







엑셀을 이용한 악성코드 공격 시나리오

구분	내용
일시	2025. 7. 18(금)
분석팀	2조(김다영, 서지민, 이우영, 임홍지)
악성 행위 요약	본 악성코드는 Excel 매크로를 이용하여 관리자 권한으로 악성코드 파일을 실행시키는 전형적인 문서 기반 공격 유형입니다.
시나리오 설명	<ol style="list-style-type: none"> 1. 직원의 이메일로 압축+암호화된 엑셀 파일 전송 2. 직원은 이메일을 열어보고 실행 3. 매크로 동작 <ul style="list-style-type: none"> - 엑셀 재시작 후 관리자 권한으로 실행 4. 관리자 엑셀에서 매크로 동작 <ul style="list-style-type: none"> - 특정 구글 드라이브에서 파일 다운로드 - 다운로드한 파일 압축 해제 후 bat 파일 작업 스케줄러에 등록 - UAC 해제 5. 컴퓨터 재부팅 시 run_scenario.bat 파일(관리자 권한으로) 자동 실행
실행 결과	<p>run_scenario.bat : scenario.ps1, scenario.bat 파일 자동 실행</p> <p>scenario.ps1</p> <ul style="list-style-type: none"> - '자동으로 표준 시간대 설정'을 '끔'으로 변경 - 화면보호기 설정을 '없음'으로 변경 - 네트워크 및 계정 정보 수집 결과를 ps1_netinfo.txt로 저장 - 실행 중인 프로세스 목록 저장 결과를 ps1_processlist.txt로 저장 <p>scenario.bat</p> <ul style="list-style-type: none"> - 자동 실행 등록 - 방화벽 해제 - UAC 해제 - Userinit 값 수정 - 환경 변수 PATH에 경로 추가 - 명령어 결과 저장 (bat_result.txt) <ul style="list-style-type: none"> - systeminfo - whoami - netstat - ipconfig - tasklist <div>  bat_result.txt  ps1_netinfo.txt  ps1_processlist.txt  run_scenario.bat  scenario.bat  scenario.ps1 </div>

Yara 탐지 결과

정상 : 5 주의 : 0 심각 : 2

파일명	수준	탐지	상세내용
C:\Users\SBA\Downloads...	정상	미검출	
C:\Users\SBA\Downloads...	심각	검출	Path : C:\Users\SBA\Downloads\scenario (1)\bat_result.txt, File...
C:\Users\SBA\Downloads...	심각	검출	Path : C:\Users\SBA\Downloads\scenario (1)\scenario.bat, File...
C:\Users\SBA\Downloads...	정상	미검출	

- 현재 특정 command(whoami)를 찾는 rule을 실행하여 2개를 탐지하였다.
/* version : 2025.07.18.7 */

```
rule Detect_whoami {
    strings:
        $s1 = /whoami/i
    condition:
        $s1
}
```

탐지 및 대응방안

[탐지 방안]

1. 이메일 및 문서 첨부파일 분석

- 모든 외부 이메일 첨부파일(.xlsm, .docm 등)에 대해 사전 정적 분석 시스템 연동
- YARA 를 기반 탐지 솔루션 운영 (EXE/문서 파일 내 .text, .rsrc, API 호출 등 탐지)
- 샌드박스 시스템에서 Office 파일 열람 시 매크로 동작 추적 (API, PowerShell 실행 여부 감시)

2. 실시간 행위 기반 탐지

- EDR(Endpoint Detection & Response)을 통한 이벤트 감지
(excel.exe → cmd.exe / powershell.exe 실행 등)

3. 파일 무결성 및 해시 기반 탐지

- 사내 실행파일(exe) 무결성 검사
- 신규 또는 미등록 .exe 자동 격리 + 보안팀 알림 정책 적용
- 정기적인 파일 해시(MD5, SHA-256) 목록 관리

[대응 방안]

1. 관리적 보안 조치

- 전사 보안 교육 강화 (매크로 위험성, 의심 문서 대처법 등)
- 의심 문서 수신 시 정보보안팀에 신고 절차 마련
- 업무상 허용된 실행파일/스크립트 목록만 허용 (허용목록 기반 정책) 운영

2. 기술적 보안 통제

- Office 문서에 대한 매크로 실행 기본 차단 정책 적용 (GPO 또는 Intune)
- 실행파일 및 매크로 포함 문서는 격리된 가상환경에서만 열 수 있도록 구성 (VDI, 가상 샌드박스)
- UAC 설정 강제 고정 (레지스트리를 통한 변경 금지 → 보안 정책 적용)
- 다운로드 폴더, 임시 폴더 실행권한 제한 (AppLocker, WDAC)

3. 로깅 및 포렌식 대응

- powershell, cmd, regedit 관련 이벤트 로깅 (Event ID 4688 등)
- Sysmon, Wazuh, Elastic 등을 통해 프로세스 간 행위 추적
- 의심 프로세스/해시 기반 차단 자동화 (SOAR 연동)