

# CATCHING APTS@HOME - HOW TO TAP YOUR HOME INTERNET

Costin G. Raiu, Director, GReAT, Kaspersky  
@craiu

GReAT

Apr 2020

2016  
Rob  
Joyce/TAO  
speech  
@USENIX  
Enigma Conf

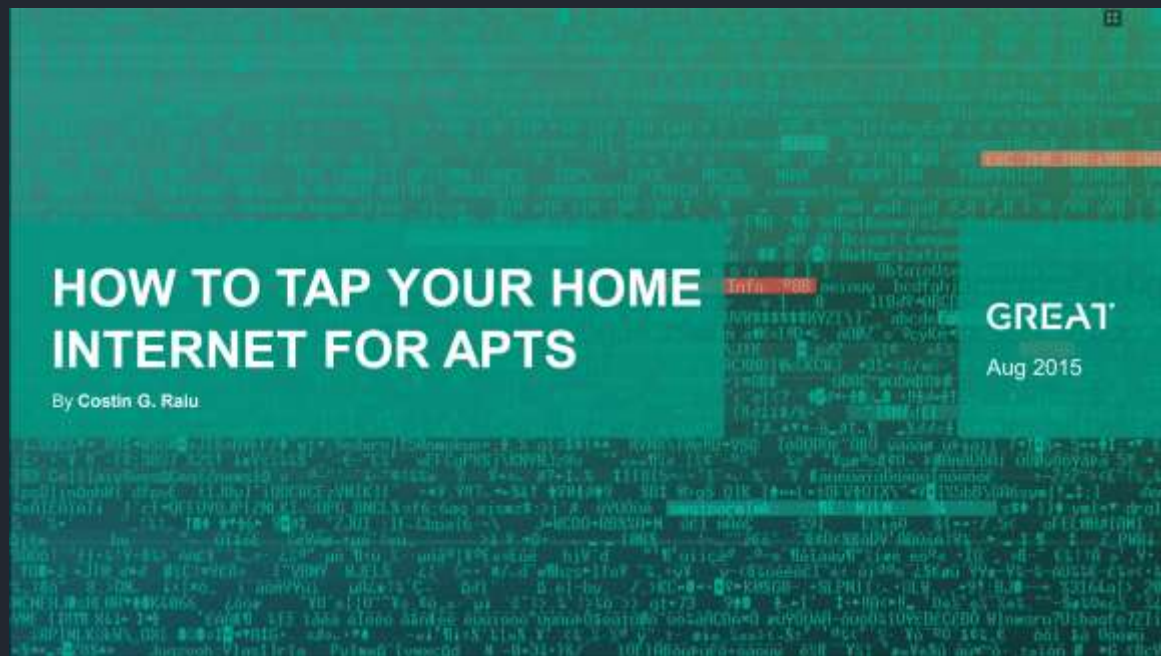


<https://www.youtube.com/watch?v=bDJb8WOJYdA>

*"One of our worst nightmares is that **out-of-band network tap** that really is capturing all the data, understanding anomalous behavior that's going on, and **someone's paying attention** to it. You've gotta know your network. Understand your network, because we're going to."*

— Rob Joyce, TAO, NSA

August 2015





# NETWORK OPSEC

## 2020 #wfh edition

# The basics

- Low profile actors are not a threat
- If hi profile actors want, they can easily infect you. It's a matter of cost justification.

Increased Payouts  
(Servers/Desktops)

**\$1,000,000** - Windows RCE (Zero Click) e.g. via SMB or RDP packets (previously: **\$500,000**)

**\$500,000** - Chrome RCE + SBX (Windows) including a sandbox escape (previously: **\$250,000**)

**\$500,000** - Apache or MS IIS RCE i.e. remote exploits via HTTP(S) requests (previously: **\$250,000**)

**\$250,000** - Outlook RCE i.e. remote exploits via a malicious email (previously: **\$150,000**)

**\$250,000** - PHP or OpenSSL RCE (previously: **\$150,000**)

**\$250,000** - MS Exchange Server RCE (previously: **\$150,000**)

**\$200,000** - VMWare ESXi VM Escape i.e. guest-to-host escape (previously: **\$100,000**)

**\$80,000** - Windows local privilege escalation or sandbox escape (previously: **\$50,000**)

## Our assumptions and objectives

1. We operate on the idea that *we are or will be infected*. This is a fact. When/if this happens, we want to *catch it*.
2. Infection is a matter of cost. We will try to *increase the cost* as much as possible.
3. Routine <> security. We will keep *changing our opsec*, adapting to latest trends.

# 1. How to monitor your home internet for APTs



# Hardware requirements:



Ethernet internet



HUB  
Smart switch



MiniPC



# Ethernet HUB

- Hub != Switch
- Hub on eBay
- \$10..\$15
- 10-100Mbps



NEW LISTING Netgear 4 Port 100BASE-TX fast ethernet hub Model FE104

**\$15.64**  
or Best Offer

From United Kingdom

Customs services and international tracking provided



NetGear (DS108) 8-Ports External Hub Dual Speed Hub 10/100 Mbps T/100 Stackable

**\$9.69**  
Trending at \$14.99  
Buy It Now

From United States

Customs services and international tracking provided



Netgear 4 Port 10/100 Mbps Dual Speed Hub DS104 10base-T Ethernet NO AC Adapter

**\$10.95**  
Trending at \$18.98  
Buy It Now

From United States

Customs services and international tracking provided

# But Costin, we rich people haz gigabit at home ;)

- Meh! Costin's got you covered!
- Instead of HUB:
- Mikrotik switch
- Model: RB260GPS
- \$39.95
- Gigabit switch with management
- Runs SwOS
- Made in Latvia
- Available anywhere



# Another option



Roll over image to zoom in

## NETGEAR GS108E-300UKS 8-Port Gigabit Smart Managed Plus Switch, Prosafe Lifetime Protection

by [NETGEAR](#)



[1,588 customer reviews](#) | [314 answered questions](#)

RRP: ~~£35.99~~

Price: **£33.99** ✓prime

You Save: **£2.00 (6%)**

**Note:** This item is eligible for **click and collect**. [Details](#)

**24 new** from **£33.99**   **5 used** from **£31.61**

Size Name:

8 Port

Style Name: **Smart Managed (Plus)**

Metal Unmanaged

Plastic Unmanaged

Unmanaged

**Smart Managed (Plus)**

Metal Web Managed

Nighthawk Pro Gaming

Plus | L2 Managed

Plastic Web Managed

Smart Managed (Click)

Smart Managed (Plus) + Cable MGMNT

Unmanaged + Cable MGMNT

Pro | L2+ Managed

# MiniPC:



100-300\$

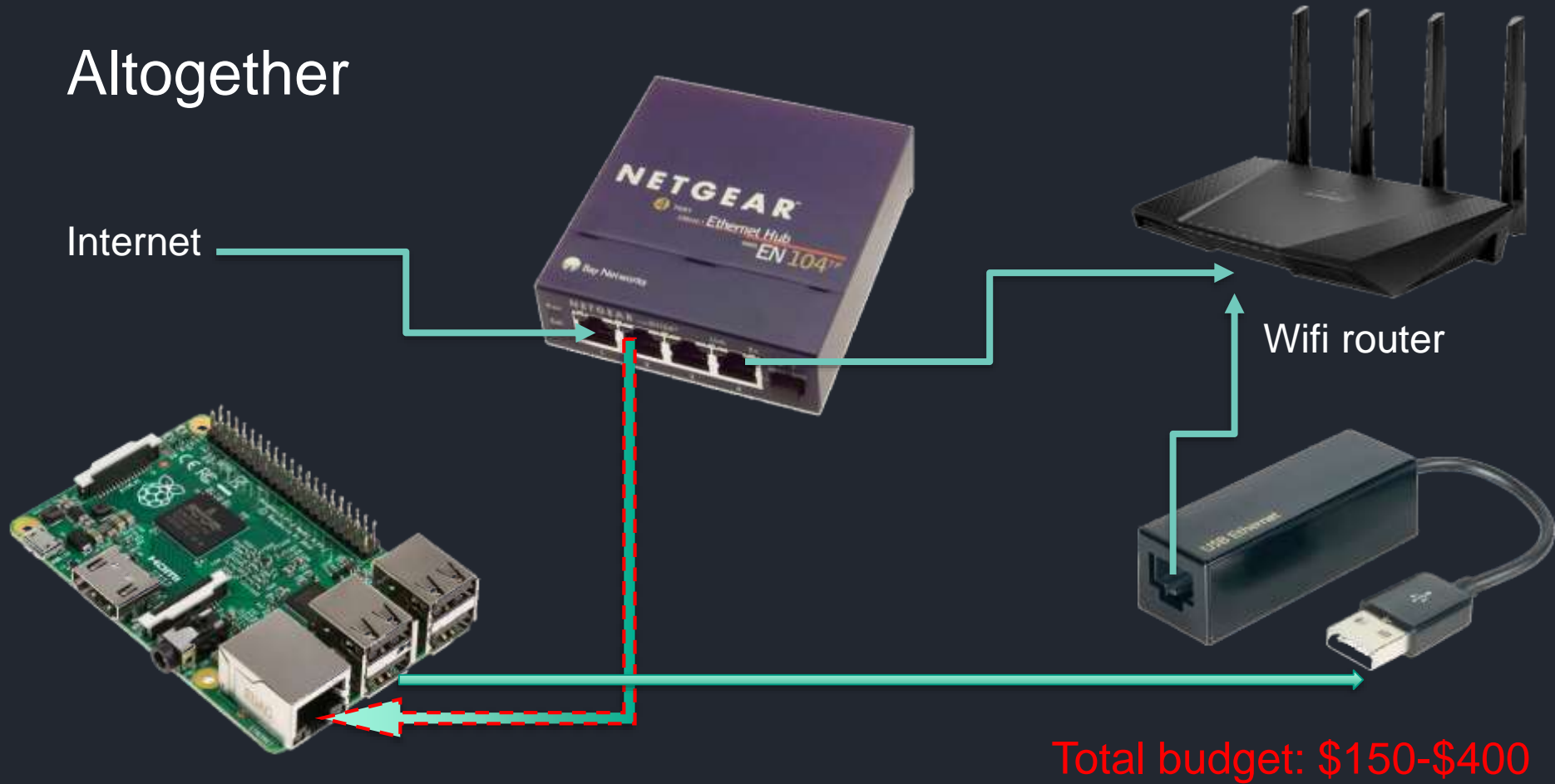


## Optional: USB network card

- Two network connections
- Tap+access
- You can also do wifi access
- I use Edimax and Anker adapters
- \$10-15



# Altogether



# Software

- On the MiniPC, I run Linux
- Suricata 3.x+ (for dns.log)
  - Enable dns.log, http.log, fast.log (extended formats)
  - Enable tls.log
  - Disable stat.log
- pmacctd - log netflow
- tcpdump – if you are paranoid and have disk space 😊
  - Idea: “not port 443”


# Logs

craniu@nuc: /var/log/suricata

```
11/05/2013-08:37:21.721056 [[*] Query TX 6299 [[*] www.forum-executive.ch [[*] AAAA [[*] 89.165.226.197:1035 -> 188.173.1.3:53
11/05/2013-08:37:21.721056 [[*] Response TX 6299 [[*] forum-executive.ch [[*] SOA [[*] TTL 10800 [[*] ns.udagdns.net [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:21.721056 [[*] Query TX ec4d [[*] www.ipu.dk [[*] A [[*] 89.165.226.197:1035 -> 188.173.1.3:53
11/05/2013-08:37:21.790569 [[*] Response TX 5348 [[*] www.iaks.org [[*] A [[*] TTL 20864 [[*] 87.230.41.4 [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:21.790569 [[*] Response TX 5348 [[*] iaks.org [[*] NS [[*] TTL 20864 [[*] ns2.hans.hosteurope.de [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:21.790569 [[*] Response TX 5348 [[*] iaks.org [[*] NS [[*] TTL 20864 [[*] ns1.hans.hosteurope.de [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:21.830444 [[*] Query TX eaee [[*] www.iaks.org [[*] AAAA [[*] 89.165.226.197:1035 -> 188.173.1.3:53
11/05/2013-08:37:21.830444 [[*] Response TX eaee [[*] iaks.org [[*] SOA [[*] TTL 2560 [[*] ns1.hans.hosteurope.de [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:21.830444 [[*] Query TX 2dcd [[*] www.ipu.dk [[*] AAAA [[*] 89.165.226.197:1035 -> 188.173.1.3:53
11/05/2013-08:37:21.856568 [[*] Query TX 22d1 [[*] www.morgenpost.de [[*] AAAA [[*] 89.165.226.197:1035 -> 188.173.1.3:53
11/05/2013-08:37:21.856568 [[*] Response TX 22d1 [[*] www.morgenpost.de [[*] CNAME [[*] TTL 3600 [[*] www.morgenpost.de.edgesuite.net [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:21.856568 [[*] Response TX 22d1 [[*] www.morgenpost.de.edgesuite.net [[*] CNAME [[*] TTL 21600 [[*] a1737.g.akamai.net [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:21.856568 [[*] Response TX 22d1 [[*] g.akamai.net [[*] SOA [[*] TTL 541 [[*] n0g.akamai.net [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:26.923357 [[*] Query TX ce87 [[*] clients4.google.com [[*] A [[*] 89.165.226.197:1035 -> 188.173.1.3:53
11/05/2013-08:37:26.923357 [[*] Response TX ce87 [[*] clients4.google.com [[*] CNAME [[*] TTL 163 [[*] clients1.google.com [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:26.923357 [[*] Response TX ce87 [[*] clients1.google.com [[*] A [[*] TTL 73 [[*] 173.194.70.113 [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:26.923357 [[*] Response TX ce87 [[*] clients1.google.com [[*] A [[*] TTL 73 [[*] 173.194.70.100 [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:26.923357 [[*] Response TX ce87 [[*] clients1.google.com [[*] A [[*] TTL 73 [[*] 173.194.70.139 [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:26.923357 [[*] Response TX ce87 [[*] clients1.google.com [[*] A [[*] TTL 73 [[*] 173.194.70.101 [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:26.923357 [[*] Response TX ce87 [[*] clients1.google.com [[*] A [[*] TTL 73 [[*] 173.194.70.138 [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:26.923357 [[*] Response TX ce87 [[*] clients1.google.com [[*] A [[*] TTL 73 [[*] 173.194.70.102 [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:26.923357 [[*] Response TX ce87 [[*] google.com [[*] NS [[*] TTL 32388 [[*] ns2.google.com [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:26.923357 [[*] Response TX ce87 [[*] google.com [[*] NS [[*] TTL 32388 [[*] ns3.google.com [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:26.923357 [[*] Response TX ce87 [[*] google.com [[*] NS [[*] TTL 32388 [[*] ns4.google.com [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:26.923357 [[*] Response TX ce87 [[*] google.com [[*] NS [[*] TTL 32388 [[*] ns1.google.com [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:26.926898 [[*] Query TX e133 [[*] clients4.google.com [[*] AAAA [[*] 89.165.226.197:1035 -> 188.173.1.3:53
11/05/2013-08:37:26.926898 [[*] Response TX e133 [[*] clients4.google.com [[*] CNAME [[*] TTL 163 [[*] clients1.google.com [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:26.926898 [[*] Response TX e133 [[*] clients1.google.com [[*] AAAA [[*] TTL 219 [[*] 2a00:1450:4001:0c02:0000:0000:0000:000b [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:26.926898 [[*] Response TX e133 [[*] google.com [[*] NS [[*] TTL 32388 [[*] ns3.google.com [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:26.926898 [[*] Response TX e133 [[*] google.com [[*] NS [[*] TTL 32388 [[*] ns1.google.com [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:26.926898 [[*] Response TX e133 [[*] google.com [[*] NS [[*] TTL 32388 [[*] ns4.google.com [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:26.926898 [[*] Response TX e133 [[*] google.com [[*] NS [[*] TTL 32388 [[*] ns2.google.com [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:27.494441 [[*] Query TX 4e27 [[*] p5-few7mimsbglyg-cuvih2ayjxqndhlo-257658-11-v6exp3-ds.metric.gstatic.com [[*] A [[*] 89.165.226.197:1035
11/05/2013-08:37:27.494441 [[*] Response TX 4e27 [[*] p5-few7mimsbglyg-cuvih2ayjxqndhlo-257658-11-v6exp3-ds.metric.gstatic.com [[*] A [[*] TTL 300 [[*] 89.165.226.197:1035
11/05/2013-08:37:27.494441 [[*] Response TX 4e27 [[*].gstatic.com [[*] NS [[*] TTL 32434 [[*] ns3.google.com [[*] 188.173.1.3:53 -> 89.165.226.197:1035
11/05/2013-08:37:27.494441 [[*] Response TX 4e27 [[*].gstatic.com [[*] NS [[*] TTL 32434 [[*] ns4.google.com [[*] 188.173.1.3:53 -> 89.165.226.197:1035
```



# Logs

 craiu@nuc: /var/log/suricata/dns

```
07/29/2015-00:02:02.091788,time-ios.g.aaplimg.com,17.253.52.253
07/29/2015-00:02:02.091791,time-ios.g.aaplimg.com,17.253.54.123
07/29/2015-00:02:02.091788,time-ios.g.aaplimg.com,17.253.54.253
07/29/2015-00:02:02.091788,time-ios.g.aaplimg.com,17.253.52.125
07/29/2015-00:03:27.118282,api.smoot-apple.com.akadns.net,17.252.27.246
07/29/2015-00:03:27.118927,e3191.dscc.akamaiedge.net,23.193.36.97
07/29/2015-00:03:27.121438,googleapis.l.google.com,216.58.211.42
07/29/2015-00:03:27.120061,ssl-google-analytics.l.google.com,173.194.113.126
07/29/2015-00:03:27.122695,rd13p04sa.guzzoni-apple.com.akadns.net,17.135.67.4
07/29/2015-00:06:35.521799,sync.pg.com,168.87.163.21
07/29/2015-00:13:00.300153,e5153.a.akamaiedge.net,23.43.114.199
07/29/2015-00:13:18.629584,p02-imap.mail.me.com.akadns.net,17.172.208.201
07/29/2015-00:14:54.913115,e7971.g.akamaiedge.net,23.45.108.11
07/29/2015-00:16:50.108440,awmdm-116-pdc-dsvs1_pub.airwatchportals.com,205.139.51.183
07/29/2015-00:20:30.860259,r2.sn-pouxga5o-vu2l.googlevideo.com,195.95.178.205
07/29/2015-00:20:30.860801,googleapis.l.google.com,216.58.211.10
07/29/2015-00:20:40.773945,gmail-imap.l.google.com,64.233.184.109
07/29/2015-00:20:40.804553,www.google.com,173.194.67.105
07/29/2015-00:20:40.773945,gmail-imap.l.google.com,64.233.184.108
07/29/2015-00:20:40.804553,www.google.com,173.194.67.104
07/29/2015-00:20:40.804553,www.google.com,173.194.67.103
07/29/2015-00:20:40.797910,caldav.icloud.com.akadns.net,17.110.244.46
07/29/2015-00:20:40.797910,caldav.icloud.com.akadns.net,17.110.240.13
07/29/2015-00:20:40.804553,www.google.com,173.194.67.99
07/29/2015-00:20:40.804553,www.google.com,173.194.67.147
07/29/2015-00:20:40.797910,caldav.icloud.com.akadns.net,17.110.242.14
07/29/2015-00:20:40.804553,www.google.com,173.194.67.106
07/29/2015-00:20:40.797910,caldav.icloud.com.akadns.net,17.110.246.14
```

DATE, HOSTNAME, IP

## countdns.sh

```
#!/bin/bash
```

```
date --date="1 days ago" +"%Y-%m-%d," | tr -d '\n' > todaycount.txt
```

```
cat /var/log/suricata/dns.log | grep `date --date="1 days ago" +"%m/%d/%Y"` | wc -l >>  
todaycount.txt
```

```
cat /var/log/suricata/dns.log | grep `date --date="1 days ago" +"%m/%d/%Y"` | awk -f  
extractdns.awk > /var/log/suricata/dns/dnslog`date +"%y%m%d"` .txt
```

```
cat todaycount.txt >> dnscountsbyday.csv
```

```
cat dnscountsbyday.csv | sort -r -u | head -n 10 | mail -s "DNS queries report - "`date --  
date="1 days ago" +"%m/%d/%Y"` -r yourmail@mail yourmail2@mail
```

# Improvement: Network tap + IOCs

GrEAT APT++ Database   Main Page   Advanced Search   Multientry Tag   Master Tags   Tags History   [Logout]

Showing 1 to 12 of 12 entries   Show 100 entries   Previous 1 Next Search:

Host	IP	Country	Firstseen	Lastseen	Countseen	Tags
	185.149.120.3	PL	2017-10-12 20:33:10	2017-10-12 20:33:10	0	BadRabbit, FlowerDandy
aerketcity.com	38.84.134.15	US	2015-07-23 19:05:58	2015-11-11 16:09:40	2	FlowerDandy, Unknown MALWARE
combativehypocrisy.com	38.84.134.15	US	2016-02-02 19:14:43	2016-02-02 19:14:43	0	FlowerDandy, Unknown MALWARE
dfkiueswbgrfrewfsd.tk	23.253.46.64	US	2018-03-27 03:43:34	2019-10-23 00:00:20	125	FlowerDandy, Unknown MALWARE
dfkiueswbgrfrewfsd.tk	172.97.69.79	US	2017-06-08 18:04:10	2017-07-12 12:34:46	14	FlowerDandy, Unknown MALWARE, FlowerDandy, TOR Exit Node
harddihead.com	38.84.134.15	US	2016-04-13 06:33:52	2016-04-13 06:33:52	0	FlowerDandy, Unknown MALWARE
hollowcondone.com	38.84.134.15	US	2016-02-01 19:23:46	2016-02-01 19:23:46	0	FlowerDandy, Unknown MALWARE
sonline.axitrblsim.com	46.20.1.96	TR	2014-09-19 03:52:28	2014-09-19 03:52:28	0	FlowerDandy, TOR Exit Node
spereptai.com	38.84.134.15	US	2015-07-23 19:37:15	2015-12-16 14:46:44	2	FlowerDandy, Unknown MALWARE
world-teenies.net	91.236.116.50	SE	2013-08-07 20:31:20	2013-11-08 01:44:32	27	FlowerDandy, Unknown MALWARE
www.dfkiueswbgrfrewfsd.tk	172.97.69.79	US	2017-06-28 17:45:05	2017-06-28 17:45:05	0	FlowerDandy, Unknown MALWARE, FlowerDandy, TOR Exit Node

# More improvements

- Heuristics:
  - TLS certificates analysis
    - Self signed certificates
  - DNS queries frequency
  - Unusual domains / TLDs (eg. .pw .cf .tk)
  - Netflow / top traffic IPs



Yeah, but what can  
you find with this?

# Yeah, case 1

## Case 1

```
03/25/2014-20:53:16.449019 [**] Query TX d260 [**] secex.info [**] A [**] 89.165.226.197:1024 -> 188.173.1.3:5
03/25/2014-22:43:56.340202 [**] Query TX c0ef [**] secex.info [**] A [**] 89.165.226.197:1024 -> 94.53.12.30:5
03/25/2014-23:35:22.484217 [**] Query TX c86f [**] secex.info [**] A [**] 89.165.226.197:1024 -> 94.53.12.30:5
03/26/2014-00:47:33.730360 [**] Query TX 1d62 [**] secex.info [**] A [**] 89.165.226.197:1024 -> 94.53.12.30:5
03/26/2014-00:47:33.730360 [**] Response TX 1d62 [**] secex.info [**] A [**] TTL 3221 [**] 64.39.22.193 [**] 9
03/26/2014-00:47:33.730360 [**] Response TX 1d62 [**] secex.info [**] NS [**] TTL 48083 [**] dns1.stabletransi
03/26/2014-00:47:33.730360 [**] Response TX 1d62 [**] secex.info [**] NS [**] TTL 48083 [**] dns2.stabletransi
03/26/2014-01:45:26.773195 [**] Query TX 9277 [**] secex.info [**] A [**] 89.165.226.197:1024 -> 94.53.12.30:5
03/26/2014-19:25:33.212361 [**] Query TX 4ac2 [**] secex.info [**] A [**] 89.165.226.197:1024 -> 188.173.1.3:5
03/26/2014-19:25:33.212361 [**] Response TX 4ac2 [**] secex.info [**] A [**] TTL 3600 [**] 64.39.22.193 [**] 1
03/26/2014-19:25:33.212361 [**] Response TX 4ac2 [**] secex.info [**] NS [**] TTL 20864 [**] dns1.stabletransi
03/26/2014-19:25:33.212361 [**] Response TX 4ac2 [**] secex.info [**] NS [**] TTL 20864 [**] dns2.stabletransi
03/26/2014-19:32:08.995921 [**] Query TX 0508 [**] secex.info [**] A [**] 89.165.226.197:1024 -> 188.173.1.3:5
03/26/2014-19:32:08.995921 [**] Response TX 0508 [**] secex.info [**] A [**] TTL 3204 [**] 64.39.22.193 [**] 1
03/26/2014-19:32:08.995921 [**] Response TX 0508 [**] secex.info [**] NS [**] TTL 20468 [**] dns2.stabletransi
03/26/2014-19:32:08.995921 [**] Response TX 0508 [**] secex.info [**] NS [**] TTL 20468 [**] dns1.stabletransi
03/26/2014-20:31:08.956861 [**] Query TX 5380 [**] secex.info [**] A [**] 89.165.226.197:1024 -> 94.53.12.30:5
03/26/2014-21:23:35.453454 [**] Query TX cff9 [**] secex.info [**] A [**] 89.165.226.197:1024 -> 94.53.12.30:5
03/26/2014-22:28:48.050464 [**] Query TX bed9 [**] secex.info [**] A [**] 89.165.226.197:1024 -> 188.173.1.3:5
03/26/2014-23:36:53.449490 [**] Query TX 077e [**] secex.info [**] A [**] 89.165.226.197:1024 -> 188.173.1.3:5
03/27/2014-00:37:24.665531 [**] Query TX d53e [**] secex.info [**] A [**] 89.165.226.197:1024 -> 94.53.12.30:5
03/27/2014-00:37:24.665531 [**] Response TX d53e [**] secex.info [**] A [**] TTL 2944 [**] 64.39.22.193 [**] 9
03/27/2014-00:37:24.665531 [**] Response TX d53e [**] secex.info [**] NS [**] TTL 30757 [**] dns1.stabletransi
03/27/2014-00:37:24.665531 [**] Response TX d53e [**] secex.info [**] NS [**] TTL 30757 [**] dns2.stabletransi
03/27/2014-01:27:26.702034 [**] Query TX 855e [**] secex.info [**] A [**] 89.165.226.197:1024 -> 94.53.12.30:5
03/27/2014-02:27:57.972108 [**] Query TX c3f0 [**] secex.info [**] A [**] 89.165.226.197:1024 -> 188.173.1.3:5
03/27/2014-03:56:12.720174 [**] Query TX 37c4 [**] secex.info [**] A [**] 89.165.226.197:1024 -> 94.53.12.30:5
```

## The mysterious case of secex.info





## Case 1

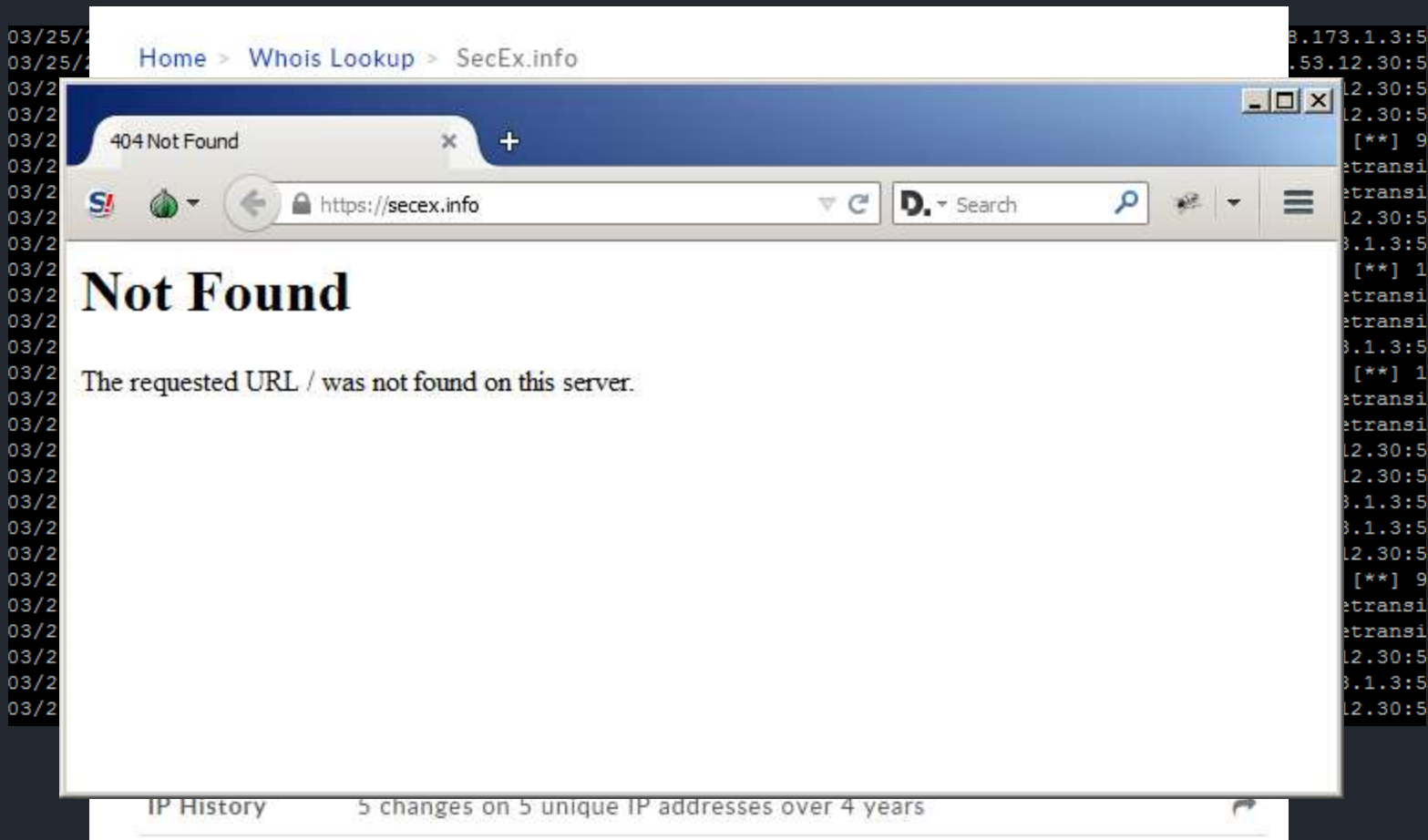
Home > Whois Lookup > SecEx.info

### Whois Record for SecEx.info

#### — Whois & Quick Stats

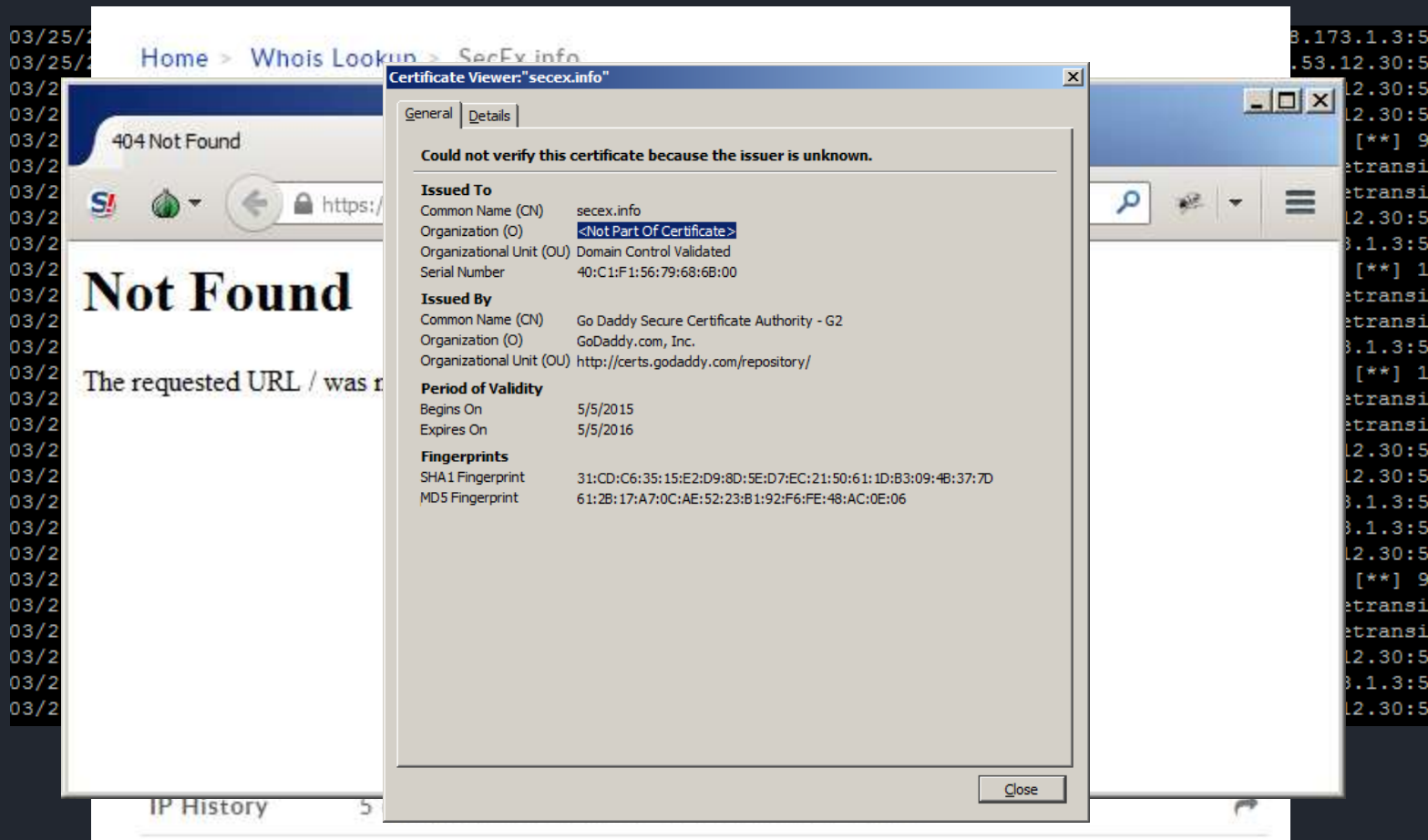
Email	310crescent@gmail.com is associated with ~5 domains robert.static@gmail.com is associated with ~87 domains	↗
Registrant Org	SecEx is associated with ~4 other domains	↗
Dates	Created on 2011-09-02 - Expires on 2015-09-02 - Updated on 2015-05-17	↗
IP Address	204.232.166.114 is hosted on a dedicated server	↗
IP Location	 - Texas - San Antonio	
ASN	 AS27357 RACKSPACE - Rackspace Hosting (registered Feb 20, 2003)	
Domain Status	Registered And No Website	
Whois History	129 records have been archived since 2011-09-04	↗
IP History	5 changes on 5 unique IP addresses over 4 years	↗

# Case 1

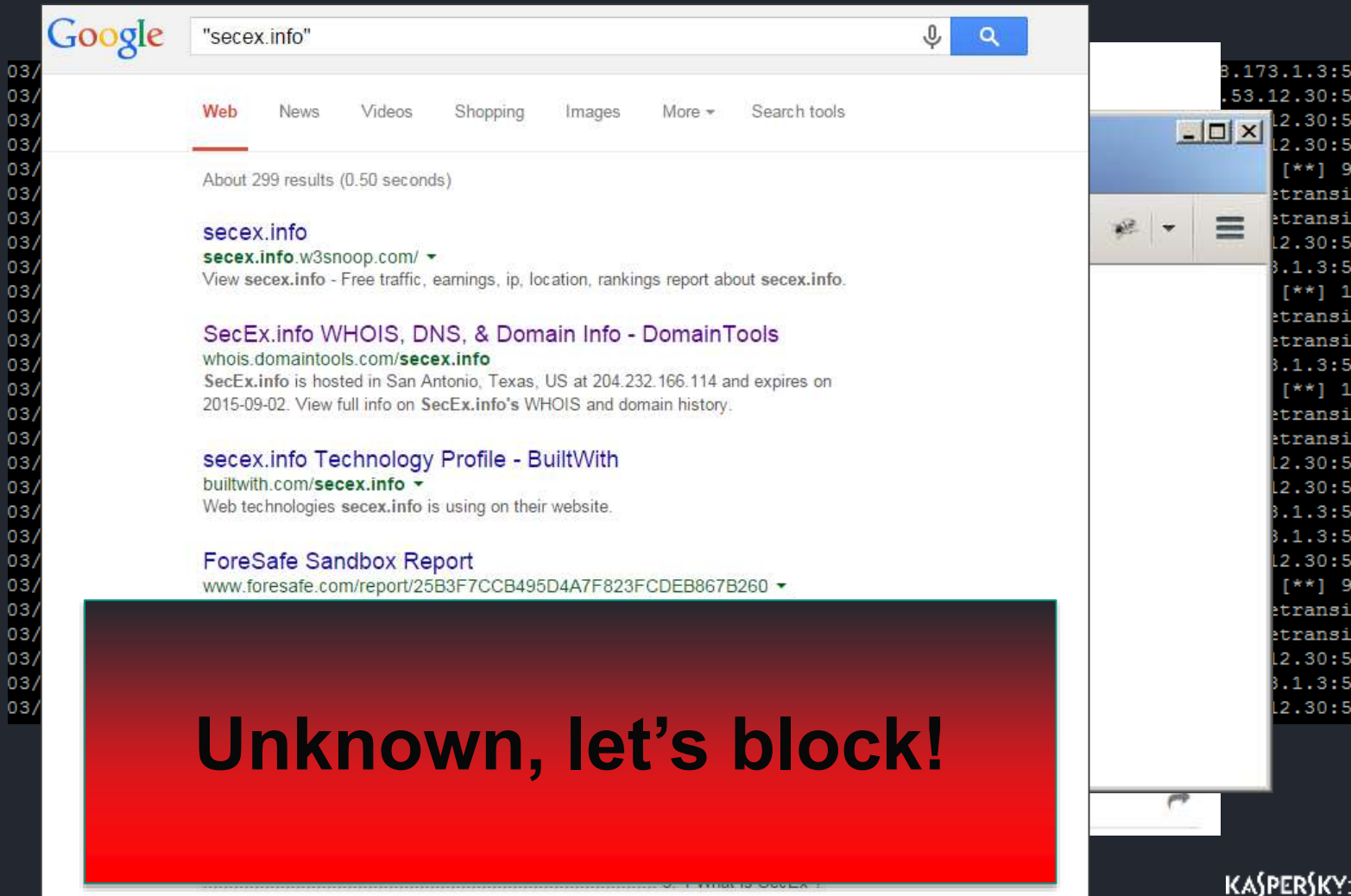




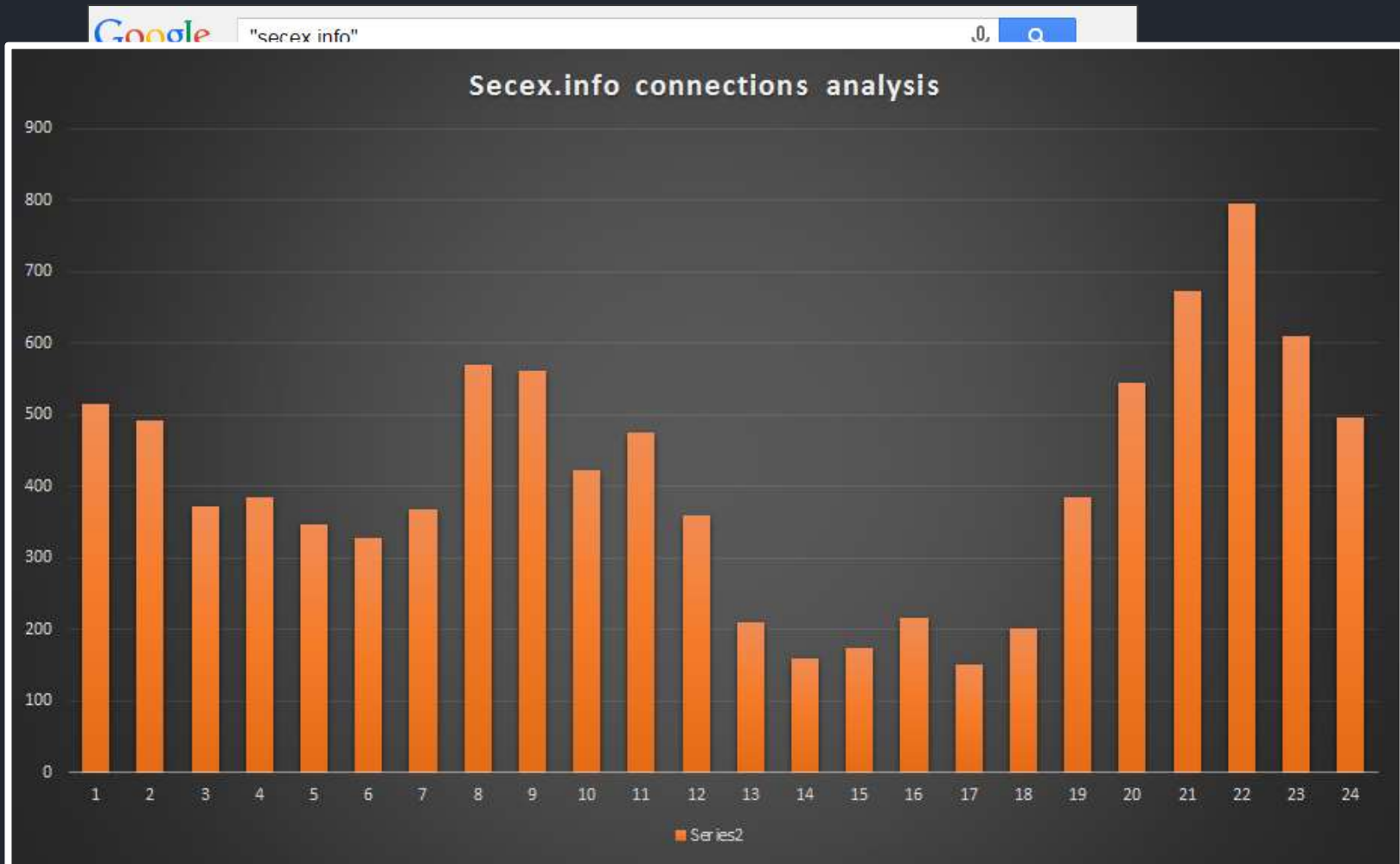
# Case 1



# Case 1



## Case 1



- No password or password hashes leave the device.
- Messages and media are forensically wiped from the device after they expire.



# Yeah, case 2



## Case 2

```
06/11/2014-03:38:57.666493 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:51385 -> 210.109.97.109:8000  
06/11/2014-04:38:58.603684 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:57916 -> 210.109.97.109:8000  
06/11/2014-05:38:59.504213 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:55153 -> 210.109.97.109:8000  
06/11/2014-06:39:00.433509 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:36630 -> 210.109.97.109:8000  
06/11/2014-07:39:01.359301 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:44859 -> 210.109.97.109:8000  
06/11/2014-08:39:02.288958 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:35839 -> 210.109.97.109:8000  
06/11/2014-09:39:03.207482 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:39236 -> 210.109.97.109:8000  
06/11/2014-10:39:04.120225 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:56061 -> 210.109.97.109:8000  
06/11/2014-11:39:05.017428 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:47542 -> 210.109.97.109:8000  
06/11/2014-12:39:05.916219 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:59969 -> 210.109.97.109:8000  
06/11/2014-13:39:06.863390 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:55702 -> 210.109.97.109:8000  
06/11/2014-14:39:07.760172 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:57774 -> 210.109.97.109:8000  
06/11/2014-15:39:08.690577 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:34631 -> 210.109.97.109:8000  
06/11/2014-16:39:09.657620 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:57435 -> 210.109.97.109:8000  
06/11/2014-17:39:10.582555 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:53973 -> 210.109.97.109:8000  
06/11/2014-18:39:11.500111 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:58487 -> 210.109.97.109:8000  
06/11/2014-19:39:12.434941 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:56095 -> 210.109.97.109:8000  
06/11/2014-20:39:13.349394 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:43158 -> 210.109.97.109:8000  
06/11/2014-21:39:14.261706 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:35675 -> 210.109.97.109:8000  
06/11/2014-22:39:15.202095 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:50473 -> 210.109.97.109:8000  
06/11/2014-23:39:16.113425 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:42540 -> 210.109.97.109:8000  
06/12/2014-00:39:17.039920 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:54650 -> 210.109.97.109:8000  
06/12/2014-01:39:17.929828 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:41378 -> 210.109.97.109:8000
```

## Case 2

```
06/11/2014-03:38:57.666493 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:51385 -> 210.109.97.109:8000  
06/11/2014-04:38:58.603684 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:57916 -> 210.109.97.109:8000  
06/11/2014-05:38:59.504213 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:55153 -> 210.109.97.109:8000  
06/11/2014-06:39:00.433509 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:36630 -> 210.109.97.109:8000  
06/11/2014-07:39:01.359301 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:44859 -> 210.109.97.109:8000  
06/11/2014-08:39:02.288958 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:35839 -> 210.109.97.109:8000  
06/11/2014-09:39:03.207482 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]
```

```
04:38:58.603684 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**]  
-> 210.109.97.109:8000  
05:38:59.504213 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**]  
-> 210.109.97.109:8000  
06:39:00.433509 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**]  
-> 210.109.97.109:8000  
07:39:01.359301 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**]  
-> 210.109.97.109:8000  
08:39:02.288958 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**]  
-> 210.109.97.109:8000  
09:39:03.207482 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**]  
-> 210.109.97.109:8000  
10:39:04.120225 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**]  
-> 210.109.97.109:8000  
11:39:05.017428 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**]  
-> 210.109.97.109:8000  
12:39:05.916219 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**]  
-> 210.109.97.109:8000
```



## Case 2

```
06/11/2014-03:38:57.666493 210.109.97.109 [**] /cgi-bin/client.cgi?fqdn=.HOST.&ip=0&serno=001C85200F63&flag=2 [**] Wget [**] <no referer> [**] GET [**]  
5.197:51385 -> 210.109.97.109:8000 [**]  
06/11/2014-04:38:58.603684 210.109.97.109 [**] [**]  
5.197:57916 -> 210.109.97.109:8000 [**]  
06/11/2014-05:38:59.504213 210.109.97.109 [**] [**]
```

```
04:38:58.603684 210.109.97.109 [**]  
-> 210.109.97.109:8000  
05:38:59.504213 210.109.97.109 [**]  
-> 210.109.97.109:8000  
06:39:00.433509 210.109.97.109 [**]  
-> 210.109.97.109:8000  
07:39:01.359301 210.109.97.109 [**]  
-> 210.109.97.109:8000  
08:39:02.288958 210.109.97.109 [**]  
-> 210.109.97.109:8000  
09:39:03.207482 210.109.97.109 [**]  
-> 210.109.97.109:8000  
10:39:04.120225 210.109.97.109 [**]  
-> 210.109.97.109:8000  
11:39:05.017428 210.109.97.109 [**]  
-> 210.109.97.109:8000  
12:39:05.916219 210.109.97.109 [**]  
-> 210.109.97.109:8000
```

## IP Information for 210.109.97.109

### Quick Stats

IP Location	 Korea, Republic Of Seoul Krnic
ASN	 AS9848 GNGAS Enterprise Networks (registered Feb 04, 2000)
Resolve Host	109.0-255.97.109.210.in-addr.arpa
Whois Server	whois.apnic.net
IP Address	210.109.97.109

```
inetnum:      210.109.0.0 - 210.115.255.255  
netname:      KRNIC-KR  
descr:        KRNIC  
descr:        Korea Network Information Center  
country:      KR
```

**OMG, malware C2?!**

```
06/11/2014-06:39:05.017428 210.109.97.109 [**]  
5.197:51385 -> 210.109.97.109:8000 [**]  
06/11/2014-06:39:05.017428 210.109.97.109 [**]  
5.197:51385 -> 210.109.97.109:8000 [**]  
06/11/2014-06:39:05.017428 210.109.97.109 [**]  
5.197:51385 -> 210.109.97.109:8000 [**]  
06/11/2014-06:39:05.017428 210.109.97.109 [**]  
5.197:51385 -> 210.109.97.109:8000 [**]
```

```
*****  
try  
like to  
l  
  
html  
*****
```

## Case 2

```
06/11/2014-03:38:51 5.197:51385 -
06/11/2014-04:04:38 5.197:57916 -
06/11/2014-04:04:38 5.197:57916 -
04:38:58.603684 210.109
-> 210.109.97.109:8000
05:38:59.504213 210.109
-> 210.109.97.109:8000
06:39:00.433509 210.109
-> 210.109.97.109:8000
07:39:01.359301 210.109
-> 210.109.97.109:8000
08:39:02.288958 210.109
-> 210.109.97.109:8000
09:39:03.207482 210.109
-> 210.109.97.109:8000
10:39:04.120225 210.109
-> 210.109.97.109:8000
11:39:05.017428 210.109
-> 210.109.97.109:8000
12:39:05.916219 210.109
-> 210.109.97.109:8000
```

```
06/11/2014-22:51:19 5.197:50473 -
06/11/2014-23:01:19 5.197:42540 -
06/12/2014-00:01:19 5.197:54650 -
06/12/2014-01:01:19 5.197:41378 -
```



```
*] <no referer> [**] GET [**]
referer> [**] GET [**]
referer> [**] GET [**]
```

```
63&flag=2 [**]
63&flag=2 [**]
63&flag=2 [**]
63&flag=2 [**]
63&flag=2 [**]
63&flag=2 [**]
63&flag=2 [**]
63&flag=2 [**]
```

```
referer> [**] GET [**]
referer> [**] GET [**]
referer> [**] GET [**]
referer> [**] GET [**]
```

# Mystery solved, it was the Xtreamer NAS

## Case 2

```
04:38:58.6 -> 210.109.97.109:8000
05:38:59.5 -> 210.109.97.109:8000
06:39:00.4 -> 210.109.97.109:8000
07:39:01.3 -> 210.109.97.109:8000
08:39:02.2 -> 210.109.97.109:8000
09:39:03.2 -> 210.109.97.109:8000
10:39:04.1 -> 210.109.97.109:8000
11:39:05.0 -> 210.109.97.109:8000
12:39:05.916219 210.109.97.109:8000
```

```
p : No Response from Http Server Http : Content Length Error Http : Transfer Encode Error
Http : ManyRedirections Error Http : BadHeader Error Http : Connection TimeOut
Http : File Not Found Http : Unknown Request Http : Unknown Error No Input URL Given
To Wget No Result File Specified for Wget /tmp/ddns.result NS_UPDATE_PASS NS_
DELETE_PASS NS_REGISTER_PASS NS_HOST_AVAIL REG_FAIL NS_NAMEEXIST NS_COMM_FAIL
NS_AUTH_MISMATCH DB_NO_DATA GEN_FAIL 0

Domain = %s SerialNo = %s Command = %c
IpAddress = %s Enter UserId : Enter PassWord : Enter Domain Name :
Enter Serial Number : Enter User Command [Registration : 0] :: [Mod : 1] :
: [Del : 2] : %c http://210.109.97.109:8000/cgi-bin/client.cgi? fqdn= %s %c ip=
serno= flag= /etc/ddns.conf Unable to Open CDisk Proc File org_mac Please Check Pr
oc File Once Again for Mac Address Parameter Line .RM. .HOST. .mvix.net .icuber
.com .ivixcube.com .dane-elec.net .moviecowboy.net .myetrayz.net 0 %.2X%.2X%.2
X%.2X%.2X%.2X eth0 1^ ^0
```

**Buffer overflow in  
response parser ☹️ Let's  
block ze basterds!**

```
06/11/2014-23:51:19 5.197:50473 -
06/11/2014-23:51:19 5.197:42540 -
06/12/2014-00:00:00 5.197:54650 -
06/12/2014-00:00:00 5.197:41378 -
```

```
63&flag=2 [**]
```

```
referer> [**] GET [**]
referer> [**] GET [**]
referer> [**] GET [**]
referer> [**] GET [**]
```



# Next time:

## 2. Increasing the cost

- 2.1 Complicate targeting
- 2.2 Complicate exploitation

# Take away's

- You don't really know what's flowing through your home internet link
- ...unless you tap it!
- Can be done with a relatively simple hardware configuration
- Offers a huge level of defense and awareness

One last thing...

When you elevate the  
cost of SIGINT, you may  
become a HUMINT target



# HAPPY HUNTING! ;)

Stay foolish, stay GReAT!

Stay in touch: @craiu

[www.securelist.com](http://www.securelist.com)