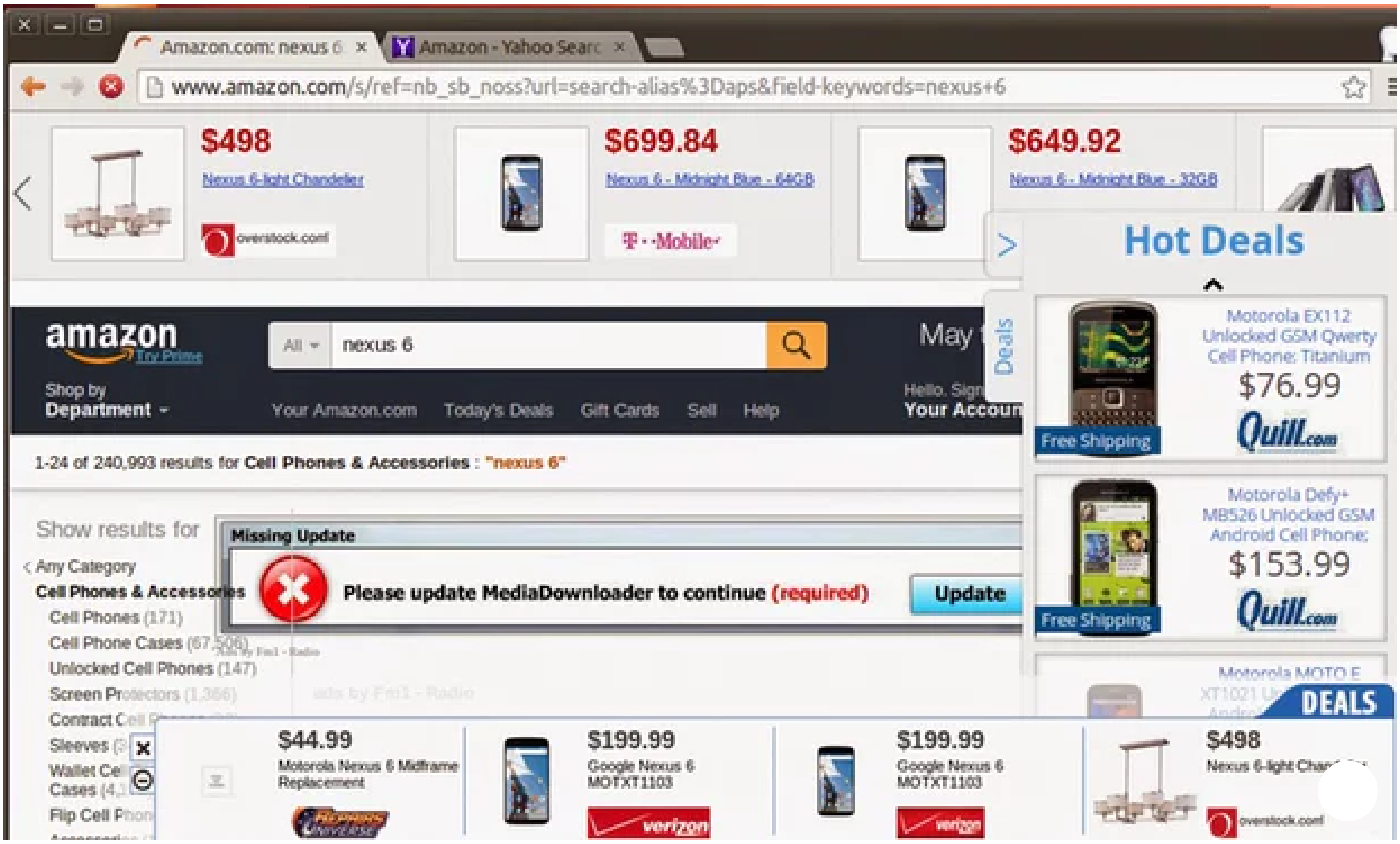
theguardian



Please update MediaDownloader to continue (required)

One in 20 web users infected with ad injection software

Google announces crackdown on software and removes ‘deceptive’ extensions from Chrome webstore following new research

Alex Hern

Thu 7 May 2015 05.20 EDT

More than one in 20 web users are infected with ad injectors, a type of malware that puts unwanted adverts on web pages, according to new research from Google.

As a result, the company has announced a new crackdown on the software, which can manifest either as a browser extension or a standalone application. Google removed almost 200 “deceptive” extensions from the web store for its Chrome browser, and has started to use Chrome’s safe browsing features to display warnings to users who are (likely unknowingly) about to download ad injection software. It has a long way to go, though, as the company’s research reveals that there are more than 50,000 browser extensions and 34,000 apps that inject ads into users’ browsers.

Perhaps most importantly, the company is also going after ad injection software at the root, informing advertisers whose ads are showing up in the software “to alert [them to] the deceptive practices and ad networks involved”. And since Google also runs one of the world’s biggest ad networks itself, through its AdWords service, it has been able to take action there, updating its polices "to make it more difficult for advertisers to promote unwanted software".

Google's Kurt Thomas explained why the company decided to act. "Ad injectors' businesses are built on a tangled web of different players in the online advertising economy," he wrote. This complexity has made it difficult for the industry to understand this issue and help fix it. We hope our findings raise broad awareness of this problem and enable the online advertising industry to work together and tackle it."

Ad injection is more than just an annoyance. It also represents a potential security hazard for browsers. In order to inject adverts into a website, the ad injector typically has to break the encryption used to deliver the page safely. In doing so, it opens users up to having their connection hijacked if any third party can insert themselves in the middle of their communications, easy enough to do if surfing on an open wireless network in a coffee shop or airport.

In February, it was revealed that PC manufacturer Lenovo had been shipping laptops with ad injection software pre-installed. The software, called Superfish, was ostensibly an "image search engine", but broke user security and injected visual adverts into Google searches.

Topics

Google