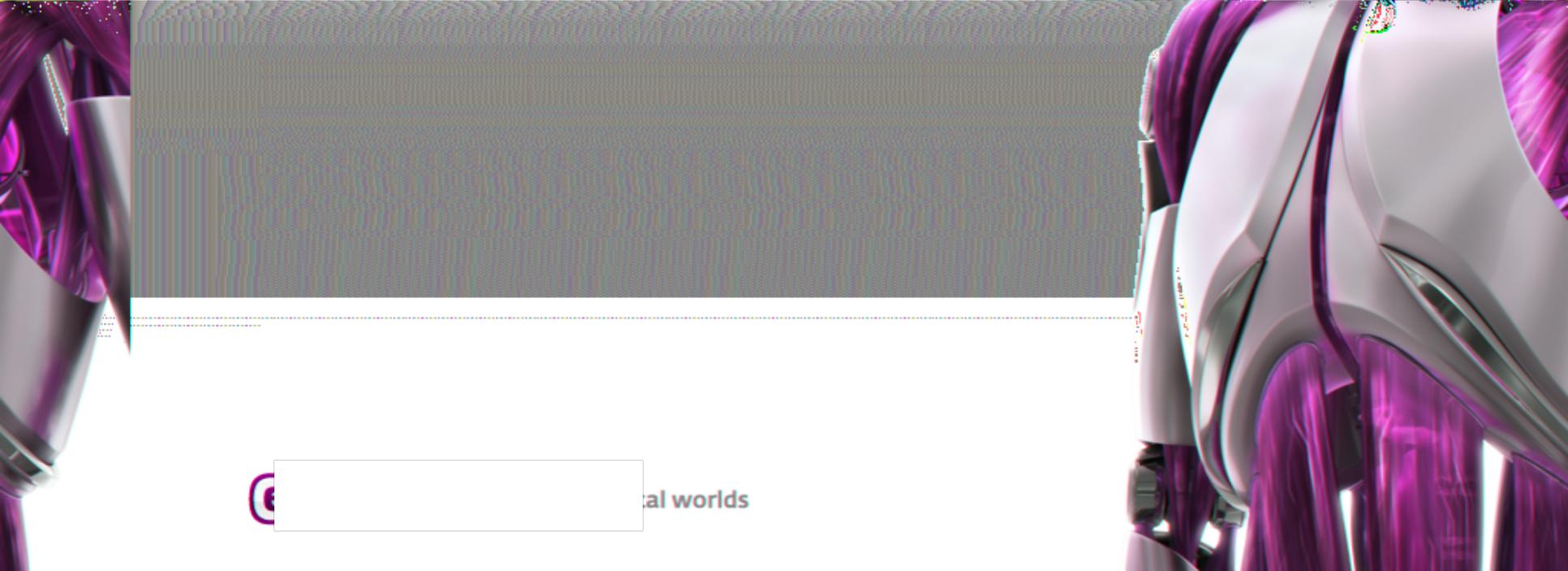
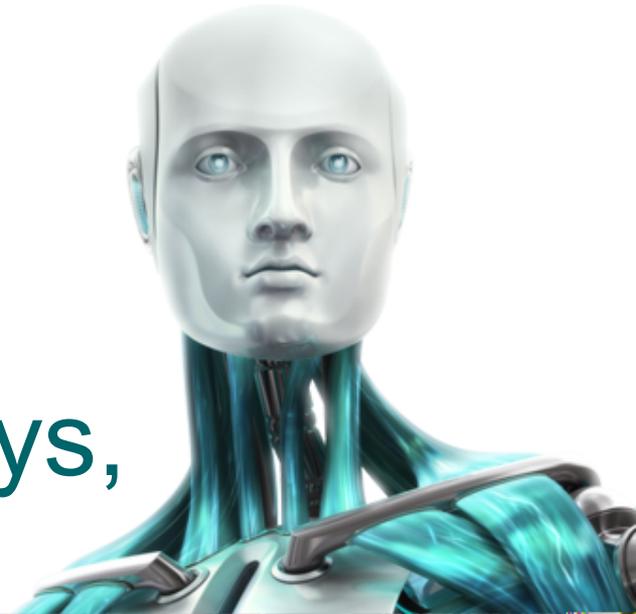


Pierre-Marc Bureau

ESET

# Same Botnet, Same Guys, New Code.



# Same Guys?

- There are less malware authors than malware samples
- Malware authors evolve over time
  - What are their motivations?
  - What is their next move?
- How are they adapting to the security industry efforts?
  - AV detection
  - Take downs

# Presentation Outline

- Win32/Kelihos
  - Software characteristics
  - Evolution
  - P2P network architecture
- Comparison with Win32/Nuwar and Win32/Waledac
  - Software
  - Network
  - Operation



Win32/Kelihos

# First Samples

Can't view this greeting? [Download Flash Player!](#)

# First Versions

#	Time	Debug Print
0	0.00000000	[2948] 14.02.2011 11:28:09 Init logging. Level=3 Log path=C:\\.
1	0.00008185	[2948] 14.02.2011 11:28:09 Client 0.0.54 started.
2	0.00013382	[2948] 14.02.2011 11:28:09 [vo]Looing for old client...
3	0.76000690	[2948] 14.02.2011 11:28:10 Looing for old client...
4	0.76011282	[2948] 14.02.2011 11:28:10 Found shared object
5	0.76025498	[2948] 14.02.2011 11:28:10 Constructed terminating object
6	0.76030499	[2948] 14.02.2011 11:28:10 Openning process...
7	0.76042289	[2948] 14.02.2011 11:28:10 getProcess Name = \\Device\\HarddiskVolume1\\Docum
8	0.76048797	[2948] ings\\Administrator\\Desktop\\flash4.exe
9	0.76054305	[2948] 14.02.2011 11:28:10 GetExitCodeProcess 259
10	0.76258993	[2948] 14.02.2011 11:28:10 TerminateProcess 1
11	1.75010931	[2948] 14.02.2011 11:28:11 Openning process...
12	1.75017750	[2948] 14.02.2011 11:28:11 Openning process failed
13	2.17856932	[2948] 14.02.2011 11:28:12 Timing zone[find_and_kill_old_clients] ms=2172
14	2.17995954	[2948] 14.02.2011 11:28:12 Autorun entry writed success.
15	2.18004060	[2948] 14.02.2011 11:28:12 Config loaded Ok. own_id=b896b535-056b-4dda-8a9
16	2.18008232	[2948] d, port = 80
17	2.18015027	[2948] 14.02.2011 11:28:12 Loaded bootstrap list:
18	2.18015027	[2948] client: 00000000-0000-0000-0000-00000
19	2.18019247	[2948] 00000000 67.160.19.3:80
20	2.18019247	[2948] client: 00000000-0000-0000-0000-000000000000 24 35 104 22

# Software Protection

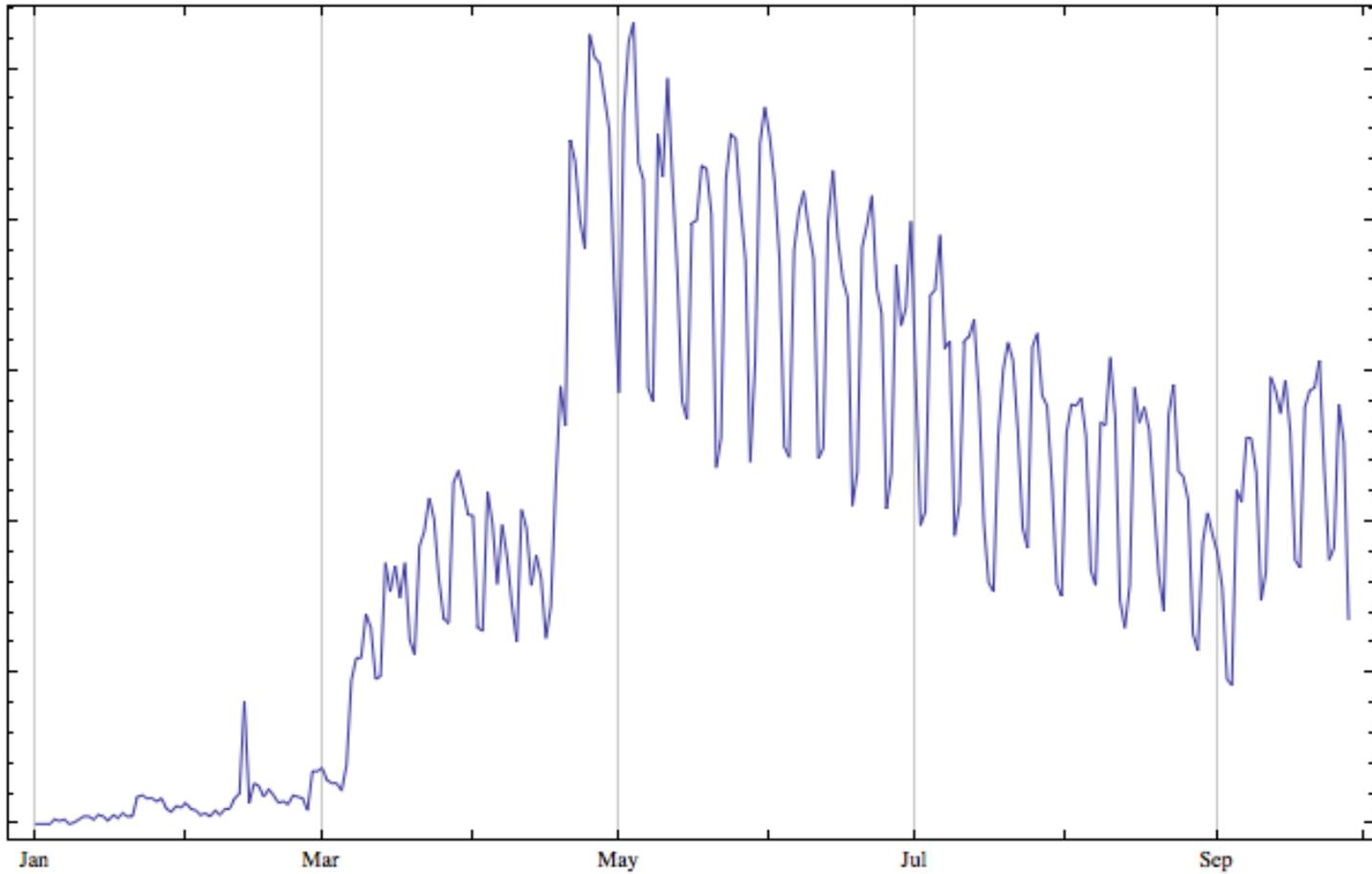
```
0090 | $ 60 | PUSHAD
0091 | . 8035 00F04900 | LEA ESI,DWORD PTR DS:[49F000]
0097 | . 6A 02 | PUSH 2
0099 | . 6A 00 | PUSH 0
009B | . 56 | PUSH ESI
009C | . E8 37010000 | CALL <JMP.&KERNEL32.LoadLibraryExA>
00A1 | . 85C0 | TEST EAX,EAX
00A3 | . 74 01 | JE SHORT client2.0049D0A6
00A5 | . C3 | RETN
00A6 | . 41 | INC EAX
```

[Flags = LOAD\_LIBRARY\_AS\_DATAF  
hFile = NULL  
FileName => "xmsiexec.exe"  
LoadLibraryExA

# LNK Exploit (CVE-2010-2568)

```
.005BFA20: 99 50 46 00-9E 51 46 00-2B 52 46 00-4D 52 46 00  ÖPF xQF +RF MRF
.005BFA30: 73 61 73 00-74 79 70 65-3D 00 00 00-44 72 69 76  sas type=  Driv
.005BFA40: 65 20 20 00-67 67 6C 31-2E 74 6D 70-00 00 00 00  e  ggl1.tmp
.005BFA50: 67 67 6C 2E-74 6D 70 00-53 68 6F 72-74 63 75 74  ggl.tmp Shortcut
.005BFA60: 20 74 6F 20-67 6F 6F 67-6C 65 2E 6C-6E 6B 00 00  to google.lnk
.005BFA70: 43 6F 70 79-20 6F 66 20-53 68 6F 72-74 63 75 74  Copy of Shortcut
.005BFA80: 20 74 6F 20-67 6F 6F 67-6C 65 2E 6C-6E 6B 00 00  to google.lnk
.005BFA90: 43 6F 70 79-20 6F 66 20-43 6F 70 79-20 6F 66 20  Copy of Copy of
.005BFAA0: 53 68 6F 72-74 63 75 74-20 74 6F 20-67 6F 6F 67  Shortcut to goog
.005BFAB0: 6C 65 2E 6C-6E 6B 00 00-92 BB 45 00-25 6F 46 00  le.lnk  ÅŋE %oF
.005BFAC0: 76 B1 41 00-60 6F 46 00-69 79 46 00-A1 BB 45 00  vA `oF iyF íŋE
```

# Propagation Evolution



# Spam Engine

Received: from unknown (HELO %^C6%^|^%.%^|^%.%^|^%.%^|^%^%) ([%^V6%^])  
by %^A^% with ESMTP; %^D%^R20-300^%^%  
Message-ID: <%^O%^V6%^:%^R3-50^%^%>  
From: "%^Fmynames^% %^Fsurnames^%" <%^Fnames^%@%^Fdomains^%>  
To: <%^0^%>  
Subject: You got to see this market alert  
Date: %^D-%^R30-600^%^%  
MIME-Version: 1.0  
Content-Type: text/plain;  
format=flowed;  
charset="%^Fcharset^%";  
reply-type=original  
Content-Transfer-Encoding: 7bit  
X-Priority: 3  
X-MSMail-Priority: Normal  
X-Mailer: Microsoft Outlook Express 6.00.%^C7%^Foutver.6^%^%  
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.%^V7^%

Silver demand will be greater than supply for years to come, no matter which way the economy turns, start researching SURE! The stock's 575% climb so far this year is merely a preview of the staggering profits about to be handed to you.

Tick: SURE  
Priced at: 0.43  
The target is: 2.50

It's time to buy. Monday, September 12th.

# Spam

ALL PRODUCTS LIST | ABOUT US | HOW TO ORDER | F.A.Q. | CONTACT US

USD GBP CAD EUR AUD CHF

### Men's Health

- ▶ [Viagra](#)
- ▶ [Cialis](#)
- ▶ [Viagra Super Active+](#)
- ▶ [Viagra Professional](#)
- ▶ [Levitra](#)
- ▶ [Cialis Super Active+](#)
- ▶ [Viagra Super Force](#)
- ▶ [Cialis Soft Tabs](#)
- ▶ [Cialis Professional](#)
- ▶ [Viagra Soft Tabs](#)
- ▶ [Propecia](#)
- ▶ [Maxaman](#)
- ▶ [Super Active ED Pack](#)
- ▶ [VPXL](#)
- ▶ [View all products](#)

### Most Popular Products

- Viagra as low as CAD 1.94** [more info](#) [order now](#)

*Generic Viagra, containing Sildenafil Citrate, enables many men with erectile dysfunction to achieve or sustain an erect penis for sexual activity. Since becoming available Viagra has been the prime treatment for erectile dysfunction.*
- Cialis as low as CAD 1.84** [more info](#) [order now](#)

*Cialis is a highly effective orally administered drug for treating erectile dysfunction, more commonly known as impotence. Recommended for use as needed, Cialis can also be used as a daily medication.*
- Viagra Super Active+ as low as CAD 2.93** [more info](#) [order now](#)

*Viagra Super Active represents the fourth generation of phosphodiesterase inhibitors. This new formulation of a world-known medication provides even more powerful penis blood circulation, increased stamina and sensitivity to stimulation.*
- Viagra Professional as low as CAD 4.04** [more info](#) [order now](#)

*Viagra Professional is a clinically tested enhanced prescription drug used to treat erection difficulties. Activating the natural blood flow, it provides sustained erection, accelerated recovery from prior sexual*

# Spam

JOHN PERSON'S

## Bottom-Line

FINANCIAL AND FUTURES NEWSLETTER

UP 575% SINCE JANUARY

### SONORA RESOURCES IS JUST STARTING ITS SURGE

*Sonora Resources (SURE.OB) is an **immediate buy**.*  
The stock's 575% climb so far this year is merely a preview of the staggering profits about to be handed to you.

Fellow Investor,

Silver is red hot -- 4 times more profitable than gold.

The yellow metal jumped 90% from November 2008 to April 2011. But silver surged FOUR TIMES HIGHER -- up 390% in that same span.

Asset	Return (%)
SILVER	400%
GOLD	90%

Nov 2008 - Apr 2011.

# Pump and Dump



# Canceling Transactions



OTCBB.com popup - Google Chrome

otcbb.com/asp/popup.asp

## Spam, Faxes and Pop-Up Ads

**If you are the recipient of email spam, unwanted faxes or pop up ads, please read the following:**

The OTCBB does NOT under any circumstances send or support in any way the generation of unsolicited messages to any person's PC, fax machine or email address. Most importantly, we do not advertise or promote any individual stocks. The OTCBB website is an informational website maintained by The Nasdaq Stock Market Inc. for investors and traders.

What you can do:

The OTCBB is unable to prevent third parties from referring people to the OTCBB website. You can prevent email spam, unwanted faxes and pop-up ads by doing the following:

- Report email spam to the Federal Trade Commission ([www.ftc.gov](http://www.ftc.gov)) or send a copy of the spam to your ISP's abuse desk.
- Complaints about unsolicited faxes should be directed to the Federal Communications Commission. You can file a complaint online at the FCC's website ([www.fcc.gov](http://www.fcc.gov)).
- Install firewall software on your computer to eliminate pop-up ads.

For more information regarding these issues and ways you can report it to the proper authorities, please see the following link: <http://www.otcbb.com/help/spam.stm>.

Submit



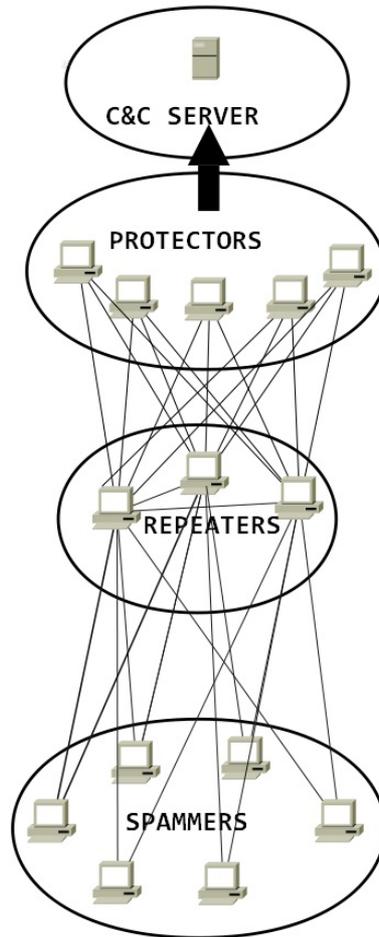
# Peer-to-peer network

# Packet Content

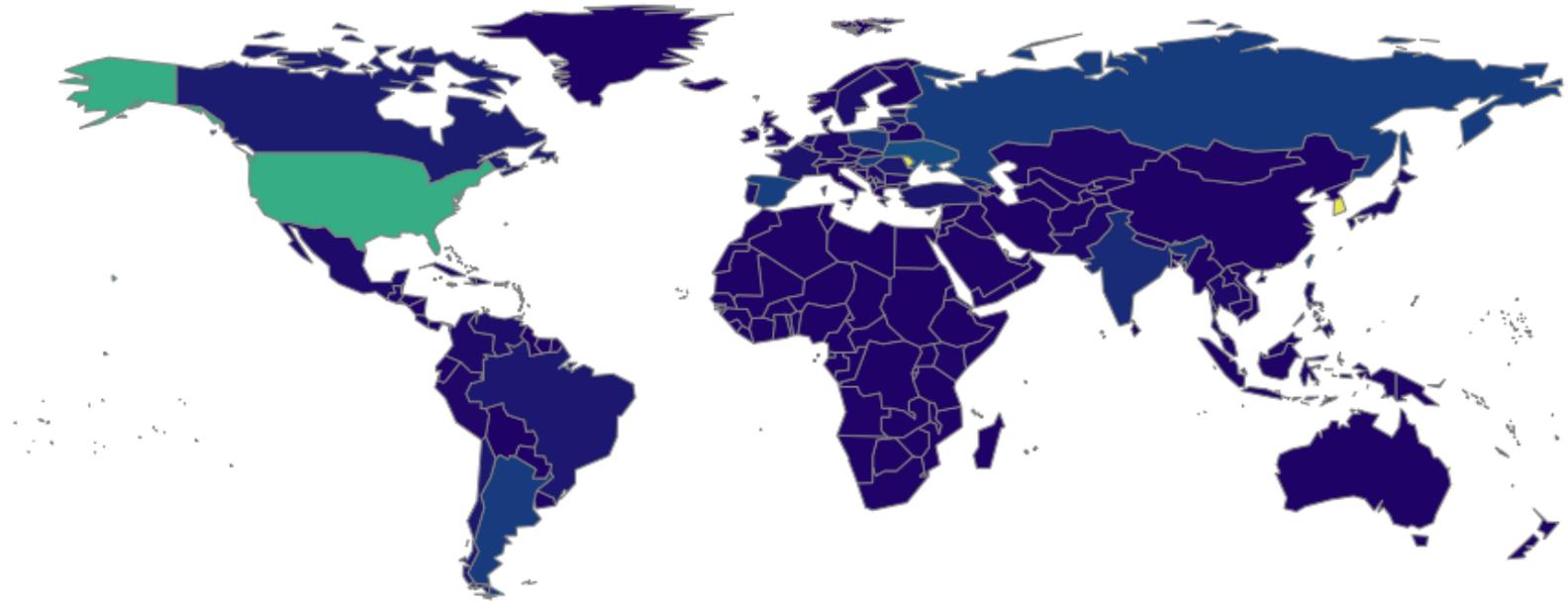
- TCP Port 80
- GET Request with data appended
- Zlib compression
- Blowfish + DES + Blowfish (?!)

```
00000000 10 d3 5a 05 15 4a 05 01 e0 07 5e 7d 3e c4 a6 7d
00000010 11 74 b9 82 01 4f 72 05 99 99 00 00 00 00 00 00
00000020 00 b0 bb 70 00 0c ec ce 67 35 35 f9 04 b0 fe 88 10 d3 5a 05 :head1
00000030 f4 a8 4f f4 27 fa 12 10 89 ba b3 4e e7 d7 30 ff 15 4a 05 01 :head2
00000040 fd ca f1 7f 04 68 7d 97 7f 9a 5d cf 76 71 1a df e0 07 5e 7d :a
00000050 ba 4d b7 55 ba e4 fb c5 bf 95 64 b2 01 d6 84 09 3e c4 a6 7d :b
00000060 d6 ec 8b 37 65 ba d5 5d ba 69 e4 f7 05 2c 3c 58 11 74 b9 82 :c
00000070 bf c3 bd 16 b6 63 26 a1 92 e8 20 80 73 1e d6 a4 01 4f 72 05 :d
00000080 42 1c f8 fd 16 0f eb bc 5c ab be ad 96 48 b0 dd 99 99 00 00 :size
00000090 8e 2b b8 6a 8f 7b 4a ac 74 d7 08 50 07 71 eb 6a 00 00 00 00 :e
00000a00 db 8d b3 1f 95 a8 ce 33 0f 25 88 dc c8 a7 18 fe 00 b0 bb 70 :f
00000b00 5d e4 15 b8 ee c2 dc 87 dd a3 f8 d4 c1 fb 52 24
00000c00 a4 da 23 77 a5 38 3d 96 70 a7 49 0b f0 e6 77 13
00000d00 7d dd 69 e9 36 17 bc aa db 8f 3c f3 43 0d 91 17
00000e00 f6 1c fd 75 85 ea 7a b0 64 ff 57 f7 6c 21 58 43
00000f00 42 a0 84 8a ee 14 ba 31 5e 82 78 67 3c 0d b1 28
00001000 d9 b0 d3 54 5f e9 06 9b 5a d1 ed 43 bf 7b 60 a7
```

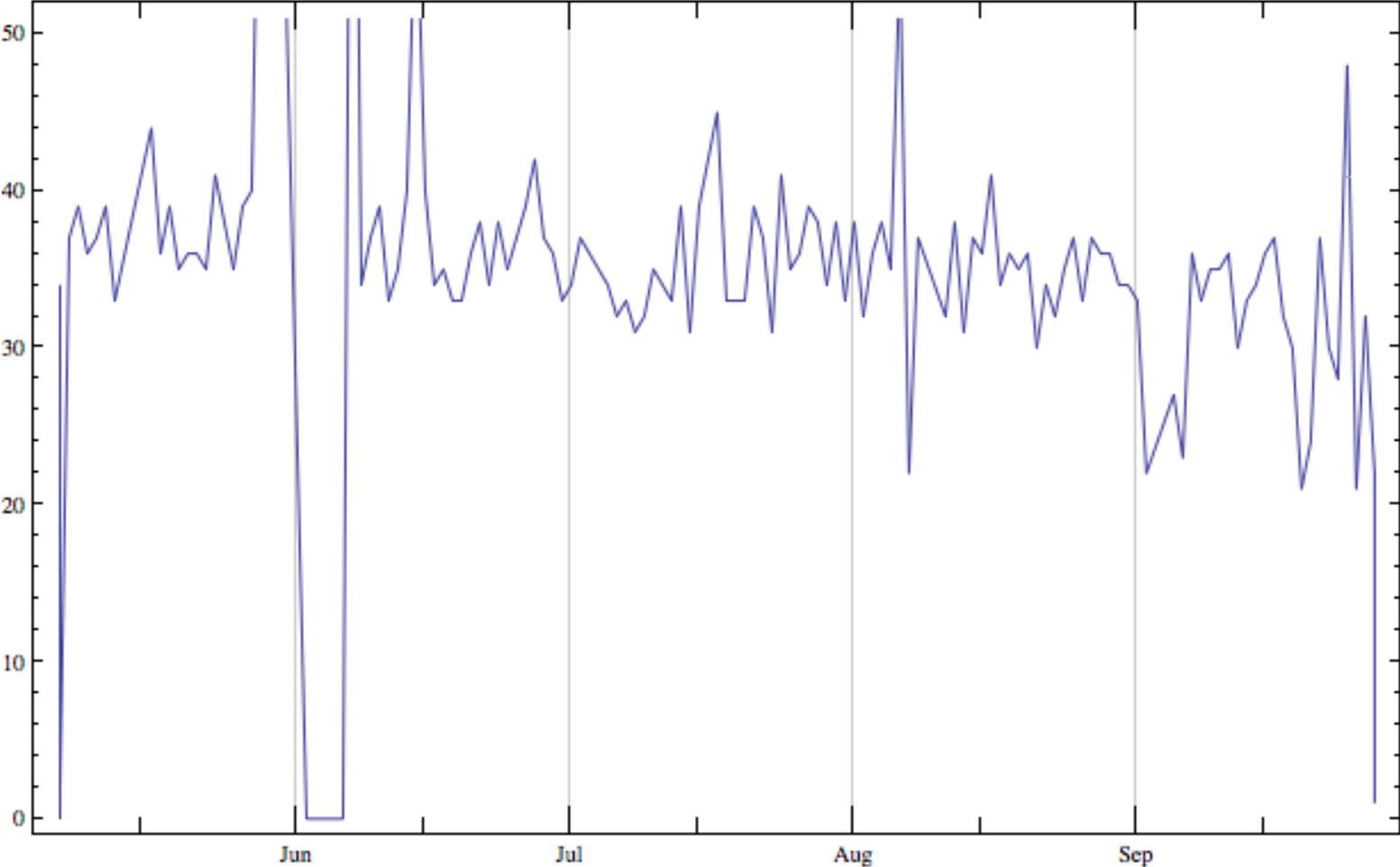
# Botnet Architecture



# Geographic Distribution of Peers



# Operation b79

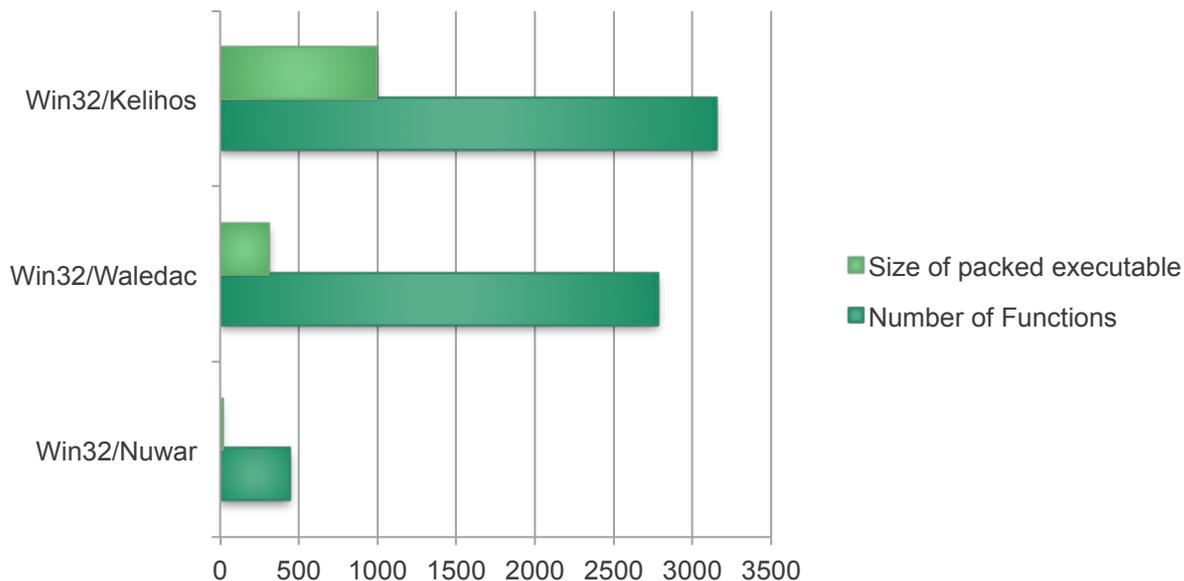




Win32/Kelihos, Win32/Waledac, Win32/Nuwar

# Binary Comparison

	Number of Functions	Size of packed executable
Win32/Nuwar	438	15K
Win32/Waledac	2778	305K
Win32/Kelihos	3145	988K

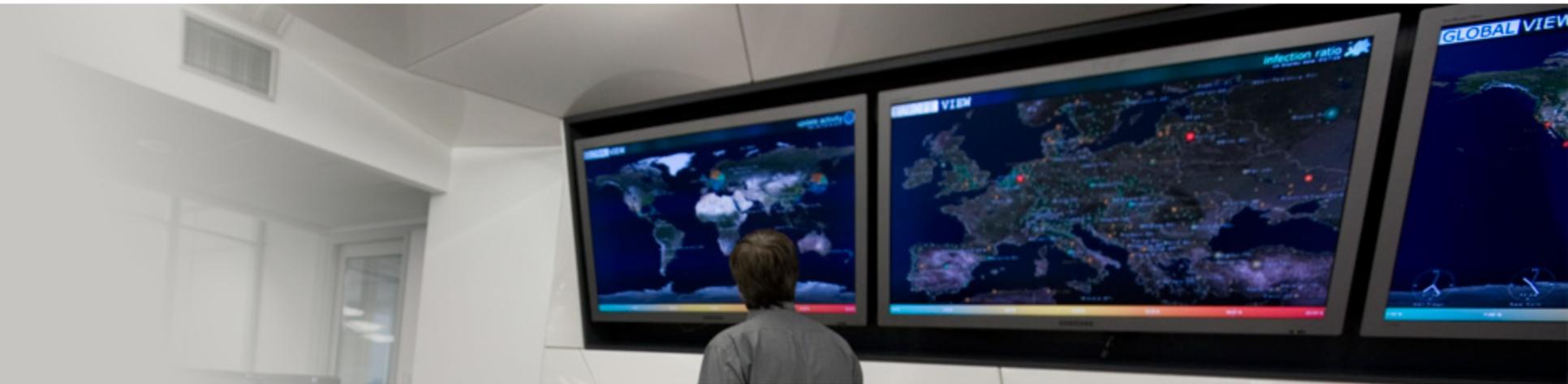


# Functionalities Comparison

	<b>Win32/Nuwar</b>	<b>Win32/Waledac</b>	<b>Win32/Kelihos</b>
<b>Propagation</b>	Spam & Links	Spam & Links	Spam & Links
<b>Information Stealing</b>		FTP / SMTP	FTP / SMTP
<b>Fast Flux</b>	X	X	X
<b>Kernel Mode Component</b>	X		
<b>Persistence</b>	Registry Key	Registry Key	Registry Key
<b>Spamming</b>	Pump and dump Pharmaceutical	Pharmaceutical	Stock Pharmaceutical

# Peer-to-peer Comparison

	<b>Win32/Nuwar</b>	<b>Win32/Waledac</b>	<b>Win32/Kelihos</b>
<b>Peer-to-peer protocol</b>	Kademlia	XML over HTTP	Serialized over HTTP
<b>Peer-to-peer network traffic</b>	UDP, variable port	TCP 80	TCP 80
<b>Peer-to-peer protection</b>	XOR	Zlib + AES + base64	Zlib + DES + blowfish
<b>Peer-to-peer "keys"</b>	Static	Rotating	Static
<b>Multi Tiered Architecture</b>	X	X	X



## Same Guys?

- Same features, different code
- Same business partners
- Different coding partners?
- Often trying new things, not really learning



## Conclusions

- Could be much worst
- As long as there is money and freedom, it will continue.
- Malware operator does not seem affected by take down efforts of the security industry.



## Credits

- Benjamin Vanheuverzwijn
- Sébastien Duquette
- David Gabris



Thank you!