S’attaquer à l’humain pour compromettre le SI

digital.security

whoami

- Sylvain HAJRI / @navlys_
  - Consultant sécurité
    - GRC
    - OSINT / Social Engineering / Intrusion physique
  - Intérêts
    - Hack (IoT, Hardware, Radio…)
    - Lock picking
    - Intelligence économique
    - Administrateur de la communauté OSINT-FR
    - Cofondateur du spying challenge

digital.security

Sylvain HAJRI

Consultant SSI

sylvain.hajri@digital.security

@navlys_

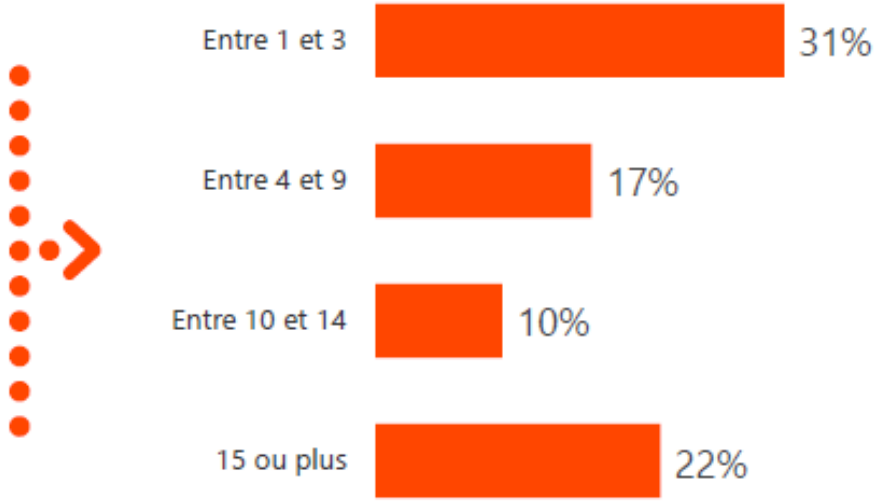
Constat

Le taux d'entreprises touchées par une cyber-attaque reste très élevé

Q5. Combien de cyber-attaques ont été constatées dans votre entreprise au cours des 12 derniers mois ?
Base : ensemble (174 répondants)

80%

des entreprises ont constaté au moins une cyber-attaque

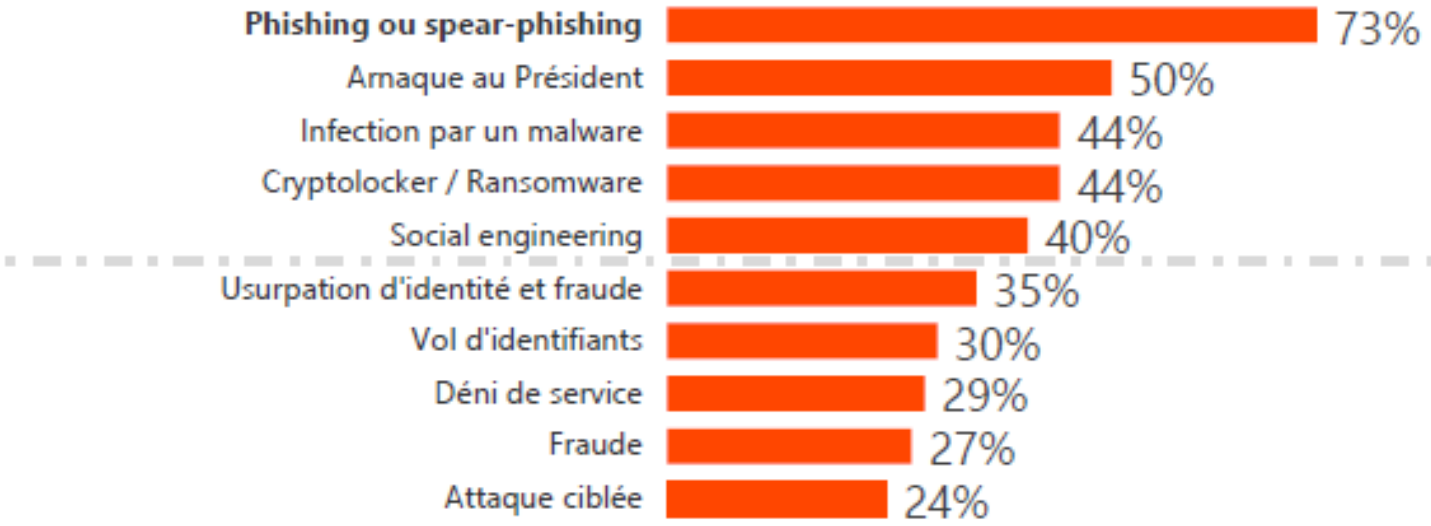


CESIN

Constat

Types de cyberattaque constatés au cours des 12 derniers mois

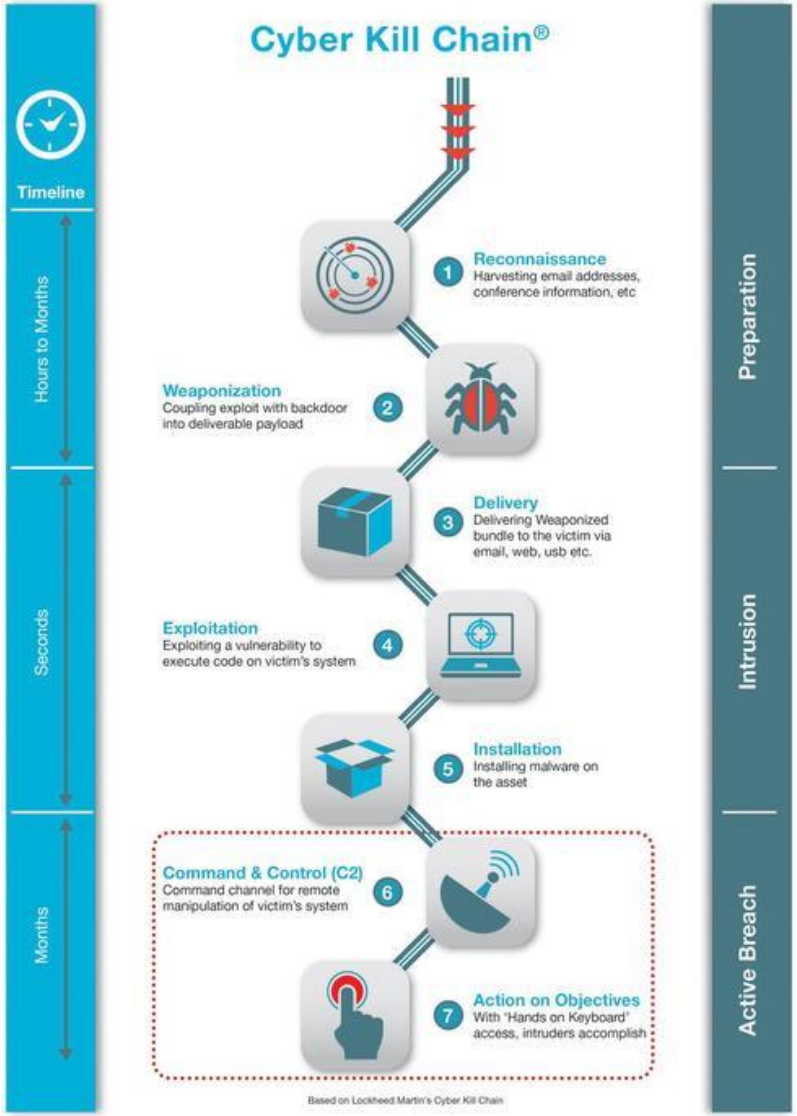
Q6. Quel(s) type(s) de cyber-attaque votre entreprise a-t-elle constaté(s) au cours des 12 derniers mois ?
Base : ont constaté une attaque (139 répondants) / Plusieurs réponses possibles



CESIN

Mettons-nous à la place d’un pirate…

Préparation de l'attaque



Préparation de l'attaque

« Tout le succès d'une opération réside dans sa préparation. »

Sun Tzu

Les types de renseignements

- HUMINT — Human Intelligence
  - Origine humaine
- SIGINT — Signal Intelligence
  - Origine électromagnétique
- IMINT – Imagery Intelligence
  - Origine images (satellites, photos, google maps…)
- OSINT – Open Source Intelligence
  - Origine source ouverte (web, journaux…)
- SOCMINT – Social media intelligence
  - Origine réseaux sociaux

OSINT / ROSO

Phase primordiale

- Connaître l'entreprise cible, son vocabulaire, son fonctionnement…
- Se renseigner sur les employés intéressants
- Connaître les prestataires de la cible
- Repérer les différents accès et procédures pour accéder aux bâtiments
- Établir un plan d'attaque

Repérage des locaux

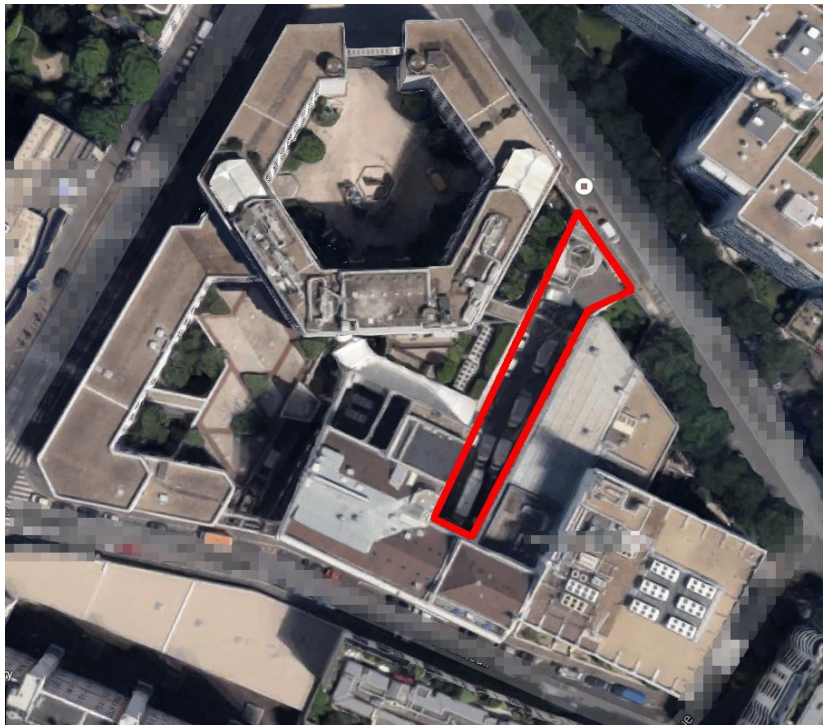
GEOINT

géoportail ...

La caserne Pasquier de Satory où est implantée le GIGN (Capture d'écran du Géoportail de l'IGN)

Les vues aériennes des sites sensibles de la Gendarmerie en libre accès sur le net

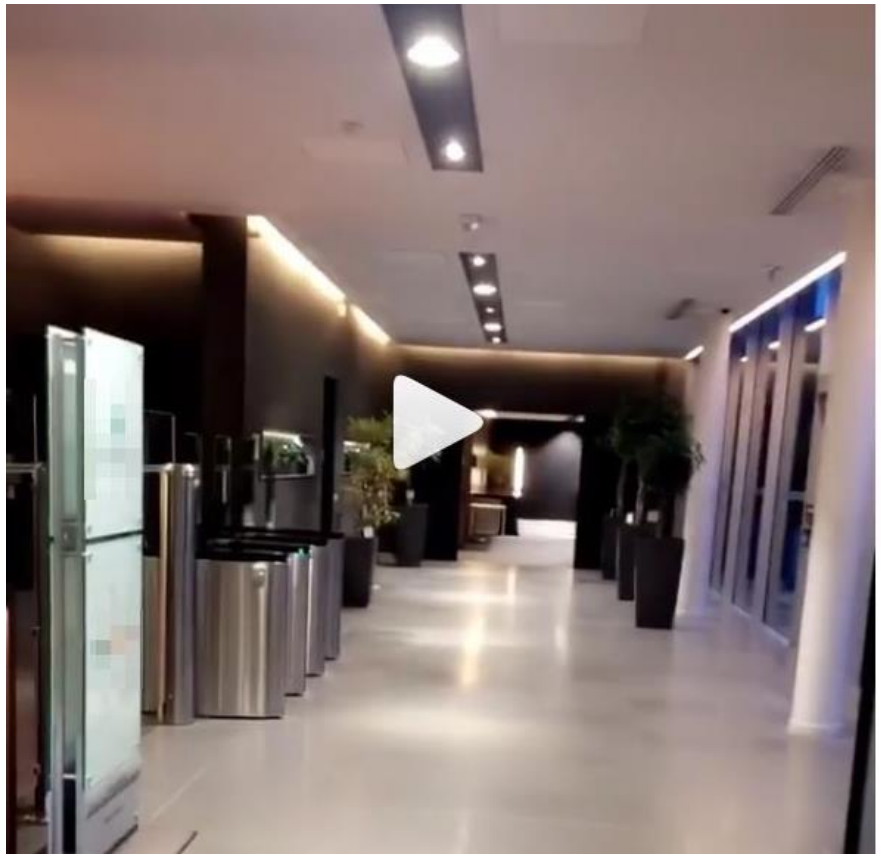
15 octobre 2018 A la une, Opérationnel Laisser un commentaire



Repérage des locaux

Réseaux sociaux personnels

...



Repérage des locaux

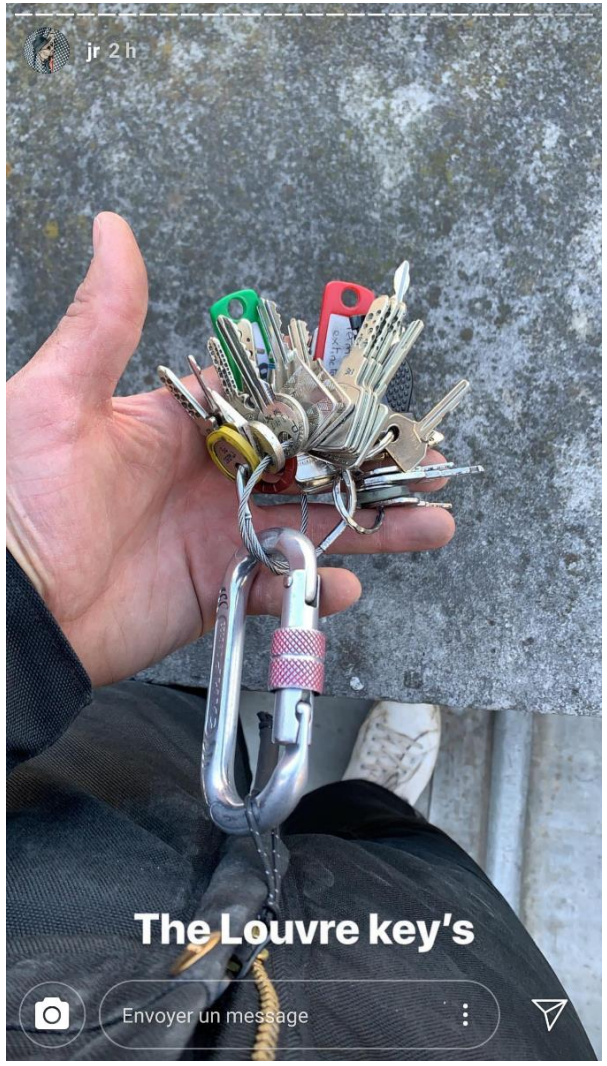
Réseaux sociaux personnels

Repérage des locaux

Réseaux sociaux personnels

Repérage des locaux

Réseaux sociaux personnels



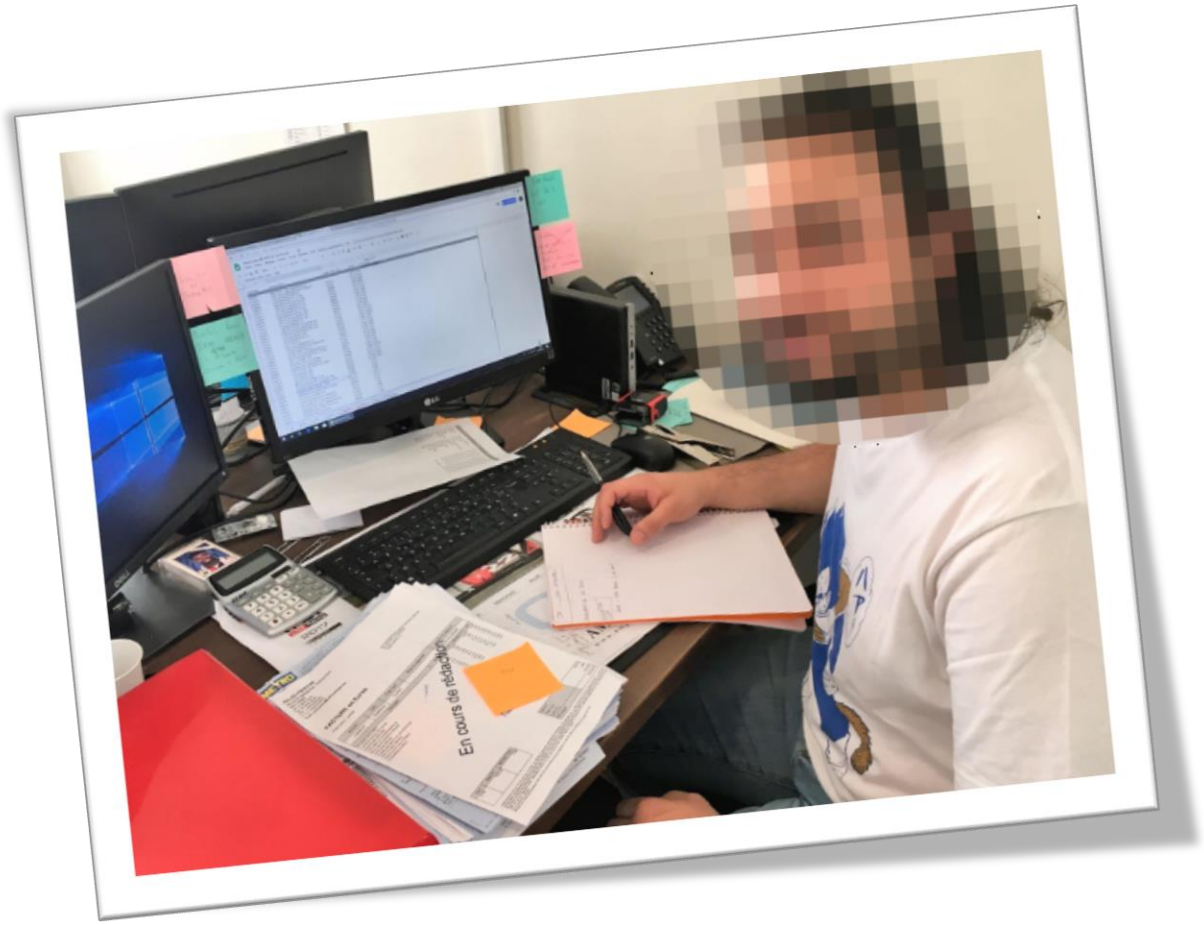
Repérage des locaux

Réseaux sociaux professionnels

[redacted]
16 988 abonnés
6 mois

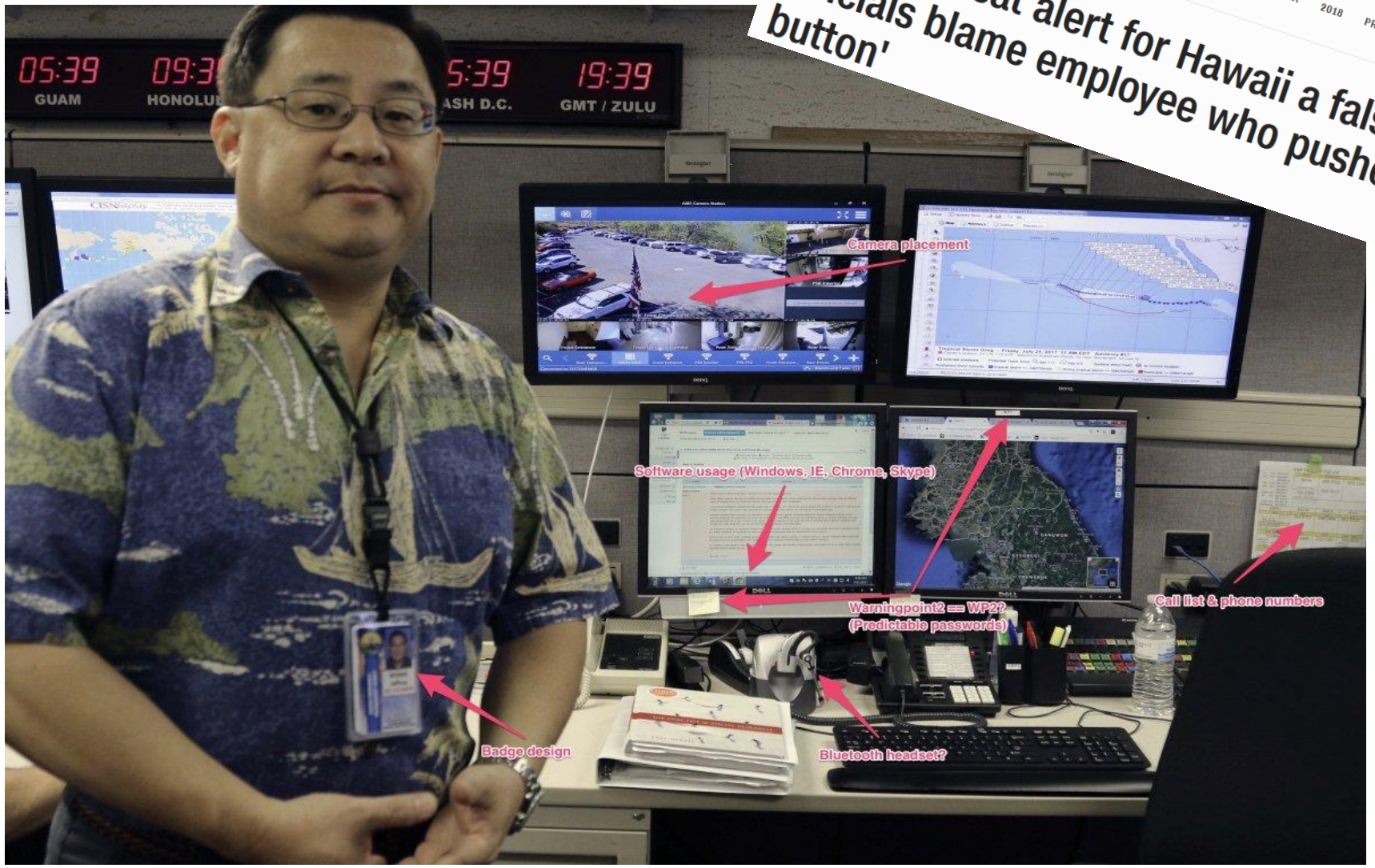
★ [redacted] Recrute ★

Lui, c'est [redacted] notre nouveau comptable fournisseur qui vien… voir plus



Repérage des locaux

Presse



CNN politics

45 CONGRESS SECURITY THE NINE TRUMPMERICA 2018 PRIMARIES

Missile threat alert for Hawaii a false alarm; officials blame employee who pushed 'wrong button'

Repérage des locaux

Applications sportives

STRAVA™

runtastic

...

Repérage des locaux

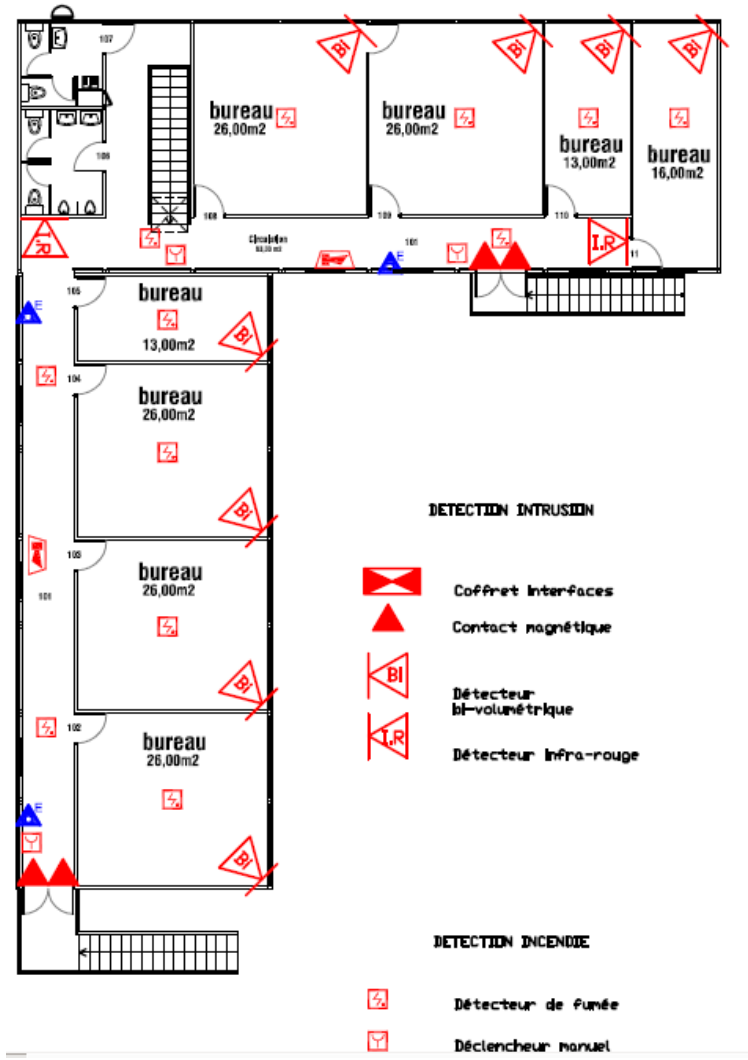
Marchés publics

Annexe n°1 à l'acte d'engagement
BORDEREAU DE PRIX UNITAIRES ANTI-INTRUSION

N°	Description
195	Outil de gestion portable, écran 17'' Processeur core 2 Duo Windows 74 Go de Ram, lecteur/graveur cd/dvd compatible tout cd et dvd et lecteur de carte mémoire 5 en 1
196	Unité de stockage mobile 250Go Port USB2, ccompatible windows
197	Unite de stockage mobile 8GoPort USB2, compatible windows

N° D'AFFAIRE	NOM DU PROJET				
[redacted]	CONSTRUCTION DU BATIMENT [redacted] PARIS [redacted]				
CONCEPTION	DESSIN	DATE	ECHELLE	NUMERO DU PLAN	INDICE
SUSS	SUSS	08/10/10	1/200	[redacted]	0

BÂTIMENT [redacted]
RDC - 1er ETAGE
INTRUSION - INCENDIE



Après les bâtiments… les personnes

Ingénierie sociale

Collaborateurs

« Art de manipuler un individu afin de lui faire réaliser des actions ou divulguer des informations »

Ingénierie sociale

Collaborateurs

Informations intéressantes

- Profiling
  - MBTI, NEOAC, Ennéagramme
- Techniques d'influence
  - MICE (Monnaie, Idéologie, Contrainte, Ego)
  - SANSOUCIS
- Centres d'intérêt, relations permettant de parfaire la crédibilité et la personnalisation des attaques
  - Vishing
  - Spear-phishing
  - Intrusion physique

digital.security

Collaborateurs sur les réseaux sociaux professionnels

Compétences et environnements technique

Ingénieur sécurité réseaux

août 2014 – janv. 2015 · 6 mois

Gestion de projet :
•Refonte Lan du siège :
- Amélioration de l'infrastructure du Siège (Cœurs réseaux, Wifi, Débit interne...)
- Sécuriser et cloisonner l'accès aux cœurs de réseau et aux serveurs.
•Refonte Lan :
- Changement du Switch (HP 3600)
- Suivi de l'implémentation avec les partenaires
Participation aux études de l'architecture technique et de son évolution.
Rôle de conseil aux évolutions de l'infrastructure SI.
Administration de la solution IMC (Intelligent Management Center)
Administration Switch HP 3600
Gestion des règles de filtrages WEB via le proxy Zscaler en SAS.
Maintient Condition Opérationnel des plateformes SI Siège
Support N3 pour la solution VPN Dell Aventail : Siege et les partenaires (Liban, UK, Tunisie et Allemagne) Voir moins

Administrateur système

nov. 2018 – févr. 2019 · 4 mois
La Défense, France

En prestation pour la société

Taches :
• Mise en œuvre de la solution Sophos Central en remplacement de la solution Trend sur le Parc Interne et Clients (Selon Expression de besoin du client et de son environnement)
• Mise à jour du parc de certains clients sur leur propre solution antivirus
• POC de la solution de supervision Helpsystem - Vityl réalisé. Mise en production (préparation des VM (SQL + Solution) selon les critères techniques requis).
• Déploiement sur tout le parc virtuel d'une nouvelle communauté SNMP dans le cadre de la future mise en place d'une supervision (Via SSH ou le déploiement d'une clé de registre)
• Rédaction Procédure diverses

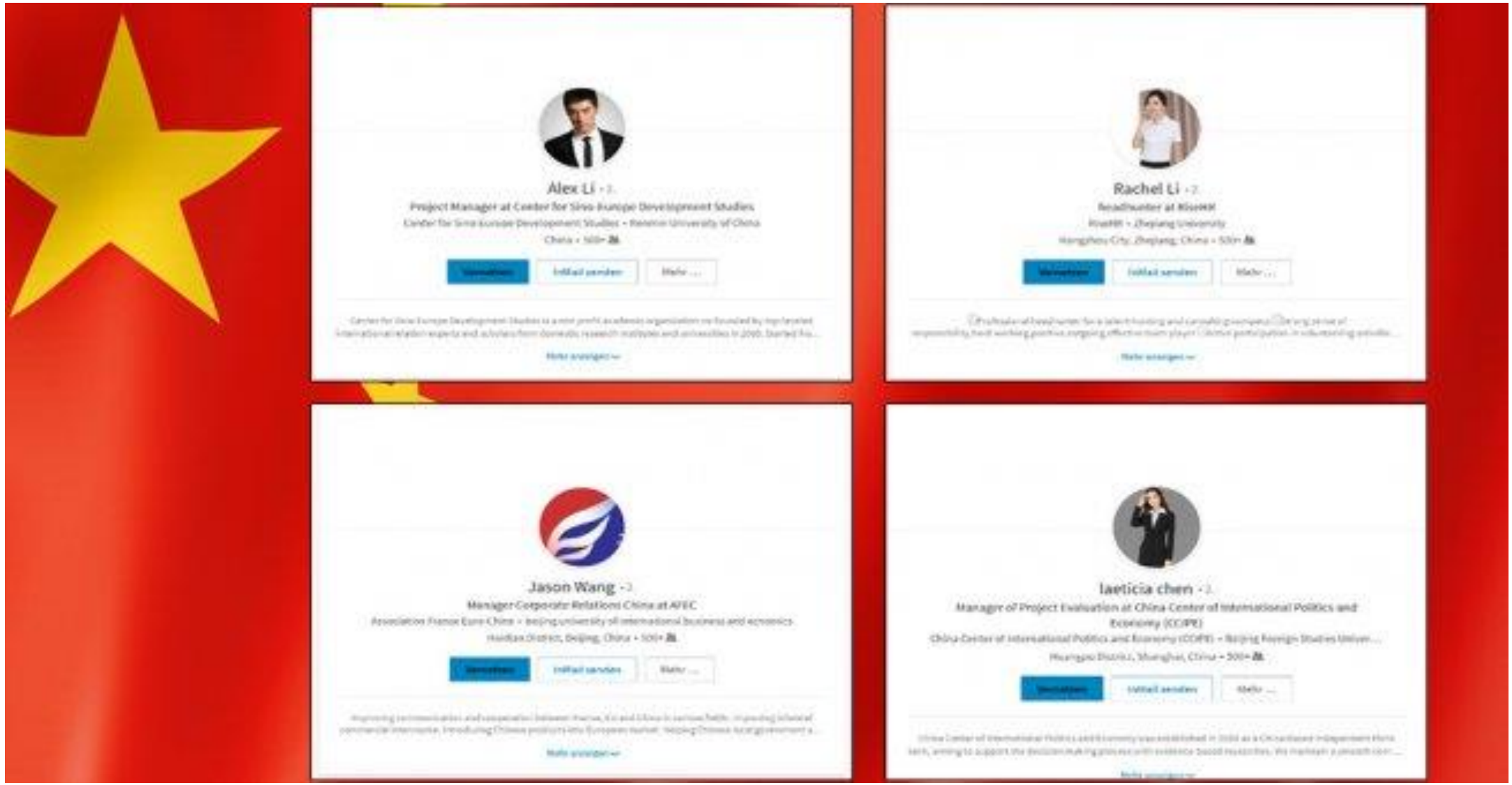
Système :
• Installation et configuration d'un Windows serveur 2016 - Rôle WSUS, remplacement de l'actuel en 2008 R2
• Installation d'un serveur SMTP/FTP sous Windows Serveur 2016
• Maintenance diverse des serveurs clients : AD, DNS, DHCP.
• Scripting PowerShell (mise en œuvre d'un script pour remplacer une solution logicielle)

Réseau :
• Installation et configuration de la solution PHPIPAM
• Juniper SSG 140 - Ajout VPN Clients - Ouverture de flux diverses
• Stormshield SN3000 : Création routes et objets réseaux - analyse des flux

Collaborateurs sur les réseaux sociaux professionnels

- Getting in bed with Robin Sage *Blackhat 2010*
  - Prise de contact avec militaires, employés de fabricants d'armes, département de la défense...
  - Accès aux mails et comptes bancaires des victimes
  - Récupération d'horaires de décollage des hélicoptères américains

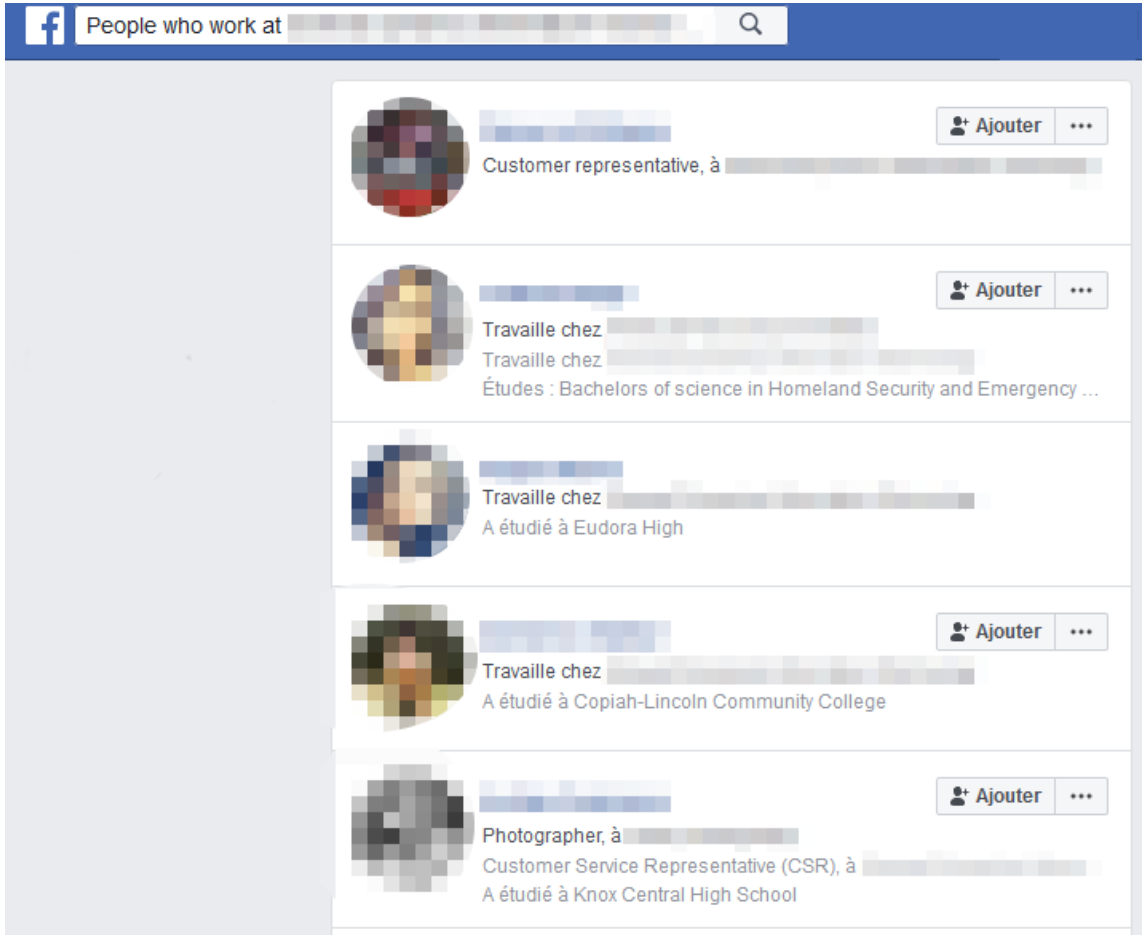
Collaborateurs sur les réseaux sociaux professionnels

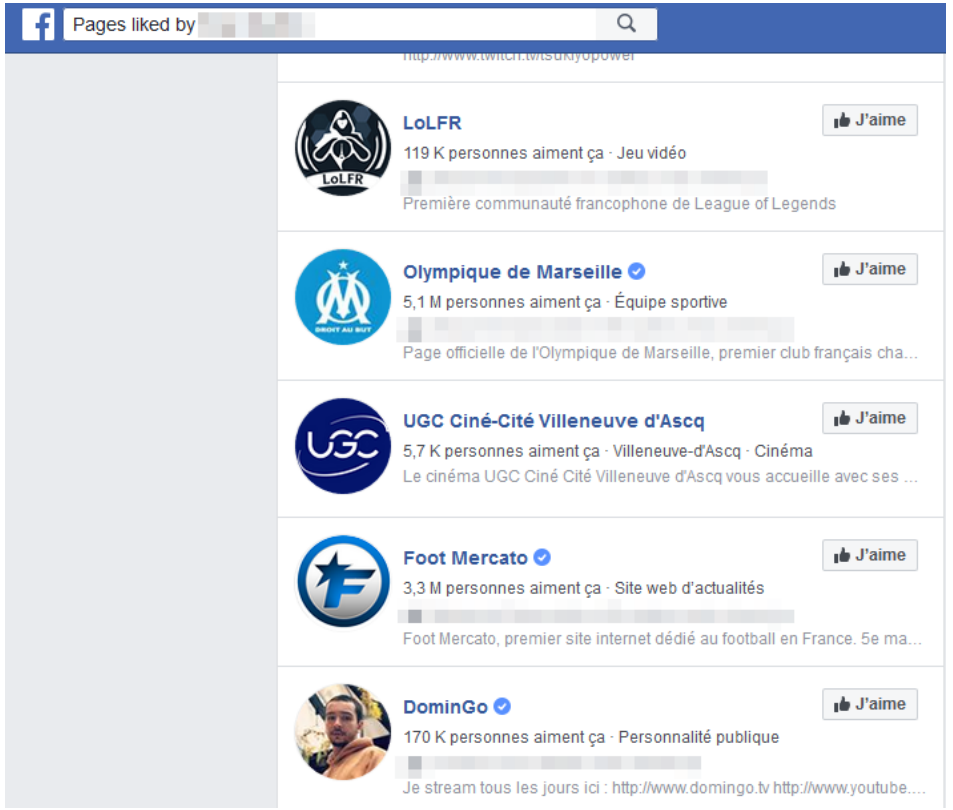


digital.security

Collaborateurs sur les réseaux sociaux personnels

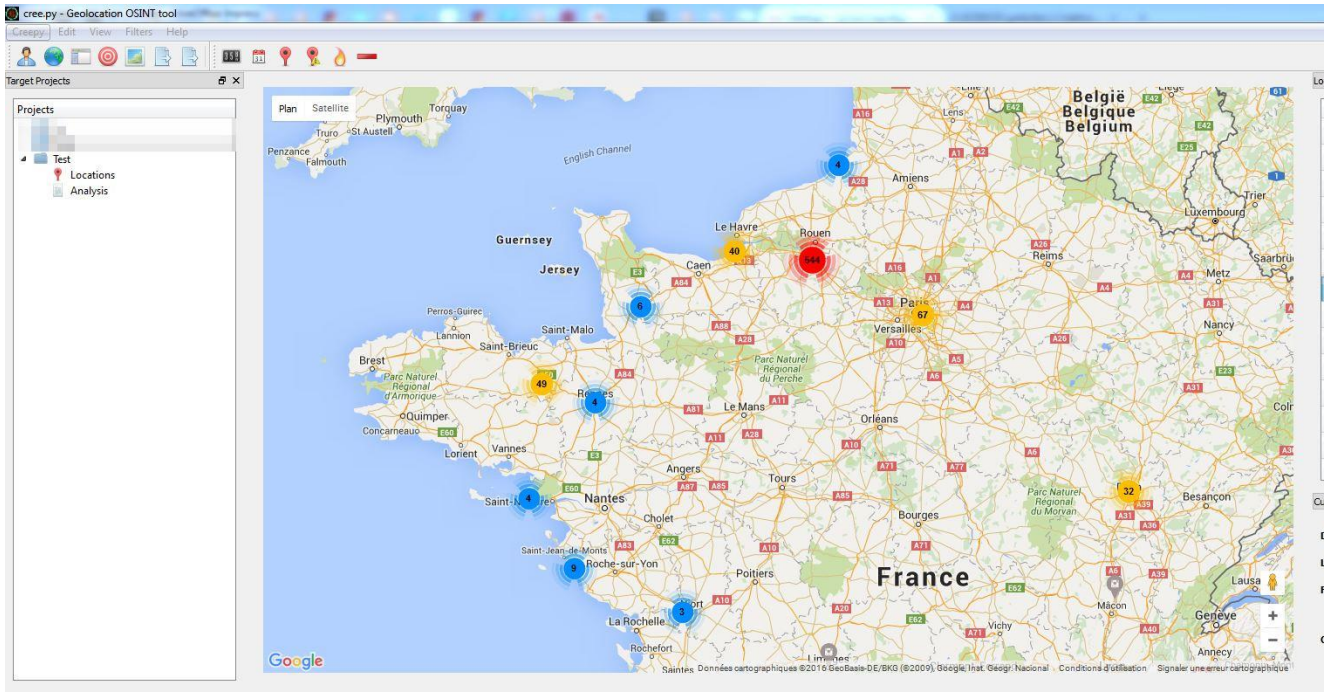
Facebook graph search





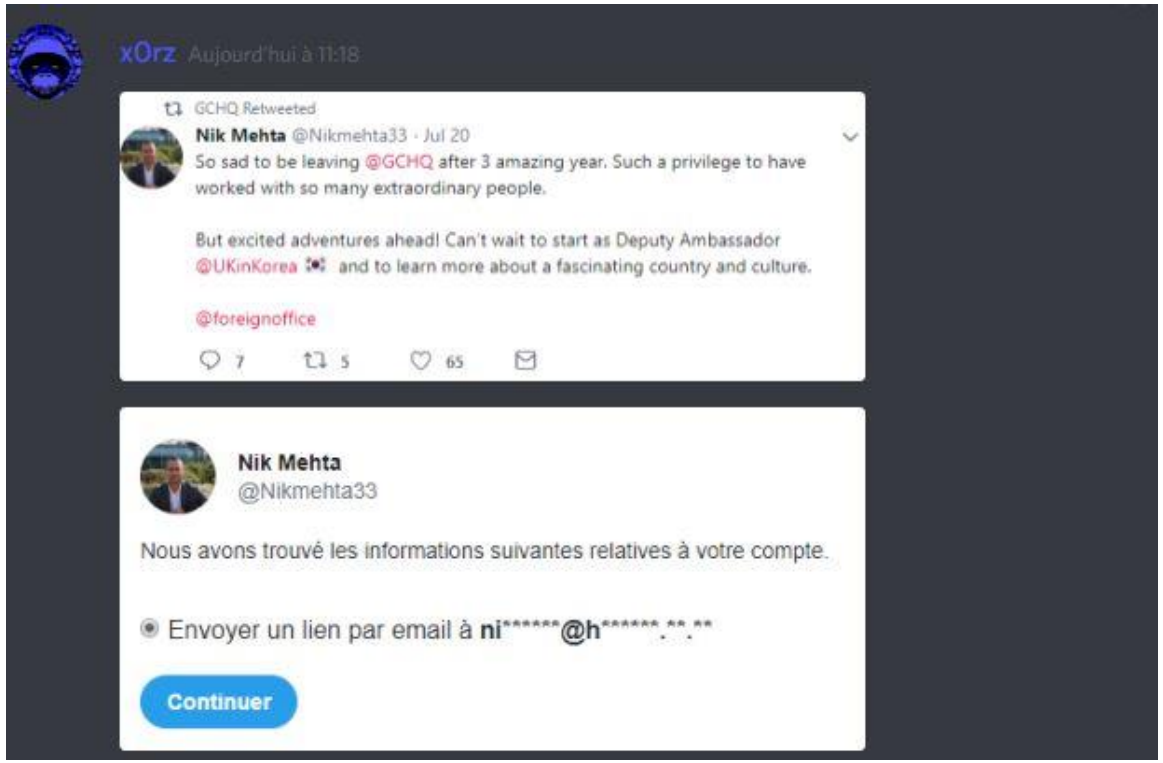
Collaborateurs sur les réseaux sociaux personnels

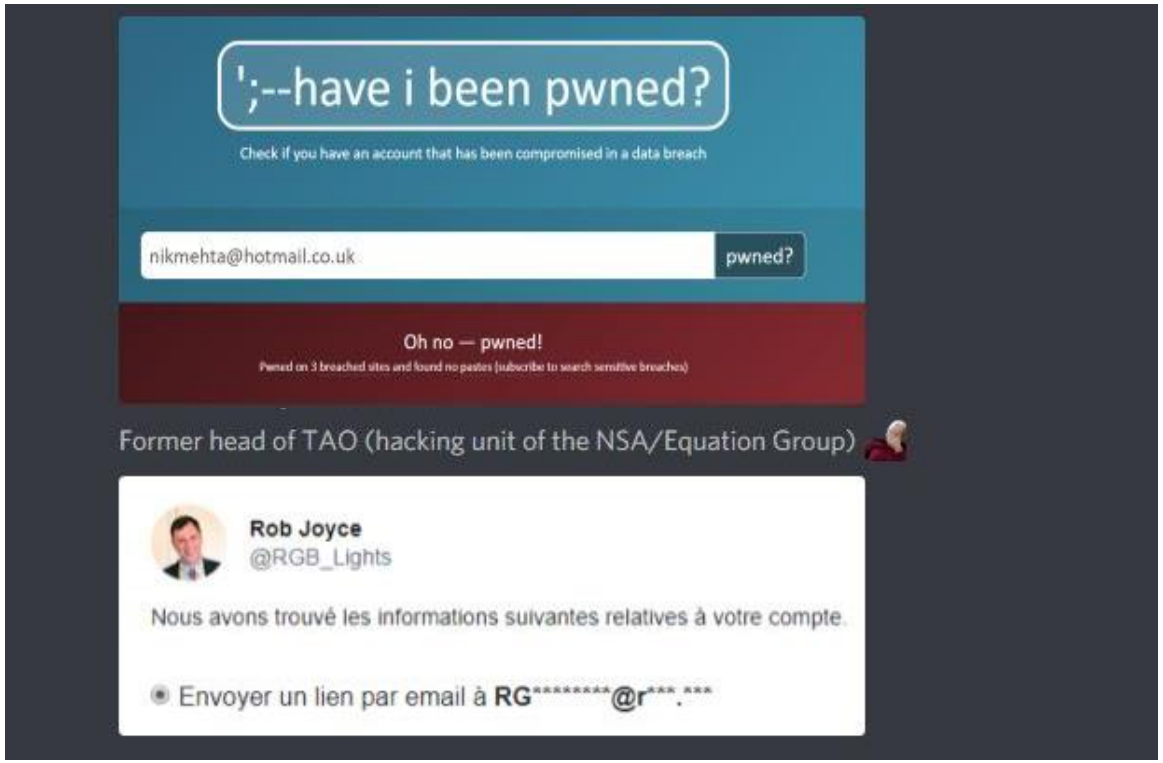
Twitter



Collaborateurs sur les réseaux sociaux personnels

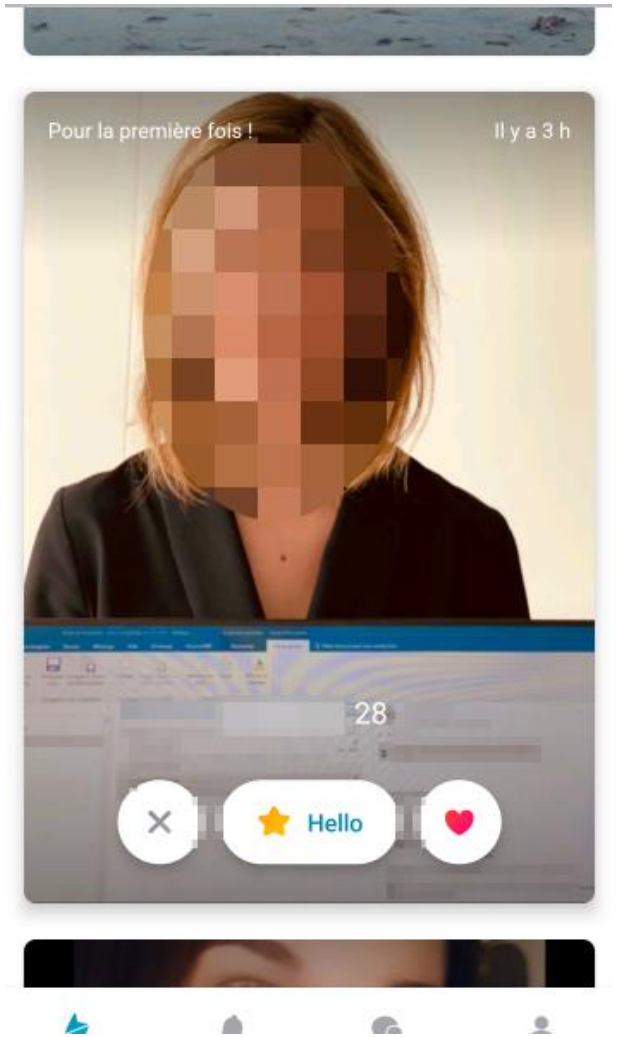
Twitter



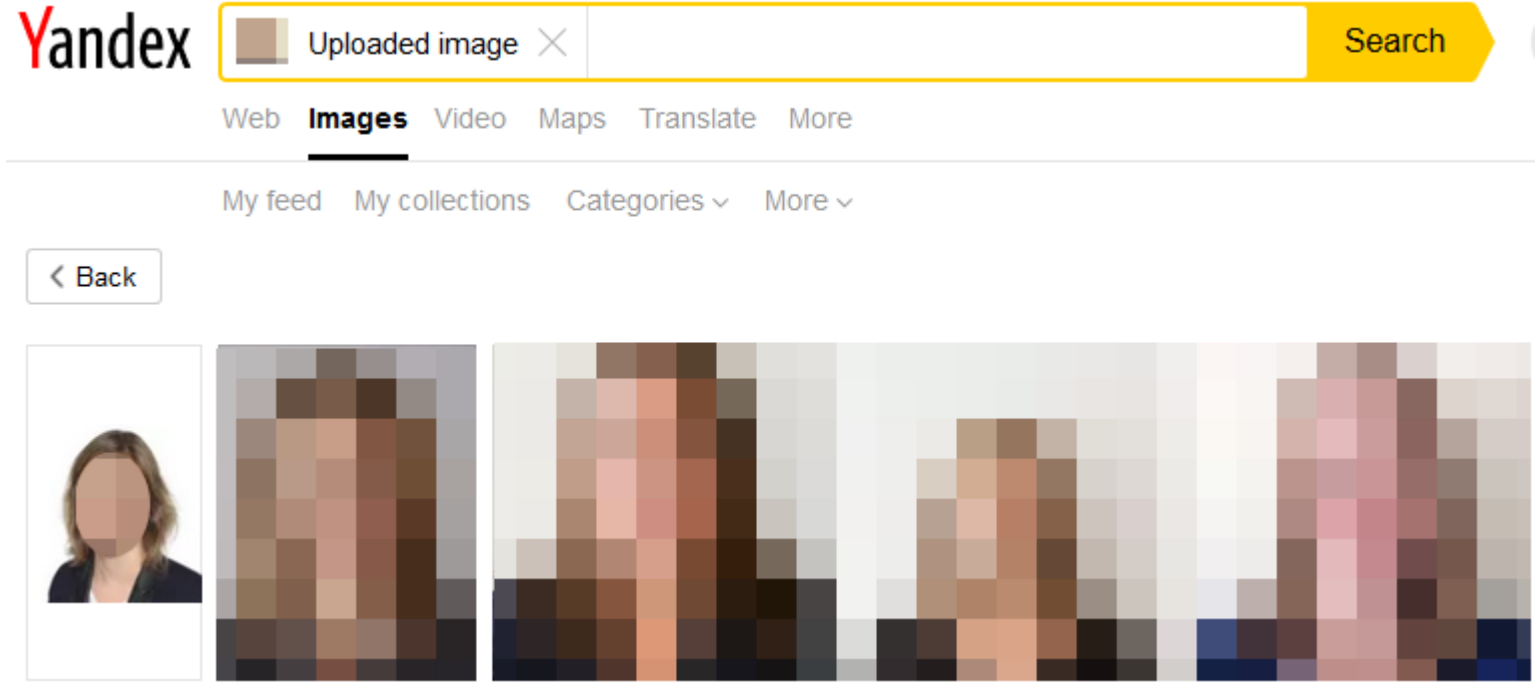


Collaborateurs sur les réseaux sociaux personnels

Applications de rencontres

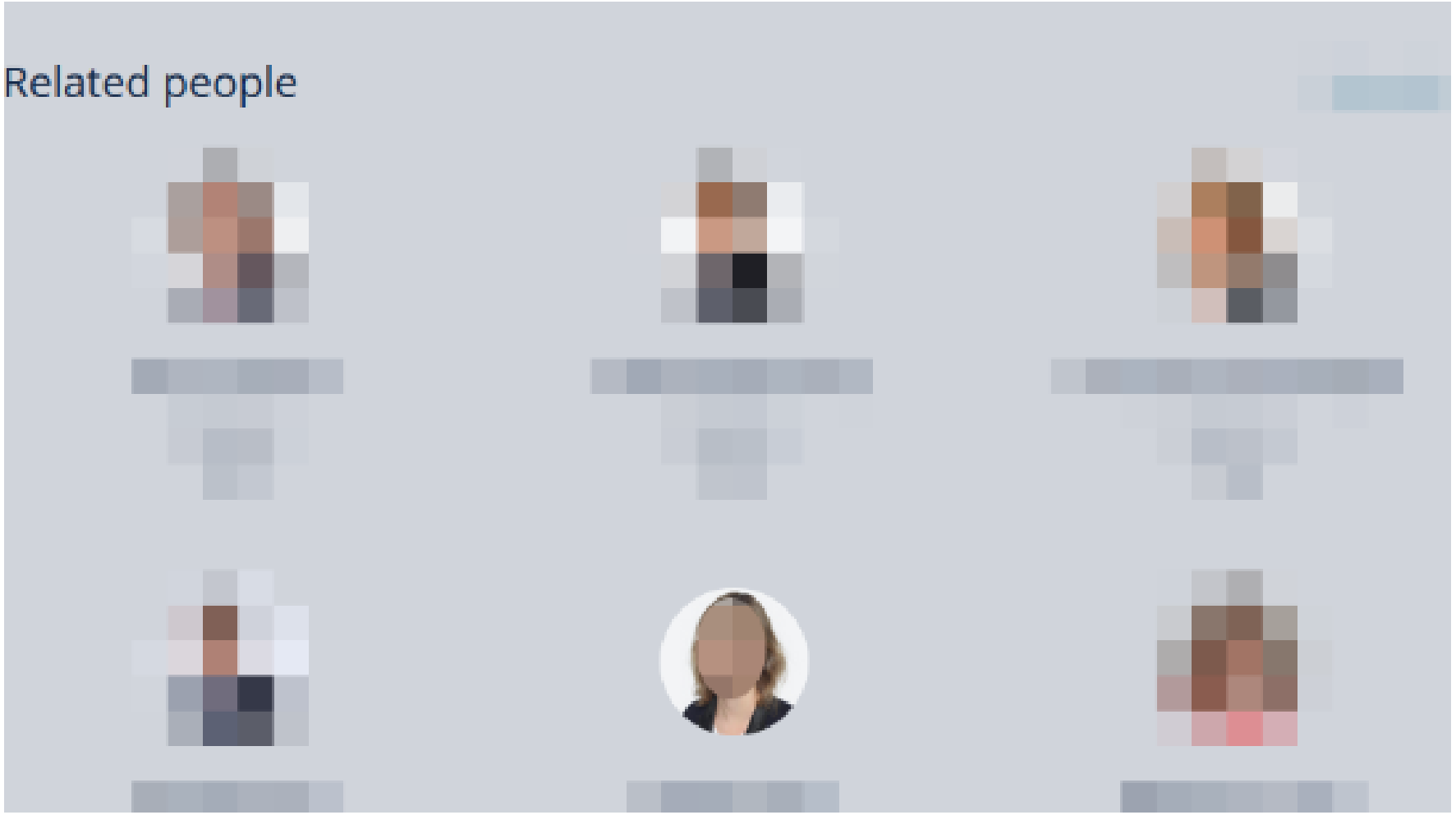


...



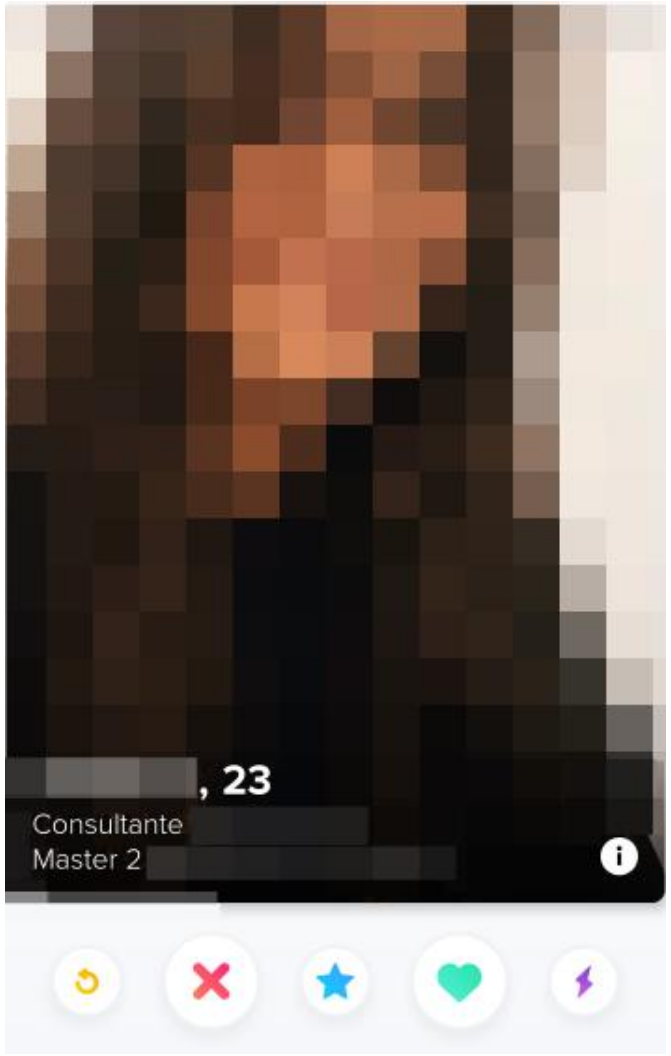
Collaborateurs sur les réseaux sociaux personnels

Applications de rencontres



Collaborateurs sur les réseaux sociaux personnels

Applications de rencontres



Collaborateurs sur les réseaux sociaux personnels

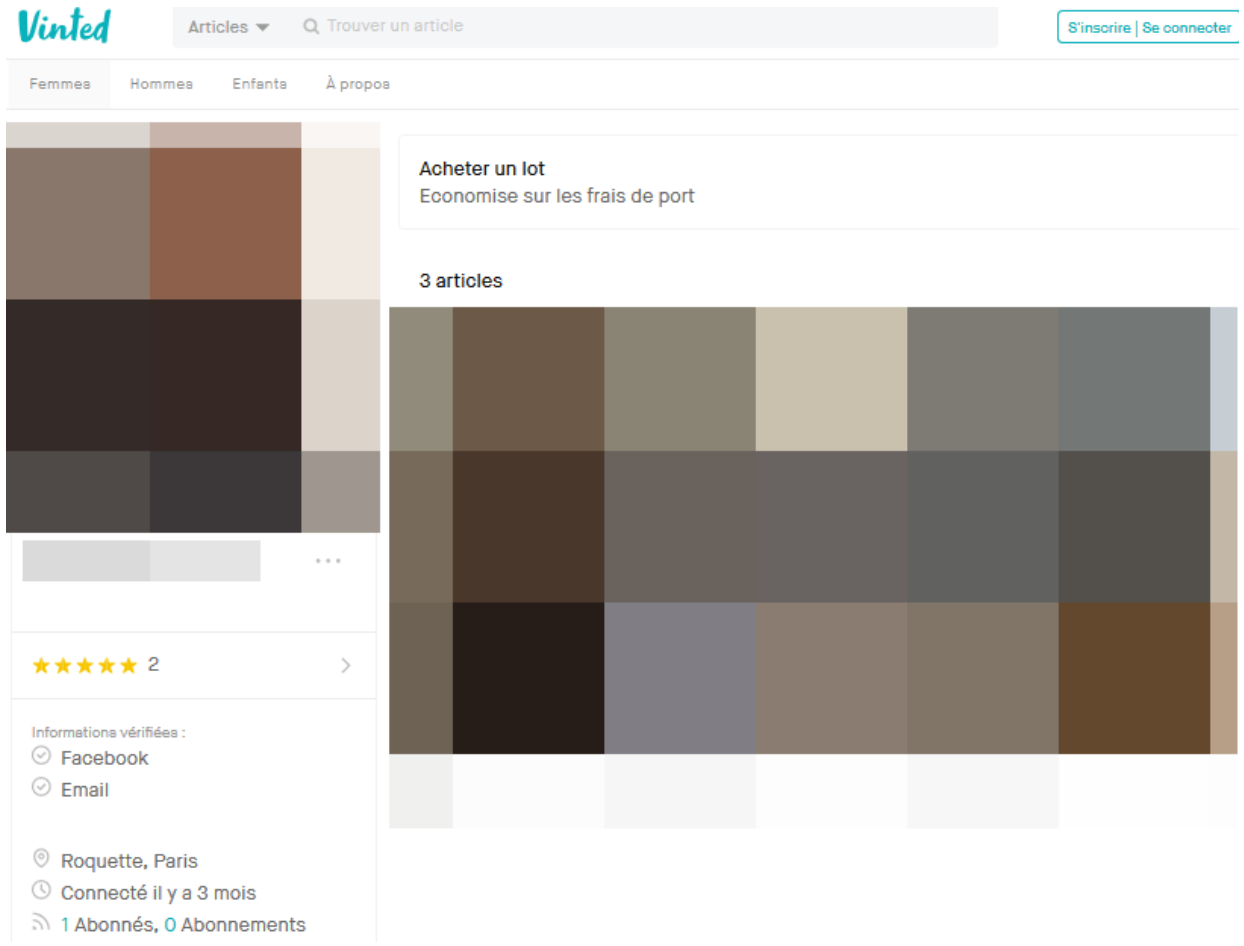
Applications de rencontres

Collaborateurs sur les réseaux sociaux personnels

Applications de rencontres

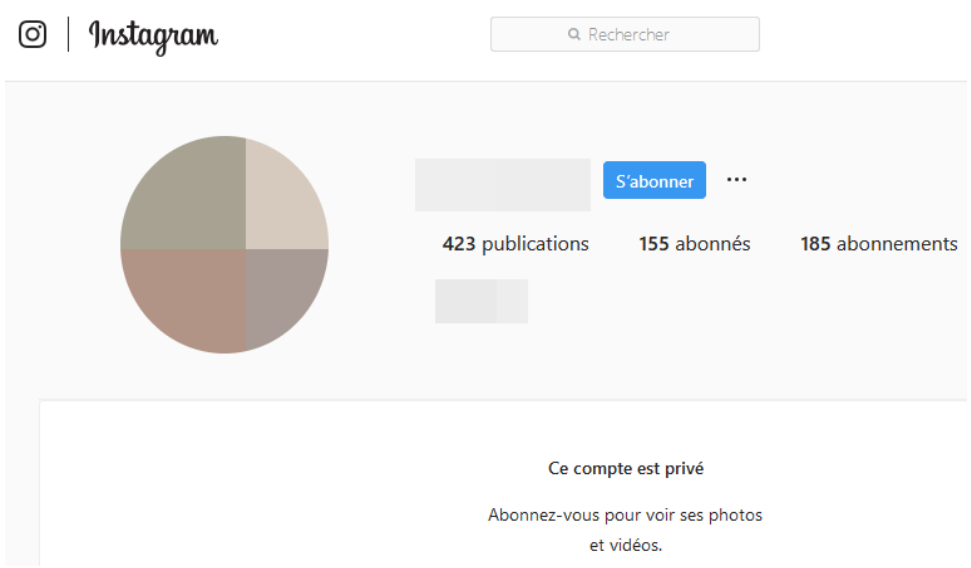
Collaborateurs sur les réseaux sociaux personnels

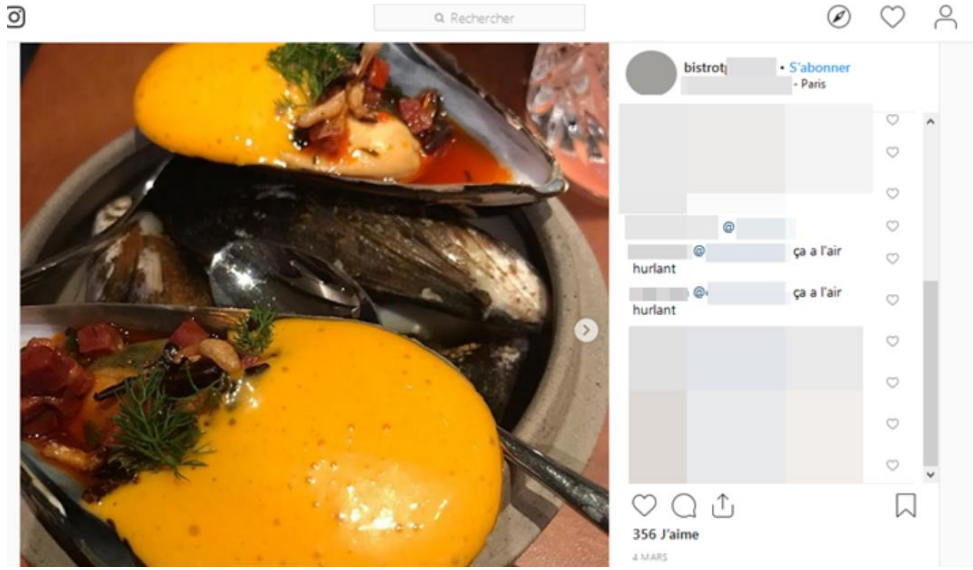
Applications de rencontres



Collaborateurs sur les réseaux sociaux personnels

Applications de rencontres





Synthèse

Récupérations d'informations

Organisation

- Informations techniques
- Informations sur le bâtiment
- Collaborateurs

Collaborateurs

- Centres d'intérêt
- Proches
- Coordonnées professionnelle et/ou personnelle

Que faire ?

Sensibiliser

- Parcours d'intégration pour les internes et prestataires
- Utilisation et configuration des réseaux sociaux
- Ingénierie sociale (vishing, spear-phishing)
- Intelligence économique (suivant le domaine de l'organisation)

Surveiller l'exposition de l'organisation et des collaborateurs

Contrôler de manière permanente

Que faire ?

Auditer régulièrement

- OSINT
- Ingénierie sociale et intrusion physique

Etablir des processus, règles, recommandations

- Publication par les métiers de contenu sur les réseaux sociaux
- Utilisation des réseaux sociaux dans la sphère privée

Former

- RH, juridique…

Conclusion

- Nous sommes des *humains*, donc sociable par essence
- Nous avons tous des *vulnérabilités*
- Nous avons une *relation à la technologie différente* suivant les profils
- Nous sommes tous capables de *nous protéger*

Conclusion

Le collaborateur est le maillon faible de la SSI, mais surtout **le maillon fort**

- Rendre acteur le collaborateur
  - Pour lui faire *adopter les bons comportements*
  - Pour lui faire *remonter des alertes*

« Nous sommes tous fournisseurs et clients de l'information »

Questions ?

Sylvain HAJRI

Consultant SSI

sylvain.hajri@digital.security

@navlys_