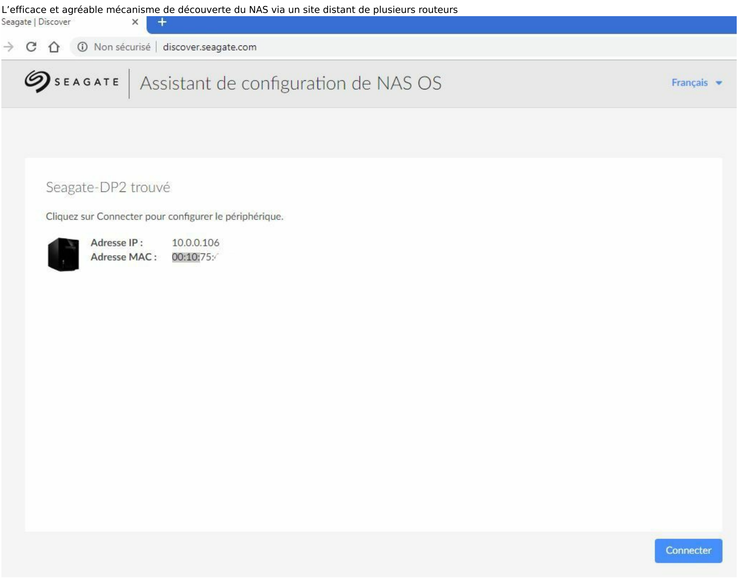
Journal : Collecte d'informations privées via un simple lien sur un navigateur

Posté par **Alexis-Emmanuel Haeringer** le 17/12/18 à 01:19. **Licence CC by-sa.**
Tags : **vie_privée**, **freenas**

Bonsoir,
Permettez-moi de vous partager ces quelques informations techniques sur les possibilités de collecte d'informations par un navigateur internet en 2018.
Ayant sous la main un NAS Seagate (vendu juste après le rachat de Lacie), j'ai pu apprécier l'effort pour faciliter l'installation et par conséquent les risques afférents.
Ainsi donc, si vous avez un disque vierge dans ce NAS, il vous est possible de réinstaller un système sans rien brancher, en effet un espace mémoire (vu comme une clef USB de 242Mo) est réservé dans le NAS, il contient un système de récupération que l'on peut lancer en appuyant sur un bouton au démarrage.
Après le lancement du système de récupération et en branchant le nas sur un réseau dédié connecté à Internet. Il suffit de lancer l'adresse **http://discover.seagate.com** pour voir apparaître le nas avec sa MAC et son IP privée.
Je trouve qu'il y a quatre éléments intéressants à considérer :

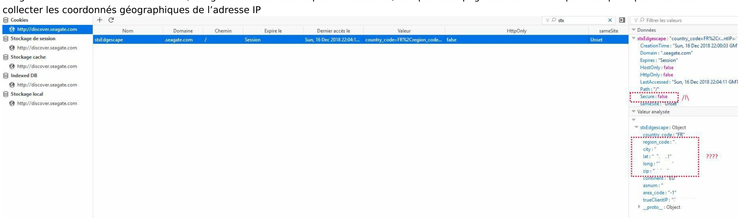
1. L'efficace et agréable mécanisme de découverte du NAS via un site distant de plusieurs routeurs



2. La capacité pour un site distant de connaître beaucoup de chose comme les coordonnés GPS, l'IP publique, mais également, l'IP privée & l'adresse MAC de l'ordinateur et celle d'un autre ordinateur sur le réseau sans aucune demande de sécurité de la part du navigateur.

3. La technologie qui est derrière pour effectuer cela : une jolie bibliothèque findmynas.js en GWT malheureusement cryptée (et à certains endroits dispo en devmod d'ailleurs ..).

4. Malgré le soin de nous faciliter la tâche, Seagate ne nous rassure pas une seconde, lorsque cette page est servie en https mais qu'en plus il semble collecter les coordonnés géographiques de l'adresse IP



Je n'ai pas pris plus le temps de regarder en détail les arcanes du mécanisme de détection, je suppose que c'est encore la « faute » aux websockets, mais surtout aux **architectes** qui n'ont pas mis en place un mécanisme d'alerte et de demande, avant de divulguer ce type d'informations (comme ceux de l'usage de la caméra ou du microphone).
Quand on travail sur les échanges réseaux où l'adresse mac est remplacée à chaque routeur, on en oublie les évolutions des navigateurs qui se moquent du modèle OSI ....

En fait initialement je voulais installer freenas, mais malheureusement la clef usb n'est pas détectée au démarrage. En me connectant en JTAG série dessus, j'ai malheureusement constaté que le bios AMI est bridé ... seul l'amorçage réseau et l'amorçage disque semblent disponible. À ce que je vois, à cette heure, il me reste : soit à débrider le bios avec **AMIBCP**, soit proposer l'iso via bootp, soit l'installer de la manière qui lui convient (mbr ou efi csm ou efi ...) sur le disque avant de l'insérer dans le NAS, mais même en temps pour bénéficier de la mise à jour de sécurité du bios va falloir quand même passer par une première installation de Seagate OS, arf ...

Pour info :
System Model Superbee Nas, STX MODEL : STDD200, équivalent 5Big NAS Pro , les mac seagate commencent par "00:10:75"

Scandaleux

Posté par **gUI** le 17/12/18 à 09:14. Évalué à 9 (+7/-0).

> Un browser qui a accès au réseau c'est proprement scandaleux en effet.
>
> L'autre jour pareil sur un gestionnaire de fichier : il lisait tous les noms de mes fichiers ! Tranquille, sans me demander la permission avant.
>
> Plus sérieusement, c'est exactement pour ça que certains utilisent "no script". Encore là Seagate il est sympa il t'affiche à peu près ce qu'il collecte, mais t'inquiètes pas, tu as déjà exécuté des milliers de fois ce style de script sans que cette fois-ci on t'en parle.

Re: Scandaleux

Posté par **fearan** le 17/12/18 à 13:41. Évalué à 3 (+1/-0).

> en fait de noscript je suis passé a umatrix, un poil plus fin, par site visité on autorise quel adresse peut faire quoi (media, cookies, script, frame...) et si on autorise le site à modifier le référant.
>
> Par contre sur certains site ça met du temps avant d'avoir quelque chose (activer machin reload, activer truc reload...); ça évite de tout où rien de noscript.
>
> --
> Il ne faut pas décorner les boeufs avant d'avoir semé le vent

Re: Scandaleux

Posté par **HL** le 17/12/18 à 14:45. Évalué à 0 (+0/-0).

> J'ai installé uMatrix, plus fin que Request Policy (même si ce n'est pas exactement le même genre de module). Par contre, l'autocomplétion des adresses du site **www.ratp.fr** (recherche d'itinéraire) ne semble plus fonctionner avec, même si je désactive les filtres matriciels. Si je désactive le module, ça se remet à fonctionner.
>
> (A côté, j'ai Noscript, uBlock Origin, Cookie AutoDelete et HTTPS Everywhere.)

GWT

Posté par **barmic** le 17/12/18 à 09:50. Évalué à 2 (+1/-1).

> > *La technologie qui est derrière pour effectuer cela : une jolie bibliothèque findmynas.js en GWT malheureusement cryptée (et à certains endroits dispo en devmod d'ailleurs ..).*
>
> Le code js GWT n'a pas besoin d'être chiffré. Il est juste le fruit d'une compilation donc oui c'est pas fait pour être lu.