# **악성코드 모의훈련 결과보고서**

## **1. 개요**

**훈련 목적**: 이메일 기반 침해 시나리오를 재현하여, 매크로 기동형 악성코드의 행위 특성과 탐지/대응 절차를 검증

**훈련 범위**:  
암호화 압축 첨부 메일 수신 → 압축 해제 → 엑셀(.xlsm) 열람  
매크로(Workbook\_Open) 트리거로 PE 실행  
PE.exe가 PowerShell 5종 실행 및 CMD 정보수집 수행

**훈련 환경**: Windows 11

**훈련 방식**: 단계별 공격 체인(피싱 메일 → 매크로 실행 → 권한 상승 → C2 연결 → 추가 페이로드 실행 → 정보수집/레지스트리 변조) 수행 및 분석

**제한 사항**: 실제 시스템 변경



## **2. 내용**

## 

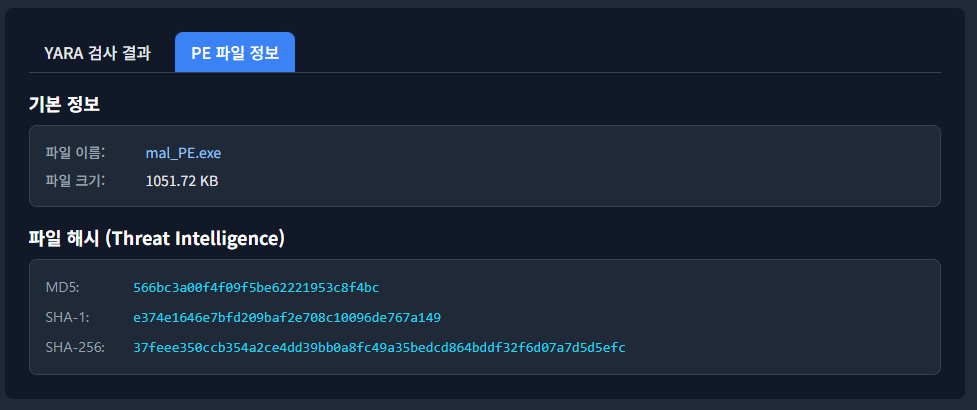
## 

## 

## **3. 파일 정보**

**파일명**: **mal\_PE.exe** = **1051.72 KB**

**해시 정보**:  
MD5: 0bd3e4fd91cd20e8e8587250e4b6e0b3  
SHA-1: 7f2ed5c1f7f38dcd550b2469c3f3258c5ba3d776  
SHA-256:c89a57d236b7b9bd4b3ff499b6f55413067266fd63090a771161bd5f6cd3caf3



## 

## 

## **4. 정적 분석**

**Excel(xlsm) 파일**

* AutoOpen 이벤트 기반 매크로 포함.
* 실행 시 RestartExcelAsAdmin, DisableUAC, DownloadFile 함수 호출 구조 확인.
* 관리자 권한 탈취 → UAC 비활성화 → 외부 Final\_PE.exe 다운로드·실행 흐름.

**PE 실행 파일 (mal\_PE.exe)**

* Windows **PE32 구조** 확인.
* 코드 내부에서 winreg, subprocess 모듈 호출 → 레지스트리 조작 및 CMD/PowerShell 실행 가능.
* 문자열 난독화 및 **UPX 패킹 흔적** 존재.
* systeminfo, ipconfig /all 등 정보수집 명령 호출 흔적 존재.
* 외부 C2 서버 연결 및 추가 페이로드 다운로드 가능성 확인.

## **4.1.파일 구조 분석 (PE 구조)**

* **DOS Header**: MZ 시그니처 확인, 표준 PE 파일 구조 유지.
* **PE Header**: Machine 값 0x14c(Intel 386), NumberOfSections = 5 (텍스트, 데이터, 리소스 등).
* **Section 구조**
  + .text : 실행 코드 포함, 일부 난독화된 문자열 존재.
  + .rdata : API 호출 테이블 저장.
  + .data : 변수·구성 데이터.
  + .rsrc : 리소스 섹션, 아이콘 및 버전 정보.
  + .UPX : 압축된 코드 영역으로 추정 (패킹 확인).
* **엔트리 포인트**: .text 영역 내 존재, WinMainCRTStartup 호출로 진입.

## **4.2.임포트 테이블 및 문자열 분석**

* **주요 API 호출**
  + CreateRemoteThread, VirtualAlloc, WriteProcessMemory → 메모리 상 코드 주입 시도
  + RegSetValueExA, RegCreateKeyExA → 레지스트리 생성 및 수정
  + URLDownloadToFileA, WinHttpOpenRequest → 외부 네트워크 연결 및 다운로드
  + ShellExecuteA, CreateProcessW → 명령 실행
* **문자열 예시**
  + "cmd.exe /c powershell -ExecutionPolicy Bypass" → PowerShell 실행 우회
  + "systeminfo", "ipconfig /all", "tasklist" → CMD 기반 정보수집
  + "HKEY\_LOCAL\_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Run" → 지속성 확보 (자동실행 등록)

## 

## 

## **5. 악성 행위 요약**

## **권한 상승 시도**

## 매크로 실행 시 현재 Excel 프로세스를 종료하고, 동일 파일을 관리자 권한으로 재실행하도록 유도.

## 이후 레지스트리 변경을 통해 UAC(User Account Control) 보안 기능 비활성화 시도.

**원격 코드 실행 및 페이로드 다운로드**

* 관리자 권한 확보 후, 외부 서버(구글 드라이브 등)에 업로드된 실행 파일(.exe) 및 PowerShell 스크립트(.ps1)를 다운로드.
* 다운로드된 파일은 로컬에 저장된 뒤 자동 실행됨.

**추가 악성 행위 실행**

* 다운로드된 실행 파일 실행 시, 추가적인 악성 행위(예: 시스템 정보 수집, 원격 명령 실행, 지속성 확보, C2 서버 통신 등) 수행 가능.

**보안 회피**

* UAC 비활성화를 통해 보안 경고 없이 악성 행위 수행 가능하도록 환경 조작.

## 

## **6. 탐지 및 대응 방안**

**1.탐지 체계 강화**

* EDR/XDR 솔루션 활용해 CreateRemoteThread, VirtualAlloc 등 메모리 기반 공격 행위 모니터링
* 이메일 게이트웨이에서 매크로 포함 문서 및 암호화 압축 파일 필터링 정책 강화
* 정기적 YARA 룰 업데이트 및 IOC 기반 탐지 적용

**2. 대응 방안**

* 감염 PC 즉시 격리 및 포렌식 조사
* 도메인 차단 및 내부 로그 확인
* 관리자 계정 비밀번호 초기화 및 AD 계정 감사

**3. 재발 방지 대책**

* 전사적 보안 인식 교육(매크로 실행 경고, 의심 파일 실행 금지)
* 매크로 기본 차단 정책 적용 (Microsoft Office 보안 설정)
* 주기적 패치 및 취약점 관리 체계 강화
* 최소 권한 원칙 적용, 불필요한 관리자 권한 제거