Trends and Detection Avoidance of Internet-Connected Industrial Control Systems

David Hasselquist
Department of Computer and Information Science
Linköping University
Linköping, Sweden
davha914@student.liu.se

Andreas Lundquist
Department of Computer and Information Science
Linköping University
Linköping, Sweden
andlu984@student.liu.se

***Abstract*—The search engine Shodan crawls the Internet for, among other things, Industrial Control Systems (ICS). ICS are devices used to operate and automate industrial processes. Due to the increasing popularity of the Internet, these devices are getting more and more connected to the Internet. These devices will, if not hidden, be shown on Shodan. This study uses Shodan, together with data found by other researches to plot the trends of these ICS devices. The studied trends focus on the country percentage distribution and the usage of ICS protocols. The results show that all studied countries, except the United States, have decreased their percentage of world total ICS devices. We suspect that this does not represent the real story, as companies are getting better at hiding their devices from online crawlers. Our results also show that the usage of old ICS protocols are increasing. One of the explanations is that industrial devices, running old communication protocols, are increasingly getting connected to the Internet.**

In addition to the trend study, we evaluate Shodan by studying the time it takes for Shodan to index one of our devices on several networks. We also study ways of avoiding detection by Shodan and show that, by using a method called port knocking, it is relatively easy for a device to hide from Shodan, but remain accessible for legitimate users.

***Index Terms*—Trends, Shodan, Avoidance, Industrial Control Systems, ICS, SCADA, Security, Internet of Things, IoT**

I. Introduction

Shodan is a search engine for devices connected to the Internet [1]. While a normal search engine, such as Google or Bing, indexes only content on the web, Shodan indexes all kind of devices such as Industrial Control Systems (ICS), web cameras and refrigerators. Shodan is publicly available, and can be used as a tool for detecting vulnerable devices, which in turn can be exploited if the user has malicious intent. In the same way, it can also be used by a system administrator as a helpful tool for improving network security.

Since devices found on the Internet can be reached from anywhere by anyone, the risk of attacks that exploits vulnerable devices increases. The consequences also differs depending on what kind of device is subjected to a successful attack. If an ICS device is the subject of a successful attack, the consequences could be critical. Many ICS devices run on outdated protocols that were never intended to be connected to the Internet, which makes them especially vulnerable [2]. Because ICS devices are both commonly vulnerable and could have critical consequences if subjected to successful attacks, this type of device is the focus of this paper.

This paper introduces the search engine Shodan, ICS and common protocols in use with these. The aim of this paper is to study the trends of the number of ICS devices and ICS protocols, both in Sweden and worldwide. This is done by comparing Shodan search results collected over time, together with results gathered by other studies using the same search queries. The following trends are in focus of our study:

- Number of ICS devices in Sweden
- Number of ICS devices worldwide
- Country percentage of ICS devices in the world
- Device usage of ICS protocols in Sweden
- Device usage of ICS protocols worldwide

After, the country percentage of ICS devices are compared to the GDP of the countries. We evaluate Shodan by studying the time Shodan takes to index different networks and lastly we show one way to avoid detection from the Shodan crawlers.

Section II covers the background theory of Shodan, port knocking and ICS. Section III covers the data collection and Shodan experiment setup together with a methodology evaluation. These results are later presented in Section IV and discussed in Section V. Lastly the conclusions and future work are presented in Section VI.

II. Background

This section contains the necessary background information about Shodan, port knocking and ICS that is needed for the scope of this paper.

A. Shodan

Shodan is a search engine that can be used to search for devices connected to the Internet [1]. These devices can be anything from a router to an ICS. Shodan also provides an option to apply a variety of filters to make searches more specific. These filters include country, port, product and category among others. An example of a search query is *port:502 country:"se" category:ics*, which will search for all ICS devices in Sweden using port number 502.

The way Shodan works is by having servers located all over the world that crawls the Internet for accessible devices

all hours around the clock [3]. The basic algorithm for the crawlers is:

1) Generate a random IPv4 address
2) Generate a random port to test from the list of ports that Shodan understands
3) Crawl the random IPv4 address on the random port and grab a banner
4) Repeat

The banner that the crawler grabs contains information in the form of text that describes a service on a device. Along with the banner, Shodan also collects information about the device's geographical location, hostname, operating system and more [3]. Those devices that are identified by the crawlers and the information gathered regarding them can be seen by using the Shodan API or the Shodan website [3, 4]. A search made with the API is more detailed and contains, among other things, the last detection time of each service independently. With the API, it is also possible to request a scan to be made, e.g. on a specific IP-address.

B. Port knocking

Port knocking is a method that can be used to access a server that has no open ports [5, 6]. It is a form of one way host-to-host communication where information is flowing to closed ports at the end device. The server uses a monitoring daemon to intercept the traffic on the closed ports and will silently process the data. There are variants of port knocking methods, using different data requirements and sequence on the data received. These requirements can be seen as a secret. If the requirements are fulfilled, the server will modify the firewall rules and allow the IP-address of the knocking user to connect to the server [5, 6]. Later, another knocking sequence can be used to close the port or the port knocking can be configured to automatically close after a certain amount of time has passed.

C. Industrial Control Systems

An Industrial Control System (ICS) is a general term for different types of control systems used to operate and/or automate industrial processes. An ICS often consists of combinations of control components that work together to achieve some sort of industrial objective. The most common type of ICS are *Supervisory Control and Data Acquisition* (SCADA) systems [7].

SCADA systems capabilities are focused on control at a supervisory level and the systems are composed of devices that are distributed in various locations. These devices are often programmable logic controllers (PLC). The main purpose of using SCADA is for control of field sites through a centralized control system and for monitoring. Example uses of SCADA can be monitoring a local environment for alarm conditions or performing local operations such as opening or closing of valves through field devices [8].

D. ICS Protocols

There are many ICS protocols using different methods and ports for communication with other interconnected devices [2]. Different protocols are used for different purposes. This section gives a brief overview of the common ICS protocols. There are many other popular ICS protocols, such as Ethernet/IP, OMRON FINS, Mitsubishi MELSEC-Q and Automated Tank Gauge, however these are outside the scope of this study. Table I shows an overview of the presented protocols and their ports used for communication.

TABLE I
ICS PROTOCOLS AND PORTS

Protocol	**Port**
Modbus	502
MQTT	1883
Niagara Fox	1911, 4911
BACnet	47808
DNP3	20000

1) Modbus: Modbus was created in 1979 and is used for serial communication with PLC devices [9]. It has become widely adopted as a defacto industrial standard in the ICS world. Since Modbus is very old and was invented before the Internet became widely used, it was not built with security in mind. This means that there is no built in encryption, integrity checks or authentication [9, 10]. There have been many attacks performed against this protocol. Huitsing et. al. [11] identified 59 attack instances and 20 distinct attacks performed. Furthermore, they identify over 100 attack instances performed on variations of the Modbus protocols. Some typical attacks that Modbus is susceptible to are man-in-the-middle, spoofing and replay attacks.

2) MQTT: Message Queuing Telemetry Transport (MQTT), is a lightweight communication protocol designed to be used by devices having low bandwidth and high latency on unreliable networks [12]. It was invented in 1999 and have since been widely adopted among the industry. MQTT uses a publish/subscribe architecture, meaning that ICS devices that implement this protocol can send and publish data to a specific server. Clients who have subscribed to this device can then be notified by the server when new data is available. In order to keep the protocol lightweight and simple, encryption is not built in and handled by the protocol itself. There is only an optional authentication by a user name and password, which is passed together with the MQTT packet [12].

3) Niagara Fox: Niagara Fox protocol is most commonly used in building automation systems such as offices, libraries and universities [2]. It is part of the Niagara framework from Tridium, and is also known as Tridium Fox. It is often used by Niagara AX systems for communication between the different stations and the central machine. Niagara Fox supports the use of SSL for secure communications between these devices. The security model of Niagara Fox resembles the classical mandatory access control and is based on the concept of Users, Permissions and Categories [13]. The protected objects

```
<html>
<header>
    <title>Shodan test</title>
</header>
<body>
    <h1>Hello World!</h1>
    <h2>Shodan test</h2>
</body>
</html>
```

Fig. 1. HTML Code of the test web page

are grouped into categories and users are given a set of permissions in each category.

4) BACnet: Building Automation and Control Networks (BACnet) is a communication protocol used for building automation and control networks. The development began in 1987 and has since then become protocol standard. BACnet is used to provide control automation in buildings, such as ventilation, fire detection system, heating and access control [2].

5) DNP3: The communication protocol DNP3 was developed in 1993 and is now an IEEE standard and a commonly used protocol for ICS devices. It is often used between automated devices and implemented in many critical infrastructure applications, such as the electricity sector [10, 14]. Similar to the Modbus protocol, it is designed to be reliable and does not enforce security such as encryption, integrity checks or authentication. In order to achieve security with this protocol, additional security specific hardware or security features in the application have to be added [10]. Compared to Modbus, DNP3 is more robust, efficient and interoperable than Modbus. However, this comes as a cost of higher complexity.

III. Methodology

This section covers how searching in Shodan was performed, the search queries used, the Shodan auto indexing and avoidance experiment and an evaluation of the methodology.

A. Search using Shodan

Searching with the Shodan search engine was performed by entering the search queries into the free text field of Shodan's web interface. The search queries that were used can be seen in Table II.

B. Shodan auto indexing

In order to evaluate Shodan, a study has been done to see which networks that are indexed, the time it takes for Shodan to index these networks and the requests that Shodan makes to these networks. Three devices have been used for this experiment: a Raspberry Pi, a 4G-router and a LAN-router. The 4G router was also able to downgrade itself and force the network to use either only 2G or 3G. Both routers were set to reply on ICMP echo requests (pings) and had port forwarding for port 80 set to the router's local IP-address of the Raspberry Pi. On the Raspberry Pi, a web server was running

TABLE II
Shodan search queries

Target results	Search query
ICS devices worldwide	category:ics
ICS devices country X	category:ics country:"X"
Modbus worldwide	port:502 category:ics
Modbus in Sweden	port:502 country:"se" category:ics
BACnet worldwide	port:47808 category:ics
BACnet in Sweden	port:47808 country:"se" category:ics
Niagara Fox worldwide	port:1911,4911 product:Niagara category:ics
Niagara Fox in Sweden	port:1911,4911 product:Niagara country:"se" category:ics
DNP3 worldwide	port:20000 category:ics
DNP3 in Sweden	port:20000 country:"se" category:ics
MQTT in Sweden	port:1883 country:"se"

Python SimpleHTTPServer containing only a simple HTML web page shown in Figure 1. Four different networks were used: 2G, 3G, 4G and a residence network using Bahnhof, a popular Internet Service Provider (ISP) in Sweden.

In order to host a public web server, a public IP is required. Bahnhof partly uses Carrier-grade NAT in their network, resulting in residence networks getting a private Wide Area Network (WAN) IP-address. We have noticed that this is a typical case in Sweden [15], most likely due to the IPv4 address exhaustion. After contacting the ISP, the residence network was given a public IP-address, making it possible to access the web server from the Internet. To detect when Shodan indexes the web server, Selenium was used to crawl the Shodan search results once every hour. The time of the indexing, as well as the requests being sent to the web server at that time, were recorded.

C. Shodan avoidance

In order to evaluate our results, we studied ways to avoid detection by the Shodan indexing. The simplest and most straight forward way was found to be port knocking. In addition to the SimpleHTTPServer web server running, SSH connection to the device using the default port of 22 was enabled. The avoidance setup was done by using Shodan on-demand scanning and the same hardware as the Shodan auto indexing, described in Section III-B. In our setup, the following three random ports were chosen as the opening knock sequence for the SSH port: 7336, 8710 and 8905. The user had to send packets with SYN flag set to these port in the correct sequence under a total of five seconds. If this was done, the server would grant this specific host IP SSH access over port 22. For this setup, the ports 22, 80, 7336, 8710 and 8905 were forwarded from the router to the device.

The Shodan API had to be used since the web interface does not show the last detection time for each service port independently. The methodology for the avoidance study consists of six on-demand scans. These scans, together with the web server and SSH status are shown in Table III. The web server was used to verify that Shodan had performed a scan on the IP-address and was therefore always active.

The first on-demand scan verified that Shodan detected both our web server and the SSH port. Later, before the second scan, the SSH port was turned off. This was done in order to verify that Shodan updates the latest detection time on the web server, however does not do this on the SSH port, meaning that it had not detected the SSH port. Before the third scan, the SSH port was turned on again, verifying that Shodan detects both the web server and SSH port again, updating their last detection time. Lastly, SSH was kept on, but is now protected by port knocking and only accessible to users knowing the knock secret. Scans 4-6 are to verify that Shodan have scanned our network, but only detected the web server.

TABLE III
SHODAN ON-DEMAND SCANS

Scan	Web server	SSH
1	Active	Active
2	Active	Inactive
3	Active	Active
4	Active	Active with port knocking
5	Active	Active with port knocking
6	Active	Active with port knocking

D. Evaluation of methodology

The service chosen for the Shodan auto indexing experiment was HTTP over port 80. However, Industrial Control Systems often use other services than HTTP to communicate and transfer data. This choice could be criticized as the detection time by Shodan could vary depending on which port and service being used. The experiment could be improved by using a real ICS device together with an ICS protocol, such as Modbus. If Shodan prioritizes some ports or services, this would most likely have an impact on the detection time.

In the case of Shodan auto indexing, Selenium was used to periodically crawl the Shodan web search results in order to see if Shodan had indexed our device. We used Selenium instead of other tools such as *curl* in order to simulate user interaction. However, if Shodan would record these interactions and queries and base their crawling algorithm on user searches, this could have an impact on our results. One alternative to using the web interface of Shodan is to use the Shodan API. However, using the API does not exclude the possibility that Shodan dynamically adjusts their crawling algorithm based on user queries.

In order to improve the reliability of our Shodan avoidance experiment, more searches and scans, especially on several networks using several devices, could have been made to better confirm the results that were collected. It would also have been interesting to find some other method for avoiding detection by the Shodan crawlers and comparing it to port knocking, both in terms of effectiveness and ease of use.

IV. RESULTS AND COLLECTED DATA

This section contains the results and trends that was collected from other studies combined with our data collection. ICS data from 2013 have been collected from a research project at Aalto University [16, 17]. ICS data from 2015 and 2016 have been collected from a recent study regarding an Internet-wide view of ICS devices [18]. ICS data from 2016 have been gathered from a study of ICS [19]. ICS data from 2017, 2018 and 2019 comes from our research department at Linköping University and the data from 2017 have also been used in a previous study [20]. GDP values have been collected from World Bank Group [21]. Lastly in this section, the results from the Shodan auto indexing and avoidance experiment is presented.

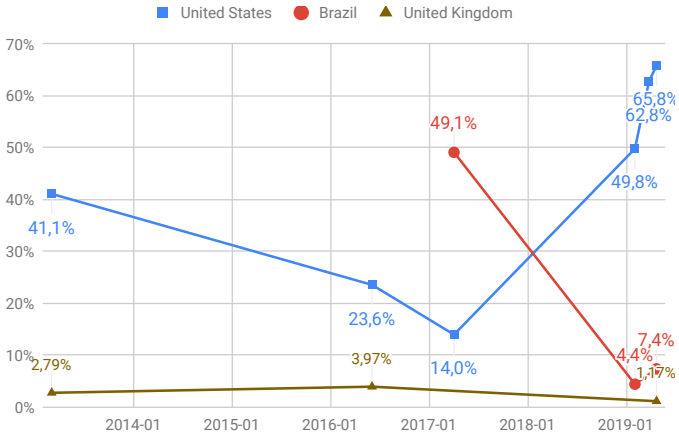

Fig. 2. United States and Brazil percentage of ICS devices worldwide

A. ICS Country Percentage Trends

This section covers the ICS country trends that can be seen from the searches performed with the Shodan search engine and the data from other studies. Figures 2, 3 and 4 shows, for the selected countries in the study, the country's percentage of the total ICS devices worldwide over the span of the years 2013 to 2019. An increase in the percentage of world ICS devices can be seen for the United States since 2013, however with a large decrease near 2017, while a decrease can be seen for the rest of the countries. The total number of ICS devices worldwide and in Sweden can be seen in Table IV. Here, it is shown that number of ICS devices worldwide have been quite stable the last few years, while in Sweden it have almost doubled. When looking at the last few months, some fluctuations can be observed. However, the increasing trend of ICS devices is clear. A comparison between the number of ICS devices for a country and that country's GDP is also interesting to explore, therefore the 2017 GDP for the study's selected countries can be seen in Figure 5, both in percentage of world total GDP and value in U.S. dollars. As seen in Figure 5 compared to figures 2, 3 and 4, the countries with the most ICS devices are generally the ones with the highest GDP. The country that significantly stands out from this is China. China has the second highest GDP value, with over 15% of total GDP worldwide. However, China only stands for a few percentage of the ICS devices.

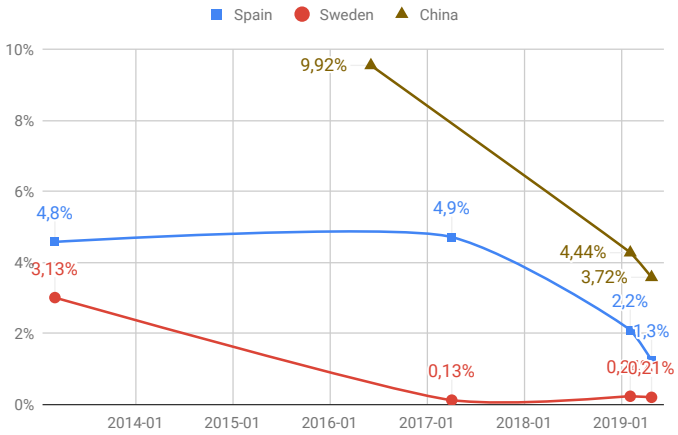

Fig. 3. Spain and Sweden percentage of ICS devices worldwide

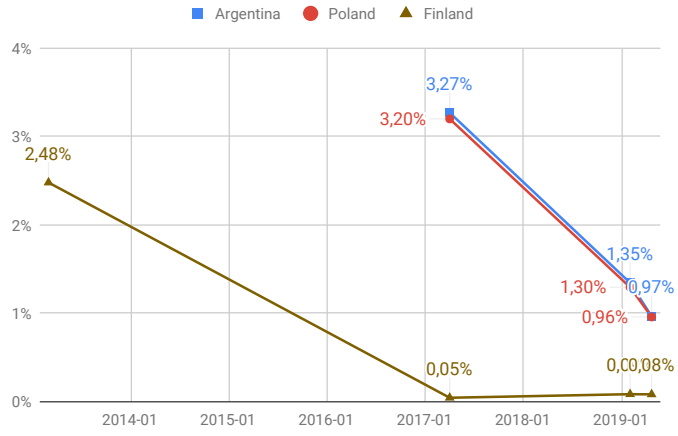

Fig. 4. Argentina, Poland and Finland percentage of ICS devices worldwide

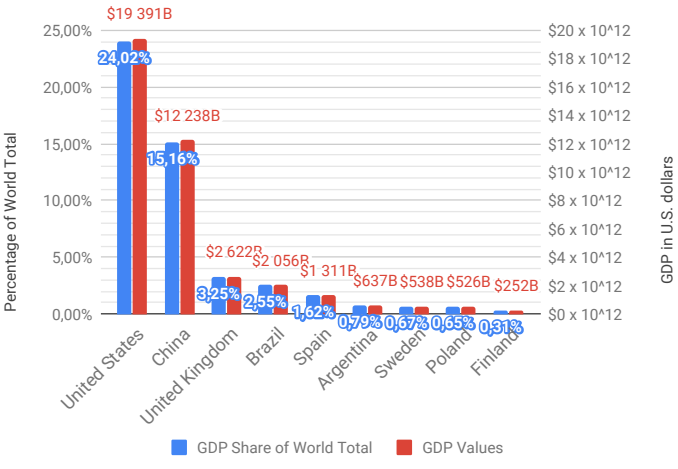

Fig. 5. 2017 GDP values for certain countries

TABLE IV
NUMBER OF ICS DEVICES

Date	Worldwide	Sweden
2017-04	2280652	2965
2019-02	2276259	5539
2019-03	2545414	5311
2019-04	2702311	5726

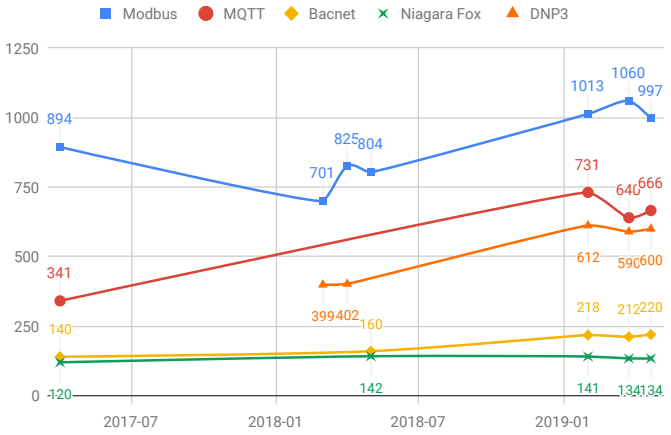

Fig. 6. Device usage of ICS protocols in Sweden

B. ICS Protocol Trends

Figure 6 shows how many devices in Sweden which used the protocols Modbus, MQTT, Bacnet, Niagara Fox and DNP3 over the span of the years 2017 to 2019. Usage of all these protocols have increased since 2017, especially MQTT which has almost doubled in usage. The number of ICS devices which uses the DNP3 protocol worldwide has significantly increased since 2018 and can be seen in Figure 7. Total number of ICS devices worldwide that used the protocols Modbus, BACnet and Niagara fox between the years 2016 and 2019 can be seen in Figure 8. All these protocols have seen an increase in usage as well, but not as significant as the DNP3 protocol.

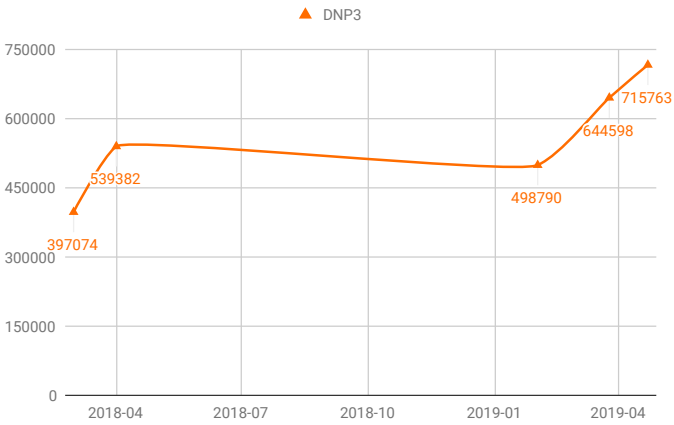

Fig. 7. Device usage of DNP3 protocol worldwide

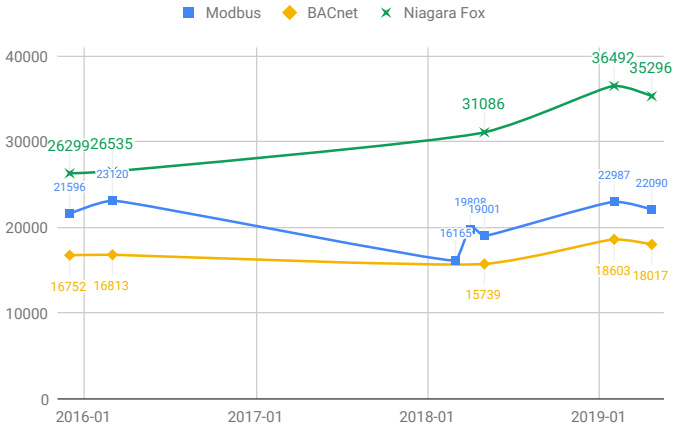

Fig. 8. Device usage of ICS protocols worldwide

C. Shodan auto indexing

The time taken for Shodan to index the web server on different networks is shown in Table V. At the time of the Shodan indexing, we also recorded the requests being made by the Shodan crawler. The IP-address of Shodan is shown in Table V and the HTTP requests are shown in Table VI. The HTTP requests are identical for both the 3G and 4G networks. For the 2G and the residence network, Shodan did not manage to index the device under 7 days.

TABLE V
SHODAN INDEXING

Network	Network IP	Shodan IP	Time
2G	80.170.92.xxx	-	$>$ 7 days
3G	176.68.52.xxx	89.248.167.131	6 hours
4G	5.241.58.xxx	89.248.172.16	23 hours
Residence	81.170.152.xxx	-	$>$ 7 days

TABLE VI
SHODAN HTTP REQUESTS IN ORDER

Shodan requests
1. GET / HTTP/1.1
2. GET /robots.txt HTTP/1.1
3. GET /sitemap.xml HTTP/1.1
4. GET /.well-known/security.txt HTTP/1.1
5. GET /favicon.ico HTTP/1.1

D. Shodan avoidance

As can be seen in Table III, six on-demand-scans were made. Every scan verified the expected behavior. The first scan detected both the web server and the SSH port. The second scan detected only the web server. The third scan detected, just like the first scan, both the server and the SSH port. Later, SSH was kept on but hidden with port knocking. The scans 4-6 showed that Shodan failed to index the SSH port, even with three attempts. This shows us that port knocking can be used as a way to avoid detection by Shodan.

V. ANALYSIS

This section analyzes the collected data and results regarding ICS trends, ICS protocols and Shodan auto indexing.

A. ICS Trends

As seen in the results, most countries have a lower percentage of the total ICS devices in the world in their latest data collection point compared to their first data collection point. The exception is the United Stated. The industry in all of these countries are still growing, especially in China and Brazil, which are rapidly increasing. More industry generally lead to more ICS devices, but the results gathered in this study do not show this. This could be explained by that the knowledge about limiting device exposure are increasing, and that companies using ICS devices are getting better at hiding them from Shodan and similar services. The exception of the United States could be explained either by that their industry is growing so fast that they can not keep up with hiding all the devices, or that they simply do not prioritize hiding their devices because they have implemented some other kind of security in them.

There are multiple ways of avoiding detection by Shodan, and in this study we have given an example of an easy way of doing so. If it is the case that companies are using this, or similar techniques for hiding from Shodan, the real number of ICS devices in the studied countries could very well be increasing, which indicates that the results gathered from Shodan could be misleading. That may further question Shodan's reliability and usefulness in such searches and cases. An alternative explanation to companies getting better at hiding their devices from Shodan is a country-wide blocking. However, according to Matherly [3], this is not the case since Shodan prevents this by placing their servers in different parts of the world.

China's GDP value stands out from the rest of the studied countries compared to the country's total number of ICS devices. The reason for this could be that China has a much larger population than any of the other countries, which might affect the result. It would have been interesting to compare the number of ICS devices of the countries with GDP per capita and see if China still would stand out from the rest of the countries. Another reason could be that companies in China is simply better at hiding their devices from Shodan compared to other countries.

With regards to the total number of ICS devices in the world, there has not been much of a change between 2017 and February 2019. We believe that this does not represent the real number. The industry has expanded in these years and so should the number of ICS devices. One explanation for this finding is that the number of ICS devices is actually increasing, but more devices are being hidden from detection. The results also show that from February 2019 to April 2019, a steady increase of around 400 000 devices, almost a 15 percent increase, has occurred. The reason for this could be that the number of active ICS devices depends on seasonal changes. For example, more devices could be activated and detected by

Shodan during the summer and then deactivated and not be detected by Shodan during the winter.

B. ICS Protocols

All studied protocols in Sweden and worldwide have increased in use since their respective first data collection point. Some of these protocols are old and the devices using them should most likely not be connected to the Internet based on security reasons. As explained in Section II-D, many of these protocols do not implement security features. The reason for the usage increase of these old protocols could be that old devices, which are using the protocols, are getting connected to the Internet without much thought of security as the Internet of Things (IoT) is growing. Another reason for the use of old protocols could be because they have proven themselves reliable and effective. Even if many protocols lack built in security, they can be used together with other security solutions to provide security.

C. Shodan auto indexing

The speed of crawling the Internet depends mainly on the network connection and the software implementation. Durumeric et. al. [22] introduce a network scanner called ZMap, specifically designed to perform Internet-wide scans and capable of scanning a port on the entire IPv4 address space under 45 minutes from a single machine, approaching the theoretical maximum speed of gigabit Ethernet. We believe therefore that it is reasonable that Shodan was able to index two of our devices under 24 hours. The question that arises is why the 2G and the residence network was unable to get indexed in under 7 days, despite having the same setup as the indexed networks. Perhaps this could be because Shodan recognizes it to be a honeypot and does not index the device. According to Shodan, honeypots are detected and still listed, but given a tag [3], so this does not seem reasonable. Bodenheim et. al. [4] performed a similar study, studying the time Shodan required to successfully identify their PLC devices and found that it took up to 19 days for Shodan to successfully index and identify their four devices. According to Shodan themselves, the entire Internet is being crawled once a month [23], which have led us to believe that in some cases, Shodan requires more than 7 days to index the device. This means that all of our devices would have most likely been indexed if they had stayed on for longer.

VI. Conclusions

The number of ICS devices connected to the Internet is growing slowly. Our results show that there has been a general increase of ICS devices since 2017, and for the United States the increase has been ongoing since 2014. We hypothesize that some countries are most likely hiding their ICS devices from search engines like Shodan, which could result in misleading statistics and also question the reliability of using Shodan for this type of research.

Many ICS devices connected to the Internet are still using old protocols, and the popularity of all protocols studied in this study has increased. This is likely due to the fact that old devices, that are running these protocols, are getting connected. As this study has shown in the experiment conducted regarding port knocking, there are simple and effective methods of blocking Shodan from detecting a device. If this, or similar methods, were to be used more, the usefulness of Shodan might decrease.

For future work, it would be interesting to continue with the ICS trends and see the future development over the coming years for number of ICS devices, both for specific countries and worldwide, as well as the protocols studied. This could give a better inclination to whether our theory about if Shodan still is a reliable device search engine is true or not. It would also be interesting to look at Shodan's historical data, provided by Shodan to users with Enterprice Data License, and compare those to the sources we have used in this study. With the historical data, a more thorough analysis could be made and a more clear trends might be seen.

Another interesting topic for future study is to find other ways of avoiding detection from Shodan and compare the effectiveness of these ways to the method presented in this paper. Also, in order to validate our results, it would also been beneficial to repeat our experiment several times, especially on a variety of networks using several devices, and see if the results differ.

Acknowledgement

We would like to thank the other researchers at Linköping University who have performed a similar study the last two years, without them we would not have had as much data. We would also like thank Andrei Gurtov and Abhimanyu Rawat at Linköping University for the feedback and material they have provided.

References

[1] Shodan. *Shodan*. URL: https://www.shodan.io/ (visited on 04/01/2019).

[2] Shodan. *Industrial Control Systems*. URL: https://www.shodan.io/explore/category/industrial-control-systems (visited on 04/10/2019).

[3] John Matherly. *Complete Guide to Shodan*. Leanpub, 2017.

[4] Roland Bodenheim et al. "Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices". In: *International Journal of Critical Infrastructure Protection* 7.2 (2014), pp. 114–123. ISSN: 1874-5482. DOI: 10.1016/j.ijcip.2014.03.001.

[5] Martin Krzywinski. "Port Knocking: Network Authentication Across Closed Ports". In: *SysAdmin Magazine* 12.6 (2003), pp. 12–17.

[6] Judd Vinet. *knockd - a port-knocking server*. URL: http://www.zeroflux.org/projects/knock (visited on 04/22/2019).

[7] Alejandro Bracho et al. “A simulation-based platform for assessing the impact of cyber-threats on smart manufacturing systems”. In: *Procedia Manufacturing* 26 (2018). 46th SME North American Manufacturing Research Conference, NAMRC 46, Texas, USA, pp. 1116–1127. ISSN: 2351-9789. DOI: 10.1016/j.promfg.2018.07.148.

[8] Keith Stouffer et al. *Guide to Industrial Control Systems (ICS) Security*. Tech. rep. National Institute of Standards & Technology, 2015. DOI: 10.6028/NIST.SP.800-82r2.

[9] Matheus K. Ferst et al. “Implementation of Secure Communication With Modbus and Transport Layer Security protocols”. In: *13th IEEE International Conference on Industry Applications*. 2018, pp. 155–162. DOI: 10.1109/INDUSCON.2018.8627306.

[10] INCIBE. *Protocols and network security in ICS infrastructures*. Tech. rep. Spanish National Cybersecurity Institute, 2015. URL: https://www.incibe.es/extfrontinteco/img/File/intecocert/ManualesGuias/incibe_protocol_net_security_ics.pdf.

[11] Peter Huitsing et al. “Attack taxonomies for the Modbus protocols”. In: *International Journal of Critical Infrastructure Protection* 1 (2008), pp. 37–44. ISSN: 1874-5482. DOI: 10.1016/j.ijcip.2008.08.003.

[12] MQTT. *Frequently Asked Questions*. URL: http://mqtt.org/faq (visited on 04/10/2019).

[13] Tridium. *Niagara Security Overview*. Tech. rep. Tridium, 2005. URL: https://www.vykon.com/library/whitepapers/Niagara_AX_Security_Overview.pdf.

[14] Irfan. A. Siddavatam and Faruk Kazi. “Security assessment framework for cyber physical systems: A case-study of DNP3 protocol”. In: *IEEE Bombay Section Symposium*. 2015, pp. 1–6. DOI: 10.1109/IBSS.2015.7456631.

[15] CyberInfo. *Fortfarande låg IPv6-utbredning i Sverige*. 2018. URL: https://www.cyberinfo.se/arkiv/fortfarande-lag-ipv6-utbredning-i-sverige/ (visited on 04/11/2019).

[16] Seppo Tiilikainen and Jukka Manner. *Suomen automaatioverkkojen haavoittuvuus*. Tech. rep. Aalto University, 2013. URL: https://research.comnet.aalto.fi/public/Aalto-Shodan-Raportti-julkinen.pdf.

[17] Seppo Tiilikainen. *Improving the National Cybersecurity by Finding Vulnerable Industrial Control Systems from the Internet*. Tech. rep. Aalto University: School of Electrical Engineering, 2014. URL: https://aaltodoc.aalto.fi/bitstream/handle/123456789/12918/master_Tiilikainen_Seppo_2014.pdf.

[18] Ariana Mirian et al. “An Internet-wide view of ICS devices”. In: *14th Annual Conference on Privacy, Security and Trust (PST)*. 2016, pp. 96–103. DOI: 10.1109/PST.2016.7906943.

[19] Brandon Wang et al. “Characterizing and Modeling Patching Practices of Industrial Control Systems”. In: *Proc. ACM Meas. Anal. Comput. Syst.* 1.1 (2017), 18:1–18:23. ISSN: 2476-1249. DOI: 10.1145/3084455.

[20] Adam Hansson, Mohammed Khodari, and Andrei Gurtov. “Analyzing Internet-connected industrial equipment”. In: *International Conference on Signals and Systems*. 2018, pp. 29–35. DOI: 10.1109/ICSIGSYS.2018.8372775.

[21] World Bank Group. *GDP (current US dollars)*. URL: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?end=2017&start=1960&view=chart (visited on 04/11/2019).

[22] Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. “ZMap: Fast Internet-wide Scanning and Its Security Applications”. In: *Proceedings of the 22nd USENIX Conference on Security*. 2013, pp. 605–620. ISBN: 978-1-931971-03-4.

[23] Shodan. *On-Demand Scanning*. 2018. URL: https://help.shodan.io/the-basics/on-demand-scanning (visited on 05/05/2019).