Bug in Android Development SDK Triggers MasterKey Detection

Sydney, Australia – July 23, 2013 - A week ago, Bitdefender announced an update to the Bitdefender Mobile Security and Bitdefender Antivirus Free to mitigate the MasterKey vulnerability.

Since then Bitdefender has started receiving reports about applications that manifest the MasterKey exploit behaviour – overwriting identically-named files inside the archive as they were cleared off digital signature inspection.

A closer look into a couple of these applications hosted on Google Play and it's revealed a potentially harmful common trait: they all had the air. prefix, a marker for applications written in Adobe Air.

Bitdefender have looked into their collection of Android applications and based on their telemetry, they have discovered that nearly 1.25 percent of the applications written in Adobe Air manifest the MasterKey behaviour and are blocked on patched Android distributions.

How the exploit works?

The MasterKey exploit works by including two duplicate files inside the same Android Package File (APK). When the Android device starts the application installation process, the operating system unpacks the APK file and extracts the files inside. However, since there are two identically-named files with the same path, the latter would overwrite the former, thus triggering the suspicious behaviour. The introduction of a duplicate file is not voluntary (as it would be in the case of a malicious attack), but rather the side effect of a bug in the development toolkit used by Android application developers – Adobe Air 3.7.0.153. The issue has been known and published on the Adobe bugtracker since April this year.

Who is impacted?

Although the icon substitution does not adversely impact device security, these applications will be denied the right to install on customers' devices if they are running a patched Android version (Cyanogen Mod or the upcoming Android 4.3, among others).

I'm a developer, how do I fix this?

If you're building Android applications using this specific version of Air, you should update to a newer version and rebuild your applications. If, for any reason, you are unable to update the development platform, you should simply remove any of the duplicate files by opening the APK file with any utility that can modify ZIP files and navigate to the resdrawable-xhdpi folder and delete one of the icon.png files inside.

***

About Bitdefender®

Bitdefender is the creator of one of the world's fastest and most effective lines of internationally certified internet security software. The company is an industry pioneer, introducing and developing award-winning protection since 2001. Today, Bitdefender technology secures the digital experience of around 400 million home and corporate users across the globe.

Recently, Bitdefender won a series of important awards and accolades in the global security industry, including "Product of the Year" by AV-Comparatives, "Best Repair 2012" by AV-Test, and "Editor's Choice" by PC Mag, that confirmed the antivirus software's leadership status among security products. More information about Bitdefender's products is available from the company's security press room. Additionally, Bitdefender publishes the HOTforSecurity blog, where readers can find stories from the underworld of internet fraud, scams, malicious software – and gossip.

For further information about Bitdefender, please contact

Danielle Zhu

Howorth Communications

02 8437 5342

Danielle@howorth.com.au