FBI hat alle Postfächer des Anonym-Dienstes Tor Mail

28. Januar 2014

«Freedom Hosting» war ein als «Hidden Service» konzipierter Webhosting-Dienst, auf dessen Servern mehrere prominente Websites des «Deep Webs» verfügbar gemacht wurden. Betreiber war Eric Eoin Marques. «Freedom Hosting» hat jedem Webspace zur Verfügung gestellt, ohne inhaltliche Ausschlusskriterien zu haben. Im Sommer 2013 wurde Eric Eoin Marques verhaftet, weil auf «Freedom Hosting» «Lolita City» und andere Kinderporno-Seiten betrieben wurden.

Kurz darauf waren alle «Freedom Hosting»-Seiten kurzfristig offline, meldeten dann aber «Down for Maintanance» (wegen Wartungsarbeiten nicht erreichbar). Allerdings lieferte diese Wartungsseite Malware an den Besucher aus. Der Schad-Code war in JavaScript geschrieben und in einem iframe versteckt. Er sendete die IP- und MAC-Adresse an einen vom Militärdienstleister SAIC betrieben Server in Virginia, wo in Langley auch der CIA ansässig ist.

Ende Januar 2014 offenbarte eine Anklageschrift wegen Kreditkartenbetrugs, dass das FBI offenbar im Besitz aller Postfächer von «Tor Mail» ist. Dieses Webmail-Angebot war nur über das Anonymisierungs-Netzwerk Tor zu erreichen. Nutzer konnten ohne Identifikation Postfächer anlegen. In der Anklageschrift heisst es, «das FBI hat im Zusammenhang mit einer anderen Ermittlung nach einem Rechtshilfeersuchen an Frankreich die Kopie eines französischen Servers erhalten, der Daten und Informationen des Tormail E-Mail-Server enthielt, darunter auch die Inhalte von Tormail E-Mail-Konten». An besagte Serverdaten gelangte das FBI zwischen dem 22. Juli 2013 und dem 2. August 2013. Obwohl das Rechtshilfeersuchen an Frankreich lediglich Kinderpornographie betraf, behält das FBI alle Daten und erwirkt bei Bedarf von einem U.S. Gericht einen Durchsuchungsbeschluss auch für andere Straftaten.

Die Betreiber des Tor-Netzwerks haben Anfang Juli 2014 eine Reihe von Servern in ihrem Netzwerk entdeckt, die fünf Monate lang Verbindungen manipuliert haben. In einem Blogpost warnen die Betreiber, dass bei dem Angriff womöglich Daten gesammelt wurden, die zum Identifizieren von Tor-Nutzern beitragen könnten.

Tor-Betreiber warnen vor möglicher Enttarnung

If You Used This Secure Webmail Site, the FBI Has Your Inbox

Anklageschrift Kredikartenbetrug

FBI hat Daten des Anonym-Dienstes Tor Mail

Schadsoftware enttarnt angeblich Tor-Nutzer