

# PHISHING, LE RETOUR

---

RéSIST, mardi 20 juin 2016

Doriane PERARD – ISAE

Stagiaire de Yann BACHY, RSSI



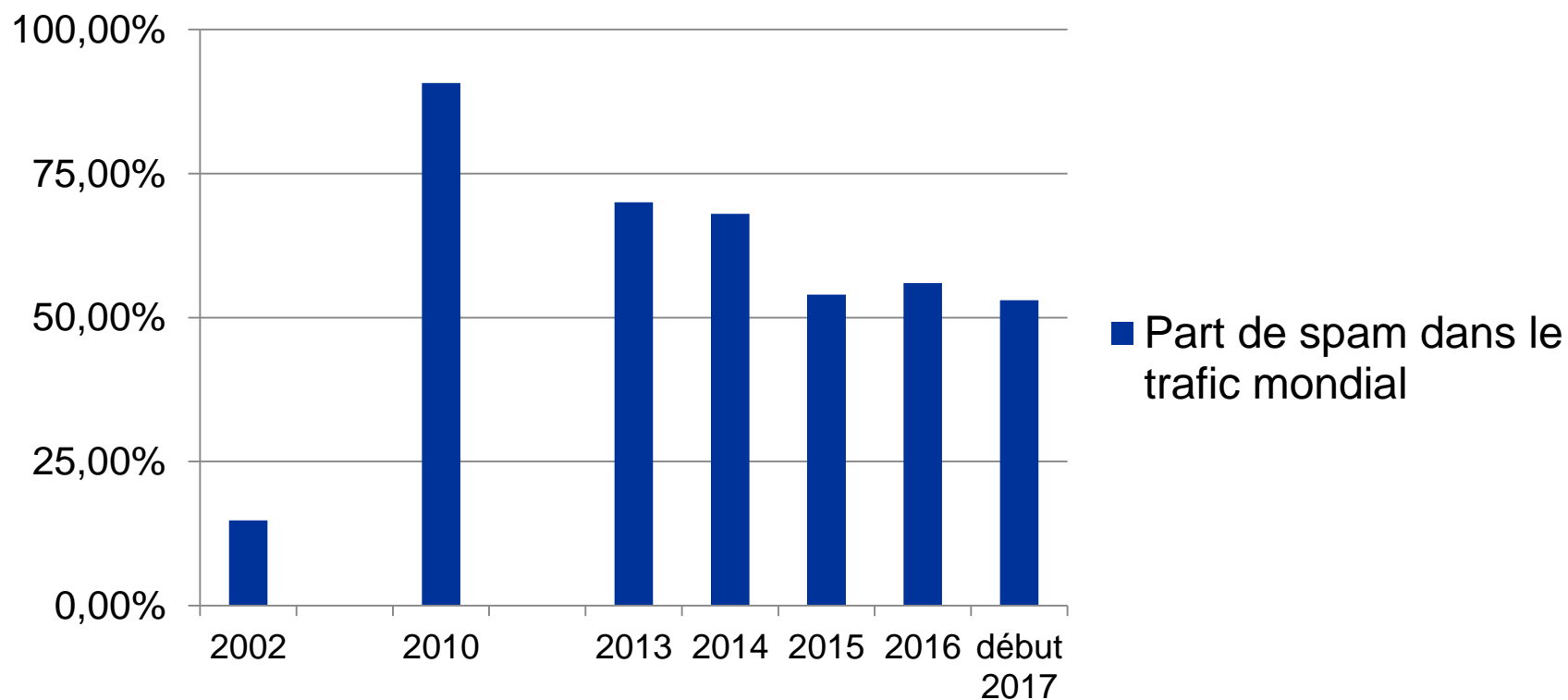
# Plan

- Contexte global
- Contexte local à l'ISAE
- Phishing pédagogique
- Futur du projet

# De l'e-mail jusqu'au spam 1/2



# De l'e-mail jusqu'au spam 2/2



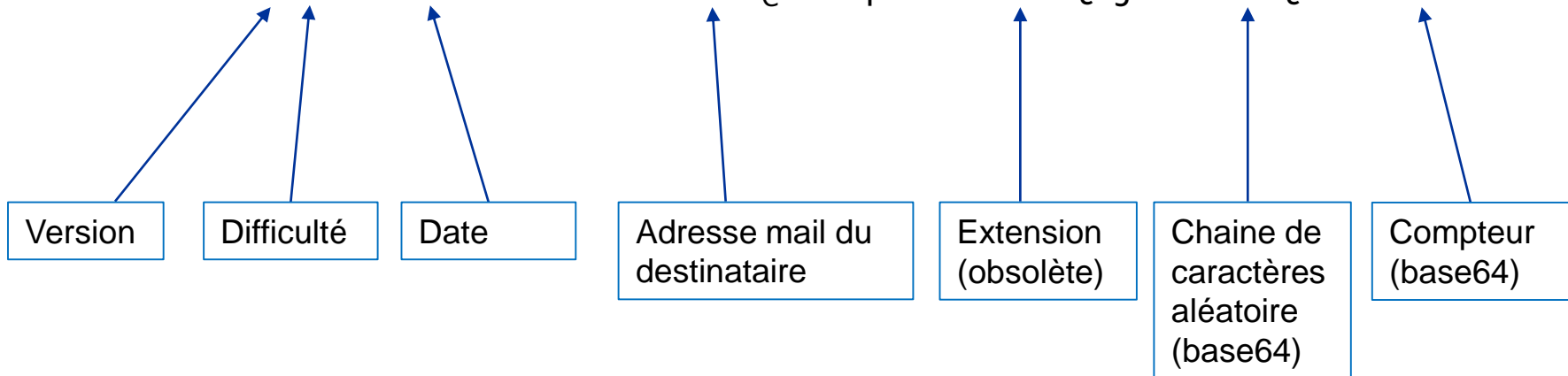
# Mesures clés anti-spam 1/3

- Proof Of Work

- Même principe que dans une blockchain
- HashCash : prouver qu'on a effectué une quantité de travail

- Exemple de challenge :

X-Hashcash: 1:20:060408:destinataire@exemple.com::1QTjaYd7niiQAsc:ePa



# Mesures clés anti-spam 2/3

- **GreyList**
  - Manuel : demande de confirmation manuelle de l'expéditeur
  - Automatique : rejet temporaire de l'e-mail
- **BlackList**
  - Selon l'IP / le nom de domaine
  - Publiques / privées
  - Critères très variés : pots de miel, dénonciations manuelles, serveurs relais ouverts, FAI, IP de certains pays,...
- **WhiteList**
  - Serveurs et IP de confiance

# Mesures clés anti-spam 3/3

- Sender Policy Framework

- Définir quels serveurs ont le droit d'émettre un e-mail pour un nom de domaine

exemple.fr. IN SPF "v=spf1 ip4:198.51.100.123 (a) (-all) "

- DomainKeys Identified Mail

- Associer un nom de domaine à un message grâce à une signature

DKIM-Signature: v=1; a=rsa-sha256; d=exemple.fr; q=dns/txt; s=default; [...]

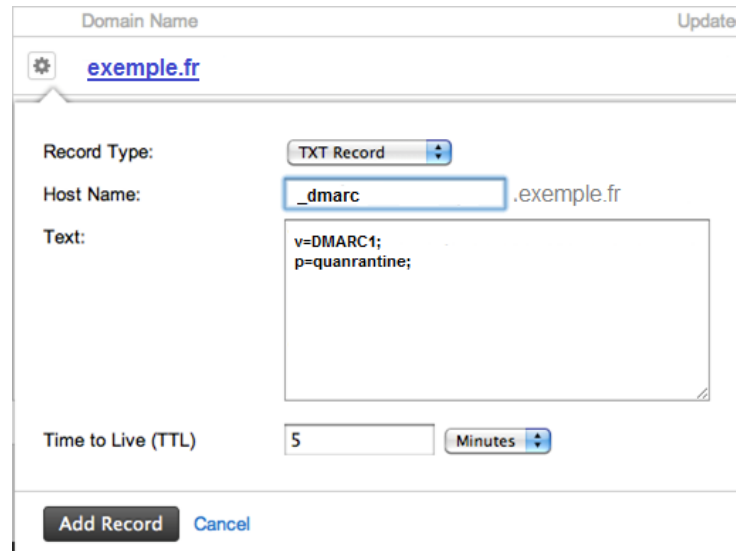
h=from:to:subject:date:keywords:keywords;

b=dzdVyOfAKCdLXdJ0c9G2q8LoXS1EniSbav+yuU4zGeeruD001szZVoG4ZHRNiYzR

The screenshot shows a configuration window for a DNS record. At the top, there is a gear icon and the domain 'exemple.fr'. The 'Record Type' is set to 'TXT Record'. The 'Host Name' is 'default.\_domainkey' with '.exemple.fr' to its right. The 'Text' field contains a long DKIM signature string: 'v=DKIM1; p=MIGfMA0GCsGqSIb3DQEBAQUAA4GNADCBiQKBgQC un+PG2rZvD9wjsGd+3RWLOz5UUXS0wtFFsMyyu2Mn9 pNIW+hxgoAhDuQtZTqSZRAXT6p+eoV08NuH2qsn+7 pXgrKYyJOxunT6Ak4jlua2Yq6wO7hmdt+jEHhA2zOIRw 14yx/rbg3/TWT9+GxtDPGMkXky4d5h1Zzc1EEGbjApl QIDAQAB'. The 'Time to Live (TTL)' is set to '5' minutes.

# Mesures clés anti-spam 3/3

- Domain-based Message Authentication Reporting and Conformance
  - Indiquer la façon dont sont « protégés » les e-mails (SPF / DKIM)
  - Indiquer ce que le serveur mail de réception doit faire d'un message dont l'authentification échoue (spam, laisser passer, rejeter)
  - Avertir l'utilisateur en cas d'échec de l'authentification



The screenshot shows a web interface for configuring a DNS record for the domain `exemple.fr`. The record is a `TXT Record` with the following details:

- Record Type:** TXT Record
- Host Name:** `_dmarc` (with `.exemple.fr` appended)
- Text:**

```
v=DMARC1;
p=quarantine;
```
- Time to Live (TTL):** 5 Minutes

At the bottom, there are buttons for `Add Record` and `Cancel`.



# Phishing

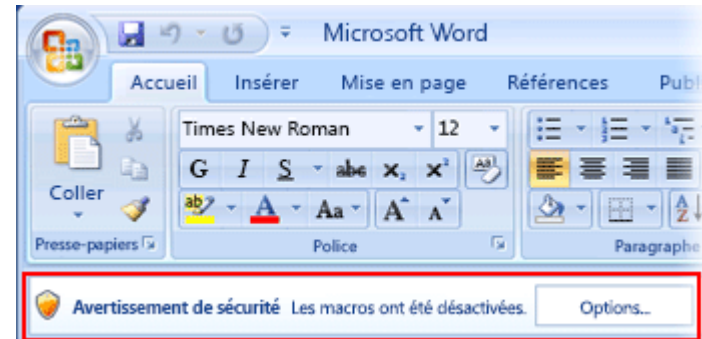
- Phreaking + fishing
- Origine : AOHell [1996]
- Exemples bien connus :
  - Fraude 4-1-9
  - Fausses factures
  - Demandes de mots de passe dans un mail
    - Message d'un administrateur système



# Différentes techniques 1/2

- Pièces jointes contaminées :

- Exécutable
- Script
- Pdf
- Image
- .doc, .xls, (VBscript)...



- Dans le corps du message :

- Javascript
- Image : `<img src='http://site_pirate.com/tracker.php'>`

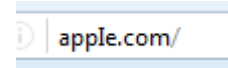
Sujet: **\*\*TEST\*\*** pour d.perard  
Expéditeur: [test@isae.fr](mailto:test@isae.fr)  
Date: Jeudi, Juin 08, 2017 14:50 CEST  
Destinataire: [doriane.perard@isae.fr](mailto:doriane.perard@isae.fr)  
Répondre à: [test@isae.fr](mailto:test@isae.fr)

Télécharger les images

# Différentes techniques 2/2

- Lien vers un faux site d'authentification :

- Obfuscation de l'url : apple.com



- DNS poisoning

- Certificats gratuits avec Let's encrypt

- Redirection et rebond

- Redirection : `<meta http-equiv=«refresh» content=«0;url=site_pirate.com»/>`

- Dyn-DNS

- Script externe, web-bug

- Arnaque au président



# Actualités 1/6

- Ransomware :
  - 81% via phishing
  - CTB-Locker [2014]
  - TeslaCrypt [2015]
  - Locky via un document word, Cerber, CrptXXX, ... [2016]
  - Jaff depuis le 11 mai 2017 via un document pdf (bulletin du certFr en cours)



# Actualités 2/6

- Elections :
  - françaises [avril 2017]
  - américaines [2016]

From: Google <[no-reply@accounts.googlemail.com](mailto:no-reply@accounts.googlemail.com)>  
Date: March 19, 2016 at 4:34:30 AM EDT  
To: [\[REDACTED\]@gmail.com](mailto: [REDACTED]@gmail.com)  
Subject: Someone has your password

Google



## Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account [\[REDACTED\]@gmail.com](mailto: [REDACTED]@gmail.com).

Details:

Saturday, 19 March, 8:34:30 UTC  
IP Address: 134.249.139.239  
Location: Ukraine

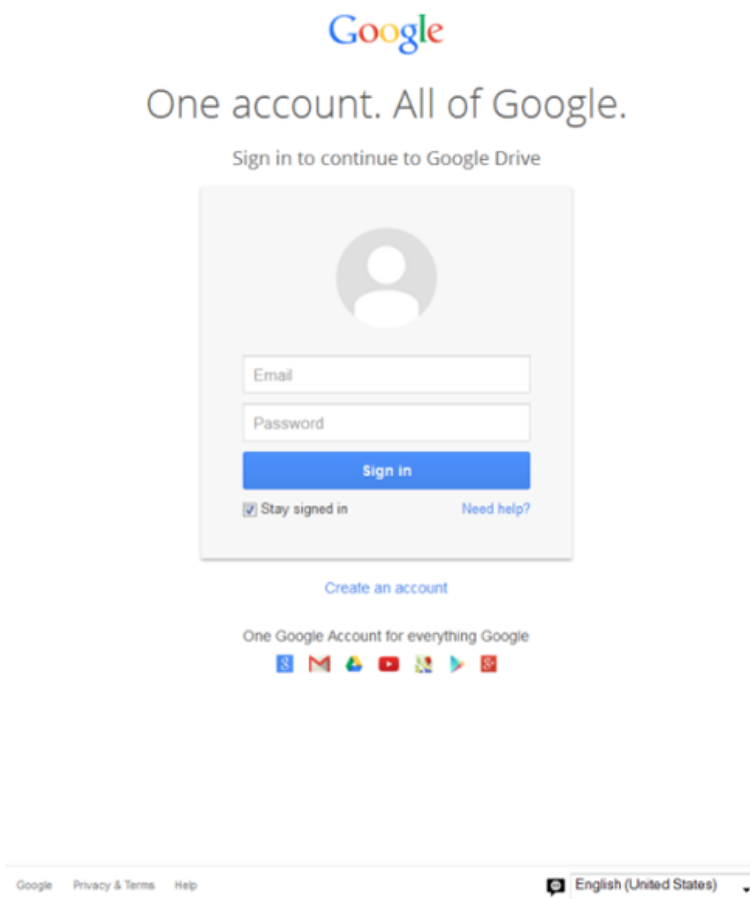
Google stopped this sign-in attempt. You should change your password immediately.

[CHANGE PASSWORD](#)

Best,  
The Gmail Team

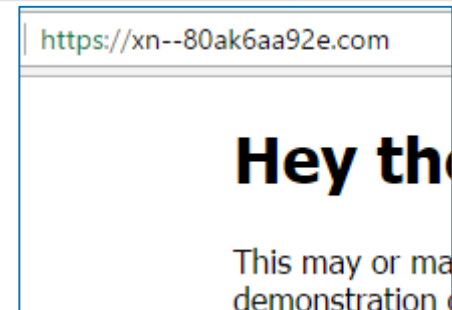
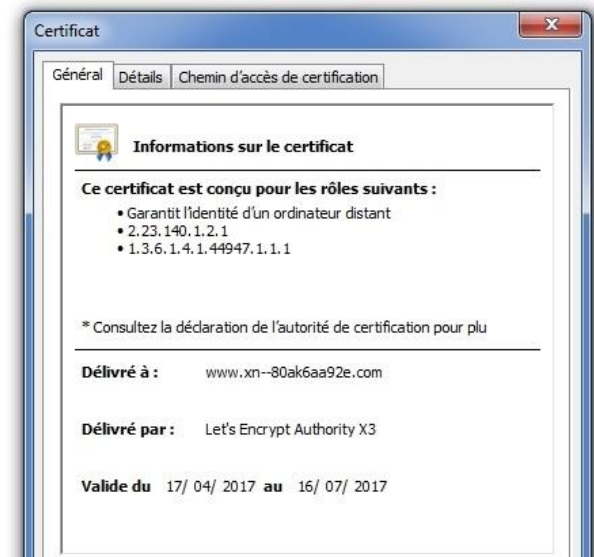
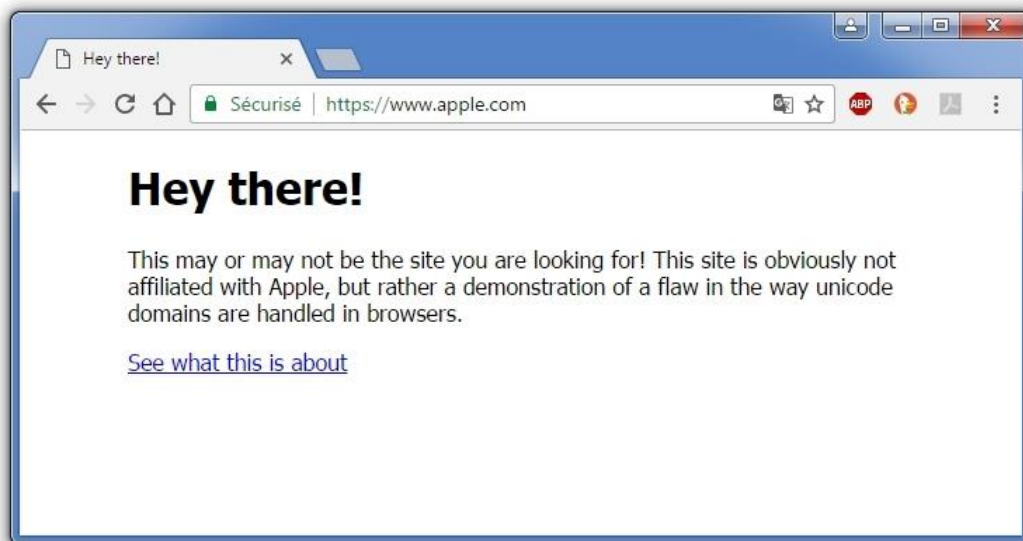
# Actualités 3/6

- Gmail et Google Docs [mai 2017]



# Actualités 4/6

- Pièces jointes contaminées (Word et zéro-day) [avril 2017]
  - Utilisées depuis janvier 2017
- Lien avec caractères en cyrillique



# Actualités 5/6

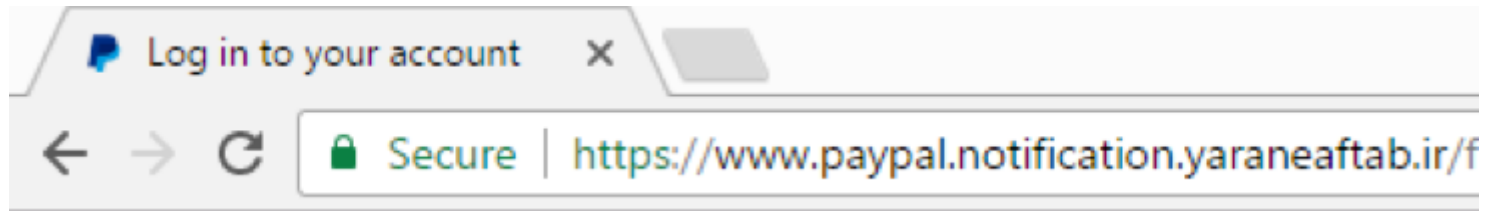
- Atteinte à l'image de marque : Vinci [novembre 2016]
  - Vinci.group
  - Chute de 18,3% du cours de l'action = 6,7 milliards d'euros





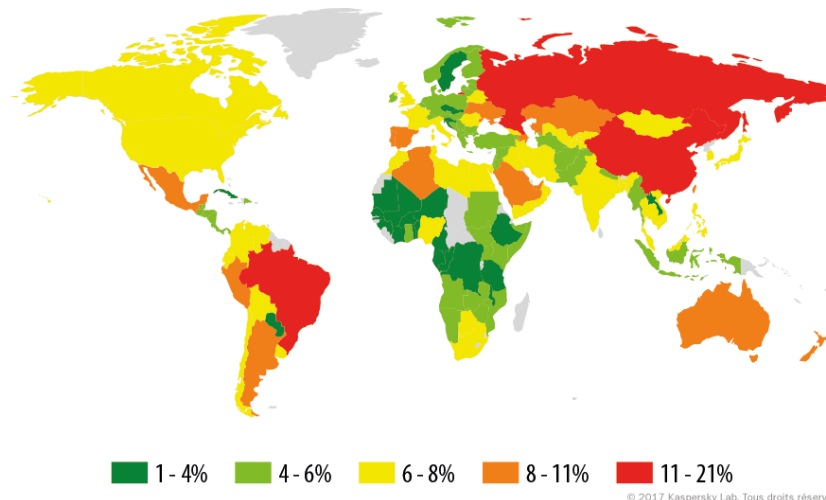
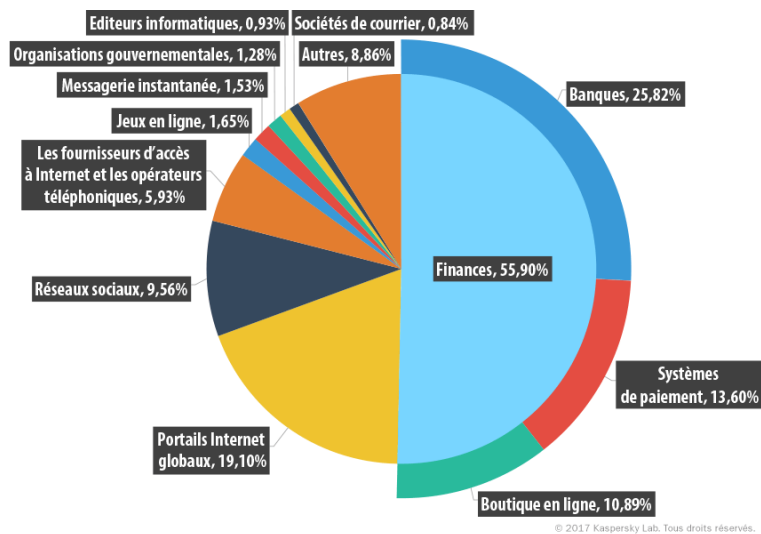
# Actualités 6/6

- Let's encrypt : nécessité de certificats Extended Validation
  - Fournit gratuitement des certificats Domain Validation
  - En mars 2017 : 15,000 certificats pour du phishing Paypal



# Chiffres clés du phishing

- 51 millions d'attaques empêchées par Kaspersky au 1<sup>er</sup> 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).

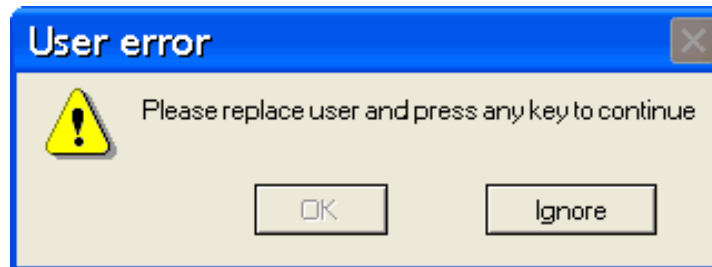
En cas de doute, n'hésitez pas à solliciter le centre de services du SI.

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



# Réponse

- Le problème se situant entre le clavier et la chaise, il convient d'éduquer et de sensibiliser les utilisateurs



# Contexte local : ISAE

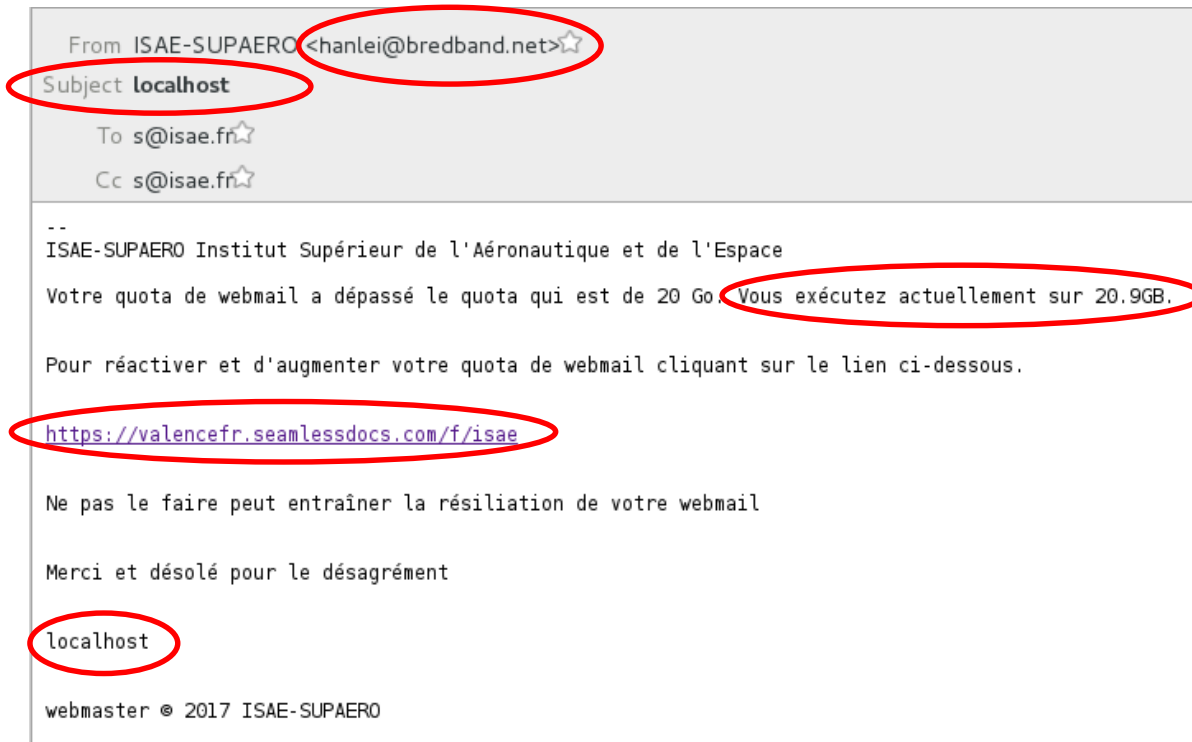
- Site sous tutelle du ministère de la Défense : informations sensibles
- Environ 3 000 utilisateurs
- Par jour :
  - 44 000 e-mails envoyés
  - 27 000 e-mails reçus
- Unicité du mot de passe pour les différents services

# Antécédents

- **Novembre 2016 :**
  - Téléchargement d'une pièce jointe malveillante
  - Ransomware
  - Chiffrement de la machine et de tout le partage réseau du service concerné
- **Conséquences :**
  - 1 semaine de perturbations dans le service sans accès aux données partagées
  - 2 personnes du SI pour rétablir les sauvegardes et désinfections des postes

# Depuis avril 2017

- Plusieurs nouvelles attaques repérées
- Une en particulier :



# Depuis avril 2017

- Plusieurs nouvelles attaques repérées
- Une en particulier :
  - Envoi rapide d'e-mails d'alertes, puis blocage de l'url sur le proxy
  - 20 clics depuis le réseau de l'école
  - 5 personnes (au moins) ont rentré leurs identifiants dont des chercheurs en informatique
  - Blocage de tous les comptes potentiellement affectés

**Depuis** : beaucoup de gens demandent conseils au RSSI concernant des e-mails douteux (dont certains déjà tagués spam)



# 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

# Modifications de l'outil 1/3

- Diversification des types de phishing : E-mail avec
  - Lien vers un faux portail d'authentification



## Central Authentication Service (CAS).

Entrez votre identifiant et votre mot de passe :

Identifiant :


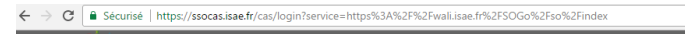
Mot de passe :

Prévenez-moi avant d'accéder à d'autres services.

Pour des raisons de sécurité, veuillez vous déconnecter et fermer votre navigateur lorsque vous avez fini d'accéder aux services authentifiés.  
En cas de question ou problème, contactez le [centre de service SI](#).

Copyright © 2005 - 2010 Jasig, Inc. All rights reserved.

Powered by [Jasig Central Authentication Service 3.4.7](#)



Entrez votre identifiant et votre mot de passe.

Identifiant:

Mot de passe:

Événuez-moi avant d'accéder à d'autres services.

Pour des raisons de sécurité, veuillez vous déconnecter et fermer votre navigateur lorsque vous avez fini d'accéder aux services authentifiés.

En cas de question ou problème, contactez le [centre de service SI](#).

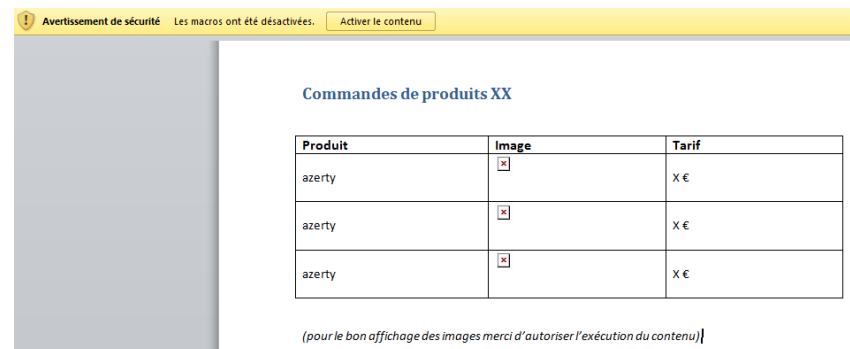
Languages: [English](#) | [Spanish](#) | [French](#) | [Russian](#) | [Nederlands](#) | [Svenski](#) | [Italiano](#) | [Urdu](#) | [Chinese](#)

# Modifications de l'outil 2/3

- Diversification des types de phishing : E-mail avec
  - Une « image » dans le corps faisant appel à un script php



- Une pièce jointe malveillante



# Modifications de l'outil 3/3

- Collecte de résultats : base de données
  - Adresse IP
  - User agent
  - Identifiant
  - Mot de passe rempli (booléen : vrai/faux)

# Campagne de sensibilisation

- Page d'hygiène de l'informatique sur l'intranet : guide de bonnes pratiques de l'informatique accessible à tous
  - Exemple des guides de l'ANSSI
- Vidéos explicatives du phishing
- Présentations en amphi et en réunions de départements aux règles d'hygiène globales
- Quizz en ligne pour situer son niveau
- Wall of spam

# 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

# Futur du projet

- Chaque début d'année sur les nouveaux arrivants
- Rappels réguliers pour les anciens
- Rendre le projet open-source ?
- Diversifier les types de campagnes (ex : téléphone)

- Merci

