Media File Jacking Threats and Protections

Shinto Kurian K, K Nirmala

***Abstract**: Media File Jacking (MFJ) is one security threat that affects media file usages within apps. Media files include image files, voice/audio files, video files and document files like pdf, docs, excel sheets, text files, etc. and these files easily find its place within our devices. The primary symptom of a Media File Jacking attack is that it will manipulate the media files, on transferring between users or apps. This type of malwares mainly targets mobile devices. The researchers from Symantec reported that this vulnerability has already found its way into the two top social media messaging apps namely, WhatsApp and Telegram. Not just limited to this, media file jacking can easily target mobile functioning's whilst managing affected media files and its managed media chat apps. This analysis in detail tries to understand the vulnerabilities that devices are left exposed to via Media file jacking and how can protect Android based mobile devise with the help of existing, upcoming, configurable or programmable features. We try to cover in detail on i.) What Media file jacking attack is? ii.) How this vulnerability is created? iii.) Under which scenario this will happen iv.) What are the different types of attacks? iv.) What are the implications of this attack? v.) what are precautionary measures and how we can mark safe our mobile devices from this attack. This study mainly help to Android media app users and app develops to get a glance about the precautionary measures from media file jacking attack.*

***Keywords** : Android, Media File Jacking (MFJ), Operating System, Social Media Apps, Telegram, WhatsApp.*

I. INTRODUCTION

Media File Jacking is one of the potential threats that social media apps are exposed to on media file transfer. Cyber criminals capitalize on the flaws within social media apps and manipulate the media files such as photos, voice messages, videos, documents, etc. for their personal benefits. The whole process occurs in a short span of time, the timespan ranging between the storage of media file to the device and accessing the same by an App stored in the device. The reason behind this threat is that media files are normally stored in external storage or common access locations, which can easily be accessed by Apps within the device. When a person sends a media file, it gets manipulated even before the recipient has to access the file. This threat is more prone in devices with Android operating system.

Many of the social media apps has implemented multiple features to enable data security, like data encryption, PIN, passwords, etc. and it so happens that the features get bypassed via MFJ. Major social media apps like WhatsApp, Telegram, Snapchat, Viber, etc has already reported MFJ threat. The attack in majority of the instances are so discrete that the actual user often fails to detect faults and rogue performance within the operating system. To sum it up, the MFJ attack intensifies when we come to realise that most of the media files have permission to access external storage, common to all the apps.

Now to draw a path on how the affected file traverses within systems (Fig 3), the media files received through social media apps, first gets stored in the phone device. Malwares present in the device manipulates the files based on preprogramed requirements and placed in the same access location. While users access files in their device, they accidentally stumble up on these affected files without realisation. These types of attacks can thereby spread fake information or news, enable wrong financial transactions, and even more.

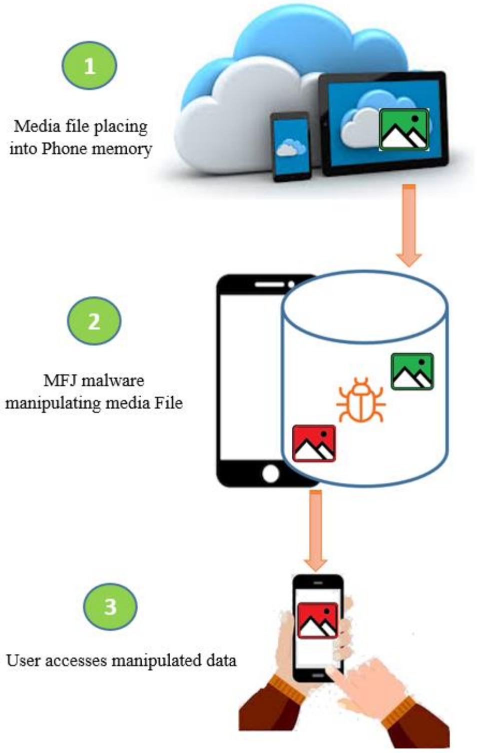

1
Media file placing into Phone memory
2
MFJ malware manipulating media File
3
User accesses manipulated data

Fig 1 – Media File Jacking

Revised Manuscript Received on April 25, 2020.

* Correspondence Author

Shinto Kurian K*, Research Scholar, Quaid-E-Millath College for Women, Chennai, Tamilnadu, India. Email: shintokuriank@gmail.com

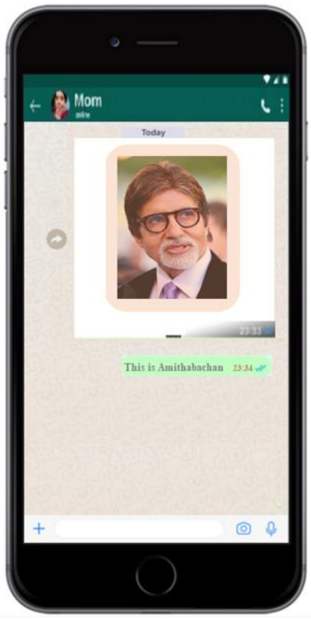
Dr K Nirmala, Assoc. Professor, Quaid-E-Millath College for Women, Chennai, Tamilnadu, India. Email: nimimca@yahoo.com

II. TYPES OF MEDIA FILE JACKING

Based on media file types, mainly there are four types of MFJ malwares or malicious apps present. Intentions of these files are interrelated, basically to twist the actual information. Few of them are using it for entertainment purpose, which has less impact, but many more are for targeted purposes like financial theft, crucial data manipulation which has bigger impacts.

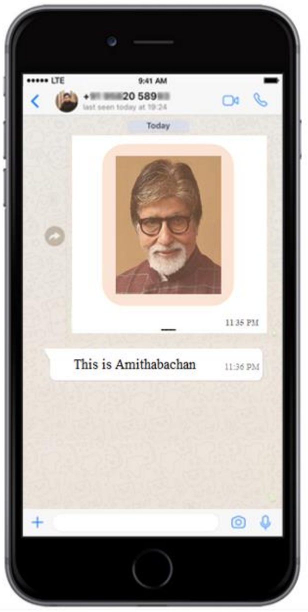
A. Image Manipulation

This type of MFJ malware app run in background and edit the images even before the receiver has to access the file in social media application. The below WhatsApp images explains the flow of image manipulation MFJ threat. In the first image (Fig - 2), the first user shares a photo to second user. Before the second user is to open that file, the malware app residing in the device of the second user access the image and edits and alters the actual photo. When the second user open the image, he will view an entirely different photo compared to the source image (Fig - 3). In the below instance, the malware edited original photo and place a different one. This type of MFJ attack might not be severe, even though it spreads wrong information. Assume an instance where the malware is to change the critical architecture or design diagrams which user sends through media apps, the situation scales.



This is Amithabachan 23:34

Fig 2 - WhatsApp Sender



This is Amithabachan 11:36 PM

Fig 3 - WhatsApp Receiver

B. Audio Manipulation

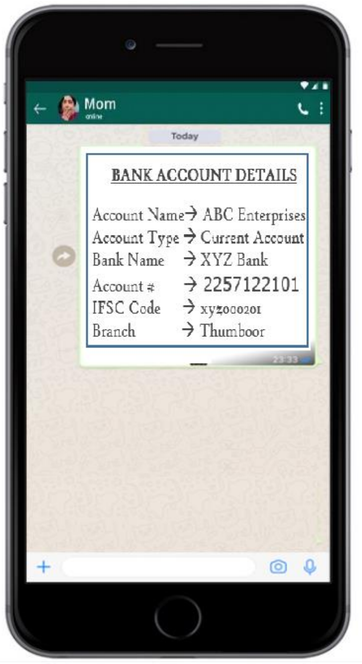
Another technique is the method of audio manipulation where original voice file gets altered and is replaced with fake voice/audio file which is misleading. This replacement happens before the receiver hears the voice or audio in social media app. Top leading information technology providers like Microsoft, Google, Amazon provides a huge repository of APIs to manage the audio files. Nowadays most of the APIs are available as cloud services and can easily be accessed from anywhere leaving users vulnerable to attacks.

C. Video Manipulation

Video manipulation is next in the list, here the original video file gets replaced and altered with videos of similar or twisted content, sometimes for entertainment purpose but otherwise can be deceptive. Hackers utilise the latest technologies like AI, Machine learning, deep learning features to enable such features. When the receiver opens the video file, they view the edited file instead of the original one.

D. Documents Manipulation

The most common and intimidating risk among file jacking are the documents manipulation technique. Here the hacker edits the original documents and places an edited one. The document file type could be pdf (portable document format), docx (Microsoft word file), xlsx (Microsoft excel file), txt (text file) or any other kind of article format. The below WhatsApp screenshots explains the impact of the MFJ threat. In the first image (Fig - 4), the first user sent bank details in a pdf file to second user. Before the second user opens that file, the malware app residing in the device of second user, accesses that file and edits the document. When the second user opens the file, he/she views the edited picture. In the below instance, the malware edited the account name and account number (Fig - 5).

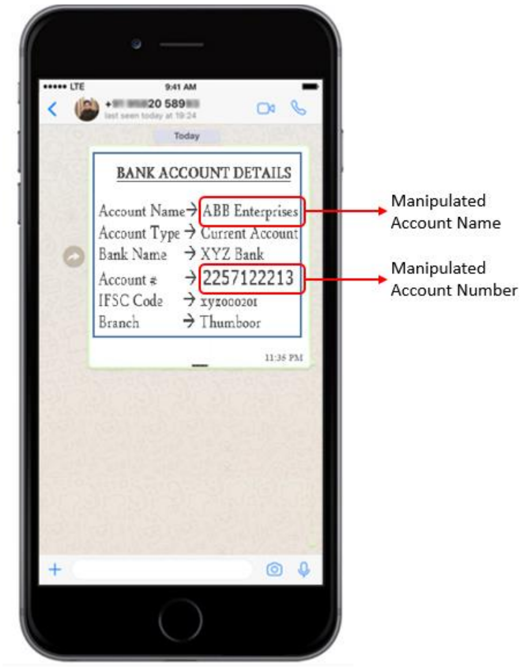


BANK ACCOUNT DETAILS

Account Name→ ABC Enterprises
Account Type → Current Account
Bank Name → XYZ Bank
Account # → 2257122101
IFSC Code → xyz000201
Branch → Thumboor

23:33

Fig 4 – WhatsApp Sender



••••• LTE 9:41 AM

+[redacted]20 589[redacted]
last seen today at 19:24

Today

BANK ACCOUNT DETAILS

Account Name → ABB Enterprises
Account Type → Current Account
Bank Name → XYZ Bank
Account # → 2257122213
IFSC Code → xyz000201
Branch → Thumboor

11:36 PM

Fig 5 – WhatsApp Receiver

III. IMPACTS OF MEDIA FILE JACKING

Media file jacking mainly targets mobile devices because they are more commonly used to transfer media files, also provided the vast variety of apps available in Android platform for mobiles. Below we outline the main MFJ attack areas.

A. Spread fake information

Fake information always create social nuisance. Image, audio and video manipulation file jacking spreads fake news and pass false information and between the people and society.

- Lose the opportunities - Lack of right information leads to losing the right opportunities to seize up on for the user
- Spoil the social status - Few of these techniques deploy vulnerable features, to damage social status of chief personalities.
- Wrongly using for marketing - Targeted social media marketing for wrong activities and illegal business is another area left open by these attacks
- Wrong social campaign - Nowadays social media apps play vital role in different types of social campaign. Few of them uses this feature wrongly and passes false information and creates social nuisance
- Deny Govt rules and regulations - Few protestors make use of this vulnerability to protest against government rules and regulations

B. Financial theft

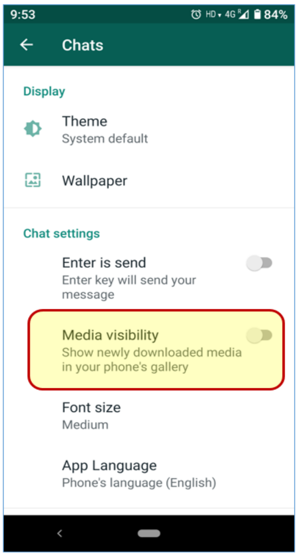
Hackers deploys MFJ malwares for financial exploitation, mainly document manipulation as well as image manipulation. They utilize the social media apps to exploit the loopholes for financial benefits. Forged information in financial transaction always make financial loses to the device users. In a convenient way few of them uses the social media apps like WhatsApp to message bank information for money transactions, hackers are targeting these opportunities to make steal financial information

IV. PRECAUTIONARY MEASURES

Around 98% of mobile phone users have Android or iOs operating systems. Media file jacking is more prominent in Android Operating system and as for iOS, the environment has comparatively better memory management mechanism to prevent this threat. Below are the main precautionary measures that can be implanted in Android OS and social media messaging applications to prevent MFJ.

A. Enable app based security features

Whatsapp and Telegram are the two key android applications affected by MFJ threat. Both applications provide security features to limit or restrict the media files accessibility for other installed applications in the device. Below screenshots explain how we can enable the security feature, Fig-6 shows the option in WhatsApp and Fig-7 shows the option in Telegram. These features provide a rapper in top of media files and restrict the media file access from malware apps, but this alone does not provide for 100% access protection.



9:53 HD 4G 84%

Chats

Display

Theme
System default

Wallpaper

Chat settings

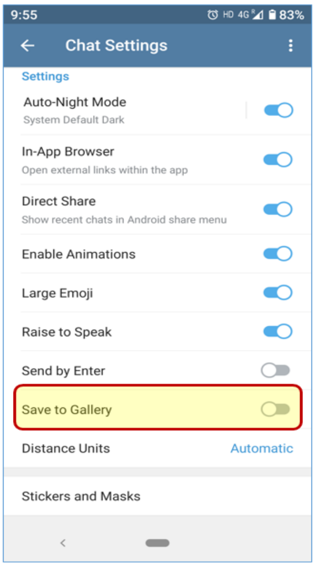
Enter is send
Enter key will send your message

Media visibility
Show newly downloaded media in your phone's gallery

Font size
Medium

App Language
Phone's language (English)

Fig 6 – WhatsApp settings



9:55 HD 4G 83%

Chat Settings

Settings

Auto-Night Mode
System Default Dark

In-App Browser
Open external links within the app

Direct Share
Show recent chats in Android share menu

Enable Animations

Large Emoji

Raise to Speak

Send by Enter

Save to Gallery

Distance Units Automatic

Stickers and Masks

Fig 7 – Telegram settings

B. Scoped Storage

Scoped storage is one of the key features introduced by Google in Android 10 (API Level 29) and later operating system versions. This feature provides the option to restrict external storage access. Once this feature is enabled, each application can access only specific clustered folders and these clustered folders cannot be accessed by other applications. This feature helps prevent malwares access to application storage area.

Now it is not mandatory to implement this feature at an application level, but as per Google's direction by end of 2020 this facility will be added as a mandatory feature. When the media files get placed in the scoped storage area, access for external apps will get restricted.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication
© Copyright: All rights reserved.

C. File integrity check

This is one of the recommended features for mobile apps, which provides secured data management. App developers has to implement this option to their application. Whenever any media files come to the application, a hash value gets added to metadata. The process flow is, first update the hash value in the metadata, and then place the actual file in the phone storage area. While the user opens the application and access any file, validates the hash value against metadata and identifies whether any infringement has happened on that particular file.

D. Encryption:

Encryption is most common methodology adopted for enabling security. Many of the mobile apps already use this mechanism for secured data transfer. Social media apps like Whatsapp and Telegram have already implemented this functionality, but the current implementation is not enough to make these applications secure from MFJ threats. Whatsapp encrypt and decrypt the data at both senders and receivers end, but MFJ attack takes place during the time period between the transfer and reception of the file at receiver's end. Therefore, one has to extend the decryption feature to receiver's end i.e. till the user opens the media files.

E. Password protection

Password protection is another data security mechanism. This feature is mainly used to protect each individual file. Few of them uses this mechanism while sharing any critical data between mobile devices and social media apps and thereby each file gets locked with a password at sender side, which then has to be shared with the receiver in a separate thread. Receiver has to open the file using the shared password.

F. Avoid Media file scanning

In Linux operating system, any folder that starts with a dot(.) character would reside in a hidden folder. For android operating system working on top of Linux kernel, those folder names starting with dot would also remain hidden. Normally hidden files will not be listed out during media file scanning. Therefore if we can keep the WhatsApp or Telegram media folders to start with a dot character, it will not be visible in media file scanning (eg:. WhatsApp Images, Telegram Videos). Avoiding media file scanning is not a real option to protect the media files from MFJ attack but it helps disable a direct fetch or view of media files from other apps.

V. RESULT AND DISCUSSIONS

Media file jacking vulnerability tied up with mobile apps from long back. Symantec research team identified and reported this vulnerability in second quarter of 2019 in in their security reports. Many of them already started more studies on this subject to bring a secured a media file storage feature. Android OS manufactures (Google) released initial version of media file security features called scoped storage along with Android 10 (API level 29). This facility is a key feature they introduced to resist the MFJ vulnerability. Scoped storage feature is not only enable the media file security features but also other security features. Android target to enable scoped storage as key and mandatory security feature from in end of 2020 mostly with Android 11. In this study analysed and illustrated different possibilities to happen the MFJ attack, different forms for MFJ vulnerabilities, impacts and precautionary measures of this vulnerability. Result of this study, here list down different proposals to be incorporated and enabled in mobile apps to prevent MFJ attacks. Table -1 explains these proposal compare with existing features.

Table 1 - Existing Vs Propose methodology

Sl #	Issue	Existing Methodology	Proposed methodology	Responsible
1	Apps are not provide the media file security features. This feature should be available in app level settings	If the application storage not mentioned specifically in app level, the files would store in default path based on content type. In Android OS, the file access would enabled to everyone by default.	All the apps should mandatory provide the application level security features to store the files in secured way. These features should be available in app level settings and users able to enable or disable based on their needs.	App developers
2	Apps are not enabled the application level security features.	Application levels security features are available in app settings but device users are not enabled those.	Enable app based security features in app settings.	Device users
3	Media Content type files not having option to store in isolated memory location to restrict the external access	Normally all apps store the secured files in internal storage. Based on current Android OS level settings, the files, which stored in internal memory can protect from other application access except media files.	Android recently introduced a new feature called scoped storage. Currently most of the apps not implemented this feature. Enable this feature helps to provisioning using the clustered memory storage feature. Media files also can store secure using this feature	Developers and OS manufactures
4	Lack of file integrity check	None of the messaging apps use file integrity check options to protect media files, all the apps are storing the media files in common access storage	An app level feature should provide to enable or disable the file integrity check based on hash values as mentioned in above section.	App developers

5	Encryption not effectively using against MFJ attack.	Many apps already using encryption features while transferring the files between the apps. But it's implementation only till app level transfer, not extended till the user open the files. Normally the receiver app decrypt the data when it's reached in receiver end.	To protect the threats happens between the file received in app side and open from user end like MFJ attack; decrypt the data only when the user open the file.	App developers
6	Password protection feature is not available in apps	Most of the apps not provides the password protection option in file level.	Provide the Password protection as desirable option in app level, so when user transfer a secured file they can use this feature.	App developers and OS manufactures
7	All media files are reachable in Media file scanning	None of the messaging apps providing media file scanning restriction option	Provide an app level desirable feature to restrict the media file scanning.	App developers

VI. CONCLUSION

Media file jacking is a moderate threat for mobile device users and it mainly affects social media messaging apps. This study precis the different types of MFJ attacks and listed out the precautionary measures a user can adopt. Mobile device users, who utilises social media messaging apps for their official work or personal work or business-related activities, strictly has to enable MFJ security measures for avoiding the above listed threats. For convenience many of them use personal mobile device for official purposes, and only a very few enable the security measures. Sometimes MFJ attacks are so intense that it often affects the financial transactions. This study recommends below options to mobile app users and respective develops.

- Media app develops has to provide specific secured media file management options like scoped data storage, file integrity check, secured media file storage, external app accessibility restriction options in application settings.
- Media chat app uses must enable the app specific security options in the application settings like scoped data/file storage, secured media file storage features, encryption and password protection, etc.

Mobile users who rely on mobile apps for financial transactions must ensure that they follow the required security guidelines and implement security measures provided or suggested by OS manufactures and reliable security forums or authorities.

REFERENCES

1. Symantec Research Information, "https://symantec-blogs.broadcom.com/blogs/expert-perspectives/symantec-mobile-threat-defense-attackers-can-manipulate-your-whatsapp-and-telegram-media".
2. Media file jacking "https://securityaffairs.co/wordpress/88485/hacking/media-file-jacking-attacks.html".
3. Android Storage "https://developer.android.com/preview/privacy/storage"
4. Android Media Scanner, "https://developer.android.com/reference/android/media/MediaScannerConnection".
5. App Setting, "https://fossbytes.com/whatsapp-telegram-vulnerable-to-media-file-jacking"

AUTHORS PROFILE

Shinto Kurian K received Bachelor of Commerce (B.Com) degree from Calicut University in 1999, Master of Computer Application (MCA) degree from Madurai Kamaraj University in 2002 and the Master of Business Administration (MBA) degree from Madurai Kamaraj University in 2008. Presently he is pursuing PhD in Madras University. He has 17+ years of work experience in software development and its life cycle management. Now he is playing as senior manager at TechMahindra, India.

Dr K Nirmala working as associate professor and research guide at Quaid-E-Millath Government College for Women. She has master's degree as well as doctorate in Computer science.