Protect Your Tech

Scams and threats to avoid, plus new security tools

WATCH OUT FOR...

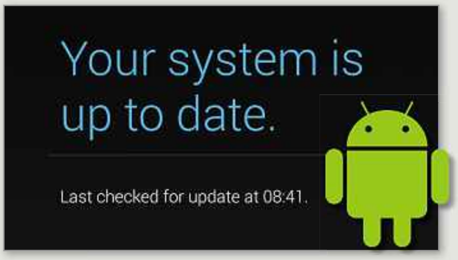
Android malware disguised as images

What happened?

Google have released an updated version of Android to fix a security flaw that could have allowed hackers to infect phones and tablets with malicious software.

The flaw was discovered by researchers Axelle Apvrille and Ange Albertini, who demonstrated how it could be exploited to disguise malware as image files (formats such as PNG and JPEG), tricking security apps into thinking it's safe. It also fools Google's Bouncer, which scans the Play Store for malicious apps.

In their research paper Apvrille and Alberti showed how an app that could steal photos, emails and other data was made to look like an image of the *Star Wars* villain Darth Vader. They said such attacks can easily bypass security tools because they don't look suspicious.



Your system is up to date.

Last checked for update at 08:41.

Fortunately, they didn't publicise the flaw until Google had fixed it in a new Android update, so hackers can't now take advantage of it on devices running the old version.

What should you do?

Make sure you're using the latest version of Android (4.4.4), which isn't vulnerable to the flaw. How you check this depends on the device, but the process doesn't vary too much. Generally, you need to open Settings (often represented by a cog icon), then scroll down and tap 'About phone' or 'About tablet'. Tap 'System updates' or 'Software update' (or something similar) and Android will search for an update or display the message "Your system is up to date" (see screenshot).

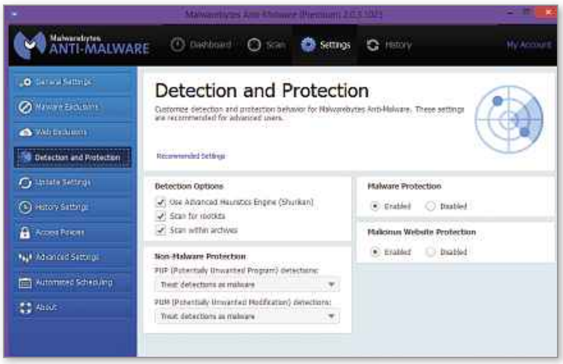
If Android needs to search for an update, agree to the installation when prompted. This will reboot your device, so make sure you're not in the middle of something important.

Unfortunately, many device manufacturers won't immediately offer this update, which means hackers do have a window of opportunity. Until you can update Android to the 4.4.4 version, make sure you only open images you know are safe.

New tools

Malwarebytes Anti-Malware 2.0.3
www.snipca.com/14096

The release of Version 2.0.3 was announced in a post on the Malwarebytes forum (www.snipca.com/14097) that listed so many repaired faults, it makes you wonder how the software ever worked properly in the first place. That said, it shouldn't stop you updating what is one of the best free security tools available.



Detection and Protection

Customize detection and protection behavior for Malwarebytes Anti-Malware. These settings are recommended for advanced users.

Recommended Settings

Detection Options
☑ Use Advanced Heuristics Engine (Shuriken)
☑ Scan for rootkits
☑ Scan within archives

Non-Malware Protection
PUP (Potentially Unwanted Program) detections: Treat detections as malware
PUM (Potentially Unwanted Modification) detections: Treat detections as malware

Malware Protection
● Enabled ○ Disabled

Malicious Website Protection
● Enabled ○ Disabled

What pleases us most is that Malwarebytes has fixed a bug that caused the program to keep crashing in Chrome. Another fix stops it crashing when you use the 'Copy to Clipboard' function. A word of warning, though – some early users of 2.0.3 reported that the Malicious Website Protection tool was showing as "disabled", and couldn't be activated. You'll find their complaints on the Forum post mentioned above, along with solutions from Malwarebytes. It's great to see the software developers responding so quickly.

ScamWatch

READERS WARN READERS

Financial Ombudsman scam

Over the past few years I've received several phone calls from scammers telling me there's a virus on my PC, but last week I was targeted by a new scam. The scammers claimed to be from the Financial Ombudsman Service (FOS), and said I was entitled to compensation. They sounded quite professional, but I smelled a scam when they asked for £150 to process the compensation. It seemed implausible to me that the FOS would phone people and ask for money. Read more on the Action Fraud website about this scam at www.snipca.com/14011.

Edmund Hardy

Warn your fellow readers about scams at letters@computeractive.co.uk