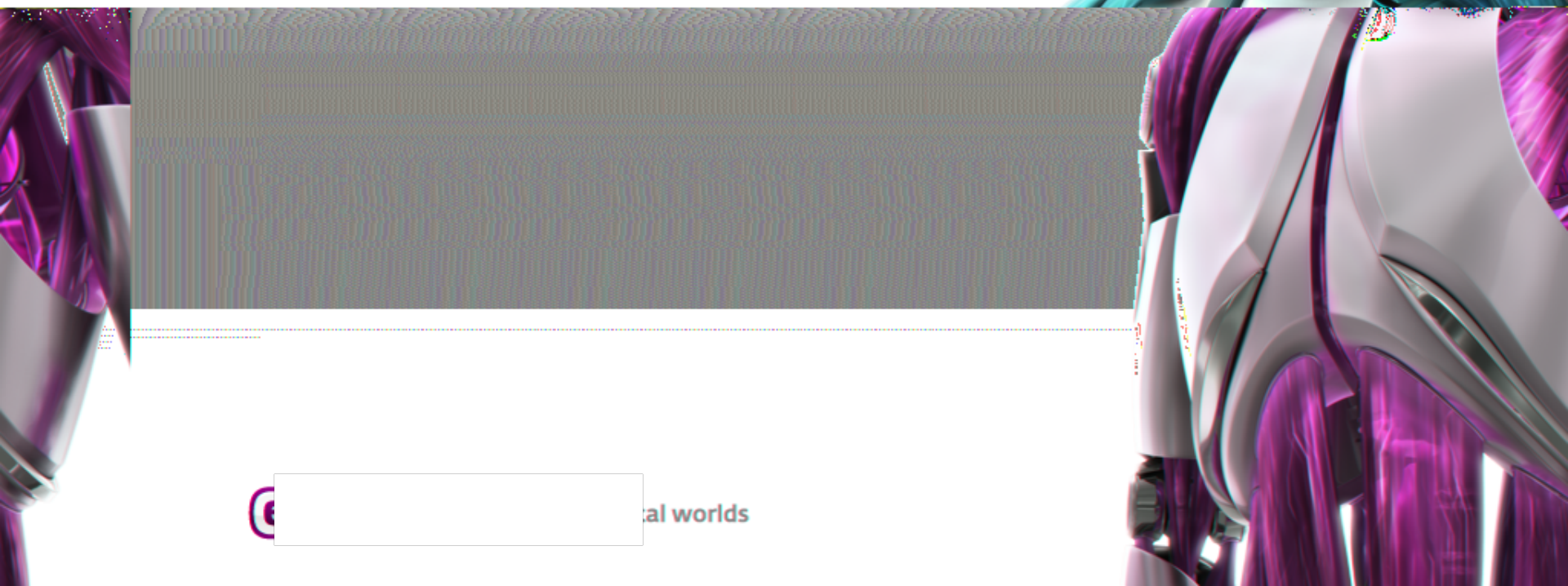
Pierre-Marc Bureau

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

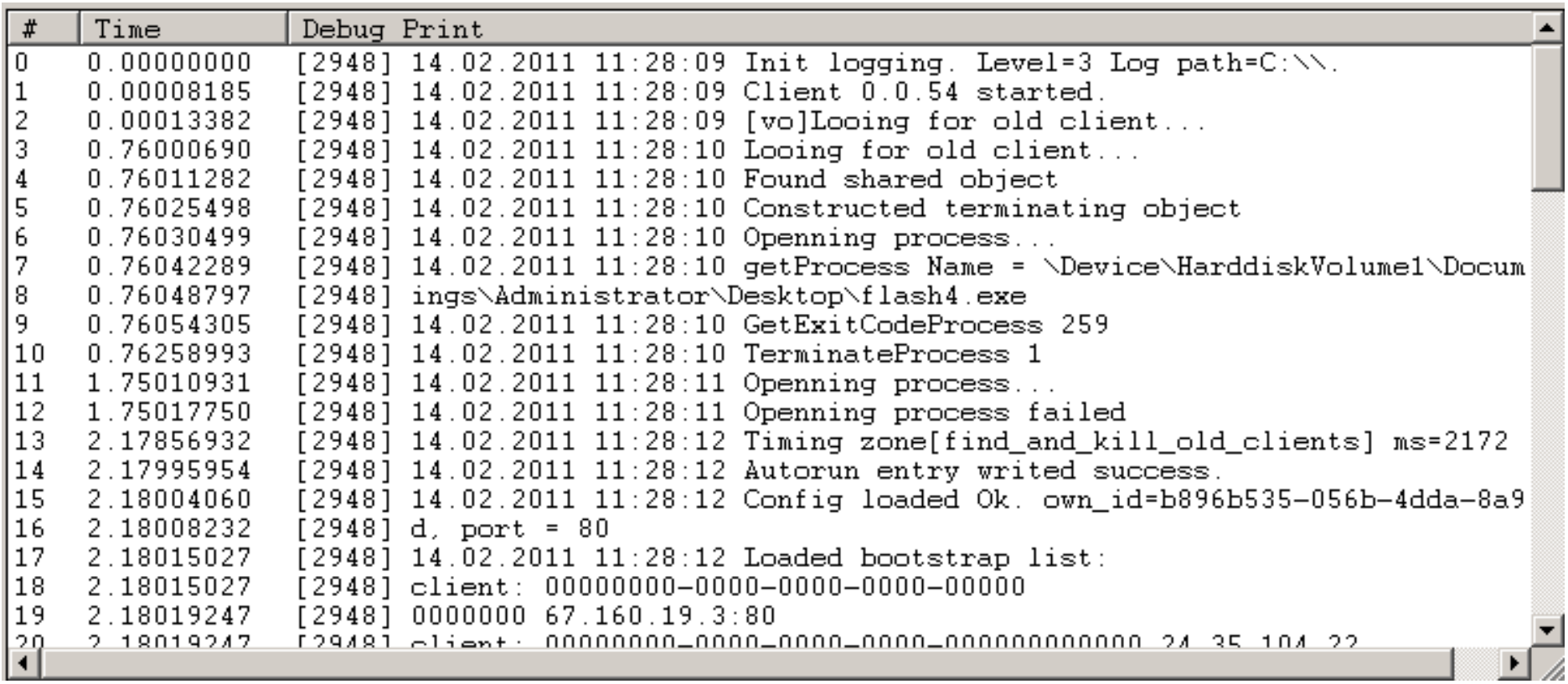
Presentation Outline

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

Win32/Kelihos

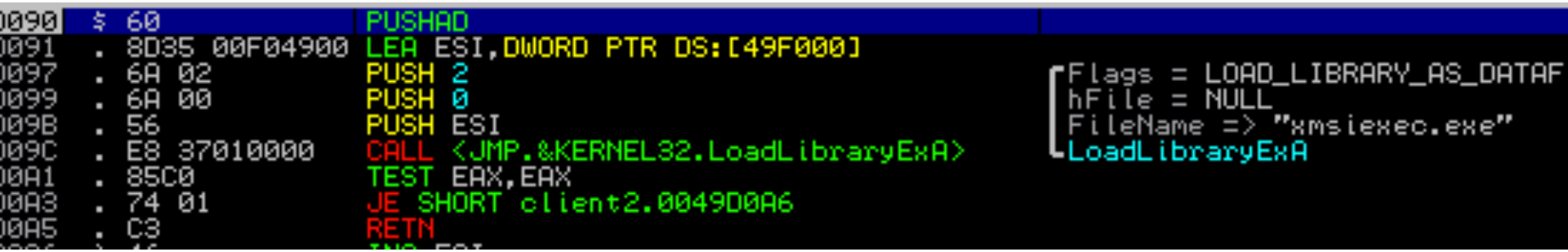
First Samples

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] 0000000 67.160.19.3:80
20	2.18019247	[2948] client: 00000000-0000-0000-0000-000000000000 24.35.104.22

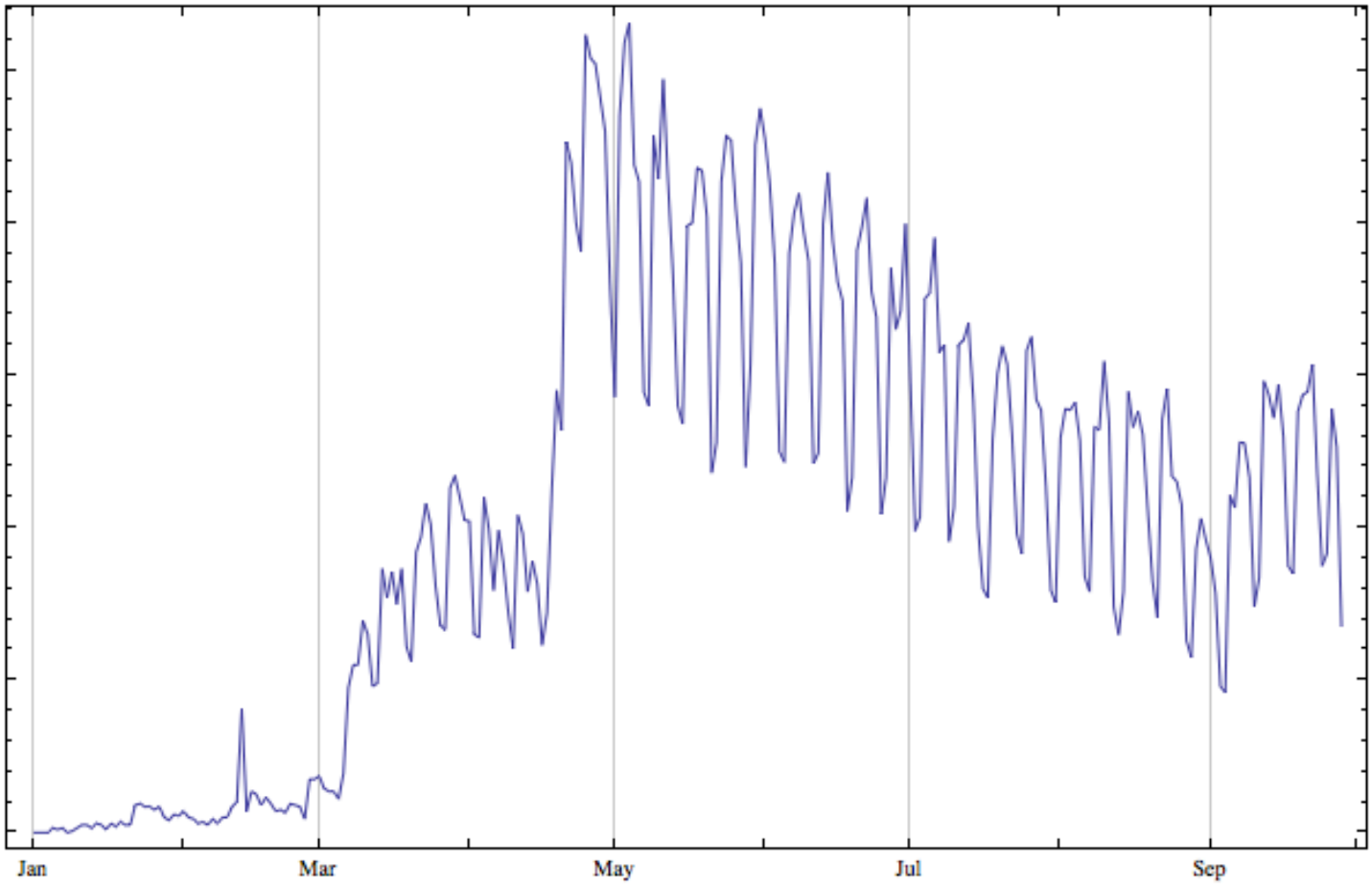
Software Protection



LNK Exploit (CVE-2010-2568)

```
.005BFA20:  99 50 46 00-9E 51 46 00-2B 52 46 00-4D 52 46 00  ÖPF ×QF +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  ÆE %oF
.005BFAC0:  76 B1 41 00-60 6F 46 00-69 79 46 00-A1 BB 45 00  v▒A `oF iyF íE
```

Propagation Evolution



Spam Engine

```
Received: from unknown (HELO %^C6%^I^%.%^I^%.%^I^%.%^I^%^%) ([%^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 se e 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 S URE! The stock's 575%
climb so far this year is merely a preview of the staggering profits about
to be handed to you.

Tick: S URE
Priced at: 0.43
The target is: 2.50

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

Spam


MyCanadianPharmacy
WE SHIP TO ALL DESTINATIONS WORLDWIDE!
ALL PRODUCTS LIST
ABOUT US
HOW TO ORDER
F.A.Q.
CONTACT US
HAPPY VALENTINE'S DAY!
$74.95
CIALIS + VIAGRA
POWERPACK
ORDER NOW
EXPERIENCE CELEBRATORY
DISCOUNTS NOW!
USD GBP CAD EUR AUD CHF
Enter product name
search
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

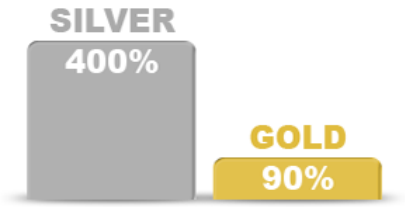
SONORA RESOURCES IS JUST STARTING ITS SURGE

***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.



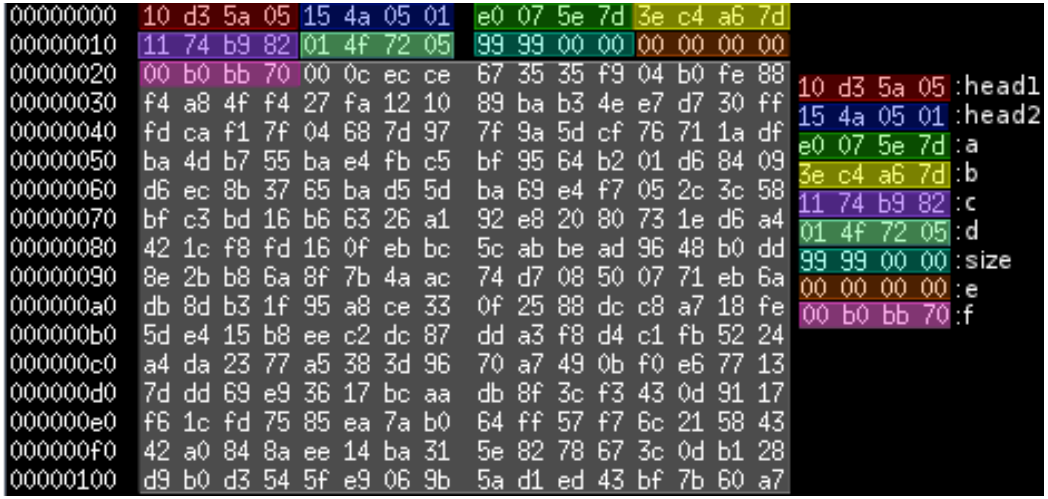
Pump and Dump

Canceling Transactions

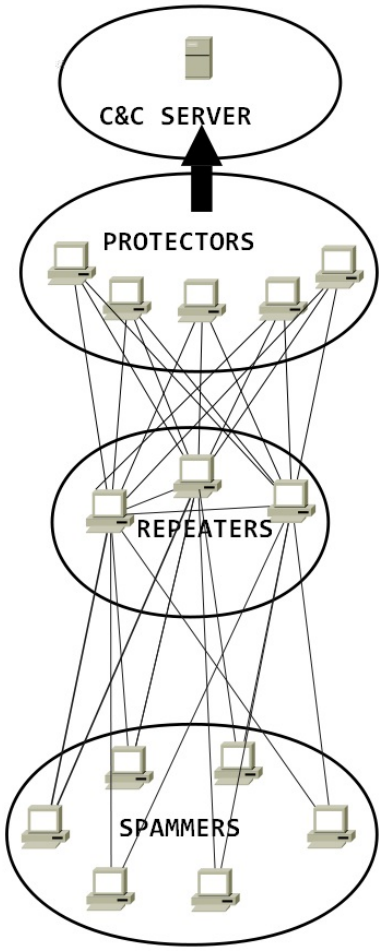
Peer-to-peer network

Packet Content

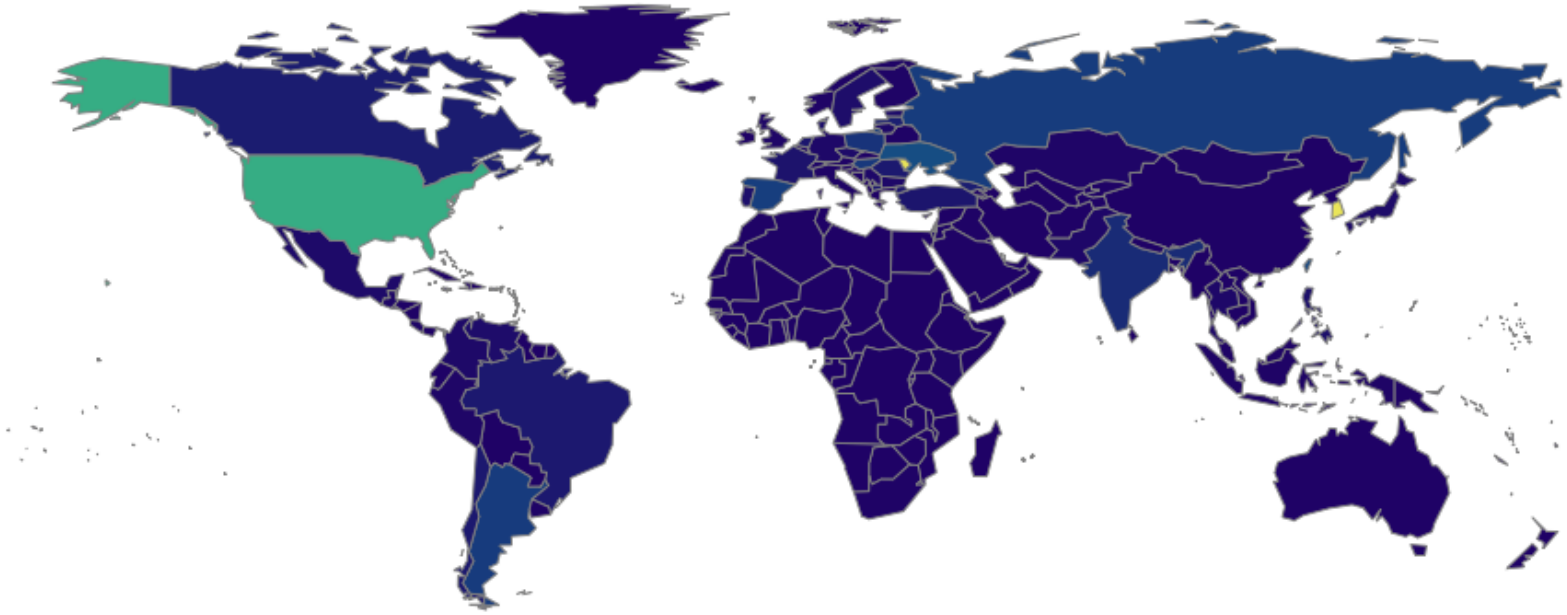
- TCP Port 80
- GET Request with data appended
- Zlib compression
- Blowfish + DES + Blowfish (?!)



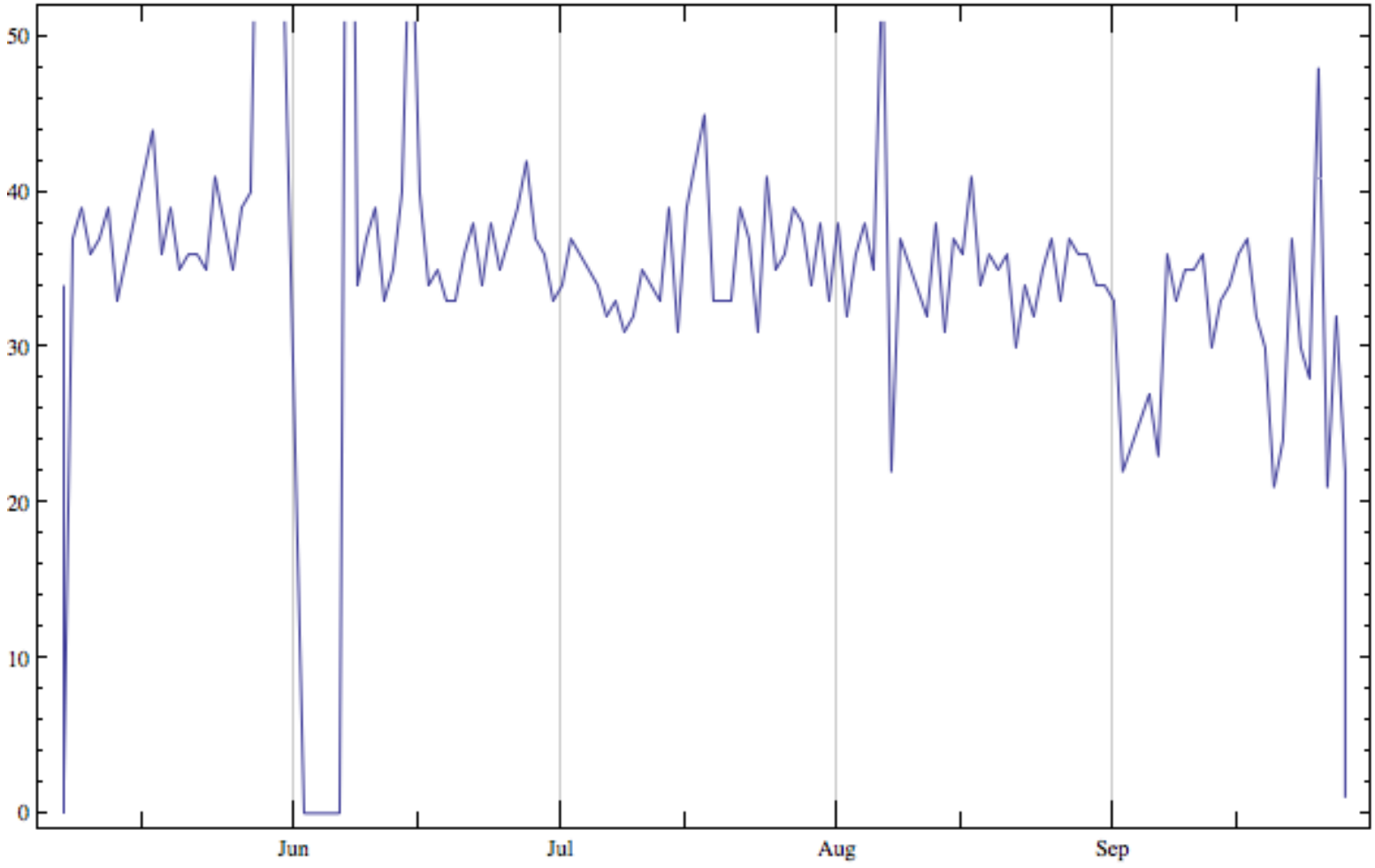
Botnet Architecture



Geographic Distribution of Peers



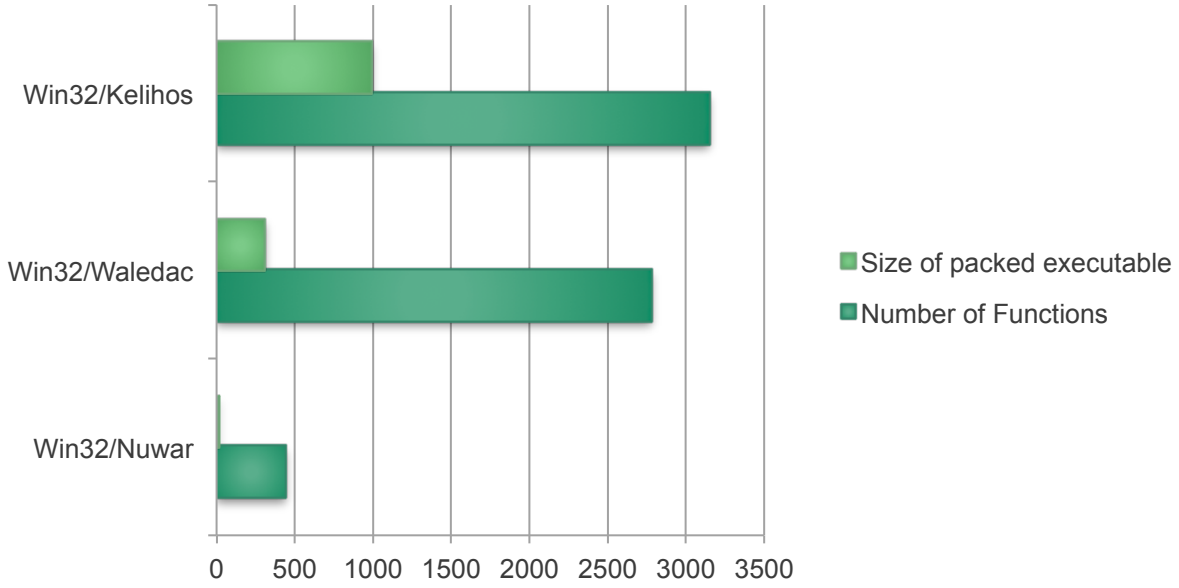
Operation b79



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

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

Peer-to-peer Comparison

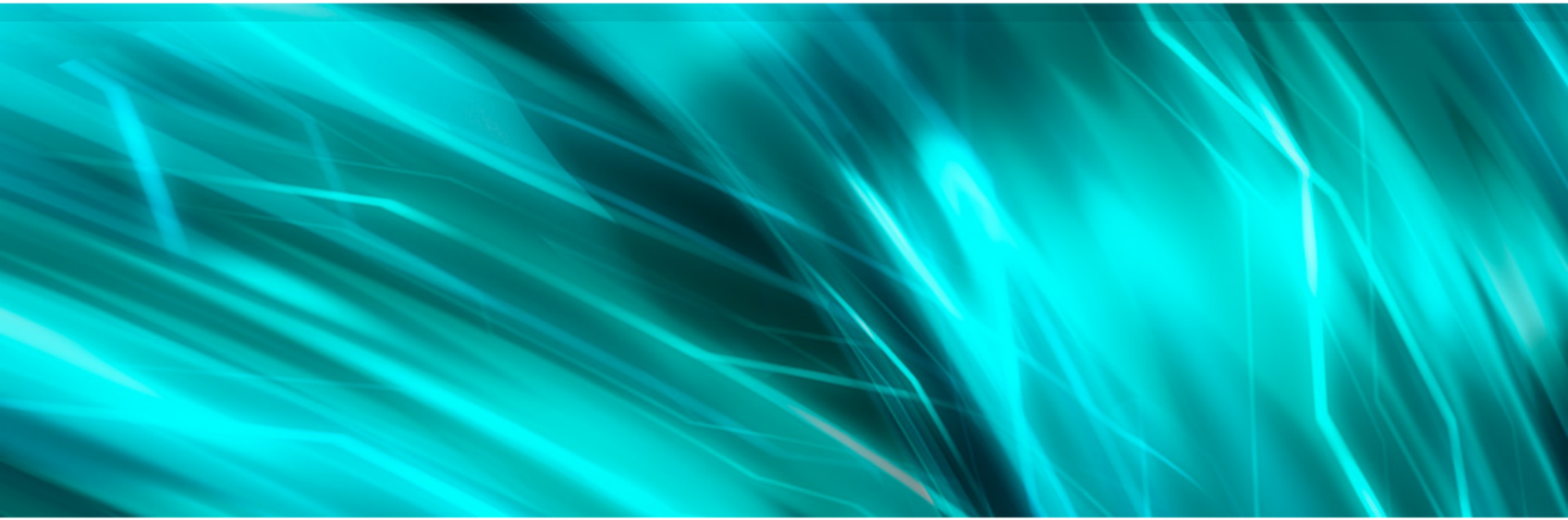
	Win32/Nuwar	Win32/Waledac	Win32/Kelihos
Peer-to-peer protocol	Kademlia	XML over HTTP	Serialized over HTTP
Peer-to-peer network traffic	UDP, variable port	TCP 80	TCP 80
Peer-to-peer protection	XOR	Zlib + AES + base64	Zlib + DES + blowfish
Peer-to-peer "keys"	Static	Rotating	Static
Multi Tiered Architecture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

Thank you!