0-Day 공격 방어를 위한 IBM의 다계층 선제 대응 방안

2011/05/18

김형욱, Security Specialist

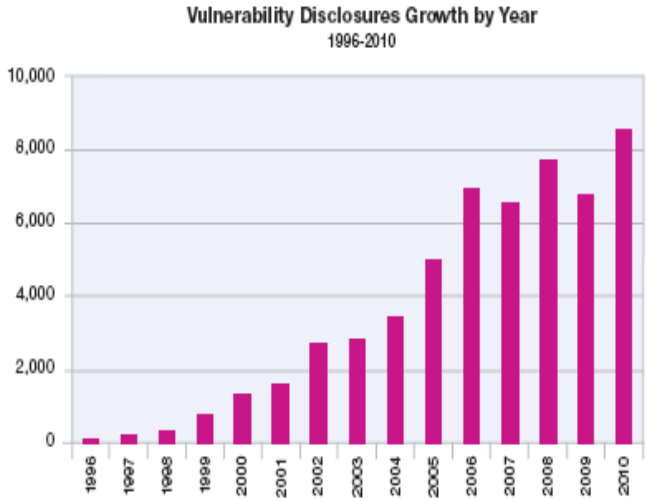
IBM Security Summit

IBM Security Solutions. Secure By Design.

Agenda

- 2010년 보안 위협 동향
- APT 사례 및 APT 공격 기술
- IBM의 다계층 선제 대응 방안
  - IBM 다계층 방어 엔진
  - 네트워크 레벨
  - 서버/클라이언트 레벨
  - 데이터 레벨
  - Ahead of Threat 사례
  - IBM Security Threat Mitigation Solutions

2010년 보안 위협 동향



Patch Release Timing – First 8 Weeks of 2010

Patch Timeline	All	Top Vendors
Same Day	3400	1814
Week 1	192	34
Week 2	55	11
Week 3	57	12
Week 4	33	7
Week 5	27	7
Week 6	22	4
Week 7	17	3
Week 8	16	8

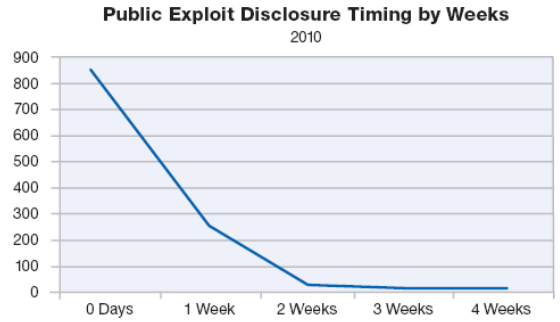
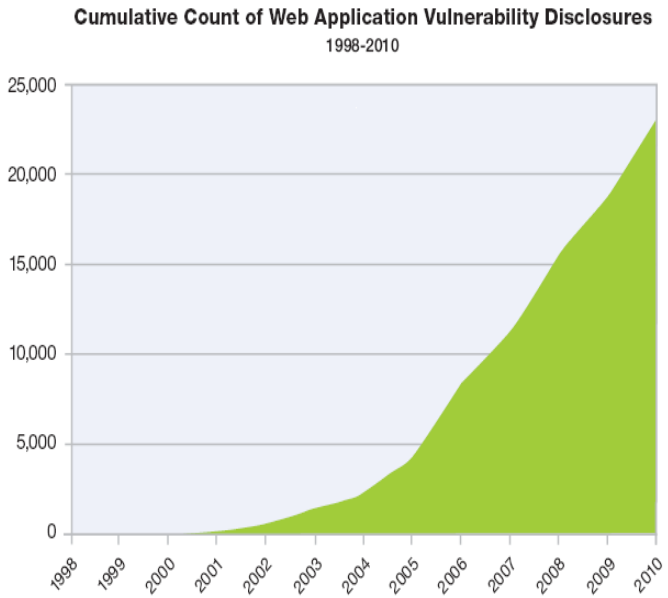
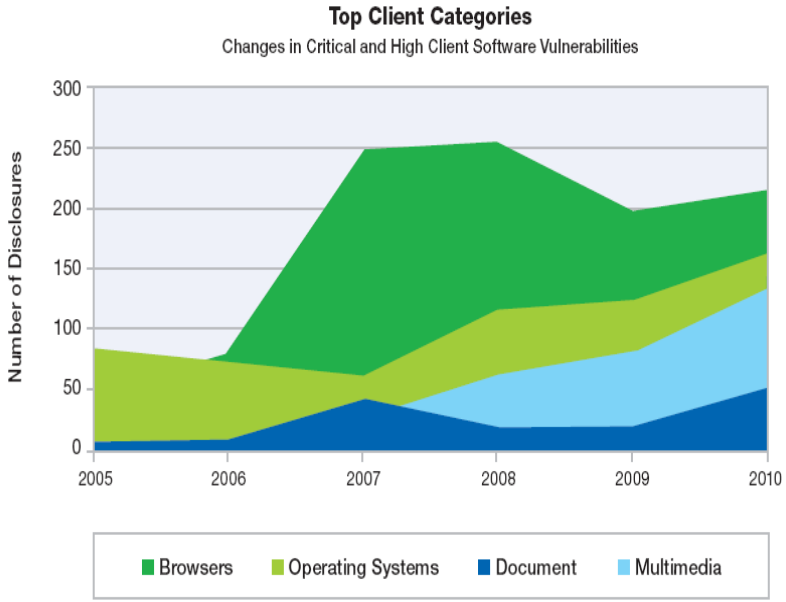


Figure 54: Public Exploit Disclosure Timing by Weeks – 2010

Exploit Timing	0 Days	1 Week	2 Weeks	3 Weeks	4 Weeks
0 Days	854	270	18	9	9



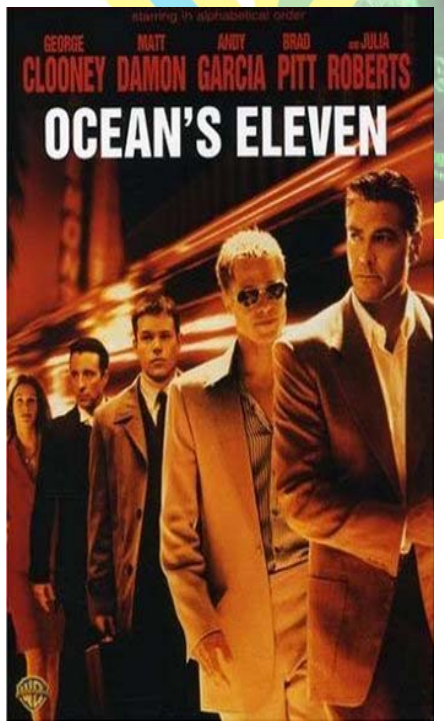


APT 사례 : 스턱스넷(Stuxnet)

2010년 7월 이란 원전 시설을 마비시킨 공격으로 독일 지멘스사의 산업자동화 제어시스템(SCADA)을 공격

- **목표 대상:**
  - 윈도우즈기반의 독인 지멘스사의 산업자동화 제어시스템(SCADA) 소프트웨어
- **최신 공격 기법 사용:**
  - 패치가 없는 Microsoft사 4개의 취약점을 공격
  - 훔친 디지털 전자 인증서로 서명된 콤포넌트 사
  - USB를 통한 감염
- **피해사례:**
  - 이란 원전을 비롯하여 중국 수력발전, 교통시스템, 국제공항 등 1000여개의 사회간접자본 시설들이 공격 당함

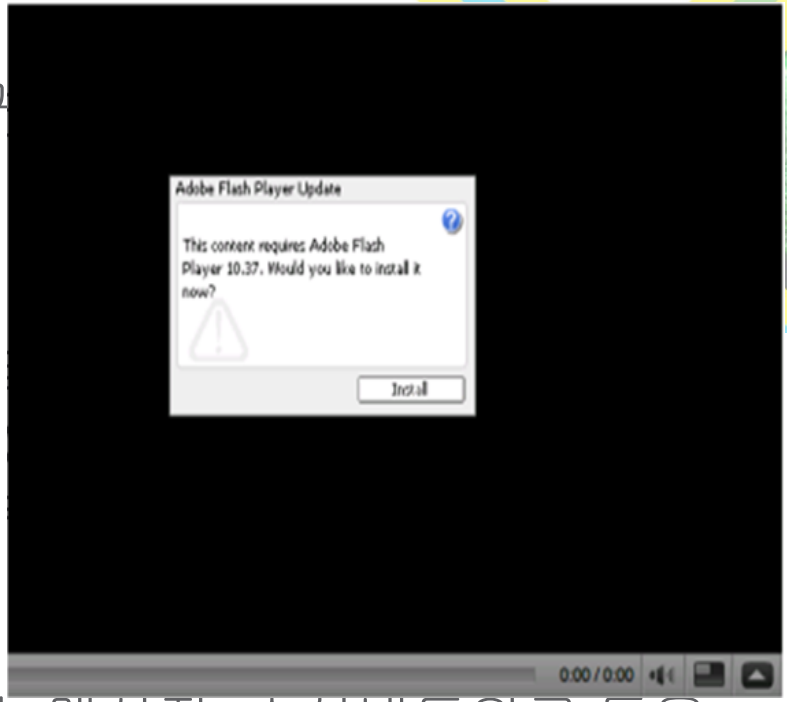
APT : Advanced Persistent Threat



- 특정 대상의 기밀정보나 정치적 목적을 위해 최신의 복합적인 공격 기법과 방식들을 통해 지속적으로 위협을 가하는 형태
- **A**dvanced
  - 기존 보안 제품을 우회하도록 새로운 형태의 악성코드 제작
  - 아직 보고되지 않은 취약점을 악용한 공격 사용(zero day)
- **P**ersistent
  - 수 개월에서 수년에 걸친 공격 수행
  - 발각에 대한 방해 및 조치 회피 시도 (내성)
- **T**hreat
  - 무작위 공격이 아님
  - 자동화된 툴과 단순한 스캐닝에 의존하지 않고 사람이 개입됨
  - 기밀 정보 획득을 위해 조직내에 특정 개인 또는 그룹을 목표로 삼음
- 대표 사례 : Aurora(2009), Stuxnet, Night Dragon(2010) 등 공격

APT 공격 기법(1)

- Reconnaissance(사전 조사)
  - 목표물을 인지하고 뚫기 위한 방법 연구
  - 초기 목표는 항상 진짜 목표가 아니다
- 0-Day 공격
  - 아직까지 발견되지 않거나 사용되지 않은 취약점을 악용
  - 주로 특수 제작된 악성코드 사용
    - 광범위한 정보 수집에 사용
- Social Engineering
  - 피싱 메일 주로 사용
  - 신뢰하는 개인, 조직을 가장하여 이메일, 메신저, 소셜네트워크 등을 이용
  - 본문에 악성코드를 포함하거나 악성코드 웹페이지로 유도하는 링크 포함
- Covert (은닉)
  - 서두르지 않고 정상적인 사용자를 가장하여 활동
  - 합법적인 계정과 프로토콜 및 시간대를 이용하여 활동



APT 공격 기법(2)

- Privilege Escalation and Lateralization(권한상승)
  - 대부분의 공격자는 현재 계정이 갖는 권한내에 수집 가능한 모든 정보를 수집
  - 일부 APT 공격의 경우 새로운 관리자 계정을 생성
- Adaptive
  - 공격이 발각되었는지에 대해 지속적으로 관찰하고, 발각 시 이에 따라 필요한 대응을 취함
  - 공격자는 낮은 레벨의 공격 방법부터 사용
- Persistence
  - 공격자는 참을성을 가지고 오래 기간 동안 목표를 관찰
  - 공격자는 타겟 네트워크에 지속적으로 접근할 수 있는 다양한 백도어를 설치

IBM의 다계층 선제 대응 방안

IBM Security

Security Infra

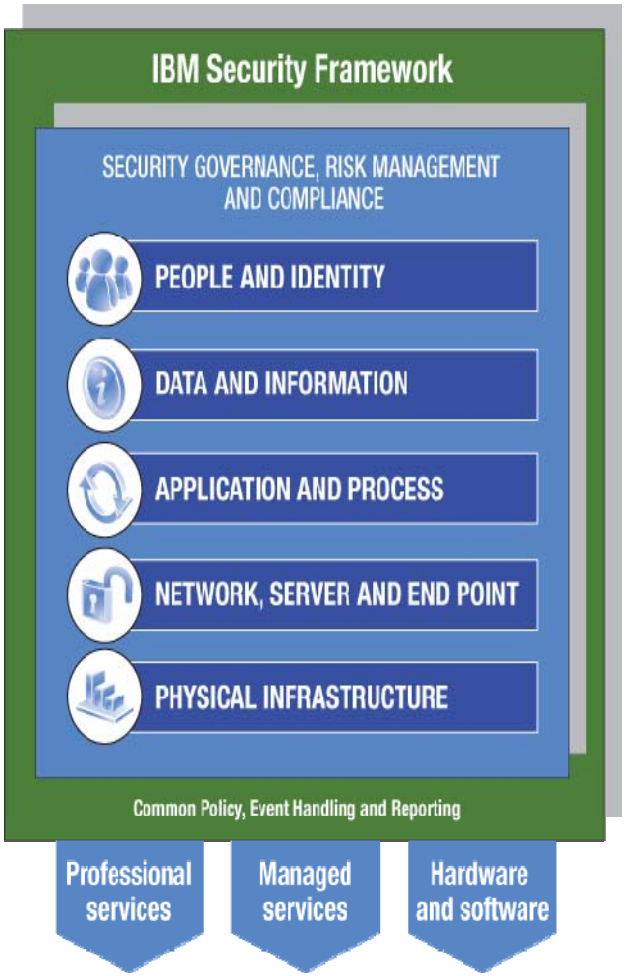
- 보안 연구소 X-FORCE
- 5개 대륙에 9개 관제 센터
- 133개국의 세계 각국에서 보안 관제 센터 운영
- 글로벌 위협 관리 센터 (GTOC)
- 48,000개 이상의 취약점 분석 정보 보유
- 15,000명의 연구자 및 개발자들이 보안을 고민

X-FORCE Research

- 전세계 기업 보안 연구소 중 가장 잘 알려진 연구소
- 평균 최근 위협보다 341일 앞선 방어를 제공
- 100억개 – 웹페이지 및 이미지 분석
- 1억5천개 – 매일 침입 시도 분석
- 4천만개 – 스팸 및 피싱 공격 분석
- 5만1천개 – 문서화된 취약점 분석
- 수백만개 – 악성 코드 샘플 분석

Technology

IBM 보안 프레임워크



- GRC 거버넌스, 위험 관리와 컴플라이언스
- 사람과 아이덴터티
- 데이터와 정보
- 어플리케이션과 프로세스
- 네트워크, 서버와 단말 등 IT 인프라
- 물리적 인프라

IBM 다계층 방어

IBM X-FORCE 보안 연구소의
끊임없는 연구 개발 노력으로
선제적 보안을 제공

IBM 다계층 방어 엔진

가상패치(Virtual Patch

가상 패치란?
소프트웨어 취약점 보호

왜 중요한가?
2010년 취약점의 44%는 벤더에서 취약점 패치를 제공하고 있지 않음

Client-Side (CS) 어플리케이션 보호

CS 어플리케이션 보호?
MS오피스, 어도비 PDF, 웹브라우저와 같은 사용자어플리케이션 보호

왜 중요한가?
개인 PC에 영향을 주는 취약점이 꾸준히 증가

웹 어플리케이션 보호 (WAP)

WAP는 무엇인가요?
SQL 인젝션, XSS와 같은 웹어플리케이션 레벨의 공격에 대한 방어

왜 중요한가?
보안위협의 진화와 컴플라이언스 요구사항을 둘다 만족하기 위해서는 보안 능력을 확장해야 함

위협 탐지 및 방어

위협 탐지 및 방어란?
광범위한 위협에 대한 탐지 및 방지

왜 중요한가?
지속적인 시그너처 업데이트를 통해 새로운 위협에 대응

Application Control

어플리케이션 통제란?
기업 네트워크상의 어플리케이션에 대한 관찰 및 통제

왜 중요한가?
기업 보안정책과 거버넌스를 반영하여 네트워크 어플리케이션과 서비스 접근을 강화

Data Security

데이터 보안이란?
개인 정보나 기밀 정보에 대한 모니터링

왜 중요한가?
개인정보나 기업의 기밀정보를 보호함

서버, 클라이언트 레벨 (OS, App) | 네트워크 레벨 | 데이터 레벨

Analyzing & Protection, Discovery & Auditing, Data in Motion

네트워크, 서버와 단말 등 IT 인프라 계층

IBM 다계층 방어의 핵심

다계층 방어 엔진 **PAM (Protocol Analysis Module)**

- IBM 위협완화 보안 솔루션의 핵심 엔진
- 네트워크 트래픽과 컨텐츠를 인지하고 분석
- 업계 최대 247개의 프로토콜 및 데이터 파일 포맷을 분석
- 새로운 기술의 차용이 쉽고, 진화하는 위협 뿐만 아니라 시장의 요구 사항을 반영
- 20가지 이상의 탐지 분석 기법 사용
- 우회 공격에 대한 탁월한 대응

  eg) IP Frag, TCP Stream Frag, RPC Frag, URL 난독화 등

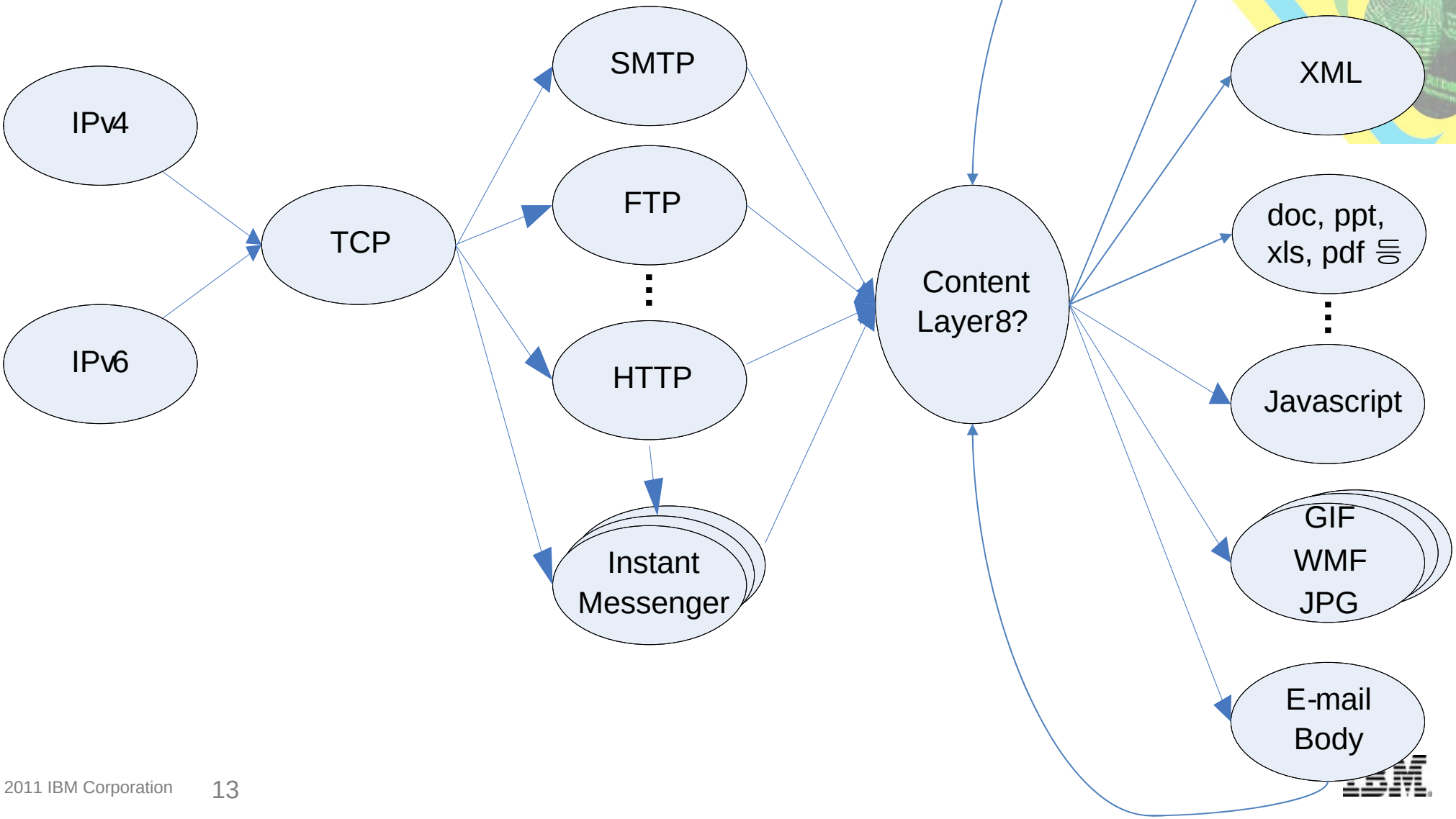
* http://www.iss.net/security_center/reference/help/pam

<프로토콜 분석 방법>

IBM 다계층 방어 엔진 (Protocol Analysis Module)	
Vulnerability Modeling & Algorithms	RFC Compliance
Stateful Packet Inspection	TCP Reassembly & Flow Reassembly
Protocol Anomaly Detection	Statistical Analysis
Port Variability	Host Response
Port Assignment	IPv6 Native Traffic Analysis
Port Following	IPv6 Tunnel Analysis
Protocol Tunneling	SIT Tunnel Analysis
Application-Layer Pre-Processing	Port Probe Detection
Shellcode Heuristics	Pattern Matching
Context Field Analysis	Custom Signatures
IBM Security Content Analyzer	Injection Logic Engine

IBM 다계층 방어 엔진

- 모든 레벨에서 Protocol/Content 분석

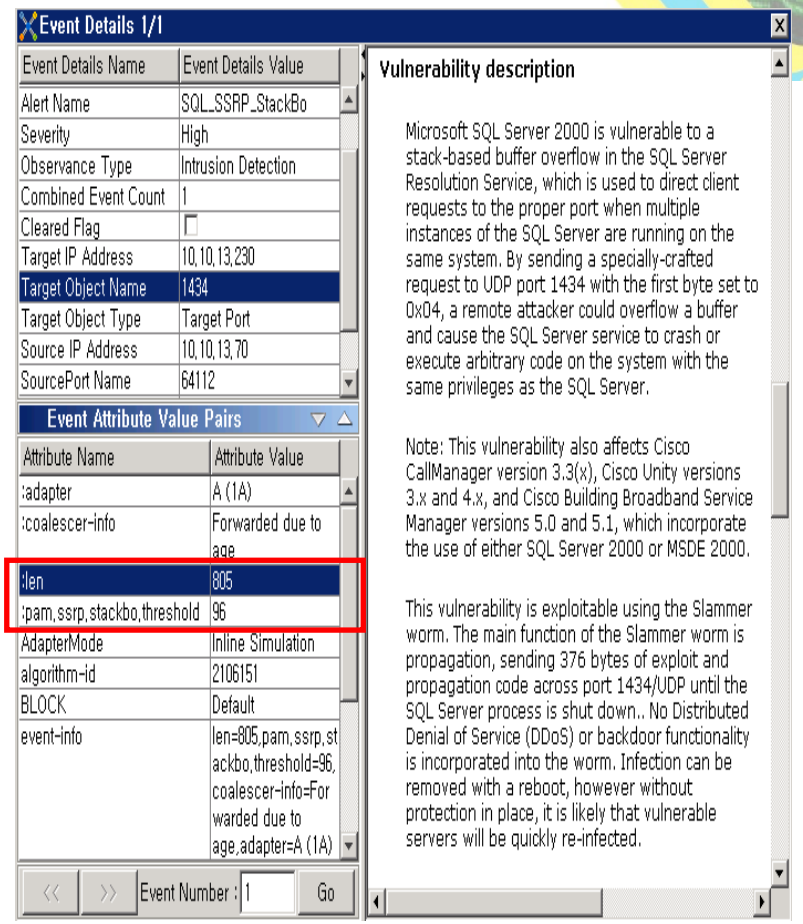


취약점 분석 기반의 위협 탐지 및 방어

- IBM의 다계층 방어 엔진은 IBM X-FORCE 보안연구소에 의해 검증된 취약점 (Vulnerability) 분석기반의 위협 탐지 및 방어를 제공

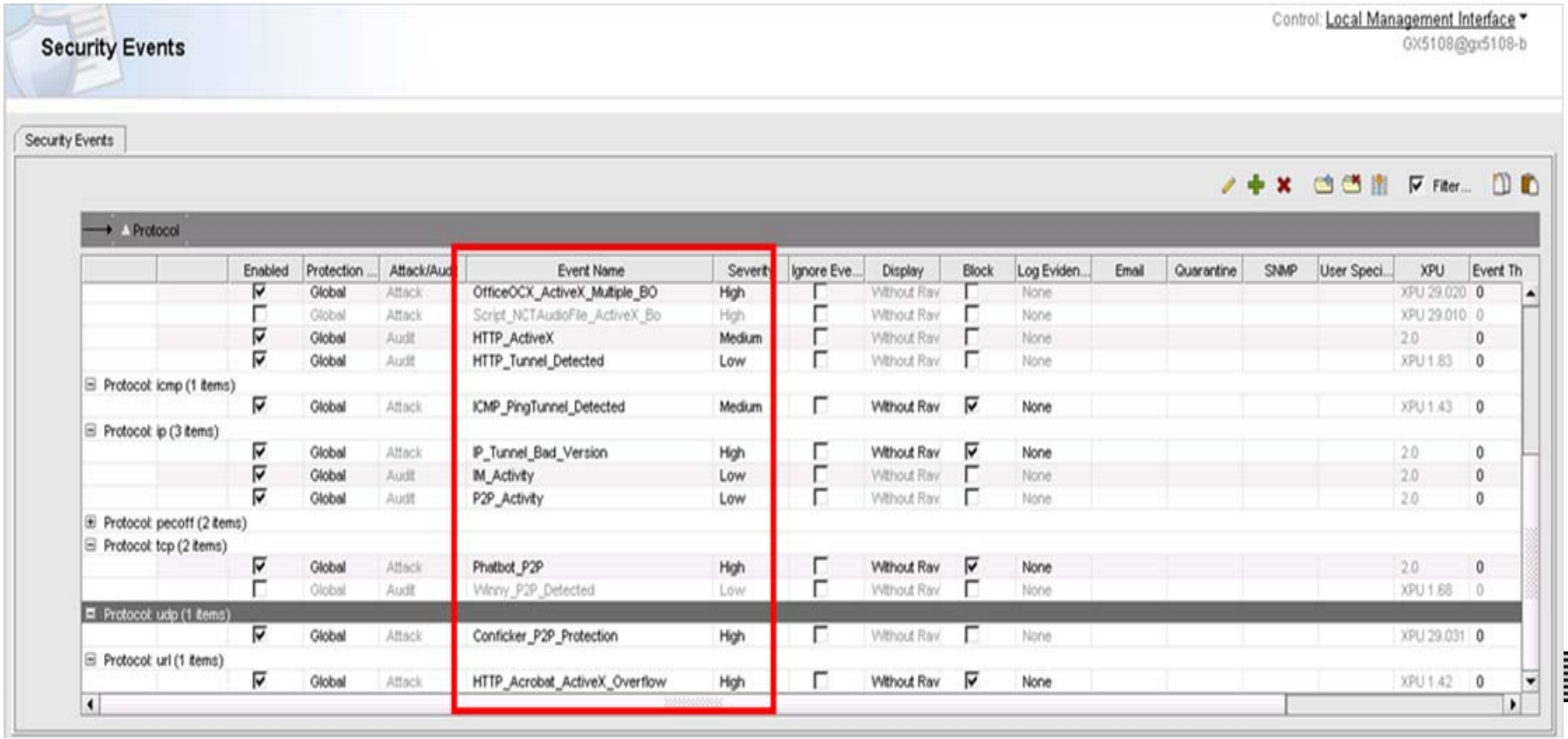
	취약점(Vulnerability) 기반	공격코드(Exploit code) 기반
Zero-day 방어	**선제적 탐지** 및 방어	탐지 및 차단 불가능
정탐 및 우회 가능성	오탐이 적으며, 우회하기 어려움	오탐이 많으며, 우회하기 쉬움
개발 용이성	기술과 축적된 노하우 요구	공개된 공격코드 기반으로 개발용이
사례 : Slammer (MSSQL웜) 탐지 방어 조건	①UDP Port 1434사용하며, 첫번째 Byte는 0x04 ②MSSQL 프로토콜을 파싱하고. 공격이 성공하는 조건인 stack buffer overflow를 발생시키는 조건(>96)을 체크함	①UDP Port 1434사용하며, 첫번째 Byte는 0x04 ②MSSQL 프로토콜을 dummy 트래픽으로 인식하고, 공격코드 트래픽에 나타나는 특정 스트링 패턴을 매칭하여 탐지 content:"l81 F1 03 01 04 9B 81 F1 01l", "sock", "send"

<IBM IPS 관리 콘솔의 이벤트 상세 정보 화면 – Slammer



네트워크 정책 집행

- 네트워크에 기업의 보안 정책을 집행하고 모니터링
  - 보안 정책에 따라 네트워크 어플리케이션, 서비스 접근에 대한 허용/차단을 모니터링함
  - ActiveX/Suspicious ActiveX, HTTP/Email_Executable/DLL, P2P, IM, Tunneling, TOR, Botnet 활동, 특정 통신 Connection 등



Virtual Patch Technology

- 소프트웨어 패치와 독립적으로 취약점을 노리는 공격을 선제적 방어
- 긴급 보안패치가 발표된 경우, 서비스 중단 없이 해당 공격으로부터 보호
- 패치관리 프로세스에 유연성을 제공
  - 정해진 유지보수 시간에 패치를 할 수 있도록 패치관리 프로세스에 일조
- One-Click으로 자산에 대해 패치효과를 구현

Patch Release Timing – First 8 Weeks of 2010

Patch Timeline	All	Top Vendors
Same Day	3400	1814
Week 1	192	34
Week 2	55	11
Week 3	57	12
Week 4	33	7
Week 5	27	7
Week 6	22	4
Week 7	17	3
Week 8	16	8

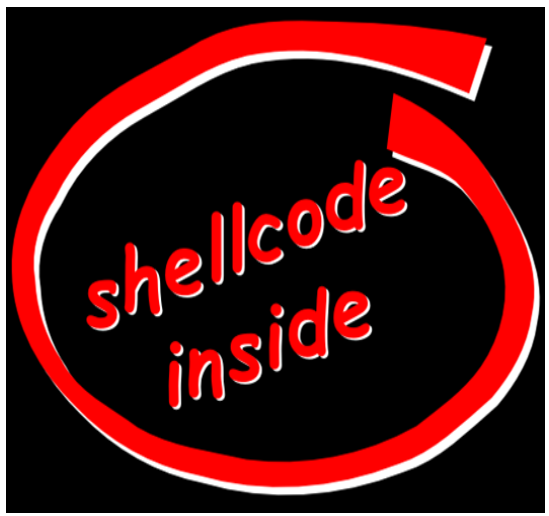
“ 2010년 말, 한 해 동안 발견된 모든 취약점 중 44%는 취약성에 대한 패치가 해당 벤더로부터 제공되지 않음 ”

Client Side 어플리케이션 보호

Shellcode Heuristics (SCH)

- 파일 포맷 취약점을 공격하는 Shellcode를 행위기반으로 인식하여 차단
- IBM X-FORCE 특허 기술로 2006년 3월 PAM 엔진에 탑재
- 시그너처 업데이트없이 Microsoft Office 관련 신규 취약점의 80% 이상을 탐지

  - 여러 개의 IE 취약점 발견 : VML(MS06-055), XML(MS06-071)
  - 낮은 오탐율 : 2천2백만개 미디어 파일에서 단 2개의 오탐율
  - 다음과 같은 어플리케이션에서 shellcode를 탐지, 방어함:
    - MS Ofice Compound documents files – doc, xls, ppt, etc
    - MS .NET Intermediate Language DLL files
    - SOCKS protocol stream
    - Javascripts, PDF
    - HTTP POST Form Data, DNS UDP Traffic, Finger/FTP/IRC/POP3/SMTP/WINS Requests, Ident Requests and Responses



Web Application 보호

- 컴플라이언스 요구 사항과 진화하는 위협에 대한 대응
  - Web Application, Web 2.0, 데이터베이스를 보호
  - 쉬운 설정으로 웹어플리케이션 방화벽(WAF) 기능 제공
  - 행위기반의 인젝션 공격 방어 엔진인 ILE (Injection Logic Engine) 탑재

- 다음과 같은 공격으로 부터 보호
  - SQL (Structured Query Language) Injection
  - XSS (Cross-site scripting)
  - PHP (Hypertext Preprocessor) file-includes
  - CSRF (Cross-site request forgery)
  - Path Traversal
  - HTTP Response Splitting
  - Forceful Browsing

데이터 유출 방지

- 네트워크에 흘러다니는 데이터 흐름을 파악하고 잠재적 위험이 존재하는지 파악/결정하는데 도움
- 개인 정보(PII) 및 기밀 정보를 인식하고 모니터링
- 유연하고 커스터마이징 가능한 데이터 서칭
- 기업의 데이터 보안 전략을 보완
- 다음과 같은 프로토콜과 컨텐츠에 대해 제공
  - 프로토콜: HTTP, FTP, SMB, SMTP, IMAI POP3, AOL IM, MS Messenger, Yahoo Messenger, IRC
  - 컨텐츠: MS 오피스 문서, PDF, Text, RTF XML, HTML, GZIP, ZIP

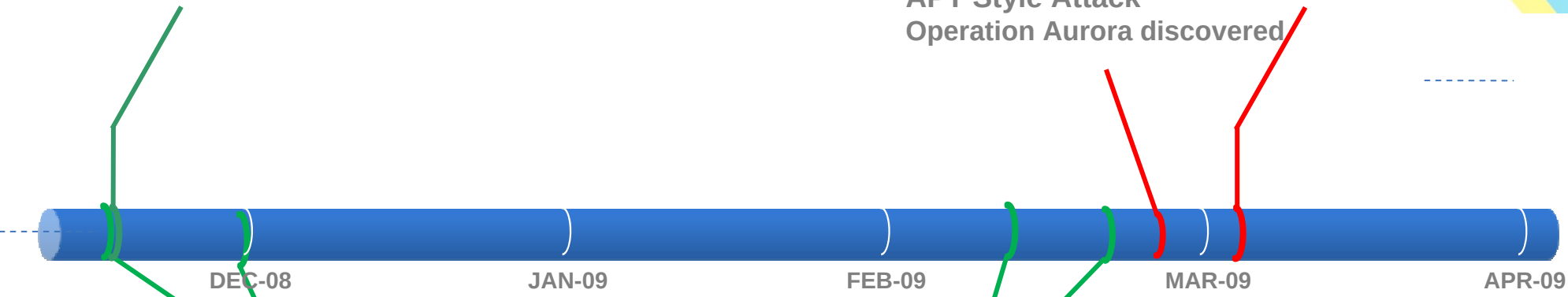
사례) Ahead of the Threat – Proven Technology

* Operation Aurora

2006
Pre-emptive "Behavioral" Decodes
Developed by X-Force

December, 2009
APT Style Attack
Operation Aurora discovered

Jan 21, 2010
Microsoft Issues Patch



Pre-emptive IBM X-Force coverage

Behavioral Decodes

Javascript_Shellcode_Detected
since Mar 28, **2006**

HTML_IE_Script_Error_Code_Execution
since Dec 13, **2006**

Pre-emptive IBM ISS coverage

Behavioral Decodes

HTML_Script_Extension_Evasion
since Jul 14, 2009

Javascript_Byte_Splitting
since Sep 8, 2009

Performance

- PAM v2.0
  - 재설계된 프로토콜 분석 엔진
  - 프로토콜 분석 처리 성능 개선
  - 선제적 방어 능력과 빠른 네트워크 성능을 제공
- 2011년 3월, 20Gbps 처리 성능의 GX7800 출시
  - 고성능의 처리 성능과 동시에 포괄적 보안을 제공하는 Research기반 위협완화 솔루션

GX7800

NEW

IBM Security Network IPS Models							
	100Mbps 환경	1~2Gbps 환경			4~20Gbps 환경		
Model	GX4004-V2-200	GX4004-V2	GX5008-V2	GX5108-V2	GX5208-V2	GX6116	GX7800
Inspected Throughput	200 Mbps	800 Mbps	1.5 Gbps	2.5 Gbps	4 Gbps	8 Gbps	23 Gbps+
Protected Segments	2	2	4	4	4	8	4

IBM Security Threat Mitigation Solutions

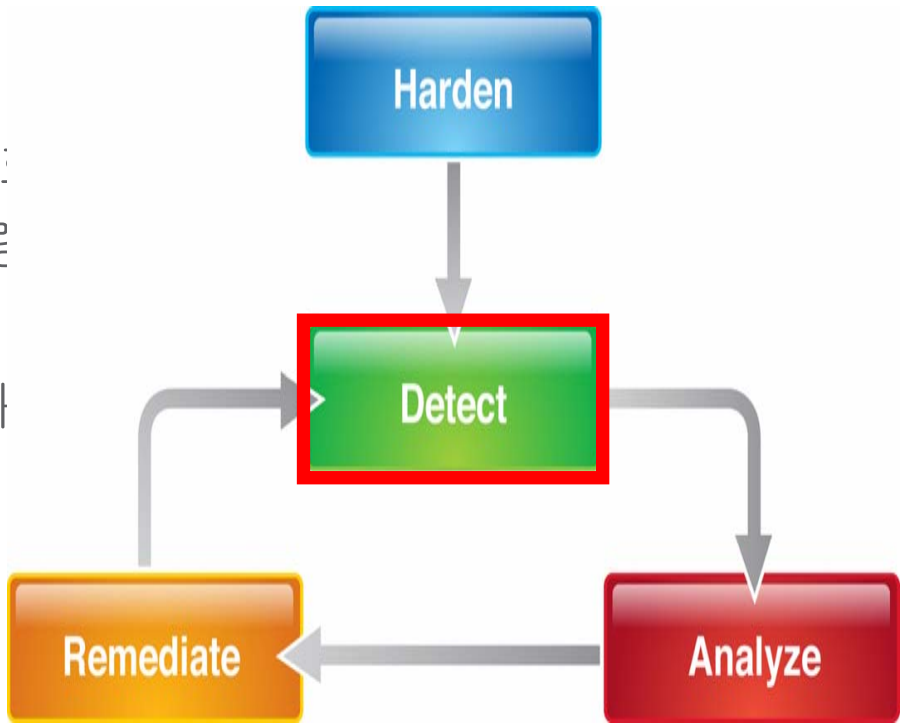
선제적 보안을 제공하는 다계층 방어엔진(PAM)을 탑재한 IBM 위협완화 솔루션

네트워크 인프라 보호	서버 보호	가상화 보안
IBM Network IPS	IBM Security Server Protection	IBM Security Virtual Server Protection for VMwsre

• 20Gbps 이상의 보안 성능 제공
• 침입방지를 통한 선제적 위협 방어
• X-FORCE 연구소의 지속적 업데이트
• 가상 패치(Virtual Patch)
• VoIP, IPv6, GTP, SCADA, DNS, 터널링 탐지, HTTP Compression, 가상화 인프라 보호
• 웹 어플리케이션 보호
• 데이터 유출 방지(DLP)
• 네트워크 정책 집행 및 모니터링
• Open Signature
	• Multi Platform 지원
	• Threat Protection
	  • 침입 방지(IPS)
	  • 방화벽(Firewall)
	  • Buffer Overflow Exploit 방지
	  • Application Control
	• System Integrity / Auditing
	  • Registry Integrity
	  • Data/File Integrity
	  • OS event/3rd part log Monitoring
	• Anti-Virus Compliance
		• 침입 방지(IPS)
		• 방화벽(Firewall)
		• 웹 어플리케이션 방어
		• Rootkit 탐지
		• 가상 NAC
		• 가상 인프라 Auditing
		• 가상 머신 자동 디스커버리
		• VM 이동 시 보안 정책 유지
		• 통합 관리 콘솔을 통한 정책, 로그 관리

APT에 대한 대응

- 사용자 교육 강화
- 물리적 Network Segmentation
- 현재 보안 상태 재점검 및 강화
  - 기 구축 보안 장비 강화
    (방화벽, IPS/IDS, WAP 등)
- 모니터링 강화
  - 내부 네트워크 Activity 모니터링 강
  - 서버 File/Registry Integrity 모니터링
- 이메일 보안 강화
- 네트워크 보안 및 엔드포인트 보안 강화
- 계정 권한 관리 시스템 강화
- SIEM



감사합니다.