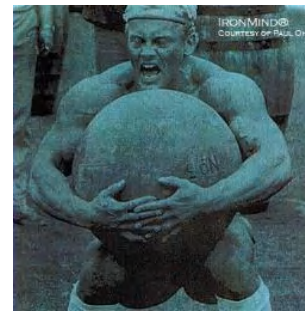


The power of the team work – Management of Dissecting Fast Flux Botnet “Unleashed”



@unixfreaxjp @DhiaLite



Outline

- Part 1
Monitoring Kelihos Fast Flux Botnet using
Recursive & Passive DNS
- Part 2
Analysis of Kelihos Weaknesses
- Part 3
Disclosure of the Actor's ID
- Part 4
Stopping the Payload Distribution

Monitoring Kelihos Fast Flux Botnet using Recursive & Passive DNS

- Real time Monitoring System
- Botnet geo distribution
- Botnet daily cycle
- OS distribution
- Daily detected domains
- Domains and IPs lifetime

Fast flux Monitoring System

Malware Must Die

While true

1. Select a seed of domains with a confirmed profile
2. Continuously milk domains for IPs
3. Continuously “inverse lookup” IPs in DNSDB, for new domains that start resolving to these IPs
4. Check detected domains for known profile (e.g. TTL, registration, existence of payload, etc)
5. Add new domains to the initial seed



Build seed domains list

Malware Must Die

- Resolve domains to IPs, TTL
- Resolve domains to NSs, TTL
- Build graph of domain, IP, NS
- Extract clusters of “same TTL domains”
- For each TTL cluster, extract largest connected component from domain, IP, NS graph

Kelihos FF domains

- Various gTLDs, ccTLDs, 1 single IP, TTL=0, hosted on Kelihos botnet IP pool (growing), infected individual machines, recent registration, delivering malware executables with known names
- Recorded case(s) of domain resolving to several IPs with TTL=600, cocala.asia, or TTL=300

Post-discovery checks

Malware Must Die

Exclude:

- Sinkholed domains
- Domains not matching sought after profile, e.g. higher TTL, not using botnet IP pool, shared hosting, old registration, not hosting malware payloads

Kelihos FF domains analysis Results

Kelihos

- Info-stealer
- Spam botnet
- P2P structure with fallback FF CnC domains
- Checks victim's IP against known CBLs, if not listed, victim's machine can be used as a proxy CnC, or spam bot

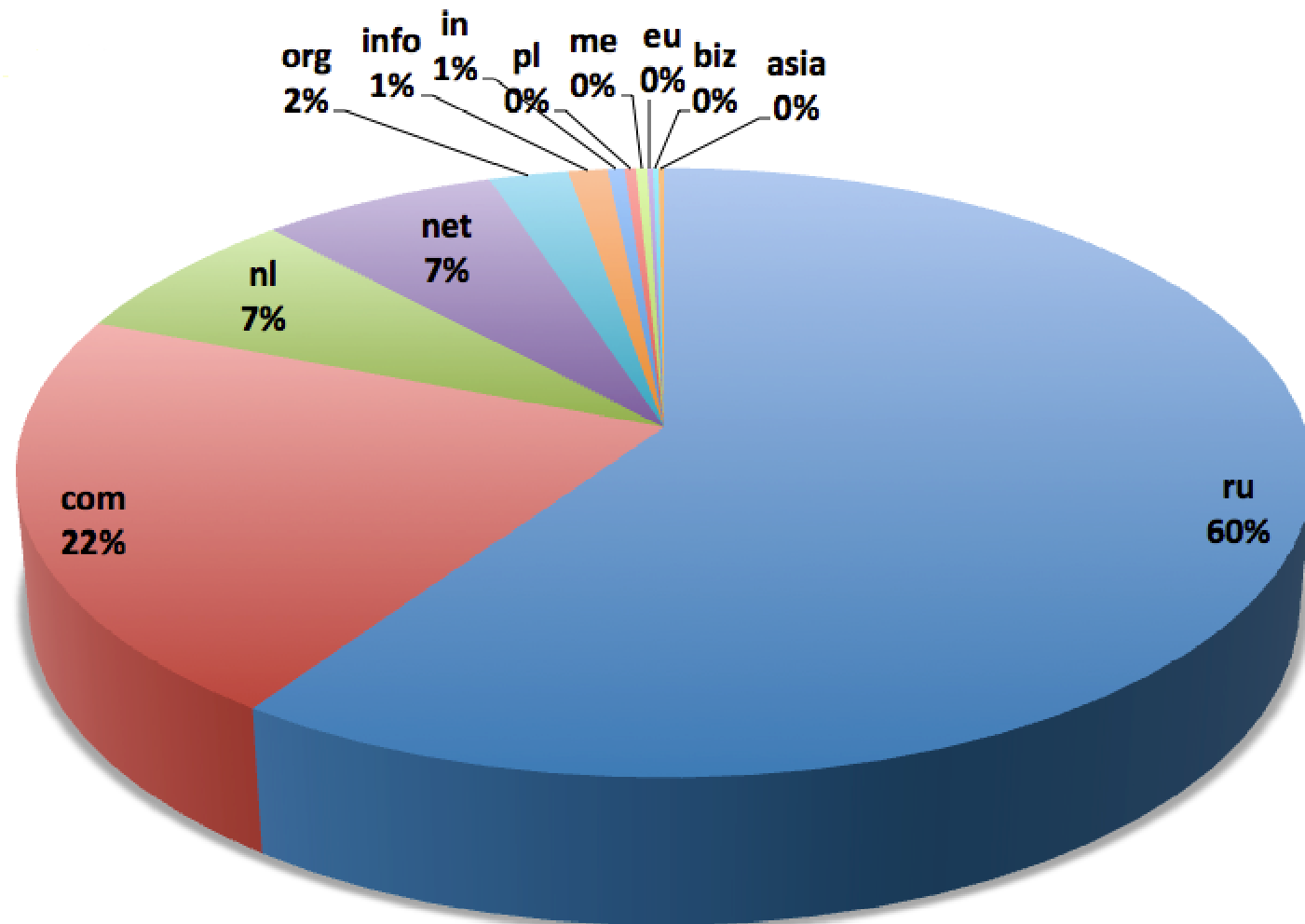


Kelihos

- Sample of 913 domains from the past 6 months



TLD distribution



TLD distribution

- Most abused registrars: bizcn, internet.bs, PDR LTD., 1API Gmbh, REGGI-REG-RIPN through resellers

Botnet Geo distribution

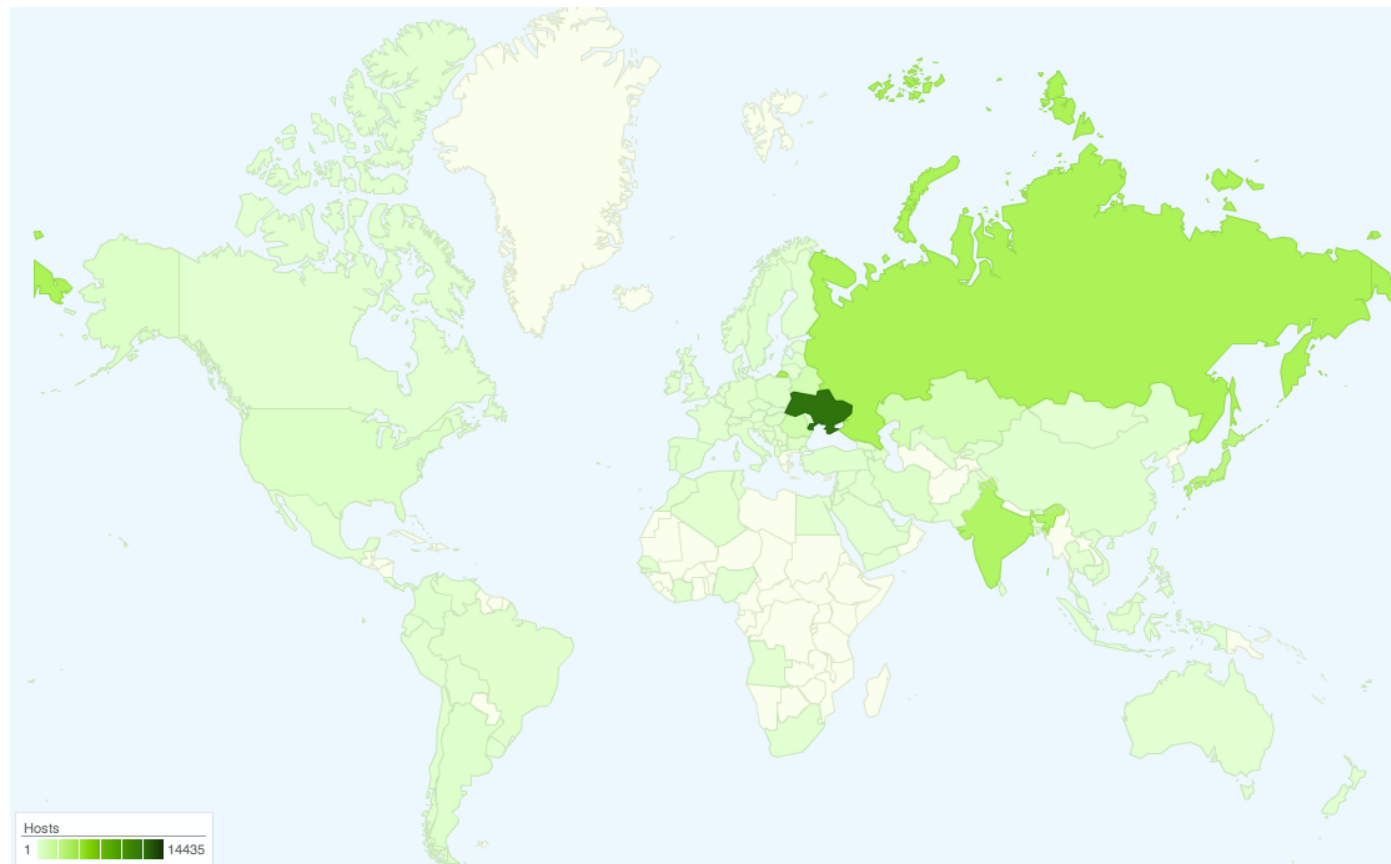
Malware **Must** Die

- Sample of 40418 alive IPs ->99 countries
- Up until early Dec 2013
- [Link to interactive map](#)



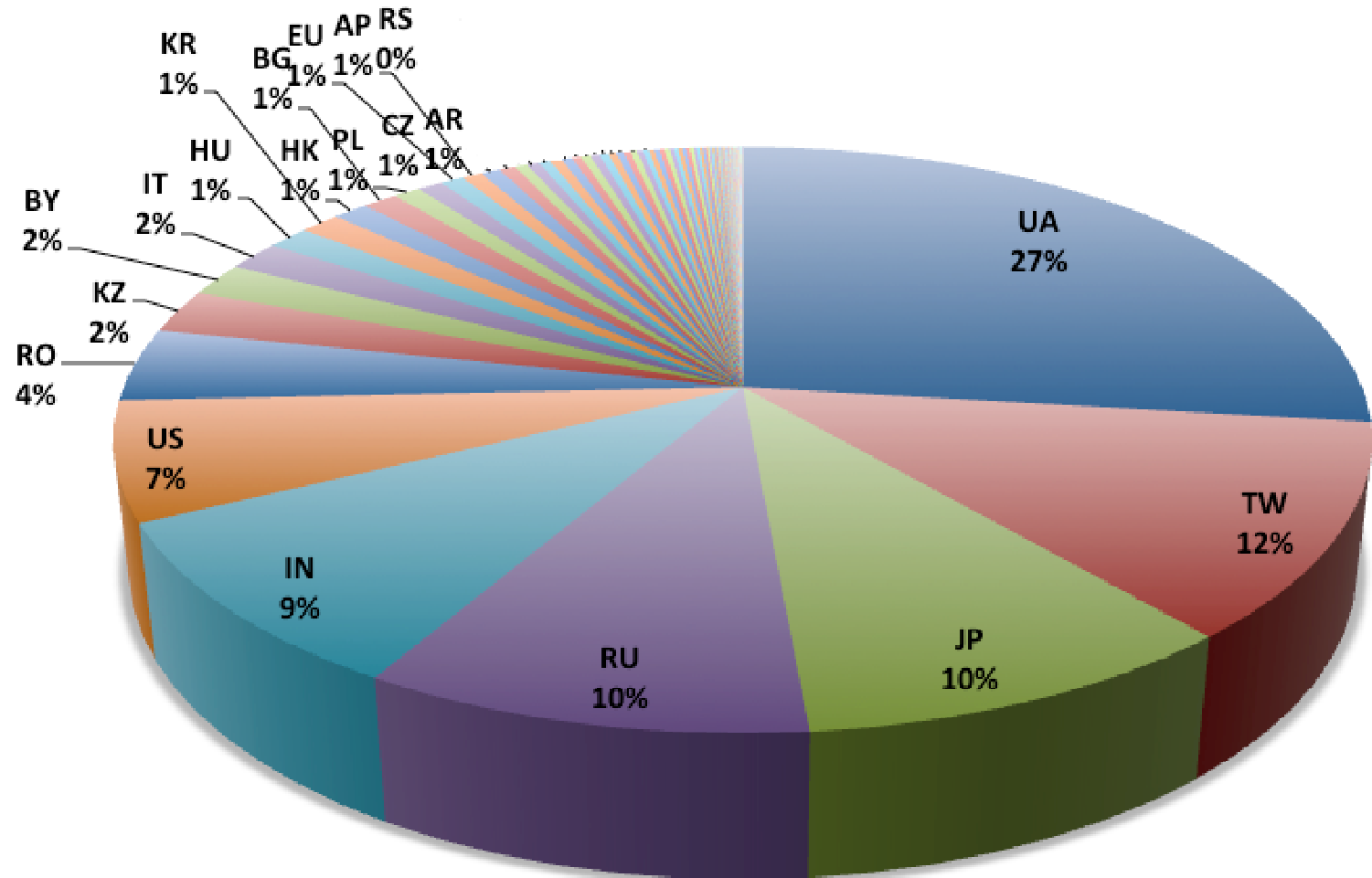
Botnet Geo distribution

~~Malware~~ **Must** ~~Die~~



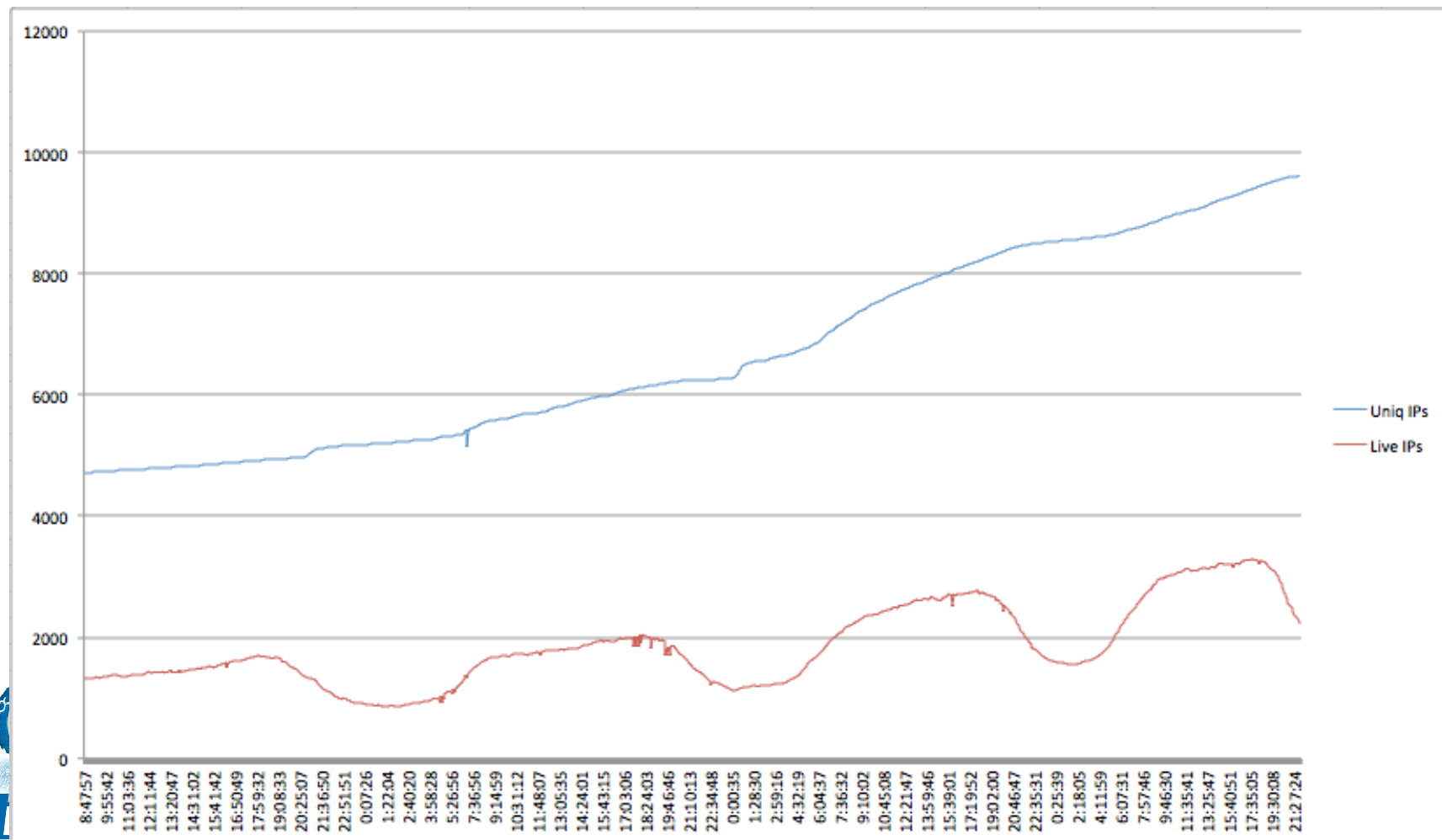
Botnet Geo distribution

~~Malware~~ **Must Die**



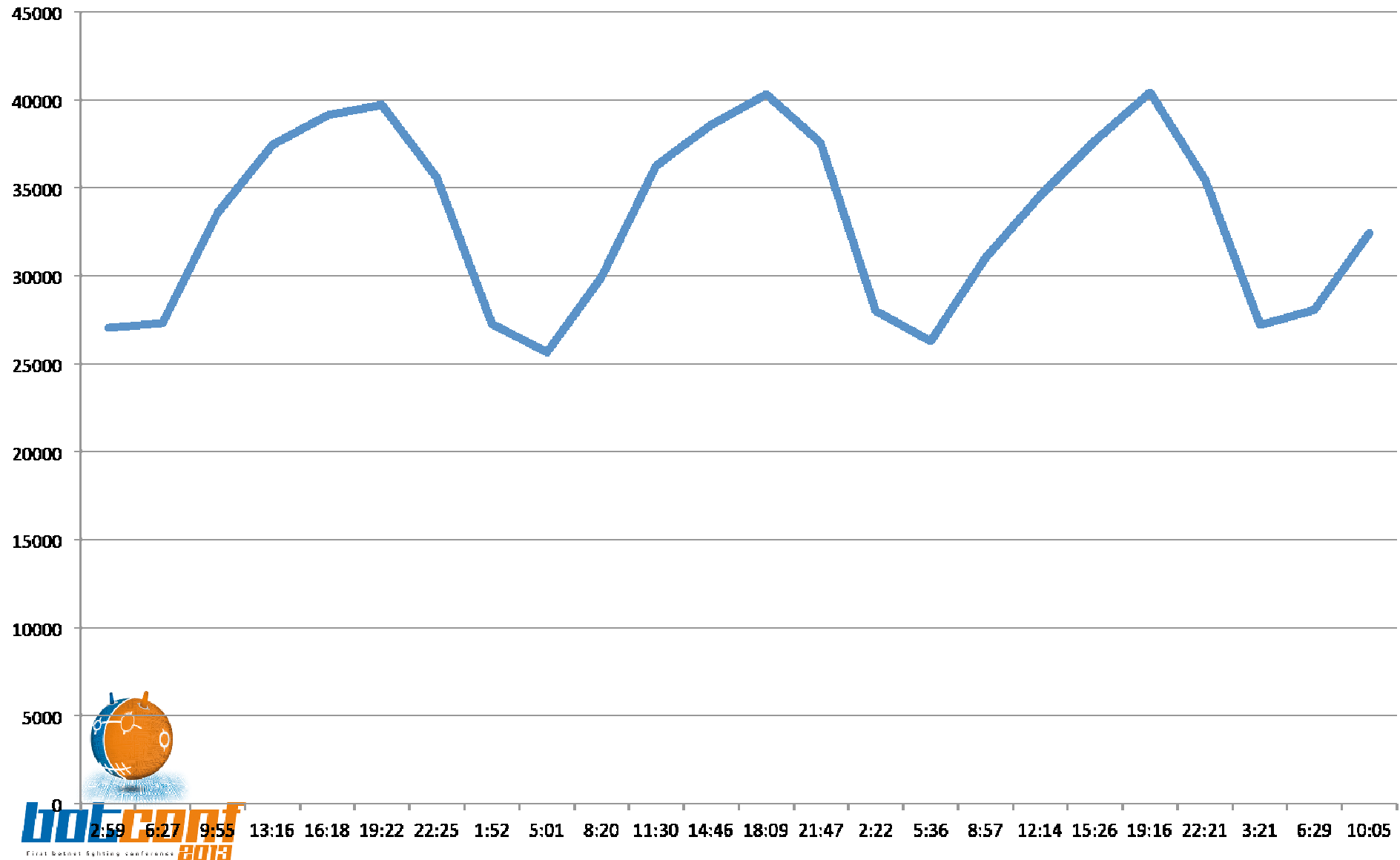
Botnet Daily Cycle

- Follows the daily cycle of Ukraine, Russia Time zone



Botnet Daily Cycle (Dec 2013)

Malware Must Die



botconf
2013
First Botnet Fighting Conference

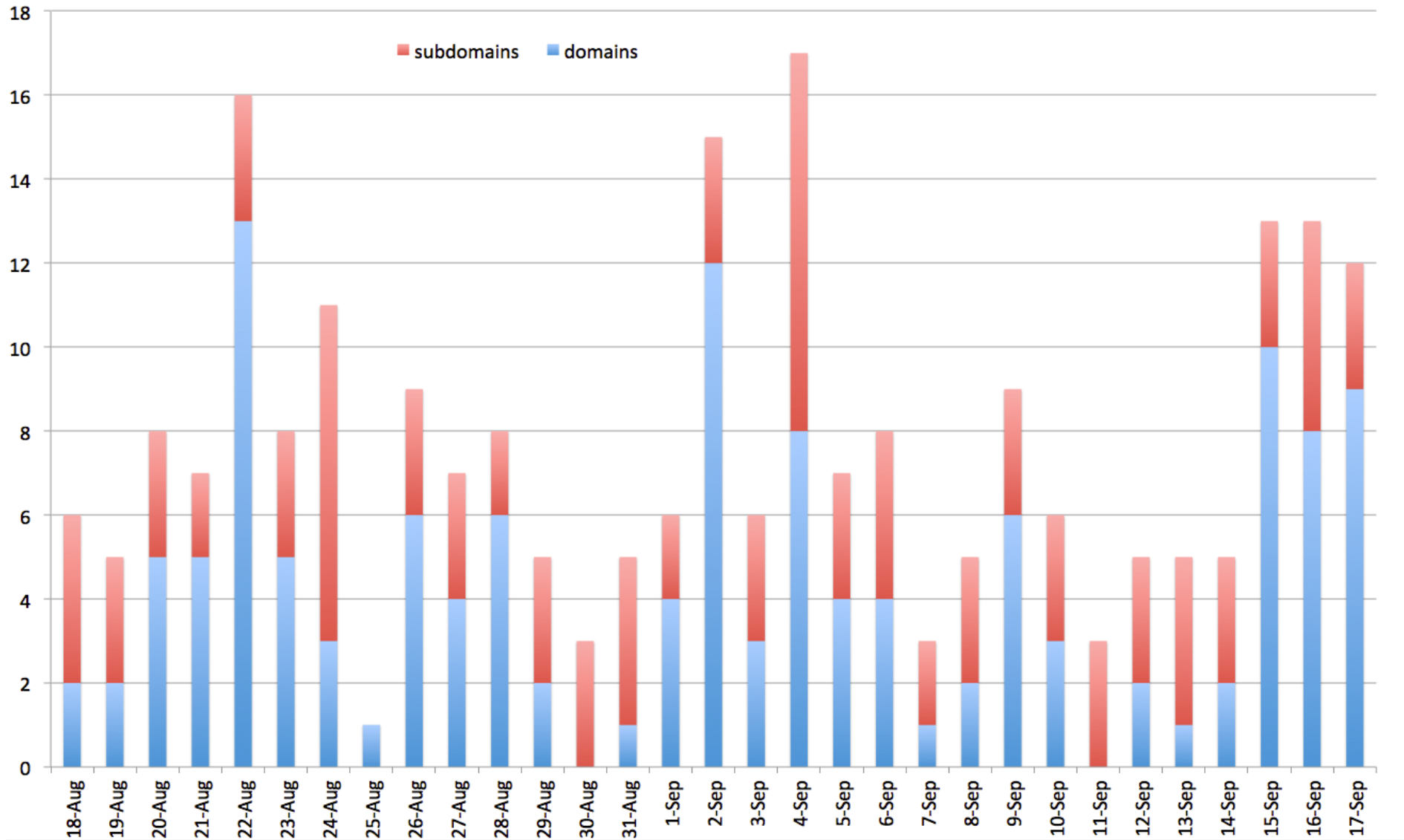
OS distribution

- 85% hosts running Windows XP or Vista
- 1/3 of them running Win XP PocketPC/CE
“nmap fingerprint”



Daily detected Kelihos domains

~~Malware~~ **Must Die**



Daily detected Kelihos domains

~~Malware~~ **Must Die**

- ns6.enjofyr.net
- agoe36yv.judnopem.nl
- akomn.insomtab.nl
- ayna.judnopem.nl
- hsej0rr7.insomtab.nl
- i0liq7i3.gewfywas.nl
- gyujsyi.ylahnel.net
- g12r5ea5.awbijis.net
- dy6gkkoi.ivynvov.net
- esp0t.ivynvov.net



Domains and IPs lifetime

Malware **Must** Die

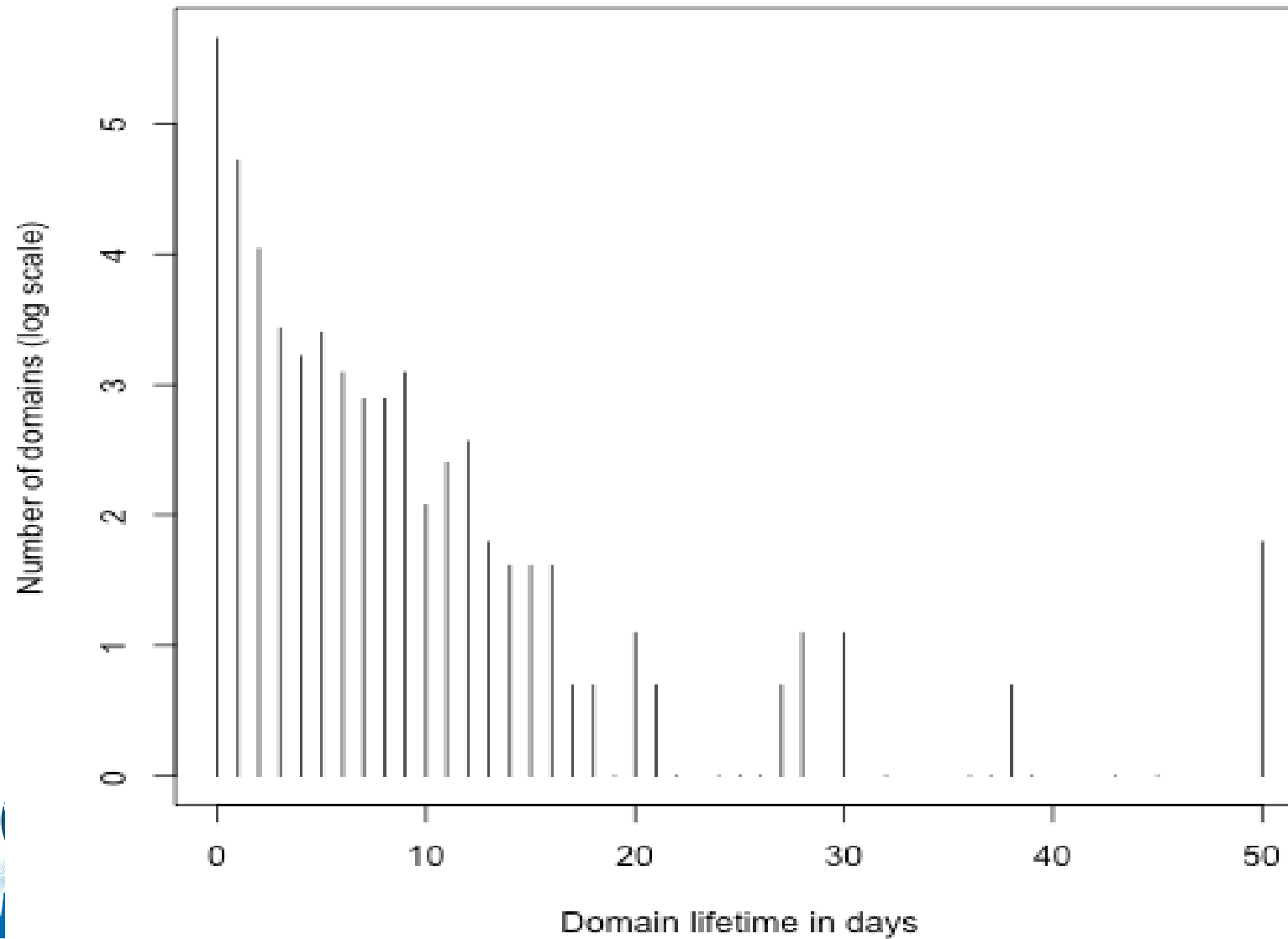
- Statistics on lifetime of domains and duration of usage of IPs in the botnet
- -> Efficiency of takedown, cleanup
- -> Efficiency of criminals' operation and botnet growth
- Case of “zombie” IPs, that serve in the botnet for a long time (months), never cleaned, residential, and also universities

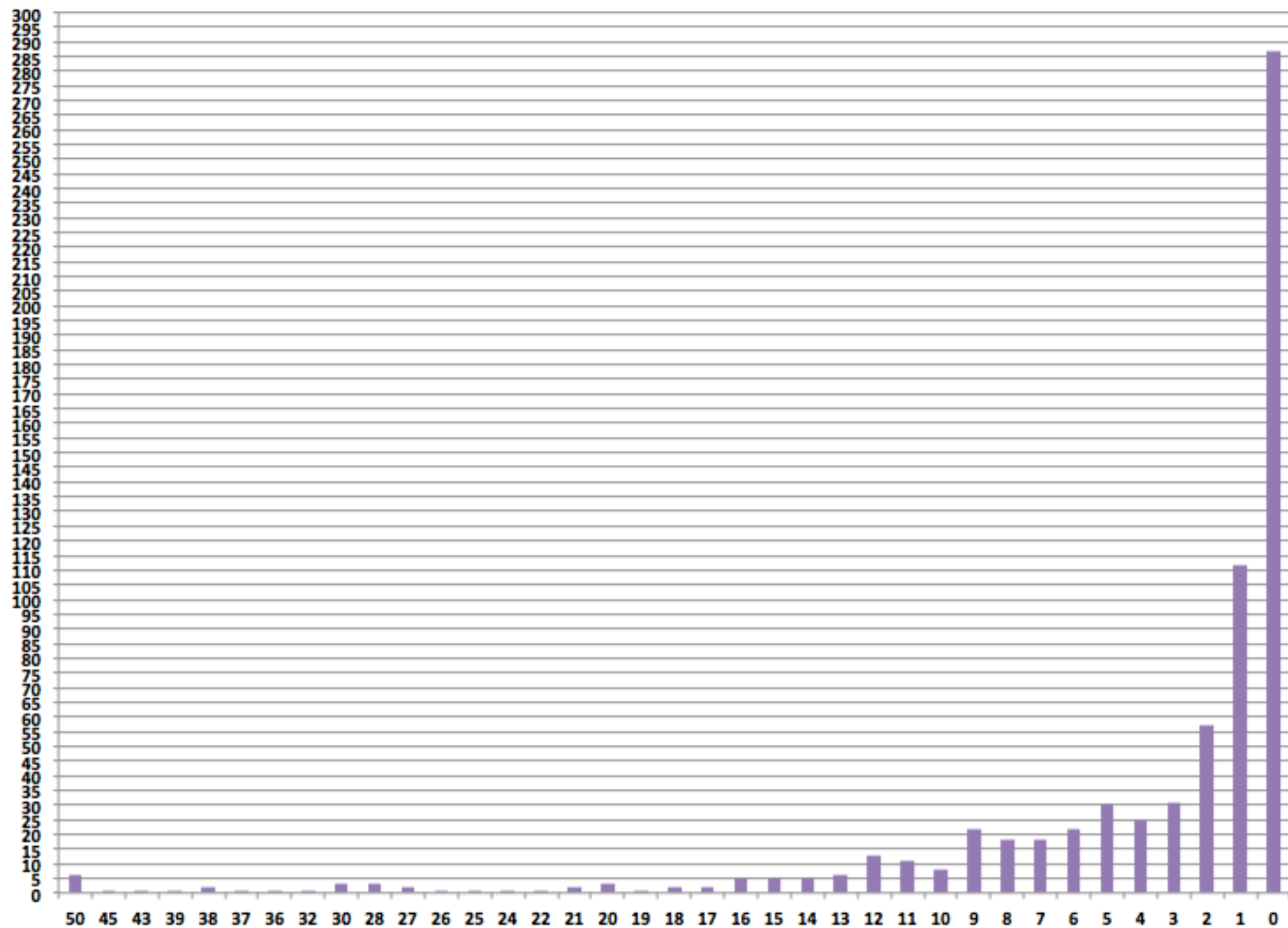
Domains' lifetime counts

Counts = $f(\text{domain lifetime in days})$

Sample size: 712 domains

Domain Lifetime Distribution



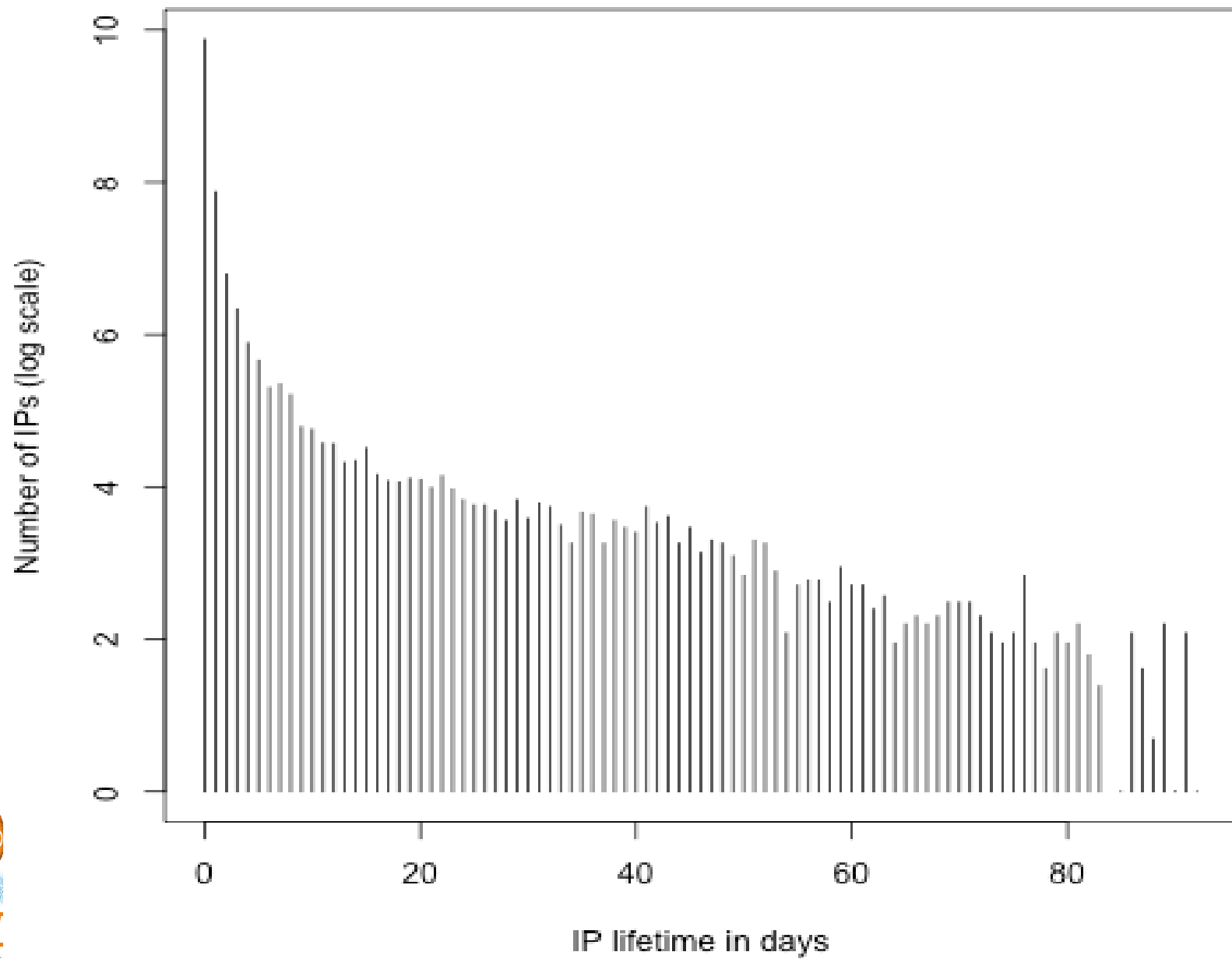


IPs' lifetime counts

Counts = $f(\text{IP lifetime in days})$

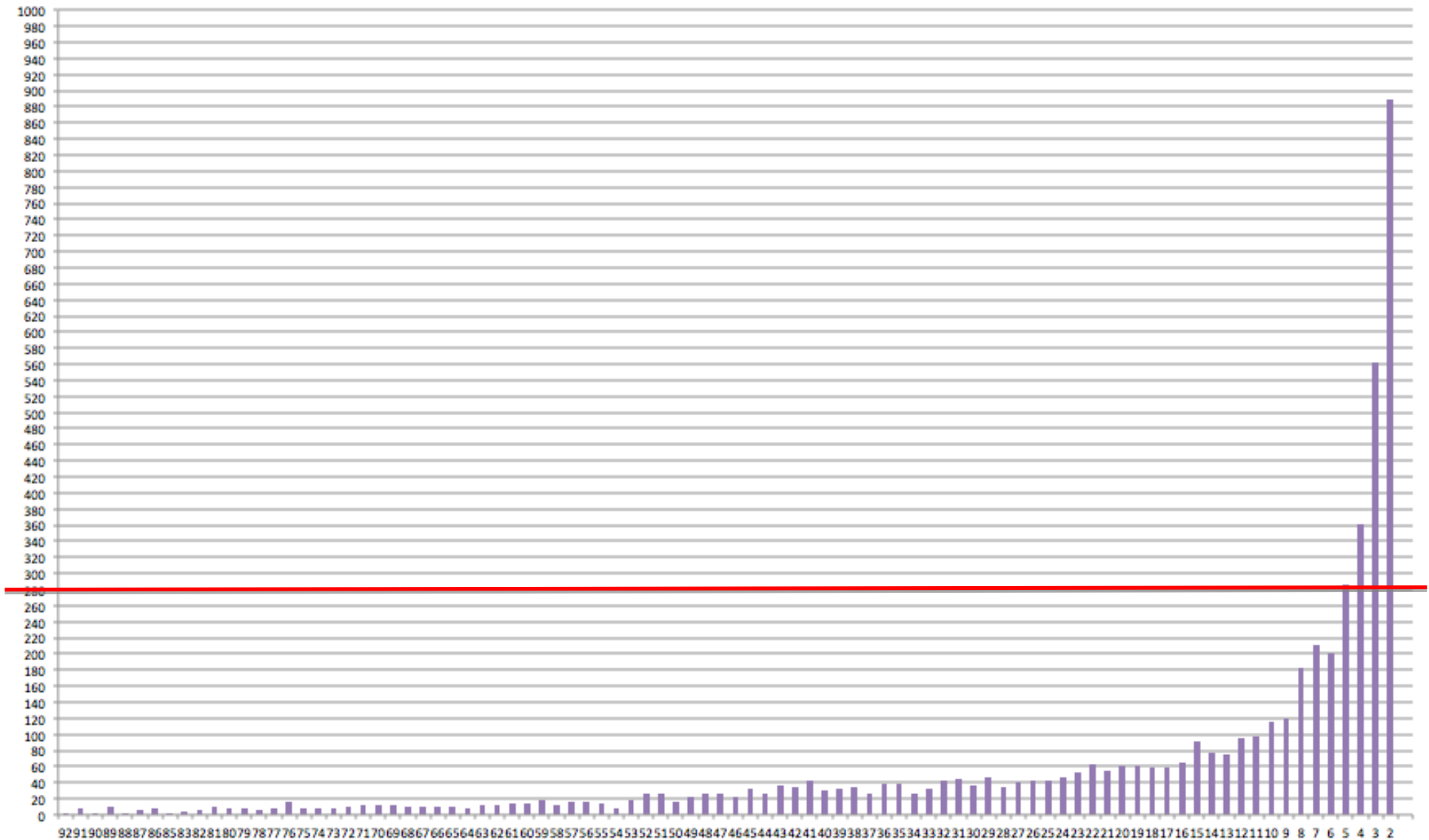
Sample size: 27,200+ IPs

IP Lifetime Distribution



Botnet's IPs lifetime

~~Maiware~~ **MustDie**



IPs' lifetime (cont'd)

Malware **Must** Die

- 2624 IPs lasted 1 day
- 19416 lasted less than a day

Botnet's IPs lifetime

Malware **Must** Die

- 110,000+ unique IPs collected over 5 months
- 11662 IPs have hosted domains



Analysis of the Botnet Weaknesses

Analysis for the weakness

- Infection Peer Scheme

The image shows a screenshot of an email client interface and the raw source code of the email. The email is from Bess Miles <peering@sewkis.com> with the subject 'Texas Explosion Injures Dozens'. A warning message is displayed: 'Be careful with this message. It contains a suspicious link that was used to steal people's personal information. Unless you trust the sender, don't click links or reply with personal information. Learn more'. The link provided is <http://94.28.49.130/news.html>.

The raw source code of the email is shown below, with various parts highlighted and annotated:

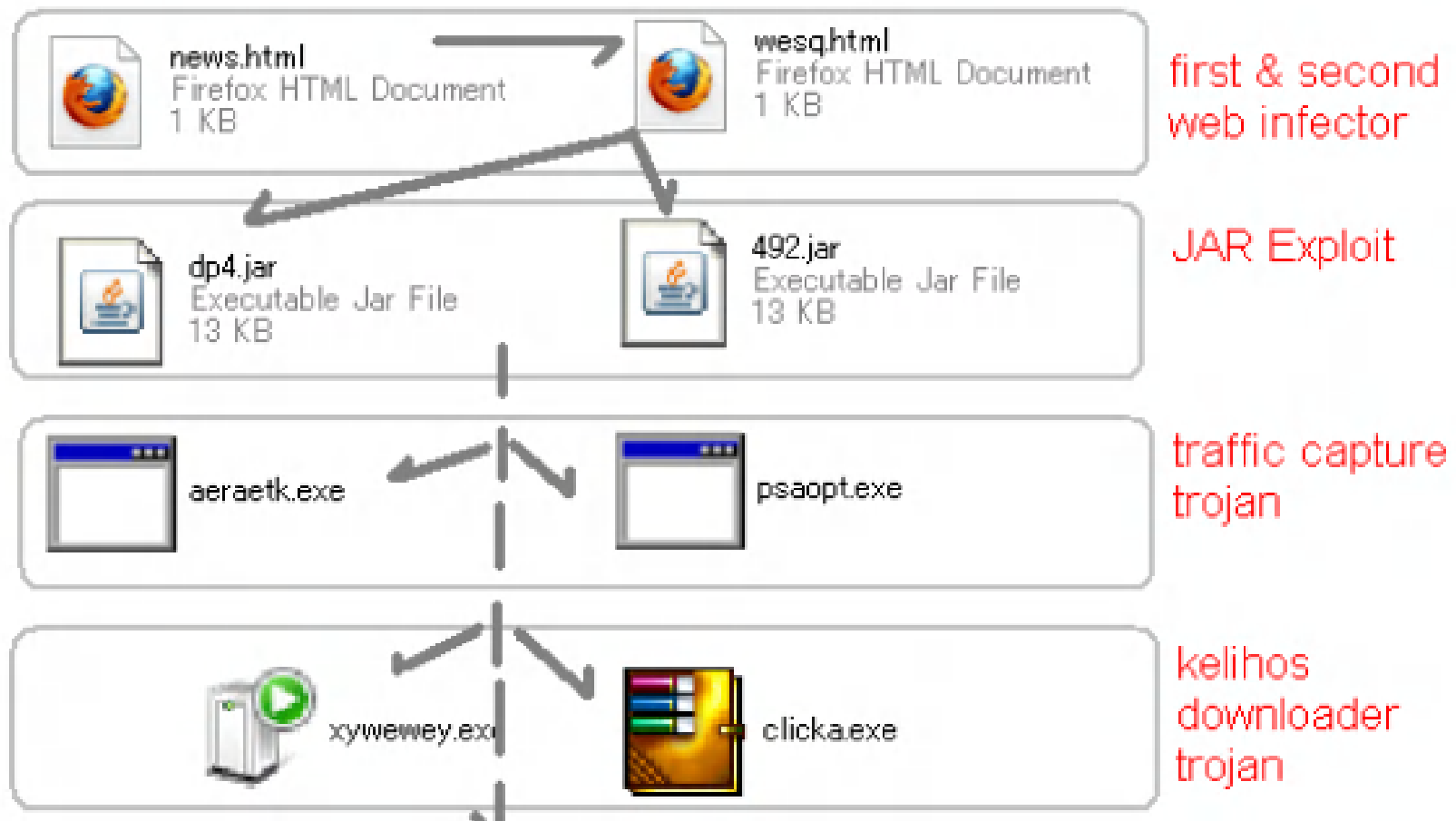
```
Return-Path: <peering@sewkis.com>
Received: from 37.45.155.190 ([37.45.145.201])
  by mx.google.com with SMTP [id oi2si5501238lab.8.2013.04.19.10.10.30;
  Fri, 19 Apr 2013 10:11:03 -0700 (PDT)]
Received-SPF: neutral (google.com: 37.45.145.201 is neither permitted nor denied by
  best guess record for domain of peering@sewkis.com) client-ip=37.45.145.201;
Authentication-Results: mx.google.com;
  spf=neutral (google.com: 37.45.145.201 is neither permitted nor denied by best
  guess record for domain of peering@sewkis.com) smtp.mail=peering@sewkis.com
Received: from unknown (HELO vt2jjg [149.47.158.222])
  by 37.45.145.201 with ESMTTP; Fri, 19 Apr 2013 20:14:15 +0300
Message-ID: <001f01ce3d20$c7674c06952f9ede@Supermanvt2jjg>
From: "Bess Miles" <peering@sewkis.com>
To: <unixfreaxjg@sewkis.com>
Subject: Texas Explosion Injures Dozens
Date: Fri, 19 Apr 2013 20:09:17 +0300
MIME-Version: 1.0
Content-Type: text/plain;
  format=flowed;
  charset="iso-8859-1";
  reply-type=original
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2800.1158
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1158
```

Annotations and analysis:

- to reply with this address (don't reply!)**: Points to the IP address 94.28.49.130 in the link.
- IP address of the open relay MTA**: Points to the IP address 37.45.155.190 in the Received header.
- ID to be grep in open-relayed MTA's log**: Points to the message ID `id oi2si5501238lab.8.2013.04.19.10.10.30;`.
- SPF rules set to neutral, to permit mail like this unblocked by gmail. preventing FP I suppose**: Points to the `Received-SPF: neutral` and `spf=neutral` lines.
- IP Address used by spammer to connect to open relayed MTA**: Points to the IP address 37.45.145.201 in the Received header.
- This HELP command accepted for open relay (must fix) in MTA's conf**: Points to the `HELO vt2jjg` command in the Received header.
- Usage of Outlook Express 6, suggested WinXP used for sending this spam by spammer...**: Points to the `X-Mailer: Microsoft Outlook Express 6.00.2800.1158` line.
- suggested the attacker can be tracked/exist in separate network**: Points to the `X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1158` line.

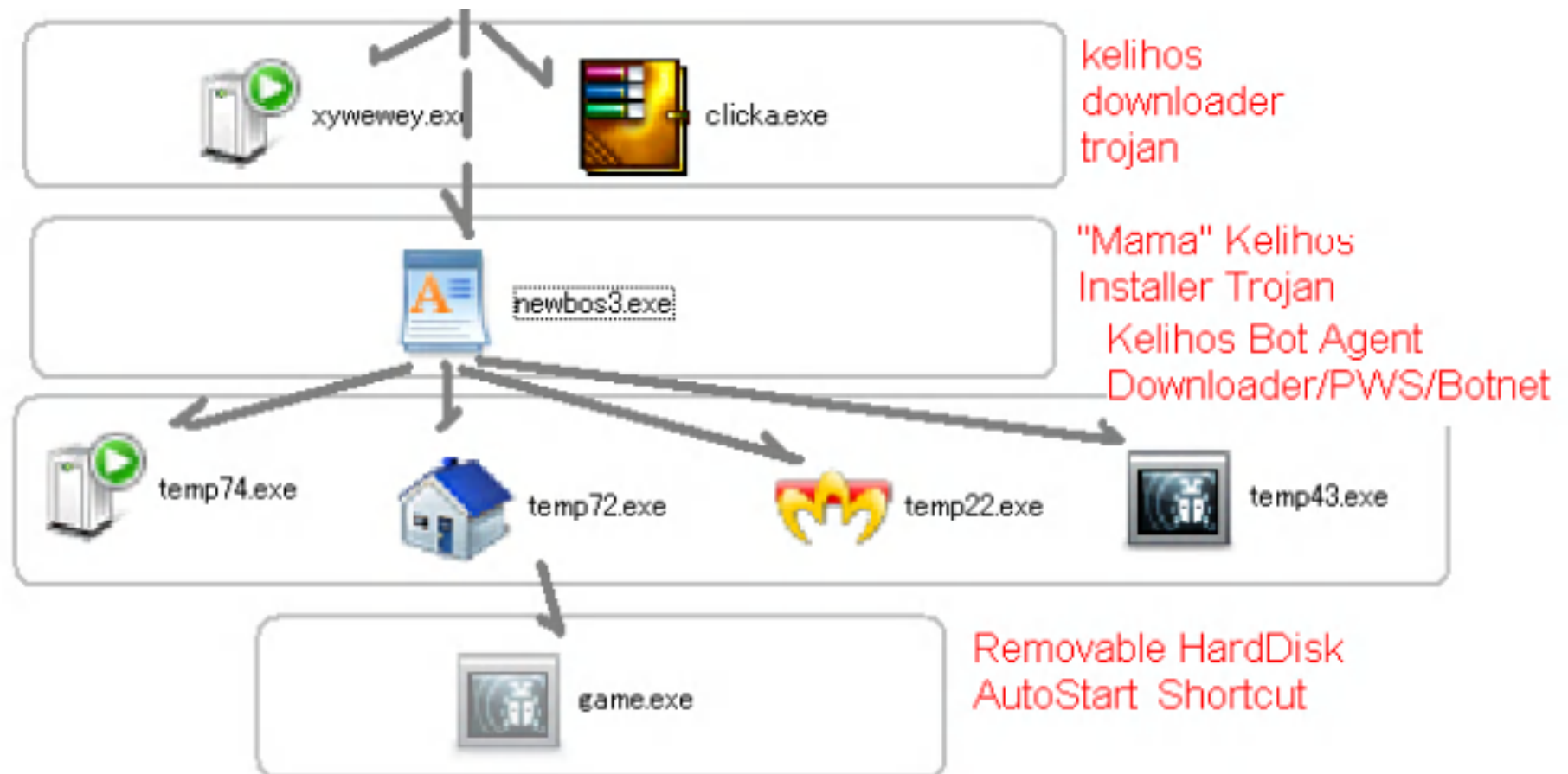
Analysis for the weakness

- Infection Peer Scheme

















Analysis for the weakness

- Infection Peer Scheme




Analysis for the weakness

- Infection Peer Scheme

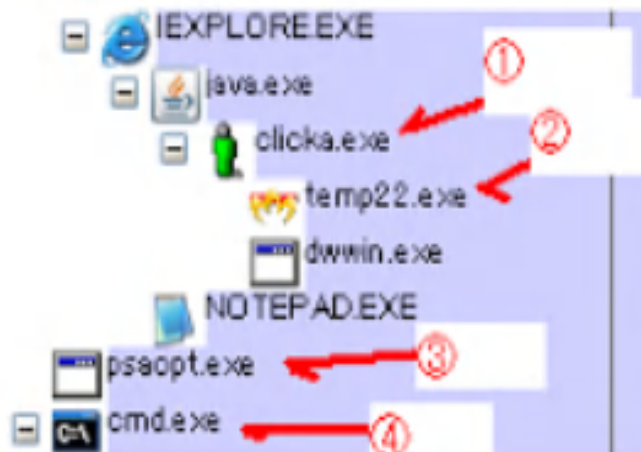
	wesq.html	1 KB	2013/04/20 13:46
	news.html	1 KB	2013/04/20 13:35
	492.jar	13 KB	2013/04/20 13:51
	dp4.jar	13 KB	2013/04/20 13:51
	clicka.exe	32 KB	2013/04/20 18:50
	xywewey.exe	32 KB	2013/04/20 15:01
	aeraetk.exe	47 KB	2013/04/20 15:01
	psaopt.exe	48 KB	2013/04/20 18:50
	game.exe	797 KB	2013/04/20 18:52
	temp22.exe	797 KB	2013/04/20 18:50
	temp43.exe	797 KB	2013/04/20 18:50
	temp72.exe	797 KB	2013/04/20 18:50
	temp74.exe	797 KB	2013/04/20 18:50
	newbos3.exe	797 KB	2013/04/20 15:57

Analysis for the weakness

- Infection Peer Scheme



iexplore.exe	2604	45,736 K	40,616 K	Internet Explorer
java.exe	3720	35,076 K	32,336 K	Java(TM) Platform SE binary
xywwey.exe	332	2,336 K	7,488 K	
temp49.exe	260	6,732 K	10,792 K	
dwwin.exe	2084	3,096 K	8,732 K	Microsoft Application Error Re
conime.exe	2592	2,908 K	936 K	Console IME
aeraetk.exe	2076	4,236 K	6,908 K	



IEXPLORE.EXE	2732	44,088 K	36,016 K	Internet Explorer
java.exe	3480	32,972 K	26,168 K	Java(TM) Platform SE binary
clicka.exe	1240	1,072 K	3,716 K	
temp22.exe	3192	5,760 K	7,692 K	
dwwin.exe	3268	1,956 K	5,396 K	Microsoft Application Error F
NOTEPAD.EXE	1972	2,228 K	4,468 K	Notepad
psaopt.exe	1440	4,004 K	6,664 K	
cmd.exe	3144	69.23	1,580 K	Windows Command Process

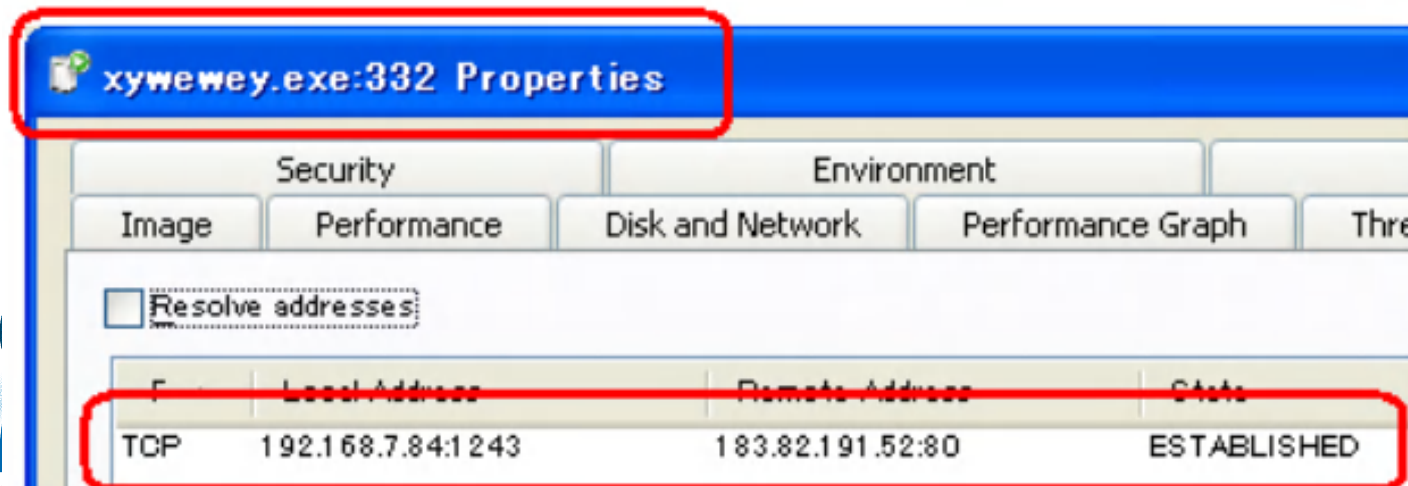
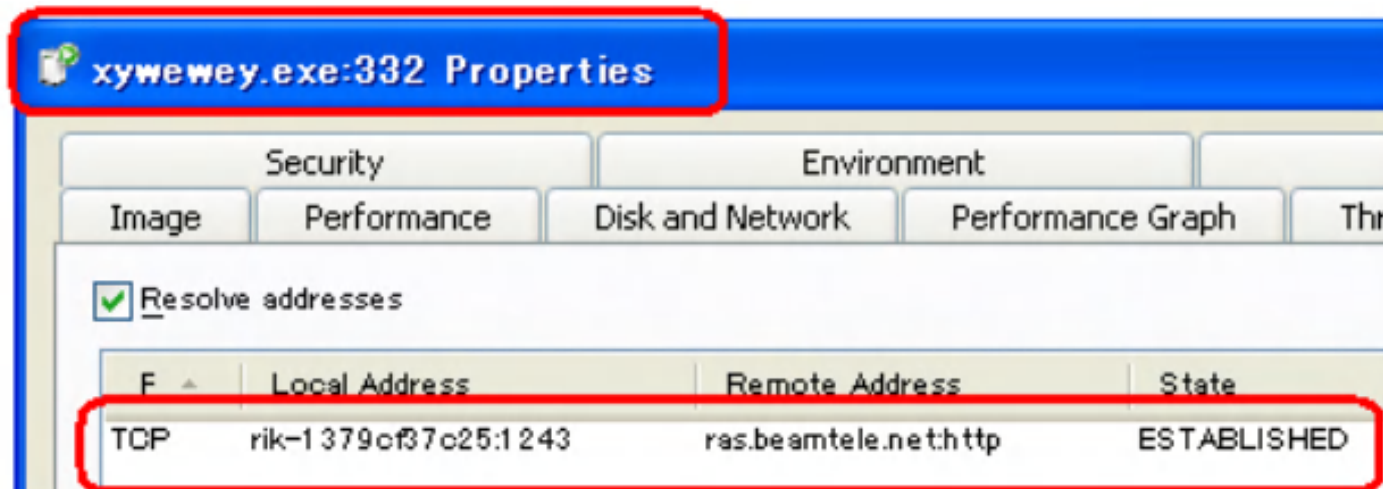
Analysis for the weakness

- Infection Peer Scheme

アドレス(D)	Settings¥MalwareMustDie¥Local Settings¥Temp		▼	➔
名前	サイズ	更新日時		
1cbe_appcompat.txt	5 KB	2013/04/20 15:02		
243b36.mst	68 KB	2013/04/20 14:39		
abcd.bat	1 KB	2013/04/20 15:02		
aeraetk.exe	47 KB	2013/04/20 15:01		
xywewey.exe	32 KB	2013/04/20 15:01		

Analysis for the weakness

- Infection Peer Scheme



Analysis for the weakness

- Infection Peer Scheme

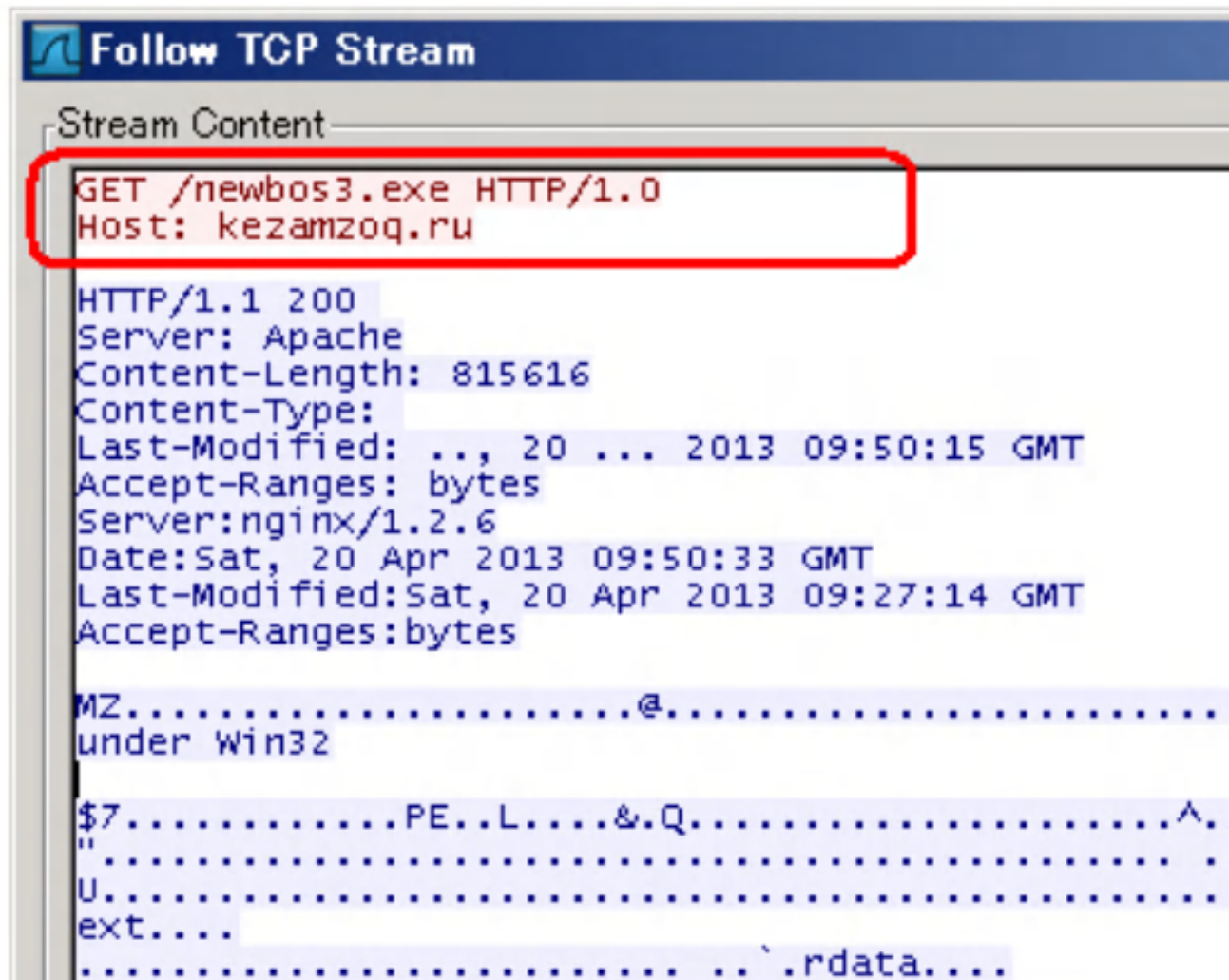
Here's the download:

No.	Source	Destination	Protocol	Info
261	192.168.7.84	183.82.191.52	TCP	1243 > 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460
262	183.82.191.52	192.168.7.84	TCP	80 > 1243 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
263	192.168.7.84	183.82.191.52	TCP	1243 > 80 [ACK] Seq=1 Ack=1 Win=16944 Len=0
264	192.168.7.84	183.82.191.52	HTTP	GET /newbos3.exe HTTP/1.0
265	183.82.191.52	192.168.7.84	TCP	[TCP segment of a reassembled PDU]
266	183.82.191.52	192.168.7.84	TCP	[TCP segment of a reassembled PDU]
267	192.168.7.84	183.82.191.52	TCP	1243 > 80 [ACK] Seq=49 Ack=1579 Win=16944 Len=0

Follow TCP Stream	
Stream Content	
GET /newbos3.exe HTTP/1.0 Host: zahebox.ru	
HTTP/1.1 200 Ok Server: Apache Content-Length: 816128 Content-Type: application/octet-stream Last-Modified: .., 20 ... 2013 06:02:07 GMT Accept-Ranges: bytes	
MZ.....@.....!..L.!..This prog win32	
\$7.....PE..L....&.Q.....'.....".....@... ".....P..... U.....	

Analysis for the weakness

- Infection Peer Scheme



```

Follow TCP Stream
Stream Content
GET /newbos3.exe HTTP/1.0
Host: kezamzoq.ru

HTTP/1.1 200
Server: Apache
Content-Length: 815616
Content-Type:
Last-Modified: .., 20 ... 2013 09:50:15 GMT
Accept-Ranges: bytes
Server:nginx/1.2.6
Date:Sat, 20 Apr 2013 09:50:33 GMT
Last-Modified:Sat, 20 Apr 2013 09:27:14 GMT
Accept-Ranges:bytes

MZ.....@.....
under Win32

$7.....PE..L....&.Q.....^..
".....
U.....
ext....
.....`.rdata....
  
```


Analysis for the weakness

- Infection Peer Scheme

1443	192.168.7.84	69.89.31.88	TCP	1068 > 80 [FIN, ACK] Seq=558 Ack=183 Win=16763 Len=0
1412	192.168.7.84	69.89.31.88	TCP	1068 > 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
1428	69.89.31.88	192.168.7.84	TCP	80 > 1068 [ACK] Seq=1 Ack=304 Win=6432 Len=0
1439	69.89.31.88	192.168.7.84	TCP	80 > 1068 [ACK] Seq=1 Ack=558 Win=7504 Len=0
1459	69.89.31.88	192.168.7.84	TCP	80 > 1068 [ACK] Seq=183 Ack=559 Win=7504 Len=0
1416	69.89.31.88	192.168.7.84	TCP	80 > 1068 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1412 SACK_PERM=1
1441	69.89.31.88	192.168.7.84	HTTP	HTTP/1.1 200 OK (text/html)
1429	192.168.7.84	69.89.31.88	HTTP	POST /default.php?e9BMLDMj6xHrq8hpRqzWuPW2ENVvAQax8l0fLWo HTTP/1.0
1440	69.89.31.88	192.168.7.84	TCP	[TCP segment of a reassembled PDU]
1418	192.168.7.84	69.89.31.88	TCP	[TCP segment of a reassembled PDU]

```

Follow TCP Stream
Stream Content
POST /default.php?e9BMLDMj6xHrq8hpRqzWuPW2ENVvAQax8l0fLWo HTTP/1.0
Host: ecojudge.com
Accept: */*
Accept-Encoding: identity, *,q=0
Content-Length: 254
Connection: close
Content-Type: application/octet-stream
Content-Encoding: binary
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)

CRYPTED0.b..%nv.M(.j.....$.v.....AG.p.<lx.j....V6.....y.-...+......b..~....!...j.-
gIRrB.Etq.34.G.E.n.....p.,n,.K.3s.M.-
Io.....q.'8.V.. .z..lY...:0....r....^y.....p..y8a.....).....Ng.nqX.c.....&.^x.k.....[...N.....9.f.)
'p....y...-...=..d.u.P...a.HTTP/1.1 200 OK
Date: Sat, 20 Apr 2013 09:50:52 GMT
Server: Apache
X-Powered-By: PHP/5.2.17
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

STATUS-IMPORT-OK

```

Analysis for the weakness

☒ Resolve addresses

F	Local Address	Remote Address	State
TOP		gw2.martun.net:80	SYN_SENT
TOP		gw2.martun.net:80	SYN_SENT
TOP		lasvegas-nv-datacenter.com:80	SYN_SENT
TOP		globalnet.pro-managed.com:80	SYN_SENT
TOP		globalnet.pro-managed.com:80	SYN_SENT
TOP		lasvegas-nv-datacenter.com:80	SYN_SENT
TOP		gw2.martun.net:80	SYN_SENT
TOP		gw2.martun.net:80	SYN_SENT
TOP		lasvegas-nv-datacenter.com:80	SYN_SENT
TOP		globalnet.pro-managed.com:80	SYN_SENT
TOP		globalnet.pro-managed.com:80	SYN_SENT
TOP		lasvegas-nv-datacenter.com:80	SYN_SENT
TOP		190.93.253.4:80	SYN_SENT
TOP		190.93.250.24:80	SYN_SENT
TOP		190.93.250.24:80	SYN_SENT
TOP		ddos-guard.net:80	SYN_SENT
TOP		ip-50-62-238-103.ip.secureserver.net:80	SYN_SENT
TOP		190.93.253.4:80	SYN_SENT
TOP		ddos-guard.net:80	SYN_SENT
TOP		190.93.253.4:80	CLOSE_WAIT
TOP		ddos-guard.net:80	SYN_SENT
TOP		190.93.250.24:80	CLOSE_WAIT
TOP		199.27.135.3:80	CLOSE_WAIT
TOP		ip-50-62-238-103.ip.secureserver.net:80	SYN_SENT
TOP		190.93.250.24:80	ESTABLISHED
TOP		199.27.135.3:80	CLOSE_WAIT
TOP		199.27.135.3:80	CLOSE_WAIT
TOP		90.156.201.193:80	CLOSE_WAIT
TOP		90.156.201.193:80	CLOSE_WAIT
TOP		90.156.201.193:80	CLOSE_WAIT
TOP		190.93.253.4:80	CLOSE_WAIT
TOP		190.93.253.4:80	SYN_SENT
TOP		ddos-guard.net:80	SYN_SENT
TOP		ip-50-62-238-103.ip.secureserver.net:80	SYN_SENT
TOP		ddos-guard.net:80	SYN_SENT
TOP		ddos-guard.net:80	SYN_SENT
TOP		ddos-guard.net:80	SYN_SENT
TOP		ddos-guard.net:80	SYN_SENT
TOP		190.93.250.24:80	ESTABLISHED
TOP		fe.shared.masterhost.ru:80	ESTABLISHED
TOP		fe.shared.masterhost.ru:80	ESTABLISHED

☒ Resolve addresses

F	Local Address	Remote Address	State
TOP		ip-50-62-238-103.ip.secureserver.net:80	SYN_SENT
TOP		globalnet.pro-managed.com:80	SYN_SENT
TOP		190.93.250.24:80	SYN_SENT
TOP		ddos-guard.net:80	SYN_SENT
TOP		gw2.martun.net:80	SYN_SENT
TOP		gw2.martun.net:80	SYN_SENT
TOP		lasvegas-nv-datacenter.com:80	SYN_SENT
TOP		globalnet.pro-managed.com:80	SYN_SENT
TOP		lasvegas-nv-datacenter.com:80	SYN_SENT
TOP		190.93.253.4:80	SYN_SENT
TOP		190.93.253.4:80	SYN_SENT
TOP		ip-50-62-238-103.ip.secureserver.net:80	SYN_SENT
TOP		ip-50-62-238-103.ip.secureserver.net:80	SYN_SENT
TOP		ip-50-62-238-103.ip.secureserver.net:80	SYN_SENT
TOP		globalnet.pro-managed.com:80	SYN_SENT
TOP		190.93.250.24:80	SYN_SENT
TOP		lasvegas-nv-datacenter.com:80	SYN_SENT
TOP		gw2.martun.net:80	SYN_SENT
TOP		gw2.martun.net:80	SYN_SENT
TOP		lasvegas-nv-datacenter.com:80	SYN_SENT
TOP		globalnet.pro-managed.com:80	SYN_SENT
TOP		190.93.253.4:80	SYN_SENT
TOP		ip-50-62-238-103.ip.secureserver.net:80	SYN_SENT
TOP		190.93.250.24:80	SYN_SENT
TOP		globalnet.pro-managed.com:80	SYN_SENT
TOP		190.93.250.24:80	SYN_SENT
TOP		lasvegas-nv-datacenter.com:80	SYN_SENT
TOP		gw2.martun.net:80	SYN_SENT
TOP		gw2.martun.net:80	SYN_SENT
TOP		lasvegas-nv-datacenter.com:80	SYN_SENT
TOP		globalnet.pro-managed.com:80	SYN_SENT
TOP		190.93.253.4:80	ESTABLISHED
TOP		190.93.253.4:80	SYN_SENT
TOP		ip-50-62-238-103.ip.secureserver.net:80	SYN_SENT
TOP		190.93.253.4:80	CLOSE_WAIT
TOP		190.93.253.4:80	CLOSE_WAIT
TOP		fe.shared.masterhost.ru:80	CLOSE_WAIT
TOP		fe.shared.masterhost.ru:80	CLOSE_WAIT
TOP		fe.shared.masterhost.ru:80	CLOSE_WAIT
TOP		ddos-guard.net:80	SYN_SENT
TOP		190.93.250.24:80	ESTABLISHED

Analysis for the weakness

- Encryption Cracking Method

```

Follow TCP Stream
Stream Content
POST /administrator/modules/mod_menu/tmp1/content.php HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)
Host: keximv1c.com.vn
Content-Length: 384
Connection: Keep-Alive
Cache-Control: no-cache

`GU=W..12&..7..$..-.m..6.[,..K.2.
.-...W.u.....wn... f2-.. ^..t.C.o.C..
.%.O&bV...f(n;...?.P.E.....[8..s.....b....T4...o..[W(a.....U.
.....G:5(Kb..q\....)w.....h86....p.....OL8F2.k{....4j.U.....w....D.h.4.u.R.....<...
$.0]....aj....s.....w.....$j.t.k..a{..hl_Ck..G
`..S.(...'.p.d9:..).b....(.y
..n.O?.....f3...B...jEe..s.....G>1....gu.R..D.....HTTP/1.1 200 OK
Date: Sat, 20 Apr 2013 06:09:12 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.2.17
X-Powered-By: PleskLin
Content-Length: 64
Connection: close
Content-Type: text/html

.d..ff.uL.\'.r.....$".
.*.9(>\\q.y..?.j.V.U]z5Q....A.Q.....|

```


Analysis for the weakness

- Encryption Cracking Method

```
POST /pro/file.php HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)
Host: tableindexcsv.com
Content-Length: 120
Connection: Keep-Alive
Cache-Control: no-cache

T<[Ij4k.Y...Bd].!5.r...M. .W...<..c.....@0.2.X..6...0..t.....b....:..(,9...01.u.!.....%
....\5.)D
..i.HTTP/1.1 200 OK
Date: Sat, 20 Apr 2013 06:19:32 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.6
Cache-Control: public
Content-Disposition: attachment; filename="%2e/files/conf.bin"
Content-Transfer-Encoding: binary
Content-Length: 7472
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/octet-stream

T_h.E,4_...?..`$..@.:.$[.!m....U9.$boq..3.V..`K.X...0.J..tsE.s.....ih....#..y[
[.7n..bv..3:.8IGwt...[.V..5...K...2...W..
.
.....x...q]..:X.T]wz].|.X.B.r.1t.Z.#]U...m..*.d.A.=...fa.|.2..j...s.^dAv.....J...
.*.....!0....\..tk...q3.....X..y.8...ZR.u...
.C
.Q...:..!....uh.v."...e.\.....M..%.DK...@Ma$1...q.W.J7..i.b...[.p.J..N.Yg...f.=>.F6.....
%......g.....>
-hK.K.+f]...%......ci....Ve....ULHg.....R..\.X...P....[m....-.B..X...e.....
+F...K.....4F....2...?..-...p....e.<.....+#.h.....x@...='....}<...7I...fh.D_+RI
G..n..N.....GO..$E..Edy....G3...n5...2E...<.....\a..S.u]z.>...
...W.RI..1...t.]d.Ib....D.N....Zx7.%...L=...L/Y..M.....0.(`V.)?..u,J..l.&.I..Z..s
[.Z..~.1.O.....;..Vw1.O..+..X..|r.2....,$...A.....:..82...W=...N....b.c.....8..SL2
(lc..t.o...@P.....[.)..c..f.v.]..g.....C..?.....vt.v.....F..8.....&.Z...Z.(....\
%...Z..J;...H.n.k..jB.N.....eMz}|...f..t..h1....de.u)...-3qo..O.....u(
.B...;...o.ZXB6$B...|ku...~".xM.$,0x..6s..1u..^ecn.-J|~.....8.K...@.0.3...w~t.'.l...
ou
```

Analysis for the weakness

- Encryption Cracking Method

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000h:	B0	E2	30	20	6C	55	55	45	03	10	48	40	52	F4	56	CB	°	â	0	1	U	U	E	.	.	H	@	R	Ö	V	È	
0010h:	B0	A9	7A	BD	B4	F3	41	F4	A8	07	E5	94	30	46	02	41	°	@	z	4	°	ó	A	ô	.	.	â	"	0	F	.	A
0020h:	00	B7	59	0C	46	AE	63	C3	B2	07	D8	33	A9	C5	DB	5F	.	.	Y	.	F	@	c	Ã	²	.	ø	3	@	Å	Û	
0030h:	92	5F	C9	87	DE	26	60	FD	25	BE	62	BA	21	9D	E1	31	'	É	+	P	&	`	ý	%	¾	b	°	!	.	á	1	
0040h:	0A	22	07	80	6A	A8	E2	14	2F	F3	D9	56	95	E7	08	E6	.	"	.	ej	"	â	.	/	ó	Ù	V	•	ç	.	æ	
0050h:	C4	DD	7C	B0	9B	E4	7C	0D	49	09	A3	AA	88	57	8B	B4	Ä	Ý		°	>	ä		.	I	.	£	°	^	W	<	'
0060h:	7B	02	01	11	59	2B	FC	41	4E	A1	E9	E5	74	0D	D1	E2	{	.	.	.	Y	+	ü	A	N	;	é	â	t	.	Ñ	â
0070h:	85	E3	C8	69	D8	3B	C5	1D	BF	96	08	9C	A1	1B	09	CD	...	ä	È	i	ø	;	Å	.	ç	-	.	æ	;	.	.	í
0080h:	81	20	9D	A6	16	71	98	D8	0D	A9	00	B2	4C	C1	5A	90	.	.	.	!	.	q	°	ø	.	©	.	²	L	Ä	Z	.
0090h:	3D	1D	34	B4	AF	E8	66	75	ED	17	0F	BB	89	93	DD	F6	=	.	4	'	°	è	f	u	í	.	.	»	%	"	Ý	ö
00A0h:	AA	8E	0E	88													a	ž	.	°												

Using the encryption know-how we can figure the peer information and the JobServer (aka CnC)

Analysis for the weakness

- Encryption Cracking Method

(The data is courtesy of Kyle Yang of Fortinet at Blackhat presentation)

0000h:	A2 49 4D F3 D9 1E 9F 88 01 01 14 6D 5F 6A 6F 62	eIM6U.Y'...m_job
0010h:	5F 62 6C 6F 62 00 02 02 45 03 A2 49 4D F3 D9 1E	_blob...E.eIM6U.
0020h:	9F 88 01 01 04 6D 5F 6A 6F 62 73 00 03 04 01 14	Y'...m_jobs.....
0030h:	6D 5F 62 75 69 6C 64 5F 6C 65 73 73 5F 6F 72 5F	m_build_less_or_
0040h:	65 71 75 61 6C 5F 63 6F 6E 64 69 74 69 6F 6E 00	equal_condition.
0050h:	02 01 10 32 00 00 00 6D 5F 62 75 69 6C 64 5F 6D	...2...m_build_m
0060h:	6F 72 65 5F 6F 72 5F 65 71 75 61 6C 5F 63 6F 6E	ore_or_equal_con
0070h:	64 69 74 69 6F 6E 00 02 01 10 00 00 00 00 6D 5F	dition.....m_
0080h:	63 6F 6D 6D 61 6E 64 00 02 01 10 01 00 00 00 6D	command.....m
0090h:	5F 63 6F 6D 6D 61 6E 64 73 5F 70 61 72 61 6D 73	_commands_params
00A0h:	00 04 02 08 78 68 74 74 70 3A 2F 2F 62 69 74 61xhttp://bita
00B0h:	67 65 64 65 2E 63 6F 6D 2F 66 6C 61 73 68 32 2E	gede.com/flash2.
00C0h:	65 78 65 4C 6D 31 75 68 75 6B 6F 75 76 33 7A 6E	exeamluhukouv3zn
00D0h:	61 6F 69 2E 65 78 65 6D 5F 6A 6F 62 5F 69 64 00	aoi.exem_job_id.

Analysis for the weakness

- Domains & Payloads

`([a-z]{6}¥.[a-z]{4}|[a-z]{7}¥.[a-z]{3}|[a-z]{8}¥.[a-z]{2})`

10

10

10

+ One Dot

11 bytes

Analysis for the weakness

- Domains & Payloads

VEHIQYR.ORG

EJEXPOC.COM

ABGYCWU.NET

CESGUMU.ORG

QYQANYB.BIZ

GOTOREF.BIZ

TOREMOA.COM

Analysis for the weakness

- Domains & Payloads

angrim2.exe
bergem1.exe
bljat01.exe
calc.exe

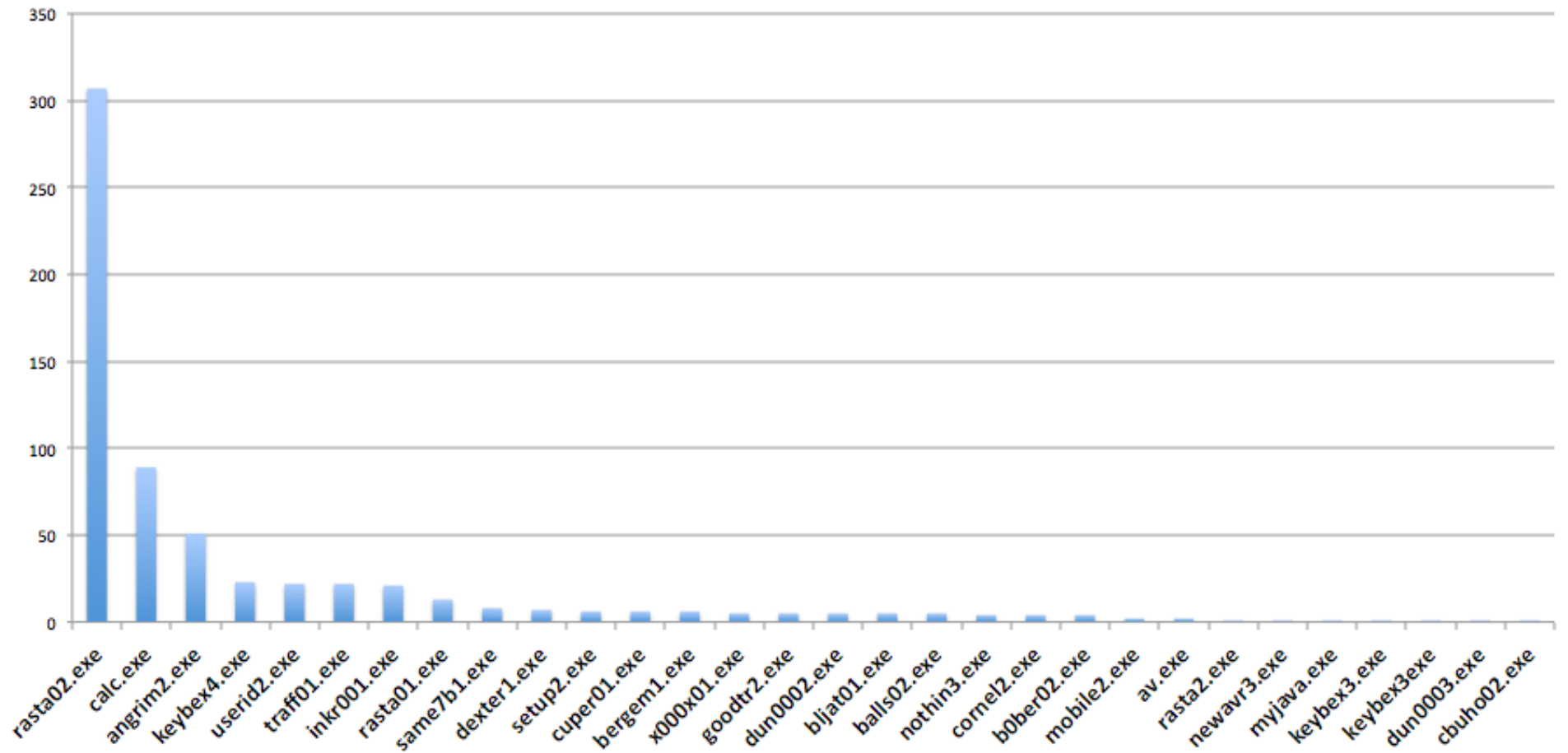
inkr001.exe
keybex4.exe
nothin3.exe
rasta02.exe

cornel2.exe
dexter1.exe
goodtr2.exe
↓

traff01.exe
userid2.exe
same7b1.exe

Malware Exes names stats

Malware Must Die



Malware samples

~~Malware~~ **Must Die**

- **VirusTotal report** calc.exe <http://bit.ly/18mEF6D>
- Payload repacked several times a day
- **VirusTotal report** cornel2.exe <http://bit.ly/19zCtrf>
- VT detection ratio got as low as 1/45
- rasta02.exe (3/45 on Sep 1) <http://bit.ly/18mIVpv>
- cornel2.exe (1/45 on Sep 1) <http://bit.ly/18mm0cV>



Analysis for the weakness

- Domains & Payloads

Active distribution registrars:

BizCN	321
INTERNET.BS	190
PDR	91
1API	68
REGGI	27
REGTIME	27
total	724

Analysis for the weakness

- Domains & Payloads Monitoring Base

```
¥/[0-9]{1,3}¥.[0-9]{1,3}¥.[0-9]{1,3}¥.[0-9]{1,3}¥/
|([a-z]{5,6}[0-9]{1,2}|calc)¥.exe
```

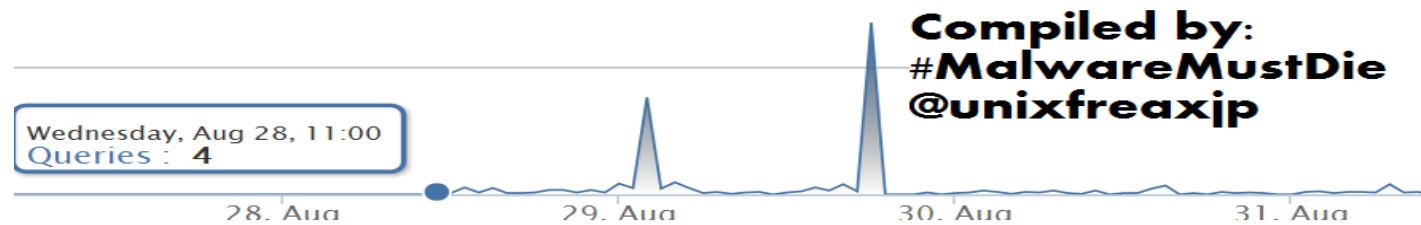
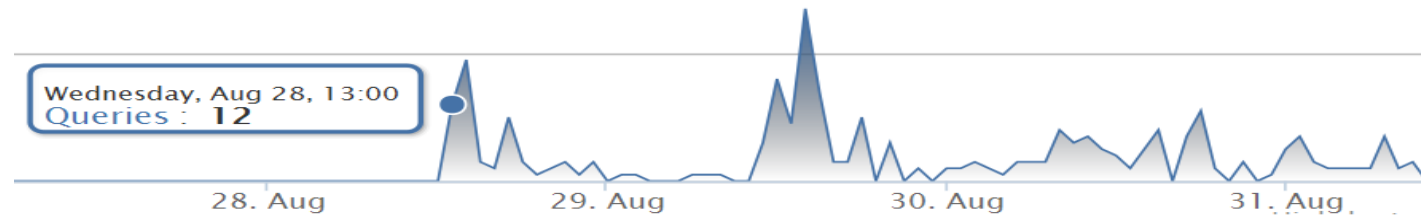
Search: ¥/[0-9]{1,3}¥.[0-9]{1,3}¥.[0-9]{1,3}¥.[0-9]{1,3}¥/([a-z]{5,6}[0-9]{1,2}|calc)¥.exe

► Advanced settings:

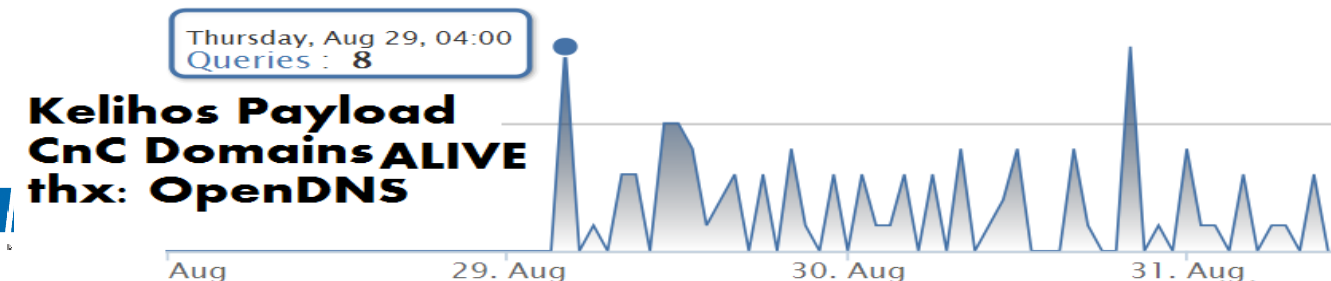
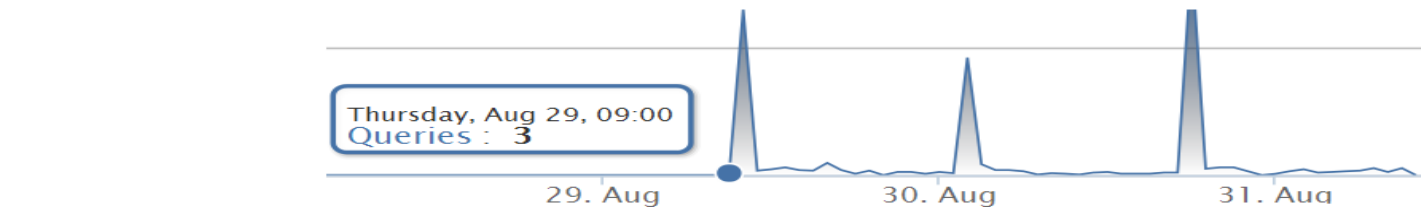
96 results returned

Date (CET)	Alerts / IDS	URL
2013-09-26 02:23:24	0 / 0	http://209.102.242.50/calc.exe
2013-09-26 02:22:40	0 / 0	http://68.112.119.181/calc.exe
2013-09-26 01:10:11	0 / 3	http://178.151.5.191/userid2.exe
2013-09-26 01:09:17	0 / 3	http://178.151.5.191/traff01.exe
2013-09-26 01:07:51	0 / 3	http://178.151.5.191/rasta02.exe
2013-09-26 01:07:22	0 / 3	http://178.151.5.191/keybex4.exe
2013-09-26 01:05:45	0 / 3	http://178.151.5.191/calc.exe
2013-09-25 23:32:26	0 / 3	http://172.242.197.124/calc.exe

Analysis for the weakness



Compiled by:
#MalwareMustDie
@unixfreaxjp



Kelihos Payload
CnC Domains ALIVE
thx: OpenDNS

Analysis for the weakness

to Roman ▾

```
>>> OLTUZMAV.ME|Nameservers:NS1.OLTUZMAV.ME
Nameservers:NS2.OLTUZMAV.ME
Nameservers:NS3.OLTUZMAV.ME
Nameservers:NS4.OLTUZMAV.ME
Nameservers:NS5.OLTUZMAV.ME
Nameservers:NS6.OLTUZMAV.ME|Sponsoring Registrar:Bizcn.com, Inc. R150-ME (471)
Last Updated by Registrar:Bizcn.com, Inc. R150-ME (471)|Domain Create Date:22-Sep-2013 22:16:28 UTC
Domain Last Updated Date:22-Sep-2013 22:22:36 UTC
Domain Expiration Date:22-Sep-2014 22:16:28 UTC
Last Transferred Date:|
```

```
>>> OLTUZMAV.ME
46.147.129.50
61.26.167.12
61.58.78.96
176.104.238.22
94.153.119.106
37.115.17.179
```

```
--2013-09-26 21:18:49-- http://oltuzmav.me/calc.exe
Resolving oltuzmav.me (oltuzmav.me)... 195.114.155.160
Connecting to oltuzmav.me (oltuzmav.me)|195.114.155.160|:80... connected.
HTTP request sent, awaiting response... 200
Length: 819200 (800K) []
Saving to: 'calc.exe'
```

```
28% [=====>
```

Disclosure of Operation (Result)

Spam Templates Order

(1) First Case, the “translator” is make_a_wish@mail.ru

On September 1st, 2013, “saever” received the template for spam from “Галчонка”
<make_a_wish@mail.ru>, with the message as per pasted below:

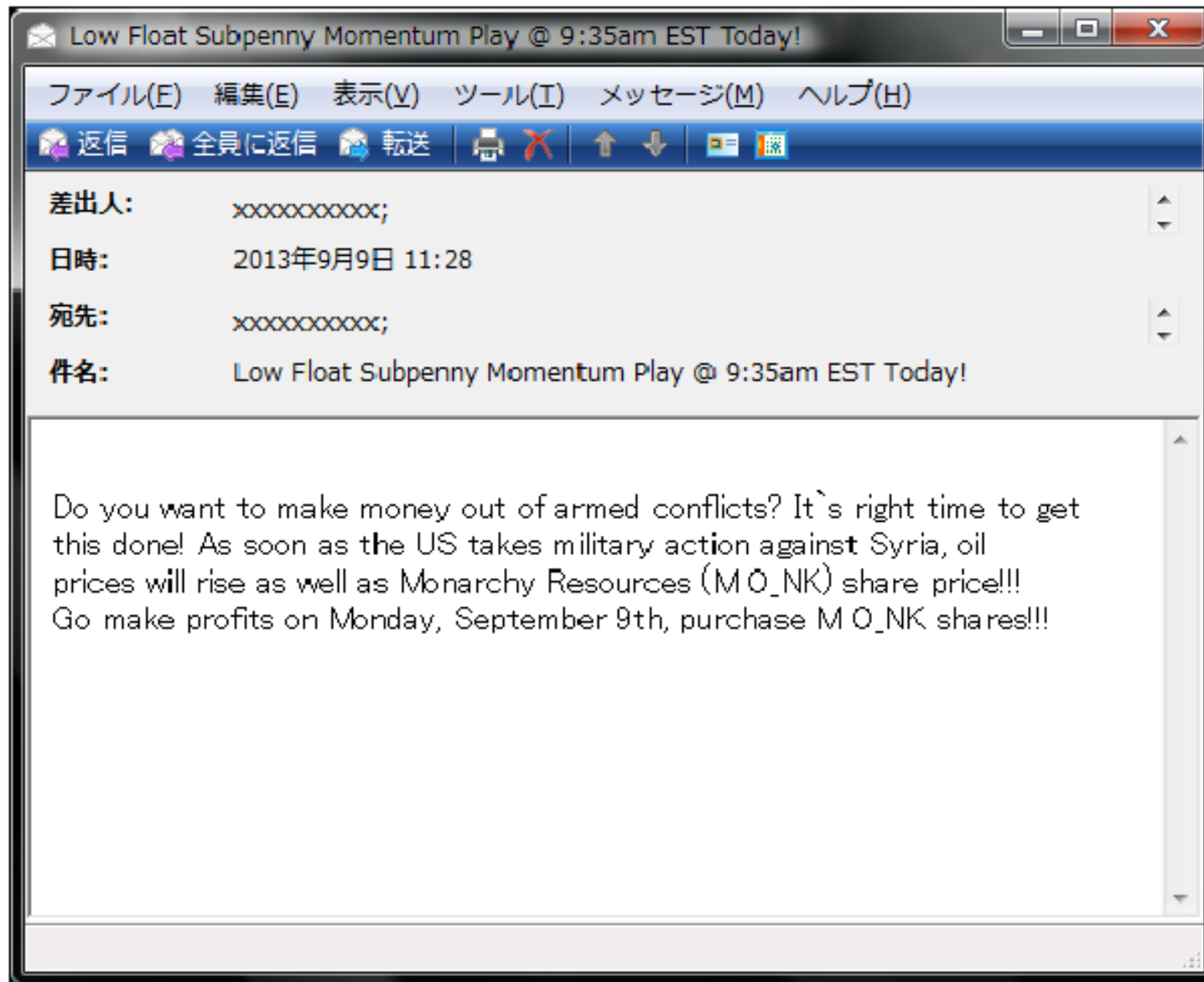
From: “Галчонка” <make_a_wish@mail.ru>
Date: 1 Sep 2013 08:42
Subject: рендомизация предложений.
To: <saever@mail.ru>
Cc:

Привет!

Вот что получилось!

1. {Do you want|Do you wish} to {earn money on|make money out of|get money from|cash in on|make a mint of money due to|become rich due to|make megabucks due to} {war|armed conflicts}? 2. It's {right time|perfect time|the very time} to {do it|realize this|make it|put your idea into force|get this done|realize your plans}! 3. {As soon as|Just as|The moment} the first {rockets|bombs|missiles} {fall on|touch the ground in|get to the earth in|descend to} Syria, {oil|petrol|black gold|petroleum|stone oil} prices will {rise|skyrocket|move up|go up} {as well as|the same as|just as} COMPANY_NAME {share|stock|securities|bond} price.

Disclosure of Operation (Result)



Disclosure of Operation (Result)

(2) Second Case, the “translator” is Ms. Lesye

On Fri, 13 Sep 2013 16:39:08 -0700 (PDT) “saever” received an email from Ms. “Lesye”:

Original header

Received: by 10.58.118.236 with SMTP id kp12csp86026veb;
Fri, 13 Sep 2013 16:39:08 -0700 (PDT)
X-Received: by 10.152.116.7 with SMTP id js7mr12983394lab.11.1379115548070;
Fri, 13 Sep 2013 16:39:08 -0700 (PDT)
Return-Path: <leskin098@mail.ru>
Received: from f367.i.mail.ru (f367.i.mail.ru. [217.69.141.9])
by mx.google.com with ESMTPS id r4si4668795lah.173.1969.12.31.16.00.00
(version=TLSv1 cipher=RC4-SHA bits=128/128);
Fri, 13 Sep 2013 16:39:08 -0700 (PDT)
Received-SPF: pass (google.com: domain of leskin098@mail.ru designates 217.69.141.9 as
permitted sender) client-ip=217.69.141.9;
Authentication-Results: mx.google.com;
spf=pass (google.com: domain of leskin098@mail.ru designates 217.69.141.9 as permitted
sender) smtp.mail=leskin098@mail.ru;
dkim=pass header.i=@mail.ru
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; d=mail.ru; s=mail2;
h=Content-Type:Message-ID:Reply-To:Date:Mime-Version:Subject:To:From;
bh=c04Y1E4A/ogsKduzq4/2EEqXSMZ2xV+5alLvmVgbAaA=;

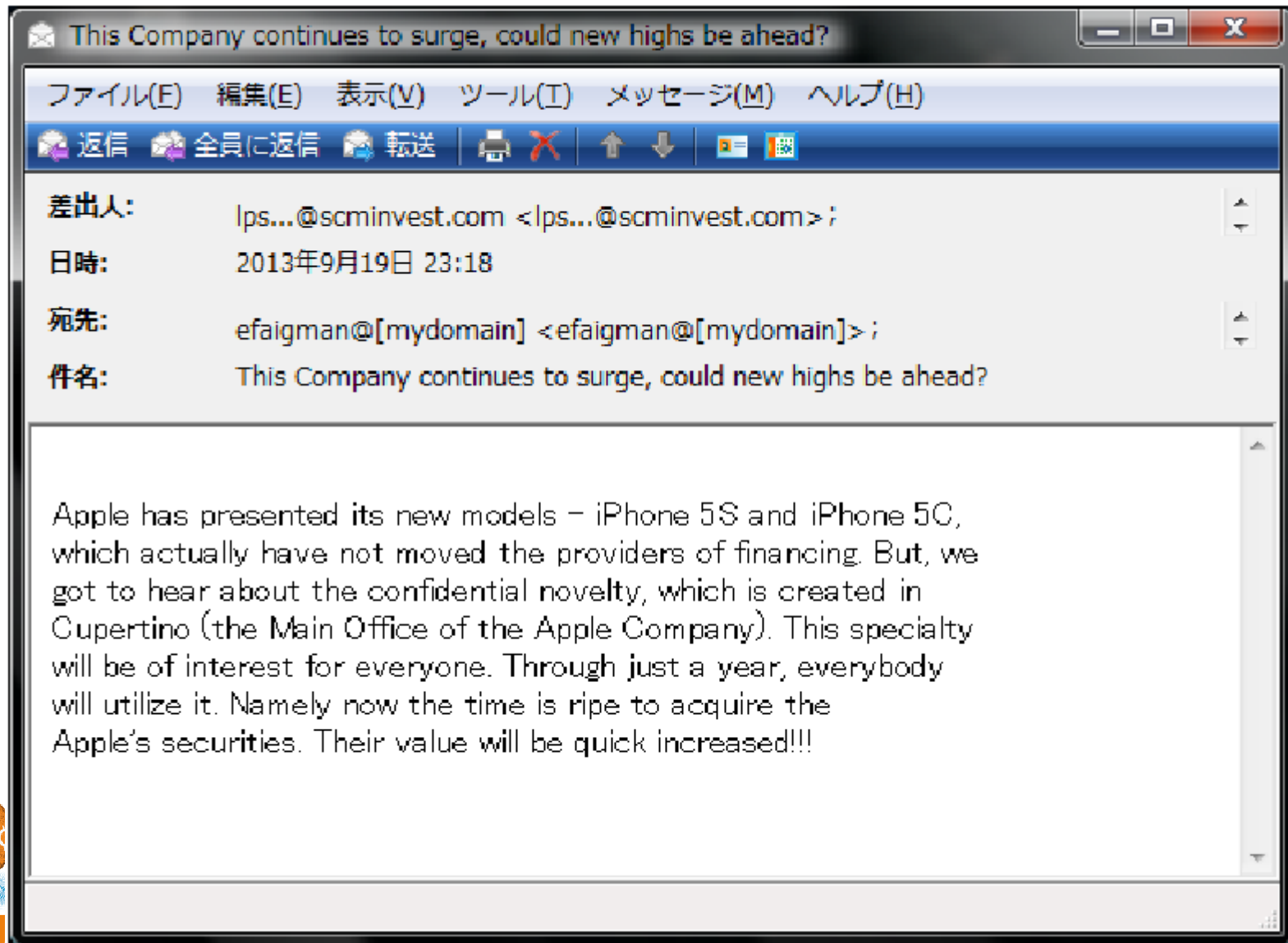
Disclosure of Operation (Result)

{The Apple Company|Apple|The Apple} {has presented|has demonstrated|has shown|has introduced|has recommended|has offered} {its new|its latter-day|the new-developed|its new-made|its fresh|its most recent} iPhone 5S and iPhone 5C, which {have not impressed|have not affected|have little effect on|have not moved|have not struck} the {investors|providers of financing|providers of capital|fund clients|business sponsors|capital providers|financiers|obligees|backers}.

{But|However|Fortunately|Nevertheless|All the same|Still}, we {came to know about|found out about|discovered|got to learn about|got to hear about|got the wind of} {a confidential|a secret|an inside|an undercover|a non-public|a private} {novelty|new product|innovation|recent development|specialty|newly-designed product|newcomer} (gadget), which {is developed|is created|is designed|is produced|is worked out|is elaborated} in Cupertino (the {Main Office|Head-Office|Headquarter|Principal Place of Business|Principal Business Office|General Headquarter|Central Office|Principal Office} of {Apple|the Apple Company|the Company|the Apple}). {Everybody|Everyone|All the people} will {need|require|sought for|have interest in} this {innovation|new product|novelty|newcomer|undercover|recent development|newly-designed product} ({in a year|during a year|within a year|through a year|during the course of a year|throughout a year}, it {will be used|will be put in use|will be utilized|will be put on|will be applied} by {all the people|everyone|everybody}).

{Now|Presently|Just now|Today|Right now}, {it's high time|the time is ripe|it's about time|is the perfect timing} to {buy|purchase|acquire|get|obtain|take possession of|get hold of} the Apple's {shares|securities|equity|stock|shareholding|capital stock|actions|shares of stock|shares of corporate stock|corporate stock|stocks}. {They|The shares|These stocks|The Company's capital stock|The shareholding|These securities|The Company's equity} will {grow|go up|increase} in {price|value} {soon|quick|quite soon|fast|very soon}!

Disclosure of Operation (Result)



Disclosure of Operation (Result)

Bad Actor “Spam Nation” contacts

Все контакты

8 контактов

Директ

Английский за попогода!

Секретный метод обучения сотрудников разведки. Изучайте прямо из дома!

Добавить

Редактировать

Написать

Удалить

В группу

Еще

А

Б

В

Г

Д

Е

Ж

З

И

К

Л

М

Н

О

П

Р

С

Т

У

Ф

Х

Ц

Ч

Ш

Щ

Ы

Э

Ю

Я

<input type="checkbox"/>	<input type="checkbox"/>	<div>А</div>	Andrei	evdesign@gmail.com
<input type="checkbox"/>	<input type="checkbox"/>	<div>-</div>	- контакт без названия -	boss@domenshop.net
<input type="checkbox"/>	<input type="checkbox"/>	<div>В</div>	brin	brin@3fn.net
<input type="checkbox"/>	<input type="checkbox"/>	<div>И</div>	Ira Billing @ Gibibits Servers	ira@gibibits.com
<input type="checkbox"/>	<input type="checkbox"/>	<div>-</div>	- контакт без названия -	lena@gibibits.com
<input type="checkbox"/>	<input type="checkbox"/>	<div>Н</div>	noc	noc@sys1.3fn.net
<input type="checkbox"/>	<input type="checkbox"/>	<div>Р</div>	Petr Klimovsky	klimovskypetr@gmail.com
<input type="checkbox"/>	<input type="checkbox"/>	<div>С</div>	Support Team	support@gibibits.com

Disclosure of Operation (Result)

CNC Servers

Germany:

Additional IP: DE-7 5.61.37.239 (additional to: 5.61.38.32) <--- CNC

Additional IP: DE-7 5.61.38.34 <--- CNC

Additional IP: DE-7 5.61.38.33 <--- CNC

Additional IP: DE-7 5.61.38.32 <--- CNC

Additional IP: DE-7 5.61.38.31 <--- CNC

Additional IP: DE-7 5.61.38.30 <--- CNC

Netherlands:

Dedicated: NL-1 - 82.192.91.11 (01/10/2013 - 31/10/2013) <---Mother fuckin ship

Dedicated: NL-1 - 95.211.22.199 (01/10/2013 - 31/10/2013) <--- CNC

Dedicated: NL-1 - 95.211.58.238 (01/10/2013 - 31/10/2013) <--- CNC

Dedicated: EASYNET-NL-1 (SWay) - 37.1.207.80 <-- Mother fuckin Ship

UK: <--- Mother Fuckin Ship with 5 IP of Job Servers (they just moved)

Dedicated: GXSGBM-004: 6 IP - srv051212 - Intel Xeon E3-1290 Sandy Bridge 3.6GHz VT,
16 GB RAM, 2x500 GB SATA-II HDD RAID 1, 100 Mbps Unmetered Traffic , 6 IP - srv051212
(17/09/2013 - 16/10/2013)

Disclosure of Operation (Result)

CNC Server Bills Invoices + ETC Invoices/ID +++

From: "GloboXhost.com" <support@globoxhost.com>
Date: 3 Nov 2013 09:21
Subject: Подтверждение оплаты || Invoice Payment Confirmation
To: "saever@mail.ru" <saever@mail.ru>
Cc:



Уважаемый(ая) saever@mail.ru,

Сообщаем, что счет 41614 от 03/11/2013 оплачен Вами.

GXSGBM-004: Intel Xeon E3-1290 Sandy Bridge 3.6GHz VT, 16 GB RAM, 2x500 GB SATA-II
HDD RAID 1, 100 Mbps Unmetered Traffic, 6 IP - srv051212 (17/11/2013 - 16/12/2013)
Операционная система: CentOS
Панель управления (установка возможна для CentOS
и Fedora): Нет \$199.00 USD

Итого: \$199.00 USD
Кредит: \$0.00 USD
К оплате: \$199.00 USD

Сумма: \$199.00 USD
Номер операции #: 943309214
Всего оплачено: \$199.00 USD
Текущий баланс: \$0.00 USD
Статус: Оплачен



Disclosure of Operation (Result)

From: "Inferno Solutions" <noreply@inferno.name>
Date: 29 Oct 2013 22:02
Subject: Счет за услугу
To: "Петр Сергеев" <saeve@mail.ru>
Cc:

From: "Inferno Solutions" <noreply@inferno.name>
Date: 28 Oct 2013 22:01
Subject: Счет за услугу
To: "Петр Сергеев" <saeve@mail.ru>
Cc:

Inferno Solutions
пока мы работаем - конкуренты отдыхают

Inferno Solutions
пока мы работаем - конкуренты отдыхают

Уважаемый Петр Сергеев (---),

Ваш счет был создан 30/10/2013.

Ваш метод оплаты: WebMoney

Счет №118164

Сумма к оплате: \$135.00 USD

Оплатить до: 14/11/2013

СКИДКИ: Выделенный сервер DE-7 - 5.61.38.34 (14/11 - 13/12/2013)

Панель управления: Без панели (только установка ОС)

Администрирование: Бесплатное (если заказана панель управления)

Оперативная память (RAM): Без изменений

Жесткий диск (HDD): Без изменений

RAM: Без RAM

Уважаемый Петр Сергеев (---),

Ваш счет был создан 29/10/2013.

Ваш метод оплаты: WebMoney

Счет №118015

Сумма к оплате: \$910.00 USD

Оплатить до: 13/11/2013

EASYNET-NL-1 (SWay) - 37.1.207.80 (13/11/2013 - 12/12/2013)

Панель управления: Без панели (только установка ОС)

Администрирование: Бесплатное (если заказана панель управления) \$910.00 USD

Итого: \$910.00 USD

Кредит: \$0.00 USD

К оплате: \$910.00 USD

Disclosure of Operation (Result)

Other Malware Collaborated; COOKIEBOMB

i.e. <http://malware.dontneedcoffee.com/2013/09/cookie-bomb-iframe-way.html>

The contact info is:

Jabber(XMPP): jabber @ honese.com

ICQ: 104967

nslookup honese.com

Server: 202.238.95.24

Address: 202.238.95.24#53

Non-authoritative answer:

Name: honese.com

Address: 5.61.38.34 <=== is in this list



Disclosure of Operation (Result)

ID Of The Bad Actor

Common Used Nick:

SAEVER@MAIL.RU

Aliases: SEVERA

{CENCORED}

What is the efficient way to Neutralize Kelihos?

Let's Stop Payloads Distribution

- STOPPING THE INFECTED PEER? NO
- STOPPING THE PAYLOAD? YES! ☺

Let's Stop Payloads Distribution

```

Status ##DCG893JP X ##dcg893 X ##DCG893GE X ##DCG893RU X
(no topic set)
[03:27] <mmd0x01> Read error (Operation timed out) in headers.
[03:27] <mmd0x01> 75.118.67.68|Fri Nov 15 03:27:24 JST 2013|d118-75-68-67.col.wideopenwest.com.|
WOWWAY.COM | WIDEOPENWEST OHIO
[03:27] <mmd0x01> 2013-11-15 03:27:36 URL:http://75.118.67.68/calc.exe [1050624/1050624] -> "/de
[03:28] <mmd0x01> 97.81.105.174|Fri Nov 15 03:28:05 JST 2013|97-81-105-174.dhcp.athn.ga.charter.
CHARTER.NET | CHARTER COMMUNICATIONS
[03:28] <mmd0x01> Read error (Operation timed out) in headers.
[03:29] <mmd0x01> 98.229.21.68|Fri Nov 15 03:29:34 JST 2013|c-98-229-21-68.hsd1.ma.comcast.net.|
COMCAST CABLE COMMUNICATIONS INC.
[03:29] <mmd0x01> Read error (Operation timed out) in headers.
[03:30] <mmd0x01> 207.198.124.110|Fri Nov 15 03:30:11 JST 2013||13768 | 207.198.124.0/22 | PEER1
[03:30] <mmd0x01> 2013-11-15 03:30:14 URL:http://207.198.124.110/calc.exe [1050624/1050624] -> "
[03:30] <mmd0x01> 98.229.21.68|Fri Nov 15 03:30:49 JST 2013|c-98-229-21-68.hsd1.ma.comcast.net.|
COMCAST CABLE COMMUNICATIONS INC.
[03:31] <mmd0x01> 2013-11-15 03:30:50 URL:http://98.229.21.68/calc.exe [193/193] -> "/dev/null"
[03:31] <mmd0x01> 207.198.124.110|Fri Nov 15 03:31:02 JST 2013||13768 | 207.198.124.0/22 | PEER1
[03:31] <mmd0x01> 2013-11-15 03:31:10 URL:http://207.198.124.110/calc.exe [1050624/1050624] -> "
[03:31] <mmd0x01> 207.198.124.110|Fri Nov 15 03:31:16 JST 2013||13768 | 207.198.124.0/22 | PEER1
[03:31] <mmd0x01> 2013-11-15 03:31:20 URL:http://207.198.124.110/calc.exe [1050624/1050624] -> "
[03:32] <mmd0x01> 74.135.38.33|Fri Nov 15 03:31:52 JST 2013|| | | US | MYINSIGHT.COM | INSIG
[03:32] <mmd0x01> 2013-11-15 03:32:01 URL:http://74.135.38.33/calc.exe [1050624/1050624] -> "/de
[03:33] <mmd0x01> 97.81.105.174|Fri Nov 15 03:33:03 JST 2013|97-81-105-174.dhcp.athn.ga.charter.

```

Let's Stop Payloads Distribution



Let's Stop Payloads Distribution

```

Status ##DCG893JP X ##dcg893 X ##DCG893RU X ##DCG893GE X ##DCG893PL X ##DCG893IN X
(no topic set)
[01:13] <@md8x87> Read error (Connection reset by peer) in headers.
[01:13] <@md8x87> 93.100.36.135|Tue Dec 3 01:13:08 JST 2013|93.100.36.135.pool.sknt.ru.|35807 | 93.100.0.0/17 | SKYNET-SPB | RU
SKYNET LTD.
[01:13] <@md8x87> No data received.
[01:13] <@md8x87> 93.100.36.135|Tue Dec 3 01:13:47 JST 2013|93.100.36.135.pool.sknt.ru.|35807 | 93.100.0.0/17 | SKYNET-SPB | RU
SKYNET LTD.
[01:13] <@md8x87> No data received.
[01:13] <@md8x87> 93.100.36.135|Tue Dec 3 01:13:48 JST 2013|93.100.36.135.pool.sknt.ru.|35807 | 93.100.0.0/17 | SKYNET-SPB | RU
SKYNET LTD.
[01:13] <@md8x87> Read error (Connection reset by peer) in headers.
[01:14] <@md8x87> 93.100.36.135|Tue Dec 3 01:15:00 JST 2013|93.100.36.135.pool.sknt.ru.|35807 | 93.100.0.0/17 | SKYNET-SPB | RU
SKYNET LTD.
[01:14] <@md8x87> No data received.
[01:17] <@md8x87> 93.100.36.135|Tue Dec 3 01:17:19 JST 2013|93.100.36.135.pool.sknt.ru.|35807 | 93.100.0.0/17 | SKYNET-SPB | RU
SKYNET LTD.
[01:17] <@md8x87> Read error (Connection reset by peer) in headers.
[01:17] <@md8x87> 93.100.36.135|Tue Dec 3 01:17:36 JST 2013|93.100.36.135.pool.sknt.ru.|35807 | 93.100.0.0/17 | SKYNET-SPB | RU
SKYNET LTD.
[01:17] <@md8x87> No data received.
[01:19] <@md8x87> 93.100.36.135|Tue Dec 3 01:19:48 JST 2013|93.100.36.135.pool.sknt.ru.|35807 | 93.100.0.0/17 | SKYNET-SPB | RU
SKYNET LTD.
[01:19] <@md8x87> Read error (Connection reset by peer) in headers.
[01:24] <@md8x87> 93.100.36.135|Tue Dec 3 01:24:19 JST 2013|93.100.36.135.pool.sknt.ru.|35807 | 93.100.0.0/17 | SKYNET-SPB | RU
SKYNET LTD.
[01:31] <@md8x87> 93.100.36.135|Tue Dec 3 01:32:01 JST 2013|93.100.36.135.pool.sknt.ru.|35807 | 93.100.0.0/17 | SKYNET-SPB | RU
SKYNET LTD.
[01:31] <@md8x87> Read error (Connection reset by peer) in headers.
[01:33] <@md8x87> 93.100.36.135|Tue Dec 3 01:33:33 JST 2013|93.100.36.135.pool.sknt.ru.|35807 | 93.100.0.0/17 | SKYNET-SPB | RU
SKYNET LTD.
[01:33] <@md8x87> No data received.
[01:33] <@md8x87> 93.100.36.135|Tue Dec 3 01:34:06 JST 2013|93.100.36.135.pool.sknt.ru.|35807 | 93.100.0.0/17 | SKYNET-SPB | RU
SKYNET LTD.
[01:34] <@md8x87> Read error (Connection reset by peer) in headers.

```


Let's Stop Payloads Distribution

```

webchat.freemove.net
Status ##DCG893JP x ##dgc893 x ##DCG893RU x ##DCG893GE x ##DCG893PL x ##DCG893IN x
(no topic set)
01:42] <@mmd0x02> 126.42.111.207|Tue Dec 3 00:51:23 JST 2013|softbank126042111207.bbtec.net.|1/6/6 | 126.42.0.0/16 | GI
SOFTBANKBB.CO.JP | JAPAN NATION-WIDE NETWORK OF SOFTBANK BB CORP.
01:42] <@mmd0x02> 27.135.39.215|Tue Dec 3 00:51:26 JST 2013|215.39.135.27.ap.yournet.ne.jp.|10013 | 27.132.0.0/14 | FBD
| FREEBIT CO. LTD.
01:42] <@mmd0x02> Read error (Connection reset by peer) in headers
01:42] <@mmd0x02> Read error (Operation timed out) in headers.
01:42] <@mmd0x02> 126.42.111.207|Tue Dec 3 00:51:49 JST 2013|softbank126042111207.bbtec.net.|17676 | 126.42.0.0/16 | GI
SOFTBANKBB.CO.JP | JAPAN NATION-WIDE NETWORK OF SOFTBANK BB CORP.
01:42] <@mmd0x02> 27.135.39.215|Tue Dec 3 00:51:49 JST 2013|215.39.135.27.ap.yournet.ne.jp.|10013 | 27.132.0.0/14 | FBD
| FREEBIT CO. LTD.
01:42] <@mmd0x02> 115.162.34.183|Tue Dec 3 00:51:49 JST 2013|p73a222b7.sitmnt01.ap.so-net.ne.jp.|2527 | 115.162.0.0/15
SO-NET.NE.JP | SO-NET SERVICE
01:42] <@mmd0x02> No data received.
01:42] <@mmd0x02> Read error (Connection reset by peer) in headers.
01:42] <@mmd0x02> Read error (Operation timed out) in headers.
01:42] <@mmd0x02> 126.42.111.207|Tue Dec 3 00:51:56 JST 2013|softbank126042111207.bbtec.net.|17676 | 126.42.0.0/16 | GI
SOFTBANKBB.CO.JP | JAPAN NATION-WIDE NETWORK OF SOFTBANK BB CORP.
01:42] <@mmd0x02> Read error (Connection reset by peer) in headers.
01:42] <@mmd0x02> 125.13.247.86|Tue Dec 3 00:52:54 JST 2013|125-13-247-86.rev.home.ne.jp.|9824 | 125.13.192.0/18 | ASN
TECHNOLOGYNETWORKS.COM | TECHNOLOGY NETWORKS INC.
01:42] <@mmd0x02> No data received.
01:42] <@mmd0x02> 126.42.111.207|Tue Dec 3 00:53:08 JST 2013|softbank126042111207.bbtec.net.|17676 | 126.42.0.0/16 | GI
SOFTBANKBB.CO.JP | JAPAN NATION-WIDE NETWORK OF SOFTBANK BB CORP.
01:43] <@mmd0x02> Read error (Operation timed out) in headers.
01:43] <@mmd0x02> 111.233.123.22|Tue Dec 3 00:53:14 JST 2013|22.123.233.111.ap.yournet.ne.jp.|10013 | 111.232.0.0/15 |
FREEBIT.COM | FREEBIT CO. LTD.
01:43] <@mmd0x02> No data received.
01:43] <@mmd0x02> 27.135.39.215|Tue Dec 3 00:53:20 JST 2013|215.39.135.27.ap.yournet.ne.jp.|10013 | 27.132.0.0/14 | FBD
| FREEBIT CO. LTD.
01:43] <@mmd0x02> No data received.
01:43] <@mmd0x02> 111.233.123.22|Tue Dec 3 00:53:29 JST 2013|22.123.233.111.ap.yournet.ne.jp.|10013 | 111.232.0.0/15 |

```


Summary

- Dedicated security researchers/engineers
- Detection
 - RT monitoring system
 - Daily zone files/regex
- Malware payload analysis
- Report domains to appropriate bodies, e.g. registrars ICANN, for suspension, sinkholing
- Report infected IPs to ISPs, regional CERTs & LE for cleanup



Hall of Fame

OP Kelihos #MalwareMustDie, thanks for contribution from:

Tracker:

@kellewic @VriesHd @Secluded_Memory @DhiaLite
@Set_Abominae

Intel;

@unixfreaxjp @kafeine @malwageddon

OP Stop Keli-Payloads (Netherlands/Germany, UK)

Markus Fritz, @wopot, Christiaan Beek, Dave Marcus,
@RazorEQX, Andre DiMino, Conrad Longmore

Question?