CATCHING MALWARE EN MASSE : DNS & IP STYLE

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

OpenDNS

DHIA MAHJOUB

- Senior Security Researcher at OpenDNS
- PhD graph theory applied on sensor networks
- Security, graphs, data analysis
- @DhiaLite

THIBAULT REUILLE

- Security Researcher at OpenDNS
- Former Software Engineer @ NVIDIA
- Security and Visualization ?
- @ThibaultReuille

ANDREE TOONK

- Manager of Network Engineering at OpenDNS
- Founder and lead of BGPMon.net
- @atoonk

Agenda

OpenDNS presentation

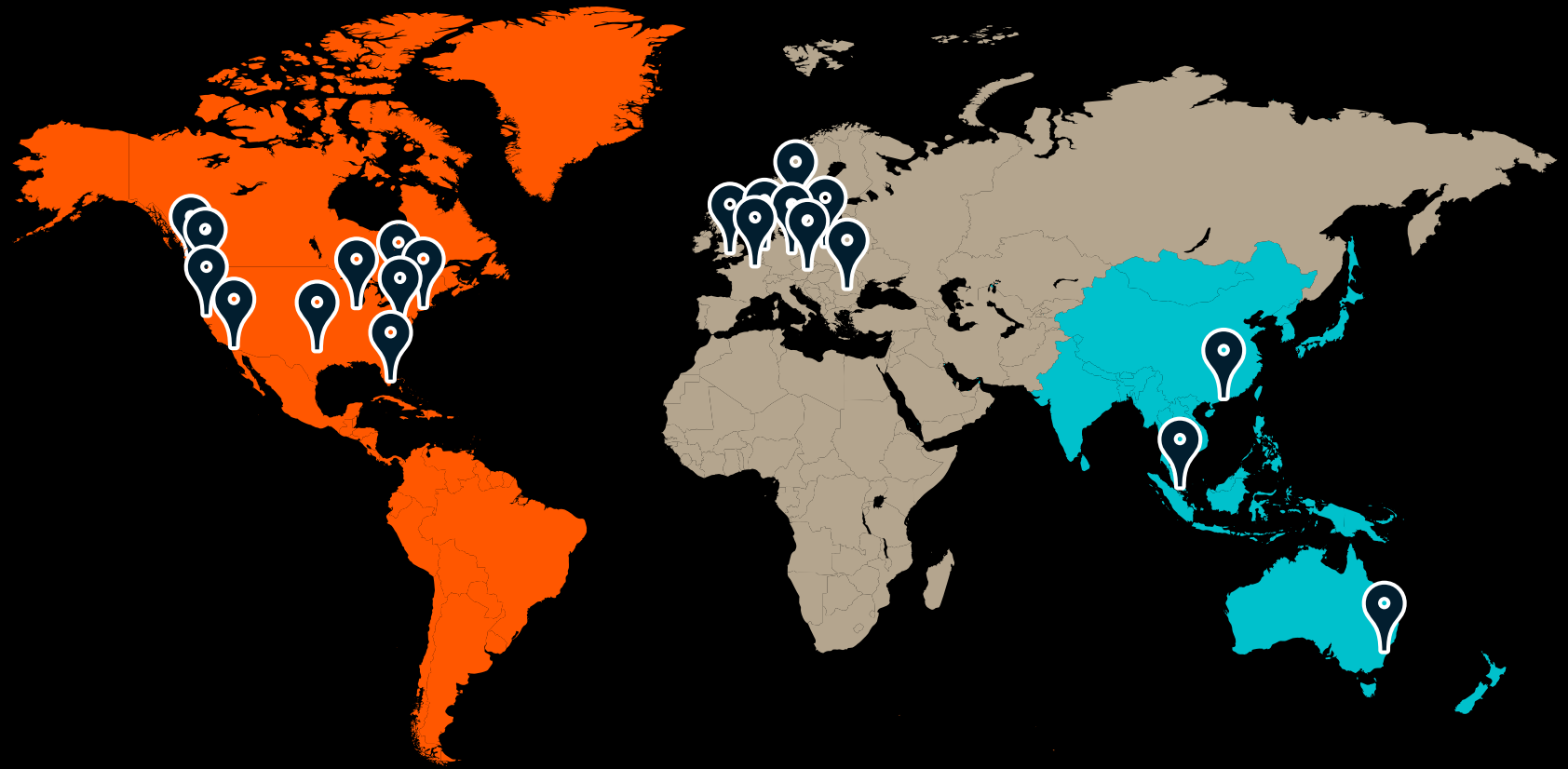
Catching Malware DNS Style

Catching Malware IP style

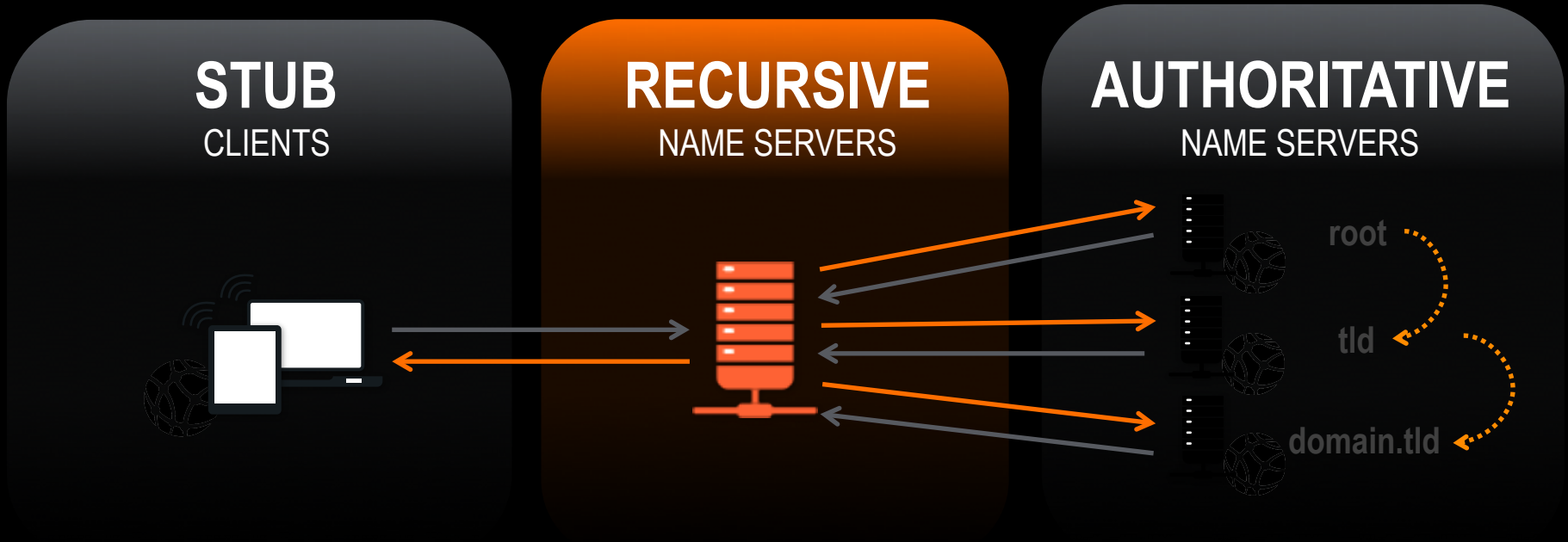
3D Data Visualization

Conclusion

OpenDNS' Network Map

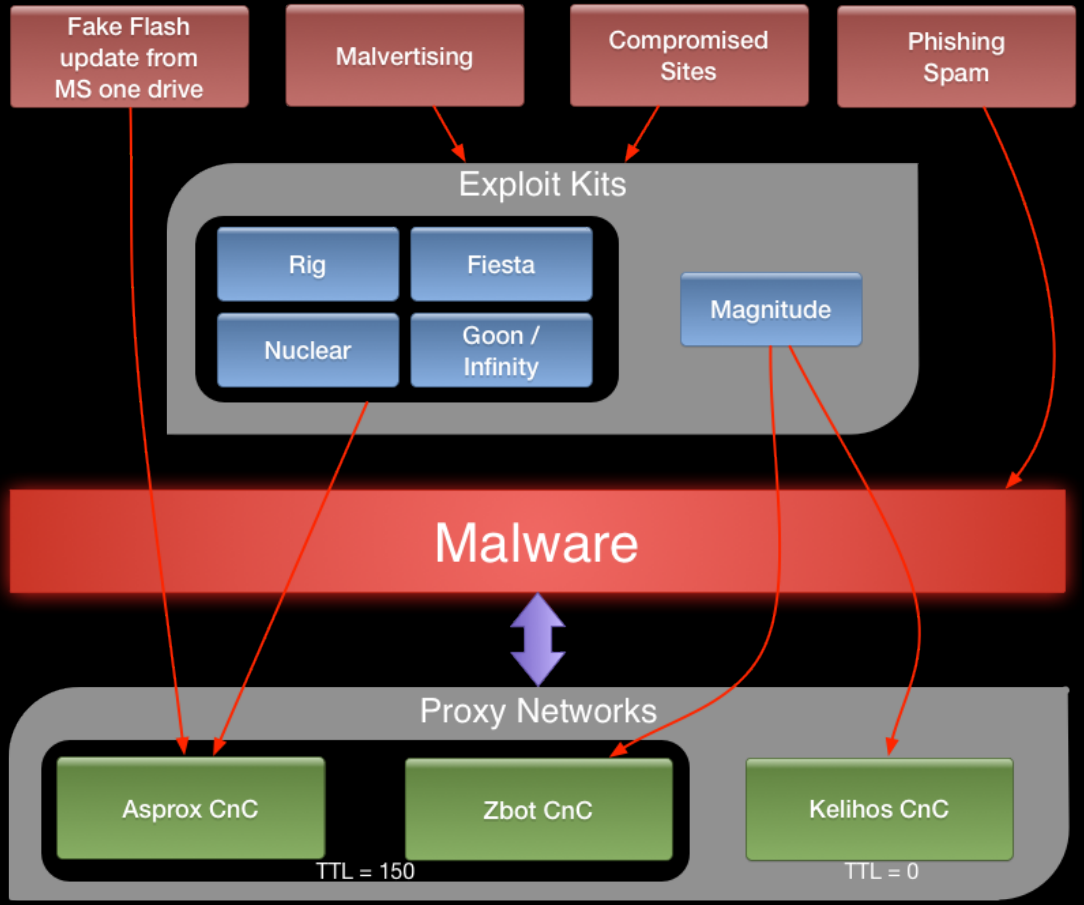


DNS Traffic


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

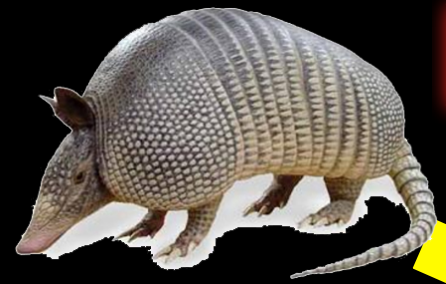
Catching Malware DNS style

Crimeware Ecosystem

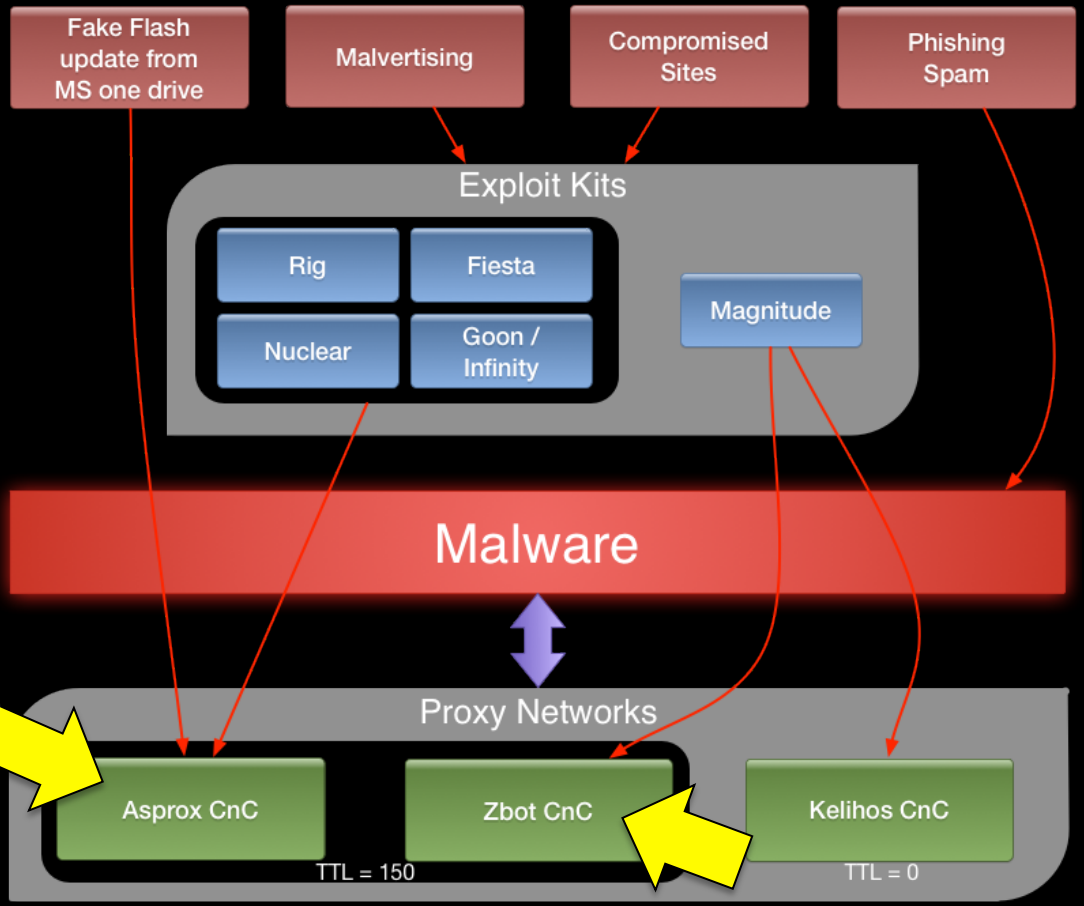


DNS style

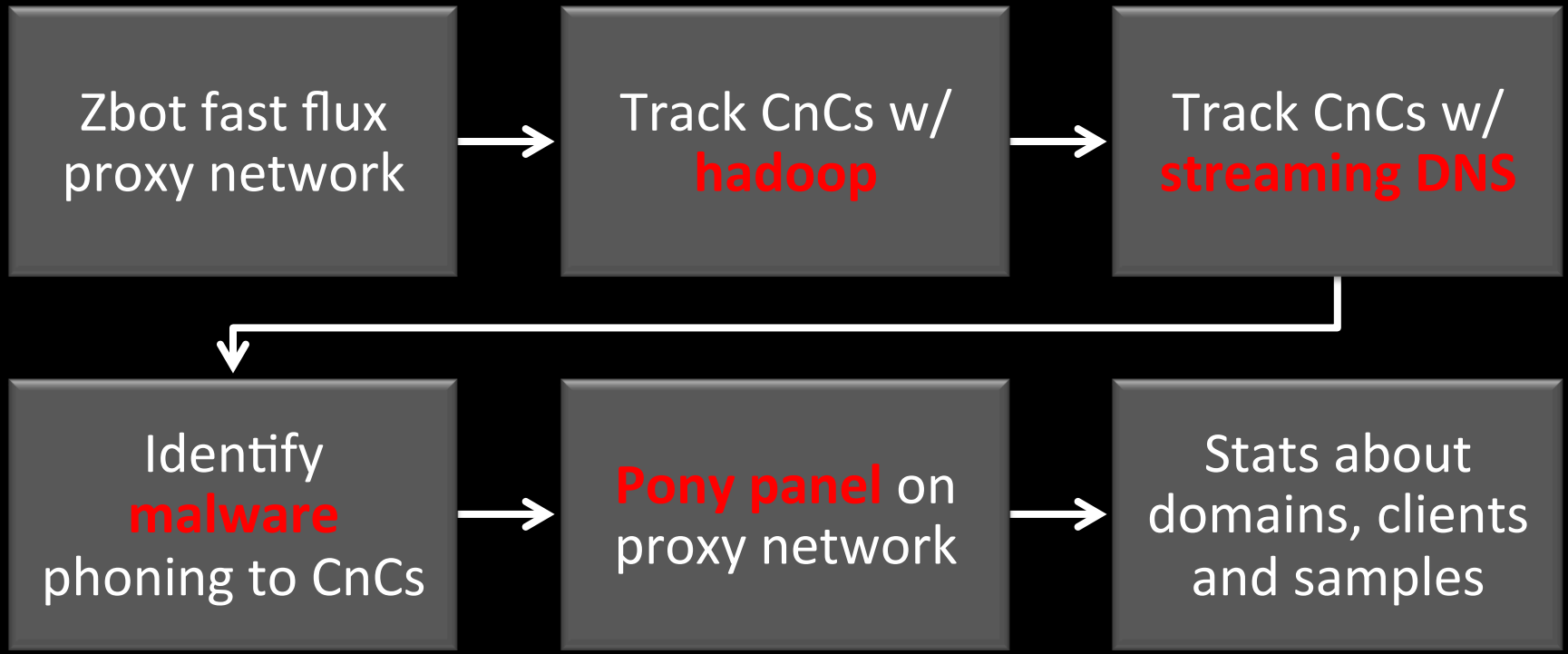
Crimeware Ecosystem



DNS style



Investigation Process



DNS style

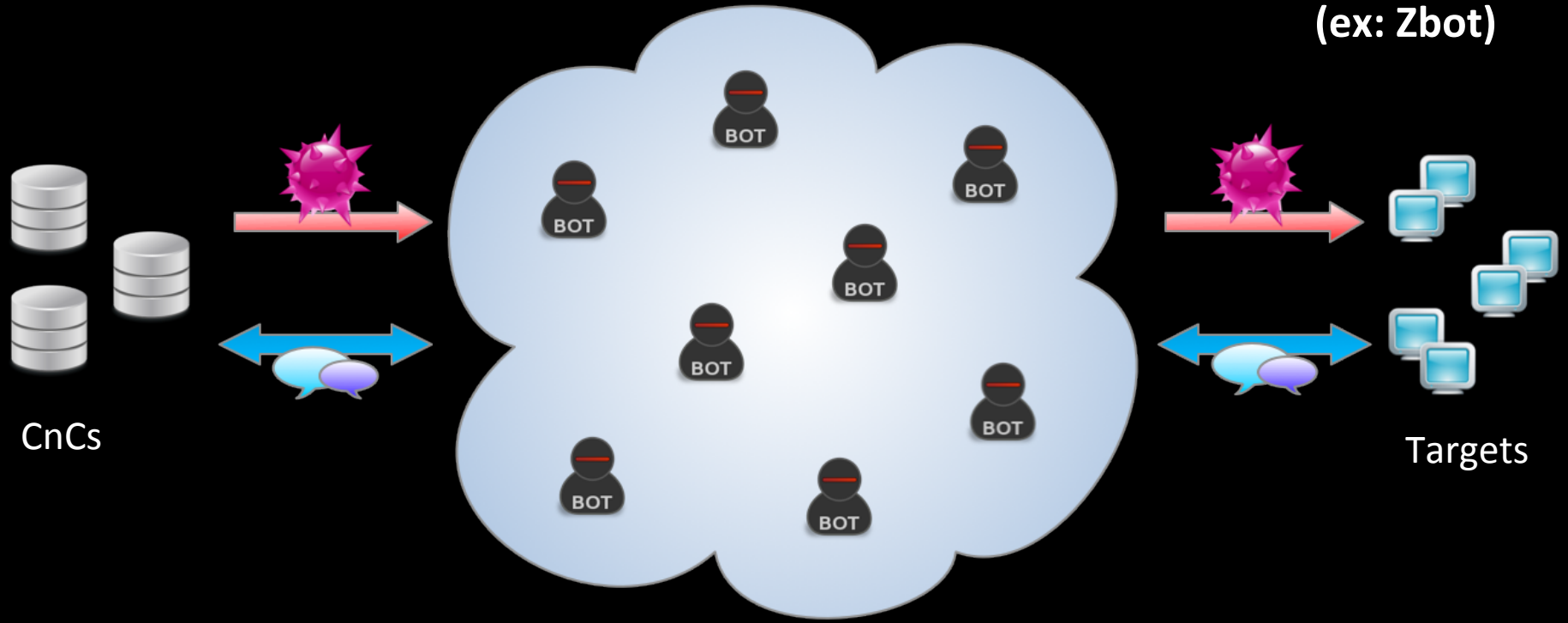
Fast Flux Networks

- DNS-based redundancy/evasion technique
- **Fast flux** domain resolves to **many IPs, many ASNs, many CCs**, relatively low TTL
- **Fast flux** domain resolves to **1 IP with TTL=0**
- Ex : Trojan CnCs, spam, scam, pharmacy, dating domains

DNS style

Fast Flux Proxy Networks

(ex: Zbot)



Kelihos TTL = 0
Zbot TTL = 150

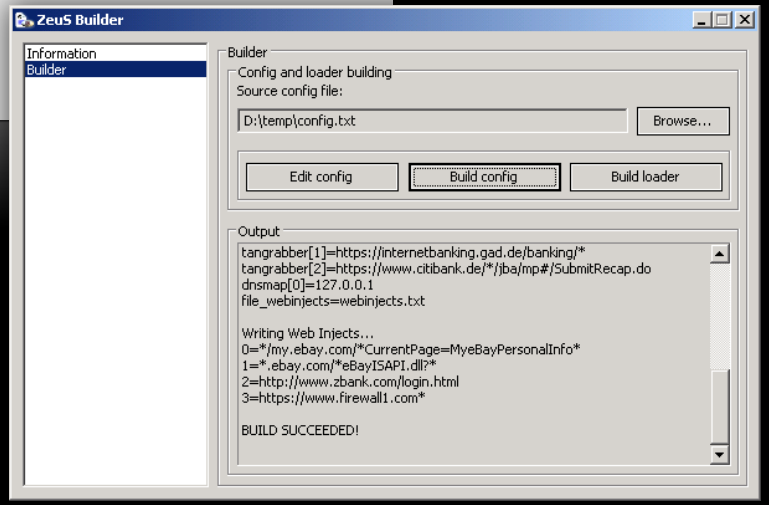
DNS style

Zeus Crimeware (1/2)

```
<Msg ID=20002 URLLastBinary FileLen=33 RealLen=33 Type='Uncompressed'>
http://evilzeusdomain.ru/zs/ldr.exe (Latest trojan binary)
</Msg>
<Msg ID=20003 URLServer0 FileLen=29 RealLen=29 Type='Uncompressed'>
http://evilzeusdomain.ru/zs/s.php (Dropzone)
</Msg>
<Msg ID=20004 URLAdvServers FileLen=37 RealLen=37 Type='Uncompressed'>
http://evilzeusdomain.ru/zs/cfg.bin (Latest config file [encrypted])
</Msg>
<Msg ID=20006 HTTPBotlogFilter FileLen=153 RealLen=188 Type='Compressed'> (Watching for the URLs below)
!*.microsoft.com/*
!http://*myspace.com*
</Msg>
<Msg ID=20008 HTTPFakesList FileLen=621 RealLen=1974 Type='Compressed'> (Fake / redirect the URLs below)
https://signin.ebay.com/ws/eBayISAPI.dll?co*
https://sitekey.bankofamerica.com/sas/signon*
https://www.paypal.com/*/cgi-bin/webscr?SESSION*
https://onlineservices.wachovia.com/auth/AuthServ*
https://banking.*.de/cgi/ueberweisung.cgi/*
[...]
</Msg>
```

Configuration file

Web injects

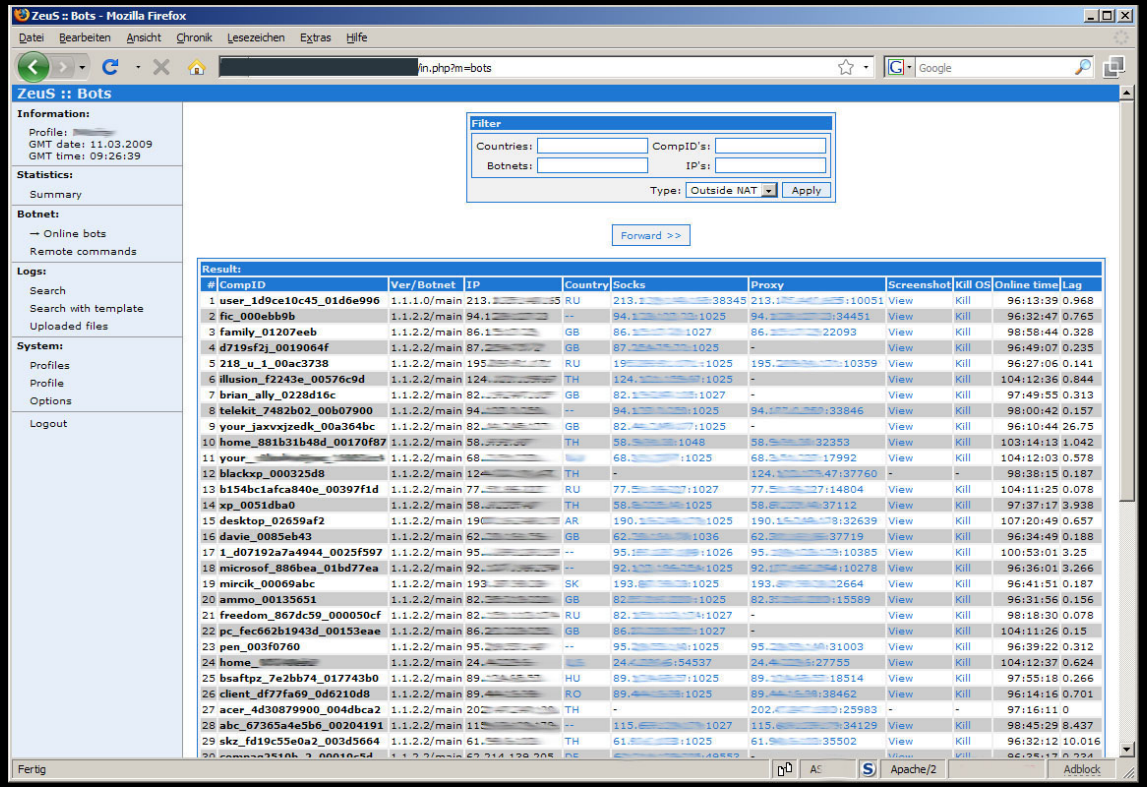


Zeus builder

Binary file

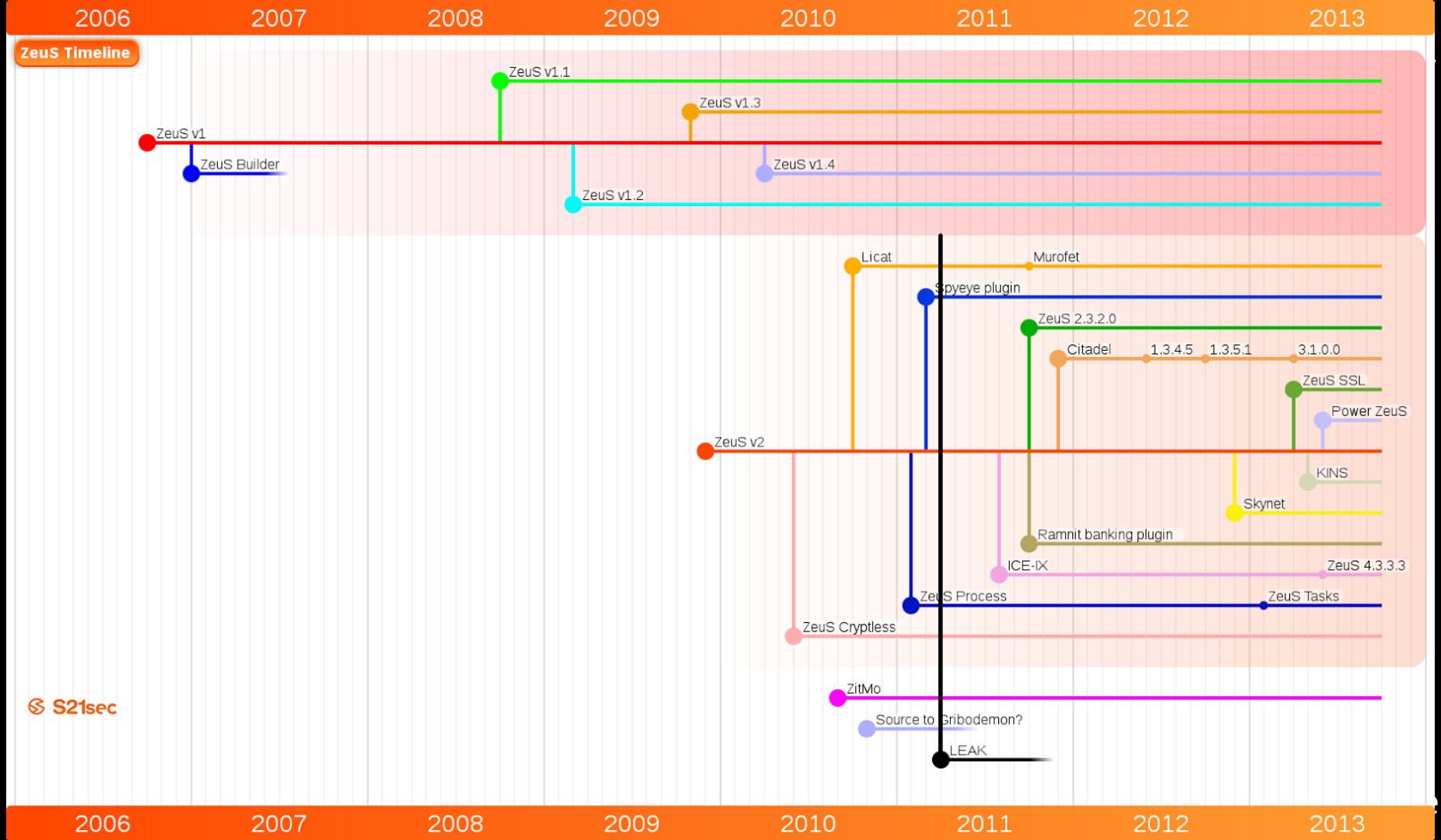
DNS style

Zeus Crimeware (2/2)



Control panel

DNS style


2006
2007
2008
2009
2010
2011
2012
2013
ZeuS Timeline
ZeuS v1.1
ZeuS v1.3
ZeuS v1
ZeuS Builder
ZeuS v1.4
ZeuS v1.2
Licat
Murofet
Spyeye plugin
ZeuS 2.3.2.0
Citadel
1.3.4.5
1.3.5.1
3.1.0.0
ZeuS SSL
Power ZeuS
ZeuS v2
KINS
Skynet
Ramnit banking plugin
ICE-IX
ZeuS 4.3.3.3
ZeuS Process
ZeuS Tasks
ZeuS Cryptless
ZitMo
Source to Gribodemon?
LEAK
S21sec
2006
2007
2008
2009
2010
2011
2012
2013

Zeus CnCs

Compromised Sites

Bulletproof Hosting

Fast Flux Botnet

DNS style

Zeus CnC URLs

Configuration Files

Binary Files

Drop Zones

DNS style

Zeus CnC detection Methods

1) Periodic batch pig job (**Hadoop** script)

2) IP harvesting + **streaming authoritative DNS** + filtering heuristics

DNS style

Detection with Hadoop

- Periodic Pig job **extracts domains with TTL = 150**
- Build **“domain to IP” bipartite graph**
- Extract **largest connected component**
- Identify new zbot CnCs to block
- Add IPs from largest connected component to **pool of zbot IPs**

DNS style

Authoritative DNS Stream

ASN, Domain, 2LD, IP, NS_IP, Timestamp, TTL, type

- 100s – 1000s entries/sec (from subset of resolvers)
- Need to implement own filters, detection heuristics
- Faster than DNSDB on Hadoop

DNS style

Detection with DNS stream

- Seed of **known Zbot CnCs**
- **Harvest IPs** and add them to **pool of Zbot IPs**
- Extract domains with IP or NS_IP in **Zbot IP pool**
- Add new Zbot CnCs to seed

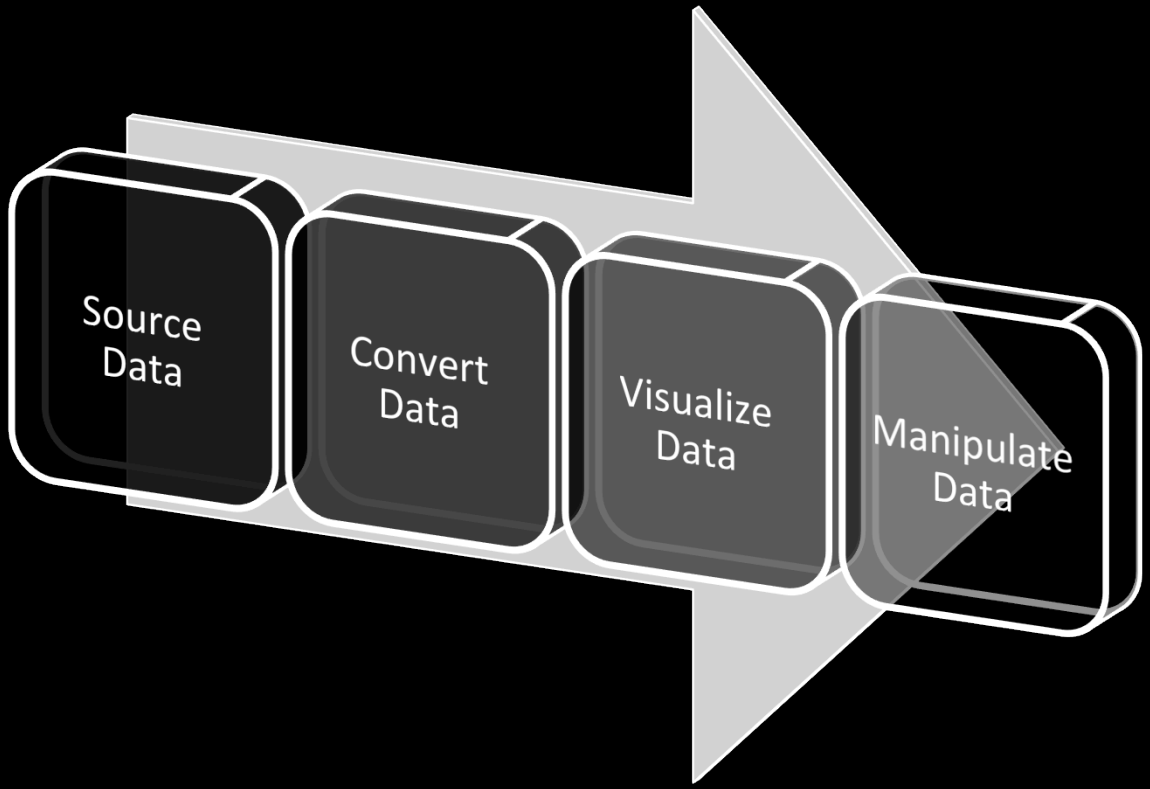
DNS style

Data Visualization

Zbot CnC domains – IP bipartite graph

DNS style

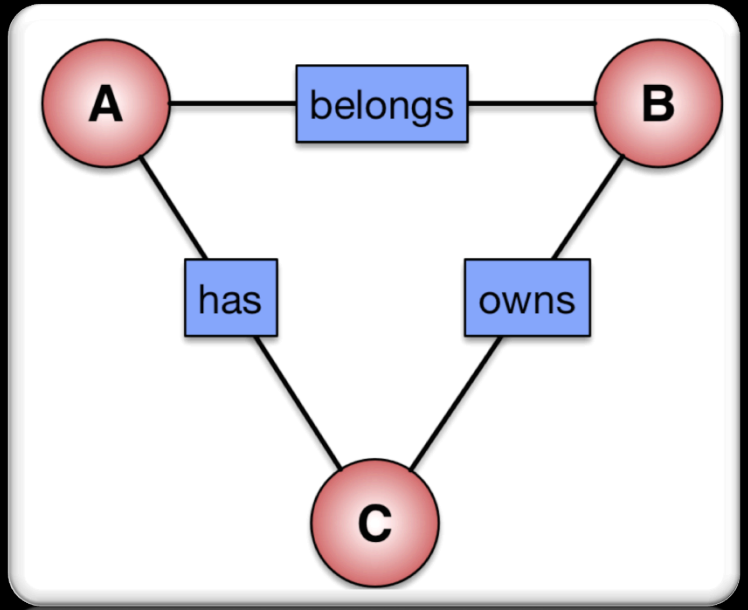
Workflow



DNS style

SemanticNet Library

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

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(“dataset.json”)
```



DNS style

DNS style

Results

Zeus

Config URLs
Binary URLs
Drop Zone URLs

Citadel

KINS
&
Ice IX

Asprox

Phishing

Misc

Results : Zeus urls

CnC domain	Url path	Url type
azg.su	/coivze7aip/modules/update.bin /coivze7aip/cde.php /coivze7aip/cde.php	ConfigURL BinaryURL DropZone
browsecheck.com	/rest/main.bin /manage/webstat.php	ConfigURL DropZone
despww.su	/3836bkuta3/modules/zte.bin /3836bkuta3/asdf.php	ConfigURL DropZone
dvs.qstatic.net	/img/pixel.jpg /img/mnn2.exe /img/rotator.php	ConfigURL BinaryURL DropZone
googleupd.com	/api/main.bin	ConfigURL
reportonh.com	/api/main.bin /pack32/sysconf.exe /manage/webstat.php	ConfigURL BinaryURL DropZone
seorubl.in	/forum/popap1.jpg /forum/explorer.exe /forum/index.php/gate.php	ConfigURL BinaryURL DropZone
servmill.com	/manage/mailo.php	DropZone
systemork.com	/api/main.bin	ConfigURL
sytemnr.com	/api/main.bin /pack32/sysconf.exe /manage/webstat.php	ConfigURL BinaryURL DropZone
vasilyaalibaba.com	/images/up.jpg	ConfigURL
veloinsurances.com	/images/logo_sav.jpg	ConfigURL
vhsonline.net	/pix.jpg	ConfigURL
vozmusa.biz	/healer/file.php /healer/gate.php	ConfigURL DropZone

DNS style

DNS style

Results : Citadel urls

CnC domain	Url path	Url type
alremi.ru	/images/images/amidstplenty/therexone/ledatic/file.php /images/images/amidstplenty/therexone/ledatic/e75.php	ConfigURL DropZone
anafis.ru	/images/kenn/eddy/file.php	ConfigURL
astrophiscinam.com	/flashcheck/file.php	ConfigURL
barakos.ru	/images/images/amidstplenty/therexone/ledaticmn/file.php /images/images/amidstplenty/therexone/ledaticmn/e75.php	ConfigURL DropZone
emonn.ru	/images/file.php /images/mon.php	ConfigURL DropZone
etot.su	/lifeisgood/IcoqW4all.php	DropZone
hotbird.su	/newadmin/file.php	ConfigURL
kaneaccess.ru	/images/images/amidstplenty/therexone/ledatic/file.php /images/images/amidstplenty/therexone/ledatic/e75.php	ConfigURL DropZone
lundu.ru	/tri4ngl3z/0v0x0/file.php	ConfigURL
m9a.ru	/images/images/amidstplenty/therexone/ledatic/file.php /images/images/amidstplenty/therexone/ledatic/e75.php	ConfigURL DropZone
p7x.ru	/CyberCartel1/file.php /CyberCartel1/gate.php	ConfigURL DropZone
panag.ru	/syst3mz/min-us/file.php /syst3mz/min-us/x!!x.php	ConfigURL DropZone
skinflexpro.eu	/treatment/53663675/wp-config.php /treatment/53663675/wp-comments-post.php	ConfigURL DropZone
verlo.ru	/syst3mz/min-us/file.php /syst3mz/min-us/x!!x.php	ConfigURL DropZone
volkojpanula.pw	/laguna/tein-industry/wp-signup.php /laguna/tein-industry/wp-login.php	ConfigURL DropZone
workflowhardware.com	/flashcheck/file.php	ConfigURL
yaler.ru	/tim3r/sw33t/file.php	ConfigURL

Results : KINS & Ice IX urls

CnC domain	Url path	Url type
construction89.ru	/spirit.jpg /qw.exe /var/czen.php	ConfigURL BinaryURL DropZone
francejustel.ru	/mail/hi.jpg	ConfigURL
newromentthere.ru	/123.jpg /g.exe /img/pic.php	ConfigURL BinaryURL DropZone
orbitmanes.ru	/sprit.jpg /01.exe /var/hy.php	ConfigURL BinaryURL DropZone
reznormakro.su	/winconf/kernl.bin /manage/webstat.php	ConfigURL DropZone

Results : Phishing

Domain	Known Url path
amazon.de.kunde-secure.com	/kunden_security/MDUuMjguMTQ%3D/4161/gp/newLogin/B007HCCOD0?charset.set=UTF&IP.hilfe=ID00320070.uberpruf28476660/
httpsj.org	/ap/deutschland/kunde /favicon.ico
httpss.biz	/sicherlich/deu/kunde

DNS style

Results : Asprox (1)

ET alert	Domain	HTTP method
ET TROJAN W32/Asprox.ClickFraudBot CnC Beacon	defie-guret.su harm-causer.com joye-luck.com joye-luck.su molinaderrec.com pg-free.com vision-vaper.su	GET /b/eve/
	bang-power.su cherry-white.com defie-guret.su grade-well.com harm-causer.com joye-luck.com joye-luck.su molinaderrec.com oak-cured.com original-lot.com pg-free.com valoherusn.su vision-vaper.su	GET /b/letr/
	biobetic-new.com carbiginer.com carbon-fix.su come-passere.com dialog-pow.com gummiringes.com head-pcs.com history-later.su lare-funer.com mitger-qaser.com mix-juert.com older-hiuwm.com preluner-ter.com unuse-bubler.com valoherusn.com zemmes-gimbl.com	GET /b/shoe/

DNS style

Results : Asprox (2)

ET alert	Domain	HTTP method
ET TROJAN W32/Asprox.ClickFraudBot POST CnC Beacon	apple-greens.com bang-power.su cherry-white.com defie-guret.su futere-poss.com garanering.su grade-well.com harm-causer.com hefu-juder.com innovation-citys.com jogurt-jetr.com joye-luck.com joye-luck.su juice-from.com molinaderrec.com nanoteches.com oak-cured.com on-bend.com original-lot.com pg-free.com ray-green.ru shark-yope.su supra-onfert.com taiborucheng.com terminus-hls.su trendf-news.ru tundra-red.com valoherusn.su vaping-qasdir.su vision-vaper.su	POST /b/opt/
	apple-greens.com cherry-white.com defie-guret.su garanering.su grade-well.com harm-causer.com joye-luck.com joye-luck.su molinaderrec.com oak-cured.com original-lot.com pg-free.com supra-onfert.com taiborucheng.com valoherusn.su vision-vaper.su	POST /b/req/

Results : Misc

- Madness Pro (Ddos bot) phoning home

netom.in, GET /1/?uid=17428742&ver=1.14&mk=bb3b62&os=WinXP&rs=adm&c=1&rq=0

with several occurring OS versions:

os=S2000

os=Win07

os=Win_V

os=WinXP

os=Win08

Results : Misc

- Downloading 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/

quarante-ml.com, GET /nivoslider98.45/ajax/

quarante-ml.com, GET /nivoslider98.45/jquery/

tundra-tennes.com, GET /nivoslider/ajax/

Results : Pony Panel Discovery

marmedladkos.com

Index of /

Name	Last modified	Size	Description
dron/	15-Feb-2013 12:55	-	
p/	11-Apr-2014 16:04	-	

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

Results : Pony Panel Discovery

- Pony 1.9 leaked for Trojan Forge in late 2012
- Info stealer
- Win32/Fareit

Payload delivered via:

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

DNS style

Results : Pony Panel Discovery

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)

DNS style

File Name **Pony.exe**
File Size: 34816
File MD5: 0ca0aa324446ffada395d644d9bfbe48
File SHA1: 3c8ea0ccbb10390c164bc2ab00370e145a3d53be
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

Results : Pony Panel Discovery

-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')

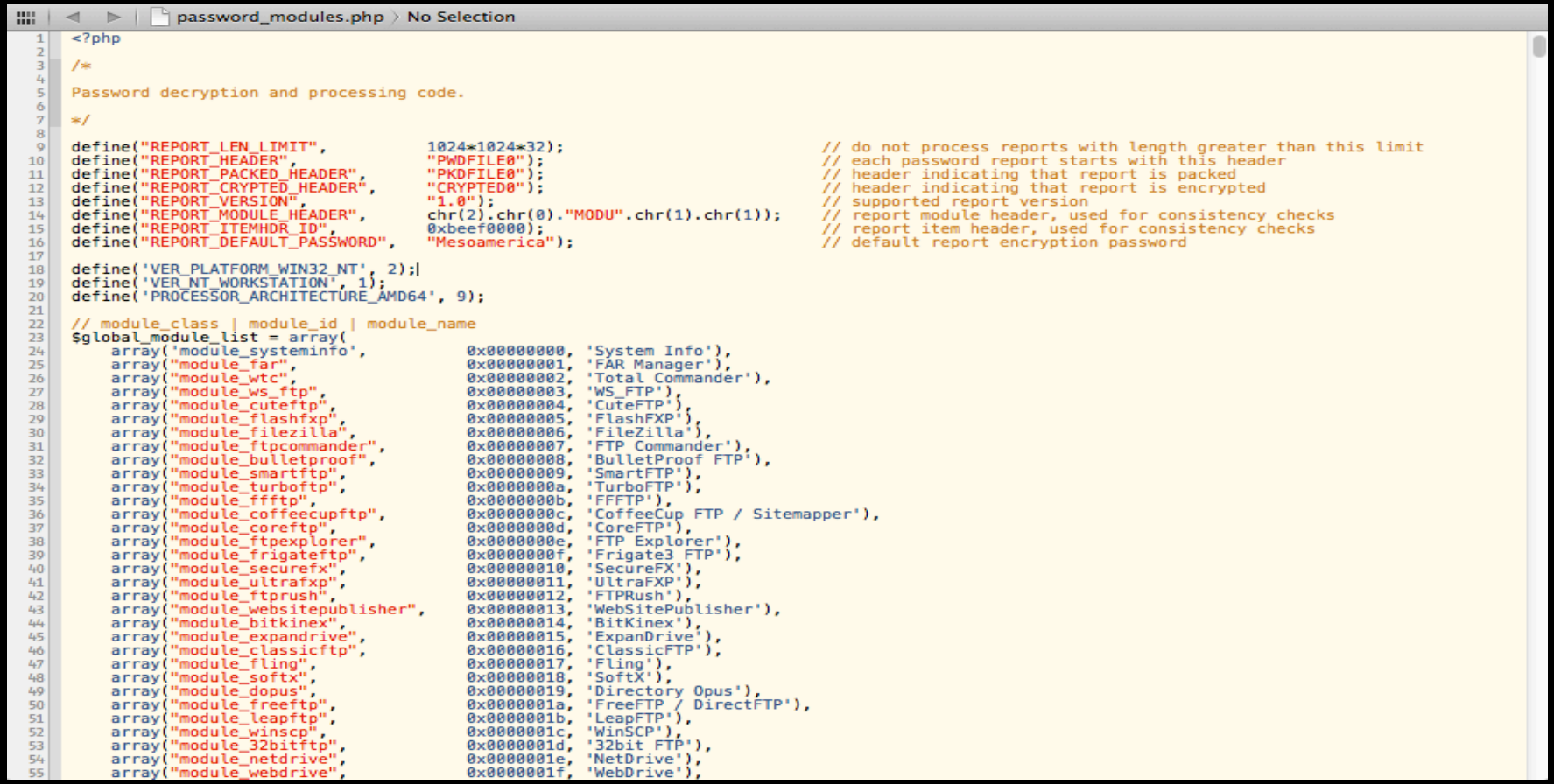
DNS style

Results : Pony Panel Discovery

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

DNS style

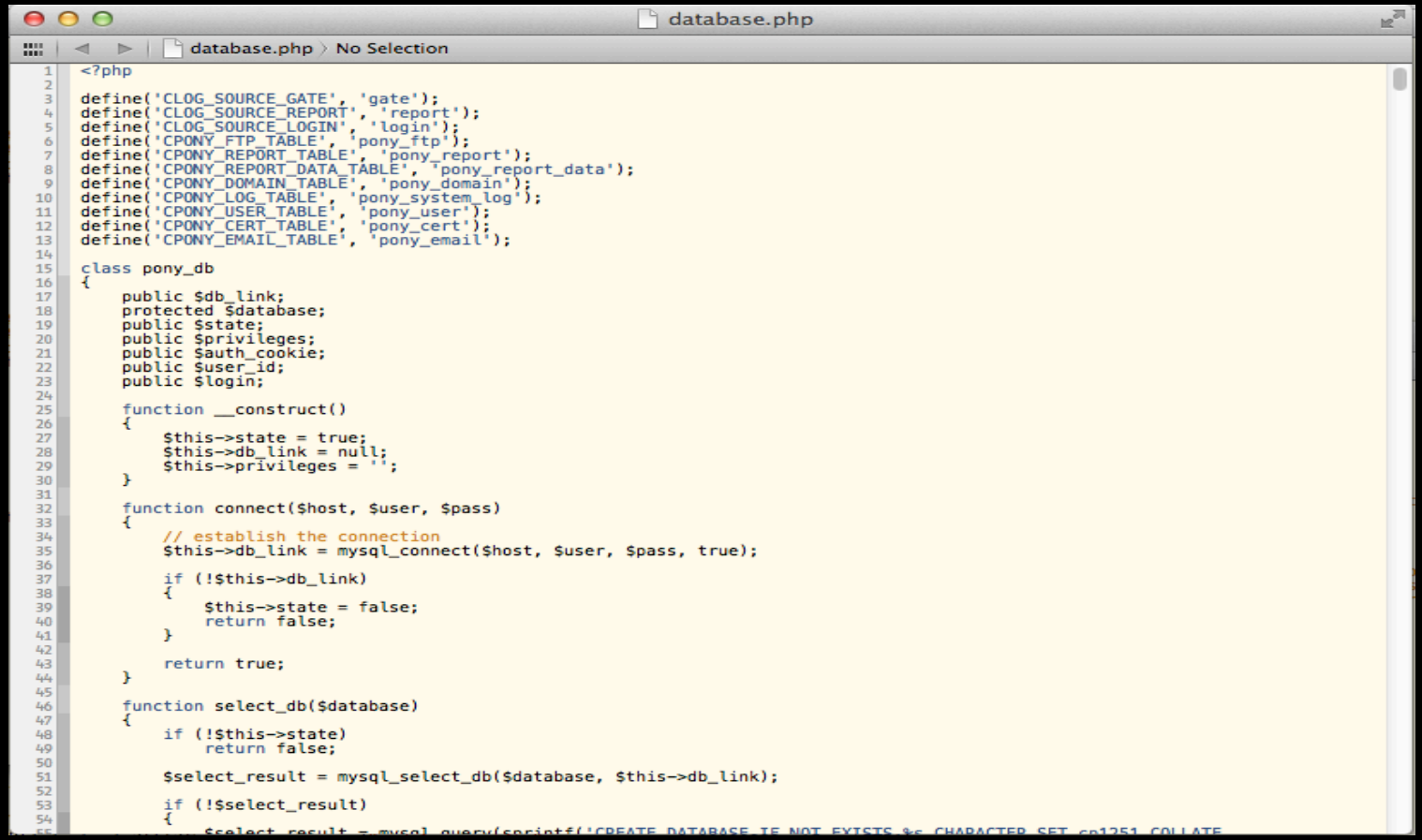
Results : Pony Panel Discovery


password_modules.php › No Selection

```
<?php

/*

Password decryption and processing code.

*/

define("REPORT_LEN_LIMIT",          1024*1024*32);                          // do not process reports with length greater than this limit
define("REPORT_HEADER",             "PWDFILE0");                            // each password report starts with this header
define("REPORT_PACKED_HEADER",      "PKDFILE0");                            // header indicating that report is packed
define("REPORT_CRYPTED_HEADER",     "CRYPTED0");                            // header indicating that report is encrypted
define("REPORT_VERSION",            "1.0");                                 // supported report version
define("REPORT_MODULE_HEADER",      chr(2).chr(0)."MODU".chr(1).chr(1));    // report module header, used for consistency checks
define("REPORT_ITEMHDR_ID",         0xbeef0000);                            // report item header, used for consistency checks
define("REPORT_DEFAULT_PASSWORD",   "Mesoamerica");                         // default report encryption password

define('VER_PLATFORM_WIN32_NT', 2);
define('VER_NT_WORKSTATION', 1);
define('PROCESSOR_ARCHITECTURE_AMD64', 9);

// module_class | module_id | module_name
$global_module_list = array(
    array('module_systeminfo',          0x00000000, 'System Info'),
    array("module_far",                 0x00000001, 'FAR Manager'),
    array("module_wtc",                 0x00000002, 'Total Commander'),
    array("module_ws_ftp",              0x00000003, 'WS_FTP'),
    array("module_cuteftp",             0x00000004, 'CuteFTP'),
    array("module_flashfxp",            0x00000005, 'FlashFXP'),
    array("module_filezilla",           0x00000006, 'FileZilla'),
    array("module_ftpcommander",        0x00000007, 'FTP Commander'),
    array("module_bulletproof",         0x00000008, 'BulletProof FTP'),
    array("module_smartftp",            0x00000009, 'SmartFTP'),
    array("module_turboftp",            0x0000000a, 'TurboFTP'),
    array("module_ffftp",               0x0000000b, 'FFFTP'),
    array("module_coffeecupftp",        0x0000000c, 'CoffeeCup FTP / Sitemapper'),
    array("module_coreftp",             0x0000000d, 'CoreFTP'),
    array("module_ftpexplorer",         0x0000000e, 'FTP Explorer'),
    array("module_frigateftp",          0x0000000f, 'Frigate3 FTP'),
    array("module_securefx",            0x00000010, 'SecureFX'),
    array("module_ultrafxp",            0x00000011, 'UltraFXP'),
    array("module_ftprush",             0x00000012, 'FTPRush'),
    array("module_websitepublisher",    0x00000013, 'WebSitePublisher'),
    array("module_bitkinex",            0x00000014, 'BitKinex'),
    array("module_expandrive",          0x00000015, 'ExpanDrive'),
    array("module_classicftp",          0x00000016, 'ClassicFTP'),
    array("module_fling",               0x00000017, 'Fling'),
    array("module_softx",               0x00000018, 'SoftX'),
    array("module_dopus",               0x00000019, 'Directory Opus'),
    array("module_freeftp",             0x0000001a, 'FreeFTP / DirectFTP'),
    array("module_leapftp",             0x0000001b, 'LeapFTP'),
    array("module_winscp",              0x0000001c, 'WinSCP'),
    array("module_32bitftp",            0x0000001d, '32bit FTP'),
    array("module_netdrive",            0x0000001e, 'NetDrive'),
    array("module_webdrive",            0x0000001f, 'WebDrive'),
```

DNS style

Results : Pony Panel Discovery




```php
<?php

define('CLOG_SOURCE_GATE', 'gate');
define('CLOG_SOURCE_REPORT', 'report');
define('CLOG_SOURCE_LOGIN', 'login');
define('CPONY_FTP_TABLE', 'pony_ftp');
define('CPONY_REPORT_TABLE', 'pony_report');
define('CPONY_REPORT_DATA_TABLE', 'pony_report_data');
define('CPONY_DOMAIN_TABLE', 'pony_domain');
define('CPONY_LOG_TABLE', 'pony_system_log');
define('CPONY_USER_TABLE', 'pony_user');
define('CPONY_CERT_TABLE', 'pony_cert');
define('CPONY_EMAIL_TABLE', 'pony_email');

class pony_db
{
    public $db_link;
    protected $database;
    public $state;
    public $privileges;
    public $auth_cookie;
    public $user_id;
    public $login;

    function __construct()
    {
        $this->state = true;
        $this->db_link = null;
        $this->privileges = '';
    }

    function connect($host, $user, $pass)
    {
        // establish the connection
        $this->db_link = mysql_connect($host, $user, $pass, true);

        if (!$this->db_link)
        {
            $this->state = false;
            return false;
        }

        return true;
    }

    function select_db($database)
    {
        if (!$this->state)
            return false;

        $select_result = mysql_select_db($database, $this->db_link);

        if (!$select_result)
        {
            $select_result = mysql_query(sprintf('CREATE DATABASE IF NOT EXISTS %s CHARACTER SET cp1251 COLLATE
```

Results : Pony Panel Discovery

Google search of distinctive key terms

DNS style

Results : Pony Panel Discovery

SHA256: 431cdc5df0009d304ec623cbe1245408010d1a0adfe85f6cfec6159449810ff9

File name: acdgei.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

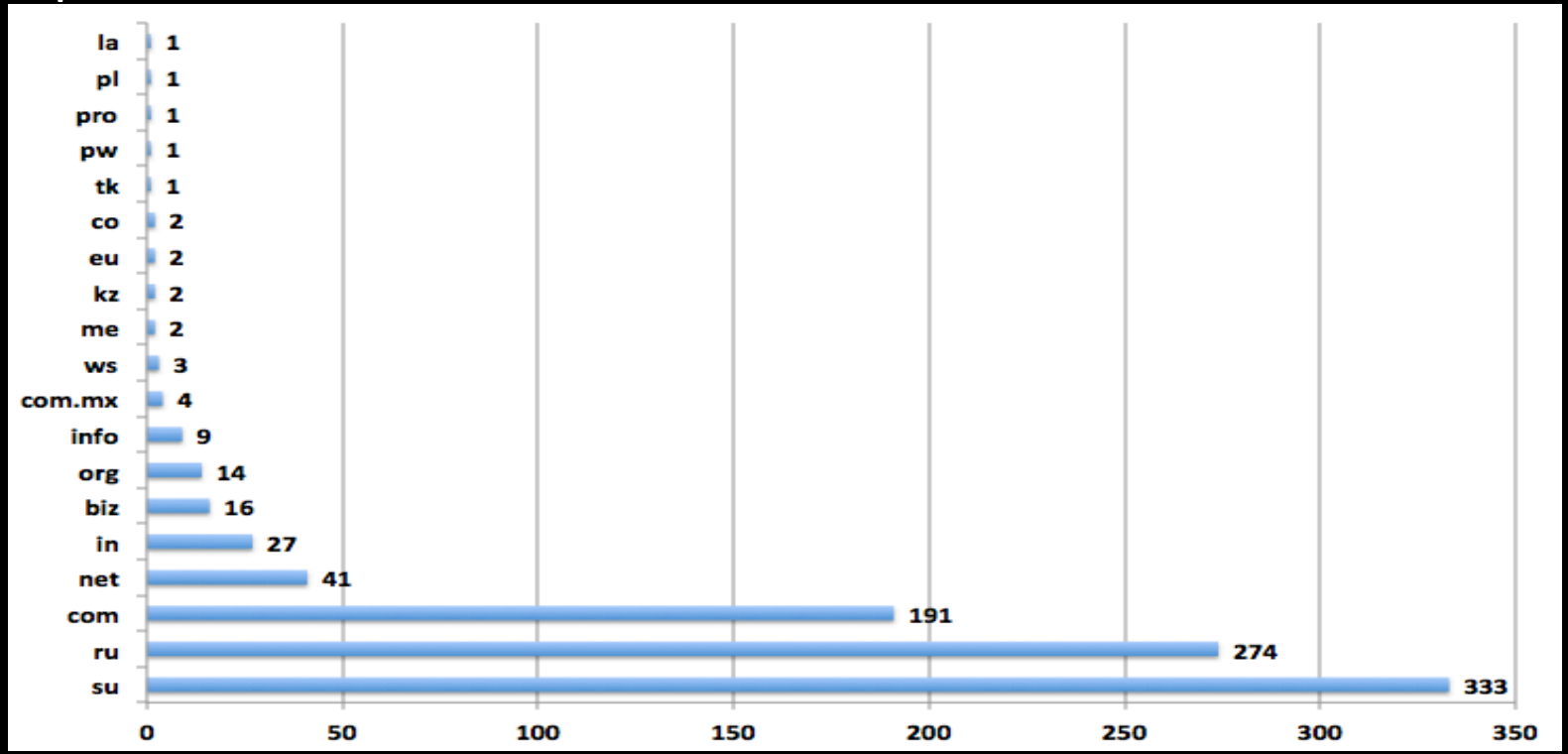
Antivirus	Result	Update
AVG	Agent4.ASJA	20140314
Ad-Aware	Gen:Variant.Kazy.188707	20140315
Agnitum	Backdoor.Androm!/7fFIrDK2mk	20140313
AntiVir	TR/Kazy.188707	20140315
Avast	MSIL:Agent-AME [Trj]	20140315
Baidu-International	Backdoor.Win32.Androm.AJ	20140315
BitDefender	Gen:Variant.Kazy.188707	20140315
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

Results : Pony Panel Discovery

epvpcash.net16.net/Panel/temp/
hgfhgfhgfhfg.net/pony/temp/
http://pantamati.com/dream/Panel/temp/
http://pantamati.com/wall/Panel/temp/
mastermetr.ru/steal/Panel/temp/
microsoft.blg.lt/q/temp/
santeol.su/p/temp/
terra-araucania.cl/pooo/temp/
thinswares.com/panel/temp/
www.broomeron.com/pn2/temp/
www.kimclo.com/cli/temp/
www.sumdfase2.net/adm/temp/
www.tripplem2.com/images/money/temp/

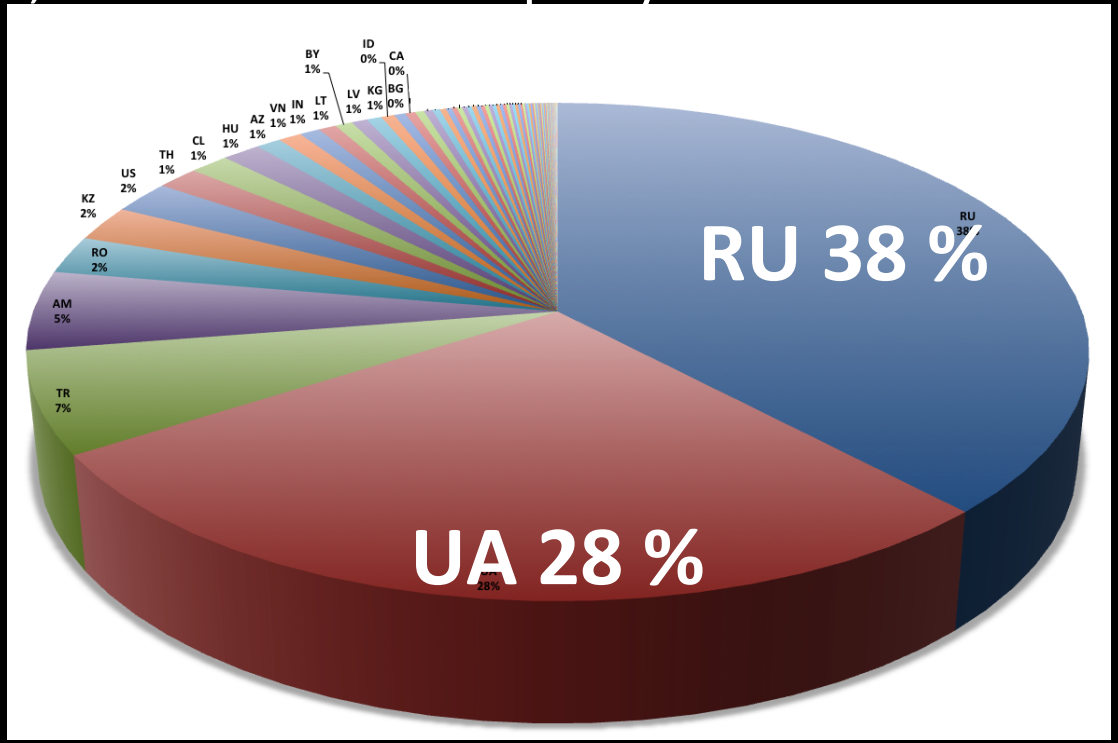
Results : TLD distribution

Sample of 925 zbot CnC domains

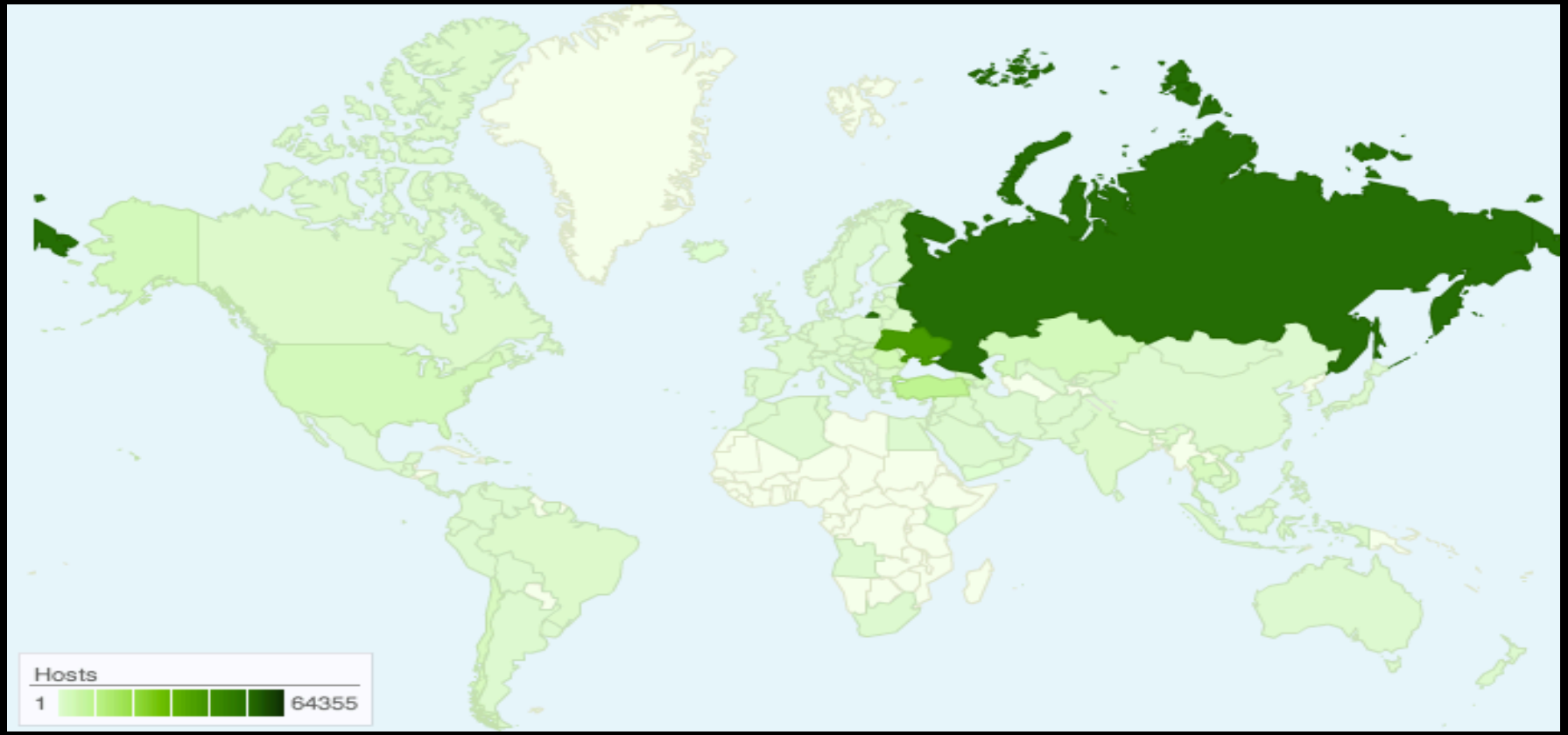


Results : Bots geo-distribution

Sample of 170,208 IPs of the zbot proxy network

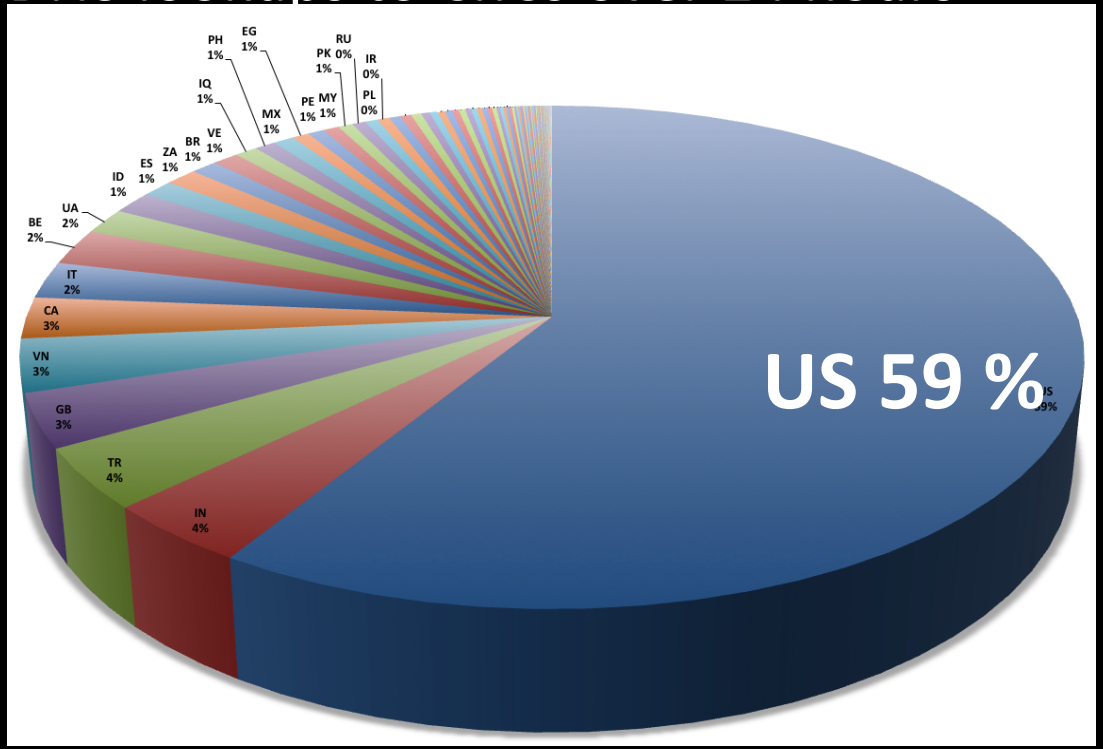


Results : Bots geo-distribution

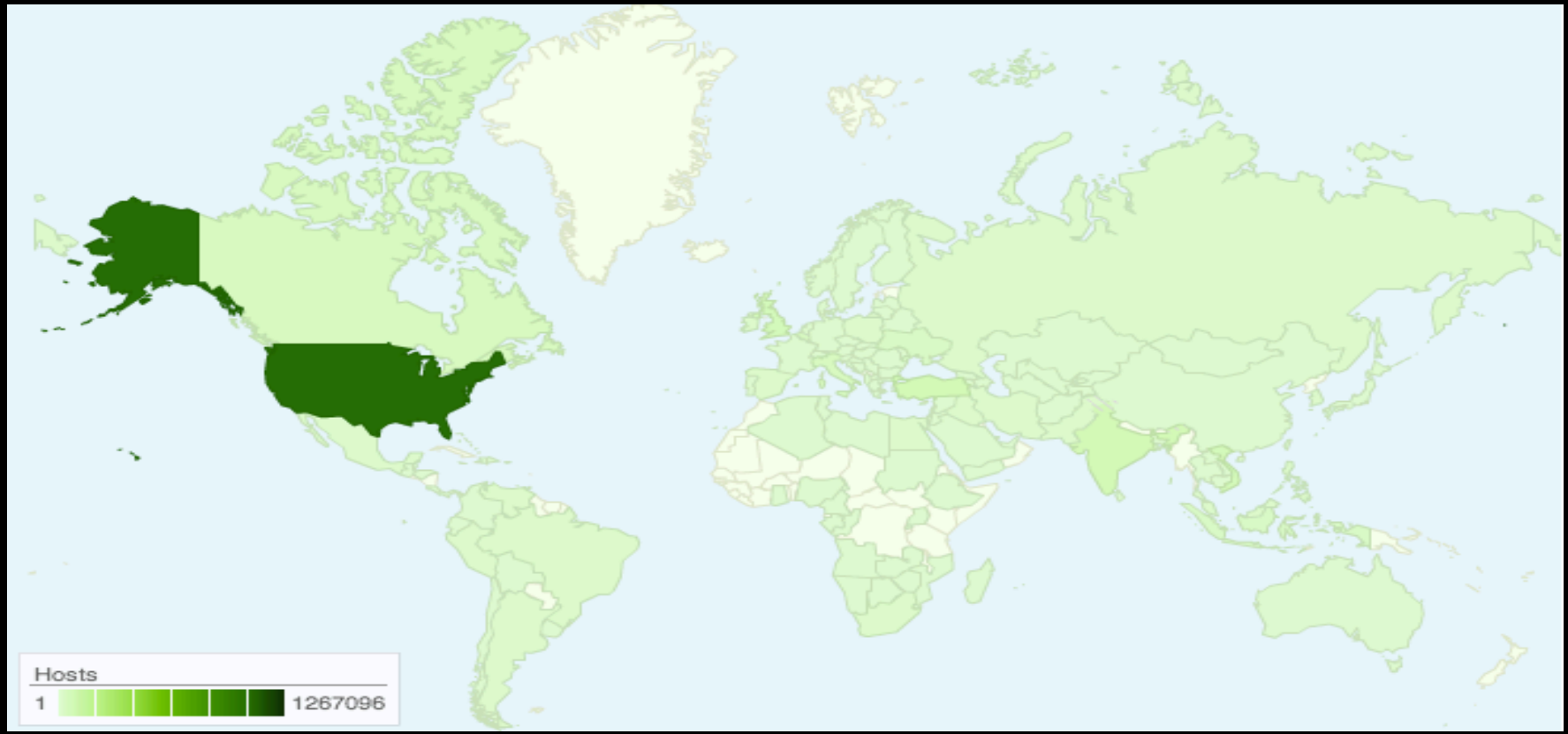


Results : Clients phoning to CnCs

2,220,230 DNS lookups to CnCs over 24 hours



Results : 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

Summary

- Zbot fast flux proxy network is **very versatile**
- **Multi-purpose** based on clients' needs
- CnCs for Zeus, Citadel, Ice IX, KINS, Asprox, Madness Pro, phishing, Pony panel
- Serve **all types of Zeus urls**: config, binary and drop zones
- .ru, .su, .com most abused TLDs
- **Bots** concentrated in **Russia, Ukraine**
- Targeted **victims** concentrated in the **US**

Catching Malware IP style

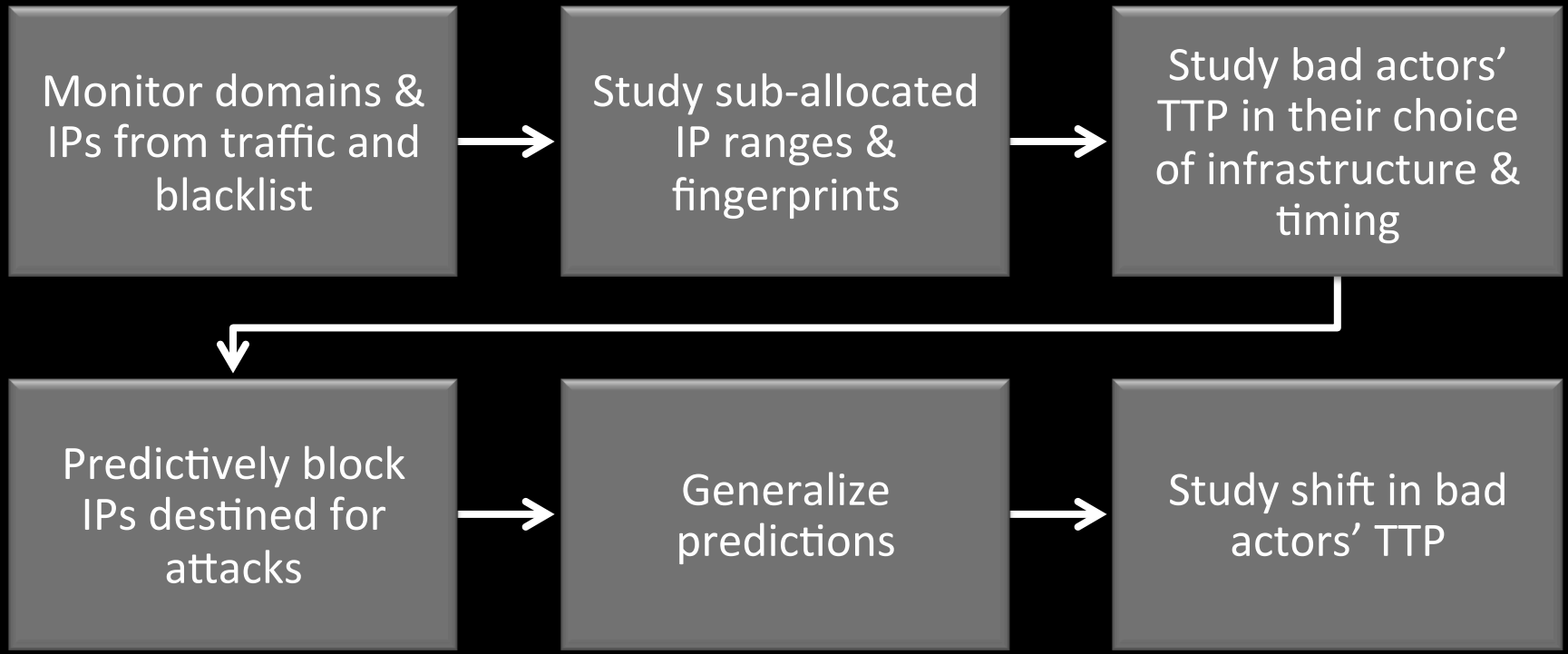
Catching Malware IP style

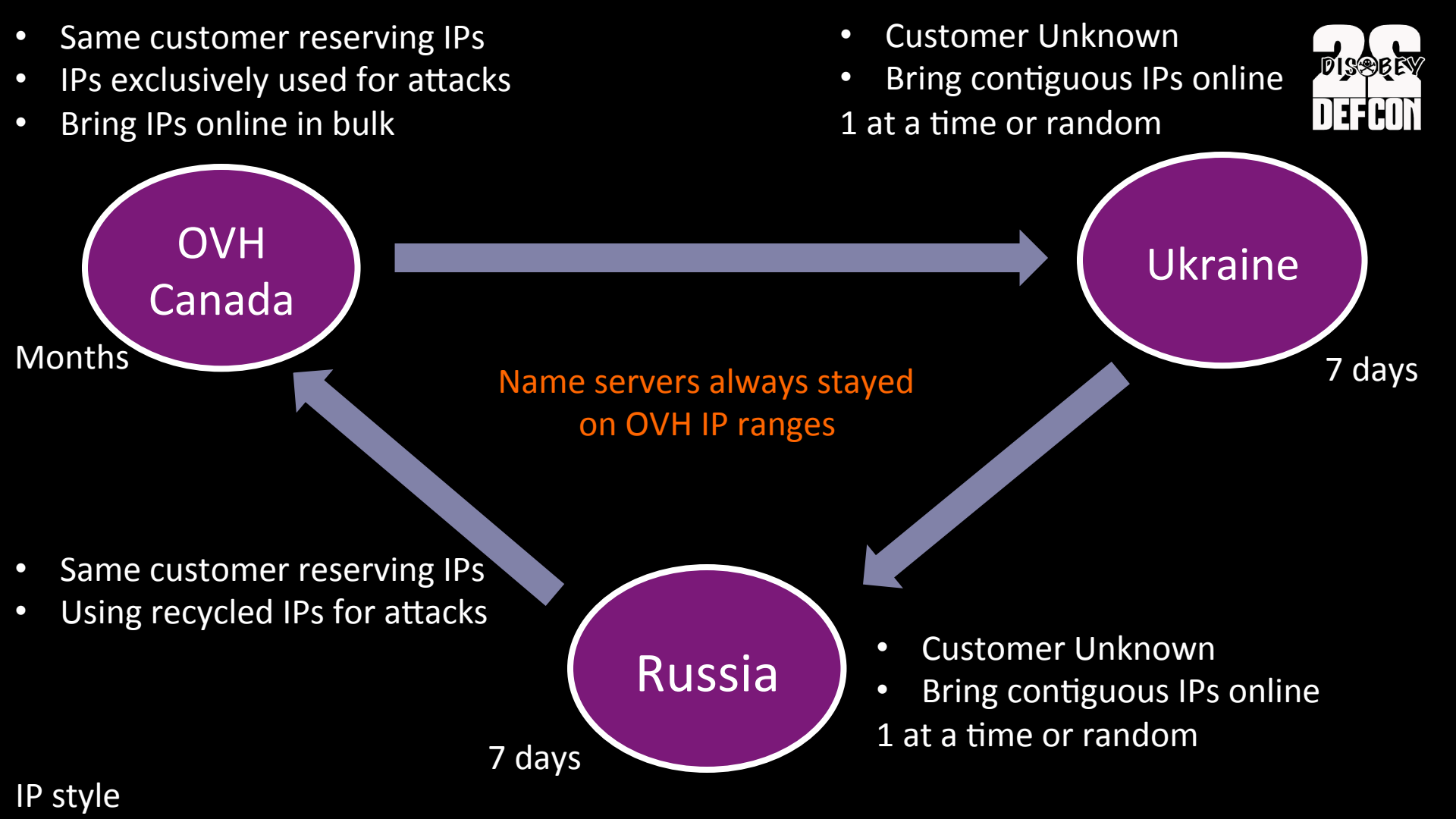
Sub-allocated ranges

ASN graph topology

Use case #1
Malicious sub-allocated ranges

Investigation Process

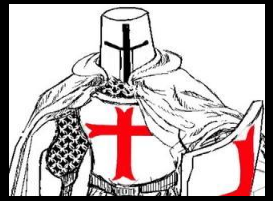



• Same customer reserving IPs
• IPs exclusively used for attacks
• Bring IPs online in bulk
• Customer Unknown
• Bring contiguous IPs online
1 at a time or random
OVH Canada
Months
Ukraine
7 days
Name servers always stayed on OVH IP ranges
• Same customer reserving IPs
• Using recycled IPs for attacks
Russia
7 days
• Customer Unknown
• Bring contiguous IPs online
1 at a time or random
IP style

IP style

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 @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

Predicting malicious domains IP infrastructure

Tracking 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

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

Tracking OVH 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

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

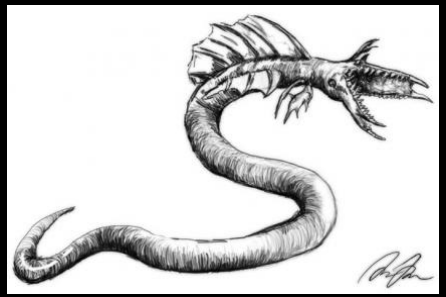
198.50.143.64 - 198.50.143.79
22/tcp open ssh OpenSSH 5.5p1 Debian 6+squeeze4 (protocol 2.0) 80/tcp open http nginx web server 0.7.67 445/tcp filtered microsoft-ds

- Combine indicators and generalize to other threats

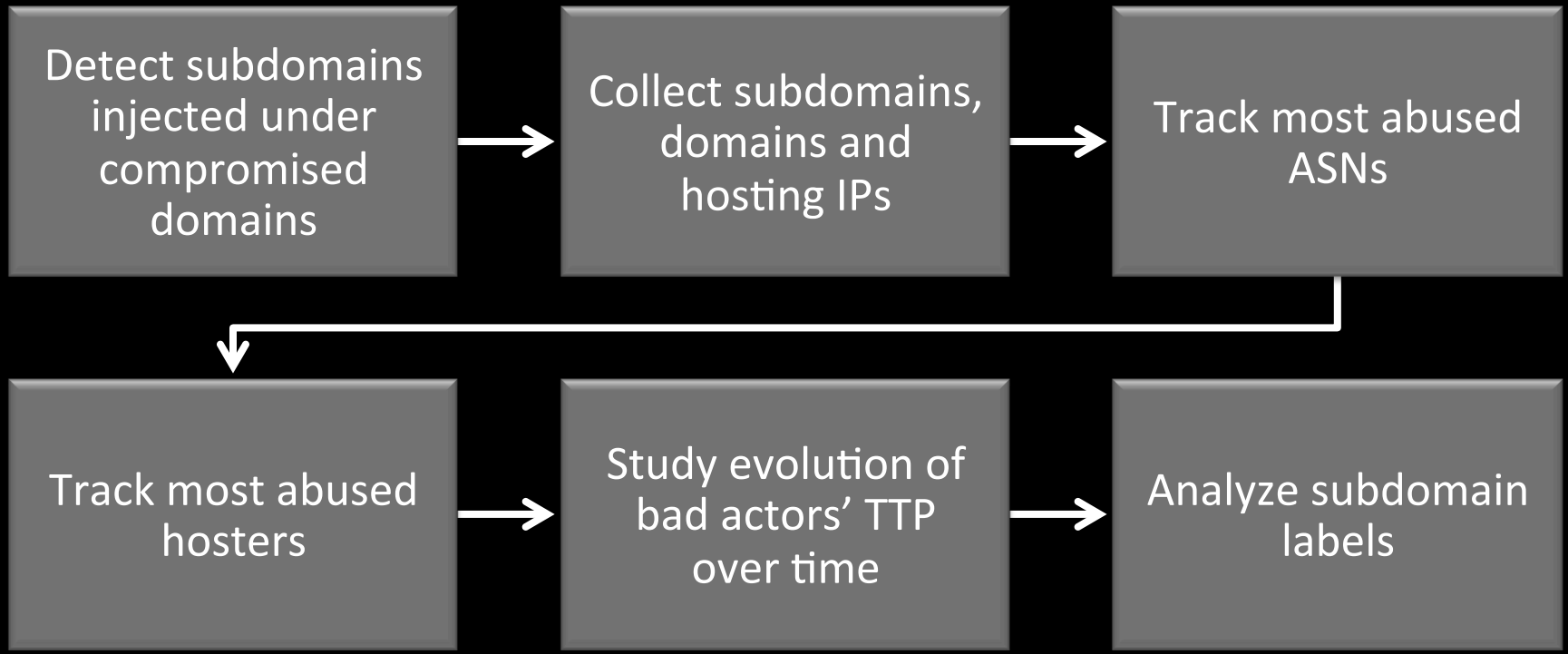
-> **Block/quarantine** IPs **before they start hosting** domains

IP style

Detecting Malicious Subdomains under Compromised domains



Investigation Process



IP style

Malicious subdomains under compromised domains

- Detect 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

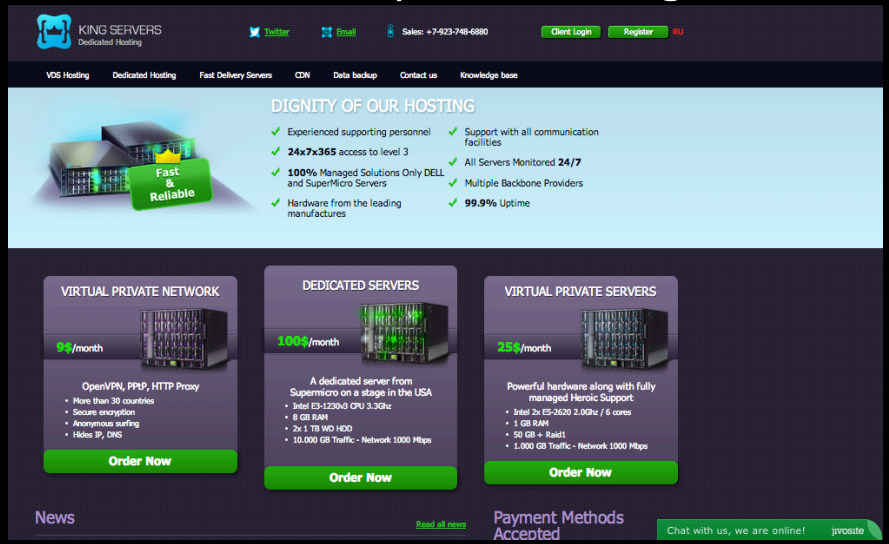
- Sample of several hundred IPs hosting malicious subdomains
- Top 5 abused ASNs
  - 16276 OVH SAS (18% of total collected malicious IPs)
  - 24961 myLoc managed IT AG
  - 15003 Nobis Technology Group, LLC
  - 41853 LLC NTCOM
  - 20473 Choopa, LLC

IP style

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)

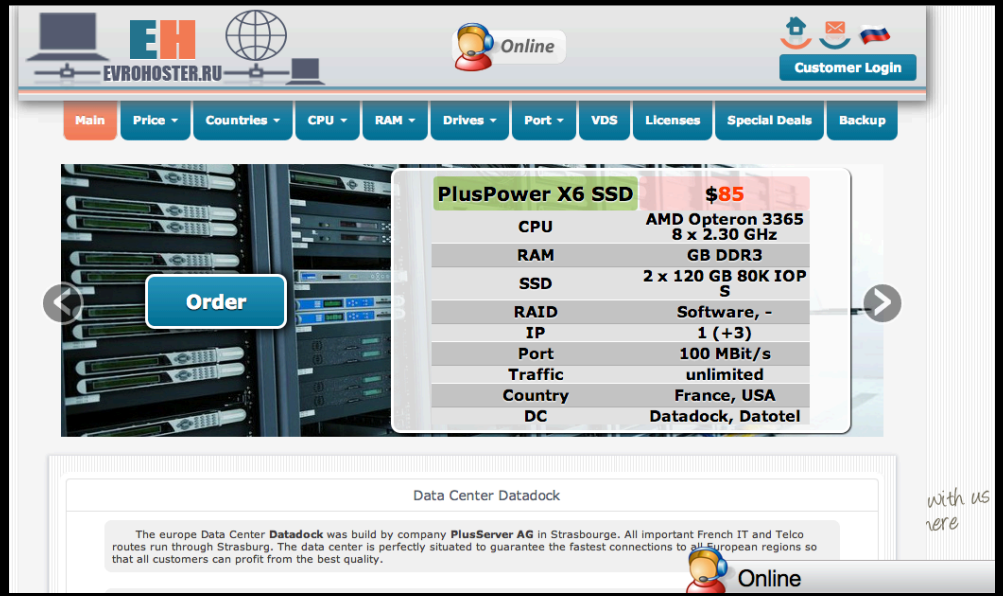
Small abused or rogue hosting providers

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



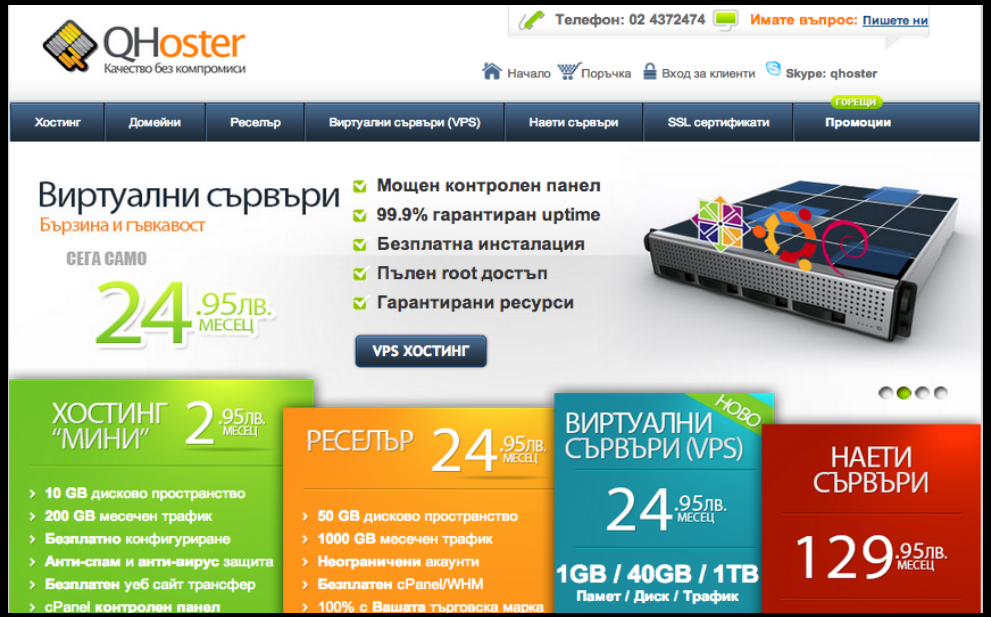
Small abused or rogue hosting providers

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



Small abused or rogue hosting providers

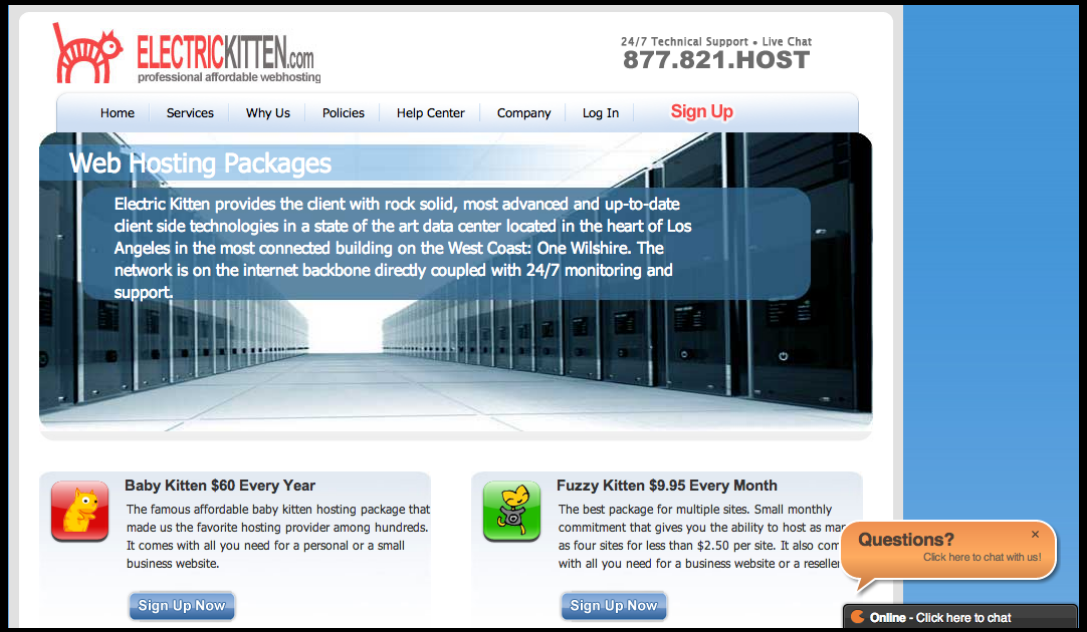
- http://www.qhoster.bg/ hosted Nuclear



IP style

Small abused or rogue hosting providers

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



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/

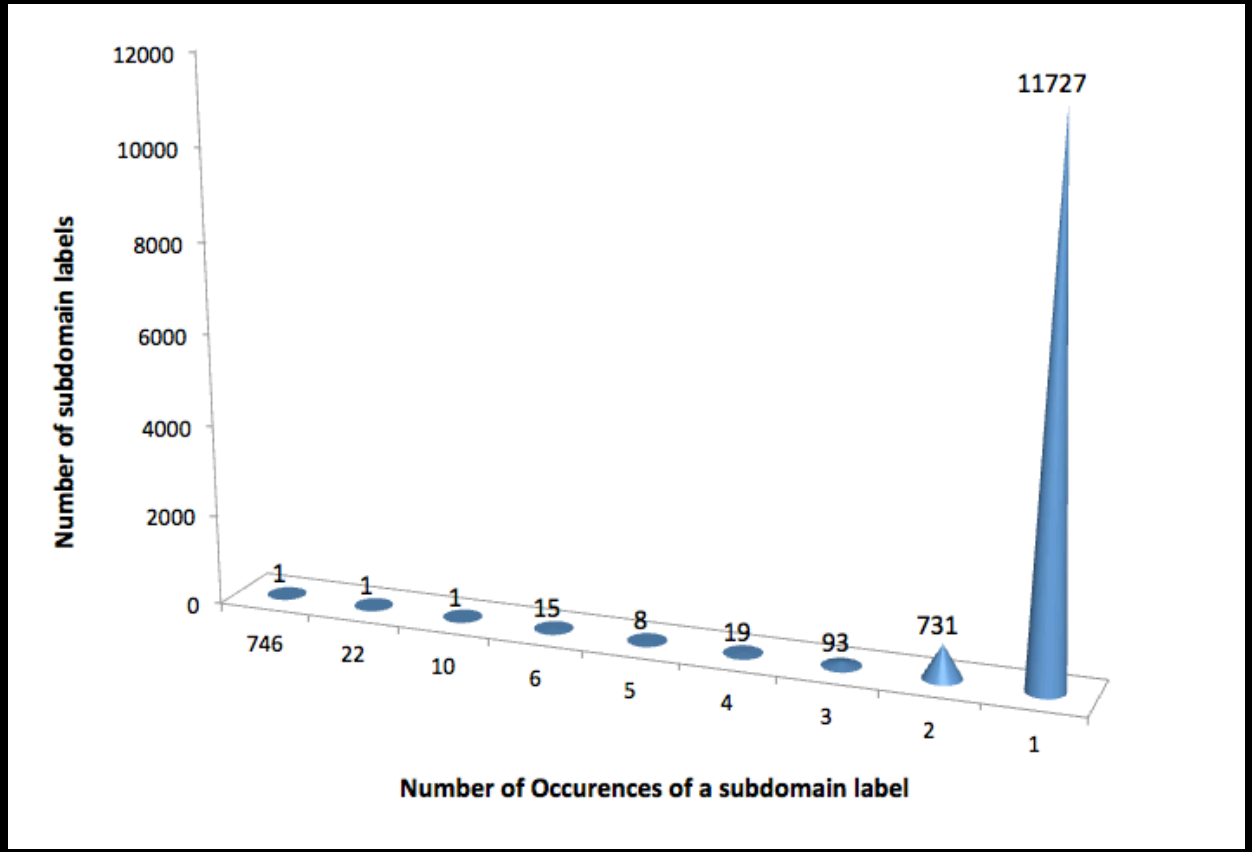
IP style

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
  - solidfileslzsr

IP style

String Analysis of injected subdomains



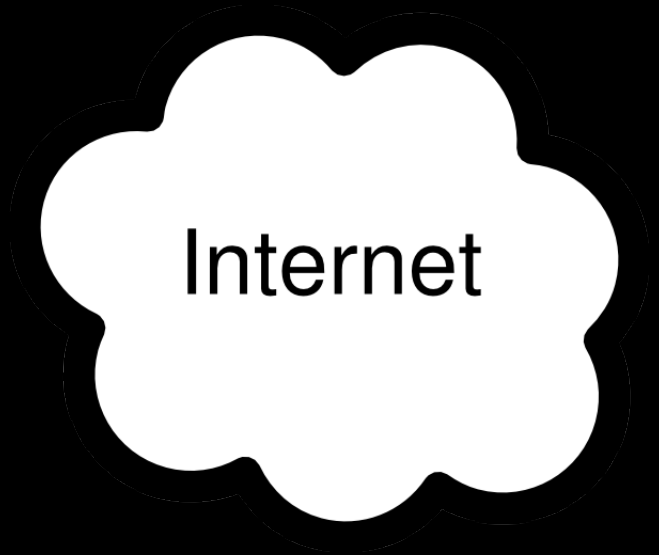
Catching Malware IP style

Sub-allocated ranges

ASN graph topology

IP style

INTERNET 101 & BGP

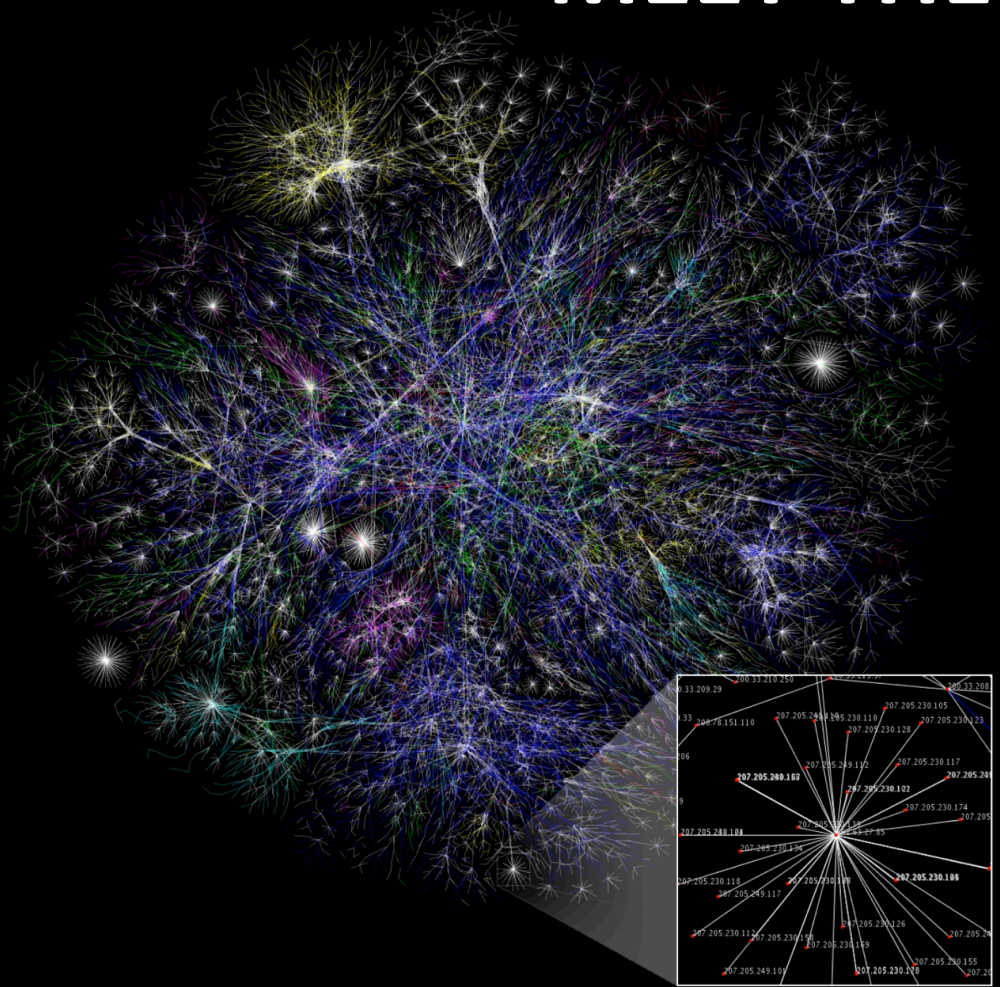


IP style

INTERNET 101 & BGP

IP style

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
- **510,000+ BGP prefixes**
- **48,000+ 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, 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:

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

CIDR REPORT for 23 Feb 14

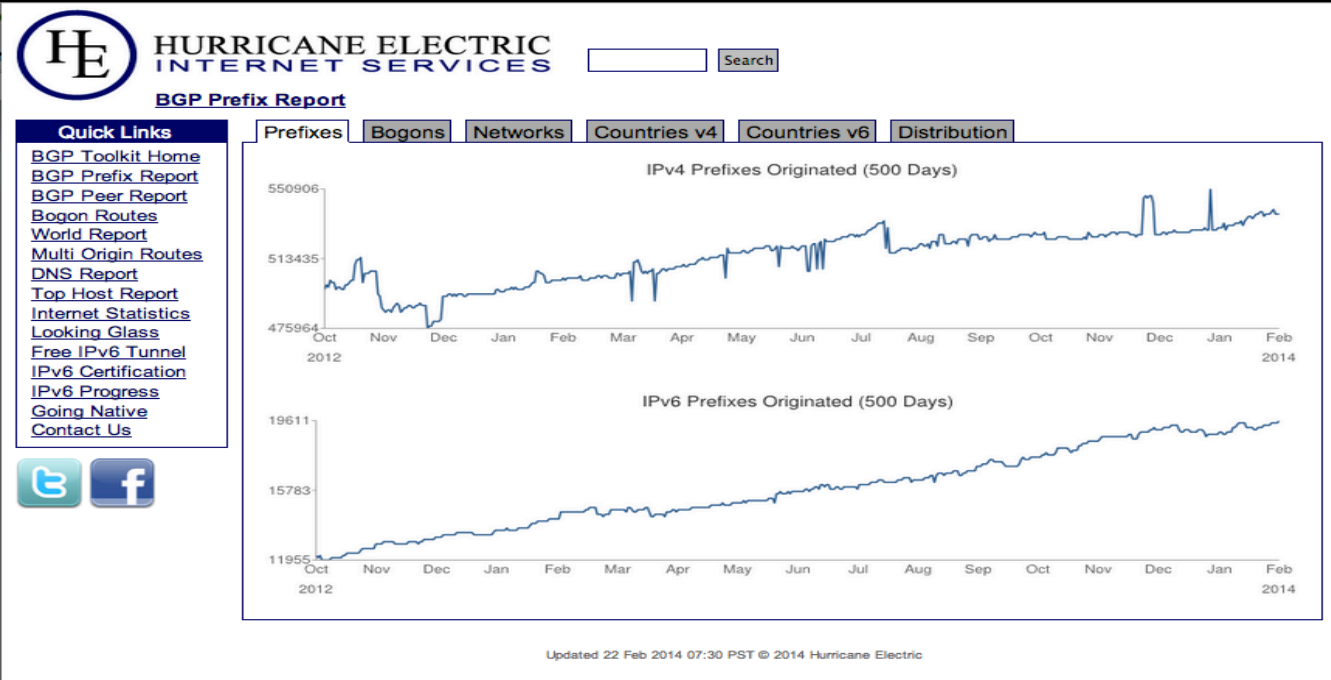
This report was generated at Sun Feb 23 06:14:14 2014 AEST.

Report Sections:

Status Summary

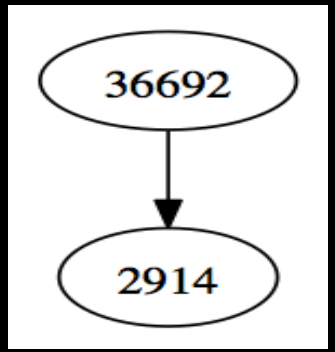
AS graph

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



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

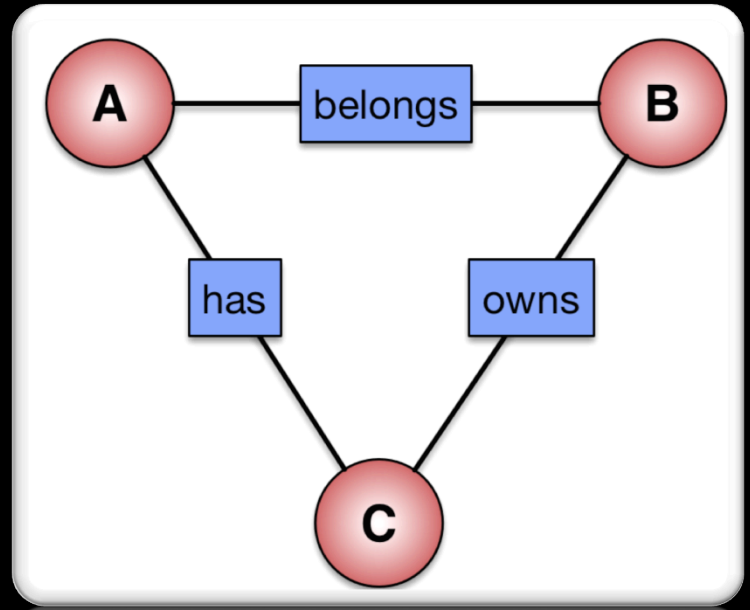
Focus of this study:

- 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

IP style

SemanticNet Library

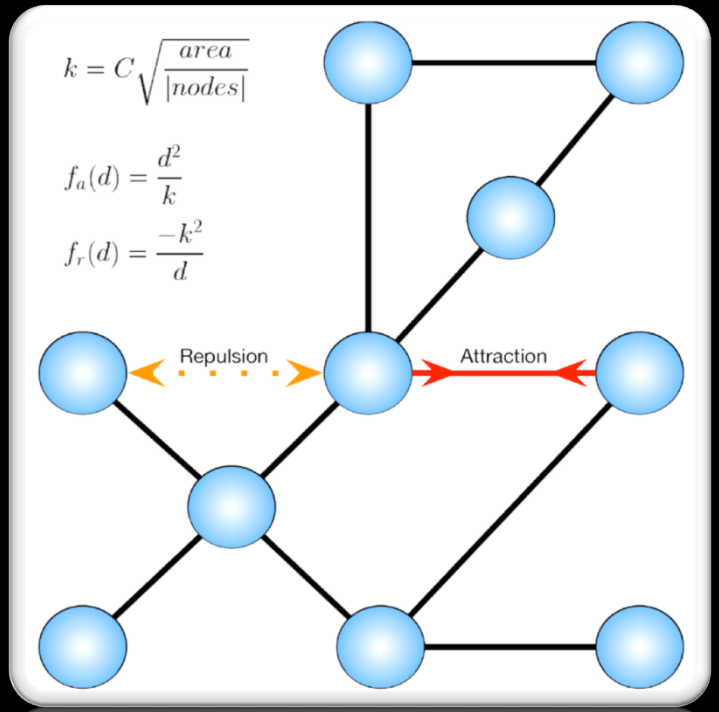
```
#!/usr/bin/env python

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(“dataset.json”)
```



DNS style

IP style

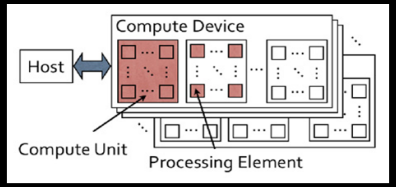
Particle Physics

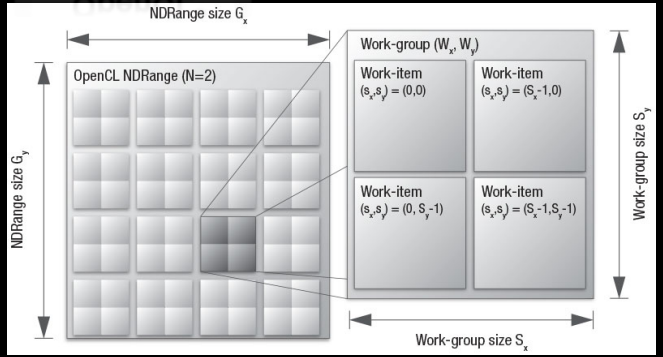


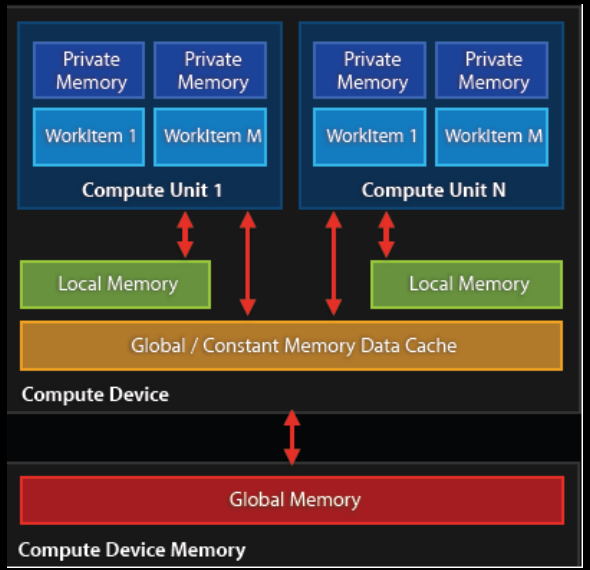
IP style

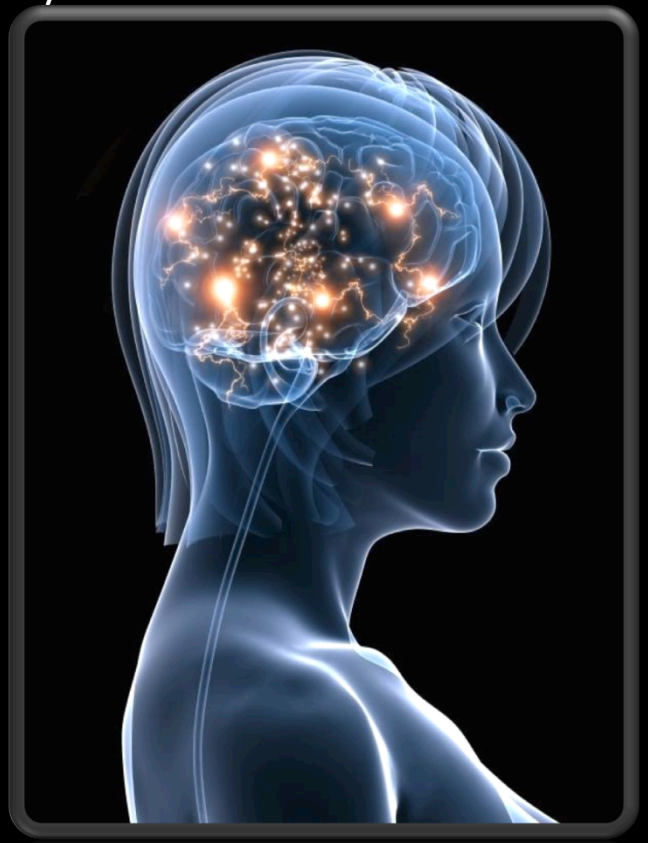
IP style

Parallelization









Why ?

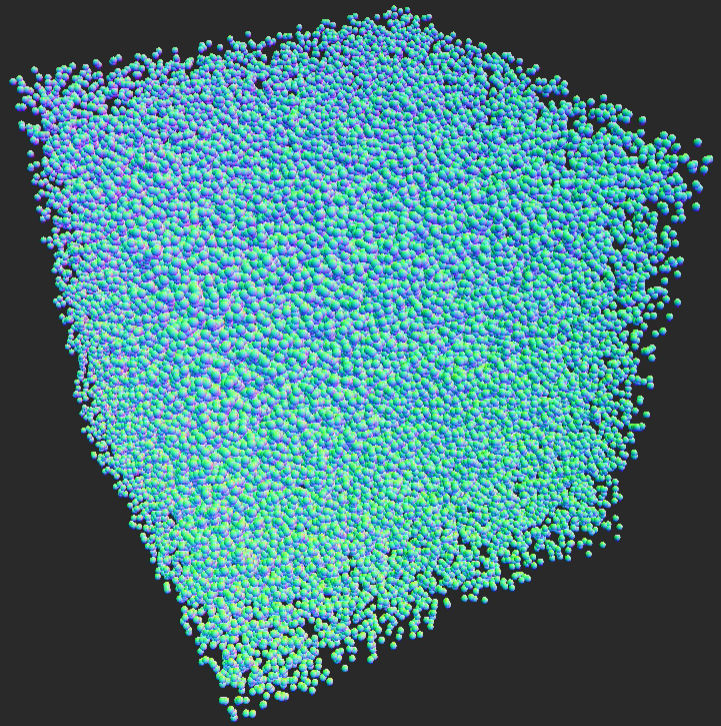
- Data driven vs user-driven
- Layout closer to the *“natural shape”* of data structure
- Take advantage of the GPU for acceleration
- Humans are good at processing shapes and colors

Data Visualization

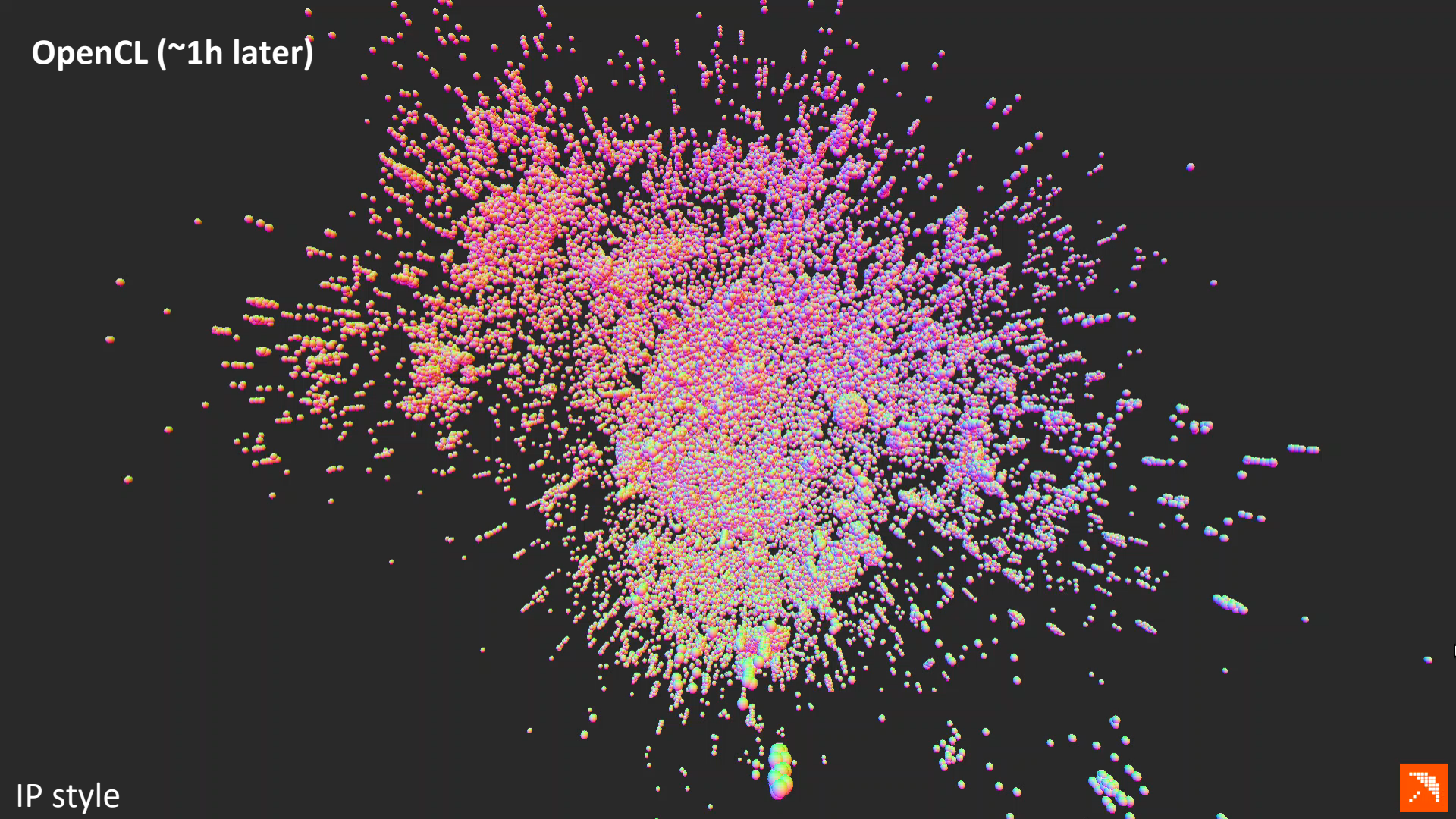
Global ASN graph

IP style

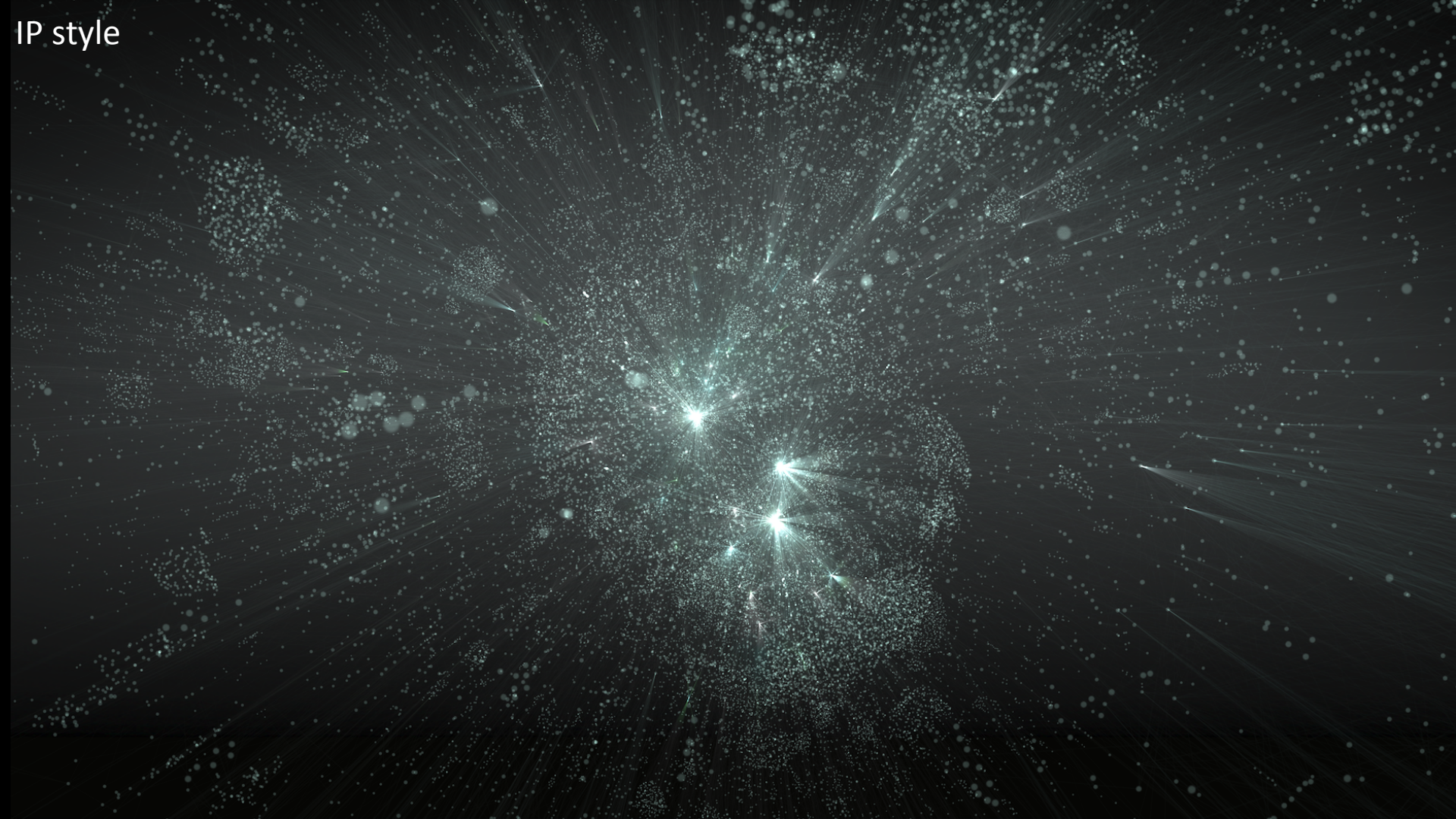
OpenCL Iterations



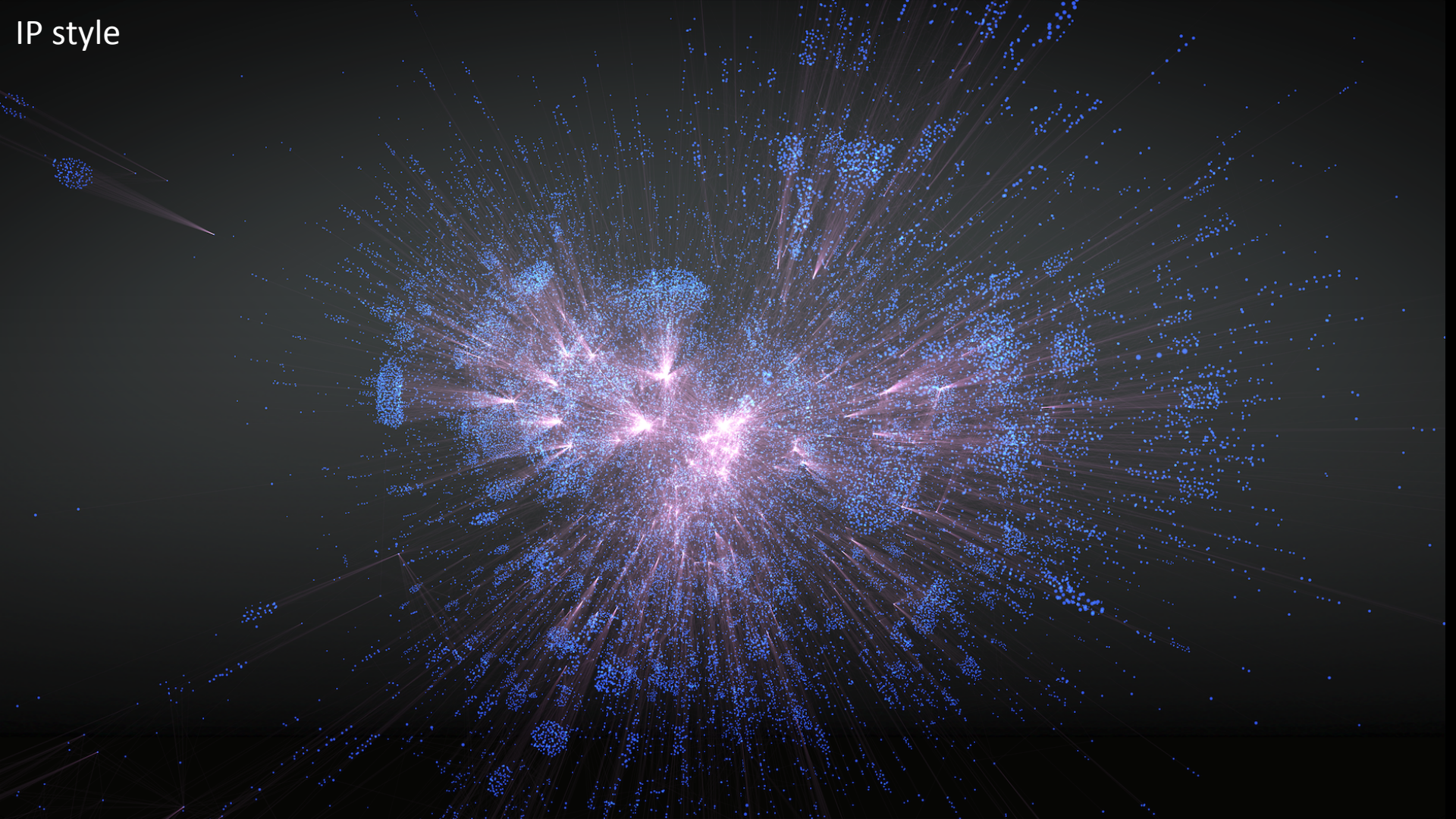
IP style


OpenCL (~1h later)
IP style

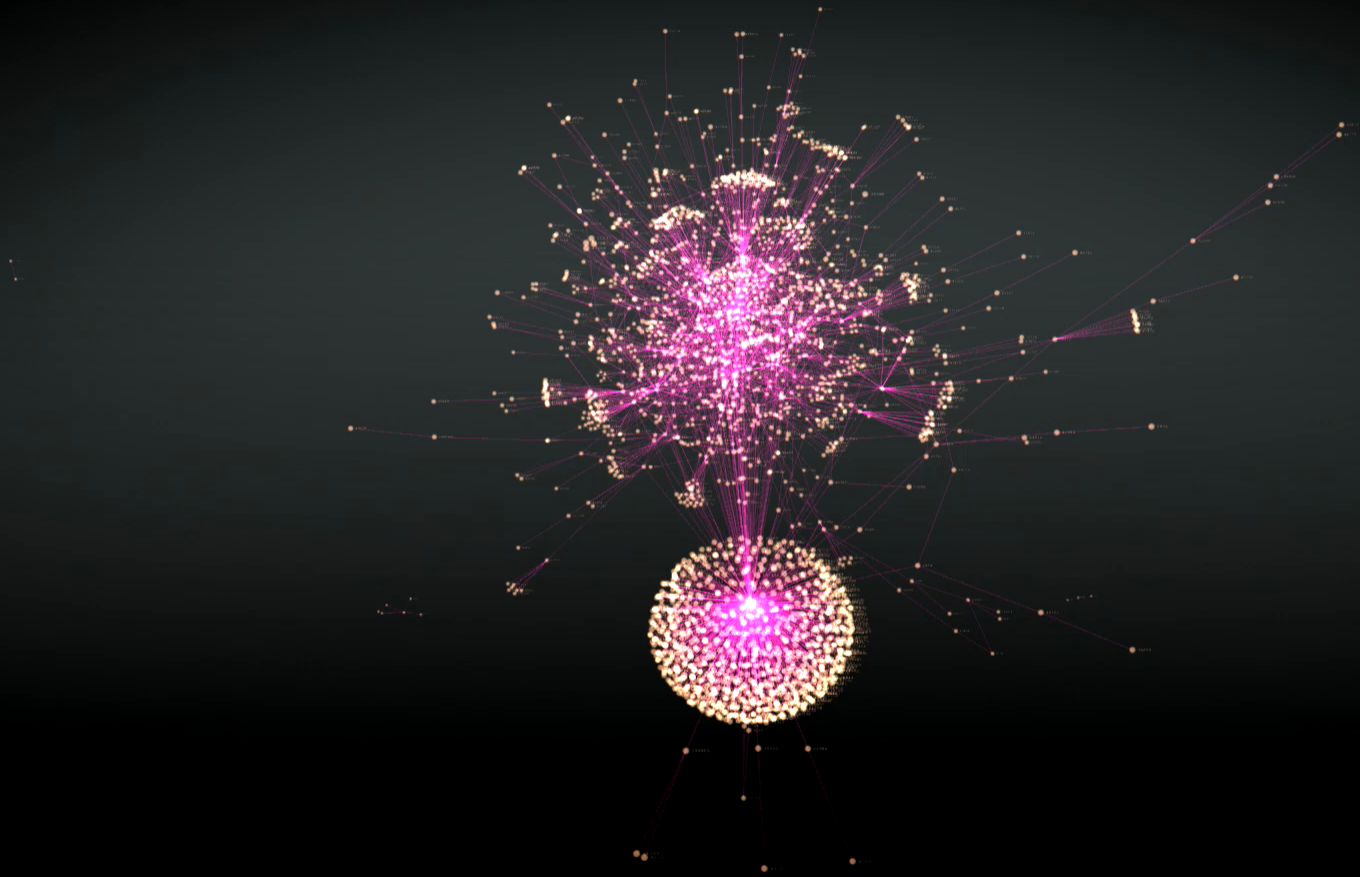

Full AS Network
IP style


IP style

IP style



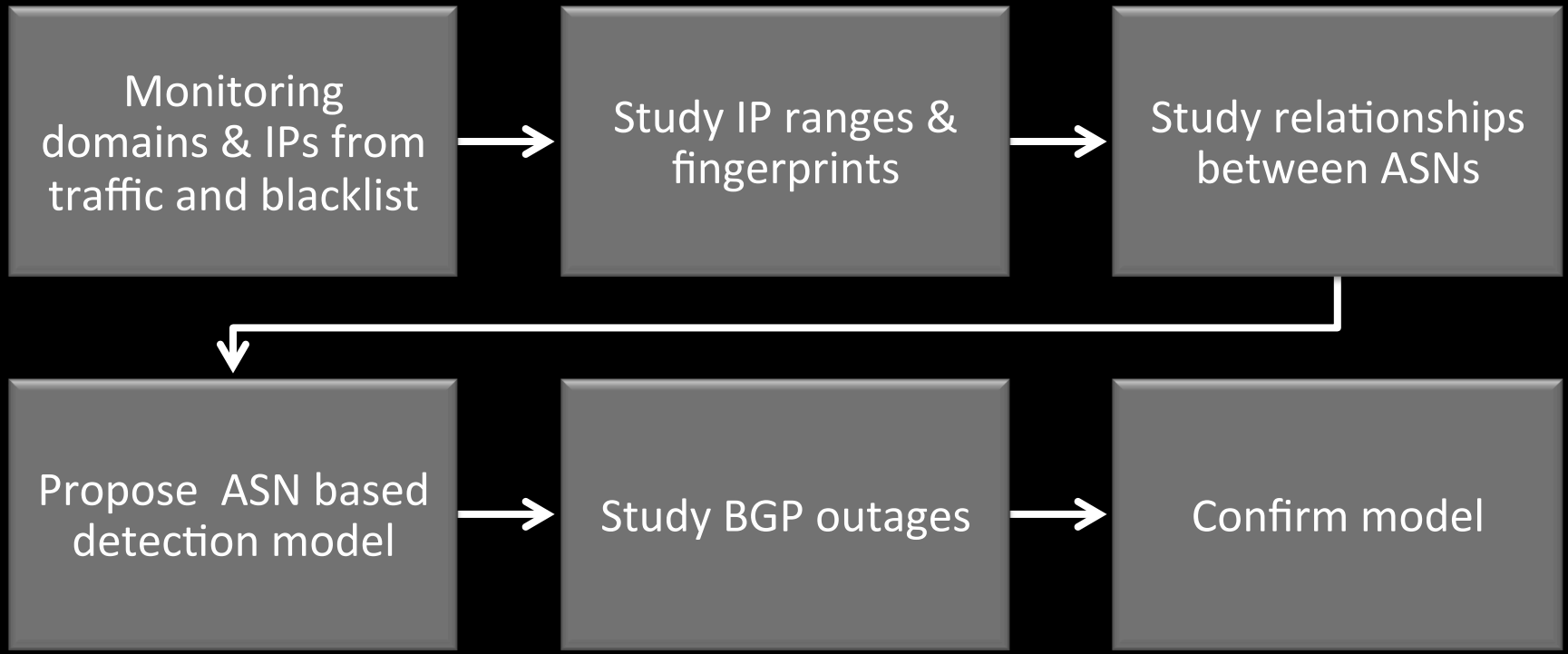
ASN Network (Ukraine)



IP style

Use Case #2
Suspicious Sibling Peripheral ASNs

Investigation Process



Study IP ranges and fingerprints

- Taking a sample of 160 live IPs from malicious domains
- /23 or /24 serving TrojWare.Win32.Kryptik.AXJX
- Trojan-Downloader.Win32.Ldmon.A

IP style

Study IP ranges and fingerprints

virustotal

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

Study IP ranges and 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:

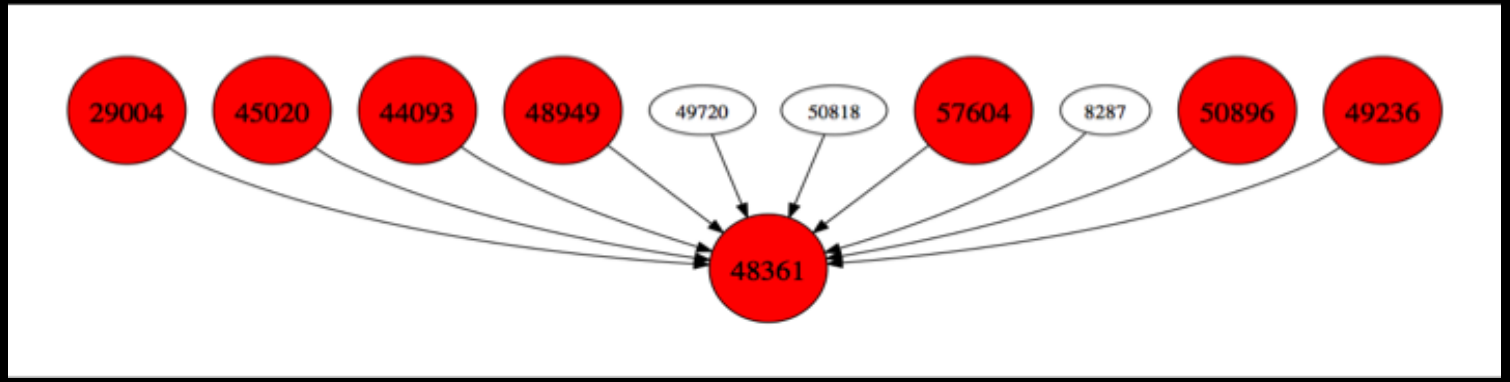
22/tcp open ssh OpenSSH 5.3 (protocol 1.99)

80/tcp open http?

Server setup is similar !

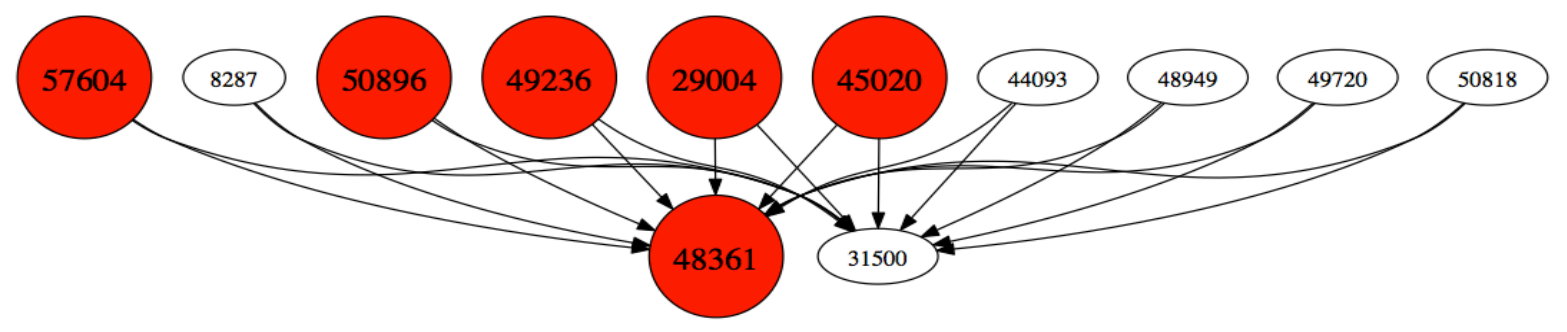
Propose ASN based detection model

SPN Concept (Sibling Peripheral Nodes)



Study relationships between ASNs

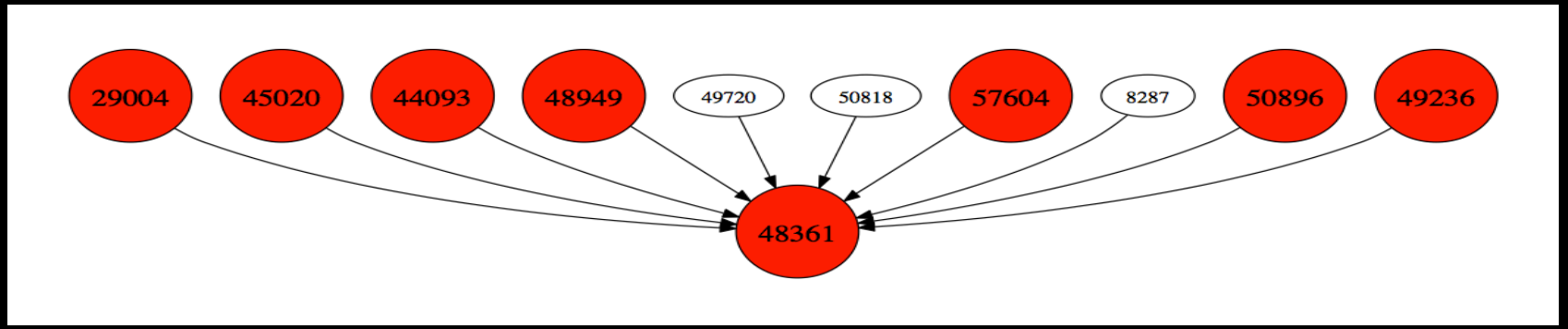
- January 8th topology snapshot, Ukraine, Russia



- 10 sibling peripheral ASNs with 2 upstream ASNs

Study relationships between ASNs

- February 21st topology snapshot, Ukraine, Russia



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

Study relationships between ASNs

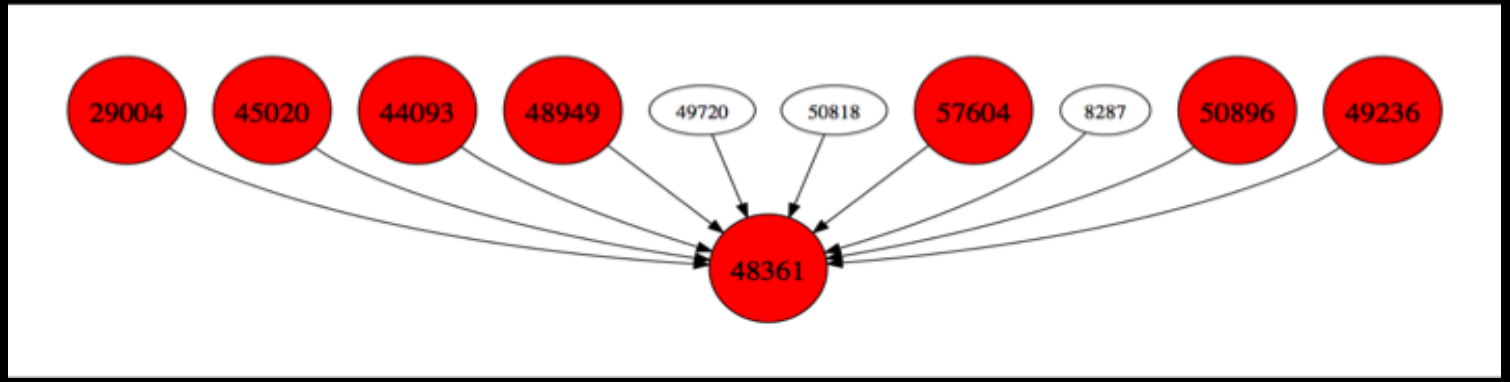
- 3100+ malware domains on 1020+ IPs !
- Payload URLs were live on entire IP ranges before any domains were hosted on them
- Seems the IP infrastructure is set up in bulk and in advance

http://pastebin.com/X83gkPY4

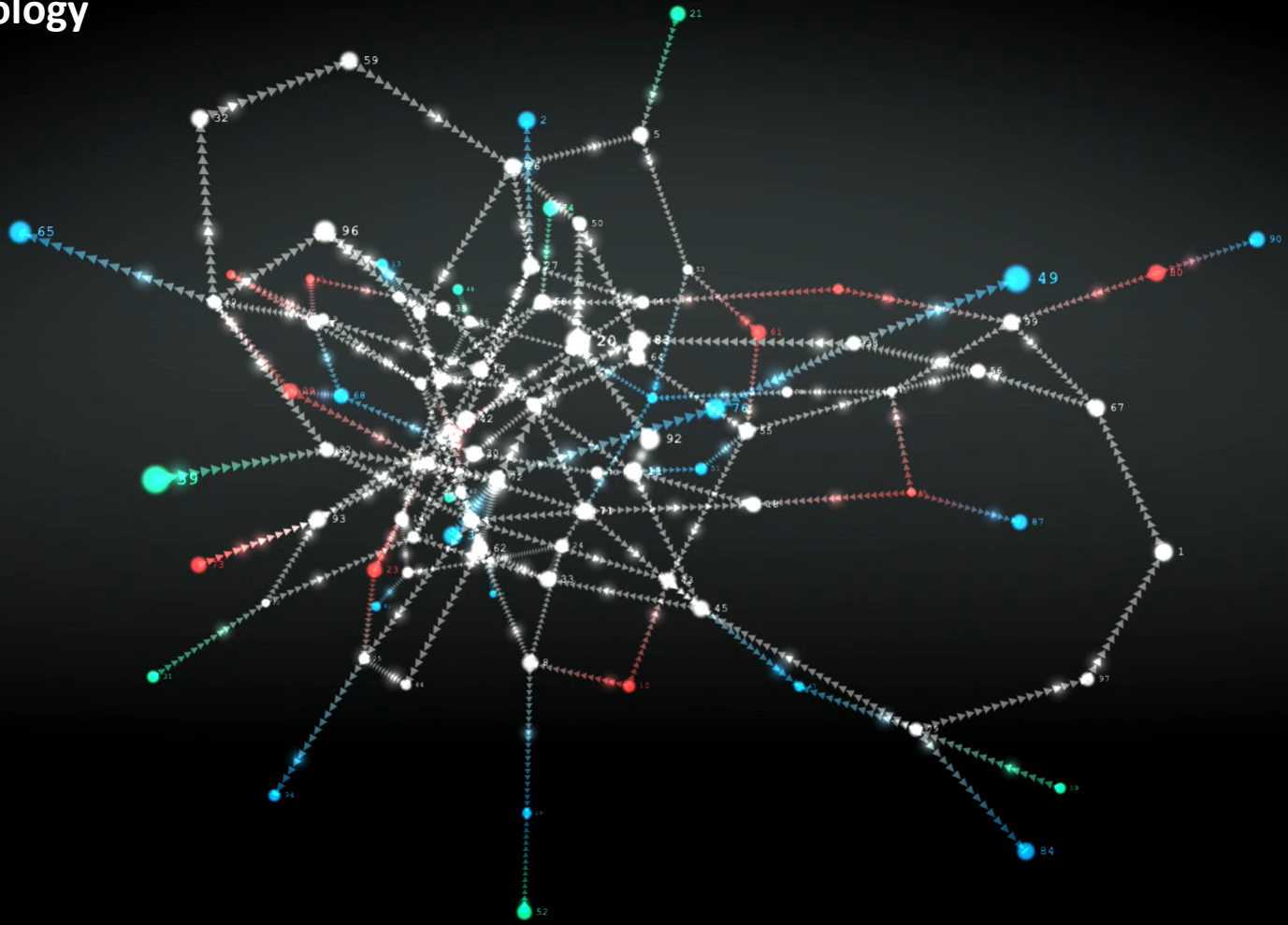
IP style

Data Visualization

SPN Concept (Sibling Peripheral Nodes)

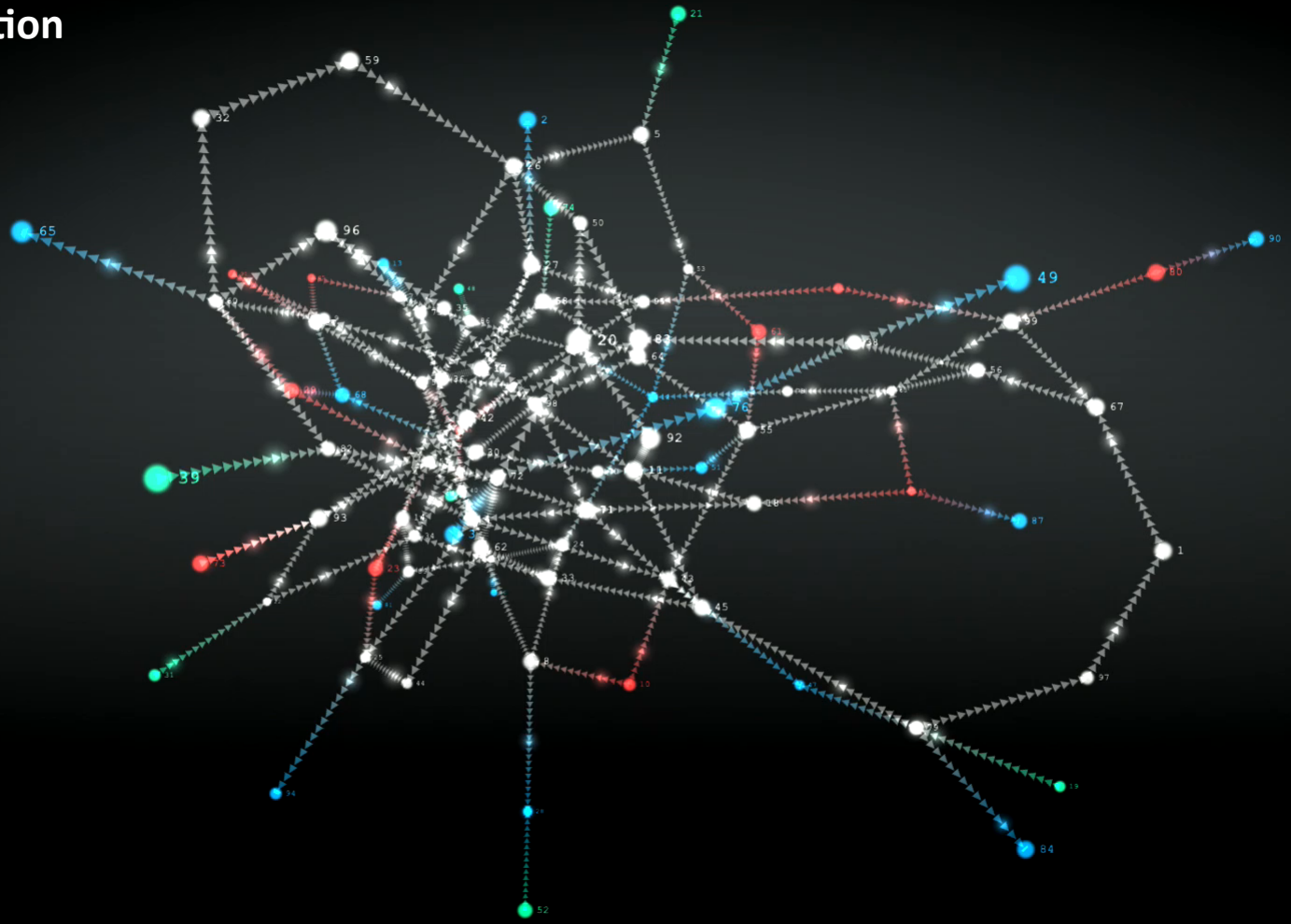


Graph Topology

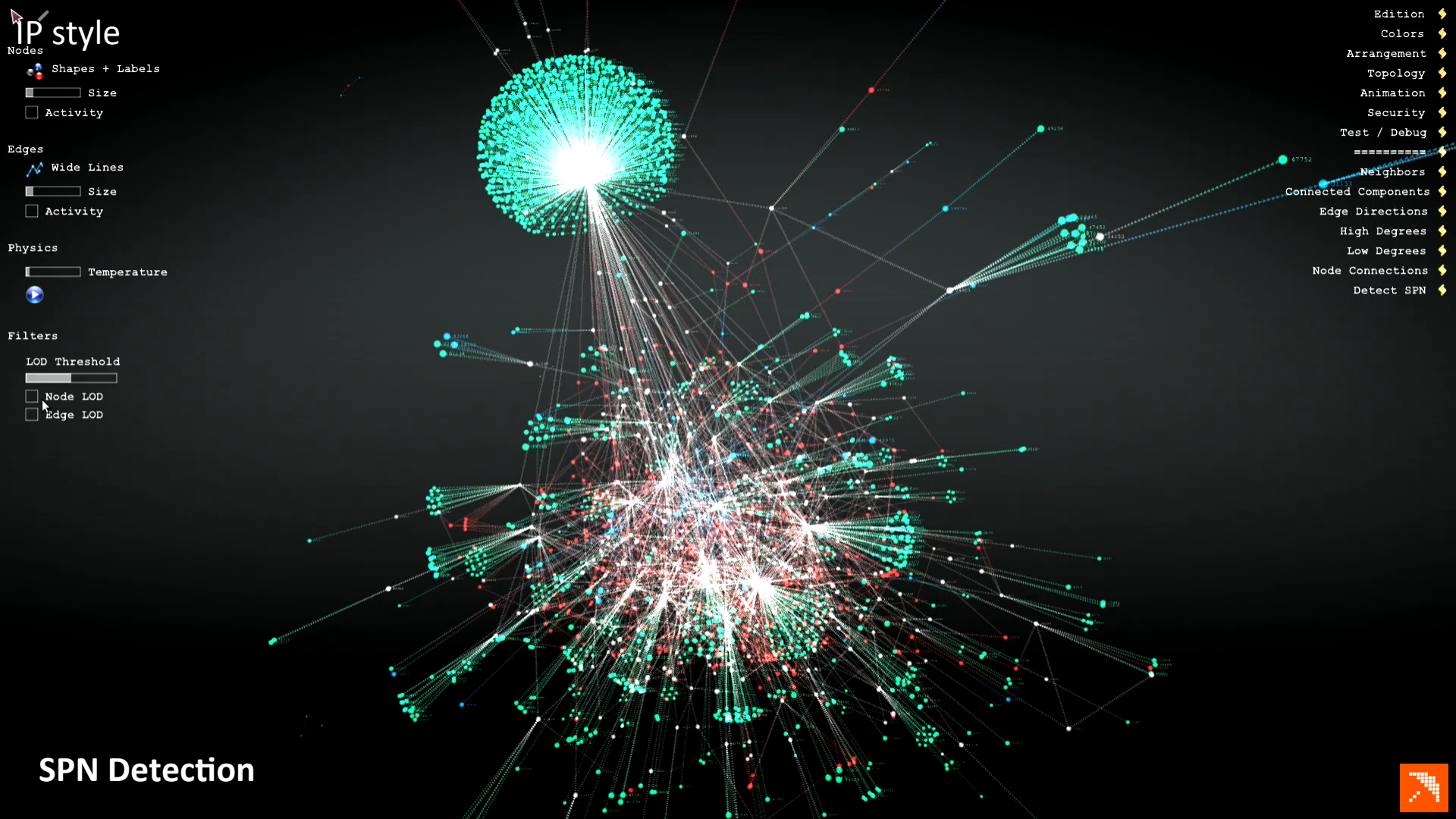


IP style

SPN Detection

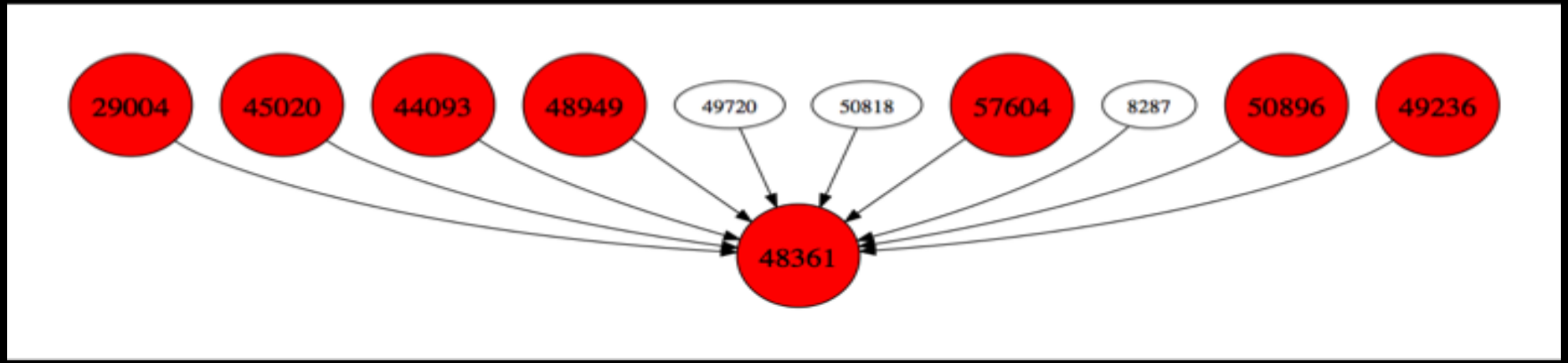


IP style


IP style
Nodes
Shapes + Labels
Size
Activity
Edges
Wide Lines
Size
Activity
Physics
Temperature
Filters
LOD Threshold
Node LOD
Edge LOD
Edition
Colors
Arrangement
Topology
Animation
Security
Test / Debug
==========
Neighbors
Connected Components
Edge Directions
High Degrees
Low Degrees
Node Connections
Detect SPN
SPN Detection

IP style

STUDY 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

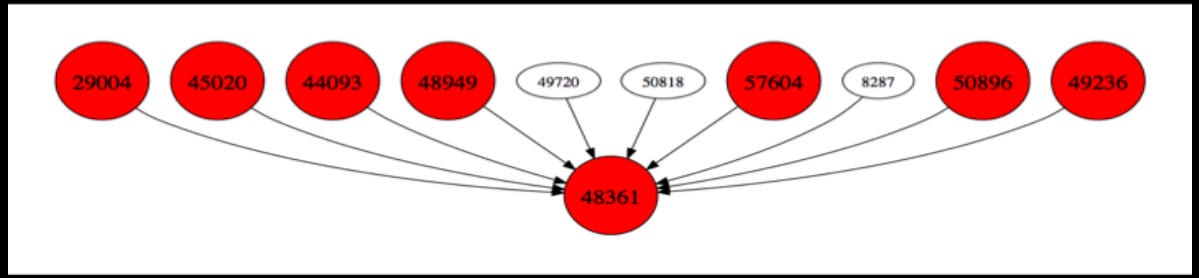
IP style

OVERLAPPING BGP OUTAGES

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

IP style

OVERLAPPING BGP OUTAGES



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

IP style

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

Conclusion

- **Zbot** fast flux proxy network
- Investigate IP space: AS graph **topology** and **sub-allocated** ranges
- 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 for graph navigation and investigation

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

DHIA MAHJOUB @DhiaLite

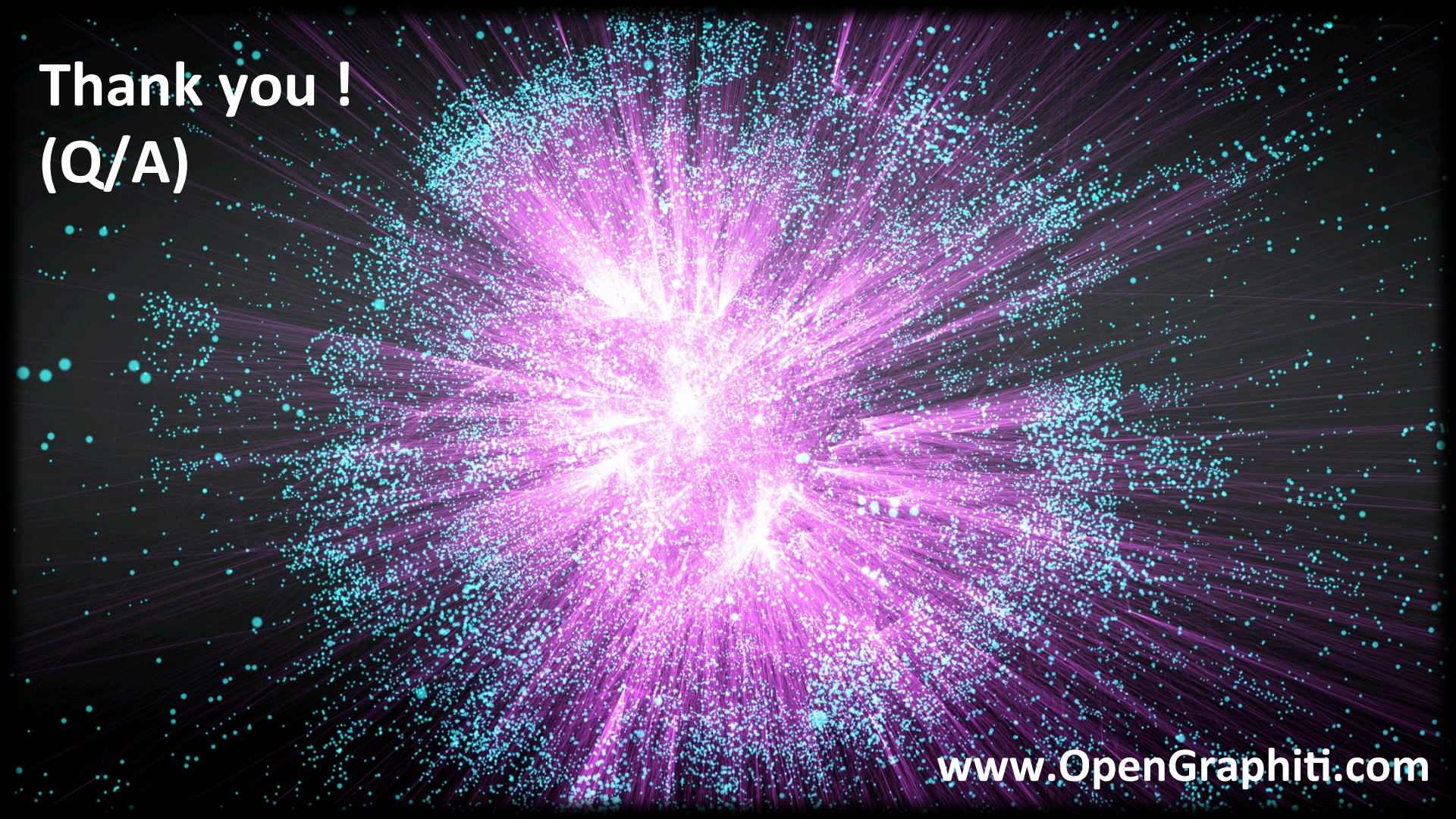
- Senior Security Researcher

THIBAULT REUILLE @ThibaultReuille

- Security Researcher

ANDREE TOONK @atoonk

- Manager of Network Engineering


Thank you !
(Q/A)
www.OpenGraphiti.com