7.7 DDoS Attack in Korea

2009. 8. 26

Ji-Young Lee
KRNIC of KISA

KISA
한국인터넷진흥원

7.7 DDoS Attack Timeline

1st Attack

- Date : '09.7.5 02:00 ~ '09. 7.5 14:00, '09.7.5 22:00 ~ '09. 7.6 18:00
- Target : (US) White House + 4 web sites

  (US) White House, Department of Homeland Security + 19 web sites

2nd Attack

- Date : '09.7.7 18:00 ~ 7.8 18:00, '09.7.7 21:00 ~ 7.8 07:00
- Target : (US) White House, NASDAQ, Washington Post + 11 web sites

  (KR) Blue House, Ministry of National Defense, National Assembly, NAVER(Portal) + 7 web sites

3rd Attack

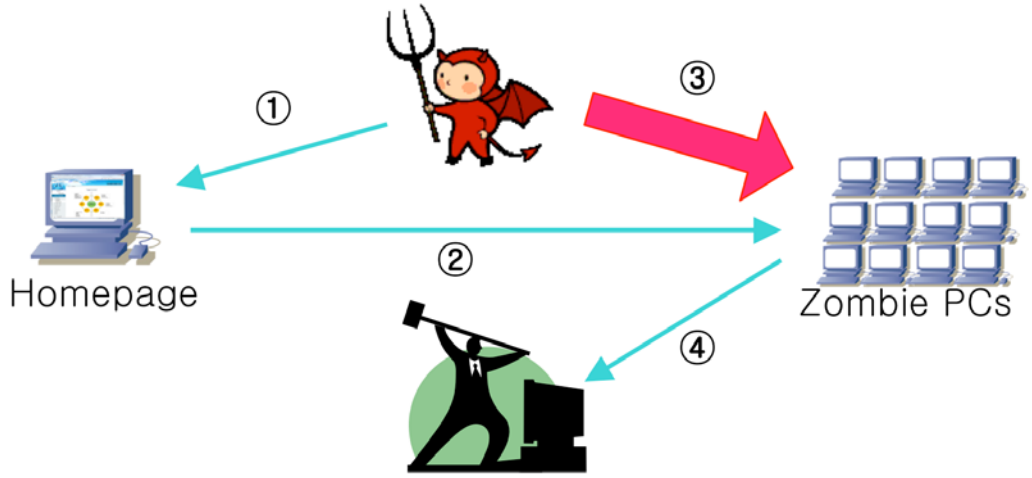
- Date : '09.7.8 18:00 ~ '09.7.9 18:00
- Target : (KR) Blue House, National Cyber Security Center, DAUM(Portal), PARAN(Portal), + 11 web sites

4th Attack

- Date : '09.7.9 18:00 ~ '09.7.10 18:00
- Target : (KR) NAVER(Portal), ChosunIlbo(Newspaper), G4C + 4 web sites

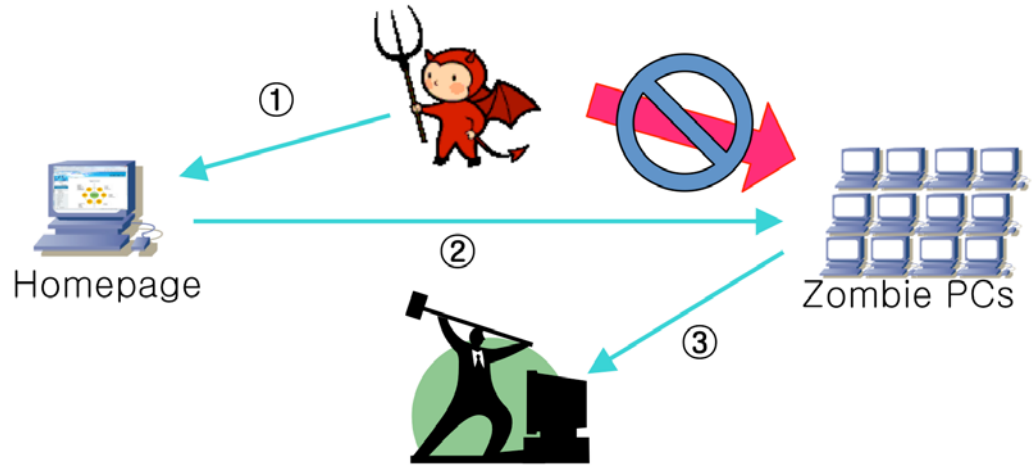
Comparison of DDoS Attack : Past and Now

DDoS Attack : Past



- C&C Server(or Hacker) sends realtime command to the zombie PCs

- Target and Attack schedule are programmed in the malicious code
  (No communication with C&C server)
- Some zombies are scheduled to delete the partition data in the hard disk



DDoS Attack : Now

How we reacted

KISA(Korea Internet & Security Agency)

- Collected zombie IP addresses from the victim sites and sent them to each ISPs(Total 127 ISPs in Korea)
- Uploaded vaccines in the major Korean portals and game sites and recommended Internet users to update them
- Opened KRNIC Whois to the victim sites to identify the zombie PCs

KISA KRNIC

ISPs

- Some of them were already aware of the zombie IP addresses from the IDS
- Contacted the subscribers and let them update their vaccines
- Disconnected their accesses

of zombie PCs from major ISPs

	Zombie PCs	Deleted	Not Deleted	Rate
ISP A	37,531	36,138	1,393	96.3%
ISP B	1,722	1,579	143	91.7%
ISP C	13,401	13,401	-	100.0%
ISP D	25,221	24,388	833	96.7%
Total	77,875	75,506	2,369	97.0%

2009. 7. 11

Lesson Learned

- It is helpful if ISPs distribute vaccines to protect their cust omers and their networks.
  - There are some ISPs in Korea who freely distributes vaccine and re commends users to update it
- Keeping correct Whois Data is very Important.
  - Not easy to identify C&C servers and zombie PCs
  - Especially when they are NATed, it's hard to track down.
- Identifying the location of zombie PCs needs collaboration among many countries.

Thank You

leejy@kisa.or.kr

한국인터넷진흥원
Korea Internet & Security Agency