# Computer Crime

By FUNG Wai-Keung
Technology Crime Division
Hong Kong Police

# Topics

- Computer Crime Trend in Hong Kong
- Case Study
- Demos on Computer Intrusion
- Working Together

# Statistics

| Nature of Case | 1998 | 1999 | 2000 | 2001 Jan - May |
|---|---|---|---|---|
| Hacking | 13 | 238 | 275 | 51 |
| Publication of Obscene Articles | 13 | 32 | 6 | 0 |
| Criminal Damage | 3 | 4 | 15 | 15 |
| On-line Shopping | 1 | 18 | 29 | 10 |
| Theft | 0 | 0 | 0 | 7 |
| Others* | 4 | 25 | 43 | 15 |
| **Total** | **34** | **317** | **368** | **98** |

# Types of Cases

- Hacking decreased ??
- Old tools (subseven, backorifice) fade out with new anti-virus software
- Increased awareness
- Deterrent Punishments

# What about real hacking activities in Hong Kong ?

- Yes, all caused by old bugs
- LINUX and Windows NT exploits
- In Linux (LPRng, RPC_Statd, WU_FTPD and BIND)
- Default settings without patches

# What about real hacking activities in Hong Kong ?

- In Windows NT
- 90% of the attacks were through IIS 4.0 or 5.0 without patches
- More on Demonstrations later

# Signs of begin hacked

- Usually none, to an unwitting victim
- Normally detected by victim after 2 weeks
- Slowness of the computer (Check abnormal ports)
- Check User accounts
- Check File integrity
- Normally your computer is being hijacked for other services (DoS Zombie, IRC …)

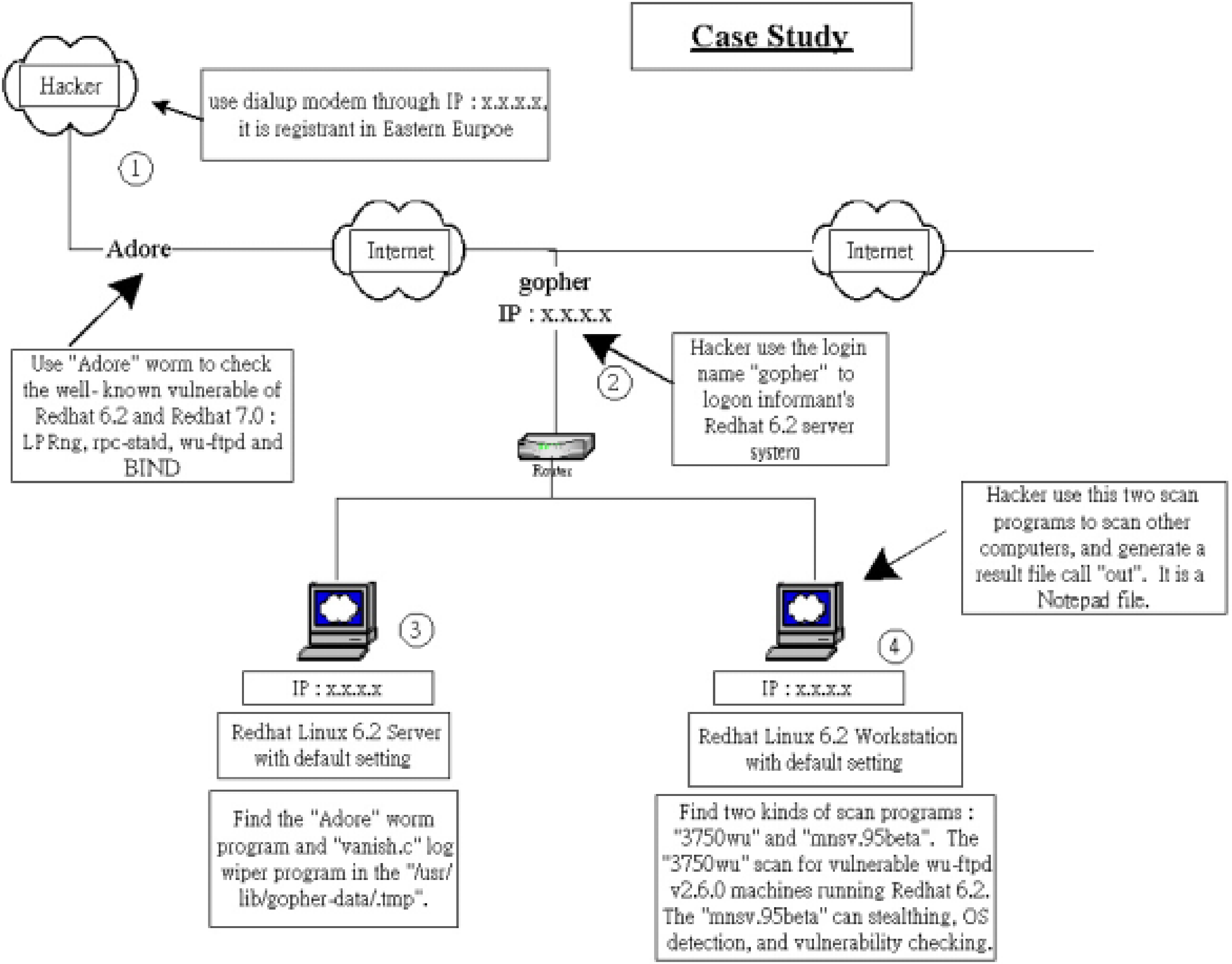
# Criminal Damage

- In 2001, the biggest problem is Viruses
- Cyberwar between CHINA and USA
- Major viruses contacted by victims in HK.
- Sadmind/IIS, Raman, Li0n
- The local culprits were mainly disgruntled workers

# Case Study

- Attacking using a worm to scan and later access into victimized computers
- Created backdoor account
- Set victimized computers to scan others
- Erase electronic footprints
- From Eastern Europe

# Case Study



① use dialup modem through IP : x.x.x.x, it is registrant in Eastern Eurpoe

Use "Adore" worm to check the well- known vulnerable of Redhat 6.2 and Redhat 7.0 : LPRng, rpc-statd, wu-ftpd and BIND

② Hacker use the login name "gopher" to logon informant's Redhat 6.2 server system

③ Redhat Linux 6.2 Server with default setting

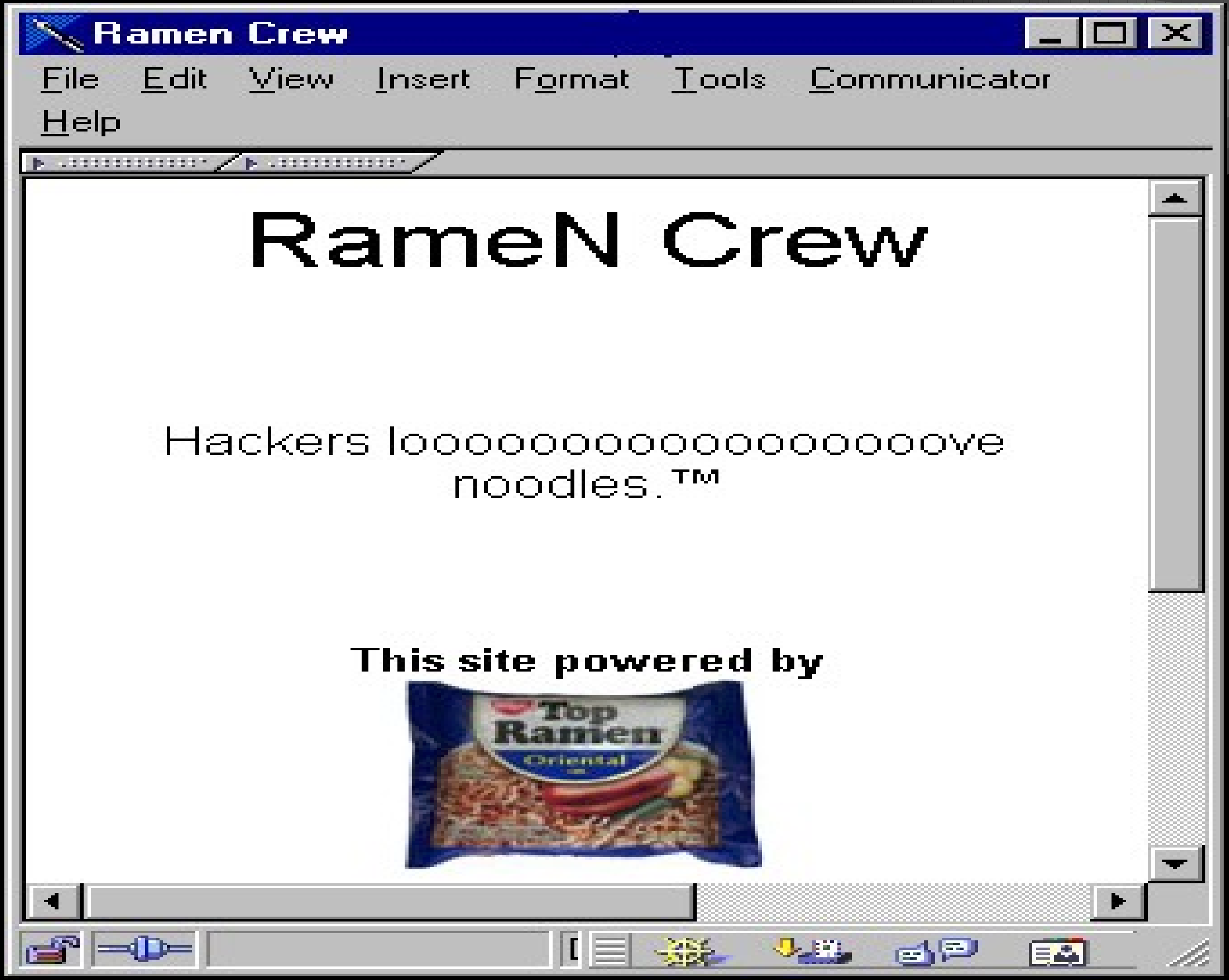
Find the "Adore" worm program and "vanish.c" log wiper program in the "/usr/lib/gopher-data/.tmp".

④ Redhat Linux 6.2 Workstation with default setting

Find two kinds of scan programs : "3750wu" and "mnsv.95beta". The "3750wu" scan for vulnerable wu-ftpd v2.6.0 machines running Redhat 6.2. The "mnsv.95beta" can stealthing, OS detection, and vulnerability checking.

Hacker use this two scan programs to scan other computers, and generate a result file call "out". It is a Notepad file.

# Linux Worm Ramen



RameN Crew

Hackers looooooooooooooooooove noodles.™

**This site powered by**

# Linux Worm Ramen

- The worm makes a hidden directory /usr/src/poop copies itself thereat
- Assumes superuser privileges.
- Defaces all webpages (eg. index.htm)
- Erases security files(eg. host.deny)
- Auto-starts itself each time (eg. /etc/rc.d/rc.sysinit)

# Linux Worm Ramen

- Files found in the ramen.tgz

  asp, asp62, asp7, bd62.sh, bd7.sh, getip.sh, hack1.sh, hackw.sh, index.html, l62 DiGiT LPRng, 17 Digit same, lh.sh, randb62, randb7, s62ronln rpc.statd, s7, scan.sh, start.sh, start62.sh, start7.sh, synscan62, sysnscan7, w62, w7, wh.sh, wu62
- the worm tries to secure the system by killing rpc.statd

# Linux Worm Ramen

- Log record

```
Jan 18 05:15:31 test ftpd[4350]: FTP session closed
Jan 18 05:15:33 test rpc.statd[330]: gethostbyname error for
    ^Xö&#732;¨^Xö&#732;¨^Yö&#732;¨^Yö&#732;¨^Zö&#
    732;¨^Zö
&#732;¨^[ö&#732;¨^[ö&#732;¨bffff750 8049710
    8052c20687465676274736f6d616e797265206520726f722
    0726f66
bffff718 bffff719 bffff71a
    bffff71b?????????????????????????????????????????????
    ??????? ?????????????????????????????????????????????
    ????????????????????????????????????????
???????????????????????????????????????????????????????
    ????????????????????????????????
?????????????????????????????????????????????????
```

# Linux Worm Ramen

```
root 4722 0.0 1.6 1648 752 pts/0 SN 15:46 0:00 sh ./scan.sh
root 4723 0.0 1.5 1648 748 pts/0 SN 15:46 0:00 sh ./hackl.sh
root 4724 0.0 1.5 1648 748 pts/0 SN 15:46 0:00 sh ./hackw.sh
root 4730 0.0 0.9 1252 460 pts/0 SN 15:46 0:00 tail -f .l
root 4731 0.0 1.6 1656 756 pts/0 SN 15:46 0:00 sh ./hackl.sh
root 4735 0.0 0.9 1252 460 pts/0 SN 15:46 0:00 tail -f .w
root 4736 0.0 1.6 1656 756 pts/0 SN 15:46 0:00 sh ./hackw.sh
root 4743 0.0 1.0 1148 492 pts/0 SN 15:47 0:02 ./synscan
   10.0.0
root 4746 0.0 0.0 0 0 pts/0 ZN 15:47 0:00 [synscan <defunct
root 4747 0.0 0.0 0 0 pts/0 ZN 15:47 0:00 [synscan <defunct
```

# Linux Worm Ramen

- Prevention

Upgrade

Redhat linux 6.2

rpm-Uvh ftp://updates.redhat.com/6.2/i386/nfs-utils-0.1.9.1-1.i386.rpm

rpm-Uvh ftp://updates.redhat.com/6.2/i386/wu-ftpd-2.6.0.14.6x.i386.rpm

# Linux Worm Ramen

Red hat 7.0

- rpm-Uvh ftp://updates.redhat.com/7.0/i386/LPRng-3.6.24-2.i386.rpm

# LIVE DEMOS

- Worm Generator
- Scan (whisker, uni.pl)
- Windows NT Browsing (Unicode)
- Windows NT Uploading (TFTP)
- Windows NT System Privilege(cmd.asp)

# More Scary News

- Planting card skimming bugs (hardware or downloaded) inside terminals to transmit credit card numbers
- 3G portable phones able to download viruses (Dialing Telephone number without prompting)
- SSL and HTTPS – already code to poison victims with wrong gateway, use man-in-the middle attack to substitute the public key.  Spoof DNS reply

# More Scary News?

- A malicious site could download virus implanted on their page  (ActiveX code on their webpage)

# How to Prevent it.

- Very Difficult !!!!
- Almost one vulnerability discovered every week
- Also Viruses.
- Constant Update and Read Security Advices

# Good Advices

- My references for this presentation
- www .securityfocus. com/
- WWW. Sans.org/
- WWW. Packetstorm.securify.com/
- WWW. Hongkongcert.org/

# Setting up Defense

- Add security tools ?
- Tripwire, COPS, TCP Wrapper, NMAP
- ftp://ftp.cert.org/pub/tech_tips/security_tools
- Use MD5 Snapshot now
- Try to move logs to a separate computer
- Firewall, use ‘Stateful Inspection’ at Hardware or Network layer

# Setting up Defense

- Is your internal network secured from staff?
- Internal Visits to hostile websites
- Do you allow downloads from any website (or trusted website)
- What is the security policy of your company
- Physical security
- Remote Access security

# Setting up Defense

- Check CERT (HK Productivity Council)
- Reporting to Police
- Calculate the damage including all potential damage (information in $$) and cost of security

# The way ahead

- Openness and cooperation between private sectors and government
- Continuous Training

# The End