



# Catching Malware En Masse : DNS and IP style

Dhia Mahjoub dhia@opendns.com @DhiaLite  
Thibault Reuille thibault@opendns.com @ThibaultReuille  
Andree Toonk andree@opendns.com @atoonk

**OpenDNS**



## Part 1: Catching Malware DNS style

- Fastflux botnets as proxy networks

## Part 2: Catching Malware IP style

- ASN graph

- Suspicious sibling ASNs

- Detecting sibling ASNs through BGP outages

- Detecting Malicious IP ranges

- Detecting Malicious subdomains under compromised domains

## Part 3: Visualizing knowledge with our 3D engine

- OpenGraphiti

- Semantic Nets

- Particle Physics

Conclusion



**Part 1:**

**Catching Malware DNS style**

# Background

Attackers seek to keep their operations online at all times

The Network = the hosting infrastructure is

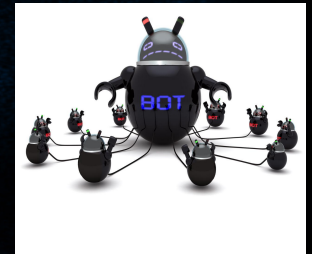
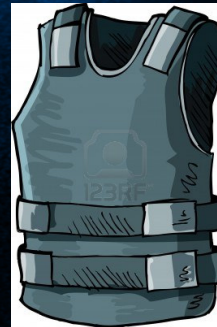
**CRUCIAL**

Spam

Phishing

Malware distribution

Botnets



# Fast flux botnets

Fast flux botnets serving as proxy networks

Extra evasion/protection layer for actual CnCs

Infected hosts <-> FF proxy network <-> Backend CnCs

## Usages of proxy network:

-Serve malware pushed from CnCs down to infected clients  
(via drive-by, spam, etc.)

-Forward communication from infected clients to CnCs

e.g. Kelihos TTL 0, zbot TTL 150

# Zeus Crimeware

- Control panel
- Config files (contains urls for: drop zone, extra payload, extra configs, target websites for web injects)
- Binary files
- Builder

## Characteristics:

- Steals financial data: online bank account info, credit card
- Steals sensitive credentials
- Web injects

# Zeus CnCs

- Compromised sites
- Bulletproof or free hosting
- Fast flux botnet

CnC domains used for 3 types of purposes:

- Serve configuration files
- Serve binary files
- Drop zones

# Zbot proxy network

Fast flux domains with TTL = 150 sec sharing same infected hosts infrastructure

## Detection methods:

- 1) Periodic batch pig job
- 2) IP harvesting + streaming auth DNS + filtering heuristics



# Detection methods (1)

- Periodic Pig job to retrieve domains with TTL = 150 from authoritative logs
- Filter out noise domains such as spam, legitimate domains known to use TTL = 150
- Build “domain to IP” bipartite graph
- Extract largest connected component
- Identify new zbot CnC domains to block
- Add IPs from largest connected component to **pool of zbot IPs**

# Streaming Authoritative DNS

- Tap into processed authoritative DNS stream before it's consolidated into a persistent DB
- asn, domain, 2LD, IP, NS\_IP, timestamp, TTL, type
- Faster than DNSDB on Hadoop
- 100s – 1000s entries/sec (from subset of resolvers)
- Need to implement your own filters, detection heuristics

## Detection methods (2)

- Start with a seed of identified zbot CnC domains
- Continuously harvest IPs and add them to **pool of zbot IPs**
- Check for any domain in authlogs DNS stream whose IP or NS\_IP is in **pool of zbot IPs**
- Identify new zbot CnC domains to block
- Add new domains to seed

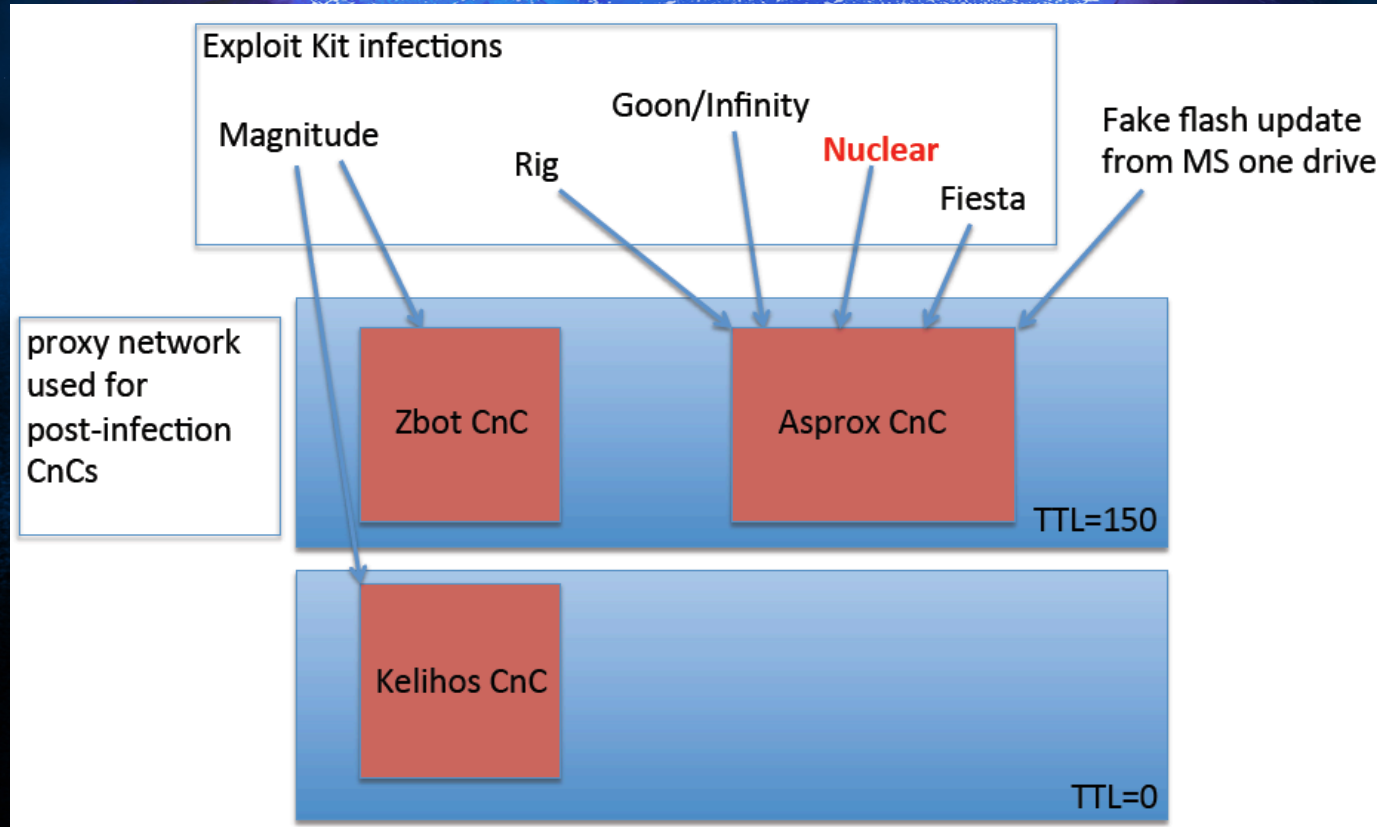
# Zbot proxy network

- Fast flux domains riding on proxy network used as CnCs post-infection by **Kuluoz**
- Various Exploit kits lead to dropping of malware and infected host joins **Asprox** botnet
- Malware used to gain control of hosts is Kuluoz/Dofail

## Infection vectors:

- Drive-by, exploit kit
- Spam emails: embedded links leading to malware, or malware in attachment (fake Flash update)

# Zbot proxy network



# HTTP traffic url patterns

Monitoring HTTP traffic to CnCs using:

-Sinkhole

and

-VirusTotal

# HTTP traffic url patterns

A Zeus CnC domain can serve 3 types of urls:

- Config
- Binary
- Drop zone

## Example Zeus CnC observed traffic

seorubl.in, GET /forum/popap1.jpg, ConfigURL

reznormakro.su, GET /winconf/kernl.bin, ICE IX, ConfigURL

orbitmanes.ru, GET /01.exe, KINS, BinaryURL

reportonh.com, GET /pack32/sysconf.exe, BinaryURL

sytemnr.com, GET /pack32/sysconf.exe, BinaryURL

# HTTP traffic url patterns

ET TROJAN W32/Asprox.ClickFraudBot CnC Beacon

GET /b/eve/0008f258b0e99d069756f425

GET /b/letr/002D63501FC3E082B1E9F290

GET /b/shoe/1480

ET TROJAN W32/Asprox.ClickFraudBot POST CnC Beacon

POST /b/opt

POST /b/req

Multiple Asprox type callbacks and binary downloads followed by click fraud



# HTTP traffic url patterns

Beaconing and announcing version, make, OS

GET /1/?

uid=01604555&ver=1.14&mk=bb3b62&os=S2000&rs=adm&c=14&rq=0

os=S2000

os=Win07

os=Win\_V

os=WinXP

os=Win08

# HTTP traffic url patterns

Other urls to get binaries and configs

azg.su, GET /coivze7aip/modules/bot.exe

tundra-tennes.com, GET /infodata/soft32.dll

tundra-tennes.com, GET /info-data/soft32.dll

bee-pass.com, GET /info/soft32.dll

quarante-ml.com, GET /nivoslider/jquery/

GET /nivoslider98.45/ajax/

GET /nivoslider98.45/jquery/

GET /nivoslider/ajax/

# Pony panel on zbot proxy network

marmedladkos.com

## Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">dron/</a>	15-Feb-2013 12:55	-	
 <a href="#">p/</a>	11-Apr-2014 16:04	-	

*Apache/2.2.22 (Debian) Server at marmedladkos.com Port 80*

# Pony panel on zbot proxy network

- Pony 1.9 leaked for Trojan Forge in late 2012
- Botnet controller via a panel, user management, logging, database, statistics
- Info stealer
- Win32/Fareit

Payload delivered via:

- Drive-by/Exploit kit
- Attachment in spam emails

# Pony panel on zbot proxy network

## Purpose and Objectives :

- Collect FTP / HTTP passwords from 95 + popular FTP-client and Web-browsers from infected computers.
  - Collect email passwords (POP3, IMAP, SMTP).
  - Collect certificates of executable files and drivers.
- Collect-RDP (Remote Desktop Connection) passwords.
  - Invisible to the user.
- The minimum amount of work and time of processing on an infected computer.

Gathering passwords from your computer and send them to the gate.

Works on all versions of Windows, from Windows 98 to Windows 8 (including Windows Server) - x86 and x64.

Implemented instantaneous decoding saved passwords for **the following programs** :

Builder coded in Delphi XE2, plugs coded in ASM ( **32** KB compressed).

**Download** : [Pony 1.9.rar](#) (panel + + builder stub Source)

File Name **Pony.exe**

File Size: 34816

File MD5: oca0aa324446ffada395d644d9bfbe48

File SHA1: 3c8ea0cbb10390c164bc2ab00370e145a3d53be

Check Time: 2012-12-23 13:38:30

RESULTS: 16 / 35

AVG Free - **Virus found Win32/Heur**

ArcaVir - **Clean**

Avast 5 - **Win32: Agent-AOOD [Trj]**

AntiVir (Avira) - **TR/Crypt.XPACK.Gen3**

BitDefender - **Gen: Variant.Kazy.61489**

VirusBuster - **Clean**

Clam - **Clean**

COMODO - **Clean**

Dr. Web - **Trojan.PWS.Stealer.1724**

eTrust-Vet - **Clean**

F-PROT - **Clean**

F-Secure - **Gen: Variant.Kazy.61489**

G Data - **Gen: Variant.Kazy.61489, Win32: Agent-AOOD [Trj]**

IKARUS - **Trojan-PWS.Win32.Fareit**

Kaspersky - **HEUR: Trojan.Win32.Generic**

McAfee - **Clean**

MS Essentials - **Clean**

ESET NOD32 - **Trojan.Win32/PSW.Fareit.A**

Norman - **Clean**

Norton - **Downloader.Ponik**

Panda - **Malware**

A-Squared - **Trojan-PWS.Win32.Fareit! IK**

Quick Heal - **Clean**

Solo - **Clean**

Sophos - **Clean**

Trend Micro - **BKDR\_PONY.SM**





























VBA32 - **Clean**

Vexira - **Clean**

# Pony panel on zbot proxy network

- p/Panel.zip — controlling php scripts
- includes/design/images/modules/\* — images for each zeus plugin supported/tracked
- includes/password\_modules.php — contains array with all software it tries to steal credentials for
- includes/database.php — contains db schema and accessors
- character set cp1251 used everywhere
- mysql storage engine is MyISAM
- config.php date\_default\_timezone\_set('Europe/Moscow')

# Pony panel on zbot proxy network

Name	Date Modified	Size	Kind
 module_3dftp.png	Feb 15, 2014 4:23 AM	214 bytes	Portab...image
 module_32bitftp.png	Feb 15, 2014 4:23 AM	220 bytes	Portab...image
 module_aceftp.png	Feb 15, 2014 4:23 AM	373 bytes	Portab...image
 module_alftp.png	Feb 15, 2014 4:23 AM	378 bytes	Portab...image
 module_becky.png	Feb 15, 2014 4:23 AM	181 bytes	Portab...image
 module_bitkinex.png	Feb 15, 2014 4:23 AM	532 bytes	Portab...image
 module_blazeftp.png	Feb 15, 2014 4:23 AM	350 bytes	Portab...image
 module_bromium.png	Feb 15, 2014 4:23 AM	715 bytes	Portab...image
 module_bulletproof.png	Feb 15, 2014 4:23 AM	494 bytes	Portab...image
 module_cert.png	Feb 15, 2014 4:23 AM	583 bytes	Portab...image
 module_chrome.png	Feb 15, 2014 4:23 AM	643 bytes	Portab...image
 module_chromeplus.png	Feb 15, 2014 4:23 AM	618 bytes	Portab...image
 module_chromium.png	Feb 15, 2014 4:23 AM	613 bytes	Portab...image
 module_classicftp.png	Feb 15, 2014 4:23 AM	335 bytes	Portab...image
 module_coffeecupftp.png	Feb 15, 2014 4:23 AM	177 bytes	Portab...image
 module_comododragon.png	Feb 15, 2014 4:23 AM	801 bytes	Portab...image
 module_coolnovo.png	Feb 15, 2014 4:23 AM	618 bytes	Portab...image
 module_coreftp.png	Feb 15, 2014 4:23 AM	171 bytes	Portab...image
 module_cuteftp.png	Feb 15, 2014 4:23 AM	290 bytes	Portab...image
 module_cyberduck.png	Feb 15, 2014 4:23 AM	546 bytes	Portab...image
 module_deluxeftp.png	Feb 15, 2014 4:23 AM	215 bytes	Portab...image
 module_dopus.png	Feb 15, 2014 4:23 AM	744 bytes	Portab...image
 module_dreamweaver.png	Feb 15, 2014 4:23 AM	556 bytes	Portab...image
 module_easyftp.png	Feb 15, 2014 4:23 AM	812 bytes	Portab...image
 module_epic.png	Feb 15, 2014 4:23 AM	733 bytes	Portab...image
 module_expandrive.png	Feb 15, 2014 4:23 AM	619 bytes	Portab...image
 module_far.png	Feb 15, 2014 4:23 AM	144 bytes	Portab...image
 module_ffftp.png	Feb 15, 2014 4:23 AM	285 bytes	Portab...image




```
1 <?php
2
3 /*
4 Password decryption and processing code.
5
6 */
7
8
9 define("REPORT_LEN_LIMIT",          1024*1024*32);           // do not process reports with length greater than this limit
10 define("REPORT_HEADER",             "PWDFILE0");           // each password report starts with this header
11 define("REPORT_PACKED_HEADER",      "PKDFILE0");           // header indicating that report is packed
12 define("REPORT_CRYPTED_HEADER",     "CRYPTED0");           // header indicating that report is encrypted
13 define("REPORT_VERSION",            "1.0");                 // supported report version
14 define("REPORT_MODULE_HEADER",      chr(2).chr(0)."MODU".chr(1).chr(1)); // report module header, used for consistency checks
15 define("REPORT_ITEMHDR_ID",         0xbeef0000);           // report item header, used for consistency checks
16 define("REPORT_DEFAULT_PASSWORD",   "Mesoamerica");        // default report encryption password
17
18 define('VER_PLATFORM_WIN32_NT', 2);
19 define('VER_NT_WORKSTATION', 1);
20 define('PROCESSOR_ARCHITECTURE_AMD64', 9);
21
22 // module_class | module_id | module_name
23 $global_module_list = array(
24     array('module_systeminfo',      0x00000000, 'System Info'),
25     array("module_far",             0x00000001, 'FAR Manager'),
26     array("module_wtc",             0x00000002, 'Total Commander'),
27     array("module_ws_ftp",          0x00000003, 'WS_FTP'),
28     array("module_cuteftp",         0x00000004, 'CutEFTP'),
29     array("module_flashfxp",       0x00000005, 'FlashFXP'),
30     array("module_filezilla",      0x00000006, 'FileZilla'),
31     array("module_ftpccommander",  0x00000007, 'FTP Commander'),
32     array("module_bulletproof",    0x00000008, 'BulletProof FTP'),
33     array("module_smartftp",       0x00000009, 'SmartFTP'),
34     array("module_turboftp",       0x0000000a, 'TurboFTP'),
35     array("module_ffftp",          0x0000000b, 'FFFTP'),
36     array("module_coffeecupftp",    0x0000000c, 'CoffeeCup FTP / Sitemapper'),
37     array("module_coreftp",        0x0000000d, 'CoreFTP'),
38     array("module_ftpexplorer",    0x0000000e, 'FTP Explorer'),
39     array("module_frigateftp",     0x0000000f, 'Frigate3 FTP'),
40     array("module_securefx",       0x00000010, 'SecureFX'),
41     array("module_ultrafxp",       0x00000011, 'UltraFXP'),
42     array("module_ftprush",        0x00000012, 'FTPRush'),
43     array("module_websitepublisher", 0x00000013, 'WebSitePublisher'),
44     array("module_bitkinex",       0x00000014, 'BitKinex'),
45     array("module_expandrive",     0x00000015, 'Expandrive'),
46     array("module_classicftp",     0x00000016, 'ClassicFTP'),
47     array("module_fling",         0x00000017, 'Fling'),
48     array("module_softx",         0x00000018, 'SoftX'),
49     array("module_dopus",          0x00000019, 'Directory Opus'),
50     array("module_freeftp",        0x0000001a, 'FreeFTP / DirectFTP'),
51     array("module_leapftp",        0x0000001b, 'LeapFTP'),
52     array("module_winscp",        0x0000001c, 'WinSCP'),
53     array("module_32bitftp",      0x0000001d, '32bit FTP'),
54     array("module_netdrive",      0x0000001e, 'NetDrive'),
55     array("module_webdrive",      0x0000001f, 'WebDrive'),
```

```
1 <?php
2
3 define('CLOG_SOURCE_GATE', 'gate');
4 define('CLOG_SOURCE_REPORT', 'report');
5 define('CLOG_SOURCE_LOGIN', 'login');
6 define('CPONY_FTP_TABLE', 'pony_ftp');
7 define('CPONY_FREPORT_TABLE', 'pony_report');
8 define('CPONY_REPORT_DATA_TABLE', 'pony_report_data');
9 define('CPONY_DOMAIN_TABLE', 'pony_domain');
10 define('CPONY_LOG_TABLE', 'pony_system_log');
11 define('CPONY_USER_TABLE', 'pony_user');
12 define('CPONY_CERT_TABLE', 'pony_cert');
13 define('CPONY_EMAIL_TABLE', 'pony_email');
14
15 class pony_db
16 {
17     public $db_link;
18     protected $database;
19     public $state;
20     public $privileges;
21     public $auth_cookie;
22     public $user_id;
23     public $login;
24
25     function __construct()
26     {
27         $this->state = true;
28         $this->db_link = null;
29         $this->privileges = '';
30     }
31
32     function connect($host, $user, $pass)
33     {
34         // establish the connection
35         $this->db_link = mysql_connect($host, $user, $pass, true);
36
37         if (!$this->db_link)
38         {
39             $this->state = false;
40             return false;
41         }
42
43         return true;
44     }
45
46     function select_db($database)
47     {
48         if (!$this->state)
49             return false;
50
51         $select_result = mysql_select_db($database, $this->db_link);
52
53         if (!$select_result)
54         {
55             $select_result = mysql_query(sprintf('CREATE DATABASE IF NOT EXISTS %s CHARACTER SET cp1251 COLLATE
```

# Pony panel on zbot proxy network

-Searching for certain strings leads to several more sites with open panels with some sites hosting other malware payload

-Example:



The screenshot shows a web browser window with the address bar containing the URL `www.dc-oc-01.org.ru/4h6fg4h6fg45hf6gh468gh/`. The browser's toolbar includes navigation buttons (back, forward, refresh) and a search bar. Below the toolbar, there are several application icons: 'Apps', 'Getting Started', 'Imported From Firefox', and 'My Applications'. The main content area of the browser displays the title 'Index of /4h6fg4h6fg45hf6gh468gh' in a large, bold, black font. Below the title, there is a list of two items, each preceded by a bullet point and underlined in blue: 'Parent Directory' and 'DC.exe'.

# Pony panel on zbot proxy network

SHA256: 431cdc5df0009d304ec623cbe1245408010d1a0adfe85f6cfec6159449810ff9

File name: aodgei.exe

Detection ratio: 29 / 48

Analysis date: 2014-03-15 17:50:52 UTC ( 2 months ago )



Analysis

File detail

Additional information

Comments 0

Votes

Antivirus	Result	Update
AVG	Agent4.ASJA	20140314
Ad-Aware	Gen:Variant.Kazy.188707	20140315
Agnitum	Backdoor.Androm!7fF1rDK2mk	20140313
AntiVir	TR/Kazy.188707	20140315
Avast	MSIL:Agent-AME [Trj]	20140315
Baidu-International	Backdoor.Win32.Androm.AJ	20140315
BitDefender	Gen:Variant.Kazy.188707	20140315
Comodo	UnclassifiedMalware	20140315
ESET-NOD32	a variant of MSIL/Kryptik.KP	20140315
Emsisoft	Gen:Variant.Barys.26071 (B)	20140315
F-Secure	Gen:Variant.Kazy.188707	20140315
Fortinet	MSIL/Kryptik.KP	20140315
GData	Gen:Variant.Kazy.188707	20140315

# Pony panel on zbot proxy network

[epvpcash.net16.net/Panel/temp/](http://epvpcash.net16.net/Panel/temp/)

[hgfhgfhgfhfg.net/pony/temp/](http://hgfhgfhgfhfg.net/pony/temp/)

<http://pantamati.com/dream/Panel/temp/>

<http://pantamati.com/wall/Panel/temp/>

[mastermetr.ru/steal/Panel/temp/](http://mastermetr.ru/steal/Panel/temp/)

[microsoft.blg.lt/q/temp/](http://microsoft.blg.lt/q/temp/)

[santeol.su/p/temp/](http://santeol.su/p/temp/)

[terra-araucania.cl/pooo/temp/](http://terra-araucania.cl/pooo/temp/)

[thinswares.com/panel/temp/](http://thinswares.com/panel/temp/)

[www.broomeron.com/pn2/temp/](http://www.broomeron.com/pn2/temp/)

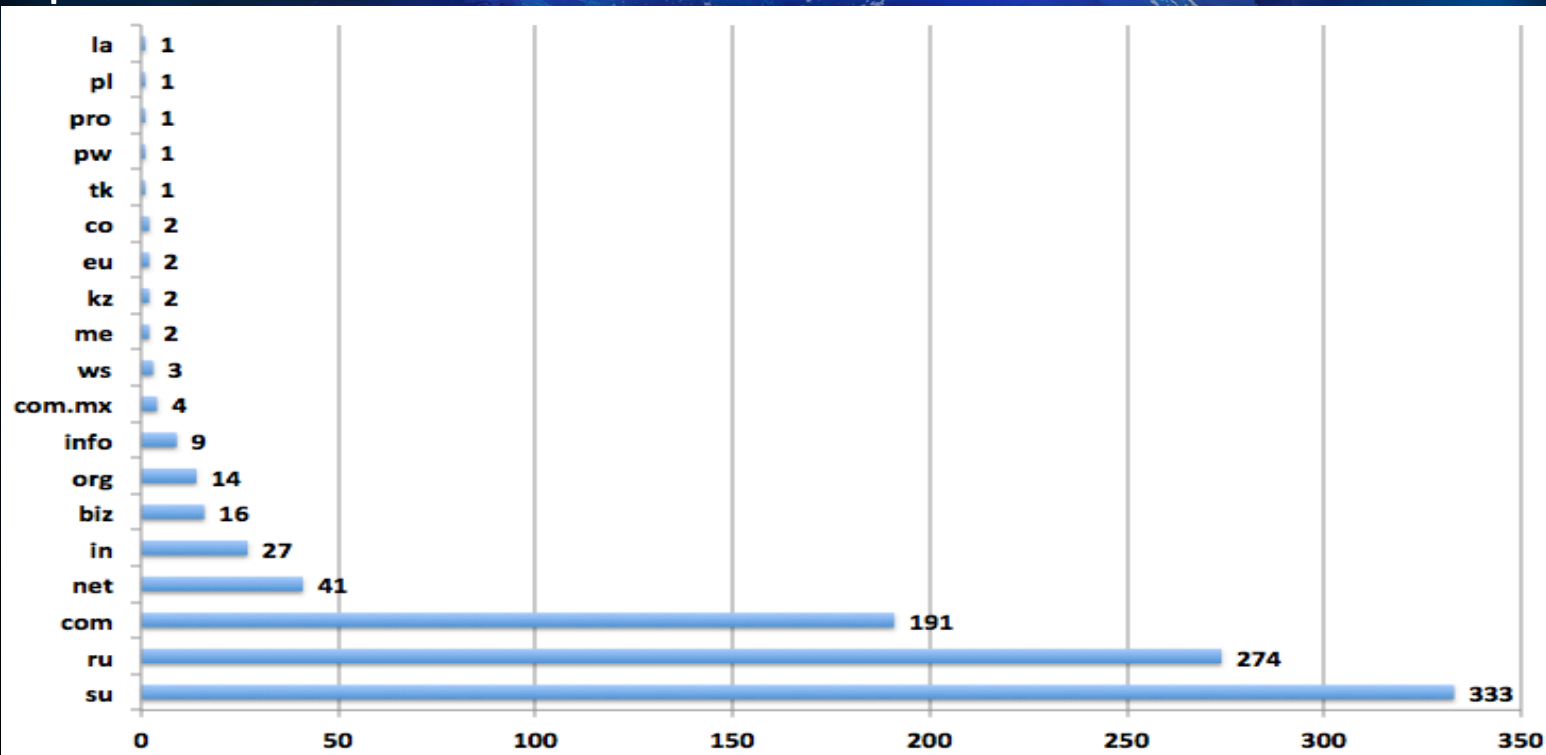
[www.kimclo.com/cli/temp/](http://www.kimclo.com/cli/temp/)

[www.sumdfase2.net/adm/temp/](http://www.sumdfase2.net/adm/temp/)

[www.tripplem2.com/images/money/temp/](http://www.tripplem2.com/images/money/temp/)

# TLD distribution of CnC

Sample of 925 zbot CnC domains



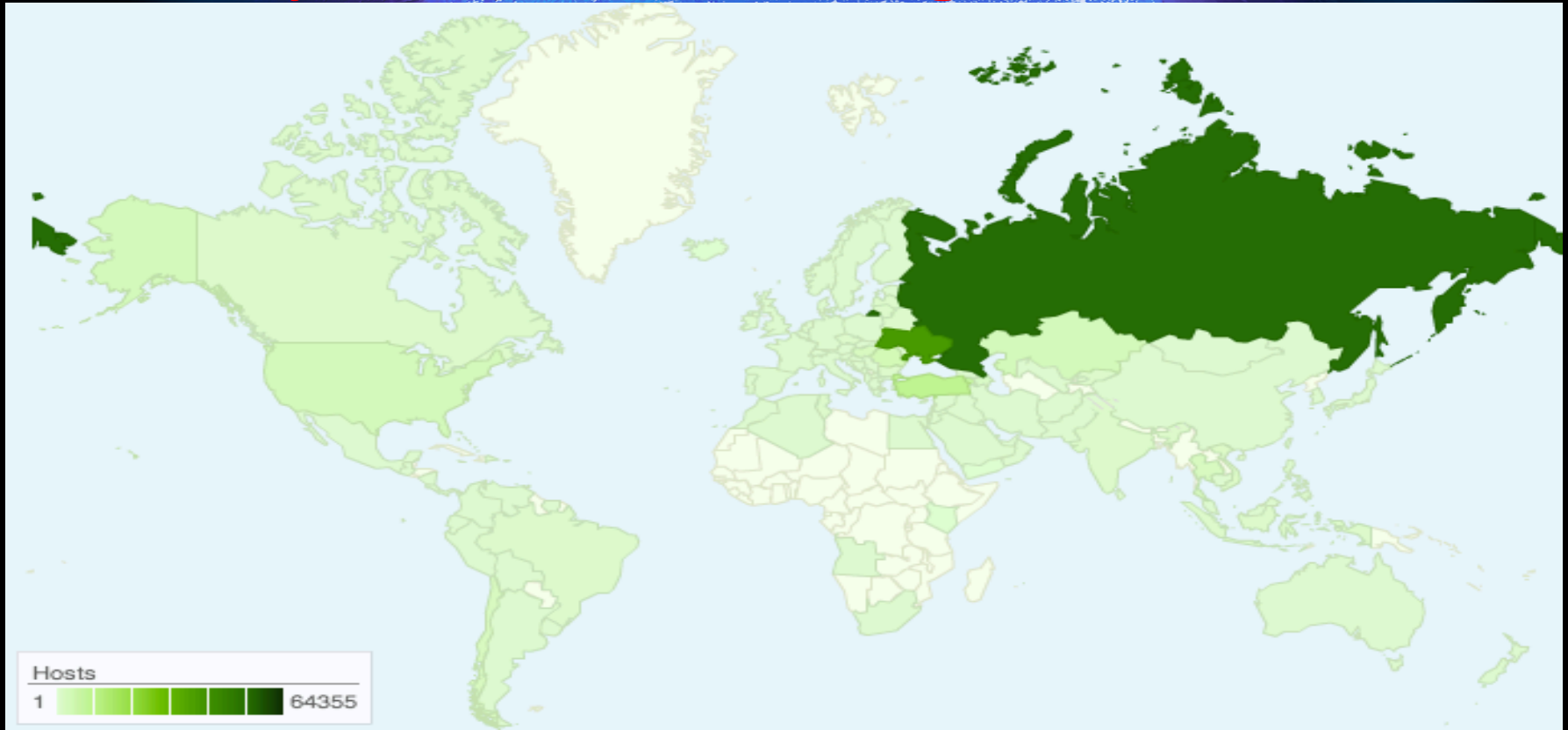
# Proxy network hosts geo-distribution

Sample of 170,208 IPs of the zbot proxy network [Map](#)

64648	RU
47480	UA
11252	TR
8790	AM
4198	RO
3943	KZ
3616	US
2552	TH
2391	CL
2345	HU
1508	AZ
1414	VN
1245	IN
1089	LT

1040	BY
969	LV
910	KG
807	ID
685	BG
617	CA
539	AR
524	BR
452	TW
378	TN
351	EE
325	PH

# Proxy network hosts geo-distribution





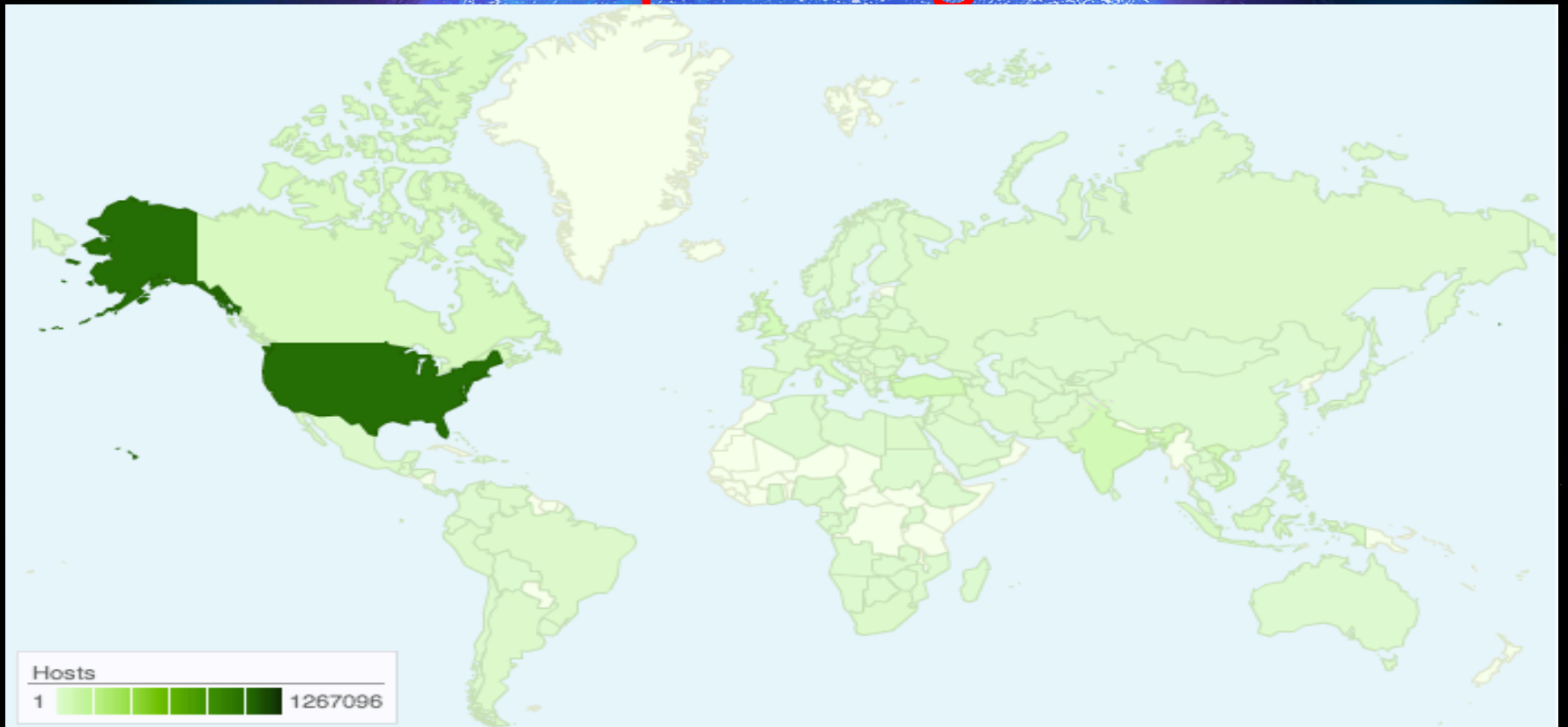
# Clients phoning to CnCs

2,220,230 DNS lookups to CnCs over 24 hours [Map](#)

1296911	US
87436	IN
86067	TR
76196	GB
74927	VN
58677	CA
52584	IT
51730	BE
36676	UA
31794	ID
25091	ES
24750	ZA
20928	BR
20324	VE
18041	IQ

16454	PH
16351	MX
13181	EG
12919	PE
12468	MY
11488	PK
10727	RU
9698	PL
9599	IR
8762	SG
8674	AR
8137	KR
6815	DE

# Clients phoning to CnCs



# CnC domains and related samples

- Sample of 337 zbot CnC domains
- 208 different samples (sha256 communicated with the CnCs)

## Top recorded sample names:

Trojan[Spy]/Win32.Zbot

TrojanDownloader:Win32/Upatre

- Upatre is used as a downloader for Zeus GameOver
- Sent as attachment in spam emails delivered by Cutwail botnet



**Part 2:**

**Catching Malware IP style**

# Motivation

- Examine malicious IP ranges in certain ASNs from a new perspective
- Look beyond the simple counting of number of bad domains, bad IPs hosted on prefixes of an ASN

## How ?

- Look at topology of AS graph
- Look at finer granularity than BGP prefix: sub-allocated ranges within BGP prefixes

  
**black hat**<sup>®</sup>  
USA 2014

# INTERNET 101 & BGP

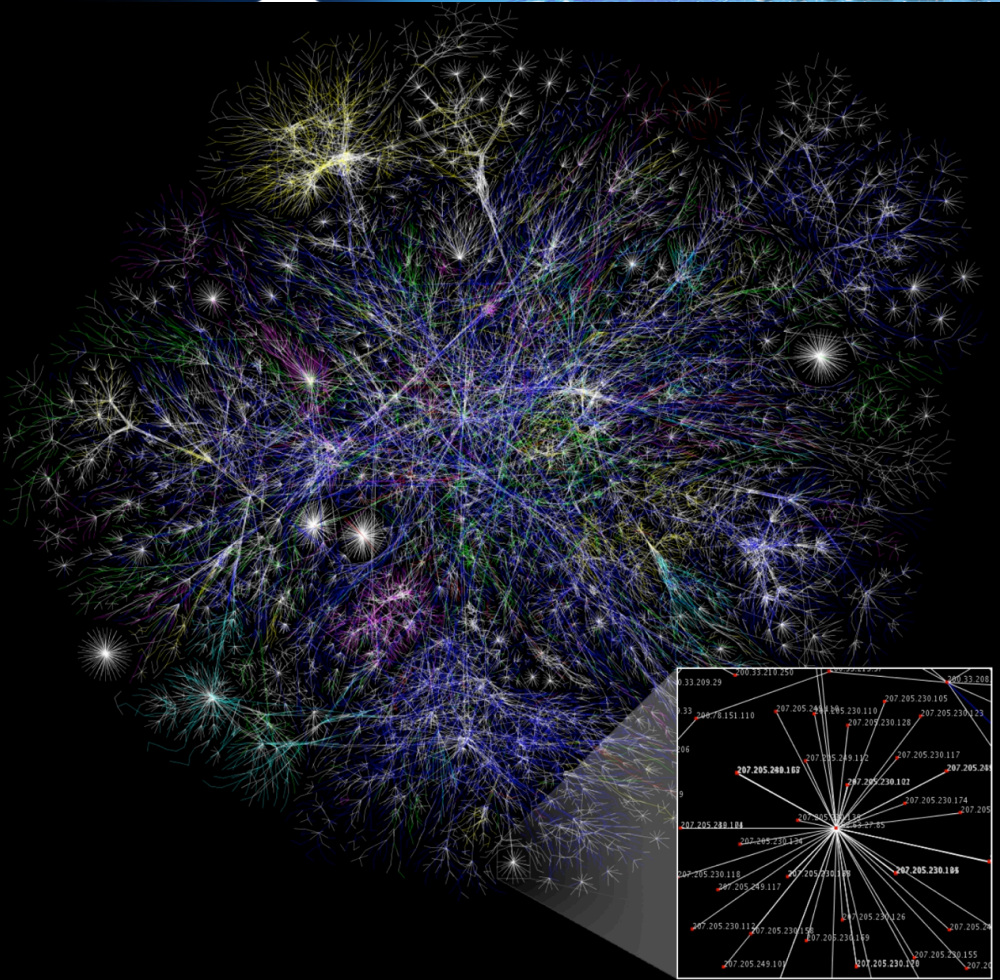


# INTERNET 101 & BGP



*This, Jen, is The Internet*

# MEET THE INTERNET



Network of Networks, it's a Graph!

Each organizations on the Internet is called an Autonomous system.

Each dot represents an Autonomous system (AS).

AS is identified by a number. OpenDNS is 36692, Google is 15169.

Each AS has one or more Prefixes. 36692 has 56 (ipv4 and IPv6) network prefixes.

BGP is the glue that makes this work!



# AS graph

- BGP routing tables
- Valuable data sources
- Routeviews
- Cidr-report
- Hurricane Electric database <http://bgp.he.net/>
- **500,000+ BGP prefixes**
- **46,000+ ASNs**

# AS 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, NLNR has used Route Views data for [AS path visualization](#) (see also [NLNR](#)), 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:

# AS graph

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

[BGP Home](#) [BGP Table](#) [CIDR](#) [BGP Updates](#) [IPv4](#) [IPv6](#) [ASNs](#) [Resource Distributions](#)



Original Concept: Tony Bates, Revised by: Philip Smith, Further Revised: [Geoff Huston](#)

IPv6 CIDR Report: [www.cidr-report/v6](http://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](#)

# AS graph

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



HURRICANE ELECTRIC  
INTERNET SERVICES

Search

## BGP Prefix Report

### Quick Links

[BGP Toolkit Home](#)  
[BGP Prefix Report](#)  
[BGP Peer Report](#)  
[Bogon Routes](#)  
[World Report](#)  
[Multi Origin Routes](#)  
[DNS Report](#)  
[Top Host Report](#)  
[Internet Statistics](#)  
[Looking Glass](#)  
[Free IPv6 Tunnel](#)  
[IPv6 Certification](#)  
[IPv6 Progress](#)  
[Going Native](#)  
[Contact Us](#)

Prefixes Bogons Networks Countries v4 Countries v6 Distribution



# AS graph

- Build AS graph
- Directed graph: node=ASN, a directed edge from an ASN to an upstream ASN
- TABLE\_DUMP2|1392422403|B|96.4.0.55|11686|67.215.94.0/24|11686 4436 2914 36692|IGP|96.4.0.55|0|0||NAG||



# AS graph

## Focus of this study:

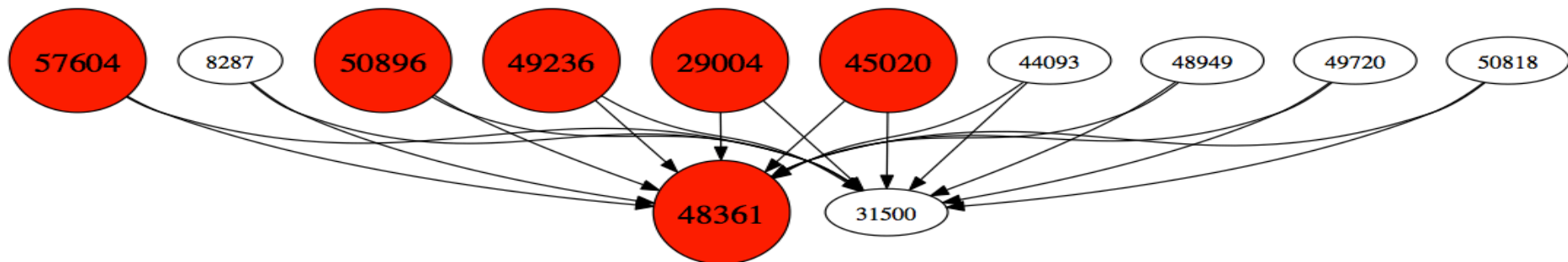
- Peripheral ASNs that are siblings, i.e. they have common parents in the AS graph (share same upstream AS)
- Cluster peripheral ASNs by country
- Find interesting patterns: certain siblings in certain countries are delivering similar suspicious campaigns

**Use Case 1:  
Suspicious Sibling Peripheral ASNs**



# Peripheral ASNs and their upstreams

- January 8<sup>th</sup> topology snapshot, Ukraine, Russia



- 10 sibling peripheral ASNs with 2 upstream ASNs
- /23 or /24 serving TrojWare.Win32.Kryptik.AXJX
- Trojan-Downloader.Win32.Ldmon.A



# Peripheral ASNs and their upstreams



SHA256: 8a8efe86fe1f4371827c6400dd16d3e5bb5a8a5d0d834908f6ab219c102affcf  
File name: 370852074  
Detection ratio: 28 / 47  
Analysis date: 2013-11-22 11:05:34 UTC ( 3 months ago )

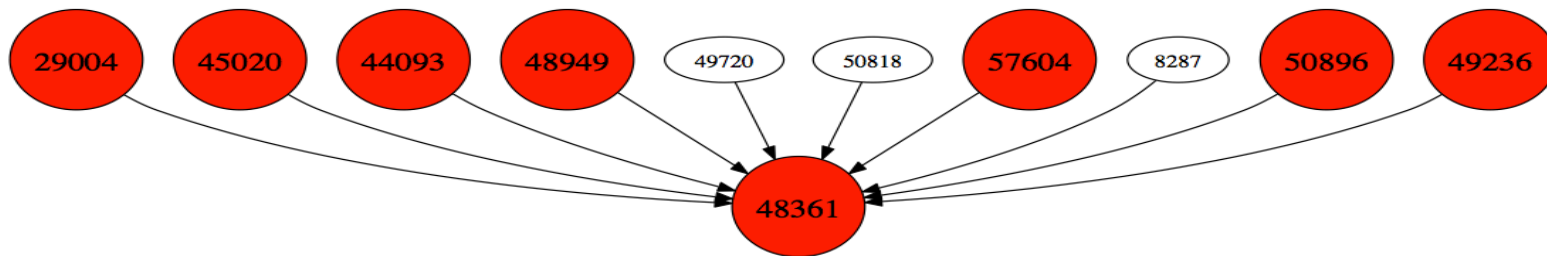


Analysis File detail Additional information Comments 0 Votes Behavioural information

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

# Peripheral ASNs and their upstreams

- February 21<sup>st</sup> topology snapshot, Ukraine, Russia



- AS31500 detached itself from the peripheral ASNs (stopped announcing their prefixes)
- More peripherals started hosting suspicious payload domains
- 3100+ malware domains on 1020+ IPs hosting malware

# Peripheral ASNs and their upstreams

- Taking a sample of 160 live IPs
- Server setup is similar:

## 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)

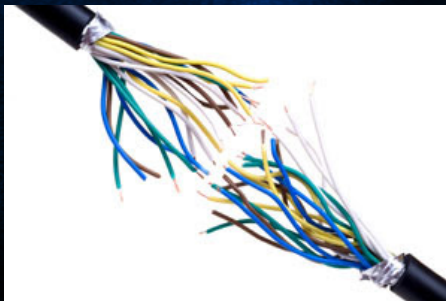
80/tcp open http?

# Peripheral ASNs and their upstreams

- The payload url were live on the entire range of IPs 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:  
Detecting Sibling ASNs through BGP outages**



# BGP MESSAGES

Two important BGP message types:

1. Update messages to announce a new path for a one or more prefixes
2. Withdrawal messages to inform BGP speakers that a certain prefix can no longer be reached.

By correlating these messages we can detect outages globally and in real time

# SIBLING ASNS

All hosting same malware

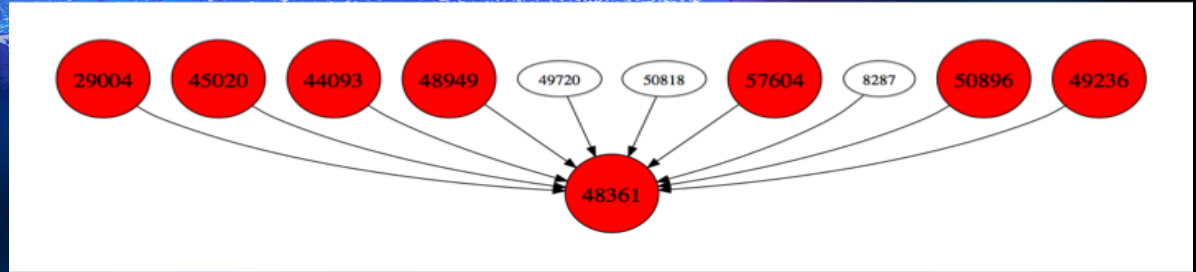


# OVERLAPPING BGP OUTAGES

	57604	8287	50896	49236	29004	45020	44093	48949	49720	50818	48361
57604x		20	17	12	22	16	11	24	20	13	5
8287	20x		41	15	17	17	15	18	18	15	5
50896	17	41x		17	16	17	18	19	16	18	7
49236	12	15	17x		8	15	13	8	12	17	3
29004	22	17	16	8x		12	22	28	18	9	6
45020	16	17	17	15	12x		12	12	12	15	4
44093	11	15	18	13	22	12x		16	10	13	6
48949	24	18	19	8	28	12	16x		20	9	8
49720	20	18	16	12	18	12	10	20x		10	4
50818	13	15	18	17	9	15	13	9	10x		4
48361	5	5	7	3	6	4	6	8	4	4x	



# OVERLAPPING BGP OUTAGES



	57604	29004	48361
57604		22	5
29004	22		6
48361	5	6	

Overlapping outages

ISP 48361	AS57604 91.233.89.0/24	AS29004 195.39.252.0/23
no outage	down for 35 minutes 2013-07-12 18:53 - 2013-07-12 19:28	down for 36 minutes 2013-07-12 18:53 - 2013-07-12 19:29
no outage	down for 497 minutes 2013-07-12 21:33 - 2013-07-13 05:50	down for 497 minutes 2013-07-12 21:33 - 2013-07-13 05:50
no outage	down for 479 minutes 2013-07-22 21:57 - 2013-07-23 05:56	down for 479 minutes 2013-07-22 21:57 - 2013-07-23 05:56
no outage	down for 33 minutes 2013-07-23 18:51 - 2013-07-23 19:24	down for 33 minutes 2013-07-23 18:51 - 2013-07-23 19:24
no outage	down for 63 minutes 2013-07-29 04:54 - 2013-07-29 05:57	down for 63 minutes 2013-07-29 04:54 - 2013-07-29 05:57



- Unique approach for finding related ASNs
- Overlapping outages could mean
  - Most likely relying on same infrastructure
  - Same Data center
  - Same Routing / Switching infrastructure
  - Same organization hiding behind different ASNs

**Use case 3:  
Malicious sub-allocated ranges**



# Malicious sub-allocated ranges

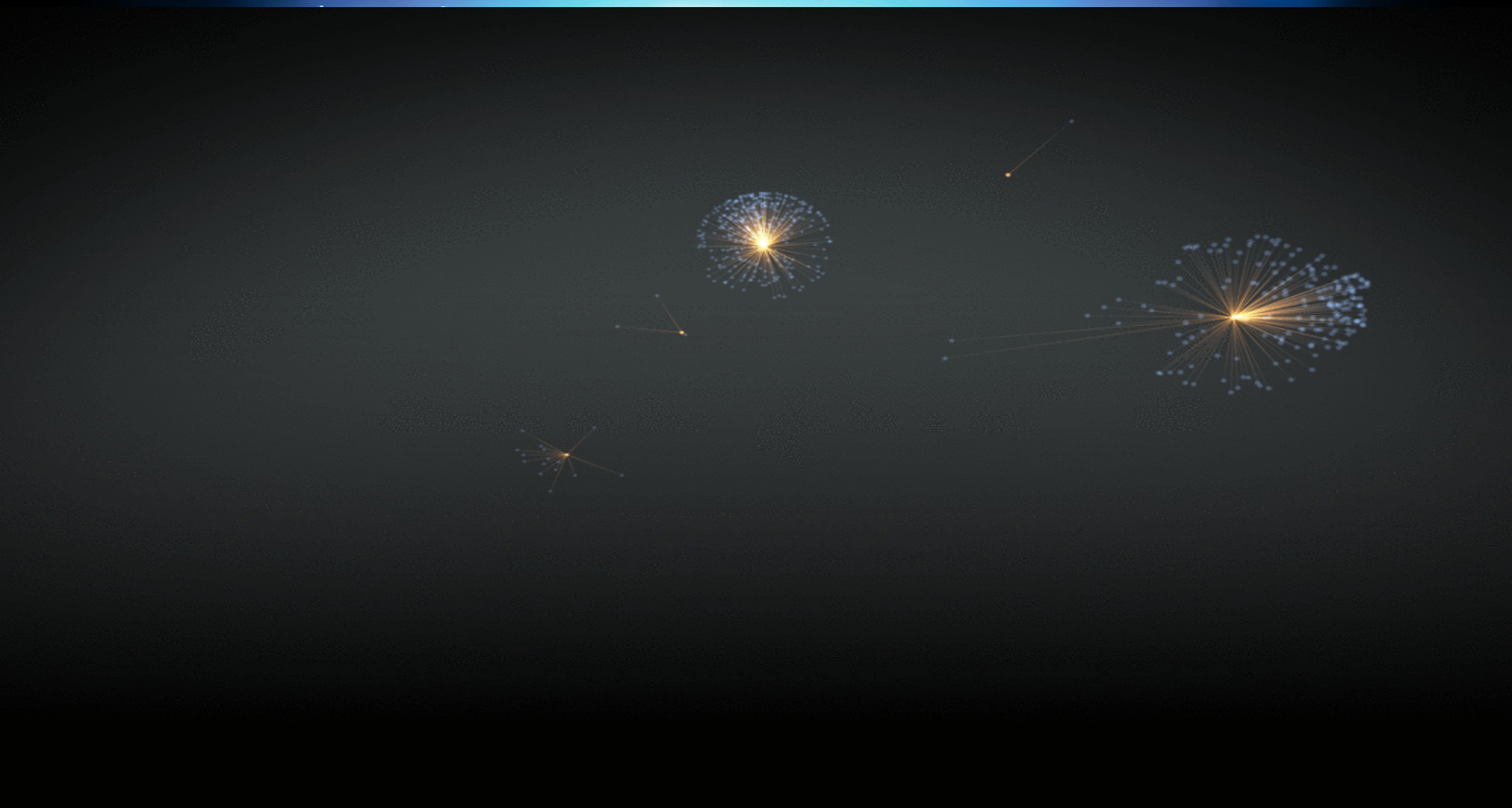
- Case of OVH
- Sub-allocated ranges reserved by same suspicious customers, serving **Nuclear Exploit** kit domains
- Users are lead to the Exploit landing sites through malvertising campaigns, then malware is dropped on victims' machines (e.g. zbot)
- Monitoring patterns for 5 months (Oct 2013-Feb 2014)



*Nuclear Pack v2.0*

# Malicious sub-allocated ranges

- For several months, OVH ranges have been abused
- **Notable fact:** IPs were exclusively used for hosting Nuclear Exploit subdomains, no other sites hosted



2013-11-18

# Malicious sub-allocated ranges

- Some OVH sub-allocated ranges used in Jan-Feb 2014 (now re-assigned)

192.95.50.208 - 192.95.50.215

198.50.183.68 - 198.50.183.71

192.95.42.112 - 192.95.42.127

192.95.6.112 - 192.95.6.127

192.95.10.208 - 192.95.10.223

192.95.7.224 - 192.95.7.239

192.95.43.160 - 192.95.43.175

192.95.43.176 - 192.95.43.191

198.50.131.0 - 198.50.131.15



# Malicious sub-allocated ranges

- Feb 7<sup>th</sup>, bad actors moved to a Ukrainian hosting provider <http://www.besthosting.ua/>
- 31.41.221.143 2014-02-14 2014-02-14 0
- 31.41.221.142 2014-02-12 2014-02-14 2
- 31.41.221.130 2014-02-12 2014-02-14 2
- 31.41.221.140 2014-02-12 2014-02-12 0
- 31.41.221.139 2014-02-12 2014-02-12 0
- 31.41.221.138 2014-02-11 2014-02-12 1
- 31.41.221.137 2014-02-10 2014-02-11 1
- 31.41.221.136 2014-02-10 2014-02-11 1
- 31.41.221.135 2014-02-10 2014-02-10 0
- 31.41.221.134 2014-02-09 2014-02-19 10
- 31.41.221.132 2014-02-08 2014-02-09 1
- 31.41.221.131 2014-02-07 2014-02-08 1



# Malicious sub-allocated ranges

- Feb 14<sup>th</sup>, bad actors moved to a Russian hosting provider <http://pinspb.ru/>
- 5.101.173.10 2014-02-21 2014-02-22 1
- 5.101.173.9 2014-02-19 2014-02-21 2
- 5.101.173.8 2014-02-19 2014-02-19 0
- 5.101.173.7 2014-02-18 2014-02-19 1
- 5.101.173.6 2014-02-18 2014-02-18 0
- 5.101.173.5 2014-02-17 2014-02-18 1
- 5.101.173.4 2014-02-17 2014-02-17 0
- 5.101.173.3 2014-02-16 2014-02-17 1
- 5.101.173.2 2014-02-15 2014-02-16 1
- 5.101.173.1 2014-02-14 2014-02-15 1



# Malicious sub-allocated ranges

- Feb 22<sup>nd</sup>, bad actors moved back to OVH



- **Notable fact:** They change MO, IPs have been allocated and used in the past for other content -> evasion technique or resource recycling
- But during all this time, bad actors still kept the **name server infrastructure on OVH** on ranges reserved by same customers

# Malicious sub-allocated ranges

- 198.50.143.73 2013-11-25 2014-02-24 91
- 198.50.143.69 2013-11-25 2014-02-24 91
- 198.50.143.68 2013-11-25 2014-02-24 91
- 198.50.143.67 2013-11-26 2014-02-24 90
- 198.50.143.65 2013-11-24 2014-02-23 91
- 198.50.143.66 2013-11-25 2014-02-23 90
- 198.50.143.64 2013-11-24 2014-01-25 62
- 198.50.143.75 2013-12-03 2013-12-10 7
- 198.50.143.79 2013-11-25 2013-12-10 15
- 198.50.143.78 2013-11-25 2013-12-10 15
- 198.50.143.74 2013-11-25 2013-12-10 15
- 198.50.143.72 2013-11-25 2013-12-10 15
- 198.50.143.71 2013-11-25 2013-12-10 15
- 198.50.143.76 2013-11-25 2013-12-09 14
- 198.50.143.70 2013-11-26 2013-12-09 13
- 198.50.143.77 2013-11-26 2013-12-05 9



# Malicious sub-allocated ranges

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

🏠 > Blog > February 2014 > When IPs go Nuclear

## 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 @maleka\_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

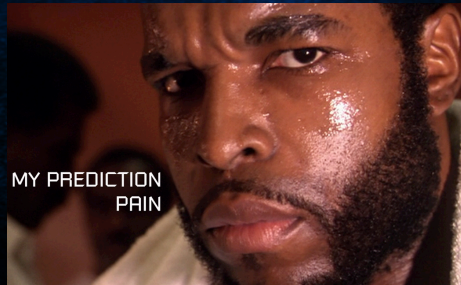
### ARCHIVES

- February 2014
- January 2014
- December 2013
- November 2013





# Predicting malicious domains IP infrastructure



# Tracking reserved ranges

- Reserved ranges on OVH by same malicious customer
- Dec 1<sup>st</sup> to 31<sup>st</sup> 2013: **28 ranges, 136 IPs, 86 used**
- Jan 1<sup>st</sup> to 31<sup>st</sup> 2014: **11 ranges, 80 IPs, 33 used**
- Feb 1<sup>st</sup> to 28<sup>th</sup> 2014: **4 ranges, 28 IPs, 26 used**
- Mar 1<sup>st</sup> to 20<sup>th</sup> 2014: **43 ranges,**
  - **40 ranges** on Mar 7<sup>th</sup> , **352 IPs, 208 used**
  - **3 ranges** on Mar 10<sup>th</sup> , **12 IPs, 7 used**
- Used for Nuclear EK domains, Nuclear domains' name servers, and browlock

# Tracking reserved ranges

- 86 ranges are all in these 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



# Malicious sub-allocated ranges

- For Nuclear, In addition to sub-allocated ranges reserved by same actors (for OVH case)
- The live IPs all have same server setup (fingerprint):
- 31.41.221.131 to 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 to 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

# Malicious sub-allocated ranges

- 198.50.143.64 to 198.50.143.79

22/tcp open ssh OpenSSH 5.5p1 Debian 6+squeeze4 (protocol 2.0)

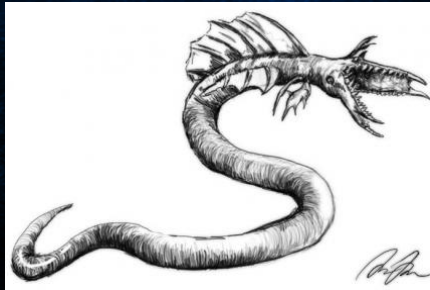
80/tcp open http nginx web server 0.7.67

445/tcp filtered microsoft-ds

- In some cases, IPs are brought online in small chunks
- The name server IPs also have the same fingerprint
- The combination of these different indicators has made predictions practically always accurate for several months, until bad actors change to a different MO
- Method still efficient when applied to other threats
- -> One can **block/monitor** IPs **before they** even **start hosting** domains



# Detecting Malicious Subdomains under Compromised domains



# Malicious subdomains under compromised domains

- Detecting malicious subdomains injected under compromised domains, most notably GoDaddy domains
- Subdomains serving Exploit kits (e.g. Nuclear, Angler, FlashPack), browlock, malvertising
- Various payloads dropped (e.g. zbot variants, kuluoz)
- Monitoring patterns for 5+ months (Feb 2014-present)

# Malicious subdomains under compromised domains

- Sample of several hundred IPs hosting malicious subdomains
- Top 5 abused ASNs
  - 16276 OVH SAS
  - 24961 myLoc managed IT AG
  - 15003 Nobis Technology Group, LLC
  - 41853 LLC NTCOM
  - 20473 Choopa, LLC

# Malicious subdomains under compromised domains

- OVH most abused with 18% of total collected malicious IPs
- Bad actors shifted MO since Use Case 3 study

# Malicious subdomains under compromised domains

## Before

Abuse ccTLDs (e.g. .pw, .in.net, .ru, etc) using rogue/victim resellers/registrars

Use reserved IPs exclusively for Exploit kit, browlock attacks

Bring attack IPs online in contiguous chunks

Abuse OVH Canada: possible to predictively correlate rogue customers with attack IPs through ARIN rwhois

## Now

Supplement with abusing compromised domains

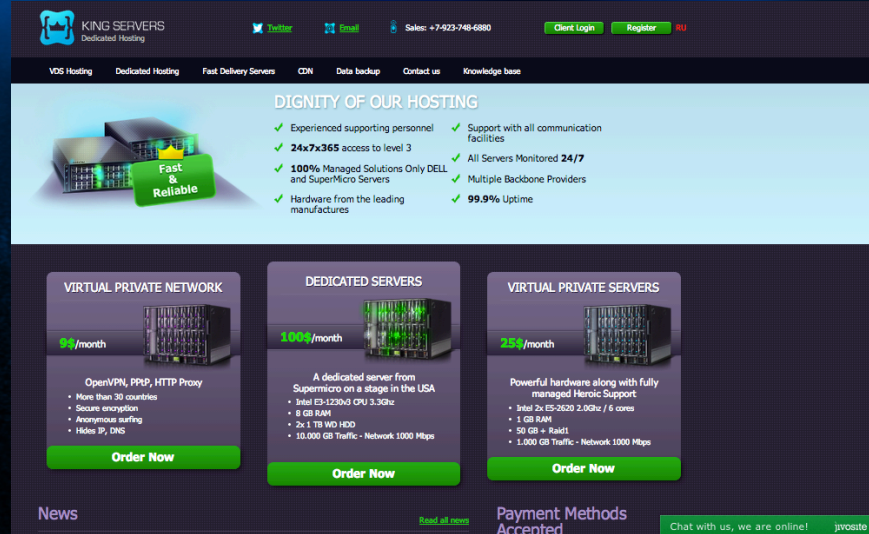
Supplement with using recycled IPs that hosted legit content in the past

Supplement with bringing IPs up in randomized sets or one at a time

Abuse OVH Europe spanning numerous countries' IP pools (e.g. France, Belgium, Italy, UK, Ireland, Spain, Portugal, Germany, Netherlands, Finland, Czech, Russia)

# 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”



The screenshot displays the King Servers website interface. At the top, there is a navigation bar with the company logo, social media links for Twitter and Email, a phone number (+7423-746-6880), and buttons for Client Login and Register. Below the navigation bar, there are several menu items: VDS Hosting, Dedicated Hosting, Fast Delivery Servers, CDN, Data backup, Contact us, and Knowledge base.

The main content area features a section titled "DIGNITY OF OUR HOSTING" with a "Fast & Reliable" badge. This section lists several benefits:

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

Below this section, there are three product cards:

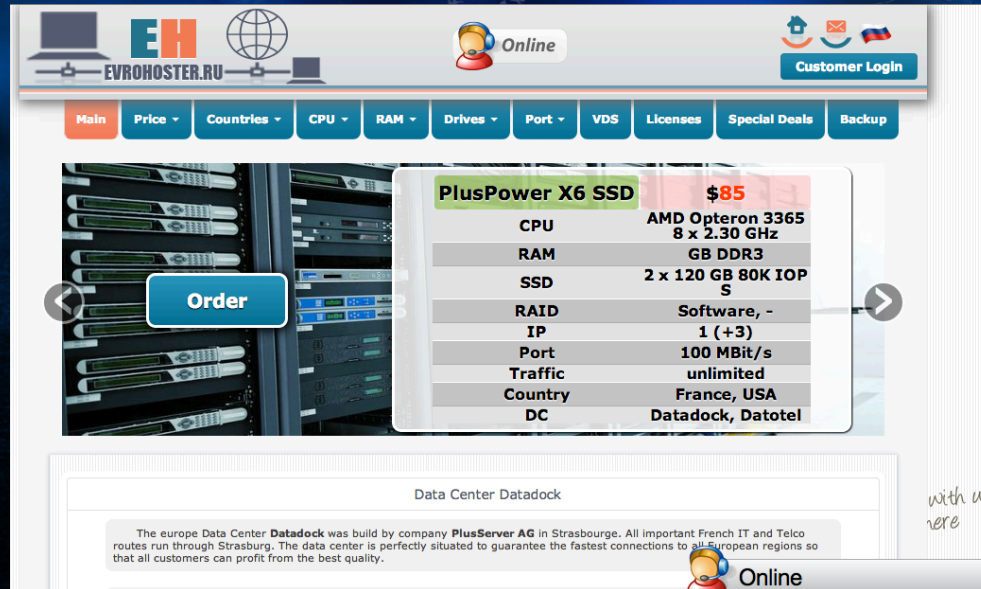
- VIRTUAL PRIVATE NETWORK:** Priced at 99\$/month. Features include OpenVPN, PPTP, HTTP Proxy, support for more than 30 countries, secure encryption, anonymous surfing, and hidden IP/DNS. An "Order Now" button is present.
- DEDICATED SERVERS:** Priced at 100\$/month. Features include a dedicated server from Supermicro on a shelf in the USA, Intel E3-1230V3 CPU 3.3Ghz, 8 GB RAM, 2x 1 TB WD HDD, and 10,000 GB Traffic - Network 1000 Mbps. An "Order Now" button is present.
- VIRTUAL PRIVATE SERVERS:** Priced at 25\$/month. Features include powerful hardware with fully managed Heroic Support, Intel XE-2620 2.0Ghz / 6 cores, 1 GB RAM, 50 GB + Raid1, and 1,000 GB Traffic - Network 1000 Mbps. An "Order Now" button is present.

At the bottom of the page, there are links for "News", "Based all news", "Payment Methods Accepted", and a "Chat with us, we are online!" button with a jivo.ru logo.



# Small abused or rogue hosting providers

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



The screenshot shows the EvroHoster.ru website interface. At the top, there is a navigation bar with the logo 'EH EVROHOSTER.RU', an 'Online' status indicator, and a 'Customer Login' button. Below the navigation bar is a menu with options: Main, Price, Countries, CPU, RAM, Drives, Port, VDS, Licenses, Special Deals, and Backup. The main content area features a server rack image on the left with an 'Order' button. To the right is a configuration table for the 'PlusPower X6 SSD' plan, priced at \$85. Below the table, there is a section for 'Data Center Datadock' with a paragraph of text and a 'with us here' note. At the bottom right, there is an 'Online' status indicator.

PlusPower X6 SSD		\$85
CPU	AMD Opteron 3365	
	8 x 2.30 GHz	
RAM	GB DDR3	
SSD	2 x 120 GB 80K IOP	
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 Strasbourg. All important French IT and Telco routes run through Strasbourg. 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.

with us here

Online

# Small abused or rogue hosting providers

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

QHoster  
Качество без компромиси

Телефон: 02 4372474 | Имате въпрос: [Пишете ни](#)

Начало | Поръчка | Вход за клиенти | Skype: qhoster

ГОРЕЩИ

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

## Виртуални сървъри

Бързина и гъвкавост

СЕГА САМО

**24.95** ЛВ. / МЕСЕЦ

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

VPS ХОСТИНГ

### ХОСТИНГ "МИНИ"

**24.95** ЛВ. / 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

**24.95** ЛВ. / МЕСЕЦ

- > 50 GB дисково пространство
- > 1000 GB месечен трафик
- > Неограничени акаунти
- > Безплатен cPanel/WHM
- > 100% с Вашата търговска марка

### ВИРТУАЛНИ СЪРВЪРИ (VPS)

НОВО

**24.95** ЛВ. / МЕСЕЦ

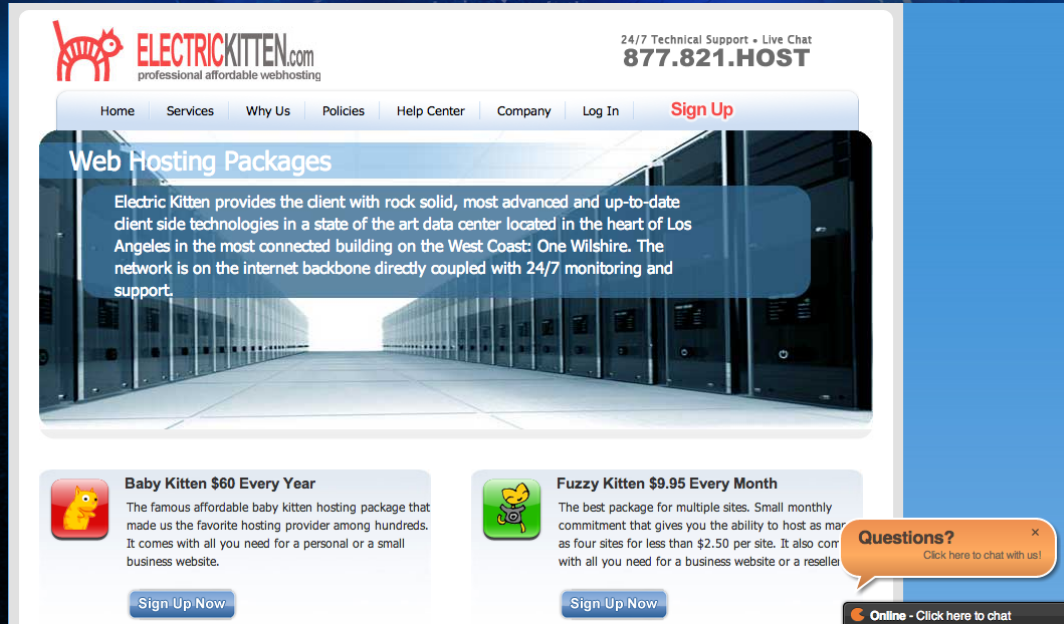
1GB / 40GB / 1TB  
Памет / Диск / Трафик

### НАЕТИ СЪРВЪРИ

**129.95** ЛВ. / МЕСЕЦ

# Small abused or rogue hosting providers

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



The screenshot displays the homepage of Electric Kitten, a web hosting provider. The header includes the company logo (a stylized orange cat), the name "ELECTRICKITTEN.com", and the tagline "professional affordable webhosting". Contact information "24/7 Technical Support • Live Chat" and the phone number "877.821.HOST" are also present. A navigation menu contains links for Home, Services, Why Us, Policies, Help Center, Company, Log In, and Sign Up. The main content area features a "Web Hosting Packages" section with a background image of server racks. A text box describes the company's infrastructure: "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." Below this, two hosting packages are listed: "Baby Kitten \$60 Every Year" and "Fuzzy Kitten \$9.95 Every Month". Each package includes a brief description and a "Sign Up Now" button. A "Questions?" chat bubble is visible in the bottom right corner, and an "Online - Click here to chat" button is at the very bottom.

**ELECTRICKITTEN.com**  
professional affordable webhosting

24/7 Technical Support • Live Chat  
**877.821.HOST**

Home Services Why Us Policies Help Center Company Log In **Sign Up**

## 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.  
[Sign Up Now](#)

**Fuzzy Kitten \$9.95 Every Month**  
The best package for multiple sites. Small monthly commitment that gives you the ability to host as many as four sites for less than \$2.50 per site. It also comes with all you need for a business website or a reseller.  
[Sign Up Now](#)

**Questions?**  
[Click here to chat with us!](#)

**Online - Click here to chat**

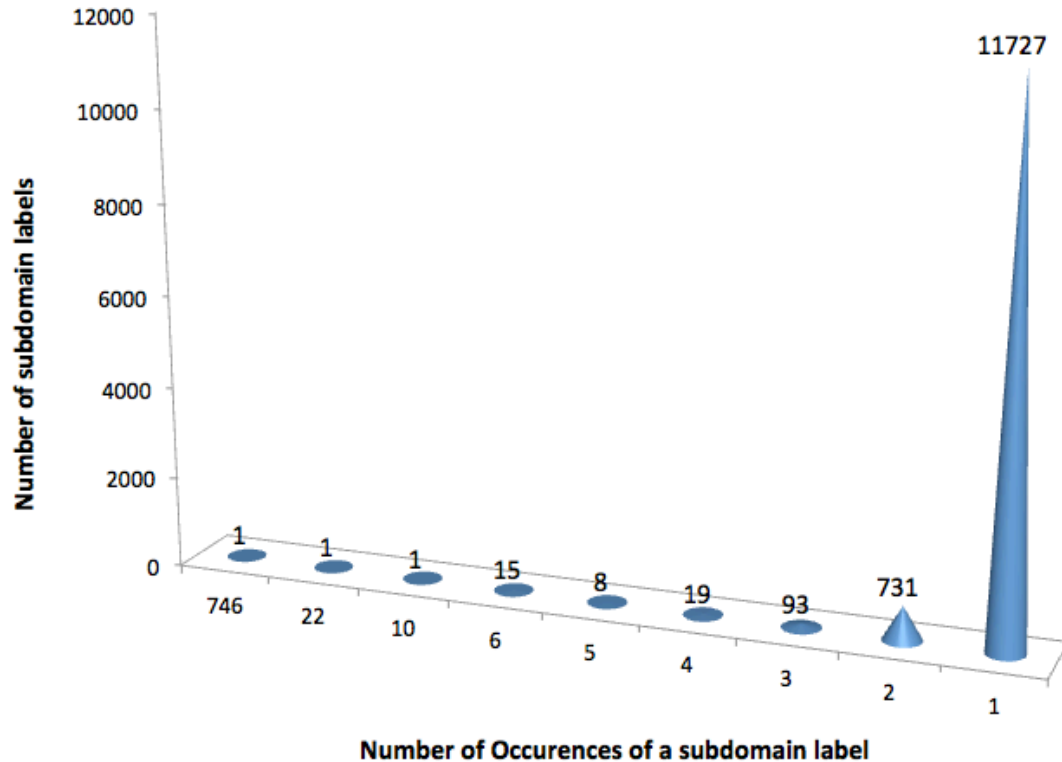
## Small abused or rogue hosting providers

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

# String Analysis of injected subdomains

- Sample of 19,000+ malicious subdomains injected under 4,200+ compromised GoDaddy domains
- 12,000+ different labels
- Top 5 used labels:
  - police
  - alertpolice
  - css
  - windowsmoviemaker
  - solidfileslzs

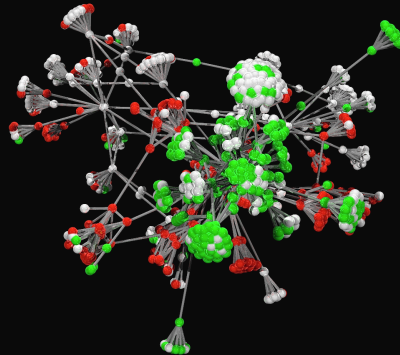
# String Analysis of injected subdomains



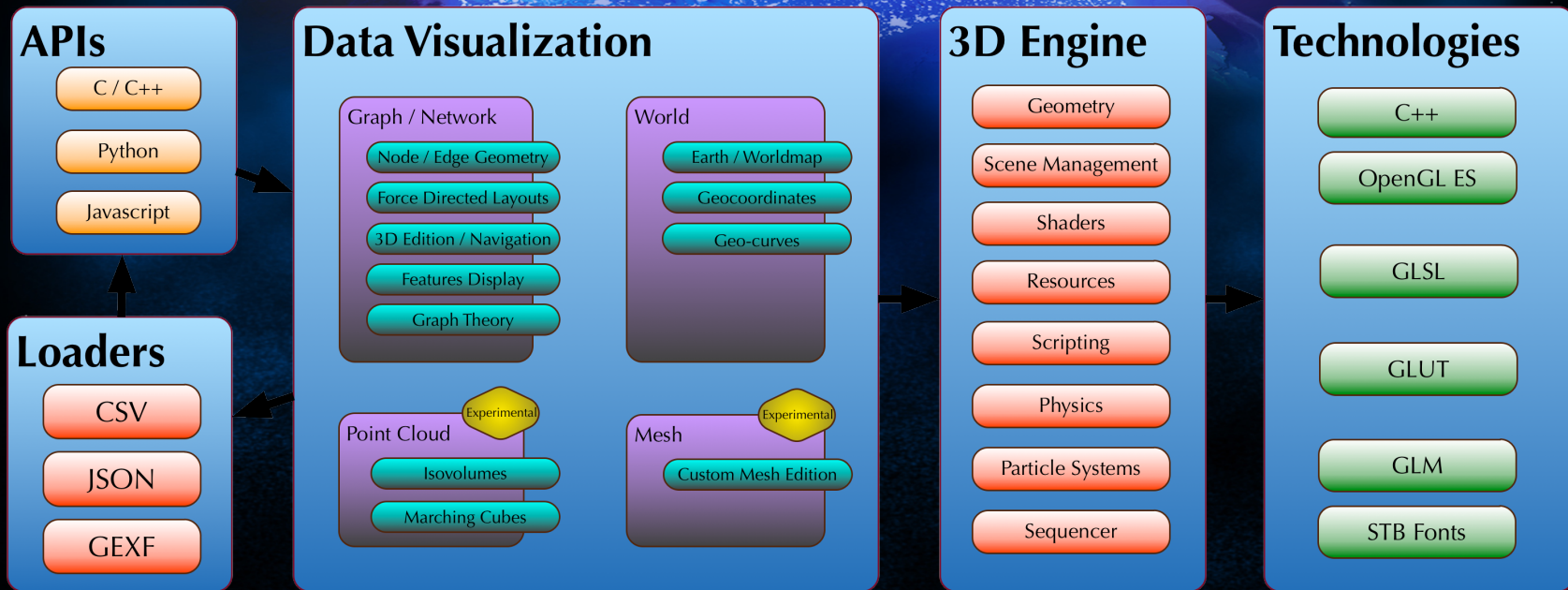


## Part 3:

# Visualizing Knowledge with our 3D engine



# OpenGraphiti





## SemanticNet Python Library

```
#!/usr/bin/env python

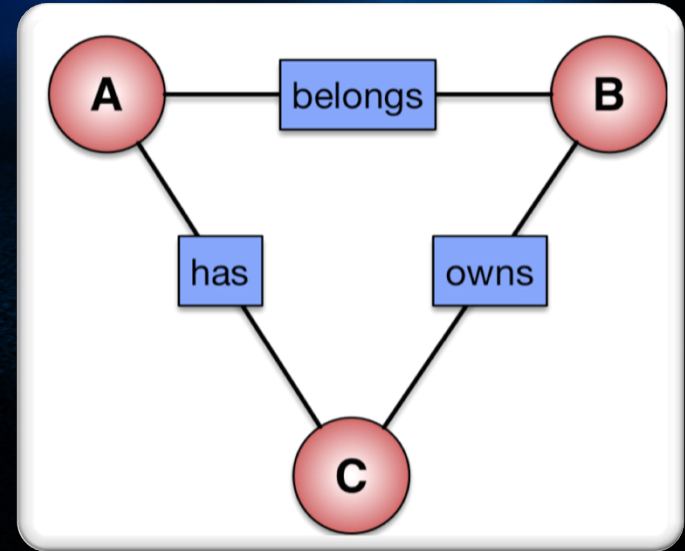
import sys
import semanticnet as sn

graph = sn.Graph()

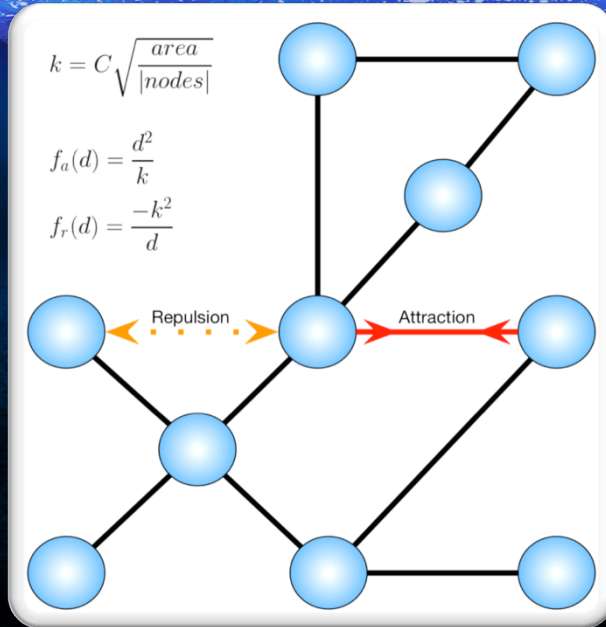
a = graph.add_node({"label": "A"})
b = graph.add_node({"label": "B"})
c = graph.add_node({"label": "C"})

graph.add_edge(a, b, {"type": "belongs"})
graph.add_edge(b, c, {"type": "owns"})
graph.add_edge(c, a, {"type": "has"})

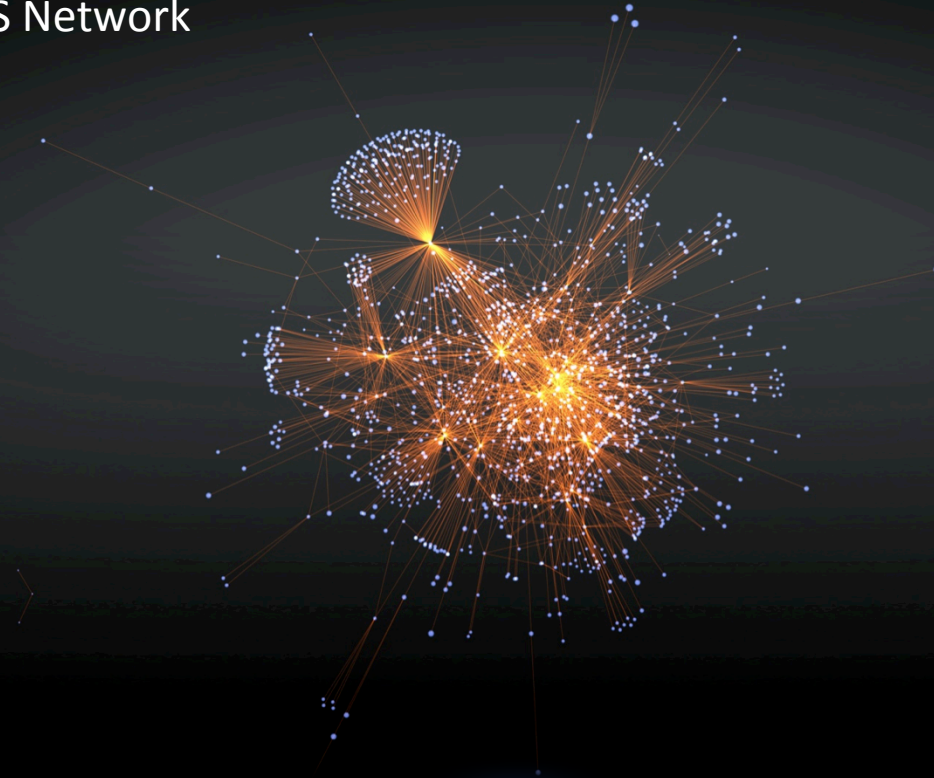
graph.save_json("output.json")
```



# Particle Physics



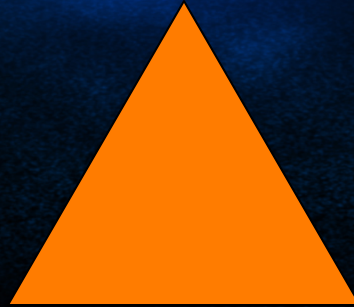
# Canadian AS Network



# Data goes Supernova

3 Generic Approaches

Grouping

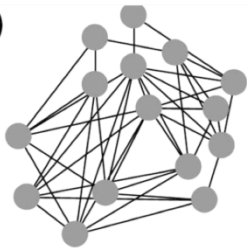


Sampling

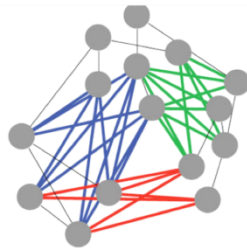
Parallelization

# Entity Grouping

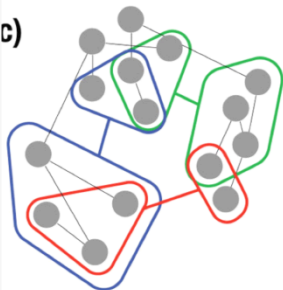
a)



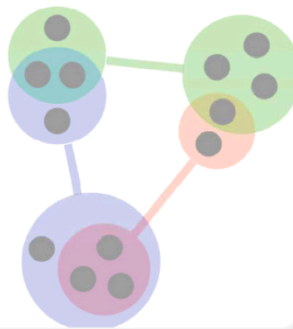
b)



c)

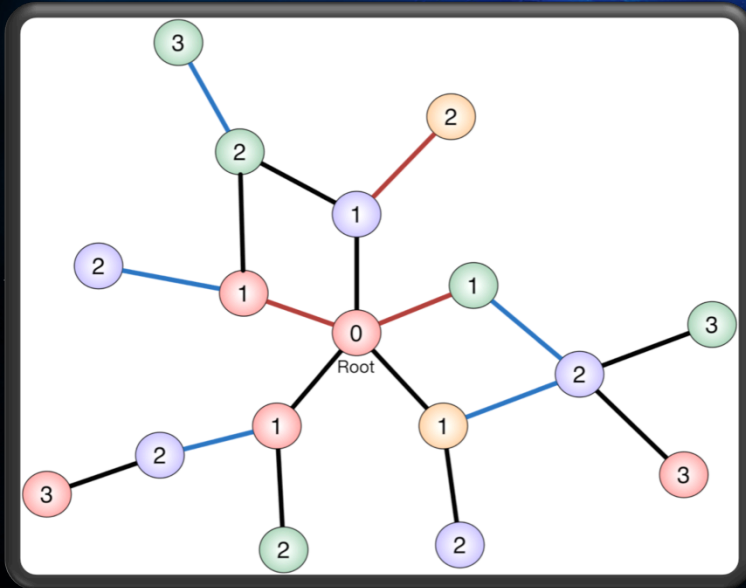


d)

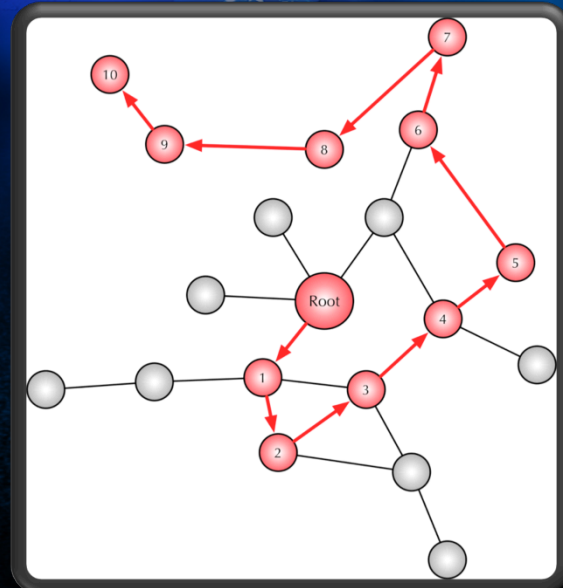


# Sampling

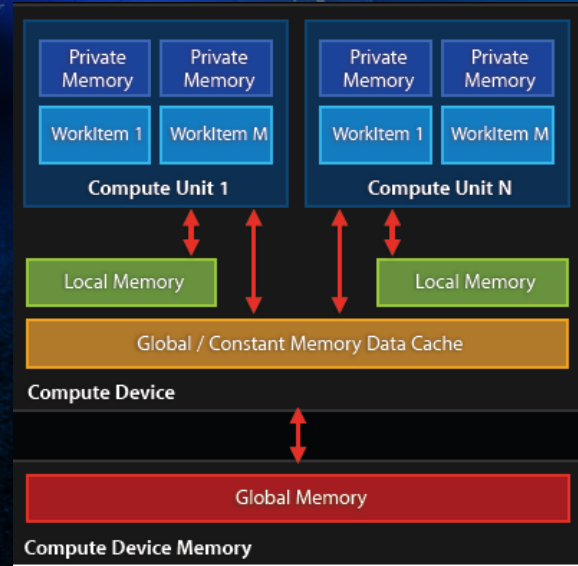
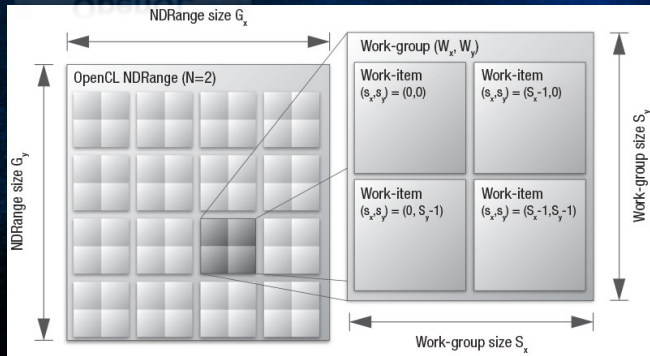
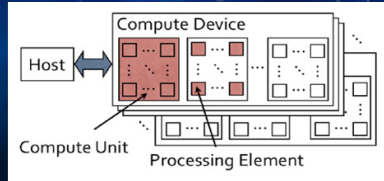
Breadth First Search



Random Walk



# Parallelization

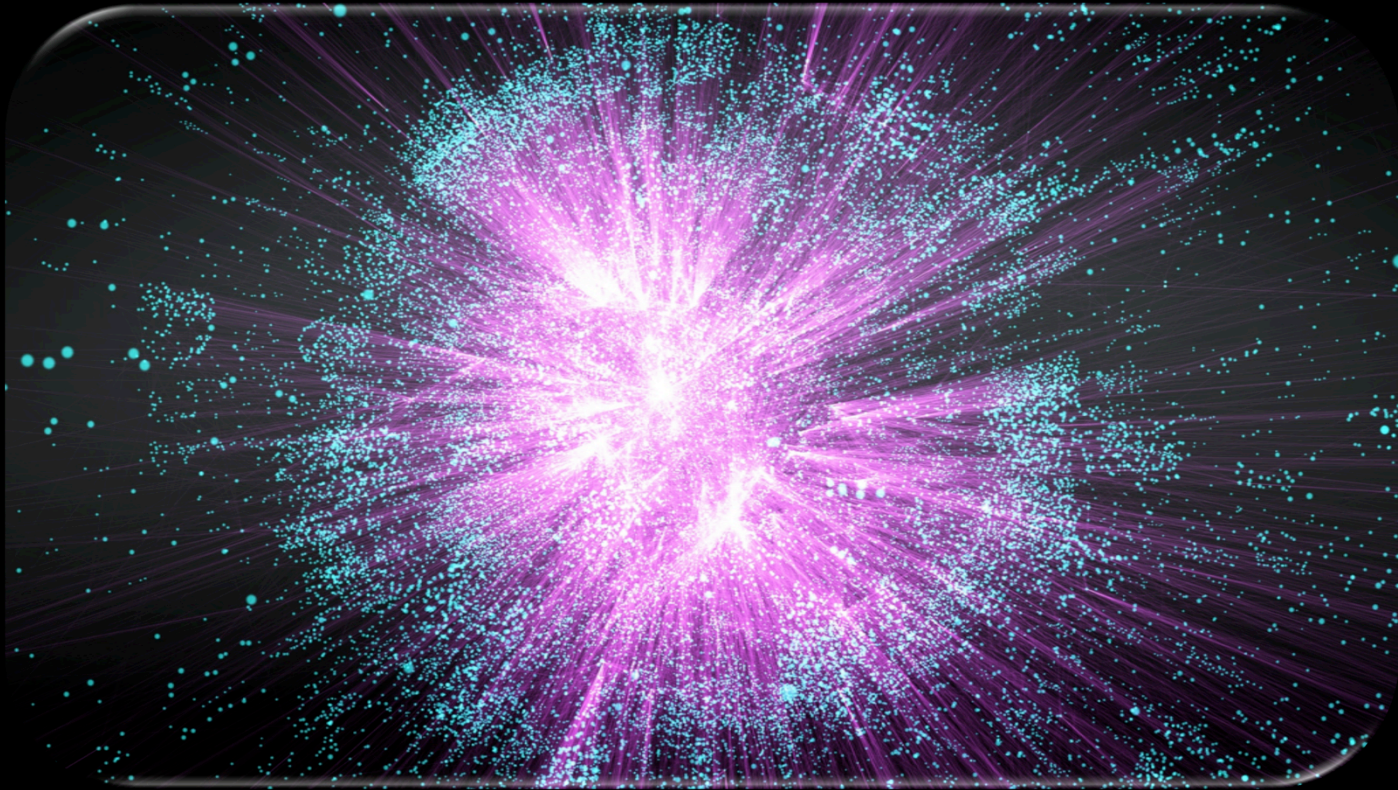


# Why ?

- Actors populate the knowledge graph
- Creation is understood, output is complex
- Layout closer to the “*natural shape*” of data structure
- Take advantage of the GPU to untangle information
- Humans are good at processing shapes and colors



# Full AS Network



# Future Work



# Conclusion

- Efficient methods to catch malware DNS and IP style
- Fast flux botnets used as proxy networks
- Investigate IP space from novel perspectives: AS graph topology, granularity finer than BGP prefix
- Detect suspicious sibling peripheral ASNs
- Detect sibling ASNs using BGP outages monitoring
- Predict malicious IP ranges
- Detect malicious subdomains under compromised domains
- Novel 3D visualization engine used as graph navigation and investigation tool
  - Supports state of the art 3D technologies (Force directed, OpenCL, GLSL Shaders, etc.)

# References

- Distributed Malware Proxy Networks, B. Porter, N. Summerlin, BotConf 2013
- <http://labs.opendns.com/2013/12/18/operation-kelihos-presented-botconf-2013/>
- <http://blog.malwaremustdie.org/2013/12/short-talk-in-botconf-2013-kelihos.html>
- <https://zeustracker.abuse.ch/>
- <http://www.malware-traffic-analysis.net/>
- <http://techhelplist.com/index.php/tech-tutorials/41-misc/465-asprox-botnet-advertising-fraud-general-overview-1>
- VirusTotal



Thank you

(Q & A)