이메일 APT 선제대응을 위한
메일보안 고도화 전략

2015. 04. 16

연구소장 고 필 주

지란지교시큐리티

Agenda

1. 메일보안 시장의 재점화
2. 통합 메일보안 필요성
3. 메일보안위협 동향과 APT
4. 메일보안 구축을 위한 제언

2014년 주요 보안사고

원전 도면, 한수원·협력업체 이메일에서 유출

'피싱'으로 업무용 메일 아이디·비밀번호 빼돌려…개인정보범죄 정부합동수사단

(서울=뉴스1) 홍우람 기자 | 2015.01.21 12:38:10 송고

기사보기 | 네티즌의견 | 좋아요 | 공유하기 | 0 | 트윗 | 0 | 인쇄 | 확대 | 축소

서울 강남구 한국수력원자력 본사 © News1 박지

지난해 말 인터넷에 유포된 한국수력원자력의 원전 도면 자료 일부는 한수원 이메일에서 유출된 것으로 조사됐다.

개인정보범죄 정부합동수사단(단장 이정수 부장검사)은 유출범 ~9월 이른바 '이메일 피싱' 수법으로 원전 도면 등 자료를 빼낸

뉴스
SW/보안

소니 해킹 피해, 이정도 였을 줄이야

데이터 유출만으로도 금전 피해 1880억원…전대 미문 해킹 사건으로 기록

성상훈 기자 | HNSH@ittoday.co.kr

승인 2015.01.04

왜 이메일일까?

중요하다

80%

가장 중요한 업무 커뮤니케이션툴로
'이메일'을 꼽은 답변 비중

아는 사람

협력업체 혹은 신뢰하는 사람/기관
주소에서 발송된 메일은 의심 X

쉽게 신뢰한다

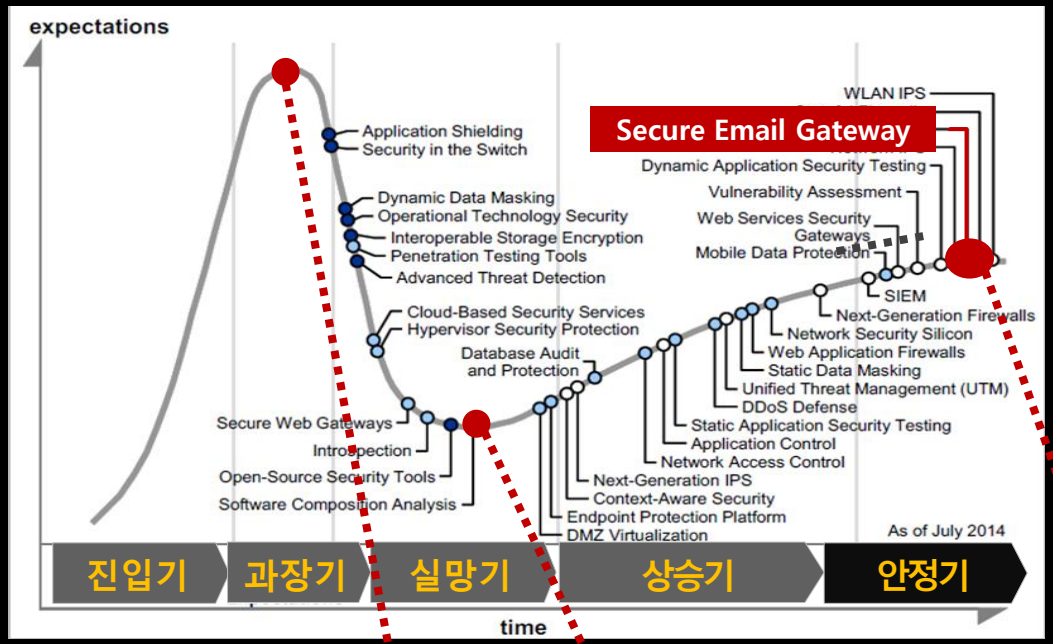
구글링

이름, 소속, 도메인만 검색해도
쉽게 이메일 주소 입수 가능

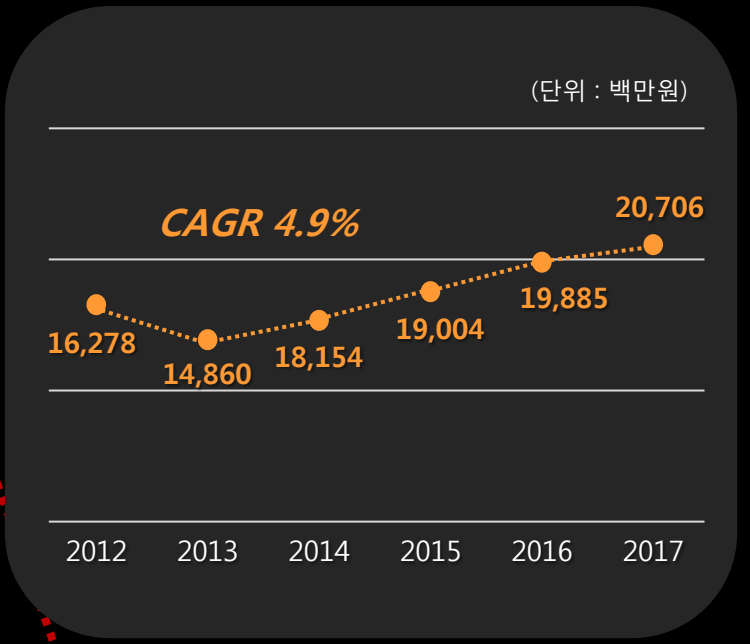
쉽게 얻는다

메일보안의 재점화

'인프라보안' 관련 솔루션 기술성장곡선, 2014



국내 스팸차단 SW 성장률



2000년대 초반

스팸메일차단SW '우후죽순'

e메일 업그레이드 열풍.. 스팸·바이러스차단 시스템 잇따라 출시
한국경제 | 기사입력 2002-02-17 17:43 | 최종수정 2002-02-17 17:43

스팸방지 시장에 돈 몰린다
디지털타임스 | 기사입력 2003-06-13 02:57 | 최종수정 2003-06-13 02:57

2000년대 중후반

국내 스팸차단SW시장의 포화

스파이웨어 창궐...스팸은 감소
아이뉴스24 | 기사입력 2004-11-05 18:11 | 최종수정 2004-11-05 18:11

스팸메일 절반으로 '뚝'...2년 연속 50% 감소세
아이뉴스24 | 기사입력 2004-12-29 18:48 | 최종수정 2004-12-29 18:48

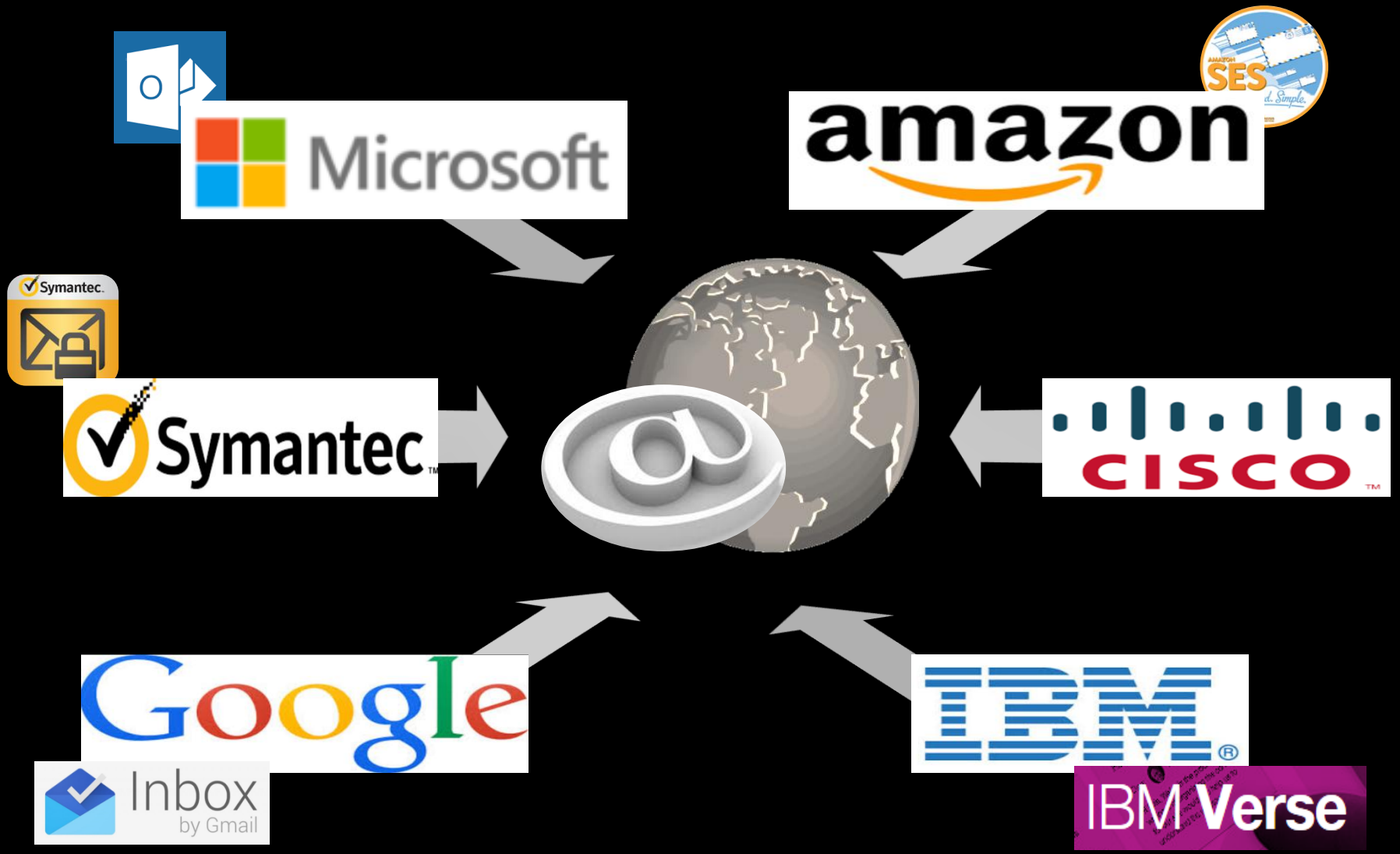
2010년대

메일보안 시장 재점화

시만텍, 이메일 보안 서비스 시장 공략 본격화
이메일 바이러스 100% 스팸 99% 차단 보장

홈 | 컴퓨팅 발행일 2013.12.16 | 트윗하기 보내기
, 보안메일 솔루션으로 보안 사업 강화

‘이메일’ 시장을 향한 기업들의 움직임



이메일 보안 강화 움직임

[정치] '성장동력' 산업 기밀이 샌다

게재 일자 : 2015년 01월 30일(金)

防産·금융·전자업체 직원 메일 '1차 표적'

개인정보 해킹뒤 기밀 빼내… 보안 허술한 협력社도 타깃

구글 지메일 보안정책 강화, 잠재 위험 내포한 애드온 차단 실시

2014/12/18 13:54:54

좋아요 1 공유

구글, 크롬용 메일 암호화 솔루션 '엔드투엔드' 소스코드 공개

2014.06.04 21:50:44

야후 "이메일 암호화 하겠다"..보안 강화 목적

입력시간 | 2014.08.09 10:01 | 김유성 기자 kys401@

세계 인터넷 및 이메일 보안 시장 분석 보고서

2017년 예상 이메일 보안 시장 규모

33억5천만 달러 (약 3조7천억원)

이메일 보안 우려 3요인

- 어플리케이션 취약
- 대처방법
- 모바일 기기

* 프로스트 앤 설리번, 2013

이메일 관련 정보보안 컴플라이언스

정보통신망법	정보통신망 이용촉진 및 정보보호 등에 관한 법률 개인정보의 기술적, 관리적 보호조치 기준 정보보호 관리체계 인증 등에 관한 고시
개인정보보호법	개인정보의 안정성 확보조치 기준 표준 개인정보 보호지침
전자금융거래법	증권회사 영업행위준칙해설 금융회사 정보기술(IT) 부문 보호업무 모범규준 금융회사 정보처리 및 전산설비 위탁 관한 규정 전자금융 감독규정
산업기술보호법	산업기술의 유출방지 및 보호에 관한 법률
기타	내부회계 관리제도 (K-SOX) 방문판매법 (금융권 모바일오피스 관련)

이메일 수신, 발송, 저장 모두 법적 규제 有

- 개인정보 분실·도난·유출·변조
  매출액 3% 이하 과징금
  (2014. 11월 시행)
- 전자금융거래 기록
  유출시 50억 이하의 과징금
  5년 보존 위반시 천만원 과태료
  (2015. 4월 시행)
- 금융회사 정보기술(IT)부문 보호업무 中
  이메일 등 비금융 전산시스템
  취약점 분석·평가 대상 포함
  (2014. 6월 시행)

WHY

메일보안, 왜 해야 하는가

메일 통한 외부위협의 증가

전세계 일일 스팸 발송량

290억건
전체 이메일 중 66%

국내 스팸메일 비중

60% 이상
메일유형 변형 지속
(스팸 → 악성)

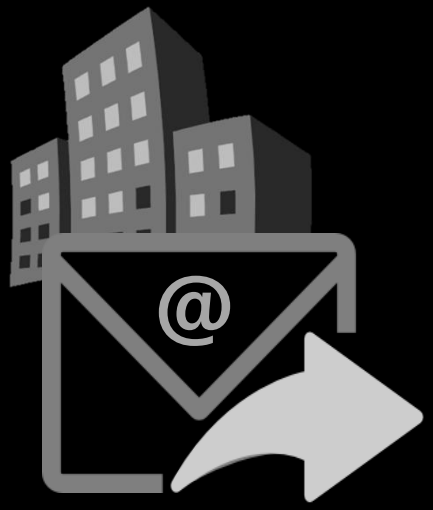
APT 공격 통로

스피어피싱 이메일
90% 이상

미래부, '15년 전망

악성코드 유포채널
홈페이지 → 이메일
중심으로 변화

메일 통한 내부유출의 증가



기업데이터 유출 통로

1위 이동식저장장치
2위 E-mail

기업 데이터 유출경험

아시아 기업 中
65% 이상

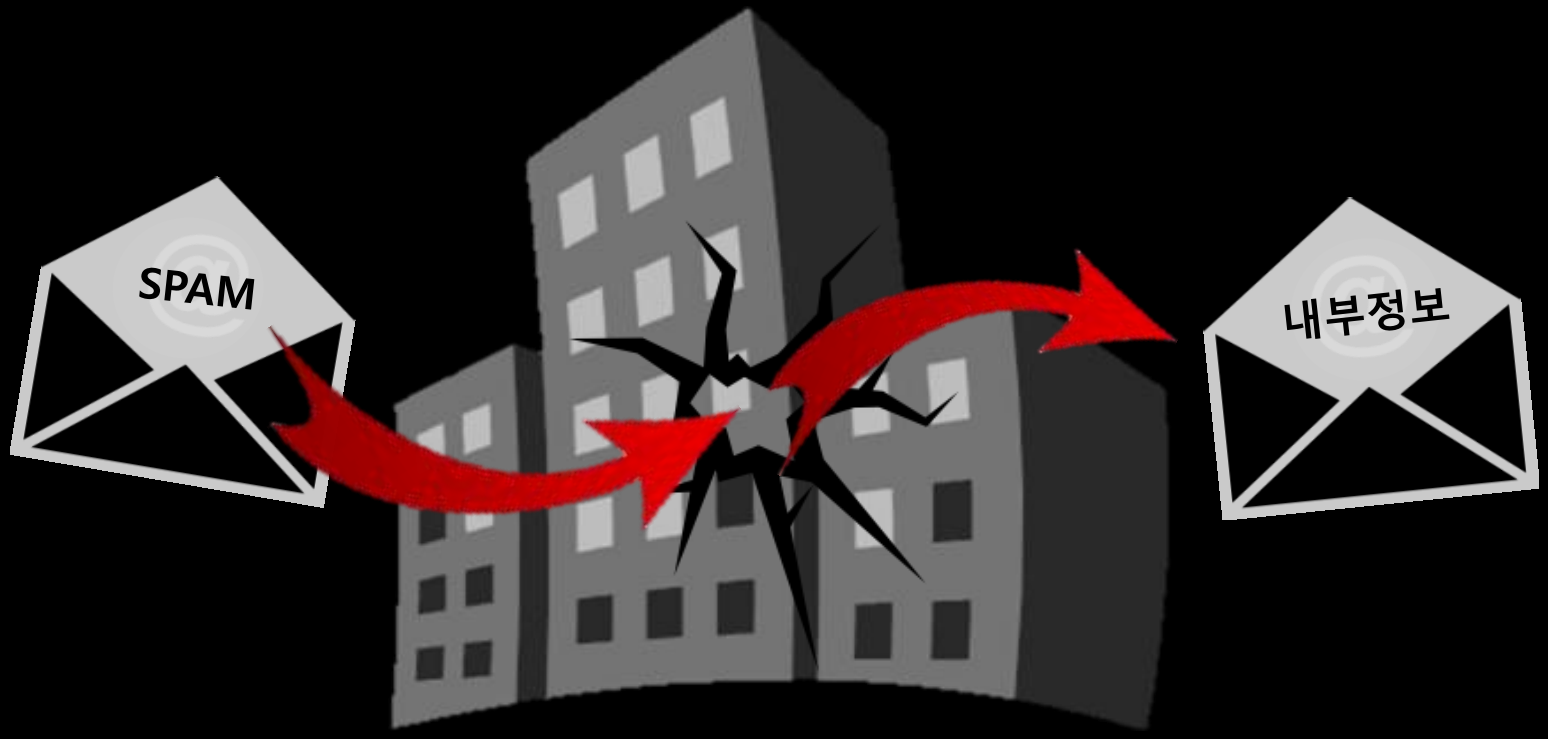
데이터유출로 인한 피해

약 60억원
유출 건당 손실액

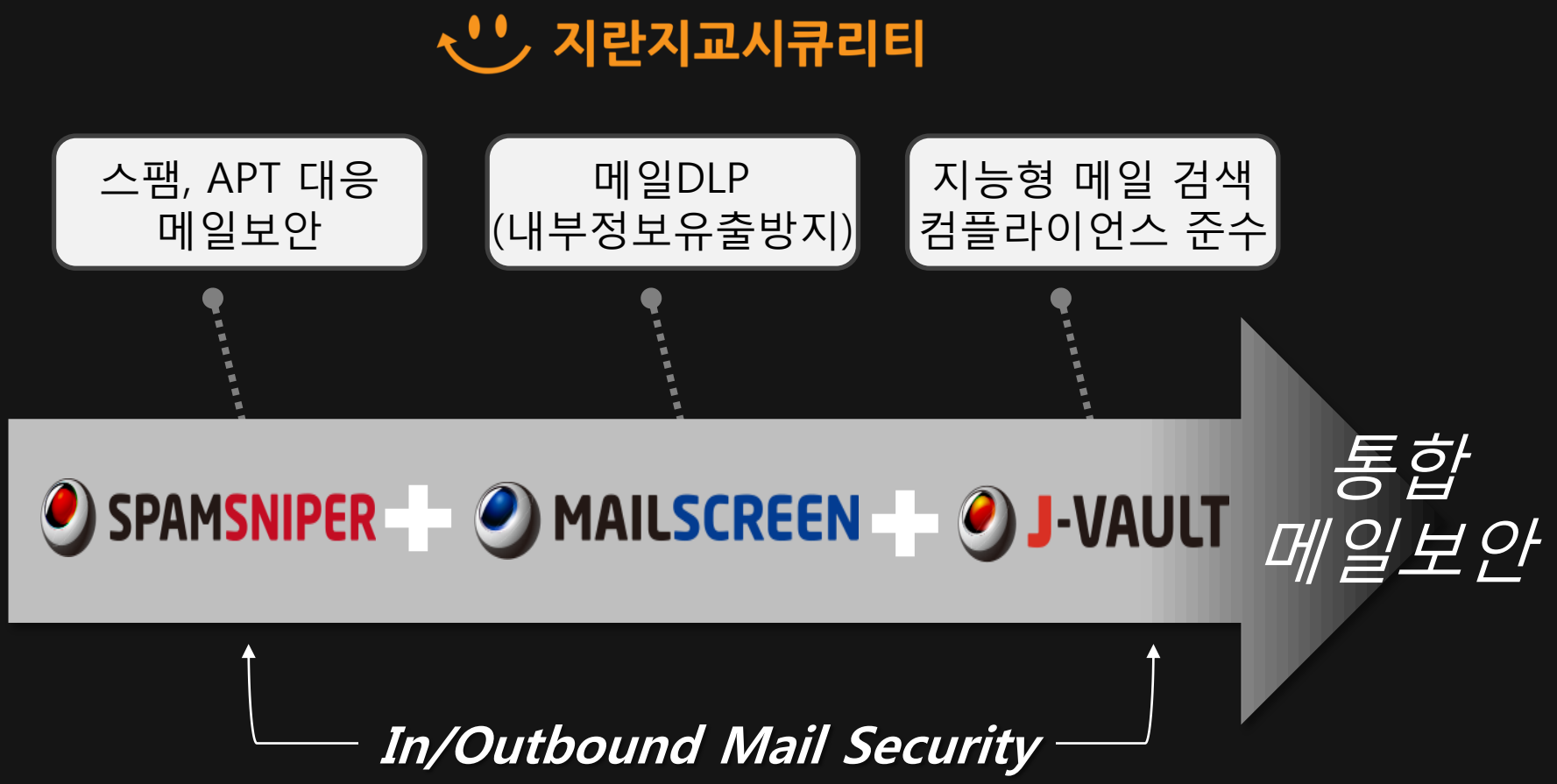
기업데이터 유출사고 주체

80% 이상
내부 임직원

메일은 '안팎으로 통하는 채널이자 구멍'



JiranSecurity 통합메일보안 라인업

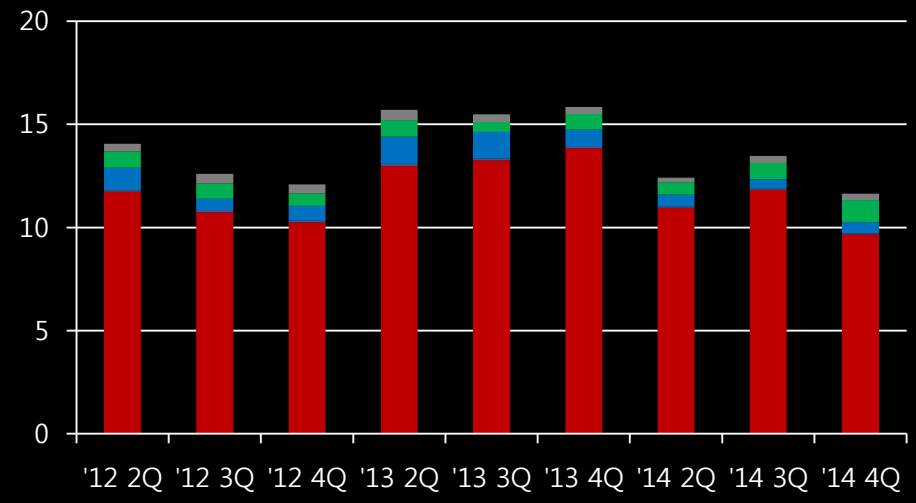


HOW

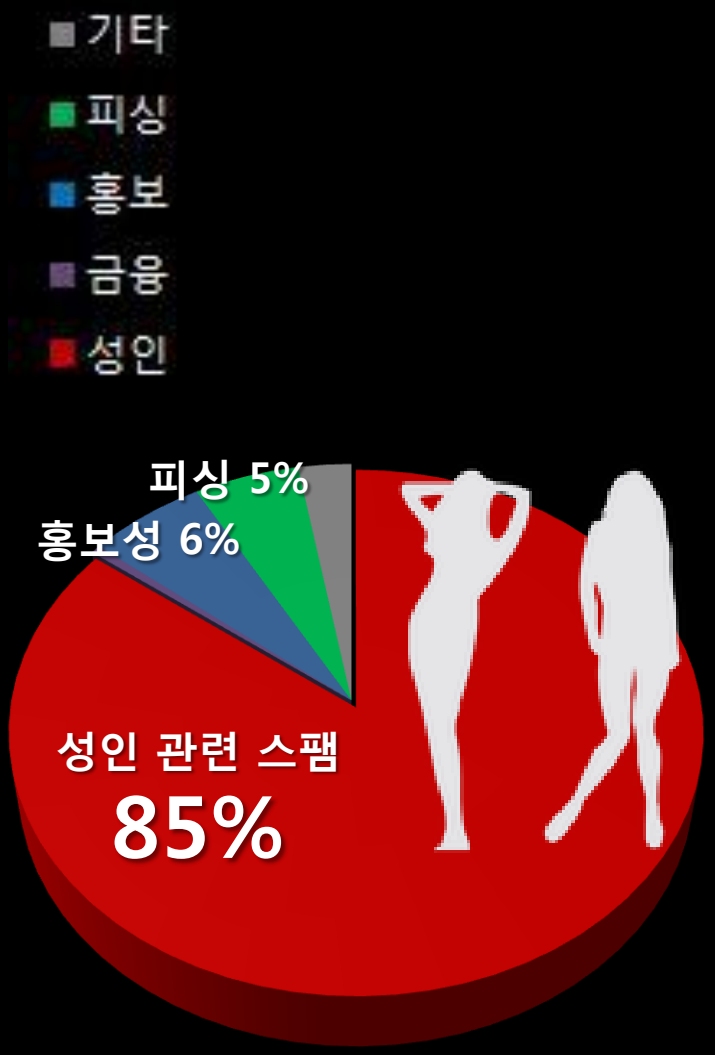
메일보안, 어떻게 해야하는가

메일보안 위협 최신 동향

'12-'14년 3개년 스팸메일 유형 비중



(단위 : 억건)



(2012~2014) 3개년 스팸유형 비중

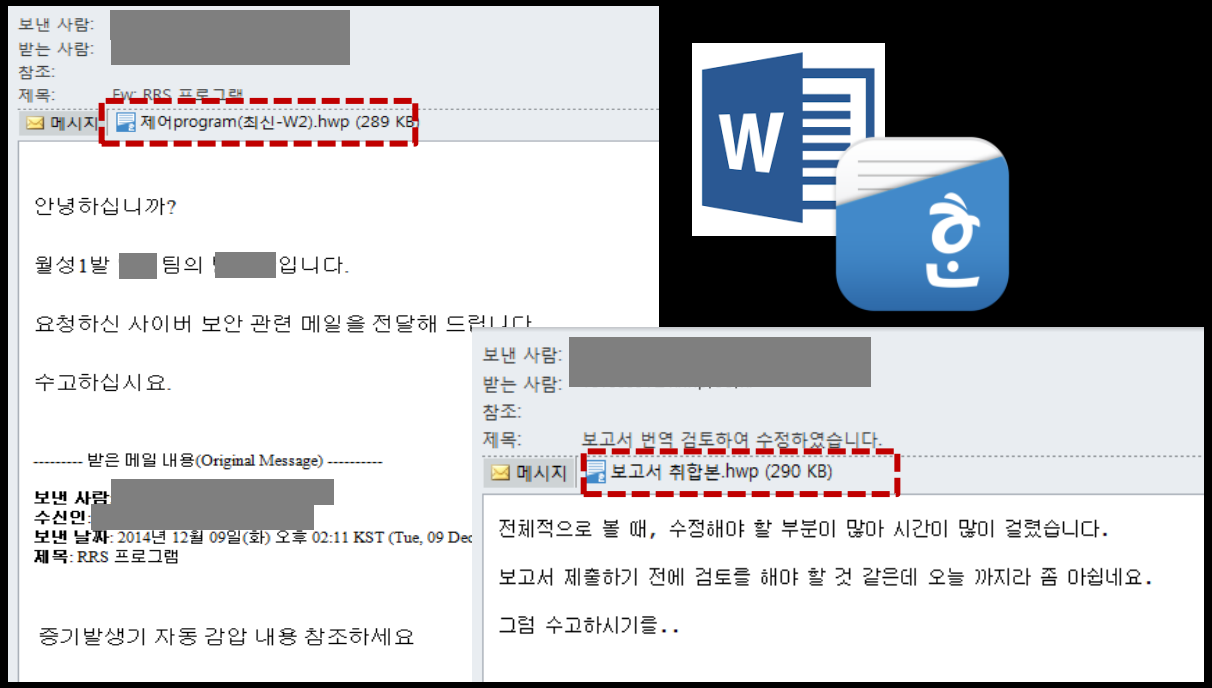
메일보안 위협 최신 동향

2012년	*2013년*	*2014년*
Facebook, 링크드인 SNS 서비스 악용	카드명세서 등 금융권 가장 악성코드	공기관, 소니픽처스 특정 타겟/ 장기간 준비
TEXT 중심 → 이미지화	알림, 보안업데이트 등 사칭 악성코드	지능화·고도화된 스피어피싱 스팸

메일보안 위협 최신 동향

#1 국내 관공서

첨부파일을 통한 악성코드 메일

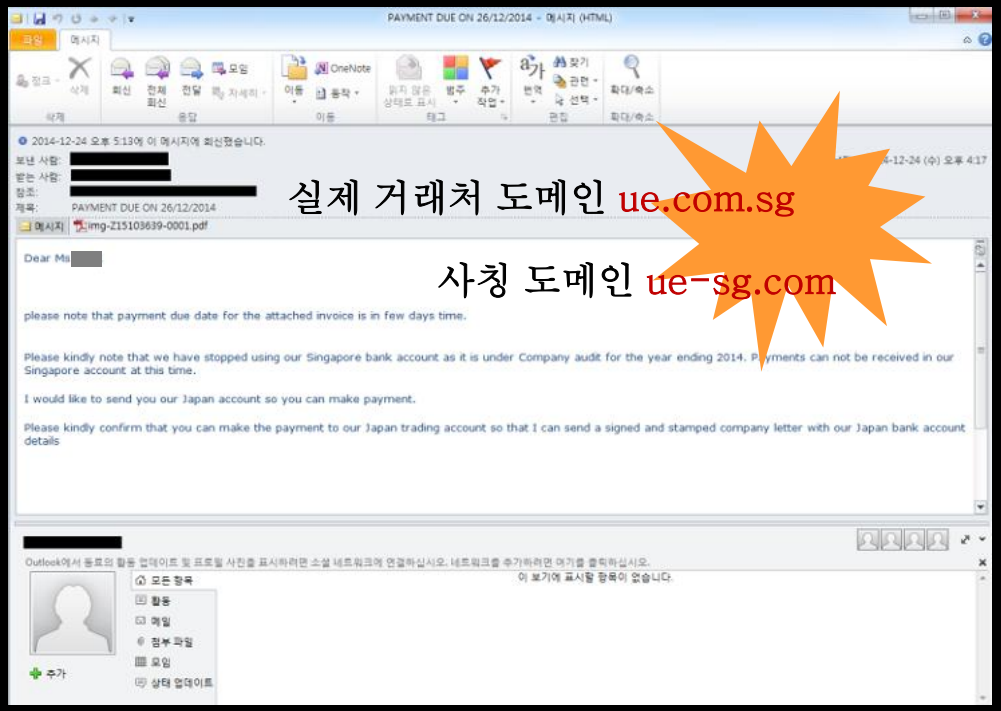


- 한글(hwp), 워드(docx) 등 Office 솔루션들의 취약점을 노린 악성 첨부파일, 다운로드 유도
- 첨부파일 실행시 악성코드 통한 사용자 PC 시스템 공격, 강제 종료 등 치명적인 피해

메일보안 위협 최신 동향

#2 국내 대기업 계열사

거래처 사칭 피싱 메일

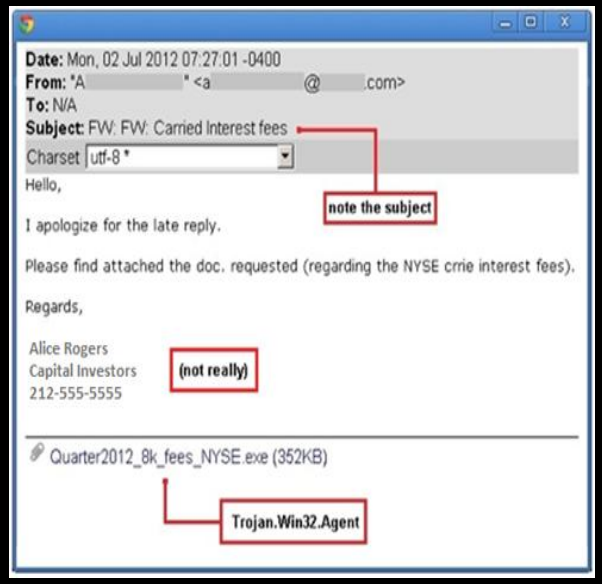


- 기존 거래처 유사 도메인 및 업무 내용으로 입금계좌 변경 요청
- 기존의 업무 패턴, 진행사항 지속 분석한 치밀한 피싱 메일

메일보안 위협 최신 동향

#3 랜섬웨어

개인정보, 금전적 탈취를 노린 랜섬웨어 배포



- 목표 달성까지 특정 문서, PC의 사용을 막아버리기 때문에 사회적인 손실로 이어짐

메일보안 위협 최신 동향

2013~2014년 글로벌 주요 APT 사례

- Operation "Red October" (동유럽, 중앙아시아 대상)
- 뉴욕 타임즈 APT 해킹
- Operation Hangover 인도 정부 기관 해킹
- **3.20 전산 대란, 언론 및 기업 마비**
- 온라인 게임사 해킹 (Winnti 해킹조직)
- **6.25 사이버 테러 국내 주요 정부 기관 공격**
- **Icefog (Hidden Lynx) 한·일 정부, 민간기관 해킹**
- Operation Ke3chang 유럽 외교통상부 해킹
- 소니픽처스 APT 해킹

이메일 통한 APT 공격 사례 지속, 타겟층 확대

메일보안 위협 최신 동향

APT 공격 라이프 사이클

공격대상 정의 → 악성코드 제작 or 구매 → 공격 대상 연구 → 악성코드 진단 테스트 → 공격대상 내부 감염 → 거점 확보 → 내부 시스템 탐색 → 데이터 탈취 → 잠복 or 흔적 제거

주요 APT 공격 대상


정부기관


기간산업시설

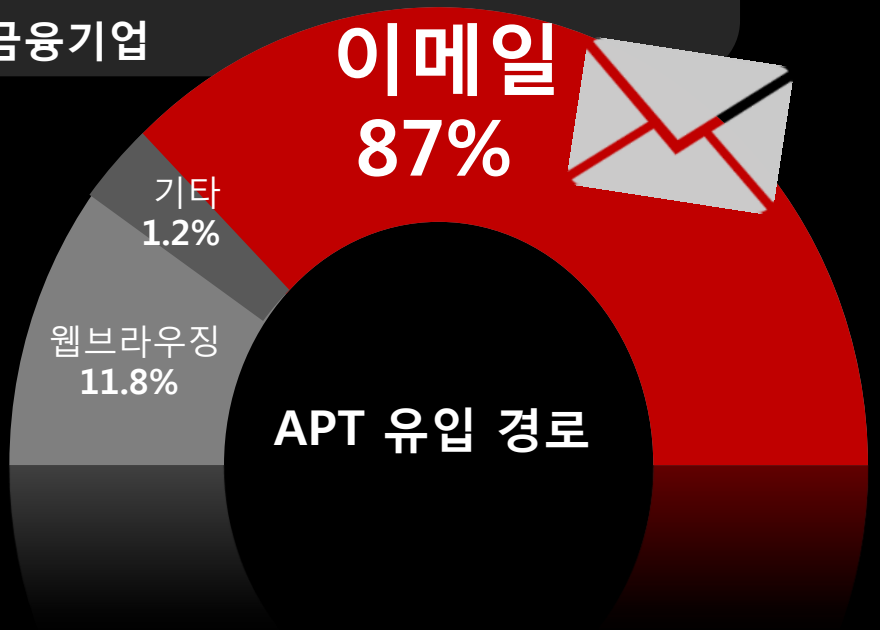

제조기업


정보통신기업


금융기업

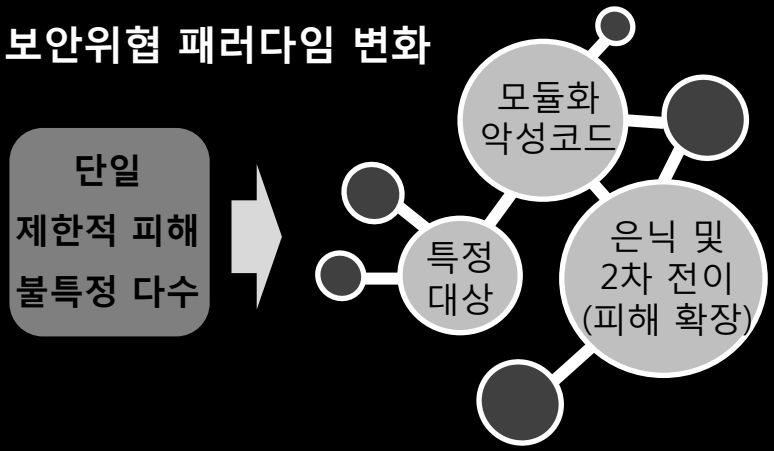
- 금융 시스템 작동 불능
- 기업 금융자산정보 탈취

(출처 : 팔로알토네트웍스, 전자신문)

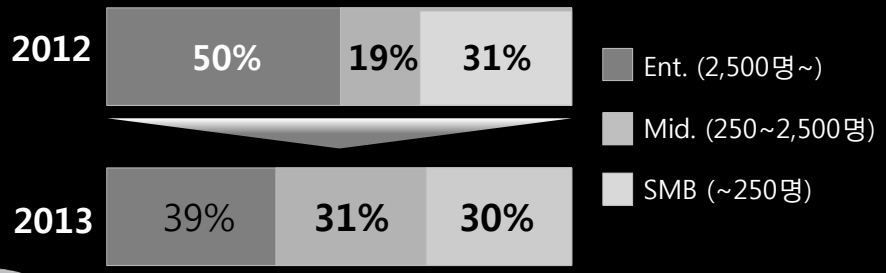


메일보안 위협 최신 동향

보안위협 패러다임 변화



스피어피싱 타겟층 확대



Advanced Persistent Threat

"6.25 사이버테러 1년, 국내 APT 대응 여전히 미흡"

입력시간 | 2014.06.24 14:54 | 김관용 기자 kky1441@

APT 공격 증가하는데…국내 APT 인식 낮아 시장 성장 정체

등록일 2014.06.24 17:30:04 | 추천 2

파이어아이, "한국, 美 이어 세계 2위 APT 공격타깃국가"

국내 APT 대응은
아직 '걸음마' 수준

메일보안 고려 요소

* Gartner 분석 참고

SpamSniper APT Edition 확장

SpamSniper APT Edition 확장

APT EDITION.

SpamSniper APT Edition 라인업

APT Edition

APT Smart

- SpamSniper +

  APT 의심메일 Alert, 메일안전보기 (스크립트 실행 차단)

APT Premium

- SpamSniper + 전문 APT솔루션 연계
- 어플라이언스형

APT Cloud

- SpamSniper + 클라우드
- 지란지교시큐리티 IDC 내 APT 분석서버 구축

SpamSniper APT Edition 강점

기술력

국내외 No.1 메일보안 시너지

MVX 기반 메일APT 분석·대응

다수 샘플 기반 강력 필터링

안정성

안티스팸SW 최다 레퍼런스

국내 메일환경 운영 노하우

24/365 기술지원·패턴 업데이트

공신력

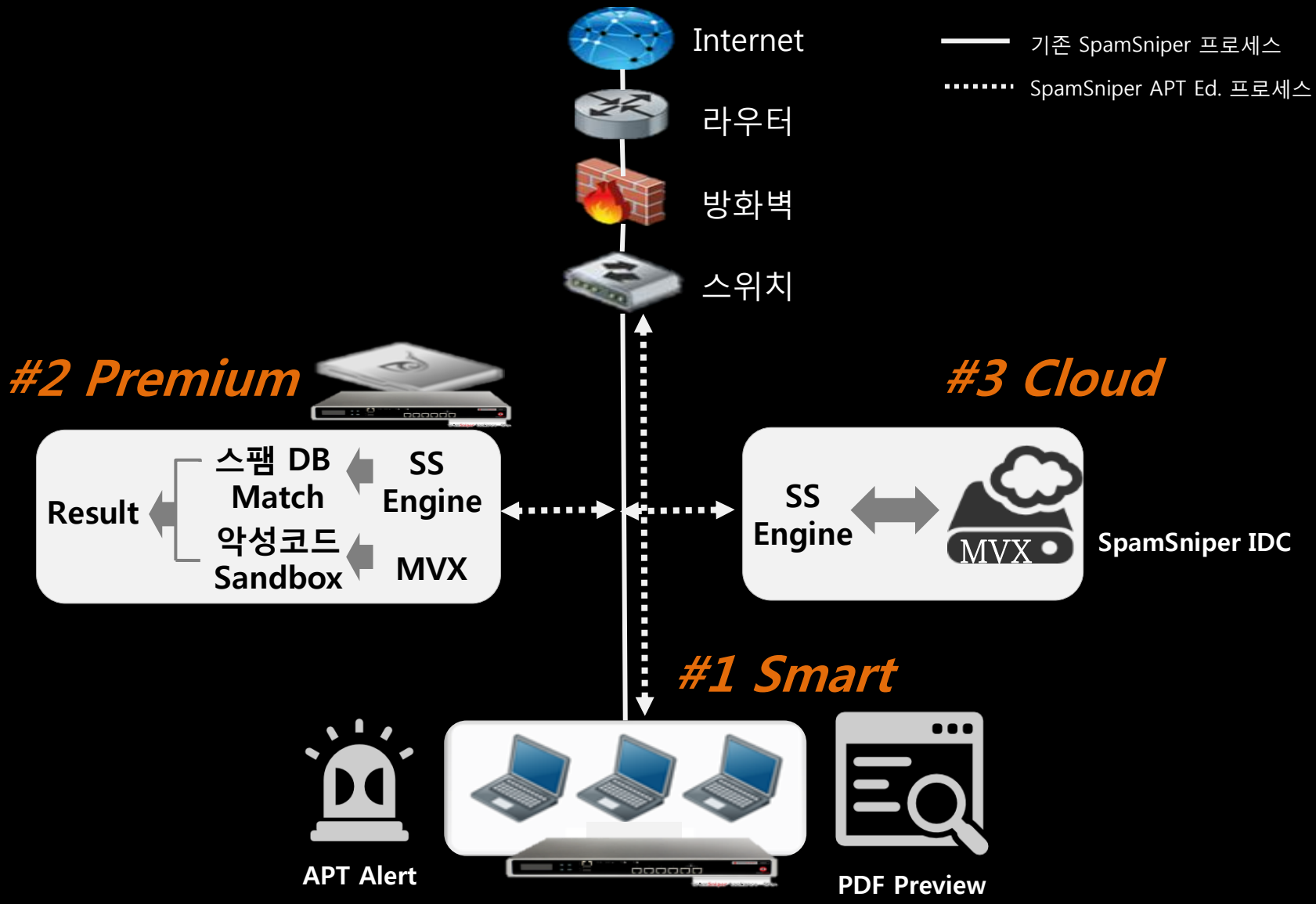
Anti Spam/APT Lab 운영
(KISA 연계 스팸리포트 발행)

일본시장 누계매출 20억원

FireEye 전략적 기술제휴 체결

SPAMSNIPER *APT Edition*

SpamSniper APT 구조도



All Roads to the Digital Future
Lead Through "Security"

Gartner 2014

정보보안, 보안의식 확립에서 시작합니다

메일보안 악순환의 고리, 이제는 끊어야 할 때

감사합니다.