eWEEK ENTERPRISE NEWS & REVIEWS

Hackers Scam Thousands with Bogus Anti-Spyware Offers

November 9, 2007

By Brian Prince

Want some anti-spyware? How about a Trojan with that?

That is not a literal sales pitch, but the end result of a multistep scam involving rogue anti-spyware that researchers at SecureWorks are warning Web surfers about. Though tricking users into downloading Trojans via bogus anti-spyware is nothing new, security researchers said the magnitude of the scam makes it problematic.

RELATED LINKS

Scammers Exploit San Diego Fire

MP3 Spam Scam Hits In-boxes

Online Publishers Powerless Against RBN's Malicious Ads

Biggest Pump-and-Dump Scam Ever Spikes Spam 445%

"Rogue anti-spyware scams have been in circulation for several years," said Don Jackson, a security researcher at Atlanta-based SecureWorks. "However, they were typically one-off-type scams. We have never seen a malicious campaign using rogue anti-spyware of this magnitude before .... SecureWorks has personally seen 10 different content providers affected by this campaign and our outside sources tell us that they have worked with another 20 or so, but we suspect it is affecting dozens of Web sites."

According to officials at SecureWorks, the plot works this way: A victim browses a legitimate, high-traffic Web site with legitimate-looking ads often served by third-party advertising platforms like Google and Yahoo. When the victim clicks on the page or takes some other action on the page, a pop-up appears warning of a security problem on the victim's computer.

The pop-up offers fake anti-spyware for sale for amounts ranging from $19.95 to $79.95 in exchange for credit card information. Once purchased, the bogus product either downloads a rootkit or a Trojan such as Zlob that steals personal information over time. The scammers make money from both the sale of the fake product as well as the victim's credit card information and access to the Trojan or rootkit-infected computer, researchers said.

The hackers are utilizing the Russian Business Network services and other hosting services for the scam, SecureWorks officials found, and content providers the company has worked with reported that incidents of the scam shot up dramatically in October.

"There are a variety of kits for sale on the Internet [that] will allow a hacker to do a turnkey setup of a site selling anti-spyware, such as SpyShredder, which is one of about 40 different rogue anti-spyware products being used in this latest scam," Jackson said. "The hackers are setting up the fake anti-spyware Web sites and then they are buying advertising direct from the legitimate Web sites or the advertising agencies that represent these Web sites."

The hackers then inject those ads randomly with malicious code to send a pop-up alert, such as, "You have encountered a piece of spyware on your machine or you have been hacked, download SpyShredder to clean it off your machine now." The visitor does not need to click on the ad, merely visit the page hosting it and perform any action.

Since the malicious code is served up at random, an ad won't deliver the alert every time, making it difficult for Web site owners to detect which ad is bad and which is good, Jackson said.

Click here to read more about the biggest spam scam ever.

Forrester Research analyst Chenxi Wang said it is difficult generally for Web sites to scrutinize their advertisers, in part because they sometimes don't know who their advertisers are.

"[Some Web sites use] Google or Yahoo's automatic algorithms to place relevant ads, but they do not deal with the advertisers personally, so they typically would not scrutinize the advertisers," she explained. "Google and Yahoo can do some vetting to a certain extent, but there is no tool that is sophisticated enough to understand the intention/behavior of arbitrary programs. Therefore it's not possible for them to determine definitively whether some ads have malware behind [them] or not."

Adding that any Web site that runs ads is at risk for this scam, SecureWorks officials recommended that Web sites, ad companies and ad aggregators protect themselves by consistently monitoring the ads on their site or the ads they are placing. Web sites should enforce strict content guidelines for their advertisers and follow stringent rules as to who they sell their ads to, making sure the buyer is legitimate.

Researchers also suggest Web surfers avoid downloading any anti-spyware software that is not a well-known product.

Check out eWEEK.com's Security Center for the latest security news, reviews and analysis. And for insights on security coverage around the Web, take a look at eWEEK's Security Watch blog.