



Anti-DDoS Attacks— Are we ready ?

Chinese Taipei

Jia-Chyi Wu

Nov. 18, 2009



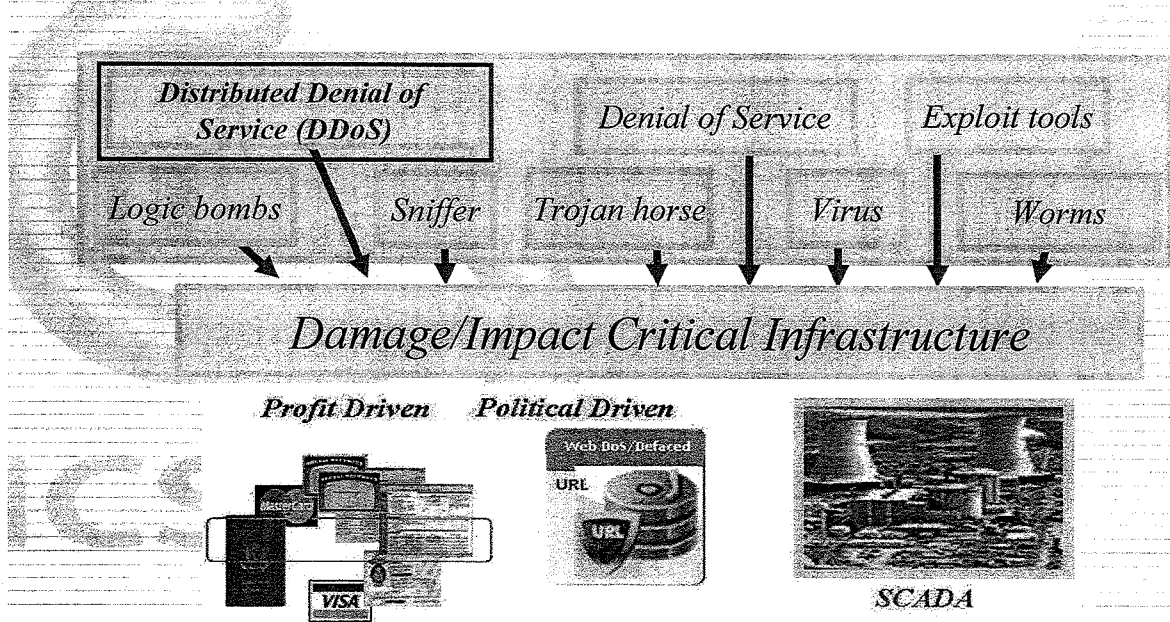
Outline

- *The threat of DDoS Attacks - from recent cases*
- *The 3 “E” s Anti-DDoS Attacks Strategies*
 - *Engineering*
 - *Enforcement*
 - *Education*
- *Conclusion*



Critical Infrastructure Face Various Cyber Threat

- Since the terrorist attacks of September 11, 2001, Warning of terrorist cyber attacks against our critical infrastructure have also increased.



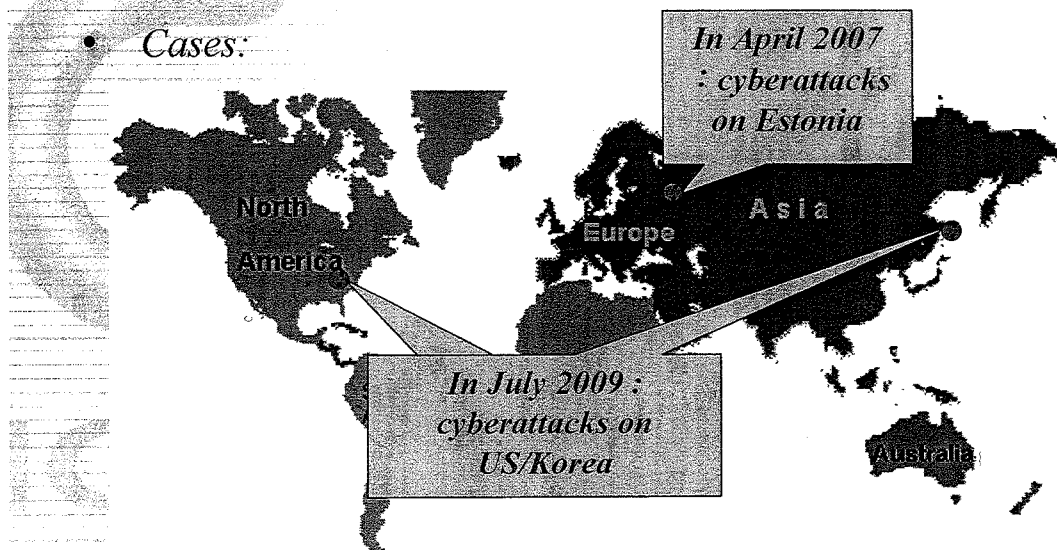
2



The threat of DDoS Attacks – from recent cases

- DDoS attacks have been launched against governments for various purposes including political or ideological ones.

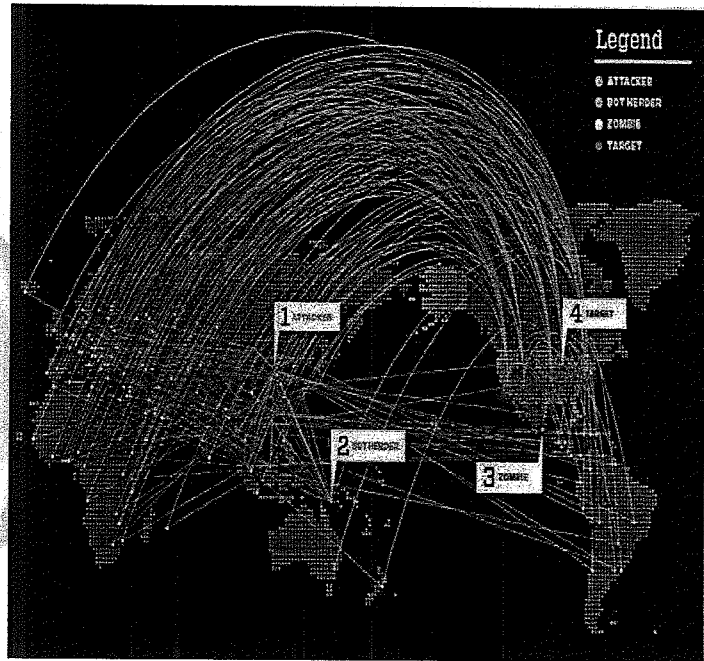
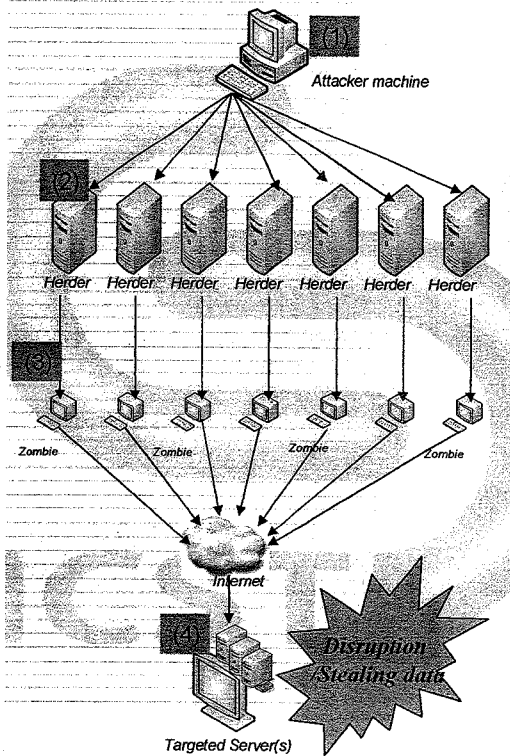
- Cases:



3



What is DDoS Attack



(Source : Wired Magazine)



2007 cyberattacks on Estonia (1/2)

- A series of cyber attacks were launched against Estonian government and commercial websites.
- At least 128 separate attacks on nine different websites in Estonia.
- Some of the attacks lasted more than 10 hours.
- Most of the attacks were launched using botnets comprised of many thousands of ordinary computers.
- Estonia's computer emergency response team (EE-CERT) acted swiftly and, in collaboration with partners from the international community, and was able to weather a very serious attack with little damage.
- The attack was primarily defended through filtering – blocking connections from outside Estonia.

Attack No.	Attack Date
21	2007-05-03
17	2007-05-04
31	2007-05-08
58	2007-05-09
1	2007-05-11



2007 cyberattacks on Estonia (2/2)

Victims May 4, 2007 - 03:48

Enough babble - Podklyuchaysya to act ... Not tired of empty pour into empty?
 "You do not agree with the policy eSStore? ?? You may think that you have no influence on the situation? ??
 You CAN have it on the Internet just never lead to "site": Ee government (rather than any government interest query to search for the Estonian site)
 Choose feel site (not Russian !!!), PRESS (Flight-> vypoint-> cmd), and introduce "ping-nl 5000 10000 estonsky_say-!" OK, ALL!!!
 Example: "ping-nl 5000 1000 www.nik.se-!"
 The three basic steps, followed by Estonian sites simply will not work!!
 Site vooablaesti government
 Revenge for the abuse Estoi
 Razoanik this message across
 eSSStore knows that Russi


Activate 115 typical ICMP-flood attacks

Hacked from RUSSIAN HACKERS (thx to ZyklonTeam, S-Teatr, Web-Hack)

The 9th MAY scheduled r

Our Freedom Our Vic

ESTONIA



6



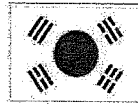
2009 cyberattacks on & (1/2)

- A series of coordinated cyber attacks against major government, news media, and financial websites in South Korea and the United States.
- The attacks involved the activation of a **botnet**—a large number of zombies—that maliciously accessed targeted websites with the intention of causing their servers to overload due to the influx of traffic, known as a **DDoS attack**.
- Most of the zombies were located in South Korea. The estimated number of the zombies around 20,000 according to the South Korean National Intelligence Service.
- The timing and targeting of the attacks have led to suggestions that they may be originating from the North Korea, although these suggestions have not been substantiated.

7



2009 cyberattacks on



&



(2/2)

<i>Timeline</i>	<i>July 4, 2009</i>	<i>July 7, 2009</i>	<i>July 9, 2009</i>
<i>Targets</i>	<i>Both the United States and South Korea : including the White House and The Pentagon.</i>	<i>Affecting South Korea : the presidential Blue House, the Ministry of Defense, the Ministry of Public Administration and Security.</i>	<i>South Korea, including the country's National Intelligence Service as well as one of its largest banks and a major news agency. The U.S. State Department said that its website also came under attack.</i>
<i>Effects</i>	<ul style="list-style-type: none"> <i>• causing disruption, rather than stealing data.</i> <i>• no immediate reports of financial damage</i> 		



Are we ready ?



Q : If we encounter the similar attacks, how to deal with the large scale attacks?
A : No single silver bullet , But..... need Anti-DDoS measures !



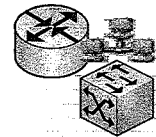
The 3 “E” s Anti-DDoS Attacks Strategies

- The work of Anti-DDoS attacks needs comprehensive and continuous response
- The 3 “E” s Strategies of Anti-DDoS attacks
 - **Engineering** : utilize network devices including firewall, IDS and Application Delivery Controller(ADC) etc. to establish front-line of defense
 - **Enforcement** : implement Anti-DDoS attacks incident response mechanism, local and international cooperation to make quick response
 - **Education** : enhance Anti-DDoS attacks awareness, response drill and lesson learn

10



Strategy 1 – Engineering



- **Product** : need automatic systems/tools

Attacks Method	Probability	Firewall	IPS	ADC
ICMP Flood	High	○	◎	○
UDP Flood	High	○	◎	○
SYM Flood	High	△—○	○	□—◎
ACK/RST Flood	Medium	◎	◎	◎
Connection Flood	Low	□	○—◎	□—◎
Zombie Flood	Medium	□	○—◎	□—◎
SSL Flood	Low	△	□	△—◎
Http Flood	High	△	△—○	△—◎
Application Flood	Low	△	△—○	□

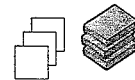
◎Very Good, ○ Good, □ Even, △Poor, × Invalid

From : Info Security No.65

11



Strategy 1 – Engineering



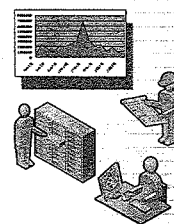
- *Procedure : need well defined Incident Handling SOP*
- *Recommended DDoS Handle procedures (for Web administrator)*
 1. *Register backup IP address, during under attacks, through DNS swap to the backup IP address*
 2. *Be familiar with ISP capability via monitor system provide the prompt alert information*
 3. *As per DDoS attacks, use firewall or router or other methods to block/redirect IP address and web flow*
 4. *Cooperate with 3rd parties including ISP and ISP of attack resource*
 5. *Web administrator can add extra reserve IP address and remove the services from the victim server*

12



Strategy 1 – Engineering

- *People : need the following response skill*
 - *Pre-process*
 - *Collect information*
 - *Sniff packets*
 - *Request ISP or IDC assistance*
 - *Request cross-border entity assistance*
 - *Take blocking*
 - *Report to LE*
 - *Lesson learn*

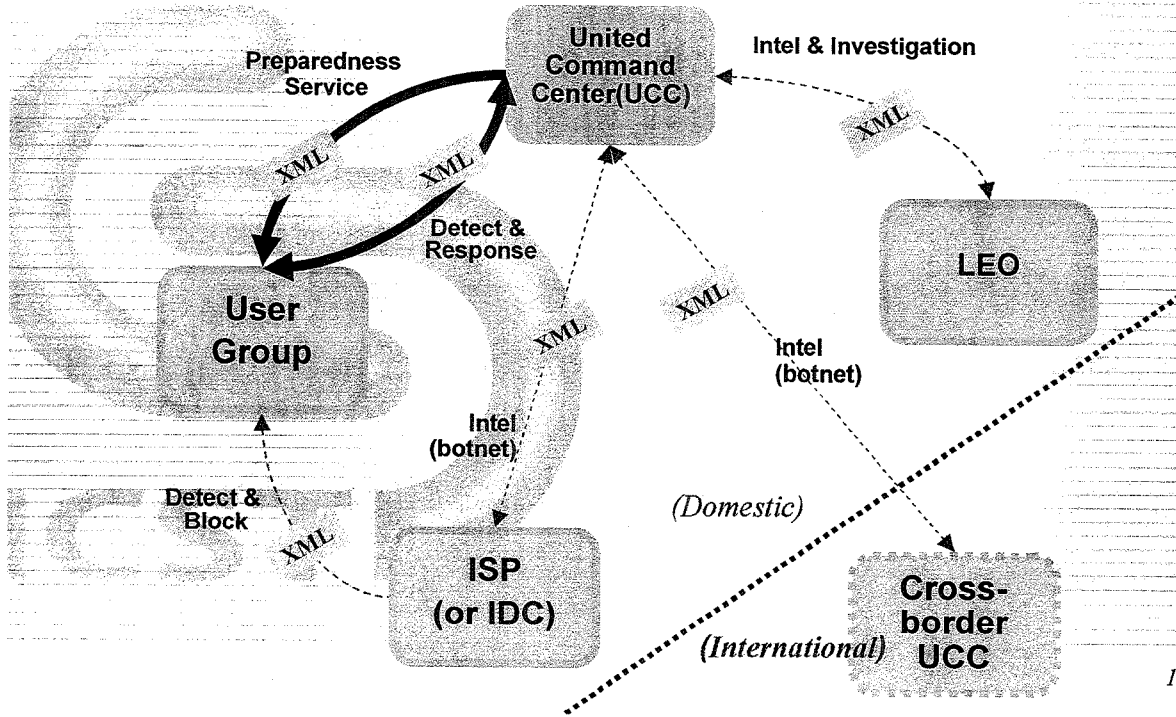


13



Strategy 2 – Enforcement

• Response entities

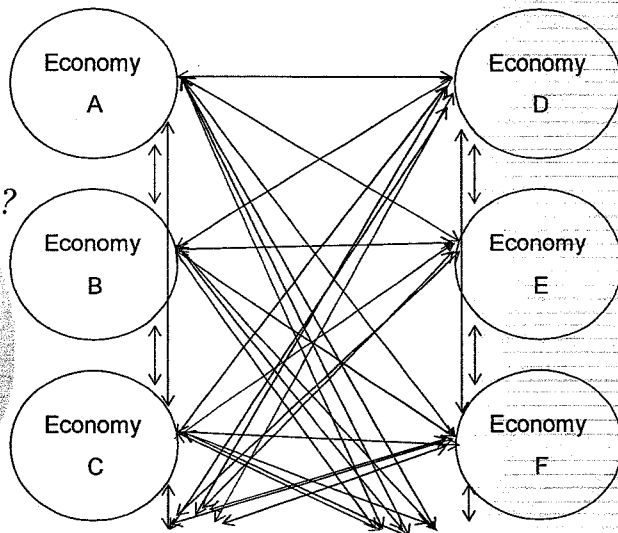


Strategy 2 – Enforcement



• International cooperation is crucial

- *Anti-DDoS Alliance ?*
- *point of contact ?*
- *cooperation protocol ?*
- *Role and responsibility ?*
- *Report system ?*
- *Legal support ?*





Strategy 3 – Education

APCERT DRILL 2007

Beijing 2008



Date: 22nd December 2007

Participation teams:

- Malaysia - MyCERT
- Australia - AusCERT
- Brunei - BroCERT
- China - CnCERT
- Singapore - SingCERT
- Thailand - ThaiCERT
- Hong Kong - HKCERT
- India - CERT-IN
- Japan - JPCERT
- Korea - KR-CERT
- Chinese Taipei - TWNCERT
- Vietnam - BKIS



CN CERT/CC KJ CERT/CC JPCERT/CC

THAI CERT



AUS CERT

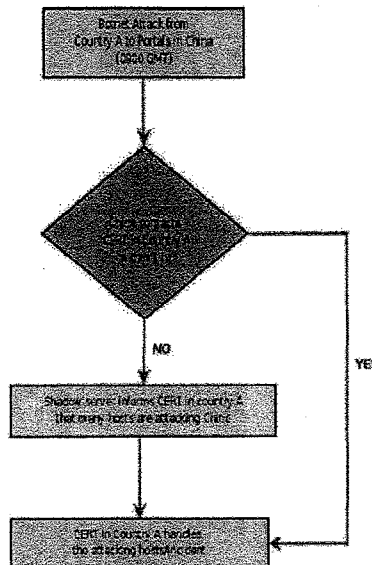
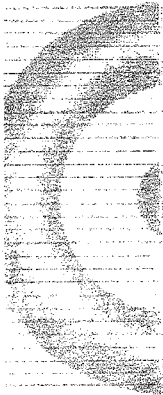
Timeline

- 0700 Lord of Armageddon (LoA) declare cyber war on Beijing Olympics
- 0900 Co-ordinated botnet attacks from AP region causing media sites and government portals inaccessible
- 1100 Spam containing malware that turns PC into zombies were filling up mailboxes in AP economies
- 1300 Border and Core routers crashing and rebooting frequently. 0-day exploit for Cisco IOS rumoured to be available. Cisco promise to release fix in a few hours
- 1430 - Cisco released patch and advisory on critical IOS vulnerability
- 1600 - Security analysts announced that bots automatically removed themselves, no more attacks



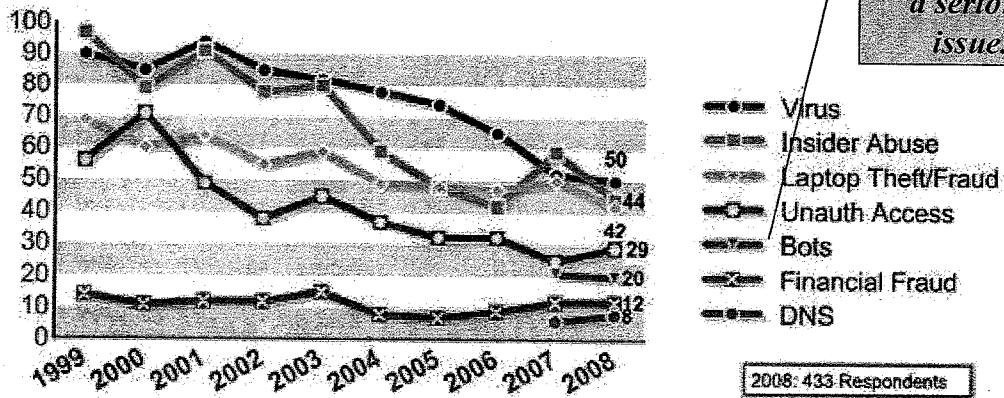
Strategy 3 – Education

Scenario Handling



➤ Percentages of key types of incident between 1999~2008

Figure 13: Percentages of Key Types of Incident



CSI/FBI 2008 The 13th Computer Crime and Security Survey
Info source : Computer Security Institute

Conclusion

- *My security relies on your security. Every economies can not avoid the cross-border DDoS attacks.*
- *Asia-Pacific economics may refer to 3 “E” s strategies to improve anti-DDoS capability.*
- *The anti-DDoS attacks of APEC based on international cooperation should be a best practice for future opportunity.*