

macker 사용 설명서

본 프로젝트는 과학기술정보통신부가 지원하는 차세대보안리더양성과정(Best of the Best) 디지털포렌식 트랙에서 막내온탑 팀이 수행한 교육·연구 과제의 일환으로 진행되었습니다.

1. 프로젝트 개요

본 프로젝트는 macOS의 통합 로깅 시스템(AUL, Apple Unified Logging System)을 기반으로 사용자의 이상행위 탐지합니다.

2. 최소 사양

원활한 구동을 위해 다음 사양 이상의 환경을 권장합니다.

HardWare

- CPU: Apple Silicon (M1) 이상 권장
- RAM: 8GB 이상

Disk

- 20GB 이상의 여유 공간

Software

- macOS Sonoma (14.0) 이상

3. 실행 방법 및 기본 정보

Docker Desktop 실행

```
git clone https://github.com/MACNEONTOP/macker.git  
cd macker  
chmod +x run.sh  
.run.sh
```

흰 배경이 나오면 Command(⌘) + L Shift + R

Kibana 기본 정보

<http://localhost:5601>

ID: elastic

PW: changeme

삭제 및 사후 정리

docker compose down

이후 삭제 된 git clone 폴더를 삭제합니다.

4. 시나리오 실행

본 프로젝트에서는 macOS AUL 기반 이상행위 탐지를 검증하기 위해 실제 실행 가능한 시나리오를 구성했습니다. 이를 위해 로컬 환경에서 동작하도록 제작한 인포스탈러, 랜섬웨어 형태의 테스트 애플리케이션을 실행하고, 그 과정에서 기록되는 AUL 로그를 기반으로 탐지 규칙이 정상적으로 발동되는 예시를 제공합니다.

Download Link(해당 악성 파일을 더블클릭하여 실행하지 않도록 주의 바랍니다.)

Link: 1

https://drive.google.com/drive/folders/1nk_y4ZktPbiqmKKi0UXg5WAV6-RJkRg-?usp=sharing

Link: 2

<https://github.com/MACNEONTOP/malware>

PW: infected

4.1 랜섬웨어

도커 실행 및 임의 디렉토리 생성 후 실행 바랍니다.

【 위협 명 】

- Turtle Ransomware (macOS)

【 위협 수준 】

- 낮음 (Low)
- 하드코딩된 키 존재로 복구 가능

【 주의 사항 】

본 악성코드는 같은 디렉토리 내에 존재하는 모든 **.txt, .doc, .doce** 파일을 암호화하기 때문에 무조건 격리되어있는 디렉토리에서 실행하길 바랍니다.

또한, 더블클릭으로 절대 실행하지 않도록 주의 바랍니다.

본 악성코드의 보고서는 아래에서 확인이 가능합니다.

https://objective-see.org/blog/blog_0x76.html

【 압축 해제 】

`unzip ./Ransomware_Test.zip`

【 상태 확인 】

디렉토리 내에 'TurtleRansom....'(악성코드)와 txt, doc, doce(원본 파일), Readme.md, decode.py 존재

【 보안 기능 우회 및 실행 권한 부여】

```
xattr -rc TurtleRansom-v0-macos-arm64  
chmod +x TurtleRansom-v0-macos-arm64  
.TurtleRansom-v0-macos-arm64
```

【 결과 관찰 】

파일명 변경

- 변경 전: test.txt
- 변경 후: test.txt.TURTLERANSv0

내용 변조

- 원본 평문이 사라지고 난독화된 암호문(Ciphertext)로 덮어쓰기 확인

【 복구 】

악성코드 제거

- 실행 파일(TurtleRansom...) 삭제

데이터 복구

- 준비된 복호화 도구(decode.py) 사용

```
python3 ./decode.py
복호화 키: wugui123wugui123
알고리즘: AES-CTR (IV=0, 고정값)
```

【 사후 조사 】

- localhost:5601 접속 후 로그인
 - ID: elastic
 - PW: changeme
- Analytics - Dashboards 이동 **[MacneOnTop] Fsevents Monitoring**

4.2 인포스틸러

도커 실행 및 임의 디렉토리 생성 후 실행 바랍니다.

【 위협명 】

- localinfostealer (macOS)

【 위협 수준 】

- 낮음 (Low)
- 로컬에서 실행하여 외부 유출 없음

【 주의 사항 】

- 해당 **infostealer** 실행 전 **server.py**를 실행하십시오.

【 압축 해제 및 이동 】

```
unzip localinfostealer.zip
cd localinfostealer
```

【 악성 행위 】

분류	사용 명령어	코드 내 실제 역할	실행 결과 및 저장 위치
탐색	<code>find, sysctl</code>	Desktop 내 PEM 키 파일 검색, 가상환경(VM) 탐지	저장: <code>SystemInfo/pem_targets.txt</code>
수집	<code>cp, rsync, cat, last, ls, os.walk</code>	중요 파일 복제(Keychain, History), 접근 제한 우회, 터미널 기록 수집	저장: <code>Artifacts/login.keychain-db</code> 저장: <code>Artifacts/Chrome_History</code> 저장: <code>Artifacts/zsh_history.txt</code>
정찰	<code>system_profiler ifconfig, ps</code>	하드웨어(VM여부 포함)/SW 정보, 네트워크/프로세스 정보 덤프	저장: <code>SystemInfo/system_summary.txt</code> 저장: <code>SystemInfo/network_config.txt</code> 저장: <code>SystemInfo/process_list.txt</code>
실행	<code>open</code>	사용자 안심용 Decoy 이미지 실행	실행: 화면에 <code>hello.jpg</code> 이미지 팝업
정보	<code>du, stat echo</code>	파일 수집 성공/실패 여부, 수집된 파일 크기 로그 기록	저장: <code>SystemInfo/File_Manifest.txt</code>
압축	<code>ditto, zip</code>	시스템 정보 풀더 압축, 전체 데이터 암호화 압축	생성: <code>info_temp.zip</code> 생성: <code>Exfil_[사용자]_[시간].zip</code>
유출	<code>curl</code>	서버 전송 및 HTTP 상태 확인	화면 출력: 터미널 화면 (Standard Output)
정리	<code>rm</code>	작업 흔적 제거	저장: <code>SystemInfo/pem_targets.txt</code>

【 상태 확인 】

- 디렉토리 내에 'localinfostealer.app(악성코드)와 cleanup.sh(정리 파일), server.py'존재

【 보안 기능 우회 및 실행 권한 부여 】

```
xattr -rc localniceview.app server.py
chmod +x localniceview.app/Contents/MacOS/hidden.sh server.py
python3 ./server.py &
open ./localniceview.app
```

【 결과 관찰 】

기만 행위 관측

- 이미지(hello.jpg) 팝업

수집 행위 관측

- Server.py와 같은 디렉토리에 upload 디렉터리 생성
- upload 내부에 수집파일을 'infected'로 복호화 후 수집 파일 확인

【 근절 및 복구 】

악성코드 제거

- 실행 파일(localniceview.app) 삭제

수집된 파일 정리

- 준비된 cleanup 도구 사용

```
chmod +x ./cleanup.sh  
./cleanup.sh
```

[사후 조사]

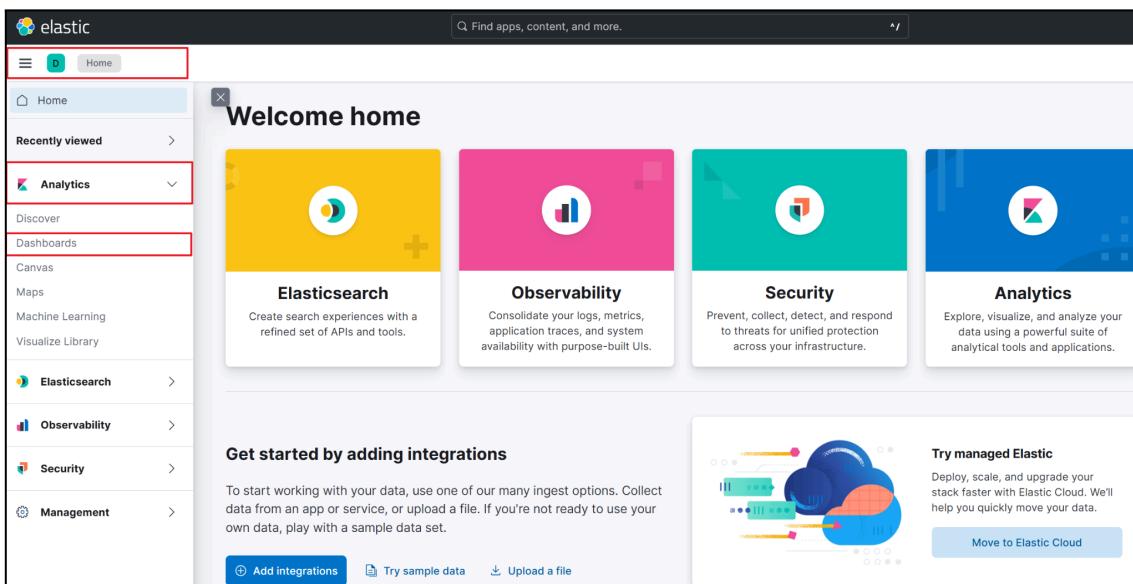
- localhost:5601 접속 후 로그인
 - ID: elastic
 - PW: changeme

Analytics - Dashboards 이동

[MacneOnTop] OverView/ [MacneOnTop] User-Risk Dashboard 확인

5. 대시보드

초기 화면 - 네비게이션 Bar - Analytics - Dashboards 이동



[탐지 를 확인]

The screenshot shows the Elastic Security interface under the 'Security' tab. On the left sidebar, 'Alerts' is highlighted with a red box. The main area displays several security views: Overview, Detection & Response, Kubernetes, Cloud Native Vulnerability Management, Entity Analytics, and Data Quality. A search bar at the top allows filtering by tag ('tag:"Security Solution"'). Below the search bar are filters for 'Recently updated', 'Tags', and 'Created by'. At the bottom right, there are 'Last updated' and 'Actions' buttons.

[Rules(SIEM)]

- Rules 페이지는 보안 탐지 로직을 정의하고 관리하는 공간으로 사전에 정의 해둔 Sigma Rules를 확인 가능합니다.

[Alerts]

- 활성화된 규칙들이 실제로 탐지한 이벤트를 시각적으로 제공하는 공간입니다.
- 탐지 규칙이 조건을 만족하는 로그를 발견하면 Alert(경보)이 생성되며, 사용자는 이를 통해 의심스러운 활동을 즉시 확인 가능합니다.

The screenshot shows the Elastic Security interface under the 'Alerts' tab. On the left sidebar, 'Alerts' is highlighted with a red box. The main area displays a list of open alerts with columns for Status, Severity, User, and Host. There are filters for 'Status: open', 'Severity', 'User', and 'Host'. Below the alert list are three cards: 'Severity levels' (showing Critical: 86, High: 272, Medium: 1k+, Low: 1k+), 'Alerts by name' (listing rule names and counts), and 'Top alerts by' (listing hosts and their alert percentages: eno-2.local 42%, ginjun-yeong-ul-macbookair.local 39.8%, hiji-macbookpro.local 18.2%). A 'Manage rules' button is located in the top right corner.

【제공된 대시보드】

[MacneOnTop] OverView



① Count of Records

- 최근 7일 내 수집된 로그를 확인할 수 있습니다.

② User Record

- 사용자 별 로그 발생량을 확인할 수 있으며, 특정 시점의 비정상적인 로그 급증을 식별할 수 있습니다.

③ Host Risk Ranking

- Threat Score와 심각도 별 탐지 건수를 기준으로 위험도를 내림차순 정렬하여, 우선 대응이 필요한 고위험 단말을 선별합니다.

④ Critical Gauge

- 즉각적인 조치가 요구되는 'Critical' 등급의 보안 위협 탐지 총건수를 페이지 차트로 직관적으로 확인할 수 있습니다.

⑤ Alert Timeline

- 시간대별 위협 탐지 추이를 심각도에 따라 누적 영역 차트로 표현하여, 공격 시도의 발생 시점과 집중도를 파악할 수 있습니다.

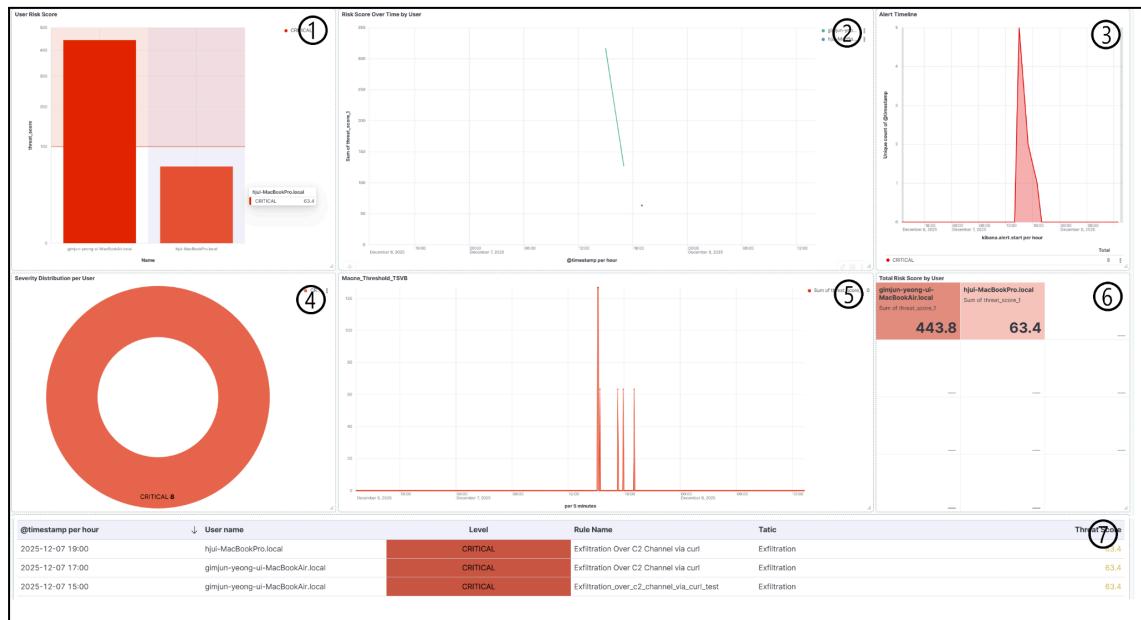
⑥ Total Detected Notifications

- 일정 주기 동안 탐지된 전체 보안 알림의 발생 빈도를 막대그래프로 나타내어, 특정 시간대에 위협 이벤트가 집중되었는지 확인할 수 있습니다.

⑦ Sum of Threat Score

- 탐지된 모든 보안 위협 점수의 총합을 나타내며, 설정된 임계값을 초과할 경우 시스템의 보안 위험도가 심각한 수준임을 판단할 수 있습니다.

[MacneOnTop] User-Risk Dashboard



① User Risk Score

- 사용자 단위 위협 점수를 CRITICAL, HIGH, MEDIUM, LOW 등급으로 구분하여 확인할 수 있습니다.

② Risk Score Over Time by User

- 시간 흐름 기준으로 사용자 단위 위협 점수를 확인할 수 있습니다.

③ Alert Timeline

- 시간 흐름 기준으로 탐지된 알람 수를 확인할 수 있습니다.

④ Severity Distribution per User

- 탐지된 알림 수를 원형 그래프로 확인할 수 있습니다.

⑤ Macne_Threshold_TSVB

- 5분 단위로 위협 점수를 그래프로 확인할 수 있습니다.

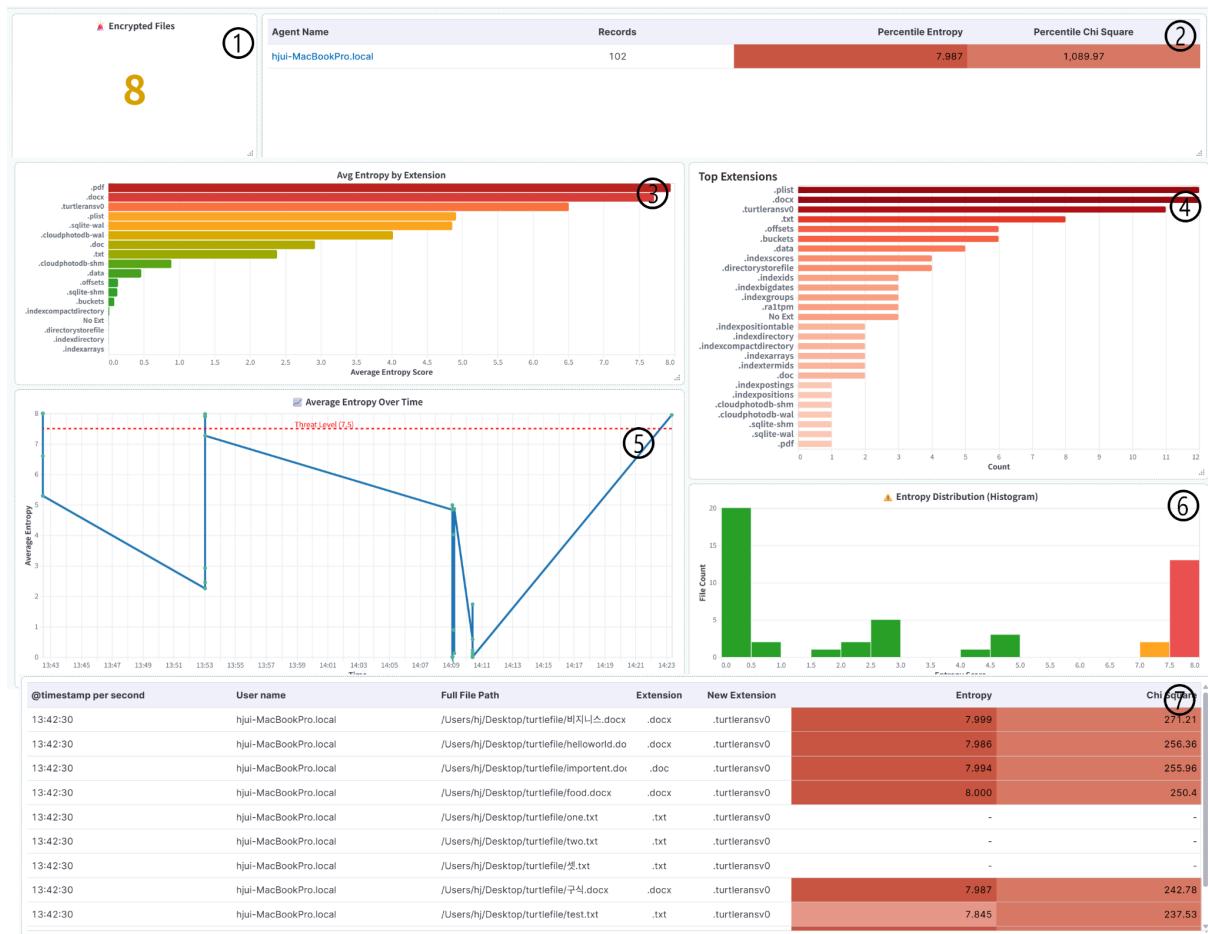
⑥ Total Risk Score by User

- 사용자 단위의 위협 점수를 확인할 수 있습니다.

⑦ Detection Rule Details Summary

- 탐지된 룰의 세부 정보를 확인할 수 있으며, 시간대별 발생 시각, 사용자명, 레벨, 룰 이름, 전술(Tactic), 위협 점수 항목을 함께 제공합니다.

[MacneOnTop] Fsevents Monitoring



개요

- 본 대시보드는 Ransomware 탐지에 특화된 대시보드입니다.
- 파일의 상태 변화를 감시할 수 있는 대시보드로, 주로 파일 암호화와 관련된 정보를 모니터링 할 수 있습니다.
- AUL이 아닌 추가 fsevents 모니터링과 엔트로피를 계산하여 그 값을 사용합니다.
- 위험성을 주로 확인할 수 있는 패널은, 1번과 3,4번, 7번입니다.

① Encrypt Files count

- 암호화 되었을 가능성이 높은 파일들의 개수를 확인할 수 있습니다.
- 본 패널을 활용하여 갑자기 암호화 의심 파일이 급증하게 되면 랜섬웨어로 의심할 수 있습니다.

② User Summary

- 로그에 존재하는 유저의 현재 상태를 요약해서 확인할 수 있습니다.

③ Avg Entropy by Extension

- 각 확장자 별 평균 엔트로피를 계산하여 그래프로 보여줍니다.
- 수상한 확장자가 해당 그래프에서 확인될 수 있습니다.

④ Top Extension

- 최근 파일 이벤트가 가장 많이 발생한 10개의 확장자를 그래프로 확인할 수 있습니다.
- 수상한 확장자가 해당 그래프에서 확인될 수 있습니다.

⑤ AVG Entropy Over Time

- 시간 순서로, 관측된 엔트로피를 꺾은선 그래프로 확인할 수 있습니다.

⑥ Entropy Distribution

- 현재 엔트로피의 분포 현황을 확인할 수 있습니다.

⑦ Encrypt Details Summary

- 암호화가 일어났다고 판단되는 로그에 대해 세부적으로 확인할 수 있습니다.

수동 동작 및 오류 해결

- Docker 설치 관련 오류

- brew install docker 방식으로 Docker를 설치할 경우, 환경에 따라 Docker Desktop과 충돌하거나 오류가 발생할 수 있습니다. 가급적 Docker Desktop 공식 설치관리자를 사용 바랍니다.

- Filebeat 관련 오류

- filebeat 소유자 권한 문제 발생 시 다음과 같은 방법으로 수동 실행합니다.

```
cd filebeat-9.2.1-darwin-aarch64  
sudo chown root: * filebeat.yml  
sudo ./filebeat -c filebeat.yml
```