Situation in Japan

Yurie Ito
JPCERT/CC

Number of the IR reports coming in 2004'

- Totally 5,217 Incident Reports
  - (2004 01-12)

Break down;

- Probe and Scan : 4974
- Intrusion : 19
- email ID theft : 30
- DoS : 2
- ID Theft (Phishing) : 30
- Others : 165

6 months ago --

- Phishing Incident reports are coming Mostly from overseas (Australia, US, UK – etc…) requesting JPCERT/CC to coordinate to take the phishing site down.
  - Most of the cases site owners are not even aware of the phishing site. i.e. server is compromised and unintended phishing site is up.

- Mainly English language financial entities are targeted – JPCERT/CC involved only because the phishing sites are hosted in Japan.
- Few Phishing sites, but "Not sophisticated" i.e. "clearly non-native" Japanese language, of Japanese financial entities that time.

-- JPCERT/CC action

- Raise awareness of the site owners --
- Released tips to advice site owners and server administrators;
  - Only provide the access to the ports on which you provide the services
  - Block access to any other ports using firewall and monitor your service for unusual traffic
  - Run services with minimum privilege as necessary
    - If the program does not run by administrator privilege, don't run with that
  - Update your software to the latest version, apply patch to avoid using vulnerable software.
  - Do user account management, such as not using easy-to-guess password, eliminate the nonessential account.

The latest situation

- Very sophisticated Japanese language phishing sites targeting Japanese financial entities are up.
  - “They” have broken the language barrier already!!!
- (from the public news sources)
  - A Japanese credit card company announced that September to October of 2004, 8 customers were identified as victims, totaling 1.5M Yen cash withdrawn from a bank using data from phishing site.
  - The phishing site was hosted in the eastern part of Europe – generally speaking it takes a long time for financial entities to take the site down especially if the site is hosted at the areas where hard to reach.

-- JPCERT/CC action

- Meeting with financial entities, raise awareness of the current situation, notify them JPCERT/CC coordinates Phishing incidents.
- Strengthen the incident response capability between CSIRT framework such as APCERT.
- Counsel of anti-Phishing
  - Japanese government created the Counsel of anti-Phishing
  - stakeholders such as financial entities, security experts, JPCERT, vendors, law enforcement, and most importantly ISPs.
  - To create the strategy, procedures, specially with the ISPs.
- Share information among CERTs

Phishing Coordination

- Procedure of coordination
  - Contact to site owner, then ISP if no response
- Difficulty to handle this issue;
  - Request comes sometimes from financial entity itself directly, sometimes from CSIRTs, sometime security service provider, the third party, sometimes multiple sources.
  - When to involve law enforcement: who reports to which law enforcement in which timing?
  - Sometimes no reply from site owner – who would take the site down with what type of authority.
  - what to do with the data at the phishing site
- Active discussion to addressing these coordination matters at APCERT.

Collaboration!!!!!

- Collaborative and cooperative approaches to the multiple disciplines is critical!!!!!!!

Thank you.

Yurie Ito (office@jpcert.or.jp)
Manager, Information Coordination Group,
JPCERT/CC
Tel: 81-3-3518-4600