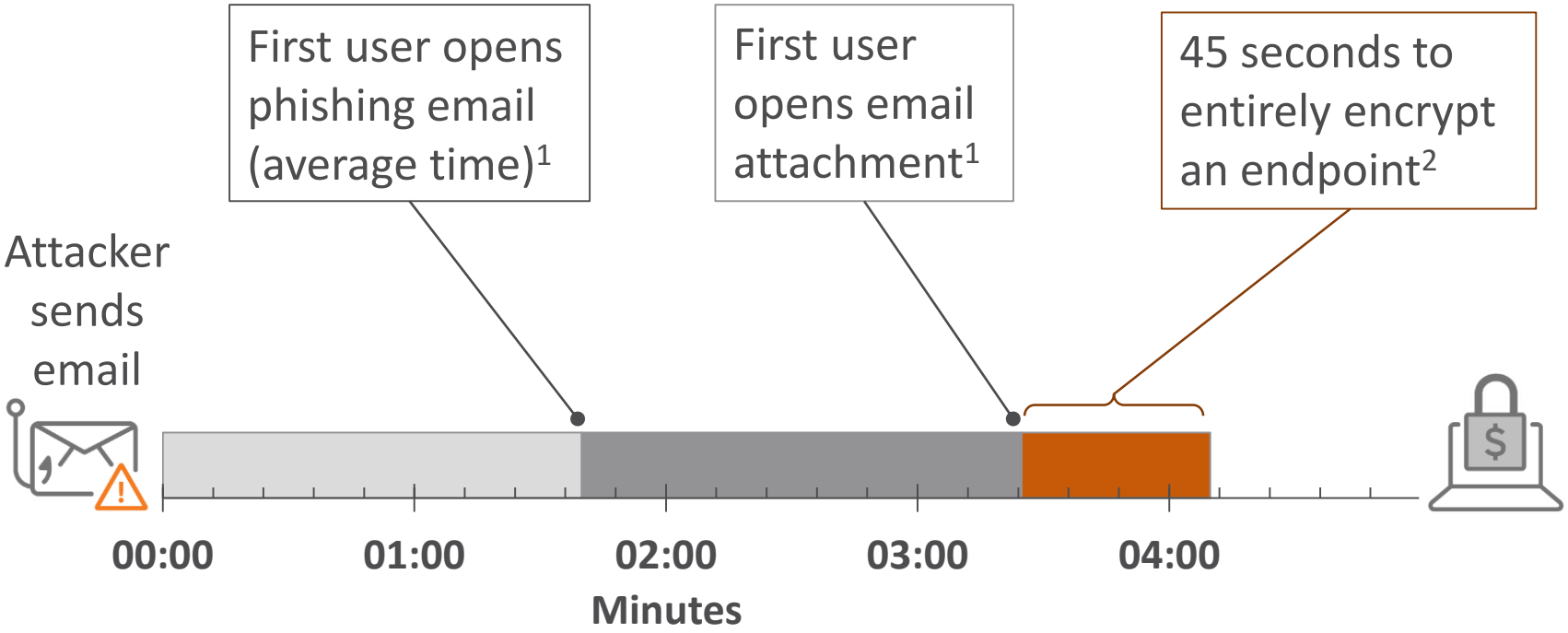
변화하는 위협에 대응하는 이메일 보안

2018/1/24

79% 랜섬웨어 공격은 피싱 이메일을 사용



1. Verizon 2016 Data Breach Investigations
2. Teslacript 3.0

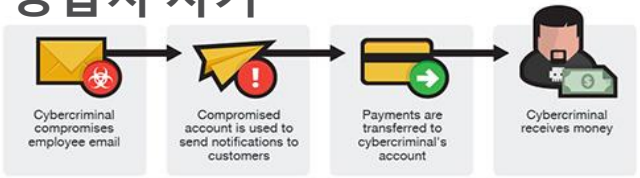
Business Email Compromise (BEC, 비즈니스 이메일 위협) 공격

- **글로벌 $5B** 가치의 손실
- 사기 건 당 평균 **$132,000** 손실

Difficult to detect – no attachment/URL

CEO Fraud

공급자 사기



계정 손상

조직 내부의 공격자:
신뢰할 수 있는 사용자의 내부 피싱 이메일

Employee A
손상된 장치 또는 이메일 자격증명

Employee B

이메일 게이트웨이 보안은 내부 메일을 볼 수 없다!

LOA

GL

Monday, 13 March 2017 at 8:01 PM
To: Transfer, Wire
: Wire Instruction.pdf (12.6 KB) Preview

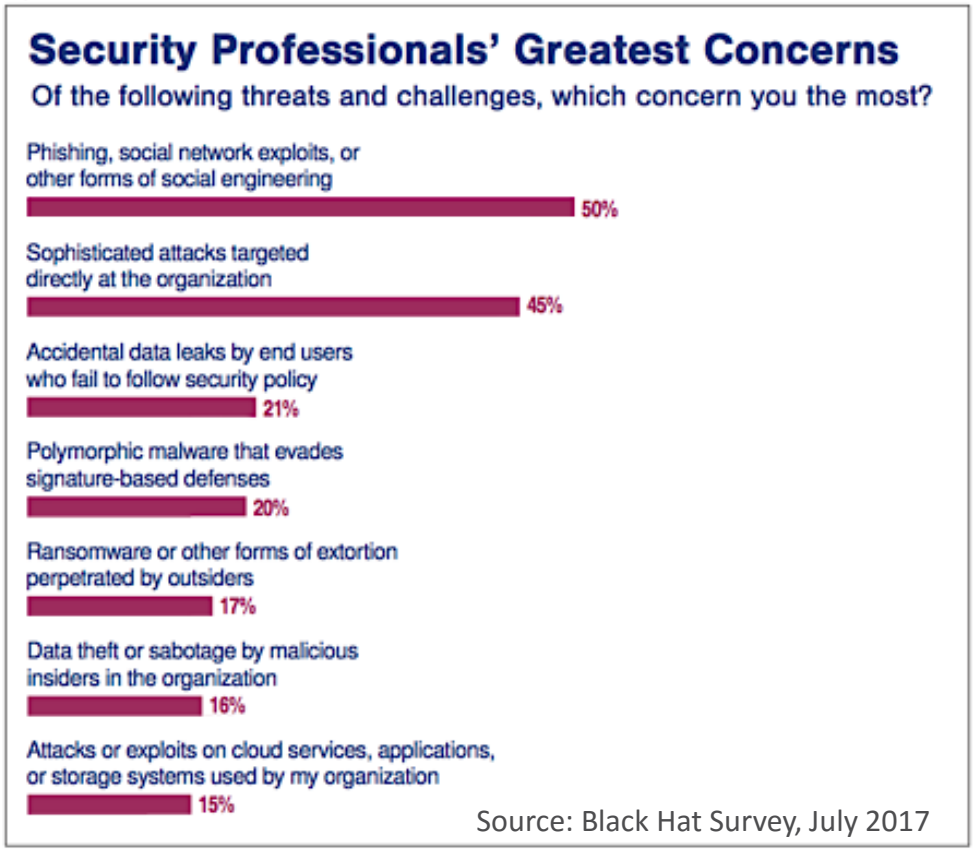
Please process this specific LOA write-off request in the amount of $120,200.39. Approvals attached and confirm with me once done

TREND MICRO

피싱 공격이 #1 보안 이슈

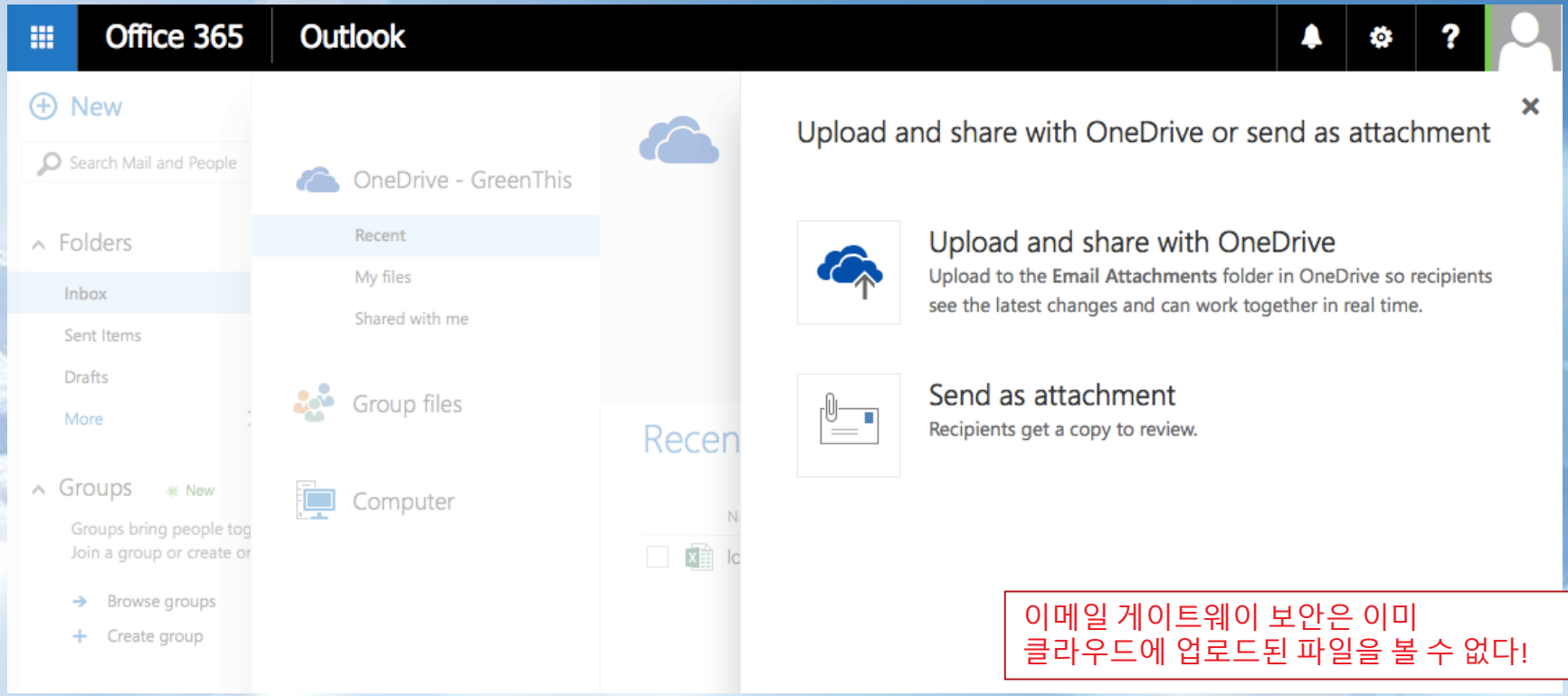
상위 5 관심사는 모두 이메일과 관련

- Phishing
- Targeted attacks
- Compliance
- Advanced Threat
- Ransomware
- Cloud services



Source: Black Hat Survey, July 2017

사용자 행위:
이메일 첨부파일 ➔ 클라우드 파일 공유



이메일 게이트웨이 보안은 이미
클라우드에 업로드된 파일을 볼 수 없다!

Office 365에 포함된 보안 기능을 보완하게 되는 이유는?

- Exchange Online is designed and SLA backed to catch 100% *known* malware

> **Anti-malware protection**
>
> Using multiple anti-malware engines, Exchange Online offers multilayered protection that's designed to catch all known malware. All messages transported through the service are scanned for malware (viruses

- **But since 90% malware infects only 1 device, *Only 10% malware is known.***
- Every customer needs a strategy to deal with unknown malware at the email layer
- E5/ATP adds sandboxing but misses significant amount of unknown malware and lacks BEC/fraud detection
- Office 365 popularity makes it worthwhile and easy for attackers to QA test their attacks on Office 365

If you bought a new home with a smoke detector guaranteed to detect 10% of fires would you supplement it?

규정 준수 및 개인 정보를 유지할 필요

- 많은 데이터 누출이 잘못된 첨부파일 또는 잘못된 수신자에 의하여 발생
- GDPR, PCI, HIPAA 또는 기타 규정을 준수해야 할 필요
- 고객은 비즈니스 요구 사항에 대한 복잡성이나 간섭이 없이 보호 받기를 원함

Wells Fargo Accidentally Releases Trove of Data on Wealthy Clients

By SERGE F. KOVALESKI and STACY COWLEY JULY 21, 2017

GOP Data Firm Accidentally Leaks Personal Details of Nearly 200 Million American Voters

Dell Cameron and Kate Conger
6/19/17 8:00am • Filed to: RNC DATA LEAK

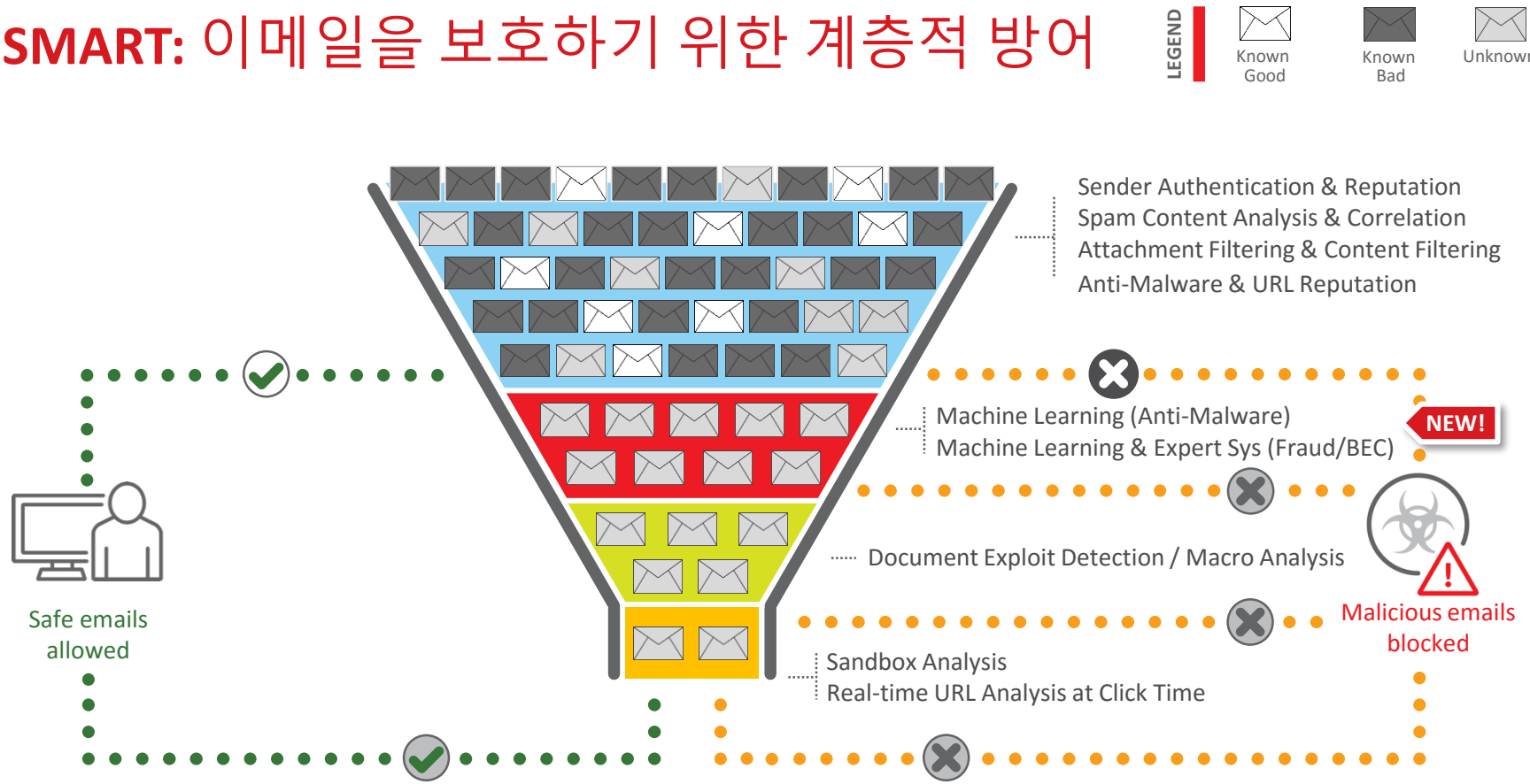
500.7K 214 23

Sweden Accidentally Leaks Personal Details of Nearly All Citizens

Monday, July 24, 2017 Swati Khandelwal

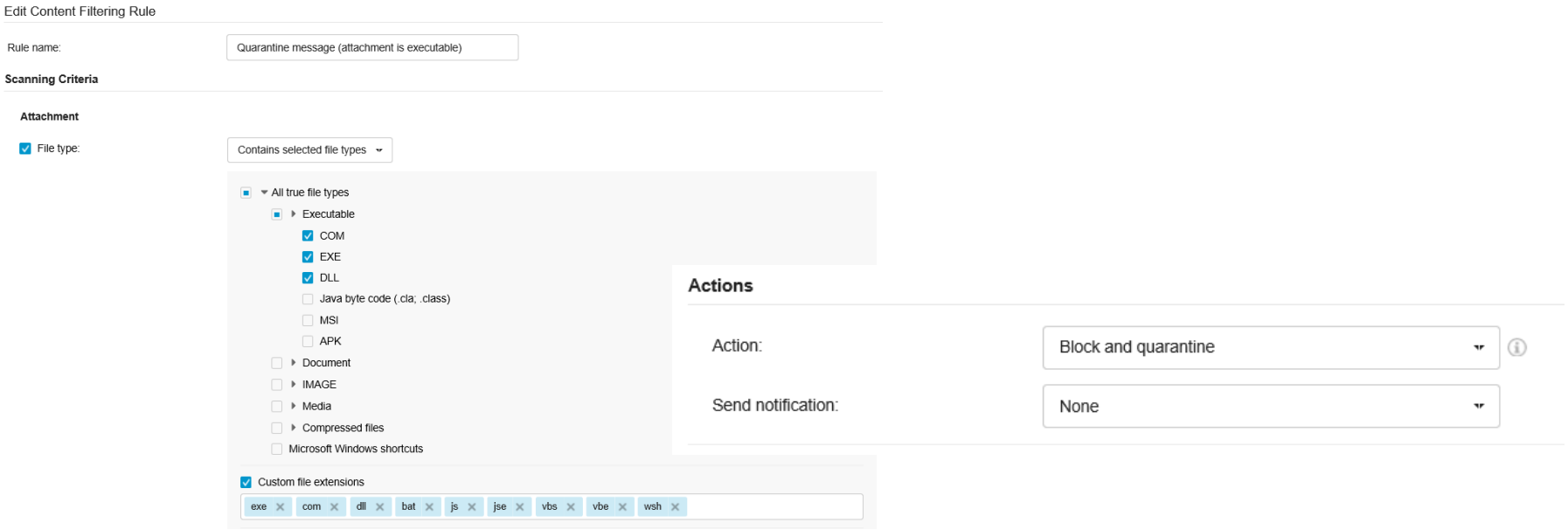
Protect

SMART: 이메일을 보호하기 위한 계층적 방어



첨부파일 필터링 정책

- 악성코드가 사용할 가능성이 있는 첨부파일 타입을 악성 유무와 관계없이 차단
- .EXE, .DLL, .JS, .JSE, .VBS, .VBE, .WSH, .PS 등



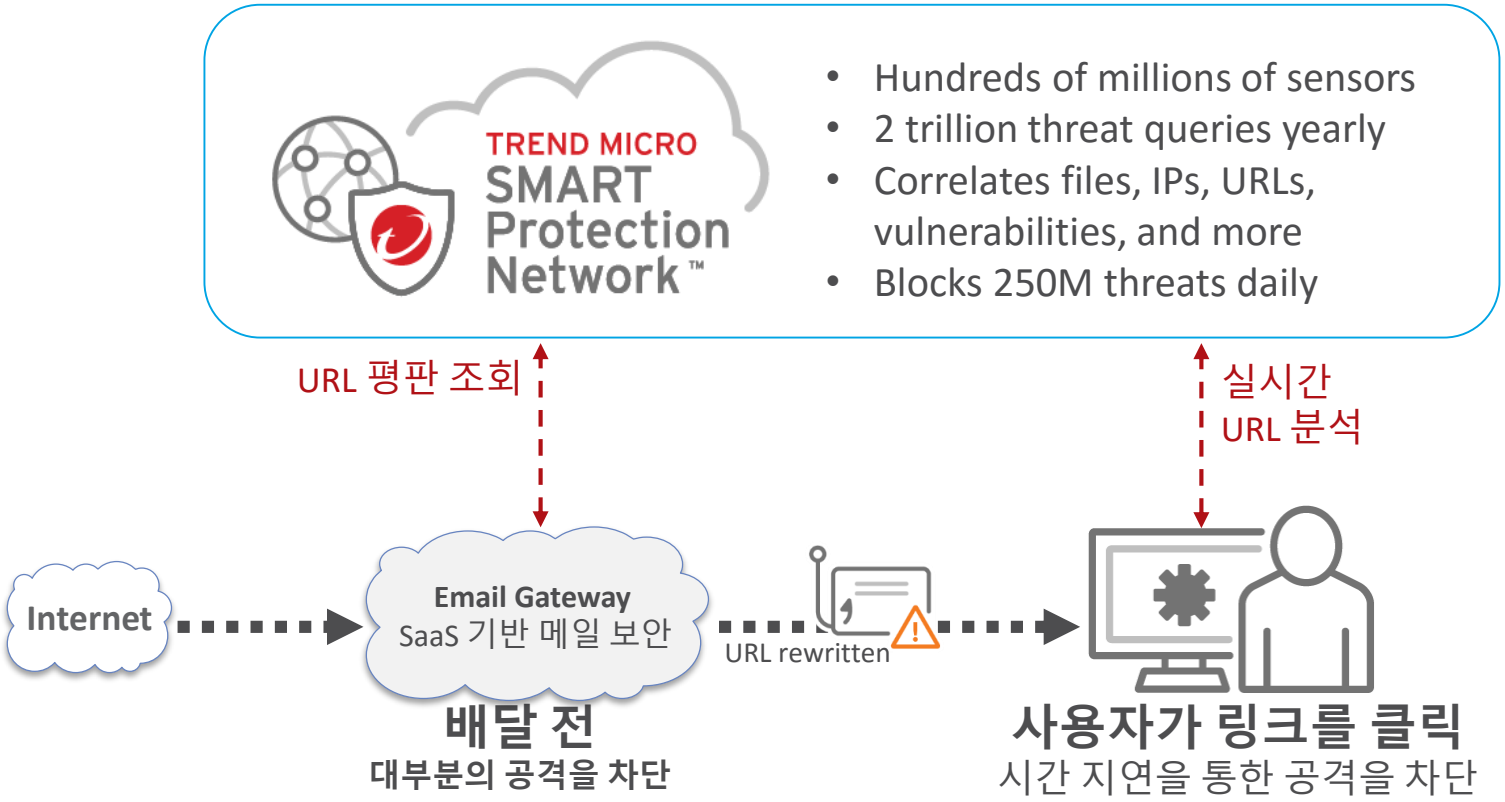
알려지지 않은 악성코드의 탐지

Pre-execution machine learning – 수 천 개의 파일 기능과 기계 학습 모델을 사용하여 악성 파일을 예측 탐지. 샌드박스 이전에 알 수 없는 악성코드를 찾아 이메일 배달 효율성을 향상

Document Exploit Detection – 파일을 구문 분석하여 의도한 애플리케이션에 대한 알려진 악성 및 잠재적 악성 코드를 탐지. 현장에서 새로운 제로 데이 익스플로잇을 탐지하는 기술

Sandbox analysis – 병렬로 멀티OS를 사용한 행위 분석. 수 분 내에 행위 분석을 완료

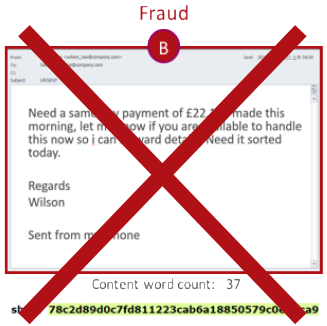
악성 URL 방어



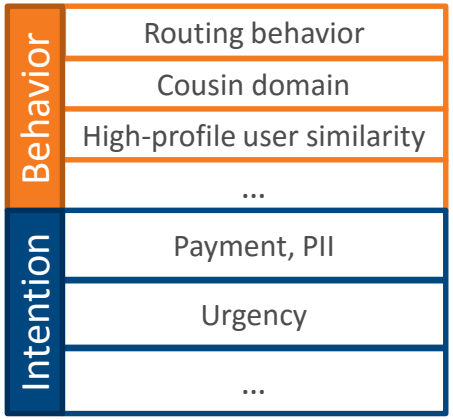
A.I. 기반의 사기 이메일(BEC) 탐지: 보안 전문가의 분석 판단모델을 대입

EXPERT RULES

MACHINE LEARNING



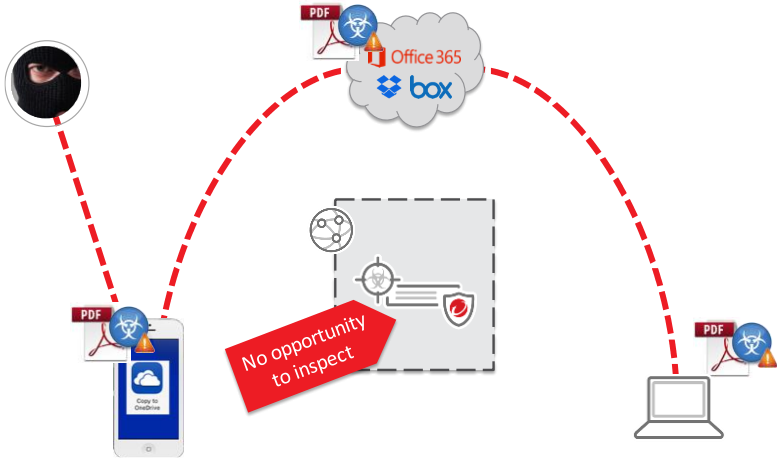
보다 정확한 식별



규칙 가중치 및 상관 관계

클라우드 파일 공유에 대한 악성코드 방어

Problem: Cloud file services include only basic AV - misses unknown malware. Network Breach Detection Systems don't see traffic between off-network devices and SaaS services

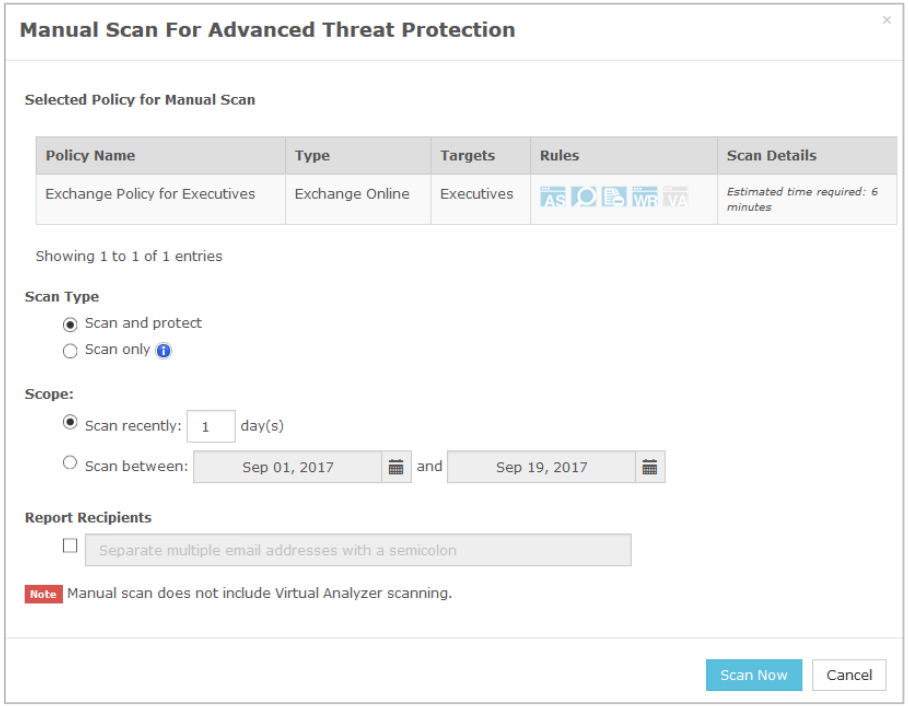


- Trend Micro prevents threats from spreading in OneDrive, SharePoint, Box, Dropbox, Google Drive:
- Advanced threat scanning
  - Machine-learning based antimalware
  - Document exploit detection
  - URL analysis
  - Sandbox analysis
- On-demand scan to discover existing threats

조직 내부에서 미리 공격을 감지

- 메일서버 자체의 악성탐지 솔루션 적용
- 내부 이메일에서 사기 위협을 검사
- 디렉토리 그룹별 세부 정책
- 조치: 태그 (warning), 삭제, 격리

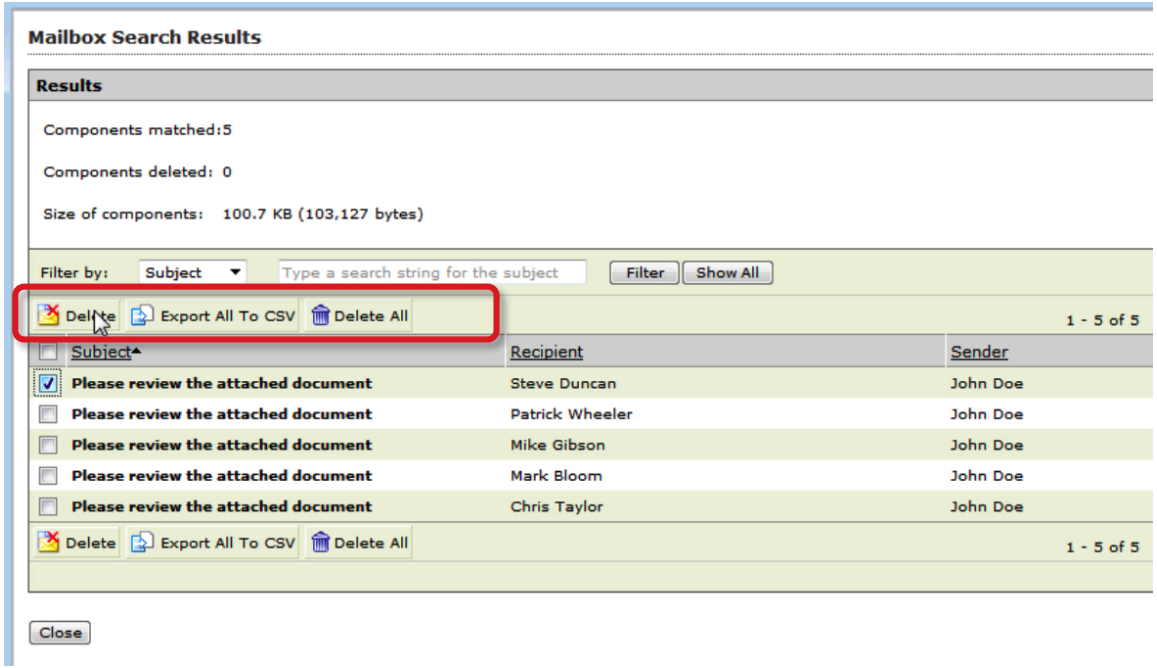
Office 365 보안 솔루션을 이용한 악성파일 검색 및 삭제



Office 365 Security

Office 365 사서함 또는 파일 공유의 첨부파일들을 검색하고 삭제하는 솔루션 적용

Exchange/Domino 사서함 내의 파일 검색 및 삭제



Trend Micro ScanMail

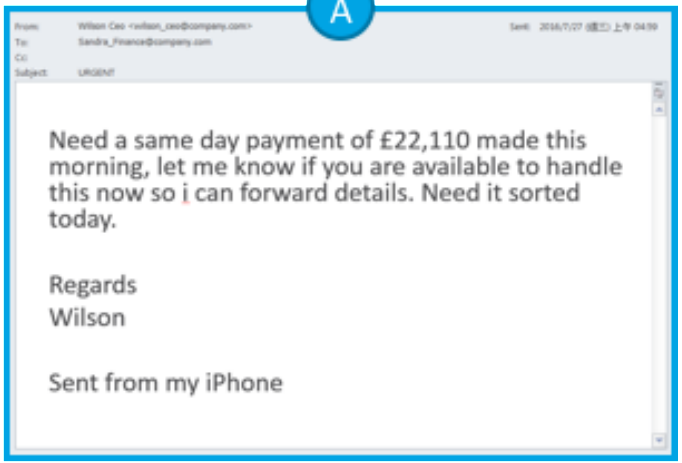
Allows you to search and delete

Business Email Compromise/Fraud Protection

교육에도 불구하고, 사용자는 Fake 이메일을 판별하지 못함

Real

A

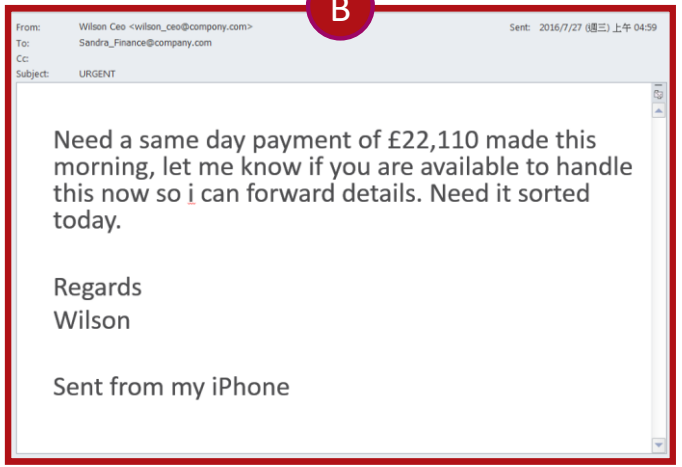


Content word count: 37

sha1: 78c2d89d0c7fd811223cab6a18850579c0e39ca9

Fraud

B



Content word count: 37

sha1: 78c2d89d0c7fd811223cab6a18850579c0e39ca9

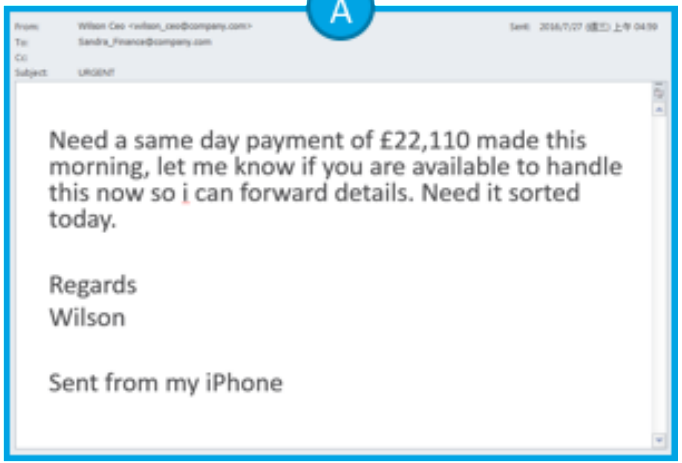
97% 의 사용자가 정교한 피싱 메일을 식별할 수 없다.

- Inspired elearning July 2017

보안 전문가만이 이를 식별할 수 있다면?

Real

A

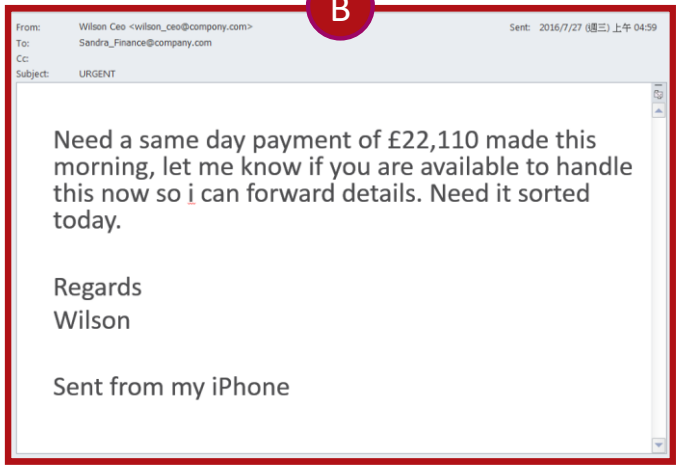


Content word count: 37

sha1: 78c2d89d0c7fd811223cab6a18850579c0e39ca9

Fraud

B

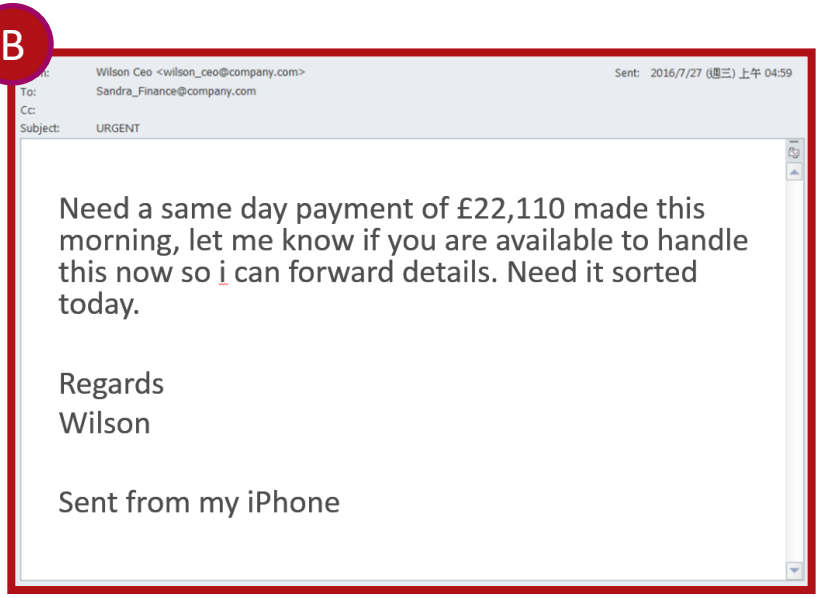


Content word count: 37

sha1: 78c2d89d0c7fd811223cab6a18850579c0e39ca9

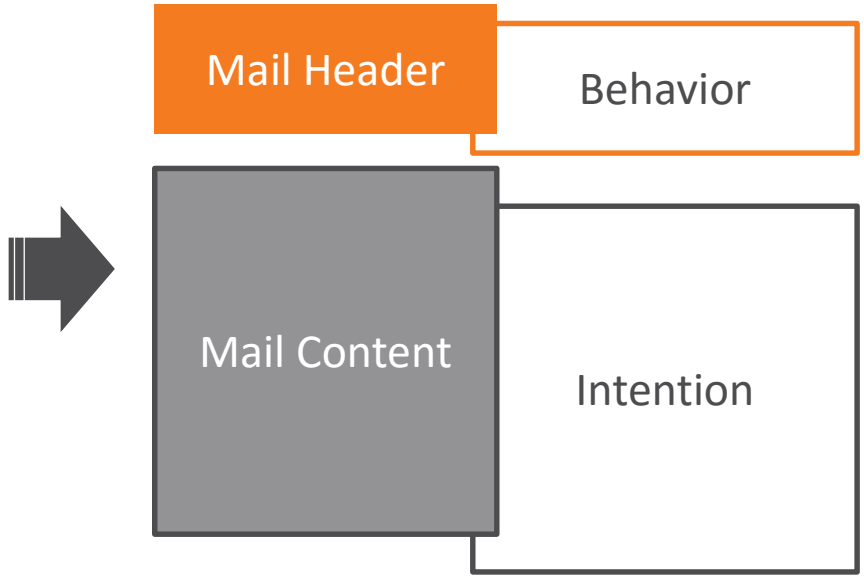
보안 전문가는 행위와 의도 두 가지 측면에서 조사

B



Content word count: 37

sha1: 78c2d89d0c7fd811223cab6a18850579c0e39ca9



해커 행동 특성

Mail Header

Received: from p3plwbeout05-06.prod.phx3.secureserver.net (p3plsmtp05-06-02.prod.phx3.secureserver.net [97.74.135.51]) (using TLSv1.2 with cipher DHE-RSA-AES128-SHA (128/128 bits)) (No client certificate requested) by itf-01.company.com (Postfix) with ESMTPS id E0B9815FC65 for <Sandra_Finance@company.com>; Mon, 1 Aug 2016 05:47:42 +0000 (UTC)
Received: from localhost ([97.74.135.4]) by p3plwbeout05-06.prod. 25 Jul 2016 20:17:32 -0700
X-CMAE: v=2.1 cv=L/aTQoj8 c=1 sm=1 tr=0 p=i-petxfovf8A:10 a=glJzh28+BKpT :10 a=9cW_t1CCXrUA:10
a=s5jvgZ67dGcA:10 a=WJA2BgnzfmMA:10 a=A7pwO9xP048A:10 a=IkcTkHD0f z7yfcEeC:21 a=QEXdDO2ut3YA:10
a=_W_S_7VecoQA:10

불안전한 이메일 공급자 !

Message-Id: <08924520399f2e65d9e0753294fa8fa4@email05.**secureserver.net**>

User-Agent: Workspace Webmail 6.4.2

X-Domain: entraser.com
X-SID: Rhni1t00205rkER01
Received: (qmail 15064 invoked by uid 99); 1 Aug 2016 05:47:42 -0000
Content-Transfer-Encoding: quoted-printable

! 위조된 폼: domain

From: "Wilson Ceo" <wilson_ceo@compony.com>

To: Sandra_Finance@company.com

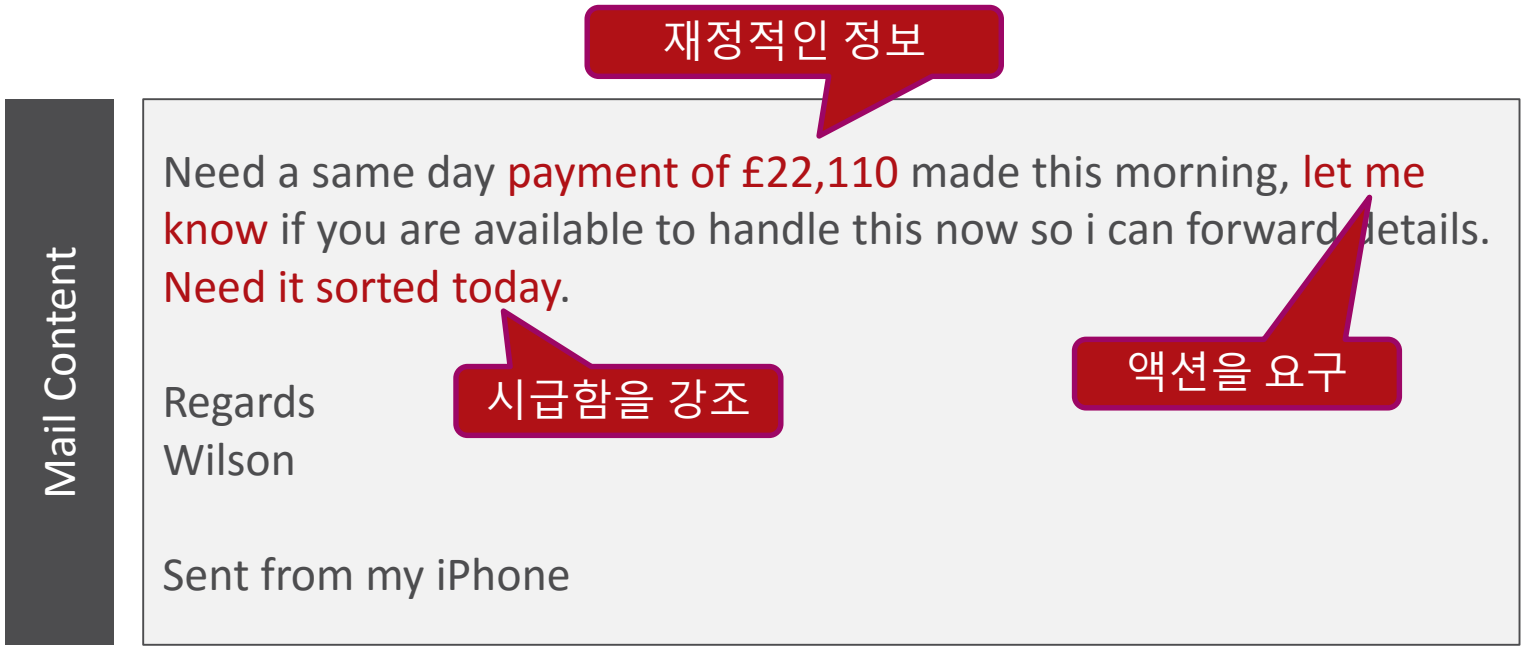
Content-Type: text/html; charset="utf-8"
X-Originating-IP: 154.118.71.165
Subject: URGENT
X-Sender: amina@entraser.com

! 참조 주소를 프리 이메일로 변경

Reply-To: "Wilson Ceo" <emailpresident2@**gmail**.com>

Date: Sun, 31 Jul 2016 22:47:40 -0700

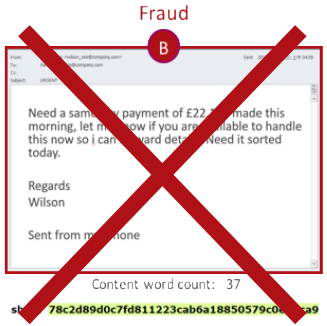
이메일 의도 특성



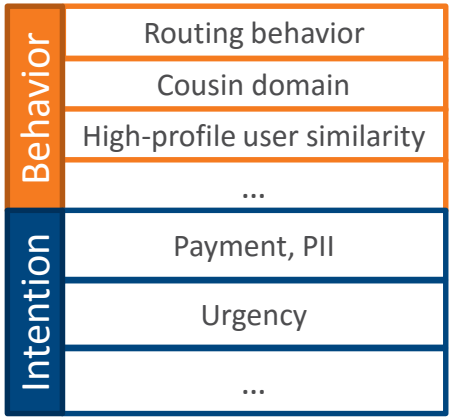
A.I. 기반의 사기 이메일(BEC) 탐지: 보안 전문가의 분석 판단모델을 대입

EXPERT RULES

MACHINE LEARNING



보다 정확한 식별

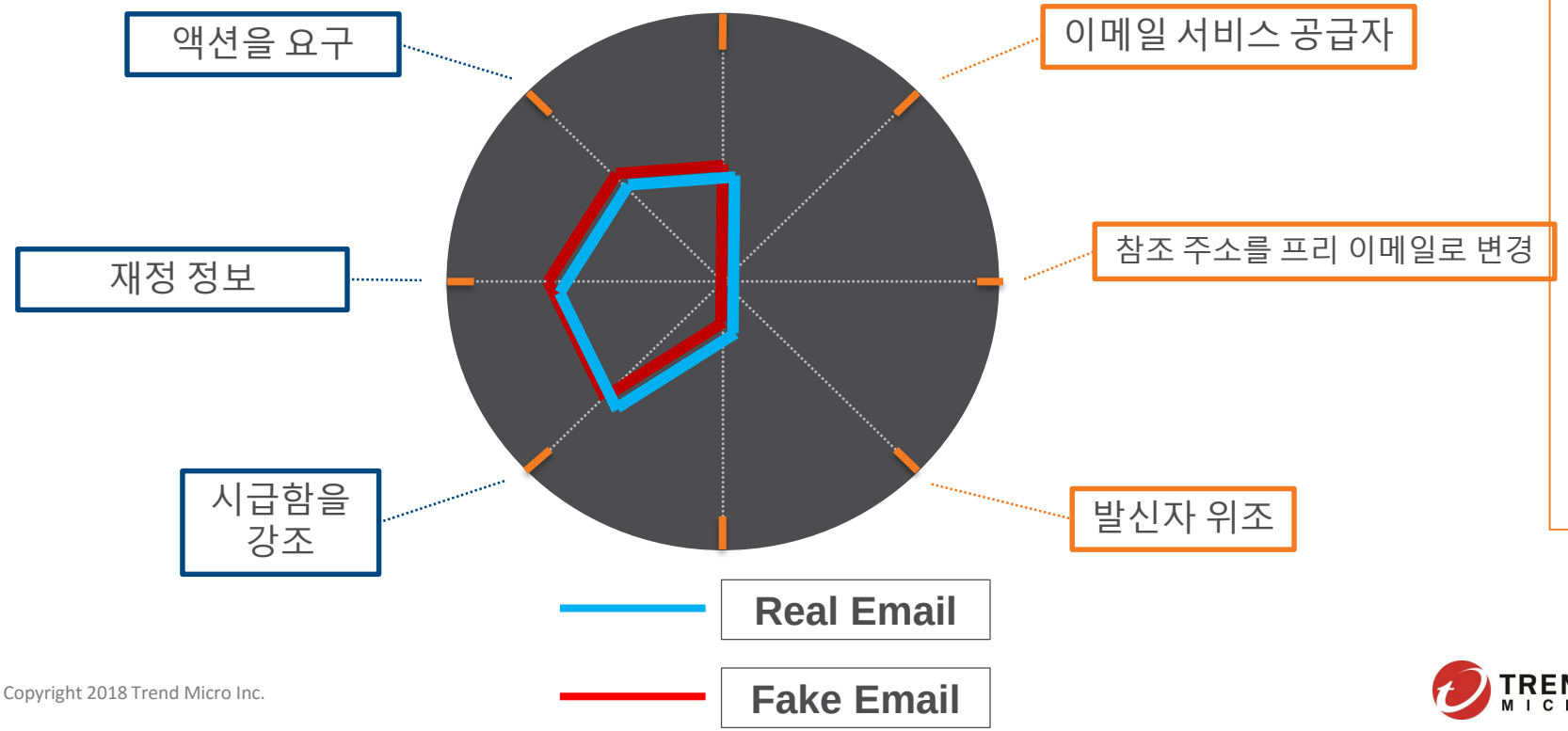


규칙 가중치 및 상관 관계

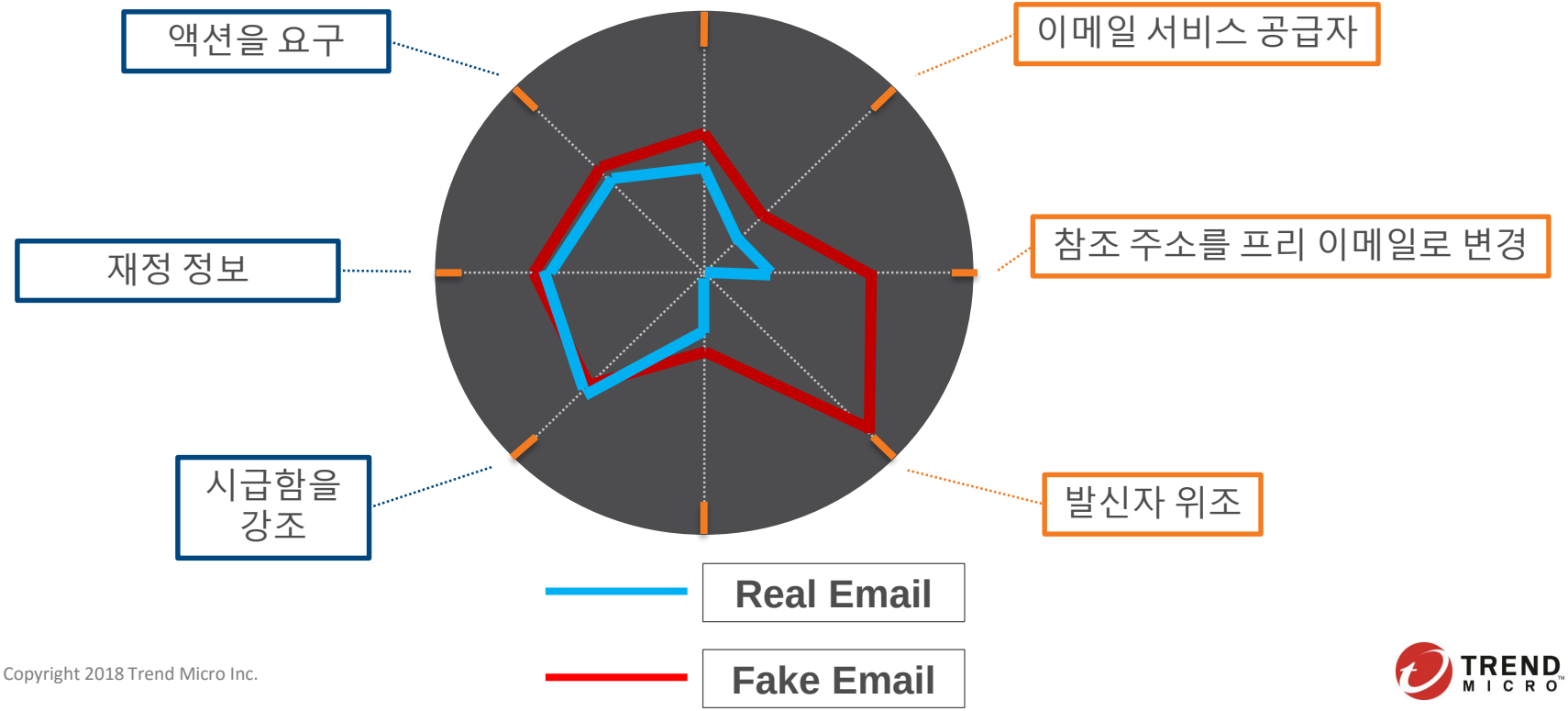
사람이 보는 관점→ 정상 메일과 Fake메일이 동일하게 보임

이메일 내 의사표시 요소

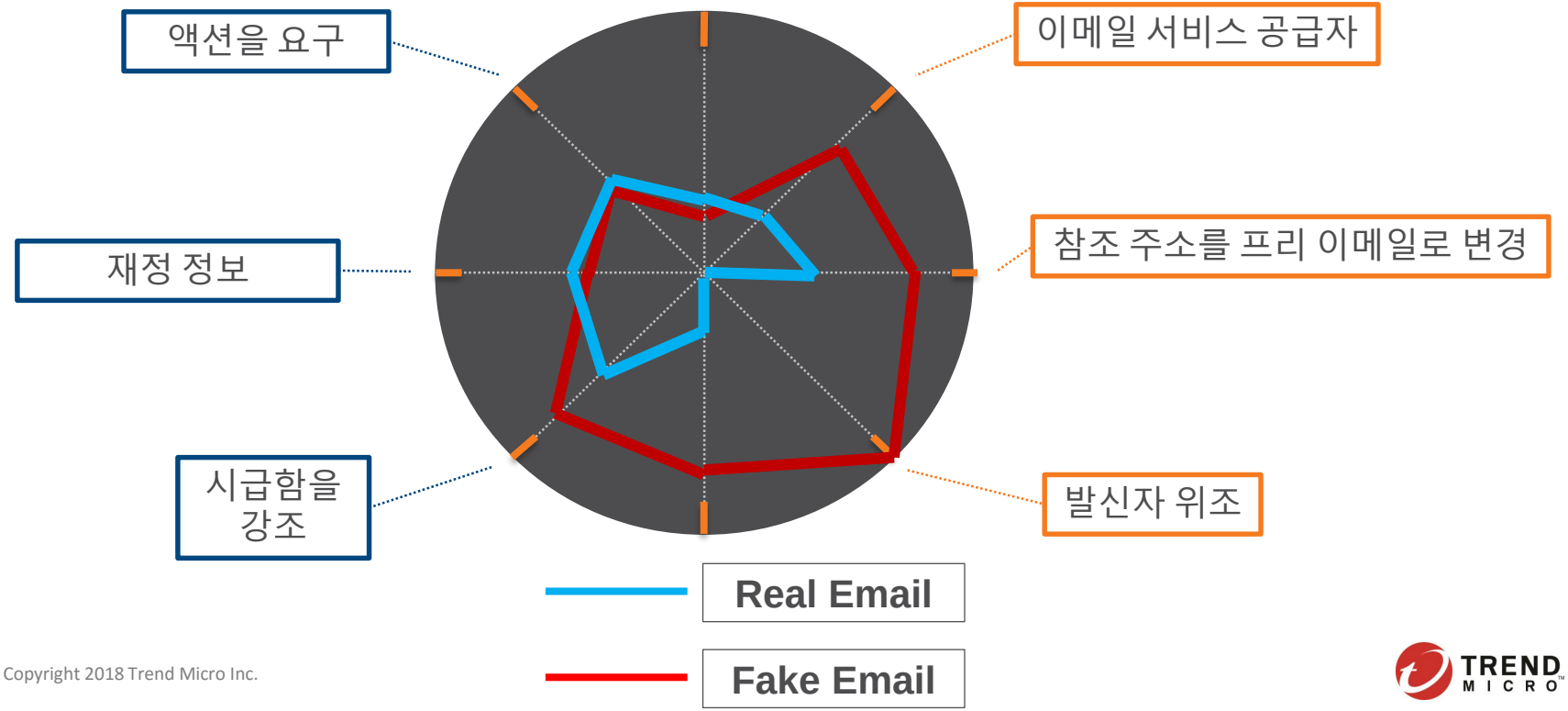
공격자의 행위 요소



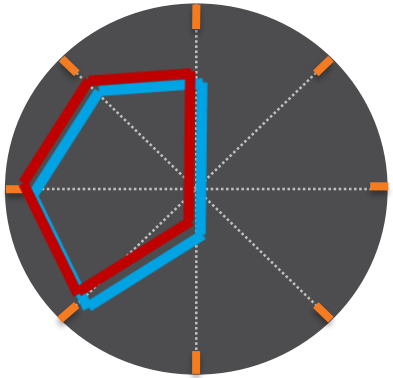
전문가 규칙에서의 관점 → 의심 메일

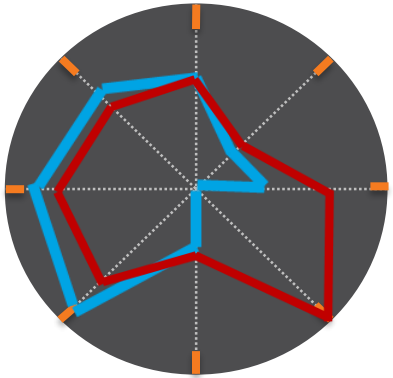


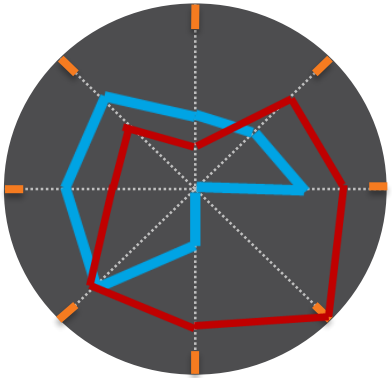
전문가 규칙 + 머신 러닝 = 사기 메일 탐지



분석의 완성도 향상 = 전문가 규칙 + 머신 러닝





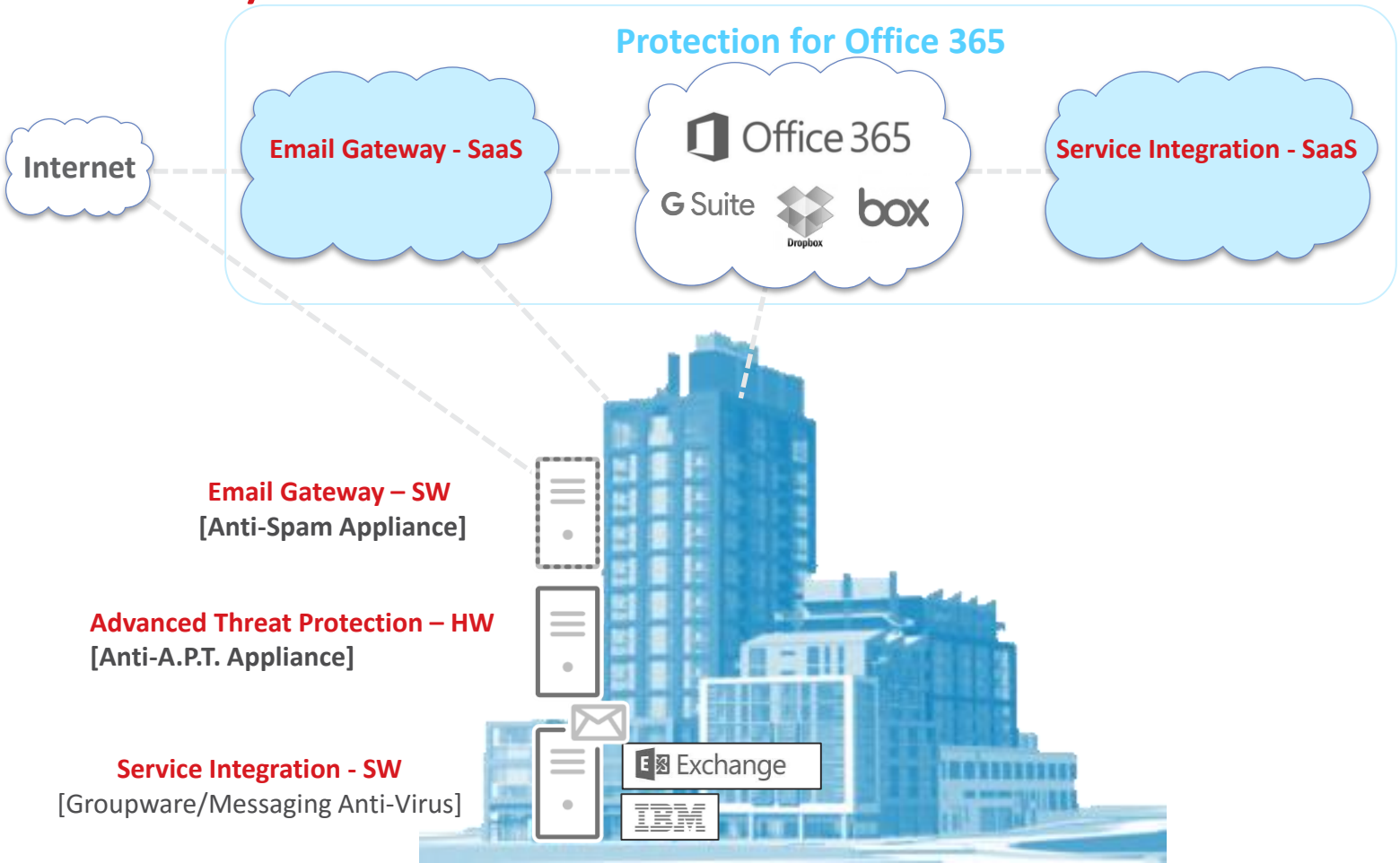


사람 → 전문가 규칙 → 전문가 규칙 + 머신러닝

정상? | **의심** | **탐지!**

Trend Micro Email Security

Email Security Portfolio



감사합니다.