UNIVERSITY OF TWENTE.

Economics of Cybersecurity

Assignment Block 2 - Project 3

Group 3:

Vincent ROCHER-MONNIER
Diego SAINZ
Uraz SEDDIGH
Ikram ULLAH

1. Introduction

The assignment involves gathering of datasets on security vulnerabilities and relevant metadata, to be able produce realistic (or unrealistic) metrics over the dataset. The goal is to be able to methodically use the gathered data in security related decision making.

Our approach involves the online metadata search engine, Shodan, as well as vulnerability databases, National Vulnerability Database (NVD) and CVE Details. During the study, we have looked into a certain category of online devices, namely Routers and SCADA systems. At the same time, on the aspect of vulnerabilities, our focus was Denial of Service attacks (DoS).

From an economic perspective, any successful DoS attack has a financial impact because of the lost productivity. This is the least effect. Depending on the operational importance of the device under attack, DoS has hefty consequences. Consider SCADA systems running the industry and infrastructure of a country coming under attack and become unresponsive.

The reason we focus on DoS is the fact that these attacks are much more feasible for the perpetrator and for this exact reason, we can see a high percentage of associated vulnerabilities with systems are categorised as DoS. Just as an example, if you search for known vulnerabilities of Siemens SIMATIC S7 (a type of industrial control hardware) in NVD, 14 out of 26 listed vulnerabilities are of the type DoS. The number of DoS vulnerabilities are 12 out of 24 for VxWorks, the most widely deployed real-time embedded operating system in industrial setups.

Routers on the other hand, might not be considered as strategic as industrial systems, but given the sheer number of installed devices, any vulnerability provides a vast attack surface. Concerning D-Link routers, 17.3% of attacks are DoS, which is in the top 3 of the most common attacks against D-Link routers since 2001.

2. Security issue (the security question)

Let us formulate a security question, which would be beneficial from a defence perspective to be answered.

Is there a relationship between patch management of hardware device firmwares and the exposed attack surface? Can we improve attack resistance by keeping devices up-to-date and what is actual practice in a production environment? How industrial devices compare to domestic devices?

Before we start accumulating data and analysing it, there are a number of immediate known facts.

- SCADA systems have and use different WAN connections and remote communication protocols, making up the attack surface and. As a result, DoS attacks are highly feasible.
- It is important to consider two important facts regarding this, the priority in industrial systems is Availability. This is in contrast to general purpose IT environments and their first priority, data Security. These facts affect the analysis and chosen metrics.
- The effectiveness of having the latest patch for a firmware also depends on how fast the vendor responds to vulnerabilities. There might be a big time gap from the current version, till the next fixed version.
- An updated firmware can solve both Software Flaws (CVE) and Misconfigurations (CCE). As an example for the latter case, a vulnerable firmware, could have a form of remote login enabled by default, using default credentials. In fact, this very example has been the case for many vendors.
- Legacy devices may not be capable of running the latest versions of available firmwares. This is a result of limited hardware performance, or an obsolete hardware platform. This point is one of the main reasons behind the fact that, legacy devices are vulnerable by definition.

2.1 Routers

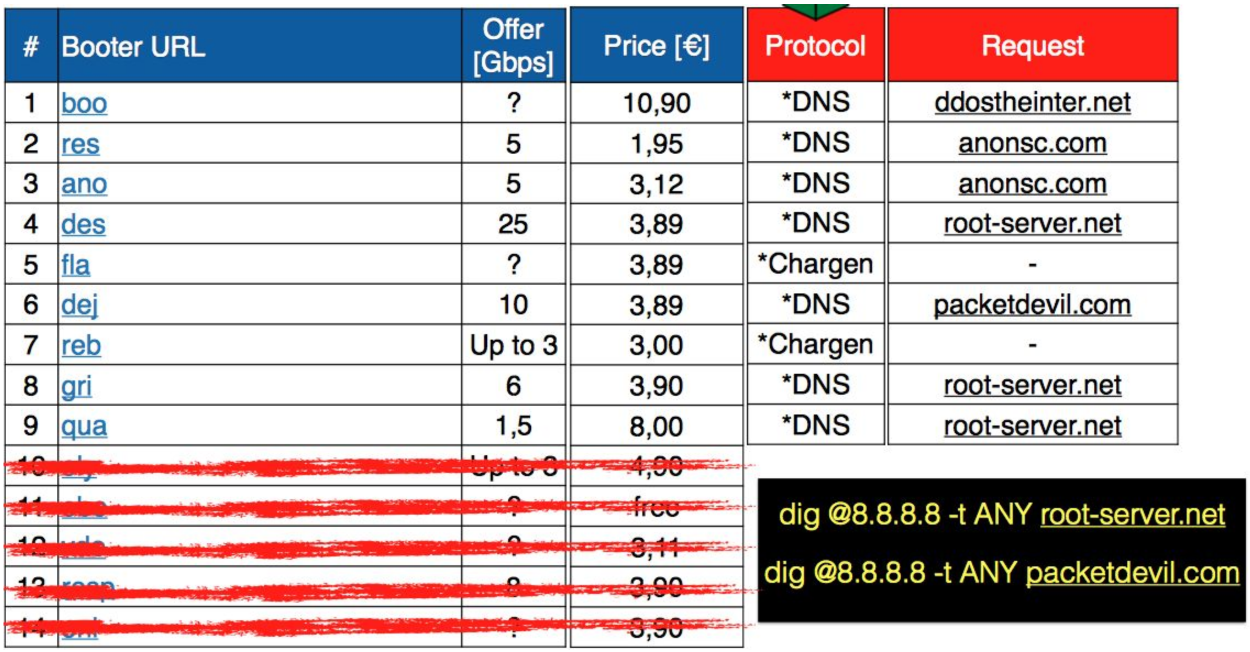
By carefully analyzing our data set, we have found out that almost all the router devices with different versions have one or more vulnerabilities. These vulnerabilities can range from basic ping-to-death attack to DoS attack. Well there can be many reasons behind these attacks. Lack of research and testing before implementation of any algorithm, wrong implementation of the algorithm, or it can be using vulnerable libraries, which can be easily exploited by the attackers. Different attacks have different disruption impact.

2.1.1 Does the attacker intentions are only limited to DoS? or he want something more disruptive DDoS?

Of course the attacker will not stop, he will continue to have a greater attack (DDoS). The worst-case scenario is when all the vulnerable devices are misused at the same time to attack a server or a system. Some time vulnerable devices are not just exploited but they can be used in some devastating and sophisticated attacks. One of these catastrophic attacks is Distributed denial of service attack (DDoS). A distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users[1].

In a typical DDoS attack, the assailant begins by exploiting vulnerability in one computer system and making it the DDoS master. The attack master, also known as the botmaster, identifies and identifies and infects other vulnerable systems with malware. Eventually, the assailant instructs the controlled machines to launch an attack against a specified target [1]. This sort of attack not only disrupts the services but it has become the biggest threat to the Internet security.

The attacker just has to make an account on any of the available booter website. It just cost 10-20 Euro. So with just few Euro it is absolutely possible to make offline any server in the world. For the botmasters , they just need to find vulnerable devices like routers and used them as reflectors and amplifiers in the attack. Also with this sort of attack it’s hard to track back the attack as the attack is coming from million of vulnerable devices throughout the world. One of the practical examples in Netherlands is when an attacker used booter to attack his school server during exam session. Figure below shows the prices of different booters.



#	Booter URL	Offer [Gbps]	Price [€]	Protocol	Request
1	boo	?	10,90	*DNS	ddostheinter.net
2	res	5	1,95	*DNS	anonsc.com
3	ano	5	3,12	*DNS	anonsc.com
4	des	25	3,89	*DNS	root-server.net
5	fla	?	3,89	*Chargen	-
6	dej	10	3,89	*DNS	packetdevil.com
7	reb	Up to 3	3,00	*Chargen	-
8	gri	6	3,90	*DNS	root-server.net
9	qua	1,5	8,00	*DNS	root-server.net
[redacted]	[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]		

```
dig @8.8.8.8 -t ANY root-server.net
dig @8.8.8.8 -t ANY packetdevil.com
```

Figure 1: Booter prices [4]

2.1.2 Impact of DDoS attack

DDoS attacks are increasing very fast. Almost becoming double every year. According to [2] in 2013, 60% of companies were DDoS attacked, up from 35% experiencing a disruptive attack in 2012. Although most of the routers are in domestic use but they can be put into work to attack commercial, health, educational and financial organizations.

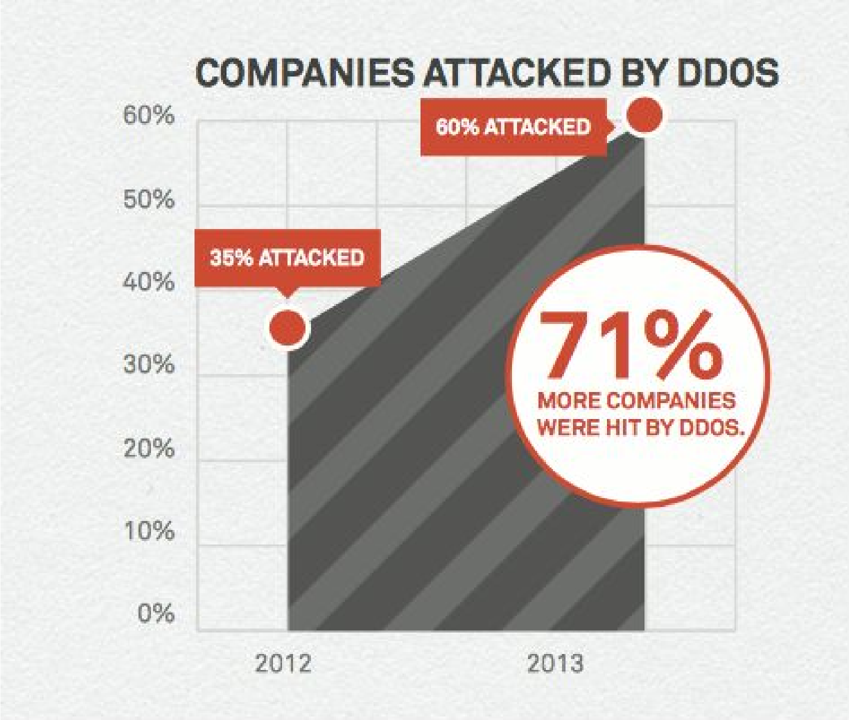


Figure 2: DDoS attacks on companies [2]

Most of the companies don’t have any detection or protection system against these attacks. Again according to [2] DDoS outrage for one hour can cost a company $50k-100k or more. In 2000 yahoo and Amazon lost over 1.2 billion due to DDoS attack.

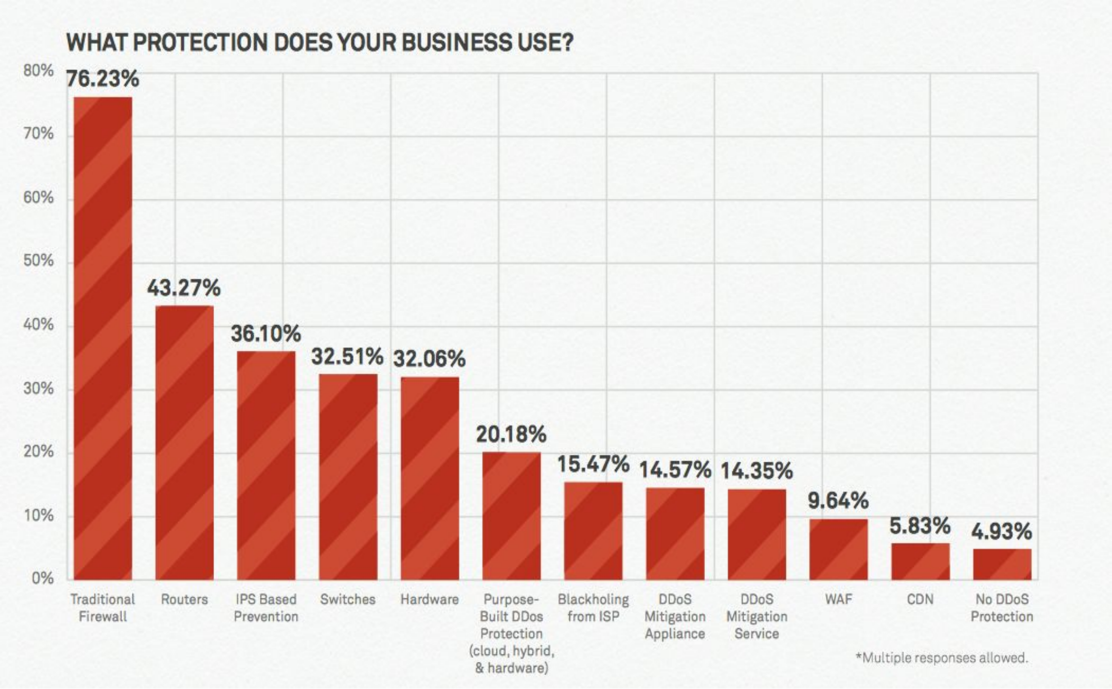


Figure 3: Distribution of employed protection [2]

DDoS attack is costing companies heavily. Below are some of the impacts in 2013.

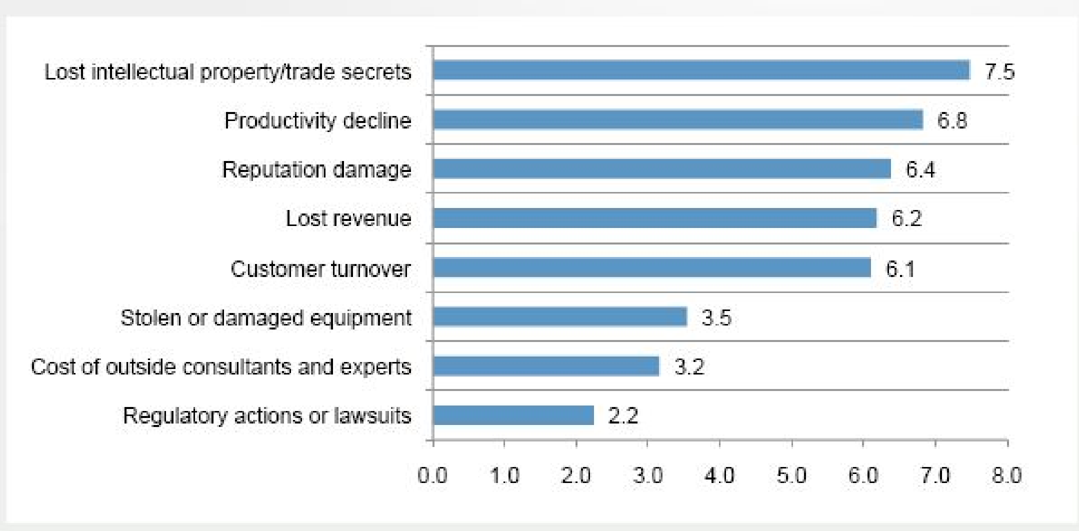
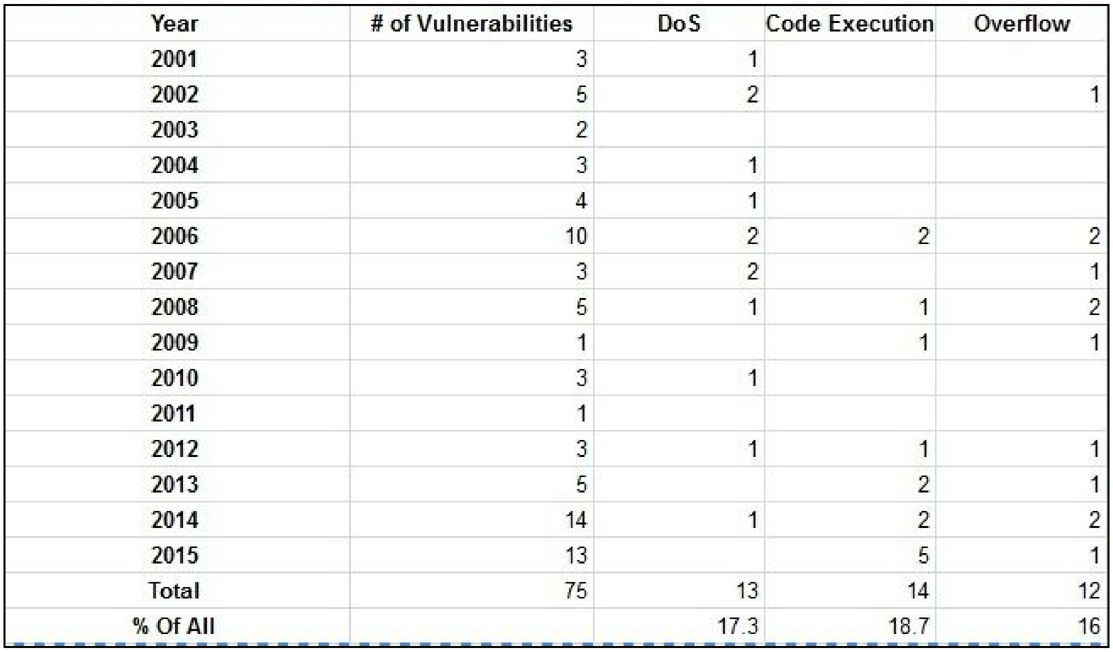


Figure 4: The impacts of DDoS on companies [3]

2.1.3 Number of vulnerabilities detected by rooter brand?

We will consider two different brands of routers that are Netgear and D-Link. If we see the dataset of Netgear, almost every version of Netgear is vulnerable to one attack or the other. From shodan we found more or less 30,000 Netgear and 29,815 D-Link routers that are vulnerable but still in use. Around 10,000-20,000 of the total are vulnerable to DoS attack. So from an attacker perspective having almost 60,000 amplifiers are more than enough for a devastating DDoS attack. Here we are only considering netgear and D-Link vulnerable devices if we consider all the brands this attack might easily paralyzing the whole Internet. Just as an example from my Network security project, few thousand vulnerable devices(that can be used as amplifiers) can generate many Gbps DoS traffic that’s enough to disrupt any server or service.

Also there are many vulnerabilities in D-Link routers, 75 listed by CVE Details (Table 1 below). The number of vulnerabilities in D-link routers in 2015 is higher than in 2001. This might be just because of the fact that the attackers are getting smarter and smarter or just simply the devices are not updated.



Year	# of Vulnerabilities	DoS	Code Execution	Overflow
2001	3	1		
2002	5	2		1
2003	2			
2004	3	1		
2005	4	1		
2006	10	2	2	2
2007	3	2		1
2008	5	1	1	2
2009	1		1	1
2010	3	1		
2011	1			
2012	3	1	1	1
2013	5		2	1
2014	14	1	2	2
2015	13		5	1
Total	75	13	14	12
% Of All		17.3	18.7	16

Table 1: Table of attacks on D-Link routers from CVE Details (extract)

If we want to consider that either these vulnerabilities are because of hardware or software issues? I think it is clear from the dataset that there are equal number of hardware and software issues. Most of these vulnerable netgear devices are in UK and Republic of Korea.

2.1.4 Why these vulnerabilities are still present?

Almost all the attacks that were present decade ago are still present in the modern versions. There can be many reasons why they are still present. Below are some of the reasons.

- Expensive to implement in practice: There are certain protocols that might be easy to proof secure on paper but hard to implement in practice. Sometime it might take decades to implement in practice. One known example is Elliptical Curve Cryptography.
- Efficiency: The vendors might prefer efficiency over security. There might be secure protocols but if they are implemented it might not be efficient in the sense of speed, and energy consumption.
- Restrictions in standards: Some standards consider compulsory to use of some algorithms or protocols. Although that protocol might be proved insecure. Like the use of RSA in DNS.
- Public is unaware: Even if the devices and algorithms are made secure still the public has least security knowledge.
- No updates: Either there are no updates or the public is reluctant to update or it is hard to update a large scale network.
- Smarter the hackers: Attackers are getting smarter and smarter day by day.

- Research: Test before implementation of any new protocols. One failed example is the implementation of DNSSEC.
- DNSSEC protocol: DNSSEC protocol made it easier for the attacker to carry on the DDoS attack. Because of the high amplification factor. According to Dan Bernstein “DNSSEC is a remote-controlled double-barreled shotgun, the worst DDoS amplifier on the internet”

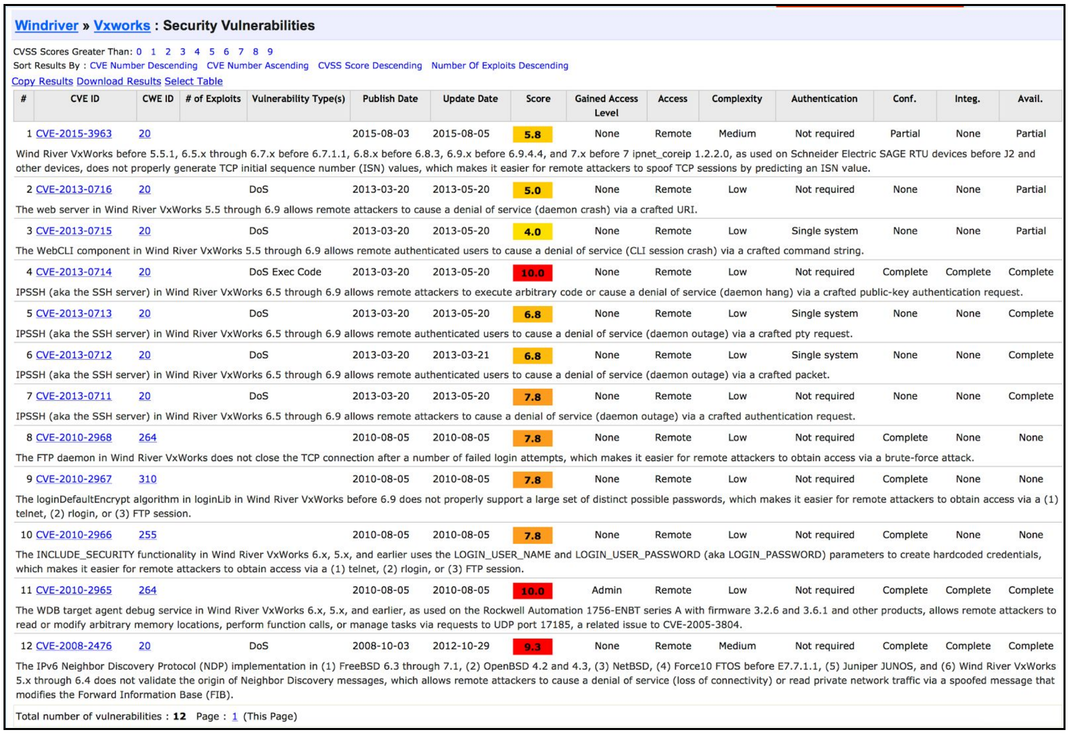
2.2 SCADA systems

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.

2.2.1 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 5.



Windriver » Vxworks : Security Vulnerabilities

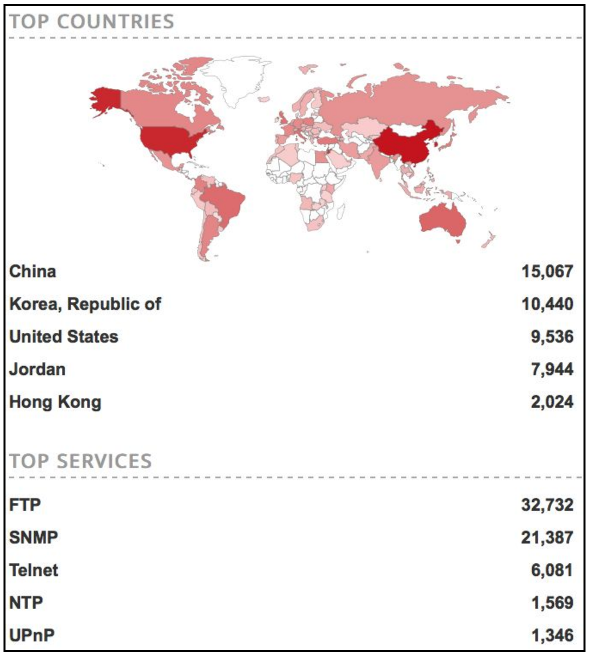
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results Select Table

<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 5: 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 6. This query is for VxWorks.



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 6: Number of available devices running 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

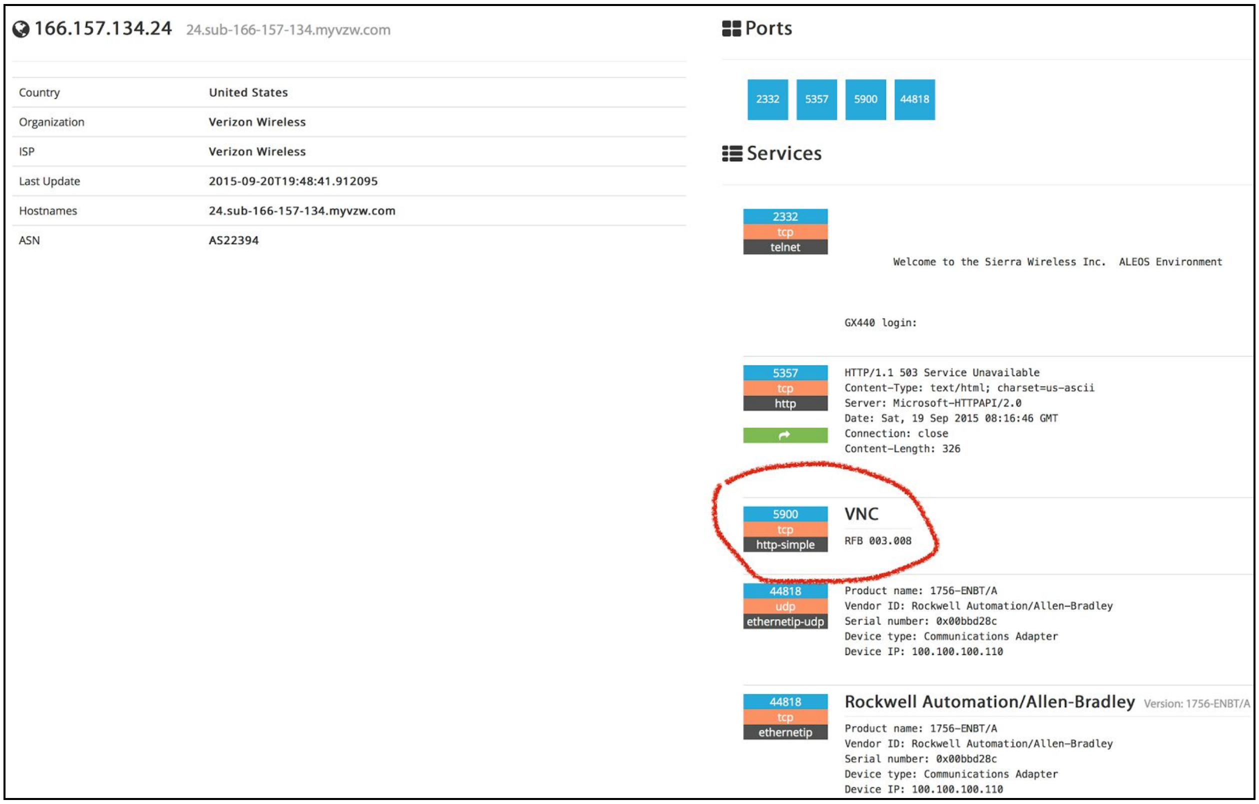
These vulnerabilities affect TSX ETG 3000, TSX ETG 3010, TSX ETG 3021 and TSX ETG 3022 models of FactoryCast HMI Gateways from Schneider (formerly Telemecanique). So one can start by looking for HMI (Human Machine Interface) in Shodan and narrow it down. Overall 17 immediate results can be found, which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

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 7 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

Ports

2332 5357 5900 44818

Services

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 7: VNC port 5900 access

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

2.2.2 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.

3. Metrics to measure the situation

By focusing on the patch management aspect, we can define our metrics as follows.

- The first and foremost, the difference of installed firmware version from the latest firmware version. This needs to be checked separately for each device model. In cases of common platform, different devices of the same platform can be combined in the dataset.
- The second metric is the ratio of up-to-date devices to all devices, within the same category, e.g. Routers. By comparing this metric, one can see if there is any difference in patch management practices, depending on the segment, e.g. industrial applications, or residential applications, or business applications.

It is important to mention that, the date of release for firmwares also comes into play. If the gap between a firmware release and the publishing of a vulnerability is big, then the effectiveness of the update is lower and as a result, the financial impact, more serious.

It is possible to create a risk scale for each device model, in regards with DoS attacks, as

$$M \times V_{fw},$$

where M is the difference between the installed firmware and the latest firmware, in months, and V_{fw} is the number of known DOS vulnerabilities of the installed firmware. The idea can be expanded by multiplying the number of similar cases with the same firmware to the previous calculation, as

$$M \times V_{fw} \times n.$$

Now to have a more realistic scale, we should make the impact of M logarithmic, meaning that the older the installed firmware, the worst will be the negative impact, in an exponential fashion. This is due to the fact that the vulnerability will be known by more people and more techniques to manipulate the vulnerability can be developed. The power needs to be calculated, but for the sake of presentation, we can consider the following formula,

$$M^2 \times V_{fw} \times n\,.$$

The scale can be useful for comparison of different product segments, e.g. industrial vs. residential vs. business applications.

Example: Simatic S7 Cpu 1212c
According to the vulnerability statistics from CVE Details, 57.1% of the vulnerabilities for this model are DoS. All DoS vulnerabilities are related to firmwares previous to version 4.0. These DOS vulnerabilities were published on 2014-03-24. A quick search in Shodan reveals that only 15 from 50 devices (just a sample) are of v.4.0 or above. Therefore, only 30% are secure against these known DoS attacks. None of the devices have the latest v4.1.3 firmware.

The distribution of vulnerabilities by type is depicted in Figure 8.

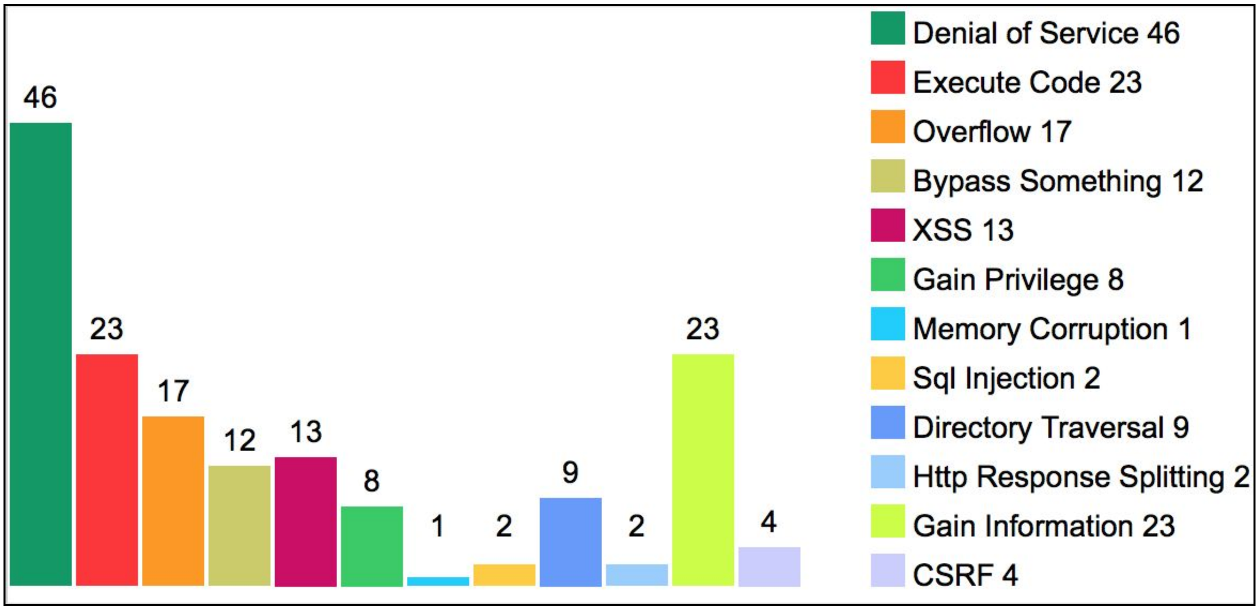


Figure 8: Vulnerability distribution for CPU-1200 series by type

Now focusing on DoS, Figure 9 shows the increase in the number of total known vulnerabilities and DoS vulnerabilities, on a yearly basis.

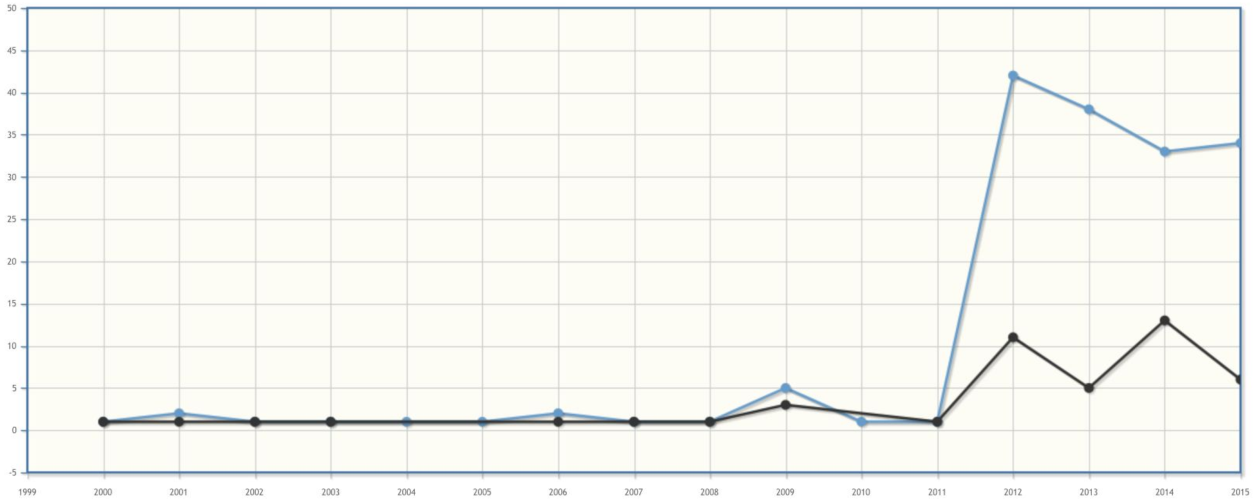


Figure 9: Number of total vulnerabilities and number of DoS vulnerabilities, on a yearly basis (blue line: total, black line: DoS)

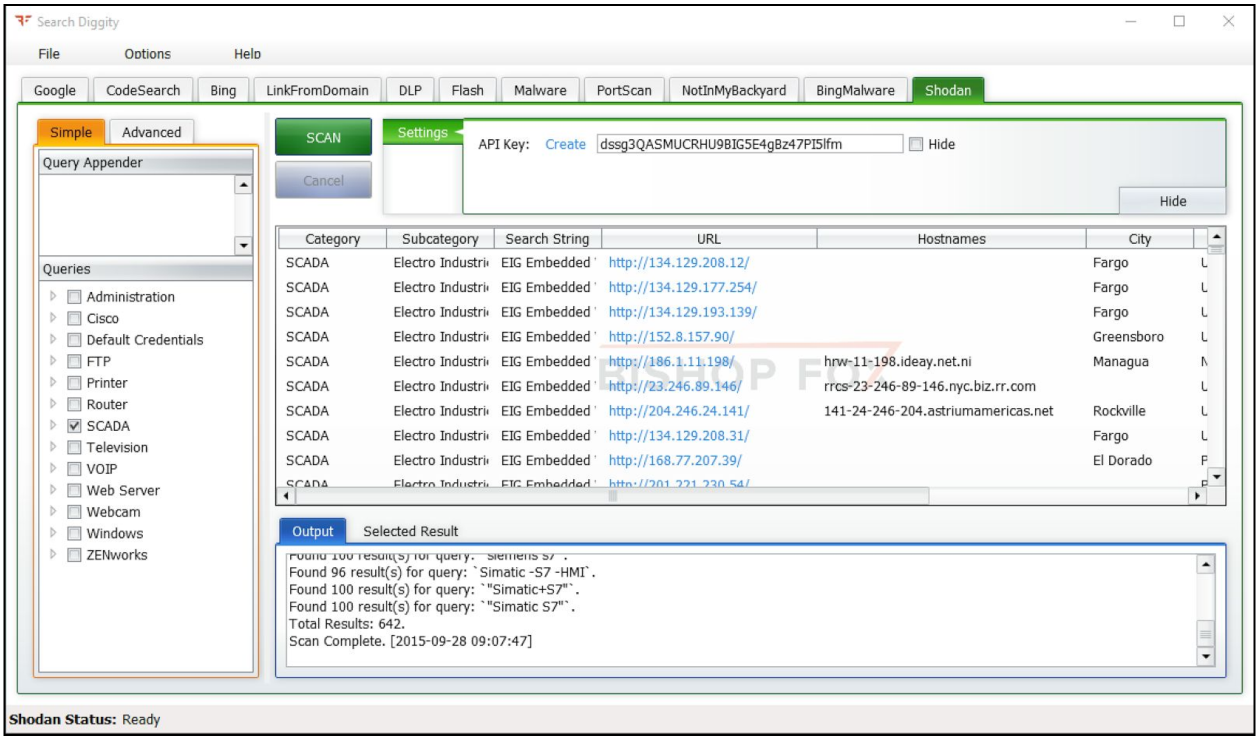
Concerning D-Link routers updates, our dataset shows that in 2001, updating firmwares could last several years (2561 days for the longest !) and in 2015, the longest is only 23 days, that shows that D-Link is now more aware of the importance of patching.

3.1 Limitations

There are a number of limitations present. In our case, to be able to use Shodan to the fullest of its features, one has to pay for the service, which we did not consider for this assignment. Another issue is that, although Shodan provides firmware information, but it is not straightforward to include it in an export. A custom data mining process needs to be in place for mass data gathering.

3.2 Alternative tool

An alternative tool to the web interface of Shodan exists, with the name of SearchDiggity, which is a GUI client for the search engine. SearchDiggity is part of Google Hacking Diggity Project and can be used to gather information on variety of subjects. Although it has more diverse export options, but the exclusion of firmware data is still an issue. The GUI can be seen in Figure 10.



Queries

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

API Key: Create dssg3QASMUCRHU9BIG5E4gBz47PI5lfm ☐ Hide

Category	Subcategory	Search String	URL	Hostnames	City	
SCADA	Electro Industri	EIG Embedded '	http://134.129.208.12/		Fargo	U
SCADA	Electro Industri	EIG Embedded '	http://134.129.177.254/		Fargo	U
SCADA	Electro Industri	EIG Embedded '	http://134.129.193.139/		Fargo	U
SCADA	Electro Industri	EIG Embedded '	http://152.8.157.90/		Greensboro	U
SCADA	Electro Industri	EIG Embedded '	http://186.1.11.198/	hrw-11-198.ideay.net.ni	Managua	N
SCADA	Electro Industri	EIG Embedded '	http://23.246.89.146/	rrcs-23-246-89-146.nyc.biz.rr.com		U
SCADA	Electro Industri	EIG Embedded '	http://204.246.24.141/	141-24-246-204.astriumamericas.net	Rockville	U
SCADA	Electro Industri	EIG Embedded '	http://134.129.208.31/		Fargo	U
SCADA	Electro Industri	EIG Embedded '	http://168.77.207.39/		El Dorado	P
SCADA	Electro Industri	EIG Embedded '	http://201.221.230.54/			P

```
Found 100 result(s) for query: `Siemens S7`.
Found 96 result(s) for query: `Simatic -S7 -HMI`.
Found 100 result(s) for query: `"Simatic+S7"`.
Found 100 result(s) for query: `"Simatic S7"`.
Total Results: 642.
Scan Complete. [2015-09-28 09:07:47]
```

Shodan Status: Ready

Figure 10: SearchDiggity

4. Conclusion

Our investigation, considering all available vulnerability databases, and metadata search engines for exposed devices on the Internet, has a number of immediate results.

DOS is the major vulnerability: As mentioned before and within the examples, the most common and thus, the costliest vulnerability is DoS attacks. This is especially a hassle for devices that are supposed to be online anyway, such as industrial remote control devices, or routers.

Poor patch management: The state of keeping firmwares up-to-date is less than ideal. This is especially prevalent in regards with SCADA devices. Industry is based on continuous availability and because of that, updates are not a priority. Another reason which should be investigated is the fact that, certain embedded devices lack the ability of online, or remote automated updates. Therefore, someone with the necessary IT knowledge should carry out the upgrade on site.

Research Matters: Before deploying any protocol or hardware, it should be extensively checked for vulnerabilities. DNSSEC(Domain Name System Security Extensions) was deployed either knowing its catastrophic impacts or just ignoring its impact. Thus it is now leading to an unstoppable DDoS attacks. So before deploying ECDSA(Elliptic Curve Digital Signature

Algorithm) as a signing algorithm in DNS it should be researched well. Fool me once, shame on you. Fool me twice…….

Public Awareness: The general public should be made aware of security issues, configuration settings and attacks.

References

[1] http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack
[2]
https://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf
[3] http://blog.radware.com/security/2013/05/how-much-can-a-ddos-attack-cost-your-business/
[4]https://learnnetsec.org/week1/slides/20150909_network_security_course_v2.pdf