ISSN 2085-4552

Methods of Stealing Personal Data on Android Using a Remote Administration Tool with Social Engineering Techniques

Ridwan Satrio Hadikusuma[1], Lukas[2], Epril M Rizaludin[3]
[1,2]Electrical Engineering Master Departement, Universitas Katolik Indonesia Atma Jaya, Jakarta, Indonesia
[3]PT. Klik Digital Sinergi, Jakarta, Indonesia
[1]ridwan.202200090017@student.atmajaya.ac.id, [2]lukas@atmajaya.ac.id, [3]epril_mohamadrizaludin@klik-ss.com

Accepted 24 March 2023
Approved 28 June 2023

***Abstract*— IT security is a significant concern of the internet because almost all communication occurs today. The purpose of testing personal data theft with the social engineering method is to ensure that the system and network on the user's Android have security holes to be hacked if the user is not aware of social engineering that allows data theft through the remote administration tool (RAT) which is accidentally downloaded on the Android User. Installing a RAT by applying social engineering is the possible and proper way to steal Android user privacy data. This study outlines some basic concepts of data theft, from recent call data and personal data to controlling Android users' cameras and microphones remotely.**

***Index Terms*— RAT; security; social engineering**.

I. INTRODUCTION

One of the most significant inventions in human history that have changed how we do things is the Internet. The Internet has changed how we communicate, do business, and interact with each other[1-2]. Today, people no longer have to wait to hear from someone because they can communicate easily through the Internet. The Internet has also enabled businesses and individuals to receive payments instantly and track their fleets and cargo [3]. Security and information technology are increasingly important to society and the ICT(Information and Communication Technology) industry in this modern era. Security experts have developed various high-performance security tools to ensure that information on the Internet remains safe and not vulnerable to attack [4]. Various techniques, such as Layered Design, Assurance or Proof of Correctness, Software Engineering Environment, and Penetration Testing, test a complete, integrated, and reliable software, hardware, and people operational computer base[5, 6].

One example is using open-source frameworks such as Metasploit for exploit creation and penetration testing, which comes with over 1,600 exploits and 495 payloads to attack computer networks and systems. No matter how strong an android's security system is, it can still be penetrated if the user is still easy to manipulate, especially using social engineering methods. Social engineering is a manipulation technique that exploits human error to access private information or valuable data [7-9]. In the world of cybercrime, this type of human hacking scam can lure unsuspecting users. The most common is manipulating Android users to install an application (possibly under the guise of an e-ticket, package delivery receipt numbers for tracking, to other deceptive applications), where these applications are remote administration tools used for personal data theft [10][11]. Remote addressing tools android hacking is a technology that allows someone to remotely access an Android device without having to be near the device. Hackers use remote addressing tools to exploit vulnerabilities or loopholes in the Android security system to access the device and gain access to sensitive data such as photos, text messages, or financial information [12, 13].

Hackers use remote addressing tools (RAT) for malicious purposes such as data theft, extortion, or other criminal activities. However, this technology can also be used positively, for example, to help Android device owners who have forgotten their passwords or pins or to monitor people who need help, such as children or the elderly [14]. It is important to remember that using remote addressing tools for unethical purposes can compromise the privacy and security of one's Android device. Therefore, keeping your Android device safe is essential by installing the latest security apps, updating the operating system regularly, and avoiding downloading apps from sources you do not trust. This article will discuss some of the most frequently used remote addressing tools in Android hacking and how to protect your Android device from these threats.

II. METHODOLOGY

Before the authors conduct research, the authors conduct several literature studies from several related studies that are still relevant to the research to be conducted. one of them is research conducted by

Huang, Y., & Han, X. [15] in his research entilted "Security Analysis of Remote Administration Tools for Android Devices". In this study, the researchers analyzed the security of six popular remote administration tools for Android devices, and found that these tools are vulnerable to social engineering attacks. this is also in line with research conducted by Iliyasu, A. M., & Ahmad, M. O [16] in his research related to "A Comprehensive Study on Android Remote Administration Tools: Threats, Vulnerabilities and Countermeasures". In this study, the researchers conducted a comprehensive analysis of Android remote administration tools, and identified various threats and vulnerabilities associated with these tools. The researchers also proposed a set of countermeasures to mitigate these risks.

Different from what Prakash, S., & Jadhav, S [17] did in an article entitled "Social Engineering Attacks in Android Platform. 2018 International Conference on Intelligent Computing and Control Systems (ICICCS)". In this study, the researchers analyzed the various social engineering attacks that can be used to exploit vulnerabilities in Android devices, and proposed a set of countermeasures to prevent such attacks. there is another study entitled "A Study on Remote Administration Tools and Their Impact on Android Devices" conducted by Ravikumar, N., & Gokulnath, C [18]. In this study, the researchers analyzed the impact of remote administration tools on Android devices, and identified various security risks associated with these tools. The researchers also proposed a set of countermeasures to mitigate these risks. Finally, what is interesting for the author's research in conducting this research is in research entitled "A Review on Security Threats and Countermeasures for Android Remote Administration Tools" conducted by Singh, G., & Kapoor, S [19]. In this study, the researchers conducted a review of the security threats associated with Android remote administration tools, and proposed a set of countermeasures to prevent these threats. The researchers also discussed the importance of user education in preventing social engineering attacks.

III. Research Method

The research method on remote administration tools Android hacking using social engineering can be done in several stages. First, researchers must select and identify the types of remote administration tools used on Android devices. Then, the researcher must identify the security vulnerabilities in each remote administration tool. After that, researchers must conduct trials of each remote administration tool by carrying out attacks by exploiting the security holes found. In this case, researchers will use social engineering techniques to trick Android device users so that they can install remote administration tools unknowingly. After successfully installing the remote administration tools on the Android device, researchers will conduct testing and analysis of the data successfully retrieved from the Android device. Furthermore, researchers will evaluate the results of the tests and analyses carried out and provide recommendations regarding actions that need to be taken to improve the security of Android devices from attacks using remote administration tools and social engineering. Briefly, the flow of this research is described in Figure 1 below.

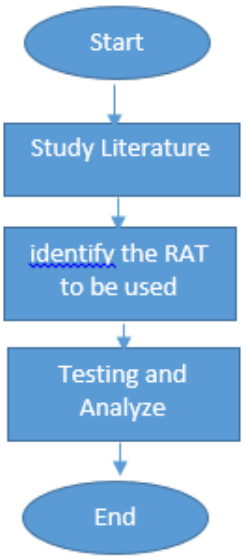

Fig. 1. Research Flowchart

A. Determination of Remote Administration Tools

Installing remote administration tools on the Kali Linux operating system can be done by downloading the installation package according to the operating system and architecture used. After that, the installation package can be installed on Kali Linux using the appropriate installation commands. However, remember that using remote administration tools in hacking activities is illegal and can violate privacy and harm others. Therefore, remote administration tools must be used with good ethics and pay attention to security and privacy aspects. In addition, using Kali Linux must be done for good and legal purposes, such as conducting security tests on a system or network owned or with permission from the owner of the system or network.

Determining remote administration tools for Android hacking can be done by looking for references from various sources, such as underground forums, websites, or blogs about information security, or using a unique search engine such as Shodan. Then, it is necessary to evaluate the tools found in terms of functionality, capability, security, and the legality of their use. Data collection methods related to Android hacking remote administration tools can be done using scanning and enumeration techniques on the target system or network. This can be done using special tools like Nmap, hoping, or the Metasploit framework. In

addition, using tools such as Wireshark can also assist in collecting data related to network traffic that occurs when using remote administration tools on the target.

B. Social Engineering Techniques

Social engineering methods of installing RAT applications can be carried out in various ways, such as creating fake messages or emails that look genuine, creating websites or pages that mimic the appearance of official sites, or using other tactics that trick the target into downloading and installing applications that contain malware. These techniques usually involve psychological manipulation of the target, such as making fraudulent offers or promises, intimidating or threatening, exploiting curiosity, and taking advantage of the target's trust or ignorance. It is important to remember that these actions are illegal and may harm others. Therefore, it is crucial for technology users always to be vigilant and careful when obtaining information or downloading applications from unknown sources. In addition, it is also essential to update the device security system and use the latest security software to avoid harmful malware attacks.

C. Methods of Data Collection and Prevention

Collecting personal data using hacking remote administration tools (RAT) on Android devices can be done in various ways. One common way is sending malicious applications embedded with RATs to the target device. Once the application is installed on the target device, RATs can collect personal data such as text messages, phone calls, and browsing history. In addition, RATs can also be used to take control of the target device, such as activating the camera or microphone and recording user activity without their knowledge. Another method is to use phishing techniques, such as sending fake messages or emails that trick users into providing their personal information or clicking on links containing malicious applications embedded in RATs. In addition, users can also become victims of RATs attacks through unprotected Wi-Fi networks or applications that are vulnerable to attack, such as banking or e-commerce applications [7].

Therefore, it is essential for Android users always to be careful and avoid downloading apps from untrusted sources and using protected and trusted Wi-Fi networks. In addition, users are also advised to use security applications to monitor and protect their devices from RATs and other malware attacks. Android's fairly tight security system protects its users from remote administration tools (RAT) attacks and other malicious applications. One way to increase Android security is to activate security features provided by the operating system, such as a password or PIN, fingerprint sensor, or screen pattern lock settings [20]. In addition, users are also advised not to download applications from untrusted sources or use antivirus applications to identify and block malicious applications. Suppose you suspect that RATs or other malicious applications have infected your Android device. In that case, the first step is to remove the application from the device and perform a system scan using an antivirus. Also, it is recommended to continuously update the Android operating system to the latest version and avoid using unprotected or untrusted Wi-Fi networks. By paying attention to these security measures, Android users can minimize the risk of attacks by RATs and other malicious applications and protect their privacy and personal data.

TABLE I. ACCEPTANCE LEVEL CATEGORY INTERVAL

Percentage Interval	Acceptance Level Category
0% - 20%	Strongly Disagree
20.01% - 40%	Disagree
40.01% - 60%	Uncertain
60.01% - 80%	Agree
80.01% - 100%	Strongly Agree

IV. RESULTS AND DISCUSSION

A. Operating System Installation and Remote Administration Tools Identification Results

Kali Linux is a distribution specifically designed for penetration testing, including in android hacking. Kali Linux has several advantages in its use that make it easier for practitioners to do hacking. One of the advantages of Kali Linux is that it is equipped with a variety of complete hacking tools. Hence, users no longer need to install additional tools manually. Apart from that, Kali Linux also has an intuitive user interface so that users can efficiently operate the system and the tools provided. Another advantage is modifying and customizing the tools according to user needs through manual configuration or built-in features such as meta-packages. Thus, Kali Linux is one of the right choices for android hacking practitioners in conducting security testing on the Android system. Here are the Kali Linux installation steps [11]:

1. Download the Kali Linux ISO file from the official Kali Linux website.
2. Prepare an empty USB flash drive with a minimum capacity of 4 GB.
3. Download and install the Rufus application to create a bootable USB. Open the Rufus application and select the USB flash drive to use.
4. In the "Boot selection" section, click the "SELECT" button and select the Kali Linux ISO file downloaded in step 1.
5. Ensure the USB flash drive partition is in "MBR" mode, and the file system is "FAT32".
6. Click the "START" button and wait until the bootable USB creation process is complete.

7. After the process, insert the USB flash drive into the computer where Kali Linux will be installed.
8. Set the BIOS settings to boot from the USB flash drive the first time. The method depends on the type and brand of your computer or laptop.
9. Select the "Graphical Install" option on the Kali Linux boot menu after successfully booting from the USB flash drive.
10. Follow the on-screen installation instructions, including selecting the language, time zone, and hard drive partition to use.
11. Select the root password setting and create a new user account.
12. Wait for the installation process to finish. Once done, Kali Linux is ready to use.

Installing Kali Linux requires basic knowledge of the operating system and BIOS settings. Therefore, ensure you understand the instructions and the associated risks before starting the installation process. Another alternative in Linux installation is to use a virtual machine (virtual server) to run the operating system.

After the operating system is installed, the next step is to determine the RAT that will be used. the author uses AhMyth as a RAT which will be used to commit personal data theft. AhMyth is a popular Android hacking tool and relatively easy to use on Kali Linux. Here are the steps to run AhMyth on Kali Linux [18]:

1. First, ensure that Kali Linux is installed and updated with the latest version.
2. Then, open the terminal on Kali Linux and run the command "git clone https://github.com/AhMyth/AhMyth-Android-RAT.git" to download the AhMyth source code from GitHub.
3. After successfully downloading, enter the AhMyth directory with the command "cd AhMyth-Android-RAT".
4. Next, run the command "sudo sh AhMyth.sh" to start the AhMyth installation process on Kali Linux.
5. Wait for the installation process to finish, and after that, open AhMyth by typing the command "sudo sh ahmyth".
6. After AhMyth opens, users can start creating an Android application that will be injected with the AhMyth payload. To do so, users can follow the instructions available on AhMyth.
7. Once done, AhMyth is ready to hack the target Android device.

However, remember that unauthorized use of AhMyth on devices not belonging to the user is illegal and can result in serious legal consequences. Therefore, AhMyth must be used ethically and comply with applicable regulations. As for AhMyth's appearance as shown in Figure 2 below.

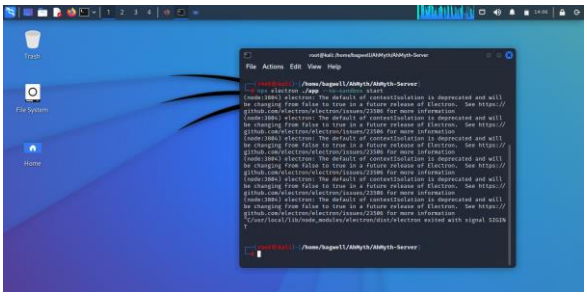

Fig. 2. Display the AhMyth RAT and run the server command

B. Results of Social Engineering

After the RAT is deployed into an application, the next step is manipulating the target to install the RAT application on their Android device. Various ways can be done, such as sending e-tickets and package delivery receipts to government assistance programs, as shown in Figure 3 below.

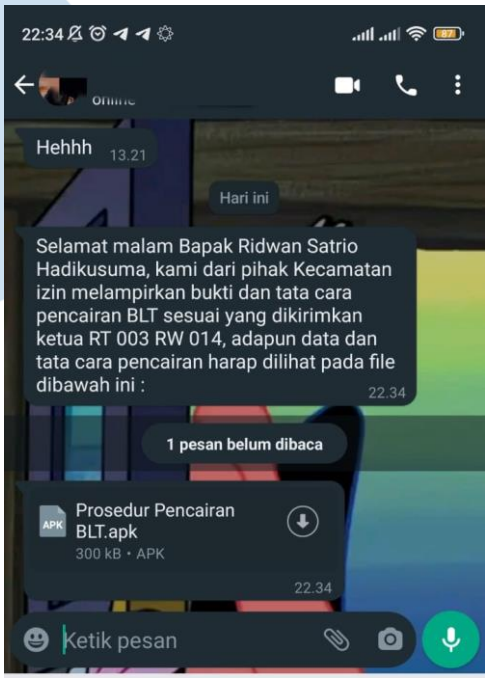

Fig. 3. Social Engineering Results

When doing social engineering to get someone to install Remote Administration Tools (RAT) on an Android device, it takes some persuasive skills to convince the victim. First, an aggressor needs to know about the victim's interests and wants. Furthermore, the attacker can create a scenario to interest the victim and make him interested in installing the RAT application. One trick often used is to promise an attractive offer, such as a free application or a premium service at a low cost. Attackers can also use phishing techniques by sending fake emails or text messages that look genuine and offer an attractive application or service. In addition, attackers can also take advantage of the

victim's fear or worry about the security of Android devices.

Attackers can promise better device security by installing a RAT application when in fact, the application is dangerous malware. To ensure success in getting someone to install the RAT application, the attacker needs to master effective and creative persuasive techniques and constantly update and improve these techniques so that they can always trick the victim. However, it is essential to remember that such actions are illegal and can cause harmful effects on others and, therefore, should not be carried out.

C. Results of Personal Data Theft

After the RAT is installed on the target device, the author can find the country, device type, and IP used, as shown in Figure 4. Since the first installation, all user data on the Android device can be accessed and fully controlled by the author (also in this research, the target is part of the author and already with permission).

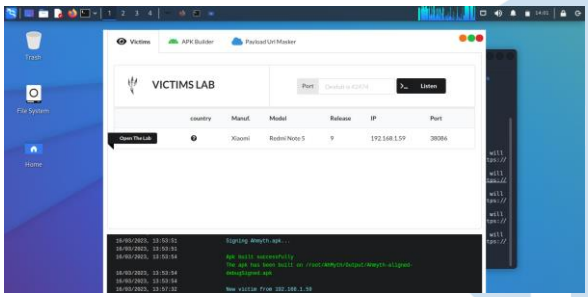

Fig. 4. Device information from the attacker side

The first data result is that the author steals or takes contact data stored on the target android device (see figure 5). the contact data can be used for various things, such as being sold to online gambling sites for marketing needs, fraud, and many other digital crimes.

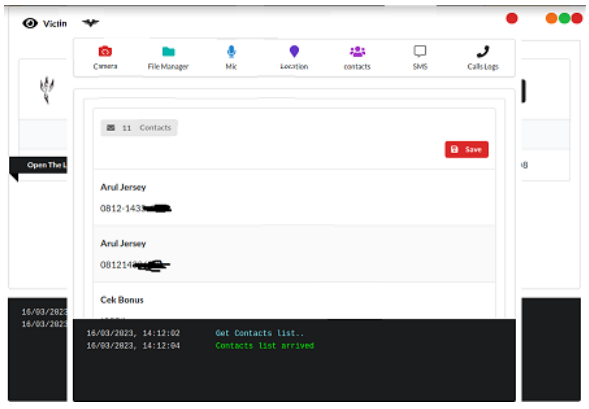

Fig. 5. Contact information is stored on the target device

The author also managed to hack the camera, microphone and real-time location of the target android device, which can be controlled 24 hours a day, as shown in Figure 6 and Figure 7.

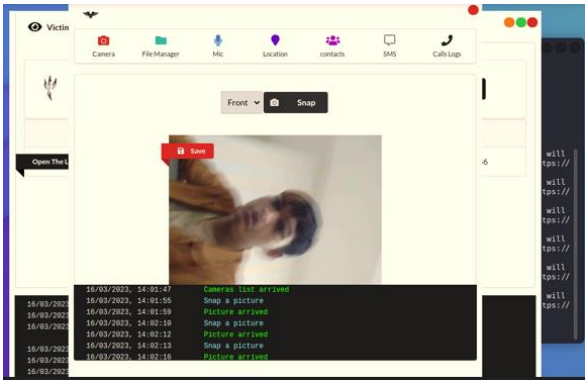

Fig. 6. The author view currently controlling the target android device's camera

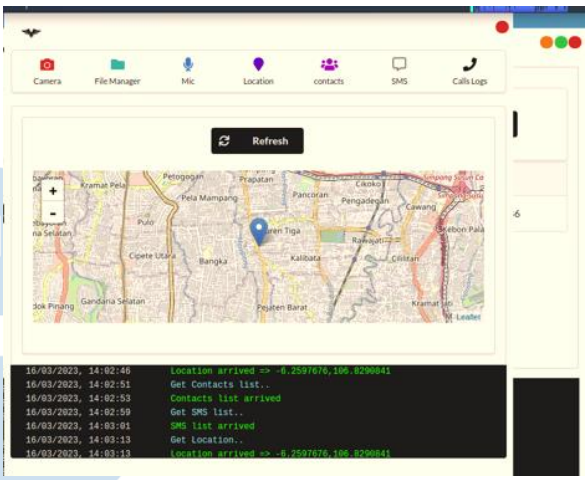

Fig. 7. Author display in monitoring the real-time location of the target device

Finally, the author can access all storage files from the target android device as a whole, starting from photo and external storage files to the android system files themselves (see fig. 8). Of course, this crucial data can be used for various digital crimes, the most dangerous of which is hacking an M-Banking account installed on a user's device.

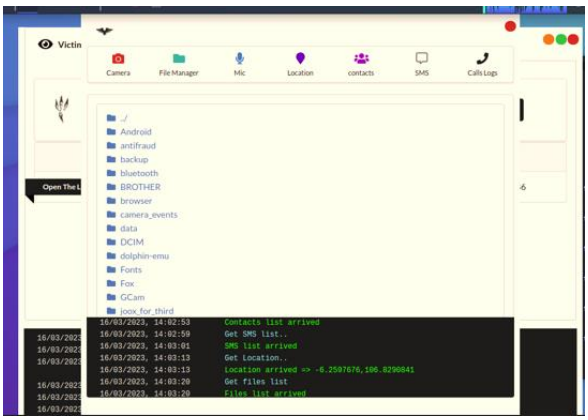

Fig. 8. Monitoring of target android device folder from author side

V. CONCLUSION

Based on the research that has been done, the use of social engineering techniques in installing Remote Administration Tools on Android devices is very effective. In this study, researchers convinced respondents to install applications containing Remote Administration Tools by making convincing fake messages or phone calls. In addition, the research results also show that security on the Android system is still very vulnerable to Remote Administration Tools attacks that can take over the device remotely and collect users' data without their knowledge.

Therefore, it is necessary to take better precautions and safeguards on Android devices to prevent malicious Remote Administration Tools attacks. Some steps to avoid these attacks include downloading apps only from trusted sources, keeping your Android device updated with the latest security patches, and installing reliable antivirus software. Additionally, awareness and education are also needed for Android users to recognize and prevent Remote Administration Tools attacks that use social engineering techniques.

REFERENCES

[1] A. R. Maulana and D. P. Wardhana, "Remote Administration Tool (RAT) Implementation using AhMyth and Social Engineering Techniques," 2020 International Conference on Computer Engineering, Network and Intelligent Multimedia (CENIM), Surakarta, Indonesia, 2020, pp. 1-5, doi: 10.1109/CENIM51083.2020.9317252.

[2] W. R. Pratama and A. F. T. Riyadi, "Uji Penetrasi Remote Administration Tool pada Android dengan Teknik Social Engineering," Jurnal Teknologi Informasi dan Komunikasi, vol. 8, no. 2, pp. 56-62, 2022.

[3] R. H. Putra, M. N. Huda and T. A. Wisesa, "Android Hacking Using AhMyth RAT with Social Engineering Techniques," 2020 4th International Conference on Informatics and Computing (ICIC), Jakarta, Indonesia, 2020, pp. 1-5, doi: 10.1109/IAC50653.2020.9259369.

[4] S. Pradana, D. D. Setiawan and N. E. Darmawan, "Remote Administration Tool (RAT) Implementation using AhMyth RAT and Social Engineering Techniques," 2021 International Conference on Advanced Informatics: Concept, Theory and Application (ICAICTA), Malang, Indonesia, 2021, pp. 1-6, doi: 10.1109/ICAICTA51487.2021.9488906.

[5] S. R. S. Maharjan, S. Maharjan and S. Adhikari, "Social Engineering Techniques and the Use of Remote Access Trojans (RATs) in Android Devices," 2019 4th International Conference on Computing, Communication and Security (ICCCS), Rome, Italy, 2019, pp. 1-6, doi: 10.1109/CCCS.2019.8887181.

[6] R. Agarwal, S. Saha, S. Chaki, "Security Issues and Threats in Android Platforms: A Survey", International Journal of Computer Applications, vol. 52, no. 6, pp. 28-35, 2012.

[7] B. Al-Duwairi, "A Study on Security Issues of Mobile Devices and Applications", International Journal of Advanced Computer Science and Applications, vol. 8, no. 9, pp. 239-244, 2017.

[8] S. Arora, A. Singh, "Mobile Malware Detection: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 7, no. 5, pp. 76-79, 2017.

[9] A. Babar, M. Masood, M. Farooq, "An Analysis of Mobile Malware: A Comprehensive Study", International Journal of Computer Science and Network Security, vol. 15, no. 3, pp. 103-112, 2015.

[10] S. Bhattacharya, S. Kumar, "A Study on Android Malware Detection and Prevention Techniques", International Journal of Computer Applications, vol. 168, no. 5, pp. 8-12, 2017.

[11] K. Chandrakar, S. Bhoi, "Mobile Security: Issues, Challenges and Future Directions", International Journal of Advanced Research in Computer Science, vol. 8, no. 3, pp. 118-123, 2017.

[12] A. Dhiman, S. Sharma, "Security Issues and Solutions for Mobile Devices", International Journal of Computer Applications, vol. 104, no. 12, pp. 21-26, 2014.

[13] N. M. N. Lestari and A. W. Nugroho, "Penerapan Teknik Social Engineering dalam Remote Administration Tools pada Android," Jurnal Keamanan Informasi, vol. 5, no. 1, pp. 12-21, 2021.

[14] D. F. Maulana, R. A. Hidayat, and R. D. Saputra, "Analisis Penggunaan Remote Administration Tool dengan Teknik Social Engineering pada Android," Jurnal Ilmiah Informatika, vol. 10, no. 2, pp. 123-130, 2019.

[15] Huang, Y., & Han, X. (2018). Security Analysis of Remote Administration Tools for Android Devices. 2018 IEEE International Conference on Cloud Computing and Big Data Analysis (ICCCBDA).

[16] Iliyasu, A. M., & Ahmad, M. O. (2021). A Comprehensive Study on Android Remote Administration Tools: Threats, Vulnerabilities and Countermeasures. Journal of Information Security, 12(2), 79-97.

[17] Prakash, S., & Jadhav, S. (2018). Social Engineering Attacks in Android Platform. 2018 International Conference on Intelligent Computing and Control Systems (ICICCS).

[18] Ravikumar, N., & Gokulnath, C. (2016). A Study on Remote Administration Tools and Their Impact on Android Devices. International Journal of Advanced Research in Computer Science and Software Engineering, 6(8), 262-268.

[19] Singh, G., & Kapoor, S. (2018). A Review on Security Threats and Countermeasures for Android Remote Administration Tools. International Journal of Advanced Engineering Research and Science, 5(11), 122-126.

[20] N. Hidayatullah, I. A. Akbar, and R. Kurniawan, "Social Engineering-Based Attack on Android Mobile Device," in 2019 International Conference on Information Management and Technology (ICIMTech), 2019, pp. 82-87.