**IoT security in the Shodan age**

Internet of things (IoT) security is a growing concern for many. New ways to gather information about devices and networks evolve daily. Shodan is a search engine like google. However, while Google shows search results for things like videos, websites, and articles, Shodan will search for information on any device connected to the internet. Most devices are connected to the internet in the modern age, for example, Traffic lights, water pumps, webcams and so much more. Just about anything with power these days is connected in some way. Anyone can use Shodan and find information on these devices. Making it easy to search for information about subnets, domains, and open ports. Shodan and similar engines can be used for both malicious and non-malicious purposes.

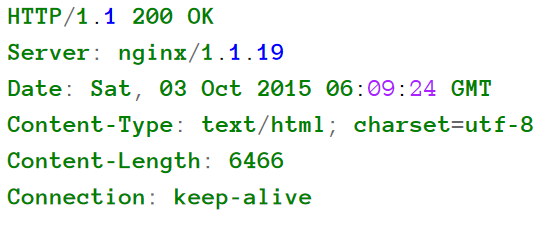


Image 1

Typical HTTP banner

(Complete guide to Shodan, Matherly, 2017, page 1)

Shodan allows the user to see a device’s banner. This device information is about the device. As seen in image 1, taken from a book made by the creator of Shodan, John Matherly, shows a typical Http banner. Banners vary greatly with each device. Shodan also gathers data such as operating system, location, and hostname. This information is completely free for the user, however, Shodan offers paid packages allowing users to do more such as setting up alerts and automatic scanning. Shodan also allows users to use filters to search for connected devices with specific vulnerabilities.

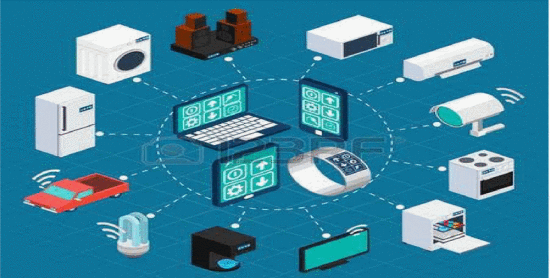
CNN headlined Shodan as “The scariest search engine on the internet” (Goldman, 2013). Allowing anyone to search for any device connected to the internet is a very scary thought. Anyone looking to attack and gain access to these devices will be able to identify vulnerabilities in these devices. However, it also allows user to search for their own vulnerabilities and protect them. Shodan is the most popular but not the only tool which makes this information available.

There is a wide range of devices that connect to the internet these days. From toasters to jets to space stations. The IoT security challenges faced are everchanging. Unfortunately, there is not a one size fits all and as security increases so do the skill of the people looking to attack. In the report form \*6 they state, “DDoS attacks increased in frequency and size where the number of DDoS attacks in 2016 is the double size of attacks in 2015 and the average attack size increased to 931 Mbps in 2016 with prediction to reach to 1.2 Gbps by the end of 2017.” (Al-Alami, 2017).

The potential harm from IoT attacks has made the subject of protection a priority for many. Shodan has now brought a lot of awareness to IoT security. An underground study so was conducted by M. Bada and I. Pete, searching the forum to gather information about how IoT attacks are discussed. Hackers often use these forums to discuss or learn information about methods of gaining access to information. The majority of these posts were found to be people talking about gaining access to CCTV cameras and webcams with Shodan and other tools. Many of these posts were ads for tools like Shodan.

The research by M. Bada and I. Pete, also goes on to speak about the human factor in IoT security which is important to understand. IoT attacks are only made possible by blind spots in people’s knowledge. These reference discussions on manipulating people or taking advantage of their skills or lack thereof. While Shodan does not directly help you access devices and can help you gain personal information such as usernames, passwords, identification of a person and medical records. With this information, attackers could get in contact with someone and manipulate them into giving them access to their devices or anything else. Every day people are scammed by people pretending to work for major companies like Telstra and using information gathered from their devices to convince people they need an update that gives the attackers access to their computers. Recently customers of the Lloyds bank were being targeted for this type of scam. An article from the Birmingham mail \*5 states that scammers ask users to log in to a fake online bank where their details are recorded and used by the scammer to access the customer’s real bank account. This would not be possible without the lack of knowledge or skill by the user to assess and protect themselves against the potential risk.

On October 12, 2016, a denial of service (DDoS) attack was launched which shut down almost half of the internet in America. This was named the Mirai botnet attack. Created by Paras Jha to boost his Minecraft server popularity by shutting down his competitor’s game servers. A botnet is what is made possible by the information gathered on Shodan. A computer is any electronic device used for storing and processing data. Hackers using Shodan search for open devices. Once they can identify unprotected devices by attempting common passwords such as ‘Password1’. Then use this in a network to create a Botnet. Finding and gaining access to even the smallest computer, such as a toaster that connects to the internet, on a large enough scale can allow someone to use them in a malicious attack. Using all the computers to send data to a network once, if large enough, can cause it to shut down. Paras Jha released his code to the public, and shortly after, someone used a similar botnet to attack Microsoft. in the words of an FBI agent who investigated the attacks, "These kids are super smart, but they didn’t do anything high-level—they just had a good idea" (Fruhlinger, 2018).



Figure

Some of the components of IoT system.

# (Vulnerability scanning of IoT devices in Jordan using Shodan, IEEE, 2017, Section I)

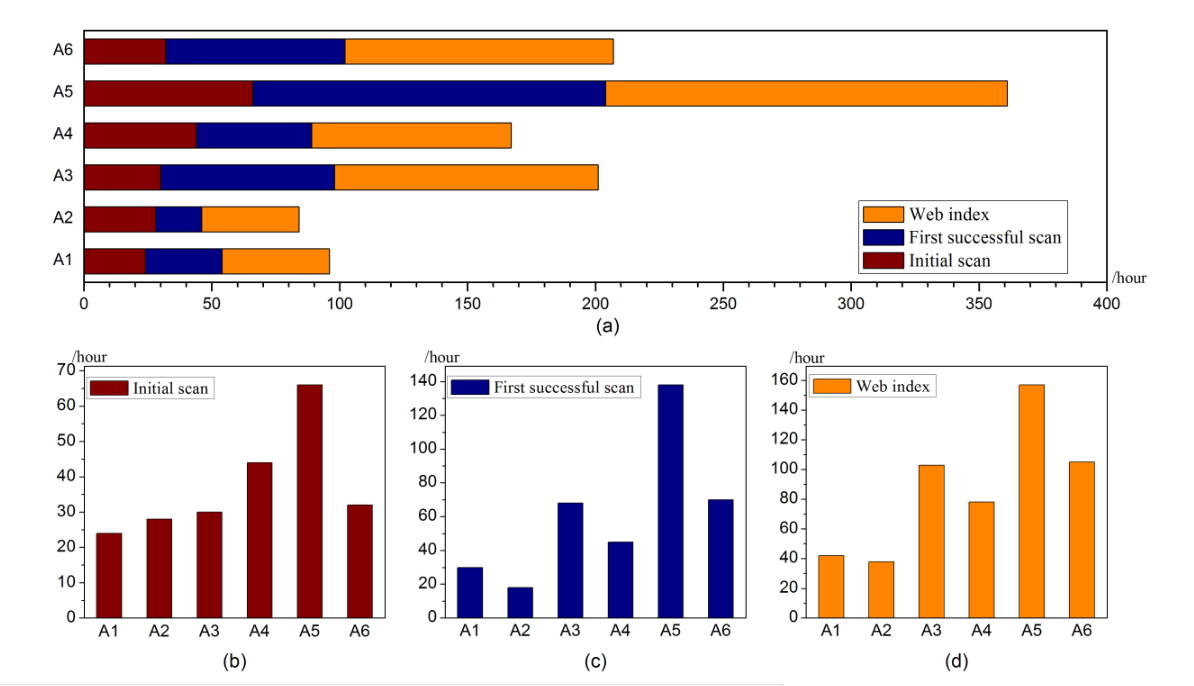
Home security challenges are a problem that many researchers are looking into. The home router connects all the devices in your home. An example of a home network is represented in figure 2 (Al-Alami, 2017). If an attacker can gain access to the router, they will have control of all connected devices. Manufacturers on these routers often set this as open by default, making setup easier for their consumers. When we consider the human factor, many users have not set up any security on these devices, often leaving logins as the default. This makes them very easy to gain control of. After that, it’s “open-season” on almost any connected device with most of them having no security of their own and relying on the router. Using Shodan to search for these devices and products is possible, along with searching for specific vulnerabilities. Unfortunately for now it is up to the user to protect themselves from these attacks.

Systems of systems (SoS) is a way to handle complex task by collaborating with a group of independent systems to complete an objective. IoT is how these systems operate and communicate. With all systems linked in a home or workspace having weak cyber security on even one device can allow attacks on the entire system. To ensure the safety of these sos’s each device must be protected. Vulnerabilities of these can include hardware, being a manufacturing fault, software design, a fault in the code, or user error, out-of-date software patches. A common target for malicious interference on smart devices is ones with low security such as refrigerators. These attacks try to interfere and change the behaviour of these devices to open the SoS and collect data. The defence of the systems has been researched by \*8 and is discussed:

“To avoid these types of security issues, we propose an approach for monitoring the behaviour of smart home devices and timely detect potential vulnerabilities. The proposed approach is based on defensive programming combined with the adoption of open-source intelligence tools on the interconnected devices through the use of Shodan APIs” (Rossi, 2020).

Being able to detect a third party accessing a device is only a warning system and the first line of defence. It will still be up to the owners of these systems to fill the gaps in their security. Resource Constraints on devices also play a role. With devices only having limited battery and storage. This directly limits the amount of security. Using cryptographic algorithms to protect the data stored on any given device takes up power and storage. With unlimited battery and storage all devices would have massive amounts of complicated security algorithms. The only perfect security against IoT attacks is to disconnect the device. In the case of a refrigerator is an option, while companies and power grids may not have that option in the modern world.

Roughly 10 billion devices are connected to the internet. That is more connected devices than people on earth. Shodan is a completely legal reconnaissance tool to find those devices. Research done by Yongle Chen and his team went and conducted a study setting up 6 devices and monitoring the activity from Shodan scans. They were able to track over 32, 522 interaction with 6 fake devices over a 3-month session. That is over an average of 60 interactions per day per device. As seen is figure 1, They were also able to determine that on average the engine can search all devices connect to the internet every 66 hours. They were also able to identify that roughly a third of these scans were from “Shodan-like scanners”. The majority of the other scans were done Censys. This shows that while Shodan is a powerful engine there are other tools for getting the same information.



Figure

Shodan scanning time.

(Exploring Shodan from the perspective of industrial control systems, Chen, 2020, page 75364)

Shodan is not new in IoT security. First released in 2009 it has only recently come into the news headlines. With cybercrime becoming more common and more devastating many people think of Shodan as a search engine for attackers. The Air force institute of technology in Ohio said:

“In fiscal 2012, Industrial Control System Cyber Emergency Response Team (ICS-CERT) responded to 198 cyber incidents involving critical infrastructure systems, a 65% increase over the 120 attacks reported in 2011. In addition, recent research identified thousands of ICS associated devices readily accessible via the Internet” (Bodenheim, 2014).

For people who take no notice of their own IoT security, they are right to be afraid of Shodan. Hopefully, with more publicity behind cyber crimes, more people will have a look at their own security and make better decisions on what devices they connect to the SoS and how protected they are. For professionals fighting cybercrime Shodan has given them a tool they can use to find their own vulnerabilities and help in creating a more protected SoS. Shodan in the modern age is not going anywhere. More and more engines like Shodan pop up every day. It is up to the individual if they wish to use it for malicious or non-malicious purposes. Every day the arms race continues to grow between attacks and cyber security, and this leads to a bigger gap in knowledge for people not educated in the subject. Everyone who has a device connected to the IoT has a responsibility to defend against malicious attacks.

# References

Al-Alami, H., 2017. *Vulnerability scanning of IoT devices in Jordan using Shodan,* Jordan: IEEE.

Bodenheim, R. C., 2014. *IMPACT OF THE SHODAN COMPUTER SEARCH ENGINE ONINTERNET-FACING INDUSTRIAL CONTROL SYSTEM DEVICES,* Ohio: U.S. Government.

Chen, Y., 2020. *Exploring Shodan From the Perspective ofIndustrial Control Systems,* China: IEEE.

Fruhlinger, J., 2018. *The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet.* [Online]   
Available at: https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

Genge, B. a. E. C., 2016. ShoVAT. *Shodan‐based vulnerability assessment tool for Internet‐facing services. Security Comm. Networks,* Volume 9, p. 2696– 2714.

Goldman, D., 2013. *The Cybercrime Economy.* [Online]   
Available at: https://www.csoonline.com/article/3276660/what-is-shodan-the-search-engine-for-everything-on-the-internet.html

Matherly, J., 2017. *Complete Guide to Shodan.* s.l.:Leanpub.

Pete, M. B. a. I., 2020. *An exploration of the cybercrime ecosystem around Shodan,* Paris: IOTSMS.

Porup, J., 2019. *Feature.* [Online]   
Available at: https://www.csoonline.com/article/3276660/what-is-shodan-the-search-engine-for-everything-on-the-internet.html  
[Accessed 22 04 2021].

Rodger, S. F. a. J., 2021. *Lloyds Bank customers urgently warned scam could empty their bank account in seconds.* [Online]   
Available at: https://www.birminghammail.co.uk/news/midlands-news/lloyds-bank-customers-urgently-warned-20285156  
[Accessed 22 04 2021].

Rossi, M. T., 2020. *Defensive Programming for Smart Home Cybersecurity,* Genoa: IEEE.