Détecter le réseau TOR avec PHP

Rédigé par Joseph MICACCIA - 15 juin 2016 - 1 commentaire

TOR est un logiciel libre qui permet de rendre anonymes les communications électroniques. Le projet Tor est une organisation à but non lucratif dédiée à la recherche, le développement et l'éducation sur l'anonymat et la vie privée en ligne. Le logo est un oignon car TOR a plusieurs couches, comme l'oignon.

Tor dirige le trafic Internet à travers un réseau de bénévoles, dans le monde entier, composé de plus de sept mille relais pour cacher l'emplacement d'un utilisateur à tous ceux qui effectuent la surveillance du réseau ou l'analyse du trafic. Les utilisateurs de TOR sont difficiles à identifier, qu'ils naviguent sur le Net, utilisent de la messagerie en ligne ou instantanée, etc...

Ainsi, l'utilisation de Tor est destinée à protéger la vie privée des utilisateurs, leur liberté et leur capacité à mener des communications confidentielles. Ce

n'est pas parce qu'on a rien à cacher qu'il faut obligatoirement tout montrer.

Celles et ceux qui ne connaissent pas encore TOR auront tous les détails en visitant le site officiel, wikipedia et les innombrables autres sites qui fournissent des tutoriels et des explications détaillées et très claires.

Cependant, pour les gestionnaires de sites Internet qui ont besoin de filtrer les internautes utilisant TOR, il existe une parade simple et efficace : TorDNSEL.

TorDNSEL, c'est quoi ?

C'est est une liste basée sur les DNS des nœuds de sortie TOR. Le site officiel de TOR précise la description de ce mécanisme.

On peut exploiter cette liste en utlisant un outil comme DIG ou via une simple requête DNS.

Les enregistrements dans TorDNSEL ont cette convention d'écriture : **X.Y.Z.ip-port.exitlist.torproject.org**

avec :

- X : adresse IP du client, inversée
- Y : port TCP du serveur
- Z : adresse IP publique du serveur, inversée

Ainsi, pour savoir si l'internaute qui arrive sur votre site utilise TOR, il suffit de faire cette requête DNS et comparer le résultat.

Voici une petite fonction, en PHP, trouvée sur Internet (auteur inconnu) qui permet d'identifier un utilisateur de TOR :

```
1. function isTorRequest()
2.     {
3.     $reverse_client_ip = implode('.', array_reverse(explode('.', $_SERVER['REMOTE_ADDR'])));
4.     $reverse_server_ip = implode('.', array_reverse(explode('.', $_SERVER['SERVER_ADDR'])));
5.     $hostname = $reverse_client_ip . "." . $_SERVER['SERVER_PORT'] . "." . $reverse_server_ip . ".ip-port.exitlist.torproject.org";
6.     return gethostbyname($hostname) == "127.0.0.2";
7.     }
```

C'est une bonne base de travail, mais ça ne suffit pas. Nous allons voir les améliorations possibles.

D'abord, rappelons à quoi correspondent les variables :

- $_SERVER['REMOTE_ADDR'] : l'adresse IP du client qui demande la page courante
- $_SERVER['SERVER_ADDR'] : l'adresse IP du serveur à partir duquel le script courant est en train d'être exécuté
- $_SERVER['SERVER_PORT'] : le port de la machine serveur utilisé pour les communications.

Il faut préciser, ici, qu'avec ces paramètres, la fonction risque de ne pas fonctionner correctement, pour deux raisons au moins :

- $_SERVER['REMOTE_ADDR'] n'est pas assez précis pour identifier l'IP du client. L'étude d'une fonction pour l'identification précise de l'IP du client fera l'objet d'un autre article.
- $_SERVER['SERVER_ADDR'] peut retourner une IP privée, inconnue par le réseau TOR. Il faut utiliser l'adresse IP publique du serveur. Il existe plusieurs technique pour identifier automatiquement l'adresse IP publique du serveur. Accessoirement, on peut la définir manuellement puisque, sauf cas particuliers, elle ne change pas.

Voici donc une amélioration possible :

```
1. function isTorRequest($IpDuClient)
2.     {
3.     $IpPubliqueDuServeur = 'XXX.XXX.XXX.XXX'; // renseigner ici l'adresse IP publique du serveur web
4.     $reverse_client_ip   = implode('.', array_reverse(explode('.', $IpDuClient)));
5.     $reverse_server_ip   = implode('.', array_reverse(explode('.', $IpPubliqueDuServeur )));
6.     $hostname            = $reverse_client_ip . "." . $_SERVER['SERVER_PORT'] . "." . $reverse_server_ip . ".ip-
port.exitlist.torproject.org";
7.     return gethostbyname($hostname) == "127.0.0.2";
8.     }
```

Pour les internautes qui souhaiteraient tester le fonctionnement de TOR, voici le lien du site officiel pour le téléchargement de TOR Browser, le navigateur permettant d'utiliser le réseau TOR.

Classé dans : PHP, Sécurité - Mots clés : TOR

1 commentaire

#1 dimanche 06 novembre 2016 - 13:48 - David a dit :

MERCI MERCI MERCI enfin un truc qui marche
il y a plein d'articles intéressants aussi pour comprendre un peu mais j'ai pas compris tout
https://www.tenable.com/blog/active-and-passive-tor-detection
https://blog.perimeterx.com/blocking-tor-a-case-for-more-accuracy/
http://security.stackexchange.com/questions/38498/detecting-tor-proxy-by-reading-request-headers
https://www.rsreese.com/detecting-tor-traffic-with-bro-network-traffic-analyzer/
https://ask.wireshark.org/questions/13590/tor-detection
http://www.netresec.com/?page=Blog&month=2013-04&post=Detecting-TOR-Communication-in-Network-Traffic
https://openclassrooms.com/forum/sujet/detecter-l-utilisation-proxy-ou-tor-26066

Répondre

Fil RSS des commentaires de cet article

Écrire un commentaire

Votre nom ou pseudo :

Votre adresse e-mail (facultatif) :

Votre site Internet (facultatif) :

Contenu de votre message :

Vérification anti-spam

Quelle est la **dernière** lettre du mot **z d d l r g** ?

Envoyer votre commentaire

CATÉGORIES

Active directory (2)
VB script (1)
Group Policy Object (1)
Microsoft Windows (2)
Linux (2)
Delphi (1)
Gestion de projets (2)
Sauvegarde (2)
PHP (2)
Sécurité (6)
PowerShell (1)
Download (1)
Android (1)

DERNIERS ARTICLES

Veeam, le partenaire idéal pour la sauvegarde des infrastructures VmWare (micaccia.priv & Co.)
Redmine : un outil flexible pour la gestion de projets
Microsoft Exchange : Signatures pour Outlook avec VBS, Active Directory et GPO
Certified StormShield Network Administrator, I am
ColorNote : Une application ANDROID performante et très facile d'utilisation

MOTS CLÉS

Vbscript Active Directory GPO Microsoft Outlook Signature Attention TOR Freeware ColorNote Bloc-note Veeam backup

DERNIERS COMMENTAIRES

Vincent Taland a dit : y a aussi onenote de krosoft https...
Dd45 a dit : other downloads http://www.rocket...
Get2work@once a dit : very good job tanku
Close2u a dit : Sinon il y a aussi vdp de vmware h...
David a dit : MERCI MERCI MERCI enfin un truc qu...

ARCHIVES

Novembre 2016 (1)
Octobre 2016 (1)
Septembre 2016 (1)
Août 2016 (1)
Juillet 2016 (1)
Juin 2016 (1)
Mai 2016 (1)
Avril 2016 (1)
Mars 2016 (1)
Février 2016 (1)
Janvier 2016 (1)

RSS

Haut de page