Check Point
SOFTWARE TECHNOLOGIES LTD.

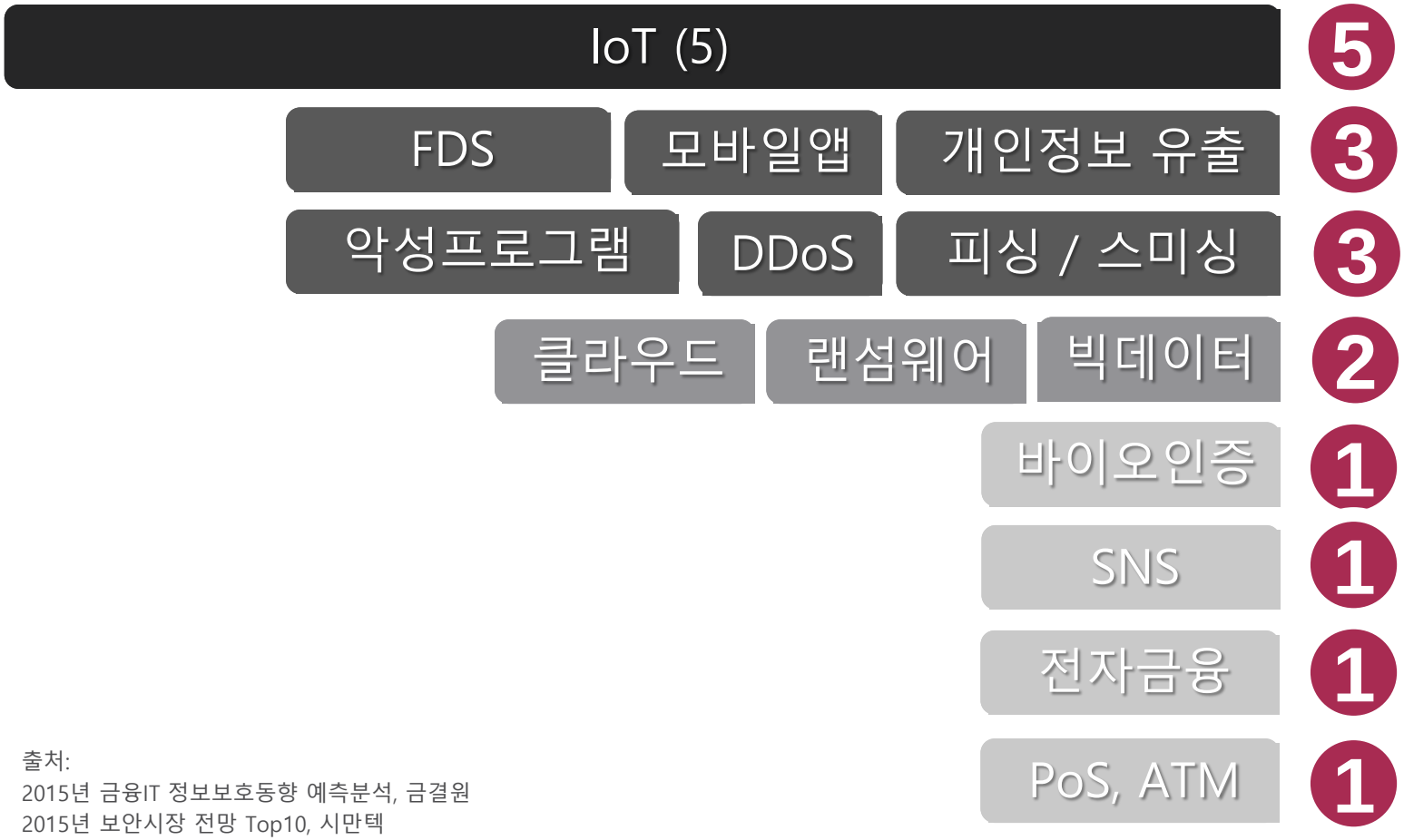
최신 보안 동향과 사례에 기반한 위협 방어전략

남인우 전무 | 기술총괄

2016. 4.

01
2016 정보보호 동향

2015 정보보호 동향



출처:
2015년 금융IT 정보보호동향 예측분석, 금결원
2015년 보안시장 전망 Top10, 시만텍
개인정보보호 트랜드정망 2015, KISA
2015 정보보호 10대 산업전망, KISA
2014년 사이버보안 침해사고 주요동향 및 15년 전망 분석, 미래부

2016 인터넷 분야 10대 이슈

2015년	2016년
오감(五感) 인지하는「**웨어러블 디바이스**」	금융 전 분야로 확산되는 「**핀테크 서비스**」
새롭게 쓰는 인터넷 금융의 역사 「**핀테크**」	서비스 플랫폼으로 확장되는 「**O2O***」
초연결사회의 하이웨이 「**기가인터넷**」	글로벌 ICT 위상 변화 「**친디아(Chindia)**」
디지털 금맥 찾기 「**데이터 사이언티스트**」	인터넷 비즈니스 팔방미인 「**드론***」
세계를 겨냥한 벤처 -「**글로벌 스타트업**」 약진	인터넷 新시장으로 부상하는 「**가상현실***」
생산의 고정관념을 바꾸는 「**3D 프린팅**」	비즈니스 허브로 진화하는 「**커넥티드카***」
미래인터넷의 지름길 「**오픈소스 생태계**」	똑똑해지는 가전, 「**스마트홈***」 시대 본격 개화
차세대 「**Neo 모바일 플랫폼**」 경쟁	생활형 서비스에 스며드는 빅데이터 기반 「**인공지능***」
「**중국 인터넷 기업**」과의 전략적 공존	웨어러블 기기를 통한 「**셀프케어족**」 증가
인터넷 인본주의의 시작 -「**인터넷 접근권**」	생산성의 혁신을 견인하는 「**산업용 사물인터넷(IIoT)***」

2016 정보보호10대 산업전망, KISA

"한국인터넷진흥원 (KISA, 원장 백기승)은 2016년에는 자동차, 제조등 전 산업 분야로 인터넷이 확산되고 (Internet on), 더불어 보안 위협도 전 분야로 확산되어 모든 산업에 보안이 내재化 (Security In)이 될 것으로 전망했다" - *2015.12.13 조간 보도자료*

2016 정보보호 10대 산업이슈 전망

2015년	2016년
IoT 실증의 관건 「**Embedded & Linked 보안**」	국민 안전을 위협하는 「**주요 기반시설 해킹**」
탐지도구도 속이는 「**악성코드의 고도화·지능화**」	新 냉전 시대의 서막, 국가간 「**사이버 갈등**」 심화
빅데이터 산업 성장 촉진제 「**개인식별정보 보안**」	공공부문의 「**클라우드 보안***」 중요성 증대
금융소비자의 안전 지킴이 「**비정상거래탐지시스템(FDS)**」	차세대 인증수단으로 부상하는 「**생체인증(FIDO)**」
개인 클라우드 서비스 확산을 위한 「**밀착형 클라우드 보안**」	금융·의료 등 전 산업에 적용되는 「**정보보호 관리체계***」
DNS, DDNS 겨냥한 「**표적화 DDoS공격**」	모바일로 확산되는 데이터 인질극, 「**랜섬웨어**」
사이버상의 국익분쟁 - 「**국가 간 해킹**」	「**개인정보 국외 이전***」 논의 본격화
「**선제적 공격 대응**」으로 전환되는 사이버戰	현실화되는 「**커넥티드카 해킹***」 우려
LTE급 「**지능형 사이버 사기**」	프라이버시의 새로운 위협 「**드론***」
스마트기기로 확산되는 「**바이오 인증**」	「**정보보호산업진흥에 관한 법률***」 본격 시행

2016 정보보호 분야 10대 이슈, KISA

2016 Top10 보안시장 전망

1. IoT 기기의 보안 이슈 확대
2. 애플 기기를 공격하는 사이버 범죄 증가
3. 랜섬웨어 범죄 집단과 악성코드 유포 집단의 경쟁 심화
4. ***모바일 앱*** 사용에 따른 프라이버시 침해
5. 주요 기간시설 겨냥한 공격 위험 증가
6. 암호화 필요성 대두
7. 생체인식 보안 본격화
8. 게임화와 시뮬레이션을 통한 보안 의식 제고

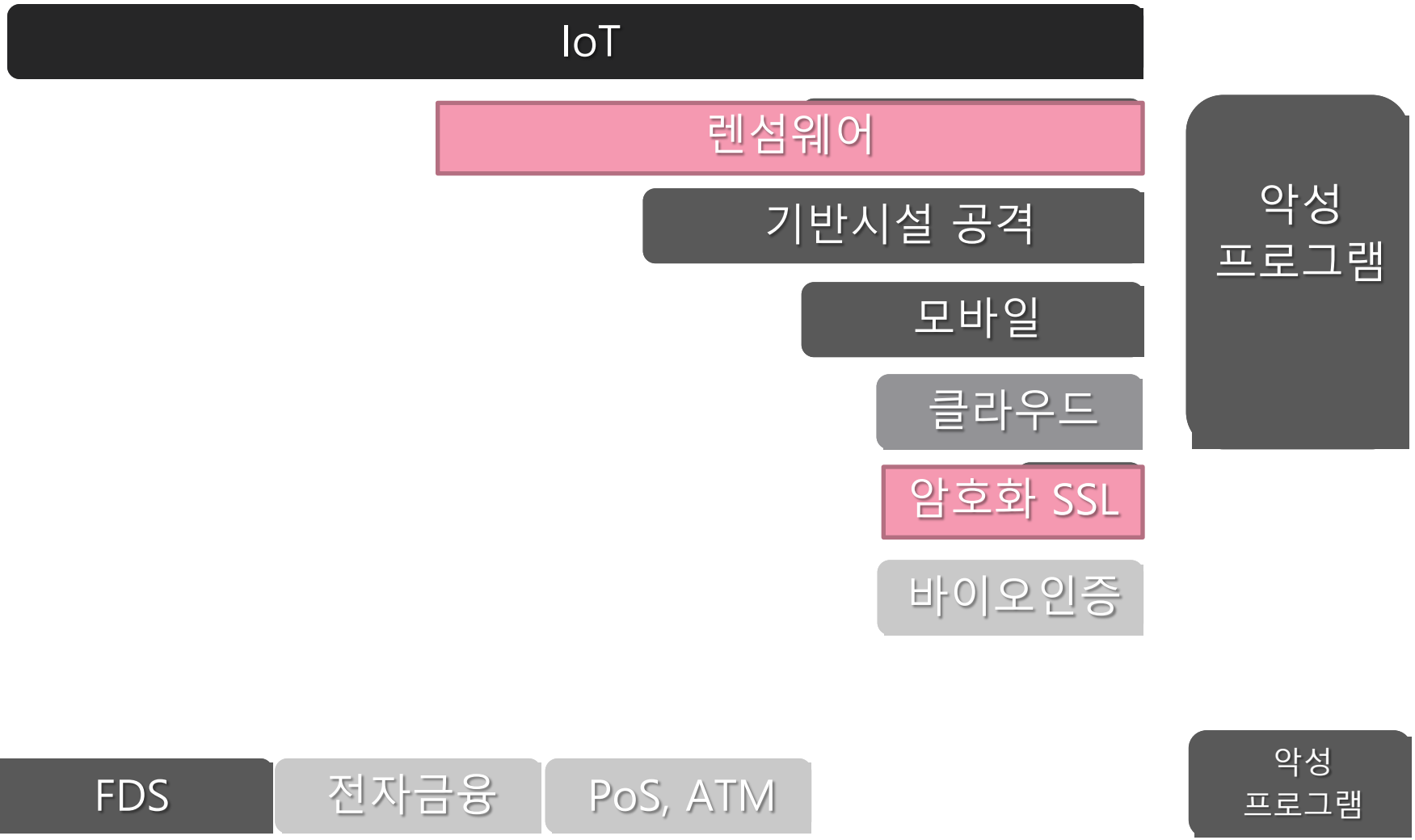
2016년 보안시장 전망 Top 10, 미 보안업체

2016 주목해야할 주요 보안사항

1. 클라우드 위협증가
2. 랜섬웨어의 확산
3. 암호와된 공격 (SSL)
4. 침해사고 대응체계
5. IoT (랜섬웨어)
6. 보안사고, 조직화된 범죄

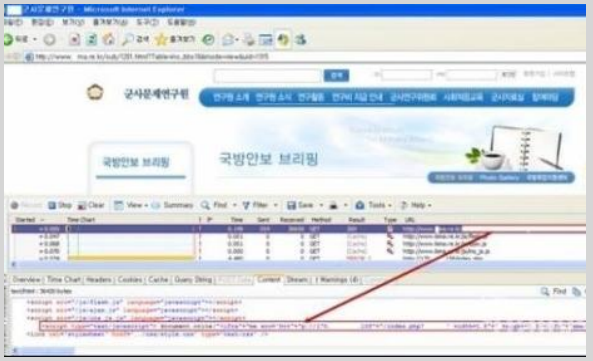
2016년 보안 업계에서 주목해야 할 주요사항, 미 보안업체

2016 정보보호 동향

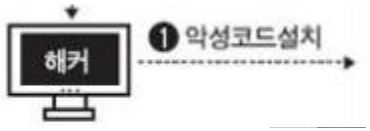


보안 이슈

감염



감염



공격 경로

30% MORE
웹 기반 공격

42% MORE
타켓형 사이버 공격

58% MORE
모바일 악성 코드

125% MORE
소셜 미디어 피싱 사이트

사례1

Check Point
SOFTWARE TECHNOLOGIES LTD.

	2013년 3월 20일. KBS,MBC, YTN, 신한, 제주, 농협
	2012.6 ~ 2013.1
C&C	Drive-by-Download
Known C&C	49 C&C 서버중 (국내 25개, 해외 24) 22개 (국내 18, 해외4)가 2009년 이후 발견된 악성 site와 일치
Known Malware	악성코드 76종 중 30종이상 재활용

사례2

2015년: 5만 3천명, 천억이상, 해외유출 3백만 달러 이상

2016년 15만명, 3천억이상, 9백만불이상

비트코인

C&C

Drive-by-download: 40%이상

Web / Mail

인터넷: 67%

이메일 첨부: 25%

어플리케이션 제어.

P2P / IM : 8%

방어전략

C&C

- "구글은 전 세계 10억개 URL을 분석해 매주 보고를 보여주고 있는데, 약 10만개 악성 URL을 보고한다. 그리고 악성 URL은 수시로 바뀌고 있다."
- Anti-Bot / Global Reputation


Anti-bot

Known Malware

- Anti-virus
- IPS


IPS


Antivirus

Web Mail

- 이메일은 물론 인테넷을 직접 통한 파일 접근에 대한 대책
- 실시간 차단 > 탐지


Web Security


Threat Emulation


Anti-Malware

어플리케이션 제어.

- NGFW


Application Control

SSL


IPSec VPN

Unknown Malware

- 샌드박스


Threat Emulation

샌드박스

샌드박스

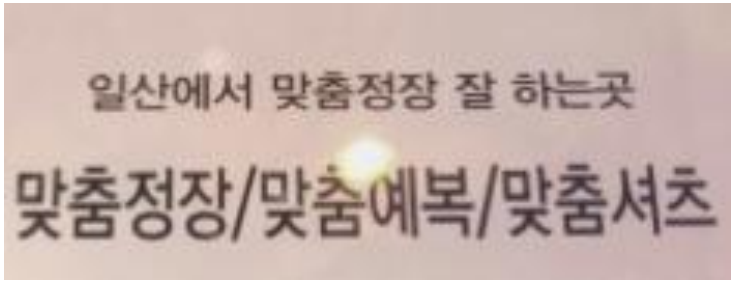
"By 2018, 85% of new deals for network sandboxing functionality will be packaged with network firewall and content security platforms"

Gartner on Threat… (Feb 2015)

샌드박스 우회

우회로

(기본값)	REG_SZ	(값 설정 안됨)
CoInstallers32	REG_MULTI_SZ	vmx_mode.dll, VMX_ModeChange
DriverDate	REG_SZ	2-17-2012
DriverDateData	REG_BINARY	00 c0 65 17 07 ed cc 01
DriverDesc	REG_SZ	VMware SVGA II
DriverVersion	REG_SZ	11.9.1.0
InfPath	REG_SZ	oem11.inf
InfSection	REG_SZ	vmx_svga
MatchingDevic...	REG_SZ	pci₩ven_15ad&dev_0405&subsys_040515ad&re...
ProviderName	REG_SZ	VMware, Inc.



우회로 대비

역이용

舊官이 名官

M2M

협업

유아독존

낮선길

원천제거

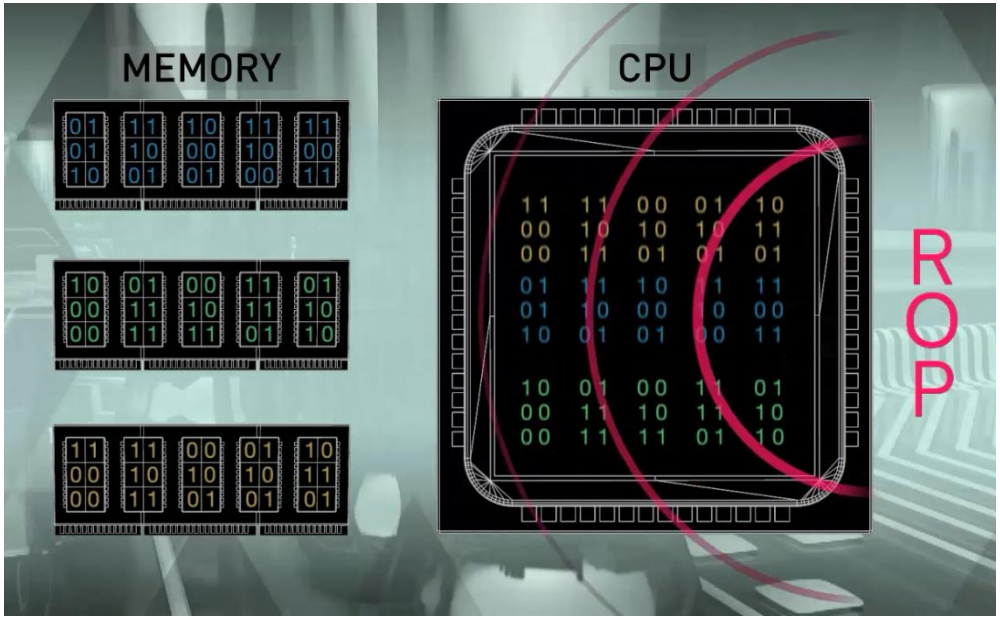
Check Point®
SOFTWARE TECHNOLOGIES, INC.

1. 가상화 샌드박스

다중 OS 환경

동적 행위 모니터

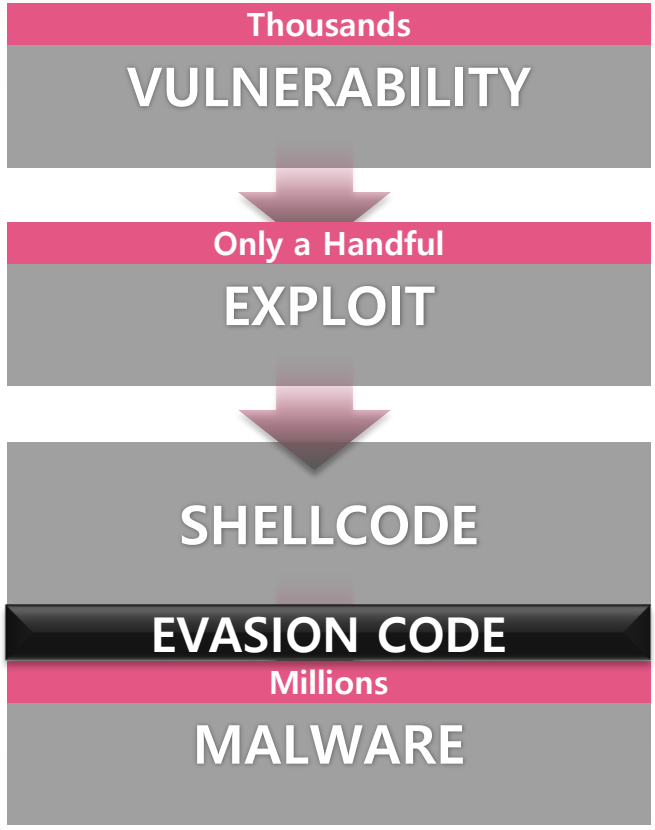
2. CPU-Level 샌드박스



	체크포인트 CPU-Level 위협방어	기존 샌드박스
샌드박스 우회 기법에 대비	YES	NO
OS에 관계없는 탐지	YES	NO
실시간에 가까운 탐지속도	YES	NO

2. CPU-Level 샌드박스

2. CPU-Level 샌드박스



CHECK POINT SandBlast™ ZERO-DAY PROTECTION

Traditional Sandbox

3. 문서 재조합

원본문서

문서 재조합

멀웨어의 원천 제거

CHECK POINT

THREAT EXTRACTION

클라우드

THREATCLOUD

2억 5천만개 이상의 봇을 발견, 분석
1천 1백만개 이상의 멀웨어 시그니처
2천 7백만개 이상의 멀웨어 감염 탐지

체크포인트의 방어전략

모바일 샌드박스

체크포인트

수준 높은
보안 경력
22 Years

복잡한
환경 구성 지원
100,000
Customers

글로벌 지원
88 Offices

가트너 Magic Quadrant – 네트워크 방화벽, 2015

1993년 창사. 1996년 IDC에 의해 Firewall Leader로 선정

18년간 'Leader'의 위치에 놓인 유일한 회사

Check Point
SOFTWARE TECHNOLOGIES LTD.

감사합니다