"Ihr PC als Komplize": Piraten-Software gezielt bekämpfen

Mit Sicherheitslücken lässt sich viel Geld verdienen. Das wissen nicht nur die Hersteller von Schutzprogrammen, sondern auch die Programmierer von Viren, Würmern und Trojanern. Eine ganze Industrie lebt mittlerweile von Datenspionage, Spam-Versand und Erpressung von Online-Diensten. Private und geschäftliche PCs werden dabei unbemerkt für illegale Zwecke missbraucht. Wer seinen Rechner davor bewahren will, braucht neben den bisherigen Schutzmaßnahmen spezielle Anti-Rootkit-Programme, empfiehlt c't in der Ausgabe 2/07.

Auf der dunklen Seite lassen sich derzeit im Wesentlichen drei Geschäftsmodelle für das Ausnutzen von Sicherheitslücken beobachten: Spam, Spionage und Sabotage. Spam gibt den deutlichsten Hinweis auf den Erfolg der Botnetze: Im letzten halben Jahr stieg die lästige E-Mail-Werbeflut sprunghaft an. Spionage und Datenklau finden hingegen im Verborgenen statt und werden oft gar nicht publik.

Die Gefährlichkeit der Schadsoftware hat dadurch, dass sie mittlerweile nicht mehr vor allem Aufmerksamkeit erregen, sondern Geld einbringen soll, keineswegs gelitten. Sie nutzt teils noch unbekannte Sicherheitslücken, um sich auf fremden Computern einzunisten. Botnet-Clients versenden unter Kontrolle von außen Spam, spionieren Daten aus, laden bezahlte Werbung oder legen durch verteilte Denial-of-Service-Attacken fremde Server lahm. Sie verstecken sich durch Rootkit-Techniken erfolgreich vor Anti-Viren-Programmen, sodass sie – auch dank Flatrate – meist lange unentdeckt bleiben. So gelingt es, Netze aus zigtausend Bots aufzubauen. Diese werden dann an Auftraggeber vermietet. In solchen Netzen hängen nicht nur Computer unvorsichtiger Privatanwender, sondern auch Firmenrechner.

Wie auch aktuelle Tests von c't ergeben haben, kommt herkömmliche Anti-Viren-Software oft nicht gegen Rootkits an. Für den Zugang zu einem Botnetz oder für eine Software, die eine bisher noch unbekannte Lücke in Windows ausnutzt, erhalten Programmierer mitunter mehrere zehntausend Dollar. "Gegen ein unbekanntes Sicherheitsloch kann man sich kaum schützen", bilanziert c't in dem Schwerpunkt "Ihr PC als Komplize" in der aktuellen Ausgabe. "Schon beim Klick auf einen Link oder dem Öffnen einer präparierten Word-Datei kann sich ein Schädling einnisten, der dann kaum noch aufzuspüren ist."

Selbst wer Anti-Viren- und Anti-Rootkit-Tools nutzt, kann nicht völlig sicher sein, dass sein Computer mit DSL-Anschluss nicht ausspioniert wird oder gar Teil eines Botnetzes ist. Die Hersteller von Anti-Viren-Software haben inzwischen reagiert und versuchen, Rootkits mit speziellen Programmen aufzuspüren und zu entfernen. Im c't-Test zeigt sich, dass AVGs "Anti-Rootkit" sowie "Blacklight" von F-Secure recht zuverlässig arbeiten und gleichzeitig einfach zu bedienen sind. Profis finden in "Rootkit Unhooker" und "GMER" zwei Programme, die ihnen zusätzliche Informationen über gefundene Rootkits liefern. "Anti-Viren-Software und die Firewall bleiben dabei genauso wichtig bisher", betont c't. Wie immer bleibt aber festzuhalten: "Einen hundertprozentigen Schutz gibt es aber nicht." Und wer sich nur auf die Schutzsoftware verlässt und nicht mit einer gesunden Portion Misstrauen und Vorsicht mit E-Mail umgeht oder sich im Web bewegt, der hat gegen die Malware-Programmierer schon verloren.