Trend Micro™

Deep Discovery Email Inspector

이메일로 유입되는 랜섬웨어와 A.P.T 차단 솔루션

랜섬웨어와 A.P.T 공격은 전통적 방식의 보안을 쉽게 통과하여 기업의 민감한 데이터와 지적 재산을 유출합니다. 이러한 공격의 90% 이상은 기존 구축되어 있는 이메일 또는 엔드포인트 보안에서 탐지하지 못하는 악성 첨부파일과 URL이 포함된 스피어 피싱 이메일을 통해 이루어집니다.

Deep Discovery Email Inspector 는 기업 데이터를 공격하는 랜섬웨어와 타겟형 메일을 탐지 및 차단하는 프로그램입니다. 멀웨어 탐지 엔진, URL 분석, 파일과 웹 샌드박싱 기술을 적용하여 바이러스에 감염된 이메일을 감지, 차단 또는 격리합니다.

Trend Micro™ Deep Discovery

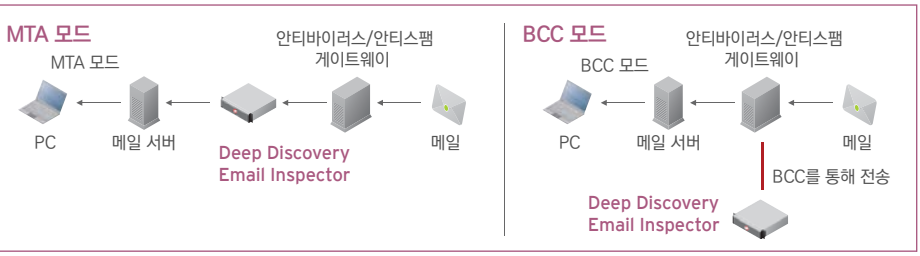
세계적인 보안평가기관 NSS Lab

2년 연속 최고 보안 등급 획득

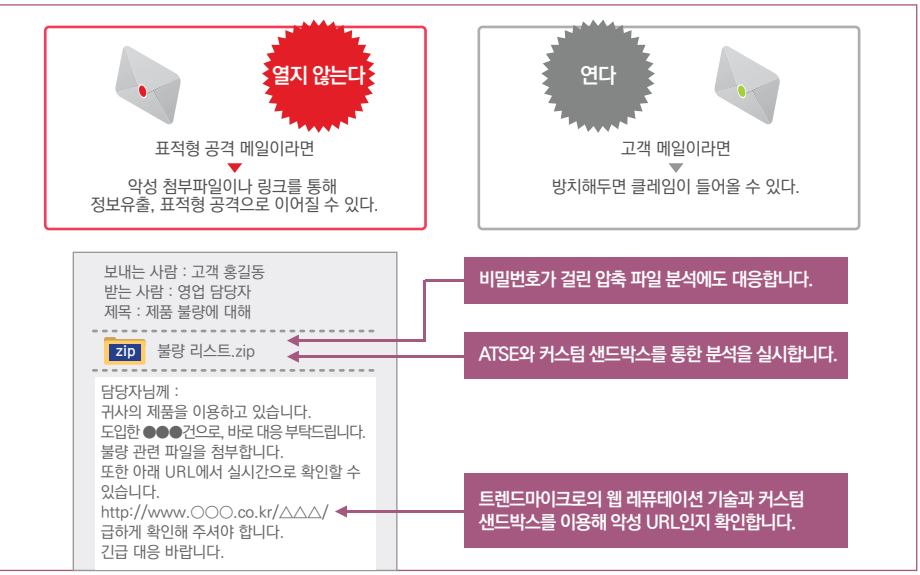
NSS LABS RECOMMENDED

정보유출탐지 시스템 테스트

Deep Discovery Email Inspector 시스템 구성도



소셜 엔지니어링 수법을 이용한 메일 공격의 예



특징 및 주요이점

- 이메일 첨부파일 분석
- 문서 위협 감지
  문서 첨부파일 위협코드 감지. 알려지지 않은 새로운 공격에 대한 샌드박스 시뮬레이션 통한 공격 감지 및 격리
- 맞춤형 샌드박스
- 웹 검증
- 관리 및 배치의 유연성
  MTA(블로킹) 또는 BCC(모니터링) TAP/SPAN 모드를 다른 이메일 보안 솔루션과 동시 배치, 활용이 가능.

랜섬웨어 탐지 화면

Advanced Threat Indicators

Period: Last 30 days — Last update: 2016-03-28 10:40:00

Indicator	High	Medium	Low	Total
Documents with exploit code	20	0	0	20
C&C callback (upon execution)	17	7	0	24
Ransomware detections	0	11	0	11

랜섬웨어 행위 탐지 통계

Hijack, redirection, or data theft (22)

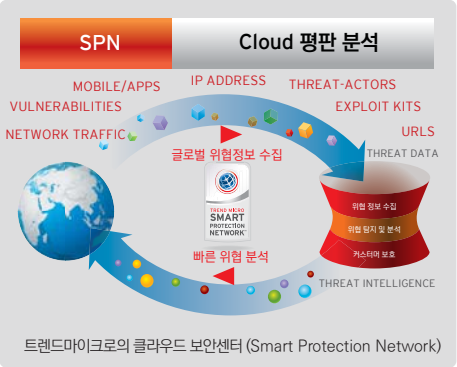
Characteristic	Details	Exhibited by
Accesses decoy file	E:\project.ppt	details_7e9f38.js
Accesses decoy file	E:\project.pptx	details_7e9f38.js
Accesses decoy file	E:\account.xlsx	details_7e9f38.js
Accesses decoy file	E:\contact.pst	details_7e9f38.js
Accesses decoy file	E:\agreement.docx	details_7e9f38.js

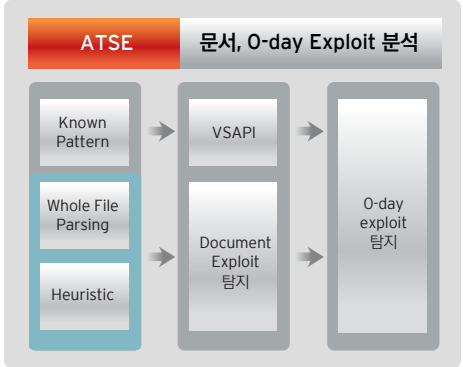
MS Word, Powerpoint, Excel 문서 등을 암호화하기 위해서 문서 오픈 시도 탐지

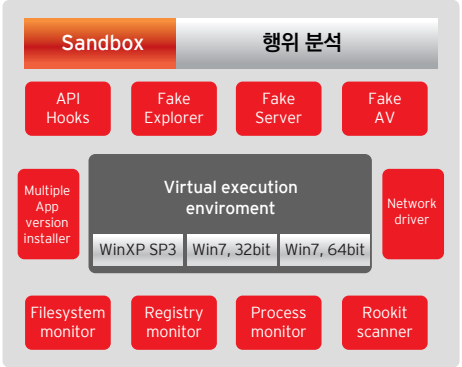
URL	Site Category	Risk Level	Threat	Accessed By
http://[redacted].10	Unrated	Unavailable	-	inv_09861.js
http://[redacted].8/main.php	Ransomware,Disease Vector	Medium	WEB-THREAT_RANSOMWARE.WRS	inv_09861.js
http://[redacted].10/main.php	Ransomware,Disease Vector	Medium	WEB-THREAT_RANSOMWARE.WRS	details_7e9f38.js
http://[redacted].116/main.php	C&C Server	Medium	CALLBACK_GENERIC.WRS	details_7e9f38.js

랜섬웨어 유포 웹사이트와 C&C서버에 접속하는 행위 탐지

3단계 분석 (평판 - 정적 - 동적)







주요 기능

첨부파일 분석 및 샌드박싱

멀웨어 탐지전용 엔진과 맞춤형 샌드박스를 통해 MS 오피스, PDF, ZIP, JAVA 등 WINDOWS에서 실행되는 다양한 종류의 첨부파일을 진단합니다.

URL 분석 및 샌드박싱

첨부된 문서 내의 URL을 포함하여 이메일 본문 및 제목에 포함된 URL을 웹 레퓨테이션 검사를 진행합니다. URL 연결 최종 컨텐츠를 스캔 및 샌드박싱하여 리다이렉트, 지능형 멀웨어, 익스플로잇, drive-by-download를 검사합니다.

EMAIL 정책관리

경고 심각도 수준에 따라 악성 이메일의 격리, 삭제, 태그하여 전달 등 다양한 옵션을 설정할 수 있습니다. 또한, 첨부파일 형태에 따라 이메일 샌드박스 진행여부를 맞춤 설정할 수 있습니다. 실시간 이메일 경고 설정을 통해 알려진/알려지지 않은 위협의 탐지를 관리자에게 즉시 알립니다.

위협 감지

추가 위협 분석을 위한 세부 샌드박싱 탐지가 가능합니다.

Deep Discovery 플랫폼

Deep Discovery Email Inspector는 네트워크, 이메일, 엔드포인트의 통합 보안을 담당하는 Deep Discovery 솔루션 그룹 중 하나입니다. 따라서, 각 기관에서 필요로 하는 곳에 A.P.T 공격에 대응하는 보안을 구축할 수 있습니다.

침해정보 수집센터

침해정보 수집센터에서 트렌드마이크로 글로벌 인텔리전스를 공유하여 잠재적인 공격 위협과 출처에 대한 정보를 얻을 수 있습니다.

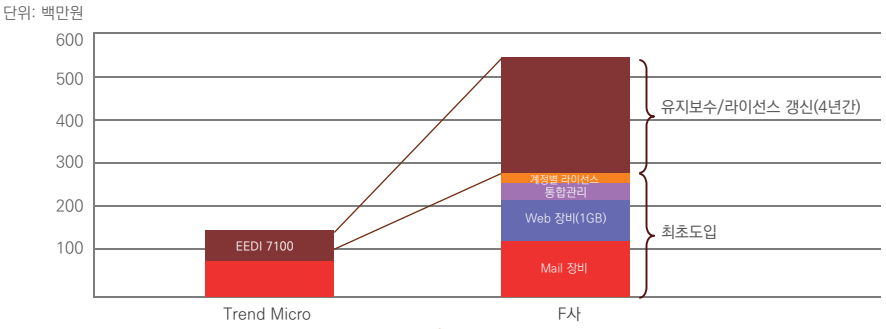
암호 인텔리전스

휴리스틱 기법과 고객이 제공하는 키워드를 사용하여, 암호로 보호된 파일과 ZIP 파일 해독을 통해 첨부파일의 안전성을 파악합니다.

2015 NSS Labs 정보유출탐지 테스트

제품	Trend Micro	F사
• Web을 통한 공격 탐지	100%	69.1%
• E-Mail을 통한 공격 탐지	100%	30.6%
• 회피 방지율	99.6%	87.1%
• 보안 효과	96.2%	51.8%

이메일 APT 방어를 위한 위한 TCO(5년) 비교



DDEI

- E-mail 첨부 파일 분석
- E-mail 포함 URL 분석
- 별도 라이선스 불필요

F사

- Mail 장비 – E-mail 첨부 파일 분석
- Web 장비 – E-mail 포함 URL 분석
- 관리 장비 – Web 장비에서 Mail 장비로 URL을 전송하기 위해 필수
- E-mail 계정수별 라이선스