

# Der Malware – Zoo

(Quelle: Fraunhofer Institut für Rechnerarchitektur und Softwaretechnik)





## Einleitung

Das Internet ist ein gefährlicher Ort. Saboteure versuchen auf vielerlei Art, über das Netz in fremde Computer einzudringen, ohne dass ihr Besitzer es merkt. Hat der Einbruch geklappt, wird der Computer mit bösartigen Programmen verseucht, seine Rechenpower missbraucht oder Nutzerdaten und Kennwörter werden ausspioniert. Solche Schadprogramme fasst man unter dem Begriff „Malware“ zusammen. Meist nennt man sie einfach „Viren“, aber tatsächlich sind Viren nur ein Malware-Typ unter vielen.

Wir haben hier ein paar der gefährlichsten und am weitesten verbreiteten Übeltäter eingefangen. Man kann unseren Zoo in zwei Gruppen unterteilen: „Virus“, „Wurm“ und „Trojanisches Pferd“ bezeichnen verschiedene Arten der Weiterverbreitung. „Backdoor“, „Rootkit“, „Keylogger“ und „Botnetz“ sind dagegen Schadfunktionen, die meist von Viren, Würmern oder Trojanischen Pferden in Computer eingeschleppt werden.

## Virus

Viren sind Skripte, die sich in ausführbare Dateien kopieren, z. B. in Programme, Dokumente mit Makros oder Bootsektoren von Datenträgern. Wird die Datei oder der Datenträger gestartet, lädt auch das Virus und kann weitere Dateien infizieren oder seine Schadfunktion ausführen. Viren verbreiten sich nicht selbständig. Sie werden übertragen, wenn eine infizierte Wirtsdatei weitergegeben wird, z. B. per Diskette, USB-Stick oder E-Mail.

## Wurm

Im Gegensatz zu Viren sind Würmer eigenständige Programme, die sich auch selbständig weiterverbreiten. Sie suchen aktiv nach Rechnern, auf denen eine Anwendung mit Sicherheitslücken läuft. Haben sie eine gefunden, verbinden sie sich direkt damit und schleusen sich so in den Computer ein, ohne dass der Benutzer dazu einen Beitrag leisten muss. Auf diese Art werden extrem hohe Verbreitungsraten erreicht.

## Botnetz

Botnetze werden vor allem benutzt, um die Rechenkapazität von Computern zu stehlen. Dazu wird ein Bot-Programm in einen Computer eingeschleust, das sich dann im Internet bei einem Server anmeldet. So öffnet es einen Kommunikationskanal, über den ein „Botmaster“ den Rechner von außen fernsteuern kann. Schaltet der Saboteur mehrere – oft bis zu 10'000 – Rechner zusammen, entsteht ein Botnetz. Botnetze haben eine gewaltige Rechenpower, man kann damit z. B. Server mit massenhaften Anfragen zum Kollaps bringen. Außerdem lässt sich mit ihnen viel Geld verdienen, etwa indem man sie zum Versenden von Spam-Mails „vermietet“.



### **Trojanisches Pferd**

Unter Trojanischen Pferden versteht man Programme, die einem Anwender eine nützliche Funktion anbieten, nebenbei aber noch etwas anderes tun, wovon der Anwender nichts weiß. Wenn er das Programm startet, um die Vordergrundfunktion auszuführen, wird die Hintergrundfunktion mitgestartet. Manche Trojanischen Pferde installieren dann weitere Schadprogramme auf dem Computer, z. B. Spionagetools oder Backdoors, die eigenständig laufen und auch nicht verschwinden, wenn das Trojanerprogramm deinstalliert wird.

### **Backdoor**

Backdoors sind entweder in Viren, Würmern oder Trojanischen Pferden enthalten oder werden als separate Programme von ihnen in einen Computer eingeschleust und dort installiert. Zweck der »Hintertüren« ist es, unter Umgehung der Sicherheitsvorrichtungen einem Unbefugten den Zugang zu dem Computer zu ermöglichen. Der Eindringling kann dann in dem Computer z. B. Daten ausspionieren oder manipulieren. Dazu warten Backdoors an bestimmten IP-Ports auf eine Kontaktaufnahme von außen.

### **Keylogger**

Keylogger schreiben mit, was über die Tastatur in einen Computer eingegeben wird. Wenn der Benutzer z. B. ein Passwort tippt, protokolliert der Keylogger, welche Tasten er dazu gedrückt hat. Diese Information speichert er entweder auf der Festplatte oder er versendet sie sofort über das Internet. Auf diese Art können Kriminelle geheime Daten, z. B. Passwörter oder PINs, ausspionieren.

### **Rootkit**

Mithilfe von Rootkits verbergen Eindringlinge ihre unbefugten Tätigkeiten auf einem geknackten Computer. Rootkits sind Sammlungen von Werkzeugen, die nach dem ersten Einbruch auf dem Computer hinterlegt werden und z. B. spätere Logins verschleiern. Außerdem machen sie Dateien unsichtbar, die der Einbrecher einschleust, oder auch Aktionen, die er ausführt. Der Name leitet sich von Unix-ähnlichen Betriebssystemen ab: Dort heißt ein Nutzer mit Administratorrechten „root“ (engl. für „Wurzel“).