Korea's experience of massive DDoS attacks from Botnet

April 12, 2011

Heung Youl YOUM Ph.D.

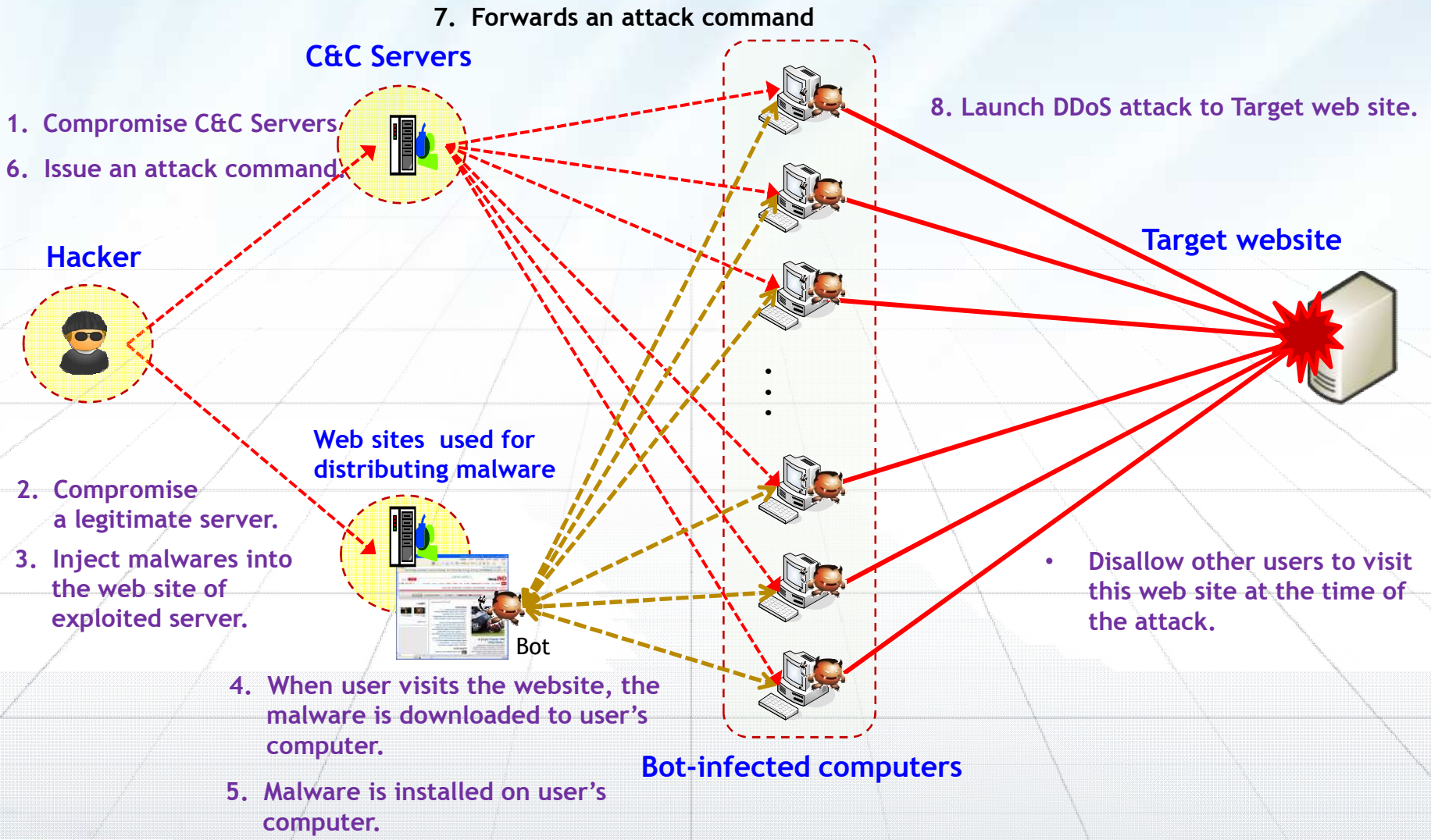
SoonChunHyang University, Korea
President, KIISC, Korea
Vice-chairman, ITU-T SG 17

Table of Contents

- Overview of 7.7 /3.4 Botnet attack
  - 7.7 DDoS Attack -scenario
  - 7.7 DDoS Attack - characteristics
  - 3.4 DDoS Attack -scenario
  - 3.4 DDoS Attack - characteristics
  - DDoS attack - how to respond to DDoS attack
- Countermeasures- legal & technical countermeasures
  - Technical countermeasure - DNS sinkhole scheme
  - Countermeasures- legal countermeasures
  - Countermeasures- online checking / help-desk service
- Concluding remark

DDoS Attacks – scenario

Typical DDoS attack scenario



Overview of 7.7 Botnet attacks

7.7 DDoS attack

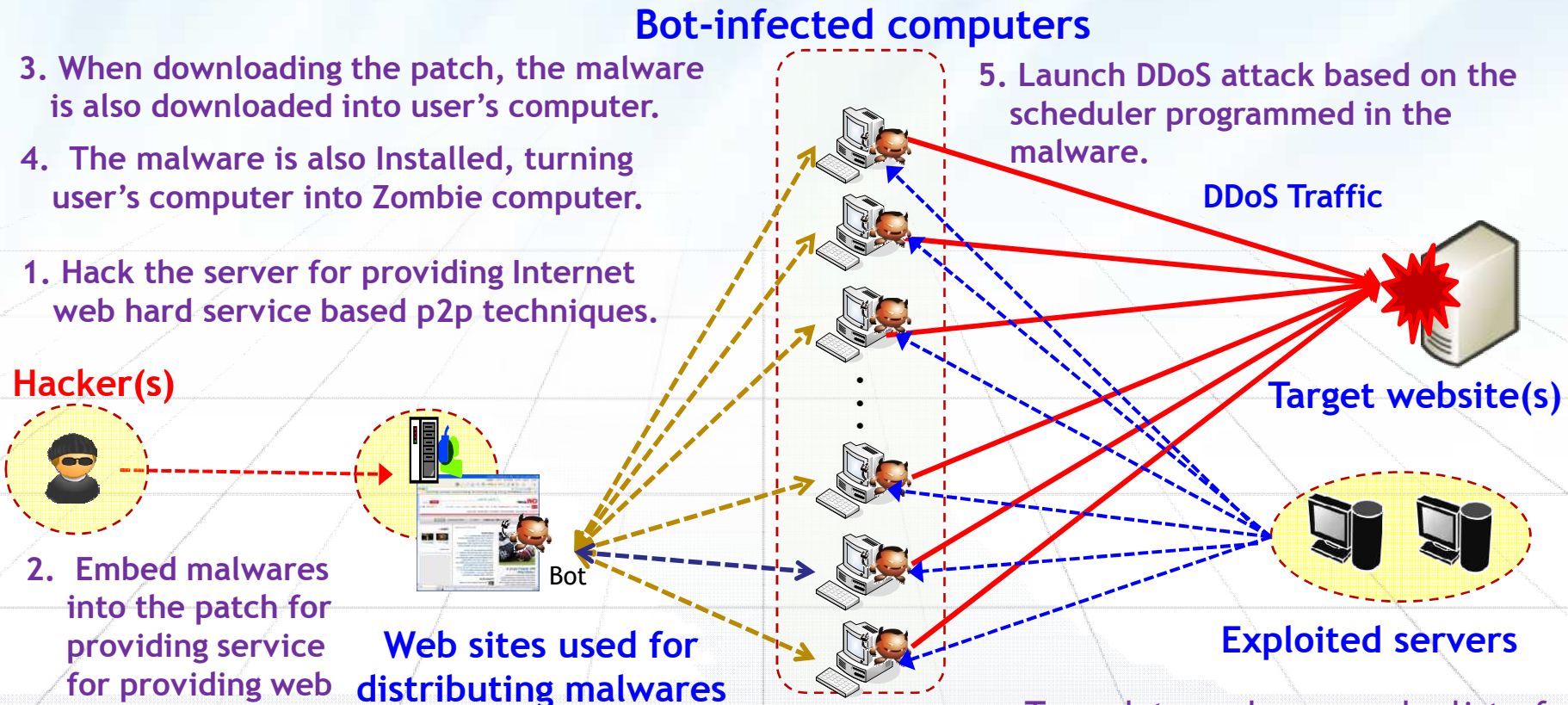
- Labeled 7.7 cyber terror by the media,
  - due to the first date when this attack occurred in Korea, July 7th, 2009 and carrying out three separate dates.
  - First massive DDoS attack, resulted in shutting down of victim sites for a while.

7.7 DDoS attack-characteristics

- No attack commands from C&C servers – most attack activities are initiated by each Bot-infected computer, instead of C&C server. 538 compromised servers mostly outside Korea were used.
- Sophisticated structure of malware used for DDoS attack
- Lots of zombie computers were used. - 115,044 zombie computers.
- Well organized and scheduled attacks scenario operated like a time bomb.
- Still, we don't know the purpose&source of this attack.

7.7 DDoS Attacks – scenario

7.7/3.4 DDoS attack scenario



- To update malware and a list of attack targets.

7.7 DDoS Attack – characteristics

Timelines of DDoS attacks

1st Attack(DDoS)

- Zombie computers: 26,209
- 7th July 18:00 PM ~ 8th July 8:00 AM, 2009
- Victims: 26 sites(US & Korea)

2nd Attack(DDoS)

- Zombie computers: 47,123
- 8th July 18:00 PM ~ 9th July 6:00 AM, 2009
- Victims: 16 sites(Korea)

3rd Attack(DDoS)

- Zombie computers: 41,712
- 9th July 18:00 PM ~ 10th July 6:00 AM, 2009
- Victims: 7 sites(Korea)

4th attack(Virus)

- To destruct the hard disk in Zombie computers
- 10th July 10:00 AM ~

- Total zombie computers: 115,044, Total Victim sites: 36
- Number of dedicated vaccines installed by users: 2,580,000

Overview of 3.4 Botnet attacks

3.4 DDoS attack

- Labeled 3.4 DDoS attack by the media,
  - due to the first date when this attack occurred in Korea, March 4th, 2011.
  - Due to the well organized public-private partnership and improved technical response established since the 7.7 DDoS attack, no serious damages were made.

3.4 DDoS attack-characteristics

- Many exploited servers such as malware distribution server, command distribution server – most attack activities first initiated by each Bot-infected computer. 748 compromised servers being mostly outside Korea were used.
- Similar structured malwares & attack scenarios as the 7.7 attack & are used for DDoS attack.
- 7 compromised local websites used for distributing malware to users
- Zombie computers used to 7.7 DDoS attack- about 116,299 zombie computers.

3.4 DDoS Attack – characteristics

Timelines of 3.4 DDoS attacks

1st Attack(DDoS)

- Zombie computers: 24,696
- 4th March, 2011 10:00 AM ~
- Victims: 29 sites

2nd Attack(DDoS)

- Zombie computers: 51,434
- 4th March, 2011 18:00 PM ~
- Victims: 40 sites

3rd Attack(DDoS)

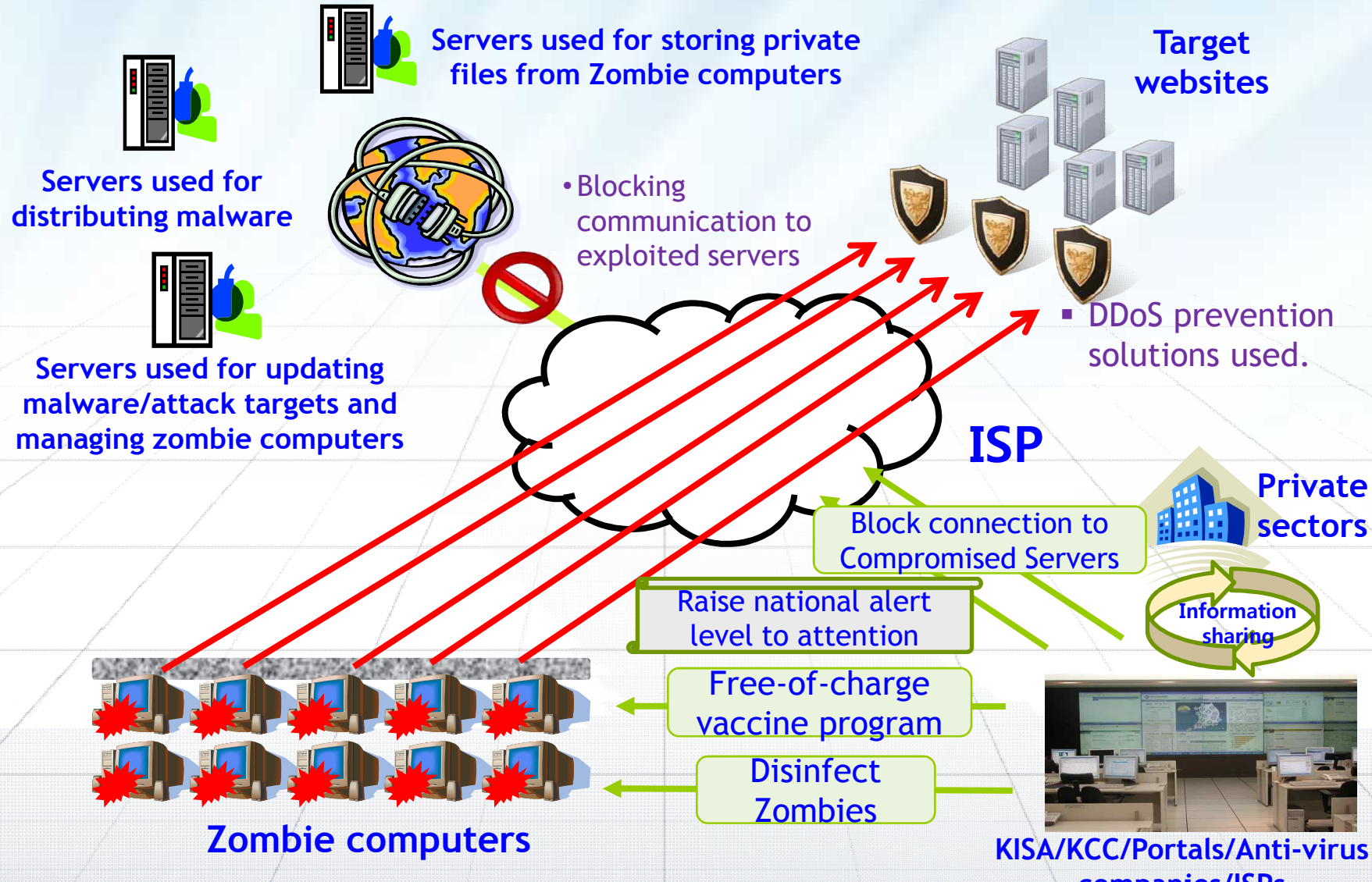
- Zombie computers: 11,310
- 5th March, 2011 10:00 AM ~
- Victims: 29 sites

4th Attack(DDoS)

- To destruct the hard disk in Zombie computers
- 5th March, 18:30 PM ~

- Total zombie computers: 116,299, Total Victim sites: 40
- Number of dedicated vaccines installed by users :11,510,000

DDoS attack – how to respond to DDoS attack



Countermeasures– three pillars

Technical framework

- Improved a real-time framework for enabling early detection, early warning, and effective response to DDoS attacks.
- Improve the real-time response system including as well as deploying DDoS prevention solutions and Bot-disinfection system.

Sharing of incident data

- Improve a real-time exchange framework of incident-related data and collaborations between KISA/KCC/NCSC and private sectors including major anti-vaccine companies and ISPs and among ISPs to respond to incidents collectively.

Legal framework

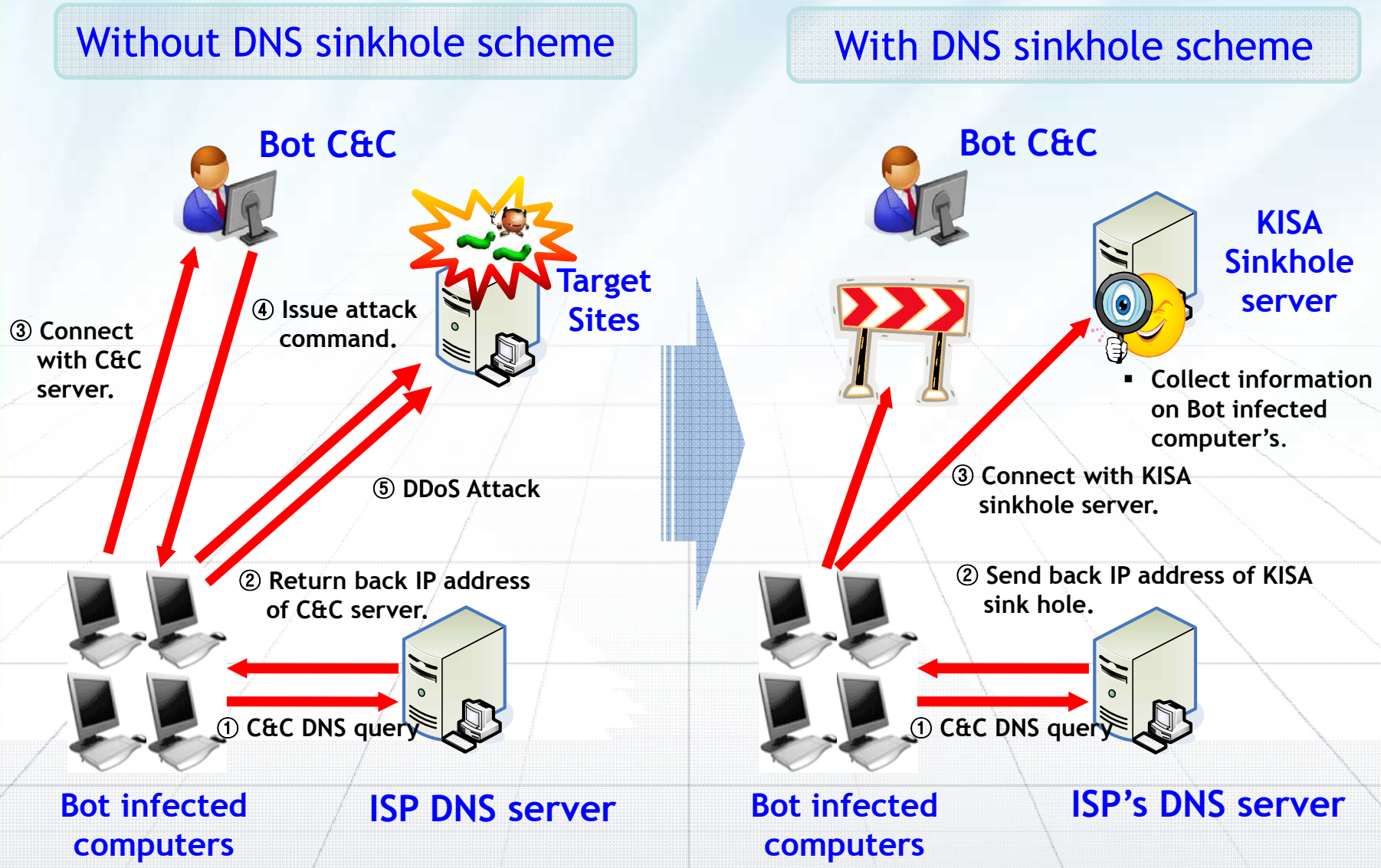
- To improve roles&responsibility of ISP, ASP, and Internet users to protect against DDoS attack by enacting “Law on malware spreading prevention” called “Zombie PC prevention law”.

Technical countermeasures – DNS sinkhole scheme

DNS sinkhole scheme

- Launched since 2005 by
  - KrCERT/CC(Korea Internet Security Center, http://www.krcert.or.kr/index.jsp), part of KISA(Korea Internet&Security Agency, www.kisa.or.kr).
- To protect aganist Botnet attacks, that is, to block the communication between bot-infected computers and C&C servers, making them to remain dormant.
  - With collaboration of ISP, the IP address of the domain name of the C&C servers are changed to that of DNS sinkhole server deployed by KISA.
  - As of September, 2010, about 60 organizations including major ISPs are employing DNS sinkhole scheme.
  - An average of 2,000 domain names are blocked by the scheme.
- Part of ITU-T X.1205 Supplement approved by ITU-T SG17 Question 4 .
- In case of Botnet using C&C server, it works against Botnet attacks.

DNS sinkhole scheme – effectiveness



Legal framework – a zombie PC prevention law (Draft)

Objectives

- A legal framework to ensure that early warning and effective response and recovery are in place.
- Filed at December 2010 by Korean parliament and expected to start a public consultation process from April 2011.

Contents

- Grant ISP's right to block communication from infected computers in an emergency state.
- Enable access to zombie computers for collecting malware's sample.
- Improve role and responsibility of ISP, ASP, users in terms of preventing zombie computer.

Issues

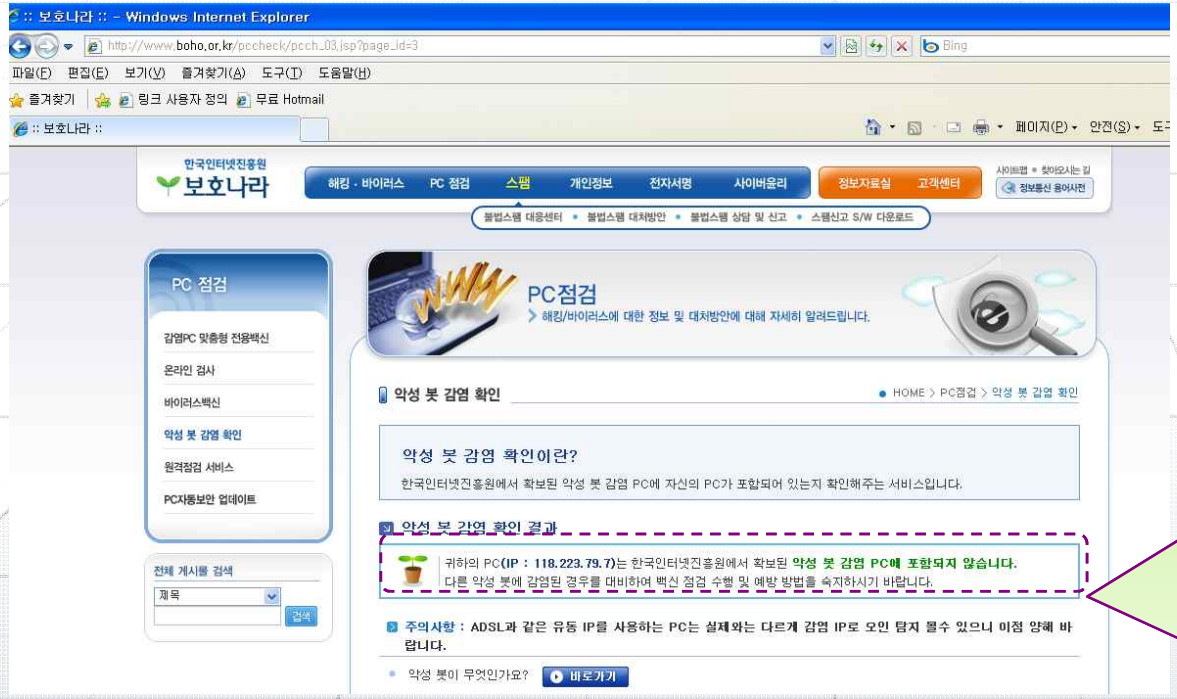
- Concerns about privacy concerns raised - concerns about potentially using deep packet inspection technology.

http://www.zdnet.com/blog/security/zombie-pc-prevention-bill-to-make-security-software-mandatory/8487

Countermeasure - Online bot-infection checking service

Online bot-infection checking service

- Provided by KrCERT/CC in KISA.
  - http://www.boho.or.kr/pccheck/pcch_03.jsp?page_id=3
- To check if the computer in question is infected with bots.
- Use database collected & monitored from DNS sinkhole scheme.

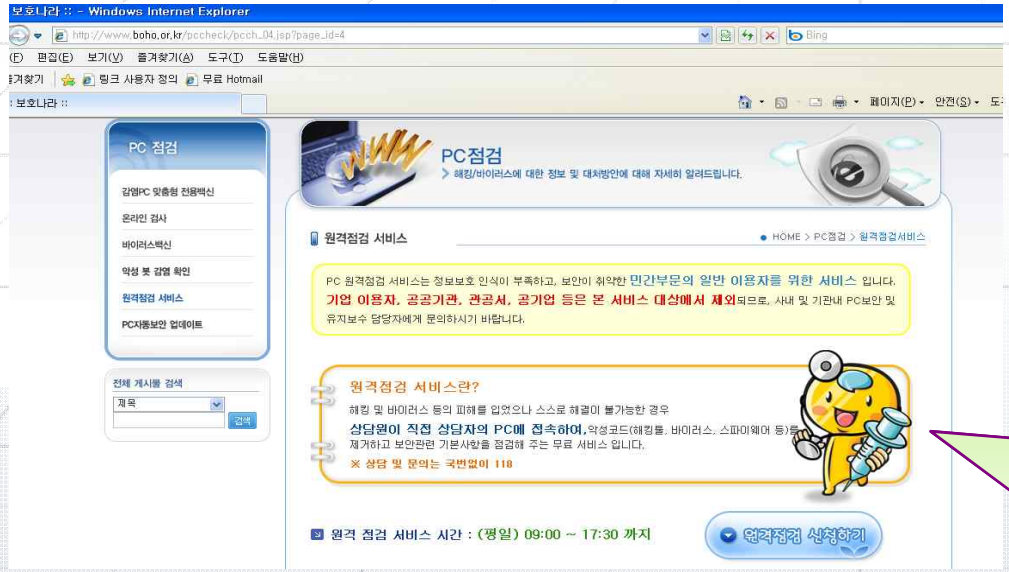


Your computers on IP address(x.x.x.x) is not infected by the malicious bots known to KrCERT/CC.

Countermeasure – Online help-desk service

Online help-desk service

- Is called e - 118 service
- Provided by the KrCERT/CC, part of KISA.
  - http://www.boho.or.kr/pccheck/pcch_04.jsp?page_id=4.
- Use telephone number “118” from any computer users in Korea.
- Remote help desk service is provided by KISA help-desk staffs to check if the computer is infected by virus, spyware, or malicious code, based on the requests reserved by users’ telephone calls.



- This service is provided from 9:00 to 17:30 only on weekdays.

Closing remark (1/2)

- Lessons learnt from this massive DDoS attacks
  - The incident data exchange based on global standards plays an important role in countering these attacks.
  - A real-time technical/administrative response systems should be established and improved.
  - In order to trace the attack source, a global scale real-time cooperation among investigation agencies is mandatory.
  - Establishing an effective legal framework which allows the technical/managerial countermeasures is important.
  - User awareness is important.

Closing remark (2/2)

- Future tasks for improvement.
  - Early attack detection, automated malware collection and behavior analysis, and effective disinfection system.
  - Effective network-wide response system including block of communication path to compromised servers from Zombie computers by ISPs.
  - Effective prevention user computers and websites from being infected by malware used for DDoS attacks
  - For example, online bot-infection checking & help-desk services should be expanded.
  - A new law on preventing spreading malicious code.

Thank you very much for your attention!!

CONTACT

E-mail: hyyoum at sch.ac.kr
Tel: +82-41-530-1328
Fax: +82-41-530-1494