MALWARE INFECTION METHODS ANALYSIS

Naga Srinu. Chalamalasetti

Masters of Science in Information Assurance & Cyber Security

Cybersecurity Foundation

Dr. Dadmehr Rahbari

09-02-2023

Exploring Malware and Cybersecurity

**Abstract:**

This document describes several types of cyber-attacks focusing mainly on distinct types of Phishing, Malvertising and Software Vulnerabilities. It is also concentrating on their consequences and the mitigation process educating about the cyber space attacks, vectors and carriers of attacks, their prevention and resolution methods. Finally presenting the graphical representation of cyber-attacks successfully launched in 2021 and 2022 in different geographical locations.

**Introduction:**

A cyber-attack is a digital attack intended to steal, alter, expose or destroy data, applications or other assets from forbidden access to a network or a system. Cyber security has evolved as a major concern for the present-day digital world for multinational organizations and individuals. With the rapid growth of information and technology, there has been enormous growth in attacking the cyberspace. It is particularly important to safeguard one's security on the web. There are multiple ways in cyber-attacks. This following document explains a brief analysis about the cyber-attacks, malware injections, their consequences and their effective safeguard methods.

**Malware Infection Methods Analysis:**

**Phishing:**

Phishing is an attack that happens to a lot of us, every day very often. It is usually done by e-mail or text messaging. It uses various attack vectors and entry points to manipulate to compromise user’s sensitive data. Clicking malicious links or downloading malware tricks the user to steal their information. They might think invoices are real because the attackers send official looking emails but instead it has a phony link. The link redirects users to a new website where they will be prompted to fill out the details of the user that the scammer is trying to collect. Besides e-mail phishing there are other ways being used, like text message phishing, social media phishing and so on. Looking into several types of phishing,

*Email Phishing*: This is the most common method of phishing, making up a major part of all phishing attacks. The attacker tries to trick you into giving away personal information through deceptive emails. One such email is below.

|  |
| --- |
| Hurray Lottery Won...!  Peter Heins [<pete@gmail.in](mailto:<pete@gmail.in)>  Dear User,  You have won a lottery for $100,000.00. To claim the amount, [click here](http://facebook.com).  Sincerely,  Pete. |

*Spear Phishing:* Making up to the second most phishing attempts, spear phishing is more targeted. The attacker uses information about the user to make the attack seem more legit.

|  |
| --- |
| Hurray Lottery Won...!  Peter Heins [<pete@gmail.in](mailto:<pete@gmail.in)>  Dear Robert,  I am Pete CEO the Official Lottery Office of the United State’s. I am writing to you to inform you that you have won a lottery for $100,000.00. To claim the amount, please [click here](http://facebook.com).  Sincerely,  Pete. |

*Whaling:* Whaling attacks, which specifically target high-ranking individuals like CEOs or managers.

|  |
| --- |
| Our new enterprise application has been released,  Peter Heins <[pete@enterprise.in](mailto:pete@enterprise.in)>  Dear CEO,  Thanks for giving us a moment to read this email. We have launched an enterprise application to build websites in a click. Please go through our [company's website](https://www.godaddy.com/websites/website-builder) to know more.  Best regards,  Pete. |

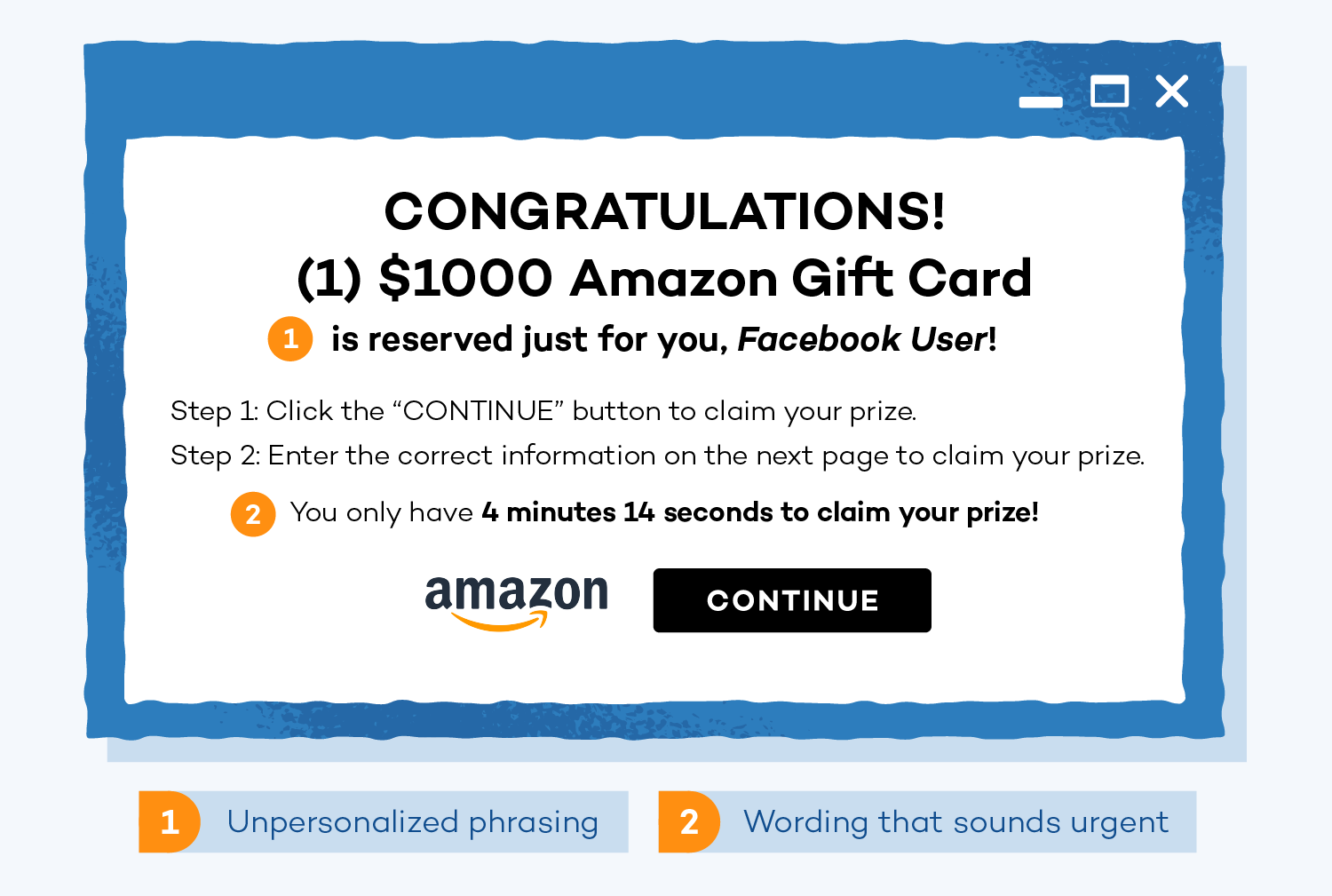
*Smishing*: Smishing, or SMS-based phishing means that the scammers send deceptive text messages attempting to gather sensitive information.

|  |
| --- |
| You have won $100,000. The prize needs to be collected ASAP. Please reply with your bank information so we can deposit the prize money into your account. |

*Vishing*: Vishing is voice phishing where scammers use phone calls pretending to be trustworthy organizations to trick you into revealing sensitive information.

|  |
| --- |
| [You tube link](https://youtu.be/xuYoMs6CLEw?si=PxfnwMmdgh8hcQeg) |

*Social Media Phishing*: These frauds occur on social media platforms. Fraudsters create fake profiles or posts to trick users into giving away personal information.



To find if an email is a phishing mail, the user must verify the mail. Check the sender's address. Review if there are any spelling mistakes or poor grammar. Any request for banking, financial or personal information.

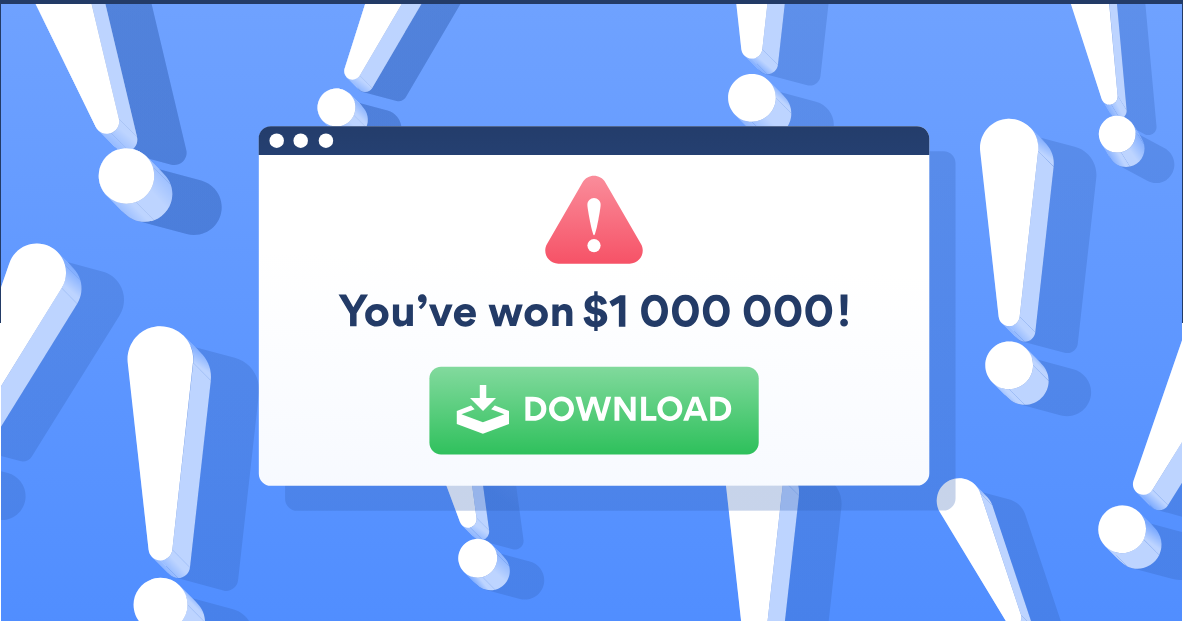
If you ever receive a phishing email or text or message, do not click on the links present in the email. Do not reveal any PI, PII or sensitive data/information. After careful examination, if the email seems like phishing, it must be reported. To confirm its trueness, do login through the official website of the organization or reach out through mobile by the numbers printed on a bill or a business card. The rate of phishing attempts stats is astonishing as 100 million per day, three billion per month and 36 billion per year.

**Malvertising/ Malicious advertising:**

Malvertising, or malicious advertising, is the term for criminally controlled advertisements within the Internet, which intentionally harm people and businesses with all manner of malware, potentially unwanted programs, and assorted frauds through digital ads. Users can fall victim to malware by either clicking on an infected ad or just by visiting a website that is home to a corrupted ad. Cybercriminals can launch malvertising attacks by buying ad space from advertising networks and then sending infected images with malicious code.

Malvertising falls into two categories, defined by the delivery method of the malware: Pre-click & Post-click.

It is a common misconception that malicious advertisements are only a risk if you click on them. Advanced malvertising can bypass some ad-blockers or automatically initiate malware downloads if you are on the same page as the attacker. It is hard to get protection from these attacks. Post clicks are also equally harmful as they can lure you to click on the advertisement and start harming the user’s device and data.



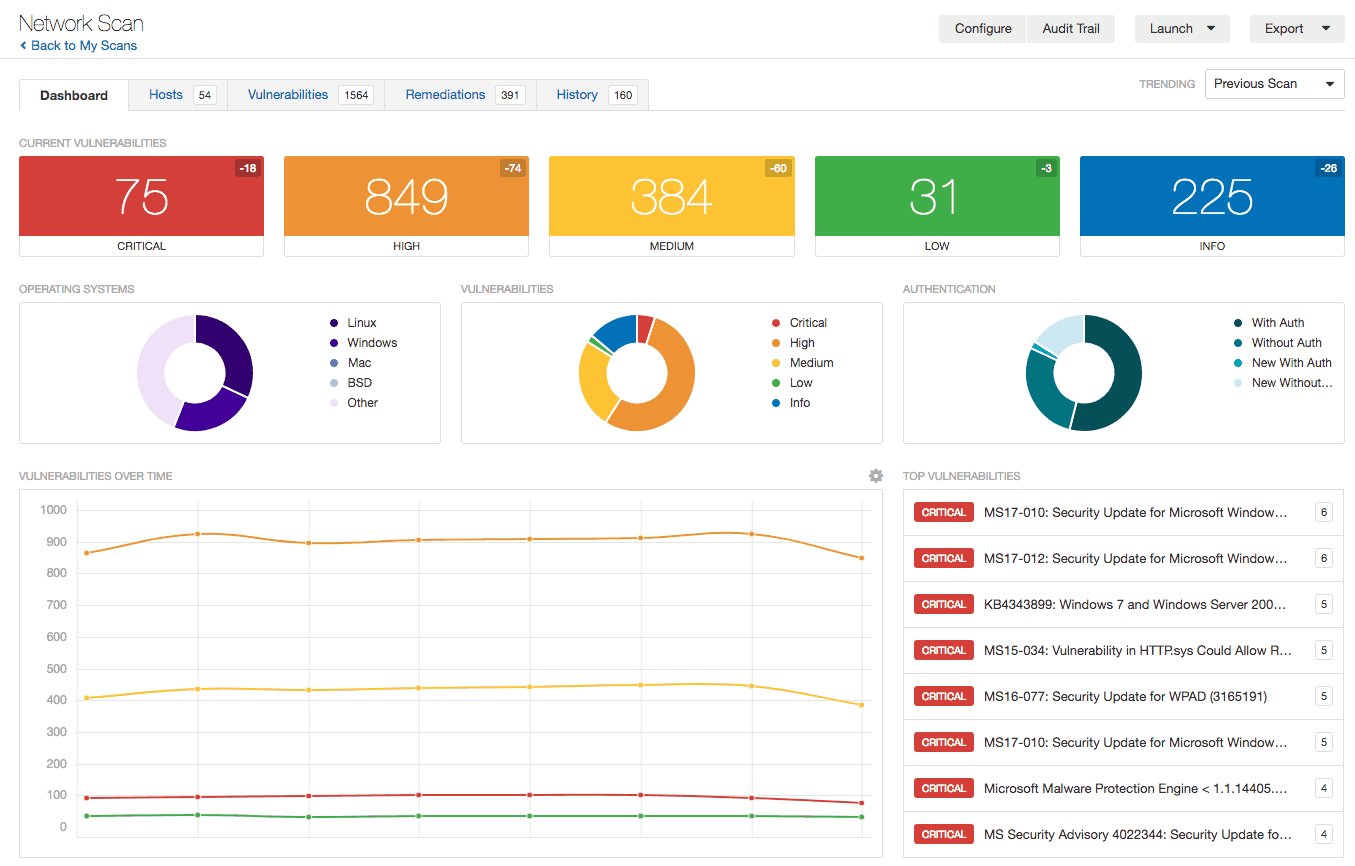
To get protection from the Malvertising, the user need to use an ad-blocker, which though is not a cent percent efficient method, but can reduce the risk of Malversement. An antivirus software can also make sure that the damage by the malicious program be limited. An updated software is to be used to keep the device protected.

**Software Vulnerabilities:**

A Software vulnerability is a glitch or a flaw in the code that the cyber attacker can exploit by accessing the sensitive data on a network. The software vulnerabilities evolve as a threat in the modern day computing. A software vulnerability can happen to an opensource or commercial licensed software as well.

A software vulnerability can be exploited when there is any usage of third-party libraries, improper Application Programming Interface (API) usages, unsecure applications installation or imposter code runs.

The software vulnerabilities can be discovered in multiple ways. One common way is running the port scan on a system to collect information on the services that are being run on the server or the system. It can further also describe the Operating system details, which further can enhance other vulnerabilities in case present in the OS. A successful injection into the system can grant the attacker with the ability to exploit the system in various methods like SQL injection, Buffer overflow, Os command Injection etc.,



To mitigate the Software Vulnerabilities, the security requirements must be defined prior to the development process. The developer should be using an encoding standard to reduce the risk the software vulnerabilities. The software testing should always be checked from end-to-end for these kinds of flaws before they are released to the client or onto the market.



**Results:**

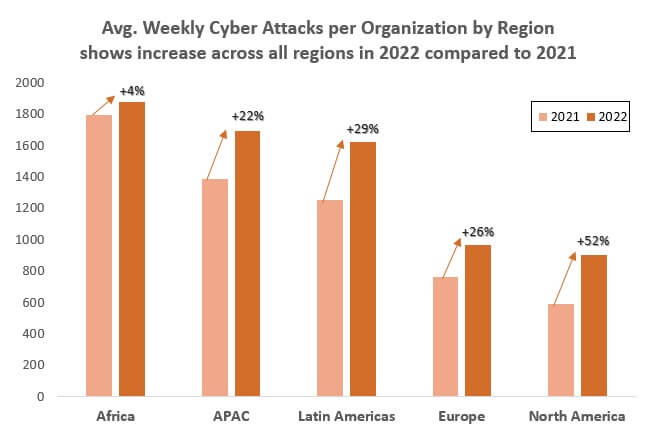
Global volume of cyberattacks reached an all-time high in Q4 with an average of 1168 weekly attacks per organization

Top 3 most attacked industries in 2022 were Education/Research, Government and Healthcare

Geography of Africa experienced the highest volume of attacks with 1875 weekly attacks per organization, followed by APAC with 1691 weekly attacks per organization

North America (+52%), Latin America (+29%) and Europe (+26%) showed largest increases in cyberattacks in 2022, compared to 2021

USA saw a 57% increase in overall cyberattacks in 2022, UK saw a 77% increase and Singapore saw a 26% increase.



**Conclusion:**

The security over the web has a puny belief power as the access is controlled over multiple users and systems. Hence there is an immediate action to be put forth to secure the systems and data from the user end. The usage of firewalls and anti-virus software must be the primary action step from the organizational point of view. Proper guidance and usage must be ensured during software development, testing and during usage. Prompt scans and checks are also needed in a continuous cycle. Educating the users about the software attacks and eradicating them to the most possible degree should be the primary step towards security on the web.

**References:**

Peter A “Cyber Security: Phishing - udemy”, 2022

Malcolm Higgins “What is malvertising? - Nordvpn” 2020.

JFrog “What is a Software Vulnerability? - Jfrog” 2021.

“Everything You Need to Know About Software Vulnerabilities - AppStudio”, 2021.

“Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks - checkpoint”, 2022.

Jasson Firch “10 Cyber Security Trends You Can’t Ignore In 2021 – purplesec" 2021.