PRACTICE

Field Trial against Cyber-attacks through International Collaboration

ISPs' Effort to Establish Quick Response Scheme

September 24th, 2013

Satoshi NORITAKE

NTT Communications / Telecom-ISAC Japan

Today's topics

1. Our Security Concerns
2. Outline of PRACTICE Field Trial
3. Quick Response against Cyber-attacks
4. Cyber-attacks observed by PRACTICE System
5. Case studies on Cyber-attacks
6. Conclusions

Our Security Concerns

Do Japanese feel secure?

- Do Japanese feel secure about using the Internet?

No Problem?

Some security reports show that Malware infection rate in Japan is significantly low compared with other countries.

Local Infection Risk reported by Kaspersky

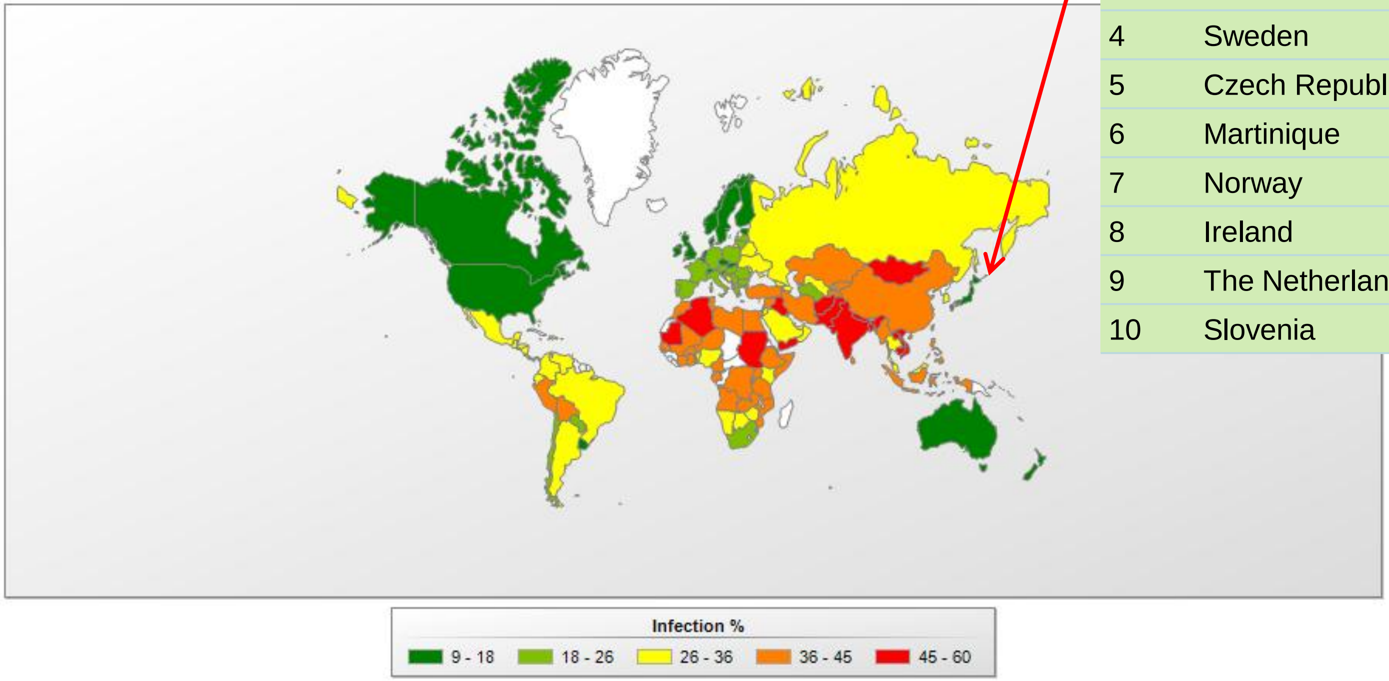
- Japan has the lowest risk of infection according to Kaspersky report.

The Top 10 countries with the lowest risk of local infection were:

IT Threat Evolution: Q2 2013

http://www.securelist.com/en/analysis/204792299/IT_Threat_Evolution_Q2_2013

Rank	Country	%
1	**Japan**	**9.01%**
2	Denmark	9.72%
3	Finland	11.83%
4	Sweden	12.10%
5	Czech Republic	12.78%
6	Martinique	13.94%
7	Norway	14.22%
8	Ireland	14.47%
9	The Netherlands	14.55%
10	Slovenia	14.70%



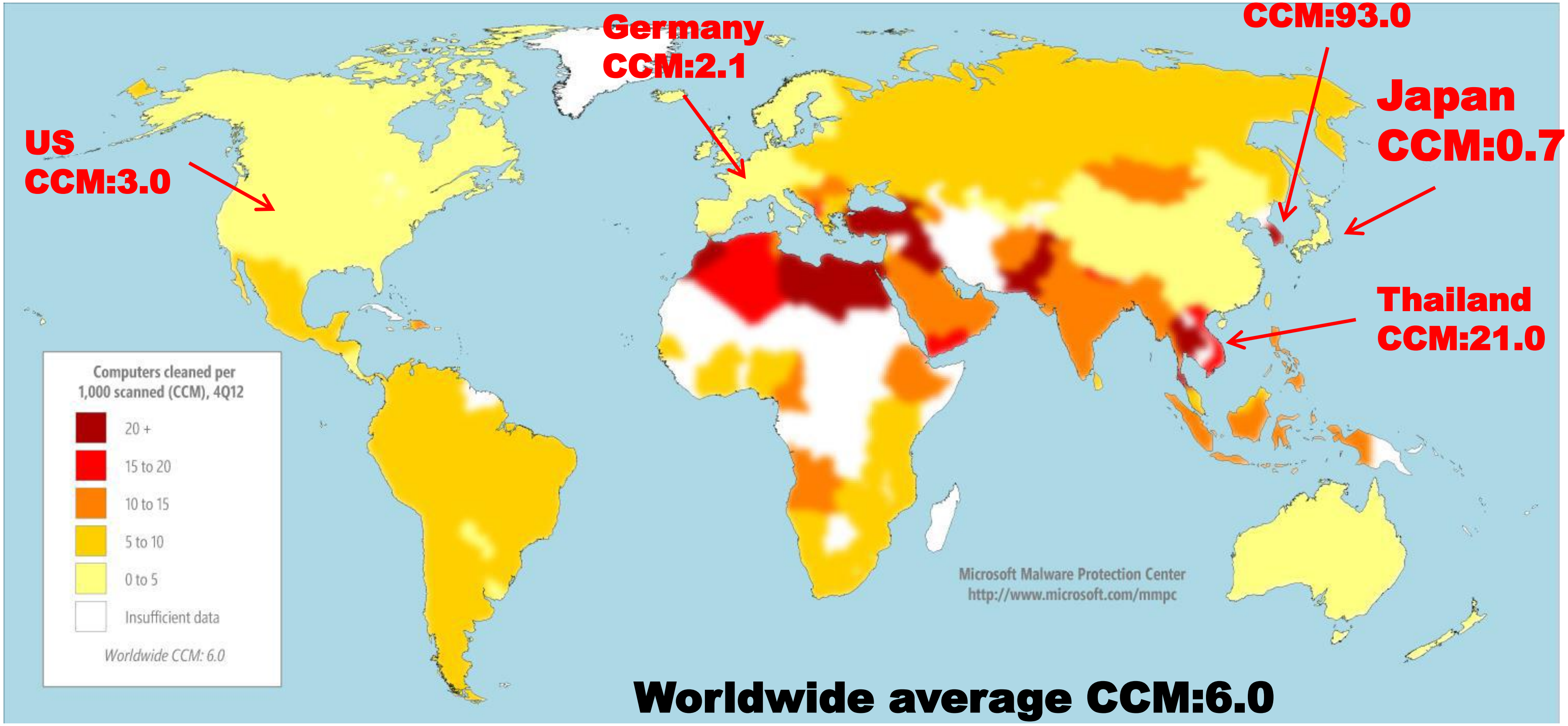
Malware infection rates reported by Microsoft

- Malware infection rate in Japan is significantly low according to Microsoft.

Microsoft Security Intelligence Report Volume 14

Infection rates by country/region in 4Q12 (bottom), by CCM

CCM is the number of computers cleaned for every 1,000 executions of MSRT.



Korea CCM:93.0

Germany CCM:2.1

Japan CCM:0.7

US CCM:3.0

Thailand CCM:21.0

Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

Worldwide average CCM:6.0

But Many Attacks occur…

- Some Security Experts comment that many malwares exist in Japan.

Citadel Makes a Comeback, Targets Japan Users

<<TrendMicro 2013-09-02>>

http://blog.trendmicro.com/trendlabs-security-intelligence/citadel-makes-a-comeback-targets-japan-users/

Through investigation and collaboration between our researchers and engineers, we discovered a malicious online banking Trojan campaign targeting users in Japan, with the campaign itself ongoing since early June of this year. We've reported about such incidents in the past, including in our Q1 security roundup – and we believe this latest discovery shows that those previous attacks have been expanded and are a part of this particular campaign.

Alert regarding compromised websites

<<< JPCERT/CC Alert 2013-06-07 >>>

https://www.jpcert.or.jp/english/at/2013/at130027.html

JPCERT/CC has been receiving a large number of incident reports
regarding compromised websites (A
According to the reports, most of the
embedded iframes or obfuscated Ja
attack site. When a user visits a co
infected by malware.

CERT China claims Japan and US lead in attacks on Chinese internet sites <<<SOPHOS 2013-03-22>>>

http://nakedsecurity.sophos.com/2012/03/22/cert-china-claims-japan-and-us-lead-in-attacks-on-chinese-internet-sites/

The People's Daily Online reported Monday that the number of foreign attacks against Chinese internet infrastructure "remain severe." China's CERT stated that a total of 47,000 foreign IP addresses were involved in attacks against 8.9 million Chinese computers last year.

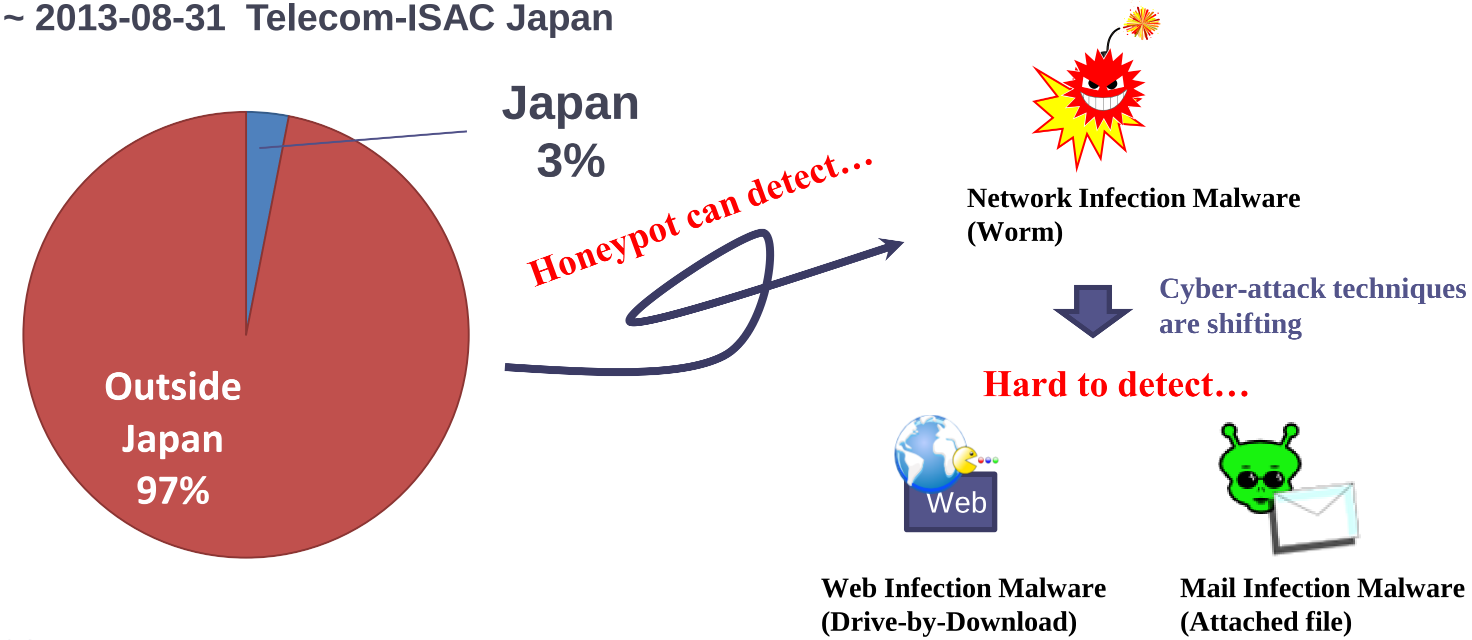
They claim that **most of these attacks originate from Japan**, the United States and the Republic of Korea (South Korea)

Our Concerns

- We evaluate that Malware Infection Rate in Japan still remains low level.
- But we are exposed to the cyber-threats.

Number of Malwares detected by honeypot

2013-01-01 ~ 2013-08-31 Telecom-ISAC Japan



Network Infection Malware (Worm)

Cyber-attack techniques are shifting

Hard to detect…

Web Infection Malware (Drive-by-Download)

Mail Infection Malware (Attached file)

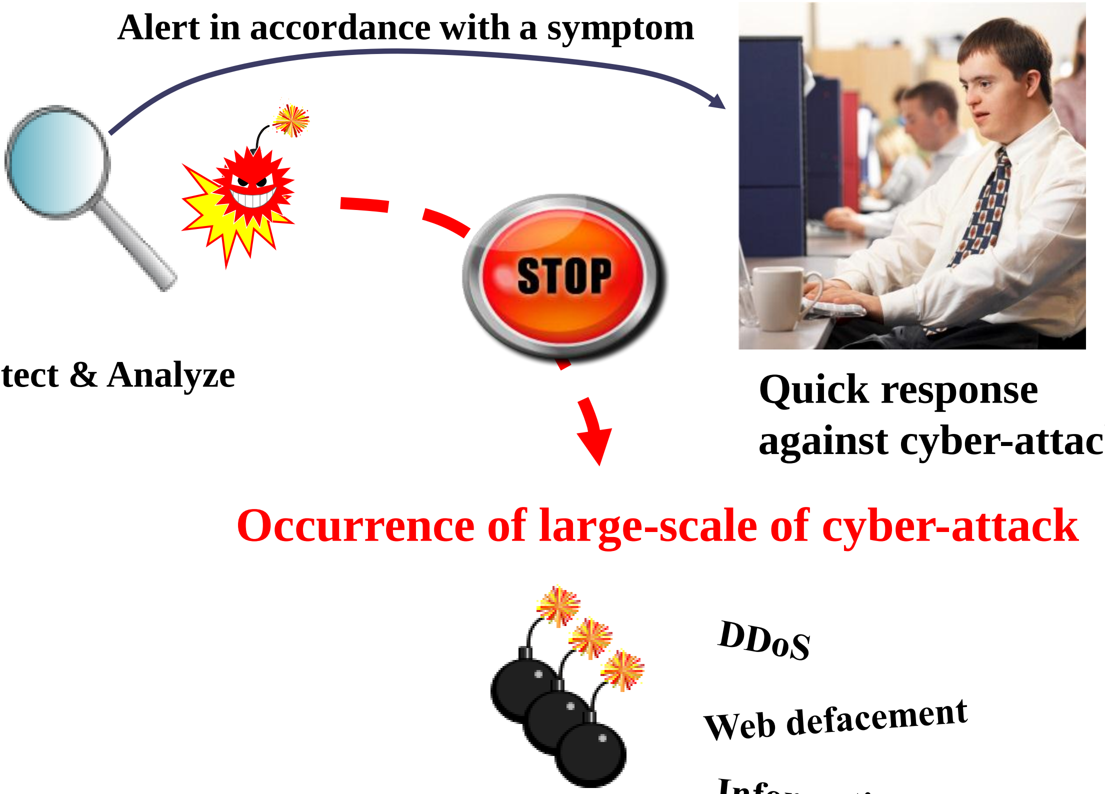
Our Concerns

- Most malwares we detected by our honeypot came from outside of Japan.
- Cyber attack techniques are more sophisticated and complicated.
- We might not detect those sophisticated and complicated cyber-attacks.
- One day, a large-scale cyber-attack may occurs…

Our challenge

- Predict an emerging cyber-attack before an actual damage occurs.

Detect a symptom of an emerging cyber-attack


Alert in accordance with a symptom

Detect & Analyze

Quick response
against cyber-attack

Occurrence of large-scale of cyber-attack

DDoS

Web defacement

Information leakage

Outline of PRACTICE Field Trial

Telecom-ISAC Japan

Established in July 2002

- As the first Information Sharing and Analysis Center (ISAC) in Japan
- 19 member companies including telecommunications carriers and ISPs
- The objective is to enhance security countermeasures for the information and telecommunication industry, by establishing a mechanism to share and to analyze the security incidents within the members

Cyber attack defense exercise

Anti-bot countermeasures project

19 member companies

Wide area monitoring

Information sharing

Incident handling

Reputation database system

Route monitoring system

Proactive Response Against Cyber-attacks Through International Collaborative Exchange

What’s PRACTICE?

PRACTICE, Proactive Response Against Cyber-attacks Through International Collaborative Exchange, has started with support from the Ministry of Internal Affairs and Communications.

ACTIVITIES

- Detect and Analyze Cyber-attacks through International Collaboration
- Predict Emerging Cyber-attacks
(Early Detection of Emerging Risks)
- Take Countermeasures
(Quick Response)

Objective of Field Trial (PRACTICE-FT)

Establish ISPs’ Quick Response Scheme through International Collaboration.

Major Players & Roles in PRACTICE

- PRACTICE-FT is trying to establish Quick Response Scheme.

PRACTICE Field Trial (PRACTICE-FT)

•Detect & Analyze Cyber-attacks
•Countermeasures (Quick Response Scheme)

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

NTT Communications

ISP Collaboration

PRACTICE

Sponsored by MIC

MIC
Ministry of Internal Affairs and Communications

International Collaboration

Foreign organizations
(Government, ISP…)

•Data Sharing
•Discussion
•Countermeasures

•Research
•Prediction
(Early Detection
of Cyber-attacks)
•Warning

PRACTICE R&D

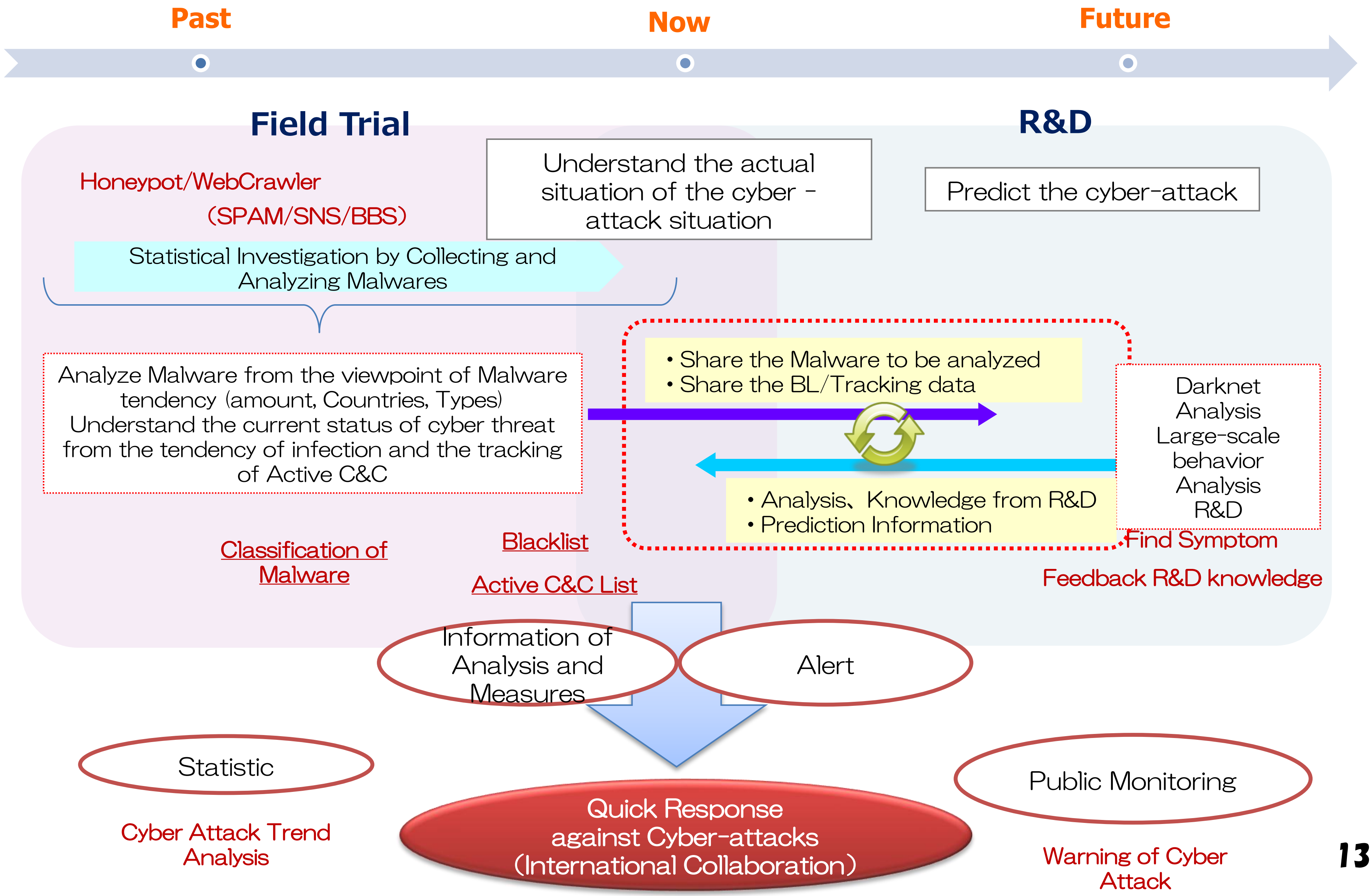
KDDI Designing The Future Etc.

Supported by NICT

NICT National Institute of Information and Communications Technology

Ref）Collaboration with PRACTICE R&D Team

Scope of field trial and R&D



Past

Now

Future

Field Trial

R&D

Honeypot/WebCrawler
（SPAM/SNS/BBS）

Understand the actual situation of the cyber - attack situation

Predict the cyber-attack

Statistical Investigation by Collecting and Analyzing Malwares

Analyze Malware from the viewpoint of Malware tendency (amount, Countries, Types)
Understand the current status of cyber threat from the tendency of infection and the tracking of Active C&C

- Share the Malware to be analyzed
- Share the BL/Tracking data

Darknet Analysis
Large-scale behavior Analysis
R&D

- Analysis、Knowledge from R&D
- Prediction Information

Classification of Malware

Blacklist

Active C&C List

Find Symptom

Feedback R&D knowledge

Information of Analysis and Measures

Alert

Statistic

Cyber Attack Trend Analysis

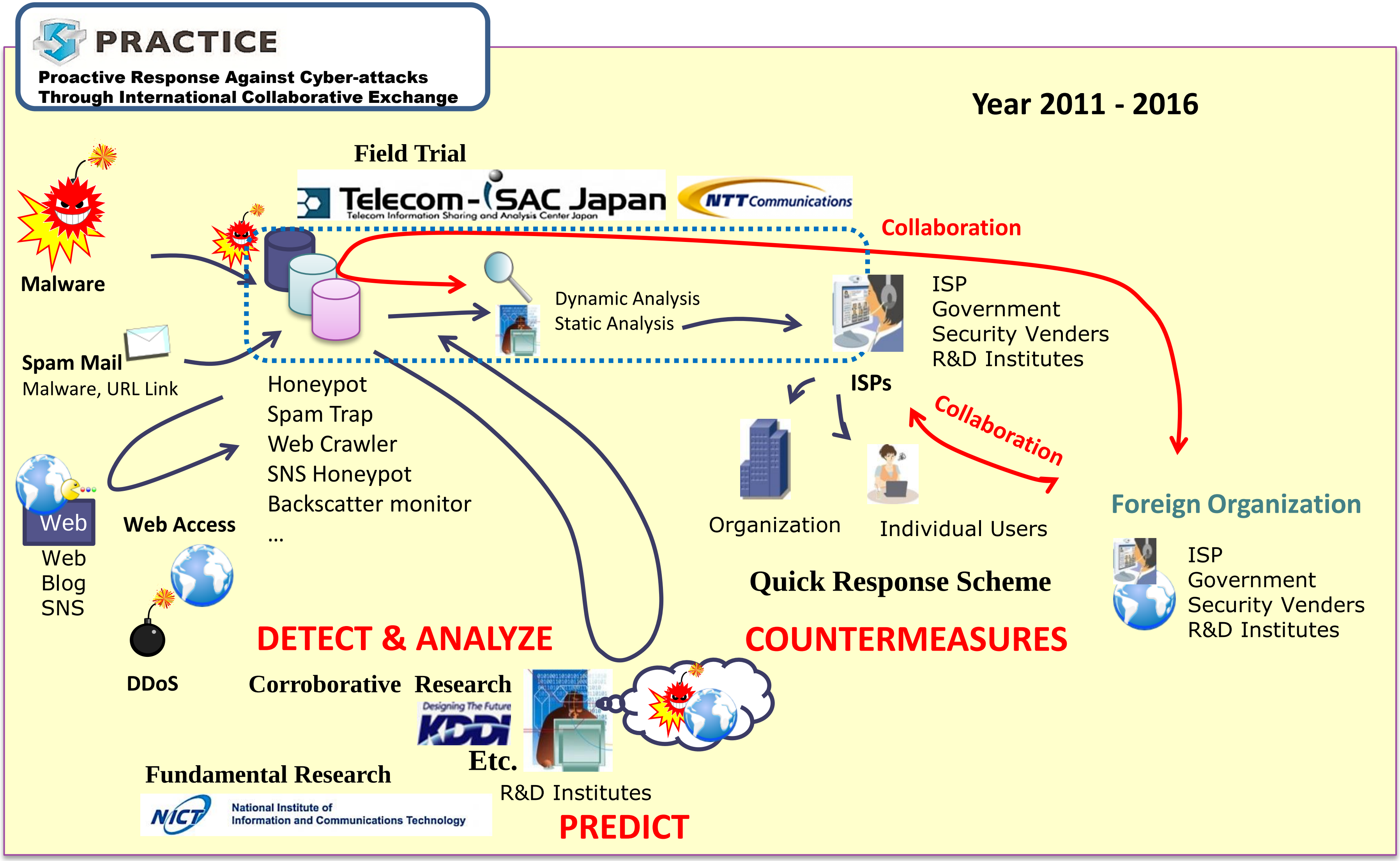
Quick Response against Cyber-attacks (International Collaboration)

Public Monitoring

Warning of Cyber Attack

Activities of PRACTICE

- Establish Quick Response Scheme against Cyber-attacks.



PRACTICE

Proactive Response Against Cyber-attacks Through International Collaborative Exchange

Year 2011 - 2016

Field Trial

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

NTT Communications

Collaboration

Malware

Spam Mail
Malware, URL Link

Web
Web
Blog
SNS

Web Access

DDoS

Honeypot
Spam Trap
Web Crawler
SNS Honeypot
Backscatter monitor
…

Dynamic Analysis
Static Analysis

ISP
Government
Security Venders
R&D Institutes

ISPs

Organization

Individual Users

Collaboration

Foreign Organization

ISP
Government
Security Venders
R&D Institutes

Quick Response Scheme

DETECT & ANALYZE

COUNTERMEASURES

Corroborative Research

Designing The Future
KDDI

Etc.

Fundamental Research

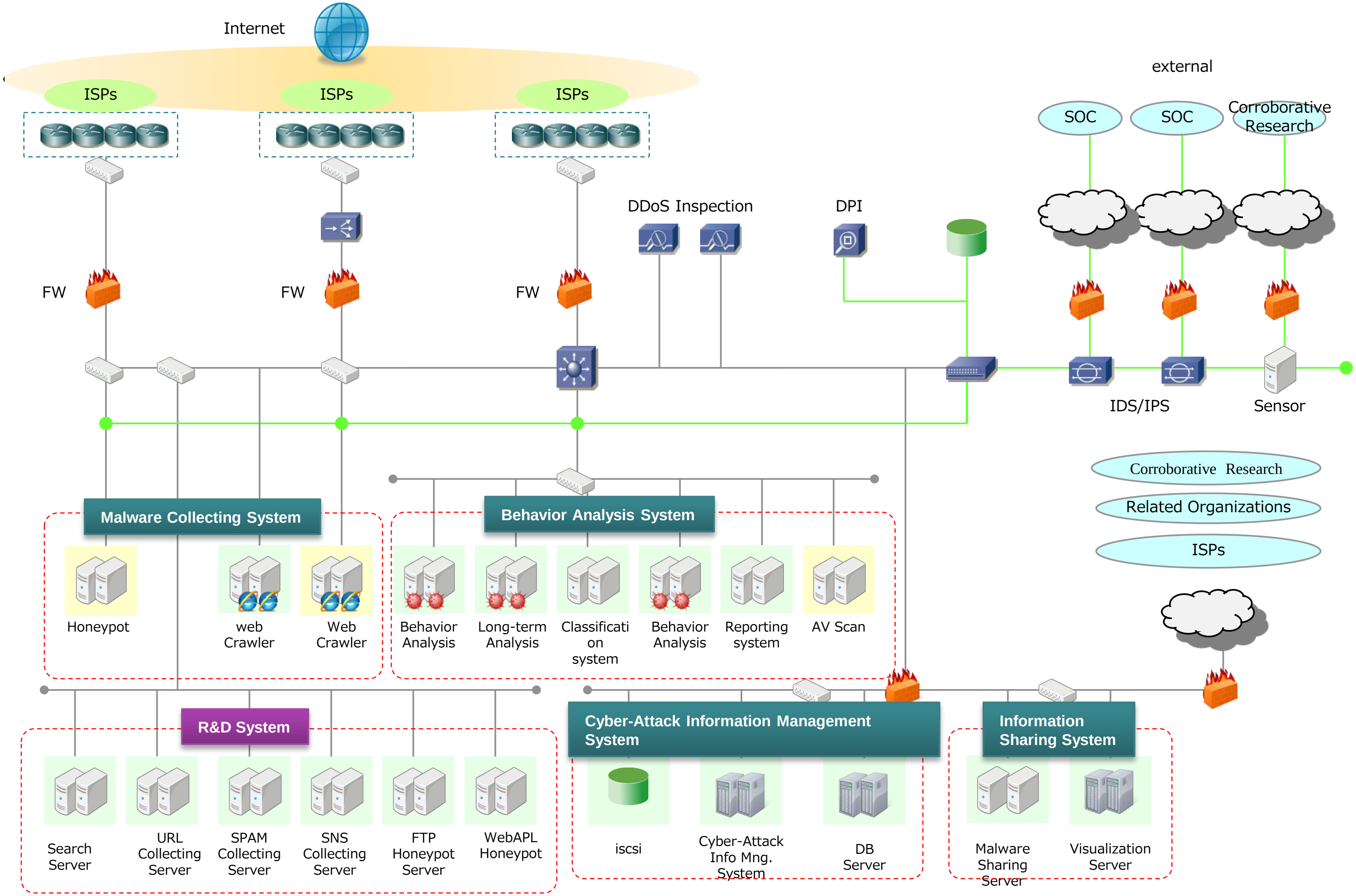
NICT
National Institute of Information and Communications Technology

R&D Institutes

PREDICT

System Configuration

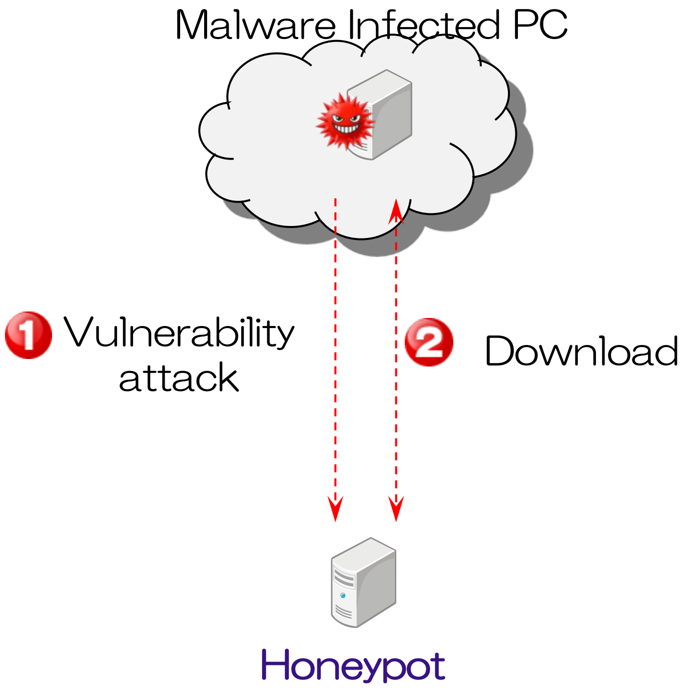
- **Build Systems to Detect and Analyze Various types of Cyber-attacks.**



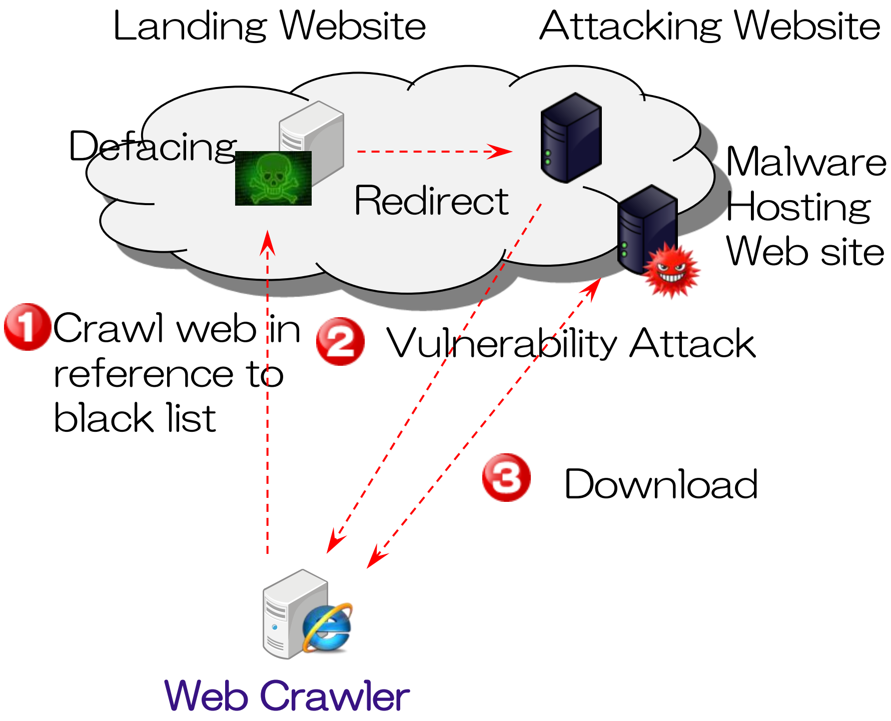
Malware Detecting Systems

- Honeypot collects Network Infection Malwares.
- Web Crawler collects Malicious URL and Web Infection Malwares.

【Network Infection Detecting System】



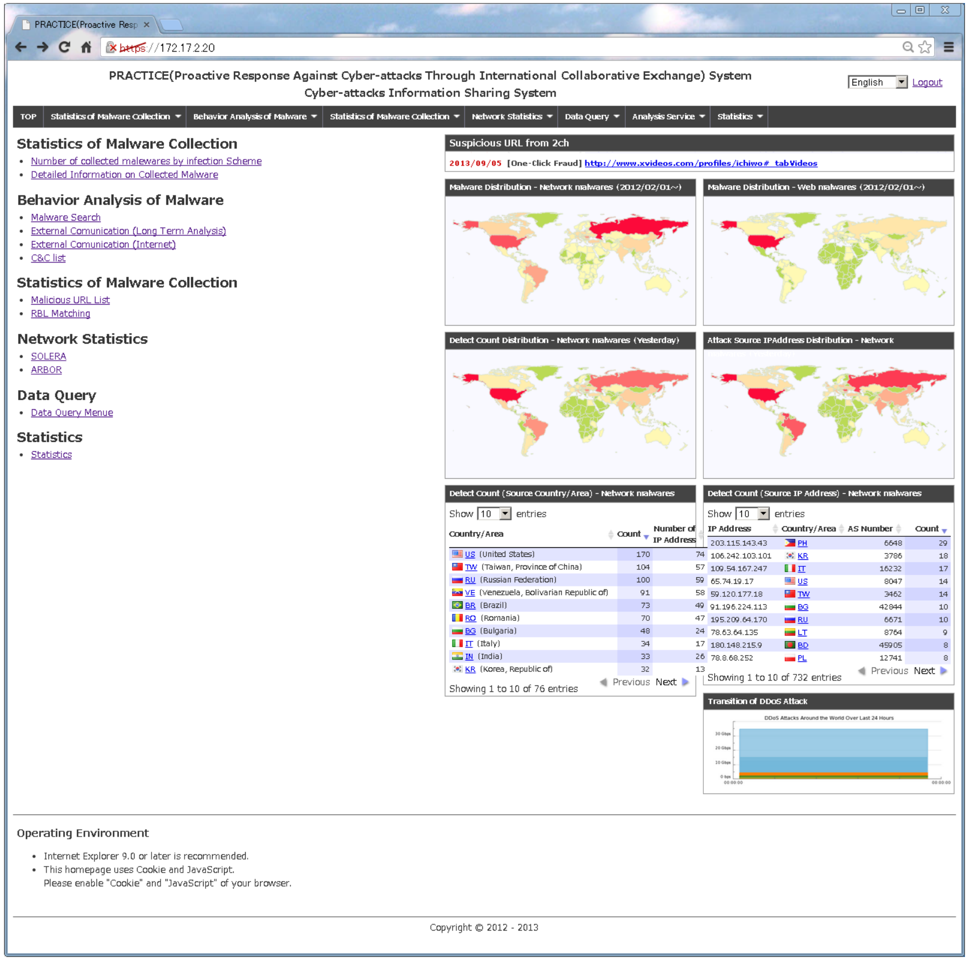
【Web Infection Detecting System】



Data Sharing with ISPs

- Information Sharing System Provides Cyber-attack Information detected and analyzed by PRACTICE System.

Information Sharing System


PRACTICE(Proactive Resp ×
~~https~~://172.17.2.20
English
Logout
TOP
Statistics of Malware Collection
Behavior Analysis of Malware
Statistics of Malware Collection
Network Statistics
Data Query
Analysis Service
Statistics
DDoS Attacks Around the World Over Last 24 Hours
30 Gbps
20 Gbps
10 Gbps
0 bps

PRACTICE(Proactive Response Against Cyber-attacks Through International Collaborative Exchange) System
Cyber-attacks Information Sharing System

Statistics of Malware Collection
- Number of collected malewares by infection Scheme
- Detailed Information on Collected Malware

Behavior Analysis of Malware
- Malware Search
- External Comunication (Long Term Analysis)
- External Comunication (Internet)
- C&C list

Statistics of Malware Collection
- Malicious URL List
- RBL Matching

Network Statistics
- SOLERA
- ARBOR

Data Query
- Data Query Menue

Statistics
- Statistics

Suspicious URL from 2ch

2013/09/05 [One-Click Fraud] http://www.xvideos.com/profiles/ichiwo#_tabVideos

Malware Distribution - Network malwares (2012/02/01~)

Malware Distribution - Web malwares (2012/02/01~)

Detect Count Distribution - Network malwares (Yesterday)

Attack Source IPAddress Distribution - Network

Detect Count (Source Country/Area) - Network malwares

Show 10 entries

Country/Area	Count	Number of IP Address
US (United States)	170	74
TW (Taiwan, Province of China)	104	57
RU (Russian Federation)	100	59
VE (Venezuela, Bolivarian Republic of)	91	58
BR (Brazil)	73	49
RO (Romania)	70	47
BG (Bulgaria)	48	24
IT (Italy)	34	17
IN (India)	33	26
KR (Korea, Republic of)	32	13

Showing 1 to 10 of 76 entries ◀ Previous Next ▶

Detect Count (Source IP Address) - Network malwares

Show 10 entries

IP Address	Country/Area	AS Number	Count
203.115.143.43	PH	6648	29
106.242.103.101	KR	3786	18
109.54.167.247	IT	16232	17
65.74.19.17	US	8047	14
59.120.177.18	TW	3462	14
91.196.224.113	BG	42844	10
195.209.64.170	RU	6671	10
78.63.64.135	LT	8764	9
180.148.215.9	BD	45905	8
78.8.68.252	PL	12741	8

Showing 1 to 10 of 732 entries ◀ Previous Next ▶

Transition of DDoS Attack

Operating Environment
- Internet Explorer 9.0 or later is recommended.
- This homepage uses Cookie and JavaScript.
  Please enable "Cookie" and "JavaScript" of your browser.

Copyright © 2012 - 2013

- Statistics of Malware Collection
- Behavior Analysis of Malware
- Malicious web
- Analysis Service
- Data Query

International Collaboration

- International Collaboration is a KSF.

Necessity of International Collaboration

- Cyber-attacks are borderless.
  90% of attacks detected by honeypot come from outside of Japan.
- Difficult to detect various types of cyber-attacks.
- Impossible to take countermeasures without International Collaboration.

To fight against Cyber-attacks, We would like to Collect and Share Cyber-attack Data through the International Collaboration

Currently, Discussing with

- ID-SIRTII (Indonesia)
- ETDA (Thailand)
- MCMC (Malaysia)
- Others

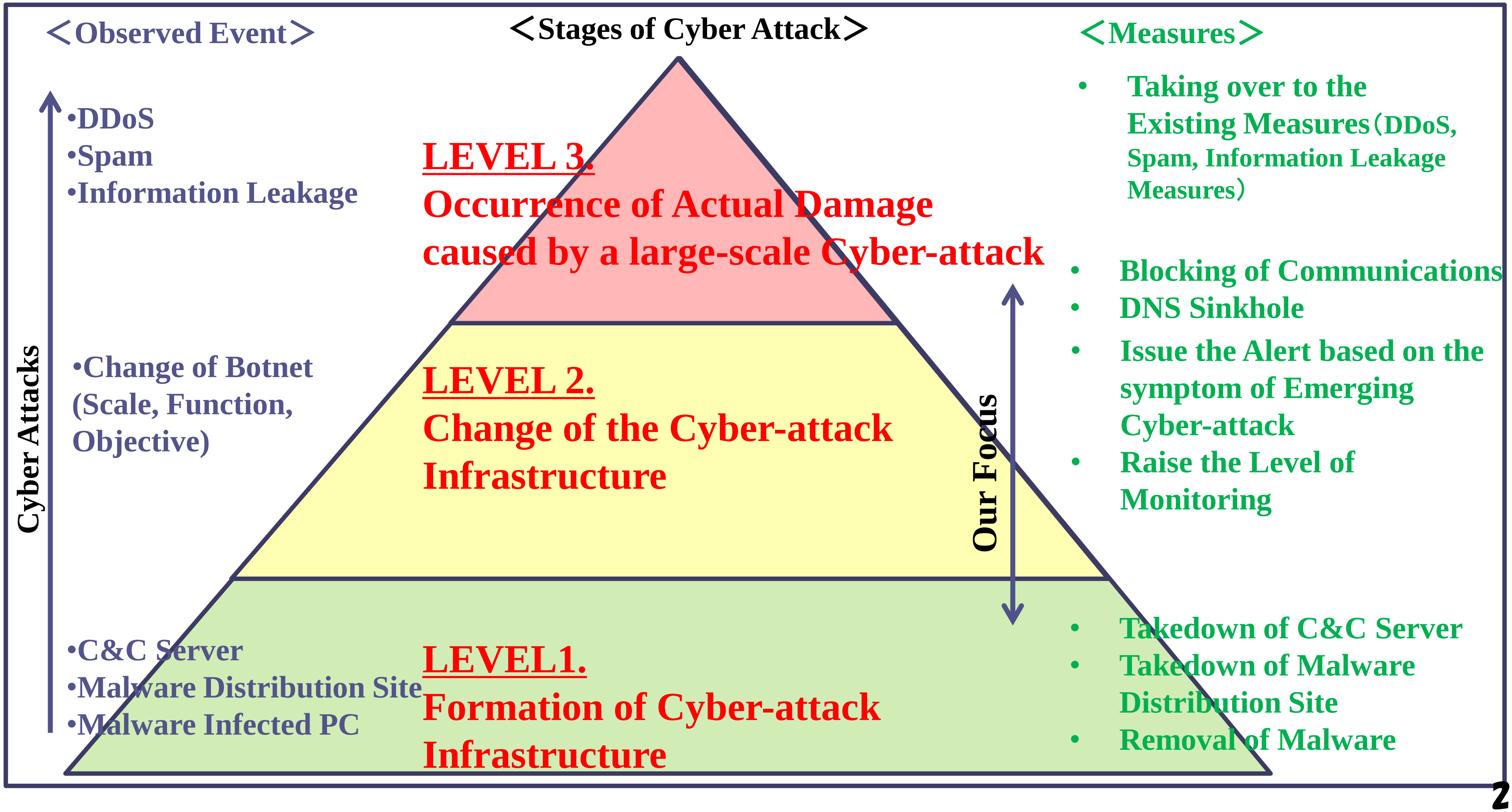
- Share Cyber-attack Information
- Analyze and Understand the Reality of Cyber-attack
- Find a symptom of Cyber-attack
- Quick Response

Quick Response against Cyber-attacks

Building Quick Response Scheme against Cyber Attack

Scope of PRACTICE Activities

- Find a Symptom of Cyber-attack by Observing Cyber-attack Infrastructure
- Build Quick Response Scheme
- Prevent the Damages before a Large-scale Cyber-attack occurs



＜Observed Event＞

＜Stages of Cyber Attack＞

＜Measures＞

Cyber Attacks

•DDoS
•Spam
•Information Leakage

LEVEL 3.
Occurrence of Actual Damage caused by a large-scale Cyber-attack

- Taking over to the Existing Measures（DDoS, Spam, Information Leakage Measures）

- Blocking of Communications
- DNS Sinkhole

•Change of Botnet (Scale, Function, Objective)

LEVEL 2.
Change of the Cyber-attack Infrastructure

Our Focus

- Issue the Alert based on the symptom of Emerging Cyber-attack
- Raise the Level of Monitoring

•C&C Server
•Malware Distribution Site
•Malware Infected PC

LEVEL1.
Formation of Cyber-attack Infrastructure

- Takedown of C&C Server
- Takedown of Malware Distribution Site
- Removal of Malware

Phase of Quick Response

- Consider Three Phases to respond an Emerging Cyber-attack quickly.

Zero-day Quick Response

Prevent Cyber-attack Damage before Cyber-attack-Infrastructure is Utilized

- Take down Malware-distribution Site
- Remove Malware from Malware-infected PC
- Take down C&C Server

Raise the Monitoring Level

Raise the Monitoring Level based on the Information on Cyber-attack symptoms

- Issue the Alert
- Raise the Monitoring Level
- Plan the Measures

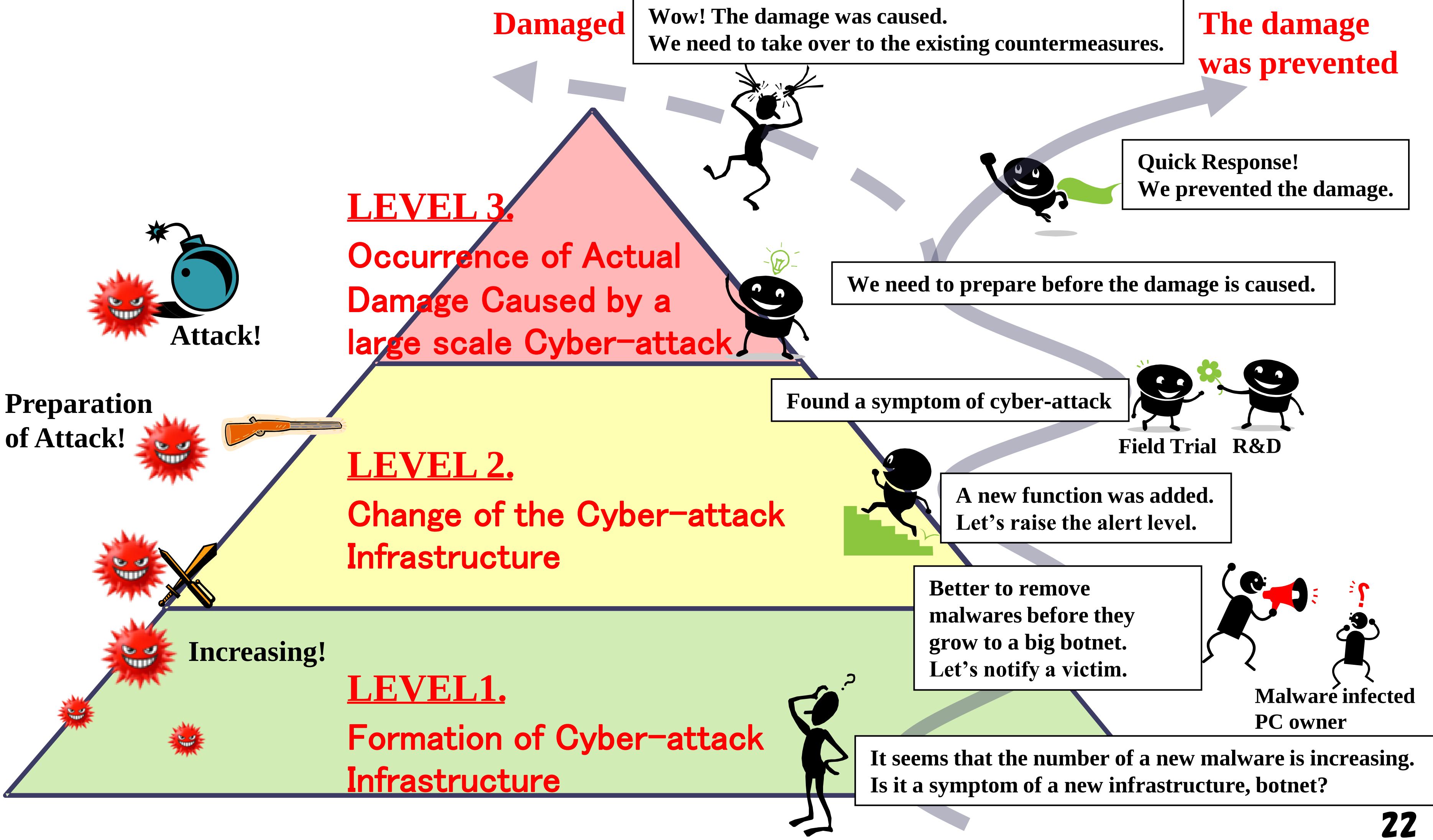
Quick Response（Measures）

Issue the Alert before Cyber-attack occurs or at an early stage, forward the Information to the existing measures (DDoS, Spam and Information Leakage) and block the Communication Channels as an Emergency Evacuation, if necessary

- Block Communication Channels to certain IP address, Port, or URL
- DNS Sinkhole

Example of Quick Response against Cyber-attack

- We monitor Cyber-attack in each level and take actions according to the level.



Damaged

Wow! The damage was caused.
We need to take over to the existing countermeasures.

The damage was prevented

Quick Response!
We prevented the damage.

LEVEL 3.

Occurrence of Actual Damage Caused by a large scale Cyber-attack

Attack!

We need to prepare before the damage is caused.

Found a symptom of cyber-attack

Field Trial R&D

Preparation of Attack!

LEVEL 2.

Change of the Cyber-attack Infrastructure

A new function was added.
Let’s raise the alert level.

Better to remove malwares before they grow to a big botnet.
Let’s notify a victim.

Malware infected PC owner

Increasing!

LEVEL1.

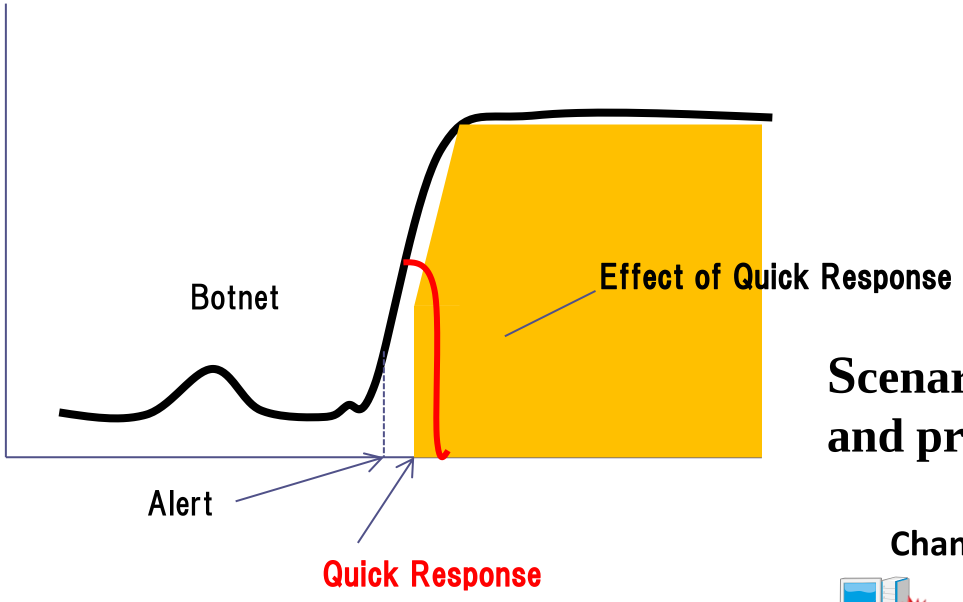
Formation of Cyber-attack Infrastructure

It seems that the number of a new malware is increasing.
Is it a symptom of a new infrastructure, botnet?

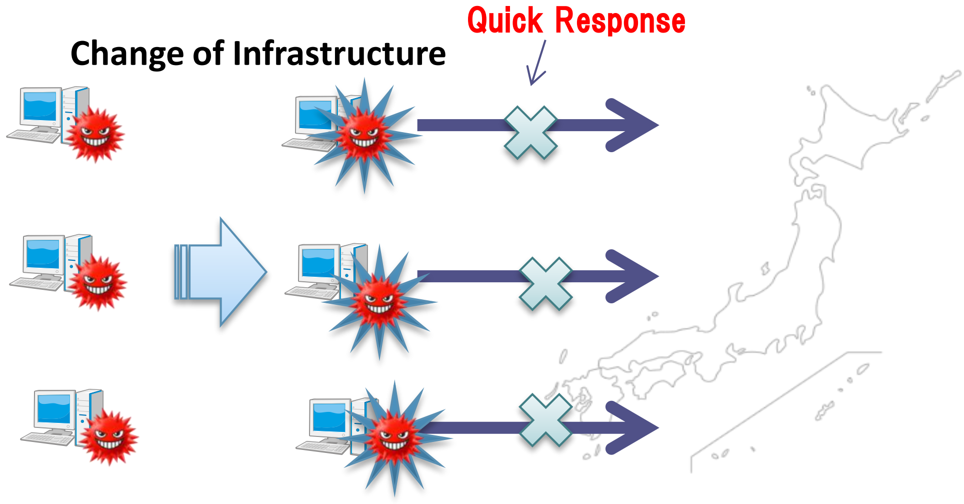
Scenarios of Quick Response

- Draw up scenarios according to each level.

Scenario 1. Detect and Takedown an emerging botnet



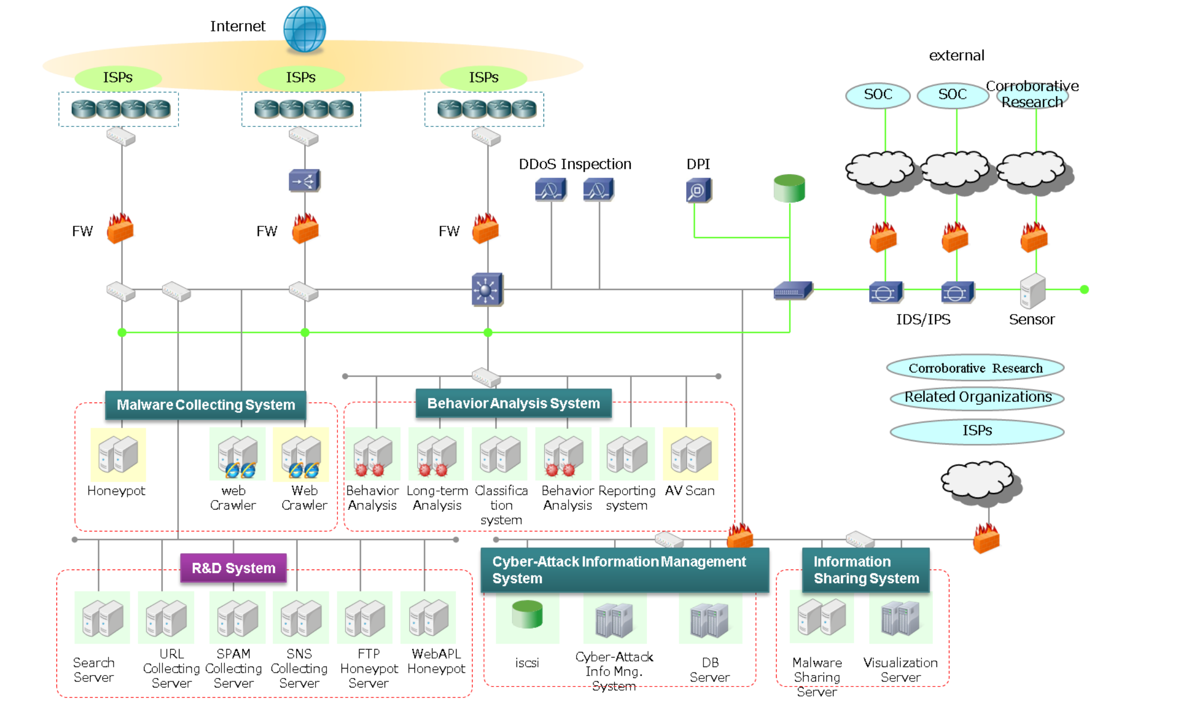
Scenario 2. Detect a change of infrastructure and prevent the occurrence of damage



Approach to Finding Symptom

- Collect and Analyze Various kinds of Cyber-attacks
- Find Symptom of Emerging Cyber-attack

Field Trial System



Deploy and Operate Field Trial System which detects various cyber attacks

＜Features＞

・Collect and Analyze Information over a long duration

・Backed up Technically, Reliable own collected data

・Large-scale System

・Information Sharing System which can aggregate data in various terms (Malaware, Countries, Duration)

Symptom Analysis

Provide Data to R&D Team

・Malware Sample

・Communication Log

・ Alert the Symptom of Cyber-attacks

・Find the Initial Behavior of Botnet

Our Approach (Field Trial Team)

①Find a change of the number of Cyber-attacks

②Estimate the Possibility of emerging cyber attack risk in Japan by observing global data

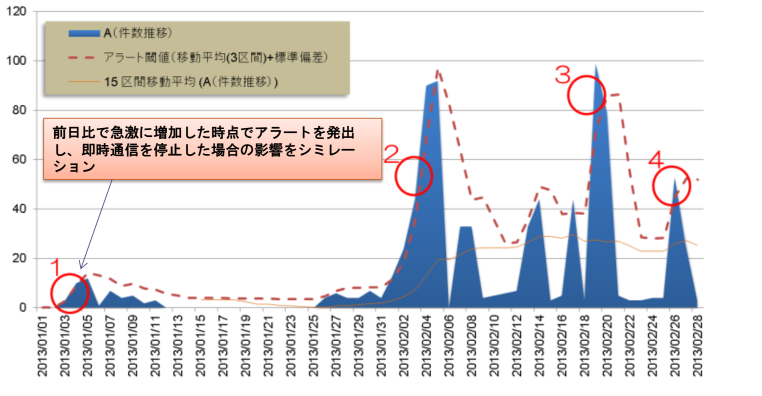
Quick Response

- Zero-day Quick Response
- Increase Monitoring
- Quick Response (Measure)

Approach to Finding Symptom
Field Trial Team's Approach

- Analyze 7-year Cyber-attack Data Collected through the Cyber Clean Center and PRACICE Project
- Estimate the Impact in case that Cyber-attack is Blocked in Early Stage

①Find a change of the number of Cyber-attacks

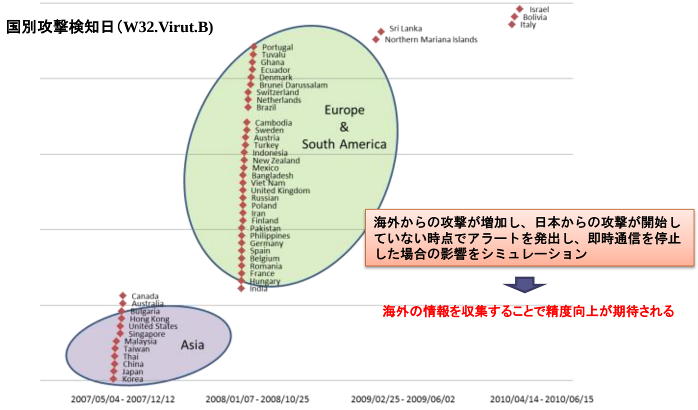


前日比で急激に増加した時点でアラートを発出し、即時通信を停止した場合の影響をシミレーション

- 項目Ａに関する日次推移件数が「アラート閾値」を越えたときにアラート情報を上げる。
- 「アラート閾値」は日次推移件数の「移動平均（3区間）」＋「日標準偏差」から求める。

②Estimate the Possibility of Emerging Cyber-attack risk in Japan by observing Global Data

国別攻撃検知日（W32.Virut.B)



海外からの攻撃が増加し、日本からの攻撃が開始していない時点でアラートを発出し、即時通信を停止した場合の影響をシミュレーション

海外の情報を収集することで精度向上が期待される

- W32.Virut.BがCCCのハニーポットで国別で初めて収集された年月日でプロット

Write an Algorithm which calculates a Symptom for Quick Response

Validate the Algorithm by Using Accumulated Real Data

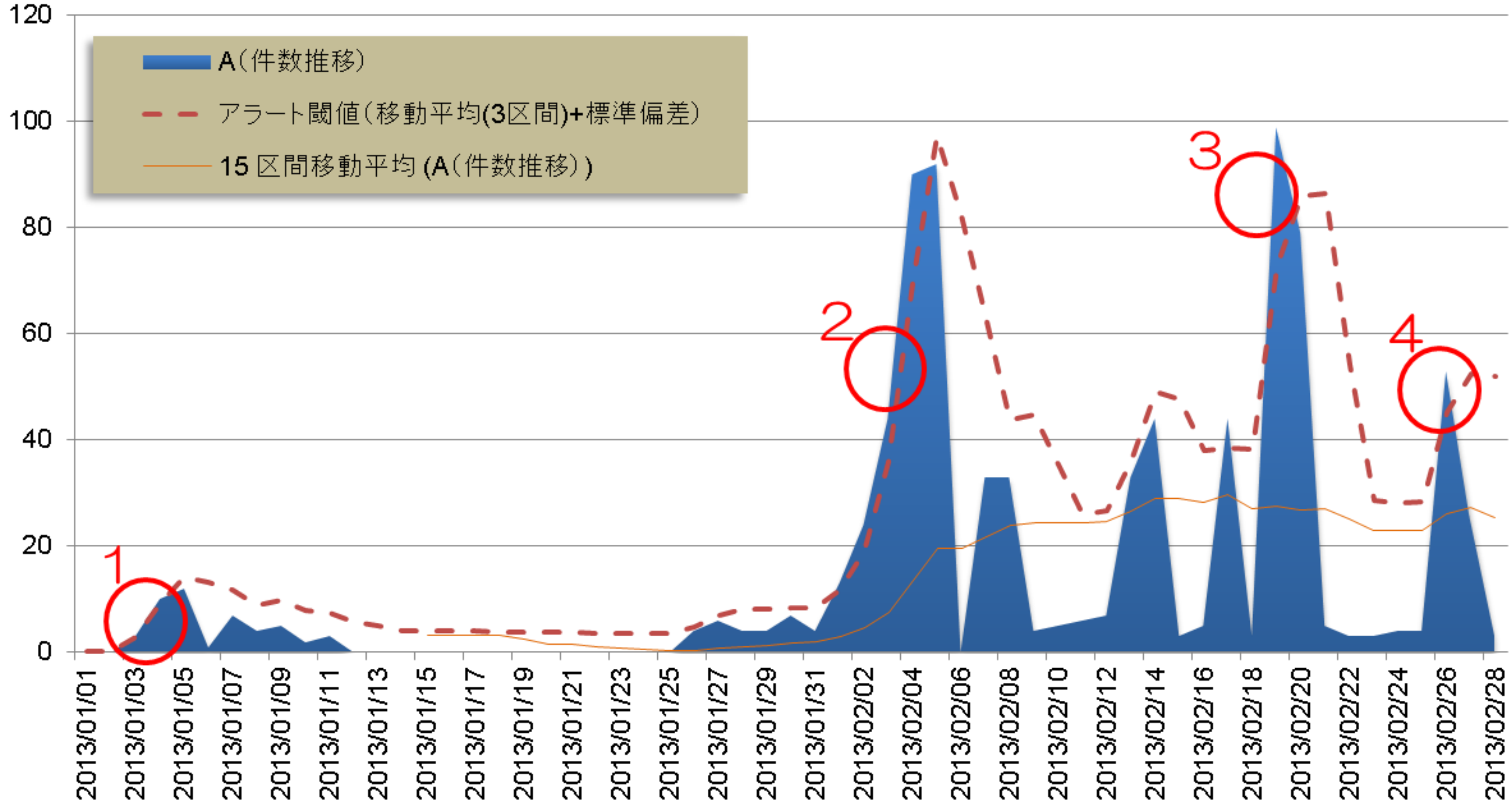
Find the best algorithm and parameter, and implement a function which issues the alert in the system.

Approach to Finding Symptom

Field Trial Team's Approach

- Issue the alert by analyzing the malware trend.

①Find a change of the number of Cyber-attacks

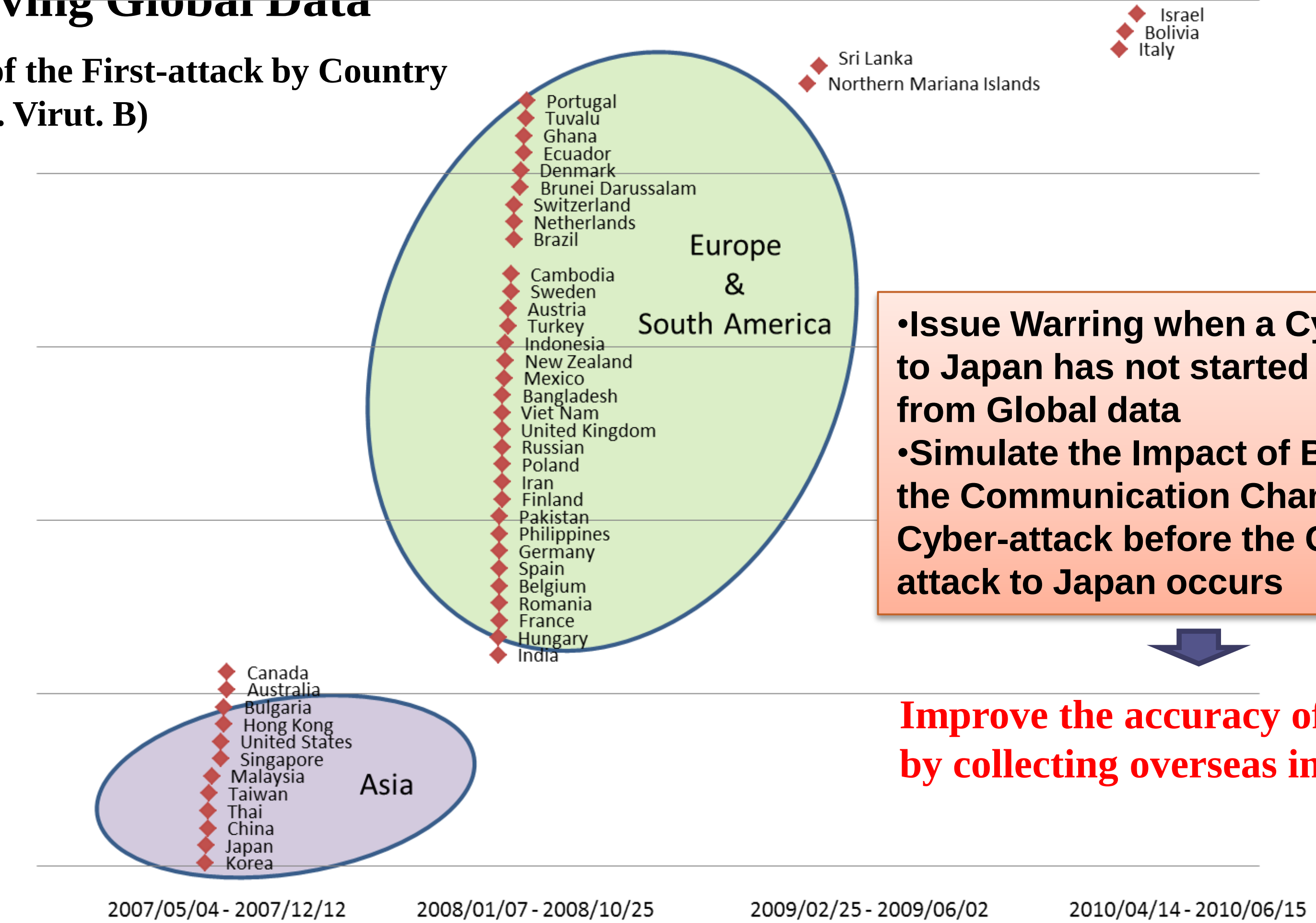


Approach to Finding Symptom
Field Trial Team's Approach

- Find the verity of Cyber-attack trend according to the region.

②Estimate the Possibility of Emerging Cyber-attack risk in Japan by observing Global Data

Date of the First-attack by Country
（W32. Virut. B)



•Issue Warring when a Cyber-attack to Japan has not started judging from Global data
•Simulate the Impact of Blocking the Communication Channel of Cyber-attack before the Cyber-attack to Japan occurs

Improve the accuracy of estimation by collecting overseas information

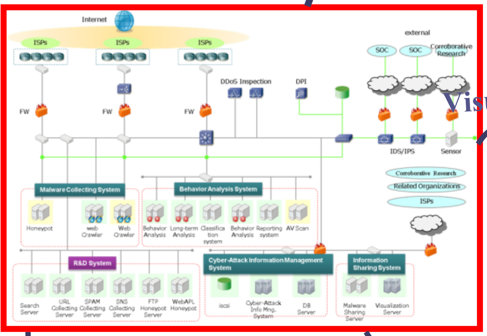
Utilizing PRACTICE Data

- PRACTICE Data can be utilized in Various Applications.

Quick Response (Countermeasures)

Symptom

Field Trial System



Statistics

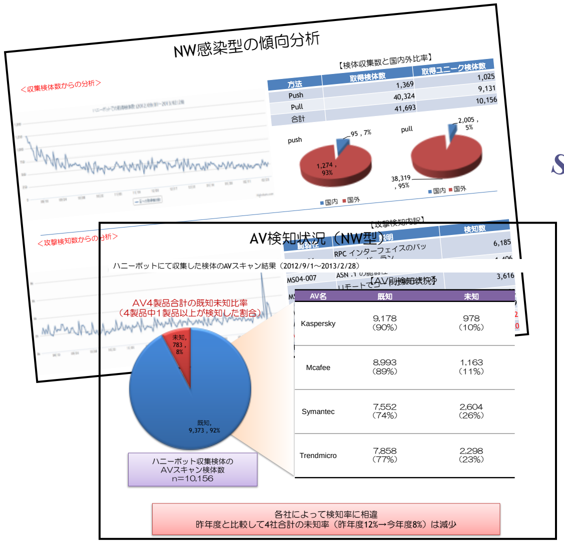
Visualization

Analysis

Blacklist

Data Sharing

Statistics



NW感染型の傾向分析

＜収集検体数からの分析＞

【検体収集数と国内外比率】

方法	取得検体数	取得ユニーク検体数
Push	1,369	1,025
Pull	40,324	9,131
合計	41,693	10,156

＜攻撃検知数からの分析＞

【攻撃検知内訳】

脆弱性	説明	検知数
	RPC インターフェイスのバッ	6,185
MS04-007	ASN.1 の脆弱性	3,616

AV検知状況（NW型）

ハニーポットにて収集した検体のAVスキャン結果（2012/9/1～2013/2/28）

AV4製品合計の既知未知比率
（4製品中1製品以上が検知した割合）

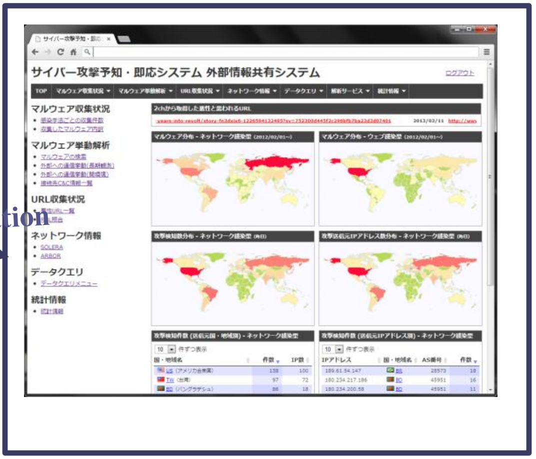
ハニーポット収集検体の
AVスキャン検体数
n=10,156

【AV別検知状況】

AV名	既知	未知
Kaspersky	9,178 （90%）	978 （10%）
Mcafee	8,993 （89%）	1,163 （11%）
Symantec	7,552 （74%）	2,604 （26%）
Trendmicro	7,858 （77%）	2,298 （23%）

各社によって検知率に相違
昨年度と比較して4社合計の未知率（昨年度12%→今年度8%）は減少

Information Sharing System



サイバー攻撃予知・即応システム 外部情報共有システム

ログアウト

マルウェア収集状況
- 感染手法ごとの収集件数
- 収集したマルウェア内訳

マルウェア挙動解析
- マルウェアの検索
- 外部への通信挙動(長期観測)
- 外部への通信挙動(疑似環境)
- 接続先C&C情報一覧

URL収集状況
- 悪性URL一覧
- URL照合

ネットワーク情報
- SOLERA
- ARBOR

データクエリ
- データクエリメニュー

統計情報
- 統計情報

2chから取得した悪性と思われるURL

2013/03/11

マルウェア分布 - ネットワーク感染型 (2012/02/01～)

マルウェア分布 - ウェブ感染型 (2012/02/01～)

攻撃検知数分布 - ネットワーク感染型 (昨日)

攻撃送信元IPアドレス数分布 - ネットワーク感染型 (昨日)

攻撃検知件数 (送信元国・地域別) - ネットワーク感染型

10 件ずつ表示

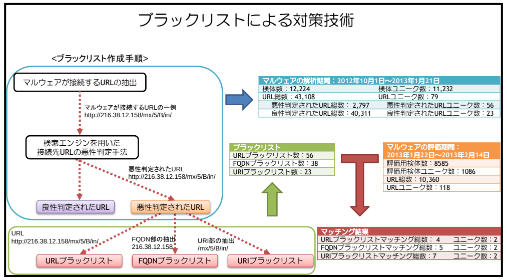
国・地域名	件数	IP数
US (アメリカ合衆国)	138	100
TW (台湾)	97	72
BD (バングラデシュ)	86	18

攻撃検知件数 (送信元IPアドレス別) - ネットワーク感染型

10 件ずつ表示

IPアドレス	国・地域名	AS番号	件数
189.61.54.147	BR	28573	18
180.234.217.186	BD	45951	16
180.234.200.58	BD	45951	11

Blacklist



ブラックリストによる対策技術

<ブラックリスト作成手順>

マルウェアの解析期間：2012年10月1日～2013年1月21日

検体数：12,224	検体ユニーク数：11,232
URL総数：43,108	URLユニーク数：79
悪性判定されたURL総数： 2,797	悪性判定されたURLユニーク数：56
良性判定されたURL総数：40,311	良性判定されたURLユニーク数：23

ブラックリスト
- URLブラックリスト数：56
- FQDNブラックリスト数：38
- URIブラックリスト数：23

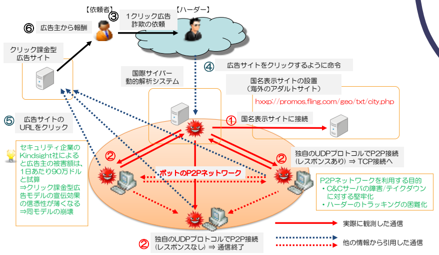
マルウェアの評価期間：
2013年1月22日～2013年2月14日
- 評価用検体数：8585
- 評価用検体ユニーク数：1086
- URL総数：10,360
- URLユニーク数：118

マッチング結果

URLブラックリストマッチング総数： 4	ユニーク数：2
FQDNブラックリストマッチング総数：5	ユニーク数：2
URIブラックリストマッチング総数：7	ユニーク数：2

Validation of Cyber-attack

「ZeroAccess」解析事例


【依頼者】
【ハーダー】
⑥ 広告主から報酬
③ 1クリック広告詐欺の依頼
クリック課金型広告サイト
④ 広告サイトをクリックするように命令
国際サイバー動的解析システム
国名表示サイトの設置（海外のアダルトサイト）
hxxp://promos.fling.com/geo/txt/city.php
⑤ 広告サイトのURLをクリック
① 国名表示サイトに接続
② 独自のUDPプロトコルでP2P接続（レスポンスあり）⇒ TCP接続へ
ボットのP2Pネットワーク
② 独自のUDPプロトコルでP2P接続（レスポンスなし）⇒ 通信終了
実際に観測した通信
他の情報から引用した通信

セキュリティ企業のKindsight社によると広告主の被害額は、1日あたり90万ドルと試算
⇒クリック課金型広告モデルの宣伝効果の信憑性が薄くなる
⇒同モデルの崩壊

P2Pネットワークを利用する目的
- C&Cサーバの障害/テイクダウンに対する堅牢化
- ハーダーのトラッキングの困難化

- •PRACTICE R&D Team⇒Prediction
- •NICT
- •Overseas PRACTICE Partner

Cyber-attacks observed by PRACTICE System

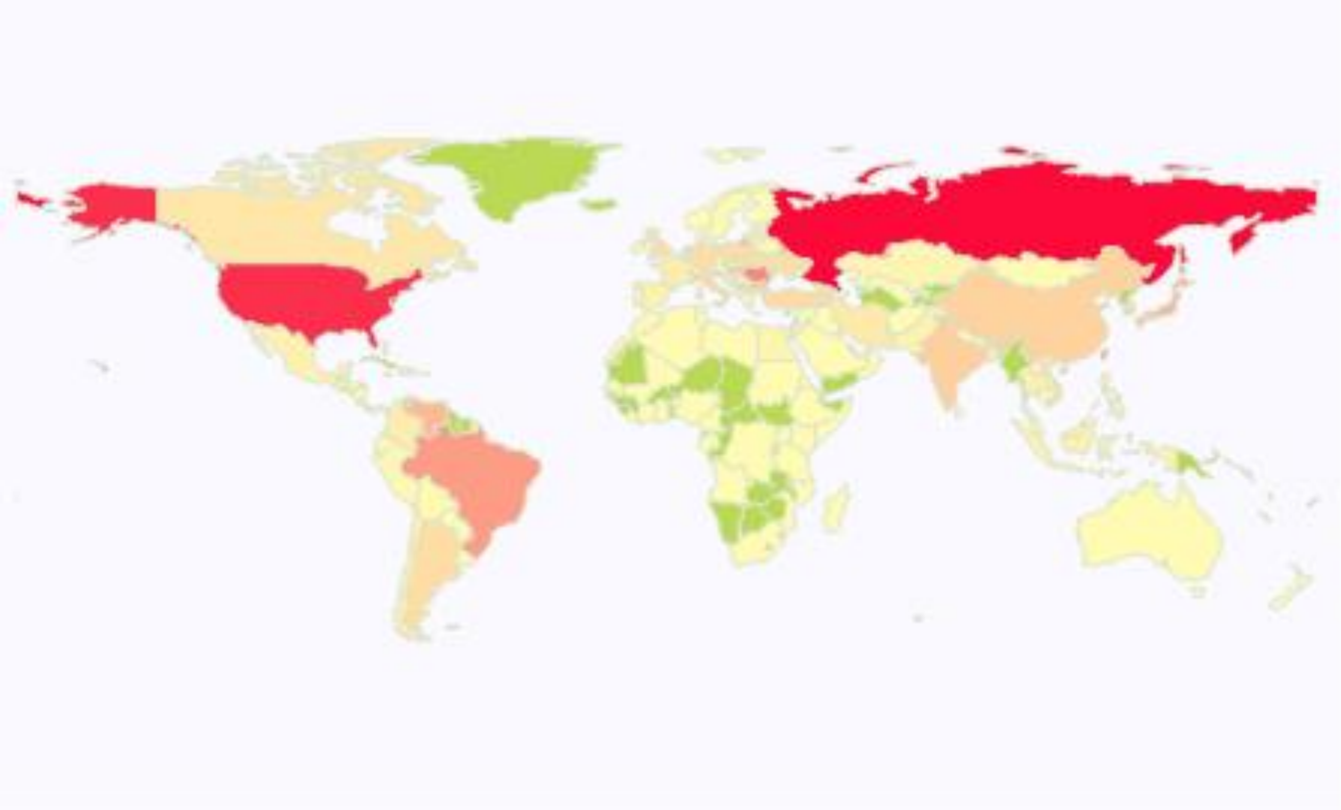
Where does malware come from?

Network Infection Malware

- Many network infection malwares come from Russia, US and Taiwan.

Number of Malware collected by honeypot

2013/01/01 ~ 2013/06/30



1	Russian Federation
2	United States
3	Taiwan, Province of China
4	Romania
5	Brazil
6	Japan
7	Venezuela, Bolivarian Republic of
8	Bulgaria
9	Hungary
10	Netherlands
11	India
12	China
13	Italy
14	Korea, Republic of
15	Turkey
16	Poland
17	Germany
18	United Kingdom
19	Argentina
20	Ukraine

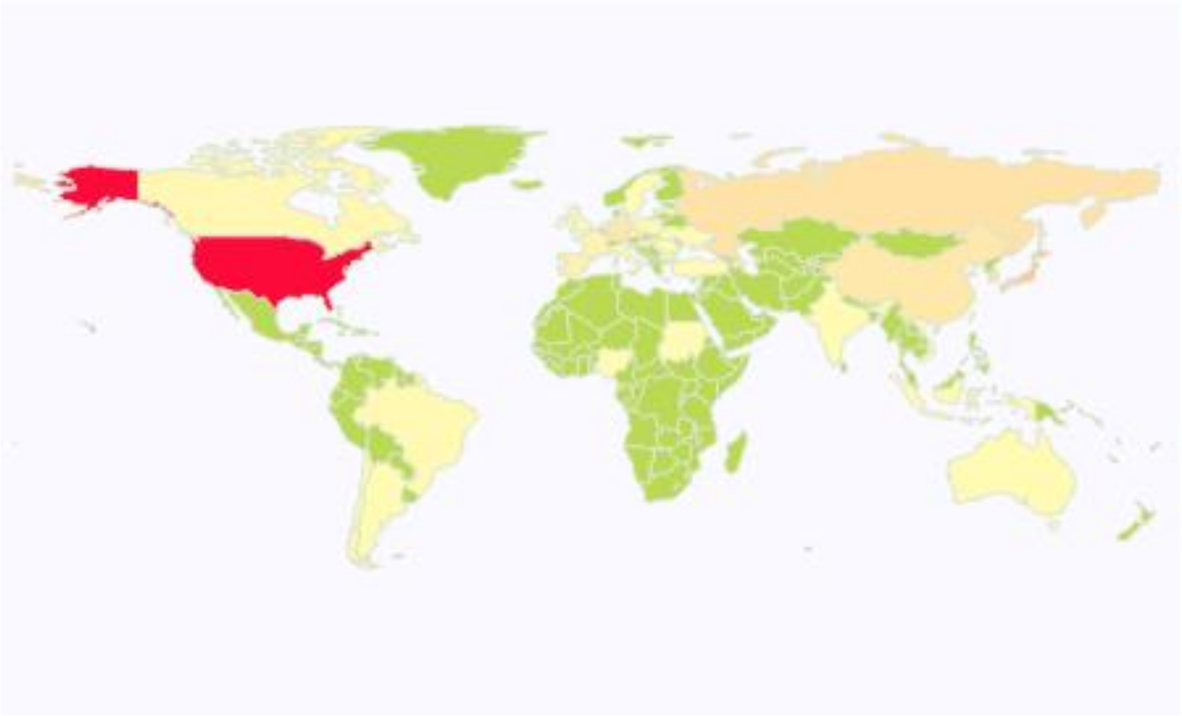
Where does malware come from?

Web Infection Malware

- 54% of web infection malwares come from US.

Number of Malware collected by Web crawler

2013/01/01 ~ 2013/06/30



1	United States
2	Japan
3	Korea, Republic of
4	Russian Federation
5	China
6	Germany
7	Spain
8	France
9	Czech Republic
10	Italy
11	EU
12	Hungary
13	Canada
14	Netherlands
15	Taiwan, Province of China
16	Poland
17	United Kingdom
18	Virgin Islands, British
19	Brazil
20	Australia

Malware and Vulnerability

- **Monthly statistics regarding malware and vulnerability remain as same as usual.**

2013/07/01 ~ 2013/07/31

◆Network Infection Malware Top5 [TrendMicro]

No.1	WORM_DOWNAD.AD
No.2	WORM_ALLAPLE.IK
No.3	Mal_DownAd-2
No.4	PE_VIRUT.AV
No5.	WORM_DOWNAD.DAM

◆Web Infection Malware Top5 [TrendMicro]

No.1	TROJ_CLIKER.SMB
No.2	TROJ_INJECT.AQW
No.3	TROJ_YSMARSYS.N
No.4	TROJ_VILSEL.BK
No.5	Mal_Socks1

◆Vulnerability used by
Network infection malware Top5

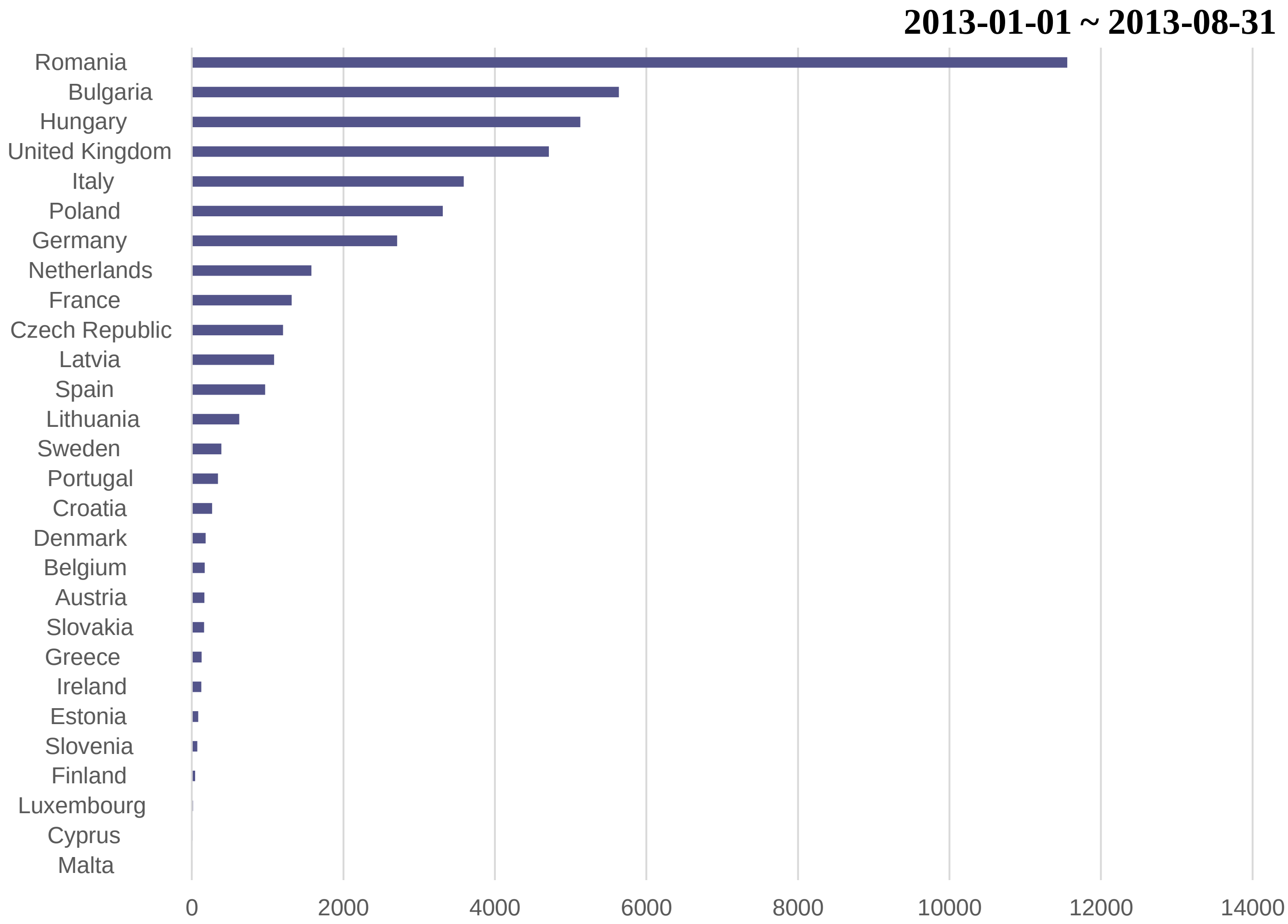
No.1	MS08-067
No.2	MS03-026
No.3	MS04-011
No.4	MS06-040
No.5	MS05-039

◆ Vulnerability used by
Web infection malware Top5

No.1	MS06-014
No.2	MS09-002
No.3	CVE-2008-2992
No.4	CVE-2009-0927
No.5	MS10-018

Number of Malwares from EU

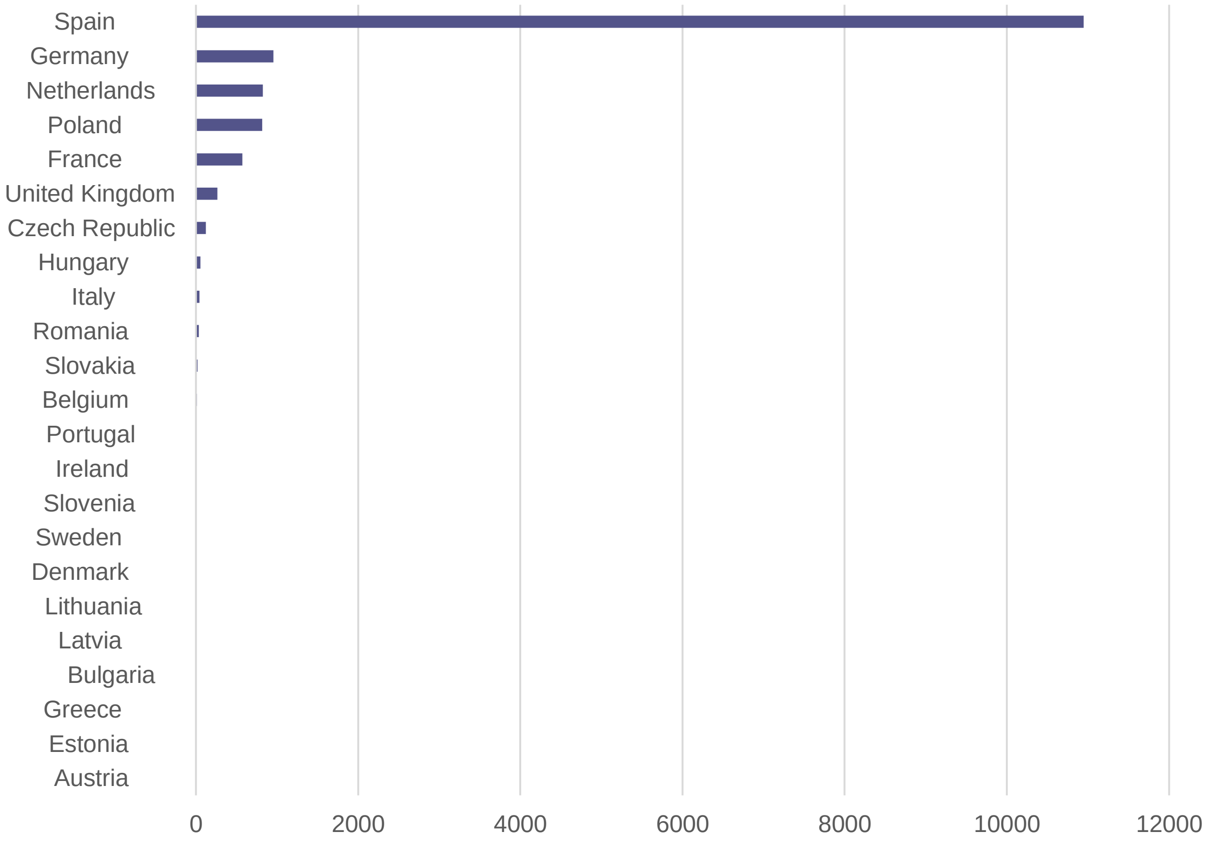
- PRACTICE system collects malware by honeypot.
- Most countries in world, number of malwares collected by honeypot is less than 1000.



Malicious URLs in EU

- PRACTICE system crawls malicious URLs based on own seed URL list.
- Spain has many malicious URLs that host malwares.
- Most countries have less than 100 URLs that host malwares

2013-01-01 ~ 2013-08-31



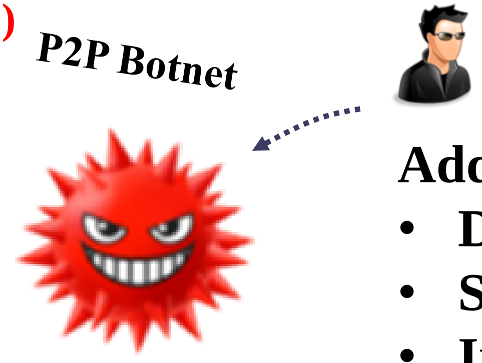
Case Studies on Cyber-attacks

Case 1. ZeroAccess

ZeroAccess could be used for a Large-scale Cyber-attack

- A Large number of ZeroAccess-infected PCs are in Japan.
- Currently, ZeroAccess is used for One-click fraud.

1,700,000 ZeroAccess-infected PCs were detected by PRACTICE System.
(Jan. 1 – Jun. 30, 2013)



Adding a New function is easy!

- DDoS
- Spam
- Information Exploitation

ZeroAccess

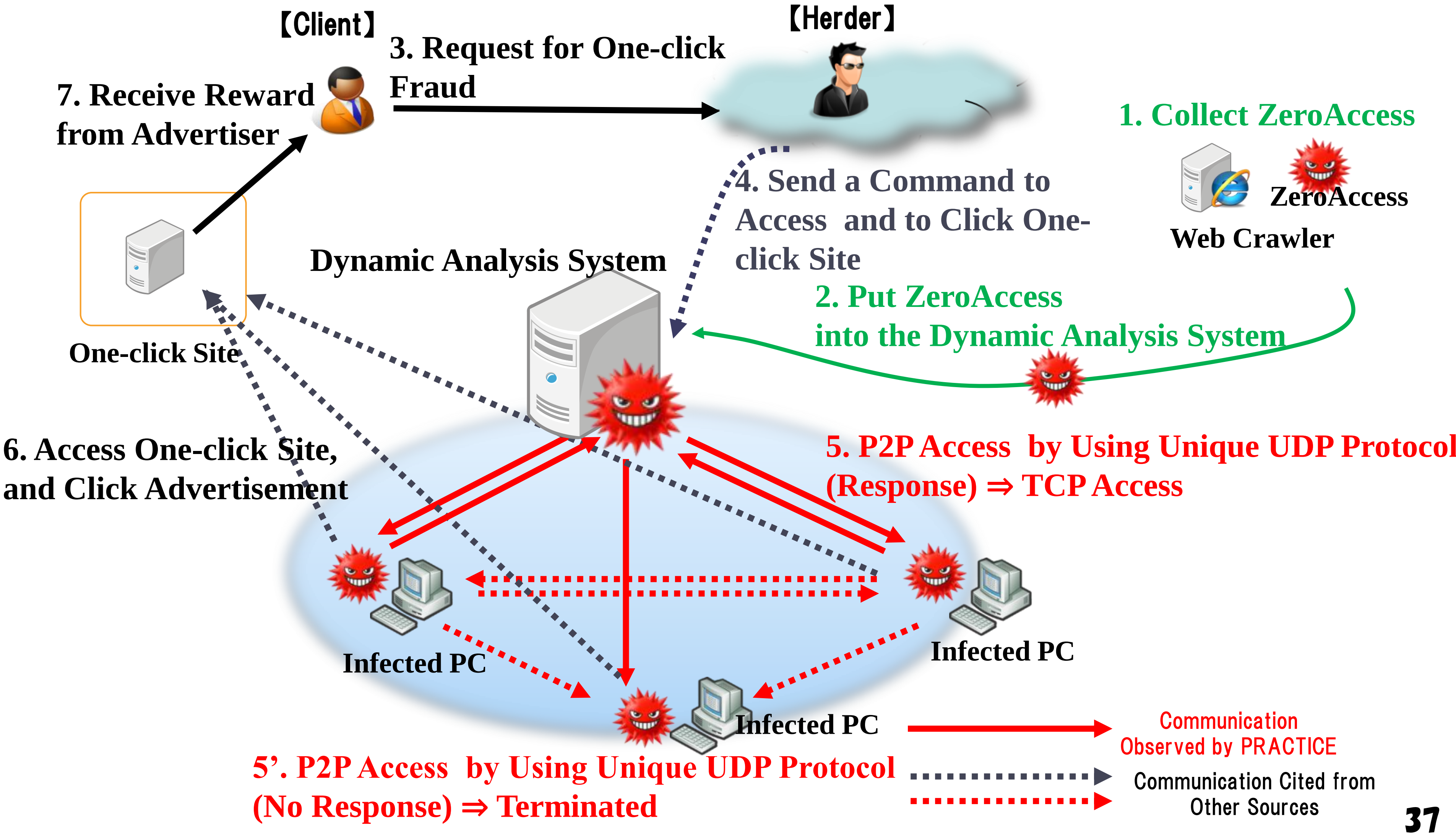
Form an Infrastructure for Cyber-attack (Botnet)

- **We are concerned that ZeroAccess will be used for a Large-scale Cyber-attack in the future.**
- **We are focusing and monitoring ZeroAccess.**

Case 1. ZeroAccess

Our Trial to Find a ZeroAccess

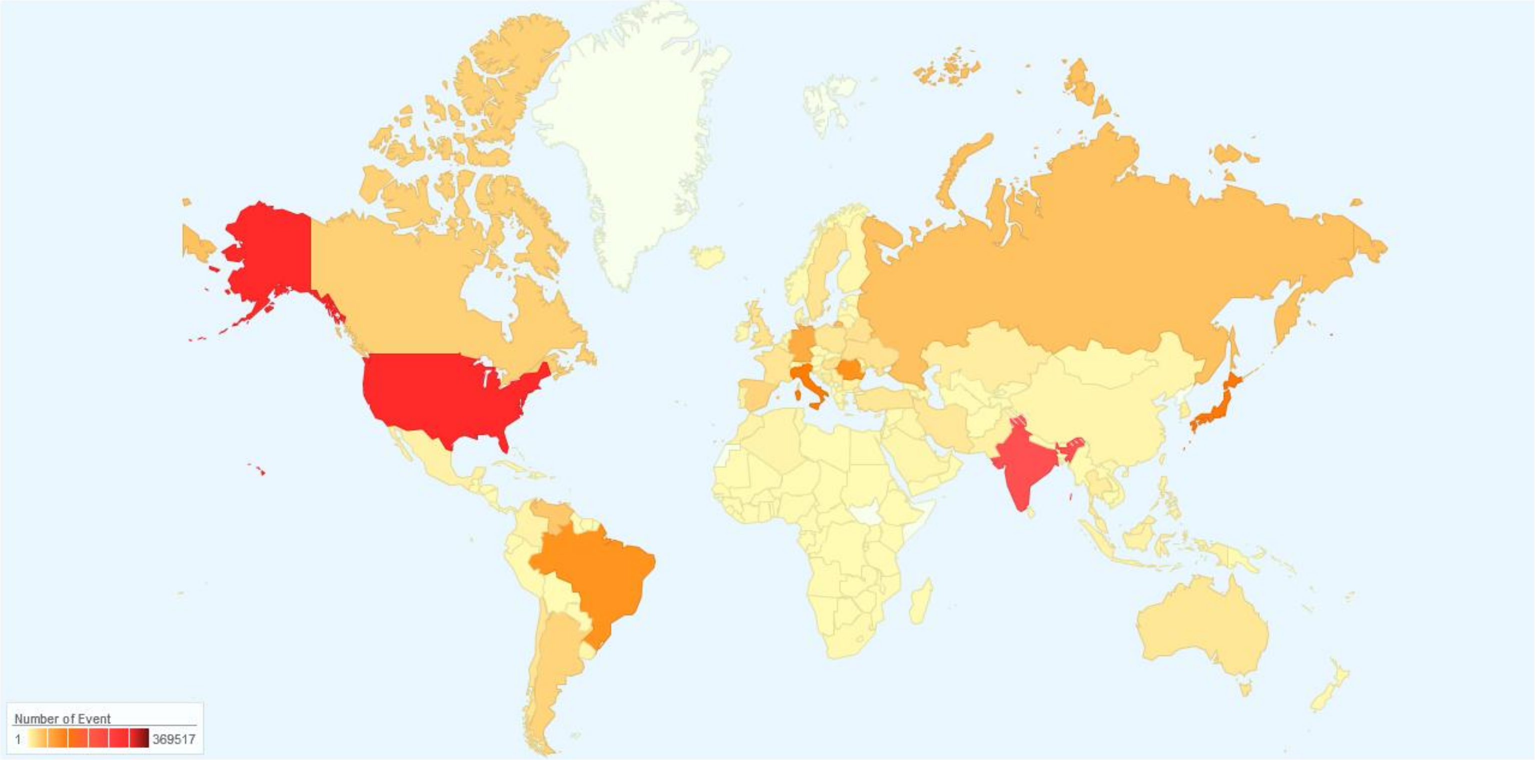
- Find a ZeroAccess-infected PC, and Observe its Behavior.


【Client】
【Herder】
3. Request for One-click Fraud
7. Receive Reward from Advertiser
1. Collect ZeroAccess
ZeroAccess
Web Crawler
4. Send a Command to Access and to Click One-click Site
Dynamic Analysis System
2. Put ZeroAccess into the Dynamic Analysis System
One-click Site
6. Access One-click Site, and Click Advertisement
5. P2P Access by Using Unique UDP Protocol (Response) ⇒ TCP Access
Infected PC
Infected PC
Infected PC
5'. P2P Access by Using Unique UDP Protocol (No Response) ⇒ Terminated
Communication Observed by PRACTICE
Communication Cited from Other Sources

Case 1. ZeroAccess

ZeroAccess Detected by PRACTICE System

- A Large Number of ZeroAccess-infected PCs are Detected by PRACTICE System.



Top10 detected countries

Country	US	IN	JP	RO	IT	TW	BR	DE	RU	CA
Number of Unique IP addresses	190,490	125,870	84,051	64,867	63,526	57,676	50,860	40,066	35,442	25,989

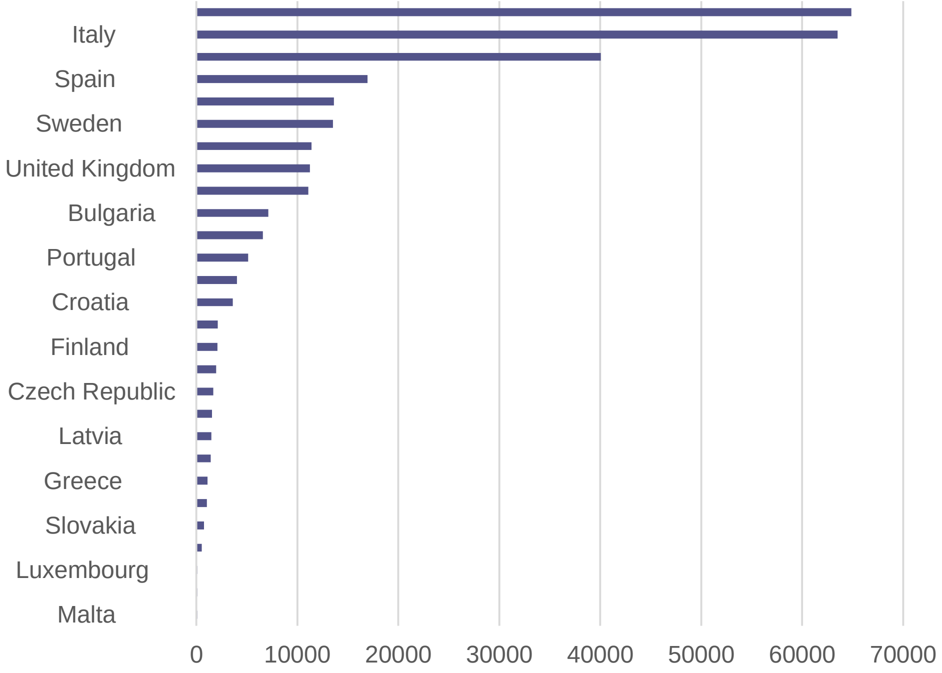
Case 1. ZeroAccess

ZeroAccess in EU Detected by PRACTICE System

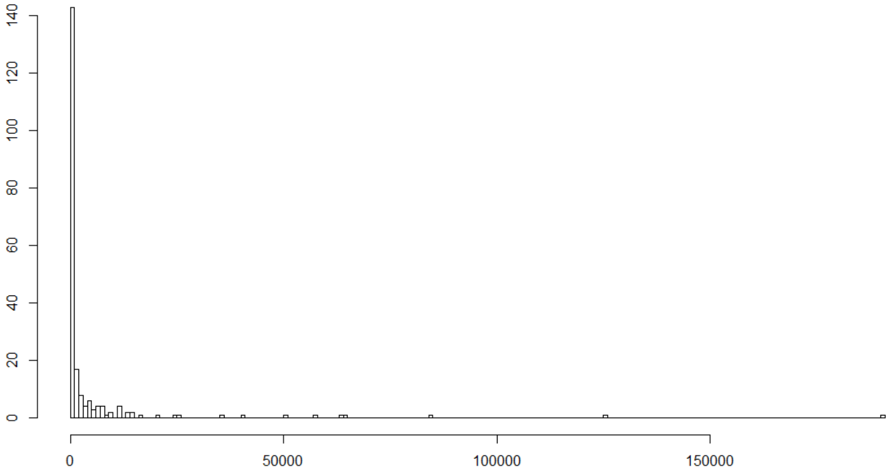
- PRACTICE system detected ZeroAccess communication from EU countries.
- Most countries in world, detected IP address are less than 1000.

Number of ZeroAccess infected IP addresses in EU

2013-01-01 ~ 2013-08-31



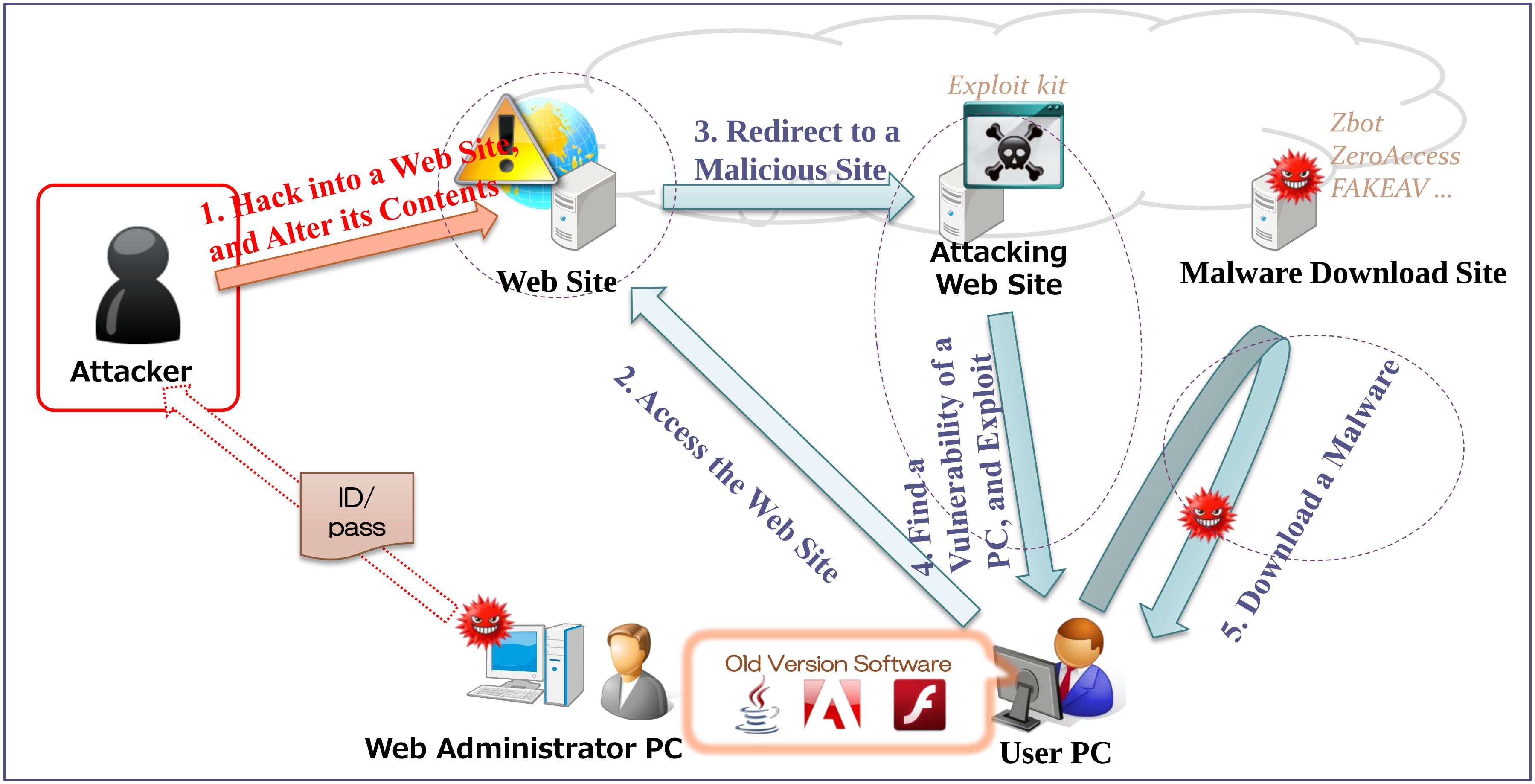
Histogram of number of ZeroAccess infected IP addresses in world



Case 2. Web Defacement

Web defacements are spreading

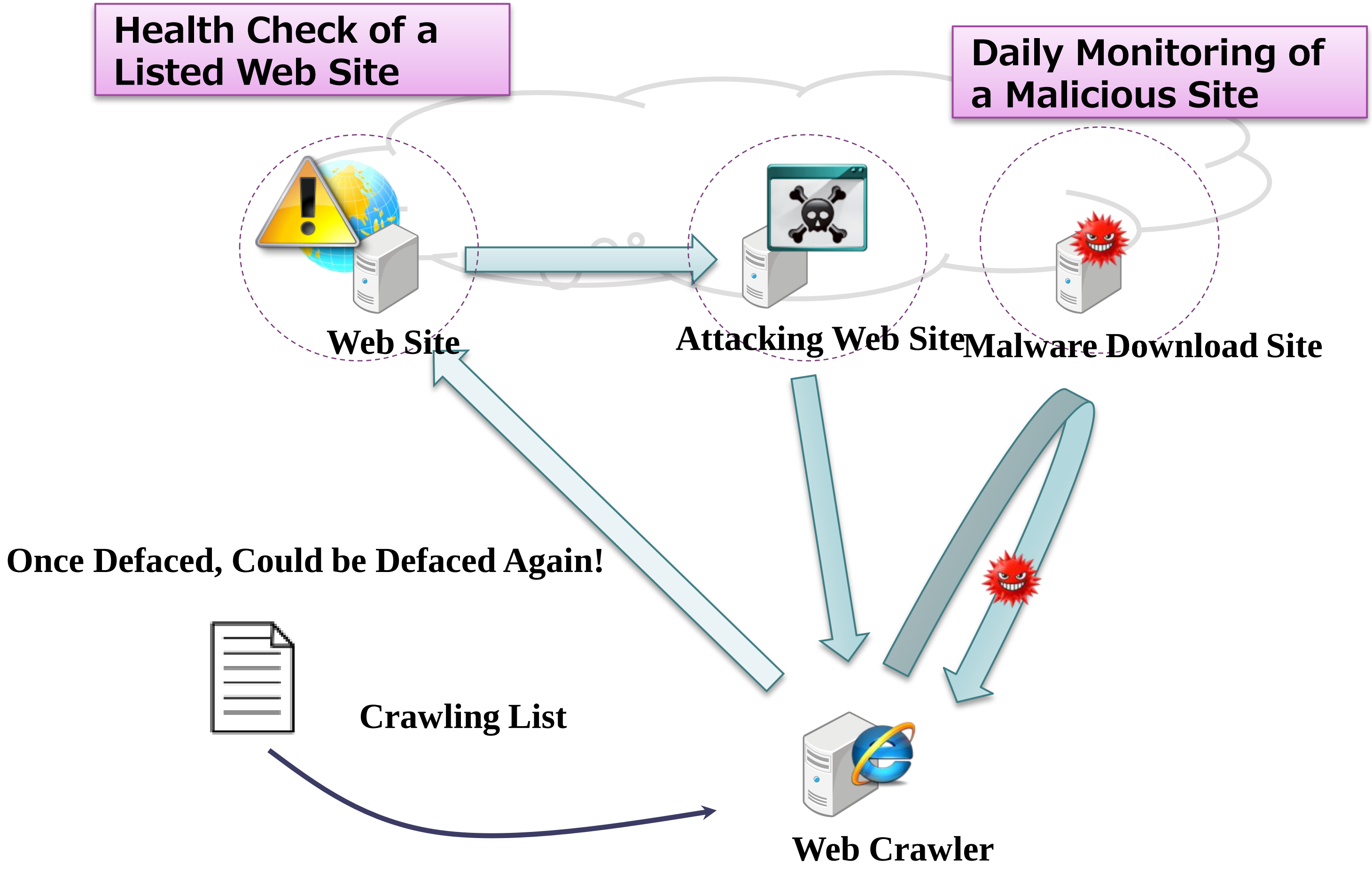
- Web Defacement is one of our concerns at this time.
- Many Web sites are defaced in Japan.
- A Parson accessing the defaced site gets infected with Zbot.



Case 2. Web Defacement

Our Trial to Find a Defaced Web Site

- Web Crawler checks Listed Web sites and finds Malicious sites.


Health Check of a Listed Web Site
Daily Monitoring of a Malicious Site
Web Site
Attacking Web Site
Malware Download Site
Once Defaced, Could be Defaced Again!
Crawling List
Web Crawler

Conclusions

Conclusions

- PRACTICE is focusing on Predict(Finding a Symptom of Cyber-attack) and Quick Response
- PRACTICE-FT is working on Establishing Quick Response Scheme
- In order to Establish Quick Response Scheme, PRACTICE-FT is trying to find a Symptom of Cyber-attack with R&D Team
  We recognize three levels in accordance with the cyber-attack
- International Collaboration is Important to Find a Symptom and Establish Quick Response Scheme

Thank you for your time and consideration.

We are looking forward to collaborating with you!

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

- *Telecom-ISAC Japan*

  https://www.telecom-isac.jp/english/index.html

PRACTICE