P2P-Botnetz infiltriert und gestört

Ein Forscher-Team der Universität Mannheim und des Instituts Eurécom hat das Botnetz hinter dem Sturm-Wurm analysiert, infiltriert und die Kommunikation im Botnetz erfolgreich gestört.

Einem Forscher-Team der Universität Mannheim und des Instituts Eurécom ist es gelungen, das Botnetz hinter dem Sturm-Wurm zu analysieren, zu infiltrieren und schließlich empfindlich zu stören. In einer Forschungsarbeit, die sie auf der Usenix in San Francisco vor zwei Wochen vorgestellt haben, beschreiben die Experten Wege, wie man Peer-to-Peer-Botnetze allgemein ausforschen kann sowie Methoden, um die Kommunikation zwischen den Botnetz-Drohnen zu unterbinden.

Die Forscher um Thorsten Holz, einem der Mitgründer des Deutschen Honeynet-Projekts und Doktorand am Lehrstuhl für praktische Informatik an der Universität Mannheim, haben dazu zunächst das P2P-Protokoll untersucht, das die Drohnen des Sturm-Wurm-Netzes verwenden. Es handelt sich dabei um das Overnet-Protokoll, das etwa Edonkey nutzt. Allerdings haben die Bot-Bastler die Kommunikation leicht modifiziert.

Mit einem modifizierten Client für das Overnet konnten die Sicherheitsspezialisten dann das Botnet beobachten und dabei etwa die Befehle und deren Verbreitungswege mitschneiden. Das Neue an der Forschung der Gruppe ist jedoch, dass die Team-Mitglieder auch in die Botnetz-Kommunikation eingegriffen haben. Indem sie etwa die Botnetz-Clients mit gefälschten Befehlen überfluteten, konnten sie die Drohnen lahmlegen. Kurze Zeit nach dem Absetzen der Befehle ging die Kommunikation im Netz drastisch zurück, erholte sich nach einiger Zeit jedoch wieder.

Traditionelle Botnetze setzen auf einzelne Command-and-Control-Server wie einem IRC- oder Webserver, von dem die Drohnen im Netz die Befehle erhalten. Der Nachteil dieser Struktur für die kriminellen Drahtzieher hinter dem Botnetz ist, dass beispielsweise Sicherheitsbehörden nur den jeweiligen Server vom Netz nehmen müssen, um das Botnetz lahmzulegen.

Die Botnetzbetreiber weichen daher zunehmend auf zweischichtige P2P-Netze aus, bei denen die Drohnen die Befehle selbst weiterverteilen. Der Artikel Hydra der Moderne beleuchtet die Strukturen neuerer Botnetze und liefert weitere Hintergründe dazu. Durch diese neuen Strukturen lassen sich die Botnetzbetreiber schwieriger aufspüren, da die Quelle der Befehle kaum aufzudecken ist; außerdem ist das Botnetz nicht so einfach abzuschalten, da die Drohnen sowohl Client als auch Server darstellen und sich so nicht durch das Entfernen eines einzelnen Servers stören lassen. Das Forscher-Team um Holz liefert nun Ansätze, wie sich auch Botnetze der neueren Art bekämpfen lassen könnten.