Joint Japan-India Workshop on *Cyber Security and Services/Applications for M2M and Fourteenth GISFI Standardization Series Meeting*

How to secure the network - Darknet based cyber-security technologies for global monitoring and analysis

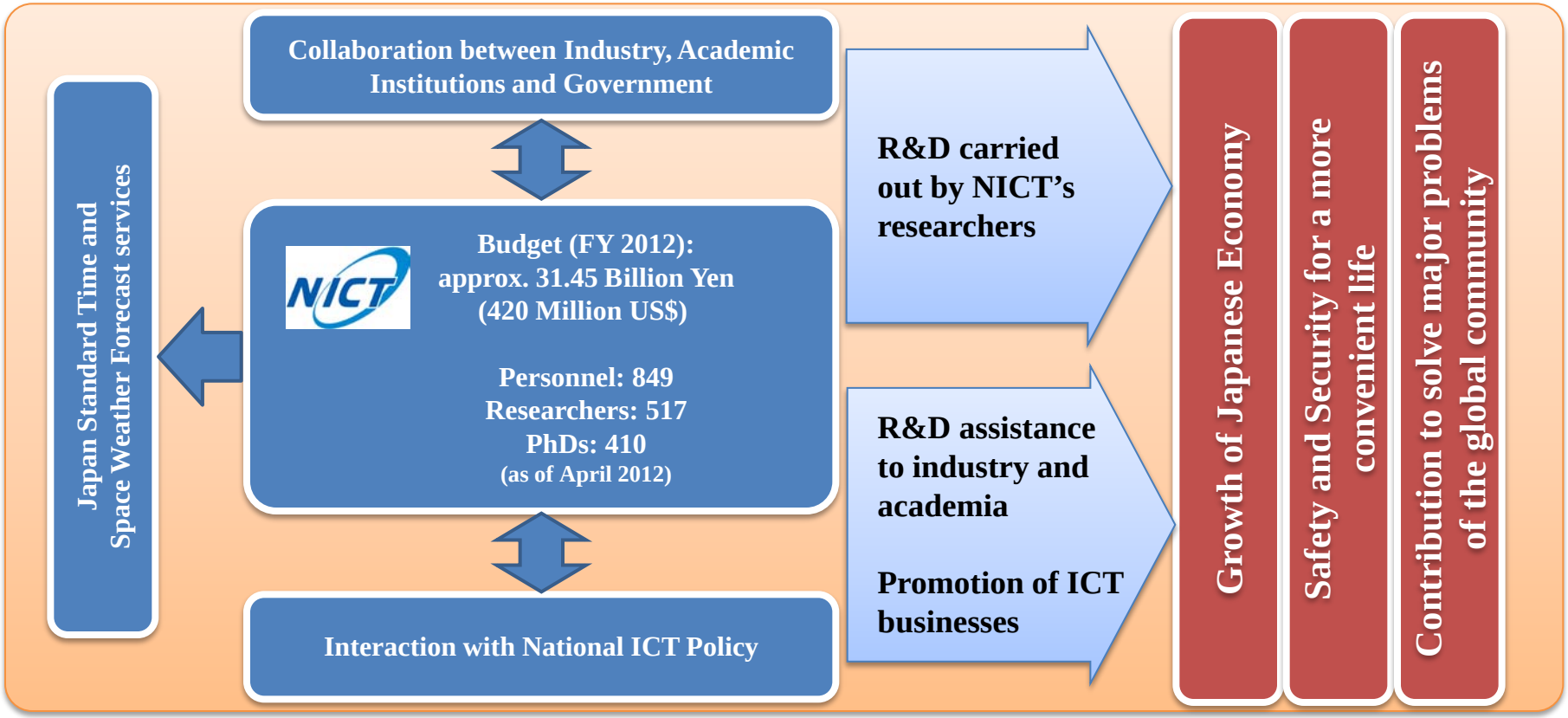
Koji NAKAO

Research Executive Director, Distinguished Researcher, NICT
Information Security Fellow, KDDI

Outline of NICT

Mission

As the sole national research institute in the information and communications field, we as NICT will strive to advance national technologies and contribute to national policies in the field, by promoting our own research and development and by cooperating with and supporting outside parties.



Network Security Research Institute

Collaboration

Security Organizations

- Cyber attack monitoring, tracking, analysis, response and prevention
- Prompt promotion of outcomes

- Dynamic and optimal deployment of security functions
- Secure new generation network design

New Generation Network Security

Cybersecurity Laboratory

Daisuke Inoue

Kazumasa Taira
(Director General)

Security Architecture Laboratory

Koji Nakao
(Distinguished Researcher)

Shin'ichiro Matsuo

Security Fundamentals Laboratory

- Security evaluation of cryptography
- Practical security
- Post quantum cryptography
- Quantum security

Shiho Moriai

Recommendations for Cryptographic Algorithms and Key Lengths to Japan e-Government and SDOs

Content for Today

- Current Security Threats
  (e.g. Malwares/Botnet, DDoS)
- Introduction of ***nicter*** project and others:
  Security Incident Analysis System for Detecting Large-scale Internet Attacks by means of Darknet traffic
  - Macro/Micro-Analysis
  - Macro-Micro Correlation Analysis
  - **DAEDALUS**
  - **NIRVANA**
- On-going new projects for cybersecurity in Japan: PRACTICE

Malware Chronology (1970-2010)

Year	Malware
1970	
1971	Creeper (1st worm)
1972	# The term “virus” first appeared in a SF novel “When HARLIE Was O
1973	
1974	
1975	# The term “worm” first appeared in a SF novel“The Shockwave Rider”
1976	
1977	
1978	
1979	
1980	Xerox PARC Worm
1981	
1982	Elk Cloner(1st virus)
1983	
1984	# Cohen defined virus in his paper “Computer Viruses - Theory and Exp
1985	
1986	Brain (1st IBMPC virus), PC-Write (1st Trojan horse), Virdem
1987	Cascade, Jerusalem, Lehigh, Christmas Tree, MacMag
1988	Byte Bandit, Stoned, Scores, Morris Worm
1989	AIDS(1stransomware), Yankee Doodle, WANK

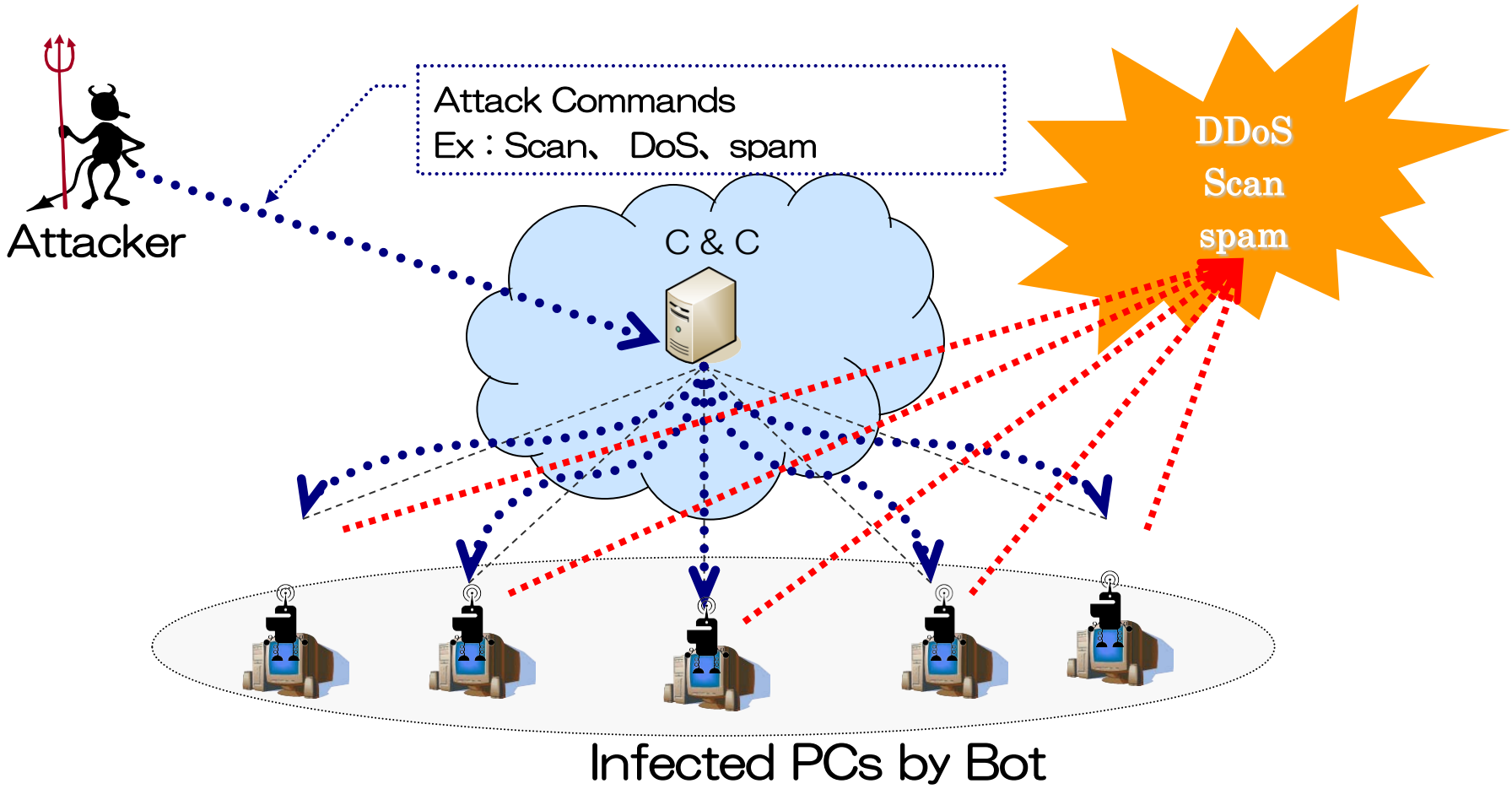
Discovery

Year	Malware
1990	1260 (1st polymorphic virus), Form, Whale
1991	Tequila, Michelangelo, Anti-Telefonica, Eliza
1992	Peach (1st anti-antivirus programs), Win.Vir_1_4 (1st Windows virus)
1993	PMBS
1994	Good Times (1st hoax)
1995	Concept (1st macro virus)
1996	Laroux, Staog (1st Linux m.w.)
1997	ShareFun, Homer, Esperanto
1998	Accessiv, StrangeBrew (1st Java m.w.), Chernobyl
1999	Happy99, Tristate, Melissa, ExploreZip, BubbleBoy, Babylonia
2000	Loveletter, Resume, MTX,Hybris
2001	Anna Kournikova,BadTrans, CodeRed I, Sircam,CodeRed II, Nimda, K
2002	LFM-926 (1st Flash m.w.), Chick, Fbound,Shakira, Bugbear
2003	Sobig, SQLSlammer, Deloder, Sdbot, Mimail, Antinny, MSBlaster, Wel Agobot, Swen, Sober
2004	Bagle, MyDoom, Doomjuice, Netsky,WildJP, Witty,Sasser, Wallon, Bob Cabir(1stSymbianm.w.), Amus, Upchan , Revcuss, Lunii, Minuka, Vund
2005	Bropia, Locknut,BankAsh,Banbra, Anicmoo, Commwarrior, Pgpcoder, Gargafx, Peerload, Cardblock,PSPBrick (1st PSP m.w), DSBrick (1st Nin m.w.), Dasher
2006	Kaiten, Leap (1st Mac OS X m.w.),Redbrowser, Cxover,Exponny, Mdropper,Flexispy, Spaceflash,Stration, Mocbot, Fujacks, Allaple
2007	Storm Worm,Pirlames, Zlob, Srizbi (1st full-kernel m.w.), Silly, Pidief
2008	Mebroot,Infomeiti, Conficker
2009	Virux, Yxes,Gumbler, Induc, Ikee (1stiPhonem.w.)
2010	Zimuse, Trojan-SMS.AndroidOS.FakePlayer (1st Androidm.w.), Stuxnet

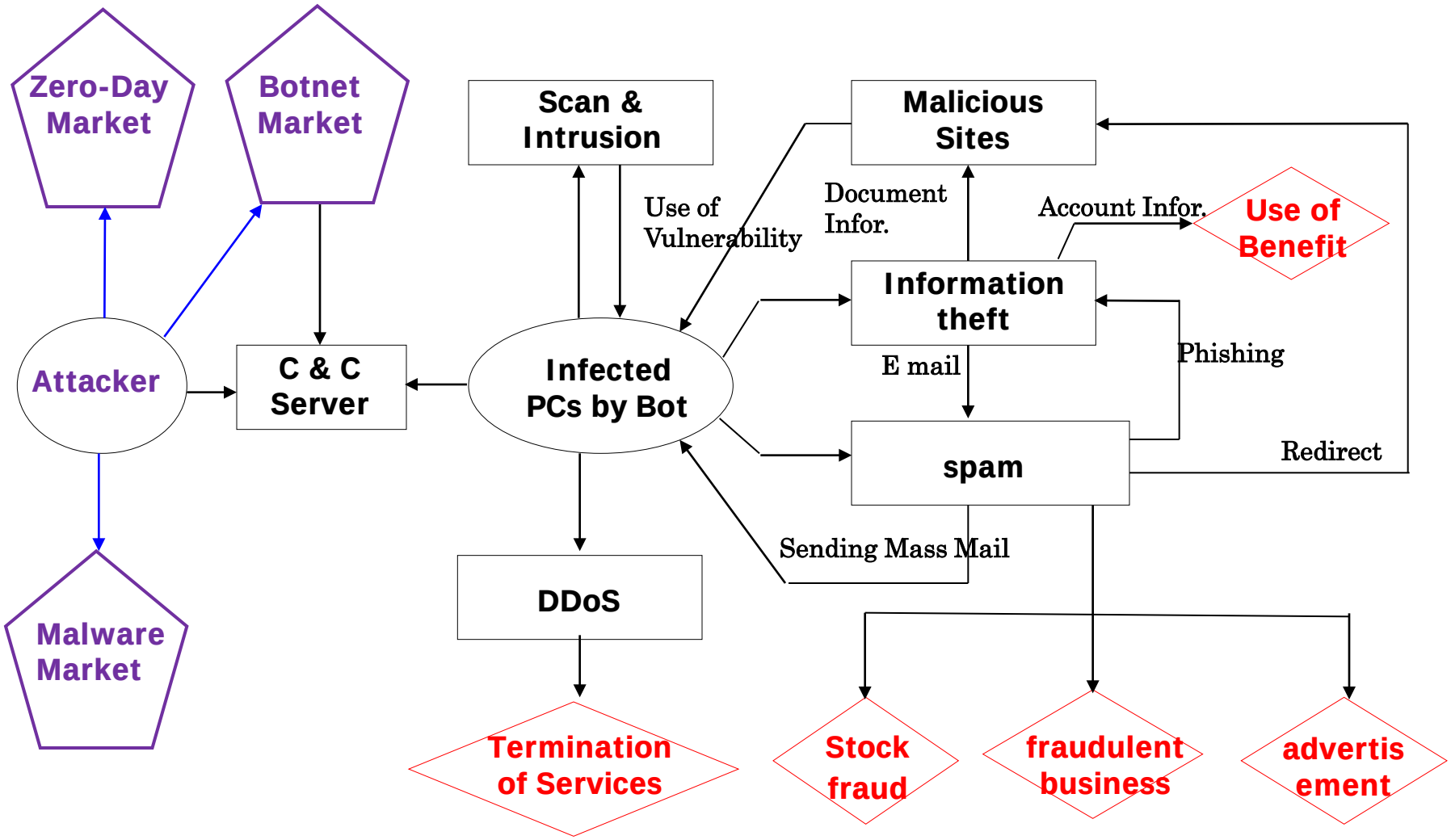
Experimentation

Criminal Exploitation

Botnet (Collaborative attacks)

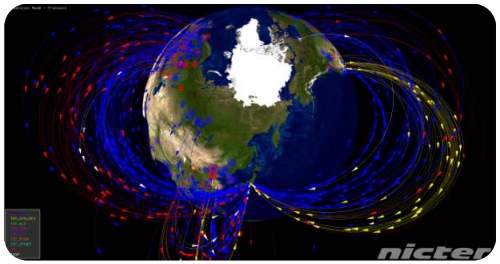


Malicious Chains based on Botnet

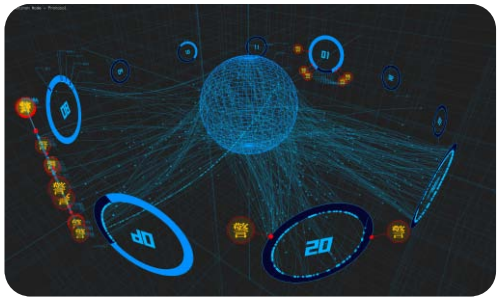


nicter and Its Spin-offs

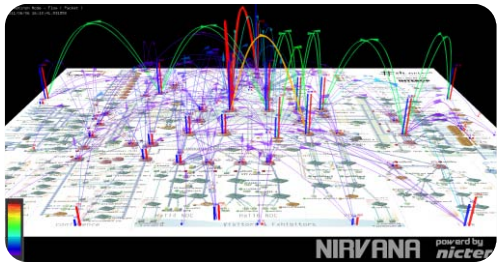
1. Incident analysis system
   nicter



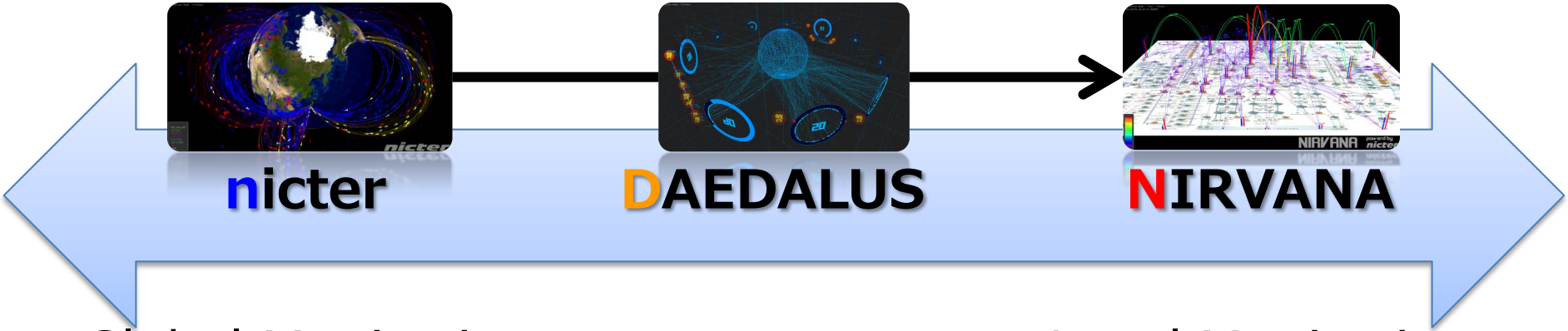
2. Darknet-based alert system
   DAEDALUS



3. Livenet real-time visualizer
   NIRVANA



Bird's-eye View / Insect's-eye View



Global Monitoring
(Darknet)

Local Monitoring
(Livenet)

nicter

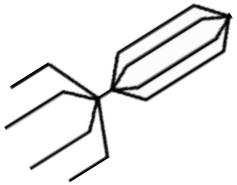
(**N**etwork **I**ncident analysis **C**enter
for Tactical Emergency Response)

What we are fighting against?

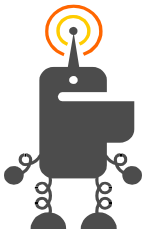
Malware

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)



Virus



Bot

Worm

Overview of the project nicter

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

Target:

Comprehensive analysis of security threats on the Internet

- What happens on the Internet?
- What is the root cause?

Strategy:

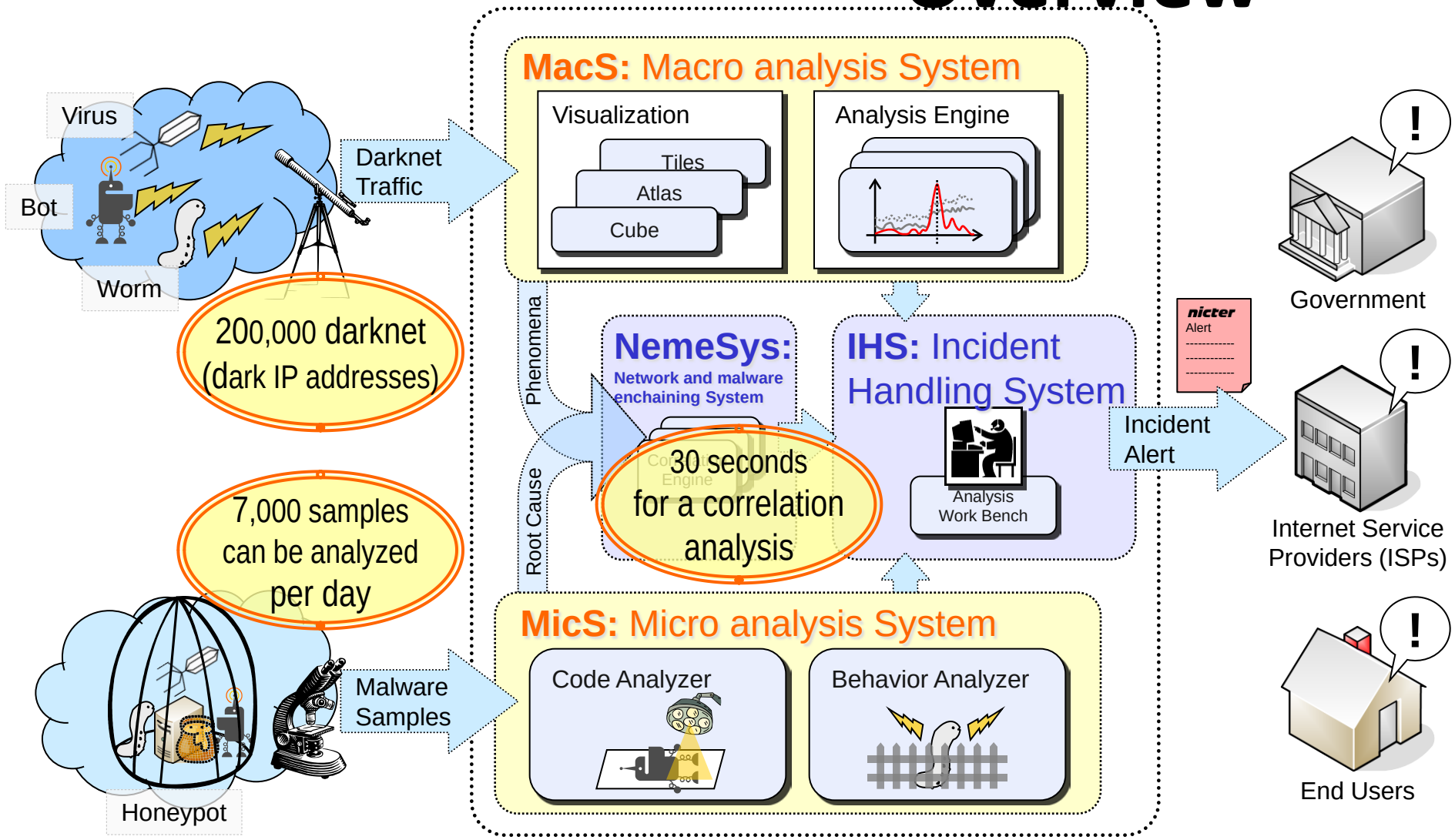
Network monitoring

+

Malware analysis

nicter Operation Room

nicter System Overview



Three Analysis Systems in nicter

Darknet based Analysis

Macro Analysis System (MacS):

- Monitors **Darknet** of over 0.2 million

  Darknet = Globally Announced **Unused** IP Addresses
  (Black-hole address spaces)

- Real-time Detection of Incident Candidates such as:
  - New Attack Patterns of Malwares
  - Rapid Increase of Attacks

Micro Analysis System (MicS):

- Automated Capture and Analysis of Malwares
- Static Analysis and Dynamic Analysis

Network and malware enchaining System (Nemesys):

- Automated Correlation of Darknet Traffic and Malwares

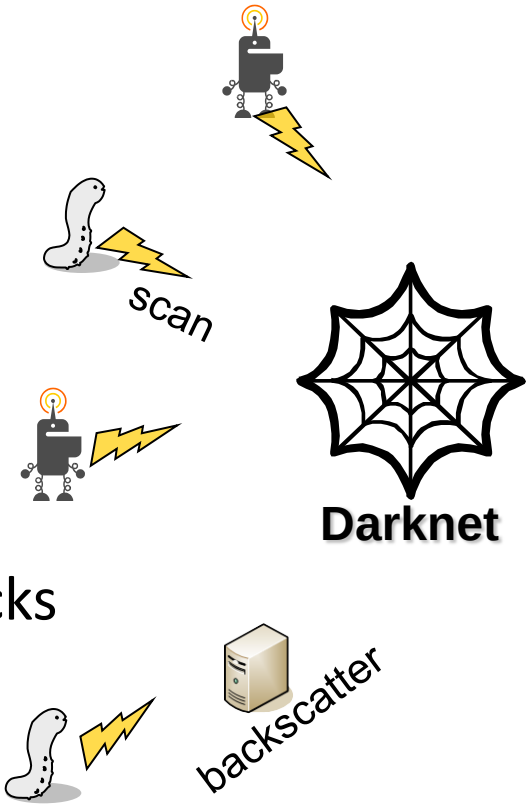
MacS: Macro Analysis System

(Darknet Monitoring and Analysis)

Monitor data through Dark-Net

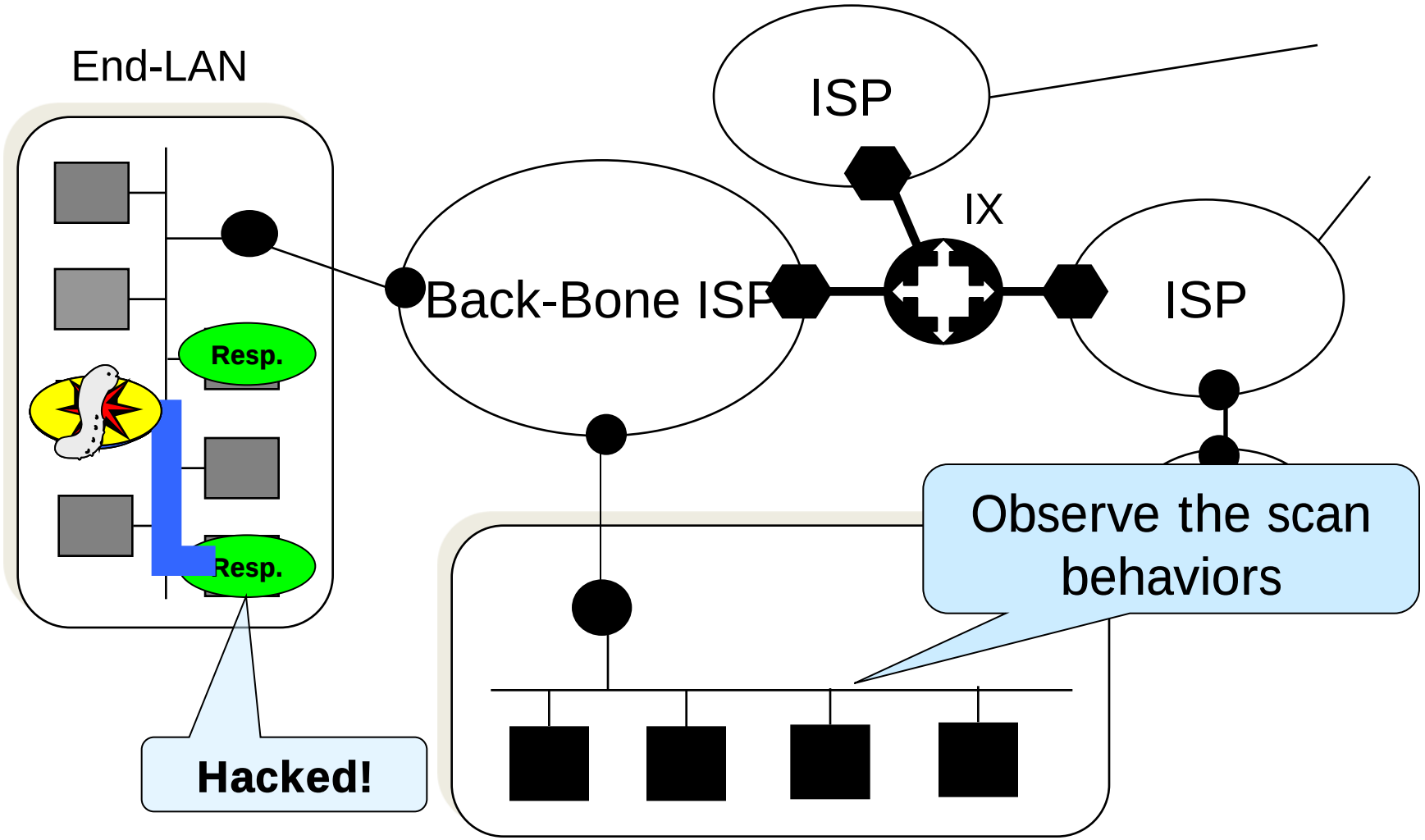
- ***Dark-Net***: Unassigned IP addresses space and they are not connected to the Real Servers/PCs.

- Types of Packets arrived to the Dark-Net:
  - Scans by means of Malwares;
  - Malwares infection behaviors;
  - DDoS attacks by Backscatter;
  - Miss configurations/mistakes



- It is very useful to ***Observe*** the serious attacks behavior over the Internet.

Malware infection behavior by means of Dark-Net monitor



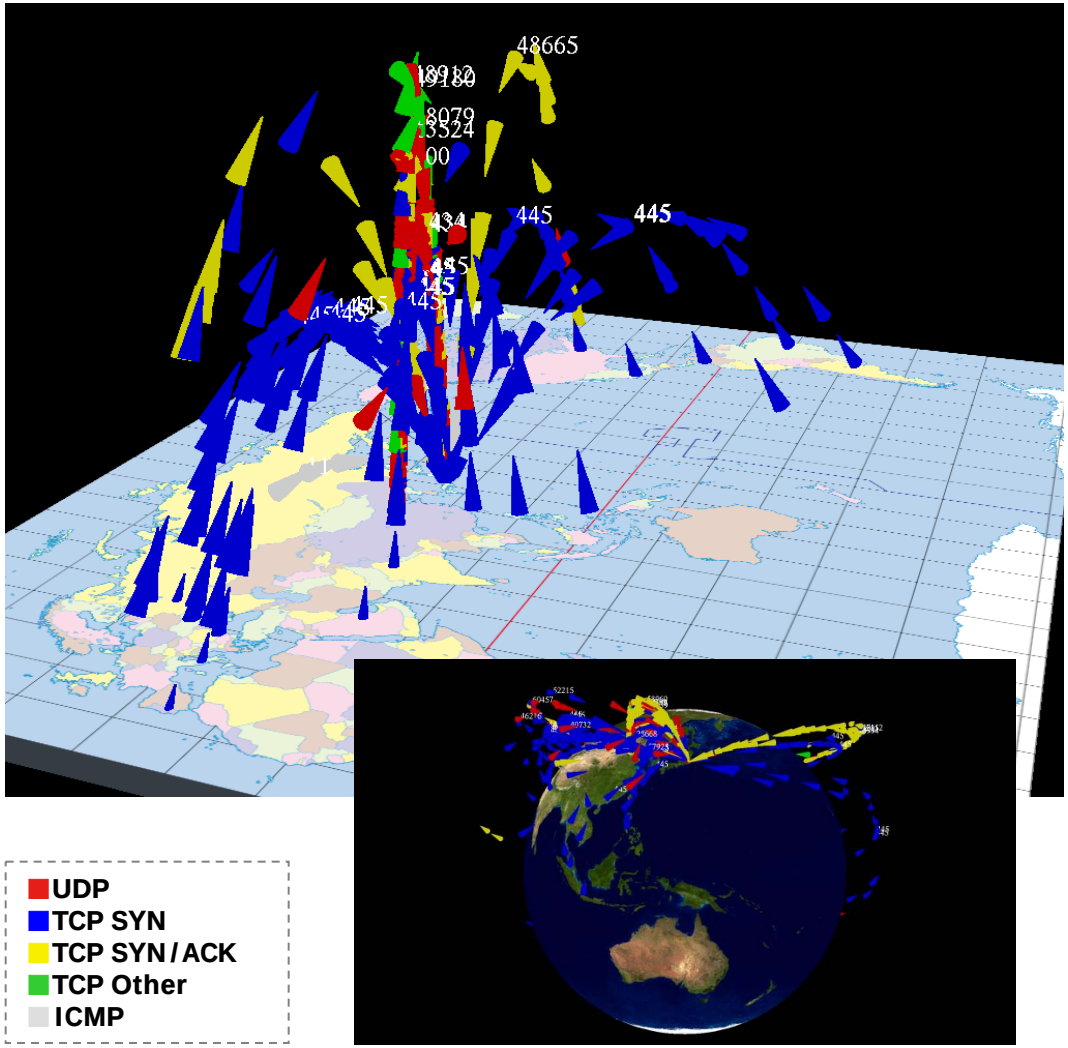
Atlas: Geographical Traffic Visualization

- Shows geographical positions of a packet's src and dst from the IP addresses **in real-time**

- **Each packet** is represented by **a rocket** traversing from source to destination

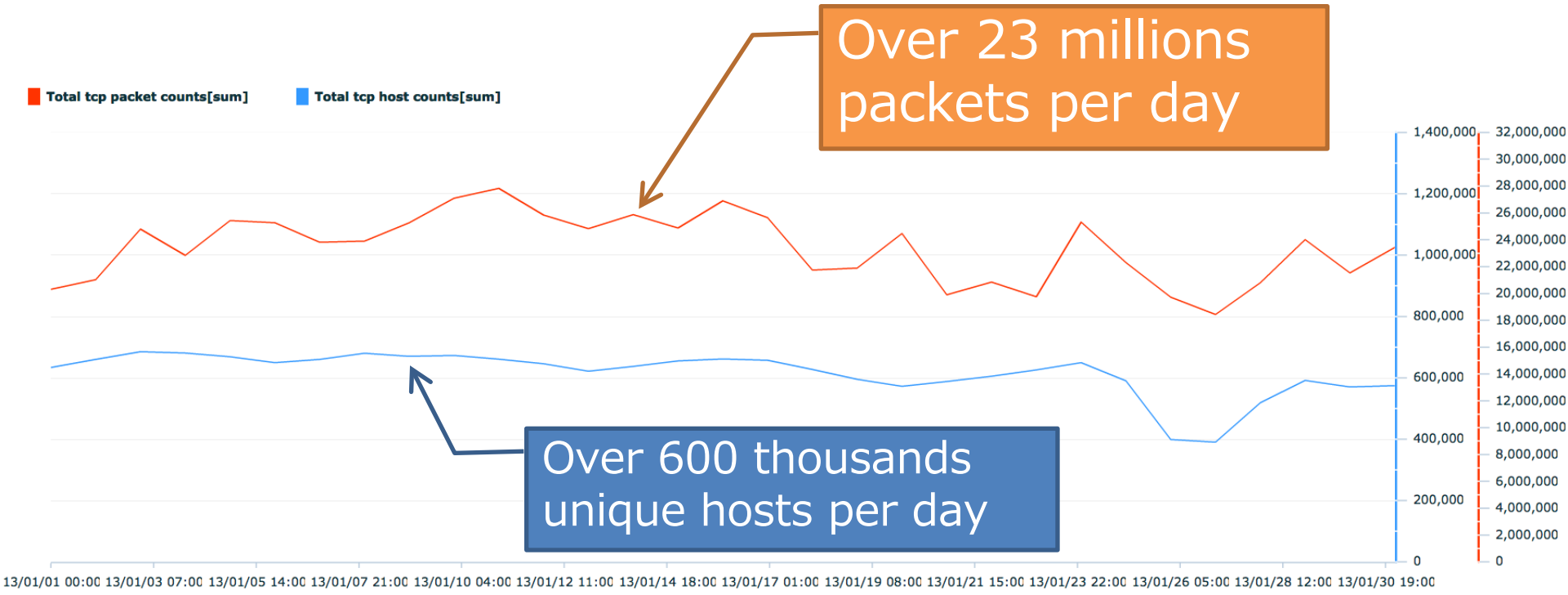
- The **color** of the rocket indicates the type of packet

- The **altitude** of the rocket is in proportion to its dst port number



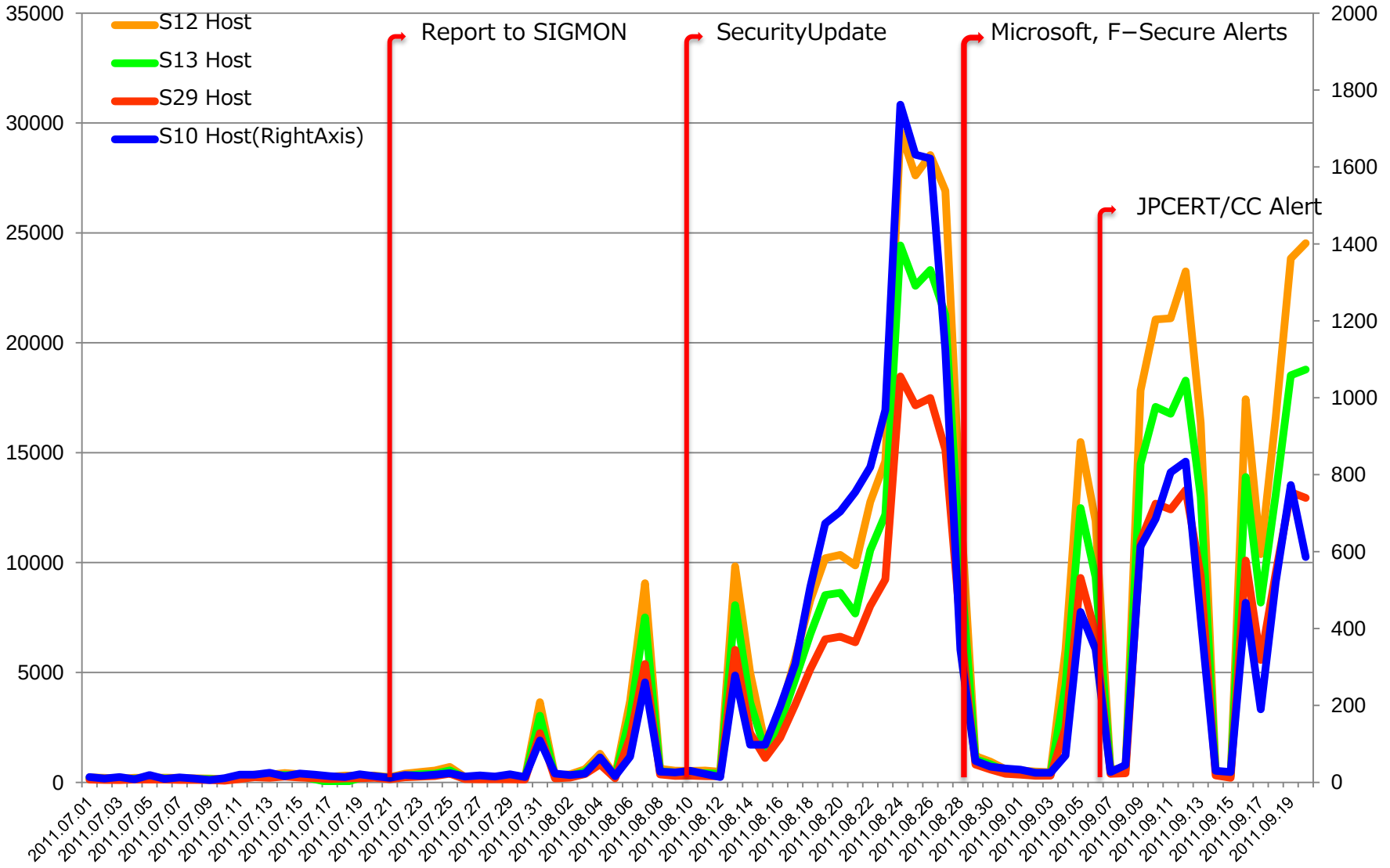
2012 | Bot | US& China

Daily Status of Darknet Traffic

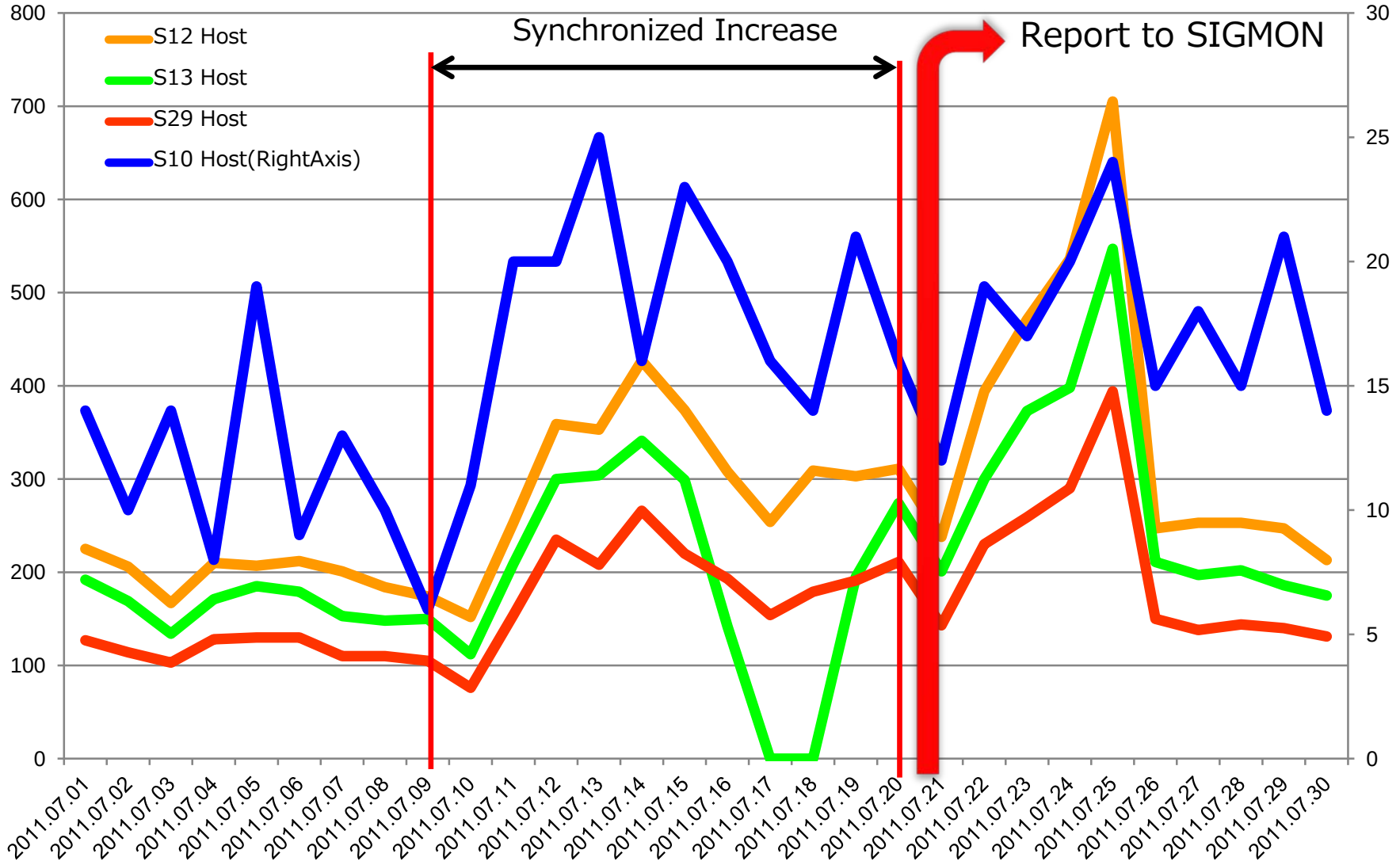


Jan 01 – Jan 31, 2013

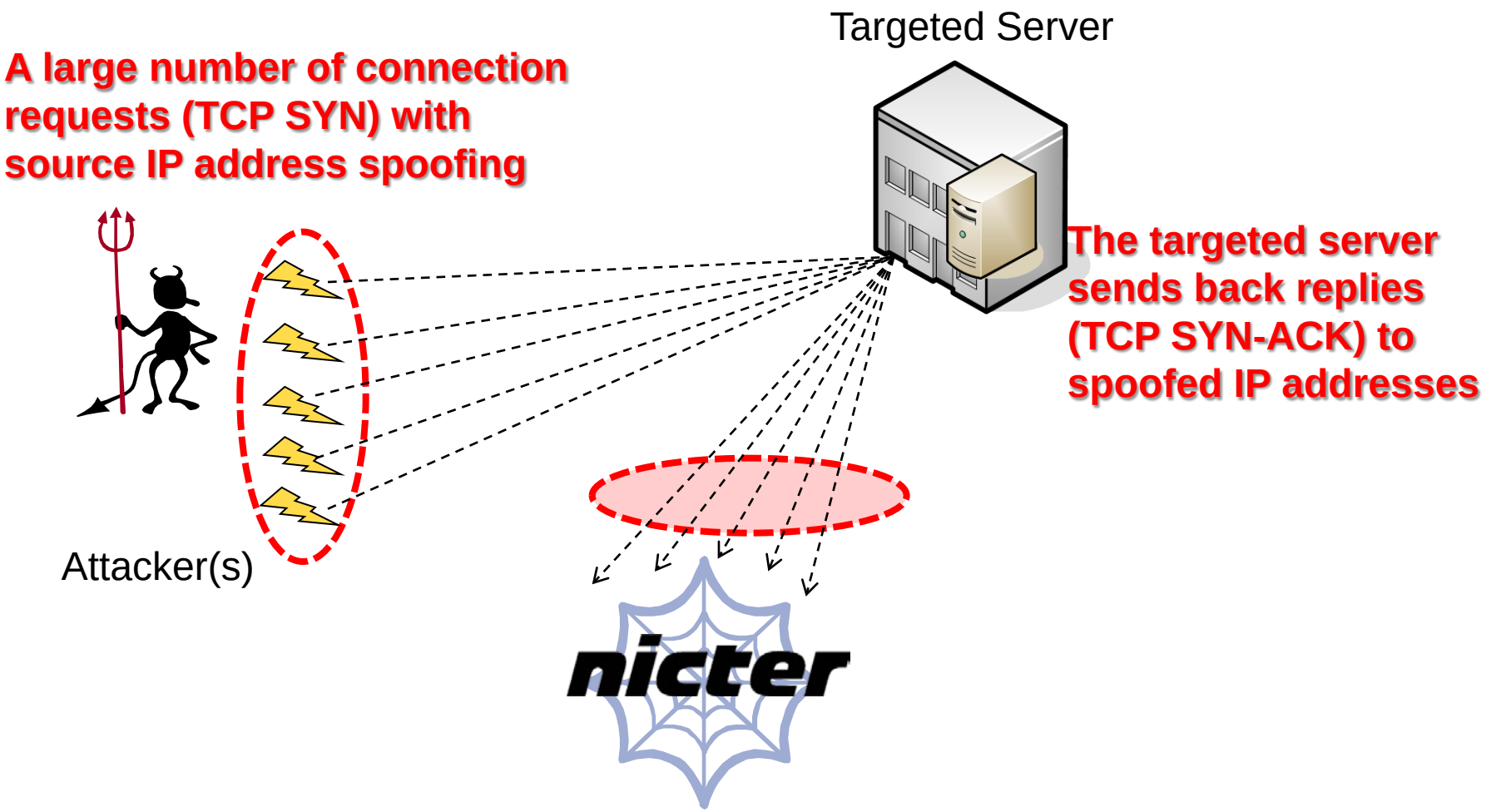
Observing 3389/tcp in dark-net



Observing 3389/tcp in dark-net (Zoom-up)



Backscatter: Reflection of DDoS Attack



Large Scale of Information Leakage: **Sony**

- Incident that individual information on 100 million totals or more flows out from online services of Sony group. The impact of the individual information leakage incident is a worst-ever scale.
- Before such a large information leakage, subsidiary companies of Sony were attacked by DDoS.
  Attacker was **"Anonymous"** hacker group. Sony's behaviors (claiming to a federal district court) bought the anger of "Anonymous".
- After DDoS, the system was hacked and the incident was occurred.

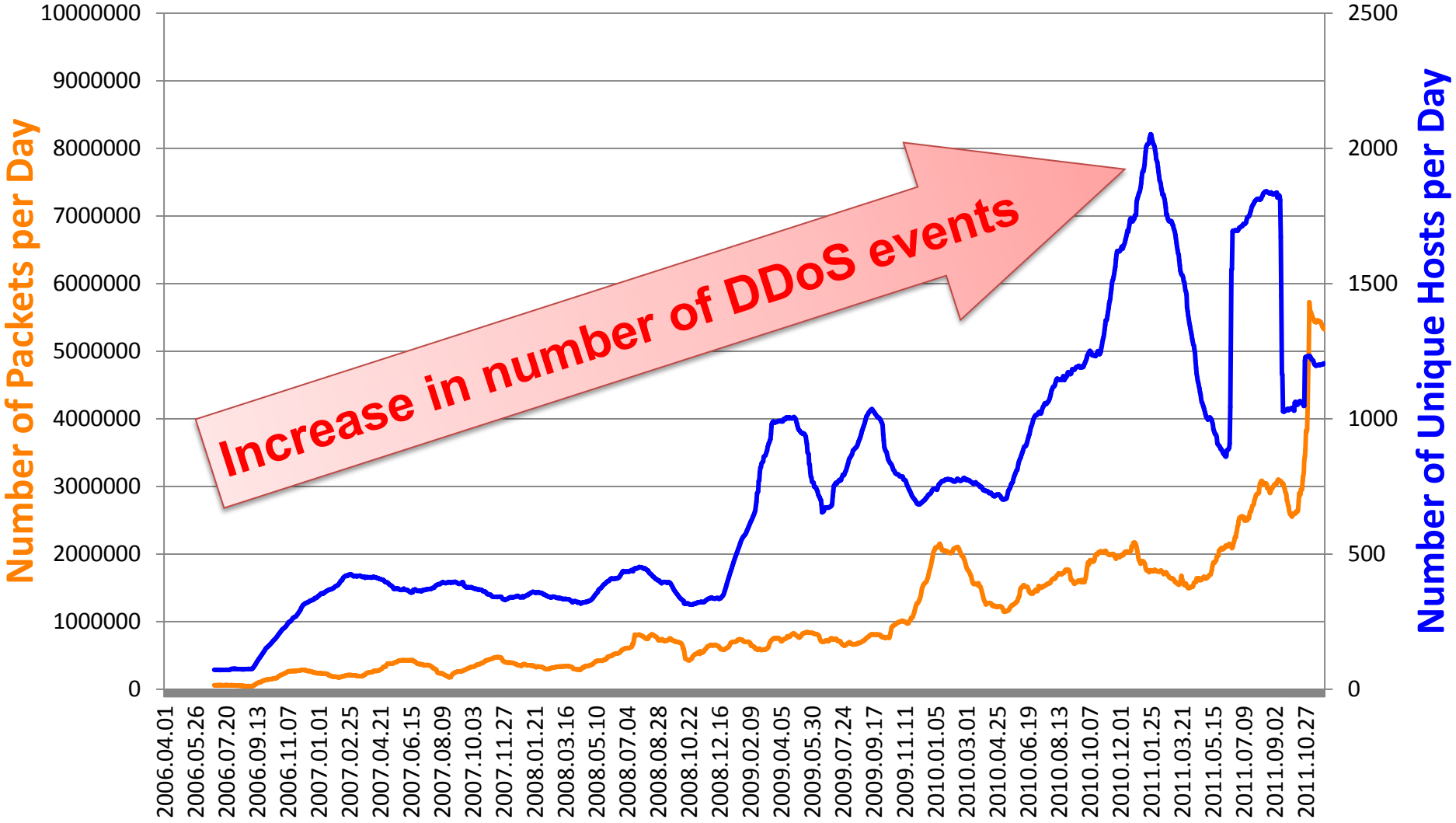
Backscatter from SONY

- Attacked by Anonymous on April 2011 -

Sony

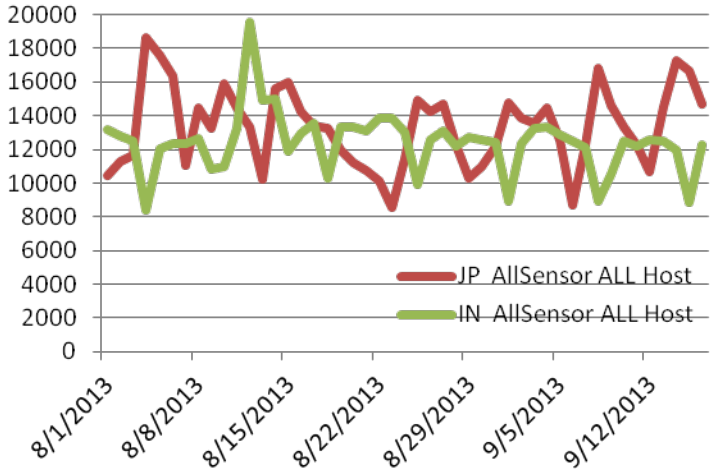
Anonymous

Long-term Observation of Backscatter

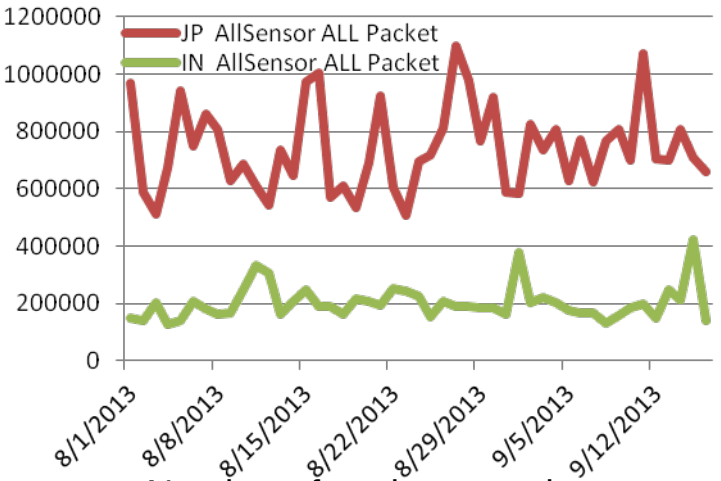


General Statistics observed in Dark-net at NICT (for India)

- Observed
  - in all sensors (sum)
  - 1, Aug ~ 16, Sep (47days)
  - From India to NICT dark-net
    - 12,401 unique hosts/day (avg)
    - 201,274 packets/day (avg)
  - From Japan to NICT dark-net
    - 13,317 unique hosts/day (avg)
    - 741,189 packets/day (avg)



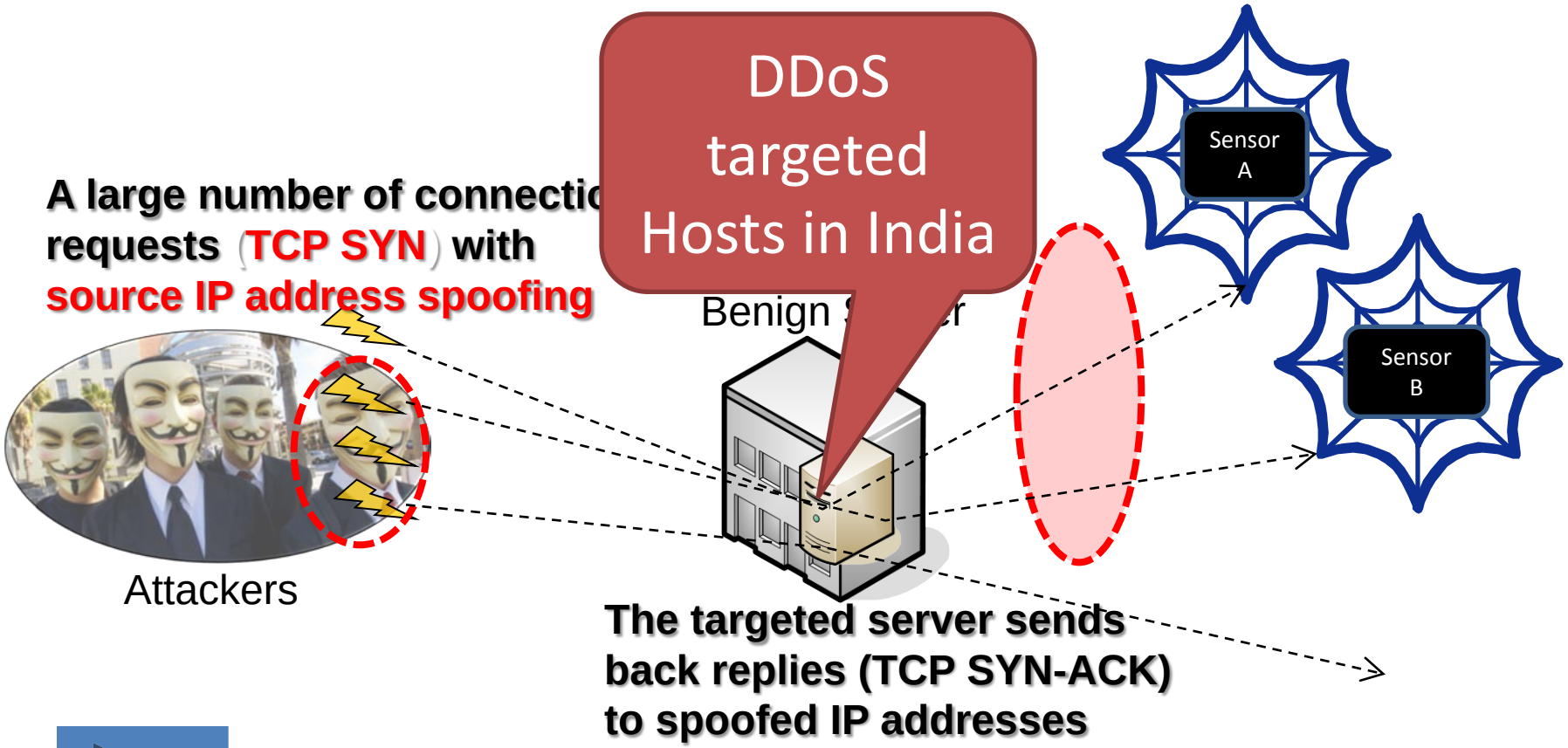
Number of unique source hosts per day



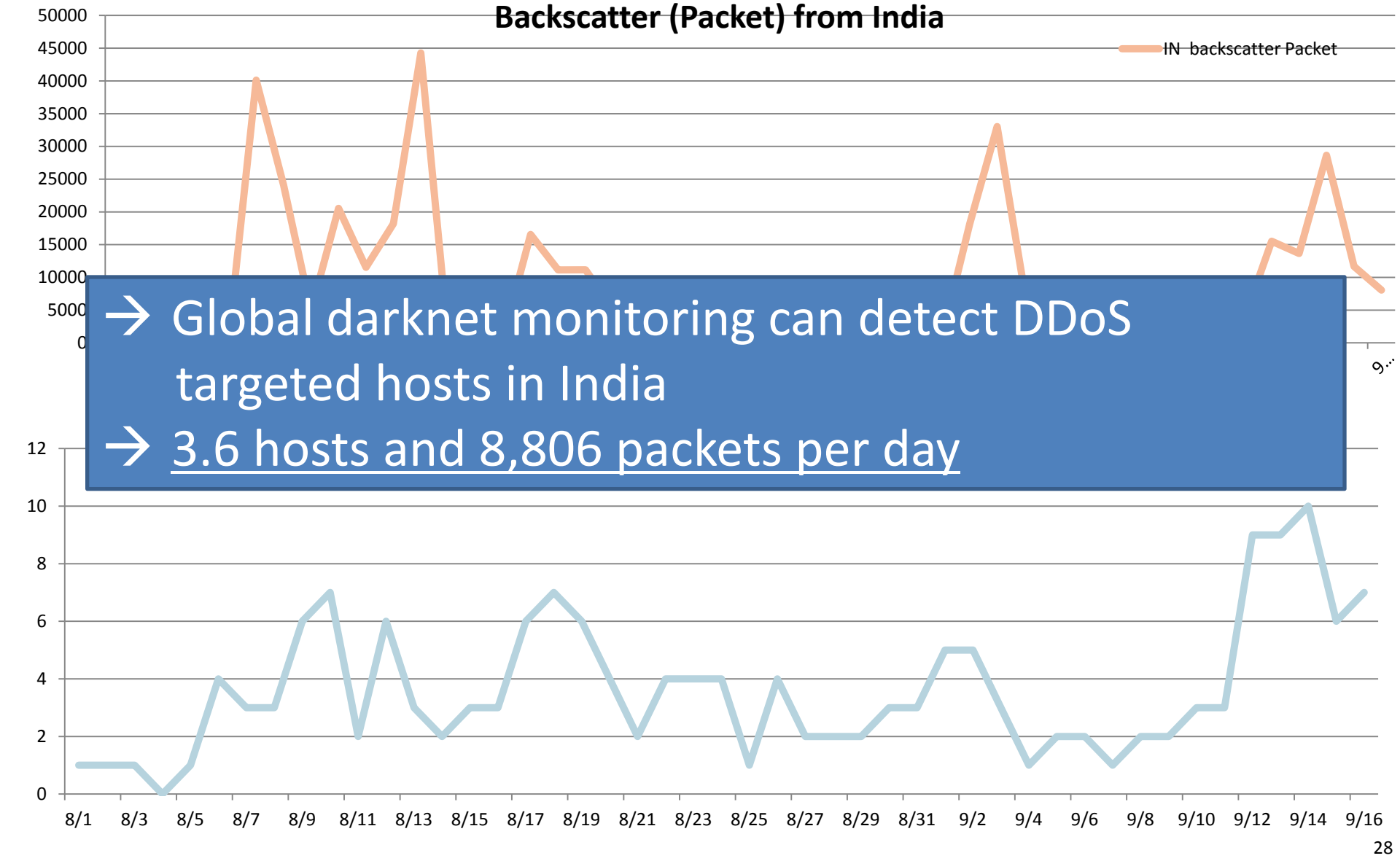
Number of packets per day

India

Backscatter Analysis (1) focusing on India



Backscatter Analysis (2)



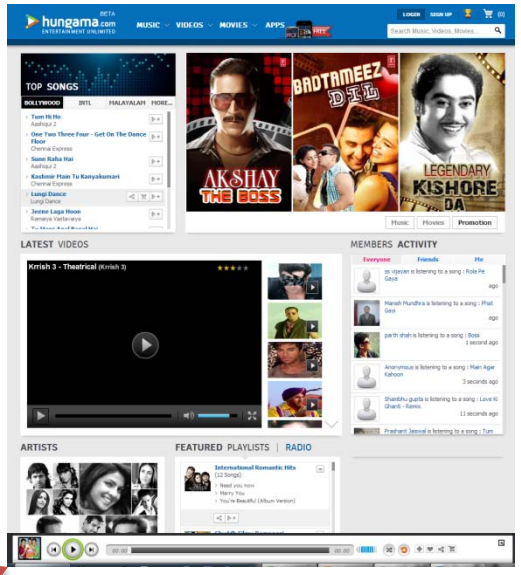
→ Global darknet monitoring can detect DDoS targeted hosts in India

→ 3.6 hosts and 8,806 packets per day

Backscatter Analysis (3)

- What kind of hosts were under the DDoS attacks?

59.165.131.33.man-static.vsnl.net.in.
triband-del-59.177.88.236.bol.net.in.
mail.sysconinfoway.com.
8-239-2-103.mysipl.com.
mum-46.fknet.flipkart.com.
111servers.com.
www.go4hosting.com.
unknown.xeex.net.
mail14.amitip.com.
115.114.191.203.static-Mumbai.vsnl.net.in.
ABTS-North-Static-217.33.160.122.airtelbroadband.in.
ABTS-North-Dynamic-233.166.162.122.airtelbroadband.in.
ABTS-TN-dynamic-143.102.174.122.airtelbroadband.in.
ws38-227-252-122.rcil.gov.in.
19-243-201-123.static.youbroadband.in.
segment-124-7.sify.net.
nicnet.nic.in.
ns1.nic.in.
nitpuguwa.nic.in.
hungama.com.
archive.gtlinfra.com.
archive.epalindia.com.
archive.gtllimited.com.
archive.globalproserv.com.
archive.globalruralnetco.com.
archive.educationforpeace.in.
pop.ghc.in.
:



hungama.com

Cube: 3D Traffic Visualization

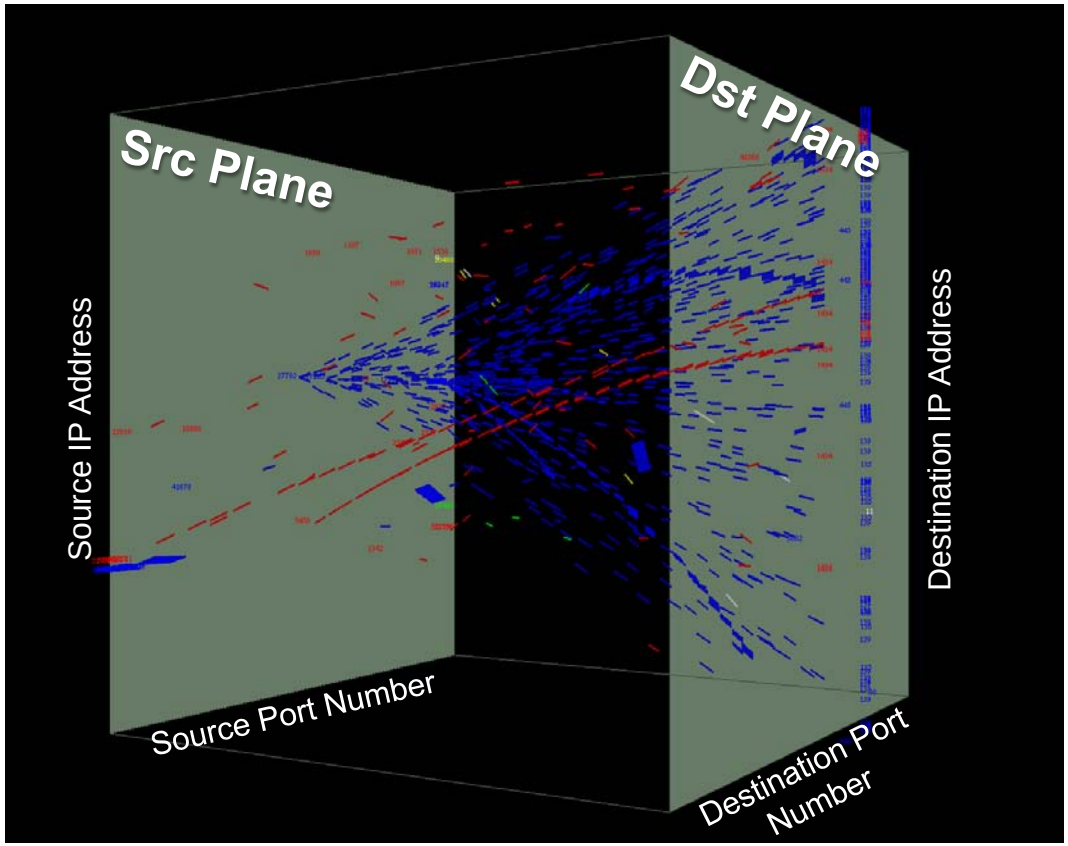
• Shows comprehensive traffic animation **in real-time**

•**Each packet** is represented by **a thin rectangle**

• The rectangle is placed on the source plane according to its **src IP addr and port number**

• It glides to the destination plane taking about six seconds

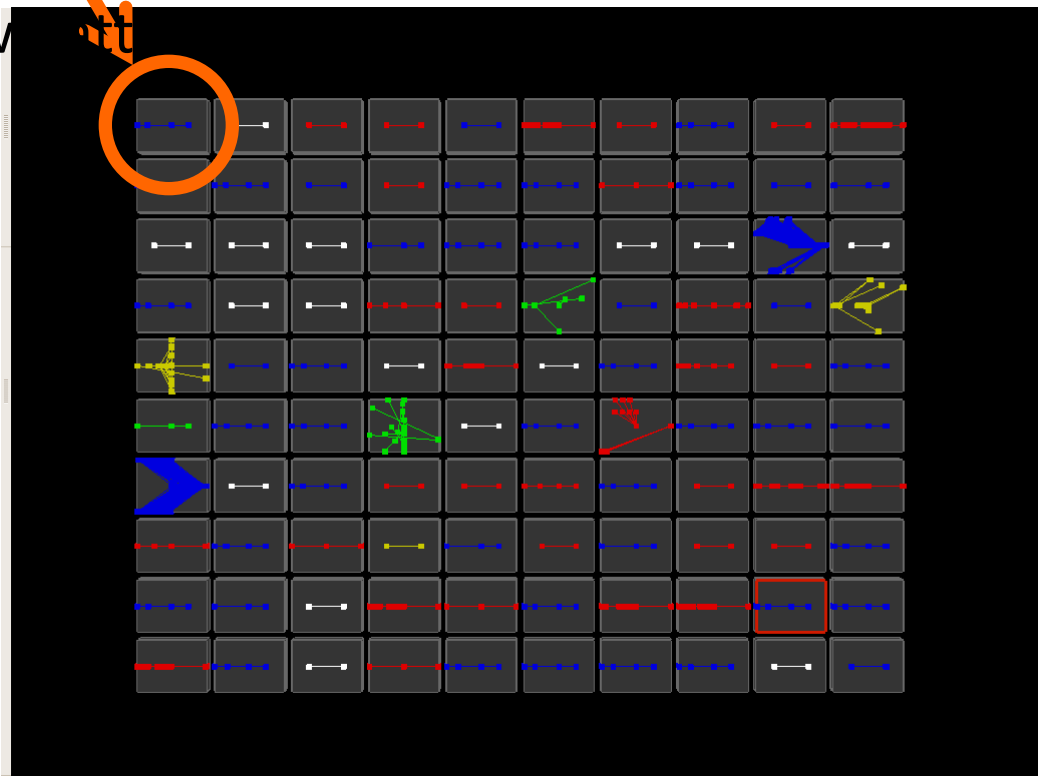
•The position it reaches is according to its **dst IP addr and port number**



Tiles:

Host-based Behavioral Analysis Engine

- One ***tile*** illustrates behavior of an attacking host in 30 sec.
- Each behavior is automatically categorized and stored in a DB.
- Unknow[illegible]tt



Tiles

MicS: Micro Analysis System

(Fully Automated and Isolated Malware Analysis)

Goals and Current Status of MicS

Goals:

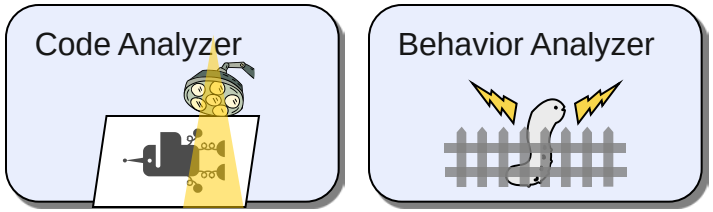
- Fully automated and isolated analysis environment
- Extract malware's internal and external activities

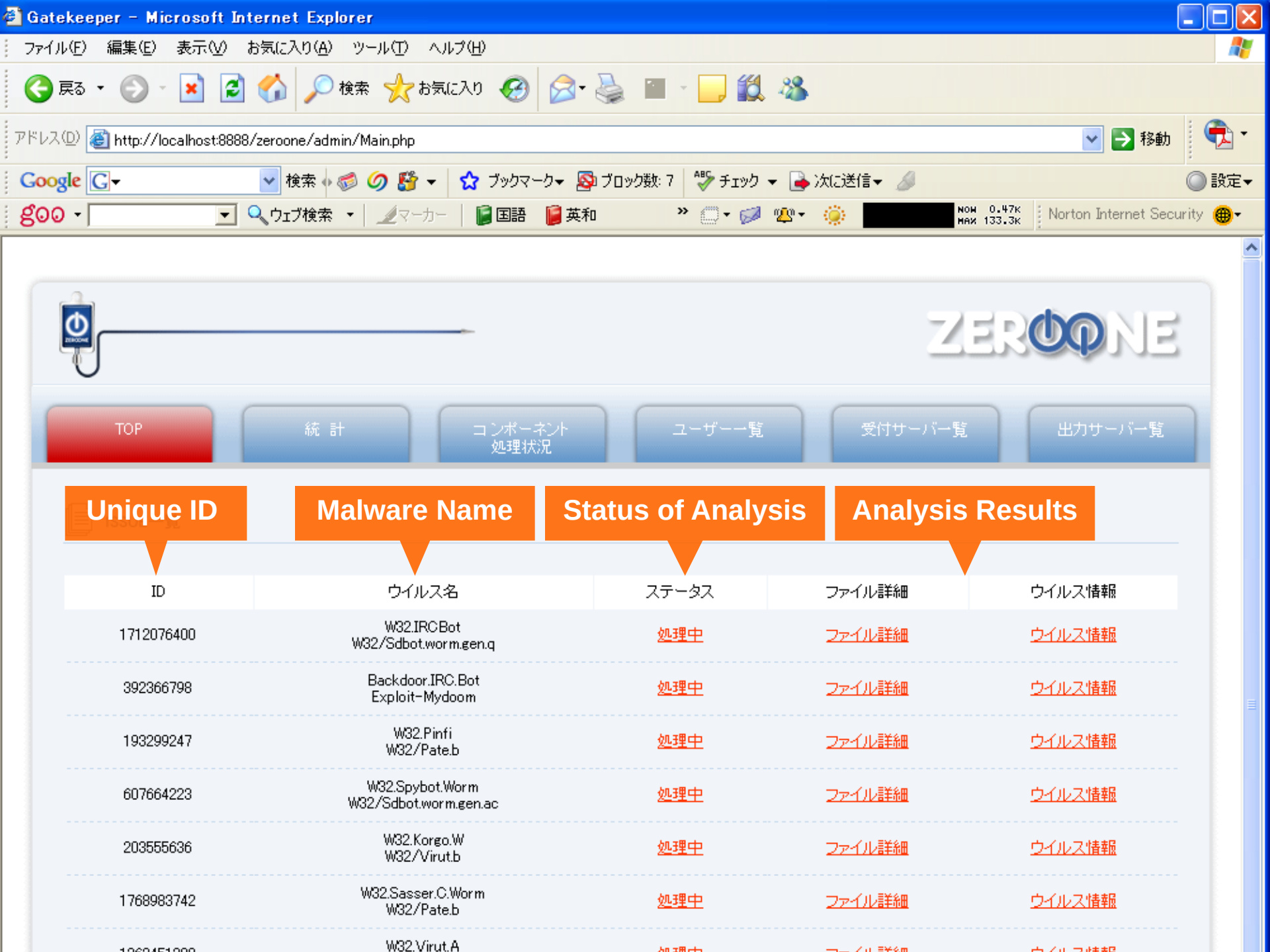
Current Achievements:

- Fully-automated malware analysis system
  - flexible to add new analysis engine
- 6 to 10 minutes per one malware sample
  - totally 1200 to 2000 samples per day

Two Analyzers:

- Malware Code Analyzer
- Malware Behavior Analyzer




Gatekeeper - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る 検索 お気に入り
アドレス(D) http://localhost:8888/zeroone/admin/Main.php
移動
Google 検索 ブックマーク ブロック数: 7 チェック 次に送信 設定
goo ウェブ検索 マーカー 国語 英和
Norton Internet Security
ZERO ONE
TOP
統 計
コンポーネント処理状況
ユーザー一覧
受付サーバー覧
出力サーバー覧
Unique ID
Malware Name
Status of Analysis
Analysis Results
ID
ウイルス名
ステータス
ファイル詳細
ウイルス情報
1712076400
W32.IRCBot
W32/Sdbot.worm.gen.q
処理中
ファイル詳細
ウイルス情報
392366798
Backdoor.IRC.Bot
Exploit-Mydoom
処理中
ファイル詳細
ウイルス情報
193299247
W32.Pinfi
W32/Pate.b
処理中
ファイル詳細
ウイルス情報
607664223
W32.Spybot.Worm
W32/Sdbot.worm.gen.ac
処理中
ファイル詳細
ウイルス情報
203555636
W32.Korgo.W
W32/Virut.b
処理中
ファイル詳細
ウイルス情報
1768983742
W32.Sasser.C.Worm
W32/Pate.b
処理中
ファイル詳細
ウイルス情報
W32.Virut.A

NemeSys: Network and malware enchaining System

(Macro-Micro Correlation Analysis)

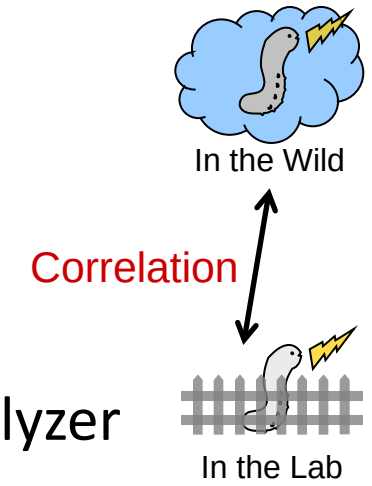
NemeSys Overview

Goal:

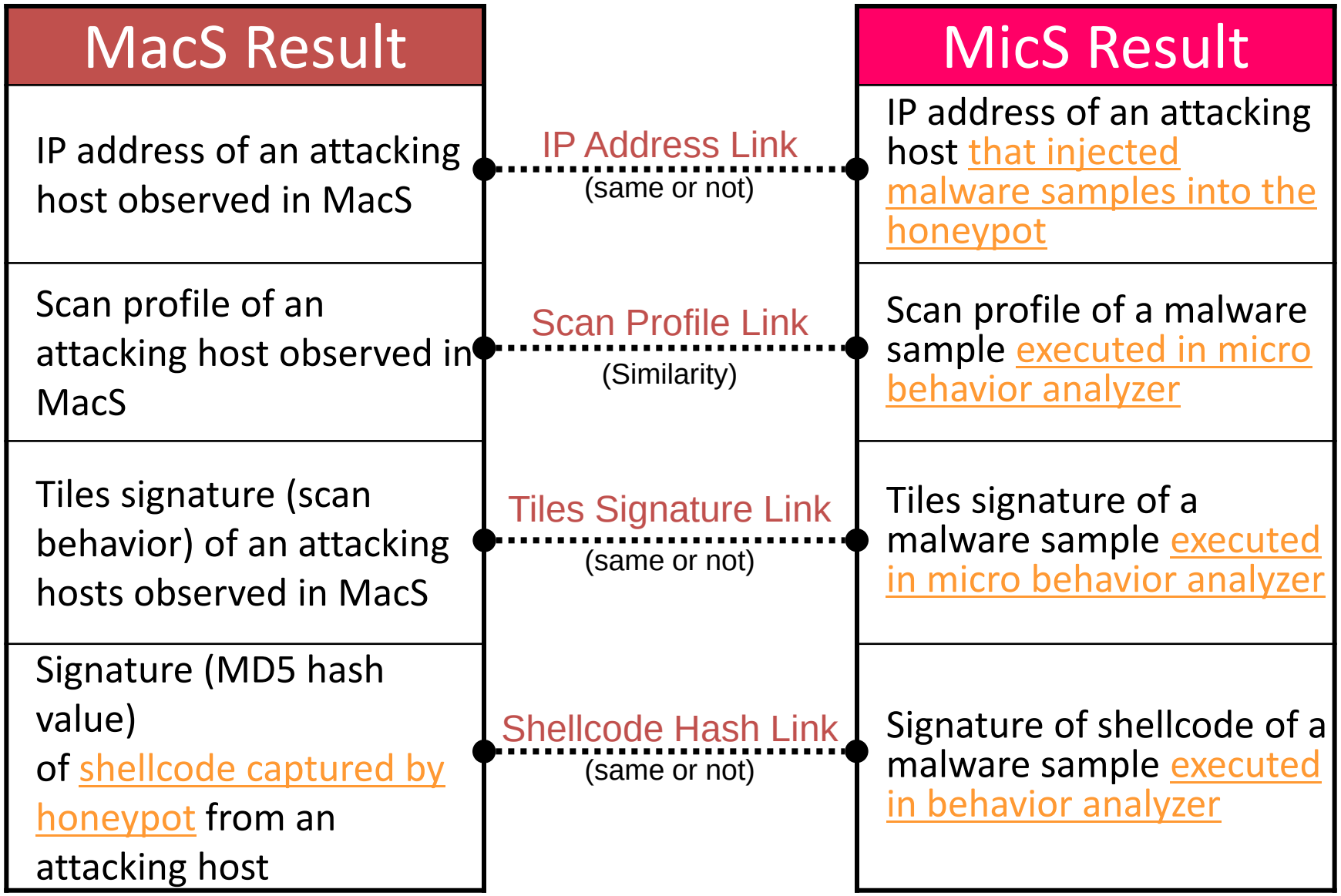
To bind phenomena (attacks) observed by the MacS and root cause(malwares) inspected in the MicS

Basic Idea (scan based correlation):

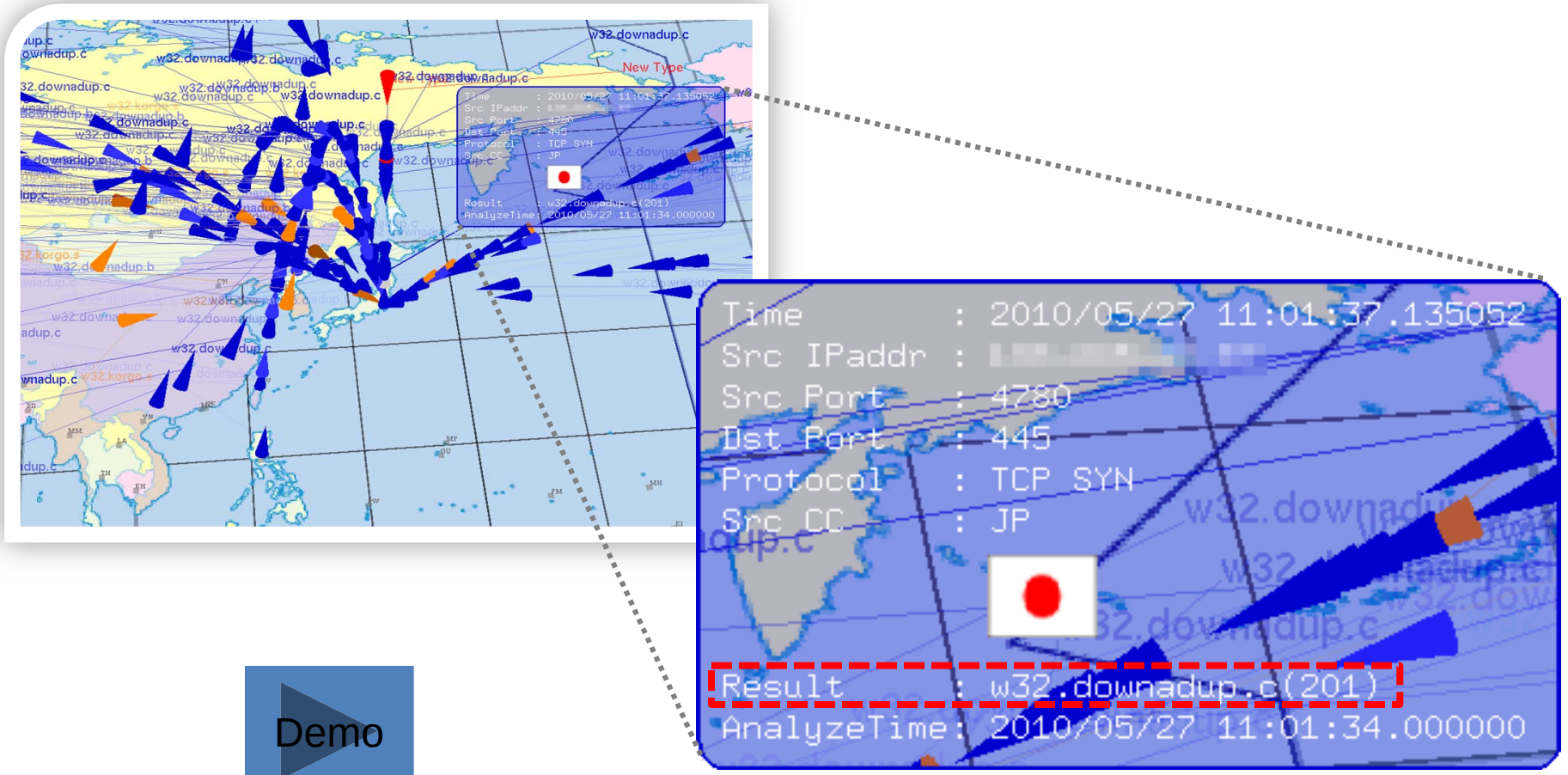
- MacS: Profiling scan sent by a certain host
- MicS: Profiling scan captured in the behavior analyzer
- Compare scan profiles by using correlation coefficient then candidates of infecting malware can be listed



Correlation Links

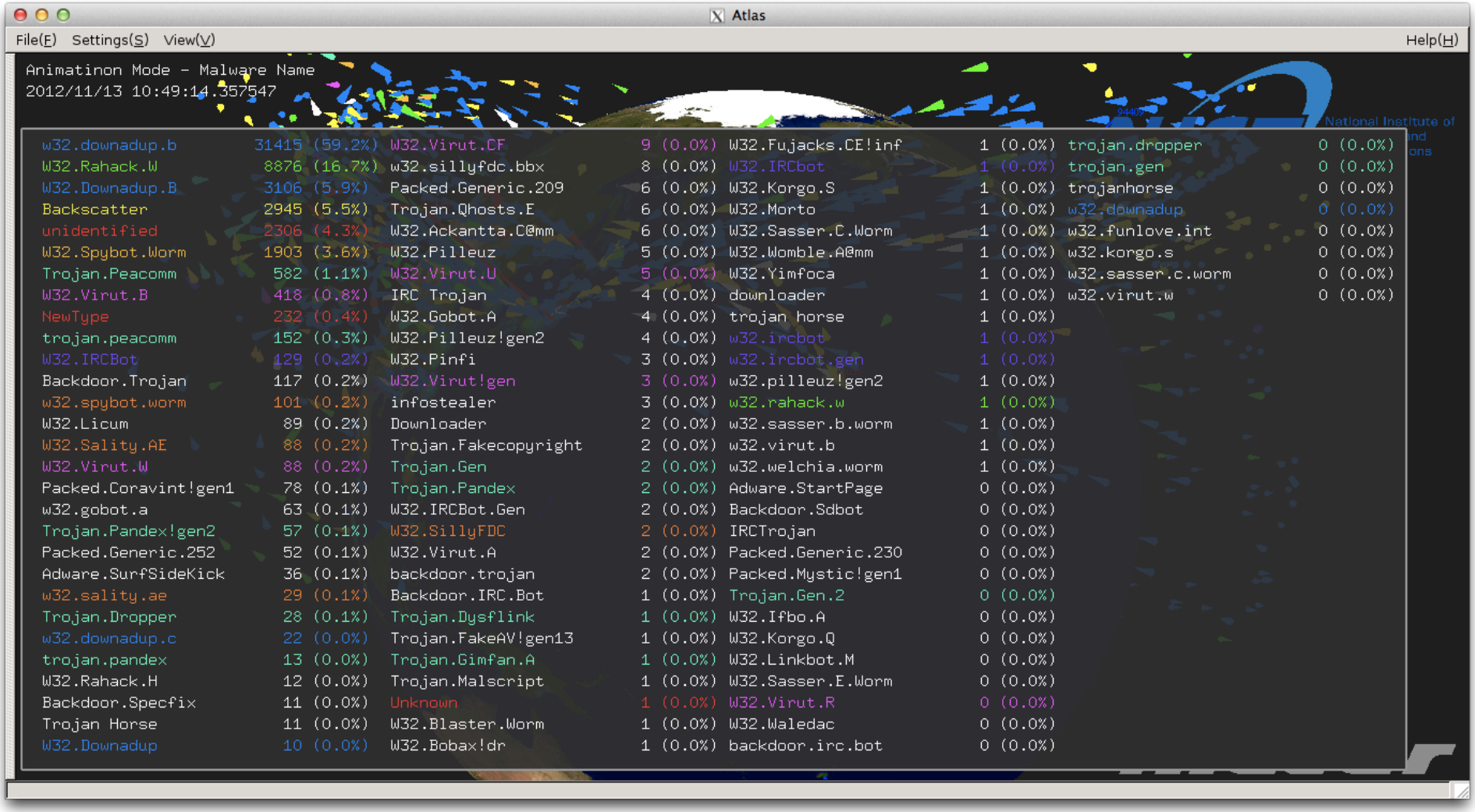


Result of Real-time Correlation Analysis (1/2)



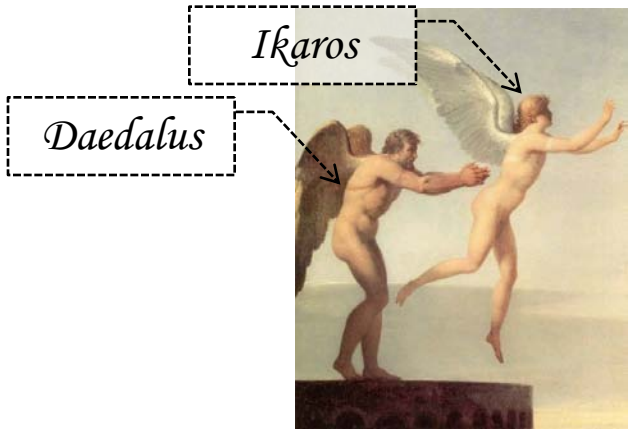
Demo

Result of Real-time Correlation Analysis (2/2)



DAEDALUS

(**D**irect **A**lert **E**nvironment for
Darknet **A**nd **L**ivenet **U**nified **S**ecurity)



Goal and Mechanism of DAEDALUS

Goal:

Utilize the darknet monitoring results

for securing the livenet.

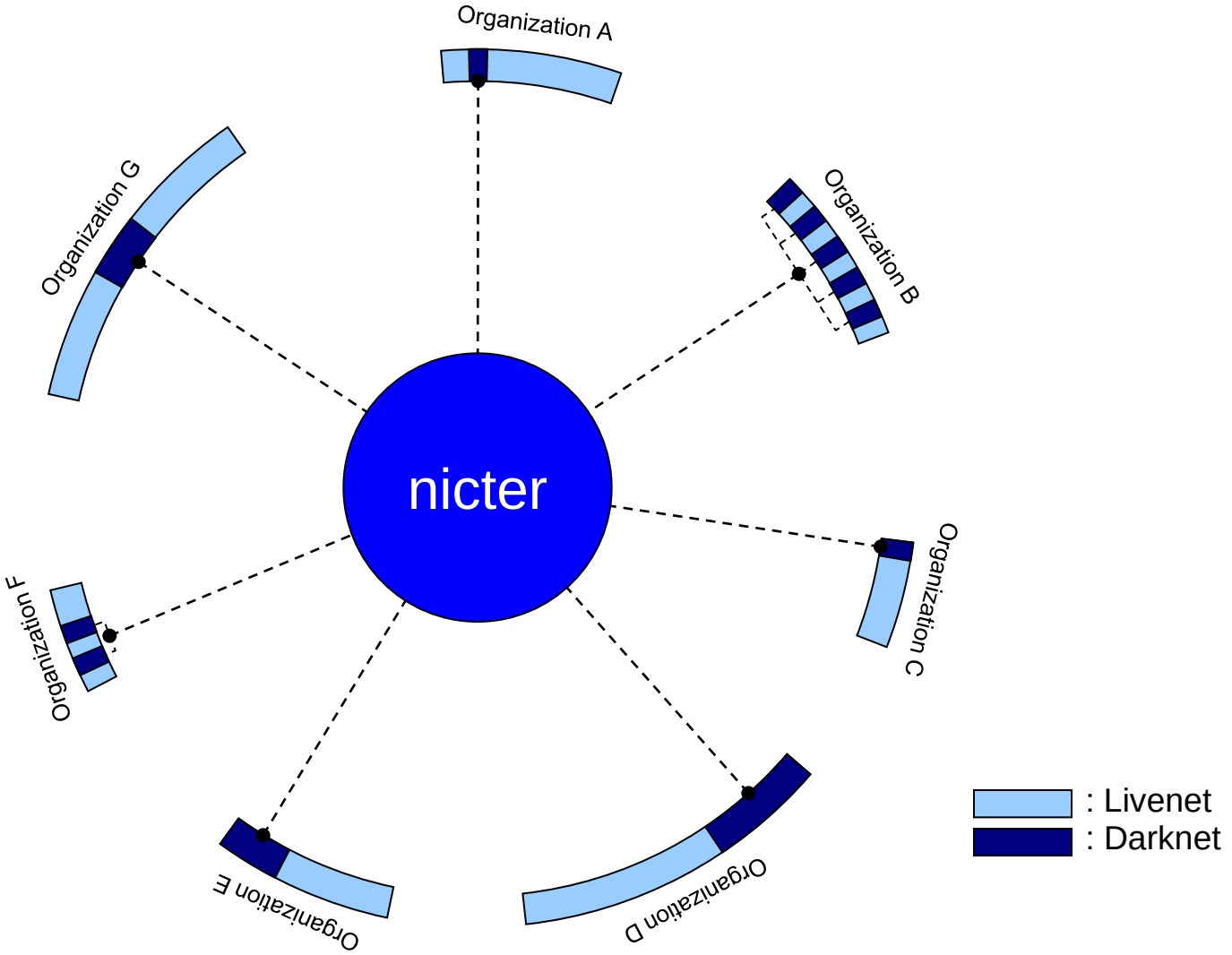
Mechanism:

if (nicter receives packets

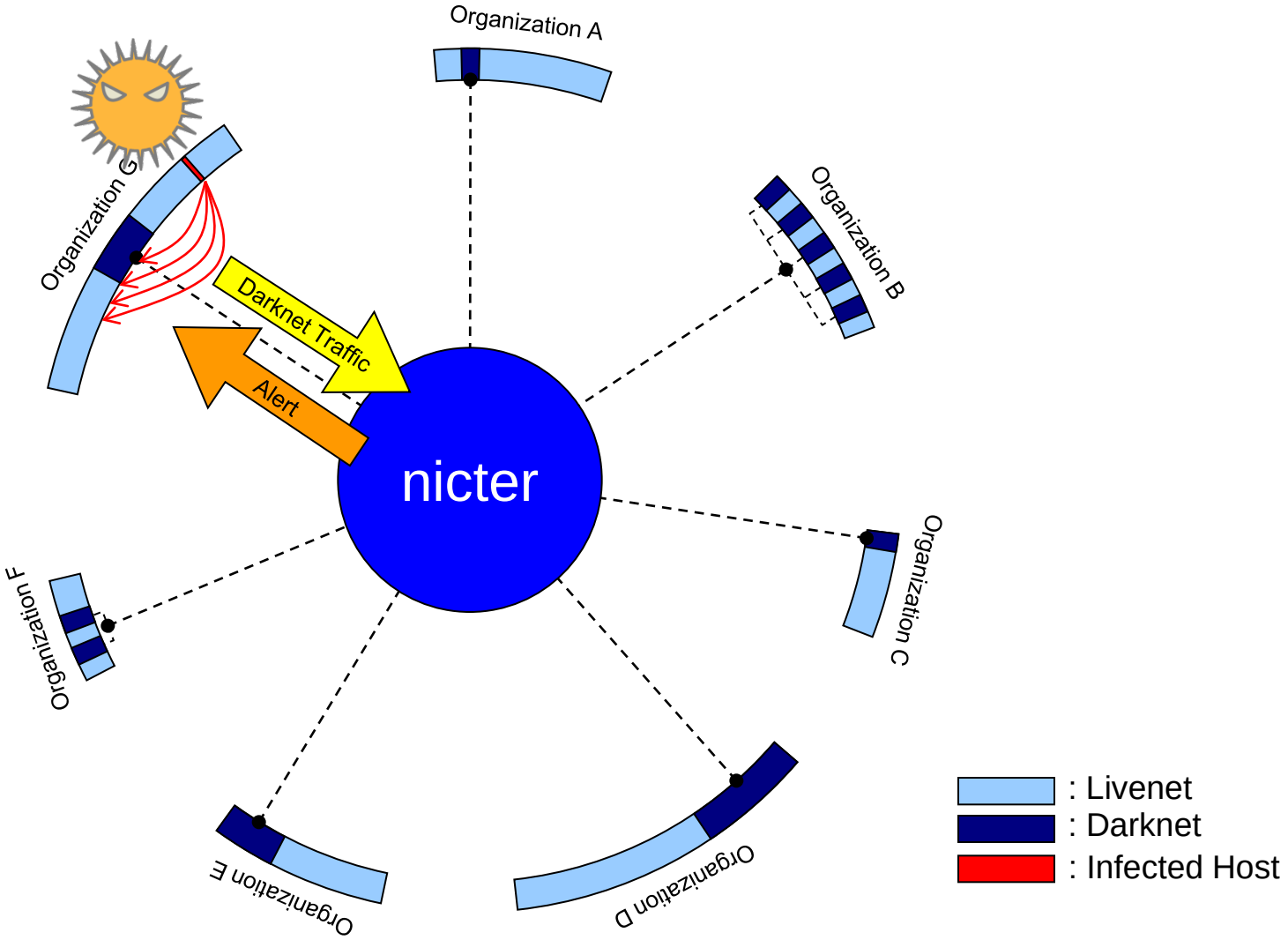
from a cooperative organization)

alert;

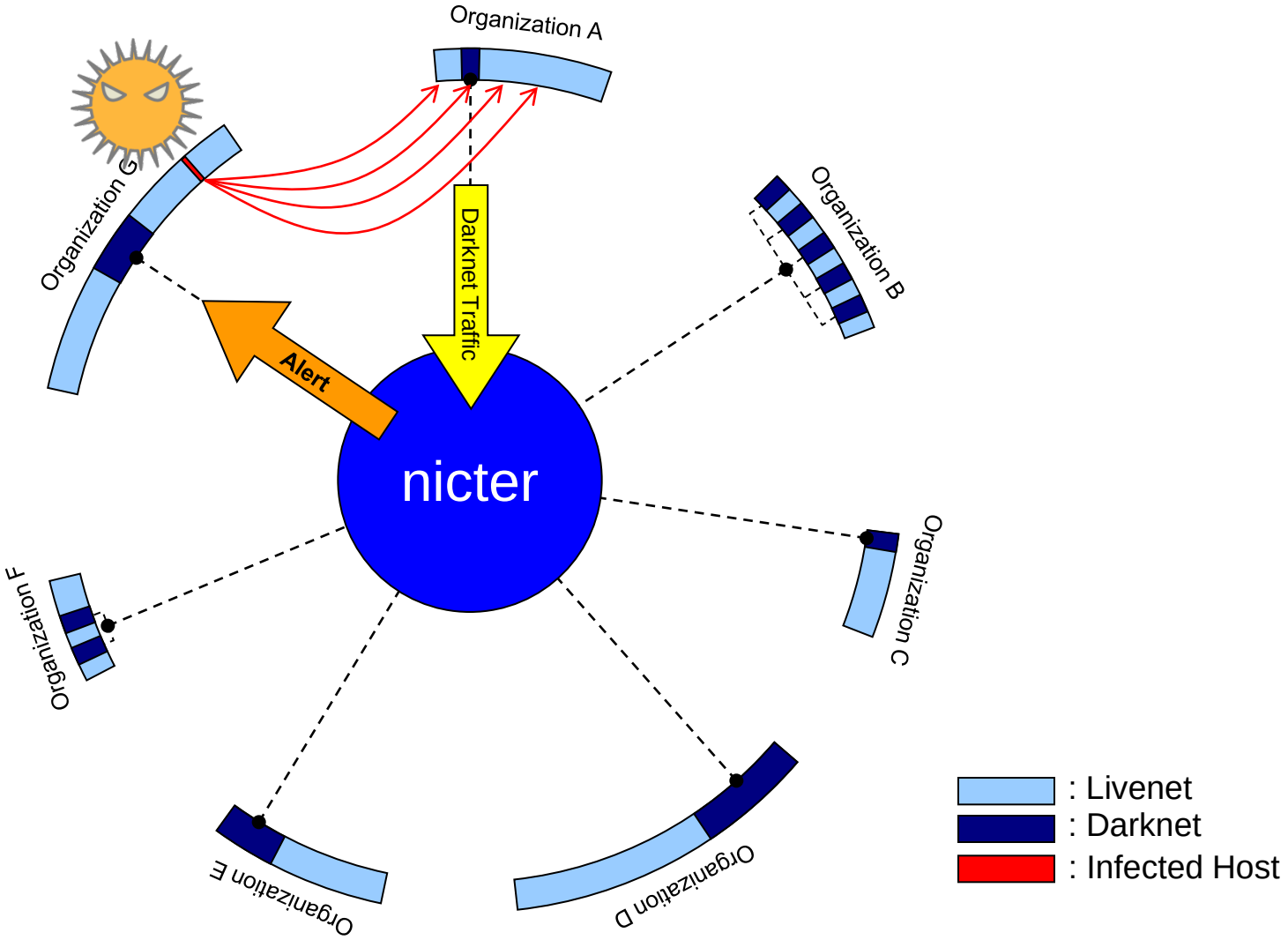
System Overview



Internal Darknet Alert (Local Scan)

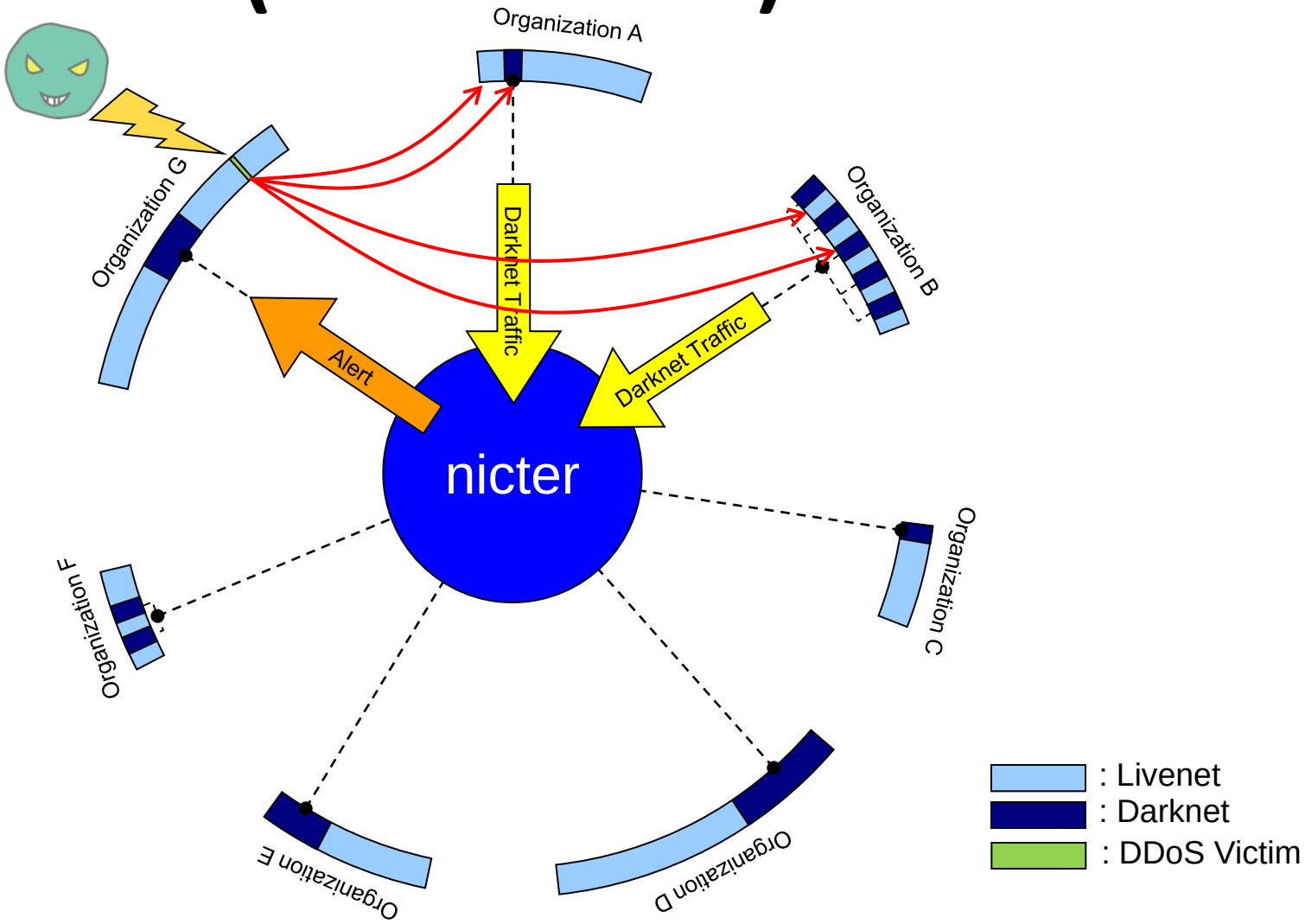


External Darknet Alert (Global Scan)



Case 3

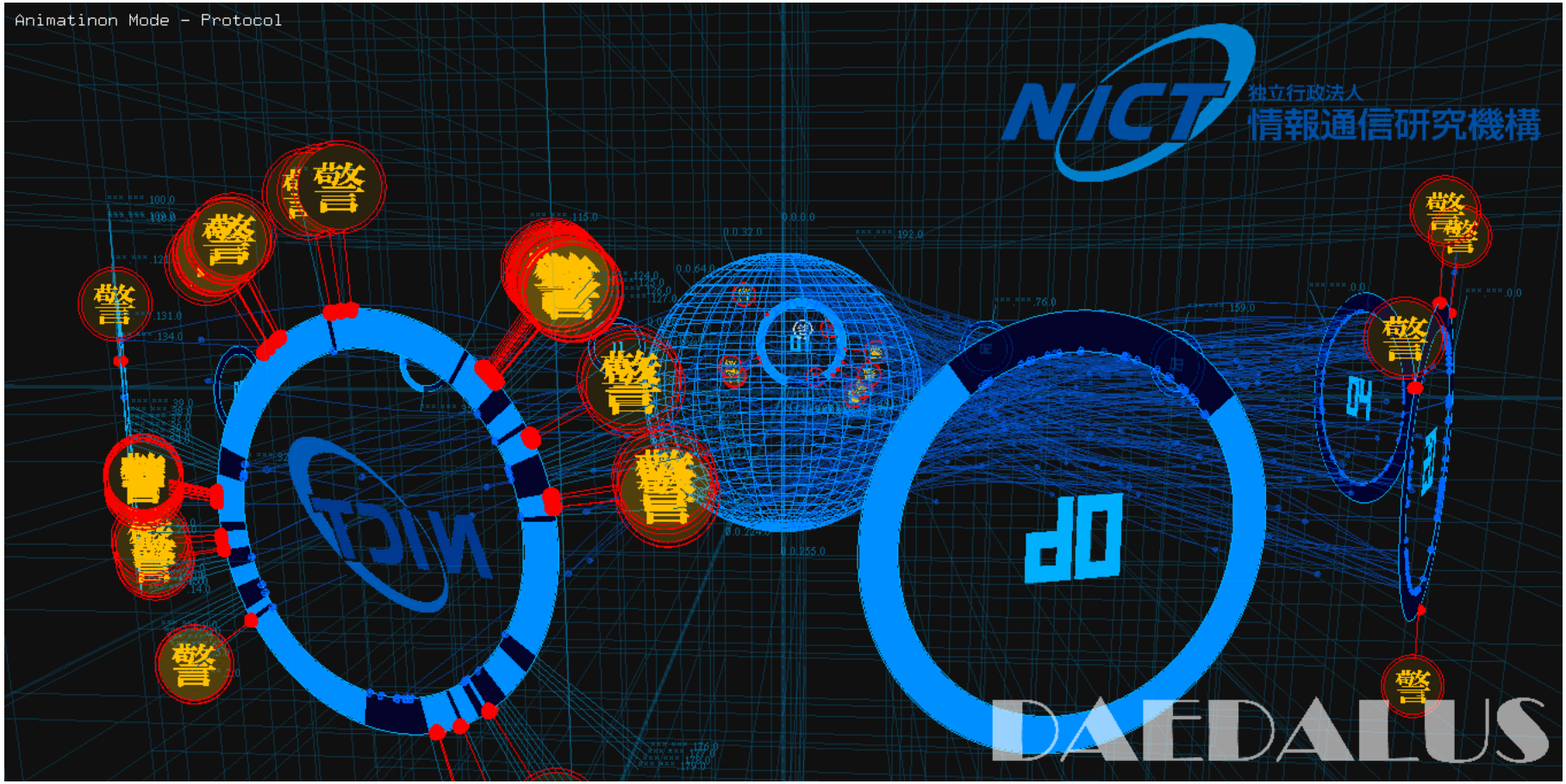
External Darknet Alert (Backscatter)



of DAEDALUS Alerts to a Certain Country

- From Jun 1, 2012 to Nov 19, 2012
- Plotting # of new alerts per day (i.e., # of attacking hosts)

DAEDALUS vis



Demo

NIRVANA

(nicter real-network visual analyzer)

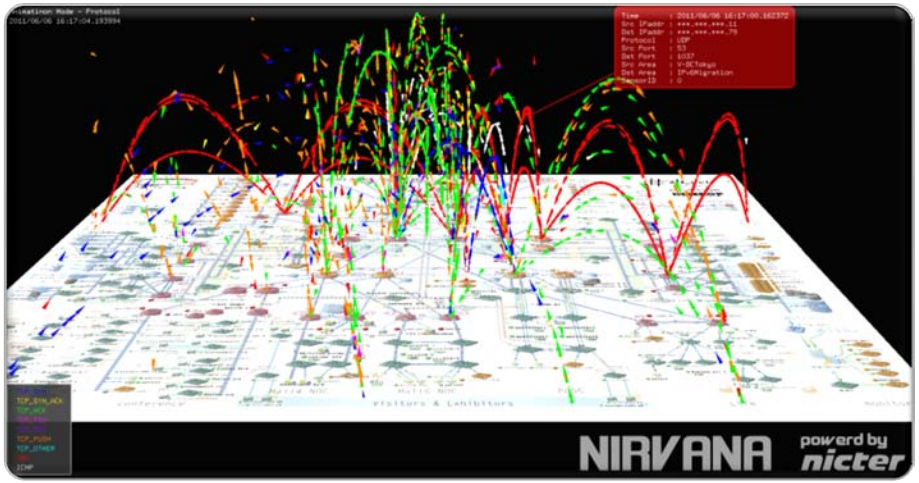
Objective

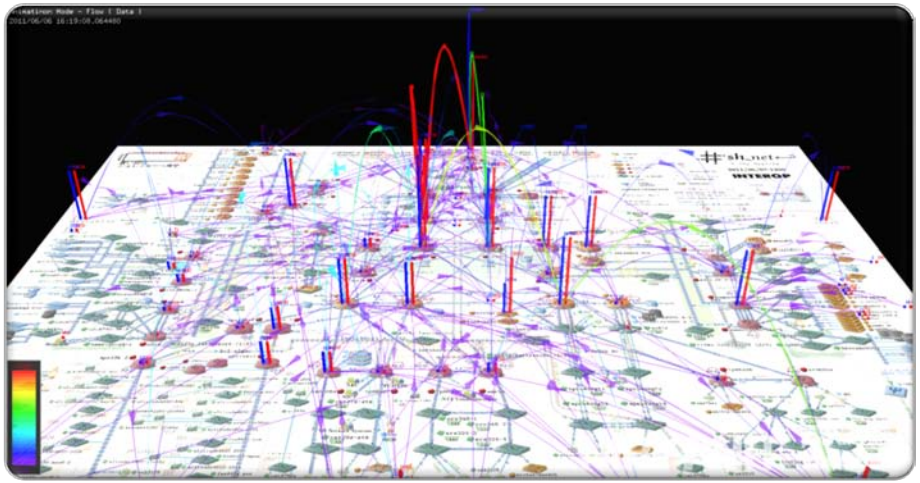
Demo

Visualizing livenet

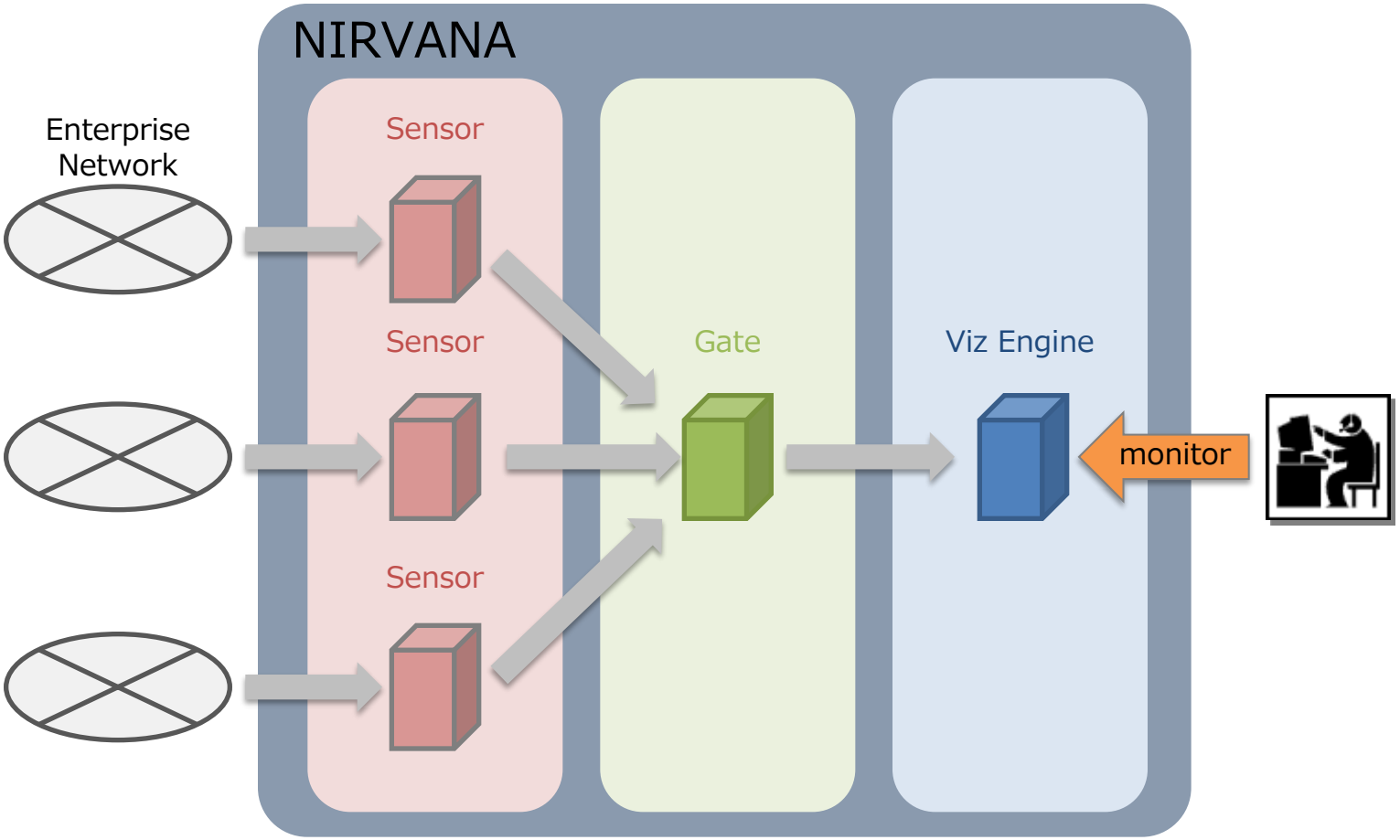
Reducing a load of network administration
(promptly find malfunction, misconfiguration and congestion)

Cost reduction



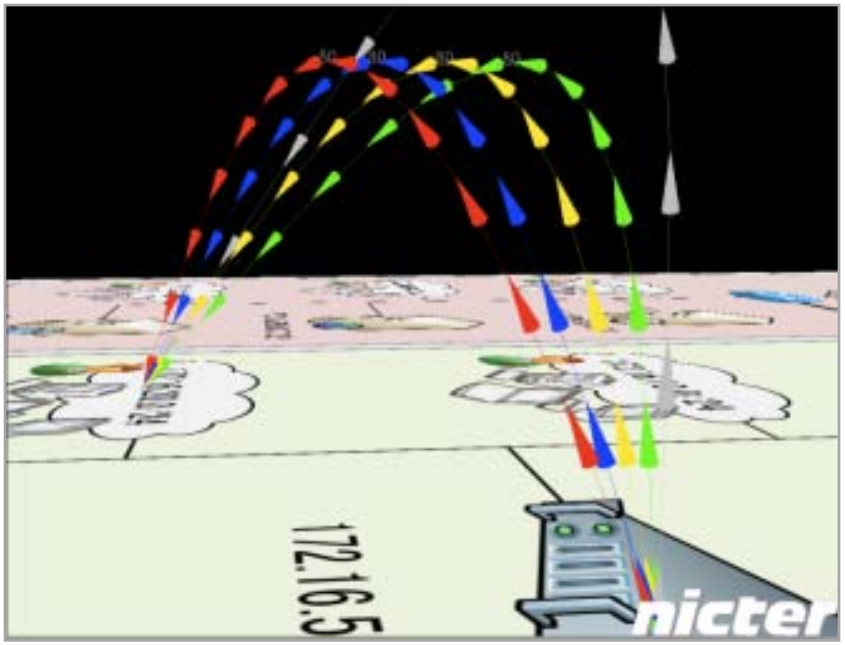


System Setting

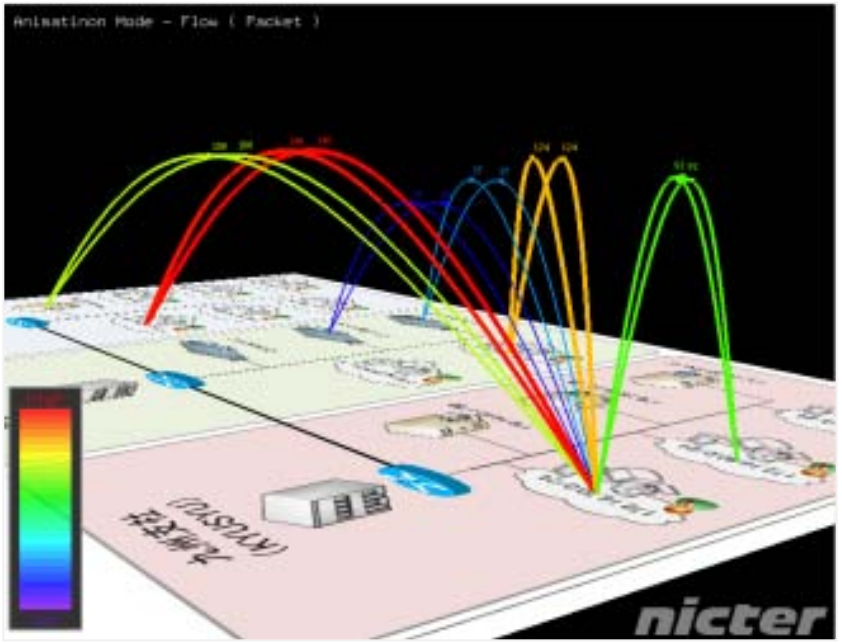


Packet Mode and Flow Mode

- Packet Mode

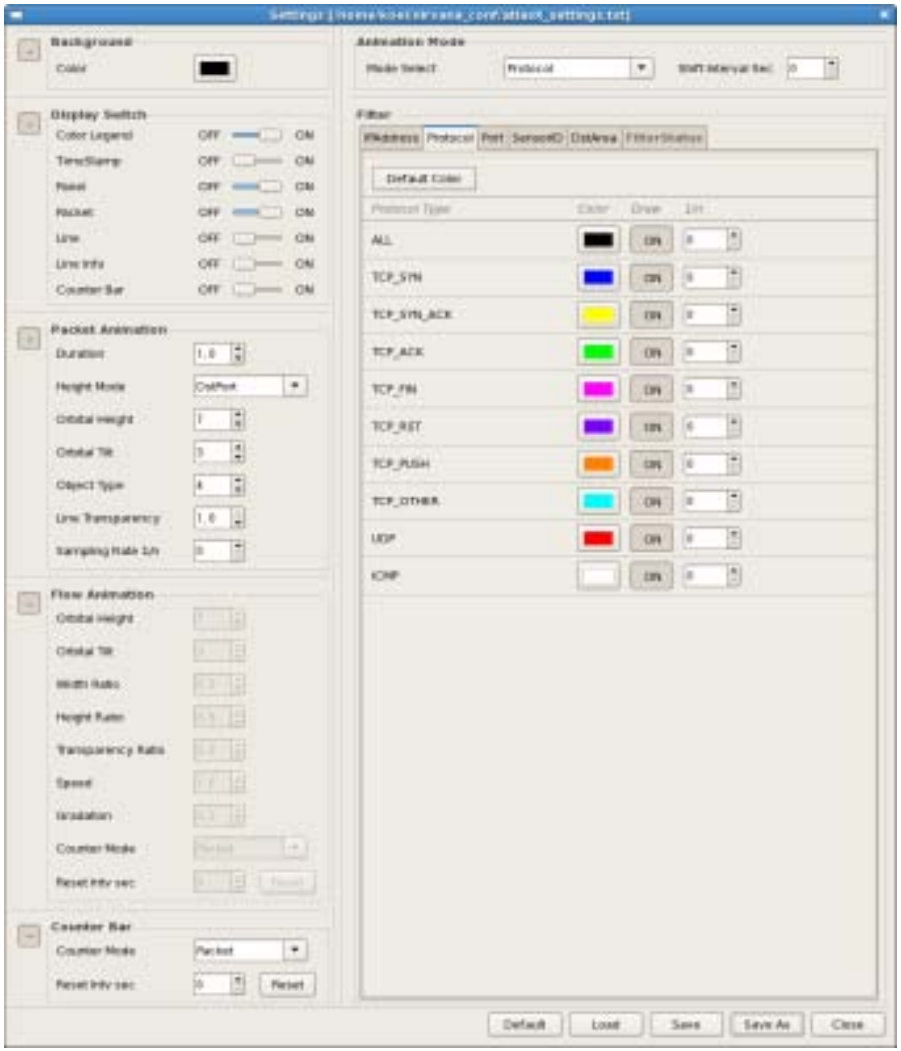


- Flow Mode



Filtering Functions

- IP Address
- Protocol
- Port Number
- Sensor ID
- Area



Sum of NICT projects

- nicter : Incident analysis system

+

- DAEDALUS : Darknet-based alert system

+

- NIRVANA+ : Livenet real-time visualizer with detector

+

- Countering Drive-by-download

+

- Boundary Protection (existing technologies)

||

New Horizon of Cybersecurity

PRACTICE Project

Proactive Response Against Cyber-attacks
Through International Collaborative Exchange

Ministry of Internal affairs and Communications
(MIC), Japan

Final Goal: Toward Proactive Response against Cyber-Attacks

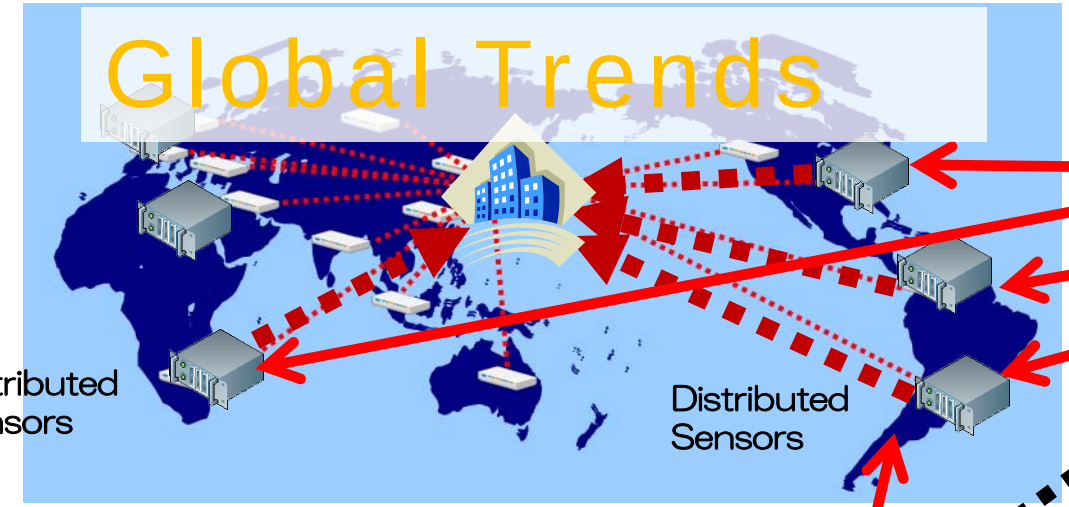
- Project is organized by MIC and is consisted of R&D part and Field Trial part.
- R&D part: Gaining maximum awareness of ongoing cyber attacks (botnets)

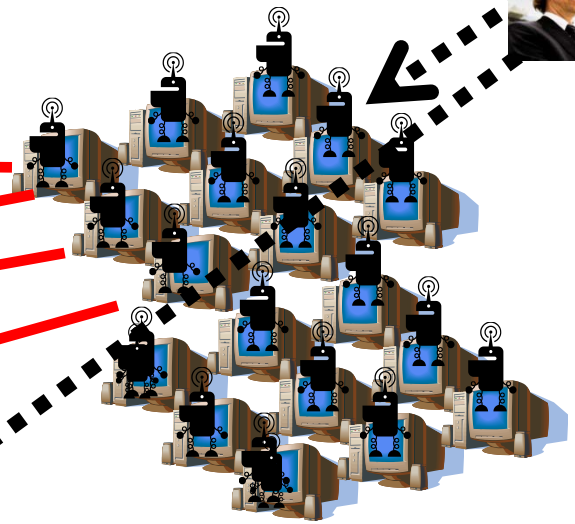
1) Macroscopic tracking of botnet attacks using various types of distributed sensors (victim-side monitoring) for grasping Global Trends

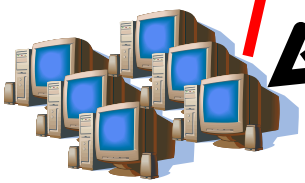
2) Microscopic tracking of individual bot-infected hosts using malware sandboxes (attacker-side monitoring) → Deep Insights

3) Based on correlation analysis among the above two approaches, Investigation of symptoms of cyber-attacks will be carried out for sharing among partners including international partners.

- Field Trial part: Establishing quick and proactive response scheme with ISPs' cooperation through a field trial by utilizing input from R&D part.







Malware sandboxes

Deep Insights

Who operates PRACTICE?

- MIC organizes the PRACTICE, which has Implementing Organizations and Supporting Organization.
- Implementing Organizations are ISP association(i.e. Telecom ISAC Japan) and related companies as a "field trial" part, and research institutes or security related companies as an "R&D" part.
- Supporting Organization is NICT which supports and assists "R&D" part of Implementing Organizations with technical expertise for cyber-attacks analysis technology.

Ministry of Internal Affairs and Communications

Implementing Organizations

Field trial of quick and proactive response based on the cooperation among ISPs.

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

NTT Communications

Data sharing

Partner countries

Data sharing

R&D of technologies which investigate symptoms of cyber attacks.

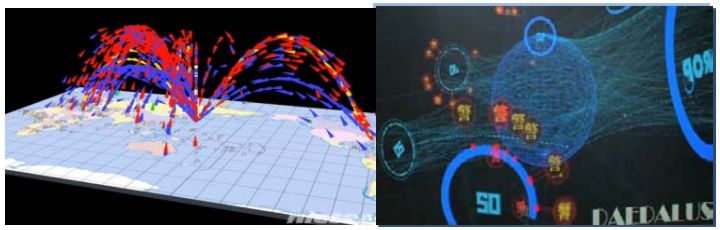
- Institute of Systems, Information Technologies and Nanotechnologies
- Japan Datacom Co., Ltd.
- KDDI R&D Laboratories
- SecureBrain Corporation
- Yokohama National University

Data & expertise

Supporting Organization

NICT

- Technical support based on NICT's excellent expertise;
- Providing captured data and the results of analysis by NICT.

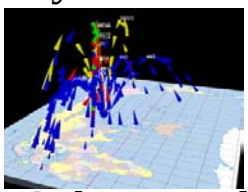


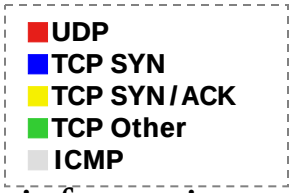
Visualization of cyber-attacks

What types of data to be shared

- **Basic data to be shared with our collaborative partner's country:**

1) Cyber attack information captured in Japan by LEU located in Japan



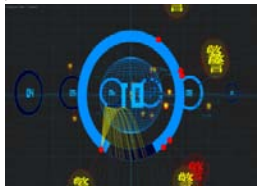


Information is visualized by means of the tool developed by NICT. Using this information, cyber-attack behaviors (mainly SCANs) to Japan can be observed. Each country could interestingly compare the trend of attacks with your own country (see below 2)).

2) Cyber attack information captured in our partner's country

Cyber-Attack Information targeted to your own country is visualized by means of the tool developed by NICT based on the captured data from darknet space in your country.

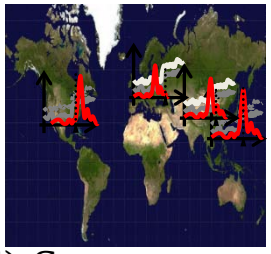
3) DAEDALUS data is provided (see Annex 1)



An organization (Use Case) : 14,000 addresses for livenet and 2,500 addresses for darknet Attacks by means of five continued alerts (with yellow) and one new alert (with red) were observed at 18:00 on July 10, 2012 in real-time basis. It is also possible to detect DDoS attack targeted to the livenet addresses just registered previously from your country.

- **Results of Analysis can also be shared with our collaborative partner's country:**

4) Attack similarity and specificity



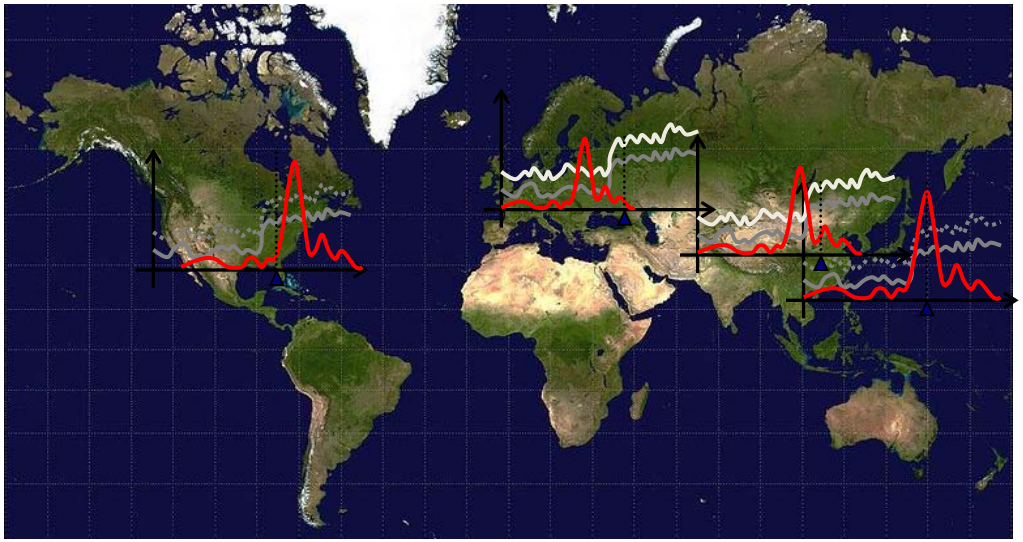
Based on several analysis engines, your country can grasp similar attack behaviors observed by many sensors located all over the world. This information can be shared among our all collaborative partners. Therefore, your country should be aware of this similar propagation of attack for your proactive response. On the other hand, attack behavior specificity in your country can be reported. In this case, your country will be required to take a special measure against specific attack only observed in your country (only shared with your country).

5) Symptoms of attack behavior

Based on data mining and other analysis methods, you will get symptoms of cyber-attack which will be very early stage of attack behavior. For example, "a new type of scan is getting observed in a synchronized manner among several sensors" will be informed.

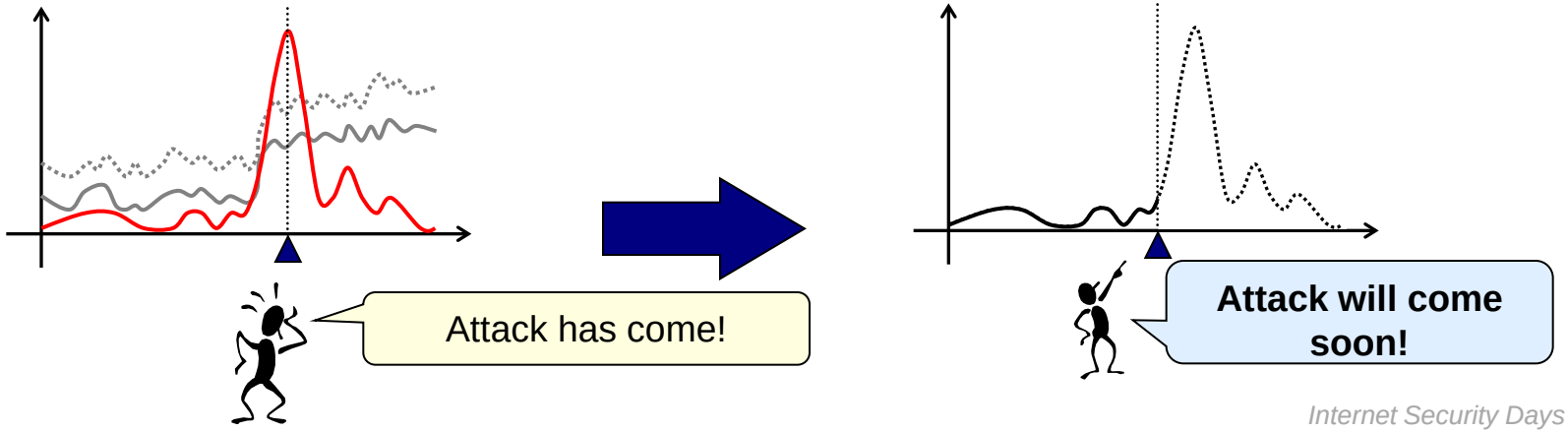
Results of Analysis can also be shared with our collaborative partner's country

Tech-1 : Prediction based on the data captured in foreign monitors

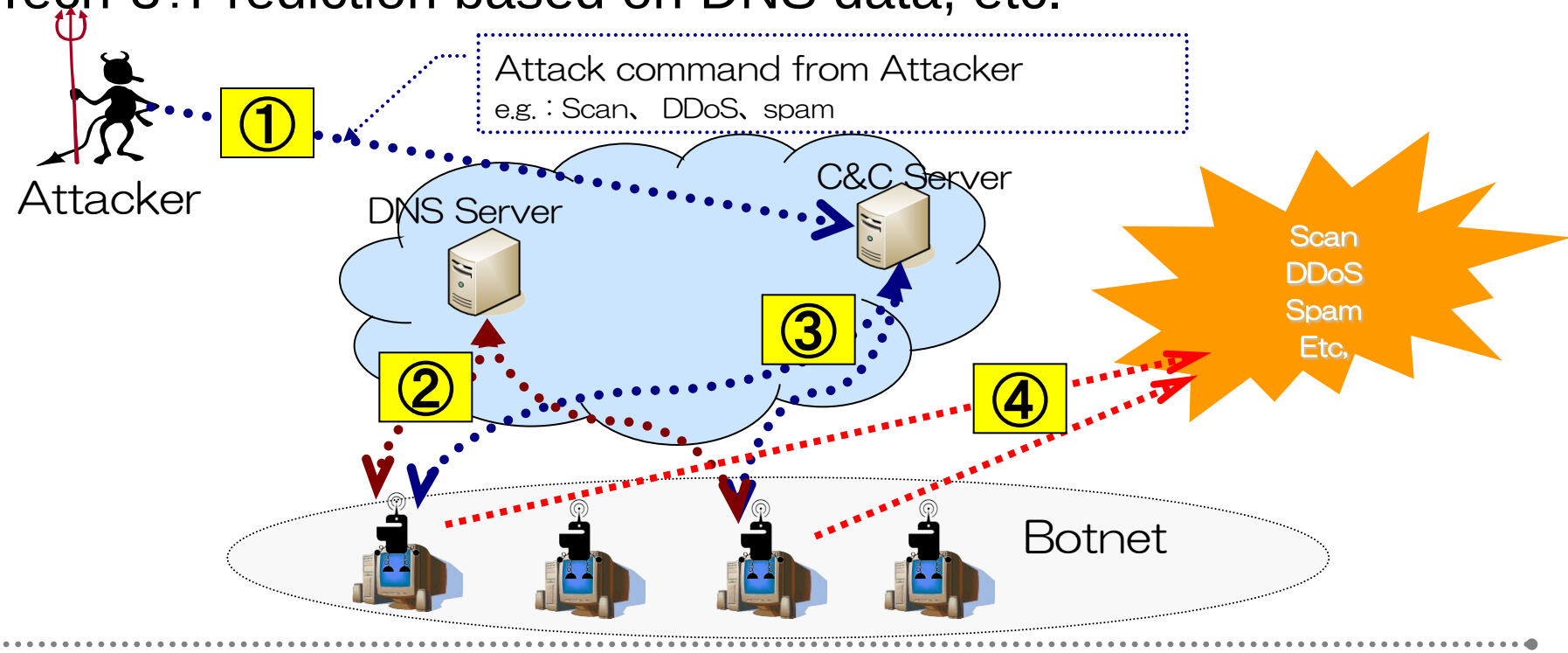


Based on the captured data from Japan, Asia, EU and US, characteristics of attack traffic and malware executable can be identified and analyzed for investigation of
-attack similarity,
-attack specificity and
-attack propagativity.

Tech-2 : Prediction by means of Data mining of traffic data



Tech-3：Prediction based on DNS data, etc.



Tech-4：Prediction based on Malware observing – New Plug-in (in the case of Zero-Access)

Malware Analysis	
Malware function 1	→ Already used in the previous attacks
New function 2	← New Plug-in
New function 3	← New Plug-in
Malware function 4	→ Already used in the previous attacks

Will be used near future!

Conclusion

- By utilizing "darknet monitoring (black-hole monitoring)", we could observe the following on-going threats/attacks:
  - Scanning behavior;
  - DDoS back-scatter;
  - Infected hosts by DAEDALUS.
- Since un-detectable attacks are apparently increasing nowadays such as targeted attacks (APT) and drive-by-download, it is getting hard to appropriately recognize specific threats and vulnerabilities by means of the existing darknet monitor tools at networks and systems.
- It is also difficult for the management of organizations, CII and Government to assess the risk which exists in their environments. Furthermore, it is necessary to be ready against new threats and/or unanticipated attacks.
- Since there are no boundaries in IT society based on the Internet, "activities for information security" should be carried out in International level. Especially, world-wide threats monitoring platform will be expected with collaboration among many countries.

Thank you for listening Q&A