RISK ASSESSMENT / SECURITY & HACKTIVISM

# My browser visited Weather.com and all I got was this lousy malware (Updated)

New rash of malvertising attacks threatens millions of Web surfers.

by **Dan Goodin** - Aug 14, 2015 11:42am PDT

218

Millions of people visiting weather.com, drudgereport.com, wunderground.com, and other popular websites were exposed to attacks that can surreptitiously hijack their computers, thanks to maliciously manipulated ads that exploit vulnerabilities in Adobe Flash and other browsing software, researchers said.

The malvertising campaign worked by inserting malicious code into ads distributed by AdSpirit.de, a network that delivers ads to Drudge, Wunderground, and other third-party websites, according to a post published Thursday by researchers from security firm Malwarebytes. The ads, in turn, exploited security vulnerabilities in widely used browsers and browser plugins that install malware on end-user computers. The criminals behind the campaign previously carried out a similar attack on Yahoo's ad network, exposing millions more people to the same drive-by attacks.

**Update:** A few hours after Ars published this article, Malwarebytes updated the blog post to say the campaign had moved to yet another ad network, which happens to be associated with AOL. Visitors to eBay were among those who were exposed to the malicious ads distributed through the newly discovered network.

Malvertising is a particularly pernicious form of attack because it can infect people who do nothing more than browse to a mainstream site. Depending on the exploit, it can silently hijack computers even when visitors don't click on links. Some browser makers have responded by implementing so-called click-to-play mechanisms that don't render Flash or Java content unless the end user actively permits the plugin to run on a particular site. Some users have resorted to ad blockers, which have the unfortunate side effect of depriving publishers of much-needed advertising revenue.

The campaign used against the AdSpirit and Yahoo networks connected to servers run by Microsoft's Azure service. Ultimately, the booby-trapped ads led to attack code distributed through the Angler exploit kit, a software package sold on the black market that makes it easy for criminals to exploit vulnerabilities in Flash, Java, and other software. The AdSpirit attacks were particularly hard to trace because most of the websites involved in the attack were using the transport layer security protocol to obscure the address and encrypt the data. There's no indication the attacks were exploiting vulnerabilities in fully patched software. That underscores the importance of installing security updates as soon as they become available.

*Update:Weather.com added to headline and first paragraph to reflect new information provided by Malwarebytes.*

*Listing image by* Malwarebytes

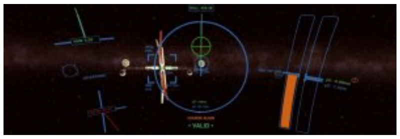
## PROMOTED COMMENTS

**Dilbert** | Ars Legatus Legionis    jump to post

No place is safe anymore. Just last week our chief financial officer got an ad-injected malware from Costco.com. No she did not misspell the URL. I looked in her browser history and it was correct. Luckily she went right over the helpdesk and called us engineers directly immediately so there was no real damage.

I refreshed the costco.com a few times. First few times there were no 3rd party ads. Then a 3rd party

## LATEST FEATURE STORY



FEATURE STORY (3 PAGES)

### *Rogue System* is a button-studded, checklist-filled space survival sim

Complex procedure-filled game aims for realism—or at least "realism"—in zero-G.

## WATCH ARS VIDEO

### Samsung Unpacked 2015

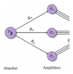
Ars looks at the Samsung Galaxy 6 Edge+ and the Note 5.

## STAY IN THE KNOW WITH

## LATEST NEWS

\M/ \M/ \M/

### Watchdog group says Soylent's cadmium and lead levels violate CA law



### How BitTorrent could let lone DDoS attackers bring down big sites

### The new, underground sport of first-person drone racing

BULK MONITORING

Amex ad appeared a few times. Then finally bam Joe's Plumbing supplies or something like that. I forgot which ad service they were using.

20860 posts | registered Mar 15, 2002

**Coriolanus** | **Wise, Aged Ars Veteran** **jump to post**

This was an interesting article about ad-injected malware until it became some sort of political holy war in the comments about topics not even in the same galaxy as the story.

893 posts | registered Aug 15, 2014

**taswyn** | **Ars Tribunus Militum** **jump to post**

The ultimate irony of this comments thread is that the people *complaining* about politics getting dragged in are almost universally the ones dragging it in.

There's nothing in the article that's overtly political. What's *fascinating* is just how much some people are reading into it, and then choosing to go down one of those two rabbit holes in response.

> flunk wrote:
> Just disable or uninstall Flash. It's nothing but a liability now.

Pretty much this. If you absolutely need flash for **specific** sites, there are ways to do that. In Chrome, it's "Let me choose when to run plugin content" which nicely disables not only flash, but also Java (if installed as a browser plugin) and even Chrome's pdf viewer. It's right click to run via context menu, so it's safe against click jacking (as far as anyone knows, for now). It's friendlier to legitimate sites in terms of advertising, as most still serve alternate ads if they detect flash not running.

Honestly, I've never been hit with malware from a purely javascript vector. It's always been some form of plugin like flash. It's not that 0 day javascript exploits that breach the sandbox don't ever happen, it's just that they're relatively more rare and quickly patched.

2059 posts | registered Jun 22, 2010

**DerHabbo** | **Ars Scholae Palatinae** **jump to post**

> Power_Struggle wrote:
> > **Quote:**
> > Some users have resorted to ad blockers, which have the unfortunate side effect of depriving publishers of much-needed advertising revenue.
>
> Two days since I read, on this very site, about Comcast paying 200M for a part of Vox.
> Much-needed advertising. So needed that the publishers cannot afford any due diligence on ads..

Most people don't use ad blockers. It really hurts the small fries more than the Matt Drudges of the world. Think Brian Krebs, that guy can't catch a break cause most of his readership is savvy to the issues with ad networks.

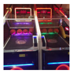
869 posts | registered Feb 14, 2011

**READER COMMENTS 218**

- - - -

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.
**@dangoodin001 on Twitter**

**AT&T's "Extreme Willingness to Help" is key to NSA Internet surveillance**



**Gallery: Japan's gaming centers provide joy for the kid inside**

**Parrot drones easily taken down or hijacked, researchers demonstrate**

← OLDER STORY NEWER STORY →

## YOU MAY ALSO LIKE

## SITE LINKS

About Us
Advertise with us
Contact Us
Reprints

## SUBSCRIPTIONS

Subscribe to Ars

## MORE READING

RSS Feeds
Newsletters

Visit Ars Technica UK

## CONDE NAST SITES

Reddit
Wired
Vanity Fair
Style
Details

Visit our sister sites
Subscribe to a magazine

VIEW MOBILE SITE

CONDÉ NAST