Online Learning of Unstructured Data in Cybersecurity

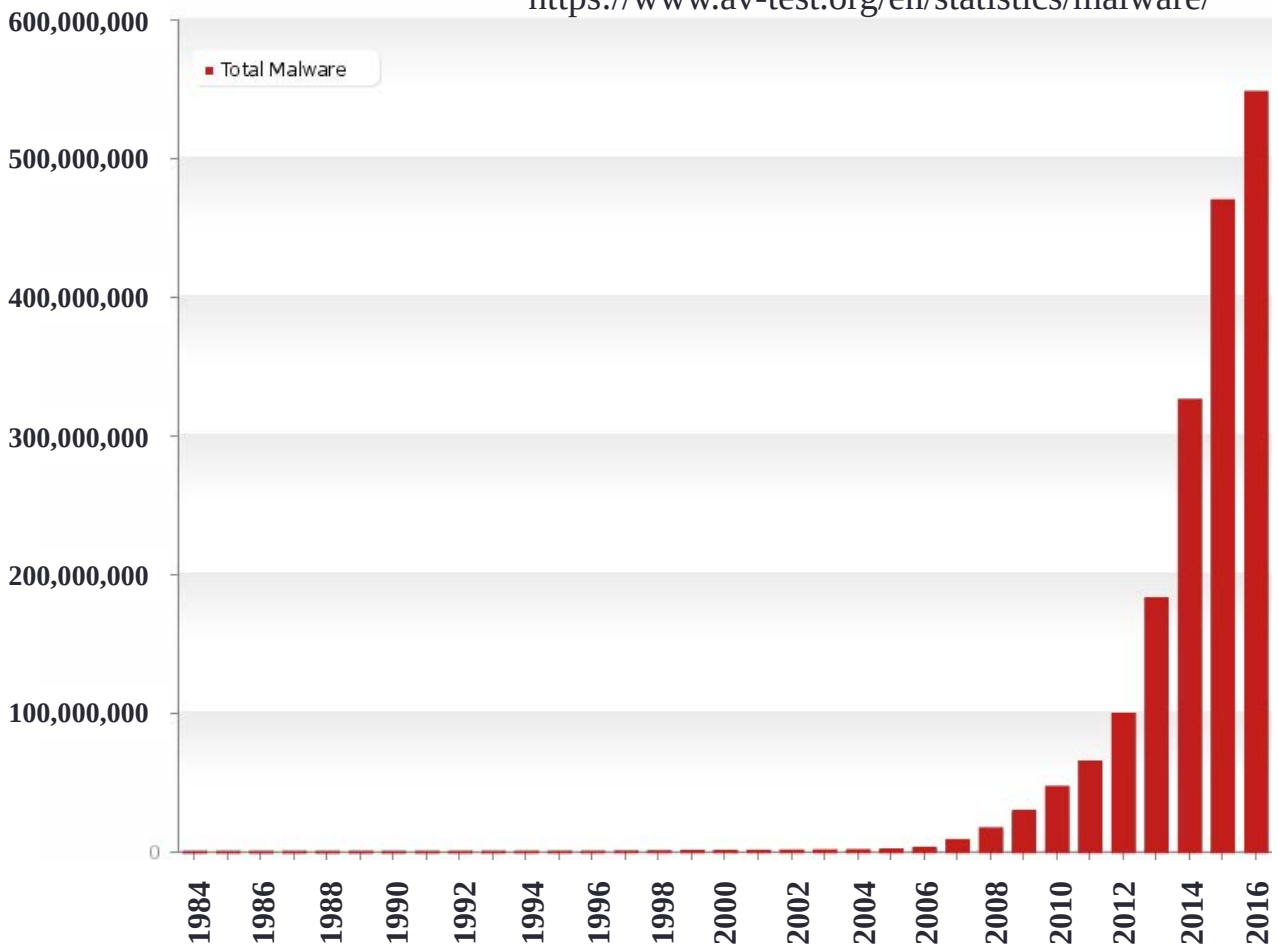
Seiichi Ozawa* and Tao Ban**

* Kobe University, Japan

** National Institute of Information and Communications Technology (NICT), Japan

Growing Cyber Threat

https://www.av-test.org/en/statistics/malware/



The total number of new malwares is growing exponentially. (AV-Test Institute)

Cyberattacks (1)

- **Network scanning** is a procedure for identifying active hosts on a network, either for the purpose of attacking them or for network security assessment.
- **Phishing** is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels.
- **Malicious spam mail** is a method to disseminate disguised URL links that appear to be for familiar websites but in fact lead to phishing web sites or sites that are hosting malware or **drive-by-download attack**.

quoted from Wikipedia

Cyberattacks (2)

- **Watering Hole** is a computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group gets infected.
- **Ransomware** is a Cryptovirology attack carried out using covertly installed malware that encrypts the victim's files and then requests a ransom payment in return for the decryption key that is needed to recover the encrypted files.
- **Denial-of-service (DoS) attack** is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

quoted from Wikipedia

Targeted Threats

- A class of malware destined for one specific organization or industry. Targeted attacks may include threats delivered via SMTP e-mail, port attacks, **zero day attack vulnerability exploits** or phishing messages.
- A **backdoor** is a method, often secret, of bypassing normal authentication in a product, computer system, cryptosystem or algorithm etc.
- An advanced persistent threat (APT) is a set of stealthy and continuous computer hacking processes. The `persistent' process suggests that a **command and control (C&C) server** is continuously monitoring and extracting data from a specific target.

quoted from Wikipedia

Phases of the Intrusion Kill Chain

U.S. Senate-Committee on Commerce, Science, and Transportation
-A "Kill Chain" Analysis of the 2013 Target Data Breach-March 26, 2014

Cybersecurity Challenges

- Emerging New Paradigms
  - cloud computing, mobile computing, IOT, ITS, automatic driving
- Big Data Issues
  - high bandwidth network – 10Gbps backbones equals 200k packet/s
  - cross borderline attacks – global views
  - real-time response requirement
- Evolving Threats
  - attackers: evasive, persistent, financial driven, fast adapting, going after the data
  - evolving attacks, zero-day attacks, highly-automated, polymorphism and metamorphism malware
  - human factors, unawareness, poor education, lag in patching
- Management and Operations
  - lack of resources and common protocols for information sharing, countermeasure
- Political Issues
  - lack of laws and regulations

What can Machine Learning do in Cybersecurity?

- **Malware Analysis (static and dynamic)**
  - ✓ malware classification
  - ✓ malware detection
  - ✓ packer identification for malware obfuscation
- **Network Intrusion Detection**
  - ✓ anomaly detection
  - ✓ monitoring malicious activities
- **Honeypot Data Analysis**
  - ✓ attack characterization
  - ✓ attack identification
- **Darknet Traffic Analysis**
  - ✓ DDoS attack event detection
  - ✓ scanning detection and analysis
  - ✓ malware identification
  - ✓ botnet activity detection and characterization
- **SPAM email analysis**

Machine Learning & Data Mining Projects

- **Malware analysis, both dynamically and statically (NICT)**
  - Malware detection using dynamic and static analysis
  - Packer identification and unpacking to counterattack malware obfuscation
  - Android malware analysis
- **Livenet traffic analysis with a focus on targeted-attack mitigation (NICT)**
  - Information visualization, stealth-scan detection, and incident analysis
  - Network based application classification for better quality of service (QoS) and malware mitigation
- **Darknet traffic analysis (NICT & Kobe-U)**
  - Early detection of DDoS-attacked hosts by backscatter-analysis
  - Scan detection and analysis (e.g., early protection from distributed reflection DoS attacks.)
  - Traffic feature clustering to discover new cyberattacks
  - Visualization of cyberattack distributions
  - Botnet activity detection and characterization
  - Malware identification based on profiling and pattern matching
  - Attack prediction based on association rule learning
  - Distributed analysis of traffic with regional information
  - Prediction on network incidents for proactive defense of network intrusion
- **SPAM email analysis (NICT & Kobe-U)**
  - Content based analysis
  - Java script and web page content analysis
- **Multi-modal analysis (NICT)**
  - Correlation analysis between unsolicited hosts both attacking darknet and performing spamming

How can we use Machine Learning?

We need to consider the followings:

(1) How can a target task be formulated as a supervised or unsupervised learning problem?
Supervised: classification, identification, anomaly detection
Unsupervised: clustering, anomaly detection, monitoring, rule mining

(2) How can unstructured raw data be transformed in feature vectors?
sanitization, decryption, unpacked, textualization, concealing (e.g., hashing), feature selection / extraction

(3) How can training data be collected and put the labels automatically?
i.e., autonomous mechanism to obtain training data

(4) Can a machine learning system be working fully autonomously?
In cybersecurity community, very negative. Then, ...

(5) How can the prediction of a machine learning system be trustable for administrators?

How Is Human Admin Monitoring Cyberattacks?

Overview of NICTER

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

Objective:

Comprehensive analysis of security threats on the Internet

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

Strategy:

Network monitoring

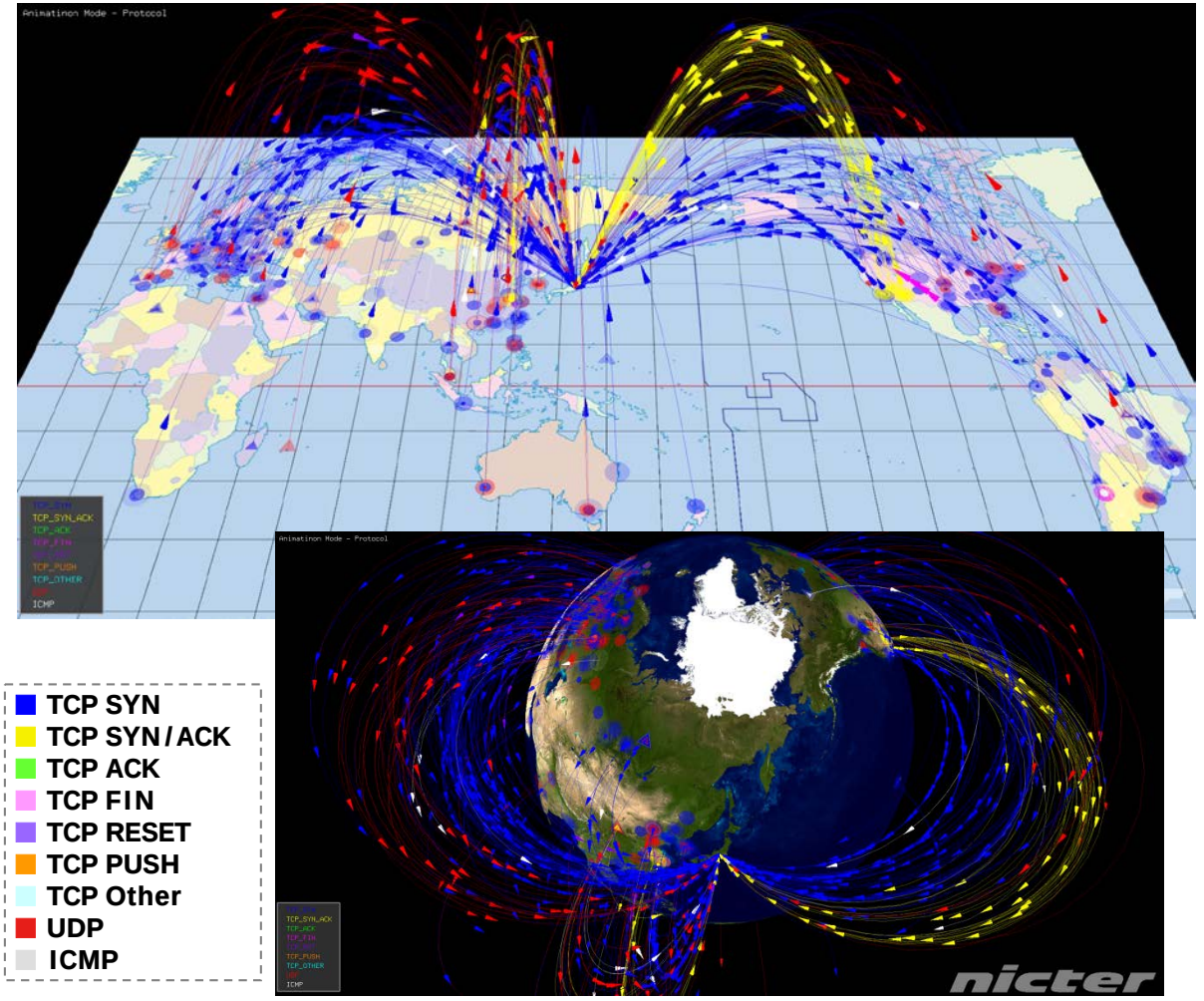
+

Malware analysis

NICTER Operation Room

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 a rocket indicates the type of packet
- The **altitude** of a rocket is in proportion to its dst port number



- TCP SYN
- TCP SYN/ACK
- TCP ACK
- TCP FIN
- TCP RESET
- TCP PUSH
- TCP Other
- UDP
- ICMP

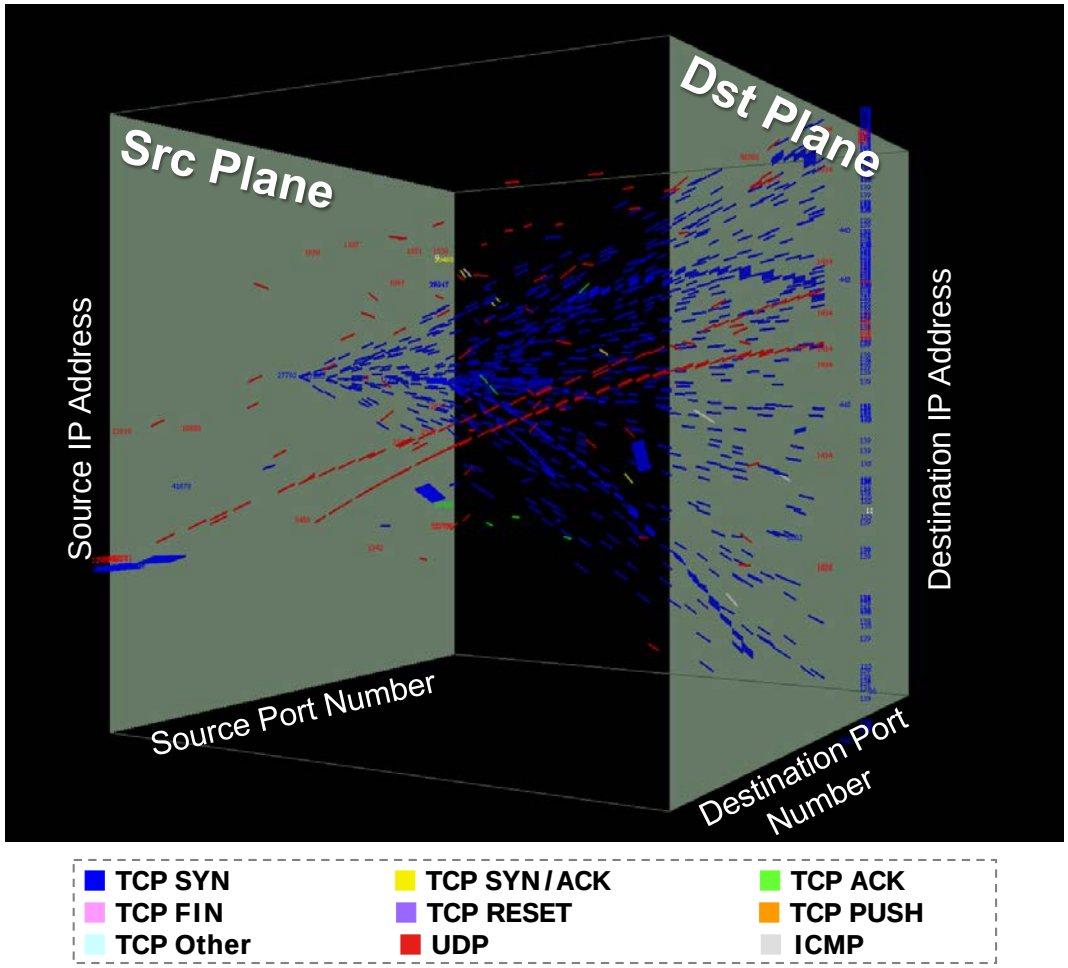
National Institute of Information and Communications Technology

NICTER

Network Incident Analysis Center for Tactical Emergency Response

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 travels to the destination plane within six seconds
- Its start and ending positions are decided by its **src/dst IP addrs and port numbers**



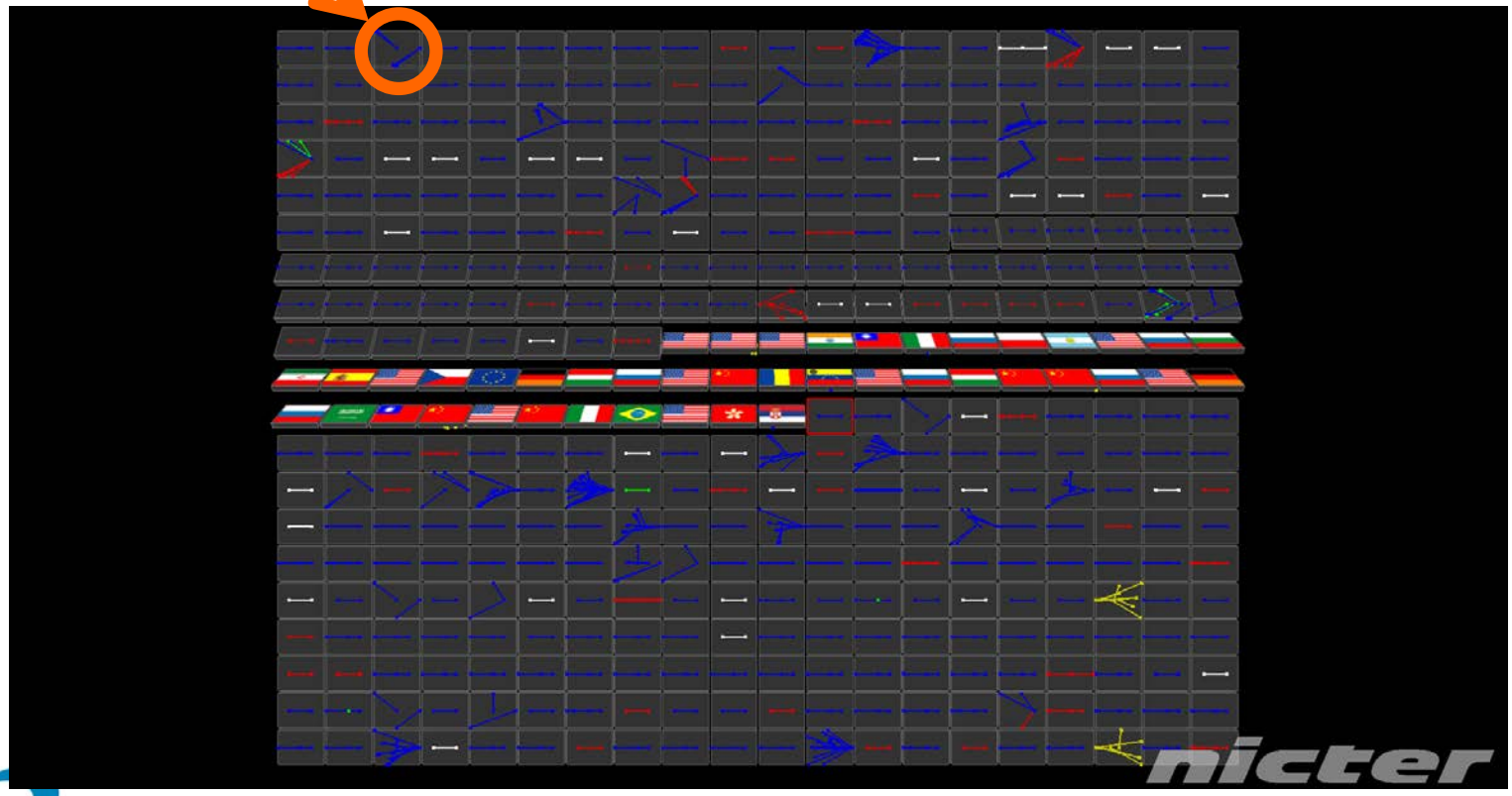
National Institute of Information and Communications Technology

NICTER

Network Incident Analysis Center for Tactical Emergency Response

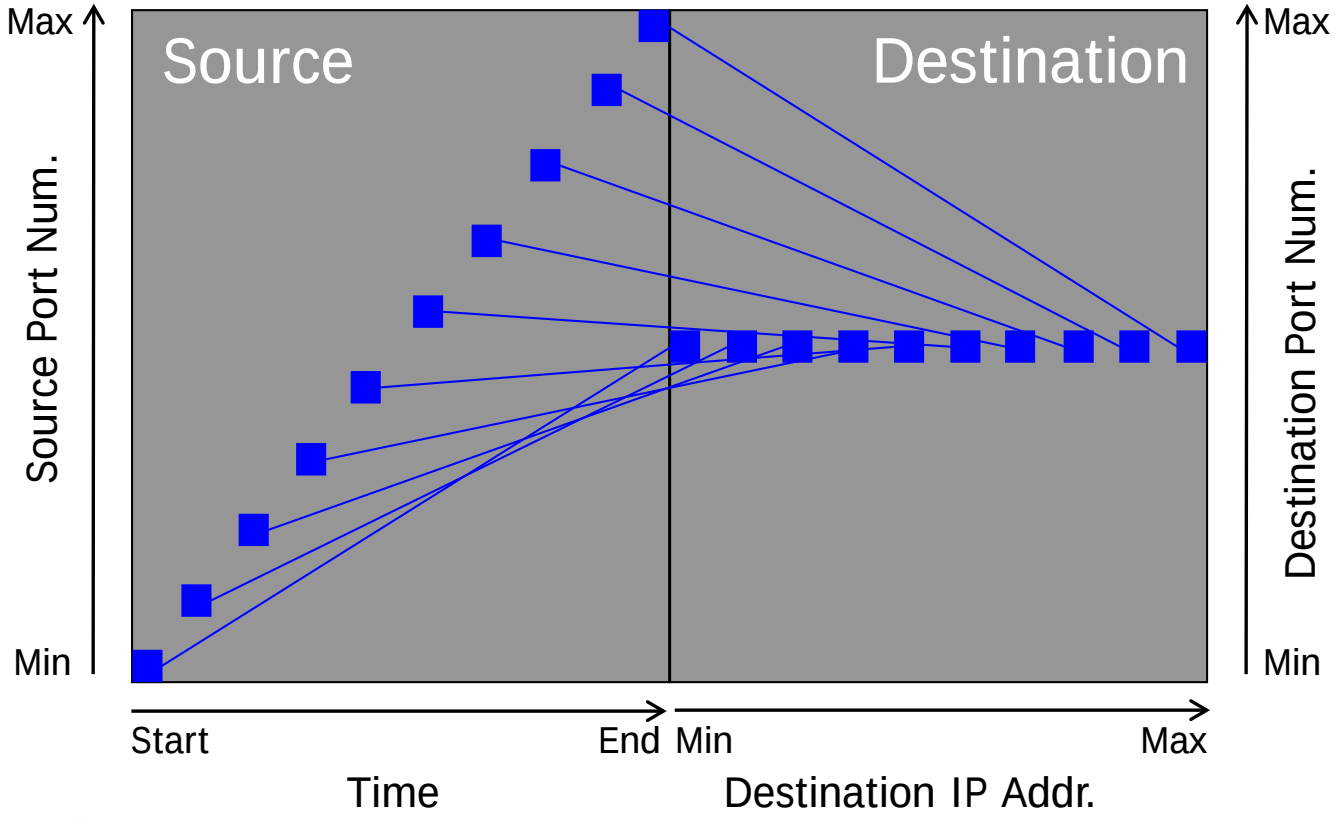
Tiles: Host-based Behavioral Analysis Engine

- One ***tile*** illustrates the behavior of an attacking host in 30 sec.
- Each behavior is automatically categorized and stored in a DB.
- Unknown attack pattern can be detected.



Visualization Method of a Tile

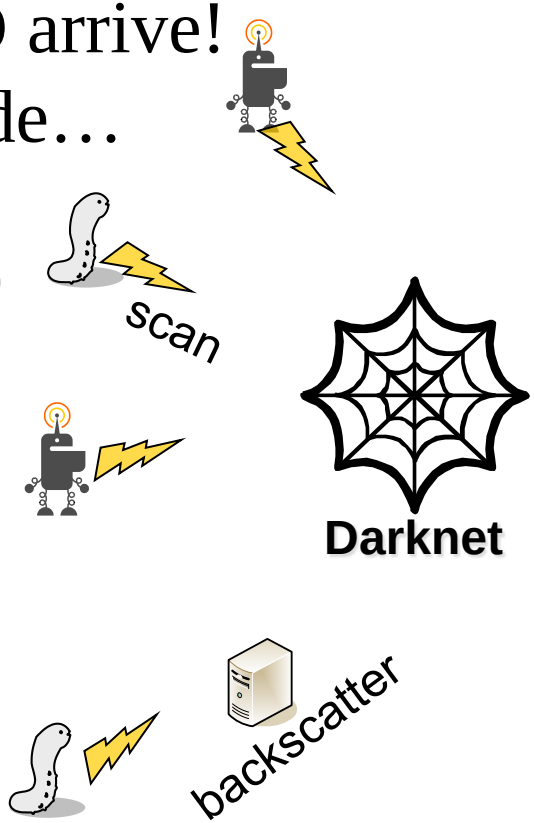
- **Source (left):** Time and Src Port Number
- **Destination (right):** IP Address and Dst Port Number



An Automatic Method to Collect Malicious Activity Data: *Darknet*

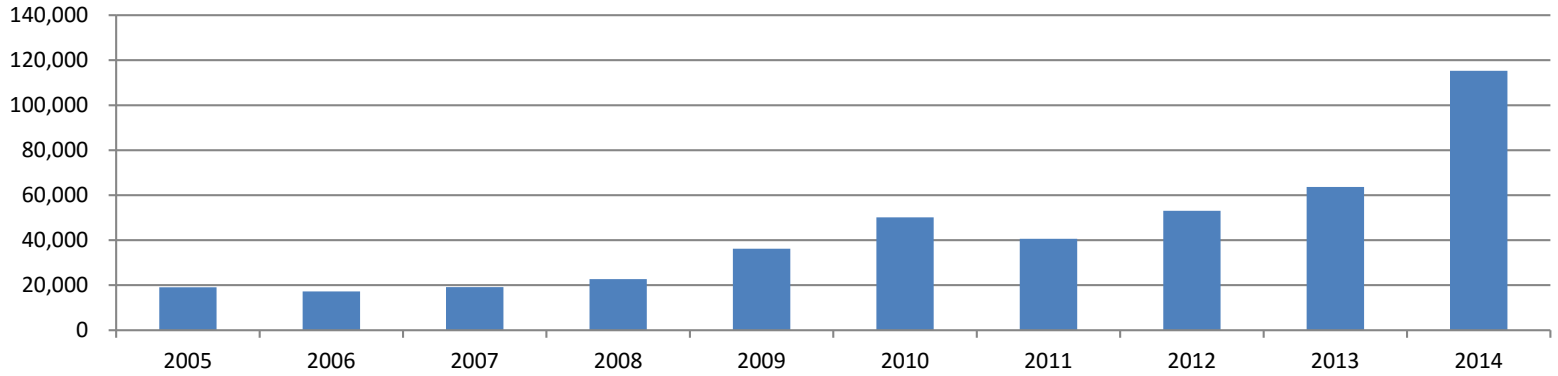
What is Darknet and Why We Work on it?

- **Darknet**: A network composed of unused IP addresses
- **Theoretically**: **NO** packet should arrive at a darknet because there is no legitimate host connected.
- **Technically**: quite a few packets **DO** arrive!
- Packets arriving at the darknet include…
  - **Scans by malwares**
  - Backscatter (reflection of DDoS attack)
  - Miss configurations etc.
- Advantages:
  - A good tradeoff between global monitoring and monitoring cost.
  - Its traffic reflects **global trend in malicious activities** on the Internet.



Darknet Traffic is Still Big

Year	Number of packets par year	Number of IP address For darknet	Number of packets par 1 IP address per year
2005	0.31 billion	16 thousands	19,066
2006	0.81 billion	100 thousands	17,231
2007	1.99 billion	100 thousands	19,118
2008	2.29 billion	120 thousands	22,710
2009	3.57 billion	120 thousands	36,190
2010	5.65 billion	120 thousands	50,128
2011	4.54 billion	120 thousands	40,654
2012	7.79 billion	190 thousands	53,085
2013	12.9 billion	210 thousands	63,655
2014	**25.7 billion**	240 thousands	**115,323**



Average number of packets observed on a darknet IP address each year.

NICTER

The Need for Data Mining

New challenges from security big data

- **Volume:** 240,000 monitored IP addresses results in a throughput of more than 500 packet/s. 5000 malware specimens dynamically analyzed by a sandbox system,
  network traffic collected from 10gbs enterprise network,…
- **Complexity:** zero-day attacks, new paradigms, non-stationary, noisiness, distributedness.

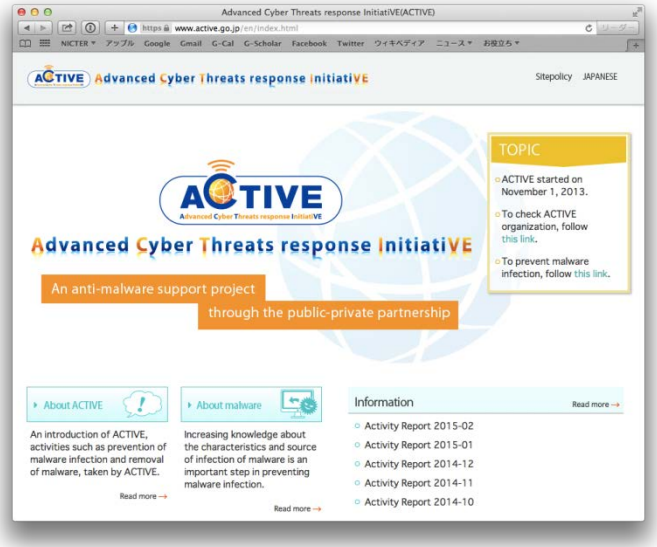
By the application of data mining techniques, improvements are expected in

- **Stability:** robust results that generalize better,
- **Scalability:** timely and proactive defense scheme for big-data,
- **Usability:** easily understandable results supported by solid facts and theories,
- **Cost reduction:** labor and system costs.

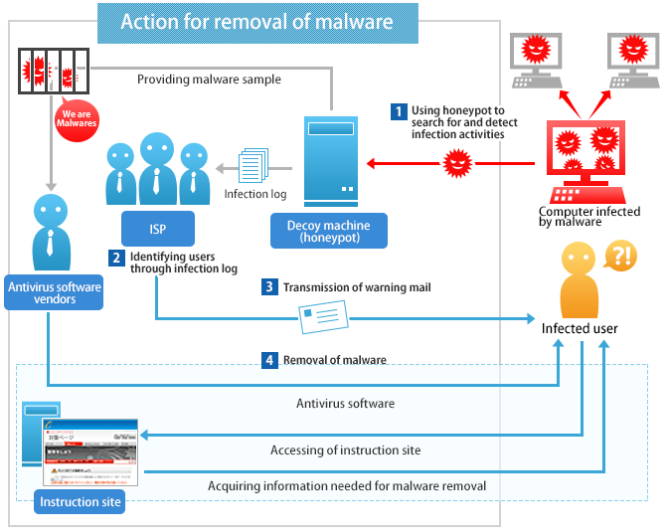
Practical Use of NICTER's Data and Knowledge

- **SIGMON** (Special Interest Group of Network Monitoring)
  - ✓ Pertners: JPCERT/CC, IPA, @Police, NICT, Universities
  - ✓ Sharing analysis results of darknet traffic (since 2004)

- **ACTIVE** (Advanced Cyber Threats response InitiatiVE)
  - ✓ Security alert and prevention activity to users via ISPs
  - ✓ NICTER provides infected IP address information (since 2014)



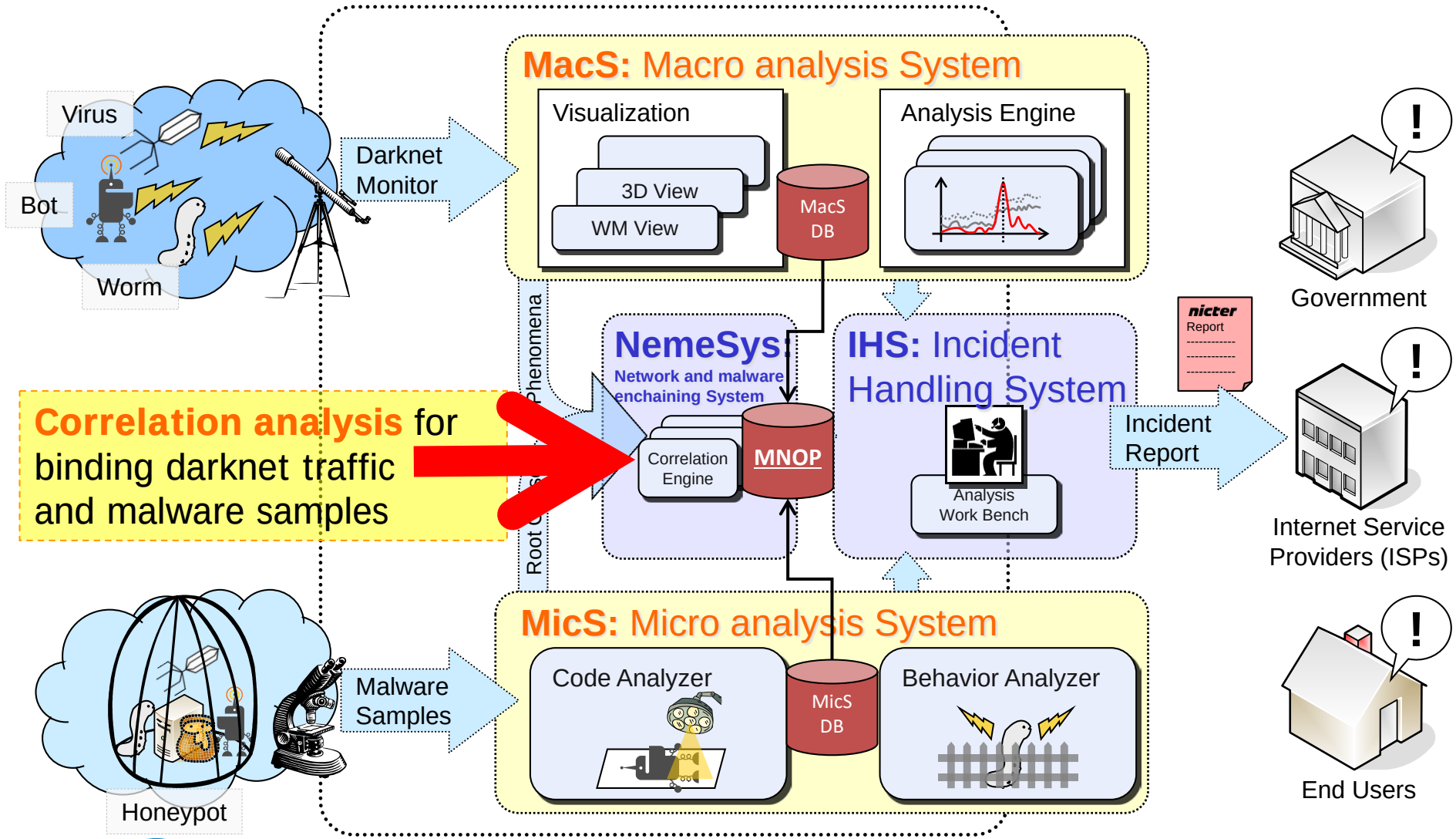
www.active.go.jp



Action for Removal of Malware by ACTIVE

Malware Profiling and Pattern Matching

Correlation Analysis (NemeSys) @NICTER



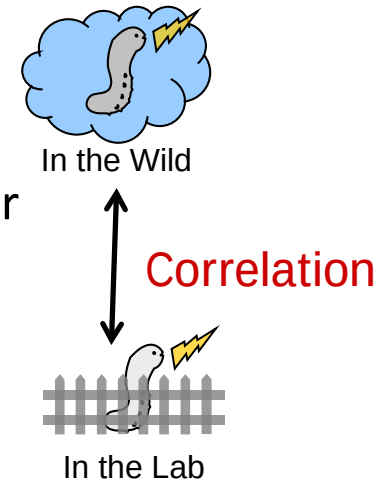
Overview of Correlation Analysis

Goal :

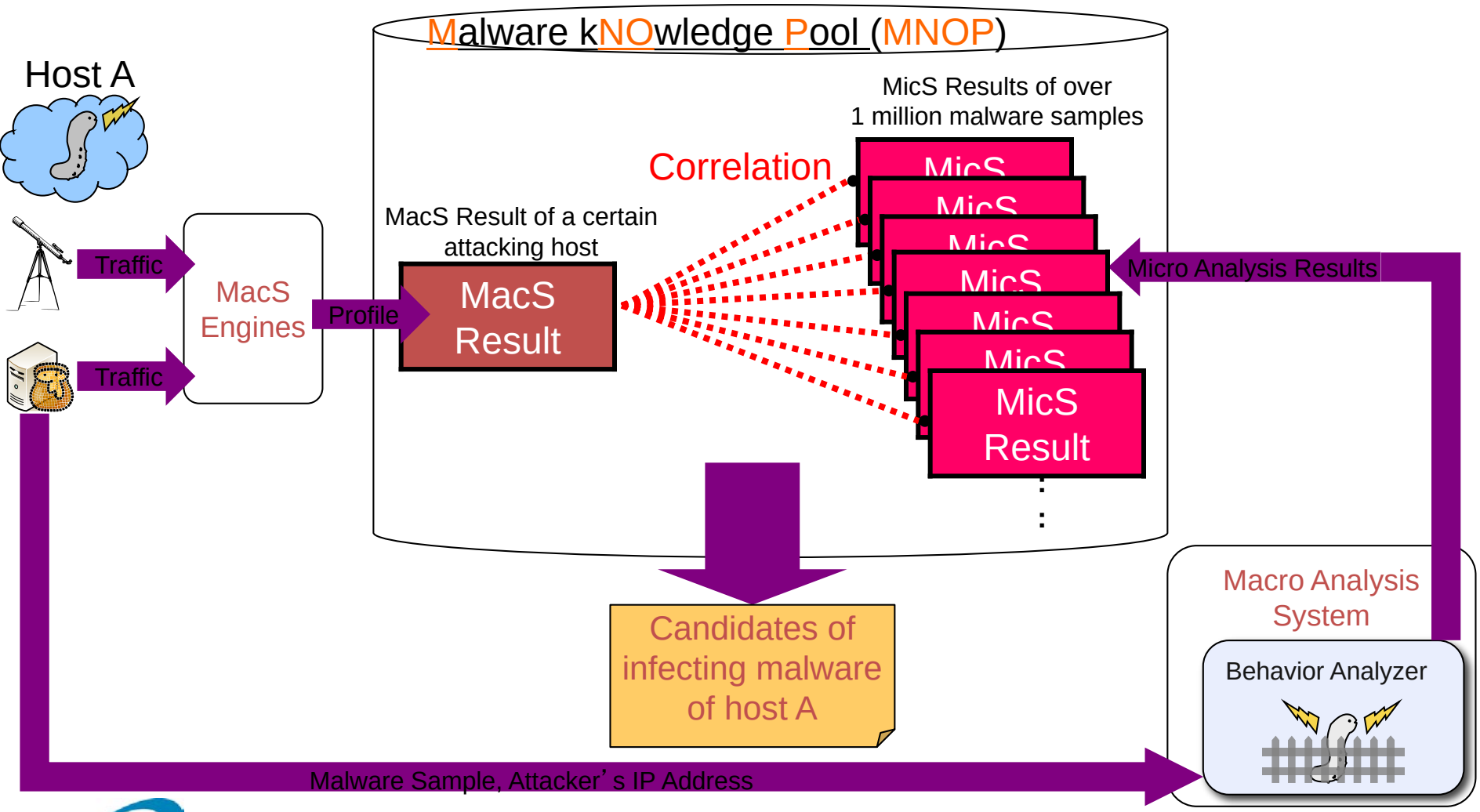
To bind phenomena (attacks) observed by the macro analysis system and root cause (malwares) inspected in the micro analysis system.

Basic Idea (scan based correlation):

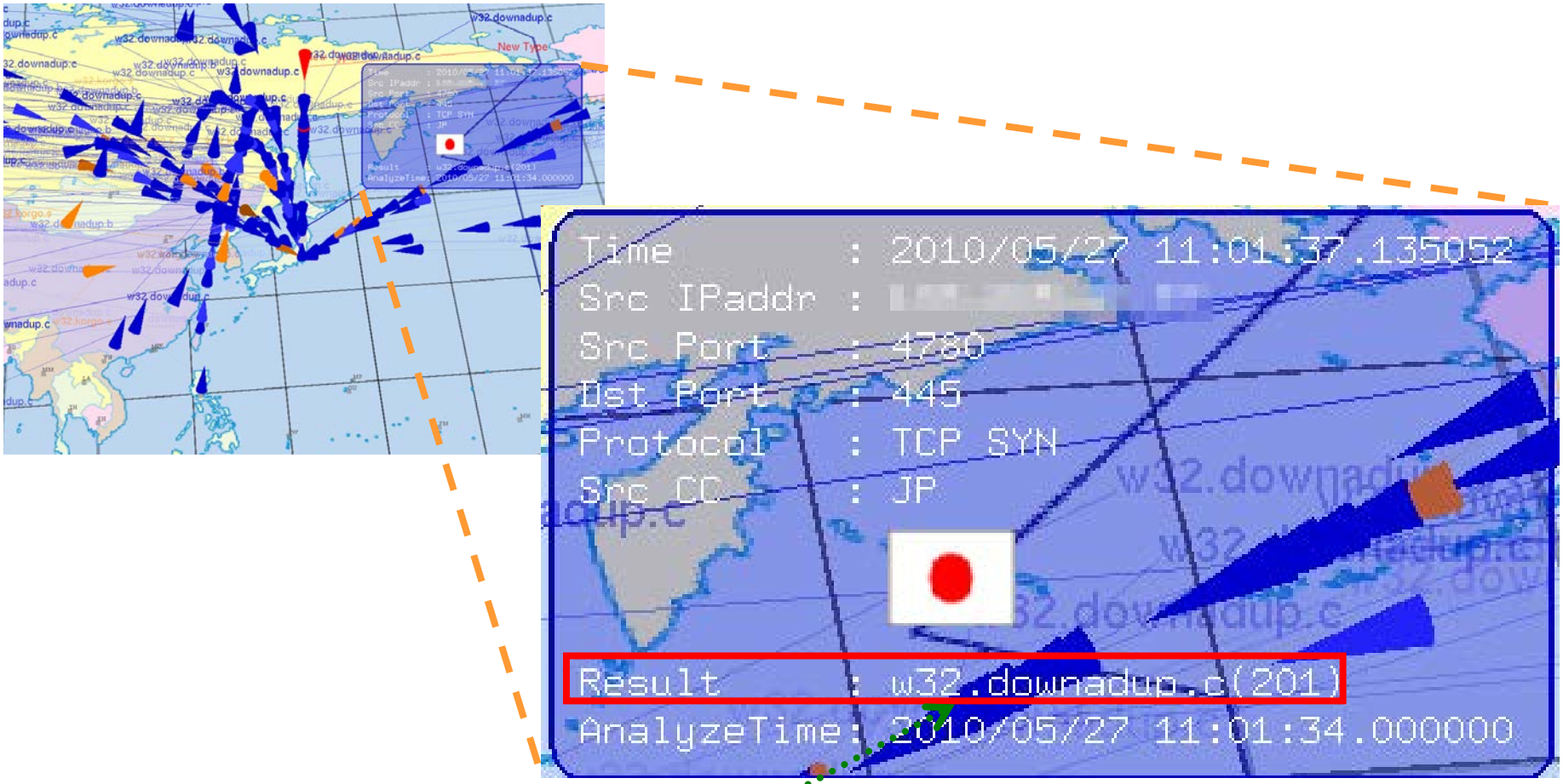
- MacS: Profiling attack packets (scan, shellcodes or malware itself) sent by a certain host
- MicS: Profiling attack packets captured in the behavior analyzer
- Compare scan profiles by using correlation coefficient then candidates of infecting malware can be listed



Overview of Correlation Analysis



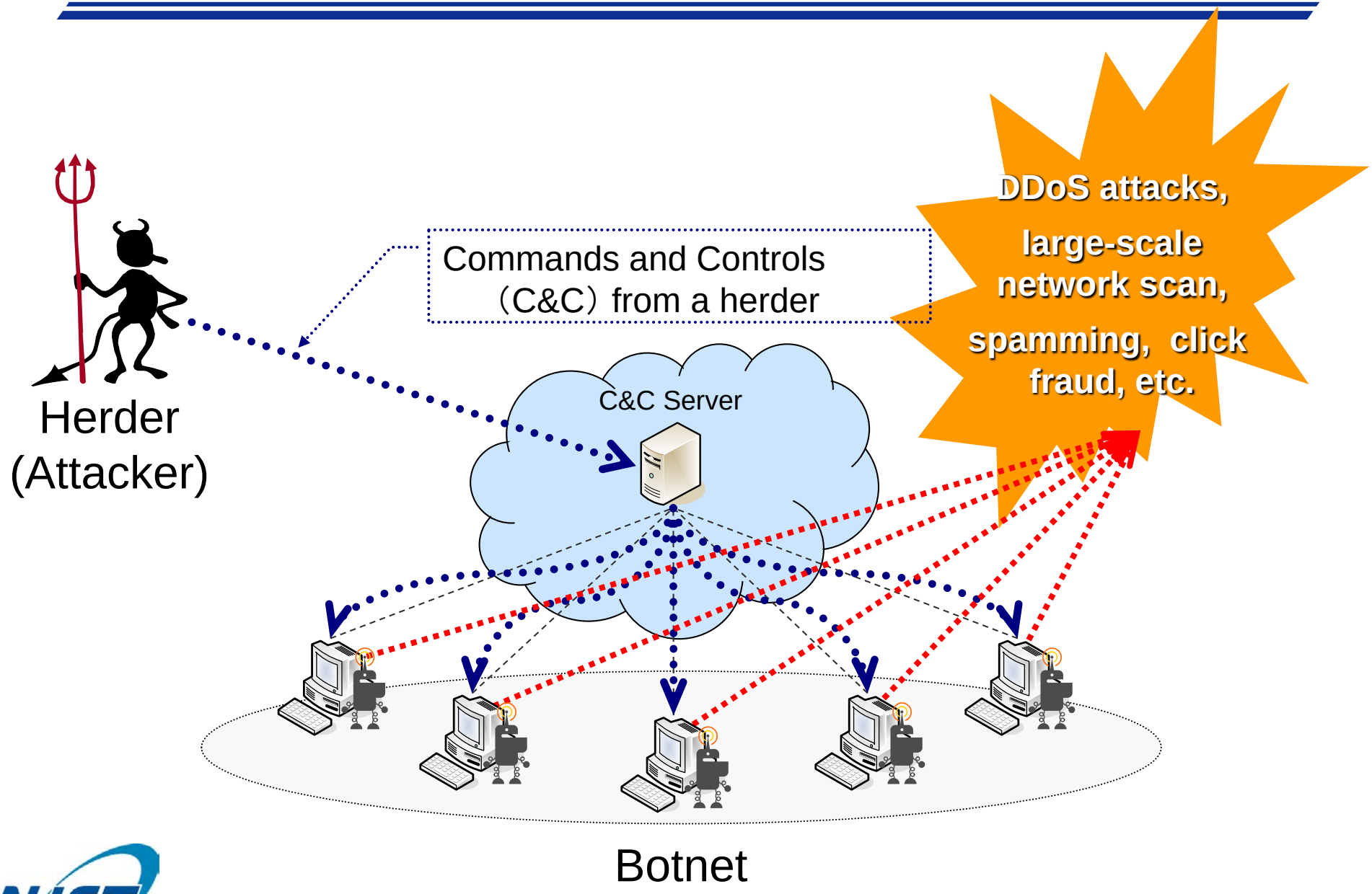
Sample Result



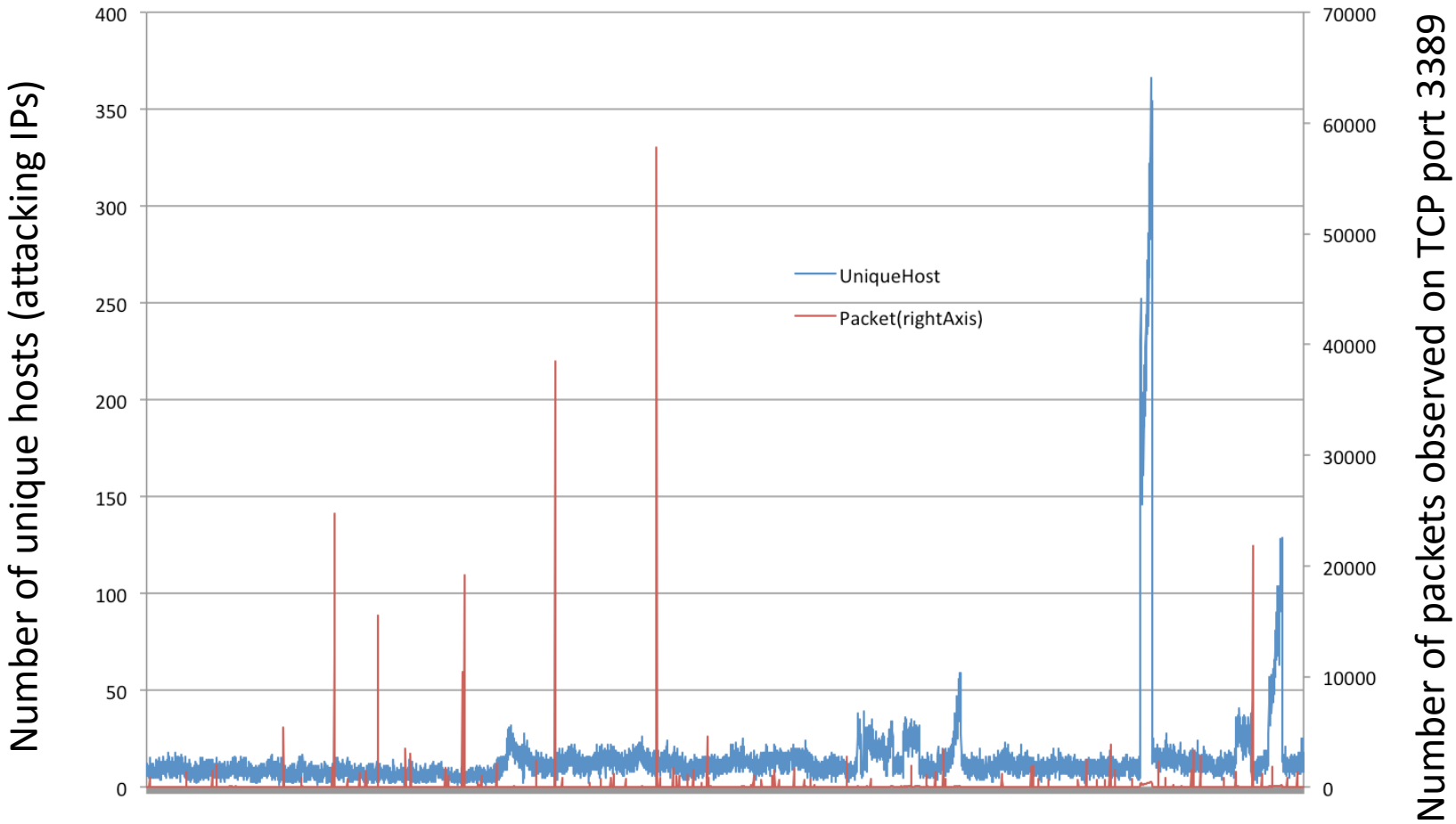
Specifies the type of assumed malware at the infected host. That is, “scan” observed in the darknet may be sent from the malware.

Botnet Activity Detection

A Serious Threat: Botnets

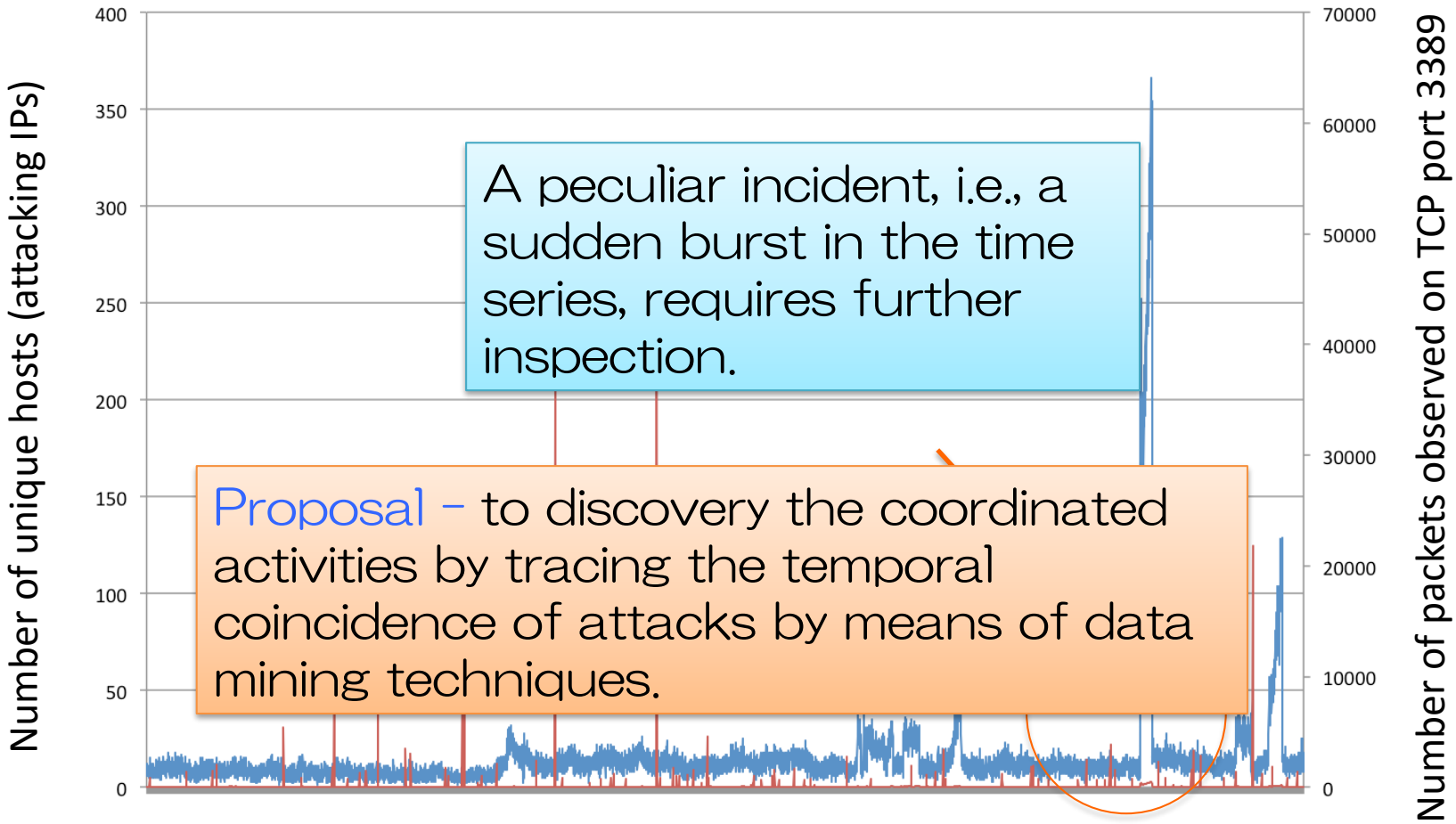


Attacks Observed in the Darknet



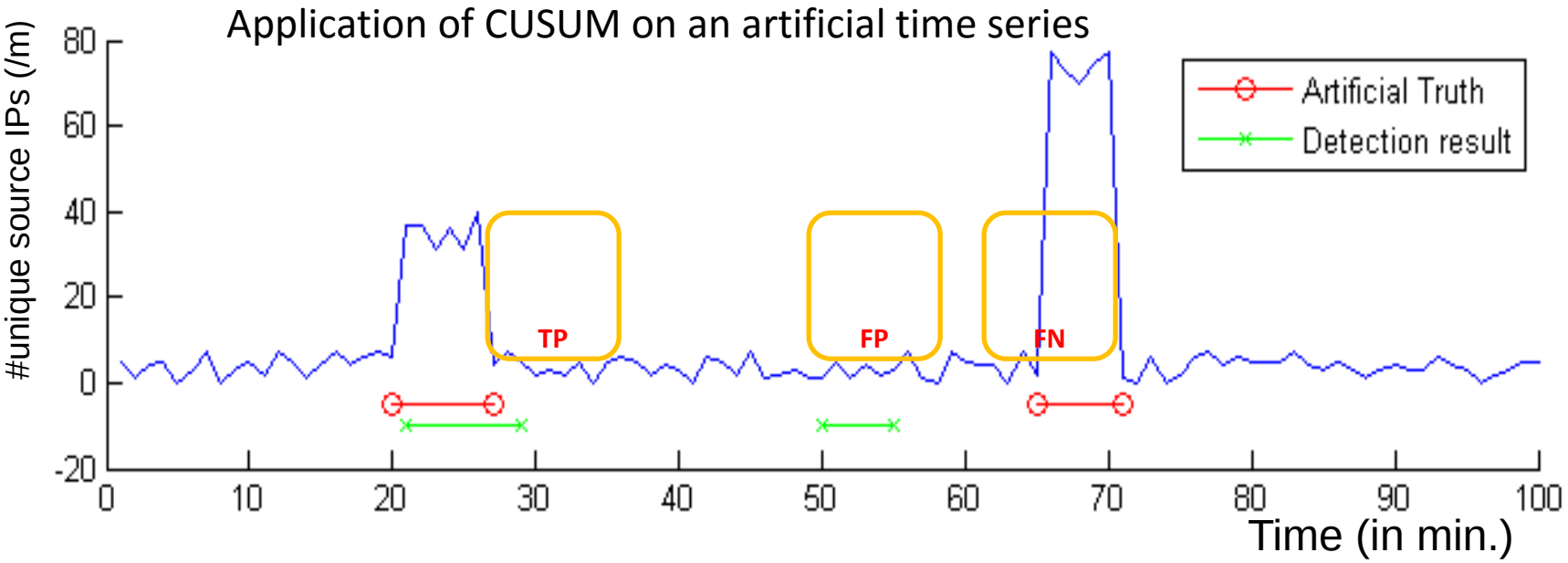
A case study: TCP_SYN packets statistics observed on port 3389.
(Data collected from 2011.7.1 to 2011.8.4 on a /16 darknet sensor.)

Attacks Observed in the Darknet



A case study: TCP_SYN packets statistics observed on port 3389.
(Data collected from 2011.7.1 to 2011.8.4 on a /16 darknet sensor.)

Methodology: Active Epoch Detection



- **Step 1:** Application of a modified Cumulated Sum (CUSUM) algorithm [1] to the number of unique source IP time series for detecting the abrupt changes associated with coordinated attack events, i.e., **active epochs**, of botnets.
- **Step 2:** Filtering and justification of the epoch detection results by removing insignificant events caused by noises and justify the starting and ending times.

[1] T. L. Lai. Sequential Changepoint Detection in Quality-Control and Dynamical Systems. Journal of Royal Statistical Society - Series B. vol. 57, no. 4, pages 613–658, 1995.

Case Study on Port 139

Service on the port

- NetBIOS (Network Basic Input/Output System)
- It provides services related to the session layer of the OSI model allowing applications on separate computers to communicate over a local area network.
- Typically used for file/printer sharing, including directory replication with Active Directory, trusts, remote access of event logs, etc.

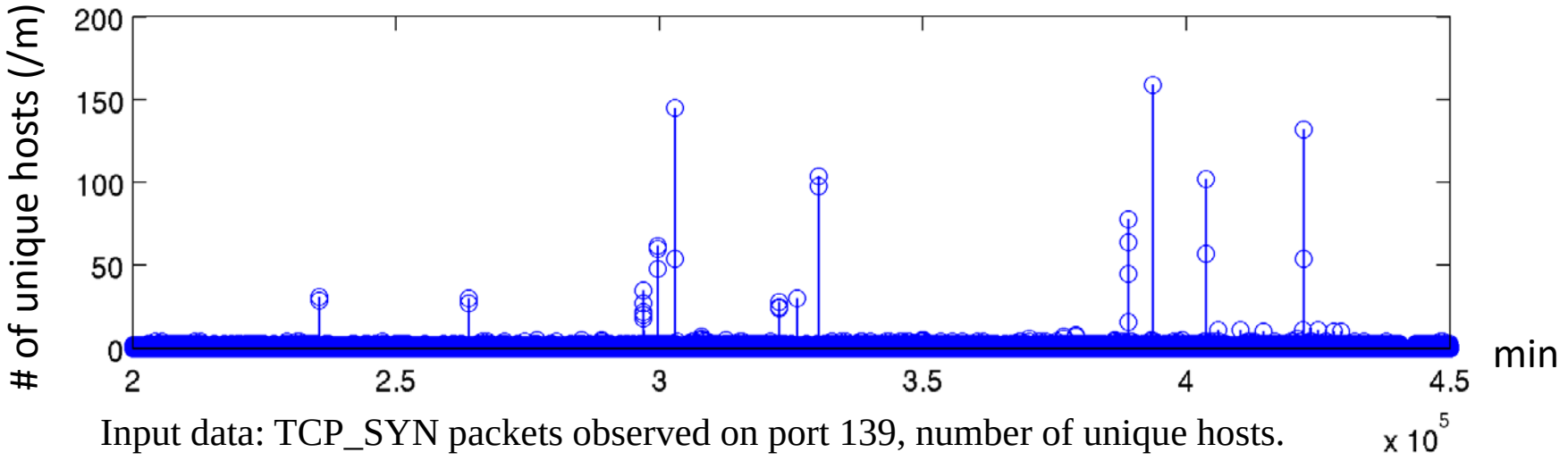
Vulnerability on the port

- When port 445 and port 139 are both on, the Windows system automatically starts SMB-service

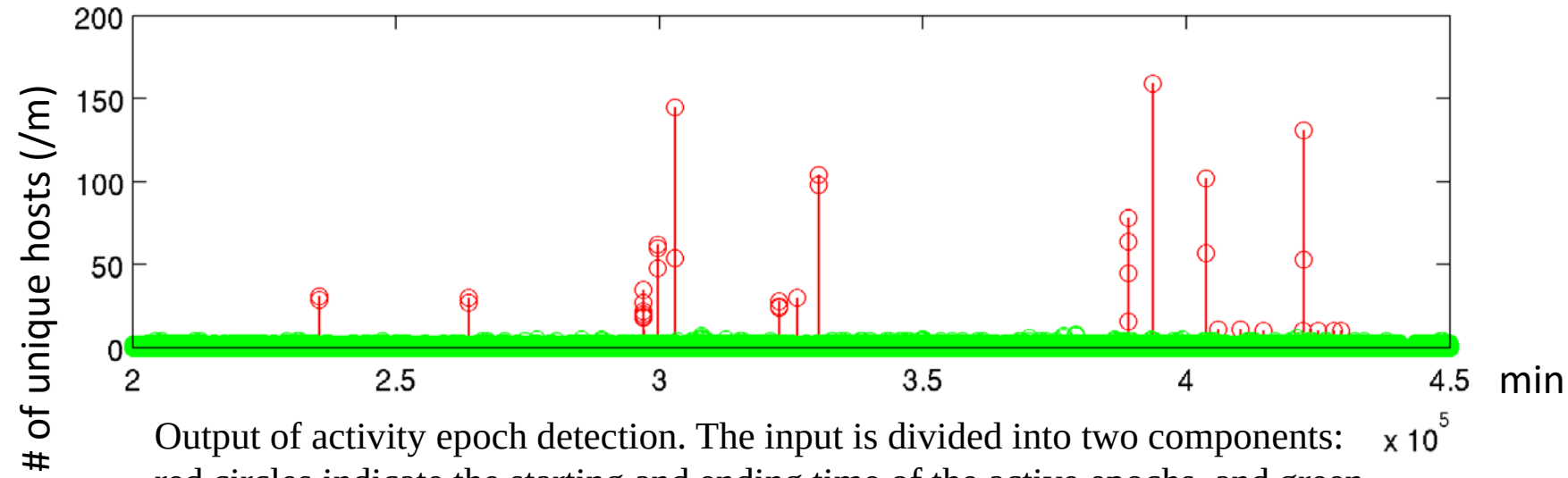
Statistics

- 20 coordinated attacks from botnets are discovered in 2011
- Maximum observed hosts in an attack event: 160+

Result of Active Epoch Detection

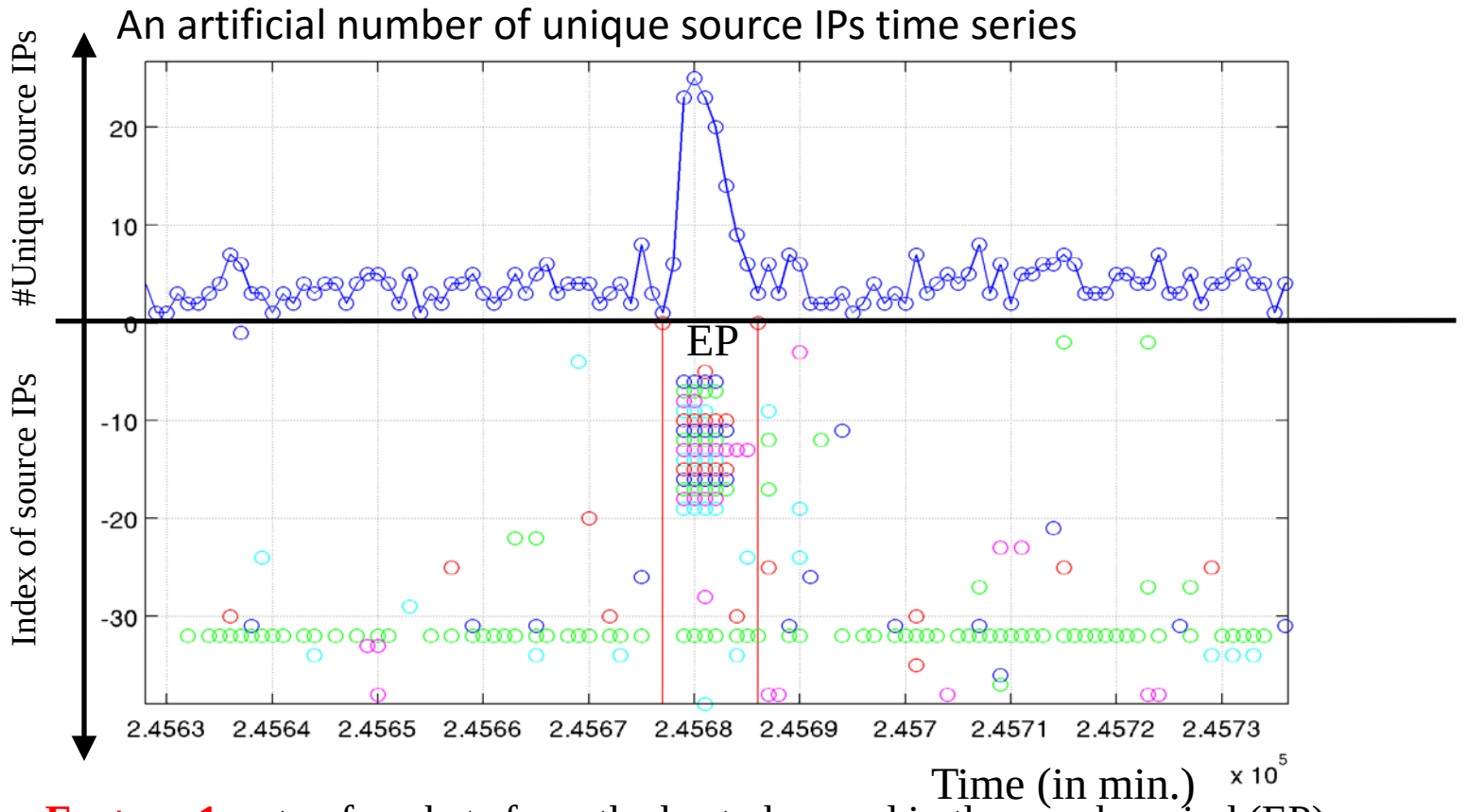


Input data: TCP_SYN packets observed on port 139, number of unique hosts.



Output of activity epoch detection. The input is divided into two components: red circles indicate the starting and ending time of the active epochs, and green circles indicates observations without botnet activities detected.

Coordination-based Feature Extraction



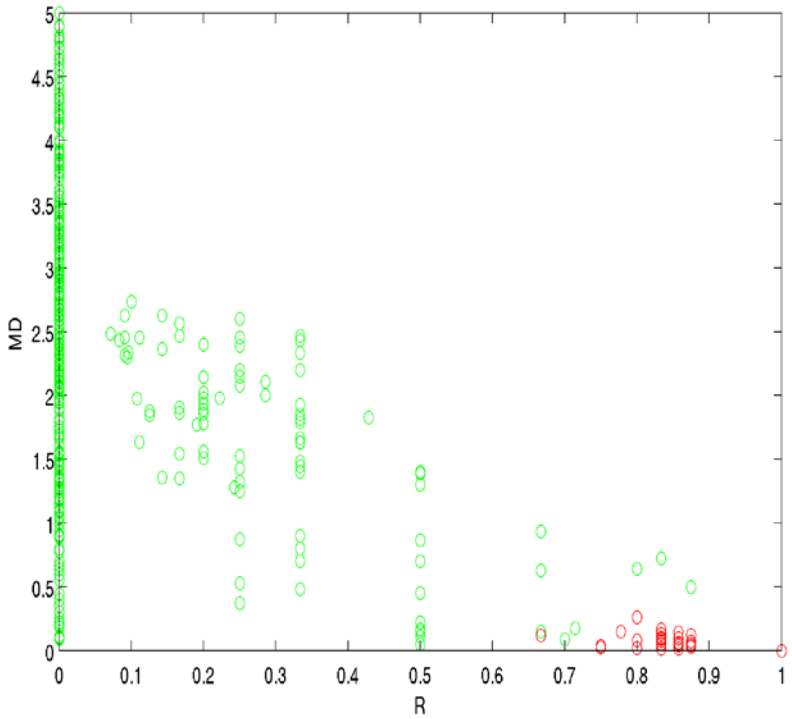
Feature 1: rate of packets from the host observed in the epoch period (EP),

R = (N_e in EP) / N, where N is the number of packets observed in the time window (size =11EP.) embracing EP.

Feature 2: average deviation of all packets from the epoch normalized by EP length,

MD = mean(d_i) / length(EP) , where d_i = min(abs(t_i-Ep_s), abs(t_i-EP_e)), EP_s and EP_e are the starting and ending times of the active epoch.

Bot Classification



Scatter plot in the 2D space

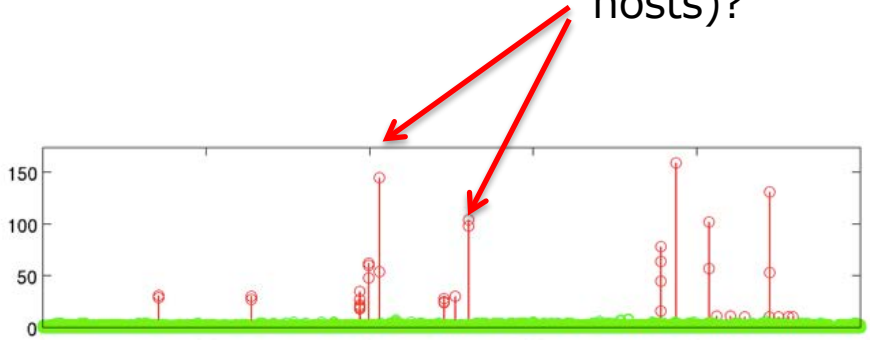
Port	Sensor	Coordination Features	Flow Features [2]
5900	1	99.59%	42.36%
5900	2	99.78%	47.21%
1433	1	100%	96.61%
1433	2	100%	92.84%
25	1	99.58%	81.91%
25	2	99.61%	89.78%
139	1	100%	79.12%
8506	1	99.44%	0
3389	1	99.90%	57.86%

G-mean values obtained by Support Vector Machine. Results of 5-fold cross validation with optimal parameters are reported.

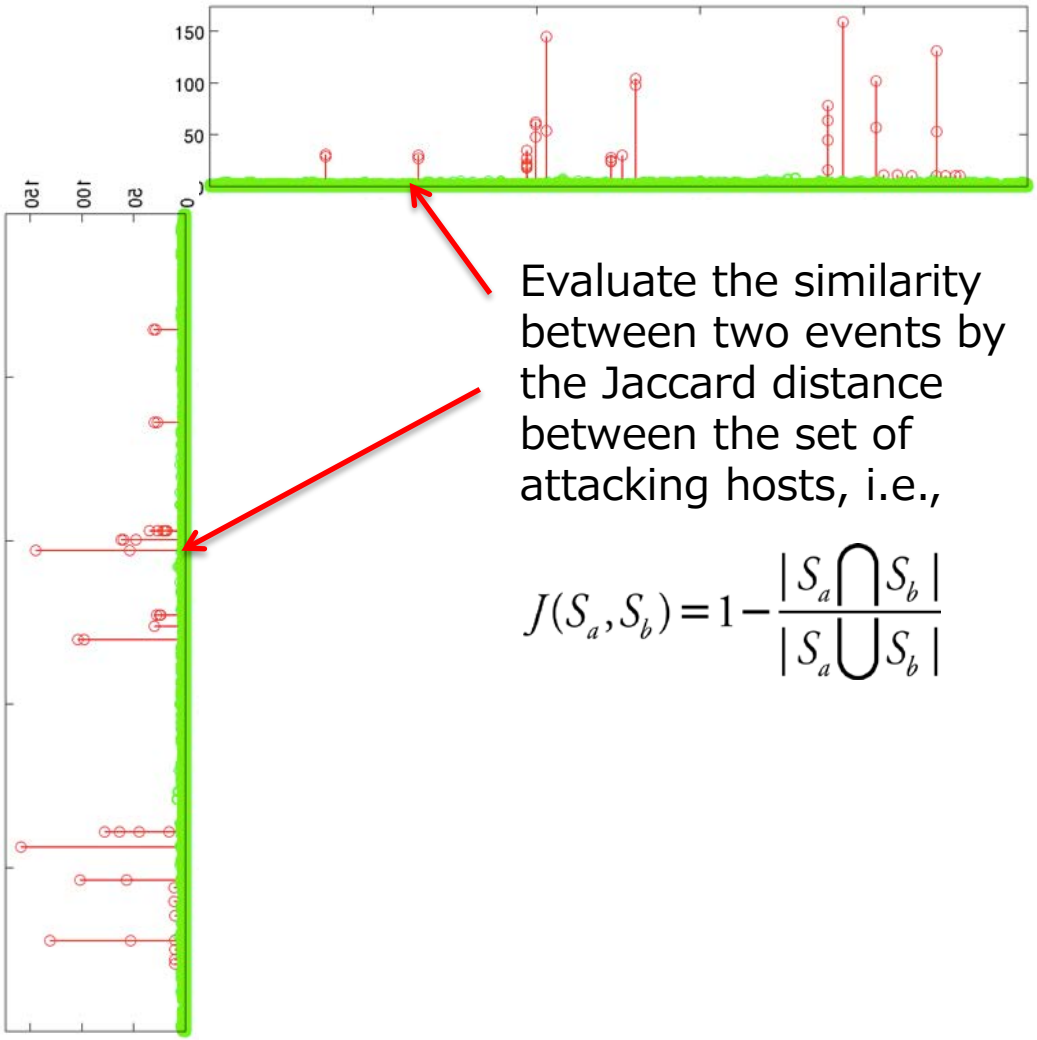
[2] T. Ban, et at., Behavior analysis of long-term cyber attacks in the darknet, ICONIP'12 Proceedings of ICONIP'12, Volume 7667, Part V, Pages 620-628.

Correlation Analysis between Active Epochs

How do attacks performed at different time relate to each other? Are they from the same botnet (group of attacking hosts)?



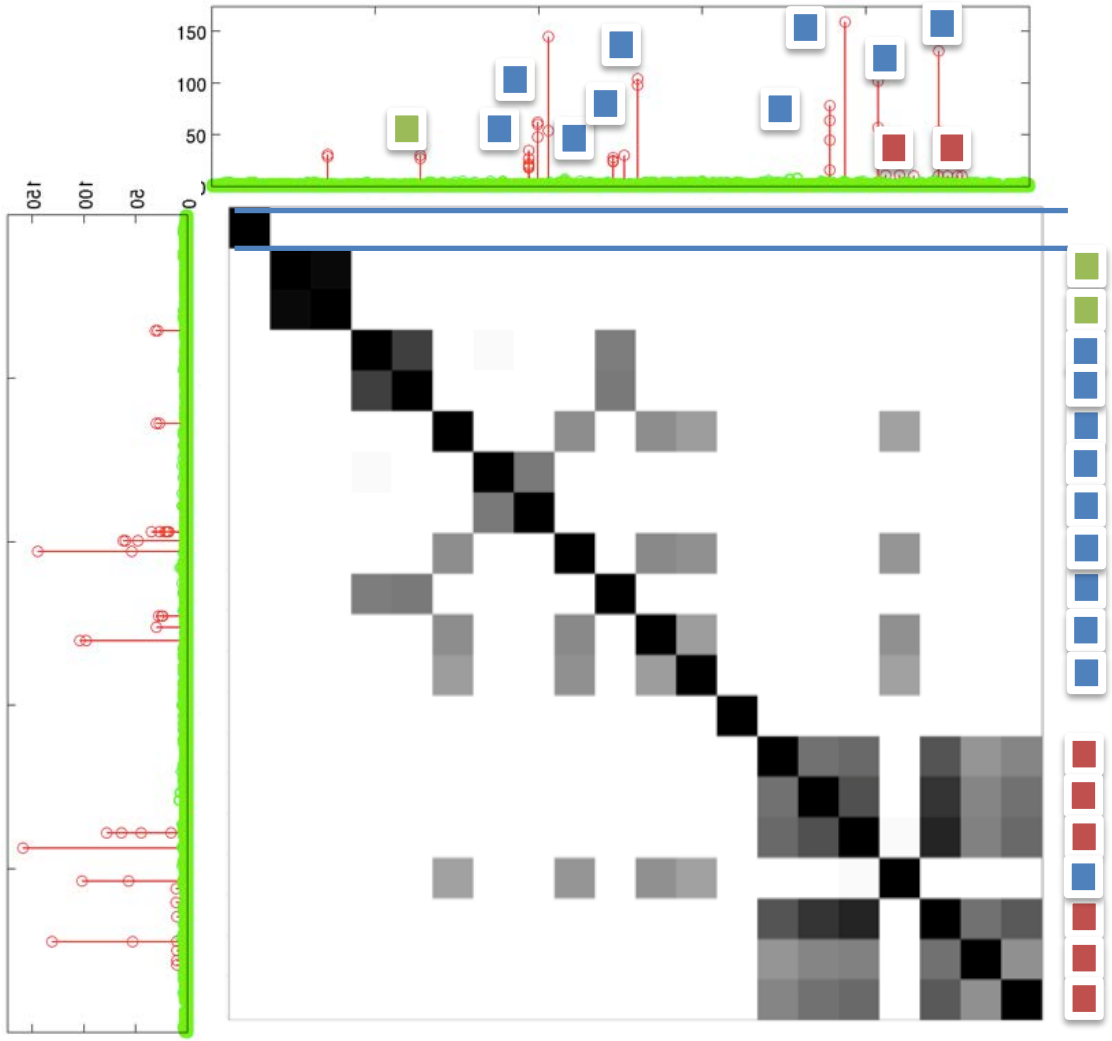
Correlation Analysis between Active Epochs



Evaluate the similarity between two events by the Jaccard distance between the set of attacking hosts, i.e.,

$$J(S_a, S_b) = 1 - \frac{|S_a \bigcap S_b|}{|S_a \bigcup S_b|}$$

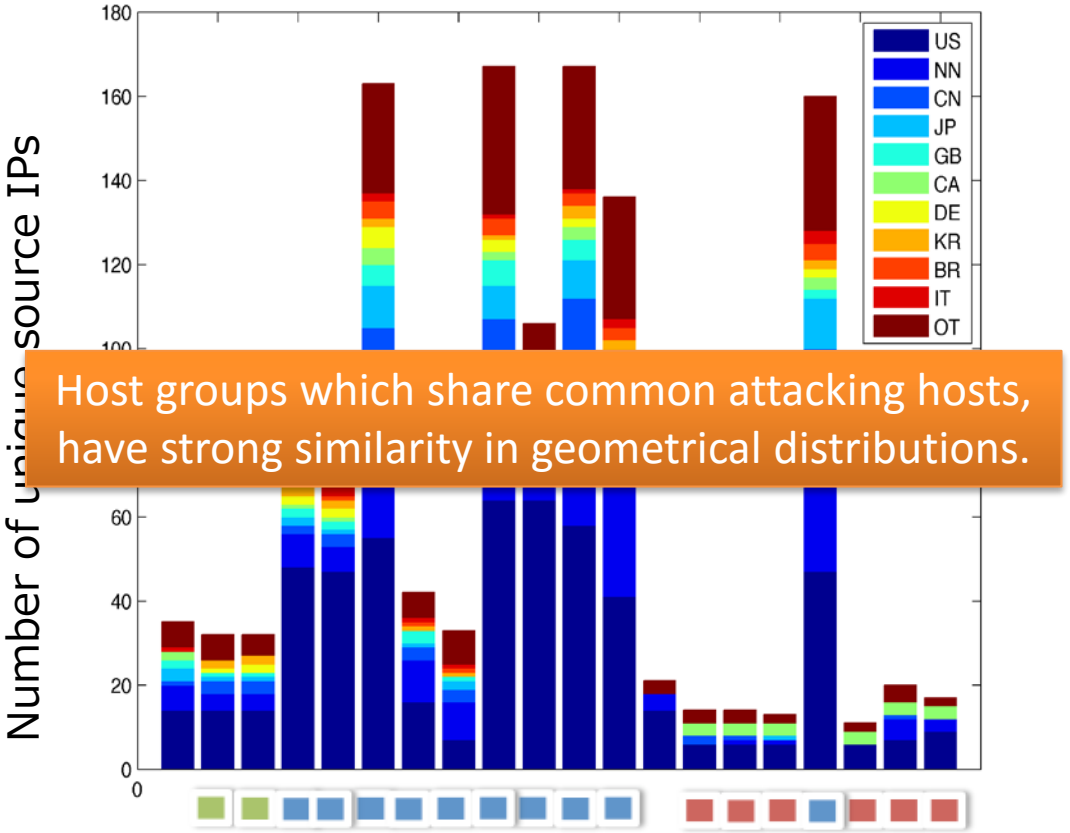
Correlation Analysis between Active Epochs



Similarity between S_1 an S_i, i = 1,⋯,m

Variations on Geo-distribution on Port 139

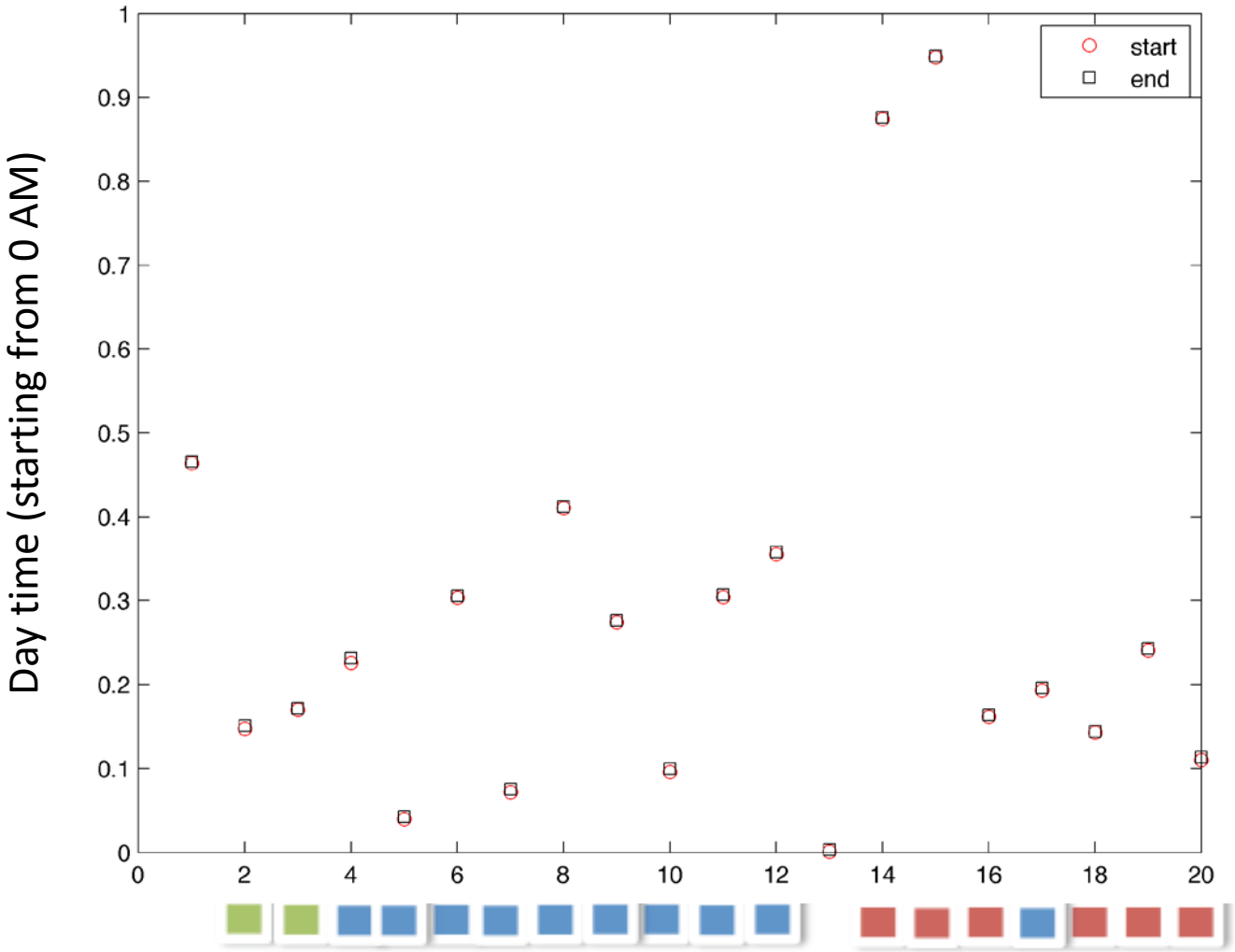
Stacked plot of geo-locations of source IPs in the active epochs detected on destination port 139, 2011.



Index of the 20 detected active epochs.

To Geo-locate the Attackers

Diurnal attacking time observed on destination port 139

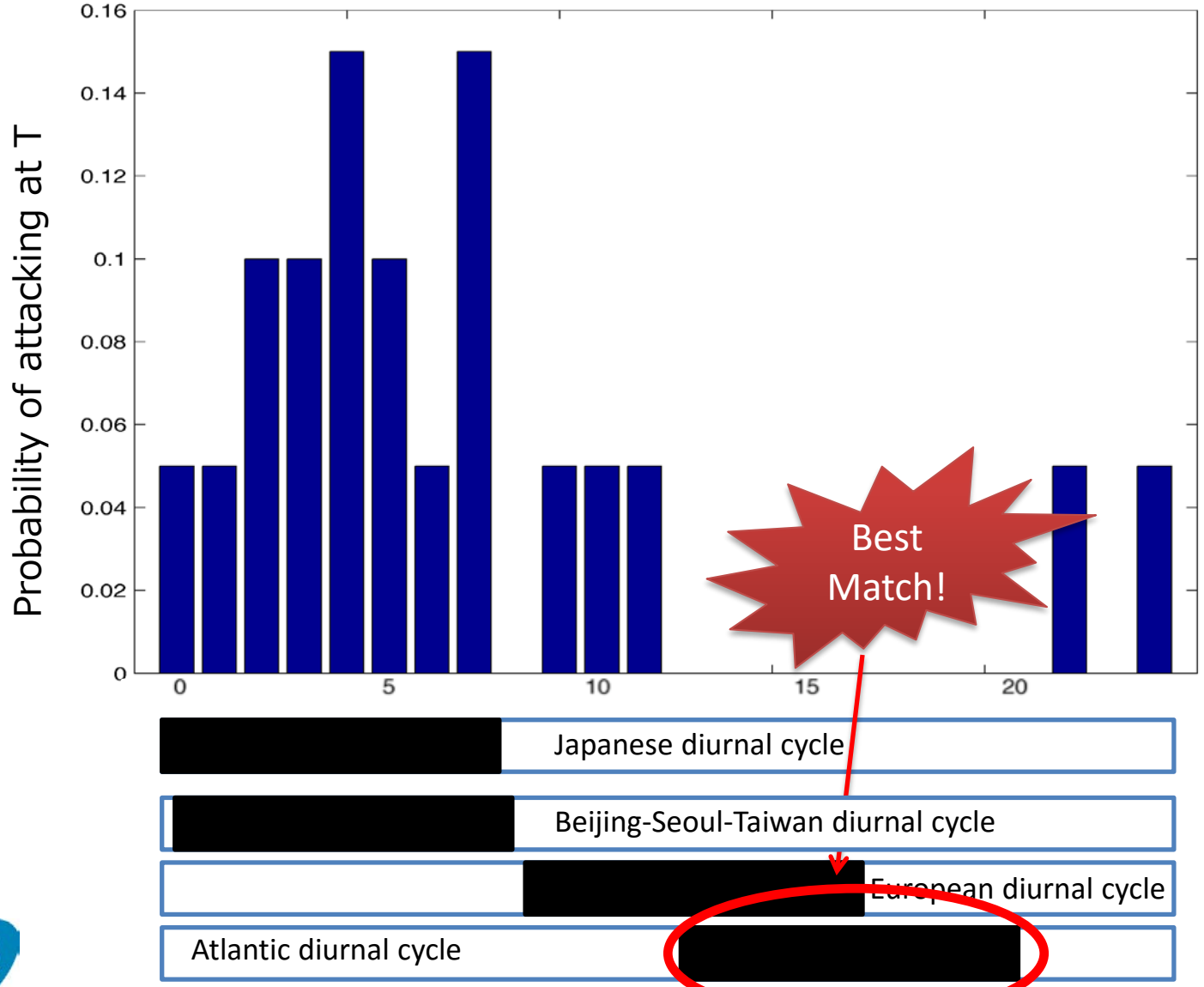


Index of the 20 active epochs.

NICTER

To Geo-locate the Attackers on DPort 139

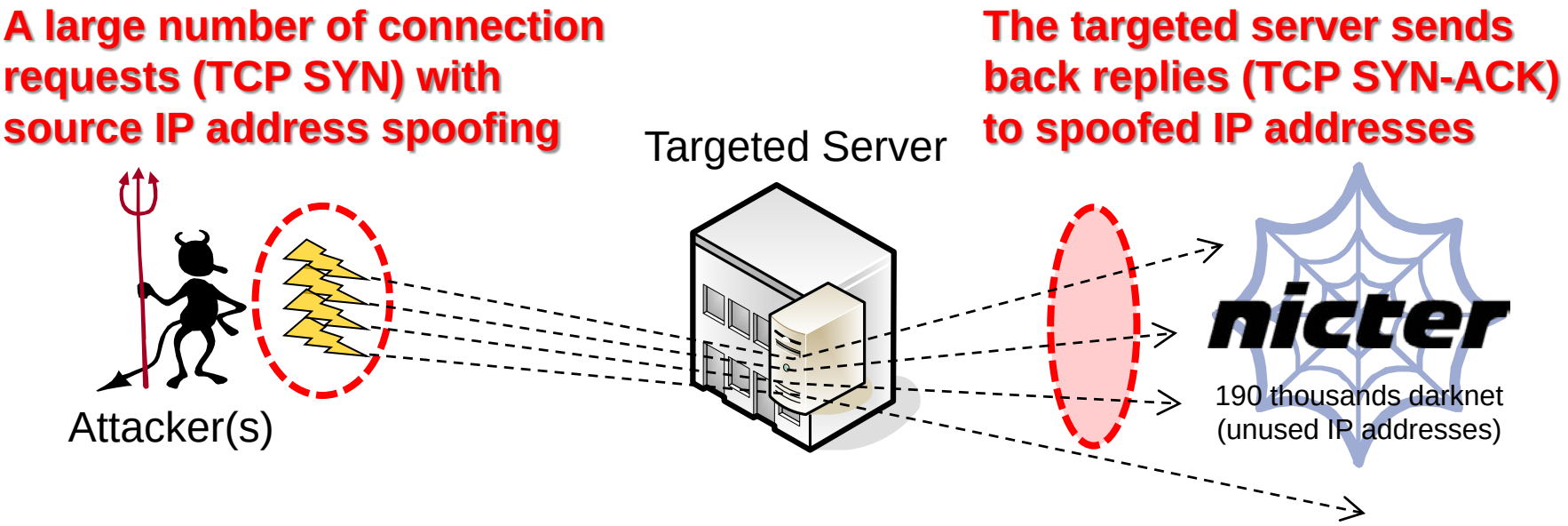
A “strong” assumption: attacks are performed by an attacker who has a “healthy” life cycle.



NICTER

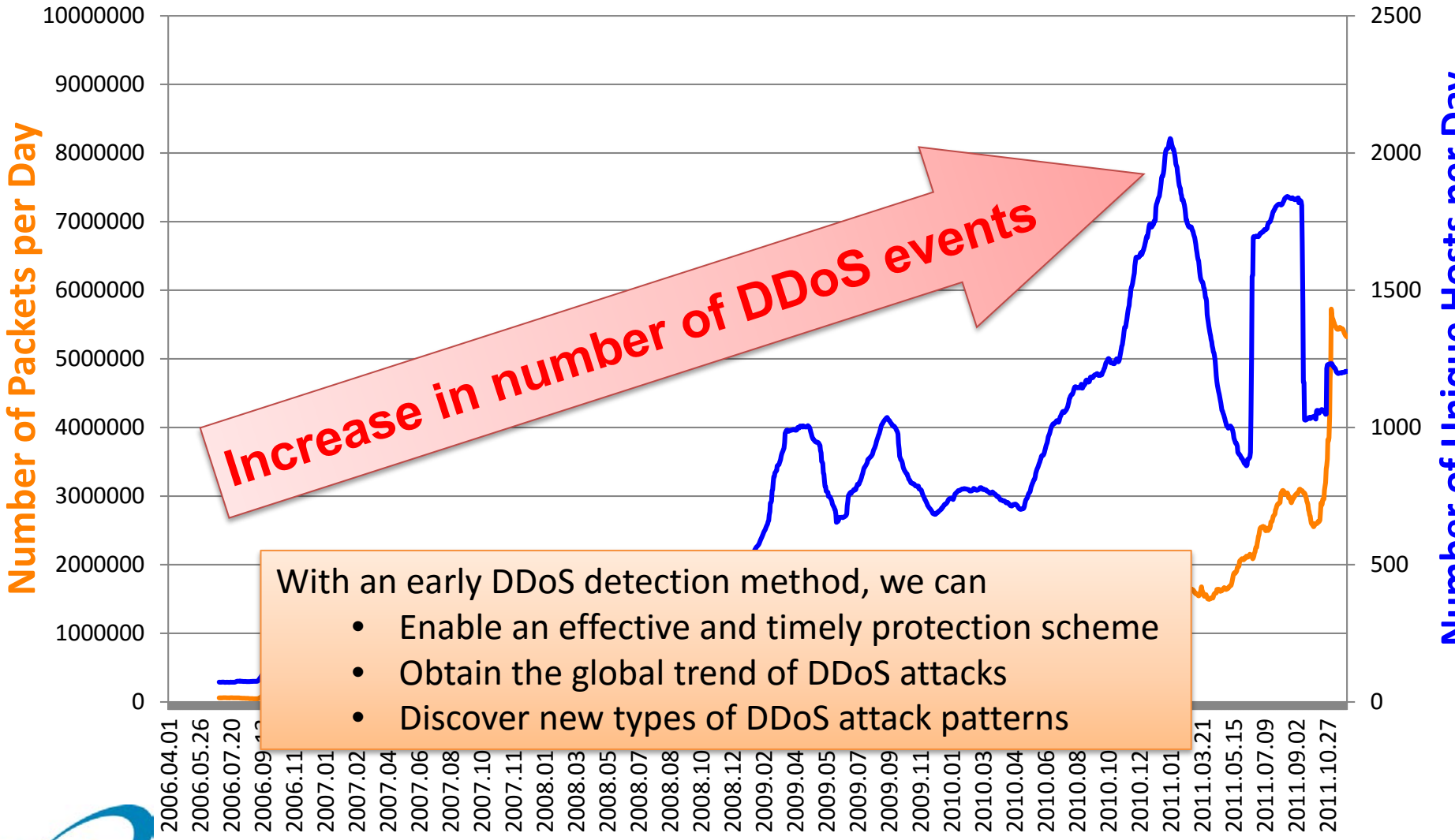
Early DDoS Event Detection

Backscatter: Reflections of DDoS Attacks



- Backscatter packets from DDoS-attacked hosts constitute a considerable proportion of darkent traffic.
- Darknet provides a unique view point to detect DDoS incidents in early stage at very low cost.

Long-term Observation of Backscatters

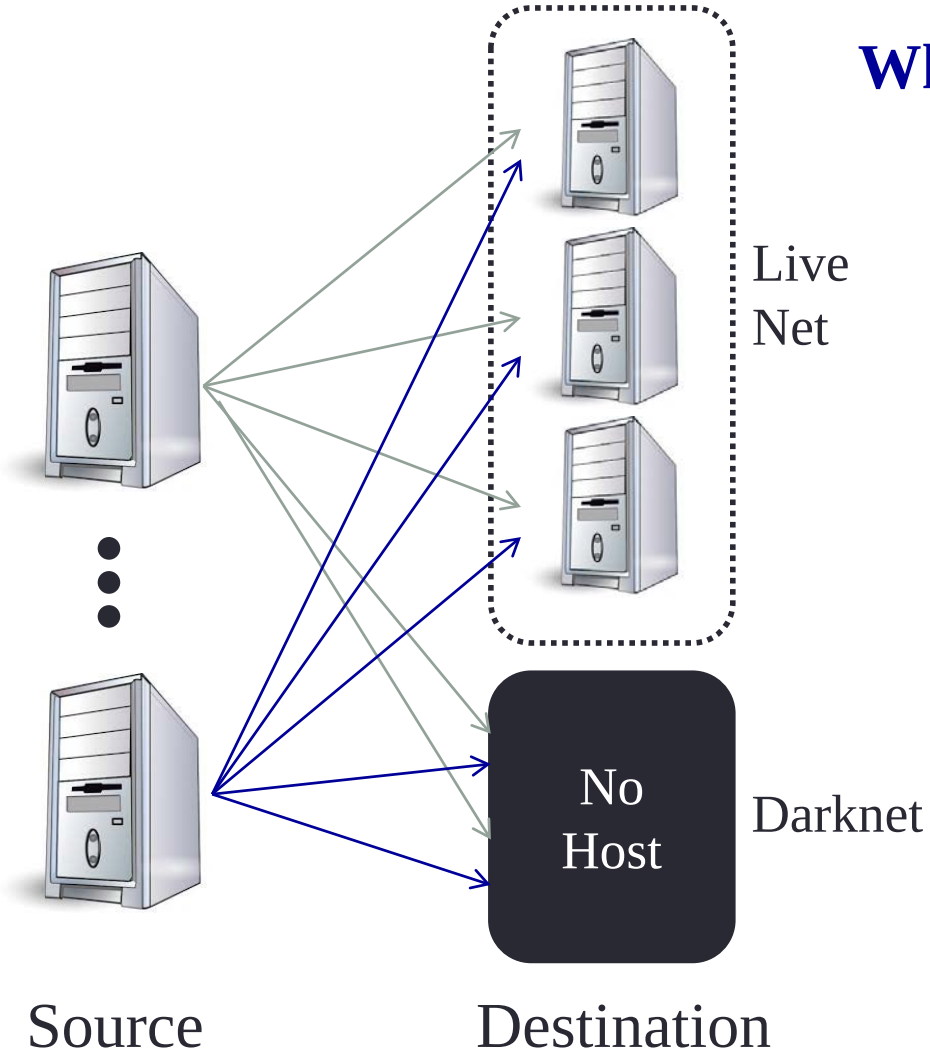


With an early DDoS detection method, we can

- Enable an effective and timely protection scheme
- Obtain the global trend of DDoS attacks
- Discover new types of DDoS attack patterns

NICTER

Data Collection on Darknet



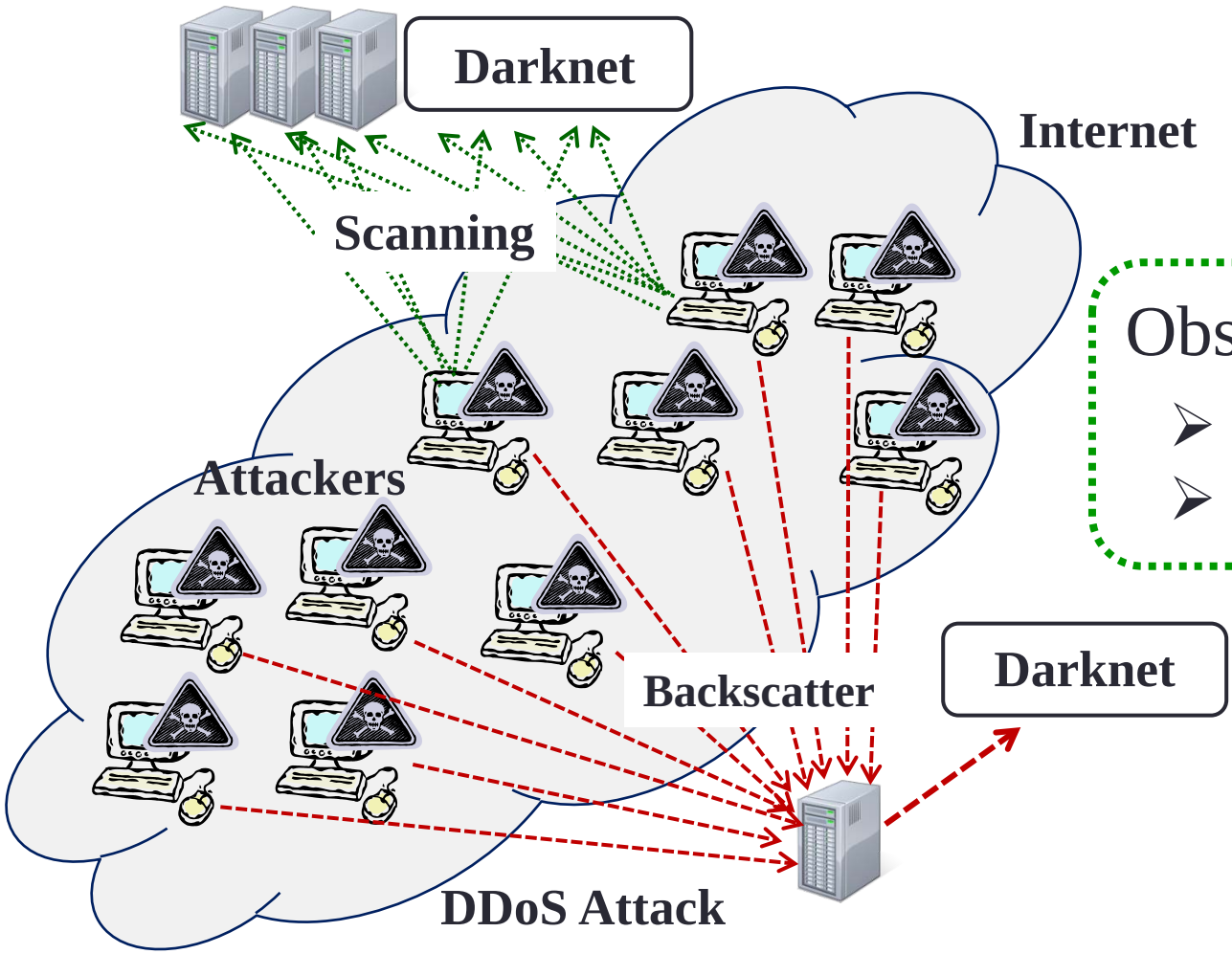
Why do such packets reach?

- Misconfiguration
- Scanning
- Exploit code
- Responses from targeted hosts by DDoS

Malicious Activities

Large-scale monitoring for cyber attacks

What types of attacks can be observed?

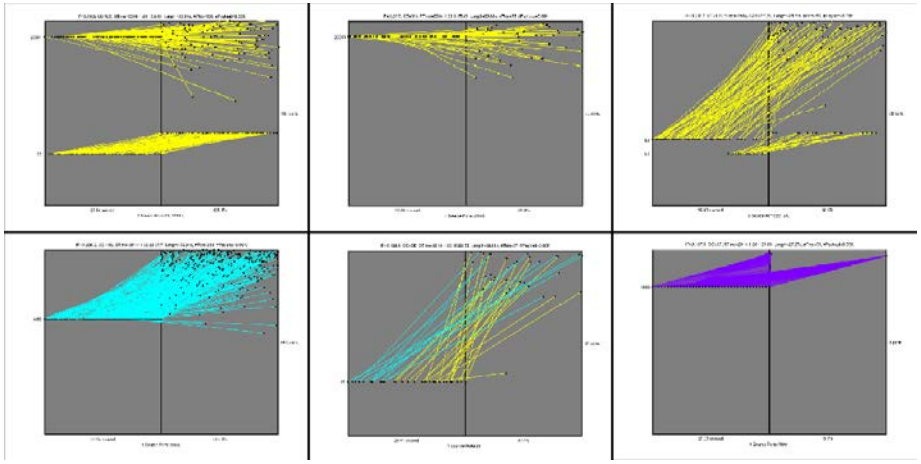


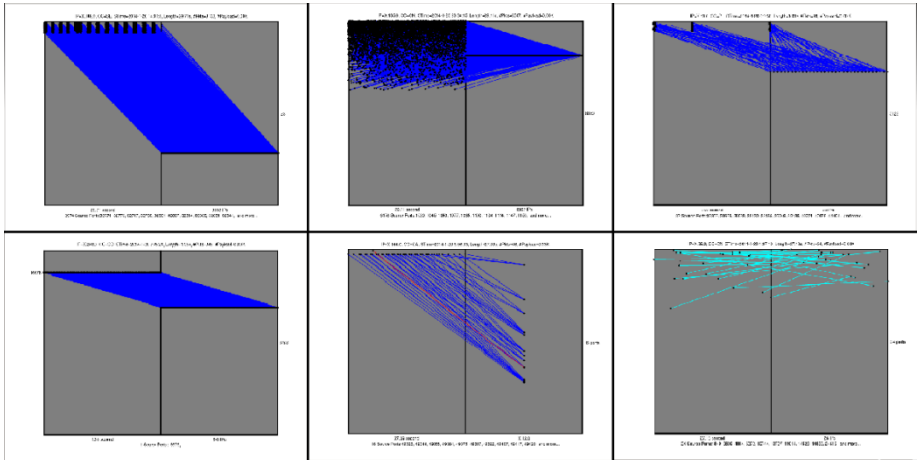
Observable Attacks

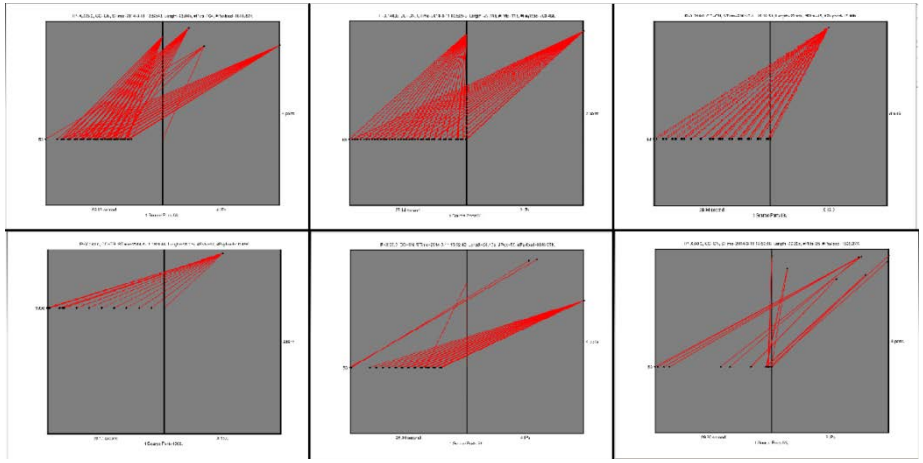
- Scanning
- DDoS

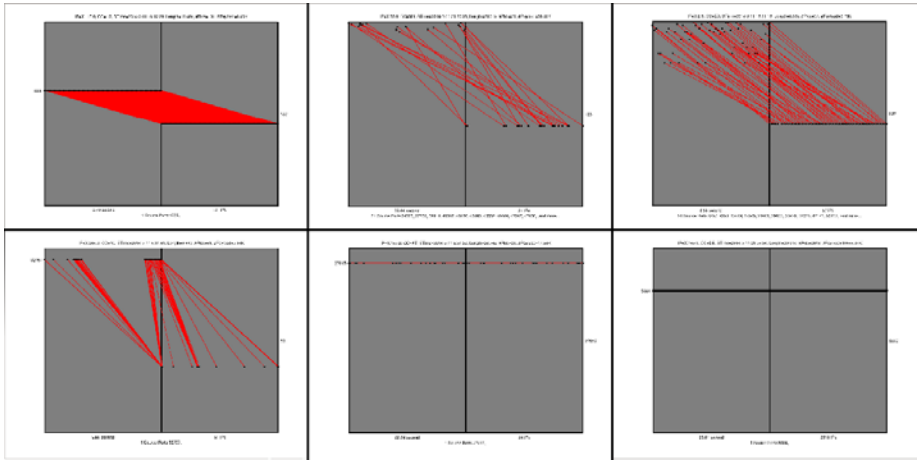
What is good feature representation for darknet traffic?

Tiles (provided by NICT)



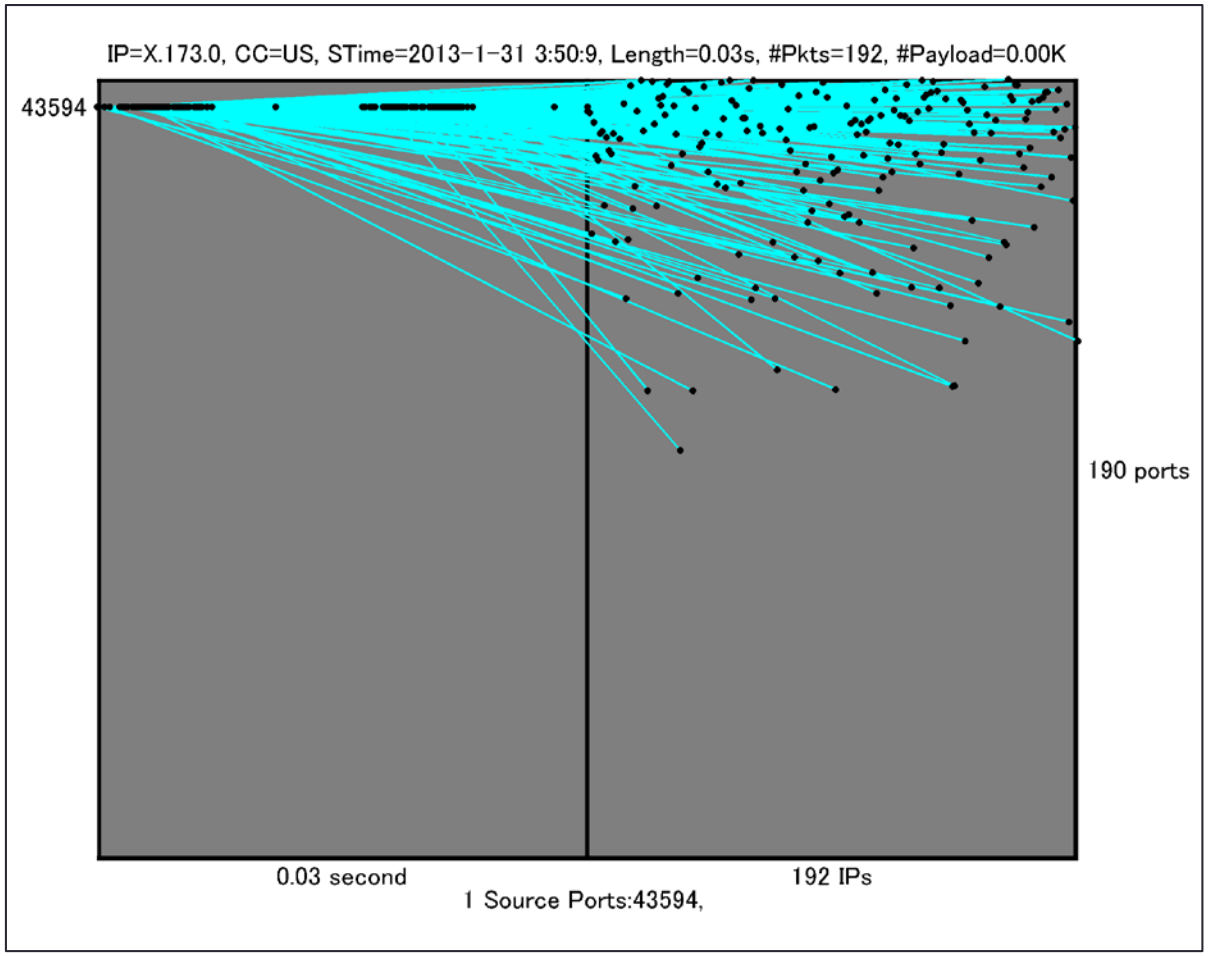






Tile Representation for DDoS Attack

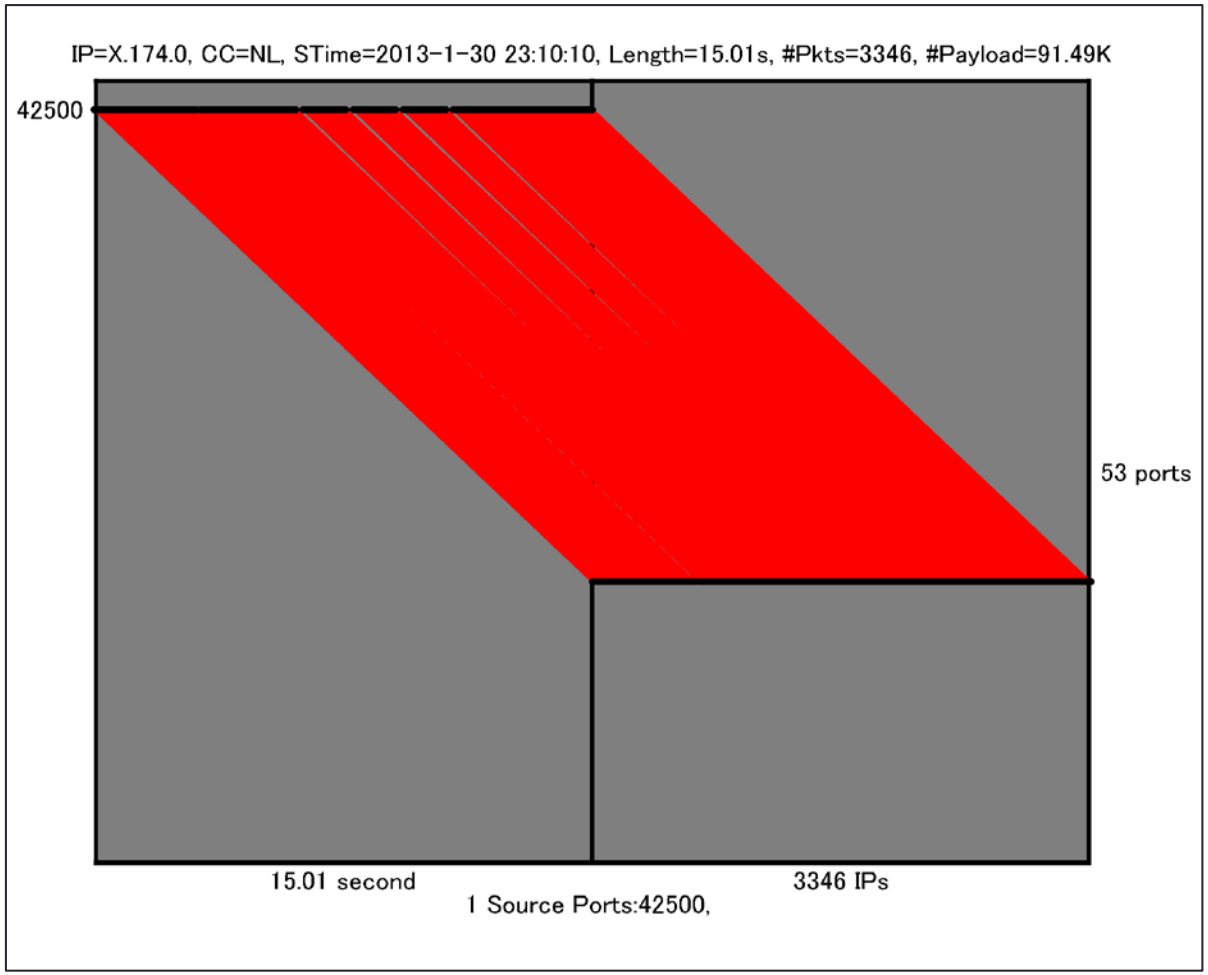
Source Side



Destination Side

Tile Representation for Scanning Attack

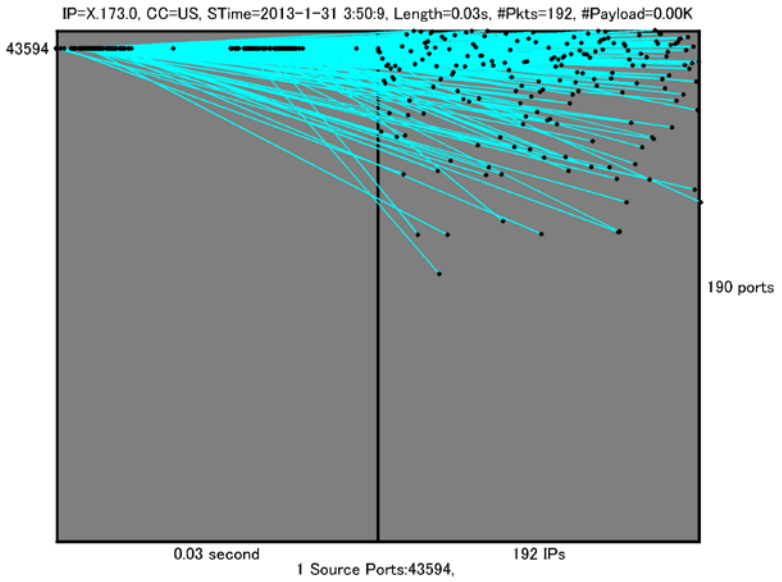
Source Side

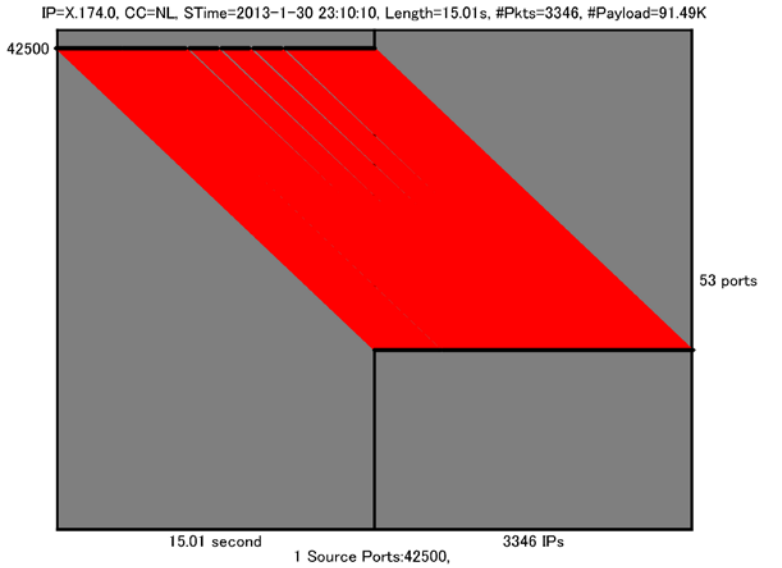


Destination Side

Traffic Features on Tiles

- *#Total Packets*
- Ave and Std of *Time Spans of Packets*
- *#Source Ports*
- Ave and Std of *#Packets from Source Ports*
- #Destination IPs
- Ave and Std of *#Packets from Dest. IPs*
- *#Destination Ports*
- Ave and Std of *#Packets from Dest. Ports*
- Ave and Std of *Spans of Dest. IP Numbers*
- *#Protocol Types*
- Ave and Std of *Payload Sizes*





Making Training Data by Labelling

Should have as much training data as possible. But how?

➔ Who labels? ⇒ Experts
including information on alert sites
(e.g. US-CERT, CERT-UK, CERT-EU)

Labelling Rules = Describe how experts judge as attacks.

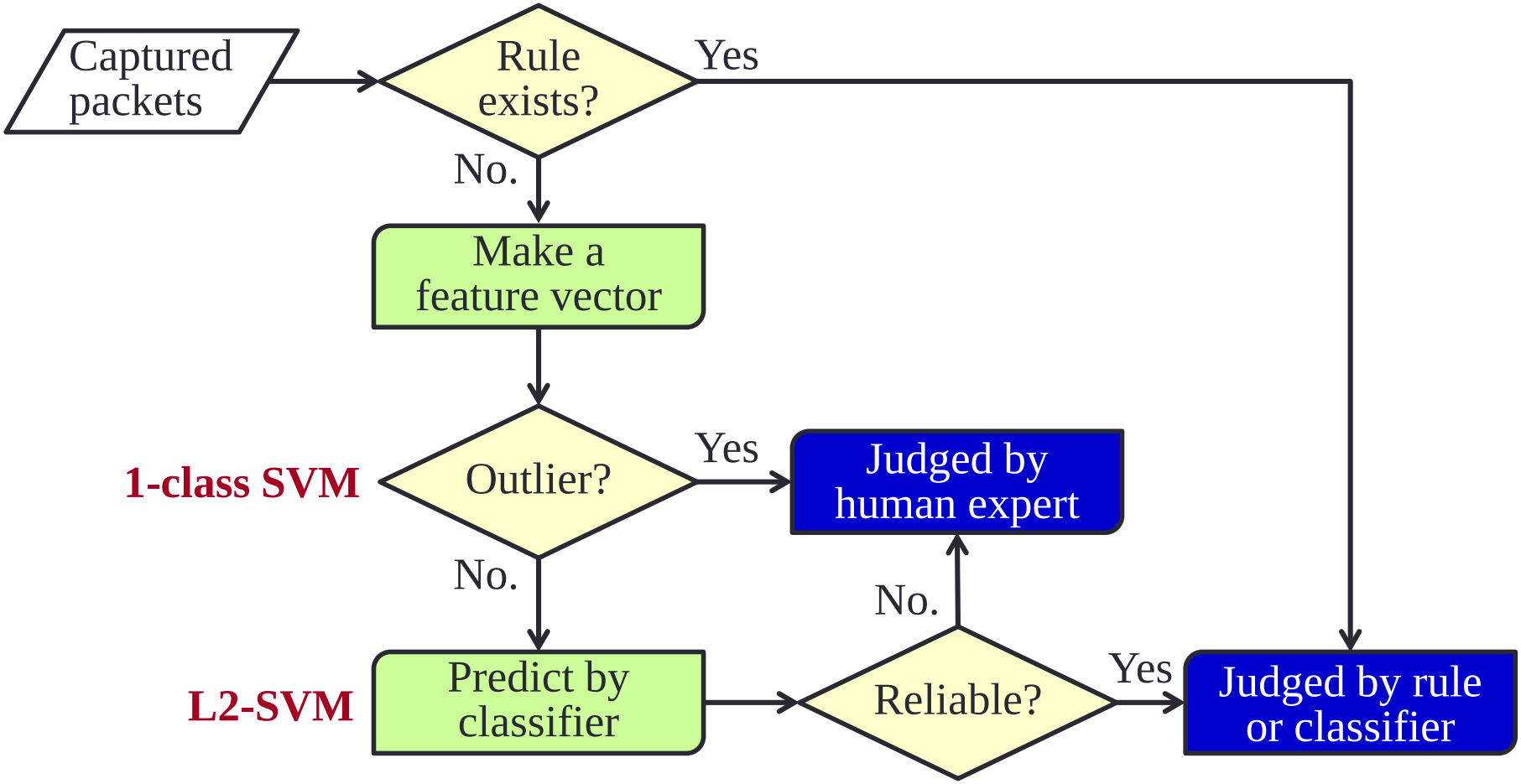
Our belief is that
not all attacks can be described with rules,
but the traffic features between *known and unknown attacks*
have some *similarity*.

Labelling Rules for DDoS Attack

Use knowledge of communication protocol, applications, and nature as reply packets.

Port /Protocol	Rules
80/tcp	Control Flag = SYN-ACK, RST-ACK, or RST
53/udp	Payload includes a domain name.
17/udp	N/A
19/udp	N/A
123/udp	N/A
137/udp	N/A
161/udp	N/A
1900/udp	Response to M-SEARCH messages in SSDP attack

Learning Scheme for Detecting DDoS Attacks



Experimental Setup

- **Darknet Packets**:
  - collected by NICT
  - 1st January – 30th June, 2014 (181 days) [77,133 data]
  - Only UDP
  - /16 IP space (65,536 destination IPs)

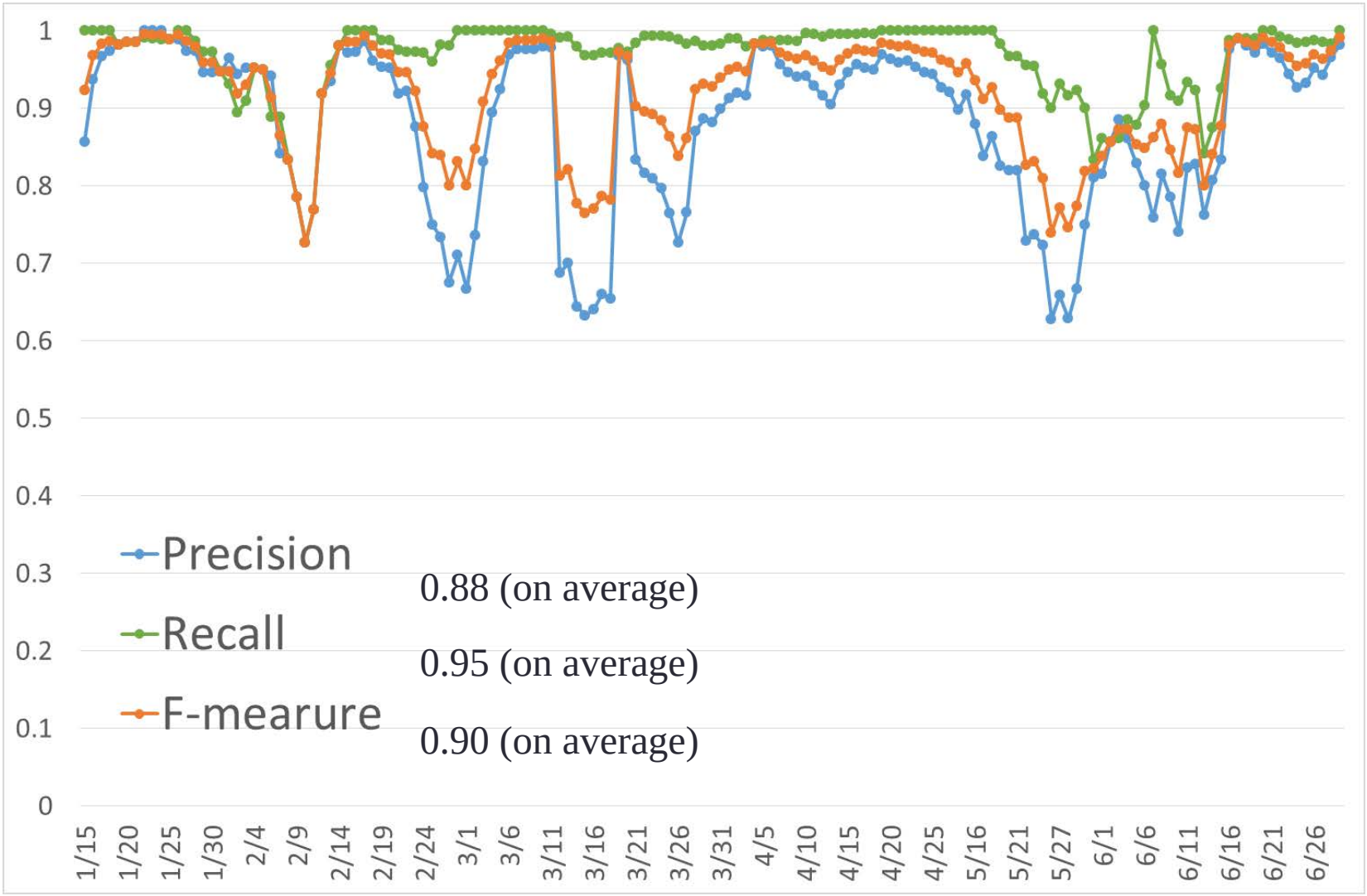
- **Initial Training**:
  - 1st January – 14th January, 2014 (14 days) [8,484 data]
  - Labelled by rules and human experts.

- **Prediction & Online Learning**:
  - Carried out every day after 15th Jan. [68,649 data]
  - Train 1-class SVM & L2-SVM day by day.

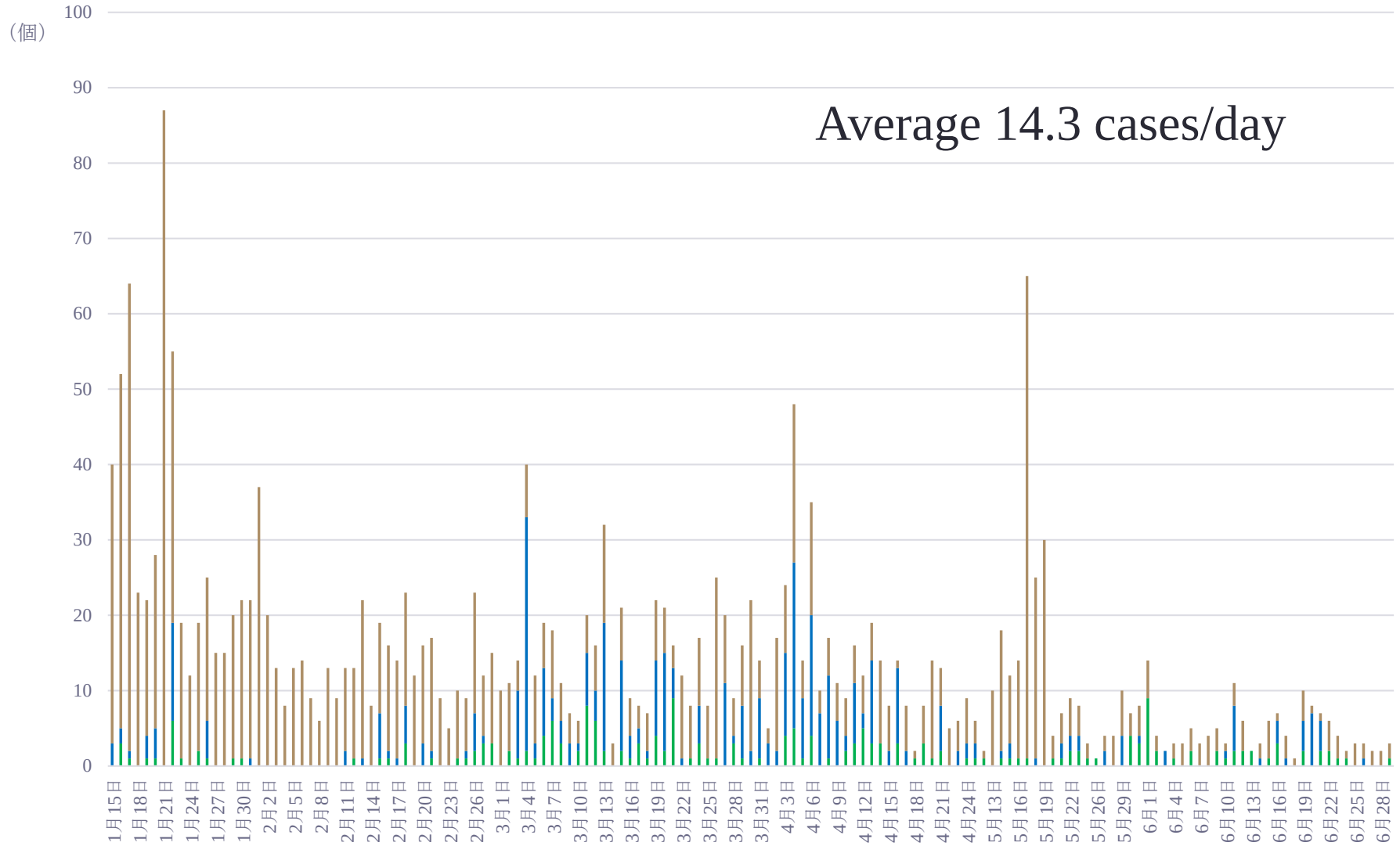
Average Detection Performance

		Precision	Recall	F-Measure
Online Learning	ν=0.100	0.83	0.95	0.87
	ν=0.075	0.88	0.95	0.90
	ν=0.050	0.84	0.95	0.88
	ν=0.025	0.85	0.95	0.88
Learning with Initial Data		0.91	0.70	0.79

DDoS Detection Performance (7-days moving average)



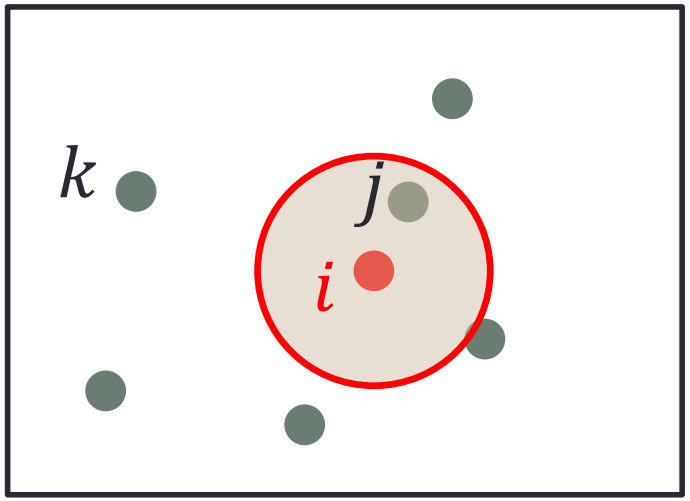
How many cases do operators handle?



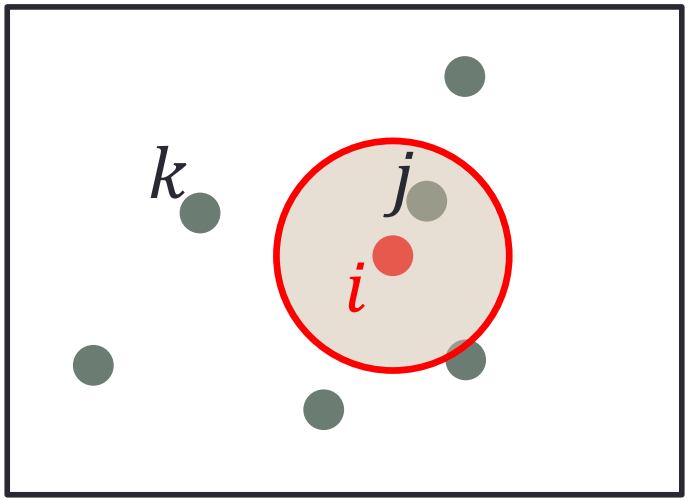
Visualization of Cyberattacks

Stochastic Neighbor Embedding (SNE)

High-D



Low-D



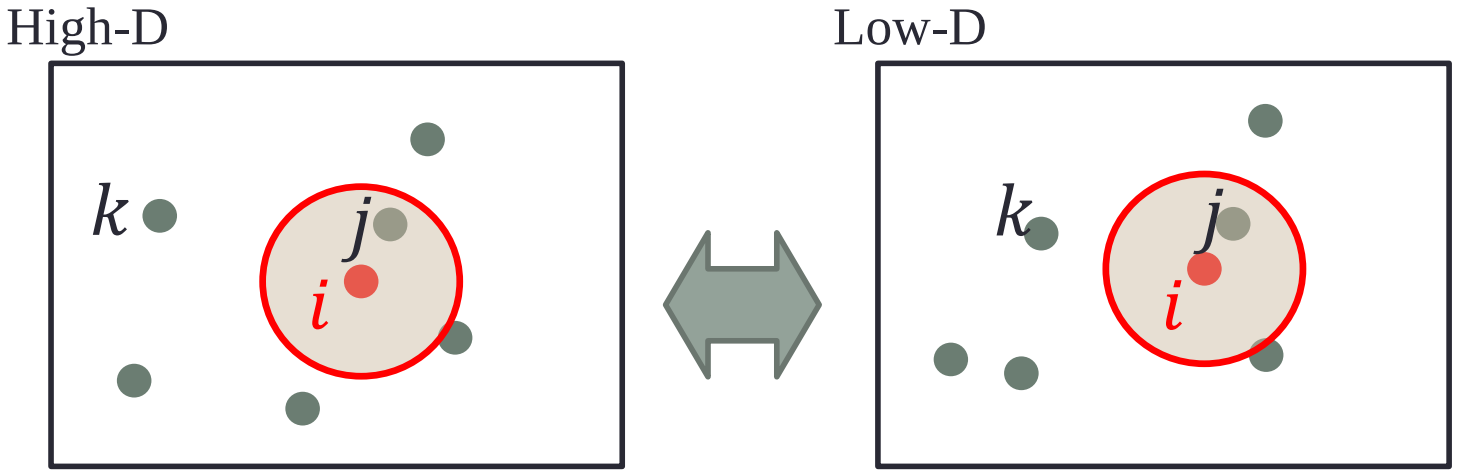
$$p_{j|i} = \frac{\exp\left(-\|x_i - x_j\|^2 / 2\sigma_i^2\right)}{\sum_{k \neq i} \exp\left(-\|x_i - x_k\|^2 / 2\sigma_i^2\right)}$$

$$q_{j|i} = \frac{\exp\left(-\|y_i - y_j\|^2\right)}{\sum_{k \neq i} \exp\left(-\|y_i - y_k\|^2\right)}$$

Probability of picking j as a neighbor of i

$$Cost = \sum_i KL(P_i \,\|\, Q_i) = \sum_i \sum_j p_{j|i} \log \frac{p_{j|i}}{q_{j|i}}$$

t-SNE (van der Maaten, 2008)



$$p_{j|i} = \frac{\exp\left(-\|x_i - x_j\|^2 / 2\sigma_i^2\right)}{\sum_{k \neq i} \exp\left(-\|x_i - x_k\|^2 / 2\sigma_i^2\right)}$$

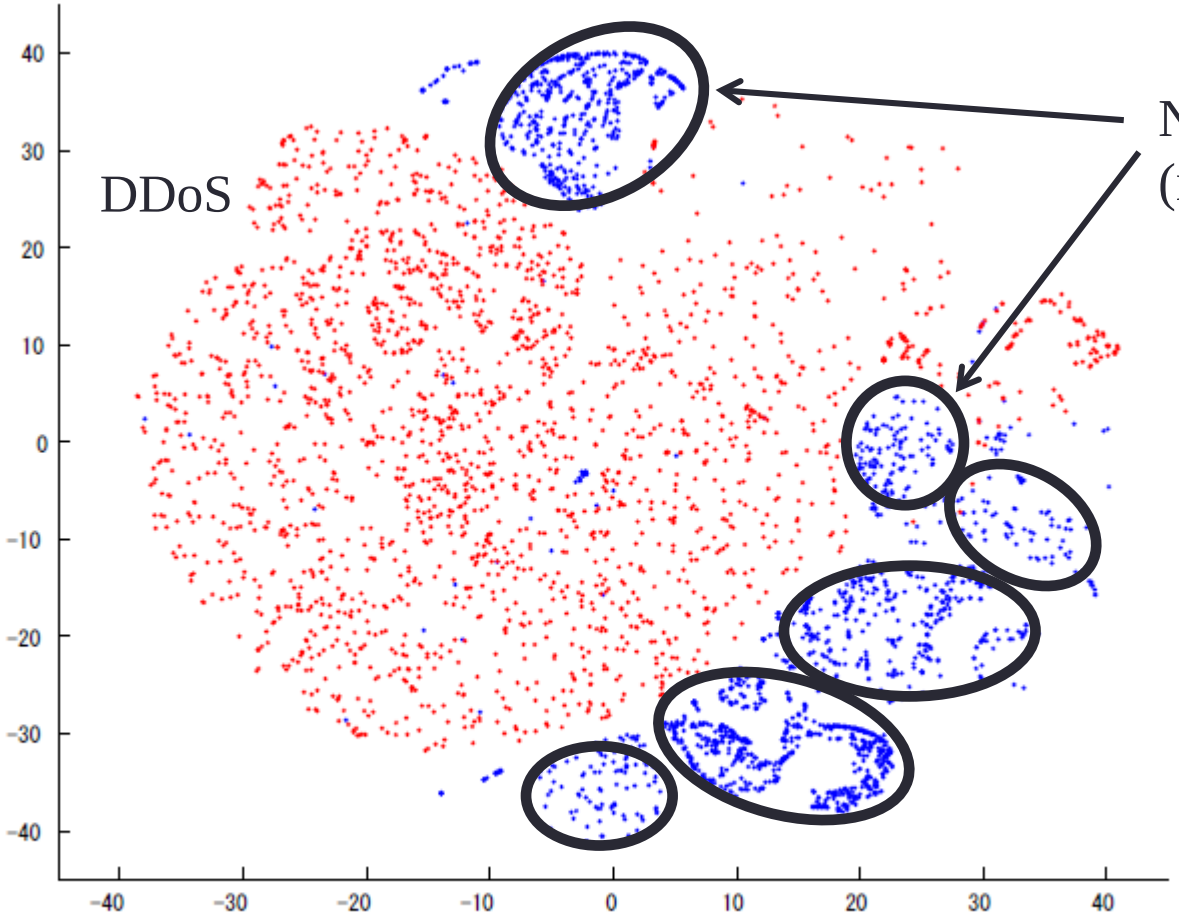
SNE

$$q_{j|i} = \frac{\exp\left(-\|y_i - y_j\|^2\right)}{\sum_{k \neq i} \exp\left(-\|y_i - y_k\|^2\right)}$$

t-SNE

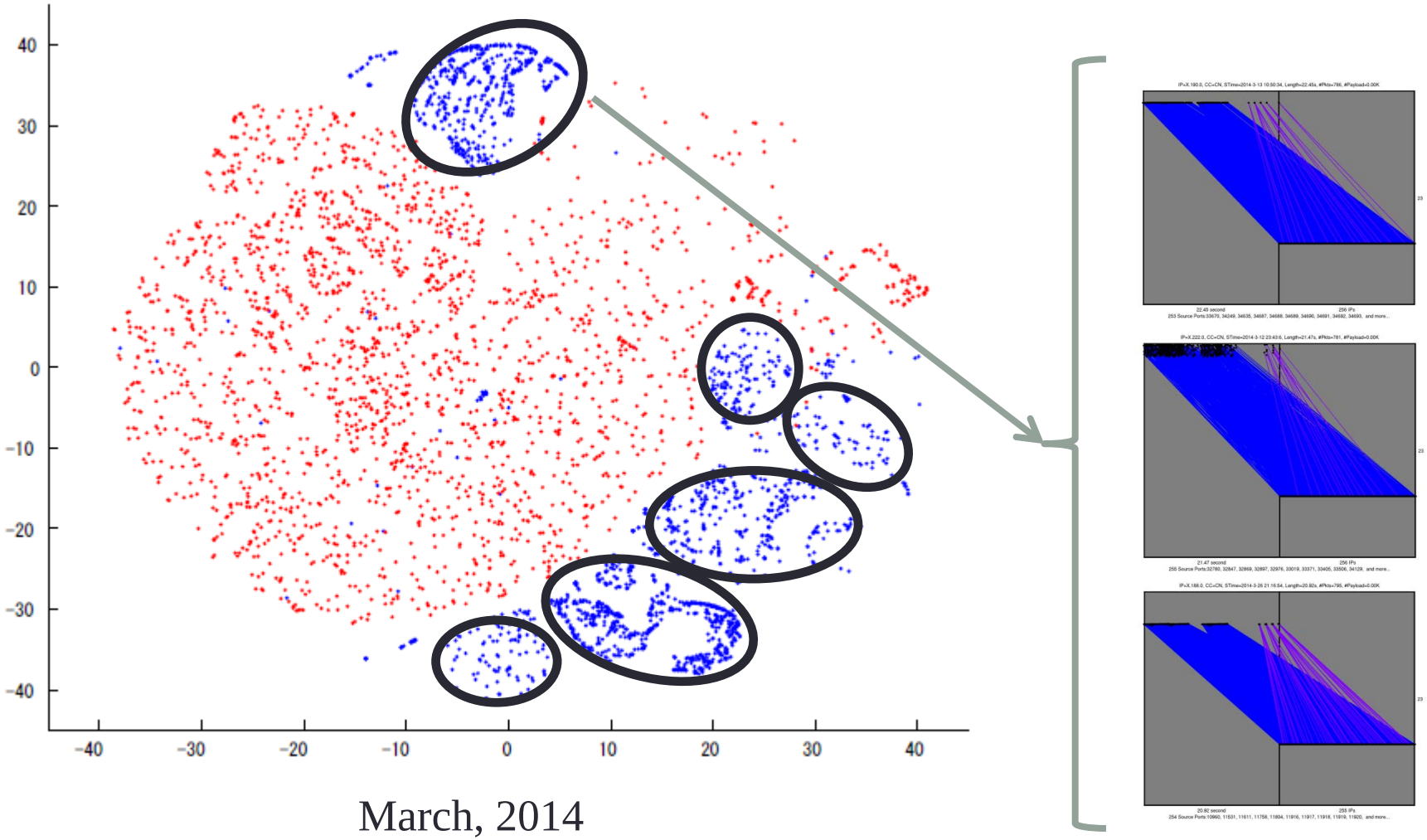
$$q_{ij} = \frac{\left(1 + \|y_i - y_j\|^2\right)^{-1}}{\sum_{k \neq l} \left(1 + \|y_k - y_l\|^2\right)^{-1}}$$

Visualization of Darknet Traffic (TCP)



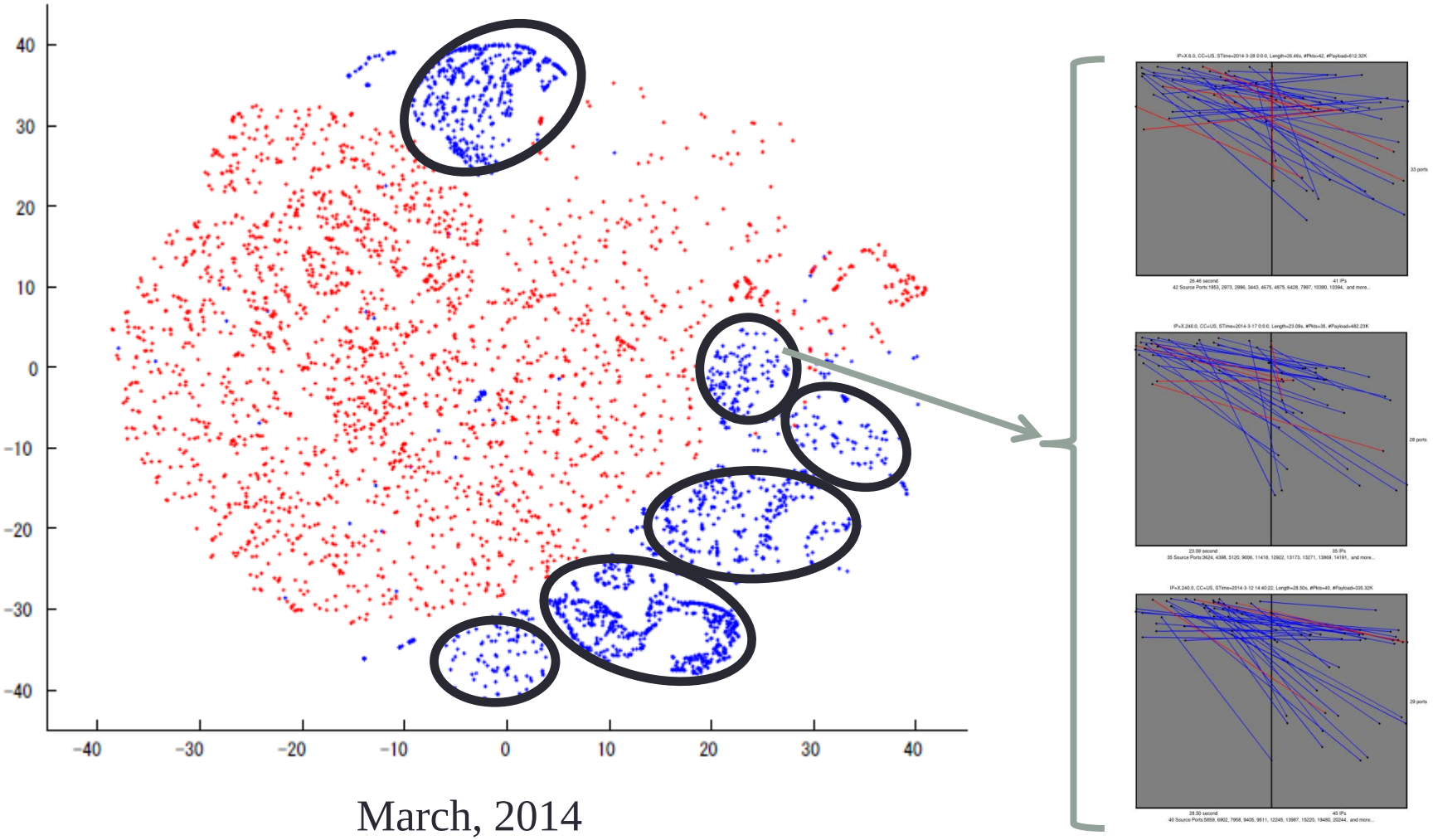
March, 2014

Visualization of Darknet Traffic (TCP)



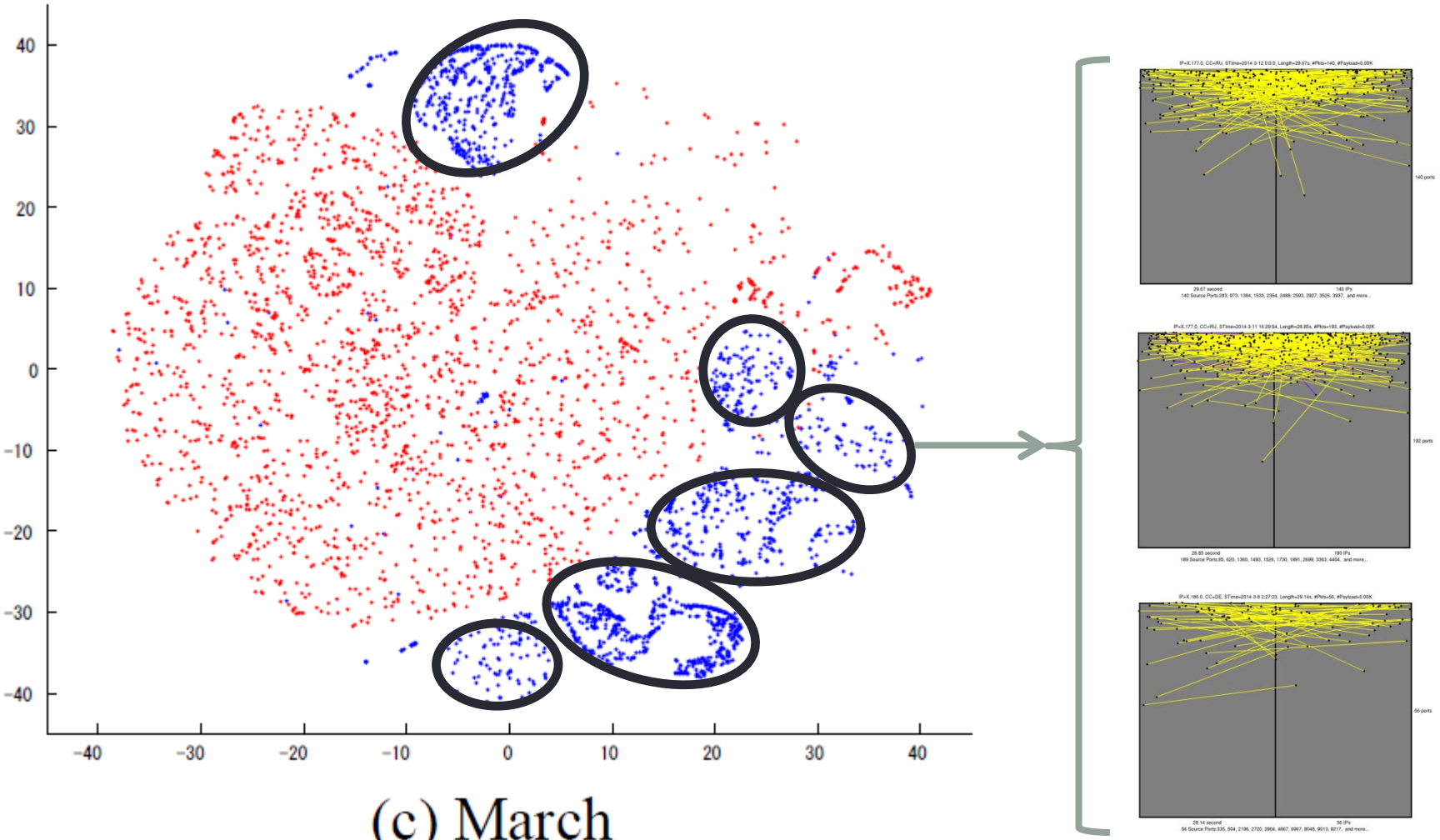
March, 2014

Visualization of Darknet Traffic (TCP)



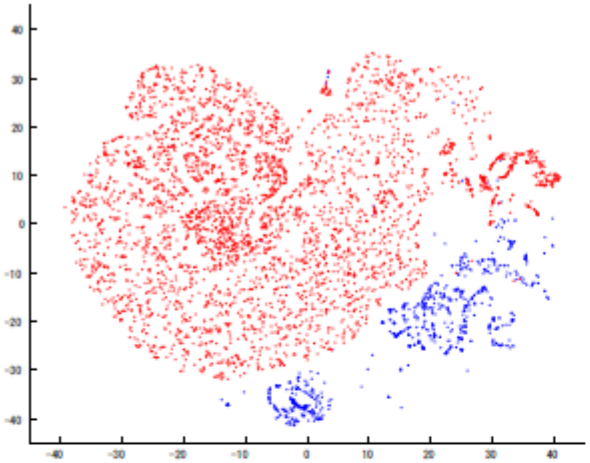
March, 2014

Visualization of Darknet Traffic (TCP)

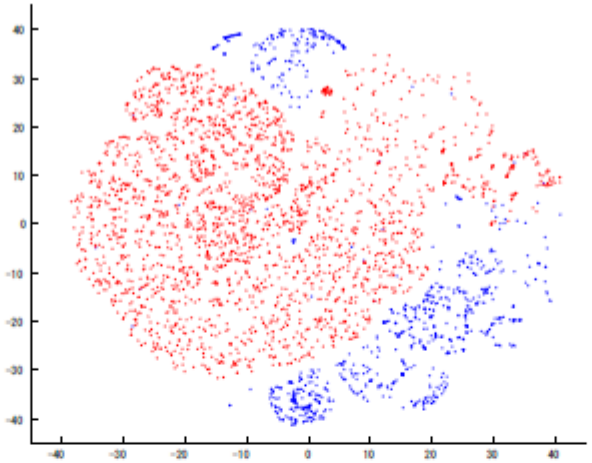


(c) March

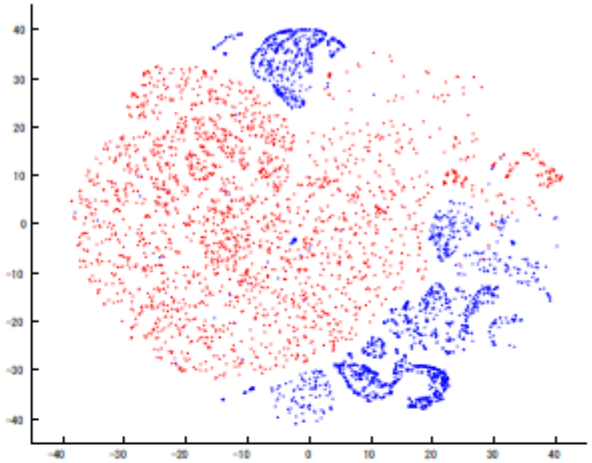
Monitoring Change of Cyber-Attacks



(a) January

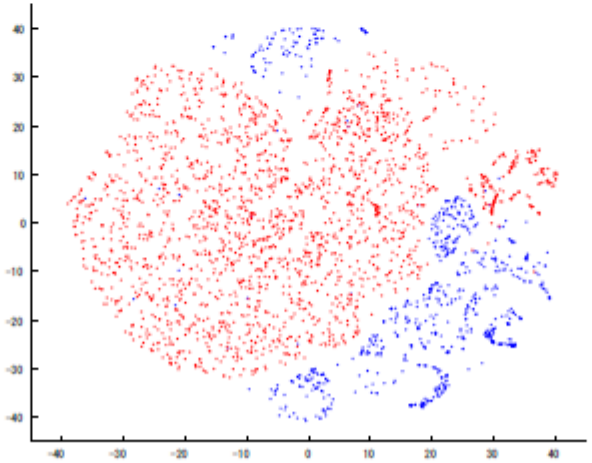


(b) February

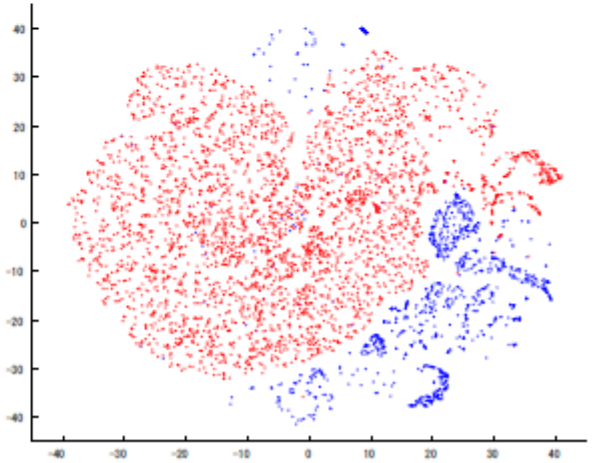


(c) March

(d) April



(e) May

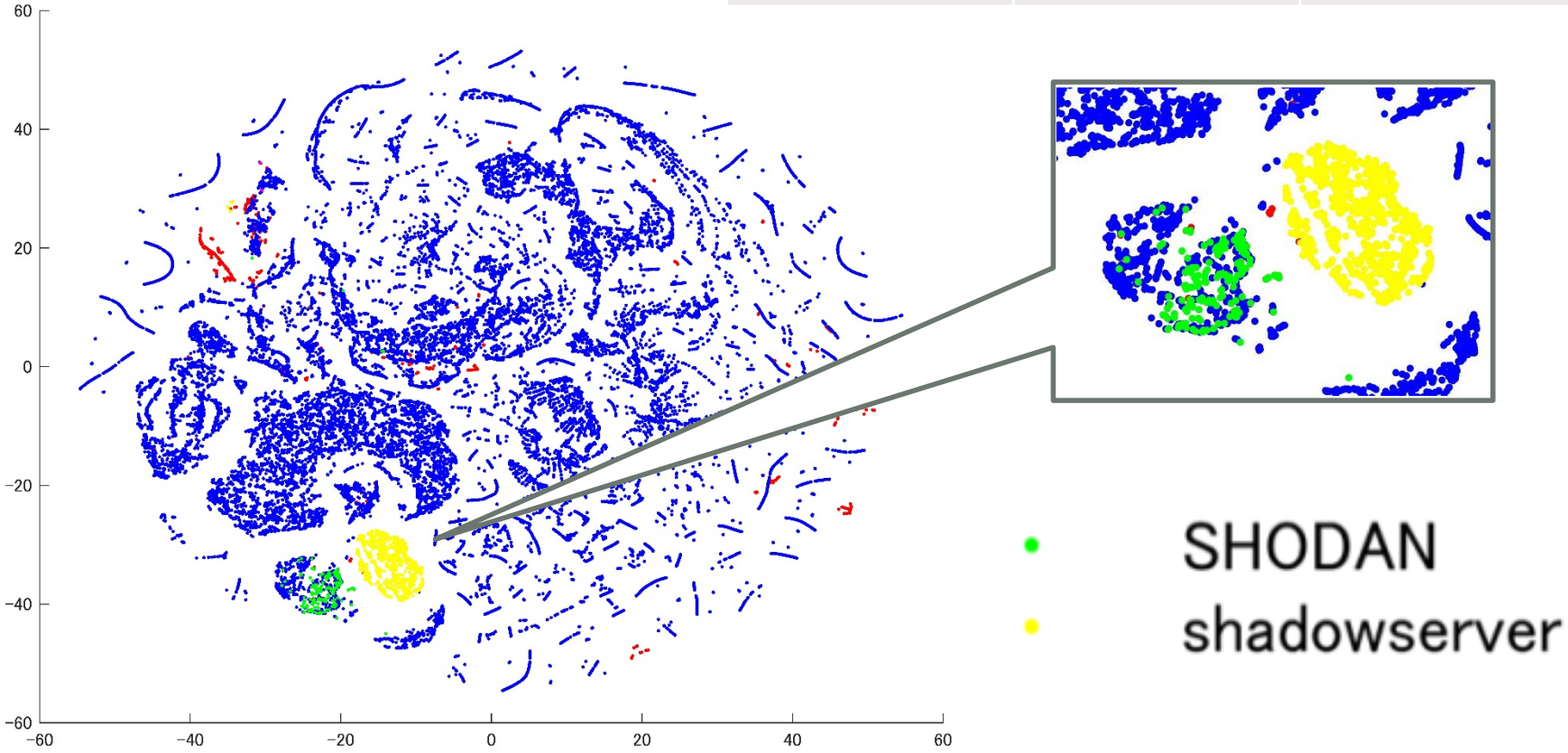


(f) June

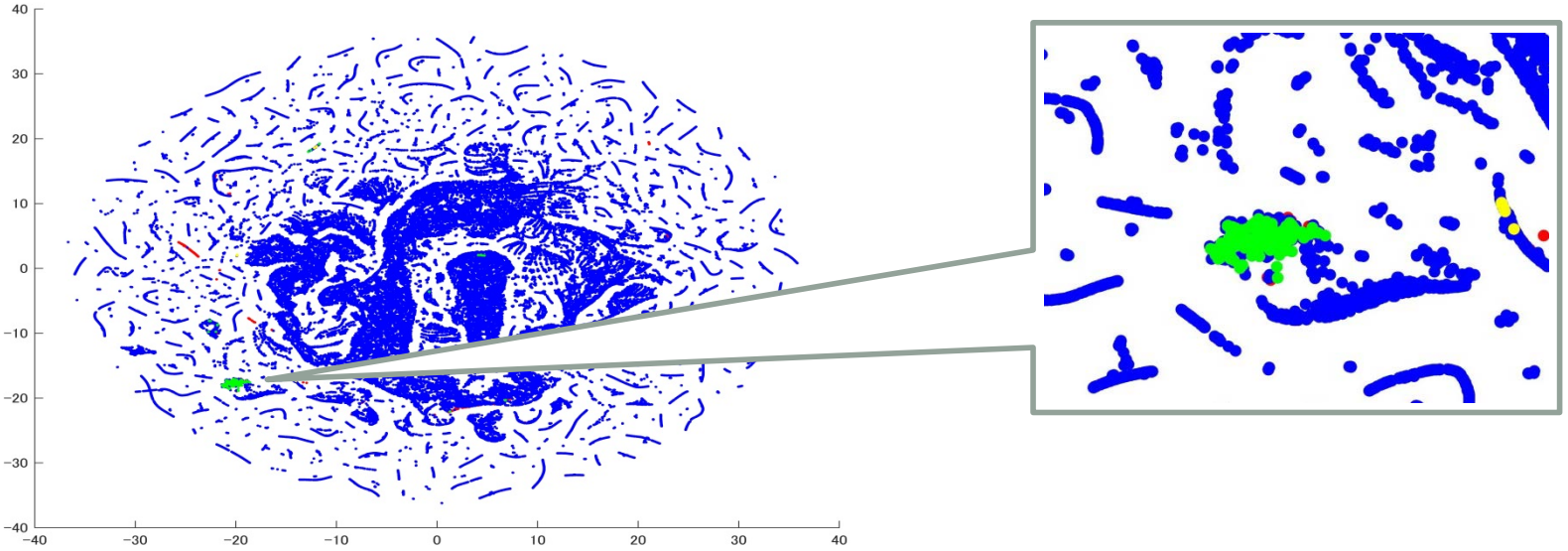
Visualization of Scanning

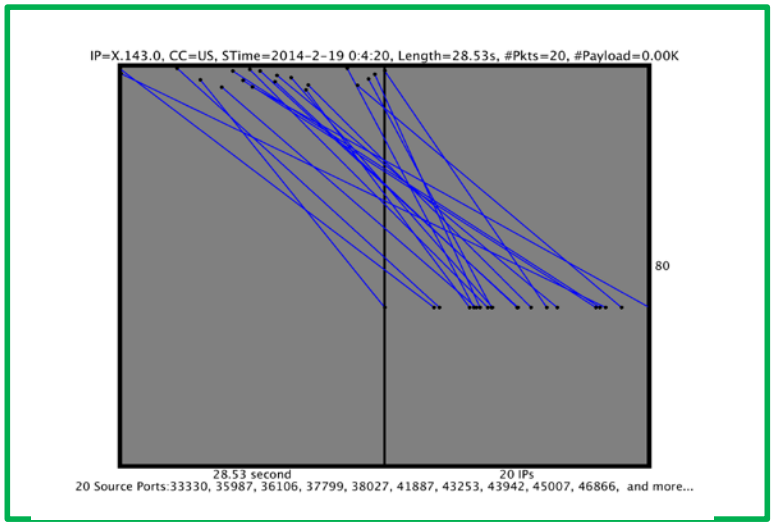
January 1st to December 31st, 2014
/16 Darknet Sensor

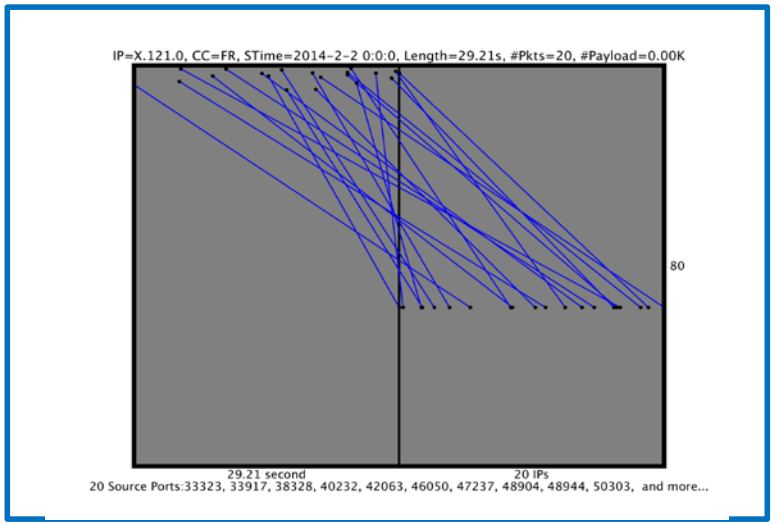
	#hosts	#feature vec.
TCP(SYN)	611,383	1,120,613
UDP	6,915	28,111



Scanning Patters of SHODAN







Large-scale Monitoring For Cyber Attacks Using Darknet Traffic Features

Traffic Analysis Profile (TAP)

(Inoue, et al., 2008)

		#dest. ports = 1		
		#dest. addr. = 1	#dest. addr. > 1	
			sequential dest. addr.	random dest. addr.
#src ports = 1	#packets = #src ports	Pong(1.1)	---	---
	#packets > #src ports	HammerN(2.N)	SequencedScan1(4.1)	RandomScan1(5.2)
#src ports > 1	#packets = #src ports	MultiPong(3.1)	SequencedScan2(4.2)	RandomScan2(5.4)
	#packets > #src ports	MultiHammer(3.2)	SequencedScan3(4.3)	RandomScan3(5.6)

		#dest. ports > 1		
		#dest. addr. = 1	#dest. addr. > 1	
			sequential dest. addr.	random dest. addr.
#src ports = 1	#packets = #src ports	---	---	---
	#packets > #src ports	FunSpan(6.1)	SequencedFunSpan(7.1)	RandomFunSpan(8.2)
#src ports > 1	#packets = #src ports	LinearSpan(6.2)	SequencedLinearSpan(7.3)	RandomLinearSpan(8.4)
	#packets > #src ports	MultiSpan(6.3)	SequencedMultiSpan(7.5)	RandomMultiSpan(8.6)

A TAP type is determined for 30-second packets from a source host.

Cyberattack Monitoring Using Darknet

To find new cyberattacks

- Large-scale monitoring using darknet sensors

  Source: Whole Internet space (monitoring unit: /16 subnet)

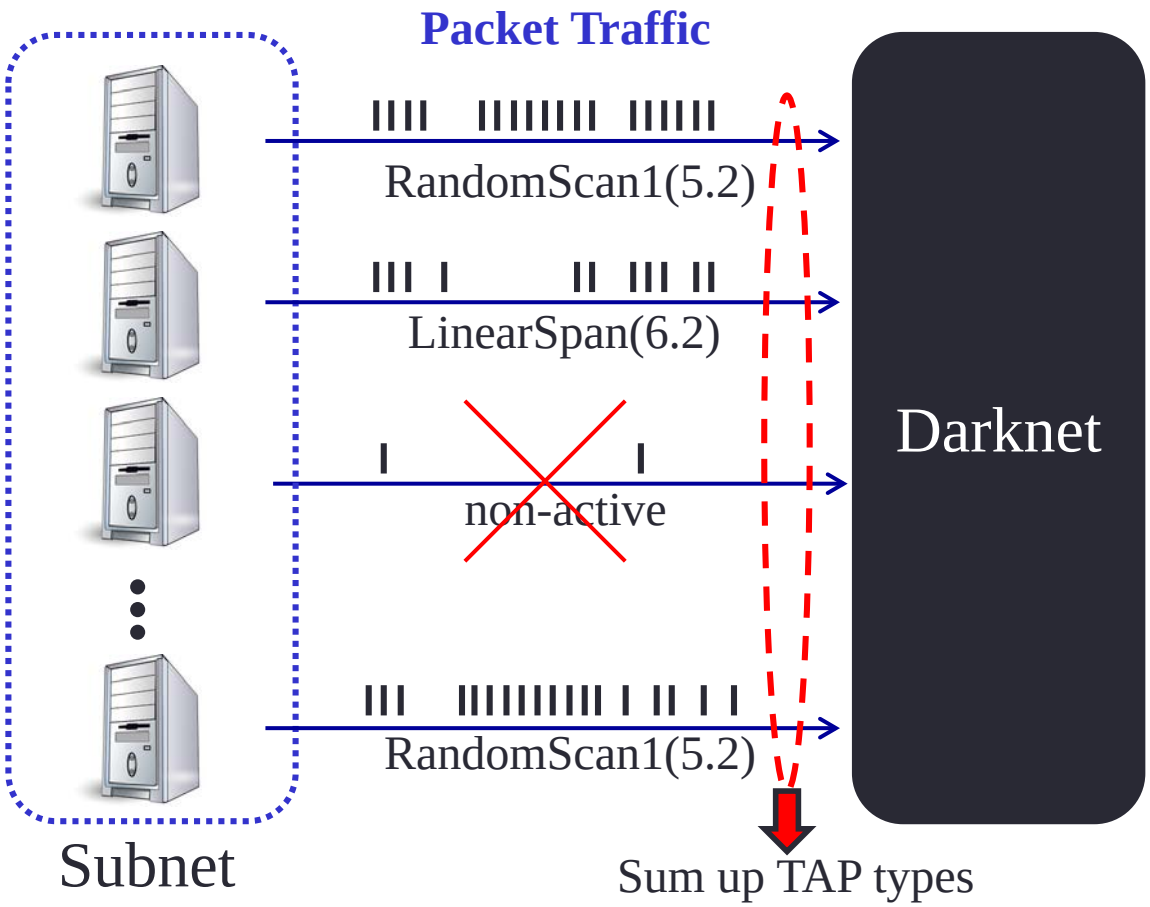
  Dest.: /16 darknet IP space (65,536 IPs)

- Clustering darknet traffic features

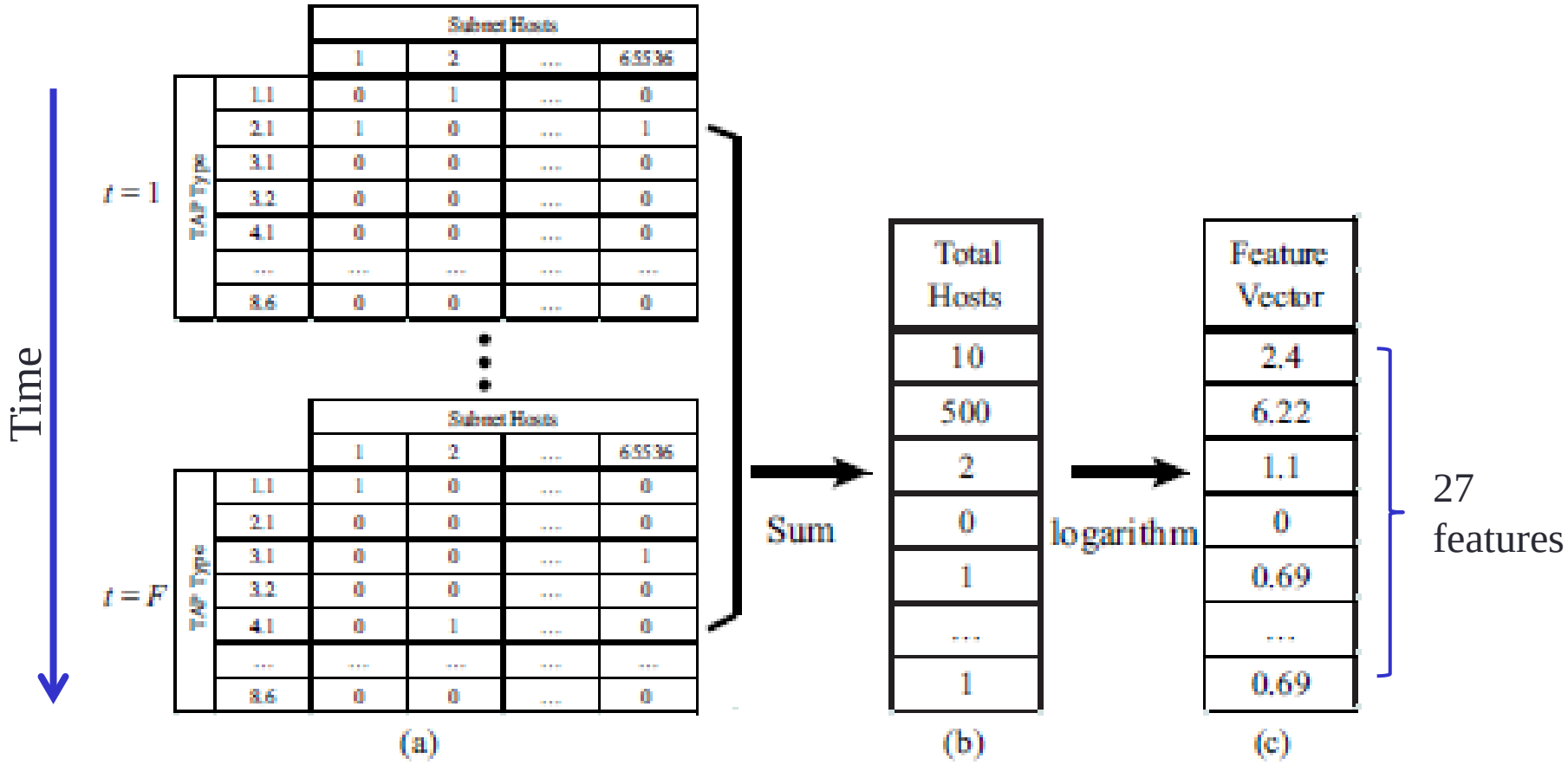
- Displaying transitions of the closest clusters for every subnets

Feature Vector of Subnet Infection State

For real-time monitoring, we take a subnet-based approach.



Feature Vector of Subnet Infection State



Processing Flows

Learning Phase

At every certain period, do the followings

- Capture darknet packets from all subnets
- For each subnet, get a feature vector
- Perform clustering with all subnet features
- Get reference vectors (prototypes)

Monitoring Phase

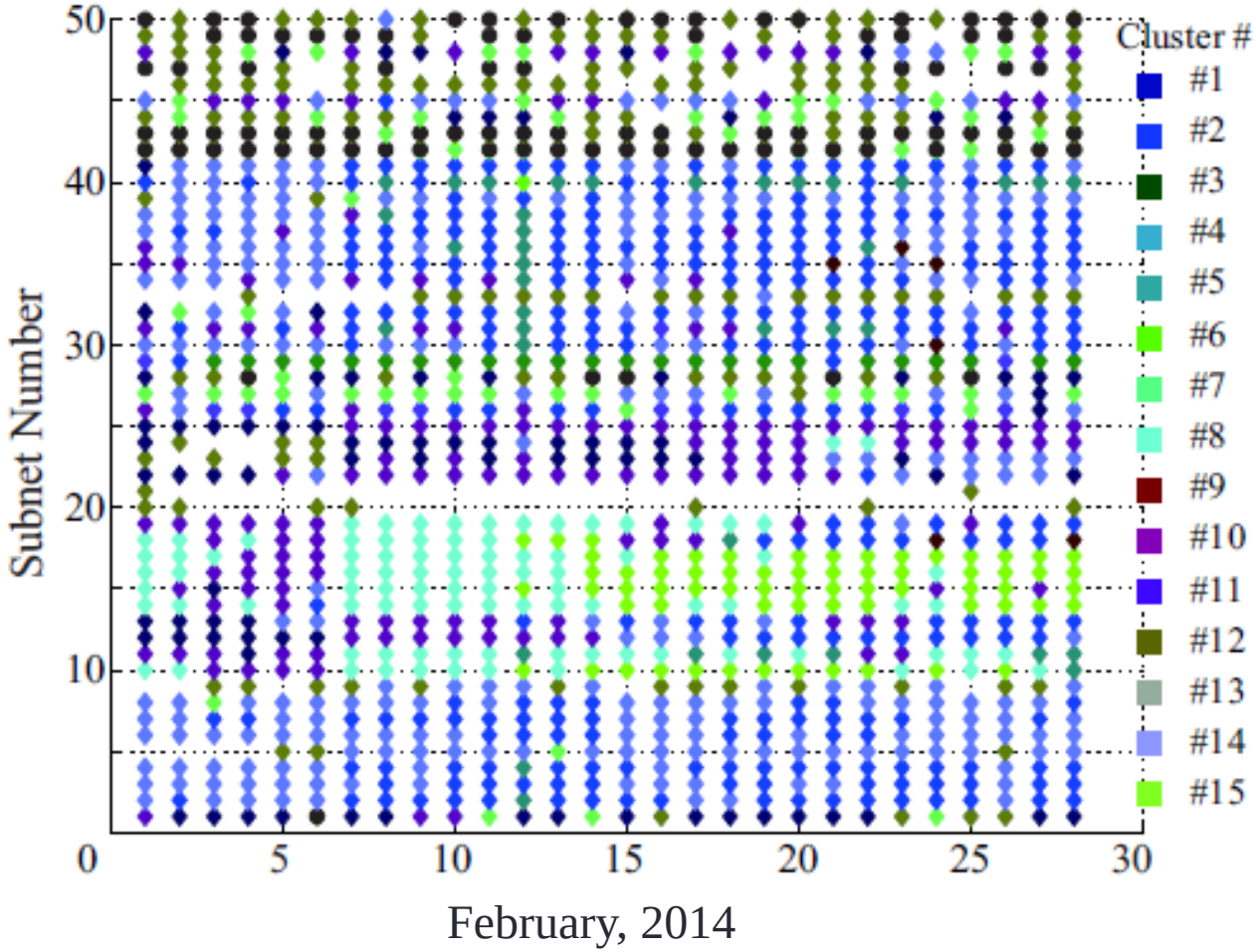
At every certain period, do the followings

- Capture darknet packets from each subnet
- Get a feature vector
- Get the nearest prototypes
- Show subnet state

Experimental Setup

- Collected Darknet Packets:
  - 1st February, 2014 – 28th February, 2014 (28 days)
  - 303,733,994 packets in total
  - Collected by NICT
- Monitored Subnets: /16 subnet mask (65,536 subnets)
- Darknet Scale: /16 IP space (65,536 destination IPs)
- TAP Feature Vectors: 27 dimensions,
  503,148 (use 20,000 for training)
- #Clusters: 15 (prototypes)

Monitoring Results

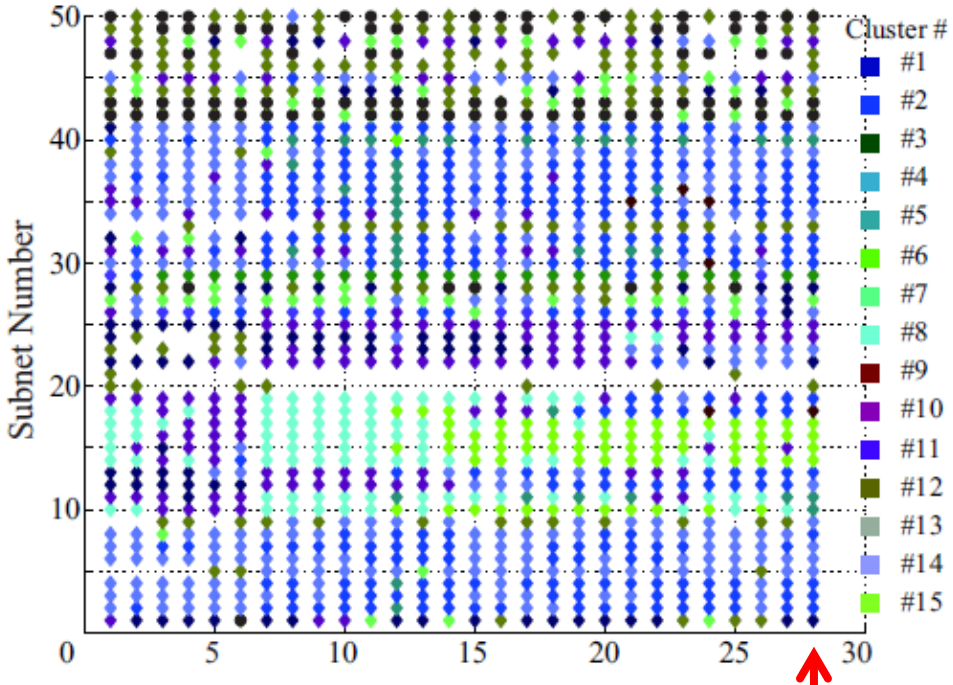


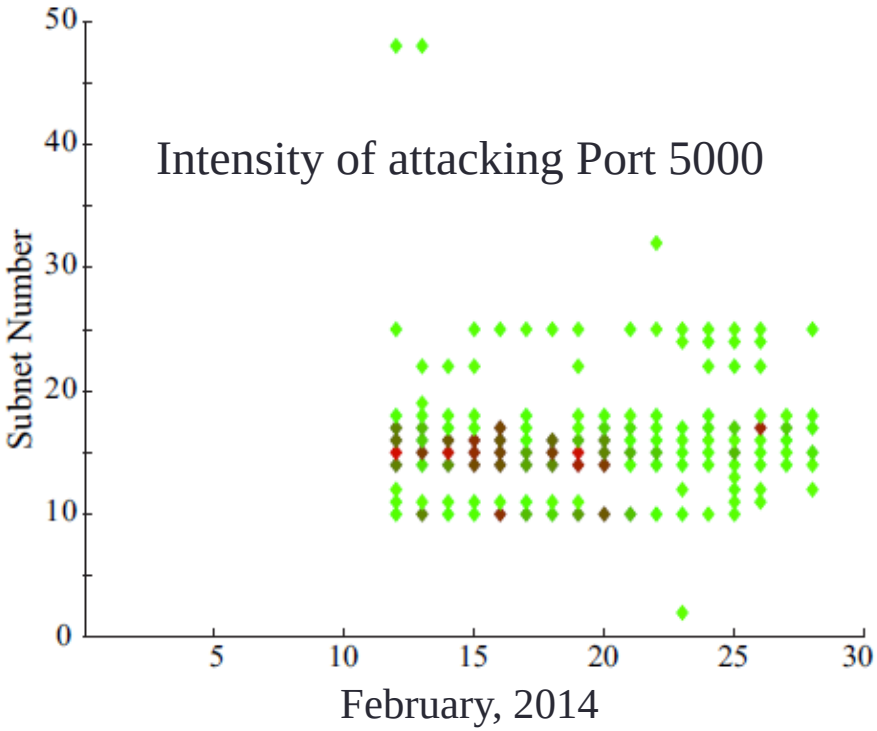
The results of 50 subnets are shown out of 65,536.

Subnets 10, 14-17

#10 → #8 → #15

Packets Analysis to Find New Attacks

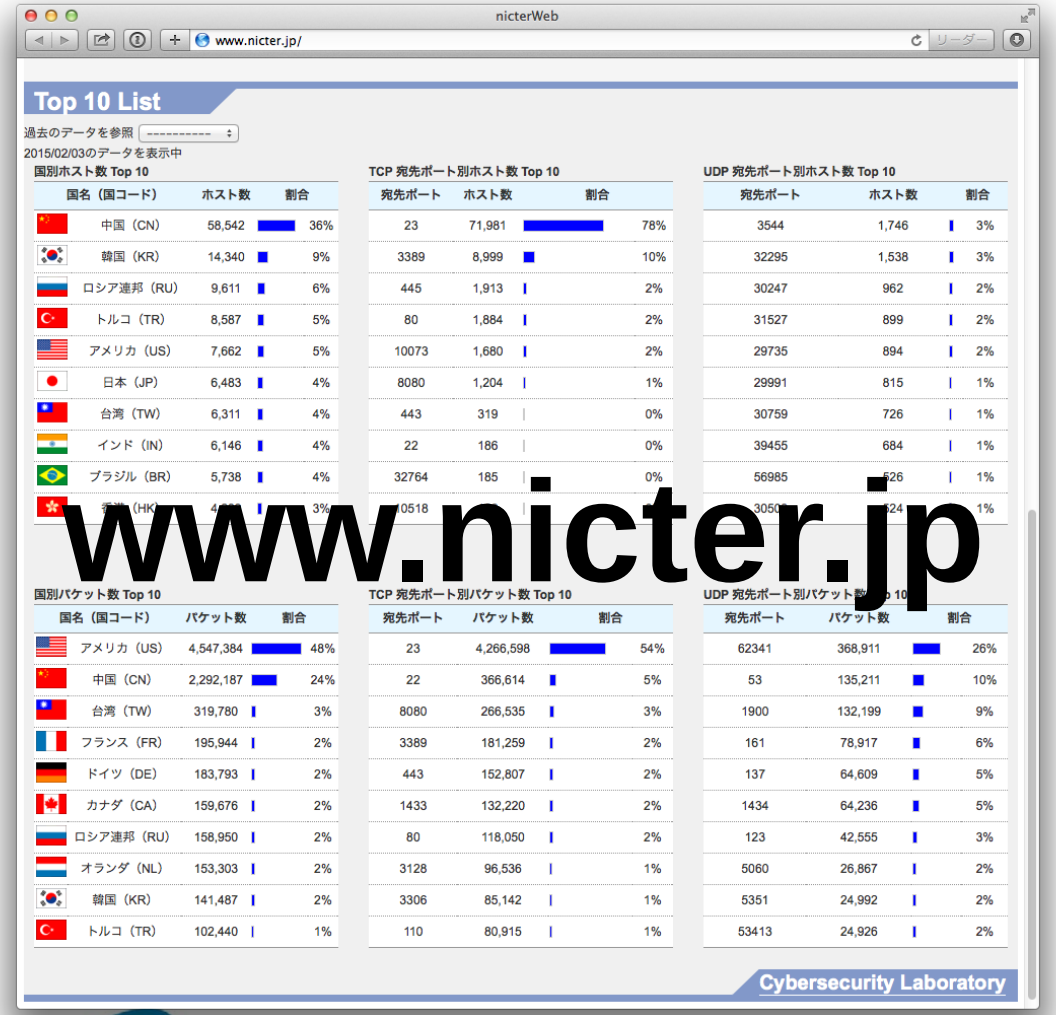




Report on the pandemic of Port 5000/TCP attack
(attacking the vulnerability Synology NAS)

Open Problem: Detection of IoT Cyberattacks

1st Reason of Increase in Darknet Traffic



Unique number of hosts / day

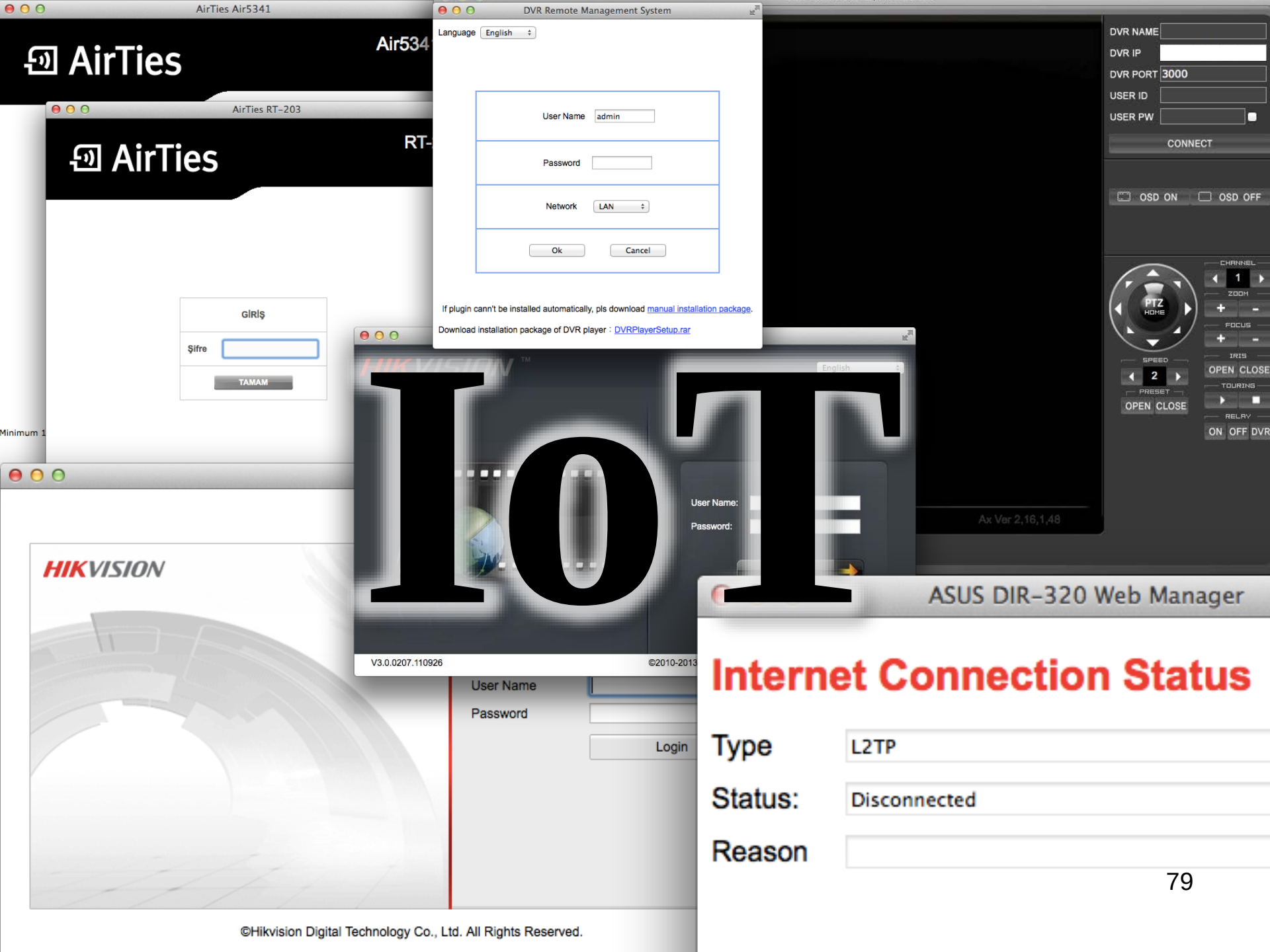
TCP 宛先ポート別ホスト数 Top 10

宛先ポート	ホスト数	割合
23	71,981	78%
3389	8,999	10%
445	1,913	2%
	1,884	

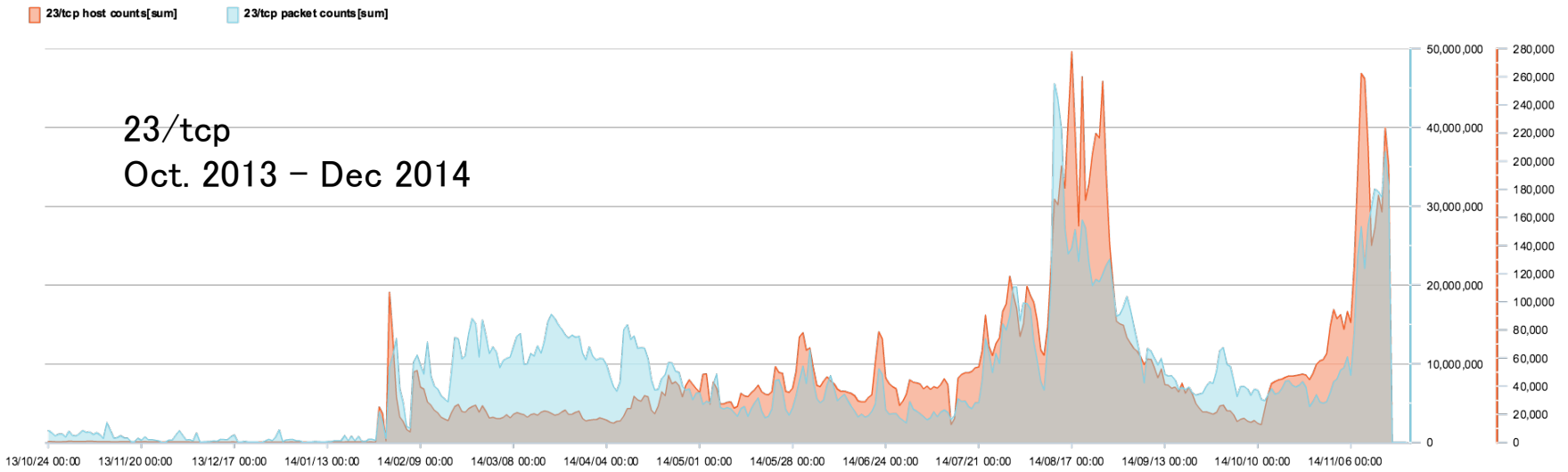
Total number of Packets / day

TCP 宛先ポート別パケット数 Top 10

宛先ポート	パケット数	割合
23	4,266,598	54%
22	366,614	5%
8080	266,535	3%
	181,259	


AirTies Air5341
AirTies
AirTies RT-203
AirTies
GİRİŞ
Şifre
TAMAM
DVR Remote Management System
Language English
User Name admin
Password
Network LAN
Ok
Cancel
If plugin cann't be installed automatically, pls download manual installation package.
Download installation package of DVR player : DVRPlayerSetup.rar
DVR NAME
DVR IP
DVR PORT 3000
USER ID
USER PW
CONNECT
OSD ON
OSD OFF
CHANNEL
ZOOM
FOCUS
IRIS
OPEN CLOSE
TOURING
RELAY
ON OFF DVR
SPEED
PRESET
OPEN CLOSE
PTZ HOME
IoT
User Name:
Password:
V3.0.0207.110926
©2010-2013
HIKVISION
User Name
Password
Login
©Hikvision Digital Technology Co., Ltd. All Rights Reserved.
ASUS DIR-320 Web Manager
Internet Connection Status
Type L2TP
Status: Disconnected
Reason

23/tcp Scan from Embedded Device



- Infected Devices
  - ✓ Home Router
  - ✓ Web Camera
  - ✓ NAS: Network Attached Storage etc. etc...

IoT Devices Attacking JP

- Investigated by Yoshioka Lab in YNU -

Wireless Router

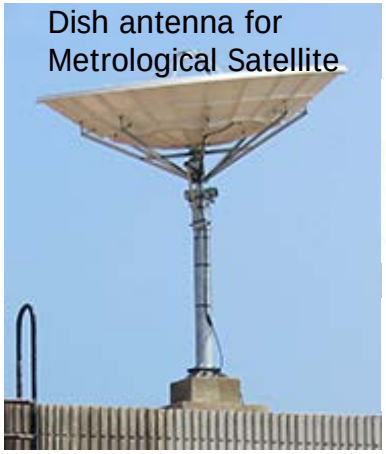
Food Processing Machine

Wifi Audio Receiver

Black Box Media Player Wireless Router

Radio Bridge Equipment

Dish antenna for Metrological Satellite



Solid State Recorder

Web Content Load Balancer

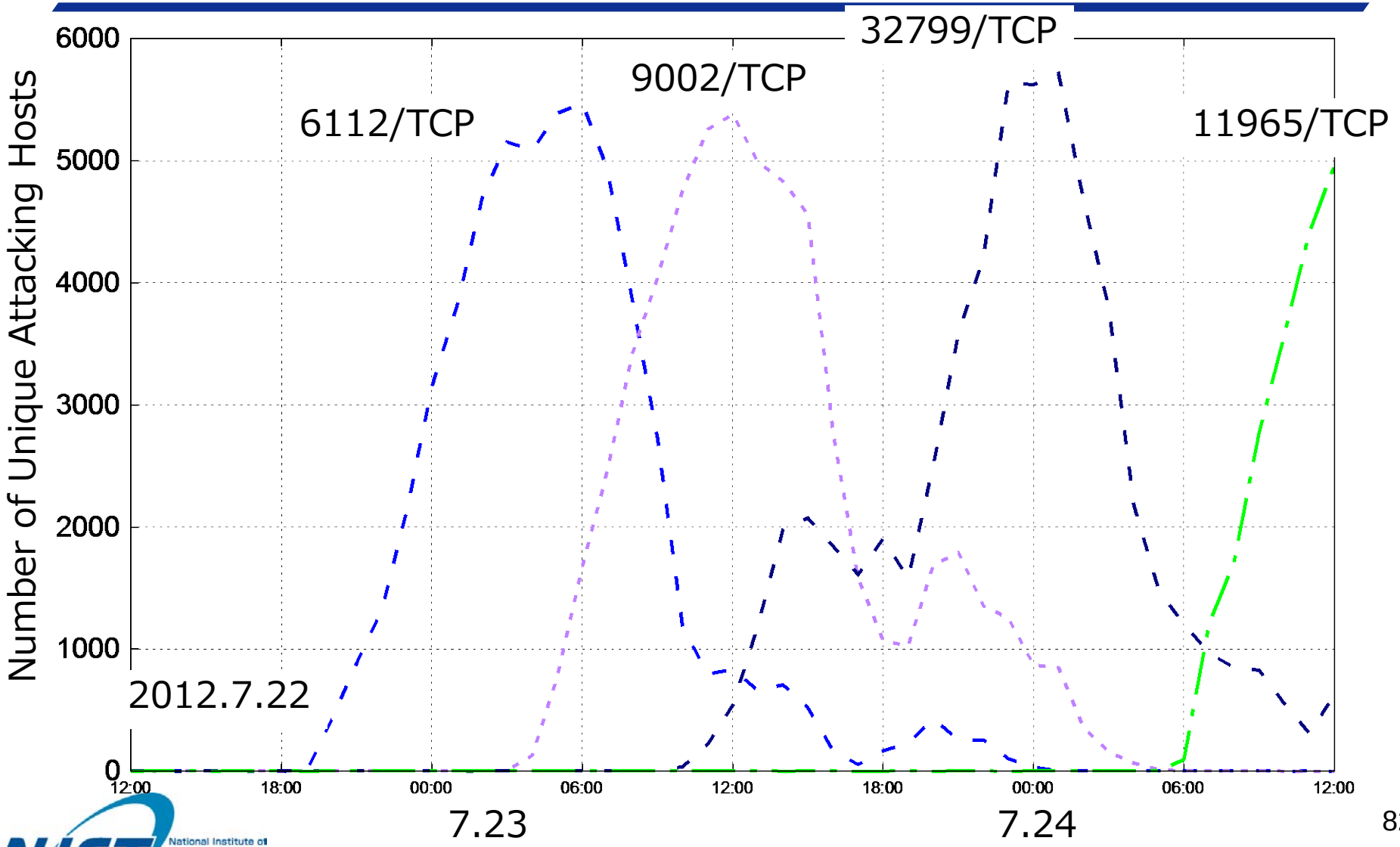
Thermal Detector

IP- Camera

OfficeServ System

Heat Pump

Scan towards Other IoT-Related Destination Ports（July 2012）



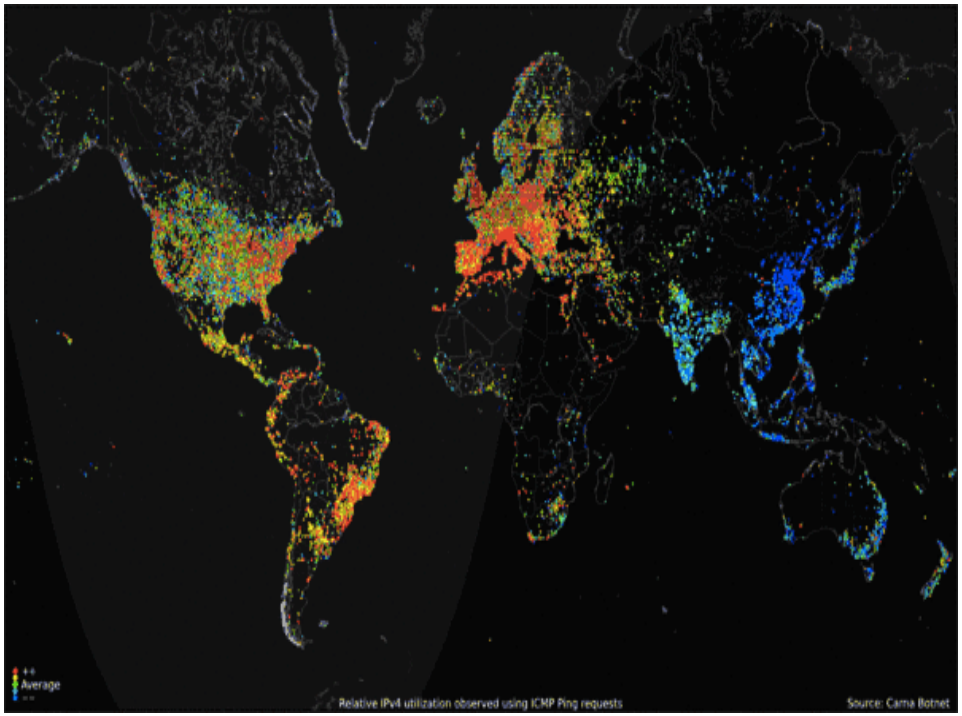
National Institute of Information and Communications Technology

NICTER

Network Incident Analysis Center for Tactical Emergency Response

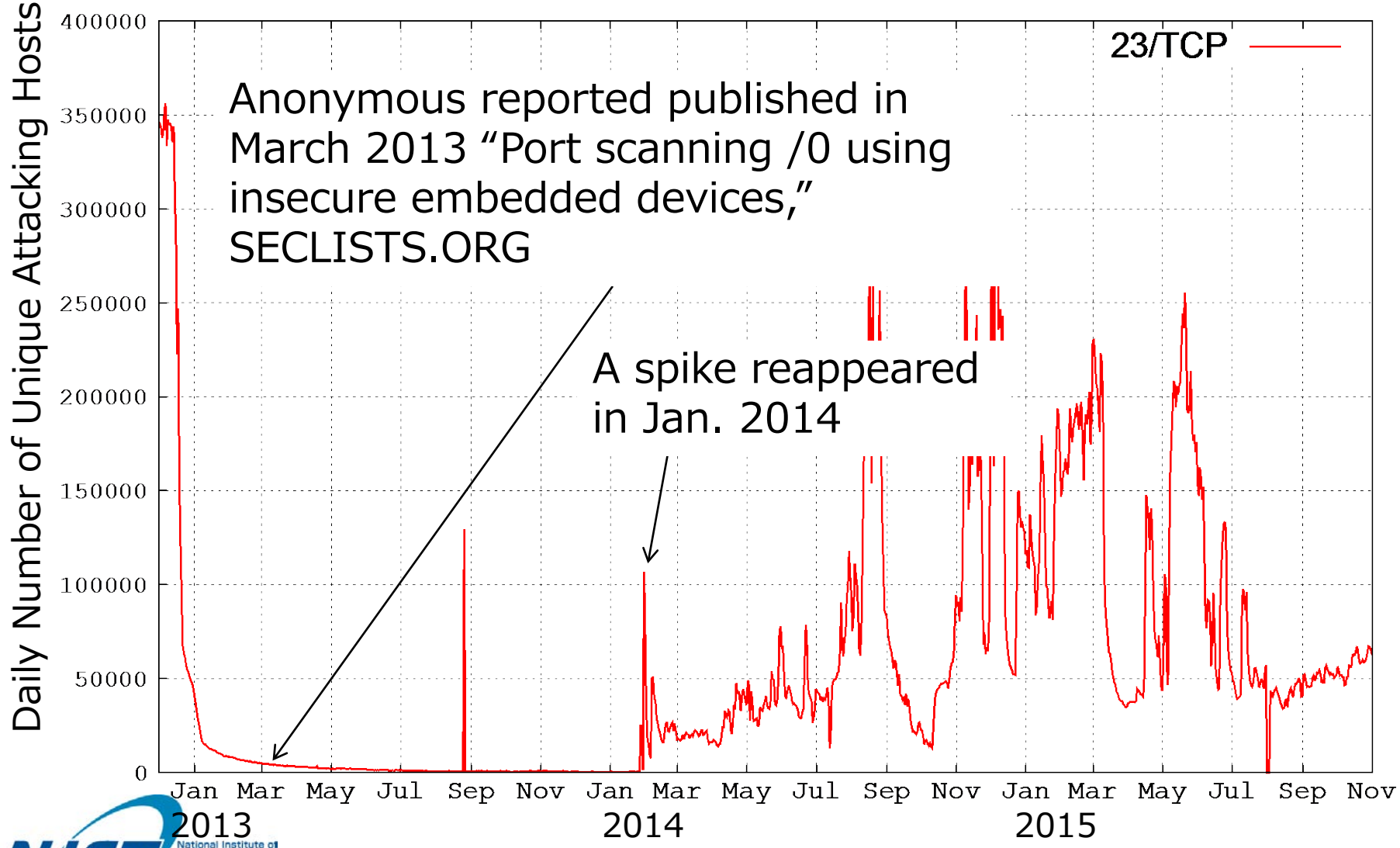
Case Study 1: Carna Botnet

- a botnet of 420,000 devices created by an anonymous hacker
- Infiltrating Internet devices, especially routers, that used a default password or no password at all.
- Result of “Internet Census of 2012”.
- Of the 4.3 billion possible IPv4 addresses,
  - 1.3 billion addresses in use (187 million in 2006),
  - 141 million behind a firewall
  - 729 million returned reverse domain name system records.
  - The remaining 2.3 billion IPv4 addresses are probably not used.



World map of 24-hour relative average utilization of IPv4 addresses observed using ICMP ping requests by Carna botnet, June - October 2012 (cited from *Wikipedia*)

Carna Botnet



NICT National Institute of Information and Communications Technology

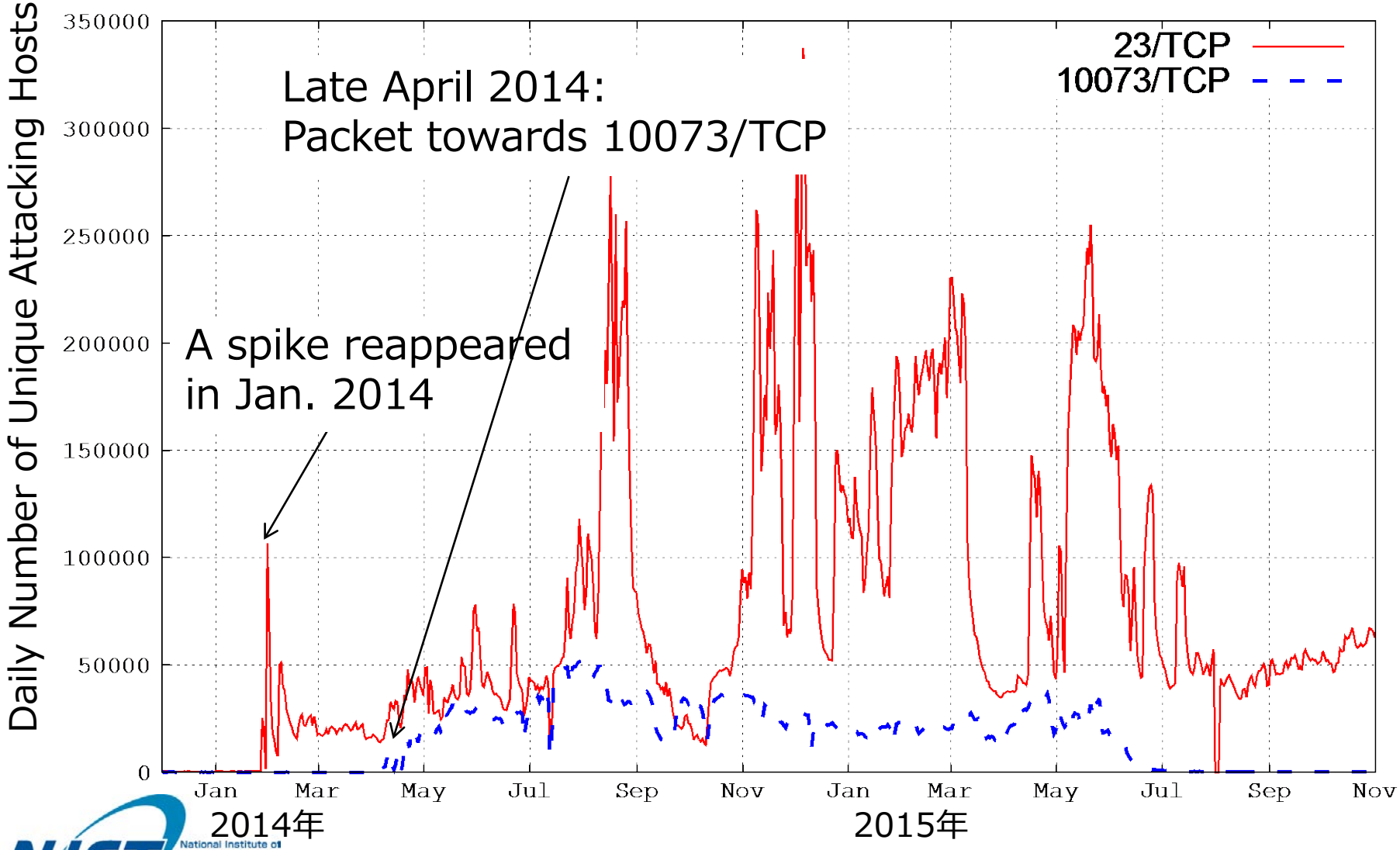
NICTER

Network Incident Analysis Center for Tactical Emergency Response

Case Study 2: Linux/Moose (Eset, “Dissecting Linux/Moose,” May 2015）

- Targets Linux-based embedded systems
  - Vendors Confirmed as Being Affected: Actiontec, Hik Vision, Netgear, Synology, TP-Link, ZyXEL, Zhone
  - Number of affected devices: 50,000
- Attack graph
  - if there is no connection possible to TCP port 10073 it tries to connect to the Telnet service of that IP (TCP port 23)
  - compromising systems with weak or default credentials
- High-level capability
  - Service listening on port 10073/TCP
  - DNS Hijacking
  - Eavesdrop on network communications
  - SNS（fraudulent social network activity）

Stats of Attacks on 10073/TCP（2014～2015）

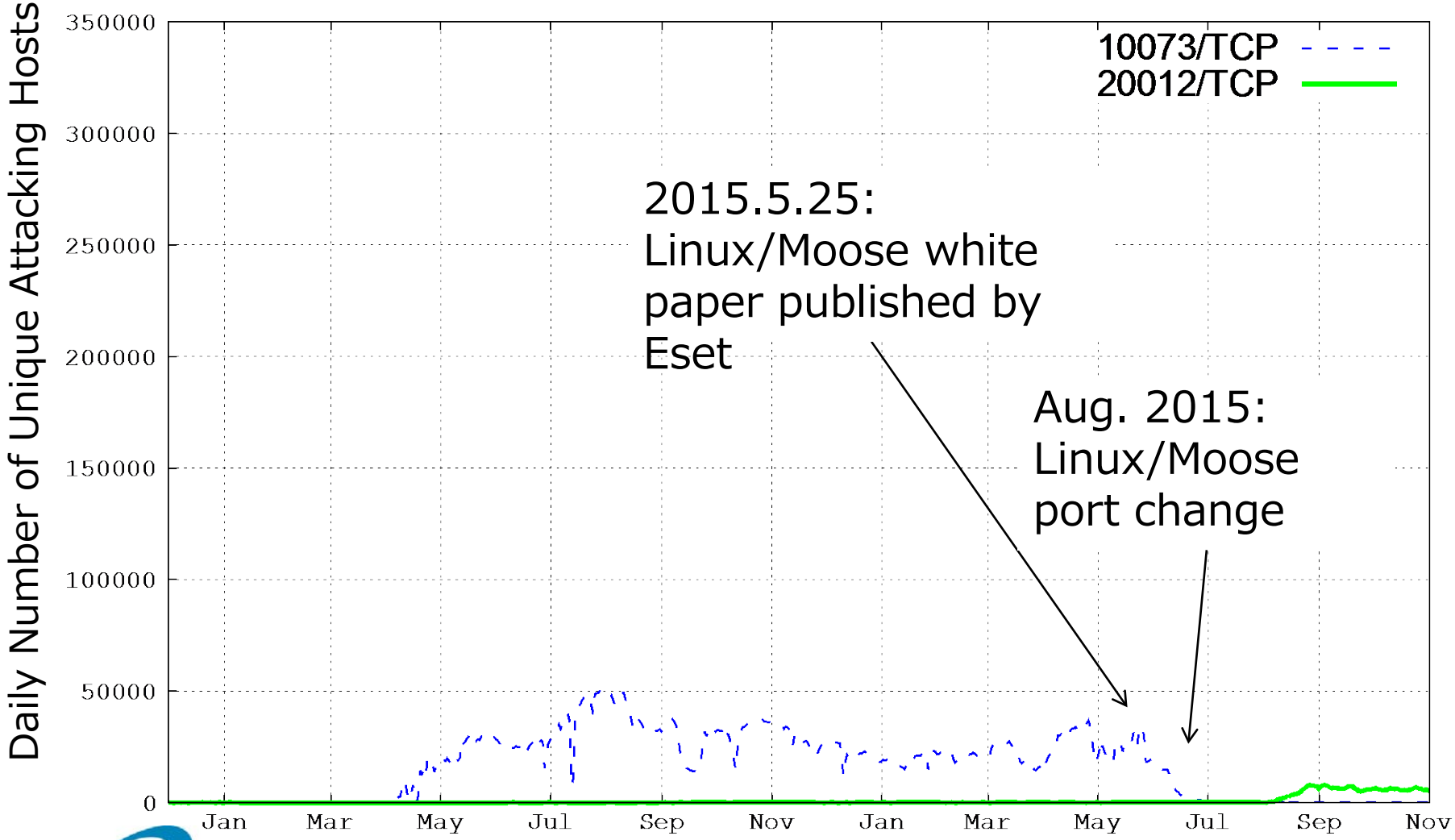


National Institute of Information and Communications Technology

NICTER

Network Incident Analysis Center for Tactical Emergency Response

Stats of Linux/Moose in（2014～2015）

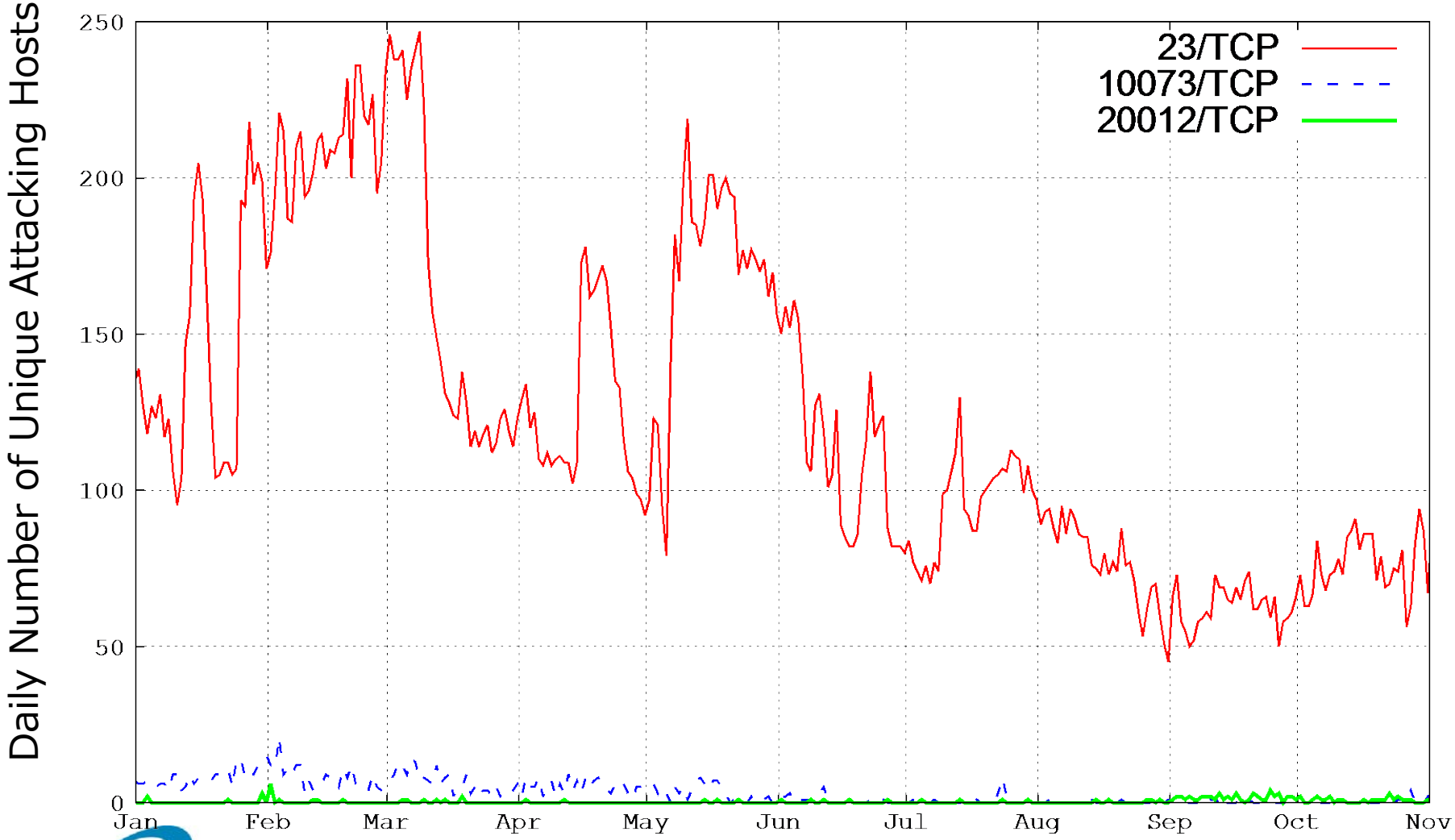


NICT National Institute of Information and Communications Technology

NICTER

Network Incident Analysis Center for Tactical Emergency Response

Stats of Unique Attacking Hosts from JP



Conclusions

- *Machine learning can be useful in cybersecurity?*

  Yes, but the applicable domains are limited. Mainly for monitoring purpose.

- *How can I get data sets?*

  You may find some real data sets, but should know cyberattacks are always evolving. To collect real live cyberattack data, need some tricks to collect malicious activities because attackers do not want to be discovered. Thus, the best way is to collaborate with security experts.

  e.g., honeypot, darknet sensor, double bounced emails

- *How can I get labels?*

  Also need tricks and some expertise on network and security

  e.g., nature of attacks, use packet header and payload information

- *Cyberseurity community expects machine learning?*

  Not much, unfortunately. But they wish it would become useful someday.

Acknowledgement

I deeply appreciate hard and excellent work by

- National Institute of Communication Technology (NICT)

  Dr. Tao Ban, Dr. Junji Nakazato

- clwit, Inc., Japan

  Jumpei Shimamura

- Kobe University, Japan

  Dr. Jun Kitazono (assistant professor)

  Nobuaki Furutani, Youki Ukawa, Shogo Osaka (Mater Students)