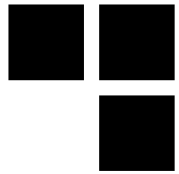
SYNACKTIV
DIGITAL SECURITY

Espionnage et prise en main à distance des postes de travail

Présenté le 29 mai 2017
Pour l'École de Guerre Économique
Par Renaud Feil

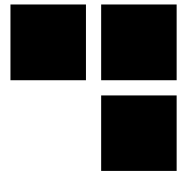
Introduction



- **Agenda**
  - Techniques d'intrusion sur les postes de travail
  - Démonstration d'une attaque

    Avertissement d'usage : ne faites pas n'importe quoi !
  - Contre-mesures et leurs limites
  - Évolutions possibles des menaces
- **Objectifs**
  - Présenter la menace technique puis élargir sur l'enjeu pour les professionnels de l'Intelligence Économique
  - Lutter contre les idées préconçues et les fausses solutions miracles
  - Donner quelques pistes pour se protéger
  - Présenter pourquoi l'espionnage informatique sera probablement croissant dans les prochaines années

Introduction



- **Synacktiv**
  - Expertise en sécurité offensive depuis 2012
  - Tests d'intrusion & recherche de vulnérabilités
  - 18 experts sécurité
- **Renaud Feil**
  - Co-fondateur de Synacktiv
  - Bonne expérience dans les audits de sécurité et les tests d'intrusion

Le spear-phishing

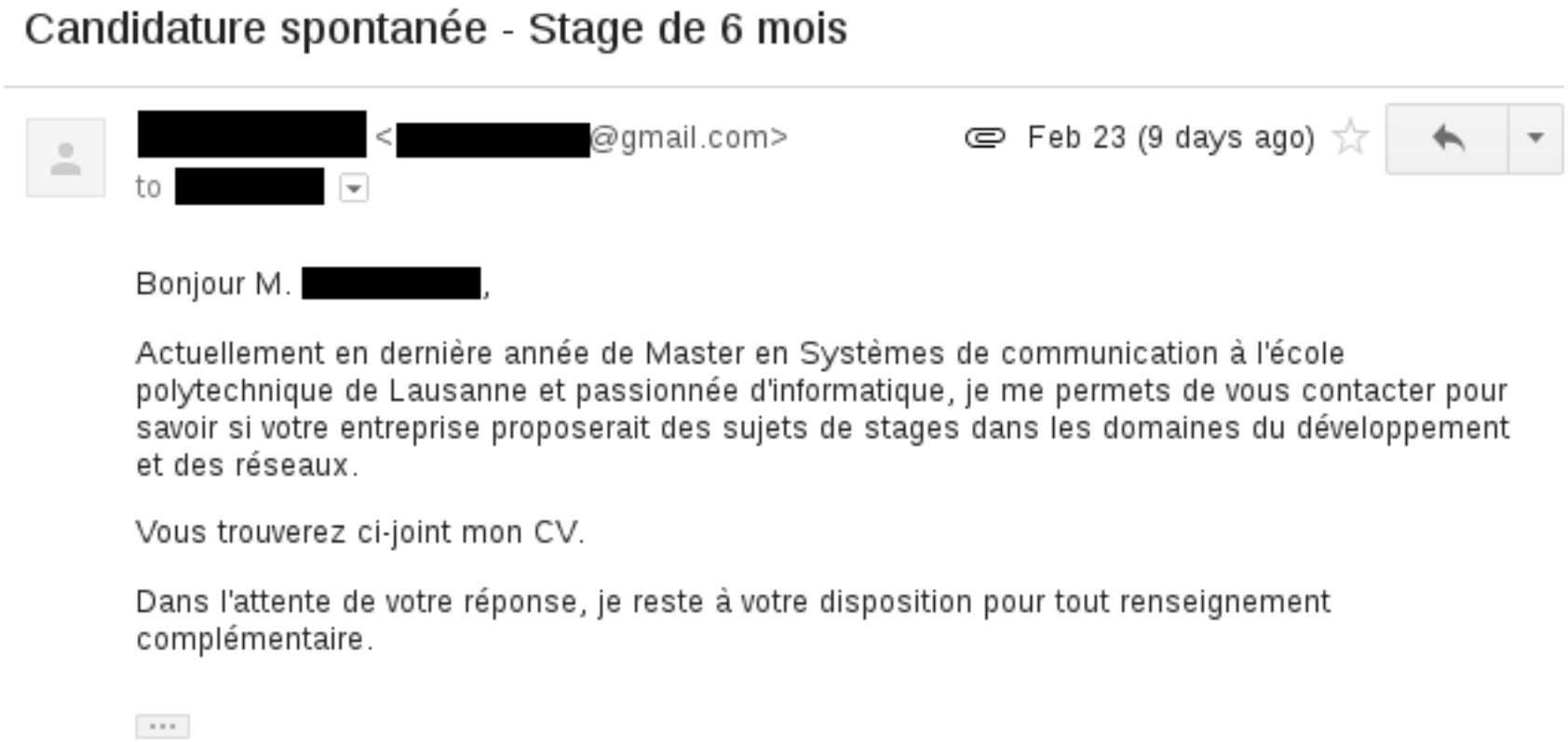
- **C'est quoi ?**
  - Harponnage en français
  - Version ciblée du phishing
  - Charges malveillantes (exploitation d'une vulnérabilité, documents piégés)

Le spear-phishing facile

- **Phases**
  - Recherche d'informations sur les employés
  - Préparation des scénarios
  - Envoi des e-mails
  - Compromission et accès à distance
  - Persistance
  - Rebonds sur le 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.

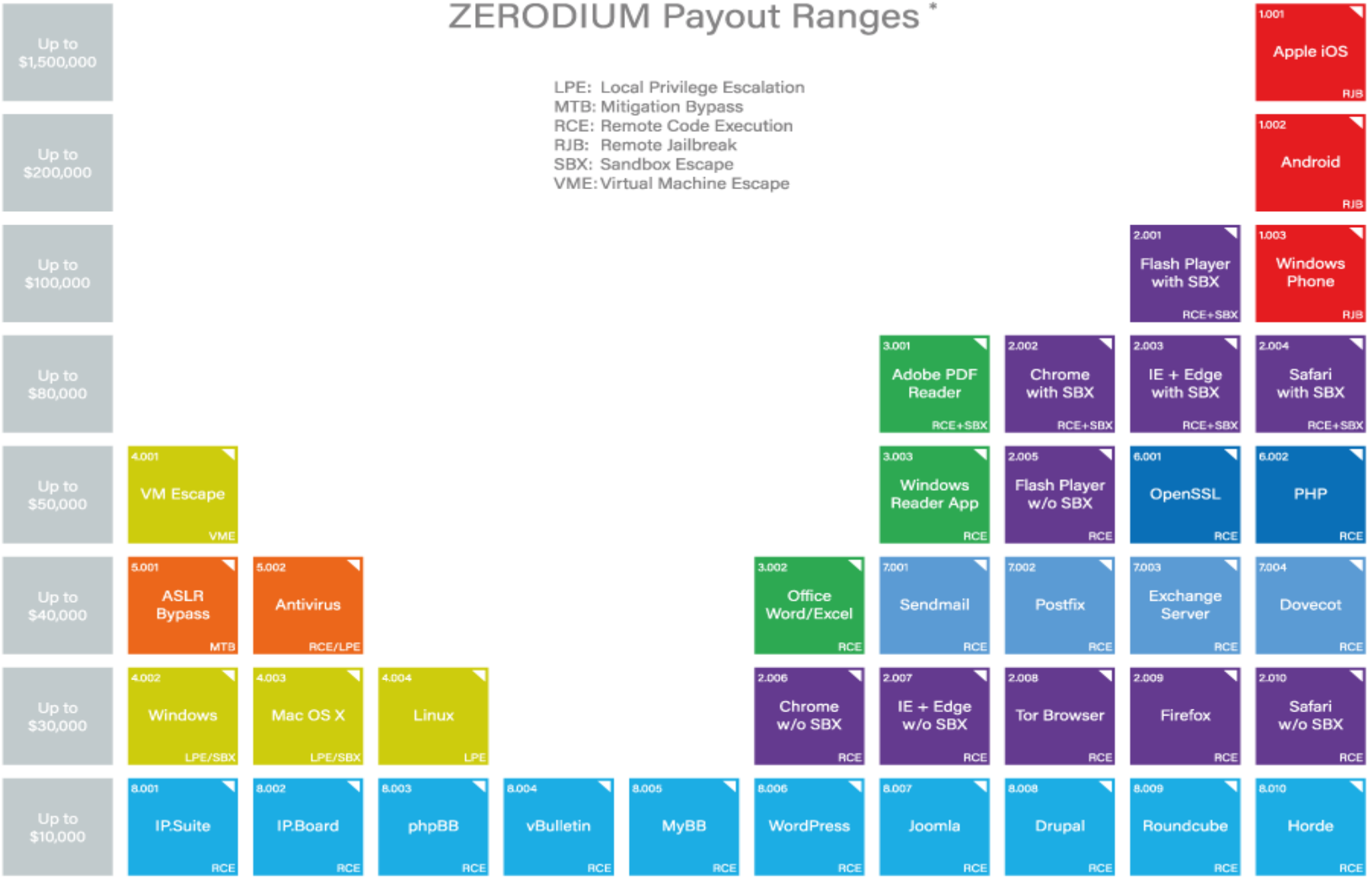
Dans l'attente de votre réponse, je reste à votre disposition pour tout renseignement complémentaire.

...

Les charges utiles : exploits

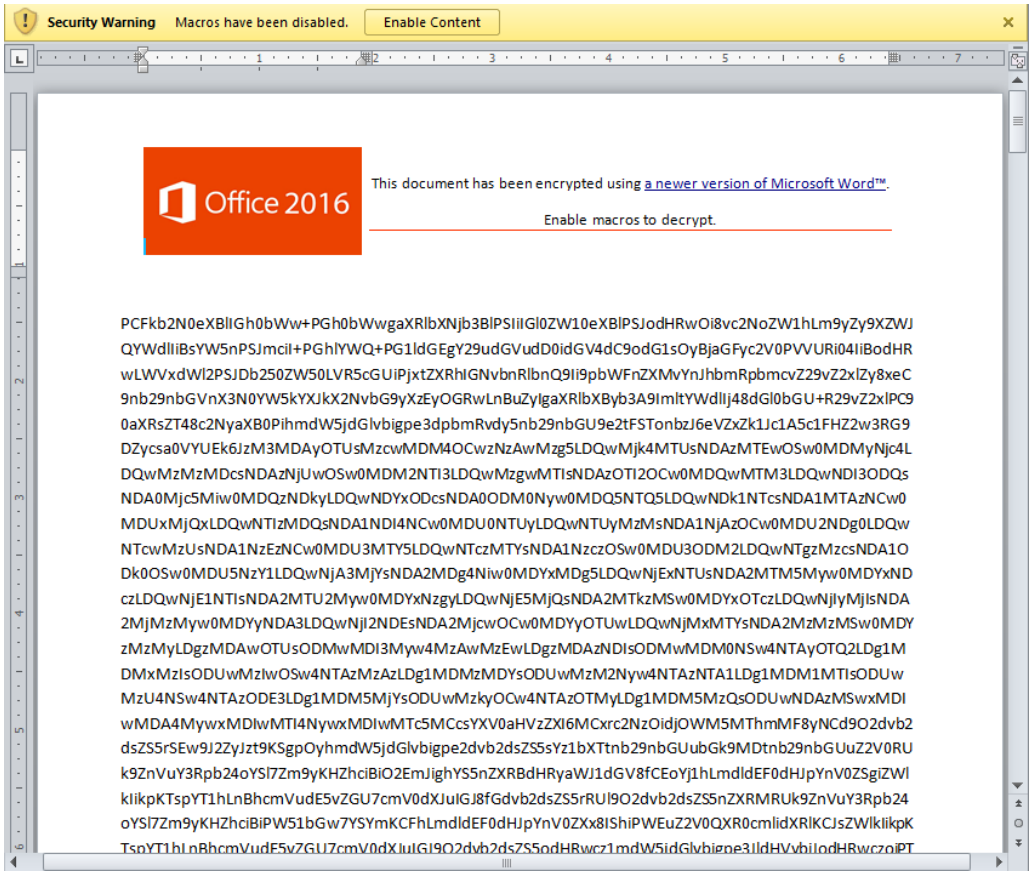
- **Différents vecteurs d'exploitation**
  - Navigateurs
  - Plugins (Flash, Silverlight, Java)
  - Clients mail (Outlook, Apple Mail)
  - Suites bureautique (Word, LibreOffice)
- **Avantages**
  - Pas d'avertissements de sécurité
- **Inconvénients**
  - Nombre de cibles limité pour les vulnérabilités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

Les 0-day et le croquemitaine



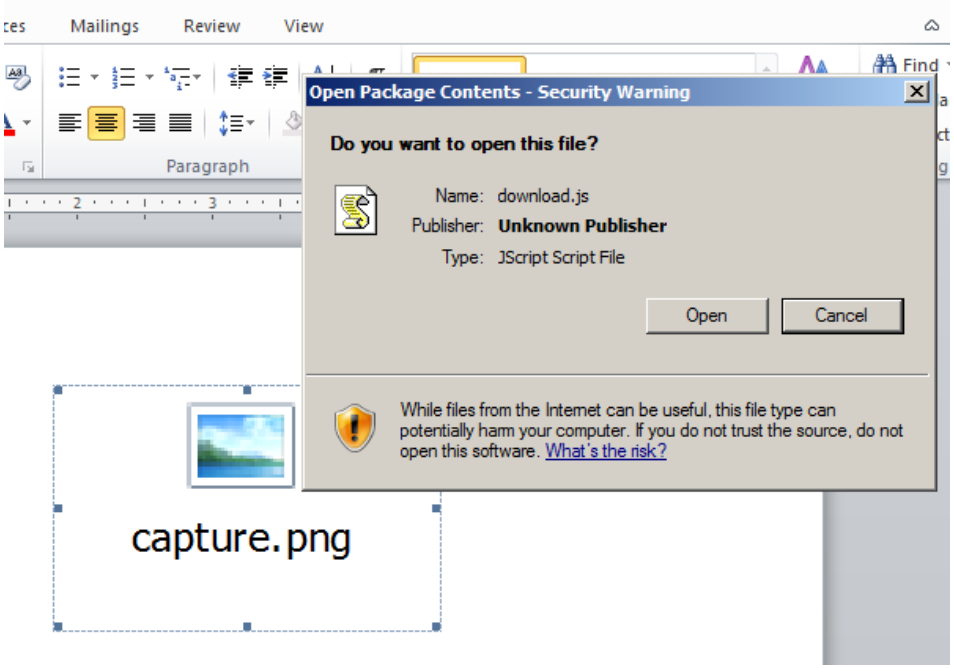
Les charges utiles : Macro Office

- **Old but gold !**
- **Avantages**
  - Exécution de code
  - Office installé presque partout
  - Faible taux de détection
- **Inconvénients**
  - Action utilisateur requise
  - Parfois désactivées



Les charges utiles : objet « lié »

- **Embarquer un objet dans document**
  - Exécutable
  - Script
  - Exploit
- **Avantages**
  - Faible taux de détection
- **Inconvénients**
  - Interaction utilisateur requise



Les charges utiles : exécutable

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

Le phishing facile : Démo

Compromission du réseau interne

- **Par design, les réseaux d'entreprise sont vulnérables**
  - Beaucoup de progrès sur les techniques d'intrusion en environnement Active Directory
  - Le piège du SSO (*Single Sign-On*) et des relations de confiance, l'effet « domino »
  - La quête des privilèges « Admins du domaine »
  - Les limites des gestionnaires de mots de passe (ex : l'outil *KeeFarce*)
  - La compromission des systèmes hors domaine
- **La recherche d'information sur le réseau compromis**
  - Crawlers automatisés
- **L'analyse des informations récupérées**

Retour d'expérience

- **Le spear-phishing à Synacktiv en 2016**
  - 18 missions de type Red Team
  - Plus de 170 e-mails malveillants envoyés
  - Plus de réussites que d'échecs (**environ 90% de réussite, 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

- **… 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.

Apport des anti-virus (et limites)

- **Fonctionnalités intéressantes**
  - Mécanismes de réputation des exécutables
  - Détection de sorties d'outils d'attaque connus
- **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 ?

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

Sensibilisation

- **Le but : entraîner les cibles potentielles**
  - Repérer les e-mails potentiellement malveillants
  - Connaître les actions dangereuses
- **Pas seulement une présentation sur les DO and DON'T**
- **Des campagnes de tests fréquentes**
- **Mais toujours imparfait**
  - 50 % de taux de clic pour une organisation non sensibilisée

    => 10 % après une sensibilisation efficace
  - Il suffit d'un seul clic pour compromettre le réseau interne…
  - Certains services doivent ouvrir les pièces jointes reçues (RH, commerciaux, etc.)

Premier conseil

- **Choisir son adversaire**
  - Ex : essayer de se protéger de la NSA... quand même un amateur peut rentrer sur votre réseau

Les leurres du « dark web » et la *threat intelligence*

- **Quelques apports**
  - Surveillance et récupération des fuites de bases de données contenant des empreintes de mots de passe (mais souvent largement diffusées)
  - Ajout de signatures pour les anti-virus
- **Limites**
  - Les canaux de communication des attaquants sérieux ne sont pas trivialement accessibles
  - Les outils disponibles sur le « dark web » utilisent pour la plupart des concepts déjà bien connus et sont rarement innovants
- **La *threat intelligence***
  - Des analyses intéressantes
  - Mais limitées par l'interdiction du « Hack Back »

    Evolution possible aux US
    https://www.usnews.com/news/articles/2017-03-09/self-defense-bill-would-allow-victims-to-hack-back

    Déjà effectué en pratique

Paranoïa et sécurité opérationnelle

- **Se considérer comme faible et vulnérable**
  - Petits groupes segmentés
  - Rester sous le radar
- **L'anonymat sur Internet**
  - Illusoire de penser être anonyme sur tous les aspects de sa vie
  - Mais une segmentation technique et opérationnelle permet d'isoler vos activités à risque
  - Apports et limites des réseaux d'anonymisation
- **Ne pas faire confiance aux prestataires tiers**
  - Malgré les discours commerciaux, les prestataires ont d'autres priorités que la confidentialité de vos informations
  - Surtout si la législation locale est hostile
  - Les hébergeurs sont une cible de choix
- **Partir du principe que tout sera découvert**

Les beaux jours à venir des attaques informatiques

- **Attribution difficile...**
  - … réaction difficile
- **Guerre de l'ombre**
  - Pas de victime corporelle
  - Plus facile à faire accepter dans certaines démocraties que les guerres ouvertes
  - « no logz, no crime »
- **L'information est un levier de pouvoir majeur**
  - R&D, stratégie, etc.
  - Opérations d'influences d'autant plus efficaces qu'elles se basent sur des informations vraies (ex : campagne présidentielle 2017, Wikileaks, etc.)
  - Le sabotage reste encore rare aujourd'hui
- **Mais nécessite de plus en plus de moyens**
  - Augmentation des moyens des attaquants et des défenseurs
  - Technicité grandissante (ex : MS17-10 VS MS08-67)
  - Mais généralisation des objets connectés, parfois plus vulnérables

AVEZ-VOUS DES QUESTIONS ?

MERCI DE VOTRE ATTENTION,

SYNACKTIV
DIGITAL SECURITY