Targeted Trojans and Industrial Espionage
Alex Shipp, Imagineer
Agenda

• Typical attack
• Patterns
• Predictions
• Metrics
The MessageLabs Global Infrastructure currently spans 13 data centers across four continents and is comprised of regional clusters of multiple data centers and mail processing facilities.

This architecture is load balanced to provide enormous processing power and complete failover protection and is backed up by strong service level agreements for network availability and email loss protection.

MessageLabs also maintains nine regional offices in eight countries around the world for localized sales, partner management and service & support.
• 0.001% of our malware capture is unlike the rest

• 'Professional' targeted malware

• Send to small number of target recipients, typically < 10
Number of emails per attack, May 2005- May 2006

- Keep infected machines owned
- Keep exploit secret
Typical botnet seeding

Comparison with typical botnet creation seeding
Social Engineering
Sample subject lines

Avian Influenza -Situation in Thailand
Bird flu’s truth in mylasia
Center for European Policy Studies’ Commentary
Challenge of developing China’s Defense
China Hosts a 2nd Taiwan Party Head
China says U.S. & EU textile issues ‘very serious’
China-Iran-Russia alliance, the counterpunch to
Washington’s global ambitions
Chinese army enters into Indian territory
CSIS: Preventing Nuclear Terrorism
Disgraceful Behavior Of Russian
ECMT-Access and Inclusion Draft Summary Record
FBI Arrests Russian U.N. Official
FDC Internet Conference Berlin
Targeted Trojans – Attachment Types

Breakdown of attachments used in attacks
May 2005 - May 2006

- doc, 206, 69%
- chm, 62, 21%
- exe, 31, 10%

- Breakdown has changed following the paper
  - PPT and XLS also common
Military, pharmaceutical, petrochemical and legal organisations organizations targeted with crafted word documents which drop and run remote control software.

1 recipient per target.

18-Nov-2005

Emails came from IP belonging to Tianjin Province of China

From Alan Chernoff CNN:

54 guns found in teen's home

LITITZ, Pennsylvania (CNN) -- Police said Thursday they found 54 firearms and ammunition at the Pennsylvania home of Daniel Ludwig, the 18-year-old accused of killing his girlfriend's parents.
1-Dec-2005

Human rights organizations targeted with crafted word documents which drop and run downloader.

1-2 recipients per target. Came from IP in China.
6-Dec-2005

Human rights organizations targeted with crafted MS Help files which drops and runs a web proxy.

1-2 recipients per target. Came from IP in Western Australia.
6-Dec-2005

Same human rights organizations targeted with crafted word documents which drop and run downloader.

1-2 recipients per target. Came from same IP in Western Australia.
Getting into the Organisation

• Typical example

Internet Company

Interesting.doc

Company

Interesting.doc

Firewall, Email Gateway, Anti-virus

THE TIMES OF INDIA
Monday, June 27, 2005

China's new JL-2 missile prevents US from the Taiwan affairs

China has successfully flight-tested a submarine-launched missile that U.S. officials say marks a major advance in Beijing's long-range nuclear program. The Bush administration has expressed new worry about China's military buildup.

The JL-2 missile was launched from the new submarine, known as the Type 094, and a U.S. official familiar with it.

(Details in the attachment)
Typical example of exploit in targeted malware

- OLE Header
- Directory
- Stream 1
- Stream 2
- Stream n
- Buffer overrun
- mov eax, [ecx]
- mov ebx, [eax]
- call SaveFile

Hidden EXE
Typical example of exploit in targeted malware

CHM Headers
Directory
Draft Agenda.hhc
Draft Agenda.hhk
Draft Agenda.htm
Exploit
<object codebase="update.exe">
Update.exe

EXE activated
Typical example of exploit in targeted malware (continued)

- Malicious EXE then typically downloads more components
  - Network may be compromised
  - Information may be leaked
  - Corporate espionage
## Targets

<table>
<thead>
<tr>
<th>Date</th>
<th>Attack vector</th>
<th>Targets</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>01 Nov 2005</td>
<td>MS Word</td>
<td>ISP</td>
<td>Hong Kong</td>
</tr>
<tr>
<td>05 Nov 2005</td>
<td>MS Word</td>
<td>Education</td>
<td>US</td>
</tr>
<tr>
<td>11 Nov 2005</td>
<td>MS Help</td>
<td>Petrochemical</td>
<td>US</td>
</tr>
<tr>
<td>11 Nov 2005</td>
<td>armoured Exe</td>
<td>Petrochemical, trade, publishing, electonics</td>
<td>China</td>
</tr>
<tr>
<td>14 Nov 2005</td>
<td>MS Word</td>
<td>Pharmaceutical</td>
<td>China</td>
</tr>
<tr>
<td>14 Nov 2005</td>
<td>MS Word</td>
<td>News</td>
<td>Taiwan</td>
</tr>
<tr>
<td>14 Nov 2005</td>
<td>MS Help</td>
<td>Legal</td>
<td>Korea</td>
</tr>
<tr>
<td>14 Nov 2005</td>
<td>MS Word</td>
<td>Trade, Electronics</td>
<td>61.217.145.123</td>
</tr>
<tr>
<td>15 Nov 2005</td>
<td>MS Word</td>
<td>News</td>
<td>211.22.165.180</td>
</tr>
<tr>
<td>16 Nov 2005</td>
<td>MS Help</td>
<td>Legal</td>
<td>61.36.170.246</td>
</tr>
<tr>
<td>17 Nov 2005</td>
<td>MS Word</td>
<td>Semi-conductor, transport, communications</td>
<td>61.218.104.163</td>
</tr>
<tr>
<td>18 Nov 2005</td>
<td>MS Word</td>
<td>Defence, pharmaceutical, legal, medical</td>
<td>China</td>
</tr>
<tr>
<td>18 Nov 2005</td>
<td>MS Help</td>
<td>Medical</td>
<td>205.118.75.84</td>
</tr>
<tr>
<td>30 Nov 2005</td>
<td>MS Word</td>
<td>Trade, paint</td>
<td>221.218.131.92</td>
</tr>
<tr>
<td>30 Nov 2005</td>
<td>Exe</td>
<td>NL transport, defense</td>
<td>China</td>
</tr>
<tr>
<td>03 Dec 2005</td>
<td>MS Word</td>
<td>Human rights</td>
<td>China</td>
</tr>
<tr>
<td>06 Dec 2005</td>
<td>MS Help</td>
<td>Human rights</td>
<td>West Australia</td>
</tr>
<tr>
<td>06 Dec 2005</td>
<td>MS Word</td>
<td>Human rights</td>
<td>West Australia</td>
</tr>
<tr>
<td>07 Dec 2005</td>
<td>Exe</td>
<td>UK &amp; NL transport, defense, electrical</td>
<td>Taiwan</td>
</tr>
</tbody>
</table>
Mr. Mike Ciscmon  
Purchasing  
IIA Corporation  
P.O. Box 1353  
Hurt Valley, DM 82030  
Subject: RVT Environmental Qualification Testing

Dear Mick:  
As XRS proceeds with RVT Environmental Qualification testing, several issues have arisen and we wish to notify you of DRS actions relative to those issues.

“ Solar load test. The RVT will be operational; however, the PCI video option cards (611 and 616) will be non-operational because of the CDL driver thermal issue which has been brought to AAI’s attention in Art Lowe’s letter, APL:04-0008:3711.

“ Transit drop and loose cargo tests. Both of...
• **Attack patterns**
  - Very small scale: 1-10 victims
  - Highly targeted recipients
  - Use zero-day exploits
  - Not detected by desktop anti-virus software (no signature)
  - Remain undetected for several months
Data from AV-test.org
Detection

Detection Oct 2006
AntiVir, BitDefender, McAfee, WebWasher

No Detection Oct 2006
@Proventia-VPS, Avast!, AVG, ClamAV, Command, Dr Web, eSafe, eTrust-INO, eTrust-VET, Ewido, F-Prot, F-Secure, Fortinet, Ikarus, Kaspersky, Microsoft, Nod32, Norman, Panda, QuickHeal, Rising, Sophos, Symantec, Trend Micro, UNA, VBA32, VirusBuster, YY_Spybot

Data from AV-test.org
• Data stealing
  - Highly targeted organisations
  - Highly targeted recipients
  - Use zero-day exploits
  - Very low volume
### Attack dates Nov-Dec 05

<table>
<thead>
<tr>
<th>Date</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>01 Nov 2005</td>
<td>中国需要更多的流感疫苗</td>
</tr>
<tr>
<td>05 Nov 2005</td>
<td>中国需要更多的流感疫苗</td>
</tr>
<tr>
<td>11 Nov 2005</td>
<td>China Needs More Tamiflu</td>
</tr>
<tr>
<td>11 Nov 2005</td>
<td>Tamiflu</td>
</tr>
<tr>
<td>14 Nov 2005</td>
<td>Do you know How the US Supplied Iran with Nuclear Know-How?</td>
</tr>
<tr>
<td>14 Nov 2005</td>
<td>Bird flu's truth in mylasia</td>
</tr>
<tr>
<td>30 Nov 2005</td>
<td>GE Transportation Signs Training Agreement with Tusas Engine Industries</td>
</tr>
<tr>
<td>03 Dec 2005</td>
<td>Do you know How the US Supplied Iran with Nuclear Know-How?</td>
</tr>
<tr>
<td>06 Dec 2005</td>
<td>Bird flu's truth in mylasia</td>
</tr>
<tr>
<td>07 Dec 2005</td>
<td>Subject: RVT Environmental Qualification Testing</td>
</tr>
</tbody>
</table>
How many gangs involved?

- **Gang 1**
  - Most active
  - Wide variety of ploys
  - Often use zero day

- **Gang 2**
  - Targets Hong Kong based organisations

- **Gang 3**
  - Very small scale
  - One email every two weeks
  - From IP in California
  - Military target
• Upward trend in attacks
• How important is this anyway?

• Very small probability of attack
  - 0.001% of all email
  - Recipient might not open email anyway
  - Recipient might not be running right software for vulnerability

• Very high cost if successful
  - Company IP is very valuable
  - May be worth $millions for a big company
  - May be worth everything for a small company

• Small number * big number
  - Hard to put a value & risk rating
Predictions

• Will continue to increase
  - Current gangs increase activity
  - Other gangs enter the fray

• Best technique is zero day exploits via email
  - Will see more zero day exploits
  - More file formats than office & help

• Other electronic ways than email

• Other ways than electronically
For more information…

Alex Shipp (ashipp@messagelabs.com)

www.messagelabs.com/intelligence