'Scareware' Scams Trick Searchers

Makers of fake anti-virus software are exploiting search engines to drive people to sites peddling 'scareware'. Using popular and mis-spelled search terms, the criminals divert people to sites that are seeded with fake warnings about virus infections.

The pop-up warnings claim that a visitor's PC is riddled with malicious programmes and spyware.

Research suggests some criminals are making as much as $10,000 a day from fake security software.

Cashing in

Computer security firm Finjan carried out the research into the techniques sellers of 'scareware' use to get their fake software in front of web users.

"They are misleading people with evidence that their machine is infected with viruses and they are encouraging them to download and buy software that basically does nothing," said Yuval Ben-Itzhak, chief technology officer at Finjan.

Studies suggest that 'scareware' is catching on among some hi-tech criminals.

A report by the Anti-Phishing Working Group, released in March 2009, found 9,287 bogus anti-malware programmes in circulation in December 2008 - a rise of 225% since January 2008.

"The reason they are making so much money is the new techniques they are using, namely search engine optimisation," he said.

Mr Ben-Itzhak said a campaign to push scareware typically involves two groups of hi-tech criminals. One group compromises webpages and injects them with popular search terms, the other sells the fake security software.

Some seed pages with popular keywords such as "Obama" but others use terms associated with recent events. Some tried to cash in on the death of Natasha Richardson by using words taken from news stories about the actress's death.

Using these popular terms mean the pages appear high up in results when people carry out a keyword search.

Anyone clicking on a booby-trapped page is then instantly re-directed to the site hosting the links to the fake security software.

Once they arrive, visitors are bombarded with pop-ups warning that their PC is infected. To clear up the infection users must download and pay for anti-virus software which typically costs about $50 (£34).Through its research, Finjan got access to the web-based systems that one group of 'scareware' peddlers used to manage their search engine campaigns.

It found that, over a 16-day period, more than 1.8m people were re-directed to the sites pushing the 'scareware'. Of those visiting the sites 7-12% installed the fake software and 1.79% paid $50 for it.

Some of the proceeds from this is handed back to those who inject the search terms into webpages, netting them about $10,800 (£7,467) a day for their work.

Mr Ben-Itzhak said people should be very wary of any pop-up window claiming to find evidence of an infection.

"It's impossible to scan your local disk without installing software," he said.

A spokesman for Google said it tried to combat efforts to trick its indexing system into crediting a page with more popularity than it deserved.

"In cases in which we feel that sites are attempting to manipulate rankings, we make adjustments to counterbalance and also discourage those efforts," said the spokesman in a statement.

"Certain actions such as cloaking - writing text in such a way that it can be seen by search engines but not by users - or setting up pages/links with the sole purpose of fooling search engines may result in removal from our index," he added. BBC