
TOR

Geschrieben von Anonymus - 2007/10/04 21:59

Hallo!
wer anonym surfen will, dem empfehle ich die OpenSource Software TOR. Mit der wird man über verschiedene Server geleitet, sodass die andere Seite nicht weiss von welcher IP die Anfrage eigentlich stammt.

Ein Haken hat die Sache aber, es schleift ganz schön, wenn man damit surft. Allerdings gibt es auch ein Plug-In für den Firefox, bei dem man einfach via Button Tor an und ausstellen kann!

=====

Re:TOR

Geschrieben von Matthias Mansfeld - 2007/10/04 22:36

Nix gegen TOR - aber den letzten beißen die Hunde (Exit-Node) - siehe <http://www.heise.de/newsticker/meldung/96070>. TOR hat auch so seine vielen Seiten. Eventuelle VDS trübe u.U. TOR-Nodes genauso (Rechtsauffassung schwammig wie Äblich), und ob mir ein TOR-Node in China oder einer, den NSA betreibt, sympathisch ist, weiß ich nicht. Der Weisheit allerletzter Schluß ist TOR auch nicht immer...
<http://www.heise.de/newsticker/meldung/95770>

mfG Matthias Mansfeld

=====

Re:TOR

Geschrieben von Silberling - 2007/10/04 23:00

Also da ist mir JAP schon lieber und sicherer. Auch dort gibt es für ein kleines Endgeld mehrere Verkettungen, aber auch noch ein kostenloses Angebot, und zum Surfen und bloggen reicht das allemal. Auch hier gibt es ein Plugin Switchproxy für den Firefox.

=====

Re:TOR

Geschrieben von Gast - 2007/10/07 22:27

Also die Hausdurchsuchung nach 0 Uhr beim Betreiber des Tor-Exit-Nodes dürfte mindestens in einer rechtlichen Grauzone liegen, wenn nicht sogar illegal gewesen sein. Stickworte:

- erlaubte Zeiten für Durchsuchung?
- keine richterliche Anordnung!
- Anhaltspunkte für "Gefahr im Verzug"?

Abgesehen davon ist hier der Tor-Server-Betreiber betroffen und nicht der Nutzer, der Tor lediglich als Client nutzt. Der zweite Heise-Beitrag betrifft lediglich unverschlüsselte Verbindungen, über die vertrauliche Daten gesendet werden. Jeder Nutzer sollte wissen, dass Tor lediglich die IP verbirgt, die Verbindung vom Exit-Node zum Ziel aber weiterhin unverschlüsselt ist, wenn nicht explizit eine verschlüsselte Verbindung (https/tls) genutzt wird. Aber für dieses fehlende Problembewußtsein Tor verantwortlich machen?

Richtig genutzt kann Tor sehr wohl nützlich sein. Und im Gegensatz zu JAP besitzt Tor keine eingearbeitete Überwachungsschnittstelle, die jederzeit aktiviert werden kann. Dazu stehen Tor-Server über die ganze Welt verstreut und nicht wie bei JAP nur in einem Land, so dass der Zugriff von staatlicher Seite deutlich erschwert ist.

=====

Re:TOR

Geschrieben von JonDos - 2007/10/07 23:46

Mittlerweile sind einige der mit JAP erreichbaren Dienste über mehrere Länder verteilt (JonDonym). Es gibt bereits Betreiber aus England und Thailand, einige Server stehen in Dänemark und Tschechien. Eine weitere Internationalisierung ist für dieses und nächstes Jahr geplant. Die Hürde zum Aktivieren der Überwachungsfunktion ist

ÄuÙbrigens hoch - alle Betreiber in der Kette mÄuÙssen jeweils Ihre Server-Software umkompilieren. Nur wenn alle ihre Daten zusammentragen, ist eine Deanonymisierung mÄuÙglich.

Eine solche Funktion ist fÄuÙr den rechtskonformen Betrieb ÄuÙbrigens notwendig. Ansonsten mÄuÙsst die Server bei einer ÄuÙberwachung abgeschaltet werden, und der Betreiber muss unter UmstÄuÙnden strafrechtlich haften: er weigert sich zu loggen, obwohl dies technisch mÄuÙglich wÄuÙre (und wenn es auch nur ÄuÙber wireshark geschieht), und warnt mit der Abschaltung mÄuÙglicherweise einen VerdÄuÙchtigen. Das gilt ÄuÙbrigens auch fÄuÙr Tor-Betreiber. Ob dann nur nutzlose Daten geloggt werden (ein- und ausgehende Verbindungen dieses Servers) oder nicht spielt jedoch keine Rolle. Der Betreiber erfÄuÙllt ja seine Pflicht, soweit es technisch mÄuÙglich ist.

Re:TOR

Geschrieben von Leecher - 2009/06/02 17:38

TOR mag ja schÄuÙn zum Surfen sein, allerdings nur solange wie die Seiten lediglich Text enthalten. MÄuÙssen Bilder heruntergeladen werden und sei es nur Werbung, kann der Seitenaufbau schonmal 20 Minuten und mehr in Anspruch nehmen.

Will man sich gar Videos anschauen, bspw. bei YouTube, hÄuÙrt der SpaÄuÙ dann auf.

An ein Herunterladen von Dateien ist garnicht zu denken. Bricht der Download nicht nach den, fÄuÙr TOR, obligatorischen 30 Sekunden ab, dauert es Stunden, wenn nicht gar Tage um einen Download abzuschlieÄuÙen. TOR iÄuÙrdt lediglich mit 30KB herunter und diese 30KB werden seltenst erreicht, eher dann 30B.

TOR ist nicht zu empfehlen bei erhÄuÙhtem Blutdruck - hier droht Herzinfarktgefahr - wenn man sich ÄuÙber das langsame Internet aufregt.

Re:TOR

Geschrieben von Jammerlappen - 2009/11/26 15:24

Hallo Leute,

ich mÄuÙchte Euch das neue CyberGhost VPN 2 vorstellen, welches das Surfen und Downloaden bestmÄuÙglichst anonymisiert.

In Tagen zunehmender Durchleuchtung Eurer InternetaktivitÄuÙten, bei der jede Webseite erkennt, was und zu welchem Zeitpunkt Ihr etwas ansieht, bieten Wir, die SAD GmbH, Euch eine sehr gute, sichere und schnellere Alternative zu Webproxies.

Mit CyberGhost VPN 2 bietet S.A.D. 2 GB 256-BIT AES VerschlÄuÙsselung fÄuÙr Eure wichtigsten Daten.

Das ganze passiert einfach wie nie: Kostenlos herunterladen (<http://cyberghostvpn.com>), installieren, verbinden und anonym surfen.

Ein umfangreiches Controlcenter ermÄuÙglichst selbst unerfahrenen Usern das anonyme Surfen in wenigen Sekunden.

Nach regem Feedback seitens der Community in der VorgÄuÙngerversion hat S.A.D. CyberGhost VPN 2 an vielen Stellen verbessert. Beispielsweise haben sie das Loginsystem vereinfacht, damit man so schnell und unkompliziert wie mÄuÙglich beginnen kann anonym zu surfen!

Und das Beste ist: S.A.D. verschenkt in der Free-Version 1GB Traffic pro Monat (ab 1.12.09)! Das ist genug fÄuÙr fast alle InternetaktivitÄuÙten im Alltag.

Hier kostenlos herunterzuladen: <http://cyberghostvpn.com>

Auf der Webseite von S.A.D. ist Folgendes zu lesen:

AusdrÄuÙcklich erwÄuÙhnt sei, dass wir NICHT speichern:

Den Inhalt irgendwelcher Kommunikation oder Daten ÄuÙber aufgerufene Webseiten.

Die Anonymität des einzelnen Users bleibt also gewährleistet. Da wir (bei sechsstelligen Userzahlen) sicherstellen können, dass sich zu jeder Zeit auf jedem unserer Server immer mehrere User aufhalten, kann eine genaue Zuordnung von User-IP zu CyberGhost-IP nicht erfolgen. Es teilen sich zu jedem Zeitpunkt immer mehrere User eine CyberGhost-IP-Adresse. Eine Rückverfolgung auf eine einzelne Person ist damit ausgeschlossen.

Also bitte nicht wieder antworten "Anonym gibt's nicht" usw., das wissen wir bereits.

Liebe Grüße

=====

Re:TOR

Geschrieben von Jammerlappen - 2009/11/26 15:25

Hallo Leute,

ich möchte Euch das neue CyberGhost VPN 2 vorstellen, welches das Surfen und Downloaden bestmöglichst anonymisiert.

In Tagen zunehmender Durchleuchtung Eurer Internetaktivitäten, bei der jede Webseite erkennt, was und zu welchem Zeitpunkt Ihr etwas ansieht, bieten Wir, die SAD GmbH, Euch eine sehr gute, sichere und schnellere Alternative zu Webproxies.

Mit CyberGhost VPN 2 bietet S.A.D. 2 GB 256-BIT AES Verschlüsselung für Eure wichtigsten Daten.

Das ganze passiert einfach wie nie: Kostenlos heruntergeladen (<http://cyberghostvpn.com>), installieren, verbinden und anonym surfen.

Ein umfangreiches Controlcenter ermöglicht selbst unerfahrenen Usern das anonyme Surfen in wenigen Sekunden.

Nach regem Feedback seitens der Community in der Vorgängerversion hat S.A.D. CyberGhost VPN 2 an vielen Stellen verbessert. Beispielsweise haben sie das Loginsystem vereinfacht, damit man so schnell und unkompliziert wie möglich beginnen kann anonym zu surfen!

Und das Beste ist: S.A.D. verschenkt in der Free-Version 1GB Traffic pro Monat (ab 1.12.09)! Das ist genug für fast alle Internetaktivitäten im Alltag.

Hier kostenlos herunterzuladen: <http://cyberghostvpn.com>

Auf der Webseite von S.A.D. ist Folgendes zu lesen:

Ausdrücklich erwähnt sei, dass wir NICHT speichern:

Den Inhalt irgendwelcher Kommunikation oder Daten über aufgerufene Webseiten.

Die Anonymität des einzelnen Users bleibt also gewährleistet. Da wir (bei sechsstelligen Userzahlen) sicherstellen können, dass sich zu jeder Zeit auf jedem unserer Server immer mehrere User aufhalten, kann eine genaue Zuordnung von User-IP zu CyberGhost-IP nicht erfolgen. Es teilen sich zu jedem Zeitpunkt immer mehrere User eine CyberGhost-IP-Adresse. Eine Rückverfolgung auf eine einzelne Person ist damit ausgeschlossen.

Also bitte nicht wieder antworten "Anonym gibt's nicht" usw., das wissen wir bereits.

Liebe Grüße

=====

Re:TOR

Geschrieben von TOR-Nutzer - 2010/03/01 16:15

Hi @ all,

Vorab: JAB wurde oben als Alternative für TOR angegeben. Das ist auch so weit richtig, allerdings gibt es bei JAB ein kleines Problem und zwar werden alle Exit-Notes von der Regierung oder Regierungsnahen Organisationen wie z.B. einer Staatlichen Universität gestellt. Dies ist weiterhin nicht schlimm, sollte es jedoch dazu kommen, dass Daten zukünftig geloggt werden, dann wird die Umstellung auf Loggen sehr schnell und unproblematisch sein, ohne dass der Endnutzer das zwingend mitbekommen wird.

Nun zu meinem eigentlichen Anliegen.

Ich nutze TOR bereits seit mehreren Jahren. Ich habe mein Surfverhalten teilweise an TOR angepasst und komme damit sehr gut klar. Ich selber betreibe 2 TOR-Server welche allerdings beide nur eine weiterleitende Funktionalität besitzen. D.h. Ich leite die Pakete von irgendwo nach irgendwo, bin selber allerdings keine Exit-Note. Damit das Prinzip von TOR funktioniert, müssen die IP-Adressen bekannt sein, damit sich die Server untereinander verbinden können. Es gibt im Internet Listen, mit den IP-Adressen der TOR-Server, welche leider auch zweckentfremdet genutzt werden. Z.B. von Google oder Wikipedia. Versucht man diese Seite mit einer IP-Adresse aufzurufen, welche auf der Liste steht, kommt es zu Komplikationen (z.B. Posten bei Wikipedia nicht möglich). Hierbei handelt es sich meiner Auffassung nach um einen tragbaren Nebeneffekt. Allerdings hat sich das letzte Woche geändert. Ich habe (beide Anschlüsse laufen nicht auf meinen Namen) letzte Woche 2 Briefe von Anwälten bekommen, welche mir unterstellt haben, dass ich illegales Filesharing betreiben würde. Als ich den 1. Brief bekommen habe, dachte ich, dass es sich um eine Verwechslung handle, da ich kein Filesharing betreibe und nicht mal die benötigte Software installiert habe. Als allerdings der 2. Brief (für den anderen Anschluss) angekommen ist, habe ich versucht der Sache auf den Grund zu gehen. Ich habe beide Systeme überprüft und festgestellt, dass unter normalen Umständen (d.h. falls ich nicht einen Trojaner habe, von dem ich nichts weiß) keine Möglichkeit besteht, dass von meinem System aus illegales Filesharing betrieben wird. Meine VERMUTUNG ist nun die, dass es Anwälte gibt, die sich TOR IP-Adressen aneignen und dann ohne jegliche Grundlage eine Klage gegen diese führen. Ich habe das Wort "Vermutung" extra groß geschrieben, da ich diese These derzeit nicht belegen kann. Dies ist auch der Grund dafür, dass ich den Namen der Hamburger Anwaltskanzlei nicht öffentlich nenne. Sollte es jedoch auch bei anderen TOR-Nutzern zu diesem Phänomen gekommen sein, würde ich mich sehr freuen, wenn diese auch damit auch an die Öffentlichkeit treten würden, da ich dieses Vorgehen selbstverständlich missbillige.

Gruß TOR-Nutzer

=====