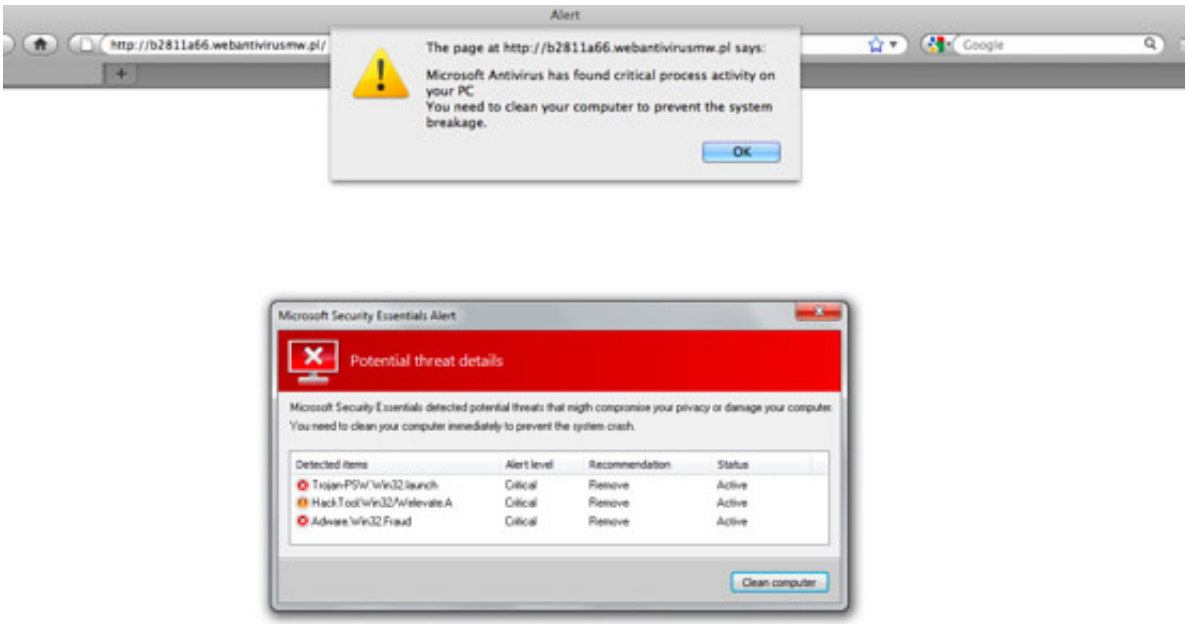
TECHNOLOGY

Newest Hacker Target: Ads

Weak Spot in Internet Security Is Network of Makers, Sellers of Advertisements

By DANNY YADRON

Jan. 31, 2014 7:28 p.m. ET



An advertisement that contained malicious computer code. *RiskIQ Inc.*

Hackers increasingly are exploiting a little-discussed weak spot in Internet security: The byzantine network of ad makers and sellers that target online ads based on users' browsing habits.

The trend was reinforced recently when Yahoo Inc. displayed an advertisement laced with malicious computer code to European users for a week. Other major websites have run malicious ads in recent months, including those of newspapers, blogs and Dailymotion, a popular destination for streaming video.

More

Target Hackers Used Stolen Vendor Credentials

Version of Target Malware Linked to Young Russian

In some cases, the fake ads can download viruses without a user even clicking on them. In other instances, the ads serve up a legitimate-looking alert — "Your computer's antivirus is out of date!"—to trick people into paying fraudsters money or downloading

Card-Theft Software Grew in Internet's Dark Alleys

a virus. The spots sometimes are served unknowingly by major ad networks and can slip by antivirus software.

The Internet advertising ecosystem is part of the problem. Ads may pass through dozens of virtual hands to match buyers with sellers in quick online auctions. The process is so fast, and there are so many players, that it can be difficult to screen every ad, according to security researchers and people in the advertising industry.

Hackers tend to move in packs, swarming to exploit a security hole until it is fixed, said an official at Rubicon Project Inc., which automates the buying and selling of ads. Hackers now appear to be swarming on Web ads.

In 2013, the cybersecurity company RiskIQ Inc. tracked nearly 384,000 malicious ads online. That's up from 205,000 the year before and 70,000 in 2011. People close to large ad companies acknowledge the number of bad ads has increased, but say that's partly because more people are online. These people also say ad companies are blocking more as well.

Google Inc., which has one of the largest ad networks online, said it disabled ads from more than 400,000 sites hiding malware in 2013, up from 123,000 in 2012.

The issue is sowing distrust between publishers and advertising companies. In December, the website for South African newspaper Mail & Guardian started fielding complaints from readers that its website was trying to deliver malicious software. A pop-up urged users to "clean your computer to prevent system breakage." If users clicked "OK," they downloaded a virus that 44 of 47 antivirus programs missed, according to an independent test in January by VirusTotal, a Google unit that tests antivirus software.

M&G Media Ltd., the paper's owner, eventually traced the problem to an ad from a new advertiser. The Mail & Guardian accepted the ad from AdDalan LLC, a company with no listed physical address. AdDalan didn't return a request for comment.

"If they don't tighten stuff up, they're going to kill the goose that lays the golden egg," Alistair Fairweather, the paper's chief technology officer, said of third-party ad networks.

One common path could work like this: An ad agency makes a Web spot, which then moves through trading desks and exchanges run by companies such as Google's Doubleclick unit. It is then moved onto one of dozens of ad networks, some of which are run by Yahoo, Google, Amazon.com Inc. or AOL. Publishers use their own technology vendors to manage which ads wind up on their sites.

Late last year, a malicious ad that appeared next to a streaming video of British television show "Doctor Who" on UKTV's website passed through 17 Web addresses before it moved through the Rubicon Project, according to researchers at RiskIQ.

Behind Facebook's Efforts to Charm Advertisers

How Lenovo Built a Chinese Tech Giant

Payment Wars: Amazon Jumps In

Why Is It Hard to Memorialize Loved Ones' Lives Online?

G Flex Review: Calling on a Curved Phone

A UKTV spokesman said the British TV channel was investigating the matter and that it serves ads through third parties. A Rubicon official said the company automatically scans for malware but malicious ads sometimes slip through.

Advertisers have known about the potential problems of malware for years, but have struggled to eliminate them. Scanning the software behind a Web ad for bugs is time-consuming, expensive and increasingly difficult as more ads include interactive graphics and complex pieces of code used to target specific types of users, industry executives say.

"There is an arms race," said Chris Olson, chief executive of Media Trust, an ad-security company in McLean, Va.

In the Yahoo case, the malicious ad was distributed between Dec. 27 and Jan. 3 before the company caught it. It's impossible to know how many people were affected because the virus only deployed in certain circumstances, according to people familiar with the investigation.

For instance, the ad tried to find a specific unpatched security hole in Java, a programming language meant to make the Web more interactive. It also appears to only have affected Windows-based machines, not Macs. If it located an opening, the bad ad infected a user's machine with a host of computer viruses. One of them, called Zeus, is often used to steal online banking credentials, according to several security researchers who studied the incident.

Weeks later, Yahoo still is investigating the matter with law enforcement.

According to Yahoo, the hacker was able to compromise the account of a legitimate advertiser and submit the ad into its network.

Write to Danny Yadron at danny.yadron@wsj.com