**Censys 오픈 서비스 등 스카다 시스템 정보 검색 방법 제시**

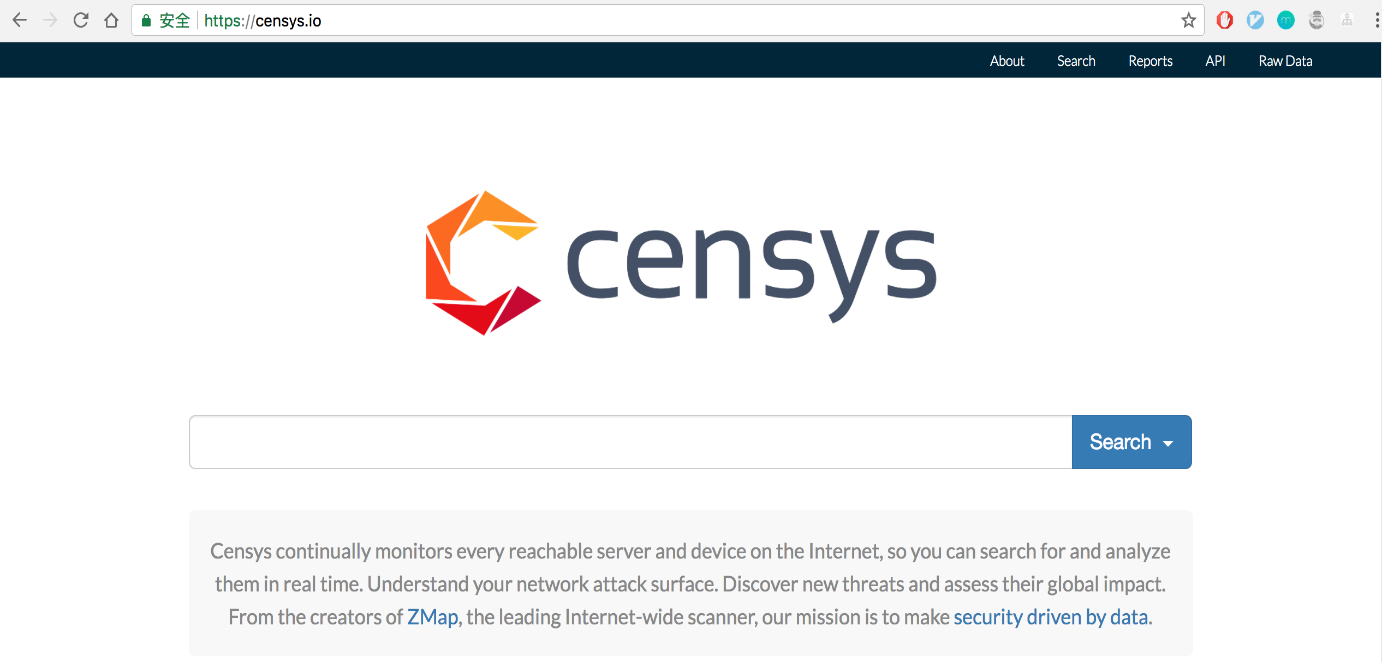
**20152689**

**산업보안학과 황성은**

* **What is “Censys”?**

**Censys**는 전 세계 인터넷 상 40억개에 달하는 IP주소를 5분 이내에 스캔해 외부 인터넷과 연결된 수많은 시스템들에 대한 정보를 조회해 볼 수 있다.

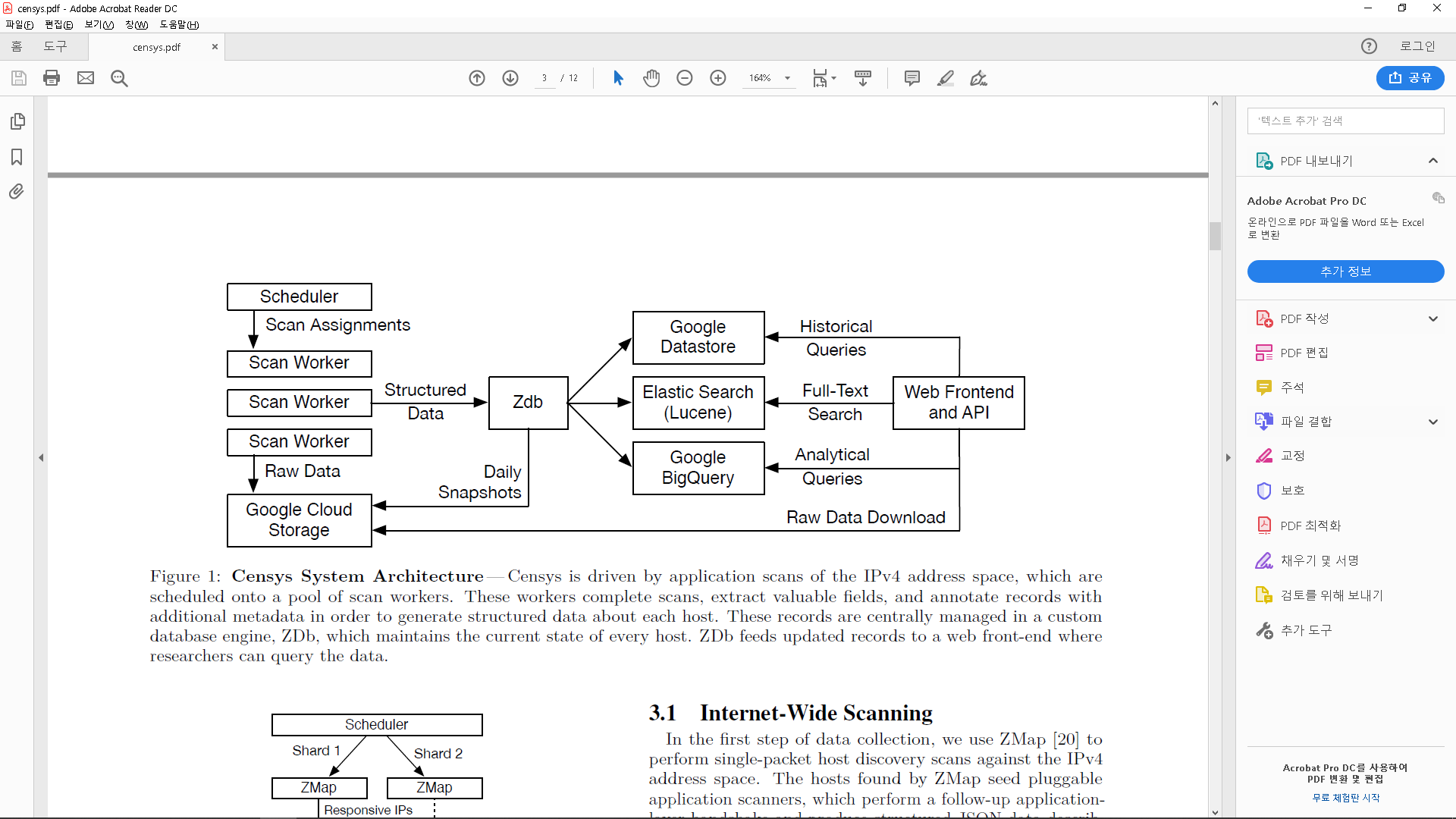
또한, 이를 활용해 모든 정보를 쉽게 확인해 볼 수 있게 한 검색엔진이다



* 1. **Censys.io 화면**
* **Features of Censys** .

1. 쇼단과 달리 직접 Heartbleed 등을 포함한 웹 취약점이 적용되는 시스템에 대한 정보를 확인할 수 있다. 여기서 발견된 정보는 **Censys**를 통해 조회가 가능하다.
2. 또한, 시스템기반시설에 사용되는 '모드버스(**Modebus**)'라는 프로토콜을 사용하는 시스템에 대한 정보도 조회가능하다.
3. Shodan.io 및 ZMap 등의 검색엔진을 통해 IP주소(IPv4), 현재 네트워크와 연결상태, 서버의 종류 등의 기본 정보를 획득하여 SCADA 및 ICS와 같이 인트라넷으로 구성되어야 하는 산업용 시스템이 스캔되어 해당 시스템을 악용할 수 있는 가능성이 있다.

* 즉, 유용한 정보인만큼 이러한 정보를 악의적인 해커가 사용할 경우, 해당 시스템이 외부 해킹에 노출될 가능성이 높아질 수 있다.



**1.2 Censys의 시스템 아키텍쳐**

Censys는 스캔 작업자 아래에서 IPv4 주소 공간의 애플리케이션 스캔에 의해 동작된다. 작업자들은 각각의 호스트에 대해 구조화된 데이터를 생성하기 위해 검색 및 필드 추출, 추가 메타데이터를 기록하는 등의 작업을 한다. 이렇게 처리된 기록은 모든 호스트의 현재 상태를 유지하는 사용자 정의 데이터베이스 엔진인 “ZDb”의 중앙에서 관리된다.

마지막으로, ZDb는 연구자들이 데이터를 조회할 수 있는 Web Frontend and API로 업데이트된 정보를 제공한다.

* **The other Engines**
* **Shodan.io**

전 세계 인터넷에 연결된 기기(서버, 네트워크 장비, 사물 인터넷 장치)들을 검색할 수 있는 검색 엔진이며, 네트워크를 검색해 인터넷과 연결된 서버, 네트워크 장비, 관리자용 서비스, 인터넷전화(VoIP), IP카메라(CCTV) 등에 대한 정보를 보여준다.

또한, 각종 검색 필터를 이용하여 특정한 컴퓨터나 사물 인터넷 장치, 서비스 정보 등을 세부적으로 검색이 가능하다.

* **ZoomEYE**

Shodan과 비슷한 서비스 및 정보를 제공하고 있는 검색엔진이며, 검색 속도가 매우 빠르지만 수집된 도메인 이름의 개수가 Shodan에 비해 적다. 장치 지문 Scanning 외에도 도메인 이름과 웹 서버에 대한 지문 Scanning의 기능도 가지고 있다.

* ㅇ

ㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡ

* **Censys 사용법**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Boolean Logic** | **And** | | | | |
| **Or** | | | | |
| **Not** | | | | |
| **parentheses** | **( )** | | |
| **범위** | **[ , ]** | **포함하는 범위** | **[2019-10-1 TO 2019-10-02]** |
| **{ , }** | **제외시킬 범위** | | |
| **정규표현식** | **?** | **하나의 문자를 대체** | | |
| **\*** | **0개 OR 그 이상의 문자를 대체** | | |
| **부스팅** | **A** | **어떤 하나의 용어를 더 적절한 용어로 사용** | **Metadata.manufacturer:Dell^2 OR “Schneider Elestric\*** |

**예를 들어,**

1. **IP주소가 23.0.0.0/8이고 8.8.8.0/24 범위를 검색하고 싶다면**

* 23.0.0.0/8 or 8.8.8.0/24

1. **한국 지역의 Telnet과 FTP를 검색하고 싶다면**

* location.country\_code: KR and protocols:("23/telnet" or "21/ftp")

1. **인기있는 웹사이트 가운데 신뢰가능한 증명서가 없는 브라우저를 검색하고 싶다면**

* not 443.https.tls.validation.browser\_trusted:true

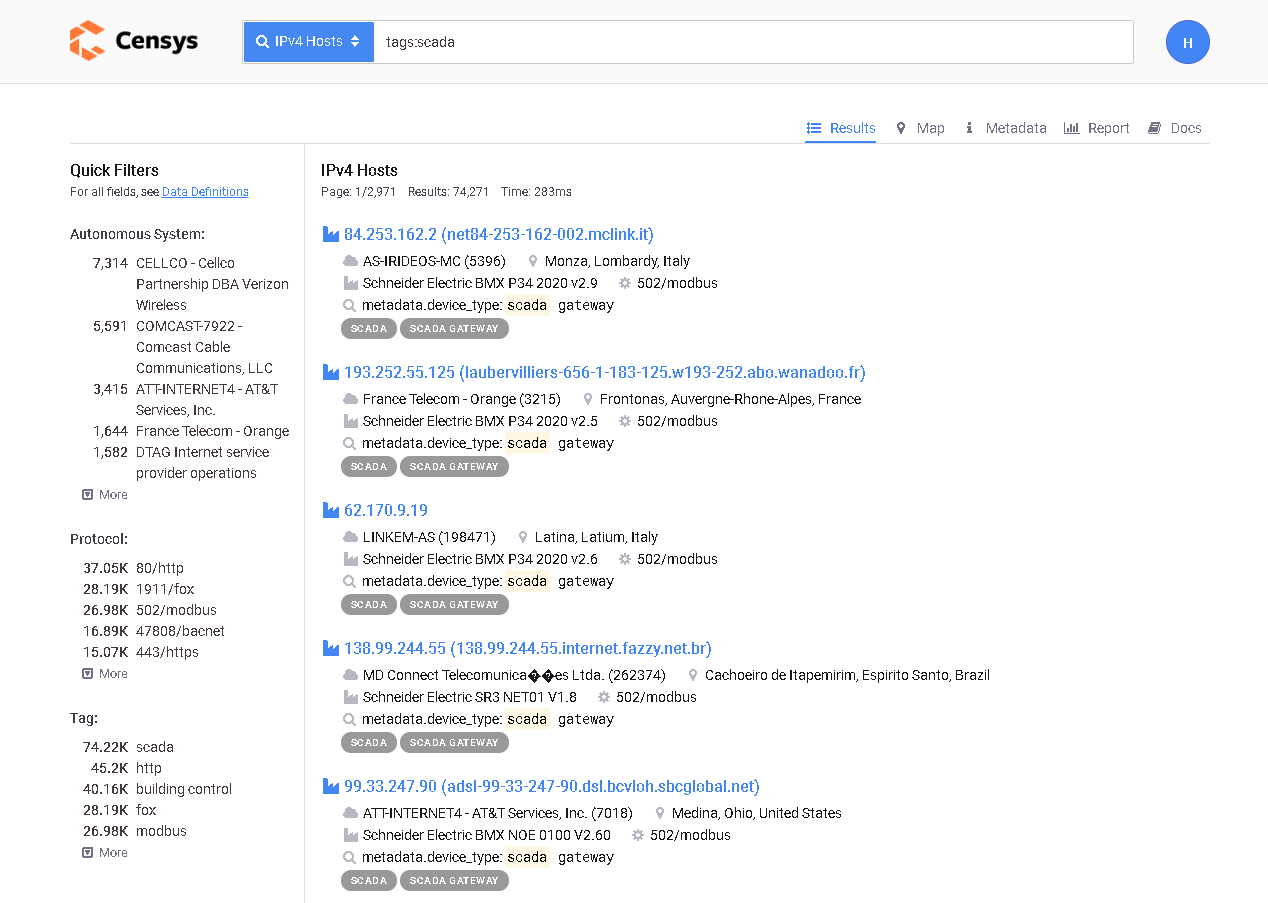
1. **한국의 산업 제어 시스템(Scada, ICS)을 검색하려면**

* location.country\_code: KR and tags: scada

**🡪 즉, Censys는 쿼리 식과 간단한 및 고급 검색 그리고 수많은 연산자를 사용하는 방식으로 (IPv4, 웹사이트, 인증서) 등의 다양한 데이터를 얻을 수 있다.**

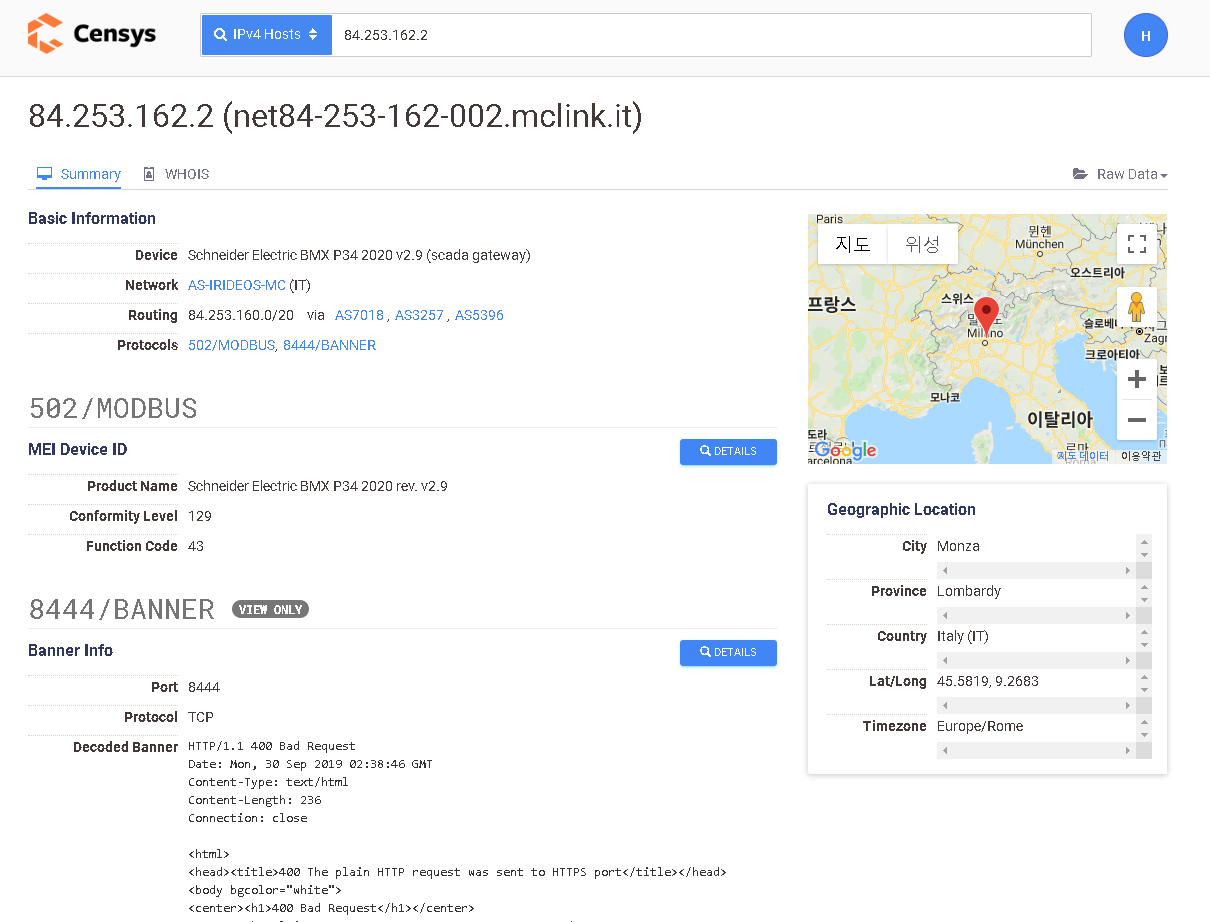
* **Censys에서 스카다 시스템(ICS, SCADA)등의 검색 옵션 실습 및 활용방안제시**

먼저, 가장 기초적인 “SCADA”태그로 필터링하여 전세계의 SCADA 시스템을 검색하기로 결정했다.



**2.1. Tag:”scada”의 결과창**

검색결과 “Scada”가 태그된 수많은 호스트들이 검색되었으며, 호스트들 중 특정 호스트가 가지고 있는 정보들을 확인할 수 있었다. Host name - 84.253.162.2 (net84-253-162-002.mclink.it)



**2.2. // 84.253.162.2 (net84-253-162-002.mclink.it) 결과창**

Censys의 태그로 검색된 특정 호스트의 정보를 요약하면 다음과 같다.

1. 지도상으로 스위스 밀라노의 Monza라는 도시에 위치하고 있다.

2. 네트워크는 AS-IRIDEOS-MC이다.

3. 라우팅 주소는 84.253.160.0/20으로 SCADA에서 사용되는 502/MODBUS와 8444/BANNER 프로토콜이 있다.

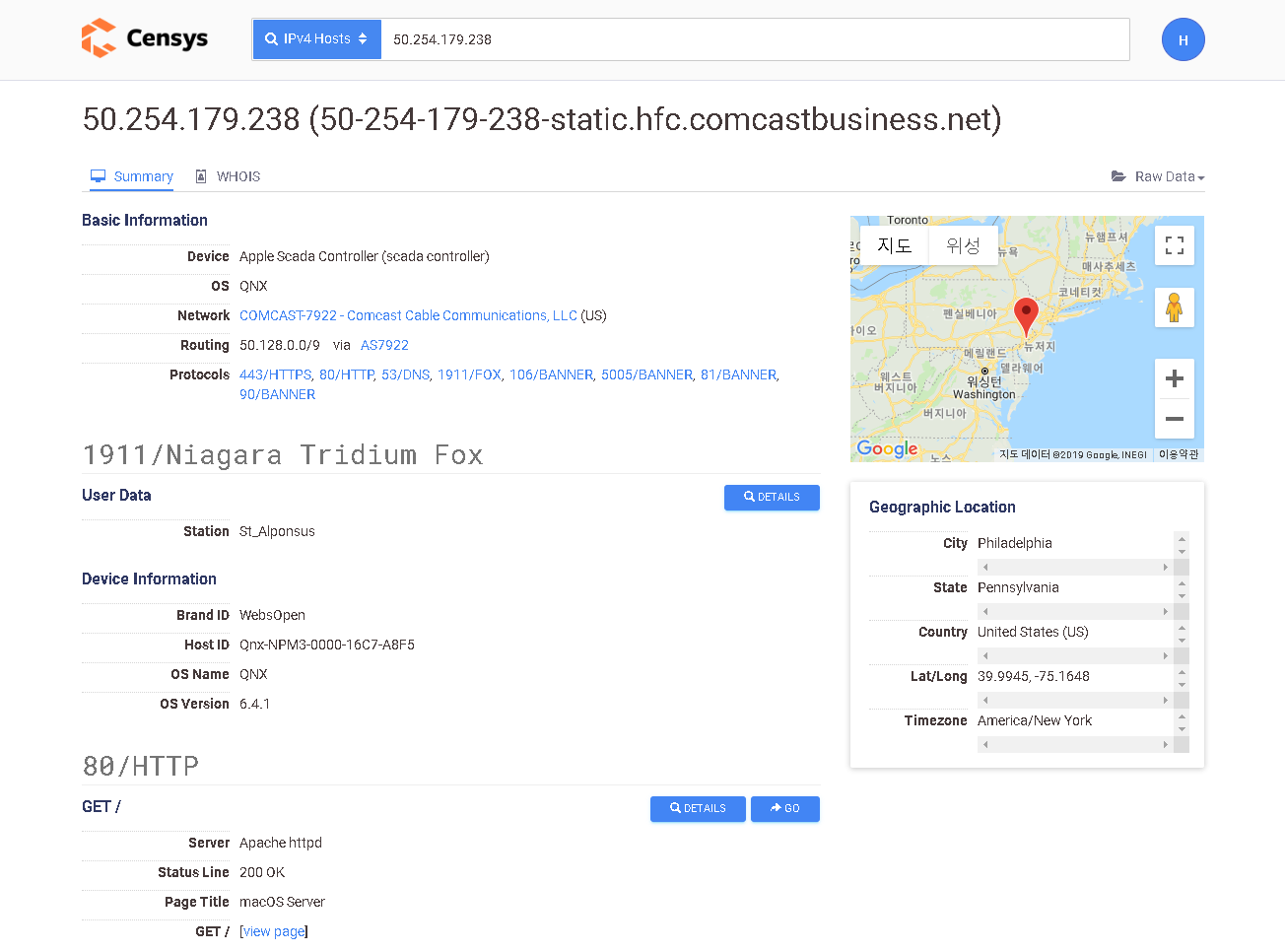
4. 마지막으로, 디바이스는 Schneider Electric BMX P34 2020 v2.9 (scada gateway)이다.

또한, Details를 클릭할 경우 Modbus 프로토콜의 포트에 대한 세부사항을 확인할 수 있다.

다양한 연산자를 이용하여 Censys의 필터를 정확하게 작성할 경우, 사용자가 원하는 굉장히 구체적이고 세부적인 특정 호스트도 도출해 낼 수 있기 때문에, 이를 한번 시도해보았다.

다음으로는 고급 검색과 필터링을 사용하여 SCADA를 태그함과 동시에 443/https이거나 21/ftp의 프로토콜을 사용하는 제조업체 Apple을 기준으로 필터링하여 Apple의 산업 제어 시스템을 검색해보겠다.

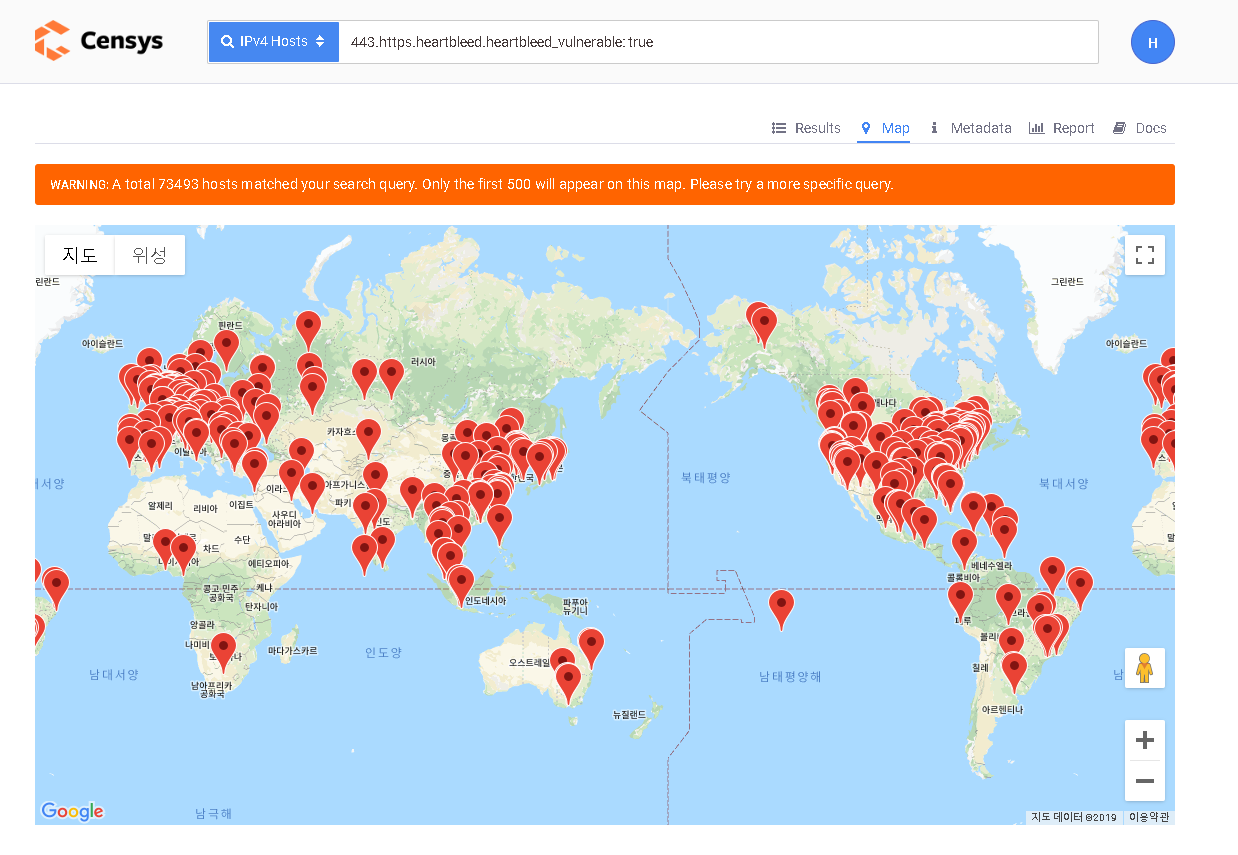
* 쿼리 식은 **metadata.manufacturer:"apple" and tags:"scada" and protocols:("443/https" or "21/ftp")** 이다.



**2.3. // 50.254.179.238 (50-254-179-238-static.hfc.comcastbusiness.net) 결과창**

이처럼, 2가지의 필터링과 1가지의 태그가 포함되었음에도 미국 필라델피아 지역에서 사용되고 있는 443/https 프로토콜을 사용하는 Apple Scada Controller의 호스트 정보를 얻을 수 있었다.

* 이를 통해서 알 수 있는 사실은 악의적인 해커들이 Shodan.io 및 Censys 등의 검색엔진에서 얻은 정보를 바탕으로 취약점을 발견하여 특정 기업의 SCADA 시스템에 대한 정보를 악용할 수 있다는 점이다.



**2.3 전세계에서 Heartbleed가 발생된 위치**

마지막으로, Censys에는 호스트의 검색과 관계없이 특정 호스트를 입력하지 않는 기타 기능이 존재하는데, “443:https.heartbleed.heartbleed\_vulnerable:true” 처럼 심각한 보안결함 –

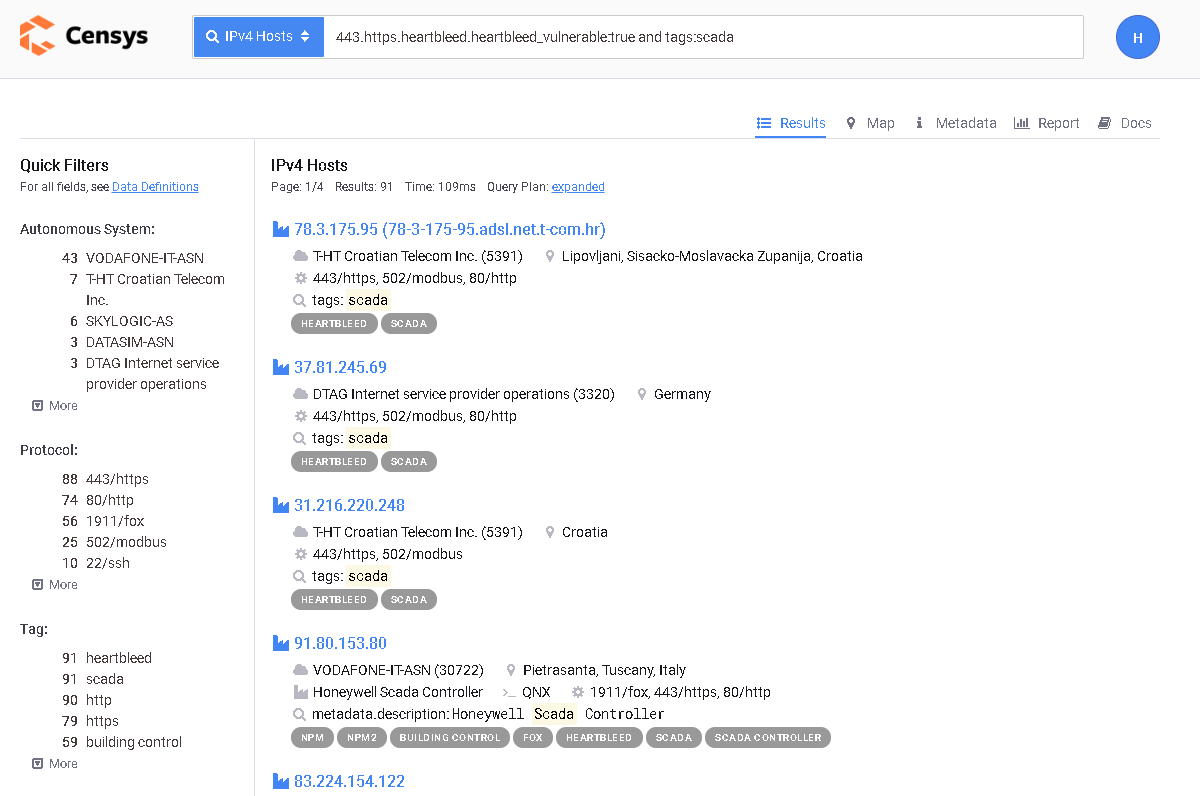
즉, Heartbleed 취약점을 가지고 있는 호스트들을 찾을 수 있다.

* **What is Heartbleed?**

하트블리드는 인터넷의 각종 정보를 암호화하는 데 사용되는 오픈소스 암호화 라이브러리인 오픈SSL 암호화 프로토콜에서 발견된 취약점이다.

국내외 대부분의 웹 서비스는 주로 오픈SSL 암호화 통신 방식을 사용하는데, 하트블리드 취약점이 악용될 경우 특정 버전의 오픈SSL을 사용하는 웹 서버에 침입 및 개인정보까지 탈취할 수 있다. 또한, 이러한 한국에서의 하트블리드 취약점 빈도는 전 세계를 기준으로 약 4%를 차지할 정도로 심각하다.

Censys를 통해 “443:https.heartbleed.heartbleed\_vulnerable:true and tags:SCADA”와 같이 Heartbeed에 감염된 것 중에서 Scada태그가 존재하는 호스트가 91개나 존재하는 것을 알 수 있었다.



**2.3 Heartbleed에 감염되었으며, SCADA의 태그를 가지는 호스트 결과창**

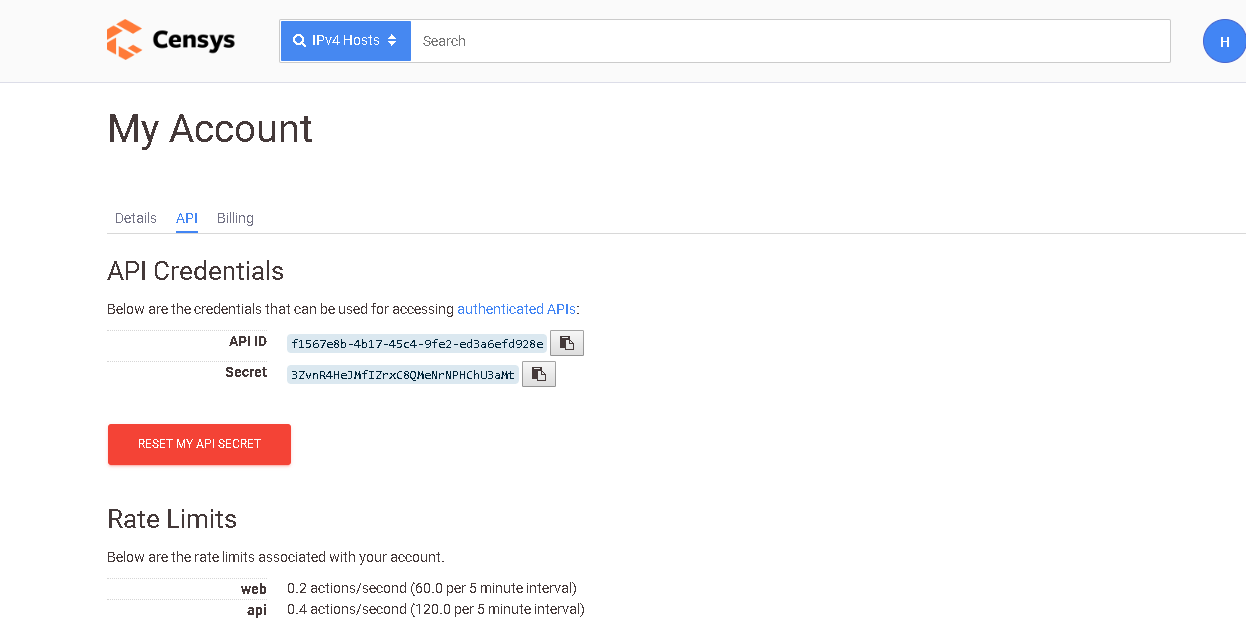
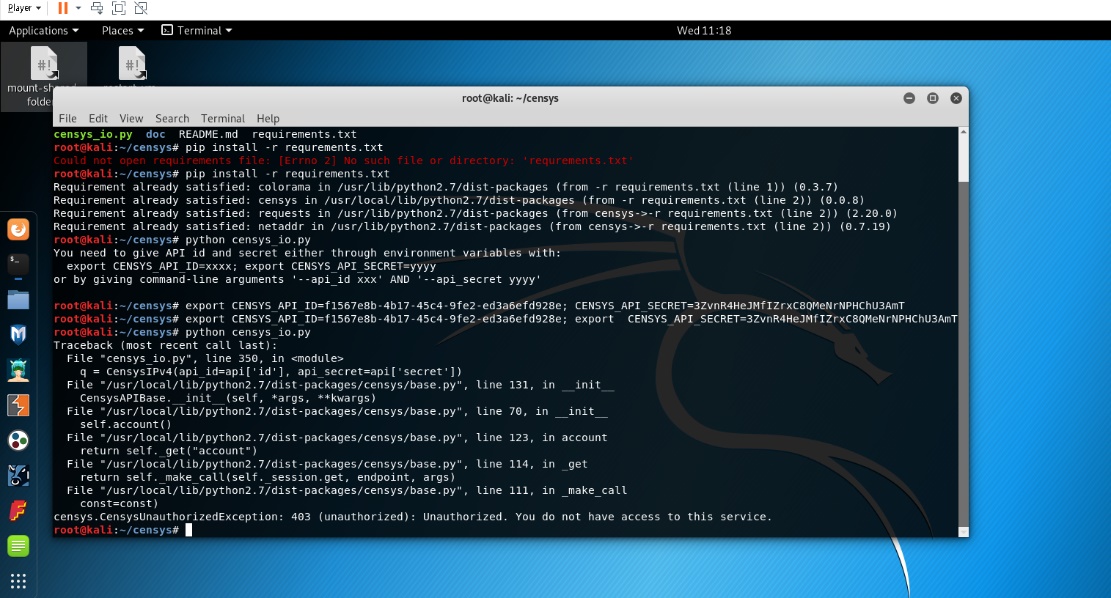
활용 방안 – 오픈 SSL을 사용하는 국내 공공기관 및 세계 웹 서비스에 대해서 censys를 사용해서 하트블리드 버그에 취약한 버전을 사용하는 기업들에게 점검을 요청하고 또한, 취약점이 발견된 사이트의 경우, 해당 사이트에 대해 관련 소식을 알린다. // 활용방안 - scada유출된 기업에 알리면 된다.

* **Censys API를 활용한 오픈소스 실습 및 활용 방안 제시**

이번에는 Censys Webservice API를 이용하여 검색을 활용하려고 한다.

먼저, kali linux를 실행하여 터미널에 git clone <https://github.com/gelim/censys>

즉, 칼리 리눅스를 통해 오픈소스의 정보가 가장 많다고도 알려져 있는 “github”로 접속하고 관련된 모듈들을 설치한다.



* 명령어 어떤 거 ?

1. censys 스캐너가 제공하는 태그를 사용하여 보안이 필요한 서버를 확인

censys\_io.py --tags heartbleed --report location.country.raw

* 보안이 필요하면, 취약하다는 말. 이거 검색해서 취약점을 찾을 수 있다.

1. Let's search for IP entries that contain the string "nmap" in one of their keys.

censy\_io.py --limit 20 nmap

1. Count how much web servers have 'SAP' in their Server header

censys\_io.py -S SAP --count

1. Get geo reparition of server with 'ABAP' in their Server header

censys\_io.py -S ABAP --report location.country.raw --report\_bucket 10

1. 'Whatsapp'조직의 SSL 인증서가있는 호스트 검색

censys\_io.py --cert-org "Whatsapp\*" --limit 10

* 이건 특정 기업의 s니 인증서가 있는 호스트 검색 / 인증서가 없는 호스트 검색으로 사용

1. Export to disk sites frontpage containing "Hacked by" in their title

censys\_io.py --html-title "Hacked by" --limit 20 –html

* 해킹당한 사이트 타이틀이므로, 여기서 하나 tmp들어가서 스크린샷 찍읍시다.

1. Use tags provided by censys scanner to look at servers that need to be secured

// 이건 하트블리드 사용하는 나라. 즉, 하트블리드 태그된 다른 포트들도 검색가능?

censys\_io.py --tags heartbleed --report location.country.raw

활용 – Censys 및 shodan을 활용하여 이러한 방식으로 포트를 스캔하는 것은 악의가 아니다, 오히려, 전세계 웹 서비스를 이용하는 이용자 및 보안전문가에게 보안 자세 인식을 높이는 데 도움이 된다는 것을 보여주는 좋은 예입니다.

* **Counclusion**

보안전문가들이 이러한 툴을 활용해 SCADA의 인터넷 연결을 막고, 취약점을 없앤다면 다행스러운 일이지만 악의적인 해커들도 이러한 툴을 악용할 수 있다는 점에서 양날의 칼이 된다.

취약점을 제대로 점검하기 위해서도 보안담당자, 침투테스트전문가들이 이러한 툴들을 적극적으로 활용할 필요가 있다

* **Reference**

<https://blog.naver.com/autumn666/221649737713>

[https://github.com](https://github.com/)

[https://chogar.blog.me](https://chogar.blog.me/)

[https://censys.io](https://censys.io/)