# July DDoS Attack and Response

November 18th, 2009

KrCERT/CC
Jinhyun CHO

KISA
Korea Internet & Security Agency

## Contents

# I. July DDoS Attack Overview

## Introduction

- DDoS attack targeting Korea and US government and business web sites caused system failure and connection delay

## Attack Overview

**Target**

- Korea and US government and biz sites(bank, e-commerce and portal)
- Motivation : political propaganda, social disorder (still unknown and under LE investigation)

**Mechanism**

- Propagate malware through online storage site
- Embed the predefined target and schedule in malware

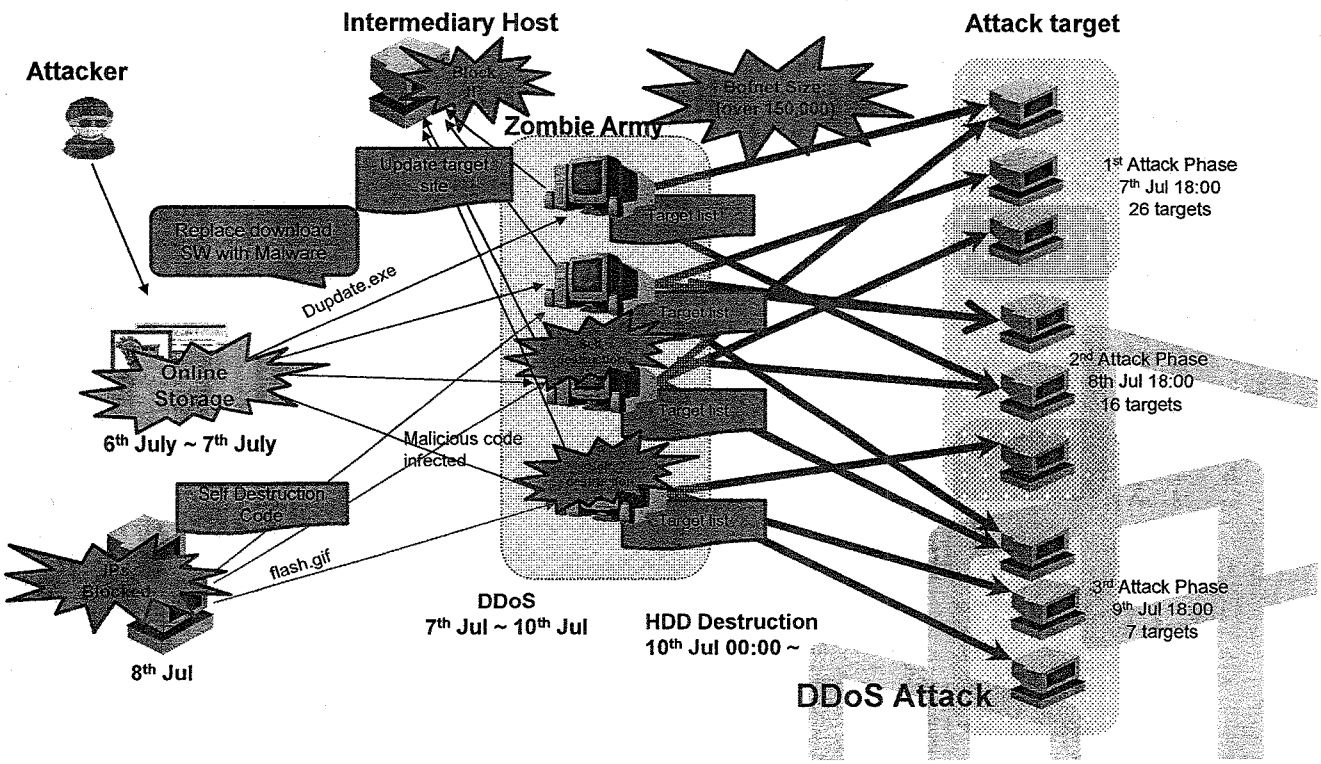
  Typical IRC botnet : real-time connection with C&C servers



# I. July DDoS Attack Overview

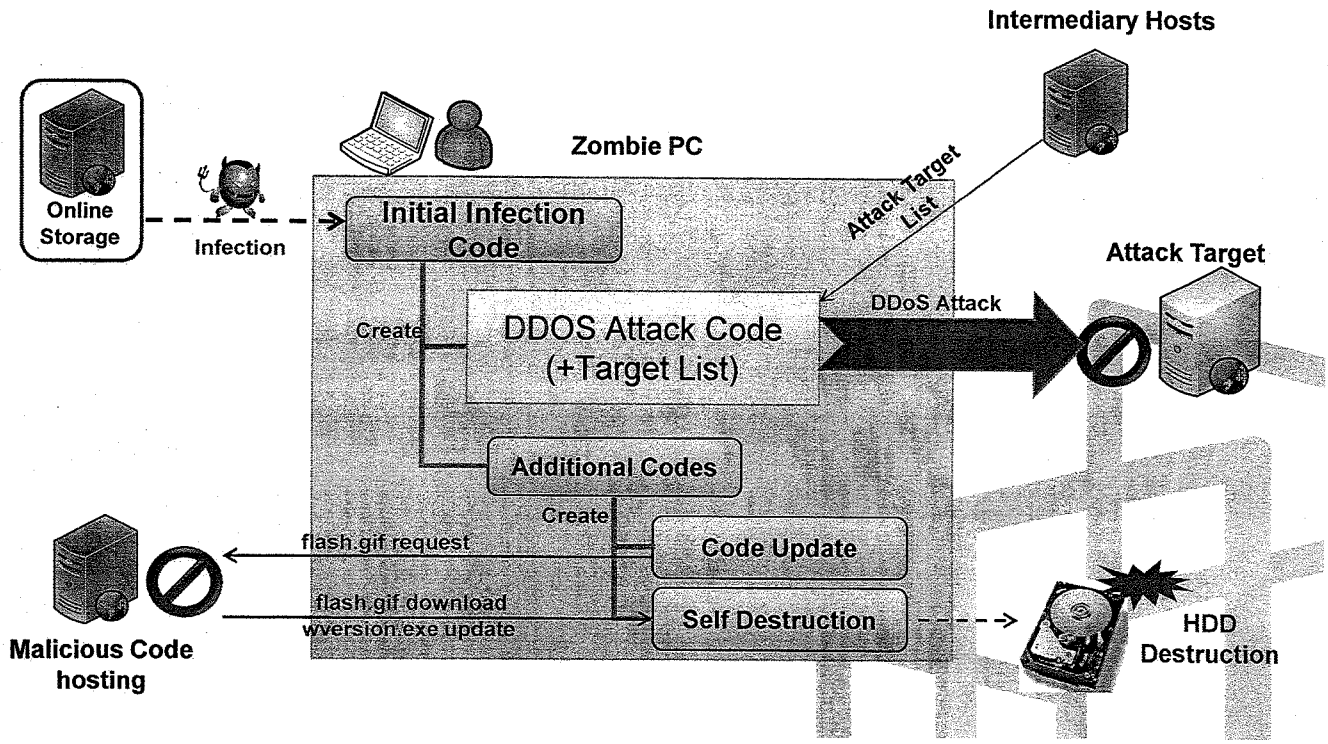
## The operation of July DDoS attack

TIME ZONE : GMT+9 (KST)



# II. July DDoS Attack in Detail

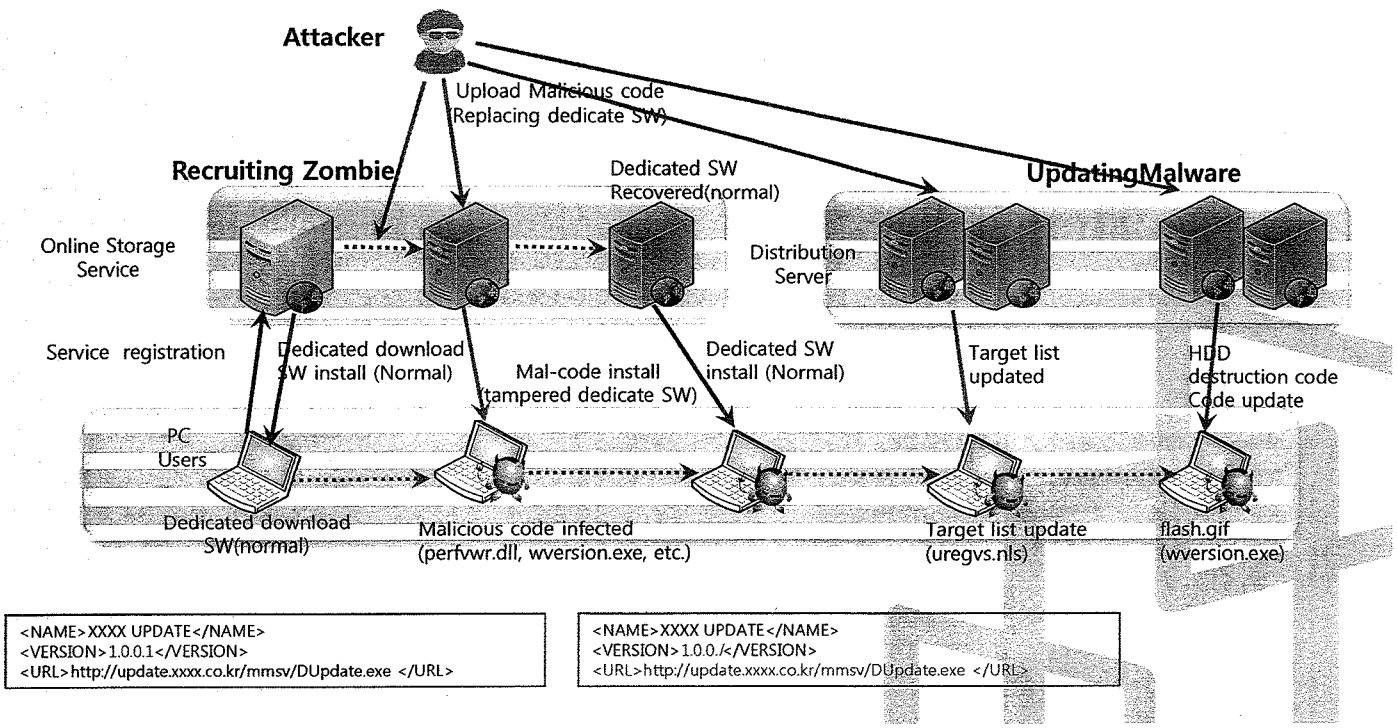
## Malware Components & Infection Mechanism





# II. July DDoS Attack in Detail


## Malware Propagation & Update Process

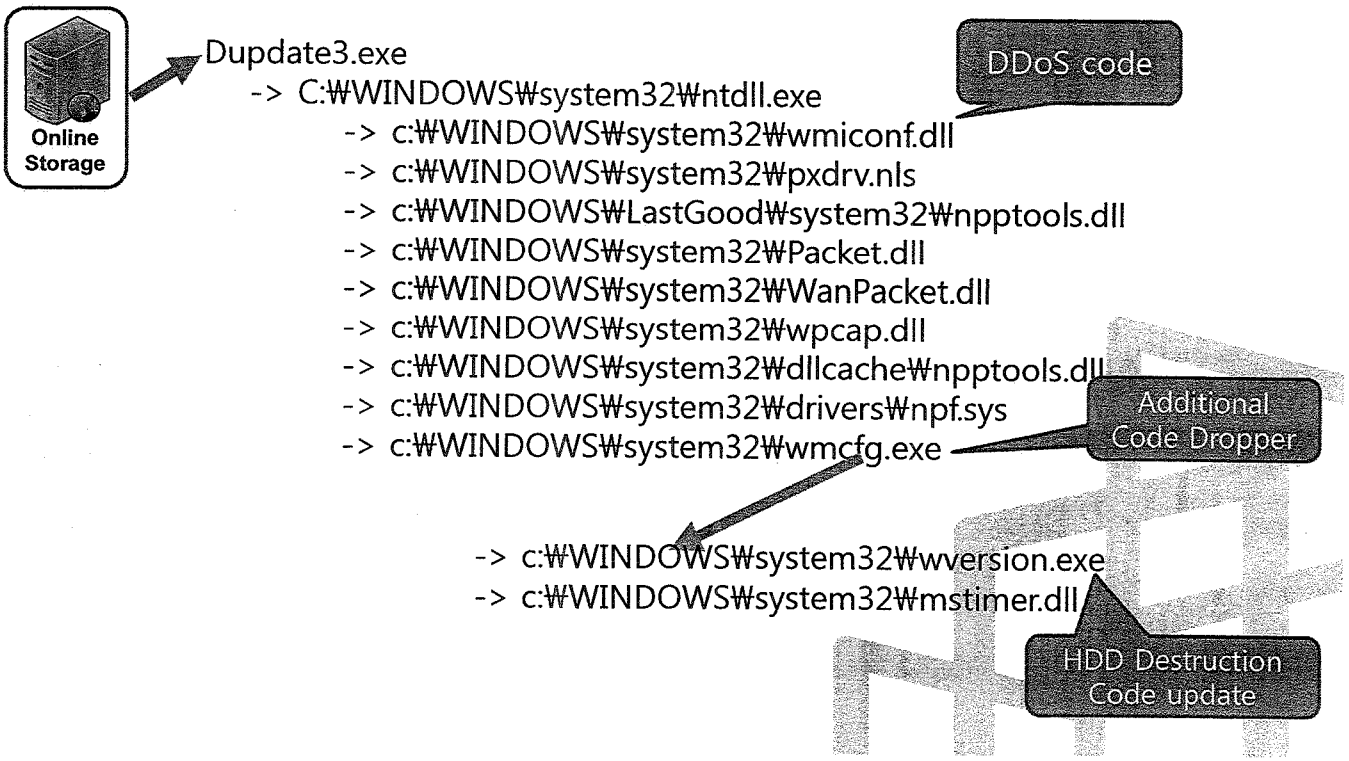



```
<NAME>XXXX UPDATE</NAME>
<VERSION>1.0.0.1</VERSION>
<URL>http://update.xxxx.co.kr/mmsv/DUpdate.exe </URL>
```

```
<NAME>XXXX UPDATE</NAME>
<VERSION>1.0.0./</VERSION>
<URL>http://update.xxxx.co.kr/mmsv/DUpdate.exe </URL>
```

# II. July DDoS Attack in Detail

## Initial Infection





# II. July DDoS Attack in Detail


## Hard Disk Destruction

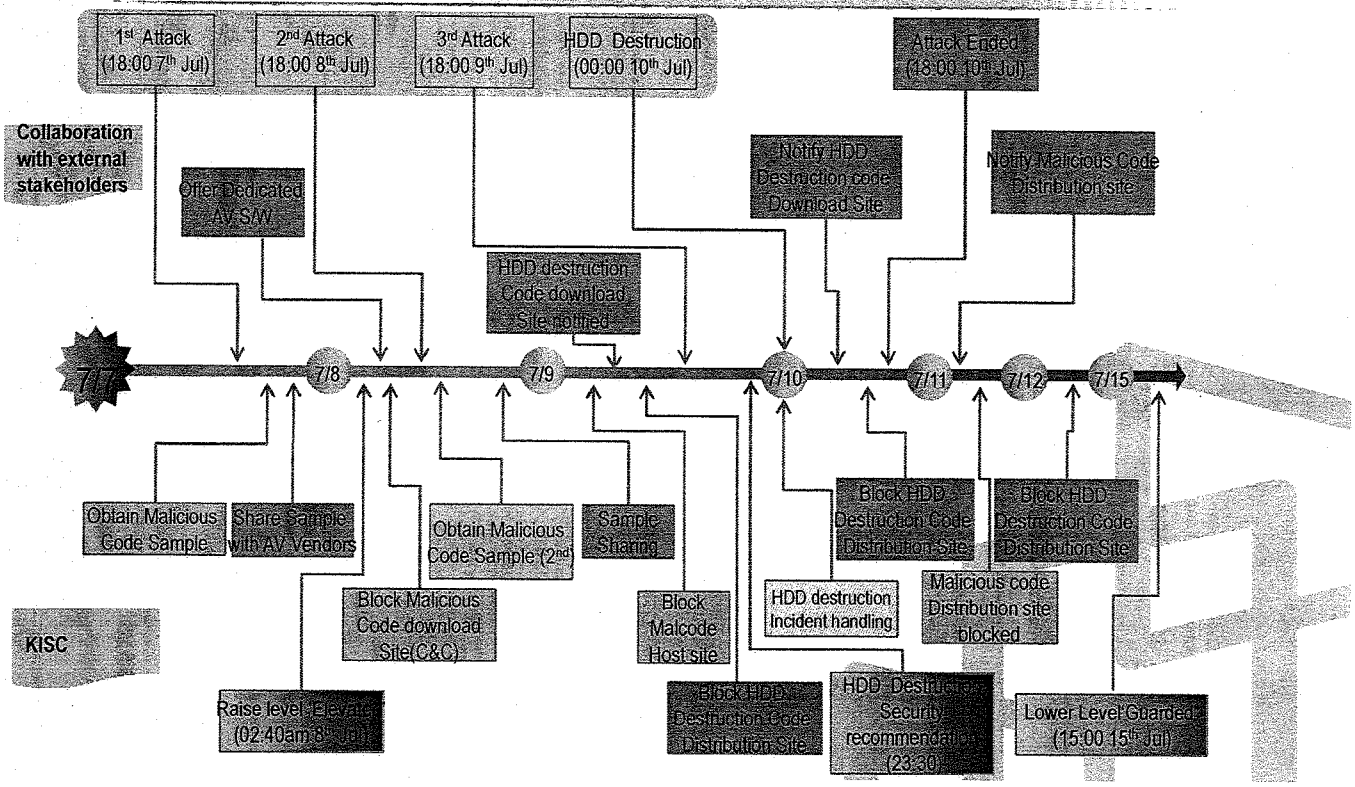
- HDDs in certain Zombie PCs destroyed
  - Destroy all kind of document file and program source file (overwrite and encryption)
  - Overwrite fixed disks MBR with specific value

```
008F1850  4D 65 6D 6F 72 79 20 6F 66 20 74 68 65 20 49 6E  Memory of the In
008F1860  64 65 70 65 6E 64 65 6E 63 65 20 44 61 79 00 00  dependence Day..
008F1870  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
008F1880  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
008F1890  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
008F18A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
008F18B0  00 00 00 00 55 55 55 55 55 55 55 55 55 55 55 55  ....UUUUUUUUUUUU
008F18C0  55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
008F18D0  55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
008F18E0  55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
008F18F0  55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
008F1900  55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
```

# III. Korea Internet Security Center's Response

## Timetable of Response to DDoS Attack

TIME ZONE : GMT+9 (KST)





# III. Korea Internet Security Center's Response


## Analysis & Emergency Response

- **On-site Incident analysis**
  - Analyze abused hosts and collect malware
    - Zombie PCs and servers
    - To identify malicious code spread site
    - To discover the correlation among hacking incidents
  - Analyze malicious code
    - To identify C&C server and takedown abused sites
- **Blocking exploited and abused sites or IPs**
  - C&C server IPs
  - HDD destruction code hosting sites

# III. Korea Internet Security Center's Response

## Response Support for Victim & Zombie PC Owners

- **Develop emergency response techniques**
  - Attack filtering rule from the security systems
- **Enforce zombies to be cured**
  - With major ISPs (happy call service)
  - Provide dedicated AV program from local vendors
  - Zombie notification service through KISC's security portal site (www.boho.or.kr)
- **Raise the awareness of the general public**
  - Mass Media : TV News and news paper
  - Dedicated banner and information page published in major domestic portals(Naver, daum, etc.)

# III. Korea Internet Security Center's Response

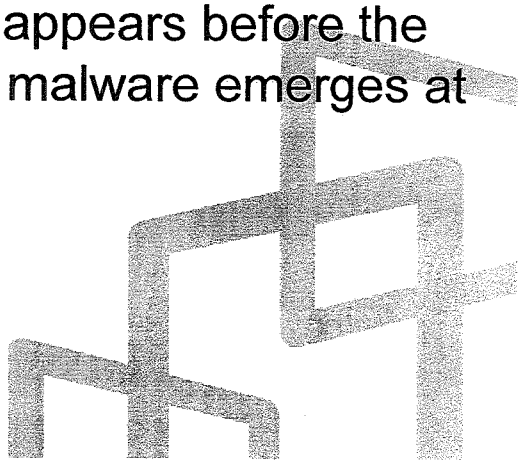
## Collaboration with Domestic and Foreign Partners

- **Cooperation with Key Partners**
  - Share analysis result with local security vendors
  - Discuss with foreign collaborators
    - Op-trust group
    - Google for identifying source of malicious code
  - NIS(NCSC) and NPA

# IV. July DDoS Attack Summary

## Difficulties to Identify DDoS Malware

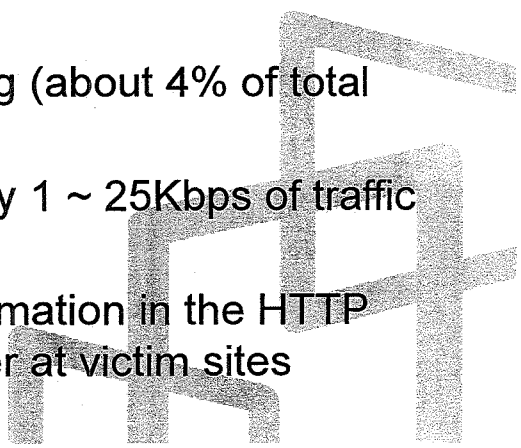
- Evidence destruction
  - All Internet browsing history in the Zombies is removed so that it is impossible to identify malware origin
  - Although no infection evidence appears before the malicious code start attack, the malware emerges at the startup



# IV. July DDoS Attack Summary

## Sophisticated DDoS Attack

- **Difficulties to respond**
  - Small amount of attack traffic generated from zombie
    - Less than 50Kbps of network traffic per PC observed
  - Various attack methods
    - Small amount of UDP/ICMP flooding (about 4% of total attack traffic)
    - Small amount of HTTP request (only 1 ~ 25Kbps of traffic measured)
    - http get flooding varying agent information in the HTTP request header made difficult to filter at victim sites



# IV. July DDoS Attack Summary

## Difficulties to Stop DDoS Attack

- **No Real-time C&C but pre-scheduled attack**
  - General IRC botnet controlled by C&C server so DDoS attacks caused by those kinds of botnet are relatively easy to control (by blocking C&C server)
  - Even though KISC blocked *certain kind of* C&C server attack did not stopped
  - The only way of response is removing individual zombie PCs (150K hosts!!!)

```
00000110h: 00 00 00 00 00 00 00 00 00 00 00 00 50 00 00 00 ; ............P...
00000120h: FF 07 00 00 32 00 00 00 00 00 00 00 00 00 00 00 ;    ...2...........
00000130h: 38 88 E3 40 00 00 00 00 58 88 E3 40 1E 00 00 00 ; 8볋@....X볋@....
00000140h: 03 00 00 00 1E 00 00 00 50 00 00 00 1F 00 00 00 ; ........P.......
00000150h: C0 61 14 00 77 77 77 2E 70 72 65 73 69 64 65 6E ; 쿰..www.presiden
00000160h: 74 2E 67 6F 2E 6B 72 3B 38 30 3B 67 65 74 3B 2F ; t.go.kr;80;get;/
00000170h: 3B 3B 00 02 00 77 77 77 2E 6D 6E 64 2E 67 6F 2E ; ;;...www.mnd.go.
00000180h: 6B 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; kr..............
00000190h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000001a0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
```

Attack time, destination, port, and method, etc.

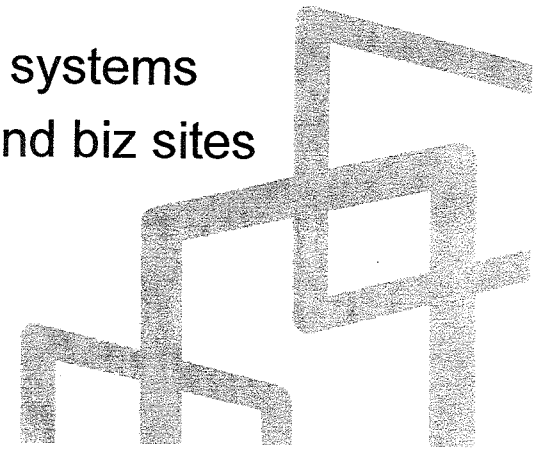
# IV. July DDoS Attack Summary

## New Attack Vector : S/W Integrity

- **Exploits Online Storage Service S/W**
  - Replace the download S/W with Malware
    - Suspicious situation has monitored but could not analyze abused host
  - Became zombie regardless of security patch installed
    - All PCs installed file download software are infected by malware through software update procedure

# V. Conclusion

- The big picture is still behind curtain
  - By who? Why?
  - Complete figure?
- Need to develop new response approach for further attacks
  - Technical measures, response systems
  - Protection of individual users and biz sites
  - Collaboration with partners



# THANK YOU !!!

한국인터넷진흥원
Korea Internet & Security Agency