Hacker: Storm-Botnet gekapert

Das Storm-Botnet wurde auf der Hackerkonferenz 25C3 live gehackt - und kann übernommen werden. Damit droht dem von Spammern errichteten Netzwerk aus infizierten PCs eine weitere Gefahr.

News – Newsredaktion Golem (uk) powered by golem.de – vom 30.12.2008

Noch besteht das Storm-Botnet aus etwa 100.000 Windows-PCs, schätzen die Redner des 25C3-Vortrags "Stormfucker: Owning the Storm Botnet". Ohne Wissen der meist ahnungslosen Besitzer versenden die Bots werbende oder mit Malware verseuchte E-Mails in alle Welt - mehrere Milliarden davon sollen bereits verschickt worden sein. Die Entwickler des Botnet können aus der Ferne neue Software aufspielen. Damit wäre es dann auch möglich, vertrauliche Daten auszuspionieren.

Seit allerdings Antivirensoftware auch das Storm-Botnet erkennt, soll selbiges deutlich geschrumpft sein. Soweit dokumentiert ist, seien bereits über 250.000 Rechner bereinigt worden, diese damit aus dem Storm-Botnet ausgeklinkt und selbiges damit stark geschrumpft. Doch auch mit den geschätzten 100.000 fernsteuerbaren Stormnodes - auch als Bots oder Zombies bezeichnet - ist dieses Botnet noch eine ernst zu nehmende Größe. Jeder Teil des Netzes kann beispielsweise als Wurmschleuder, SMTP-Relay oder DDoS-Angreifer dienen.

Das macht es auch interessant für Wissenschaftler und Hacker wie Georg "oxff" Wicherski, Mark Schlösser, Felix Leder und Tillmann Werner. Sie erklärten auf der 25C3 in Berlin, wie sie durch Reverse-Engineering die Funktionsweise des Storm-Botnet ergründet haben - sie beobachteten und beeinflussten Kommunikation und Speicherabbilder der Software. Und sie fanden heraus, wie sich das Botnet kontrollieren und angreifen lässt.

Bereits bekannt war, dass das Storm-Botnet ein modifiziertes eDonkey-Protokoll nutzt. Die frisch auf einem PC installierte Software kennt bereits einige Stormnodes und sucht dann weitere Knoten für die eigene Routingtabelle. Darüber machen sich die Stormnodes dann im Botnet auf die Suche nach weiteren Knoten und so genannten Command & Control Servern (C&C Server), um sich von letzteren ihre Befehle selbst abzuholen. Das kann der Versand von E-Mails oder die Installation von Software sein.

Die Entwickler des Storm-Botnets nutzen den Hakkern zu Folge bisher keine besonders sichere Verschlüsselung oder komprimieren die zwischen Knoten ausgetauschten Daten nur. Auch die Authentifizierung und das Einschleusen ausführbarer Dateien ist für die Hacker keine Hürde mehr, so dass es möglich wurde ins Botnet falsche C&C Server einzuschleusen und Bots nach dem Löschen installierter Botnet-Würmer unter die eigene Kontrolle zu bringen. Demonstriert wurde das Botnet-Hacking live in einer virtuellen Maschine.

Theoretisch lässt sich das ganze Botnet damit von einem Rechner aus lahmlegen. Allerdings würde dieser dann durch die Masse der Bots und sehr wahrscheinlich auch durch die wütenden Storm-Entwickler mit einer DDoS-Attacke getroffen. Ziel der Hacker ist deshalb eine "intelligente und schnelle und noch nicht fertige" verteilte Übernahme des Botnets.

Um die Sache zu beschleunigen und ihre Erkenntnisse auch anderen zukommen zu lassen, wollen die Hacker in Kürze ein selbst geschriebenes C-Programm veröffentlichen, das einen Teil der dafür nötigen Aufgaben bereits erledigt. Es ist also damit zu rechnen, dass es bald zu einem versteckten Kampf um Stormnodes kommt.