**The Register®**
*Biting the hand that feeds IT*

Software

# Google nukes ad-blocker AdNauseam, sweeps remains out of Chrome Web Store

## Web advertising giant declares plugin is malware

5 Jan 2017 at 22:34, Thomas Claburn

Google has removed ad blocking and privacy extension AdNauseam from its Chrome Web Store, and has taken the unusual step of flagging the extension as malware, thereby preventing AdNauseam from being used by those who have installed the software via Chrome's developer mode.

Chrome users who put their browser into developer mode and install the extension – by dragging the AdNauseam .crx file onto the extension management page – will see it install. But Google overrides that choice, presenting a prompt that says, "To make Chrome safer, we have disabled the following extension that isn't listed in the Chrome Web Store and may have been added without your knowledge."

Google's action does not entirely preclude the possibility of using the software. Because AdNauseam is open-source software, a developer can install his or her own version of the code as a local extension or through enterprise policy. The makers of AdNauseam have provided instructions to do so.

Google in 2013 banned ad blocking for Android apps in the Google Play Store, for violating its prohibition on interfering with the function of other apps. It conducted another purge in early 2016, banning stand-alone ad blocking apps like Adblock Fast and Crystal. It subsequently formalized its stance with a Play Store policy update, allowing browsers with built-in content blocking support to remain.

Ad blocking continues to hurt online publishers, even as some acknowledge that ad-driven online media is a "broken system." Internet users who block online ads cite security, page load performance, and privacy among their reasons for doing so.

Web technology has traditionally been more open than native code on mobile devices, but over the past few years, Google has tightened control over its browser – urged on, the company claims, by complaints from users.

In May 2014, Google implemented a new policy, ostensibly to protect Windows users, by requiring that Chrome extensions be hosted on the Chrome Web Store. According to a May 2015 blog post written by Google extensions platform product manager Jake Leichtling, the policy was a success, reducing customer support help requests to remove unwanted extensions by 75 per cent.

As a result, Google extended its Chrome extension oversight to Windows and Mac users. According to Leichtling, Google originally did not enforce this policy for developers. But he said that malicious software took advantage of the exception and forced users into the developer channel to install off-store extensions. Consequently, in July 2015, Google applied its malware enforcement mechanism to general release and developer Chrome channels.

AdNauseam's stated goal is "to obfuscate browsing data and protect users from tracking by advertising networks" and to serve as "a means of amplifying users' discontent with advertising networks that disregard privacy and facilitate bulk surveillance agendas."

It thus opposes the current, largely unrestrained practices of the online advertising business, upon which Google depends. The creators of the software, Daniel C Howe, Mushon Zer-Aviv, and Helen Nissenbaum, characterize AdNauseam as a form of protest against online surveillance.

"We are attempting to bring to light a system that has taken over the web, whereby ads are just the tip of the iceberg and serve as a delivery system for a massive back-end surveillance architecture that tracks us from site to site," the trio explain on the project's Github repository. "It is not advertising we are protesting, but advertising insofar as it represents a dominant means of tracking users without their consent."

Google did not respond to a request to explain its decision to disable AdNauseam. It informed the company, "An extension should have a single purpose that is clear to users..."

"Frankly it is quite patronizing to argue users don't know what they're doing when they install AdNauseam, especially since they need to explicitly allow AdNauseam to hide and click ads and to completely block malicious ads," Zer-Aviv said in an email to *The Register*. "They are spying on us, we're trying to protect against that and we're flagged as malware?"

AdNauseam is based on uBlock, a popular open-source ad blocking application. But it takes ad blocking a step further by clicking on the ads it has hidden, in order to pollute behavioral profiles used for ad targeting. In so doing, it costs advertisers money (which arguably gets wasted anyway).

In online discussions, people have suggested that automated ad clicking meets the legal definition of fraud.

Zer-Aviv disputes this claim. "Unlike click fraud, we do not benefit financially from these clicks," he said. "Moreover, users of the web are not signed on any financial agreement that limits what they can or cannot click online. If the banner is there, it is clickable."

Zer-Aviv acknowledged that such clicks could be counted as billable ads, but he suggests it's appropriate to attempt to impose costs on an advertising system that fails to respect privacy. He said, "...this is where we're deliberately trying to offset the financial incentives of the surveillance advertising model."

Zer-Aviv and his colleagues have submitted another version of AdNauseam that they hope Google will allow. "We switched the language of the start page from 'Block Malware' to 'Block Malicious Ads' which clarifies everything we do is about our privacy solution," he said. "We also have new features that we were going to launch anyway, like making exception for sites that respect the Do Not Track standard, and estimating how much money do these ad clicks end up costing, and other minor improvements."

Viva la Revolución. ®

Tips and corrections

92 Comments

**More like this**

Security Privacy Advertising Development

**Whitepaper Downloads**

How to protect your business from ransomware

Ur and Penn refuses to give malware the time of day

The business case for layered security

At PAPSTAR GmbH, malware no longer crashes the party

Why layered security is important

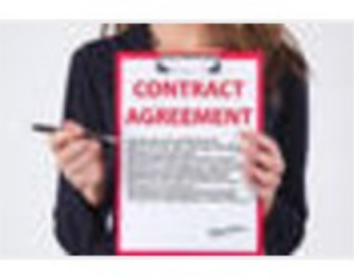
## Most read

I was authorized to trash my employer's network, sysadmin tells court

Ah, the Raspberry Pi 3. So much love. So much power ... So turn it into a Windows thin client

Cloudbleed: Big web brands leaked crypto keys, personal secrets thanks to Cloudflare bug

US judge halts mass fingerprint harvesting by cops to unlock iPhones



'First ever' SHA-1 hash collision calculated. All it took were five clever brains... and 6,610 years of processor time

**Whitepaper Downloads**

The total economic impact of Scality RING with Dell storage servers

Why layered security is important

Technology as a catalyst for cultural change

Modern backup eBook

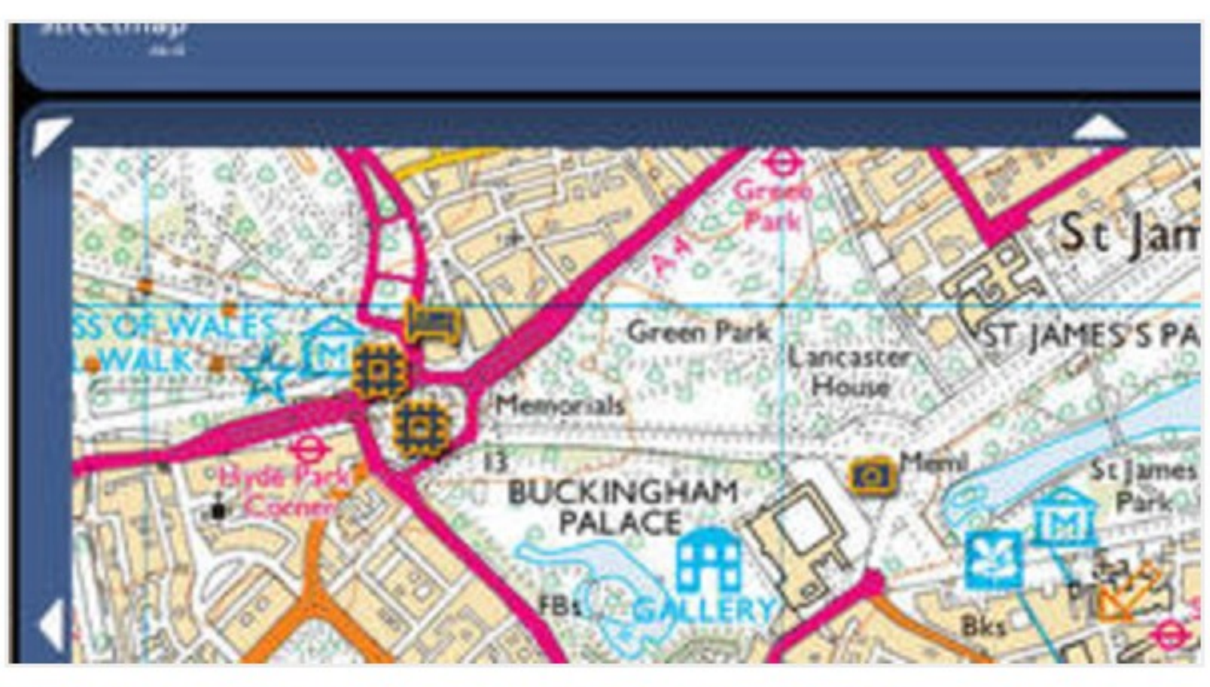
Detecting malware and viruses in a dynamic threat environment

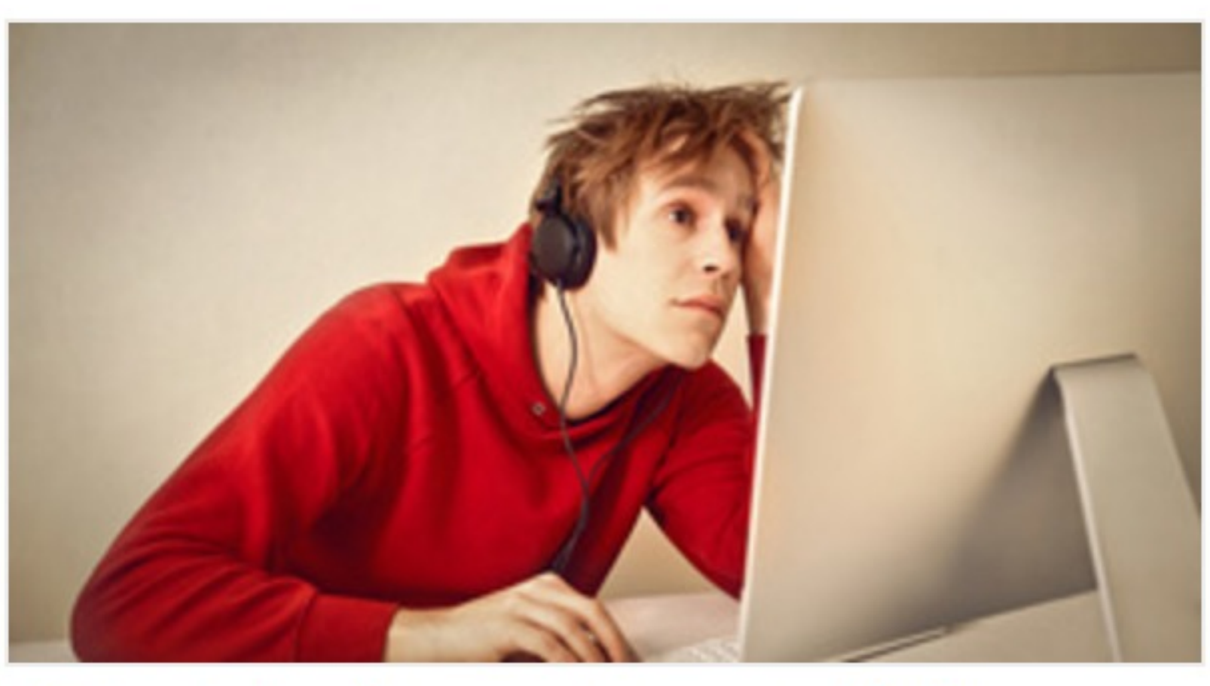
## Spotlight

**Different judge, different verdict? Diageo's £54m SAP legal slap could have gone another way**

**Clone it? Sure. Beat it? Maybe. Why not build your own AWS?**

**Meet the chap open-sourcing US govt code – Paul, an ex-Microsoft anti-piracy engineer**


**'At least I can walk away with my dignity' – Streetmap founder after Google lawsuit loss**


**Dirty data, flogged cores: YES, Microsoft SQL Server R Services has its positives**