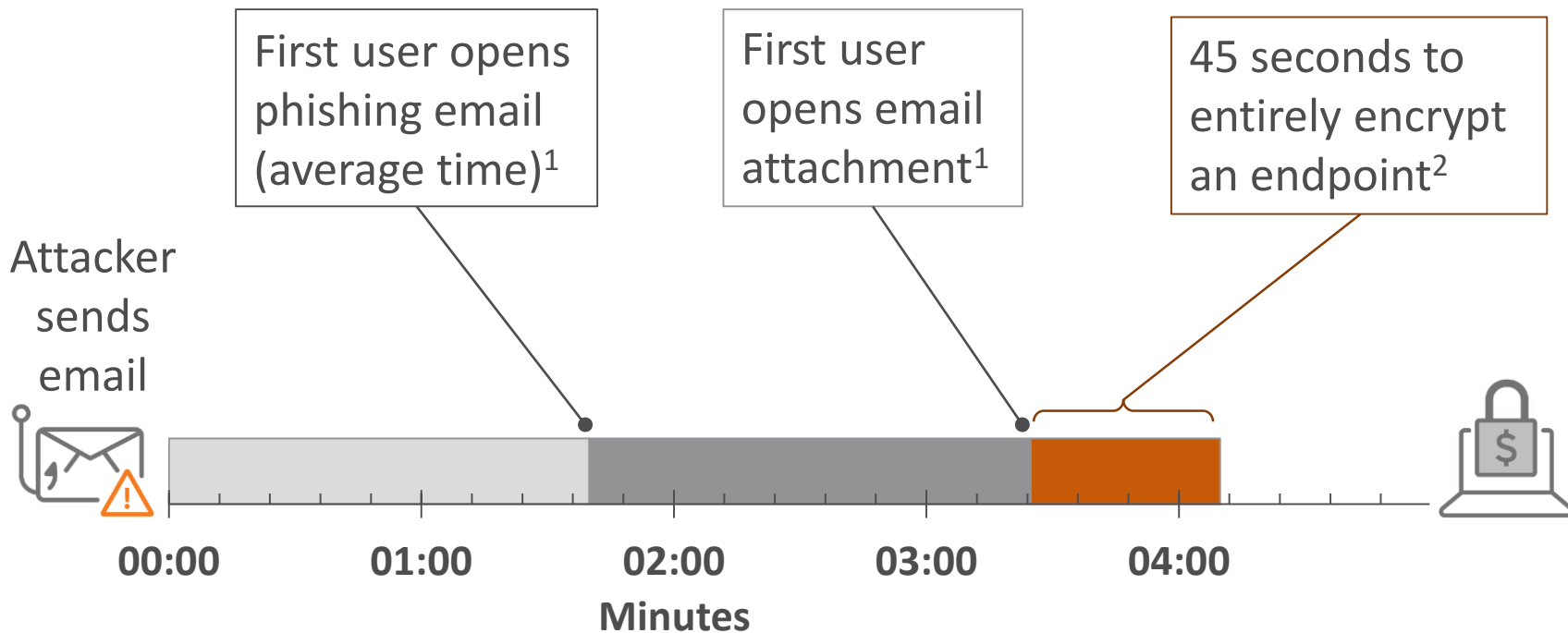


변화하는 위협에 대응하는 이메일 보안

2018/6/8

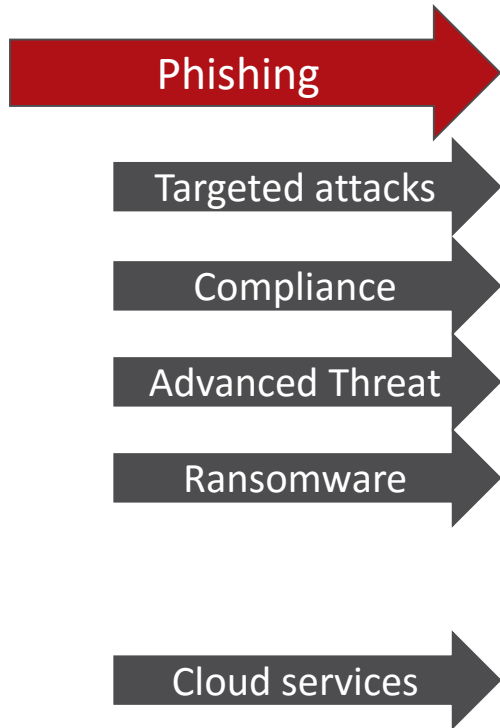


79% 랜섬웨어 공격은 피싱 이메일을 사용



피싱 공격이 #1 보안 이슈

상위 5
관심사는
모두
이메일과
관련



Security Professionals' Greatest Concerns

Of the following threats and challenges, which concern you the most?

Phishing, social network exploits, or other forms of social engineering



Sophisticated attacks targeted directly at the organization



Accidental data leaks by end users who fail to follow security policy



Polymorphic malware that evades signature-based defenses



Ransomware or other forms of extortion perpetrated by outsiders



Data theft or sabotage by malicious insiders in the organization



Attacks or exploits on cloud services, applications, or storage systems used by my organization



Source: Black Hat Survey, July 2017

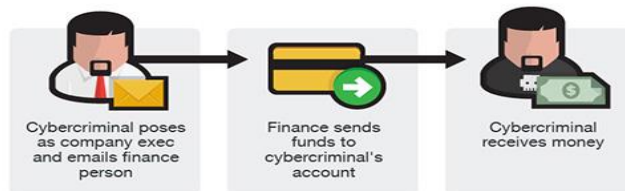
Business Email Compromise (BEC, 비즈니스 이메일 위협) 공격



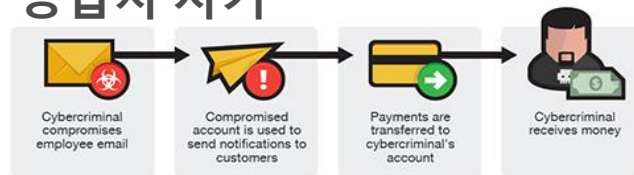
- **글로벌 \$5B** 가치의 손실
- **사기 건 당 평균 \$132,000** 손실

Difficult to detect – no attachment/URL

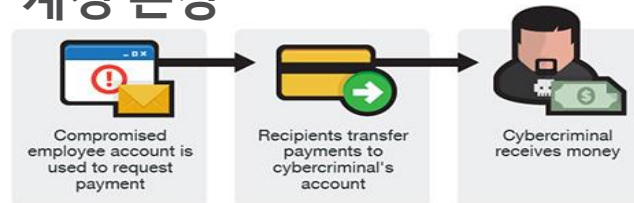
CEO Fraud



공급자 사기



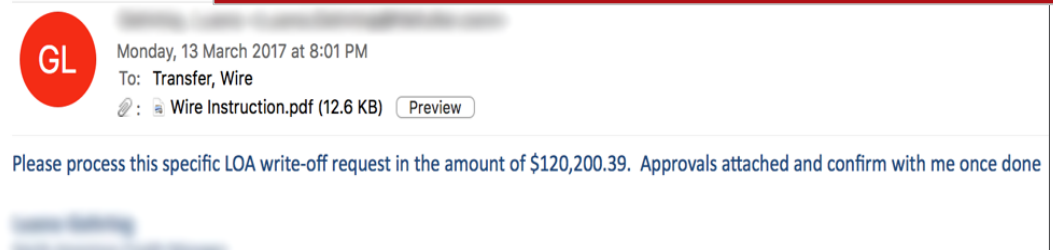
계정 손상



조직 내부의 공격자: 신뢰할 수 있는 사용자의 내부 피싱 이메일



이메일 게이트웨이 보안은 내부 메일을 볼 수 없다!



Protect

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



첨부파일 필터링 정책

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

Edit Content Filtering Rule

Rule name: Quarantine message (attachment is executable)

Scanning Criteria

Attachment

File type: Contains selected file types

- All true file types
 - Executable
 - COM
 - EXE
 - DLL
 - Java byte code (.cia, .class)
 - MSI
 - APK
 - Document
 - IMAGE
 - Media
 - Compressed files
 - Microsoft Windows shortcuts

Custom file extensions

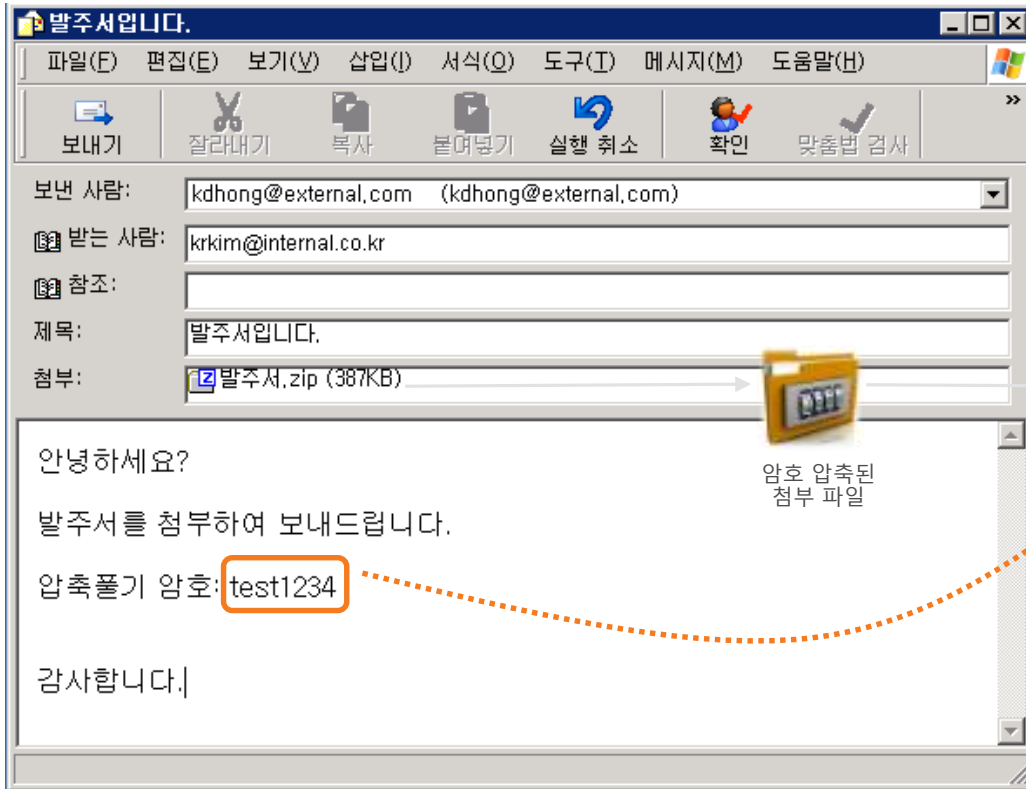
exe x com x dll x bat x js x jse x vbs x vbe x wsh x

Actions

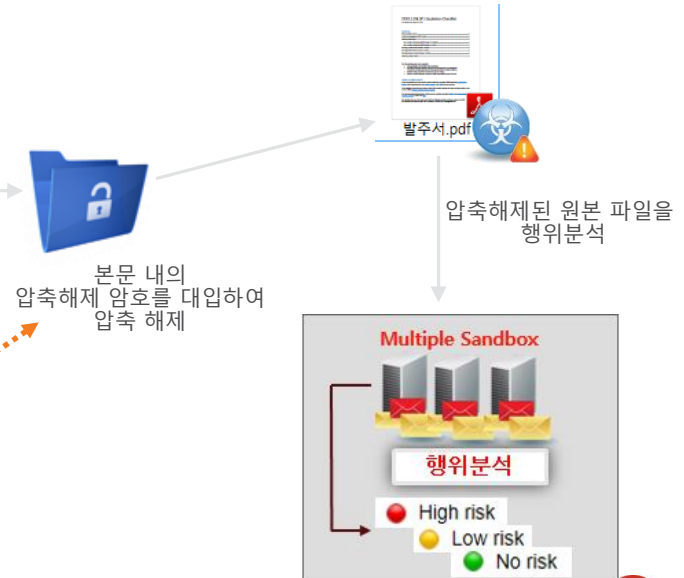
Action: Block and quarantine 

Send notification: None

압축 암호 첨부파일에 대한 정책



- 메시지 본문 내에 포함된 첨부파일 압축풀기 암호를 사용하여 자동으로 압축해제 및 행위분석



악성 URL 탐지 정책

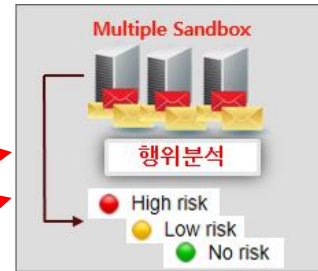
- 첨부된 문서 내의 URL들을 행위분석
- 메시지 본문 뿐만 아니라 제목에 포함된 URL도 행위분석

Required Applications

The Virtual Analyzer image requires the following necessary applications for threat analysis:

TABLE F-1. Required Applications

APPLICATION	DESCRIPTION
Microsoft Office	2003, 2007, or 2010 Ensure that macros are enabled. See https://support.office.com for details.
Adobe Reader	Trend Micro recommends installing the version of Adobe Reader that is most widely used in your organization. To download the most current version of Adobe Reader, go to http://www.adobe.com/downloads/ . If you have Adobe Reader installed, check Preparing Adobe Reader on page F-4 for details. If you do not install Acrobat Reader, Virtual Analyzer does the following: <ul style="list-style-type: none">• Automatically installs Adobe Reader 8, 9, and 11 on all images.• Uses all three versions during analysis. WARNING! This consumes additional computing resources. <ul style="list-style-type: none">• If the image runs Windows XP, install .NET Framework 3.5 (or later).



건적서 - http://www.eicar.org

받는 사람: kskim@internal.co.kr

제목: 건적서 - http://www.eicar.org

안녕하세요?

요청하신 건적서는 제목에 있는 링크를 통해서 확인하실 수 있습니다.

감사합니다.

홍길동 배상

악성 URL 시간차 공격 차단(Time Click Protection)



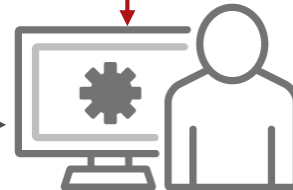
- Hundreds of millions of sensors
- 2 trillion threat queries yearly
- Correlates files, IPs, URLs, vulnerabilities, and more
- Blocks 250M threats daily

URL 평판 조회

실시간 URL 분석



배달 전
대부분의 공격을 차단



사용자가 링크를 클릭
시간 지연을 통한 공격을 차단

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



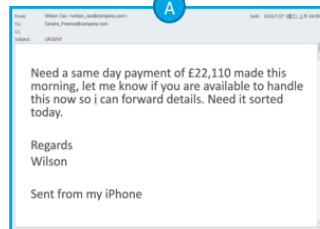
EXPERT
RULES



MACHINE
LEARNING



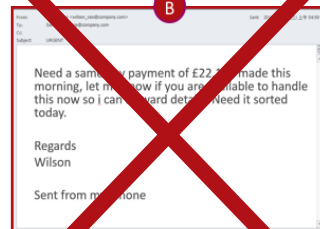
Real



Content word count: 37

sha1: 78c2d89d0c7fd811223cab6a18850579c0e39ca9

Fraud



Content word count: 37

sha1: 78c2d89d0c7fd811223cab6a18850579c0e39ca9

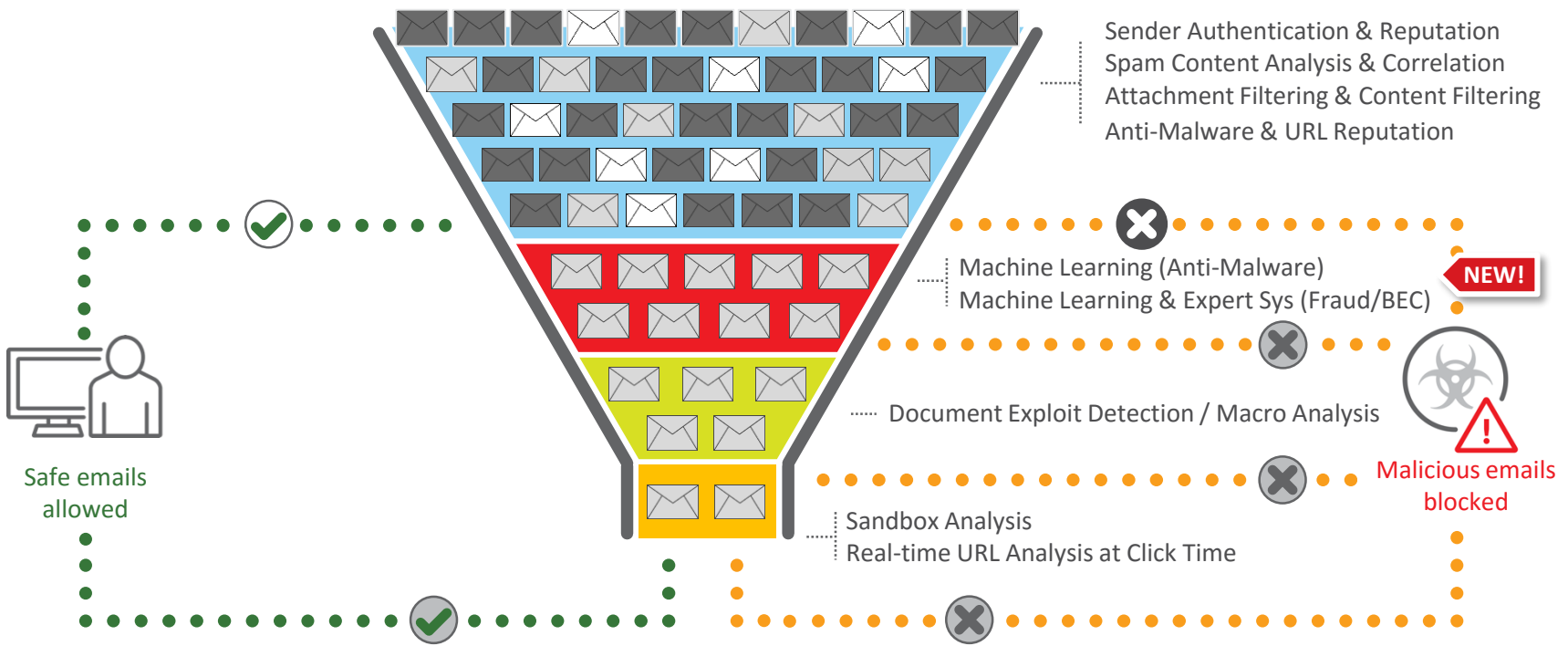
Behavior	Routing behavior
	Cousin domain
	High-profile user similarity
	...
Intention	Payment, PII
	Urgency
	...

규칙 가중치
및 상관 관계

보다 정확한
식별

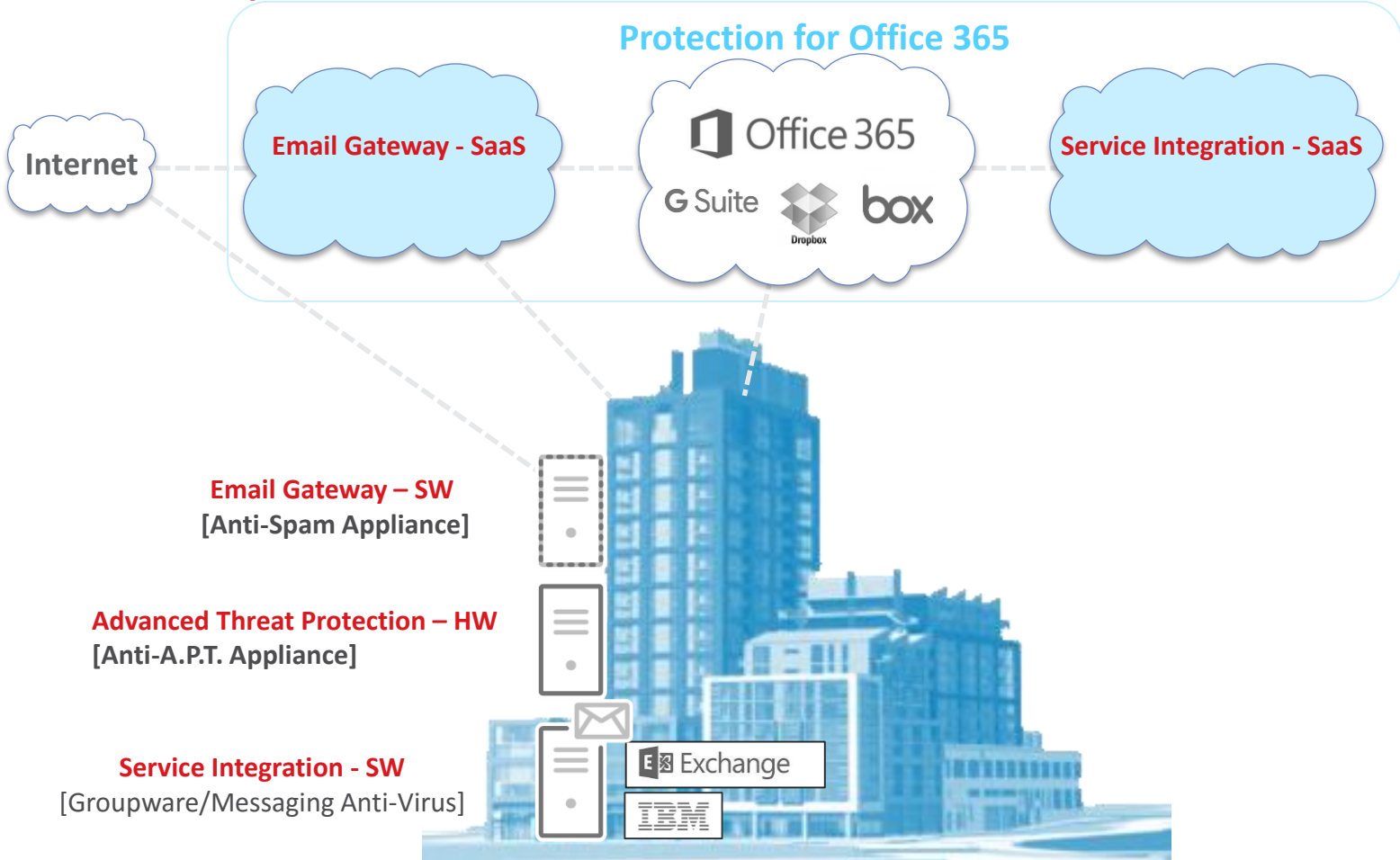
SMART: 이메일을 보호하기 위한 계층적 방어

LEGEND



Trend Micro Email Security

Email Security Portfolio

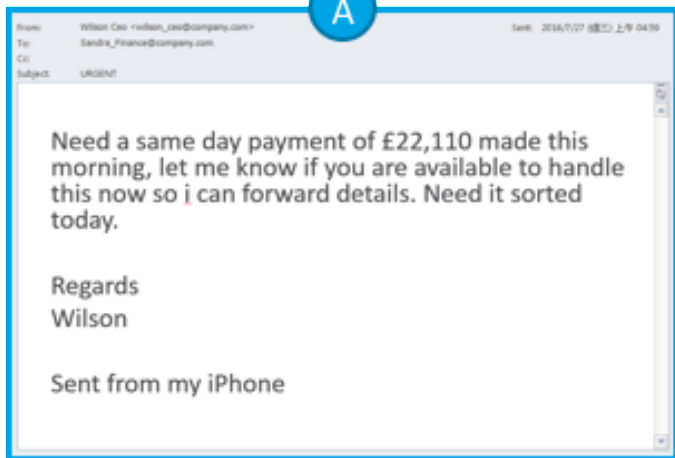


Business Email Compromise/Fraud Protection

교육에도 불구하고, 사용자는 Fake 이메일을 판별하지 못함

Real

A



Content word count: 37

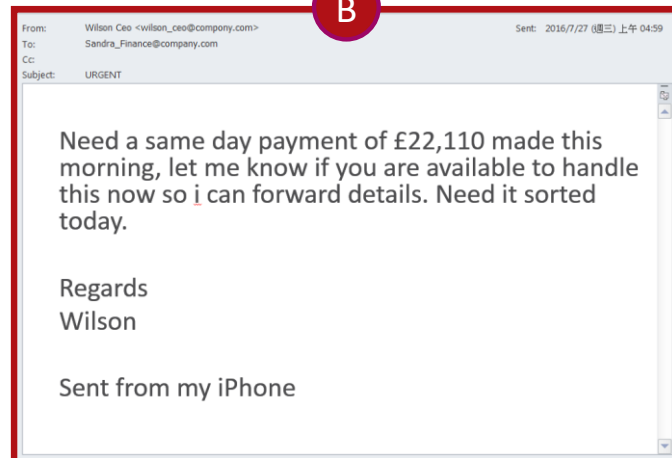
sha1: 78c2d89d0c7fd811223cab6a18850579c0e39ca9

?



Fraud

B



Content word count: 37

sha1: 78c2d89d0c7fd811223cab6a18850579c0e39ca9

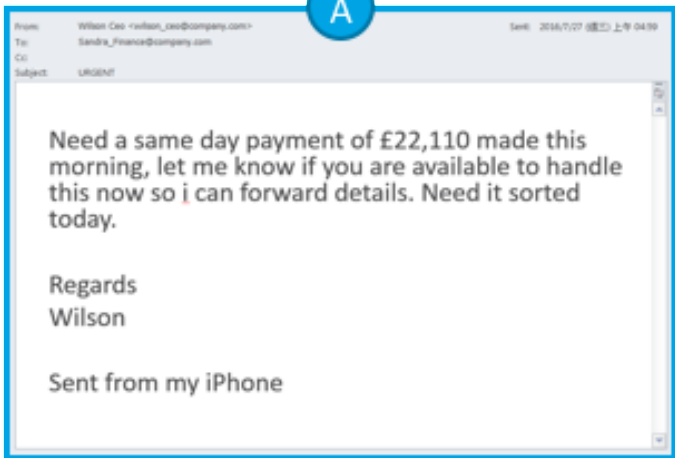
97%의 사용자가 정교한 피싱 메일을 식별할 수 없다.

- Inspired elearning July 2017

보안 전문가만이 이를 식별할 수 있다면?

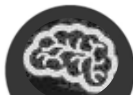
Real

A



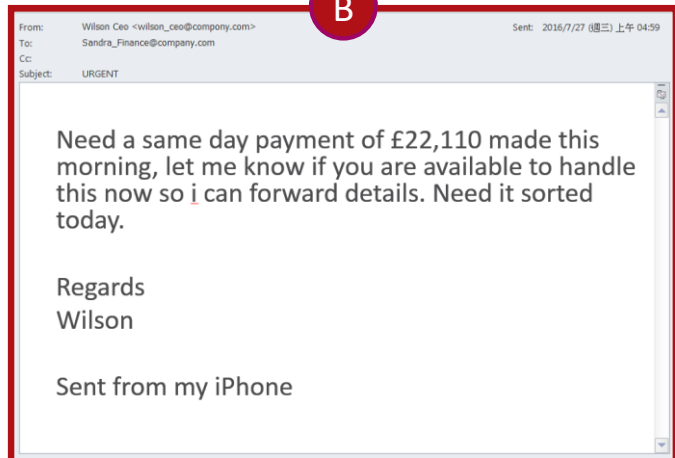
Content word count: 37

sha1: 78c2d89d0c7fd811223cab6a18850579c0e39ca9



Fraud

B

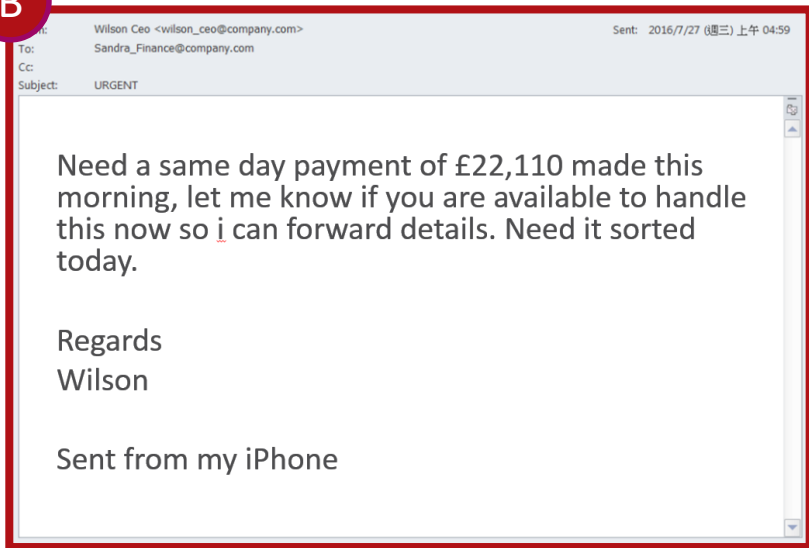


Content word count: 37

sha1: 78c2d89d0c7fd811223cab6a18850579c0e39ca9

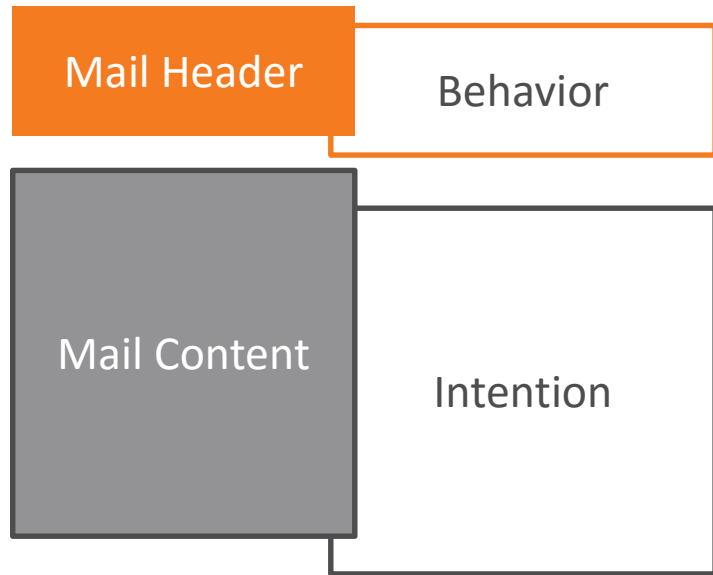
보안 전문가는 행위와 의도 두 가지 측면에서 조사

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.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)

불안정한 이메일 공급자 !

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

User-Agent: Workspace Webmail 6.4.2

X-Domain: entraser.com

X-SID: Rhni1t00205rker01

Received: (gmail 15064 invoked by uid 99); 1 Aug 2016 05:47:42 -0000

Content-Transfer-Encoding: quoted-printable

From: "Wilson Ceo" <wilson_ceo@company.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

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

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

! 위조된 품: domain

! 참조 주소를 프리 이메일로 변경

이메일 의도 특성

Mail Content

재정적인 정보

Need a same day **payment of £22,110** made this morning, **let me know** if you are available to handle this now so i can forward details.
Need it sorted today.

시급함을 강조

액션을 요구

Regards
Wilson

Sent from my iPhone

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



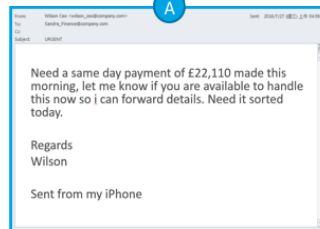
EXPERT
RULES



MACHINE
LEARNING



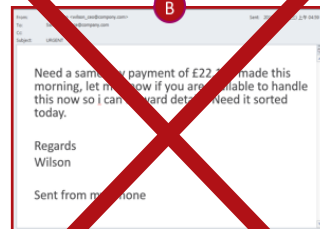
Real



Content word count: 37

sha1: 78c2d89d0c7fd811223cab6a18850579c0e39ca9

Fraud



Content word count: 37

sha1: 78c2d89d0c7fd811223cab6a18850579c0e39ca9

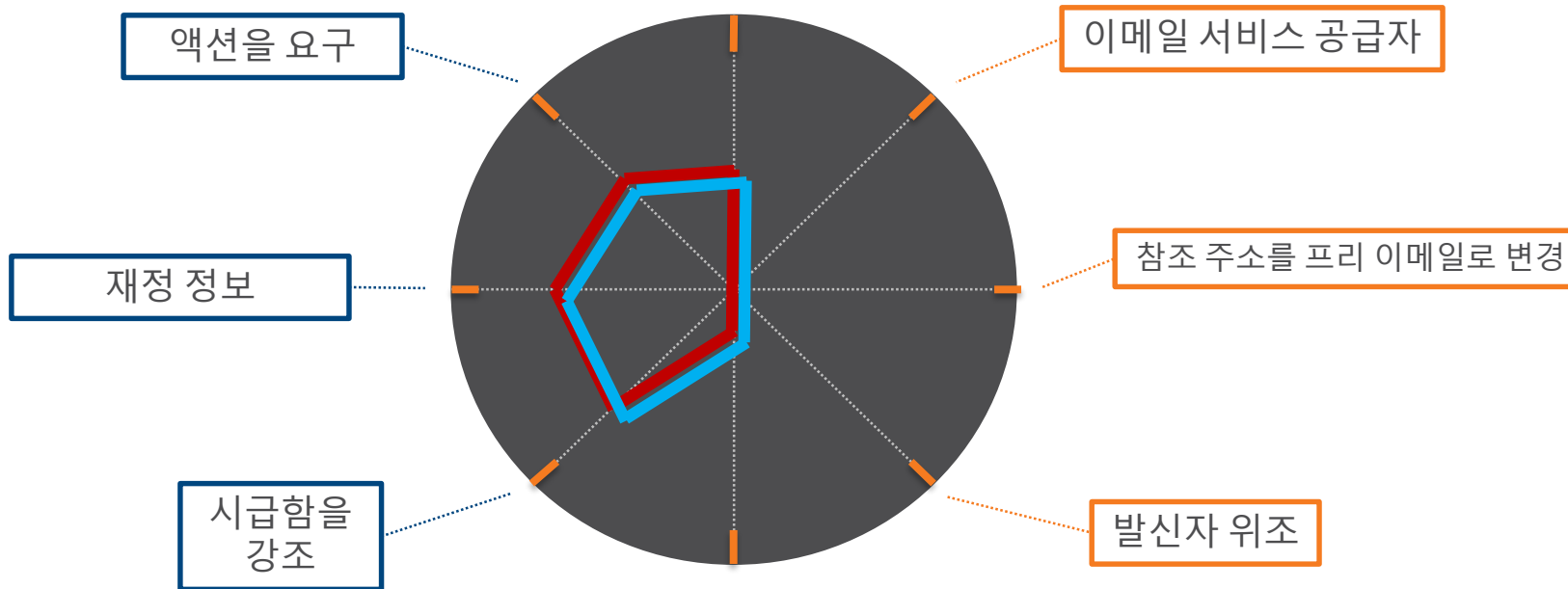
Behavior	Routing behavior
	Cousin domain
	High-profile user similarity
	...
Intention	Payment, PII
	Urgency
	...

규칙 가중치
및 상관 관계

보다 정확한
식별

사람이 보는 관점 → 정상 메일과 Fake 메일이 동일하게 보임

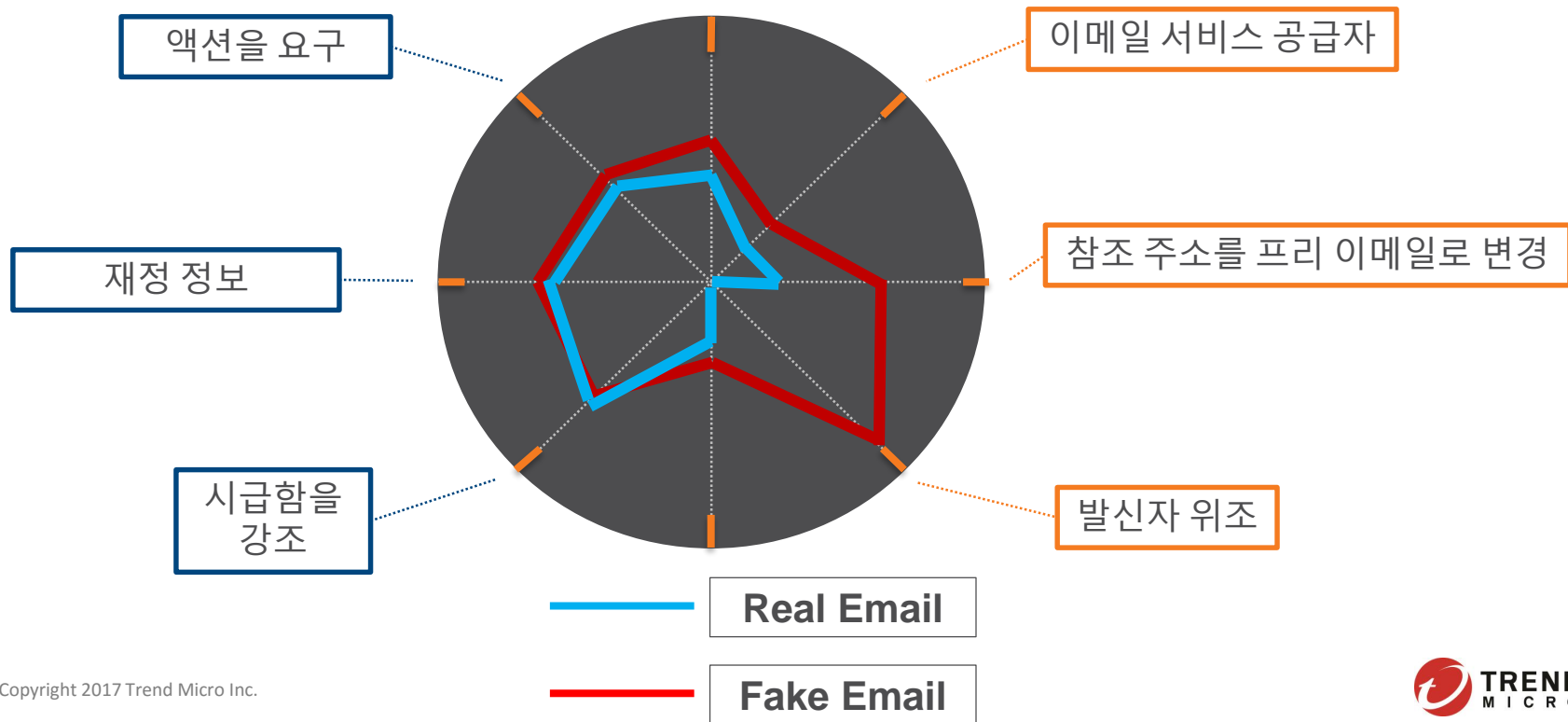
이메일 내의 사표시 요소



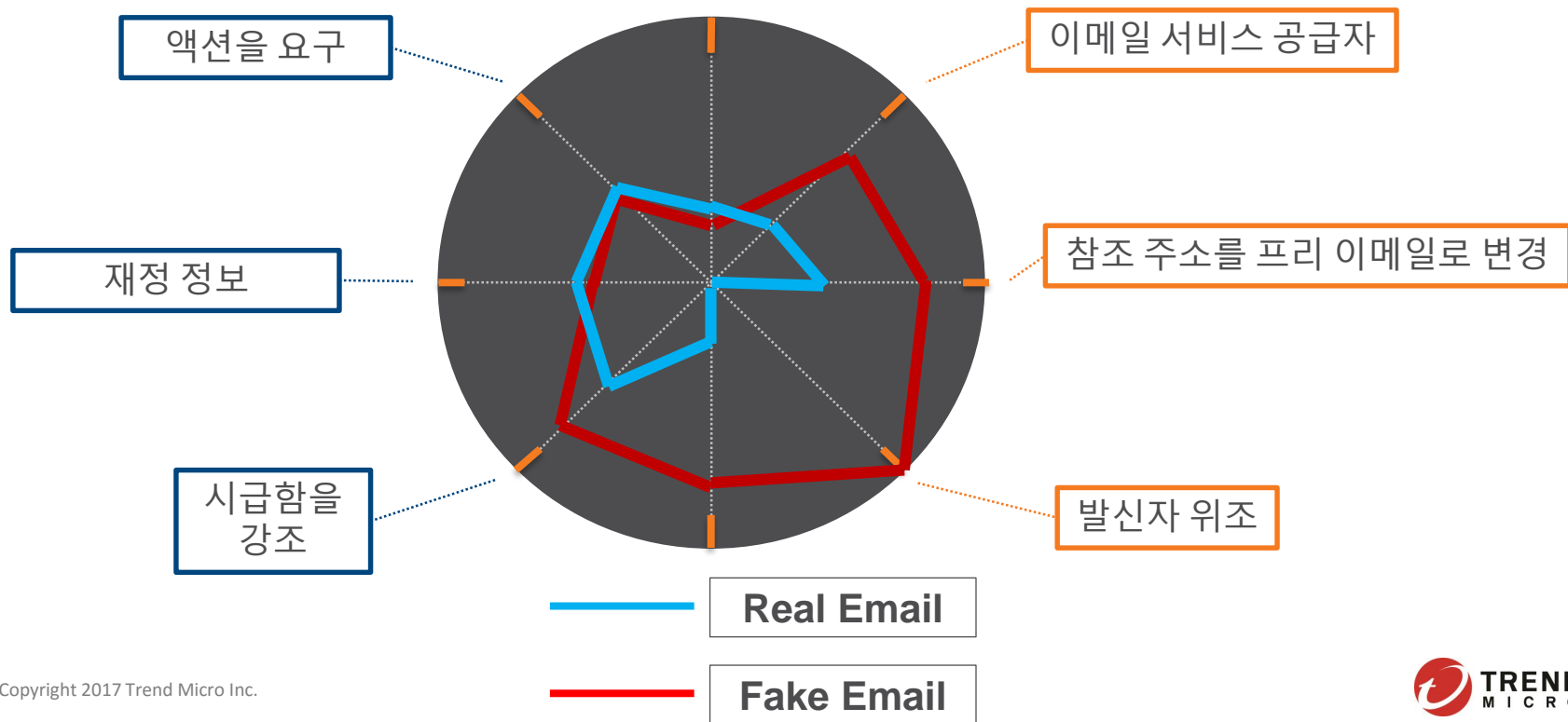
악격자의 행위 요소



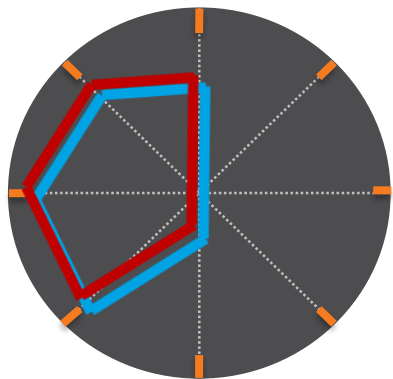
전문가 규칙에서의 관점 → 의심 메일



전문가 규칙 + 머신 러닝 = 사기 메일 탐지

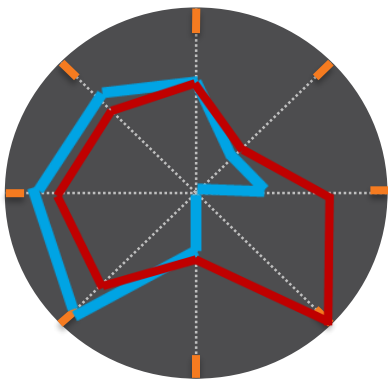


분석의 완성도 향상 = 전문가 규칙 + 머신러닝



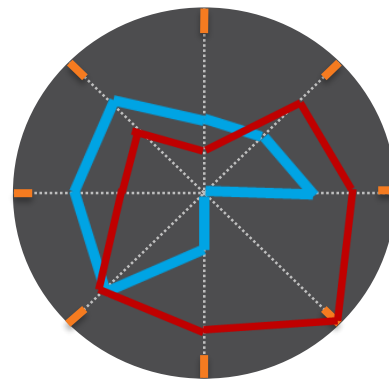
사람

정상?



전문가 규칙

의심



전문가 규칙 +
머신러닝

탐지!

BEC 탐지 설정

You are here: Administration > Scanning / Analysis

Scanning / Analysis

Scanning / Analysis

- Virtual Analyzer
 - Overview
 - Settings
 - External Integration
- Other Settings
 - File Passwords
 - Smart Protection
 - Smart Feedback
 - YARA Rules
 - Time-of-Click Protection
- Business Email Compromise Protection**

High-Profile Users

Given name:* Middle name: ⓘ Family name:*

<input type="checkbox"/>	Given Name ↑	Middle Name	Family Name
<input type="checkbox"/>	andy	a.	wang
<input type="checkbox"/>	jeremy		lin

Records: 1 - 2 / 2 | 10 per page | 1 / 1 | < >

Internal Domains

Domain name:*

<input type="checkbox"/>	Domain Name ↑
<input type="checkbox"/>	trendmicro.ae
<input type="checkbox"/>	trendmicro.co.jp
<input type="checkbox"/>	trendmicro.com

Records: 1 - 3 / 3 | 10 per page | 1 / 1 | < >

BEC 탐지 사례

Detected	Risk Level	Recipients	Email Header (To)	Sender	Email Header (From)	Email Subject	Attachments	Threat	Action
2017-08-26 19:11:58	✘	test@trend.com	cfo@trendmicro.com	test@todd.com	cxo@gmail.com	request ASAP !!	0	Phishing: BEC_CEO-FRAUD.ERS	Quarantined

[View in Threat Connect](#) [View Screenshot](#) [Download](#) (Password: virus)

Overview Message ID: **Details**

Inconsistent sender host names	The Message-ID host name (trendmicro.com) does not match the From host name (gmail.com).
Significant time gap during email message transit	Significant time gap (> 30.0 minutes) detected during email message transit between hops (10.79.75.129 & 192.ddei) from time (Thu, 21 Jan 2016 20:55:50 -0800 (PST)) to time (Sat, 26 Aug 2017 19:11:57 +0000 (UTC)).
Inconsistent recipient accounts	Envelope recipient (test@trend.com) is inconsistent with header recipient (cfo@trendmicro.com).
Short message body	The body text or the HTML text of the email is short. The text length (43/80 characters, for body text/HTML text respectively) may suggest that the email content has little meaning.
Inconsistent host domains or unexpected server-side relay or forward	The sender host (192.ddei) belongs to a different domain from the sender account (cxo@gmail.com). This message may occur from an unexpected server-side relay or forward.

Appendix - Email Security Appliance PoC 구성

PoC 구성 1 - Mirror 포트 사용

1. 외부로부터 메일을 수신

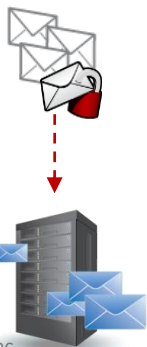


스팸차단 솔루션

SMTP 트래픽을
미러링하여
보안장비로 전송

백본 스위치

2. 메일 배달에는
영향없음



백본스위치의 미러포트와 보안장비를 연결

- SMTP트래픽이 보안장비로 복제되며, 보안장비에서는 행위분석을 진행
- 모든 메일들은 메일서버로 그대로 배달됨 (서비스 영향 없음)
- 총 4개의 미러포트 사용
- 미러포트의 사용이 많을 수록 스위치에서의 부하가 증가하여 미러트래픽 유실이 발생할 가능성이 있음

미러포트

A사 제품



관리 콘솔 접속
패턴/엔진 업데이트 등

관리포트

B사 제품



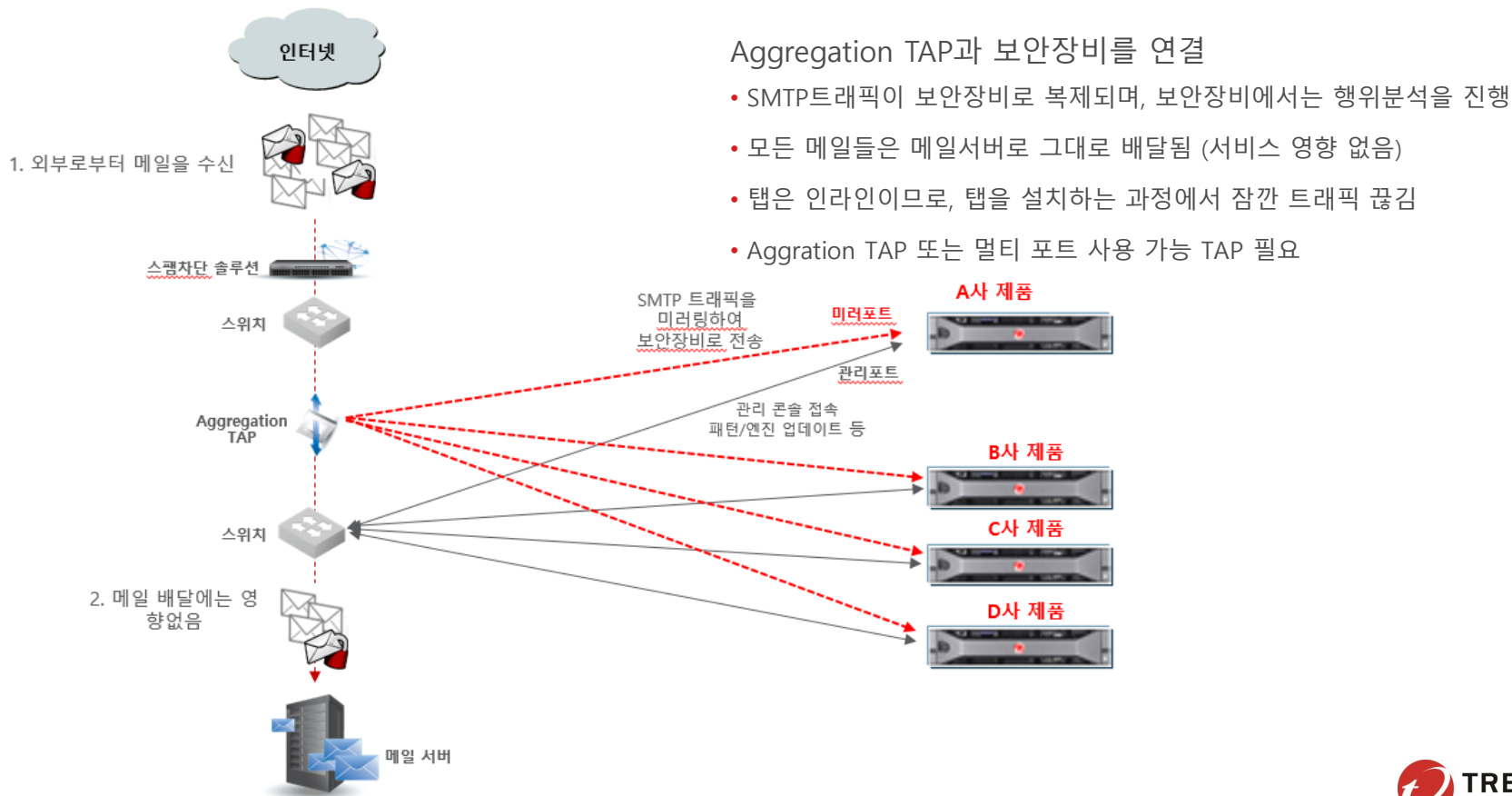
C사 제품



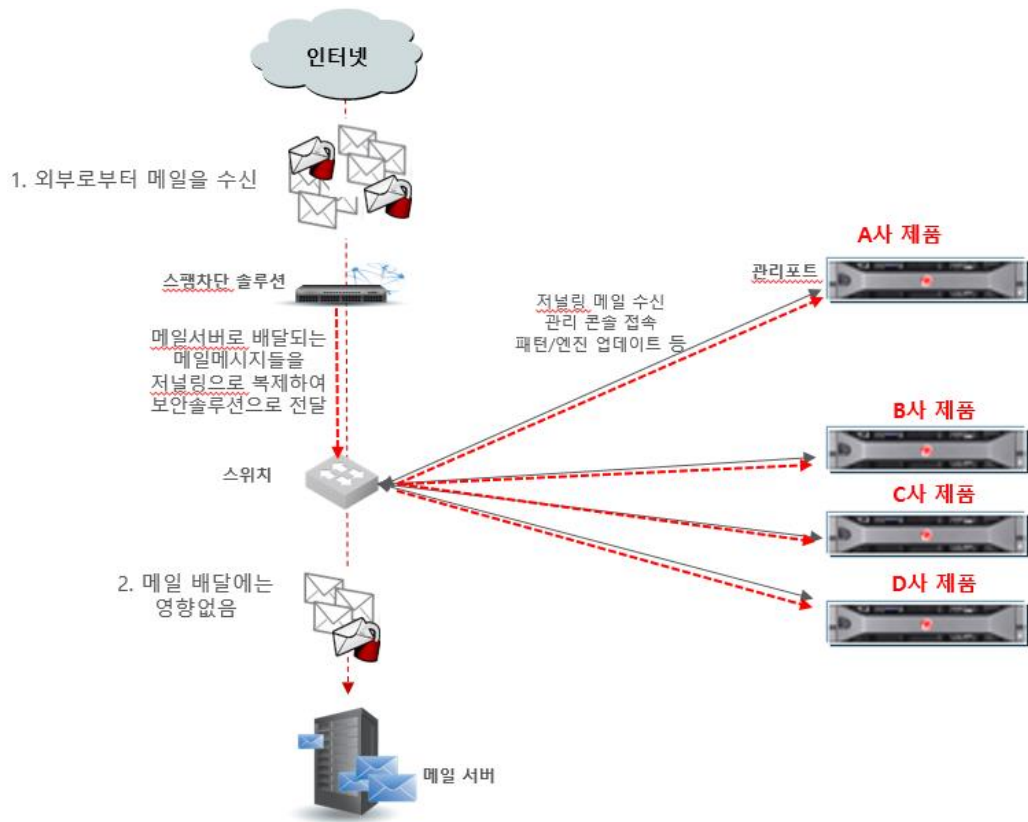
D사 제품



PoC 구성 2 - TAP 사용



PoC 구성 2 – BCC(저널링)모드



스팸차단 솔루션에서 BCC(또는 저널링)를 설정하여

SMTP트래픽이 보안장비로 복제되며, 보안장비에서는 행위분석을 진행

- 모든 메일들은 메일서버로 그대로 배달됨 (서비스 영향 없음)
- 스팸차단 솔루션의 기술지원 필요
- 현재 사용 중인 스팸차단 솔루션에서 이 BCC(또는 저널링)을 지원하는지 확인 필요
- 다수의 IP주소로 BCC(저널링)을 발송할 수 있는지 확인 필요

감사합니다.
