Date de publication Jeudi 29 janvier 2009 à 22:06:57 **par** colok
Catégorie Nouveautés

La justice Française condamne ZATAZ.COM à se taire

Pour avoir aidé une société à protéger ses données sensibles, le fondateur de ZATAZ.COM se retrouve devant la justice. Nous ne donnerons pas le nom de l'entreprise qui nous a assigné devant le TGI de Paris, la justice Française vient de nous interdire de publier son nom et de remettre en ligne l'article qui concerne notre différent...

...Mais nous vous devons la transparence, d'autant plus que vous avez été plusieurs lecteurs à vous rendre compte de la disparition de cet article sur ZATAZ.COM. Il était une fois... Tout a débuté fin septembre 2008. Un lecteur [son anonymat est resté et restera de mise... même sous la menace, NDR] nous informait d'une découverte qu'il trouvait très étonnante.

Via un moteur de recherche, du même type que Google, le lecteur s'était aperçu qu'une société avait été référencée par le spider, le robot référenceur du moteur en question.

Seulement, à défaut de pages web référencées, le moteur de recherche a aspiré le répertoire, le Directroy, l'arborescence d'un espace FTP en accès libre. Celui de la société en question.

Informé de la chose, ZATAZ.COM met en place sa procédure d'alerte. D'abord, je vais vérifier les propos de notre lecteur, comme je le fais depuis 13 ans. Je me rends sur ce moteur de recherche, je tape les mots clés que le lecteur m'avait indiqué, ainsi que quelques autres mots clés, afin de constater cet étrange référencement.

Il ne me faudra pas plus de 30 secondes pour comprendre le problème et la dangerosité des données proposées par le moteur de recherche. L'arborescence en question donnait accès à des informations sensibles.

Les répertoires de cette entreprise avaient été aspirés. Il suffisait ensuite de cliquer sur les liens proposés par le moteur de recherche pour se retrouver dans des comptes bancaires, des documents administratifs, marketing, appartenant à cette société. Je n'ai strictement rien téléchargé, sauvegardé. Seul téléchargement, la cache de mon navigateur lors du clic de souris sur le lien donné par le moteur de recherche.

Je vais réaliser deux uniques captures écrans et prévenir, par deux fois d'abord, la société.

Une quarantaine d'heures plus tard, toujours aucune réponse à mes deux courriels. Je décide, cette fois, de continuer la procédure d'alerte par un appel téléphonique. Je réussi à joindre une responsable commerciale de l'entreprise. S'en suit une explication de ma constatation.

Elle va me transmettre deux courriels. Le sien et celui de l'informaticien de l'entreprise. Puis, plus rien ! Une semaine passe, je vais recevoir un courrier de remerciement de l'employée contactée par ttéléphone: "Merci de nous avoir signalé cette sérieuse anomalie, cela a permis à notre informaticien de corriger immédiatement."

Bref, tout est bien qui finit bien. Le problème est corrigé, je décide d'en écrire un petit article. Ce dernier se contentait de relater les faits, l'aide (comme nous avons pu le faire auprès de 7.000 entreprises, PME, sites étatiques, associations, ...) et un petit rappel de la Loi Informatique et Liberté (CNIL 1978). Dans l'article, aucunes informations techniques, aucunes

informations sur l'adresse du serveur, ni le nom du moteur de recherche, les mots clés, ... alors que nous aurions pu le faire. L'accès avait été corrigé et cela aurait pu prouver nos dires. J'ai préféré vous proposer deux captures écrans (Les données sensibles avaient été cachées dans ces photographies). 24 décembre, 10 heures du matin Deux mois plus tard, nous sommes le 24 décembre, il est 10h. Le ciel est bleu, le Père-Noël était attendu sous le sapin familial... et, joie de la nativité, un huissier toc à la porte de mon domicile.

Il vient m'annoncer que la société avait fait appel à la justice "en urgence" pour faire retirer l'article. Soit, deux mois après la diffusion de ce dernier. Une assignation en référé d'heure à heure devant le Président du Tribunal de Grande Instance de Paris. Bien évidement, je retire illico l'article. Je suis invité à m'expliquer le 12, puis le 19 janvier devant Monsieur le Juge.

Pour cela, il me faut prendre un avocat (6.000 euros); payer les constations d'huissier (155 " ; 3 x 175 "); me déplacer (Prendre des jours de congés, essence, péage, ...). A partir de là, je peux avoir accès au dossier du cabinet d'avocat de cette entreprise.

Pour faire disparaître l'article de ZATAZ.COM, l'argument mis en avant par la société est limpide comme de l'eau de roche. Il m'est reproché tout simplement d'avoir piraté le ftp de l'entreprise pour écrire l'article ! Bilan, en plus de demander la destruction de l'article via le TGI, cette société m'assigne aussi devant le Tribunal Correctionnel pour diffamation, en fevrier prochain. Son nom est Pert, Expert Le cabinet d'avocats de cette société se base sur un rapport d'expertise particulièrement étonnant. Comme déjà expliqué, j'ai eu la preuve de l'existence de ces données en utilisant un moteur de recherche et mon navigateur web. [A noter que ous sommes le 28 janvier, le moteur de recherche en question recense TOUJOURS l'ensemble des dossiers, répertoires et fichiers sensibles de cette société].

L'expert explique, par exemple, que cet accès était la résultante obligatoire d'un piratage.

Il explique dans son rapport l'apparition d'un étrange login "Anonymous" dans les logs de l'entreprise. Les logs du serveur de cette entreprise indiquaient ceci :

29/09/2008 - IP - User Anonymous 331 - Pass Mozilla@example.com 530 ou encore

02/10/2008 - IP - User Anonymous 331 PASS IEUser@ 530 ou encore

02/10/2008 - IP - User Anonymous 331 Pass ieuser@microsoft.com 530 Pour l'expert de cette société, aucun doute, se sont de mystérieux codes pirates.

Pour avoir une explication de l'existence de ces « mystérieux codes », il aurait suffit de lire un article diffusé par l'université de Marseille traitant de ce Monsieur Anonymous « ANONYMOUS : pour permettre les accès publics sous le compte anonymous sans avoir a donner de mot de passe secret. (dans ce cas, seule l'adresse de messagerie suffit comme mot de passe). »

Dans les trois cas des logs de l'entreprise, le code USER et PASS sont générés automatiquement par les navigateur Firefox (Mozilla@example.com) et Internet Explorer (IEUser@; ieuser@microsoft.com) lors d'une connexion autorisée ! Plus intéressant, dans les logs fournis par cette société, nous avons découvert que le moteur de recherche était passé par deux fois sur le serveur de cette entreprise. Le 11 septembre, puis le 28 septembre, pour rafraichir son contenu, sa base de données. Les log

affichaient l'ip et le nom du robot référenceur... avec un joli "Anonymous" d'accès. Détail qu'il est toujours possible de vérifier ce 28 janvier.

Pour rappel, j'ai eu l'information du lecteur le 29 septembre. Bizarrement les logs entre le 11 et 28 septembre ne donnaient plus aucunes informations, pas un ip, connexions, ... mais à partir du 29 septembre, date de ma constatation et de mon alerte, un véritable arbre de Noël d'IP dans des logs en question.

A noter que le moteur de recherche affiche toujours, ce jour, les répertoires de cette société. Ils ne sont plus accessibles d'un simple clic depuis mon intervention, mais le moteur de recherche a toujours dans sa mémoire ce qu'il a vu, lu et répertorié. Condamné Fin janvier, le juge a rendu son verdict. Il a constaté que l'article avait été retiré de ZATAZ.COM (Constatation pas bien difficile à faire, j'ai payé un huissier pour le faire constater). J'ai d'ailleurs précisé que je ne souhaitais pas remettre en ligne cet article dans la mesure ou le moteur de recherche continuait à référencer les données sensibles, que dans les logs j'ai découvert qu'au moins un pirate Turc avait tenté de pénétrer le serveur, 48 heures après sa correction.

Le juge a donc ordonné la suppression de toutes données ou fichier auxquels j'ai pu accéder sur le serveur en question et m'interdit de publier ou diffuser tous contenus s'y rapportant sous peine de payer 400 euros par jour. Comme vous le savez, nous n'avons JAMAIS rien téléchargé et ne diffusons JAMAIS rien qui puisse mettre en danger qui que se soit. Et bien évidement, pas question de remettre cet article. Ce qui est "rassurant", dans cette ordonnance, est le fait que le verdict de Monsieur le Juge semble indiquer que les données étaient bien accessibles ! Mais ce n'est pas le problème. Mission avoué de l'entreprise, faire disparaître l'article. Je suis aussi condamné à rembourser les frais d'avocats en plus de ce que j'ai déjà déboursé pour me défendre !

C'est la première fois qu'une telle aventure me tombe sur le coin de la souris. Nous avons pu aider (Les lecteurs, amis et moi) plus de 7.000 entreprises. Dans certains cas j'ai relayé l'information pour en avertir les utilisateurs, rappeler ce qu'indique la loi. C'est aussi mon métier de journaliste que d'informer, donner les faits.

Bref, nous obeissons, comme nous l'avons toujours fait, à la loi et à la justice. L'article et les deux captures écrans ont été détruits. Certes, il aurait été si simple de diffuser cet article, ailleurs, sur d'autres sites, journaux, pour qui je travaille. Mais je ne suis pas comme ça.

Je n'en veux pas un seul instant au patron de cette entreprise. Il a protégé son travail, sa création en écoutant son personnel. Des employés qui lui ont dit qu'il y avait eu piratage. Espérons seulement que maintenant, il va faire le ménage en interne pour son bien et celui de ses clients. Espérons aussi et surtout pour lui qu'aucun client n'aura eu le moindre prélèvement frauduleux entre le 11 et le 28 septembre, date ou le moteur de recherche a référencé les données laissées en accès libre. Cette aventure n'est pas une mésaventure pour moi. Cela ne m'empêchera pas de continuer à faire mon métier de journaliste. Je le suis depuis bientôt 18 ans. Je continuerai à alerter, prévenir, aider, les lecteurs, comme je le fais gratuitement sur ZATAZ.COM depuis 1996. Je vais juste reprendre un propos d'un de mes professeurs qui me disait un jour qu'"Un journaliste doit tout savoir, mais ne pas tout dire!".

Cela ne m'empêchera pas, non plus, de relayer des informations de lecteurs, tout en garantissant l'anonymat de ces derniers. Au risque de me retrouver devant la Justice. Si jamais vous souhaitez nous soutenir financièrement, il en dépend clairement de la survie de ZATAZ.COM, nous avons mis en place deux possibilités : Par Le service Allopass ou via Paypal. Nous vous tiendrons au courant, à partir de cette page, du montant des dons, si dons il y a ! ATTENTION, aucune demande de dons par courriel, forum, ... ne sera demandé. Petite précision pour les trous "d'cul" de phishers.

Billet issu du site internet Colok Traductions:
https://www.colok-traductions.com

URL du billet
https://www.colok-traductions.com/index.php?op=billet&bid=1320