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 about using the Internet?

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

No Problem?
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

<table>
<thead>
<tr>
<th>Rank</th>
<th>Country</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Japan</td>
<td>9.01%</td>
</tr>
<tr>
<td>2</td>
<td>Denmark</td>
<td>9.72%</td>
</tr>
<tr>
<td>3</td>
<td>Finland</td>
<td>11.83%</td>
</tr>
<tr>
<td>4</td>
<td>Sweden</td>
<td>12.10%</td>
</tr>
<tr>
<td>5</td>
<td>Czech Republic</td>
<td>12.78%</td>
</tr>
<tr>
<td>6</td>
<td>Martinique</td>
<td>13.94%</td>
</tr>
<tr>
<td>7</td>
<td>Norway</td>
<td>14.22%</td>
</tr>
<tr>
<td>8</td>
<td>Ireland</td>
<td>14.47%</td>
</tr>
<tr>
<td>9</td>
<td>The Netherlands</td>
<td>14.55%</td>
</tr>
<tr>
<td>10</td>
<td>Slovenia</td>
<td>14.70%</td>
</tr>
</tbody>
</table>

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

IT Threat Evolution: Q2 2013

<table>
<thead>
<tr>
<th>Rank</th>
<th>Country</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Japan</td>
<td>9.01%</td>
</tr>
<tr>
<td>2</td>
<td>Denmark</td>
<td>9.72%</td>
</tr>
<tr>
<td>3</td>
<td>Finland</td>
<td>11.83%</td>
</tr>
<tr>
<td>4</td>
<td>Sweden</td>
<td>12.10%</td>
</tr>
<tr>
<td>5</td>
<td>Czech Republic</td>
<td>12.78%</td>
</tr>
<tr>
<td>6</td>
<td>Martinique</td>
<td>13.94%</td>
</tr>
<tr>
<td>7</td>
<td>Norway</td>
<td>14.22%</td>
</tr>
<tr>
<td>8</td>
<td>Ireland</td>
<td>14.47%</td>
</tr>
<tr>
<td>9</td>
<td>The Netherlands</td>
<td>14.55%</td>
</tr>
<tr>
<td>10</td>
<td>Slovenia</td>
<td>14.70%</td>
</tr>
</tbody>
</table>
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.

Worldwide average CCM: 6.0

- Japan CCM: 0.7
- Korea CCM: 93.0
- Germany CCM: 2.1
- Thailand CCM: 21.0
- US CCM: 3.0

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

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

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…

Outside Japan 97%
Japan 3%

Honeypot can detect...
Network Infection Malware (Worm)
Hard to detect...
Web Infection Malware (Drive-by-Download)
Mail Infection Malware (Attached file)
Cyber-attack techniques are shifting
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
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

Reputation database system

Route monitoring system

Proactive Response Against Cyber-attacks Through International Collaborative Exchange

Cyber attack defense exercise

Wide area monitoring

Anti-bot countermeasures project

Information sharing

Incident handling

19 member companies

Telecom-ISAC Japan
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)

ISP Collaboration
- Research
- Prediction (Early Detection of Cyber-attacks)
- Warning

PRACTICE R&D
- Etc.

Supported by NICT

International Collaboration
- Foreign organizations (Government, ISP...)
- Data Sharing
- Discussion
- Countermeasures

Sponsored by MIC
Ministry of Internal Affairs and Communications
**Ref) Collaboration with PRACTICE R&D Team**

**Scope of field trial and R&D**

---

**Past**

- Honeypot/WebCrawler (SPAM/SNS/BBS)
- Statistical Investigation by Collecting and Analyzing Malwares

**Now**

- 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
- Classification of Malware
- Active C&C List
- Information of Analysis and Measures
- Alert

**Future**

- R&D
- Understand the actual situation of the cyber-attack situation
- Predict the cyber-attack
- Share the Malware to be analyzed
- Share the BL/Tracking data
- Analysis, Knowledge from R&D
- Prediction Information
- Darknet Analysis
- Large-scale behavior Analysis R&D
- Find Symptom
- Feedback R&D knowledge

---

**Quick Response against Cyber-attacks (International Collaboration)**

---

**Statist**

**Cyber Attack Trend Analysis**

---

**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

Quick Response Scheme

Corroborative Research
Etc.

Fundamental Research

R&D Institutes

Proactive Response Against Cyber-attacks Through International Collaborative Exchange

Malware
Spam Mail
Malware, URL Link
Web Access
Web Blog SNS

Honeypot
Spam Trap
Web Crawler
SNS Honeypot
Backscatter monitor ...

Dynamic Analysis
Static Analysis

ISP
Government
Security Vendors
R&D Institutes

ISPs

Organization
Individual Users

Foreign Organization
ISP
Government
Security Vendors
R&D Institutes

ISPs

Collaboration

Field Trial

Telecom ISAC Japan

Telecom Information Sharing and Analysis Center Japan

ISP
Government
Security Vendors
R&D Institutes

Collaboration

Corroborative Research Etc.

R&D Institutes

PREDICT

Fundamental Research

DDoS

DETECT & ANALYZE

ISPs

Collaboration

Year 2011 - 2016

Quick Response Scheme

Corroborative Research
Etc.

Fundamental Research

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**

1. Vulnerability attack
2. Download

Malware Infected PC → Honeypot

**Web Infection Detecting System**

1. Crawl web in reference to black list
2. Vulnerability Attack
3. Download

Landing Website → Attacking Website → Malware Hosting Web site → Web Crawler

Crawl web in reference to black list → Vulnerability Attack → Download
Data Sharing with ISPs

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

Information Sharing System

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

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

**LEVEL 1.**
Formation of Cyber-attack Infrastructure

**LEVEL 2.**
Change of the Cyber-attack Infrastructure

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

**Cyber Attacks**
- C&C Server
- Malware Distribution Site
- Malware Infected PC
- Change of Botnet (Scale, Function, Objective)
- DDoS
- Spam
- Information Leakage

**Our Focus**
Cyber Attacks
- Issue the Alert based on the symptom of Emerging Cyber-attack
- Raise the Level of Monitoring
- Change of Botnet (Scale, Function, Objective)

**<Observed Event>**

**<Stages of Cyber Attack>**

**<Measures>**
- Taking over to the Existing Measures (DDoS, Spam, Information Leakage Measures)
- Blocking of Communications
- DNS Sinkhole
- Issue the Alert based on the symptom of Emerging Cyber-attack
- Raise the Level of Monitoring
- 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.

LEVEL 1.
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?

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.

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

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

Quick Response!
We prevented the damage.

We need to prepare before the damage is caused.

Found a symptom of cyber-attack

Field Trial R&D

Malware infected PC owner

The damage was prevented

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

- 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 (Malware, 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)
① Find a change of the number of Cyber-attacks
② Estimate 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

① Find a change of the number of Cyber-attacks

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

![Graph showing changes in Cyber-attacks](image)

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.
① Find a change of the number of Cyber-attacks

- Issue the alert by analyzing the malware trend.
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.

Statistics

Quick Response (Countermeasures)

Information Sharing System

Field Trial System

Validation of Cyber-attack

• 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.

**◆ Network Infection Malware Top5**

[TrendMicro]

No.1 WORM_DOWNAD.AD
No.2 WORM_ALLAPPLE.IK
No.3 Mal_DownAd-2
No.4 PE_VIRUT.AV
No.5 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.

<table>
<thead>
<tr>
<th>Country</th>
<th>Malware Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Romania</td>
<td>12,345</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>10,234</td>
</tr>
<tr>
<td>Hungary</td>
<td>8,976</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>7,654</td>
</tr>
<tr>
<td>Italy</td>
<td>6,432</td>
</tr>
<tr>
<td>Poland</td>
<td>5,321</td>
</tr>
<tr>
<td>Germany</td>
<td>4,210</td>
</tr>
<tr>
<td>Netherlands</td>
<td>3,198</td>
</tr>
<tr>
<td>France</td>
<td>2,345</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>1,234</td>
</tr>
<tr>
<td>Latvia</td>
<td>1,023</td>
</tr>
<tr>
<td>Spain</td>
<td>897</td>
</tr>
<tr>
<td>Lithuania</td>
<td>765</td>
</tr>
<tr>
<td>Sweden</td>
<td>654</td>
</tr>
<tr>
<td>Portugal</td>
<td>532</td>
</tr>
<tr>
<td>Croatia</td>
<td>421</td>
</tr>
<tr>
<td>Denmark</td>
<td>319</td>
</tr>
<tr>
<td>Belgium</td>
<td>234</td>
</tr>
<tr>
<td>Austria</td>
<td>123</td>
</tr>
<tr>
<td>Slovakia</td>
<td>102</td>
</tr>
<tr>
<td>Greece</td>
<td>89</td>
</tr>
<tr>
<td>Ireland</td>
<td>76</td>
</tr>
<tr>
<td>Estonia</td>
<td>65</td>
</tr>
<tr>
<td>Slovenia</td>
<td>54</td>
</tr>
<tr>
<td>Finland</td>
<td>43</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>34</td>
</tr>
<tr>
<td>Cyprus</td>
<td>23</td>
</tr>
<tr>
<td>Malta</td>
<td>12</td>
</tr>
</tbody>
</table>

2013-01-01 ~ 2013-08-31
**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

![Bar chart showing malicious URLs in EU countries from 2013-01-01 to 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)

- 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.

1. Collect ZeroAccess
2. Put ZeroAccess into the Dynamic Analysis System
3. Request for One-click Fraud
4. Send a Command to Access and to Click One-click Site
5. P2P Access by Using Unique UDP Protocol (Response) ⇒ TCP Access
5’. P2P Access by Using Unique UDP Protocol (No Response) ⇒ Terminated

- One-click Site
- Infected PC
- Dynamic Analysis System
- Web Crawler
- ZeroAccess

7. Receive Reward from Advertiser
Case 1. ZeroAccess
ZeroAccess Detected by PRACTICE System

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

Top 10 detected countries

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

<table>
<thead>
<tr>
<th>Country</th>
<th>Number of IP addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Italy</td>
<td>60,000</td>
</tr>
<tr>
<td>Spain</td>
<td>40,000</td>
</tr>
<tr>
<td>Sweden</td>
<td>30,000</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>20,000</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>15,000</td>
</tr>
<tr>
<td>Portugal</td>
<td>10,000</td>
</tr>
<tr>
<td>Croatia</td>
<td>5,000</td>
</tr>
<tr>
<td>Finland</td>
<td>3,000</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>2,000</td>
</tr>
<tr>
<td>Latvia</td>
<td>1,000</td>
</tr>
<tr>
<td>Greece</td>
<td>500</td>
</tr>
<tr>
<td>Slovakia</td>
<td>500</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>500</td>
</tr>
<tr>
<td>Malta</td>
<td>500</td>
</tr>
</tbody>
</table>

Histogram of number of ZeroAccess infected IP addresses in world

0  20  40  60  80  100  120  140

0  50000  100000  150000
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.

1. Hack into a Web Site and Alter its Contents
2. Access the Web Site
3. Redirect to a Malicious Site
4. Find a Vulnerability of a PC, and Exploit
5. Download a Malware

Attacker
Web Administrator PC
User PC
Exploit kit
Malware Download Site
Web Site
Attacking Web Site
Zbot
ZeroAccess
FAKEAV...
Old Version Software
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**
  