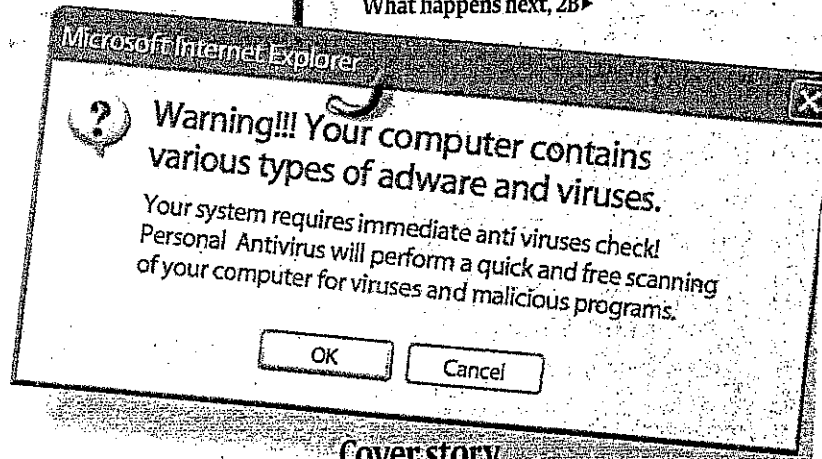




How scareware trickery ensnares Internet users

- 1 Criminals buy blocks of ad space on websites, intermittently slipping in a tainted ad.
- 2 Just visiting a webpage with a tainted ad causes a fake warning box to appear.
- 3 Clicking "OK" or "Cancel" launches the same thing: a "free scan."

What happens next, 2B▶

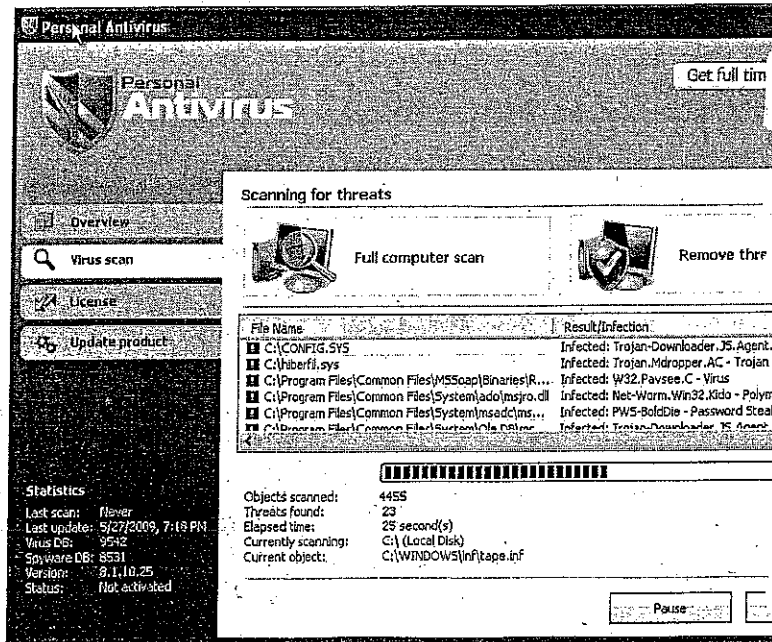


Cover story

Don't get hooked by fishy scare tactics

Pitches for fake security show up in surprising places

Once false click and you're stuck in a scareware loop



Scans uncover non-existent viruses

After you've been lured into a fake "free" scan of your PC:

- 4 The bogus scan will purport to find a virus infestation.
- 5 Ensuing boxes steer the user to activate "Personal Antivirus," on left.
- 6 The activation prompts take the user to a shopping cart.
- 7 Declining to place an order triggers endless fake scans.

Sources: Purewire, AVG, USA TODAY research



Scareware's pitches for fake security show up in odd places

By Byron Acohido, USA TODAY

Scareware has become the scourge of the Internet.

Those deceptive promotions crafted to panic you into spending \$30 to \$80 for worthless antivirus protection can hit you just about anywhere you turn on the Web. They arrive as booby-trapped Web links in e-mail and social network messages. They lurk hidden, and set to activate, when you click to popular, legitimate websites.

BLOG: Twitter used to spread scareware

And now scareware purveyors are embedding triggers in places you wouldn't expect: on advertisements displayed at mainstream media websites; amid search results from Google, Yahoo Search and Windows Live search; alongside comments posted on YouTube videos; and, most recently, in "tweets" circulating on Twitter.

"Scareware is becoming a dominating force," says Joe Stewart, director of SecureWorks Counter Threat Unit. "There are hundreds of criminals using every tactic they can think of to push these programs."

Click on a trigger and you'll get caught in an unnerving loop impossible to abort. A scanner window will appear with red-letter warnings listing viruses purportedly infesting your hard drive. A series of dialogue boxes will follow giving you choices that all lead to the same screen: a sales pitch.

Make the purchase, and you get a bogus inoculation. Try to cancel it, and you'll get repeated offers. "It's like stepping into quicksand," says Paul Royal senior researcher at security firm Purewire. "The more you try to get out of it, the deeper you sink."

Scareware has been a prominent part of the Internet since 2004, when a cybergang based in St. Petersburg, Russia, launched the iframecash.biz website and began offering commissions to anyone who helped them spread the SpySheriff fake antivirus program. Hackers began to taint legitimate websites so that pop-up ads for SpySheriff would launch on the PC of anyone who visited a corrupted Web page.

That simple arrangement has evolved into a steadily growing industry that marked a banner year in 2008. By late last year, more than 9,200 different types of scareware programs were circulating on the Internet, up from 2,800 at midyear, according to The Anti-Phishing Working Group. Microsoft recently reported that scareware infections rose 48% in the second half of 2008 vs. the first half. Microsoft analyzed data collected by use of its Malicious Software Removal Tool and found one specific fake security program on 4.4 million PCs.

"These guys are very innovative," says Roel Schouwenberg, senior virus researcher at Kaspersky Lab. "They're constantly looking for newer and easier ways to make money."

Cutting-edge scareware marketing campaigns are being delivered via:

- **YouTube and Twitter.** The bad guys sign up for a handful of new YouTube or Twitter accounts. In the case of YouTube, crooks recently used about a dozen new accounts to begin posting comments on 30,000 videos, says Luis Corrons, technical director of PandaLabs. The comments enticed users to click on a link that triggered a scareware promotion.

In a variation of this ploy, crooks in late May created new Twitter accounts and began broadcasting tweets declaring "Best video" with a Web link of <http://juste.ru>, says Schouwenberg. Clicking on the link launched a sequence that replicated the message to everyone on the victim's friends list, then launched a scareware promo.

•**Search results.** The bad guys create malicious Web pages and fill them with words and phrases that are likely to be popular search queries, such as "American Idol winner" or "NCAA tournament bracket," says Yuval Ben-Itzhak, CTO of security firm Finjan. Next they insert tiny copies of their bad links on popular, legit websites that don't do a thorough job of preventing such hacks.

"Search engine optimization" then takes over. SEO is the technology that determines the relevance of Web links to search queries. By embedding a malicious link on a popular website, the hackers imbue their Web page with high relevance. So when the legit site turns up as the No. 1 or No. 2 result for a popular search query, their bad link turns up as the No. 4 or No. 6 result. Anyone who clicks on the bad link gets a scareware pitch.

•**Online ads.** The bad guys purchase blocks of ad space on popular websites through a legit ad agency, says Roger Thompson, senior researcher at AVG. Next they instruct the ad agency to begin posting innocuous ads. To avoid detection, they only sporadically feed a corrupted ad into the mix. The bad ad looks safe, but carries instructions to route anyone who clicks to a scareware pitch. "It's the most common attack we see every day," Thompson says.

Mind-boggling profits

Powerful incentives undergird scareware. Security researchers say the industry is run by no more than a dozen or so top-level suppliers orchestrating the activity of several hundred "affiliate" distributors.

The top-level groups supply bogus scanners and cleanup tools — actual software — and collect payments and pay commissions. Bonuses can be generous. One top supplier, for instance, recently ran a contest offering a \$36,000 Lexus sedan to the top-selling affiliate, says F-Secure senior researcher Mikko Hypponen.

"The top-level groups incentivize the affiliates and don't get their hands dirty," says Hypponen. "If they get any complaints, they can just blame the affiliate."

Top-level groups typically work with 100 or more affiliates, who can earn commissions many different ways. Last fall, SecureWorks researcher Stewart infiltrated a Russian group known as the Baka Software gang. He accessed documentation showing one affiliate earned \$146,525 in 10 days by spreading promotions for a worthless program, called Antivirus XP 2008, to more than 154,000 people, and closing sales to 2,772 of them. Another record showed five top Baka Software affiliates earning weekly commissions averaging \$107,604.

"The sheer amounts of money involved in installing just one rogue program are mind-boggling," Stewart says.

A few scareware affiliates have been slowed by regulators. Last fall, Microsoft and Washington state Attorney General Rob McKenna filed civil lawsuits against Branch Software, of The Woodlands, Texas, and Alpha Red, of Houston, charging that they were marketing scareware. And last December, the Federal Trade Commission obtained court orders prohibiting Innovative Marketing, of Belize, and ByteHosting Internet Services, of Cincinnati, from selling WinFixer, WinAntivirus, DriveCleaner, ErrorSafe, and XP Antivirus, all worthless.

The top-level suppliers, however, continue to operate with impunity, mainly based in Russia. And new affiliates crop up every day, full of fresh ideas to spread increasingly invasive promotions, security researchers say.

Consumer trust at risk

In the past two months, AVG's free LinkScanner tool, which prevents users from clicking on malicious Web links, has been flushing out — on a daily basis — more than 30,000 Web pages displaying ordinary-looking ads embedded with hidden scareware triggers. Earlier this year the daily average was roughly 5,000, Thompson says.

The tech giants supplying the infrastructure for Web commerce, and media and social-networking companies capitalizing on Web marketing, are cognizant of the threat posed by escalating scareware, says Mike Zaneis, vice president of public policy

for the Interactive Advertising Bureau, a trade association, whose members include Google, Yahoo, Microsoft, Facebook, NBC, USA TODAY and The New York Times.

"The industry is very committed to combating these attacks, because consumer trust is vital for us to do business," Zaneis says. "It's what keeps people online."

Yet affiliates continue to demonstrate remarkable ingenuity. Contaminating search results is a complex endeavor. The affiliate group infiltrated by Finjan demonstrated how SEO hacks can result in a high-volume of promotions launched. Over a 16-day period, the group corrupted some 500,000 legitimate Web pages, and got nearly 2 million people to click on tainted search results. "These cybercriminals are motivated by the huge amount of money they can make very quickly," says Ben-Itzhak.

Google spokesman Andrew Kovacs says the search giant works hard to preserve the integrity of search results. "We make constant improvements to our systems," Kovacs says. "This issue is not specific to one company, and we encourage people to be vigilant about checking the URLs (Web links) of the websites they visit."

That's good advice, since scareware purveyors have shown they will strike wherever consumers congregate in large numbers. Take the affiliates who spread booby-trapped Web links via Twitter in late May. Kaspersky researcher Schouwenberg says anyone who clicked on one of their tweeted links got hit with a particularly nasty program. It shut down — and locked out — all other software applications, and insisted on purchase of a two-year license, for \$49.95, to unlock the other apps. A lifetime license cost \$79.95. "They're beginning to cripple machines to make it more likely that you will pay up," he says.

Pressure for change is growing

As scareware continues to escalate, public pressure for relief from deceptive promotions will increase, predicts John Pironti, a member of the education committee of the Information Systems Audit and Control Association, a global organization of auditors and security pros.

Pironti, president of IP Architects, a risk-management consultancy, would like to see more public-awareness campaigns and tighter controls to curtail scareware.

"Commercial industry has pushed us to use the Internet more, and interact in person with them less," he says. "So now they need to take on a bigger responsibility for making things safer."

Find this article at:

http://www.usatoday.com/tech/news/2009-06-09-cybergangs-scware-hackers_N.htm?loc=interstitialskip