Network Monitoring & Web Portal Site Project in AP region

- Arnold Yoon, KrCERT/CC
  (snyoon@certcc.or.kr)
- Yurie Ito, JPCERT/CC
  (yito@jpcert.or.jp)

Agenda

- Security Incidents Trend
- Why Network Monitoring?
- Activities in Japan/Korea
- Data sharing (Using IODEF)
- WEB Portal Site & Early Warning System
- Conclusion
- Q&A

Security Incidents Trend

- Before 2001, most attacks were system based attacks. (Eg. Sadmind)
- These days, most attacks are targeted to network utilization. (Eg. MS Slammer, DDoS)
- Also, most attacks are generated from the thousands of end-users' system.
- Major concern is the **HARMNESS(or EFFECTS) ON THE NETWORK INFRASTRUCTURE.**
- Before major attacks we observe some **ABNORMAL SYMPTOMS ON THE NETWORK.** (Eg. Sasser Worm)

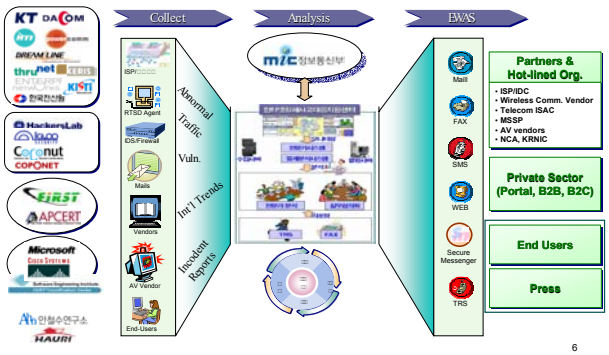
Why Network Monitoring?

- **To catch & predict the symptom** of major attacks in a step advance by monitoring the statistics of network traffic.
- By prediction, **provide the Early Warning Service.**
- By Early Warning Service, **Minimize the Damage.**

Activities in KOREA

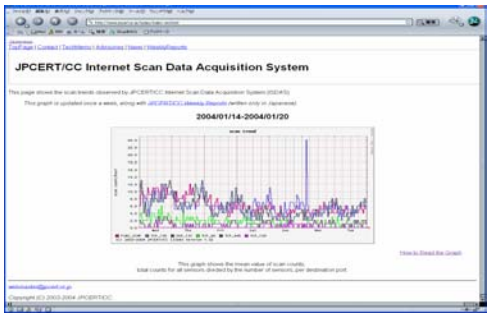
- Since Dec. 2003, KISC(Korea Information Security Center) has been activated.
- Monitors Network Traffic, Security Events and Trends from various sources

Activities in KOREA (Cont'd)

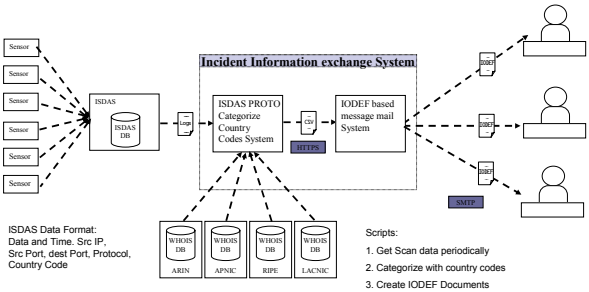


Activities in Japan

ISDAS (Internet Scan Data Acquisition System)



Outlook of System Architecture

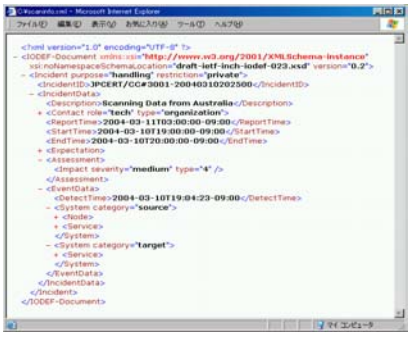


ISDAS Data Format:
Data and Time. Src IP,
Src Port, dest Port, Protocol,
Country Code

Scripts:

1. Get Scan data periodically
2. Categorize with country codes
3. Create IODEF Documents
4. Verify IODEF Documents
5. Send IODEF Document as e-mail periodically

IODEF Profile message transformed by Incident information exchange system

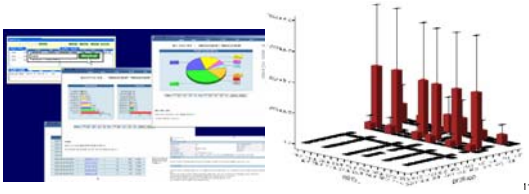


Data sharing (using IODEF)

- For a larger view of network traffic, data collector in various location is essential.
- Type of sensor does NOT have to be defined. Format of data exchanging MUST be defined.
- Japan and Korea is exchanging data based on IODEF & IODEF additional fields

WEB Portal Site & Early Warning System

- Based on exchanged data, the WEB portal site shows the graph of network traffics.
  (Eg. Top attack ports, Abnormal increase of traffic)



Conclusion

- To provide Early Warning Service & minimize the effect of major incidents, network monitoring and data sharing is the **major factor of PREDICTION, DETERMINATION & ANALYSIS.**
- As many volunteers for this project will improve the effectiveness and value of the WEB portal site data.
- WEB portal site could have the value which indicates the activity & trends in each region.

Q&A

- JPCERT/CC
  - http://www.jpcert.or.jp
- KrCERT/CC
  - http://www.krcert.or.kr
- Arnold Yoon
  - snyoon@certcc.or.kr
- Yurie Ito
  - yito@jpcert.or.jp