

To InformationWeek

[Advertise With Us](#)

[About Us](#)

[Contact Us](#)

[Digital Subscription](#)

Welcome Guest

[Login to your account](#)

[Register](#)

SECTIONS ▼



[Home](#)

[News & Commentary](#)

[Authors](#)

[Slideshows](#)

[Video](#)

[Reports](#)

[White Papers](#)

[Events](#)

[Black Hat](#)

[Attacks/Breaches](#)

[App Sec](#)

[Cloud](#)

[Endpoint](#)



-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

-
-
-
-
-
-

[Mobile](#)
[Perimeter](#)
[Risk](#)
[Operations](#)
[Analytics](#)
[Vulns/Threats](#)



-
-
-
-
-
-

[Login to your account](#)
[Register](#)
[About Us](#)
[Contact Us](#)
[Digital Subscription](#)
[Advertise with Us](#)



-
-
-
-

[Facebook](#)
[Twitter](#)
[LinkedIn](#)
[Google+](#)

[RSS](#)



Follow DR:

[Home](#)

[News & Commentary](#)

[Authors](#)

[Slideshows](#)

[Video](#)

[Radio](#)

[Reports](#)

[White Papers](#)
[Events](#)
[Black Hat](#)

[Attacks/Breaches](#)

[App Sec](#)

[Cloud](#)

[Endpoint](#)

[Mobile](#)

[Perimeter](#)

[Risk](#)

[Operations](#)

[Analytics](#)

[Vulns/Threats](#)

Mobile

11/29/2013

08:06 AM



Mathew J. Schwartz
Slideshows

Connect Directly



9 comments

[Comment Now](#)

[Login](#)


100%

Like 59 Tweet 9 Share g+1 35

Android Security: 8 Signs Hackers Own Your Smartphone

Security experts share tips on how to tell if attackers are in control of your Android smartphone.

Searching for signs of Android infection



Image (derived) courtesy of Flickr user [.RGB.](#)

How can you tell if your Android smartphone or tablet been pwned?

That was the question recently posed by one InformationWeek reader, who suspected that her phone had been compromised by attackers. "I've only owned my Droid phone for two months and had a Trojan horse panic attack, and wiped my phone," she said via email.

Sponsor video, mouseover for sound

Can you tell by observation alone if your Android device has been infected with malware? On Windows PCs, for example, some types of infections leave no signs at all. Conversely, some virus, malware, and Trojan infections -- as well as adware and spyware -- may slow systems to a crawl, begin redirecting browsers to arbitrary websites or search engines, trigger pop-up ads, block access

to information security websites, disable security software, alter the user interface, or email everyone in your address book, leading to a flurry of outraged emails, bounce-backs, and warnings from recipients.

As with some Windows infections, some types of Android malware might sport telltale signs of infection. For example, the reader -- who asked not to be named -- said she became concerned when a text message preview appeared on her lock screen, then mysteriously disappeared and couldn't be found. Perhaps not coincidentally, she'd also recently installed an app -- but not from the official Google Play store.

"What happened was I downloaded an app from a non-Play store site -- against my better judgment. Then not too long after I was looking at some article about security issues, and I had something really bizarro happen," she said. "A text notification with a partial preview flashed in my notifications bar and then vanished -- from a number not in my contacts. ... I went into my text messages app to try and read the full message, and it wasn't there. At that point I panicked and was convinced my phone must be hijacked -- even though nothing else seemed amiss -- and just wiped it."

But was her phone infected? And if it was, how might other Android users spot a malware attack? Recent versions of the Android operating system, as well as mobile antivirus software, can [help spot and block](#) malware-infection attempts. But neither approach is infallible. So no matter which security tools you might be using, be sure also watch for the following telltale warning signs:



[Comment](#) | [Email This](#) | [Print](#) | [RSS](#)

More Insights

Webcasts

[Simplified IT 105: Making the Most Of the Cloud](#)

[eSecurity 102: Protecting Back-End Systems](#)

More Webcasts

White Papers

[The State of Data Center Networking](#)

[7 Security Gaps in the Neglected 90% of Your Application](#)

More White Papers

Reports

[Ponemon Institute Research: How IT security is addressing threats to structured and unstructured data](#)

[IBM System Storage Interactive Product Guide: Intelligent, efficient and automated storage for your IT infrastructure](#)

More Reports

Comments

**[FreeTipss](#),**

User Rank: Apprentice

8/6/2014 | 7:44:11 PM

[Login](#)

50%0%

More security tips for the Smartphones.

That's cool. You might want to check these 10 important Smartphone security Tips too.

<http://freetipss.com/smartphone-security-tips-10-useful-tips/>

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)

**[RoopaL731](#),**

User Rank: Apprentice

7/25/2014 | 6:40:19 AM

[Login](#)

50%0%

secure android mobiles

this app <http://hangoverstudios.com/mobileantitheft/> which helps you find lost phone's location and picture of thief.

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)



[mrhobbes](#),

User Rank: Apprentice

7/9/2014 | 9:21:59 AM

[Login](#)



100%

Android Security needs to be increased

Nice article on Android Security, Mathew, Great work.

Android is more prone to malware impacts due to Google's loose developer agreement, you can check it on my blog post regarding the same topic <http://goo.gl/LyLHse> you can of course, give your opinion regarding the same. If Google increases there security measure, then surely a lot of malware and PAU's can be avoided.

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)



[anon9673719294](#),

User Rank: Apprentice

6/26/2014 | 2:37:51 AM

[Login](#)



50%

Interesting

I recently found a useful app in Amazon that not required any unnecessary permissions and store all your passwords - [MyPasswords](#)

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)



[pnally,](#)

User Rank: Apprentice
12/12/2013 | 11:52:21 AM

[Login](#)



50%0%

I'm only seeing 7 "signs"

I'm only seeing 7 "signs" listed in the article... Was it hacked? ;)

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)



[anon6601743669,](#)

User Rank: Apprentice
12/11/2013 | 9:10:33 PM

[Login](#)



0%100%

Re: MISCONCEPTION

Jailbreaking is an iOS term because Apple keeps iSheep in jail as it were with the locking down of the OS. Rooting on the Android side is from the Linux world, which basically means you gain root access of the OS.

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)



[WayneT637](#),

User Rank: Apprentice
12/10/2013 | 12:47:36 AM

[Login](#)



50%0%

The Benefits of Rooting-

The first benefit of accessing administrator privileges over Android is full control over the applications installed on your handset. No longer do you have to suffer from the cluttered app drawers and reduced memory space taken up by pre-installed carrier and manufacturer applications, you can instantly cut the bloatware and keep only the apps that you really want.

Even if you're up to date with Android 4.1 or above, which grants users the ability to disable these pre-installed apps if you don't want to see or use them, you can't permanently remove them, they're still there eating up your memory space. Rooting is the only way to permanently get rid of these pesky apps, but please don't uninstall something crucial or your handset may stop working properly. Apps like Titanium Backup are particularly helpful for organising and culling this bloatware.

This brings me nicely on to the next major benefit of Android, improved backup and restore options. As already mentioned, Titanium Backup is one of the most popular backup apps used by rooters, and this, or a similar app, is essential if you're going to start tinkering around with Android software. But as well as acting as a safety net in case you uninstall something important, Titanium Backup can also be used to backup your user data, from SMS messages to browser bookmarks.

ClockworkMod Recovery Backup Cropped

ClockworkMod Recovery offers superior protection against faulty updates and bricking your handset.

Even better still, once rooted you can create complete backups of your entire handset using the ClockworkMod Recovery option, providing you with extra protecting in case of a major malfunction. Recovery can only be accessed before booting into Android, but it provides additional backup options in case, for whatever reason, Android fails to boot properly or experiences a crippling error. This makes ClockworkMod Recovery an essential tool for those looking to install custom versions of Android.

Once you're fully backed up you're ready to move up to one of the other major perks of rooting, installing different versions of Android.

We all know that manufacturers are often pretty slow at delivering the latest Android offerings even to their flagship handsets, let alone aging devices. So if you're not a Nexus or Play

Edition device owner, rooting opens the door to much faster Android updates, thanks to the developers who put time into porting the latest updates to various handsets.

Pretty much every semi-popular handset has a decent following of developers working on porting the latest versions of Android to their handsets, most of which can be found over on the XDA Forum. The only sacrifice here is that you won't receive official manufacturer versions of Android, so no updated Touchwiz or Sense5 features, but if we were really too worried about that we probably wouldn't be rooting in the first place.

If stock Android isn't your thing, there are also tons of other customized ROMs offering unique features and improvements to the default Android experience.

AOSP has given us so many custom ROM's, and has extended the lifespan of many an Android.

AOSP has given us so many custom ROM's, and has extended the lifespan of many an Android handset.

I'm sure you've all heard of the biggest names, CyanogenMod, Paranoid Android, MIUI to name just a few of the most popular ones. Many custom ROMs are actually at the forefront of innovation on Android, offering several features that aren't available anywhere else. Paranoid Android's Halo feature or OmniROM's multi-workspace mode are just a couple of examples.

But as well as these big third party developments, you'll also find a lot of smaller developers tweaking away at the core Android experience, offering ROMs with vastly superior battery life

or overclocked processor speeds. Not to mention that most custom ROMs are updated to the latest version of Android very quickly too, bringing you the best of both worlds.

As rooting opens up administrator type privileges on your handset you'll instantly have access to all the core files on your handset. File browser apps can take full advantage of this, allowing you to move stuff around on your internal memory if so require.

App wise, we've already touched on Titanium Backup, but there are far more apps that can make use of root permissions, and simply aren't available with a non-rooted device. The speed junkies among you could take advantage of overclocking software to boost performance or save on battery life, providing that your Kernel supports overclocking. Alternatively, fans of custom ROMs can use a ROM manager to install and update their operating system without the need to flash zip files from Recovery.

Rooting is sometimes criticized for compromising handset security, but security apps, such as Cerberus, use root functions to bury themselves deep down into the operating system, making them hard for would be thieves to remove. These apps can also be granted permissions that aren't available on unrooted devices, such as access to GPS data even when the device is locked.

There's also additional gesture apps, data syncing software, and even theme managers to customize the look of your handset.

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)



[sjennison](#),

User Rank: Apprentice

12/9/2013 | 8:19:59 PM

[Login](#)



50%~~0~~%

Re: MISCONCEPTION

Agreed. In fact, custom ROMs are generally *more* secure, due to constant updates (nightly, weekly, or monthly, depending on the developer). That is assuming, of course, your ROM dev is fast on their updates.

In fact, the major "master key" exploit, which is one of the biggest security holes, was patched by Cyanogenmod long before the vast majority of manufacturers got around to fixing it.

<http://www.ubergizmo.com/2013/07/cyanogenmod-10-1-2-fixes-android-master-key-exploit/>

Also, generally rooting allows you to do things like *fix* the security holes in the system. Rooting installs a root control app (Superuser/SuperSu, etc) that restricts access to only apps the user allows. While the device can still be compromised using privilege escalation vulnerabilities just like any other device, rooting will not make your device insecure. The very fact that a device can be rooted using exploits means it is inherently insecure due to those same exploits. A malicious piece of software could exploit them just as easily. Rooting doesn't change that, unless you go deeper and actually fix the hole (assuming you can). Hence where custom ROMs come in - when a vulnerability is found, they release patches in less than a month. The only other OEM who comes close to that speed is Google. Nearly every other

manufacturer takes months if not years to push an update through to end users.

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)



[krishel67801](#),

User Rank: Apprentice

12/5/2013 | 2:47:00 PM

[Login](#)



100%

google aps

Google Play Store is malware in itself. I have numerous aps that require play store services to be activated. Play store then accesses your phone whenever it wants to. Also play store will not allow aps that block advertising to be obtained through them. Another good reason for rooting your phone. Take control away from google.

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)



[Aroper-VEC](#),

User Rank: Apprentice

12/2/2013 | 10:31:04 PM

[Login](#)



50%

Re: MISCONCEPTION

Jailbreaking and rooting are synonymous. This is because of the nature of the action. Technically speaking, you use root access to jailbreak a device running iOS. It is only called "rooting" in Android because they want to be different than anything having to do with Apple but, the sum result is the same. When jailbreaking an iOS device in order to unlock the device and load a "clean" or alternate version of the OS and to get rid of bloatware you are doing the same thing in Android. The term is irrelevant since the process and the result are the same.

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)

Page 1 / 2 > >>



Subscribe to Newsletters

Partner Perspectives [What's This?](#)



In a digital world inundated with advanced security threats, Intel Security seeks to transform how we live and work to keep our information secure. Through hardware and software development, Intel Security delivers robust solutions that integrate security into every layer of every digital device. In combining the security expertise of McAfee with the innovation, performance, and trust of Intel, this vision becomes a reality.

As we rely on technology to enhance our everyday and business life, we must too consider the security of the intellectual property and confidential data that is housed on these devices. As we increase the number of devices we use, we increase the number of gateways and opportunity for security threats. Intel Security takes the “security connected” approach to ensure that every device is secure, and that all security solutions are seamlessly integrated.

[VIEW LATEST PERSPECTIVES](#)

Featured Writers



Live Events

Webinars



More UBM Tech
Live Events

**App Developer Conference @
GDC Next**

**iBeacons, BLE beacons and
Everything in Between: Unpacking
Proximity Sensing Technology @
Black Hat Europe**

**Consumerization of IT?: Worry
About the Consumerization of
Service**

White Papers

[AT&T Synaptic Storage as a Service with Enterprise File Sync and Share](#)

Privileged Identity Management

Federate Identities - Key to Seamless SSO

Healthcare Information Management: A New Urgency

Top 10 Things Every Web Application Firewall Should Provide

More White Papers

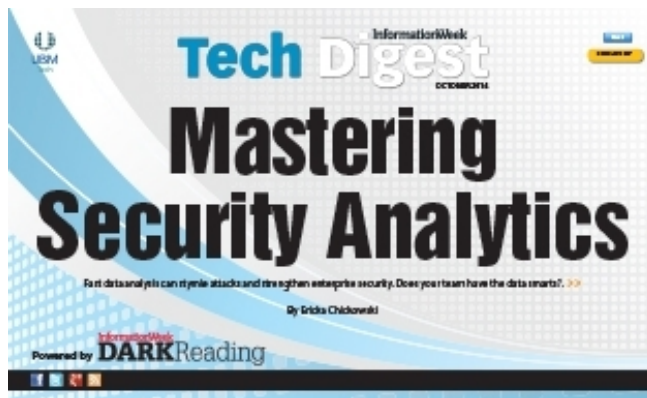
Cartoon



Latest Comment: [Great to have strong password. But look carefully at how easy it is for somebody to reset your password - often so easy that cracking the ...](#)

Cartoon Archive

Current Issue



Dark Reading's October Tech Digest

Fast data analysis can stymie attacks and strengthen enterprise security. Does your team have the data smarts?

[Download This Issue!](#)

[Subscribe Now!](#)

[Back Issues | Must Reads](#)

Flash Poll

What steps are you taking or planning to take in response to the Shellshock/Bash bugs? (Check all that apply.)

- Patching what we can and trying to stay up to date on new vulnerabilities
- Checking vendors' patch information against the

CVEs

Taking an inventory of the

- contents of every smart device in our company

Replacing every non-upgradeable or un-auditable

- device with something we can control

- We're not doing anything

- What's Bash?

- Other (please describe in the comments)

Submit

All Polls

Reports

Infographics



Containing Corporate Data on Mobile Devices

If you're still focused on securing endpoints, you've got your work cut out for you. WiFi network provider iPass surveyed 1,600 mobile workers and found that the average US employee carries three devices -- a smartphone, a computer, and a tablet or e-reader -- with more than 80% of them doing work on personal devices.

Download Now!

More Reports

Video



All Videos



Slideshows



The Internet of Things: 7 Scary Security Scenarios

 **5 comments** | [Read](#) | [Post a Comment](#)

[Be Aware: 8 Tips for Security Awareness Training](#)


 **13**


[7 Reasons To Love Passwords](#)

 **12**


[More Slideshows](#)

[Twitter Feed](#)

 **DarkReading** @DarkReading 17 Oct
The Internet of Things: 7 Scary Security Scenarios #IoT
ubm.io/1tzQuFn pic.twitter.com/TyTDHT77LK
Retweeted by Vineet Bhatia



Expand

 **Secure360 Conference** @Secure360 8m
Survey shows most orgs can't keep up with new threats: ubm.io/1xneBFd? From @DarkReading



Bug Report

Enterprise Vulnerabilities From DHS/US-CERT's National Vulnerability Database

[CVE-2014-7484](#)

Published: 2014-10-20

The Coca-Cola FM Guatemala (aka com.enyotech.radio.coca_cola.fm_gu) application 2.0.41725 for Android does not verify X.509 certificates from SSL servers, which allows

man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.

[CVE-2014-7485](#)

Published: 2014-10-20

The Not Lost Just Somewhere Else (aka it.tinytap.attsanotlost) application 1.6.1 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.

[CVE-2014-7486](#)

Published: 2014-10-20

The Mitsubishi Road Assist (aka com.agero.mitsubishi) application 1.0 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.

[CVE-2014-7487](#)

Published: 2014-10-20

The ADT Aesthetic Dentistry Today (aka com.magazinecloner.aestheticdentistry) application @7F080181 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.

[CVE-2014-7488](#)

Published: 2014-10-20

The Vineyard All In (aka com.wVineyardAllIn) application 0.1 for Android does not verify

X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.

Best of the Web

[**In A First, Commerce Department Fines Intel Subsidiary For Exporting Encryption**](#)

[**Apple Updates \(not just Yosemite\)**](#)

[**What Microsoft's Agile Development Plans Mean for Application Security**](#)

[**Hacker-hunters finger 'Keyser Soze' of Russian underground card sales**](#)

[**'Malvertising' targets U.S. military firms in new twist on old web threat**](#)

More Articles

Dark Reading Radio

Archived Dark Reading Radio

Security Reports From the Field

Follow Dark Reading editors into the field as they talk with noted experts from the security

world.

FULL SCHEDULE | ARCHIVED SHOWS



[About Us](#)

[Contact Us](#)

[Customer Support](#)

[Sitemap](#)

[Reprints](#)

[Twitter](#)

[Facebook](#)

[LinkedIn](#)

[Google+](#)

[RSS](#)



Featured UBM Tech Sites **InformationWeek** | **Network Computing** | **Dr. Dobbs** | **Dark Reading**

Our Markets: **Business Technology** | **Electronics** | **Game & App Development**

Working With Us: Advertising Contacts | Event Calendar | Tech Marketing Solutions | Corporate Site | Contact Us / Feedback

[Terms of Service](#) | [Privacy Statement](#) |

Copyright © 2014 UBM Tech, All rights reserved
