

Fake Security Software

technolytics

Quarterly Intelligence Brief

May 2009

Moves to Top Threat

REWARD

A \$500,000 reward is being offered for information leading to the arrest and conviction of those responsible for the Conficker worm.

FACTS

According to a Microsoft' report, scareware or rogue security software infections grew by 66 per cent during the last six months. They report 3 million computers were infected in the second half of 2008.

The lure of large profits is a huge temptation, especially in a poor economy. Criminals can make as much as \$5 million a year, planting fake or nearly worthless security software and coaxing unsuspecting users with so many bogus malware warnings that they fork over their credit card

A recent scareware mutation now claims to remove the widespread and highly publicized Conficker worm and instead compromises the computer. Conflicker is estimated at having infected nearly 4 million computers worldwide.

More and more Google's search rankings are being inundated with links to fake security software. Links to the rogue sites are located, not in search results, but advertisements that appear to the right.

The risks of security software or scareware as it has been dubbed is on the rise. Scareware is fake security products that actually installs malicious software on the computer of an unsuspecting user. It is one of most successful malware scams today and is making millions for criminals.



The fake security software acts like real security products and presents a screen that looks like it is scanning for security breaches. If or when the user clicks on the pop up box center screen, it downloads malicious software. It appears the target of the malicious software is the acquisition of personal information, specifically account information such as user names and passwords as well as credit card information. One of the more prominent pieces of scareware is said to come from antivirus-quickscan.com that is operated from Russia and others sources are emerging.

Another tactic being used by the criminals focuses on emails about security. The criminals mimic e-mail messages sent routinely by Microsoft to their security communications subscribers covering security software release information or a specific security incident. The fake security communications appears to be from Microsoft but is not and contain malicious links, scripts and other harmful booby-traps.

These tactics may not be new ones, but they are growing more and more popular as the cyber criminals and others are pushing the boundaries of tradecraft trickery. At this point we estimate there are over 7,500 variants of this type of scareware and infections are increasing rapidly.

These techniques have been around for a while now, but more and more users are falling prey to these deceptive practices. Social engineering is one of the thirty-four cyber attacks vectors. Addressing it is the most difficult problem faced by security professionals today. Technology alone cannot fix the problem. A recent study by the Psychology Department of North Carolina State University revealed that most Internet users don't exercise much caution when presented with fake dialog boxes and pop-up windows with obvious warning signs of malware. Security awareness training for all end users is a start, but it must be reinforced regularly through an internal communications campaign. These campaigns typically include physical posters, pop-up messages during user log-in, posts in the company news letter and so on. **Get the word out.**

The Technolytics Institute

4017 Washington Road
Mail Stop 348
McMurray, PA 15317
P 888-650-0800
F 412-291-1193
I www.technolytics.com

Confidential & Proprietary

© Copyright 2001-2009