Fortinet Educates Internet Users with Top Ten Guide to Finding Spyware, Adware and Other ‘Grayware'

Submitted by: Cohesive Communications
Thursday, 9 September 2004

Fortinet Educates Internet Users with Top Ten Guide to Finding Spyware, Adware and Other ‘Grayware’

Users and Enterprise Administrators Urged to Address the Dangers of Adware, Spyware, Dialers, Hijackers, Key-Loggers and other ‘Ghost’ Threats

LONDON, September 9th 2004 ― Fortinet – the only provider of ASIC-powered, network-based antivirus firewall systems for real-time network protection – is offering enterprise Internet users an education in tackling the threat of ‘Grayware’; the wide range of unsolicited applications which install themselves onto unsuspecting computers to track and report back user information to an external source. Previously only identified as a home/SoHo user issue, today the wide-scale prevalence of grayware is affecting businesses, corporations and government agencies as numerous recent analyst reports have shown. In Fortinet’s view – ‘Grayware’ is the new ‘Virus’.

As part of a ground-breaking Fortinet white paper on the subject: “Protecting Networks Against Spyware, Adware and Other Forms of Grayware”, a Top Ten list of self-diagnosis tips is provided for users and network managers to test whether any such harmful, illegal or nuisance applications are present and operational on their systems.

“One of the key ways of protecting against any form of IT security threat is through user education. Grayware is a serious and growing threat, and I urge all Internet users to take these simple steps to recognise whether or not they are infected,” said Jonathan Mepsted, regional director, Fortinet. “While it’s clearly the role of the network manager/administrator to locate and acquire the best technical tools for remedying and protecting against security threats, the awareness and proper care of individual users is a powerful tool in itself - presenting a notable opportunity to avoid making unfortunate matters worse.”

Fortinet points out that while some grayware applications are little more than an annoyance, others are more sinister with enough sophistication to secretly read and record credit card numbers, personal messages and password keystrokes, track web-browsing habits or secretly dial premium-rate operator numbers. Perhaps most worrying of all is the ability of some grayware applications to disable existing desktop-based anti-virus programs, leaving the computer immediately prone to infection – often by duping the user into unwittingly switching it off.

“The emergence of grayware points to the need for businesses to adopt universal security threat management tools, as attackers adopt increasingly holistic and combined approaches to causing damage,” added Mepsted. “Installing grayware protection at the network perimeter where the private network meets the public Internet, can help identify and eradicate dubious applications before they even reach the end user’s computer.”

FortiOS 2.8, Fortinet’s Dynamic Threat Prevention technology, which is now shipping on all FortiGate™ antivirus firewall platforms, uniquely protects customers against all forms of grayware by blocking these

malicious applications before they enter customers' networks.

For more information about countering this clear and present threat, all concerned parties are invited to download a free, essential practice guide to stopping grayware in the enterprise by going: www.fortinet.com/promo/grayware.html

Fortinet's Top Ten Grayware Identifiers

1 Your computer is slower. The grayware application is taking more CPU and memory resources and causing the computer to slow down.
2 Your Windows Task Manager reveals that several "unknown" applications are operating.
3 The send/receive lights on your cable/DSL modem or the network/modem icons on the task bar flash to indicate traffic transmitted to and from your computer, even though you are offline.
4 The computer displays pop-up messages and advertisements when it's not connected to the Internet or when the browser is not running.
5 The home page on your web browser has been changed mysteriously. Changing it back may not fix the problem
6 Internet Explorer's search engine has been changed from the default setting, and search results are delivered by an unexpected search site.
7 Your web browser's 'favourite' list has been modified and changing it back or removing the new additions does not work.
8 Your search or web browser toolbars are modified and new options are installed. Attempts to remove the toolbar items fail.
9 Your phone bills increase due to numbers (particularly premium services numbers) that you did not use.
10 Your Antivirus, Anti-Spyware, or other security related program stops working. You receive warnings of missing application files and replacing them does not solve the problem.

About Fortinet (www.fortinet.com)
Fortinet's award-winning FortiGate™ series of ASIC-accelerated antivirus firewalls, winner of the 2003 Networking Industry Awards Firewall Product of the Year, are the new generation of real-time network protection systems. They detect and eliminate the most damaging, content-based threats from email and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time – without degrading network performance. FortiGate systems, the only security products that are quadruple-certified by the ICSA (antivirus, firewall, IPSec, NIDS), deliver a full range of network-level and application-level services in integrated, easily managed platforms. Named to the "Visionaries" category in the 2003 Gartner Enterprise Firewall Magic Quadrant, Fortinet is privately held and based in Sunnyvale, California.

# # #