The Traffic Monitoring Portal Site

Jungu Kang

jgkang@certcc.or.kr

KrCERT/CC

KISA

Korea Information Security Agency

Contents

I. Methodology to predict incidents

II. Estimating the impact of the incidents

III. The traffic monitoring portal site

IV. Is the traffic data critical information ?

V. Conclusion

I. Methodology to predict incidents

❑ **HoneyPot**

- Hacking Tools and worm samples being spread in the net
- Analysis for the current attack

❑ **Monitoring activities in underground**

- Vulnerabilities being used in the recent attacks
- Attack Information (When and who will they attack?)

❑ **Traffic Monitoring**

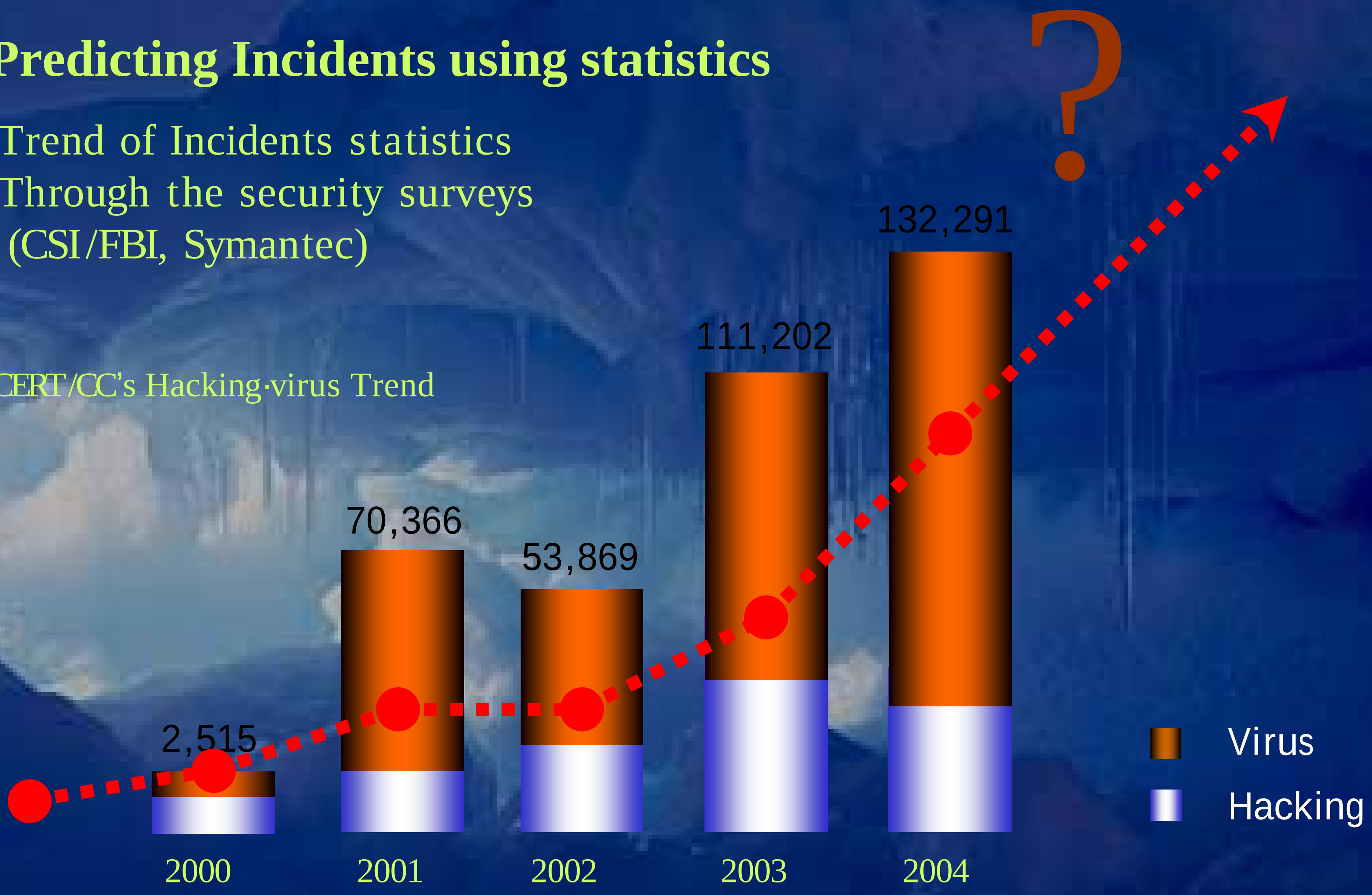
- Cooperation with ISP, IDC, etc.
- Conflict with privacy

I. Methodology to predict incidents

❑ Predicting Incidents using statistics

- Trend of Incidents statistics
- Through the security surveys (CSI/FBI, Symantec)

※KrCERT/CC's Hacking·virus Trend

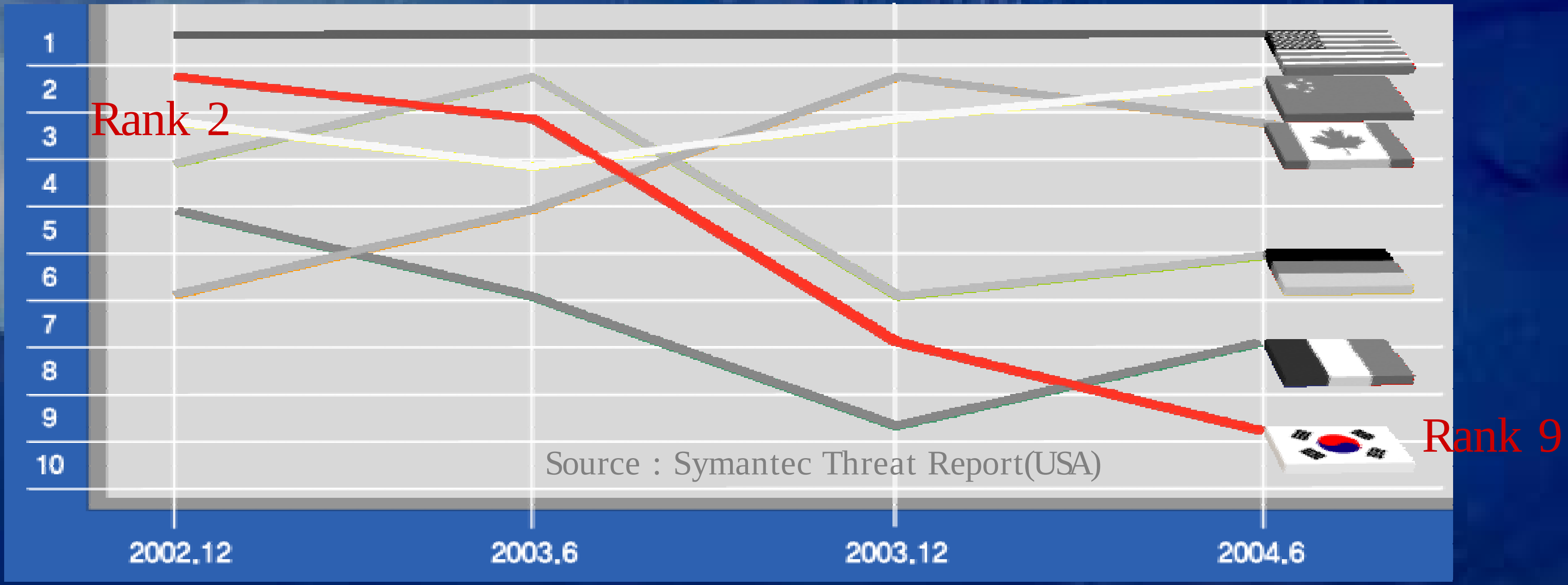


I. Methodology to predict incidents

❑ What level is your economies' security in?

- No methodology available in AP
- Need our standard to get the figures in AP

Top Countries of Attack Origin (In case of Korea)



Source : Symantec Threat Report(USA)

Ⅱ. Estimating the impact of the incidents

EUROPE
RIPE
ASIA
APNIC
AFRICA
OCEANIA
N. AMERICA
ARIN
S. AMERICA
Worm
Trojan Horses
Backdoor

Ⅱ. Estimating the impact of the incidents

❑ Research or Incidents Trend

- Each research shows different figures regarding the impact(eg. Mi2G, CSI/FBI)

❑ Fact : Input(Time & Cost)

- Setting up the model with enough data to estimate
- Time and cost required for prevention or recovery

❑ Delivery of information regarding impacts

- Email, Telephone, or Fax are also available (Passive)
- But recommend a portal site (Proactive)
- Who will get that information? (Members only or not?)

Ⅲ. The Traffic Monitoring Portal Site

❑ Goal

- Enhancing International security protection methodology

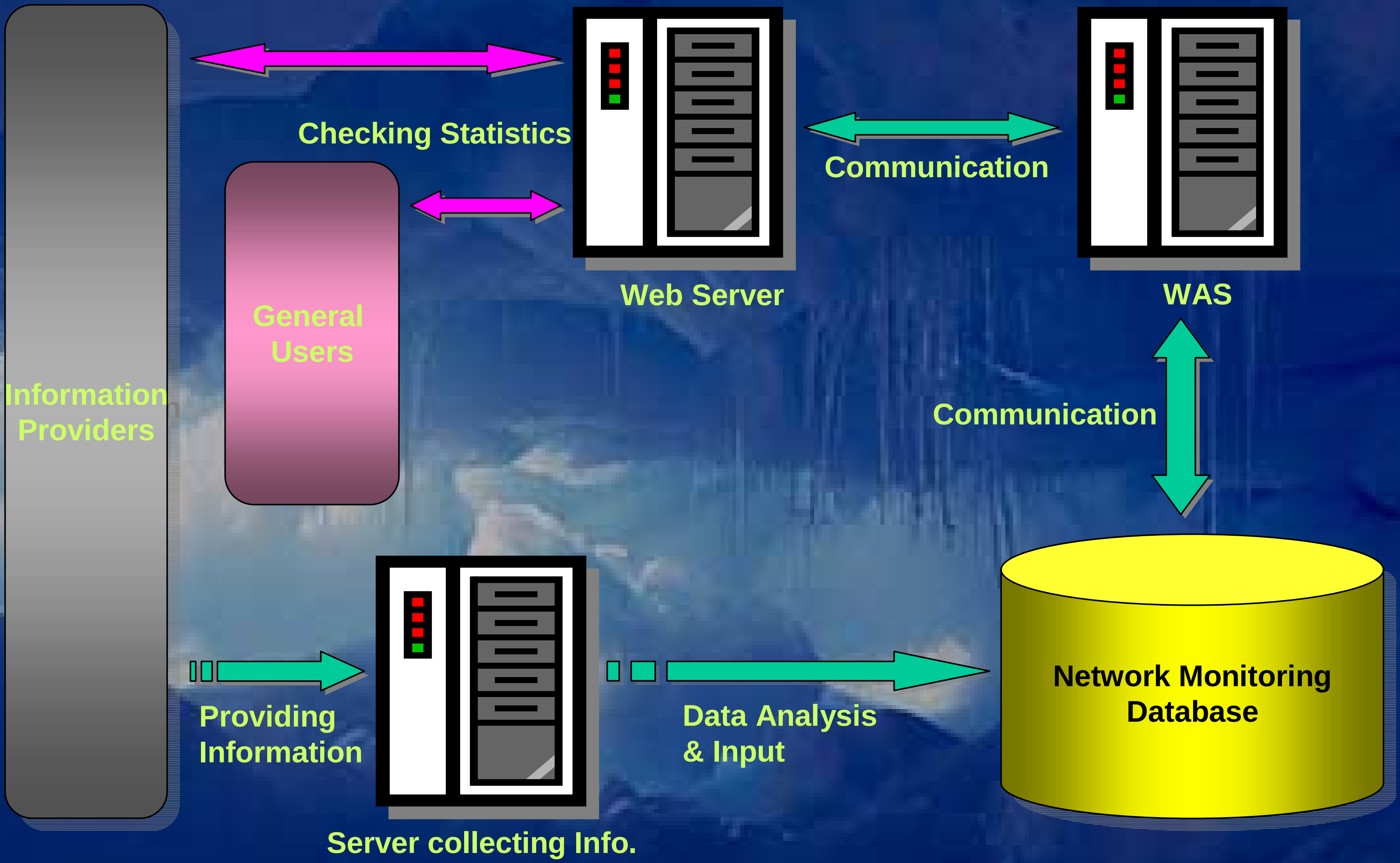
- Developing a communication channel for international cooperation

❑ Overview

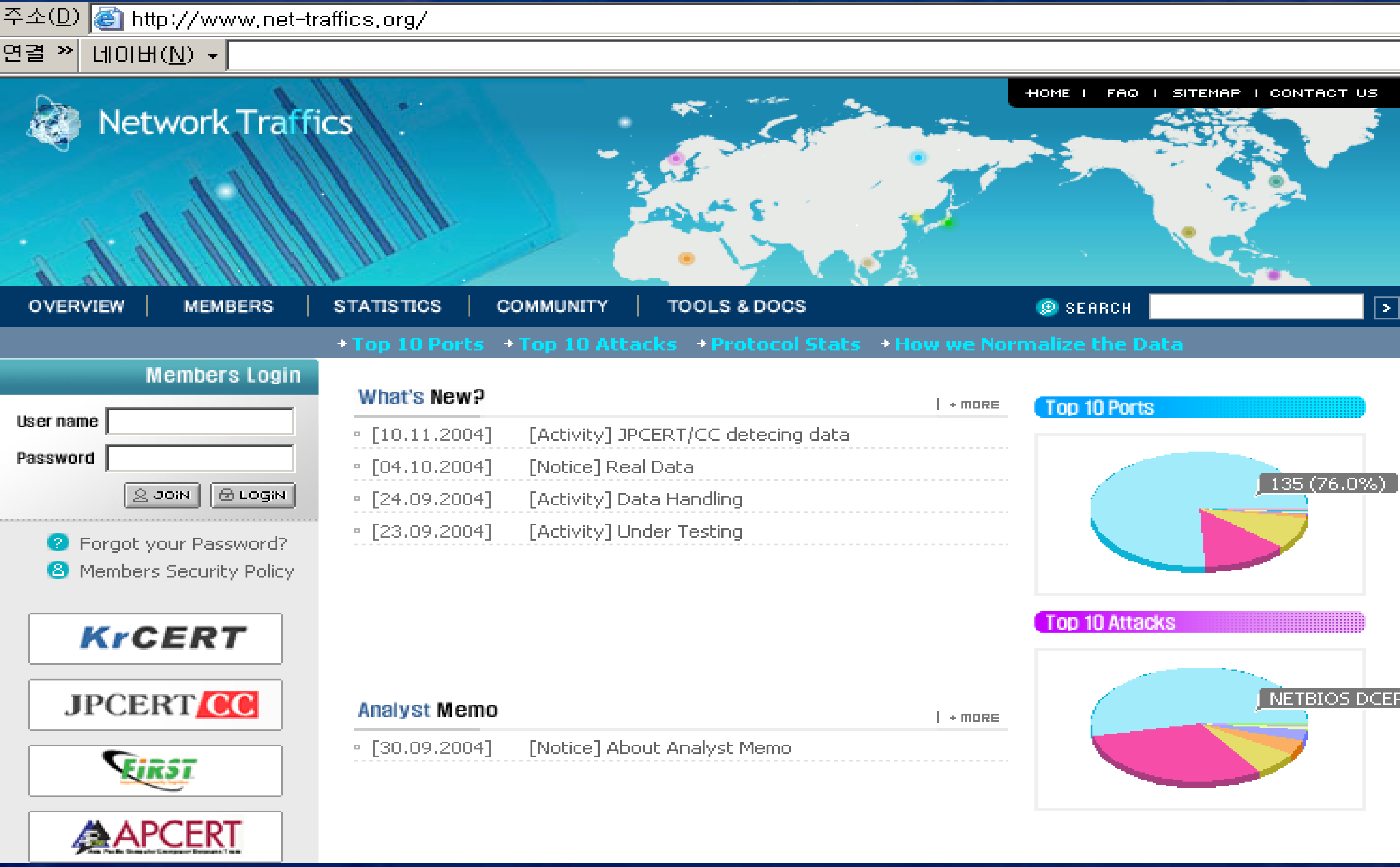
- Traffic data in SSH and IODEF format

- OS : Sun Solaris, DB : oracle

III. The Traffic Monitoring Portal Site



III. The Traffic Monitoring Portal Site



What's New?

- [10.11.2004] [Activity] JPCERT/CC detecing data
- [04.10.2004] [Notice] Real Data
- [24.09.2004] [Activity] Data Handling
- [23.09.2004] [Activity] Under Testing

Analyst Memo

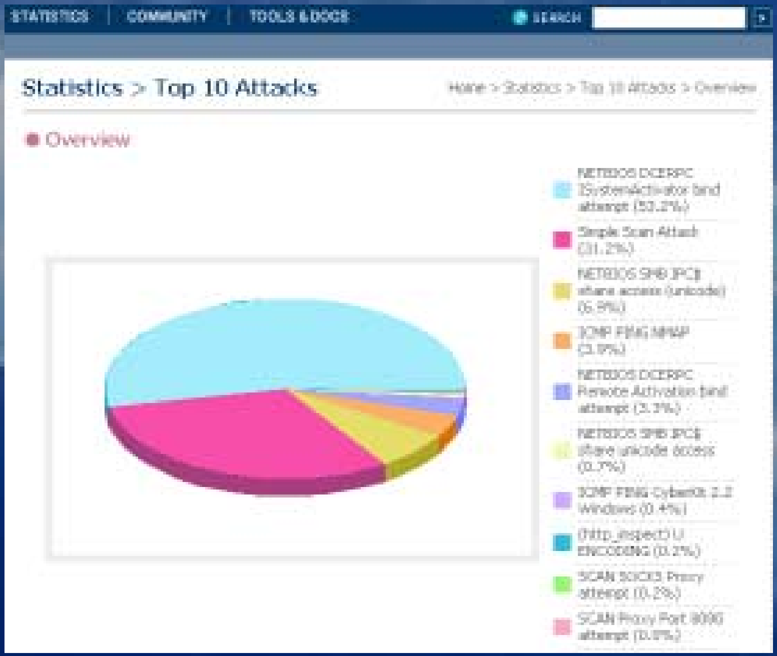
- [30.09.2004] [Notice] About Analyst Memo

III. The Traffic Monitoring Portal Site

❑ Developing the site

http://www.net-traffics.org/

- Need a graph to show the detail of statistics
- About 1,200 logs an hour per country

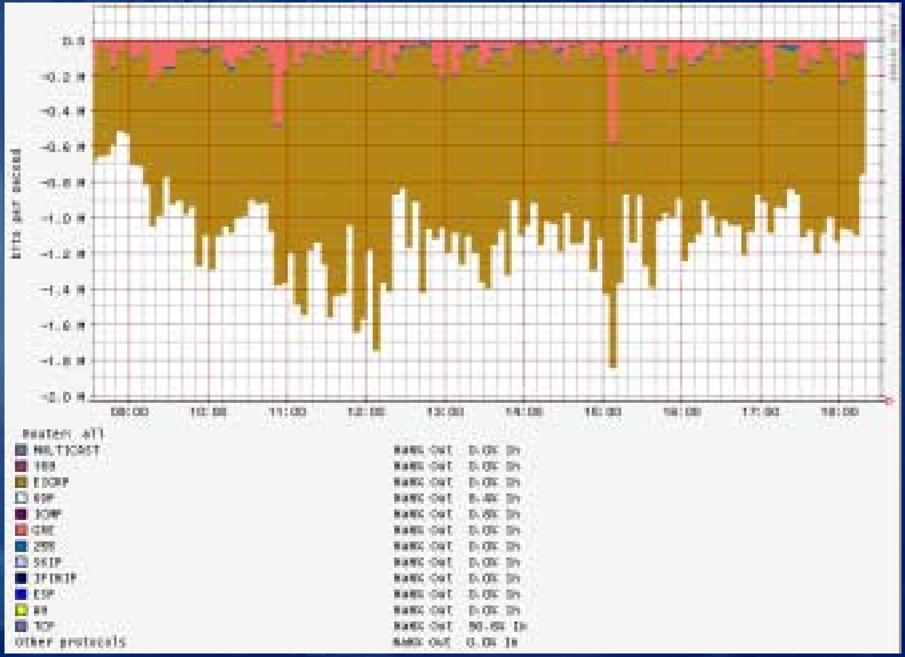


Statistics > Top 10 Attacks

Home > Statistics > Top 10 Attacks > Overview

● Overview

- NETBIOS DCERPC ISystemActivator bind attempt (53.2%)
- Simple Scan Attack (31.2%)
- NETBIOS SMB IPC$ share access (unicode) (6.9%)
- ICMP PING NMAP (3.9%)
- NETBIOS DCERPC Remote Activation bind attempt (3.3%)
- NETBIOS SMB IPC$ share unicode access (0.7%)
- ICMP PING CyberKit 2.2 Windows (0.4%)
- (http_inspect) U ENCODING (0.2%)
- SCAN SOCKS Proxy attempt (0.2%)
- SCAN Proxy Port 8080 attempt (0.0%)



Now

Future

Ⅳ. Is the traffic data critical information?

□ Critical Information

- Depending on each economies' view
- Yes, it is only if the data includes private information
- Don't need any private information in the portal site

□ What is in the traffic data?

- Protocol types, Source IP addresses, etc.

□ Conflict

- Policy view
- Technology view

V. Conclusion

□ **Open mind and Join the project**

□ **Have a look at the contents of the data, then you will think in a different way**

□ **The concrete achievement in AP**

- A portal site
- Incidents Response Drill (IRD)

Thank You for Your Listening