PHISHING

Capitoul, jeudi 19 octobre 2017

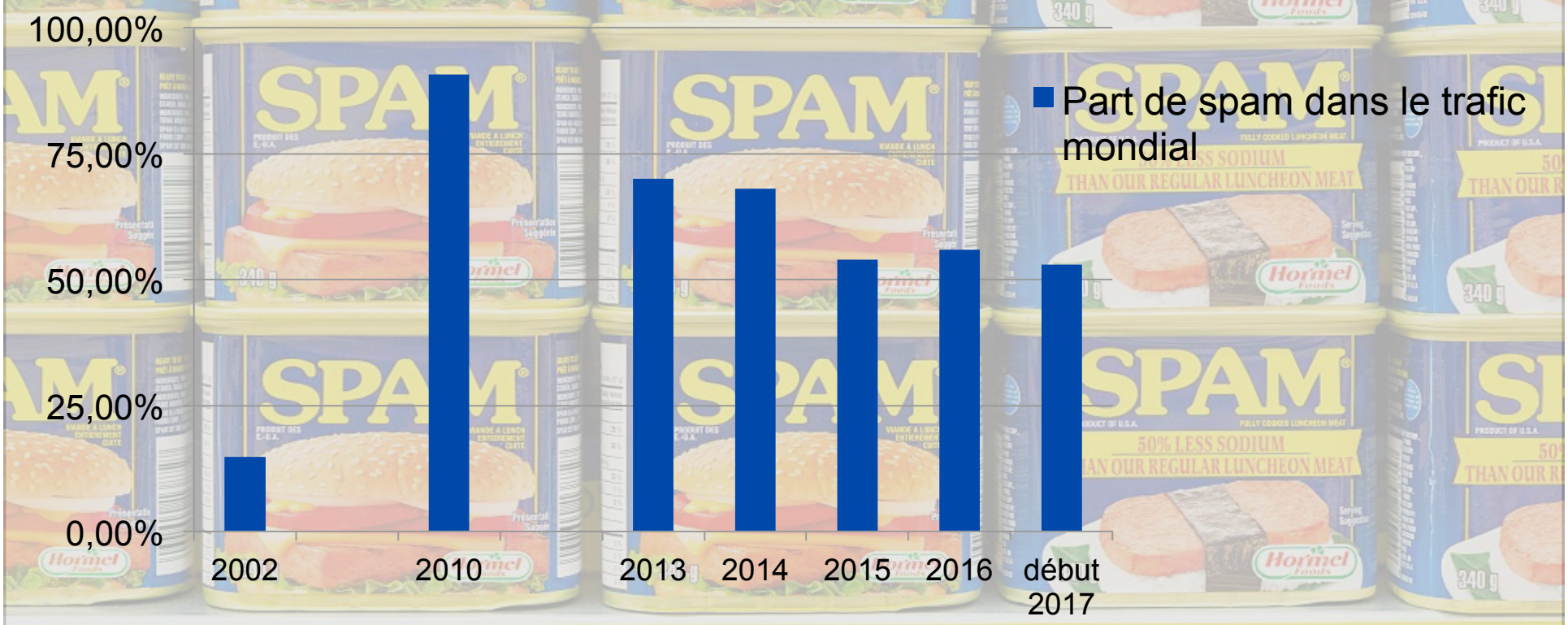
Yann BACHY, ISAE-SUPAERO

De l'e-mail jusqu'au spam

1974
Premier e-mail

1978 premier spam

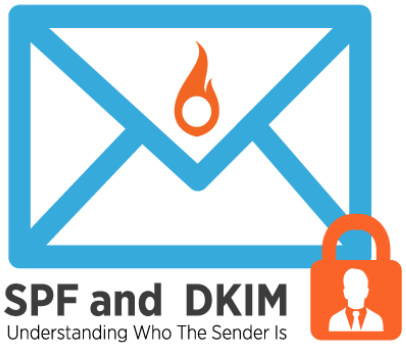
2015
400 milliards



La lutte anti-spam

protected by SPF

SpamAssassin



Phishing

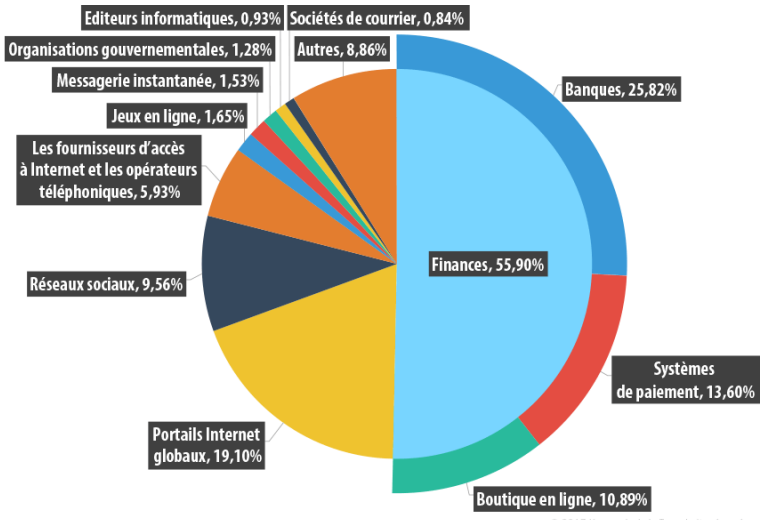
- Phreaking + fishing : Hameçonnage, filoutage

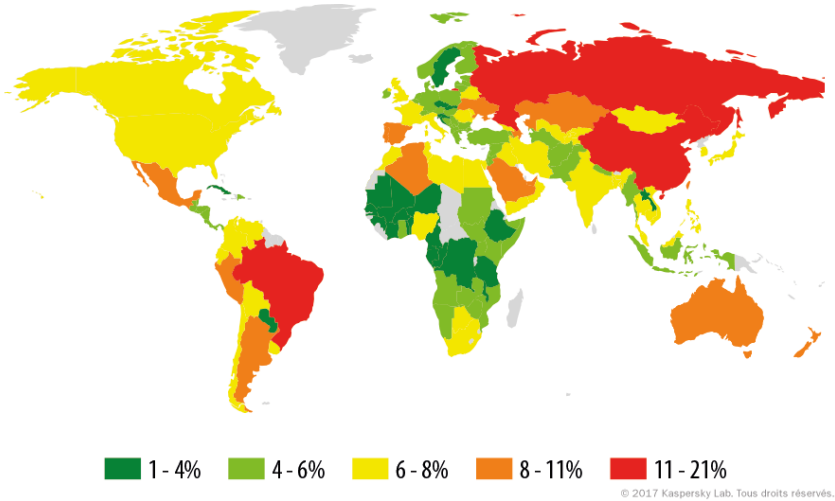
- Exemples bien connus :
  - Fausses factures
  - Demandes de mots de passe dans un mail (administrateu système)
  - Demande de rappel

- Techniques variées
  - Pièces jointes contaminées (script VB)
  - Liens similaires (i.e.: www.societegeneral.fr au lieu de www.societegenerale.fr)
  - Redirections et rebonds
  - Utilisation de caractères unicode
  - …

Chiffres clés du phishing

- 51 millions d'attaques empêchées par **Kaspersky** au 1er trimestre 2017





- Conséquences : pertes financières, de temps, atteinte à l'image de marque, conséquences politiques,…
- Première étape d'une attaque plus étendue (APT)

Problème

- Le phishing étant quotidiennement mentionné dans la presse, dans la vie courante, la majorité des utilisateurs connaissent son existence et les risques

Les consignes restent identiques:
- n'ayez pas une confiance aveugle dans le nom de l'expéditeur des messages que vous recevez,
- vérifiez l'existence de l'expéditeur en cas de doute (Organnuaire, etc.),
- méfiez-vous des pièces jointes, n'ouvrez jamais une pièce jointe si vous ne connaissez pas l'expéditeur du mail.
- ne répondez jamais à une demande d'informations confidentielles (Mot de passe, etc.), sachez que le SI ne vous demandera jamais votre mot de passe,
- avant de cliquer sur un lien présent dans un message, passez votre souris au-dessus du lien, afin de vérifier la destination réelle du lien en bas de votre écran,
- faites attention aux caractères accentués dans le texte ainsi qu'à la qualité du français ou de la langue pratiquée par votre interlocuteur (le niveau de français doit être conforme avec ce que vous connaissez de votre correspondant, ainsi que le contenu général du message)
- paramétrez correctement votre logiciel de messagerie (dans la mesure du possible).

En cas de doute, n'hésitez pas a solliciter le centre de services du SI.

- Pourquoi reste-il aussi efficace et comment lutter contre ?

Réponse


CYBERSÉCURITÉ
Bercy a envoyé des faux emails de phishing à ses employés
par LOUISE MILLON le 4 OCTOBRE 2017
4 COMMENTAIRES

Outil existant

- Travaux de Fabrice PRIGENT
  - Améliorer la résistance de la communauté universitaire par rapport au phishing
  - Rappels par message sur le phishing
  - Envoi automatique d'e-mails de faux phishing
  - Statistiques sur les résultats

- Présentation des résultats à RéSIST en 2013
  - Résultats même avec du « mauvais » phishing
  - Une même personne peut se faire avoir plusieurs fois
  - Les communications institutionnelles ne sont pas lues
  - Pas de corrélation avec le niveau d'étude, ni le domaine !
  - Pédagogie par l'exemple efficace

Reprise en main de l'outil

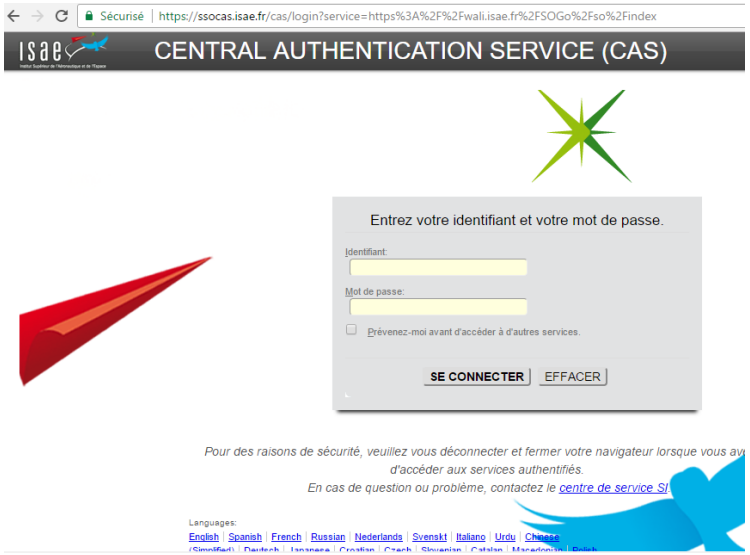
y.bachy@port-bachy: ~/Documents/ISAE/OSSI/Sensibilisation/tmp/html_phishing

Fichier Édition Affichage Rechercher Terminal Aide

```
##############################################################################################################
#
#       Ceci est un manuel rapide d'installation pour un outil de campagne de phishing pédagogique
#
#       Version du 11 juin 2016
#       Auteur : Fabrice Prigent
#
Il vous faudra FORCEMENT modifier des éléments manuellement. Les explications ci dessous peuvent vous y aider, ains
i que le script install.sh, mais
en aucun cas, tout cela ne pourra faire le travail à votre place.


Vous avez une arborescence web qui comporte les éléments suivants
- ce fichier install.txt
- le repertoire "send" qui contient tout ce qu'il faut pour envoyer la campagne
        - le fichier "send_config.pm" qui contient les paramètres de votre environnement
        - le fichier install.sh qui va vous aider à personnaliser votre campagne. A ne lancer que lorsque le fichie
r send_config.pm ci dessus est rempli.
        - le fichier "users.txt" qui contient la liste des mails à tester (c'est à vous de le mettre à jour réguliè
rement)
        - le repertoire "campagnes" qui contient les mails des campagnes
                - 0.txt qui est la première campagne pour vos utilisateurs (elle est "gentillette")
                - 1.txt et les suivantes sont des campagnes plus agressives (copie de votre interface d'authentific
ation)

                VERIFIEZ LEURS THEMES !!! Sans rien dévoiler aux intéressés, vous devez prévenir correctement la di
rection que les campagnes sont REALISTES (dans le sens utilisés pour de vrai par des pirates) et que certaines peuv
ent être pénalisantes pour certains services !!!!

- le repertoire "cas" qui contient les formulaires et leurs éléments
:
```

Fonctionnalités de l'outil 1/3

- E-mail avec lien vers un faux portail d'authentification



Fonctionnalités de l'outil 2/3

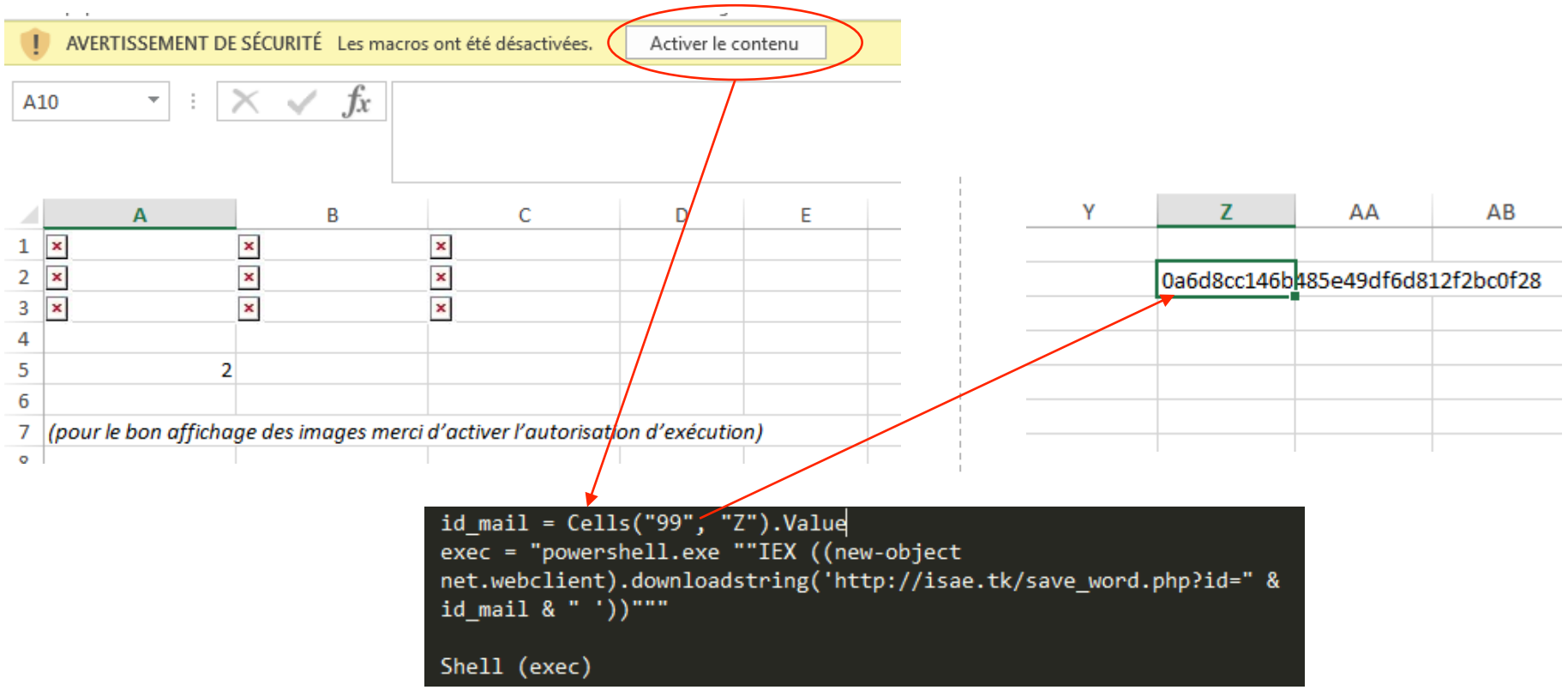
- E-mail avec une « image » dans le corps faisant appel à un script php

Cette "image" que vous avez ouverte fait partie de notre campagne de sensibilisation au **phishing**.
Ne vous inquiétez pas, vos informations personnelles ne sont pas compromises. Cependant, nous vous invitons vivement à relire attentivement les points suivants :

- n'ayez pas une confiance aveugle dans le **nom de l'expéditeur** des messages que vous recevez,
- vérifiez l'existence de l'expéditeur en cas de doute (Organnuaire, etc.),
- méfiez-vous des **pièces jointes**,
- faites attention aux caractères accentués dans le texte ainsi qu'à la **qualité du français** dans le texte ou de la langue pratiquée par votre interlocuteur,
- **paramétrez** correctement votre logiciel de messagerie (dans la mesure du possible).

Fonctionnalités de l'outil 3/3

- E-mail avec une pièce jointe malveillante faisant appel à un script php



Tout est géré dans une base de données

- Les résultats sont stockés dans une base de données :
  - Date
  - Adresse IP
  - Nom de la machine (si dans le réseau de l'école)
  - User agent
  - Identifiant d'envoi (hash unique permettant de retracer l'utilisateur cible)
  - Nom d'utilisateur rempli
  - Mot de passe rempli (booléen : conformité à la politique de mot de passe de l'établissement)
  - Résultat de la vérification des identifiants sur l'annuaire d'entreprise (LDAP)

Points d’attention

- Nécessité de prévenir les utilisateurs en amont des campagnes
- Signalement par Firefox et autres navigateurs
- Nécessité de prévenir les éventuels partis concernés
  - Exemple en 2015 du gouvernement flamand avec Thalys
  - Exemple récent à la DGA avec un cabinet d‘avocats
- Ne pas divulguer les identités précises, juste des statistiques globales

Vous le voulez aussi ?