



IT R&D Global Leader

What was wrong with our DDoS defense strategy against 7.7 DDoS attack in Korea

2009. 9. 29.

Jintae Oh

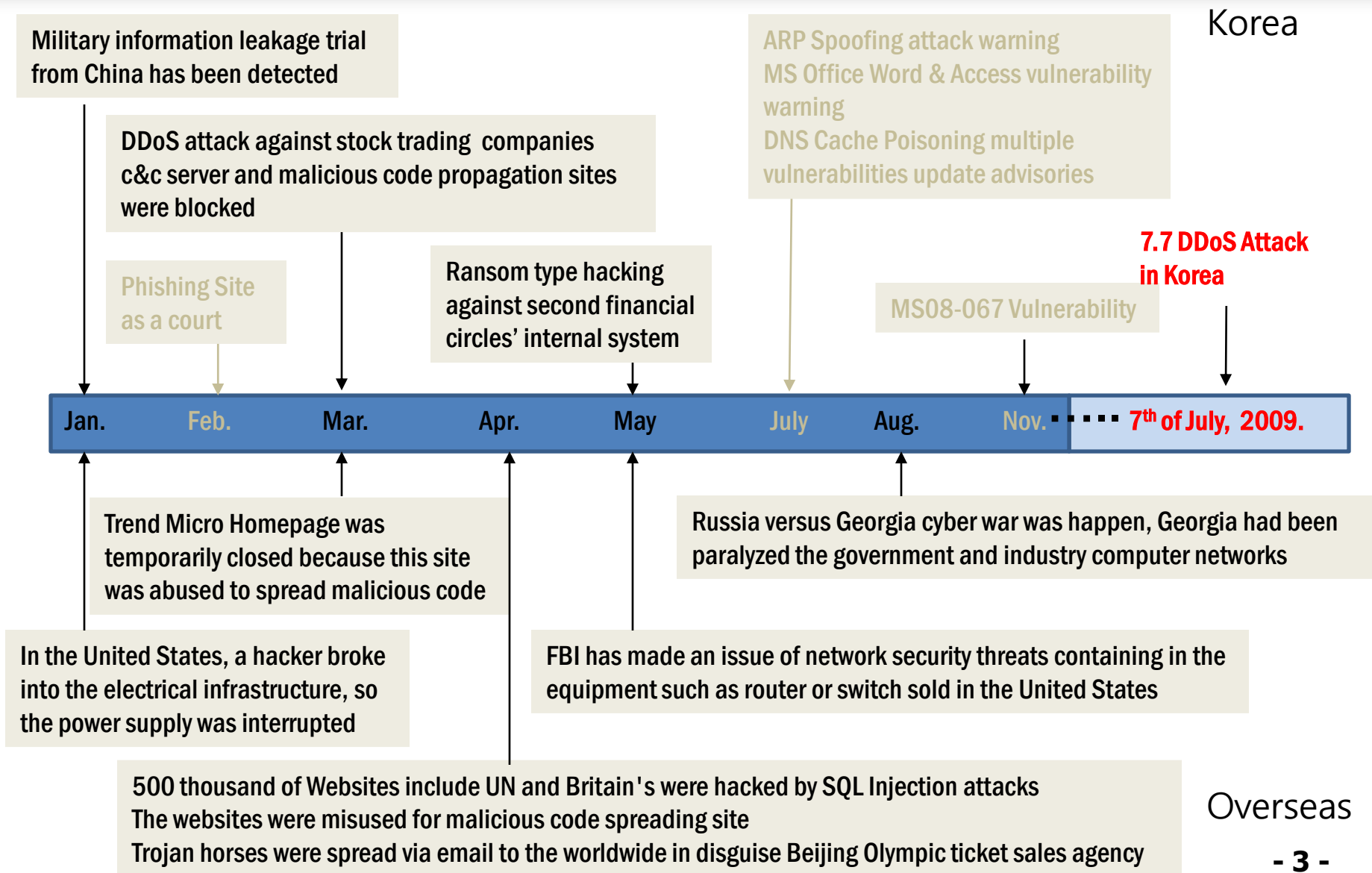
[showme@etri.re.kr]

ETRI

Electronics and Telecommunications
Research Institute

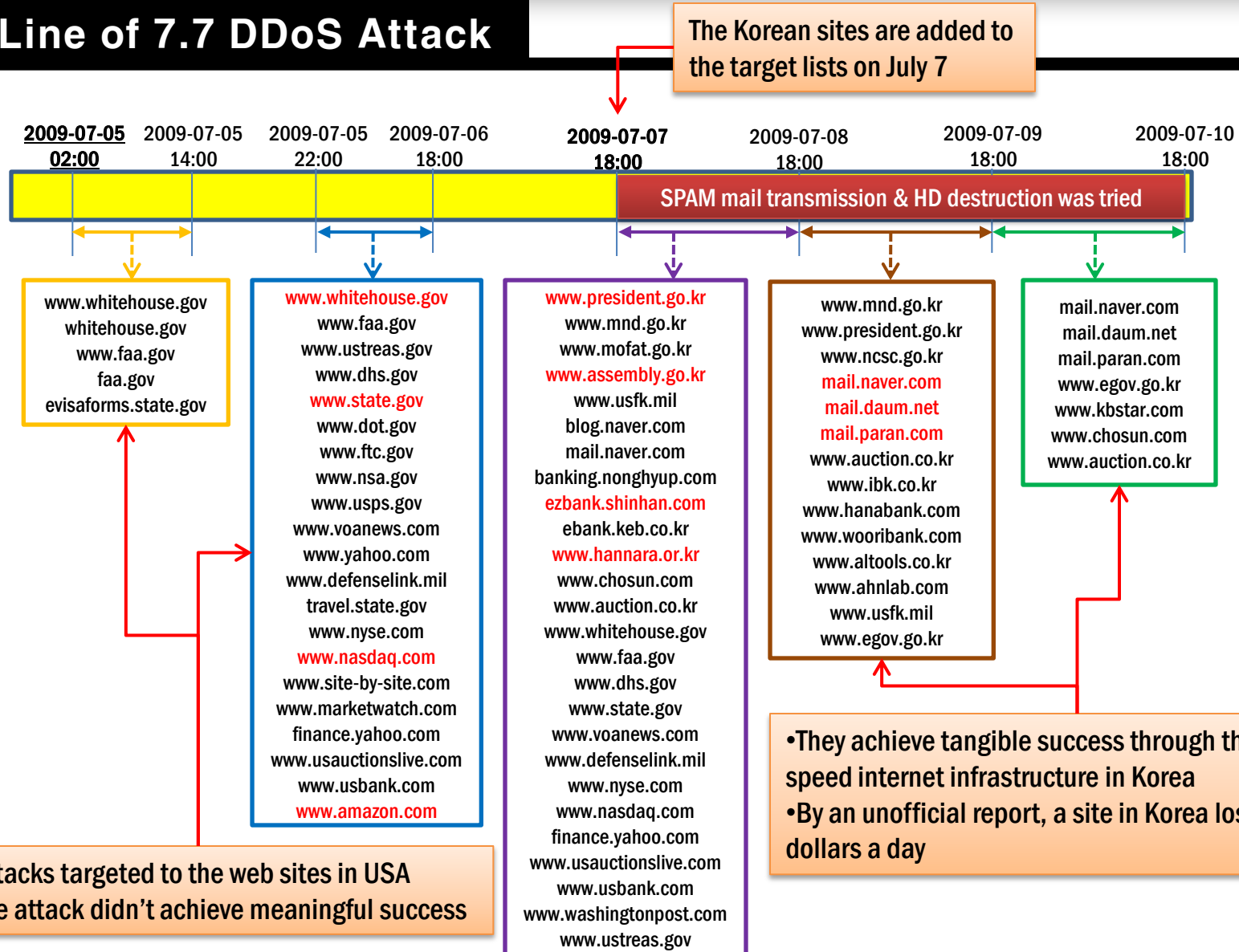
- I Cyber Attack Incidents**
- II 77 DDoS Attack**
- III Responses and Check Points**
- IV New DDoS Attacks Defense Framework**
- V Conclusions**

Cyber Attack Incidents (2008~)



7.7 DDoS Attack(1)

TimeLine of 7.7 DDoS Attack



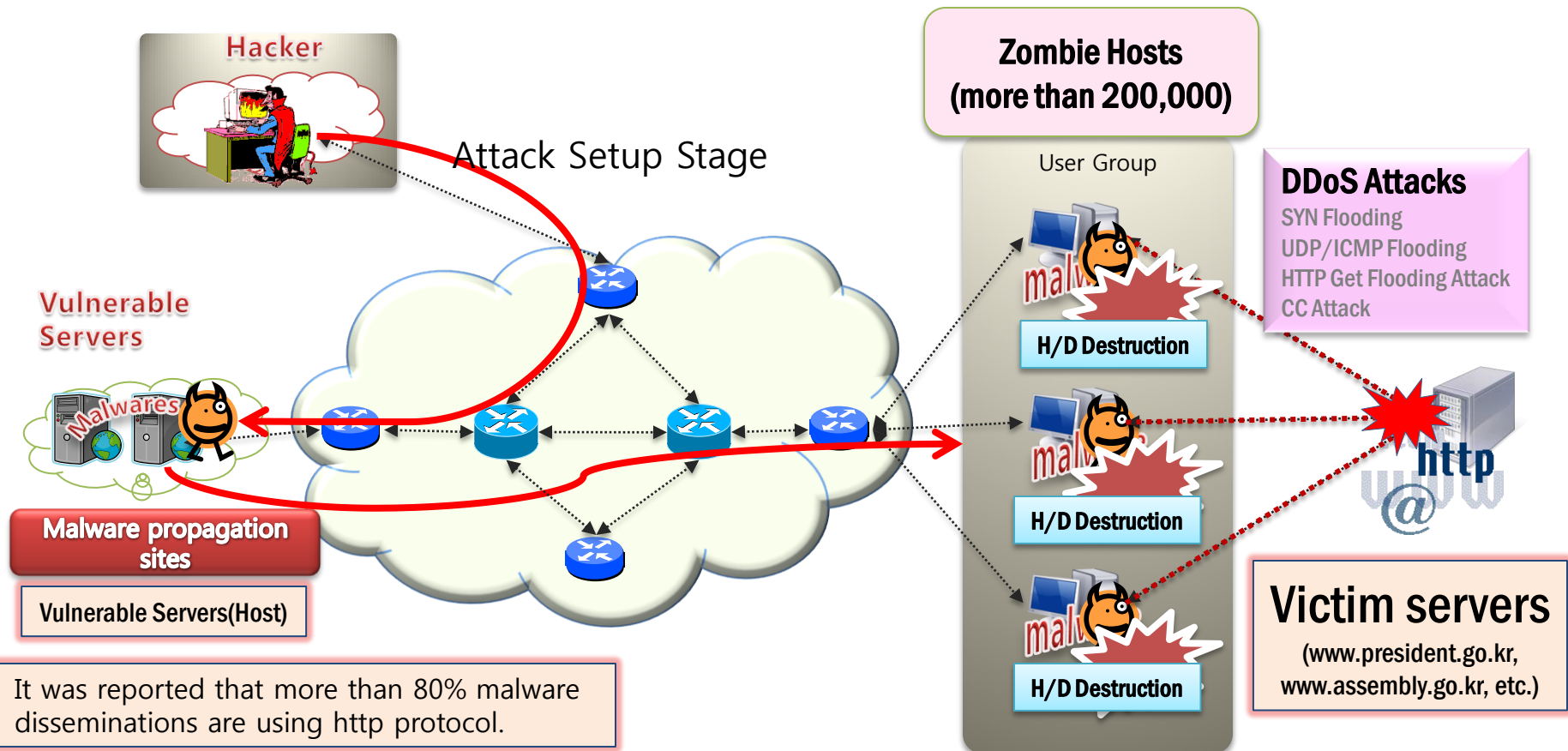
7.7 DDoS Attack(2)

7.7 DDoS attack outline

- On July 7, Zombies started to **attack major web sites in Korea** such as Blue House, a political party, banks, and some major portal sites
- The attack changed to **several phases**
 - Phase1 : DDoS Attack against web sites **in USA**(from 2009-07-05)
 - Phase2 : DDoS Attack against web sites **in Korea**(from 2009-07-07)
 - Phase3 : **SPAM mail transmission**
 - Phase4 : **Self destruction** (Hard disk destruction)
- No traditional C&C Server (Non-Real time control)
 - It was a new type of attack that did not employ the traditional Command & Control server
 - **Back tracing and blocking was difficult**
 - **Attack target list** was already included in the first malware
- Sophisticated Attacks
 - Various types of attacks are mixed such as **TCP SYN Flooding**, **HTTP Get Flooding**, **CC Attack**, and **UDP/ICMP Flooding**
 - More than 90% packets were HTTP GET or CC attack
 - Attack traffic was **relatively smaller than usual DDoS attacks**, therefore it is very difficult to detect
 - Less than 100pps and 1Mbps

7.7 DDoS Attack(3)

7.7 DDoS Attack Overview



Responses against 7.7 DDoS

DDoS response (1)

- Malware propagation servers IP block
 - The malware propagation IPs were found by hands (need automation)
 - We might miss some IPs from blocking list
 - We detected malware downloading events on July 8
- Increasing the network and server capacity
 - It gave only temporal solution
 - If more than millions of Zombies involved in the future, what we can do?
- Packet signature
 - Some anti-DDoS system blocked the attack packet with signature generated by hands
 - Failed to the real time response
 - L7 equipment can do the same function
 - Why do we have to purchase a new machine for DDoS?
 - Easy to obfuscate
- Moving target (Change URI temporally)
 - Ex) mail.xxx.xxx -> mail1.xxx.xxx
 - The attack technique also will evolve

DDoS response (2)

- How accurate dose the detection result?
 - We usually use the traffic anomaly to detect a DDoS
 - Detection Rates are not good. High false alarm is generated
 - How could the flesh cloud be separated from attack?
 - More accurate DDoS attack detection algorithm is needed
 - Zero False Positives with low False Negatives
- How quickly can we detect the DDoS attack?
 - Milliseconds? Several seconds? Before the victim's service is halted?
- How efficiently can we block the attacks?
 - Mitigation(Rate limit): Legitimate traffic also could be dropped
 - Session based (ACL): IP spoofing problem
 - Per packet based (Signature): Easy to obfuscate
- It's not efficient to defense the DDoS attack after the attack outbreak
 - What should we do to prevent from DDoS attack?
 - Isn't there any proactive attack defense mechanism at all?

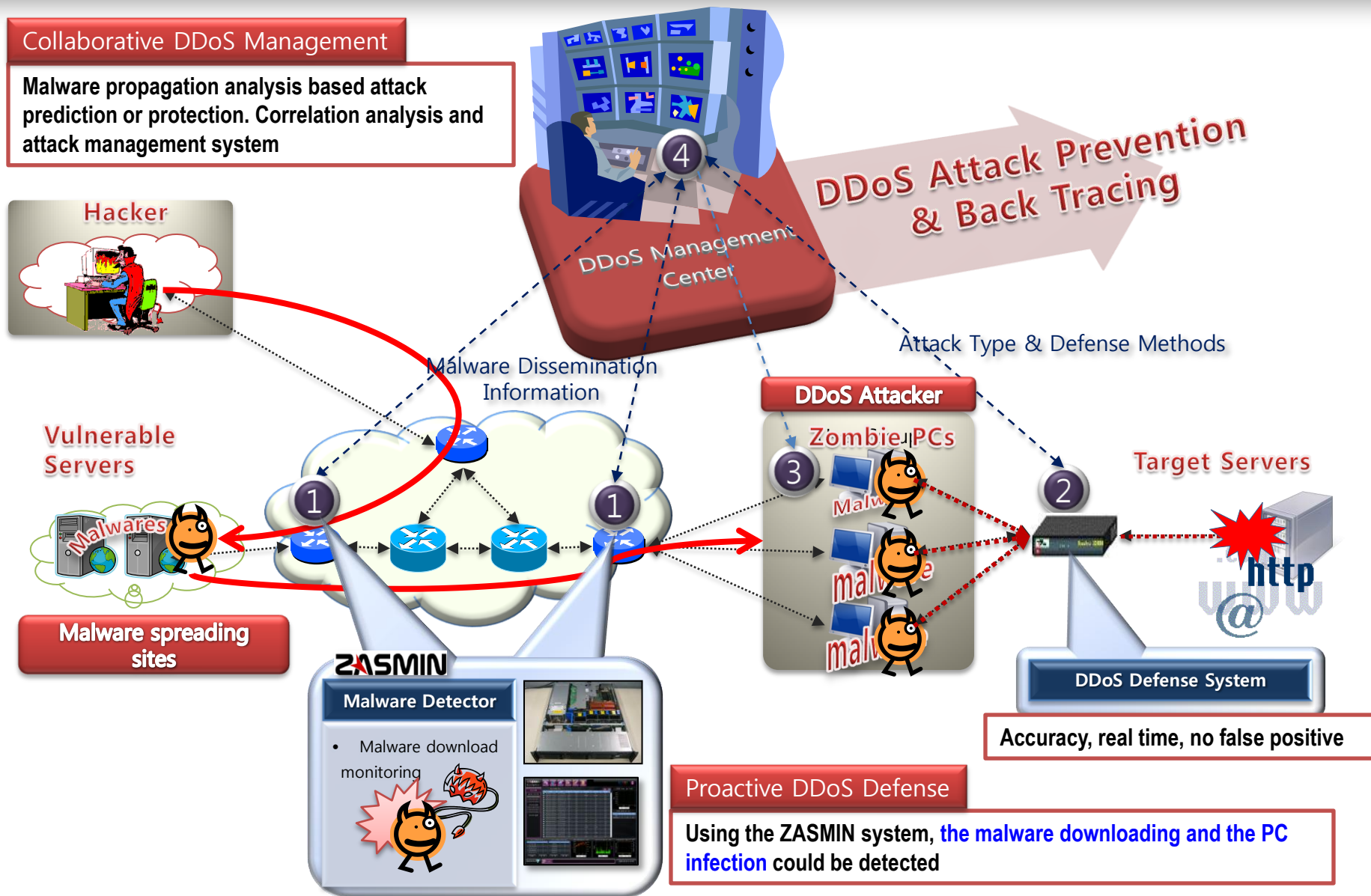
How to defense

- We only focused to reduce the DDoS attack traffic
 - Signature based packet filtering
 - It could not provide real time defense
 - Non of Anti-DDoS system has zero false positive detect algorithm
 - ACL could not be used
 - Traffic mitigation could hurt legitimate user also
- Malware propagation monitoring and analysis
 - Malwares were collected from Zombies and analyzed at the post
 - We need automation to reduce the collecting and analyzing time
 - It will give more information, if the malware propagation logs or samples are available
- Collaborative DDoS monitoring technique is needed
 - Now we only have traffic engineering result
 - Do you satisfy with the result?
 - Attacker IP and executable file download event should be processed in a system
 - Still, We don't know the attacker
 - Vulnerable servers log file gives limited information
 - DDoS attack environments were prepared before the attack
 - We need a proactive defense mechanism

DDoS Defense Framework

Collaborative DDoS Management

Malware propagation analysis based attack prediction or protection. Correlation analysis and attack management system



Malware detection

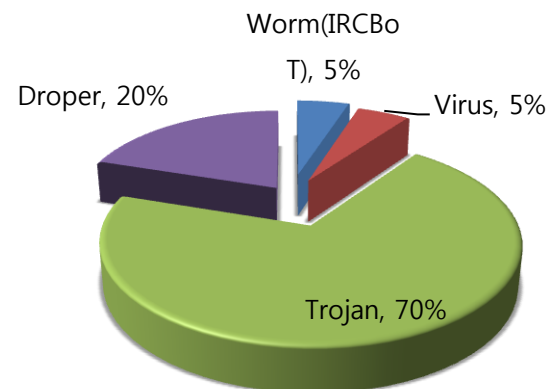
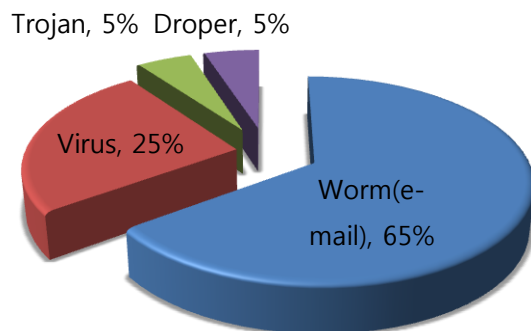
- Honey pot is OK?
 - Honey pot can collect the self-propagation malware
 - Is it the same malwares between the enterprise network and honeynet?
 - If it is not, what can we do?
- Can we collect malware in the network?
 - Is it feasible?
 - We have to consider the service header of the data
 - Are executable files exchanged via internet?
 - Can we check the maliciousness of the files?
 - If we have known normal and malicious list, we can reduce the unknown
- Is it helpful the malware propagation log and sample file for protecting the DDoS?
 - Known malware (ex. netbot)
 - We can control the infected host very easily
 - Unknown malware
 - After finding attacker's IPs from the anti-DDoS system, we can extract some file download correlations from the malware monitoring system
 - It will give a big picture on the relationship of DDoS attack and malicious codes

Change of Malware and spreading

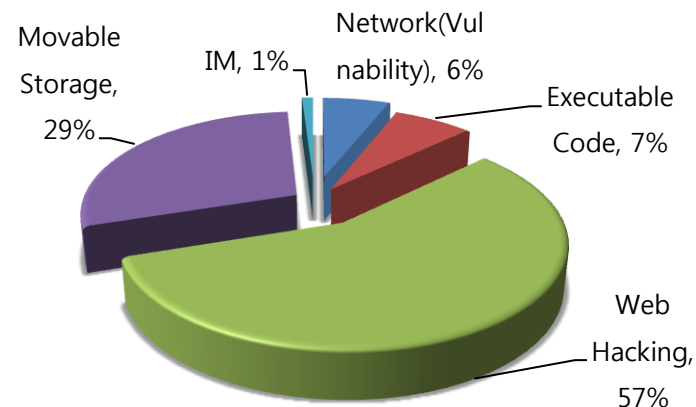
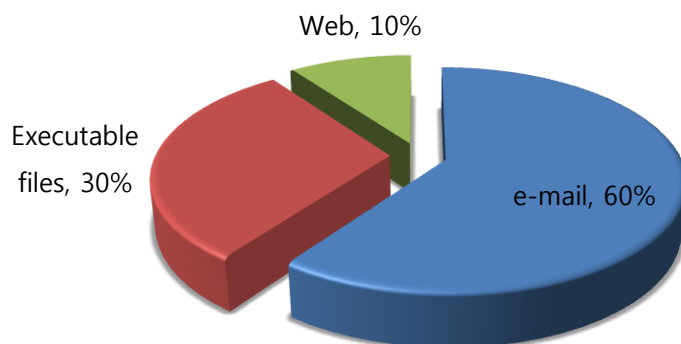
2006

Malware type top 20

2007



Spreading method top 20

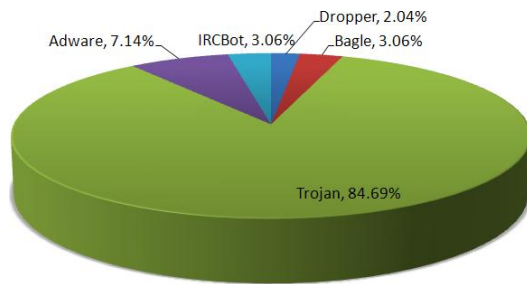


Source: Ahn Lab

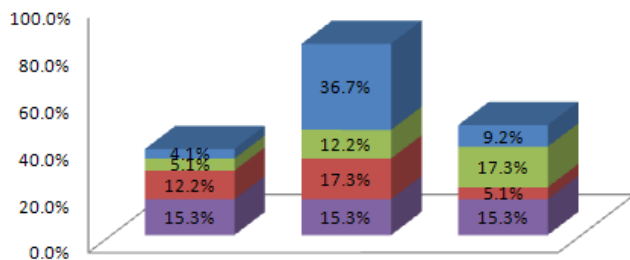
Malwares at Monitoring Point

Enterprise Network

- ZASMIN run during a week (13~20 Aug. 2008)
 - total 34,707 executable files were collected
 - not duplicated 98 malwares were verified by vaccines
 - used port : (80, 8080) 93.88%, (443, 5131, 3364, 19101) 6.12%



Malware Types

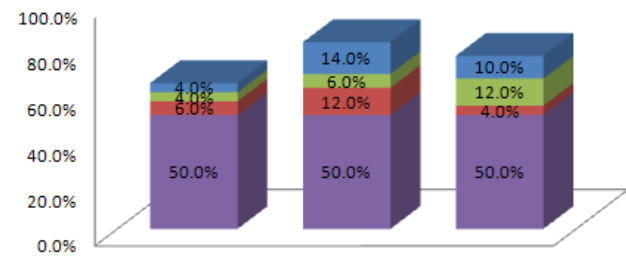
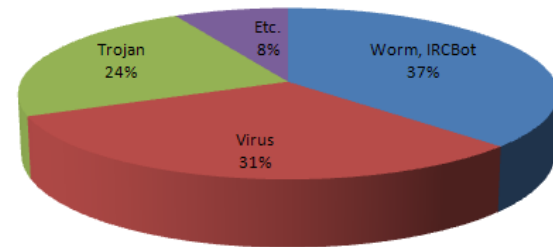


Vaccines detection results

■ (A,B,C) ■ (A,B), (B,C), (C,A) ■ (A,C), (B,A), (C,B) ■ (A),(B),(C)

HoneyNet

- ZASMIN run during a week (12~18 Aug. 2008)
 - total 3,897 executable files were collected
 - not duplicated 50 malwares were verified by vaccines



■ (A,B,C) ■ (A,B), (B,C), (C,A) ■ (A,C), (B,A), (C,B) ■ (A),(B),(C)

- The malware types are different between the locations
- Most of malware come from infected Web site
 - Honey net or IDS couldn't detect the malware
- Vaccines work relatively good for Honey-net
 - 3 commercial vaccines are used to verify malwares

Malware monitoring in Network

Network based executable file reconstruction

Malware spreading IP address

Zombie PC IP Address



ZASMIN
Zero-Day Attack Signature Management Infrastructure

시그니처 환경설정 보고서 보안감사 도구

관리 대상 조합 파일 정보

FileID	SrcIP	SrcPort	DestIP	DestPort	Protocol	AttackType	FileLength	AttackTime
2790620	202.14.70.116	80	129.xxx	2565	TCP	KnownAttack	40960	2009-07-08 20:49:46
2790229	202.14.70.116	80	129.xxx	3458	TCP	KnownAttack	40960	2009-07-08 19:45:01
2790049	75.151.32.182	80	129.xxx	61205	TCP	KnownAttack	40960	2009-07-08 19:14:25
2789949	75.151.32.182	80	129.xxx	61205	TCP	KnownAttack	40960	2009-07-08 18:59:41

Known Attack Detection Information

File ID: 2789949 File Name: i90708/tcp_2789949.exe File Length: 40960
Hash Value: cdf14366b1e11c82eaaa26e3f01ef757 W/B 유형: KNATK(KnownAttack)
Vaccine Name: V3 Malware Name: Win-Trojan/Destroyer.40960
Description:

K/AID	Vaccine Name	Malware Name	Description
4062	V3	Win-Trojan/Destroy...	

검색 조건

시작: 2009-07-08 수 18 Hour 0 Min
종료: 2009-07-08 수 20 Hour 59 Min

SRC IP: DST IP: SRC Port: Result: KnownAttack

검색 통계 정보

종류	KA	KN	UA	UN
총개수	4	4	0	0

조합파일 생성 통계

KA(0.3%) KN(24.7%) UA(1.2%) UN(73.8%)

시스템/네트워크 사용량 추이 그래프

Network Usage(Kbytes) CPU & Memory Usage(%)


시작: 2009-07-11 19:02:53
종료: 2009-07-14 13:21:59

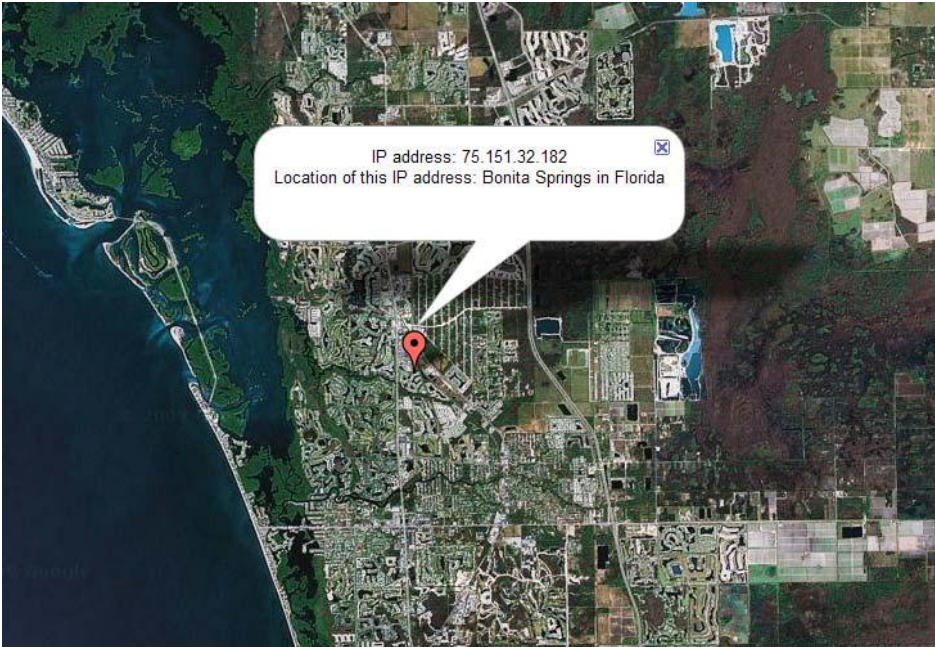
ETRI_ZASMIN4 Ver2.0 20090228p1

Add Modify Delete Close

V3 detects it as a malware

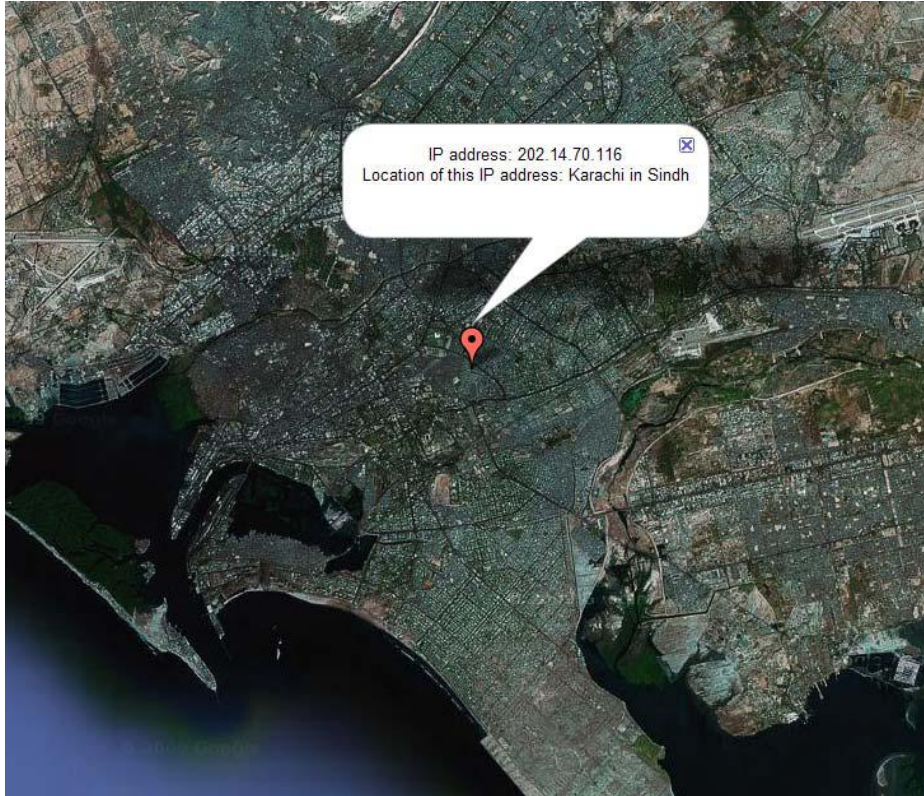
Malware Propagation Sites

IP address: 75.151.32.182
IP country:  United States
IP Address state: Florida
IP Address city: Bonita Springs
IP latitude: 26.3672
IP longitude: -81.8034
ISP: Comcast Business Communications
Organization: Comcast Business Communications
Host: 75-151-32-182-
Naples.hfc.comcastbusiness.net



IP address: 75.151.32.182
Location of this IP address: Bonita Springs in Florida

IP address: 202.14.70.116
IP country:  Pakistan
IP Address state: Sindh
IP Address city: Karachi
IP latitude: 24.8667
IP longitude: 67.0500
ISP: Pakistan International Airlines
Organization: Pakistan International Airlines

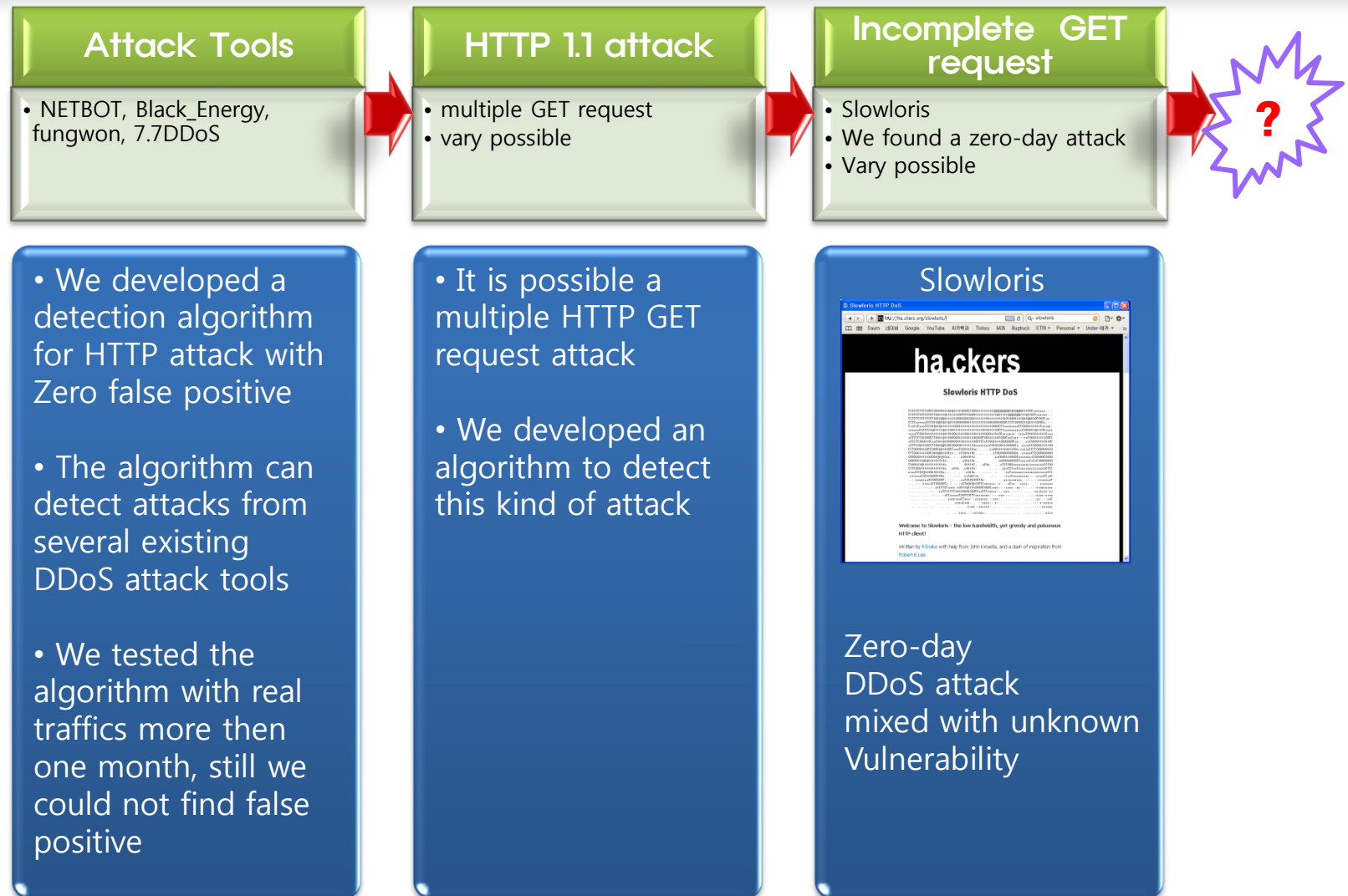


IP address: 202.14.70.116
Location of this IP address: Karachi in Sindh

Detection algorithms

- Can you satisfy with the traffic engineering and mitigation?
 - Traffic engineering result has false alarm
 - Because of the false positive alarm, we can not use ACL
 - Normal user traffics are also hurt by the mitigation
 - Sick and tired of traffic engineering
 - We researched more than several years with traffic engineering
 - It gave results including false alarm
 - We need an algorithm to detect exact IP of attack host
 - Network level attack can spoof IP
 - How about the application attack?
 - But people say the application attacks are very difficult to detect
- A DDoS attack mixed with Zero-day vulnerability is possible
 - We taped a demo of a kind of DDoS attack
 - Victim server system is rebooted or stuck
 - We mailed the attack code to MicroSoft

Application DDoS Attacks



Zero-day DoS attack Demo

- Web Server (windows XP SP3, IIS)
- Windows series are vulnerable
- Attacker (one computer is used to attack)
- It is a kind of HTTP Get flooding
- Web Server is Rebooted or stuck within 1 Minute
- [Demo 1](#)(Windows server reboot)
- [Demo 2](#)(windows server stuck)

- Real time DDoS management system is needed
 - We need a monitoring system that displays DDoS zombie IPs and the corresponding malware information
 - Known malware : we have much space to protect the attack
 - Unknown malware : we get more information from the collaborative analysis
 - We can find potential attackers that download the same malwares in the network
 - We can estimate new zombies from the malware downloading event
 - We need real time visualization system to monitor the attack progress
 - How many Zombies are involved in the attack?
 - What kind of malicious codes cause the attack?
 - Where is the most effective location to protect?
 - What kinds of attack traffics are used (ex. Syn flooding, HTTP Get flooding)
 - We need a national wide control center for DDoS attack

- For accurate and effective DDoS attack detection and prevention
 - Before the attack: To **Monitor, Analyze and Control Malware Propagation**
 - We need a network-based executable file monitoring system
 - The system provides a clue to trace the Zombie PCs and the Master
 - During the attack: Anti-DDoS system with **accurate detection algorithm**
 - We developed application layer DDoS Attack detection algorithms
 - We haven't had false positive yet
 - We prepare papers about the algorithms
 - Traffic volume based rate limit
 - More accurate detection algorithm is needed
 - **Collaborative DDoS management system**
 - A national wide control center is need for Attack Monitoring, Analysis & Management with various networking components and security systems

Thank you!

