Capstone of 2022: Research Into Spyware

J. Biedrzycki
Computer Scientist B.S. UWRF

A. Lamberty
Computer Scientist B.S. UWRF

M. Olive
Computer Scientist B.S. UWRF

A. Oradei
Software Developer B.S. UWRF

***Abstract*—Spyware is a vast and intricate field of study that requires garnering some background knowledge and modern vernacular before understanding the intricacies of it. With some basic understanding of spyware it is possible to understand the various methods that spyware is utilized. With things such as firewalls and encryption it is possible to prevent spyware from being implemented on personal computers, but with so many holes in the system it is impossible to be completely safe all the time.**

We have all heard modern-day computer lingo such as "spyware" or "hacked" or "encrypted" but are these terms of any relevant concern to the average citizen? Or are terms like this thrown around to hype-up click-bait articles and to scare the public into buying McAfee antivirus software? The spyware world may at times sound like Hollywood fiction that only a paranoid conspiracy theorist would be concerned about, but before you scoff at the tinfoil hat folks you might want to know what the company Cisco has to say about it.

Cisco, whose industry focus is on networking hardware and software, surpassed the value of Microsoft in the year 2000 [1]. So if any company would be familiar with the intricacies of computer communications and the vulnerabilities thereof, it would be Cisco. And from Cisco's very own website they talk about a term called "lawful intercept" which is a process that enables a law enforcement agency to perform electronic surveillance on an individual [2]. In the same article Cisco goes on to boast that one of the benefits of lawful intercept is that it "cannot be detected by the target" [2]. This proves that electronic snooping is possible. But it beckons the question as to whether these communication intercept capabilities are exclusive to Cisco and law enforcement or if a more savvy tech person could likewise intercept your electronic communications. This paper aims to explain what exactly spyware is, spyware tools and what

preventative measures people can take to make their communications more secure.

WHAT IS SPYWARE

According to Avast a Cyber security company with 435 million active users in an article What is Spyware? States that “Spyware is a form of malware that keeps itself hidden while secretly recording and tracking your activity on a computer or mobile device. It can monitor and copy everything you enter, upload, download, and store. Some spyware even have the capability to turn on microphones and cameras without the user even knowing” [3]. Spyware allows opponents to use data collected to hold ransoms, collect sensitive user data to sell and can be hard to detect, which we will discuss more about later on.

Spyware is a very broad topic and is not easily defined. However, an article by Norton indicates that spyware is classified as any type of malicious software that can be installed on a person’s personal devices. It can be software or hardware and can easily gain access to an unwitting victim’s personal information. After gaining access to this information, it can be held for ransom or it can immediately be transferred to other parties with malicious intentions. Spyware has progressed such that it can now have an effect on all kinds of operating systems and devices. It is no longer just restricted to Windows or devices that run by using Microsoft Windows. There are several common ways with which attackers can convince innocent users to accidentally place spyware on their devices. Some of these ways include, opening pop-ups, downloading software from an unreliable source, pirating media, etc.

The way that most opponents get Spyware onto a device is typically through a backdoor. Now according to Malwarebytes a cyber security company that provides cybersecurity products for all businesses in their article What is a backdoor? They state that a “backdoor refers to any method by which a user is able to get around normal security measures and gain high level user access on a computer system, network, or software application.” Once an opponent has breached through a backdoor they use their spyware to track and collect data on the user's compromised systems.

Malwarebytes is a cybersecurity company that provides cybersecurity products for all businesses. Malwarebytes is at home, in the home, on-the-go, and in the corporate conference room. Made for individuals, public organizations, private entities, and everything in between.

A backdoor is a malware type that allows an attacker to bypass normal authentication procedures. It is often used when an attacker needs a way to re-access a system that has already been compromised. Imperva claims that backdoor installation can happen when a vulnerable component in a web application is taken advantage of and exploited. This kind of attack allows the perpetrators to remotely impact a person’s device by giving them access to their files and other personal information. These backdoors can be used to commit data theft, deface websites, hijack servers, and overall make a system run horribly. A Trojan horse is a type of backdoor and can be used to repeatedly control a system in a negative manner from a remote location for as long as the owner/user does not know their system has been compromised. They are incredibly difficult to find and handle once they are placed and utilized.

Spyware can work from within or without routers. A router can be compromised in any number of ways and these many ways can be physical or remote. In other words, a router can be attacked by an individual physically changing it, or by an attacker who lives far away and is attacking the router through its firmware, even if that firmware is updated and strong. A router can receive a virus if malware is able to make it through the router’s initial login checkpoint in order to then modify the router’s settings. Once these settings are changed to give the malware more access, the router’s firmware can be bypassed and then the software can be attacked. Avast claims that a router can be attacked by malicious malware capable of changing the DNS

settings of the router, committing phishing attacks, as well as Trojan attacks. Wifi routers can also get viruses and these viruses are especially dangerous. These viruses, once they gain access to your router, can easily spread to any device connected to that router or network. This is because the router acts as a bridge between your device/s and the internet. If that bridge is compromised, both sides can be attacked and taken advantage of. Modems can also get viruses. Modems can be infected by malicious malware the same way that routers can.

To check if a router is infected, one can compare their router's performance with common router virus symptoms. These symptoms include crashing apps and programs, slow or spotty internet, passwords that no longer work, slow computers or devices in general, fake virus messages or pop-ups, and many other potential symptoms. Malware attacks routers, modems, and devices in a very large number of ways. These ways are advancing as the technology behind our devices is progressing. You can also check if your router has been attacked by looking up the recent IP addresses on your network. If there are any you don't recognize, that could be a sign that your router has been made vulnerable.

HARDWARE

Spyware can work from within or without routers. A router can be compromised in any number of ways and these many ways can be physical or remote. In other words, a router can be attacked by an individual physically changing it, or by an attacker who lives far away and is attacking the router through its firmware, even if that firmware is updated and strong. A router can receive a virus if malware is able to make it through the router's initial login checkpoint in order to then modify the router's settings. Once these settings are changed to give the malware more access, the router's firmware can be bypassed and then the software can be attacked. Avast claims that a router can be attacked by malicious malware capable of changing the DNS settings of the router, committing phishing attacks, as well as Trojan attacks. Wifi routers can also get viruses and these viruses are especially dangerous. These viruses, once they gain access to your router, can easily spread to any device connected to that router or network. This is because the router acts as a bridge between your device/s and the internet. If that bridge is compromised, both sides can be attacked and taken advantage of. Modems can also get viruses. Modems can be infected by malicious malware the same way that routers can.

To check if a router is infected, one can compare their router's performance with common router virus symptoms. These symptoms include crashing apps and programs, slow or spotty internet, passwords that no longer work, slow computers or devices in general, fake virus messages or pop-ups, and many other potential symptoms. Malware attacks routers, modems, and devices in a very large number of ways. These ways are advancing as the technology behind our devices is progressing. You can also check if your router has been attacked by looking up the recent IP addresses on your network. If there are any you don't recognize, that could be a sign that your router has been made vulnerable.

Spyware can also take the form of a virtual implementation such as cookies, trojan attacks, or keylogging software. As such, this can be much harder to detect and easier to install within a target system.

The simpler a system is, the more likely it is to be taken advantage of. Spyware takes advantage of peoples' comfort and trust whenever they click on a link or ad that is not trustworthy. Spyware also takes advantage of the most common keystrokes a user makes while typing in their personal information. This makes it possible for an attacker to log down your email or card info from input information. Spyware is also capable of exploiting built-in cameras on laptops and smaller devices.

The main reason so many people are victimized through spyware is because it is meant to be discrete, so that it can harvest data for as long as possible. Spyware is also hard to detect because there is usually no indication that it is even there to begin with. Good spyware does not

cause computer glitches, warnings, or errors, and so a user may never even know that they are being exploited. A user must know what to look for in order to effectively stop spyware from monitoring them. A person may never know that their personal information is out there and being used illegally until their bank informs them of a suspicious transaction or attempted transaction. The best way to avoid accidental spyware installation is to be sure to only interact with credible sources.

At its very worst, spyware can be used to harvest peoples' personal information and then that information is relayed back to whoever is in control of said spyware. The information could then be sold to a third party to do with as they please. This can happen in any number of ways and can be different for each organization or attacker. The information can be transferred to a remote server somewhere else in the world immediately after it is collected, or it can be transferred back to its progenitor through a simple email. Every situation is different, but what matters is that the information is being spread for malevolent reasons. This is often what happens in illegal spyware cases.

UTILIZATION

Spyware can be used by people and opponents. Not all opponents use spyware though so we will first break down the different types of opponents. Now according to a writer named GreyHat4Life on Cybrary, a leading cybersecurity professional development platform in their article 7 Types of Hackers you Should Know, they explain that there are 7 different types of opponents and they can be broken up into Black Hats, White Hats, Script Kiddies, Gray Hats, Green Hats, Red Hats and Blue Hats. Now a Black Hat is your typical cybercriminal. They typically target weak security systems of companies and banks to try and steal sensible information or money. This group of opponents are the ones that create malware that gains unauthorized access to targeted devices. Some Black Hats are in organized criminal groups or foreign governments to use espionage, but most Black Hats hack for the profits. White Hats are the opposite of Black Hats and hone their skills in hacking to better the cyber security scene. White Hats are often called "Ethical Hackers" because they help companies by testing security defenses and help find viruses to remove from their security systems. White hats typically have some sort of college degree in the computer science field. Next, is the Script Kiddies and they are named this because they have no experience or desire to learn programming and have little to no IT knowledge, but use security tools already online to execute cyber-attacks. Blue Hats are just the same as a Script Kiddie but seek vengeance instead. Green Hats are the opposite of a Script Kiddie. They may be new to the hacking world but they try and master the skills of hacking. Now Gray Hats are the opponents in the middle of White and Black hats. They use their hacking skills to penetrate security systems but not maliciously. They discover vulnerabilities in systems without being authorized but report the problems to the owner with usually a small fee for their findings. If the owner does not comply with the Gray Hats they expose their vulnerabilities to the internet. Lastly, Red Hats work alongside White Hats in protecting cyber security systems but in a different way. The Red Hats go after Black Hats to try and expose their identity and crimes [4].

Now, Balck Hats are the opponents that typically use spyware to monitor and capture a user's computer activity and store the information for third parties to buy and use. These opponents use delivery vectors like drive-by downloads, continual prompting and chained installs to get spyware onto a target's computer according to Eric Chein, a member of Symantec corporation in his paper Techniques of Adware and Spyware. Drive by downloading is a technique used by cyber criminals which gives a prompt to a user to install a program just by simply browsing the web. Sometimes drive-by downloads are even able to be downloaded without the user even knowing. Continual prompting is another technique used by cyber Black Hat opponents which essentially keeps giving a user a prompt to

download a hidden malicious program. The prompt to download will continue to pop up until the user finally caves in to download it. The last technique we will talk about is chained installs which is when spyware is bundled with third party software. A user could unwillingly or not even know that they downloaded spyware onto their computer through software downloads [5]. These techniques are used to get their spyware onto a target's system. Once on the system the spyware is able to silently monitor and transfer data to the opponent. They use this data for many things like sell it to third party companies, blackmail or even worse espionage for political figures. That is why it's important to always know if a piece of downloaded software is safe and trusted. So make sure to do some research before downloading any software.

The common user uses spyware using cookies. Now cookies aren't technically a form of spyware because the user has the knowledge and capabilities to delete them, but cookies act just like spyware by storing data for a website for the next time you visit. According to an Employee at Norton Security, an antivirus software company that supports millions of systems world wide in an Article What are cookies? The use of cookies is to help websites keep track of your activity on that webpage. Cookies have many different functionalities from storing items in a user's shopping cart, storing usernames and passwords, and to keep track of what you have recently bought or looked at to give suggestions suited to you [6]. Just remember that you can always delete your cookies if you don't want a website to have information on you. Now White Hats and maybe Some Red Hats were able to use their knowledge in spyware to find breakthroughs in missing person cases in Australia according to an article by a cybersecurity journalist WAQAS Authorities use hackers to find missing persons on Hackread.com. This Hackathon event was the first event ever geared towards finding missing persons. In 2019 over 300+ White Hats and investigators teamed up and had success finding leads on 12 missing person cases. This event was a clear representation on how spyware can be used for good.

PREVENTATIVE MEASURES

Knowing all the potential opponents that would be interested in accessing your network, it would be beneficial to discuss some preventative measures to prevent access to your information, such as encryption. As defined by Kevin Stine and Quynh Dang, members of the National Institute of Standards and Technology: encryption is a security control used primarily to provide confidentiality protection for data. It is a mathematical transformation to scramble data (plaintext) into a form not easily understood by unauthorized people or machines (ciphertext). After being transformed into ciphertext, the plaintext appears random and does not reveal anything about the content of the original data. Once encrypted, only someone with the decryption will be able to access the data. [7]. There are many different techniques for encryption, and many times these processes can be combined to create even higher levels of protection. For now, we will discuss the three most utilized encryption processes.

The RSA cryptosystem was created in 1997 by professional cryptographers Ron Rivest, Adi Shamir, and Leonard Adleman and has since become the most used encryption algorithm in the world [8]. The RSA allows an inverse function for public encryption and decryption, depending on whether the encryption key was public and the decryption key was private or vice versa. The formula for the encryption/decryption process is as follows using the following variables:

- *m*—The decrypted message.
- *c*—The cypher.
- *N*—Product of two prime numbers whose length is half of N.
- *e*—A small variable that is greater than 2.
- *d*—The inverse of e modΦ.
- Φ—Used in the Euler method to represent an unknown constant.

And these are the formulas:

$$c = m^{e} m\Phi dN \quad (1)$$

$$m = c^{d} m\Phi dN \quad (2)$$

The public encryption key is generated with eN, while the private key is created with d. You could use a random number generator to create Φ, however these could create a vulnerability in your cryptosystem if the generator has a backdoor [9]. While it is dependable, the RSA is one thousand times slower than symmetric cryptography, thus it is primarily used in hybrid cryptosystems and in web browsers. The second process we will discuss is the Advanced Encryption Standard, or AES encryption, that was established by the National Institute of Standards and Technology in 2001. It is a variant of the Rinjndael block cipher which has different key and block sizes. The AES selects three block sizes with corresponding keys that are 128, 192, and 256 bits long. Unlike the RSA which creates a key pair with a private and public key, the AES is a symmetric-key algorithm that allows the same key to be used when encrypting or decrypting [10]. The last process we will cover is Elliptic-curve cryptography (EEC) that was created by Levichin Prize winners Victor Miller and Neal Koblitz in 1985, and has since become the leading process used in security protocols worldwide. The EEC creates an elliptic curve used to generate a random nonce, g, which becomes the perfect private number for encryption and can be used to replace Φ for RSA encryption or any other cryptosystems, and allows smaller keys to provide equivalent security [11]. The EEC is considered mathematically more efficient and it is nearly impossible to reverse this process to determine g, making it perfect for symmetric encryption schemes and integer factorization algorithms [12].

Some users may wonder why encryption is considered a vital process, when it seems only users who have mal-intent would have something to hide. Encryption helps ensure a user's privacy for anything from business files to emails. RSI Security, experts of data security consulting and providers of reliable, flexible, and scalable cybersecurity resources, explains two reasons why any user or company should have reliable encryption. The first reason is regarding information in transit. “Signs of email hacking are difficult to detect and virtually non-existent. Unlike typical systems based on-premise or in the cloud which are constantly monitored for signs of hacking, the same efforts are difficult to achieve with email data in transit” [13]. For this reason, many companies utilize email encryption so in the event an opponent does acquire the message, they won't have the requisite private or public keys to access the data within the email.

The second reason to utilize encryption is to protect against potential threats from opponents who would target emails as an access point into a network. RSI explains the three main techniques to do this are spamming, phishing, and viruses. Spamming “goes far beyond receiving emails that you have little interest in. Spam emails, if improperly opened, handled, or clicked, can result in serious damage to business and technology systems, and can result in losing sensitive or confidential information” [13]. Spam emails invite another type of threat to a system, malicious malware implemented through email attachments such as pictures or links. If the user were to download the file, a malware program is then installed, the opponent can now spy on or extract information about the user. Phishing is “any fraudulent attempt to obtain confidential or sensitive information. This can include usernames, passwords, credit card details, and even direct access to money” [13]. Phishing is often done through emails that look secure, however some key elements to a phishing email are suspicious links and generic usernames such as “Representative Desk of US Bank”. It is recommended that in the event that a phishing email is received, or an email is suspected of being a phishing scam, the recipient should delete the email without opening any attachments. The largest threat, and arguably the most damaging, are viruses. Opponents can use

viruses for several reasons, “such as network or service disruption, harvesting confidential information, or spying on a network. Computer viruses sent via email, just as in nature, are designed to replicate and spread to other hosts as quickly as possible” [13].

FIREWALLS

The most common use for encryption is to protect users and their information as they connect to outside resources through the network firewall. A firewall is a security protocol within a computer's hardware or software to protect the device by filtering traffic and blocking unauthorized users from gaining access to private data within the network, and preventing malicious software from entering the system. Every computer or system currently active will have one or more firewalls implemented to provide protection as the user interacts with open sites or systems that may be compromised. That being said, because they are so prominent, many opponents have made it their goal to find vulnerabilities within firewalls or create software to get through them.

The most common vulnerability exploited by opponents are misconfigurations within a firewall. Explained by Guardicore, a prominent innovator in data center and cloud security, misconfigurations are the most prominent reason opponents can infiltrate a system. For individuals, network firewalls are updated inconsistently to meet the new complex and dynamic environments and applications. Due to this, firewall policy is often behind the current status of many applications and data, increasing the risk of unauthorized access until the rules are manually set. For company systems, these businesses must comply with mandates and governance set for cloud environments. The increased agility of hybrid cloud ecosystems is helpful for streamlining business processes but causes many organizations to fall short of compliance requirements [14]. When implementing a firewall or updating the permissions and security measures, there are common misconfigurations that are seen for individuals and corporations alike. EC2 and VPC errors are considered the most common misconfigurations. EC2 instances are security groups that have been configured incorrectly within a virtual machine or server, while VPC access configures the rules to allow or deny connections to or from the network. A mistake here can lead to blind spots within firewall security or unauthorized IP addresses gaining access to the network. Service Permission errors and Inconsistent Authentication are another set of misconfigurations that are commonly seen. Service permissions are set on applications and software that are implemented in a device or network, and typically have permissions set during their installation. During this process, some services are given access to go through the firewall while in use, and if this process is left running unchecked it has the potential to become an access point into the network. Inconsistent Authentication on the other hand is created when companies have networks across multiple locations and environments. If some authentication requirements are weaker than others, this creates a misalignment within security that can be leveraged for access into the network [14].

While a properly configured firewall will protect against most threats, a determined opponent can still find other access points. Four other root causes of firewall breaches have been outlined by Firemon, an enterprise security management company that helps organizations find, correct, and avoid gaps in their existing network security infrastructure. Not all firewalls are created equal and some may be designed for a more relaxed environment, leading to overly permissive rules which contain large network object ranges or the term“any” within the rule statements. Broad terminology like this can become an open door to allow access for unwanted operators. A set of vulnerabilities that go hand in hand are inadvertent access and known but unpatched vulnerabilities. Inadvertent access is created when a resource is decommissioned, but its associated rules were not removed from the policy regulating its access. This allows any old IP address to be reused and allows opponents to gain entry to the network. In a similar fashion, known but unpatched vulnerabilities within a

network can provide unauthorized or unexpected access. While not done intentionally, any known vulnerability should be fixed immediately rather than putting off the patch until a later date, as this extends the risk of an opponent taking notice and entering the network. Shadowed rules are another cause for concern, as these are considered “a gift to opponents”. Rules become shadowed when one rule contradicts another, thus rendering both obsolete and creating a gap within the firewall for an opponent to enter through.

While reading the list of potential vulnerabilities that can be exploited within a firewall, I would like to remind the reader that all these risks are avoidable and manageable with the proper implementation and consistent monitoring to catch any irregularities or vulnerabilities that can develop later on. Security teams can be hired to monitor the firewall or some systems can be automated to maintain themselves. Individuals and companies are encouraged to maintain their firewalls and if so inclined to get more than one and compound the accumulated protection.

CONCLUSION

It is plainly obvious that spyware and snooping on personal computers is part of our reality. And unless people revert back to internetless computing, it will remain a very real concern. While encrypting is a useful tool that may prevent the average snooper from reading your message, keep in mind that Cisco has lawful intercept that is designed to be undetectable by the user. Likewise, firewalls act as safeguards or bumper lanes to keep you protected and it will not always be perfectly protective since there are so many new and evolving ways to gain access to your computer. As people engage in the ancient cat and mouse game of sending encoded messages perhaps the best thing to remember is that someone is always watching.

ACKNOWLEDGMENT

We thank the illustrious UWRF for being such a hospital school. A special thank you is owed to Dr. Jacob Hendricks for being such an effective, supportive guide and tutor not just for this course but throughout our academic career. And of course we would like to thank our fellow classmates. Not just for reviewing our paper and giving us thoughtful insight, but also for being there and enduring with us.

REFERENCES

1. “Cisco,” Wikipedia, 18-Apr-2022. [Online]. Available: https://en.wikipedia.org/wiki/Cisco. [Accessed: 22-Apr-2022].
2. “Lawful intercept overview,” Cisco, 21-Mar-2015. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/routers/10000/10008/feature/guides/lawful_intercept/10Llovr.html. [Accessed: 22-Apr-2022].
3. P. Seguin, “What Is Spyware, Who Can Be Attacked, and How to Prevent It,” What is spyware, who can be attacked, and how to prevent it, 20-Feb-2020. [Online]. Available: https://www.avast.com/c-spyware. [Accessed: 20-Apr-2022]. [What is Spyware?: What is Spyware? | Spyware Definition | Avast]
4. G. H. L. GrayHat4Life, “7 Types of Hackers You Should Know,” Cybrary, 23-Nov-2020. [Online]. Available: https://www.cybrary.it/blog/0p3n/types-of-hackers/#:~:text= 7 Types of Hackers You Should Know,who lack programming knowledge and IT... More. [Accessed: 20-Apr-2022]. [7 Types of Hackers You Should Know | Cybrary]
5. E. Chien, “Techniques of Adware and Spyware,” Virus Bulletin. [Online]. Available: https://www.virusbulletin.com/conference/vb2005/abstracts/techniques-adware-and-spyware/. [Accessed: 22-Apr-2022].
6. “What Are Cookies?,” Norton, 07-Jul-2021. [Online]. Available: https://us.norton.com/internetsecurity-how-to-what-are-cookies.html. [Accessed: 22-Apr-2022].
7. K. Stine and Q. Dang, “Encryption Basics,” Journal of AHIMA. [Online]. Available: https://library.ahima.org/doc?oid=104090#.Yik48YnMLMY. [Accessed: 20-Apr-2022]. [Encryption Basics (ahima.org)]
8. “RSA (cryptosystem),” Wikipedia, 08-Apr-2022. [Online]. Available: https://en.wikipedia.org/wiki/RSA_(cryptosystem). [Accessed: 20-Apr-2022]. [RSA (cryptosystem) - Wikipedia]
9. A. Vance, “How the RSA Algorithm Works, Including How to Select d, e, n, p, q, and ϕ (phi),” YouTube, 14-Oct-2014. [Online]. Available: https://www.youtube.com/watch?v=Z8M2BTscoD4&t. [Accessed: 20-Apr-2022]. [How the RSA algorithm

works, including how to select d, e, n, p, q, and ϕ (phi) - YouTube]
10. "Advanced Encryption Standard," Wikipedia, 06-Apr-2022. [Online]. Available: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard. [Accessed: 20-Apr-2022]. [Advanced Encryption Standard - Wikipedia]
11. M. Pound, "Elliptic Curves - Computerphile," Youtube, 16-Jan-2018. [Online]. Available: https://www.youtube.com/watch?v=NF1pwjL9-DE. [Accessed: 21-Apr-2022]. [https://www.youtube.com/watch?v=NF1pwjL9-DE&feature=emb_logo]
12. "Elliptic-curve Cryptography," Wikipedia, 10-Apr-2022. [Online].Available: https://en.wikipedia.org/wiki/Elliptic-curve_cryptography. [Accessed: 20-Apr-2022]. [Elliptic-curve cryptography - Wikipedia]
13. "5 things you need to know about how email encryption works," RSI Security, 26-Oct-2018. [Online]. Available: https://blog.rsisecurity.com/5-things-you-need-to-know-about-how-email-encryption-works/#:~:text=In today's world%2C email encryption functions on the, Public Key to encrypt the message before sending. [Accessed: 20-Apr-2022]. [What is Spyware?: 5 things you need to know about how email encryption works (rsisecurity.com)]
14. D. Burton, "The Dangers of Firewall Misconfigurations," Guardicore, 05-Apr-2022. [Online]. Available: https://www.guardicore.com/blog/the-dangers-of-firewall-misconfigurations-and-how-to-avoid-them/. [Accessed: 20-Apr-2022]. [The dangers of firewall misconfigurations | Guardicore]

Jacob Biedrzycki is finally finishing up his 10-year degree from UWRF after turning in this paper. Contact him at Jacob.Biedrzycki@my.uwrf.edu.

Alexa Lamberty is finishing up her 4-year degree from UWRF. Contact her at Alexa.Lamberty@my.uwrf.edu.

Max Olive is finishing up his 4-year degree from UWRF. He also is an accomplished powerlifter who has never missed leg day. Contact him at Maxwell.Olive@my.uwrf.edu.

Alia Oradeiecond B. Author, Jr., is finishing up her 4-year degree from UWRF. Contact her at Alia.Oradei@my.uwrf.edu.