L'affaire Bluetouff, c'est l'histoire incroyable d'un internaute qui sera condamné au pénal (3000 € d'amende et inscription au casier judiciaire) pour avoir simplement suivi un lien Google puis téléchargé des documents accessibles publiquement. Depuis son début, initié par la plainte de l'Anses le 6 septembre 2012, jusqu'à son terme conclu par l'arrêt de la cour de cassation le 20 mai 2015, l'affaire Bluetouff a fait l'objet de très nombreux articles dans la presse ou sur le Net. Mais une affaire de cybercriminalité n'est jamais très simple à comprendre car elle demande des connaissances juridiques et des compétences en sécurité informatique ou plus précisément en matière d'investigation numérique légale (forensic). En tant qu'expert judiciaire près la cour d'appel de Montpellier, je vous propose de réexaminer en détail le déroulement de cette histoire. L'objectif n'est pas de débattre une nouvelle fois sur le bien-fondé de la décision de la cour d'appel ou de la compétence informatique des magistrats mais plutôt de comprendre pourquoi Bluetouff a été condamné et ce qu'il aurait dû faire pour ne pas l'être malgré la plainte de l'Anses et les investigations de la DCRI.

- Rappel des faits
- Le jugement en 1ère instance par le TGI de créteil
- Le jugement de la Cour d'appel de Paris
- Le jugement de la Cour de cassation
- En garde à vue le silence est un droit !
- Sans aveux, une condamnation était-elle possible ?
- Conclusion

Rappel des faits

En août 2012, un internaute blogueur (reflets.info, bluetouff.com) dénommé Bluetouff, de son vrai nom Olivier Laurelli, navigue sur Internet via un serveur VPN hébergé au Panama. Il fait des requêtes sur Google puis suit un des liens proposés par le moteur de recherche pour atterrir sur un serveur de l'Anses (*l'Agence nationale de la sécurité sanitaire et l'alimentation, de l'environnement et du travail).* Il parcourt l'arborescence des répertoires du serveur et remonte jusqu'à la page d'accueil sur laquelle il constate la présence d'un contrôle d'accès (authentification par identifiant et mot de passe). *Il continue ensuite sa navigation dans les sous-répertoires et télécharge de nombreux documents (environ 8000 documents représentant un volume de* 7,7 Go). Il utilise quelques extraits issus de cette extraction (environ 200 Mo) pour publier (sous le pseudo Bluetouff) un article sur les nano-matériaux sur le site reflets.info. Il est important de noter à cet instant, qu'il n'y a strictement aucune protection d'accès à ces documents (aucun mot de passe ni chiffrement des données) et que tout internaute peut y accéder via Google avec un simple navigateur. Il faut préciser également, qu'il n'existe aucune mention de confidentialité sur les-dit documents.

Le 3 septembre 2012, un chef d'unité de l'Anses découvre un article relatif aux nano-matériaux mis en ligne sur le site d'information reflets.info, article accompagné d'un document Powerpoint de l'agence destiné uniquement à un usage interne provenant vraisemblablement de l'Extranet de l'Anses.

Le 6 septembre 2012, le RSSI de l'Anses dépose plainte auprès des services de police de Maisons-Alfort (94) pour intrusion dans le système informatique de l'Anses et vol de données. L'Anses étant considérée par l'état comme un opérateur d'importance vitale (OIV), c'est la DCRI (devenue DGSI depuis le 12 mai 2014) qui sera chargée de l'enquête.

L'analyse des journaux de connexions du serveur extranet et du firewall de l'Anses confirme les éléments fournis par l'agence lors du dépôt de plainte à savoir l'extraction les 27 et 28 août 2012 d'un volume d'environ 8 Go de donnée vers une adresse IP localisée au Panama. Cette adresse est rapidement identifiée comme provenant d'un serveur d'une société Panaméenne fondée et dirigée par Olivier Laurelli. D'autre part l'enquête de la DCRI permet d'identifier très rapidement Olivier Laurelli comme étant l'internaute agissant sous le pseudonyme Bluetouff.

Le 21 novembre 2012, Olivier Laurelli est placé en garde à vue durant 30 heures au siège de la DCRI. Lors de son audition, il reconnait avoir récupéré via son VPN panaméen l'ensemble des données accessibles sur le serveur extranet de l'Anses. Il reconnait également avoir parcouru l'arborescence des répertoires et être remonté jusqu'à la page d'accueil sur laquelle il constate l'apparition d'une « mire de login » destinée à restreindre les accès par une authentification utilisateur. C'est

le point clé de cette affaire : la reconnaissance formelle par Olivier Laurelli que les données n'étaient pas publiques mais bel et bien protégées par un mécanisme d'authentification mais dont une défaillance technique (dont l'entière responsabilité appartient à l'Anses) rendait accessibles publiquement. C'est d'ailleurs pour cette même raison que les données ont pu être indexées par Google.

Le jugement en 1ère instance par le TGI de créteil

L'affaire sera jugée en correctionnelle par le Tribunal de Grande instance de Créteil. Dans son jugement en date du 23 avril 2013, le tribunal indique :

Concernant l'accès frauduleux et le maintien frauduleux dans un système de traitement automatisé de données :

Néanmoins, il n'est pas contesté par l'Anses qu'une défaillance technique existait dans le système et que Monsieur Olivier L. a pu récupérer l'ensemble des documents sans aucun procédé de type « hacking ».
Compte tenu de l'ensemble de ces éléments, même s'il n'est pas nécessaire pour que l'infraction existe que l'accès soit limité par un dispositif de protection, le maître du système, l'Anses, en raison de la défaillance technique, n'a pas manifesté clairement l'intention de restreindre l'accès aux données récupérées par Monsieur Olivier L. aux seules personnes autorisées. Monsieur Olivier L. a pu donc légitimement penser que certaines données sur le site nécessitaient un code d'accès et un mot de passe mais que les données informatiques qu'il a récupérées étaient en libre accès et qu'il pouvait parfaitement se maintenir dans le système. En conséquence, il convient de relaxer Monsieur Olivier L. des chefs d'accès frauduleux et maintien frauduleux dans un système de traitement automatisé des données.

Concernant le vol des documents téléchargés et enregistrés sur plusieurs supports :

Selon l'article 311-1 du code pénal, le vol est la soustraction frauduleuse de la chose d'autrui.

En l'espèce, en l'absence de toute soustraction matérielle de documents appartenant à l'Anses, le simple fait d'avoir téléchargé et enregistré sur plusieurs supports des fichiers informatiques de l'Anses qui n'en a jamais été dépossédée, puisque ces données, élément immatériel, demeuraient disponibles et accessibles à tous sur le serveur, ne peut constituer l'élément matériel du vol, la soustraction frauduleuse de la chose d'autrui, délit supposant, pour être constitué, l'appréhension d'une chose. En tout état de cause, Monsieur Olivier L. a pu légitimement penser que ces documents étaient librement téléchargeables puisque non protégés par un quelconque

système. Il n'y a pas eu de sa part une volonté d'appropriation frauduleuse de ces fichiers informatiques et donc il n'y a pas d'élément intentionnel de l'infraction.

Le 23 avril 2013, Olivier Laurelli est donc relaxé par le tribunal de créteil. « Tout est bien qui finit bien » devait-il sans doute se dire mais c'était sans compter sur le parquet de Paris qui décide de faire appel de cette décision.

Le jugement de la Cour d'appel de Paris

Devant la cour d'appel, Bluetouff devait répondre de trois chefs d'accusation :

- avoir accédé frauduleusement au serveur de l'Anses,
- s'y être maintenu frauduleusement,
- avoir soustrait frauduleusement les documents stockés sur cet extranet, en les dupliquant sur plusieurs supports.

Par un arrêt en date du 5 février 2014, la Cour d'appel de Paris confirme le jugement du TGI de Créteil concernant l'absence de caractère frauduleux de l'accès mais elle déclare *Bluetouff* coupable de maintien frauduleux et de vol de données.

S'agissant de l'accès frauduleux et dans la mesure où l'Anses avait elle-même reconnue une erreur de sa part dans la gestion des accès à leur serveur, les magistrats de la cour d'appel relaxe Bluetouff de ce chef d'accusation.

Concernant le maintien frauduleux, la Cour d'appel souligne qu'après avoir accédé au site de l'Anses, *Bluetouff*, en parcourant l'arborescence, avait pu constater que l'accès était soumis à des restrictions d'accès. Il avait donc :
« parfaitement conscience de son maintien irrégulier dans le système de traitement automatisé de données visité où il a réalisé des opérations de téléchargement de données à l'évidence protégées ».

Concernant le vol de données, la Cour de cassation avait déjà par le passé qualifié de vol une copie de données (Cass.crim., n°07-84.002, 4 mars 2008, X/ Société Graphibus). Dans ses conclusions sur l'affaire *Bluetouff*, l'avocat général Frédéric Desportes s'est ainsi exprimé : *« Il serait paradoxal que la soustraction frauduleuse d'un document papier sans intérêt soit passible de trois ans d'emprisonnement mais non celle de milliers de fichiers stratégiques alors même que ces fichiers ne sont jamais que des documents numériques ou numérisés pouvant être imprimés et donc matérialisés ».*

A ce sujet, il est important de noter un changement récent de la législation. Ainsi

en application de la Loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, le code pénal (art. 323-3) sanctionne désormais l'extraction de données, mettant ainsi un terme au débat relatif au « vol de données ». Le Code pénal réprime donc aujourd'hui non seulement l'introduction, la modification et la suppression frauduleuses de données mais également l'extraction, la détention, la reproduction et la transmission frauduleuses de ces données. Bien entendu, la promulgation de ce texte étant postérieure aux faits, il ne pouvait être appliqué dans le cas de l'affaire Bluetouff.

Ainsi, par un arrêt en date du 5 février 2014, la cour d'appel de Paris a condamné Olivier Laurelli pour maintien frauduleux dans un système de traitement automatisé de données et vol de données à une peine délictuelle de 3000 € assortie d'une inscription au bulletin no2 de son casier judiciaire.

Le jugement de la Cour de cassation

Suite à la décision de la cour d'appel, Olivier Laurelli a donc décidé, par l'intermédiaire de son avocat Me Olivier Iteanu, de formuler un pourvoi en cassation. Dans son pourvoi, Me Iteanu avance de nombreux arguments :

- On ne commet pas le délit de maintien frauduleux dans un système de traitement automatisé de données (STAD) quand on utilise un moteur de recherche et un navigateur pour pénétrer un système non protégé.
- On ne peut déduire de la découverte d'un contrôle d'accès, la conscience d'un maintien irrégulier dans un système informatique.
- Il revient au responsable du système de manifester clairement et expressément sa volonté d'interdire ou restreindre l'accès.
- Les informations contenues dans une partie d'un site non protégé sont du coup réputées non confidentielles et publiées avec l'accord des intéressés.
- Il y a une contradiction évidente à reprocher à un internaute d'avoir « *réalisé des opérations de téléchargement de données à l'évidence protégées* » et « *fait des copies de fichiers informatiques inaccessibles au public* » en admettant dans le même temps qu'il a pu accéder librement à ces données.
- Le vol exige juridiquement la soustraction frauduleuse de la chose d'autrui (tel un individu a une chose, il se la fait voler, il ne l'a plus). Il n'y a donc pas de vol lorsqu'il n'y a pas de dépossession, sauf à violer le Code pénal qui est d'interprétation strict.

Malgré cet argumentaire tout à fait pertinent de Me Iteanu, les magistrats de la Cour de cassation ont estimé que la Cour d'appel avait jugé en droit et avait correctement interprété la Loi. En conséquence et en l'absence d'éléments nouveaux

dans le dossier, la Cour de cassation rejette le pourvoi par un arrêt du **20 mai 2015** et confirme la condamnation prononcée par la Cour d'appel de Paris à l'encontre d'Olivier Laurelli.

Le dernier recours pour Olivier Laurelli est maintenant de saisir la CEDH (Cour Européenne des Droits de l'Homme) comme l'a indiqué son avocat Me Olivier Iteanu dans Le Parisien. Ce recours reste cependant très hypothétique dans la mesure où seulement 5 % des plaintes reçues par la CEDH sont effectivement examinées par la Cour. La CEDH n'accepte en effet d'examiner que les affaires démontrant une certaine probabilité de violation des droits garantis par la Convention européenne des droits de l'homme dont l'entrée en vigueur remonte à 1953.

En garde à vue le silence est un droit !

Il y a bien sûr un coté subjectif dans le jugement d'une affaire pénale et une procédure n'est rarement jouée d'avance. Il n'est pas rare en effet d'être condamné en première instance puis relaxé en appel même si dans le cas de l'affaire Bluetouff c'est le contraire qui s'est produit. Dans ces conditions, et même si l'on pense n'avoir rien fait de répréhensible, il vaut mieux lors des auditions en garde à vue, ne rien dire ! C'est ce l'on appelle le droit au silence et qui reste un droit de défense peu connu des citoyens et qui aurait peut-être évité à Bluetouff d'être condamné par la justice. Le droit au silence c'est la possibilité de garder le silence et d'être informé de ce droit dans le cadre d'une garde à vue. Il peut être utile de rappeler ce qu'est précisément une garde à vue telle qu'est est définie à l'article 62-3 du Code de procédure pénale : « *La garde à vue est une mesure de contrainte prise au cours de l'enquête par laquelle une personne soupçonnée d'avoir commis ou tenté de commettre un crime ou un délit puni d'emprisonnement est maintenue à la disposition des enquêteurs.* »

La Convention européenne des droits de l'homme considère depuis longtemps que « *le droit de se taire lors d'un interrogatoire de police et le droit de ne pas contribuer à sa propre incrimination* » sont des normes internationales, au cœur d'un procès équitable (aff. Murray/ Royaume-Uni, 1996). Mais en France, la culture de l'aveu est bien ancrée dans notre système judiciaire. Or, depuis la Loi n° 2011-392 du 14 avril 2011, les policiers sont désormais dans l'obligation d'informer un suspect qu'il n'est pas tenu de répondre à leurs questions. Le Conseil Constitutionnel, dans sa décision du 30 juillet 2010, avait déjà jugé que l'absence de notification du droit de se taire était contraire à la Constitution. Mais il a fallu attendre la condamnation de la France par la CEDH (Cour Européenne des Droits de l'Homme) dans l'arrêt *Brusco c. France du 14 octobre 2010, n°1466/07*, pour que s'engage une véritable réforme du régime de la garde à vue pour le rendre plus

respectueux des droits de la défense. La France s'est donc pliée aux règles européennes et la Loi n° 2011-392 du 14 avril 2011 relative à la garde à vue a modifié le Code de procédure pénale. Le nouvel article 63-1 du Code de procédure pénale mentionne bien que la personne gardée à vue a le droit *« de faire des déclarations, de répondre aux questions qui lui sont posées **ou de se taire** »*.

Au terme de sa garde à vue, la personne concernée est soit remise en liberté, soit déférée, c'est-à-dire présentée à un magistrat qui décidera des suites à donner aux poursuites. Dans le cas où elle n'est pas remise en liberté, la personne gardée à vue peut être retenue par les services de police, avant d'être présentée, suivant sa situation, au procureur de la République, au juge d'instruction ou au juge des libertés et de la détention. Cette rétention supplémentaire, dont la durée maximale est de 20 heures, n'est qu'une simple attente et il est impossible de l'utiliser pour mener un nouvel interrogatoire. Précisons également et pour finir que l'article 116 du code de procédure pénale prévoit que le juge d'instruction, lors de la première comparution devant lui d'une personne qu'il envisage de mettre en examen, doit lui signifier « *qu'elle a le choix soit de se taire, soit de faire des déclarations, soit d'être interrogée* ».

Sans aveux, une condamnation était-elle possible ?

Dans l'affaire Bluetouff, il est évident que ce sont les déclarations d'Olivier Laurelli concernant la fameuse mire de login repérée tout en haut de l'arborescence qui ont entrainé sa condamnation. Sans ces aveux, quels sont les éléments qui auraient permis d'établir que Bluetouff avaient connaissance du caractère privé de ces documents ? Dans cette affaire, il y a pour les enquêteurs de la DCRI quatre sources d'information exploitables :

1. Les journaux d'évènements (logs) du serveur VPN situé au Panama
2. Les logs des fournisseurs d'accès Internet utilisés par Bluetouff (à Orléans et dans le Val de marne)
3. Les logs dans l'infrastructure d'hébergement du serveur de l'Anses (Firewall, reverse proxy et serveur Web Extranet)
4. L'historique de navigation et plus généralement toute information disponible sur le ou les postes clients utilisés par Bluetouff (historique, cache navigateur, fichiers résiduels,…)

Analysons, point par point, ces différentes sources d'information.

Source no1 : le serveur VPN

L'objectif du déploiement du service VPN de Bluetouff étant d'assurer l'anonymat, il est fort probable qu'il n'y ait aucune trace exploitable dans le serveur Panaméen en question. Pour exploiter cette source d'information dans le cadre d'une perquisition, c'est l'article 57-1 du code procédure pénale qu'il convient d'appliquer.

« *Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.*
S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur. »

La seule convention internationale existante en la matière est la convention sur la cybercriminalité de Budapest du 23 novembre 2001 (Traité international No 185). Dans le cadre de la perquisition effectuée par la DCRI en novembre 2012, cette convention n'aurait pas pu s'appliquer puisque le Panama ne l'a ratifié que le 3 mars 2014 et qu'elle n'est entrée en vigueur avec ce pays qu'à compter du 1er juillet 2014.

Précisons que si l'enquête avait lieu aujourd'hui, les choses seraient bien différentes, puisqu'au-delà de l'application de la convention de Budapest (articles 25 et 32-b en particulier), la LOI n° 2014-1353 du 13 novembre 2014 relative à la lutte contre le terrorisme (Chapitre V – article 13) a modifié l'article 57-1 du code procédure pénale en renforçant les moyens d'investigation des services de police judiciaire .

Source no2 : Les logs des FAI
Et bien pas grand-chose aussi à exploiter ici par la DCRI car tout est chiffré entre le poste client et le serveur VPN. Les seules choses que peut voir un FAI sont les métadonnées des connexions (adresses IP sources et destinations, heure de connexion, volume des données échangées,…) mais en aucun cas le contenu des requêtes et donc la preuve que l'URL de la page de connexion a bien été sollicitée. Bien sûr, si l'internaute Bluetouff était déjà sous surveillance et soupçonné de terrorisme, il y aurait la possibilité (technique et juridique) pour la DCRI de déposer un mouchard d'interception sur son poste client (via un 0-day exploit dans flash player par exemple, technique très à la mode en cette année 2015…) afin d'analyser intégralement tous les flux échangés avec son ordinateur quelque soient les solutions ou techniques cryptographiques mises en œuvre (https, TOR, I2P, Freenet,

SSH, VPN IPsec ou SSL).

Source no3 : L'infrastructure d'hébergement du serveur de l'Anses

Beaucoup plus intéressant pour la DCRI car, que l'accès au serveur Web se fasse via http ou https (c'est le serveur Web de l'Anses qui décide et non pas le serveur VPN de bluetouff), les requêtes effectuées apparaissent en clair dans les journaux de logs du serveur Extranet et également dans les logs d'un éventuel reverse proxy déployé en amont. Mais quel est la valeur juridique d'un fichier de logs ? La preuve d'un fait juridique pouvant se faire par tout moyen, il est par conséquent possible d'utiliser un fichier de logs à titre de preuve dans le cadre d'une procédure pénale. Toutefois, sa recevabilité à titre probatoire est subordonnée à sa fiabilité. Ce critère dépend d'une part, des conditions dans lesquelles le fichier a été collecté puis conservé et d'autre part, de la qualité de la partie qui a réalisé ces opérations. Ainsi, la force probante d'un fichier de logs est maximale si son authenticité et son intégrité peuvent être tracées et garanties de la collecte de l'information recherchée jusqu'à sa fourniture aux enquêteurs judiciaires. Dans le cas de l'affaire Bluetouff, il est fortement vraisemblable que ce fichier de logs soit géré directement par l'Anses et que les administrateurs de l'agence aient la possibilité de l'altérer en toute discrétion. On peut par exemple imaginer d'y ajouter une ligne d'accès à la fenêtre d'authentification du serveur en provenance de l'adresse IP du serveur VPN pour incriminer Olivier Laurelli. Dans ces conditions, on peut difficilement imaginer que ce fichier logs soit recevable à titre de preuve. Il est important de noter que, même si un fichier de logs est recevable à titre probatoire, il reste néanmoins soumis à l'appréciation du juge qui peut décider de l'écarter des discussions.

Source no4 : Les informations sur le poste client de Bluetouff

Dernière source d'information intéressante à exploiter par les enquêteurs de la DCRI : le ou les ordinateurs dont s'est servi Olivier Laurelli pour accéder au serveur de l'Anses via son VPN. C'est d'ailleurs pour pouvoir exploiter cette source qu'il est placé en garde à vue pendant 30 heures, que son domicile à Orléans (Loiret) est perquisitionné et que son matériel informatique est saisi. Rappelons que la garde à vue (article 62-2 du code de procédure pénale) doit constituer l'unique moyen de parvenir à certains objectifs comme empêcher que la personne ne modifie des preuves ou des indices matériels. N'ayant pas eu accès aux pièces du dossier, il est impossible de se prononcer sur les éléments récupérés dans le matériel saisi par les enquêteurs. Une chose est sûre cependant, c'est que la solution VPN utilisée dans l'affaire Bluetouff (solution totalement différente d'un VPN entreprise utilisé pour le télé-travail par exemple) permet d'assurer l'anonymat. En d'autre terme, cela rend impossible à un Webmaster d'identifier l'origine réelle d'une requête effectuée sur son serveur Web. Mais si un enquêteur dispose physiquement du poste de l'utilisateur du service VPN, il peut alors retrouver un ensemble de traces informatiques comme par exemple la requête à la page d'authentification du serveur de l'Anses avec la date et l'heure exacte de l'opération. Il va sans dire que si ces éléments coïncident parfaitement avec le

journal de logs fourni par l'Anses et indiquent qu'une requête sur la page d'authentification a bien été effectuée, les aveux de Bluetouff ne semblent plus nécessaires pour démontrer à la Cour qu'il avait bien conscience de son maintien irrégulier dans le système. On peut également imaginer que Bluetouff n'est pas le premier venu et qu'il a pris quelques précautions au niveau de son poste client. Quoique la première des précautions qu'il me viendrait à l'esprit si je souhaitais naviguer de façon réellement anonyme via un VPN serait sans doute de ne pas m'appuyer sur le serveur VPN de ma propre entreprise fût-elle immatriculée au Panama ou ailleurs dans le monde. Cela dit, si Bluetouff a eu par exemple la bonne idée d'utiliser Tails ou de naviguer dans une machine virtuelle chiffrée puis de supprimer cette VM par une opération de « crypto shredding », il y a fort à parier qu'aucune information pertinente n'a pu être récupérée par la DCRI.

Conclusion

Pour gagner ce procès, il aurait fallu qu'Olivier Laurelli garde le silence lors de ses auditions mais qu'il soit également en mesure de faire disparaître toute trace de navigation sur les ordinateurs utilisés les 27 et 28 août 2012. Dès lors, comme il n'y pas eu d'accès frauduleux (ce qui est acté par tous y compris par l'Anses) et qu'il n'y a plus de moyen de prouver le maintien frauduleux, la Cour d'appel de Paris n'aurait pu que confirmer le jugement du TGI de créteil :
« En tout état de cause, Monsieur Olivier L. a pu légitimement penser que ces documents étaient librement téléchargeables puisque non protégés par un quelconque système. Il n'y a pas eu de sa part une volonté d'appropriation frauduleuse de ces fichiers informatiques et donc il n'y a pas d'élément intentionnel de l'infraction. »

Autres ressources :

- Bluetouff condamné pour maintien frauduleux et vol de fichiers
- 3000€ d'amende et un casier judiciaire pour une requête Google
- Affaire Bluetouff : la Cour de cassation consacre le vol de fichiers informatiques
- Notre pourvoi en cassation est rejeté

- Introduction
- Scénario double échange rapide
- Scénario double échange persistant
- Scénario simple échange (rapide ou persistant)
- Détection et remédiation

Introduction

Vous connaissiez sans doute l'attaque Man in the middle (MITM) qui consiste à intercepter des données sur un flux de communication. Vous connaissiez peut-être également, l'attaque Man in the browser (MITB) qui permet de compromettre les flux (http mais également https) via un code malveillant installé sur le poste client et bien voici maintenant l'attaque Man in the Cloud (MITC) qui permet de compromettre vos données dans le Cloud.

Man in the Cloud, c'est le nom donné à cette attaque par Imperva, la société de sécurité israélienne à l'origine de cette découverte. L'attaque MITC vise exclusivement les applications de stockage en ligne. L'étude d'Imperva porte en particulier sur Box, Dropbox, Google Drive et OneDrive et démontre la possibilité de compromettre intégralement les données hébergées dans le Cloud avec en prime la possibilité d'infecter le poste client et d'exfiltrer des données via le service de synchronisation.

Dans ce type d'application, afin d'éviter que l'utilisateur ne soit obligé de se ré-authentifier à chaque requête, un jeton de synchronisation est créé puis stocké sur le poste client dans le registre (pour Google Drive), dans un fichier (Dropbox) ou dans le gestionnaire d'identités de Windows (pour OneDrive et Box). Deux mécanismes d'authentification différents sont utilisés sur les services testés par Imperva. Alors que Box, Drive et OneDrive s'appuient sur le standard OAuth 2.0, Dropbox utilise un système d'authentification propriétaire.

SYNCHRONIZATION APPLICATION	ONEDRIVE	BOX	GOOGLE DRIVE	DROPBOX
Token Type	OAuth Refresh Token	OAuth Refresh Token	OAuth Refresh Token	Proprietary
Location	Windows Credential Manager	Windows Credential Manager	Encrypted in Registry	Encrypted SQLite file

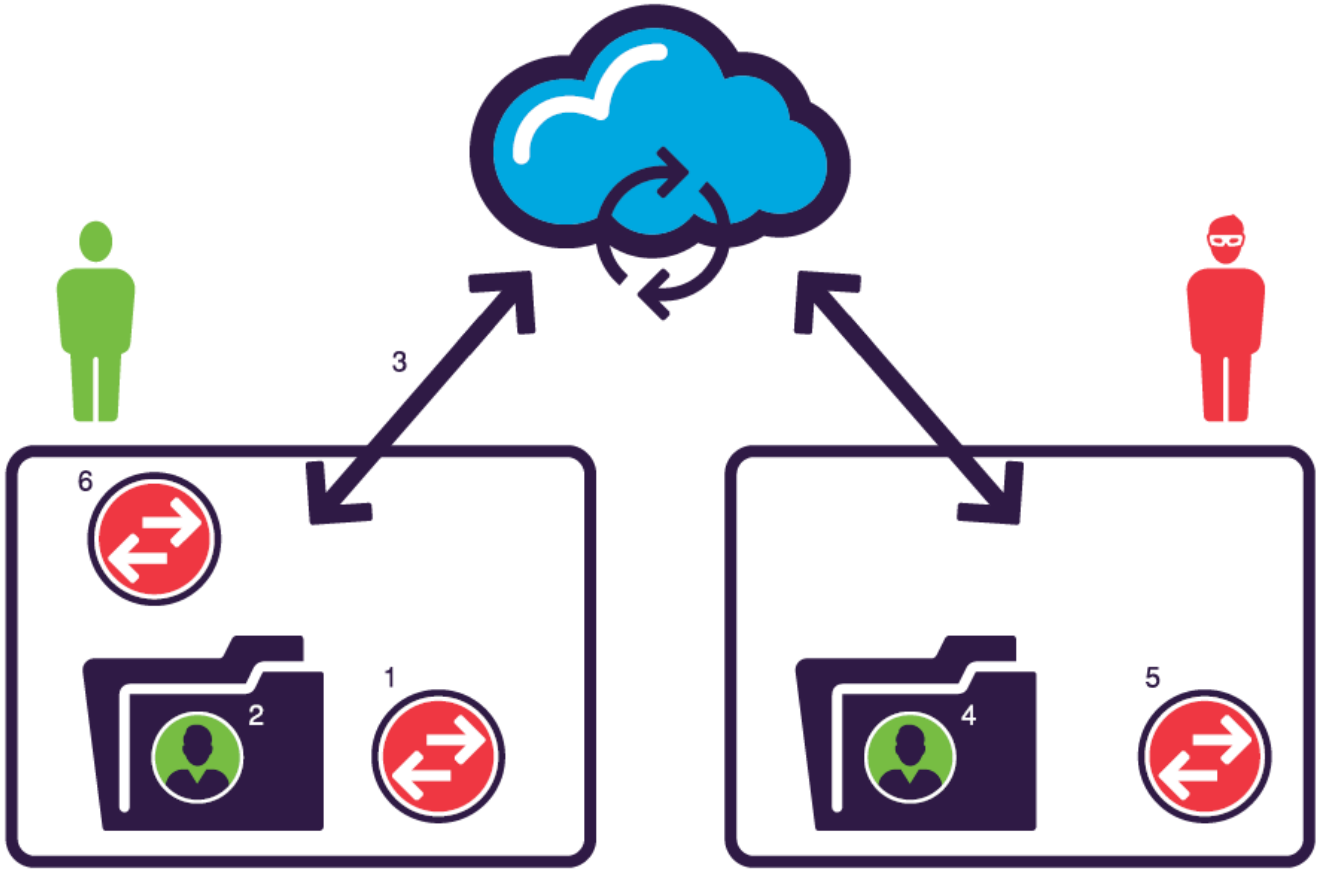
L'utilisation du jeton est très simple. Une fois installé sur le poste client, c'est le seul élément demandé par le service Cloud pour authentifier l'utilisateur et lui donner accès aux données hébergées. Les chercheurs d'Imperva ont remarqué que le jeton de synchronisation n'était pas lié à la machine ni à la session utilisateur en cours. Dans ces conditions, si un même jeton de synchronisation peut être utilisé sur des ordinateurs différents, il suffit de voler le jeton pour accéder au compte de l'utilisateur sans avoir à connaitre son identifiant ou son mot de passe.

Pour démontrer la vulnérabilité des services Cloud et matérialiser l'attaque, Imperva a développé l'outil Switcher. Un attaquant s'authentifie sur le service Cloud et génère un jeton. Switcher prend ce jeton et le stocke dans l'endroit approprié (selon le tableau ci-dessus) sur le poste Client de la victime. Switcher copie également le jeton original (celui de la victime) dans le répertoire de synchronisation. Le hacker peut maintenant récupérer le jeton de l'utilisateur et s'emparer de toutes ses données hébergées dans le Cloud. Une fois l'opération accomplie, Switcher remet en place le jeton original et donne à l'utilisateur l'impression que tout va bien dans le meilleur des mondes…

Dans son rapport, Imperva détaille trois scénarii possibles pour effectuer l'attaque : double échange rapide, double échange permanent et simple échange (rapide ou permanent).

Scénario double échange rapide

Cette attaque assez simple permet à l'attaquant de récupérer le jeton de synchronisation de la victime. L'attaquant est alors en mesure d'accéder aux fichiers qui sont synchronisés par la victime et peut infecter ces fichiers avec un code malveillant. L'attaque est décrite dans la figure suivante :



1. L’attaquant trompe l’utilisateur par ingénierie sociale (malware dans un email par exemple) ou exploite une faille dans le navigateur ou un de ses plugins (drive-by-download) pour exécuter Switcher sur le poste de la victime. Switcher installe le jeton de synchronisation de l’attaquant dans le système.
2. Switcher copie le jeton de synchronisation original dans le dossier de synchronisation
3. L’application synchronise le dossier avec le compte de l’attaquant.
4. L’attaquant a alors en sa possession le jeton de synchronisation de la victime.
5. En réutilisant Switcher sur son poste, l’attaquant installe le jeton volé et accède à toutes les données de la victime stockées dans le Cloud.
6. Switcher est utilisé une seconde fois sur le poste de la victime (double échange) afin de rétablir le jeton de synchronisation d’origine de la victime afin qu’il ne se doute de rien.

C’est la forme « plus propre » de l’attaque. En effet, une fois l’attaque terminée, l’état du dossier de synchronisation de la victime est la même qu’avant l’attaque. Le programme Switcher s’auto détruit et ne laisse aucune trace.

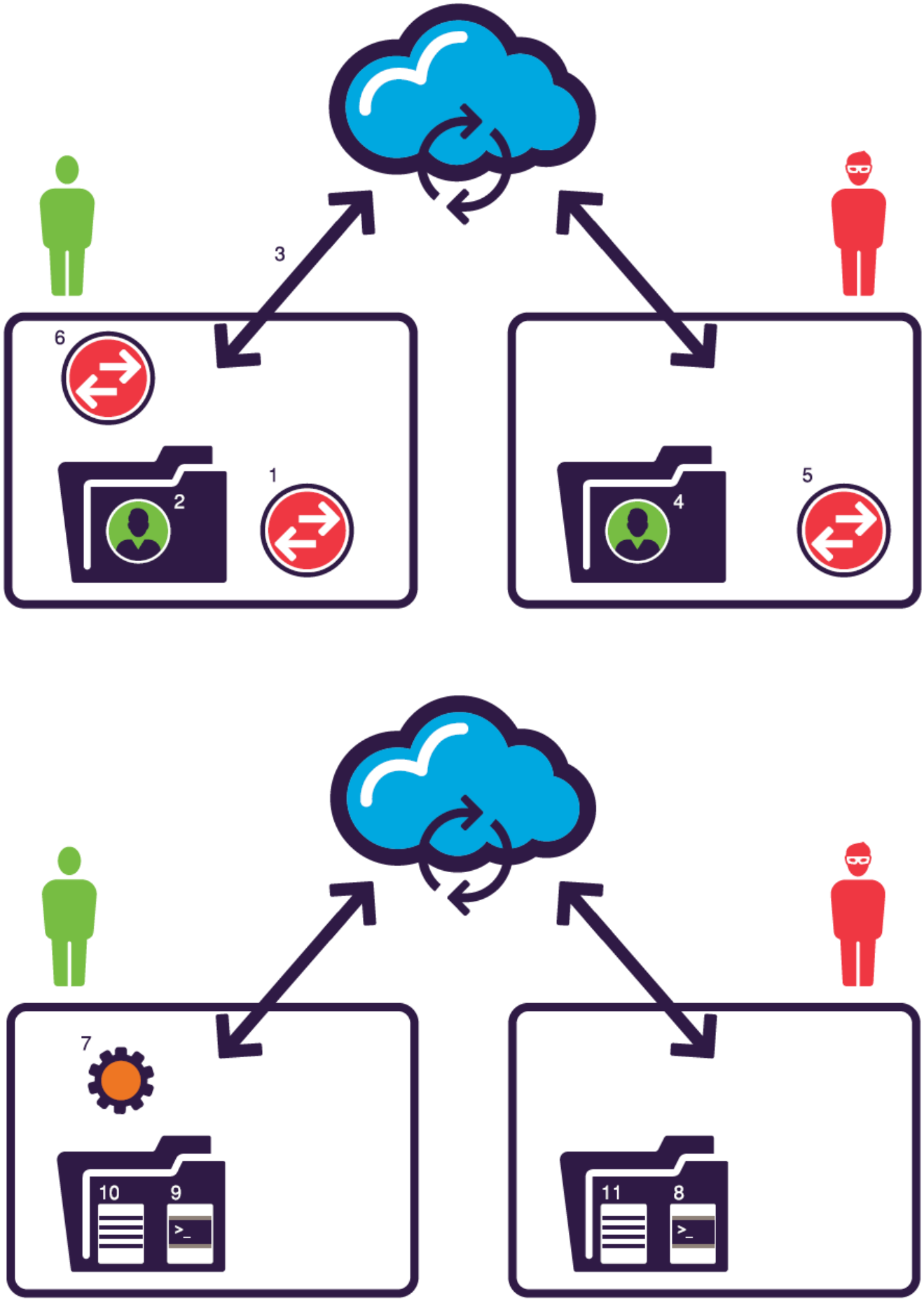
L’attaque en double échange est potentiellement très dangereuse car les services de synchronisation dans le Cloud ne restreignent pas l’accès de plusieurs appareils à partir de plusieurs endroits sur un même compte utilisateur. Ainsi, il est possible pour un attaquant de maintenir une activité de synchronisation fraduleuse avec le

compte de la victime à partir de n’importe où, à tout moment et ceci sans qu’aucune notification ne soit envoyée au propriétaire du compte.

En plus d’avoir accès aux données de l’utilisateur, l’attaquant peut manipuler les fichiers dans le dossier de synchronisation sur sa machine de sorte que les modifications se propagent à la machine de la victime. Par exemple, un attaquant peut insérer du code malveillant dans les documents (exemple un macro dans un document Office ou un script dans un document PDF) qui s’exécutera dès que la victime ouvrira un fichier infecté sur son poste. Cerise sur le gâteau, les résultats de l’exécution peuvent être envoyés dans le dossier de synchronisation puis récupérés par l’attaquant. Après l’opération, l’attaquant peut même supprimer les fichiers résultats dans le dossier de synchronisation et restaurer les fichiers originaux de la victime afin d’éliminer toute trace de l’attaque. Il est possible d’imaginer d’autres scénarios d’attaque comme par exemple une nouvelle façon de pratiquer le « Ransomware ». Dans ce schéma, l’attaquant crypte tous les fichiers de la victime. Une fois les fichiers synchronisés avec tous ses autres appareils, la victime se retrouve dans l’impossibilité d’avoir accès à ses propres documents tant qu’il n’accepte de payer une rançon au hacker.

Scénario double échange persistant

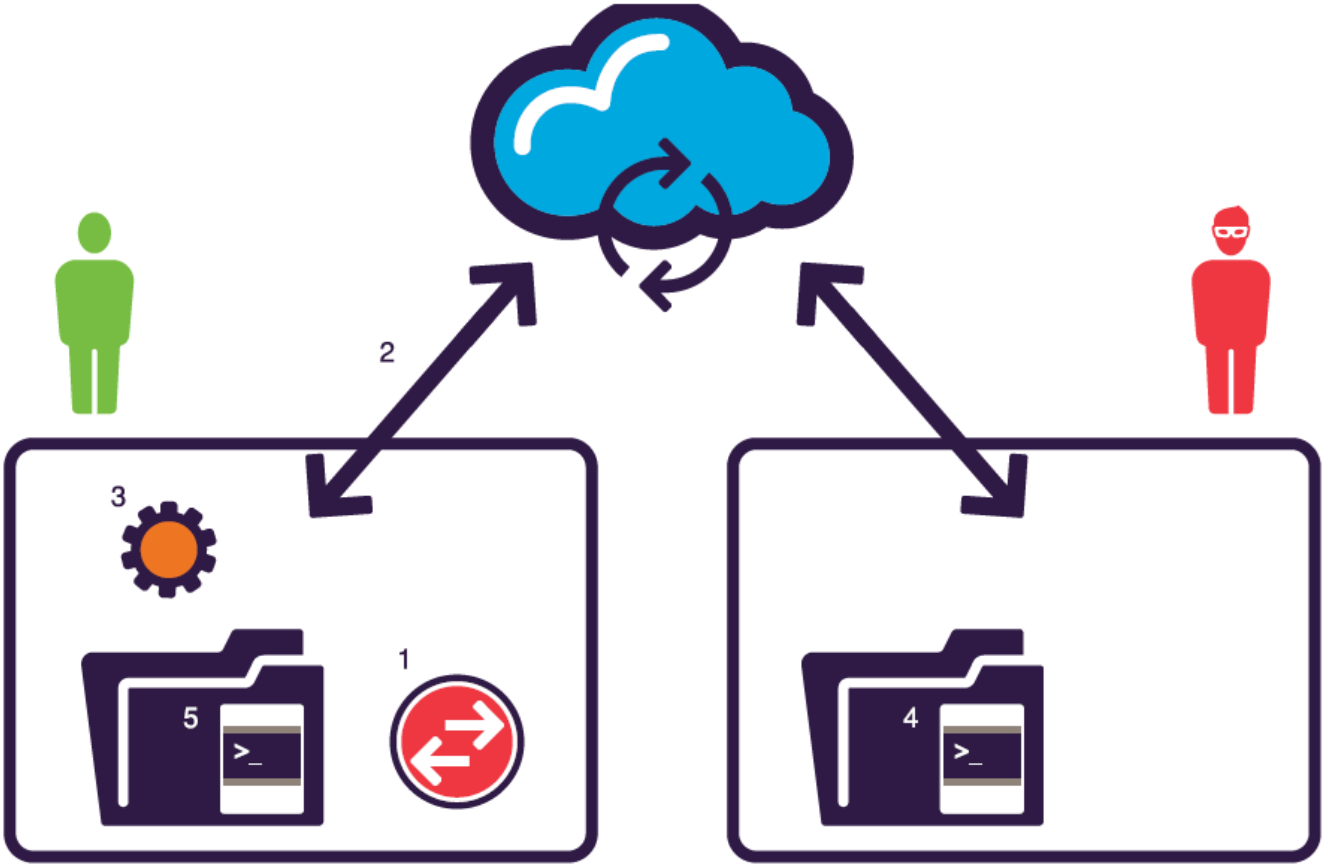
Cette attaque est semblable à la précédente, à l’exception que l’attaquant souhaite maintenir l’accès à distance à la victime. Cet accès permet à l’attaquant d’interagir avec la machine de la victime de temps à autre, exécuter du code arbitraire, et de recueillir la sortie de ce code. L’attaque est décrite en deux phases dans les deux figures suivantes :


3
6
2
1
4
5
7
10
9
11
8

1. L’attaquant trompe l’utilisateur par ingénierie sociale (malware dans un email par exemple) ou exploite une faille dans le navigateur ou un de ses plugins (drive-by-download) pour exécuter Switcher sur le poste de la victime. Switcher installe le jeton de synchronisation de l’attaquant dans le système.
2. Switcher copie le jeton de synchronisation original dans le dossier de synchronisation
3. L’application synchronise le dossier avec le compte de l’attaquant.
4. L’attaquant a alors en sa possession le jeton de synchronisation de la victime.
5. En réutilisant Switcher sur son poste, l’attaquant installe le jeton volé et accède à toutes les données de la victime stockées dans le Cloud.
6. Switcher est utilisé une seconde fois sur le poste de la victime(double échange) afin de rétablir le jeton de synchronisation d’origine de la victime afin qu’il ne se doute de rien.
7. Après le second échange, l’attaquant met en place un outil d’accès à distance de type RAT (Remote Access Tool) paramétré pour attendre l’apparition d’un fichier à un endroit particulier dans le dossier de synchronisation afin de l’exécuter.
8. Un code malveillant est mis dans l’emplacement spécifique dans le dossier de synchronisation de l’ordinateur de l’attaquant
9. Le dossier est synchronisé avec la machine de la victime. Le RAT l’identifie et l’exécute.
10. Le résultat de l’exécution est écrit dans le dossier de synchronisation sur la machine de la victime puis récupéré par l’attaquant via une synchronisation.
11. Une fois les données récupérées, l’attaquant peut alors supprimer le résultat et le code de l’attaque.

Scénario simple échange (rapide ou persistant)

Dans ce type d’attaque, les données de la victime sont synchronisés avec un compte contrôle par l’attaquant.



- L’attaquant lance l’exécution du programme Switcher sur le poste de la victime (typiquement via une opération d’ingénierie sociale ou une attaque de type drive-by-download). Switcher installe le jeton de synchronisation de l’attaquant dans le système.
- Le dossier de synchronisation de la victime est synchronisé avec celui de l’attaquant.
- L’attaque est désormais terminée et l’attaquant a maintenant accès aux données de l’utilisateur. Dans une attaque persistante, l’attaquant met en plus, sur le poste de la victime, un outil d’accès à distance de type RAT (Remote Access Tool) paramétré pour attendre l’apparition d’un fichier à un endroit particulier dans le dossier de synchronisation afin de l’exécuter.
- Un code malveillant est mis dans l’emplacement spécifique dans le dossier de synchronisation de l’ordinateur de l’attaquant
- Le dossier est synchronisé avec la machine de la victime. Le RAT l’identifie et l’exécute.

L’avantage de cette technique est que même si le service de synchronisation met en place un mécanisme de contrôle des accès suspicieux (pour détecter par exemple des accès simultanés à partir de deux endroits différents) la notification de l’anomalie sera envoyée à l’attaquant plutôt qu’à la victime puisque c’est le jeton de synchronisation de l’attaquant qui est utilisé. L’inconvénient est que, comme le jeton installé n’est pas celui de la victime, la synchronisation ne va pas s’effectuer correctement sur les autres dispositifs de l’utilisateur. Pour minimiser

les soupçons, l'attaquant peut périodiquement revenir réinstaller le jeton original de la victime pour permettre une synchronisation avec le compte d'origine.

Détection et remédiation de l'attaque

L'attaque MITC est difficilement détectable car elle s'appuie sur du code déjà installé (l'agent de synchronisation) et sur des canaux de communication légitimes car nécessaires au bon fonctionnement du service. Pour la détection, Imperva propose 2 approches possibles : La détection de la compromission du compte de synchronisation ou plus important encore la détection d'un usage abusif des données internes de l'entreprise. Imperva pense en effet que les attaquants seront probablement plus intéressés par d'autres données dans l'entreprise que celles situées dans les répertoires de synchronisation des postes clients.

Pour la détection de la compromission du compte de synchronisation, Imperva précise que la tâche risque d'être difficile avec les techniques traditionnelles (détection de code malveillant ou analyse des flux de communication vers le C&C). En conséquence, Imperva recommande d'utiliser des solutions de CASB (Cloud Access Security Broker) afin de surveiller l'utilisation des services de Cloud par les utilisateurs. Toujours, selon Imperva, les solutions de CASB sont tout à fait capables de détecter en temps réel ce type d'attaque. D'autres solutions de CASB déployées en mode SecaaS (dans le Cloud) peuvent également stopper l'attaque en bloquant l'accès aux périphériques non officiellement reconnus par l'entreprise.

Pour la seconde approche, Imperva recommande aux entreprise de déployer des solutions de type DAM (Database Activity Monitoring) ou FAM (File Activity Monitoring) pour détecter tout trafic suspicieux.

Les préconisations d'Imperva ne sont pas vraiment surprenantes puisque la société israélienne commercialise des produits CASB avec Imperva Skyfence Cloud Gateway , DAM avec Securephere Database Security et FAM avec File Activity Monitor. C'est de bonne guerre, les vendeurs de solutions de sécurité cherchent des vulnérabilités et des POC (proof of concept) dans le but d'expliquer en quoi leur offre répond à de véritables problématiques de sécurité. Mais n'y aurait-il pas d'autres solutions plus efficaces et moins chères ? Bien sûr que oui et commençons par traiter l'origine du problème. Et si les fournisseurs de service Cloud en profitaient pour mieux sécuriser leur service ? En mettant tout simplement en œuvre un jeton de synchronisation utilisable sur un seul et même device. C'est facile à faire, radical contre l'attaque et ne coûte pas un Kopeck à l'utilisateur. Une autre solution, tout à fait complémentaire, consisterait à chiffrer systématiquement les données que l'on envoi dans le Cloud. Outre le fait que l'attaquant ne pourra plus les lire, ni y insérer de malware, cela protégera également vos données contre un éventuel administrateur malveillant opérant chez le prestataire. La difficulté étant de

trouver une solution de chiffrement fiable, ergonomique et compatible avec les différents OS des dispositifs sur lequel on souhaite partager les informations. Enfin et contrairement à ce qu'affirme Imperva, l'attaque peut être détectée au niveau de poste client. Il suffit pour cela de mettre en œuvre une solution de contrôle d'intégrité. Le lecteur intéressé par cette approche pourra consulter l'article Detecting Man-in-the-Cloud (MitC) Attacks with Adaptive Threat Protection sur le site de Tripwire (éditeur de solutions de contrôle d'intégrité…).

Il est vrai cependant que dans la plupart des cas, l'attaque MITC sera assez difficile à détecter et même si l'utilisateur s'en aperçoit, il lui sera parfois difficile de la stopper. En effet, pour cela il faut impérativement révoquer le jeton de l'attaquant et la tâche n'est pas toujours facile selon le service de Cloud utilisé. La révocation du jeton est particulièrement simple avec Google Drive car il suffit d'effectuer un changement de mot de passe. Cette opération entraine alors la révocation de tous les jetons associés au compte utilisateur et impose pour chaque appareil une nouvelle authentification avec l'identifiant et le mot de passe. D'autre part, comme le changement de mot de passe entraine une révocation immédiate des jetons, toute tentative d'accès au service avec un jeton révoqué sera systématiquement refusée. La situation est assez similaire avec Microsoft Onedrive. La seule différence est toute session déjà en cours et initialisée avec un jeton avant révocation reste active et valide. Il faut donc supprimer manuellement ces périphériques associés dans l'onglet d'administration du compte OneDrive. Avec Box, il faut également changer le mot de passe mais utiliser en plus l'option « révoquer tous les jetons » pour stopper l'attaque. Pour finir, c'est avec Dropbox que la tâche est la plus ardue car un simple changement de mot de passe ne modifie pas le jeton (valeur de la variable host id présente dans le fichier SQLite config.dbx). Pour les détails techniques, on se référera au document d'Imperva. Dans ce dernier cas, il sera sans doute plus simple de supprimer le compte Dropbox existant et d'en créer un nouveau. Bienvenu dans le monde merveilleux du cloud…

[Introduction] [Résultats] [Analyse] [Conclusion]

Introduction

Pour créer et administrer des machines virtuelles dans un IaaS public, les fournisseurs mettent à disposition de leurs clients des interfaces Web accessibles via le protocole sécurisé https. Ces interfaces sont des éléments particulièrement sensibles car elles sont accessibles publiquement sur Internet et leur compromission permettrait à un attaquant de prendre le contrôle total de nos machines dans le Cloud.

Le problème est que le protocole https utilise des fonctions cryptographiques (SSL/TLS), historiquement développées par Netscape au début des années 90 et que ces fonctions cryptographiques ont subi ces dernières années de nombreuses attaques : attaque sur la renegociation, attaque sur RC4, collision MD5, BEAST, CRIME, POODLE, etc… Il y a également d'autres problèmes non pas liés à la cryptographie SSL elle-même mais plutôt à de mauvaises implémentations logicielles comme par exemple le bug dans OpenSSL (Heartbleed) mais aussi celui dans la librairie open source utilisée par Apple (goto fail). Et les problèmes ne sont pas terminés comme en témoigne l'annonce de 8 nouvelles vulnérabilités dans OpenSSL le 8 janvier 2015 dont l'une d'elles permet de réaliser l'attaque SSL/TLS du moment : FREAK (Factoring attack on RSA-Export Keys).

Nous avons donc décidé de vérifier si les interfaces d'authentification de 4 fournisseurs IaaS français (OVH, Numergy, Cloudwatt et Outscale) étaient correctement paramétrées d'un point de sécurité. En d'autres termes, les fournisseurs nationaux respectent-ils les bonnes pratiques de sécurité concernant les flux chiffrés SSL/TLS.

Nos tests ont porté exclusivement sur la gestion des flux chiffrés. Il ne s'agit en aucun cas d'un audit de sécurité, ni d'un test d'intrusion mais tout simplement d'une vérification de la configuration SSL/TLS. Les vulnérabilités spécifiques aux applications Web (XSS, CSRF, SQL injection, etc…) n'entrent pas dans le périmètre de notre étude.

Pour ce faire, nous avons utilisé sur www.ssllabs.com, un outil gratuit et disponible publiquement sur Internet proposé par Qualys. Il a été développé par Ivan Ristic, le concepteur du pare-feu applicatif mod_security.

Son utilisation est très simple. On soumet le nom du serveur à tester à ssllabs et le service effectue une vérification approfondie de la configuration SSL/TLS de la cible et délivre une note globale de sécurité sous forme d'une lettre de A à F.

Il faut ensuite interpréter les résultats de la façon suivante :

Excellente configuration SSL/TLS
Aucune vulnérabilité connue n'est exploitable

Mauvaise configuration SSL/TLS
Une ou plusieurs vulnérabilités peuvent compromettre la session

Très mauvaise configuration SSL/TLS
Une ou plusieurs vulnérabilités facile à exploiter peuvent compromettre la session

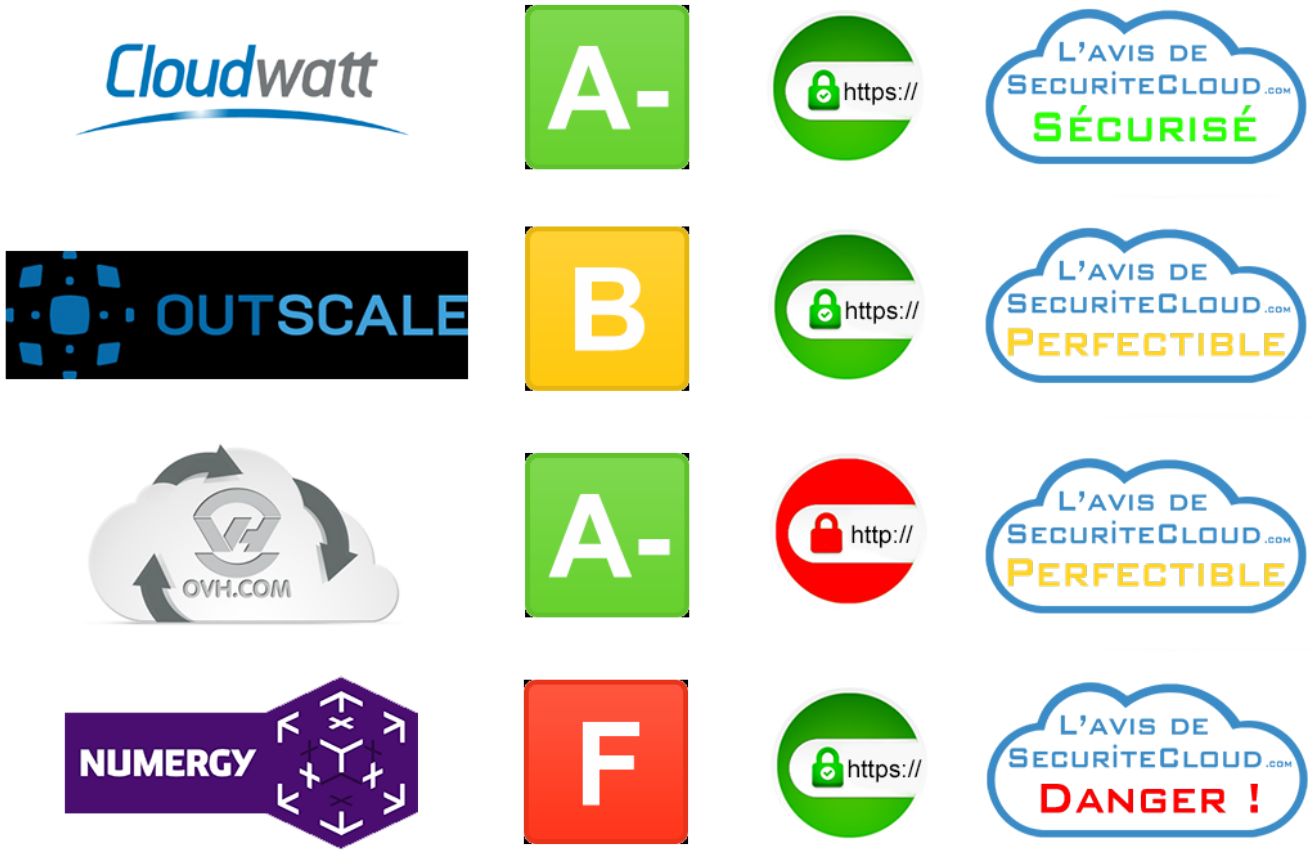
Compte tenu de la criticité de ces interfaces Web dans l'infrastructure Cloud, il va sans dire que pour un fournisseur de IaaS public, on ne s'attend pas à autre chose que la lettre A. Une note A+ serait bien sûr idéale mais un A- sera tout à fait acceptable. Les lettres B, C, D et E indiquent quelques lacunes en matière de sécurité sur lesquelles le fournisseur doit agir assez rapidement. La lettre F traduisant quant à elle de graves lacunes de sécurité sur lesquelles le fournisseur n'a apparemment réalisé aucune évaluation de sécurité et doit maintenant intervenir dans les plus brefs délais. Précisons enfin qu'il n'y a aucun coût financier pour

passer de la lettre F à la lettre A (Pas d'obligation d'acquérir un certificat SSL EV ou un boitier HSM). Il faut simplement effectuer quelques modifications dans les paramètres SSL/TLS des serveurs et l'opération ne prend que quelques minutes.

Nous avons également regardé comment les clients arrivent sur la page d'authentification du service. Si le lien vers la page d'authentification s'effectue via le site Web du fournisseur lui-même accessible uniquement en https alors l'accès à l'interface d'administration est correctement sécurisée. Par contre si l'accès se fait via une page Web en http alors la connexion sera potentiellement vulnérable. Pourquoi ? Parce qu'un site Web accessible via le protocole http signifie qu'aucune authentification du serveur n'est réalisée par le navigateur. L'attaquant peut ainsi très facilement réaliser une attaque de type Man In The Middle (MITM) et substituer ainsi la page d'authentification originale par une page frauduleuse par une simple réécriture d'URL à la volée. Une telle attaque ne pose pas aucune difficulté et plusieurs outils existent pour la réaliser comme par exemple sslsnif et sslstrip de Moxie Marlinspike.

D'autre part, tout site Web accessible via http est beaucoup plus vulnérable aux opérations de phishing toujours en raison de l'absence d'authentification du serveur. En conclusion, même si son contenu n'est pas confidentiel (chiffrement des flux non nécessaire) l'intégralité du site Web du fournisseur doit être uniquement accessible via le protocole https.

Résultat des tests



Les copies d'écran du test ssllabs.com sont disponibles sur cette page.

Analyse des résultats

Cloudwatt propose un accès correctement sécurisé pour ses services. Toutes les erreurs classiques de paramétrage d'un serveur https ont été évitées. On regrettera cependant l'absence de certificat à validation étendue (Certificat SSL EV) permettant d'accroître la confiance dans le site. En effet avec un certificat SSL, identifiable par le cadenas en vert dans la barre d'adresse, l'utilisateur connaît immédiatement quelle société se trouve derrière le site par l'affichage de son nom et du pays dans lequel elle réside. D'autre part, la délivrance d'un certificat SSL EV par une autorité de certification fait l'objet de contrôles bien plus rigoureux sur l'organisme demandeur (existence juridique de 3 ans minimum, inscription au RCS, etc…) que pour un certificat SSL classique ou seule la possession du nom de domaine peut s'avérer suffisante.

4 recommandations pour améliorer la sécurité de Cloudwatt :

- Remplacer les certificats X509 standards par des certificats SSL EV
- Remplacer la signature sha1 des certificats par une signature sha2
- Activer le support du *Forward Secrecy* sur le serveur
- Ne pas se contenter de faire un http redirect vers https et forcer le protocole sécurisé avec HSTS (Strict Transport Security – RFC 6797)

Outscale n'utilise pas non plus de certificat SSL EV. D'autre part, la configuration laisse apparaître la disponibilité du protocole SSL v3 qui est obsolète et surtout extrêmement vulnérable depuis la découverte en octobre 2014 d'une vulnérabilité dénommée POODLE.

5 recommandations pour améliorer la sécurité de Outscale :

- Corriger immédiatement les problèmes de configuration SSL/TLS sur toutes les interfaces Web en particulier désactiver le protocole SSLv3
- Remplacer les certificats X509 standards par des certificats SSL EV
- Remplacer la signature sha1 des certificats par une signature sha2
- Activer le support du *Forward Secrecy* sur le serveur
- Ne pas se contenter de faire un http redirect vers https et forcer le protocole sécurisé avec HSTS (Strict Transport Security – RFC 6797)

OVH dispose d'une configuration SSL correcte et utilise de plus des certificats SSL EV. Dommage que le site www.ovh.com soit toujours accessible via http.

5 recommandations pour améliorer la sécurité du Cloud OVH :

- Mettre l'intégralité du site accessible uniquement via https
- Pour les accès en http sur la page d'accueil, faire une redirection (HTTP redirect) vers https

- Positionner le flag HSTS (RFC 6797) pour forcer le navigateur à utiliser exclusivement https
- Remplacer la signature sha1 des certificats par une signature sha2
- Activer le support du *Forward Secrecy* sur le serveur

Pour Numergy, tout commence bien avec l'apparition d'un certificat SSL EV sur la page d'accueil du site (www.numergy.com). On passe ensuite sur la page d'authentification (login.numergy.com) qui elle n'utilise pas de certificat EV. Les choses se compliquent ensuite puisque l'analyse détaillée de la configuration révèle de graves lacunes de sécurité.

Pour la page d'authentification du service (login.numergy.com – 87.255.157.62), on dénombre pas moins de 7 problèmes de sécurité dont 3 très graves :

- Utilisation d'algorithme asymétrique (DH) vulnérable pour l'échange des clés
- Support d'anciens algorithmes vulnérables et exploitables via l'attaque FREAK publiée le 3 mars 2015 et découverte par Antoine Delignat Lavaud chercheur à l'INRIA.
- Le protocole SSL v3 est activé et le site est vulnérable à l'attaque POODLE sans aucune contre-mesure permettant d'en limiter l'impact (TLS_FALLBACK_SCSV)

Devant une telle situation, nous avons souhaité voir ce qui se passait derrière la page d'authentification. Nous avons donc crée un compte utilisateur avec nos informations carte bancaire pour la facturation. Pour la petite histoire, on notera que la saisie des informations carte bancaire s'effectue sur un site de paiement de la société générale (paiement.socgenactif.com) qui n'est pas non plus un modèle de sécurité puisqu'il obtient la même note (F) dans le test ssllabs.

Après le paiement, le service nous indique que notre compte a été créé et que notre mot de passe nous sera envoyé par SMS. Le mot de passe arrive et surprise, il ne tient que sur 8 caractères (6 caractères alphabétiques, un caractère numérique et un seul caractère spécial). Nous essayons alors d'utiliser ce même mot de passe pour la création d'un compte chez le concurrent (Cloudwatt), pour voir ce que ça donne :

Tiens, il semblerait que les deux fournisseurs n'aient pas la même approche sur la robustesse des mots de passe. On se dit que tout ceci n'est pas bien grave et que Numergy va évidemment nous imposer dès la première connexion de changer ce mot de passe. Et bien pas du tout ! Le mot de passe envoyé par mail est utilisable en permanence sur la console d'administration du service IaaS. Nous avons essayé l'option « j'ai oublié mon mot de passe » et une fenêtre nous demande notre e-mail et nous renvoi un nouveau mot de passe par SMS. Ce mot de passe est toujours aussi faible avec 8 caractères (dont un numérique et un spécial) et toujours permanent. Ce choix technique n'est évidemment pas judicieux quand on sait que de nombreuses vulnérabilités (sous iOS et Androïd en particulier) permettent de récupérer les SMS des smartphones. On peut par exemple récupérer en quelques secondes l'intégralité des SMS dans un iPhone lorsque celui-ci est jailbreaké. D'autre part, sur de nombreux téléphones, tout SMS reçu s'affiche en clair sur l'écran même si le téléphone est verrouillé. Pour prendre le contrôle d'un compte administrateur sur Numergy, il suffit donc de saisir l'adresse email de la victime et d'avoir l'écran de son téléphone en visuel. Scénario, on ne peut plus simple à réaliser. Ensuite, on constate que le mot de passe a été créé par Numergy et une règle de base en sécurité est qu'il ne faut jamais conserver un mot de passe généré par un algorithme inconnu. D'autre part, ce mot de passe est potentiellement connu de l'opérateur Télécom puisqu'il est envoyé par SMS et éventuellement d'un autre fournisseur Cloud si l'administrateur a synchronisé son smartphone dans le nuage. Ca fait quand même beaucoup de monde qui peuvent potentiellement avoir accès à nos données dans le Cloud Numergy sans pour autant avoir besoin de faire appel aux services du GCHQ ou de la NSA…

Tant qu'à être connecté, nous avons également testé la gestion de session. Nous ouvrons donc une session dans un navigateur que nous laissons ensuite en totale inactivité pendant plus de 4 heures. Nous revenons ensuite sur le navigateur et nous constatons que la session d'administration est toujours active.

Nous vérifions maintenant les mécanismes anti « brute force ». On tente de se connecter avec notre identifiant valide en injectant une trentaine de mots de passe erronés. L'interface réagit à chaque fois immédiatement en nous indiquant l'échec d'authentification et en nous invitant à recommencer. Aucun délai entre les mires de login et aucun CAPTCHA ne viennent perturber notre test. Nous essayons maintenant de nous connecter pour voir si notre compte n'est pas verrouillé et là encore pas de problème, ça passe. Une fois connecté, aucun message d'alerte ne vient nous informer des tentatives infructueuses que vient de subir le compte.

Pour terminer cette très rapide évaluation de sécurité, nous avons lancé deux autres tests ssllabs :

Site d'administration des machines virtuelles
mon2.numergy.com – Adresse IP : 87.255.151.7

API Rest du service Numergy
api2.numergy.com – Adresse IP 87.255.151.6

6 recommandations pour améliorer la sécurité SSL/TLS chez Numergy :

- Corriger immédiatement les problèmes de configuration SSL/TLS sur toutes les interfaces Web du Cloud Numergy et en particulier celles accessibles publiquement via Internet (login.numergy.com, mon2.numergy.com)
- Même chose avec les API Rest du service (api2.numergy.com)
- Ne pas se contenter de faire un http redirect vers https et forcer le protocole sécurisé avec HSTS (Strict Transport Security – RFC 6797)
- Remplacer la signature sha1 des certificats par une signature sha2
- Activer le support du *Forward Secrecy* sur les serveurs
- Généraliser l'usage des certificats SSL EV sur l'ensemble des serveurs

+ 7 recommandations complémentaires pour Numergy :

- Ne pas générer de mot de passe permanent pour les clients
- Imposer au strict minimum 10 caractères avec minuscules, majuscules, chiffres et caractères spéciaux
- Ne jamais envoyer un mot de passe permanent par SMS
- Gérer un timeout d'inactivité sur la session
- Intégrer un mécanisme anti brute force et en cas d'attaque verrouiller le compte et informer le client
- Proposer une option d'authentification à deux facteurs (comme le font tous les leaders mondiaux du Cloud)
- Prendre en compte plus rapidement les alertes de sécurité en provenance des clients (suivi d'incident détaillé en fin d'article)

Conclusion

Premier constat et ce n'est pas pour nous une véritable surprise : La seule société à ne pas être certifiée ISO 27001, Cloudwatt, est celle qui obtient la meilleure note de sécurité. Rappelons encore une fois qu'une certification ISO 27001 ne garantit pas un niveau de sécurité. Elle ne garantit pas non plus que les solutions de sécurité ont été déployées conformément aux bonnes pratiques et à l'état de l'art. La norme ISO 27001 atteste simplement que le fournisseur a mis en œuvre un processus de gestion de la sécurité de son système d'information (SMSI) conforme à la politique de sécurité qu'il a lui-même défini. Elle ne certifie donc en aucun cas que les données du fournisseur ou celles de ses clients seront correctement sécurisées et notre étude en est une parfaite illustration.

Second constat, de nombreux clients font une confiance aveugle aux fournisseurs de services Cloud. Les labels de sécurité, les discours marketing et l'opacité des infrastructures de Cloud public rendant les audits indépendants impossibles sont d'autant de moyens pour convaincre les clients de la sécurité du service. Nous recommandons donc naturellement à tous les clients d'aller plus loin dans l'évaluation de la sécurité de leur fournisseur avant de leur confier leurs données.

Et pour finir, que faut-il penser de la sécurité des Clouds souverains ? En effet, Numergy est une société française créée en 2012 par SFR, Bull et l'état français dans le cadre du projet de Cloud souverain français (Andromède).
Pour beaucoup de fournisseurs et de médias français, la souveraineté se réduit trop souvent à deux choses. Une menace clairement identifiée : l'USA PATRIOT Act et une réponse imparable : la localisation des datacenters en France. Les fournisseurs français ont-ils bien intégré que le Patriot Act n'était pas la seule menace qui

pèse sur les entreprises françaises et qu'il fallait agir en conséquence pour démontrer leur capacité à contrer toutes les menaces potentielles dans le Cloud ?

Et si l'on en revient un instant au Patriot Act et plus généralement à la menace en provenance des USA, posons-nous les bonnes questions :

- Peut-on véritablement être souverain lorsque l'infrastructure de sécurité réseau s'appuie sur les technologies israélo-américaines de Cisco, F5, Fortinet et Checkpoint ? Qui pourrait imaginer un seul instant un pare-feu Airbus Defense & Space dans un GovCloud AWS ?
- Peut-on assurer la sécurité de nos données face à une puissance étrangère si les flux de communication chiffrés sont affectés par de multiples vulnérabilités ?
- Peut-on assurer la sécurité de nos données, si l'on envoie les mots de passe d'administration par SMS que la NSA peut intercepter facilement tant sur le réseau de l'opérateur que sur les terminaux mobiles ?

Note importante

Vendredi 13 mars 2015 à 20h30 : Ouverture Ticket d'incident Numergy
Plus de 3 jours avant la publication de cet article, nous avons ouvert un ticket incident (Priorité 1 : Very high) au support Numergy pour les informer des vulnérabilités sur leurs interfaces Web. Nous réactualiserons ci-dessous cet article dès que Numergy nous fera un retour.

Message dans le ticket d'incident :
En tant que nouvel utilisateur du Cloud Numergy (compte crée ce jour – 13/03/2015), je me suis permis de vérifier si vos interfaces Web étaient correctement paramétrées d'un point de vue sécurité.
A l'aide du service sslabs.com, j'ai testé :
login.numergy.com, mon2.numergy.com et api2.numergy.com.
Il apparait que ces 3 systèmes sont extrêmement mals configurés avec pour conséquence la possible compromission de toutes nos machines virtuelles dans le Cloud Numergy.
Je vous invite à remédier à ces problèmes dans les plus brefs délais et de me tenir au courant dès que cela sera fait.
Je vous remercie de votre compréhension.

Samedi 14 mars 2015 à 12h33 : 1ère réponse de Numergy
Bonjour,
Dans un premier temps nous vous remercions de votre vigilance .
Sachez que Numergy porte une attention particulière à la sécurité .
Tout nos systèmes sont régulièrement scanné pour en vérifier la sécurité .

Dans ce sens , votre remarque a été remontée a notre équipe de supervision et sécurité qui vous recontactera dans les plus brefs délais.
Cordialement,
L'Equipe Numergy

Mercredi 23 mars 2015 à 15h33 : 2eme message de Numergy
Monsieur, je vous remercie de votre retour.

Nous mettons tout en œuvre au quotidien pour assurer la sécurité de la plateforme et des environnements clients.
Certains des points remontés ont été jugés pertinents et les actions associées ont été menées.

Nous vous souhaitons une excellente journée.

Cordialement,
Service Support

Suite à la prise en compte de notre message au support Numergy, deux interfaces (mon2.numergy.com et api2.numergy.com) ont été corrigées le 18 mars et sont maintenant classées « A » par ssllabs. La troisième interface (login.numergy.com) a été corrigée le 23 mars et obtient également la même note pour la configuration SSL/TLS. Nous ne pouvons que féliciter le support Numergy qui a pris en compte notre alerte.
Si le comparatif avait lieu aujourd'hui, Numergy obtiendrait désormais la meilleure note avec la lettre A pour configuration SSL/TLS et https pour l'intégralité du site Web.