IT 패러다임의 변화와 지식정보보안산업

AhnLab

2008.10.30

안철수연구소

Tables of Contents

AhnLab

I. IT Trend

1. 주목할 패러다임 변화

IT Convergence	Mobility	Everything as a Service(XaaS)	Outsourcing
• Performance (Session, Latency, QoS) • 정량적분석 • 가용성 • 지능형 인증 시스템	• Mobile Device Protection (AV, FW, ..) • Device & User 인증 • Management	• Web Server Security • Endpoint (Browser) Protection • XML, DB 보안	• 내부정보유출 (기술, 고객정보, 비밀문서..) • System Hacking

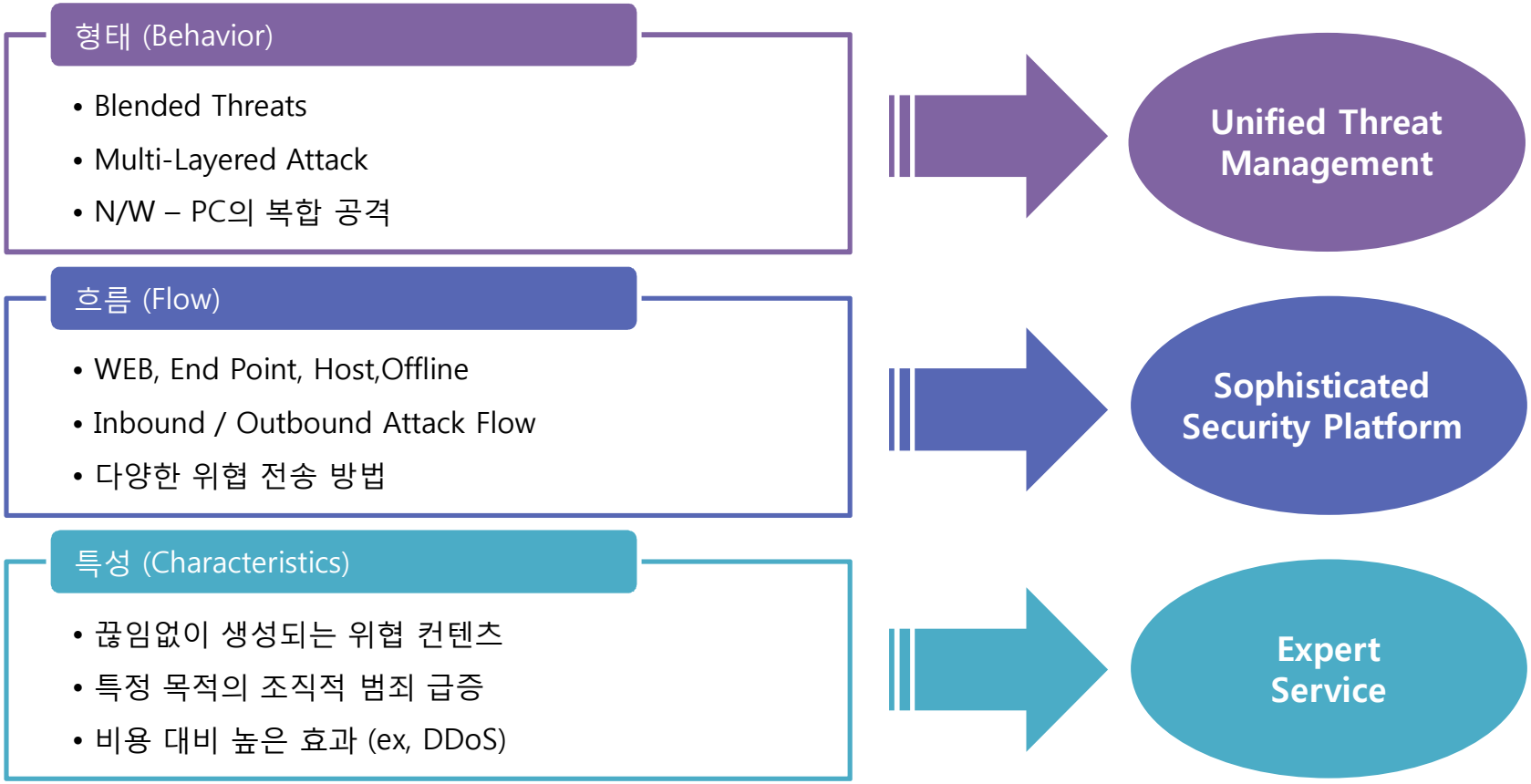
I. IT Trend

2. Security Challenges

개방형 IT 인프라	• 인터넷 기반 • Wired and Wireless
다양한 IP Device	• PC, Notebook • 휴대폰, PDA, 스마트폰
Multimedia Service	• VoIP • Multicast
메시지공유의 다양성	• Offline • Email, Messenger, P2P • 전화, 영상
업무 활동의 역동성	• Global Biz Process • 합병 및 구조조정

II. Cyber Attack Trends

Summary



II. Cyber Attack Trends

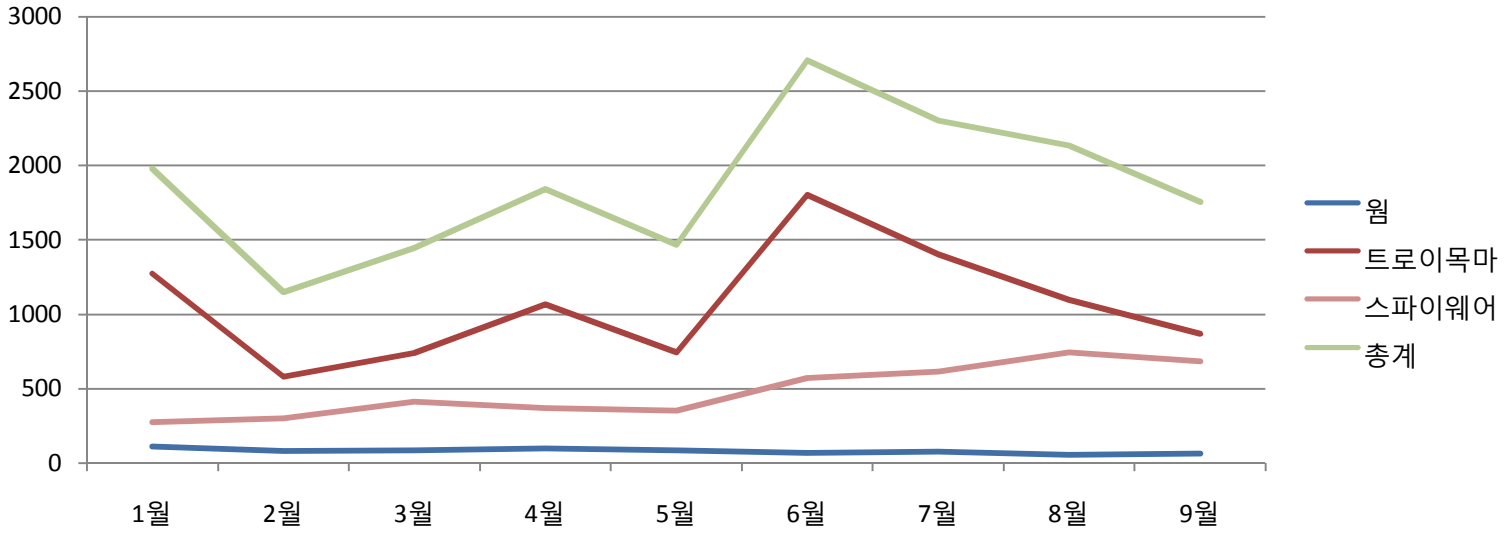
1. 중국발 트로이목마/스파이웨어

개인정보 탈취를 목적으로 하는 트로이목마와 스파이웨어의 폭증

- 2008년 악성코드 증가는 전년도 대비 2배의 증가를 기록

- 트로이목마의 증가가 악성코드 폭증의 주 원인,

- 웜 및 파일바이러스 등 전통적인 악성코드 감소



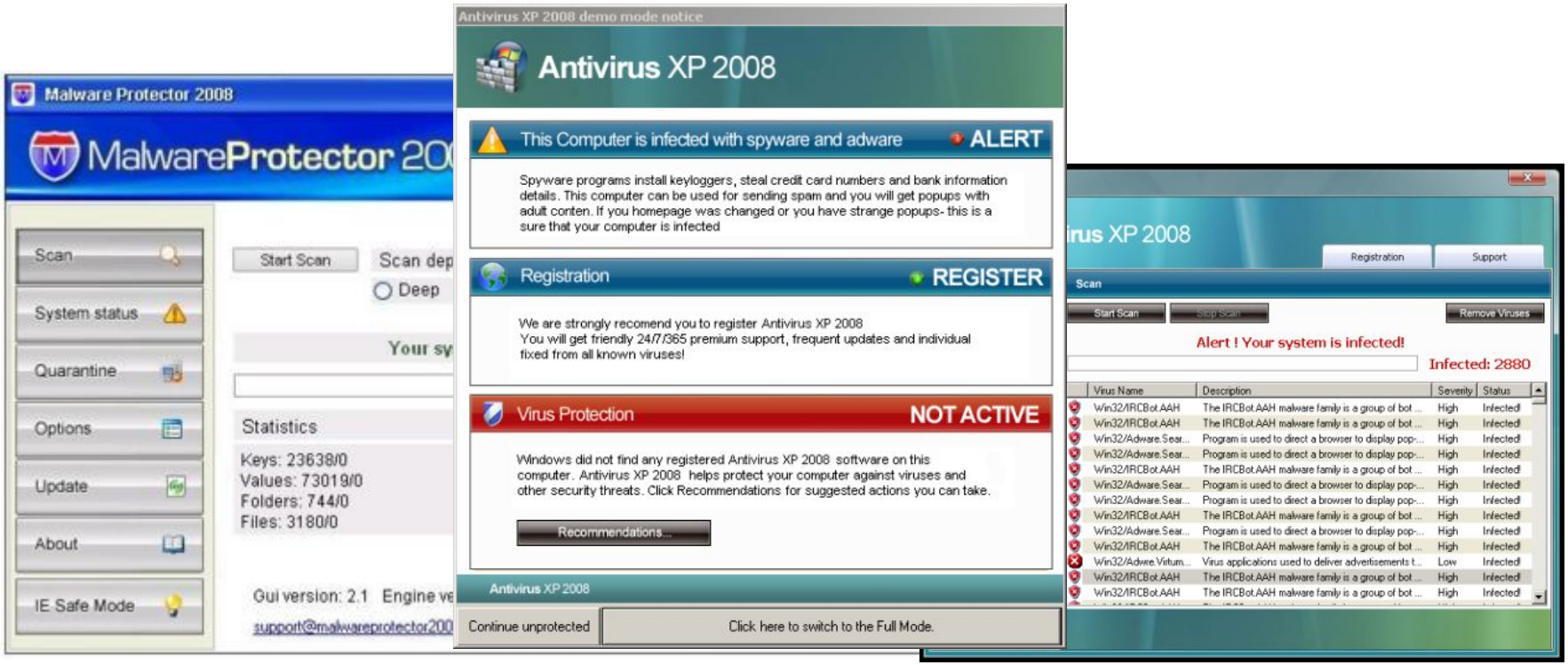
• 출처 : 안철수연구소 ASEC Report 2008. 09월호

II. Cyber Attack Trends

2. Rogue Anti-spyware

백신 프로그램으로 위장, 설치된 후 스팸메일을 발송하거나, 다른 악성코드를 설치하는 "가짜 백신" 증가

- **총 100여개의 변종 발생**
- AntivirusXP 2008, AntivirusXP 2009, VistaAntivirus 2008, WinXSecurityCenter, XPProtector2009
- **백신의 진단/치료를 막기 위한 Access Protection 기법사용으로 치료 방해**



II. Cyber Attack Trends

3. DDoS Attack

가장 쉽게 돈을 벌 수 있는 해킹 도구로 사용

- **광범위한 BotNet 인프라 구축 완료**
- **적절한 가격과 신뢰도 있는 Hacking Service 제공**
- DDoS, **스팸메일 발송 인프라로 활용**

최근 주요 DDoS 공격 사례

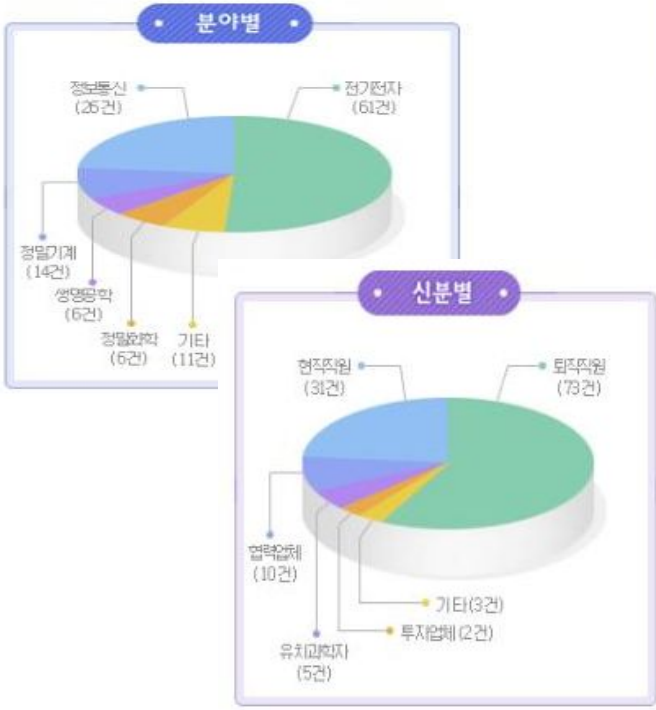
<출처 : KISA>

II. Cyber Attack Trends

4. Data Breach

금전 이득을 목적으로 하는 산업기술 문서, 개인정보데이타 유출 문제 대두

- 07년 한해 32건 적발, 산업가치 89조 7천억원
- 발각되지 않으면 피해사실 조차 알 수 없는 상황
- 보안 솔루션의 기술적 장애와 사용편의성에 영향을 주는 프로세스 제약 문제 상존



• 출처 : 국가정보원 산업기밀보호센터

II. Cyber Attack Trends

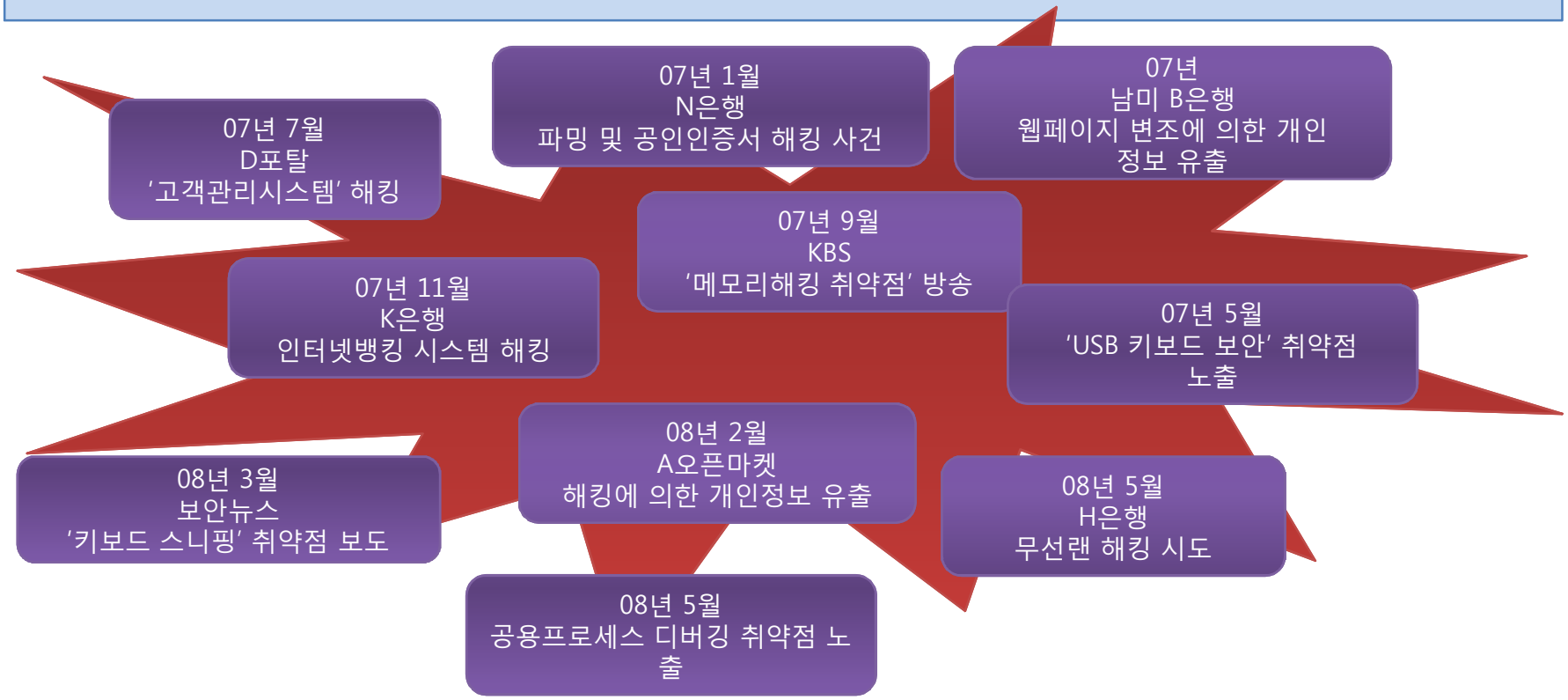
5 Internet 상거래 취약성

인터넷 기반 상거래의 지속적인 증가

– 기존 금융권 및 쇼핑몰

- 인터넷 은행 설립 법률안 검토

– 인터넷 금융/상거래를 대상으로하는 Trojan, Phishing, Parming 공격 증가



Emerging Issues :
지식정보유출

III. 지식정보 유출

1 Market 호칭

- IPC (Information Protection and Control) - *IDC*
- CMF (Contents Monitoring and Filtering*)* – *Gartner*
- DLP (Data Loss Prevention) – Gartner
- ILP (Information Leak Prevention) – *Forrester Wave*
- OCC (Outbound Content Compliance)
- ILD&P (Information Leakage Detection and Prevention)
- Extrusion Prevention

2 Scope

Data in Motion	• Network • Multi-Channel (e-mail, Messaging, P2P, Web, FTP, ..)
Data at Rest	• Discovery, Analysis, Protection and Control • PC, Server, USB, Other Media
Data in Use	• Integrity • End Point, Network Interface

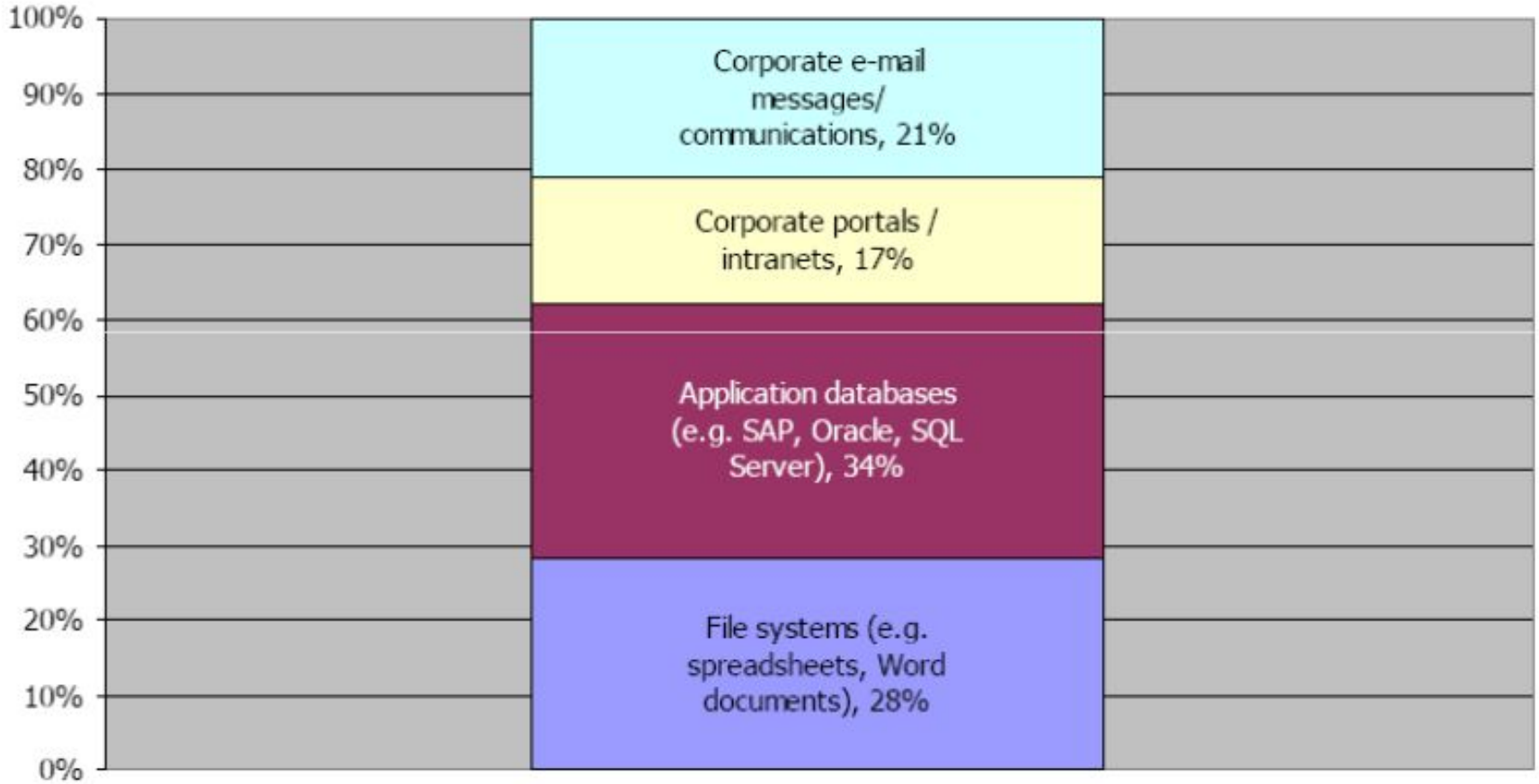
III. 지식정보 유출

3. 보호 대상 Data의 유형

구분	세부내용	비고
Customer Data (Privacy Information)	Social Security Numbers Credit card numbers Health Information	개인 정보보호법 의료 정보보호법
Intellectual Property	Technical Document (CAD, CAM) Source Code Engineering Specs Strategy Documents	산업기술유출방지법 (07년 4월 제정)
Corporate Data	Financial Data M&A Materials Contract Negotiation CEO internal E-Mail HR Data Patents Trade Secrets	
Governmental Data	Economical data Defense Capabilities and planning Intelligence information Law enforcement information	

III. 지식정보 유출

4. Intellectual Property의 저장 위치



Source : Enterprise Strategy Group, Intellectual Property Rules Feb. 2007

III. 지식정보 유출

5. 지식정보유출 방지의 난제

1) Long Battle Line / Guerilla War

- 다양한 장소에 정보는 산재하고,
- 정보의 모습은 지속적으로 변형된다.

2) Too Complicated Technology

Dynamic Policy Enforcement
Resource
Risk
End Point Analysis
Multi-layered Outbound Contents Control
AAA
DLP
Virtualization
Fingerprint
Encryption
Forensic
DRM
Access Control
Document Parsing
Peripheral Device Control
Watermarking
Database
Application
Log Management
Managements
Network
Linguistic Analysis
Threat
Server

3) Working Process

- 금융위기에 의한 경기 침체
- 정보 라이프사이클에(생성, 통합, 소멸) 따른 의 오너쉽 불명
- 고유 업무에 대한 정체성 미고려
- 사용성을 고려하지 않은 기술적 접근

IV Emerging Issues : IE & Memory Hacking

IV. IE & Memory Hacking

1. Endpoint Tool – Internet Explore

공용 프로세스 보호의 한계

- 공용 프로세스에 대한 메모리 보호의 한계
- 공용 프로세스에 대한 모듈 제어의 한계
- 공용 프로세스에 대한 Reversing/Debugging 방어의 한계

IE의 구조적 취약점

- ActiveX의 취약점
- COM 후킹과 Script 조작
- BHO 기능의 악용

데이터 보호의 한계

- 정보의 조작여부 판단의 어려움

IV. IE & Memory Hacking

2. Endpoint Tool – Memory Hacking Demo

DMA(Dynamic Memory Allocation)

- 프로그램이 실행되면서 할당되는 동적 메모리
- 다른 프로세스의 메모리에 Read/Write 접근이 가능함

API Hook

- 프로세스가 사용하는 함수를 중간에서 가로채서 원하는 작업을 수행
- IAT(Import Address Table) 변조

DLL Injection

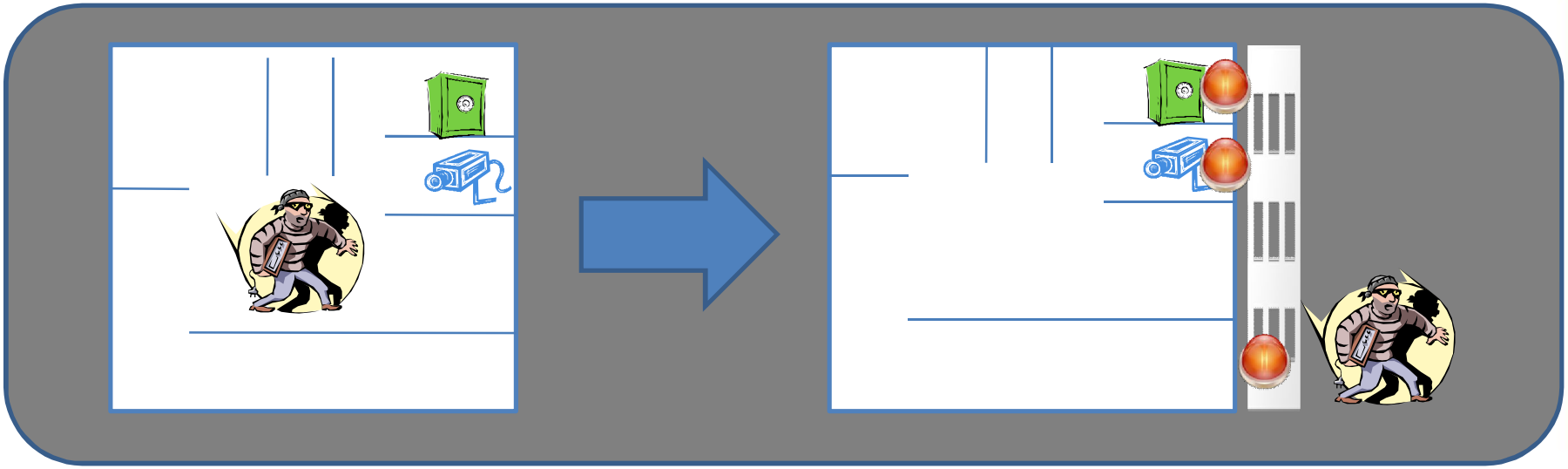
- 다른 프로세스의 영역에 Module을 이식하여 프로세스의 코드/데이터를 원하는대로 구동

IV. IE & Memory Hacking

3. 제언

공격 코드가 전자상거래 단말자체에 접근을 못하도록 방어하는 패러다임의 변화가 필요

- 보안 프로그램의 Self Protection 구현
- 암호화 및 감시/차단 기술의 동시 차용으로 보안 이중화 구현
- 웹페이지 변조에 대한 보안
- 구축/사용에 대한 사용자 거부감 완화



V. 2009 지식보안산업 예측

V. 2009 지식보안산업 예측

기회요소

- Mobile Device / Service 확산
- NW Infra의 지속적인 증설
- 기술 정보 보안의 중요성 인식
- 소프트웨어 분리발주

장애요소

- 세계적인 경기 침체
- 무료 Marketing
- 기술적 한계
- Compliance 관련 입법 지연

주목 할만한 보안 기술

- Virtualization, Behavior Detection, Anti-Debugging, Whitelist

감사합니다

Ahn 안철수연구소