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!
<table>
<thead>
<tr>
<th>#</th>
<th>Time</th>
<th>Debug Print</th>
</tr>
</thead>
</table>
| 0  | 0.0000000000     | [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]OoOing 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 Opening 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                              |
| 10 | 0.76258993       | [2948] 14.02.2011 11:28:10 TerminateProcess 1                              |
| 11 | 1.75010931       | [2948] 14.02.2011 11:28:11 Opening process...                              |
| 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: 00000000-0000-0000-0000-0000000000000000000000000000000000000000 |
Software Protection

```
090  60: PUSHAD
091  8D35 00F04900: LEA ESI, DWORD PTR DS:[49F000]
097  6A  02: PUSH 2
099  6A  00: PUSH 0
09B  56: PUSH ESI
09C  E8 37010000: CALL <JMP.&KERNEL32.LoadLibraryExA>
0A1  85C0: TEST EAX, EAX
0A5  74  01: JE SHORT client2.0049D0A6
0A6  C3: RETN
```

Flags = LOAD_LIBRARY_AS_DATAFILE
hFile = NULL
FileName = "xmsiexec.exe"
LoadLibraryExA
LNK Exploit (CVE-2010-2568)
Propagation Evolution
Spam Engine

Received: from unknown (HELO %C6%l%m.%l%m.%l%m.%l%m.%l%m.%l%m.%l%m.%l%m.) ([%V6%])
        by %A% with ESMTP; %D%R20-300%A%
Message-ID: <%^O%V6%R3-50%A%>
From: "%^Fmynames% %^Fsurnames%" <%^Fnames%@%^Fdomains%>
To: <%^O%>
Subject: You got to see this market alert
Date: %D-%R30-600%A%
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%A%
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.
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
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) 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).
- 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.htm.
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

<table>
<thead>
<tr>
<th></th>
<th>Number of Functions</th>
<th>Size of packed executable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Win32/Nuwar</td>
<td>438</td>
<td>15K</td>
</tr>
<tr>
<td>Win32/Waledac</td>
<td>2778</td>
<td>305K</td>
</tr>
<tr>
<td>Win32/Kelihos</td>
<td>3145</td>
<td>988K</td>
</tr>
</tbody>
</table>

![Bar chart showing the comparison between Win32/Nuwar, Win32/Waledac, and Win32/Kelihos in terms of number of functions and size of packed executable.](chart.png)
# Functionalities Comparison

<table>
<thead>
<tr>
<th></th>
<th>Win32/Nuwar</th>
<th>Win32/Waledac</th>
<th>Win32/Kelihos</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Propagation</strong></td>
<td>Spam &amp; Links</td>
<td>Spam &amp; Links</td>
<td>Spam &amp; Links</td>
</tr>
<tr>
<td><strong>Information Stealing</strong></td>
<td>FTP / SMTP</td>
<td>FTP / SMTP</td>
<td>FTP / SMTP</td>
</tr>
<tr>
<td><strong>Fast Flux</strong></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Kernel Mode Component</strong></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Persistence</strong></td>
<td>Registry Key</td>
<td>Registry Key</td>
<td>Registry Key</td>
</tr>
<tr>
<td><strong>Spamming</strong></td>
<td>Pump and dump</td>
<td>Pharmaceutical</td>
<td>Stock Pharmaceutical</td>
</tr>
</tbody>
</table>
# Peer-to-peer Comparison

<table>
<thead>
<tr>
<th></th>
<th>Win32/Nuwar</th>
<th>Win32/Waledac</th>
<th>Win32/Kelihos</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Peer-to-peer protocol</strong></td>
<td>Kademlia</td>
<td>XML over HTTP</td>
<td>Serialized over HTTP</td>
</tr>
<tr>
<td><strong>Peer-to-peer network traffic</strong></td>
<td>UDP, variable port</td>
<td>TCP 80</td>
<td>TCP 80</td>
</tr>
<tr>
<td><strong>Peer-to-peer protection</strong></td>
<td>XOR</td>
<td>Zlib + AES + base64</td>
<td>Zlib + DES + blowfish</td>
</tr>
<tr>
<td><strong>Peer-to-peer “keys”</strong></td>
<td>Static</td>
<td>Rotating</td>
<td>Static</td>
</tr>
<tr>
<td><strong>Multi Tiered Architecture</strong></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
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!