Current and Future R&D Activities on Cybersecurity:

Fight against Emerging Security Threats with Transnational Collaboration

Daisuke INOUE

Director, Cybersecurity Laboratory
Network Security Research Institute (NSRI)
National Institute of Information and Communications Technology (NICT)
What we are fighting against?

Malware

short for **malicious software** designed to **disrupt or deny operation**, **gather information** that leads to loss of privacy or exploitation, **gain unauthorized access** to system resources, and other abusive behavior.

(from Wikipedia)
Overview of the project **nicter**

**nicter** = Network Incident analysis Center for Tactical Emergency Response

**Target:**
Integrated analysis of security threats in large scale networks
- What happens on the Internet?
- What is the root cause?

**Strategy:**
Network monitoring + Malware analysis

**nicter Operation Room**
nicter

Overview

MacS: Macro analysis System
- Visualization
  - Tiles
  - Atlas
  - Cube
- Analysis Engine

NemeSys: Network and malware enchaining System
- Correlation Engine

IHS: Incident Handling System
- Analysis Work Bench

MicS: Micro analysis System
- Code Analyzer
- Behavior Analyzer

Phenomena
- Root Cause

Darknet Traffic
- Virus
- Bot
- Worm

Government

Internet Service Providers (ISPs)

End Users

Honeypot

Malware Samples

Network Incident Analysis Center for Tactical Emergency Response
Overview

**MacS: Macro analysis System**
- Visualization
  - Tiles
  - Atlas
  - Cube
- Analysis Engine

**NemeSys: Network and malware enchaining System**
- Phenomena
- Root Cause

**IHS: Incident Handling System**
- Analysis Work Bench

**MicS: Micro analysis System**
- Code Analyzer
- Behavior Analyzer

**Darknet Traffic for 6 Years**
- 140,000 darknet (dark IP addresses)
- 2,000 samples can be analyzed per day
- 30 seconds for a correlation analysis
- 2 Million Malware Samples

**End Users**
- Government
- Internet Service Providers (ISPs)

**NICT**
- National Institute of Information and Communications Technology

**Report**
- nicter

**Analysis**
- Work Bench

**Incident Report**
What can we see with current nicter?

• **Widespread Malwares**
  - attacking next targets *actively*
  - passive darknet monitoring works well

• **Emerging Security Threats**
  - **Drive-by Download** (web-based attack)
  - **SNS Malware** (spread along social connections)
  - **Advanced Persistent Threat** (targeted attack)
  - **Threats on IPv6 Network** (no scan any more?) etc…
NICT’s R&D Activities on Cybersecurity

Practical Cybersecurity Technology

1. Cutting-edge Cyber attack monitoring/analysis environment (wider, deeper and more active)
2. Cyber attack prevention technology for tracking and anticipating emerging security threats
3. Novel security technologies for emerging networks such as IPv6
4. Secure research framework to promote external use of collected security data

Outcomes

Analysis and Prevention Plane

- SNS analysis
- Livenet analysis
- SPAM analysis
- Web analysis
- Darknet analysis (current nicter)

Monitoring Plane

- SNS monitor
- Livenet monitor
- SPAM monitor
- Web monitor
- Darknet monitor (current nicter)

Infra Plane (IPv4, IPv6, Cloud, NWGN etc.)

- IPv6 threats and countermeasures
- Secure Research Framework

= NEW
Toward Transnational Collaboration
- Security Big Data Exchanging -

- Cyber-attacks are highly organized and have no border.
- World wide collaboration is crucial for world wide attack attribution.
- Both EU and Japan have “Security Big Data”.

Challenges
- Scalability
- Interoperability
- Real-timeness
- Disclosure control
- Collaborative analysis
- Legal issue etc. etc...