itworldcanada.com

Understanding Android Malware Families (UAMF) – The Trojan: An impersonator in the background (Article 2)

Gurdip Kaur and Arash Habibi Lashkari

17-22 minutes

IT WORLD CANADA

Source: Sitthiphong | Getty Images

Introduction

The trojan is a sneaky impersonator that behaves like a legitimate program. It can hide in the background and steal information from the device. Trojan samples often delete, modify, block, and copy data to disrupt services provided by the operating system. It is the

most significant malware category representing several Trojan categories, including Trojan-Banker, Trojan-Dropper, Trojan-SMS, and Trojan-Spy. This article uncovers prominent Trojan categories and provides deep insights into functions, activities, and communication processes used by famous Trojan families. It presents imperative indicators to understand that smartphones are infected by Trojan malware. It also digs deeper into technical features that can detect Trojan on a smartphone. Finally, the article introduces some preventive measures to protect the device from Trojan families.

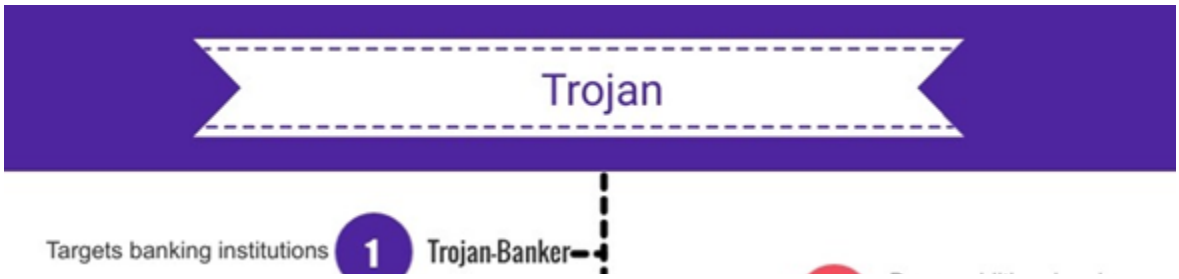
In case you missed it

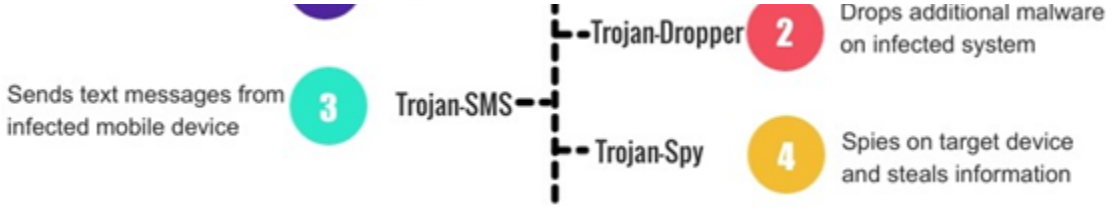
Understanding Android Malware Families (UAMF) – The Foundations (Article 1)

Trojan categories and families

The prominent Trojan malware categories include Trojan-Banker, Trojan-Dropper, Trojan-SMS, and Trojan-Spy. This section discusses the pertinent functions performed by each of these malware categories and names some important malware families under these malware categories. Figure 1 shows an overview of Trojan malware categories.

Figure 1: Trojan Malware Categories





Trojan-Banker: Trojan-Banker is a malware category that targets banking institutions. It is designed to access confidential information processed during online banking transactions. For example, when a user accesses his online banking payment system to transfer an amount, Trojan-Banker may access the user's confidential information such as bank account number, credit card details, date of birth, and account balance. The curious question that comes to mind is, "from where this malware comes to target a banking system?" The logical answer to this question is that it is installed in one way or the other on the target computers. It may come embedded with genuine software that the user installed on his machine without knowing that it contains a Trojan. Trojan-Banker is legitimate software until it is installed on a computer system. Once installed, it may gain unauthorized access to steal user's files and systems. In more severe cases, it may transfer a handsome amount of money from a user's account. Let us take an example in which a user received a phishing email from an attacker that appears to be sent by his bank. The email asks him to urgently change the password of his online banking system due to security reasons. It also provides a link at the bottom of the text to open the banking portal. Unconscious and the scared user will believe in the requirement to click the link in the email to change their password. As soon as he clicks the link, a phishing web page is opened that appears remarkably like the genuine banking online portal. The user enters his login name and password and clicks on the submit button. The attacker grabs his

username and password to do whatever he can. Some famous Trojan-Banker families include *asacub, fakebank, faketoken, marcher, minimob, bankbot, gugi, wroba, zitmo, svpeng*, and *guerrilla*.

Trojan-Dropper: Trojan-Dropper is a helper malware that drops additional malware on the infected device. It does not perform any malicious activity independently; instead, it supports the malicious activities performed by other Trojan categories. It downloads and installs legitimate-looking malicious files on the infected smartphone and decompresses some harmless files. Trojan-Dropper removes itself automatically after installing the malware. Some common activities that result in downloading and installing malware include visiting malicious websites, opening suspicious attachments, and downloading unknown free applications. For example, a user downloads a radio streaming APK from an online Android application store. The application is played by FM radio channels at different frequencies. However, the user observes that the smartphone keeps awake unnecessarily after downloading the radio application. On digging deeper, a reverse engineer identified that apart from playing radio channels, the application is performing some malicious activities such as accessing the network state of the phone, installing additional applications without user consent, deleting some files from the phone, mounting file systems, visiting malicious and unknown websites, and keeping the phone awake when all these activities are being performed in the background. The radio streaming application acts as a Trojan-Dropper that itself is not malicious. Still, it comes bundled with a bunch of malicious APKs that get installed with this APK and then start doing malicious things on the target device.

Some famous Trojan-Dropper families include *cnzz, locker, rooter, xiny, boqx, hqwar, ramnit, ztorg, and gorpo*.

Trojan-SMS: Trojan-SMS is primarily involved in sending Short Message Service (SMS) from an infected mobile device. It accesses the telephony manager of the Android operating system by virtue of which it can access the contact list on the infected device and send short and multi-part text messages to other contact numbers accessed from the contact list of the infected device. The critical part of the activities is that these activities are performed without the user knowing about them. There is a fee associated with sending text messages to premium-rate SMS numbers. Therefore, the victim is financially targeted by Trojan-SMS. As an aftermath of the malicious activities performed by Trojan-SMS, a user is notified of the unexpected charges of sending such messages from his phone. It is fascinating to mention that Trojan-SMS is installed automatically with some free applications that intend to provide some useful functionality. Some famous Trojan-SMS families include *opfake, hipposms, podec, feejar, smsdel, plankton, jsmshider, smsbot, boxer, fakeinst, and vietsms*.

Trojan-Spy: Trojan-Spy is a spyware that spies on the infected cell phone. It is designed to steal information from the target device by several means. Trojan-Spy malware grabs the device information such as International Mobile Equipment Identity (IMEI) number, IP address, and list of installed applications. Some unusual activities performed by Trojan-Spy include switching the mobile ringer (for example, from normal mode to silent mode), sending and deleting SMS, accessing Wi-Fi and turning it off, and connecting to available Wi-Fi access points other than the one to

which user is already connected. Some famous Trojan-Spy families include *spynote, kasandra, spyagent, spyoo, tekwon, sandr, qqspy, smforw, smsthief, smszombie, and spydealer*.

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

Table 1: Summary of Trojan categories

Malware Category	General Description of Behavior	Common Malware Families
Trojan	An impersonator that hides itself in the background and disrupts the services provided by the operating system.	autosms, gluper, hiddenapp, mobtes, qysly, boogr, subspod, drosel, autoinst, obtes, noicondl
Trojan-Banker	Picks out banking system to steal username and password, and illegitimately transfers money from user's account to attacker account.	asacub, fakebank, faketoken, marcher, minimob, bankbot, gugi, wroba, zitmo, svpeng, guerrilla
Trojan-Dropper	Acts as a helping software to Trojan malware, drops additional malware, installs it, and removes itself automatically.	cnzz, locker, rooter, xiny, boqx, hqwar, ramnit, ztorg, gorpo
Trojan-SMS	Send text messages to premium contact numbers that result in unexpected	opfake, hipposms, podec, feejar, smsdel, plankton, ksmshider,

	charges to the target user.	smsbot, boxer, fakeinst, vietsms
Trojan-Spy	Spies target cell phones to steal device information such as IMEI number, IP address, and list of installed applications.	spynote, kasandra, spyagent, spyoo, tekwo, sandr, qqspy, smforw, smsthief, smszombie, spydealer

Imperative indicators to detect Trojan on a smartphone

There are several general and technical indicators that help detect a Trojan on a smartphone. This section delves into both types of indicators.

General indicators: Following general indicators point at the presence of Trojan malware that are easy to observe on an infected mobile device:

- *High battery and data usage:* Trojan malware consumes a lot of battery and data. It downloads and installs malicious applications in a hidden manner that results in high battery drainage and data consumption.
- *Getting slower:* Every Trojan malware category makes the target device much slower since it consumes a lot of memory by running in the background.
- *Unexpectedly installed applications:* Evidently Trojan installs suspicious applications that perform malicious activities. No need to mention that these applications are installed without any user

permission.

Technical indicators: Following technical indicators hint that the smartphone is infected by a Trojan malware:

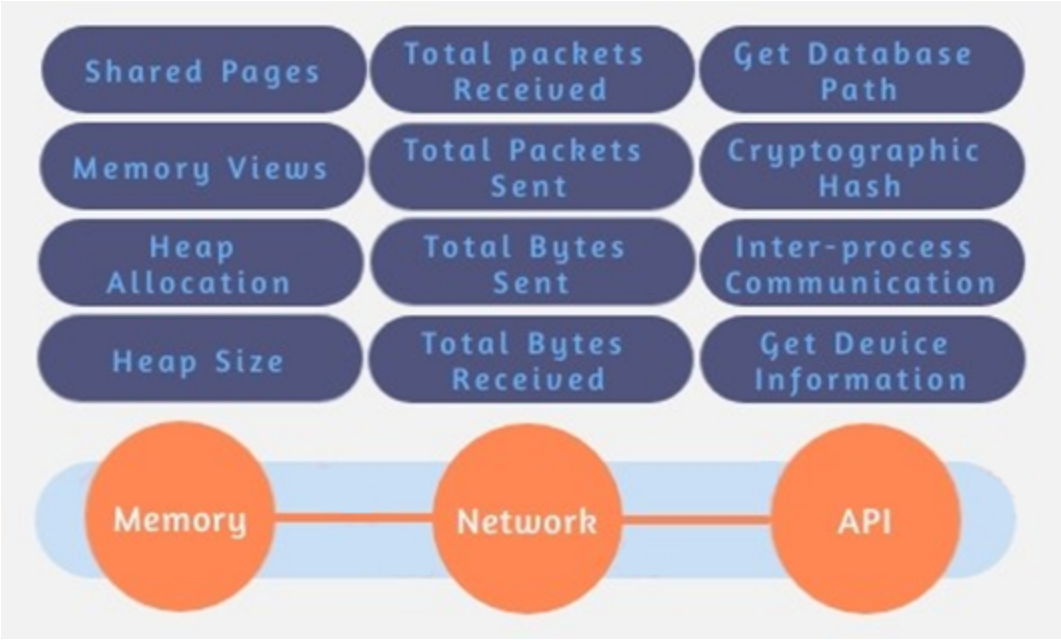
- *Automatic device reboot:* Some Trojan samples automatically reboot the phone repeatedly. This activity is performed so that the configuration changes made to the device after installing malware can take place.
- *Send/Receive SMS:* Trojan-SMS and Trojan-Spy malware families send and receive chargeable premium text messages to premium numbers. If such a text message appears in the phone message list, it indicates infection by any Trojan malware family.
- *Access telephony manager:* Like text messages, Trojan accesses the telephony manager of Android operating system to make unknown calls. These calls are logged in to the phone call log.
- *Keep the device awake:* When Trojan installs unwanted malicious applications in the background, it keeps the phone awake when such an operation is under process. It accesses permission related to the wake lock feature of the Android operating system. This feature does not let the device sleep until a background activity is taking place.
- *Switch phone state:* Trojan accesses permissions related to current phone state and switches it abruptly. For example, if the phone is in ringer mode, it may be switched to vibrate mode or silent mode and vice versa.
- *Network change:* Trojan malware accesses Wi-Fi state of the device and toggles it to connect to other available access points.
- *Restart packages:* Trojan-Dropper restarts some packages in the

Android operating system. However, it is not that easy to detect until an adverse effect comes in effect.

Technical features that can detect Trojan

Based on our research in a representative Android dataset, named *CCCS-CIC-AndMal-2020*, published in collaboration with Canadian Centre for Cyber Security (CCCS) and the Canadian Institute for Cybersecurity (CIC), there are certain set of features that can be used to detect Android malware, especially Trojan. Figure 2 presents high ranked features that detect Trojan with high accuracy. These features are divided into three categories: memory, network, and API.

Figure 2: Features to detect Trojan with high accuracy



Memory features: Memory features define activities performed by malware by utilizing memory.

- *Shared Pages:* It depicts pages in memory that are shared between two processes. It considers sharing pages across

processes. Malware always involves many processes that communicate with each other and share memory. This way, malware utilizes high memory usage, usually heats the phone, and drains the battery faster.

- *Memory Views:* Memory views are related to memory leaks in applications. Memory leak is a flaw that is exploited by the Trojans.
- *Heap Allocation:* Heap is an area in memory which is dynamically allocated to apps on execution. Simply put, memory used by an Android application during execution is called heap. Heap allocation keeps track of the Android application. Trojan malware families utilize a lot of heap memory because they perform a massive number of activities on execution. These activities include communicating with attacker machines, visiting websites, and interacting with other processes.
- *Heap Size:* As indicated by the name, heap size represents the amount of heap memory used by Android applications. Trojan takes a larger heap size to perform malicious activities.

Network features: Network features describe the data transmitted and received between other devices on the network. It indicates foreground and background network usage.

- *Total Packets Received:* It presents a total number of packets received at the corresponding time interval.
- *Total Packets Sent:* It presents a total number of packets transmitted at the corresponding time interval.
- *Total Bytes Sent:* It presents a total number of bytes transmitted at the corresponding time interval.

- *Total Bytes Received:* It presents a total number of bytes received at the corresponding time interval.

  API features: Application Programming Interface (API) features delineate the communication between two applications. Whenever a user browses some information in a browser, checks weather forecast, sets a timer, or uses Twitter on phone, he is using an Android API in the background.

- *Get Database Path:* This API is used to access and steal data from databases. Trojan malware families attempt to steal confidential information stored in databases, especially banking databases. The purpose is to obtain username and passwords of bank users to perform money frauds.

- *Cryptography Hash:* Cryptography hashes are used to encrypt data before transmission for security purposes. Some Trojan families strive to obtain the algorithm used for hashing so that secured data can be decrypted.

- *Inter-process Communication:* As clear from the name, this API contains the details of communication between two processes. By sniffing the inter-process communication, Trojan families try to bind malicious processes and fork new threads to legitimate processes. As a result, malicious processes and threads are executed along with legitimate processes.

- *Get Device Information:* Trojan families try to get critical device information such as settings, IP addresses, and IMEI numbers. This information is used to identify the type of device and network used by the user. Further, it is helpful to reveal services performed by the operating system and applications installed on the device.

What to do if your device is infected with Trojans?

To stop the Trojans from doing any further damage to the device, it is important to remove them by following the steps mentioned below:

- *Identify unwanted applications that you did not install:* The easiest step is to identify and uninstall all unwanted applications that are installed without your permission and knowledge. This will also free phone memory and make the device faster. Although this step does not completely remove the Trojan from the device, but it prevents any further damage.
- *Reboot the device in safe mode:* Power off the device and reboot it in safe mode. Every Android phone has different options to restart in safe mode. Some phones provide a direct option to do so whilst others do not. So, you need to find the option on your phone to reboot in a safe mode.
- *Restore an earlier backup:* Most people do not take backup of their phone data. It is helpful to uninstall all data from the infected device and restore everything from a backup.
- *Factory reset:* If nothing works, the last step is to perform a factory reset. This will delete every installed application, settings, and data from the phone and revert the phone to a bare state.

Preventive measures to protect your device

Here are some imperative preventive measures that can be adopted to protect your device from the havoc created by Trojan Malware.

- *Use secure Wi-Fi connection:* Never connect to the free Wi-Fi available in public places. Always prefer to use a secure and password-protected Wi-Fi access point.
- *Install applications from a verified source:* Avoid using third-party applications. Even all applications in Google Play Store are not secure. As a user, you need to be aware of installing only legitimate applications.
- *Check application permissions:* Some applications request unnecessary permissions before installation. For example, an application meant for photography requires access to a camera and gallery which is understood. What if it is also requesting permission for accessing Wi-Fi state and device settings? You need to deny such permissions.
- *Update the operating system and applications:* It is the rule of thumb to update all applications and operating system to the latest version available.
- *Beware of phishing messages:* Do not click any links in any suspicious messages and emails. These links are intended to redirect the victim to malicious websites, software downloads, and other malicious activities.
- *Use strong passwords:* Always use strong and complicated passwords. Never use the same password for multiple accounts.

Conclusion

This article brings forward the fundamentals of Trojan malware categories and families. It is equipped with malicious functions performed by Trojans on the target device. We established imperative indicators of compromise that point to the fact that the

phone is infected by Trojan families. Based on our public dataset on Android malware, named *CCCS-CIC-AndMal-2020*, we open on technical features that are extremely useful to detect Trojan families. We divided these features into three types: memory, network, and API. As a non-technical person, every smartphone user must know the things that can be done if a Trojan is detected on a smartphone. We introduce the primary steps that can be performed if a Trojan is detected. Finally, the article introduces preventive measures to protect the device. The next article of the UAMF series will dig into ransomware (a crypo-locker) and scareware (a fear coaxer) malware categories.

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