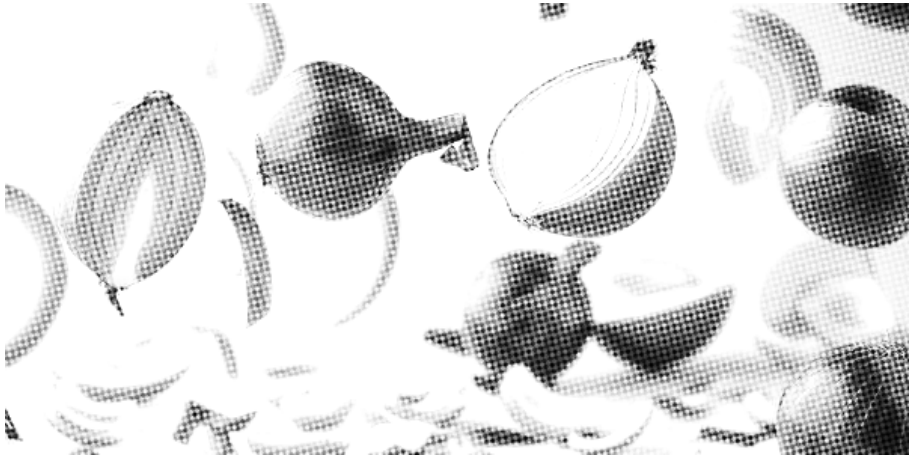
Mitte September wurde durch Recherchen des öffentlich-rechtlichen Rundfunks (Panorama und STRG_F) bekannt, dass das BKA und die Generalstaatsanwaltschaft Frankfurt a.M. erfolgreich einen Deanonymisierungsangriff im Tor-Netzwerk durchgeführt haben. […] Der Angriff wirft die Frage auf, ob Tor und Tails noch sicher sind. In diesem Text wagen wir den Versuch einer vorläufigen Auswertung auf Basis der spärlichen öffentlich zugänglichen technischen Informationen und geben einige Handlungsempfehlungen zur sichereren Verwendung von Tor.

No Trace Project / No trace, no case. Eine Sammlung von Werkzeugen um Anarchist:innen und anderen Rebell:innen zu helfen, die Fähigkeiten ihrer Feinde zu **verstehen**, Überwachungsanstrenungen zu **unterlaufen**, und letztlich zu **handeln** ohne geschnappt zu werden.

Abhängig von deinem Kontext, kann es sein, dass der Besitz bestimmter Dokumente kriminalisiert wird oder ungewollte Aufmerksamkeit auf sich zieht. Sei bedacht bezüglich der Broschüren, die du druckst und wo du sie lagerst.

„Ist das schon kaputt?“

Eine vorläufige Einordnung des Angriffs auf das Tor-Netzwerk



„Ist das schon kaputt?“ Eine vorläufige Einordnung des Angriffs auf das Tor-Netzwerk

Originaltext auf Deutsch

capulcu & friends

2024

capulcu.noblogs.org/post/2024/10/22/ist-das-schon-kaputt-eine-vorlaeufige-einordnung-des-angriffs-auf-das-tor-netzwerk

Layout

No Trace Project

notrace.how/resources/de/#ist-das-schon-kaputt

hinaus weisen. Wir stehen in unserer Diskussion erst am Anfang, möchten aber schon jetzt einige unserer Fragen teilen:

- Lohnt es sich das Tor-Netzwerk (als Teil autonomer Politik) zu stärken, weil es so wesentlich ist für die eigene Handlungsfähigkeit oder ist das eine Verschwendung von Ressourcen und damit eine Aufgabe, die bürgerliche Organisationen wie Reporter ohne Grenzen mit großem Spendenaufkommen besser erledigen können?
- Wie ist es wirklich bestellt um den Zustand des Tor-Netzwerks? Wie viele Knoten werden von Angreifern betrieben oder komplett überwacht und wie lange dauert es, bis wir davon erfahren? Wie schwierig sind Deanonymisierungsangriffe überhaupt noch in Zeiten internationaler Kooperation der Repressionsbehörden aus den Ländern, in denen die meisten Tor-Knoten stehen?
- Macht es mittelfristig Sinn eine grundlegende technische Überarbeitung/Erweiterung des Tor-Protokolls anzustreben? Wie sinnvoll wäre es etwa einen dauerhaften Cover-Traffic zu erzeugen oder Multipathing zu nutzen? Wie sinnvoll wäre es höhere Latenzen in Kauf zu nehmen, und in Richtung Mix-Netzwerke zu gehen, d.h. zufällige Verzögerungen bei der Weiterleitung der Datenpakete innerhalb des Netzwerks einzuführen, um Traffic Analysis zu erschweren?
- Welche politischen Konsequenzen hätte es, wenn Tor derart unsicher ist/wird, dass wir es trotz aller Zusatzmaßnahmen nicht mehr vertreten können, es für kritische Aktivitäten zu verwenden. Können wir dann überhaupt noch anonym im Internet unterwegs sein? Welche Konsequenzen hätte es für die Bewegung, wenn das nicht mehr ginge? Müssen wir jetzt damit anfangen uns auf einen solchen Fall vorzubereiten? Wie können wir wieder unabhängiger werden vom Internet bzw. vom „anonymen“ Internet?

dafür verantwortlich ist. Hier wird klassische Polizeiarbeit vermutlich recht erfolgreich sein.

- Für kritische Recherchen und Veröffentlichungen empfiehlt es sich, wechselnde Orte zu verwenden, die nicht schon durch vorherige Aktivitäten verbrannt sind. Dabei sollte man natürlich nicht beobachtet werden. Letzteres ist in Zeiten immer weitgehender Videoüberwachung (mit Gesichtserkennung) zunehmend schwieriger. Ein solches Vorgehen bietet aber auf jeden Fall einen Schutz gegenüber dem nun von Telefónica durchgeführten IP-Catching.
- Für kritische Recherchen und Veröffentlichungen aus öffentlichen Netzen empfiehlt es sich, randomisierte MAC-Adressen zu verwenden und sicher zu gehen, dass kein Fingerprinting der WLAN-Karte möglich ist. Dies ist am Einfachsten zu erreichen, indem Tails in Kombination mit einem externen WLAN-Adapter verwendet wird, der anschließend sicher entsorgt wird.[35]

Wir hoffen bald noch weitere praktische Maßnahmen empfehlen zu können und werden uns auch noch einmal genauer mit Tails beschäftigen, da dort keine persistenten Guard-Knoten verwendet werden. Das soll heißen: ggf. kommt noch ein weiterer Text zu dem Thema.

Welche strategischen Konsequenzen ziehen wir?

Die in Kooperation von Behörden aus mehreren Staaten erfolgreich durchgeführte Deanonymisierung eines Onion Services wirft strategische Fragen auf, die über den sicheren Einsatz von Tor und Tails als Werkzeuge der digitalen Selbstverteidigung

[35] Eine ausführliche Besprechung des Trackings von Geräten und mögliche Schutzmaßnahmen dagegen finden sich in „Deanonymisierung eures WLAN-Adapters trotz Tails?“, Autonomes Blättchen, Nr. 49.[a]

[a] https://autonomesblaettchen.noblogs.org/files/2022/06/nr49web.pdf

Mitte September wurde durch Recherchen des öffentlich-rechtlichen Rundfunks (Panorama und STRG_F) bekannt, dass das BKA und die Generalstaatsanwaltschaft Frankfurt a.M. erfolgreich einen Deanonymisierungsangriff im Tor-Netzwerk durchgeführt haben. Sie konnten so den Betreiber der Pädoplattform Boystown identifizieren und festnehmen. Dazu betrieben sie eigene Tor-Knoten und überwachten Teile des Netzwerks über mehrere Jahre und Ländergrenzen hinweg. Der Angriff wirft die Frage auf, ob Tor und Tails noch sicher sind. In diesem Text wagen wir den Versuch einer vorläufigen Auswertung auf Basis der spärlichen öffentlich zugänglichen technischen Informationen und geben einige Handlungsempfehlungen zur sichereren Verwendung von Tor. Denn Tor bleibt das beste verfügbare Werkzeug, um die eigene Identität im Internet zu verschleiern. Wer sich nur für die praktischen Folgen und nicht für die technischen Details des Angriffs interessiert, kann ab dem Abschnitt, Gesundheit des Tor-Netzwerks, S. 13 anfangen zu lesen.

Inhalt

chen Problemen ebenfalls durch die beschriebenen Angriffe verwundbar sind.

- Einen Onion Service über mehr als einen Monat zu betreiben, ist nicht empfehlenswert, wenn davon auszugehen ist, dass Repressionsorgane großen Aufwand betreiben werden, um diesen zu deanonymisieren. Das betrifft auch die dauerhafte Wiederverwendung etwa von OnionShare-Adressen.[34]
- Wenn ihr trotz der Risiken einen anonymen Onion Service betreiben möchtet, der nicht öffentlich bekannt sein muss, gebt die Adresse nur auf sicheren Kanälen weiter. Damit erschwert ihr es Ermittlungsbehörden, den Onion Service überhaupt zu finden und ihnen fehlt der Ansatzpunkt für den hier beschriebenen Angriff.
- Es ist nach allem, was wir bisher wissen, weiterhin relativ sicher den Tor-Client zu benutzen. Es ist auch sicherer Onion Services aufzurufen als die normalen Domainnamen, da die Daten in diesem Fall das Tor-Netzwerk gar nicht verlassen und die Kommunikation mit Onion Services immer authentifiziert und verschlüsselt ist.
- In den Einstellungen des Tor Browsers sollte eine möglichst hohe Sicherheitsstufe gewählt werden und Javascript deaktiviert sein, wenn es nicht unbedingt benötigt wird.
- Tor ist insbesondere dann unsicher, wenn sowohl der genutzte Dienst als auch der genutzte Internetzugang oder die Nutzer:in selbst bereits überwacht werden,31 d.h. wenn ich im überwachten Netzwerk im örtlichen Autonomen Zentrum mein Bekennerschreiben, bei einer ebenfalls überwachten Seite veröffentliche, stehen die Chancen für die Behörden nicht schlecht, dass sie das zuordnen können. Dann stellt sich nur noch die Frage, ob sie wissen, wer zu diesem Zeitpunkt im AZ war und möglicherweise

[34] Vgl. die Empfehlungen, wann Full Vanguards verwendet werden sollte.[a]
[a] https://spec.torproject.org/vanguards-spec/full-vanguards.html

(Guard-, Mittel-, Exit-Knoten) im Tor-Netzwerk trotz mehrfacher Versuche die bösartigen Knoten zu entfernen. Die Knoten wurden schließlich im November 2021 entfernt. Allerdings ist es für Tor ein praktisch kaum lösbares Problem, bösartige Knoten rechtzeitig zu entdecken und entfernen. Ein paar Zahlen zum Ausmaß von KAX17:

- Zeitweise wurden über 900 Knoten in über 50 verschiedenen AS's betrieben mit 155Gbit/s Bandbreite.
- Die Wahrscheinlichkeit einen KAX17-Knoten als Guard auszuwählen betrug maximal 16%.
- Die Wahrscheinlichkeit einen KAX17-Knoten als Mittelknoten auszuwählen betrug maximal 35%.
- Die Wahrscheinlichkeit einen KAX17-Knoten als Exit-Knoten auszuwählen betrug maximal 5%.
- KAX17 versuchte in Diskussionen aktiv Einfluss darauf zu nehmen, bösartige Knoten nicht aus dem Netzwerk zu entfernen.

Die Tatsache, dass so wenige Exit-Knoten betrieben wurden und so viele Mittelknoten deutet darauf hin, dass ein Ziel von KAX17 Deanoymisierungsangriffe gegen Onion Services gewesen sein könnten.

Soll ich Tor weiter nutzen?

Nach all dem stellt sich die Frage: Soll ich Tor (weiter) nutzen und wie viel Vertrauen kann ich in die Anonymisierung durch Tor setzen? Eine pauschale Antwort ist schwierig, da es darauf ankommt, wozu genau Tor genutzt wird und gegen welche Angreifer:innen ich mich schützen möchte. Dennoch hier ein paar allgemeine Überlegungen:

- Es ist immer besser offline zu machen, was möglich ist.
- Tor ist das beste Werkzeug, das wir haben. Es ist auf jeden Fall besser, online Tor zu verwenden als keine Werkzeuge zur Anonymisierung oder etwa VPNs, die neben zusätzli-

Wie funktioniert Tor?

Bevor wir auf die technischen Details des Angriff eingehen, fassen wir kurz zusammen, wie Tor funktioniert.[1] Tor kann sowohl eingesetzt werden, um staatliche Zensur zu umgehen als auch um die eigene Identität bzw. den Aufenthaltsort im Internet zu verbergen. Für diesen Text interessiert uns nur der Einsatz von Tor als Werkzeug zur Anonymisierung im Internet.

Betrachten wir zunächst den Fall, dass wir anonym eine Webseite abrufen wollen, z.B. radikal.news. Dazu benutzen wir den Tor Browser. Einen Überblick über die folgende Beschreibung einer Tor-Verbindung liefert Abbildung 1. Nach Eingabe der Adresse wählt die Tor Software aus den etwa 8000 Servern des Tor-Netzwerks,[2] auch Knoten oder relays genannt, drei zufällige aus. Zunächst wird eine verschlüsselte Verbindung zum ersten Knoten, dem Guard, aufgebaut, dann von dort zum Mittelknoten und vorn dort weiter zum Exit-Knoten. Erst der Exit-Knoten löst den Domainnamen radikal.news in eine IP-Adresse auf und baut eine Verbindung zum Webserver an dieser Adresse auf. Dabei verschlüsselt der Tor Client (in diesem Fall der Tor Browser) die Anfrage an radikal.news je Tor-Knoten einmal. Jeder Knoten auf dem Weg zum Ziel entfernt eine Verschlüsselungsschicht—daher auch das Bild der geschälten Zwiebel. Durch dieses Prinzip wird erreicht, dass keiner der Knoten des Tor-Netzwerks ausreichende Informationen hat, um uns, den Client, mit dem Webserver zu verknüpfen. Der Guard-Knoten sieht nur, dass wir uns mit dem Tor-Netzwerk verbinden und welchen Mittelknoten wir verwenden. Der Exit-Knoten sieht zwar, dass eine Anfrage an radikal.news zugestellt wird, aber er sieht nur, dass er sie von irgendeinem Mittelknoten weitergeleitet wurde und nicht woher sie stammt. Der Mittelknoten sieht nur den Guard und den Exit-Knoten. Er weiß gar nicht, wessen

[1] Wer genauer erfahren möchte, wie Tor funktioniert und was bei der Verwendung zu beachten ist, sollte einen Blick in unsere Tails-Broschüre.[a]

[a] https://capulcu.noblogs.org/neue-texte/bandi

[2] https://metrics.torproject.org/networksize.html

Kommunikation er weiterleitet. An dieser Stelle sei erwähnt, dass es sehr wichtig ist Transportverschlüsselung[3] zu verwenden, um zu verhindern, dass der Exit-Knoten alle Kommunikation mit dem Zielserver im Klartext mitlesen kann.[4]

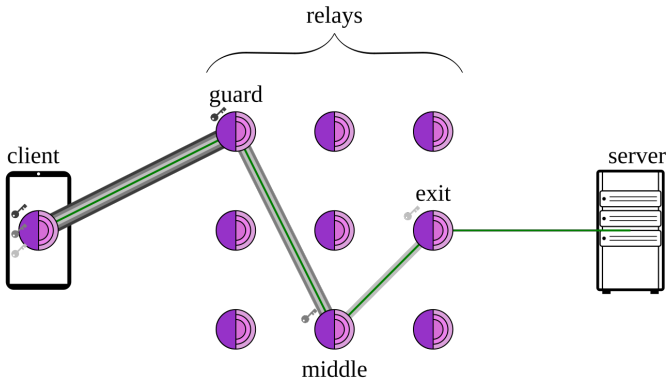


Abbildung 1: Die Abbildung zeigt, wie der Client sich über drei Tor-Knoten mit dem Server verbindet. Dabei entfernt jeder Knoten eine Verschlüsselungsschicht, so dass sie jeweils nur ihre Nachbarn kennen. Quelle.[5]

Mit diesem Verfahren wird technisch sichergestellt, dass der Internetprovider lediglich sieht, dass wir uns mit Tor verbinden und der Webserver andererseits lediglich sieht, dass ein beliebiger Tor-Nutzer eine Anfrage schickt—jedenfalls gilt das solange wir nichts tun, das uns identifiziert, etwa uns in einen nicht-anonymen Account einzuloggen. Tor ist also so designt, dass es sowohl vor Angriffen schützt, die darauf abzielen herauszufinden, wer etwas macht, als auch was eine bereits verdächtige Person macht.

[3]Transportverschlüsselung meint hier, dass die Kommunikation zwischen dem Tor Browser und dem Webserver unabhängig von Tor verschlüsselt ist. Der Tor Browser verwendet standardmäßig Transportverschlüsselung mittels HTTPS (im Unterschied zu HTTP, wo die Daten für den Exit-Knoten les- und veränderbar wären).

[4]Der Vollständigkeit halber: auf dem Weg zurück zum Client kehrt sich das Prinzip um, d.h. die Antwort des Webservers wird von jedem Knoten einmal zusätzlich verschlüsselt und erst der Client entfernt beim Erhalt der Nachricht alle drei Verschlüsselungsschichten.

[5]https://en.wikipedia.org/wiki/File:Tor_Circuit_Diagram.svg

gleich selbst von den Behörden betrieben. Es stellt sich also die Frage, ist das Tor-Netzwerk noch gesund oder kontrollieren die Ermittlungsbehörden in den USA und der EU schon so weite Teile, dass wir sie als globalen Angreifer betrachten müssen?

Diese Frage lässt sich nicht ohne Weiteres beantworten. Denn prinzipiell ist es möglich Tor-Knoten anonym zu betreiben. Auch wissen wir derzeit noch relativ wenig darüber, welchen Umfang die Kooperation der Behörden unterschiedlicher Jurisdiktionen tatsächlich hat. Geschieht dies nur bei großen Pädoplattformen oder ist es längst gängige Ermittlungspraxis? Sicher ist jedoch, dass das Tor-Netzwerk nicht divers genug aufgestellt ist. Ein Großteil der existierenden Knoten befindet sich in wenigen EU-Staaten und den USA. Außerdem stehen die Tor-Knoten in verhältnismäßig wenig Rechenzentren, d.h. sie befinden sich in wenigen AS's und ihr Traffic geht durch die gleichen Internet Exchange Points (IXPs).[31][32]

Die Zeit der Ermittlungen gegen Boystown fällt zusammen mit dem bisher größten bekannt gewordenen Betrieb von Tor-Knoten durch einen bösartigen Akteur: KAX17.[33] Es ist möglich, aber nicht gesichert, dass diese Knoten u.a. für die oben geschilderten Angriffe genutzt wurden. Auch wenn die Absichten von KAX17 letztlich nicht bekannt sind, erwähnen wir den Fall. Denn er zeigt exemplarisch, wie anfällig, das Tor-Netzwerk gegenüber motivierten Angreifern mit großen Ressourcen, also z.B. staatlichen Stellen ist. Diese sind in der Lage, so große Teile des Netzwerks über ländere Zeit hinweg selbst zu betreiben, dass Angriffe, wie die oben beschriebenen, überhaupt erst möglich werden. KAX17 betrieb mindestens von 2017 bis November 2021 zahlreiche Knoten in allen Position

[31]IXPs werden die Schnittstellen genannt, an denen viele unterschiedliche AS's (z.B. Internet Provider) ihre Daten austauschen. Daher sind IXPs für eine weitflächige Überwachung des Datenverkehrs besonders prädestiniert. Der weltweit größte IXP befindet sich in Frankfurt a.M.

[32]https://metrics.torproject.org/bubbles.html#as

[33]https://nusenu.medium.com/is-kax17-performing-de-anonymization-attacks-against-tor-users-42e566defce8

einen längeren Zeitraum beibehalten wird, sondern auch die verschiedenen Ebenen der Mittelknoten. Durch diese Veränderung wird es für einen Angreifer wesentlich unwahrscheinlicher und damit aufwendiger, den Mittelknoten nach dem Guard zu kontrollieren und so den Guard-Knoten aufzuspüren.[29] Allerdings sollte an dieser Stelle auch erwähnt werden, dass die Vanguards-Erweiterung zwar 2018 als Add-On veröffentlicht, jedoch erst 2022 in der Lite-Variante in C-Tor implementiert wurde. 2020 hätte es also noch manueller Zusatzschritte bedurft, um Vanguards zu nutzen.

Das Tor Project schätzt den Angriff so ein, dass er nur gegen Onion Services durchgeführt werden konnte, insbesondere weil nur hier der Angreifer in der Lage ist, Tor dazu zu zwingen, neue Verbindungen aufzubauen. Verbindungen von einem Client seien demnach weiterhin sicher. Allerdings zeigt aus unserer Sicht die prinzipielle Machbarkeit eines solches Angriffs, dass—ausreichende Motivation der Geheimdienste und Ermittlungsbehörden vorausgesetzt—in Zukunft möglicherweise vergleichbare Angriffe auch gegen Tor-Clients erfolgreich durchgeführt werden könnten. Außerdem gibt es insbesondere bei aktiviertem Javascript oder Anwendungen, bei denen über einen längeren Zeitraum Daten fließen, wie Instant Messaging auch für Clients eine erhöhte Anfälligkeit gegenüber Guard-Discovery-Angriffen bzw. den darauf folgenden Angriffsschritten.[30]

Gesundheit des Tor-Netzwerks

Das Neuartige an dem Angriff auf die Tor-Anonymisierung ist, dass nun offenbar erstmals bestätigt ein theoretisch schon immer für möglich gehaltener Angriff von Ermittlungsbehörden praktisch erfolgreich durchgeführt worden ist. Um dies zu erreichen, wurden bedeutende Teile des Tor-Netzwerks überwacht oder

[29] https://blog.torproject.org/announcing-vanguards-for-arti

[30] https://petsymposium.org/popets/2022/popets-2022-0026.pdf

Die Sicherheitsgarantien gelten allerdings nicht gegenüber einem globalen Angreifer. Das bedeutet, wenn ein Angreifer in der Lage ist, sowohl an meinem zufällig gewählten Guard-Knoten als auch am Exit-Knoten die ein- und ausgehenden Pakete zu überwachen. Dann kann er die an den Webserver gesendete Anfrage mit hoher Wahrscheinlichkeit mir zuordnen. Tor hat nicht den Anspruch gegen solche globalen Angreifer zu schützen, da dies große Verzögerungen (Latenzen) in der Kommunikation mit sich bringen würde.[6]

Um es auf Dauer, d.h. über viele Verbindungen hinweg unwahrscheinlicher zu machen, dass ein Guard-Knoten ausgewählt wird, der von einem Angreifer betrieben wird, wählt Tor nicht bei jeder Verbindung einen neuen Guard, sondern verwendet einen einmal ausgewählten Guard-Knoten über einen zufälligen Zeitraum von mehreren Wochen.[7] Dadurch wird es für einen Angreifer, der nur einen kleinen Teil des Netzwerks überwachen kann, sehr lange dauern bis ein für einen Angriff geeigneter Guard-Knoten ausgewählt wird. Dieser Schutzmechanismus wird für den hier diskutierten Angriff noch relevant. Dazu später mehr.

Was sind Onion Services?

Der nun öffentlich gewordene Angriff richtete sich gegen einen Onion Service. Neben der schon beschriebenen Anonymisie-

[6] https://svn-archive.torproject.org/svn/projects/design-paper/tor-design.html

[7] Bei Verwendung von Tor in Tails trifft dies nicht zu, da Tails den Zustand von Tor mit jedem Neustart verwirft. Die Tails-Entwickler:innen sind sich bewusst,[a] dass die fehlende Verwendung von persistenten Guard-Knoten die Anfälligkeit gegenüber Deanonymisierungsangriffen wie dem hier diskutierten erhöht. Die Verwendung von persistenten Guard-Knoten hat jedoch insbesondere bei Verwendung von Tails an unterschiedlichen Orten auch Nachteile, da sie ein Tracking anhand der IP-Adresse der Guard-Knoten ermöglichen kann.

[a] https://gitlab.tails.boum.org/tails/blueprints/-/wikis/persistent_Tor_state

rung des Clients ermöglicht es Tor, selber anonym Dienste als sogenannte Onion Services anzubieten, beispielsweise einen Webserver zu betreiben, ohne dass die Besucher:innen der Webseite erfahren, wo der Server steht bzw. wer ihn betreibt. Einen Überblick über eine aufgebaute Verbindung zwischen Client und Onion Service bietet Abbildung 2. Der Onion Service hält dauerhaft Verbindungen zu einem oder mehreren als Introduction Points (IP)[8] bezeichneten Tor-Knoten aufrecht.[9] Die ausgewählten IPs veröffentlicht der Onion Service als Onion Service Descriptor in den Hidden Service Directories (HSDirs), einer über das Netzwerk verteilten Datenstruktur, sodass (nur) diejenigen, die die Onion-Adresse kennen, abfragen können, über welche IPs sie den Service erreichen.[10] Wenn der Tor-Client sich mit dem Onion Service verbinden möchte, wählt er zunächst einen weiteren Knoten aus, den sogenannten Rendezvous Point (RP) und baut eine Verbindung dorthin auf. Anschließend baut er eine Verbindung zu einem IP auf und teilt dem Onion Service darüber verschlüsselt die Adresse des RP mit. Daraufhin verbindet sich auch der Onion Service mit dem RP und Client und Onion Service können über den RP kommunizieren, ohne den Standort des jeweiligen Gegenübers zu kennen.

[8] Wir kürzen Introduction Point mit IP ab und Internet Protokoll Adresse mit IP-Adresse.

[9] Mit Verbindungen sind hier und im Folgenden sogenannte Tor-Circuits gemeint, also keine direkten Verbindungen, sondern eine wie oben beschriebene mehrfach verschlüsselte Verbindung über mindestens drei Knoten.

[10] An dieser Stelle gibt es gravierende Unterschiede zwischen v2 und v3 Onion Services. V2 Onion Services sind veraltet und inzwischen abgeschaltet. Wir verzichten auf eine detaillierte Erörterung der Unterschiede.

Fest steht, dass zur Deanonymisierung des Onion Services eine ganze Reihe anspruchsvoller, aufwendiger und langwieriger Angriffe verknüpft werden musste. Wir müssen davon ausgehen, dass die internationale Kooperation der Behörden und die technischen Fähigkeiten in den vier Jahren seit diesem Angriff nicht abgenommen haben.[27] Vermutlich ist es auch kein Zufall, dass der erste öffentlich bekannt gewordene Fall dieser Art Ermittlungen gegen eine Pädoplattform betrifft—dürfte die gesellschaftliche Akzeptanz gegenüber weitreichenden Überwachungsmaßnahmen wie bei Telefónica hier am größten sein.[28]

Wie reagiert das Tor Project?

Das Tor Project ist die Organisation, die sich um die Entwicklung der Tor Software, die Betreuung der Community und die Überwachung der Gesundheit des Netzwerks kümmert—wobei die letzten beiden Punkte auch maßgeblich durch andere Organisationen mitgetragen werden. In einem Blogpost[18] hat sich das Tor Project zu den Angriffen geäußert und insbesondere mehr Informationen erbeten, um den Angriff im Detail besser verstehen zu können und mögliche Gegenmaßnahmen ergreifen zu können. Außerdem weist die Organisation darauf hin, dass der Angriff gegen den seit vielen Jahren nicht mehr weiterentwickelten Tor-basierten Messenger Ricochet u.a. deswegen möglich wahr, weil inzwischen ausgerollte Verbesserungen bei der Auswahl der Knoten einer Verbindung nicht verwendet wurden. Konkret handelt es sich dabei um die Erweiterung Vanguards, die sogenannte Guard-Discovery-Angriffe vor allem dadurch erschweren soll, dass nicht nur der Eintrittsknoten über

[27] Während des Schreibens dieses Artikels wurde eine weitere große Pädoplattform im Darknet deanonymisiert.[a]

[a] https://www1.wdr.de/nachrichten/ruhrgebiet/erfolgreicher-schlag-gegen-kindesmissbrauch-100.html

[28] Ob das angeordnete „IP-Catching“ zur Ermittlung der IP-Adresse des Verdächtigen rechtmäßig war, wurde aufgrund seines Geständnisses im Prozess nicht festgestellt und ist zumindest fragwürdig.

Telefónica alle 43 Millionen Kund:innen für drei Monate überwachen sollte, um herauszufinden, welche davon sich mit dem identifizierten Guard-Knoten verbinden.[21] Bereits nach wenigen Tagen konnten die Behörden den Betreiber von Boystown auf diese Weise identifizieren. Unklar bleibt, woher die Ermittler:innen wussten, dass der Verdächtige Telefónica-Kunde ist. Angeblich erhielt das BKA einen Tipp von einer ausländischen Behörde. Doch auch dann lässt sich nur spekulieren, woher die Eingrenzung auf Telefónica stammt. Wahrscheinlich ist, dass die Behörden nach der erfolgreichen Aufdeckung des Guard-Knotens weitere Netzwerkanalysen durchgeführt haben, durch die sie zwar nicht direkt die IP-Adresse des Onion Services, aber zumindest das Autonome System (AS)[22] ableiten konnten. Dieses Vorgehe wurde möglich, weil erstens der Guard-Knoten bereits bekannt war und zweitens die Angreifer (wie oben beschrieben) selbst bestimmen konnten, wann Daten in Form von Chatnachrichten zwischen dem Guard-Knoten und dem Onion Service gesendet wurden. Denkbar wären solche Analysen auf aggregierten Flussdaten zwischen AS's etwa mit dem Protokoll Netflow, das auf den meisten Internetroutern läuft und zu deren Monitoring entwickelt worden ist. Forschungen[23][24][25][26] zeigen, dass es unter Umständen schon reichen kann, auf die Netflow Records normaler Internetrouter zuzugreifen, die sich in der Nähre des bekannten Guard-Knoten befinden, um den Kreis der Verdächtigen etwa auf ein AS einzugrenzen. Bis zur Veröffentlichung weiterer Details bleiben solche Überlegungen jedoch spekulativ.

[21] https://tagesschau.de/investigativ/panorama/telefonueberwachung-telefonica--bka-ermittlungen-paedokriminelle-100.html

[22] Das Internet ist kein flaches Netzwerk, sondern setzt sich aus vielen Teilnetzwerken, den AS's zusammen. Diese werden jeweils von unterschiedlichen Anbieter:innen selbständig betrieben.

[23] https://murdoch.is/papers/pet07ixanalysis.pdf

[24] https://mice.cs.columbia.edu/getTechreport.php?techreportID=1545&format=pdf

[25] https://ieeexplore.ieee.org/document/9408011

[26] https://spec.torproject.org/proposals/344-protocol-info-leaks.html

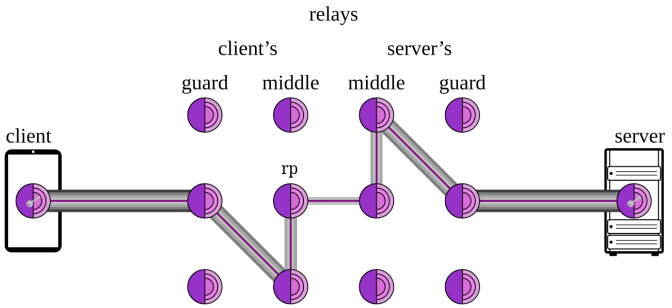


Abbildung 2: Die Abbildung zeigt, wie sich der Client mit dem Onion Service verbindet. Beide Seiten bauen dazu einen Circuit zu dem vom Client gewählten RP auf. Für den ersten Teil des Verbindungsaufbaus über den IP funktioniert dies analog. In dem Fall wäre der IP der Knoten rechts von dem der hier als RP bezeichnet ist. Quelle (von uns bearbeitet).[5]

Der Deanonymisierungsangriff mittels Traffic Analysis

Reporter von Panorama und STRG_F haben recherchiert,[11][12] dass das BKA und die Generalstaatsanwaltschaft Frankfurt am Main in den Ermittlungen gegen die Pädoplattform Boystown[13] (ein Onion Service) mehrere Timing Analysen, auch Traffic Analysis genannt, erfolgreich durchführten. Diese Art von Angriff ist möglich, da Tor ein Anonymisierungsnetzwerk mit niedriger Latenz ist. Dadurch können Sequenzen gesendeter Pakete (z.B. nach Anzahl, zeitlichen Abständen, Umfang des Datenverkehrs etc.), die an verschiedenen Punkten im Netzwerk korrelieren, mit einfachen statistischen Mitteln verknüpft werden. Um den Angriff erfolgreich durchzuführen, betrieben die Behörden über Jahre eigene Tor-Knoten und überwachten

[11] https://ndr.de/fernsehen/sendungen/panorama/aktuell/Anonymisierungsdienst-Tor-angreifbar-Snowden-Effekt-verpufft,tor192.html

[12] https://tagesschau.de/investigativ/panorama/tor-netzwerk-100.html

[13] Boystown war eine der größten Darknet-Pädoplattformen aller Zeiten mit zeitweise 400.000 Nutzer:innen.

bestehende Knoten über mehrere Monate hinweg. Zudem kooperierte das BKA mindestens mit niederländischen Behörden in der Überwachung des Tor-Netzwerks. Deutschland und die Niederlande sind die beiden Länder, in denen mit Abstand die meisten Tor Server betrieben werden.[14] Daher kann bei einer Kooperation der Behörden dieser Länder zumindest theoretisch ein signifikanter Teil des Netzwerks überwacht werden. Mittels des Betriebs eigener Knoten und der oben genannten Traffic Analysis gelang es den Behörden mindestens viermal den Guard-Knoten von Verdächtigen aufzudecken. Dieser sogenannte Guard-Discovery-Angriff war der erste Schritt in der Deanonymisierung des Onion Services: Er lieferte die IP-Adresse des Guard-Knotens und damit den Ansatzpunkt für weitere Angriffe auf die Anonymität des Onion Service selbst.

Die erfolgreiche Deanonymisierung gelang, weil die Behörden einen langen Atem bewiesen und mehrere sehr schwer zu bewerkstelligende Teil-Angriffe miteinander verknüpften. Nach allem, was wir wissen, lassen sich als grober Überblick mindestens die folgenden Schritte herauskristallisieren:[15]

1. Identifikation des Angriffsziels (Onion-Adresse)[16]
2. Betrieb eigener[17] bzw. Überwachung existierender Tor-Knoten
3. Guard-Discovery-Angriff mittels Timing Analyse
4. Eingrenzung der IP-Adresse des Ziels auf das Telefónica-Netz
5. IP-Catching durch Telefónica

[14] https://metrics.torproject.org/bubbles.html#country

[15] Die Schritte 2-4 sind als direkte Angriffe gegen Tor und nicht unabhängig voneinander zu betrachten. Schritt 3 wäre ohne 2 z.B. so nicht möglich gewesen.

[16] Es ist unklar, ob dies durch klassische Polizeiarbeit gelang oder durch einen weiteren Angriff gegen v2 Onion Services: onion address harvesting. Möglicherweise gelang es den Ermittler:innen auch die Community zu infiltrieren und so Zugang zu den Chats zu erhalten. Das uns nicht bekannt.

[17] Dies wird auch als Sybil attack bezeichnet.

Wir wollen nun einige dieser Schritte detaillierter beleuchten. Laut dem Tor Project basierte der konkrete Angriff darauf, dass der Verdächtige den seit 2017 nicht mehr weiterentwickelten Messenger Ricochet verwendete.[18] Immer wenn der Messenger online ist, erstellt er einen Onion Service, über den Nachrichten ausgetauscht werden können.[19] Die Adresse des Onion Services ist zugleich die Nutzer:innen-ID. Sie bleibt daher dauerhaft gleich und es ist anhand des Onion Service Descriptor in Echtzeit ersichtlich, wann die Betreiber:in online ist. Die Behörden nutzten bei dem Angriff auf Ricochet aus, dass es möglich ist, beliebig viele Nachrichten, beliebiger Größe an den Onion Service zu schicken. Dabei erstellt der Onion Service jedes mal eine neue Verbindung zu einem RP. Es ist also nur eine Frage der Zeit, bis ein vom Angreifer kontrollierter Mittelknoten gewählt und damit auch die IP-Adresse des Guard-Knoten bekannt wird. Da der Angreifer den Datenfluss kontrolliert, d.h. selbst bestimmt, wann er Nachrichten sendet, kann er sehr leicht einen verdeckten Kanal innerhalb des Torprotokolls oder einen Seitenkanal ausnutzen, z.B. über Verzögerungen der einzelnen Pakete, die zu einer Nachricht gehören. So lässt sich am vom Angreifer kontrollierten Mittelknoten feststellen, dass es sich tatsächlich um die gesuchte Verbindung zum Onion Service handelt.[20]

Nachdem der Guard-Knoten identifiziert war, ordnete das Amtsgericht Frankfurt a.M. am 17. Dezember 2020 an, dass

[18] https://blog.torproject.org/tor-is-still-safe

[19] Ricochet verwendete noch die inzwischen abgeschalteten v2 Onion Services. Diese können von den HSDirs gefunden werden. Es ist unklar, woher die Behörden die Adresse dieses Onion Services hatten, z.B. ob diese durch klassische Ermittlungsarbeit zu erfahren war oder ob auch HSDirs betrieben haben, um den verdächtigen Service zu finden.

[20] Prinzipiell lässt sich ein vergleichbarer Angriff auch gegen Echtzeitanwendungen fahren, die nicht auf einem Onion Service basieren (z.B. ein über Tor anonymisierter Jabber-Chat). Allerdings werden hier nicht beliebig schnell neue Verbindungen (Circuits) vom Tor-Client erstellt und der Angriff würde erheblich länger benötigen, bis ein bösartiger Mittelknoten ausgewählt wird.