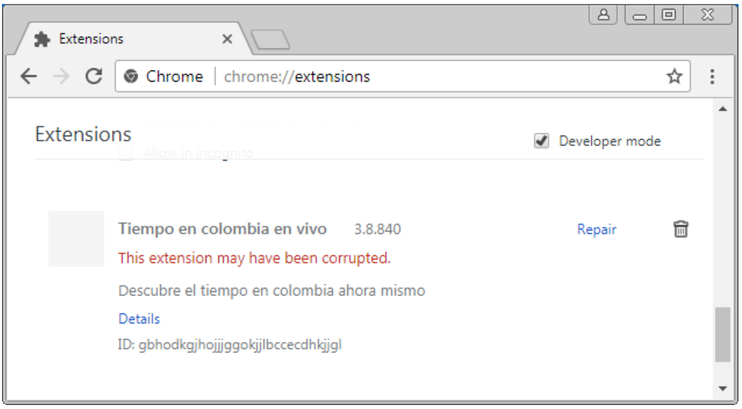
BIZ & IT TECH SCIENCE POLICY
CARS GAMING & CULTURE FORUMS
STORE SIGN IN

BIZ & IT —

Malicious Chrome extension is next to impossible to manually remove

Extensions remain the Achilles heel for an otherwise highly secure browser.

DAN GOODIN - 1/19/2018, 10:36 AM



Tiempo en colombia en vivo 3.8.840

This extension may have been corrupted.

Descubre el tiempo en colombia ahora mismo

ID: gbhodkgjhojjjggokjjlbccecdhkjjgl

Malwarebytes

121

Proving once again that Google Chrome extensions are the Achilles heel of what's arguably the Internet's most secure browser, a researcher has documented a malicious add-on that tricks users into installing it and then, he said, is nearly impossible for most to manually uninstall. It was available for download on Google servers until Wednesday, 19 days after it was privately reported to Google security officials, a researcher said.

Once installed, an app called "Tiempo en colombia en vivo" prevents users from accessing the list of installed Chrome extensions by redirecting requests to chrome://apps/?r=extensions instead of chrome://extensions/, the page that lists all installed extensions and provides an interface for temporarily disabling or uninstalling them. Malwarebytes researcher Pieter Arntz said he experimented with a variety of hacks—including disabling JavaScript in the browser, starting Chrome with all extensions disabled, and renaming the folder where extensions are stored—none of them worked. Removing the extension proved so difficult that he ultimately advised users to run the free version of Malwarebytes and let it automatically remove the add-on.

When Arntz installed the extension on a test machine, Chrome spontaneously clicked on dozens of YouTube videos, an indication that inflating the number of views was among the things it did. The researcher hasn't ruled out the possibility that the add-on did more malicious things because the amount of obfuscated JavaScript it contained made a comprehensive analysis too time consuming. The researcher provided additional details in a blog post published Thursday.

Tiempo en colombia en vivo racked up almost 11,000 installs before Google removed it, but it may have found its way onto still more computers. That's because a variety of abusive websites are using a technique that tricks inexperienced users into installing the extension. As Malwarebytes explained in late 2016, the forced install trick uses JavaScript to provide a dialog box that says visitors must install the extension before they can leave the page. Clicking cancel or closing the tab produces an unending series of variations on that message. Arntz said he privately reported the extension to Google on December 29 and that it remained available on the Chrome Store until Wednesday.

Arntz said he found a Firefox extension that also resisted user attempts to uninstall it, but the block was relatively easy to bypass. The researcher has yet to find any indication the add-on was available in the Firefox Extensions store.

FURTHER READING
Google Chrome extensions with 500,000 downloads found to be malicious

Malwarebytes' finding comes a few days after a separate security firm uncovered four malicious extensions with more than 500,000 combined downloads from the Google Chrome Web Store. The extensions found by ICEBRG were used in a click fraud scheme, but company researchers said the add-ons just as easily could have been used to do more nefarious things. Google removed the extensions after ICEBRG privately reported them.

On Thursday, Ars e-mailed Google officials with the following questions:

- Is all of this information [from Malwarebytes] correct?
- If it is, why did it take Google 19 days to remove the extension from the Chrome Store?
- The researcher was able to determine the extension inflated the number of

views of various YouTube videos, but he said the sheer amount of JavaScript contained in the extension prevented him from determining if the extension spied on users or performed other malicious actions. Has Google had a chance to analyze the extension to see exactly what it did to computers it was installed on?
- Is Google notifying users who installed the extension or providing assistance in uninstalling it?
- Do Google developers have plans to redesign Chrome to make it easier to remove malicious or abusive extensions?
- What is Google doing to prevent malicious or abusive extensions from winding up in the Chrome Store?

A few hours after this post went live on Friday, a Google spokeswoman responded with the following statement: "We've automatically removed Tiempo en colombia en vivo and Play Red Bull version 4 from the machines of affected Chrome users. Security is a core tenet of Chrome and the browser automatically blocks over one thousand malicious or abusive extensions per month."

On background, the company representative said that the difficulty in manually removing the extension was at least in part the result of its logo being a square with the exact same color as the Chrome toolbar. The identical color prevented users from seeing the Chrome omnibox, from which extensions can be removed. The spokeswoman didn't address the other questions, either on background or on the record. Company officials almost exclusively communicate with reporters on background, a condition that prevents officials from being named or quoted.

But wait ... there's more

A half hour before this post was to go live, James Oppenheim, an editor of a review site for children's games, emailed to report yet another malicious extension that remained in the Chrome Store, despite his attempts to get it removed. Oppenheim's e-mail, which Ars got permission to publish, reads:

> I'm writing to you with a

follow up to your piece about chrome extensions. I cover family technology for my site JamesGames.com. I appear frequently on SiriusXM and have been a Today Show contributor since the '90s.

Eleven days ago I received an offer to buy my extension, Play Red Ball version 4 from a fellow in India named "Ganesh". Since I haven't ever written an extension, I thought this was just a spam mailing gone wrong. I didn't respond.

However, by the third email Ganesh had an insistent tone. It seemed human-generated.

So, I decided to google the extension he thought I had written. Turns out it is a Chrome extension, a game. Interestingly, it is named similarly to a lot of children's software (the beat I cover). When I clicked on the extension page it shows my site as the official site of the app, and it lists the developer as "James Extensions!" (sic), again with a link to my site.

Though it has a four out of five rating, there are many comments that the program is malware.

It appears that whoever published it knows enough about what I do reviewing kid's software to think that my name would help make the malware more trustworthy.

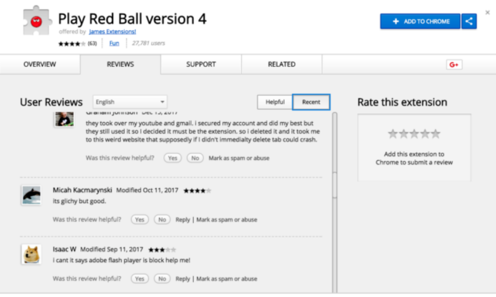
I posted a comment on the extension page and also wrote to Google via the reporting button on the page asking them to take down the app, or at the least, take my site off of it. It's been a week and I have had no response. I just checked today and it is still there.

The presumably malicious app has 27,781 users according to the extension's page. Makes me wonder how seriously Google is taking this problem.

I can't seem to get through to anyone at

> Google, saw that you're covering this area. Perhaps you can help and get a story out of it at the same time.
>
> I haven't responded to Ganesh. I have wondered if when I do if the offer to buy is legit or is just a way to get me to check out the app's page, see that they are using my name, and then offer to remove it if I pay them. Could be paranoia on my part, but the whole thing is just bizarre. I'm pasting in his email below my signature.

Here's a sampling of recent comments left by people who downloaded the game from the Chrome store:



Graham Johnson Dec 13, 2017
they took over my youtube and gmail. i secured my account and did my best but they still used it so I decided it must be the extension. so i deleted it and it took me to this weird website that supposedly if i didn't immedialty delete tab could crash.
Was this review helpful? Yes No Mark as spam or abuse

Micah Kacmarynski Modified Oct 11, 2017 ★★★★☆
its glichy but good.
Was this review helpful? Yes No Reply | Mark as spam or abuse

Isaac W Modified Sep 11, 2017 ★★★☆☆
i cant it says adobe flash player is block help me!
Was this review helpful? Yes No Reply | Mark as spam or abuse

Enlarge

In Google's defense, Chrome is by most accounts the Internet's most widely used browser,

FURTHER READING

After phishing attacks, Chrome extensions push adware to millions

making it also the one most tempting to target. What's more, the number of people who wind up installing a malicious Chrome add-on is a small sliver of the overall user base.

Still, the message is clear. Chrome may have an industry-leading security sandbox and the quickest security updates among any of the major browsers, but the extensions remain a key weakness. Users, particularly those with less technical expertise or who are especially large targets, should avoid installing extensions unless they provide a true benefit and then only after carefully researching the developer and the title.

Post updated to add comment from Google.

Promoted Comments

Urist / Wise, Aged Ars Veteran

JUMP TO POST

Youtube, Android App Store, Chrome Extensions. Google has a very lethargic attitude when it comes to vetting 3rd party content on their platforms. Likely nothing will be done until a critical mass of users are affected and it starts affecting profits. As far as chrome is concerned I am not sure there is any direct-profit feedback as there exists with Youtube and the threat of advertisers pulling out, so I don't expect them to make any changes to the process unless they lose a significant portion of the browser market share. It is really concerning that one of the foremost technology companies is not more proactive in protecting their customers (although I suppose end users are not really their customers but rather the raw data resource to sell to their actual customers the advertiser networks).

124 posts | registered 9/12/2017

Ysleiro / Smack-Fu Master, in training

JUMP TO POST

Ars might want to dig into

what I've just experienced. Quick note back in August this (https://arstechnica.com/information-tec ... -millions/) happened and I was affected. I suspect this may have something to do with my story.

I just experienced the same thing this past Monday. I started noticing Chrome would crash on certain sites after initial render (the crashing was relentless).

At first I just thought I needed to re-install Chrome. I then got rid of all my extensions and 2 extensions kept re-installing themselves.

Side note: I'm a web developer.

The extensions that kept re-installing themselves are Tampermonkey and Acescript.

I did have a program installed that I suspect was installing Acescript because acescript stopped re-installing itself after I uninstalled it. I was only able to get Tampermonkey to stop re-installing itself after wiping my machine however the crashing did not relent. I wiped my machine via Window 10's built in system refresh capabilities (soft reset, c:/ wipe and c:/ overwrite with 1s and 0s). None stopped the problem.

At that moment I deduced that whatever it was had also piggy backed into Window's system installation files (hence why it could survive system wipes). So I grabbed Ubuntu on a USB and overwrote the entire drive Windows files and all.

Problem solved.

PS. I don't know when I was exposed or what extension it was. I'm not sure if Ace Script and Tampermonkey were the culprits, I never really found the culprit I was just interested in wiping it out.

51 posts | registered 7/18/2013

DAN GOODIN

Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001

READER COMMENTS 121 SHARE THIS STORY

← PREVIOUS STORY NEXT STORY →

Related Stories

Today on Ars

RSS FEEDS
VIEW MOBILE SITE
ABOUT US
CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS