An implementation of a Virus focuses on Mobile Devices with Android. An Ethical Hacking Event

Implementación de un virus enfocado en dispositivos móviles Android. Un evento de hacking ético

ARTICLE HISTORY

Received 01 October 2020
Accepted 16 October 2020

Carlos Andrés Estrada Vásquez
Department of Computer Sciences
Universidad de las Fuerzas Armadas - ESPE
Sangolquí, Ecuador
caestrada4@espe.edu.ec

Walter Fuertes
Department of Computer Sciences
Universidad de las Fuerzas Armadas - ESPE
Sangolquí, Ecuador
wmfuertes@espe.edu.ec

Amy Rashell Sánchez Cárdenas
Department of Computer Sciences
Universidad de las Fuerzas Armadas - ESPE
Sangolquí, Ecuador
arsanchez5@espe.edu.ec

An implementation of a Virus focuses on Mobile Devices with Android. An Ethical Hacking Event

Implementación de un virus enfocado en dispositivos móviles Android. Un evento de hacking ético

Carlos Andrés Estrada Vásquez
Department of Computer Sciences Universidad de las Fuerzas Armadas ESPE
Sangolquí, Ecuador
caestrada4@espe.edu.ec

Walter Fuertes
Department of Computer Sciences
Universidad de las Fuerzas Armadas ESPE
Sangolquí, Ecuador
wmfuertes@espe.edu.ec

Amy Rashell Sánchez Cárdenas
Department of Computer Sciences
Universidad de las Fuerzas Armadas - ESPE
Sangolquí, Ecuador
arsanchez5@espe.edu.ec

Abstract — Mobile devices have become part of daily social life. However, the vulnerabilities of this equipment are widespread, affecting information or damaging the system internally. Within this problem, this research proposes the implementation of a virus that allows affecting the Android victim device focusing on finding the vulnerabilities through penetration tests. The virus was designed through the principle of thread programming to a generation of scripts. Furthermore, the attack on Android devices' vulnerable systems is conducted, applying social engineering techniques. Thus, through imper- ative programming techniques and functional, the access and use have been achieved, given that the virus had classes that allow connection and communication with the device. Each class was developed together so that in this way, there is a precise relationship between them. In this study, Kali Linux, with different Metasploit commands, was used. The proofs of concept were conducted using controlled virtual network environments. For this, a server and a platform were used to use the IP and the Ngrok host, which allows us to generate a link with the application that will violate Android's services and security over secure tunnels. The results show that the operating system tends to be prone to internal damage. At the same time, users can be affected when their security and pri- vacy are compromised. The proposal contributes significantly to a new version of Android's security patches, implementing a malware model that will integrate techniques to mitigate this problem in the future.

Index Terms — Android, computer security, vulnerabilities, pen- testing, Metaseploit.

Resumen — Los dispositivos móviles se han convertido en parte de la vida social diaria. Sin embargo, las vulnerabilidades de este equipo están muy extendidas, afectando la información o dañando el sistema internamente. Dentro de esta problemática, esta investigación propone la implementación de un virus que permita afectar al dispositivo Android víctima enfocándose en encontrar las vulnerabilidades mediante pruebas de penetración. El virus fue diseñado a través del principio de programación de subprocesos para una generación de scripts. Además, se realiza el ataque a los sistemas vulnerables de los dispositivos Android, aplicando técnicas de ingeniería social. Así, mediante técnicas de programación imperativas y funcionales, se ha logrado el acceso y uso, dado que el virus contaba con clases que permiten la conexión y comunicación con el dispositivo. Cada clase se desarrolló en conjunto para que de esta manera, haya una relación precisa entre ellas. En este estudio se utilizó Kali Linux, con diferentes comandos de Metasploit. Las pruebas de concepto se realizaron utilizando entornos de red virtual controlados. Para ello se utilizó un servidor y una plataforma para utilizar la IP y el host Ngrok, lo que nos permite generar un enlace con la aplicación que vulnerará los servicios y la seguridad de Android sobre túneles seguros. Los resultados muestran que el sistema operativo tiende a ser propenso a sufrir daños internos. Al mismo tiempo, los usuarios pueden verse afectados cuando su seguridad y privacidad se ven comprometidas. La propuesta contribuye significativamente a una nueva versión de los parches de seguridad de Android, implementando un modelo de malware que integrará técnicas para mitigar este problema en el futuro.

Palabras clave — *Android, seguridad informática, vulnerabilidades, pentesting, metaseploit.*

ISSN: 1390 -9266 – 2020 LAJC

I. INTRODUCTION

Mobile devices have become part of daily social life. However, these devices' vulnerabilities are varied, affect- ing information or damaging the system internally. While researchers trying to improve security, there are groups of hackers who seek out vulnerabilities in a scheme to intercept the various insecurities.

Attacks on mobile devices are frequent. Today, it is im- perative to seek alternative solutions and understand which users are most affected. In fact, from a particular perspective, those who do not control their information and do not handle protocols to protect what they share are those who have a security cyber-attack. That is almost non-existent or unknown to these users, so it is easy to access personal information with the right tools. In particular, users do not activate the encryption system to protect their mobile devices' confidential data. Besides, they do not know the proper procedure to do it [1].

Unfortunately, with this information in the wrong hands, users are vulnerable to cyber-crime. They become victims of extortion, revenge, financial exploitation, among other possible consequences. Against this background, the follow- ing question arises: How can a virus focus on the Android system be implemented using ethical hacking methods? In this sense, implementing hacking methods and using them ethically against the Android operating system is a complex task [5] since being open-source somehow has a security level for users.

This study explains the use of Kali Linux as a system of attack on Android devices. For this reason, we use different tools to achieve this, such as a server to clone a web page and a backdoor that hides an Android application extension (APK) format inside an image. APK is a compressed ZIP file with a different extension to be opened and inspected using archive software.
The procedure is based on Ngrok as a server to store the attack, so the device is compromised. The Metasploit framework of the Kali Linux is also used, which will act as the primary agent to provide the commands and connect to the previously created host or server. The way the attack is carried out is through social engineering. The APK would penetrate all access to the device, including files, photos, videos, calls, text messages, histories, navigation [3]. It would also activate the device's different peripherals, such as the camera, the microphone, among others. It is possible to start geolocation to know the exact location, thus allowing an attack on the victim.

For this study, also we attacked the LAN, using a con- figuration of the perimeter router that is accessed remotely. Then it connects to the IP network server. We highlight that we have designed a virtual network environment with VirtualBox, which allows us to generate the appropriate space for a simulation of the Kali Linux. It was considered essential to carry out this distribution because it is the most complete for computer security.

Also, we demonstrated the different insecurities that the Android device has. Since it is based on the Linux Kernel, it is more prone to cyber-attacks, especially outside the LAN. The image will be sent through a social network platform, where the victim will be encouraged to open it. It will then generate a direct link to the download, which will run in the background and executed in the same way, without the victim noticing its attack. Risks based on this type of vulnerability [4] can enable information to be stolen from any device as if it were the user's own.

Consequently, real attacks to IP networks act so that services can be lifted through Kali Linux frameworks. One of the main and most used is Metasploit. Because most people use different Android devices, it is a standard system of interest for the hacker community to conduct various outlaw activities, such as identity theft, spying, and phishing. The results show that the operating system tends to be prone to internal damage. At the same time, users can be affected when their security and privacy are compromised. The proposal contributes significantly to a new version of Android's security patches, implementing a malware model that will integrate techniques to mitigate this problem in the future.

This study's main contribution is the implementation of an Android Operating System virus to show the insecurity in Android devices through a variant of a virus called Chip.I, which lets an attacker access smartphones. Furthermore, it encourages us to be aware of the necessity and importance of having an antivirus to protect the terminals of this kind of attack.

The remainder of this document is structured as follows. Section 2 explains the highlighted work done by other researchers, which were the basis of this study. Section 3 mentions the implementation of the test platform, the ele- ments and tools used, and the theoretical basis related to the attacks on Android that support the present study. Section 4 describes the design and implementation of the virus. Section 5 shows the results obtained from the experiment and its discussion. Finally, Section 6 explains the outcomes and proposes future work lines.

II. RELATED WORK

There are several studies where that talk about the de- tection and prevention of malware on mobile devices. It was known that for the year 2017, Android was the most used operating system worldwide [2]. For this reason, the developer community has managed to improve the security of this Operating System throughout its trajectory. To conduct a vulnerability and mitigation analysis, for example, Alawneh [5] demonstrates how they use data mining to detect mal- ware focused on the Kernel level and the performance of the CPU. The information collected is used to create a learning model about suspicious behavior [5]. In another instance, a machine learning-based on Java API is used and the characteristics that allow them to be differentiated into good or bad [6]. It should be noted that there must be an initial attack. However, the techniques go unnoticed by antivirus or detectors, making it more difficult to eradicate them [3]. It is easy to create malicious APKs installed on mobile phones thanks to a series of social engineering tools and techniques and thus access all the stored information, be it contacts, bank details, social networks, emails, among others [4].

The mechanisms used to evade detecting malicious ap- plications for Android are linking with a backdoor. This allows technicians to match the APK with the virus, which is a design and implementation of backdoor [7]. This study shows the persistence and effectiveness of implementing it to be activated and temporarily run and control the device remotely to our benefit. Another case study for analyzing a malicious extension of Android was focused on a specific user, which used reverse engineering to face malware, demonstrating its relevance in strategies to protect the user [8].

The study carried out by [9] mentions the feasibility of pen-testing in android devices, which present an attack test using a Metasploit service. This study contributes to our work through the developed framework and the backdoor principle hidden in the device. The results show access to the databases and files saved on the device, generating an innovative study for android security.

According to the study proposed by [10], the use of the Internet with pen-tester methods is mentioned. This study contributes to our work in a gratifying way, given the use of Metasploit. Also, in the function of the successful results and the demonstration of a framework capable of violating Android devices' security. Also, the authors use Linux as an operating system and tools capable of violating security patches. Its code is based on Java for the connection and contributes to a different virus's innovative reason.

The proposal of [11] shows how using machine learning lets researchers implement a malware detection system. This detection system, called DroidMark, looks for potential sources of data leakage, and returns are built by reverse engineering, an APK file capable of finding. Compared with our work, they were collecting sensitive data through an Android application created with Java, whose accuracy level is 96.88 %.

III. METHODS

This section presents an experimental platform's de- sign and implementation, which will evaluate the different Android systems' insecurity through test devices. In this context, we applied a series of steps to verify that the devices would be successfully attacked, demonstrating the initial hypothesis of this operating system's insecurity with this type of virus called Chip.I.

A. Virtualization platforms

Virtualization allows users to run several virtual ma- chines simultaneously, each with its virtual guest operating system, which shares the same physical computer (Host) [12]. That is, the software and hardware part and its in- teraction creates an external interface for the user, which also provides a cost-effective solution for the next remote hands-on education [13].

Among the virtualization platforms, VirtualBox is a virtualizer available for free and open-source [14]. This platform has been chosen for this project, compared to other platforms, since it allows creating, loading, and managing virtual machines remotely via Virtual Desktop Protocol (VRDP) [15].

B. Experimental Platform Design.

a) Kali Linux. Kali is a Debian-based Linux distribu- tion intended for advanced penetration testing and security auditing [16]. It is the most applied for computer security due to its default installer tools and frameworks. In this study, Kali allows it to be the central penetration platform to the Android device through Metasploit and Msfvenom [16]. It is common used for computer security due to its default installer tools and frameworks. In this study, it was the central penetration platform to the Android device through Metasploit and msfvenom.

b) Android. For 2017, the Android operating system around the world surpassed Windows according to data from StatCounter [2], which shows that it reaches 37.93% of total use, while the second decrease to 37.91%, followed by Ios, MacOs, and Linux. As one of the most used operating sys- tems in the world, based on Linux, open-source, it facilitates the detection of faults quickly, and thus these can be adapted more efficiently for users [17]. It should be noted that more than one billion users use it from 5G to tablet devices as it is customizable, easy to use, and compatible with Google applications.

C. Metasploit

A Metasploit framework is an open-source tool that allows users to execute exploits or attacks on different oper- ating systems from a machine with the Kali Linux operating system. It is integrated into it, whose main objective is oriented on computer security. This platform also allows users to find, exploit, and validate vulnerabilities, where it is usually used to perform pen-testing and offer security audits. The Metasploit Framework can connect to almost all penetration test life cycle stages, making complex tasks more manageable [18].

D. Exploitation settings

Among the exploits' configuration, the best known for these cases were used, the Meterpreter type of payload [19]. It has the necessary facilities when carrying out an exploit. It uses a system of channeled communication and encrypted communications. Also, in this process, the execution time will be increased, and it will be loaded through the network [20]. As part of the framework Metasploit, other scripts used for this research project are msfvenom, which includes msfpayload and msfencode. Them combining functionality to generate a shellcode can be injected into an application APK for android. With the multi-handler tool, it allows receiving connections with Meterpreter, which is why it facilitates the exploitation of a victim system [21].

E. Apache Web Server

The Apache HTTP Server is a project of The Apache Software Foundation, whose objective is to provide a secure server with HTTP services [22], synchronously with HTTP standards, contained in the same HTTP standards. Apache Web Server almost always uses data from MySQL, PHP script language, and others like Python and Perl. The con- figuration is named LAMP (Linux, Apache, MySQL, and Perl / Python / PHP), where it can be developed and deploy in web-based applications. In the present study, this tool is used to create a fake web page by generating a fake IP made by Ngrok, which will download and install the APK in the background [23].

F. Backdoor for Android

This tool is usually used maliciously. However, in this project, it is merely handled for academic and research pur- poses. It is useful to access systems and perform malicious activities without the victim (in this case, Android user) having knowledge or understanding its functionality [24]. This type of Trojan gives access to an infected system where it allows remote control and can deleting or modifying files, executing them, or carrying out activities related to the device's use. In this sense, the backdoor functionalities are incorporated to inject a Trojan, using the social engineering technique, through image concealment.

G. Reverse Engineering with APKtool

Apktool is a powerful software developed by iBot- Peaches; it is part of Kali Linux tools for reengineering Android APK files. Used to send applications to previously unsupported devices [25], which also can be used mali- ciously to hide malware, to another distribution capacity, or otherwise for analysis penetration testing Android appli- cation. Any other application for Android can be broadcast through the Google Play platform. However, since the risk of exposure is known in this case study, it was very likely to be detectable and discarded before affecting the user. So by using social engineering techniques, it avoids being revealed and can go unnoticed, to meet the objective of this practice.

ISSN: 1390 -9266 – 2020 LAJC

IV. IMPLEMENTATION

To understand how Chip. I works, it is necessary to observe the following steps. As a first instance, prepare the working environment, starting with the initialization and use of the Kali Linux virtual machine in VirtualBox and a second virtual machine to start the Ubuntu Server. Next, the virtual network must be initialized to be able to work in a simulated environment. It was required to open the tools and consoles to be used. Then, we proceed to configure the router to work outside the LAN. In the first instance, it must enter the default IP address, in this case, 192.168.1.1, and thus configure it to accept DMZ's parameters. Later, we proceed to download the tool from the Ngrok website, which will allow linking the configuration with Android devices. Besides, the connection is made, and the following commands are executed to detect the link with the android devices (see Fig. 1 and Fig. 2).

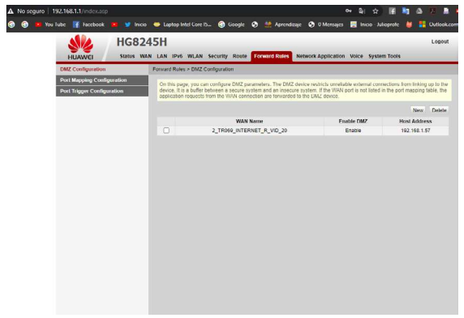


Fig. 1. Login to the router and configure access outside the LAN

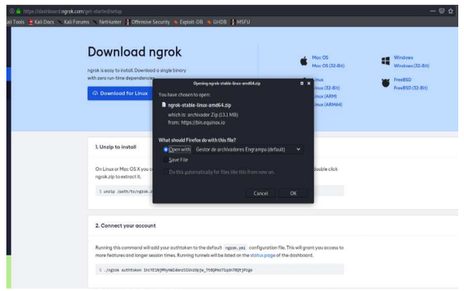


Fig. 2. Download of Ngrok's Package

Afterward, the created Apache2 Web server is initialized, and the previously created web page is accessed through and verification of the link in the virtual machine through the internal NAT network. To verify that the Apache2 page is open, enter the server's IP network, verify that it is running, and create the fake web page (see Fig. 3).

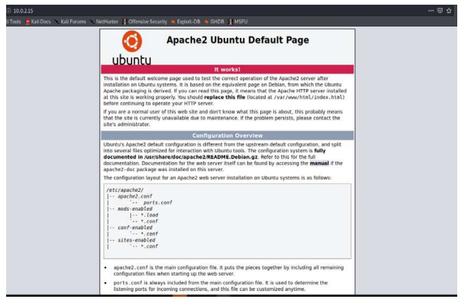


Fig. 3. Access to the created server "Fake web page"

With the following command (see Fig. 4), we call the MSFvenom framework. It was possible to generate and initialize port 4444 and the host, the address, and the appli- cation by creating a package in the format .apk. It allows us to install inside the android device. In this way, we could get access to the data of the victim.

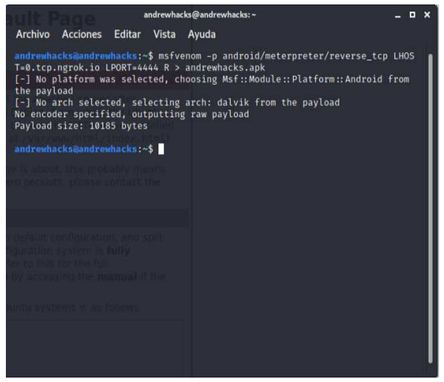


Fig. 4. Creation of the Ngrok package and the APK for Android

As can be observed, the Metasploit was initialized, so it is linked to the console. In this way, access to the required service is obtained. Also, the addresses of the false port are acquired to avoid detections in the LAN network. Thus, we create a false address IP, sharing port 2020 as the central server to the Ngrok platform. When we perform the exploit attack, a reverse TCP

ISSN: 1390 -9266 – 2020 LAJC

attack is carried out, implying to apply social engineering concepts. In other words, instead of the attacker initiating the connection to the device. Once the exploit has been conducted, the Meterpreter is activated.

In the following class diagram (see Fig. 5), it is pos- sible to observe all the attributes. In addition to showing the programming language used, Java users can see the different kinds of data, methods, attributes, and constructors. Whereby the code works is to make a gateway to the appli- cation. As Android is known and its applications work with Java, when establishing a URL connection [26], it passes to the class's established port. It activates the service and the respective SSL validations, also known as certificates.

The main class speaks of MainActivity, which will be re- sponsible for receiving parameters from a Bundle class that creates the connection. It then calls the other methods, in- cluding UrlConnect, which is responsible for connecting the fake web page with the Ngrok server, performing execution, and installation using the Connection class MainService.

V. RESULTS AND DISCUSSION

Once the process is complete, the test is carried out on two terminals. The first is on a device that has Avast antivirus, and the second without any security. Once the attack with Kali Linux is accomplished, the APK file is sent through the WhatsApp social network, achieving to the victim to open the image and be redirected to the false web page's link it is downloaded in the background.

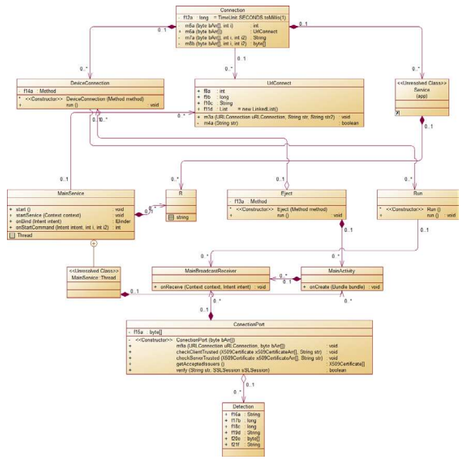


Fig. 5. UML of the APK

As can be seen in the first case (see Fig. 6), the Avast antivirus blocks the installation, preventing it from being carried out and ending the termination of the Chip.I virus. Therefore, an alternative solution is considered to avoid being affected or harmed by data theft, information, and infiltration in the first case. Otherwise, on another device that lacks antivirus security, the application is installed in the background, and the attack is executed. It proceeds to access all the information, and it is installed automatically, which generates a gateway to the server created earlier. The installation has been successful, so the hack performed from the *Meterpreter* exploit.

Once the terminal is accessed, we verify what commands exist and send emails to the victim or text messages. In this way, and at the same time, it can be verified that the hack was successful. Thus, what Meterpreter, as an exploit, allows, is even to remove the call information and observe the conversations that have been had in the different social networks or messaging (see Fig. 7 and Fig. 8).

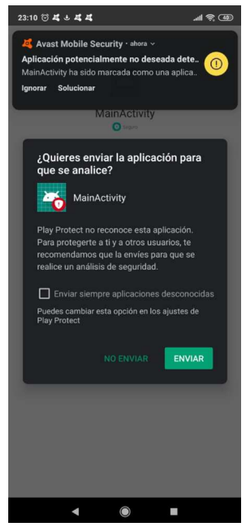


Fig. 6. Installation blocking by avast antivirus

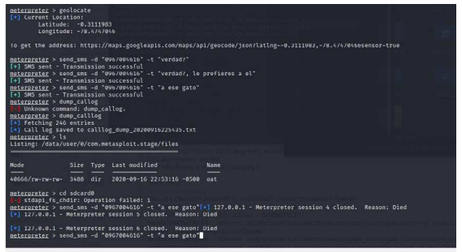


Fig. 7. Management commands in Meterpreter for sending messages and geolocation

The following statistical illustrations show the number of packets received and the transmission and reception band width when the application is active. Also, their performance outside the LAN considers that there is no very high net- work consumption. Figure 9 displays the number of packets received and the time in which they are present, as well as the average transmission or reception speed.

Figure 10 presents the transmitted and received data for the application being executed with the Android device in a pie diagram.

Figure 11 illustrates the received and transmitted data on a timeline, using the bar chart, which indicates that the received packets are more significant due to the amount of data from the attacked device.

Fig. 8. Verification of the hacking in the another device

When analyzing the network's behavior (see Fig. 12), we deduce that this is due to the large number of packets transferred to the mobile device when the antivirus was disabled. Consequently, during transmission, it is likely to receive any infected information on the system. The network received a large number of packets when the attack was perpetrated. However, when the antivirus was activated, its behavior differed, as it prevented the *Chip's.I* entry virus. After the attack is conducted, the packets received to the virtual machine are greater than those transmitted, which is likely to cause the system to collapse. Figure 12 also depicts the network's behavior when the antivirus detected the Chip.I virus. In this case, at 10:00 p.m., it shows little traffic, and the network is stable without much data received.

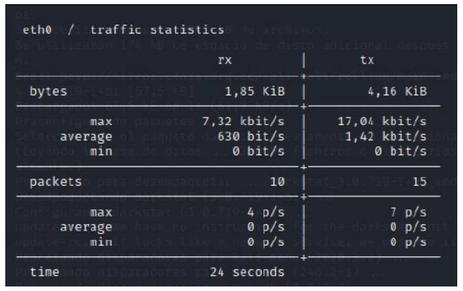


Fig. 9. Statistical data received and transmitted on the network with the application

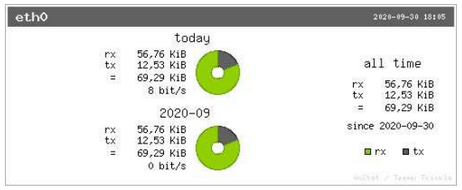


Fig. 10. Pie diagram chart of statistical data

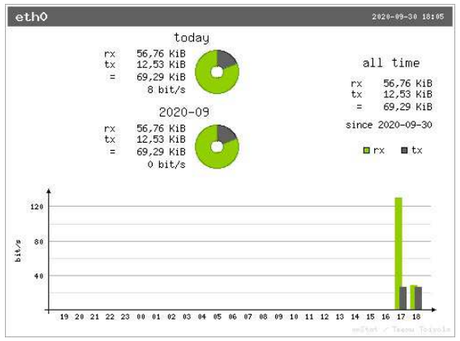


Fig. 11. Bar chart showing the number of packets received by the device

ISSN: 1390 -9266 – 2020 LAJC

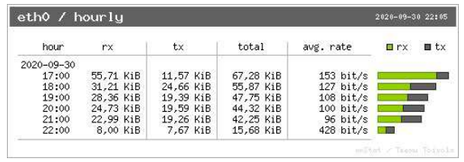


Fig. 12. Bar chart showing the number of packets received by the device

Discussion

After observing that the attack was successful, it is advisable to raise awareness since most of the population uses Android. It can be deduced that the initial Android insecurity hypothesis has been tested as part of the research objective. In this sense, it is stated that having a Linux kernel or having been based on this OS tends to be vulnerable and prone to internal damage. Simultaneously, in the primitive version of Chip.I using the option to affect the peripherals of said server, it was shown that it is possible to overheat the processor and affect its performance. On the other hand, it was also determined that the way it works could be changed, installing the antivirus to make it "invisible," undetectable.

Given that the research gave the expected results, it is confirmed that it was used ethically only for academic purposes. Finally, it should be noted that the controlled virtual network environment, using open source software, can be used to test these devices. As a result, users can be affected by violating their security and privacy, exposing them to the theft of information, their identity, and their credentials, among other possible options. It can even access bank or account details, depending on what the victim has on their terminal.

On the other hand, to perpetuate the attack, it was necessary to access the victim and apply social engineering to convince her to open the image. This image was infected to trick the user into accessing the cloned page through the link inserted in such an image. This method is also known as a backdoor.

For academic testing, it is recommended to have an active server on Apache running Linux, to spoof the desired web page. For the test to be successful, it was necessary not to have any antivirus active or installed. If it existed, the virus to be injected would be detected and automatically eliminated. It is also essential to have the Kali Linux pen- etration test tools, which allow us several options to perpe- trate attacks. Kali Linux is the perfect tool for vulnerability analysis and hackers, who look for cracks in the security of networks and computer systems.

Another aspect that benefited the research was working with port 4444, which uses the Transmission Control Protocol, which is connection-oriented, verifying the link to determine communications from one end to another. Port 4444 guarantees the delivery of data packets in the same order in which they were sent. Once the connection was made, it was necessary to keep the screen active to perform the necessary tests.

Finally, it is confirmed that this study is part of a project created for educational and ethical purposes to detect and mitigate Social Engineering attacks. It is also focused on ex- ploring weaknesses in the security of networks and systems for personal and business use. We use Kali Linux as a tool for forensic analysis, penetration testing, and vulnerability analysis. We try to develop solutions to discover where a computer system has been attacked and find the possible activities carried out by its attacker.

VI. CONCLUSION

This study is focused on demonstrating the vulnera- bilities of the operating systems of mobile devices. Con- sequently, we concluded that the Android system is not safe when installing an APK, and it is vulnerable to being attacked in the form of a backdoor. Thus, it could cause insecurity for users who work with this type of device and damage their integrity, security, and data privacy. It is considered that the Chip.I virus is capable of entering any device with the aforementioned operating system since it is based on the Linux Kernel. It is easily controllable or hack-able, using the commands that were explained during this study. In addition to its easy access to the different types of files, whether hidden or encrypted, also thanks to the tools that Kali Linux has, the attack is more precise and simple through IP networks outside the LAN. Thanks to the different Frameworks such as MSFVenom, Metasploit

through Meterpreter or Ngrok as access server path to it in connection with the Host. So, finally, the research hypothesis is accepted, inferring that the virus is capable of violating security and remaining as a Trojan inside the device, without being detected, unless it has an antivirus, either Avast, AVG, among others, which would be responsible for eliminating it avoiding the attack on the terminal.

As future work, we plan to make a version capable of forcing security and mitigation using Deep Learning to any Android device using a convolutional neural network. Our proposal contributes significantly towards a new version of the security patches for Android in implementing a malware model, which will integrate techniques capable of mitigating it.

ACKNOWLEDGMENTS

The authors would like to thank the financial support of the Ecuadorian Corporation for the Development of Research and the Academy (RED CEDIA) in the development of this study, within the Project Grant GT-Cybersecurity.

VII. REFERENCES

[1] W. Fuertes, F. Meneses, L. Hidalgo, and J. Torres, "RSA over-encryption implementation for networking. A proof of concept using mobile devices", Revista Investigación Operacional, vol. 41, no. 5, Article ID 586598, 2020. Available: https://rev-invope. univ-paris1.fr/fileadmin/rev-inv-ope/files/41420/41420-10.pdf.[Online; Accessed on October 23, 2020].

[2] R. Simpson, "Android overtakes Windows for first time", Statcounter GlobalStats, vol. 3, Abril 2017. Available: https://gs.statcounter.Com8/press/android-overtakes-windowsfor-first-time. [Online; Accessed onSeptember 28, 2020].

[3] M. Costas, "Desarrollo de malware para dispositivos móviles con S.O Android con fines docentes", 2019. Available: http: castor.det.uvigo.es:8080/xmlui/bitstream/handle/123456789/439/CostasPardoManuel.pdf?sequence=1. [Online; Accessed on September 30, 2020].

[4] M. J. Gutiérrez Fernández, "Inyección de malware en aplicación Android legítima", Universidad de Sevilla, 2019.

[5] H. Alawneh, "Android malware detection using data mining techniques on process control block information", Auburn University, Departament of Computer Science and Software Engineering, 2020. Available: http://hdl.handle.net/10415/7390. [Online; Accessed on September 30, 2020].

[6] A. Pérez, M. Montero y V. Pérez, "Android malware detection using machine learning", en XIII Seminario Iberoamericano de Seguridad en las Tecnologías de la Información, Havana, 2018.

[7] J. Cho, G. Cho, S. Hyun y H. Kim, "Open Sesame! Design and Implementation of Backdoor to Secretly Unlock Android Devices", J. Internet Serv. Inf. Secur., vol. 7, pp. 35-44, 2017.

[8] C. A. Venegas Sánchez, "Using Reverse Engineering to Face Malware", Revista IngenieriaSolidaria, vol. 15, no. 28, 2019.

[9] A. Zadjali, B. Mohammed, "Penetration testing of vulnerability in Android Linux kernel layer via an open network (Wi-Fi)", International Journal of Computer Applications, vol. 975, no. 8887, 2016.

[10] S. Raj and N. K. Walia, "A Study on Metasploit Framework: A Pen-Testing Tool", International Conference on Computational Performance Evaluation (ComPE), Shillong, India, 2020, pp. 296-302

[11] D. Rathi and R. Jindal, "DroidMa: A Tool for Android Malware Detection using Taint Analysis and Bayesian Network", International Journal on Recent and Innovation Trends in Computing and Communication, vol 6., no 5., pp. 71-76, 2018. Available: https://arxiv.org/ftp/arxiv/papers/1805/1805.06620.pdf [Online; Accessed on October 24, 2020].

[12] W. Fuertes, J. E. López de Vergara, F. Meneses and F. Galán, "A generic model for the management of virtual network environments", IEEE Network Operations and Management Symposium (NOMS)", 2010, pp. 813-816, doi: 10.1109/NOMS.2010.5488367, 2010. https://www.overleaf.com/project/5f720fce6ae2940001a2b161 [Online; Accessed on September 28,2020].

ISSN: 1390 -9266 – 2020 LAJC

[13] P. Li, "Selecting and using virtualization solutions, our experiences with VMware and Virtualbox", Journal of Computing Sciences in Colleges, vol. 25, no. 3, pp. 11-17, 2009.

[14] Oracle, VirtualBox, Available: https://www.virtualbox.org/manual/ch04.html, [Online; Accessed on September 28, 2020].

[15] Oracle, VirtualBox Home Page, Available at: http:// www.virtualbox.org. [On-line; Accessed on September 28, 2020].

[16] Kali, "What is Kali Linux?, Ofensive Security", 2020. Available: https://www. kali.org/docs/introduction/what-is-kalilinux/. [On-line; Accessed on September 28, 2020]."

[17] Rastreator, "Android overtakes Windows for first time", 2020. Available: https://www.rastreator.com/telefonia/articulosdestacados/el-sistema-operativoandroid.aspx, [Online; Accessed on September 28, 2020].

[18] Kali Tools, "Metasploit Pro User Guide", 2020. Available: https://tools.kali.org/exploitation-tools/metasploit-framework, [Online; Accessed on September 28, 2020].

[19] Offensive Security, "About the Metasploit meterprete", 2020. Available: https://www.offensive-security.com/metasploit-unleashed/aboutmeterpreter/, [Online; Accessed on September 28,2020].

[20]Rapid 7, "Using Exploits", 2020. Available: https://docs.rapid7.com/metasploit/using-exploits/, [Online; Accessed on September 28, 2020].

[21] Z. Mohammed, MSFVenom,21 Abril 2020. Available: https://medium.com/@mzainkh/msfvenom-b57267a5bd9d, [Online; Accessed on September 28, 2020].

[22] ApacheCon, "The number one HTTP Server on the Internet, Apache HTTP Server Project", 2020. Available: https://http.apache.org/the-number-one-httpserver-on-the-internet, [Online; Accessed on September 28, 2020].

[23] Ubuntu Server, "HTTPD-Apache2 Web Server", Canonical, 2020. Available: https://ubuntu.com/server/docs/web-serversapache, [On- line; Accessed on September 28, 2020].

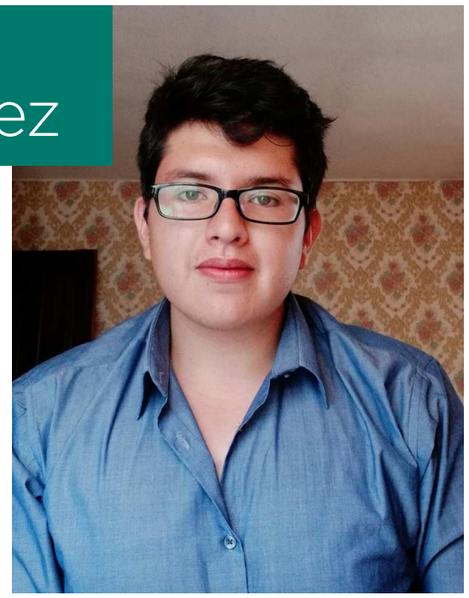
[24] Welivesecurity, "¿Sabes qué es un backdoor y en qué se diferencia de un troyano?", ESET, Abril 2015. Available: https://www.welivesecurity.com/la-es/2015/04/17/quees-un-backdoor/ [Online; Accessed on September 28, 2020].

[25] M. Sweeney, "Decompile and modify APKs on the go with APKTool for Android [XDA Spotlight]", xda-developers, Marzo 2017. Available: https://www.xda-developers.com/decompile-and-modify-apks-on-thego-with-apktool-for-android/ [Online; Accessed on September 28, 2020].

[26] E. Benavides, W. Fuertes, S. Sanchez-Gordon, and M. Sanchez, "Classification of Phishing Attack Solutions by Employing Deep Learning Techniques: A Systematic Literature Review", in Rocha A. and Pereira R. (eds) Developments and Advances in Defense and Security. Smart Innovation, Systems and Technologies, vol. 152. Springer, Singapore, 2020. DOI https://doi.org/10.1007/978-981-13-9155-2 5 [Online; Accessed on October 23, 2020].

AUTHORS

Carlos Andrés Estrada Vásquez

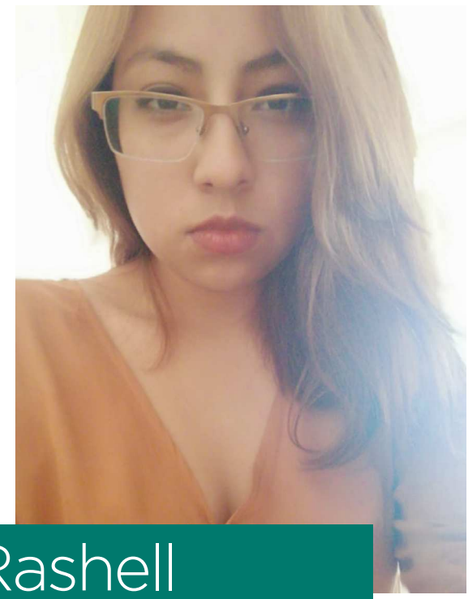


Was born in Quito, Ecuador. Currently, he studies Information Technology Engineering at the Universidad de las Fuerzas Armadas ESPE at Sangolqui-Ecuador. Also, he is a research assistant in the School of Computer Science. Andres is interested in learning and researching by himself in computer science, artificial intelligence, information security, computational mathematics. He has done different courses in Data Analytics and Machine learning through virtual platforms such as Coursera or edX, also he has done courses in computer vision, artificial intelligence, and Python for Data Mining in the Bootcamp IEEE."

Walter Fuertes

Was born in Arenillas, El Oro, Ecuador. Currently, he works at the Universidad de las Fuerzas Armadas ESPE in Sangolquí, Ecuador. He is a full professor (lecturer-researcher) in the School of Computer Science, where he received an engineering degree in Computer Systems in 1995. Later, he received his master's with a science degree in Computer Networking from the Escuela Politécnica Nacional in Quito, Ecuador, in 1999 and the Ph.D. (Hons.) degree in Computer Science and Telecommunications engineering from the Universidad Autónoma de Madrid, Spain in 2010. Since 2006, he has actively participated in several research projects focused on applying virtualization technologies, data sciences, microservice architecture, and cybersecurity. His research interests include managing distributed environments, network security, cybersecurity, the applied research of virtualization technologies, and serious games.

ISSN: 1390 -9266 – 2020 LAJC



Amy Rashell Sánchez Cárdenas

Amy was born in Quito, Ecuador. She is currently studying at the Universidad de las Fuerzas Armadas ESPE in Sangolqui, Ecuador. She is a full-time student at the College of Computer Science, where she is studying to receive an engineering degree in Information Technology. She has a great interest in learning and researching in the different fields of information technologies applied in psychology, computer security, virtual reality, augmented reality, among others.