

Information Security Threats Landscape

*2ND APEC SEMINAR ON PROTECTION OF CYBERSPACE FROM
TERRORIST USE AND ATTACKS
NOVEMBER 18-19, 2008, SEOUL, KOREA*

Koichiro Komiyama, CISSP
JPCERT Coordination Center

About JPCERT/CC

<https://www.jpcert.or.jp/>

- JPCERT/CC stands for ...
 - Japan Computer Emergency Response Team Coordination Center
- Officially established in 1996
- Independent, non-profit organization sponsored by METI (Ministry of Economy, Trade and Industry)
- Coordination and collaboration on Computer Security Incidents with domestic/international organizations
- Issue security bulletins and advisories for Japanese IT professional

- JPCERT/CC, Who we are.
- Threats
 - DoS
 - Bot/Botnet
 - Targeted Attacks
 - Vulnerable Control System
 - New Technology Penetration
 - Twitter
 - BlackBerry
 - Blog
 - Cloud Computing
- Measures
 - Tsubame (Network Visualizing)
 - IT Security Inoculation (User Education)

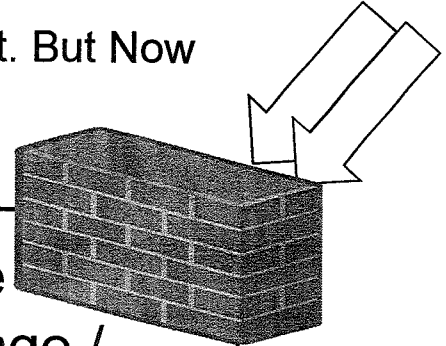
We have fought against threats like ...

- Virus/Worm
- DDoS
- Cyber Terrorism
- Web Site Defacement



**Government/
Enterprise**

We are protected against external threat. But Now the threats are within us too...



Government/Enterprise

1. Malicious Insiders(IT Sabotage / Theft of Information)
2. Change of Media Technology (e.g. Twitter)
3. Beginners, Less-Educated

Threat 1:

MALICIOUS INSIDERS

■ What is Meant by "Insider Threat?"

A current or former employee, contractor, or business partner who

- has or had authorized access to an organization's network, system, or data and
- intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems

CERT/CC's definition



■ Is it Really a Threat?

- 31% of E-crimes were committed by insiders (source: 2007 E-Crime Watch Survey)

■ Category

— IT Sabotage

- Shinsei Bank (2008): ex-contract employee sneak in corporate network with his credential. Delete more than 2600 files, sneak a peek boss's emails.

— Information Theft

- Japan Ground Self-Defense Force (2009/9): An officer of JSDF has admitted leaking personal data on 140,000 members, , nearly the entire force, in exchange for 1 million yen(\$100) in cash.

— Misc (Fraud, System misuse)

■ Measures

- Need to have strict background checks
- Consistently Enforce Policies and Controls
- Deactivate User Account soon after the termination

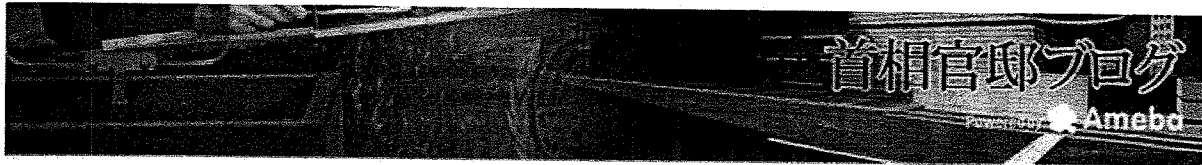
Threat 2:

CHANGE OF MEDIA TECHNOLOGY

New Technologies Coming in: Twitter

The image shows a screenshot of a Twitter profile for Barack Obama. The profile header includes the name "BarackObama" and a "Following" button. A tweet from the account "whitehouse" is visible, containing the text: "RT @FDA_Drug_Info Q&A · Care Providers: Renal Dos". The tweet is timestamped "at 3:15 via strator Mills on credit". The tweet content is partially obscured by a black redaction box. To the right of the tweet, a sidebar shows profile information for "whitehouse", including a verified status, name, location (Washington), and a bio. Below the tweet, the text "In Singapore, continuing the visit to Asia Watch trip updates by staff on the" is visible.

PM starts blogging!



プロフィール



[ルームを見る]

ニックネーム:首相官邸ブログ

[記事作成・編集]

このブログの読者になる(チェック)

1 | 2 | 3 | 4 | 5 [最初 次ページ]

2009-11-12

メコン地域諸国との信頼と絆

テーマ:鳩山内閣総理大臣

天皇陛下御在位20年を、国民のみならずとも、心よりお慶び申し上げます。

いつもかなるときも、国民と共に歩み、心をお寄せになられておられる天皇陛下、皇后陛下のご健康と皇室のご繁栄を心からお祈り申し上げます。

最近の記事一覧

メコン地域諸国との信頼と絆
中小企業金融円滑化法案について
天皇・皇后両陛下からいただいた
励まし
経産部から
強固な日米関係をめざして
行政の大掃除で、コンクリートから
人へ
触れ合い、懸念、励まし…… 全
力で取り組まれた20年
経産部から
新しい国づくり
新型インフルエンザ対策について
[一覧を見る]

- MoFA minister's press briefings are uploaded on Youtube immediately after.
- Ministry of Health, Labour and Welfare , Ministry of Defense , Ministry of Justice , Ministry of Foreign Affairs



- I have my own server on Amazon EC2!
- Though I don't know where my confidential information is ...

The screenshot shows the AWS Management Console interface. At the top, there's a 'My Instances' section with a table listing instances. One instance, 'i-d17070b8', is selected. Below the table, a modal window titled 'Loading, please wait...' is open, displaying the details for the selected EC2 instance.

Instance	AMI ID	Security Groups	Type	Status	Public DNS	Key Pair Name	Mo
<input checked="" type="checkbox"/> i-d17070b8	ami-4b10f122	default, snortmonit	m1.small	running	ec2-174-129-9-55.compute-1	forTimor	dis

1 EC2 Instance selected

EC2 Instance: i-d17070b8

Loading, please wait...
[esc] to cancel

Description	Monitoring
AMI ID:	ami-4b10f122
Security Groups:	default, snortmonitoring
Status:	running
Reservation:	r-ef603786
Platform:	-
Kernel ID:	aki-a71cf9ce
AMI Launch Index:	-
Public DNS:	ec2-174-129-9-55.compute-1.amazonaws.com

Zone:	us-east-1b
Type:	m1.small
Owner:	221413895703
Ramdisk ID:	ari-a51cf9cc
Key Pair Name:	forTimor
Monitoring:	disabled
Elastic IP:	-

- First government web service which powered by Salesforce.com was launched (2009/7)
- Ask users to input+

- Name
- Address
- Phone number

The screenshot shows a web browser displaying the 'Eco-Points' application. The URL is 'https://eco-points.secure.force.com/WebFormInput2'. The page has a header with the title 'エコポイント' and navigation links like 'ホーム', 'エコポイント制度とは', '対象商品', and '交換商品'. Below the header, there's a section titled 'インターネット申請フォーム' with a sub-link 'ホーム > インターネット申請'. At the bottom, there's a form titled '申請者情報欄' with a date field set to '平成 21 年 11 月 17 日' and a text input field for '氏名(全角カナ)' with a note '(例)カンキョウ ※全角で入力してください'.

- Government/CIP need services like twitter, blogs and Cloud Computing Service
 - relatively low in price
 - Better performance, functions, usability
- We should consider about risks arise with them.
 - Those services are not under our control
 - Where those server are located? (Does Japanese Law have any effect there?)

- Measures
 - Keep up to new technologies/services
 - Update policies

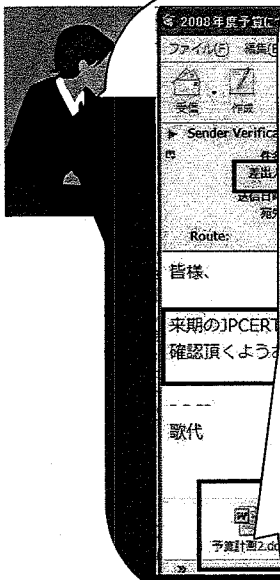
Threat 3:

BEGINNERS, LESS-EDUCATED

- Target Trojan Attacks are steadily increasing
 - customized message for few recipients
- How to prevent employee opening those malicious attachment?
- Inoculation!
 - What is Inoculation?
 - An exercise to raise awareness toward mail attacks such as targeted attacks/phishing. Users receive fake targeted attack mails with attachment which does not harm their computer.



Inoculation How it works.



本件に関するお問い合わせ先: ●●部●●、●●部●●

ご注意! このような怪しいメールの添付ファイルを不用意に開封すると

あなたを狙うウイルス等に感染する恐れがあります。

(このメールは統計調査のためのものです)

本添付ファイルを添付したメールは、調査のために不審メールを模したもので、本文・件名に記載された内容は架空のものです。

調査結果は有限責任中間法人による脅威への予防策が公表されることは一切ありません。

調査精度を上げるため、実施にご協力をいただけます。

本添付ファイルに危険性の添付ファイルを開いた際、添付ファイルの

○不要なメールと添付ファイル

近年、特定の組織・職員を標的型攻撃の偽メールはメールボックスまで直接届かしてしまうと、ウイルス等への被害を避けるためには、

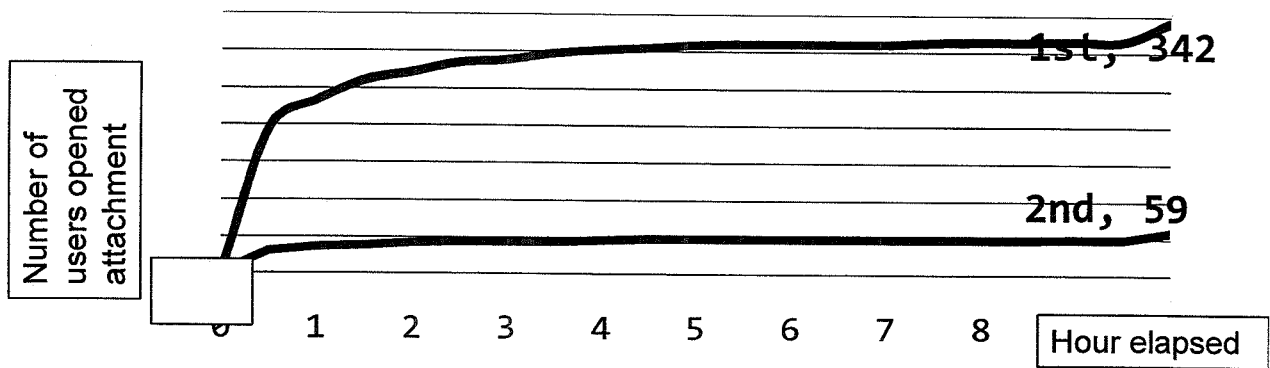
- Contact Information
-Instruction

-Characteristics of attack mails

-How you should react

-- Invisible BMP image on a web server. "Beacon"

- 14 Companies from 8 industries, 2600 recipients
- 44.0% of users opened suspicious attachments the 1st time. The rate went down to 13.0% in the 2nd time.
- More than 50% of users who opened the attachment responded within 30 minutes of the beginning.



Copyright© 2009 JPCERT/CC All rights reserved.

1. Threats exist inside our organization as well.
2. Economic crisis accelerated government/CIP using twitter, Youtube, cloud computing.
 - Used to be conservative to adopt new tech.
3. User education is key to build secure organization. The inoculation raised user awareness against targeted attack/phishing. IT reduced rate of suspicious mails being opened.

- Email : office@jpcert.or.jp
- Tel: +81-3-3518-4600
- Fax: +81-3-3518-4602
- <https://www.jpcert.or.jp>

■ Incident Report

- Incident Reporting Form
<https://www.jpcert.or.jp/english/ir/form.html>
- Email : info@jpcert.or.jp
PGP Fingerprint : FC89 53BB DC65 BD97 4BDA D1BD 317D 97A4
69EC E048