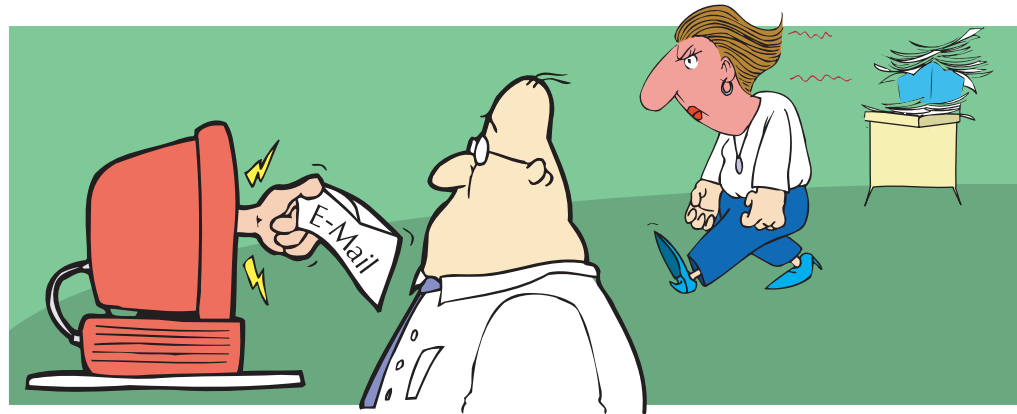


# The stealth-based



Fortinet's Ben Teh outlines the various threats such as spyware, adware and phishing that make up the growing category of greyware and he also provides ways of combating these insidious threats. If you haven't fallen victim to one of these threats, you are likely to suffer their impact soon. Indeed, the chances are that some form of greyware is already affecting your PC.

The newest threat to hit the internet, greyware operates by stealth, so many end users are only vaguely aware of it and its potential impact on their systems. But the probability of their PCs or laptops being infected by greyware is extremely high and many users are already experiencing the symptoms.

Many of the most threatening results of greyware, such as usage pattern tracking, and invasion of privacy and information, can occur without the user ever knowing it. With email worms and viruses making headline news, users are beginning to understand the potential dangers of opening an unsolicited email — even if it's from someone they know. But with greyware, users don't need to open an attachment or execute a program to become infected. Just visiting a website that harbours this technology is enough for the user to become a victim.

And while some types of greyware such as pop-ups may be viewed in the same manner as spam — more of an annoyance than a true security threat — there is a fine line between 'harmless' greyware and those types that can compromise valuable information such as credit card numbers, passwords and even a user's identity.

## What is greyware?

Greyware is an umbrella term applied to a wide range of applications 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 greyware come as Trojan applications that trick users into installing them. Sources of greyware can come from any number of places and activities, including:

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

Not all greyware sources are malevolent or dangerous. Website developers are using newer techniques to customise their websites and obtain better results. Tracking the usage patterns of visitors to offer more customised search results that lead to higher sales is the ultimate goal of many greyware applications. Typically, the symptoms of having greyware installed on a

# threat to computing



host may be slower performance, more pop-up advertising, or web browser home pages being redirected to other sites. Generally these effects are more of an annoyance than a security threat. But hackers have learned that greyware 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 inflict other kinds of damage.

Although the most common greyware category gaining worldwide attention is spyware, greyware can fall into many categories, including:

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

**Diallers** — Used to control the PC's modem. Usually used to make long distance calls or call premium 900 numbers to create revenue for the thief.

**Gaming** — Usually installed to provide joke or nuisance games.

**Joke** — Applications that change system settings without damaging the system. Examples include changing the system cursor or Windows' background image.

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

**Spyware** — Usually included with freeware, spyware tracks and analyses a user's activities such as web browsing habits. The information is sent back to the originator's website where it may be recorded and analysed.

**Key Logging** — Programs installed to capture the keystrokes made on a keyboard. They can capture user and password information, credit card numbers, email, chat, instant messages and more.

**Hijacking** — Applications that manipulate the web browser or other settings to change the user's favourite or bookmarked sites, start pages

or menu options. Some hijackers can manipulate DNS settings to re-route DNS requests to a malicious DNS server.

**Plug-ins** — 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** — Installed for malicious purposes, these applications change network settings, disrupt network security or cause other forms of network disruption.

**Remote Administration Tools** — Allow an external user to gain access, change or monitor a computer on a network.

**BHO** — DLL files that are often installed as part of a software application to allow the program to control Internet Explorer. Not all BHOs are malicious, but the potential exists to track surfing habits and gather information.

**Toolbars** — 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.

**Downloads** —

Applications that allow other software to be downloaded and installed without the user's knowledge. Usually these are run during the start-up process and can be used to install advertising, dial software or other malicious code.

*"Greyware 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."*

## Symptoms of greyware

Some of the most common symptoms of an infected system include:

1. Slower computer performance because the greyware application is taking more CPU and memory resources. The applications may be identified by opening the Windows Task Manager and viewing the processes consuming the CPU and memory resources. Often, the greyware comprises applications the user does not recognise.

2. The send and receive lights on a cable/DSL modem or the network/modem icons on the task bar are flashing to indicate traffic, even though you are not performing any online processes that might cause such traffic.
3. The computer displays pop-up messages and advertisements when it is not connected to the internet, or when the browser is not running.
4. The home page on a web browser has been changed from the selected default. 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. A web browser's 'favourites' list has been modified and changing it back or removing the new additions does not work.
7. Search or web browser toolbars are modified and new options installed. Attempts to remove the toolbar items fail.
8. Phone bills increase due to numbers or premium services that you did not use.
9. Your anti-virus 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 greyware applications may disable popular security programs before installing themselves.

### Protecting against greyware

A multi-faceted approach that combines security education with the proper technology is essential

*"A multi-faceted approach that combines security education with the proper technology is essential to stopping greyware and preventing it from infecting hosts."*

to stopping greyware and preventing it from infecting hosts.

Education on the nature and dangers of greyware is the first step towards identifying and protecting

against it. Corporations are strongly advised to implement established policies that prohibit employees from downloading and installing applications that are not approved by the company.

Other steps include increasing the web browser's security settings, configuring email programs such as Microsoft Outlook to not automatically download internet pictures or other material in HTML email and turn off auto-preview, as well as staying on top of the latest security patches for your operating system and applications.

### Host-based anti-spyware programs

The more computer-savvy have begun to use client-based software applications that spot, remove and block spyware, based on their signature database. The new breed of anti-spyware applications functions similarly to the anti-virus programs installed on nearly all computer systems today. Host-based anti-spyware applications can

detect, remove and block greyware applications, based on their signature database. Their success will depend on the number of greyware signatures and the accuracy of their signature databases.

The difficulty with this approach is the overhead normally associated with installing and maintaining client software applications on all corporate PCs. Depending on the anti-spyware's licence scheme, the cost may be prohibitive.

Another danger lies in the possibility of having the anti-spyware protection disabled by the end user, or by a malicious application. Trojan and greyware applications are becoming more proactive with their installation routines and may check for the presence of protection software such as anti-virus or personal firewalls. By disabling the protection software, during their installation process, they have a better chance running undetected.

### Network-based greyware protection

The network approach to detecting greyware applications, by installing a perimeter security device where the private corporate network connects to the public internet, can identify and eradicate greyware before it reaches the end user's computer. This approach significantly lowers the maintenance overhead of installing, maintaining and keeping signature databases up to date. Automatically updating the gateway protection appliance protects all computers behind the gateway.

But a centralised solution is vulnerable when users leave the office and rely on security programs installed on their computers to protect them against threats.

### The fail-safe solution

The ideal approach to combating greyware should combine both the network-based approach and the host approach. Network protection should come from anti-virus firewall devices that guard against viruses, worms, Trojans, intrusions, spam, inappropriate web content and greyware; while the host approach should comprise security software with a VPN client, anti-virus protection and personal firewall protection, in addition to greyware detection.

Combining key security components in this manner into a single gateway security platform delivers the ultimate in security. Identified by global research company IDC as Unified Threat Management, this allows threat information to be shared and coordinated between each security component to identify and stop new and blended threats that might otherwise sneak past traditional security appliances, such as standard firewalls, anti-virus or intrusion detection systems.

Ideal real-time protection against a wide range of threats should include both signature-based threat recognition and protection, and heuris-tic and anomaly detection technology to scan for new blended threats before the data protection companies have written signatures for them.

As the volume of threats and vulnerabilities continues to grow, the need to stay on top of operating system patches, application patches and anti-virus signatures is becoming more critical and increasingly difficult.



*Benjamin Teh is the Fortinet Sales Director for South Asia and Country Manager for Australia and New Zealand. Prior to joining Fortinet, Teh was Country Manager (South Asia) for Watchguard with responsibilities for India, Malaysia, Singapore, Indonesia, the Philippines and Australia. Teh brings with him considerable sales experience from his extensive coverage of the Asia region. He has also previously worked for technology distributors and system integration companies, dealing with products from Shiva, Exabyte and Fore Systems. Teh is a graduate of La Trobe University in Melbourne, Australia. He majored in computer science and communications engineering.*