Identifying Industrial Devices Potentially Vulnerable
using the search engine Shodan

Juan Basaez
Linköping University
Linköping, Sweden
juaba731@student.liu.se

***Abstract*—Shodan can be used by anyone. Using it, anyone can gather information about internet-connected devices. Information about their location, operating system, model, manufacturer, and their communication protocols. That information can be used to secure a network, but it can also be used to plan and perform an cyber attack. Industrial Control Systems (ICS) are considered critical systems; therefore, they leaking sensitive information, and as a consequence of that, being a target of a successful cyber attack, can signify considerable damages. That is why it is important to study if there are vulnerable industrial devices being used and publicly connected to the internet. Previous researches at Linköping University have shown the most used protocols, their relation to well-known vulnerabilities, and the number of devices using every protocol; now, the focus have been put on identifying the specific devices being used through those protocols in Sweden. Exposing not only the amount of internet-connected devices using every protocol, but also their specifications or even exact location, makes it easier for any attacker to gather information and plan a cyber attack. Shodan, previous performed researches, and security vulnerabilities databases have been used to identify industrial devices connected in Sweden. The obtained results show that hundred of the exposed devices can be identified and that many of them could be considered potentially vulnerable because of the information they are leaking, their lack of support, their relation to well-knwon vulnerabilities, or the access they are giving to.**

***Index Terms*—ICS, Shodan, vulnerabilities, Sweden**

I. Introduction

The world becoming more and more industrialised and internet-connected seems to be an endless process. A process which contributes to development and improvements, but which could also becomes a problem when tools like Shodan [1] exists and it is used for malicious purposes.

Shodan is a search engine that crawls the internet for internet-connected devices being able to find information about devices like webcams, routers, or even refrigerators. Shodan finding a device means that information about that device's location, manufacturer, model, operating system, ports and communication protocols, can be obtained. Then, among that information, some sensitive information can be gathered and used to plan and try an attack. Many of those attacks can failed, or many of them can gain access to webcams and may not cause significant damage at all. But what could happen when the sensitive information can be used to gain access to some industrial device being a part of some critical system? That is why industrial devices, constituting critical systems, being publicly connected to the internet can lead to serious security issues when the found information can be used to perform an attack. That is the reason why it is imperative to analyse the state of industrial devices connected to the internet and identify if any of them are potentially vulnerable.

This paper presents statistics about ICS protocols in Sweden, the number of devices being used, and the ones that have been identified. Four of the five most used ICS protocols have been analysed in depth in order to learn the number of devices that could be identified by manufacturer, model and version. A possible relation between devices and well-known vulnerabilities was also studied. In addition to that, a parallel research was performed in order to gather information about vulnerabilities affecting specific ICS devices; so by using Shodan, it was possible to find out if any of those devices were exposed to the internet.

This paper is structured as follows:

- Background (II): Definitions of important terminology named later in the paper.
- Methodology (III): Description of the implemented methodology.
- Results (IV): The results are structured as follows.
  - Number of internet-connected devices using ICS protocols in Sweden.
  - The identified devices using protocols Modbus, BACnet and Omron.
  - Other industrial devices potentially vulnerable (using other ICS protocols)
- Related previous work (V): Comparison to previous related work.
- Conclusion (VI). Brief discussion around obtained results and conclusion of the paper.

II. Background

This section contains background information about some of the subjects that are mentioned in this paper.

A. Industrial Control Systems

ICS is the terminology used when making reference to systems that allow to control and monitor operation of industrial processes. The industrial process may involve the usage of devices programmable logic controllers (PLCs), programmable automation controllers (PACs), remote terminal units (RTUs), intelligent electronic devices (IEDs) and sensors. Among the types of ICS, the Supervisory Control and Data Acquisition (SCADA) figures as the most common followed by Distributed

Control Systems (DCS) and Industrial Automation and Control Systems (IACS) . [2] [3] [4]

B. Shodan

Shodan is a search engine for everything internet-connected, it crawls the internet in order to finds devices that exist online. Shodan indexes things like web cams, water treatment facilities, medical devices, wind turbines, traffic lights, as well as smart technologies like Tvs, refrigerators or even smart houses. This search engine works by scanning the entire Internet and parsing the banners that are returned by various devices. Shodan can be used to manage enterprise's networks and lock down security vulnerabilities, but its usage has become more popular among *hackers* because it provides a powerful reconnaissance tool for attackers. Using Shodan, anyone can easily find, for example, information about ICS devices exposed on the Internet, including related IP address, open services/ports, devices specifications, attached web interfaces and existing vulnerabilities associated. [5] [6] [7]

III. Methodology

As already mentioned, the main tool used to find the ICS devices being used in Sweden was the search engine Shodan. In order to start looking for the devices using every ICS protocol, it was needed to know which ports the protocols are using. With that information, the search on Shodan could be based on the port and the country Sweden; for instance, the filter *port:502 country:se* fetches devices using the Modbus protocol in Sweden. The name of the searched protocols and their respective default ports are shown in table I.

TABLE I
ICS PROTOCOLS

Protocol	port
Modbus	502
BACnet	47808
DNP3	20000
Omron Fins	9600
Tridium Fox	1911
Mitsubishi MELSEC-Q	5006/5007
General Electric SRTP	18245/18246
ProConOS	20547
EtherNetIP	44818
RedLion	789
PCWorx	1962
Siemens S7	102
Codesys	2455
IEC-104	2404
Tridium Fox + SSL	4911

Two different methods have been used in order to identify, from one side, the specific devices being used through protocols Modbus, BACnet, DNP3 and Omron; and from the other side, devices potentially vulnerable to well-known exploits.

A. Protocols analysed in depth

In order to identify the devices using the 4 mentioned protocols, an analysis in depth was performed. In depth means that the results obtained when looking for ports 502, 47808, 20000 and 9600 in Sweden, were analysed one by one. When searching for a port in Shodan, besides the pages of results of IP addresses using the service, it lists the countries and organisation related to those IP addresses, as well as the *products* using the searched protocol. That list of products contains information about model or name of devices, but since many devices do not disclose their model name in the banner, that list is possibly missing a considerable number of products; so, deeper searches were required to try to identify as much devices as possible. The methodology consisted then of analysing all the IP addresses obtained as results, one by one. Some devices were disclosing enough specifications to identify them by manufacturer, model and version, but other ones only showed slaves messages which led nowhere. Many devices required further internet searching and even deeper search on Shodan using, for example, some banner field as filter for the searching.

B. Identification of other vulnerable devices

Internet searches were performed looking for well-known vulnerabilities affecting ICS devices. After finding a vulnerability, information about devices potentially affected by it could be gathered, so that information related to those devices could be used as filter in Shodan. Different combinations of keywords were then used as filter. Combinations like *port: country: manufacturer:*, *port: country: banner_field*, *port: country: http.title*, or even deeper like *port: country: manufacturer: server: version:*. They are not the exact keywords used, neither the only ones, but they are a good example to show the many different variants of filters Shodan allows to be used. Basically, any word that is displayed in a banner, can be used as pivot to search further for a specific device.

IV. Results

Figure 1 shows the complete results obtained with Shodan when searching for all the ports listed in table I. In the figure, it is detailed the number of devices using those services in Sweden.

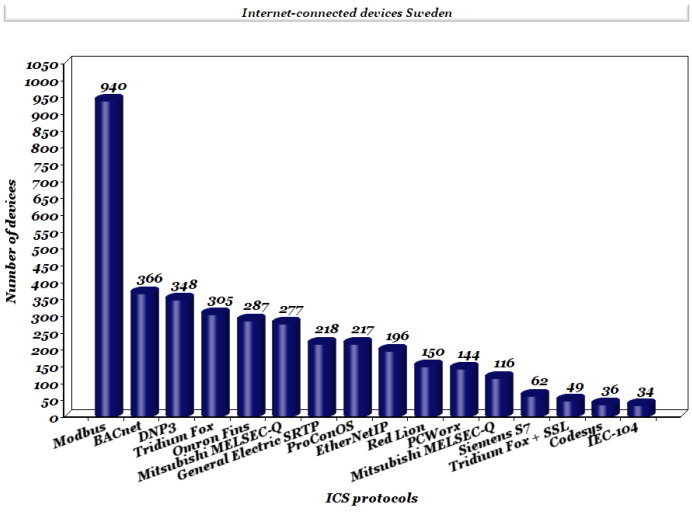

Fig. 1. Number of devices using ICS protocols in Sweden.

As it can be noticed in figure 1, the total number of devices that can be found with Shodan is **3745**; being Modbus the most used service with 940 devices, followed by BACnet with 366. The ports being *assigned* to a service like an ICS protocol, or being known as the port used by an ICS protocol, does not mean that the port is exclusively used for that service. That means that the obtained results are illustrating the number of devices internet-connected using the searched ports, but the results do not ensure that all those devices are ICS devices. Showing the total number of devices using the ports facilitate the later comparison made with previous researches done at the university, where the exact number of ICS devices using every port was not detailed. For this study, the exact number of existing ICS devices communicating through every port was neither illustrate since no complete reliable and accurate methodology to do it has been found. According to Shodan, Sweden is in the 28 th place using the mentioned protocols worldwide, where the total of exposed devices is 1.001.448. Figure 2 shows the 10 countries with most exposed devices using the protocols, and Sweden as comparison.

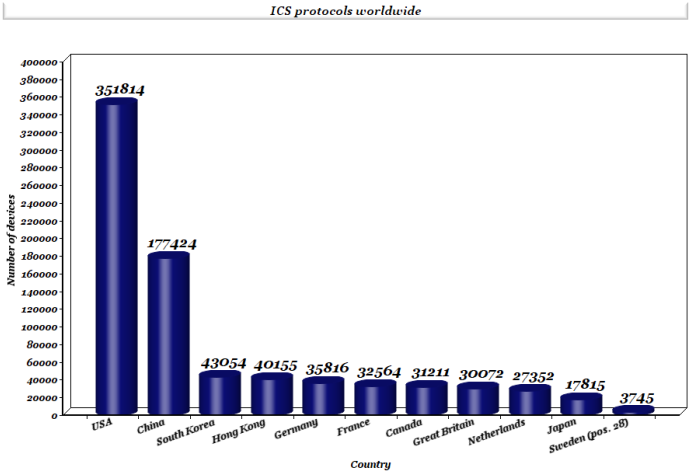

Fig. 2. ICS devices using protocols listed in table I worldwide.

The protocols Modbus, BACnet, DNP3 and Omron were analysed in depth in order to learn how many devices, out of the total found, could be identified with certainty. Their possible relation to well-known vulnerabilities were also studied, as well as the risk their online exposure could signify based on the information they are leaking. Based on well-known vulnerabilities related to ICS devices, potentially vulnerable devices, using other protocols, were identified. The following information is divided in the mentioned protocols and the rest of the identified devices.

A. Modbus

Out of 940 devices using Modbus, **462** have been identified with certainty. Figure 3 illustrates the number of identified devices and the manufacturer they belong.

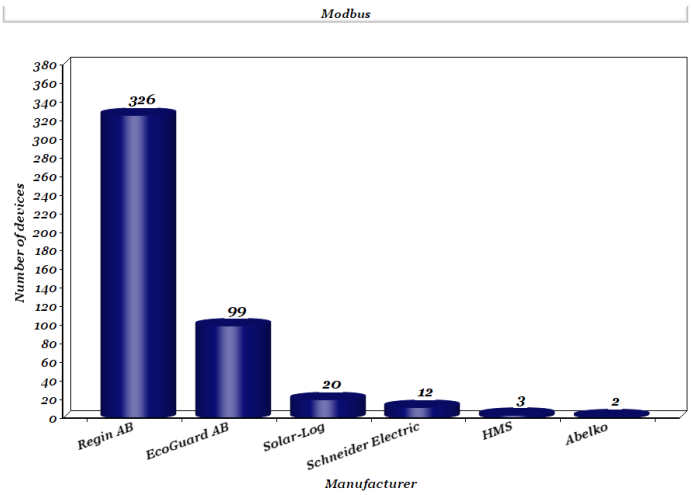

Fig. 3. Identified devices using Modbus.

1) Regin AB: **326** devices have been found under the vendor name *Regin AB*. They are a type of controller named *Corrigo* [19]. They can be controllers for ventilation and heating, or heating only. No vulnerabilities related to these controllers have been found, nothing more than the fact that almost all of them are giving access to a login panel, most by ports 80/443. Nevertheless, the login panel is presenting some kind of problem, or it is no longer used; therefore no login action can be performed.

2) EcoGuard: **99** EcoGuard devices were identified thanks to the information they are attached to through ports 80/443 where access to a web server interface called *EcoCom* is given. The EcoCom service is offered by *EcoGuard* and used to monitor and control measurement of temperature, water and energy. The first worrisome thing around these devices is that none of them requires authentication, that is, anyone can get direct access to the monitoring interface. An even more worrisome detail is that 11 of those 99 contains more detailed information about M-bus devices (sensors), their measurements and even the M-bus converter being used (*Elvaco CMeX13S* [22]. The risks here are the sensitive information that is being leaked, information about measurements and what is being used, but even about the network and ports. Besides, the interface allows any *user* to modify settings or configuration related to the connected M-bus devices. Figure 4 below shows the diagram of the communication between the monitoring device *EcoCom*, the M-bus converter and the M-bus devices.

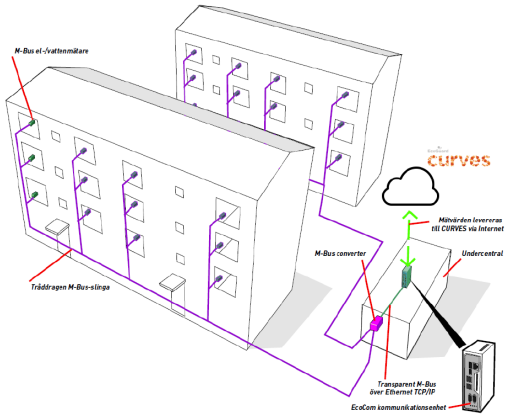

Fig. 4. Communication between EcoCom, Elvaco converter and M-bus devices.

As previously mentioned, it was possible to identify 99 EcoGuard devices because of the EcoCom web interface that can be reached. The Shodan banner obtained through port 502 showed only the *slave id data LMB 3.0.3*, but nothing related to that information was found. It becomes relevant to mentioned this because 202 devices were showing the same slave id data. 103 were not attached to any web interface, but since the 99 devices identified with certainty had the same slave id data then the other 103, it is possible that the 202 devices are the same EcoCom service. Under that supposition, the number of identified EcoGuard devices would ascend to **202** and the total of Modbus to **565**.

3) Solar-Log: Solar-Log products are described as products setting new international standards when it comes to monitoring and managing photovoltaic plants [20]. The **20** Solar-Log devices found with Shodan are attached to a web server called *Solar-Log Web Enerst*, a portal for presentation and monitoring of functions of Solar-Log devices. Table II shows the models of Solar-Log products that were found, and their respective quantity.

TABLE II
IDENTIFIED SOLAR-LOG PRODUCTS

Product	Number of devices
Solar-Log 50	1
Solar-Log 250	2
Solar-Log 300	3
Solar-Log 1000	1
Solar-Log 1200	13

No specific vulnerability related to these devices was found, but since no authentication is required to get access to the monitoring interface, these devices signify a risk to their users. The web server shows a complete specification of the devices itself, but more worrisome, it discloses sensitive information about the network, the production (see figure 5), and other connected devices. Configurations can also be modified and information adulterated. Figure 6 shows a screenshot taken from one of the product's interfaces.

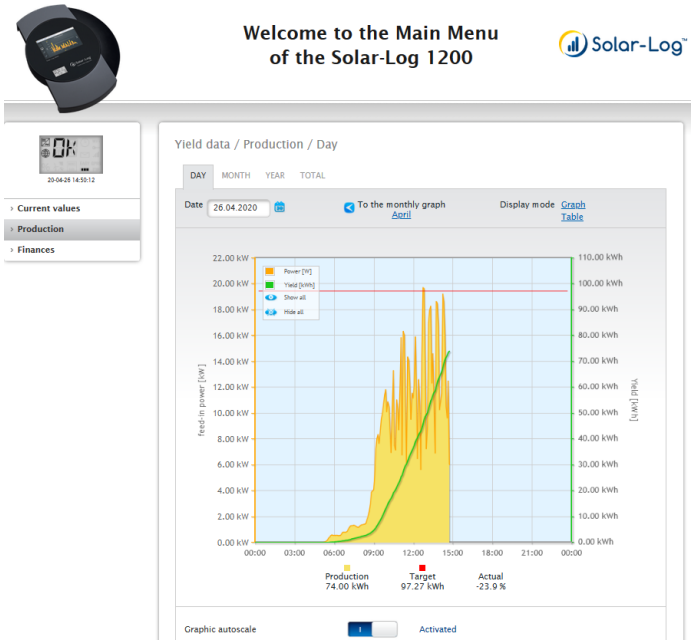

Fig. 5. Screenshot of Solar-Log 1200 web interface.

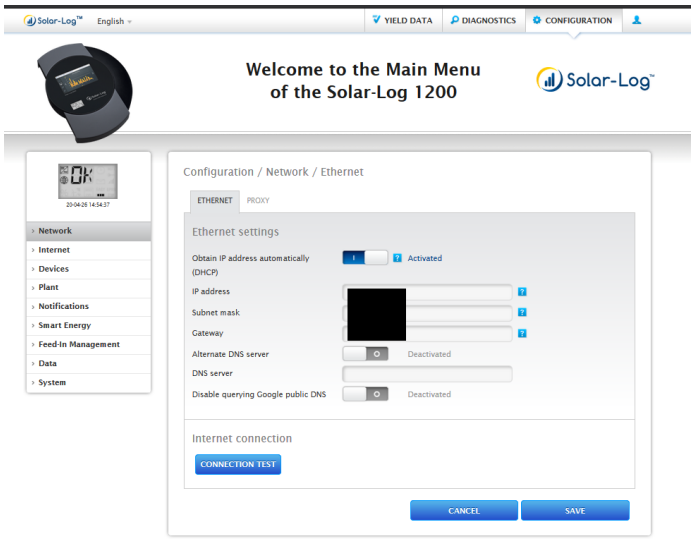

Fig. 6. Screenshot of Solar-Log 1200 web interface.

4) Schneider Electric: **12** Schneider Electric devices were found using Modbus. Table III contains the details about identified devices, their model, type and quantity.

These devices are not giving access to any web server, but some of them are though leading to some router's login panel. No information related to who could have been using the devices or where they are being used, was gathered. Nevertheless, vulnerabilities related to them have been found.

The products **TM221CE16R** (4 found), **TM221CE24R** (2 found) and **TM221CE24T** (1 found) belongs to the *Modicon controller 221* product range. A vulnerability has recently been published (14 April 2020) regarding, among others, all the

TABLE III
IDENTIFIED SCHNEIDER ELECTRIC PRODUCTS

Product	Type	Number of devices
TM221CE16R	PLC	4
TM221CE24R	PCL	2
TM241CE24R	PLC	1
TM221CE24T	PLC	1
SAS TSXETY4103	Ethernet TCP/IP module	2
HMIGTO4310	Touchscreen	1
BMX P342020	Processor (CPU) module	1

models of Modicon 221 (CVSS v3.0 Base Score 8.2) [8]. The same day, a vulnerability affecting *Modicon 241* (1 found) was published (CVSS v3.0 Base Score 5.4) [9]. The product **BMX P34 2020** (1 found) belongs the products Modicon M340 which also is related to a recently published vulnerability (CVSS v3.0 Base Score 7.5) [10] [11]. This vulnerability affects also the *Modicon Premium Automation platform*, which means that it also affects the other 2 identified devices of the product **SAS TSXETY4103**.

5) Abelko: 6 devices are showing the *slave data Abelko 0.0.2* through port 502. No specific Abelko product was found based on that information, but **2** of the 6 found are attached to port 80/443 leading to the web interface of a control and monitoring unit for ventilation, heating, cooling, water and lighting. The involved device is the *IMSE UltraBase 30*. No vulnerability related to this device has been found, but one interesting thing to add about these exposed devices is the access they are giving to routers login panel. Some of them are even disclosing the name of the company using them.

6) HMS Industrial Networks AB: **3** HMS devices could be identified using Modbus. One of them is attached to a web server called *EcoStruxure* belonging to *Schneider Electronic*. The *EcoStruxure* machine is being affected by one of the Schneider's vulnerabilities previously mentioned [8]. The other 2 HMS devices are attached to the *Anybus M-bus to Modbus TCP* web server interface. A web server related to a gateway used for decoding M-bus telegrams for overview and mapping of meter values. When accessing these interfaces, no authentication is required, configurations can be modified, and sensitive information can be gathered. Figure 7 shows a screenshot taken to one of interfaces.

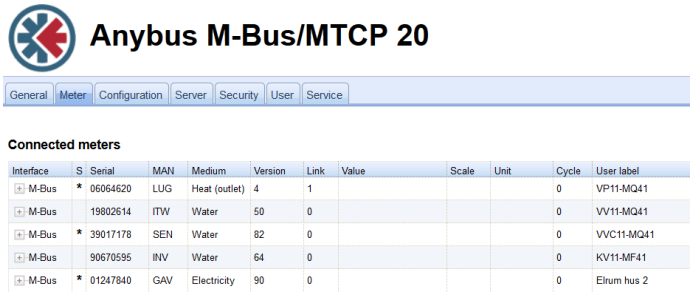

Fig. 7. Screenshot of one Anybus interface.

No published vulnerability related to the *Anybus* was found.

B. BACnet

366 devices can be found using BACnet; out of them, **127** have been identified with certainty. Figure 8 shows the number of devices and their respective manufacturer.

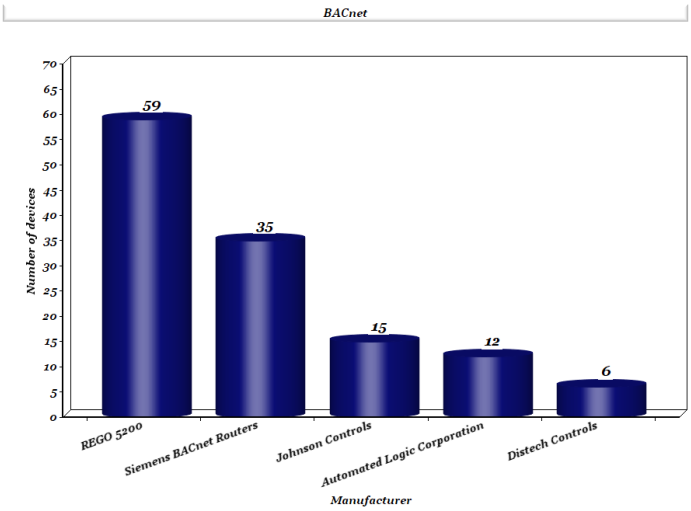

Fig. 8. Identified devices using BACnet.

1) REGO 5200: **59** devices under the object name *REGO 5200*, and vendor name *AB Regin*, have been found online in Sweden. Of those 59, 46 attached to a port leading to the web interface of the *Corrigo* controller previously described on section IV-A1. The *REGO 5200* is a central regulator with display used for control of heat pumps. No related vulnerability was found, indeed no many information about REGO 5200 seems to be available. Anyway, its manual can be found online.

2) Siemens: 47 Siemens products, using BACnet, can be found with Shodan. **35** of them have been identified with certainty. Table IV contains information about the product and number of findings.

TABLE IV
SIEMENS BACNET DEVICES

Product	Type	Number of devices
PXG3.L	Router	14
PXG3.W100	Router	4
PXC36-E.D	Automation station	4
PXC22-E.D	Automation station	4
PXC12-E.D	Automation station	1
PXM30.E	BACnet/IP Touch Panel	2
PXC100-E.D + PXA40-W0	Automation station + option module	4
INSIGHT	Building automation system	2

The automation stations **PXC100-E.D**, **PXC22-E.D** and **PXC36-E.D** could be vulnerable to a denial-of-service condition on their web servers (CVSS v3 5.3) [21]. Both **PXC22** and **PXC36** seem, at least, to be using a recommended version of firmware, but the found PCX100 is still using a vulnerable firmware. Besides the mentioned vulnerabilities, it is important to add that all found routers and the touch panels are giving access to their login panel while the automation stations are not attached to any web server, but some of them are leaking information about their position. Figure 9 shows how that

information is being shown, but the leaked location has been covered for security reasons.

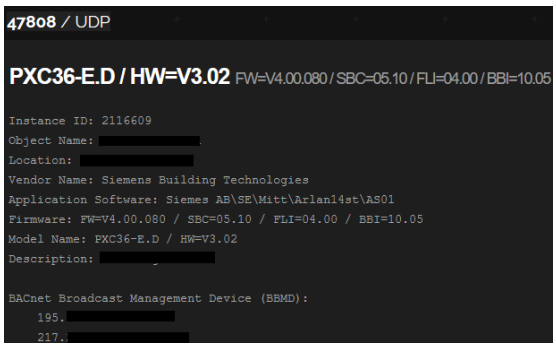

Fig. 9. BACnet banner of an Automation Station PXC36-E.D.

Another interesting thing to add about the Siemens BACnet findings is that all devices which are giving access to any king of web server, are using the server *Siemens Switzerland Ltd*. A quickly search for the server with Shodan, showed that 59 devices are using port 80 giving access to a login panel. The interesting thing about them is that many of them are leaking information of their exact location or the name of the company using them. Figure 10 shows a screenshot of one of those interfaces.

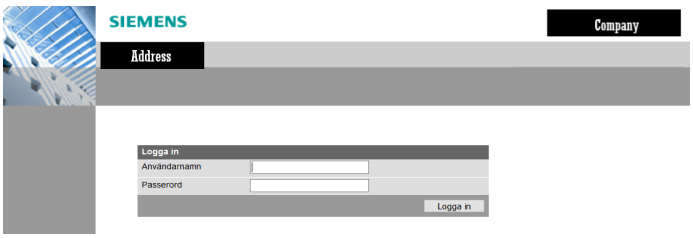

Fig. 10. Login panel where location and company's name are leaked.

3) Automated Logic Corporation: **12** devices under the name *Automated Logic Corporation* have been found using port 47808 in Sweden. 11 of them are different models of routers/gateway of the line *LGR* [12]. These devices are used within building automation systems. Table V shows the details.

TABLE V
LGR AUTOMATED LOGIC CORPORATION

LGR model	Number of devices
25	2
250	5
1000	4

The 12 th product is a controller *ME812-U* described as a controller capable of controlling multiple pieces of HVAC equipment simultaneously. No vulnerability affecting any of the mentioned LGRs have been found. No device is neither leading to any king of web interface.

4) Distech Controls: **6** devices under the vendor name *Distech Controls* have been identified using BACnet. All seem to be the controller *ECY-303*, used for HVAC applications. Only 1 of them is attached to the *ECLYPSE* web server where, according to the product's datasheet, the user could monitor and control the whole connection. Figure 11 shows the interface that can be reached.

Fig. 11. ECLYPSE login panel.

5) Johnson Controls: **15** devices have been found under the vendor name *Jhonson Controls* (JCI). 13 of them are different models of a *Network Control Engine* (NCE) used within building automation. Specifically, the NCE are used for integration of central plants and large built-up air handlers into existing networks *Metasys* networks [13]. Table VI contains the different models of NCE and the respective found quantity.

TABLE VI
NCE CONTROLLERS

MS-NCE model	Number of devices
2500-0	6
2510-0	2
2560-0	5

The other 2 JCI products found are a *Network Automation Engine* (NAE), which is a web-enabled, Ethernet-based, supervisory device used to monitor and control networks of field-level building automation devices, HVAC equipment, and lighting [14]. The model of NAE found online in Sweden is the *MS-NAE3510-1*.

According to the product's specifications, both NAE and NCE have a web user interface, but they can not be reached through Shodan. Nevertheless, both products could potentially be affected by several vulnerabilities. The NCE could be vulnerable to an attack where a successful exploitation could allow decryption of captured network traffic (CVSS v3 6.8) [15]. The NAE controllers could be vulnerable to Denial of Service attack(CVSS v2 Base Score: 6.4, Impact Score: 4.9, Exploitability Score: 10) [16] [17]. Based on the recommendations about updates of firmware to address these vulnerabilities, all the found devices seem to be running a vulnerable firmware version.

C. Omron Fins

240 devices could be found using port 9600 in Sweden. **20** of them have been identified as Omron Industrial products, either PLCs or CPUs. Table VII contains the details related to the findings.

TABLE VII
OMRON INDUSTRIAL PRODUCTS

Model	Type	Number of devices
CP1L-EL20DR-D	PLC	5
CP1L-EL30DR-D	PLC	1
CJ2M-CPU31	CPU	3
CJ2M-CPU32	CPU	2
CJ2M-CPU33	CPU	4
CJ2M-CPU34	CPU	2
CJ1M-CPU13	CPU	2
CJ2H-CPU65-EIP	CPU	1

Some of the listed devices are giving access to login panels, but only one of them leads to a specific web server. Nevertheless, the CJ series products could be vulnerable to uncontrolled resource consumption, whose exploitation can cause a denial-of-service condition (CVSS v3 7.5) [18]. The main recommendation as mitigation is to protect the devices with a firewall and block remote access to port 9600.

Other interesting thing to highlight here is the fact that two of those potentially vulnerable devices are attached to port 1732 where their exact position is being disclosed at their *hostname* field, as shown in figure 12. Both *CJ2M-CPU32* show the name of the business associated to them. Name that can be searched for and then it would not take more than a couple of minutes to get the address and even a satellite view, as shown in figure 13.

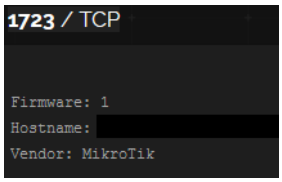

Fig. 12. Banner of a CJ2M-CPU32 device via port 1732.

Fig. 13. Devices exact location.

D. DNP3

As shown in table I, the *Distributed Network Protocol 3* (DNP3) has port 20000 as default port. According to Shodan, 348 IP addresses are using the service in Sweden, but among them, no ICS device has been identified. Neither the banner shown via port 20000 nor the other services the IP addresses are using, have got any relation to ICS devices. One of the possible answers to this, perhaps, particular situation is that the port 20000 is not exclusively used for DNP3 communications (where DNP3 is used for communication between a master station and RTUs or IEDs). Port 20000 is also being used for *Usermin* sevices (a web-based interface for, among other services, webmail, password changing and mail filters on a Unix system [23]) and *Voice over Internet Protocol* (VoIP). The study has indeed shown that many of the found IP addresses are attached to *Usermin* services or simply leading to websites. Other interesting thing to mention is about the organisations with most IP addresses. *Amazon*, with 46 Ip results, is the organisation with most results and 40 of them being used as cloud services. Amazon is followed by *Quantil Networks* (29 results), which offers customised content acceleration solutions for video stream, web site and big data files [24] and *GleSYS Internet Services AB* (27), which offers cloud VPS and dedicated servers [25]. The rest of the found IP addresses are, as mentioned, related to Usermin service, websites, servers, and 4 of them are leading to some routers login interface. A quite singular characteristic present in the majority of the found IP addresses is the big number of other services being used. That opens the possibility that many of those IP addresses have port 20000 open but are not necessarily using it, or at least, not for anything related to the DNP3 protocol. Since the name *DNP3* is officially assigned to the service used through port 20000, Shodan does not distinguish if the service is really being used as DNP3 protocol or something else. As mentioned, no ICS device was identified among the 348 results obtained with Shodan, but neither the exact number of IP addresses really using DNP3, or related to ICS, have been identified.

E. Other devices

In this section, the results obtained by implementing the second method mentioned on section III-B are described.

1) Lantronix: In 2017 it was published that several Lantronix devices, of the models *UDS1100-IAP* [26] and *xDirect* [27], could be leaking their Telnet passwords [29]. The first one is a external device server while the second one is a Serial-to-Ethernet device server; both used to connect older control hardware devices that have a serial output to Ethernet networks, and can be managed over Ethernet connection [28]. With Shodan, **48** devices can still be found leaking their Telnet passwords through port 30718, figure 14 shows the Lantronix banner and all the information that can be gathered there.

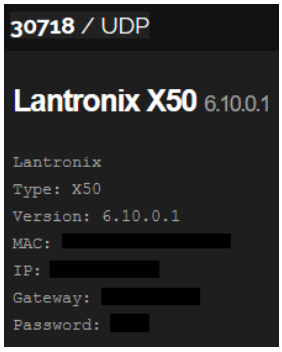

Fig. 14. Banner of a Lantronix device.

All the found devices are attached to their web interface where sensitive data can be gathered and malicious actions, as a part of an attack, can be performed. Figure 15 shows the mentioned interface.

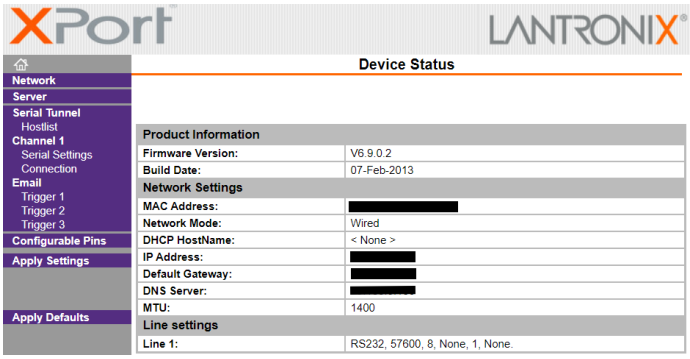

Fig. 15. XPort web interface

2) Siemens S7: There are well-known vulnerabilities that could be affecting the line/family of Siemens products *SIMATIC S7-1200* [31] [30] and *SIMATIC S7-300* [33]. Both CPUs that are being used in Sweden. Siemens S7 devices use port 102, services that, according to Shodan, it is being used by 62 devices in Sweden (see figure 1). Table VIII shows statistic about the S7 findings.

TABLE VIII
SIEMENS S7-300/1200S FAMILY

Model	Number of devices
S7-300	7
S7-1200	4

The found S7-1200 and some of the S7-300 seem to be running a firmware version older than the recommended as mitigation.

3) Ubiquiti: Ubiquiti manufactures wired and wireless networking products for enterprise and wireless broadband providers. Ubiquiti uses port 10001 (included by Shodan as a ICS port/service) as, among other variety of thing, *discovery service*. That is, a service to easily locating of Ubiquiti devices in a managed environment [35].

At least 444 Ubiquiti devices, using port 10001 in Sweden, can be found with Shodan; 423 of them have been identified. Table IX contains statistic about the identified Ubiquiti devices. Since a majority of the exposed devices are attached to a login panel, the table contains also the exact amount of devices giving that kind of access through port 80/443/8080.

TABLE IX
UBIQUITI DEVICES IN SWEDEN

Model	Type	Quantity	Login Panel
LAP	-	85	44
LAP-HP	-	84	55
ERPoe-5	Edge Router	41	36
ERLite-3	Edge Router	39	35
ER-X	Edge Router	37	30
LM2	Nano Station	29	28
UCK-G2	Cloud key	22	19
ER-X-SFP	Edge Router	14	13
LM5	Nano Station	11	9
N5N	Nano Station	10	9
pS5	Power Station	9	9
ERPro-8	Edge Router	8	8
P5B-400	Popwer Beam	6	2
NS2	Nano Station	4	3
ER-8	Edge Router	3	3
pS2	Power Station	2	0
PowerBeam 5AC	Power Beam	2	0
NB5	Nano Bridge	2	2
— ES-8	Edge Switch	2	2
ES-24	Edge Switch	3	2
ES-12F	Edge Switch	2	2
AGW-LR	Air Gateway	2	1
UVC G3	Video Camera	1	1
P5B-300	Power Beam	2	1
P2B-400	Power Beam	1	1
N5B-16	Nano Beam	1	1
ER-10X	Edge Router	1	1
EP-R6	Edge Router	1	1
AirCam	Camera	1	1

It has not been possible to identify with certainty neither the LAP nor the LAP-HP models, but all the performed researched led to the same type of networking products; AirRouter and AirRouter HP [36]

Last year, it was published that attackers had been using the discovery service to carry out DDos amplification attacks. It was estimated that around 485000 devices could have been affected [37] [38]. During the studies related to that vulnerability, researchers discovered that many devices had already been hacked. Today, in Sweden, 46 of those compromised devices can still be found with Shodan. Figure 16 shows a device's banner as example.

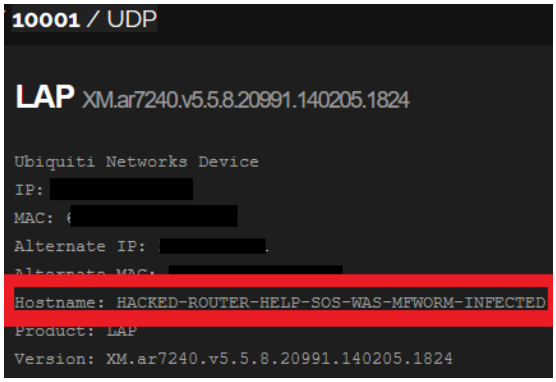

Fig. 16. Ubiquiti LAP device's banner

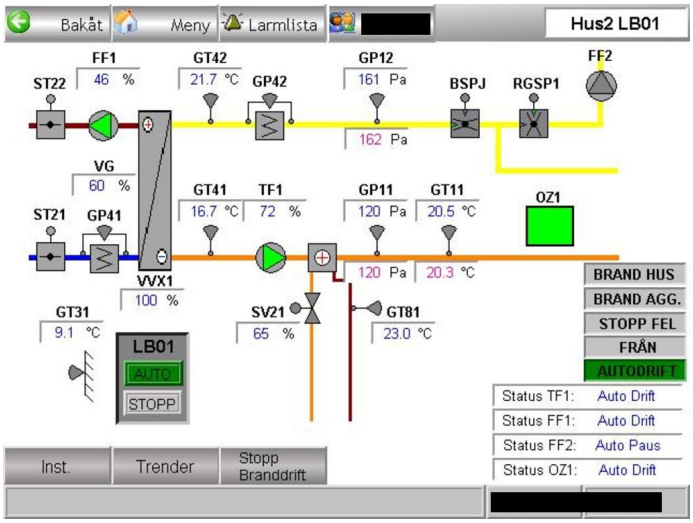

Fig. 17. Air Treatment System

It was stated that those devices were apparently not hacked but defaced as a form of warning the users about the risks of being exposed online [34]. Devices like the one shown in figure 16 could recently have been defaced as well as in 2016, nevertheless it is not possible to know if the user have noticed the attack, but anyway, they are still there being exposed disclosing information and giving access to their login panels. The use of the discovery service seems to be an extra risk some Ubiquiti users are taking, but not only that became interesting during this study but also the fact that 423 of 444 exposed devices found with Shodan, are giving access to their login panels.

4) Virtual Network Computing VNC: Something interesting related to VNC is the number of used VNCs being used with authentication process disabled. In order to find the ones exposed and unsecured being connected in Sweden, ports 5900, and 5901 were analysed; table X contains the details.

TABLE X
VNC AUTHENTICATION DISABLED

port	Total VNC Sweden	Authentication disabled
5900	2,964	1592
5901	285	21

The problem with the exposure of the VNC becomes more worrisome when even images of the no authenticated system can be obtained. Then, more sensitive information is disclosed and critical systems more exposed. Figure 17 shows as example an image of what seems to be an air treatment system.

9 IP addresses disclosing images of the system have been found during the study. For those addresses showing images, Shodan shows only one screenshot, but it is possible to use the Shodan Command Line and get the history of the IP address where more images can be retrieved.

5) Wind Farms:

- *Nordex: Nordex* [39] is one of many wind turbines manufacturer currently being used in Sweden. In 2015, a vulnerability affecting *Nordex Control 2 Wind Farm Portal*, the web interface attached to the Nordex turbines, was published. The portal was vulnerable to a cross-site scripting (XSS) attack because it failed to sanitize the user input during the authentication process [40]. A successful attack would not have had any impact to the confidentiality, integrity or availability of the system, but it was interesting to mention the vulnerability since 17 Nordex Web portal can today be found with Shodan. In fact, due to the information disclosure, it is possible to identify the wind farms where these turbines are operating. So, not only the Nordex web interface can be reached but also the wind farm behind can be identified with certainty. The study of these Nordex devices has showed that three wind farms can directly be identified by the Shodan's banner while the other ones have been identified using the program *OWASP ZAP* [41] (see figure 19. Figure 18 shows the Nordex portal and figure 20 shows an identified turbine shown with a satellite view.

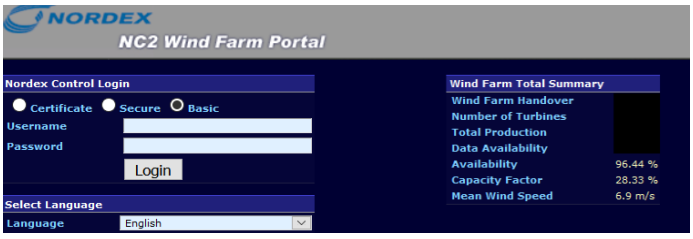

Fig. 18. Nordex Control Portal

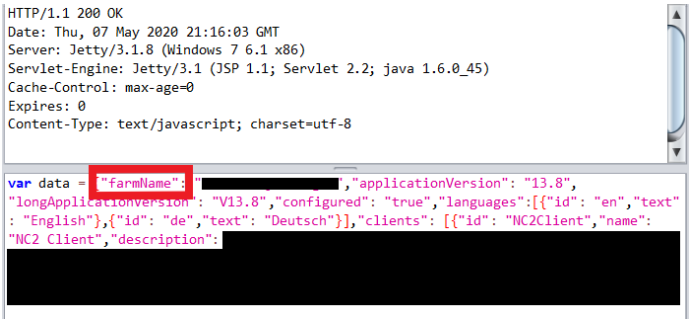

Fig. 19. Obtaining the name of the wind farm using OWASP ZAP

Fig. 20. A wind turbine identified in Sweden.

V. Related previous work

Results obtained during two previous researches, performed at Linköping University in 2018 [42] and 2019 [43], have been used to show here if the number of exposed devices, using the studied ports, in Sweden have decreased or increased through the years 2017-2020. The paper written in 2019, contains information about the number of devices that could be found with Shodan using ICS protocols during the years 2017 and 2019. Table XI contains the data taken from the paper and the one corresponding to year 2020 obtained during the present study.

TABLE XI
ICS devices exposed in Sweden

Date	Number of devices
April 2017	2965
February 2019	5539
Mars 2019	5311
April 2019	5726
June 2019	7292
May 2020	7505*

The data gathered last year involved the ICS devices found with Shodan, as well as the study presented here, but during that study, the devices using ports 10001 and 30718 were also considered. So, in order to get a more accurate comparison, the same Shodan filter was applied and the result was **7505**. That is why the number shown as data from May 2020 does not coincide with those 3745 devices reported at section IV. The Shodan filter used was *category:ics country:se*. In order to make a comparison worldwide, filter *category:ics* was applied; figure 21 shows the 10 countries exposing most devices. According to Shodan, when applying filter *category:ics* Sweden occupy the place 26 [th].

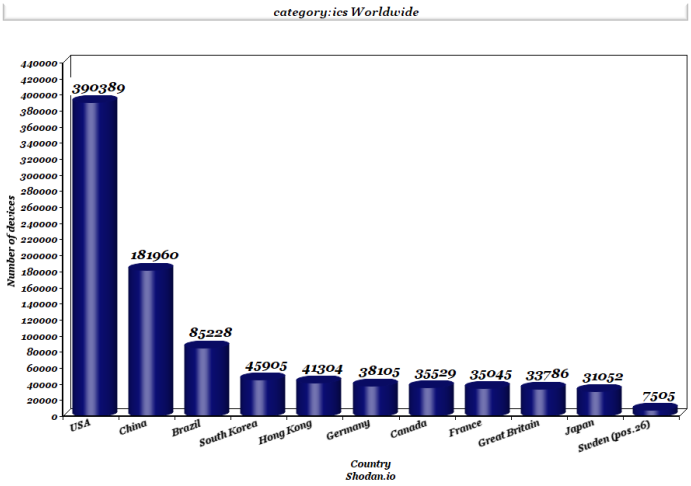

Fig. 21. category:ics worldwide.

The other paper that has been used to show a comparison is the one containing, among other information, data about the usage of ICS protocols in 2018 [42]. Table XII contains the information with the addition of this year's results.

TABLE XII
ICS Protocols Sweden

Protocol	Devices 2018	Devices 2020
Modbus	894	940
BACnet	140	366
Tridium Fox	120	305
Omron Fins	19	287
Melsec-Q	7	277
Siemens S7	30	62

VI. Conclusion

This study has shown that Internet-connected ICS devices can not only be found by number with Shodan but also be identified with certainty, which increases their exposure to malicious intentions. Knowing the name of a specific device, model, version and manufacturer, it is more than enough to find (on the internet) its user and installation manual, how and where it is usually used, and even what other kind of devices are often used together with it. The implemented methodology was simple and did not require any kind of previous knowledge neither about ICS protocols, devices, nor about the search engine Shodan, which lead us to the conclusion that *anyone* could easily reach and gather sensitive information about ICS devices.

The results show that many of the identified devices are disclosing sensitive information and even giving access to web interfaces and login panels where input validations could be bypassed. The results also show that many devices do not

even require authentication to monitor and control web servers where sensitive data can be gathered or even modified. It is though not possible to estimate the real impact an attack could have on these devices or the system behind them. Neither it is to know if the companies are implementing security layers, and what kind of them. Many devices are internet-connected intentionally as a need for the companies since they are used for remote control and monitoring reasons; so they are hopefully well protected and the companies prepared for possible attacks on the devices or the web servers. But it still is peculiar the big number of devices unnecessarily disclosing too much information when it is possible, and not even difficult, to hide from tools like Shodan without affecting functionalities [43].

The number of devices that can be found with Shodan continue to increase in Sweden, signal that seems to be in accordance with the fact that the world is becoming more and more industrialised and internet-connected. But a number of around 300 devices do not seem to be a considerable increase. That number not being bigger can be a signal that companies are indeed aware of the risks of being internet-reachable [44] [45], and that they are implementing security measures to protect critical systems.

The last thoughts of this conclusion have to be dedicated to the devices found based on well-known vulnerabilities potentially affecting ICS devices. It would be interesting to know why it is still possible to find, after three years, Lantronix devices leaking their Telnet passwords when it is known that, for example, the devices can be infected with malware via Telnet so bot devices can send malicious telnet packets searching for other potential targets [46]. It is inevitable to wonder if Solar-log users (of the presented devices) are aware of the information their devices are disclosing and the access their are giving to anyone. The Nordex devices may be protected to the old exploit bypassing the username input validation at the web interface, but do they need to be internet-reachable, show their specifications and even disclose the exact name and location of the wind farm behind them? And finally, it would be much better to be unable to find any Siemens S7 PLCs when they seem to be an *attractive* and recurrent target of attacks like ransomware [47].

1) Future Work: The performed study can be used as a start for a more deeper analysis of the ICS situation in Sweden. The following step could be to analyse in depth the rest of the protocols (as it was done with Modbus, BACnet, Omron and DNP3) in order to obtain a more complete statistic about the devices that can be identified with certainty. That more complete statistic about Sweden could then be used to decide if a more sophisticated analysis is required in order to identify the real risk of the internet-connected devices, and possibly illustrate the relation between the number of exposed devices and performed attacks (if the companies report them).

REFERENCES

[1] Shodan®, "Shodan is the world's first search engine for Internet-connected devices", https://www.shodan.io/explore/category/industrial-control-systems, 2013-2020.

[2] ICS, https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system,.

[3] ICS, https://whatis.techtarget.com/definition/industrial-control-system-ICS,.

[4] ICS, https://en.wikipedia.org/wiki/Industrial$_control_system$, .

[5] A. Hansson, M. Khodari, and A. Gurtov, "Exploring Shodan From the Perspective of Industrial Control Systems,", IEEE Access, vol. 8, p. 75359-75369, 2020,.

[6] Shodan, https://danielmiessler.com/study/shodan/,.

[7] Shodan, "What is Shodan? The search engine for everything on the internet", https://www.csoonline.com/article/3276660/what-is-shodan-the-search-engine-for-everything-on-the-internet.html,.

[8] , https://www.se.com/ww/en/download/document/SEVD-2020-105-01/,.

[9] , https://www.se.com/ww/en/download/document/SEVD-2020-105-02/,.

[10] , https://www.se.com/ww/en/download/document/SEVD-2019-316-02/,.

[11] . https://www.securityweek.com/industrial-controllers-still-vulnerable-stuxnet-style-attacks,.

[12] , https://www.automatedlogic.com/specsheets/lgr$_c s.pdf$, .

[13] , https://www.johnsoncontrols.com/building-automation-and-controls/building-management/building-automation-systems-bas,.

[14] , https://www.johnsoncontrols.com/building-automation-and-controls/building-management/building-automation-systems-bas/network-automation-engines,.

[15] , https://www.us-cert.gov/ics/advisories/icsa-19-227-01,.

[16] , https://www.johnsoncontrols.com/cyber-solutions/security-advisories,.

[17] , https://nvd.nist.gov/vuln/detail/CVE-2020-9044,.

[18] , https://www.us-cert.gov/ics/advisories/icsa-20-063-03,.

[19] , https://www.regincontrols.com/en-GB/product1/corrigo-ardo—controllers-for-ventilati/3279/30476/topcats,.

[20] , https://www.solar-log.com/en/products-components/,.

[21] , https://www.us-cert.gov/ics/advisories/icsa-19-318-03,.

[22] , https://www.elvaco.se/en/product/infrastructure1/cmex13s-m-bus-master-for-256-meters–1050052,.

[23] , http://www.webmin.com/usermin.html,.

[24] , https://www.quantil.com/,.

[25] , https://glesys.se/,.

[26] , https://www.lantronix.com/products/uds1100-iap/,.

[27] , https://www.lantronix.com/products/xdirect/,.

[28] , https://www.securitynow.com/mobile/author.asp?section$_i d$ = $649 doc_i d = 738705$, .

[29] , https://www.bleepingcomputer.com/news/security/thousands-of-serial-to-ethernet-devices-leak-telnet-passwords/,.

[30] , https://cert-portal.siemens.com/productcert/pdf/ssa-232418.pdf,.

[31] , https://new.siemens.com/global/en/products/automation/systems/industrial/plc/s7-1200.html

[32] , https://cert-portal.siemens.com/productcert/pdf/ssa-306710.pdf,.

[33] , https://mall.industry.siemens.com/mall/sv/se/Catalog/Product/6ES7314-1AG13-0AB0

[34] , https://www.bleepingcomputer.com/news/security/tens-of-thousands-of-defaced-mikrotik-and-ubiquiti-routers-available-online/

[35] , https://blog.rapid7.com/2019/02/01/ubiquiti-discovery-service-exposures/?

[36] , https://dl.ubnt.com/datasheets/airrouter/airRouter$_D atasheet.pdf$

[37] , https://securityaffairs.co/wordpress/80685/hacking/ubiquiti-vulnerable-devices.html

[38] , https://www.zdnet.com/article/over-485000-ubiquiti-devices-vulnerable-to-new-attack/comment-4323241658

[39] , https://www.nordex-online.com/en/

[40] , https://www.cvedetails.com/cve/CVE-2015-6477/

[41] , https://owasp.org/www-project-zap/

[42] A. Hansson, M. Khodari, and A. Gurtov, "Analyzing Internet-connected industrial equipment,", 2018 IEEE International Conference on Signals and Systems (ICSigSys), p. 29-35, May 2018.

[43] D. Hasselquist, A. Rawat and A. Gurtov, "Trends and Detection Avoidance of Internet-Connected Industrial Control Systems,", 2019 IEEE Access, vol. 7, p. 155504-155512, 2019.

[44] W. Schwab, M. Poujol, "The State of Industrial Cybersecurity 2018,", June 2018.

[45] Thomas Menze, "The State of Industrial Ccybersecurity,", July 2019.

[46] S. Abe, M. Fujimoto, S. Horata, Y. Uchida and T. Mitsunaga, "Security threats of Internet-reachable ICS,", 2016 55th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE), p. 750-755, 2016.

[47] J. Ibarra, U. Javed, A. Do, H. Jahankhani and A. Jamal, “Ransomware Impact to SCADA Systems and its Scope to Critical Infrastructure,”, 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), p. 1-12, 2019.