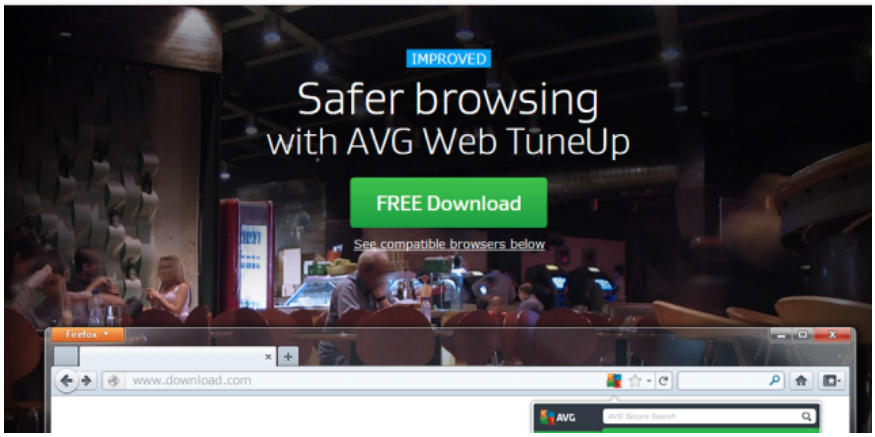
RISK ASSESSMENT / SECURITY & HACKTIVISM

Google slams AVG for exposing Chrome user data with “security” plugin

AVG AntiVirus "force-installed" Chrome plugin that left browsing data vulnerable.

by **Sean Gallagher** - Dec 30, 2015 8:27am PST

121



Safer browsing... except someone can watch everything you search?

A free plugin installed by AVG AntiVirus bypassed the security of Google's Chrome browser, potentially exposing the browsing histories and other personal data of customers to the Internet. The vulnerability, demonstrated in an exploit by a Google researcher earlier this year, has now been patched after initial stumbling attempts by AVG, according to a discussion of the bug in Google's security research discussion list.

AVG's "Web TuneUp" tool is a free download from the Chrome Store intended to provide reputation-based protection against malicious websites, and it was "force-installed" by AVG AntiVirus. The install, an "in-line" installation, happened only with user permission, but was performed in a way that broke the security checks Chrome uses to test for malicious plugins and malware.

The plugin works by sending the Web addresses of sites visited by the user to AVG's servers to check them against a database of known malicious sites. But the way the plugin was constructed meant that information could be easily exploited by an attacker through cross-site scripting [XSS], according to a post by Google Security researcher Tavis Ormandy on December 15.

"This extension adds numerous JavaScript API's to Chrome, apparently so that they can hijack search settings and the new tab page," Ormandy wrote. "The installation process is quite complicated so that they can bypass the chrome malware checks, which specifically tries to stop abuse of the extension API. Anyway, many of the API's are broken."

Ormandy attached a proof-of-concept exploit that stole the authentication cookies from AVG's website, which "also exposes browsing history and other personal data to the internet." Ormandy added, "I wouldn't be surprised if it's possible to turn this into arbitrary code execution."

Ormandy then sent what he described as an "angry e-mail" to AVG about the bugs. "Apologies for my harsh tone, but I'm really not thrilled about this trash being installed for Chrome users," he wrote to AVG. "The extension is so badly broken that I'm not sure whether I should be reporting it to you as a vulnerability, or asking the extension abuse team to investigate if it's a PuP [Potentially unwanted Program]. Nevertheless, my concern is that your security software is disabling web security for 9 million Chrome users, apparently so that you can hijack search settings and the new tab page."

LATEST FEATURE STORY

FEATURE STORY (2 PAGES)

Space for Europe and for all humankind: A brief history of the ESA

From ESRO to Rosetta, the unheralded organization's contributions go far beyond Europe.

WATCH ARS VIDEO

Ars visits Nest Labs

We learn about their programmable, self-learning, sensor-driven, Wi-Fi-enabled thermostats.

STAY IN THE KNOW WITH

LATEST NEWS

RIP JAR JAR

George Lucas criticizes “retro” feel of new *Star Wars*, describes “breakup”

REACH OUT AND TOUCH FAITH

Oculus announces “Touch” VR controller delay to second half of 2016

Gene editing tech named *Science* magazine’s Breakthrough of the Year

In 2015, promising

hosts that contained the string "avg.com" in their name. Malicious websites that used avg.com in their names (such as the example provided on Ormandy's response, https://www.avg.com.www.attacker.com) could still spoof the AVG servers, and attackers could still use a man-in-the-middle attack to pass malicious JavaScript back to a victim—regardless of whether the connection was secure or not. And, as Ormandy noted, "Any XSS on avg.com can be used to compromise Chrome users"—a quick search of AVG's sites found plenty of opportunity for such attacks.

As of December 28, AVG had completed a more secure patch, but installations of the plugin were still frozen while Google's Chrome Web Store team investigated possible policy violations by AVG—violations that could get AVG kicked off the Chrome Store completely.

Update: A Google spokesperson contacted Ars to clarify the nature of the freeze on AVG's plugin. The block on AVG's usage of inline installation has no effect on the extension update process, so users with the AVG extension installed should have automatically received the updated version, as with any routine update.

An AVG spokesperson sent a statement to Ars, claiming that the Web TuneUp Chrome extension is "offered as an option, not forcibly or automatically installed. Installation only begins once the customer has initiated the process and confirmed acceptance in Chrome—a double opt-in." The spokesperson added, "There is no auto-installation of Google Chrome extensions; the “inline” option allows third parties to offer installation from their own site or product, rather than requiring customers to visit the Chrome Store. We fixed the reported vulnerability just prior to the holidays and do not expect Google to confirm the availability of inline installation until early next year. In the meantime, anyone wishing to install the extension may easily do so from the Chrome Store.”

READER COMMENTS 121

Sean Gallagher / Sean is Ars Technica's IT Editor. A former Navy officer, systems administrator, and network systems integrator with 20 years of IT journalism experience, he lives and works in Baltimore, Maryland.
@thepacketrat on Twitter

← OLDER STORY NEWER STORY →

YOU MAY ALSO LIKE

Ars’ favorite science images of 2015

Ian Murdock, father of Debian, dead at 42

About Us
Advertise with us
Contact Us
Reprints

SUBSCRIPTIONS

Subscribe to Ars

RSS Feeds
Newsletters

Visit Ars Technica UK

Reddit
Wired
Vanity Fair
Style
Details

Visit our sister sites
Subscribe to a magazine

VIEW MOBILE SITE

CONDÉ NAST