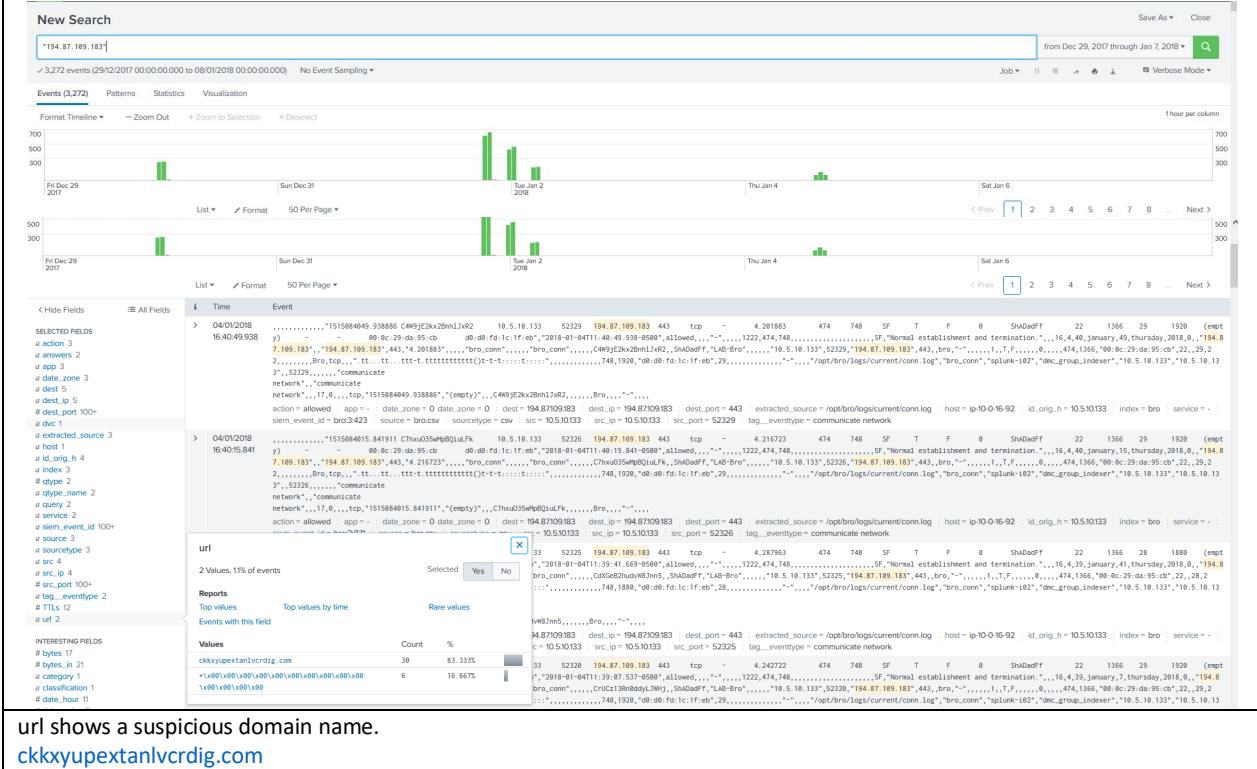
Open any alert and it shows Trojan detected.

02/01/2018 01/02-00:39:55:187994 [**] [1:33600:1] <ens192> MALWARE-CNC Win.Trojan.Ramnit variant outbound detected [**] [Classification: A Network Trojan was Detected] [Priority: 1] (TCP) 10.5.10.132:49864 -> 194.87.109.183
00:39:55:187 09.183:443

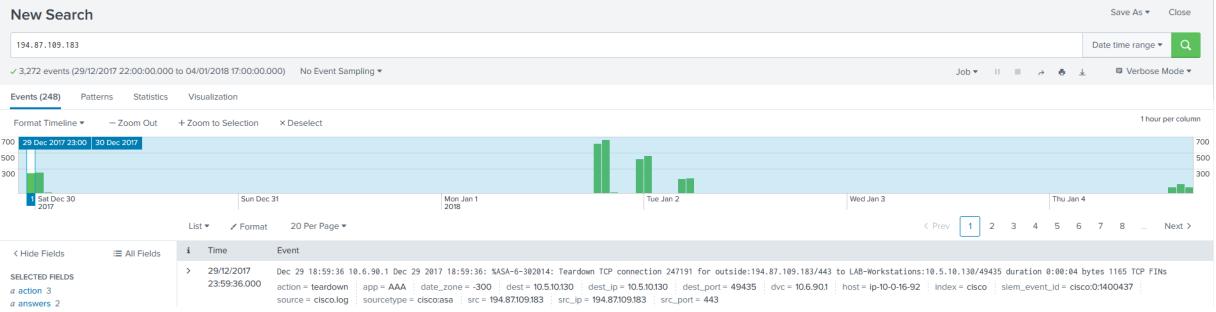
Event Actions ▾

Type	Field	Value
Selected	date_zone	local
Selected	dest_ip	194.87.109.183
Selected	dest_port	443
Selected	host	ip-10-0-16-92
Selected	index	snort
Selected	siem_event_id	snort:0:8
Selected	source	snort.log
Selected	sourcetype	snort
Selected	src_ip	10.5.10.132
Selected	src_port	49864
Event	category	A Network Trojan was Detected
Event	classification	A Network Trojan was Detected
Event	eventtype	snort-alert
Event	generator_id	snort_trojan
Event	interface	1
Event	name	ens192
Event	priority	MALWARE-CNC Win.Trojan.Ramnit variant outbound detected

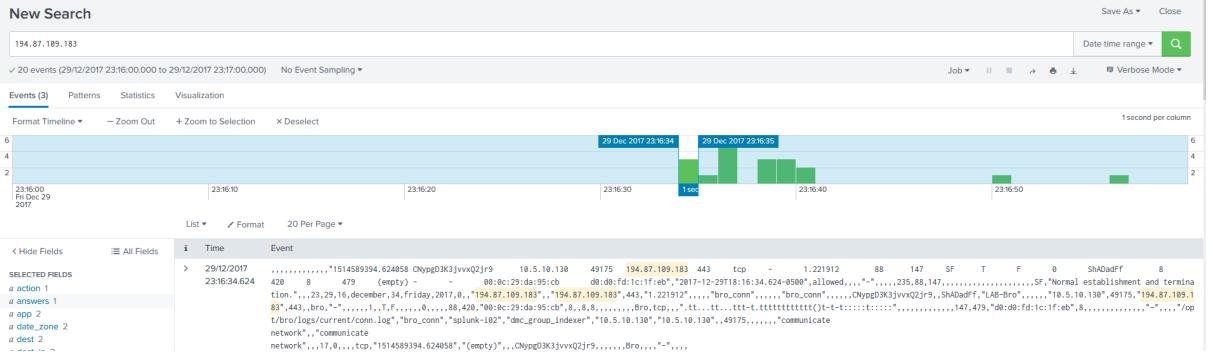
Remove index snort from search and investigate the url.



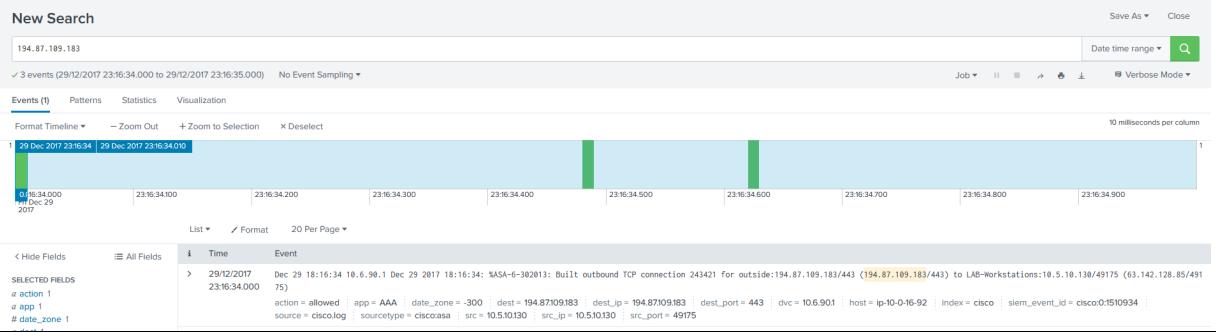
To establish first contact start on first block and +zoom.



+zoom again



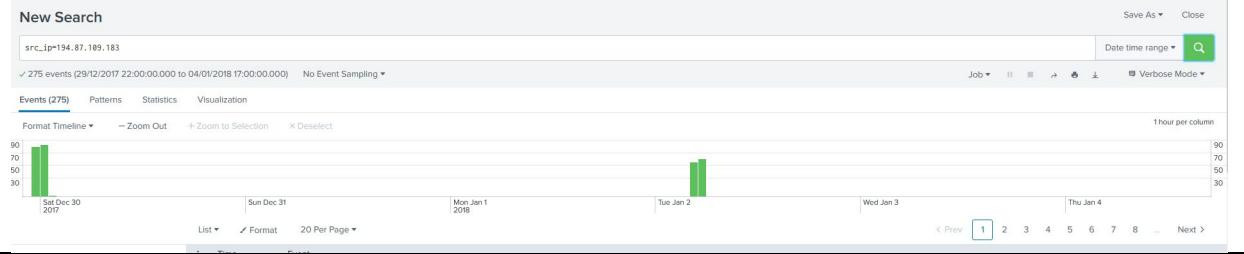
+ zoom again



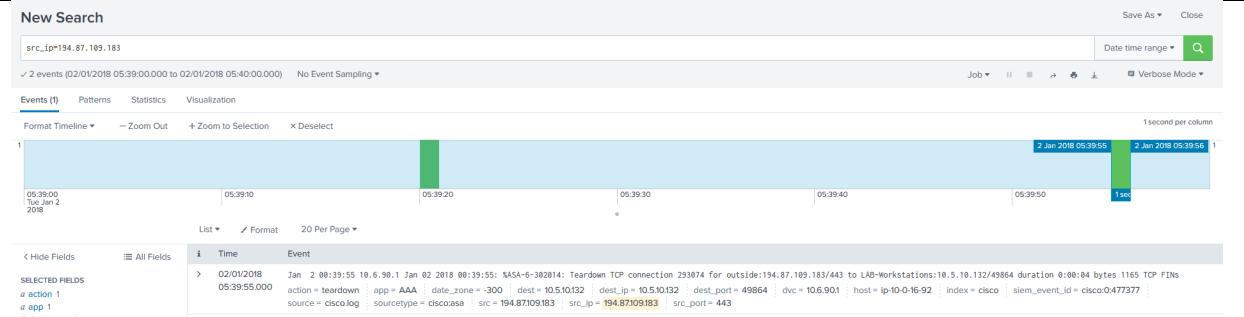
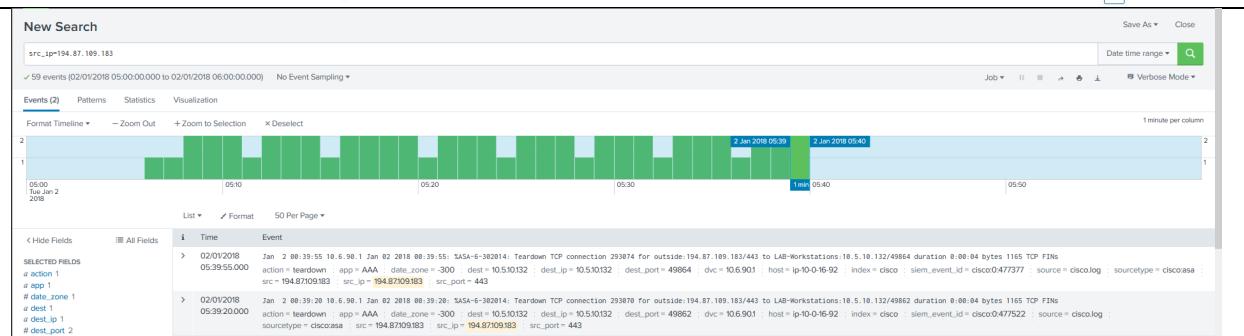
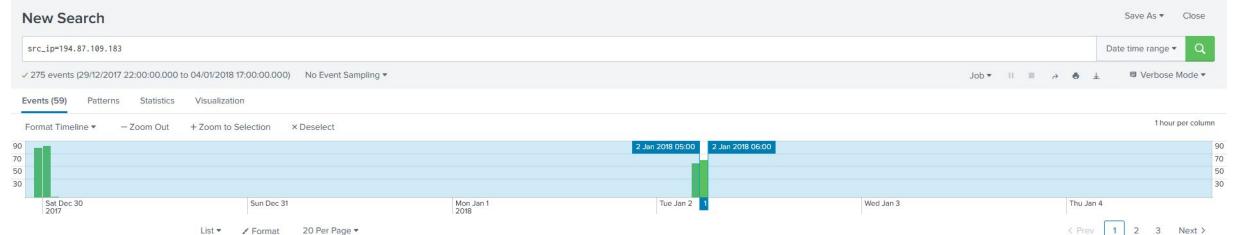
This shows the first time the device made a connection

23:16:34.000

Zoom back out and set ip address as src address



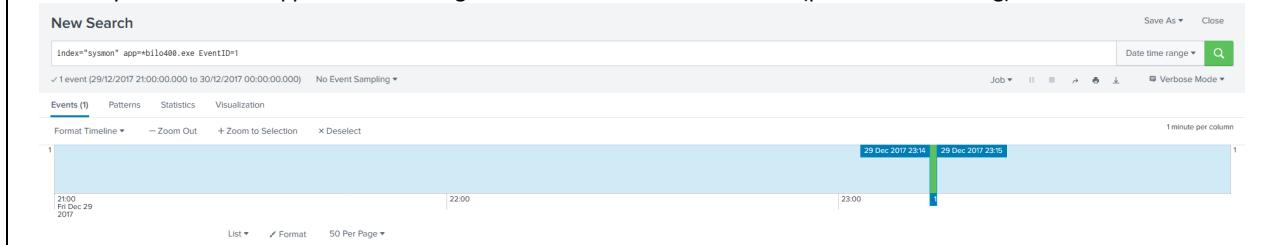
Zoom in on last event



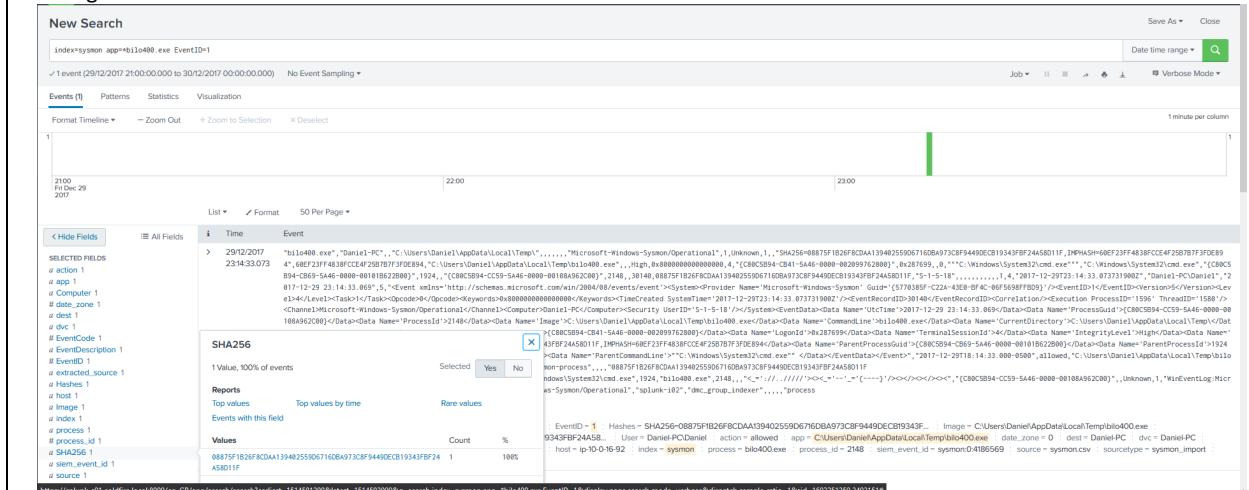
Last successful comms event is at 05:39:55.000

7 - IDENTIFYING FIRST EXECUTION OF THE MALWARE BINARY

Use the sysmon with the app that's executing the bilo400 and the Event Code 1 (process creation log)



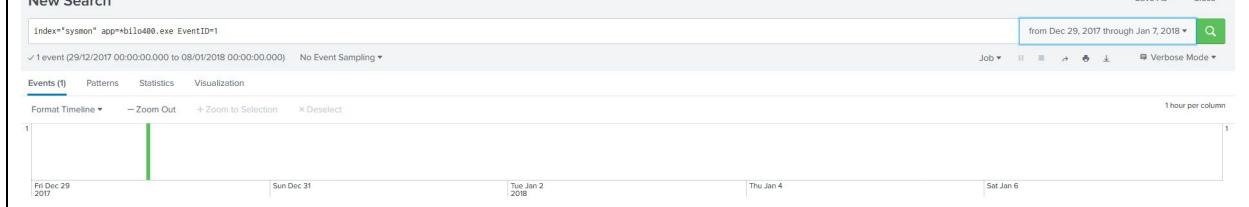
Investigate the SHA256



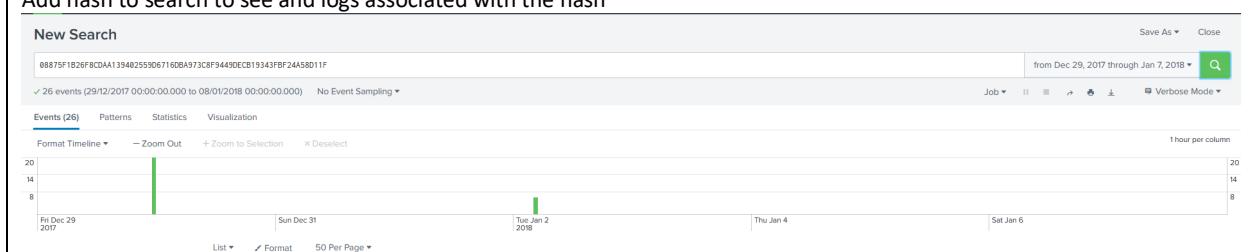
Expand the dates



New Search



Add hash to search to see and logs associated with the hash



Narrow search by including Event Code 1

List ▾ Format 50 Per Page ▾

Hide Fields All Fields

SELECTED FIELDS

- a action 1
- a app 6
- a Computer 1
- # date_zone 1
- a dest 1
- a dvc 1
- # EventCode 2
- a EventDescription 1
- # EventID 2
- a extracted_source 1
- a Hashes 1
- a host 1
- a Image 6
- a index 1
- a process 4

EventCode

2 Values, 100% of events Selected Yes No

Reports

Average over time	Maximum value over time	Minimum value over time
Top values	Top values by time	Rare values

Events with this field

Avg: 4.923076923076923 Min: 1 Max: 7 Std Dev: 2.9109871442255035

Values	Count	%
7	17	65.385%
1	9	34.615%

New Search

Save As ▾ Close

88875f1826f8cdaa1394025580671608a9713cf94450e0b19343f9f24a58011f EventCode=1

from Dec 29, 2017 through Jan 7, 2018 ▾

9 events (29/12/2017 00:00:00.000 to 08/01/2018 00:00:00.000) No Event Sampling ▾

Events (9) Patterns Statistics Visualization

Format Timeline ▾ -Zoom Out +Zoom to Selection × Deselect

1 hour per column

Fri Dec 29 2017 Sun Dec 31 2017 Tue Jan 2 2018 Thu Jan 4 2018 Sat Jan 6 2018

There are 9 separate events which gives proof of persistence.

8 - REGISTRY EVENTS

Event ID 12: RegistryEvent (Object create and delete)

Registry key and value create and delete operations map to this event type, which can be useful for monitoring for changes to Registry autostart locations, or specific malware registry modifications.

Sysmon uses abbreviated versions of Registry root key names, with the following mappings:

Key name	Abbreviation
HKEY_LOCAL_MACHINE	HKLM
HKEY_USERS	HKU
HKEY_LOCAL_MACHINE\System\ControlSet00x	HKLM\System\CurrentControlSet
HKEY_LOCAL_MACHINE\Classes	HKCR

Event ID 13: RegistryEvent (Value Set)

This Registry event type identifies Registry value modifications. The event records the value written for Registry values of type `DWORD` and `QWORD`.

Event ID 14: RegistryEvent (Key and Value Rename)

Registry key and value rename operations map to this event type, recording the new name of the key or value that was renamed.

Use the sysmon with the app that's executing the bilo400 and the Event Code 1



This shows that bilo 400 executed on Daniel-PC at 23:14:33.073 resulting in the device becoming infected with Ramnit Malware

+Zoom into event



New Search

Index=system Computer="Daniel-PC" app="bt10400.exe" EventID=1

✓ 1 event (29/12/2017 23:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling

Events (1) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

23:00 29 Dec 2017 23:10 29 Dec 2017 23:20 6 minutes 23:30 23:40 23:50

List ▾ Format 50 Per Page ▾

New Search

Index=system Computer="Daniel-PC" app="bt10400.exe" EventID=1

✓ 1 event (29/12/2017 23:14:00.000 to 29/12/2017 23:20:00.000) No Event Sampling

Events (1) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

23:14 29 Dec 2017 23:15 23:16 23:17 23:18 23:19

Save As ▾ Close Date time range ▾

Adjust search to focus on registry events.

New Search

Index=system Computer="Daniel-PC" EventID IN [12, 13, 14]

✓ 1 event (29/12/2017 23:14:00.000 to 29/12/2017 23:20:00.000) No Event Sampling

Events (1) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

23:14 29 Dec 2017 23:15 23:16 23:17 23:18 23:19

Save As ▾ Close Date time range ▾

New Search

Index=system Computer="Daniel-PC" EventID IN [12, 13, 14]

✓ 1,318 events (29/12/2017 23:14:00.000 to 29/12/2017 23:20:00.000) No Event Sampling

Events (1,318) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

400 300 200 100 23:14 29 Dec 2017 23:15 23:16 23:17 23:18 23:19 400 300 200 100

Now search for modifications you could expect to see for implementation of the Ramnit Malware.

Admin parameter

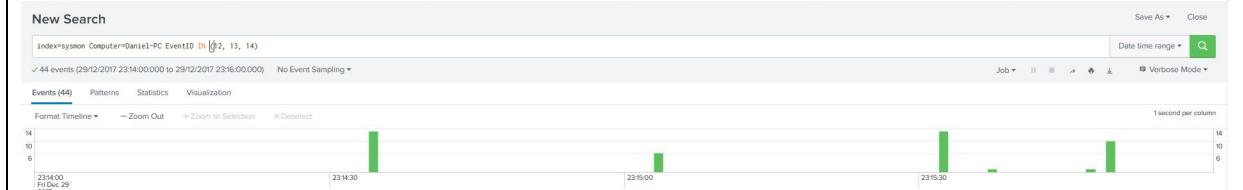
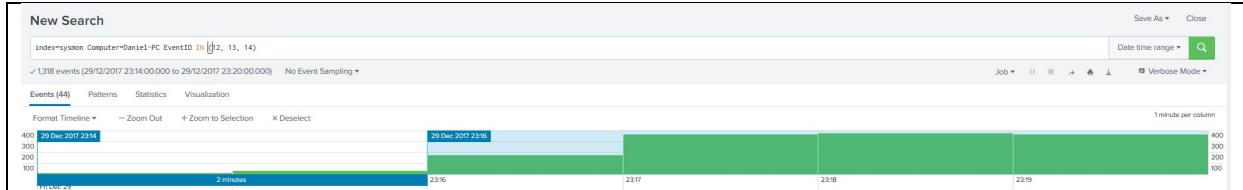
When the “admin” parameter is supplied, the installer creates a mutex as previously described, using 0x14D7 as the seed value. The installer force-exits if it fails to successfully create the mutex.

Then, the installer attempts to lower the computer’s security by modifying the following registry entries and subkeys:

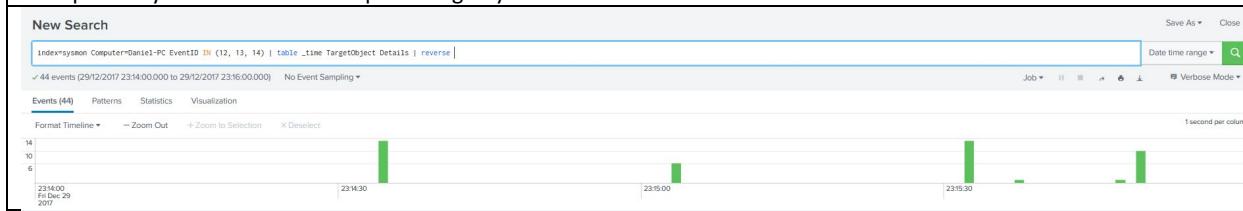
Sets

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\“EnableLUA” = “0”
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center\FirewallOverride” = “1”
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center\AntiVirusOverride” = “1”
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center\Svc\“AntiVirusOverride” = “1”
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wscsvc\“Start” = “4”
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\“EnableFirewall” = “0”
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\“DoNotAllowExceptions” = “0”
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\“DisableNotifications” = “1”

Because there are 1,318 events...narrow the search to the first 2 minutes and investigate in smaller time chunks.



Now profile sysmon to be more helpful in registry fields



New Search

Events (44) Patterns Statistics (44) Visualization

100 Per Page ▾ Format Preview ▾

time	TargetObject	Details
2017-12-29 23:14:34.618	\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\DHcpNameServer	
2017-12-29 23:14:34.611	\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{C73EE532-FF45-46B1-B0B3-1AFABAABBBB0\}\DHcpNameServer	
2017-12-29 23:14:34.612	\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\DHcpDomain	
2017-12-29 23:14:34.613	\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{C73EE532-FF45-46B1-B0B3-1AFABAABBBB0\}\DHcpDomain	
2017-12-29 23:14:34.615	\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{C73EE532-FF45-46B1-B0B3-1AFABAABBBB0\}\DHcpDefaultGateway	
2017-12-29 23:14:34.617	\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\DHcpNameServer	8.8.8.8.8.4.4
2017-12-29 23:14:34.618	\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{C73EE532-FF45-46B1-B0B3-1AFABAABBBB0\}\DHcpDefaultGateway	Binary Data
2017-12-29 23:14:34.618	\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{C73EE532-FF45-46B1-B0B3-1AFABAABBBB0\}\DHcpNameServer	8.8.8.8.8.4.4
2017-12-29 23:14:34.619	\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\DHcpDomain	at-usa.co
2017-12-29 23:14:34.620	\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{C73EE532-FF45-46B1-B0B3-1AFABAABBBB0\}\DHcpDomain	at-usa.co
2017-12-29 23:14:34.623	\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{C73EE532-FF45-46B1-B0B3-1AFABAABBBB0\}\DHcpIpAddress	18.5.10.130
2017-12-29 23:14:34.624	\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{C73EE532-FF45-46B1-B0B3-1AFABAABBBB0\}\DHcpServer	18.5.10.1
2017-12-29 23:14:34.624	\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{C73EE532-FF45-46B1-B0B3-1AFABAABBBB0\}\DHcpSubnetMask	255.255.255.0
2017-12-29 23:15:03.164	\REGISTRY\USERS\1-5-21-3683720883-912195923-1324197430-1000\Software\Microsoft\Windows\CurrentVersion\Run\OboMhdf	C:\Users\Daniel\appData\Local\guwayhtr\obommhdf.exe
2017-12-29 23:15:03.184	\REGISTRY\USERS\1-5-21-3683720883-912195923-1324197430-1000\Software\Microsoft\Windows\CurrentVersion\Run\OboMhdf	DWORD (0x00000004)
2017-12-29 23:15:03.189	\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\wscsvc\Start	DWORD (0x00000004)
2017-12-29 23:15:03.189	\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\mpssvc\Start	DWORD (0x00000004)
2017-12-29 23:15:03.190	\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\wuauserv\Start	DWORD (0x00000004)

Ramnit does 8 pseudo-random characters

\Software\Microsoft\Windows\CurrentVersion\Run\OboMhdf

C:\Users\Daniel\AppData\Local\guwayhtr\obommhdf.exe

One of the ways Ramnit sets up persistence is it modifies the Run key to ensure a copy of the malware that it made of itself runs at the start.

Another way it takes affect...

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wscsvc\”Start” = “4”

\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\wscsvc\Start	DWORD (0x00000004)
\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\wscsvc\Start	DWORD (0x00000004)
\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\mpssvc\Start	DWORD (0x00000004)
\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\wuauserv\Start	DWORD (0x00000004)
\REGISTRY\ACHINE\SYSTEM\ControlSet001\services\WinDefend\Start	DWORD (0x00000004)

An additional way to help locate events is to add the Event ID to the search

New Search

Index=system Computer=Daniel1-PC EventID IN (12, 13, 14) | table _time EventID TargetObject Details | reverse

44 events (29/12/2017 23:14:00.0000 to 29/12/2017 23:16:00.0000) No Event Sampling ▾

Events (44) Patterns Statistics (44) Visualization

100 Per Page ▾ Format Preview ▾

_time	EventID	TargetObject	Details
2017-12-29 23:14:34.610	12	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\DHcpNameServer	
2017-12-29 23:14:34.611	12	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{C73EE532-FF45-46B1-BD83-1AFABAA00000\}\DHcpNameServer	
2017-12-29 23:14:34.612	12	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\DHcpDomain	
2017-12-29 23:14:34.613	12	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{C73EE532-FF45-46B1-BD83-1AFABAA00000\}\DHcpDomain	
2017-12-29 23:14:34.615	12	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{C73EE532-FF45-46B1-BD83-1AFABAA00000\}\DHcpDefaultGateway	8.8.8.8.8.8.4.4 Binary Data
2017-12-29 23:14:34.617	13	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\DHcpNameServer	8.8.8.8.8.4.4 at-usa.co
2017-12-29 23:14:34.618	13	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{C73EE532-FF45-46B1-BD83-1AFABAA00000\}\DHcpDefaultGateway	8.8.8.8.8.4.4 at-usa.co
2017-12-29 23:14:34.618	13	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{C73EE532-FF45-46B1-BD83-1AFABAA00000\}\DHcpNameServer	8.8.8.8.8.4.4 at-usa.co
2017-12-29 23:14:34.619	13	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\DHcpDomain	at-usa.co
2017-12-29 23:14:34.620	13	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{C73EE532-FF45-46B1-BD83-1AFABAA00000\}\DHcpDomain	at-usa.co
2017-12-29 23:14:34.622	13	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{C73EE532-FF45-46B1-BD83-1AFABAA00000\}\DHcpIpAddress	19.5.10.130 19.5.10.1
2017-12-29 23:14:34.624	13	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{C73EE532-FF45-46B1-BD83-1AFABAA00000\}\DHcpServer	255.255.255.0 C:\Users\Daniel\AppData\Local\guawayhtr\boonmhdf.exe
2017-12-29 23:14:34.624	13	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{C73EE532-FF45-46B1-BD83-1AFABAA00000\}\DHcpSubnetMask	255.255.255.0 C:\Users\Daniel\AppData\Local\guawayhtr\boonmhdf.exe
2017-12-29 23:15:03.164	13	\REGISTRY\USER\{1-5-21-3681720036-912159523-1324197430-1000\}\Software\Microsoft\Windows\CurrentVersion\Run\boonmhdf	DHOD (0x00000004)
2017-12-29 23:15:03.184	13	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\wccsvc\Start	DHOD (0x00000004)
2017-12-29 23:15:03.189	13	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\wccsvc\Start	DHOD (0x00000004)
2017-12-29 23:15:03.189	13	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\wpsvc\Start	DHOD (0x00000004)
2017-12-29 23:15:03.198	13	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\wuaserv\Start	DHOD (0x00000004)
2017-12-29 23:15:03.198	13	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Wlde fend\Start	DHOD (0x00000004)

You can now see Event 13 listed which is Setting a Value which is evident above.

It sets up persistence and then it makes the changes it needs to ensure it will keep running.

At 23:15:03.164 - .190 registry modifications occurred that decreased the security settings on Daniel-PC.

9 - EK COMPROMISE VERIFICATION & MALWARE SUCCESS / FAILURE

Look for all traffic between the compromised device and the EK server

New Search
18.5.10.129 176.57.214.183
✓ 85 events (29/12/2017 00:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling ▾
Events (85) Patterns Statistics Visualization
Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect
Save As ▾ Close during Fri, Dec 29, 2017 [Search] Verbose Mode ▾
1 hour per column
90
60
30
00:00 04:00 08:00 12:00 16:00 20:00
Fri Dec 29 2017

Refine the search even further

New Search
18.5.10.129 176.57.214.183
✓ 85 events (29/12/2017 00:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling ▾
Events (85) Patterns Statistics Visualization
Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect
Save As ▾ Close during Fri, Dec 29, 2017 [Search] Verbose Mode ▾
1 hour per column
90
60
30
00:00 04:00 08:00 12:00 16:00 20:00 24:00 28:00
Fri Dec 29 2017

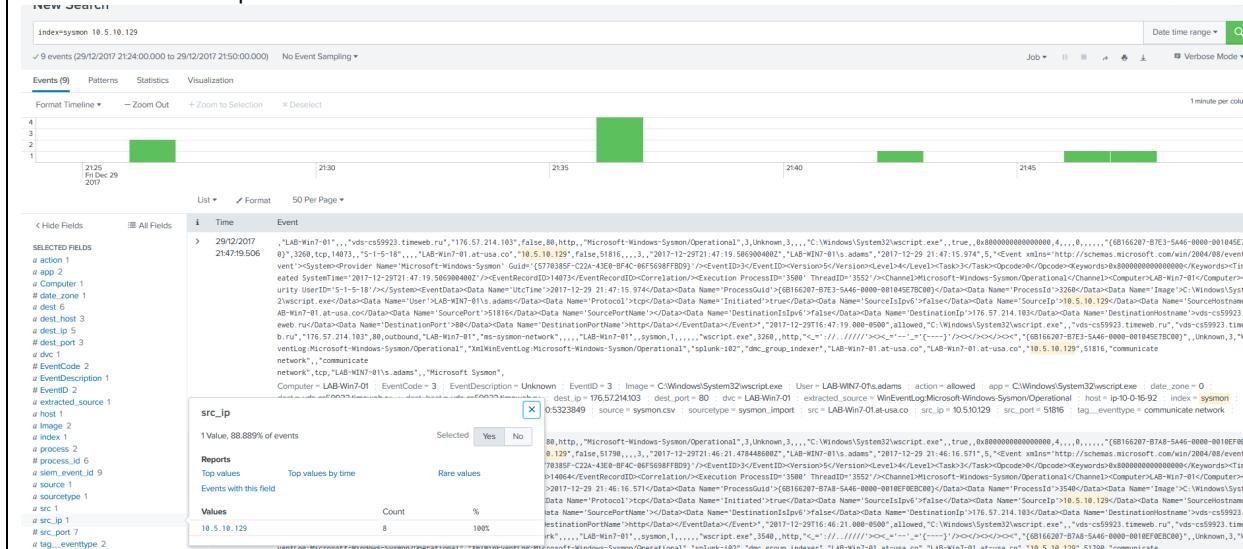
New Search
18.5.10.129 176.57.214.183
✓ 85 events (29/12/2017 21:00:00.000 to 29/12/2017 22:00:00.000) No Event Sampling ▾
Events (85) Patterns Statistics Visualization
Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect
Save As ▾ Close Date time range [Search] Verbose Mode ▾
1 minute per column
18
12
6
21:00 21:10 21:20 21:30 21:40 21:50
Fri Dec 29 2017

New Search
18.5.10.129 176.57.214.183
✓ 85 events (29/12/2017 21:24:00.000 to 29/12/2017 21:50:00.000) No Event Sampling ▾
Events (85) Patterns Statistics Visualization
Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect
Save As ▾ Close Date time range [Search] Verbose Mode ▾
1 minute per column
18
12
6
21:25 21:30 21:35 21:40 21:45
Fri Dec 29 2017

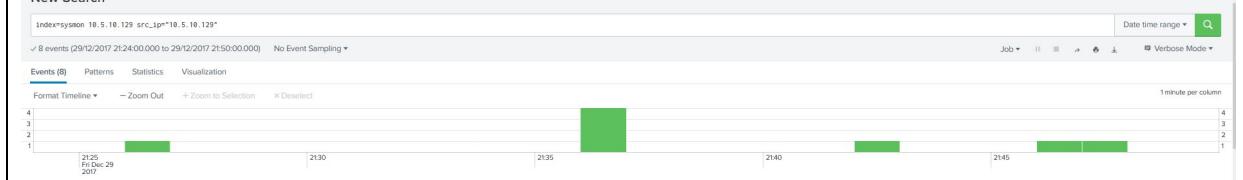
Now pivot to host base logs and specify

New Search
Index=esymon 10.5.10.129
✓ 9 events (29/12/2017 21:24:00.000 to 29/12/2017 21:50:00.000) No Event Sampling ▾
Events (9) Patterns Statistics Visualization
Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect
Save As ▾ Close Date time range [Search] Verbose Mode ▾
1 minute per column
4
3
2
1
21:26 21:30 21:35 21:40 21:45
Fri Dec 29 2017

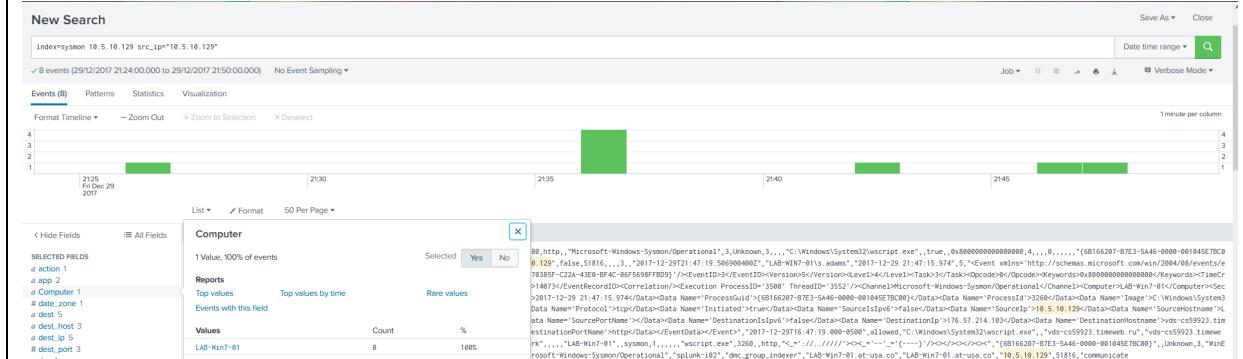
Now set thew source ip address



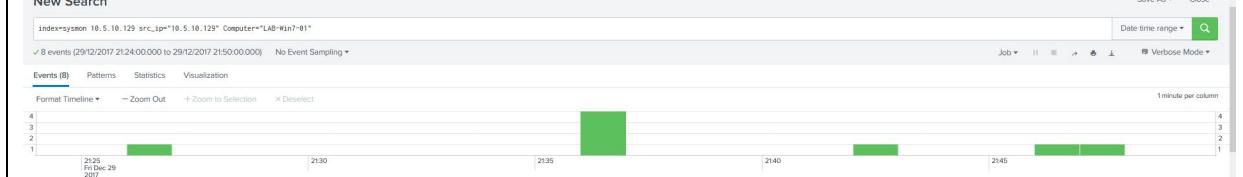
New Search



Now you can identify the computer



New Search



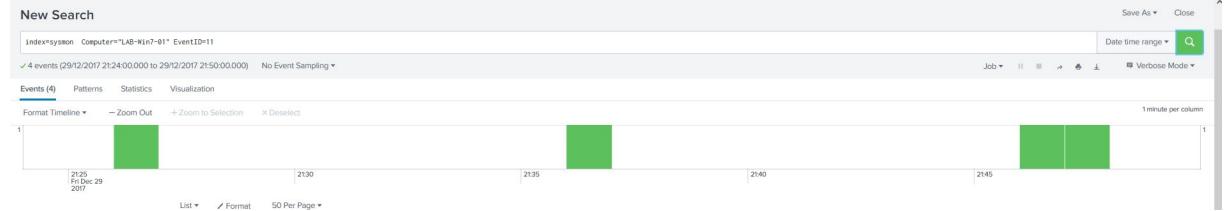
Because I now have the host name I can get rid of the ip address

Now looking for all the events for LAB-Win7-01 during the specified time span

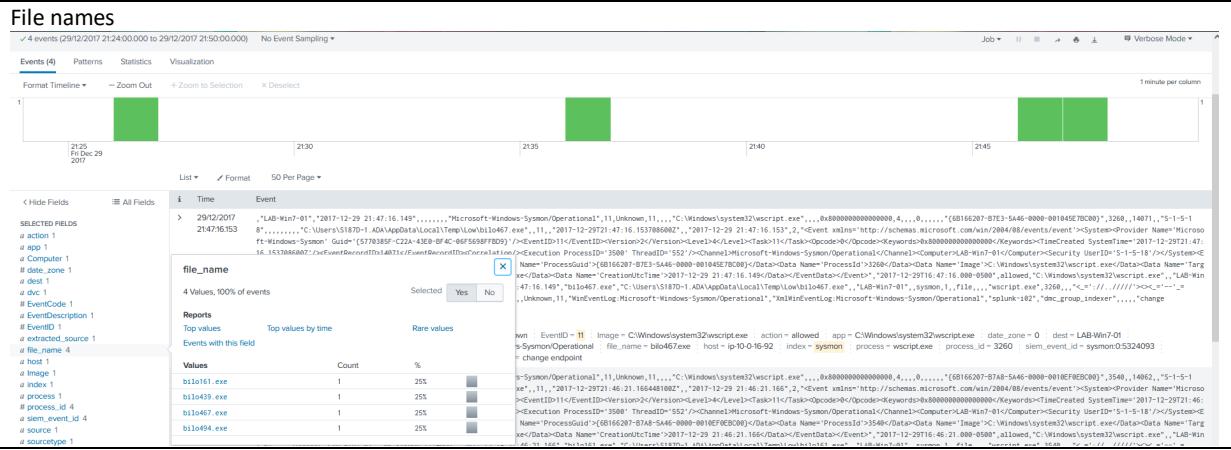


Now looking for the payload delivered...

File Creation (Event 11 is file creation in sysmon)



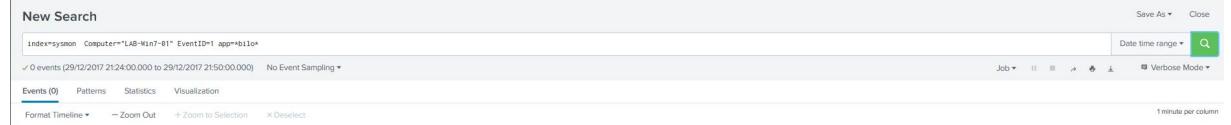
This search reveals 4 events



This is evidence of compromise by Rig EK...

Now look for process creation logs by changing from File Creation EventID 11 to Process Creation EventID 1 to see if there is evidence of execution / malware infection.

The search shows no results



To be able to prove that the search is correct we can verify with Daniel-PC (you need to change the time range)

1 process creation event which verifies infection on Daniel-PC, but no process creation events were evident on LAB-Win7-01, verifying that the device was not infected, but payloads were delivered.

Stepping further...

By using the hash in the search and checking the application field you see multiple 8 random character files...which are windows type files in trying to camouflage itself...

To see when they didn't execute create the following search parameters

New Search	Save As ▾	Close							
index=system Computer="LAB-Min7-01" EventID IN (1, 1) table _time EventID parent_process process CommandLine file_path reverse	Date time range ▾	🔍							
✓ 46 events (29/12/2017 21:24:00.000 to 29/12/2017 21:50:00.000) No Event Sampling ▾	Job ▾		☰	↶	↷	↶↶	↷↷	Verbose Mode ▾	
Events (46) Patterns Statistics (46) Visualization									
100 Per Page ▾	✓ Format	Preview ▾							
EventID									

New Search

By seeing the Explorer exe cmd.exe prompt is the first sign of Win7-01 is compromised by the EK.

```

PC 6.0; .NET4.0C; rv:11.0) like Gecko"
2017-12-29 11 wscript.exe
21:26:28.957

2017-12-29 1 C:\Windows\System32\cmd.exe "C:\Windows\System32\cmd.exe" /c bilo439.exe
21:26:28.917

2017-12-29 1 C:\Program Files\Internet Explorer\iexplore.exe "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:3120 CREDAT:3028042 /prefetch:2
21:32:44.434

1 C:\Windows\System32\wscript.exe cmd.exe "C:\Windows\System32\cmd.exe" /c bilo439.exe
1 C:\Program Files\Internet Explorer\iexplore.exe "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:3120 CREDAT:3028042 /prefetch:2

2017-12-29 11 wscript.exe
21:36:30.535

2017-12-29 1 C:\Windows\System32\wscript.exe cmd.exe "C:\Windows\System32\cmd.exe" /c bilo494.exe
21:36:30.574

2017-12-29 11 wscript.exe
21:46:21.166

2017-12-29 1 C:\Windows\System32\cmd.exe "C:\Windows\System32\cmd.exe" /c bilo161.exe
21:46:21.213

2017-12-29 11 wscript.exe
21:47:16.153

2017-12-29 1 C:\Windows\System32\wscript.exe cmd.exe "C:\Windows\System32\cmd.exe" /c bilo467.exe
21:47:16.225

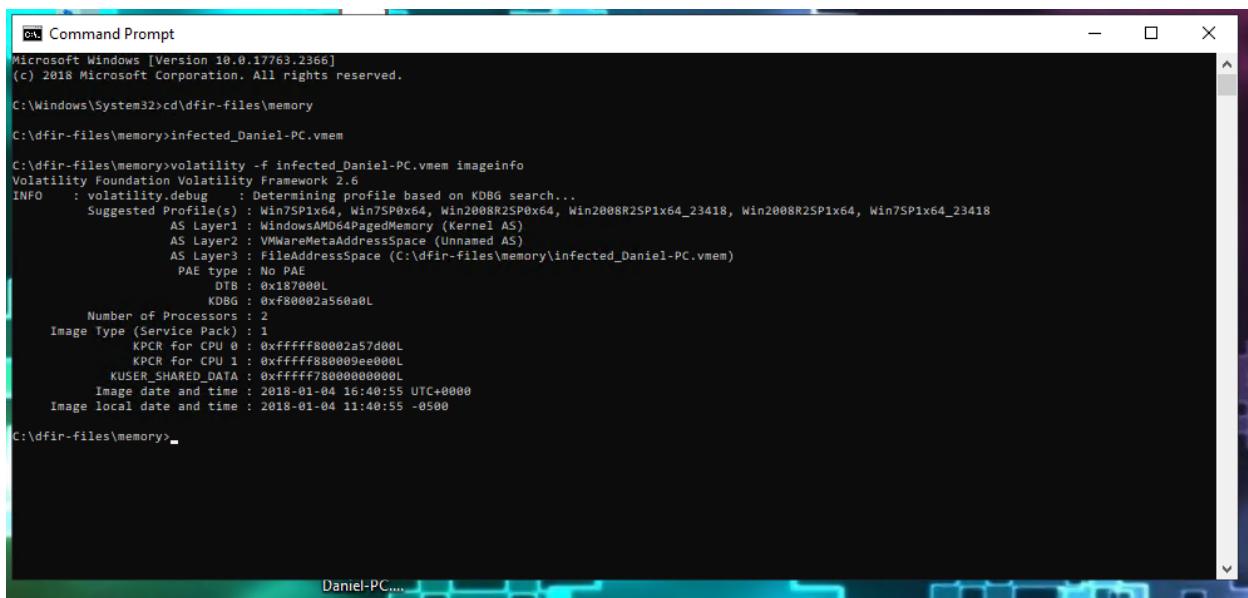
2017-12-29 1 C:\Windows\taskmgr.exe "C:\Windows\system32\taskmgr.exe" /

```

We can see where the 4 bilo payload files tried to execute but you do not see a process creation event which you should see as the next line...below the cmd.exe line...it is the same on all 4.

Despite trying to get the process file something did not work.

10 – MEMORY



```
cmd Command Prompt
Microsoft Windows [Version 10.0.17763.2366]
(c) 2018 Microsoft Corporation. All rights reserved.

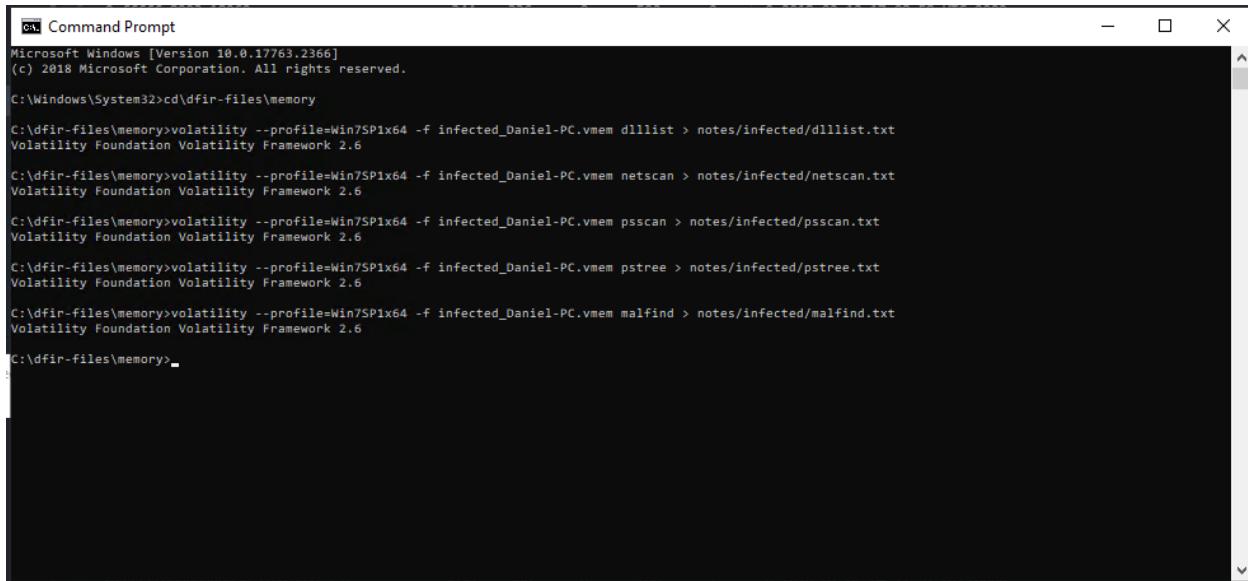
C:\Windows\System32>cd\dfir-files\memory

C:\dfir-files\memory>infected_Daniel-PC.vmem

C:\dfir-files\memory>volatility -f infected_Daniel-PC.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
AS Layer1 : WindowsMDA PagedMemory (Kernel AS)
AS Layer2 : VMWareMetaAddressSpace (Unnamed AS)
AS Layer3 : FileAddressSpace (C:\dfir-files\memory\infected_Daniel-PC.vmem)
PAE type : No PAE
DTB : 0x187000L
K08G : 0xf80002a560a0L
Number of Processors : 2
Image Type (Service Pack) : 1
    KPCR for CPU 0 : 0xfffffff80002a57d00L
    KPCR for CPU 1 : 0xfffffff80009ee000L
    KUSER_SHARED_DATA : 0xfffff78000000000L
Image date and time : 2018-01-04 16:40:55 UTC+0000
Image local date and time : 2018-01-04 11:40:55 -0500

C:\dfir-files\memory>
```

Select various modules for both baseline and infected volatility...



```
cmd Command Prompt
Microsoft Windows [Version 10.0.17763.2366]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd\dfir-files\memory

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem dlllist > notes/infected/dlllist.txt
Volatility Foundation Volatility Framework 2.6

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem netscan > notes/infected/netscan.txt
Volatility Foundation Volatility Framework 2.6

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem psscan > notes/infected/psscan.txt
Volatility Foundation Volatility Framework 2.6

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem pstree > notes/infected/pstree.txt
Volatility Foundation Volatility Framework 2.6

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem malfind > notes/infected/malfind.txt
Volatility Foundation Volatility Framework 2.6

C:\dfir-files\memory>
```

Investigate plist for both baseline and infected

The screenshot shows two side-by-side Atom code editors. Both have tabs for 'Project' and 'plist.txt'. The left editor is titled 'Project — C:\dfir-files\memory\notes\baseline — Atom' and contains 21 entries. The right editor is titled 'Project — C:\dfir-files\memory\notes\infected — Atom' and contains 68 entries. Both lists include columns for Offset(V), Name, PID, PPID, Thds, Hnds, Sess, Wow64, Start, and Exit.

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
1	System	4	0	84	365	-----	0	2018-02-12 17:08:56 UTC+0000	
4	smss.exe	264	4	2	29	-----	0	2018-02-12 17:08:56 UTC+0000	
5	csrss.exe	344	336	9	592	0	0	2018-02-12 17:08:58 UTC+0000	
6	wininit.exe	396	336	3	75	0	0	2018-02-12 17:08:58 UTC+0000	
7	csrss.exe	408	388	9	155	1	0	2018-02-12 17:08:58 UTC+0000	
8	winlogon.exe	456	388	5	114	1	0	2018-02-12 17:08:58 UTC+0000	
9	svchost.exe	500	396	18	216	0	0	2018-02-12 17:08:58 UTC+0000	
10	lsass.exe	516	396	8	531	0	0	2018-02-12 17:08:58 UTC+0000	
11	lsm.exe	524	396	10	198	0	0	2018-02-12 17:08:58 UTC+0000	
12	svchost.exe	624	500	11	353	0	0	2018-02-12 17:08:59 UTC+0000	
13	svchost.exe	692	500	7	254	0	0	2018-02-12 17:08:59 UTC+0000	
14	svchost.exe	744	500	16	353	0	0	2018-02-12 17:08:59 UTC+0000	
15	svchost.exe	876	500	20	430	0	0	2018-02-12 17:08:59 UTC+0000	
16	svchost.exe	928	500	34	865	0	0	2018-02-12 17:08:59 UTC+0000	
17	svchost.exe	288	500	12	490	0	0	2018-02-12 17:08:59 UTC+0000	
18	svchost.exe	284	500	28	495	0	0	2018-02-12 17:09:01 UTC+0000	
19	spoolsv.exe	1036	500	13	268	0	0	2018-02-12 17:09:00 UTC+0000	
20	svchost.exe	1072	500	19	389	0	0	2018-02-12 17:09:00 UTC+0000	
21	Graylog-collect	1160	500	15	122	0	0	2018-02-12 17:09:01 UTC+0000	
22	obommhdf.exe	1176	1120	8	67	0	0	2018-02-12 17:09:01 UTC+0000	
49	TrustedInstall	2564	500	0	-----	0	0	2018-01-01 21:35:13 UTC+0000	2018-01-02 04:22:32 UTC+0000
50	VSSVC.exe	1276	500	0	-----	0	0	2018-01-01 21:40:24 UTC+0000	2018-01-02 04:12:36 UTC+0000
51	taskhost.exe	1420	500	0	-----	0	0	2018-01-02 04:12:33 UTC+0000	2018-01-02 04:14:38 UTC+0000
52	SearchProtocol	2632	1764	0	-----	0	0	2018-01-02 04:14:10 UTC+0000	2018-01-02 04:14:10 UTC+0000
53	SearchFilterHo	3368	1764	0	-----	0	0	2018-01-02 04:12:37 UTC+0000	2018-01-02 04:14:10 UTC+0000
54	dllhost.exe	3612	644	0	-----	0	0	2018-01-02 04:12:57 UTC+0000	2018-01-02 04:13:02 UTC+0000
55	taskhost.exe	3656	500	8	186	1	0	2018-01-02 04:12:57 UTC+0000	
56	taskhost.exe	3716	896	0	-----	0	0	2018-01-02 04:12:57 UTC+0000	2018-01-02 04:17:59 UTC+0000
57	userinit.exe	3744	472	0	-----	1	0	2018-01-02 04:12:57 UTC+0000	2018-01-02 04:13:27 UTC+0000
58	obommhdf.exe	3764	896	1	0	-----	1	2018-01-02 04:12:57 UTC+0000	2018-01-02 04:13:28 UTC+0000
59	dwm.exe	3780	864	3	73	1	0	2018-01-02 04:12:57 UTC+0000	
60	explorer.exe	3824	3744	30	992	1	0	2018-01-02 04:12:57 UTC+0000	
61	GrayscaleHlan	3912	3884	0	-----	0	0	2018-01-02 04:12:58 UTC+0000	2018-01-02 04:12:59 UTC+0000
62	GrayscaleHlan	3920	3884	0	-----	0	0	2018-01-02 04:12:58 UTC+0000	2018-01-02 04:12:59 UTC+0000
63	svchost.exe	669	3824	6	131	1	0	2018-01-02 04:13:00 UTC+0000	
64	jusched.exe	2736	2532	10	361	1	1	2018-01-02 04:13:01 UTC+0000	
65	chrome.exe	3444	3824	0	-----	1	0	2018-01-02 04:13:05 UTC+0000	2018-01-04 15:12:12 UTC+0000
66	wmpntrbk.exe	4132	500	9	223	0	0	2018-01-02 04:13:08 UTC+0000	
67	svchost.exe	2612	4652	16	291	1	1	2018-01-02 04:13:58 UTC+0000	
68	svchost.exe	4104	4652	12	285	1	1	2018-01-02 04:13:58 UTC+0000	
69	TRACERT.EXE	3098	4104	3	56	1	0	2018-01-02 04:14:15 UTC+0000	

In the infected I can see line 58 which is an anomaly of Ramnit (8-character name) obommhdf.exe

Lines 67 & 68 show svchost.exe with incorrect Parent PID (should only and always be 500, but is 4652).

Now investigating on Splunk

New Search

Index=symon Computer=Daniel-PC ProcessId=4652
from Dec 29, 2017 through Jan 4, 2018

Events (10) Patterns Statistics Visualization

Format Timeline ▾ Zoom Out ▾ Zoom to Selection × Deselect

1 hour per column

Fri Dec 29 2017 Sat Dec 30 Sun Dec 31 Mon Jan 1 2018 Tue Jan 2 Wed Jan 3 Thu Jan 4

EventCode 4
a EventDescription 1
EventID 4
a extracted_source 1
a file_name 1
a Hashes 7
a host 1
a Image 5
a index 1
a process 5
process_id 1
a SHA256 7
a siem_event_id 10
a source 1
a sourcetype 1
a tag_eventtype 2
a User 3
a user 3

process

Log:Microsoft-Windows-Sysmon/Operational", "XmlWinEventLog:Microsoft

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
xwgrttj1.exe	4	40%
LogonUI.exe	3	30%
rdpclip.exe	1	10%
taskhost.exe	1	10%
vmtoolsd.exe	1	10%

EventCode 4
a EventDescription 1
EventID 4
a extracted_source 1
a file_name 1
a Hashes 7
a host 1
a Image 5
a index 1
a parent_process 5
parent_process_id 5
ParentProcessId 5
a process 5
process_id 1
ProcessId 1
a SHA256 7
a siem_event_id 10
a source 1
a sourcetype 1

parent_process

Log:Microsoft-Windows-Sysmon/Operational", "XmlWinEventLog:Microsoft

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
C:\Users\Daniel\AppData\Local\guwayhtr\obommhdf.exe	1	20%
C:\Windows\System32\services.exe	1	20%
C:\Windows\System32\svchost.exe	1	20%
C:\Windows\System32\winlogon.exe	1	20%
C:\Windows\explorer.exe	1	20%

New Search

1 Index=symon Computer="Daniel-PC" ProcessId=4652 parent_process="C:\Users\Daniel\AppData\Local\guawayhtr\obommhdf.exe"

✓ 1 event (29/12/2017 00:00:00.000 to 05/01/2018 00:00:00.000) No Event Sampling ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾

1 hour per column

Fri Dec 29 Sat Dec 30 Sun Dec 31 Mon Jan 1 Tue Jan 2 Wed Jan 3 Thu Jan 4

EventID 1
 a extracted_source 1
 a Hashes 1
 a host 1
 a Image 1
 a index 1
 a parent_process 1
 # parent_process_id 1
 # ParentProcessId 1
 a process 1
 # process_id 1
 # ProcessId 1
 a SHA256 1
 a siem_event_id 1
 a source 1
 a sourcetype 1
 a tag__eventtype 1

ParentProcessId

1 Value, 100% of events Selected

Reports

Average over time	Maximum value over time	Minimum value over time
Top values	Top values by time	Rare values

Events with this field

Avg: 3764 **Min:** 3764 **Max:** 3764 **Std Dev:** 0

Values	Count	%
3764	1	100%

New Search

1 Index=symon Computer="Daniel-PC" ProcessId=4652 | table _time, siem_event_id, Computer, source_ip, EventID, user, CurrentDirectory, process, ProcessId, Image, CommandLine, ParentProcessId, ParentImage, ParentCommandLine, SHA256

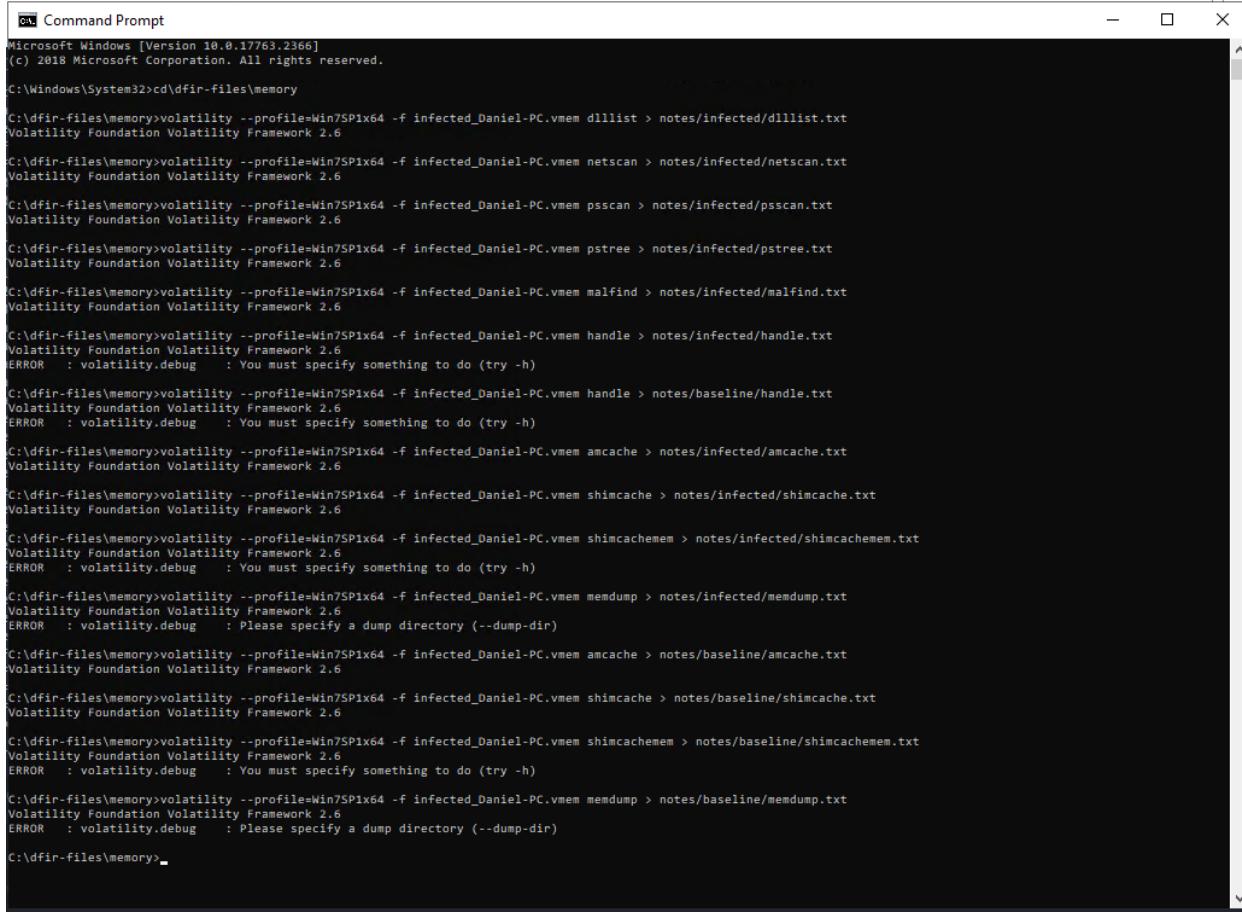
✓ 10 events (29/12/2017 00:00:00.000 to 05/01/2018 00:00:00.000) No Event Sampling ▾

Events (10) Patterns Statistics Visualization

So, by pivoting between our two log sources, we can now reconstruct what happened:

1. obommhdf.exe (PID 3764) spawned a second instance of the 08875f1b... Ramnit executable: xwgrttjl.exe (PID 4652).
2. xwgrttjl.exe (PID 4652) then spawned the two rogue (== without PPID of services.exe (PID 500)!) svchost.exe's: svchost.exe (PID 4104) and svchost.exe (PID 2612).
3. xwgrttjl.exe (PID 4652) then exited the process list, having served its function.
4. obommhdf.exe (PID 3764), svchost.exe (PID 4104) and svchost.exe (PID 2612) remain running.

Volatility Command Prompt



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The window contains a series of Volatility commands run against a file named "infected_Daniel-PC.vmem". The commands include memory dump extraction, DLL list analysis, network scanning, process listing, handle enumeration, and cache analysis. Most commands succeed, while some like "memdump" fail due to missing dump directory specification.

```
Microsoft Windows [Version 10.0.17763.2366]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd\dfir-files\memory

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem dlllist > notes/infected/dlllist.txt
Volatility Foundation Volatility Framework 2.6

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem netscan > notes/infected/netscan.txt
Volatility Foundation Volatility Framework 2.6

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem psscan > notes/infected/psscan.txt
Volatility Foundation Volatility Framework 2.6

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem ps-tree > notes/infected/pstree.txt
Volatility Foundation Volatility Framework 2.6

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem malfind > notes/infected/malfind.txt
Volatility Foundation Volatility Framework 2.6

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem handle > notes/infected/handle.txt
Volatility Foundation Volatility Framework 2.6
ERROR : volatility.debug : You must specify something to do (try -h)

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem handle > notes/baseline/handle.txt
Volatility Foundation Volatility Framework 2.6
ERROR : volatility.debug : You must specify something to do (try -h)

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem amcache > notes/infected/amcache.txt
Volatility Foundation Volatility Framework 2.6

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem shimcache > notes/infected/shimcache.txt
Volatility Foundation Volatility Framework 2.6

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem shimcachemem > notes/infected/shimcachemem.txt
Volatility Foundation Volatility Framework 2.6
ERROR : volatility.debug : You must specify something to do (try -h)

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem memdump > notes/infected/memdump.txt
Volatility Foundation Volatility Framework 2.6
ERROR : volatility.debug : Please specify a dump directory (--dump-dir)

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem amcache > notes/baseline/amcache.txt
Volatility Foundation Volatility Framework 2.6

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem shimcache > notes/baseline/shimcache.txt
Volatility Foundation Volatility Framework 2.6

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem shimcachemem > notes/baseline/shimcachemem.txt
Volatility Foundation Volatility Framework 2.6
ERROR : volatility.debug : You must specify something to do (try -h)

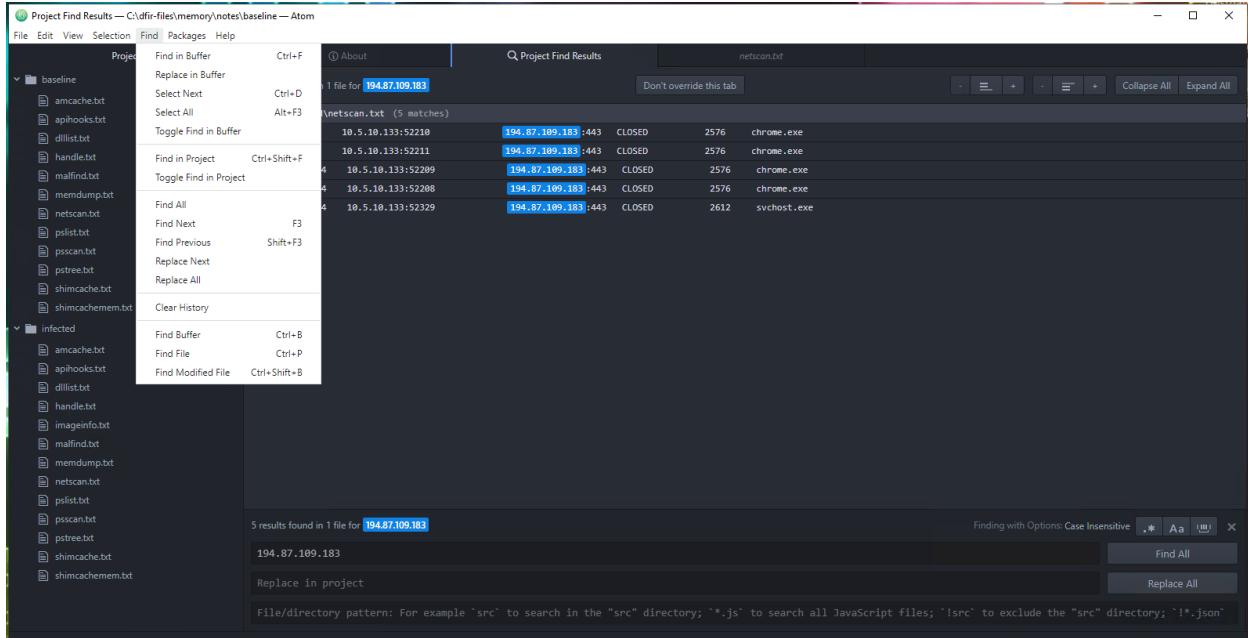
C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem memdump > notes/baseline/memdump.txt
Volatility Foundation Volatility Framework 2.6
ERROR : volatility.debug : Please specify a dump directory (--dump-dir)

C:\dfir-files\memory>
```

To construct the report, you need to bounce back and forth between Atom and Splunk identifying the various processes taking place ie PID & PPID

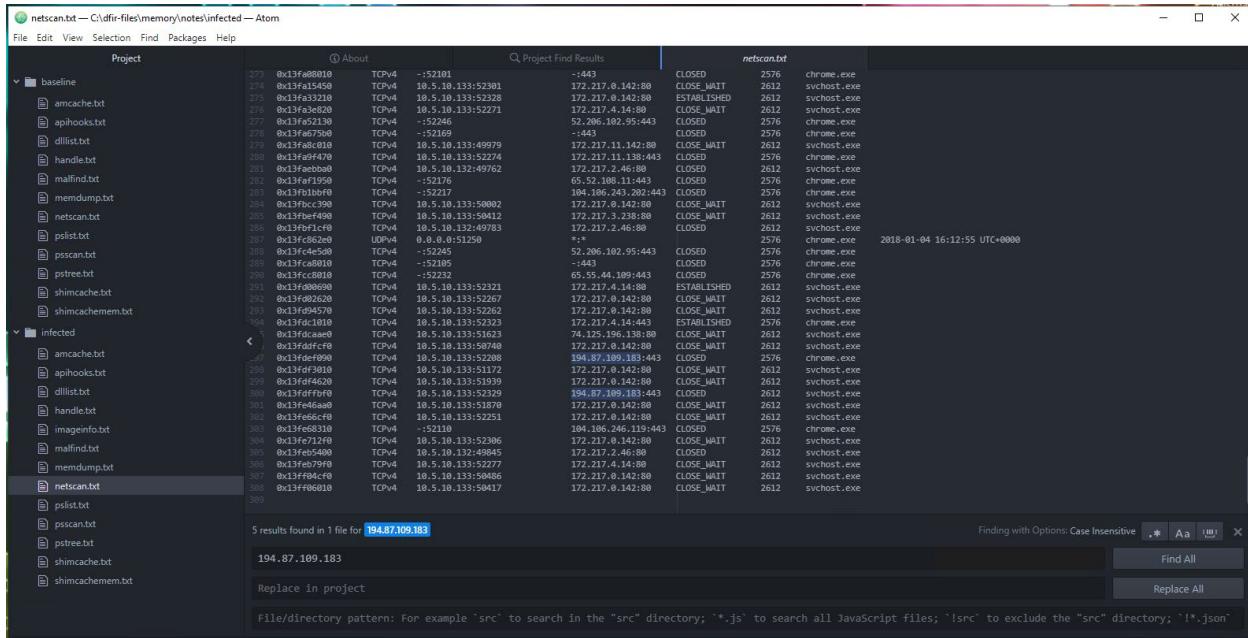
Conduct a search for 194.87.109.183 (known suspect ip address)

Used the Search in Project tab in Find



It returned the above results

Now select any one of the results



1. Examine the line items and take note of the different identifiers such as: Foreign Address, State, Pid, and Owner.

2. Keep access to the Ramnit white paper available to understand what you're looking at.
3. In the search you see that there are two types of Owner...(chrome.exe and svchost.exe)
 - Research the white paper and find...
 - Purpose: Main installer. Drops device driver and launches it as a service. Injects two DLLs into any newly created process instances of svchost.exe or iexplorer.exe
 - Next, the installer copies itself to %UserProfile%\Application Data\[EIGHT PSEUDO-RANDOM CHARACTERS].exe and attempts to locate the path for svchost.exe and iexplore.exe.

Processes

Table 3 details any processes created during the installation routine and their purpose.

Table 3. Processes created during installation

Action	Process	Purpose
Create	svchost.exe or iexplore.exe	Inject DLL_1
Create	svchost.exe or iexplore.exe	Inject DLL_2

- The DLL_1 component acts as a bridge between DLL_2 and a log file. It communicates with DLL_2 using a named pipe to request and receive modules from a remote C&C server. DLL_1 is responsible for storing the received modules in an encrypted form in a log file. It also has the ability to load, decrypt, and execute these external modules.

11 – EXECUTION TREE PROCESS

Open command prompt

Add Volatility modules to folders baseline and infected

```
C:\ Command Prompt
Microsoft Windows [Version 10.0.17763.2366]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\AgencyGuestAdmin>cd\dfir-files\memory

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f infected_Daniel-PC.vmem dumpfiles > notes/infected/dumofiles.txt
Volatility Foundation Volatility Framework 2.6
ERROR : volatility.debug : Please specify a dump directory (--dump-dir)

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f baseline_Daniel-PC.vmem handles > notes/baseline/handles.txt
Volatility Foundation Volatility Framework 2.6

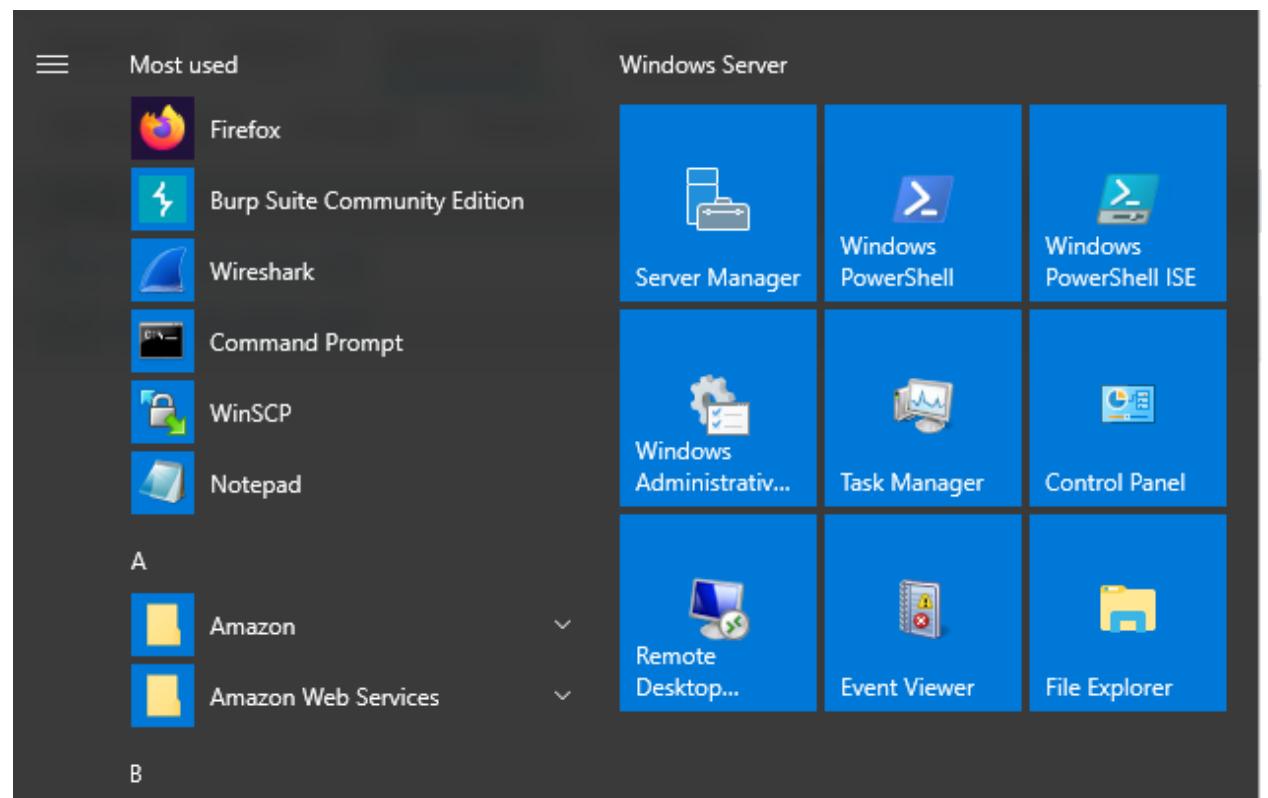
C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f baseline_Daniel-PC.vmem ldrmodules > notes/baseline/ldrmodules.txt
Volatility Foundation Volatility Framework 2.6

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f baseline_Daniel-PC.vmem printkey > notes/baseline/printkey.txt
Volatility Foundation Volatility Framework 2.6

C:\dfir-files\memory>volatility --profile=Win7SP1x64 -f baseline_Daniel-PC.vmem modscan > notes/baseline/modscan.txt
Volatility Foundation Volatility Framework 2.6

C:\dfir-files\memory>
```

Open Remote Desk Top



Remote Desktop Connection

Computer: 10.0.100.123

User name: EC2AMAZ-9LGFK4H\AgencyGuestAdmin

Saved credentials will be used to connect to this computer.
You can [edit](#) or [delete](#) these credentials.

Show Options Connect Help

obommhdf.exe

My Servers

Servers for Task 4: Examine a Compromised Host's Memory

Cyber Team 10's forensics server

Conduct your forensic analysis on this remote Windows machine. You will need to use the Remote Desktop Connection to do so.

IP: 10.0.100.123
Username: AgencyGuestAdmin
Password: Vt3iXeqW38iwG2GUkuQs

Open Atom

Open Splunk

Amazon WorkSpaces View Settings Support

10.0.100.123 - Remote Desktop Connection

Project Find Results — C:\dfr\file\memory\notes\baseline — Atom

File Edit View Selection Find Packages Help

New Search

Events (1) Patterns Statistics

Format Timeline — Zoom Out

00:00 Fri Dec 29 2017

Events (1)

Selected Fields

SELECTED FIELDS

- # action 1
- # app 1
- # Computer 1
- # date_zone 1
- # dest 1
- # dvc 1
- # EventCode 1
- # EventDescription 1
- # EventID 1
- # extracted_source 1
- # Hashes 1
- # host 1
- # Image 1
- # index 1
- # parent_process 1

Project Find Results

9 results found in 7 files for obommhdf.exe

- baseline\shimcache.txt (2 matches)
 - 75 UTC+0000 17\1\100\123\Users\Daniel\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\obommhdf.exe
 - 75 2017-12-28 22:38:32 UTC+0000 17\1\100\123\Users\Daniel\AppData\Local\gwawhtn\obommhdf.exe
- infected\utillist.txt (1 match)
 - 1976 obommhdf.exe pid: 3764
- infected\handles.txt (1 match)
 - 12272 \Device\HarddiskVolume2\Users\Maxwing\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\obommhdf.exe
- infected\pslist.txt (1 match)
 - 50 0xfffffa80804597b30 obommhdf.exe 3764 472 0 1 0 2018-01-02 04:12:57
- infected\pscreen.txt (1 match)
 - 0x000000000f997b30 obommhdf.exe 3764 472 0x000000006da80000 2018-01-02 04:12:57 UTC+0000 2018-01-02
- infected\pstree.txt (1 match)
 - 11 0xfffffa80804597b30 obommhdf.exe 3764 472 0 2018-01-02 04:12:57 UTC+0000
- infected\shimcache.txt (2 matches)
 - 75 UTC+0000 17\1\100\123\Users\Daniel\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\obommhdf.exe
 - 75 2017-12-28 22:38:32 UTC+0000 17\1\100\123\Users\Daniel\AppData\Local\gwawhtn\obommhdf.exe

Don't override this tab

Finding

Start point: known event process...bilo400

Set Date range:

The screenshot shows a search interface with a sidebar on the left containing navigation links: Presets, Relative, Date Range (selected), Date & Time Range, and Advanced. The main area displays a date range selector with the following configuration:

- Between: 01/12/2017 and 07/01/2018
- Time range: 00:00:00 to 24:00:00
- An "Apply" button is visible.

Identify proper Event...in this case start at EventID – 1 Process Creation

The screenshot shows a search results page with a timeline visualization. The timeline spans from Fri Dec 1, 2017, to Fri Jan 5, 2018. A single green bar represents an event occurring on Fri Dec 29, 2017. The interface includes a search bar at the top with the query: index=sysmon Computer=Daniel-PC app=*bilo400.exe EventID=1. Below the search bar are tabs for Events (selected), Patterns, Statistics, and Visualization. The Events tab shows a count of 1 event and a time range of 01/12/2017 00:00:00.000 to 08/01/2018 00:00:00.000. The Visualization tab shows the event as a green bar on the timeline.

index=sysmon Computer=Daniel-PC app=*bilo400.exe EventID=1

Identify Process Identification Number

The screenshot shows a search interface with a sidebar on the left listing various fields: host, Image, index, parent_process, parent_process_id, ParentProcessId, process, process_id, ProcessId, SHA256, siem_event_id, source, sourcetype, tag_eventtype, and User. The process_id field is selected, highlighted with a blue border. The main panel displays details for the selected field:

- process_id**: 1 Value, 100% of events. A "Selected" button with "Yes" and "No" options is shown.
- Reports**: Average over time, Maximum value over time, Minimum value over time, Top values, Top values by time, and Rare values.
- Events with this field**: Avg: 2148 Min: 2148 Max: 2148 Std Dev: 0
- Values** table:

Values	Count	%
2148	1	100%

What created bilo400 - Identify Parent Process and Parent Process ID

EventDescription :
 # EventID 1
 a extracted_source 1
 a Hashes 1
 a host 1
 a Image 1
 a index 1
 a parent_process 1
 # parent_process_id 1
 # ParentProcessId 1
 a process 1
 # process_id 1
 # ProcessId 1
 a SHA256 1

EventID 1
 a extracted_source 1
 a Hashes 1
 a host 1
 a Image 1
 a index 1
 a parent_process 1
 # parent_process_id 1
 # ParentProcessId 1
 a process 1
 # process_id 1
 # ProcessId 1
 a SHA256 1
 a siem_event_id 1
 a source 1

parent_process

1 Value, 100% of events Selected Yes No

Reports

[Top values](#) [Top values by time](#) [Rare values](#)

Events with this field

Values	Count	%
C:\Windows\System32\cmd.exe	1	100%

parent_process_id

1 Value, 100% of events Selected Yes No

Reports

[Average over time](#) [Maximum value over time](#) [Minimum value over time](#)

[Top values](#) [Top values by time](#) [Rare values](#)

Events with this field

Avg: 1924 Min: 1924 Max: 1924 Std Dev: 0

Values	Count	%
1924	1	100%

What created cmd.exe PID 1924

To continue backwards....repeat process as above...

What created cmd.exe - Identify Parent Process and Parent Process ID

index=sysmon Computer=Daniel-PC process=*cmd.exe process_id=1924

a extracted_source 1
 a Hashes 1
 a host 1
 a Image 1
 a index 1
 a parent_process 1
 # parent_process_id 1
 # ParentProcessId 1
 a process 1
 # process_id 1
 # ProcessId 1
 a SHA256 1

parent_process

1 Value, 100% of events Selected Yes No

Reports

[Top values](#) [Top values by time](#) [Rare values](#)

Events with this field

Values	Count	%
C:\Windows\explorer.exe	1	100%

EventID 1
 a extracted_source 1
 a Hashes 1
 a host 1
 a Image 1
 a index 1
 a parent_process 1
 # parent_process_id 1
 # ParentProcessId 1
 a process 1
 # process_id 1
 # ProcessId 1
 a SHA256 1
 a siem_event_id 1
 a source 1

parent_process_id

1 Value, 100% of events Selected Yes No

Reports

Average over time	Maximum value over time	Minimum value over time
Top values	Top values by time	Rare values

Events with this field

Avg: 728 **Min:** 728 **Max:** 728 **Std Dev:** 0

Values	Count	%
728	1	100%

To continue backwards....repeat process as above...

What created explorer.exe - Identify Parent Process and Parent Process ID

index=sysmon Computer=Daniel-PC process=*explorer.exe process_id=728

EventID 2
 a extracted_source 1
 a Hashes 4
 a host 1
 a Image 1
 a index 1
 a parent_process 1
 # parent_process_id 1
 # ParentProcessId 1
 a process 1
 # process_id 1
 # ProcessId 1
 a SHA256 4
 EventDescription 1
 EventID 2
 extracted_source 1
 Hashes 4
 host 1
 Image 1
 index 1
 parent_process 1
 parent_process_id 1
 ParentProcessId 1
 process 1
 process_id 1
 ProcessId 1
 SHA256 4
 siem_event_id 4
 source 1

parent_process

1 Value, 25% of events Selected Yes No

Reports

Top values	Top values by time	Rare values
Events with this field		

Values	Count	%
C:\Windows\System32\userinit.exe	1	100%

parent_process_id

1 Value, 25% of events Selected Yes No

Reports

Average over time	Maximum value over time	Minimum value over time
Top values	Top values by time	Rare values

Events with this field

Avg: 2364 **Min:** 2364 **Max:** 2364 **Std Dev:** 0

Values	Count	%
2364	1	100%

To continue backwards....continue to repeat process as above...until you've reach the stopping point or beginning...

What created explorer.exe - Identify Parent Process and Parent Process ID

index=sysmon Computer=Daniel-PC process=*userinit.exe process_id=2364

parent_process

1 Value, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
C:\Windows\System32\winlogon.exe	1	100%

parent_process_id

1 Value, 100% of events

Selected Yes No

Reports

Average over time Maximum value over time Minimum value over time

Top values Top values by time Rare values

Events with this field

Avg: 1420 Min: 1420 Max: 1420 Std Dev: 0

Values	Count	%
1420	1	100%

To continue forward to discover what happens next: example obommhdf as start point

Set correct timeline

Search correct Event

index=sysmon Computer=Daniel-PC app=*obommhdf.exe EventID=1

New Search

Save As Close

Index: sysmon Computer=Daniel-PC app=*obommhdf.exe EventID=1

4 events (29/12/2017 00:00:00.000 to 08/01/2018 00:00:00.000) No Event Sampling

Events (4) Patterns Statistics Visualization

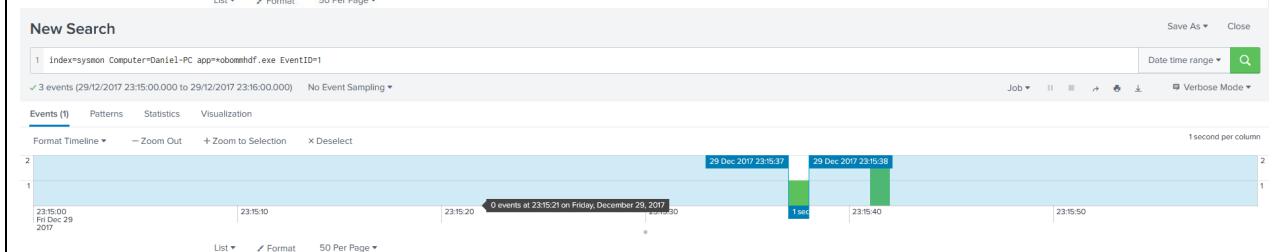
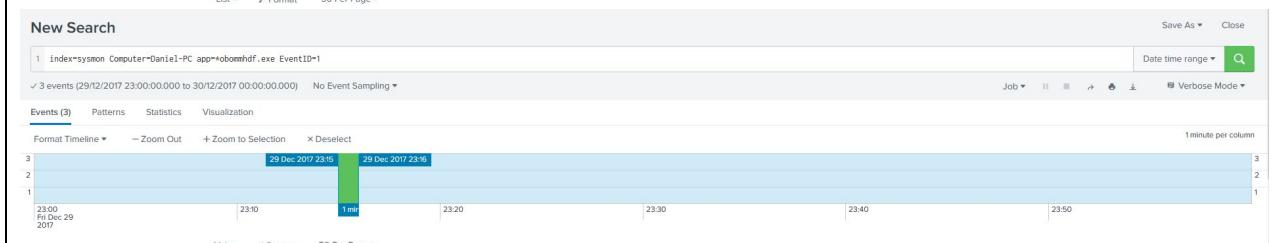
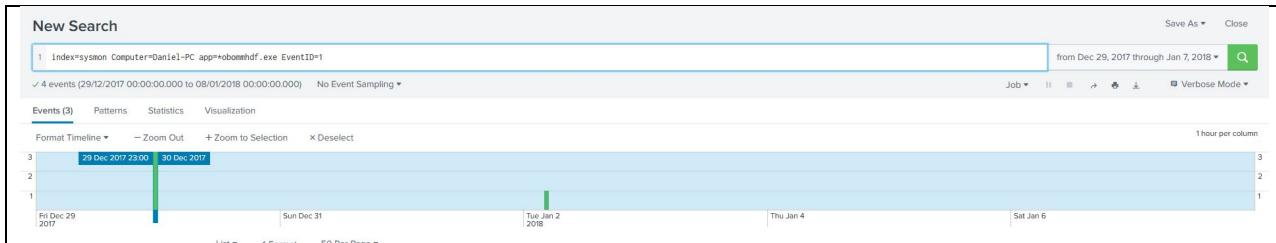
Format Timeline - Zoom Out + Zoom to Selection Deselect

1 hour per column

3
2
1

Fri Dec 29 2017 Sun Dec 31 2017 Tue Jan 2 2018 Thu Jan 4 2018 Sat Jan 6 2018

Zero in on (for this example the first instance) by zooming in to single event



As before in the earlier steps discover what created each step working backwards...
To continue working forward to determine what happened after the event.

Set Splunk timeline

Will work with the first obommhfd.exe first

New Search

1 index=ssymon Computer=Daniel1-PC app=robomhdf.exe EventID=1

✓ 3 events (29/12/2017 00:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling ▾

Events (3) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection X Deselect

1 hour per column

Zoom in

New Search

1 Index=ssymon Computer=Daniel1-PC app=robomhdf.exe EventID=1

✓ 3 events (29/12/2017 23:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling ▾

Events (3) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection X Deselect

1 minute per column

Zoom in

New Search

1 index=ssymon Computer=Daniel1-PC app=robomhdf.exe EventID=1

✓ 3 events (29/12/2017 23:15:00.000 to 29/12/2017 23:16:00.000) No Event Sampling ▾

Events (3) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection X Deselect

1 second per column

Zoom in

New Search

1 index=ssymon Computer=Daniel1-PC app=robomhdf.exe EventID=1

✓ 1 event (29/12/2017 23:15:37:000 to 29/12/2017 23:15:38:000) No Event Sampling ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection X Deselect

10 milliseconds per column

1 Event check process ID

α Hashes 1

- α host 1
- α Image 1
- α index 1
- α parent_process 1
- # parent_process_id 1
- # ParentProcessId 1
- α process 1
- # process_id 1
- # ProcessId 1
- α SHA256 1
- α siem_event_id 1
- α source 1
- α sourcetype 1
- α tag__eventtype 1
- α User 1

process_id

1 Value, 100% of events

Selected Yes No

Reports

Average over time	Maximum value over time	Minimum value over time
Top values	Top values by time	Rare values

Events with this field

Avg: 2292 **Min:** 2292 **Max:** 2292 **Std Dev:** 0

Values	Count	%
2292	1	100%

Check Parent Process

```
# EventID 1
# extracted_source 1
# Hashes 1
# host 1
# Image 1
# index 1
# parent_process 1
# parent_process_id 1
# ParentProcessId 1
# process 1
# process_id 1
# ProcessId 1
# SHA256 1
```

parent_process

1 Value, 100% of events

Selected

Reports

[Top values](#) [Top values by time](#) [Rare values](#)

Events with this field

Values	Count	%
C:\Windows\System32\winlogon.exe	1	100%

Check Parent Process ID

```
# EventDescription 1
# EventID 1
# extracted_source 1
# Hashes 1
# host 1
# Image 1
# index 1
# parent_process 1
# parent_process_id 1
# ParentProcessId 1
# process 1
# process_id 1
# ProcessId 1
# SHA256 1
# siem_event_id 1
# source 1
# sourcetype 1
```

parent_process_id

1 Value, 100% of events

Selected

Reports

[Average over time](#) [Maximum value over time](#) [Minimum value over time](#)

[Top values](#) [Top values by time](#) [Rare values](#)

Events with this field

Avg: 492 Min: 492 Max: 492 Std Dev: 0

Values	Count	%
492	1	100%

Winlogon is as far as is needed but If you wanted to continue back...

Edit search to winlogon and process 492

New Search

1 index=syamon Computer:Daniel1-PC process==winlogon.exe process_id=492

1 event (29/12/2017 23:15:00.000 to 29/12/2017 23:16:00.000) No Event Sampling ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ [Zoom Out](#) [+ Zoom to Selection](#) [Deselect](#)

1 second per column

23:15:00 Fri Dec 29 2017 23:15:10 23:15:20 23:15:29 23:15:30 23:15:40 23:15:50

Check Parent Process

```
# EventID 1
# extracted_source 1
# Hashes 1
# host 1
# Image 1
# index 1
# parent_process 1
# parent_process_id 1
# ParentProcessId 1
# process 1
# process_id 1
# ProcessId 1
# SHA256 1
```

parent_process

1 Value, 100% of events

Selected

Reports

[Top values](#) [Top values by time](#) [Rare values](#)

Events with this field

Values	Count	%
C:\Windows\System32\smss.exe	1	100%

Check Parent Process ID

```
# EventID 1
a extracted_source 1
a Hashes 1
a host 1
a Image 1
a index 1
a parent_process 1
# parent_process_id 1
# ParentProcessId 1
a process 1
# process_id 1
# ProcessId 1
a SHA256 1
a siem_event_id 1
a source 1
```

parent_process_id

1 Value, 100% of events

Selected

Reports

Average over time Maximum value over time Minimum value over time

Top values

Top values by time

Rare values

Events with this field

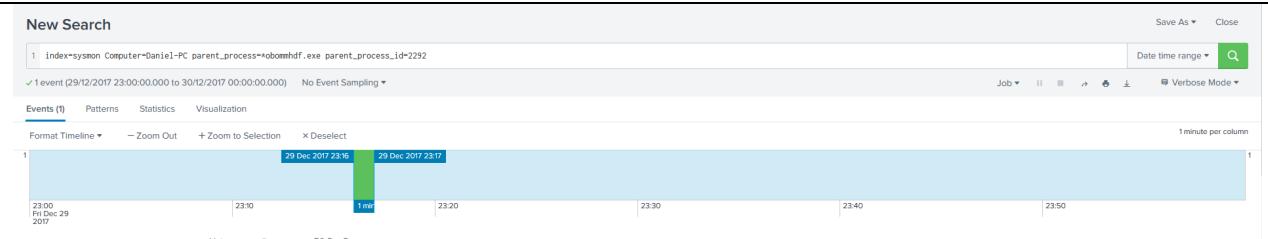
Avg: 396 Min: 396 Max: 396 Std Dev: 0

Values	Count	%
396	1	100%

Continue all the way back system at a later time for interest...as per the above steps

Now move forward with obommhdf.exe to see if it created any children...shift the search from app= to parent process

Be sure to zoom out enough to open the timeline.



Check the process

```
a host 1
a Image 1
a index 1
a parent_process 1
# parent_process_id 1
# ParentProcessId 1
a process 1
# process_id 1
# ProcessId 1
a SHA256 1
a siem_event_id 1
a source 1
a sourcetype 1
```

process

1 Value, 100% of events

Selected

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
xwgrttj1.exe	1	100%

Check Process ID

```
a Hashes 1
a host 1
a Image 1
a index 1
a parent_process 1
# parent_process_id 1
# ParentProcessId 1
a process 1
# process_id 1
# ProcessId 1
a SHA256 1
a siem_event_id 1
a source 1
a sourcetype 1
a tag__eventtype 1
a User 1
```

process_id

1 Value, 100% of events Selected Yes No

Reports

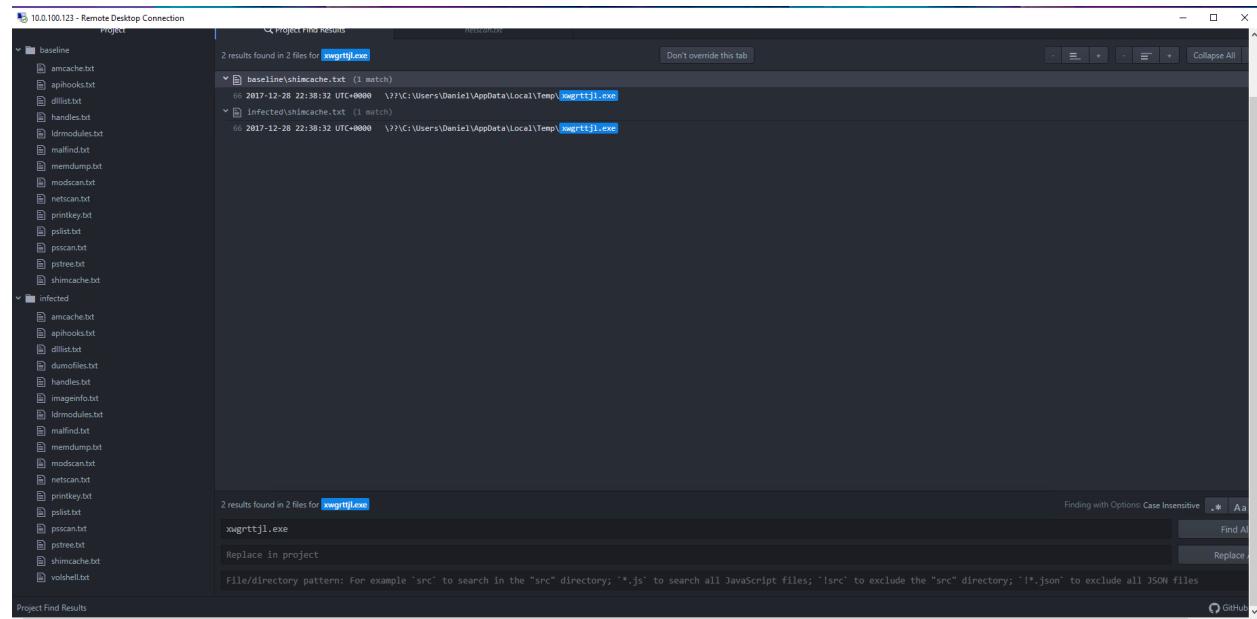
Average over time	Maximum value over time	Minimum value over time
Top values	Top values by time	Rare values

Events with this field

Avg: 3804 **Min:** 3804 **Max:** 3804 **Std Dev:** 0

Values	Count	%
3804	1	100%

Now copy xwgrttjl.exe and go into Atom and search project



Shows up in new module shimcache

Click onto line item and it opens up

55	2009-07-17 01:35:35 UTC+0000	\??\C:\Windows\System32\WBEM\WMI2\p3\WV.exe
59	2010-11-21 03:25:56 UTC+0000	\??\C:\Windows\System32\sppsvc.exe
60	2009-07-14 01:39:48 UTC+0000	\??\C:\Windows\system32\tracert.exe
61	2009-07-14 01:14:35 UTC+0000	\??\C:\Windows\SysWOW64\sdbinst.exe
62	2009-07-14 01:14:35 UTC+0000	\??\C:\Windows\system32\sdbinst.exe
63	2009-07-14 01:14:41 UTC+0000	\??\C:\Windows\SysWOW64\svchost.exe
64	2009-07-14 01:14:41 UTC+0000	\??\C:\Windows\system32\svchost.exe
65	2017-12-28 22:38:32 UTC+0000	\??\C:\Users\Daniel\AppData\Local\Temp\Low\fghroxg.exe
66	2017-12-28 22:38:32 UTC+0000	\??\C:\Users\Daniel\AppData\Local\Temp\xwgrttjl.exe
67	2009-07-14 01:39:21 UTC+0000	\??\C:\Windows\System32\msdtc.exe
68	2017-11-29 18:15:08 UTC+0000	\??\C:\Program Files\SplunkUniversalForwarder\bin\splunk-winevtlog.exe
69	2010-11-21 03:25:05 UTC+0000	\??\C:\Program Files\Windows Media Player\wmpnetwk.exe
70	2017-11-29 18:15:06 UTC+0000	\??\C:\Program Files\SplunkUniversalForwarder\bin\splunk-perfmon.exe
71	2009-07-14 01:39:37 UTC+0000	\??\C:\Windows\system32\SearchIndexer.exe
72	2010-11-21 03:23:48 UTC+0000	\??\C:\Windows\System32\prnfldr.dll

A new 8-character name appears...
fgkhroxg.exe

Now do the dance between Splunk and Atom

Copy fgkhroxg.exe and go into Splunk to see if there is any evidence of it

Save existing search (duplicate tab) before moving onto the new...

The screenshot shows the Splunk 7.2.3 interface. A search bar at the top contains the query "fgkhroxg.exe". Below the search bar, a timeline visualization shows event counts over time, with a green bar indicating activity around December 29, 2017. The main pane displays the results of the search, which found 12 events from December 29, 2017, to January 1, 2018.

Check event codes with this file

The screenshot shows the "EventCode" report for the selected file. It indicates that there are 4 values representing 100% of the events. The report includes sections for Reports (Average over time, Maximum value over time, Minimum value over time, Top values, Top values by time, Rare values), and Events with this field. The summary statistics are: Avg: 6.333333333333333, Min: 1, Max: 11, Std Dev: 3.1139957766460924. The table below shows the distribution of event codes:

Values	Count	%
7	6	50%
1	2	16.667%
11	2	16.667%
5	2	16.667%

Event Code 11 – probably when this file showed up

The screenshot shows the Splunk interface again, this time with a search for "fgkhroxg.exe EventCode=11". The results show 2 events, both occurring on December 29, 2017. The timeline visualization highlights the event count for that day.

i	Time	Event
v	29/12/2017 23:16:32.205	,"Daniel-PC","2017-12-29 23:16:32.123",,,,,"Microsoft-Windows-Sysmon\Operational",11,Unknown,11,,,,"C:\Users\Daniel\AppData\Local\Temp\xwgrttjl.exe",,,0x8000000000000000,4,,,0,,,,"{C80C5B94-CBC1-5A46-0 com/win/2004/08/events/event">>System>Provider Name='Microsoft-Windows-Sysmon' Guid='{577038F-C22A-43E0-B4C-06F5698FB3D}'><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2017-12-29T23:16:32.20584400Z'>2017-12-29 23:16:32.125</TimeCreated><EventRecordID>30313</EventRecordID><CorrelationId><Execution ProcessID='1528' ThreadID='1204'><Channel>Microsoft-Windows-Sysmon\Operational</Channel><Computer>Daniel-PC</Computer><Security UserID='S-1-5-18'></System><EventData><Data Name='UtcTime'>2017-12-29 23:16:32.125</Data><Data Name='ProcessGuid'>{C80C5B94-CBC1-5A46-0080-0010D370A00}</Data><Data Name='ProcessId'>3804</Data><Data Name='Image'>C:\Users\Daniel\AppData\Local\Temp\xwgrttjl.exe</Data><Data Name='TargetFilename'>C:\Users\Daniel\AppData\Local\Temp\xwgrttjl.exe</Data><Data Name='FileName'>C:\Users\Daniel\appdata\local\temp\xwgrttjl.exe</Data><EventID>11</EventID><EventCode>11</EventCode><EventDescription>Unknown</EventDescription><EventID>11</EventID><Image>C:\Users\Daniel\AppData\Local\Temp\xwgrttjl.exe</Image><ProcessId>3804</ProcessId><action>allowed</action><app>C:\Users\Daniel\AppData\Local\Temp\xwgrttjl.exe</app><date_zone>0</date_zone><dest>Daniel-PC</dest><dvc>Daniel-PC</dvc><extracted_source>Min EventLog:Microsoft-Windows-Sysmon\Operational</extracted_source>

This shows that:

xwgrttjl.exe created fgkhroxg.exe

Now continue forward with original search

New Search

Save As ▾ Close

1 index=ssymon Computer="Daniel-PC" parent_process==obomhdf.exe parent_process_id=2292 Date time range ▾

✓ 1 event (29/12/2017 23:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling ▾ Job ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect 1 minute per column

1 29 Dec 2017 23:16 29 Dec 2017 23:17 1 minute per column

23:00 23:10 23:20 23:30 23:40 23:50

23:00 Fri Dec 29 2017

List ▾ Format 50 Per Page ▾

New Search

Save As ▾ Close

1 index=ssymon Computer="Daniel-PC" parent_process==xxwgrtt1.exe parent_process_id=3804 Date time range ▾

✓ 3 events (29/12/2017 23:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling ▾ Job ▾

Events (3) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect 1 minute per column

3 29 Dec 2017 23:16 29 Dec 2017 23:17 1 minute per column

2 29 Dec 2017 23:16 29 Dec 2017 23:17 1 minute per column

1 29 Dec 2017 23:16 29 Dec 2017 23:17 1 minute per column

23:00 23:10 23:20 23:30 23:40 23:50

23:00 Fri Dec 29 2017

Shows that xwgrttl.exe created 3 things

Selected Fields	EventCode	X
a action 1 a app 2 a Computer 1 # date_zone 1 a dest 1 a dvc 1 # EventCode 1 a EventDescription 1 # EventId 1 a extracted_source 1 a Hashes 2 a host 1 a Image 2 a index 1 a parent_process 1	1 Value, 100% of events	Selected Yes No
Reports		
Average over time	Maximum value over time	Minimum value over time
Top values	Top values by time	Rare values
Events with this field		
Avg: 1 Min: 1 Max: 1 Std Dev: 0		
Values	Count	%
1	3	100%

Check process

```
a Hashes 2
a host 1
a Image 2
a index 1
a parent_process 1
# parent_process_id 1
# ParentProcessId 1
a process 2
# process_id 3
# ProcessId 3
a SHA256 2
a siem_event_id 3
a source 1
a sourcetype 1
a tag__eventtype 1
```

process

2 Values, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
svchost.exe	2	66.667%
sdbinst.exe	1	33.333%

Set time search to list everything chronologically

New Search

1 index=system Computer=Daniel-PC parent_process==xwgrttj1.exe parent_process_id=3884 | table _time process process_id | reverse|

3 events (29/12/2017 23:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling ▾

Events (3) Patterns Statistics (3) Visualization Save As ▾ Close Date time range ▾

100 Per Page ▾ Format Preview ▾

_time	process	process_id
2017-12-29 23:16:32.079	svchost.exe	2156
2017-12-29 23:16:32.206	svchost.exe	2960
2017-12-29 23:16:32.392	sdbinst.exe	3224

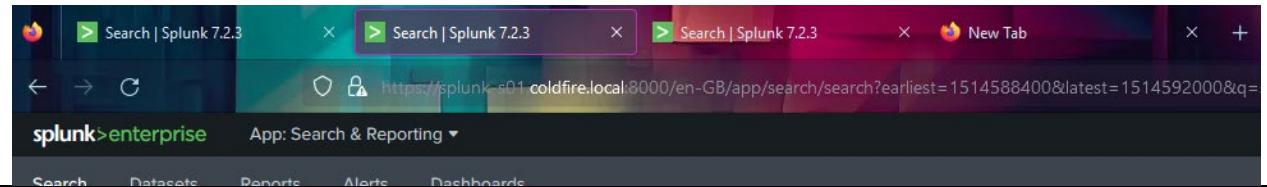
Repeat the above process with each newly identified processes...

svchost.exe (PID: 2156,
svchost.exe (PID: 2960,

sdbinst.exe (PID: 3224,

Now going back to verify that Winlogon didn't create anything else

Duplicate tab to save current search which will be used to continue on moving forward...



Rest time to full day to ensure proper coverage

Change parent to winlogon

New Search

1 index=system Computer=Daniel-PC parent_process==winlogon.exe parent_process_id=494|

3 events (29/12/2017 00:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling ▾

Events (3) Patterns Statistics Visualization Save As ▾ Close during Fri, Dec 29, 2017 ▾

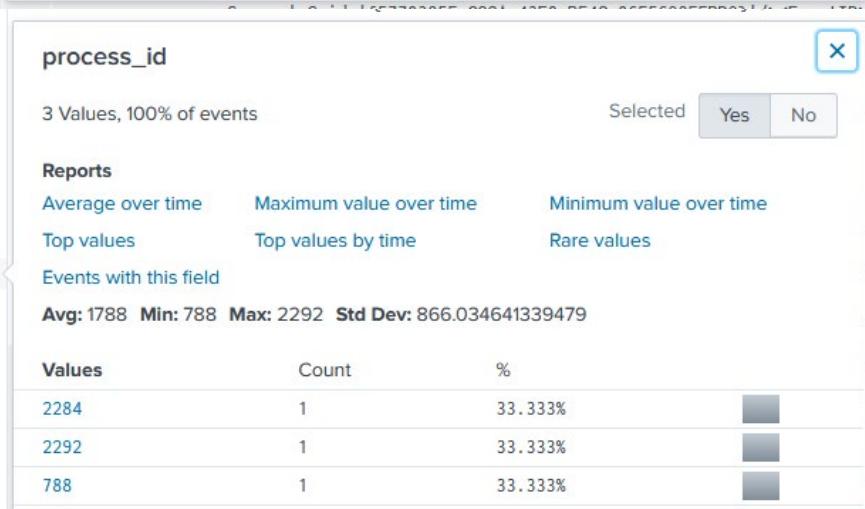
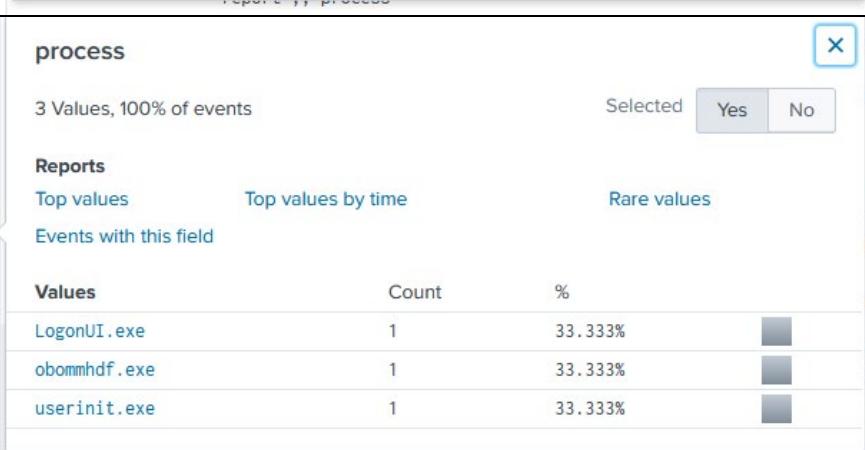
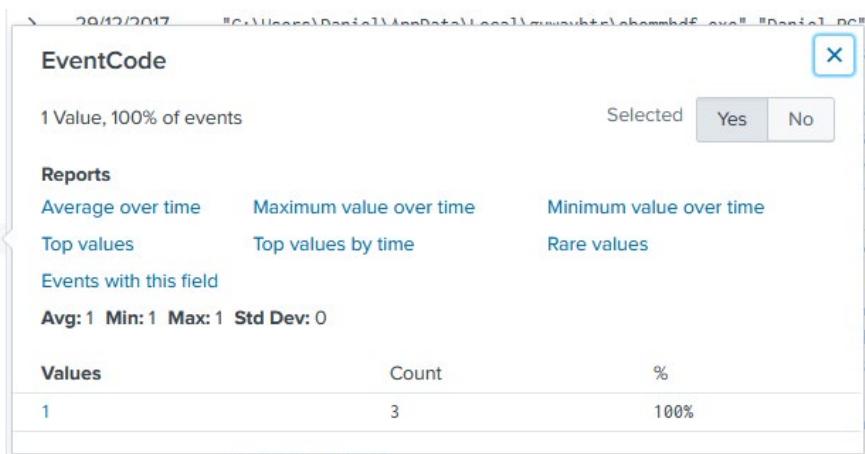
Format Timeline ▾ - Zoom Out + Zoom to Selection X Deselect 1 hour per column

Time	process	process_id
00:00 Fri Dec 29 2017	winlogon.exe	494
04:00		
08:00		
12:00		
16:00		
20:00		

Winlogon created 3 process

SELECTED FIELDS

a action 1
a app 3
a Computer 1
date_zone 1
a dest 1
a dvc 1
EventCode 1
a EventDescription 1
EventID 1
a extracted_source 1
a Hashes 3
a host 1
a Image 3
a index 1
a parent_process 1
a Hashes 3
a host 1
a Image 3
a index 1
a parent_process 1
parent_process_id 1
ParentProcessId 1
a process 3
process_id 3
ProcessId 3
a SHA256 3
a siem_event_id 3
a source 1
a sourcetype 1
a tag_eventtype 1
a User 2
a extracted_source 1
a Hashes 3
a host 1
a Image 3
a index 1
a parent_process 1
parent_process_id 1
ParentProcessId 1
a process 3
process_id 3
ProcessId 3
a SHA256 3
a siem_event_id 3
a source 1
a sourcetype 1
a tag_eventtype 1
a User 2
a user 2



The screenshot shows a search interface for the Symon platform. The search bar contains the query: index=symon Computer=Daniel-PC parent_process=*LogonUI.exe.exe parent_process_id=78. Below the search bar, it says "0 events (29/12/2017 00:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling". The main area displays a timeline with the heading "Events (0)". At the bottom, there are buttons for "Format Timeline", "Zoom Out", "Zoom to Selection", and "Deselect". On the right side, there are buttons for "Job", "Save As", "Close", and "Verbose Mode". A status bar at the bottom right indicates "1 hour per column".

0 processes created by LogonUI.exe

New Search

1 index=ssymon Computer=Daniel-PC parent_process=userinit.exe parent_process_id=284

1 event (29/12/2017 00:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling *

Events (1) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

1 hour per column

00:00 Fri Dec 29 2017 04:00 08:00 12:00 16:00 20:00

1 processes created by userinst.exe

a host 1
a Image 1
a index 1
a parent_process 1
parent_process_id 1
ParentProcessId 1
a process 1
process_id 1
ProcessId 1
a SHA256 1
a siem_event_id 1
a source 1
a sourcetype 1

process

1 Value, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
explorer.exe	1	100%

a Hashes 1
a host 1
a Image 1
a index 1
a parent_process 1
parent_process_id 1
ParentProcessId 1
a process 1
process_id 1
ProcessId 1
a SHA256 1
a siem_event_id 1
a source 1
a sourcetype 1
a tag_eventtype 1
a User 1

process_id

1 Value, 100% of events Selected Yes No

Reports

Average over time Maximum value over time Minimum value over time

Top values Top values by time Rare values

Events with this field

Avg: 2376 Min: 2376 Max: 2376 Std Dev: 0

Values	Count	%
2376	1	100%

Continue search forward with Explorer and 2376

New Search

1 index=ssymon Computer=Daniel-PC parent_process==explorer.exe parent_process_id=2376

1 event (29/12/2017 00:00:00.000 to 30/12/2017 00:00:00.000) No Event Sampling *

Events (1) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

1 hour per column

00:00 Fri Dec 29 2017 04:00 08:00 12:00 16:00 20:00

7 processes were created...

```
a dvc 1
# EventCode 1
a EventDescription 1
# EventID 1
a extracted_source 1
a Hashes 7
a host 1
a Image 8
a index 1
a parent_process 1
# parent_process_id 1
# ParentProcessId 1
a process 7
# process_id 12
# ProcessId 12
a SHA256 7
a siem_event_id 12
a source 1
a sourcetype 1
a tag_eventtype 1
a User 1
```

process

7 Values, 100% of events

Selected Yes No

Reports

Top values

Top values by time

Rare values

Events with this field

Values	Count	%
wmpnscfg.exe	3	25%
chrome.exe	2	16.667%
iexplore.exe	2	16.667%
obommhdf.exe	2	16.667%
explorer.exe	1	8.333%
runonce.exe	1	8.333%
vmtoolsd.exe	1	8.333%

obommhdf.exe reappears...

investigate each process

