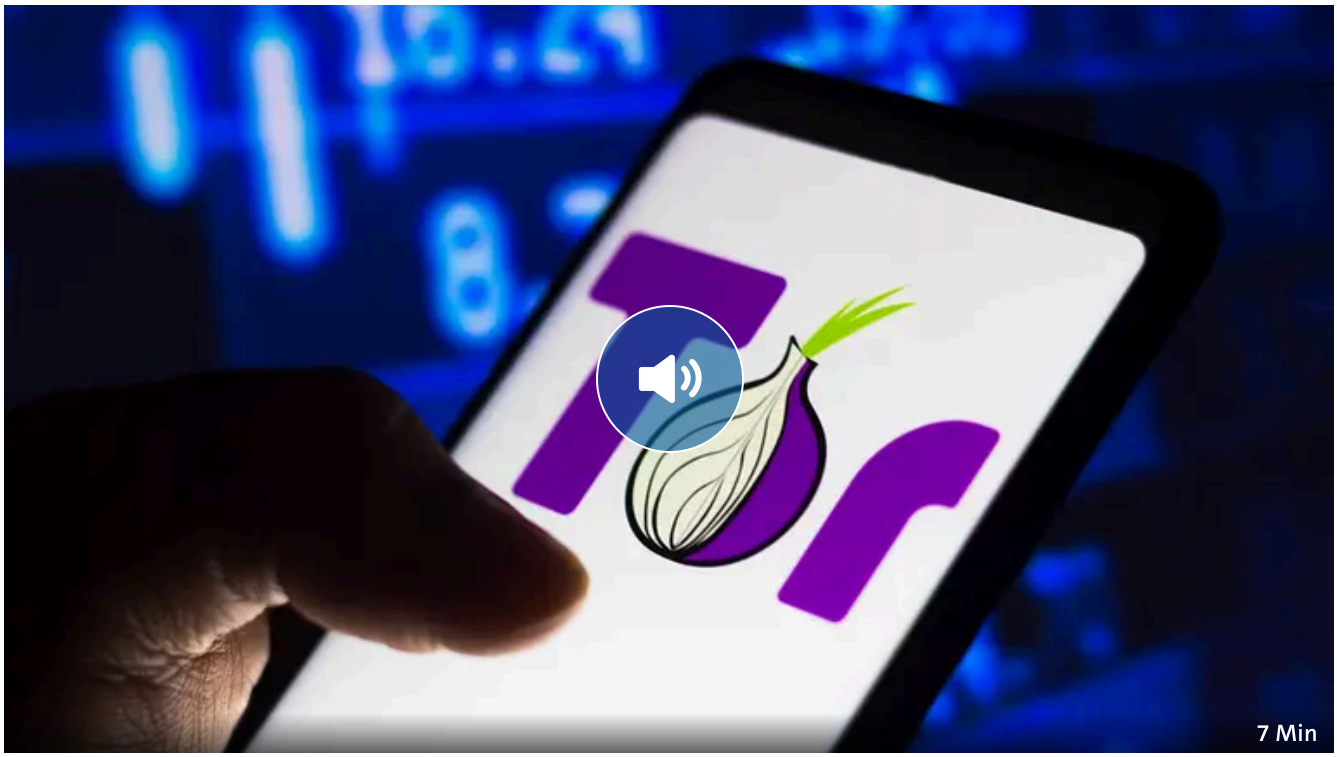
tagesschau



EXKLUSIV Ermittlungen im Darknet

Strafverfolger hebeln Tor-Anonymisierung aus

Stand: 18.09.2024 • 06:01 Uhr

Das Tor-Netzwerk gilt als wichtigstes Werkzeug, um sich anonym im Internet zu bewegen. Behörden haben begonnen, es zu unterwandern, um Kriminelle zu enttarnen. In mindestens einem Verfahren waren sie erfolgreich.

Strafverfolgungsbehörden in Deutschland lassen Server im Tor-Netzwerk teils monatelang überwachen, um Tor-Nutzerinnen und -Nutzer zu deanonymisieren. Besonders betroffen sind Seiten im sogenannten Darknet. Dies zeigen Recherchen des *ARD*-Politikmagazins *Panorama* und *STRG_F (funk/NDR)*.

Die bei der Überwachung gewonnenen Daten werden demnach in statistischen Verfahren so aufbereitet, dass die Tor-Anonymität gänzlich ausgehebelt wird. Reporter von *Panorama* und *STRG_F* konnten Unterlagen einsehen, die vier erfolgreiche Maßnahmen in nur einem Ermittlungsverfahren zeigen. Es sind die weltweit ersten belegten Fälle dieser sogenannten "Timing-Analysen". Bisher galt dies als quasi unmöglich.

Größtes Anonymisierungsnetzwerk der Welt

Bei Tor handelt es sich um das weltweit größte Netzwerk, um sich anonym im Internet zu bewegen. Tor-Nutzerinnen und -Nutzer leiten ihre Verbindung über Server, sogenannte Tor-Knotenpunkte, um zu verschleiern, was sie tun: Mit dem Tor-Browser können sie Websites im Internet anonym ansteuern oder Seiten im sogenannten Darknet aufrufen. Aktuell sind bei Tor fast 8.000 Knotenpunkte in rund 50 Ländern in Betrieb. Rund zwei Millionen Menschen sind hier täglich unterwegs.

Es ist bei Journalistinnen und Journalisten, aber auch Menschrechtsaktivistinnen und -aktivisten beliebt, gerade in Ländern, in denen das Internet zensiert ist. Auch in Deutschland betreiben Medien, darunter auch der *NDR*, im Tor-Netzwerk anonyme "Briefkästen", damit Whistleblower sicher Daten übermitteln können. Die *Deutsche Welle* etwa hat ihre Website im Darknet erreichbar gemacht, um der Zensur in einigen Ländern zu entgehen.

Unterwanderung des Tor-Netzwerkes

Die Anonymität lockt jedoch auch Kriminelle an, die über Tor beispielsweise Cyberangriffe verüben oder im Darknet illegale Marktplätze betreiben. Für Ermittlungsbehörden stellte Tor über Jahre hinweg eine technisch kaum zu überwindende Hürde dar. Recherchen von *Panorama* und *STRG_F* ergaben nun, dass sie ihre Strategie zuletzt offenbar erweitert haben, um Tor zu überwinden. Nötig dafür ist eine teils jahrelange Überwachung einzelner Tor-Knotenpunkte.

Die Logik hinter der Maßnahme, die Fachleute "Timing-Analyse" nennen: Je mehr Knotenpunkte im Tor-Netzwerk durch Behörden überwacht werden, desto wahrscheinlicher ist es, dass ein Nutzer seine Verbindung über einen der überwachten Knotenpunkte zu verschleiern versucht. Durch die zeitliche Zuordnung ("Timing") einzelner Datenpakete lassen sich so anonymisierte Verbindungen zum Tor-Nutzer zurückverfolgen, obwohl Datenverbindungen im Tor-Netzwerk mehrfach verschlüsselt sind.

Chatdienst "Ricochet" als Falle

Nach den Recherchen von *Panorama* und *STRG_F* waren das Bundeskriminalamt (BKA) und die Generalstaatsanwaltschaft Frankfurt am Main mit dieser Methode erfolgreich: Im Ermittlungsverfahren gegen die pädokriminelle Darknetplattform "Boystown" gelang ihnen mehrfach, Tor-Knoten zu identifizieren, die einem der Hintermänner dienten, um sich zu anonymisieren.

So ermittelte das BKA zweimal Tor-Knoten, mit denen sich vom damaligen "Boystown"-Administrator Andreas G. betriebene Plattformen ins Tor-Netzwerk verbanden. Dabei handelte es sich zum Beispiel um einen Chat, in dem sich führende Mitglieder verschiedener pädokrimineller Foren austauschten. Zweimal gelang es überdies,

sogenannte "Eintrittsserver" vom Chatdienst "Ricochet" zu identifizieren, den G. nutzte - es war der Durchbruch für das BKA. Zur finalen Identifikation verpflichtete das Amtsgericht Frankfurt am Main schließlich den Provider Telefónica, unter allen o2-Kundinnen und -Kunden herauszufinden, wer von ihnen sich zu einem der identifizierten Tor-Knoten verband.

Die Ermittlungen führten zur Festnahme von Andreas G. in Nordrhein-Westfalen. Im Dezember 2022 wurde er zu einer langjährigen Haftstrafe verurteilt. Das Urteil ist noch nicht rechtskräftig.

Zunehmende internationale Kooperation

Entscheidende Hinweise im "Boystown"-Verfahren erreichten das BKA aus den Niederlanden. Offenbar kein Zufall: In Deutschland, den Niederlanden und den USA werden die meisten Torknotenpunkte betrieben. Die verantwortliche Generalstaatsanwaltschaft Frankfurt am Main teilte auf Anfrage mit, eine "Timing Analyse" im "Boystown"-Verfahren weder bestätigen noch dementieren zu wollen. Auch das Bundeskriminalamt wollte sich dazu nicht äußern.

Reporter von *Panorama* und *STRG_F* konnten jedoch mit Personen sprechen, die unabhängig voneinander Kenntnis über breit angelegte Überwachungsmaßnahmen solcher Tor-Server haben. Die Zahl der überwachten Torknoten in Deutschland soll demnach in den vergangenen Jahren stark gestiegen sein. Auch die überwachten Daten legen nahe, dass diese für "Timing-Analysen" genutzt werden dürften.

Experten, die Rechercheunterlagen von *Panorama* und *STRG_F* einsehen konnten, bestätigten unabhängig voneinander die Rechercheergebnisse. So erklärt Matthias Marx, einer der Sprecher des Chaos Computer Clubs (CCC): "Die Unterlagen in Verbindung mit den geschilderten Informationen deuten stark darauf hin, dass Strafverfolgungsbehörden wiederholt und seit mehreren Jahren erfolgreich Timing-Analysen-Angriffe gegen ausgewählte Tor-Nutzer durchführten, um diese zu deanonymisieren."

Schwerer Schlag für das Tor Project

Die Enthüllungen sind ein schwerer Schlag für das Tor Project. Die gemeinnützige Organisation mit Sitz in den USA, die die Aufrechterhaltung des Anonymisierungsnetzwerkes sichern will, erklärte auf Anfrage, ihm sei bisher kein belegter Fall einer "Timing-Analyse" bekannt gewesen. Bisher deute allerdings nichts darauf hin, dass der Tor-Browser angegriffen worden sei: "Tor-Nutzer können den Tor-Browser weiterhin verwenden, um sicher und anonym im Internet zu surfen."

Matthias Marx vom CCC warnt vor den Konsequenzen der Maßnahme: "Diese technische Möglichkeit besteht nicht nur für Deutsche Strafverfolgungsbehörden zur Verfolgung

schwerer Straftaten, sondern gleichermaßen für Unrechtsregime bei der Verfolgung von Oppositionellen und Whistleblowern. Das Tor-Projekt ist daher jetzt unter Zugzwang, den Anonymitätsschutz zu verbessern."

Zur Startseite