"Toward Proactive Response against Cyber-Attacks based on global monitoring and analysis: PRACTICE project (Research Part)"

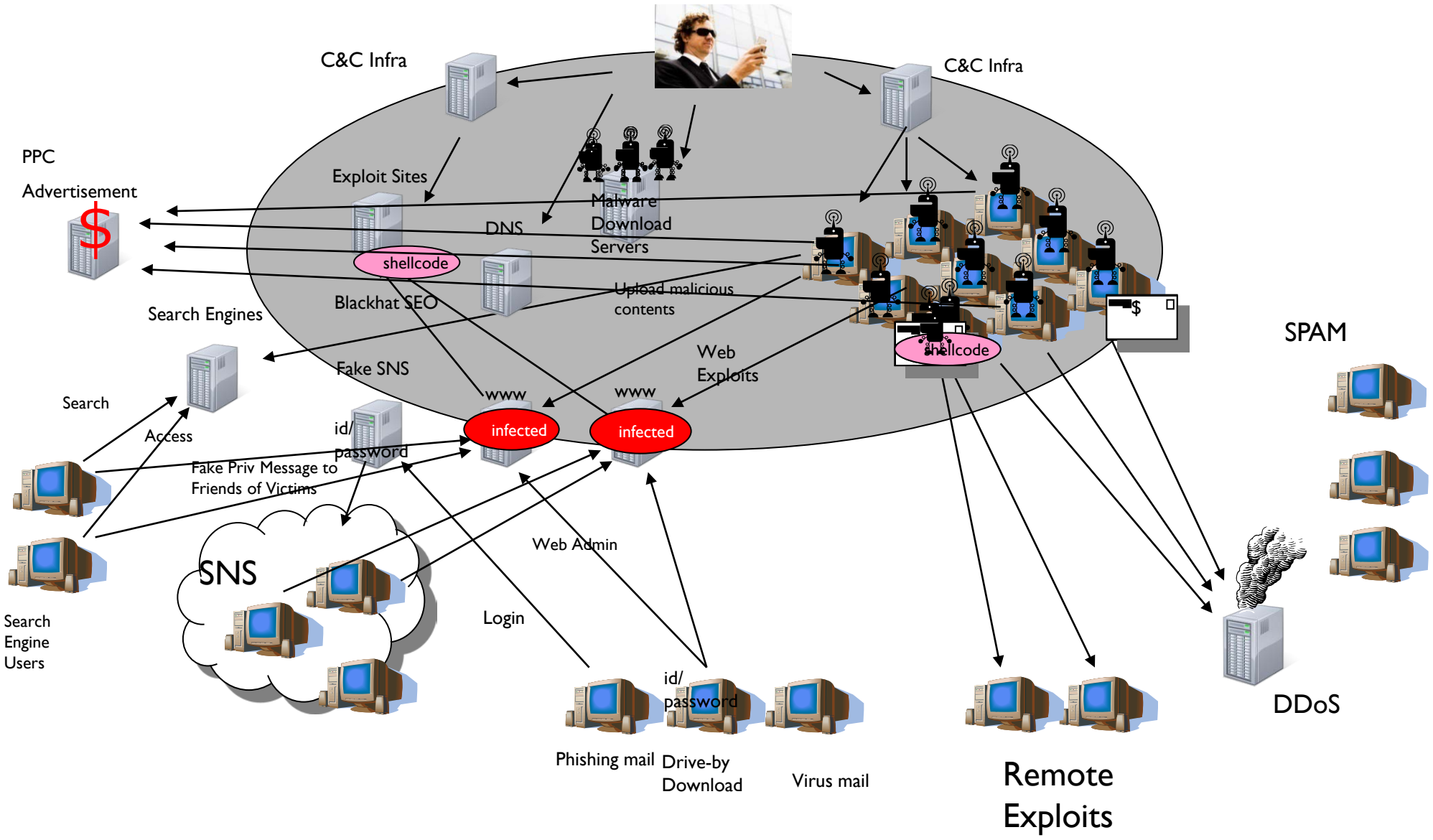
Koji NAKAO

Information Security Fellow, KDDI
Research Executive Director, Distinguished Researcher, NICT
Telecom-ISAC Japan, Vice-Chairman

PRACTICE Project

Proactive Response Against Cyber-attacks Through International Collaborative Exchange

Botnets: Core of problems...



Goal: Toward Proactive Response against Cyber-Attacks

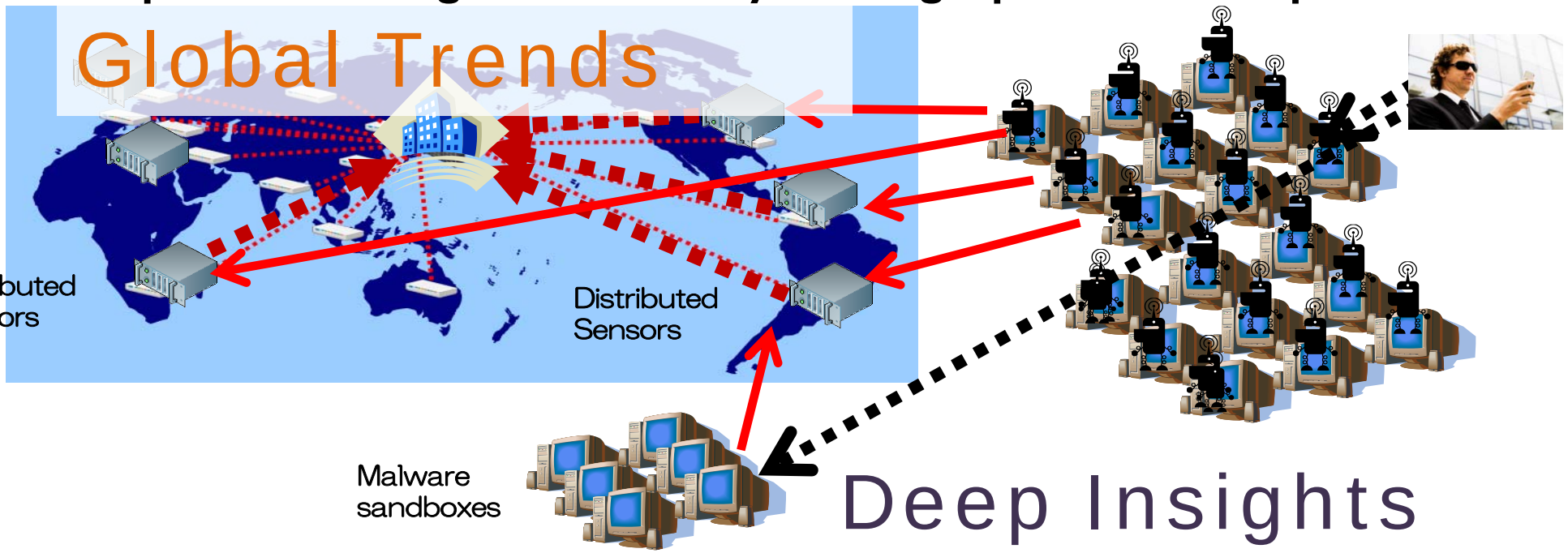
- **Project is organized by MIC and is consisted of R&D part and Field Trial part.**
- **R&D part: Gaining maximum awareness of ongoing cyber attacks (botnets)**

1) Macroscopic tracking of botnet attacks using various types of distributed sensors (victim-side monitoring) for grasping Global Trends

2) Microscopic tracking of individual bot-infected hosts using malware sandboxes (attacker-side monitoring) → Deep Insights

3) Based on correlation analysis among the above two approaches, Investigation of symptoms of cyber-attacks will be carried out for sharing among partners including international partners.

- **Field Trial part: Establishing quick and proactive response scheme with ISPs' cooperation through a field trial by utilizing input from R&D part.**



Who operates PRACTICE?

- MIC organizes the PRACTICE, which has Implementing Organizations and Supporting Organization.
- Implementing Organizations are ISP association(i.e. Telecom ISAC Japan) and related companies as a "field trial" part, and research institutes or security related companies as an "R&D" part.
- Supporting Organization is NICT which supports and assists "R&D" part of Implementing Organizations with technical expertise for cyber-attacks analysis technology.

Ministry of Internal Affairs and Communications

Implementing Organizations

Field trial of quick and proactive response based on the cooperation among ISPs.

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

NTT Communications

Data sharing

Partner countries

Data sharing

R&D of technologies which investigate symptoms of cyber attacks.

Designing The Future KDDI

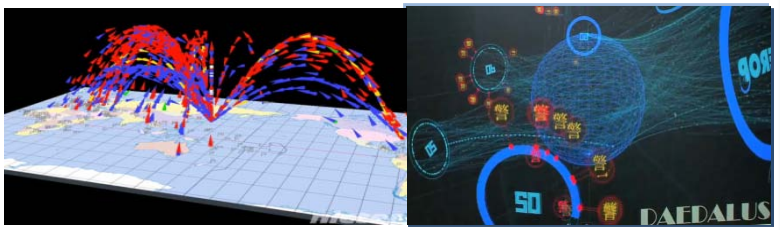
- Institute of Systems, Information Technologies and Nanotechnologies
- Japan Datacom Co., Ltd.
- KDDI R&D Laboratories
- SecureBrain Corporation
- Yokohama National University

Data & expertise

Supporting Organization

NICT National Institute of Information and Communications Technology

- **Technical support based on NICT's excellent expertise;**
- **Providing captured data and the results of analysis by NICT.**

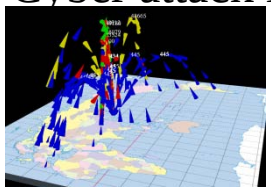


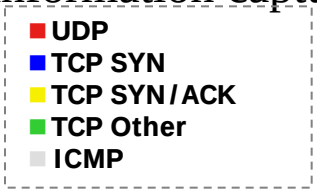
Visualization of cyber-attacks

What types of data to be shared through PRACTICE

- **Basic data to be shared with our collaborative partner's country:**

Atlas 1) Cyber attack information captured in Japan by LEU located in Japan (/20 network)





Information is visualized by means of the tool developed by NICT. Using this information, cyber-attack behaviors (mainly SCANs) to Japan can be observed. Each country could interestingly compare the trend of attacks with your own country (see below 2)).

Bot

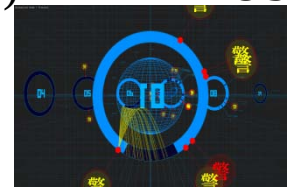
US&CH 2) Cyber attack information captured in our partner's country

GE

Cyber-Attack Information targeted to your own country is visualized by means of the tool developed by NICT based on the captured data from darknet space in your country.

3) DAEDALUS data is provided (supported by NICT, Japan)

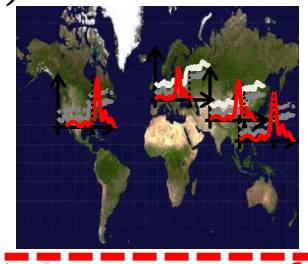
DAE



An organization (Use Case) : 14,000 addresses for livenet and 2,500 addresses for darknet Attacks by means of five continued alerts (with yellow) and one new alert (with red) were observed at 18:00 on July 10, 2012 in real-time basis. It is also possible to detect DDoS attack targeted to the livenet addresses just registered previously from your country.

- **Results of Analysis can also be shared with our collaborative partner's country:**

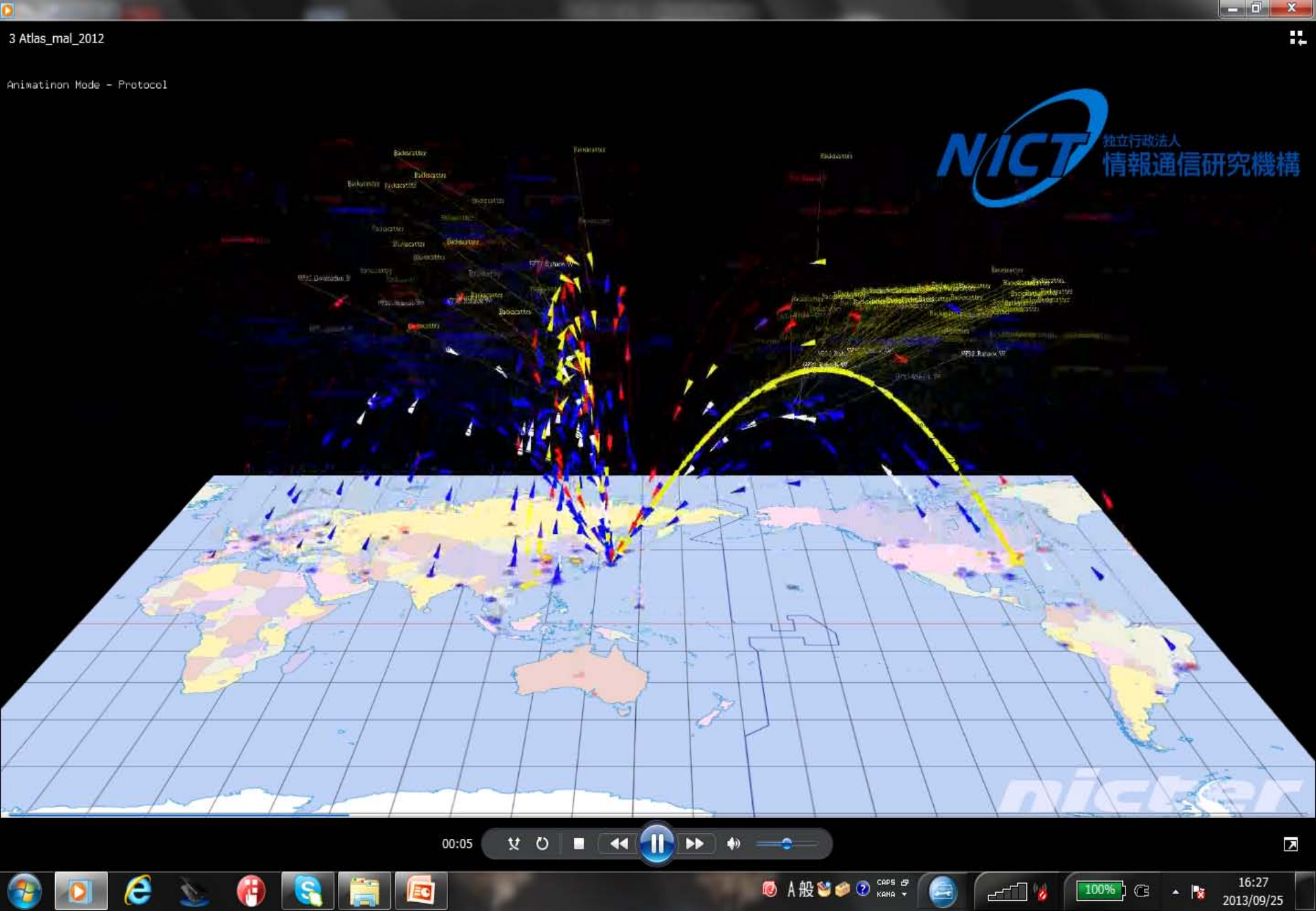
4) Attack similarity and specificity

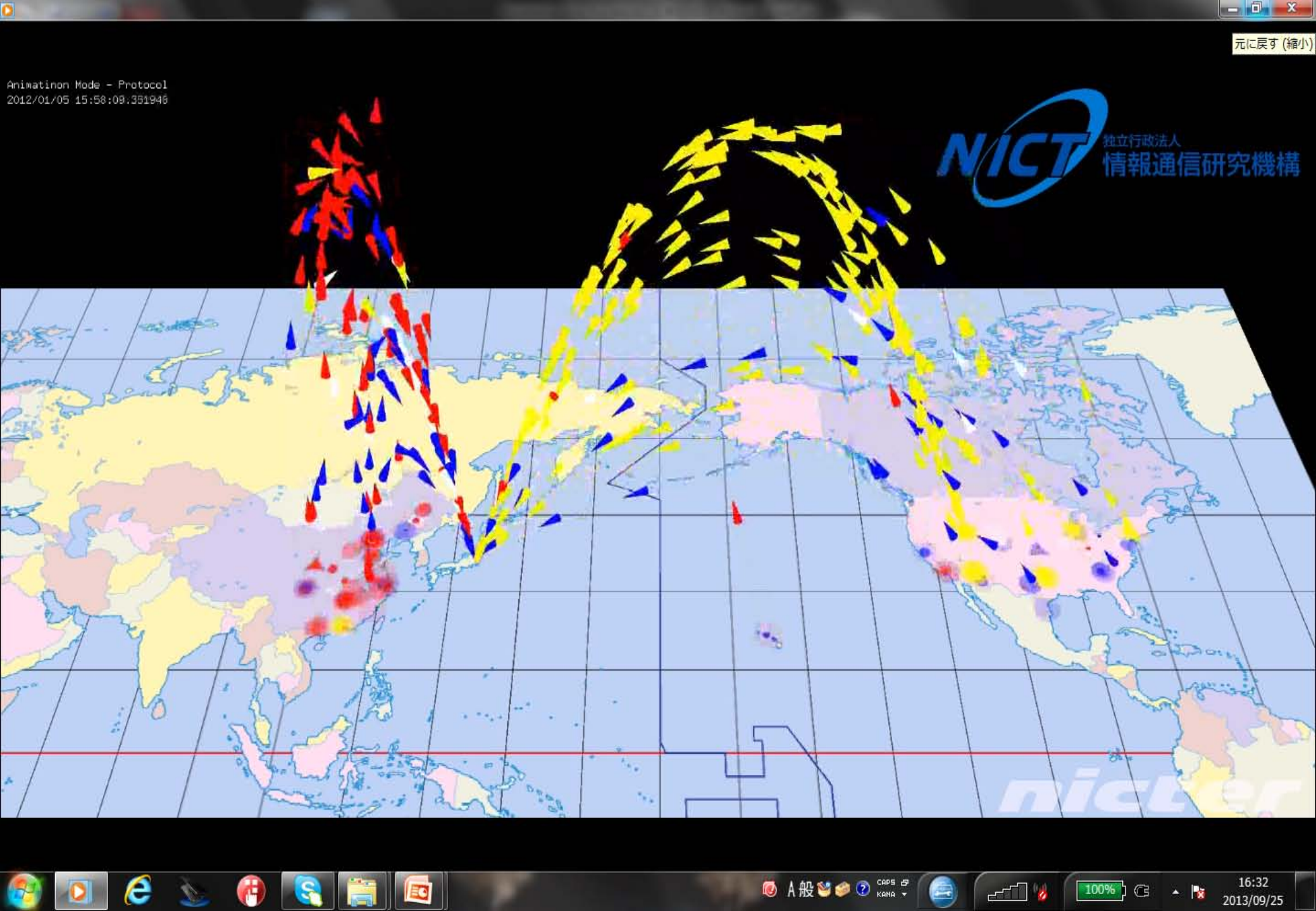


Based on several analysis engines, your country can grasp similar attack behaviors observed by many sensors located all over the world. This information can be shared among our all collaborative partners. Therefore, your country should be aware of this similar propagation of attack for your proactive response. On the other hand, attack behavior specificity in your country can be reported. In this case, your country will be required to take a special measure against specific attack only observed in your country (only shared with your country).

5) Symptoms of attack behavior → Today's topic

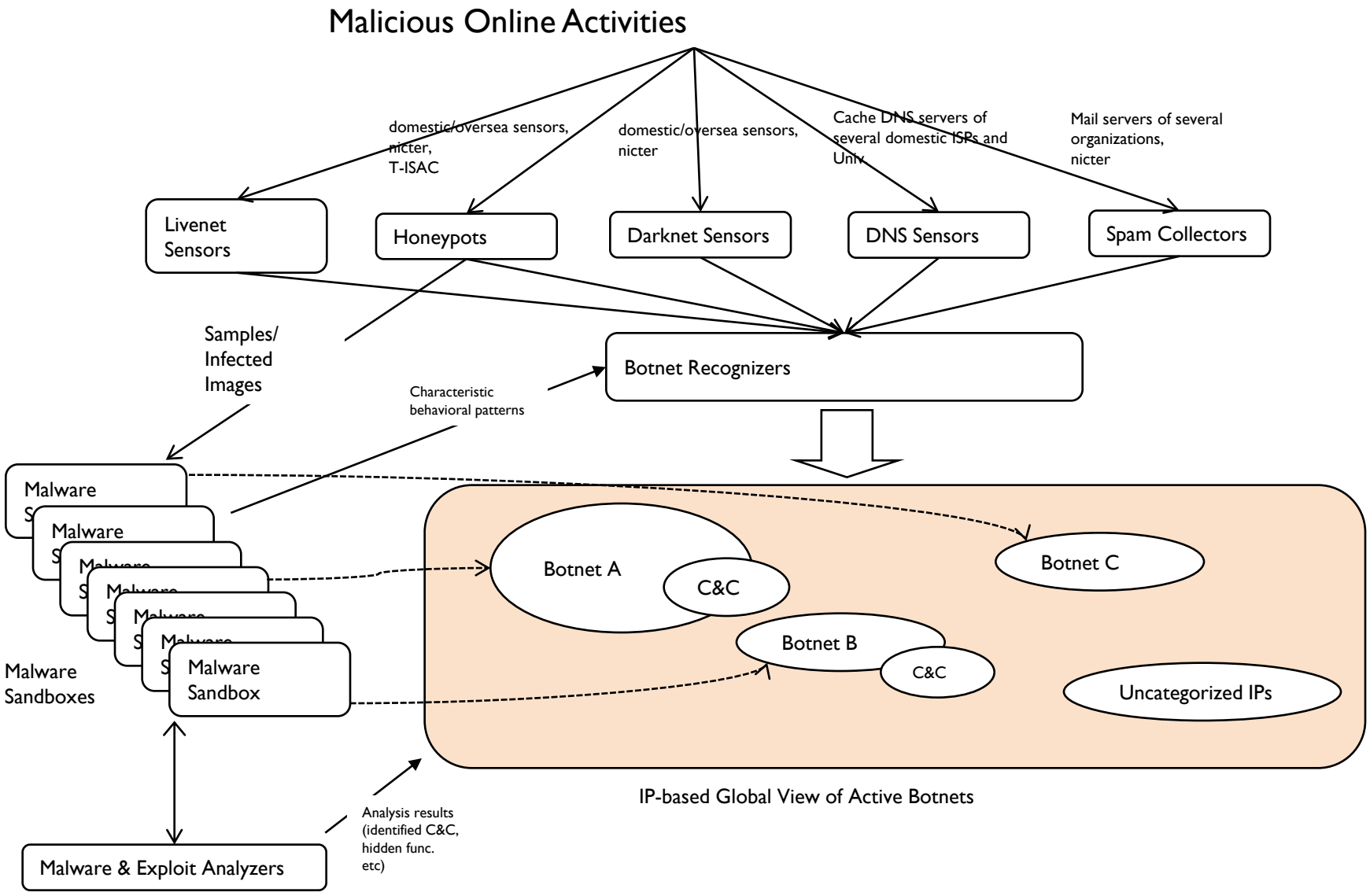
Based on various analysis methods, you will get symptoms of cyber-attack which will be very early stage of attack behavior. For example, "a new type of scan is getting observed in a synchronized manner among several sensors" will be informed.


3 Atlas_mal_2012
Animation Mode - Protocol
NICT
独立行政法人
情報通信研究機構
00:05
100%
16:27
2013/09/25

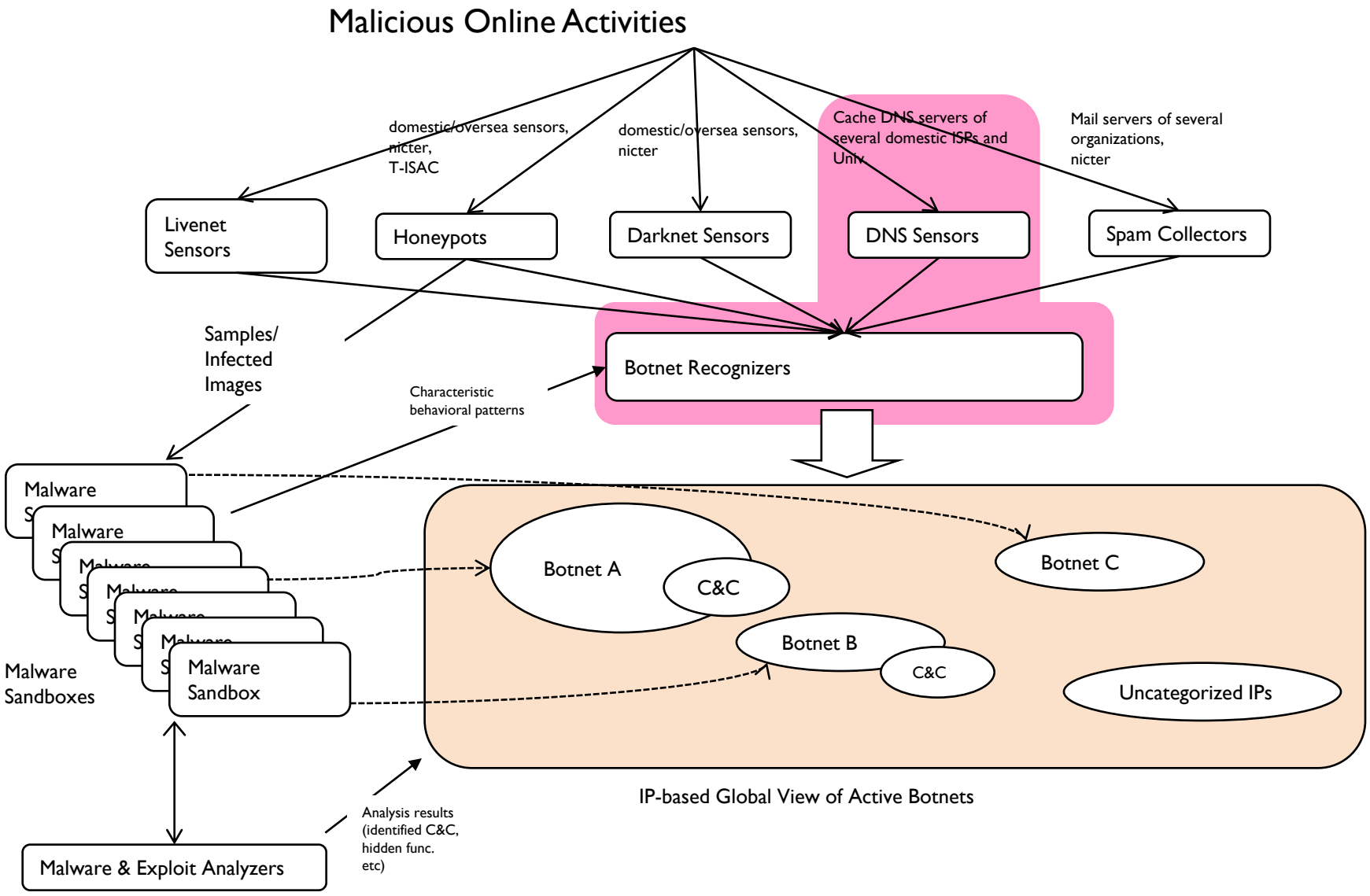

元に戻す (縮小)
Animation Mode - Protocol
2012/01/05 15:58:08.351946
NICT
独立行政法人
情報通信研究機構
nict


Animatinon Mode - Protocol
National Institute of Information and Communications Technology
Time : 2012/09/10 13:33:40.620397
SensorID : 100
Src IPaddr : 188.109.224.129
Protocol : TCP_SYN
Src Port : 54392
Dst Port : 25
Src CC : DE
City : Mlheim (Nordrhein-Westfalen)
TCP_SYN
TCP_SYN_ACK
TCP_ACK
TCP_FIN
TCP_PUSH
TCP_OTHER
ICMP
nicter
100%
16:25
2013/09/25

System Overview

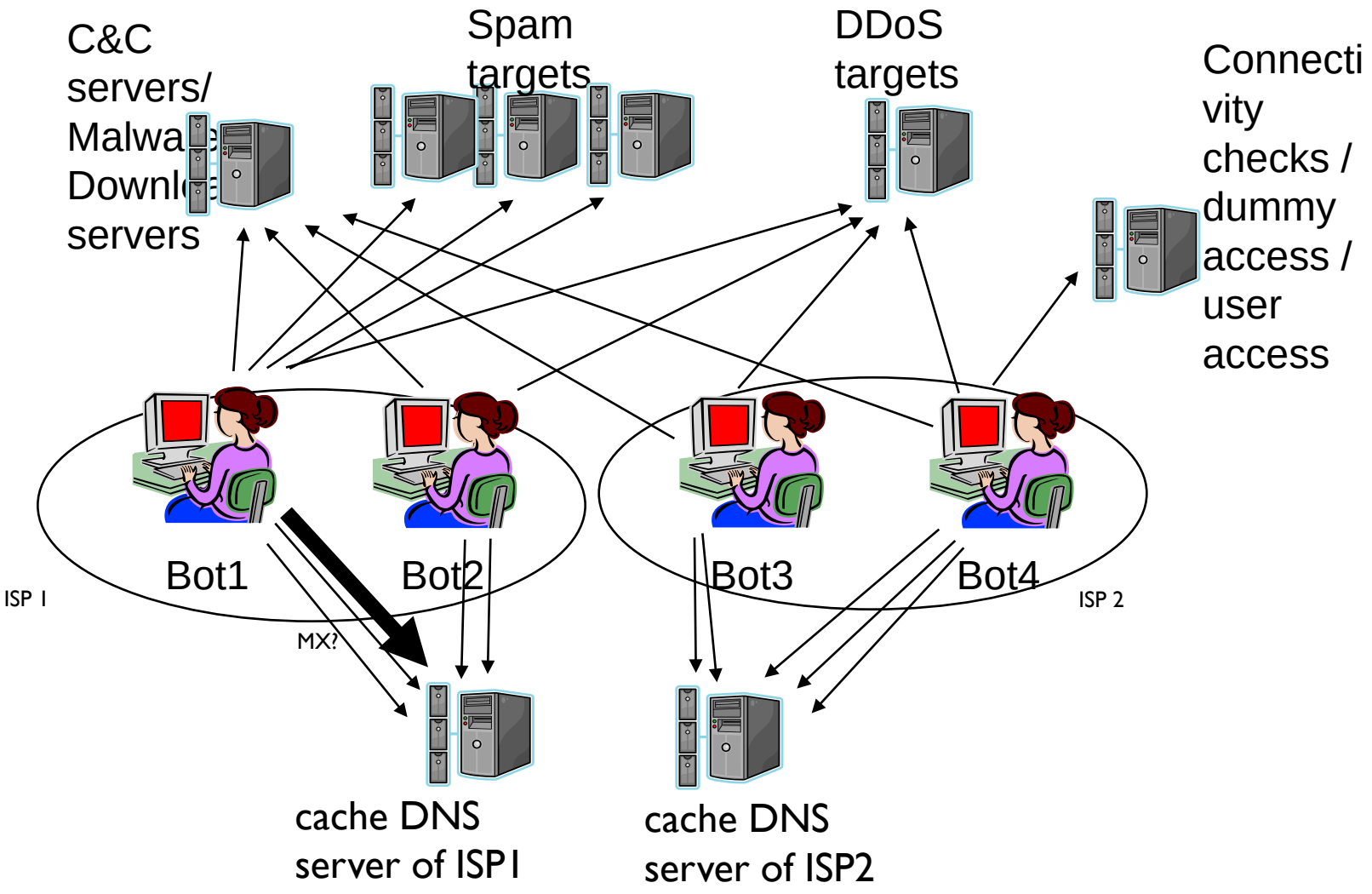


System Overview



Botnet Recognition from DNS traffic

Bot-infected hosts create various DNS traffic



Trials of microscopic botnet tracing

We executed different types of bot samples for several days～weeks in Internet-connected sandboxes.

Bobax.worm.gen / W32.Spybot.Worm 3b7eb30a8309d9ec39ce22f07c958f15	W32/Sality.gen / W32.Spybot.Worm Ff0aae1480ab4975829996d17af3314b
W32/Virut.gen.a / Virut.W 017f3b27048857ffd08495fb6d58da4e	W32/Virut.gen / Backdoor.Trojan e2c01dd431b22364483629f0ac4c5a18
Exploit-Mydoom / W32.Gobot.A 4681d09d953a3952208b9e55aefccffb	/ Trojan.Smoaler a0d25e76c01de3be961343e4389182f8
PWS-Zbot.gen.aac / Trojan Horse 65dc0682604e08c4bb2201ea67204181	FakeAlert-SecurityTool.gf / W32.Waledac.C!gen2 a64037fcb070da113694fa6972f8573e
W32/Pift / W32.Morto.B 0475c97ddb96252febff864fb778b460	W32/Bobax.worm.gen / fbf26c7e7040abc53fa1e161268414cf
Generic BackDoor.u / Backdoor.Makadocs 546fa31bb7a4164ca25c8667d4352338	W32/Sdbot.worm / W32.IRCBot.Gen Fbacdd87c0dd445d0235261e41ce9928
W32/Pate.b / W32.Pinfi a6345baeb3ca0270ebdbae9a70f6ddbd	W32/Sdbot.worm.gen.z / Suspicious.IRCBot fa8c73b67bc9d320d3c2c56870f3149d
W32/Bobax.worm.gen / W32.Bobax!dr 02921989f9c6ebd7436993dc2bf5b852	McAfee / Symantec Md

Characteristic DNS behaviors

1. Periodic Queries

2. Spam Related Queries

3. DGA (Domain Generation Algorithm) Queries

1. Periodic DNS Queries by Several Bots

Classic bots makes periodic DNS queries
(Rather easy to detect at cache DNS)

Zbot

Domains	Interval mins	hours
mail.loaadss.pl.	79.6	1.3
mx.loaadss.pl.	77.4	1.3
smtp.loaadss.pl.	75.4	1.3
pop.loaadss.pl.	76.9	1.3
mx2.finansgroups.com.	133.6	2.2
mx3.finansgroups.com.	132.1	2.2
mx4.finansgroups.com.	133.6	2.2
mx5.finansgroups.com.	133.6	2.2
in1.smtp.messagingengine.com.	569.8	9.5
alt4.gmail-smtp-in.l.google.com.	17.5	0.3
gmail-smtp-in.l.google.com.	3.4	0.1
mail7.digitalwaves.co.nz.	5.1	0.1
mxs.mail.ru.	52.8	0.9

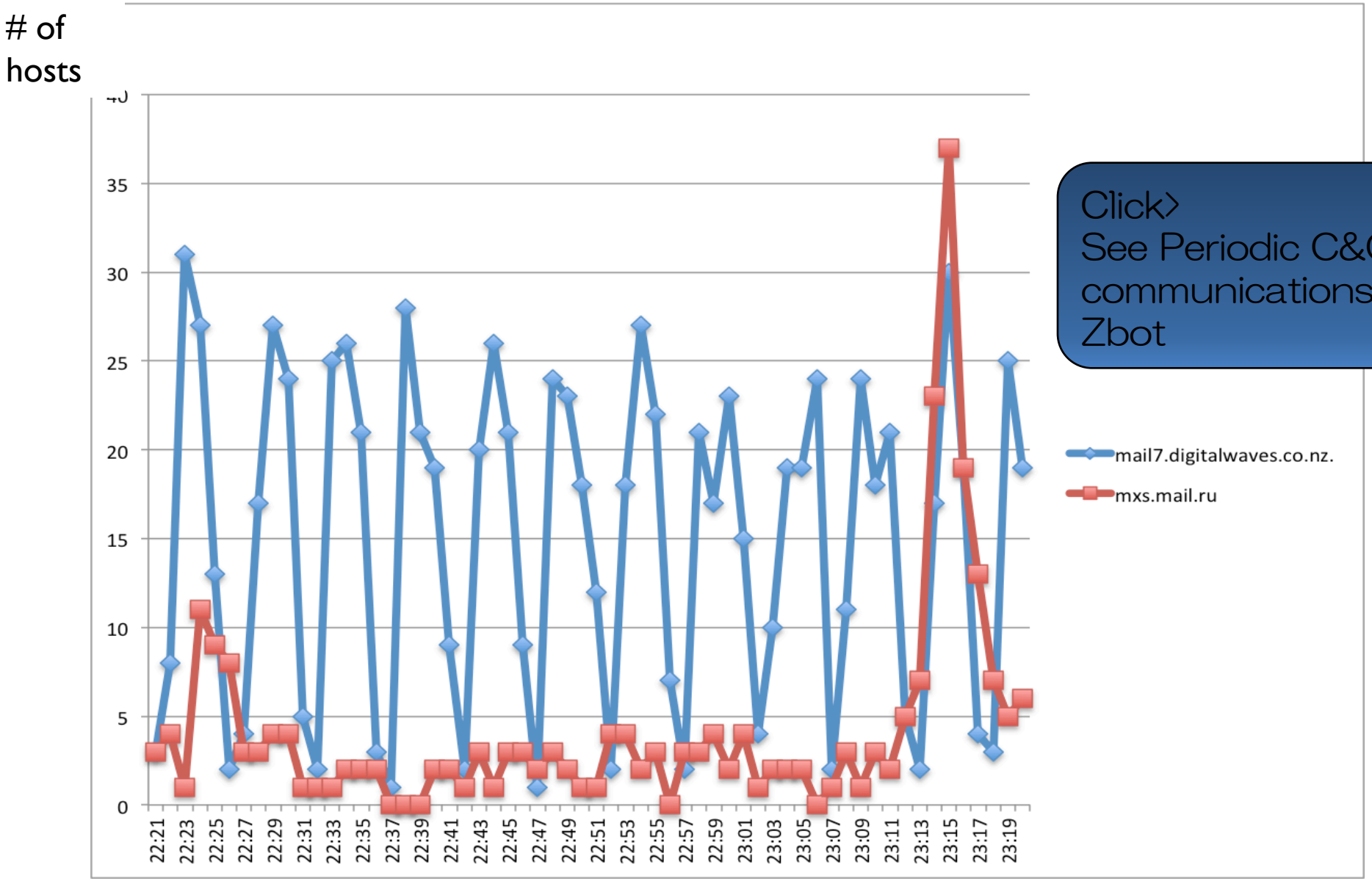
Virut

Domains	Interval mins
mxs.mail.ru	18.4
alt4.gmail-smtp-in.l.google.com.	7.4
gmail-smtp-in.l.google.com.	4.0

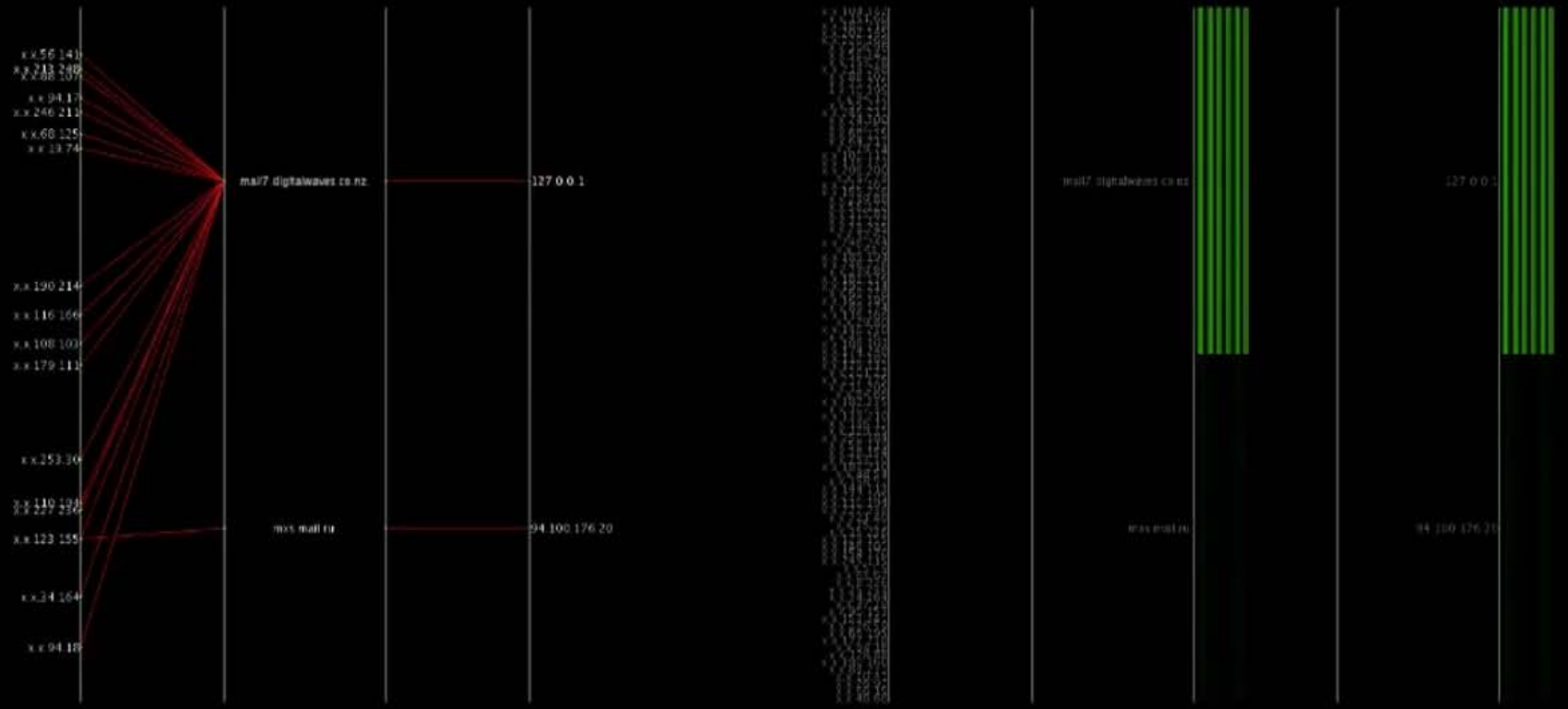
Gobot

Domains	Interval mins
fucko.servebeer.com.	1.9
fucko1.servebeer.com.	1.8
fucko2.servebeer.com.	1.8

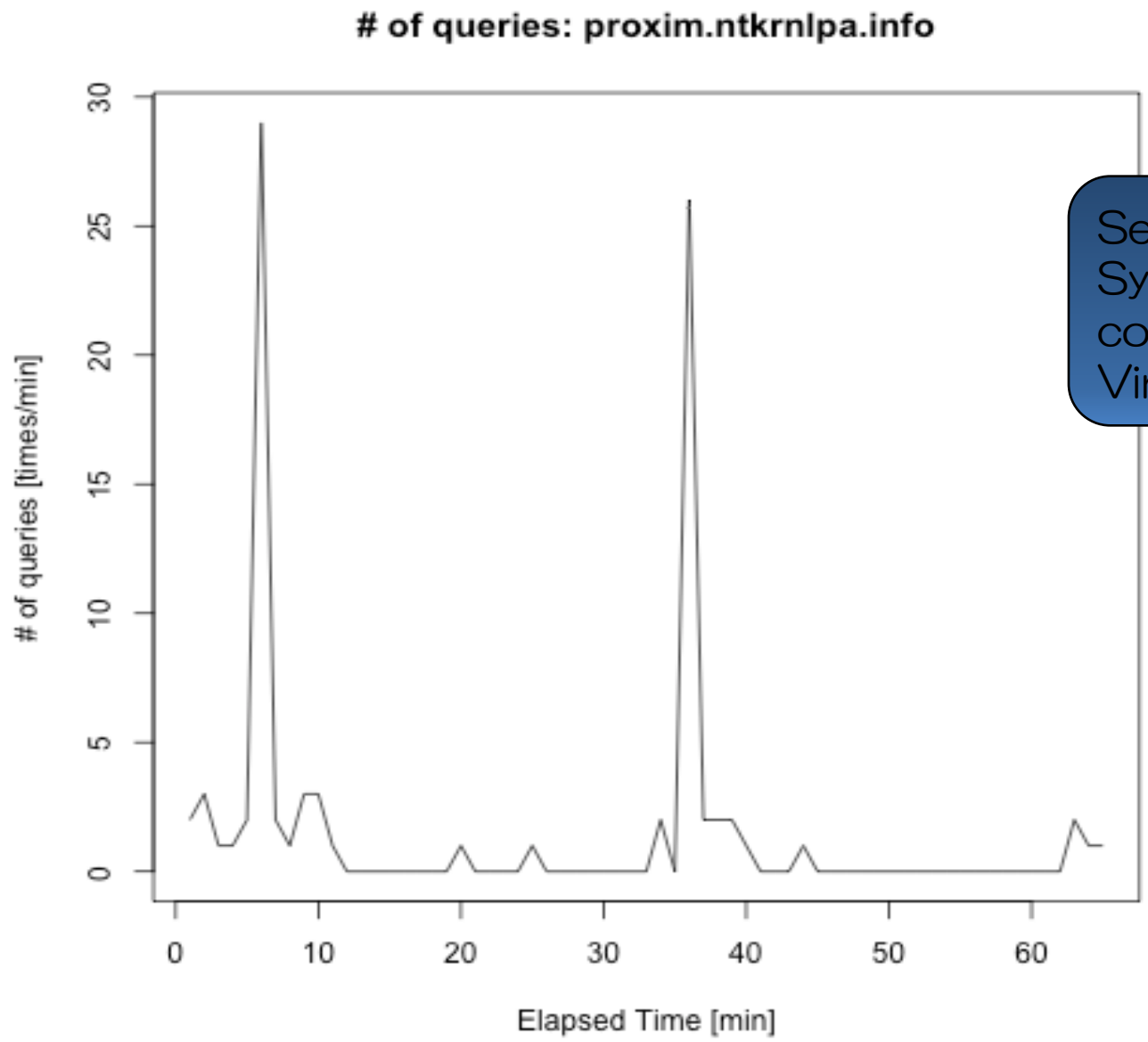
Zbot Detected at Real Cache DNS Server



2012/06/XX XX:51:00



Virut.g Detected at Real Cache DNS Svr

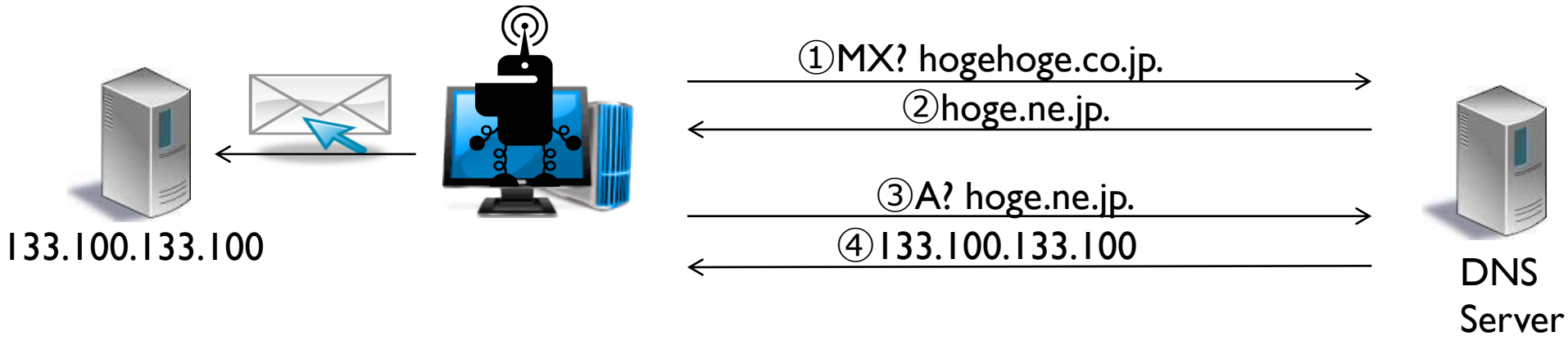


See Well Synchronized C&C communications by Virut.g

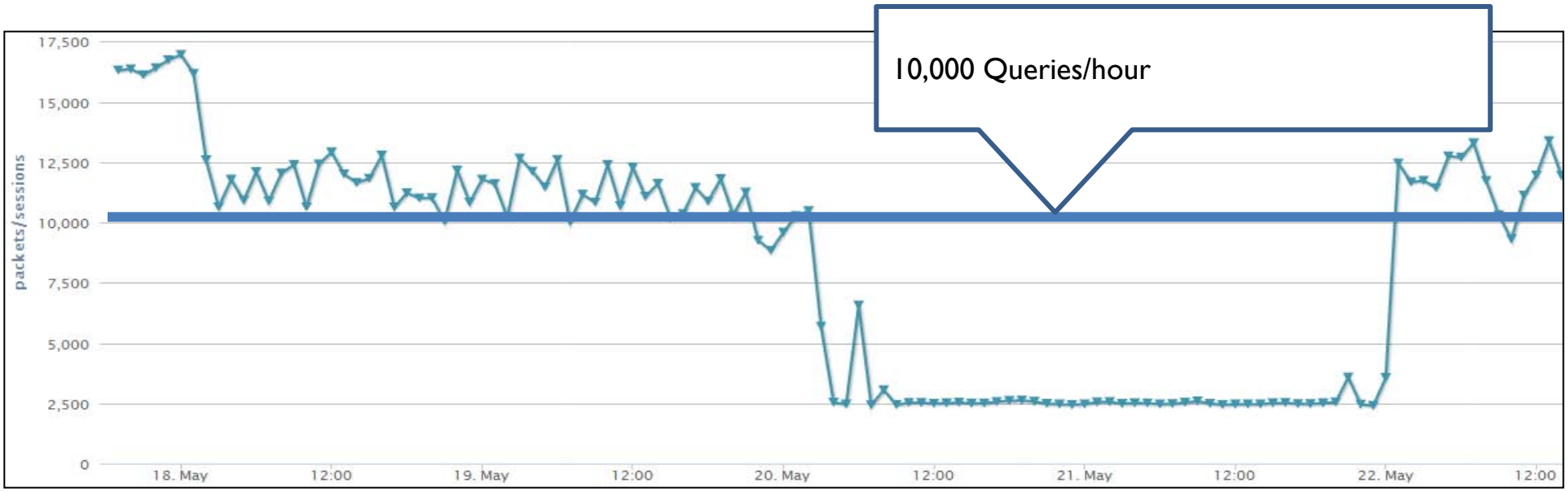
2. Spam Related Queries (Direct Spam)

Average DNS Queries per Hour

	Spybot	Zbot	Virut	Gobot	Morto
Total	14406	32	5218	65	10
MX	7268	0	2072	0	0
Failure	932	0.36	1177	0	0.68



2. Spam Related Queries (Direct Spam)

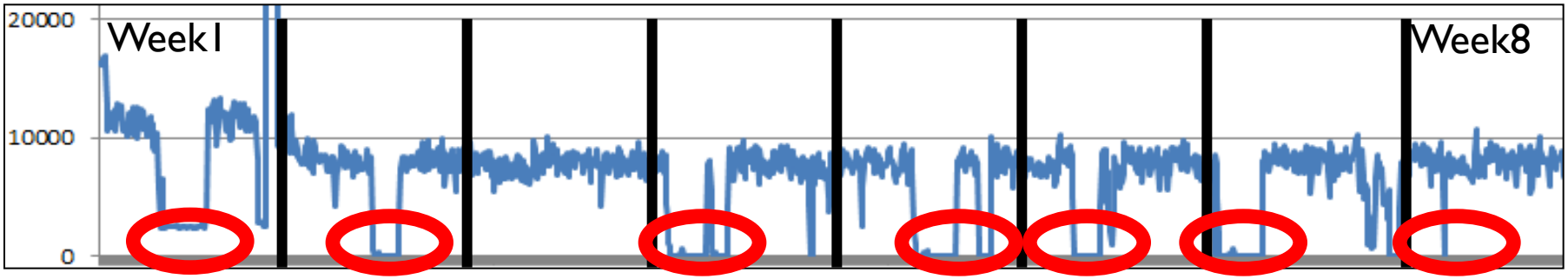


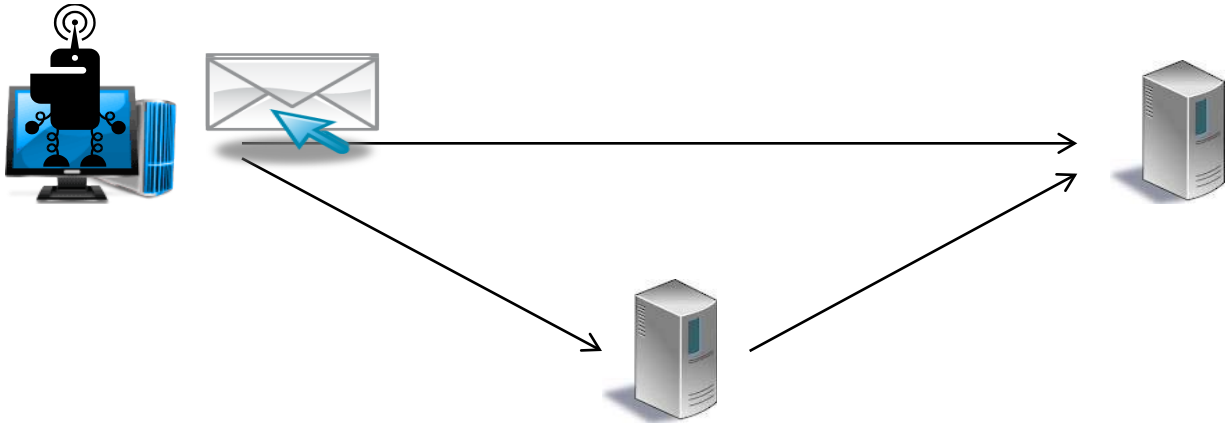
Half of the queries are for MX records and the other half are for A records

2. Spam Related Queries (Via Relay)

There are some periods with low-frequency queries

Spybot DNS traffic for 8 weeks





Open Relay/Malicous SMTP

Instead of sending spam directly to its destination, the samples used open relay

3. DGA Queries

- Spybot and Virut contained Domain Generation Algorithm (DGA) to generate domains internally to connect their C&C servers.
- Many DGA domains point to same IP address.
- These DGA generated domains created many domain resolution failures (NX Domain, etc)

Average DNS Queries per Hour

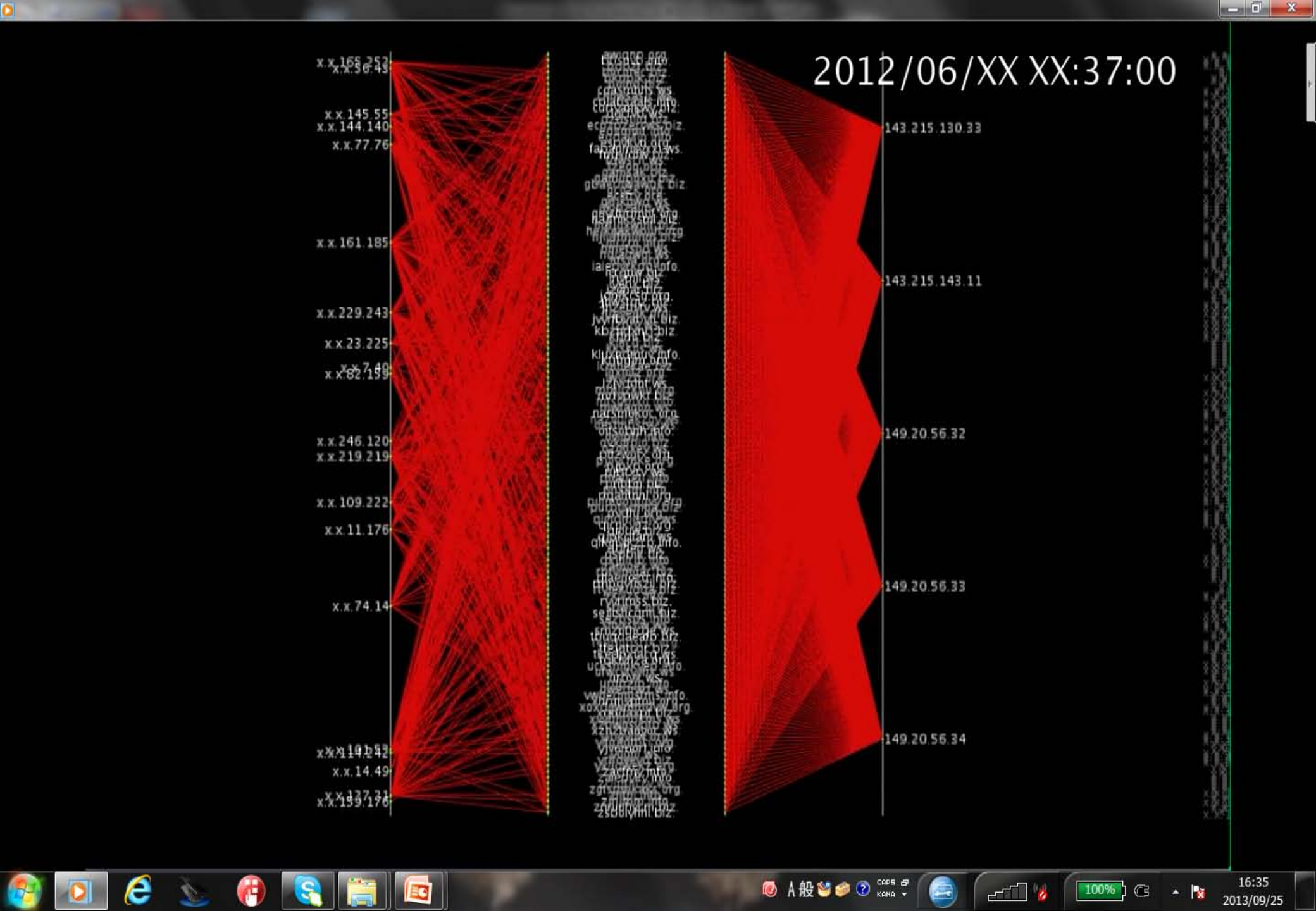
	Spybot	Zbot	Virut	Gobot	Morto
Total	14406	32	5218	65	10
MX	7268	0	2072	0	0
Failure (NX Domain)	932	0.36	1177	0	0.68

See an Example of DGA traffic

Examples of Failed Domains

acdgnkru.dynserv.com
ajfgffpjh.dynserv.com
anwgtctvxr.dynserv.com
bjlydbagnlu.dynserv.com
bqlevrolvaa.dynserv.com
bvqffersost.dynserv.com
celmvuqkwkn.dynserv.com
cfrntdejpqz.dynserv.com
ciwsdmi.dynserv.com

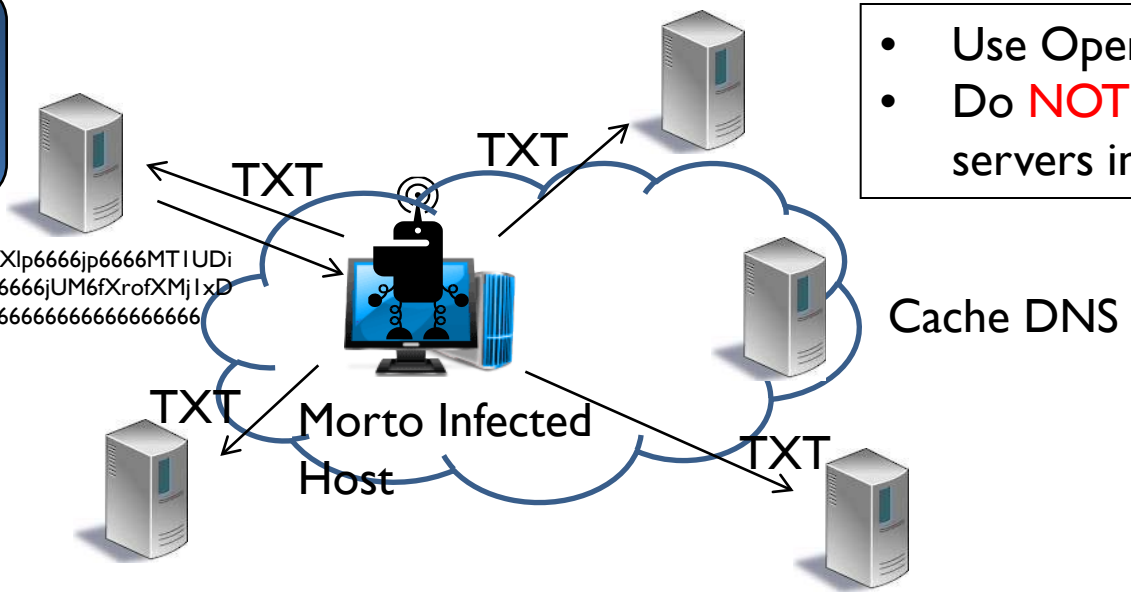
[8] Manos Antonakakis, Roberto Perdisci, Yacin Nadji, Nikolaos Vasiloglou, Saeed Abu-Nimeh, Wenke Lee and David Dagon "From Throw-Away Traffic to Bots: Detecting the Rise of DGA-Based Malware" Usenix 2012, 21st , p.491-506 2012-08-10

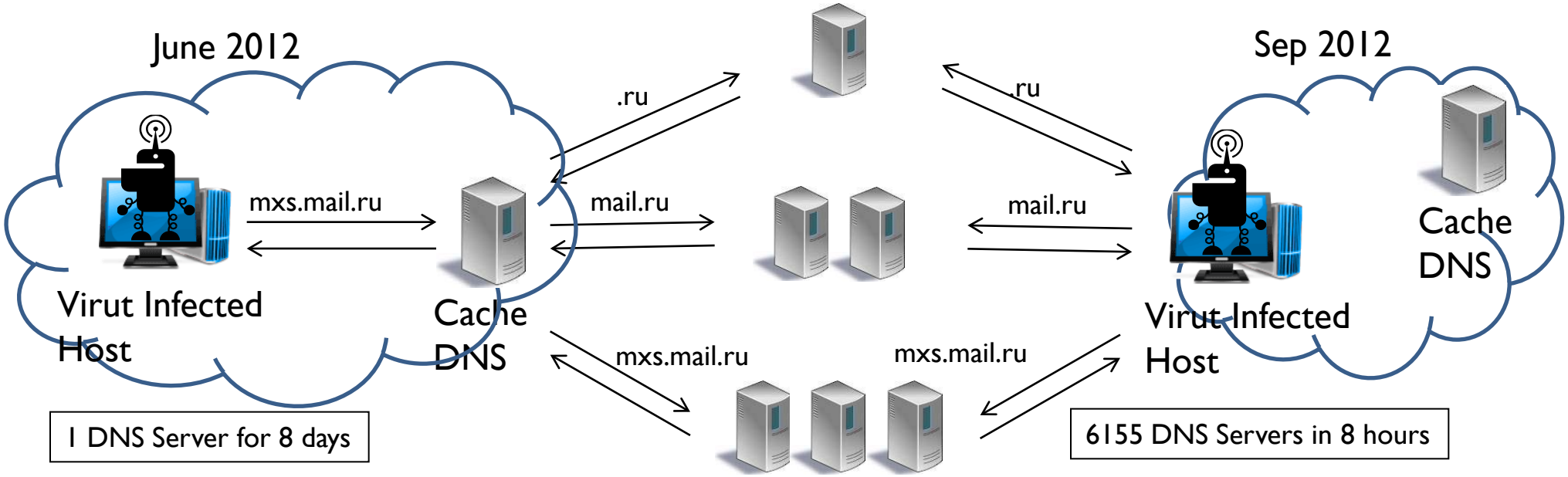

2012/06/XX XX:37:00
x.x.165.253
x.x.56.43
x.x.145.55
x.x.144.140
x.x.77.76
x.x.161.185
x.x.229.243
x.x.23.225
x.x.82.159
x.x.246.120
x.x.219.219
x.x.109.222
x.x.11.176
x.x.74.14
x.x.14.49
x.x.159.176
143.215.130.33
143.215.143.11
149.20.56.32
149.20.56.33
149.20.56.34

Escaping from Detection at Local Cache DNS server

See Morto DNS queries to Open DNS

- Use Open Resolvers
- Do NOT use default DNS servers in the Network





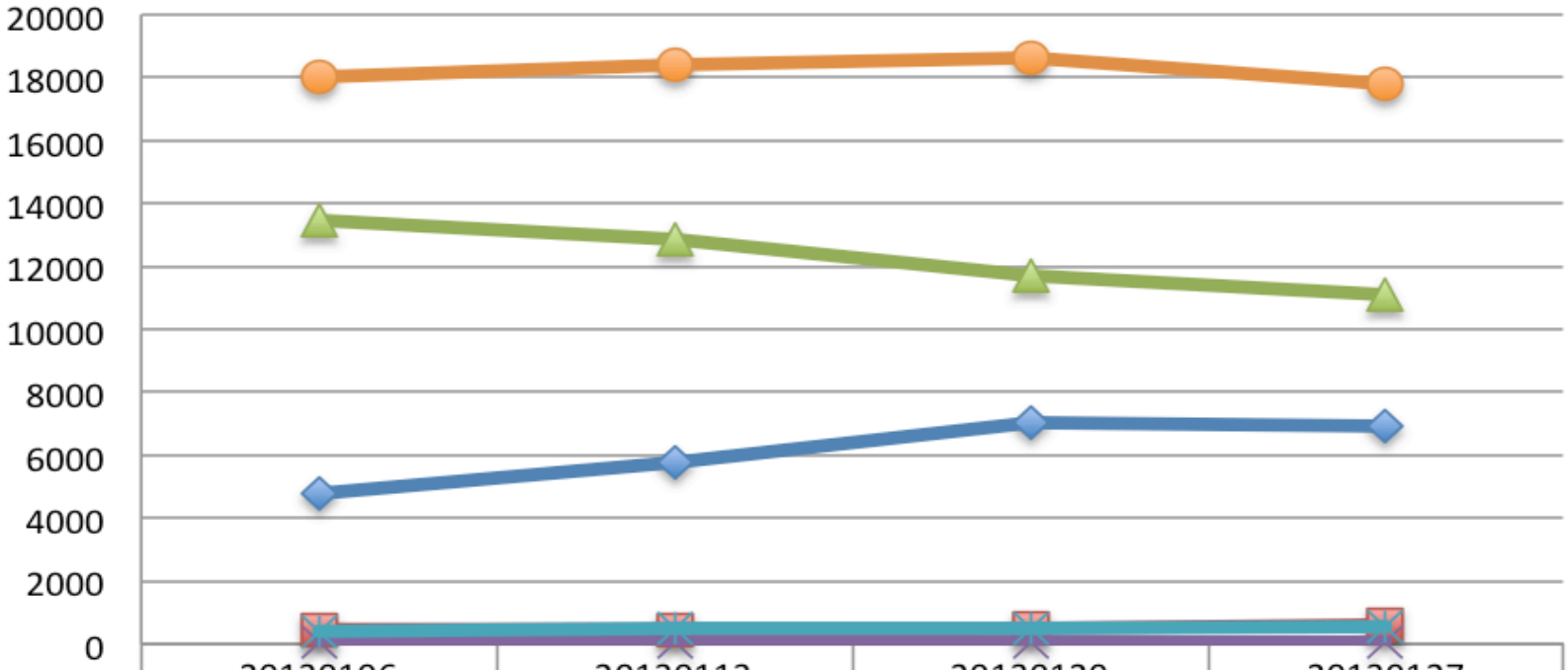
Morto DNS queries

Queries	query type	domain name
1	A	wpad.
47	A	d.ppiftns.in.
16	A	ppift.vb.cn8u.cn.
6	A	www.google.com.
27	TXT	e.ppiftns.in.
162	TXT	fd1.ppiplg.com.
247	TXT	e.ppift.com.
68	TXT	e.ppift.net.
18	TXT	fd2.ppiplg.com.
29	TXT	e.ppift.in.

Open DNS used by Morto

	154.70.1		141.192.60
	154.70.22		67.220.123
	154.71.1		67.220.220
	154.71.22		67.222.123
	180.96.54		67.222.222
	95.1.1		166.160.36
	95.192.1		141.112.163
	211.253.2		196.3.183
	2.0.20		220.163.82
	175.39.39		199.54.9
	153.192.1		250.36.130
	153.194.1		.1
	138.103.100		.2
	138.96.2		9.140.194
	146.237.237		44.127.16
	236.43.5		8.200.200
	248.252.2		.4
	171.2.65		.8
	171.3.65		91.109.10
	210.42.205		85.53.4

Number of Morto-Infected Hosts Detected at Open DNS in Jan 2013



	20130106	20130113	20130120	20130127
.jfrmt.	4769	5792	7052	6944
.jiafr.	462	464	513	599
.jifr.	13466	12869	11711	11094
.qfsl.	68	58	58	59
f1.fku*	401	473	510	575
ALL	18019	18433	18610	17790

DNS sensors + Other sensors

- Darknet
  - Scans and back scatters
- (Server/Client)Honeypot
  - Remote exploits
  - Drive-by-download
- Real traffic from backbone NW
  - DDoS (Syn flood, DNS Amp, L7-DDoS)
  - P2P-based Botnet (Zero Access, etc)

DNS sensors + Darknet sensors

- Morto is known to randomly access remote hosts on port 3389/tcp (thus detectable on darknet)
- We matched infected hosts from DNS data with ones accessing darknet on 3389/tcp

<June, 2012>
4-day darknet: 60,153 hosts
1-hour DNS: 23,518 hosts
Matched hosts: 16202 hosts (68.8%)

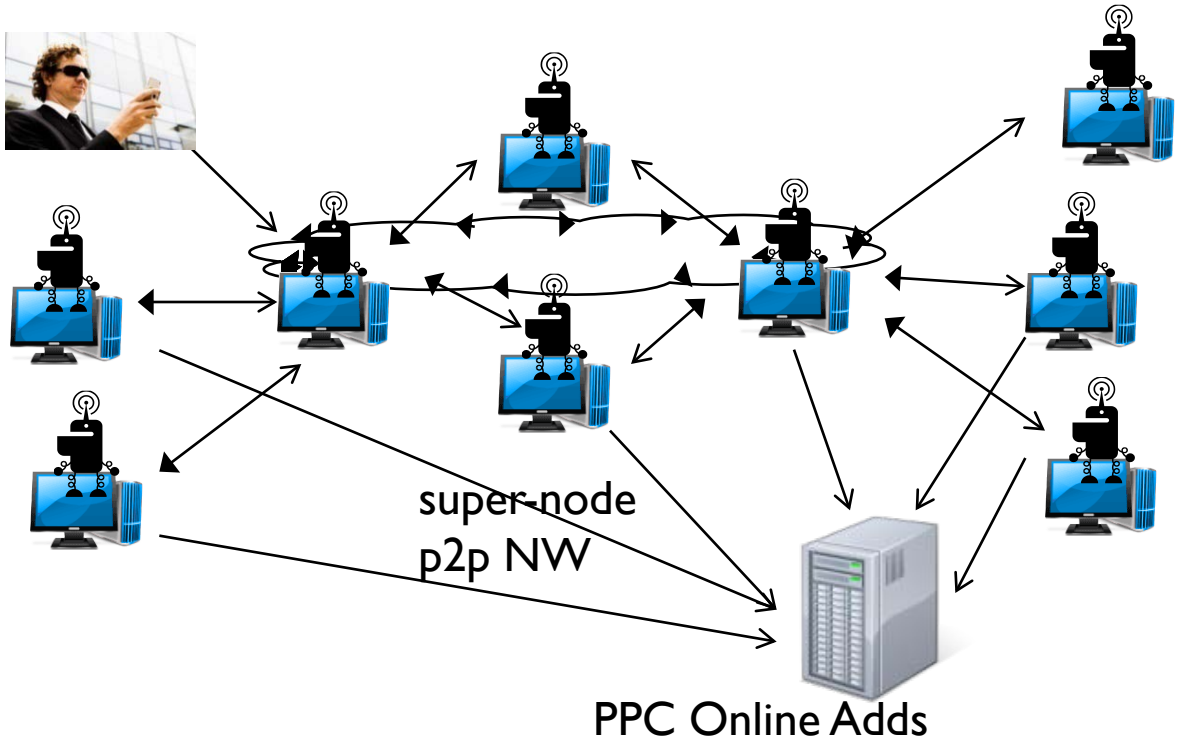
<March, 2012>
1-day darknet: 20,065 hosts
4-hour DNS: 63,921 hosts
Matched hosts: 13,653 hosts (68.0%)

DNS sensors + Other sensors

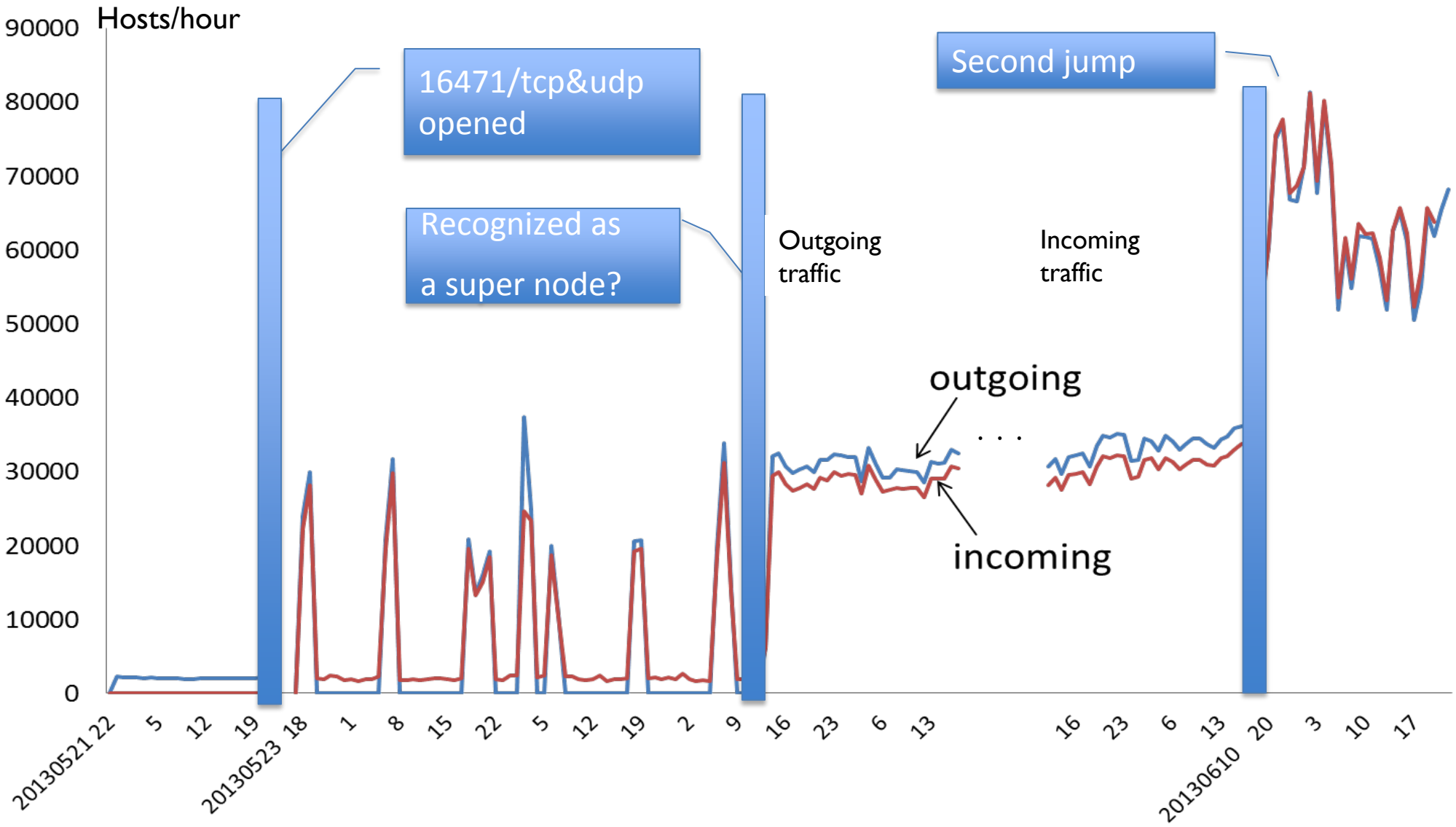
- Darknet
  - Scans and back scatters
- (Server/Client)Honeypot
  - Remote exploits
  - Drive-by-download
- Real traffic from backbone NW
  - DDoS (Syn flood, DNS Amp, L7-DDoS)
  - P2P-based Botnet (Zero Access, etc)

Zero Access: Huge P2P botnet

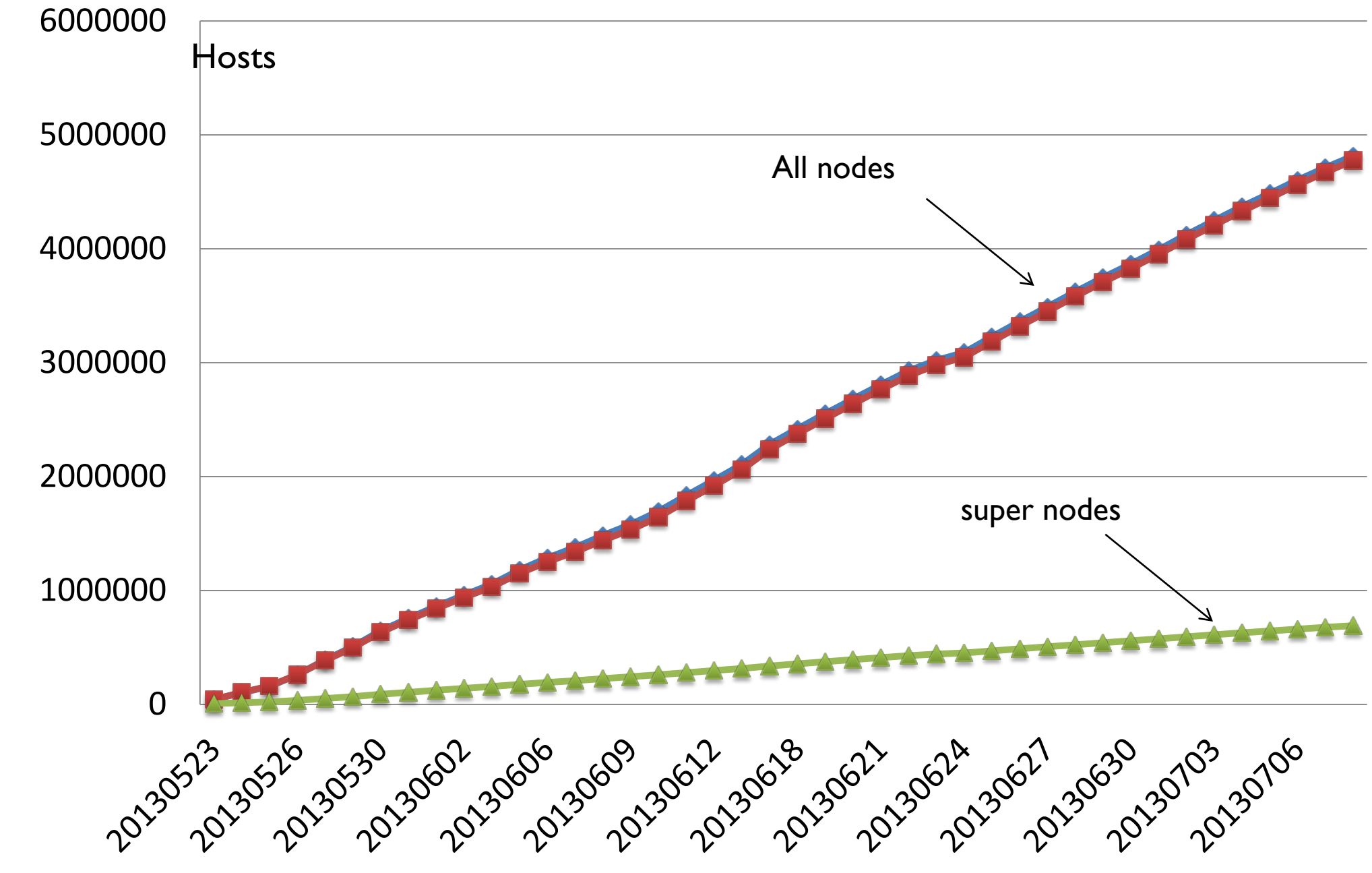
- Zero Access is a P2P botnet known to consist of a few millions of infected hosts over world
- Exchange commands, infected IP lists, and plug-in files through its own P2P network (thus, undetectable by darknet nor DNS)
- Reported to make140M ad-clicks/day, earn up to $1M/day (From Kindsight's report at RSA Conference 2013)



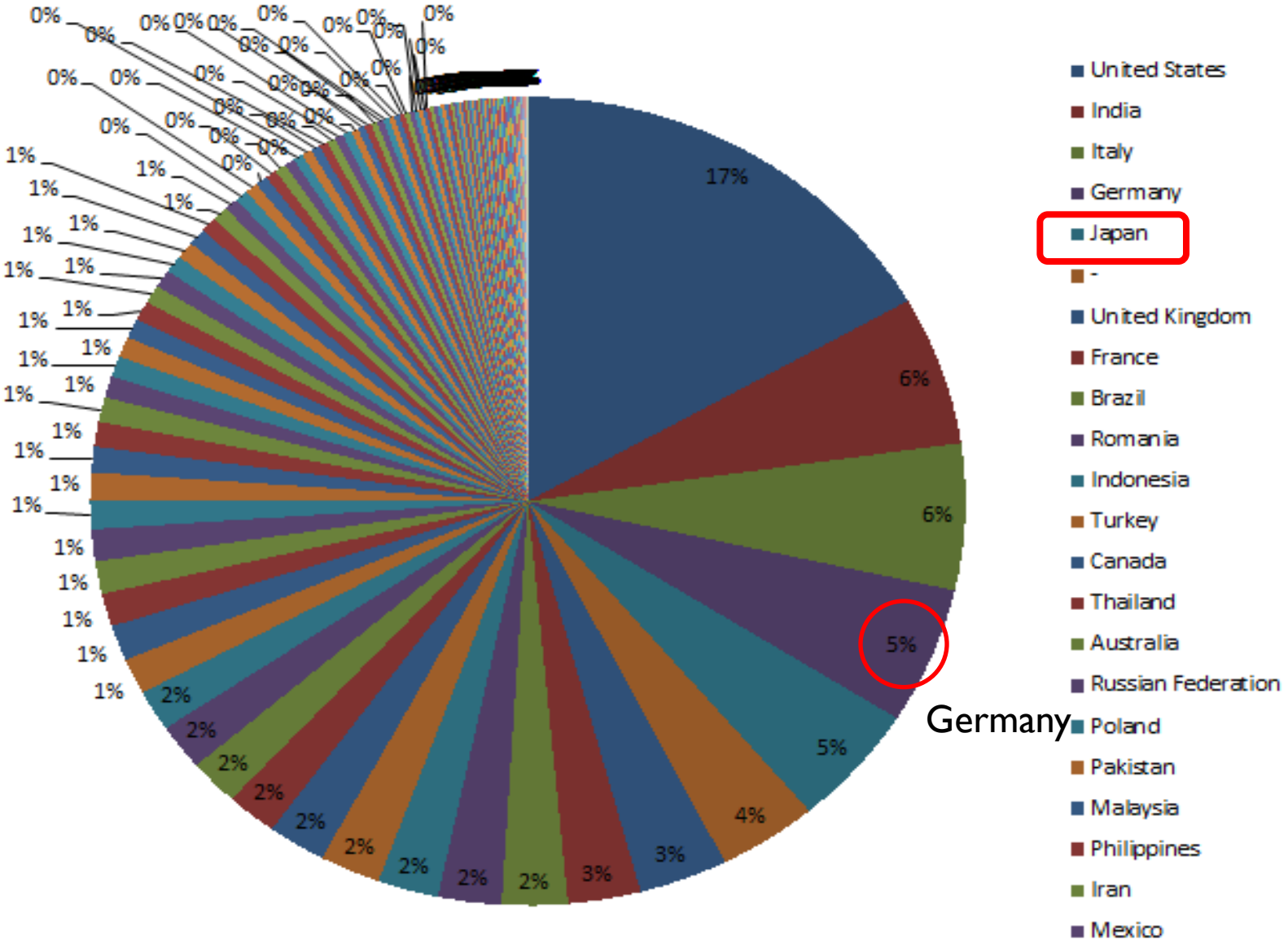
Monitoring P2P communication(16471/tcp, 16471/udp) of Zero Access in Sandbox



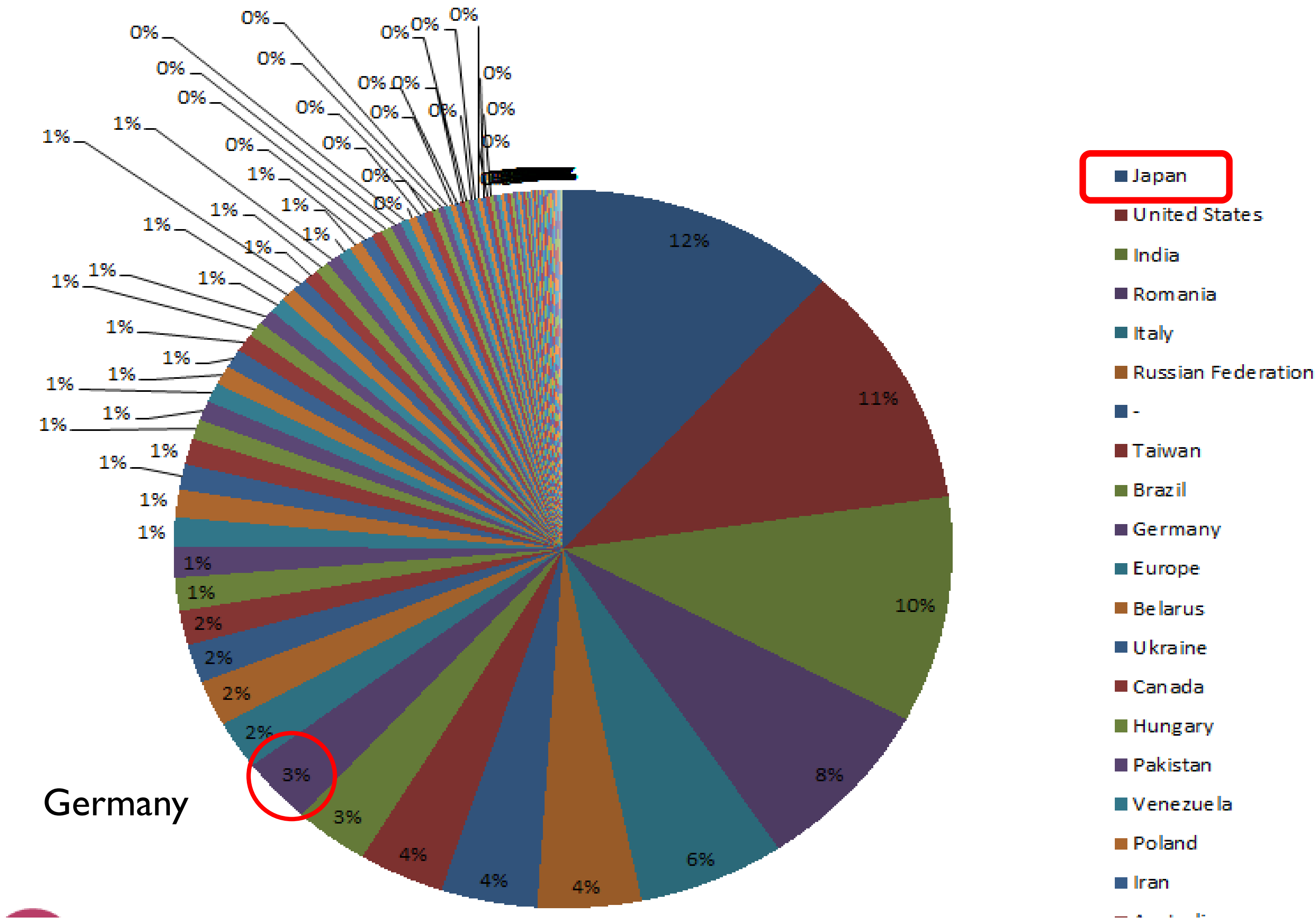
Total # of hosts suspected to be infected



Geographic locations of regular nodes



Geographic locations of super nodes

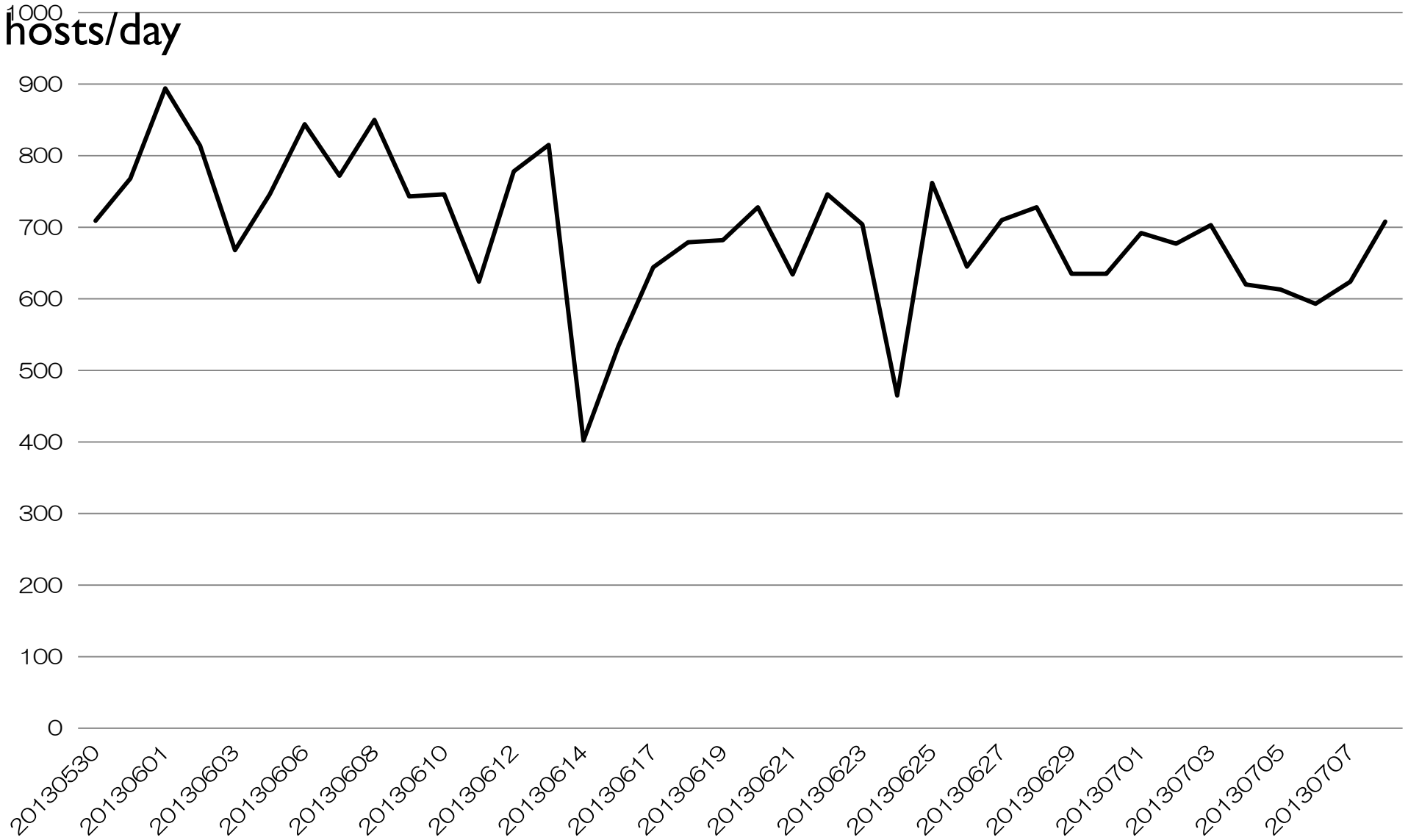


Sandbox Monitoring + Backbone traffic

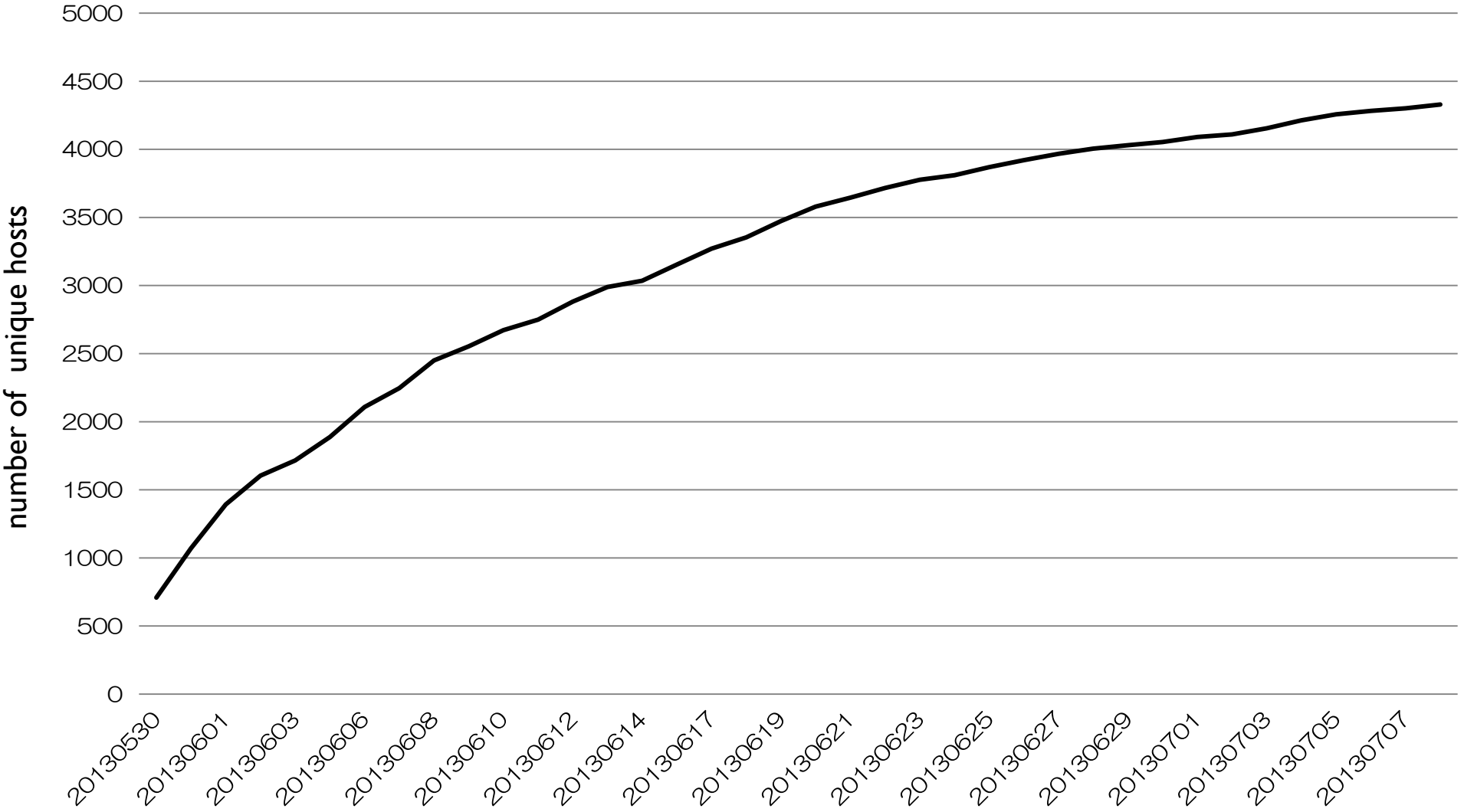
Matched with backbone traffic on 2013/4/23

Ports	# hosts(src+dst))
(src port 16470 or dst port 16470) and proto udp	29590
(src port 16471 or dst port 16471) and proto udp	56244
(src port 16468 or dst port 16468) and proto udp	1720
(src port 16472 or dst port 16472) and proto udp	849
(src port 16469 or dst port 16469) and proto udp	688
(src port 16473 or dst port 16473) and proto udp	656
(src port 16467 or dst port 16467) and proto udp	605
(src port 8080 or dst port 8080) and proto udp	13805
(src port 80 or dst port 80) and proto udp	17516
(src port 53 or dst port 53) and proto udp	822318
(src port 1935 or dst port 1935) and proto udp	722
(src port 6667 or dst port 6667) and proto udp	1153

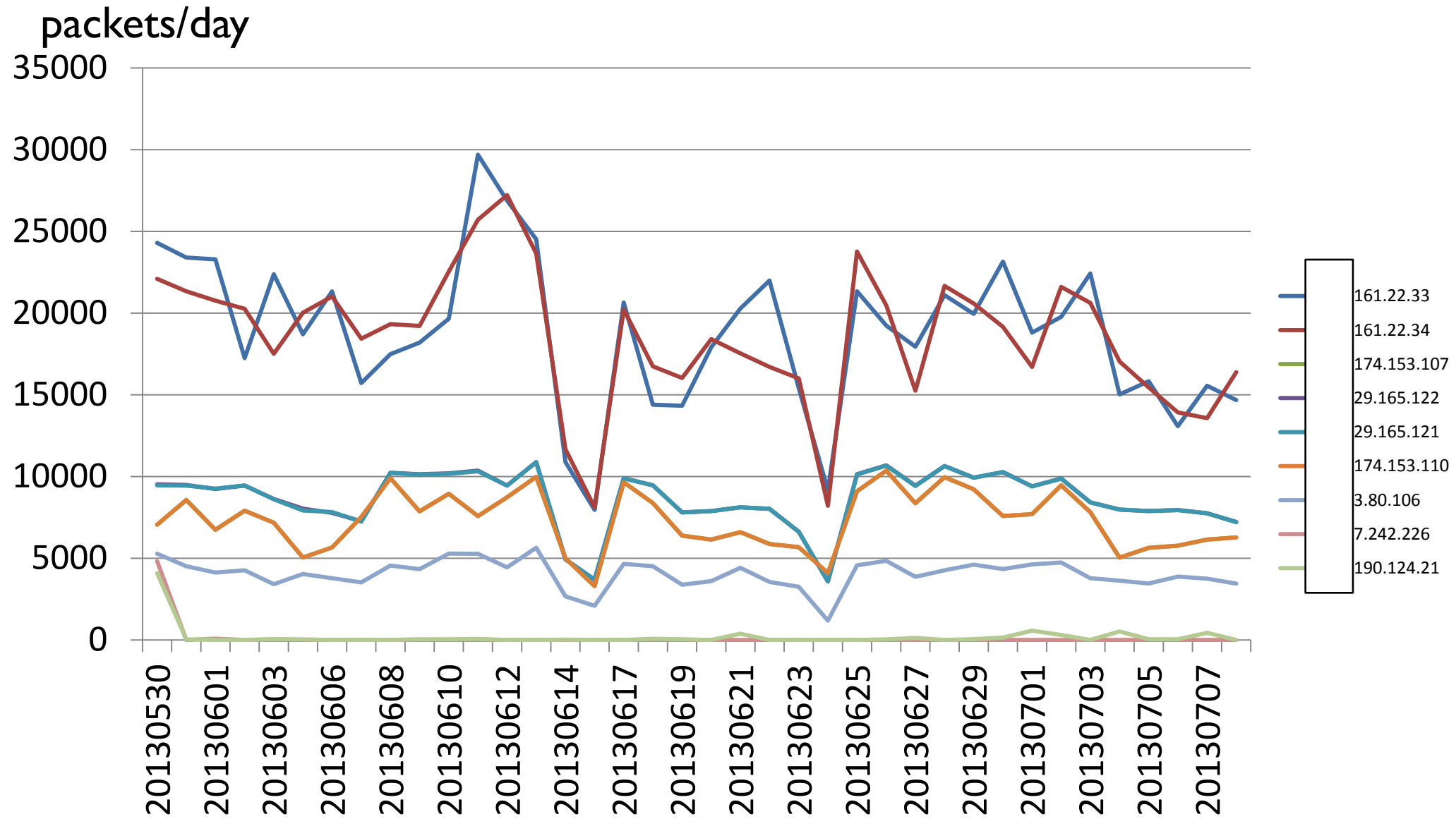
Observed Pay-Per-Click(80/tcp) from single ZeroAccess-infected host in sandbox



Total number of PPC targets



Heavily clicked web sites (> 4000 pkts/day)



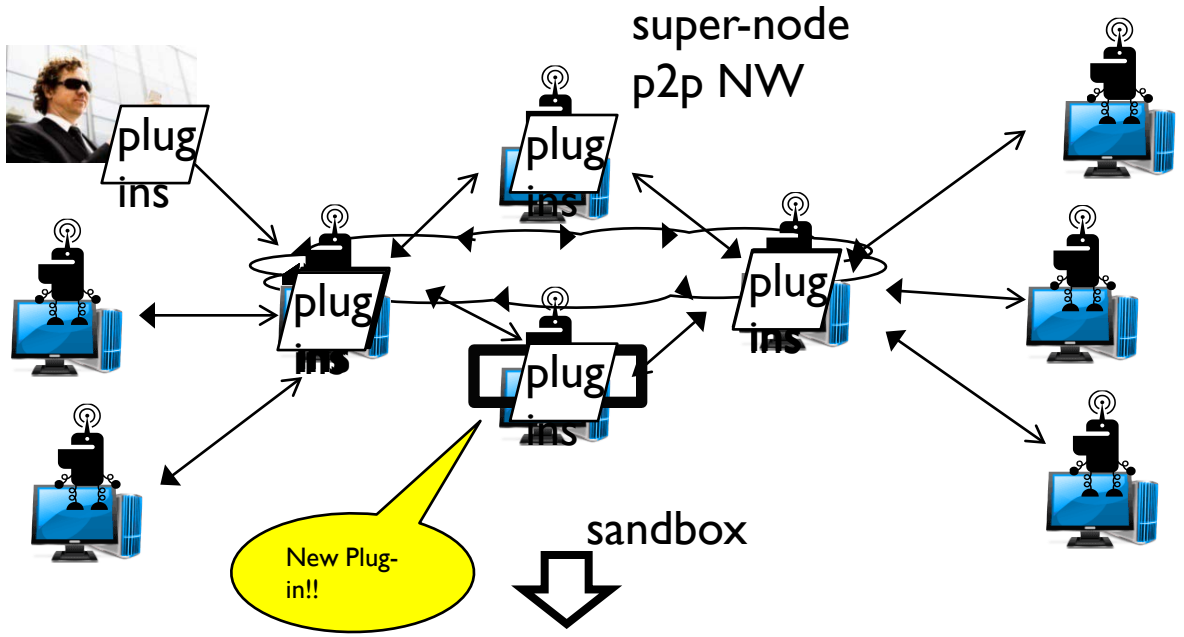
Heavily Clicked Web Site（20130530-20130708）

	1.22.33	Korea	om
	1.22.34	Korea	om
	4.153.107	United States	
	.165.122	Ukraine	
	.165.121	Ukraine	
	4.153.110	United States	
	30.106	United States	
	242.226	United States	rse.softlayer.com
	0.124.21	Hong Kong	
	.55.13	United States	om
	9.145.163	-	
	.45.163	United States	
	8.241.155	United Kingdom	
	.55.12	United States	om
	39.76	United States	c.akamaitechnologies.com
	.216.55	United States	
	.30.200	United States	tnoc.net
	.237.229	United States	static.akamaitechnologies.com

We are now matching with DNS queries for these sites.

Monitoring/analysis of ZeroAccess Plug-ins

The attacker can update Zero Access functionality by sending plug-ins (DLL) through P2P NW.
We plan to detect the circulation of new plug-in and analyze its functionality for finding new attack vectors.



Dynamic Taint Analysis
Malware Fuzzing

Plug-in Analyzer

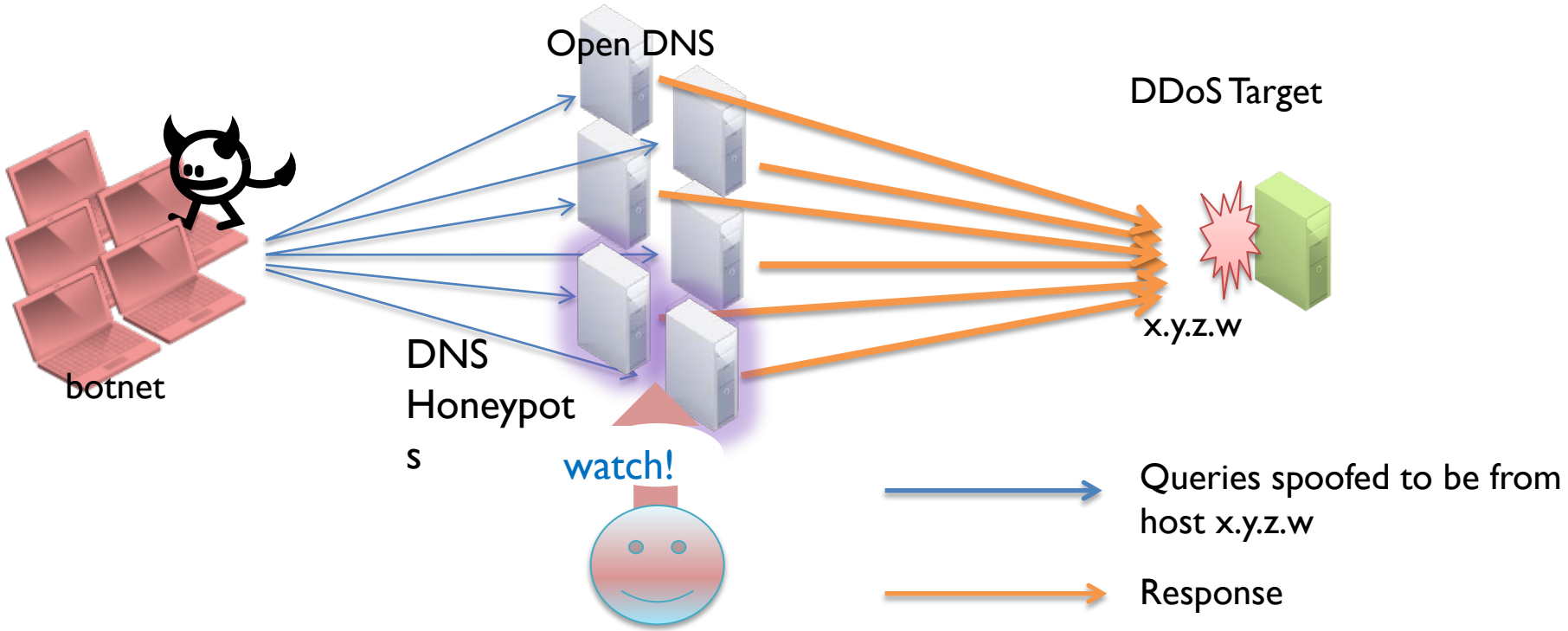
New Attack Vectors (e.g. DOS)

DNS sensors + Other sensors

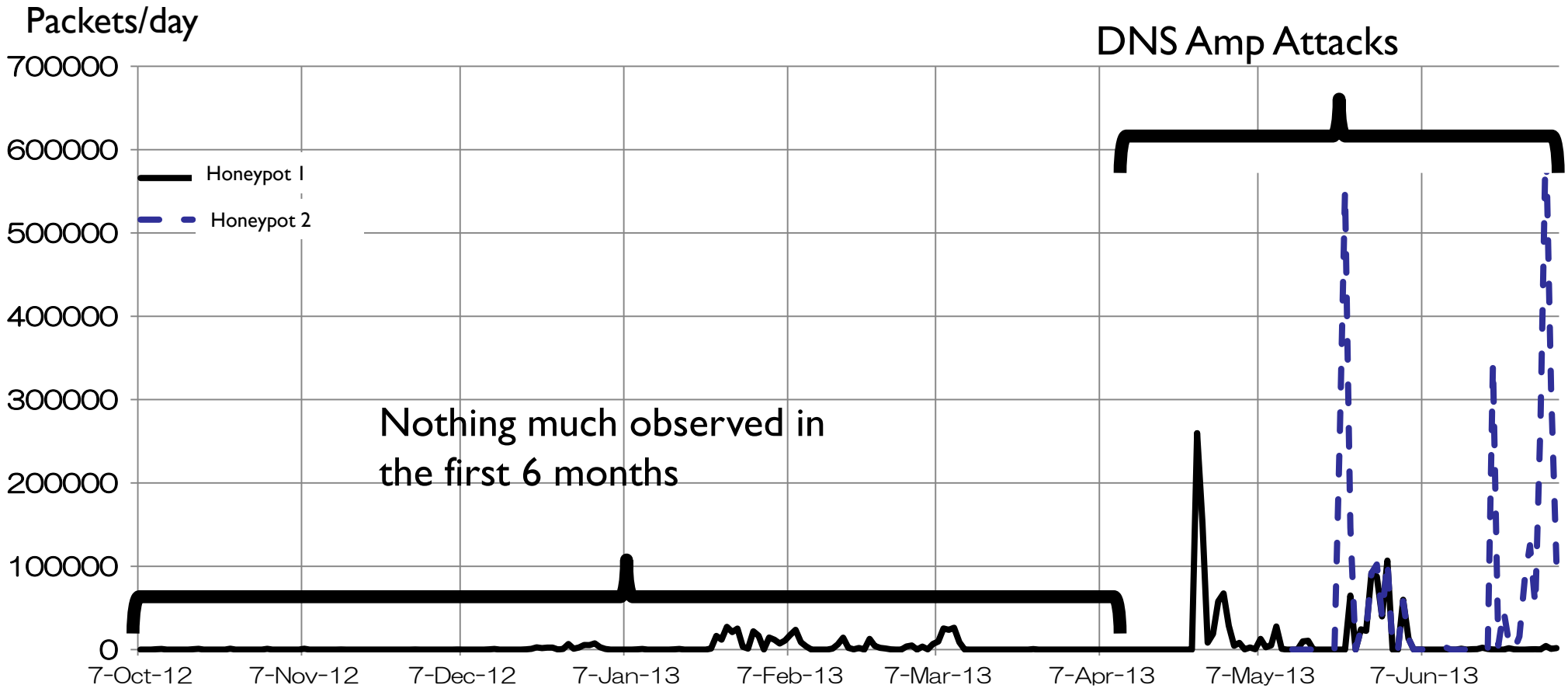
- Darknet
  - Scans and back scatters
- (Server/Client)Honeypot
  - Remote exploits
  - Drive-by-download
- Real traffic from backbone NW
  - DDoS (Syn flood, DNS Amp, L7-DDoS)
  - P2P-based Botnet (Zero Access, etc)

DNS Amplification Attack and DNS honeypot

- DDoS Attacks that misuse open DNS servers
- Bots send IP-spoofed queries to open DNS servers so that the spoofed host (DoS Target) receives amplified DNS responses
- We setup (open but bandwidth-controlled) DNS servers to monitor DNS AMP attacks



Attacks Observed by DNS Honeypots



	honeypot1 (261days)	honeypot2 (51days)
Total Queries	1,667,085	3,411,687
Source IPs of queries	1,129	565
Domains	1,136	80

Frequently queried domains

Honeypot1

Queries	Domain	Type
1,110,870	isc.org	ANY
405,441	ripe.net	ANY
32,196	www.2sf999.com	ANY
31,330	8845.582878.com	ANY
28,298	www.ntdtv.com	ANY

Honeypot2

Queries	Domain	Type
2,209,146	isc.org	ANY
899,334	ripe.net	ANY
382,190	www.58wgw.com	ANY
31,553	www.2sf999.com	ANY
31,187	8845.582878.com	ANY

Gains of Amplification (Observed on 2013/6/17)

Domain	Query size	Response Size※1	Gain※2
isc.org (ANY)	78byte	3,497byte	4483.3%
ripe.net (ANY)	79byte	2,882byte	3648.1%

※1 Maximum response size
※2 Gain = Response size/Query size×100 [%]

Honeypot vs backbone monitoring

We compare DoS alerts by honeypots and backbone monitoring (June 2013).

- 34 of 81 alerts by honeypots match with backbone alerts
- Honeypots detect DoS 4.5 mins on average earlier than backbone monitoring.
- Some alerts are remarkably earlier (10mins～1hour) than detected at backbone.
- Early alerts on watched IPs /domains (e.g. .gov) may be possible but false alerts need to be concerned.

DOS S (H						Start Time Difference (Mins)	End Time Difference (Mins)
201						-2	2
201						-2	-1
201						-1	-1
2013						-10	2
2013						-3	7
201						-2	4
201						-1	2
201						-2	1
201						-7	1
201						-3	6
2013						-2	-11
201						-2	-1
201						-1	-13
201						-2	0
2013						-2	-1
201						-2	0
201						-1	0
201						-1	-1
2013						-2	0
201						-2	6
2013						-3	0
201						-2	-1
2013						-3	3
2013						-6	0
201						-1	118
201						-2	-30
201						-12	-1
201						-2	0
2013						-1	0
2013/6/30 2:57	2013/6/30 3:01		178.33.194.25	2013/6/30 2:59	2013/6/30 3:02	-2	-1
2013/6/30 5:03	2013/6/30 5:13		178.33.194.25	2013/6/30 5:04	2013/6/30 5:12	-1	1
2013/6/30 6:52	2013/6/30 9:05		184.82.163.4	2013/6/30 7:51	2013/6/30 7:51	-59	74
2013/6/30 11:08	2013/6/30 11:31		89.47.182.207	2013/6/30 11:13	2013/6/30 11:31	-5	0
2013/6/30 9:16	2013/6/30 9:44		17.172.170.68	2013/6/30 9:18	2013/6/30 9:44	-2	0

Summary

- Our awareness on ongoing botnet activities has improved with following approaches:

- Long-term sandbox analysis of bot samples reveals their microscopic behavior (e.g. characteristic DNS queries) for detecting infected hosts as well as understanding the details of threats (e.g. Spam, PPC).

- Multiple sensors (cache DNS, darknet, livenet, and honeypots) are complementary to each other enabling us to grasp macroscopic picture of various botnet activities.

Sum of Approaches for Early Detection of Cyber Attacks

- Close monitoring of existing botnets
  - Increase of infected hosts
  - Change of functionality
    - Automated monitoring and analysis of Zero Access Plug-ins
- Early Warning of DDoS (DNS Amplification)
  - Trial using DNS Honeypots
- Early Warning of Worm Pandemic (Not explained today)
  - Case study of Conficker and Morto cases

Thank you for listening Q&A