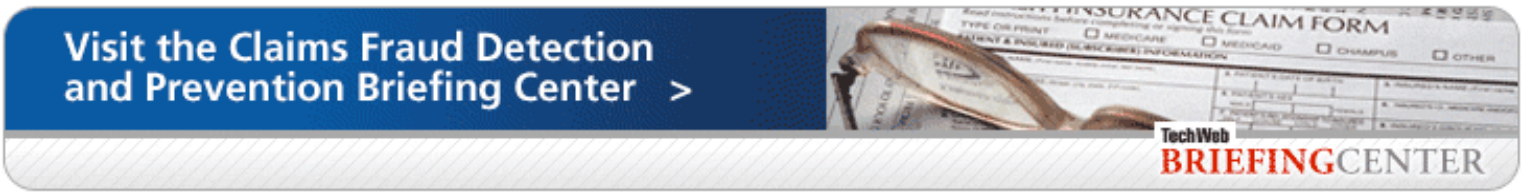

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Criminals Using Botnet To Attack iPhone Buyers

About 7,500 zombie computers are getting an additional piece of malware -- a Trojan that redirects iPhone shoppers to phony and malicious Web pages.

By Sharon Gaudin, InformationWeek
July 16, 2007
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=201001607

Looking to buy an iPhone?

Beware that the Web site you think you're visiting actually may be a phony site set up to empty your bank account instead of sell you a new iPhone.

That's the warning that comes from researchers at PandaLabs. Botnet herders are downloading a new Trojan onto already infected or zombie computers. The new malware -- Aifone.A bot Trojan -- enables the botnet herder to redirect the browser to certain pages if the user tries to visit a specific URL.

Panda reported that the cybercriminals are setting up the zombie computers so that if a user tries to visit an official Apple iPhone site, or if a user visits a Web page with a link to a page dealing with the iPhone, he or she will be redirected to the false page. The Trojan also forces the zombie machines to show specific results and redirect users to the phony pages whenever the user does an Internet search for specific keywords.

Researchers also noted that pop-up and banner advertisements display iPhone ads on the infected computers, further luring users to the fraudulent sites.

If users try to buy an iPhone off the phony pages, they actually are giving their financial and personal identification information to the botnet herders.

"This is one of the most sophisticated attacks we have seen targeting a user community, in this case iPhone users," said Luis Corrons, technical director of PandaLabs, in a written statement. "It is a really complex, dangerous attack that combines elements of malware (the Trojan), phishing (the spoofed Web page), and even adware (pop-ups, modification of search results, etc.)."

The real danger, according to Panda, is that the attack easily could be modified to work with any product that users might be shopping for.

The iPhone, which was released amid great furor on June 29, combines Apple's iPod music and video player with a mobile phone and wireless Internet access for e-mail and Web surfing.