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

NiCT National Institute of Information and Communications Technology

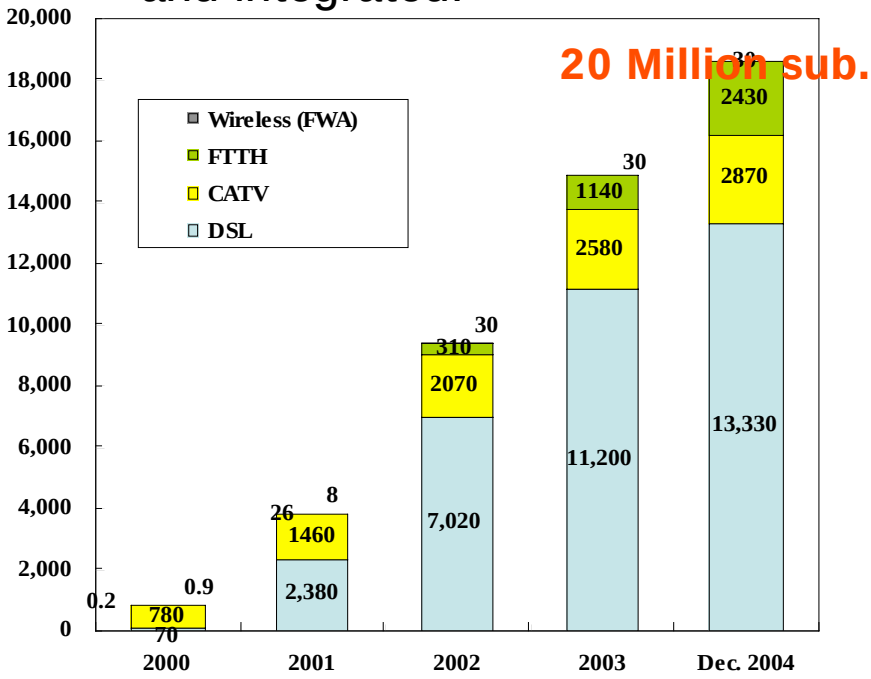
nicter Network Incident Analysis Center for Tactical Emergency Response

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.



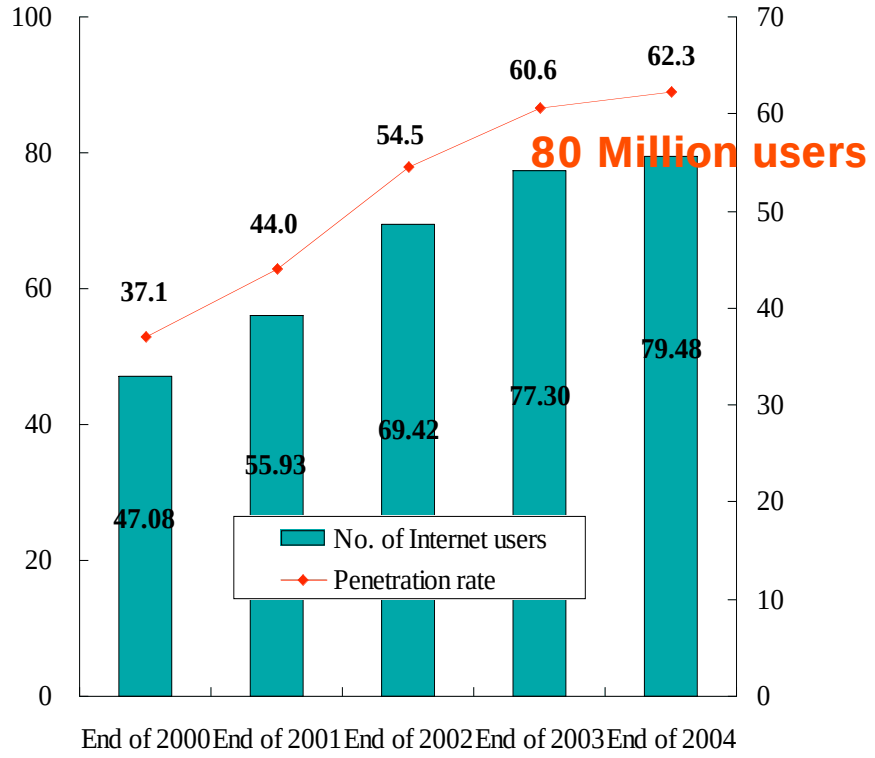


Figure 1: Number of Internet users and penetration rate

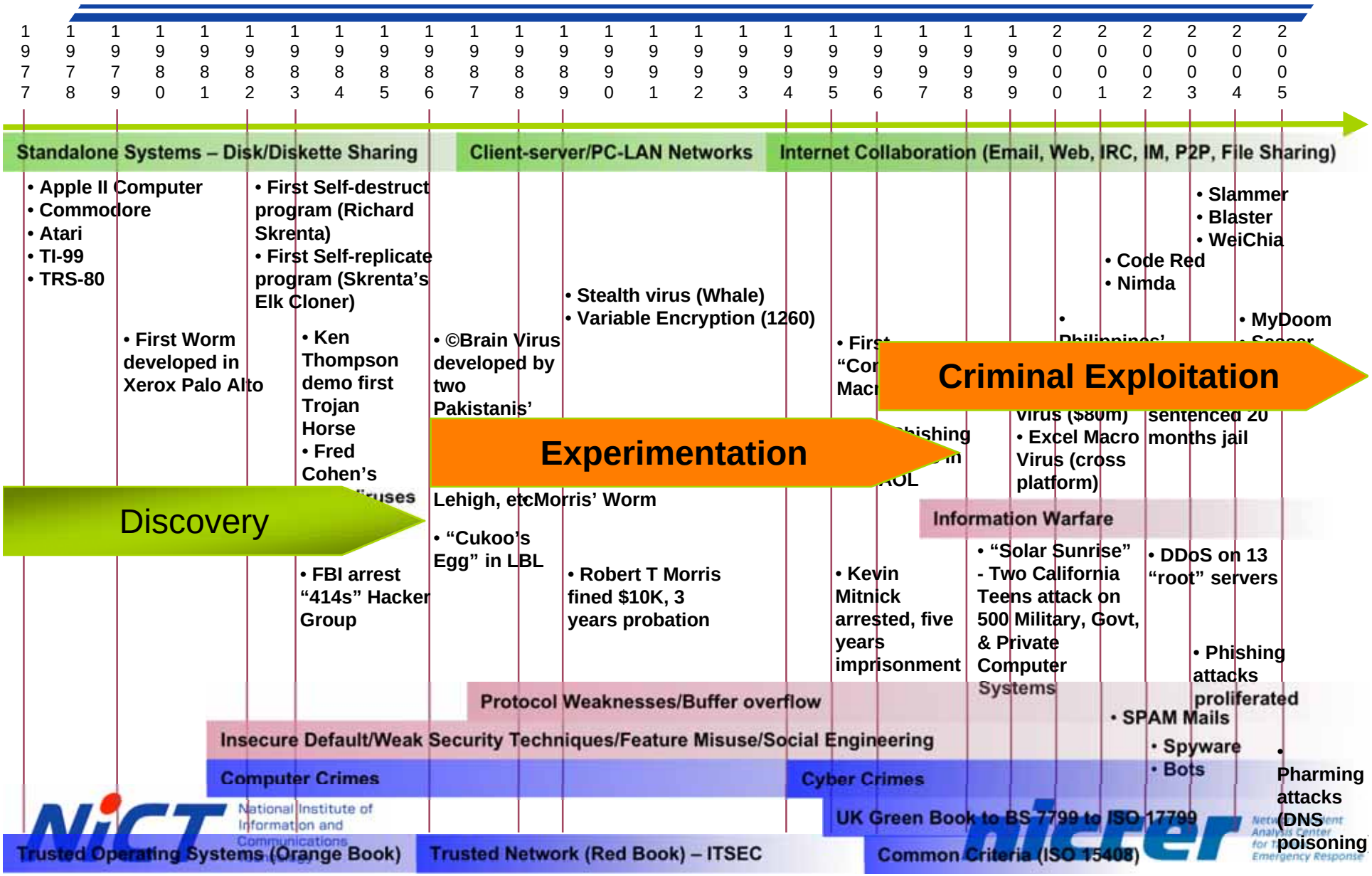
Figure 2: Transition in the number of broadband subscribers

NiCT National Institute of Information and Communications Technology

nicter Network Incident Analysis Center for Tactical Emergency Response

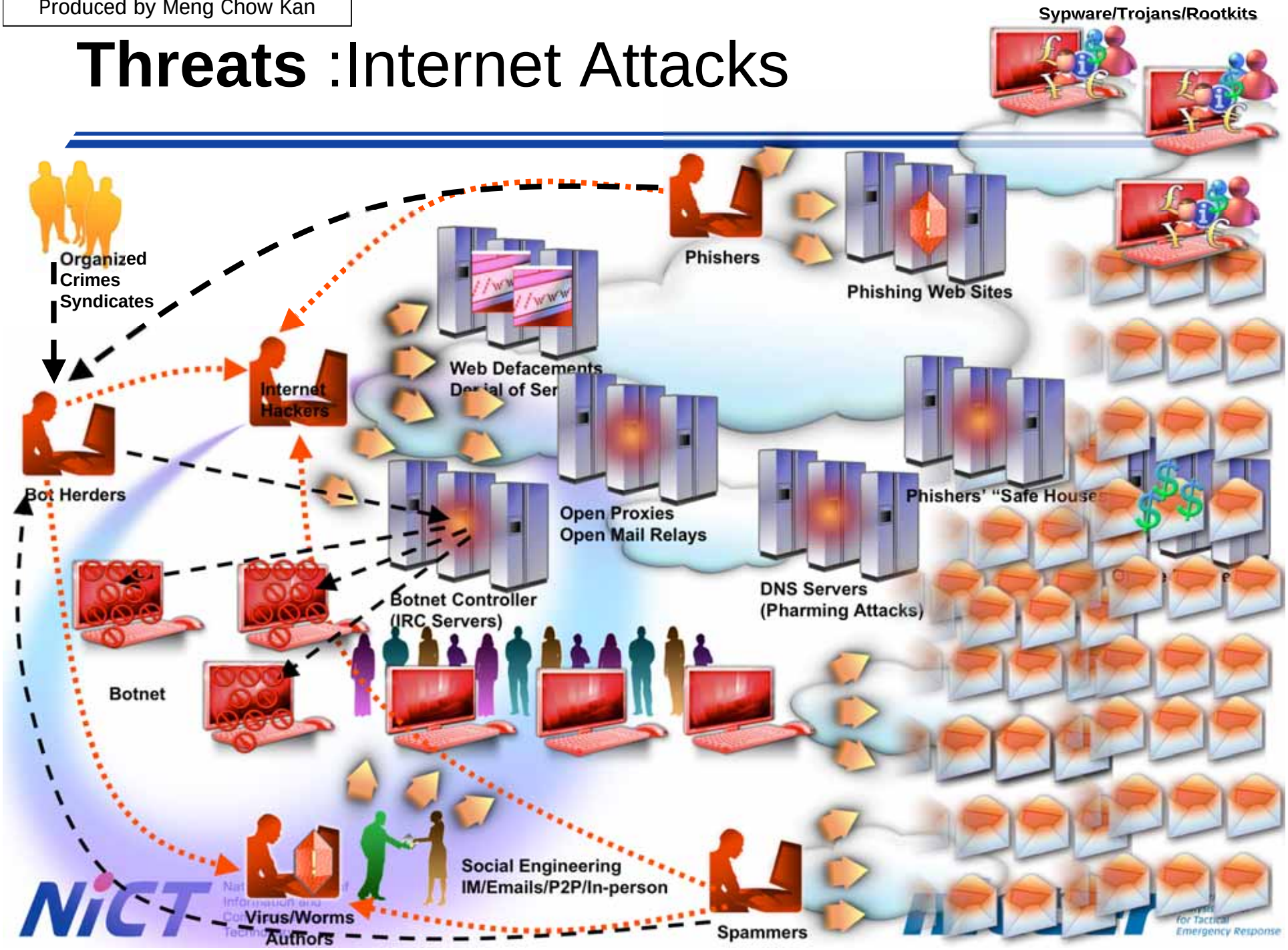
Produced by Meng Chow Kan

A short history of computing & insecurity



Produced by Meng Chow Kan

Threats :Internet Attacks



Overview of the project

nicter = **N**etwork **I**ncident analysis **C**enter for **T**actical **E**mergency **R**esponse

Objectives:

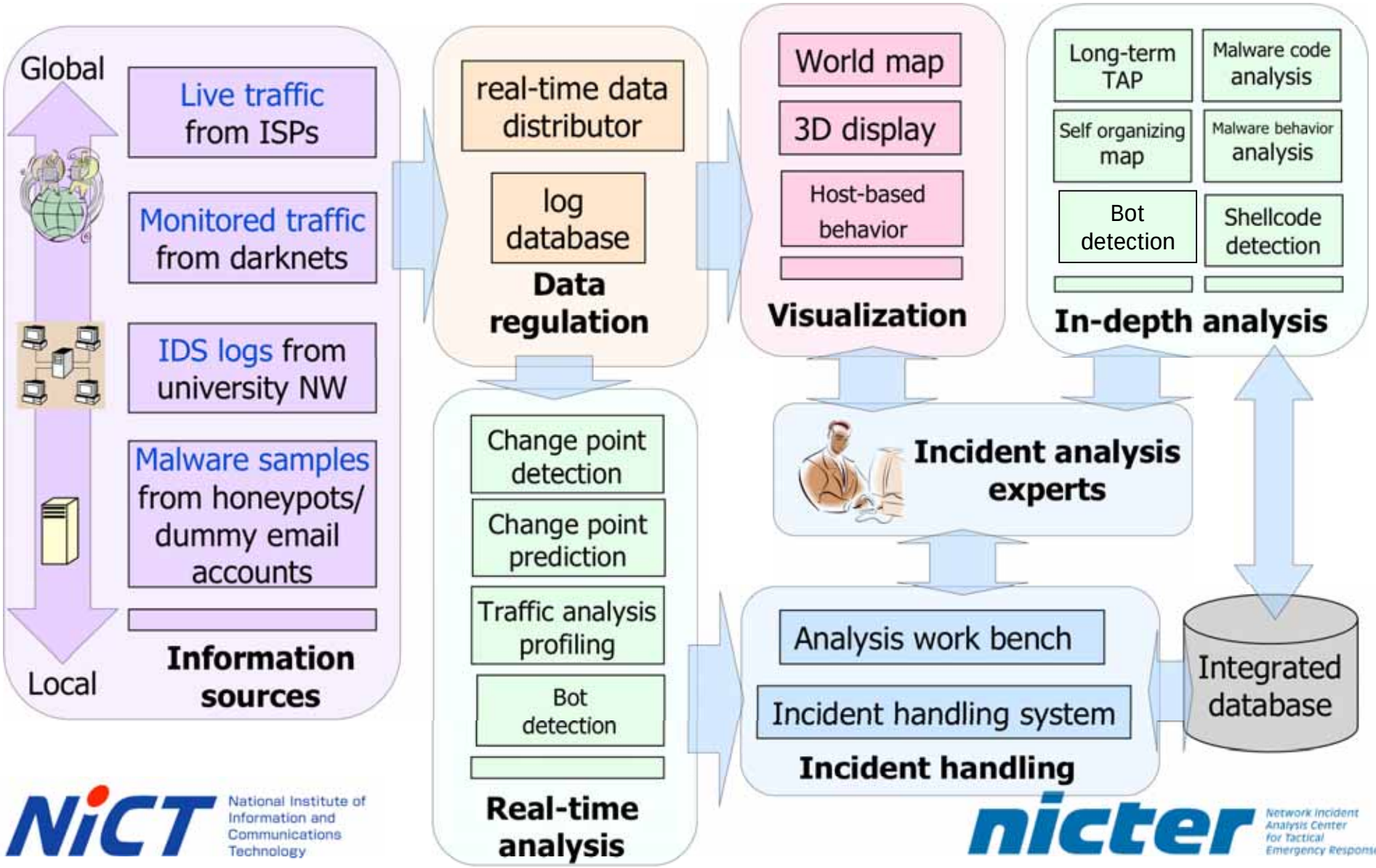
- Integrated analysis of network security incidents in large networks
  - Monitoring nation-wide large networks with various sources
  - Real-time and automated analysis for detecting precursors before outbreaks
  - **Macro-micro correlation analysis** to identify the latest incidents detected
  - Providing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

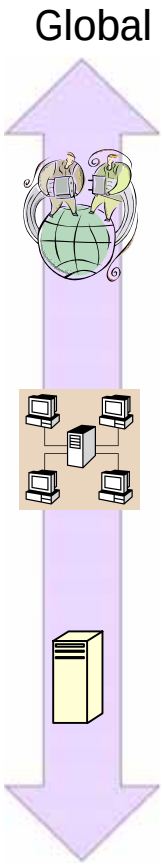
nicter beta operation center

System functional overview



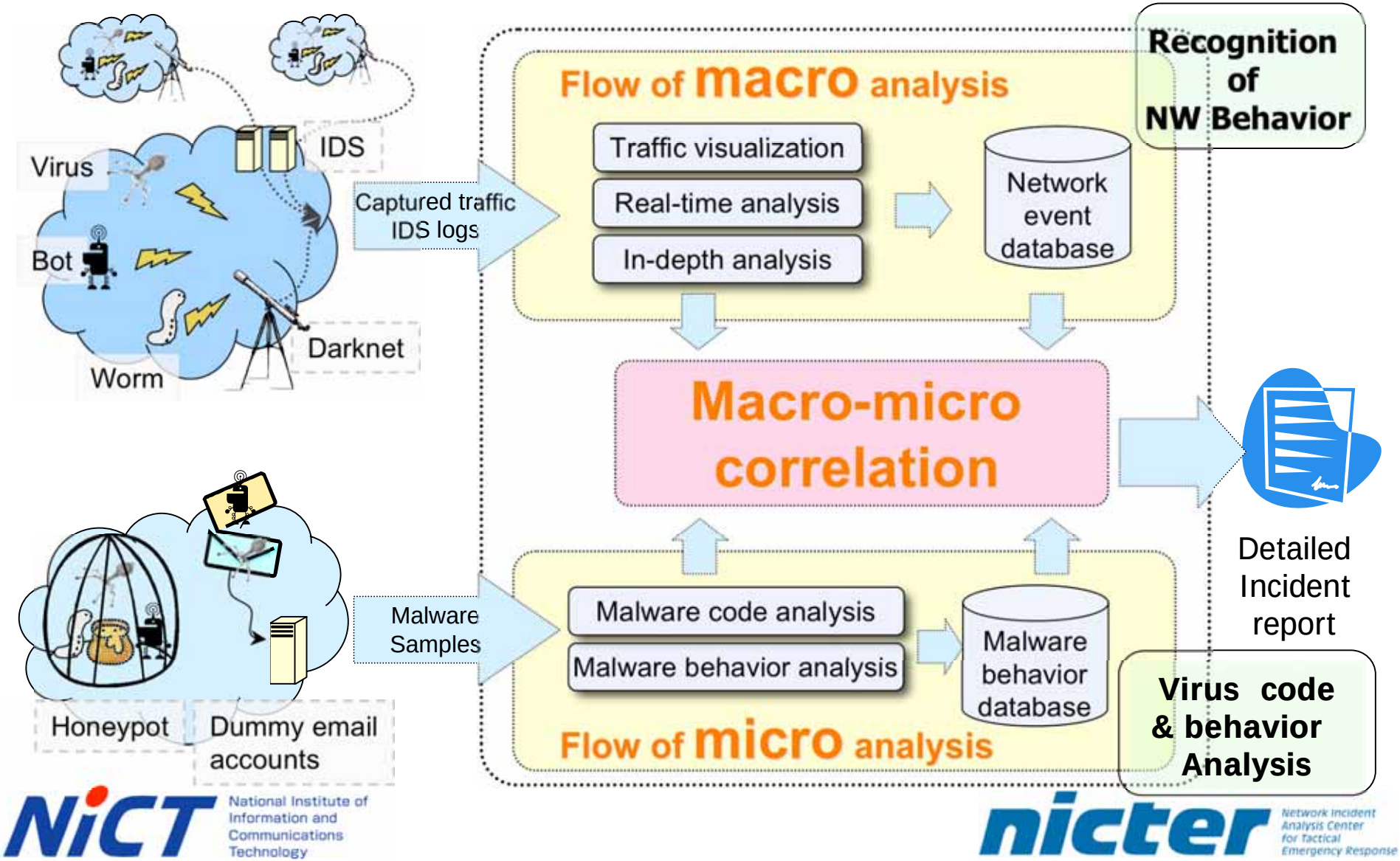
Information sources

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

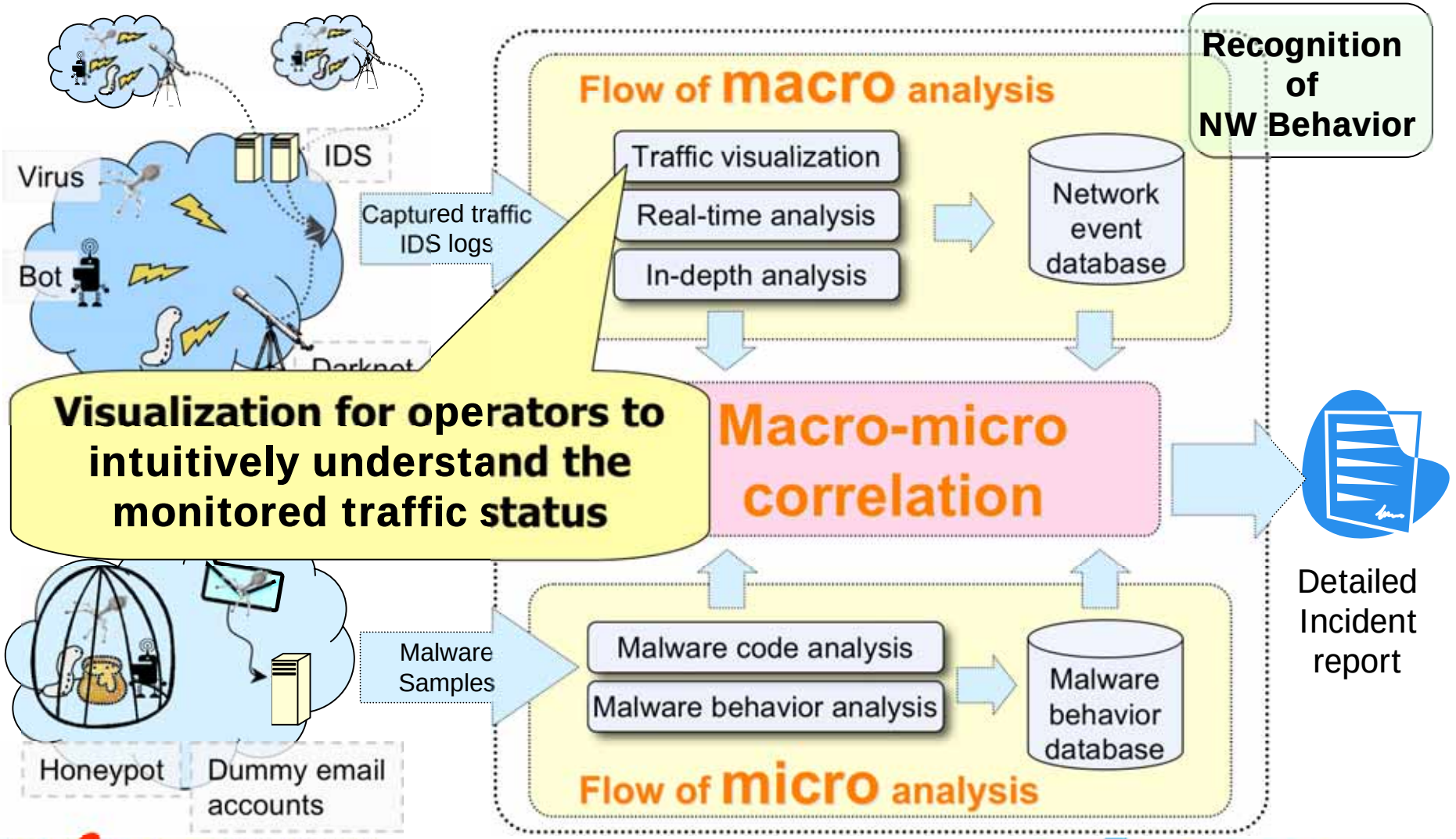


NiCT National Institute of Information and Communications Technology

nicter Network Incident Analysis Center for Tactical Emergency Response

Macro analysis

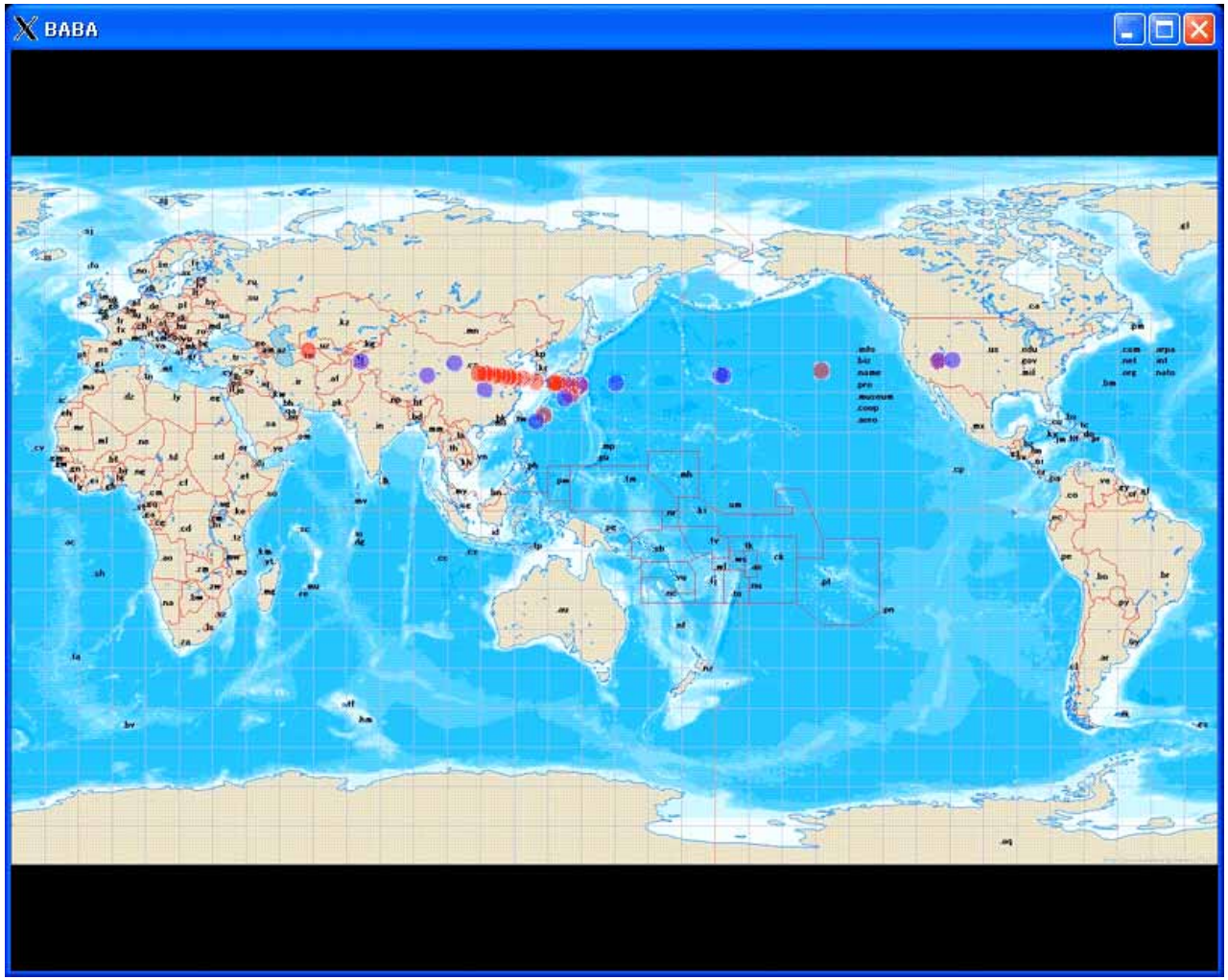
Visualization of monitored traffic



NiCT National Institute of Information and Communications Technology

nicter Network Incident Analysis Center for Tactical Emergency Response

Real-time packet source visualization

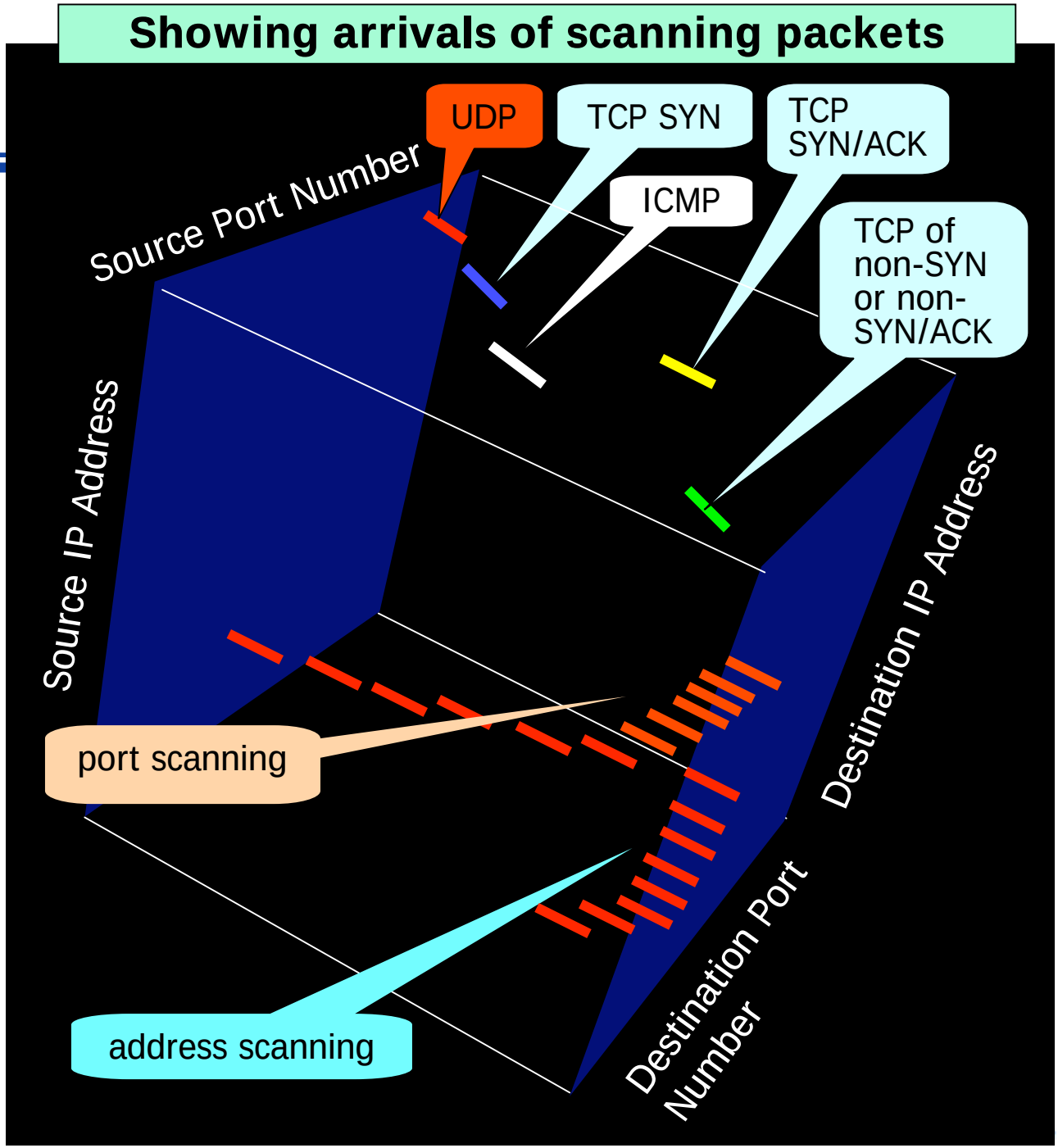


Visualizing source of incoming packets at our darknet

NiCT National Institute of Information and Communications Technology

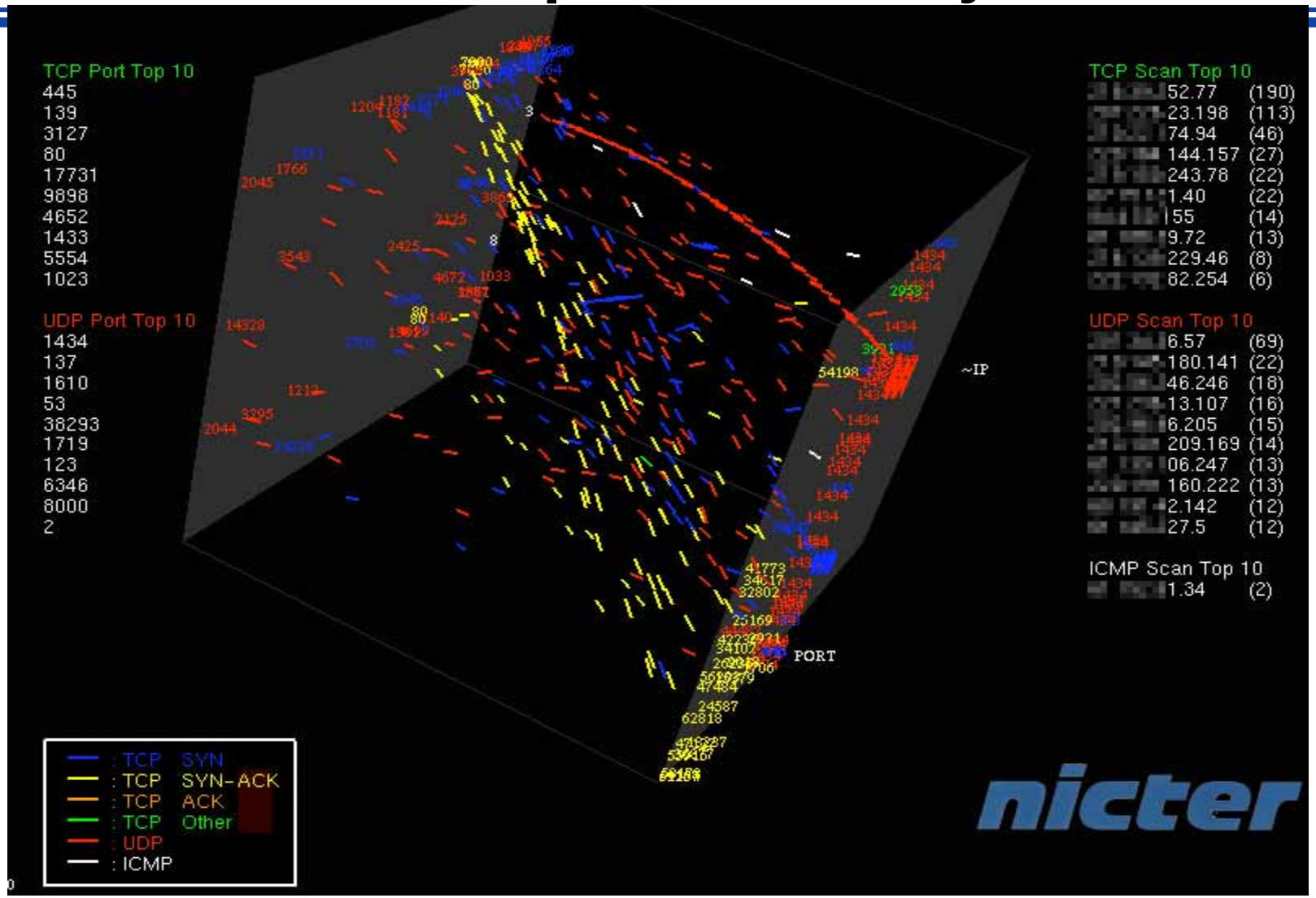
nicter Network Incident Analysis Center for Tactical Emergency Response

3-D display of real-time incoming packet flow



NiCT National Institute of Information and Communications Technology

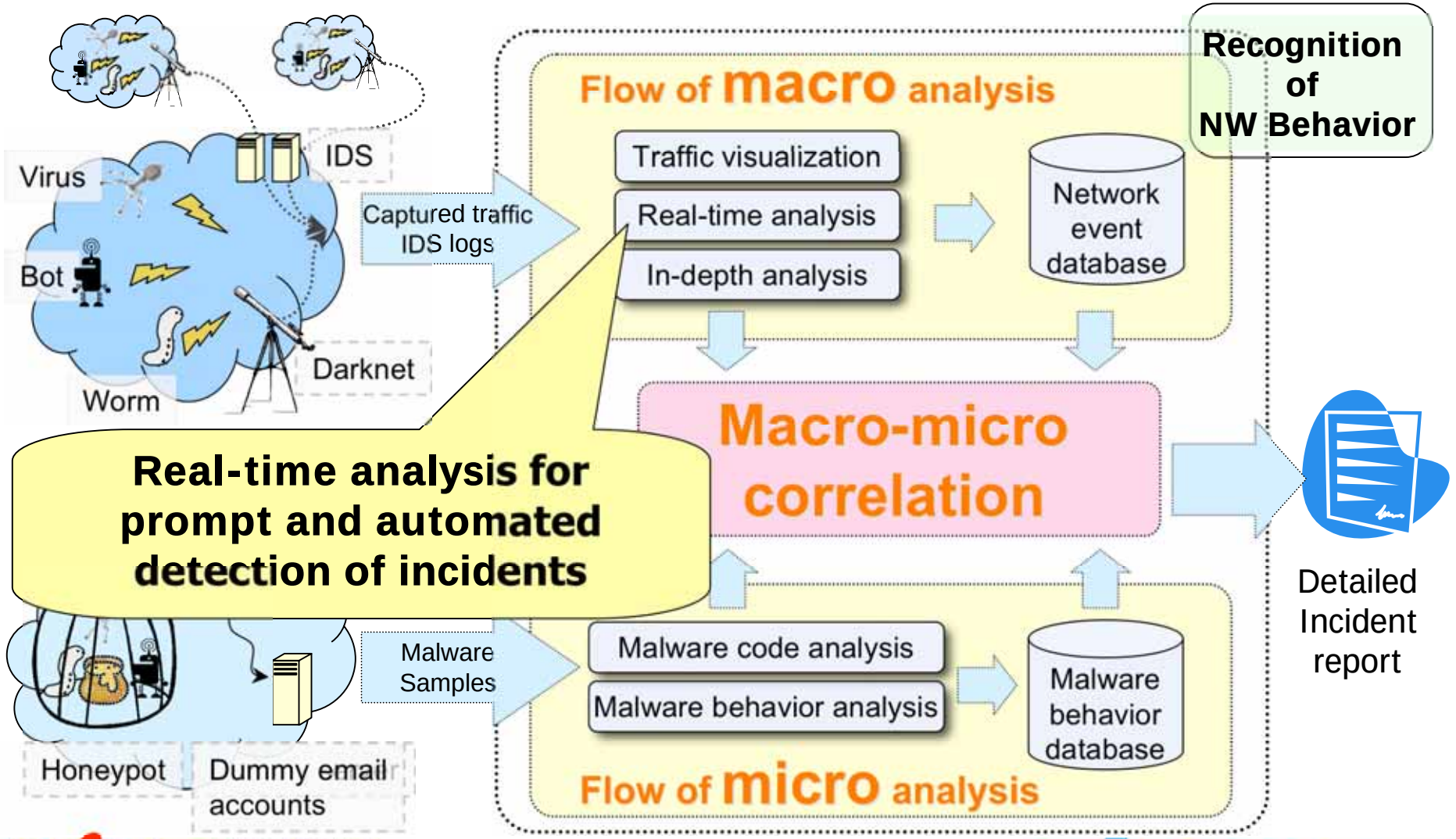
Scan activities detected in Interop 2006 in Tokyo



NiCT National Institute of Information and Communications Technology

nicter Network Incident Analysis Center for Tactical Emergency Response

Real-time analysis



NiCT National Institute of Information and Communications Technology

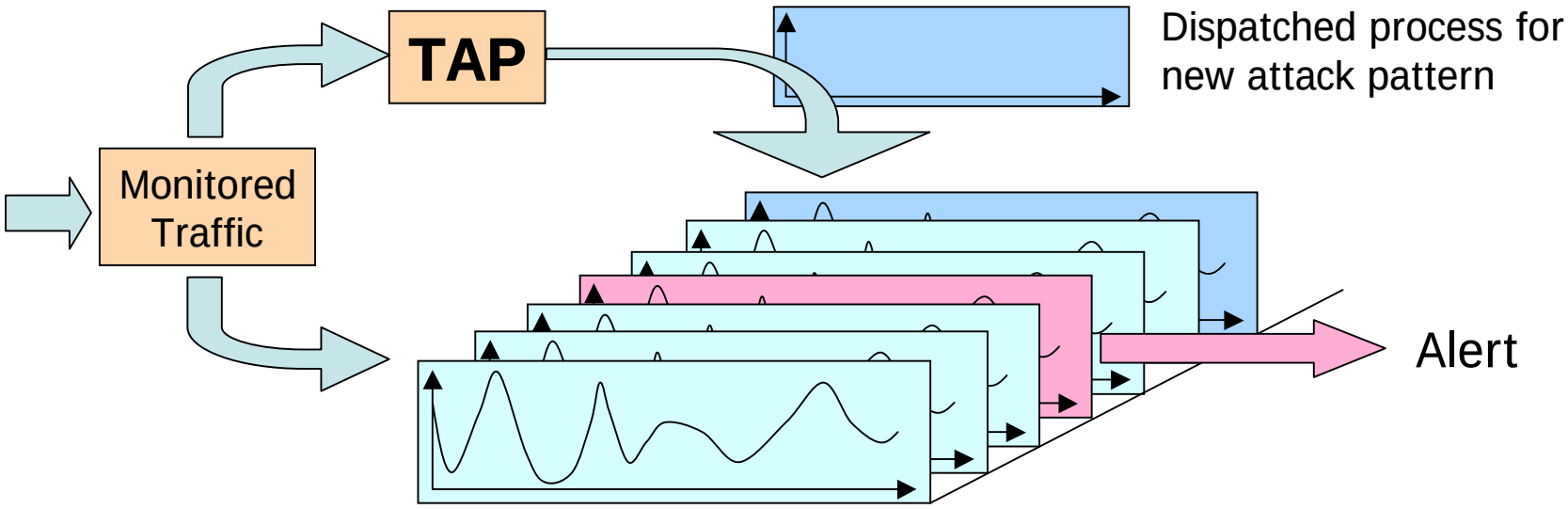
nicter Network Incident Analysis Center for Tactical Emergency Response

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

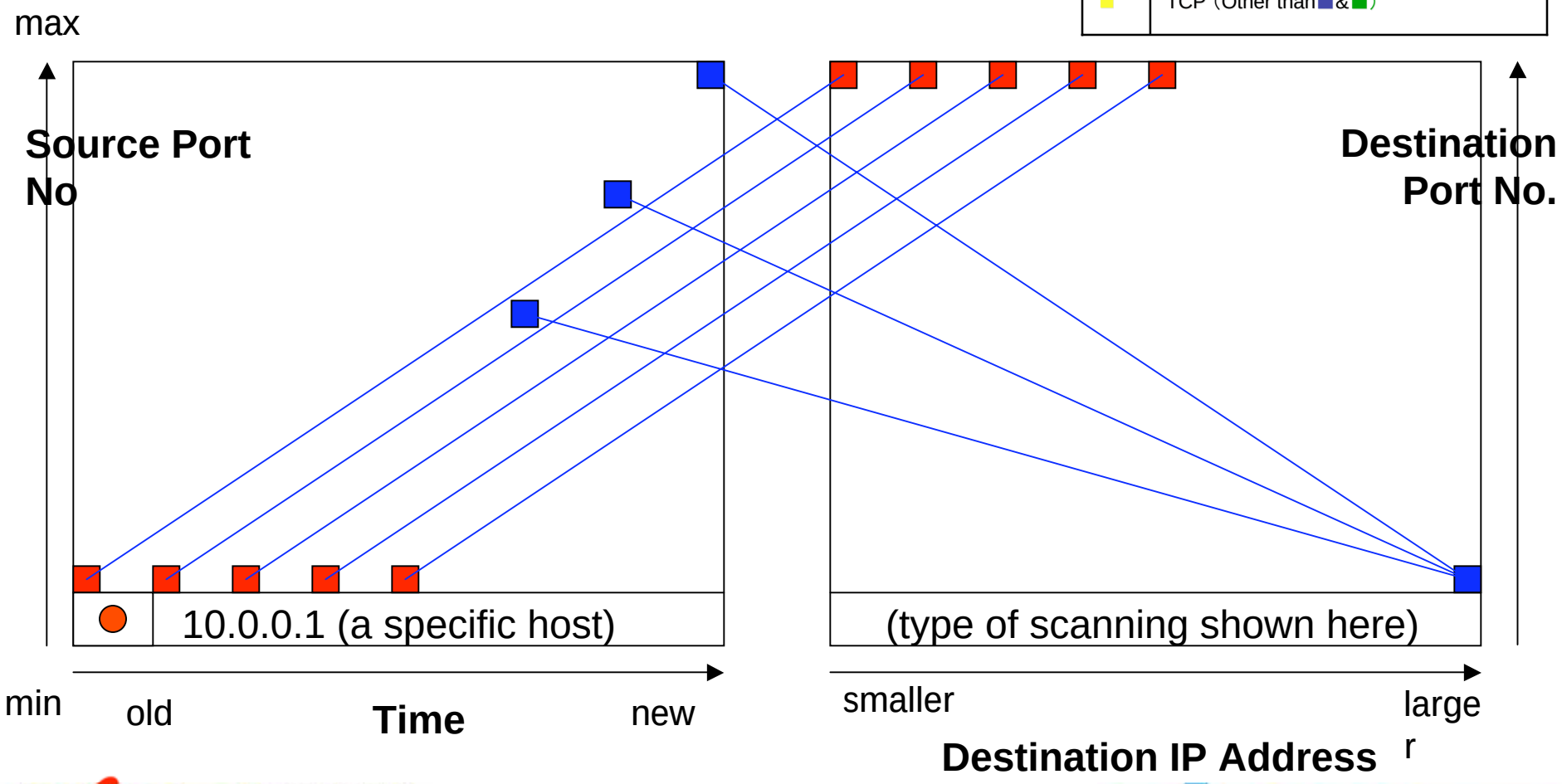
Overview of real-time analysis

- **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



Graphical representation of TAP behavioral analysis

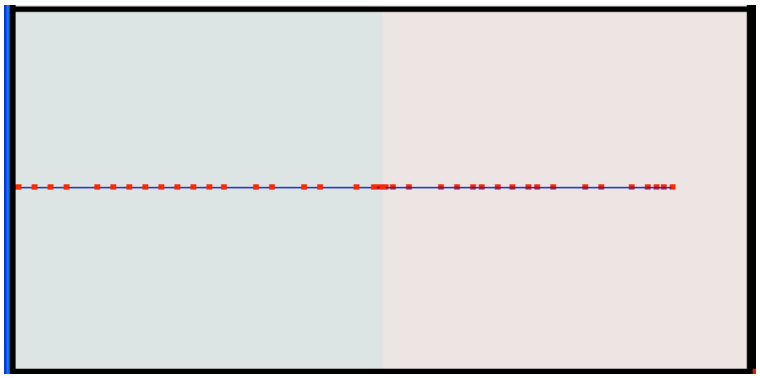
■	TCP SYN
■	UDP
□	ICMP
■	TCP SYN+ACK
■	TCP（Other than■&■）



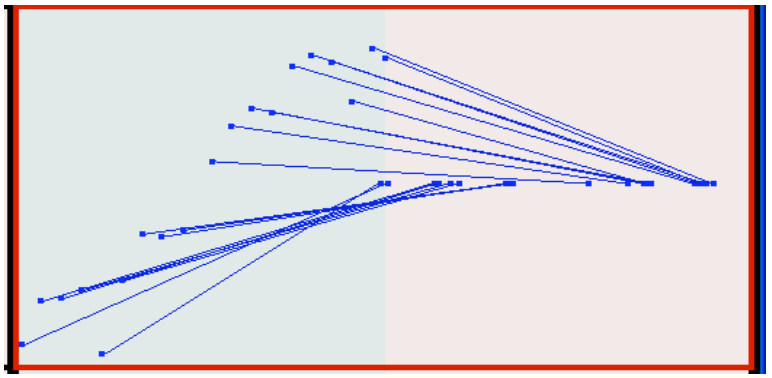
National Institute of Information and Communications Technology

nicter Network Incident Analysis Center for Tactical Emergency Response

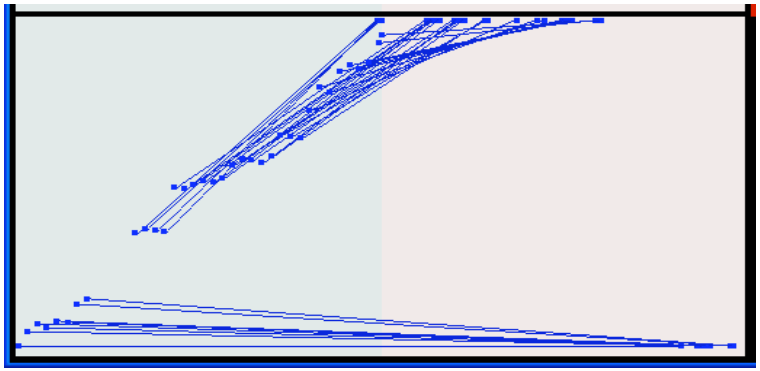
Examples of TAP analysis results



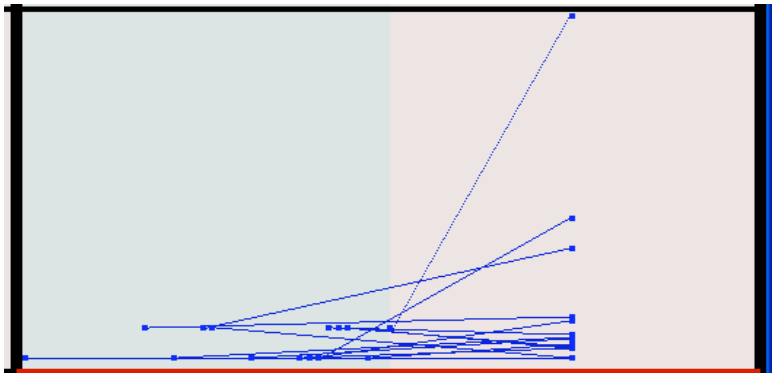
UDP scanning for many IP addresses



Network scanning to many IP addresses

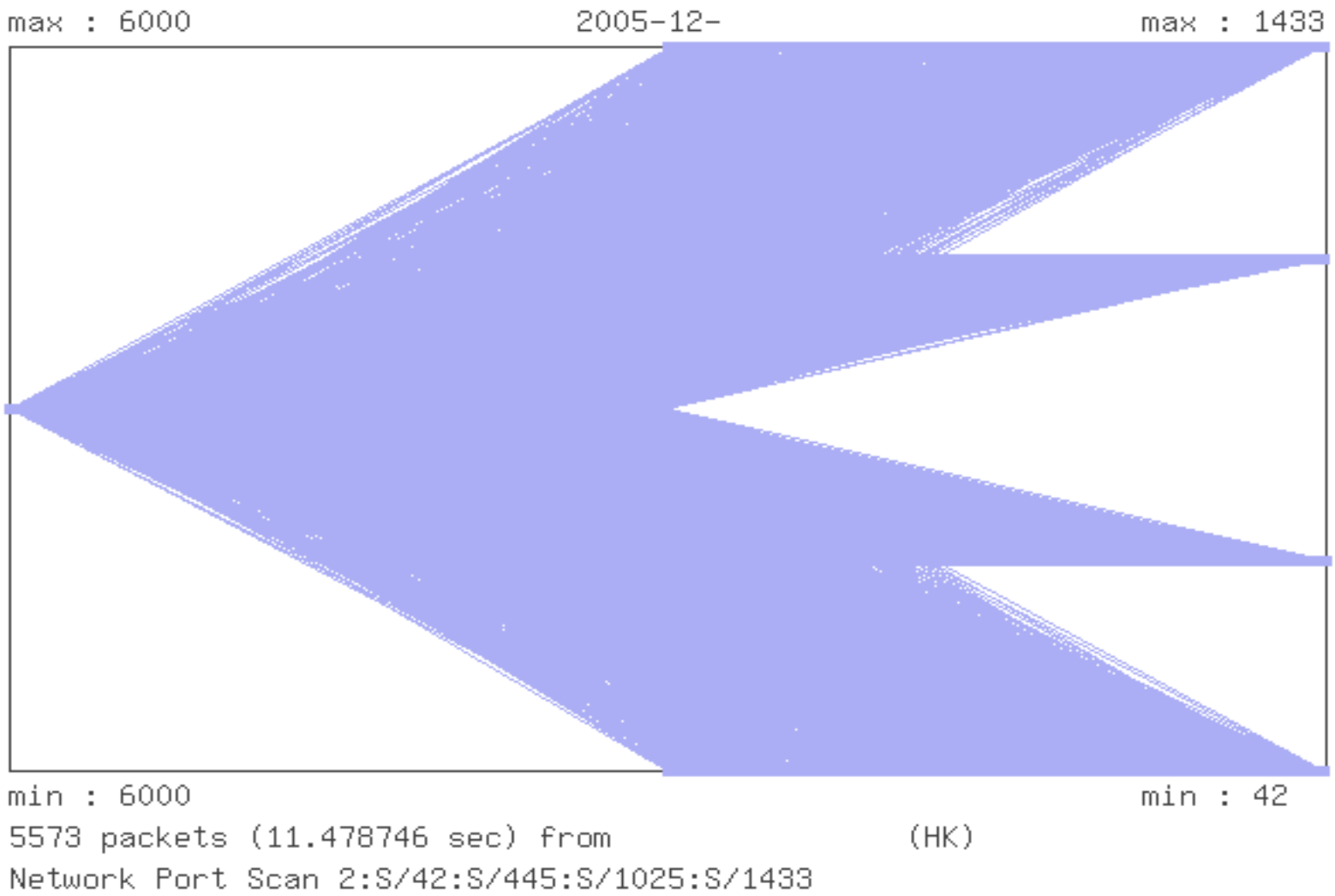


Two types of simultaneous scannings
(network scanning (up) +
port scanning (down))



Multiple port scan for a single IP address

A Dasher worm's TAP behavior



Change-Point Detection (CPD)

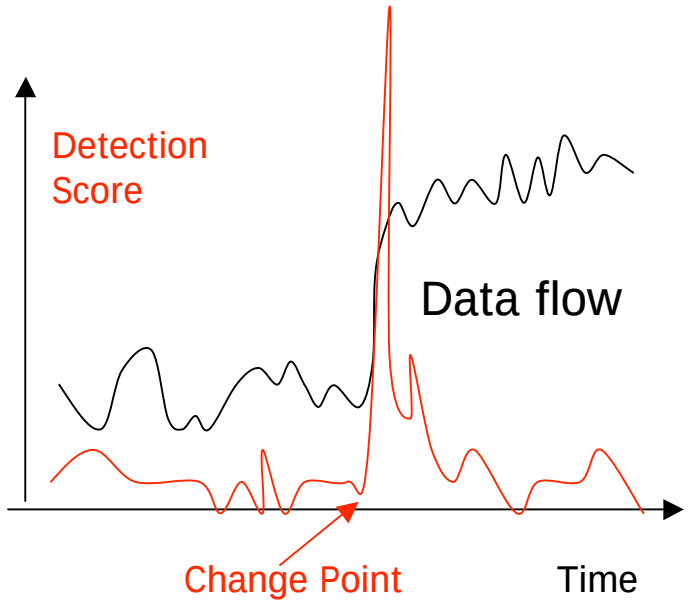
- Detecting rapid change of time-variant data
  - calculating scores of change
  - generating alerts when score exceeds threshold value

Fast real-time learning

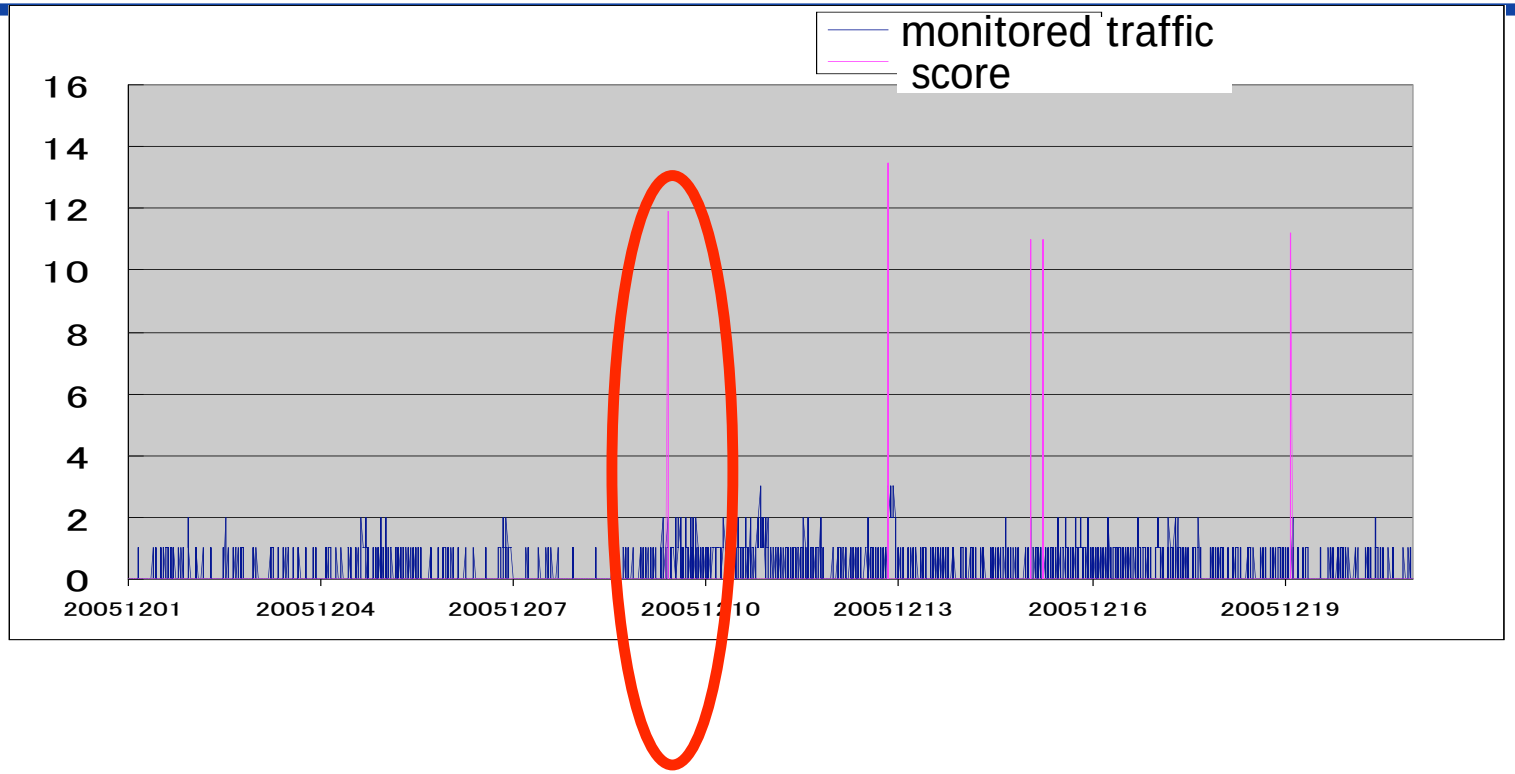
Adaptive to long-term change

Low false-alarm rate

Faster than repetitive statistical testings

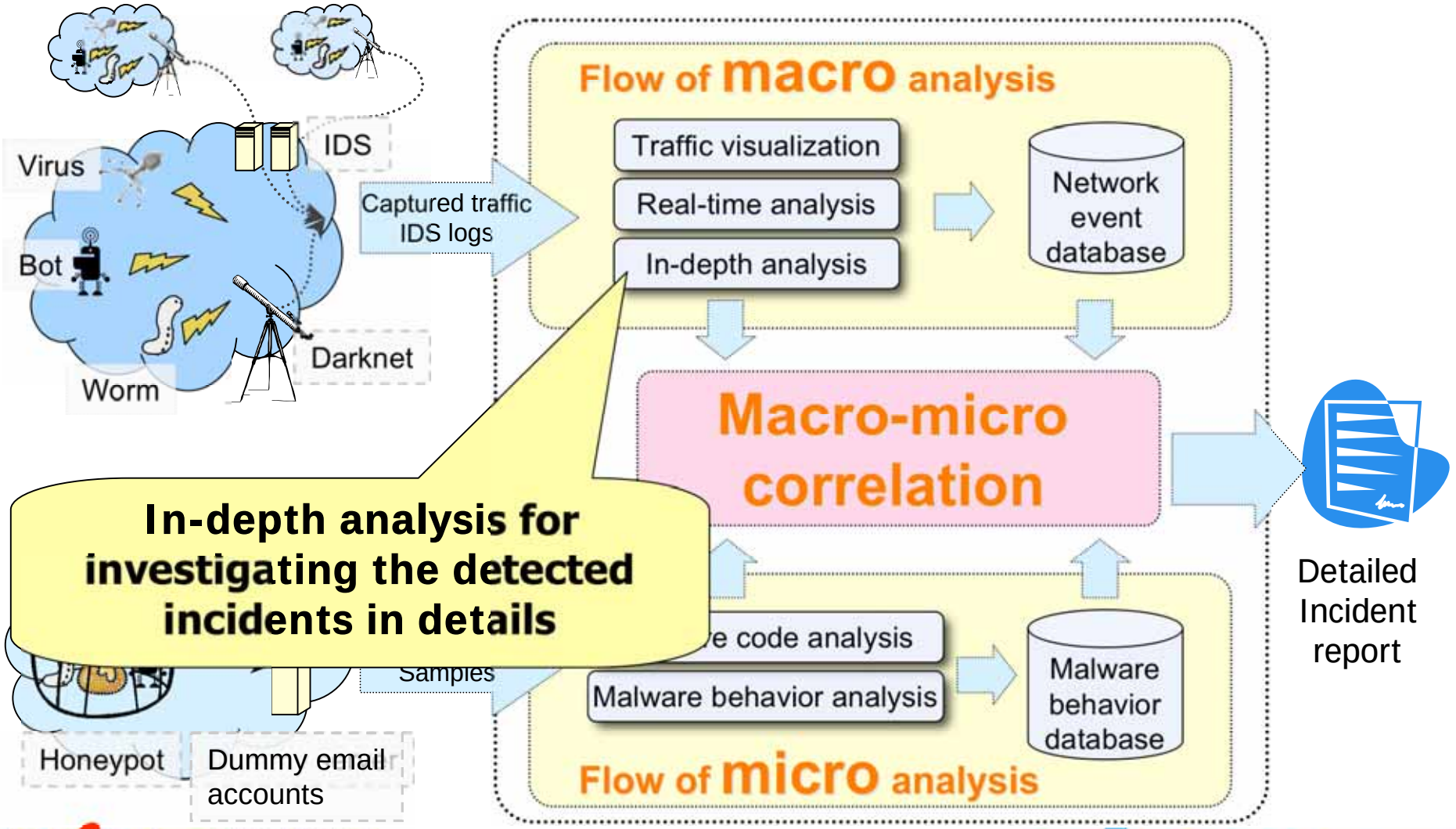


Example (Dec. 2005)



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



NiCT National Institute of Information and Communications Technology

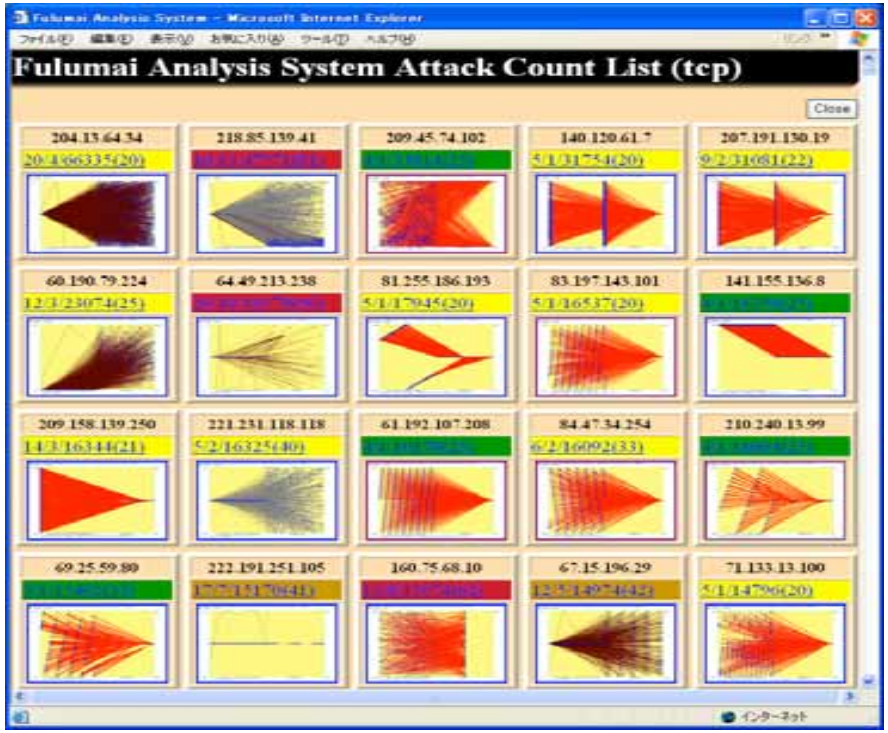
nicter Network Incident Analysis Center for Tactical Emergency Response

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

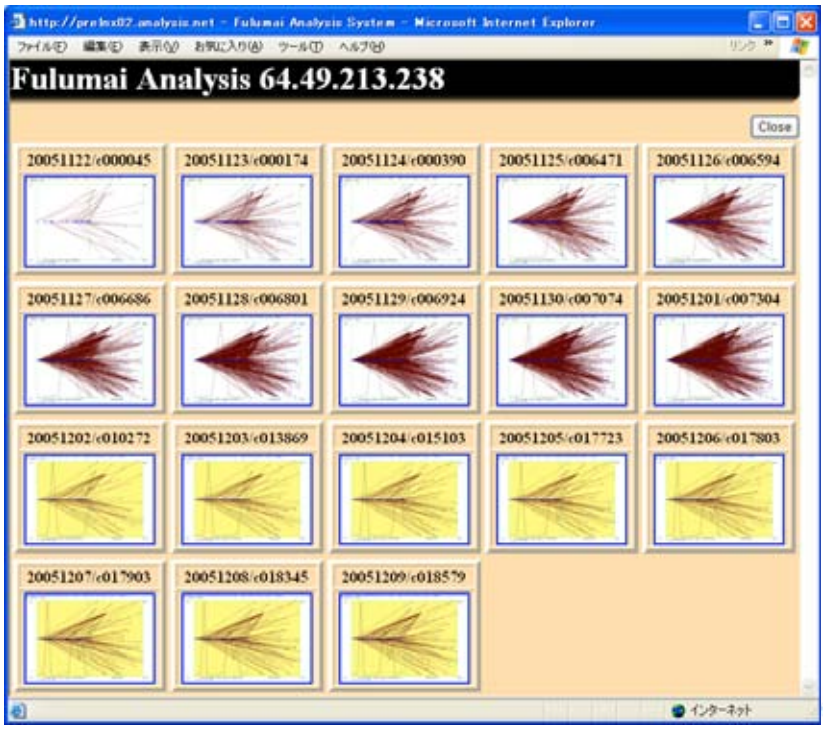
Long-term TAP graph analysis

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

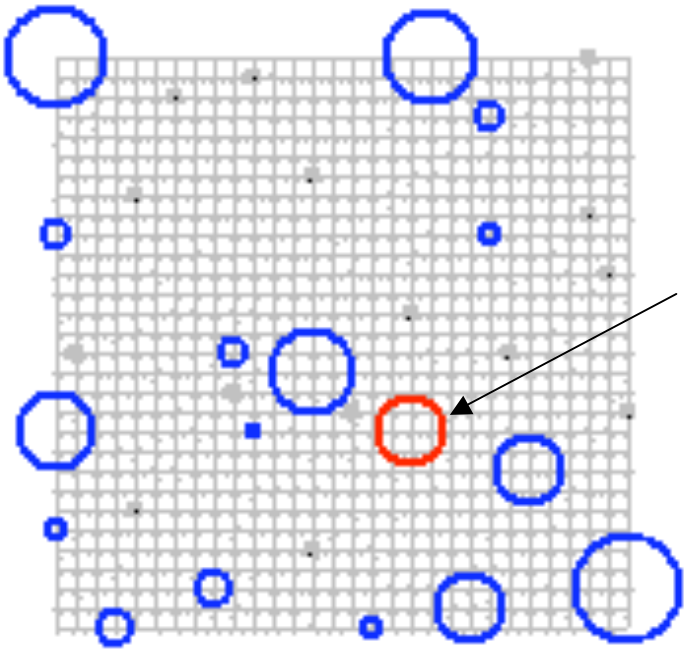
Showing long-term change of per-host trends



NiCT National Institute of Information and Communications Technology

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

Specified parameter → tcp/1025

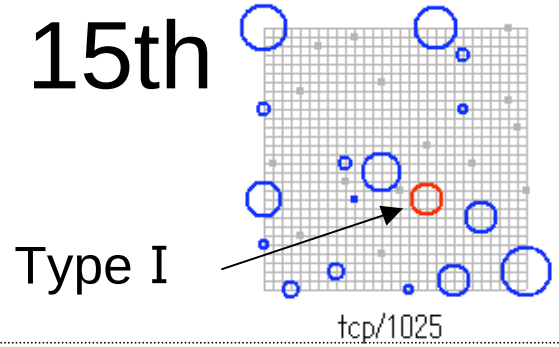
Example : Finding worm variants by SOMs

Dec 15th

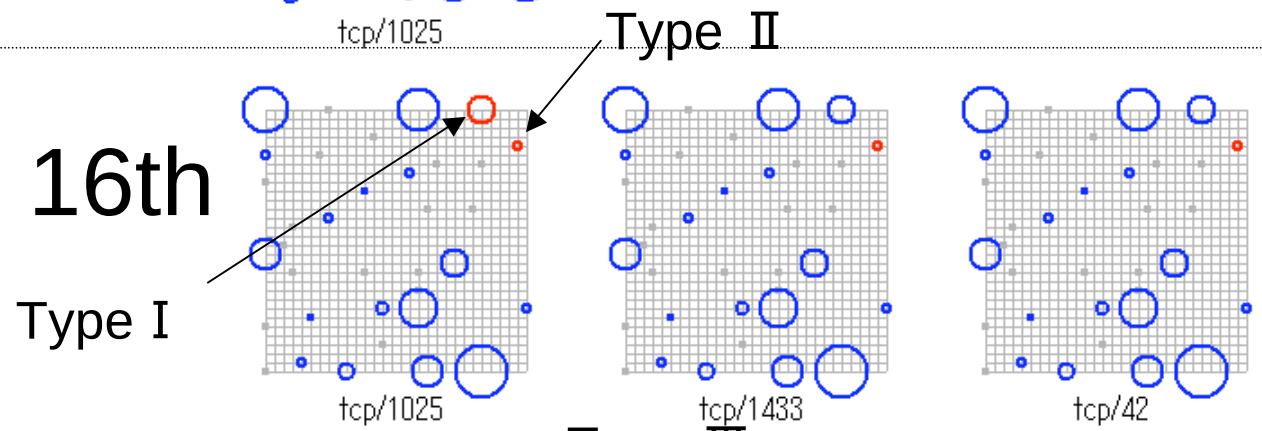
Type I (Dasher.A-C) : tcp/1025

Type II (a Dasher variant) : tcp/1025, 1433, 42

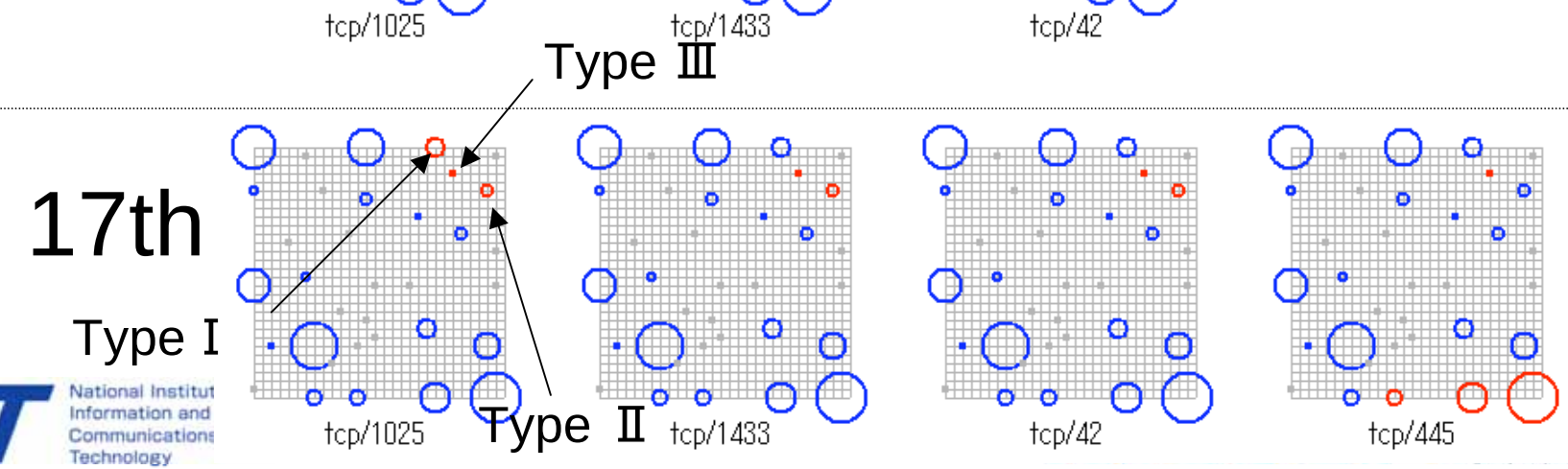
Type III (Dasher.D) : tcp 1025, 1433, 42, 445



Dec 16th



Dec 17th



NiCT National Institut Information and Communications Technology

Shellcode detection

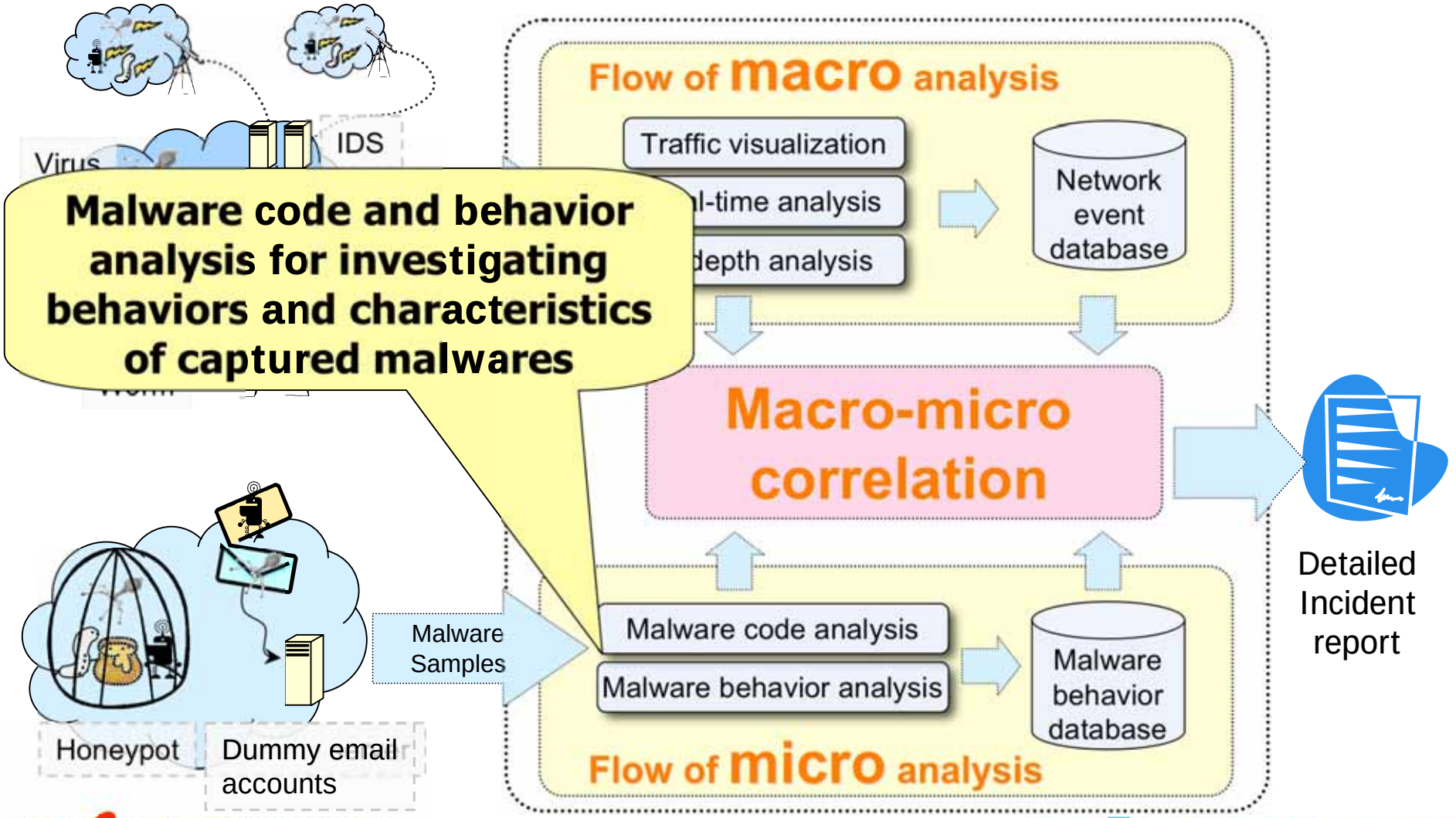
(Security Program based on structural analysis)

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

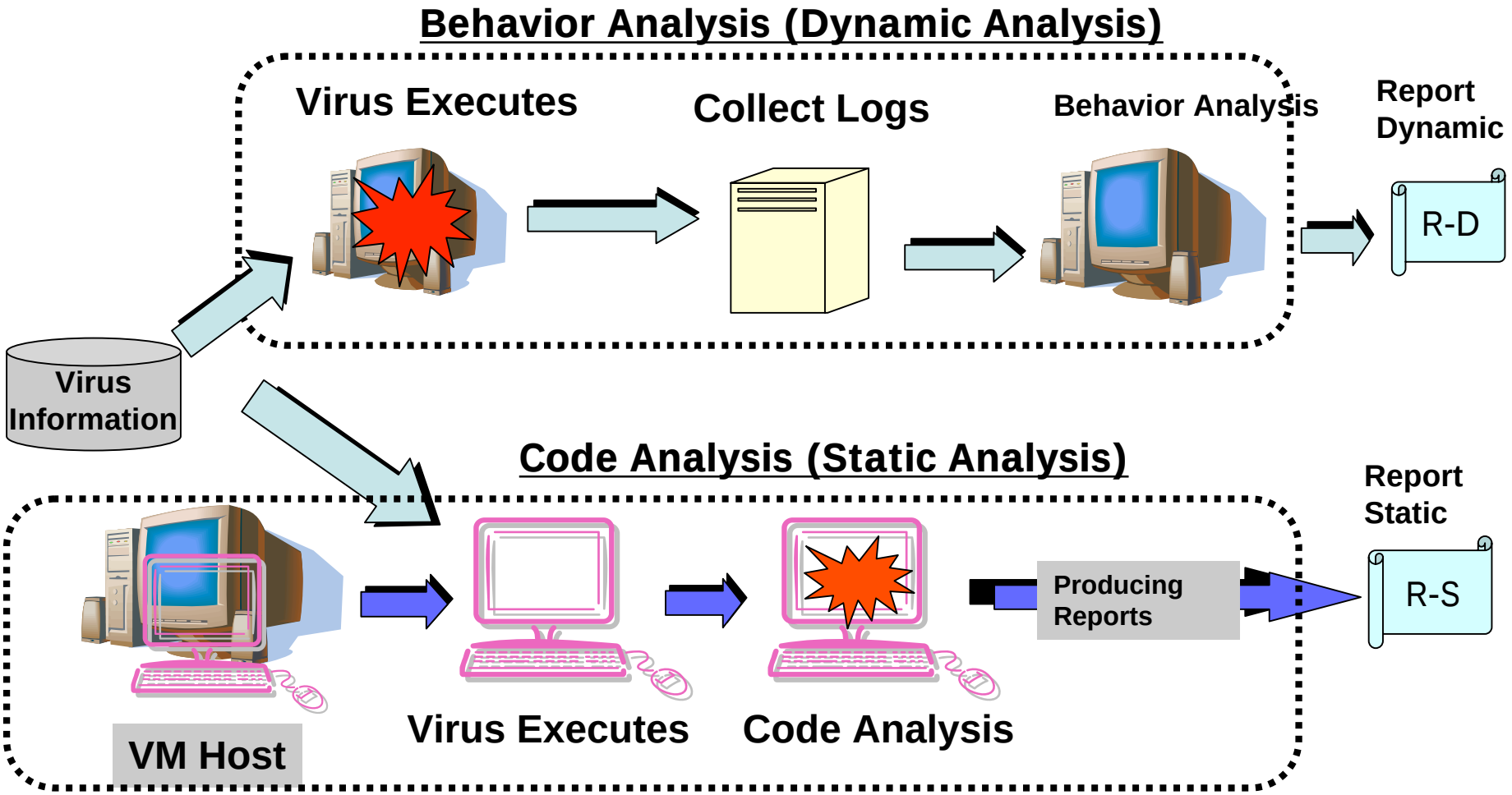
Malware code and behavior analysis



NiCT National Institute of Information and Communications Technology

nicter Network Incident Analysis Center for Tactical Emergency Response

Micro Analysis of Malware by means of two methods



Example of description by XML in the case of Happy99.Worm

```
<?xml version="1.0" encoding="Shift-JIS"?>
<MaliciousCodeXML>
  <MaliciouCode>
    <Name>Happy99.Worm</name>
    <Attribute><worm/></Attribute>

    <Trigger>Online</trigger>
    <Action>
      <openWindow>
        <windowtitle>Happy NewYear 1999!!</windowtitle>
      </openWindow>
      <createFile>
        <directry>WINDOWS\SYSTEM</directry>
        <file>SKA.DLL</file>
      </createFile>
     <if>
                    ……
     </Action>
  </MaliciousCode>
</MaliciousCodeXML>
```

Information non-action related

Information regarding Actions of this worm

More specifically

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

XML→ Human Readable Description

W32.Sobig.B@mm

- 種別:
  - ワーム
- 影響を受ける可能性のあるシステム:

[OS]
- Windows 95
- Windows 98
- Windows NT
- Windows 2000
- Windows XP
- Windows Me

[アプリケーション]

- 発症トリガ:
  以下の日にちに発症します.
  2003年 05月 31日以前

動作内容

1. 以下のファイルをコピーします.
   ※[Windir]は可変であり，このワームはWindowsのインストール先フォルダ（標準では C:¥Windows または C:¥Winnt）を探し出し，その場所に自分自身をコピーする.
   - ファイルパス名：[Windir]¥msccn32.exe
2. 以下のファイルを作成します.
   - ファイルパス名：[Windir]¥hnks.ini
3. 以下のファイルを作成します.
   - ファイルパス名：[Windir]msdbrr.ini
4. 以下のレジストリを追加します.
   ※Windowsの起動時に必ずワームが実行されるように以下の値をレジストリキーに追加する
   - レジストリ値："System Tray"="[Windir]¥msccn32.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，次の動作を行います.
   [条件]
   以下の条件のうちいずれかにあてはまるとき
   OSが
   - Windows NT
   - Windows 2000
   - Windows XP

   [動作]
   - 以下のレジストリを追加します.
     - レジストリ値："System Tray"="[Windir]¥msccn32.exe"
     - レジストリキー：HKEY_CURRENT_USER¥SOFTWARE¥Microsoft¥Windows ¥CurrentVersion¥Run
6. 以下のファイルをコピーします.
   - ファイル名：自分自身
   - ディレクトリ名：Windows¥All Users¥Start Menu¥Programs¥StartUp
7. 以下のファイルをコピーします.
   - ファイル名：自分自身
   - ディレクトリ名：Documents and Settings¥All Users¥Start Menu¥Programs¥Startup
8. 以下の条件でメールアドレスを検索します.
   以下の拡張子を持つファイルを検索
   - .wab
   - .dbx
   - .htm
   - .html
   - .eml
   - .txt
9. 以下の条件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

   [件名]
   - Your details
   - Approved (Ref: 38446-263)
   - Re: Approved (Ref: 3394-65467)
   - Your password
   - Re: My details
   - Screensaver
   - Cool screensaver
   - Re: Movie
   - Re: My application

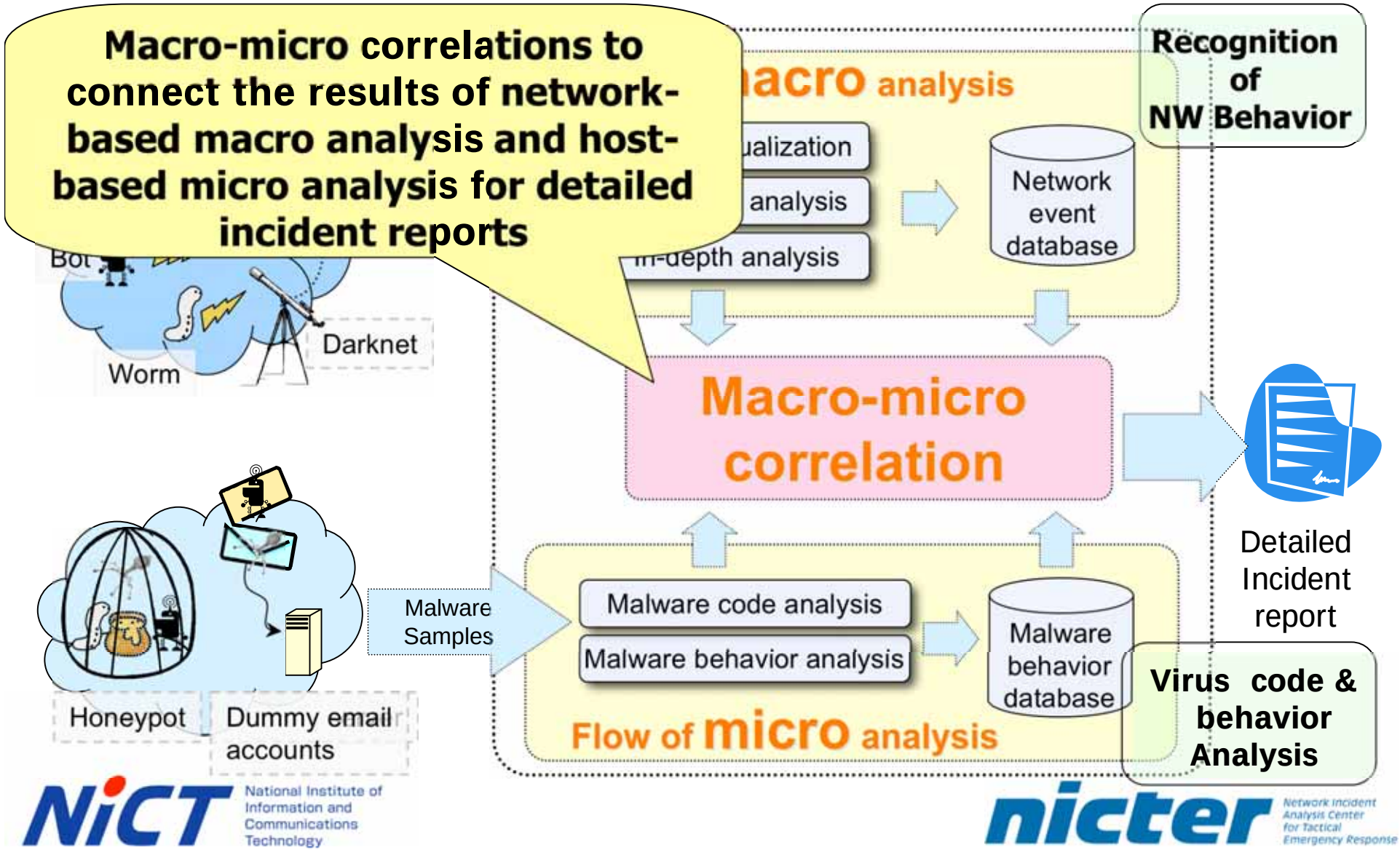
   [本文]
   - All information is in the attached file.

   [添付ファイル]
   - your_details.pif
   - ref-38-1755.pif
   - approved.pif
   - password.pif
   - doc_details.pif
   - screen_temp.pif
   - screen_doc.pif
   - movie28.pif
   - application.pif

   [差出人]
   - support@microsoft.com

Sorry in Japanese.
This is automatically generated within 10min.

Macro-micro correlation



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

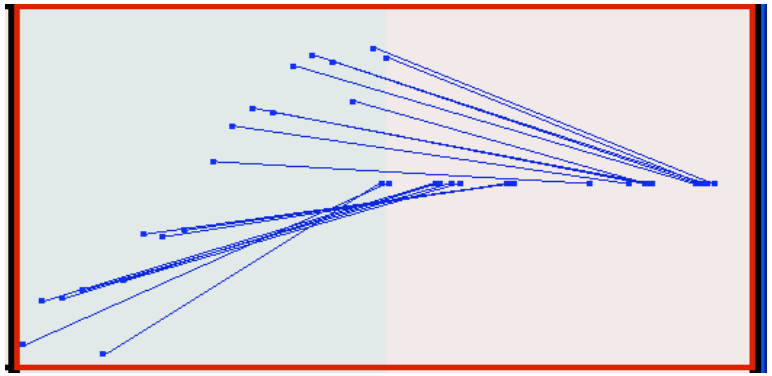
Outputs from the Correlation

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

See an example:

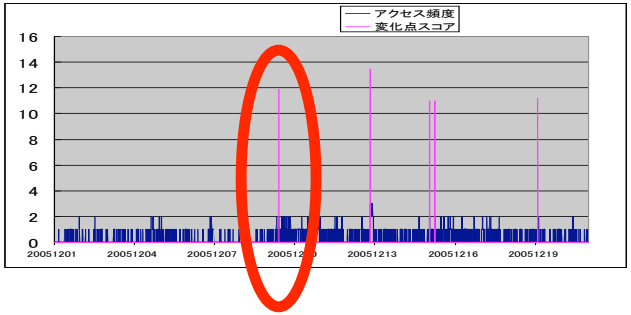
Examples of Macro and Micro Correlation 1/3 (Macro Analysis)

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

Examples of Macro and Micro Correlation 2/3 (Code and Behavior Analysis : Sasser case)

1) Attempts to create a mutex named JumpallsNlsTillt 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

NiCT National Institute of Information and Communications Technology

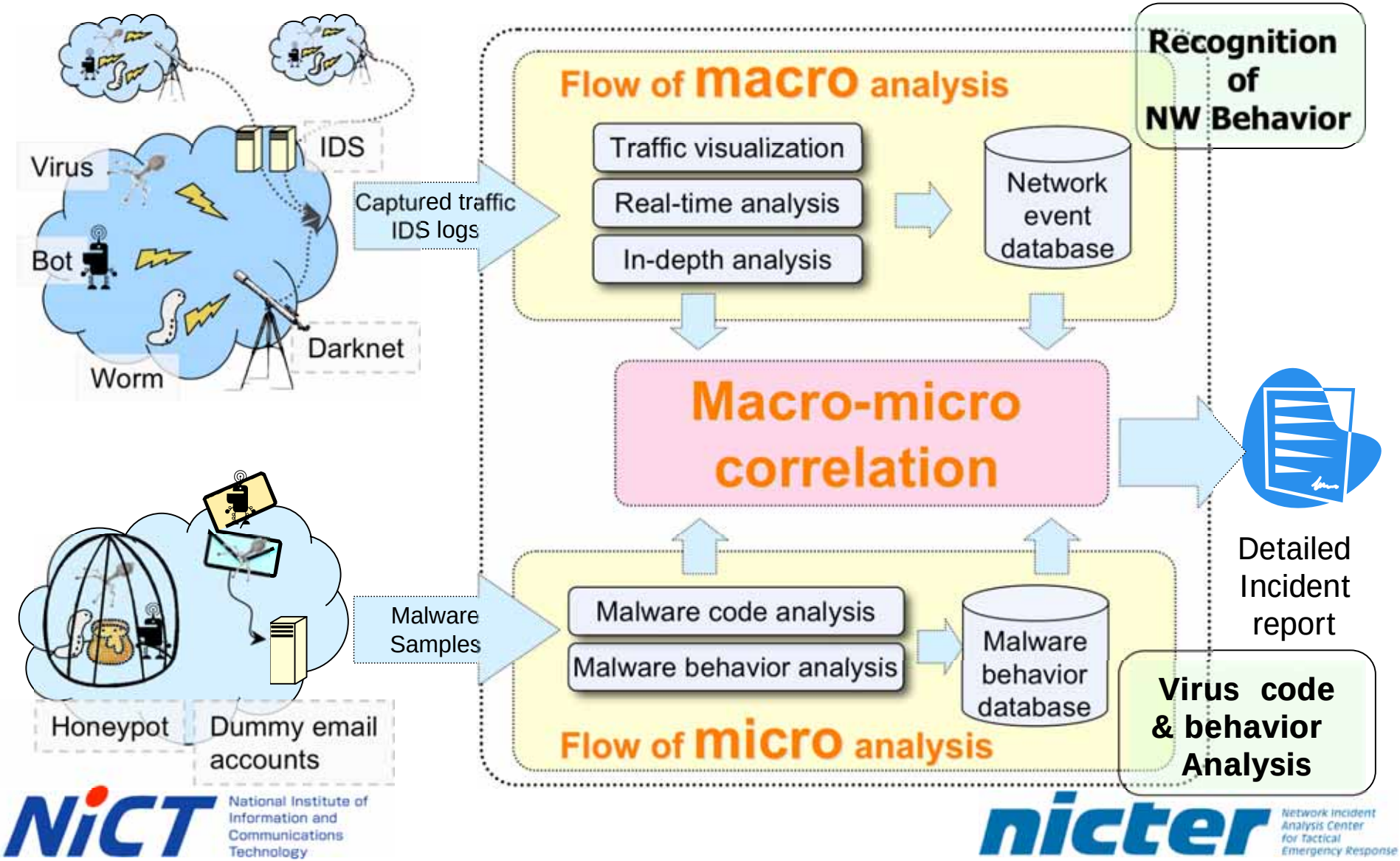
nicter Network Incident Analysis Center for Tactical Emergency Response

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



NiCT National Institute of Information and Communications Technology

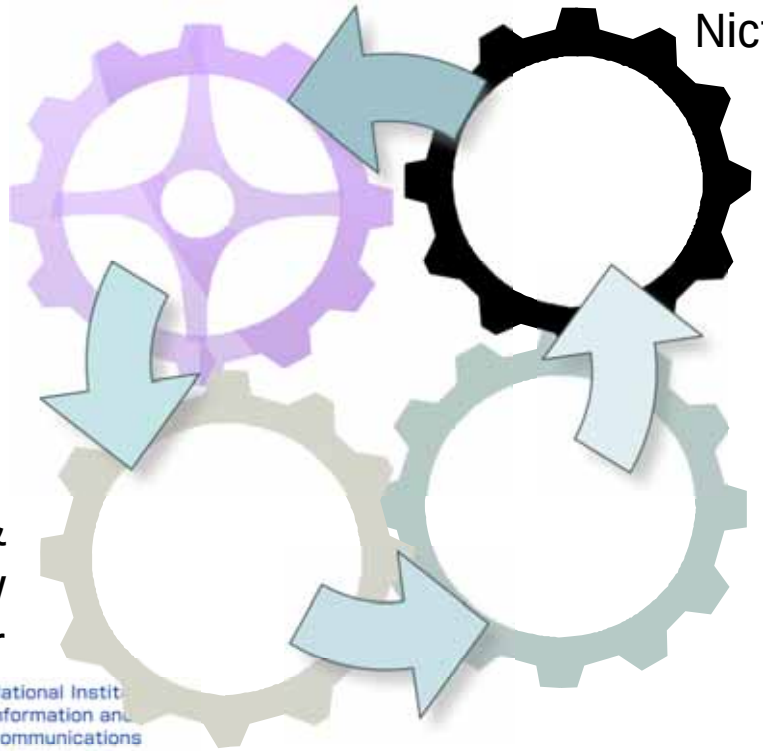
nicter Network Incident Analysis Center for Tactical Emergency Response

Thank you for listening

Q&A

Implement & operate Nicter

Design Nicter



Maintain & improve Nicter

Monitor & review Nicter

NiCT National Institute of Information and Communications Technology

nicter Network Incident Analysis Center for Tactical Emergency Response