Campagnes de phishing automatiques

Denis Joiret
Inria Rocquencourt
Domaine de Voluceau
BP 105
78153 LE CHESNAY CEDEX

Résumé

Le phishing (ou hameçonnage en français) est l'une des principales techniques d'ingénierie sociale utilisée pour capter les identifiants. Afin de sensibiliser ses collaborateurs, Inria a décidé depuis plusieurs années de lancer régulièrement de fausses campagnes de phishing. Une campagne consiste à transmettre à un ensemble d'utilisateurs un mail contenant un lien vers un faux site sur lequel l'utilisateur est incité à saisir ses identifiants.

Les traitements associés à ces campagnes se sont améliorés au cours du temps pour aboutir à une solution désormais complètement automatisée.

Le fonctionnement et l'organisation générale sont détaillés : paramétrage et envoi des mails, fonctionnement d'un faux site, base de données contenant les informations sur les utilisateurs, les campagnes et les résultats. Les informations stockées et traitées étant des données à caractère personnel, l'aspect RGPD est abordé.

En final, sont présentés les enseignements généraux tirés des résultats des campagnes de phishing au cours du temps, en particulier de savoir si l'objectif d'améliorer la vigilance des utilisateurs est atteint.

Mots-clefs

Phishing, hameçonnage, sensibilisation des utilisateurs, RGPD, sécurité

1 Historique de la solution

Comme beaucoup d'organismes, Inria est régulièrement la victime de messages de phishing dans le but de capter les identifiants (*login* et *mot de passe*). L'utilisation principale constatée des identifiants volés est de permettre la transmission massive de *spams* via les relais de messagerie d'Inria, avec comme conséquence leur mise en liste noire par les autres services de messagerie Internet, isolant ainsi Inria. Une utilisation davantage ciblée reste toutefois possible : un pirate peut utiliser des identifiants volés pour se connecter à divers services Inria.

En 2012, nous déplorions une dizaine de personnes victimes chaque année. Suite à une présentation de Fabrice Prigent faite à la conférence JSSI[1], nous avons décidé de sensibiliser nos utilisateurs en organisant de fausses campagnes de phishing, nous basant au départ sur les modèles que Fabrice nous a fournis.

Au tout début, les campagnes étaient réalisées de manière manuelle : sélection des utilisateurs et extraction des adresses mail depuis la base LDAP, exécution du script d'envoi des mails, analyse des résultats. Les résultats des connexions sur le faux site étaient stockés dans un fichier texte qui devait ensuite être traité afin d'obtenir des statistiques. Pour les premières campagnes, seuls les utilisateurs nouvellement arrivés étaient ciblés. Par la suite, des utilisateurs « anciens » ont également été pris en compte.

1. Le diaporama de cette présentation des disponible au lien https://ossir.org/paris/supports/2013/2013-02-12/OSSIR_phishing.pdf

De nombreuses améliorations ont été apportées pour aboutir à la solution utilisée actuellement, comme : la sélection automatique du thème de la campagne et des utilisateurs y participant, l'envoi des mails, le stockage des données dans une base de données et la réalisation d'une page permettant d'accéder aux résultats. La dernière évolution importante a consisté en la mise en conformité de l'application au RGPD.

2 Déroulement d'une campagne de phishing

Toutes les étapes se déroulent de manière automatique. Les envois de mails se font à l'aide de scripts développés en langage Perl orchestrés par `cron` et envoyés à des jours et heures ouvrées aux participants à une campagne. Actuellement, quatre campagnes sont lancées chaque année.

Voici le déroulement type d'une campagne de phishing.

1. Quelques jours avant le lancement de la campagne, les Correspondants Sécurité des Systèmes d'Information (CSSI) ainsi que les personnes liées au scénario qui sera utilisé (par exemple les personnes en charge du service mail pour un scénario impliquant le mail) sont prévenus par mail de la campagne à venir ;
2. Le jour du début de la campagne, un script effectue plusieurs actions :
    a. Choix du scénario qui sera utilisé pour la campagne ;
    b. Choix des utilisateurs qui vont y participer ;
    c. Envoi des mails de phishing ;
3. Une fois le scénario choisi, la campagne est démarrée : le site est ouvert et les utilisateurs peuvent cliquer sur le lien dans le mail qu'ils ont reçu et y accéder ; les informations relatives aux connexions sont stockées dans la base de données (quand, depuis où, mot de passe correct fourni, etc.) ;
4. Au bout de 3 jours, la campagne s'arrête (le site ne fonctionne plus) ;
5. Suite à l'arrêt de la campagne, un message est envoyé à l'ensemble des participants pour les informer ; ce message contient un lien vers une page d'explications donnant les indices qui permettaient de détecter qu'il s'agissait d'un phishing ainsi qu'un lien vers la page d'information générale (RGPD) ;
6. Au bout de 10 jours, fermeture de l'accès à la page d'explications sur la campagne, la page d'informations reste, quant à elle, accessible en permanence.

3 Scénario d'une campagne

La solution dispose d'une bibliothèque de scénarios créés en amont des campagnes. Le scénario d'une campagne est constitué de plusieurs éléments.

- Un mail qui sera transmis aux participants.
- Un site web sur lequel se connecteront les utilisateurs qui cliquent sur le lien dans le mai. Le site comprend :
    - une page d'accueil avec un formulaire pour saisir le login et le mot de passe,
    - des pages qui seront affichées à la suite d'une connexion selon le données du formulaire (login inexistant, login correct, mais mauvais mot de passe, login et mot de passe corrects).
- Une page d'explications présentant les indices permettant d'identifier un phishing.

Toutes les pages existent en version française et anglaise, le choix de la version à afficher se fait automatiquement selon les préférences du navigateur de l'utilisateur.

Figure 1 : Exemple de mail envoyé

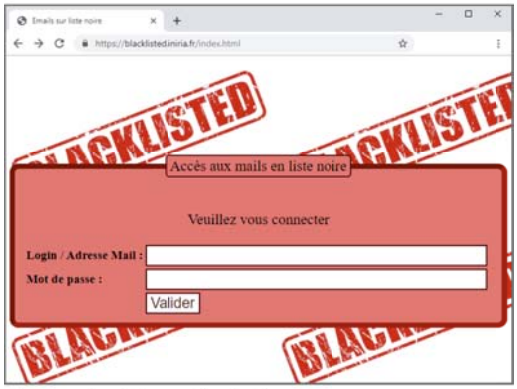


Figure 2 : Exemple de faux site

Les scénarios peuvent être plus ou moins crédibles, ce qui influence le taux de victimes. Voici les principaux leviers :

- l'orthographe et la syntaxe du mail ;
- le thème de la campagne (problème lié au mail, problème lié au mot de passe, etc.) ;
- le domaine utilisé pour le faux site (proche du domaine institutionnel « *inria.fr* » ou pas du tout) ;
- l'utilisation d'un certificat auto signé ou d'un vrai certificat (pour les dernières campagnes, des certificats issus de *Let's Encrypt* ont été utilisés).

Les messages transmis ainsi que les pages web des faux sites sont, à l'exception de la page d'accueil qui est réalisée spécifiquement, tous produits à l'aide du moteur de modèles « *Template Toolkit* » (`TT2`[2]). Les pages sont ainsi personnalisables et leur apparence uniformisée. Plusieurs pages des faux sites utilisent le même fichier modèle, paramétrées avec le nom de domaine et le nom de site utilisé par le scénario.

4 Sources de données

4.1 Fichier de configuration

Un fichier au format `yaml`[3] contient certains paramètres de fonctionnement ainsi que les informations relatives aux divers scénarios. Pour chacun, le fichier de configuration comporte les éléments suivants :

- informations sur le scénario : nom, index, état (scénario actif ou désactivé.
- nom de domaine pour le faux site (par exemple `iniria.fr`) ainsi que le nom du site (par exemple `blacklisted`, le nom qualifié sera alors `blacklisted.iniria.fr`).
- paramètres du mail : sujet, émetteur, destinataire, fichier modèle du corps du mail et paramètres pour le modèle (URL du faux site et texte associé).

4.2 Base de données

Une base de données est utilisée pour stocker les données des campagnes. Le choix s'est porté sur `sqlite3` pour plusieurs raisons.

- L'implémentation SQL de `sqlite3` est tout à fait suffisante pour répondre aux besoins.
- Il y a peu d'enregistrements à stocker au total.

2. http://www.template-toolkit.org
3. https://yaml.org/spec/1.2/spec.html

– Les connexions des participants aux faux sites générant très peu d'accès simultanés en écriture à la base, le fait que les accès concurrents soient gérés par `sqlite3` en verrouillant la base n'est pas un problème.

La base de données est constituée de 3 tables.

– *Table des campagnes :* contient la liste des campagnes, avec pour chacune ses caractéristiques (nom du scénario, date de la campagne).

– *Table des utilisateurs :* contient les informations sur les utilisateurs ayant participé à au moins une campagne (nom patronymique, login, mail, site Inria appartenance, identifiant Inria unique). Les données sont obtenues à partir de la base LDAP (voir ci dessous).

– *Table des participants :* contient les informations de participation des utilisateurs aux différentes campagnes. Chaque enregistrement référence à la fois l'index de l'utilisateur dans la table des utilisateurs et l'index de la campagne dans la table des campagnes. Cet enregistrement contient les données suivantes :

  – le fait que l'utilisateur est nouveau ou pas (au moment du lancement de la campagne),
  – la date/heure d'envoi du mail,
  – la date/heure de la connexion au faux site,
  – l'adresse IP utilisée,
  – le fait que l'utilisateur a fourni son login seulement ou également son mot de passe,
  – la date/heure d'accès à la page d'explications sur la campagne.

4.3 Annuaire LDAP

L'annuaire LDAP d'Inria est utilisé à la fois pour sélectionner les utilisateurs qui participeront à une campagne et pour authentifier les personnes se connectant sur le faux site. Toutes les connexions LDAP se font au travers de *TLS* pour bénéficier du chiffrement.

L'annuaire comporte classiquement une branche « *people* » dans laquelle chaque utilisateur est enregistré. En plus de la classe standard `inetOrgPerson`, chaque enregistrement dispose d'attributs d'une classe auxiliaire spécifique à Inria de nom `inriaPerson`.

Les attributs suivants sont utilisés (les attributs spécifiques à Inria ont le préfixe « `inria` ») :

Attribut	**Valeur**	**Attribut**	**Valeur**
`createTimeStamp`	Date à laquelle a été ajouté l'enregistrement	`uid`	Identifiant unique de l'utilisateur
`mail`	Adresse mail de l'utilisateur	`ou`	Site Inria d'appartenance
`cn`	Nom patronymique de la forme *NOM Prénom*	`inriaLogin`	Login de l'utilisateur
		`inriaEntryStatus`	Compte actif ou fermé

Les attributs à gauche dans le tableau sont utilisés de manière standard. Ce n'est pas le cas de ceux de droite. Outre l'attribut spécifique `inriaLogin`, l'attribut `uid` ne contient pas, comme souvent, le login de l'utilisateur, mais un identifiant utilisé comme clé dans plusieurs applications Inria pour identifier l'utilisateur. Enfin, l'attribut `inriaEntryStatus` permet de savoir si le compte est actif ou désactivé.

5 Lancement de la campagne

L'ensemble des actions décrites ci-dessous sont effectuées par un unique script Perl qui est lancé par `cron`.

5.1 Choix du scénario de la campagne et des utilisateurs

Le scénario est choisi parmi ceux qui se trouvent dans le fichier de configuration. La stratégie est de prendre, dans les scénarios actifs, celui dont la date de dernière campagne est la plus ancienne, en exploitant les données de la table des campagnes de la base de données. Ceci permet de ne pas rejouer trop souvent le même scénario et rend prioritaire tout nouveau scénario jamais utilisé. Une fois le scénario sélectionné, un nouvel enregistrement est ajouté dans la table des campagnes.

Pour choisir les participants, les enregistrements des comptes actifs (filtre sur `inriaEntrySatus`) de la base LDAP sont parcourus. Les utilisateurs choisis en priorité sont :

- les nouveaux arrivants depuis la dernière campagne (utilisation de l'attribut `createTimeStamp`) ;
- les utilisateurs victimes lors de la campagne précédente.

Une partie des « anciens » utilisateurs est également sélectionnée, avec les critères suivants : la dernière participation à une campagne de phishing doit être suffisamment ancienne et le scénario différent de celui de la campagne en cours. L'objectif est d'avoir entre 1000 et 1500 participants au total.

Une fois les utilisateurs sélectionnés, leurs informations sont ajoutées ou mises à jour dans la table des utilisateurs et les enregistrements de la table des participants sont initialisés.

5.2 Transmission des mails

Après la préparation des données dans la base de données comme décrit ci-dessus, les mails sont envoyés. Le script gère la communication avec les serveurs de courrier d'Inria. Quelle que soit la campagne, les mails et leur transmission obéissent à un même schéma.

- Le message envoyé est identique pour tous les utilisateurs : le champ destinataire est identique pour tous les messages (comme pour un destinataire en « bcc »).
- Le script travaille au niveau transport pour l'envoi des mails et utilise TLS pour chiffrer les communications.
- Des paramètres de fonctionnement régulent le processus d'envoi : temps entre deux connexions sur un serveur de courrier, nombre de destinataires du message lors d'un envoi.

Cette façon de procéder permet de récupérer les messages d'erreur ou d'information transmis par les serveurs de courrier et corriger le fonctionnement. Ainsi, si le serveur refuse l'envoi d'un message en raison d'un taux d'envois trop important, un mécanisme d'augmentation du délai entre deux connexions est activé jusqu'à la réussite d'un envoi. Ensuite, une diminution progressive de ce délai est effectuée.

En pratique, l'envoi des messages aux participants est effectué en 1 heure environ.

6 Le faux site

6.1 Fonctionnement du faux site

Lorsqu'une personne tente d'accéder au site au travers de l'URL de connexion, un script CGI (écrit en Perl) vérifie que la campagne est bien en cours. Si ce n'est pas le cas, la personne est redirigée vers la page de *Wikipedia* traitant du phishing. Dans le cas contraire, la page d'accueil du site contenant le formulaire de connexion s'affiche, en version française ou anglaise, selon les préférences linguistiques du navigateur.

La page de réponse affichée suite à l'envoi du formulaire de connexion diffère selon le cas.

- *Cas 1* : l'utilisateur a renseigné des valeurs quelconques comme login et mot de passe.
- *Cas 2* : l'utilisateur a saisi son login, mais pas le bon mot de passe.
- *Cas 3* : il a saisi ses vrais identifiants (login et mot de passe).

Les données du formulaire sont traitées par un script CGI qui contrôle en premier lieu l'existence du login renseigné. Cela se fait par consultation de la base LDAP et recherche du *distinguised name* (`dn`) associé à ce login.

Lorsque le login n'existe pas (*Cas 1*), la page de réponse félicite l'utilisateur de sa prudence d'avoir entré un login inexistant. Bien sûr, cela peut résulter d'une faute de frappe, mais il n'est pas possible de le déterminer.

Lorsque le login existe, le mot de passe est testé à l'aide d'un *BIND* LDAP. En cas de mot de passe incorrect (*Cas 2*), une page similaire à celle du *Cas 1* est renvoyée. Dans le dernier cas (*Cas 3*), la page de réponse indique que l'utilisateur est victime d'un phishing organisé par la DSI et précise quels sont les indices permettant de détecter que le message et le site n'étaient pas authentiques.

Dès lors qu'un login existant a été transmis (*Cas 2* ou *Cas 3*), les champs suivants de l'enregistrement dans la table des participants sont renseignés : date/heure de connexion, adresse IP de l'utilisateur, mot de passe transmis correct ou non, langue du navigateur.

6.2 Fiabilisation des données

Plusieurs mécanismes sont mis en œuvre pour renforcer la fiabilité des données recueillies.

- Une connexion faite par un utilisateur ne participant pas à la campagne est purement ignorée.
- Lorsque l'enregistrement dans la table des participants a déjà été mis à jour pour un utilisateur donné, toute connexion avec son login n'est plus prise en compte.
- Dans tous les cas, suite à la validation du formulaire, un *cookie* est mis en place dans le navigateur avec la page de réponse. Si par la suite l'utilisateur tente à nouveau l'envoi du formulaire, les données transmises seront ignorées à cause de la présence du cookie.

Ces différentes mesures visent à ce que seule la toute première connexion au site soit prise en compte dans les résultats.

7 Clôture de la campagne

Au bout de 3 jours, la campagne se termine. Le site est fermé, toute connexion sur le faux site renvoie vers la page consacrée au phishing sur *Wikipedia*.

Un mail d'information est alors envoyé à tous les participants, expliquant qu'il y a eu une campagne de phishing organisé par la DSI à laquelle l'utilisateur a participé. Un premier lien dans le mail pointe vers une page donnant des explications sur les indices permettant de détecter que le message et le site n'étaient pas authentiques. Un second lien donne accès à la page d'informations liées au RGPD.

La page des explications sur la campagne nécessite une authentification par CAS[4] et se fait au travers d'un script CGI. Lorsqu'un utilisateur y accède, son enregistrement dans la table des participants est mis à jour avec la date/heure d'accès. Au bout de 10 jours, la page n'est plus accessible, il est alors possible d'effectuer des statistiques sur la consultation des explications.

4. https://www.apereo.org/projects/cas

8 Traitement des résultats

8.1 Traitements effectués

La grande majorité des traitements ne se fait pas sur les données individuelles, mais au contraire sur des données agrégées. Voici quelques exemples :

- informations sur une campagne (date, thème, nombre de participants) ;
- statistiques sur le temps entre l'envoi du mail et la connexion d'un utilisateur sur le site ;
- nombre de victimes par site Inria et pourcentage relatif ;
- victimes par catégorie (nouvel utilisateur ou non) et pourcentages ;
- victimes par langage préféré du navigateur ;
- victimes par origine de la connexion (depuis un site Inria ou depuis ailleurs).

L'accès aux résultats se fait au travers d'une page protégée par une authentification CAS, ce qui permet de savoir qui y accède. Les résultats agrégés sont accessibles par tout utilisateur Inria, les résultats individuels uniquement par le SOC[5] d'Inria, les CSSI[6] et le RSSI[7].

Voici à titre d'exemple un tableau donnant les informations sur la répartition des victimes, pour une campagne donnée, selon les sites Inria :

Site	Participants	Victimes	% Victimes
Bordeaux	77	4	5,2 %
Lille	64	5	7,8 %
Lorraine	149	4	2,7 %
Paris	138	9	6,5 %
Rennes	202	4	2,0 %
Rhone-Alpes	144		
Rocquencourt (Siège)	72	4	5,6 %
Saclay	108	2	1,9 %
Sophia	137	8	5,8 %

5. Security Operations Center : Centre d'Opérations de Sécurité

6. Correspondant Sécurité des Systèmes d'Information

7. Responsable de la Sécurité des Systèmes d'Information

Cet autre exemple montre la répartition des victimes selon leur catégorie :

Catégorie	Participants	Victimes	% Victimes
Nouveau	341	24	7,0 %
Ancien	750	16	2,1 %
Global	1091	40	3,7 %

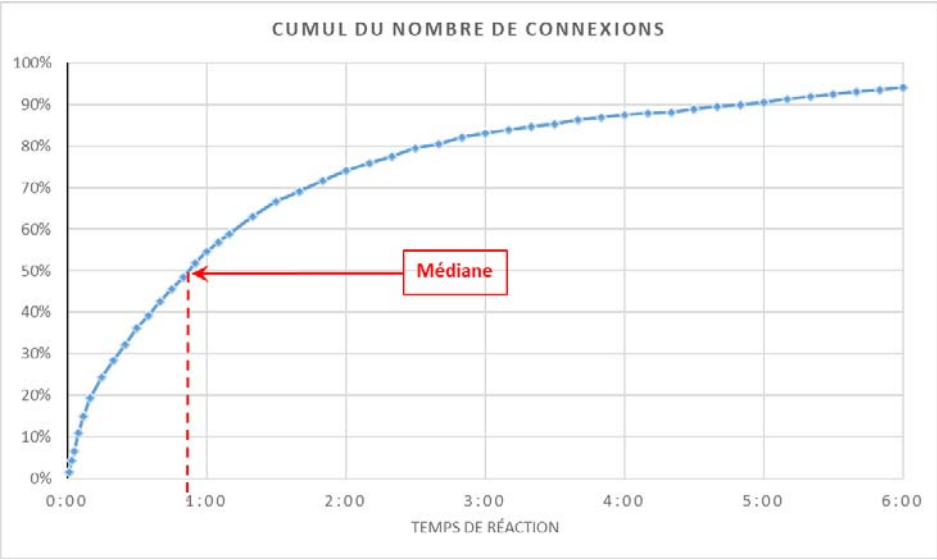
Les utilisateurs victimes lors d'une campagne, notamment ceux qui ont été victimes à plusieurs reprises, sont susceptibles d'être contactés par un CSSI pour des compléments d'information, afin améliorer leur vigilance quant aux mails qu'ils reçoivent. Cela nécessite que les CSSI des centres aient accès aux données individuelles des utilisateurs de leur centre :

- utilisateurs participant à la campagne ;
- utilisateurs victimes ;
- victimes récidivistes (victimes lors de la campagne et lors de la précédente campagne également).

8.2 Analyse des résultats

Plusieurs tendances se dégagent des résultats des campagnes.

En premier lieu, l'analyse du temps de réaction des victimes (temps écoulé entre l'envoi du mail et la connexion sur le site) permet de constater que la majorité des personnes réagit très vite. Le graphique ci-dessous montre le cumul du nombre de connexions (en pourcentage) en fonction du temps de réaction pour l'ensemble des campagnes. La médiane des temps de réactions est inférieure à une heure :



Une autre constatation concerne l'origine des connexions sur les faux sites : en moyenne, de l'ordre de 50 % des connexions ne se font pas depuis un site Inria.

Ces deux constations montrent qu'une approche visant à bloquer l'accès au site grâce à un filtre sur les équipements réseau ou même faire une information générale sera inefficace dans le cas d'une « vraie » campagne de phishing. Il en est de même pour signaler le site sur des services comme *Phishing Initiative*[8].

8. https://phishing-initiative.fr/contrib/

Pour l'ensemble des campagnes, le pourcentage de nouveaux utilisateurs victimes est systématiquement beaucoup plus élevé que celui des anciens utilisateurs victimes. De plus, en comparant des campagnes utilisant le même scénario, on constate que le pourcentage des anciens utilisateurs victimes a tendance à baisser sensiblement (voir tableau ci-contre qui reprend pour 4 scénarios sur 3 années les pourcentages des utilisateurs anciens victimes).

	2014	**2015**	**2016**
Scénario 1	4,3 %	4,6 %	1,8 %
Scénario 2	5,8 %	6,4 %	3,7 %
Scénario 3	1,8 %	1,1 %	0,9 %
Scénario 4	3,9 %	2,3 %	3,3 %
Moyenne	**4,0 %**	**3,6 %**	**2,4 %**

On peut déduire de ces deux dernières constatations que la vigilance des anciens utilisateurs tend à se renforcer, ce qui démontre l'utilité des campagnes. Et qu'il est indispensable de poursuivre ces campagnes, notamment pour les nouveaux utilisateurs, d'autant que le taux de *turn over* chez Inria, dû notamment à la typologie des personnels (doctorants, chercheurs invités, etc.), est très important (de l'ordre de 25 % chaque année).

9 Prise en compte du RGPD

Suite à la mise en application du Règlement Général sur la Protection des Données (RGPD) le 25 mai 2018, il a fallu rendre l'application conforme. Pour ce faire, plusieurs actions ont été menées.

9.1 Informations sur le traitement

Une page dont l'accès est protégé par une authentification CAS a été créée pour fournir aux utilisateurs les mentions d'information, notamment :

- finalité du traitement ;
- licéité du traitement ;
- données recueillies ;
- destinataires des données ;
- durée de conservation des données ;
- lieu de stockage des données ;
- coordonnées du DPO[9].

Du fait de l'authentification par CAS, on sait quel est l'utilisateur qui accède à la page, les données recueillies sur cet utilisateur sont donc également montrées sur cette page d'informations.

9.2 Conservation des données

Anciennement, les données étaient conservées sans limitation de durée, de manière à pouvoir disposer de mesures statistiques et d'évolution sur la plus longue période possible. Avec le RGPD, il devenait nécessaire de limiter la durée de conservation des données à caractère personnel.

Pour préserver la possibilité de statistiques sur les campagnes anciennes, les données sont anonymisées, au lieu d'être supprimées. Après anonymisation, elles ne peuvent plus être reliées à une personne. Ce ne sont donc plus des données à caractère personnel et elles peuvent alors être conservées sans limites.

Le processus d'anonymisation d'une campagne consiste à rattacher les données collectées lors de cette campagne à des utilisateurs fictifs. Ainsi, on substitue à un utilisateur d'un site donné un utilisateur fictif appartenant au même site. Le site n'est pas une donnée à caractère identifiante, même de manière indirecte, au vu du grand nombre de personnes appartenant au même site. Ce processus effectue également le remplacement des adresses IP par l'adresse « `0.0.0.0` ».

9. Délégué à la Protection des Données

Ensuite, les enregistrements de la table des utilisateurs devenus inutiles sont supprimés.

9.3 Droits des utilisateurs

Deux autres traitements ont été implémentés pour l'application du droit à l'oubli et du droit d'opposition. Le droit à l'oubli consiste à anonymiser immédiatement les données d'un utilisateur. Pour le droit d'opposition, une table supplémentaire dans la base de données contient les identifiants Inria des personnes ayant exercé ce droit afin de les filtrer des participants aux campagnes. Sur la page d'informations sur le traitement, un paramètre de fonctionnement `TT2` autorise l'affichage de formulaires qui permettent aux utilisateurs d'exercer ces droits.

Toutefois, la licéité du traitement résulte de la PSSIE[10] dont l'une des mesures prévoit la formation des utilisateurs à la sécurité. Il s'agit donc d'un traitement licite du fait d'une obligation légale (article 6.1c du RGPD) qui ne nécessite pas d'obtenir le consentement des utilisateurs. Les droits qu'ils peuvent exercer sont très limités, en particulier, les droits à l'oubli et d'opposition ne sont pas proposés actuellement sur la page d'information.

10 Conclusions et perspectives

L'utilité de ces campagnes de phishing, notamment concernant les nouveaux utilisateurs, est démontrée. Du fait de l'arrivée quasi permanente de nouveaux utilisateurs, il est indispensable de lancer des campagnes régulièrement. Bien que les anciens utilisateurs soient plus vigilants que les nouveaux, il y a toujours des victimes. Il faut donc également continuer à les faire participer.

Comme les « vrais » phishings sont de mieux en mieux faits avec quelquefois de très bonnes copies de sites Inria existants, il est nécessaire de créer régulièrement de nouveaux scénarios réalistes et d'augmenter la difficulté de découverte.

Quelques pistes d'amélioration de l'application ont été identifiées.

- Placer dans le fichier de configuration des paramètres de fonctionnement qui sont actuellement directement définis dans les scripts.
- Ajouter au script d'envoi de mails la possibilité d'avoir les participants comme destinataires des messages . Cette modification entraînera immanquablement une durée plus importante pour la transmission de l'ensemble des mails puisque les messages devront alors être envoyés de manière individuelle.

Pour lutter contre le phishing ou les conséquences d'un phishing réussi, des possibilités sont également à l'étude.

- Mettre en place une authentification multi facteurs : même si le mot de passe est capturé lors d'un phishing réussi, cela ne sera plus suffisant pour usurper le compte d'un utilisateur.
- Implémenter dans le service mail d'Inria des possibilités comme SPF (déjà mis en œuvre), DKIM et DMARC afin de détecter et traiter les messages indésirables (phishing. Spam, etc.).

10. https://www.ssi.gouv.fr/entreprise/reglementation/protection-des-systemes-dinformations/la-politique-de-securite-des-systemes-dinformation-de-letat-pssie/