



Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/15795

DOI URL: <http://dx.doi.org/10.21474/IJAR01/15795>



RESEARCH ARTICLE

STUDY OF VULNERABILITIES IN IOT ENVIRONMENTS USING SHODAN AND CENSYS TOOLS

Lucas Correa Gonçalves, Jaqueline Silva De Souza Pinheiro and Jean Mark Lobo De Oliveira

Manuscript Info

Manuscript History

Received: 30 September 2022

Final Accepted: 31 October 2022

Published: November 2022

Key words:-

Vulnerabilities, Internet of Things, Security

Abstract

The present study on the vulnerabilities that concern The Internet of Things technology was carried out in order to identify which flaws are present in ubiquitous computing devices in the national scenario, attaching evidence that was found when using the search engines Shodan and Censys, which act on the web in order to find security flaws that are evident. After verification, a document was developed in the form web format, with the evidence found, using questions that instigate the interviewee about the knowledge he has about the failures found, whether he has any practice to protect his devices that are connected to the network and if it occurred to have experienced some experience of data theft or invasion of their devices. Thus, with quantitative data collected in both surveys, we can have a survey of how the deficiency of the security practice affects the defense of devices that are part of the Internet of Things.

Copy Right, IJAR, 2022,. All rights reserved.

Introduction:-

Current technology develops to adapt to personal needs in order to create a synergy between individual and machine. Formerly in the rise of the digital age, the world was admiring the arrival of bytes, zeros and one, software and hardware. Not long after, came the means of connection between people and information, the internet. Today the ease of communication, speed and storage have changed life as a whole, we had to evolve from digital to cloud, from physical to connection for everyone, all everywhere.

This connection, despite barriers, overcomes any obstacles in order to facilitate personal life. According to Magrani (2018, p. 20) "In general, it can be understood as an environment of physical objects interconnected with the Internet through small, embedded sensors." In this way we have a description of how the devices interact, continuing Magrani (2018, p.20)".. creating a ubiquitous computing ecosystem, focused on facilitating people's daily lives, introducing functional solutions in everyday processes." Finally, the whole of this technology is based on the IoT (Internet of Things) set that has been shaping the 21st century. Internet of Things or IoT is all that is incorporated into sensors in order to exchange information with other devices over the internet.

It is essential to develop on the theme Internet of Things, its benefits and how it is being used in everyday life, as well as, we should care about the security of the devices and connections that are integrated in this environment, therefore, there are tools with the design of investigating and attest to the quality of these connections.

In the technological environment there are several cases of attempts to steal information, particularly in devices that are connected to the Internet. Therefore, "these numerous connected devices that will routinely accompany us will collect, transmit, store, and share a huge amount of data, many of them strictly private and even intimate."

(MAGRANI, 2018, p. 24). In order to exploit connectivity, we will use tools to identify vulnerabilities in the connection of these IoT devices, using the Shodan and Censys search engines that are able to scan vulnerabilities in various devices that are connected to the network worldwide. According to Costa (2018, p. 27). "The Shodan search engine is dedicated to indexing thousands of IoT devices with open doors to the internet. Through this search engine you can find thousands of web applications." These vulnerabilities can be exploited by people with malicious intent.

This article aims to use the tools mentioned that scan the global network to find vulnerabilities in Internet of Things related devices, then, using a form, to collect information about the knowledge about network security that a group of people contains and about the flaws we encounter, as well as, protection measures and whether they have ever suffered some kind of data theft or intrusion into their devices in order to stimulate the practice of security on devices on the network and prevent possible unwanted access from occurring, protecting your data, devices and family members.

Theoretical Reference

As a theoretical basis, the following topics served as inspiration for the recognition of the problem found in IoT devices, as well as their popularity brought visibility and also the importance of maintaining user security with these new technologies.

1. IoT in the world
2. IoT Security
3. Vulnerability search tools
4. User Security

IOT In The World

The IoT came with an object connecting devices to each other over wireless networks such as wifi or bluetooth. With the growth of this sphere, new devices such as artificial intelligence and machine learning have come to integrate and reduce activities that were previously done repeatedly by humans and are now routines performed by software and machines. Automating tasks, creating routines to activate or disable electrical circuits, analyzing environmental data, constantly learning, with each step that of this technology the most automated future becomes present. According to SYDLE (2022) "According to a report by Statista, there are more than 35.8 billion connected IoT devices in the world by 2021 and this number could more than double to 75.4 billion by 2025." The world followed a pace of scale with the emergence of this new technology, SYDLE (2022) continuous, "This clearly indicates that, more than a trend, the Internet of Things is a rule for the daily routine of billions of human beings."

IOT Security

The basis of IoT is to use sensors and capture data from the environment and transmit to a receiver, as well as perform tasks automatically. Therefore, these devices become targets of attacks because they are usually connected to an internet network. These networks can be compromised thus generating a gateway so that malicious people can hack into and connect to any device. Of course, IoT works for multiple audiences, whether it's that person who is implementing routines to automate tasks in their home environment, or for industries that use sensors with artificial intelligence on a production line. According to Lourenço (2021) "A Kaspersky survey revealed the panorama of hacker attacks on Internet of Things ecosystems around the world and pointed out that the number has nearly doubled." These data obtained in September 2021 total 1.5 billion intrusions into smart devices during the first half of the year. Lourenço (2021) continues, "The figure already corresponds to twice that of all cases of invasions of smart homes and other devices in 2020."

According to Lourenço (2021) "Brazil is the deputy leader of these occurrences in Latin America, ahead of Argentina (5.6 million) and the Dominican Republic (1.2 million)."

Vulnerability Search Tools

With the considerable need for network connection, IoT devices carry a list of security concerns. From devices that no longer have support for the model, old or factory default configuration and even those that already bring recurring defects from the production line. There are people who considered security researchers are constantly looking for vulnerabilities that these threats have. In order to raise awareness and demonstrate to the manufacturer the flaws found. Even, there are tools on the web that can scour the network in order to find possible security flaws in various IoT objects. One of these tools is Shodan, a search engine that tracks various devices that are part of the internet of things and indexes them for easy search.

With this information we can find several devices in public network, offices and residences. According to Borges (2020), research on shodan has the applicability of:

Security search: Several IoT devices have their firmware versions listed directly on the login page. This means that researchers can find devices running specific versions of firmware with known vulnerabilities and possibly contact ISPs to inform them of such existing vulnerabilities on their networks. Sales/marketing research: IoT devices also display their brands and model numbers directly on login pages and HTTP headers, which opens up sales and marketing search topics. Consumer research: IT managers, Red and Blue Teams teams, and general SOC teams in enterprises can look for devices they're about to buy to determine if these devices have any known security issues (for example, new large-scale campus security camera deployments). Users can observe their own IP addresses to see if any devices in their home are also listed on Shodan. This works as a security tool for finding home devices that do not need to be in the public Internet space.

With a larger search area, Censys has a more comprehensive search engine with a deeper range to monitor multiple assets on the network. Its purpose resembles the Shodan, are tools that assist developers, researchers, security enthusiasts to detect possible flaws in their security.

Each failure puts at risk not only these devices, but also people, who in today's world have their lives integrated into the internet, such as: personal data, photos and videos, confidential documents, bank accounts. Almenara (2022) states that:

More than 5 billion people use the internet, a survey by consulting firm DataReportal pointed out. This impressive brand highlights that about 63% of the world's population is somehow connected to the world's computer network.

It is for this reason that it is necessary to highlight the security flaws that occur with the devices that are most present in our daily lives, such as IoT, in order to create a security awareness to minimize the risks of unauthorized access.

User Security

By performing a security practice, which means reevaluating the settings of each device, the user creates barriers that prevent the invasion of their data and the protection of their personal life, as well as that of their family members.

Today each person's life is connected, their bank accounts have become digital, documents, photos and videos are in the cloud, including personal data or even the history that each accesses on the internet. Many of these connections are stored in smartphones, smartwatches, virtual hosting services, in order to facilitate the life of each, this data is accessed by IoT devices, so these are connected on a network, it can be public or private. If each device has an outdated configuration, this is a sign that is leaving a loophole for a possible intrusion.

Each user can prevent their devices from being accessed without authorization, such as changing the login and password data, which in some cases are still in the factory default setting; Rename and password of the wi-fi network with some frequency, avoiding using names and passwords that are easy to deduce; Enable two-factor authentication; Keep your devices up to date at all times; Make the change if possible when there is no further support from the manufacturer. Every attitude like this creates a culture of protection and security, reducing the chances of undue access.

Methodology:-

In this study, two exploratory studies were conducted, which began with the use of Shodan and Censys search engines, in order to find vulnerabilities in IoT devices nationwide. The devices that the search engines found and their vulnerabilities were catalogued. Next, a direct survey was carried out in a group of people about the knowledge that the set had about web security practices, for this, Google Forms was used to create the form, because this method has the possibility of reaching various types of people in a practical and fast way. The data obtained from both surveys are quantitative, where in the first survey we obtained numbers of devices with obvious security flaws, while in the second survey, through the questionnaire with questions and answers of the type "Yes" or "No", the level of knowledge that the interviewee had was evaluated. The search engines that were used have functionalities that are only released after making a payment, are filters that cover the radius of analysis of territory and amount of

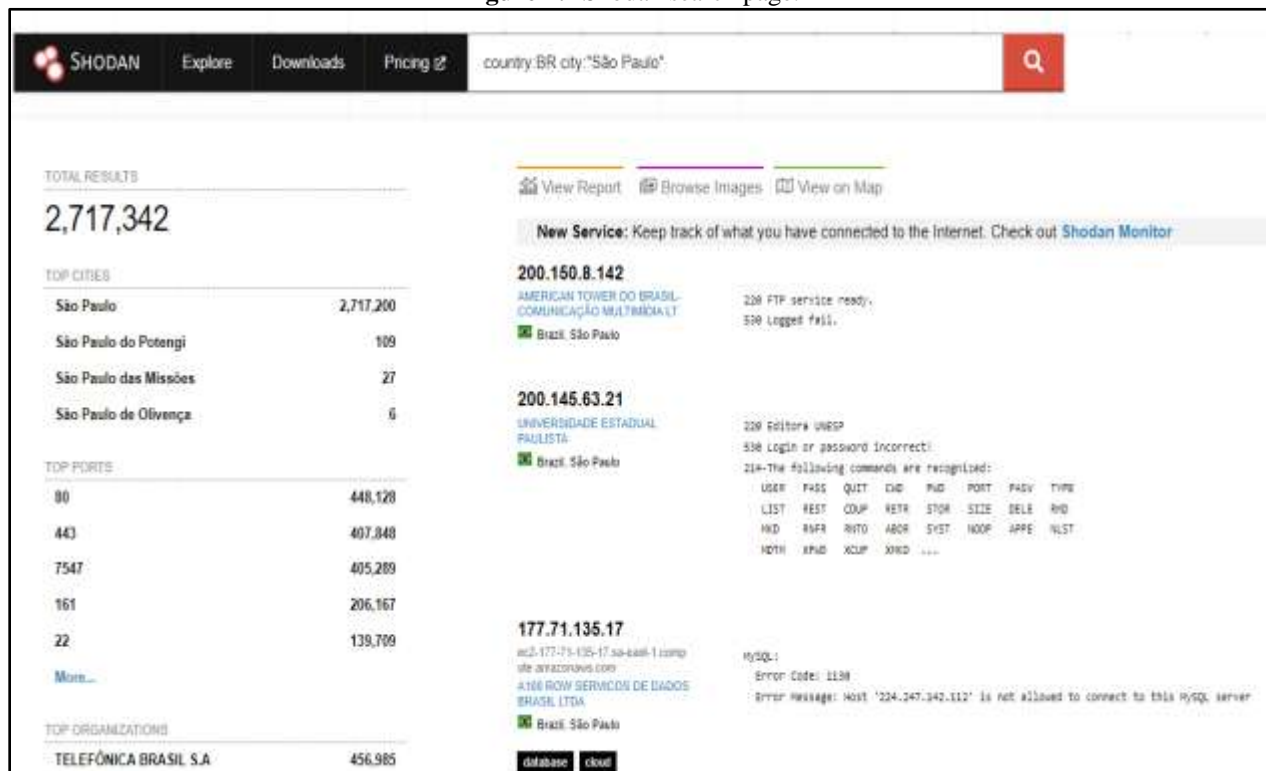
equipment, thus affecting the type of search, becoming more superficial, as a solution, two search engines were used, so each would supply the limitation of the other. **FINDINGS**

The search was started by searching for devices that would have vulnerabilities exposed on the network with the two Shodan and Censys search engines. After the research was raised about the knowledge of a group of people about the Internet of Things and about device security through an online form..

Search Engines

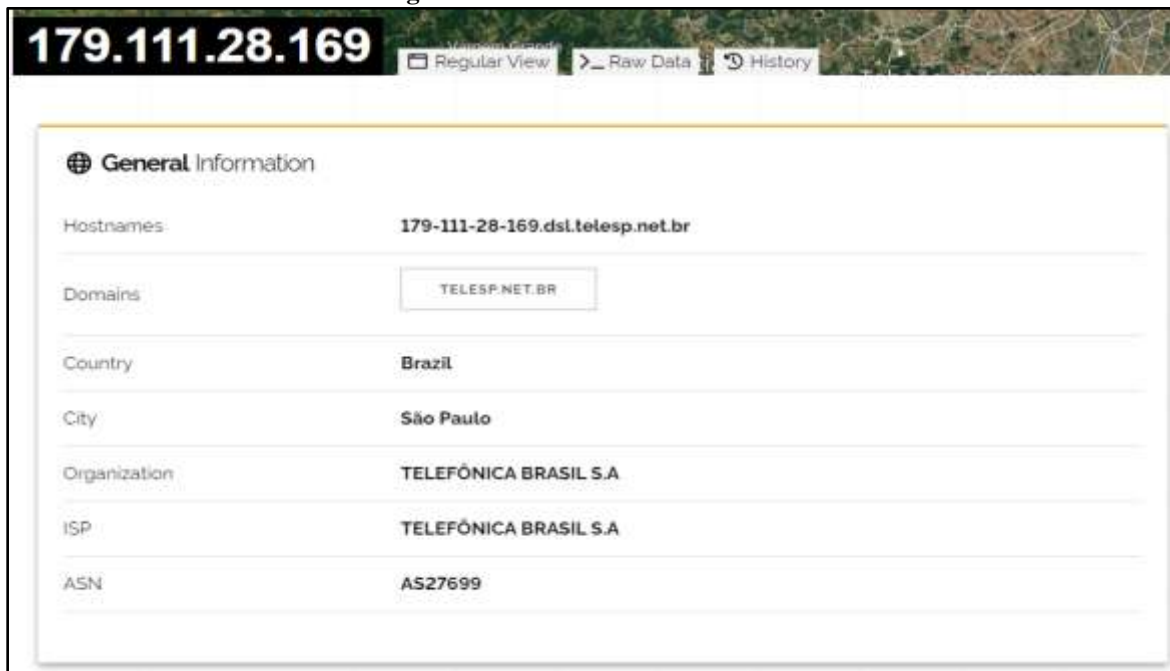
With the Shodan tool were found several devices in the network with specific information, from the port being used, location and protocols being used. To start the search, a registration was made on the tool's website. Only after informing the requested data, such as email, username, password for access, among others, can you use the search engines on the network. The great difficulty was learning how the search was done, its syntax from which the filters are mounted, these are the special keywords that Shodan uses to find specific properties, example: "country:BR". All tags follow the standard of the English language, then the text you want to consult, in the case "country" would be the country, followed by the signal two points the required text, "BR" the acronym of the desired country, in the case of Brazil. The filters can be combined to further measure the research, for example: "country:BR city:"São Paulo", where the term "city" was inserted into the filter, which would be the city and finally the text searched, "São Paulo".

Figure 1:- Shodan search page.



Source: Authors, 2022.

With this search it was possible to find 2,717,342 devices on the network, only in brazil country and in the city of São Paulo. By selecting the ip of the device you can see in more detail the registry.

Figure 2:- General device information.

Source: Authors, 2022.

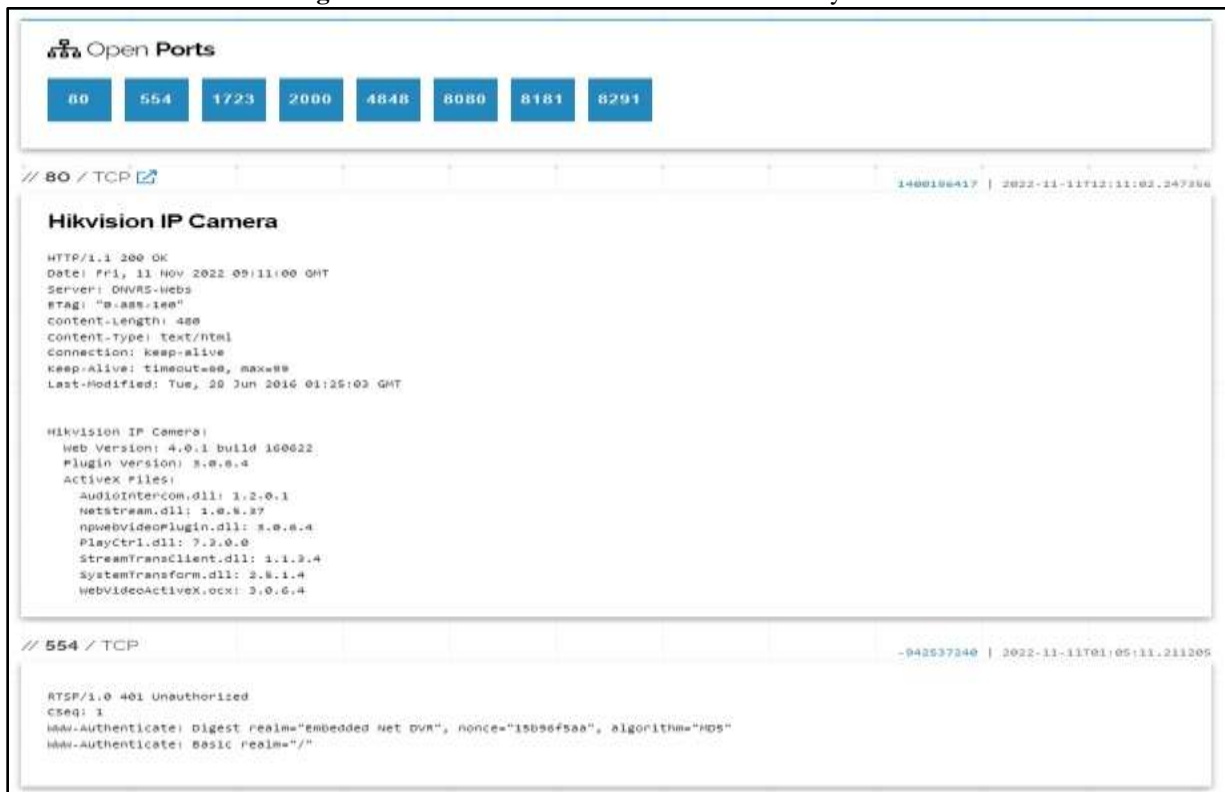
In General Information, brings the main information of the device, such as hostname, the name of the machine in the network, domain, country, city, organization, ISP, internet service provider and ASN, number of autonomous system on the network.

Figure 3:- Information about device ports and services.

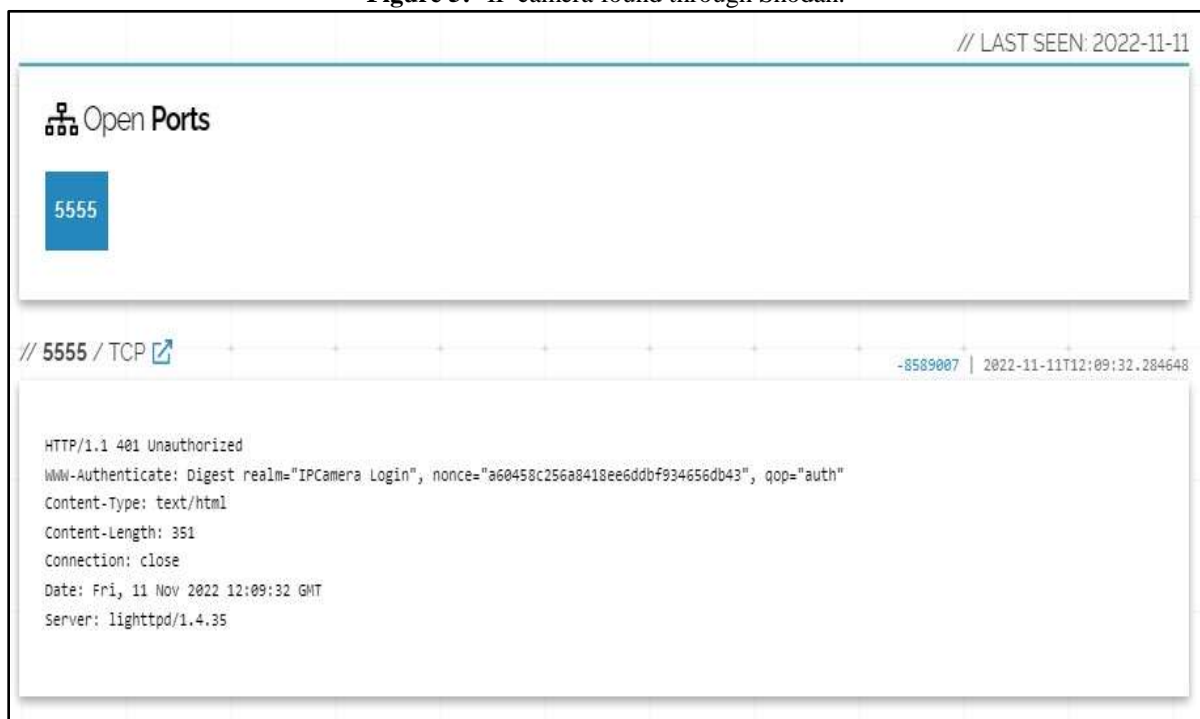
Source: Authors, 2022.

On the same page you can view the port that this device is using, the service that was used, and the device model. This information is available with a simple registration with Shodan, and anyone can have that access. For free accounts access is limited to a certain amount of search and pages that the user tries to access.

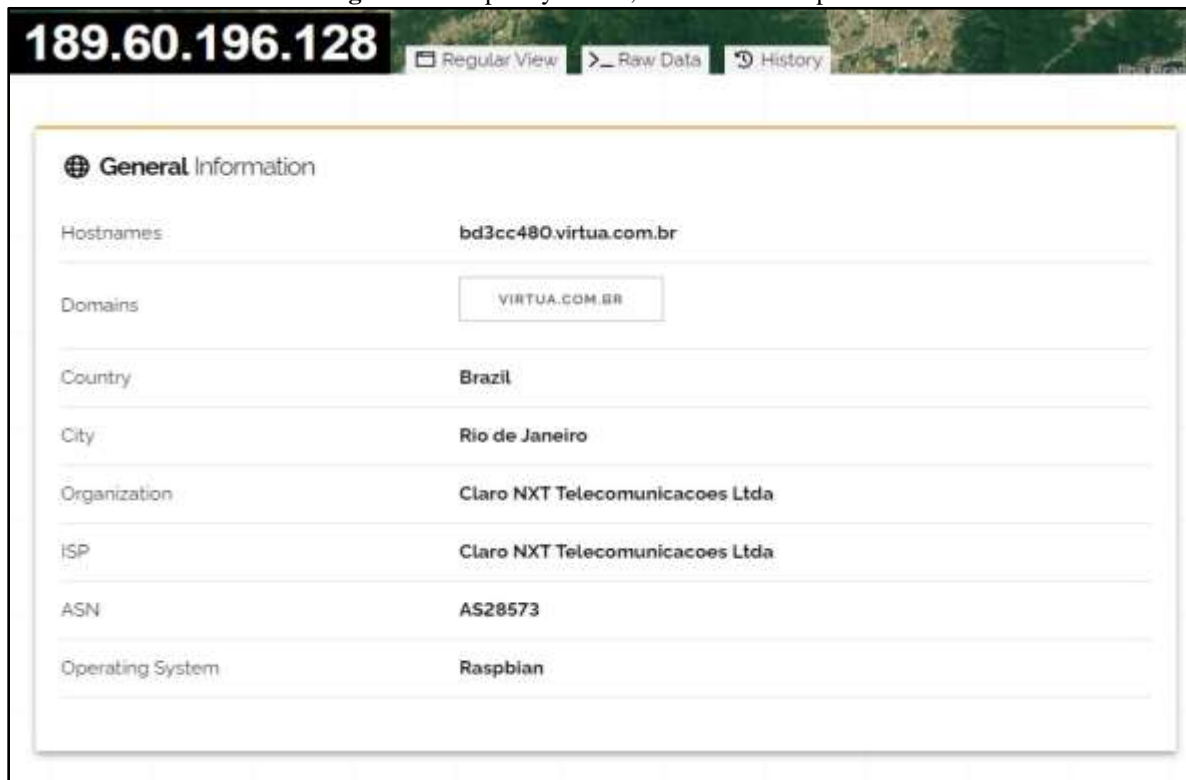
Performing other search filters, devices such as cameras, microcontrollers, video games and computers with released remote access were found.

Figure 4:- Hikvision Camera Information found by Shodan.

Source: Authors, 2022.

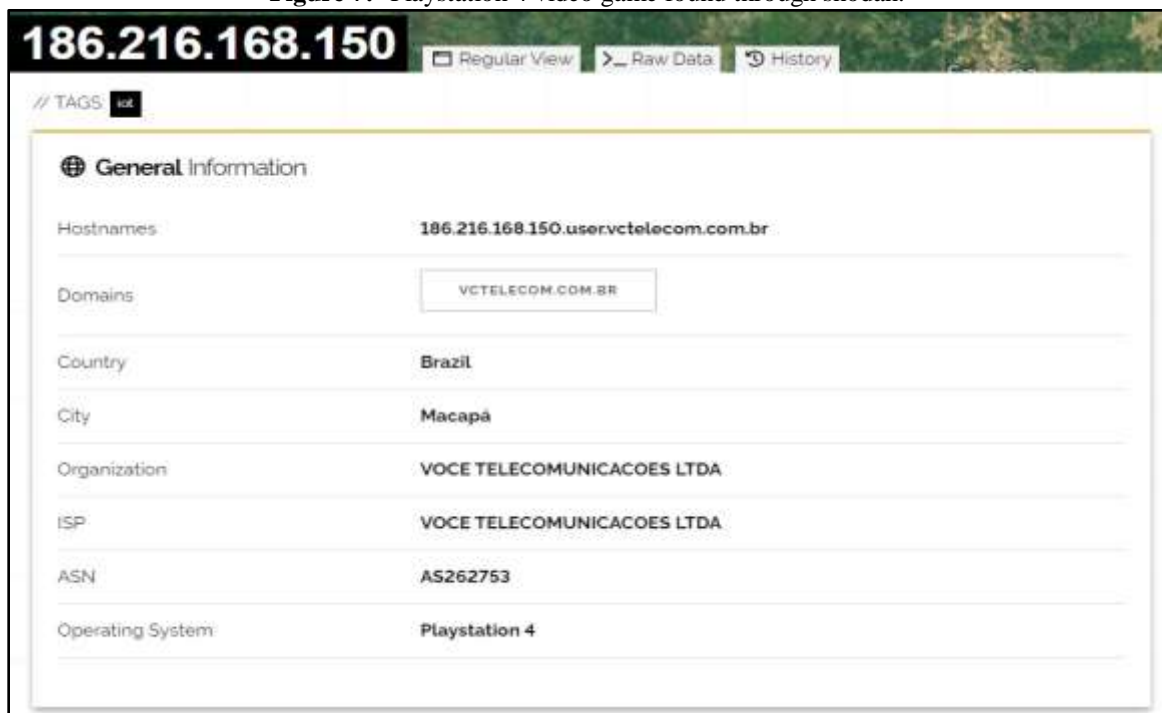
Figure 5:- IP camera found through Shodan.

Source: Authors, 2022.

Figure 6:- Raspberry device, microcontroller plate.

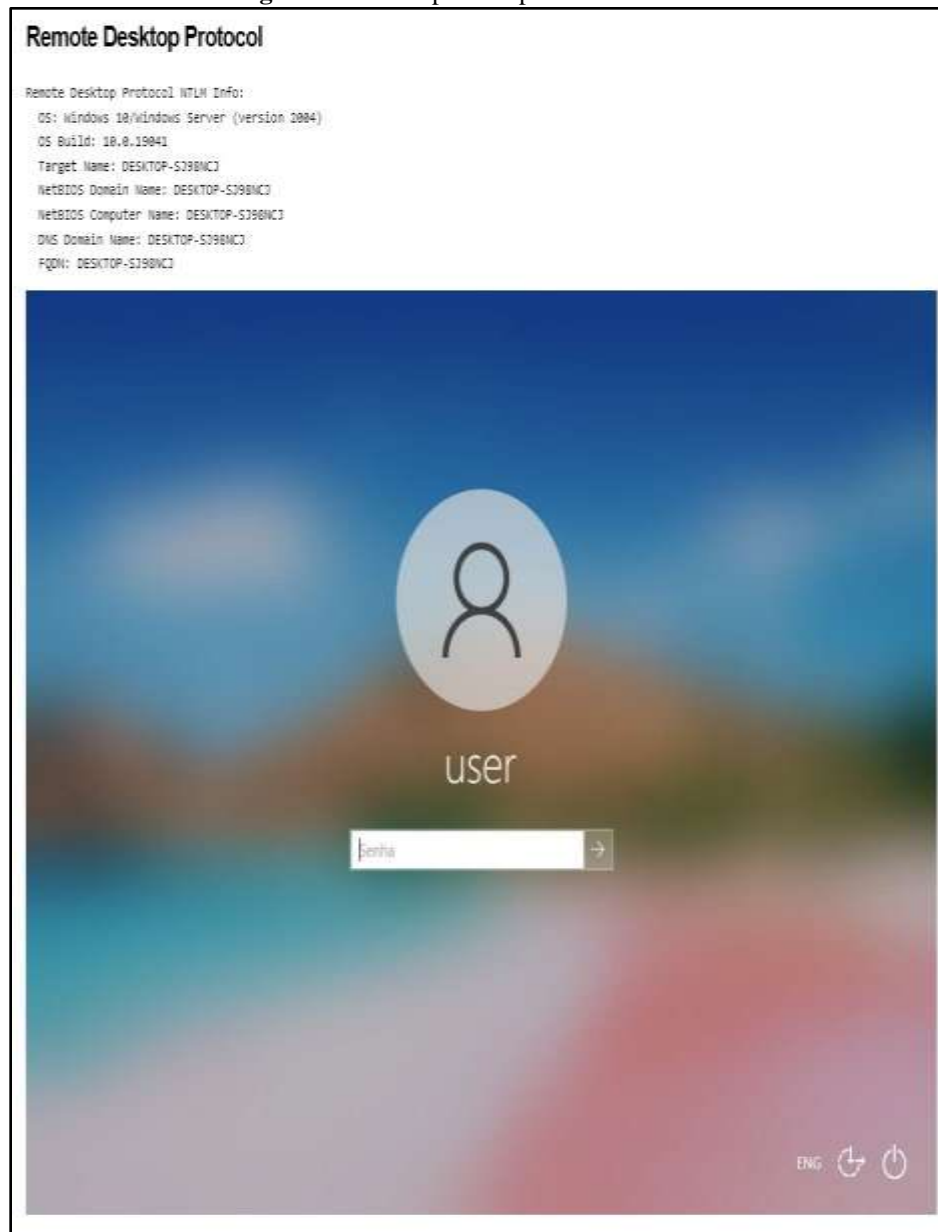
189.60.196.128		Regular View	Raw Data	History
General Information				
Hostnames	bd3cc480.virtua.com.br			
Domains	VIRTUA.COM.BR			
Country	Brazil			
City	Rio de Janeiro			
Organization	Claro NXT Telecomunicacoes Ltda			
ISP	Claro NXT Telecomunicacoes Ltda			
ASN	AS28573			
Operating System	Raspbian			

Source: Authors, 2022.

Figure 7:- Playstation 4 video game found through shodan.

186.216.168.150		Regular View	Raw Data	History
// TAGS iot				
General Information				
Hostnames	186.216.168.150.uservctelecom.com.br			
Domains	VCTELECOM.COM.BR			
Country	Brazil			
City	Macapá			
Organization	VOCE TELECOMUNICACOES LTDA			
ISP	VOCE TELECOMUNICACOES LTDA			
ASN	AS262753			
Operating System	Playstation 4			

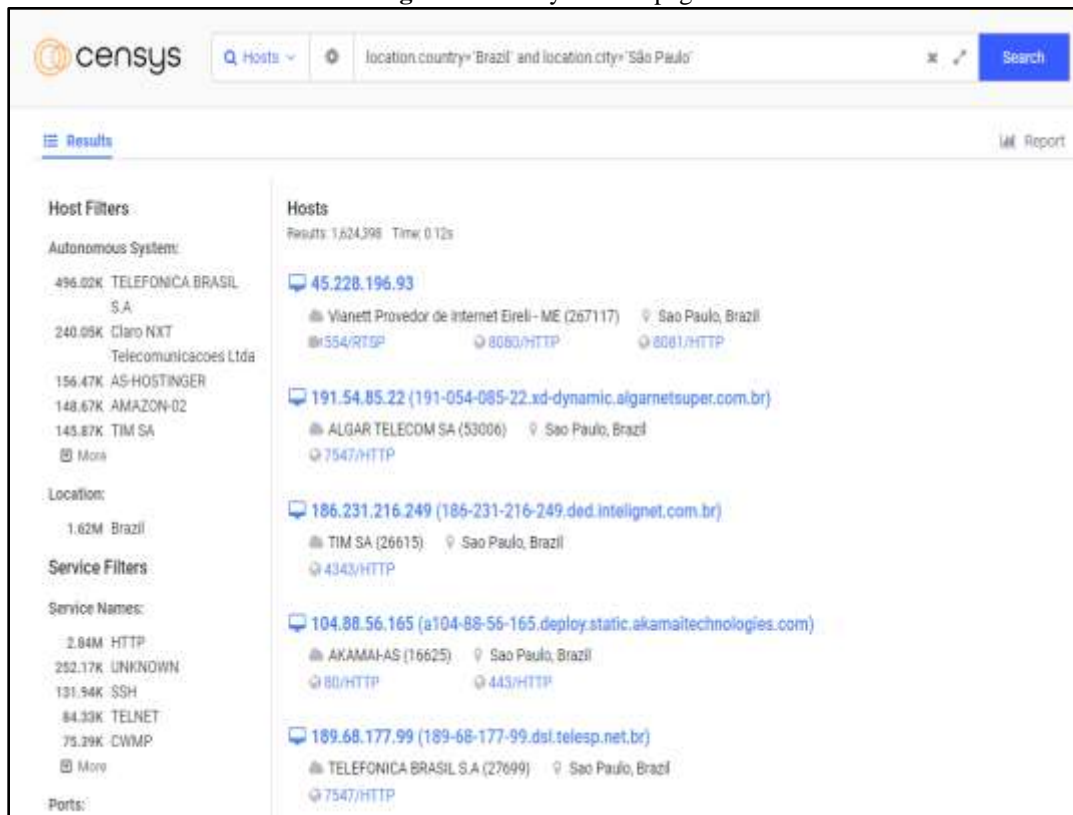
Source: Authors, 2022.

Figure 8:- Desktop with open remote access.

Source: Authors, 2022.

Common devices that are connected to the network, but have some kind of opening so that your data can be received by search engines, may be vulnerable to people with sufficient knowledge who can use this information for illicit means.

Another search engine used was Censys, a search engine similar to Shodan, with more search capacity and freedom for free accounts. The search method is similar, using English tags with small differences, for example: "location.country='Brazil'". When performing the search only for the country Brazil, we can count 1,624,398 results, a difference of 1,092,944 for the search engine Shodan, when performing the search only in Brazil and the city of São Paulo.

Figure 9:- Censys search page.

Source: Authors, 2022.

The search result brought us similar devices and when you click the ip, advanced information is displayed such as the type of service, the most detailed location, and the protocols that are used.

Figure 10:- Device with exposed vnc found through Censys.

Source: Authors, 2022.

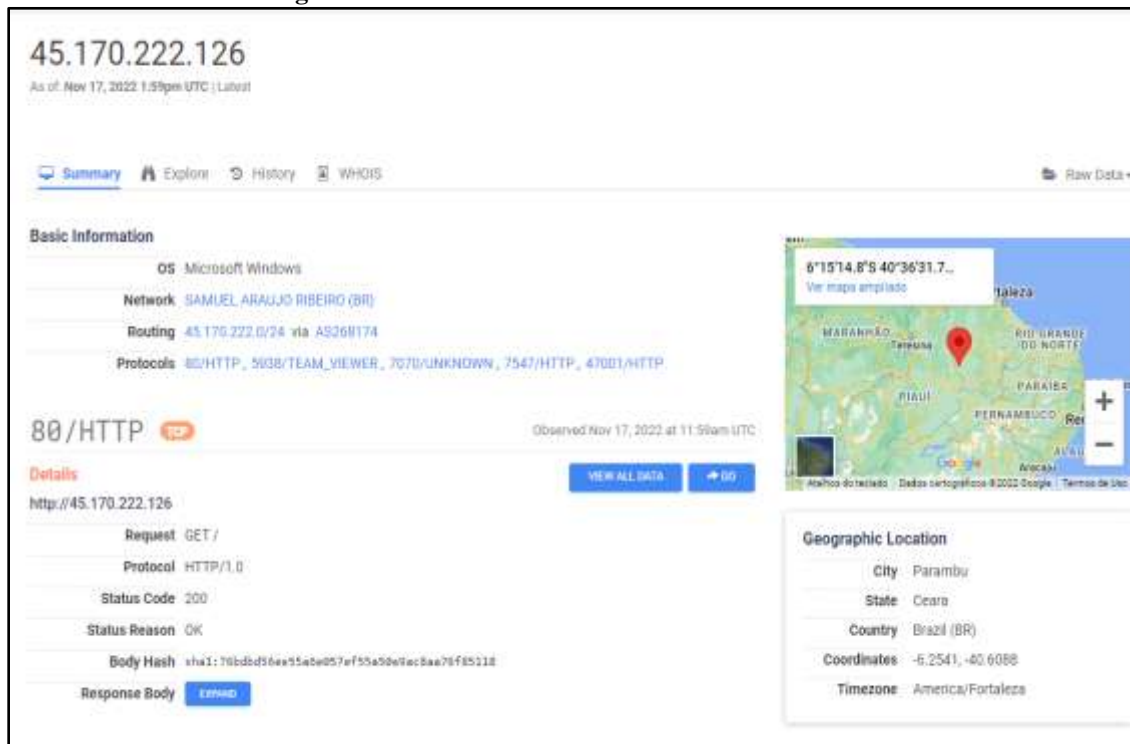
On this device, the display with details brought us an exact print of the screen of the device from which the vnc service was unprotected.

Figure 11:- Screen of a smartphone found by Censys.

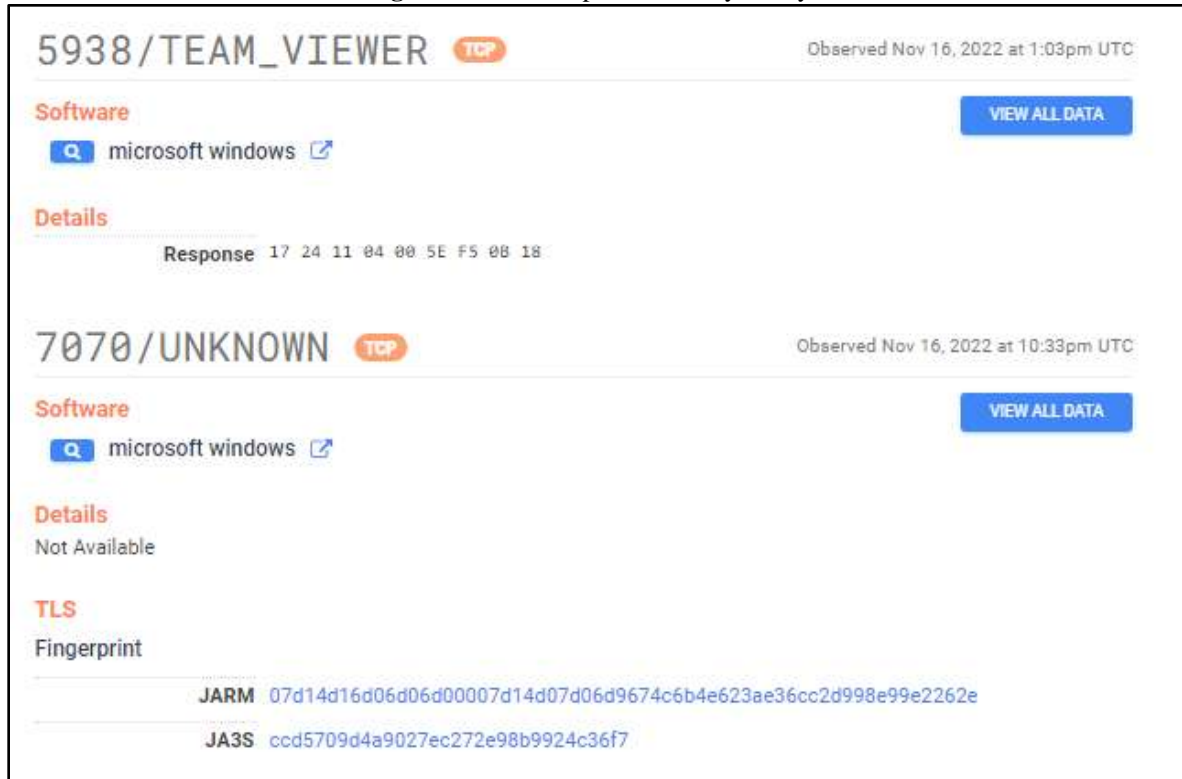
The screenshot shows a mobile application interface with a blue header bar. The status bar at the top displays location, signal, 4G, and the time 11:18. The app header features a logo and the title 'Detalhe'. Below the header is a blue bar with the text 'E65179 / 03 / 5,0'. The main content area contains three input fields: 'Leitura' with the placeholder '#####', 'Nota', and 'Comentário'. Below these fields is a list of text entries: 'COND EDF ESPLANADA DO MAR', '0001588127, RESIDENCIAL, Ativo', 'RUA JORN HERCILIO CELSO, 559', 'CANDEIAS, JABOATAO DOS GUARARAPES', 'C006904', 'COND EDF ESPLANADA DO MAR', and 'C006904'. At the bottom are two blue buttons labeled 'SAIR' and 'LER'.

Source: Authors, 2022.

Services such as remote access may be vulnerable on the Internet, using the search tags "location.country='Brazil'" and services.team_viewer.response=*"", where we seek services of the Teamviewer application with possible doors open in brazil country, such as:

Figure 12:- Screen with all the information on a device.

Source: Authors, 2022.

Figure 13:- Device ports found by Censys.

Source: Authors, 2022.

In the more detailed view, all the ports that this device is using and its protocols appear.

Discussion Of Results:-

Through the data obtained, we can see that devices on the network have some kind of vulnerability and can be easily found by search engines specialized in cataloging devices that have some kind of open door or security flaw. With the questionnaire we were able to analyze that the Internet of Things is in the daily life of each person, whether in devices that act in the background to facilitate our daily life or even in our mobile devices. And that security practice has become a means of protecting against intrusions or data theft, each person can perform some kind of practice, such as periodically changing the password of their accesses and as well as constantly updating their devices. It was found that 54.5% of the people who participated have had some kind of stolen data or undue access in their devices, as well as 90.9% have some kind of security practice to protect themselves.

Confinal Siderações

The internet of things has become allied with many people, whether they are of any age or social class, it is a network that connects devices and performs all kinds of information exchange. But as a network that is constantly connected it is necessary to perform security practices to be secure. Protection is ideal for devices that are part of this network and for users who enjoy the advantages that, for example, use of artificial intelligences, sensors, and even banking transactions provide us. The world is constantly evolving, and its technologies are already outdated, as new ones emerge every moment, new trends and new wireless connections are emerging. Failures and vulnerabilities will always exist, as will tools that can detect these exposures. It is necessary for each person to have a security practice, this can save their data from intrusions and provide peace in knowing that their devices are safe from unwanted access.

Bibliographic Reference:-

1. ALMENARA, Igor. More than 5 billion people have access to the internet, research shows. **CanalTech**, April 26, 2022. Available in: <<https://canaltech.com.br/internet/mais-de-5-bilhoes-de-pessoas-tem-acesso-a-internet-214836>>. Accessed: Oct 11, 2022.
2. BORGES, Esteban. Shodan: Diving into the Google of IoT Devices. **SecurityTrails**, Oct 29. Available in: <<https://securitytrails.com/blog/what-is-shodan>>. Accessed: Oct. 11. 2022.
3. COSTA, Carlos Luiz. Vulnerabilities in IoT Devices for Smart Home Environment. Polytechnic Institute of Beja. 2018.
4. TOTVS TEAM. Internet of Things: what it is, emergence, applications and impacts. **TOTVS**, Oct. 10, 2022. Available in: <<https://www.totvs.com/blog/inovacoes/aplicacoes-da-internet-das-coisas>>. Access: September 20, 2022.
5. LOURENÇO, Gabriel D. Hacker attacks on the Internet of Things in the world double — and Brazil is 2nd largest in Latin America. **Digital Look**, Sep. 22, 2021. Available in: <<https://olhardigital.com.br/2021/09/22/seguranca/hackers-internet-das-coisas>>. Accessed: Oct 11, 2022.
6. MAGRANI, Eduardo. The Internet of Things. Rio de Janeiro: FGV Editora, 2018.
7. PAREDES, Arthur, 2019. Learn about the history of the Internet from its first connection to today. **IEBS**, 30 April 2019. Available in: <<https://www.iebschool.com/pt-br/blog/software-de-gestao/conheca-a-historia-da-internet-desde-sua-primeira-conexao-ate-hoje/#:~:text=A%20verdadeira%20origem%20da%20Internet,da%20Stanford%20e%20da%20UCLA>>. Accessed: Sep 19, 2022.
8. SYDLE. What is the Internet of Things? Learn all about IoT, March 22, 2022. Available from: <<https://www.sydle.com/br/blog/internet-das-coisas-6239c79c3bbdd676577a1e76/#:~:text=Isto%20significa%20que%2C%20em%20m%C3%A9dia,de%20bilh%C3%B5es%20de%20seres%20humanos.>>. Accessed: Oct. 11. 2022.