SSRG International Journal of Computer Science and Engineering
ISSN: 2348 – 8387 /doi:10.14445/23488387/IJCSE-V8I6P103
Volume 8 Issue 6, 9-12, June 2021

Computer Analysis Vulnerabilities Related To The Coronavirus Pandemic

Dr. Abdourahime Gaye

Department of Computer Engineering and Communication,
University Alioune DIOP, Bambey, Senegal

Received Date: 26 May 2021
Revised Date: 27 June 2021
Accepted Date: 05 July 2021

Abstract *— The pandemic has accelerated the digital Transformation of most companies. The IT business has become even more critical for companies that had to adapt In an agile and efficient way during the crisis. As containment was implemented, companies worked at breakneck speed to ensure that the entire workforce could Continue to work from home efficiently. However, this new switchover creates new security constraints that create Vulnerabilities in IT systems. To carry out our work, after a short introduction, we studied the context of cyberattacks And the Covid-19 pandemic. We then analyzed the vulnerabilities in a computer system related to the Coronavirus. Our work ends with a proposal of protection mechanisms or barrier gestures against computer vulnerabilities related to the coronavirus and an example of the algorithm named FNCOVID to counter fake news or Phishing related to the coronavirus.*

Keywords *— Computer system, Covid-19 pandemic, cyberattacks, fake news, protection mechanisms, Phishing, vulnerabilities.*

I. INTRODUCTION

Millions of employees around the world currently work remotely. They are turning to videoconferencing tools to meet their business and social commitments. With this widespread telecommuting happening unannounced, some employees are using their personal devices to do their work. And this is one of the biggest vulnerabilities of the corporate network.

Indeed, companies have moved quickly to adapt to telecommuting, but few have integrated employees' laptops, tablets and mobiles into their update management Programs, which could leave corporate data exposed. Even the least sophisticated attack can take advantage of these Unsecured devices.

But such an influx of users will always attract the the attention of security researchers as well as malicious actors
who thus seek and discover vulnerabilities in high-traffic Platforms, albeit for very different purposes.

In order for organizations to operate securely, they need a complete picture of all the devices connected to their Networks. However, they struggle to gain full visibility of their IT assets [01, 02, 05, 08,09].

II. CYBERATTACKS AND THE COVID-19 PANDEMIC

In the midst of a health crisis, cyber attackers are not Letting up. Cybercriminals follow the news very closely: as soon as a national or international event arouses the interest of Internet users, they send millions of emails Impersonating companies or ONG. Medical circles are Concerned as well as companies. Their objective: to Recover personal data or money. The coronavirus epidemic Do not escape this type of scam...

The quarantine measures and the social distances required in response to the coronavirus pandemic have forced companies to switch to teleworking, which makes Them more vulnerable. Many are talking about a "digital Pandemic risk". While Covid-19 is mobilizing health services around the world and disrupting economic sectors, cybersecurity professionals are particularly fearful of another evil, that of data theft and computer ransomware [02, 04, 06].

III. VULNERABILITIES IN A COMPUTER SYSTEM RELATED TO THE CORONAVIRUS

The pandemic and telecommuting weaken the security systems of companies and individuals, who are more exposed to the risks of personal and banking data theft and Ransomware. Several dissemination vectors have been identified [01, 02, 03, 05, 10, 11, 12], including :

- **Email**: Email exchanges have exploded during this period Of containment. Email is the preferred communication tool for all employees working remotely, which explains Why it is highly targeted by cybercriminals. The hacker pretends to be a known service (administration, bank, International organization etc.). They encourage users to Click on a link or download an attachment. Indeed, users

often scared do not hesitate to open emails that contain a Word related to the coronavirus. Especially since the messages claim to provide masks or hydro-alcoholic solutions;

- **Fake websites Phishing campaigns**: These sites could be used for phishing purposes, a technique that consists in extorting personal information (password, bank card code) by pretending to be a legitimate site;
- **Fake news:** As the coronavirus epidemic arrives on the African continent, a lot of false information is circulating About the epidemic. The World Health Organization (WHO) warns against the effects of a harmful "infodemia". The Top "fake news" in circulation related to Covid19: Immunity by youth, Digital spread to 5G, cure by temperature, bioweapon rumor, etc.;
- **False maps of the spread of the disease around the world**: maps are produced to track and visualize reports of the total number of confirmed cases, as well as deaths And recoveries from the epidemic. They can use erroneous data that do not come from the Centers for Disease Control and Prevention, the World Health Organization and other reliable sources to spread panic and confusion during an epidemic;
- **Fake telecommuting applications:** they look like Legitimate sites but are actually fraudulent replicas. They encourage users to fill in personal information and/or click on malicious links and/or download malicious files, sometimes without their knowledge;
- **The exploitation of resources and electricity consumption**:
  Attackers can also take advantage of an employee's Wi-Fi connection at home to break into the company's network and plant a software time bomb, which may wake up after The crisis... Moreover, the use of energy is rather redirected from companies to homes;
- **Computer viruses**: E-mails or malicious sites can also be used to spread computer viruses, in addition to extorting Information or credit card numbers. Most e-mails ask recipients to download a Microsoft Word document for More information. Once downloaded, the Word file activates malware, allowing attackers to access sensitive Data. Several authorities and specialized companies have discovered that these emails carry, for example, ransomware, viruses that make a computer's data inaccessible and demand a ransom to unlock it, or malware designed to retrieve bank account identifiers;
- **Increased scams**: Authorities are more concerned about the emergence and spread of deceptive business practices, such as sites that sell masks but never deliver them or that deliver fake hydro-alcohol gel;
- **Resource availability:** Many companies will be challenged by the lack of equipment that allows employees to work remotely on company-provided Devices. As a result, they are often forced to allow Employees to use their own equipment. These personal devices are unlikely to have the same level of protection As company-owned devices. There is also the issue of large numbers of people accessing the company's work Network using virtual private networks (VPNs).

IV. THE BARRIER ACTIONS OR PROTECTION MECHANISMS AGAINST COMPUTER VULNERABILITIES RELATED TO THE CORONAVIRUS

There are a number of barrier actions, digital ones, that can be taken to avoid falling victim to a scam or virus that exploits the anxiety around the Covid-19 pandemic [03, 04, 05, 07, 08, 09, 10, 11, 12]:

- **Treat unsolicited messages or calls with extreme caution**, especially when they ask for personal or secret information, or contain an attachment;
- **Verify the authenticity of messages received, regardless of the medium**: email, SMS, instant Messaging, social networks, etc. The elements to check are the sender, the content of the message, the urgency, The promise of a gain, the notion of an unusual request. In case of doubt, the best course of action is as follows: do not click on the links, do not open or download the attached content, check the information on official websites, forward the e-mail to the internal security Department. In the case of a request for confidential information, medical or otherwise, it is important to ensure that the sender is authorized to hold this information (i.e., you must be familiar with the company's internal processes);
- **Use various communication channels**: First of all, make sure you know the usual channel for transmitting information within the company (dedicated e-mail Address identified the person in charge of the subject, etc.). It
  It is also important to have a second channel of communication (telephone, instant messaging), allowing you to confirm information, especially if it seems to come from the company;
- **Ensure the legitimacy of the sales site** in the event of an online purchase (presence of the name of a company registered in the commercial register, general sales Conditions, etc.). Do not hesitate to report malicious or suspicious sites on the Pharos platform or to the Directorate-General for Competition, Consumer Affairs and Repression of Fraud (DGCCRF);
- **Beware of the numerous false information,** which has spread on a large scale these last days and do not relay them;
- **Verify that the fundraiser to which volunteers** are about to give in support of hospitals, patients, or research is legitimate, such as the one organized by the WHO or the Pasteur Institute;
- **Use of VPNs** for home-based workers accessing corporate network resources to ensure secure connections From a location away from the corporate network. It is

advisable to check with IT partners who have close relationships with leading VPN providers, including Cisco and Palo Alto, and may have access to preferential pricing options put in place to help companies meet the the challenge raised by the coronavirus outbreak ;

- **Control the cloud applications**: Some users are able to Work using only cloud applications. For these users, VPN Access to the corporate network may be unnecessary. However, these users, who access cloud applications without connecting to the network, will not be governed by the company's policies and will not benefit from the Protections in place on the network. This, of course, presents security risks;
- **Adopt a secure single sign-on (SSO**) portal that allows users to log in once and then authenticate to the cloud Applications when they need to. With them connected through the SSO portal, IT can enforce company policies, such as controlling which cloud applications each user Can access. SSO can be quickly up and running, configured and launched in as little as two to three hours;
- **Use web filtering tools**, such as Cisco Umbrella, for example, which can manage access to corporate websites whenever a corporate laptop is used to access the internet, Anywhere in the world.

V. EXAMPLE OF PROPOSAL ALGORITHM TO COUNTER FAKE NEWS OR PHISHING RELATED TO CORONAVIRUS: FNCOVID

The operations of the algorithm named FNCOVID is illustrate as:

Begin

1. Receiving a message ;
2. Verification of the origin of the message;
3. If the message comes from a trusted source (official source);
4. If the message has been transferred;
5. Verification of the authenticity of the original message;
6. If the source is reliable, the message can be accepted;
7. If not, blacklist the message and consider it as fake news or phishing.

End

The following figure illustrates an example of an algorithm to counter fake news or phishing related to the Coronavirus.

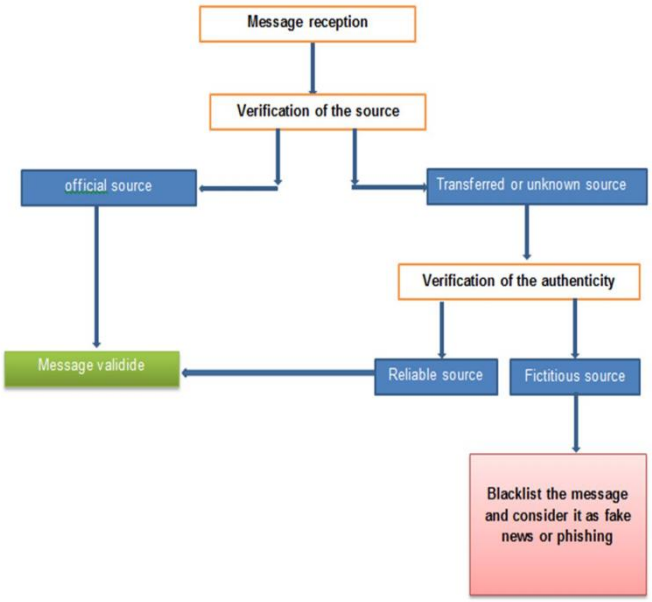

Fig. 1 An algorithm to counter fake news or phishing related to the coronavirus

VI. CONCLUSIONS

Security and IT operations managers must come together To reduce risk. Only by taking a holistic view of all computers, applications, and data - including machines that are unpatched and therefore vulnerable, as well as their Location can priorities be set and immediate attention given to exposed client assets. Companies that migrated their business components to digital platforms before the pandemic performed better during pandemic. Regardless of the dimension of competition (better customer experience, lower operating costs, better employee experience), they want to get there quickly, do it conveniently, and do it at scale.

However, companies that are going digital at scale are Finding that the dual-mode model limits operations. It Creates too much friction. Legacy applications running in the existing infrastructure is not agile enough, and their ability to share data across applications is significantly Limited.

Today, it becomes critical to educate users on the various IT threats associated with the Covid19 pandemic so that they can adopt barrier measures in the face of the many IT Attacks that are being caused.

REFERENCES

[1] Ingrid Vergara, Télétravail généralisé et contexte anxiogènefavorisent la multiplication des attaques, mars (2020).
[2] Florian Dèbes, Covid-19 : pas de trêve pour les cyberattaques, mars(2020).
[3] Martin Untersinger, Coronavirus : comment pirates informatiques et escrocs profitent de la pandémie, mars (2020).

[4] Patricia Herau-Yang, Coronavirus et télétravail: quid de la sécurité Informatique?, avril (2020).
[5] Ali LAIDI , Le coronavirus, nouveau cheval de Troie des cybercriminels, avril (2020).
[6] Michael Cooney, IDG NS (adapté par Jean Elyan), Covid-19 : quel impact sur les réseaux publics et la sécurité ?, le Mars (2020).
[7] Sekurigi, télétravail et sécurité informatique durant la crise du Coronavirus Covid-19, avril (2020).
[8] Sébastien Brocard, Covid-19: comment mieux se protéger contre les risques cyber?, avril (2020).
[9] Philippe RICHARD, COVID-19: attention aux arnaques informatiques !, lmars(2020).
[10] Forbes, Modernisation de l'informatique post-Covid et pénurie de talents, février (2021)
[11] Panda Security, Les 5 tendances post-covid à ne pas négliger en sécurité informatique, janvier (2021).
[12] Marie Gasnier, Cyberattaques et Covid-19 : attention à renforcer la sécurité informatique des hôpitaux, janvier (2021).