Security at the Expense of Privacy

Leira C. Quiñones Torres
Master in Cybersecurity
Jeffrey Duffany
Computer Science Department
Polytechnic University of Puerto Rico

Abstract *— The security field has been increasing in recent years. Smart devices have enabled people to monitor and be connected remotely to their homes. Therefore, in the technology field, we must provide people with the knowledge to take full advantage of these devices while ensuring that their privacy has not been compromised or exposed. The challenge is to understand the responsibility of acquiring a security or monitor camera and the considerations we must keep in mind while installing and configuring a system. People are continually monitoring the wireless systems around us, searching specifically for admin accounts. If our camera system's configuration is the default one, we are putting our devices and privacy at risk. The purpose of using our secure passwords for the admin accounts is to restrict the possibilities of people accessing our system without our authorization.*

Key Terms *— admin accounts, smart devices, wireless, vulnerabilities*

INTRODUCTION

The security field has been increasing in recent years. Smart devices or security and monitor systems have enabled people to monitor and be connected remotely to their homes at all the time. This connection means that these IP cameras and the associated devices are connected to a network. It is no secret that all devices connected to a network are at risk of being hacked; for this reason, Internet-connected cameras require special consideration regarding security and configuration. One way that security cameras are vulnerable to hacks is through a technique called credential stuffing, a cyberattack method in which attackers use the list of compromised user credentials to breach into a system. The attack uses bots for automation and scale, and is based on the assumption that many users reuse usernames and passwords across multiple services. [1] With this in mind, we must be aware that vulnerabilities are discovered daily. Calculating the level of critical risk will depend on how easily a vulnerability can be exploited and how the exploitation could impact the rest of the system. Nowadays, we have had the Mirai botnet attacks, which focus on the tendency to use a default password for all the devices, including web cameras, DVRs, routers, and others. It took advantage of insecure IoT devices by scanning the open Internet port and logging in with the default password. In reality, this practice doesn't require much knowledge for hackers to gain access to cameras to snoop around businesses, record videos, and even sell other parties access to cameras.

In the technology field, we must provide the people with the knowledge to take full advantage of these devices while ensuring that their privacy has not been compromised or exposed. Hackers are continually monitoring the wireless systems around us, searching specifically for admin accounts. If our camera system's configuration is the default one, we are putting our devices and privacy at risk. The purpose of using our secure passwords for the admin accounts is to restrict the possibilities of people accessing our system without our authorization.

BACKGROUND

The reason for this research topic as a design project is that, in light of the high mount of burglary cases due to the pandemic, I decided to install security cameras at my home. In the decision-making process, I researched and compared the most recognized security systems in Puerto Rico and what they offer, and even security cameras sold in stores that can be self-installed. At this time, I noticed people preferred store-bought, self-installed cameras. They discarded security provider companies because most of them require two- or three-year contracts with a monthly monitoring membership.

Verifying the security company's devices, they found a famous vulnerability in their most-used DVRs. The use of a predefined password to access their home cameras created a serious vulnerability in which the privacy of the customer was exposed. In the case of home security cameras, the regular consumer is not aware of the appropriate configuration for their system, and they usually leave the cameras unprotected or with default passwords, creating vulnerabilities for their system. This research topic aims to verify the level of security of the DVR of the security provider and compare other cameras that are more accessible to people.

PROBLEM

As mentioned before, security systems have enabled us to monitor and be connected remotely to our homes at all time. People are buying and installing these devices to record what happens indoors and outdoors. With the implementation of a movement detector sensor, parents install these cameras to monitor their children at all hours. If these cameras are not secured, we share our privacy, habits, and all of our belongings to the world. Today, these attacks are more common than expected, since simple tools help attackers obtain the information required to access our cameras and other devices connected to the same network. Hackers can reuse scripts or code to commit the attack rather than create one of their own. Secondly, the data captured in video surveillance cameras and what they can do with it has become the “goal” to look for insights to steal and sell.

Many companies use default settings for their system since it is more cost-effective for them to set the same default configuration. This configuration includes administrator credentials (username and password), and they made this information public in their manuals. Many hackers have created pages where they shared the discovered credentials for administrator accounts. Hence, if we keep our systems with the default configuration, the exposure risk is significant. We are probably exposing ourselves instead of adding a security layer by monitoring our home and family.

Following the description of the hardware and software used, I present the most common steps to gain access to security cameras and how the security monitor companies fixed their most significant vulnerabilities in their DVRs.

EQUIPMENT AND MATERIALS

Hardware Components

- **Hikvision DVR model DS-7208HQI-K2:** a Digital Video Recorder (DVR), a consumer electronics device designed for recording video in a digital format to a disk drive, USB flash drive, SD memory, or other networked storage devices. [2]

Software Components

- **Angry IP Scanner:** an open-source and cross-platform network scanner designed to be fast and simple to use. It scans IP addresses and ports. [3]
- **Shodan:** the search for everything on the Internet. It helps to find specific types of devices (webcams, routers, servers, etc.) connected to the Internet using a variety of filters. [4]

METHODOLOGY

This research goes on two approaches. The first one consists of testing the security flaw discovered by the community in Hikvision DVRs. The exploited backdoor allows the user to gain access to security cameras. Figure 1 describes the process of connecting our computer to a network and using the IP Angry Scanner. We obtain the device IP address to which the cameras are connected to the DVR device.

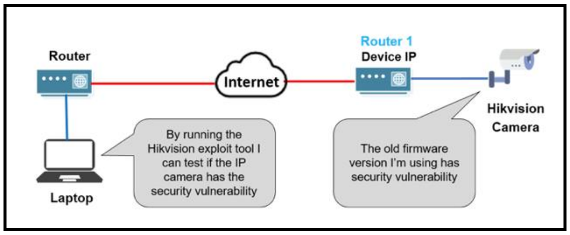
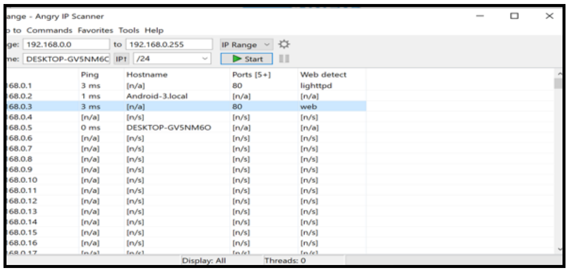

Router
Internet
Router 1
Device IP
Hikvision Camera
Laptop
By running the Hikvision exploit tool I can test if the IP camera has the security vulnerability
The old firmware version I'm using has security vulnerability

Figure 1
How the Hikvision backdoor was exploited

After installing, we can proceed to configure the IP Angry Scanner. In this case, we need to set the preferences of the tool to search for the ports 80 (HTTP/HTTPS), 23 (Telnet), 8080 (HTTP/HTTPS), 8081(TCP), and 8082 (TCP/UDP). After this, in the fetchers option, the Web detects need to be included. Then we are ready to establish the IP range to search in the surrounding networks (figure 2). During the scan, by right-clicking on the Web detect column, the Angry IP Scanner finds a DVR and takes the user to the DVR login page (figure 3).


ange - Angry IP Scanner

ge: 192.168.0.0 to 192.168.0.255 IP Range

me: DESKTOP-GV5NM6C IP↑ /24 Start

	Ping	Hostname	Ports [5+]	Web detect
168.0.1	3 ms	[n/a]	80	lighttpd
168.0.2	1 ms	Android-3.local	[n/a]	[n/a]
168.0.3	3 ms	[n/a]	80	web
168.0.4	[n/a]	[n/s]	[n/s]	[n/s]
168.0.5	0 ms	DESKTOP-GV5NM6O	[n/a]	[n/a]
168.0.6	[n/a]	[n/s]	[n/s]	[n/s]
168.0.7	[n/a]	[n/s]	[n/s]	[n/s]
168.0.8	[n/a]	[n/s]	[n/s]	[n/s]
168.0.9	[n/a]	[n/s]	[n/s]	[n/s]
168.0.10	[n/a]	[n/s]	[n/s]	[n/s]
168.0.11	[n/a]	[n/s]	[n/s]	[n/s]
168.0.12	[n/a]	[n/s]	[n/s]	[n/s]
168.0.13	[n/a]	[n/s]	[n/s]	[n/s]
168.0.14	[n/a]	[n/s]	[n/s]	[n/s]
168.0.15	[n/a]	[n/s]	[n/s]	[n/s]
168.0.16	[n/a]	[n/s]	[n/s]	[n/s]
168.0.17	[n/a]	[n/s]	[n/s]	[n/s]

Display: All Threads: 0

Figure 2
Angry IP Scanner Results

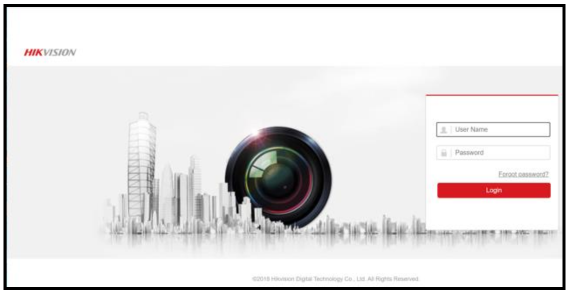

HIKVISION
User Name
Password
Forgot password?
Login
©2018 Hikvision Digital Technology Co., Ltd. All Rights Reserved.

Figure 3
Hikvision device login

In the community's tutorial, these three easy steps were all that was required to access all the cameras connected to this office or home. The use of a default password for the admin account in their devices opened a vulnerability easy to exploit, which affected their firmware versions from the V5.2.0 build 140721 to V5.3.9 build 170209. The company fixed this vulnerability by asking each user to set their own admin password. If a user forgets the password and wants to change it, it can be done by configuring the Hik-Connect App, answering the security question, or through the GUID File, which the user needs to export in advance from the DVR. Then, in the configuration window, the user will export the GUID File, and the password will be reset.

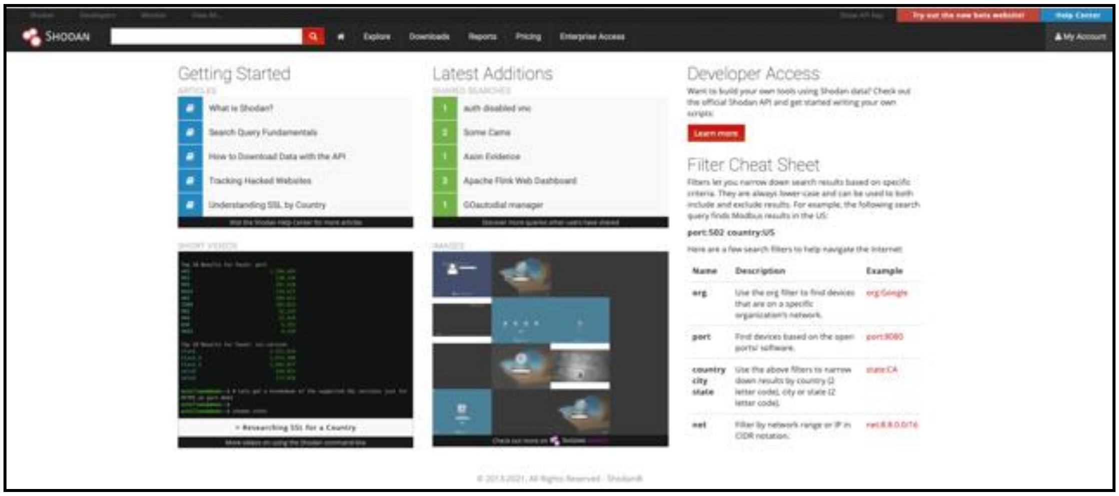
The second approach is the use of Shodan. Shodan is a free website that shows all the Internet devices connected around the world, including routers, cameras, DVRs, etc. (figure 4). Even Although this tool is free, it requires the user to register before using the application filters that will allow them to make a more precise search.

For this research, I used the filters “yawcam” and “AXIS” in Shodan. Yawcam stands for “Yet Another WebCAM.” Yawcam is a webcam software for windows. This application includes features of video streaming, image snapshots, a built-in web server, and motion detector, among others. AXIS Communications is a company dedicated to providing secure solutions, including cameras, audio, online video software, etc.

Shodan provides a list of results according to the filter written in and allows users to apply additional filters by country, top services, top organizations, and top products (figure 5).

The tool allows users to select the IP address. Once opened, users will find additional information related to that IP address. Shodan provides details about the device, location, and owner; device ports and services; and, on occasion, the system’s vulnerabilities. One of the results analyzed is from North Fork, United States. The ports available are 8081 and 9002. The services were TCP, and it identified the server as yawcam. Clicking the green button took me to the camera home (figure 6).

In this case, since the camera was not password-protected, I was able to access and view the image from a camera that was located outside a house (figure 7).



Getting Started

- What is Shodan?
- Search Query Fundamentals
- How to Download Data with the API
- Tracking Hacked Websites
- Understanding SSL by Country

Latest Additions

- 1 auth disabled vnc
- 2 Some Cams
- 1 Axin Evidence
- 3 Apache Flink Web Dashboard
- 1 GOautodial manager

Developer Access

Want to build your own tools using Shodan data? Check out the official Shodan API and get started writing your own scripts:

Learn more

Filter Cheat Sheet

Filters let you narrow down search results based on specific criteria. They are always lower-case and can be used to both include and exclude results. For example, the following search query finds Modbus results in the US:

port:502 country:US

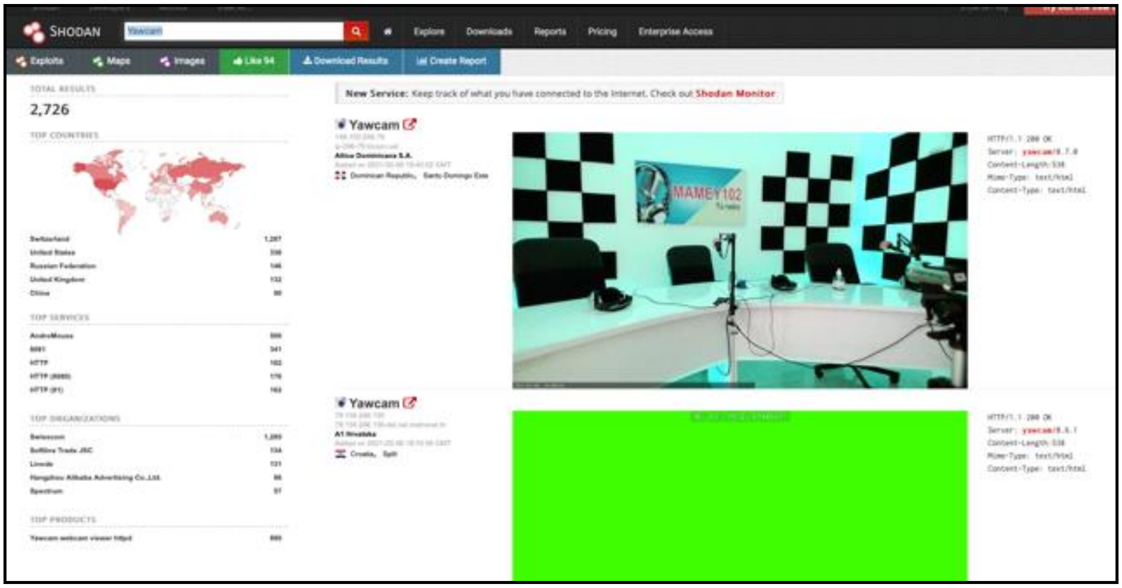
Here are a few search filters to help navigate the internet:

Name	Description	Example
org	Use the org filter to find devices that are on a specific organization's network.	org:Google
port	Find devices based on the open ports/ software.	port:8080
country city state	Use the above filters to narrow down results by country (2 letter code), city or state (2 letter code).	state:CA
net	Filter by network range or IP in CIDR notation.	net:8.8.0.0/16

© 2013-2021, All Rights Reserved - Shodan®

Figure 4

Shodan website



TOTAL RESULTS

2,726

TOP COUNTRIES

Switzerland	1,287
United States	336
Russian Federation	146
United Kingdom	132
China	90

TOP SERVICES

AndroMouse	399
8081	341
HTTP	182
HTTP (8080)	176
HTTP (81)	163

TOP ORGANIZATIONS

Swisscom	1,285
Softline Trade JSC	134
Linode	121
Hangzhou Alibaba Advertising Co.,Ltd.	96
Spectrum	57

TOP PRODUCTS

Yawcam webcam viewer httpd	880

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

Yawcam

Altice Dominicana S.A.

Dominican Republic, Santo Domingo Este

```
HTTP/1.1 200 OK
Server: yawcam/0.7.0
Content-Length:538
Mime-Type: text/html
Content-Type: text/html
```

Yawcam

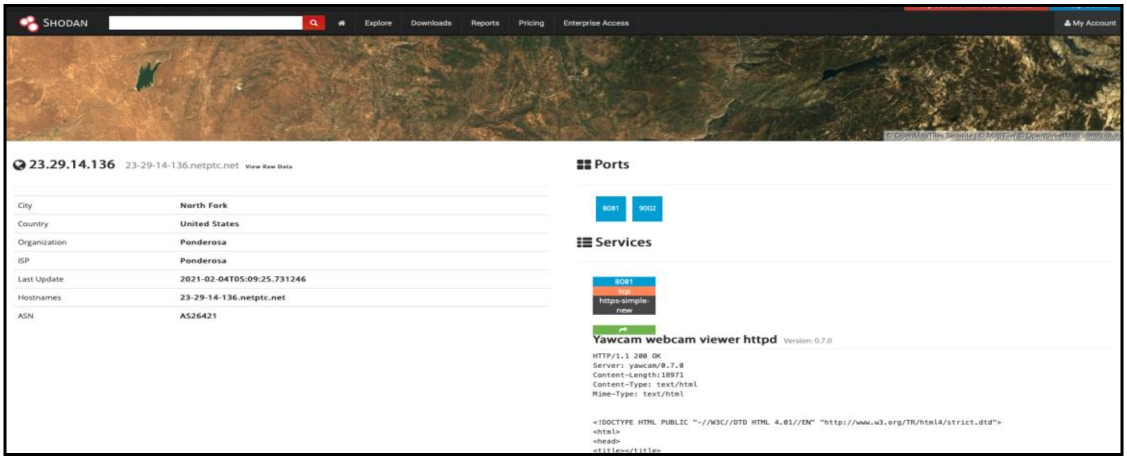
A1 Hrvatska

Croatia, Split

```
HTTP/1.1 200 OK
Server: yawcam/0.6.1
Content-Length:538
Mime-Type: text/html
Content-Type: text/html
```

Figure 5

Shodan Search result



23.29.14.136 23-29-14-136.netptc.net

City	North Fork
Country	United States
Organization	Ponderosa
ISP	Ponderosa
Last Update	2021-02-04T05:09:25.731246
Hostnames	23-29-14-136.netptc.net
ASN	AS26421

Yawcam webcam viewer httpd Version: 0.7.0

```
HTTP/1.1 200 OK
Server: yawcam/0.7.0
Content-Length:18971
Content-Type: text/html
Mime-Type: text/html


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<title></title>
```

Figure 6

Shodan website results for the selected IP

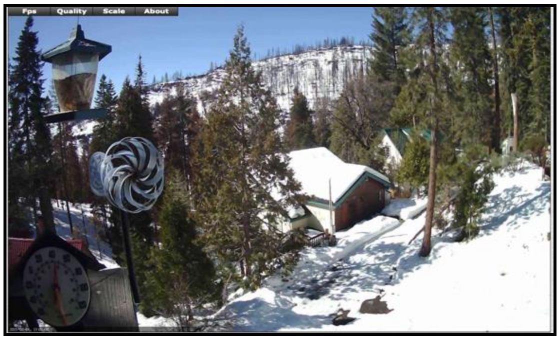


Figure 7
Camera in first selected IP Address

A similar result was obtained using yawcam to search. This other example uses the city of Elkin, United States. I could access their interior camera. (figure 8).

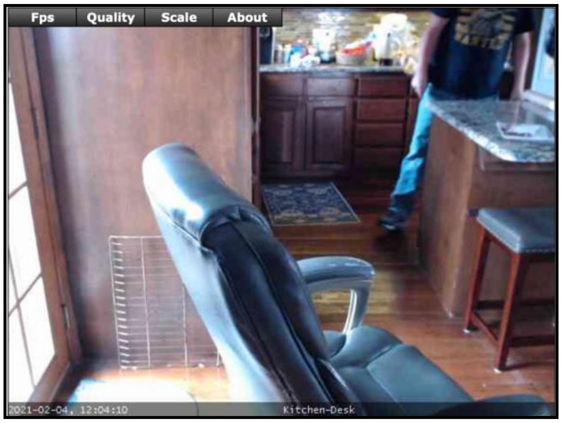
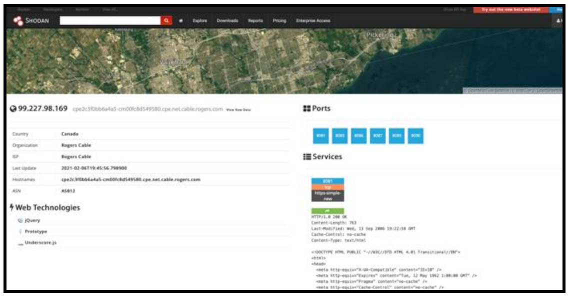


Figure 8
Camera in second selected IP Address

Using the keyword for AXIS in Shodan's tools, access was gained to the interior of a veterinary clinic in Canada. In this case, the Shodan tool also provided information about the Web technologies used in this targeted IP (figure 9).



99.227.98.169 cpe2c3f0bb6a4a5-cm00fc8d549580.cpe.net.cable.rogers.com

Country	Canada
Organization	Rogers Cable
ISP	Rogers Cable
Last Update	2021-02-06T19:45:56.798900
Hostnames	cpe2c3f0bb6a4a5-cm00fc8d549580.cpe.net.cable.rogers.com
ASN	AS812

Web Technologies
- jQuery
- Prototype
- Underscore.js

Ports

Services

```
HTTP/1.0 200 OK
Content-Length: 763
Last-Modified: Wed, 13 Sep 2006 19:22:58 GMT
Cache-Control: no-cache
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
  <meta http-equiv="X-UA-Compatible" content="IE=10" />
  <meta http-equiv="Expires" content="Tue, 12 May 1962 1:00:00 GMT" />
  <meta http-equiv="Pragma" content="no-cache" />
  <meta http-equiv="Cache-Control" content="no-cache" />
```

Figure 9
IP details of third selected search

In this search, the information collected allowed access to other three cameras connected to the same network (figure 10).

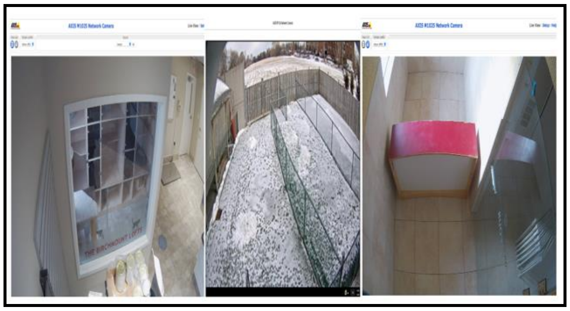


Figure 10
Cameras in fourth selected IP Address

Results and Discussion

The results obtained have shown that all the devices connected to a network are at risk. Vulnerabilities in the systems are developing continuously and, at the same time, hackers are finding creative ways to identify and exploit these vulnerabilities. The most significant vulnerability in any organization's security is the human at the end of the system. I always understood there were two ways to separate exposures. First, we had those that, even if we cannot control, we can make more difficult to be exploited, and then we had faults in the system or coding that are the responsibility of the company that developed or installed the device. Using these two categories, I can determine that we, as users, are responsible for creating vulnerabilities due to connectivity and poor password management. This validated that the more devices we have connected to our network, the higher the risk of exposure. Using the IP Angry Scanner, we scanned a range of IP addresses in seconds, and the more connected devices there are, additional devices were able to select to spy or as targets. For example, if a hacker can access our cameras, it is also possible that other devices, like smart assistants, can also work as microphones. The greatest vulnerabilities are due to poor password management. Passwords represent a challenging task for all of us. Setting up a different password for each website, social media site, and other accounts is “hard.” For this reason, sometimes we use a default password as a quick solution or, on occasion, we opt to use personally identifiable information such as family names, birth dates, common words, or credit card numbers. This practice is not recommended, since this information can be easily obtained from public social media profiles.

Let's see the first approach in this research—the Hikvision DVR. Imagine that you are trusting your home or office is “secure,” relying on if something unpredictable comes up; I will be able to monitor and obtain the video as evidence. But for years, that same person was having their private life exposed to the world without a single clue. In their minds, they were "secure." Companies that maybe have this system to monitor the employees, how much information inadvertently they shared by this simple mistake of not changing the default password. Another scenario to consider is that something indeed happens, and in this case, since the hackers have the admin account, they deleted all the evidence stored on the DVR. Let's follow the best practices regarding password management. Let's change the default password from all of our devices to ensure that the security addition we include in our daily is not exposing us to the world. Another recommendation is to keep updating our devices. It is essential to know that some devices are not revised automatically. As responsible users with concerns about our security, we must update it immediately when a new release has been made. In the DVR case, hundreds of people were affected by this vulnerability. If they didn't update their firmware, they would still be at potential risk of exposure.

The second approach during this research was the use of Shodan. Shodan is a free webpage that contains essential information for all the devices connected to the network. This page is so detailed that you can even search for webpages or devices that have default passwords. In the cases analyzed during the research, we found cameras that even didn't contain any passwords. By searching for webcams explicitly, a lot of results were provided by the tool. I use the tool filters to search for those webcams connected specifically to HTTP protocols. As expected, we found various cameras that required the admin or root passwords but found a variety of them that are not close and that anyone can access without any barrier. The first example was from an exterior camera from North Forth, United States. Using port 8081, I was able to connect to the camera and view the surroundings.

The second search in Shodan was from Elkin, United States. In this case, the camera without any password was located in the home's interior, near the kitchen. During the time accessed, the kitchen people were unaware that everything they were doing in the "privacy" was live for everyone to see. This case is a clear example of why we need to be more careful when selecting a camera and where to install it—using again the model of the parents that put cameras on their children's bedroom to keep monitoring them. These parents inadvertently are putting their children's room, the kid's behaviors, and routine for anyone to see. This doesn't mean that putting cameras in the room is terrible, but let's be aware of the risk of exposure that will be present all the time. This is a lesson to also keep in mind the protection keys we must consider during the decision making on which camera to buy. Many pages that talk about this type of issue suggest to the users to search for cameras that require two-factor authentication. This extra layer of security will ensure that if hackers have gained access to your username or password, they will be unable to access it unless they gain access to the device that provides the authentication code.

The last scenario in this research was to use the Shodan Tool to search for a security vendor. Using the same port that the other cases 8081, we were able to access one camera in the surroundings. Still, we also gained access to all the cameras inside a veterinarian clinic in Canada. This finding validates the connectivity and the risk that the number of devices connected to the same network. Once one vulnerability is detected, other vulnerabilities in connected devices may arise and make it visible to the hackers.

Eavesdropping

Eavesdropping is one of the leading cybersecurity threats that has evolved over the years targeting unsecured networks. The security threat targets information transmitted via an unsecured network. In other cases, the network may be secured but lacks security measures during data transmission. In secured networks, eavesdroppers hack the content of the information through detailed hacking techniques that unveil the content of the information to the malicious person. Secondly, when transmitting through secured networks, the users may fail to encrypt their information. Failed encryption exposes the transmitted information to security threats. This is possible due to overreliance on security plans provided by the internet provider.

With the increasing need for digitalization and automation of processes, companies resort to capturing information through cameras. The cameras are assigned specific IP addresses for the cameras to transfer the data to databases or share the information between themselves. Eavesdroppers keep track of the activities occurring within a certain network. They subject the networks to attacks trying to find a vulnerability. When they hack the IP address of a single camera due to using default passwords, eavesdroppers gain access to the information transmitted between them. They also gain access to any other device that communicates with the camera.

Eavesdropping formulates a larger percentage of cybercrimes. Unlike the man-in-the-middle attacks, eavesdropping ensure the data reaches its destination regardless of any form of assistance. Once the hackers gain access through hacking the camera IP address, they access users' confidential information such as credit card numbers, passwords, and usernames. They use such information to blackmail the user or for extortion.

Artificial Intelligence-Based Cyberattacks

New technology comes with new security threats in the market. The introduction of artificial intelligence (AI) introduced new security challenges in the market, with some becoming undetectable. It is harder to detect an AI-based attack when using the internet. Most internet users do not have the knowledge to identify AI software. This difficulty makes it impossible to prevent people from falling victims to an AI program.

AI programs come in the form of a genuine internet user. In most cases, the programs lure the user with whatever task they can enable the user to accomplish effectively and accurately. Since internet users wish for fast, effective, and accurate software to accomplish tasks, they easily click on such programs. Once clicked, these programs install themselves in the user's computer. They phish user's confidential information to malicious people. The information phished includes passwords and credit details.

Security cameras allow attacks through AI programs through the exploitation of weak passwords and unsecured default camera IP addresses. A malicious person would launch an attack on a network once they gain access to the network. Default passwords unchanged from vendors formulate a larger percentage of vulnerabilities exploitable by the malicious people in a networked camera security system. Once the malicious individual launches the AI program in the network, it learns the network users' behaviors. Having mastered the interests of the users, they push any program that may seem beneficial to the user. Opening the file or folder activates the software, which then installs itself in the computer, phishing users' confidential information to unauthorized users.

IP Cameras Cybersecurity Best Practices: A Collaboration of Network Security Measures by both the Vendor and the User

Technically, most vendors have no after-sale device security monitoring options. Once they sell a company the security cameras, they are done with. It is up to the client to maintain their information collected via the cameras through passwords and secured IP addresses. This strategy has failed most of the time since not all clients understand cybersecurity measures. Clients fail to monitor threats posed to the devices due to a lack of knowledge. After-sales, even if the device came with a security plan, failure to update the information security system to the latest version allows access to emerging attacks. Therefore, to curb security threats emanating through surveillance devices, both the vendor and the user should be actively involved.

Periodic Password Change

Changing passwords periodically reduces brute force attacks. After acquiring the security cameras, the users fail to change passwords. This makes it easier for a malicious person to launch an attack. Therefore, it is recommended that users change their passwords periodically to reduce the chances of being attacked through password guessing.

Network Lockdown

Unplugging one camera and replacing it with a laptop grants access to all other cameras connected to that network. It is advisable to configure the network such that only the cameras installed in the network can communicate via the ports available.

CONCLUSION

The Axi page states that cybersecurity should be approached in two steps awareness and mitigation. This research has provided evidence that if we are not aware of the risks surrounding us, we will not continue to avoid and prevent them. Organizations and vendors opt to keep these vulnerabilities hidden because they state that sharing these vulnerabilities to the public will be making hackers easy exploits these vulnerabilities at a large scale. But as we see in the several cases studied during the research, many people are unaware of their risk and how their privacy is exposed to the world. I'm sure that if this was your case and you know that your camera is live to the world, you will be making all the required changes to make sure that your privacy is preserved. As a recommendation, protect your devices with strong passwords, limit the number of devices connected to your network. In case you are not using a machine, disconnect it from the internet. Do not use default passwords, and make sure that all of your devices are running in the last updated version.

FUTURE WORK

Cybersecurity is a large field, and there are several ways to provide a more comprehensive analysis of how security cameras can expose your privacy to the world. Continues work can include brute force attacks to access the security cameras around the world. This analysis can provide a more completed and detailed report of the most commonly used passwords in security systems. It can also provide statistics about the people who are still using the default passwords.

Future work will be to develop new guidelines to protect the camera's devices and mitigate exposure risk.

REFERENCES

[1] Imperva, "Credential Stuffing." Accessed Feb. 12, 2021. [Online]. Available: https://www.imperva.com/learn/application-security/credential-stuffing/

[2] Techopedia, "Digital Video Recorder (DVR)." Accessed Feb. 12, 2021. [Online]. Available: https://www.techopedia.com/definition/4702/digital-video-recorder-dvr

[3] MacUpdate, "Angry IP Scanner." Accessed Feb. 12, 2021. [Online]. Available: https://www.macupdate.com/app/mac/50267/angry-ip-scanner

[4] J. M. Porup, "What is Shodan? The search engine for everything on the internet," CSO, November 19, 2019. [Online]. Available: https://www.csoonline.com/article/3276660/what-is-shodan-the-search-engine-for-everything-on-the-internet.html