itworldcanada.com

Understanding Android Malware Families: file infector and potentially unwanted applications (Article 6) | IT World Canada Blog

Gurdip Kaur and Arash Habibi Lashkari

10-12 minutes

Introduction

File infector is a malware that attaches itself to APK files, which contain all the data related to an Android application. File infector gets installed with APK files, and it gets executed when the APK file is installed. The APK file can be any Android application such as a game, word processing file, location navigation, or any other application. Recently, Google deleted several apps from the Play Store because they were suspected of containing malware. File infector families attempt to slow down the device and consume a lot of battery.

PUAs are potentially unwanted applications that come bundled with genuine applications that are available free of cost. They are sometimes called potentially unwanted programs (PUPs). PUAs are not always destructive – it all depends on their use. PUAs automatically get installed when the application to which it is bundled with is installed; they can take the form of adware, spyware, or hijackers. When PUAs behave like popping up an advertisement, it is referred to as adware. PUAs slow down the device by consuming memory. They can also lead to other PUPs and spyware programs that aim to steal sensitive data from the target device and send it to the attacker.

According to a report published by Avira, Android PUA malware samples decline by two per cent in Q3 as compared to Q2 of 2020. However, 29.3 per cent cyber-attacks in the same quarter are attributed to file infectors. According to another report published by AVTest, 927,553 Android malware samples were detected by the end of March 2021. Out of these samples, 1.48 million samples are PUAs. These reports and statistics are alarming. Figure 1 shows the growth of PUA samples in last five years based on AVTest report. It is evident that number of PUA Android malware samples are continuously increasing every year.

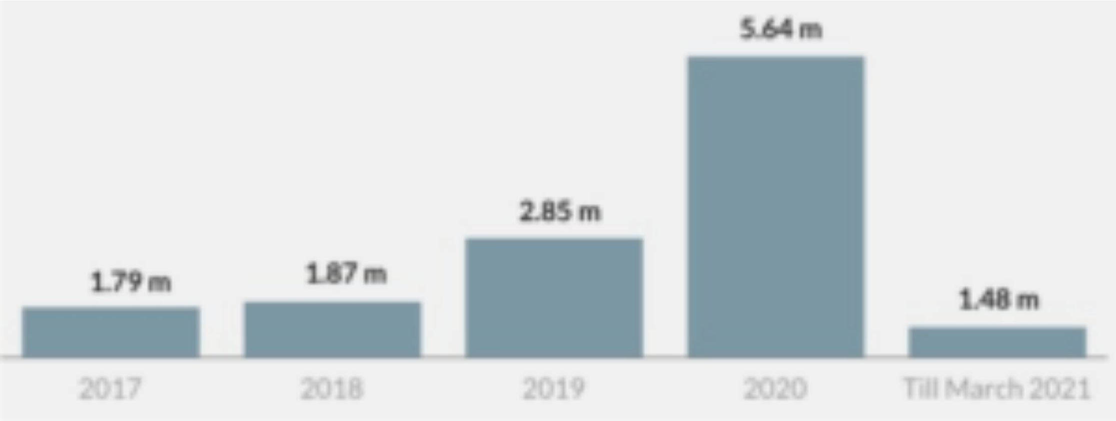

Figure 1: Growth of PUA malware samples

This article is the last in the UAMF series to understand Android malware families, uncovering prominent file infector and PUA families. It provides deep insights into functions, activities, and communication processes used by popular file infector and PUA malware families based on our public dataset on Android malware, named *CCCS-CIC-AndMal-2020*. It presents imperative indicators to understand that the smartphone is infected by file infector and PUA malware. It also digs deeper into technical features that can detect these families on a smartphone. Finally, the article introduces some preventive measures to protect the device from file infector and PUA malware families.

File Infector and PUA families

Some common activities performed by file infector families include collecting device ID, International Mobile Equipment Identity (IMEI) numbers, and phone status. They may block, delete or use phone applications, and they can modify, collect, and access files and device settings. In the worst case, file infectors can root the device. *Gudex* and *tachi* are the two main families under file infector malware category that fetch network country ISO. Additionally, *tachi* gets system properties to fetch IP address of the WiFi device while *gudex* updates message digest and sends text message.

PUAs collect personal information and user contacts from the device. They access device location through Global Positioning System (GPS), display pop-up advertisements/notifications /warnings, objectionable URLs, and shortcuts on the user screen. *Umpay* executes database queries. *Scamapp* opens URL connections and input files, starts new activities, and gets network country ISO. *Apptrack* opens input and output files and gets network operator. Five file infector and eight PUA families analyzed for this article are presented in Figure 2.

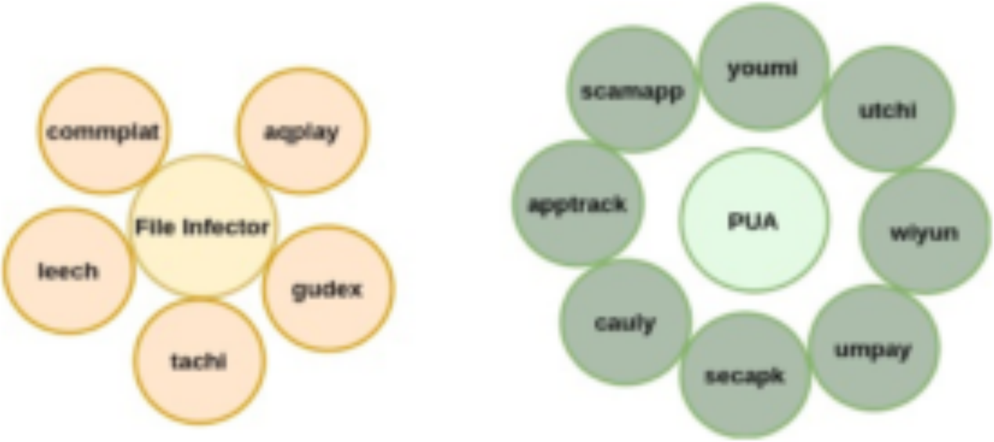

Figure 2: File Infector and PUA families

Behavioural changes on execution

Based on the results of our Android dataset (*CCCS-CIC-AndMal-2020*), the behavioural changes in file infector malware families on execution are shown in Figure 3. The left side of the figure represents behaviour corresponding to starting a device whilst the right side of the figure shows behavioural curves after restarting the device. Without going into the technical details of x- and y-axis of the graph, it is apparent that the four families plotted in Figure 3 follow a similar curve before and after restarting the device. This indicates that the behaviour of these families remains similar on starting and restarting the device. Simply out, restarting the device does not make any changes to behaviour exhibited by file infector families.

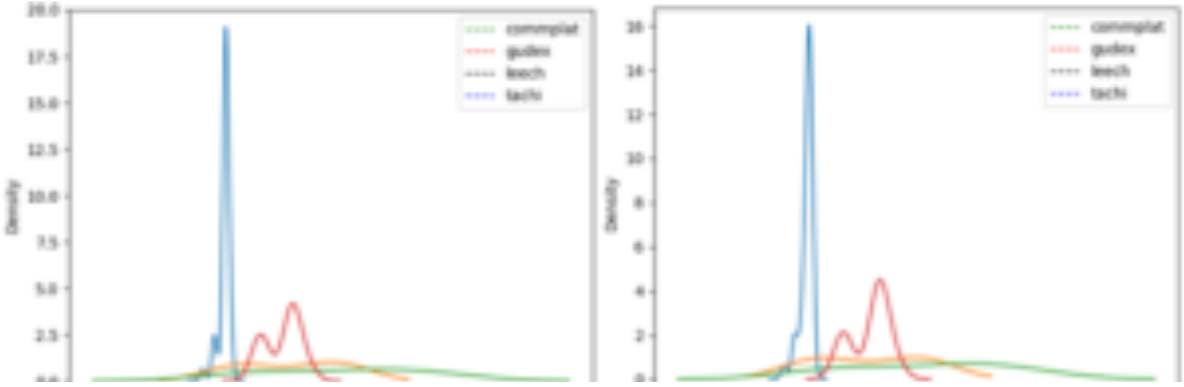

Figure 3: Behaviour changes in File Infector families

The behavioural changes in PUA malware families on execution are shown in Figure 4. Similar to Figure 3, The left side of the figure represents behaviour corresponding to starting a device whilst the right side of the figure shows behavioural curves after restarting the device.

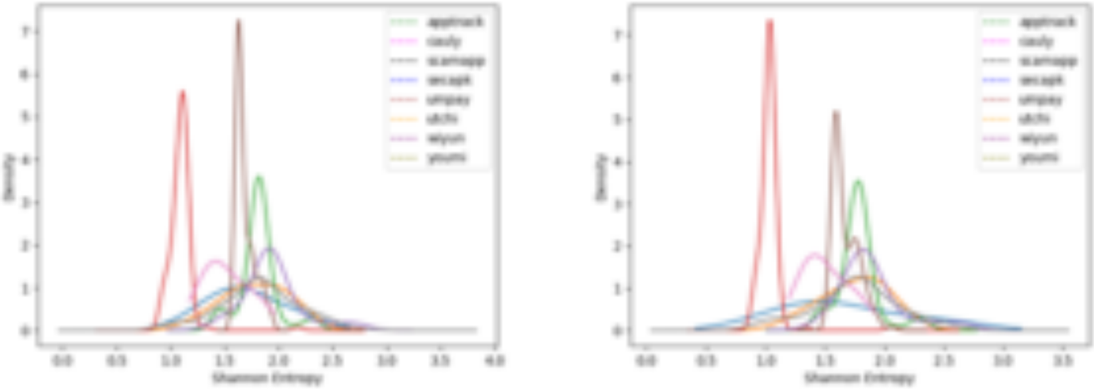

Figure 4: Behaviour changes in PUA families

Overall, there are two prominent spikes in red and brown curves in left and right side of the figure. The red curve corresponds to *umpay* family. It is clear that after restarting the device, *umpay* family shows a spike in behaviour changes. This means that the randomness in behaviour of *umpay* increases after the device on which it is installed is rebooted. The second prominent change corresponds to brown curve which shows that the randomness in behaviour decreases after rebooting the device. This curve belongs to *youmi* family. For the rest of the families, there is no change in behaviour before and after rebooting the device.

Types of PUAs

PUAs can come in the form of following malware categories:

- *Adware:* Adware represents advertisement malware. It is a malicious application that throws unwanted advertisements on the user screen, especially when accessing web services. Adware lures the user towards flashing advertisements that attract them to click on the advertisement. Once a user clicks on the advertisement, revenue is generated by the developer of this unwanted application.
- Browser hijacker: Browser hijacking is a term associated with malicious software. It is used to display advertisements, visit a malicious website, and redirect user to fraudulent websites that can download malware on phone.
- *Spyware:* Spyware is a malicious software installed on user's device to steal sensitive information. The data collected by spyware is passed to advertisers, external agencies, or firms. This data is later used to carry out malicious activities.

How do PUAs spread?

PUAs often get installed with a legitimate application. It is not always harmful, but the user still needs to be aware of the malicious activities that it can perform. PUAs spread through social engineering tactics. Legitimate apps trick users to install additional apps. It is done through the following ways:

- Tricking users to take unnecessary actions.
- Assigning additional permissions to apps.
- Convincing users to install additional apps.
- Installing additional apps by default.

Affect of PUAs

PUAs can affect the target device in following ways:

- *User privacy:* PUAs can sniff user’s activities and surfing habits. They collect sensitive information from the device and send it to a remote attacker.
- *Exhaust resources:* PUAs drain mobile battery and utilize device memory by storing non-essential data.
- Compromise security: PUAs can expose the sensitive information collected from the device to unexpected applications and websites.

Technical features that can detect File Infector and PUA

Based on the results of our Android dataset (*CCCS-CIC-AndMal-2020*), following technical features are very helpful to detect file infector and PUA:

- *Memory features:* Memory features define activities performed by malware by utilizing memory.
- *API features:* Application Programming Interface (API) features delineate the communication between two applications. Whenever a user searches information in a browser, checks the weather forecast, sets a timer, or uses social media, they are using an Android API in the background.
-
- *Network features:* Network features describe the data transmitted and received between other devices in the network. It indicates foreground and background network usage.
- *Logcat features:* Logcat features write log messages corresponding to a function performed by malware.

Indicators of infection

Following points indicate that the device is infected by file infector or PUA:

- Frequent display of unwanted apps on the screen.
- Battery drainage at a much faster rate.
- Low device memory.
- Slow speed of device.
- Applications and services will crash more frequently.
- Device is heated up.
- Unrecognized apps downloaded on device without user consent.

Preventive measures to protect your device

The following are some important measures to protect your device:

- Check the pre-checked boxes before downloading and installing any application. The pre-checked boxes authorize PUAs for malicious activities.
- Skim the terms and conditions before installing any app. It appears nasty but essential for the security of the device. PUAs are referred to as their name in the terms and conditions agreement.
- Scan the device with a good anti-virus or anti-malware to detect malware.
- Do not download apps from third-party stores.
- Keep the device updated.
- Manually check any unwanted apps installed on the device.

- Be aware of the social engineering tactics such as phishing emails and messages.
- Review the access permissions assigned to an app.

Conclusion

This article brings forward the fundamentals of file infector and PUA malware families. It comes equipped with malicious behaviour exhibited by these families on the target device. We established imperative indicators of compromise that points to the fact that the phone is infected by file infector and PUA families. Based on our public dataset on Android malware, named *CCCS-CIC-AndMal-2020*, we open on the technical features that are very useful to detect these families. Finally, the article introduces preventive measures to protect the device. This is the last article of the UAMF series to make the readers understand the Android malware families.