Battling the Threat of the Internet

Dr. Ahmed M. Manasrah
National Advanced IPv6 Centre, Universiti Sains Malaysia, 11800 USM, Penang, Malaysia.
Introduction

Is the emerging security threats tends to be a science fiction?

Starting to sound like a science fiction movie. Unfortunately, it's real.
1982: Start with Viruses
- User Intervention

1988: Other forms of Malwares
- Self-replication, self-preservation

2007: What is next?
- Self-replication
- self-preservation
- Distributed
- Coordinated
- Remote controlled

**Action:**
- Erase hard drive
- Delete Files

**Action:**
- DDoS
- SPAMM
- SCANNING
- Phishing

**Action:**
- Leave a backdoor
- Steal Info
Botnet: refer to a collection of compromised computers (zombies) under a common command-and-control infrastructure.
1. BotMaster send commands to his bots through the CnC server
2. Bots Pull the commands from the CnC server
3. Bots are Patched
4. Bots Ready to attack
5. Bots will start the attack

In General the amount of traffic is equal to:
Traffic per second x number of Pcs involved x time in seconds

(one second attack, the amount of traffic is equal to 1KB/s x 5machines=5KB/s)

* Assume each machine can send out Max. of 1KB/s (which is not the case)
Use of Botnets

- Attacks usually target servers belonging to government organizations.
- The attacks can be used as provocation, with a cyber attack on one country being conducted from servers in another country and controlled from a third country. (USA attack)
- Revenge (estonia Attack)

- Theft of application serial numbers, login IDs, and financial information (credit card numbers).
- Creation or misuse of SMTP mail relays for spam (Spambot).
- Click fraud.

Botnet Purposes

- Fun
- Challenge
- Exploring, Trying
What do we need?

A Platform that brings together the social, law, cultural and communities together.

To evaluate and study the various cultural factors that contributes towards the continuous infection series worldwide despite that fact that various security vendors and products are in use by different users.
Cyber-Security Platforms

Policy  Strategy  Technical
Policy Platform

Cyber Security Policies

- The purpose of a Security Policy is to decide how an organization is going to protect itself.
- The policy will require two parts: a general policy & specific rules.
- The general policy sets the overall approach to Internet Security.
- The rules define what is and what is not allowed. The rules may be supplemented with procedures and other guidance.

Cyber Law

- Summarizes the legal issues related to the use of communicative, transactional, and distributive aspects of networked information devices and technology.
- It is less a distinct field of law in the way that property or contract is, as it is a domain covering many areas of law and regulation.
- Some leading topics include intellectual property, privacy, freedom of expression, and jurisdiction.
Strategy Platform

**Awareness**
- To build a strong foundation of cyber aware public

**Human Resource Capacity Building**
- To create a pool of skilled personnel in the cyber security area

**Roadmap**
- Creation of a national guideline which identifies the areas to work on as well as the stakeholders roles and responsibilities

**Pilot Project**
- Pilot implementation of the Botnet Mitigation Toolkit
Technical Platform

- Innovate & produce detection, monitoring & traceback mechanism
- Better dynamic protection
- Framework - provide various cybersecurity requirement controls & baselines
- Facilitate the development of various tools