Is Troy Burning ?

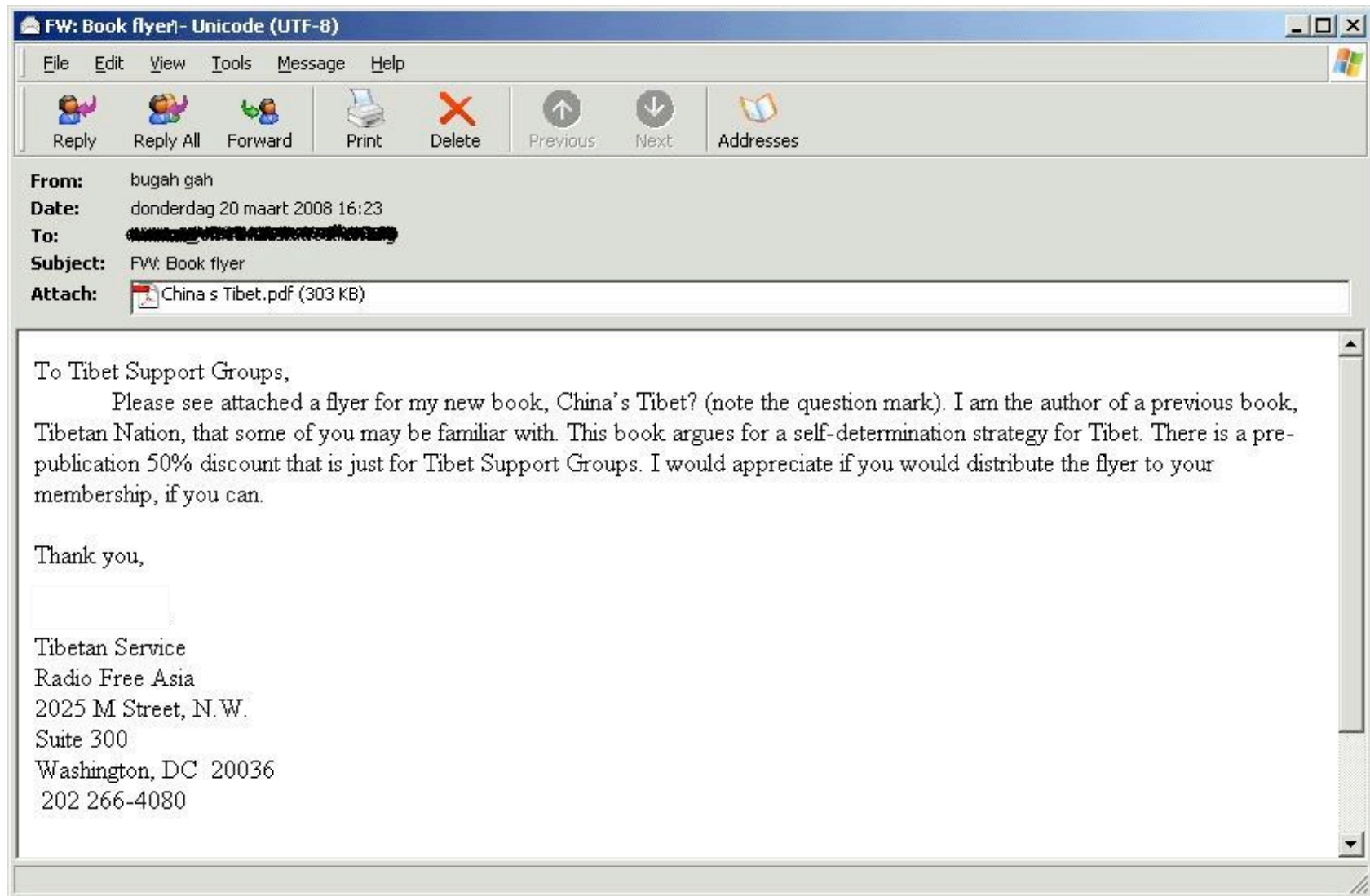**An overview of targeted trojan attacks**

SANSFire 2008, Washington DC

Maarten Van Horenbeeck
SANS Internet Storm Center

Thursday Morning

FW: Book flyer - Unicode (UTF-8)

File   Edit   View   Tools   Message   Help

Reply | Reply All | Forward | Print | Delete | Previous | Next | Addresses

From:	bugah gah
Date:	donderdag 20 maart 2008 16:23
To:	████████████████████████
Subject:	FW: Book flyer
Attach:	China s Tibet.pdf (303 KB)

To Tibet Support Groups,

Please see attached a flyer for my new book, China's Tibet? (note the question mark). I am the author of a previous book, Tibetan Nation, that some of you may be familiar with. This book argues for a self-determination strategy for Tibet. There is a pre-publication 50% discount that is just for Tibet Support Groups. I would appreciate if you would distribute the flyer to your membership, if you can.

Thank you,

Tibetan Service
Radio Free Asia
2025 M Street, N.W.
Suite 300
Washington, DC 20036
 202 266-4080

An advertisement

Behind the curtains

China's Tibet.pdf
MD5 70d0d15041a14adaff614f0b7bf8c428

AhnLab-V3 2008.3.22.1 2008.03.21 -
AntiVir 7.6.0.75 2008.03.21 -
Authentium 4.93.8 2008.03.20 -
Avast 4.7.1098.0 2008.03.21 -
AVG 7.5.0.516 2008.03.21 -
BitDefender 7.2 2008.03.21 -
CAT-QuickHeal 9.50 2008.03.20 -
ClamAV 0.92.1 2008.03.21 -
DrWeb 4.44.0.09170 2008.03.21 -
eSafe 7.0.15.0 2008.03.18 -
eTrust-Vet 31.3.5631 2008.03.21 -
Ewido 4.0 2008.03.21 -
F-Prot 4.4.2.54 2008.03.20 -
F-Secure 6.70.13260.0 2008.03.21 -
FileAdvisor 1 2008.03.21 -
Fortinet 3.14.0.0 2008.03.21 -
Ikarus T3.1.1.20 2008.03.21 -
Kaspersky 7.0.0.125 2008.03.21 -
McAfee 5257 2008.03.21 -
Microsoft 1.3301 2008.03.21 -
NOD32v2 2966 2008.03.21 -
Norman 5.80.02 2008.03.20 -
Panda 9.0.0.4 2008.03.21 -
Prevx1 V2 2008.03.21 -
Rising 20.36.42.00 2008.03.21 -
Sophos 4.27.0 2008.03.21 Mal/JSShell-B
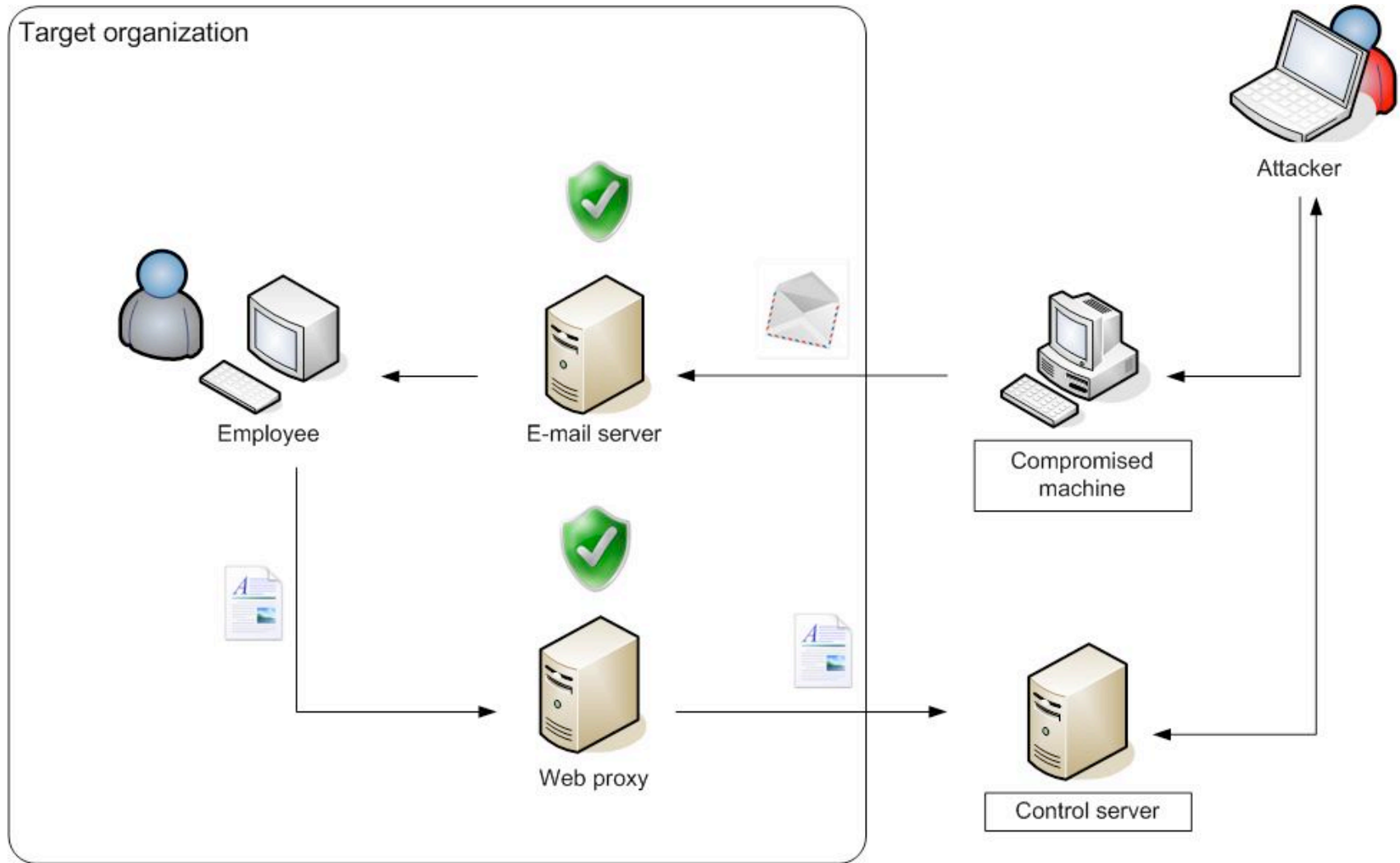Sunbelt 3.0.978.0 2008.03.18 -
Symantec 10 2008.03.21 -
TheHacker 6.2.92.250 2008.03.19 -
VBA32 3.12.6.3 2008.03.21 -
VirusBuster 4.3.26:9 2008.03.21 Exploit.PDF.A
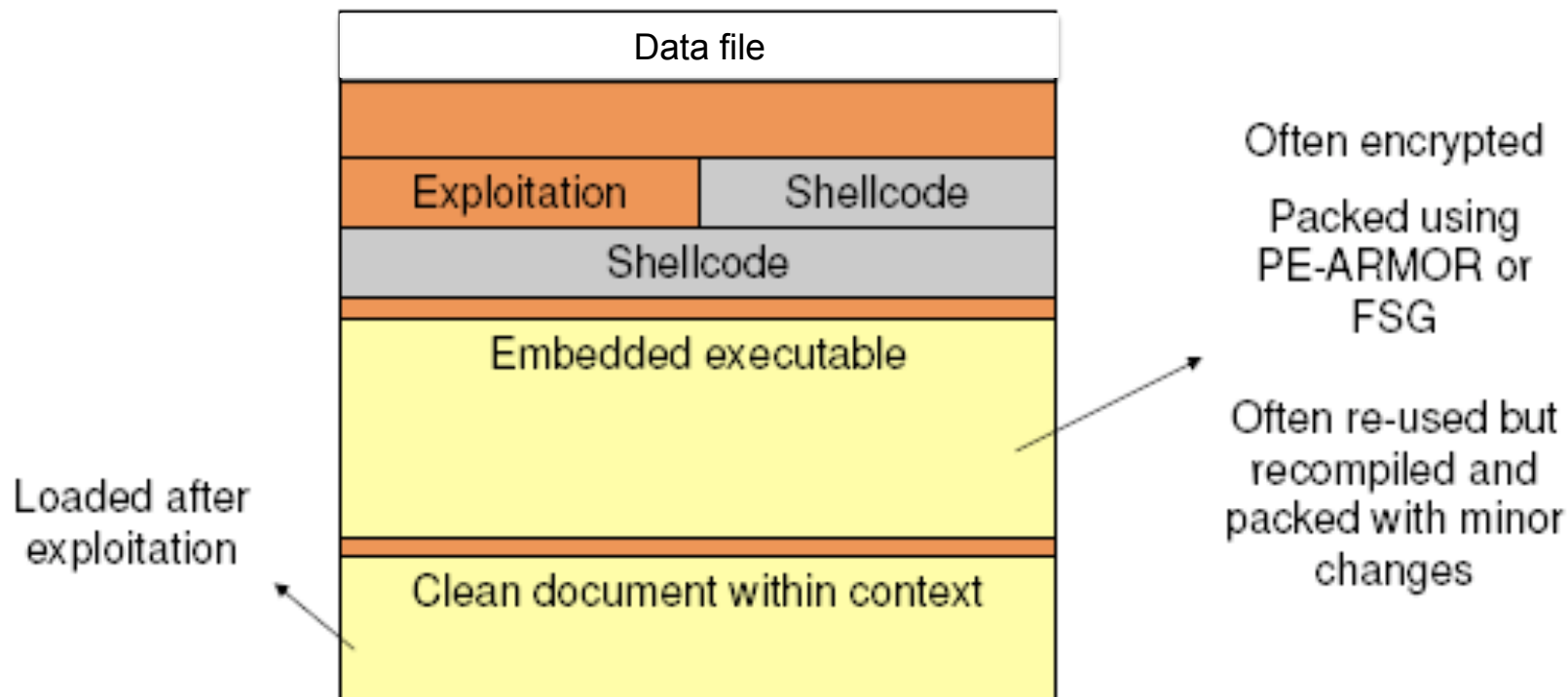**Webwasher-Gateway 6.6.2 2008.03.21 Exploit.PDF.ZoneBac.gen (suspicious)**

Behind the curtains

Social Engineering

- **Cognitive dissonance:** one President visiting another

- **Mimic writing style**
  - Reuse public blog information or previous communications

- **Match content to a topic of interest**
  - Backdoored Videos of "Lhasa" protests

- **Convince users to forward messages along**
  - Improves trust in the message
  - Users will confirm they sent the message

- **Backdoor viral content**
  - Tech memes are identified, backdoored and forwarded
  - Users unable to distinguish between viral and non-viral content

The exploit: anatomy of a dropper

Data file

Exploitation | Shellcode

Shellcode

Embedded executable

Clean document within context

Loaded after exploitation

Often encrypted

Packed using PE-ARMOR or FSG

Often re-used but recompiled and packed with minor changes

Weapon of choice: attack vectors and vulnerabilities

- **Plain binaries**

- **CHM Help files with embedded objects;**

- **CVE-2008-0655: Acrobat Reader PDF exploit**

- **CVE-2006-2492, CVE-2007-3899: Word**

- **CVE-2006-3590, CVE-2006-0009: Powerpoint**

- **CVE-2008-0081: Excel**

- **CVE-2005-0944: Microsoft Access**

- **CVE-2006-3845: LHA files exploiting vulnerabilities in WinRAR.**

Weapon of choice: application bugs

- **Attack on collab.CollectEmailInfo Javascript method**

```
1:6BFCh:  endobj.24 0 obj<</S/JavaScript/JS 26 0 R>>.endobj.25 0 obj 1
1:6C38h:  116.endobj.26 0 obj<</Length 25 0 R/Filter[/FlateDecode]>>st
1:6C74h:  ream..H..WMo.6....[]P....o@Q"%."..=..C....\.p....."......DKNP.
1:6CB0h:  2....7o.#...........S[]..o...D.w?..^.s..=E.........`.../0.~}..
1:6CECh:  7{..."[]...M.....[..-;..t..[..K.<.Gsi...^.}S.i....q/.....6u.+
1:6D28h:  .L.[S......D.~-D...$Xgq..o#..h.....gVV...r.d.8..Fxi-,]D....V
1:6D64h:  yM..[.f.9dAR..V..v.....d&+..:..17..E~Z.Q:....Mv.'.M.T.)..H.<
1:6DA0h:  ...:Ix..@C96..r.4..J.,1....7.5....K.3./F&.2.n.~B...*.\!.....
```

```
0F3Ch:   ream.endobj.27 0 obj<</F(ctfmon.exe)/EF<</F 29 0 R>>/Type/Fi
0F78h:   lespec>>.endobj.29 0 obj<</Length 8904/Filter/FlateDecode/Su
0FB4h:   btype/application#2Fx-msdownload/Params<</Size 15360/ModDate
0FF0h:   (D:20080423164652Z)/CreationDate(D:20080423164652Z)/CheckSum
102Ch:   <4cc6277445d2d388a4cd827086a5f5f0>>>/DL 15360>>stream..H...i
1068h:   X.W.!(.r...\3...PP..7C3..3.....0;.0;C7.....f.........x."...P.
10A4h:   s.......E..b ..."...`..3.....UW..........'Y...`.....*.......
10E0h:   ...g..i.kn...57Y...%.T,.....IR.o%...$. y..)/.R.^vvC'......#.
```

Weapon of choice: application bugs

- **Operating systems have become significantly more secure**

- **Interest focuses on specific types of applications**
  - File parsing code
  - Massive installed base
  - Lack of auto-update features

- **Anti virus protection proving a challenge**
  - Effective sandboxing not feasible
  - Lack of file format parsers and encoding support
  - Few limitations on length of shellcode
  - Difficult to assess the targeted application

The backdoor

```
event_0310_result.exe
MD5 7d62cec8f022e9599885ad7d079d2f60

AhnLab-V3 2008.3.4.0/20080310 found nothing
AntiVir 7.6.0.73/20080310 found [HEUR/Malware]
Authentium 4.93.8/20080307 found nothing
Avast 4.7.1098.0/20080309 found nothing
AVG 7.5.0.516/20080310 found nothing
BitDefender 7.2/20080310 found nothing
CAT-QuickHeal 9.50/20080308 found nothing
ClamAV None/20080310 found nothing
DrWeb 4.44.0.09170/20080310 found nothing
eSafe 7.0.15.0/20080309 found nothing
eTrust-Vet 31.3.5597/20080307 found nothing
Ewido 4.0/20080310 found nothing
F-Prot 4.4.2.54/20080309 found nothing
F-Secure 6.70.13260.0/20080310 found [Suspicious:W32/Malware!Gemini]
FileAdvisor 1/20080310 found nothing
Fortinet 3.14.0.0/20080310 found nothing
Ikarus T3.1.1.20/20080310 found nothing
Kaspersky 7.0.0.125/20080310 found nothing
McAfee 5247/20080307 found nothing
Microsoft 1.3301/20080310 found nothing
NOD32v2 2935/20080310 found nothing
Norman 5.80.02/20080307 found nothing
Panda 9.0.0.4/20080309 found nothing
Prevx1 V2/20080310 found [Heuristic: Suspicious Self Modifying File]
Rising 20.35.02.00/20080310 found nothing
Sophos 4.27.0/20080310 found [Mal/Behav-116]
Sunbelt 3.0.930.0/20080305 found nothing
Symantec 10/20080310 found nothing
TheHacker 6.2.92.239/20080309 found nothing
VBA32 3.12.6.2/20080305 found nothing
VirusBuster 4.3.26:9/20080309 found nothing
Webwasher-Gateway 6.6.2/20080310 found [Heuristic.Malware]
```

The backdoor

- **Riler trojan: popular in 2005-2006**

- **Network traffic:**

```
NAME:
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
```

The backdoor

- **Command set:**

```
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 backdoor

- **Known malware families**

- **Recompiled or repacked to evade detection**

- **Hide from the end user and administrator**
  - Rootkit functionality (ADS, hooking of file system and network access calls)
  - Network traffic often encrypted

- **Actions:**
  1. Register the compromised station using its hardware (MAC address)
  2. Download updates
  3. Fetch commands over web, e-mail and proprietary protocols
  4. Log keystrokes, search for files and submit them to the control server

- **Observed behaviour includes searches for:**
  - Web mail and mail client configuration settings
  - Documents
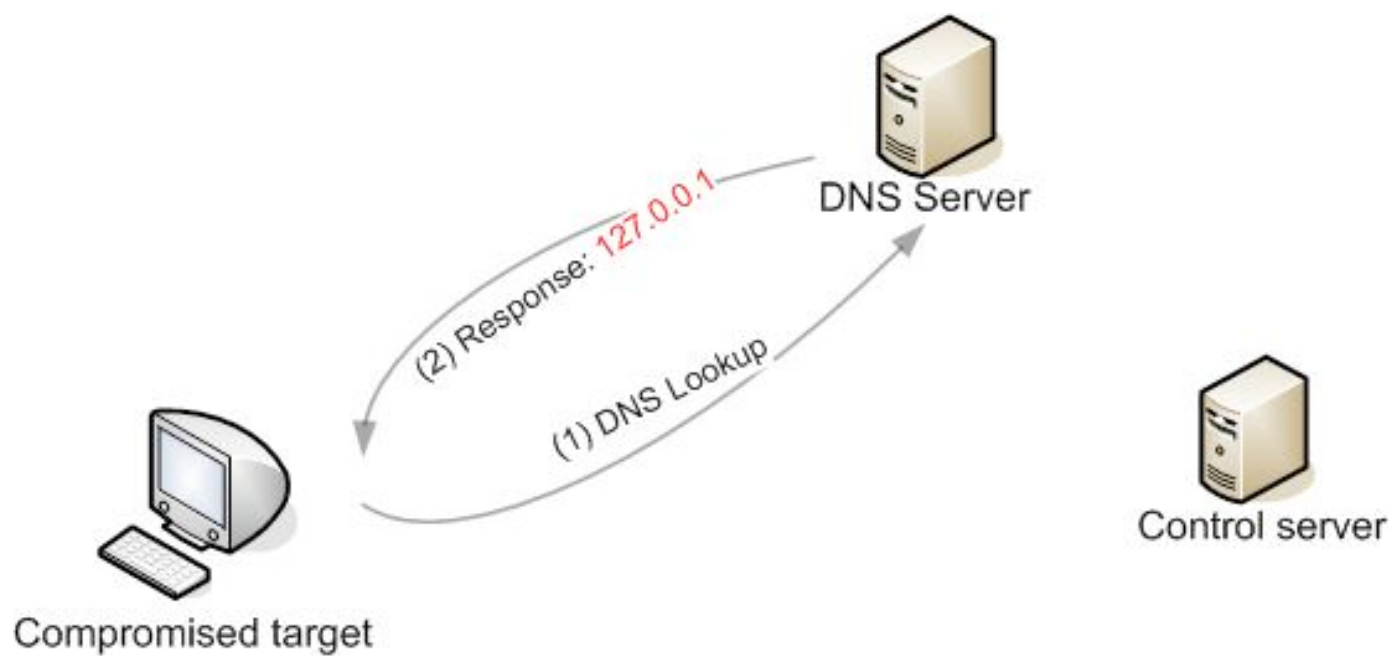 - PGP Keyrings

Control infrastructure

Deep compromise: host name parking

- **Active attack**
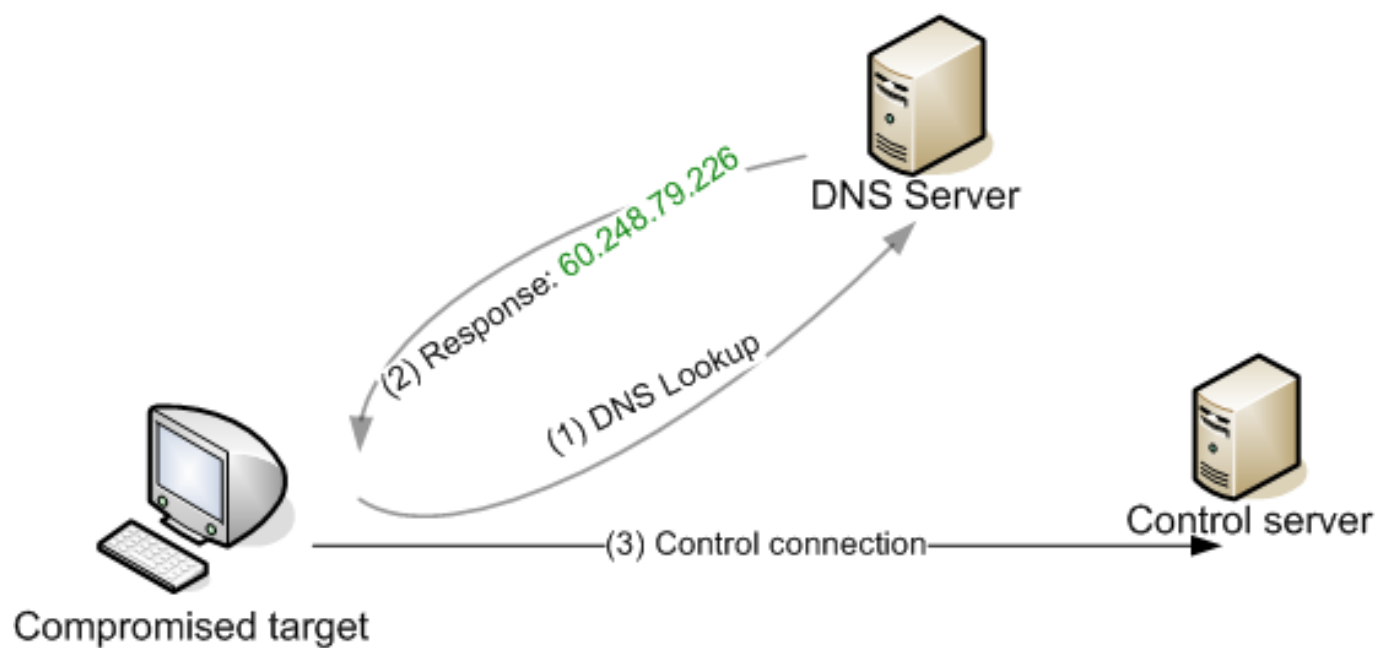
Deep compromise: host name parking
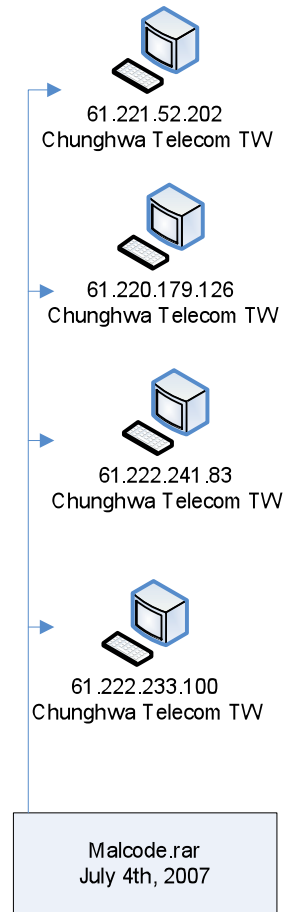
- **Disabled attack**

Deep compromise: host name parking
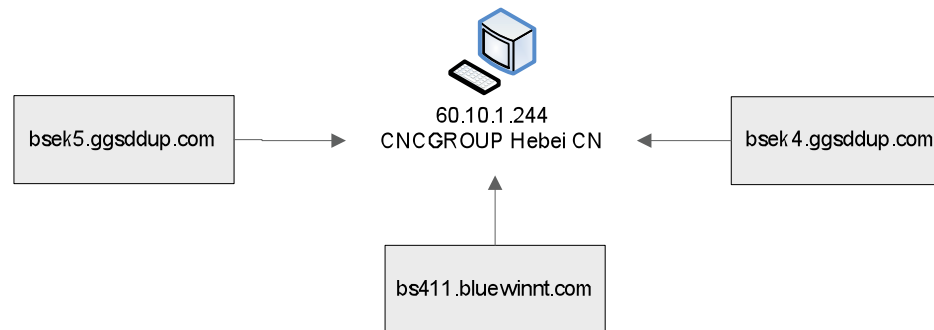
- Host name parking

```
+ 2008-03-31 11:49 | sds.bi-apple.net | a.b.c.d

+ 2008-03-31 14:44 | sds.bi-apple.net | 63.64.63.64

- 2008-03-31 14:44 | sds.bi-apple.net | 63.64.63.64

+ 2008-04-01 11:55 | sds.bi-apple.net | a.b.c.d

- 2008-04-01 11:55 | sds.bi-apple.net | 63.64.63.64

+ 2008-04-01 13:43 | sds.bi-apple.net | 63.64.63.64

- 2008-04-01 13:43 | sds.bi-apple.net | a.b.c.d

+ 2008-04-02 01:17 | sds.bi-apple.net | a.b.c.d

- 2008-04-02 01:17 | sds.bi-apple.net | 63.64.63.64

+ 2008-04-04 14:08 | sds.bi-apple.net | 63.64.63.64

- 2008-04-04 14:08 | sds.bi-apple.net | a.b.c.d
```

Safety in numbers

61.221.52.202
Chunghwa Telecom TW

61.220.179.126
Chunghwa Telecom TW

61.222.241.83
Chunghwa Telecom TW

61.222.233.100
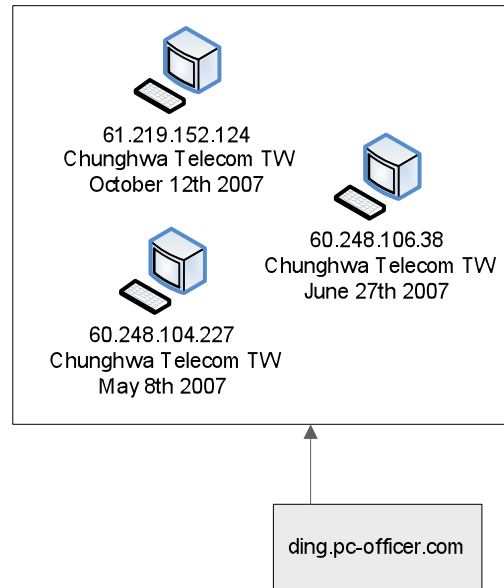Chunghwa Telecom TW

Malcode.rar
July 4th, 2007

- Single sample connects to multiple different control servers sequentially

- Removes single point of failure (server or hostname)

- Ability to use multiple exit strategies
  - **Ephemeral port**
  - **HTTP & HTTPS**
  - **SMTP**

Multiple hostnames

bsek5.ggsddup.com → 60.10.1.244 CNCGROUP Hebei CN ← bsek4.ggsddup.com

bs411.bluewinnt.com

- Defeats detection of the hostname

- Enables the re-use of a compromised server

- Different host names for different targets
  - **Organization 1: bsek4.ggsddup.com**
  - **Organization 2: bs411.bluewinnt.com**

Swapping servers

61.219.152.124
Chunghwa Telecom TW
October 12th 2007

60.248.106.38
Chunghwa Telecom TW
June 27th 2007

60.248.104.227
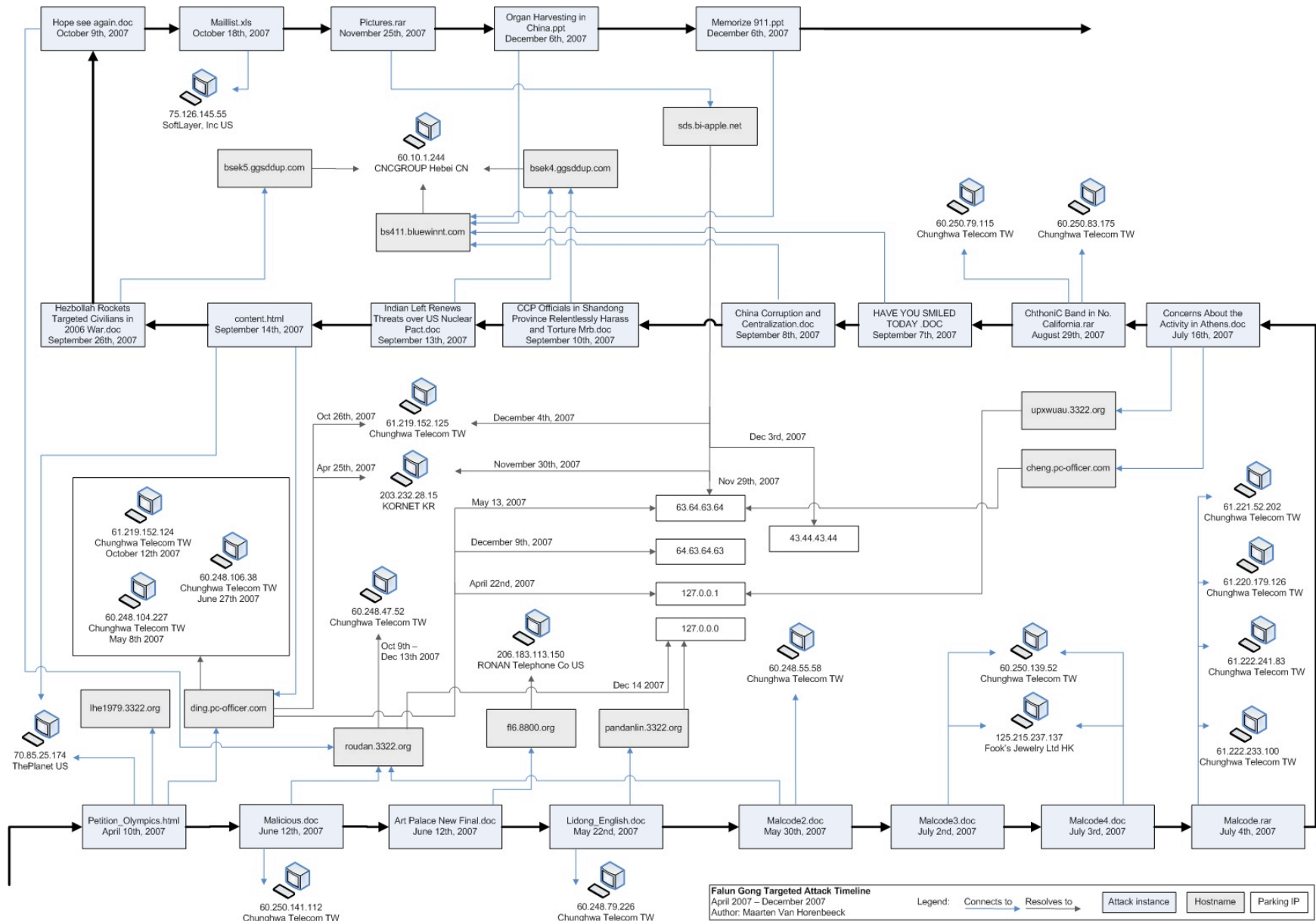Chunghwa Telecom TW
May 8th 2007

ding.pc-officer.com

- Single host name points to a single server

- Once server is cleaned up, DNS entry is changed

- Control servers can even be on home connection

Mapping the control infrastructure

- **DNS based gathering techniques**
  - Passive DNS replication
    - Anonymously gather DNS logs from organizations
    - Store DNS responses in a central database

  - DNSWatch
    - Log all known hostnames
    - Continuously perform DNS lookups to ascertain status

  - **A word of caution**
    - Attacker may control his own DNS infrastructure
    - DNS responses can be influenced based on querying source ("views")

Control infrastructure

Falun Gong Targeted Attack Timeline
April 2007 – December 2007
Author: Maarten Van Horenbeeck

Legend: Connects to Resolves to   Attack instance   Hostname   Parking IP

The first hop

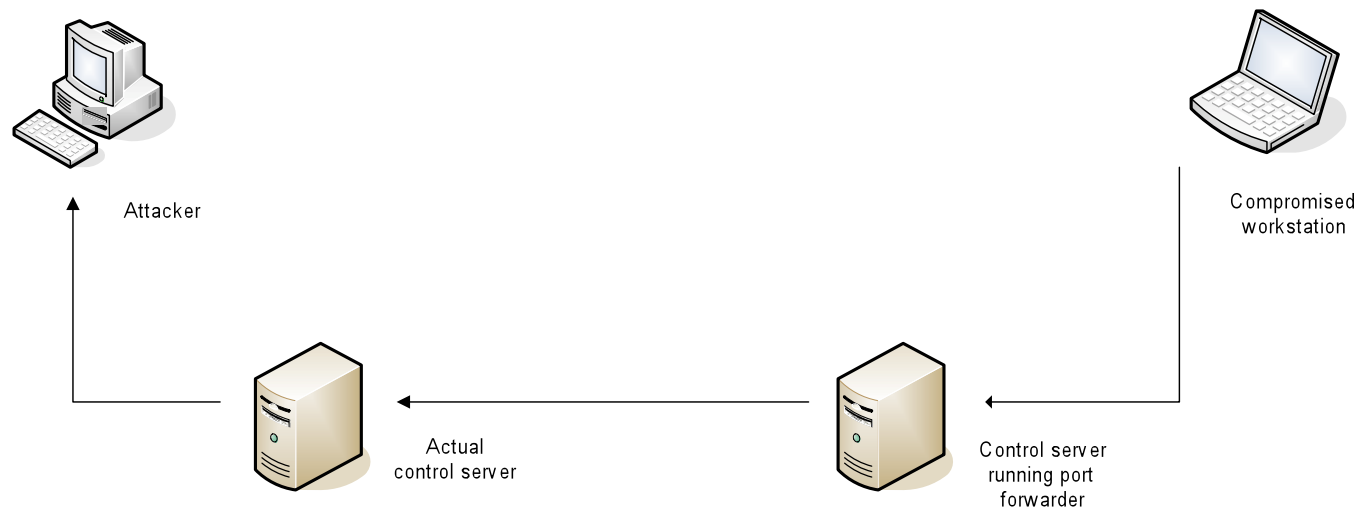- **Common attack vectors**
  - Terminal Services (RDP)
  - Cracked through password brute forcing

- **Location by popularity**
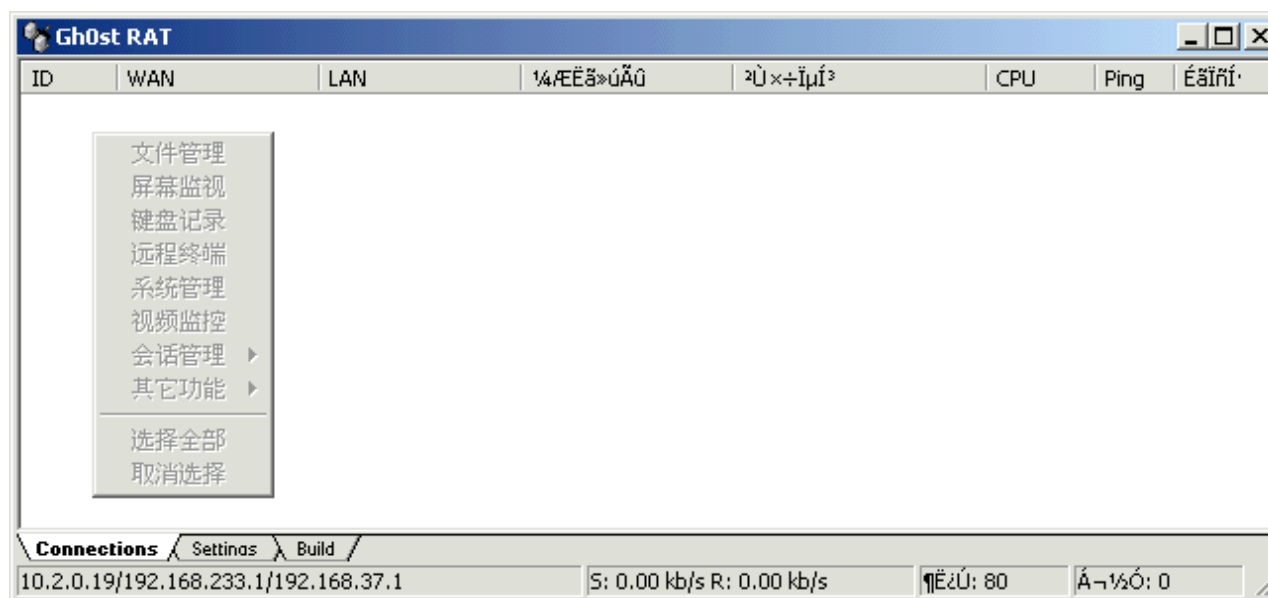 - Mainland China
  - Taiwan
  - South Korea
  - Japan
  - USA

Control server functionality

- **Port forwarder**
  - E.g. PortTunnel

Control server functionality

- **Remote Control application**
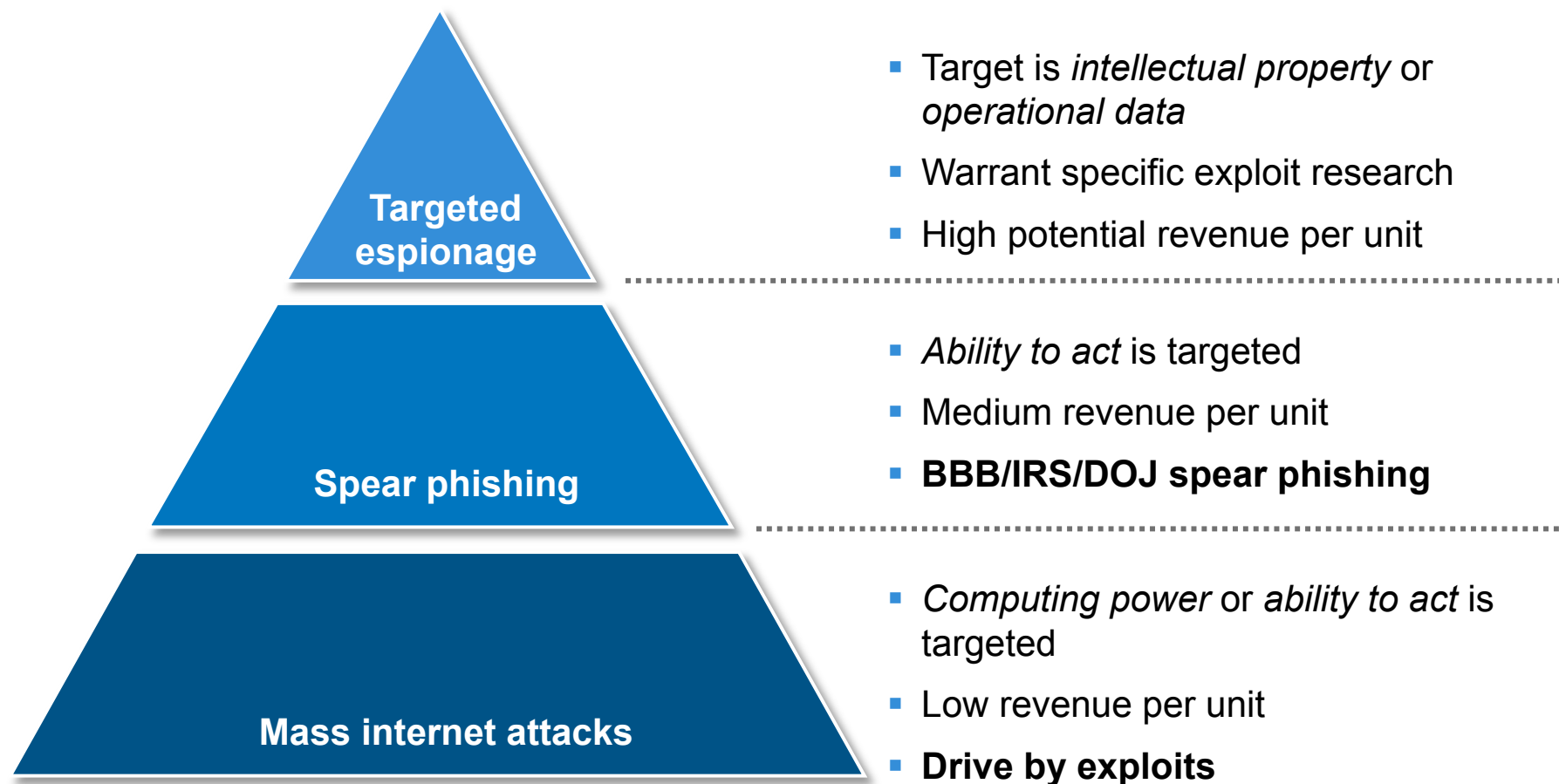

- **Gh0st RAT, Poison Ivy, Darkmoon, Riler**

The targeted economy

The targeted economy: modus operandi

1   Actors with access to target data are identified

2   Mapping of communities

3   Identify actor reputation

4   Design a malicious code sample

5   Apply social engineering

The targeted economy

Targeted espionage

- Target is *intellectual property* or *operational data*
- Warrant specific exploit research
- High potential revenue per unit

Spear phishing

- *Ability to act* is targeted
- Medium revenue per unit
- **BBB/IRS/DOJ spear phishing**

Mass internet attacks

- *Computing power* or *ability to act* is targeted
- Low revenue per unit
- **Drive by exploits**

Investment indicators

- **Custom vulnerability development**
  - 0day exploits:
    - e.g. **MS08-014** (Excel)
  - Attack vector research
    - Use of **Word documents as MDB attack vector**
    - First groups to **actively use 2008 PDF Reader Javascript method overflow**
  - Release of exploits around patch time

Investment indicators

- **Target customization**
  - Target used PGP encryption tool
    - Attackers sent commands to search for encryption keys

    ```
    <Command Begin>
    netmgetr usb:\*.doc
    netmgetr usb:\*.pkr
    netmgetr usb:\*.skr
    netlsr usb:\*.*
    <Command End>
    ```

  - Reuse of harvested data
    - Aid in selection of new targets
    - Steers social engineering efforts

The threat agent

The threat agent

- **Indications the attacks originate in China**
  - Chinese software tools on compromised hosts
  - Trojans from Chinese sites **(hacker01.com)** are popular
  - Binary files with Chinese resources loaded
  - Preference for Chinese control servers **(language)**
  - Target selection

- **No evidence of PRC involvement**

- **Red Hacker Alliance**
  - Large community, more cooperation and knowledge sharing
  - Well known interest in patriotic hacking
    - **Spy plane hacking row (2001)**
    - **Chinese Embassy in Yugoslavia (1999)**
  - But vulnerability research requires motivation & funding

Incident: attack on Japanese companies

Email Spoofed from Japanese Government
Agency Targets Japanese Companies

Today, Symantec Security Response has received reports from
a number of our customers of a possible targeted spam attack
against several Japanese companies.

The spam email associated with this attack spoofs itself as an
email from a Japanese government agency and entices the user
to open the attached .zip file to check organizational changes
made recently. The attached .zip file contains 2 files: 0414.xls
and 0414.exe. 0414.xls is a legitimate file containing a list of
names, addresses, personnel positions, which may or may not
really exist. There is no evidence to suggest that any exploit
attempts are made on this file.

The other file, 0414.exe, is a variant of Backdoor.Darkmoon,
which has a keylogging capabilities. At the time of writing, we
have seen several variants of Backdoor.Darkmoon associated
with this spam attack. One variant saves stolen information as
the filename msvidctl, sends it to the remote attacker, and
awaits further commands from cyhk.3322.org. Another variant
sends information as the filename taskame to hi222.3322.org
and opens a back door to the same site.

```
- 2008-04-08 02:43 | hi222.3322.org | 60.x.x.x

+ 2008-04-08 08:19 | hi222.3322.org | 60.x.x.x

- 2008-04-08 08:19 | hi222.3322.org | 60.x.x.x

+ 2008-04-09 02:37 | hi222.3322.org | 60.x.x.x

- 2008-04-09 02:37 | hi222.3322.org | 60.x.x.x

+ 2008-04-10 13:17 | hi222.3322.org | 60.x.x.x

- 2008-04-10 13:17 | hi222.3322.org | 60.x.x.x
```

Symantec.com, April 15th 2008

- **Also used in an attack on a Canadian Tibetan community member,
  spoofed as originating from Reporters without Borders**

Incident: spear phishing against USG employees

US-CERT Critical Infrastructure Information Notice CIIN-08-074-01
March 14, 2008

Spear Phishing Campaign Directed at USG Employees
(U//FOUO)

Overview (U//FOUO)

US-CERT has received reports of spear phishing campaign currently underway that may be directed towards US defense contractors and government employees. US-CERT is issuing this

Contained within this ZIP file are two files:

080312.doc
data source.db

The file "data source.db" is a Microsoft Access Database that is designed to exploit a stack buffer overflow in the Microsoft Jet Engine. Details of the vulnerability can be found at http://seclists.org/bugtraq/2007/Nov/0235.html.

BusinessWeek, April 11th 2008

- **Same sample reported by member of a Tibetan NGO on March 12th**

Incident: cvnxus.8800.org

On Aug. 21, 2007, e-mail attacks originating in China targeted 28 defense contractor sites in the United States. In this case, defense contractors were tempted with an attachment purporting to discuss engine modifications for the Pioneer unmanned aerial vehicle.

According to the FBI, the e-mail text contained an actual presentation that had embedded a malicious code known as "Poison Ivy."

The FBI soon traced the attack to Internet Protocol address 218.106.252.77—which turned out to belong to CNC Group-BJ, CNC Group Beijing Province Network.

Air Force Magazine Online (Dogs of Web War)

```
+ 2008-02-07 07:46 | cvnxus.8800.org | 218.106.252.77

+ 2008-02-07 07:46 | cvnxus.8800.org | 218.106.252.77

- 2008-03-08 22:23 | cvnxus.8800.org | 218.106.252.77

+ 2008-03-08 22:29 | cvnxus.8800.org | 218.106.252.77

+ 2008-03-14 16:38 | cvnxus.8800.org | 218.106.251.85
```

- **cvnxus.8800.org used in several attacks on several NGOs**
- **Hostname disappeared in April 2008, now replaced**

Nodal link analysis

- **Identifies relationships between attacks graphically**

- **DNS data allows relationships to be identified**
  - Identify all IP addresses once associated with a host
  - Identify all hostnames once associated with each IP address
  - Identify all IP addresses once associated with each new host
  - Review timing (hosts should map consistently)
  - *Lather, rinse, repeat.*

Nodal link analysis

- **Combination with qualitative parameters**
  - Type of exploit
  - Type of backdoor
  - Language preference
  - Preferred control server location
  - Timeframe of connections
  - Type of data targeted

- **Allows mapping and forecasting of techniques**
  - Methodologies stand out
  - Exploit sequences

- **Set investigative and takedown priorities**

US Government warning in 2007

- **attacker.example.com (2 known addresses)**

  - *Strong connection with:*
    - Hostname A (11 logged addresses)
    - Hostname B (107 logged addresses)
    - Hostname C (48 logged addresses)
    - Hostname D (48 logged addresses)
    - Hostname E (235 logged addresses)
    - Hostname F (161 logged addresses)

  - *Weak connection with:*
    - Hostname X (127.100.100.100)
    - Hostname Y (127.100.100.100)
    - Hostname Z (127.100.100.100)

*NOTE: hostnames have been anonymised for public distribution

US Government warning in 2007

- **Removal of duplicates leaves 394 unique addresses**

- **Attacker.example.com difficult to investigate**
  - 2 unique IP addresses, both in China
  - Full threat agent discovery provides addresses in
    - Indiana, US (*alas*, a private VPN gateway)
    - Sweden
    - China
  - Many DSL links, limited set of actual machines

  - **Limitations do apply**
    - Groups may "trade" addresses
    - Sharing of resources

Defense against targeted attacks

Defense against targeted attacks

- **Black listing**
  - Common anti virus approach
  - Ineffective for new samples
  - More advanced approaches (shellcode detection, stub binary scanner)

- **White listing**
  - Limits functionality for the end user
  - Needs to be carefully scoped:
    - Depending on level of execution of malicious code, may be bypassed
    - White lists only filter a specific component (web, binaries)
  - Requires stringent control over the execution environment

Defense against targeted attacks

- **Behavioral process profiling**
  - Assigns score to potentially suspicious behavior
  - Alerts when maximum score is exceeded
  - Some behavior may not be assessed correctly yet
  - Higher amount of false positives

- **Communications security**
  - User education & advanced awareness training for critical personnel
  - Enforce trust in the communications process (encryption and signing)

- **Security Intelligence**
  - Enable exchange of anonymous data relevant to attacks
  - Data can be used as intrusion signatures

Defense against targeted attacks

- **Workstation hardening**

  - Beyond the operating system level
  - Application software
    - Ensure all software is covered with patches
    - PDF Readers: lock down Javascript
    - Microsoft Office: use MoICE
      - Pre-parser which converts binary document formats into Office Open XML

  - Gateways
    - Allow file types only based on business requirements
    - RAR rarely a necessity

Future evolution: a forecast

- **Targeting becoming more community based**
  - Why take data from one organization ?
  - Community members tend to "socialize" across companies

- **Other attack vectors**
  - Deployment of code on web sites frequented by attackers
    - Highly visible, highly effective, short lifecycle
    - Minimal access to a wide variety of organizations
  - Compromise of e-mail servers

- **Less re-use of control servers**
  - Tracking of a threat agent will become more difficult
  - New control servers are relatively "cheap" to attain

Thank you!

E-mail: **maarten@daemon.be**