# DroidCleaner

Threat: **Cross-Platform Malware**

Author: **Jeffrey Farnan** Date Originally Published: **October 29th, 2021**

## 1. SUMMARY


- DroidCleaner is a cross-platform attack which infects Android Smartphones but also transfers malware to USB connected Windows devices. The Android app poses as a system cleaner used to free up memory, and boost performance by cleaning out old data. The malware spies on the Android and Windows devices and sends the collected data back to the attacker's servers. This attack is not very sophisticated and only works against users running older or unpatched versions of Windows.


## 2. MALWARE FAMILY

- **Type** = Cross-Platform Malware.
- **Sub-type** = Spyware.

- **Cross-Platform:** Cross-Platform Malware is a malicious attack which involve multiple platforms in their attack method. Here are some example of cross-platform threats:
    - Threats that attack the same way in different platforms.
    - Threats that have specialized payloads for each platform they target.
    - Threats that have components that allow it to run on different platforms.
    - Threats that begin their attack routine on one platform to lead to more malicious routines on another platform.
- One of the factors making this attack possible is the popularity of inter-connectivity between mobile devices and laptops / desktops. With mobile devices such as phones / tablets, users are connecting these devices to their work / home system to sync their files and documents, allowing these threats to jump across platforms.
- **Spyware**: The Android malware is designed to steal data such as contacts, photos, SMS and the contents of memory cards on your smartphone. The Windows malware once executed is able to record input from your microphone, encrypt this information and send it back to the attacker's servers.

## 3. MALWARE CHARATERISTICS

- **Suspected country of origin** = Unknown.
- **First seen date/period** = 2013.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** = October 28th, 2021.

## 4. MALWARE HISTORY

- DroidCleaner was first seen in 2013, it was a new attack vector infecting Windows Operating systems from an Android device.
- Droidcleaner is also known as SuperClean, both billed themselves as apps which can free up memory making them run faster, which they actually don't do that at all.
- When this malware was discovered it was removed from Google Play, who said violated their policies. Before the apps were removed by Google, they may together have been downloaded up to 6000 times.
- The apps are still available from other sites, the malware authors may be targeting older versions of widows and may think there is enough unsophisticated users to make this malware worthwhile. With updated security measures this infection is less effective.

## 5. MALWARE DESCRIPTION

- This malware disguises itself as a tool called DroidCleaner / Superclean, which are actually the same application but released with two different names. The tool is supposed to clean memory for the Android operating system, making their phone run faster. The user is shown a fake graphical user interface, showing three different cleaning options that lead to the same fake progress bar.
-


- In the background the malware starts the infection process:

1. **Application installation**

   After installing the app on your Android Smartphone it seeks permissions so it can configure the device. These permissions give it access, change the Wi-Fi state, allow SMS manipulations, reads the user contact list details and uploads the SD card contents. Some of its other the features include:

   - Gathered information about the device
   - Opened arbitrary links in a browser
   - Sent the entire contents of the SD card to the attacker
   - Uploaded all the contacts/photos/coordinates from the device to the attacker
   - Enabled Wi-Fi
   - Uploading all SMS messages, delete SMS messages, enabled the sending SMS messages.

2. **Malware download**

   Once the malware is installed on the Android phone, it calls home to the attacker's remote server where it downloads executable malicious files on the root of the secure digital (SD) card.

3. **Malware infection**

   The malware known as **Backdoor.MSIL.Ssucl** lays in wait for you to connect it to your PC through the USB emulation mode, which allows your PC to view the device as an external storage device. The malware consists of three files "autorun.inf", "folder.ico" and "svchosts.exe". If AutoRun is enabled on your Windows machine, the transfer from the device to the PC is carried out via **autorun.inf**. Once this malware is executed the attackers now have a backdoor running on your PC.

4. **Information stealing**

   The Windows malware can control your microphone to eavesdrop on you, as soon as the microphone detects sound, it can begin to record the audio. It also targets voice chat software like Skype and records conversations. It can capture instant messaging conversations from apps such as Yahoo Messenger. All of the captured content is sent back to the attacker's server in encrypted format. The Windows component of this malware isn't nearly as apt as its Android counterpart.

## 6. POTENTIAL CUSTOMER DEFENSE

- All current and updated versions of Windows pose no risk to this malware, which have AutoRun for external devices is disabled by default. If you are downloading apps from Google Play Store look for apps from trusted developers. Here are some helpful tips to protect you from this malware:

  - People should be alert for unusual behaviour on their phone and make sure they have up to date security. People should look out or unknown applications being installed without user consent, SMS messages being sent to unknown recipients and automatic phone call being dialled.
  - If a user does have this app they need to remove it manually, unless they have an anti-virus solution which should remove it automatically.
  - Android users should be wary of apps which promise to speed up their devices, there is no miracle solution for old devices with low memory.

- The best piece of advice from security experts is to have anti-virus solutions on both Android and Windows operating systems.

**Research Sources:**


- https://www.firstpost.com/tech/news-analysis/android-app-supercleandroidcleaner-is-malware-says-net-security-agency-2-3619573.html
- https://redmondmag.com/articles/2013/02/06/android-malware-aims-to-infect-pc.aspx
- https://en.softonic.com/articles/kapersky-finds-new-android-and-pc-threat
- https://phys.org/news/2013-02-kaspersky-users-pc-infecting-malware.html


***Disclaimer:*** All opinions expressed in this article are the opinions solely of the author.