



Vermeidung von Informationslecks mit Outpost Firewall Pro 4.0

**Ein Leitfaden zum Thema Leak-
Tests**

Inhaltsverzeichnis

Überblick	3
Gliederung	3
Sicherheit ist ein vielschichtiges Problem	3
Tools zur Überprüfung der Firewall-Wachsamkeit	6
Neue Datenschutz-Funktion in Outpost Firewall Pro 4.0.....	7
Ein Überblick zum Thema Leak-Tests	7
Arten von Informationslecks	8
Nun ist es Zeit für die Leak-Tests selbst.....	9
Leak-Test Nr. 1 "Firewall Leakage Tester"	10
Leak-Test Nr. 2 "TooLeaky"	10
Leak-Test Nr. 2 "TooLeaky"	11
Leak-Test Nr. 3 "WallBreaker"	12
Leak-Test Nr. 4 "Ghost"	13
Leak-Test Nr. 5 "YALTA"	14
Leak-Test Nr. 6 "DNSTester"	15
Leak-Test Nr. 7 "FireHole"	16
Leak-Test Nr. 8 "pcAudit"	17
Leak-Test Nr. 9 "Comodo Parent Injection Leak Test"	18
Leak-Test Nr. 11 "Copycat"	20
Leak-Test Nr. 12 "Atelier Web Firewall Tester"	21
Leak-Test Nr. 13 "Surfer"	22
Leak-Test Nr. 14 "PCFlank Leaktest"	23
Leak-Test Nr. 15 "Breakout"	24
Leak-Test Nr. 16 "MBtest"	25
Leak-Test Nr. 17 "OutBound"	26
Leak-Test Nr. 18 "Jumper"	27
Hintergrundinformationen über Agnitum.....	28
Schlussfolgerung.....	28
Über Agnitum	29
Kontakt.....	29

Überblick

Outpost Firewall Pro 4.0 ist die erste Personal Firewall mit einer Anti-Leak-Technologie, die alle bekannten Leak-Tests besteht und speziell dazu entwickelt wurde, zu verhindern, dass Malware-Programme durch Hijacking die Zugriffs-Autorisierungen einer vertrauenswürdigen Anwendung übernehmen und so Informationen von einem geschützten Computer nach außen übermitteln.

Dieses Dokument befasst sich hauptsächlich mit dem umfassenden Schutz, den Outpost Firewall Pro 4.0 bietet und dadurch verhindert, dass persönliche und private Informationen durch Sicherheitslecks von Ihrem PC in die Hände von Hackern und Cyberkriminellen gelangen. Beispiele aus der Praxis haben bewiesen, dass Outpost Firewall Pro 4.0 alle Leak-Tests von Drittanbietern besteht und Benutzern von PCs mit Internetverbindung erheblich mehr Sicherheit bietet.

Gliederung

Das vorliegende Dokument enthält alle Informationen, die Privatanwender benötigen, um die Themen Systemsicherheit und besonders Firewalls zu verstehen und um nachvollziehen zu können, wie Tools von Drittanbietern dazu eingesetzt werden, zu überprüfen, wie zuverlässig Firewalls die Anwender gegen Informationslecks schützen.

Das Dokument ist in drei Teile gegliedert:

1. Der erste Teil bietet einen Überblick über die derzeitige Sicherheitslage für Windows-basierte Computer, über die Rolle und den Funktionsumfang von Personal Firewalls und darüber, wie sich Outpost Firewall Pro von anderen Personal Firewalls unterscheidet.
2. Kernstück des Dokuments sind die Ergebnisse einer Reihe von Leak-Tests, denen Outpost Pro unterzogen wurde. Diese Tests wurden dazu entwickelt, die Firewall-Leistungsfähigkeit bei der Filterung ausgehender Daten zu überprüfen. Jeder Satz von Testergebnissen wird von erklärenden Abbildungen und einem kurzen Kommentar in leicht verständlicher, nicht allzu technischer Sprache begleitet.
3. Den Schlussteil des Dokuments bildet ein kurzes Interview mit dem leitenden Software-Entwickler von Agnitum, Alexey Belkin, der über seine Beweggründe dafür spricht, diesen starken Anti-Leak-Schutz in Outpost Firewall Pro 4.0 zu integrieren.

Sicherheit ist ein vielschichtiges Problem

Wir alle haben wertvolle Informationen auf unseren Computern gespeichert, also sollten wir auch unbedingt darüber nachdenken, wie diese Daten zuverlässig geschützt werden können. Im Internet wimmelt es nur so von Schadprogrammen, die dazu entwickelt wurden, persönliche Informationen wie Passwörter, Bankverbindungen und andere vertrauliche Daten ohne Wissen des Besitzers zu stehlen und diese Informationen nach außen an Hacker und andere Cyberkriminelle zu übermitteln.

Durch die Angreifbarkeit dieser Informationen ist es von entscheidender Bedeutung, dass Computerbenutzer kontrollieren können, welche und wie viele Informationen von ihren Computern nach außen übermittelt werden. Sie sollten ausgehende Verbindungen so überwachen können, dass unzulässige Datenübertragungen nicht möglich sind.

Während Antiviren- und Anti-Spyware-Programme Malware, die aus dem Internet auf einen PC herunter geladen wurde, erkennen und entfernen können, hat eine Firewall ein weiter gefasstes Aufgabengebiet. Firewalls verhindern, dass sich bösartige Programme mit dem Internet

verbinden, indem sie als virtueller Kontrollpunkt für Daten im Transfer dienen und nur die genehmigten Verbindungen zulassen. Selbst wenn ein Virus oder Spyware es bis auf den Computer eines Anwenders geschafft hat, kann eine Firewall verhindern, dass diese Malware vom befallenen Computer aus kommuniziert oder sich weiter ausbreitet. Sowohl Antiviren- als auch Spyware-Programme hängen in einem bestimmten Maß von zeitnahen Aktualisierungen der Signaturen ab, um neue Bedrohungsmuster zu erkennen, so dass die Malware-Entwickler eigentlich immer Richtung und Tempo vorgeben. Die Firewall dient dazu, Computer vor Schäden durch neue Malware-Bedrohungen zu schützen, während die Antiviren- und Spyware-Hersteller an ihren Updates arbeiten.

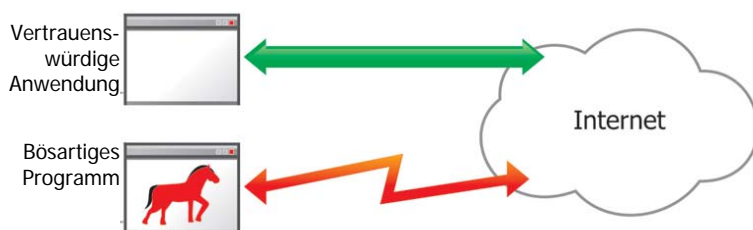
Windows XP bietet einen recht stabilen Schutz, besonders wenn Service Pack 2 installiert ist – das Sicherheits-Upgrade hat dazu beigetragen, das nun viele der Sicherheitslücken geschlossen sind, die vorher von Malware zur Beschädigung des Systems ausgenutzt wurden. Auch die integrierte Firewall wurde verbessert, um neuen Bedrohungen besser entgegenzutreten zu können. Leider reichen diese Verbesserungen jedoch nicht aus, auch die Sicherheitslücken im Betriebssystem selbst zu schließen.

Zunächst einmal fehlt der Windows-XP-Firewall der Schutz für ausgehende Verbindungen – jeder ausgehende Datentransfer wird standardmäßig als sicher und zugelassen eingestuft. Dass das nicht immer unbedingt eine sichere Annahme ist, zeigt der neueste Anstieg von Spyware, Backdoor-Programmen, Botnet-Aktivitäten und anderen Bedrohungen für die Sicherheit der Informationen, die auf Windows-XP-Systemen gespeichert sind.

Zum zweiten ist Windows XP so entwickelt und aufgebaut, dass es einem auf dem Computer installierten Programm uneingeschränkt erlaubt, zu kommunizieren, Daten auszutauschen und interne Komponenten mit anderen Programmen zu teilen und dabei völlige Zulässigkeit voraussetzt. So wird zum Beispiel durch Anklicken eines Hyperlinks in einer E-Mail der Standard-Browser gestartet und der angegebene Link geöffnet; dies geschieht automatisch, ohne die Notwendigkeit, manuell den Browser zu öffnen und die URL einzugeben. Das erleichtert natürlich die Arbeit, gleichzeitig verringert es jedoch auch die Systemsicherheit – ein Malware-Programm kann auf die gleiche Weise ohne irgendwelche Rückfragen eine zulässige Anwendung öffnen und ausführen. Viele Firewalls von Drittanbietern, ebenso wie die in Windows XP enthaltene Firewall, können solch ein verstecktes Verhalten nicht erkennen und erlauben es Schadprogrammen, die Internetverbindung des Computers zu benutzen.

Unten sehen Sie drei Szenarien, die das Schutzlevel eines Computers mit unterschiedlichen Firewall-Konfigurationen zeigen:

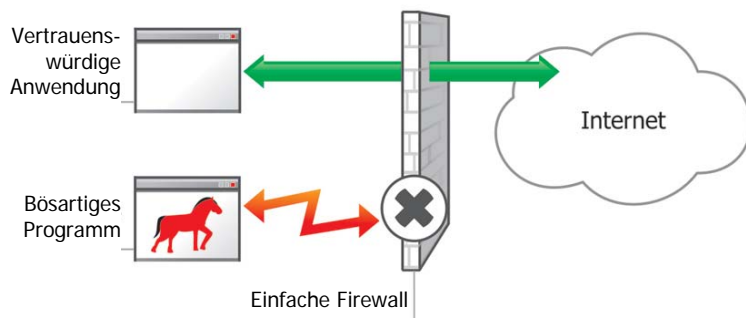
1. Keine Firewall



Zugriff auf Netzwerk und Internet werden ohne Einschränkung erlaubt. Sowohl zulässige Daten (grüne Pfeile) als auch unzulässige Daten (rote Pfeile) dürfen ungehindert in und aus dem Computer gelangen. Die Verbindungen des Computers (Ports) sind jeder Art von ein- und ausgehenden Zugriffen ausgesetzt.

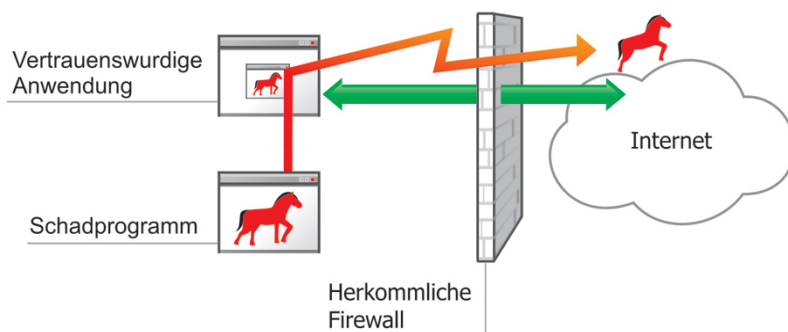
2. Windows XP oder andere einfache Firewall

a) Bösartige Programme können Daten nicht direkt nach außen übermitteln.



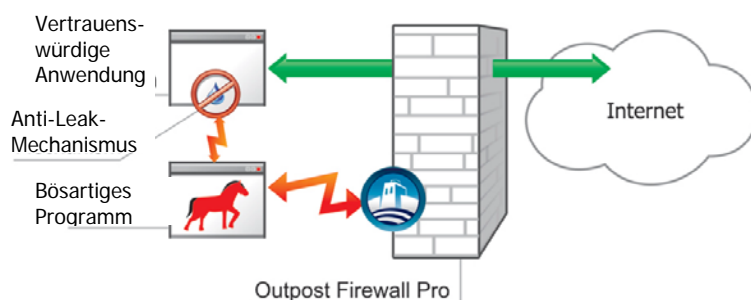
Diese Art von Firewall führt eine einfache und grundlegende Filterung des ausgehenden Datenverkehrs durch; sie würde z.B. Versuche von Schadprogrammen wie Trojanern, unzulässige Informationen nach außen an einen Hacker zu übermitteln, erkennen und verhindern. Sie könnte jedoch nicht erkennen, wenn dasselbe böse Programm eine vertrauenswürdige Anwendung infiltrieren und unter Nutzung deren Zugriffserlaubnis Daten vom Computer versenden würde (siehe auch b) unten).

b) Bösartiges Programm schafft es, durch Hijacking der Zugriffserlaubnis einer vertrauenswürdigen Anwendung Daten zu übertragen



Wenn der direkte Weg durch die Firewall blockiert wird, wird das Schadprogramm als nächstes versuchen, durch Hijacking eine vertrauenswürdige Anwendung zu übernehmen und deren Berechtigungen zu benutzen, um Daten vom Computer herunter zu übertragen und so die Firewall zu manipulieren (engl. "Spoofing").
Gewöhnliche, einfache Firewalls sind nicht in der Lage, unangemessene Kommunikation zwischen Programmen zu erkennen und würden es daher dem bösen Programm erlauben, sich mit der Hacker-Zielseite zu verbinden, was zu einem Sicherheitsrisiko für private Informationen führen würde.

3. Outpost Firewall Pro



Die hochentwickelten Anti-Leak-Kontrollen von Outpost Firewall Pro erkennen und verhindern nicht nur Versuche von Malware-Anwendungen, Daten auf direktem Wege vom Computer zu übertragen. Outpost Firewall Pro v4.0 überwacht auch die Aktivitäten zwischen einzelnen Programmen und stellt so sicher, dass Malware nicht die Berechtigungen zulässiger Anwendungen benutzen kann, um Daten vom PC nach außen zu übertragen.

Kombiniert bieten diese beiden Funktionen einen vielschichtigen Schutz gegen böswillige Datenlecks von privaten Informationen.

Im weiteren Verlauf dieses Dokuments erhalten Sie Informationen über die Arten von Techniken, die Hacker benutzen, um Daten an der Ausgangsverteidigung der Firewall vorbeizuschleusen und darüber, wie Outpost 4.0 die Anwender gegen jede einzelne von ihnen schützt.

Tools zur Überprüfung der Firewall-Wachsamkeit

Wie bereits erwähnt, sollten Firewalls in der Lage sein, Programme auf nach außen gehende Aktivitäten hin zu überprüfen. Selbst wenn ein Programm versucht, sich als andere Anwendung auszugeben, die bei der Firewall als "vertrauenswürdig" vorkonfiguriert ist, sollte eine leistungsfähige Firewall ein solches Anwendungs-Hijacking erkennen und verhindern können, dass auf diese Art Daten vom PC nach außen übertragen werden.

Die Informationssicherheits-Branche hat spezielle Tools entwickelt, um die Leistungsfähigkeit der Firewalls zu testen, unzulässige Programm-Interaktivität zu erkennen und Malware-Programme davon abzuhalten, sich mit der ID zulässiger Programme mit dem Netzwerk zu verbinden. Diese Software-Tools, "Leak-Tests" genannt, ahmen den Versuch von Malware nach, Daten von einem PC nach außen zu schicken. So können die Anwender sehen, wie ihre Firewall auf eine solche Bedrohung reagieren könnte.

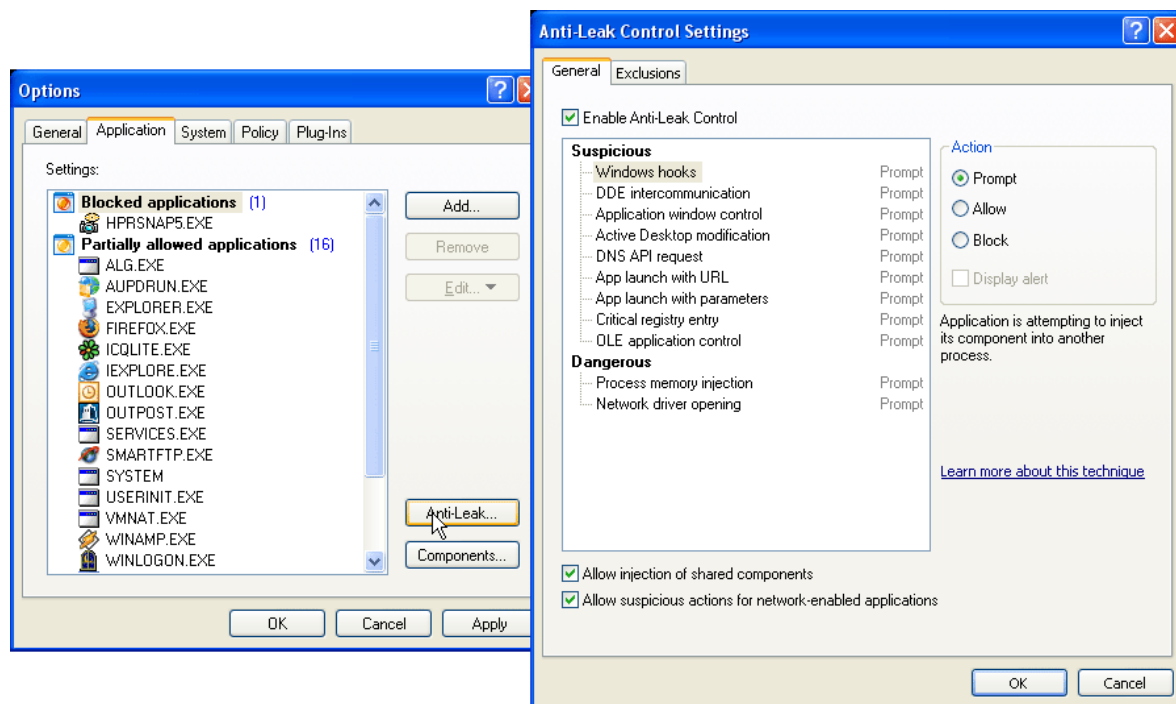
Leak-Tests arbeiten mit einer ganzen Reihe von Techniken und Mechanismen, um die Fähigkeit einer Firewall zu testen, unbefugte, ausgehende Datenübertragungen zu verhindern. Es handelt sich um legitime Hilfsprogramme, die nur die vom Anwender erlaubten Informationen an isolierte Test-Zielorte senden und die das System nicht beschädigen können.

Einige Leute sind der Meinung, dass Leak-Tests keine realen Praxis-Situationen darstellen und daher nur Labor-Beispiele zum Machbarkeitsbeweis („Proof of Concept“) seien. Da die verwendeten Techniken jedoch von tatsächlich existierenden Malware-Programmen eingesetzt werden können und auch schon eingesetzt wurden, dienen sie als wertvoller Indikator für die tatsächliche Leistungsfähigkeit einer Firewall im Umgang mit ausgehenden Angriffen.

Neue Datenschutz-Funktion in Outpost Firewall Pro 4.0

Outpost 4.0 bietet eine Reihe von Verbesserungen, die dazu entwickelt wurden, Datendiebstahl ein für allemal zu verhindern, unter anderem auch zwölf neuen Anti-Leak-Funktionen.

Im Outpost-Fenster **Optionen** wurde auf der Registerkarte **Anwendungen** eine neue Schaltfläche "Anti-Leak" hinzugefügt, mit der Sie das Level des Schutzes vor unzulässigen ausgehenden Anwendungsaktionen anpassen können.



Später werden Sie im Zusammenhang mit unterschiedlichen Leak-Tests sehen, wie diese neuen Funktionen dazu beitragen, Ihnen auf Ihrem PC den unerlässlichen, vielschichtigen Schutz von Outpost zu bieten.

Ein Überblick zum Thema Leak-Tests

Auf den Websites [Firewall Leak Tester](#) und [PC Flank](#) finden Sie eine Fülle an Informationen über Leak-Tests. Die Zahl von Leak-Tests steigt ständig an, genau wie ihre Fähigkeiten und technische Ausgereiftheit bei der Anwendung neuer Techniken zur Umgehung der Firewall. Firewall-Softwareentwickler wie Agnitum überprüfen ihre Produkte ständig mit Hilfe der neuesten Leak-Tests, ungefähr so wie die Handhabung und Leistung eines neuen Automodells auf einer Rennstrecke überprüft wird, bevor der Wagen auf den Markt kommt.

Obwohl es noch keine 100-prozentige Garantie für die Undurchlässigkeit Ihrer Firewall bedeutet, wenn sie alle aktuellen Leak-Tests besteht (für Sicherheit gibt es keine Garantie), ist es doch ein gutes Zeichen, dass sie auch entschlossenen Versuchen, Ihre Daten zu stehlen, Widerstand leisten kann. Wie Sie auf den oben erwähnten Websites sehen können, hat es noch keine einzige Firewall geschafft, alle Leak-Tests zu bestehen, die es gibt – bis jetzt. Outpost Firewall Pro v4.0 besteht ohne Probleme jeden einzelnen Test – ein schlagkräftiger Beweis für seine Fähigkeit, Hacker im Zaum zu halten.

Lassen Sie uns jedoch zunächst betrachten, auf welche Arten Hacker versuchen könnten, Informationen von Ihrem PC zu stehlen.

Arten von Informationslecks

Da Leak-Tests auf unterschiedlichen Techniken (oder Kombinationen mehrerer Techniken) beruhen, Informationen unter Umgehung der Firewall-Abwehr nach außen zu bringen, bietet dieser Abschnitt eine Übersicht über die derzeit bekannten Techniken und berichtet dann über Einzelheiten jedes Leak-Tests, auch darüber, wie Outpost in jedem einzelnen Fall die vorgetäuschten Angriffe erkennt und erwidert.

Leak-Technik Nr. 1 "Dateinamen-Ersetzung"

Dieser Ansatz ist der am einfachsten zu bekämpfende ausgehende Angriff. Er besteht aus einem Programm, das sich selbst umbenennt, um denselben Namen wie ein zulässiges Programm zu haben, und das dann auf das Internet zugreift, während es vorgibt, ein genehmigtes Programm zu sein.

Leak-Technik Nr. 2 "Start einer Anwendung per URL"

Programme, die diese Technik benutzen, öffnen ein separates Programm mit Internetzugriff (normalerweise einen Browser) mit der URL der Website, auf die sie programmiert sind. Der Prozess kann in einem versteckten Fenster stattfinden, um die Aktivität vor dem Anwender zu verbergen.

Leak-Technik Nr. 3 "Manipulation durch Erlaubnisregeln"

Eine selten angewandte, aber wirkungsvolle Technik, mit der ein Programm die Art ausnutzt, wie die Firewall Zugriffsregeln innerhalb des Systems verarbeitet. Dazu versucht der Test auf Ports zuzugreifen, die die Firewall als vertrauenswürdig eingestuft hat und durch sie unzulässigen Datenverkehr zu übertragen.

Leak-Technik Nr. 4 "Vorgetäuschte DNS-Anfrage"

Die DNS-Adressauflösung wird dazu benutzt, eine internetfähige Anwendung zu einer entsprechenden numerischen IP-Adresse zu leiten, die sich auf den Ziel-Remoteserver bezieht. Sie wandelt eine vom Benutzer bereitgestellte Hostnamen-Adresse (z.B. www.agnitum.com) in eine IP-Adresse um, so dass der Computer den Befehl verstehen und auf die angeforderte Website (z.B. 67.15.103.130) zugreifen kann. Die Technik der vorgetäuschten DNS-Anfrage bedeutet, dass empfindliche Daten unter dem Deckmantel einer normalen DNS-Anfrage an einen durch Hijacking übernommenen oder illegalen DNS-Server weitergegeben werden.

Leak-Technik Nr. 5 "Injektion von Komponenten"

Diese Technik wird angewandt, wenn ein Malware-Programm eine andere Anwendung auf einem Computer öffnet und seine internen Komponenten oder eine DLL-Datei in den Zielprozess injiziert. Die injizierte Komponente fordert die übernommene Anwendung dann zum Zugriff auf das Netzwerk auf und versucht so, die Firewall zu täuschen.

Leak-Technik Nr. 6 "Injektion von Prozessen"

Ähnlich wie die Injektion einer Komponente in ein vertrauenswürdiges Programm kann eine Malware-Anwendung ihren gesamten Inhalt in den Datenspeicher-Block einer vertrauenswürdigen Anwendung injizieren, so dass eine neue Instanz des Ursprungsprozesses geöffnet wird und mit der Berechtigung des vertrauenswürdigen Programms auf das Netzwerk zugreift.

Leak-Technik Nr. 7 "DDE-Interkommunikation"

Diese Technik wird von einem Programm angewandt, um Befehle an ein anderes (üblicherweise an einen Browser) zu schicken, damit dieses sie ausführt. Mit einem DDE-Auftrag können

Programme Inhalte verwalten und miteinander teilen. Die DDE-Technik der Anwendungskontrolle wird in einem Leak-Test dazu benutzt, zu überprüfen, ob die Firewall erkennt, wenn ein Programm die DDE-Interaktion zur Kontrolle der Aktivität einer internetfähigen Anwendung benutzt.

Leak-Technik Nr. 8 "Einsatz der OLE-Funktion zur Kontrolle von Anwendungen"

Dieser relativ neue Ansatz setzt die Technik der Inter-Programm-Kontrolle OLE (eine Abkürzung für den Datenaustausch-Standard Object Linking and Embedding) in Leak-Tests ein. OLE ist ein Windows-Mechanismus, der es einem Programm ermöglicht, die Aktionen eines anderen Programms zu steuern.

Leak-Technik Nr. 9 "Kontrolle von Anwendungsfenstern durch Windows-Nachrichten"

Eine Anwendung kann den Inhalt und die Befehle anderer Fenster durch Windows-Nachrichten kontrollieren. Einige Leak-Tests benutzen diese Technik, um die Aktivität internetfähiger Anwendungen zu kontrollieren und über sie auf das Netzwerk zuzugreifen.

Leak-Technik Nr. 10 "Direkter Zugriff auf die Netzwerkschnittstelle"

Wenn das Prinzip des Direktzugriffs auf die Netzwerkschnittstelle angewandt wird, erstellt der Test eine zusätzliche Netzwerkebene, indem er einen entsprechenden Gerätetreiber in das System injiziert und durch diese Ebene Datenverkehr sendet/empfängt. So werden die von der Firewall überwachten Standard-Kommunikationskanäle umgangen. Diese Technik ermöglicht es dem Leak-Test (oder jeder anderen Anwendung), Daten zu senden und zu empfangen, was den Prozess der Datenfilterung durch die Firewall erschwert. In einer Windows-XP-Umgebung ist das eine ziemlich komplexe Aufgabe, da es dem Testprogrammierer einiges an Fähigkeiten abverlangt, die Systemkonfiguration zu manipulieren. Man kann mit diesem Test jedoch sehr gut die Widerstandsfähigkeit und Flexibilität einer Firewall überprüfen.

Leak-Technik Nr. 11 "Zugriff durch Veränderung des Windows Active Desktop"

Leak-Tests können eine HTML-Seite erstellen, die auf eine bestimmte Website verweist und sie als Windows Active Desktop (AD) einrichten. Wenn der Active Desktop aktiviert ist, ist es erlaubt, die in der HTML-Seite enthaltene Website-Adresse zu besuchen. Das geschieht im Namen des Systems, so dass die Sensoren der Firewall umgangen werden.

Leak-Technik Nr. 12 "Veränderung der System-Registrierungsdatenbank"

Die Registrierungsdatenbank (Registry) ist der allgemeine Speicherort für Systemeinstellungen und Programmkonfigurationen. Die Veränderung ihres Inhalts kann zu Programmfehlern oder sogar zum Systemabsturz führen. Leak-Tests, die mit dieser Technik arbeiten, nehmen kleine Änderungen an Registry-Elementen vor und ermöglichen so einem nicht überprüften Programm trotz vorhandener Firewall einen uneingeschränkten Zugriff auf das Netzwerk, indem sie ihre Komponenten zu den registrierten Anwendungen hinzufügen und in deren Namen agieren.

Nun ist es Zeit für die Leak-Tests selbst

Nun werden wir alle Leak-Tests unter die Lupe nehmen, einen nach dem anderen, und untersuchen, wie Outpost Firewall Pro 4.0 auf sie reagiert. Die Leak-Tests sind nach den angewandten Techniken sortiert, und das Ergebnis jedes Tests wird kurz kommentiert.

Zur Zeit gibt es achtzehn Leak-Tests und wir haben Outpost jedem einzelnen von ihnen unterzogen. Fangen wir an.

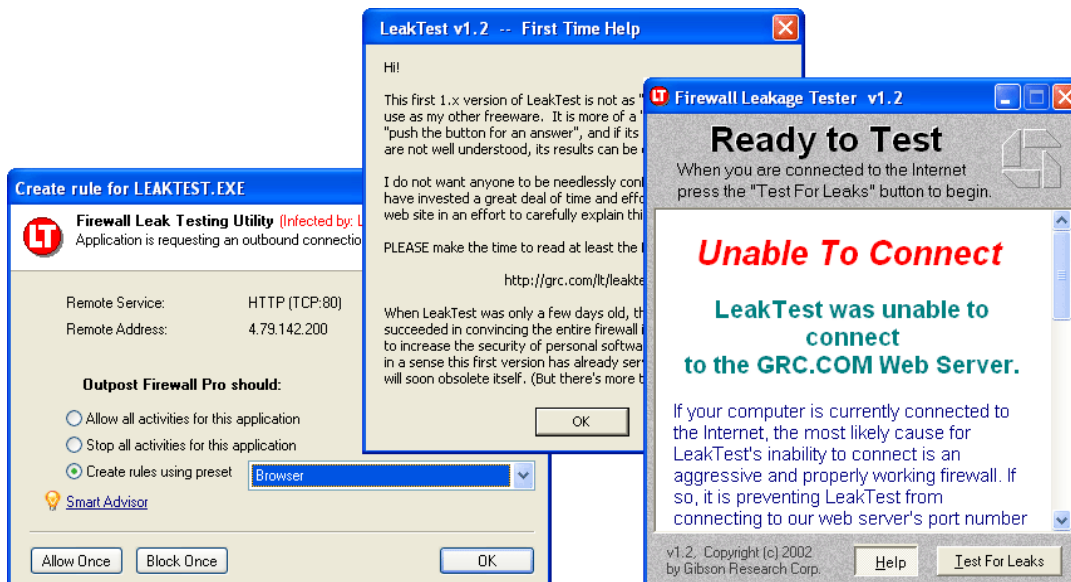
Leak-Test Nr. 1 "Firewall Leakage Tester"

Name/Link zum Sofort-Download	Eingesetzte Umgehungstechnik	Leak-Test-Info/Homepage	Angewandte Outpost-Funktion
Firewall Leakage Tester (Leak Test)	Dateinamen-Ersetzung	 LeakTest.exe Firewall Leak Testing Utility Gibson Research Corp.	Überprüfung des Fingerabdrucks

Hier handelt es sich um einen leicht zu bestehenden Leak-Test, die die Technik der **Dateinamen-Ersetzung** benutzt, um die Firewall zu testen.

Der Test versucht sich selbst in eines der zugelassenen Programme auf einem Computer umzubenennen (z.B. Internet Explorer) und unter dem Deckmantel dieses Namens eine ausgehende Verbindung mit einem Remote-Server herzustellen. Dieser Test würde Firewalls ausschalten, die sich ausschließlich auf den Dateinamen verlassen, um eine Anwendung zu identifizieren und keine gründlichere Auswertung (z.B. Überprüfung des Fingerabdrucks) durchführen. Obwohl es ein relativ leichter Test ist, bestehen ihn nicht alle Firewalls.

Hier sehen Sie, wie Outpost reagiert:





Outlook überprüft über den Namen eines Programms hinaus auch seine einzigartigen Identifizierungszeichen oder Fingerabdrücke. SHA256 wird benutzt, um Anwendungen durch aktualisierte Standardwerte zu identifizieren, und die MD5-Identifizierung wird eingesetzt, um in aktiven Programm-Regelsätzen Anwendungen zu identifizieren und so die getarnten Programme von der Verbindung abzuhalten.

Das bedeutet für den Anwender, dass jede bösartige oder unerwünschte Anwendung, die versucht, sich als zulässige Anwendung auszugeben und so einen Zugriff nach außen herzustellen, von Outpost entdeckt wird und der Benutzer aufgefordert wird, die Verbindung zuzulassen oder abzulehnen.

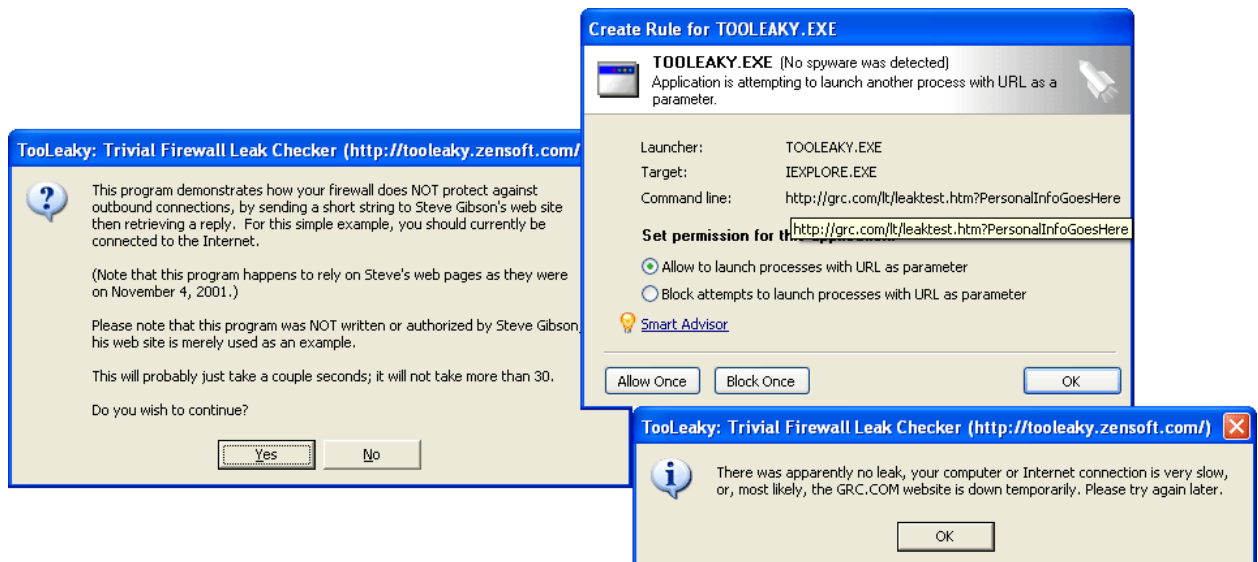
BESTANDEN

Leak-Test Nr. 2 "TooLeaky"

Name/Link zum Sofort-Download	Eingesetzte Umgehungstechnik	Leak-Test-Info / Homepage	Angewandte Outpost-Funktion
TooLeaky	Programmstart per URL	 tooleaky.exe	"Programmstart per URL" 

Dieser Leak-Test ist eine etwas höher entwickelte Version des vorherigen Tests, da er mit einer vorkonfigurierten Web-Adresse den Standard-Internetbrowser in einem versteckten Fenster öffnet und so versucht, der Firewall vorzutäuschen, dass eine zulässige Aktion stattfindet. Firewalls, die einer Anwendung standardmäßig vertrauen, ohne darüber hinaus zu überprüfen, wer sie tatsächlich gestartet hat und welche zusätzlichen Verbindungsparameter bereitgestellt werden, würden diesen Test nicht bestehen.

Hier sehen Sie, wie Outpost reagiert:



The screenshot shows three overlapping windows:



- TooLeaky: Trivial Firewall Leak Checker (http://tooleaky.zensoft.com/)**: A window with a question mark icon and text explaining the program's purpose: "This program demonstrates how your firewall does NOT protect against outbound connections, by sending a short string to Steve Gibson's web site then retrieving a reply. For this simple example, you should currently be connected to the Internet." It includes a "Do you wish to continue?" prompt with "Yes" and "No" buttons.
- Create Rule for TOOLEAKY.EXE**: A dialog box from Outpost Firewall Pro. It shows:
 - Launcher: TOOLEAKY.EXE (No spyware was detected)
 - Target: IEXPLORE.EXE
 - Command line: http://grc.com/lt/leaktest.htm?PersonalInfoGoesHere
 - Set permission for this rule: Allow to launch processes with URL as parameter
 - Buttons: "Allow Once", "Block Once", and "OK".
- TooLeaky: Trivial Firewall Leak Checker (http://tooleaky.zensoft.com/)**: A smaller window with an information icon and text: "There was apparently no leak, your computer or Internet connection is very slow, or, most likely, the GRC.COM website is down temporarily. Please try again later." with an "OK" button.

Outposts Anti-Leak-Funktion "Programmstart per URL" erkennt den Versuch, ein Programm mit einer Ziel-URL zu starten und wird den Anwender zur Eingabe auffordern, ob eine solche Aktion für ein bestimmtes Programm zugelassen werden soll.

Das bedeutet für den Anwender, dass Outpost jedes Programm, das auf einem Computer geöffnet wird, beobachtet und die Genehmigungen zum Öffnen von Programmen mit Internetzugriff kontrolliert, ungeachtet der Tatsache, ob die Programmanforderung zulässig ist.

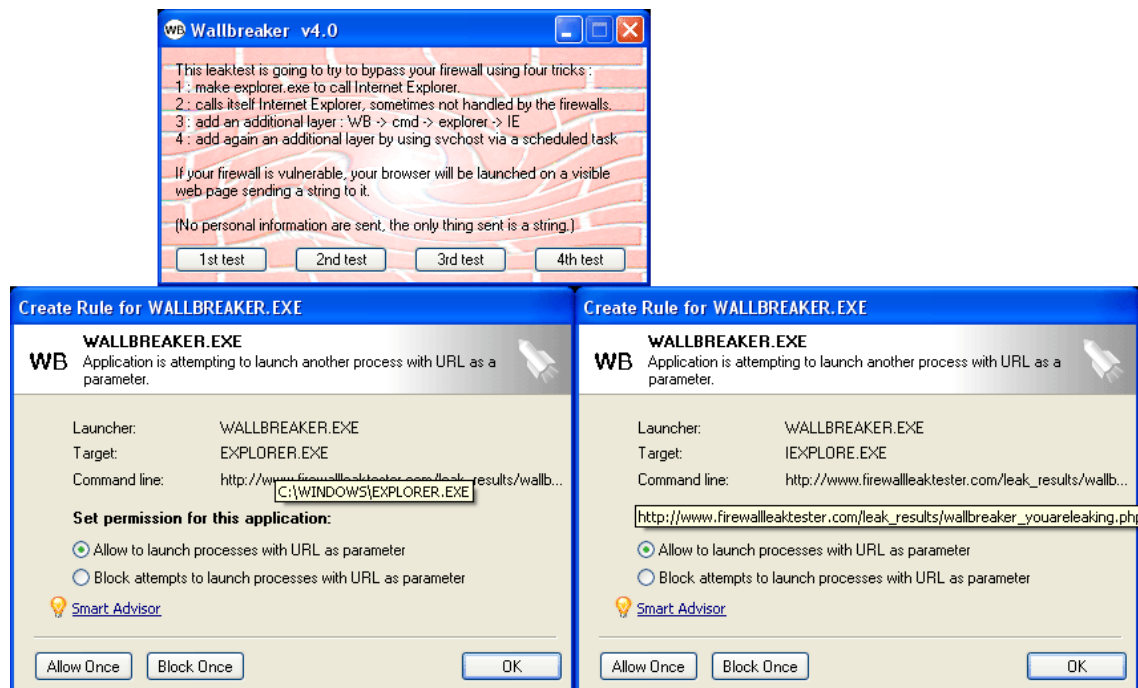
BESTANDEN

Leak-Test Nr. 3 "WallBreaker"

Name/Link zum Sofort-Download	Eingesetzte Umgehungstechnik	Leak-Test-Info / Homepage	Angewandte Outpost-Funktion
WallBreaker	Programmstart per URL	 WallBreaker.exe	"Programmstart per URL" 

WallBreaker besteht aus mehreren Tests, die eine Reihe von unterschiedlichen Techniken verwenden, um die Stärke einer Firewall nach außen hin zu überprüfen. Der Test versucht, eine Programmstartsequenz zu verbergen und die Identität der Ursprungsanwendung in einer Kette von Programmstart-Ereignissen zu verstecken. Das Ziel ist es, die Firewall mit Befehlen zum Programmaufruf auf mehreren Ebenen zu verwirren, so dass sie nicht mehr nachvollziehen kann, wer tatsächlich ein vertrauenswürdige Programm gestartet hat. Außerdem startet er in einem versteckten Fenster ein vertrauenswürdige Programm mit einem vordefinierten Befehl in der Adresszeile.

Hier sehen Sie, wie Outpost reagiert:





The image shows three screenshots related to the WallBreaker test and Outpost Firewall Pro's response:

- Top Screenshot:** A window titled "WB Wallbreaker v4.0" with a red brick background. It lists four tricks to bypass a firewall:
 - 1: make explorer.exe to call Internet Explorer.
 - 2: calls itself Internet Explorer, sometimes not handled by the firewalls.
 - 3: add an additional layer: WB -> cmd -> explorer -> IE
 - 4: add again an additional layer by using svchost via a scheduled task
 It also states: "If your firewall is vulnerable, your browser will be launched on a visible web page sending a string to it." and "(No personal information are sent, the only thing sent is a string.)". There are buttons for "1st test", "2nd test", "3rd test", and "4th test".
- Bottom Left Screenshot:** A dialog box titled "Create Rule for WALLBREAKER.EXE". It shows the application is attempting to launch another process with URL as a parameter.
 - Launcher: WALLBREAKER.EXE
 - Target: EXPLORER.EXE
 - Command line: http://www.firewallleaktester.com/leak_results/wallb... C:\WINDOWS\EXPLORER.EXE
 - Set permission for this application:
 - Allow to launch processes with URL as parameter
 - Block attempts to launch processes with URL as parameter
 - Buttons: Allow Once, Block Once, OK
- Bottom Right Screenshot:** A dialog box titled "Create Rule for WALLBREAKER.EXE". It shows the application is attempting to launch another process with URL as a parameter.
 - Launcher: WALLBREAKER.EXE
 - Target: IEXPLORE.EXE
 - Command line: http://www.firewallleaktester.com/leak_results/wallb... http://www.firewallleaktester.com/leak_results/wallbreaker_youareleaking.ph...
 - Set permission for this application:
 - Allow to launch processes with URL as parameter
 - Block attempts to launch processes with URL as parameter
 - Buttons: Allow Once, Block Once, OK

Outpost Firewall Pro entdeckt alle Versuche der WallBreaker-Tests, die Firewall zu täuschen mit Leichtigkeit und schützt den Computer wirkungsvoll gegen diese Arten von Programmstart-Techniken.

BESTANDEN

Leak-Test Nr. 4 "Ghost"

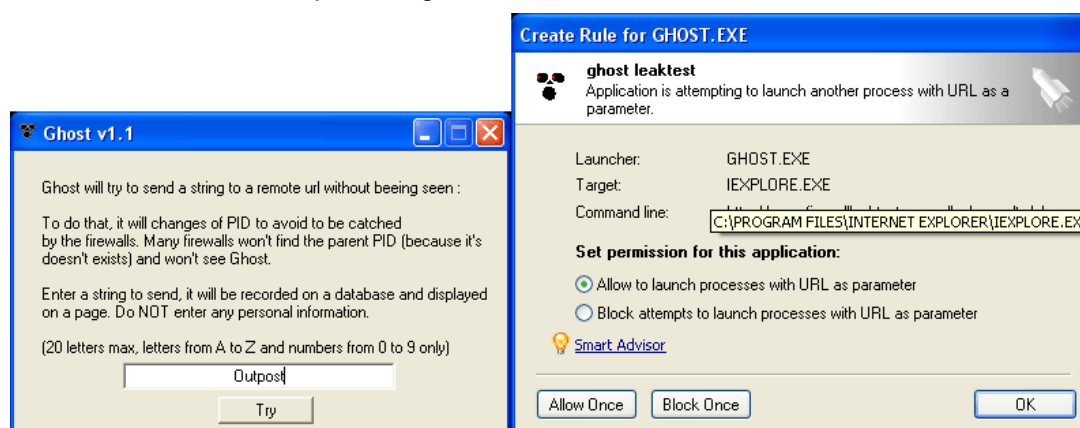
Name/Link zum Sofort-Download	Eingesetzte Umgehungstechnik	Leak-Test-Info / Homepage	Angewandte Outpost-Funktion
Ghost	Programmstart per URL	 Ghost.exe ghost leaktest gkweb	"Programmstart per URL" 

Der Leak-Test Ghost benutzt die Programmstart-Techniken im Zusammenhang mit URL-Adressen und Prozess-Identifizierungszeichen (PID)-Manipulation.

Die PID ist ein einzigartiges Identifizierungszeichen, das jedem in einem Windows-Computer geöffneten Prozess oder Programm zugewiesen und vom System verwendet wird, um aktive, ausgeführte Tasks zu erkennen.

Der Leak-Test Ghost ändert seine PID ständig, in dem er sich selbst mehrmals schnell hintereinander öffnet und schließt. Das Ziel ist es, die Firewall mit verschiedenen PID-Nummern für dieselbe Anwendung zu verwirren, damit sie den Ursprungsprozess nicht erkennen kann.

Hier sehen Sie, wie Outpost reagiert:



Das bedeutet für den Anwender, dass Outpost erkennen kann, wenn eine Anwendung versucht, ihre PID-Nummer zu ändern und die Firewall zu verwirren. Outpost wird den Anwender einfach fragen, ob es in Ordnung ist, einer ständig ihre Identität ändernden Anwendung den Zugriff auf das Internet zu erlauben, sei es direkt oder durch ein externes, internetfähiges Programm.

BESTANDEN

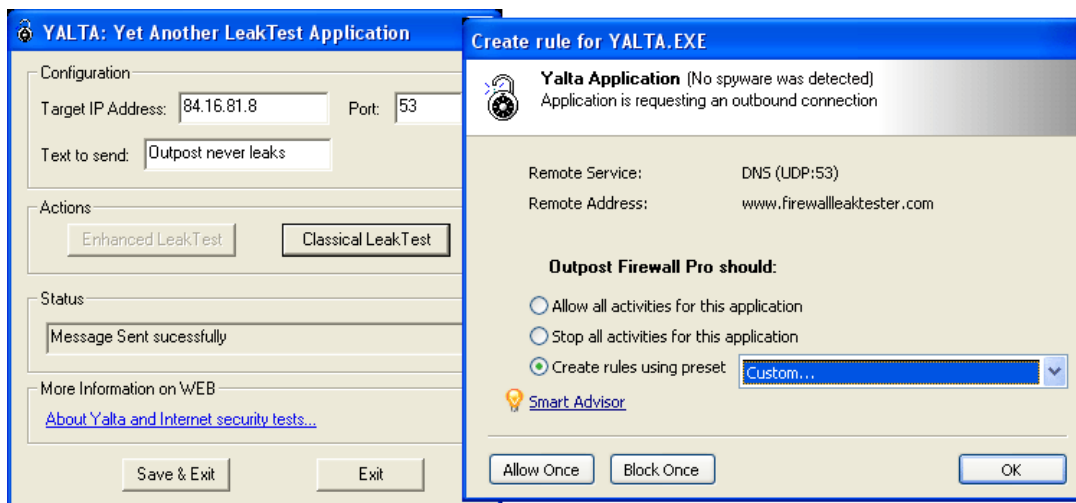
Leak-Test Nr. 5 "YALTA"

Name/Link zum Sofort-Download	Eingesetzte Umgehungstechnik	Leak-Test-Info/Homepage	Angewandte Outpost-Funktion
YALTA (Yet Another Leak Test Anwendung)	Manipulation durch Erlaubnisregeln	 Yalta.exe Yalta Application Soft4Ever	Globale Regeln & Zugriff pro Anwendung

Yalta ist ein sehr ausgeklügelter Test – er überprüft, ob die Firewall eine anscheinend zulässige Verbindungsaktivität erkennen kann, die von einem unzulässigen Programm gestartet wurde. Dazu versucht er, mit einem üblichen UDP-Zugriffsprotokoll über Port 21 (normalerweise für FTP-Verkehr benutzt) Daten zu übertragen, um die Firewall glauben zu lassen, dass die Daten zulässigerweise übertragen werden. Es gibt außerdem einen weitergehenden Test (für Windows-XP-Systeme nicht verfügbar), der einen neuen Netzwerktreiber erstellt und versucht, durch ihn Daten zu übertragen, wobei der übliche, von einer Firewall überwachte TCP/IP-Stack umgangen wird.

Firewalls, die den Urheber einer genehmigten Verbindung nicht identifizieren, sondern nur überprüfen, ob die vom Programm durchgeführte Aktivität einem allgemeinen Muster akzeptabler Handlungen entspricht, werden diesen Test nicht bestehen.



Hier sehen Sie, wie Outpost reagiert:



Die oben abgebildeten Screenshots zeigen, dass Outpost die Genehmigungen einer Anwendung überprüft, bevor sie eine allgemein erlaubte Aktion durchführen darf und den Anwender benachrichtigt, wenn ein verdächtiges Verhalten bemerkt wird.

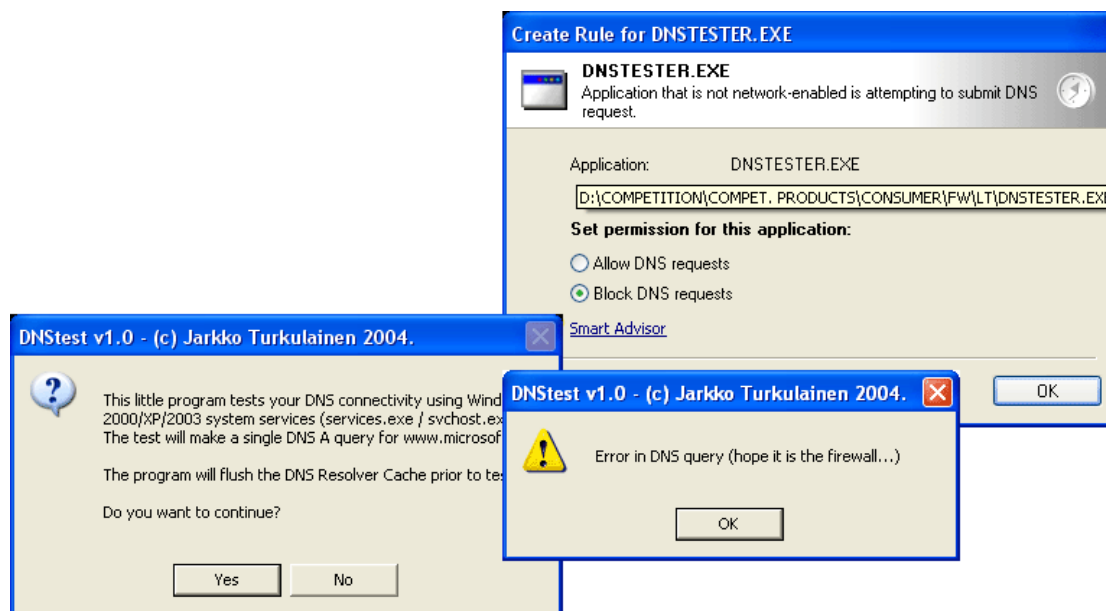
BESTANDEN

Leak-Test Nr. 6 "DNSTester"

Name/Link zum Sofort-Download	Eingesetzte Umgehungstechnik	Leak-Test-Info/Homepage	Angewandte Outpost-Funktion
DNSTester	Vorgetäuschte DNS-Anfrage	 dnstester.exe	"DNS-API-Anfrage" 

Der DNSTester benutzt rekursive DNS-Anfragen und versucht damit, von der Firewall unentdeckt Daten zu senden. Dadurch, dass auf diese Weise eine DNS-Anfrage vorgetauscht wird, ahmt DNSTester den Ansatz nach, mit dem böstige Programme durch unzulässige Anfragen an den DNS Client Service (svchost.exe) empfindliche Daten aus dem Computer herausziehen. Die Rolle des DNS Client Service ist es, die aufgelösten DNS-Adressen, die vom DNS-Server bereitgestellt wurden, abzurufen, so dass Anwendungsprogramme schnell den richtigen Remote-Host im Internet finden können.



Hier sehen Sie, wie Outpost reagiert:



Outpost überprüft die Genehmigungen einer Anwendung, die auf den DNS Client Service zuzugreifen und fordert den Anwender zu einer Entscheidung auf, wenn eine nicht übereinstimmende Anfrage entdeckt wird, so dass die Anwender gegen einen Missbrauch des DNS-Service geschützt sind.

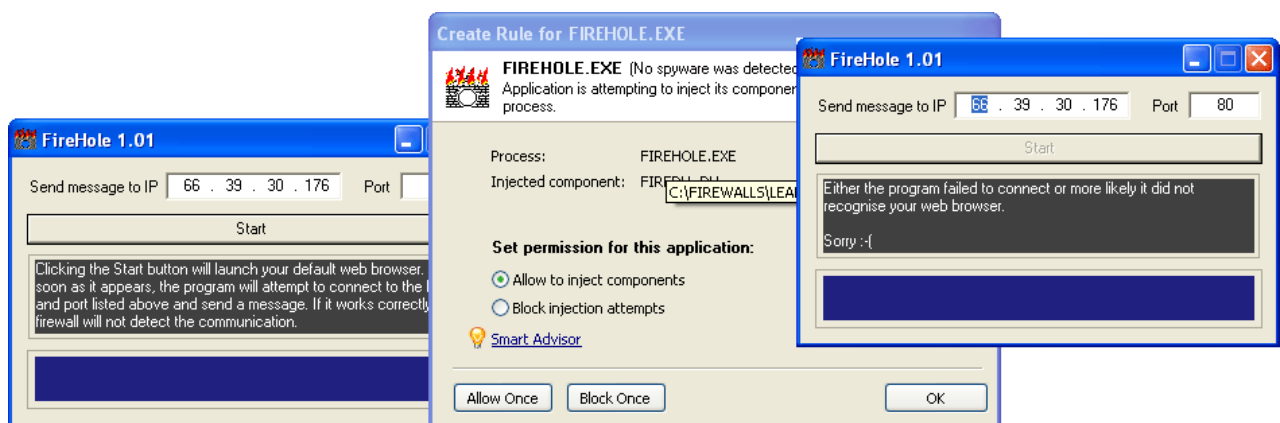
BESTANDEN

Leak-Test Nr. 7 "FireHole"

Name/Link zum Sofort-Download	Eingesetzte Umgehungstechnik	Leak-Test-Info / Homepage	Angewandte Outpost-Funktion
FireHole	Injektion von Komponenten	 firehole.exe	"Windows Hooks" 

Dieser Leak-Test öffnet den Standard-Browser und injiziert eine kleine Datei – eine ausführbare Datei mit einer DLL-Endung (auch als "Komponente" der Hauptanwendung bekannt) – in den Browser. Diese Datei veranlasst den Browser dazu, eine Verbindung zu einem bösartigen Remote-Server herzustellen. Diese Technik ist als "Komponenteninjektion" bekannt und wird von Firewalls, die die internen Module einer Anwendung und deren Verbindungsziele nicht überwachen, nicht erkannt.



Hier sehen Sie, wie Outpost reagiert:



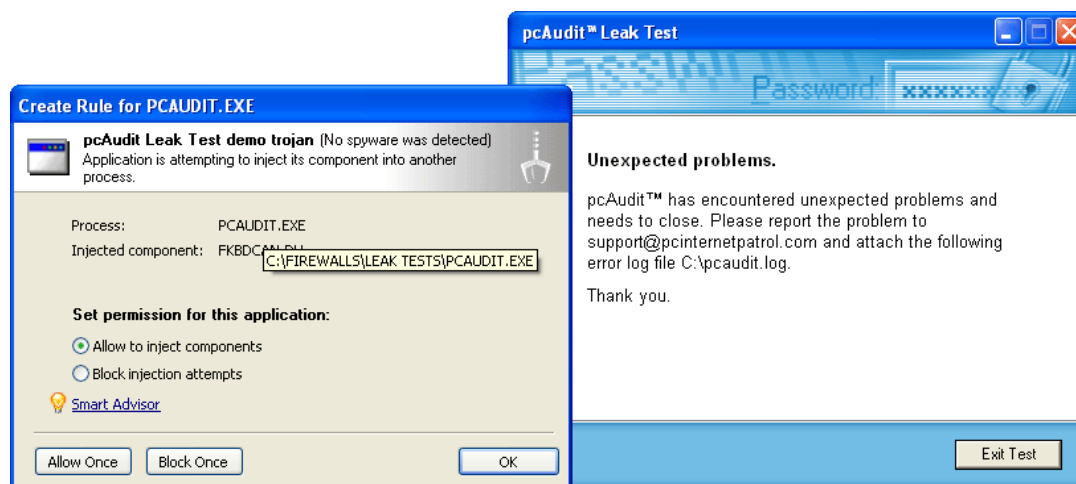
Wenn Outpost entdeckt, dass eine Anwendung versucht, einen Code in einen anderen Prozess zu injizieren und durch diesen auf das Netzwerk zuzugreifen, wird der Anwender benachrichtigt und zu einer Entscheidung aufgefordert, ob dieser Prozess zugelassen werden soll.

BESTANDEN

Leak-Test Nr. 8 "pcAudit"

Name/Link zum Sofort-Download	Eingesetzte Umgehungstechnik	Leak-Test-Info / Homepage	Angewandte Outpost-Funktion
pcAudit	Injektion von Komponenten	 pcaudit.exe pcAudit Leak Test demo trojan Internet Security Alliance, LLC	"Windows Hooks" 



Der Leak-Test pcAudit arbeitet nach demselben Prinzip wie das auf der vorigen Seite beschriebene Programm FireHole – es injiziert eine Komponente in den Datenspeicherplatz eines vertrauenswürdigen Programms. PcAudit zeigt eine sehr informative, wirkungsvolle und leicht zu verstehende Ergebnisseite an, wenn der Test mit einem negativen Ergebnis (durchgefallen) endet: Der Desktop des Anwenders wird angezeigt, zusammen mit vor kurzem eingegebenem Text und Schlüsselinformationen über den Host-Computer. Wenn Outpost läuft, sieht das Ergebnis sogar noch einfacher aus:



Das bedeutet, dass Outpost erfolgreich verhindert hat, dass der Leak-Test pcAudit Daten vom Computer des Anwenders übermittelt.

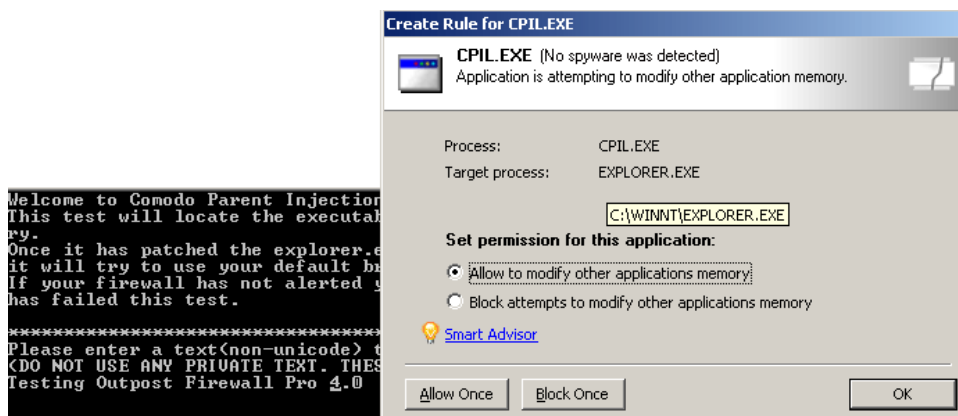
BESTANDEN

Leak-Test Nr. 9 "Comodo Parent Injection Leak Test"

Name/Link zum Sofort-Download	Eingesetzte Umgehungstechnik	Leak-Test-Info / Homepage	Angewandte Outpost-Funktion
Comodo Parent Injection Leak Test (CPIL)	Prozess-Injektion	 cpil.exe	"Prozess-Speicher-Injektion" 

Der Leak-Test Comodo ist ein neues Programm, das die Technik der Injektion von Komponenten in den Windows Explorer (explore.exe) verwendet, um im Namen des Explorers auf das Netzwerk zuzugreifen. Der Test funktioniert nur unter dem Betriebssystem Windows 2000 und ist nicht mit Windows XP SP2 kompatibel.



Hier sehen Sie, wie Outpost reagiert:



Outpost-Anwender, die mit Windows 2000 arbeiten, können also sicher sein, dass Outpost den Leak-Test Comodo Parent Injection zuverlässig besteht.

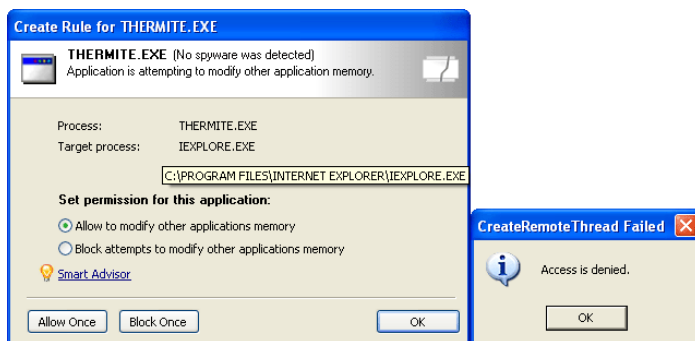
BESTANDEN

Leak-Test Nr. 10 "Thermite"

Name/Link zum Sofort-Download	Eingesetzte Umgehungstechnik	Leak-Test-Info / Homepage	Angewandte Outpost-Funktion
Thermite	Prozess-Injektion	 thermite.exe	„Prozess-Speicher-Injektion“ 

Der Leak-Test Thermite benutzt eine hoch entwickelte Hacker-Technik für den Versuch, den Firewall-Schutz zu umgehen. Er injiziert seinen vollständigen Code direkt in den Datenspeicher eines anderen Prozesses, öffnet so eine neue Instanz des Ursprungsprozesses und benutzt diesen Prozess, um Daten an der Firewall vorbei zu übertragen. Die Voraussetzung dafür ist, dass die Firewall nicht bemerkt, dass ein zugelassenes Programm durch Hijacking von Malware-Code gesteuert wird.



Hier sehen Sie, wie Outpost reagiert:



Durch die Art und Weise, wie Outpost überprüft, wie die Programme auf einem Computer interagieren, kann es erkennen, wenn ein Programm versucht, die Kontrolle über ein anderes Programm zu übernehmen und mit dessen Berechtigung auf das Netzwerk zuzugreifen. In solchen Fällen wird der Benutzer aufgefordert, diese Aktion zuzulassen oder abzulehnen.

BESTANDEN

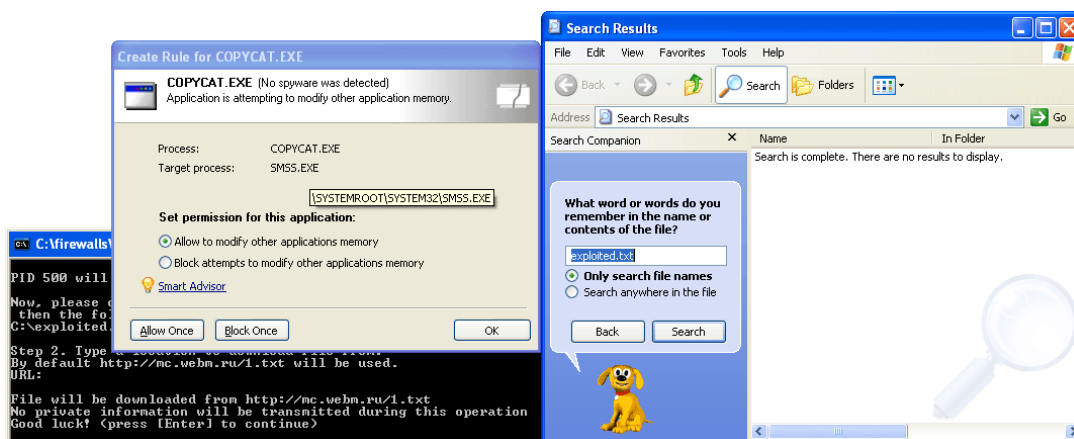
Leak-Test Nr. 11 "Copycat"

Name/Link zum Sofort-Download	Eingesetzte Umgehungstechnik	Leak-Test-Info / Homepage	Angewandte Outpost-Funktion
Copycat	Prozess-Injektion	 copycat.exe	"Prozess-Speicher-Injektion" 

Der Leak-Test Copycat beruht auf demselben Prinzip wie der Test Thermite – direkte Injektion von fremdem Code in den residenten Speicher eines genehmigten Prozesses. Der Unterschied bei diesem Test liegt darin, dass er keine neue Instanz des Ursprungsprozesses öffnet, sondern stattdessen direkt im Namen des fremd gesteuerten Prozesses handelt.

Wenn dieser Test erfolgreich ist, ist Ihre Firewall durch Prozess-Injektion von Hackern angreifbar.



Hier sehen Sie, wie Outpost reagiert:



Outpost verhindert, dass Copycat sich selbst in den Datenspeicherblock eines internen Windows-Programms einspeist und demonstriert damit seine Fähigkeit, lokale Programme und Prozess-Interaktionen auf dem System des Anwenders zu überwachen.

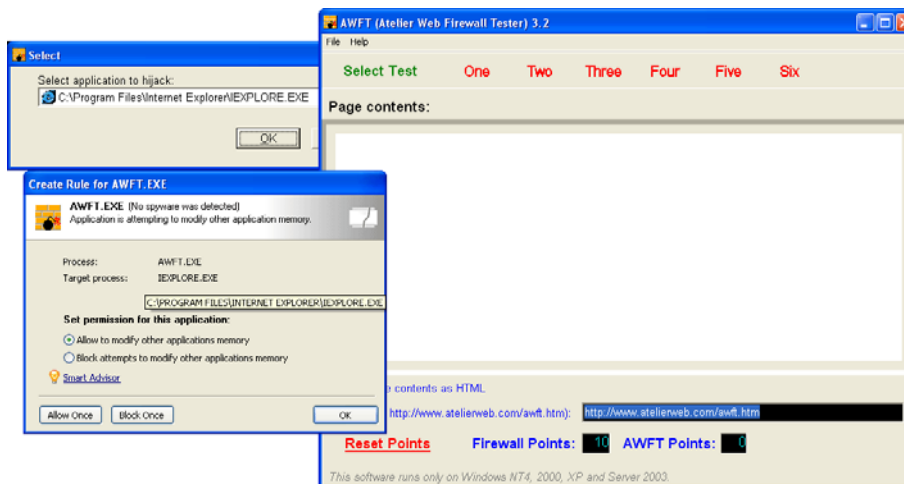
BESTANDEN

Leak-Test Nr. 12 "Atelier Web Firewall Tester"

Name/Link zum Sofort-Download	Eingesetzte Umgehungstechnik	Leak-Test-Info / Homepage	Angewandte Outpost-Funktion
Atelier Web Firewall Tester (AWFT)	Prozess-Injektion	 awft.exe	"Prozess-Speicher-Injektion" 

Der AWFT-Test besteht aus einer Suite von sechs Tests in einem Programm. Es handelt sich um einen sehr komplexen Test, der zahlreiche Techniken kombiniert, die dazu entwickelt wurden, die Firewall außer Gefecht zu setzen: direkte Prozess-Injektion in den Datenspeicher eines vertrauenswürdigen Prozesses, Öffnen des Standard-Browsers und Änderung seines Datenspeicherblocks, Öffnen einer zusätzlichen Instanz im Speicherplatz eines vertrauenswürdigen Prozesses und andere Techniken.



Hier sehen Sie, wie Outpost reagiert:



Die Höchstpunktzahl – Kennzeichen für die bestmögliche Firewall – ist zehn. Das ist auch die Punktzahl, die Outpost Firewall Pro 4.0 erreicht, was bedeutet, dass es maximalen Schutz gegen Informationslecks bietet

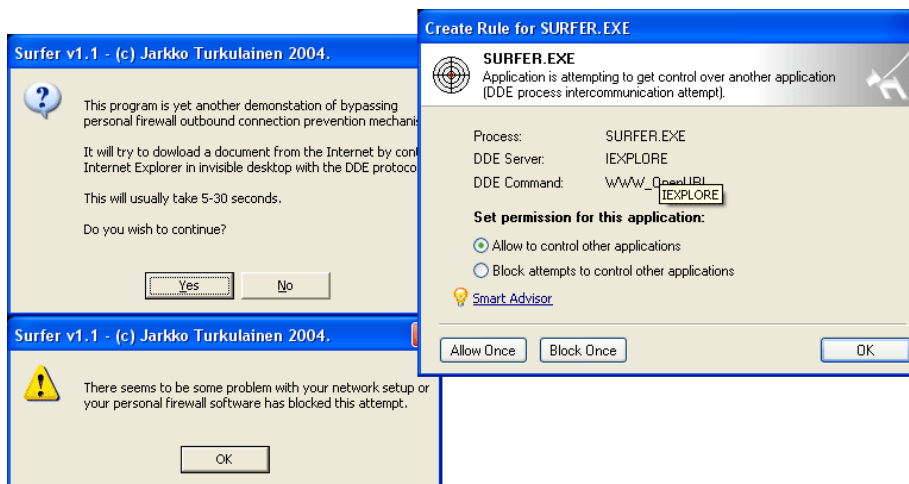
BESTANDEN

Leak-Test Nr. 13 "Surfer"

Name/Link zum Sofort-Download	Eingesetzte Umgehungstechnik	Leak-Test-Info / Homepage	Angewandte Outpost-Funktion
Surfer	DDE-Inter-Kommunikation	 surfer.exe	"DDE-Inter-Kommunikation" 

Der Test Surfer hat das Ziel, eine Firewall zu umgehen, indem mit Hilfe des DDE-Protokolls (Direct Data Exchange) die Aktionen einer vertrauenswürdigen Anwendung kontrolliert werden. Der Test öffnet den Standard-Browser mit URL-Parametern über die DDE-Schnittstelle.


Hier sehen Sie, wie Outpost reagiert:



Da Outpost die Befehle überwacht, die eine Anwendung über die DDE-Schnittstelle erhält, kann es das Anwendersystem schützen, indem es feststellt, ob die Aktivität zulässig ist.

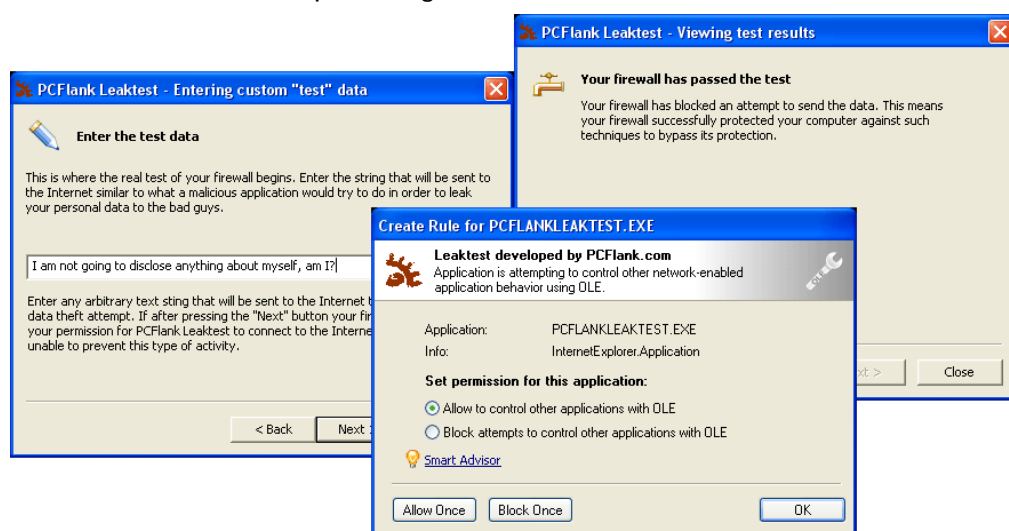
BESTANDEN

Leak-Test Nr. 14 "PCFlank Leaktest"

Name/Link zum Sofort-Download	Eingesetzte Umgehungstechnik	Leak-Test-Info / Homepage	Angewandte Outpost-Funktion
PCFlank Leaktest	Anwendungs-kontrolle durch OLE-Automa-tisierung	 PCFlankLeaktest.exe Leaktest developed by PCFlan PCFlank.com	"Kontrolle von OLE-Anwendungen" 

Der Leak-Test PCFlank benutzt die Technik der OLE-Interkommunikation, um Daten und Befehle zwischen Anwendungen auszutauschen. Der Test wendet das OLE-Modell an, um IE-Aktivitäten zu manipulieren und bestimmte Daten an den Test-Zielort des Autors zu senden.





Hier sehen Sie, wie Outpost reagiert:



Outpost kann OLE-Kommunkationen erkennen und fordert den Anwender auf, es für das Programm (in diesem Fall für den Leak-Test PCFlank) zuzulassen oder abzulehnen, die Aktivität der anderen Anwendung zu kontrollieren. Eine ablehnende Antwort blockiert die Übertragung und schützt die Daten des Anwenders.

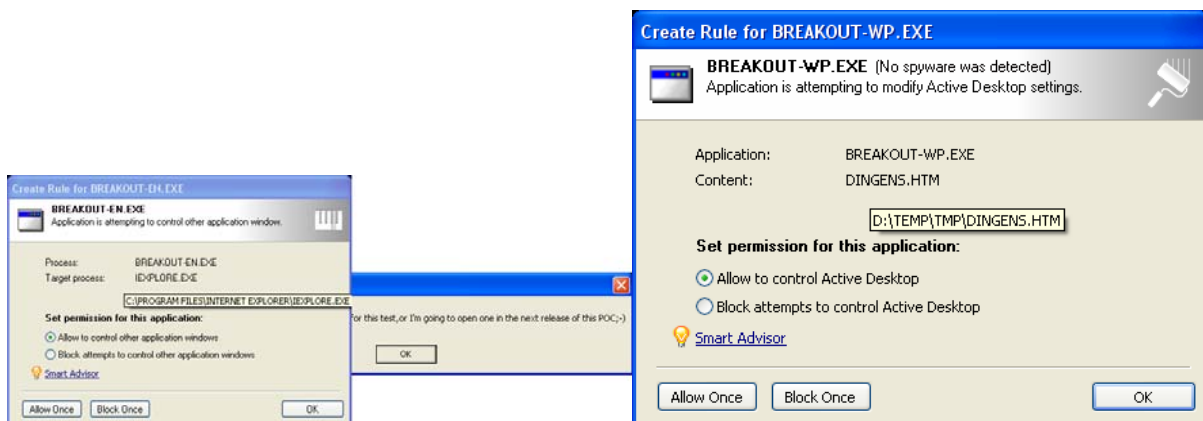
BESTANDEN

Leak-Test Nr. 15 "Breakout"

Name/Link zum Sofort-Download	Eingesetzte Umgehungstechnik	Leak-Test-Info / Homepage	Angewandte Outpost-Funktion
Breakout	Windows-Nachrichten	 breakout-en.exe	"Kontrolle von Programmfenstern" 
Breakout	Veränderung des Active Desktop	 breakout-wp.exe	

Der Test Breakout startet den Internet Explorer im Hintergrund und versucht, sein Verhalten mit Hilfe der Inter-Prozess-Kommunikation "SendMessage API" zu kontrollieren, die es einem Programm ermöglicht, die Aktivität eines anderen Programms im versteckten Modus zu steuern. Dieselbe Technik wird von diesem Test eingesetzt, um den Windows Active Desktop dazu zu veranlassen, eine lokal erstellte HTML-Seite anzuzeigen und sie als Desktop-Hintergrund einzurichten. Jede Firewall, die nicht kontrolliert, wie Anwendungen mit Internetverbindung Befehle aus anderen Programmen unter Windows interpretieren, würde bei diesem Test versagen.



Hier sehen Sie, wie Outpost reagiert:



Sobald Outpost den Versuch entdeckt, versteckte Fenster zu benutzen, benachrichtigt es den Benutzer.

BESTANDEN

Leak-Test Nr. 16 "MBtest"

Name/Link zum Sofort-Download	Eingesetzte Umgehungstechnik	Leak-Test-Info / Homepage	Angewandte Outpost-Funktion
MBtest	Direkter Zugriff auf die Netzwerkschnittstelle	 mbtest.exe	"Öffnen des Netzwerk-Treibers" 

Der Leak-Test MBtest erstellt eine ganze Flut von gefälschten Datenpaketen und sendet sie an den Netzwerk-Adapter. So wird der von der Firewall überwachte übliche TCP/IP-Stack umgangen, um den Techniken zur Verhinderung von Datenlecks zu entgehen.



Hier sehen Sie, wie Outpost reagiert:



Outpost Firewall entdeckt, wenn eine Anwendung versucht, Daten direkt an einen Netzwerk-Adapter zu senden und benachrichtigt den Anwender.

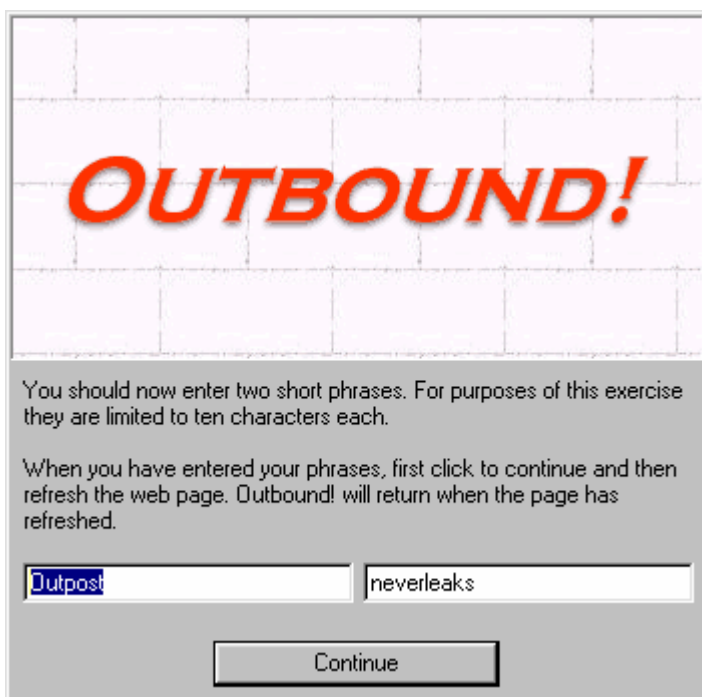
BESTANDEN

Leak-Test Nr. 17 "OutBound"

Name/Link zum Sofort-Download	Eingesetzte Umgehungstechnik	Leak-Test-Info / Homepage	Angewandte Outpost-Funktion
OutBound	Direkter Zugriff auf die Netzwerkschnittstelle	 outbound.exe	"Öffnen des Netzwerk-Treibers" 

OutBound ist ein älterer Leak-Test, der den Betrieb unter Windows 98 sowie die Installation mehrerer älterer Gerätetreiber voraussetzt. Da Outpost (im Gegensatz zu Microsoft) ältere Betriebssysteme wie Windows 98 jedoch immer noch unterstützt, war es uns wichtig, diesen Test zu bestehen.

Genau wie vorherige Tests mit derselben Technik versucht OutBound durch Öffnen des Netzwerk-Treibers und Versand der Daten über diesen Kanal Informationen nach außen zu senden. In unseren Tests sieht es jedoch so aus, als würde dieser Test nicht mehr korrekt funktionieren, der Testcode wurde nicht korrekt ausgeführt, und die Information wurde nie übertragen. Wir glauben, dass dieses Versagen von Outpost verursacht wurde, obwohl wir es tatsächlich nicht beweisen können.



BESTANDEN

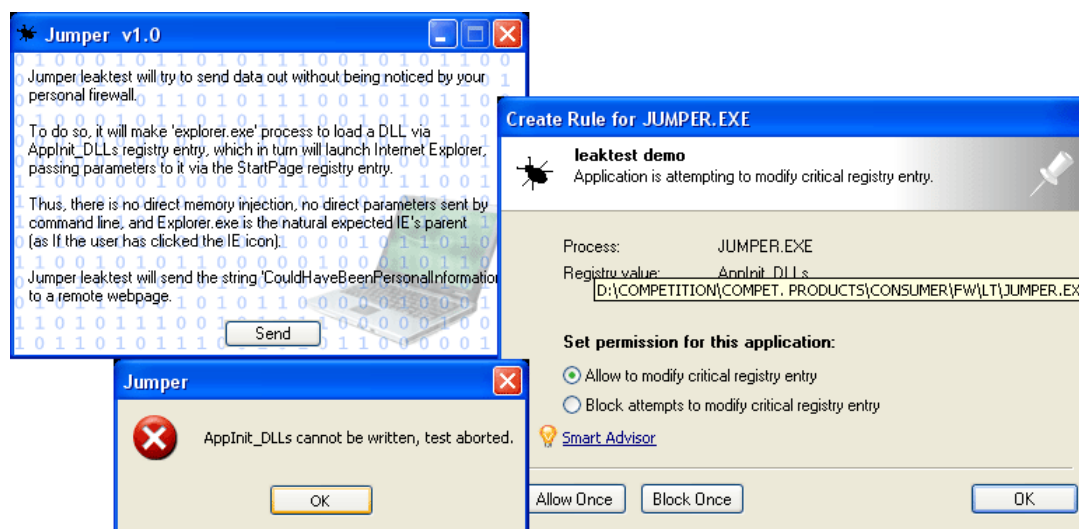
Leak-Test Nr. 18 "Jumper"

Name/Link zum Sofort-Download	Eingesetzte Umgehungstechnik	Leak-Test-Info / Homepage	Angewandte Outpost-Funktion
Jumper	Veränderung der System-Registrierungsdatenbank	 jumper.exe leaktest demo http://www.firewallleaktester..	"Kritischer Registry-Eintrag" 

Der Test Jumper benutzt sowohl die Programmstart- als auch die Registry-Änderungstechniken, um die Firewall-Sensoren zu umgehen.

Durch Manipulieren der Registrierungsdatenbank bringt der Test Windows dazu, beim nächsten Öffnen des Windows Explorers die DLL-Datei von Jumper zu laden. Die bösertige DLL modifiziert darauf hin den Registrierungseintrag für die Browser-Startseite, so dass sie beim nächsten Start die in einer URL-Adresse enthaltenen empfindlichen Daten übermitteln kann.

Hier sehen Sie, wie Outpost reagiert:



Da Outpost kritische Systemgebiete des Computers überwacht, können unerlaubte Versuche, in die Registrierungsdatenbank zu schreiben und somit bösertige Veränderungen nicht erfolgen.

BESTANDEN

Hintergrundinformationen über Agnitum

Alexey Belkin, leitender Software-Entwickler von Agnitum, erklärt, wie er über die zusätzlichen Anti-Leak-Komponenten in Outpost denkt.



"Man muss immer einen Kompromiss zwischen Sicherheit und Benutzerfreundlichkeit eingehen. Nehmen Sie zum Beispiel ein normales Türschloss. Einige Leute sind völlig zufrieden damit, mit einem ganz normalen, werksmäßig eingebauten Schloss in ihrer Tür zu leben, während andere sich mit einem stärkeren, umfangreicheren Schließsystem, für das sie mehrere Schlüssel brauchen, einfach sicherer fühlen. Letzteres erfordert mehr Zeit, aber Ihr Haus wird dadurch sicherer.

Der gleiche Ansatz kann auch auf Firewalls angewandt werden – einige bieten nur einen Grundschatz gegen einfachere Bedrohungen, sind aber einfach zu verwenden, während andere einen stärkeren Schutz bieten, aber etwas Zeit und Mühe erfordern können, um richtig konfiguriert zu werden.

Wir haben Outpost so entwickelt, dass es so stark wie möglich ist, um die Anwender gegen eine breite Vielfalt von Malware-Angriffen und Eindringen von Hackern zu schützen. Obwohl Outpost Ihnen mehr Fragen stellen wird, als Sie das normalerweise bei einer grundlegenden Firewall während der ersten Nutzungszeit erleben, bietet es, wie Sie an diesen Test-Ergebnissen sehen können, den besten Schutz seiner Art gegen alle bekannten Methoden von Informationslecks. Wir behaupten, dass ein undurchlässiger Schutz wichtiger und notwendiger ist als das kleine Ärgernis durch zusätzliche Eingabeaufforderungen in den ersten paar Nutzungstagen. Wir nehmen Datenschutz ernst, und das sollten Sie unserer Meinung nach auch tun.

Wir haben den Anwendern eine Möglichkeit geboten, die Anzahl von Fragen der Firewall zu verringern. Im 'Anti-Leak'-Bereich der Software haben wir die Registerkarte 'Ausnahmen' hinzugefügt, mit der das Level des Anti-Leak-Schutzes für jede internetfähige Anwendung auf dem Computer des Anwenders angepasst werden kann."

Schlussfolgerung

Wie man in dieser Analyse sehen kann, besteht Outpost Firewall Pro 4.0 alle derzeit verfügbaren Leak-Tests und liefert so den unabhängigen Beweis, dass das Programm ein Höchstmaß an Schutz bietet.

Zusammenfassung:

- Leak-Tests dienen als unabhängige, sichere Möglichkeit, die Qualität des Schutzes nach außen zu messen, den eine Firewall für programmabhängigen Zugriff bietet.
- Zurzeit sind achtzehn Leak-Tests bekannt, die auf mehr als einem Dutzend unterschiedlicher Programm-Interaktivitäts-Techniken beruhen.
- Outpost Firewall Pro 4.0 besteht alle derzeitigen Leak-Tests und bietet widerstandsfähigen Schutz gegen Malware, die versucht, unerlaubte Verbindungen herzustellen und vertrauliche Informationen nach außen zu senden.

Darüber hinaus stellen leistungsfähige Filter sicher, dass geschützte Informationen nie vom Computer gelangen können, so dass sogar die vernichtendsten Hacker-Angriffe abgewehrt werden.

Die neue Version von Outpost Firewall Pro wird die Internet- und Netzwerkverbindungen der Anwender schützen, egal, in welche Richtung sich die Malware-Evolution entwickelt.

Über Agnitum

Seit der Gründung im Jahr 1999 hat Agnitum Ltd. (www.agnitum.com) das Ziel, hochwertige und einfach anzuwendende Sicherheits-Softwareprodukte und den entsprechenden Support zu liefern. Produkte der Firma sind Outpost Firewall Pro zur Sicherung von Einzel- und Familiencomputern und Outpost Network Security für den zuverlässigen Endpunktschutz und sichere Leistung für kleine Firmennetzwerke. Anwender können auf der Firmenwebsite eine kostenlose Testversion von Outpost Firewall Pro herunterladen.

Kontakt

Agnitum Ltd.
Bolshoy Sampsonievskiy 60, Liter "A"
St.Petersburg, 194044, Russland

Tel.: +7-(812)-3365246
Fax: +7-(812)-3365244
E-Mail: pr@agnitum.com, www.agnitum.com