Joker Is Still No Laughing Matter

July 13, 2021

- Richard Melick
- Android
- Jul 13 2021

As one of the key members of Google's App Defense Alliance, Zimperium helps ensure the Android ecosystem is safer by processing all apps before they reach Google Play. Despite this direct involvement, malicious applications can find their way to Android devices through various app stores, sideloaded applications, and compromises malicious websites that trick users into downloading and installing apps.

Since 2017, over 1,800 Android applications infected with Joker have been removed from the Google Play store, highlighting a long history of this malware and its evolution throughout the years. Despite Google's advanced technologies and its partnerships with malware security companies like Zimperium, the malicious actors have routinely found new and unique ways to get this malware into both official and unofficial app stores. While they are never long for life in these repositories, the persistence highlights how mobile malware, just like traditional endpoint malware, does not disappear but continues to be modified and advanced in a constant cat and mouse game.

Recently, the Zimperium zLabs mobile threat research team has noticed a large uptick in Joker variants on Android marketplaces, with over 1000 new samples since our last coverage in September of 2020. These variants were found using the same malware machine learning engine powering zIPS on-device detection and Google's App Alliance, proving that on-device detection capabilities are a must to ensure full protection of an enterprises' mobile endpoints.

Let's first recap why Joker is so effective and popular for Android malware.

What Is Joker?

Joker trojans are malicious Android applications that have been known since 2017 for notoriously performing bill fraud and subscribing users to premium services. The outcome of a successful mobile infection is financial gain for the cybercriminal, oftentimes under the nose of the victim until long after the money is gone, with little to no recourse for recovery.

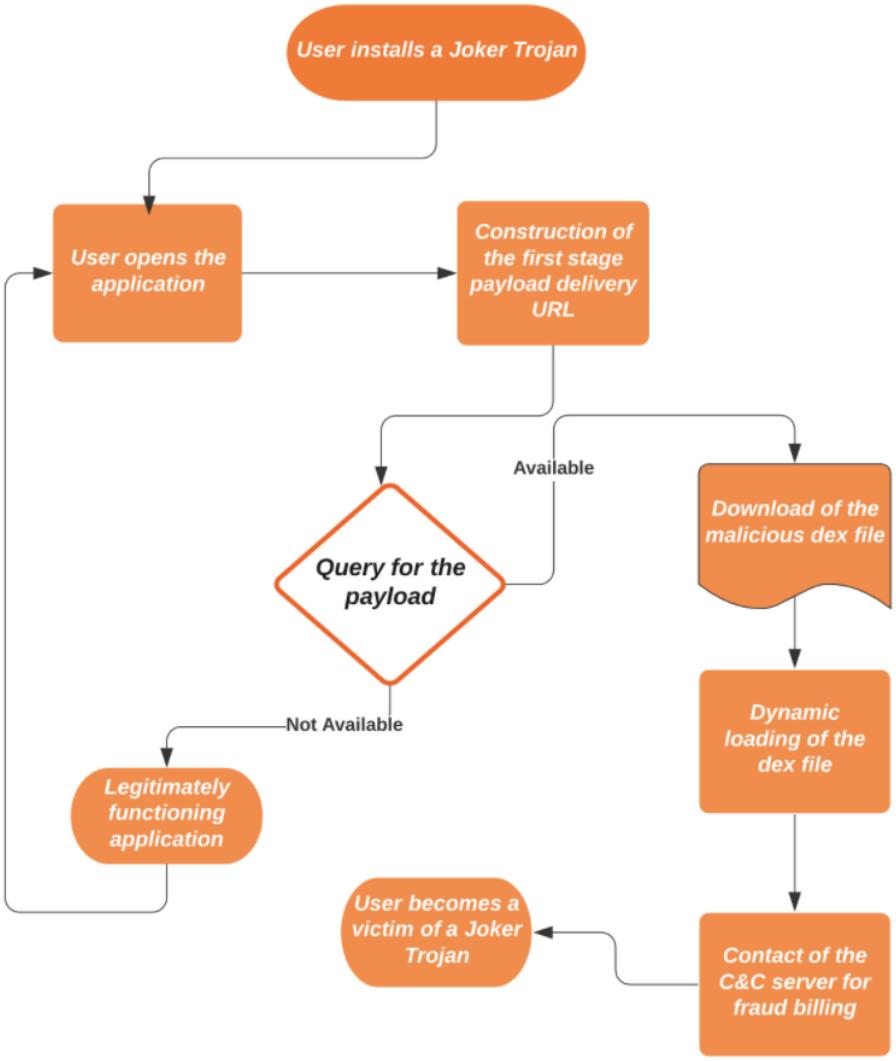
The trojan's main functionality is to load a **dex** file and perform malicious activities like inspecting the notifications or sending SMS messages to premium subscriptions. While Google Play have worked hard to bring alerts to the mobile user, Joker counts on the distracted nature of mobile alerts and social engineering for them to be accepted or even ignored.

The malicious activities can be divided into the following categories:

1. Decode or decrypt the strings to get the first stage URL.
2. Download the payload **dex** file from the above URL.
3. Load the payload **dex** file using reflection techniques to invoke the DexClassLoader constructor.
4. The **dex** file performs malicious activities and communicates with the C&C server.

In the following flowchart, the full attack chain is shown.

Flowchart.1:



These are the four pivot points each Joker sample uses, and it employs several evasion techniques to remain undetected. Most often, Joker is disguised as commonly downloaded applications like games, wallpapers, messengers, translators, and photo editors.

What Has Changed Since September 2020

The malicious developers behind the current, most advanced forms of Joker are taking advantage of legitimate developer techniques to try and hide the actual intent of the payload from traditional, legacy-based mobile security toolsets. They are starting by using the common framework Flutter to code the application in a way that is commonly seen by traditional scanners. Due to the commonality of Flutter, even malicious application code will look legitimate and clean, whereas many scanners are looking for disjointed code with errors or improper assemblies.

The malicious developers are embedding Joker as a payload that can be encrypted in different ways, either a **.dex** file xored or encrypted with a number, or through the same .**dex** file as before, but hidden inside an image using steganography. Both manners are obfuscating the intent of the payload from the legacy scan and mobile security tools.

After successful installation, the application infected with Joker will run a scan using Google Play APIs to check the latest version of the app in Google Play Store. If there is no answer, the malware remains silent since it can be running on a dynamic analysis emulator. But if the version found in the store is older than the current version, the local malware payload is executed, infecting the mobile device. If the version in the store is newer than the current one, then the command and control servers are contacted to download an updated version of the payload.

Joker Trojan's never seen before behavior includes URL shorteners, checking the current time against a hardcoded launch-time, image infected using steganography on legit cloud file hosting services, and a combination of native libraries to decrypt the offline payload from the APK's assets or connect to C&C for the payload.

Joker vs. Zimperium

Zimperium zIPS customers are protected against 100% of these Joker variants analyzed with our zero-day, on-device z9 Mobile Threat Defense machine learning engine model and static analysis.

As a standard protocol, the Zimperium zLabs team checks new malware samples against not only the current machine learning model but past ones as well. In the case of Joker, Zimperium zIPS customers have been constantly protected against these latest variants of this aggressive Android trojan.

To ensure your Android users are protected from the Joker malware, we recommend a quick risk assessment. Inside zConsole, admins can review which apps are side-loaded onto the device that could be increasing the attack surface and leaving data and users at risk.

About Zimperium

Zimperium, the global leader in mobile security, offers the only real-time, on-device, machine learning-based protection against Android, iOS, and Chromebook threats. Powered by z9, Zimperium provides protection against device, network, phishing, and malicious app attacks. For more information or to schedule a demo, contact us today.

Follow Us

← Michigan Secure Wins 'State IT Innovation of the Year' Award For 2021