Draft Report Group 3

Contents

Introduction

This course project is a data analytics project that will combine some data set in a particular domain with some statistical or analytical technique to answer a research question related to the topics explained during the course.

This project is related to the websites Shodan, a search engine indexing metadata and content about everything accessible via a public IP address, CleanMX, a real-time database that consists of virus URI, collected and verified, and Virustotal, a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses. Besides, we decided to use CVE Details as well, a government repository of standards based vulnerability management data, which is consistent with the subject and very useful.

We decided to gather data sets in order to measure how vulnerable are devices, using different specifications. Then, we will try to find a link with the costs for the companies.

Security issues

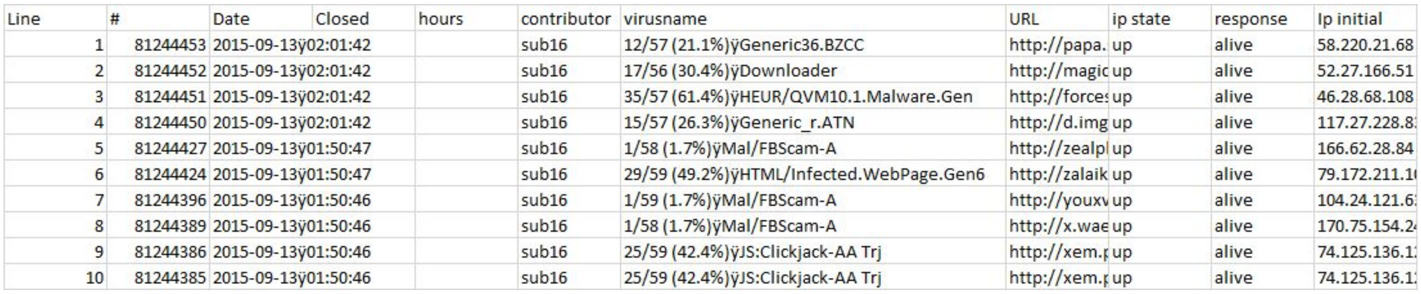
First we have to define what are the different security issues we want to analyze. Concerning the vulnerable devices, we decided to focus on SCADA devices, Netgear routers and D-Link routers, famous on the market. Using CVE Details, we have access to the different vulnerabilities and their danger level. For example, for the D-Link devices we have :

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2013-7308			DoS +Info	1/23/2014	1/23/2014	5.4	None	Local Network	Medium	Not required	Partial	Partial	Partial

The OSPF implementation on the D-Link DES-3810-28 switch with firmware R2.20.B017 does not consider the possibility of duplicate Link State ID values in Link State Advertisement (LSA) packets before performing operations on the LSA database, which allows remote attackers to cause a denial of service (routing disruption) or obtain sensitive packet information via a crafted LSA packet, a related issue to CVE-2013-0149.														
2	CVE-2013-5998			DoS	11/22/2013	3/5/2014	7.8	None	Remote	Low	Not required	None	None	Complete
Unspecified vulnerability in the Web manager implementation on D-Link Japan DES-3800 devices with firmware before R4.50B58 allows remote attackers to cause a denial of service (device hang) via unknown vectors, a different vulnerability than CVE-2013-5997.														
3	CVE-2013-5997			DoS	11/22/2013	3/7/2014	6.8	None	Remote	Low	Single system	None	None	Complete
Unspecified vulnerability in the SSH implementation on D-Link Japan DES-3800 devices with firmware before R4.50B58 allows remote authenticated users to cause a denial of service (device hang) via unknown vectors, a different vulnerability than CVE-2013-5998.														

Figure : 3 vulnerabilities of D-Link devices obtained by using CVE Details

Then, with CleanMX, we can see in real time the name of viruses present on websites :



Line	#	Date	Closed	hours	contributor	virusname	URL	ip state	response	Ip initial
1	81244453	2015-09-13ÿ02:01:42			sub16	12/57 (21.1%)ÿGeneric36.BZCC	http://papa.	up	alive	58.220.21.68
2	81244452	2015-09-13ÿ02:01:42			sub16	17/56 (30.4%)ÿDownloader	http://magic	up	alive	52.27.166.51
3	81244451	2015-09-13ÿ02:01:42			sub16	35/57 (61.4%)ÿHEUR/QVM10.1.Malware.Gen	http://forces	up	alive	46.28.68.108
4	81244450	2015-09-13ÿ02:01:42			sub16	15/57 (26.3%)ÿGeneric_r.ATN	http://d.img	up	alive	117.27.228.8
5	81244427	2015-09-13ÿ01:50:47			sub16	1/58 (1.7%)ÿMal/FBScam-A	http://zealp	up	alive	166.62.28.84
6	81244424	2015-09-13ÿ01:50:47			sub16	29/59 (49.2%)ÿHTML/Infected.WebPage.Gen6	http://zalaik	up	alive	79.172.211.1
7	81244396	2015-09-13ÿ01:50:46			sub16	1/59 (1.7%)ÿMal/FBScam-A	http://youxv	up	alive	104.24.121.6
8	81244389	2015-09-13ÿ01:50:46			sub16	1/58 (1.7%)ÿMal/FBScam-A	http://x.wae	up	alive	170.75.154.2
9	81244386	2015-09-13ÿ01:50:46			sub16	25/59 (42.4%)ÿJS:Clickjack-AA Trj	http://xem.	up	alive	74.125.136.1
10	81244385	2015-09-13ÿ01:50:46			sub16	25/59 (42.4%)ÿJS:Clickjack-AA Trj	http://xem.	up	alive	74.125.136.1

Figure 1: 10 latest results of CleanMX

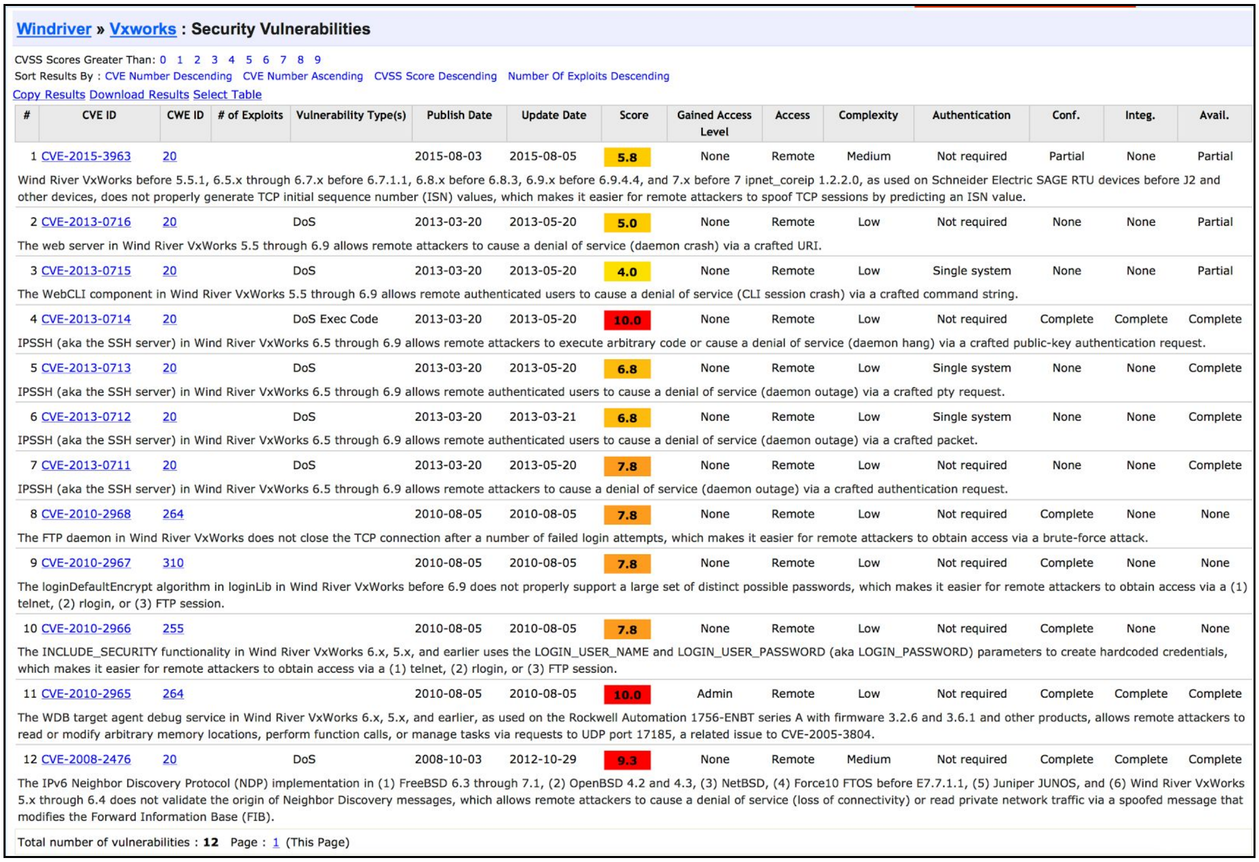
On the figure, we can see that some viruses are present several times, and we are able to determine the viruses that are more present on the Internet.

SCADA systems

When dealing with SCADA systems, dealing with security issues is a hands-on task. We can look into this from two different perspectives, attacker's and defender's.

The attacker

From an attacker's point of view, to be able to exploit systems, or rather, to find exploitable systems, a certain workflow can be drawn out. It is important to point out that in this report we are interested in finding vulnerable systems and not hacking into them, which is another story. Since SCADA systems are mostly devices with embedded operating systems and in many cases proprietary ones, attacks against them are based on present vulnerabilities and misconfigurations. Therefore the starting point is vulnerability databases. National Vulnerability Database and CVE Details are two good resources for this purpose. An example from CVE Details is depicted in Figure 2.



Windriver » Vxworks : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results Select Table

<table>
<tr><th>#</th><th>CVE ID</th><th>CWE ID</th><th># of Exploits</th><th>Vulnerability Type(s)</th><th>Publish Date</th><th>Update Date</th><th>Score</th><th>Gained Access Level</th><th>Access</th><th>Complexity</th><th>Authentication</th><th>Conf.</th><th>Integ.</th><th>Avail.</th></tr>
<tr><td>1</td><td>CVE-2015-3963</td><td>20</td><td></td><td></td><td>2015-08-03</td><td>2015-08-05</td><td>5.8</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>Partial</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">Wind River VxWorks before 5.5.1, 6.5.x through 6.7.x before 6.7.1.1, 6.8.x before 6.8.3, 6.9.x before 6.9.4.4, and 7.x before 7 ipnet_coreip 1.2.2.0, as used on Schneider Electric SAGE RTU devices before J2 and other devices, does not properly generate TCP initial sequence number (ISN) values, which makes it easier for remote attackers to spoof TCP sessions by predicting an ISN value.</td></tr>
<tr><td>2</td><td>CVE-2013-0716</td><td>20</td><td></td><td>DoS</td><td>2013-03-20</td><td>2013-05-20</td><td>5.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">The web server in Wind River VxWorks 5.5 through 6.9 allows remote attackers to cause a denial of service (daemon crash) via a crafted URI.</td></tr>
<tr><td>3</td><td>CVE-2013-0715</td><td>20</td><td></td><td>DoS</td><td>2013-03-20</td><td>2013-05-20</td><td>4.0</td><td>None</td><td>Remote</td><td>Low</td><td>Single system</td><td>None</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">The WebCLI component in Wind River VxWorks 5.5 through 6.9 allows remote authenticated users to cause a denial of service (CLI session crash) via a crafted command string.</td></tr>
<tr><td>4</td><td>CVE-2013-0714</td><td>20</td><td></td><td>DoS Exec Code</td><td>2013-03-20</td><td>2013-05-20</td><td>10.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">IPSSH (aka the SSH server) in Wind River VxWorks 6.5 through 6.9 allows remote attackers to execute arbitrary code or cause a denial of service (daemon hang) via a crafted public-key authentication request.</td></tr>
<tr><td>5</td><td>CVE-2013-0713</td><td>20</td><td></td><td>DoS</td><td>2013-03-20</td><td>2013-05-20</td><td>6.8</td><td>None</td><td>Remote</td><td>Low</td><td>Single system</td><td>None</td><td>None</td><td>Complete</td></tr>
<tr><td colspan="15">IPSSH (aka the SSH server) in Wind River VxWorks 6.5 through 6.9 allows remote authenticated users to cause a denial of service (daemon outage) via a crafted pty request.</td></tr>
<tr><td>6</td><td>CVE-2013-0712</td><td>20</td><td></td><td>DoS</td><td>2013-03-20</td><td>2013-03-21</td><td>6.8</td><td>None</td><td>Remote</td><td>Low</td><td>Single system</td><td>None</td><td>None</td><td>Complete</td></tr>
<tr><td colspan="15">IPSSH (aka the SSH server) in Wind River VxWorks 6.5 through 6.9 allows remote authenticated users to cause a denial of service (daemon outage) via a crafted packet.</td></tr>
<tr><td>7</td><td>CVE-2013-0711</td><td>20</td><td></td><td>DoS</td><td>2013-03-20</td><td>2013-05-20</td><td>7.8</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>None</td><td>Complete</td></tr>
<tr><td colspan="15">IPSSH (aka the SSH server) in Wind River VxWorks 6.5 through 6.9 allows remote attackers to cause a denial of service (daemon outage) via a crafted authentication request.</td></tr>
<tr><td>8</td><td>CVE-2010-2968</td><td>264</td><td></td><td></td><td>2010-08-05</td><td>2010-08-05</td><td>7.8</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>None</td><td>None</td></tr>
<tr><td colspan="15">The FTP daemon in Wind River VxWorks does not close the TCP connection after a number of failed login attempts, which makes it easier for remote attackers to obtain access via a brute-force attack.</td></tr>
<tr><td>9</td><td>CVE-2010-2967</td><td>310</td><td></td><td></td><td>2010-08-05</td><td>2010-08-05</td><td>7.8</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>None</td><td>None</td></tr>
<tr><td colspan="15">The loginDefaultEncrypt algorithm in loginLib in Wind River VxWorks before 6.9 does not properly support a large set of distinct possible passwords, which makes it easier for remote attackers to obtain access via a (1) telnet, (2) rlogin, or (3) FTP session.</td></tr>
<tr><td>10</td><td>CVE-2010-2966</td><td>255</td><td></td><td></td><td>2010-08-05</td><td>2010-08-05</td><td>7.8</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>None</td><td>None</td></tr>
<tr><td colspan="15">The INCLUDE_SECURITY functionality in Wind River VxWorks 6.x, 5.x, and earlier uses the LOGIN_USER_NAME and LOGIN_USER_PASSWORD (aka LOGIN_PASSWORD) parameters to create hardcoded credentials, which makes it easier for remote attackers to obtain access via a (1) telnet, (2) rlogin, or (3) FTP session.</td></tr>
<tr><td>11</td><td>CVE-2010-2965</td><td>264</td><td></td><td></td><td>2010-08-05</td><td>2010-08-05</td><td>10.0</td><td>Admin</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">The WDB target agent debug service in Wind River VxWorks 6.x, 5.x, and earlier, as used on the Rockwell Automation 1756-ENBT series A with firmware 3.2.6 and 3.6.1 and other products, allows remote attackers to read or modify arbitrary memory locations, perform function calls, or manage tasks via requests to UDP port 17185, a related issue to CVE-2005-3804.</td></tr>
<tr><td>12</td><td>CVE-2008-2476</td><td>20</td><td></td><td>DoS</td><td>2008-10-03</td><td>2012-10-29</td><td>9.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">The IPv6 Neighbor Discovery Protocol (NDP) implementation in (1) FreeBSD 6.3 through 7.1, (2) OpenBSD 4.2 and 4.3, (3) NetBSD, (4) Force10 FTOS before E7.7.1.1, (5) Juniper JUNOS, and (6) Wind River VxWorks 5.x through 6.4 does not validate the origin of Neighbor Discovery messages, which allows remote attackers to cause a denial of service (loss of connectivity) or read private network traffic via a spoofed message that modifies the Forward Information Base (FIB).</td></tr>
</table>

Total number of vulnerabilities : **12** Page : 1 (This Page)

Figure 2: A query result for known vulnerabilities

Different known manufacturers and vendors can be used as the initial criteria for queries. It is also useful to search for known vulnerabilities of common operating systems. For instance, the result of a query for a real-time OS, used in many SCADA devices, is shown in Figure 2. This query is for VxWorks.

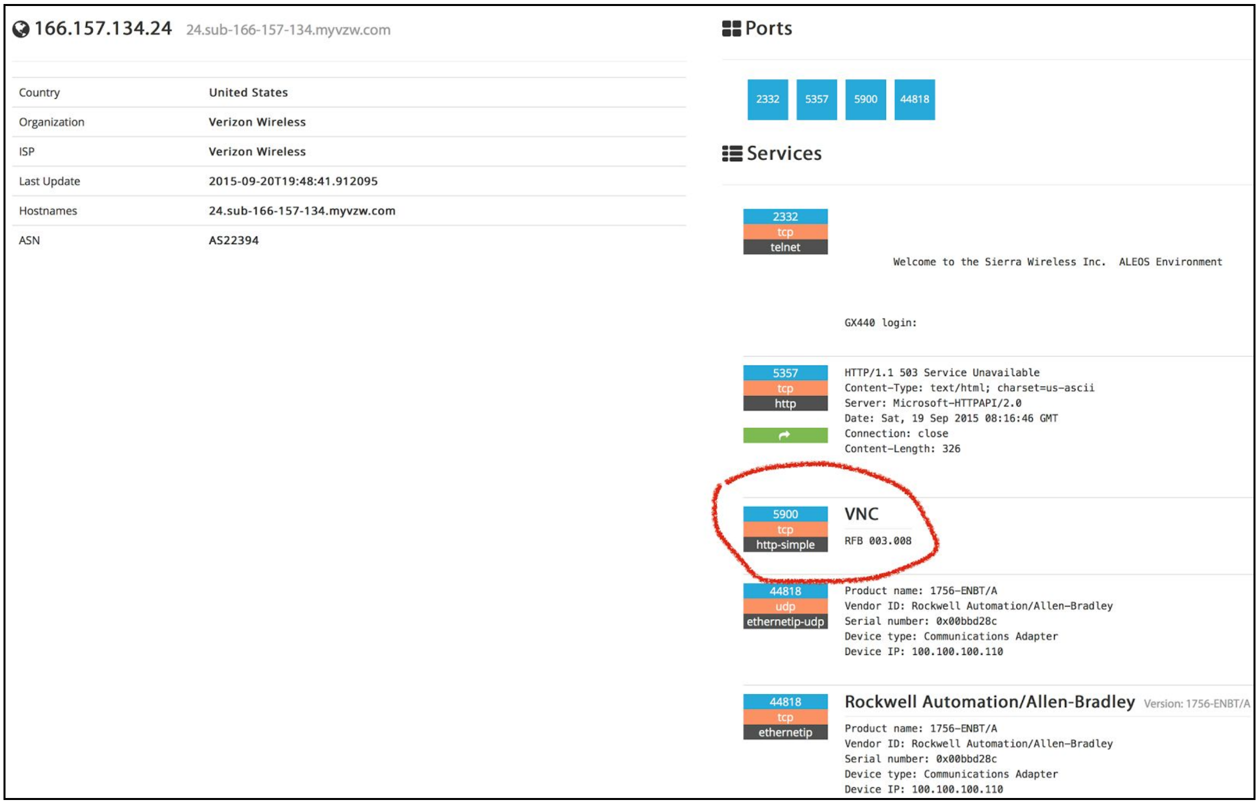
The next step is to pick one, or more vulnerabilities. One can always spend more time and energy on high score listings. Usually, the listing involves the mentioning of a service which is

up and running by default, using default credentials, as well as a firmware version, or model number. The mentioned credentials can be obtained through product documentation.
The final query is to be done in Shodan search engine. Here depending on the details given in the vulnerability and using different filters, plus some hands-on manual search in the details of each result, a set of exploitable systems can be collected.

Example: CVE-2014-9197, CVE-2014-9198
These vulnerabilities affect TSX ETG 3000, TSX ETG 3010, TSX ETG 3021 and TSX ETG 3022 models of FactoryCast HMI Gateways from Schneider (formerly Telemecanique). So one can start by looking for HMI (Human Machine Interface) in Shodan and narrow it down. Overall 17 immediate results can be found, which all have the outdated firmware, mentioned in the vulnerability. Default credential data can be found in the user manual from the vendor's website.

Note: It is important to consider two important facts regarding SCADA systems. These devices have and use different WAN connections and remote communication protocols, making the attack surface. Also, the priority in industrial systems is Availability. This is in contrast to general IT environments and their first priority, Security. These facts affect the analysis and chosen metrics.

Example: CVE-2010-2965
Wind River VxWorks is the widely deployed real-time embedded OS for ICS and SCADA systems. Searching the National Vulnerability Database and taking a quick look at the result, this vulnerability is noticeable. Main reason is the severity. The vulnerability is present on a specific model, 1756-ENBT/A from Rockwell Automation, and for certain firmware versions. A Shodan query will result in more than 250 devices. The amount of metadata shared by these exposed devices is amazing. They even advertise the internal IP address scheme of their respective LAN.
Another useful metric for an attacker is the IP address range. If the attacker is able to locate a vulnerable device with all the characteristic mentioned and the attack is successful, the first octet of the IP address can be used as a query criteria. It is likely that there are more devices connected in the same location. This was actually the case during our experimentation for a 166.157.0.0 and 166.156.0.0 network. As a confirmation of the relation, a vulnerable service (TCP port 5900-VNC) was running on most of these devices with the default password *“admin”*. Similar LAN IP range of 100.100.100.0 is also another confirmation. Figure 3 shows the presence of attack vector, as part of detailed metrics from Shodan.



166.157.134.24 24.sub-166-157-134.myvzw.com

Country	United States
Organization	Verizon Wireless
ISP	Verizon Wireless
Last Update	2015-09-20T19:48:41.912095
Hostnames	24.sub-166-157-134.myvzw.com
ASN	AS22394

2332 tcp telnet

```
                Welcome to the Sierra Wireless Inc.  ALEOS Environment



GX440 login:
```

5357 tcp http

```
HTTP/1.1 503 Service Unavailable
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 19 Sep 2015 08:16:46 GMT
Connection: close
Content-Length: 326
```

5900 tcp http-simple

VNC

```
RFB 003.008
```

44818 udp ethernetip-udp

```
Product name: 1756-ENBT/A
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x00bbd28c
Device type: Communications Adapter
Device IP: 100.100.100.110
```

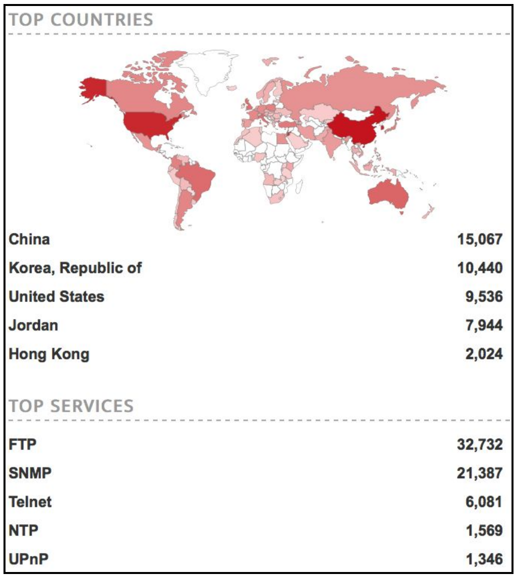
44818 tcp ethernetip

Rockwell Automation/Allen-Bradley Version: 1756-ENBT/A

```
Product name: 1756-ENBT/A
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x00bbd28c
Device type: Communications Adapter
Device IP: 100.100.100.110
```

Figure 3: VNC port 5900 access

Searching just for the word VxWorks results in around 45000 devices, as shown in Figure 4.



TOP COUNTRIES

China	15,067
Korea, Republic of	10,440
United States	9,536
Jordan	7,944
Hong Kong	2,024

TOP SERVICES

FTP	32,732
SNMP	21,387
Telnet	6,081
NTP	1,569
UPnP	1,346

Figure 4: Number of available devices running VxWorks

The decision maker (defender)

The same procedure as the attacker, is more or less valid for the defender as well. For this to make sense, we need to assume that the defender is dealing with a large collection of already deployed systems. Since an installation from scratch, can be done by following best practices in a proper manner. ICS and SCADA systems are especially important for governments, hence the existence of governmental organisations such as, ICS-CERT.
Such a defender can follow the same procedure, but the search needs to be done in a broader fashion. The defender does not have the luxury of choosing a target, but instead, they should defend all possible victims.

Metrics to measure the situation

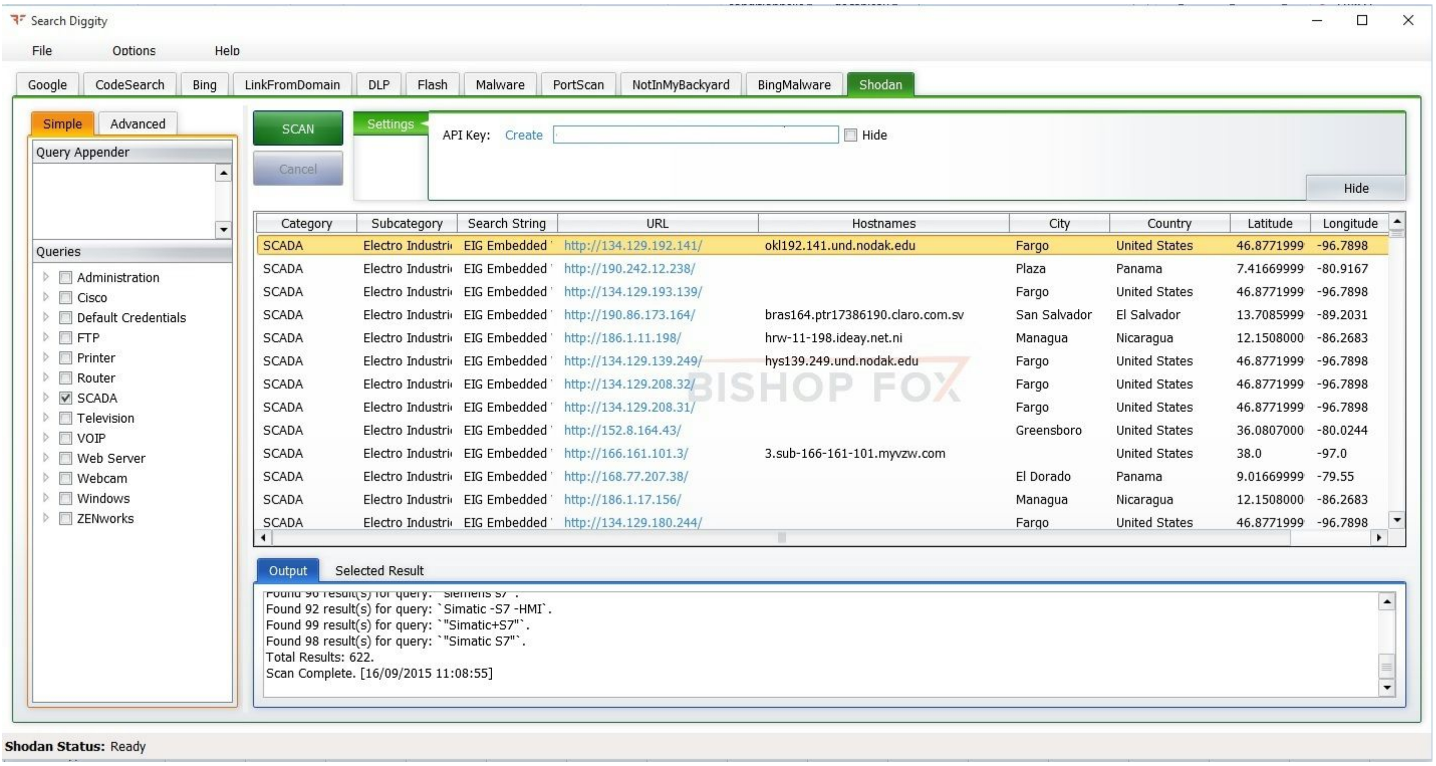
Now, we have to choose the metrics we want to use in the project. For instance, the danger level given by CVE Details can be used. The number of devices or firmware by brand can be used as well, and the geographic location of the vulnerability can be interesting too.

Scada systems

As we have discussed in the previous section, the metrics are generally vendor, firmware, service, port and IP addresses. These are to be chosen on a case-by-case basis and according to the details of the vulnerability on the focus at the time.

How many IPs, how many networks?

To find how many IPs are involved in a security issue, we can use SearchDiggity, a software allowing the copy of Shodan’s results :



API Key: Create □ Hide

Queries

- □ Administration
- □ Cisco
- □ Default Credentials
- □ FTP
- □ Printer
- □ Router
- ☑ SCADA
- □ Television
- □ VOIP
- □ Web Server
- □ Webcam
- □ Windows
- □ ZENworks

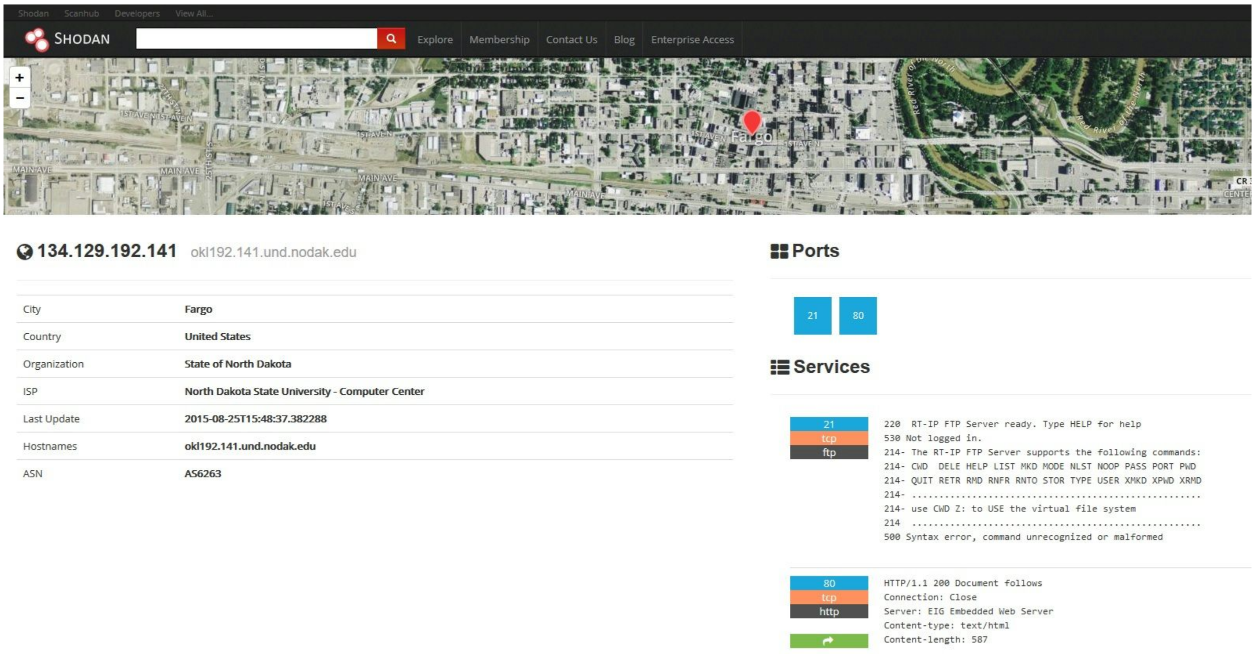
Category	Subcategory	Search String	URL	Hostnames	City	Country	Latitude	Longitude
SCADA	Electro Industri	EIG Embedded '	http://134.129.192.141/	okl192.141.und.nodak.edu	Fargo	United States	46.8771999	-96.7898
SCADA	Electro Industri	EIG Embedded '	http://190.242.12.238/		Plaza	Panama	7.41669999	-80.9167
SCADA	Electro Industri	EIG Embedded '	http://134.129.193.139/		Fargo	United States	46.8771999	-96.7898
SCADA	Electro Industri	EIG Embedded '	http://190.86.173.164/	bras164.ptr17386190.claro.com.sv	San Salvador	El Salvador	13.7085999	-89.2031
SCADA	Electro Industri	EIG Embedded '	http://186.1.11.198/	hrw-11-198.ideay.net.ni	Managua	Nicaragua	12.1508000	-86.2683
SCADA	Electro Industri	EIG Embedded '	http://134.129.139.249/	hys139.249.und.nodak.edu	Fargo	United States	46.8771999	-96.7898
SCADA	Electro Industri	EIG Embedded '	http://134.129.208.32/		Fargo	United States	46.8771999	-96.7898
SCADA	Electro Industri	EIG Embedded '	http://134.129.208.31/		Fargo	United States	46.8771999	-96.7898
SCADA	Electro Industri	EIG Embedded '	http://152.8.164.43/		Greensboro	United States	36.0807000	-80.0244
SCADA	Electro Industri	EIG Embedded '	http://166.161.101.3/	3.sub-166-161-101.myvzw.com		United States	38.0	-97.0
SCADA	Electro Industri	EIG Embedded '	http://168.77.207.38/		El Dorado	Panama	9.01669999	-79.55
SCADA	Electro Industri	EIG Embedded '	http://186.1.17.156/		Managua	Nicaragua	12.1508000	-86.2683
SCADA	Electro Industri	EIG Embedded '	http://134.129.180.244/		Fargo	United States	46.8771999	-96.7898

```
Found 96 result(s) for query: `Siemens S7`.
Found 92 result(s) for query: `Simatic -S7 -HMI`.
Found 99 result(s) for query: `"Simatic+S7"`.
Found 98 result(s) for query: `"Simatic S7"`.
Total Results: 622.
Scan Complete. [16/09/2015 11:08:55]
```

Shodan Status: Ready

Figure : Example of SCADA results using SearchDiggity

Moreover, we can use Shodan to find the number of "infected" ports :



134.129.192.141 okl192.141.und.nodak.edu

City	Fargo
Country	United States
Organization	State of North Dakota
ISP	North Dakota State University - Computer Center
Last Update	2015-08-25T15:48:37.382288
Hostnames	okl192.141.und.nodak.edu
ASN	AS6263

Ports

21 80

Services

21 tcp ftp

```
220  RT-IP FTP Server ready. Type HELP for help
530 Not logged in.
214- The RT-IP FTP Server supports the following commands:
214- CWD  DELE HELP LIST MKD MODE NLST NOOP PASS PORT PWD
214- QUIT RETR RMD RNFR RNTO STOR TYPE USER XMKD XPWD XRMD
214- ......................................................
214- use CWD Z: to USE the virtual file system
214  ......................................................
500 Syntax error, command unrecognized or malformed
```

80 tcp http

```
HTTP/1.1 200 Document follows
Connection: Close
Server: EIG Embedded Web Server
Content-type: text/html
Content-length: 587
```

Figure : Shodan result with 2 ports listed

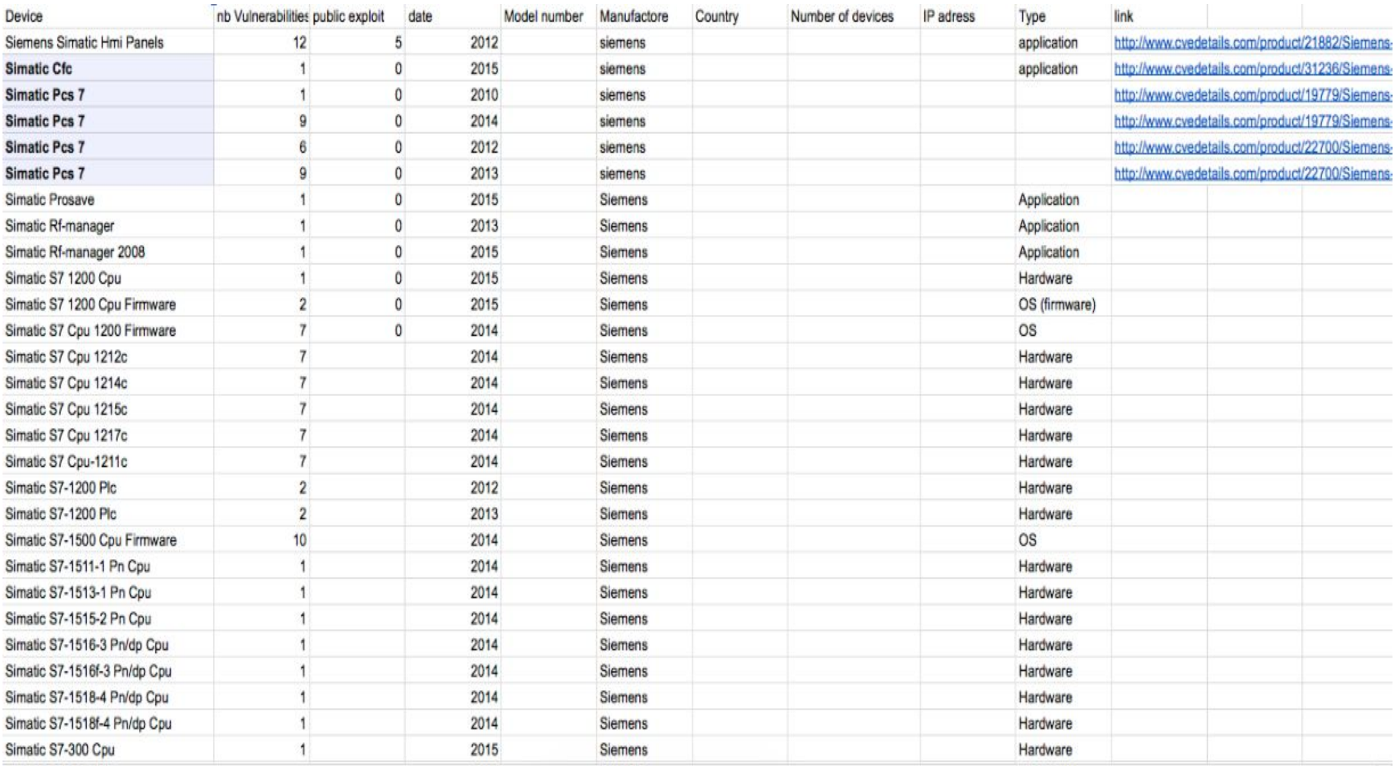
Visualisation of the dataset metrics

The picture below, is a glimpse of how our dataset metrics looks like so far. Although we have different datasets metrics. We need to finalize either to have one dataset for each device or a combined dataset for all the devices.

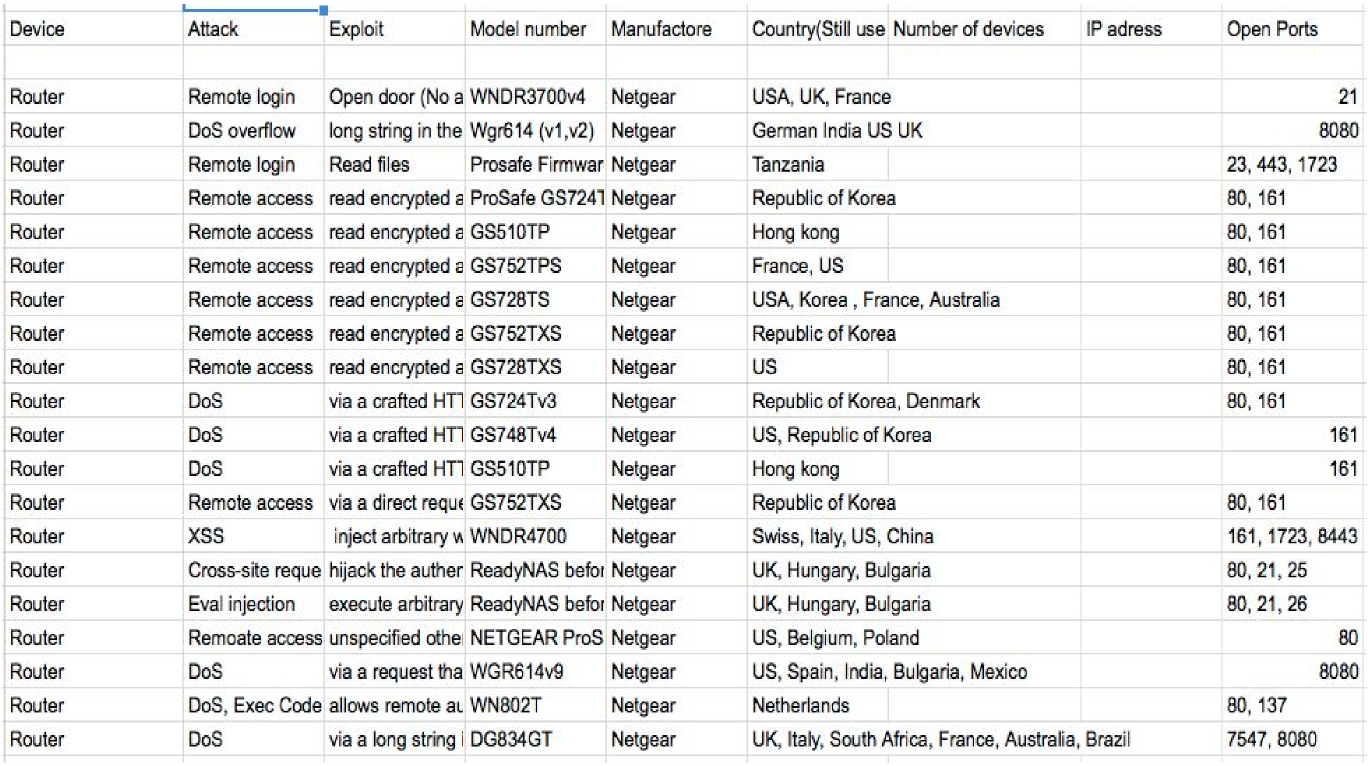
Links to the two data sets

https://docs.google.com/spreadsheets/d/100MptJoORhU4xIF_yzUGkJiDMoTILFlVmejwRwJKNl0/edit#gid=0

https://docs.google.com/spreadsheets/d/1D0CdV_CkaUC41sBfn3G6rMjLtIOYAWBuwUNgKPhS6mI/edit#gid=0



Device	nb Vulnerabilities	public exploit	date	Model number	Manufactore	Country	Number of devices	IP adress	Type	link
Siemens Simatic Hmi Panels	12	5	2012		siemens				application	http://www.cvedetails.com/product/21882/Siemens-
Simatic Cfc	1	0	2015		siemens				application	http://www.cvedetails.com/product/31236/Siemens-
Simatic Pcs 7	1	0	2010		siemens					http://www.cvedetails.com/product/19779/Siemens-
Simatic Pcs 7	9	0	2014		siemens					http://www.cvedetails.com/product/19779/Siemens-
Simatic Pcs 7	6	0	2012		siemens					http://www.cvedetails.com/product/22700/Siemens-
Simatic Pcs 7	9	0	2013		siemens					http://www.cvedetails.com/product/22700/Siemens-
Simatic Prosave	1	0	2015		Siemens				Application	
Simatic Rf-manager	1	0	2013		Siemens				Application	
Simatic Rf-manager 2008	1	0	2015		Siemens				Application	
Simatic S7 1200 Cpu	1	0	2015		Siemens				Hardware	
Simatic S7 1200 Cpu Firmware	2	0	2015		Siemens				OS (firmware)	
Simatic S7 Cpu 1200 Firmware	7	0	2014		Siemens				OS	
Simatic S7 Cpu 1212c	7		2014		Siemens				Hardware	
Simatic S7 Cpu 1214c	7		2014		Siemens				Hardware	
Simatic S7 Cpu 1215c	7		2014		Siemens				Hardware	
Simatic S7 Cpu 1217c	7		2014		Siemens				Hardware	
Simatic S7 Cpu-1211c	7		2014		Siemens				Hardware	
Simatic S7-1200 Plc	2		2012		Siemens				Hardware	
Simatic S7-1200 Plc	2		2013		Siemens				Hardware	
Simatic S7-1500 Cpu Firmware	10		2014		Siemens				OS	
Simatic S7-1511-1 Pn Cpu	1		2014		Siemens				Hardware	
Simatic S7-1513-1 Pn Cpu	1		2014		Siemens				Hardware	
Simatic S7-1515-2 Pn Cpu	1		2014		Siemens				Hardware	
Simatic S7-1516-3 Pn/dp Cpu	1		2014		Siemens				Hardware	
Simatic S7-1516f-3 Pn/dp Cpu	1		2014		Siemens				Hardware	
Simatic S7-1518-4 Pn/dp Cpu	1		2014		Siemens				Hardware	
Simatic S7-1518f-4 Pn/dp Cpu	1		2014		Siemens				Hardware	
Simatic S7-300 Cpu	1		2015		Siemens				Hardware	



Device	Attack	Exploit	Model number	Manufactore	Country(Still use	Number of devices	IP adress	Open Ports
Router	Remote login	Open door (No a	WNDR3700v4	Netgear	USA, UK, France			21
Router	DoS overflow	long string in the	Wgr614 (v1,v2)	Netgear	German India US UK			8080
Router	Remote login	Read files	Prosafe Firmwar	Netgear	Tanzania			23, 443, 1723
Router	Remote access	read encrypted a	ProSafe GS724T	Netgear	Republic of Korea			80, 161
Router	Remote access	read encrypted a	GS510TP	Netgear	Hong kong			80, 161
Router	Remote access	read encrypted a	GS752TPS	Netgear	France, US			80, 161
Router	Remote access	read encrypted a	GS728TS	Netgear	USA, Korea , France, Australia			80, 161
Router	Remote access	read encrypted a	GS752TXS	Netgear	Republic of Korea			80, 161
Router	Remote access	read encrypted a	GS728TXS	Netgear	US			80, 161
Router	DoS	via a crafted HTT	GS724Tv3	Netgear	Republic of Korea, Denmark			80, 161
Router	DoS	via a crafted HTT	GS748Tv4	Netgear	US, Republic of Korea			161
Router	DoS	via a crafted HTT	GS510TP	Netgear	Hong kong			161
Router	Remote access	via a direct reque	GS752TXS	Netgear	Republic of Korea			80, 161
Router	XSS	inject arbitrary w	WNDR4700	Netgear	Swiss, Italy, US, China			161, 1723, 8443
Router	Cross-site reque	hijack the auther	ReadyNAS befor	Netgear	UK, Hungary, Bulgaria			80, 21, 25
Router	Eval injection	execute arbitrary	ReadyNAS befor	Netgear	UK, Hungary, Bulgaria			80, 21, 26
Router	Remoate access	unspecified othe	NETGEAR ProS	Netgear	US, Belgium, Poland			80
Router	DoS	via a request tha	WGR614v9	Netgear	US, Spain, India, Bulgaria, Mexico			8080
Router	DoS, Exec Code	allows remote au	WN802T	Netgear	Netherlands			80, 137
Router	DoS	via a long string i	DG834GT	Netgear	UK, Italy, South Africa, France, Australia, Brazil			7547, 8080

Conclusion

As we are group of 4 students. And according to the plan we decided to investigate 4 different systems or different brands of a system. Among all the systems, we decide to concentrate on Netgear, D-Link, Scada systems, and Siemens and find out how vulnerable these devices are. First we research about the possible vulnerabilities in different versions, firmware of the intended systems. For the above task we used CVE and national vulnerability Database. But later on we realized CVE Database is not that trustworthy. So we started looking for some other sources to verify the information we get from CVE Datasets. Although most of the information we got from CVE database were also mentioned by other sources.

So we start looking for these vulnerable devices if they are still in use. We used shodan to look for these devices using the devices firmware or model number. We found significant number of these devices still in used in different countries. The last challenging part which unfortunately we couldn't accomplished is that to get the IP address of the vulnerable devices from shodan and look for these IP address in virustotal to verify if these IP address are really blacklisted. We couldn't accomplish this task because when we search for these IP address in virustotal, virustotal doesn't give any result. But we are trying to find some alternative way to accomplish this challenge. We looked for some API to extract data from virustotal and cleanMX but so far no success.