EXHIBIT 11
TO DECLARATION
OF MATTHEW FISCHER

DroidDream Autopsy: Anatomy of an Android Malware Attack

Now that Google has flipped the kill switch to wipe out the DroidDream apps, the work to determine how the attacks work and prevent future attacks can begin.

By Tony Bradley
Mar 7, 2011 11:26 AM

The Android world is still reeling from the DroidDream invasion of the Android Market. Google has flipped the kill switch to wipe out apps associated with DroidDream, but the work of investigating how this Android Trojan infiltrated Google, and how to prevent similar attacks in the future is just beginning. Lookout--a mobile security company with tools to protect Android smartphones--has been diligently exploring the DroidDream apps to figure out what makes this malware tick. First and foremost, DroidDream is a Trojan attack that is hidden within seemingly legitimate apps. What makes it more insidious than other Android Trojans is that DroidDream managed to weasel its way into the actual Android Market. Let's break down what else we know about this threat:

• The malware is aptly named because it is designed to only run while the Android smartphone owner is sleeping--ostensibly dreaming peacefully. DroidDream is configured to do its dirty work between 11pm and 8am.

• DroidDream relies on two known exploits--exploid and rageagainstthecage--to break out of the Android security sandbox. Ironically--both of the targeted vulnerabilities were patched in Android 2.3 "Gingerbread". In this case, Android's fragmentation proved to be an Achilles heel because--although Gingerbread has been available for a couple months--less than one percent of all Android smartphones have received the update. Android users are at the mercy of individual smartphone vendors to deploy the Android OS update for their specific smartphone model.

• Once the Android smartphone is rooted, DroidDream searches for a specific package named "com.android.providers.downloadsmanager". If the package is not found, DroidDream silently installs a second malicious app without the user's knowledge. Other malicious apps can be installed in stealth from the DroidDream command and control servers.

• DroidDream sends a variety of information from the smartphone to the remote command and control center, including: IMEI, IMSI, device model, SDK version, language, country, and user ID.

Lookout has found that DroidDream is a powerful zombie agent that can silently install any applications and execute code with root privileges at will. According to Lookout, DroidDream is also the first piece of Android malware that uses an exploit to gain root permissions and assume virtually limitless control of the infected smartphone.

The elephant in the room, though, is the fact that DroidDream exploits vulnerabilities that have already been identified and patched, but that 99 percent of Android users are still exposed because their smartphone has not yet been graced with the update to Gingerbread.

Subscribe/Manage Account   Place Ad   LAT Store   Jobs   Cars

Los Angeles Times | BUSINESS

LOCAL   U.S.   WORLD   **BUSINESS**   SPORTS   ENTERTAINMENT   HEALTH   LIVING   TRAVEL

MONEY & CO.   TECHNOLOGY   PERSONAL FINANCE   SMALL BUSINESS   COMPANY TOWN   JOBS

IN THE NEWS: BARRY BONDS | LAKERS BEAT HORNETS | 'X FACTOR' | FINAL FOUR | LIBYA | RADIATION

Technology

THE BUSINESS AND CULTURE OF OUR DIGITAL LIVES,
FROM THE L.A. TIMES

« Previous Post | Technology Home | Next Post »

Google removing virus-infected Android apps from phones, tablets

March 7, 2011 | 10:57 am

(109)   (115)   (1)

Google is remotely removing virus-infected Android apps from thousands of phones and tablets in its continuing cleanup of what has become known as the "Droid Dream" scare.

Last Tuesday, Google removed 21 free apps that were hacked and loaded with malware, and then distributed on the company's Android Marketplace.

Since then, reports state that Google has removed more than 50 malicious apps from its Android Marketplace -- though, while Google has acknowledged that it has removed a number of apps, it so far has declined to say just how many.

On Saturday, Google began entering people's phones and tablets and killing the infected apps directly on those devices, said Rich Cannings, Google's Android security lead, in a blog post.

"For affected devices, we believe that the only information the attacker(s) were able to gather was device-specific (IMEI/IMSI, unique codes which are used to identify mobile devices, and the version of Android running on your device)," Cannings said.

"But given the nature of the exploits, the attacker(s) could access other data, which is why we've taken a number of steps to protect those who downloaded a malicious application."

Not only did Google start removing malware-infested applications from both its Android Marketplace and Android devices that had downloaded the bad apps, the tech giant has also suspended the Android Marketplace accounts of developers who've uploaded the virus-containing apps, he said.

Google is also passing along information on the attack to law enforcement agencies, Cannings said.

The removal of the malware apps from devices is one of the many increased security measures Google has had to employ in this ordeal, he said.

"We are pushing an Android Market security update to all affected devices that undoes the exploits to prevent the attacker(s) from accessing any more information from affected devices," Cannings said.

Google has sent out e-mails from its android-market-support@google.com address to the owners of affected Android phones or tablets beginning this Saturday through the end of the day Monday, detailing its actions, he said.

"You may also receive notification(s) on your device that an application has been removed," Cannings said, addressing affected Android users. "You are not required to take any action from there; the update will automatically undo the exploit. Within 24 hours of the exploit being undone, you will receive a second email."

Many of the affected apps removed from Android devices and the Android Market are believed to have been downloaded virus-fee, from their original publishers, and then hacked with malware, before being re-uploaded to Google's official app store by the new publisher.

Some have expressed privacy concerns over Google's ability to remove apps from devices remotely, though it is an action that Google makes clear it has the right to perfom in its Android Market Terms of Service, stating: "2.4 From time to time, Google may discover a Product on the Market that violates the Android Market Developer Distribution Agreement or other legal agreements, laws, regulations or policies. You agree that in such an instance Google retains the right to remotely remove those applications from your Device at its sole discretion."

The problems with the infected apps on the Android Marketplace, which have been nicknamed "Droid Dream" by many Android fan blogs and forums, follows news last month that multiple apps distributed on third-party websites have been known to run-up user's phone bills by taking over text messaging and Web browser functions.

Android is the world's most popular mobile operating system and the OS and its apps are built on and largely distributed on an open-source platform, which makes it very accessible to developers and hackers alike.

Amazon also announced last week that it was launching an Android app store of its own to compete with Google's official Android Market, and is calling it the Amazon Appstore.

RELATED:

Google removes 21 apps infected with malware from its Android Market, report says

Hacked Android apps rack up texting charges on users' bills

-- Nathan Olivarez-Giles

twitter.com/nateog

Photo: Google's Android 3.0 Honeycomb OS is demonstrated on a Motorola Xoom tablet during a press event at Google headquarters on Feb. 2 in Mountain View, Calif. Credit: Justin Sullivan/Getty Images

Twitter: @latimestech
Facebook: latimesbiz

More in: Android, Applications, Google, Mobile, mobile apps, Nathan Olivarez-Giles, Phones, Tablet, Tablet Computers

Comments (1)

Add a comment...

☑ Post to Facebook   Posting as Michael O'Donnell (log out)   **Comment**

Michael Vega · Arlington, Texas
Android Evo owners... watchalé its just the beginning!
Like · Reply · March 18 at 7:46pm

Facebook social plugin

fi
7

A

G

See

Mc

24
All
Bal
Bo
Cha
Cu
Da
Fal
Gr
Ho
L.A
L.A
La
Mi
Op
Pol
Pop
Sh
Top
Va

Los Angeles Times

Coastline Pilot | Daily Pilot |Huntington Beach Independent |Valley Sun | Burbank Leader |News Press |KTLA |Hoy |Brand X |LA, Los Ang
|Daily Press |Hartford Courant |LA Times |Orlando Sentinel |Sun Sentinel |The Morning Call

A Tribune Web site

Mail Online

Google issues hacking alert to 260,000 smartphone users who downloaded virus-infected apps

By Daily Mail Reporter
Last updated at 8:51 AM on 10th March 2011

Google yesterday admitted that up to 260,000 smartphones have been hacked after handset users unwittingly downloaded virus-infected apps.

The threat came to light last week when the technology giant was forced to withdraw at least 50 apps from its official Android Market.

Google operated a 'killswitch' and remotely removed all of the affected apps from peoples' phones.

Infected: Google has admitted that up to 260,000 smartphones have been hacked after handset users unwittingly downloaded virus-infected apps

The firm has now sent text messages warning those affected that the malicious applications could access their personal information and take control of their handset.

Studies have found that the dodgy applications were downloaded after they had been repackaged with a code that corrupted them.

Google Android is an open-source software stack for mobile devices that includes an operating system, middleware and key applications.

The deadly apps were simply copies of existing programs which had malware DroidDream found in them, and were swiftly taken off the site and recalled - but not before affecting hundreds of thousands of users.

DroidDream fires sensitive data, such as a phone's unique ID number, to a remote server.

In addition the malware will check if the phone has been infected already. If it hasn't the program bypasses security controls and hands its creator access to the handset.

This means that the user can access information, including passwords for other personal things.

Security expert Mikko Hypponen said the incident is embarrassing for Google because it shows the firm hasn't fully tested the safety of its apps.

'I do think Android phones are more vulnerable than any of the other major smartphones out there at the moment,' he told Metro.

A Reddit user first noticed the problem late last week after one program, which teaches people how to play a guitar on their mobile handset, was titled under the name of a publisher who didn't write it.

'Lompolo' discovered that the application was a carbon-copy of the original, however it had a name change and virus code added to is.

The user had worked out that the corrupted application had been downloaded more than 200,000 times after they were placed on the Marketplace.

The latest version of the Android operating system, known as Gingerbread, is not vulnerable to the exploits DroidDream uses.

Google has suspended three accounts being used by the developer of the apps.

Comments (23)

Newest
Oldest
Best rated
Worst rated

View all

. I must confess as a Mac user my comments here are more tongue in cheek wind ups than serious views based on personal experience. Childish I know... - John C, Rotherham S.Yorks, ---------- to be fair who can blame you. when you got people who cannot accept any criticism and defend it like crazy even though the companies dont really care and arent going to award you in any way and comments like "apple invented the world, i'd lived in darkness before apple gave me the light" "fandroids are unemployed" to "apple are for simpletons who cannot handle tech android is gives me freedom " "iSheeples", it's hard not to goad people

- iron man, london, 11/3/2011 11:34

Click to rate _ _ Rating   2

Report abuse

"I wished we lived in the world where android closed off a bit more and apple opened up a bit more, like everything in life a bit of balance is needed. But i doubt this would happen as fanboys form all sides will be up in arms and ruin another tech article. - iron man, london"---------------> Probably the most sensible comment in this thread. I must confess as a Mac user my comments here are more tongue in cheek wind ups than serious views based on personal experience. Childish I know...

- John C, Rotherham S.Yorks, 11/3/2011 07:37

Click to rate _ _ Rating   2

Report abuse

". Apples operating syetm is rarely hacked because so few people use it - Chris Davies , Stalybridge UK"------------------> No, it's rarely (if ever - effectively) hacked because it's much much harder to hack than Windows. Actually, Windows users should be grateful to Apple. The only reason Windows has improved so much since Microsoft highjacked the name is the competition it's getting from Apple. Without that stimulus...

- John C, Rotherham S.Yorks, 10/3/2011 23:29

Click to rate _ _ Rating   3

My goodness, looks like I struck a sensitive nerve or two! :-)) Well, there are certain things I don't do. I'm not a 'social networker' for the reasons and pitfalls others have stated, and I don't take photos of nearest and dearest (apart from my cats). I'm honestly going to try not to throw my new one down the loo (why is it the only time the world beats a pathway to your door is when you are in the bathroom?), and yes, I was mindful of the need to protect the screen (the only weak design fault, I think), so I bought a slip cover for it. For me I think that about covers what disadvantages there are to it, and it still means that I think Apple are ahead of the game from Android. I wasn't advised by a salesman, but a friend who is more tech-savvy than I am and researches all he buys very thoroughly. I think if you're happy with what you've got and can cope with the issues this article highlights, whether it's Android or Apple based, you're the person that counts. I'm 'Appy!

- Hilary, Oxfordshire, 10/3/2011 16:09

Click to rate _ _ Rating   2

Wow, looks like all the "I Hate Apple" crew is out Hilary. - Dazed and Confused, Where witches aren't allowed, US, -- And what the "i hate android" aint? have you seen tim in london comment - lol! Speaking of which "More fool you cheapskate Fandroids! Shoulda got that iPhone like your employed mates! - Tim, London" -- you must be a child, as if you're adult, i fear for this country's state, where you get people like you going crazy over a choice of phone. Steve Jobs isn't going to give you a medal you know(!)---- Anyway to the article, google should have beefed up security long before this, they are and open source, and it was a matter of time. I wished we lived in the world where android closed off a bit more and apple opened up a bit more, like everything in life a bit of balance is needed. But i doubt this would happen as fanboys form all sides will be up in arms and ruin another tech article.

- iron man, london, 10/3/2011 11:46

Click to rate _ _ Rating   1

More fool you cheapskate Fandroids! Shoulda got that iPhone like your employed mates!- Tim, (a bit dim) London, 10/3/2011 07:19..Seriously? All android owners are unemployed? What a stupid comment, and BTW my Galaxy tab cost more than your iphone.

- Mr V, Cheltenham, 10/3/2011 10:49

Click to rate _ _ Rating   6

Headlines
Most Read

- Mechanical wonder: Robot bird mimics flight so accurately it could be mistaken for the real thing
- Scientists to drill FIVE miles down: First journey to below the Earth's crust will go deeper than ever before
- That's just bananas! Cars made from FRUIT could be on the roads within two years, claim scientists
- The final cut: Hollywood director James Cameron's plans for 3D glasses to view Mars voyage scrapped by Nasa
- iPhone alarm glitch strikes again, leaving many an hour late for work
- Facebook puts vulnerable children at risk of depression, warn doctors
- Fighting fire with volts: How water hoses could be replaced with electric wands
- From candy floss to rock: Study shows the Solar System's soft beginnings
- Gone in 24 hours: iPad 2 fever as Apple's must-have tablet sells out
- Creationists say this petroglyph in Utah is proof dinosaurs and humans co-existed. But is it just a mud stain?
- Scientists hope DNA tests will be a plus for UK's dwindling adder population
- The final cut: Hollywood director James Cameron's plans for 3D glasses to view Mars voyage scrapped by Nasa
- International blackout: Iconic landmarks across the world are left in darkness to celebrate 'Earth Hour'
- Breakthrough technology that makes gadgets work faster - and uses less battery power
- U.S. develops cell phone 'panic button' that wipes out address books and sends emergency alerts

- Throw away those silly specs! Nintendo's 3D console does away with glasses... but some gamers can't see past the $250 price
-

- Creationists say this petroglyph in Utah is proof dinosaurs and humans co-existed. But is it just a mud stain?
- Gone in 24 hours: iPad 2 fever as Apple's must-have tablet sells out
- The picture of 21 magpies in a tree that proves population IS out of control
- Breakthrough technology that makes gadgets work faster - and use less battery power
- Scientists to drill FIVE miles down: First journey to below the Earth's crust will go deeper than ever before
- Ewe have got to be kidding! The 'puppy' born to a SHEEP
- Throw away those silly specs! Nintendo's 3D console does away with glasses... but some gamers can't see past the $250 price
- Scientists hope DNA tests will be a plus for UK's dwindling adder population
- The final cut: Hollywood director James Cameron's plans for 3D glasses to view Mars voyage scrapped by Nasa
- Technicolour dream planet: Earth as you've never seen it before
- The 'Holy Grail' of science: The artificial leaf researchers claim will turn every home into its own power station
- 100 bombs are washed up by the Supermoon: Lunar phenomenon blamed as Second World War devices are detonated on Hampshire beach
- Fighting fire with volts: How water hoses could be replaced with electric wands
- Killed by pollution: Hundreds of pieces of plastic found inside stomach of sea turtle
- Mechanical wonder: Robot bird mimics flight so accurately it could be mistaken for the real thing
- The health spa visited by SHARKS: Killers of deep go to cleaning stations to have dead skin nibbled off by tiny fish (just like us)
- MOST READ IN DETAIL

GADGET REVIEWS

Suunto M4 sports watch
Once you get over the feeling that you must be ill or at risk in some way to be monitoring your heart rate, the data supplied by this device offers some real surprises.

Google Nexus S smartphone
The Samsung Google Nexus S proved a rollercoaster of emotions for the first couple of weeks.

Review: Wireless TDK headphones
Straight out of the box and the TDK WR700 headset looks compact enough to wear on the Tube, with the cushioned earpieces offering a snug fit that.

Vogel iPad WallMount
Oh no, not another iPad accessory that I'll struggle to find a use for... Admittedly, that was my first thought when Vogel's iPad wall mount landed on my desk.

Samsung Galaxy Tab
Samsung's tablet PC is a lot more compact than the iPad and boasts some impressive features - but still fails to outshine its rival
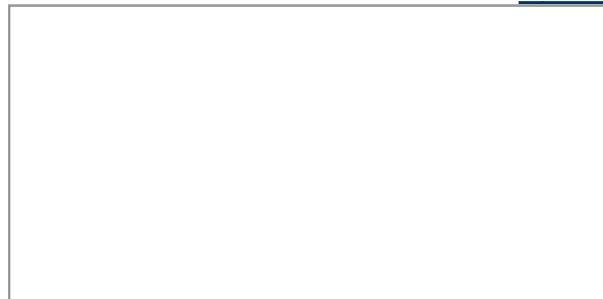
Altec Lansing's Octiv 202 dual dock
Now this is handy – not only can I charge my iPhone and listen my iPod at one and the same time but I can also do so on a unit that fits neatly into a corner.

Published by Associated Newspapers Ltd

Part of the Daily Mail, The Mail on Sunday & Metro Media Group

GlamEntertainment

© Associated Newspapers Ltd

BBC NEWS

TECHNOLOGY

3 March 2011 Last updated at 06:14 ET

Android hit by rogue app malware

More than 50 applications available via the official Android Marketplace have been found to contain malware.

Analysis suggests that the booby-trapped apps may have been downloaded up to 200,000 times.

The malicious apps were copies of existing software, such as games, that had been repackaged to include hidden code.

All the bogus applications have now been removed from the Android Marketplace.

Remove and recall
The rogue apps **were discovered by a Reddit user called Lompolo who realised that one program** was listed under the name of a publisher he knew had not written it.

He found that the app, which let people play guitar on their handset, was the same as the original but for a name change and some new code buried within it.

Lompolo said the rogue apps had been downloaded between 50,000 and 200,000 times since they were placed on the Marketplace.

Lompolo initially found 21 apps bearing malware but, **according to an investigation by mobile security site Android Police**, the final tally is believed to involve more than 50. The apps are also known to be available on unofficial Android stores too.

Once a booby-trapped application is installed and run, the virus lurking within, known as DroidDream, sends sensitive data, such as a phone's unique ID number, to a remote server.

It also checks to see if a phone has already been infected and, if not, uses known exploits to bypass security controls and give its creator access to the handset. This bestows the ability to install any code on a phone or steal any information from it.

The latest version of the Android operating system, known as Gingerbread, is not vulnerable to the exploits DroidDream uses.

Open access

As well as removing the applications from the Android Marketplace, Google has also suspended the three accounts being used by the developer behind the apps.

It also has the option to use a security tool that can recall and uninstall rogue applications from phones. It is not thought to have yet done this as its investigation continues. Google has yet to issue a formal statement about the rogue applications while it completes the investigation.

Writing on the Trend Micro security blog, Rik Ferguson, pointed out that remote removal of the booby-trapped apps may not solve all the security problems they pose.

"This remote kill switch will not remove any other code that may have been dropped onto the device as a result of the initial infection," he wrote.

He advised anyone who believed they had installed one of the malicious apps to find out whether they need to get a new handset or re-install the operating system on the one they have.

The open nature of the Android platform was a boon and a danger, he warned.

"This greater openness of the developer environment has been argued to foster an atmosphere of creativity," he wrote, "but as Facebook have already discovered it is also a very attractive criminal playground."

More Technology stories

Hackers target business secrets [/news/technology-12864666]
Intellectual property and business secrets are fast becoming a target for cyber thieves, study by security firm McAfee says.

Internet pioneer Paul Baran dies [/news/technology-12879908]

Apple iPhones hit by alarm glitch [/news/technology-12878517]

B B C

Subscribe/Manage Account   Place Ad   LAT Store   Jobs   Cars

Los Angeles Times | BUSINESS

LOCAL   U.S.   WORLD   **BUSINESS**   SPORTS   ENTERTAINMENT   HEALTH   LIVING   TRAVEL

MONEY & CO.   TECHNOLOGY   PERSONAL FINANCE   SMALL BUSINESS   COMPANY TOWN   JOBS

IN THE NEWS: BARRY BONDS | LAKERS BEAT HORNETS | 'X FACTOR' | FINAL FOUR | LIBYA | RADIATION

Technology

THE BUSINESS AND CULTURE OF OUR DIGITAL LIVES,
FROM THE L.A. TIMES

« Previous Post | Technology Home | Next Post »

Google removing virus-infected Android apps from phones, tablets
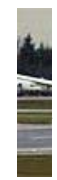
March 7, 2011 | 10:57 am

(109)   (115)   (1)

Google is remotely removing virus-infected Android apps from thousands of phones and tablets in its continuing cleanup of what has become known as the "Droid Dream" scare.

Last Tuesday, Google removed 21 free apps that were hacked and loaded with malware, and then distributed on the company's Android Marketplace.

Since then, reports state that Google has removed more than 50 malicious apps from its Android Marketplace -- though, while Google has acknowledged that it has removed a number of apps, it so far has declined to say just how many.

On Saturday, Google began entering people's phones and tablets and killing the infected apps directly on those devices, said Rich Cannings, Google's Android security lead, in a blog post.

"For affected devices, we believe that the only information the attacker(s) were able to gather was device-specific (IMEI/IMSI, unique codes which are used to identify mobile devices, and the version of Android running on your device)," Cannings said.

"But given the nature of the exploits, the attacker(s) could access other data, which is why we've taken a number of steps to protect those who downloaded a malicious application."

Not only did Google start removing malware-infested applications from both its Android Marketplace and Android devices that had downloaded the bad apps, the tech giant has also suspended the Android Marketplace accounts of developers who've uploaded the virus-containing apps, he said.

Google is also passing along information on the attack to law enforcement agencies, Cannings said.

The removal of the malware apps from devices is one of the many increased security measures Google has had to employ in this ordeal, he said.

"We are pushing an Android Market security update to all affected devices that undoes the exploits to prevent the attacker(s) from accessing any more information from affected devices," Cannings said.

Google has sent out e-mails from its android-market-support@google.com address to the owners of affected Android phones or tablets beginning this Saturday through the end of the day Monday, detailing its actions, he said.

"You may also receive notification(s) on your device that an application has been removed," Cannings said, addressing affected Android users. "You are not required to take any action from there; the update will automatically undo the exploit. Within 24 hours of the exploit being undone, you will receive a second email."

Many of the affected apps removed from Android devices and the Android Market are believed to have been downloaded virus-fee, from their original publishers, and then hacked with malware, before being re-uploaded to Google's official app store by the new publisher.

Some have expressed privacy concerns over Google's ability to remove apps from devices remotely, though it is an action that Google makes clear it has the right to perfom in its Android Market Terms of Service, stating: "2.4 From time to time, Google may discover a Product on the Market that violates the Android Market Developer Distribution Agreement or other legal agreements, laws, regulations or policies. You agree that in such an instance Google retains the right to remotely remove those applications from your Device at its sole discretion."

The problems with the infected apps on the Android Marketplace, which have been nicknamed "Droid Dream" by many Android fan blogs and forums, follows news last month that multiple apps distributed on third-party websites have been known to run-up user's phone bills by taking over text messaging and Web browser functions.

Android is the world's most popular mobile operating system and the OS and its apps are built on and largely distributed on an open-source platform, which makes it very accessible to developers and hackers alike.

Amazon also announced last week that it was launching an Android app store of its own to compete with Google's official Android Market, and is calling it the Amazon Appstore.

RELATED:

Google removes 21 apps infected with malware from its Android Market, report says

Hacked Android apps rack up texting charges on users' bills

-- Nathan Olivarez-Giles

twitter.com/nateog

Photo: Google's Android 3.0 Honeycomb OS is demonstrated on a Motorola Xoom tablet during a press event at Google headquarters on Feb. 2 in Mountain View, Calif. Credit: Justin Sullivan/Getty Images

Twitter: @latimestech
Facebook: latimesbiz

More in: Android, Applications, Google, Mobile, mobile apps, Nathan Olivarez-Giles, Phones, Tablet, Tablet Computers

A

G

Se

Comments (1)

Add a comment…

☑ Post to Facebook   Posting as Michael O'Donnell (log out)   **Comment**

Michael Vega · Arlington, Texas
Android Evo owners... watchalé its just the beginning!
Like · Reply · March 18 at 7:46pm

f Facebook social plugin

Mc

Corrections   Horoscopes   Media Kit   About Us   Co

Los Angeles Times

Coastline Pilot | Daily Pilot |Huntington Beach Independent |Valley Sun | Burbank Leader |News Press |KTLA |Hoy |Brand X |LA, Los An\
|Daily Press |Hartford Courant |LA Times |Orlando Sentinel |Sun Sentinel |The Morning Call

A Tribune Web site

Mail Online

Google issues hacking alert to 260,000 smartphone users who downloaded virus-infected apps

By Daily Mail Reporter
Last updated at 8:51 AM on 10th March 2011

Google yesterday admitted that up to 260,000 smartphones have been hacked after handset users unwittingly downloaded virus-infected apps.

The threat came to light last week when the technology giant was forced to withdraw at least 50 apps from its official Android Market.

Google operated a 'killswitch' and remotely removed all of the affected apps from peoples' phones.

Infected: Google has admitted that up to 260,000 smartphones have been hacked after handset users unwittingly downloaded virus-infected apps

The firm has now sent text messages warning those affected that the malicious applications could access their personal information and take control of their handset.

Studies have found that the dodgy applications were downloaded after they had been repackaged with a code that corrupted them.

Google Android is an open-source software stack for mobile devices that includes an operating system, middleware and key applications.

The deadly apps were simply copies of existing programs which had malware DroidDream found in them, and were swiftly taken off the site and recalled - but not before affecting hundreds of thousands of users.

DroidDream fires sensitive data, such as a phone's unique ID number, to a remote server.

In addition the malware will check if the phone has been infected already. If it hasn't the program bypasses security controls and hands its creator access to the handset.

This means that the user can access information, including passwords for other personal things.

Security expert Mikko Hypponen said the incident is embarrassing for Google because it shows the firm hasn't fully tested the safety of its apps.

'I do think Android phones are more vulnerable than any of the other major smartphones out there at the moment,' he told Metro.

A Reddit user first noticed the problem late last week after one program, which teaches people how to play a guitar on their mobile handset, was titled under the name of a publisher who didn't write it.

'Lompolo' discovered that the application was a carbon-copy of the original, however it had a name change and virus code added to is.

The user had worked out that the corrupted application had been downloaded more than 200,000 times after they were placed on the Marketplace.

The latest version of the Android operating system, known as Gingerbread, is not vulnerable to the exploits DroidDream uses.

Google has suspended three accounts being used by the developer of the apps.

Comments (23)

Newest
Oldest
Best rated
Worst rated

 View all

. I must confess as a Mac user my comments here are more tongue in cheek wind ups than serious views based on personal experience. Childish I know... - John C, Rotherham S.Yorks, ---------- to be fair who can blame you. when you got people who cannot accept any criticism and defend it like crazy even though the companies dont really care and arent going to award you in any way and comments like "apple invented the world, i'd lived in darkness before apple gave me the light" "fandroids are unemployed" to "apple are for simpletons who cannot handle tech android is gives me freedom " "iSheeples", it's hard not to goad people

- iron man, london, 11/3/2011 11:34

Click to rate _ _ Rating   2

Report abuse

"I wished we lived in the world where android closed off a bit more and apple opened up a bit more, like everything in life a bit of balance is needed. But i doubt this would happen as fanboys form all sides will be up in arms and ruin another tech article. - iron man, london"---------------> Probably the most sensible comment in this thread. I must confess as a Mac user my comments here are more tongue in cheek wind ups than serious views based on personal experience. Childish I know...

- John C, Rotherham S.Yorks, 11/3/2011 07:37

Click to rate _ _ Rating   2

Report abuse

". Apples operating syetm is rarely hacked because so few people use it - Chris Davies , Stalybridge UK"------------------> No, it's rarely (if ever - effectively) hacked because it's much much harder to hack than Windows. Actually, Windows users should be grateful to Apple. The only reason Windows has improved so much since Microsoft highjacked the name is the competition it's getting from Apple. Without that stimulus...

- John C, Rotherham S.Yorks, 10/3/2011 23:29

Click to rate _ _ Rating   3

[Report abuse](#)

My goodness, looks like I struck a sensitive nerve or two! :-)) Well, there are certain things I don't do. I'm not a 'social networker' for the reasons and pitfalls others have stated, and I don't take photos of nearest and dearest (apart from my cats). I'm honestly going to try not to throw my new one down the loo (why is it the only time the world beats a pathway to your door is when you are in the bathroom?), and yes, I was mindful of the need to protect the screen (the only weak design fault, I think), so I bought a slip cover for it. For me I think that about covers what disadvantages there are to it, and it still means that I think Apple are ahead of the game from Android. I wasn't advised by a salesman, but a friend who is more tech-savvy than I am and researches all he buys very thoroughly. I think if you're happy with what you've got and can cope with the issues this article highlights, whether it's Android or Apple based, you're the person that counts. I'm 'Appy!

- Hilary, Oxfordshire, 10/3/2011 16:09

Click to rate _ _ Rating   2

[Report abuse](#)

Wow, looks like all the "I Hate Apple" crew is out Hilary. - Dazed and Confused, Where witches aren't allowed, US, -- And what the "i hate android" aint? have you seen tim in london comment - lol! Speaking of which "More fool you cheapskate Fandroids! Shoulda got that iPhone like your employed mates! - Tim, London" -- you must be a child, as if you're adult, i fear for this country's state, where you get people like you going crazy over a choice of phone. Steve Jobs isn't going to give you a medal you know(!)---- Anyway to the article, google should have beefed up security long before this, they are and open source, and it was a matter of time. I wished we lived in the world where android closed off a bit more and apple opened up a bit more, like everything in life a bit of balance is needed. But i doubt this would happen as fanboys form all sides will be up in arms and ruin another tech article.

- iron man, london, 10/3/2011 11:46

Click to rate _ _ Rating   1

[Report abuse](#)

More fool you cheapskate Fandroids! Shoulda got that iPhone like your employed mates!- Tim, (a bit dim) London, 10/3/2011 07:19..Seriously? All android owners are unemployed? What a stupid comment, and BTW my Galaxy tab cost more than your iphone.

- Mr V, Cheltenham, 10/3/2011 10:49

Click to rate _ _ Rating   6

[Report abuse](#)

The views expressed in the contents above are those of our users and do not necessarily reflect the views of MailOnline.

[Headlines](#)
[Most Read](#)

- [Mechanical wonder: Robot bird mimics flight so accurately it could be mistaken for the real thing](#)
- [Scientists to drill FIVE miles down: First journey to below the Earth's crust will go deeper than ever before](#)
- [That's just bananas! Cars made from FRUIT could be on the roads within two years, claim scientists](#)
- [The final cut: Hollywood director James Cameron's plans for 3D glasses to view Mars voyage scrapped by Nasa](#)
- [iPhone alarm glitch strikes again, leaving many an hour late for work](#)
- [Facebook puts vulnerable children at risk of depression, warn doctors](#)
- [Fighting fire with volts: How water hoses could be replaced with electric wands](#)
- [From candy floss to rock: Study shows the Solar System's soft beginnings](#)
- [Gone in 24 hours: iPad 2 fever as Apple's must-have tablet sells out](#)
- [Creationists say this petroglyph in Utah is proof dinosaurs and humans co-existed. But is it just a mud stain?](#)
- [Scientists hope DNA tests will be a plus for UK's dwindling adder population](#)
- [The final cut: Hollywood director James Cameron's plans for 3D glasses to view Mars voyage scrapped by Nasa](#)
- [International blackout: Iconic landmarks across the world are left in darkness to celebrate 'Earth Hour'](#)
- [Breakthrough technology that makes gadgets work faster - and uses less battery power](#)
- [U.S. develops cell phone 'panic button' that wipes out address books and sends emergency alerts](#)

- Throw away those silly specs! Nintendo's 3D console does away with glasses... but some gamers can't see past the $250 price
-

- Creationists say this petroglyph in Utah is proof dinosaurs and humans co-existed. But is it just a mud stain?
- Gone in 24 hours: iPad 2 fever as Apple's must-have tablet sells out
- The picture of 21 magpies in a tree that proves population IS out of control
- Breakthrough technology that makes gadgets work faster - and use less battery power
- Scientists to drill FIVE miles down: First journey to below the Earth's crust will go deeper than ever before
- Ewe have got to be kidding! The 'puppy' born to a SHEEP
- Throw away those silly specs! Nintendo's 3D console does away with glasses... but some gamers can't see past the $250 price
- Scientists hope DNA tests will be a plus for UK's dwindling adder population
- The final cut: Hollywood director James Cameron's plans for 3D glasses to view Mars voyage scrapped by Nasa
- Technicolour dream planet: Earth as you've never seen it before
- The 'Holy Grail' of science: The artificial leaf researchers claim will turn every home into its own power station
- 100 bombs are washed up by the Supermoon: Lunar phenomenon blamed as Second World War devices are detonated on Hampshire beach
- Fighting fire with volts: How water hoses could be replaced with electric wands
- Killed by pollution: Hundreds of pieces of plastic found inside stomach of sea turtle
- Mechanical wonder: Robot bird mimics flight so accurately it could be mistaken for the real thing
- The health spa visited by SHARKS: Killers of deep go to cleaning stations to have dead skin nibbled off by tiny fish (just like us)
- MOST READ IN DETAIL

GADGET REVIEWS

Suunto M4 sports watch
Once you get over the feeling that you must be ill or at risk in some way to be monitoring your heart rate, the data supplied by this device offers some real surprises.

Google Nexus S smartphone
The Samsung Google Nexus S proved a rollercoaster of emotions for the first couple of weeks.

Review: Wireless TDK headphones
Straight out of the box and the TDK WR700 headset looks compact enough to wear on the Tube, with the cushioned earpieces offering a snug fit that.

Vogel iPad WallMount
Oh no, not another iPad accessory that I'll struggle to find a use for... Admittedly, that was my first thought when Vogel's iPad wall mount landed on my desk.

Samsung Galaxy Tab
Samsung's tablet PC is a lot more compact than the iPad and boasts some impressive features - but still fails to outshine its rival
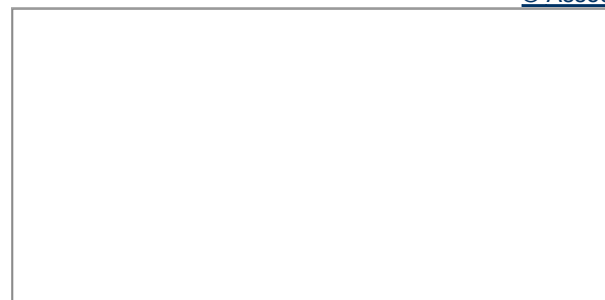
Altec Lansing's Octiv 202 dual dock
Now this is handy – not only can I charge my iPhone and listen my iPod at one and the same time but I can also do so on a unit that fits neatly into a corner.

Published by Associated Newspapers Ltd

Part of the Daily Mail, The Mail on Sunday & Metro Media Group

GlamEntertainment
© Associated Newspapers Ltd

BBC NEWS

TECHNOLOGY

3 March 2011 Last updated at 06:14 ET

Android hit by rogue app malware

More than 50 applications available via the official Android Marketplace have been found to contain malware.

Analysis suggests that the booby-trapped apps may have been downloaded up to 200,000 times.

The malicious apps were copies of existing software, such as games, that had been repackaged to include hidden code.

All the bogus applications have now been removed from the Android Marketplace.

Remove and recall
The rogue apps **were discovered by a Reddit user called Lompolo who realised that one program** was listed under the name of a publisher he knew had not written it.

He found that the app, which let people play guitar on their handset, was the same as the original but for a name change and some new code buried within it.

Lompolo said the rogue apps had been downloaded between 50,000 and 200,000 times since they were placed on the Marketplace.

Lompolo initially found 21 apps bearing malware but, **according to an investigation by mobile security site Android Police**, the final tally is believed to involve more than 50. The apps are also known to be available on unofficial Android stores too.

Once a booby-trapped application is installed and run, the virus lurking within, known as DroidDream, sends sensitive data, such as a phone's unique ID number, to a remote server.

It also checks to see if a phone has already been infected and, if not, uses known exploits to bypass security controls and give its creator access to the handset. This bestows the ability to install any code on a phone or steal any information from it.

The latest version of the Android operating system, known as Gingerbread, is not vulnerable to the exploits DroidDream uses.

Open access
As well as removing the applications from the Android Marketplace, Google has also suspended the three accounts being used by the developer behind the apps.

It also has the option to use a security tool that can recall and uninstall rogue applications from phones. It is not thought to have yet done this as its investigation continues. Google has yet to issue a formal statement about the rogue applications while it completes the investigation.

Writing on the Trend Micro security blog, Rik Ferguson, pointed out that remote removal of the booby-trapped apps may not solve all the security problems they pose.

"This remote kill switch will not remove any other code that may have been dropped onto the device as a result of the initial infection," he wrote.

He advised anyone who believed they had installed one of the malicious apps to find out whether they need to get a new handset or re-install the operating system on the one they have.

The open nature of the Android platform was a boon and a danger, he warned.

"This greater openness of the developer environment has been argued to foster an atmosphere of creativity," he wrote, "but as Facebook have already discovered it is also a very attractive criminal playground."

More Technology stories

 Hackers target business secrets [/news/technology-12864666]
Intellectual property and business secrets are fast becoming a target for cyber thieves, study by security firm McAfee says.

Internet pioneer Paul Baran dies [/news/technology-12879908]
Apple iPhones hit by alarm glitch [/news/technology-12878517]