Malware: Eine Bestandsaufnahme

Ein Beitrag von MobyDuck

Bevor wir uns mit der Abwehr schädlicher Programme beschäftigen, müssen wir uns zunächst einen Überblick verschaffen, welche Arten von Malware es überhaupt gibt und wie diese Plagegeister ausgeführt werden. In vielen Foren und auch anderswo geht da nämlich einiges durcheinander. Da werden Würmer als Viren, Trojaner als Würmer bezeichnet und so weiter. Wir werden bei dieser Gelegenheit auch sehen, dass der zentrale Begriff aller Malware das simple Wörtchen "Fehler" ist. Und wenn man dies verstandenen hat, ist man im Kampf um ein sauberes System schon einen guten Schritt weiter.

Klassische Viren

Zunächst machen wir einen kurzen Ausflug in die Geschichte. Klassische Viren sind nämlich derzeit kaum noch verbreitet. Es mag zwar sein, dass sie irgendwann eine Renaissance erleben, aber das wäre ein anderes Thema.

Bereits im Jahr 1980 schrieb ein Student eine Diplomarbeit, in der er die Möglichkeit zeigte, dass sich bestimmte Programme ähnlich wie (echte) biologische Viren verhalten können. Und wie immer im Leben, was machbar ist, wird auch irgendwann gemacht. 1981 wurde der 1. Virus für Unix-Systeme geschrieben, 1986 tauchte der erste Virus für MS-DOS auf. Zwei Pakistaner schrieben ein Programm, das sich selbst über Disketten weiterverbreitete und das Hauptverzeichnis der Disketten in „Brain“ umbenannte. Danach ging es Schlag auf Schlag und das Katz-und-Maus-Spiel zwischen den Herstellern von Antiviren-Software und den Virenautoren begann.

Klassische Viren zeichnen sich dadurch aus, dass sie ausführbare Dateien befallen und diese dazu bringen, weitere Dateien zu infizieren und sich dadurch zu verbreiten. Um ausgeführt zu werden, benötigen sie den Fehler des Users, sich Programme aus unsicheren Quellen zu besorgen und diese ungeprüft zu starten. Man unterscheidet Bootviren, Linkviren, Hybridviren und andere. Einzelheiten kann ich uns an dieser Stelle ersparen.

Interessant für die weitere Entwicklung wurde es durch eine spezielle Virenart, die Makroviren. Das sind Schädlinge, die zu ihrer Verbreitung und zum Ablauf der Schadroutine Makros benutzen, wegen der flächendeckenden Verbreitung bevorzugt die Makrosprache von MSOffice. Im Jahr 1999 tauchte der Word-Makro-Virus Melissa auf. Kurz gesagt verschickte sich Melissa über Outlook an die Mailadressen im Adressbuch. Das Internet als Massen-Kommunikationsmittel war im Kommen und innerhalb von Stunden war der Virus über die ganze Welt verbreitet. Der Melissa-Schöpfer kam dafür in den Knast, aber die Malware-Autoren kamen ins Grübeln und wandten sich einer ganz anderen Schädlingsgattung zu, den Würmern. Und es dauerte auch gar nicht lange, da tauchte im 2000 der I love-you-Wurm auf, der sich ähnlich rasant verbreitete wie zuvor Melissa.

Würmer

Bei Würmern handelt es sich im Gegensatz zu Viren um selbständige Programme, die sich über Computernetzwerke, also auch dem Internet verbreiten. Sie haben die klassischen Viren nahezu abgelöst, die Antivirenprogramme müssten heutzutage eigentlich Wurmkuren heißen.
Auch Würmer müssen, wie jedes Programm, ausgeführt werden. Da man dies normalerweise nicht freiwillig tut, hoffen die Wurmautoren ebenfalls auf Fehler. Dies kann eine Interaktion des Users sein ("Klick") oder die Ausführung geschieht durch einen Fehler in einem Programm ohne Zutun des Users.

Nach wie vor beliebt ist die Masche, Emails zu verschicken und zu hoffen, dass die Empfänger so dumm sind, auf die beigefügten Anhänge zu klicken. Derartige Anhänge sind meist durch doppelte Endungen getarnt. Das hört sich zunächst banal an, ist es aber gar nicht. Die Würmer Netsky und Mydoom sind nach wie vor weit verbreitet und arbeiten nach diesem simplen Prinzip. Nach dem verhängnisvollen Klick wird der Wurm ausgeführt: Er installiert sich im System, errichtet meist einen eigenen Mailserver und verschickt sich darüber weiter. Häufig trickst er auch noch Antiviren-Software und Software-Firewalls aus, um weitere schädliche Programme wie Keylogger, Backdoors oder ähnliches nachzuladen. Es hilft nichts, bei diesen Würmern über Windows oder andere Programme zu meckern. Windows hat nur das getan, was man von dem Betriebssystem erwartet, nämlich Programmcode ausgeführt. Der Fehler liegt einzig und allein beim Anwender, der leichtfertig auf einen Mailanhang, eine Datei aus einer Tauschbörse oder ähnliches geklickt hat.

Wie schon angesprochen, gibt es auch Würmer, die zu ihrer Ausführung Fehler in weit verbreiteten Programmen ausnutzen und sich ohne Zutun des Users verbreiten. Windows und der Internet Explorer sind die häufigsten Angriffsziele dieser Schadprogramme. Von Blaster und Sasser hat bestimmt jeder schon gehört, die beide Fehler in Windows-Diensten ausnutzen. Es gibt auch Würmer, die HTML-Code in Mails und damit indirekt Schwachstellen im Internet Explorer zur automatischen Ausführung nutzen. Ganz schuldlos ist aber auch das Opfer nicht. In den allermeisten Fällen ist der Patch des fehlerhaften Programms vor dem Wurm da, so dass man auch sagen kann,

dass der Fehler beim User liegt, der leichtfertig nicht gepatcht hat.

So, jetzt wird es richtig gemein: Wenden wir uns kurz den Bots zu. Diese Unterart der Würmer ist derartig vielfältig, dass man allein über dieses Thema ein Buch schreiben könnte. Wie der Name schon sagt, dienen Bots der Fernsteuerung fremder Rechner, übertragen und ausgeführt werden sie meist ebenfalls über Schwachstellen in Windows oder im Internet Explorer. Im großen Stil angefangen hat es mit dem Agobot. Unglücklicherweise wurde der Quellcode im Internet veröffentlicht, mit der Folge, dass unzählige Varianten das Netz überschwemmen. Letzteres ist auch kein Wunder, so ein Bot ist für den Urheber mehr als praktisch. Einmal ausgeführt, bietet der Bot dem Urheber Zugang zu dem befallenen System, man kann nach Belieben Systemdateien löschen oder einfügen, weitere Malware nachladen, Passwörter ausspionieren, kurz alles, was einem kriminellen Urheber so einfällt. Dazu kommt die bereits erwähnte Fernsteuerung. Man kann damit viele befallene Computer zusammenfassen und DDoS –Angriffe fahren. Oder die Opfer-Computer als Spam-Versender missbrauchen. Oder Spyware installieren und die Ergebnisse meistbietend verkaufen. Oder den Internet Explorer auf bestimmte Seiten entführen und am Traffic verdienen. Da man mit diesen Praktiken richtig Geld machen kann, wird uns das Thema der Bots noch eine ganze Weile beschäftigen. Bei einem Befall liegt auch hier der Fehler letztendlich beim User, weil er ein nicht ausreichend gepatchtes System nutzte.

Trojanische Pferde

Anders als Viren oder Würmer können sich Trojaner nicht selbständig verbreiten, sondern sind auf Wirtsprogramme angewiesen. Allerdings gibt es auch Mischformen, oder die Trojaner werden per Wurm auf das System geschleust, was im Einzelfall die Abgrenzung Wurm-Trojaner schwierig macht. Dieses theoretische Problem soll uns hier jedoch egal sein.

Auch Trojaner müssen ausgeführt werden. Normalerweise erreicht man dies durch eine Täuschung des Users, indem man ihm vorspiegelt, ein Programm sei nützlich oder indem man in einem nützlichen Programm die Schadfunktion versteckt. Einbauen kann man alles, was man möchte und was Profit verspricht: Von Backdoors über Sniffer zum Ausspähen des Datenverkehrs bis hin zur Umleitung auf bestimmte Websites. Der Fehler des Users liegt meist darin, leichtfertig dubiose Software zu installieren.

Spy- und Adware

Für mich handelt es sich hierbei um einen Unterfall der Trojaner. Vernünftigerweise installiert man sich so etwas nicht freiwillig. Adware blendet meist Reklame ein, mit Spyware wird das Verhalten des Users ausspioniert. Das kann das Surfverhalten sein oder etwa wie bei den Treibern der HP-Drucker das Druckverhalten und das Verwenden von Fremdpatronen.

Der Unterschied zum eigentlichen Trojaner liegt nach meiner Meinung nur darin, dass Spyware in der rechtlichen Grauzone angesiedelt ist. Meist findet sich im Setup der Programme ein versteckter Hinweis auf die Spyware und die Urheber sagen mit unschuldiger Miene, der User habe doch der Installation zugestimmt. Also hat der betroffene Anwender den Fehler gemacht, bei der Installation nicht genau genug hingesehen zu haben.

Browser-Hijacker

Diese Nervtöter sind in letzter Zeit in Mode gekommen. Es handelt sich um kleine Programme, die die Einstellungen des Internet Explorers manipulieren um Seitenaufrufe oder Suchanfragen auf bestimmte Seiten zu lenken. Auch hier wird natürlich richtig Geld verdient. Die Hijacker nutzen Schwachstellen in Windows und dem Internet Explorer aus, der User macht somit den Fehler, nicht gepatcht zu haben und / oder den Internet Explorer mit unsicheren Einstellungen zu nutzen. Die Hijacker installieren sich meist über aktive Funktionen des Internet Explorers. Aber es gibt auch andere Infektionsmöglichkeiten und täglich kommen neue Hijacker-Modelle dazu.

Ausblick

Die Tendenz geht weiter dahin, dass sich die obigen Arten der Schädlinge immer mehr vermischen: Würmer öffnen z.B. Backdoors oder laden Trojaner nach. Auch die Infektionsmöglichkeiten, etwa durch den Besuch präparierter Seiten mit unsicher konfigurierten Browsern werden immer vielfältiger. Bereits jetzt ist es zur Regel geworden, dass nach einem unbedachten Klick die Schädlinge auf den leichtfertigen User geradezu niederprasseln. Jeder will nun mal mitverdienen und man kennt sich in der Szene. Wen es interessiert, was dann alles passieren kann, hier ist es eindrucksvoll beschrieben:

http://www.heise.de/security/artikel/49687

So, das wär's. Nicht erwähnt habe ich aus Platzgründen die Dialer und das Phishing. Erstere sind

strenggenommen keine Malware und das Phishing ist ebenfalls keine Malware, sondern ein Ziel des Malwareeinsatzes. Mir kam es darauf an, einen Überblick zu geben und deutlich zu machen, dass zur Ausführung schädlicher Programme immer ein Fehler des Users nötig ist.