Größe der Botnetze hat sich vervierfacht

Über die möglichen Ursachen für den Sprung der Zahl infizierter PCs in den vergangenen Monaten gibt es unterschiedliche Vermutungen.

Meldung vom 02.09.2008

In den vergangenen drei Monaten hat sich die Größe der Botnetze nahezu vervierfacht, wie eine Statistik der ShadowServer Foundation, einem Zusammenschluss mehrerer Sicherheitsspezialisten, die Botnetze, Malware und Phishing-Aktivitäten beobachten, nahelegt. Allerdings gibt es unterschiedliche Interpretationen über die möglichen Ursachen für diesen Sprung in der Zahl infizierter PCs.

Das Internet Storm Center (ISC) vermutet die groß angelegten SQL-Injection-Angriffe auf Webseiten dahinter, bei denen normalerweise harmlose Webseiten so manipuliert wurden und immer noch werden, dass der Besucher beim Aufruf der Seite über Lücken im Browser einen Schädling untergeschoben bekommt. Möglicherweise könnten die Bot-Herder neuerdings einen komprimittierten PC einfach länger unter ihrer Kontrolle halten, bevor dem Besitzer eine Anomalie oder einem Virenscanner die Infektion auffällt.

Nach Meinung von Thorsten Holz, einem der Mitgründer des Deutschen Honeynet-Projekts, dürften eher die Mail-basierten Angriffe der vergangenen Wochen und Monate dahinter stecken, bei denen sich die Schädlinge etwa als vermeintliche UPS-Rechnungen, Angelina-Jolie-Videos, Meldungen über den Einmarsch der USA in den Iran und nicht zuletzt als Olympia-Screensaver tarnten. Dafür spreche auch, so Holz gegenüber heise Security, dass ShadowServer hauptsächlich IRC-Botnetze beobachte, die nicht mit den SQL-Injection-Angriffen in Verbindungen stünden.

Interessante Beobachtungen zu Bot-Netzen machten kürzlich auch die Sicherheitsdienstleister FireEye und SecureWorks: Bei den beiden größten bekannten rivalisierenden Botnets Srizbi und Rustock gibt es Überschneidungen. Offenbar nutzt ein Auftraggeber beide Netze, um Spam-Mails zu versenden. Ungewöhnlich ist dabei auch die Beobachtung, dass über das Rustock-Netz E-Mails verschickt werden, die Srizbi-Bots verteilen.