Schadsoftware enttarnt angeblich Tor-Nutzer

5. August 2013

Die irische Polizei verhaftet den Betreiber eines Dienstes, der versteckte Websites über das Tor-Netzwerk betreibt. Er soll Geschäfte mit Kinderpornografie gemacht haben. Nach der Verhaftung verbreiten seine Seiten einen Computer-Schädling - angeblich soll er die Identität von Tor-Nutzern enthüllen.

Irische Polizisten haben den Betreiber einer Internetfirma für verschlüsselte, im sogenannten Darknet versteckte Websites festgenommen. Der 28-Jährige wurde in Dublin verhaftet, berichtet der "Irish Independent". Die US-Bundespolizei FBI wirft dem Mann vor, einer der "weltweit grössten Unterstützer von Kinderpornografie" zu sein - und ersuchte bereits Ende Juli um seine Auslieferung nach Amerika. Die Verhaftung hat womöglich weitere Folgen: Tor-Nutzer fürchten, das FBI versuche nun mit Hilfe eines Virus, die Nutzer des Anonymisierungsdienstes zu enttarnen.

Eric Eoin M. soll der Betreiber von Tor Freedom Hosting sein, einer Internetfirma, die Webspace im sogenannten Darknet vermietet. Der Begriff bezeichnet Websites, die nur über den Tor-Anonymisierungsdienst erreicht werden können. Theoretisch können in diesem Netz sowohl die Surfer als auch die Website-Betreiber anonym bleiben.

Bei einem versteckten Dienst im Tor-Netzwerk wird zufällig ein Tor-Server als Treffpunkt ausgewählt. Dort werden die Anfragen und die Daten des Anbieters und des Abrufenden ausgetauscht, jeweils über drei sogenannte Tor-Relays, zwischengeschaltete weitere Rechner. Einer der bekanntesten versteckten Dienste ist Silkroad, ein anonymer Drogenmarkt - für den sich Polizeibehörden brennend interessieren.

Vorwurf: Verbreitung von Kinderpornografie

M.'s Festnahme gingen einjährige Ermittlungen des FBI voraus. Er soll die Verbreitung von Kinderpornografie und Darstellung von sexualisierter Gewalt an Kindern unterstützt haben, sagen die Behörden. Über sein Konto seien grosse Geldmengen geflossen. In den USA drohten ihm bis zu 30 Jahre Haft. Freiheit gegen Kaution wird ihm wegen Fluchtgefahr nicht gewährt. Die Verhandlung geht kommenden Donnerstag weiter. Wie gut die Chancen auf Auslieferung stehen, ist nicht klar. M. hat die irische und die amerikanische Staatsbürgerschaft.

Anders als in einem mittlerweile korrigierten ersten Bericht eines grossen IT-Fachdienste behauptet, ist M. weder Gründer noch Mitentwickler des Tor-Netzwerks. Er nutzte sich lediglich die Tor-Infrastruktur für seine darauf aufbauenden Dienste. Die Stiftung hinter Tor distanziert in ihrem Blog von Freedom Hosting: Die Person oder die Personen hinter dem Unternehmen hätten nie in Verbindung zu The Tor Project gestanden.

Schadprogramm jagt Kunden von Freedom Hosting

Doch die Geschichte um M. hat noch eine weitere Facette: Nach der Festnahme bemerkten Darknet-Surfer, dass die Websites und Foren von Tor-Freedom-Hosting-Kunden Schadcode

übertrugen: einen cleveren Javascript-Virus, der es auf Windows-Nutzer abgesehen hat, die mit Firefox surfen, mit der Firefox-Version, die im Tor Browser Bundle genutzt wird, einem Software-Paket, das auf jedem Rechner schnell eine Tor-Verbindung ermöglicht.

Zwar gibt es keine Hinweise auf einen Zusammenhang mit den FBI-Ermittlungen, doch behaupten viele Forenposter und Blogger, dass das Vorgehen "typisch" für das FBI sei, um Betreiber und Kunden von Kinderpornografie-Webangeboten ausfindig zu machen. Eine frühe Analyse des Schadcodes weist darauf hin, dass er einen Cookie auf dem Rechner des vermeintlich anonymen Surfers platziert, um so dessen echte IP-Adresse herauszufinden, sobald Tor deaktiviert ist.

Cookies zum Ausspähen der Identität von Tor-Nutzern?

Da Tor Freedom Hosting der vermutlich grösste Anbieter von Webhosting im Darknet ist, dürfte damit ein Grossteil der dortigen Websites kompromittiert sein und, so die Furcht, die Identität vieler Tor-Nutzer offengelegt sein - zumindest für das FBI.

Diese Befürchtungen greifen die Tor-Macher in ihrem Blog auf. Sie wissen nichts Genaues, versprechen eine genaue Überprüfung der Angriffe und versichern: "Derzeit sieht es so aus, als ob die Software von Freedom Hosting und nicht die von Tor geknackt wurde."

Hintergrund zum Tor-Netz

Abkürzung: Tor steht für "The Onion Router", einen Dienst, der wie eine Zwiebel mit ihren vielen Lagen auch den eigenen Internetverkehr durch verschiedene "Schichten" schickt, bevor er am Ziel ankommt. Wer über das Tor-Netzwerk auf welche Inhalte von wo aus zugreift, lässt sich schwer feststellen.

Nutzer: Nach Angaben der Tor-Betreiber nutzen ausser Journalisten, Staatsanwälten und Firmen sogar Mitarbeiter der U.S. Navy das Netzwerk, um ihre Spuren im Internet zu verwischen. Über Tor können Nutzer auch auf gesperrte Inhalte zugreifen, die beispielsweise im eigenen Land nicht zugänglich sind. Das betrifft nicht nur Nutzer in Ländern wie China oder Iran.

Infrastruktur: Der Tor-Dienst lebt vor allem von Privatpersonen und Freiwilligen, die ihren Rechner und einen kleinen Teil ihrer Internetverbindung mit anderen teilen. Sie dienen als Stationen, über die der Internetverkehr abgewickelt wird. Von einer wachsenden Zahl dieser sogenannten Relays - gerade wenn sie in privater Hand sind - profitiert das System: Das anonyme Internet wird schneller und sicherer, aber auch automatisch interessant für Überwacher.

Risiken: An Exit-Nodes können unverschlüsselte Inhalte belauscht werden. Ausserdem ist es theoretisch möglich, dass jemand den Verlauf der über das Tor-Netz vermittelten Daten nachvollziehen kann, wenn er viele Tor-Relays kontrolliert. Wer über Tor beispielsweise E-Mails verschickt, sollte diese verschlüsseln.