SYNACKTIV
DIGITAL SECURITY

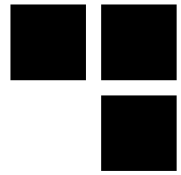
Techniques et outils pour la compromission des postes clients

Présenté le 7 avril 2016

Conférence GS Days

Par Renaud Feil et Clément Berthaux

Introduction



- **Synacktiv**
  - Expertise en sécurité offensive depuis 2012
  - Red Team, recherche de vulnérabilités,…
  - 15 experts sécurité
- **Renaud Feil & Clément Berthaux**
- **Agenda**
  - Menaces, techniques et outils
  - Démonstration de l'outil Oursin
  - Protections techniques et sensibilisation des utilisateurs

Spear-phishing

- **Le spear-phishing, c'est quoi ?**
  - Harponnage en français
  - Version ciblée du phishing
  - Charges malveillantes
    (exploits, documents piégés)

Une menace significative

- **+ 18% d'attaques en Europe au Q3 2015**

  (https://securelist.com/analysis/quarterly-spam-reports/72724/spam-and-phishing-in-q3-2015/)

- **Utilisé dans 91 % des APT**

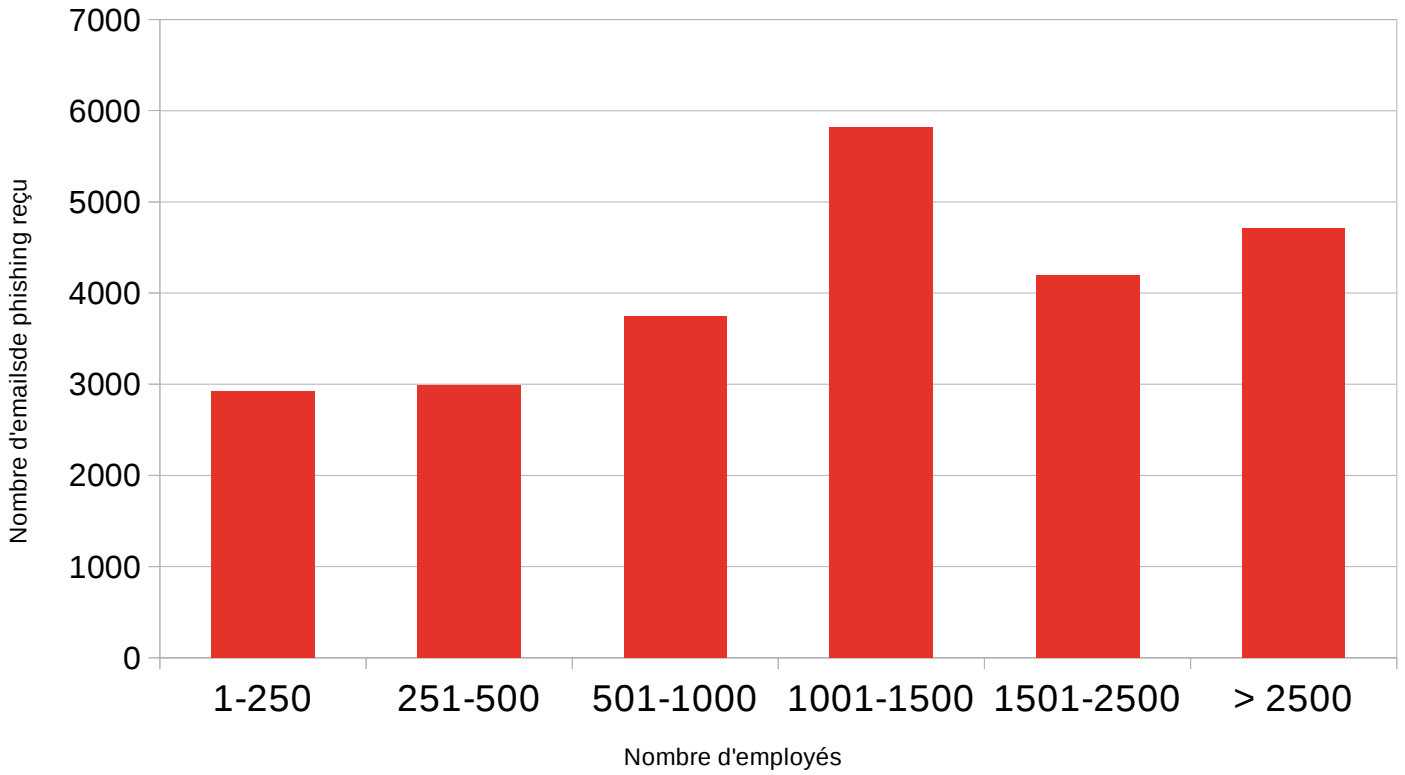
  (http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf)

- **Coût annuel moyen pour une entreprise de 10 000 employés : 3.7 millions USD**

  (http://www.csoonline.com/article/2975807/cyber-attacks-espionage/phishing-is-a-37-million-annual-cost-for-average-large-company.html)

Les organisations ciblées

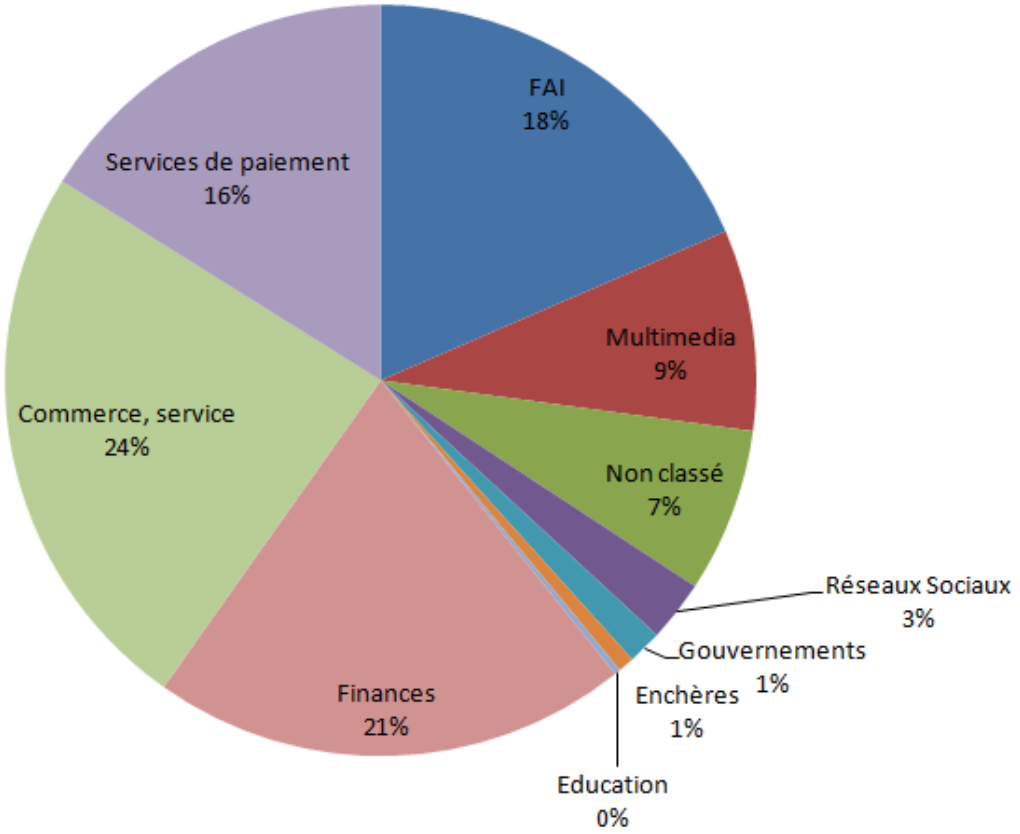
- **Taille de l'entreprise**



Statistiques février 2016 par Symantec
https://www.symantec.com/security_response/publications/monthlythreatreport.jsp#Phishing

Les organisations ciblées

- **Secteur d'activité**



Statistiques pour le Q4 2015 par le APWG
http://docs.apwg.org/reports/apwg_trends_report_q4_2015.pdf

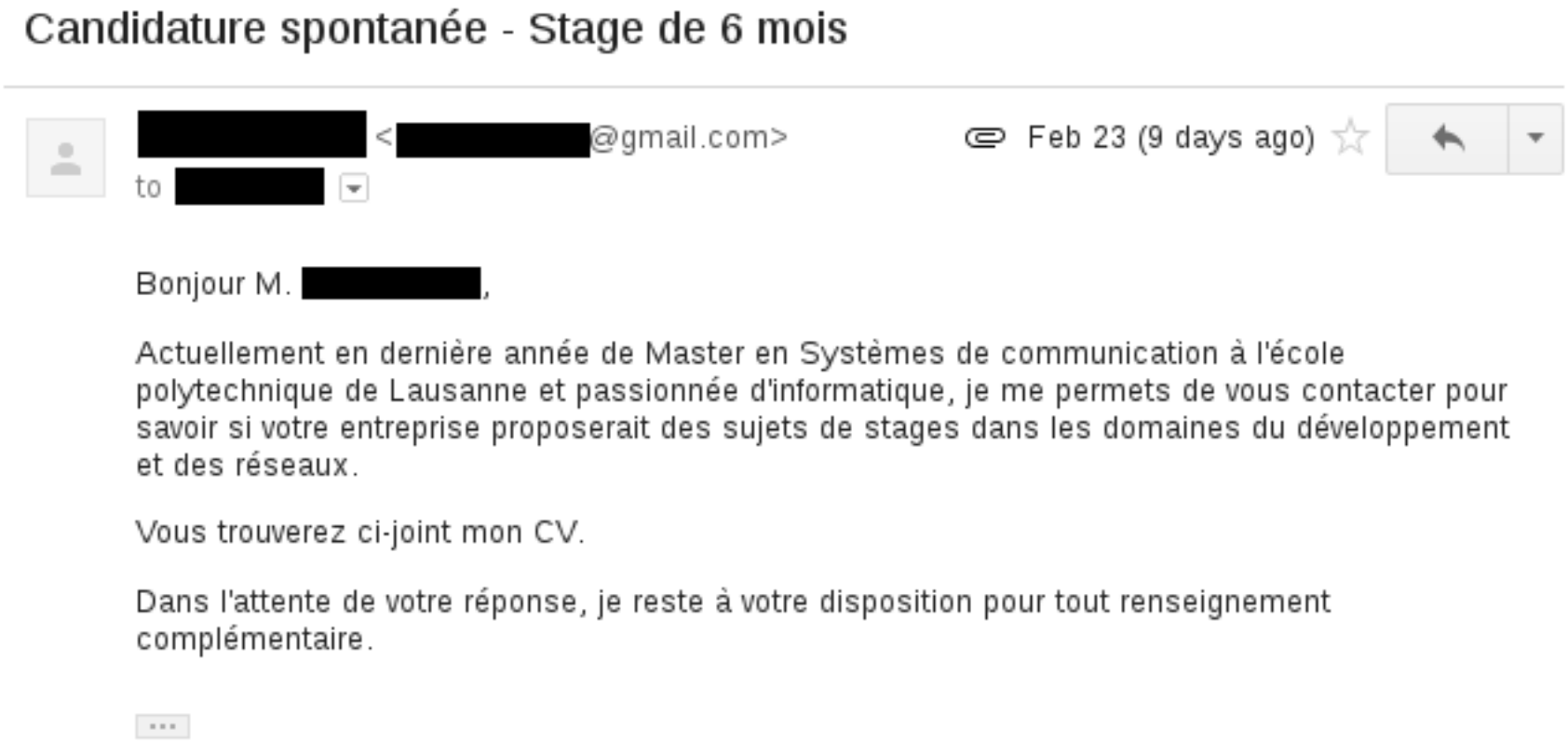
Le « prix du marché »

Le spear-phishing facile

- **Phases**
  - Recherche d'informations sur les employés
  - Préparation des scénarios
  - Envoi des e-mails
  - Attente...
  - Get shellz !
  - Compromission du réseau interne

Un exemple de scénario

- **Etudiant(e) cherchant un stage**



Candidature spontanée - Stage de 6 mois

[redacted] <[redacted]@gmail.com> Feb 23 (9 days ago)

to [redacted]

Bonjour M. [redacted],

Actuellement en dernière année de Master en Systèmes de communication à l'école polytechnique de Lausanne et passionnée d'informatique, je me permets de vous contacter pour savoir si votre entreprise proposerait des sujets de stages dans les domaines du développement et des réseaux.

Vous trouverez ci-joint mon CV.

Dans l'attente de votre réponse, je reste à votre disposition pour tout renseignement complémentaire.

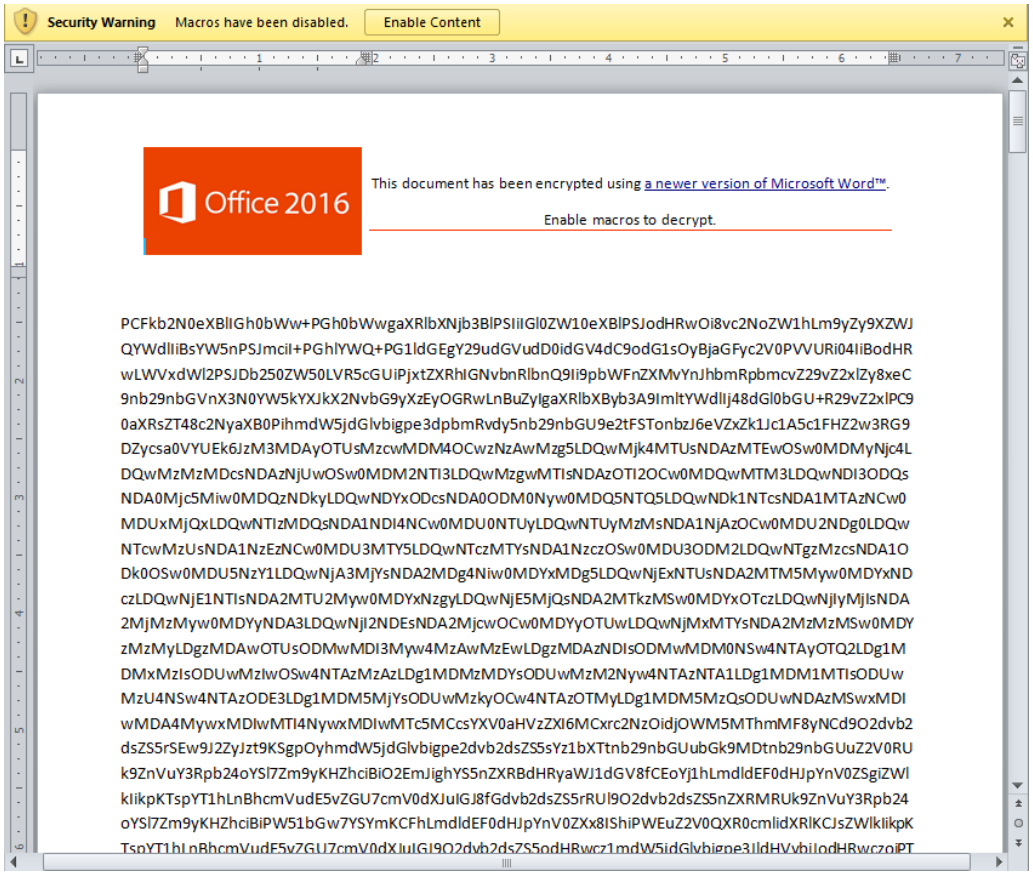
...

Les charges utiles : exploits

- **Différents vecteurs d'exploitation**
  - Navigateurs (aussi appelés brouteurs)
  - Plugins (Flash, Silverlight, Java)
  - Clients mail (MS Outlook, Apple Mail)
  - Suites bureautique (Word, LibreOffice)
- **Avantages**
  - Pas d'avertissements de sécurité
- **Inconvénients**
  - Nombre de cibles limité pour les vulnérabilités publiques
  - Mesures de protection (bac à sable)
  - Développement et fiabilisation coûteux

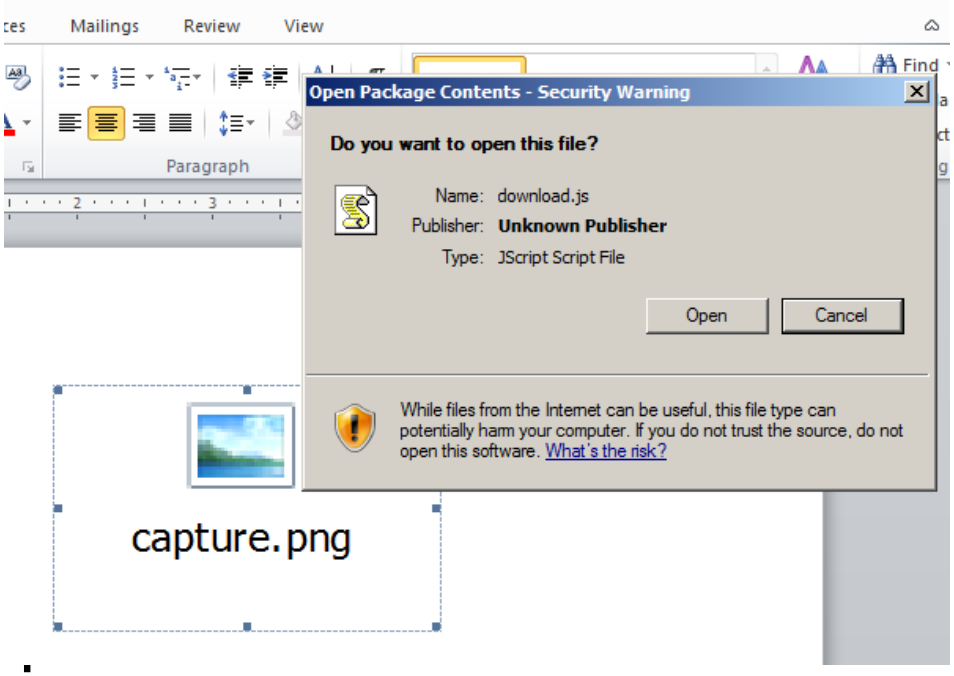
Les charges utiles : Macro Office

- **Old but gold !**
- **Avantages**
  - RCE as a feature
  - Office installé presque partout
  - Faible taux de détection
- **Inconvénients**
  - Action utilisateur requise
  - Parfois désactivées



Les charges utiles : objet lié

- **Embarquer un objet dans un conteneur OLE**
  - Exécutable
  - Script (VBS, JS)
  - Exploit
- **Avantages**
  - Faible taux de détection
- **Inconvénients**
  - Interaction utilisateur requise



Les charges utiles : exécutable

- **Envoi direct du .exe**
- **Avantages**
  - Fiable
- **Inconvénients**
  - Extension souvent bloquée
  - Détection par les AV (réputation)
  - Interaction utilisateur

Le phishing facile : Démo

Retour d'expérience

- **Le spear-phishing à Synacktiv en 2015**
  - 19 missions
  - Plus de 280 e-mails malveillants envoyés
  - Plus de réussites que d'échecs (**environ 90% de réussites, provoquant la compromission du réseau interne**)
- **Les facteurs clés**
  - Taille de l'entreprise
  - Présence de mesures de protection techniques
  - Niveau de sensibilisation des équipes

Hall of fame

- **La plupart du temps les cibles ne s'inquiètent pas…**

Bonjour [redacted],

Nous n'avons pas su ouvrir ton CV.
Peux-tu me renvoyer ton CV je le transmettrai aux RH.

Bonne journée,

Bonjour

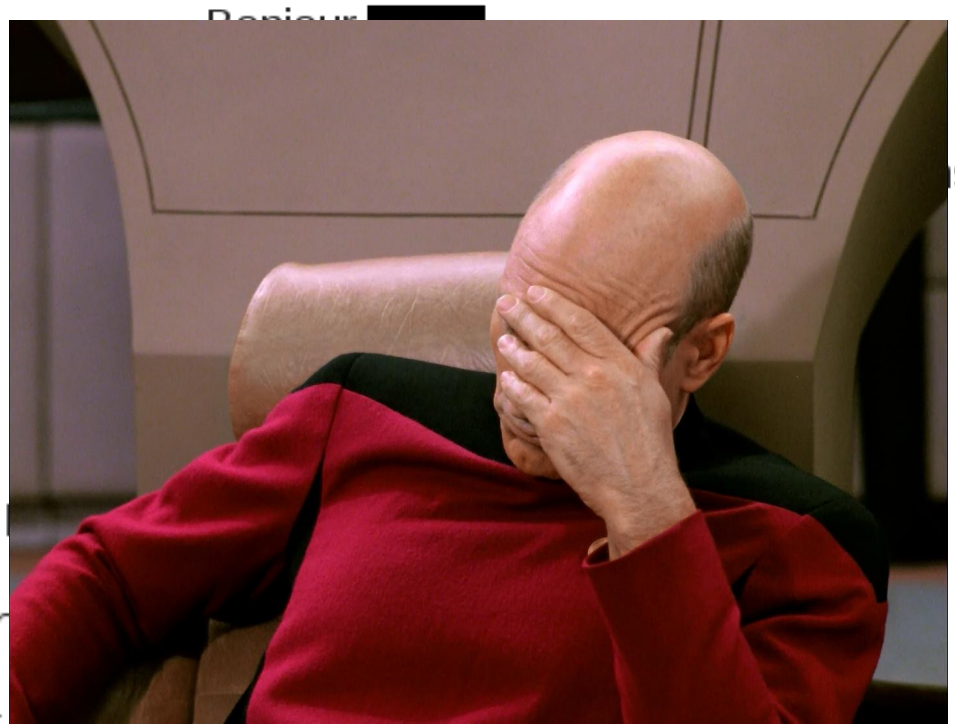
Même en activant les macros, je n'arrive pas à lire votre CV.

Merci de me le renvoyer.

Bien cordialement,

Hall of fame

- **La plupart du temps les cibles ne s'inquiètent pas…**



Bonjour

Même en activant l

Merci de me le ren

Bien cordialement,

smettrai aux RH.

Hall of fame

- **… ou nous prennent pour des incompétents**

bonjour,

suite à votre message à [redacted], je vous informe que je suis dans l'impossibilité d'ouvrir votre CV.

Je vous fais les remarques ci-dessous, afin de vous aider dans votre recherche :
- soit votre CV ne peut pas s'ouvrir et cela donne une mauvaise image de vos compétences
- soit votre CV peut s'ouvrir et c'est moi qui suis trop "bête" pour l'ouvrir ce qui renvoie une image négative à mon propre égo et ne m'encourage pas à vous recevoir.

Hall of fame

- **… ou nous prennent pour des incompétents**

bonjour,

suite à votre r ossibilité
d'ouvrir votre

Je vous fais le ne :
- soit votre CV compétences
- soit votre CV renvoie une
image négativ

Se protéger contre le spear-phishing

- **Pas facile**
- **Mesures techniques**
  - IDS, IPS
  - Équipements révolutionnaires, big data dans le nuage et sandboxes
  - Durcissement de configuration
- **Sensibilisation**
  - Campagnes de tests fréquentes

Anti-virus

- **Fonctionnalités intéressantes**
  - Mécanismes de réputation des exécutables
  - Détection de sorties d'outils d'attaque connus (non, nous ne mentionnerons pas Mimikatz)
- **Efficacité dépend de la configuration**

Peut freiner un attaquant et générer des alertes cruciales pour la Blue Team

Durcissement des configurations

- **Exécution des macros Office**
  - Entièrement désactivées
  - Signer les macros internes, et seulement autoriser les macros d'entités de confiance
- **Filtrage des exécutables avec Applocker**
  - Plusieurs modes : liste blanche, noire, par éditeur, par chemin
  - Powershell ? Macro Office ? Bypass AppLocker (cf conférence de ce matin par Damien)

Peut freiner un attaquant, l'obligeant à envoyer plus d'e-mails pour compromettre un poste client (et risquer de se faire détecter)

En parlant d'Applocker…

- **Réponse de MS**

Hello,

Thank you for contacting the Microsoft Security Response Center (MSRC). AppLocker is not a security boundary and we do not currently service issues related to it.

Again, we appreciate your report.

Regards,

Jonathan
MSRC

Sensibilisation

- **Le but : entraîner les cibles potentielles**
  - Répérer les e-mails potentiellement malveillants
  - Connaître les actions dangereuses
- **Pas seulement une présentation sur les DO and DON'T**
- **Des campagnes de tests fréquentes**
- **De nombreux services existent dans ce but**

Oursin

- **Plate-forme d'automatisation pour les tests de spear-phishing**
- **Alternative non-intrusive de l'outil utilisé lors des tests Red Team**
- **Différents modes d'attaque**
  - Pièces jointes malveillantes
  - Lien vers un site malveillant
- **Pas de shell (on a dit non-intrusif !), mais des statistiques**
  - Evolution du taux d'ouverture des pièces jointes
  - Versions des technologies utilisées par les utilisateurs et les vulnérabilités associées

Conclusion

- **Pas de miracle, mais de sérieux efforts à faire du côté des Blue Team**
- **Pour réduire les risques**
  - Utiliser toutes fonctionnalités de sécurité à disposition
  - Durcir les configurations des postes client
  - Entraîner les utilisateurs à discerner les menaces et à avertir en cas de doute

AVEZ-VOUS DES QUESTIONS ?

MERCI DE VOTRE ATTENTION,

SYNACKTIV
DIGITAL SECURITY