DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 89194 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Malware und Viren – was ist eigentlich der Unterschied?

In Sicherheitswissen by Adrian on March 8, 2012 | Русский, Italiano, Français, English, Deutsch

Immer wieder ist in diversen Foren die Frage zu lesen, ob ein Anti-Malware Programm wie Emsisoft Anti-Malware denn auch vor Viren schützt. Die kurze Antwort lautet: ja. Der Terminus Malware setzt sich aus den beiden Begriffen „malicious“ und „Software“ zusammen, was so viel wie „schädliche Software“ bedeutet. Da Computerviren zweifelsohne schädlich sind, fallen sie ebenfalls in die Kategorie Malware, genauso wie Trojaner, Rootkits oder Spyware.

Im Endeffekt verhält sich das also genauso wie mit den Dackeln und Hunden: jeder Virus ist Malware, wie jeder Dackel ein Hund ist. Aber genauso wenig wie jeder Hund ein Dackel ist, ist nicht jede Malware ein Virus, sondern in diesem Fall eine Unterart. Genau genommen gibt es heutzutage sogar kaum noch neue Viren, den Großteil der aktuellen Malware machen andere virtuelle Schädlinge aus.

Anti-Virus: heute ein irreführender Begriff

Leider sind die in vielen Schutzprogrammen verwendeten Begriffe „Anti-Virus“ und „Anti-Malware“ ein wenig irreführend. Einige Anwender halten Anti-Virus Lösungen fälschlicherweise für leistungsfähiger als jene gegen Malware, wobei letzteres ja der Überbegriff ist. Die Angelegenheit ist sogar noch etwas komplizierter, da fast alle gängigen Anti-Virus Programme inzwischen auch Schutz vor allen anderen Malwarte-Arten bieten. Dazu kommt noch, dass die Bezeichnung Anti-Malware vereinzelt auch von Programmen verwendet wird, die gar

keinen umfassenden Schutz vor allen Bedrohungen bieten, sondern beispielsweise nur auf bestimmte Kategorien oder schwer zu entfernende Malware spezialisiert sind.

Korrekterweise müssten die Anti-Virus Anwendungen jedenfalls eigentlich umbenannt werden. Die Bezeichnung stammt noch aus den Ursprüngen der Computersicherheit gegen Ende der 1980er Jahre. Damals tauchten die ersten Computerviren auf, wobei mit Michelangelo 1992 dem ersten Vertreter überhaupt enorme Medienpräsenz zuteilwurde. Diese „Urformen der Malware“ waren keine eigenständigen Programme, sondern schleusten ihren schadhaften Code in normale Anwendungsprogramme ein, welche diesen dann als Überträger weiter verbreiteten.

Das erklärt auch die Bezeichnung Computervirus. Denn genauso wie ein biologisches Virus eine bestimmte fremde Zelle benötigt, in die es seine DNS einschleust und diese in der Folge zur eigenen Verbreitung nutzt, braucht auch ein Computervirus ein bestimmtes Anwendungsprogramm für die virtuelle Reproduktion. Ebenfalls ist es damit mehr als einleuchtend, dass die ersten Schutzprogramme „Anti-Virus“ getauft wurden. Bei vielen hat sich das bis heute nicht geändert, da sie so bei Kunden und Anwendern bekannt sind. Die Hersteller möchten nicht Gefahr laufen ihre Markenidentität zu verlieren, auch wenn wie bereits angedeutet viele moderne Anti-Virus Tools eigentlich komplette Anti-Malware Lösungen sind. Sicherheit bringt ein Blick auf die Beschreibung-schauen Sie nach, vor welchen virtuellen Schädlingen genau Sie ein Sicherheitsprogramm bewahrt, egal ob Anti-Virus oder Anti-Malware. Der Inhalt ist wichtig, nicht der Name oder die Verpackung.

Welche Arten von Malware gibt es eigentlich?

Viren kennt jeder, Trojaner, Spyware oder Adware die meisten auch. Aber wie steht es mit Rootkits, Ransomware und Rogues? Im Folgenden möchten wir Ihnen die diversen Malwarearten kurz vorstellen.

- **Virus**Ein Computervirus verbreitet sich selber weiter, indem es seinen Code in Anwendungsprogramme einschleust. Der Name stammt von seinem biologischen Vorbild ab. Nicht selten führt ein Computervirus neben der eigentlichen Verbreitung, die das Wirtsprogramm unbrauchbar machen kann, auch noch Schadroutinen aus.
- **Trojanisches Pferd / Trojaner**Das trojanische Pferd ist eine als nützliches Programm getarnte Form von Malware. Ziel ist die Ausführung durch den Anwender, wodurch der Trojaner die Kontrolle über den Computer erlangen und diesen für vielfältige eigene Zwecke verwenden kann. Dazu wird meist auch andere Malware auf dem System installiert, beispielsweise Backdoors oder Keylogger.
- **Wurm**Würmer sind schädliche Programme mit dem Ziel sich sofort nach Ihrer Ausführung so weit wie möglich zu verbreiten. Im Gegensatz zu einem Virus werden zur Verbreitung nicht andere Programme, sondern Speichermedien wie USB-Sticks, Kommunikationsmedien wie E-Mails oder Lücken im Computersystem verwendet. Die Verbreitung mindert die Leistung von PCs und Netzwerken, teilweise werden auch direkte Schadroutinen implementiert.
- **Keylogger**Keylogger zeichnen heimlich sämtliche Tastatureingaben auf, wodurch Passwörter und andere wichtige Daten wie Online Banking Zugänge ausgespäht werden können.
- **Dialer**Dialer (frei übersetzt „Wähler“) sind ein Relikt aus der Zeit, als für die Einwahl ins Internet noch Modems oder ISDN verwendet wurden. Sie wählten unbemerkt kostenpflichtige Mehrwertnummern an und sorgten so durch teilweise enorm hohe Telefonrechnungen für finanziellen Schaden bei den Opfern. Bei ADSL- oder Kabelanschlüssen sind Dialer wirkungslos, weshalb sie inzwischen als eigentlich ausgestorben gelten.

- **Backdoor / Bot**Eine Backdoor (Englisch für „Hintertür“) ist ein oft vom Autor des Programms eingebauter Teil einer Software, der es ermöglicht, Zugang zum Computer oder einer sonst geschützten Funktion eines Computerprogramms zu erlangen. Backdoors werden oft von Trojanern direkt nach deren Ausführung installiert, damit der Angreifer von außen Zugriff auf den attackierten Computer erhält. Der infizierte PC (Bot) wird dadurch meist Teil eines Botnets.
- **Exploit**„To exploit“ bedeutet „ausnutzen“, synonym werden Exploits eingesetzt, um Schwachstellen in Computerprogrammen gezielt auszunutzen. Der Angreifer verschafft sich mit ihrer Hilfe Kontrolle über das Computersystem oder zumindest Teile davon.
- **Spyware**„Spy“ bedeutet übersetzt „Spion“, entsprechend handelt es sich bei Spyware um ein Spionageprogramm, das unbemerkt diverse Daten eines Anwenders sammeln möchte.
- **Adware**Das „Ad“ leitet sich von „Advertisement“ ab, dem englischen Wort für Werbung. Neben der eigentlichen Funktion des Programms wird dem Anwender Werbung angezeigt. Adware ist per se nicht gefährlich, massiv Werbung einblendende Programme gelten aber allgemein als unerwünscht und werden daher von guten Anti-Malware Lösungen erkannt.
- **Rootkit**Ein Rootkit besteht meist aus mehreren Komponenten, die dem Autor unbemerkbar Zugriff auf das Zielsystem geben. Dazu werden Prozesse und Programmteile versteckt. Die Installation kann beispielsweise durch einen Exploit oder Trojaner geschehen.
- **Rogues / Scareware**Auch als „Rogue Anti-Spyware“ oder „Rogue Anti-Virus“ bezeichnet, gaukeln Rogues dem Opfer vor, dass es sich dabei um ein Schutzprogramm handelt. Oft kommen dabei gefälschte Warnhinweise zum Einsatz, die zum Kauf des Schutzprogramms verleiten sollen, wodurch der Angreifer auf illegale Weise Profit erwirtschaftet.
- **Ransomware**„Ransom“ lässt sich leicht mit „Lösegeld“ übersetzen. Und genau dieses fordert Ransomware auch, indem persönliche Daten des Anwenders einfach verschlüsselt oder gar der gesamte Computer softwareseitig gesperrt wird. Erst nach Bezahlung über einen anonymen Dienst wird der Computer wieder freigegeben.

Vergangenheit und Zukunft von Malware

Falls Sie eines unserer Programme mit Malware-Scanner einsetzen, beispielsweise Emsisoft Anti-Malware oder das Emsisoft Emergency Kit, erhalten Sie von uns pro Tag 20.000 bis 30.000 neue Signaturen für Ihre Sicherheit. Dabei verschiebt sich die prozentuale Verteilung der Malware Arten regelmäßig, seit es Personal Computer gibt war fast jede Gattung irgendwann einmal voll im Trend.

Viren hatten ihren absoluten Höhepunkt beispielsweise in den 90er Jahren des letzten Jahrhunderts, bevor Trojaner wie Sub7 und Netbus und Würmer wie SQL Slammer, W32.Blaster oder Sasser das neue Jahrtausend einleiteten. Dialer gelten heute als nahezu ausgestorben, aber auch sie machten vor 10-15 Jahren uns Computeranwendern das Leben schwer. Erst letztes Jahr lag Ransomware wieder hoch im Kurs, vielleicht erinnern Sie sich noch an die beiden bekanntesten Beispiele BKA respektive Gema Trojaner. Die Bezeichnung Trojaner kennzeichnet hier nur den Infektionsweg, die eigentliche Malware zeigt das Verhalten klassischer Ransomware.

Ein klarer Trend zeichnet sich in den letzten Jahren allerdings ab: Malware kommt immer seltener einzeln zum Einsatz, so dass wie bei dem Gema Trojaner eine klare Artenbestimmung schwierig wird. Vielmehr werden mehrere Malware Arten auf einmal verwendet. Zum Angriff auf einen Computer wird beispielsweise wahlweise ein Trojaner, Exploit oder Wurm verwendet. Dieser installiert dann eine Backdoor, so dass der Verursacher Zugriff auf den Computer erhält, wo folglich oft ein Keylogger, Rootkit, Spyware oder ähnliches installiert wird. Damit hat der Hacker dann vollen Zugriff, liest eifrig alle Passwörter auf dem gehijackten Computer mit, kopiert wichtige private Daten und kann ihn für DOS Angriffe missbrauchen – selbstverständlich gegen Bezahlung oder um Unternehmen zu erpressen. Nicht selten kontrolliert ein Hacker dabei mehrere hundert bis zehntausende Computer, die dann auch als „Bots“ und das Netzwerk als Botnet bezeichnet werden. Schätzungen zur Folge sind in Deutschland alleine etwa 500.000 Computer Teil eines solchen Botnets – selbstverständlich ohne Wissen des Besitzers.

Der Kampf gegen Malware ist in den letzten 10 Jahren für die Hersteller von Sicherheitsprodukten jedenfalls nicht leichter geworden. Denn Malware-Autoren werden immer professioneller und raffinierter. Die Folge sind hochentwickelte Schadprogramme, die der Anwender oft nicht bemerkt oder erst dann, wenn es schon zu spät ist. Damit sind auch viele Weisheiten, die immer noch auf Webseiten und in Foren verbreitet werden, überholt. Es reicht beispielsweise nicht als Computerschutz aus, dubiose Webseiten zu meiden und keinen Administratoraccount zu verwenden, wenn Malware anhand eines Exploits auf den Computer gelangt. Und auch das wöchentliche Scannen mit einem kostenfreien Anti-Virus Programm bringt wenig, wenn sich ein einmal installiertes Rootkit durch Versteckroutinen unauffindbar im Systemkern verankert hat.

Egal wie versiert der Anwender ist, ein aktuelles Sicherheitsprogramm mit Echtzeitschutz sollte auf keinem Computer fehlen. Emsisoft Anti-Malware schützt Ihren PC beispielsweise gleich dreifach: der Surf-Schutz unterbindet den Besuch gefährlicher Webseiten. Der leistungsstarke Dual-Engine Scanner erkennt Malware, sollte Sie doch auf Ihren Computer gelangen und selbst bis dato gänzlich unbekannte virtuelle Schädlinge werden zuverlässig durch die fortschrittliche Verhaltensanalyse abgewehrt. So sind Sie auch vor den Malware-Trends von morgen sicher geschützt.

Quelle: https://blog.emsisoft.com/de/2012/03/08/tec120308de/