PROTECTING NETWORKS AGAINST SPYWARE, ADWARE, AND OTHER FORMS OF "GRAYWARE"

FORTINET™

REAL TIME NETWORK PROTECTION

www.fortinet.com

Contents:

OVERVIEW

Grayware is a new term that is starting to appear on IT and security profession-als' radar screens. Many end users are only vaguely aware of grayware and its potential impact on their systems. But the probability of their PCs or laptops being infected with grayware is extremely high and many users have experi-enced the symptoms produced by grayware installed on their PCs. In addition, many of the most threatening impacts of grayware, such as usage pattern track-ing, invasion of privacy and information theft can remain unseen and all possi-ble without the user having to consciously download and execute any applica-tions.

With the many email viruses making headline news every few months, users are now beginning to understand the potential dangers of opening an unsolicited email - even if it's from someone they know! With grayware, users don't even have to open an attachment or execute a program to become infected. Just vis-iting a Web site that harbors this technology is enough to become a victim. And while some types of grayware such as pop-ups may be viewed in the same manner as spam - more of an annoyance that a true security threat - there is a fine line between "harmless" grayware and those types that can compromise valuable information such as credit card numbers, passwords, and even a user's identity.

>> *These applications are usually installed and run without the permission of the user*

WHAT IS GRAYWARE?

Grayware is an umbrella term applied to a wide range of applications that are installed on a user's computer to track and/or report certain information back to some external source. These applications are usually installed and run without the permission of the user. Some forms of grayware come as Trojan applications that trick users into installing them. Sources of grayware can come from any number of places and activities:

- Downloading shareware, freeware, or other forms of file sharing services
- Opening infected emails
- Clicking on pop-up advertising
- Visiting frivolous or spoofed web sites
- Installing Trojan applications

All grayware sources are not necessarily malevolent, as Web site developers are using newer techniques to customize their web sites and obtain better results. Tracking the usage patterns of visitors to offer more customized search results to result in higher sales is the ultimate goal of many of grayware applications.

Typically, the symptoms of having grayware installed on a host may be slower performance, more pop-up advertising, web browser home pages being redirected to other sites, and so forth. Generally these effects are more of an annoyance than a security threat. But hackers have also learned that grayware techniques can be used for other purposes too and have started using many of the web browser's capabilities to load and run programs that open access, collect information, track keystrokes, modify system settings, or to inflict other kinds of damage.

Although the most common grayware category gaining world wide attention is "Spyware", grayware can fall into many categories including:

Adware - Adware is usually embedded in freeware applications that users can download and install at no cost. Adware programs are used to load pop-up browser windows to deliver advertisements when the application is open or run.

Dialers - Dialers are grayware applications that are used to control the PC's modem. These applications are generally used to make long distance calls or call premium 900 numbers to create revenue for the thief.

Gaming - Gaming grayware applications are usually installed to provide joke or nuisance games.

Joke - Joke grayware are applications that are used to change system settings, but do no damage to the system. Examples include changing the system cursor or Windows' background image.

Peer-to-Peer - P2P grayware are applications that are installed to perform file exchanges. (P2P) While P2P is a legitimate protocol that can be used for business purposes, the grayware applications are often used to illegally swap music, movies, and other files.

Spyware - Spyware applications are usually included with freeware. Spyware is designed to track and analyze a user's activity, such a user's web browsing habits. The tracked information is sent back to the originator's Web site where it may be recorded and analyzed. Spyware can be responsible for performance related issues on the user's PC.

Key Logger - Key Loggers are perhaps one of the most dangerous grayware applications. These programs are installed to capture the keystrokes made on a keyboard. These applications can be designed to capture user and password information, credit card numbers, email, chat, instant messages, and more.

Hijacker - Hijackers are grayware applications that manipulate the Web browser or other settings to change the user's favorite or bookmarked sites, start pages, or menu options. Some Hijackers have the ability to manipulate DNS settings to reroute DNS requests to a malicious DNS server.

Plugins - Plugin grayware applications are designed to add additional programs or features to an existing application in an attempt to control, record, and send browsing preferences or other information back to an external destination.

Network Management - Network Management Tools are grayware applications that are designed to be installed to for malicious purposes. These applications are used to change Tools network settings, disrupt network security, or cause other forms of network disruption.

Remote Administration Tools - Remote Administration Tools are grayware applications that allow an external user to remotely gain access, change, or monitor a computer on a network.

BHO - BHO grayware applications are DLL files that are often installed as part of a software application to allow the program to control the behavior of Internet Explorer. Not all BHOs are malicious, but the potential exists to track surfing habits and gather other information stored on the host.

Toolbar - Toolbar grayware applications are installed to modify the computer's existing toolbar features. These programs can be used to monitor web habits, send information back to the developer, or change the functionality of the host.

Download - Downloaders are grayware applications that are installed to allow other software to be downloaded and installed without the user's knowledge. These applications are usually run during the startup process and can be used to install advertising, dial software, or other malicious code.

SYMPTOMS OF GRAYWARE

Grayware applications can perform many different tasks as outlined in the grayware categories above. Some of the most common symptoms that an infected system can exhibit include the following:

1. The performance of your computer is slower. The grayware application is taking more CPU and memory resources and causing the computer to slow down. By opening the Windows Task Manager and viewing the processes that are consuming the CPU and memory resources, grayware

applications may be identified. Often, the grayware applications running on the computer are "unknown" applications to the user.

2. The send and receive lights on your cable/DSL modem or the network/modem icons on the task bar are flashing to indicate traffic transmitted to and from your computer, even though you are not performing any online processes at that time to cause such traffic to occur.

3. The computer displays pop-up messages and advertisements when it's not connected to the Internet or when the browser is not running.

4. The home page on your web browser has been changed from your selected default and you did not instigate the change. And changing it back may not fix the problem.

5. Internet Explorer's search engine has been changed from the default setting and search results are delivered by an unexpected search site.

6. Your web browser's "favorite" list has been modified and changing it back or removing the new additions does not work.

7. Your search or web browser toolbars are modified and new options are installed. Attempts to remove the toolbar items fail.

8. Your phone bills increase due to numbers or premium services (900 numbers) that you did not use.

9. Your Antivirus program, Anti-Spyware program, or other security related program stops working. You receive warnings of missing application files and replacing them does not solve the problem. Sophisticated grayware applications may disable popular security programs before installing themselves.

PROTECTION AGAINST GRAYWARE

Stopping and preventing grayware from infecting hosts can be performed in several ways.

USER EDUCATION

Though not a sure-all method, every grayware mitigation program should start with development, communication, and enforcement of policies to guide end user behavior. This can be as simple as educating employees regarding the nature and dangers of grayware and establishing policies that prohibit downloading and installing applications that are not approved by the company. In the case where download and installation are allowed, users should be instructed to carefully research the provider's web site and read the fine print in the "End User License Agreement". By doing this, they may be surprised to learn what is being installed onto their and what the application are designed to do when they click on the software license's "I Agree..." button.

Grayware and Trojan applications designed for malicious intent will always be deceptive and try to stay well hidden to prevent disinfection and removal.

Other things that can help reduce the chances of grayware infection is to increase the security settings on the Web browser, configure email programs such as Microsoft Outlook to not automatically download Internet pictures or other material in HTML email, turn off auto-preview, and to stay on top of the latest security patches for all of your operating system and applications.

HOST-BASED ANTI-SPYWARE PROGRAMS

Users and IT professionals that have become "grayware educated" and understand the threats that these applications bring have started turning to client-based software applications that spot, remove, and block spyware. The new breed of Anti-Spyware applications functions similarly to the antivirus programs that are installed on nearly all computer systems today. Host-based anti-spyware applications have the ability to detect, remove, and block grayware applications, based on their signature database and the success will depend on the number of grayware signatures and the accuracy of their signature databases.

The difficulty with a client-based approach is the overhead that is normally associated with installing and maintaining client software applications on all corporate PCs. This includes the resources to purchase and install the software on each computer and to perform routine upgrades and updates to the software and its signature database. Depending on the anti-spyware's license scheme, the cost may also be intrusive to full corporate-wide adoption for some cost conscious customers.

One other danger of client-based security software is the possibility of having the Anti-spyware protection disabled by the end user or by a malicious application. Trojan and grayware applications are becoming more proactive with their installation routines and may check for the presence of protection software such as antivirus or personal firewalls. By disabling the protection software, during their installation process, they have a better chance running undetected.

NETWORK-BASED GRAYWARE PROTECTION

A third way of detecting grayware applications is through a network gateway approach. Installing grayware detection on a perimeter security appliance where the private corporate network connects to the Public Internet can help identify and eradicate grayware applications before they reach the end user's computer. The network-based approach centralizes the intelligence at the ingress point into the corporate network where grayware enters the company and significantly lowers the maintenance overhead of installing, maintaining, and keeping signature databases up-to-date. By performing an update on the gateway appliance performing the grayware protection, all computers behind the gateway are automatically protected.

The drawback of a centralized solution is when the user leaves the office and is no longer behind the security appliance. In these cases, the mobile users must rely on individual security programs that are installed on their computers to protect them against threats - such as antivirus and personal firewall programs.

FORTINET'S GRAYWARE PROTECTION SOLUTION

Fortinet takes a unique approach to combating grayware and utilizes both the network-based approach and the host approach. The network-based approach

>> Fortinet offers not only signature based threat recognition and protection, but also provides heuristic and anomaly detection technology to scan for new blended threats that do not currently have signatures

is provided by Fortinet's FortiGate™ Antivirus Firewall platforms, which are ASIC-accelerated devices that protect against viruses, worms, Trojans, intrusions, spam, inappropriate Web content - and grayware - in high performance, cist-effective, easy-to-deploy systems. The host approach is provided by Fortinet's FortiClient™ Host Security software, which provides a VPN client, antivirus protection, and personal firewall protection in addition to grayware detection. Fortinet combines several key security components into one gateway security
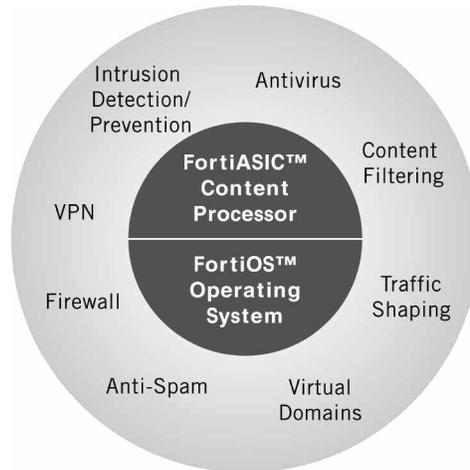

platform to deliver a unique security capability called the "Dynamic Threat Prevention System". By combining Antivirus, Stateful Firewalling, Intrusion Detection & Prevention (IPS), Virtual Private Network (VPN), Web Filtering, Spam Filtering, Grayware Detection & Protection, and Bandwidth Shaping into one security platform, it allows threat information to be shared and coordinated between each security component. This functionality allows Fortinet FortiGate security units to identify and stop new and blended threats that may otherwise sneak past traditional security appliances - such as traditional firewalls, antivirus, or IDS systems.

Fortinet's Dynamic Threat Prevention Systems makes use of its ICSA Lab certified Antivirus, IDS and IPS technologies to provide real-time protection against a wide range of threats. Fortinet offers not only signature based threat recognition and protection, but also provides heuristic and anomaly detection technology to scan for new blended threats that do not currently have signatures. This offers customers the best possible network-based security platform.
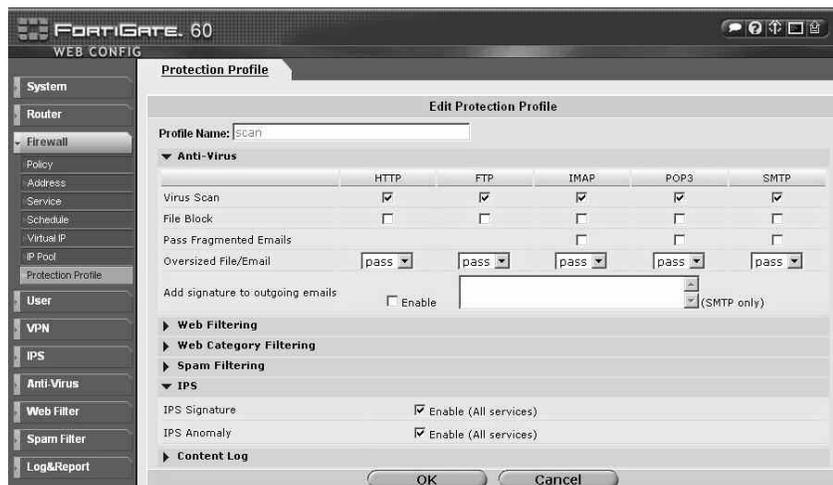
FORTIGATE PROTECTION POLICIES

Fortinet's Grayware Protection System leverages the full complement of Fortinet's signature, heuristic, and anomaly detection capabilities to detect grayware as it traverses the network. Administrators can customize the level of grayware scanning employed by enabling or disabling each grayware category, such as spyware, adware, dialers, etc.
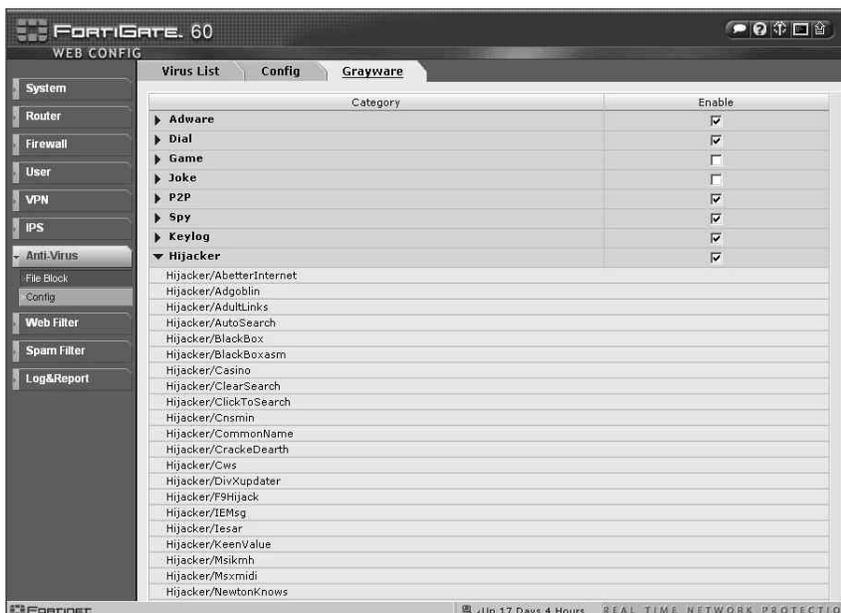
FORTIGATE GRAYWARE CONFIGURATION

Fortinet's network-based grayware protection minimizes the amount of resources required to install and maintain grayware security across a large number of end nodes. FortiGate security platforms installed at the network perimeter can detect, remove and block grayware applications before they enter the corporate network to prevent malicious applications from infecting and spreading on corporate resources. By centralizing security functions on a hardened network-based security platform, it makes it extremely difficult, if not impossible, for malicious applications to disable security functionality on the FortiGate units. For mobile workers, the FortiClient Host Security software extends AV, firewall, and grayware protection to users who do not have the benefit of protection from their company's FortiGate Antivirus Firewall.
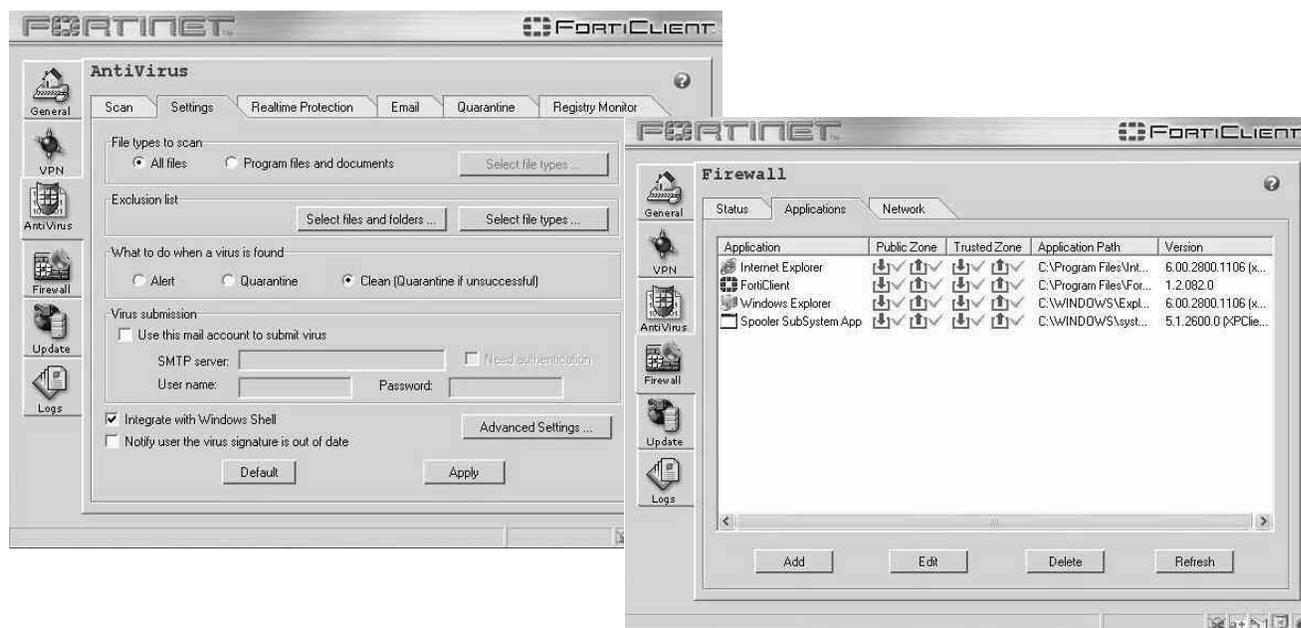
FORTICLIENT ANTIVIRUS AND PERSONAL FIREWALL

FortiGate systems and FortiClient software are kept up to date automatically with protection against new threats via the FortiProtect™ Network. This global network of people and systems across 3 continents identifies new threats, develops detection signatures and prevention actions, and loads updates whenever needed to FortiGate systems and FortiClient users wherever they are, 24x7x365.
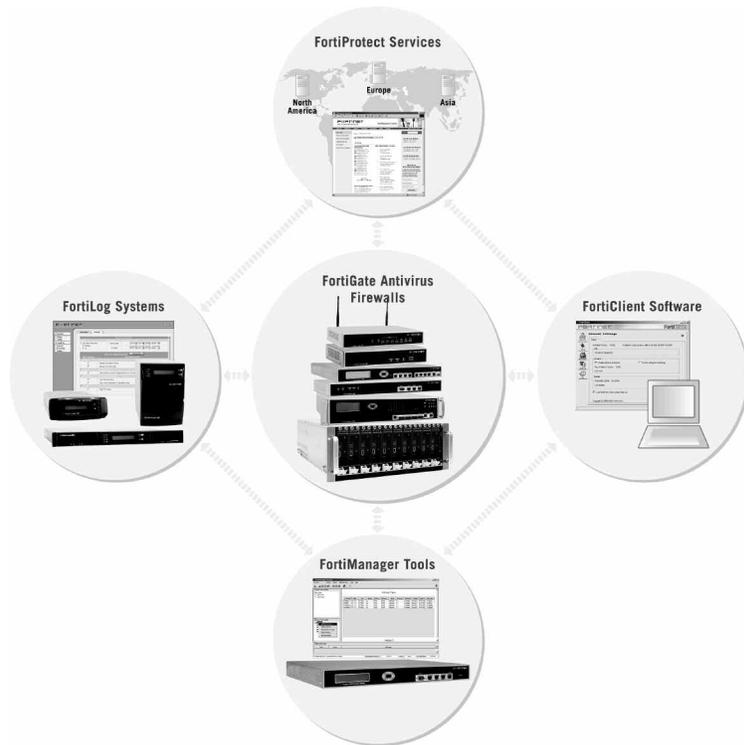
SUMMARY

The number of threats and vulnerabilities are continuing to grow and the need to stay on top of operating system patches, application patches, antivirus signatures, and so forth are becoming more critical and difficult to do. Fortinet solves this problem with its award winning FortiGate security platforms by providing a Dynamic Threat Prevention System to detect, remove, and block both known and unknown threats and anomalies.

To create this multi-tiered security system without major performance penalties, Fortinet developed a high-performance security asic (FortiASIC) that is specifically designed to speed up the computationally intensive routines commonly associated with complete content protection, which goes beyond Deep Packet Inspection and performs real-time content reassembly and analysis. This unique approach delivers performance for antivirus, grayware, IDS, encryption, content analysis, and related functions that is increased significantly over software-based security applications - and at a much lower cost.

To provide solid inspection, detection and prevention services, FortiGate units are ICSA Labs certified for Firewall, Antivirus, Intrusion Detection & Prevention, and IPSec VPN. The dedicated hardened FortiOS™ operating system provides real-time, high-performance, robust and reliable network security that can be applied at the network perimeter and into the network core. There are over a dozen FortiGate models starting with compact, low-cost devices to support telecommuter and SOHO applications and scaling to address high-performance,

www.fortinet.com

non-stop applications in the service provider core. To extend Fortinet's security to mobile users when they are not in the office, Fortinet's FortiClient software provides a well-rounded set of security applications to protect all corporate assets on the PC. FortiClient v1.2 provides Virtual Private Network, Personal Firewall, Antivirus, and Grayware protection to help keep unwanted traffic out.

To keep the security components up-to-date, Fortinet provides the FortiProtect Network to automatically update every FortiGuard unit when new security threats are identified - in real-time! Unlike traditional security solutions that require manual updating, the FortiProtect Network updates the FortiGuard security signatures as new threats become known - greatly decreasing the likeli-

hood of being attacked by new security threats.
Coupled with Fortinet's central management, reporting, logging systems and FortiProtect updates, enterprises can feel confident when implementing grayware security solutions from Fortinet. With Fortinet's simple licensing scheme that avoids per-user or per-seat licenses, the cost of implementing a world-class enterprise security system is much lower than competitive solutions.

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 and the 2004 Security Product of the Year Award from Network Computing Magazine, are the new generation of real-time network protection systems. They detect and eliminate the most damaging, content-based threats from e-mail and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time - without degrading network performance. FortiGate systems are the only security products that are quadruple-certified by the ICSA (antivirus, firewall, IPSec, NIDS), and deliver a full range of network-level and application-level services in integrated, easily managed platforms. Named to Red Herring Top 100 Private Companies, Fortinet is privately held and based in Sunnyvale, California.

For more information
More information about Fortinet, FortiGate Antivirus Firewall products, FortiProtect Center and other services provided by Fortinet is available from the following sources:

Sales
Please contact us at sales@fortinet.com, toll-free in the U.S. (866) 868-3678 or +1(408) 235-7700.

Potential Partners
Please contact us at partners@fortinet.com or visit us at www.fortinet.com.

FORTINET™
REAL TIME NETWORK PROTECTION

www.fortinet.com