

anubisnetworks™
a BITSIGHT® company



The many faces of Mevade

Martijn Grooten (Virus Bulletin)

@martijn_grooten

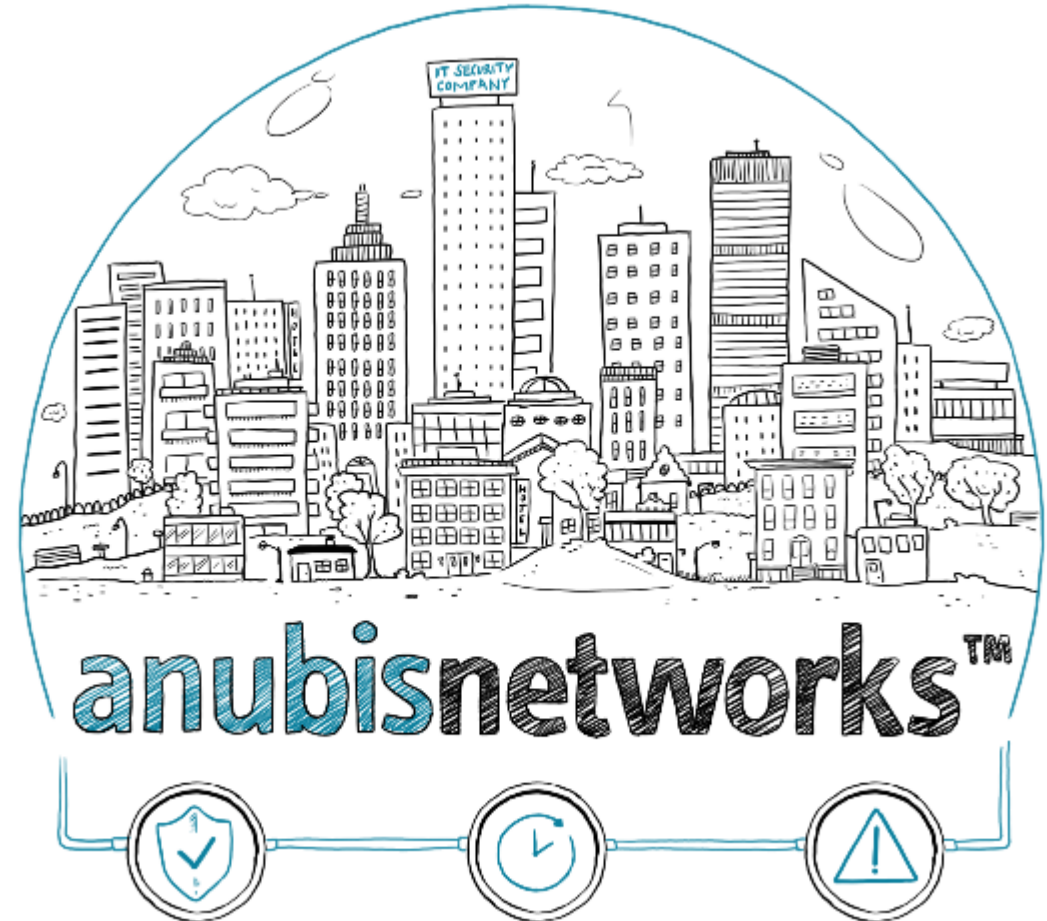
João Gouveia (AnubisNetworks)

@jgouv



> About US!

AnubisNetworks is focused in
Real-time Threat Intelligence



www.anubisnetworks.com

> About Virus Bulletin



Virus Bulletin publishes technical articles, organises an annual security conference and tests security software.



www.virusbtn.com

> Mevade (aka Sefnit, aka SBC)



Martijn Grooten
@martijn_grooten

This is awkward, as I'll give a talk about it next week, but how does one actually pronounce Mevade? Rhymes to 'shade' or as in German?



9:32 PM - 27 Nov 2014

> Mevade vs Regin



> January 2012

[Sign in](#)

Malware Protection Center



☒ Search this blog ☐ Search all blogs

[Home](#)[About](#)[View More Blogs](#)[Resources](#)

TechNet Blogs » Microsoft Malware Protection Center » January '12 MSRT: Win32/Sefnit

January '12 MSRT: Win32/Sefnit

[mmpc2](#)

10 Jan 2012 11:51 AM



0

[Share Article](#)

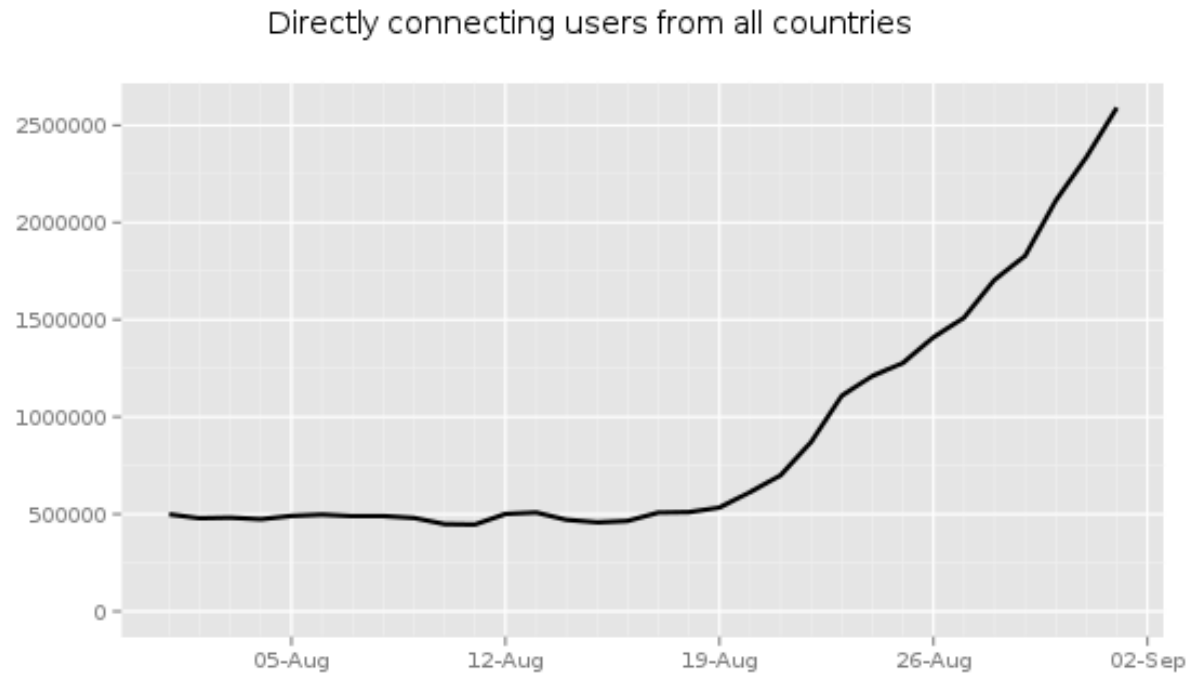
This trojan family moderates and redirects web browser search engine results for Bing, Yahoo! and Google.

The earliest reported variant in this family can be traced back to August 2010. The installation mechanism employed by early samples remains very similar to samples we observe in the wild today. Variants of Sefnit employ the use of a Nullsoft Scriptable Install System (NSIS) dropper to install an obfuscated a dynamic link library (DLL) component. The component is executed by the dropper by using "rundll32.exe" and also will execute during Windows logon.

The obfuscation technique used has changed from the "spaghetti-style" of numerous unconditional branches between small islands of code to one that is "in plain sight". In the following example, we can see the immediate value of 1Bh move via the local variable 'var_1' to the cl register, rather than being moved directly

[Follow Us](#)[@msftmmpc](#)[facebook](#)[Security@Microsoft](#)[Security Newsletter](#)


Tor reports sharp increase in connections from all countries.



All countries?

But I am compelled to point out that your table has one data point that will keep the bellies of conspiracy theorists full for months: the only -- only! -- country that didn't gain was Israel.

--Roger

 **FOX IT**

[Home](#) [About](#) [Back to fox-it.com](#)

SBC [Hosts](#) [Data center](#) [Session User](#) [Sock list](#) [BotUpdate](#) [Bot Update Country](#) [Bot Update Url](#)

Please sign in

1

☐ Remember me

Posted on [September 5, 2013](#) by [ydklijnsma](#)

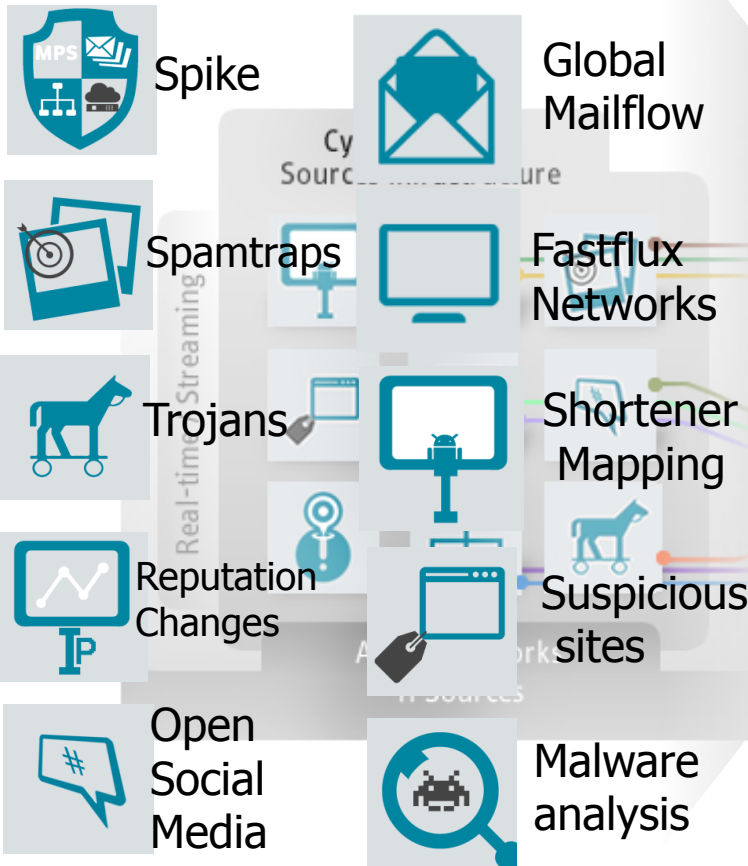
★★★★★ ⓘ 31 Votes

Recently, [Roger Dingledine described](#) a sudden increase in Tor users on the Tor Talk mailinglist. To date there has been a large amount of speculation as to why this may have happened. A large number of articles seem to suggest this to be the result of the recent global espionage events, the evasion of the Pirate Bay

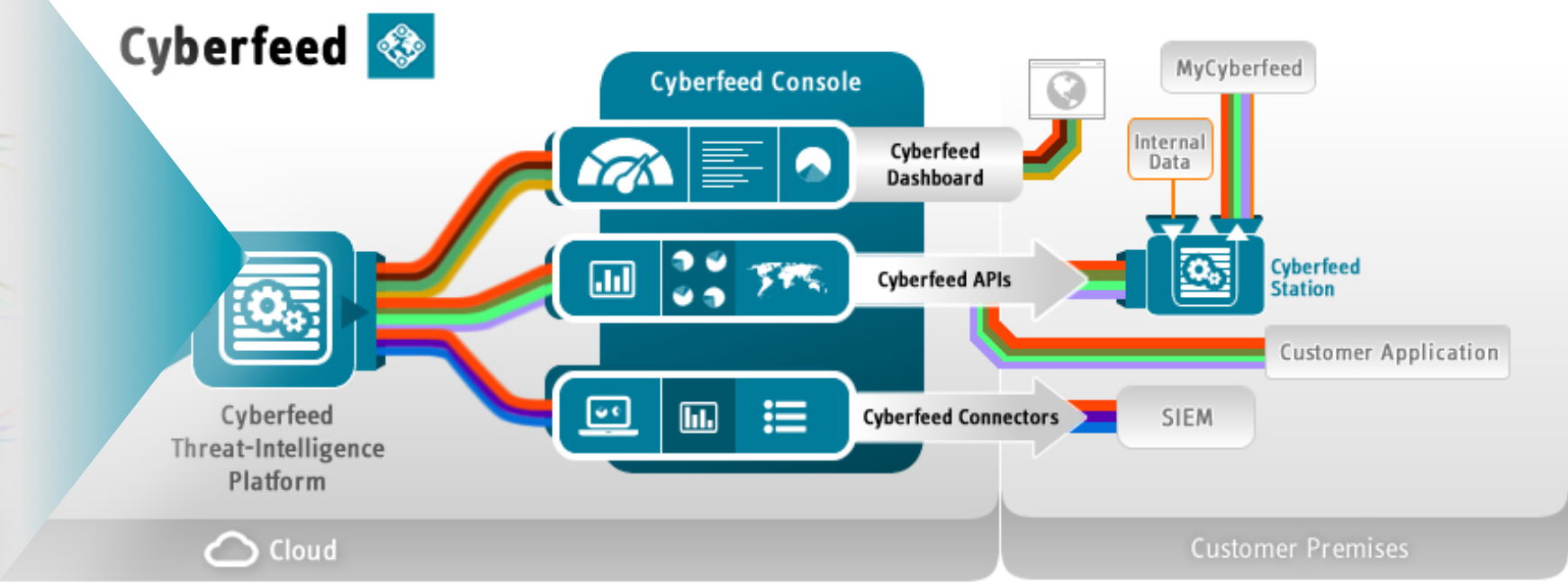
> Cyberfeed Architecture



Security Feeds Available



Cyberfeed



With great power ...



- Streaming, real time, high performance **complex event processor** (CEP)
- Publish subscriber model
- HTTP Rest
- JSON
- Pre/Post processing functions and modules
 - Do something with the data
 - Show it to me in a different way
 - Customize to my own needs



SINKHOLING METHODOLOGY

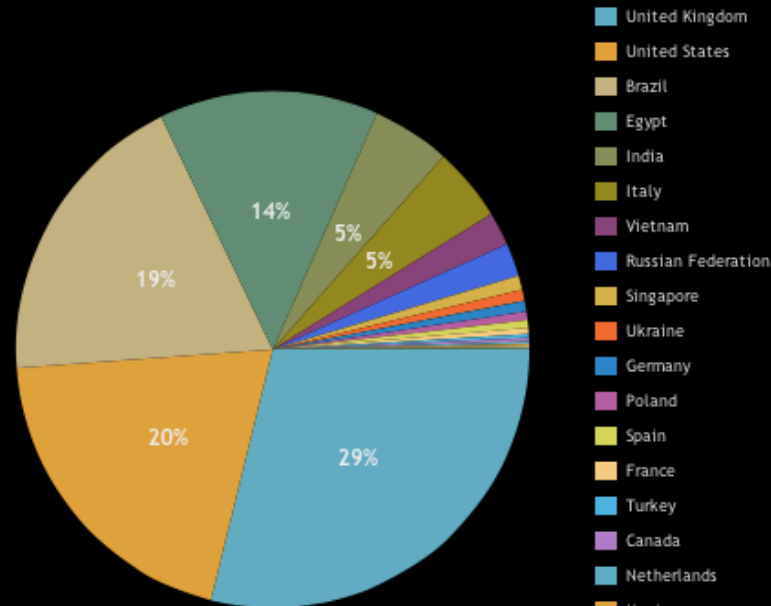
> Sinkholing methodology



Sensors



Anubisnetworks Sensors distribution



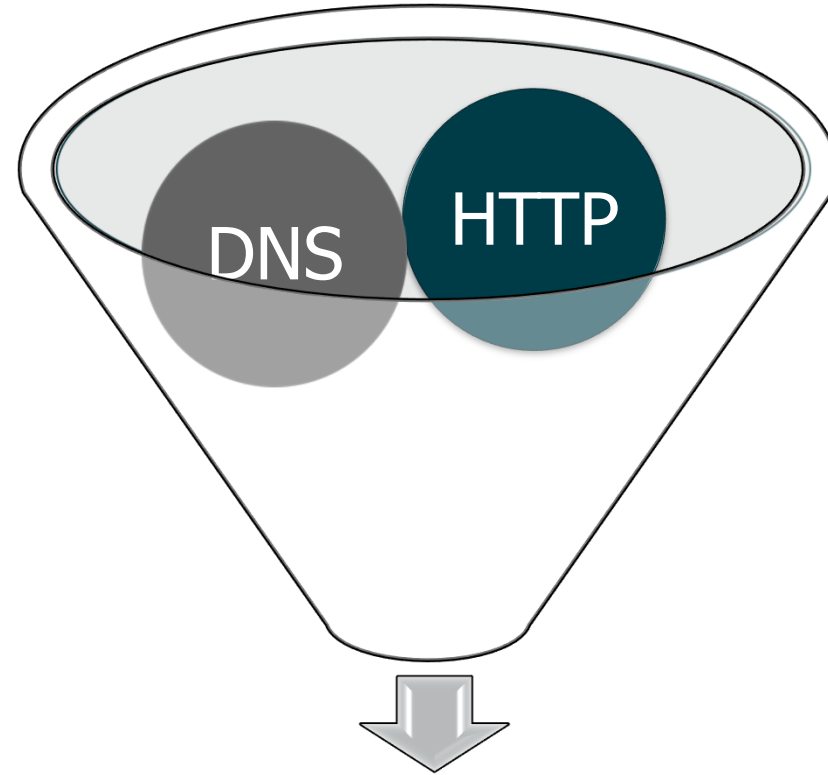
Anubisnetworks Sensors distribution

Name	Value	Status
United Kingdom	384.6605	↑
United States	266.9202	↑
Brazil	251.4452	↑
Egypt	185.3184	↓
India	64.8448	↑
Italy	61.549	↑
Vietnam	28.537	↑
Russian Federation	27.2066	↑
Singapore	11.5442	↑
Ukraine	9.3611	↑
Germany	8.9439	↑
Poland	6.785	↑
Spain	6.5431	↑
France	5.2792	↑
Canada	3.0357	↑
Turkey	2.951	↑
Netherlands	2.1467	↑

> Sinkholing methodology



Sampling



Complex Event Processor

> Sinkholing methodology



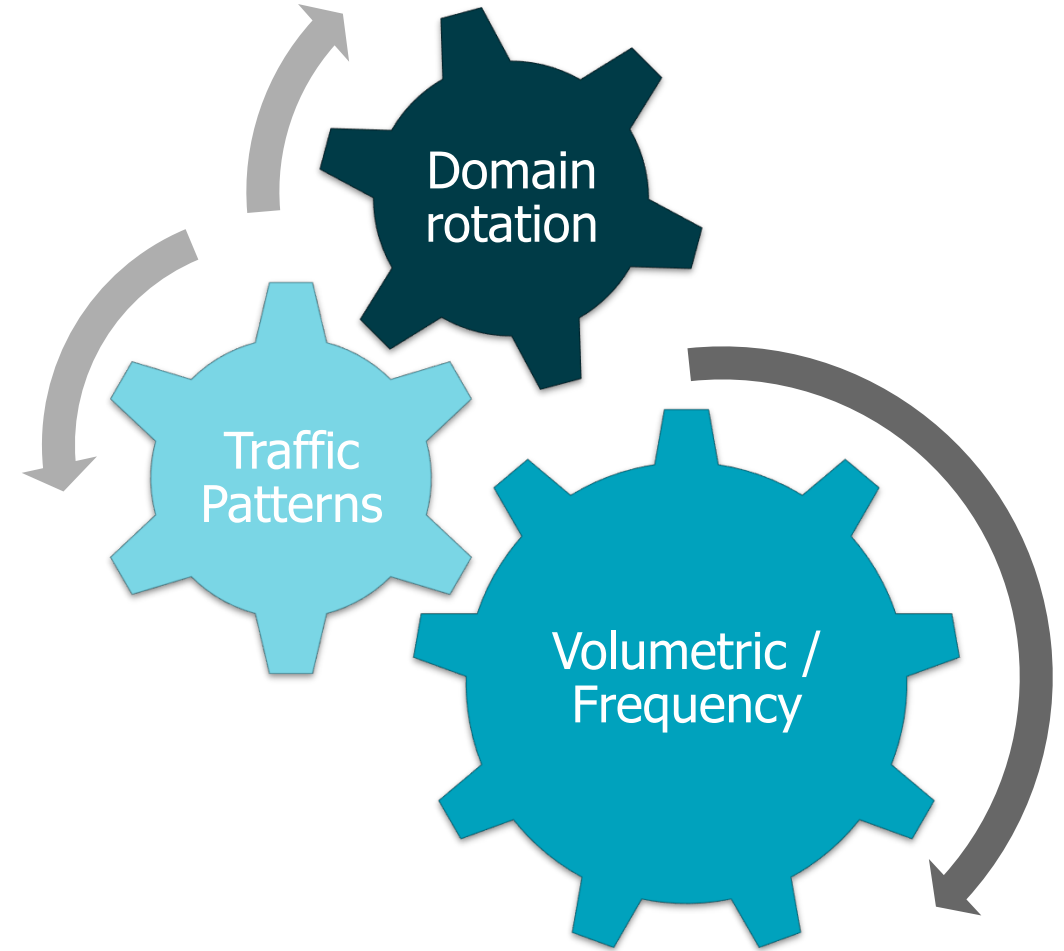
Detection



- ✓ Cluster formation detection + tracking
- ✓ Geo distribution
- ✓ Known patterns
- ✓ DGA detection



Sinkhole



> Sinkholing methodology



Early stage detection



■ examples

frymuc-okuv.ru:2:w32expiro
ffefex-orah.ru:2:w32expiro
fxuxyl-ariv.ru:2:w32expiro
ftykit-agah.ru:2:w32expiro
fqozi-kibol.com:2:w32expiro
fmapo-pufuz.com:2:w32expiro
frores-ezer.ru:2:w32expiro
fkuda-bifik.com:2:w32expiro
ffikop-ehuf.ru:2:w32expiro
fhexog-akib.ru:2:w32expiro
flarer-yxum.ru:2:w32expiro
(...)

ziladkideal.kz pushdo/1778/11039
jeowebvono.kz pushdo/4197/25880
cixizobukqan.kz pushdo/16/58
jupdapuxwocu.kz pushdo/143/485
rufullimasr.kz pushdo/22/58
seorangasl.kz pushdo/30/91
pofajezmoxo.kz pushdo/8/58
pimojitjije.kz pushdo/5970/29330
zeivujunup.kz pushdo/4080/22086
nufilxeiv.kz pushdo/1907/14213
pebqanpeb.kz pushdo/4593/24642
joxabunuxeab.kz pushdo/4641/24571
wukgabukl.kz pushdo/23/91
(...)

> Sinkholing methodology

Early stage detection



■ ex

Massive Sinkholing infrastructure

- Usually over 7,000,000 infected devices tracked on a 24 hour period
- Full access to all C2 communication events (over 6,000 events per second), all the way to the payload, in real time
- Tracking dozens of known and unknown malware families and variations

(...)

039
25880

185

330
80/22086

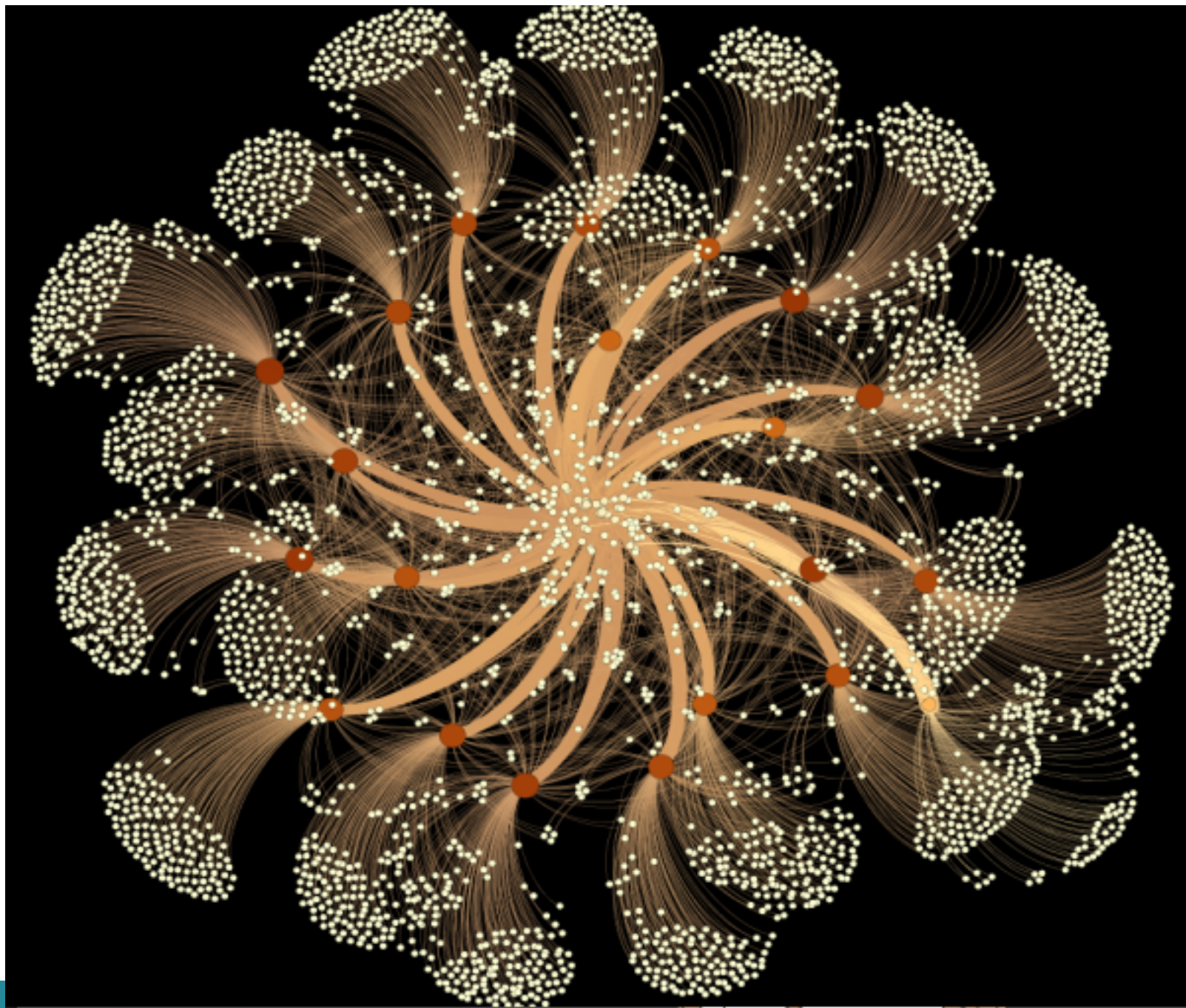
1907/14213

do/4593/24642

ashdo/4641/24571

abukmz pushdo/23/91

UNKNOWN DGA17 – THE MEVADE CONNECTION



> FIRST SIGHTINGS - DNS



- NXDomain DNS queries to a fixed set of 21 .su domains
- Consistent with automated behavior (beacon frequency)
- Multiple geographies
- No substantial overlap with known infections

yj07pit2l4c7.su qsflakuyeefmpi.su
fbllleps83ihm.su xrcuzxrt.su
wh4u6igxiglekn.su iussmddyhezvlg.su
gl5w9dm29sky.su 5x69x0i9x39s.su
z036sazjfh64gz.su irthnalfasxsfd.su
ju3wkr6xwrhr.su gysjkae2wbcpvf.su
fct4ulsg7ofv.su lbd4y25vn6d3pe.su
hgtmzzkvewljdn.su bauxykujfngmpk.su
yzu7vviowjdu.su rreyomnn.su
p3po7xdt9ba2q4.su hypyysycglcwhl.su
dc6h0uvpmg91.su

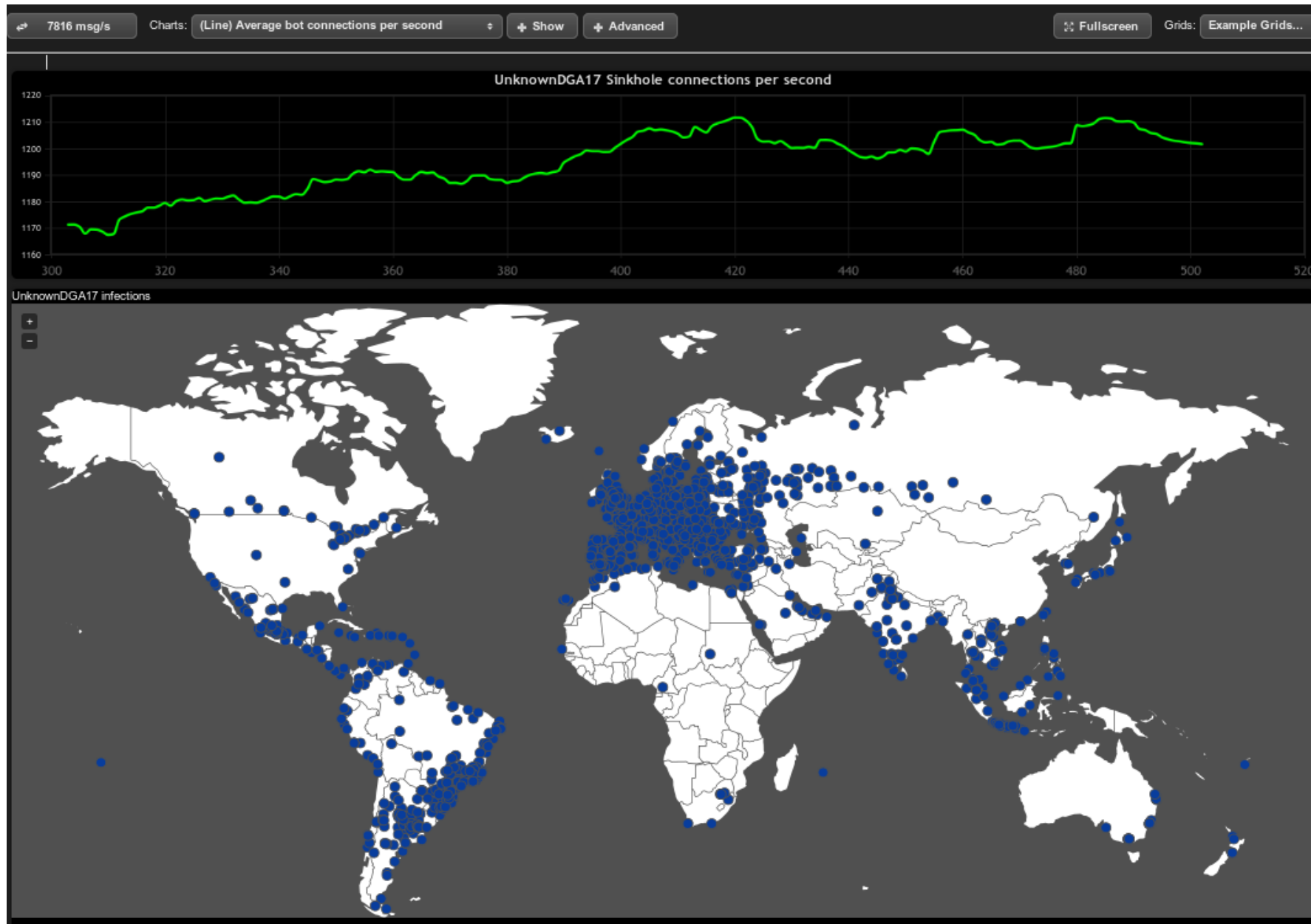
> FIRST SIGHTINGS – HTTP sampling <

- HTTP POST requests to either /cache or /policy resources
- No User-Agent header
- A strange 'uuid' HTTP header
- Binary payload

```
POST /policy HTTP/1.1
Host: wh4u6igxiglekn.su
uuid: d53824ff-25cb-45e5-9b06-0754a4bd4222
Content-transfer-encoding: binary
Content-Type: binary/octet-stream
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg,
application/x-shockwave-flash, */*
Connection: Close
Content-Length: 191

(..payload.. )
```

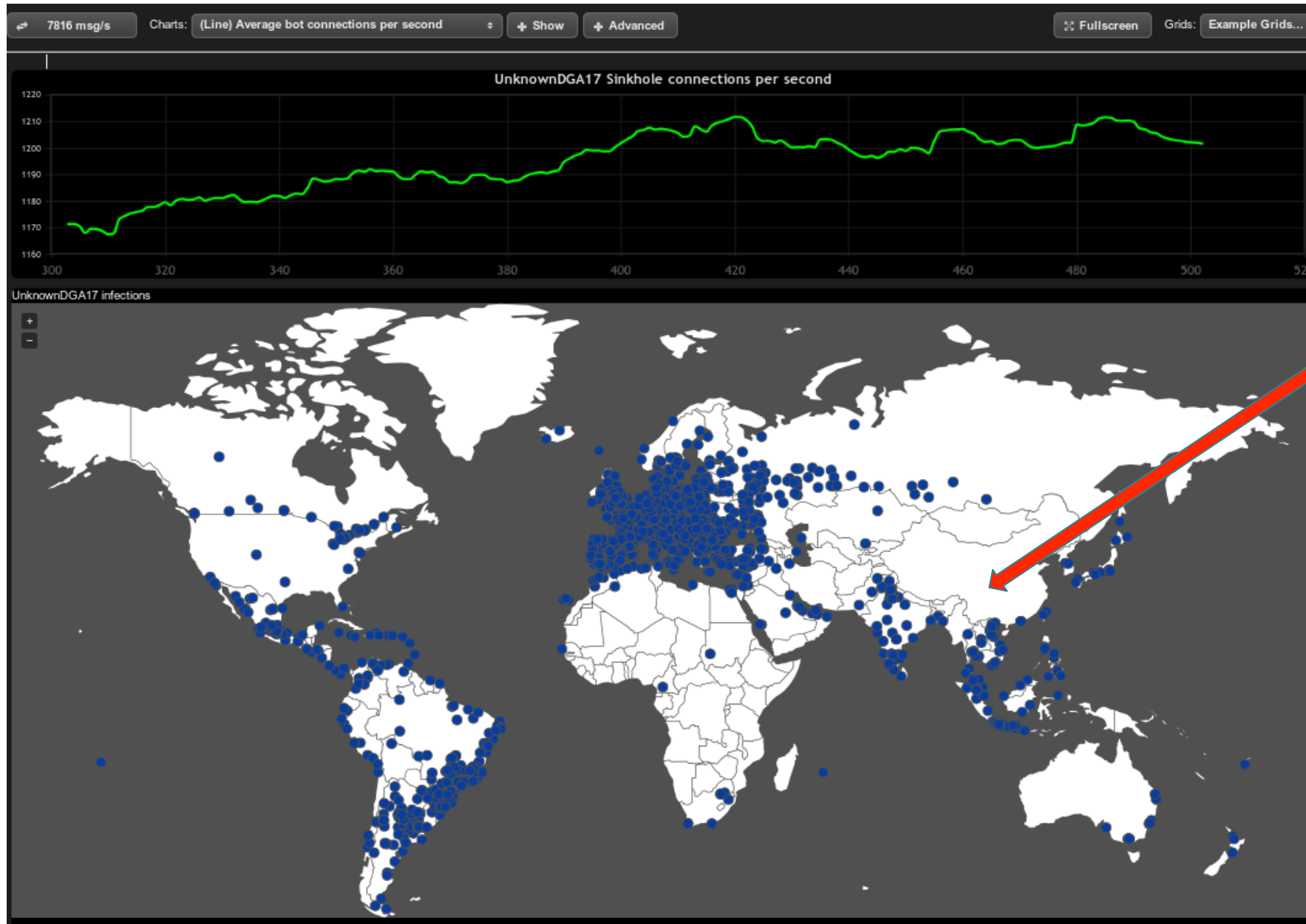
> FIRST SIGHTINGS – Sinkhole it! <



■ *UnknownDGA17* ~10 minutes of traffic

- Initial 24 hours measuring period shows ~**500k** infections
- At its peak, reaches **>1m infections** tracked on a daily basis (24 hour sliding window)

> FIRST SIGHTINGS – Sinkhole it! <



- *UnknownDGA17* ~10 minutes of traffic

Hmmm ... ?

- Initial 24 hours measuring period shows ~**500k** infections
- At its peak, reaches **>1m infections** tracked on a daily basis (24 hour sliding window)

Mevade with a 'sick' twist?

> October 2013: UnknownDGA17



João Gouveia @jgouv

7h

Now tagging new botnet as UnknownDGA17 (soon to be available on [#cyberfeed](#)). 21 rotating SU DGA domains.

pic.twitter.com/mdITLmzG0u

[View photo](#)



João Gouveia @jgouv

8h

We have just identified and sunked a new DGA driven botnet. Details and stats soon. [@anubisnetworks](#) [#cyberfeed](#)

Expand

> Trying all possible C&C algorithms



Citadel?

No.

Sality?

No.

ZeroAccess?

No.

> When all else fails...



Google

> Meanwhile, on a LAN in Thailand



Squid Analysis Report Generator

Squid User Access Reports

Period: 25 Nov 2014—30 Nov 2014

User: 192.168.1.54

Sort: bytes, reverse

User report

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
f.ptcdn.info	556	158.28M	33.12%	1.30%	98.70%	00:44:08	2,648.679	19.23%
www.bloggang.com	921	74.33M	15.55%	0.22%	99.78%	00:23:49	1,429.816	10.38%
contents.louisvuitton.com	2.24K	29.29M	6.13%	1.23%	98.77%	00:06:31	391.373	2.84%
topicstock.pantip.com	321	27.52M	5.76%	0.08%	99.92%	00:13:20	800.653	5.81%
www.prada.com	519	19.95M	4.18%	0.51%	99.49%	00:04:16	256.797	1.86%
2g.pantip.com	197	18.52M	3.88%	1.08%	98.92%	00:05:22	322.311	2.34%
www.chatrium.com	188	10.41M	2.18%	0.12%	99.88%	00:03:08	188.564	1.37%
celebrating.monogram.lv	62	8.84M	1.85%	0.05%	99.95%	00:01:48	108.421	0.79%
static.louisvuitton.com	215	5.93M	1.24%	0.01%	99.99%	00:01:19	79.634	0.58%
www.bakeryland.co.th	309	5.51M	1.15%	11.06%	88.94%	00:01:44	104.568	0.76%
www.tangjibseng.com	247	5.03M	1.05%	4.07%	95.93%	00:00:58	58.181	0.42%
scontent-a.cdninstagram.com	124	4.49M	0.94%	0.00%	100.00%	00:02:23	143.500	1.04%
scontent-a-sin.cdninstagram.com	78	4.19M	0.88%	0.00%	100.00%	00:02:46	166.254	1.21%
www.aommoney.com	75	3.78M	0.79%	0.13%	99.87%	00:02:15	135.167	0.98%
scontent-b-sin.cdninstagram.com	72	3.66M	0.77%	0.00%	100.00%	00:02:29	149.116	1.08%
www.ensogo.com	125	3.64M	0.76%	8.64%	91.36%	00:02:03	123.440	0.90%
scontent-b.cdninstagram.com	96	3.41M	0.72%	0.00%	100.00%	00:01:53	113.171	0.82%
apps.ensogo.com	80	3.39M	0.71%	2.45%	97.55%	00:01:55	115.077	0.84%
pantip.com	870	3.29M	0.69%	17.19%	82.81%	00:01:50	110.660	0.80%
www.accorhotels.com	287	3.28M	0.69%	0.00%	100.00%	00:03:07	187.055	1.36%
static.weloveshopping.com	333	2.95M	0.62%	4.66%	95.34%	00:01:58	118.955	0.86%

> Connections to the 'UnknownDGA17' sinkhole



Linked to:

- whatismyip.com
- angelikajongedijk.no-ip.biz 37.9.53.113
- 'Bprotect' adware

> Looking at the neighbours



37.9.53.113 angelikajongedijk.no-ip.biz

37.9.53.114 olivasonny.no-ip.biz (says VirusTotal)

known Mevade domain!

> Everything is an APT if you try hard enough <

WebSense Security Labs Blog

WebSense Security Labs discovers, investigates and reports on advanced Internet threats that traditional security

research methods miss.

The majority of Command and Control related IP addresses can be attributed back to the following ...primarily targeting the business services, government, manufacturing, and transportation sectors in the US, UK, Canada, and India

Registration Date: 2007-11-09

Registrar: ripencc

Owner: PIN-AS Petersburg Internet Network LLC

> Doctor, doctor



angethymagndnjkohzshbzuk
ingpnyyngnyjyduzshbzuk

 **HIPAA Space** 

[Change Text Size](#) | [Sign In](#) | [Document](#)

Lookups

SOAP/REST

Medicare/Medicaid

EINs

X-walks

1500 Form

B

Medical Data Services divider Healthcare Lookup Services divider NPI Lookup divider **1003850512**

 1003850512 NPI Number — TIMOTHY MAHONEY MSW,
LICSW

Table of Content

 [Additional Information](#)

> Replaying the payload



```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
X-Roll-Ntime: 1
X-Long-Polling: /lp
Server: TwistedWeb/12.0.0
Connection: close
X-Stratum: stratum+tcp://95.211.162.102:7103
Date: Thu, 07 Nov 2013 00:35:34 GMT
Content-Type: application/json
64
{"error": {"message": "Unexpected error during authorization", "code": -1}, "id": 0, "result": null}
0
0000a0 9c 28 c0 7b bc 6d 92 8d 0c 7c 00 e4 b4 85 56 84
0000b0 ad f2 1b a4 30 fb f4 36 8d bd 1e 42 4b 1d 16 a0
```

Note the 'stratum' Bitcoin mining protocol.

What have we learned? Conclusions

> What we learned



'UnknownDGA17' was a non-Tor variant of Mevade.

This botnet was very large (>1m infections).

Mevade was engaged in Bitcoin mining (apart from search engine-hijacking and performing click-fraud).

> April 2014: 'new' Mevade variant doesn't use Tor <



> May 2014: Panic on the streets of Redmond



CATEGORIES

FEATURED

PODCASTS

VIDEOS



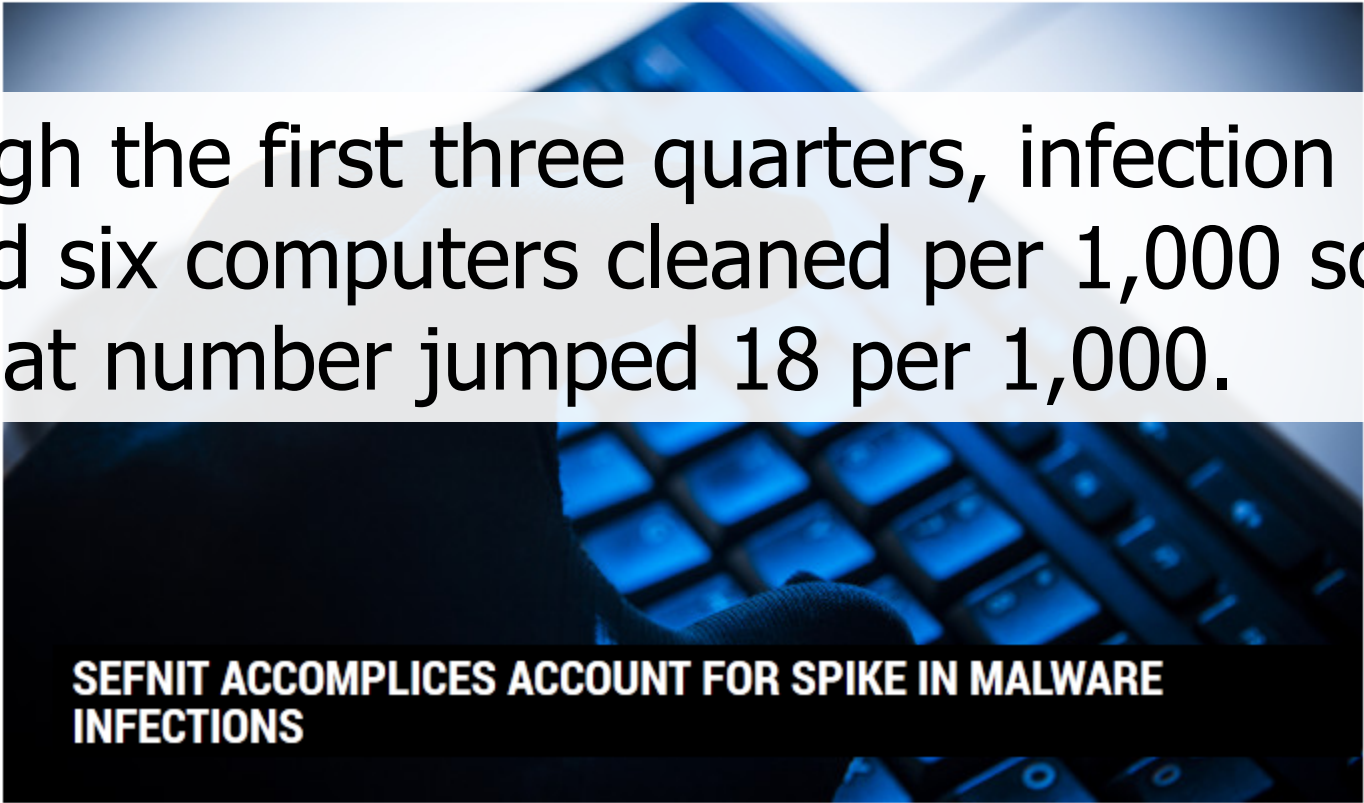
12/01/14 7:49



Researcher Releases Database of Known-Good ICS and
#SCADA Files - <http://t.co/VRZSlvFs8U>

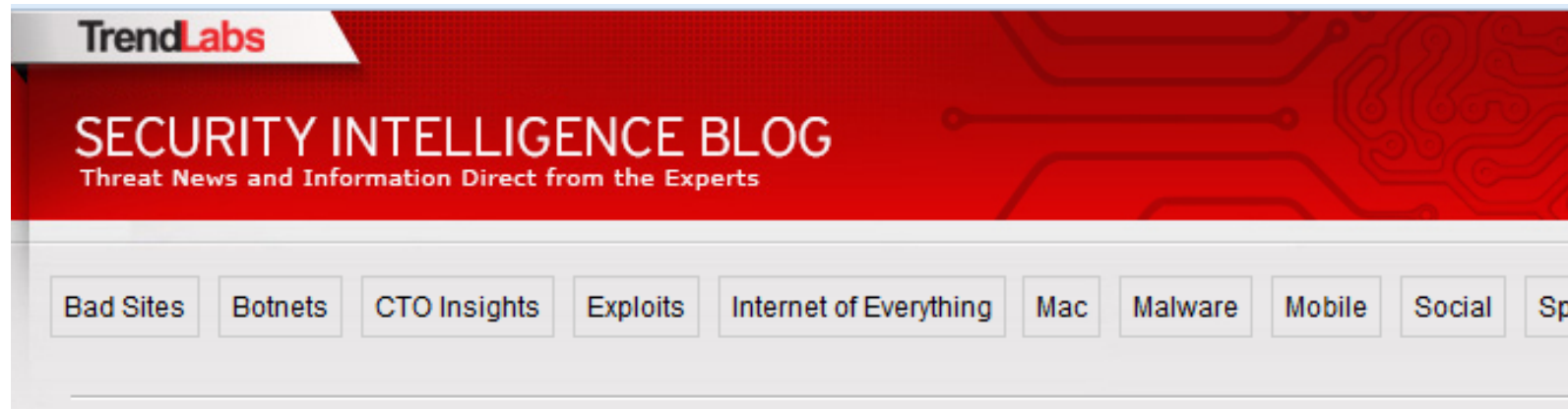
Welcome > Blog Home > Microsoft > Sefnit Accomplishes Account for Spike in Malware Infections

Through the first three quarters, infection rates at around six computers cleaned per 1,000 scanned. In Q4, that number jumped 18 per 1,000.



SEFNIT ACCOMPLISHES ACCOUNT FOR SPIKE IN MALWARE INFECTIONS

> July 2014: Remember Israel?



...adware that turns out to have been developed by an **Israeli company** called iBario Ltd...



> Conclusions



Chasing botnets doesn't have to start with (or even involve) malware samples.

There is a lot of useful information out there on the Internet.

Some botnets are really big, even if you don't hear about them often.

Adware can serve you more than just ads.

Questions?