New Tekya Ad Fraud Found on Google Play

blog.trendmicro.com/trendlabs-security-intelligence/new-tekya-ad-fraud-found-on-google-play/

June 5, 2020

In late March, researchers from CheckPoint found the Tekya malware family, which was being used to carry out ad fraud, on Google Play. These apps have since been removed from the store, but we recently found a variant of this family that had made its way onto Google Play via five malicious apps, although these have also been removed. (We detect these as AndroidOS_Tekya.HRX.)

Figures 1 and 2. Apps with Tekya malware (Click to enlarge)

Connections between two versions

This variant of Tekya shares many similarities with the previously found version. For example, the encryption remains essentially identical. The same algorithms and keys are used in both versions.

Figure 3. Encryption code from previous Tekya version

Figure 4. Encryption code from this Tekya version

How this Tekya variant works

The malware registered a receiver that responds to the actions “com.tenjin.RECEIVE” or “android.intent.action.BOOT_COMPLETED”. The latter action gives the malware the ability to wake after the device boots:

Figure 5. Registered receiver

The functionality of the receiver is implemented in libtenjin.so. Once called, it would then call a method which hides itself in a common package — specifically, com/google/android/gms/internal/ads/.

Figure 6. Malicious method call

The method called is responsible for downloading a .dex file and loading it. In the case we were analyzing, the said file would be downloaded twelve hours after the malware was installed. The downloaded file is encrypted; it is decrypted and loaded by libtenjin.so.

Figure 7. Decryption and loading of decrypted file

Once the downloaded .dex file been loaded, it would attempt to register itself with a configuration server. The information that is part of the registration includes device ID, user accounts, location, MAC address, and others (as seen below):

Figure 8. Properties uploaded to the configuration server

If the server did not reject the registration, an encrypted configuration file would be downloaded. This contains information about the ads to be loaded and control flags. (The blurred text contains information about about the ad accounts potentially used by the attacker, which we have opted to remove.)

Figure 9. Contents of downloaded configuration file

The malware would do various checks, including time, control flags, and so on based on the downloaded configuration. If those checks passed, Tekya would hide itself.

Figure 10. Code to hide icon

According to its code, Tekya would target up to 11 advertising networks, including: Admob, Facebook, and Unity. Advertisements from these networks would be displayed, and user touch events imitated through InputManager.

Figure 11. Code to load Admob

Figure 12. Code to inject input event

Tekya would try to trick victims into believing those advertisements were opened by other applications by changing its icon and label to that of another app on the device.

Figure 13. Code for Tekya to choose which icon and label to imitate

We originally found several of these apps on Google Play, but Google removed these from the App Store while our research was underway. We are still watching for any similar threats that may emerge in the wild.

Trend Micro solutions

Users can install security solutions, such as Trend Micro™ Mobile Security, that can block malicious apps. End users can also benefit from their multilayered security capabilities that secure the device owner’s data and privacy, and features that protect them from ransomware, fraudulent websites, spyware, and identity theft.

For organizations, the Trend Micro™ Mobile Security for Enterprise suite provides device, compliance and application management, data protection, and configuration provisioning. The suite also protects devices from attacks that exploit vulnerabilities, prevents unauthorized access to apps, and detects and blocks malware. Trend Micro’s Mobile App Reputation Service (MARS) covers Android and iOS threats using leading sandbox and machine learning technologies to protect users against malware, zero-day and known exploits, privacy leaks, and application vulnerability.

Indicators of Compromise (IOCs)

All of the malicious files below are detected as AndroidOS_Tekya.HRX.

Package name	SHA256 hash
awakens.download.mp3pro	35f9077b4774456526b088496413bd5559c293b7ae49da89c5b7b51132667879
com.waygame.hoppingcat	359f581980faa4e27acf19a9bfae0214d6e92690bcbce0d19e9b0053200f6cd2
com.halfbrain.trafficjam	114b8f6a345ee403487e79d4110fcd28e5a9b67ebe5821cd2f7a296d06ae1de2
com.halfbrain.petjumping	c4e00591e0eb947fded1ea925c3aa4e5e2f47a8adbfc096f174a84a2205bbf5a
com.runninggame.squarefish	0d58e04908a506adf06ec49e55227892d1abbe4ad245a822ff0dab15c774f2f4

Mobile

We observed a Tekya variant that had made its way onto Google Play via five malicious apps. Said apps were already removed from the Play Store.

By: Ford Quin June 05, 2020 Read time: (words)

Content added to Folio