Security At The Expense Of The Privacy

Author: Leira C. Quinones Torres
Advisor: Jeffrey Duffany
Computer Science Department

Abstract

The security field has been increasing in recent years. Smart devices have brought the opportunity for people to monitor and be connected remotely to their homes. Therefore, as people 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. 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 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 to the admin accounts is to restrict the possibilities of people accessing our system without our authorization.

Introduction

Smart devices or security and monitor systems have brought the opportunity for 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 the network. It is not a 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. **Credential stuffing** is 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] Having this in mind, we must be aware that vulnerabilities are discovered daily. Calculating the level of criticality of risk will depend on how easily a vulnerability can be exploited and how the exploitation could impact the rest of the system. Today, we have the Mirai botnet attacks, which focused on the tendency to use default passwords to all the devices, including web cameras, DVRs, routers, and other devices. It took advantage of insecure loT devices by scanning the open internet port and logging in with the default passwords

Background

The reason for this research topic as a design project is that due to the high 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, what they offer, and even the security cameras sell in stores that can be installed by yourself. During this time, I noticed that people preferred the cameras sold in stores, since the camaras offered by the security provider companies require contracts of two to three years paying 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 where the privacy of the customer was exposed. In the case of the home security cameras, the regular consumer is not aware of the appropriate configuration for their system, and usually, they leave the cameras unprotected or using default passwords, creating vulnerabilities on their system.

Problem

Systems have brought the opportunity to monitor and be connected remotely to our homes at all the time. People are buying and installing these devices to record what happens indoors and outdoors. If these cameras are not secured, we share our privacy, habits, and all of our belonging 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.

Methodology

This research goes on two approaches. The first one consists of testing the security flaw discovered by the community in Hikvision DVRs. The backdoor exploited allows the user to gain access to the security cameras.

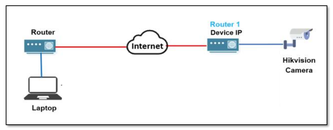

Figure 1- How the Hikvision backdoor was exploited.

Using the IP angry scanner tool and configure the web ports that we are targeting. We need to establish the IP range to search in the networks around me During the scan and by right click the Web detect column, the DVR was found in the Angry IP Scanner tool and took me to the DVR login page.

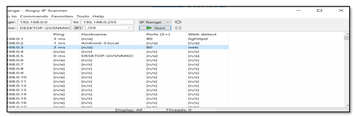

Figure 2 –IP Angry Scanner

The company fixed this vulnerability by asking each user to set their own admin password. If the user didn't remember the password and want to be changed, it can be done using the Hik-Connect App configured, answering the security question, or GUID File. For the GUID file, the user needs to export it in advance from the DVR. Then in the configuration windows, you 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 and DVRs. For the purpose of this research, I use the filter “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, motion detector, among others. AXIS communications are a company dedicated to providing secure solutions, including cameras, audio, online video software. The tool allows you to select an IP address and provides you details about the device, location, and the owner, provides you details about the device ports, services, and on occasions, it includes details about the system vulnerabilities. One of the results analyzed is from Elkin, United States, The ports available are 8081 and 9002 taking me to their interior camera (Figure 3).

Figure 3-Camera from the selected IP Address

The second case analyzed was using the keyword AXIS in Shodan Tool. The access was gained was to the interior of a veterinary clinic in Canada. In this search, the information collected allowed access to other three cameras connected on the same network. (Figure 4).

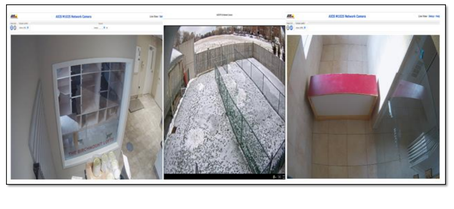

Figure 4- Cameras from the selected IP Address

Results and Discussion

The results obtained have demonstrated 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. This research-validated that as more devices we have connected to our network, the risk of exposure is bigger. Using the IP Angry Scanner, we scanned a range of IP addresses in seconds, and as more devices we have connected, additional devices were able to select to spy or as targets. For example, if a hacker could access our cameras, it is also possible that other devices like smart assistants can also work as microphones. The biggest vulnerabilities are due to poor password management. Passwords represent a challenging task for all of us. Setting a different password for each site, social media, accounts are "hard."

The first approach we had in this research—the Hikvision DVR. Imagine yourself trusting that 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."

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.

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.

Conclusions

The AXIS 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 big 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.

Acknowledgements

I want to acknowledge Dr. Jeffrey Duffany for guiding me through this research. I want to thank all the professors in the Computer Science department that have provided the knowledge and all the learning opportunities offered during my courses.

References

[1] “What is Credential Stuffing: Attack Example & Defense Methods: Imperva,” *Learning Center*, 07-Jul-2020. [Online]. Available: https://www.imperva.com/learn/application-security/credential-stuffing/.
[2] Techopedia, “What is a Digital Video Recorder (DVR)? - Definition from Techopedia,” Techopedia.com, 29-Mar-2016. [Online]. Available: https://www.techopedia.com/definition/4702/digital-video-recorder-dvr.
[3] “Angry IP Scanner3.7.53.7.5See all Versions,” Angry IP Scanner for Mac: Free Download + Review [Latest Version], 05-Feb-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 Online, 19-Nov-2019. [Online]. Available: https://www.csoonline.com/article/3276660/what-is-shodan-the-search-engine-for-everything-on-the-internet.html.