Final Paper: Red Panda

Ogadimma Chibuike

Department of Cybersecurity

CYSE 494: Entreprenuership in Cybersecurity

Dr. Akeyla Porcher

June 17, 2023

Introduction

There is new technology and systems being created every day to help people get through day-to-day tasks. With the rapid advancement of technology, also comes the creation of different methods used to exploit and hack into this technology. User interfaces are created to make things easier for users. But sometimes, the design choices that make things comfortable for users can also make it easier for attackers to sneak in malware without being detected (Witte, 2020). Phishing and typosquatting are two sneaky tricks that cybercriminals use to trick people online. Phishing is when scammers pose as legitimate companies, such as banks or email providers, to deceive you into giving them your personal information, including passwords and credit card details.

Typosquatting, on the other hand, takes advantage of common spelling mistakes people make when typing website addresses. These scammers create fake websites that look just like the real ones, and when you accidentally type the wrong address, they try to steal your information or infect your computer with malware. Both mismatched file extensions and malicious links are examples of social engineering attempts. Social engineering involves manipulating and influencing people online to engage in unsafe actions (Williams et al., 2017). For instance, it could include enticing people to open email attachments that contain harmful software or tricking them into revealing sensitive information like usernames and passwords. These deceptive tactics aim to exploit human vulnerabilities and persuade people to unknowingly put their security at risk. It's important to be aware of these tactics and stay cautious to protect yourself from falling into their traps.

Mismatched file extensions pose a significant problem as they can deceive users into thinking a file is safe when, in fact, it contains malicious content. By disguising a harmful file

with a different extension, cybercriminals can trick users into downloading and opening files that can lead to malware infections, data breaches, or other cyber-attacks. These files may appear harmless at first glance, but they can execute malicious code that compromises the security and integrity of a user's system. Correspondingly, malicious links pose a serious threat to online security. Cybercriminals often use techniques such as phishing to trick users into clicking on deceptive links that appear legitimate. These malicious links can redirect users to fake websites that mimic trusted platforms, aiming to steal sensitive information like usernames, passwords, or financial details. Clicking on such links can lead to identity theft, financial losses, or unauthorized access to personal or corporate accounts. Both mismatched file extensions and malicious links exploit users' trust and their tendency to rely on visual cues when evaluating the safety of files or links. The deceptive nature of these elements makes them particularly dangerous, as they can easily bypass traditional security measures and exploit vulnerabilities in users' behavior. To mitigate these risks, it is crucial to raise awareness among users about the dangers of mismatched file extensions and malicious links. Implementing robust security measures, such as scanning and analyzing files and links for potential threats, is essential in detecting and preventing such attacks. Developing proactive solutions, like the browser extension you have created, that can identify and alert users about mismatched file extensions and malicious links can significantly enhance online security and protect users from falling victim to these types of cyber threats.

My team and I have created a web browser extension software named Red Panda Security. This browser extension is created to scan mismatched file extensions and links for abnormalities and protect users from falling victim to malware.

When developing a browser extension that scans for mismatched file extensions, there are several potential barriers to consider. First, there may be technical limitations imposed by the browser's extension API, which could restrict the access to certain information or system resources, affecting the effectiveness of the scanning capabilities. Privacy concerns are also important to address, as scanning and analyzing URLs and downloaded files may raise privacy issues among users. It's crucial to handle user data securely and transparently, following privacy regulations and implementing strong data protection measures. Additionally, developing an accurate algorithm for detecting mismatched file extensions can be challenging, with the risk of false positives (flagging legitimate files incorrectly) and false negatives (failing to detect potentially harmful files). The real-time scanning process can also impact browser performance, potentially slowing down the browsing experience or straining system resources. Lastly, ensuring compatibility across different browsers may require additional development efforts, as each browser has its own extension API and feature support. By addressing these barriers effectively, your browser extension can overcome challenges and provide a valuable solution for users.

In 2023, we have increased the use of technology in our day-to-day lives, giving bad actors more opportunities to be able to exploit and steal from innocent people without leaving the comfort of their own homes. In the past, thieves would break into houses when people were busy watching their favorite TV shows. These incidents happened in the physical world, and it was thought that the online world would be immune to such crimes. Unfortunately, that's not the case. Experienced hackers can infiltrate a computer system while someone is engrossed in watching a video file. Many computer users enjoy watching videos, whether they are casual users or individuals working with critical systems like banking, defense, nuclear power plants, or space

agencies. Unfortunately, playing a video file can lead to a serious security risk in the cyber world as well (Nath and Mehtre, 2015).

To understand this issue first, we must define a malicious link and understand how it is implemented. A malicious link is a web address or URL that is designed to trick people into visiting a dangerous or harmful website. These links may appear legitimate at first glance, but they are created by cybercriminals with the intention of causing harm. The characteristics of malicious links include deceptive tactics such as disguising a malware link to look like a trusted source, using enticing messages or offers to lure people into clicking on them, and leading to websites that can infect computers with viruses or steal personal information. It is important to be cautious and avoid clicking on unfamiliar or suspicious links to protect yourself from the potential risks associated with malicious links. Studies have shown that malware can come in many different forms, such as hardware, firmware, images, movies, software, and documents like Office or PDF files. Malware is basically any harmful content that is hidden within videos, audios, programs, or even physical devices. Cybercriminals use malware as a major tool to carry out various stages of their targeted attacks. (Nath and Mehtre, 2015).

The background behind malicious links lies in cybercrime and the constant evolution of hacking techniques. As the internet became more widespread and integrated into our daily lives, cybercriminals saw an opportunity to exploit vulnerabilities for personal gain. Malicious links emerged as a deceptive method to trick users into visiting websites designed to steal sensitive information, infect systems with malware, or carry out various forms of cyber-attacks. Cybercriminals employ social engineering tactics, such as phishing, to create authentic-looking links that appear trustworthy and legitimate. They often exploit human emotions and curiosity by enticing users with offers, urgent messages, or intriguing content. These malicious links are

shared through various communication channels, including emails, social media, messaging apps, and compromised websites. Over time, the techniques and sophistication of malicious links have evolved. Hackers continually adapt their strategies to bypass security measures and increase the chances of success. They exploit software vulnerabilities, use obfuscation techniques to hide the true destination of the link, and use URL shorteners to mask their intentions. The background behind malicious links is rooted in the ever-present threat landscape of the digital world. It emphasizes the importance of user awareness, security measures, and continuous efforts to combat cybercrime and protect individuals, businesses, and organizations from falling victim to these deceptive tactics.

There are many ways to carry out these malicious link attacks. Phishing attacks encompass a range of techniques, each with its own unique approach to deceiving individuals and compromising their security. One prevalent type is email phishing, where cybercriminals send deceptive emails masquerading as trustworthy sources such as banks, online services, or reputable organizations. These emails often contain malicious links or attachments designed to trick users into clicking on them, leading to the theft of sensitive information or the installation of malware. Spear phishing takes a more targeted approach, focusing on specific individuals or organizations. Attackers invest time and effort into gathering information about their targets, allowing them to personalize the phishing emails and make them appear highly credible. By including familiar names, job titles, or referencing specific events, the attackers aim to establish trust and increase the likelihood of the victim falling for the scam. Another technique is smishing, which relies on fraudulent text messages. These messages appear to be from legitimate entities and often create a sense of urgency or offer enticing deals to prompt immediate action. By tricking recipients into clicking on malicious links or disclosing personal information,

smishing attacks aim to exploit individuals' trust in SMS communication. Pharming involves manipulating the Domain Name System (DNS) or utilizing malware to redirect users to fraudulent websites. Victims are unknowingly directed to these fake sites, which mimic legitimate ones, and their personal information is collected, or malware is downloaded onto their devices. In more sophisticated attacks, whaling targets high-profile individuals, such as executives or prominent figures, with customized phishing campaigns. These attacks often aim to gain access to valuable or sensitive information, such as corporate data or financial accounts, by exploiting the individual's status or authority. Lastly, malvertising refers to the use of malicious advertisements displayed on legitimate websites. These ads can redirect unsuspecting users to websites hosting malware or prompt them to download infected files unknowingly. Each of these techniques exploits human vulnerabilities and trust, posing significant risks to individuals, businesses, and organizations. By understanding these types of phishing attacks, users can become more vigilant and employ appropriate measures to protect themselves from falling victim to such deceptive tactics.

One of the primary reasons for security breaches on our personal computers is our inherent vulnerability as humans to deception (Goel and Dincelli, 2017). Cybercriminals take advantage of this vulnerability by sending phishing emails that trick users into clicking on malicious links. These links can lead to the download of malware or deceive victims into disclosing their personal and confidential information to the hackers. This exploitation of human vulnerability through phishing emails and malicious links poses a significant problem in today's digital landscape. The widespread use of email and the internet has made it easier for cybercriminals to reach a larger audience and execute their deceptive tactics. As a result, individuals, businesses, and organizations face an increased risk of falling victim to these attacks,

leading to financial losses, identity theft, data breaches, and compromised systems. Moreover, the evolving sophistication of phishing techniques and the constant development of new malware strains make it increasingly challenging to detect and prevent these attacks. This ongoing problem highlights the urgent need for cybersecurity awareness, robust protective measures, and continuous adaptation to combat the ever-present threat of phishing and malicious links in our interconnected world.

To understand how to prevent phishing attacks using malicious links, one must understand how these links are created and made destructive. Malware is typically embedded into a malicious link through various techniques employed by cybercriminals. One common method involves using exploit kits, which are malicious software packages designed to identify vulnerabilities in a user's computer or software. When a user clicks on a malicious link, the exploit kit scans its system for any known vulnerabilities and attempts to exploit them to deliver the malware payload. Another technique utilized by cybercriminals is typosquatting, which takes advantage of human error when typing website addresses. Typosquatting (also referred to as "URL hijacking") is a technique that is based on the concept of registering domain names with typing errors and similar mistakes made by users when entering a popular web address (Dam et al., 2020). They register domain names that closely resemble popular or legitimate websites but contain slight typographical errors, such as changing a letter or adding an extra character. For example, they may register a domain as "gogle.com" instead of "google.com". Unsuspecting users who mistakenly enter the incorrect address may end up on a malicious website that appears similar to the legitimate one. Through typosquatting, cybercriminals can redirect users to websites that distribute malware. Another very similar method is called a homograph attack. The objective of this attack is to conceal the true origin of a domain by altering certain letters in the

URL. As the internet expands to encompass a global user base beyond English speakers, the threat posed by this technique will escalate, especially with the increasing use of non-Latin scripts in domain names. This presents a significant challenge as it becomes harder to identify and distinguish between legitimate and malicious websites, making users more vulnerable to falling victim to phishing and other online scams (Helou and Tilley, 2010). These malicious websites may prompt users to download a file, claiming it to be a necessary software update or a document of interest. However, the file is a malware payload that infects the user's device upon execution. Additionally, typosquatting can also be used in phishing attacks. Cybercriminals may create fake login pages that closely mimic the design and branding of popular websites. When users enter their credentials on these spoofed pages, the information is captured by the attackers, who can then use it for unauthorized access or identity theft. It's important to exercise caution when entering website addresses manually and to double-check the spelling and legitimacy of the URL. Implementing security measures such as robust antivirus software, using reputable browser extensions, and regularly updating software can also help mitigate the risks associated with typosquatting and prevent malware infections.

The presence of harmful links and downloaded files in today's digital world has serious consequences, including financial losses from fraud and identity theft, as well as disruptions to personal and organizational security. Privacy and data breaches are a major concern associated with the problem of malicious links and downloaded files. When individuals unknowingly click on malicious links or download infected files, their personal information and sensitive data are put at risk. Cybercriminals can gain unauthorized access to usernames, passwords, credit card details, social security numbers, and other confidential information. This compromised information can then be sold on the dark web or used for various malicious purposes, such as

identity theft, financial fraud, or even targeted phishing attacks. The consequences of such breaches are severe, causing significant harm to individuals and organizations alike. Victims may face financial losses, damaged reputations, and emotional distress, while businesses can suffer legal repercussions, loss of customer trust, and regulatory penalties. Financial implications resulting from fraud, identity theft, and monetary losses are significant concerns related to the problem of malicious links and downloaded files. When individuals fall victim to phishing attacks or inadvertently download malware through deceptive links, they become vulnerable to financial exploitation. Fraudulent activities, such as unauthorized access to bank accounts or credit card fraud, can lead to direct monetary losses for victims. Cybercriminals may gain access to sensitive financial information, such as credit card numbers, banking credentials, or social security numbers, which they can exploit to make unauthorized transactions or open fraudulent accounts in the victims' names. This can result in substantial financial damage, including unauthorized charges, drained bank accounts, and damaged credit histories. Identity theft is another grave concern. When personal information is compromised through malicious links or downloaded files, criminals can assume the victim's identity to commit various financial crimes. They may open new lines of credit, apply for loans, or engage in fraudulent activities, all of which can have severe financial consequences for the victim. Recovering from identity theft can be a long and costly process, involving legal fees, credit monitoring services, and efforts to repair damaged credit. Furthermore, victims of phishing attacks or malware infections may suffer indirect financial losses. Malware can infiltrate systems and compromise critical data, leading to operational disruptions, loss of productivity, and potential damage to a company's reputation. Organizations may incur substantial financial expenses to recover from such incidents, including incident response, system repairs, data recovery, and cybersecurity enhancements.

My partners and I have come up with what we think is the best solution to solve this issue. We have created a browser extension, named Red Panda Security, that scans URL and download links for mismatched file extension and malicious links. We used a deep learning algorithm to create our product. This algorithm falls under the category of unsupervised machine learning. Unlike supervised learning, it doesn't rely on pre-labeled data but instead learns from existing data on its own. It can then apply its knowledge to new data, making it highly effective in detecting newly created phishing websites. Its ability to adapt and recognize patterns in real-time makes it a powerful tool for identifying and combating emerging threats in the online world (Adebowale et al., 2020).

Our browser extension can scan for mismatched file extensions by intercepting and analyzing the URLs of downloaded files. When a user initiates a download, the browser extension can capture the URL and extract the file extension from it. Then, it can compare the extracted file extension with the actual file type of the downloaded file. If there is a mismatch between the file extension and the actual file type, the browser extension can raise an alert or provide a warning to the user. This comparison can be done by using predefined lists or databases that map file extensions to their corresponding file types. Additionally, the extension can leverage file signature analysis to verify the file's integrity and determine its true type. By implementing such checks, the browser extension can help users identify potentially malicious or misleading files that have mismatched file extensions. Our browser extension can also scan for links containing malware. First, Red Panda can check the website addresses (URLs) of the links and look for signs that indicate they might be harmful. This includes comparing them to a list of known bad links or using special algorithms to spot suspicious patterns. Second, our product can

use reputation services that keep track of dangerous websites. It can ask these services if a link is safe or if it has a bad reputation. Another approach is to follow the links and examine the web pages they lead to. By looking at the content on those pages, our product can identify signs of phishing attempts or malware. Additionally, our product can use machine learning to learn from examples of known malicious links and then use that knowledge to spot similar ones in the future. Lastly, we can let users give feedback on suspicious links they come across, helping to improve the scanning process. By combining these methods and regularly updating our product, it can become better at scanning for and identifying malicious links, ultimately keeping users safe online.

This problem is not only a concern for cybersecurity students and professionals, but pretty much anyone who uses the internet. Students and professors can fall victim to clicking a malicious link while doing research or completing an assignment. Malicious links and the product we created have connections to different areas beyond the cybersecurity field. For example, in businesses and marketing, understanding the risks of malicious links is crucial for protecting customers and maintaining a good reputation. Our, which scans links for malware, can be seen as a useful tool for businesses to enhance their online security and provide a safer experience for customers. Additionally, consumer protection is important, as everyone wants to stay safe online. Red Panda can help individuals detect and avoid harmful links, ensuring their online safety regardless of their specific field. In the technology and software development field, cybersecurity is vital, and our product contributes to creating secure software and applications. Moreover, user experience and design professionals play a role in ensuring a smooth and secure user journey. By incorporating our product into their designs, they can improve the user

experience by alerting users about potential security risks related to links. Lastly, education and awareness are essential in promoting digital literacy and cybersecurity. Red Panda can be used in educational institutions and awareness campaigns to teach students and individuals how to identify and avoid malicious links, fostering a more informed and secure online community. In short, malicious links and our product have relevance in different areas like business, marketing, consumer protection, technology, user experience, design, and education, all aimed at enhancing online security and protecting individuals and businesses from cyber threats.

To determine the effectiveness of our Red Panda Security web extension, we need to assess many key factors. First, we must consider the browser's speed and performance in loading web pages, executing JavaScript, and handling multimedia content. A fast and responsive browsing experience is crucial for user satisfaction. We can do this by running time trials to on link scans to record the amount of time each scan takes. Next, we evaluate its compatibility with modern web standards and its ability to render pages accurately across platforms and devices. Security features are also important, such as built-in protection against malware, phishing detection, and sandboxing to prevent malicious activities. Privacy controls, like blocking third-party cookies and enabling private browsing mode, are essential for safeguarding personal information. Additionally, examine the availability of customization options, an intuitive user interface, and ease of navigation. Cross-platform availability ensures flexibility, while a strong developer support system with tools and documentation indicates ongoing improvements. Considering user reviews and feedback, as well as conducting thorough testing in various scenarios, can provide valuable insights. Before releasing our web extension, we plan to release a beta version where we could have customers test out our product and we write a review after. We

can also use this beta version to run tests and fix any bugs we may find in Red Panda. After releasing, regularly comparing our browser's performance against industry benchmarks, and seeking user input can help gauge its effectiveness. By evaluating these aspects, we can determine the overall efficiency, security, and user experience of our web browser.

Our business plan outlines the key elements required to bring our product to reality. First, we must have a clear understanding of our product's purpose, features, and unique selling points. Extensive market research has been conducted to identify our target audience, competitors, and market trends. With this, we can ensure that we can convince our target audience that this product will work for them. To secure the necessary funding, we have explored various channels such as personal savings, loans, grants, and attracting investors. We plan to sell our product to customers as a free product that operates on a trial basis. We will require all users to create an account, but not require payment details upfront. The software will continue working after the free trial is over and will only be required to pay to remove free trial notification pop-up. This works as a business model for local software that’s doesn’t require much infrastructure to run. The main idea of it is that businesses will be required to pay for the licenses which, will support the company while getting familiarity from the average consumer because it’s essentially free. Intellectual property protection is a priority, and we will file for patents and trademarks to safeguard our innovative ideas. A comprehensive marketing strategy has been devised, utilizing digital marketing techniques, social media platforms, and targeted advertising to create awareness and generate interest. A successful product launch will be backed by a well-structured plan, creating a buzz, and attracting early adopters. We are committed to gathering user feedback and iterating on our product to continuously improve its features and user experience. Scalability and growth are key considerations, with a plan in place to handle increasing user demand.

Providing excellent customer support channels and maintaining high levels of customer satisfaction are central to our long-term success. Our business plan encompasses all these elements, ensuring a solid foundation for bringing our product to reality and achieving market success.

From this project, I have learned several valuable lessons. First, I have gained a deeper understanding of the importance of cybersecurity and the threats posed by malicious links and mismatched file extensions. I have realized the need for proactive measures to protect users from falling victim to phishing attacks and malware infections. Additionally, I have acquired knowledge about different techniques and approaches that can be employed to detect and mitigate these risks effectively. This project has also highlighted the significance of user education and awareness in promoting safe online practices. Finally, I have gained practical experience in developing a web extension and implementing scanning functionalities, which has enhanced my technical skills in the field of cybersecurity. Overall, this project has provided valuable insights into the complex nature of cybersecurity challenges, and the importance of developing innovative solutions to address them. Looking back at this project, there are a few things I would have done differently. First, I should have spent more time researching existing solutions and technologies related to scanning for mismatched file extensions and detecting malicious links. This would have given me a better understanding of this subject. It also would have provided me with a stronger starting point and allowed me to include more advanced features in my web extension. I also should have asked for more feedback from group members. This would have helped me create a better business plan. It would have been helpful to get advice and input from cybersecurity experts too, to make sure the extension was effective and

accurate. By continuously improving the extension, I could have provided users with a better tool to protect against harmful links and file extensions that don't match.

Reference:

Adebowale, M. A., Lwin, K. T., & Hossain, M. A. (2020). Intelligent phishing detection scheme using Deep Learning Algorithms. *Journal of Enterprise Information Management, 36*(3), 747–766. https://doi.org/10.1108/jeim-01-2020-0036

Al Helou, J., & Tilley, S. (2010). Multilingual web sites: Internationalized domain name homograph attacks. 2010 12th IEEE International Symposium on Web Systems Evolution (WSE). https://doi.org/10.1109/wse.2010.5623562

Dam, T., Klausner, L. D., & Schrittwieser, S. (2020). Typosquatting for Fun and Profit: Cross-Country Analysis of Pop-Up Scam. Cornell University Library, arXiv.org. https://doi.org/10.13052/jcsm2245-1439.924

Goel, S., Williams, K., & Dincelli, E. (2017). Got Phished? internet Security and Human Vulnerability. *Journal of the Association for Information Systems, 18*(1), 22-44. http://proxy.lib.odu.edu/login?url=https://www.proquest.com/scholarly-journals/got-phished-internet-security-human-vulnerability/docview/1870606552/se-2

Nath, H. V., & Mehtre, B. M. (2015). Analysis of a multistage attack embedded in a video file. *Information Systems Frontiers, 17*(5), 1029-1037. https://doi.org/10.1007/s10796-015-9570-5

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior, 72*, 412–421. https://doi.org/10.1016/j.chb.2017.03.002

Witte, T. N. (2020). Phantom Malware: Conceal Malicious Actions From Malware Detection Techniques by Imitating User Activity. *IEEE Xplore*, *8*. https://doi.org/10.1109/ACCESS.2020.3021743