2025.06

WannaCry 랜섬웨어 대응 플레이북

Wannacry Ransomware Playbook

시큐리티아카데미 SK쉴더스 트랙

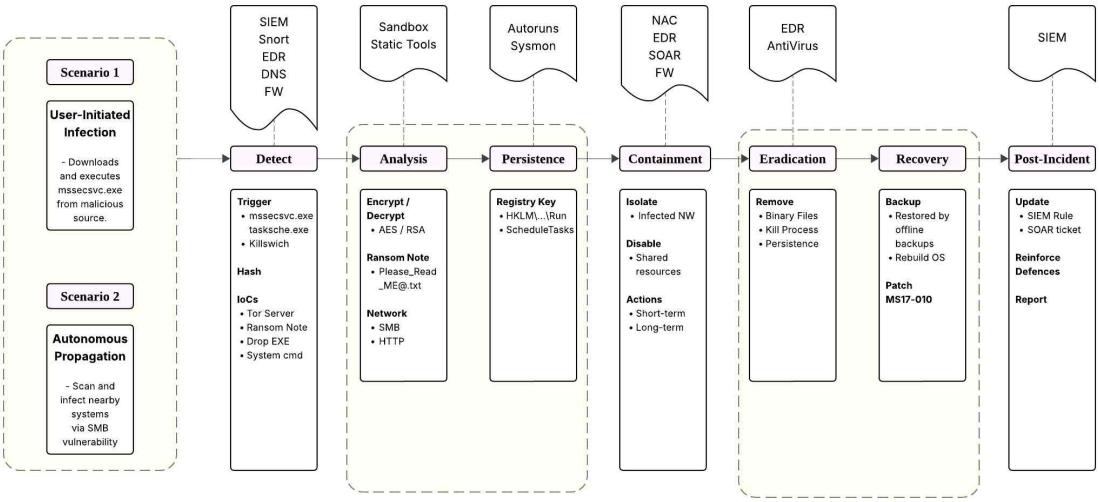
워너스마일

멘토 : SK쉴더스 조원준 수석

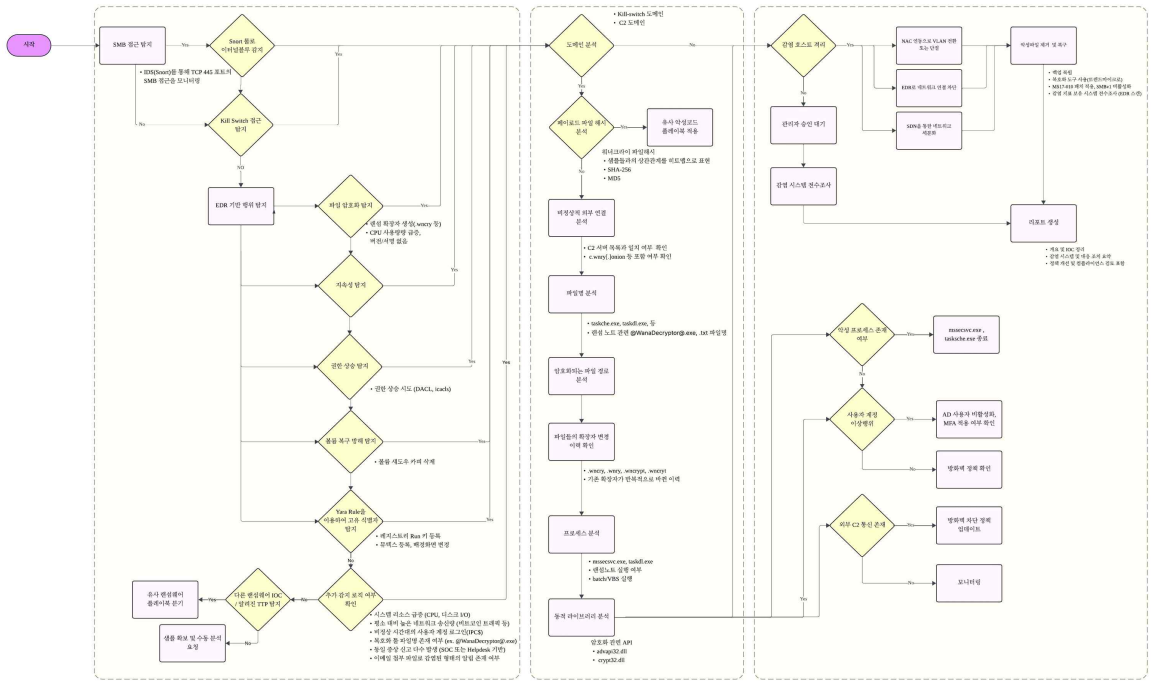
팀원 : 문무현, 김예은, 김재이, 이승은, 유현선

목 차

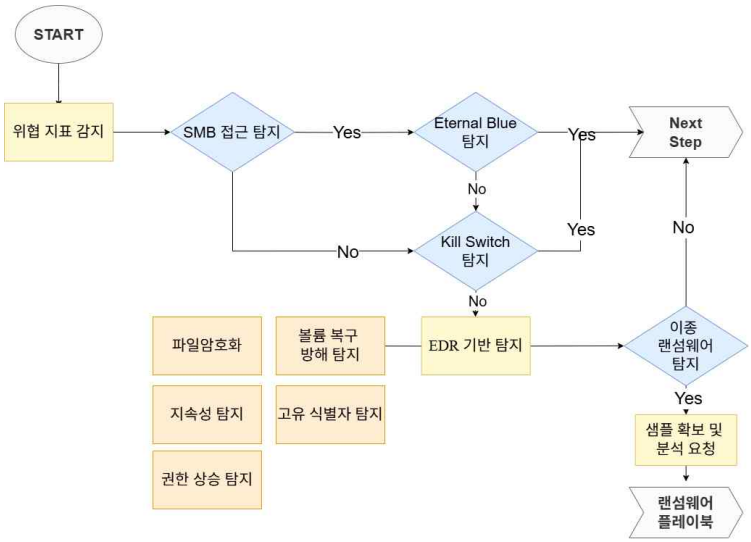
1. Action Guidelines



WannaCry 랜섬웨어에 감염되셨나요? WannaCry는 SMB 취약점(MS17-010, EternalBlue)을 악용하여 사용자의 개입 없이도 빠르게 내부망으로 확산되는 대표적인 웜형 랜섬웨어입니다. 파일 암호화뿐 아니라 서비스 중단, 핵심 서버 마비 등 전사적 피해를 일으킬 수 있으며, 킬스위치 도메인 응답 여부에 따라 암호화가 즉시 중단되기도 합니다.
아래는 WannaCry 감염 발생 시 단계별로 필요한 보안 대응 절차입니다.



2. Detection



WannaCry 감염의 초기 단계에서는 다양한 위협 지표를 통해 의심 이벤트를 식별할 수 있습니다. 보안 운영 센터(SOC) 및 EDR, SIEM, 사용자 장비(PC, 노트북)로부터 다음과 같은 이상 징후가 보고될 수 있습니다:

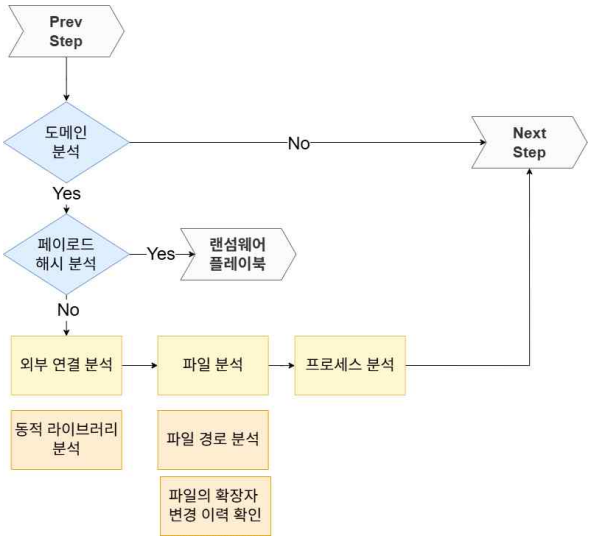
- 시스템 리소스(CPU, 디스크 IO) 사용률이 급증하거나 비정상적인 트래픽(예: 비트코인 관련 전송량)이 발생합니다.
- 근무시간 외 시간대의 사용자 계정 로그인(IPC$)이 탐지되거나, HelpDesk에 동일한 증상(파일 암호화, 강제 종료 등)을 보고하는 사용자가 다수 발생합니다.
- 이메일 첨부파일로 감염이 유입된 정황이 확인되며, EDR 또는 안티바이러스 솔루션에서 파일 암호화 이벤트가 감지됩니다.

특히 네트워크 트래픽에서 SMB 포트(445)에 대한 접근이 시도되었거나, 킬스위치 도메인(iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com)에 대한 접속이 로그로 남은 경우, 이는 WannaCry 감염의 핵심 지표로 분석 단계로 즉시 진입해야 합니다.
이외에도 다음과 같은 EDR 기반 지표들이 탐지될 수 있습니다:

- .wnry, .wncry 등의 확장자가 생성되며, 파일 암호화가 진행
- taskdl.exe, mssecsvc.exe 등 악성 프로세스 실행
- icacls.exe를 통한 권한 상승 시도
- HKLM\...\Run, Services.msc, Task Scheduler에 지속성 확보 흔적 등록
- 볼륨 섀도우 복사본 삭제 및 뮤텍스 생성, 바탕화면 변경

만약 샘플 분석 결과 WannaCry가 아닌 다른 종류의 랜섬웨어일 경우, 별도 플레이북을 기준으로 분기 처리하여 대응합니다.

3. Analysis



분석 단계에서는 WannaCry의 고유 특성을 기반으로 다양한 측면에서 악성코드 행위를 식별하고, 유사 샘플과의 연관성을 파악합니다. 이 과정에서 다음과 같은 분석 절차를 수행합니다:

1. 도메인 접속 이력을 분석합니다.
   - 킬스위치 도메인 및 C2 도메인 접속 시도 여부를 DNS 로그 기반으로 확인
   - 특히 .onion 도메인을 통한 외부 접속 시도가 있었다면 고위험 지표로 판단

2. 해시값을 비교 분석합니다.
   - 현재 페이로드와 기존 WannaCry 샘플 간의 해시 유사도를 비교
   - 유사도가 높은 경우, 히트맵 등의 상관분석 시각화를 통해 변종 여부를 판단

3. 외부 연결 및 암호화 API 호출 여부를 확인합니다.
   - C2 서버 접속 기록 및 이상 네트워크 트래픽 유무를 점검
   - advapi32.dll, crypt32.dll 등 암호화 관련 DLL 호출 여부를 분석
   - CryptEncrypt, CryptImportKey 등의 API 호출 흐름을 기반으로 실제 암호화 행위 여부를 검토

4. 파일 생성 및 수정 이력을 분석합니다.
   - taskdl.exe, tasksche.exe 등 악성 실행파일이 존재하는지 확인
   - 랜섬노트 파일(@WanaDecryptor@.exe, .txt)의 생성 여부를 확인
   - .wnry, .wncry, .wncrypt 등의 확장자 변경 이력을 통해 피해 파일 범위를 추출

5. 실행 중인 프로세스를 분석합니다.
   - mssecsvc.exe 프로세스 실행 여부와 랜섬노트 자동 실행 기능 유무를 확인
   - Batch 또는 VBS 스크립트에 실행되었는지 검토

4. Prevent Spread & Elimination

감염이 확인되면 즉시 확산을 방지해야 하며, 이는 다음과 같은 조치를 통해 수행됩니다:

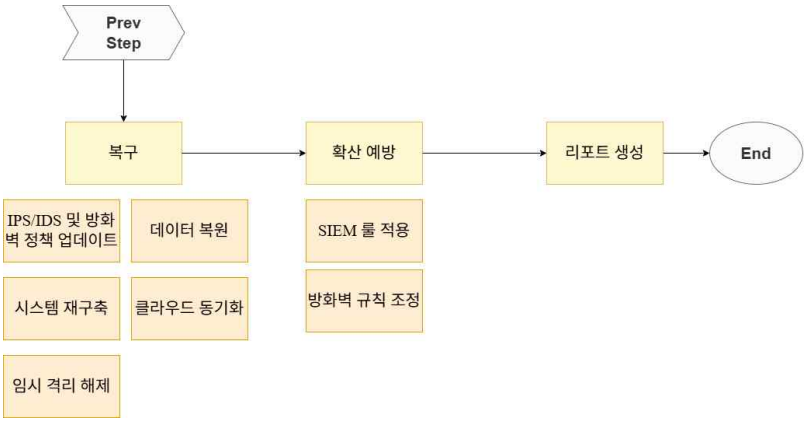
1. mssecsvc.exe, taskdl.exe와 같은 실행 중인 악성 프로세스를 종료 및 삭제하고, 킬스위치 도메인 접속 시도는 DNS Sinkhole을 통해 차단합니다.

2. SIEM 및 EDR에 다음과 같은 탐지 룰을 적용하여 자동 경고 체계를 강화합니다.
   - 짧은 시간 내 다수의 내부 IP에 SMB 연결 시도 (예: 1분 내 10개 이상)
   - @WanaDecryptor@, .wnry, taskdl.exe 등 주요 IOC 기반 실행 탐지
   - 킬스위치 도메인에 대한 DNS 요청 탐지
   - 단시간 내 수십~수백 건의 파일 확장자 변경 탐지

3. 방화벽과 NAC 정책을 통해 SMB, RPC 등의 프로토콜을 차단하며, C2 통신 경로를 차단합니다.

이후 감염된 시스템에 존재하는 모든 악성 파일을 제거하고, 로그 기반으로 잔여 악성 요소가 없는지 확인합니다.

5. Recover



복구 단계에서는 감염된 시스템에 대해 백업 복원을 수행하고, WannaCry가 악용한 SMBv1 관련 취약점(MS17-010)에 대한 패치 여부를 점검합니다. 복구 절차는 다음과 같이 이뤄집니다:

1. 백업 이미지를 기준으로 OS 재설치 또는 데이터 복원을 진행합니다.
2. 보안 패치 적용 여부(MS17-010), Windows Update 최신 상태를 유지합니다.
3. 방화벽 및 IDS/IPS 정책에 대해 Snort 기반 룰셋을 재정비하여 재감염 방지합니다.
4. 로컬 및 클라우드 백업 간의 데이터 정합성을 검토한 후 격리 해제 여부 결정합니다.
5. 최종적으로 감염 대응 경과에 대한 내부 보고서 생성 및 향후 대응 매뉴얼에 반영합니다.