



Die Anti-Malware-Technologie der Outpost Security Suite Pro

Zeitersparnis durch schnellere Überprüfung!

Zusammenfassung

Dieses Dokument beschreibt die neuen Technologien in der Outpost Security Suite Pro, die dazu beitragen, schädliche Programme ohne Beeinträchtigung der Systemleistung wirksam zu bekämpfen.

Einleitung

Outpost Security Suite Pro enthält ein spezielles Anti-Malware-Modul, das im Gegensatz zu herkömmlichen Antiviren- oder Anti-Spyware-Programmen vor einer Vielzahl von Bedrohungsarten schützt: vor Viren, Spyware, Botnet-bildenden Trojanern, Rootkits uvm. Das Modul wurde so optimiert, dass es eine schnellere Überprüfung bietet, ohne dabei die normalen Aktivitäten zu unterbrechen.

Zwei Engines, ein umfassender Scanner

Das Anti-Malware-Modul der Outpost Security Suite Pro erweitert die Spywareschutz- und Trojanerschutz-Technologie in der Outpost Firewall Pro durch das Hinzufügen einer speziellen Antiviren-Engine. Der kombinierte Anti-Malware-Scanner bietet zwei eigenständige Mechanismen zur Bekämpfung von Schadprogrammen. Sie werden von zwei unabhängigen Experten-Forschungsteams aktualisiert, die zusammenarbeiten, um für einen reibungslosen Schutz gegen die heutigen Bedrohungen, die häufig in gemischter Form auftreten, zu sorgen.

Die Antiviren-Engine wurde von Virus Buster aus Ungarn lizenziert, hat bereits zahlreiche Auszeichnungen gewonnen und ist durch West Coast Labs, ICSA Labs und Virus Bulletin zertifiziert (weitere Informationen in englischer Sprache finden Sie [hier](#).)

Wenn der Anti-Malware-Scanner nach schädlichen Programmen sucht, verwendet er beide Engines gleichzeitig, um Bedrohungen zu finden und zu entfernen. Die Aktualisierungen der Malware-Definitionen sind zusammengefasst und werden täglich übermittelt, um zu gewährleisten, dass der Schutz ständig auf dem neuesten Stand ist.

Steigerungen der Scan-Leistung

Die meisten Sicherheitsprodukte bieten Schutz gegen Viren und andere Schadprogramme, indem sie auf das Vorhandensein von Virencodes hin überprüfen. Im Grunde bedeutet das die Konzentration darauf, dass jedes Objekt bei der Übertragung gescannt und mit einem Satz bekannter Malware-Fingerabdrücke verglichen wird, die aus vergangenen Bedrohungen herausgefiltert wurden.

Das Vergleichen einer Datei mit einer großen Datenbank von Malware-Definitionen benötigt Zeit und Systemleistung. Wenn der überprüfte Computer noch dazu eine große Anzahl von Dateien enthält, wie das bei den riesigen Festplatten heute oft der Fall ist, dann kann die Aufgabe, den gesamten Computer zu überprüfen, ausgesprochen zeitaufwendig sein.

Bei den meisten Anwendern ändern sich jedoch nur relativ wenige Dateien auf der Festplatte täglich. Der typische tägliche Scan bewegt sich also unnötig über zum Großteil bereits bekanntes Terrain. Outpost Security Suite Pro nutzt die neue SmartScan-Technologie, um einen intelligenteren Ansatz zu verwenden, bei dem nur die Objekte überprüft werden, die seit dem letzten Scan auf irgendeine Weise verändert wurden. So läuft die Überprüfung wesentlich schneller ab und beansprucht wesentlich weniger Systemressourcen.

Wie der SmartScan funktioniert

Wenn ein System bereits mindestens einmal mit dem Anti-Malware-Modul von Outpost überprüft wurde, kann die für einen weiteren Scan benötigte Zeit durch SmartScan erheblich verringert werden. Diese

Optimierung wird durch die Verwendung von Cache-Dateien erreicht, die Informationen über den Status der letzten Überprüfung jedes Objekts speichern. Wenn das Objekt sich seit der letzten Überprüfung nicht geändert hat, wird es von den nachfolgenden Scans ausgeschlossen. Auch der speicherresidente Scanner verwendet die SmartScan-Technologie: Wenn eine neue Anwendung in den Arbeitsspeicher geladen wird, wird sie nur dann überprüft, wenn sie nicht zuvor bereits validiert wurde oder wenn sie sich seit der letzten Ausführung geändert hat. So wird nicht nur die Geschwindigkeit der Echtzeit-Überprüfung erhöht, so dass das System schneller reagiert, sondern auch der Programmstart wird beschleunigt.

Technische Umsetzung

Während des ersten Scans erstellt Outpost Security Suite Pro zwei Hilfs-Indexdateien in jedem Ordner - OP_CACHE.ATR und OP_CACHE.IDX. Diese Dateien sind im Dateiverzeichnis versteckt, so dass sie so unmanipulierbar wie möglich sind. Außerdem werden diese Dateien durch die Selbstschutz-Funktion von Outpost geschützt, die dafür sorgt, dass die Outpost-Komponenten nicht durch unautorisierte Programme aufgerufen, verändert oder deaktiviert werden können.

Um vergangene Scan-Ergebnisse zurückzuverfolgen, aktualisiert Outpost die interne Registrierungsdatenbank dieser Index-Dateien mit Daten wie etwa Informationen darüber, welche Dateien in einem Ordner bereits überprüft wurden und wann, dem Datum der letzten Änderung der Datei und anderen Wartungsinformationen. Der Scanner sammelt Informationen von diesen Dateien über den Status bisheriger Anti-Malware-Scans aller Elemente, die zu einem bestimmten Ordner gehören.

Jedes bereits überprüfte Objekt wird von weiteren Scans ausgeschlossen, solange sich seine Inhalte nicht ändern oder Ihre Malware-Signaturen nicht aktualisiert werden. Andernfalls werden die Cache-Dateien zurückgesetzt und das Objekt verliert seinen privilegierten „sauberen“ Status, was bei der nächsten Überprüfung zwingend eine Überprüfung auslöst.

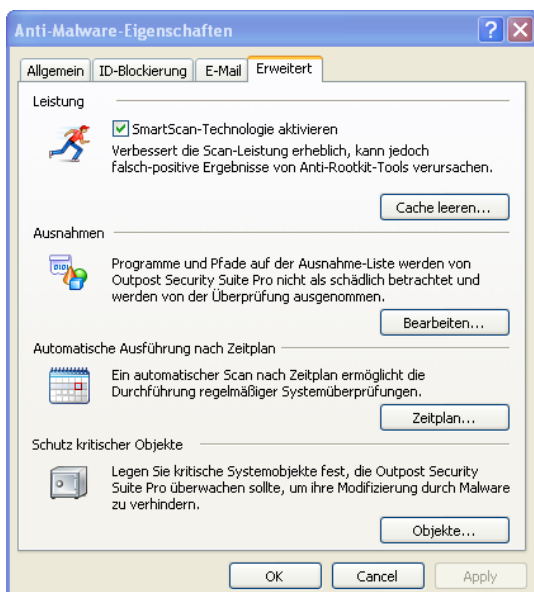
Anders als andere beliebte Anti-Malware-Produkte, die oberflächlich ähnliche Cache-Technologien verwenden, unterstützt SmartScan alle Arten von PC-Dateisystemen, nicht nur NTFS.

Die Leistungsvorteile der SmartScan-Technologie sind in Diagrammform am Ende dieses Dokuments in Anhang 1 zusammengefasst.

Die Verwendung von SmartScan

Sie können die Verwendung von SmartScan nach der Installation von Outpost Security Suite Pro im Konfigurationsassistenten aktivieren. Alternativ können Sie jederzeit auf die SmartScan-Eigenschaften zugreifen, wenn Sie folgende Schritte befolgen: 1) Klicken Sie in der Outpost-Benutzeroberfläche auf Optionen und gehen Sie zu den Plug-In-Einstellungen. 2) Wählen Sie das Plug-In Anti-Malware. 3) Klicken Sie auf die Registerkarte Erweitert. 4) Aktivieren Sie das Kontrollkästchen ‚SmartScan-Technologie aktivieren‘, wie unten abgebildet.

Sie können die Cache-Dateien jederzeit bereinigen, indem Sie auf die Schaltfläche ‚Cache leeren‘ klicken. Diese Dateien werden automatisch entfernt, wenn Outpost deinstalliert wird.



Ein Hinweis zu Anti-Rootkit-Tools: Cache-Dateien sind schreibgeschützt und mit herkömmlichen Datei-Managern wie dem Windows Explorer vielleicht nicht sichtbar. Einige Anti-Rootkit-Programme können Cache-Dateien als verdächtig melden, da die Methode, Inhalte zum Schutz vor Malware-Befall zu verbergen, als typische Eigenschaft von Rootkits gedeutet werden kann. Da Anti-Rootkit-Programme mit den unterschiedlichsten Methoden arbeiten, haben wir leider nicht die Möglichkeit, die Cache-Dateien von Outpost als harmlos zu kennzeichnen; wir können Ihnen jedoch versichern, dass diese Dateien tatsächlich sicher sind.

Optimierung des residenten Scanners

Wenn eine von Malware befallene Datei geöffnet wird, besteht ein sehr hohes Risiko, dass die Infektion sich aktiviert und ausbreitet. Zum Glück besteht dieses Risiko nicht, wenn die Datei einfach kopiert oder umbenannt wird oder wenn ihre Eigenschaften angezeigt werden; die Ladung wird erst bei Ausführung der Datei aktiviert.

Outpost Security Suite Pro bietet den Anwendern die Wahl, auf welche Weise die Anti-Malware-Komponente Programmaktivitäten in Echtzeit überprüfen soll: bei Zugriff oder bei Ausführung. Die letztgenannte Möglichkeit führt eindeutig zu einer besseren Leistung.

- **Dateien bei Ausführung überprüfen.** Das verhindert den Start schädlicher Programme und überprüft Dateien nur dann, wenn sie geöffnet werden. Andere Datei-Zugriffsbefehle wie etwa das Kopieren der Datei oder das Ansehen der Dateieigenschaften oder Anzeigen von Ordnerinhalten sind von dieser Möglichkeit nicht betroffen.
- **Dateien bei Zugriff überprüfen.** Dieser Modus löst einen Malware-Scan aus, wenn irgendeine Form von Dateizugriff versucht wird.

Vorteile

Dieser Ansatz bietet maßgeschneiderten Schutz für jeden. Einige Leute fühlen sich erst dann sicher, wenn sie jedes Fenster und jede Tür in ihrem Haus täglich überprüfen - für diese Anwender ist die Datei-Überprüfung bei Zugriff für ein möglichst sicheres Gefühl sinnvoll. Andere sind voll und ganz damit zufrieden, eine Überprüfung nur dann vorzunehmen, wenn tatsächlich ein Risiko besteht - für diese Anwender ist die Datei-Überprüfung bei Ausführung die bessere Wahl.

Technische Umsetzung

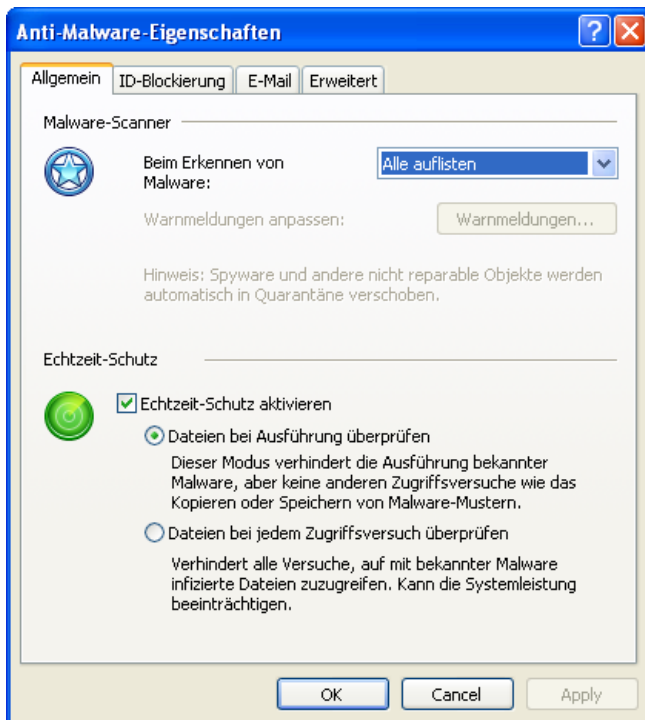
Im Modus der Überprüfung bei Ausführung überprüft Outpost Security Suite Pro das Laden von Modulen, die für die Code-Ausführung verantwortlich sind. Dieser Code wird durch das Anti-Malware-Plug-In gründlich überprüft, bevor er die Kontrolle übernehmen darf. In diesem Modus werden sowohl ausführbare Programmdateien als auch Dokumentendateien (wie Word oder Excel) überprüft, die eventuell Makro-Befehle und anderen "versteckten ausführbaren" Code enthalten können. Die Dateien werden jedoch nicht beim Kopieren oder Speichern auf Viren überprüft.

Im Modus der Überprüfung bei Zugriff werden alle Zugriffsversuche auf die Datei überwacht. So wird gewährleistet, dass auch der Zugriff auf Dateien überwacht und gesichert wird, die eigentlich nicht dazu entwickelt wurden, Programmcode zu enthalten, bei denen jedoch vielleicht bereits eine Sicherheitslücke ausgenutzt wurde.

Auswahl des entsprechenden Modus

Um den entsprechenden Modus auszuwählen:

- 1) Wählen Sie im Options-Menü von Outpost das Plug-In Anti-Malware.
- 2) Klicken Sie auf die Registerkarte Allgemein.
- 3) Aktivieren Sie das Kontrollkästchen ‚Echtzeit-Schutz aktivieren‘ und wählen Sie dann das entsprechende Kontrollfeld für den gewünschten Betriebsmodus, wie unten angegeben.



Zusammenfassung

Die neue Kombination der Outpost Security Suite Pro von Anti-Malware-Modul mit SmartScan-Technologie ist immer auf der Hut vor allen möglichen Risiken. Sie überprüft schnell und genau, verringert die Belastung für die Systemressourcen, aktiviert sich nur im Bedarfsfall und ist sehr einfach zu bedienen. Weitere Informationen sowie die Möglichkeit zum Herunterladen der Testversion finden Sie unter <http://www.agnitum.de/products/security-suite/index.php>.

Anhang 1: Leistung Diagramme

