Android RATs Branch out with Dendroid

1 Recommend

Mar 05, 2014 09:24 AM

Migration User

Darwinism is partly based on the ability for change that increases an individual's ability to compete and survive. Malware authors are not much different and need to adapt to survive in changing technological landscapes and marketplaces. In a previous blog, we highlighted a free Android remote administration tool (RAT) known as AndroRAT (Android.Dandro) and what was believed to be the first ever malware APK binder. Since then, we have seen imitations and evolutions of such threats in the threat landscape. One such threat that is making waves in underground forums is called Dendroid (Android.Dendoroid), which is also a word meaning something is tree-like or has a branching structure.

Figure 1. *Dendroid advertisement banner*

Dendroid is a HTTP RAT that is marketed as being transparent to the user and firmware interface, having a sophisticated PHP panel, and an application APK binder package. The APK binder used by Dendroid just so happens to share some links to the author of the original AndroRAT APK binder.

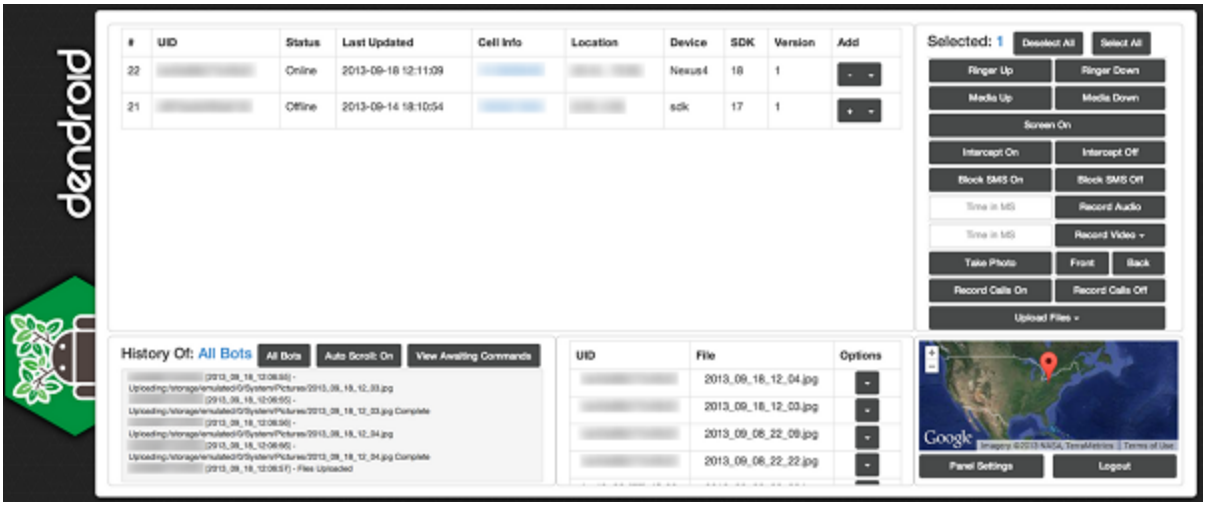

Figure 2. *Dendroid control panel*

According to postings on underground forums, the official seller of Dendroid is known as “Soccer.” The seller markets Dendroid as offering many features that have never been seen before and comes with 24/7 support, all for a once off payment of $300 to be paid through BTC, LTC, BTC-e, or other services. Some of the many features on offer include the following:

- Delete call logs
- Call a phone number
- Open Web pages
- Record calls and audio
- Intercept text messages
- Take and upload photos and videos
- Open an application
- Initiate a HTTP flood (DoS) for a period of time
- Change the command-and-control (C&C) server

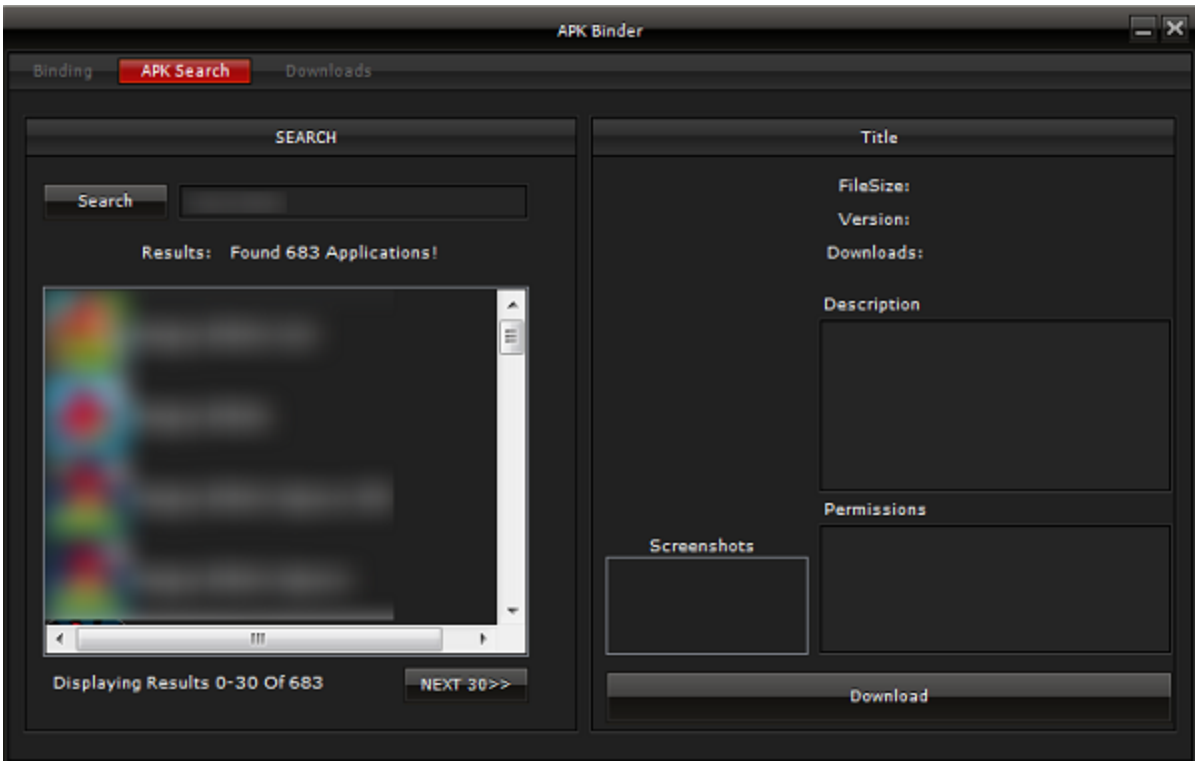

Figure 3. *Dendroid APK binder*

As previously mentioned, according to reports on underground forums, the author of the Dendroid APK binder included with this package had assistance writing this APK binder from the author of the original AndroRAT APK binder.

The evolution of remote access tools on the Android platform was inevitable. The creation of Dendroid and the positive feedback on underground forums for this type of threat shows that there is a strong cybercriminal marketplace for such tools. On the PC platform, other crimeware toolkits like Zeus (Trojan.Zbot) and SpyEye (Trojan.Spyeye) started off in a similar manner and grew quickly in popularity due to their ease of use and notoriety stemming from the high profile crimes perpetrated as a result of their usage. While this may be early days for Dendroid, Symantec will be keeping a close eye on this threat.

To stay protected, Symantec recommends installing a security app, such as Norton Mobile Security, which detects this threat as Android.Dendoroid. For general safety tips for smartphones and tablets, please visit our Mobile Security website.

Statistics

0 Favorited

0 Views

0 Files

0 Shares

0 Downloads

Tags and Keywords

Related Entries and Links

No Related Resource entered.