# DroidDream

## Your Guide to This Mobile Infection

### What you need to know about the DroidDream Mobile Malware

*If you love your Google Android phone and keep up with the latest in Android-related news, the chances are that you came across some scary stories this month about a new, malicious program designed to infect them. That program, dubbed DroidDream, was the subject of close coverage on Threatpost.com – and within the IT security community, which has been awaiting a tidal wave of mobile malware almost since the first smart phones hit store shelves more than six years ago. But what is DroidDream? And is it something to worry about, or just another example of security companies crying 'Wolf!' over something you're unlikely to ever come across in the real world? To answer your questions, Threatpost's editors have put together the following Spotlight to take a close look at DroidDream and answer some basic questions that mobile phone users need to know about this new mobile malware.*

### What is DroidDream, anyway?

*Like most malicious programs, DroidDream's name tells you absolutely nothing about what it actually is or does. Well, that's not entirely true – the 'Droid' part of DroidDream refers to Google's Android mobile operating system. The malware targets devices running Android. And the 'Dream' part? We have no idea about that, though – obviously – it rhymes with 'Droid,' which gives the malware a fun, alliterative name that bounces around in your mouth. In truth, DroidDream is more of a nightmare than a dream – a rootkit program that uses a known exploit known as "rageagainstthecage" or CVE-2010-EASY to defeat Android's native security features and gain root (administrative) access to the device.*

### How was DroidDream discovered?

*Largely by accident. The first reports of something suspicious came from the online news aggregation site Reddit, where one contributing user noticed that a number of popular mobile applications in the Android Marketplace appeared to be offered from two publishers simultaneously – one legitimate and the other new and suspicious. The user posted that observation in a section of the Reddit site devoted to Android discussion. After that, other users quickly downloaded copies of the applications and began analyzing them. They discovered that the applications in question, which had been downloaded tens of thousands of times (estimates put the number as high as 200,000 times) were functional copies of the real mobile apps that had been equipped with a rootkit program. Google was contacted shortly thereafter and acted quickly (as in 'within five minutes') to remove the applications from the Marketplace and from infected phones. Threatpost first reported on DroidDream on March 2.*

**Featured Articles:**

## Malware-Infected Apps Yanked From Android Market

***By Dennis Fisher***

A large number of apps in the Android Market have been found to contain a piece of malware known as DroidDream, a Trojan that not only is able to harvest sensitive data from an infected device, but also can break out of the Android sandbox and download additional malicious code to the phone from remote servers.

The infected apps were discovered and publicized on Tuesday and researchers immediately contacted officials at Google, who responded by removing the malicious apps from the Android Market. However, some researchers reported that tens of thousands of Android owners already had downloaded the malicious apps. The list of apps supposedly infected with DroidDream is long, and includes titles such as Super Guitar Solo, Falling Down, Super History Eraser and others, according to an analysis by researchers at Lookout Mobile Security. The infected apps seemed to be tied to a couple of publishers, including one named Myournet and another called KingMall2010.

Google has the ability to remotely remove apps from Android devices and it has used the functionality in the past to erase apps, including one developed by researcher Jon Oberheide as a proof of concept that was benign. It's not clear at this point whether Google has started removing any of the infected apps from devices, but the apps have been pulled from the Android Market.

The DroidDream malware has the ability to gather sensitive data, such as the IMEI number and IMSI identifier, and also can download additional code, according to one analysis.

"I asked our resident hacker to take a look at the code himself, and he's verified it does indeed root the user's device via rageagainstthecage or exploid. But that's just the tip of the iceberg: it does more than just yank IMEI and IMSI," wrote Aaron Gingrich in a post at Android Police. "There's another APK hidden inside the code, and it steals nearly everything it can: product ID, model, partner (provider?), language, country, and userID. **But that's all child's play; the true pièce de résistance is that it has the ability to download more code**. In other words, there's no way to know what the app does after it's installed, and the possibilities are nearly endless."

An analysis of the DroidDream malware by Kaspersky Lab malware researcher Tim Armstrong showed that it's quite stealthy and efficient at its tasks.

"So what is the purpose of this Trojan? The application will attempt to gather product ID, device type, language, country, and userID among other things, and then upload them to a remote server. Unlike most of the other samples seen so far, there is no attempt at sending or receiving premium rate SMS messages," Armstrong wrote in his analysis of the Android malware.

> "This discovery is important because up until now most of the Android malware has been found outside of the Android Market, which requires a number of special steps to be taken in order to infect the phones. In this case, users are even able to install from the web with the new Android Market format. We have previously talked about this here: The Dark Side of the new Android Market."

The Android Market is the official store for apps for Android-powered devices and comprises thousands of free and paid apps. It's not certain at this point how many users downloaded one or more of the infected apps, but users on Reddit began discussing the problem Tuesday.

"I appreciate being able to publish an update to an app and the update going live instantly, but this is a bit scary. Some sort of moderation, or at least quicker reaction to malware complaints would be nice," one user named Lompolo wrote. "After some dexing and jaxing, the apps seem to be at least posting the IMEI and IMSI codes to http://184.105.245.17:8080/GMServer/GMServlet, which seems to be located in Fremont, CA. The apps are also installing another embedded app (hidden as assets/sqlite.db), "DownloadProvidersManager.apk". Not sure what it does yet on top of monitoring what apps the user installs."

## What does DroidDream do to infected phones?

*DroidDream wasn't public for long before Google eradicated it from its Marketplace and auto removed it from infected phones. But that didn't stop some mobile security folks from taking a look at it first. What they found was concerning. As Threatpost reported on March 2, DroidDream had the ability to gather sensitive data such as the IMEI and IMSI identifier from infected phones. That data was piped off to a Web based server and could open the door to device cloning. Other functionality, hidden deeper in DroidDream's code, vacuumed up an even wider range of data: the phone model, installed language, country and user ID. It also contained a downloader program that could be used to dynamically update DroidDream with any number of different models: changing or adding functionality on the fly or even updating the code running on it with other, malicious programs. As Threatpost reported, that kind of modular design suggests that DroidDream was created with the goal of making money off of infected phones – possibly through the installation of adware or spyware, though its not clear whether the creators ever got that far.*

# *Analysis Shows DroidDream Trojan Designed for Future Monetization*

***By Dennis Fisher***

A detailed analysis of the DroidDream Trojan that was found in dozens of apps in the Android Market this week shows that the malware has a modular construction that likely was designed to give attackers the ability to monetize infected devices through installations of adware or spyware.

The Trojan itself is not especially clever or sophisticated and its communications with its command-and-control server on the back end are essentially by the book, as well. After infection, the DroidDream malware calls home to its C&C server to announce its presence and ask for further instructions. That's all rote, pro forma stuff.

What's most interesting in the DroidDream construction is that the Trojan is designed to act mainly as a downloader module, a shell to pull down other malicious modules in the future. This is the kind of malicious behavior that has been common in desktop and server malware for years now, but hasn't been seen widely on mobile devices as of yet. Most mobile malware up till now has been designed to carry out one or two specific tasks, say sending SMS messages to premium numbers or stealing online banking credentials.

"The highly modular architecture of the Trojan is interesting and points out of a few important conclusions. First of all, it has been designed to be easy to include in popular applications, to be uploaded on the Market with misleading names. Secondly, it has a classical command-and-control architecture – it sends an initial 'I'm here' query with basic info and then deploys a more complex downloader to infect the device further," Kaspersky Lab malware researcher Denis Maslennikov wrote in his analysis of the DroidDream Trojan. "This is pretty similar to many Windows Trojans. Finally, the ability to install other applications on the devices hints at the way through which the author was planning to monetize the infections – by deploying Adware or Advertising-supported apps on the device."


DroidDream was found in several dozen applications that were in the official Android Market this week. The apps that included the Trojan apparently were uploaded by three publishers after they had been loaded with the malware. Google quickly removed the apps from the market after researchers notified the company. Researchers estimated that more than 50,000 users had downloaded at least one of the apps, and some other estimates put the number at closer to 200,000 downloads.

The placement of malicious or malware-infected apps in mobile marketplaces has emerged as one of the more troubling attack vectors in the last year or so. None of the major mobile markets do full code reviews of apps before they are deployed in the markets and users tend to have a higher level of trust in apps from the iTunes App Store or Android Market than they do from third-party providers. Attackers have begun to exploit

the app store weaknesses in recent months and that trend is only going to expand as the penetration of smartphones continues to rise and the value of the data on those devices increases.

## Should I be concerned that DroidDream has infected my mobile phone?

*Yes and no. As Threatpost reported, Google acted quickly to remove the rogue applications from the Android Marketplace after learning of them. The company also disabled the accounts of the publishers who posted the rogue applications and used a remote "kill switch" feature to uninstall the compromised versions of the applications from infected phones. In theory, that should have taken care of any infections. Google also e-mailed affected users to inform them that they were infected and that their phones had been updated to remove the infection. So the short answer is that if you didn't receive such an e-mail, you don't have anything to worry about. If you did receive such a message, you're still probably OK. However, as we mentioned, DroidDream had the ability to install additional components on phones that it had compromised. There's no evidence that this happened, but if it did, its not clear that Google would be able to remove those additional programs from infected phones. If you're concerned, you may want to contact Google's Android Market Help Center (no, really) for more specific instructions on determining whether your phone was infected. You can get information about doing that from the Android blog.*

## *Google Throws App Kill Switch On DroidDream*

***By Brian Donohue***


Google has announced plans to implement new security features in order to strengthen the defenses of the Android Market following the appearance of a Trojan horse, DroidDream, targeting devices running the company's Android mobile operating system.

In a post on Google's official Android blog, Rich Cannings, the Android Security Lead, said that Google has removed malicious applications from the Android Market, suspended the accounts of developers associated with these applications, and contacted law enforcement. The company has also used a security feature that remotely removes malicious applications from affected devices.

Google plans to push a security update to all infected devices. The update, "Android Market Security Tool March 2011" will undo the exploit that led to the attack, and prevent attackers from gaining access to any further information. Owners of affected devices should receive an email from Google's support staff, notifying them that they were indeed infected and that the new security update has been applied.

In his post, Cannings also promised a number of less-specific measures to prevent similar occurrences in the future and to provide a fix for the specific, underlying security weaknesses that led to this in the first place.

Security experts have long predicted a wake-up call for mobile security, as powerful, late model smart phones become ubiquitous. In particular, the DroidDream Trojan horse, which was designed to monetize infected mobile phones, underscored weaknesses in Google's loosely monitored application Marketplace.

Writing in his blog post, Cannings said that security is a priority for the Android team. "We're committed to building new safeguards to help prevent these kinds of attacks from happening in the future," he wrote.

## What are my chances of getting infected with this thing?

*DroidDream infections happened when Android users downloaded and installed one of a list of malicious applications from the Android Marketplace. If you haven't downloaded one of the applications known to have been carrying the DroidDream Trojan, your chances of getting infected with it are practically nil. DroidDream isn't self replicating – it doesn't spread from phone to phone. And, as far as anyone knows, it was only available from the Android Marketplace. However, there are some caveats: we're not 100 percent sure there aren't other mobile applications out there that also contain the DroidDream code. That's especially true on loosely monitored third party application marketplaces where few checks – if any – are put on applications prior to publication.*

### Could DroidDream spread from a mobile phone to, say, a Windows computer?

*The short answer is: 'no.' DroidDream is written to run on Android mobile devices and hasn't been shown to be able to spread to non-Android devices, so you don't have to worry about it infecting your Windows or Apple OS X device. However, that doesn't mean you shouldn't worry. As Yankee Analyst Ted Julian wrote in an editorial for Threatpost, DroidDream is a wake-up call: the first time that clearly malicious (versus merely suspicious) applications have wound up on the official Android Market. "DroidDream's capabilities aren't revolutionary," Julian wrote, "but they are a clear step up for mobile malware. Notably: DroidDream has the ability to download additional code once it has infected its host, meaning that Google's application removal feature alone will not be sufficient to protect victims whose phones are already rooted."*

## DroidDream: Our Wake-Up Call For Mobile Security

***By Ted Julian, Yankee Group***

Security researchers today pulled more than 20 apps in the Official Android Market after they were found to have been infected with the DroidDream malware. Analysis of the DroidDream malware suggests that it can gather sensitive data like a mobile device's IMEI (International Mobile Equipment Identity) number and user ID, break out of Android's application security sandbox and download additional code. Sounds pretty scary, huh? Sure, but to grizzled security pros, it's a story that's also sadly familiar - and a sign of what's to come in the mobile devices market.

After all, security researchers have been discussing the risk of mobile application malware for some time. I've heard of at least one proof concept demonstration on Android (it was benign). Threatpost, among others, has written about the weakness inherant in the AppStore model. And though DroidDream's capabilities are perhaps novel on Android, they are run-of-the-mill components for modern malware more generally, and especially the ocean of malicious programs targeting devices running versions of



Microsoft's Windows operating system.

There are important differences between PC based malware and the environment in which DroidDream must operate. For one thing, Google has the ability to remotely remove apps from devices running Android, and will presumably leverage that capability in this case. There have already been multiple instances of rogue mobile apps in the wild (most in Russia andChina), but mobile application malware and the losses associated with it are still a small problem, overall, and mostly confined to so-called SMS Trojans that direct infected phones to send text messages to premium-rate lines outside of the U.S.

But we shouldn't take too much comfort from the similarities between malicious mobile applications and other kinds of malicious computer programs. Security threats over the past several decades have been shown to follow a well-establish path from theoretical, to practical, to weaponized releases seen in the wild, to proven damage. Sometimes this evolution happens very quickly, in other cases, it takes years to occur – if it ever does. But the stages are well established and security veterans have learned to watch them as a way of gauging theoretical risk vs. real and present danger (that warrants spending real money to defend against).

From this perspective, DroidDream is interesting because it represents an escalation of risk: the first time that clearly malicious (versus merely suspicious) applications have wound up on the official Android Market. DroidDream's capabilities aren't revolutionary, but they are a clear step up for mobile malware. Notably: DroidDream has the ability to download

additional code once it has infected its host, meaning that Google's application removal feature alone will not be sufficient to protect victims whose phones are already rooted. In short: DroidDream is a professional job: stealthy with multiple functions including the ability to gather valuable data and enhance its capabilities.

DroidDream is evidence (if we needed it) that we've failed to learn the lessons of the past in our haste to build out a broader mobile ecosystem. The result is that we risk suffering the same fate, but on an even broader and more global scale.

*Ted Julian is a Principal Analyst in Yankee Group's Anywhere Network Research Group and a frequent contributor to Threatpost. Ted leads Yankee's research in the area of network intelligence.*

## Will my anti-virus software spot DroidDream?

*Anti virus software for Android mobile devices from major vendors will generally detect a DroidDream infection if it has occurred. Threapost's parent company, Kaspersky Lab, offers a mobile security product that will both spot DroidDream infections and the exploits used to jailbreak the phone.*

## Is there anything really different about Droiddream compared to other mobile malware?

*Once again – the answer is 'yes,' and 'no.' Certainly, there are millions of examples of Windows-based malware with similar features as DroidDream. An analysis of the DroidDream malware by Kaspersky Lab malware researcher Tim Armstrong showed that DroidDream is quite stealthy and efficient at its tasks, and different from the most common form of mobile malware that's currently circulating: so-called SMS Trojans, that send Short Message Service (SMS) messages to premium rate phone numbers. In addition, DroidDream is notable because it was discovered lurking on the Android Market, a reputable hub for downloading mobile applications that is overseen by Google. "This discovery is important because up until now most of the Android malware has been found outside of the Android Market, which requires a number of special steps to be taken in order to infect the phones. In this case, users are even able to install from the web with the new Android Market format," Armstrong wrote.*

## Should I feel safe using mobile markets like Google's Android Marketplace or Apple's AppStore?

*Good question! The truth is that the vast, vast majority of applications offered on Android Marketplace or Apple's AppStore are perfectly safe and legitimate. That said, DroidDream has exposed real weaknesses in the way these application marketplaces are run. As Threatpost Editor in Chief Dennis Fisher wrote, DroidDream was just the latest piece of evidence that the app store model is broken, with no vetting of application code prior to publication and, obviously, loose monitoring of individual publishers. Of course, that kind of wide-open environment is great for enabling a fast and flexible application environment, but it's also ripe for abuse, as the publication of compromised applications in the case of DroidDream illustrates. Google seems to have gotten the message and has promised more scrutiny to application security. But that's hardly the only danger. Security researchers have also discovered security holes in the marketplace itself, that could allow attackers to force the installation of a malicious mobile application on Android users' phones. Google has since fixed the cross site scripting vulnerability, but it underscores the dearth of checks and speed bumps between mobile marketplaces and the devices themselves. That's something that malware authors and cybercriminals are sure to exploit as time goes by.*

## DroidDream Attack Underscores Weaknesses of App Stores

***By Dennis Fisher***

The Android Market incident that surfaced Wednesday in which Google was forced to pull more than 20 apps that had been Trojaned is the latest piece of evidence that the mobile app store model is broken and is setting users up for failure.

The details of the Android Market episode should be familiar by now. A handful of publishers in the market recently published several dozen apps that had been loaded with a piece of malware called DroidDream, which is capable of all kinds of nastiness. Among other things, the Trojan can grab a laundry list of information about the infected device and upload it to a remote server and also can download further malicious code, all in the background and without any interaction from the user.

This is hardly the first time that malware-infected apps have been found in a mobile app store, and there have been many examples of benign apps that researchers have uploaded to app stores that were proof of concept exercises that could have performed malicious actions. And Google has responded by removing the most recent batch of malicious apps from the Android Market and has the ability to remotely remove the apps themselves from devices.

However, as Chris Wysopal of Veracode points out, wiping the apps from the phones doesn't address the real problem, which is the persistent malware infection.

"The mobile devices are already compromised as the malware took advantage of kernel vulnerabilities to root the devices and download more malware that didn't come through the app store. Anyone who ran the malicious apps now has a compromised device running software with root permissions that Google cannot wipe," Wysopal wrote in a blog post.

"The exact same thing could happen tomorrow even though we know what Android kernel exploit code was used and there are new versions of Android that fix these issues. This is because many Android phones cannot be updated to the new versions of Android, 2.2.2 and 2.3, that fix the root holes. Many Android phone providers have customized their versions of Android so up to half of Android phones running 2.0, 2.1, 2.2 are sitting ducks to the same problem tomorrow."

Some of the same pieces that enabled this attack to take place on the Android Market also are in place in other app stores, such as the iTunes App Store. The lack of code review of new apps makes it relatively simple for attackers to get malicious apps into these repositories, and the implicit level of trust that users have in the app stores amplifies the effect.

The Android Market attack appears to have succeeded to a large degree, as somewhere north of 50,000 Android owners apparently downloaded at least one of the Trojaned apps. What the attackers plan or planned to do with those infected devices isn't clear, but what is clear is that this kind of operation is the coming thing. Attackers know it, researchers know it and now users know it.

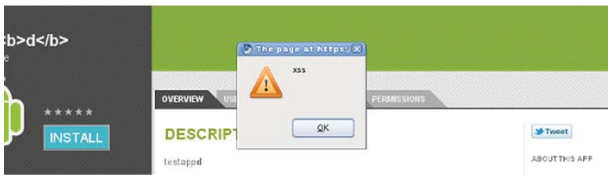


## Android Market XSS Bug Allowed Code Execution on Mobile Devices

***By Dennis Fisher***

A simple, trivially exploitable persistent cross-site scripting bug on the Google Android Web Market allowed anyone to upload an app that could be used to later run arbitrary code on the user's Android device. The vulnerability, which Google has patched, enabled an attacker to silently install his malicious app and then get any and all permissions on the device.

Security researcher Jon Oberheide discovered the



vulnerability recently and developed an exploitation scenario in which an attacker who could entice a user into clicking on a URL in the Web Market could force the user to install his malicious app. The attacker could then use one of a couple of methods to gain arbitrary code execution with the malicious app on the Android device. By inserting a small bit of HTML code in the field that developers use to describe their apps when their publishing them, an attacker can trigger the XSS vulnerability on a user's browser when he clicks on the link the Web Market to install an app.

The Android Web Market includes functionality that enables users who are browsing the Market on a desktop machine to automatically install apps on their devices simply by clicking on a link in the Market. The Android OS doesn't give users a prompt on the device to confirm an app install, which makes the attack scenario simpler.

"Since there is no on-device prompt or confirmation for these INSTALL_ASSET requests pushed to your phone, an attacker can silently trigger an malicious app install simply by tricking a victim into clicking a link while logged in to their Google account on their desktop or on their phone. The malicious app delivered to the victim's phone can use any and all Android permissions, allowing for all sorts of evil behavior," Oberheide said. "Simply installing the app does not result in code execution since apps do not auto-start upon install on Android. However, we can easily emulate this functionality effectively to auto-start our app and gain code execution."

There are two methods that an attacker could use to gain code execution once his app is installed. The first scenario involves having the app register for the PACKAGE_ADDED broadcast intent in Android. One that's done, the malicious app will run anytime another app is installed on the device, and because the attacker can control the user's browser via the XSS bug, he can force another app install and then use this method. The second way to gain code execution uses the mobile browser.

"Alternately, if our XSS is taking place within the browser of the mobile device itself, we can simply insert a hidden IFRAME in our XSS payload, continually set the src of the IFRAME to something like 'trigger://blah', and then have our installed malicious app register an intent filter on the 'trigger://' URI scheme," Oberheide said. "This will cause our malicious app to be triggered and gain code execution as soon as it is finished installing."

The vulnerability that Oberheide discovered, which Google has now patched, was present since the Android Web Market launched in February. It is just the latest issue to affect the security of the Android Market and comes just a week after researchers discovered that more than 50 apps had been uploaded to the Market that were infected with the DroidDream Trojan. That malware was designed to steal data about the infected phone and then download further malicious code.

Google removed the apps from the Market and is using its remote-wipe capability to delete them from infected Android devices as well. The company said over the weekend that it was pushing a fix for the Android vulnerability that the DroidDream attack leveraged and also is adding some unspecified new security measures to the Android Market to prevent future attacks like this.