International Journal of Mathematics and Computer Research

ISSN: 2320-7167

Volume 10 Issue 11 November 2022, Page no. – 2956-2960

Index Copernicus ICV: 57.55, Impact Factor: 7.362

DOI: 10.47191/ijmcr/v10i11.02

Malicious Links and Their Harmful Effects on Internet Users

Bernard KABUATILA KABUATILA[1], Blaise MUBADI BAKAJIKA[2], Augustin NYEMBO MPAMPI[3]

[1] Department of Computer Networks, Faculty of Computer Science, University Our Lady Of Kasayi (U.KA), DRC

[2] Department of Computer Networks, Faculty of Computer Science, University Our Lady Of Kasayi (U.KA), DRC

[3] Faculty of Computer Science, University Our Lady Of Lomami (UNILO), DRC

ARTICLE INFO

Published Online:
11 November 2022

Corresponding Author:
Bernard KABUATILA

ABSTRACT

Cybercriminals have become experts in using sophisticated techniques to trick victims into sharing personal or financial information. But the best way to protect ourselves remains the implementation of the rules that we are going to recommend in this article because as much as we seek to protect ourselves as much as hackers are continually seeking to develop malicious attacks that will be difficult to differentiate from real e- genuine emails and communications. Thus through this study, we wanted to inform our readers about the various attacks that are constantly gaining momentum on the global web with the innovative and growing use of the Internet of Things (IoT) and portable devices.

KEYWORDS: Cybercriminals, Malicious links, Internet, Internet of Things, victims

I. INTRODUCTION

Threats from the Internet such as: *Spam, viruses, spyware, pharming* or other Trojan horses are ever more numerous and insidious. While some of these computer attacks have existed for several years now, the motivations behind them are very different today and therefore much more pernicious and difficult to counter. Hacking used to be done for glory. Currently it is mainly about making money, tarnishing a person's image, creating *buzz*, etc. The hackers are determined to ransom their victims' money. To do this, *hackers* now belong to organized crime gangs on whose behalf they set up attacks aimed at making money easily and with less danger than drug trafficking or prostitution[1].

Generally, the attacks are discreet and the pirate does not want to be detected. This is the genesis of the new internet attack technique using malicious links as tools. For example, a phishing-type link may very well only last two hours, giving the pirate time to recover some useful data, while ensuring that he is not detected. But in the past, the attacks were massive and intended to do the maximum damage in the maximum possible networks. Once again " *I Love You* " constitutes a good example of a virus intended to affect the greatest number[2].

The malicious links that are the subject of our study constitute all the attacks allowing cybercriminals to take control of Internet users' devices (computer, tablet, smartphone, etc.) connected to the Internet. Examples include *phishing, spyware*, and error message redirection attacks. All of these attacks and threats now target any unsuspecting Internet user who falls into the trap of clicking on any link they receive on the global web.

Not being the first to address this theme, we referred to certain researchers who preceded us in this field such as:

- DAISAY Charles; who spoke on " Phishing: the Puy du Fou victim of a scam".
- ONGEMBA YALLO Roda, who spoke on: " Sanitary pass. Beware of this fake email from the police, it's a scam.

The difference between our study and those of the aforementioned researchers is that the studies carried out by our predecessors were limited to the theoretical approach, but ours will start from the theoretical approach through a scenario of the unfolding of this type of attack. , to fall by the recommendations to observe to protect oneself from these threats on the world web.

That said, our study will include three parts, the first and second will look at the theoretical outline and the course of an attack, so the third will focus on knowing how to protect against malicious links.

II. THEORICAL CONTOUR

In today's digital world, even the most comprehensive security system can be defeated if one manages to outsmart its guardian. Attacks on the global web become commonplace, cybercriminals formalize Legit-looking links that include a malicious link to a known website like Facebook, Amazon, etc. By clicking on the link, victims are directed to a fake website identical to the original site where they are encouraged to confirm or update their account information. This rise in power of cyberattacks obliges us to inform those around us of the risks associated with them and the means of prevention.

II.1 *Terminology*

A. Attack

A computer attack is any action that aims to harm the computer system. It is a voluntary and malicious action carried out by means of a computer network aimed at causing damage to information and to the people who process it (individuals, companies, hospitals , institutions , etc.). An attack can be the act of a single person (hacker), a group of pirates, a State or a criminal organization . Attacks are facilitated by the increasing amount of information put online (cloud) and by security flaws in the systems.

B. Malware

Malicious software or malware also referred to as harmful software or malware or spam is a program developed for the purpose of harming a computer system , without the consent of the user whose computer is infected. Nowadays, the term "virus" is often used, incorrectly, to refer to all kinds of malicious software. Malware includes viruses , worms , Trojan horses , and other threats.

C. Cyber attack

A cyberattack is any type of offensive action that targets computer systems, infrastructures or networks, or even personal computers, using various methods to steal, modify or destroy data or computer systems[3].

D. Cybercrime

A cybercrime is a " criminal offense likely to be committed on or by means of a computer system generally connected to a network ". It is therefore a new form of crime and delinquency which differs from traditional forms in that that it is located in a virtual space, " cyberspace ". In recent years, the democratization of access to computers and the globalization of networks have been factors in the development of cybercrime[4].

E. Cybercrime

Cybercrime is criminal activity that targets or uses a computer, computer network or networked device. It is also defined as any criminal activity carried out through cyberspace and the Internet. By extension, it includes any form of electronic maliciousness carried out using computer and telecommunications technologies (telephony, smart cards, etc.). Whether fraud, scam, extortion, vandalism or harassment, for example, malicious or criminal behavior exploits the characteristics of the Internet and harms Internet users, organizations and society.

II.2 Malicious links

Malicious links are presented as the set of hypertext links designed by cybercriminals to infiltrate computers and mobile devices, perform unauthorized activities and steal personal information. A single click on this link, a single pirate URL, is enough for the computer, the smartphone to be infected, the password exposed, the data blocked or stolen. So this part of our thinking will lay out some types of these attacks[5].

A. The Computer Hoax

A computer hoax (in English : *hoax*) is content produced online or offline by a person and then disclosed to other people by means of a hyperlink , an email or a chain letter [6]. Unlike spam , which is most of the time sent in an automated way to a list of recipients, these types of messages are relayed "manually" by people in good faith who are asked to forward the message to everyone they know. or to a specific email address which floods the server with unnecessary network and requests and makes network traffic slow. This type of link is too common on social networks; the following figure illustrates an example of a computer hoax relayed on facebook messenger asking each Internet user to share the message with 50 friends on his list; the question that each Internet user should ask is to know the origin of the message but unfortunately as we quote God in the attack the Internet users are content to share forgetting that this message would hide an attack of saturation of the network.

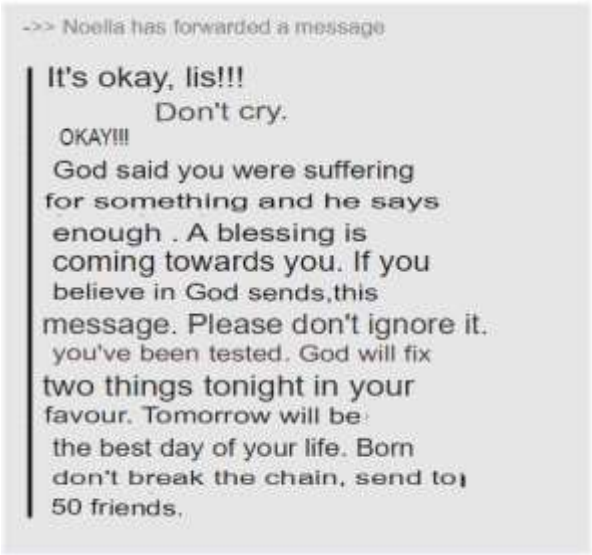


Figure 1. The computer hoax

B. ***Baiting***

This is a type of malicious link where the attacker makes a tempting offer to Internet users and tries to

convince them to go ahead with a transaction or provide him with information that gives him access to their accounts. With this kind of scam, the person responsible for the attack is probably trying to gain access to the system to introduce a malicious program[7]. We present in the figure below a baiting attack where the attacker pretends to be the Ministry of Employment and the DRC which offers subsidies to state officials; the attacker creates a link which he shares on social networks thus enticing people to follow the link to provide the information he will use to continue his attack.

Figure 2. The example of a baiting link

So once the Internet user clicks on the link, he is redirected to the pirate site as shown in the following figure; on the site everything is planned to seduce the Internet user to continue to provide his confidential information. However, as we notice in the Democratic Republic of Congo we have the Congolese franc as currency but the site already offers the CFA franc, and even the structure of the URL of the site does not correspond to any site in the DRC, by extension we know that the parent domain of our country is the ***.cd*** , starting from these elements it becomes easy to directly detect the attack that the open link hides.

Figure 3. The example of a pirate site

D. Phishing

Phishing is a scam that tricks people into sharing sensitive information, such as passwords and credit card numbers. Just as there are many types of hooks, there are many ways to catch a victim, but one specific phishing tactic is on the rise. Victims receive an email or text message that impersonates (or " impersonates ") a person or organization they trust, such as a colleague, bank, or government office. When the victim opens the email or text message, they find a disturbing message that plays on fear to prevent them from reasoning. This message asks the victim to go to a website and immediately perform an action or, if not, face the consequences.

If users take the bait and click the link, they are sent to a site that imitates a legitimate site. There, they are asked to login with their username and password[8]. If they are gullible enough to agree, the login credentials are passed on to the criminal, who uses them to steal identities, plunder bank accounts, and sell personal information on the black market. On the following lines we present two types of phishing attacks.

E. Whatsapp scam

Phishing attempts (or phishing) are currently invading smartphone owners, via the Whatsapp messaging application . The modus operandi is not recent but, well established, it continues to rage and claim victims. The attacker will encourage the target to click on the inserted link leading to a fake site of the impersonated brand. After answering a series of questions, the target is told that he is eligible to win or obtain a gift[9]. But, before obtaining them, she will have to send the message received to twenty of her contacts via Whatsapp , in order to spread the scam. Here is an example of this type of phishing.

Figure 4. The example of a phishing link

C. Inheritance scams

The scammers send out an e-mail message offering huge commissions in exchange for using a bank account to make very large transfers. These are generally alleged funds that would be blocked in a bank in the name of alleged heirs who cannot recover their assets without the intervention of a third party[10]. Scam artists excel at instilling doubt in the minds of people who are being tricked into impersonating real people and real banks by creating suggestive but fake email addresses. The scammers' objective is either to obtain your bank account number and a copy of the signature in order to give false transfer orders to the bank, or to make the target pay a so-called preliminary "application fee", which will then follow in cascade.

III. UNFOLDING OF A MALICIOUS LINK ATTACK

We have just presented some types of malicious link attacks above. This second part of our study is responsible for spreading the scenario of one of this type of attack. We start from the generation of the link, its sharing on the network to end up exploiting the equipment of our victim; in the context of this scenario we will use the Kali Linux *Metasploit tool* for the generation of malicious links, this same tool will serve as our victim's spying interface.

Figure 5. Metasploit 's main interface

A. Scam link generation

There are several environments that hackers use to develop their attacks, the *Metasploit* that we used here is one of the powerful tools of the free environment Kali linux distribution skilled in computer security and hacking; indeed ; we present link generation with Kali Linux; the generated link will be sent as a message to a smartphone.

Figure 6 . pirate link generation

B. Taking control of a victim smartphone

This process begins once the victim clicks on the trapped link and his smartphone is still connected to the network, on the Kali Linux side a message indicates the presence of a connected victim by providing a few elements (Type, Brand, Port number of listening and the Ip address) of the equipment as shown in the capture below[13].

Figure 7. The detection of a victim

C. Spying on the victim smartphone

A click on the target gives us the opportunity to browse the information available to the victim smartphone, all that remains is to click on the tab corresponding to the information we need to explore[11]. The following screenshot shows our target's file manager.

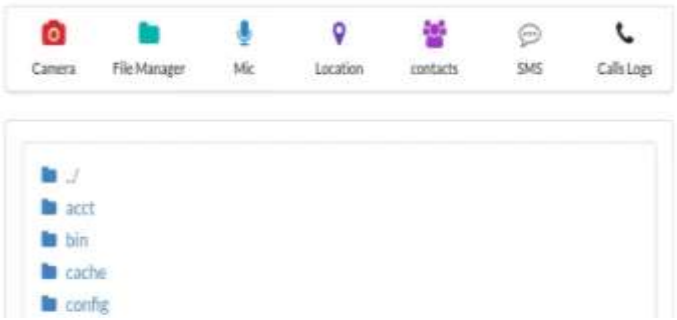


Figure 8 The exploitation of the victim's files

It should be emphasized here that the growing number of *Sextups* on social networks is above all not the work of the person concerned, the hacker goes through such mechanisms by activating the victim's camera remotely, which gives him the possibility of monitoring any movement of its target and can even start recording the video; that he will use in exchange for a sum of money otherwise swing on the canvas to tarnish the image of the victim.

Figure 9. Taking control of the victim's camera

D. How do I know if my devices are infected?

Sometimes it is not obvious that a device has been infected. Malware can operate very well secretly. Sometimes also certain signs will warn you that your device has been infected with malware:

- ✓ Your computer may slow down, crash or freeze.
- ✓ Changes to your browser's toolbar may occur and you may end up on websites you did not request.
- ✓ Your cell phone data usage is skyrocketing.
- ✓ You notice an app on your cell phone that you haven't downloaded.

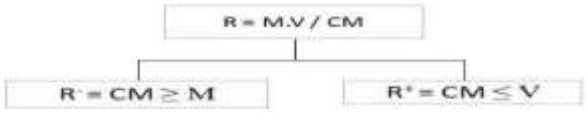
IV. PROTECT YOURSELF FROM MALICIOUS LINKS

It is true that in the computer world there is not absolute security, but it is preferable to minimize the risk of attacks by defining a protection threshold because if the level of faults in your equipment is high, you are exposed to at any time to attacks of various forms; that's why we start by presenting this simple risk calculation formula to assess

how much we are all exposed when we are connected to the global web[12].

Risk= Threat *Vulnerabilty/Countermeasure

- ✓ ***Risk:*** This is the probability that a threat will exploit a vulnerability . In other words, it is a possibility that a harmful event will occur.
- ✓ ***Vulnerability:*** It is an inherent weakness in a system (software or hardware). Sometimes called a fault or breach, it represents the level of exposure to the threat in a particular context.
- ✓ ***Threat:*** it is the danger (internal or external) such as an attack , a virus, etc.
- ✓ ***Countermeasure*** : it is a way to reduce the risk in an organization.



The risk is all the more reduced as the countermeasures are numerous. The risk is greater if there are many vulnerabilities. So we must observe the following rules to minimize the risk of falling victim to attack when we surf the Net.

- ➲ Always have up-to-date anti-virus and anti-spyware software;
- ➲ Avoid downloading free apps, files, programs and software.
- ➲ Never respond to pop-up messages that appear on sites or apps asking for your confidential information.
- ➲ Take all the time and don't let urgent messages impress. Always take the time to carefully consider details and facts before acting.
- ➲ Never share information, be careful when sharing personal or professional information;
- ➲ Carefully observe the URL of the link, any spelling error or irregularity must attract attention;
- ➲ Check that the site is secure: a padlock must be present in the URL and the site address must begin with HTTPS (and not HTTP);
- ➲ Enter username and passwords only when using a secure connection.

V. CONCLUSION

Cybercriminals have become experts in using sophisticated techniques to trick victims into sharing personal or financial information. But the best way to protect ourselves is to put the rules listed above into practice, because as much as we seek to protect ourselves, hackers are constantly seeking to develop malicious attacks that will be difficult to differentiate from real e-mails and authentic communications. Thus through this study, we wanted to inform our readers about the various attacks that are constantly gaining momentum on the global web with the innovative and growing use of the Internet of Things (IoT) and portable devices.

REFERENCES

1. Stern, J. 2011. "The Science of the Secret", Paris, Odile Jacob,
2. Atelin, P. 2014. "Modern Cryptography", Brussels, ENI Edition,.
3. Salem, O. 2012. "Network protection against attacks", Paris, 3rd Ed Eyrolles,
4. Anderson, R. 2018. "Security Engineering: A Guide to Building Dependable Distributed Systems", London, 2nd Ed. Wiley ,
5. Martin, U. 2014, "Introduction to cybercrime", London, Ed. Wiley.
6. BERRY G. 2010. Why and how is the world going digital?, Paris, Ed. Eyrolles,
7. Kauffer R. 2018, World History of the Secret Services , Paris, Ed Eyrolles,
8. Pujolle G. 2019. *Security and Cryptography* , Paris, 6th Ed . Eyrolles,
9. Lescop, Y. 2016. *Computer attacks* , Paris, Ed. Hermès,
10. Liorens, C. 2008. *Network security dashboards* , Paris, 2 nd Ed. Eyrolles,
11. https://www.cisco.com/web/FR/documents/pdfs/solutions/borderless/doc1_internet_threats.pdf , accessed on 04/13/2022 at 9:22 p.m.
12. https://softwarelab.org/fr/maliciel.html consulted on 03/12/2022 accessed on 04/13/2022 at 4:35 p.m.
13. https://summarynetworks.com/securite-des-reseaux-informatique-et-telecom/pirater-et-controler-un-telephone-portable-via-metasploit-sous-kali-linux-2020/ consulted on 04/02/ 2022 at 00:22'