

Time2Watch - The End

Novembre 2020

Table des matières

1	Introduction	2
2	Time2Watch	2
2.1	Les raisons de l'existence de Time2Watch	2
2.2	La raison de notre fermeture	3
2.3	Dernier message à nos utilisateurs	3
3	DMCA, menaces, ayants droits	5
3.1	Rivendell et Leakid	5
3.2	Le méconnu CoPeerRight	5
3.3	Les menaces de Wakanim	6
3.4	Les démarches douteuses de l'ALPA	6
3.5	L'efficacité du blocage par DNS en France	7
4	Le Warez	8
4.1	Anonymat et mesures de protection	8
4.2	Cloudflare ne vous protège pas	9
4.3	Hébergeurs offshore et bulletproofs	9
4.4	Registrar offshore	10
4.5	Les hébergeurs (Uptobox, 1Fichier, ...)	10
4.6	L'argent dans tout ça	11
5	Conclusion	12

1 Introduction

Ce document sans prétention a pour objectif de démystifier un tant soit peu le Warez, certains fonctionnements sous-jacent aux sites de streaming et de téléchargement. Mais aussi de notifier de certaines pratiques d'autorités ou d'ayants droits.

Notre avis sur le Warez, sur l'offre légale, la raison de notre existence et de notre fermeture, tout y est ou presque.

2 Time2Watch

2.1 Les raisons de l'existence de Time2Watch

Time2Watch tel qu'il était au moment de sa fermeture existait depuis environ 5 ans, mais il existe sans doute depuis plus de 11 ans.

Time2Watch a été créé par conviction.

- Premièrement, pour combattre l'offre légale qui est loin d'être satisfaisante pour plusieurs raisons. Notamment par la trop grande diversité des offres, et cette guerre que se livrent les principales plateformes de streaming (Netflix, Prime, ...) qui dessert les utilisateurs par leur concurrence. À notre grand dam, légal ou pas, l'objectif premier reste l'argent (nous ne sommes pas candide, nous savons que c'est le but d'une entreprise). Grand bien leur fasse, mais ils n'ont pas encore tout compris. Et puis il y a le combat vain des DRM : même avec un compte Netflix, il est possible que vous ne disposiez pas de la meilleure qualité visuelle lorsque vous regardez un programme, Netflix n'autorisant pas la 1080p sur Chrome (la couche L3 de Widevine, la partie software -la plus faible- du DRM de Google qu'utilise Netflix). Pourquoi Netflix fait-il cela ? Pour compliquer la tâche de ceux qui essaieront de récupérer leurs programmes en bonne qualité pour les diffuser illégalement, donc, pour empêcher le piratage. Sauf que ça ne stoppe pas grand monde, et que ça ne fait qu'encourager le piratage pour les gens qui recherchent la qualité, oups.

La France a aussi contribué à motiver la création du site. Vous remercieriez (ou pas) la chronologie des médias, cette directive obsolète qui ne devrait plus exister aujourd'hui et qui nous motivait à rendre disponible en France les œuvres sans délai, mais aussi la grande blague qu'est la redevance pour copie privée. Il fallait bien rendre cette redevance rentable pour les français, à une époque où plus personne ne se partage des "copies privées" sur disquette, une époque où tout est streaming (à quand l'application de la redevance sur la RAM).

- Deuxièmement, pour combattre l'offre illégale, le Warez d'hier et encore plus d'aujourd'hui. Tapez "voir **** en streaming gratuit" sur Google, et vous tomberez dans 100% des cas sur un site de streaming qui vous affichera au moindre clic des tonnes de publicités intrusives (allant jusqu'à bloquer votre navigateur) et des "click-and-redirect" vous amenant sur des fausses façades de sites vous demandant de sortir votre carte bleue pour continuer. C'est le Warez d'aujourd'hui. C'est dommage. Et c'est donc une autre raison pour laquelle

Time2Watch a vu le jour, pour construire un site qui soit à la fois mieux foutu en terme d'ergonomie que certains site légaux à la ramasse, mais aussi sans pub pour une meilleure expérience utilisateur (on en avait, bien entendu (on avait même dérapé à une époque avec quelques popups), mais si discrètes que la plupart des utilisateurs ne la voyait pas, ou la bloquait facilement). Nous voulions que Time2Watch se démarque par ce respect des utilisateurs, et c'est une des choses qui nous a fait le plus connaître. Un site propre, qualitatif, qui rend service, qui a des valeurs, efficace. C'est en tout cas ce qu'on visait, aux utilisateurs de le confirmer.

Time2Watch, c'était des fonctionnalités bien pratiques, pouvoir mettre en favoris des fiches pour suivre la sortie des épisodes grâce à un système de notifications, pouvoir suivre son avancement dans une série, à quel épisode on s'est arrêté, le prochain à voir, avoir un aperçu rapide des films vus, etc... Mais c'était aussi une bibliothèque de qualité, avec des releases préparées aux petits oignons tout en respectant les règles de la Scene; vous ne pouviez d'ailleurs trouver aucune release CAM, TS ou autre horreur du genre. Quitte à attendre quelques semaines de plus et ne pas avoir l'exclusivité, nous visions la qualité. Ces fonctionnalités et cette qualité, quoique vous puissiez dire, vous ne la retrouverez nul part ailleurs, et c'était une des raisons d'exister de Time2Watch.

2.2 La raison de notre fermeture

Cela risque d'en décevoir certains, mais ce n'est pas à cause d'un drama, ou d'une dénonciation d'un membre de l'équipe, ou encore d'un coup de pression des autorités ou des ayant droits, ni même encore d'une arrestation (nous ne serions pas la pour écrire ce document). La raison est plus simple, sans doute plus égoïste mais certainement plus réfléchie. Le site nous a beaucoup apporté en terme de connaissance techniques en tout genre, et aussi beaucoup humainement à travers toutes les personnes qu'on a pu côtoyer. Mais arrive un moment où l'on a fait le tour de tout ce qu'il était intéressant de faire, où même l'envie de combattre ces géants des offres légales, de coiffer sur le poteau cette chronologie des médias bien française, et de rentabiliser cette blague de redevance pour copie privée... tout ça n'apporte plus assez de motivation pour continuer à s'investir autant, après tant d'années pour certains, face à la fatigue et à l'envie de passer à autre chose, tout simplement.

Vous l'aurez sans doute remarqué, notre nom de domaine a été suspendu par le registry .io, mais nous avions prévu depuis un moment déjà de fermer avant Noël, cette suspension de nom domaine nous a juste donné une occasion de le faire plus tôt.

2.3 Dernier message à nos utilisateurs

On avait l'habitude de se dire que si un jour l'offre légale venait à devenir assez bonne pour qu'on ne serve plus à rien, on fermerait. Alors on aimerait vous dire de passer sur Netflix, ou Amazon Prime, ou Disney+, ou Apple+, ou OCS, ou Salto (lol) ... mais non, il y en a trop, et c'est selon nous un des problèmes majeur de l'offre légale actuelle. Et cela sans parler des anime (manga), avec Crunchyroll, Wakanim et ADN sous le giron de Sony.

Une offre aussi éparpillée, qui s'arrache les exclusivités, qui perd les droits du jour au lendemain... Non vraiment l'offre légale n'est plus intéressante, sauf si vous souhaitez payer tous ces abonnements. Et quand bien même vous payeriez tous les services disponibles dans votre pays, il vous manquerait encore beaucoup de contenu non "licencié" que vous seriez forcé d'obtenir... par un autre moyen.

Mais d'un autre côté il faut bien se rendre à l'évidence : aujourd'hui le Warez ce sont des sites qui existent exclusivement pour l'argent, à base de publicités intrusives et arnaques à gogo (chose contre laquelle on s'est toujours battu). Donc le choix n'est pas si simple. Beaucoup d'utilisateurs de Time2Watch avaient d'ailleurs un compte sur une offre légale (généralement Netflix), et se servaient de Time2Watch pour les oeuvres qu'il ne trouvaient pas sur Netflix (ou que Netflix faisait disparaître de leur catalogue d'un claquement de doigt). Et c'est une formule que nous trouvons équitable.

Un dernier mot : Time2Watch a fermé et ne rouvrira jamais sous aucune autre forme. La base de données a été détruite ainsi que le code source du site, et ils n'ont été transmis à personne, impossible donc de voir un Time2Watch revenir. Tous les sites que vous verrez à l'avenir ressemblant au nôtre (avec un nom de domaine ou un design ressemblant) ne seront que des clones qui en voudront à votre portefeuille, faites attention aux arnaques.

Aussi, pour ceux qui se plaignent d'avoir payé un compte premium et de nous voir fermer : Time2Watch a toujours été 100% gratuit, vous avez acheté un compte premium Uptobox, pas un compte premium Time2Watch, et Uptobox est utilisé par tous les sites Warez français, arrêtez de vous plaindre, vous ne pouvez pas niquer le système et venir pleurer quand ça se retourne contre vous (alors que ce n'est même pas le cas ici).

À nos utilisateurs fidèles, merci de nous avoir suivis jusqu'ici.

Si vous vouliez seulement connaître la raison de notre fermeture et lire notre dernier mot, la suite vous intéressera sans doute moins, elle s'adresse plus à un public intéressé par les dessous du Warez.

3 DMCA, menaces, ayants droits

3.1 Rivendell et Leakid

À plusieurs reprises, la société LeakID a remonté à Cloudflare des URLs de notre site, que nous pouvions identifier comme unique par adresse IP. URLs qui sont apparues au même moment sur le site LumenDatabase comme ayant été déréférencées par Google sur la demande de... Rivendell. Ces URLs étant uniques par IP vous le voyez venir : les "deux" sociétés utilisent donc les mêmes outils de scraping, depuis les mêmes adresses IP, depuis le même compte inscrit à notre site que nous avons aussi pu identifier. Tirez-en les conclusions que vous voulez.

Rivendell a d'ailleurs un comportement bien original, des pouvoirs bien à lui. Sur ce compte que nous avons identifié, nous avons pu relever (sur une période de plusieurs mois) des connexions depuis plus de 10 000 adresses IP d'opérateurs français (Orange, Bouygues, SFR...), chacune de ces IPs ne faisant que 3-4 requêtes (dans le mois) sur notre site pour récupérer l'URL de la page comportant notre captcha pour accéder aux liens, afin de l'envoyer à Google et Cloudflare. Est-ce un accord spécial avec les opérateurs, un abus ? Nous ne le savons pas, mais nous savons bien qu'il est possible sur certains sites de louer des adresses IP résidentielles dans plusieurs pays (dont la France), ces sites vendant aussi des VPNs qui une fois installés chez l'utilisateur serviront de passerelle pour louer l'adresse IP résidentielle à une autre clientèle.

Rivendell ne se fatiguait d'ailleurs pas à résoudre notre captcha pour vérifier les liens qui se trouvaient derrière, ils se contentaient de signaler nos URLs en masse, sans vérification aucune.

3.2 Le méconnu CoPeerRight

Jamais dans les médias français nous n'avons vu passer le nom CoPeerRight Agency [2], et pourtant ce sont eux qui ont été les plus virulents, d'autant qu'on se souvienne.

Ce sont les seuls qui, lorsqu'ils obtiennent par Cloudflare le nom et l'IP de notre hébergeur, vont aller contacter (harcéler) ce dernier et lui faire pression pour que : soit les liens soient retirés, soit qu'ils coupent l'accès au site (ce qui arrivera si vous n'utilisez pas de serveurs bulletproof, ou que vous n'avez pas de chance).

Aucune autre autorité ou ayant-droit n'a jamais même ne serait-ce que tenté ce genre de démarche, alors qu'elles peuvent se révéler fructueuses dans bien des cas (s'en est presque affolant pour les autres autorités, vous foutez quoi de vos journées, avec l'argent que vous

paient les ayant droits, les diffuseurs... ?). Donc mention spéciale à Anna Lapteva de Co-PeerRight, vous êtes les seuls qui essayez de faire votre travail correctement.

3.3 Les menaces de Wakanim

On ne se plaint pas de ces menaces, on constate.

Si vous êtes consommateur d'anime, vous connaissez sans doute Wakanim. Vous avez aussi peut-être déjà entendu parler des pressions qu'ils exercent ou exerçaient sur certains groupes partageant leur contenu.

Quand Wakanim est venu à nous, ils n'ont pas contacté l'administrateur (dont le mail était disponible sur toutes les pages du site). En fait il ne nous ont jamais officiellement contacté. Ils (souvent Olivier Cervantes) préfèrent contacter les petits uploaders ou modérateurs pour leur faire peur, les menacer, chercher des cibles plus faciles pour instaurer un climat de peur. Wakanim tentera de vous faire croire qu'ils ont des éléments sur vous pour vous faire peur et vous forcer à arrêter vos activités. Si vous êtes un minimum soucieux de votre sécurité, que vous prenez les précautions qu'il faut, pas d'inquiétude, il ne s'agit que de bluff.

Ces pratiques sont d'autant plus hypocrites quand on remarque que le CTO de Wakanim (Ludovic Alcalá) a été identifié sur notre site en utilisant un compte sous une adresse IP NordVPN (lorsqu'il testait un bot pour signaler nos liens de manière massive), et que nous avons remarqué plus tard qu'il utilisait aussi ce compte pour visionner des films (qui n'avaient aucun lien avec Wakanim, donc pour son plaisir personnel). "Faites ce que je dis pas ce que je fais".

Wakanim est le seul service légal à avoir ce genre de pratiques, nous n'avons jamais reçu de menaces directes de la part de Netflix, Amazon, ADN, Crunchyroll, OCS... nous avons donc trouvé qu'il pouvait être intéressant de le mentionner ici.

3.4 Les démarches douteuses de l'ALPA

On ne se plaint pas de leurs abus, on constate.

Après tant d'années d'existence, c'est en Mars 2020 que nous avons eu affaire pour la première fois à l'ALPA, et ce par un blocage DNS de notre nom de domaine principal par les principaux FAI français, dont la demande avait été faite par l'ALPA [5]. Okay, fair enough.

Cependant, et c'est là que la bât blesse, l'ALPA s'est servie de ce jugement rendu par le tribunal de Paris qui ne visait que le blocage DNS, pour demander à Google le déréférencement de ces noms de domaines dont le nôtre, demandes effectuées sous le nom d'Etienne Brohon, agent assermenté de l'ALPA. Nous avons alors changé de nom de domaine, en passant de .in à .gg, et la semaine qui suivait, ce nom de domaine avait lui aussi été déréférencé de Google sur une nouvelle demande de l'ALPA qui brandissait encore une fois ce

même jugement du 16 Janvier, alors que ce nouveau nom de domaine ne figurait bien sûr pas dessus. Ce jugement invitait pourtant les parties à revenir devant le tribunal judiciaire pour actualiser la liste au besoin, ce qui n'a pas été fait [4]. Google n'ayant sans doute pas les ressources pour vérifier ce genre de détails, ils répondent positivement à la demande sans vérifications supplémentaires. Eh bien, nous ne sommes apparemment pas les seuls à profiter du système.

Ce jugement a -encore- été détourné pour réclamer la fermeture de notre compte sur l'instance Mastodon de la Quadrature du Net [1], où notre compte mamot.fr/@Time2Watch a donc été supprimé, mais aussi à 2 reprises auprès de Twitter, obtenant le blocage de 2 comptes.

"LeeLoo Dallas Multipass!"

Suite à cela, nous avons pour notre part décidé de ne plus tenter de re-référencement, et nous sommes donc restés pendant plus de 9 mois sans être référencé sur Google. Et pendant ces 9 mois, le site n'a plus entendu parler de l'ALPA, plus de blocage par DNS ni aucune autre mesure.

3.5 L'efficacité du blocage par DNS en France

Contrairement à ce qui se dit en réponse aux blocages par DNS, cette mesure peut être efficace, sous certaines conditions.

À notre modeste niveau, lorsque nous avons été bloqué au niveau DNS et déréférencé en Mars 2020, notre trafic avait diminué de 20% et donc d'autant plus nos revenus. Les internautes diront "il suffit de changer de nom de domaine", ou encore "il suffit de changer les DNS de son device", tout à fait, cependant il ne faut pas confondre utilisateur régulier et nouvel utilisateur. Comme le blocage par DNS est généralement suivi d'un déréférencement, on remarque une perte énorme (20%) au niveau du trafic organique (ces "nouveaux utilisateurs") pendant un certain laps de temps, et c'est clairement ce trafic qui rapporte le plus. Une fois ce laps de temps écoulé (qui correspond à la mise en place d'un nouveau nom de domaine et à son référencement), les utilisateurs lambda recommenceront à retrouver le site, qui reprendra doucement sa progression, il aura pris une bonne flèche dans le genou mais ça ne le gênera pas tant si on ne l'embête pas tout de suite de nouveau.

Mais si vous passez à un blocage par DNS dynamique *ET* un déréférencement dynamique, le site mourra petit à petit, acculé par ses revenus publicitaires dégressifs. Et il n'y aura plus d'alternatives pour les administrateurs, à part bourrer encore plus de popups et d'arnaques pour essayer de compenser la perte de trafic organique, ou encore accepter des donations des utilisateurs, mais ça ne sera jamais suffisant pour les sites du top FR qui ne recherchent que l'argent, et pas pérenne sur le long terme.

4 Le Warez

4.1 Anonymat et mesures de protection

On ne devrait pas donner de conseils, certaines personnes qui liront ce document ne le méritent pas, mais certains autres font vraiment pitié. Si nous étions de la Gendarmerie (C3N/N'Tech...) nous aurions sans doute déjà pu faire fermer plusieurs sites ou trackers privés avec les informations que l'on peut récolter rien qu'en OSINT -et sinon par relation- (on ne le fera pas). Donc voici quelques conseils pour ne pas foncer droit dans le mur si vous souhaitez vous lancer, à vous de choisir de les appliquer ou non. Ce sont d'ailleurs plus des bonnes pratiques et du bon sens que des conseils, rien de bien fou ici, et pourtant...

Premièrement, il est important de faire table rase du passé, si vous avez publié sur internet (par exemple si vous aviez un compte Facebook), des informations privées tel que votre nom et prénom, lieu d'habitat etc... supprimez tout, supprimez votre compte Facebook, Twitter, tapez votre nom ou des anciens pseudos sur divers moteurs de recherches et si des résultats apparaissent essayez d'en supprimer le maximum possible, vous pouvez faire marcher le "RGPD" si la situation s'y prête.

Quand vous vous lancez dans ce genre d'activité, n'utilisez jamais un pseudo (ou avatar) que vous auriez déjà utilisé ailleurs avant. C'est la suite du premier conseil, ce que vous souhaitez le moins c'est qu'on puisse vous relier au profil d'un autre site, ou relier des anciens pseudos entre eux. Utilisez aussi des pseudos passe-partout, n'utilisez pas des pseudos uniques tel que 4S5@s3_, cherchez un pseudo qui sera susceptible de renvoyer à des résultats qui ne vous concernent pas lorsqu'on le tape sur Google, noyez vous dans la masse (Jean Pierre, Luffy, ...).

Utilisez *au minimum* un VPN, soyez sûr que celui-ci ne log rien, et mettez en place des moyens techniques permettant d'empêcher tout leak. Mais pas besoin non plus de chaîner 7 VPN + 7 proxies + Tor, vous ne vous battez pas contre la NSA.

Si vous avez une discussion avec quelqu'un qui est au courant de vos activités, ne racontez pas votre vie, même si vous avez entièrement confiance en cette personne, ou que vous avez envie de vous la péter, vous ne savez jamais ce que l'avenir vous réserve. Pour X raisons cette personne pourrait être celle qui causera votre perte dans un futur très lointain.

Ne payez jamais rien avec votre compte bancaire (ou Paypal), c'est vraiment con à dire mais on l'a déjà vu se faire... Et le sens inverse est aussi vrai, à partir du moment où vous toucherez ne serait-ce qu'1 euro sur votre compte bancaire, considérez vous comme foutu sur le long terme, quelques soient les moyens que vous aurez mis en oeuvre pour vous protéger. On en reparle plus tard, mais si vous faites cette activité pour l'argent, c'est Game Over.

Ne faites confiance à personne. N'allez pas sur les serveurs Discord, ne partagez pas par envie d'être populaire, n'allez pas vous vanter auprès de vos amis ou de certaines communautés de ce que vous faites, faites profil bas, partagez vos fichiers et ne commettez pas une

erreur qui pourrait vous retomber dessus même dans un futur très lointain.

Enfin, même en appliquant toutes les méthodes de protection possible, il faut garder les pieds sur terre, le risque zéro n'existe pas, c'est lorsque vous commencez à prendre confiance que vous êtes le plus susceptible de faire des erreurs.

4.2 Cloudflare ne vous protège pas

Si vous pensez utiliser Cloudflare pour protéger votre serveur des plaintes DMCA ou cacher son IP des autorités et des ayants droits, et bien c'est râté. Cloudflare ne vous protégera PAS UNE SECONDE. Ils donneront le nom de votre hébergeur, et sinon l'adresse IP de votre serveur, à n'importe quelle autorité qui lui en fera la demande. Et même dans certains cas votre adresse IP de connexion, vos données de compte, moyens de paiements si vous en avez défini, etc.

Et ces autorités ne le savent que très bien puisqu'elles n'hésitent pas à faire ces demandes (ce n'est pas une légende, puisque Cloudflare nous transfère les demandes auxquelles ils répondent positivement, et il y en a chaque semaine), mais l'hypocrisie de ces autorités ou leur impuissance les amène à clamer dans tous leurs rapports que les sites Warez se cachent derrière Cloudflare et qu'il est donc impossible de connaître leurs serveurs, que Cloudflare les protège, les anonymise (coucou l'ALPA [3]). Ne rejetez pas votre incompetence sur un mensonge.

Une bêtise que l'on voit beaucoup pour les gens qui se lancent dans le milieu est d'acheter un serveur avec leur compte Paypal ou bancaire, généralement chez OVH, en pensant qu'ils seront tranquille avec Cloudflare devant... fuyez pauvres fous, pendant qu'il en est encore temps !

En conclusion, Cloudflare ne doit en aucun cas servir de protection face aux autorités. Sa seule utilité doit être d'alléger la charge de votre serveur grâce à leur fonctionnalité de CDN, et de vous protéger de certaines attaques DDoS grâce à leur firewall. Et c'est tout. Pour le reste, il faudra compter sur votre hébergeur qui sera derrière Cloudflare.

4.3 Hébergeurs offshores et bulletproofs

C'est l'erreur que font souvent les gens, confondre offshore et bulletproof.

Un hébergeur offshore est un hébergeur situé dans un pays étranger qui n'attendra pas que vous donniez votre identité réelle et que vous pourrez dans la plupart des cas payer en bitcoin. Mais cet hébergeur n'ignorerait pas forcément les plaintes DMCA qui lui seront envoyées et pourrait vous demander de soit supprimer les pages incriminées, soit vous demander de dégager. À contrario, un hébergeur dit bulletproof est censé ignorer les plaintes DMCA qui lui seront envoyées. Dans la plupart des cas, vous ne devriez pas avoir trop de problème avec un hébergeur bulletproof.

Bien sur, votre serveur "frontal" (directement accessible ou juste derrière Cloudflare) ne doit en aucun cas être votre serveur principal car il pourra à tout moment être bloqué par l'hébergeur par une quelconque pression juridique. Bulletproof ou pas, ce n'est pas une science exacte. Ce serveur doit donc seulement être un reverse proxy vers le reste de votre infra, un serveur que vous pourrez changer à tout moment (et même en avoir plusieurs en avance pour changer rapidement).

Parmi ces hébergeurs offshore et bulletproof, on retrouve les très connus FlokiNET, AbeloHost, Novogara ou BlueAngelHost (qui sont d'ailleurs conseillés par la MPA, merci à eux [6]) qui ont fait leurs preuves pour avoir servis à ThePirateBay et d'autres grands sites (dont beaucoup de sites du top FR), et puis d'autres hébergeurs qui seront un peu moins bulletproof mais qui pourront aussi vous être utiles, comme Shinjiru, Here-Host, etc.

4.4 Registrar offshore

Le registrar du nom de domaine n'est pas très important, s'il est un minimum offshore et réputé. Nous utilisons Namecheap et n'avons jamais eu de problème avec. La MPA conseille (merci encore) aussi le registrar Njalla (créé par le cofondateur de ThePirateBay), qui semble les agacer de par leur résistance.

Ne vous fatiguez pas non plus à essayer de protéger votre Whois, vous avez de toute façon mis de fausses informations dedans.

Le seul endroit où il faut faire attention est le TLD de votre nom de domaine, vérifiez que son Registry n'a pas la main légère (comme celui de notre .io qui nous l'a suspendu). Vous trouverez des articles sur Google parlant des TLD qui ont l'habitude de bloquer, évitez les juste (.to, .io, .ws ...).

L'important est d'avoir plusieurs noms de domaines en réserve à l'avance.

4.5 Les hébergeurs (Uptobox, 1Fichier, ...)

Nous n'avons jamais eu aucun partenariat avec aucun hébergeur présent sur le site, même si certains nous l'avaient proposé, nous n'avons pas besoin de leur argent (note : ni Uptobox ni 1Fichier n'a jamais rien proposé, nous n'avons aucun contact avec eux). On se contentait d'utiliser les services qui nous semblaient être intéressants pour les utilisateurs.

Il faudra tout de même noter que les hébergeurs de fichiers (ou lecteurs streaming), et particulièrement Uptobox, sont très efficaces sur les réponses aux plaintes DMCA. Uptobox avait une réactivité de moins de 24h sur la suppression des fichiers qui recevaient des plaintes. Cela pouvait monter à 800 liens supprimés par jour, et 2000 liens quand les ayants-droits se chauffaient (en tout cas avant qu'on mette en place notre captcha Made in Time2Watch, qui a stoppé 80% des plaintes).

Autant dire que si vous n'avez pas de système de détection de liens morts et de réupload automatique, vous allez devenir un cimetière de liens assez rapidement. À vous de trouver un système pour sauvegarder tous vos fichiers efficacement (et pas chez vous...).

4.6 L'argent dans tout ça

L'argent, que ce soit dans ce milieu ou ailleurs, a toujours été un sujet tabou en France. Et de ce côté-là nous ne pourrions pas vous apporter plus de détails sur les entreprises -que les médias aiment bien qualifier de mafieuses- de certains sites Warez du top FR, tout simplement car nous n'avons jamais trempé là-dedans. C'est un sujet qui est sans doute très intéressant, le blanchiment, les sociétés écrans, etc, mais c'est surtout un sujet que nous ne maîtrisons pas du tout (et sur lequel nos relations étaient toujours muettes), alors nous n'avons rien à dire dessus, sinon des bêtises. Et comme c'est un sujet que nous ne maîtrisons pas, nous n'avons jamais joué avec non plus. Maîtrisez ce que vous faites, ne faites que ce que vous maîtrisez.

Ce que nous pouvons néanmoins affirmer, c'est qu'aucun membre de l'équipe n'a jamais touché d'argent généré par les revenus publicitaires du site (que ce soit les administrateurs ou le reste de l'équipe). Ce n'était tout simplement pas notre philosophie, l'argent n'était pas notre motivation (on en voit certains qui rigolent au fond, ça vous fait bizarre hein). Pouvez-vous donner le nom d'un site Warez avec si peu de publicité que Time2Watch ? Non. La plupart des pages du site n'en comportaient d'ailleurs même pas une seule (dont la page d'accueil), et les seules publicités étaient sous la forme de 2 faux boutons de téléchargement sur certaines pages. Alors oui ce genre de bouton est sale, ça trompe les gens qui ne sont pas habitués ou qui n'ont pas Adblock, mais c'est le grand minimum qu'on pouvait se permettre pour faire tourner le site avec les régies de ce milieu.

On ne vous conseillera d'ailleurs pas non plus de régie publicitaire, quand vous aurez suffisamment de visibilité ce sont elles qui viendront vous démarcher par mail avec des phrases accrocheuses du style "Nous travaillons déjà avec [tel ou tel site], venez chez nous, on vous offre 15% de plus que votre régie actuelle".

"Si vous ne gagnez pas d'argent, où vont les millions que le site génère ?". Avec le peu de pubs et la perte de trafic organique, rassurez vous, le site ne générerait pas tant, et l'argent restait dans un cercle fermé pour rendre le site autosuffisant, et n'en sortait pas. Entre 60 et 80% (suivant les mois) nous servaient pour les différents serveurs, notre infrastructure (qui n'était pas si exorbitante mais quand même bien foutue), puis pour l'acquisition de certains outils et services nécessaires au site, un peu de côté pour prévenir des coups durs (changements de serveurs à l'improviste etc), et le reste dans des donations comme aux associations Save The Children ou Trees For The Future (donations dont vous aviez pu vérifier certaines transactions bitcoin sur notre compte Twitter). C'est d'ailleurs là qu'ira le peu qu'il reste.

Nous n'essayons pas de nous laver les mains, ou de jouer aux Saints. Déjà ce serait bien hypocrite, mais surtout nous n'avons en fait pas grand chose à faire de votre avis sur le sujet, de ce que vous croyez ou non. Mais c'est un fait, et c'est important. Et croyez-nous, l'argent

n'apporte que des problèmes, si c'est votre motivation, eh bien bon courage...

Une chose est sûre, le peu de publicités que nous mettions était largement suffisant pour faire tourner un gros site, même un site du top 3 FR. Si vous voyez un gros site avec plus de publicités que ce qu'on avait (c'est à dire tous les sites du Warez français), alors c'est que le but de ce site est uniquement de gagner de l'argent, quoiqu'ils puissent vous dire. On connaît le coût de l'offshore, les coût de fonctionnement d'un site similaire au nôtre, vous ne bernez personne, en tout cas pas nous.

5 Conclusion

It's not Time to Watch anymore.

Références

- [1] AERIS22. *L'ALPA qui détourne une ordonnance*. URL : <https://twitter.com/aeris22/status/1233124830507085824>.
- [2] CoPeerRight AGENCY. *The first international agency fully specialized in online content protection*. URL : <https://www.co-peer-right-agency.com/>.
- [3] Alexandre ARCHAMBAULT. *S'abriter derrière des solutions de type CloudFlare ne plaide pas en faveur des sites*. URL : <https://twitter.com/AlexArchambault/status/1233422504418586624>.
- [4] Marc Rees - NEXTINPACT. *L'Alpa réclame de Google le déréférencement d'une centaine de sites de streaming*. URL : <https://www.nextinpact.com/article/30090/108761-lalpa-reclame-google-dereferencement-dune-centaine-sites-streaming>.
- [5] Tribunal Judiciaire de PARIS. *Jugement en la forme des référés rendu le 16 janvier 2020*. URL : <https://cdn2.nextinpact.com/medias/jugement-timewatch.pdf>.
- [6] TORRENTFREAK. *RIAA and MPA Want Domain Registries and Njalla on US Piracy Watchlist*. URL : <https://torrentfreak.com/riaa-and-mpa-want-domain-registries-and-njalla-on-us-piracy-watchlist-201110/>.