



Output  
07-08/2008



## Bock als Gärtner

Cybercrime ist ein florierender Geschäftszweig. Laut Studien wurde damit im letzten Jahr erstmals mehr Geld bewegt als im internationalen Drogenhandel. Betrachtet man die Vielzahl an neuen Schädlingen und welche Tricks dabei angewandt werden, bleibt einem vor Staunen über diese Chuzpe einfach die Spucke weg.

Jüngstes Beispiel sind die in den letzten Tagen vermehrt aufgetauchten Web-Seiten, die mit vermeintlichen Viren-/Spyware-Scannern auf vorgebliche Sicherheitslücken hinweisen («Achtung kein Virenschutz vorhanden») und den Anwender zum Download eines Antivirus- oder Antispyware-Tools auffordern. Der vermeintliche Gratis-PC-Scann fördert schnell einen Virenfund zu Tage. Der ist jedoch nur vorgetäuscht und verschleiert die Tatsache, dass die eigentliche Viren- oder Spyware-Infektion schon mit der Installation des »Gratis-Scann-Tools« erfolgt ist. Von diesen Fake-Scannern gibt es zwei Varianten. Die erste scannt den PC per Web-Oberfläche und fordert den Besucher nach einem vorgetäuschten Virenfund auf, einen Remover downzuloaden. Dies erfolgt gratis oder gegen Geld. Bei der Installation des »Removers« werden nicht nur die vermeintlichen Viren entfernt, sondern noch ein oder mehrere »Zusatztools« ohne Wissen des Anwenders installiert, im Regelfall Ad- oder Spyware, immer öfter auch Backdoors und andere Trojaner.

Variante 2 fordert den Besucher gleich zum Download und der Installation des »Scanners« auf. Malware wird so vom Besucher freiwillig mit dem »Virens scanner« installiert. Nur dass man die Sache mit dem Virens scanner halt fast zu wörtlich nimmt. – Auch die weiteren »Marketing-instrumente« tragen rasch zur »Vermögensbildung« bei – z.B. nach erfolgreicher Installation den Rechner zu sperren und zum Anruf einer kostenpflichtigen Telefonnummer aufzufordern, damit der Rechner wieder entsperrt werden kann.

Als Anti-Malware-Spezialist könnte man fast ein wenig neidisch werden auf die neue »Konkurrenz«...

Josef Pichlmayr  
Geschäftsführer von IKARUS Software  
[www.ikarus.at](http://www.ikarus.at)  
[www.mymailwall.com](http://www.mymailwall.com)