

Solving the Spyware & Rootkit Problem

SpyWall™



Q: What is the most desirable feature of an anti-spyware solution, is it spyware prevention or removal?

A: Prevention is paramount. An overwhelming majority (~85%) of the attacks are via the Web browser. If the anti-spyware solution does not defend against web-based threats, then the user will spend a lot of time scanning and cleaning the machine.

Newer spyware and rootkits cannot be cleaned by majority of today's anti-spyware products and that makes prevention even more important.

Q: Desktop or Gateway?

A: Desktop security is very important in defeating spyware. Gateway-based anti-spyware, while important, can only provide limited protection and will not catch attacks based on new web browser exploits or spyware coming over SSL connections. Mobile PCs are not protected by gateway based solutions.

Q: How good are anti-spyware softwares in removing spyware?

A: Not very good. In the best case they may detect about 90% of malware, but can only remove about 20-50%. SpyWall is the only anti-spyware software that enables the removal of 100% of spyware from the PC.

Q: What is the best way to keep a PC spyware free?

A: Your security solution should:

- Block the attack vector
- Run periodic scan and clean
- Prevent unauthorized downloads.

Only SpyWall has all of the above features.

Q: How do I tell if my anti-spyware solution is good enough?

A: Were you able to clean an infected PC or did you have to rebuild it? Are your PCs getting infected even with the anti-spyware software in place? Answer to these two question tells you how good is your current anti-spyware solution.

SpyWall is the only solution that addresses the problem at all layers (network, OS, application, & user). It can not only detect and remove regenerative spyware and rootkits, it also blocks the spyware attack vectors.

To solve the spyware problem, and to understand why SpyWall is the best solution, it is important to first get a better understanding of the spyware problem.

UNDERSTANDING SPYWARE

The nature, reason, and mechanism for spyware.

Nature

Spyware can reside on user PC or it can reside on a website that the user visits.

When the spyware is on a PC (local spyware), it can:

- Hijack resources, e.g. browser settings
- Serve unwanted advertisements & pop-ups
- Steal information from files, keyboards etc.

When spyware resides on a website (remote spyware), it can:

- Collect user information by coaxing them into providing that information, i.e. phishing or farming
- Infect the PC of a user visiting that site

Reason

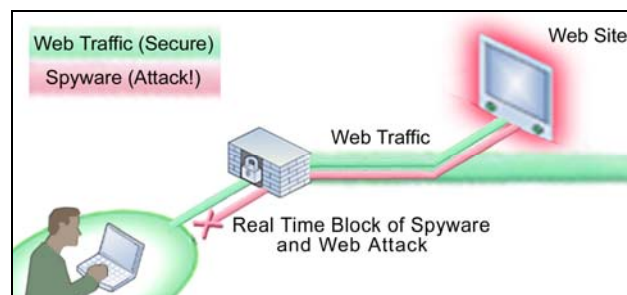
The main reason for spyware is financial. Because spyware has become a major source of revenue generation, this problem is getting worse and is not likely to get better anytime soon.

Mechanism

Web access is the prime mechanism used by spyware to infect PCs. Spyware infection can also happen via instant messengers (IMs), e-mail, infected portable media, and self propagating worms. User actions are also a cause for spyware, but not always.

Web access accounts for 85% of spyware problems and is the method of choice for spyware infection.

WHY IS SPYWALL "THE BEST" PROTECTION AGAINST SPYWARE?



SpyWall™ addresses the root cause of spyware.



TRLOKOM
Secure Networks

Solving the Spyware & Rootkit Problem

SpyWall™



Web traffic to the Internet is the main source for spyware. It provides hackers with a direct channel into the enterprise network to easily install spyware. Not protecting this channel is unwise at best.

SpyWall is the first and only firewall/sandbox for the web browser that provides comprehensive protection against these threats. SpyWall attacks the spyware problem at four layers i.e. Network, OS, Application, and User. This comprehensive protection ensures that no channel is left open for spyware to come into enterprise network.

In addition to proactive protection at four layers, SpyWall will remove even the most difficult spyware from you PC. It will also block phishing attacks, monitor web usage by users, and block malicious websites.

WHY IS SPYWALL BETTER IN DETECTING AND REMOVING SPYWARE?

SpyWall has a database of over 100,000 spyware signatures which is comparable to the databases of other anti-spyware products. However, SpyWall does not primarily rely on signatures and uses application behavior monitoring and system audit to detect spyware. Recent report by CERT has shown that malware writers are easily able to bypass detection by popular anti-spyware and anti-virus products as these products rely mostly on signatures to detect spyware.

Some of the stealthier spyware can inject themselves into the operating system by modifying kernel files and are not detectable by other anti-spyware software. SpyWall has a specialized scanner that finds rootkits, keyloggers, and spyware that is hidden inside the kernel or applications.

Polymorphic spyware mutates continuously to evade detection, regenerates if removed, and may even start even in safe mode to prevent removal. Since most anti-spyware solution cannot clean such spyware, they sometimes release new “spyware specific” tools for cleaning. This becomes very tedious as it the user has to download these tools and clean the machine manually. Often these tools are not able to remove the spyware.

SpyWall is the only product that can successfully remove regenerative spyware. A new patent pending

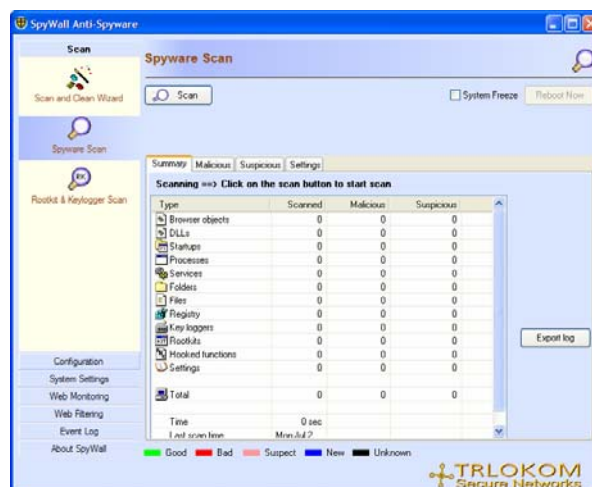
method used by SpyWall enables the removal of even the most difficult to remove spyware.

The comprehensive and leading edge coverage provided by SpyWall in removing and preventing spyware makes SpyWall the ideal choice in solving the spyware menace.

Trlok, Inc.

Tel: 1 626 357 3706

Email: spywall@trlok.com



SpyWall trial version

<http://www.trlok.com/product/spywall.php>

Central management tool for SpyWall

www.trlok.com/product/trlok_central_management.php



TRLOKOM
Secure Networks