Mid-Term Presentation

Group 6

Q1

Survey the various characteristics of cyber attacks to the London Olympics.
Choose the one you believe is the most important and explain your reasoning.

Q2

What is the impact of the attack you chose in Q1 to the Tokyo Olympics,
how can we achieve resiliency against that?

Q3

What problems or issues may occur at the Tokyo Olympics
which do not occur at the London Olympics

Q1

Survey the various characteristics of cyber attacks to the London Olympics.
Choose the one you believe is the most important and explain your reasoning.

Q2

What is the impact of the attack you chose in Q1 to the Tokyo Olympics,
how can we achieve resiliency against that?

Q3

What problems or issues may occur at the Tokyo Olympics
which do not occur at the London Olympics

Attack on power infrastructure / opening ceremony

At opening ceremony in London Olympics, power infrastructure was attacked many times. (DoS attack)

"The visual cyber attack"

Because the opening ceremony is a one-time event, people all over the world will be watching and will be looking forward to the Games, leaving the ceremony extremely vulnerable to attack.
The opening ceremony is largely symbolic, representing countries from around the world coming together to compete.
A large-scale cyber attack would hurt the principles of what the Olympic Games represent, the very idea of peaceful international cooperation and competition.

Attack on critical infrastructure

Hacktivists, political or social activists who commit cyber attacks, are regarded as a group of people who strive to send a social or political message through cyber attacks. Because hacktivists often form organized groups via social media (either Twitter, Facebook, or the deep web), the Olympic committee responds by looking over SNS trigger words or hashtags before the Olympics to be able to take action before hacktivist groups can mobilize and coordinate any attacks. OCCT (Olympic Cyber Co-operation Team), the special team established in MI5 (Military Intelligence Section 5), prepares multiple scenarios of mock cyber attacks to test the strength of the systems powering the Olympics in several different ways to identify and fix security flaws before they can be exploited by malicious hackers.

Q1

Survey the various characteristics of cyber attacks to the London Olympics.
Choose the one you believe is the most important and explain your reasoning.

Q2

What is the impact of the attack you chose in Q1 to the Tokyo Olympics,
how can we achieve resiliency against that?

Q3

What problems or issues may occur at the Tokyo Olympics
which do not occur at the London Olympics

1. Political Affiliation / Company Affiliation

2. Technical Aspect

1. Political Affiliation / Company Affiliation

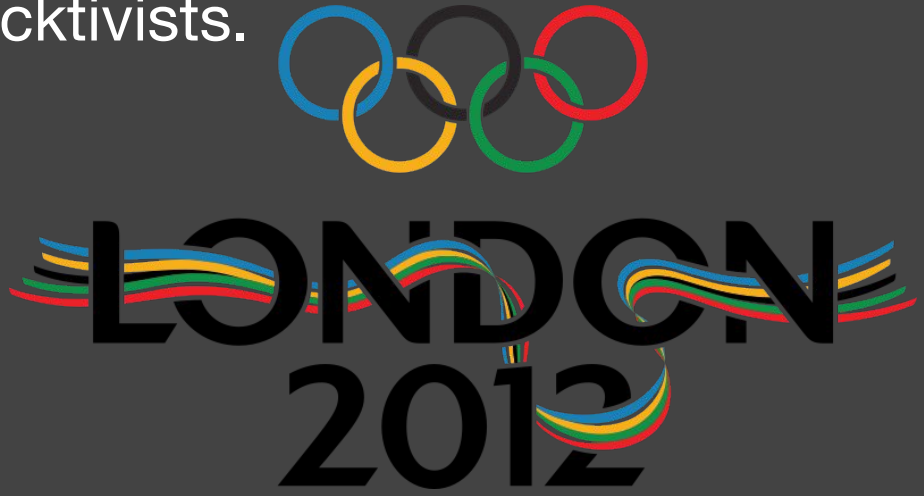
2. Technical Aspect

Analysis of Possible Threats to Olympic Games

Type of Cyber Attack	Content of Cyber Attack
DDoS Attack	11,000 DDoS attacks through to focused HTTP application floods using simultaneous vector attacks. Usage of overflooding servers with packets of information (ping flooding).
Phishing scams	Set up fake copies of official Olympic sites to be used for scamming/illegitimate purposes
Virus and worm programs	Virus and worm programs to release “low orbit ion cannon”-style DDoS attacks or phish for information. Also to create botnet network for other types of cyber attacks.
Attacks on Olympic lighting system	Manually override system to be able to switch off or disable the electrical power grid during the Olympics, causing mass panic and chaos


acer
Coca-Cola
Atos
DOW
OMEGA
Panasonic
P&G
General Electric
McDonald's
VISA
SAMSUNG

Sponsors include Critical Infrastructure Key Resources (CIKR) or Information Sharing Analysis Center (ISAC) members. The actions or credibility of the sponsors may become targets for cyber criminals or hacktivists.



The purpose of this bulletin is to provide a strategic outlook for the 2012 Summer Olympic Games and similar events to assist partners in detecting and mitigating related attacks.

EXAMPLE

FIFA Corruption Scandal

Coca-Cola

McDonald's

VISA

Same sponsors in Olympics

Incentive for Cyber Attacks

1. Political Affiliation / Company Affiliation

2. Technical Aspect

Important considerations regarding DDoS attacks

- Multiple groups could be responsible
  - Nation-states / state-sponsored organizations
  - Private groups (hacker collectives e.g. Anonymous)
  - Individual hackers
  - Different groups have different motivations, but most are trying to bring down a network/service
- Attack could come at different network layers or attack different targets
  - Layer 3 or layer 7 network attack
  - Could target network infrastructure (routers, DNS servers, web servers, database resources)
  - Could target non-Internet infrastructure (power grid, security systems,
- Uptime/availability is priority
  - During Olympics, any service unavailability would be disastrous
  - Can’t block legitimate users
  - Security mechanisms cannot excessively interfere with normal network operation

DDoS Mitigation

Easiest solution: simple firewall/hardware appliance, not extremely effective

most effective solution: traffic filtering/analysis, able to stop sophisticated attacks

Most DDoS-attack prevention companies work by scrubbing and sanitizing data as it passes from the public internet through their network to the designated recipient. By analyzing traffic and looking for patterns in network activity, it is possible to establish a baseline of what “normal” activity is. The most effective solutions involve behavior analysis that “teaches” the system after each attack, not a simple pattern-matching rule set. These “next-gen” systems are generally more effective because they continuously evolve and learn from attacks, and they are capable of detecting attacks that look like legitimate user traffic. An added benefit of adding DDoS-protection equipment is that the site will be more reliable and able to handle more users because fewer malicious requests will reach the target web server.

Past Large-scale DDoS attacks and styles

- 2014 GitHub attack (believed to be sponsored by Chinese government)
- 2012 London Olympic power grid attack
- 2013 attack on Spamhaus
- 2012 attack on WikiLeaks

- Attack styles and vectors
  - DNS amplification, NTP amplification, mobile ad networks, traffic redirection, botnet using infected computers

Q1

Survey the various characteristics of cyber attacks to the London Olympics.
Choose the one you believe is the most important and explain your reasoning.

Q2

What is the impact of the attack you chose in Q1 to the Tokyo Olympics,
how can we achieve resiliency against that?

Q3

What problems or issues may occur at the Tokyo Olympics
which do not occur at the London Olympics

This, we leave blank for NAIST, if your wondering

Citation & Sources

http://www.bbc.com/news/uk-23195283