OpenDNS

Sweeping the IP space: the hunt for evil on the Internet

Dhia Mahjoub
Senior Security Researcher

September 24th, 2014

Dhia Mahjoub

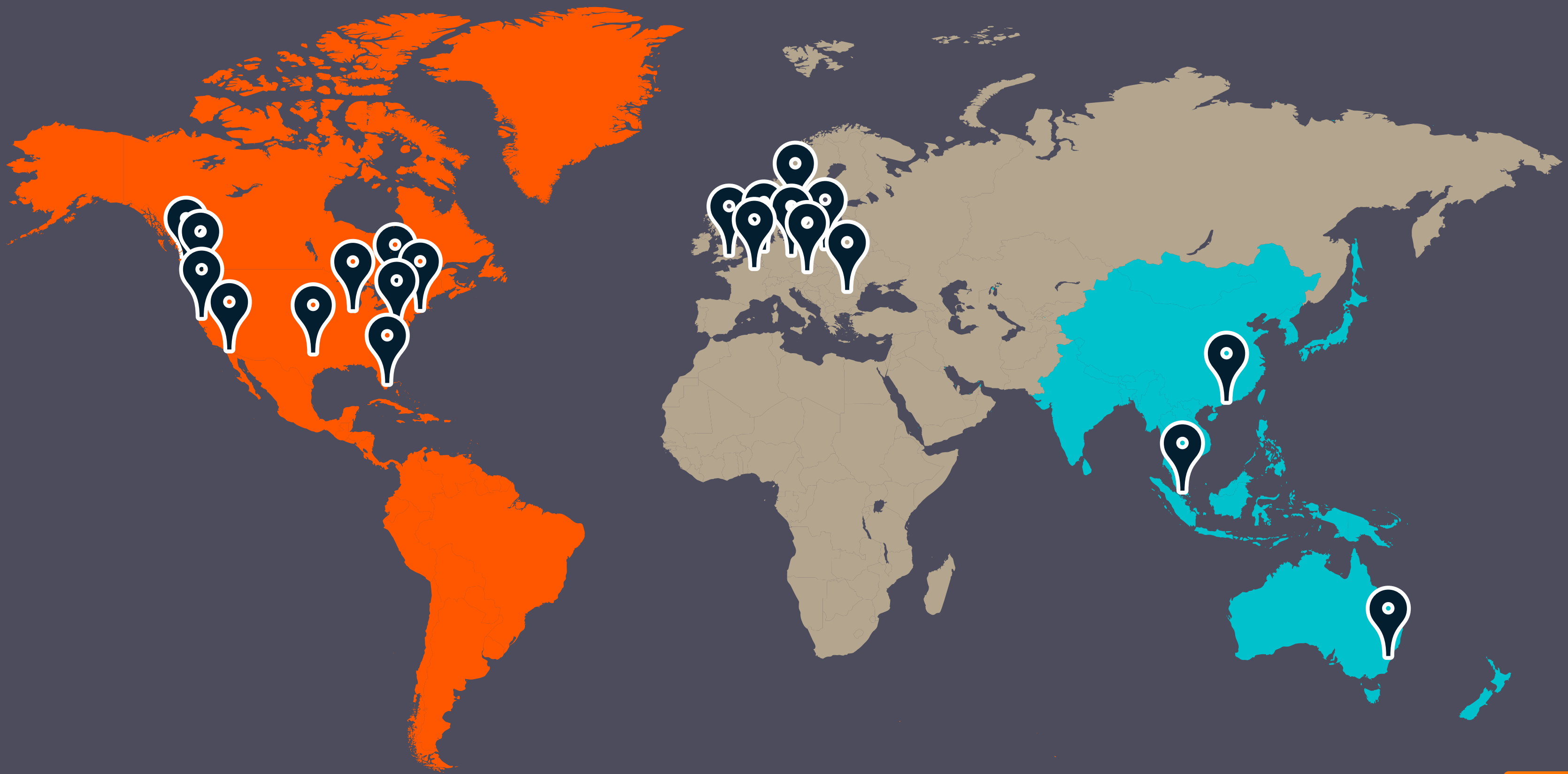
- PhD graph theory applied on sensor networks
- Security, graphs, data analysis
- Spoke at BotConf, ISOI, Source, BlackHat, DefCon

Agenda

- OpenDNS presentation
- ASN graph, Investigating Suspicious Sibling Peripheral ASNs
- Malicious sub-allocated IP ranges
- Predicting malware domains' IP infrastructure
- Malicious subdomains under compromised domains
- Conclusion

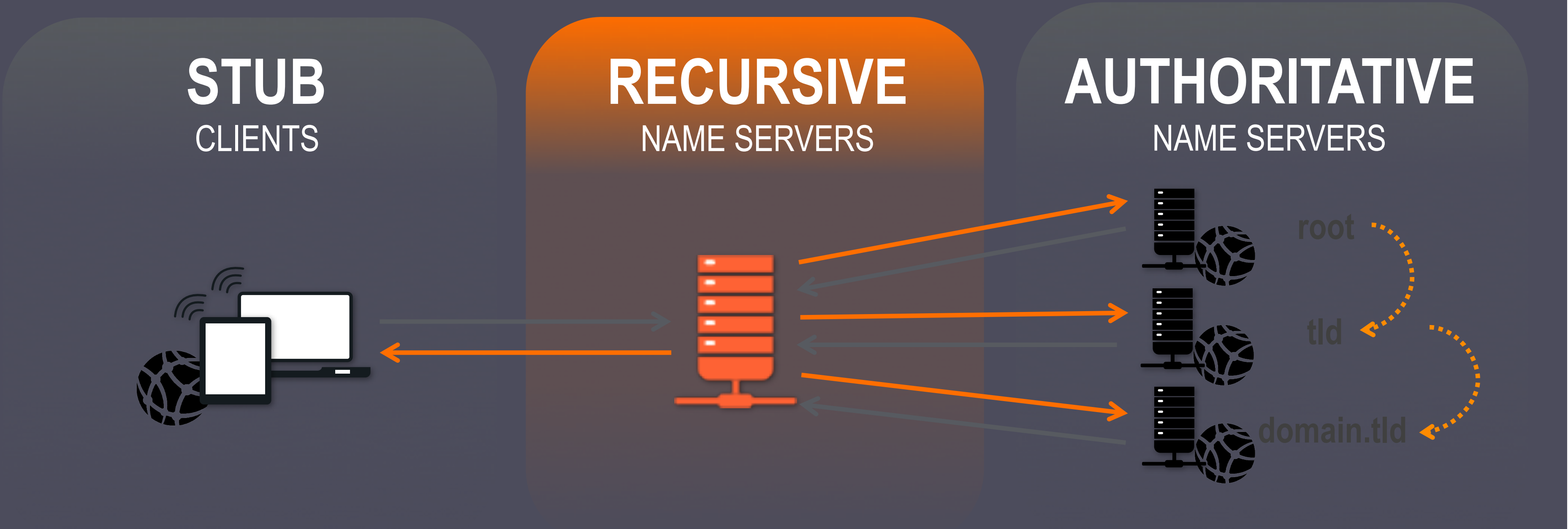
OpenDNS presentation

OpenDNS' Network Map



OpenDNS

DNS traffic


STUB
CLIENTS
RECURSIVE
NAME SERVERS
AUTHORITATIVE
NAME SERVERS
root
tld
domain.tld

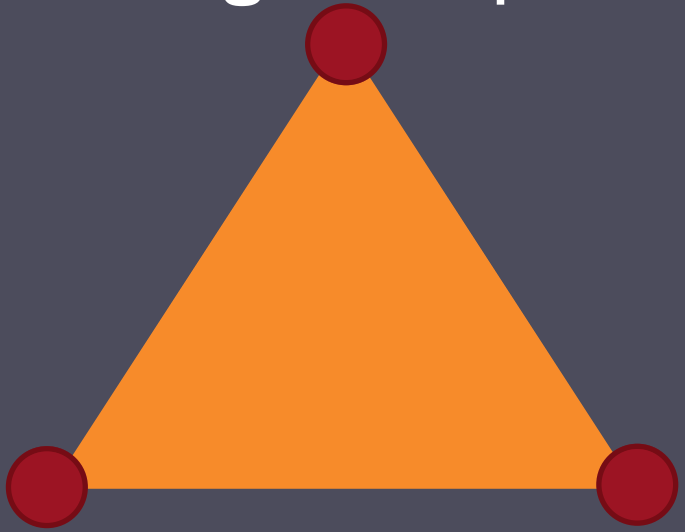
Problem statement

- Classical reputation systems assign scores to IPs, BGP prefixes, ASNs based merely on counting hosted content

➢ **Adopt a different approach: look at qualitative and behavioral aspects of hosting and IP space usage**

➢ **Consider unconventional granularities: ASN graph topology, and sub-allocated IP ranges**

Research Study Components



Investigate IP space

ASN graph

Sub-allocated ranges

ASN graph

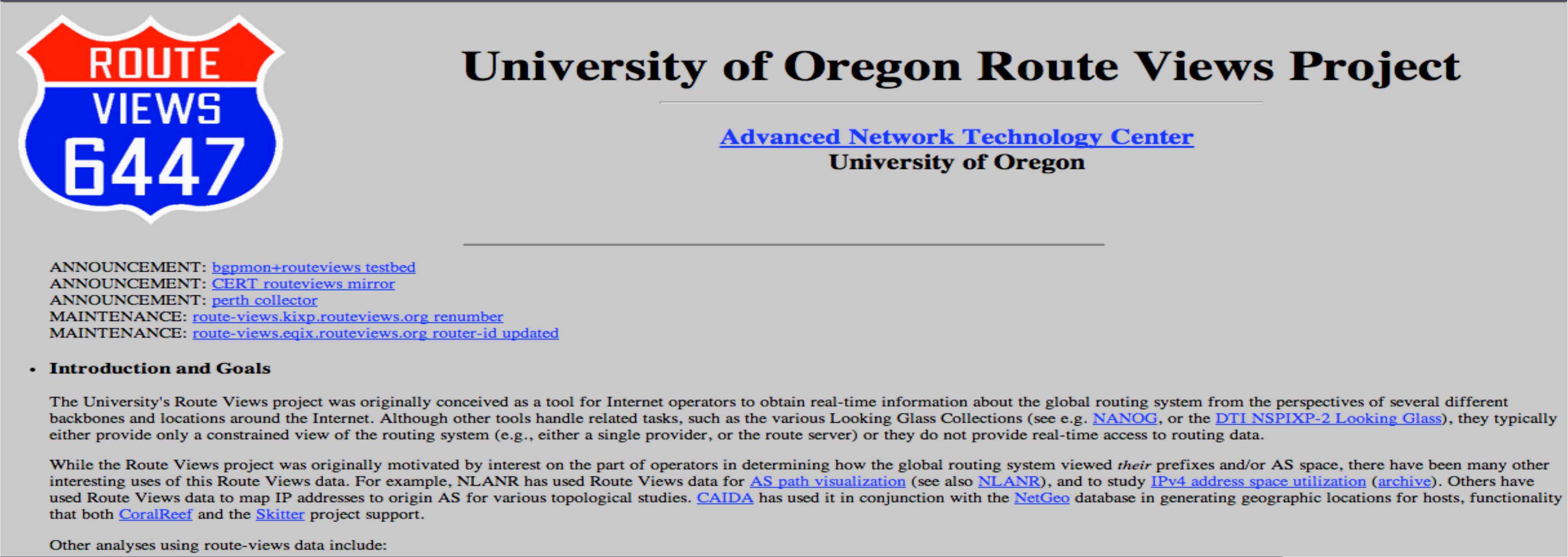
Full AS Network

ASN graph

- BGP routing tables
- Valuable data sources
  - Routeviews
  - Cidr report
  - Hurricane Electric database
- 500,000+ BGP prefixes
- 46,000+ ASNs

ASN graph

- Route Views http://archive.routeviews.org/bgpdata/



University of Oregon Route Views Project

Advanced Network Technology Center
University of Oregon

ANNOUNCEMENT: bgpmon+routeviews testbed
ANNOUNCEMENT: CERT routeviews mirror
ANNOUNCEMENT: perth collector
MAINTENANCE: route-views.kixp.routeviews.org renumber
MAINTENANCE: route-views.eqix.routeviews.org router-id updated

- **Introduction and Goals**

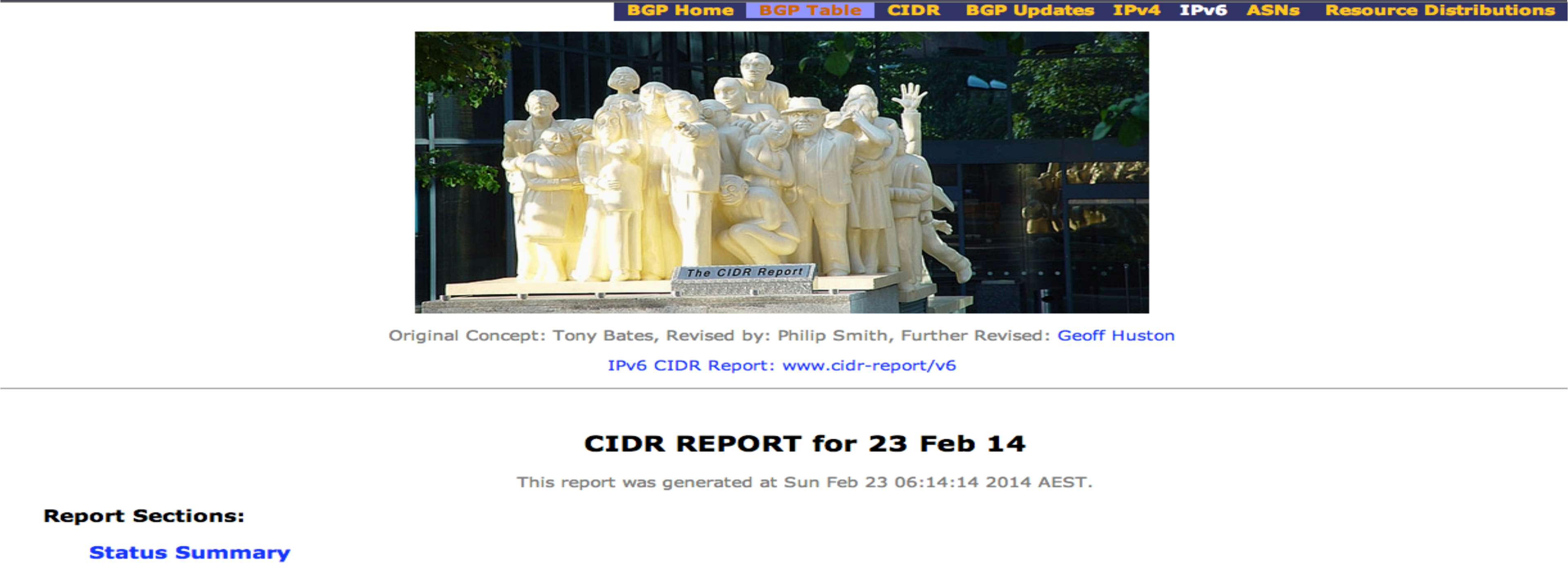
The University's Route Views project was originally conceived as a tool for Internet operators to obtain real-time information about the global routing system from the perspectives of several different backbones and locations around the Internet. Although other tools handle related tasks, such as the various Looking Glass Collections (see e.g. NANOG, or the DTI NSPIXP-2 Looking Glass), they typically either provide only a constrained view of the routing system (e.g., either a single provider, or the route server) or they do not provide real-time access to routing data.

While the Route Views project was originally motivated by interest on the part of operators in determining how the global routing system viewed *their* prefixes and/or AS space, there have been many other interesting uses of this Route Views data. For example, NLANR has used Route Views data for AS path visualization (see also NLANR), and to study IPv4 address space utilization (archive). Others have used Route Views data to map IP addresses to origin AS for various topological studies. CAIDA has used it in conjunction with the NetGeo database in generating geographic locations for hosts, functionality that both CoralReef and the Skitter project support.

Other analyses using route-views data include:

ASN graph

- Cidr Report http://www.cidr-report.org/as2.0/



Original Concept: Tony Bates, Revised by: Philip Smith, Further Revised: Geoff Huston

IPv6 CIDR Report: www.cidr-report/v6

CIDR REPORT for 23 Feb 14

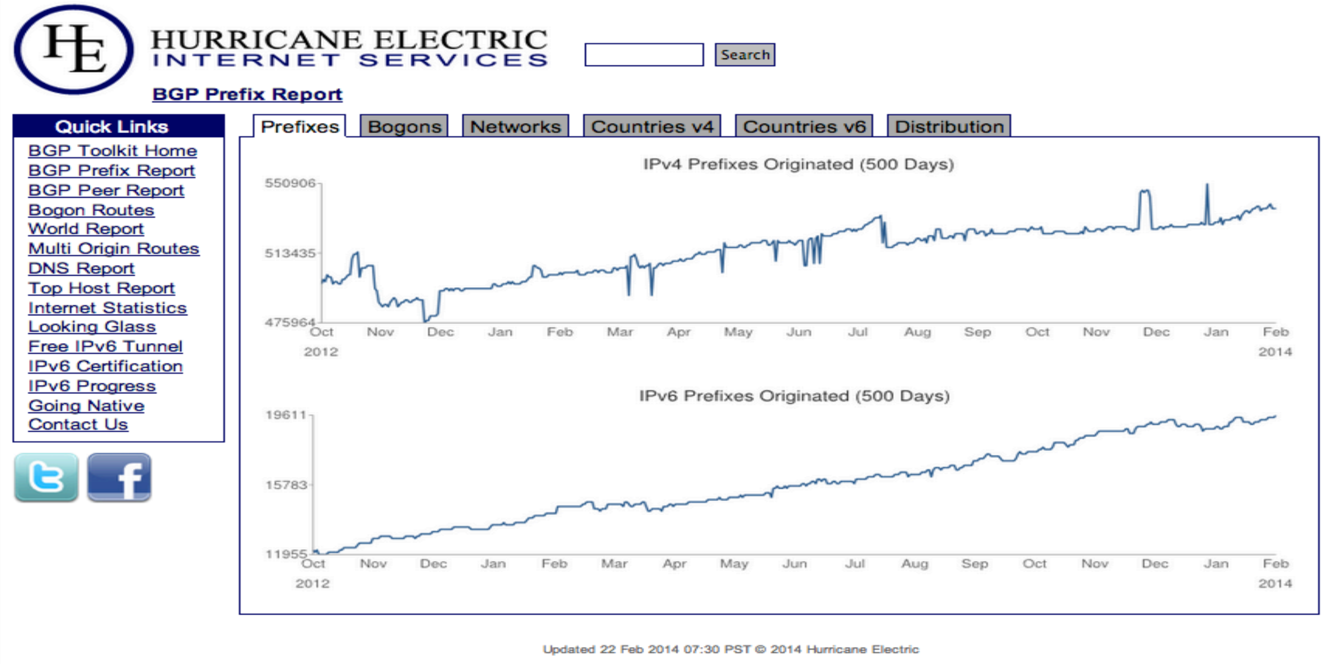
This report was generated at Sun Feb 23 06:14:14 2014 AEST.

Report Sections:

Status Summary

ASN graph

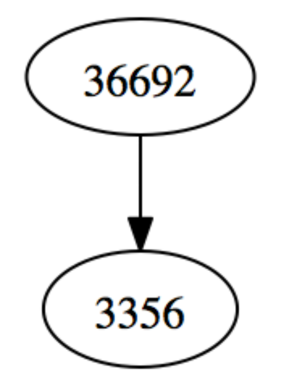
- Hurricane Electric database http://bgp.he.net/



Updated 22 Feb 2014 07:30 PST © 2014 Hurricane Electric

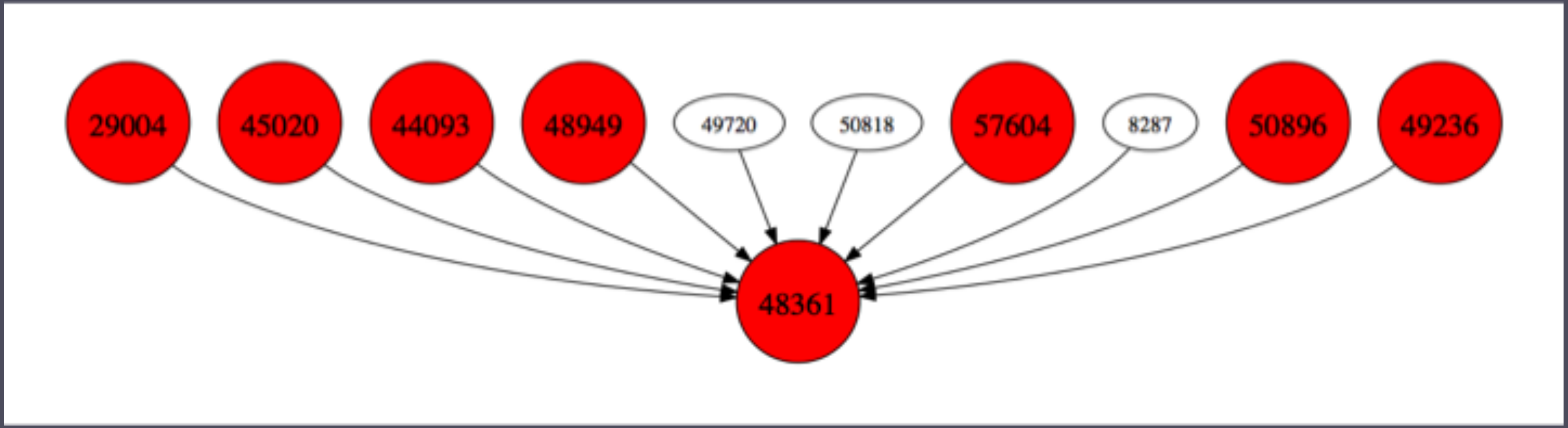
ASN graph

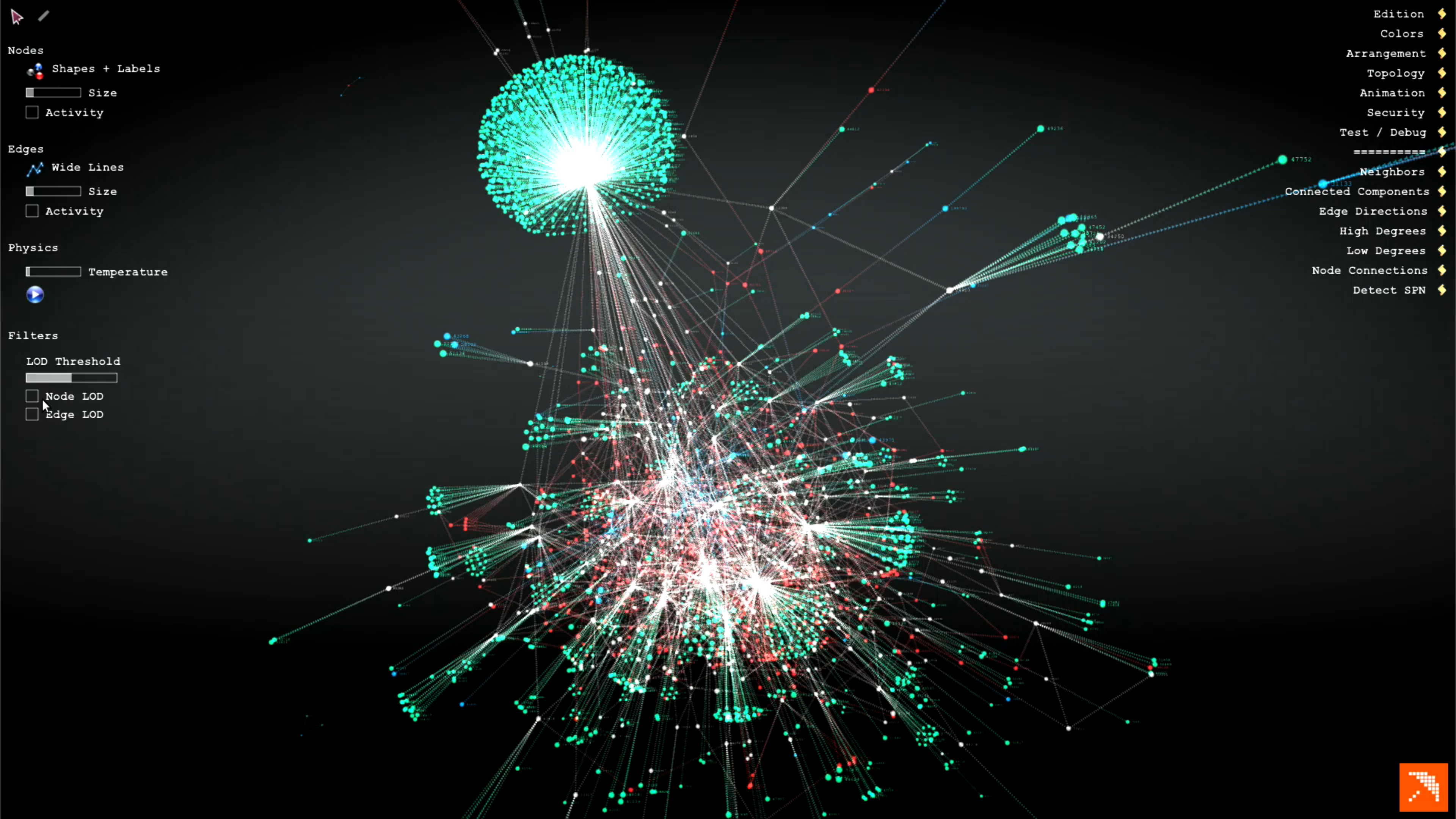
- Directed graph: node=ASN, a directed edge from an ASN to an upstream ASN
- TABLE_DUMP2|1392422403|B|194.153.0.253|5413|67.215.64.0/19|5413 3356 36692|IGP|194.153.0.253|0|1015||AG|36692 38.103.65.97|



ASN based detection model

SPN Concept (Sibling Peripheral Nodes)





Nodes

Shapes + Labels

Size

□ Activity

Edges

Wide Lines

Size

□ Activity

Physics

Temperature

Filters

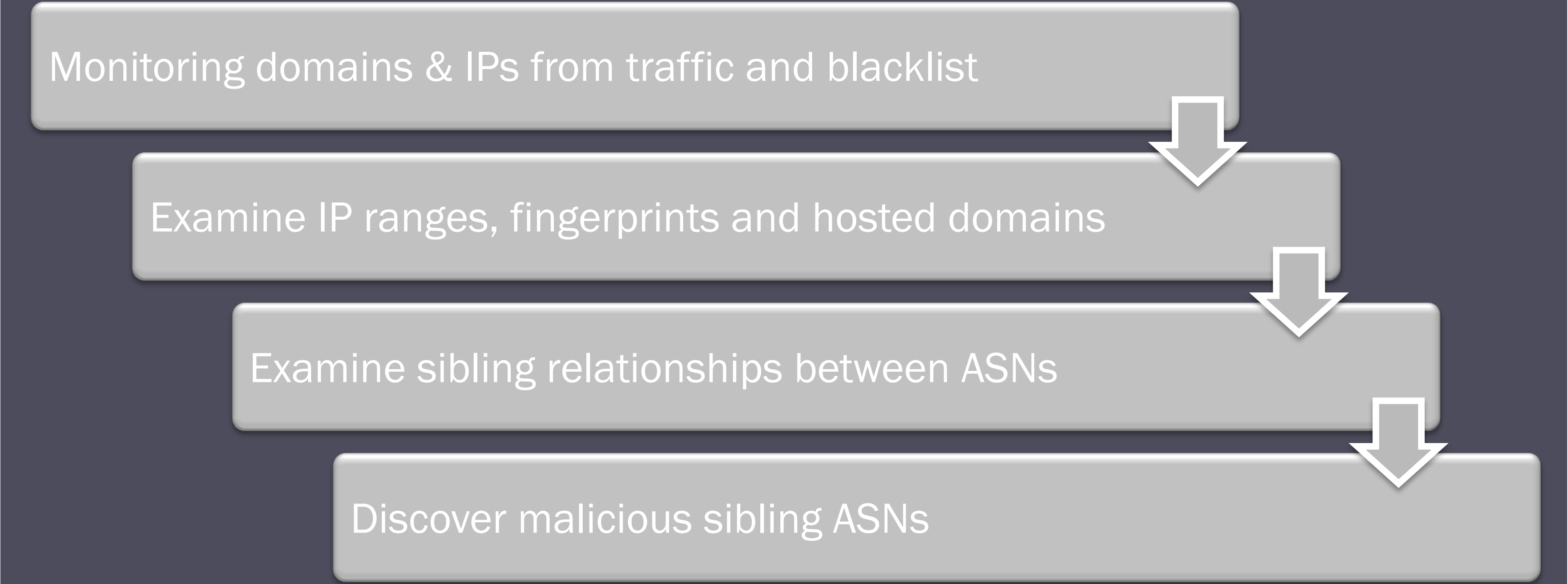
LOD Threshold

□ Node LOD

□ Edge LOD

Use Case #1
Suspicious Sibling Peripheral ASNs

Investigation Process



Monitoring domains & IPs from traffic and blacklist

Examine IP ranges, fingerprints and hosted domains

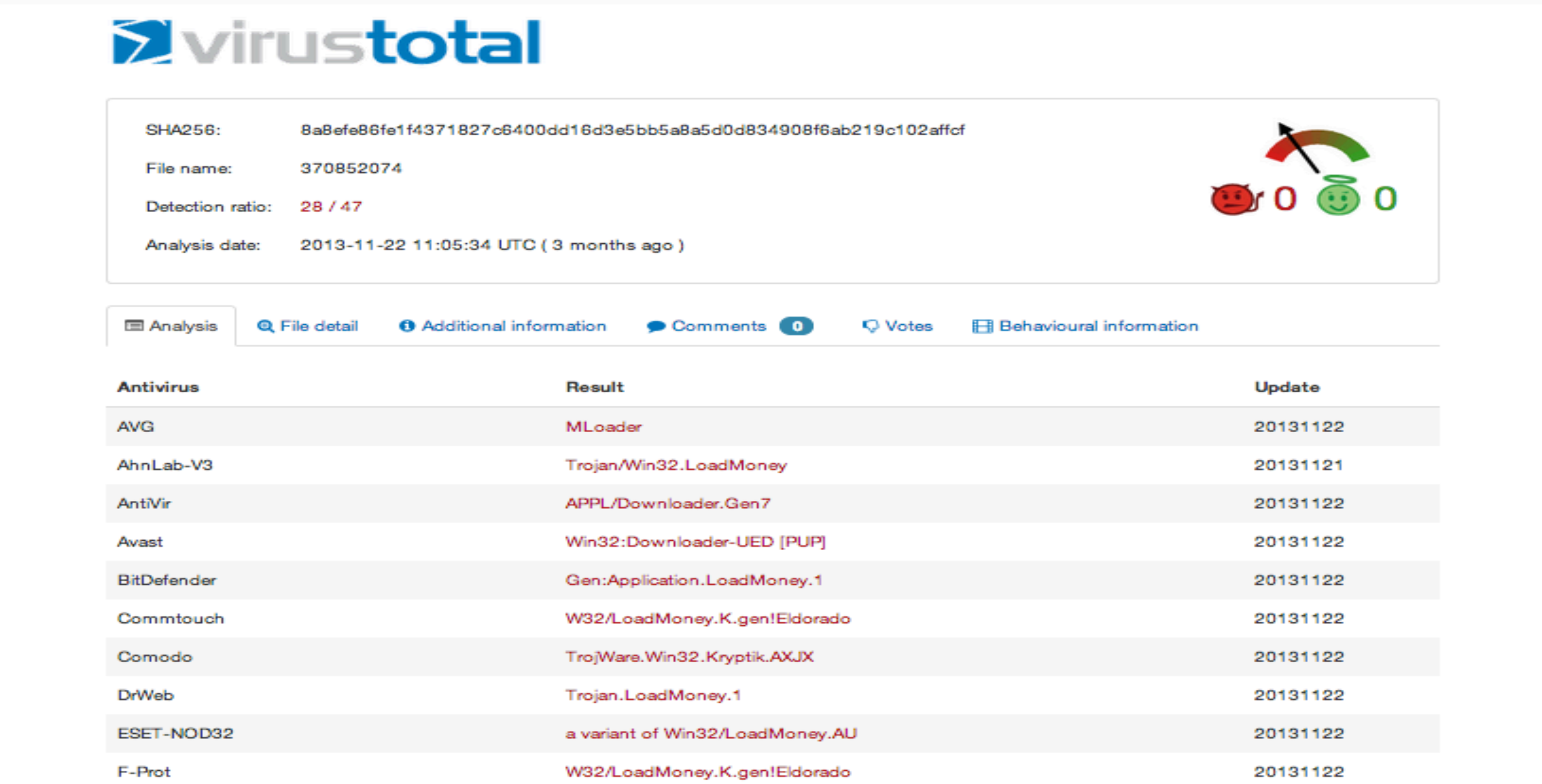
Examine sibling relationships between ASNs

Discover malicious sibling ASNs

Examine IP ranges and fingerprints

- Collect a sample of 160 live IPs hosting similar malicious domains
- /23 or /24 prefixes serving TrojWare.Win32.Kryptik.AXJX
- Also labeled as Trojan-Downloader.Win32.Ldmon.A

Examine IP ranges and fingerprints



SHA256: 8a8efe86fe1f4371827c6400dd16d3e5bb5a8a5d0d834908f6ab219c102affcf

File name: 370852074

Detection ratio: 28 / 47

Analysis date: 2013-11-22 11:05:34 UTC (3 months ago)

Antivirus	Result	Update
AVG	MLoader	20131122
AhnLab-V3	Trojan/Win32.LoadMoney	20131121
AntiVir	APPL/Downloader.Gen7	20131122
Avast	Win32:Downloader-UED [PUP]	20131122
BitDefender	Gen:Application.LoadMoney.1	20131122
Commtouch	W32/LoadMoney.K.gen!Eldorado	20131122
Comodo	TrojWare.Win32.Kryptik.AXJX	20131122
DrWeb	Trojan.LoadMoney.1	20131122
ESET-NOD32	a variant of Win32/LoadMoney.AU	20131122
F-Prot	W32/LoadMoney.K.gen!Eldorado	20131122

Examine IP ranges and fingerprints

Sample of IPs consists in two clusters of identical host fingerprints

50 IPs with:

```
22/tcp   open  ssh        OpenSSH 6.2_hpn13v11 (FreeBSD 20130515; protocol 2.0)
8080/tcp open  http-proxy 3Proxy http proxy
Service Info: OS: FreeBSD
```

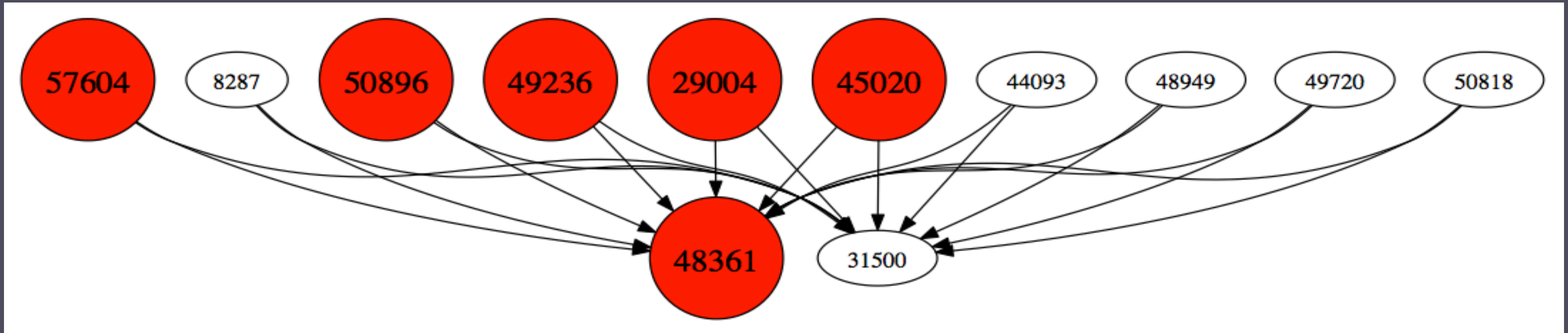
108 IPs with:

```
22/tcp open  ssh     OpenSSH 5.3 (protocol 1.99)
80/tcp open  http?
```

Hosting servers setup is similar !

Examine relationships between ASNs

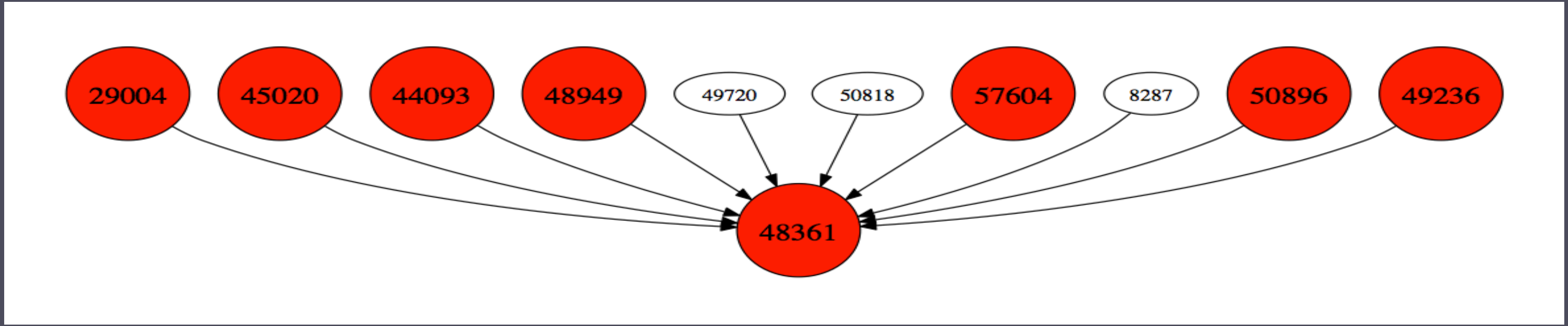
- January 8th topology snapshot, Ukraine, Russia



- 10 sibling peripheral ASNs with 2 upstream ASNs

Examine relationships between ASNs

- February 21st topology snapshot, Ukraine, Russia



- AS31500 stopped announcing its downstream ASNs' prefixes !
- More peripherals started hosting suspicious payload domains !

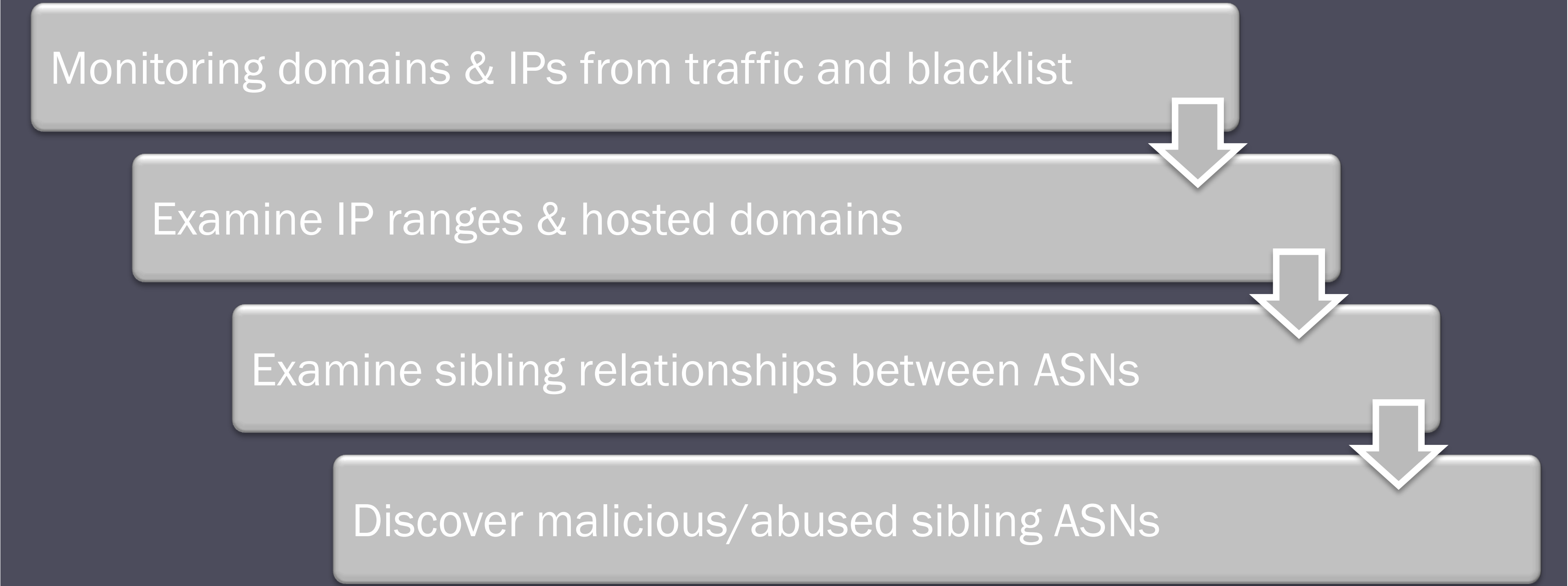
Examine relationships between ASNs

- 3100+ malware domains on 1020+ IPs !
- Payload URLs were live on entire IP ranges before any domains were hosted on them
- Seems the IP infrastructure is set up in bulk and in advance

http://pastebin.com/X83gkPY4

Use Case #2
Abused Sibling Peripheral ASNs

Investigation Process



Monitoring domains & IPs from traffic and blacklist

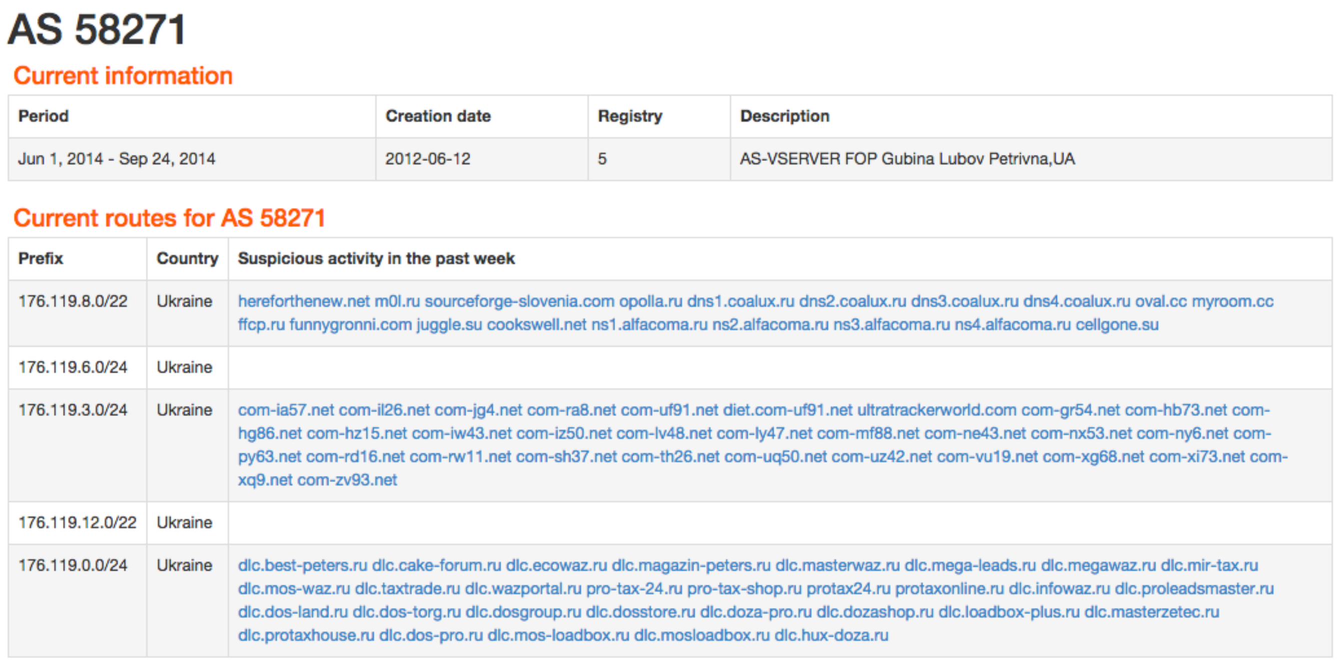
Examine IP ranges & hosted domains

Examine sibling relationships between ASNs

Discover malicious/abused sibling ASNs

Examine IP ranges and hosted domains

- AS58271 hosting spam, trojan downloader domains, and zbot fast flux CnCs



AS 58271

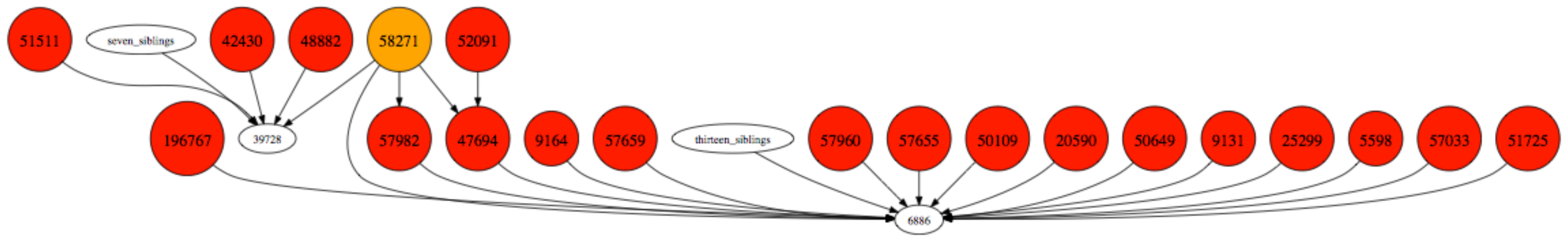
Current information

Period	Creation date	Registry	Description
Jun 1, 2014 - Sep 24, 2014	2012-06-12	5	AS-VSERVER FOP Gubina Lubov Petrivna,UA

Current routes for AS 58271

Prefix	Country	Suspicious activity in the past week
176.119.8.0/22	Ukraine	herefothenew.net m0l.ru sourceforge-slovenia.com opolla.ru dns1.coalux.ru dns2.coalux.ru dns3.coalux.ru dns4.coalux.ru oval.cc myroom.cc ffcp.ru funnygronni.com juggle.su cookswell.net ns1.alfacoma.ru ns2.alfacoma.ru ns3.alfacoma.ru ns4.alfacoma.ru cellgone.su
176.119.6.0/24	Ukraine	
176.119.3.0/24	Ukraine	com-ia57.net com-il26.net com-jg4.net com-ra8.net com-uf91.net diet.com-uf91.net ultratrackerworld.com com-gr54.net com-hb73.net com-hg86.net com-hz15.net com-iw43.net com-iz50.net com-lv48.net com-ly47.net com-mf88.net com-ne43.net com-nx53.net com-ny6.net com-py63.net com-rd16.net com-rw11.net com-sh37.net com-th26.net com-uq50.net com-uz42.net com-vu19.net com-xg68.net com-xi73.net com-xq9.net com-zv93.net
176.119.12.0/22	Ukraine	
176.119.0.0/24	Ukraine	dlc.best-peters.ru dlc.cake-forum.ru dlc.ecowaz.ru dlc.magazin-peters.ru dlc.masterwaz.ru dlc.mega-leads.ru dlc.megawaz.ru dlc.mir-tax.ru dlc.mos-waz.ru dlc.taxtrade.ru dlc.wazportal.ru pro-tax-24.ru pro-tax-shop.ru protax24.ru protaxonline.ru dlc.infowaz.ru dlc.proleadsmaster.ru dlc.dos-land.ru dlc.dos-torg.ru dlc.dosgroup.ru dlc.dosstore.ru dlc.doza-pro.ru dlc.dozashop.ru dlc.loadbox-plus.ru dlc.masterzetec.ru dlc.protaxhouse.ru dlc.dos-pro.ru dlc.mos-loadbox.ru dlc.mosloadbox.ru dlc.hux-doza.ru

Examine IP ranges and hosted domains



Examine IP ranges and hosted domains

- Sibling ASNs of AS58271 comprise University networks, ISPs for businesses and residential customers
- 13106 botnet CnC
- 43124 Sality CnC
- 52091 ZeroAccess peer IPs
- 196767, 20590, 25299, 42430, 47694, 48882, 50649, 51511, 51725, 57033, 57659, 57982, 9131 hosting zbot fast flux CnCs
- 50109 trojan downlaoder, pharma, porn
- 57960 malware downloaders
- 5598, 57033, 57655, 57960, 9164 kelihos CnCs

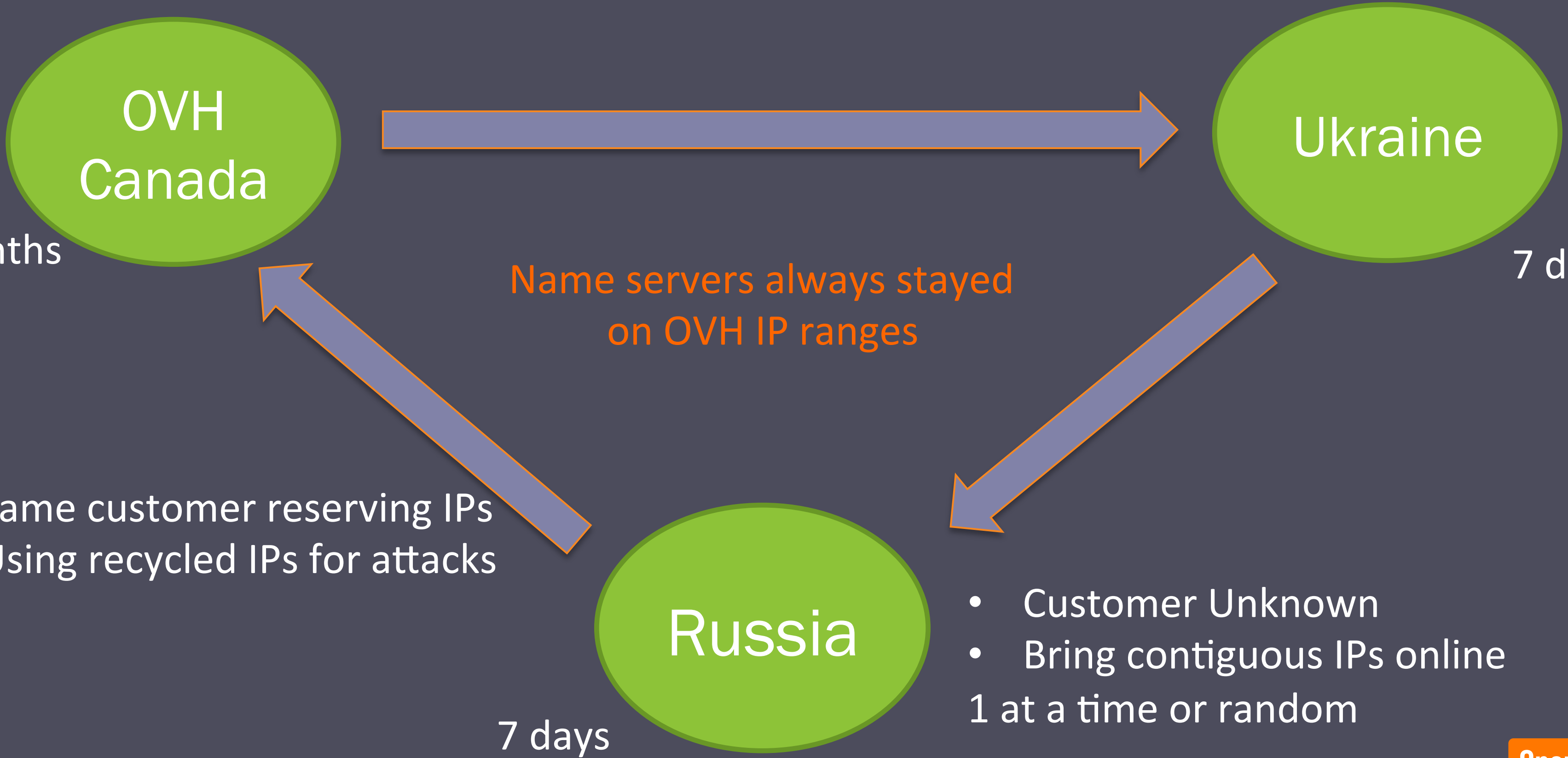
Sub-allocated IP ranges

Malicious sub-allocated ranges

- Same customer reserving IPs
- IPs exclusively used for attacks
- Bring IPs online in bulk

- Customer Unknown
- Bring contiguous IPs online

1 at a time or random



OVH Canada

Months

Ukraine

7 days

Name servers always stayed on OVH IP ranges

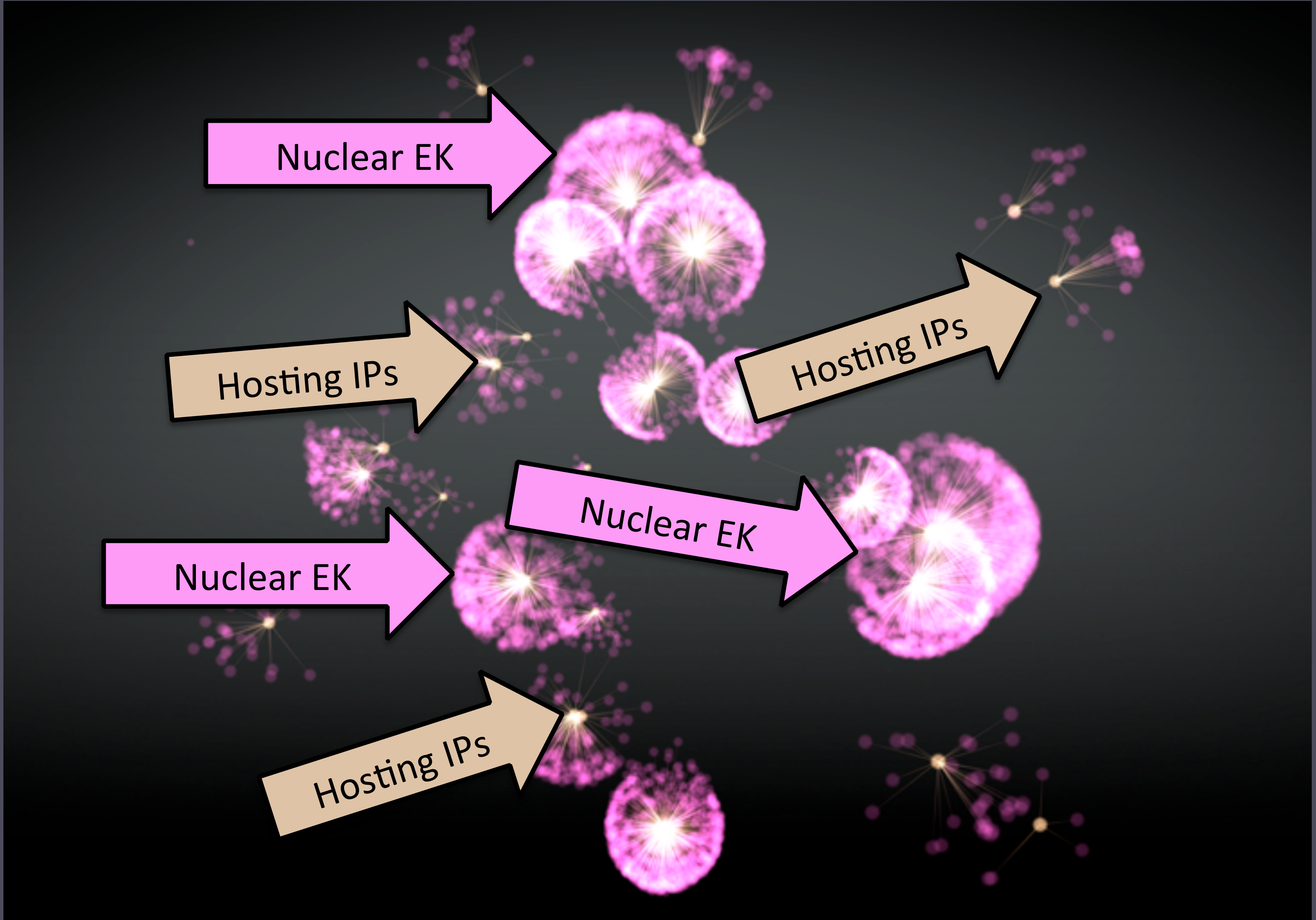
- Same customer reserving IPs
- Using recycled IPs for attacks

Russia

7 days

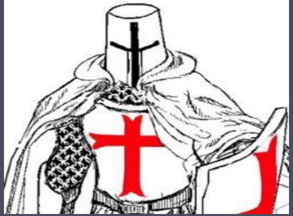
- Customer Unknown
- Bring contiguous IPs online

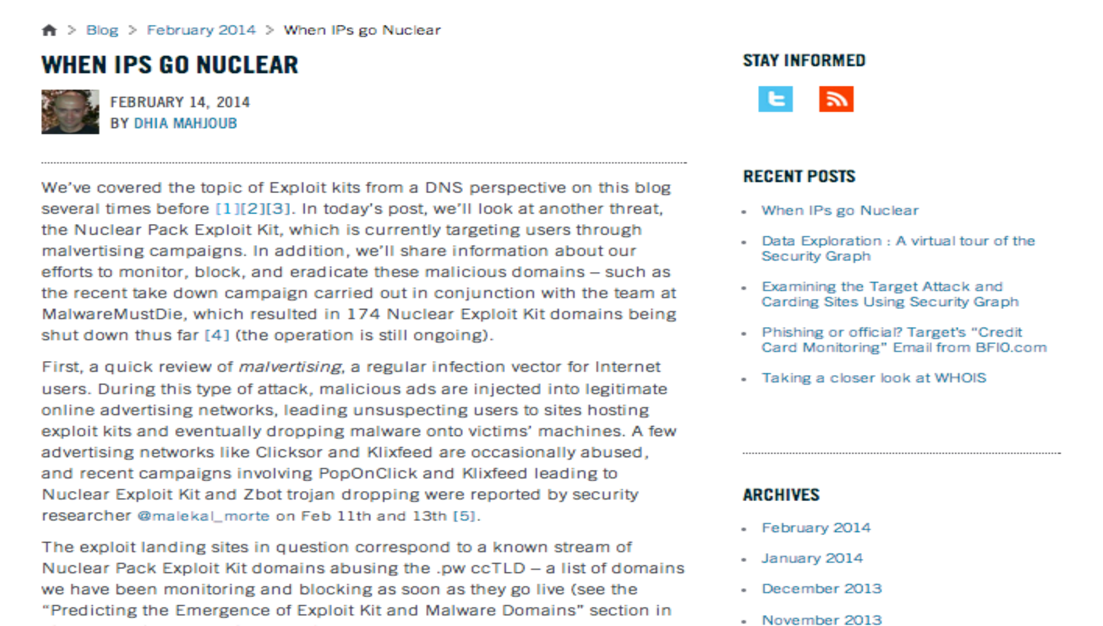
1 at a time or random


Nuclear EK
Hosting IPs
Hosting IPs
Nuclear EK
Nuclear EK
Hosting IPs

Malicious sub-allocated ranges

- http://labs.umbrella.com/2014/02/14/when-ips-go-nuclear/
- Take down operations of domains





WHEN IPS GO NUCLEAR

FEBRUARY 14, 2014
BY DHIA MAHJOUB

We've covered the topic of Exploit kits from a DNS perspective on this blog several times before [1][2][3]. In today's post, we'll look at another threat, the Nuclear Pack Exploit Kit, which is currently targeting users through malvertising campaigns. In addition, we'll share information about our efforts to monitor, block, and eradicate these malicious domains – such as the recent take down campaign carried out in conjunction with the team at MalwareMustDie, which resulted in 174 Nuclear Exploit Kit domains being shut down thus far [4] (the operation is still ongoing).

First, a quick review of *malvertising*, a regular infection vector for Internet users. During this type of attack, malicious ads are injected into legitimate online advertising networks, leading unsuspecting users to sites hosting exploit kits and eventually dropping malware onto victims' machines. A few advertising networks like Clicksor and Klixfeed are occasionally abused, and recent campaigns involving PopOnClick and Klixfeed leading to Nuclear Exploit Kit and Zbot trojan dropping were reported by security researcher @malekal_morte on Feb 11th and 13th [5].

The exploit landing sites in question correspond to a known stream of Nuclear Pack Exploit Kit domains abusing the .pw ccTLD – a list of domains we have been monitoring and blocking as soon as they go live (see the "Predicting the Emergence of Exploit Kit and Malware Domains" section in

STAY INFORMED
RECENT POSTS
When IPs go Nuclear
Data Exploration : A virtual tour of the Security Graph
Examining the Target Attack and Carding Sites Using Security Graph
Phishing or official? Target's "Credit Card Monitoring" Email from BFIO.com
Taking a closer look at WHOIS
ARCHIVES
February 2014
January 2014
December 2013
November 2013

OpenDNS

Predicting malicious domains IP infrastructure

Abused OVH reserved ranges

Time period	Nb. ranges	Nb. IPs	Nb. IPs used	Usage
Dec 1st -31st 2013	28 ranges	136 IPs	86 used	63% malicious
Jan 1st - 31st 2014	11 ranges	80 IPs	33 used	41% malicious
Feb 1st - 28th 2014	4 ranges	28 IPs	26 used	92% malicious
Mar 1st - 20th 2014	43 ranges	364 IPs	215 used	59% malicious

- Nuclear EK domains, Nuclear domains' name servers, and browlock

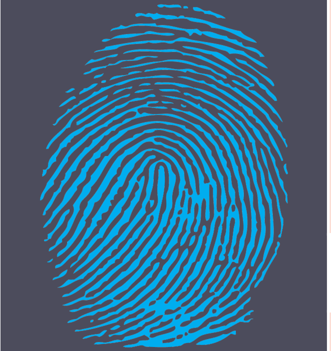
Abused OVH reserved ranges

- 86 sub-allocated ranges are part of 4 BGP prefixes

388	198.50.128.0/17
128	192.95.0.0/18
80	198.27.64.0/18
12	142.4.192.0/19

- BGP prefix granularity is too coarse
- Sub-allocated ranges provide finer granularity for better tracking

Fingerprinting malicious ranges



31.41.221.131 - 31.41.221.143

```
22/tcp  open  ssh     OpenSSH 5.5p1 Debian 6+squeeze4 (protocol 2.0)
80/tcp  open  http    nginx web server 0.7.67
111/tcp open  rpcbind
```

5.101.173.1 - 5.101.173.10

```
22/tcp  open  ssh     OpenSSH 6.0p1 Debian 4 (protocol 2.0)
80/tcp  open  http    nginx web server 1.2.1
111/tcp open  rpcbind
```

Fingerprinting malicious ranges

198.50.143.64 - 198.50.143.79

```
22/tcp  open     ssh      OpenSSH 5.5p1 Debian 6+squeeze4 (protocol 2.0)
80/tcp  open     http     nginx web server 0.7.67
445/tcp filtered microsoft-ds
```

- Indicator 1: Reserved sub-allocated ranges
- Indicator 2: Fingerprints of suspicious IPs

-> Combine indicators and generalize to other attacks

-> **Block/quarantine** IPs **before they start hosting** domains

Detecting Malicious Subdomains under Compromised domains

Malicious subdomains under compromised domains

- Growing trend of injecting malicious subdomains under compromised domains, most notably GoDaddy’s

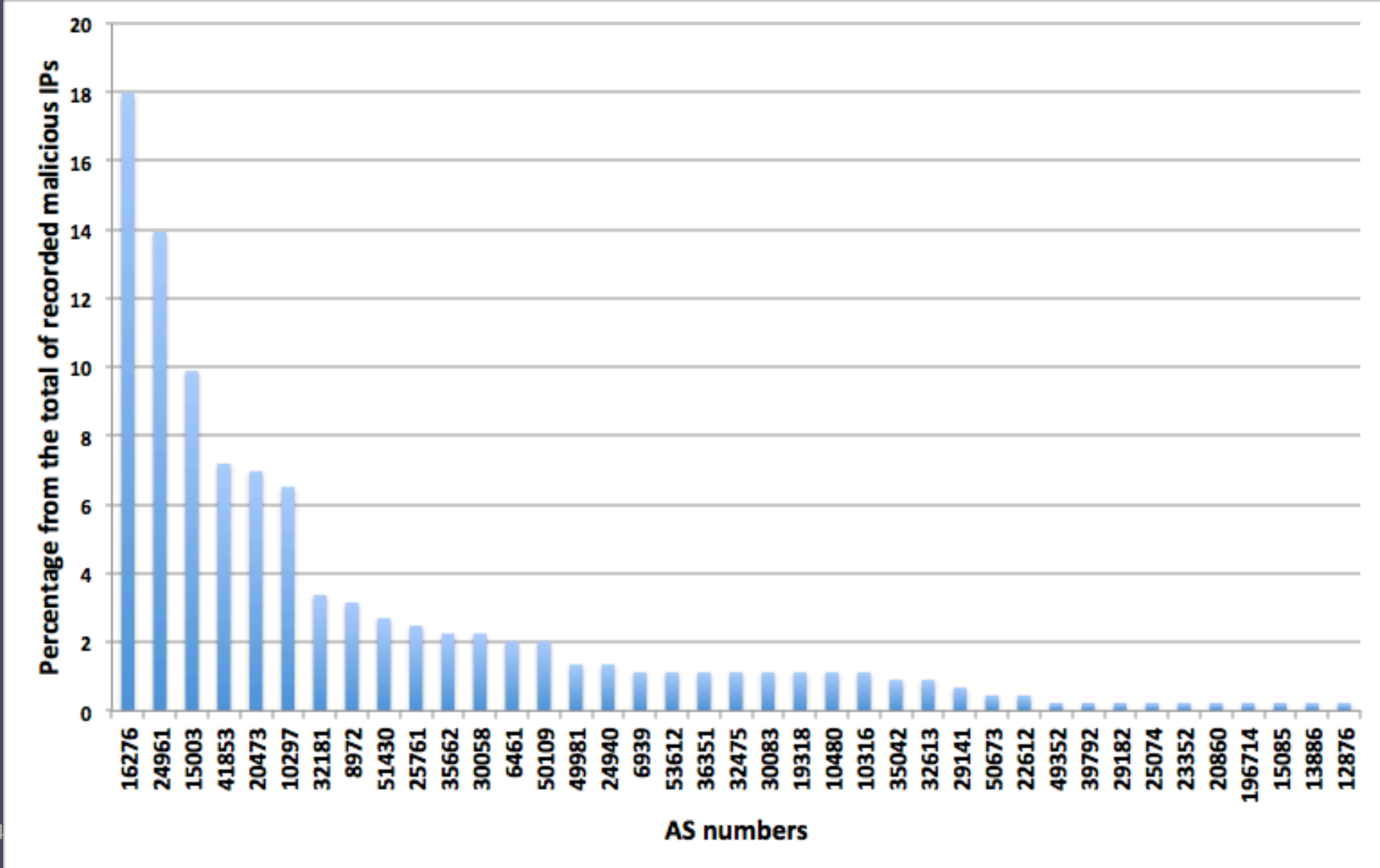
- Monitoring patterns for 7+ months (Feb 2014-present)

- Subdomains serving Exploit kits (e.g. Nuclear, Angler, FlashPack), browlock, malvertising

- Various payloads dropped (e.g. zbot variants, kuluoz)

Malicious subdomains under compromised domains

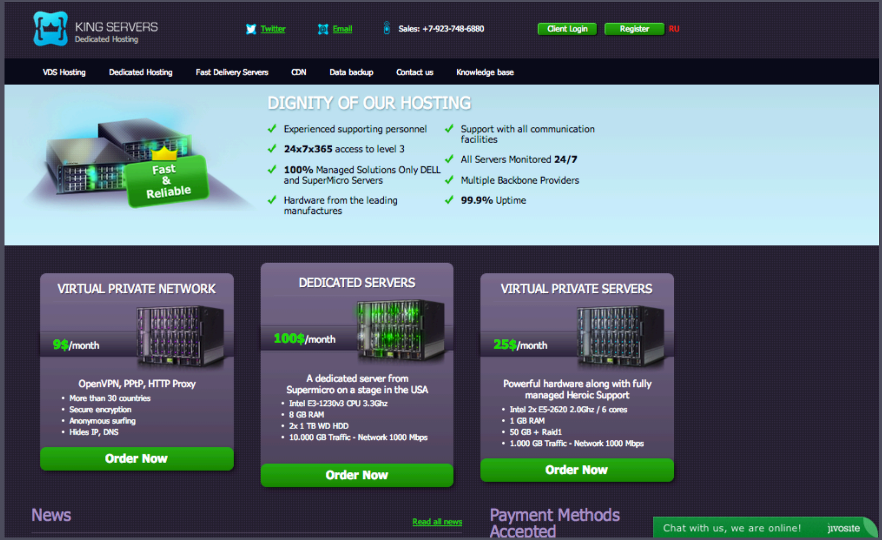
- Sample of several hundred IPs hosting malicious subdomains
- Most abused ASNs
  - 16276 OVH SAS (18% of total collected malicious IPs)
  - 24961 myLoc managed IT AG
  - 8972 PLUSSERVER-AS intergenia AG
  - 41853 LLC NTCOM
  - 20473 Choopa, LLC


Percentage from the total of recorded malicious IPs
20
18
16
14
12
10
8
6
4
2
0
16276
24961
15003
41853
20473
10297
32181
8972
51430
25761
35662
30058
6461
50109
49981
24940
6939
53612
36351
32475
30083
19318
10480
10316
35042
32613
29141
50673
22612
49352
39792
29182
25074
23352
20860
196714
15085
13886
12876
AS numbers

Before	Now
Abuse ccTLDs (e.g. .pw, .in.net, .ru, etc) using rogue/victim resellers/registrars	Supplement with abusing compromised domains
Use reserved IPs exclusively for Exploit kit, browlock attacks	Supplement with using recycled IPs that hosted legit content in the past
Bring attack IPs online in contiguous chunks	Supplement with bringing IPs up in randomized sets or one at a time
Abuse OVH Canada: possible to predictively correlate rogue customers with attack IPs through ARIN rwhois	Abuse OVH Europe spanning numerous countries' IP pools (e.g. FRA, BEL, ITA, UK, IRE, ESP, POR, GER, NED, FIN, CZE, RUS)

Small abused or rogue hosting providers

- http://king-servers.com/en/ hosted Angler, Styx, porn, pharma
- Described on WOT “offers bulletproof hosting for Russian-Ukrainian criminals”



Sales: +7-923-748-6880

DIGNITY OF OUR HOSTING

- ✓ Experienced supporting personnel
- ✓ **24x7x365** access to level 3
- ✓ **100%** Managed Solutions Only DELL and SuperMicro Servers
- ✓ Hardware from the leading manufactures
- ✓ Support with all communication facilities
- ✓ All Servers Monitored **24/7**
- ✓ Multiple Backbone Providers
- ✓ **99.9%** Uptime

VIRTUAL PRIVATE NETWORK

9$/month

OpenVPN, PPtP, HTTP Proxy

- More than 30 countries
- Secure encryption
- Anonymous surfing
- Hides IP, DNS

DEDICATED SERVERS

100$/month

A dedicated server from Supermicro on a stage in the USA

- Intel E3-1230v3 CPU 3.3Ghz
- 8 GB RAM
- 2x 1 TB WD HDD
- 10.000 GB Traffic - Network 1000 Mbps

VIRTUAL PRIVATE SERVERS

25$/month

Powerful hardware along with fully managed Heroic Support

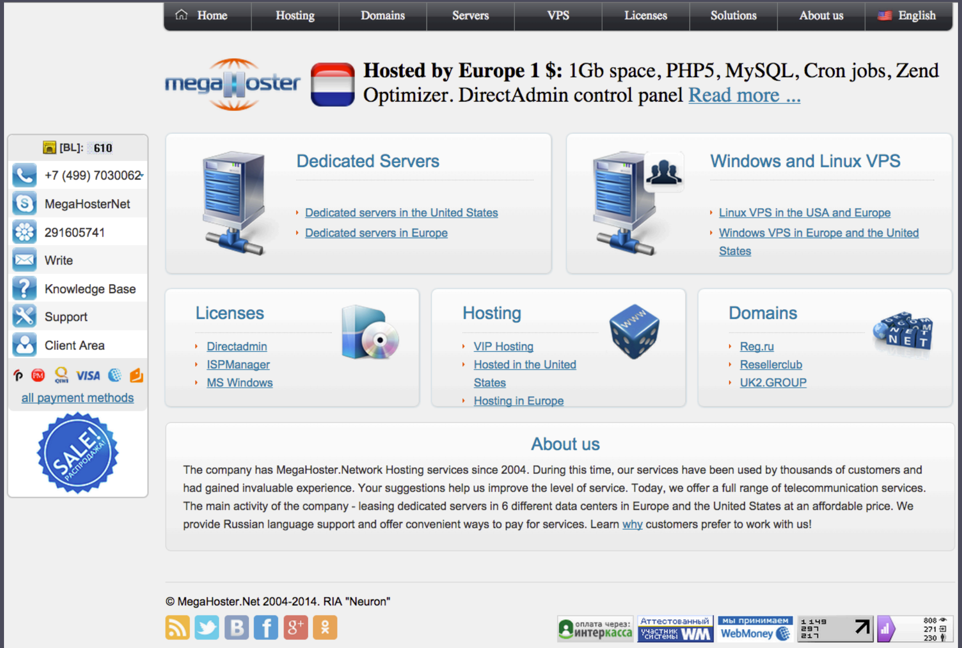
- Intel 2x E5-2620 2.0Ghz / 6 cores
- 1 GB RAM
- 50 GB + Raid1
- 1.000 GB Traffic - Network 1000 Mbps

News

Payment Methods Accepted

Small abused or rogue hosting providers

- http://megahoster.net/ hosted Exploit kit domains, browlock



Hosted by Europe 1 $: 1Gb space, PHP5, MySQL, Cron jobs, Zend Optimizer. DirectAdmin control panel Read more ...

Dedicated Servers

- Dedicated servers in the United States
- Dedicated servers in Europe

Windows and Linux VPS

- Linux VPS in the USA and Europe
- Windows VPS in Europe and the United States

Licenses

- Directadmin
- ISPManager
- MS Windows

Hosting

- VIP Hosting
- Hosted in the United States
- Hosting in Europe

Domains

- Reg.ru
- Resellerclub
- UK2.GROUP

About us

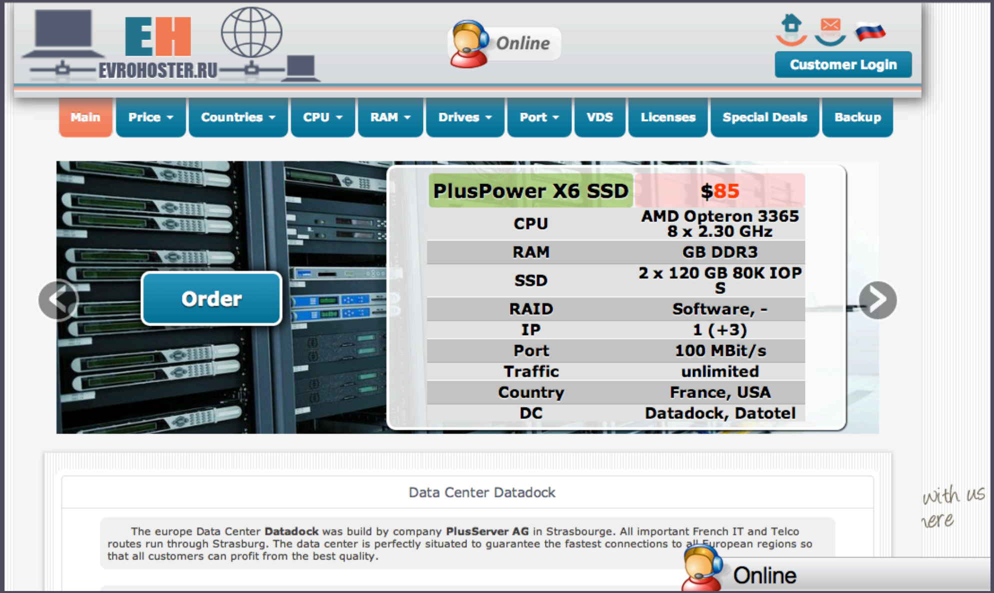
The company has MegaHoster.Network Hosting services since 2004. During this time, our services have been used by thousands of customers and had gained invaluable experience. Your suggestions help us improve the level of service. Today, we offer a full range of telecommunication services. The main activity of the company - leasing dedicated servers in 6 different data centers in Europe and the United States at an affordable price. We provide Russian language support and offer convenient ways to pay for services. Learn why customers prefer to work with us!

© MegaHoster.Net 2004-2014. RIA "Neuron"

OpenDNS

Small abused or rogue hosting providers

- http://evrohoster.ru/en/ hosted browlock through redirections from porn sites



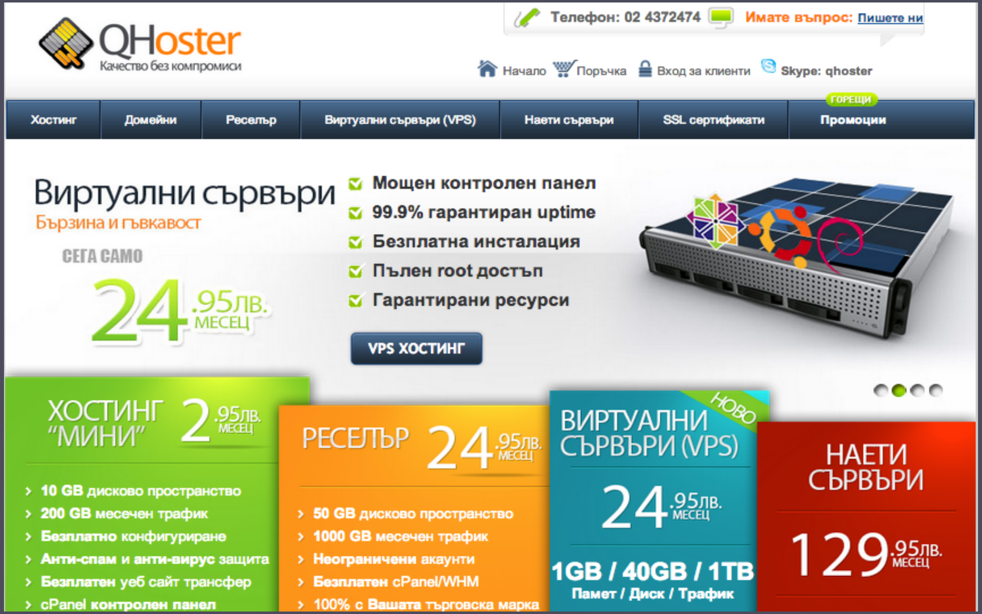
PlusPower X6 SSD	$85
CPU	AMD Opteron 3365 8 x 2.30 GHz
RAM	GB DDR3
SSD	2 x 120 GB 80K IOP S
RAID	Software, -
IP	1 (+3)
Port	100 MBit/s
Traffic	unlimited
Country	France, USA
DC	Datadock, Datotel

Data Center Datadock

The europe Data Center **Datadock** was build by company **PlusServer AG** in Strasbourge. All important French IT and Telco routes run through Strasburg. The data center is perfectly situated to guarantee the fastest connections to all European regions so that all customers can profit from the best quality.

Small abused or rogue hosting providers

- http://www.qhoster.bg/ hosted Nuclear



Телефон: 02 4372474 Имате въпрос: Пишете ни

QHoster
Качество без компромиси

Начало Поръчка Вход за клиенти Skype: qhoster

Хостинг | Домейни | Реселър | Виртуални сървъри (VPS) | Наети сървъри | SSL сертификати | ГОРЕЩИ Промоции

Виртуални сървъри
Бързина и гъвкавост
СЕГА САМО
24.95лв. МЕСЕЦ

☑ Мощен контролен панел
☑ 99.9% гарантиран uptime
☑ Безплатна инсталация
☑ Пълен root достъп
☑ Гарантирани ресурси

VPS ХОСТИНГ

ХОСТИНГ "МИНИ" 2.95лв. МЕСЕЦ
- 10 GB дисково пространство
- 200 GB месечен трафик
- Безплатно конфигуриране
- Анти-спам и анти-вирус защита
- Безплатен уеб сайт трансфер
- cPanel контролен панел

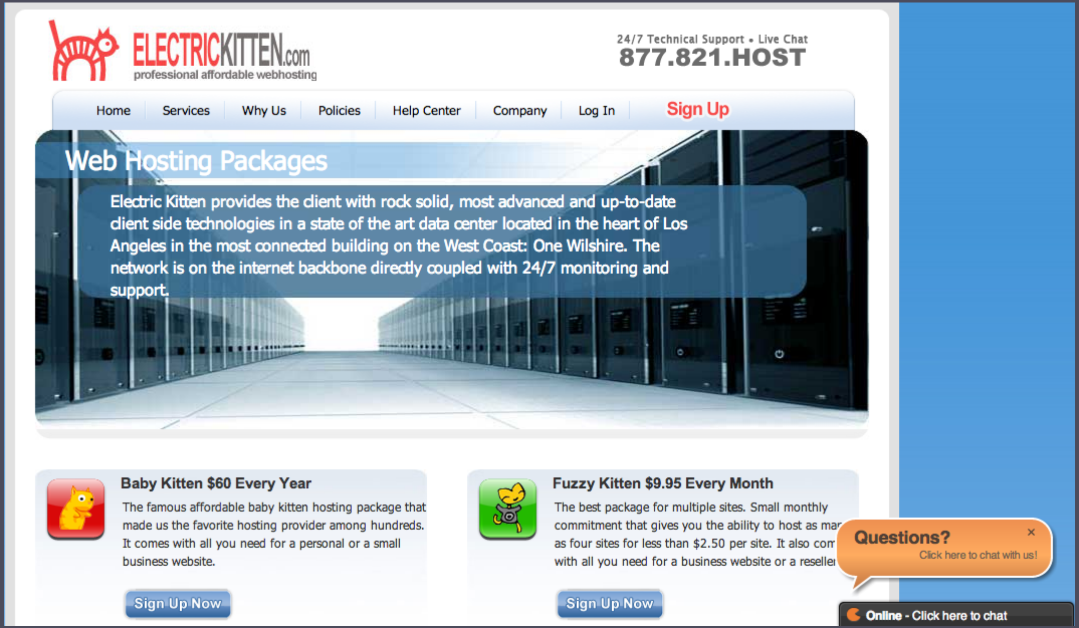
РЕСЕЛЪР 24.95лв. МЕСЕЦ
- 50 GB дисково пространство
- 1000 GB месечен трафик
- Неограничени акаунти
- Безплатен cPanel/WHM
- 100% с Вашата търговска марка

ВИРТУАЛНИ СЪРВЪРИ (VPS) НОВО
24.95лв. МЕСЕЦ
1GB / 40GB / 1TB
Памет / Диск / Трафик

НАЕТИ СЪРВЪРИ
129.95лв. МЕСЕЦ

Small abused or rogue hosting providers

- http://www.electrickitten.com/web-hosting/



professional affordable webhosting

24/7 Technical Support • Live Chat

877.821.HOST

Web Hosting Packages

Electric Kitten provides the client with rock solid, most advanced and up-to-date client side technologies in a state of the art data center located in the heart of Los Angeles in the most connected building on the West Coast: One Wilshire. The network is on the internet backbone directly coupled with 24/7 monitoring and support.

Baby Kitten $60 Every Year

The famous affordable baby kitten hosting package that made us the favorite hosting provider among hundreds. It comes with all you need for a personal or a small business website.

Fuzzy Kitten $9.95 Every Month

The best package for multiple sites. Small monthly commitment that gives you the ability to host as mar as four sites for less than $2.50 per site. It also com with all you need for a business website or a reseller

Small abused or rogue hosting providers

- http://www.xlhost.com/ hosted Angler EK domains
- https://www.ubiquityhosting.com/ hosted browlock.
- http://www.codero.com/
- http://hostink.ru/

Conclusion

- Investigate IP space: ASN graph topology and sub-allocated ranges
- Detect suspicious sibling peripheral ASNs
- Combine indicators to predict malicious IP ranges
- Detect malicious subdomains under compromised domains

Dhia Mahjoub

- @DhiaLIte
- dhia@opendns.com
- http://labs.opendns.com/author/dhia/
- https://www.linkedin.com/in/dhiamahjoub