APEC-OECD Malware Workshop Session 4

Panel Discussion: Gaps and Challenges

Pei-Wen Liu, Ph.D.
Director, Information & Communication Security Technology Center,
Chinese Taipei

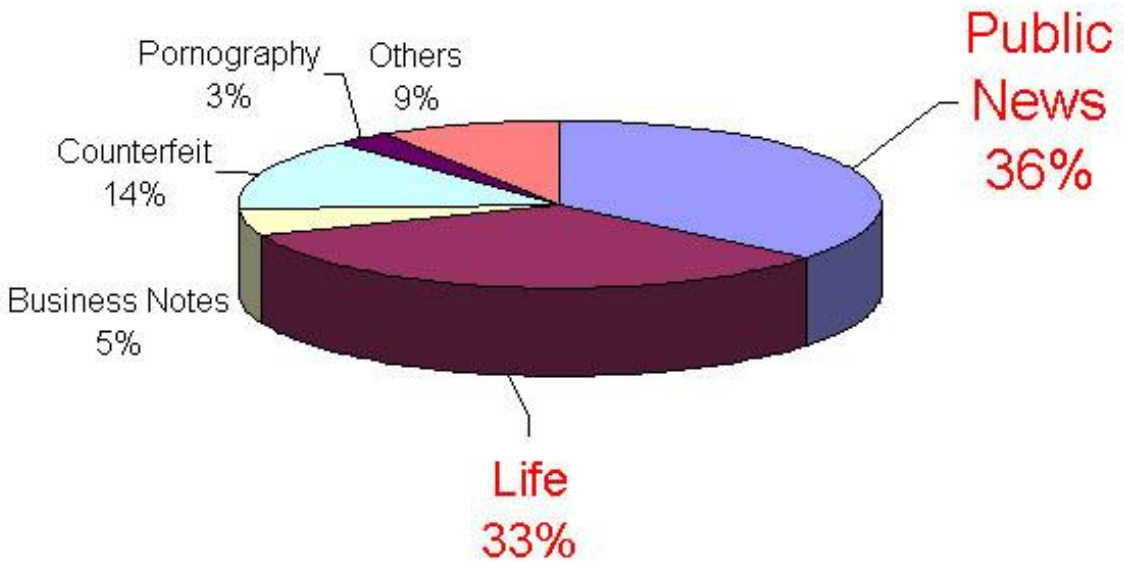
TEL 35, Manila, The Philippines
April 22 and 23, 2007

Some Background

- Who We Are
  - ICST (Information & Communication Security Technology Center)
  - Public Sector CSIRT in Chinese Taipei
- Experiences with Malware
  - Observed and handled constant ***targeted/social engineering malware attacks*** toward our clients since 2004
  - First time zero-day malware (***MS05-36***) discovery in 2005 and presented our handling process in ***APEC TEL 32***

Malicious Email Analysis

- Manual Analysis
  - ICST technicians manually analyze 417 suspected emails collected from our clients in the past 2 years
  - 287 of these emails (i.e., 68.8%) contain malware attachments
  - ***We expect to see more counterfeit emails (even with self-signed certificate) in the near future***



Malicious Email Analysis

- Automatic Analysis System
  - HoneyBear： **B**ehavior-based **E**mail **A**nomaly **R**econnaissance
  - Online since Dec., 2006 with Web-based submission interface
  - Within submitted 184 email samples, 38.6% contained malware

Zero-Day Vulnerabilities

CVE	Description	Bulletin	Affected
CAN-2005-0558	Vulnerability in Microsoft Word May Lead to Elevation of Privilege	MS05-023	Word
CVE-2006-0009	Malformed Routing Slip Buffer Overflow	MS06-012	Office
CVE-2006-2492	**Word Malformed Object Pointer Vulnerability / Smart Tags**	**MS06-027 (*)**	**Word**
CVE-2006-1540	Office Malformed String Parsing Vulnerability	MS06-038	Excel
CVE-2006-3649	Visual Basic for Applications Vulnerability, Buffer Overrun in Word after Unicode Transformation	MS06-047	Word
CVE-2006-3059	Excel Malformed File Vulnerability	MS06-037	Excel
CVE-2006-3590	**PowerPoint Malformed Shape Vulnerability / MSO.DLL**	**MS06-048 (*)**	**Powerpoint**
CVE-2006-3649	Vulnerability in Microsoft Visual Basic for Applications Could Allow Remote Code Execution	MS06-047	Word
CVE-2006-4534	Vulnerability in Word	MS06-060	Word
CVE-2006-4694	Vulnerability in Powerpoint	MS06-058	PowerPoint
CVE-2006-5994	**Vulnerability in Microsoft Word Could Allow Remote Code Execution**	**MS07-014 (*)**	**Word**
CVE-2007-0515	Microsoft Word Document Code Execution Proof of Concept	MS07-014	Word
CVE-2006-6456	**Vulnerability in Microsoft Word Could Allow Remote Code Execution**	**MS07-014 (*)**	**Word**

Source：Microsoft Response Center

Note：items with * were discovered and reported by ICST

Zero-Day Vulnerabilities

Microsoft Security Bulletin MS06-027

Vulnerability in Microsoft Word Could Allow Remote Code Execution (917336)

Published: June 13, 2006 | Updated: June 21, 2006

Summary

Who Should Read this Document: Customers who use Microsoft Word

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: Critical

Recommendation: Customers should apply the update immediately

Security Update Replacement: This bulletin replaces a prior security update. See the frequently asked questions (FAQ) section of this bulletin for the complete list.

Caveats: None

Tested Software and Security Update Download Locations:

Acknowledgments

Microsoft thanks the following for working with us to help protect customers:

- Shih-hao Weng of Information & Communication Security Technology Center for reporting the Microsoft Word Malformed Object Pointer Vulnerability - CVE-2006-2492.
- Andreas Marx of AV-Test.org for working with Microsoft on the Microsoft Word Malformed Object Pointer Vulnerability - CVE-2006-2492.

Look At the Window

Discover Date	CVE #	Affected Software	Patch Release Date	Affected Window (Day)
2006/04/27	CVE-2006-2492	Word	MS06-027 2006/06/13	48
2006/07/05	CVE-2006-3590	Powerpoint	MS06-048 2006/08/08	35
2006/11/27	CVE-2006-5994	Word	MS07-014 2007/02/13	79
2007/01/18	CVE-2006-6456	Word	MS07-014 2007/02/13	27

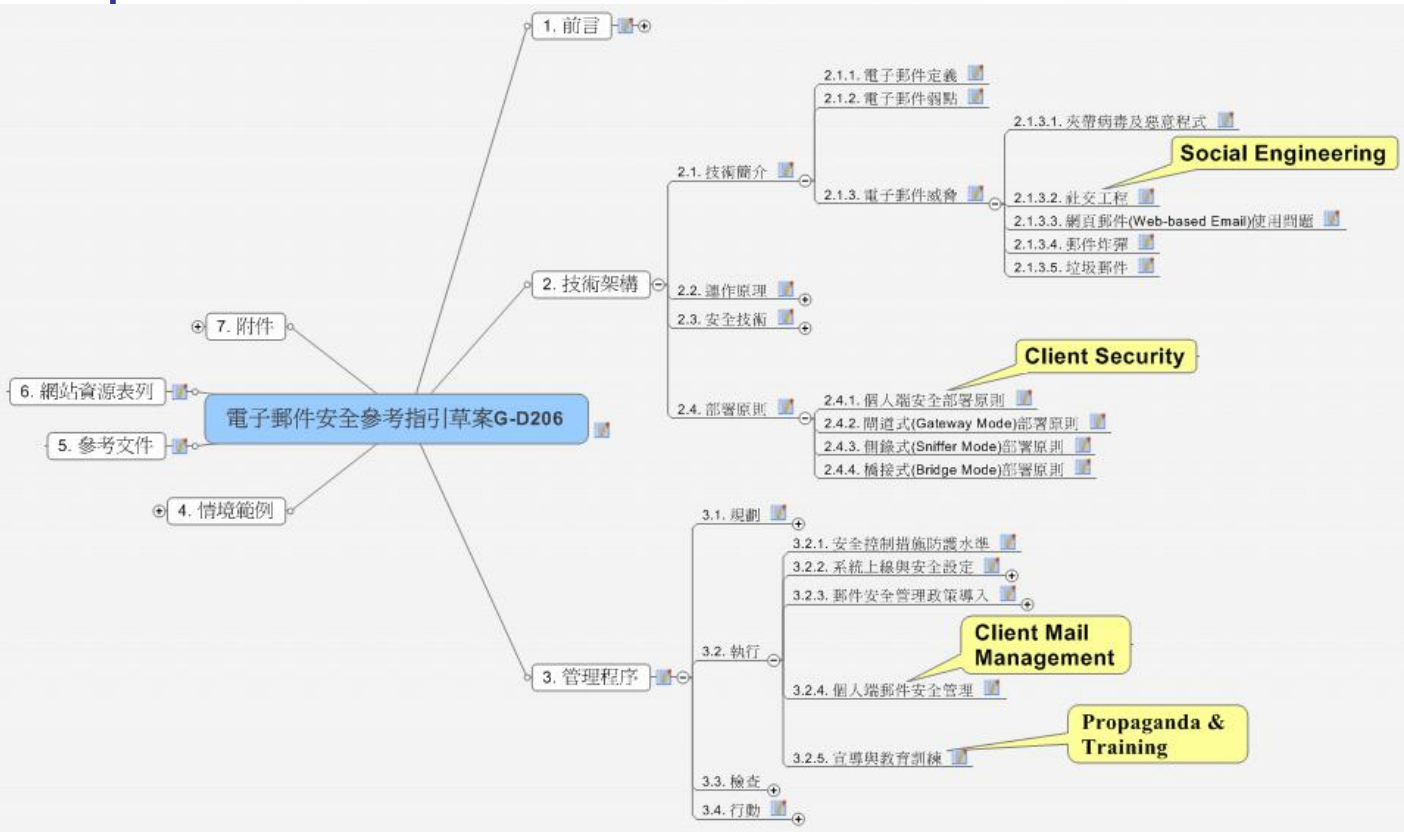
189

Awareness & Education

- Workshops
- E-Learning
  - ICST has developed 41 cyber security e-learning course-ware (50 hours)
  - 4 courses (6 hours) focus on malware prevention for end-users

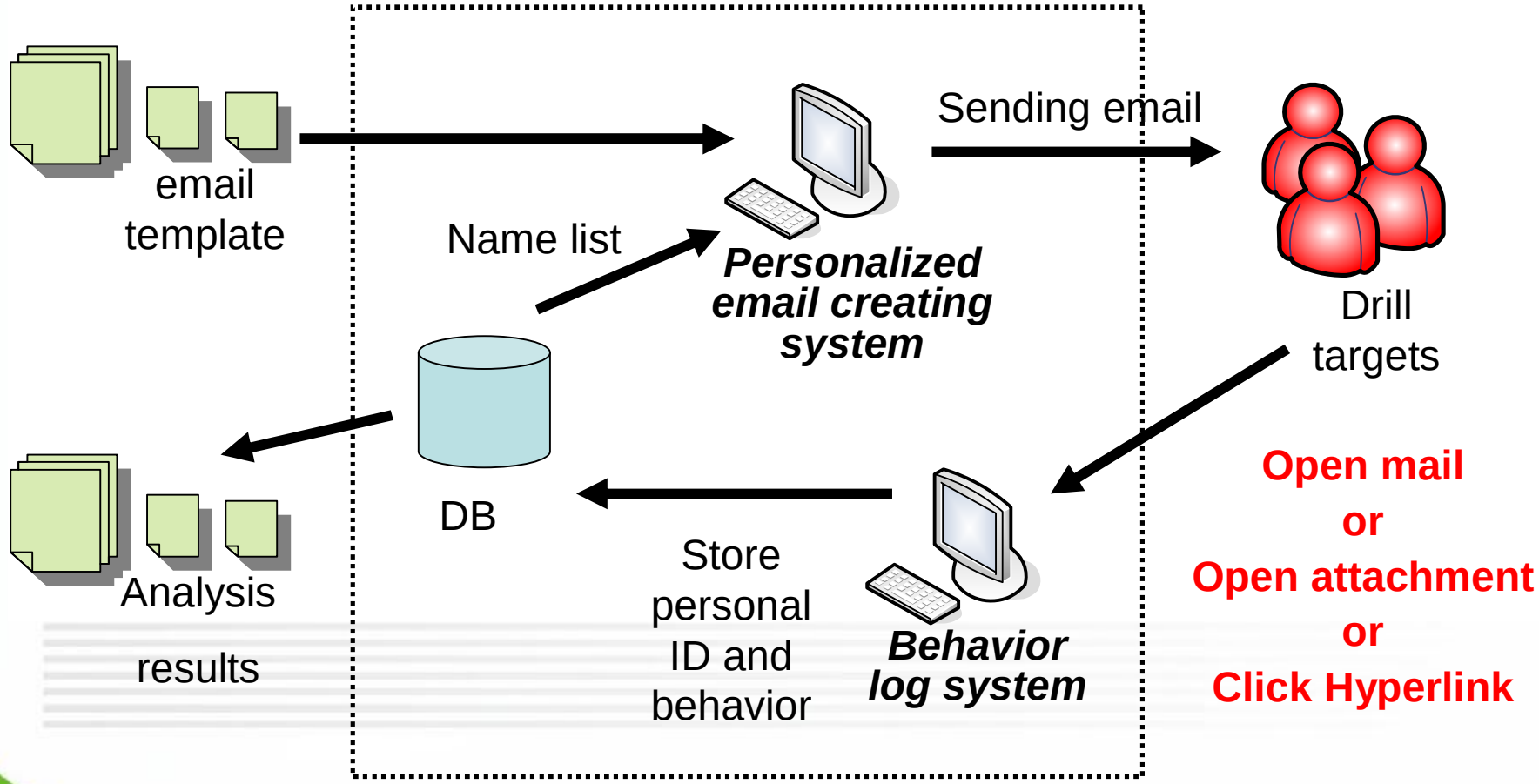
Awareness & Education

- E-mail Security Guideline
  - One of the 37 guidelines developed to supplements the implementation of ISMS



Social Engineering Drill

- How



Social Engineering Drill

- Drill Result
  - Sent 51,300 testing emails of 6 types (contain hyperlinks or attachments) to our 8,550 clients during Dec, 2006
  - ***43.0%*** of our clients opened the testing emails
  - ***23.9%*** of our clients open the attachment or click hyperlink in the testing emails

Major Challenges and Gaps

- With the evolving trend of “Targeted Attack + Zero-Day Attack” in Malware, we found
  - Signature-based solutions often fails
  - End-users are vulnerable to “social engineering” attacks, even defense-in-depth is in place
  - Awareness and education can’t reduce malware risk completely
  - Implementing an air gap or physical separation to protect sensitive networks, though effective, is both resource-intensive and user-unfriendly (against the trend of ubiquitous network society)
  - Generic information security management standard does not address malware issue directly

Mechanisms or Countermeasures

- More Secured End-point
  - Virtualization / Segregation within Device
- Behavior-based Detecting Solution
  - Responsive, High Accuracy and Low Resource Requirement
- Technical Audit Standard
  - combine with more generic ISMS standard