itworldcanada.com

Understanding Android Malware Families (UAMF) – The Foundations (Article 1)

Gurdip Kaur and Arash Habibi Lashkari

18-22 minutes

IT WORLD CANADA

Source: Sitthiphong | Getty Images

Android malware is one of the most serious threats on the internet and has witnessed an unprecedented upsurge in recent years. There is a need to share the fundamental understanding of behaviour exhibited by prominent Android malware categories and families.

With the increasing number of Android users and devices, the number of exploits on Android apps is also on the rise. It has

affected all sectors of business including healthcare, finance, transportation, government, and e-commerce. As the current trend continues, mobile attackers are developing more sophisticated intrusions by deploying malicious apps and malware. The *Understanding Android malware families (UAMF)* series features six articles that will highlight the main Android malware categories and families. Readers will learn about the threats' behaviour and examine mitigation procedures. The articles in this series present the results of our Android malware analysis research project, which has been underway since 2017. We generated four datasets AAGM2017, AndMAl2017, InvestAndMAl2019, and AndMal2020 and related academic articles along with proposed Android malware detection and characterization solutions and techniques.

Introduction

Android is the leading operating system that provides high-performance platforms for users. According to a report published by the International Data Corporation (IDC), Android is dominating the market with 85 per cent of the global market share in the last quarter of 2020. Further, the annual shipment rate of Android is expected to grow by 150 million units in 2021. With the surging demand for Android in the global market, the challenges associated with Android malware are also escalating at a rapid rate. According to a report, as of March 2020, the total number of Android malware samples amounted to 482,579 per month [3]. These statistics are alarming and draw our attention to the menace accompanied by the legacy of the Android operating system. These malware samples can create havoc, if not detected.

Android malware is malicious software that targets smartphone

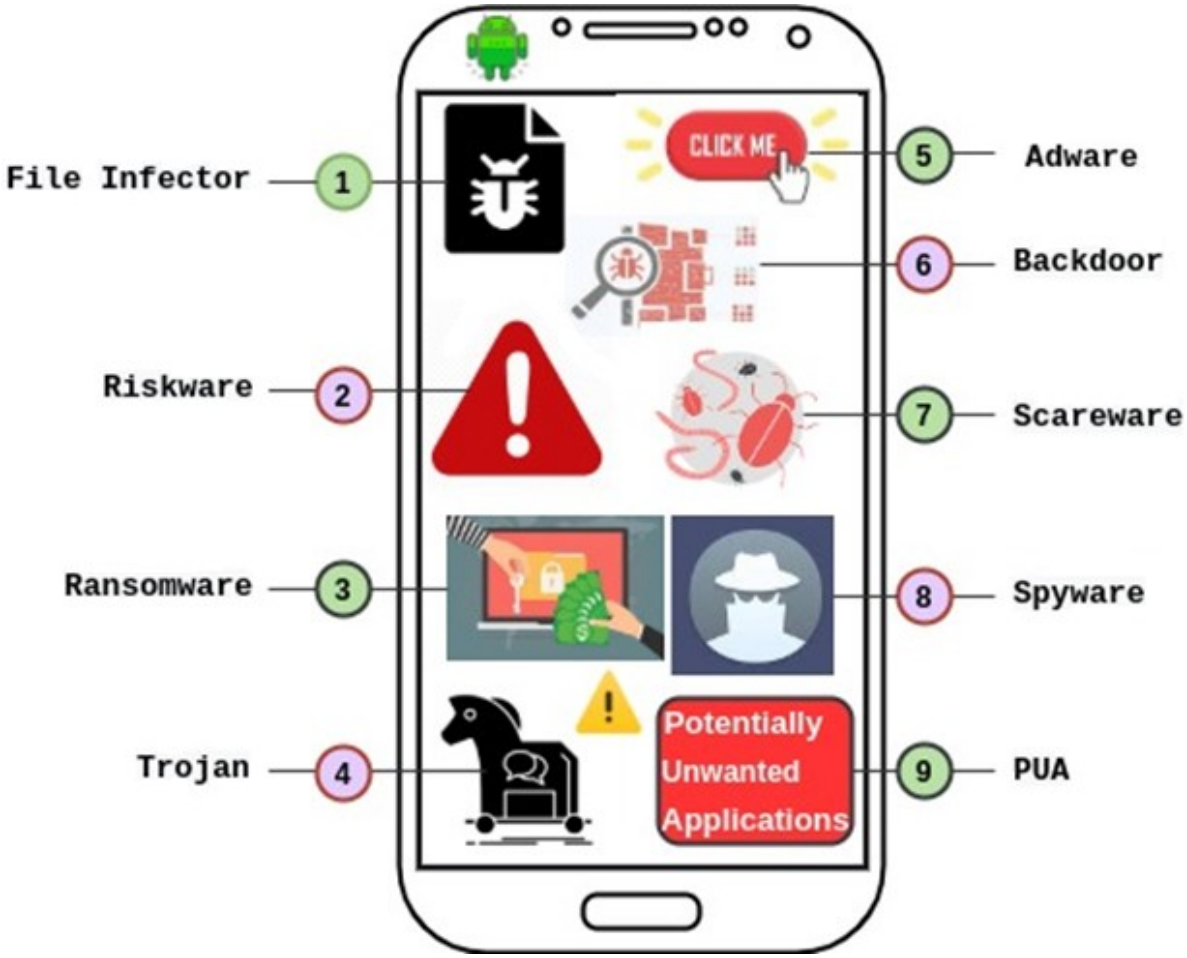
devices running Android operating systems. It is like other malware samples that run on desktops or laptop computers. Android malware is alternatively called mobile malware which is any piece of malicious software intended to harm the mobile device by performing some illegitimate activities. It can be classified into different malware categories such as adware, backdoor, file infector, potentially unwanted application (PUA), ransomware, riskware, scareware, spyware, and trojan. Each malware category has some unique characteristics that differentiate it from the other malware categories. Android malware also grows like humans. Every malware category has several malware families associated with it.

The unrivalled threat of Android malware is the root cause of myriads of security problems on the internet and is an open challenge for researchers and cybersecurity experts. The only way to get rid of this threat is to timely detect and mitigate the malware samples. Fundamental knowledge of Android malware categories and families is the key to doing so. This article aims to shed light on prominent Android malware categories and related families under each malware category. In addition, it also makes the reader familiar with abnormal activities performed by each malware category. Finally, the article suggests some mitigation or prevention measures for Android malware.

Android malware categories and families

The prominent Android malware categories include adware, backdoor, file infector, PUA, ransomware, riskware, scareware, spyware, trojan, trojan-sms, trojan-spy, trojan-banker, and trojan-dropper. This section discusses the functions performed by each

of these malware categories and names some important malware families under these malware categories.



1. ***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 offer lucrative products and attract them to click on the advertisement. Once a user clicks on the advertisement, revenue is generated by the developer of this unwanted application. Some common examples of adware include weight loss programs, making money in less time, and bogus virus warnings on screen. This is not the only way that adware attacks users. Some adware samples are downloaded when any software or application is installed on the smartphone. Some important adware families include **gexin, batmobi, ewind,**

shedun, pandaad, appad, dianjin, gmobi, hummingbird, mobisec, loki, kyhub, and **adcolony**. Adware, in general, collects personal information from the device such as phone number, email address, application accounts, IMIE number of the device, device ID, and status. Some adware families access device cameras to collect pictures. In some cases, adware attempts to encrypt data on devices and install other malicious applications, code, or files.

2. ***Backdoor:*** Backdoors act as hidden gateways into a smartphone. In other words, backdoors are a way to bypass the authentication of a smartphone and raise privileges allowing the attacker to access the device any time. Backdoors facilitate the launch of remote attacks without having the device physically. They can be completely new programs or part of an existing one. Attackers cleverly embed the malicious code in legitimate programs so that it's executed only when a special environment or condition is met. It's observed in some cases that if users do not change their default passwords of any account that they created on their device; these passwords can be used as backdoors to inject malicious code for remotely controlling the device. Some common examples of backdoor Android malware families include **mobby, kapuser, hiddad, dendroid, levida, fobus, moavt, androrat, kmin, pyls,** and **droidkungfu**. Backdoor malware collects personal information from the phone, sends/receives messages, makes phone calls and collects call history, collects lists of installed and running applications, and creates memory space in the device. In some severe cases, the backdoor is rooted to the Android device on which it was installed. Backdoors can be linked with adware. Attackers often use advertisement malware to lure the users in. Once the user clicks the advertisement, a backdoor is

installed on their device.

3. ***File infector:*** A file infector is malware that attaches itself to APK files. APK stands for Android Package Kit which contains all the data related to an application. The file infector gets installed with APK files. The malware is then executed when APK files are 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 suspected of containing malware. Some common file infector families include leech, tachi, commplat, gudex, and aqplay. File infector families attempt to slow down the device and consume a lot of battery. These families collect device ID, IMEI number, and phone status. They may block, delete or use phone applications. They can modify, collect, and access files and device settings. In the worst case, file infectors can root for the device.
4. ***PUA:*** 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. A PUA automatically gets installed when the application it's bundled with is installed. It can take the form of adware, spyware, or hijackers. When PUAs start popping up advertisements, it's 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. Some famous PUA malware families for Android devices include **apptrack, secapk, wiyun, youmi, scamapp, utchi, cauly**, and **umpay**. PUAs collect personal information and user contacts from the device. They can access the device's

location through Global Positioning System (GPS), display pop-up advertisements, notifications and warnings, objectionable URLs, and shortcuts on the user screen.

5. ***Ransomware:*** Ransomware is malware that encrypts files and directories on the machine to make them inaccessible to users. It asks for a handsome amount of ransom to provide the decryption key that is used to unlock the data. Ransoms are often paid for bitcoins. Certain incidents, however, have confirmed that some users were unable to get their data back after paying the ransom. Some of them reported receiving incomplete files. At times, files simply vanished. We can't confirm that paying a ransom is helpful. Android ransomware has evolved significantly and new variants are emerging. Some ransomware samples masquerade as popular apps and manage to escape detection. Some common ransomware malware families include **congur, masnu, fusob, jisut, koler, lockscreen, slocker,** and **smsspy**. Ransomware families are involved in sending/receiving SMSs, locking SIM cards and smartphones, stealing network information such as Wi-Fi connection details, and communicating to the remote server controlling the ransomware attack.
6. ***Riskware:*** Riskware is a legitimate program that poses potential risks to the security vulnerabilities on the device. Although it is a genuine program, it's used to steal information from the device and redirect users to malicious websites. It can be alternatively termed as risky software that performs functions at the cost of device security. Some common riskware families include **badpac, mobilepay, wificrack, triada, skymobi, deng, jiagu, smspay, smsreg,** and **tordow**. Riskware families collect personal and phone information, send/receive SMSs, steal network information,

connect to malicious websites, install malicious content on devices, show malicious advertisements, and modify system settings and files on the device.

7. ***Scareware:*** Scaeware is a fear coaxer that raises fear in users' minds to download or buy malicious apps. For example, convincing users to install a fake application that pretends to safeguard the device. Famous scareware families include **avpass, mobwin**, and **fakeapp**. Scareware families attempt to collect device information and GPS location and install malicious code on the device.
8. ***Spyware:*** Spyware is malicious software that can steal sensitive information once installed on the device. The data collected by spyware is passed to advertisers, external agencies, or firms. This data is later used to carry out malicious activities. Android asks users to provide permission to access device information such as location, camera, and settings, but spyware is installed without the user's authorization. Common spyware families include **spynote, qqspy, spydealer, smsthief, spyagent, spyoo, smszombie,** and **smforw**. Spyware families collect personal information, send/receive SMSs, collect phone information and device location, steal network information such as Wi-Fi connections to which the device is connected, and access system files and settings to modify them.
9. ***Trojan:*** Trojans are sneaky impersonators that behave like legitimate programs. They can hide in the background and steals information from the device. It's the biggest malware category that represents several malware categories including trojan-banker, trojan-dropper, trojan-sms, and trojan-spy. Extremely popular trojan families include **gluper, lotoor, rootnik, guerrilla, gugi,**

hqwar, obtes, and **hypay**. Trojans often engage in deleting, modifying, blocking, and copying data to disrupt services provided by the operating system.

Table 1 provides a brief description of Android malware categories and lists some common malware families under them.

Table 1: Summary of Android malware categories

Malware Category	General Description of Behavior	Common Malware Families
Adware	Serves unwanted pop-up advertisements to the user.	gexin, batmobi, ewind, shedun, pandaad, appad, dianjin, gmobi, hummingbird, mobisec, loki, kyhub, and adcolony
Backdoor	Exploits the device covertly by hiding in the background.	mobby, kapuser, hiddad, dendroid, levida, fobus, moavt, androrat, kmin, pyls, and droidkungfu
File Infector	Contaminates the files, especially the executable (APK) files.	leech, tachi, commplat, gudex, and aqplay

PUA	Acts as an unwanted interruption to normal activities performed by the device.	apptrack, secapk, wiyun, youmi, scamapp, utchi, cauly, and umpay
Ransomware	Acts as a crypto locker that encrypts the files and directories and demands a ransom from the user to access his own data.	congur, masnu, fusob, jisut, koler, lockscreen, slocker, and smsspy
Riskware	Poses risk to the potential vulnerabilities on the smartphone.	badpac, mobilepay, wificrack, triada, skymobi, deng, jiagu, smspay, smsreg, and tordow
Scareware	Serves as a fear coaxer that ignites fear in the user's mind and forces them to download malicious apps.	avpass, mobwin, and fakeapp
Spyware	Indulges into spying activities to steal useful information from the device and send it to a remotely controlled server.	spynote, qqspy, spydealer, smsthief, spyagent, spyoo, smszombie, and smforw
Trojan	Behaves like an impersonator in the background that keeps	gluper, lotoor, rootnik, guerrilla, gugi, hqwar, obtes,

	stealing information from the device. It is represented in several forms including trojan-banker, trojan-dropper, trojan-sms, and trojan-spy.	and hypay

Mitigating Android malware

Android malware attaches itself to a legitimate APK file to avoid detection. As a cybersecurity professional, mitigating Android malware involves a deep understanding of some imperative technical concepts such as packing techniques, source code analysis, and reverse engineering. All these concepts are introduced below for a better understanding. We've also listed important tools that are used to perform all these tasks.

Packing techniques

Android malware samples are packed using programs called packers. Packers hide the malicious programs in an envelope so that it remains undetected. They encrypt the malicious APK file and use the device's memory to execute it. Packers were originally created to protect sensitive applications from leakage. These applications include intellectual property rights. However, packers were applied to hiding malware samples later. Packers have become more sophisticated and complex over time. They pose serious challenges to cybersecurity professionals. A lot of Android malware is packed with services provided by packers. To detect Android malware on a device, it's necessary to unpack it to remove

it from the envelope. Unpacked malware is then analyzed to determine its behaviour. To identify the behaviour, malware is executed in a special environment so that it doesn't affect the Android device. *ApkProtect.com* and *Bangcle.com* are one of the first packers that provide online packing services for Android apps.

Source code analysis

After unpacking the malware samples, the very first step is to analyze its source code to reveal its functionality and behaviour. Source code can be analyzed statically or dynamically. In static malware analysis, source code is not executed. It deals with the logical structure and flow of instructions in the program. On the other hand, dynamic malware analysis prepares a special run-time environment called sandbox to execute the malware and determine its behaviour. Dynamic malware analysis reveals more information compared to static malware analysis because it executes the malware in a sandbox. However, some complex malware samples are programmed to detect the sandbox environment before execution. Once they find themselves in a sandbox environment, they are not executed. This makes dynamic malware analysis a challenging task malware analyst. ***Frida*** is a famous tool for performing a dynamic analysis of Android malware.

Reverse engineering

Reverse engineering is a process of determining the functionality of any object. It's used to obtain the source code of the mobile app from the APK file. Several reverse engineering tools are used to inspect hidden malicious code inside a legitimate application.

Some common reverse engineering tools for Android apps include *APKInspector*, *APKTool*, *Bytecode Viewer, Smali,* and *Jadx*. These tools take APK file as the input and obtain its original source code to build the functionality of the app.

How to secure your device?

There are several preventive measures to adopt by a layman to prevent Android malware. Some important measures include:

1. ***Do not download apps from unreliable sources:*** Users are encouraged not to download any apps from unreliable sources. Even all the apps in Google Play Store are not secure. Google Play regularly deletes suspicious apps from its repository.
2. ***Avoid third-party app stores****:* Third-party app stores do not contain legitimate apps. At least Google Play Store is safe to download apps. Moreover, third-party apps may require rooting for the device.
3. ***Say no to clickables****:* Avoid clicking any advertisement in an app without properly reading and understanding it. Adware and PUA malware attack targeted phones by displaying luring advertisements that can attract users to click on the flashing link in the advertisement. Once the user clicks on the link, he may be redirected to malicious websites that are used to download malware on the targeted device. In some cases, clicking the flashing link itself leads to downloading malicious software on the phone.
4. ***Assigning permissions to apps:*** Most apps ask user to assign permissions and rights to the application so that they can access device settings, contact details, and camera. Avoid assigning such

permissions to all apps until it is required for the functioning of the app.

5. ***Install system updates:*** It is highly recommended to install system updates so that apps installed on the smartphone are always updated. Upgrade to the latest version of the operating system, if possible.

What's next

This article introduces the fundamentals of Android malware, prominent malware categories, their behaviour, abnormal activities, and important malware families under them. We've also included some important mitigation techniques used by malware analysts. The next article of this UAMF series will be a deep-dive introduction to the trojan malware category, which acts as an impersonator in the background.

Would you recommend this article?

Thanks for taking the time to let us know what you think of this article!
We'd love to hear your opinion about this or any other story you read in our publication. **Click this link to send me a note →**

Jim Love, Chief Content Officer, IT World Canada

Related Download

Sponsor: **CanadianCIO**

Cybersecurity Conversations with your Board – A Survival Guide

A SURVIVAL GUIDE BY CLAUDIO SILVESTRI, VICE-PRESIDENT AND CIO, NAV CANADA

Download Now