CNCERT/CC

Introduction of Malware Issues

Yuejin Du
Ph.D
Deputy CTO of CNCERT/CC

APEC-OECD Malware Workshop
APEC-TEL 35. 2007.4.22.Manila

CN CERT/CC

Contents

- What is Malware
- Introduction: some of the most common types of malware
- Summary

What is Malware

- Comp
- Malw
  this '
- Usually the malwares hurt you by:
  - the malware themselves
  - bad guys 'behind' them

•steal your sensitive information (and money);
• watch your private activities;
•abuse YOUR computer and network resources;
•control your computer and systems secretly;
•launch attacking behavior and commit crime
•etc.

•destroy your important work or personal data;
•make your computer system unusable

Virus: destroy personal data and computer system

- Computer v
  virus in our
  - Basic feat
    - Invisibl
    - Propaga
      environ
    - Harmful
      handle
  - Basic feat
- This term is now often used to refer all kinds of malware,

Invisible: hide in programs, document files, storage devices, etc.

Propagable: self-replicate after they compromised in computers

Harmful: destroy your personal data, applications, or computer system when the pre-set condition matched

About Virus (cont.)

- Nobody's behind the malware: even the writer can not control the propagation. Threat comes from the code itself.
- How the target is chosen: randomly
- How can it come in:
  - In the past: boot devices; file/document sharing;
  - Now: USB and other storage devices (auto-run function); email (spam) and other network applications; etc.

Trojan & Spyware: hidden spy in your computer

- Trojan Horse: just like the ancient story about Trojan horse in Trojan War
  - YOU let it come in (run some software, aware it or not)
  - YOU think it is a wooden horse (an interesting application)
  - But there are hidden hostile soldiers (hidden program remotely controlled by somebody)
- Spyware: some ‘ware’ works like a spy in your computer
  - Steal your information and send it out

Threats of Trojan and Spyware

- Sensitive information leakage
  - Personal ID info. and other privacy
  - Confidential info. of company, organization, and nation
- Lose control of running system: personal computers, key servers, important application systems, etc.
  - You're not the only owner, and you can not suppose the hidden 'owner' who controls your all resources is your friend!
- Unlike computer virus, the danger of Trojan and spyware does not come from the malware itself, but from the guy behind it.

Trojan: Features and Evolution

- According to the report from Symantic, Trojan horse is the most popular in AP area during the later half year of 2006, 48% malware is Trojan
- CNCERT/CC found more than 500,000 IPs of China had been controlled by trojan horses during the first 3 months of 2007. More than 40,000 computers outside China was controlling those infected hosts
- Spread: by worm, email, web pages and any online services

Worm: huge threat that could make the whole Internet crashed

- Worm: just like the worm in our real world
  - Independent creatures (program run without a host one)
  - Move around by themselves (self-replicate and propagate around in the network)
  - Come into your house from the gaps of your doors and windows (infect online computers through tech. or management vulnerabilities)
- Fast propagation can use up the network bandwidth thus cause large area of network blocked
  - Many examples: Morris, Codered, SQL SLAMMER, etc.
  - One of the biggest danger to CIIP

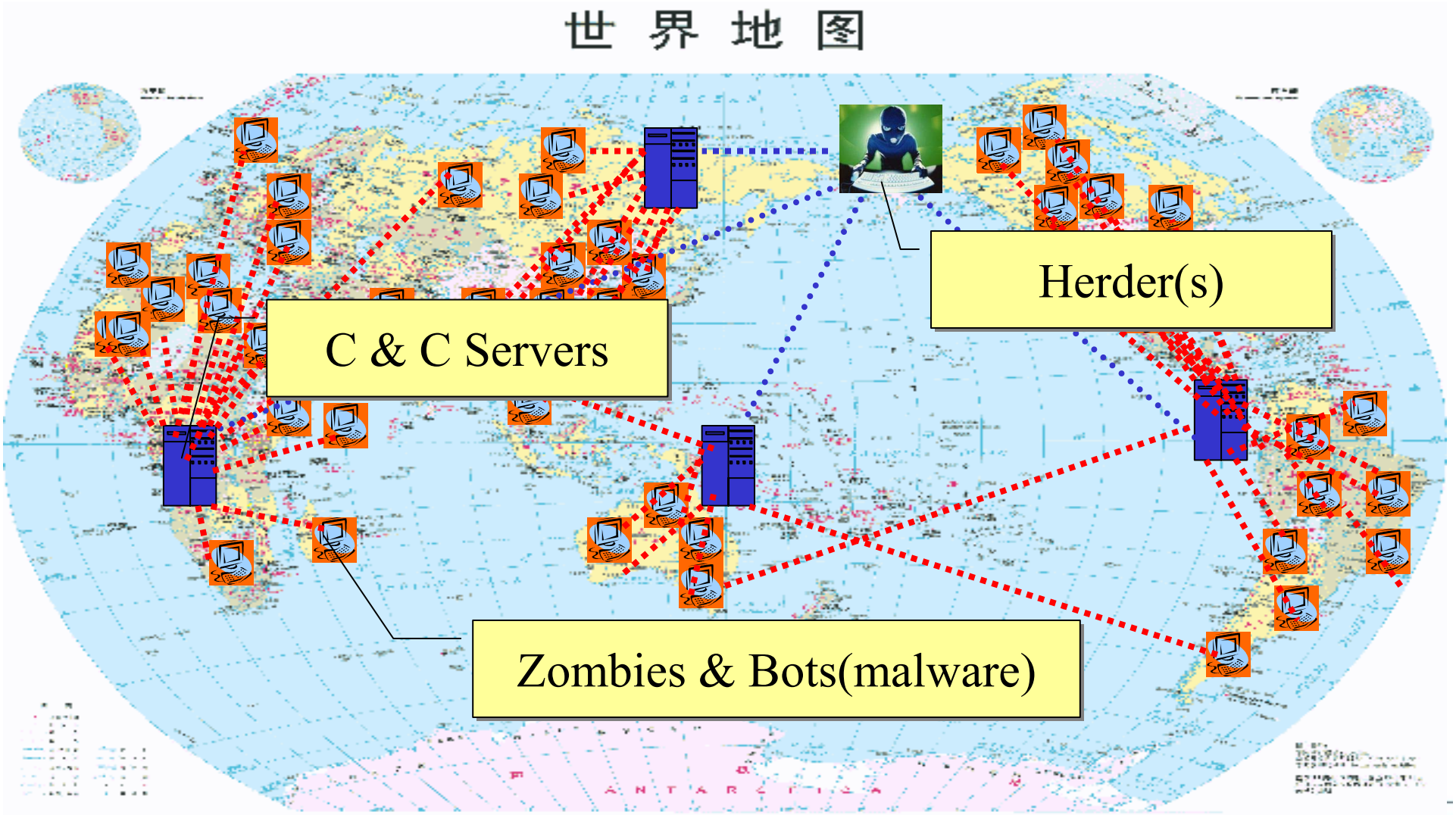
‘none-traditional’ threats and new trend

- Worm is not ‘pure’ any more, abuse the bandwidth is not the only threat it can cause
  - Leave backdoor : Codered (to the whole world)
  - Build up Botnet : Deloader
  - Launch DDoS: Msblast
- 0-day attack and number of vulnerabilities
- Worm is becoming the most common tool for spreading other malwares

Botnet: underground dark army

- The most severe threat to the information society now:
- Botnet is just like an amplifier: it can dramatically enlarge the damage of nearly all other attacking behavior:
  - Launch worm to break down backbone
  - DDoS
  - Online ID theft
  - Deploy trojan or spyware (for Secret control or info stealing)
- Bad guys have their super power and under-ground ‘army’ now
  - Millions of online computers are under their control and they can command these ‘army’ to do anything

What is Botnet



How big the army is

- In 2006 CNCERT/CC found:
  - 12 million IPs in China were controlled by botnets (2.5 million in 2005)
  - More that 500 botnets (contained at least 50 bots), more than 16000 C&C Servers outside China
  - The biggest botnet contained 1.29 million bots
- In AP area, 71% bots were in China in the second half year of 2006 (from Symentic)

Severe attacks related to malware

- DDoS: very dangerous to CII and the whole Internet; very difficult to deal with
  - Reason: bad guys can control a GREAT amount of infected hosts to do that
  - 63% DDoS attacks were targeted to China in 2006 second half year (From Symentic)
- Online ID theft: key logger; redirection; spam and malware in fake website (phishing);
  - 31055 phishing sites located in China in 2006 (from APWG)
  - 576 phishing incident reported (2005: 456; 2004: more than 200)

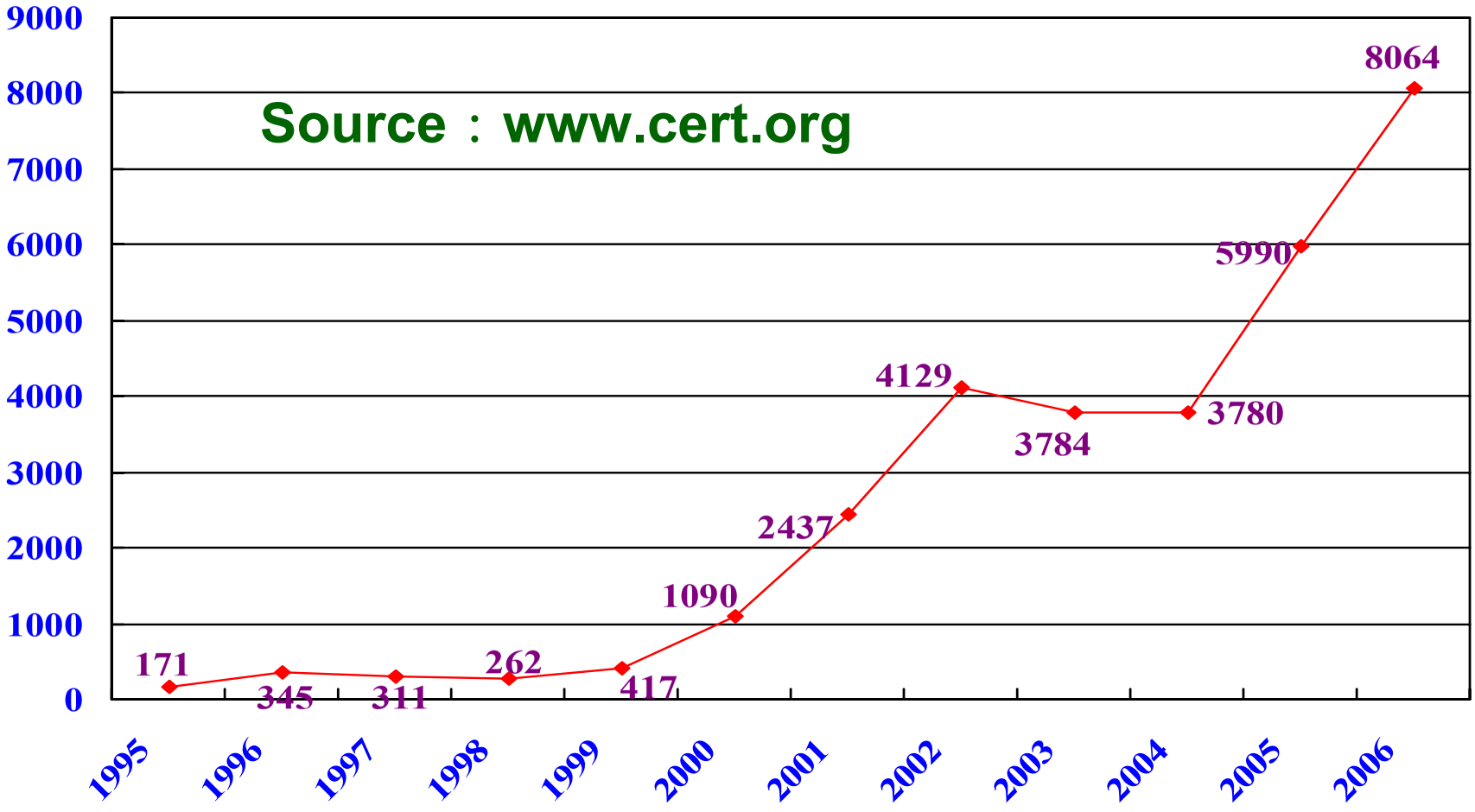
Phishing


世 界 地 图
Victims: End users
Attackers: Gather info. from dummies and get money from bank/market
Tools: Fake websites
Victims: Companies and their websites
news

Malware downloadable everywhere

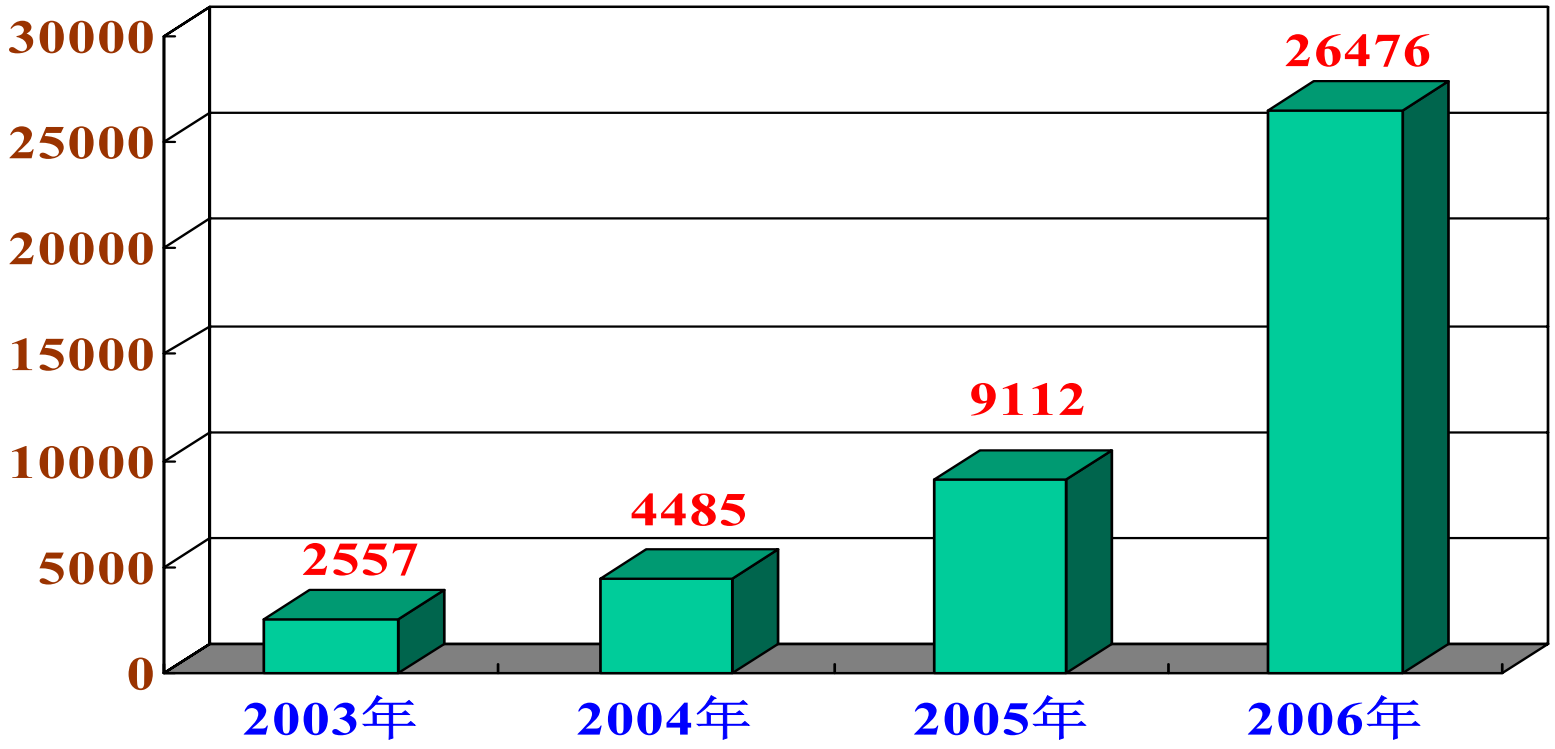
```
├─rootkit      (0 folders, 19 files, 8.50 MB, 8.50 MB in total.)
│       AFXRootkit2005.zip      280.78 KB
│       eeyebootroot.zip      79.37 KB
│       FU_Rootkit.zip      2.54 MB
│       Genc Kit.rar      901.56 KB
│       He4Hook215b6.zip      241.61 KB
│       hxdef100r_2005_11_20.zip      236.67 KB
│       MyNetwork.zip      1.30 MB
│       Nrootkit1.0.rar      451.64 KB
│       ntrootkit1.22.rar      136.10 KB
│       ntrootkit1.22无壳版.rar      101.54 KB
│       Nuclear Rootkit 1.0.rar      451.64 KB
│       patchfinder_w2k_2.11.zip      102.87 KB
│       rk_044.zip      252.44 KB
│       scantool.zip      1.04 MB
│       vanquish-0.2.1.zip      42.74 KB
│       vice.zip      65.64 KB
│       winlogonhijack-v0.3-src.rar      109.27 KB
├─Security      (2 folders, 9 files, 3.10 MB, 3.48 MB in total.)
│   │   ActivePorts.exe      119.50 KB
│   │   [Bifrost]AntiFrost.rar      170.08 KB
│   │   [捆绑检测]FBFD.exe      7.59 KB
│   │   EST-EvilHsu.rar      206.96 KB
│   │   IceSword_1.12.rar      1.97 MB
│   │   IceSword_en1.12.rar      564.98 KB
│   │   knlps.exe      8.00 KB
│   │   Scanner.rar      6.98 KB
│   │   魔龙EXE捆绑检测工具.rar      64.19 KB
│   ├─MT      (0 folders, 2 files, 62.93 KB, 62.93 KB in total.)
│   │       MT.exe      40.00 KB
│   │       MT.txt      22.93 KB
│   └─灰鸽子      (0 folders, 3 files, 328.00 KB, 328.00 KB in total.)
│           Kill_huigezi_2005.exe      268.50 KB
│           灰鸽子免疫 工具(GPKiller).exe      37.00 KB
│           灰鸽子清除器B3.exe      22.50 KB
└─Trojan      (19 folders, 0 files, 0 bytes, 131.73 MB in total.)
    ├─Assasin      (0 folders, 2 files, 3.39 MB, 3.39 MB in total.)
    │       Assasin2.3汉化版.rar      1.79 MB
    │       Assasin2.3原版.rar      1.60 MB
    ├─Beast      (0 folders, 2 files, 1.45 MB, 1.45 MB in total.)
    │       Beast v2.07 06-08-2004.zip      733.26 KB
    │       Beast v2.07 06-08-2004_unpack.rar      756.33 KB
    ├─Bifrost      (0 folders, 4 files, 2.55 MB, 2.55 MB in total.)
```

Number of Vulnerabilitie's increasing



Incidents reported to CNCERT/CC (scanning is excluded)

CNCERT/CC接收非扫描类网络事件年度统计



International cooperation needed

- Law issues
- Tech issues
- Info sharing
- Tech sharing
- Incident handling
- etc.

CNCERT/CC

Thanks

www.cert.org.cn