

Proactive Protection as a Means of Defense against Internet-Borne Threats

Abstract

This TechNote explains why proactive protection is a vital component in today's security products. It goes on to show how the intelligent use of technologies that monitor program activity and block unauthorized operations can proactively defend an Internet-connected PC against the majority of malware threats. The document also incorporates a video demonstration of Outpost proactively preventing real-world malware from propagating on a user's PC.

Threat landscape

Personal data stored on home and small office PCs is at risk of being stolen and misused by cybercriminals every time users go online. Examples of high-profile data compromises are numerous and incidents of this type appear in the media almost daily: a keylogger can be silently embedded into the system and transmit all your passwords to a hacker, or a botnet can take over a vulnerable PC and use it to stage concerted attacks on other victims. A Trojan can be invisibly downloaded to your PC while you're surfing the Web that not only mines documents and sends them to outside servers, but encrypts this information and demands a ransom to return it to the legitimate owner (you). Users frequently don't know they are being attacked until it's too late.

Even users with up-to-date antivirus and antispymware protection can suffer data breaches and 0-day infections. This happens because their current protection doesn't reliably protect against unknown malware - they are unable to detect new threats because there is no corresponding signature to identify the malicious code.

Security threats evolve almost daily. New viruses, Trojans and other malicious programs are being written with a purpose of intruding upon our safe and productive Internet use. Unpatched vulnerabilities¹ leave computers open to infection by zero-day exploits which can inflict serious damage within a matter of hours of first appearing on the Internet.

Security researchers report that the volume of threats has risen considerably over the past five years, and acknowledge that it becomes ever harder for signature detection to keep pace with the malware writers². Readily-available toolkits for creating custom malware from code samples enable even amateur programmers to come up with their own unique malware that deviates only slightly from the original sample, but is different enough to evade detection by traditional signature-based solutions. And security companies' research staffs are tiny in size when compared with the number of "dark side" programmers now working in populous nations like China and India and swelling the ranks of hackers and cybercriminals.

¹ One such example is the Windows Animated Cursor vulnerability (<http://secunia.com/advisories/24659>). The flaw allows an attacker to access data and run unauthorized code on the user's machine. Microsoft issued a patch some time ago, but users continue to be infected if they have not patched their systems.

² See this article for one of such mentioning <http://www.pcadvisor.co.uk/news/index.cfm?newsid=11723&pn=1>

Successful threat mitigation is further impeded by the fact that virus writers are adopting the same quality control techniques as the anti-malware developers, testing their latest creations against the latest versions of anti-malware to make sure they remain one step ahead.

Clearly, it's pretty much impossible to protect against new, altered or obscure malware with a signature-based solution alone; writers of malicious programs will always be able to maintain an edge over this reactive type of defense³.

As reactive security scanners struggle to keep pace with emerging malware, it's vital that users consider the use of alternate, proactive solutions that monitor the behavior of suspect code and proactively block unauthorized activity.

The need for additional measures

While reactive protection remains an important component of malware protection for precise identification and disinfection of known malware, there is clearly a need for proactive protection that can prevent unauthorized program activity from occurring in the first place.

As opposed to examining whether a sample corresponds to a known malicious fingerprint and quarantining the offending application, proactive security products analyze the sample's behavior and limit its activity in case it is determined to be unauthorized. By adding proactive protection that monitors what programs do, with which programs and components any given program is allowed to communicate, any attempted modifications to the operating system, computers are better protected against inappropriate activity and better positioned to prevent infections at an earlier stage.

Application interactivity - a key vulnerability

Windows provides multiple ways for programs to interact on a PC⁴, and most such interaction is quite legitimate. Programs can freely share common components, call and launch each other's executable files, and use a number of different hooks to simplify program interaction and render the user's computing experience more streamlined and convenient. As an illustration, all one has to do to read a PDF file attachment to an email is to click on the file icon and the PDF is automatically loaded into the default viewer. It would be a lot more time consuming if one had to save the file to disk, open Acrobat Reader, and load the file into the application.

However, Windows also permits rather less benign interactions to take place, and this constitutes a major security risk. Applications themselves may also be allowed to perform malicious activity, from hijacking memory to using another program's privileges for nefarious purposes to making illegal modifications to the Windows configuration.

This type of interaction is of course totally unacceptable and must be controlled. The best way to do this is to use specialized tools that are designed specifically to monitor for this type of activity and block illegal operations before they are even attempted.

³ "Anti-Virus is Dead: Long Live Anti-Malware" - this Yankee Group research is discussed extensively in a [PC World article](#).

⁴ Assuming a user has Administrator privileges in Windows XP. For Windows Vista users, UAC is implemented to restrict a set of permissible actions without escalating program privileges, but it is fairly obtrusive and unable to 'learn' what is allowable activity.

Use case

A typical Windows user is exposed to multiple risk windows every day. The main attack vectors are:

1) *Drive-by download of malware after visiting a malicious or compromised website that hosts an embedded exploit or executes malicious script.*

This can occur, for example, when a person is surfing the Internet looking for popular content like screensavers, music downloads or Java games and accidentally visits a poisoned website that silently injects rogue code into the browser. The browser is then compromised and may leak the infection into the PC. An unwitting victim can also be lured to unscrupulous sites through spam or phishing.

2) *Running programs obtained from peer-to-peer networks.*

It's important to remember that files obtained from untrusted sources are not always what they seem to be. "Britney.mpg" file is not necessarily a video clip of Britney Spears but can easily be a Trojan horse. If this malware is relatively new, traditional anti-malware software may not catch it before it's able to execute.

3) *Opening infected attachments or downloading from links sent over IM communication.*

Virus propagation through email remains one of the most common attack vectors, and users should be careful when opening email attachments. Files with .exe and other non-data-type extensions should always be regarded with suspicion unless you are expecting a file from a person you know and can check the legitimacy of the attachment by phone or other non-computer means.

4) *Running or installing a seemingly innocuous file or program that contains malicious payload.*

Any component of a downloaded application can have viral content. Freeware programs are notorious for having spyware components embedded in them. And **never** download anything from a warez site.

The proactive difference

So, how does proactive protection help avoid infection?

Because the majority of inter-application operations take place under the supervision of tools that control program activity, the user can choose what kind of activity should be allowed, and what should be blocked. Users can thus prevent unauthorized activity in advance by proactively monitoring for it and preventing malware from activating, communicating or propagating beyond the protected PC. Reactive signature-based anti-malware detection products are unequal to this task; all they can do is disinfect or remove already-infected objects.

Outpost's solution

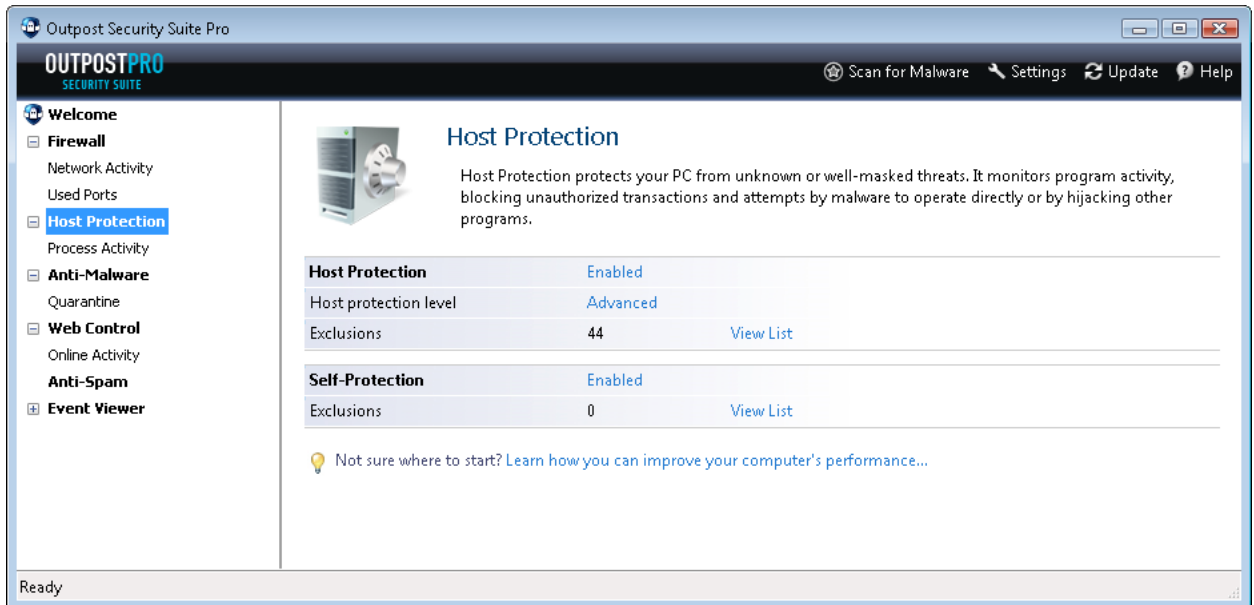
Outpost Security Suite Pro includes a module called Host Protection, which enables users to control program activity and limit the scope of actions any program can take. With Host Protection, users can assign custom policies for installed programs, including designating which programs are allowed to interact with other software and alter system settings. This helps prevent unauthorized activity by any program on a PC, so malware scanning becomes a secondary rather than a primary defense mechanism.

Users can decide for themselves the types of activity the module should monitor and control, and compile their own list of trusted applications.

To see this module in action and get a real sense of how it can counter security threats just by

monitoring and alerting on suspicious behavior, watch this Proactive Protection [video](#).

The robust Host Protection module will keep you shielded from inappropriate activity



The strength of the Host Protection mechanism has been extensively tested by independent third party testers as well as by our internal team and found to be the most effective among available firewalls.

Conclusions

Proactive protection is a key element of any desktop defense strategy. By monitoring for unauthorized behavior, it can radically reduce the PC's susceptibility to threats without depending entirely on the currency and accuracy of signature databases.