Macro-Micro Correlation Analysis for Detecting Network Security Incidents in the Large Network

Koji Nakao

Group Leader
Network Security Incident Response Group, Information Security Research Center, National Institute of Information and Communications Technology (NICT), Japan

Director
Information Security Department, KDDI Corporation, Japan
Network dependency and Security Incidents are now co-relatively and heavily increased

**Increasing Security Threads**

Security Incidents are getting serious by Slammer, Blaster, Sasser worms
Malignant worms are getting skillful and integrated.

![Diagram showing the increase in the number of Internet users and penetration rate from 2000 to 2004, with a peak of 80 million users by the end of 2004.](image)

**Figure 1:** Number of Internet users and penetration rate

![Diagram showing the transition in the number of broadband subscribers from 2000 to Dec. 2004, with a peak of 20 million subscribers by the end of 2004.](image)

**Figure 2:** Transition in the number of broadband subscribers
A short history of computing & insecurity

### Standalone Systems – Disk/Diskette Sharing
- Apple II Computer
- Commodore
- Atari
- TI-99
- TrS-80
- First Worm developed in Xerox Palo Alto
- First Self-destruct program (Richard Skrenta)
- First Self-replicate program (Skrenta's Elk Cloner)
- Ken Thompson demo first Trojan Horse
- Fred Cohen’s Morris’ Worm
- FBI arrest “414s” Hacker Group

### Client-server/PC-LAN Networks
- Stealth virus (Whale)
- Variable Encryption (1260)
- ©Brain Virus developed by two Pakistanis’
- Lehigh, etcMorris’ Worm
- Robert T Morris fined $10K, 3 years probation

### Internet Collaboration (Email, Web, IRC, IM, P2P, File Sharing)
- First “Concept” Macro
- First Self-destruct (Richard Skrenta)
- First Self-replicate (Skrenta’s Elk Cloner)
- First Worm (Morris’)
- First Self-destruct (Richard Skrenta)
- First Self-replicate (Skrenta’s Elk Cloner)

### Criminal Exploitation
- Code Red
- Nimda
- Slammer
- Blaster
- MyDoom
- Sasser
- DDoS on 13 “root” servers
- Phishing attacks proliferated
- SPAM Mails
- Spyware
- Bots
- Pharming attacks (DNS poisoning)

### Experimentation
- Kevin Mitnick arrested, five years imprisonment
- “Solar Sunrise” – Two California Teens attack on 500 Military, Govt, & Private Computer Systems
- “Cukoo’s Egg” in LBL

### Protocol Weaknesses/Buffer overflow
- FBI arrest “414s” Hacker Group
- First Worm (Morris’)
- First Self-destruct (Richard Skrenta)
- First Self-replicate (Skrenta’s Elk Cloner)

### Discovery
- MDGC
- First Worm (Morris’)
- First Self-destruct (Richard Skrenta)
- First Self-replicate (Skrenta’s Elk Cloner)

### Insecure Default/Weak Security Techniques/Feature Misuse/Social Engineering
- First Worm (Morris’)
- First Self-destruct (Richard Skrenta)
- First Self-replicate (Skrenta’s Elk Cloner)

### Trusted Operating Systems (Orange Book)
- Trusted Network (Red Book) – ITSEC

### Trusted Network (Red Book) – ITSEC

### UK Green Book to BS 7799 to ISO 17799
- Common Criteria (ISO 15408)

### Information Warfare
- Kevin Mitnick arrested, five years imprisonment
- “Cukoo’s Egg” in LBL
- First Worm (Morris’)
- First Self-destruct (Richard Skrenta)
- First Self-replicate (Skrenta’s Elk Cloner)

### Computer Crimes
- National Institute of Information and Communications Technology

### Cyber Crimes
- Phishing attacks (DNS poisoning)
- Pharming attacks (DNS poisoning)
Threats: Internet Attacks

- Online Business Botnet Controller (IRC Servers)
- DNS Servers (Pharming Attacks)
- Virus/Worms
- Authors
- Social Engineering (IM/Emails/P2P/In-person)
- Web Defacements
- Denial of Services
- Open Proxies/Open Mail Relays
- Phishers
- Phishing Web Sites
- Phishers’ “Safe House”
- Botnet
- Botnet Controller (IRC Servers)
- Organized Crimes Syndicates
- Hot Herders
- Spammers
- Open Mail Relays
- DNS Servers (Pharming Attacks)
- Spammers
- Sympware/Trojans/Rootkits
- Sypware/Trojans/Rootkits

Produced by Meng Chow Kan
Overview of the project

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

**Objectives:**
- Integrated analysis of network security incidents in large networks
  - Monitoring nation-wide large networks with various sources
  - Real-time and automated analysis for detecting precursors before outbreaks
  - **Macro-micro correlation analysis** to identify the latest incidents detected
  - Providing prompt and detailed incident reports to ISPs and others

**Activities:**
- Research and development of individual technologies
  - Event visualization, virus analysis, change point detection, etc
- Building beta operation center (photo in right)
- Operational practices (in progress)
  - Telecom ISAC Japan
  - National Information Security Center, Cabinet Secretariat of Japan
System functional overview

Global
- Live traffic from ISPs
- Monitored traffic from darknets
- IDS logs from university NW
- Malware samples from honeypots/dummy email accounts

Local
- Information sources

Real-time data distributor
- Log database

Data regulation
- Change point detection
- Change point prediction
- Traffic analysis profiling
- Bot detection

Real-time analysis

World map
- 3D display
- Host-based behavior

Visualization
- World map
- 3D display
- Host-based behavior

Visualization
- Incidents analysis experts
- Incident analysis

In-depth analysis
- Long-term TAP
- Self organizing map
- Malware code analysis
- Malware behavior analysis
- Bot detection
- Shellcode detection

Integrated database

Analysis work bench
- Incident handling system

Integrated database

Incident handling

NiCT
National Institute of Information and Communications Technology

NICT
Network Incident Analysis Center for Tactical Emergency Response
Information sources

Various information sources from local to global networks

- **Live traffic from ISPs**
  - Privacy-related data (e.g., payloads) are sanitized
- **Monitored traffic from darknets (100-150MB/day)**
  - Responding only to ICMP echo requests / TCP syn
  - No actual hosts – only attack packets coming
- **IDS logs from university NWs (100MB/day)**
  - Collecting alerts by multiple IDSes located at university networks
- **Malware samples from honeypots and dummy email accounts**
  - Imitating vulnerable hosts/server to attract and capture viruses
  - Setting up mail servers with dummy accounts to collect emails including viruses.
Macro-micro correlation analysis

Flow of macro analysis
- Traffic visualization
- Real-time analysis
- In-depth analysis

Flow of micro analysis
- Malware code analysis
- Malware behavior analysis

Recognitions of NW Behavior
- Detailed Incident report
- Virus code & behavior Analysis

Captured traffic
IDS logs

Malware behavior database
Network event database

NiCT
National Institute of Information and Communications Technology

nicter
network incident analysis center for tactical Emergency Response
Macro analysis
Visualization of monitored traffic

Visualization for operators to intuitively understand the monitored traffic status

Flow of macro analysis
- Traffic visualization
- Real-time analysis
- In-depth analysis

Network event database

Macro-micro correlation

Flow of micro analysis
- Malware code analysis
- Malware behavior analysis

Malware behavior database

Recognition of NW Behavior

Detailed Incident report

NiCT National Institute of Information and Communications Technology

nicter Network incident analysis center for tactical Emergency Response
Real-time packet source visualization

Visualizing source of incoming packets at our darknet
3-D display of real-time incoming packet flow

Showing arrivals of scanning packets:
- TCP SYN
- TCP SYN/ACK
- UDP
- ICMP
- TCP of non-SYN or non-SYN/ACK

Source IP Address
Source Port Number
Destination IP Address
Destination Port Number

port scanning
address scanning
Scan activities detected in Interop 2006 in Tokyo
Real-time analysis

Flow of macro analysis:
- Traffic visualization
- Real-time analysis
- In-depth analysis

Flow of micro analysis:
- Malware code analysis
- Malware behavior analysis

Macro-micro correlation

Network event database

Recognition of NW Behavior

Detailed Incident report

Real-time analysis for prompt and automated detection of incidents

NiCT
National Institute of Information and Communications Technology

nicter
Network incident analysis center for Tactical Emergency Response
Real-time analysis

• TAP (Traffic Analysis & Profiling)
  – Short-term Behavioral analysis of individual hosts (approx. 30 seconds)
  – Analyzing and categorizing scanning behavior for each host by
    • Scanned source/destination port/address
    • Sequential/random
    • Define behavior by (scan type : port set)
      – e.g., network scan 2 : UDP/1434, port scan 1 : TCP/445, etc.
    – Detecting new attack patterns

• CPD (Change Point Detection)
  – Detecting rapid changes of monitored traffic
Overview of real-time analysis

- **Continuous CPD monitoring on known-vulnerability**
  - Ex. scan frequencies on ports with well-known vulnerability

- **Dynamic CPD monitoring on newly detected attacks**
  - New CPD process dispatched by TAP upon detection of new attack patterns

---

Monitored Traffic → TAP

CPD processes

Over 10,000 parallel CPD processes

Alert
Graphical representation of TAP behavioral analysis

<table>
<thead>
<tr>
<th>Source Port No.</th>
<th>Destination Port No.</th>
<th>Time</th>
<th>Destination IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1 (a specific host)</td>
<td>(type of scanning shown here)</td>
<td>old</td>
<td>new</td>
</tr>
</tbody>
</table>

**Legend:**
- TCP SYN
- UDP
- ICMP
- TCP SYN+ACK
- TCP (Other than & )
- smaller
- larger

NiICT
National Institute of Information and Communications Technology

nicter
Network incident analysis center for tactical emergency response
Examples of TAP analysis results

- UDP scanning for many IP addresses
- Network scanning to many IP addresses
- Two types of simultaneous scannings (network scanning (up) + port scanning (down))
- Multiple port scan for a single IP address
A Dasher worm’s TAP behavior

Change-Point Detection (CPD)

- Detecting rapid change of time-variant data
  - calculating scores of change
  - generating alerts when score exceeds threshold value

Fast real-time learning
Adaptive to long-term change
Low false-alarm rate
Faster than repetitive statistical testings
Detected change point of scan frequency on tcp/1025
detected on 09:05 JST Dec. 9, 2005
(later found as an activity of Dasher. A worm)
In-depth analysis

Flow of macro analysis
- Traffic visualization
- Real-time analysis
- In-depth analysis

Flow of micro analysis
- Malware behavior analysis
- Code analysis

Macro-micro correlation

Detailed Incident report

In-depth analysis for investigating the detected incidents in details

NiCT
National Institute of Information and Communications Technology
In-depth analysis methods

• Long-term TAP analysis
  – TAP analysis for several hours to several days
  – Analyzing and categorizing behaviors of individual malicious hosts

• SOMs (Self-Organizing Maps)
  – Detecting similarities between different datasets
  – Computationally complex

• Shellcode detection
  – Detection of buffer-overflow shellcodes
  – Applicable for both real-time and in-depth detection

• IRC bot analysis (experimental phase)
  – Distinguishing bots from human users
Long-term TAP graph analysis

Performing long-range TAP analysis contributes to find out long-term history and trends of activities of specific hosts.

Long-term analysis emphasizes the host characteristics.

Showing long-term change of per-host trends.
Self-Organizing Maps (SOMs)

• Clustering hosts with similar behaviors
  – The radius indicates the number of hosts
  – The color shows the intensity of the specified parameter

Cluster of hosts intensively accessing tcp/1025
Example: Finding worm variants by SOMs

- **Dec 15th**
  - Type I (Dasher.A-C): tcp/1025
  - Type II (a Dasher variant): tcp/1025, 1433, 42
  - Type III (Dasher.D): tcp 1025, 1433, 42, 445

- **Dec 16th**
  - Type I
  - Type II
  - Type III

- **Dec 17th**
  - Type I
  - Type II tcp/1433
  - Type III tcp/42
  - tcp/445
Shellcode detection
(Security Program based on structural analysis)

**Key technology**

- Detect attacks against buffer overflows
- Decode binary streams into Intel x86 machinery, and analyze it
- Detect critical and specific structure of attack codes when it is going to get control of process
- It detects how system call is called, not where
- It is independent of applications
- It can be applicable to Network-based AND host-based IDS
Micro analysis
Malware code and behavior analysis for investigating behaviors and characteristics of captured malwares

Flow of **macro** analysis
- Traffic visualization
- Real-time analysis
- In-depth analysis

Macro-micro correlation

Flow of **micro** analysis
- Malware code analysis
- Malware behavior analysis

Network event database

Detailed Incident report
Micro Analysis of Malware by means of two methods

Behavior Analysis (Dynamic Analysis)
- Virus Executes
- Collect Logs
- Behavior Analysis
  - Report Dynamic
    - R-D

Code Analysis (Static Analysis)
- VM Host
- Virus Executes
- Code Analysis
  - Producing Reports
  - Report Static
    - R-S

Virus Information

(VM Host: Virtual Machine Host)
Example of description by XML in the case of Happy99.Worm

```xml
<?xml version="1.0" encoding="Shift-JIS"?>
<MaliciousCodeXML>
  <MaliciousCode>
    <Name>Happy99.Worm</name>
    <Attribute><worm/></Attribute>
    <Trigger>Online</trigger>
    <Action>
      <openWindow>
        <windowtitle>Happy NewYear 1999!!</windowtitle>
      </openWindow>
      <createFile>
        <directory>WINDOWS\SYSTEM</directory>
        <file>SKA.DLL</file>
      </createFile>
      <if>......</if>
    </Action>
  </MaliciousCode>
</MaliciousCodeXML>
```
More specifically

<Action>
  <openWindow>  ① Open the Window
    <windowtitle>Happy New Year 1999!!</windowtitle>
  </openWindow>
  <createFile>  ② Create a file
    <directory>WINDOWS\SYSTEM</directory>
    <file>SKA.DLL</file>
  </createFile>
  <if>  ③ If Condition
    <condition>  ④ If the file is activated, then continue
      <execute><file>WSOCK32.DLL</file></execute> == true
    </condition>
  </if>
  <block>  ⑤ Add Registry
    <addReg>
      <registrykey>HKEY_LOCAL_MACHINE\</registrykey>
      <registryvalue>SKA.EXE</registryvalue>
    </addReg>
  </block>
</Action>
W32.Sobig.B@mm

種別: ワイルド
影響を受け可能性のあるシステム:
- Windows 95
- Windows 98
- Windows NT
- Windows 2000
- Windows Me

アプリケーション:
- 動作トリガー: 以下の日付に発動します。
  2003年06月31日以降

動作内容
1. 以下のファイルをコピーします。
   [条件] 次の状態が見つかった場合、このウイルスはWindowsのインストール先フォルダ（標準ではC:\WindowsまたはC:\Winnt）を探出し、その場所に自身をコピーします。
   - ファイル名: [Win.ini]mmcr0932.exe
2. 以下のファイルを作成します。
   - ファイル名: [Win.ini]hmlie.ini
3. 以下のファイルを作成します。
   - ファイル名: [Win.ini]redmbr.ini
4. 以下のレジストリを追加します。
   - 「Windowsの起動時に実行される」という值をレジストリに追加する
   - レジストリ値: "System Tray" = "[Win.ini]mmcr0932.exe"
   - レジストリキー: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
5. 以下の条件のとき、以下の動作を行います。
   - 次の状態が見つかった場合、次の動作を行います。
     - ファイル名: [Win.ini]hmlie.ini
     - ファイル名: [Win.ini]redmbr.ini
     - レジストリ値: "System Tray" = "[Win.ini]mmcr0932.exe"
6. 以下のファイルをコピーします。
   - ファイル名: [Win.ini]mmcr0932.exe
7. 以下のファイルをコピーします。
   - ファイル名: [Win.ini]mmcr0932.exe
8. 以下の条件でメールアドレスを検索します。
   - メールアドレス情報の持ファイルを検索
     - end
     - html
     - ini
     - txt

9. 以下の場合でメールを送信します。
   - 送信されるメールは次のいずれかの件名、添付ファイル、本文を記載してください。
   - 件名: Your details
     - Approval: Ref. 304-4590
     - File: Approved (Ref. 3994-38567)
     - File: Install
     - File: Screnaver
     - File: Screnner
     - File: My application
   - All information is in the attached file.
   - User's email: support@microsoft.com

Sorry in Japanese.
This is automatically generated within 10min.
Macro-micro correlation

Macro-micro correlations to connect the results of network-based macro analysis and host-based micro analysis for detailed incident reports.
Macro-Micro Analysis 1/2

**From Macro Analysis**

By means of

- Visualization
  - TAP (Traffic Analysis and Profiling)
  - CPD (Change Point Detection)

Current Outputs

- Visualization → Current trend of 3D image & World map
- TAP  → Latest Traffic Pattern (combination of Ports…)
- CPD  → Traffic pattern newly increased

**From Micro Analysis**

By means of

- Code analysis and Behavior analysis

Outputs: Analysis Reports in XML and in Human Readable
Macro-Micro Analysis 2/2

**Correlation**

Current Outputs
Visualization → Current trend of 3D image & World map

* Correlate with Malware Analysis report in Human Readable
  * TAP → Latest Traffic Pattern (combination of Ports…)
  * CPD → Traffic pattern newly increased

* Correlate with Malware Analysis report in XML

**Outputs from the Correlation**

Identify what’s really happening in the large network providing with the cause why it behaves like that.

See an example:
Examples of Macro and Micro Correlation 1/3
(Macro Analysis)

**TAP Analysis**
Network scanning port 445 to many IP addresses

**CPD Analysis**
Detected change point of scan frequency on tcp/445

**Visualization:** 3D and World map ➔ Video

NiCT
National Institute of Information and Communications Technology

nicter
Network incident analysis center for tactical Emergency Response
1) Attempts to create a mutex named JumpallsNilsTillt and exits if the attempt fails.
2) Attempts to create a mutex named Jobaka3.
3) Copies itself as %Windir%\Avserve2.exe.
4) Adds the value: "avserve2.exe"="%Windir%\avserve2.exe" to the registry key: so that the worm runs when you start Windows.
5) Starts an FTP server on TCP port 5554. This server is used to spread the worm to other hosts.
6) Retrieves the IP addresses of the infected computer, using the Windows API, gethostbyname.
7) Generates another IP address, based on one of the IP addresses retrieved from the infected computer.
8) Connects to the generated IP address on TCP port 445 to determine whether a remote computer is online.
9) If a connection is made to a remote computer, the worm will send shell code to it, which may cause it to open a remote shell on TCP port 9996.
10) Uses the shell on the remote computer to reconnect to the infected computer's FTP server, running on TCP port 5554, and to retrieve a copy of the worm. This copy will have a name consisting of four or five digits, followed by _up.exe.
11) continued
Examples of Macro and Micro Correlation 3/3

**Correlation**
Visualization → Current trend of 3D image & World map

* Correlate with Malware Analysis report in Human Readable
* Similar tcp/445 scan can be recognized as visualization

* TAP → Latest Traffic Pattern (tcp/445…)
* CPD → Traffic pattern tcp/445 newly increased

* Correlate with Malware Analysis report in XML

**Outputs from the Correlation**

tcp 445 scan can be frequently detected in both TAP and CPD and the reason of this scan must be Sasser worm. This type of correlation analysis should be carried out in a few minutes with minimum operator skill. This type of analysis also can be applied for the non-detected virus attacks.
Our partners

- **Telecom-ISAC Japan**
  - Organization of Japanese ISPs
  - Sharing incident information among the members
  - Wide-area monitoring with probes on ISPs
  - Incident handling with contingency plans
  - Clearing house of incident info for ISPs

- **Internet Security research communities**
  - Academic network administrators
  - Virus and malware analysis experts
  - Data mining and statistics experts
  - ... and we need more interdisciplinary partners

Output of our system will be transferred for Telecom-ISAC and NISC
Our plans on 2006

• research and development
  – Improving accuracy of packet/event analysis
  – Efficient collaboration with static/dynamic virus/malware analysis methods
  – Effective visualization system implementation

• Publicizing our achievements and results
  – Collaboration with related projects
    • e.g., Univ. of Michigan
  – Integration with Telecom-ISAC-Japan operation
  – Publication of academic papers and symposiums
Macro-micro correlation analysis

Flow of *macro* analysis
- Traffic visualization
- Real-time analysis
- In-depth analysis

Network event database

Macro-micro correlation

Flow of *micro* analysis
- Malware code analysis
- Malware behavior analysis

Malware behavior database

Recognition of NW Behavior

Detailed Incident report

Virus code & behavior Analysis

Captured traffic IDS logs

IDS

Virus

Bot

Worm

Darknet

Honeypot

Dummy email accounts

NiICT

National Institute of Information and Communications Technology

nicter
Thank you for listening.

Q&A

- Implement & operate Nicter
- Design Nicter
- Monitor & review Nicter
- Maintain & improve Nicter