iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52927

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Review of Malware and Phishing in the Current and Next Generation of the Internet

Tanmay Chandel
Amity University, Uttar Pradesh

Abstract: ***The advent of Web 2.0 and Web 3.0 technologies has created new opportunities for cybercriminals to launch malware and phishing attacks. This review paper aims to provide an overview of the current state of these types of attacks in Web 2.0 and Web 3.0 environments, as well as the tools and strategies that can be used to prevent them. The paper begins by defining malware and phishing and describing the basic methods used to execute these attacks. It then delves into the specific characteristics of Web 2.0 and Web 3.0 environments that make them vulnerable to these types of attacks. For example, the ability to share information and collaborate in real time in Web 2.0 environments can create opportunities for cybercriminals to exploit trust relationships and launch phishing attacks. In Web 3.0 environments, the use of blockchain and decentralized technologies introduces new challenges for preventing malware and phishing attacks.***

The paper discusses the the functioning and the procedures which are followed in the event of a malware attack or phishing attack in unison with social engineering and also takes a look at a case study of a real life phishing attack in web 3.0. The paper concludes by outlining some of the key tools and strategies that can be used to prevent malware and phishing attacks in Web 2.0 and Web 3.0 environments. These include technical measures such as anti-malware software, firewalls, and spam filters, as well as user education and training to recognize and avoid phishing attacks. Overall, the paper provides a comprehensive overview of the current state of malware and phishing attacks in Web 2.0 and Web 3.0 environments, as well as the strategies and tools that can be used to prevent them. As the use of these technologies continues to grow, it is essential that individuals and organizations take steps to protect themselves against these types of cyber attacks.

I. INTRODUCTION

The evolution of the internet has brought about many advances in technology and communication, but it has also created new opportunities for cybercriminals to launch attacks on individuals and organizations. Malware and phishing are two of the most common types of cyber-attacks, and they have become increasingly prevalent in recent years. With the emergence of Web 2.0 and Web 3.0 technologies, these types of attacks have become even more sophisticated and difficult to prevent.

Malware is any software that is intended to harm or steal information from computer systems. Malware pertains to a wide range of programs, including trojans, viruses, ransomware, and spyware. They can be spread via attachments in emails, downloaded files, and corrupted USB drives, among other methods. Once installed on a computer, malware can cause significant damage, such as stealing personal information or rendering the computer unusable.

Phishing, meanwhile, is a type of cyber-attack that includes convincing people into disclosing sensitive information including usernames, passwords, and financial data. Phishing attacks often involve sending out of fake emails alleging to be from a genuine source, such as a bank or an online merchant. These emails may contain links to fake websites that ask for personal information, or they may contain attachments that install malware on the recipient's computer.

Web 2.0 and Web 3.0 technologies have created new opportunities for cybercriminals to launch malware and phishing attacks. Web 2.0 technologies, such as social media platforms and cloud computing, have made it easier for individuals and organizations to share information and collaborate in real time. However, these technologies have also created new opportunities for cybercriminals to exploit trust relationships and launch phishing attacks.

Web 3.0 technologies, such as blockchain and decentralized networks, have the potential to revolutionize the way we store and share information. These technologies offer benefits such as tamper-proof records and the ability to enforce smart contracts. However, they also present new challenges for preventing malware and phishing attacks. Decentralized networks, for example, may not have the same level of security measures as centralized networks, putting them at risk of attacks.

As the usage of Web 2.0 and Web 3.0 technologies grows, it is critical that people and organisations take precautions against malware and phishing scams. This review article seeks to offer an overview of the present state of these sorts of attacks in Web 2.0 and Web 3.0 settings, as well as tools and tactics for preventing them.

The paper will begin by defining malware and phishing and describing the basic methods used to execute these attacks. It will then delve into the specific characteristics of Web 2.0 and Web 3.0 environments that make them vulnerable to these types of attacks. For example, the ability to share information and collaborate in real time in Web 2.0 environments can create opportunities for cybercriminals to exploit trust relationships and launch phishing attacks.

In Web 3.0 environments, the use of blockchain and decentralized technologies introduces new challenges for preventing malware and phishing attacks. The paper will discuss the potential benefits of these technologies for security, such as the ability to create tamper-proof records and enforce smart contracts but will also highlight the need for new tools and strategies to protect against attacks on these technologies.

The paper will conclude by outlining some of the key tools and strategies that can be used to prevent malware and phishing attacks in Web 2.0 and Web 3.0 environments. These will include technical measures such as anti-malware software, firewalls, and spam filters, as well as user education and training to recognize and avoid phishing attacks. It will also study real life case of an individual who has been a victim to such crimes.

Overall, this review paper will provide a detailed assessment of the present state of malware and phishing attacks in today's cyber security world.

Phishing and malware are two forms of popular cyber-attacks that can cause considerable harm to persons and organisations. Phishing attacks entail misleading people into disclosing sensitive information, whereas malware is any software designed to disrupt computer systems and steal information. These kinds of attacks can take multiple forms, including email phishing, compromised downloaded files, and hard drives.

The targets of phishing and malware attacks can vary widely, from individuals to large corporations. Attackers may be motivated by financial gain, political motivations, or simply a desire to cause chaos. Regardless of the motivation, the damage caused by these attacks can be significant, including stolen personal information, financial losses, and system damage.

To prevent these types of attacks, there are various tools and strategies that can be used. Technical measures, such as anti-malware software, firewalls, and spam filters, can help detect and prevent these attacks. User education and training is also essential to recognize and avoid phishing attacks, such as avoiding suspicious links or attachments and verifying the authenticity of emails and websites.

Individuals and organisations must understand the fundamentals of phishing and malware crimes, the sorts of incidents that can occur, and the tools and techniques available to avoid them. Others can reduce the danger of these incidents and protect themselves from possible damage by adopting proactive preventative measures.

II. CREATION OF MALWARES

Malware is typically coded using programming languages such as C, C++, Java, Python, and Assembly language. The specific language used depends on the type of malware being created and the platform it is designed to target. Malware can be written from scratch or modified from existing code. Some attackers may use publicly available malware code or exploit kits, which are pre-packaged sets of tools designed to exploit vulnerabilities in software or systems. Others may create custom malware specifically designed to target a particular victim or organization.

The coding process for malware typically involves several stages. The first stage involves identifying the vulnerability or weakness in the target system that the malware will exploit. The attacker will then develop a plan for how the malware will be delivered to the target system, such as through email or a malicious website. Once the delivery method is determined, the attacker will begin to write the actual code for the malware. This involves creating the necessary functions and modules to carry out the attack, such as keylogging or data exfiltration.

To avoid detection by anti-malware software, the attacker may also use various techniques to obfuscate the code, such as using encryption or code compression. Additionally, the attacker may use code signing certificates or other methods to make the malware appear legitimate or trusted. After the malware is coded, it will typically undergo testing and refinement to ensure that it can effectively carry out the intended attack. The attacker may also develop additional features or functionality to expand the malware's capabilities or increase its effectiveness.

In summary, malware is coded using various programming languages and techniques, with the specific code and delivery method determined by the attacker's objectives and the target system's vulnerabilities. While anti-malware software can detect and prevent some types of malwares, attackers continue to develop new and more sophisticated techniques to evade detection and carry out attacks.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

III. DEPLOYMENT OF MALWARES

Malware can be deployed in various ways, depending on the attacker's objectives and the target system's vulnerabilities. Some common methods of deploying malware include:

1) *Email attachments:* Malware can be delivered to a victim's computer as an attachment in an email message. The attacker may use social engineering tactics to convince the victim to open the attachment, which can then execute the malware on their system.
2) *Malicious websites:* Malware can be embedded in a website or downloaded when the victim clicks on a link or downloads a file. Attackers may use search engine optimization (SEO) tactics to ensure that their malicious websites appear high in search results.
3) *Drive-by downloads:* When a victim visits a compromised website or views an infected piece of advertisements, malware is immediately downloaded to their desktop computers.
4) *Removable media:* Malware can be propagated by corrupted USB flash drives or other portable storage devices that are plugged into a victim's computer.
5) *Software weaknesses:* Malware can take advantage of flaws in software or operating systems to gain access to a victim's machine. An attacker, for example, may use a weakness in a browser plugin to install malware on a victim's machine.
6) *Social engineering:* Viruses may be distributed by social engineering techniques such as scam emails or bogus software upgrades. In such instances, the person may unintentionally download and install malware.

Once the malware is deployed, it can carry out a range of malicious activities, such as stealing data, controlling the victim's computer, or using the system to launch further attacks.

IV. HOW MALWARES INFECT MACHINES?

Here is a step-by-step breakdown of how malware works when activated:

1) *Delivery:* Malware is delivered to the victim's computer through various means, such as email attachments, infected websites, or software vulnerabilities.
2) *Activation:* Once the malware is on the victim's computer, it needs to be activated before it can start carrying out its malicious tasks. This can happen automatically when the victim opens an infected email attachment or visits a compromised website.
3) *Installation:* Malware needs to be installed on the victim's computer in order to execute its malicious code. This can involve creating files or registry entries on the victim's system.
4) *Execution:* Once the malware is installed, it can start executing its malicious code. This can involve a range of activities, such as stealing sensitive data, logging keystrokes, or creating backdoors for remote access.
5) *Communication:* Malware may communicate with a command-and-control server to receive instructions or send stolen data back to the attacker. This communication can happen over the internet or other communication channels.
6) *Persistence:* Malware may be designed to persist on the victim's system, even after the initial infection is removed. This can involve creating hidden files or processes that are difficult to detect and remove.
7) *Propagation:* Malware may also be designed to spread to other systems, either on the victim's network or beyond. This can happen through various means, such as using email or exploiting vulnerabilities in software.

In summary, malware works by being delivered to a victim's computer, activated, installed, and then executing its malicious code. It may also communicate with a command-and-control server, persist on the victim's system, and propagate to other systems.

V. WHAT IS BLOCKCHAIN?

Blockchain is a distributed ledger system that enables safe and transparent transactions without the use of middlemen. It was initially designed for Bitcoin, a digital currency, but it has subsequently been adapted to a variety of other applications, including supply chain management, polling systems, and more. Blockchain, at its fundamental level, is a database comprised of a sequence of blocks. Each block comprises a series of transactions, and each block in the chain is connected to the preceding block. This generates a chronological and immutable log of all of the transactions, making it challenging to change or manipulate the data.

Blockchain uses a system of consensus to guarantee that all parties involved in a transaction agree on the transaction's legitimacy before it is added to the blockchain. This consensus is achieved by mining, a process in which a network of computers competes to solve complicated mathematical puzzles in order to validate and add transactions to the blockchain.

One of the most important characteristics of blockchain is its decentralisation. Blockchain runs on a peer-to-peer network of nodes that collaboratively maintain the blockchain, rather than depending on a central authority to oversee transactions. Because there is no single point of failure, it is more secure and resistant to hackers or attacks. Transparency is another crucial aspect of blockchain. All transactions are recorded on the blockchain and are viewable by anybody with network access. This guarantees that all parties engaged in a transaction may have confidence that the transaction is genuine and that the data on the blockchain is genuine.

In essence, blockchain is a decentralised and distributed ledger system that uses a consensus method to enable safe and transparent transactions without the use of middlemen. Its primary characteristics are decentralisation, openness, and permanence, making it a potential technology for a wide range of applications.

VI. PHISHING IN BLOCKCHAIN

In the context of blockchain and Web3, phishing attacks can target individuals who hold digital assets or participate in decentralized applications (dApps). For example, attackers may create fake websites or dApps that mimic legitimate ones and trick users into entering their private keys or other sensitive information. Once the attacker obtains this information, they can access the victim's digital assets and steal them.

Another type of phishing attack in the blockchain and Web3 space involves social engineering tactics. For instance, attackers may send messages or emails that appear to be from a trustworthy entity, such as a blockchain project or a prominent community member, and ask for sensitive information or a donation in exchange for a reward. This type of attack preys on individuals' trust in the blockchain community and can lead to significant financial losses.

In addition, blockchain and Web3 projects can take steps to protect their users from phishing attacks. This includes implementing security measures such as two-factor authentication and encryption, as well as educating users on best practices for staying safe in the decentralized ecosystem.

Overall, phishing attacks are a significant threat in the blockchain and Web3 space, and individuals and projects must remain vigilant and take proactive measures to prevent them.

VII. MALWARE IN WEB3/CRYPTOCURRENCY

Malware is a type of malicious software that is designed to infiltrate a computer system or network and cause harm. While malware is not unique to Web3, it can pose a significant threat to individuals and organizations operating in this decentralized environment. In Web3, malware can be used to steal digital assets or private keys, compromise smart contracts, or conduct other nefarious activities. Malware can be spread through various methods, including social engineering tactics such as phishing attacks or through the exploitation of vulnerabilities in software and smart contracts.

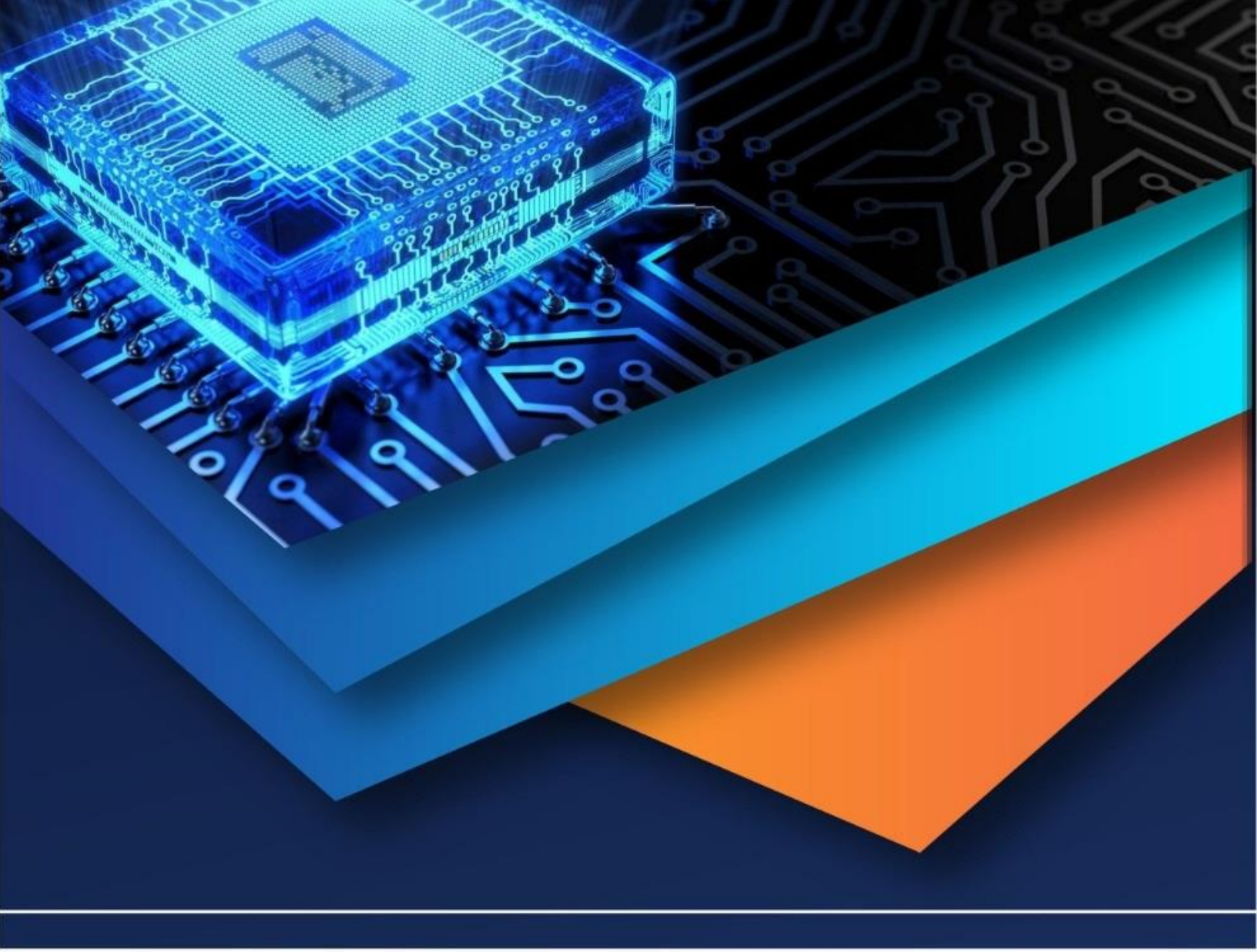
Ransomware is a sort of virus that is becoming more common in the Web3 environment.

Ransomware is a form of virus that encrypts the information or documents of a victim and demands a monetary ransom in return for the decryption key. Ransomware may be propagated in a variety of ways, including scam emails, software flaws, and malicious URLs.

Cryptojacking is another sort of malware on Web3. Cryptojacking is a sort of malware that uses the computer or network resources of a victim to mine coins. This can result in major performance difficulties for the victim as well as hardware component damage.

REFERENCES

[1] Bashir, I. Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained. (2018).
[2] Hadnagy, C., & Fincher, M. Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails. (2015).
[3] Ligh, M. H., Adair, S., Hartstein, B., & Richard, M. Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. (2010).
[4] Drescher, D. Blockchain Basics: A Non-Technical Introduction in 25 Steps. (2017).
[5] James, L. Phishing Exposed. (2015).
[6] Ligh, M. H., Case, A., Levy, J., & Walters, A. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. (2014).
[7] Tapscott, D., & Tapscott, A. Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World. (2016).
[8] Hadnagy, C. Social Engineering: The Science of Human Hacking. (2010).
[9] Sikorski, M., & Honig, A. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. (2012).
[10] Larence, T. Blockchain for Dummies. (2017).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY