Tor-Betreiber warnen vor möglicher Enttarnung

31. Juli 2014

Monatelang haben Unbekannte das Tor-Netzwerk manipuliert und möglicherweise Daten gesammelt, die Nutzer identifizieren könnten. Die Betreiber hoffen, dass es wohlgesonnene Forscher waren.

Die Betreiber des Tor-Netzwerks haben Anfang Juli eine Reihe von Servern in ihrem Netzwerk entdeckt, die fünf Monate lang Verbindungen manipuliert haben. Eigentlich soll Tor der Anonymisierung von Internetnutzern dienen. Der Angriff richtete sich genau gegen diese Funktion. In einem Blogpost warnen die Betreiber, dass bei dem Angriff womöglich Daten gesammelt wurden, die zum Identifizieren von Tor-Nutzern beitragen könnten.

Betroffen sind demnach Nutzer und Betreiber von sogenannten Hidden Services, im Tor-Netzwerk versteckten Websites. Über bekannte Schwächen und bis dahin unbekannte Sicherheitslücken wurden demnach Verbindungen manipuliert und an verschiedenen Knotenpunkten miteinander verglichen. Tor schickt Verbindungen über mehrere solcher Knoten, um die Herkunft zu verschleiern. Zeitweise sollen die Angreifer 6,4 Prozent aller Tor-Knoten gestellt haben.

Diese Server wurden von den Betreibern mittlerweile entfernt. Außerdem wurde die Tor-Software verbessert, auch wenn die Angriffsmethode damit wohl nicht vollständig ausgeschlossen werden kann.

Angriff hat Tor-Nutzer in Gefahr gebracht

Wer hinter dem Angriff steckt, wissen die Tor-Betreiber nicht. Es könnte sich aber um zwei Forscher handeln, die eigentlich auf der anstehenden Hacker-Konferenz Black Hat von einer Methode berichten wollten, Tor-Nutzer zu enttarnen. Der Auftritt wurde jedoch abgesagt, weil der Arbeitgeber der beiden Forscher, die Carnegie Mellon University, angeblich keine Genehmigung dafür erteilt hatte.

Die Tor-Betreiber warnen, dass nicht nur die Angreifer versucht haben könnten, Daten zum Identifizieren von Nutzern zu sammeln. Durch die Art der Attacke sei dies auch anderen Beobachtern wie etwa einem Geheimdienst möglich gewesen. Selbst wenn die Angreifer eine gute Absicht verfolgten, hat ihre Attacke womöglich Menschen in Gefahr gebracht.

Denn genutzt wird das Tor-Netzwerk auch von Oppositionellen, Aktivisten und Journalisten, die ihre Kommunikation vor autoritären Regimen verstecken müssen. Die US-Regierung fördert die Entwicklung des Netzwerks deswegen, allein im vergangenen Jahr mit 1,8 Millionen Dollar.

Gleichzeitig versuchen sich Geheimdienste an Methoden zur Enttarnung von Nutzern, darunter die NSA und der britische GCHQ. Der russische Geheimdienst hat gerade eine Belohnung ausgelobt: Finden Hacker einen Angriffsweg, winken umgerechnet 82.000 Euro.