TechTarget
Security Media

SearchSecurity.com SearchSecurity.co.UK SearchSecurity.in SearchFinancialSecurity.com SearchMidmarketSecurity.com
SearchSecurityChannel.com INFORMATION SECURITY DECISIONS FINANCIAL INFORMATION SECURITY DECISIONS INFORMATION SECURITY

SearchSecurity.com Pocket E-Guide

How to Prevent Rogue Antivirus Programs in the Enterprise

Why have so many smart people fallen prey to rogue antivirus scams? Rogue antivirus program creators have leveraged the end-user fear created by mass media scare tactics to trick users into downloading software that's too good to be true. In this expert pocket e-guide, get tips on safeguarding your organization from rogue antivirus because security education and awareness training isn't a sufficient method on its own.

Sponsored By: eset

TechTarget
Where Serious
Technology Buyers
Decide

ESET NOD32 Antivirus 4

Fast, Effective, Proactive, Antivirus and Antispyware

Our award-winning proactive threat-detection technology delivers the most effective protection from viruses, spyware, and other internet threats. ESET software blocks most threats the moment they are released, avoiding detection latency common to competing products. And with super-fast, super-easy operation, we keep your users productive, and your help-desk load down.

www.eset.com

eset

How to prevent rogue antivirus programs in the enterprise

Expert Response from Nick Lewis

Rogue antivirus programs have been one of the most successful attacker schemes, according to SANS. Why do you think so many people have fallen for these scams, and what are some best practices that can prevent my employees from downloading rogue antivirus software on enterprise machines?

Rogue antivirus programs have preyed on users' fears for several years now, and their presence has increased. As the mass media used scare tactics and warned of dangerous computer attacks, many have sought out cheap and easy ways to try to defend against threats. However, there are legitimate ways for employees to protect themselves.

Users should pause before clicking on a window and not install software download links from emails or websites that offer them something that's too good to be true. Unfortunately, this relies on your employees having "common sense," which is not a given. Users should make sure that they run up-to-date antimalware software, a personal firewall and an updated Web browser with antiphishing features. It is also important to have patched applications and a patched OS. All auto-update features should be enabled as well. Users could also ask their ISPs to provide them with a service (for free or a minimal cost) that filters out known malware. There are several best practices enterprises can use to prevent employees from downloading rogue AV on enterprise machines. First is to provide basic security awareness training about the risks involved with installing questionable software.

From a technical perspective, your enterprise should try to address the issues with filtering malware, but malicious code will find its way through these filters or other layers of protection. Users should run as limited users with least permissions and user rights (not as administrators or power users) and follow the best practices mentioned above. Without the user permissions or rights, malicious code usually is unable to effectively infect the system. For example, many rogue antivirus programs require users install software on their computers, and without this type of access, users can avoid getting infected. Not all rogue antivirus programs require users to install software and some exploit vulnerabilities on the computer.

Ultimately though, security education training and awareness among employees is the first and last line of defense against rogue antimalware software, but not the only one, since proper policy and technical controls can also serve to reduce the threat.

Resources from ESET

Endpoint security suites: What to consider before renewal

Top Five Security Threats for 2010

ESET NOD32 Antivirus 4 Trial

About ESET
ESET provides award winning security solutions that combined fast system scans with the ultimate in proactive protection against both known and unknown online threats. ESET NOD32 Antivirus was awarded "The Best Proactive On-demand Detection" and "The Best Overall Speed Performance" for 2008 by AV Comparatives.

By delivering state-of-the-art endpoint security, ESET Smart Solutions^{TM} increase your security while reducing your TCO. ESET's updated Remote Administrator, delivers a highly scalable enterprise-ready defense against malware, reducing your attack surface resulting in fewer help-desk loads. A light system footprint and blazing fast scanning speed can even extend the useful life of PCs and laptops.

ESET has also been named to the INC500 for the third consecutive year, and has an extensive partner and customer network, including corporations like Intel, Canon, Dell and Microsoft.