Cybersécurité : les 5 erreurs fatales de Mossack Fonseca

Après avoir accédé en quelques heures à une popularité mondiale, via les révélations des Panama Papers, le cabinet d'avocats panaméen Mossack Fonseca a eu droit à un audit de sécurité à l'échelle planétaire. Nombreux sont les chercheurs en cybersécurité à s'être rués sur les infrastructures de Mossack Fonseca pour les décortiquer et en identifier les potentielles failles de sécurité. Le moins que l'on puisse dire, c'est que le cabinet spécialisé dans les montages d'évasion fiscale l'est beaucoup moins en matière de cybersécurité. Et à un degré qui, dans certains cas, ne cesse pas de surprendre.

Si la firme panaméenne affirme que la gigantesque fuite de données (2,6 To de données, 11 millions de documents entre 1977 et 2015, portant sur 214 488 structures offshore) à l'origine des révélations de la presse résulte d'un piratage informatique, visant à « *saper sa compétitivité* », la somme incroyable des lacunes sécuritaires dévoilées au fil des jours s'apparente à de la négligence. Revue de détails :

1) Les lacunes du serveur d'e-mails

MX Server	Pref	Con-nect	All-owed	Can Use	TLS Adv	Cert OK	TLS Neg	Sndr OK	Rcvr OK
smtp.mossfon.com [200.46.144.4]	10	OK (94ms)	OK (1,324ms)	OK (224ms)	FAIL	FAIL	FAIL	OK (1,737ms)	FAIL
smtp2.mossfon.com [200.46.144.136]	20	OK (93ms)	OK (93ms)	OK (225ms)	FAIL	FAIL	FAIL	OK (506ms)	FAIL
micron.mossfon.com [200.46.144.2]	20	OK (93ms)	OK (93ms)	OK (227ms)	FAIL	FAIL	FAIL	OK (507ms)	FAIL
smtp1.mossfon.com [200.46.144.135]	20	OK (93ms)	OK (93ms)	OK (224ms)	FAIL	FAIL	FAIL	OK (504ms)	FAIL
Average		100%	100%	100%	0%	0%	0%	100%	0%

Dans une lettre envoyée à ses clients le 1er avril – défense de rire -, Mossack Fonseca admet avoir lancé une enquête sur le piratage d'un serveur de mails. Chez nos confrères de *Reuters*, Ramon Fonseca, un des deux co-fondateurs, assure que cette attaque a eu une portée « *limitée* ». Utilisant un outil librement disponible (CheckTLS), le chercheur en sécurité Christopher Soghoian, également expert de l'ACLU (American Civil Liberties Union, une association de défense des libertés publiques), assure que les serveurs d'e-mails de la firme d'avocats **n'emploient pas le chiffrement TLS**, tableau à l'appui (voir ci-dessus). De quoi faciliter l'interception des communications. Et Christopher Soghoian de s'amuser à interpeller les cabinets d'avocats dans un tweet : « *Si vous ne voulez pas ressembler à Mossack Fonseca, demandez notamment à votre département IT de chiffrer vos e-mails.* » Ajoutons à ce tableau déjà peu reluisant que le webmail de Mossack Fonseca repose sur une version d'Outlook Web Access datant de… 2009.

> *Law firms: You don't want to be like Mossack Fonseca. Among other things, ask your IT dept to encrypt your emails. pic.twitter.com/Yxut3g28Ng*
>
> *— Christopher Soghoian (@csoghoian) 5 avril 2016*

2) Des CMS troués

Dès mardi dernier, un article de *Forbes* pointait le fait que le site principal de Mossack Fonseca utilisait une version vieille de trois mois de WordPress, mouture connue pour renfermer des vulnérabilités. Juste un hors d'œuvre, car le magazine américain relève surtout que le portail clients du cabinet, utilisé par ces derniers pour accéder à des informations confidentielles, tourne sur une version de Drupal, vieille de trois ans. Or, cette mouture étiquetée 7.23 renferme **25 failles connues à ce jour**, dont probablement la plus grave jamais découverte dans Drupal (cet épisode, datant d'octobre 2014, est connu par la communauté travaillant sur le CMS comme le 'Drupalgeddon'). Une autoroute permettant à des pirates dotés de bonnes connaissances techniques de piocher dans les données sous-jacentes du portail. Par ailleurs, *Wired UK* relève que le même portail est vulnérable à l'attaque Drown, qui touche les serveurs supportant le protocole obsolète SSL v2.

3) Un serveur HTTP mal configuré

Mais, il y a pire. Si on en croit une enquête poussée de *Unicorn Riot*, un collectif de journalistes, le portail en question souffre aussi de graves lacunes de configuration, qui aboutissent à exposer sa structure et son code source aux navigateurs standards. Selon les conclusions de *Unicorn Riot*, qui se fonde sur les données librement accessibles sur ce portail – sans authentification -, Mossack Fonseca emploie pour ce service **un serveur HTTP et une base de données Oracle**. Le premier est un fork d'Apache 2.2. « *Il est si mal configuré qu'il publie pour tous les visiteurs une bonne partie du code du portail sous la forme de texte brut* », écrit Unicorn Riot. Bref, le portail souffre non pas d'une grave vulnérabilité – celle de Drupal -, mais bien de plusieurs. Et cette erreur de configuration peut, selon cette même analyse, permettre à un assaillant d'installer et de faire tourner un code PHP malicieux sur le serveur.

Plus cocasse encore : parmi ces données librement accessibles, *Reflets.info* a d'ailleurs déniché les fichiers de sauvegarde d'une application interne et d'un jeu de données associé. Les fichiers de configuration donnant eux accès au login et mot de passe, affichés en clair ! Les deux étant d'ailleurs identiques…

4) Une base Oracle qui interpelle

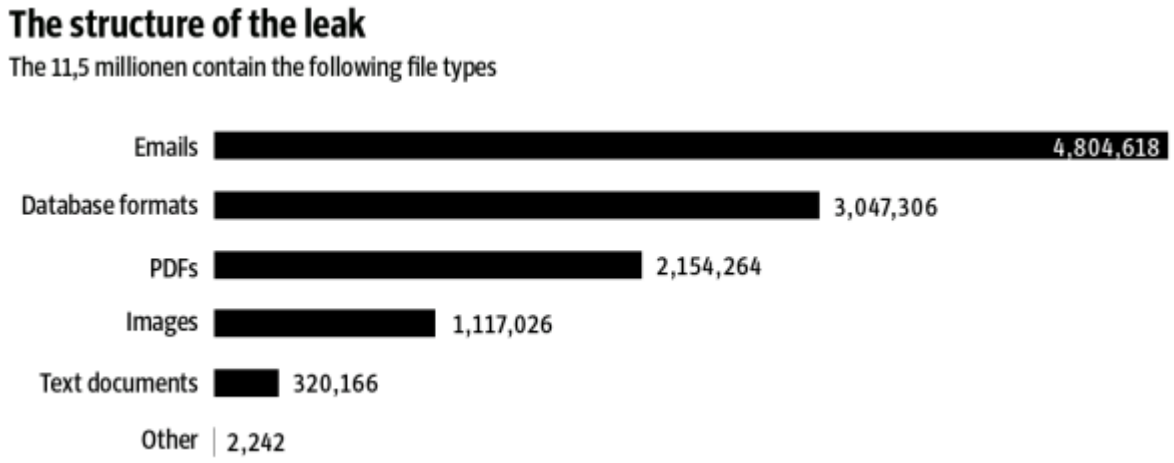
Parmi les informations librement accessibles sur le portail via une simple URL, figurent les modules qui viennent se greffer à Drupal. Parmi eux, un add-on autorisant l'emploi du CMS au-dessus d'une base de données Oracle. Plus mis à jour depuis 2013, ce module trahit l'emploi d'une architecture peu banale : rares sont en effet les sites Web à reposer sur une base Oracle, réputée très onéreuse. *Unicorn Riot* y voit un indice de la façon dont les documents pourraient avoir fuités. « *En général,*

mettre en œuvre des technologies coûteuses comme une base et un serveur HTTP Oracle pour faire tourner un site isolé n'a pas de sens économique », relève l'analyse de Unicorn Riot, suggérant que la base de données pourrait être le support d'autres applications de Mossack Fonseca, donc renfermer de grands volumes de données.

L'association d'**un Drupal vintage et d'une base de données probablement centrale** dans l'infrastructure IT du cabinet s'avère explosif. *Unicorn Riot* décrit ainsi une attaque par piratage de session, permettant à un hacker d'apparaître comme un utilisateur légitime. L'utilisation de cette technique associée à un compte administrateur ouvrirait un passage vers l'ensemble des données de la base Oracle.

5) Le script Google Analytics qui tue

Quand on a un site Web, on aime savoir combien de visiteurs y accèdent. Si possible gratuitement, via un service comme Google Analytics. Sauf, serait-on tenté d'ajouter, quand on préfère la discrétion. Repéré par *Reflets.info*, la présence d'un script Google Analytics sur le portail client de Mossack Fonseca relève presque du gag. Ou du **cadeau au fisc américain**. La présence de ce script permet en effet à Google de stocker les adresses IP des personnes se connectant au portail, une base de données que l'administration américaine pourrait être tentée de se procurer…



Hack ou *insider job* ? En l'état, cette collection d'erreurs ne suffit pas à valider la thèse du piratage, une thèse que défend mordicus le cabinet d'avocats. Ramon Fonseca, un de ses co-fondateurs, a ainsi affirmé à la *BBC* que le scandale des Panama Papers ne résultait pas d'une fuite interne, mais d'un piratage orchestré depuis des serveurs situés hors du Panama. Si tel est le cas, le ou les assaillants ont manifestement pris leur temps (exfiltrer 2,6 To de données – 10 fois plus que la fuite de Sony Pictures – sans se faire repérer demande de la patience) et ont probablement infiltré plusieurs systèmes sur de longues durées, les documents transmis par la source anonyme du quotidien allemand *Süddeutsche Zeitung* étant de nature diverse (voir le graphique ci-dessus). Un profil qui pourrait, notamment, correspondre à celui d'**un service de renseignement** d'un état décidé à porter un coup décisif à la fraude fiscale. Ou à celui d'**un ou plusieurs activistes**, exploitant patiemment les grossières erreurs de sécurité de Mossack Fonseca.

A lire aussi :

Linkurious, la start-up du Big Data qui surfe sur les Panama Papers

Crédit photo : Garagestock / Shutterstock