OSSIR : Education au Phishing

Fabrice Prigent

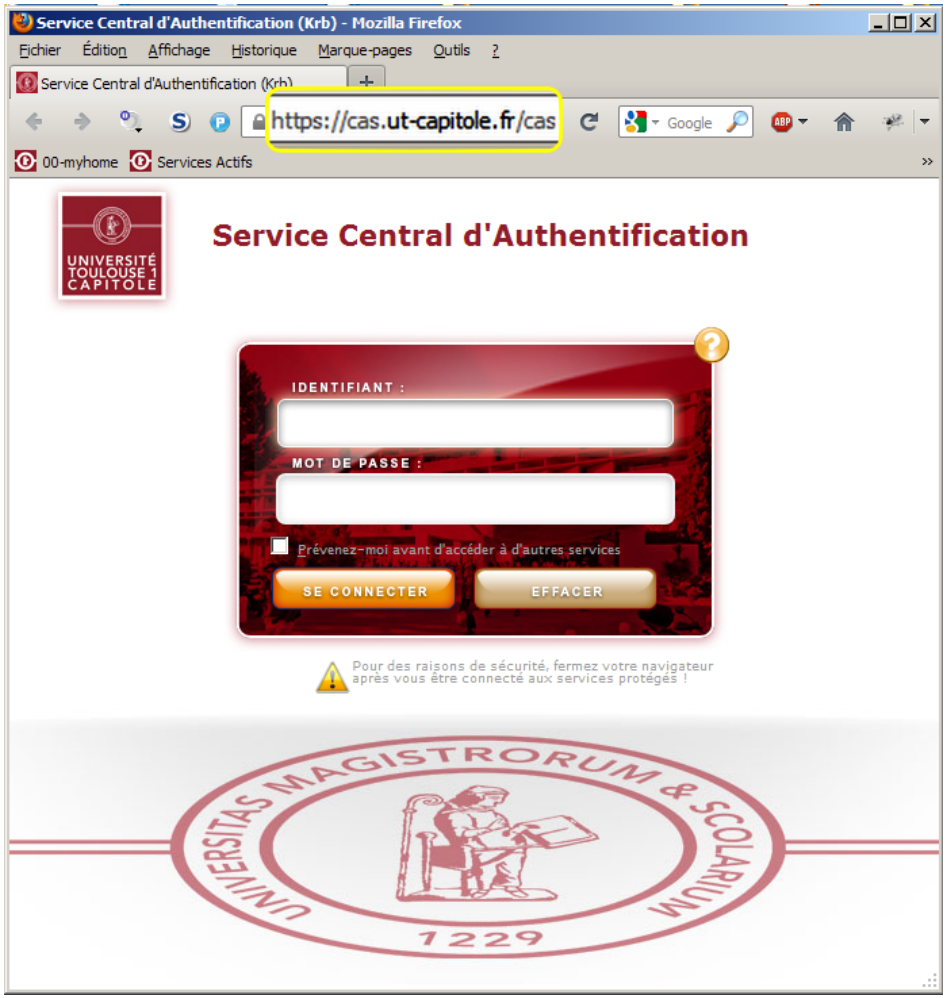
Université Toulouse 1 Capitole

Mardi 12 Février 2013

L'université Toulouse 1 Capitole

- Université en droit, économie et gestion, avec une petite UFR informatique,
- 21000 étudiants,
- 2100 personnels (dont 1000 vacataires),
- très forte centralisation (2 entités semi-indépendantes),
- une seule adresse officielle,
- un annuaire avec les mails des personnels,
- une unicité du mot de passe,
- une quasi-unicité de l'authentification web (CAS)

Notre CAS


Service Central d'Authentification (Krb) - Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
Service Central d'Authentification (Krb)
https://cas.ut-capitole.fr/cas
Google
00-myhome
Services Actifs
UNIVERSITÉ TOULOUSE 1 CAPITOLE
Service Central d'Authentification
IDENTIFIANT :
MOT DE PASSE :
Prévenez-moi avant d'accéder à d'autres services
SE CONNECTER
EFFACER
Pour des raisons de sécurité, fermez votre navigateur après vous être connecté aux services protégés !
UNIVERSITAS MAGISTRORUM & SCOLARIUM
1229

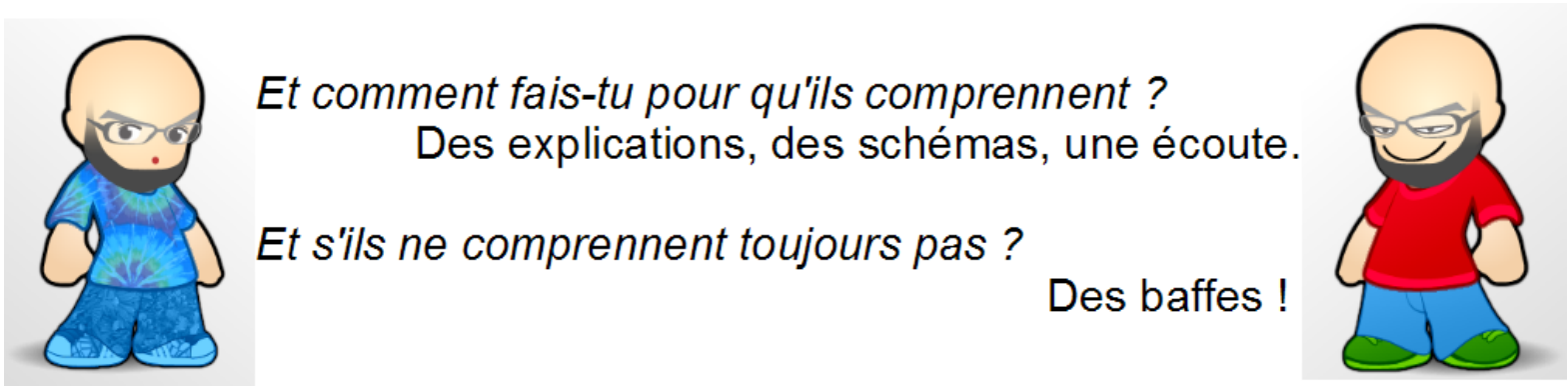
UT1 : les comportements

- Les étudiants lisent peu leur mail institutionnel :
  - 20% le lisent par le webmail, ou en salles informatiques,
  - 30% le redirigent sur leur adresse personnelle,
  - 50% laissent mourir leur mail.
- Les personnels ont un comportement variable :
  - 50% le lisent directement,
  - 40% le redirigent sur leur adresse personnelle,
  - 10% laissent mourir leur mail.
- Des membres globalement peu contestataires

La situation en novembre 2011

- Aucun compte étudiant "phishé" en 3 ans :
  - mail non référencé,
  - mail peu lu.
- 3 à 5 campagnes de phishing par jour
- 3 à 6 phishing réussis par an
- Et ceci malgré :
  - des bulletins,
  - des rappels en réunion des chefs de service,
  - des messages web.

Pédagogie


Et comment fais-tu pour qu'ils comprennent ?
Des explications, des schémas, une écoute.
Et s'ils ne comprennent toujours pas ?
Des baffes !

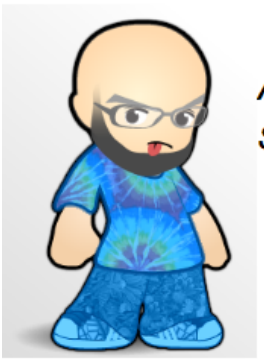
Phase 1 : la victime de trop

Après une 3ème victime de l'année universitaire (fin octobre 2011), une évaluation est mise en place.

- Nous créons univ-tty.tk (qui pointe chez nous).
- Nous décidons de "tester" 75 personnes :
  - sans le moindre avertissement,
  - un mail sans le moindre rapport avec l'UT1,
  - un site web de phishing.

Phase 1 : résultats

- 25 personnes répondent avec leurs identifiants (33%),
- La DSI bloque "in extremis" le "pirate", (effet Superman)
- Nous recommandons aux personnes de changer leur mot de passe.



A ce que l'on dit le RSSI s'est jeté par la fenêtre de son bureau quand il a vu les résultats !

Du rez- de chaussée, c'est malin.

Phase 2 : première campagne pédagogique

Avec l'accord de la DGS, une campagne pédagogique à destination du personnel est lancée.

- On avertit, par mail, le jeudi 3 novembre 2011 et on rappelle :
  - la physionomie du CAS,
  - la définition du phishing,
  - l'arrivée de la future campagne,
  - la manière de se prémunir.
- La campagne est prévue pour le 10 novembre, pouvant être décalée plus tard.

Objectifs

Nous avions un objectif clair :

Améliorer

Améliorer la résistance de l'ensemble de la communauté UT1 aux phishing actuellement en activité.

et non de

- faire une expérimentation,
- garantir une résistance à un phishing ciblé : on connait le résultat :-(
- s'occuper des phishing "pur mail" (A réévaluer)

Phase 2 : campagne pédagogique

Moi, quand on m'en fait trop, j'correctionne plus, j'dynamite, j'disperse, j'ventile.

Phase 2 : le phishing de trop

Pas de chance, le 4 novembre, une vraie campagne a lieu et piège un utilisateur :

- samedi 5 novembre à 11h09 : un spammeur, en Afrique, utilise le compte,
- samedi 5 novembre à 20h20 : le problème est détecté par hasard,
- samedi 5 novembre à 23h00 : le problème est contenu,
- 241 188 destinataires étaient visés,
- 70 944 spams ont été envoyés avant d'être bloqués,
- au moins 3 blacklists nous ont référencés :
  - une locale chez Yahoo,
  - une locale Hotmail,
  - la blacklist LASHBACK.

Phase 2 : le phishing de trop

Les méthodes de "confinement" habituelles ont échoué :

- à chaque blocage d'IP un changement d'adresse :
  - 24 adresses IP différentes
    - dont la majorité en Afrique (4 FAI),
    - certaines aux USA,
    - quelques unes en France,
    - une à Istanbul,
- une utilisation très progressive de nouveaux expéditeurs.

Phase 2 : j'disperse, j'ventile

- La campagne pédagogique est lancée le dimanche 6 novembre à 8h05 du matin.
- Le mail et le site n'ont rien à voir avec notre site web.
- Le mail est en français correct.
- 2366 mails sont envoyés.

Phase 2 : les résultats

- 632 personnes ont consulté la page de phishing.
- 70 personnes se sont faites piéger.
- Aucune des 25 personnes précédemment piégées ne l'a été cette fois-ci.
- Beaucoup d'appels arrivent au service informatique (avant de tomber dans le piège ou après y être tombé) :
  - une trentaine de mails,
  - une vingtaine d'appels,
  - une dizaine d'interceptions dans le couloir,
  - puis, vers 10h30 tout s'est calmé.

Phase 2 : explications

- Ce qui facilite le phishing :
  - l'absence de fautes d'orthographe (très important !),
  - l'adresse d'expédition (service.informatique@univ-tlse1.fr).
- Ce qui protège du phishing :
  - la date d'expédition par le service informatique : "les informaticiens ne travaillent pas le dimanche",
  - le bouche à oreille des collègues piégés,
  - le côté massif de l'envoi,
  - dans une faible mesure, le bulletin,
  - la lecture du mail par un webmail (déport du lien).

Phase 3 : campagne permanente

- Il est décidé de mettre en place une campagne quotidienne :
  - 20 personnes tirées aléatoirement chaque jour,
  - une campagne renouvelée tous les 3 mois (nouveau message, nouveau site).

Phase 3 : Campagne 1

Saturation de votre espace disque

Nous vous rappelons les consignes pour votre messagerie :

- Nettoyer les spams
- Effacer les mails de blagues (powerpoint et autres) qui prennent **beaucoup** de place.
- Vider régulièrement votre corbeille
- Hormis cas exceptionnel, les mails de plus de 1 an ne servent à rien

login :
Mot de passe :
Valider Effacer

Phase 3 : résultats des 2 premiers jours

- 154 personnes ont été ciblées (un départ un peu rapide....).
- 13 personnes sont tombées dans le piège dont certains avec des comptes extérieurs à l'université (FAI, autre université toulousaine, etc.).
- 4 de ces personnes avaient déjà été piégées par la première campagne.

Phase 3 : premières conclusions

- Les communications institutionnelles ne sont pas lues.
- Les explications ne sont utiles qu'à des utilisateurs technophiles.
- Certaines personnes, indépendamment de leurs diplômes, sont hermétiques à la compréhension de l'informatique.

J'ai reçu un mail d'eBay me demandant mes coordonnées, alors que je n'ai pas de compte eBay. C'est pour cela que j'ai mis mon mot de passe de la fac.
J'ai bien fait ?

- La pédagogie par l'exemple semble malgré tout efficace pour un très grand nombre de personnes.

Phase 3 : campagne 2

Phase 3 : campagne 3

Phase 3 : campagne 4

Phase 3 : résultats sur 12 mois

Les résultats sont très encourageants :

- 4 campagnes,
- 1 seul vrai phishing réussi au lieu des 3-6 habituels.

Phase 3 : conclusions

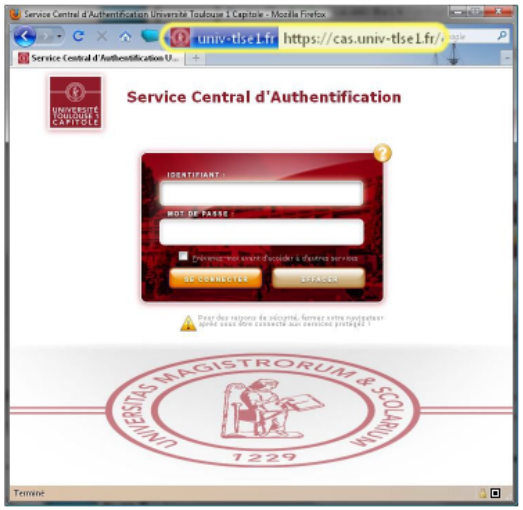
- Un personnel obéissant est un personnel piégeable.
- Se faire avoir est une petite vexation, attention à ne pas tomber dans l'humiliation.
- Il est nécessaire de simplifier les consignes de détection :
  - la forme et l'url sont suffisantes dans notre environnement,
  - le mail ne fait même pas partie des critères de détection.
- Les personnes sont plus attentives si leur vie privée est en jeu (téléphone)
- Il faut expliquer CLAIREMENT pourquoi elles ont été piégées par la DSI.

Phase 3 : les explications

Vous venez de vous faire piéger

Et par chance, ce n'est pas par un pirate

Vous avez fourni votre mot de passe à une page web qui ne ressemble en rien à ceci :



Vous l'avez fait alors que l'adresse internet indiquée plus haut dans votre navigateur web est **http://www.univ-tty.tk/admin** (université TTY dans l'archipel de Tokelau ???) et non **https://cas.univ-tlse1.fr** (regardez la zone entourée de jaune dans l'image ci-dessus).
Il est acceptable de cliquer sur des liens dans les mails, **mais** vous devez **vérifier** que l'adresse web de la page correspond à ce que vous attendez et ce **même si**

- le mail vient de Bruno Sire, Fabrice Prigent, l'élysée, la CIA, le Pape ou le Père Noël
- le fait de ne pas obéir va faire tomber une météorite, noyer vos poissons rouges, vous faire pousser des oreilles de lapin
- c'est urgentissime, toutdesuitesque, sanslemoindretoutpetitdelaideriendutout
- c'est sous la menace d'une commission rogatoire ou d'une condamnation à manger 2 kilos de haribo par jour pendant 30 ans

Le service informatique d'UT1

Novembre 2012

Pour prouver son immense compétence et sa fantastique découverte, l'extraordinaire, le magnifique, l'incroyable, l'irrésistible RSSI de l'UT1 va refaire pour vous, et rien que pour vous l'expérience, et cette fois ci sans filet.

Conditions

Afin de préparer convenablement une présentation aux JRSSI (pas les JSSI ;-)), l'expérience suivante est menée :

- les mails ne sont envoyés QUE pendant les heures ouvrées,
- on ne cible que par petits groupes,
- le style de campagne est identique : "saturation de quota",
- l'avertissement reste classique (un bulletin à tout le monde),
- au cas où quelques malheureux se feraient avoir, on récupère leur catégorie professionnelle.

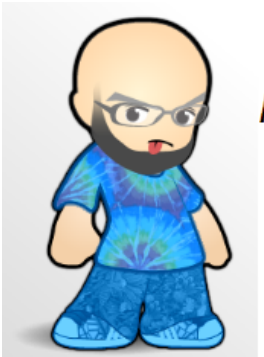
Résultat

Et le résultat est :

22% de piégés

soit :

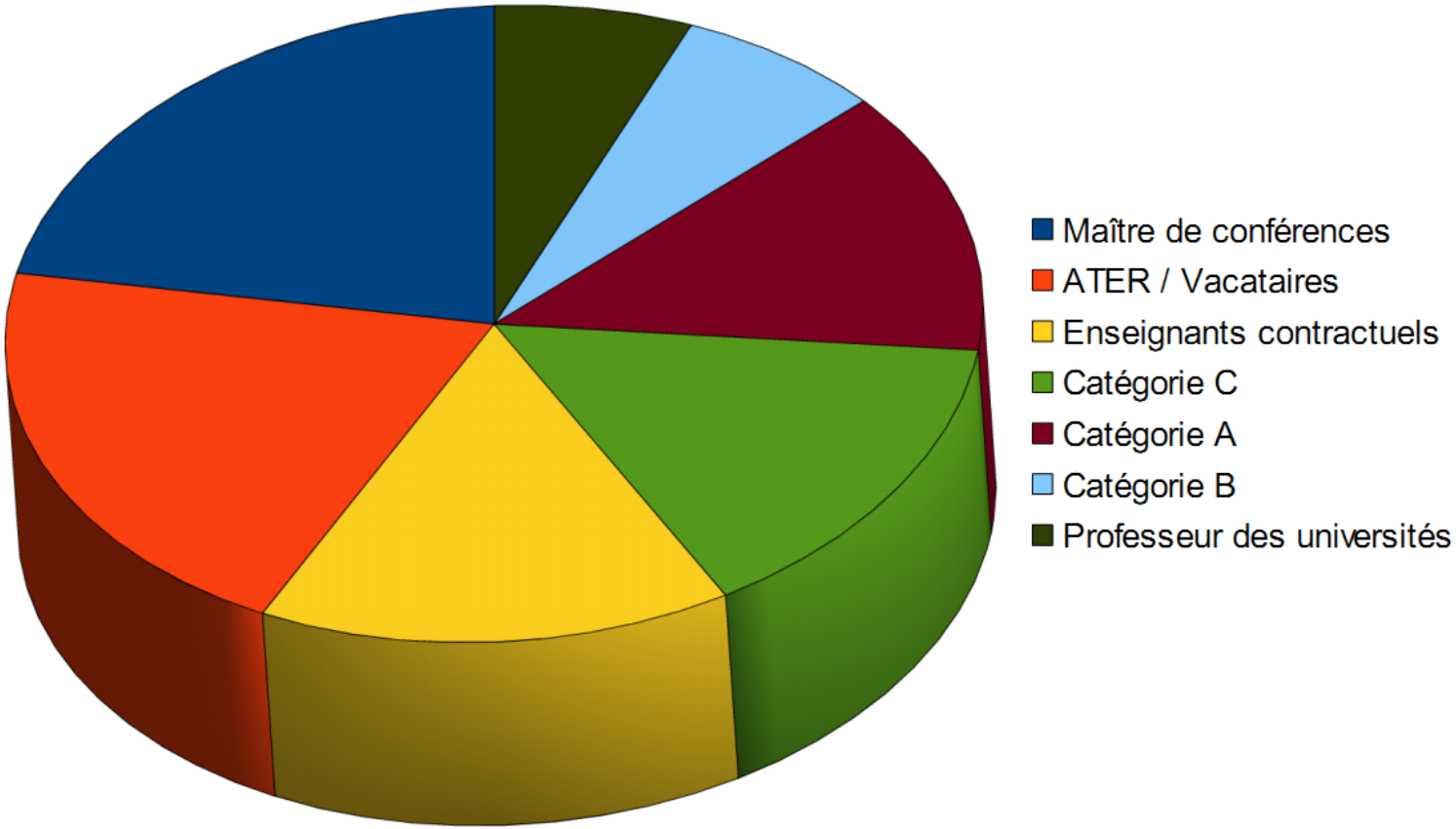
422 personnes



Il veut se suicider au gaz le RSSI ?

Avec la tête dans le four micro-ondes ? Original !

Qui sont-ils ?


Maître de conférences
ATER / Vacataires
Enseignants contractuels
Catégorie C
Catégorie A
Catégorie B
Professeur des universités

Est-ce un échec ?

Doit-on considérer que c'est un échec de l'éducation ? Vérifions :

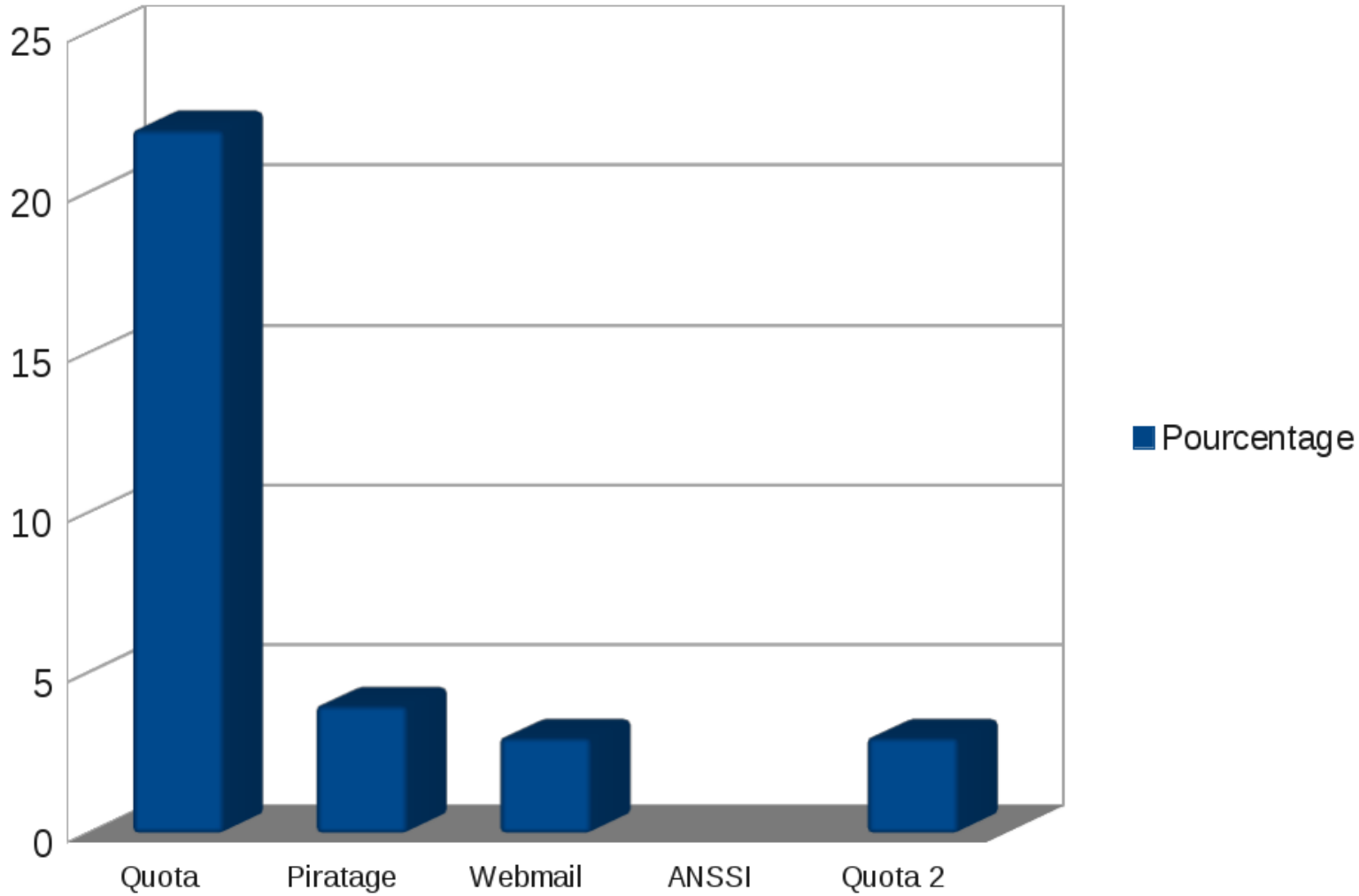
- un nouveau phishing "compte piraté",
- uniquement sur les piégés.

Est-ce un échec ?

C'est une réussite :

- 6 sont dans le "je me suis pas fait avoir et je te le fais savoir".
- 5 se font piéger (sur 422 !) :
  - 1 directeur de composante,
  - 2 personnels catégorie C,
  - 1 enseignant,
  - 1 vacataire.
- Une quarantaine de personnes contactent la DSI.

Et depuis ?


25
20
15
10
5
0
Quota
Piratage
Webmail
ANSSI
Quota 2
Pourcentage

Conclusion

- La pédagogie par la pratique marche :
  - si vous avez un objectif clair (entrainer et non piéger),
  - si vous êtes en condition favorable (heures ouvrées, site "crédible"),
  - si le contexte est clair (explications, prévention, avertissement).
- Mais comme les vaccins, il faut des rappels, tous les 3 mois au minimum.
- Il ne faut faire aucun postulat sur les futures victimes, elles sont parfois TRES gradées...
- Ne pas se faire avoir à UNE campagne, ne signifie pas que l'on résistera aux autres.

Conclusion

On se dit que l'on est sur la bonne voie quand on entend cela :