Interview with JPCERT/CC

Taiji Kimura, Izumi Okutani
JPNIC

Introduction

- We would like to share how WHOIS service is used for abuse handling by a CSIRT in Japan.

- We visited JPCERT/CC office and had an interview with their incident response group.

About JPNIC WHOIS

- Database and query service for all information related to number resources managed by JPNIC,in both English and Japanese
- Mirror information with APNIC WHOIS once a day (English part, and without POCs)
- We share some POC objects with JPRS, the ccTLD registry for .JP

About JPCERT/CC

- Its role in Japan:
  - JPCERT/CC is the first CSIRT (Computer Security Incident Response Team) established in Japan.
  - JPCERT/CC, as a national CSIRT, handles computer security incidents at a national level
  - Coordinates with various players in the industry;
    - “network service providers”, “security vendors”, “government agencies”, “the industry associations”.

- In AP region and Globally:
  - In the Asia Pacific region, JPCERT/CC helped form APCERT (Asia Pacific Computer Emergency Response Team) and provides a secretariat function for APCERT. JPCERT/CC is the current Chair team of APCERT.
  - Globally, as a member of the Forum of Incident Response and Security Teams (FIRST), JPCERT/CC cooperates with the trusted CSIRTs worldwide

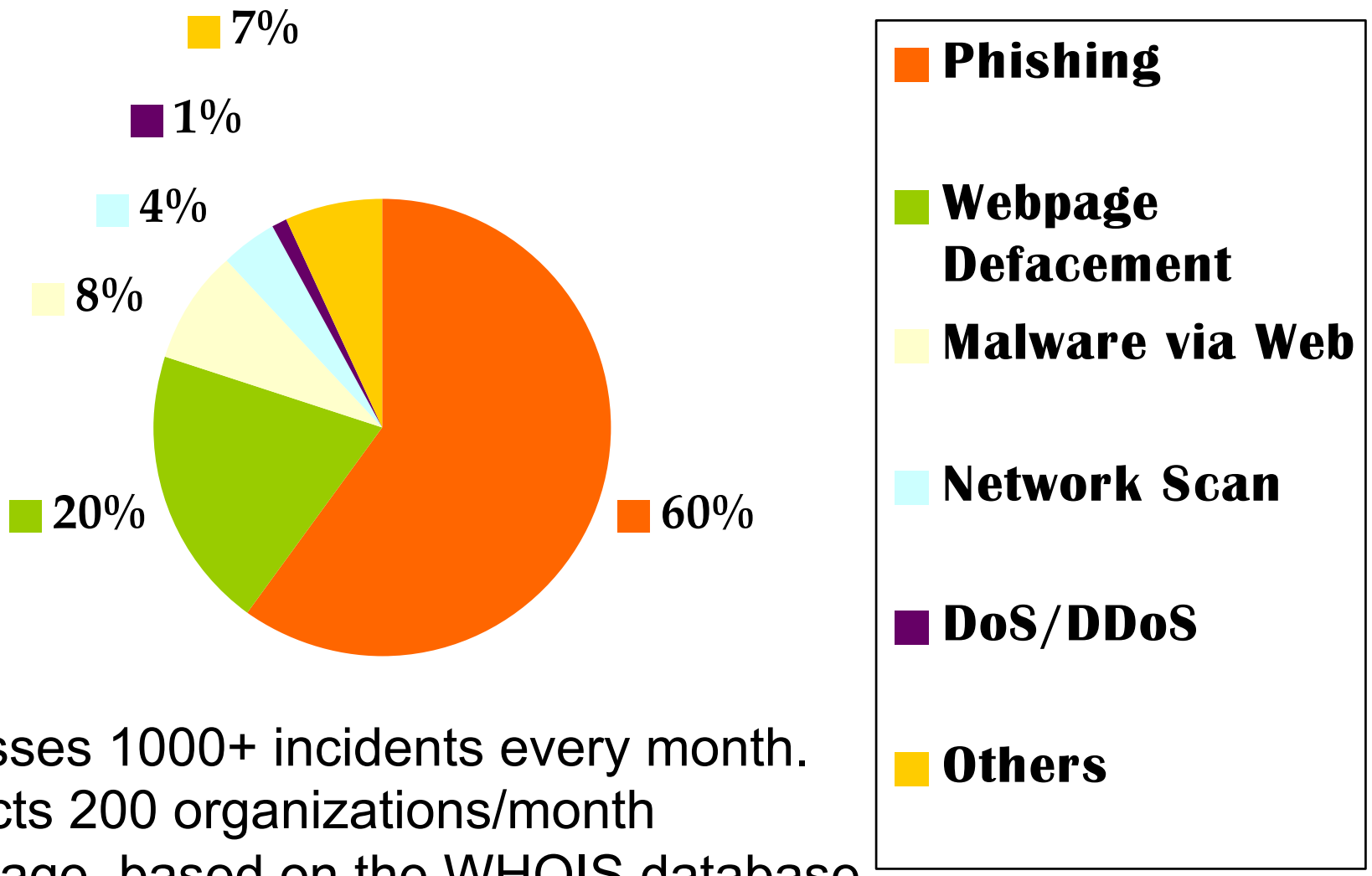
Major Activities of JPCERT/CC

- Incident Response and Analysis
  - Provides technical support for those who report security problems.
  - Incidents can be reported to JPCERT/CC by e-mail
- Security Alert
  - Gathers computer security related information and provides a security alert and advisory message
  - A weekly report which contains potential threats and advisory message, is sent to the constituencies via email.
- Coordination with other CSIRTs
  - Has established close relations with many CSIRTs in the Asia and Pacific region as well as in other regions.
- Vendor Coordination, Education & Training, Research & Analysis

How JPCERT/CC supports reported security problems

- Based on information provided from the reporters, JPCERT/CC assesses the damage;
- Identifies the threats and/or vulnerabilities; and
- Provides technical support through coordination with other local and overseas CSIRTs and ISPs

Trends in Handling Incidents by JPCERT/CC



- Processes 1000+ incidents every month.
- Contacts 200 organizations/month in average, based on the WHOIS database.

Steps taken by JPCERT/CC in Handling Incidents

1. Analyze the type of incident reported
2. Identify IP address involved in the incident
3. Contact tech-c in the inet-num (assignment)
4. If POC of inet-num of the assignment is not reachable, contact the upstream ISP

Also collaborates with National CSIRT in abuse handling

Use of WHOIS in Handling Incidents

- WHOIS is used for all handling of incidents by JPCERT/CC
- The first preference is to contact the organization directly involved rather than its upstream ISP
- Information used in abuse handling
  - Technical POCs (tech-c, abuse)
  - IP address range
  - Country
  - Abuse related information in remarks section

What We Found out (1)

- JPCERT/CC have different needs for WHOIS service from ISPs
  - WHOIS is very actively used
    - They use WHOIS almost 100% for abuse handling
    - We have heard ISPs in JP tend to use information other than WHOIS
  - “Inet-num” objects for “assignments” are the primary contact in handling of incidents by JPCERT/CC
    - Important to reach the organization directly
    - JPNIC tends to receive requests from ISPs not to disclose POCs of their customers
    - We assumed contacting end sites is not high priority if upstream ISPs are reachable

What We Found out (2)

- Regular, standardized format is necessary to enable machine search
  - It is currently not possible because of various WHOIS data formats across registries
  - Having abuse contacts in “remarks” section of “inet-num” does not allow automation

- WHOWAS could be useful for abuse handling
  - Some incidents last over a long period of time and helps track back the address holder in the past

Request from JPCERT about WHOIS service

- Helps to develop machine query system if:
  - Abuse related information is in standard fields (not in remarks)
  - Standardized the data in WHOIS across Internet Registries

- Helps if high rate queries to WHOIS are allowed for JPCERT/CC
  - Currently, JPNIC does not make special case for JPCERT/CC in WHOIS limits to high rate queries
  - How do other Internet Registries handle it?

Room for considerations

- Would better collaborations between Internet Registries and Regional/National CSIRTs may make us both happy?
- Is there anything we can do about various WHOIS formats to help in machine search?
  - Discussions related to WIERDS?
- Should APNIC/NIRs help in more outreach on abuse related issues in APNIC region?
  - Currently, less focus compared to routing related topics

Thanks to

- JPCERT staff who have given us their time & inputs.

Special thanks to:

- ◆Yozo Toda
- ◆Keishi Kubo
- ◆Masayuki Nakatani
- ◆Hideaki Kobayashi

We would also love to hear about experiences of other Internet Registries about collaborations with Regional/ National CSIRTs