



Schutz vor Bedrohungen durch Malware & Trojanische Pferde Defending

Malware, d.h. Software, die geschrieben wurde, um PCs von Privatanwendern zu infizieren und kriminelle Handlungen wie Online-Betrug oder Identitätsdiebstahl verüben zu können, ist zu einem profitablen Geschäft für die virtuelle Unterwelt geworden. Demzufolge setzen Sie sich jedes Mal, wenn Sie einen Computer zum Surfen, Einkaufen, Online-Banking, Spielen oder zur Nutzung von E-Mail oder Instant Messaging verwenden, einem hohen Risiko aus.

Durch das Ausnutzen von Schwachstellen in Betriebssystemen und Browsern ist Malware in der Lage, bösartige Trojaner-Programme in ungesicherte PCs einzuschleusen. Ahnungslose und ungeschützte Benutzer können sich darüber hinaus in dem Glauben, es handele sich um legale Spiele, Musik, Filme oder Grußkarten Trojaner herunterladen.

Trojaner können darüber hinaus in Dateien lauern, die Sie gemeinsam mit Freunden, Familienmitgliedern oder Kollegen unter Verwendung von Peer-to-Peer-Netzwerken nutzen.

Während Trojaner bisher in per E-Mail verbreiteten Würmern und Viren versteckt waren, erscheinen sie nun zunehmend in Instant Messages oder auf PDAs und Handys. Organisierte Verbrecherringe haben aggressive neue Methoden zur Verbreitung von Trojanern entwickelt, und Benutzer müssen über die neuesten Tricks stets auf dem Laufenden sein. Um sich vor solchen vielschichtigen Angriffen zu schützen, benötigen Sie integrierte Antiviren-, Firewall- und Antispyware-Technologien. Nachstehend finden Sie die 10 wichtigsten Dinge, die Sie wissen müssen, um sich vor Angriffen durch Malware & Trojaner zu schützen.

Wie funktionieren Trojaner?

Trojaner manipulieren wichtige Dateien und infizieren Systeme mit Adware, Spyware, Keyloggern und Screen-Scrapern, die persönliche Daten stehlen und Ihre Online-Aktivitäten ausspionieren können. Darüber hinaus können Trojaner Sie zu gefälschten Phishing-Webseiten umleiten, sogar wenn Sie eine gültige Internetadresse (URL) in Ihren Browser eingeben.

Trojaner-Programme gehören zu den gefährlichsten Bedrohungen, da sie eine [Hintertür](#) auf Ihrem Computer öffnen können, die bösartigen Hackern direkten Zugriff auf Ihr System ermöglicht. Einmal installiert, können Trojaner Ihren PC ausspionieren und, solange wie sie unentdeckt bleiben, Benutzernamen, Kennwörter, Kreditkartennummern, Sozialversicherungsnummern und Kontonummern auf andere Computer hochladen.

Hacker nutzen Chaträume und Peer-to-Peer-Netzwerke, um ungeschützte PCs aufzuspüren und zu überfallen. Sobald ein Trojaner eine Hintertür geöffnet hat, gehört der Computer zu zahllosen anderen "Zombie"-Computern, die der Hacker anschließend aus der Ferne steuern kann.

Nun kann der Hacker Denial-of-Service (DoS)-Angriffe starten, Werbung generieren, infizierte Software an andere anfällige Computer verschicken und massenhaft Spam versenden.

Internetgangs vermieten sogar ganze Netzwerke von Zombie-Computern (auch "Bots" genannt) stundenweise an andere Kriminelle mit Erpressungs- und Betrugsabsichten. Benutzer bemerken nur selten, dass ihr Computer gekidnappt wurde, da das System weiterarbeitet wie bisher, wenn auch bisweilen etwas langsamer.

Ein neuer Trend im Bereich Malware besteht inzwischen darin, Geld zu erpressen. Bei der so genannten "Ransomware" handelt es sich um einen Trojaner, der die Dateien auf einem PC verschlüsselt oder damit droht, diese nacheinander zu löschen, wenn das Opfer das geforderte Lösegeld nicht zahlt. Nachdem der betroffene Benutzer über einen Geldtransferservice gezahlt hat, sendet der Erpresser ihm einen speziellen Deaktivierungscode oder eine Entschlüsselungsanwendung. Hacker nutzen Trojaner außerdem dazu, Sicherheitslücken in Webseiten für Online-Banking, elektronische Rechnungsabwicklung und E-Commerce von seriösen Unternehmen auszunutzen.

Auf welche Weise gelangt ein Trojaner auf meinen PC?

Trojaner können sich heute über "Drive-by-Downloads" verbreiten, d.h. das Programm wird im Hintergrund heruntergeladen, sobald Sie auf eine manipulierte Website zugreifen. Shellcode führt einen Trojaner aus, der weiteren schädlichen Code über HTTP herunterlädt, wie z.B. verschiedene Arten von Bots, Spyware, Backdoors und andere Trojaner-Programme. Anschließend versenden Hacker Phishing-E-Mails, um Benutzer auf Websites zu locken, wo ahnungslose Opfer zur Preisgabe von persönlichen Daten verleitet werden. Darüber hinaus nutzen Hacker Sicherheitslücken auf Webseiten aus und fügen ihre Trojaner legalen Softwareprogrammen hinzu, die anschließend von nichts ahnenden Benutzern heruntergeladen werden.

Die 10 besten Tipps zum Schutz vor Malware & Trojanern

Auch wenn Hacker ständige neue Tricks entwickeln, um Benutzer zu betrügen und ihre Identitätsdaten zu stehlen, können diese ihre Systeme durch präventive Maßnahmen schützen. Alles, was dazu nötig ist, ist eine Kombination aus zuverlässiger Sicherheitssoftware und die Beachtung folgender grundlegender Sicherheitsregeln.

- 1. Schützen Sie Ihren Computer mit zuverlässiger Sicherheitssoftware** und stellen Sie sicher, dass ihr Schutz immer auf dem neuesten Stand ist. McAfee SecurityCenter garantiert zuverlässigen PC-Schutz vor Trojanern, Hackern, Spyware und anderen Bedrohungen. Die integrierten Antiviren-, Antispyware-, Firewall-, Antispam-, Antiphishing- und Backup-Technologien greifen zum Schutz vor den heutigen hochentwickelten und vielschichtigen Angriffen nahtlos ineinander. Die Lösung scannt Datenträger, E-Mail-Anhänge, aus dem Internet heruntergeladene Dateien sowie mit Textverarbeitungs- oder Tabellenprogrammen erstellte Dokumente.

- 2. Wählen Sie einen sicherheitsbewussten Internet Service Provider (ISP),** der leistungsstarke Antispam- und Antiphishing-Verfahren einsetzt. AOL beispielsweise blockiert bekannte Phishing-Seiten, so dass Kunden nicht darauf zugreifen können. Die Organisation [SpamHaus](http://www.spamhaus.org) <www.spamhaus.org> führt die 10 derzeit schlechtesten ISPs in dieser Kategorie auf. Berücksichtigen Sie diese Liste bei Ihrer Wahl.
- 3. Aktivieren Sie die automatische Update-Funktion von Windows** oder laden Sie die Microsoft-Updates regelmäßig herunter, um Ihr Betriebssystem mit den entsprechenden Patches für bekannte Sicherheitslücken zu aktualisieren. Installieren Sie auch Patches von anderen Software-Herstellern, sobald diese veröffentlicht werden. Ein mit sämtlichen Patches versehener Computer hinter einer Firewall ist die beste Verteidigung gegen Trojaner- und Spyware-Installationen.
- 4. Seien Sie äußerst vorsichtig, wenn Sie Anhänge öffnen.** Konfigurieren Sie Ihre Virenschutzsoftware so, dass alle E-Mail- und Instant-Message-Anhänge automatisch gescannt werden. Achten Sie darauf, dass Ihr E-Mail-Programm Anhänge nicht automatisch öffnet oder Grafiken automatisch wiedergibt und stellen Sie sicher, dass das Vorschaufenster deaktiviert ist. So verhindern Sie, dass Makros ausgeführt werden. Anweisungen dazu finden Sie in den Sicherheitsoptionen oder im Einstellungsmenü Ihres Programms. Öffnen Sie nie unverlangt zugesandte Werbemails oder Anhänge, die Sie nicht erwarten, auch nicht von Personen, die Sie kennen.
- 5. Seien Sie wachsam, wenn Sie auf Peer-to-Peer (P2P)-Netzwerke zugreifen.** Trojaner lauern in Filesharing-Programmen und warten nur darauf, heruntergeladen zu werden. Befolgen Sie beim Downloaden von gemeinsam genutzten Dateien dieselben Vorsichtsmaßnahmen wie bei der Nutzung von E-Mail und Instant Messaging. Laden Sie möglichst keine Dateien mit der Endung *.exe*, *.scr*, *.lnk*, *.bat*, *.vbs*, *.dll*, *.bin* oder *.cmd* herunter. Virenschutzsoftware und eine gute Firewall schützen Ihr System vor bösartigen Dateien.
- 6. Laden Sie die neueste Version Ihres Browsers herunter,** um sicherzustellen, dass dieser vollständig aktualisiert ist und die neuesten Technologien zum Identifizieren und Herausfiltern von Phishing-Seiten, die Trojaner installieren können, nutzt.
- 7. Treffen Sie Sicherheitsvorkehrungen für Ihren PDA, Ihr Handy und Wi-Fi-Geräte.** Trojaner werden als E-Mail-/Instant-Message-Anhang übertragen, aus dem Internet heruntergeladen oder zusammen mit anderen Daten von einem Desktop hochgeladen. Handy-Viren stecken noch in den Kinderschuhen, treten jedoch immer häufiger auf, da immer mehr Menschen Handys mit erweiterten Funktionen nutzen. Antivirensoftware ist auch für PDAs und Handys erhältlich. McAfee bietet darüber hinaus zuverlässige Sicherheitslösungen für Wi-Fi-Geräte an.
- 8. Konfigurieren Sie Ihre Instant-Messaging-Anwendung richtig.** Stellen Sie sicher, dass diese nicht automatisch geöffnet wird, wenn Sie Ihren Computer hochfahren. Schalten Sie Ihren Computer aus und trennen Sie die DSL- oder Modemverbindung, wenn Sie diese nicht benötigen. Nehmen Sie sich vor Spam-basierten Phishing-Methoden in Acht - klicken Sie nicht auf Links in E-Mails oder Instant Messages.

9. **Stellen Sie sicher, dass eine Website seriös ist, bevor Sie darauf zugreifen.** Verwenden Sie Software, die dies automatisch überprüft, wie z.B. [AccountGuard](#) von eBay oder [ScamBlocker](#) von Earthlink. Sie können die Authentizität einzelner Internetadressen (URLs) darüber hinaus mit einer „Wer ist“-Suche, z.B. über www.DNSstuff.com, überprüfen.
10. **Sichern Sie Ihre Dateien regelmäßig** und speichern Sie die Backups außerhalb Ihres PCs. Wenn Sie Opfer eines Trojaner-Angriffs werden, können Sie Ihre Fotos, Musik, Filme und persönlichen Daten wie Steuererklärungen oder Bankauszüge wiederherstellen. McAfee® PC Protection Plus bietet zuverlässigen Schutz vor Viren, Spyware und Hackern sowie automatische Backups Ihrer Festplatte.

McAfee®

McAfee GmbH
Ohmstr. 1
85716 Unterschleissheim
+49-89-3707 0
www.mcafee.de