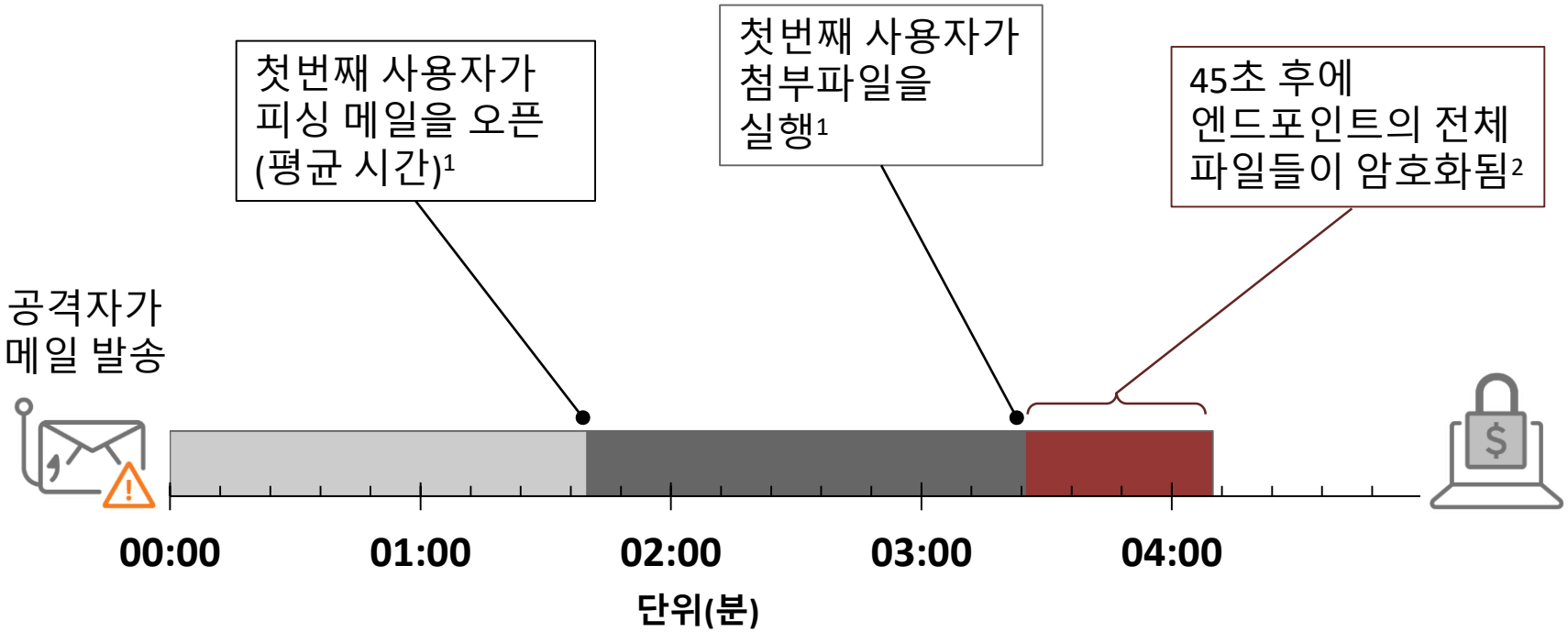
TREND MICRO

Security
TRENDS 2018

보안 위협의 시작점이 되고 있는 이메일 공격에 대한 대응

트렌드마이크로
윤명익 부장

랜섬웨어 공격의 79%는 피싱 이메일을 사용

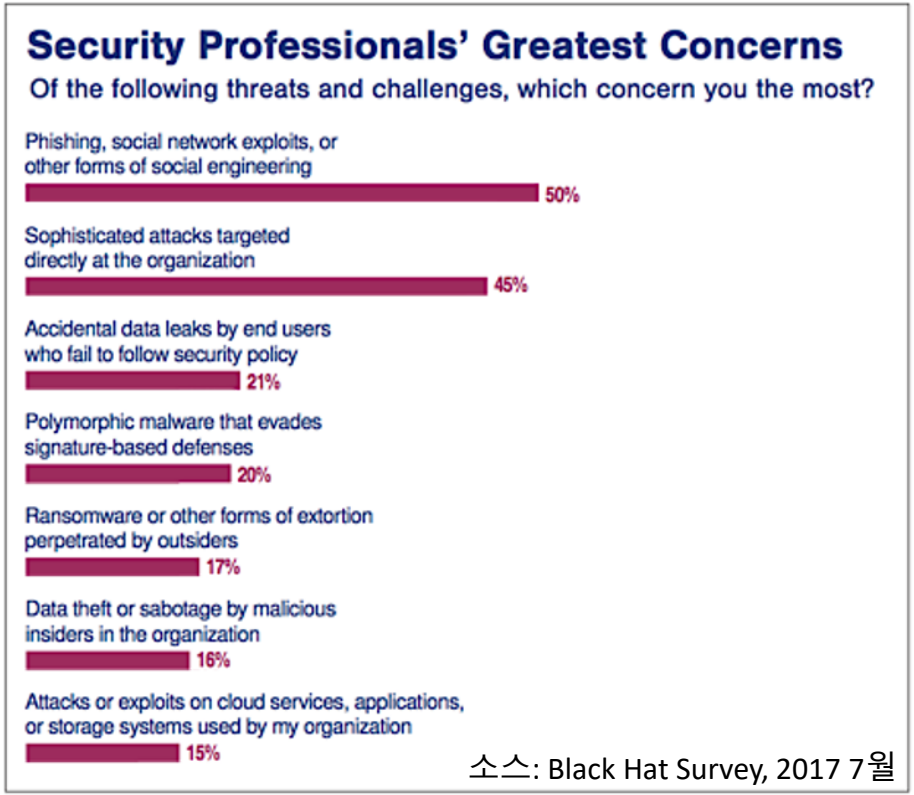


1. Verizon 2016 Data Breach Investigations
2. Teslacript 3.0은 10,000여개의 파일을 40초만에 암호화

이메일 공격이 #1 보안 이슈

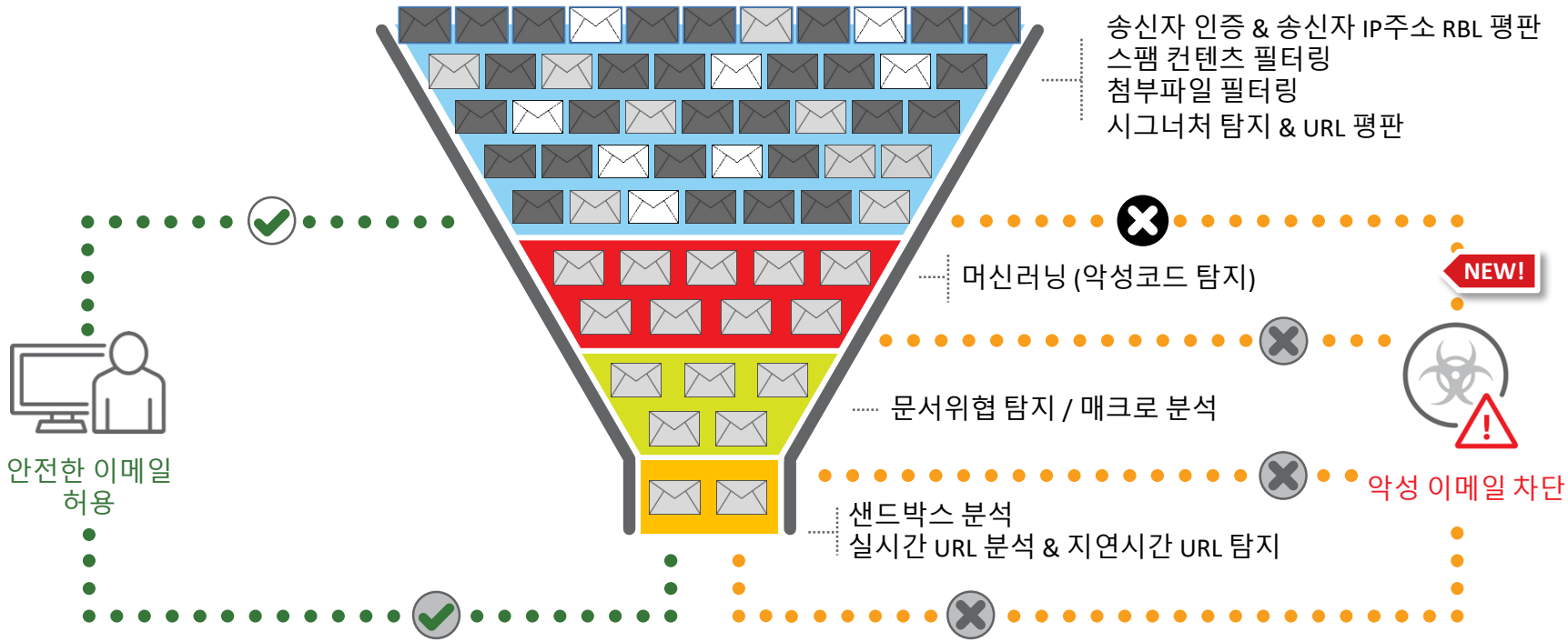
상위 5 관심사는 모두 이메일과 관련

- 피싱
- 타겟 공격
- 정합성
- 악성코드 탐지기술
- 랜섬웨어
- 클라우드 서비스



소스: Black Hat Survey, 2017 7월

계층적 방어를 통한 이메일 방역 필요



Email Inspector Appliance

악성 첨부파일과 악성 URL을 포함한 이메일을 탐지 및 차단하는 이메일 보안 전용 어플라이언스

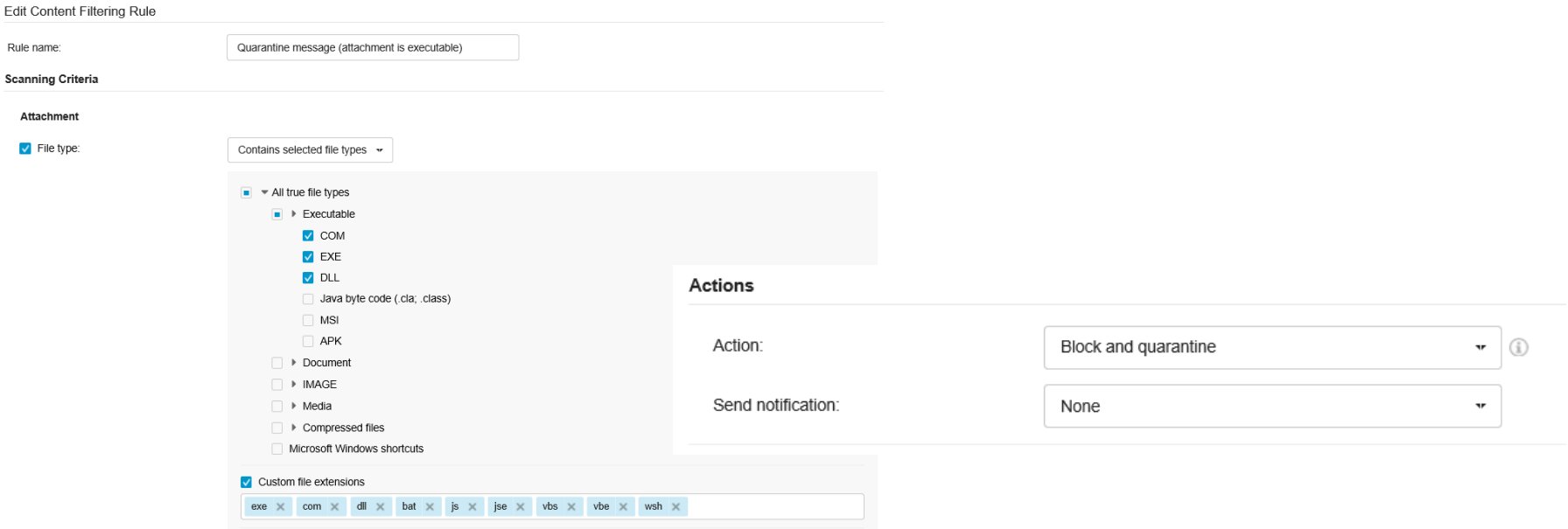
- 사내 표준PC환경과 동일하게 구성하여 첨부파일과 URL을 행위분석하는 커스텀 샌드박스
- 다양한 포맷의 URL 분석
- 암호압축 첨부파일 분석
- 국내외 다양한 스팸차단 솔루션들과 MTA모드(차단모드)로서 안정적으로 호환
- 이기종 네트워크 보안장비들과 탐지 정보 공유

➢ ***이메일을 사용한 타겟 공격 및 랜섬웨어 공격 차단***

이메일 첨부파일 보안

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

TREND MICRO | Security TRENDS 2018

파일 실행 전 탐지 머신 러닝 – 수 천 개의 파일 기능과 기계 학습 모델을 사용하여 악성 파일을 예측 탐지. 샌드박스 이전에 알 수 없는 악성코드를 찾아 이메일 배달 효율성을 향상

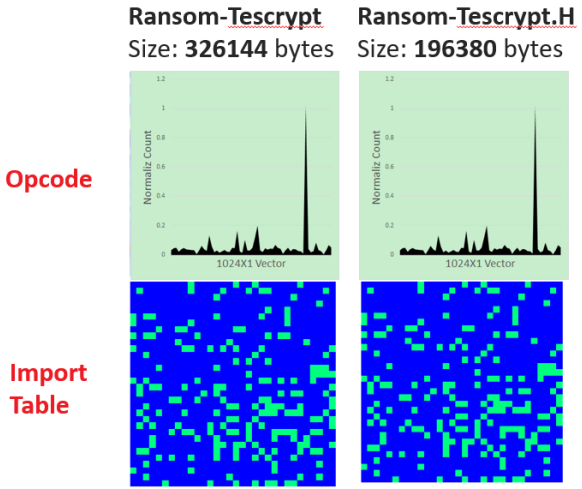
문서 취약점 탐지 – 파일을 구문 분석하여 의도한 애플리케이션에 대한 알려진 악성 및 잠재적 악성 코드를 탐지. 현장에서 새로운 제로 데이 익스플로잇을 탐지하는 기술

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

머신러닝 탐지

- TrendX
  - 파일 실행 전 머신 러닝 탐지
  - 파일 및 동작 기능을 기반으로 한 데이터집합 사용
  - 알려지지 않은 악성 PE파일과 스크립트(JS 등) 탐지

- Macrowave
  - 오피스 매크로 악성코드 탐지용 머신러닝 엔진 적용



문서 취약점 탐지

- 악성코드를 드롭하거나 인젝션하려는 행위를 탐지하기 위하여 문서를 파싱
  - 알려진 익스플로잇을 탐지하여 격리
  - 알려지지 않은 익스플로잇이 내포된 경우 샌드박스로 분석
- 제로데이 취약점을 이용한 A.P.T공격에 대한
- Microsoft Office, PDF, HWP 첨부파일 대응


May 12

Targeted Attack Against Taiwanese Agencies Used Recent Microsoft Word Zero-Day

2:31 am (UTC-7) | by Trend Micro

Share Recommend 34 Tweet 103 +1 4

Vulnerabilities, particularly zero-days, are often used by threat actors as the starting point for targeted attacks. This was certainly the case for a (then) zero-day vulnerability (CVE-2014-1761) affecting Microsoft Word. In its security

샌드박스 분석

TREND MICRO | Security TRENDS 2018

첨부파일과 URL에 대한 다이내믹 샌드박스 분석

- 첨부파일의 악성 행위 탐지(C&C통신, 파일드롭, 보안 무력화, 랜섬웨어 행위, 루트킷, 자동시작 행위)
- 멀티 운영체제 샌드박스에서 동시 분석
- 샌드박스 회피행위 탐지기술
- 네트워크 기반 솔루션과 엔드포인트 백신에도 탐지정보 공유

Risk level:
Notable Characteristics
Anti-security, self-preservation
Autostart or other system reconfiguration
Deception, social engineering
File drop, download, sharing, or replication
Hijack, redirection, or data theft
Malformed, defective, or with known malware traits
Process, service, or memory object change
Rootkit, cloaking
Suspicious network or messaging activity
Other threat characteristics

NSS LABS RECOMMENDED

Trend Micro™ Deep Discovery

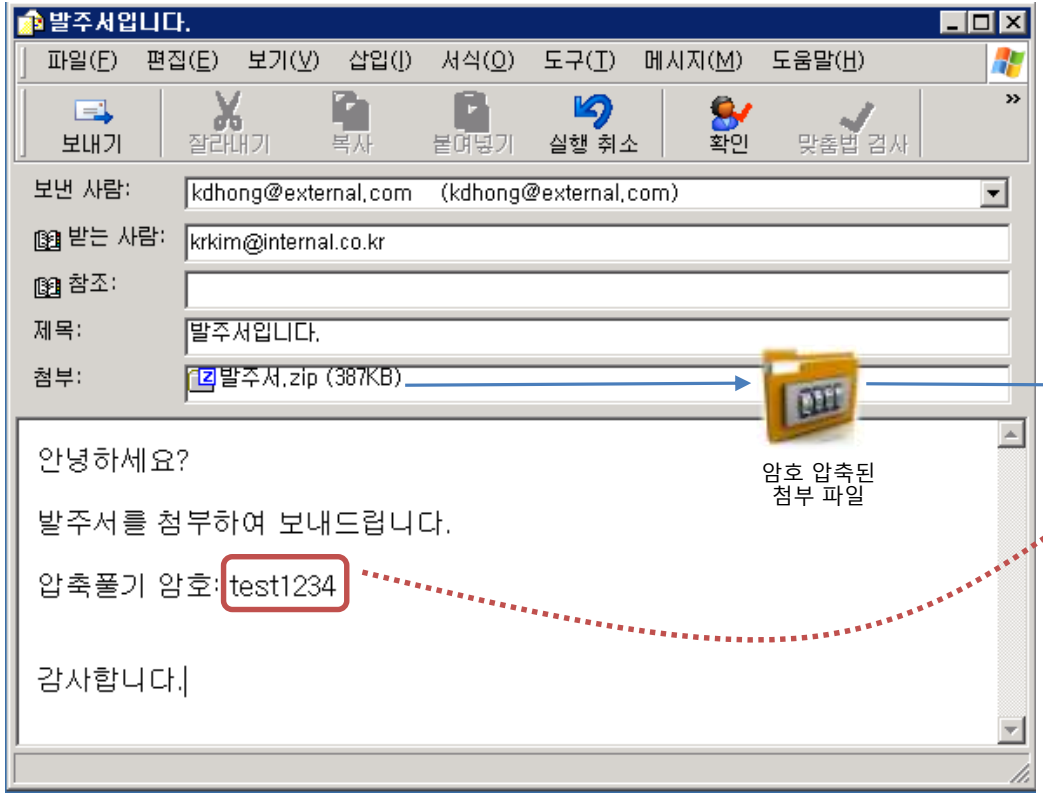
100%

Breach Detection Rate

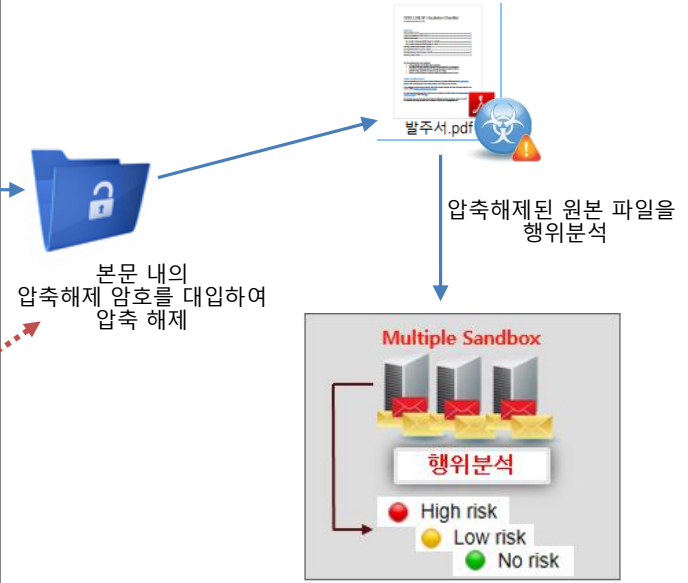
- 2017 -

RECOMMENDED 4 years in a row

암호 압축 첨부파일에 대한 탐지

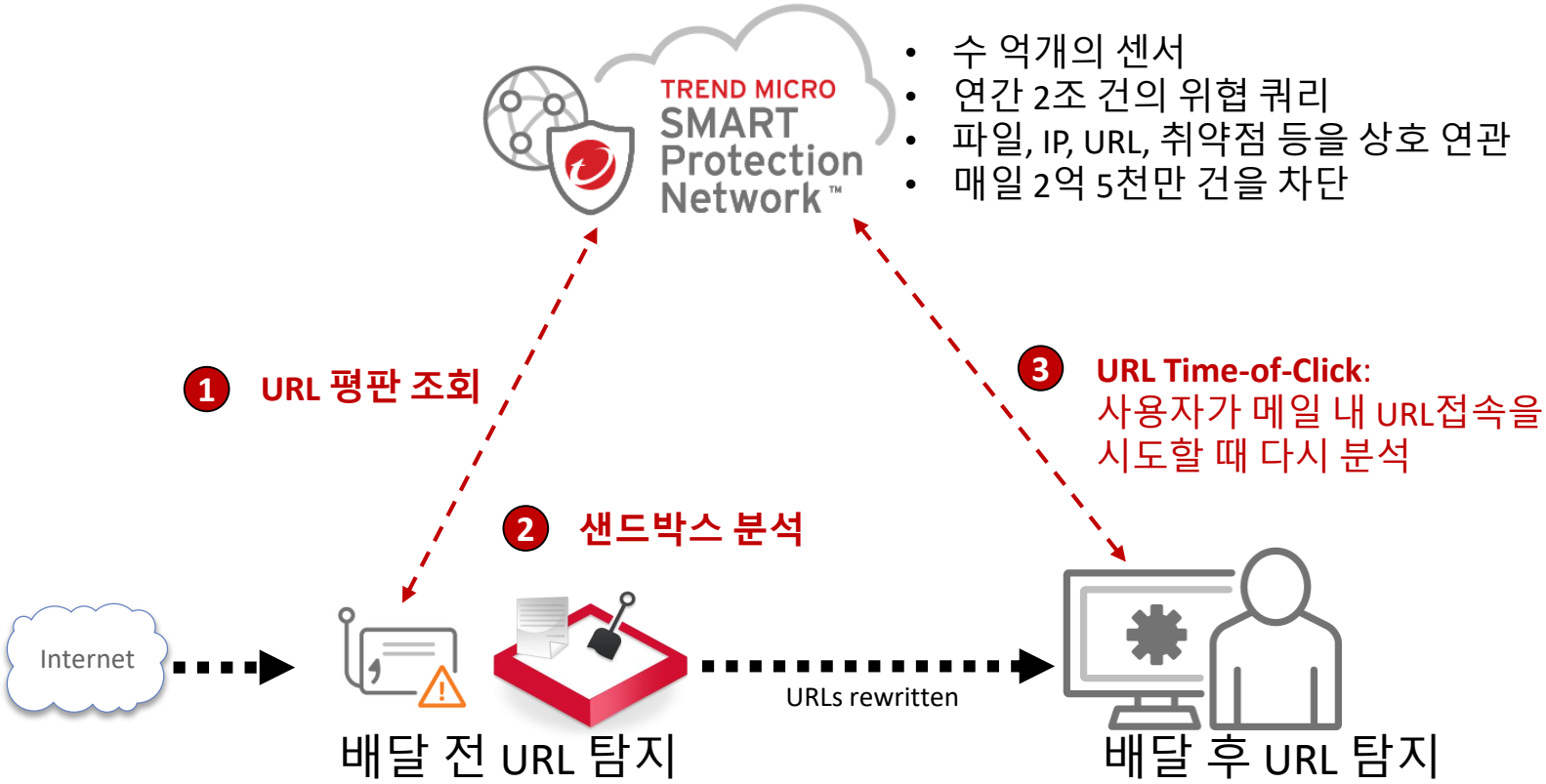


- 메시지 본문 내에 포함된 첨부파일 압축풀기 암호를 사용하여 자동으로 압축해제 및 행위분석



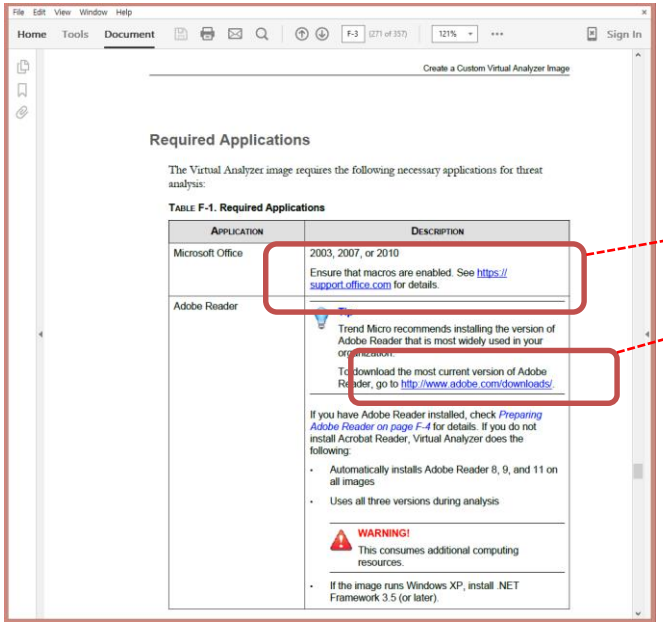
이메일 URL 보안

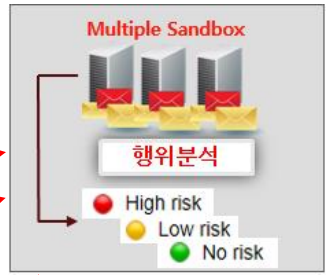
지연시간 악성 URL 클릭 탐지

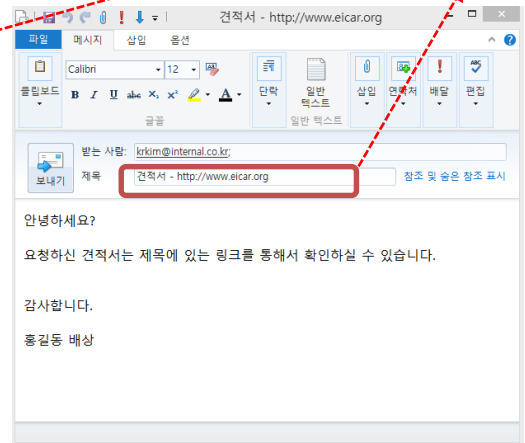


첨부 파일 내 악성 URL 탐지

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

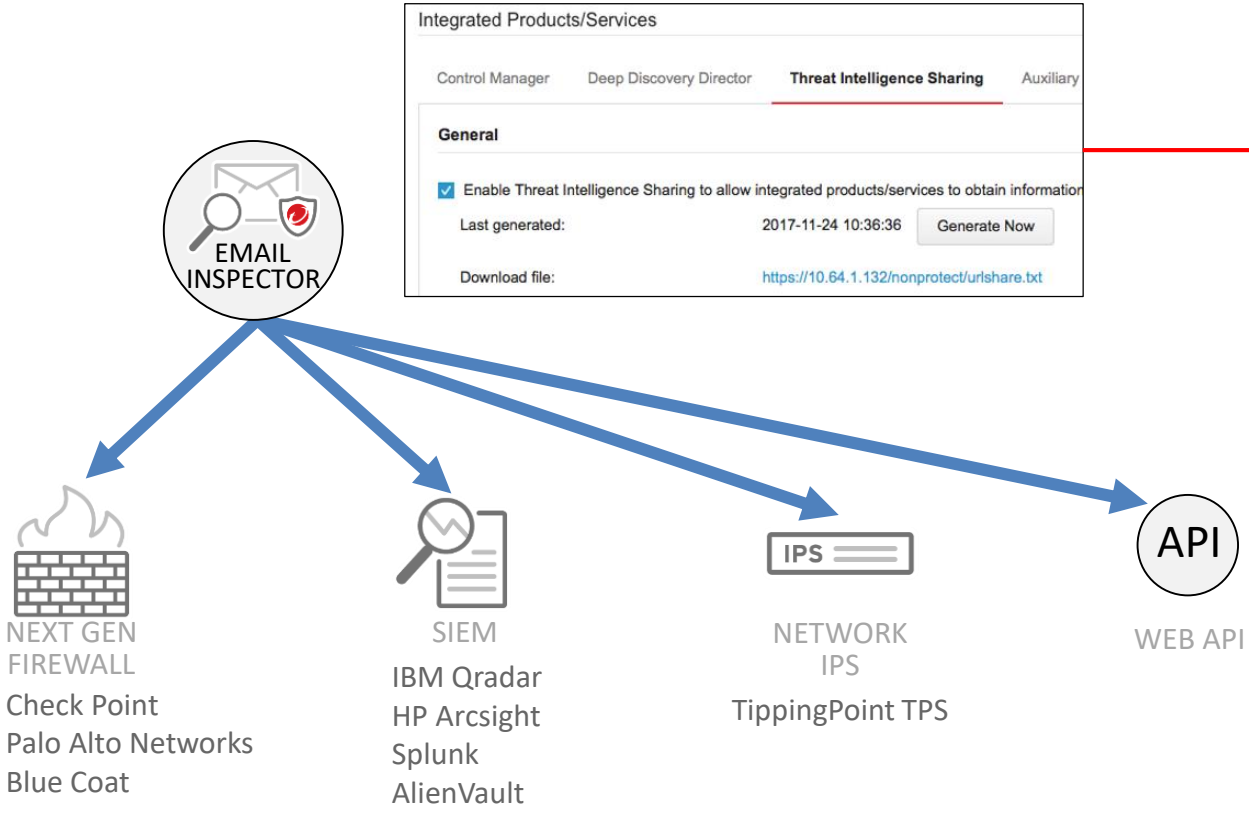


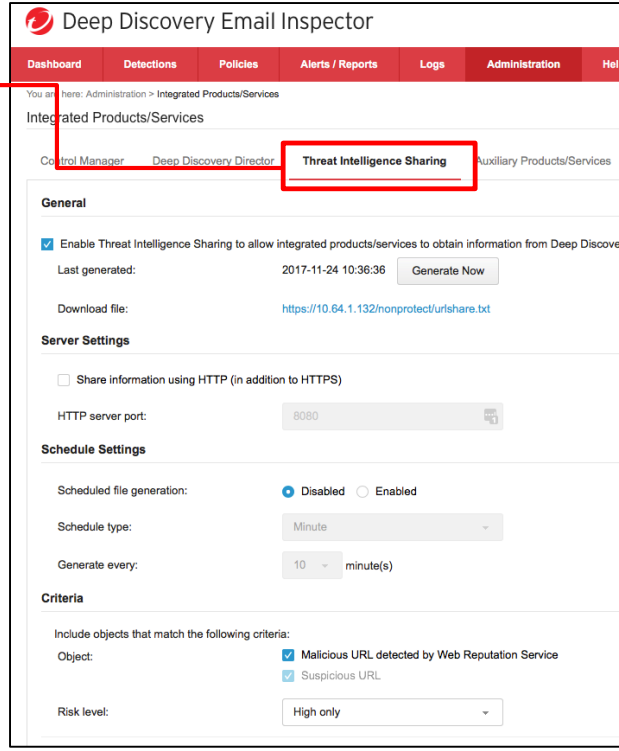




이메일 보안을 통한 네트워크 보호

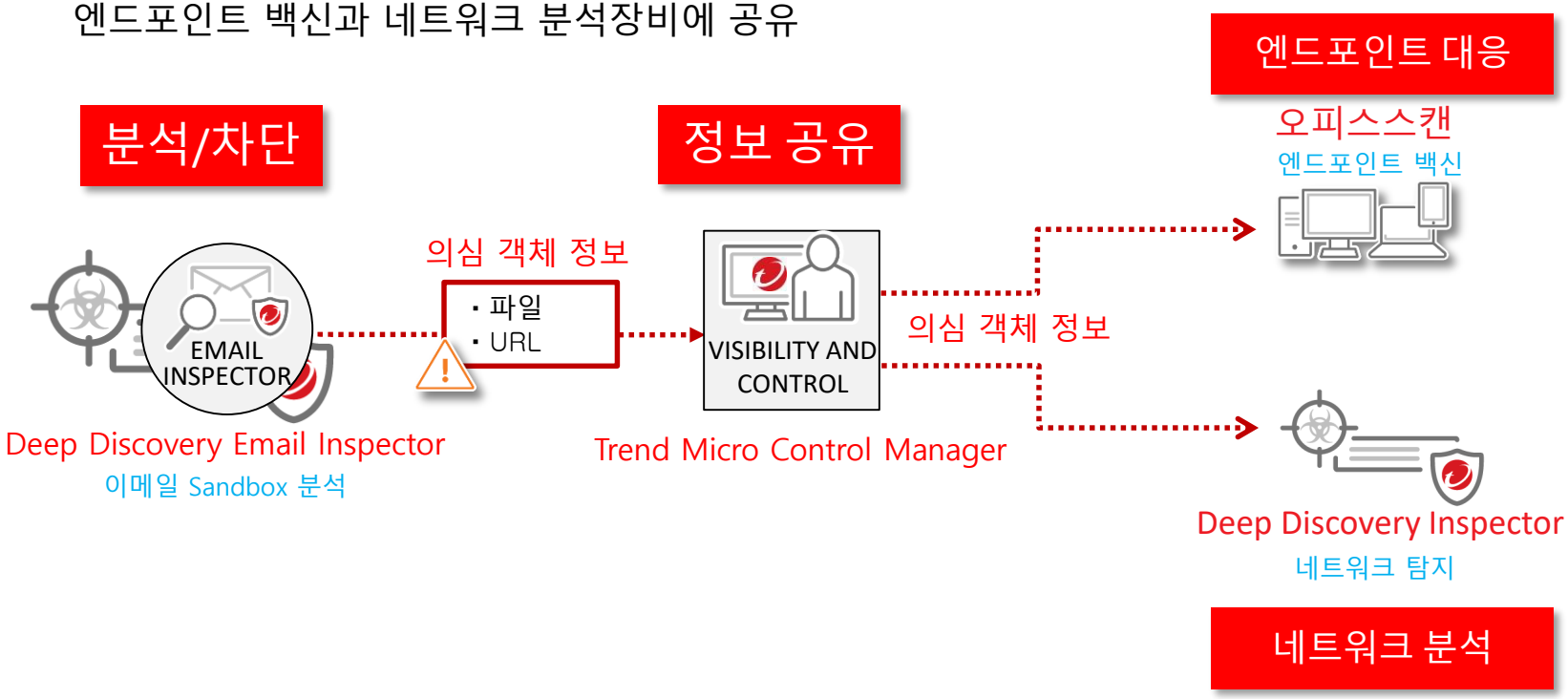
이기종 보안 솔루션 연동


Integrated Products/Services
Control Manager
Deep Discovery Director
Threat Intelligence Sharing
Auxiliary
General
Enable Threat Intelligence Sharing to allow integrated products/services to obtain information
Last generated:
2017-11-24 10:36:36
Generate Now
Download file:
https://10.64.1.132/nonprotect/urlshare.txt
EMAIL INSPECTOR
NEXT GEN FIREWALL
Check Point
Palo Alto Networks
Blue Coat
SIEM
IBM Qradar
HP Arcsight
Splunk
AlienVault
IPS
NETWORK IPS
TippingPoint TPS
API
WEB API


Deep Discovery Email Inspector
Dashboard
Detections
Policies
Alerts / Reports
Logs
Administration
You are here: Administration > Integrated Products/Services
Integrated Products/Services
Control Manager
Deep Discovery Director
Threat Intelligence Sharing
Auxiliary Products/Services
General
Enable Threat Intelligence Sharing to allow integrated products/services to obtain information from Deep Discove
Last generated:
2017-11-24 10:36:36
Generate Now
Download file:
https://10.64.1.132/nonprotect/urlshare.txt
Server Settings
Share information using HTTP (in addition to HTTPS)
HTTP server port:
8080
Schedule Settings
Scheduled file generation:
Disabled
Enabled
Schedule type:
Minute
Generate every:
10
minute(s)
Criteria
Include objects that match the following criteria:
Object:
Malicious URL detected by Web Reputation Service
Suspicious URL
Risk level:
High only

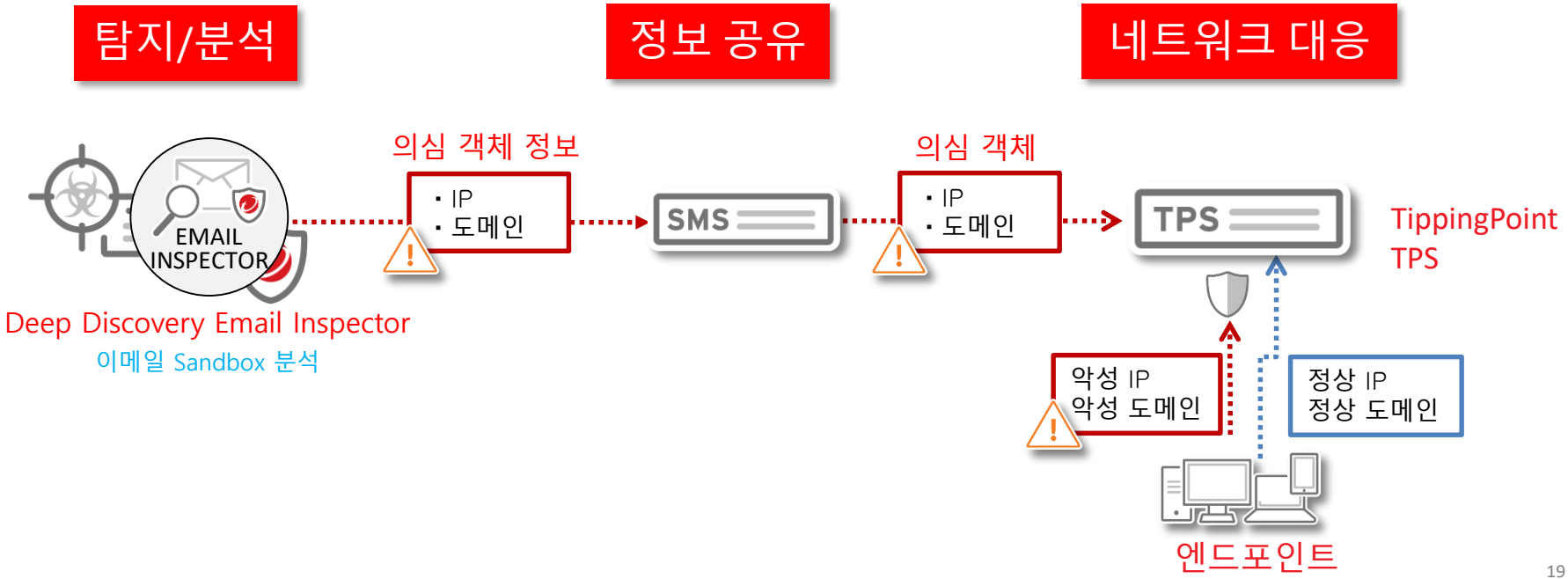
네트워크 & 엔드포인트 연동

Connected Threat Defense : 이메일 APT장비에서 샌드박스 분석으로 탐지된 의심 파일/URL을 엔드포인트 백신과 네트워크 분석장비에 공유



네트워크 사전 차단

이메일 APT장비에서 샌드박스 분석으로 탐지된 의심 IP/도메인(의심객체정보)을 IPS 정책에 자동 반영



TREND MICRO

Security
TRENDS 2018

THANK YOU

트렌드마이크로
윤명익 부장