INTRODUCTION À LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

I-TRACING

TELECOM nancy

Ingénieurs du numérique • Inspiring your digital future

SOMMAIRE

INTRODUCTION

INTRODUCTION
WHOAMI

2015 – Ingénieur diplômé TELECOM Nancy (TRS)

Depuis 2015 – Auditeur sécurité I-Tracing

Depuis mars 2017 – Membre de la section opérationnelle de la Réserve Citoyenne de Cyberdéfense

(je ne travaille pas comme ça)

Depuis avril 2017 – ISO 27001 Auditor

Mais aussi :

Bug hunter

Electronic Hacker

Geek

Introduction
Contact

@MickaelWalter

https://www.kilawyn.fr

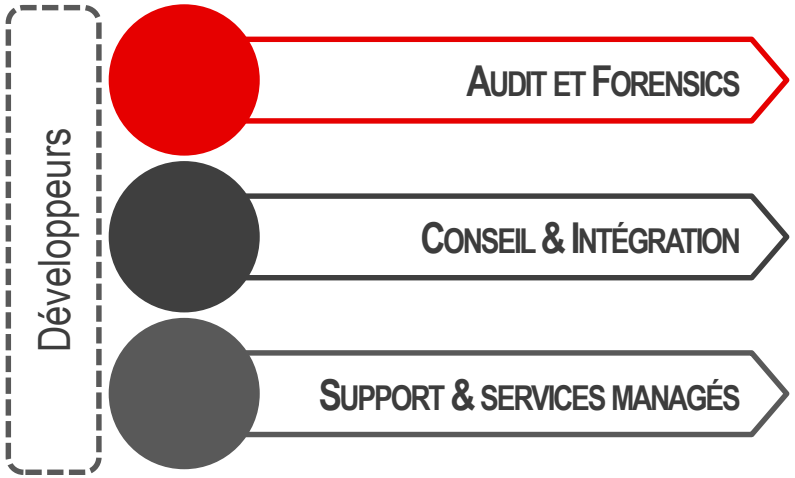
@Kilawyn@mastodon.xyz

mickael.walter@telecomnancy.net

https://fr.linkedin.com/in/mickaël-walter-531b18109

Société française (SAS) fondée à Paris fin 2005 entièrement indépendante

- Société spécialisée dans la **Sécurité** et la **Traçabilité** des Informations et des Systèmes d'Informations

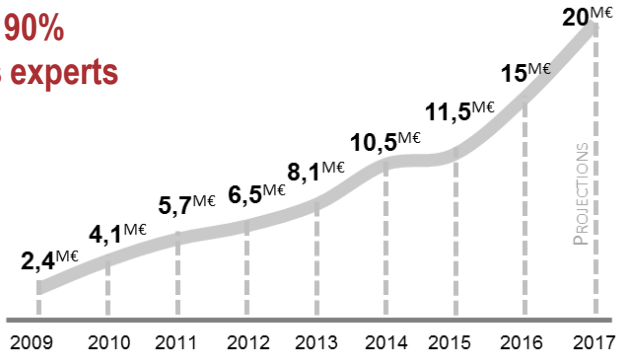


Plus de **150 Clients** Grands Compte, dont **50% du CAC 40**
Aucun ne représente plus de 9% du CA

Présence à l'international via **I-TRACING ltd** et **I-TRACING APALIA**

Près de 100 collaborateurs dont **plus de 90% d'ingénieurs experts**

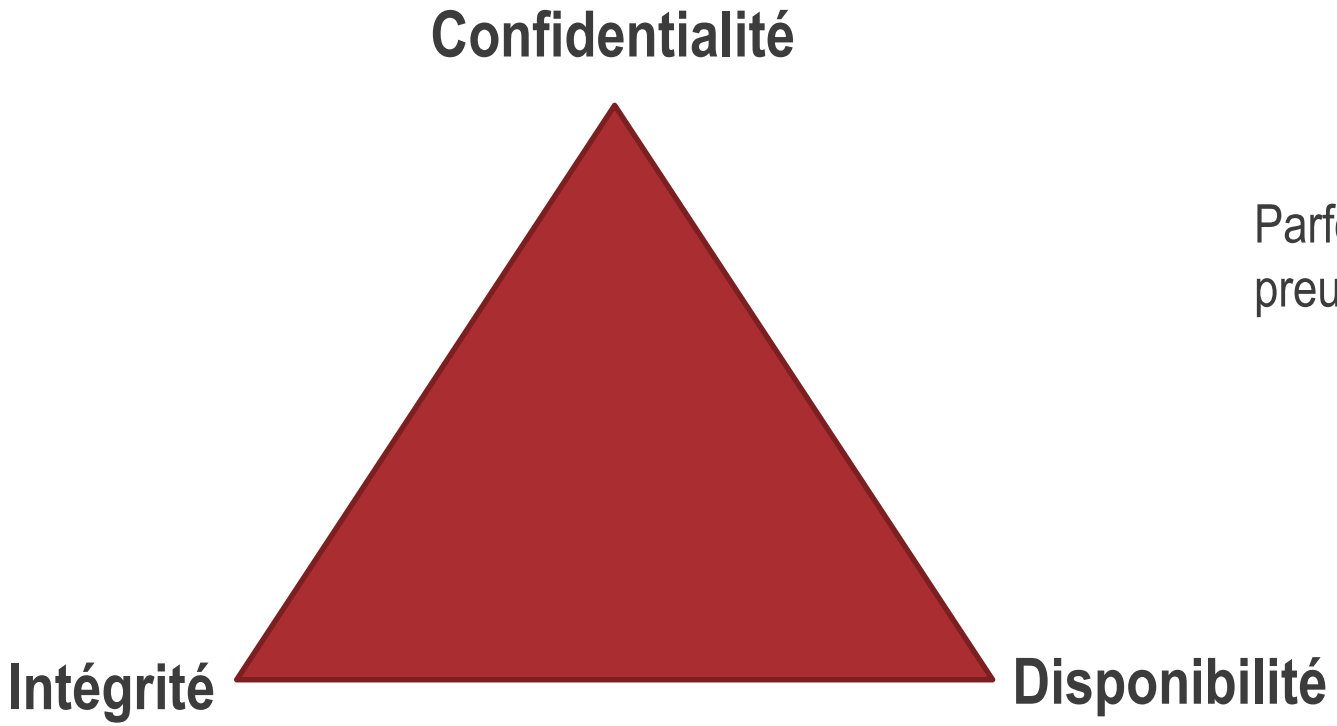
Membre fondateur du CESIN
Et du CSA cloud security alliance®



Croissance résistante

SECURITY 101

- Sécurité de l'information
  - Pas uniquement sur support informatique mais aussi papier !



Parfois on inclut aussi preuve (ou traçabilité)

SECURITY 101
JARGON

- Confidentialité :

- Intégrité :

TV5MONDE

In The Name of Allah, The Most Beneficent, The Most Merciful, CyberCaliphate continues its CyberJihad against the enemies of Islamic State.

Hollande, you've made a great mistake! You've send your military to serve sneaky American kuffar in a footless war with our brothers.

That's why Parisians received January "gifts" in Charlie Hebdo and kosher supermarket from our brothers mujahideen Cheriffe and Said Kuashi and Amedi Coulibaly may Allah accept them.

Now, with Allah's permission CyberCaliphate hunts for families of French soldiers from naval base Peace Camp and from aircraft carrier Charles de Gaulle who sold out themselves to Americans.

French Kuffar, if you want to save your families you'd better stay out of war against the Islamic State. It's the only way you can keep a whole skin and insure your relatives from retaliation.

Today we disrupt the TV5Monde channel and publish French department's confidential data.

With Allah's permission we'll continue fighting USA and its butlers. CyberCaliphate and Islamic State Hacking Division prepare new "gifts" for you.

There's no God but Allah and Muhammad is His Prophet! There is no law but Sharia!

- Disponibilité :

- Faille : défaut induisant une atteinte à la sécurité
- Impact : conséquences d'une exploitation (CID)
- Probabilité de survenance : ~ difficulté d'exploitation

Vulnérabilité = Faille * Impact

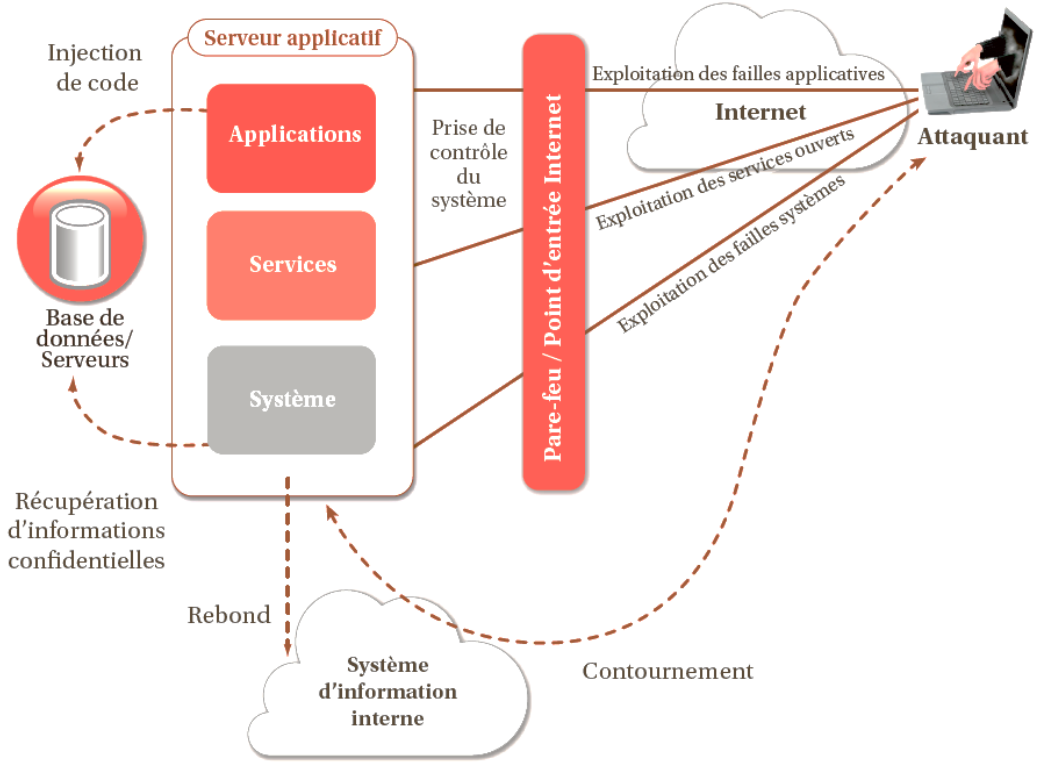
Risque = Vulnérabilité * Probabilité de survenance

Impact/Exploitation	Avancée	Elevée	Modérée	Simple
Mineur	Mineur	Mineur	Modéré	Modéré
Modéré	Mineur	Modéré	Modéré	Majeur
Important	Modéré	Majeur	Majeur	Critique
Très Important	Majeur	Majeur	Critique	Critique

SECURITY 101
CYCLE DE LA SÉCURITÉ

- Simuler le comportement d'une personne malveillante tentant d'attaquer depuis Internet

- Successivement :
  - En boîte noire *(sans aucune information de manière à simuler le comportement d'un attaquant externe)*
  - En boîte grise *(avec des comptes valides correspondant aux 3 profils utilisateurs représentatifs permettant d'accéder aux différents écrans de manière à simuler le comportement d'un utilisateur malveillant (ou d'un attaquant externe qui aurait réussi à récupérer des credentials valides).*



SECURITY 101
DÉROULEMENT D'UN TEST D'INTRUSION

Préparation
- Signature d'une convention autorisant les tests
- Définition avec le client des points d'attention

Reconnaissance
- Découverte de l'application
- Recherche d'informations sur Internet

Intrusion
- Découverte des vulnérabilités
- Exploitation des vulnérabilités pour établir des scénarios de risque

Restitution
- Ecriture du rapport
- Proposition de mesures correctives

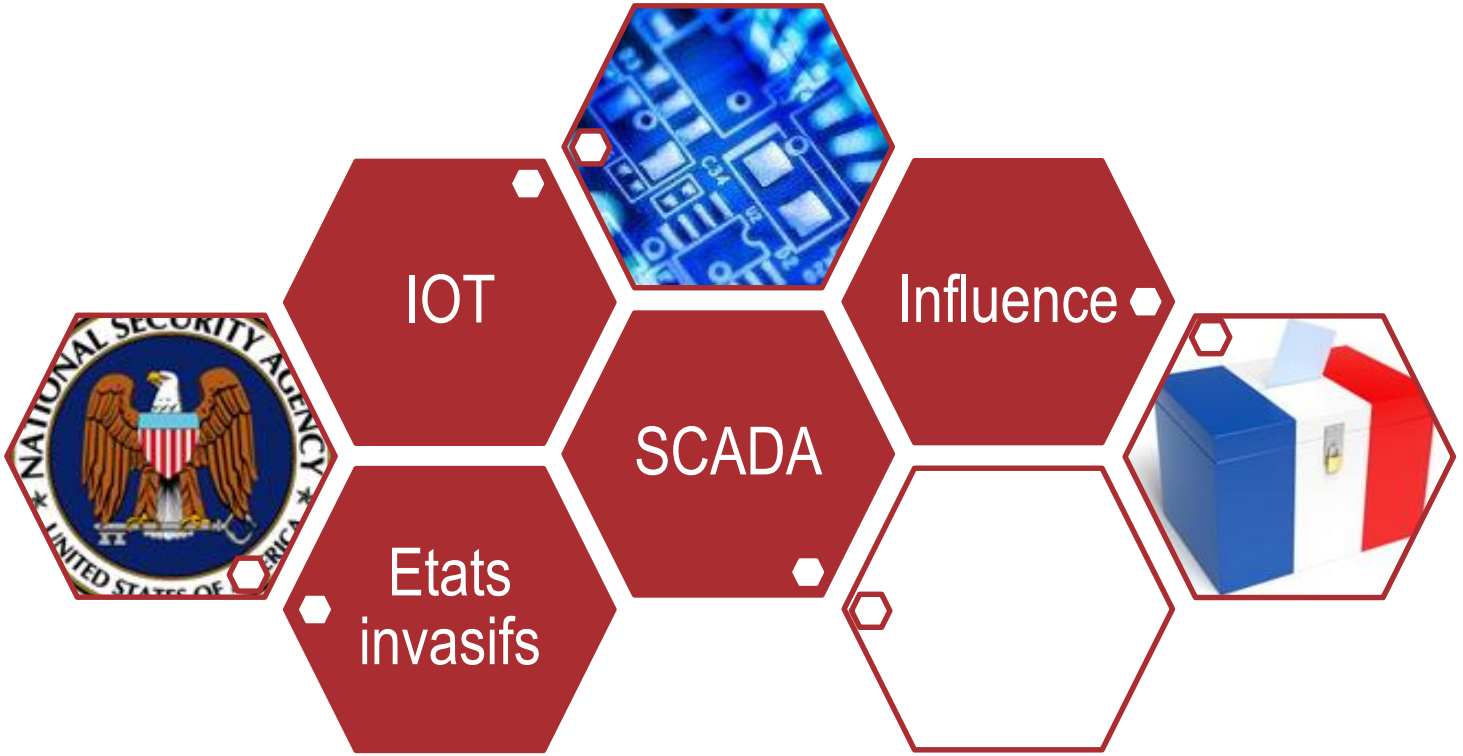
- Flexibilité :
  - Diversité des missions (technologies, types d'audits, etc…)
  - Horaires parfois contraignants (tests hors heures ouvrées, etc…)
- Curiosité :
  - De nombreuses technologies à connaître
  - Des métiers différents à découvrir
- Rigueur :
  - Un audit est fondé sur des preuves
- Intégrité :
  - L'auditeur doit rester impartial
  - Les informations collectées sont en général confidentielles

ENJEUX

- Les enjeux sont différents selon le contexte métier :
  - Boutique en ligne : une perte de disponibilité résulte en une perte rapide de Chiffre d'Affaires
  - Banque : une perte de confidentialité peut être dramatique pour ses clients
  - Cabinet de notaire : une perte d'intégrité peut avoir des conséquences néfastes pour les procédures officielles
- Mais un seul élément des CID suffit à des pertes conséquentes

Enjeux
Enjeux communs

ENJEUX
NOUVEAUX ENJEUX



ETUDES DE CAS

TV5 MONDE
CONTEXTE

- 8 avril 2015 vers 20h : les serveurs d'encodage s'arrêtent
- S'ensuivent une série de pannes de différents services
- Les comptes des réseaux sociaux de TV5 Monde sont piratés
  - Ils affichent des messages à la gloire du Djihad

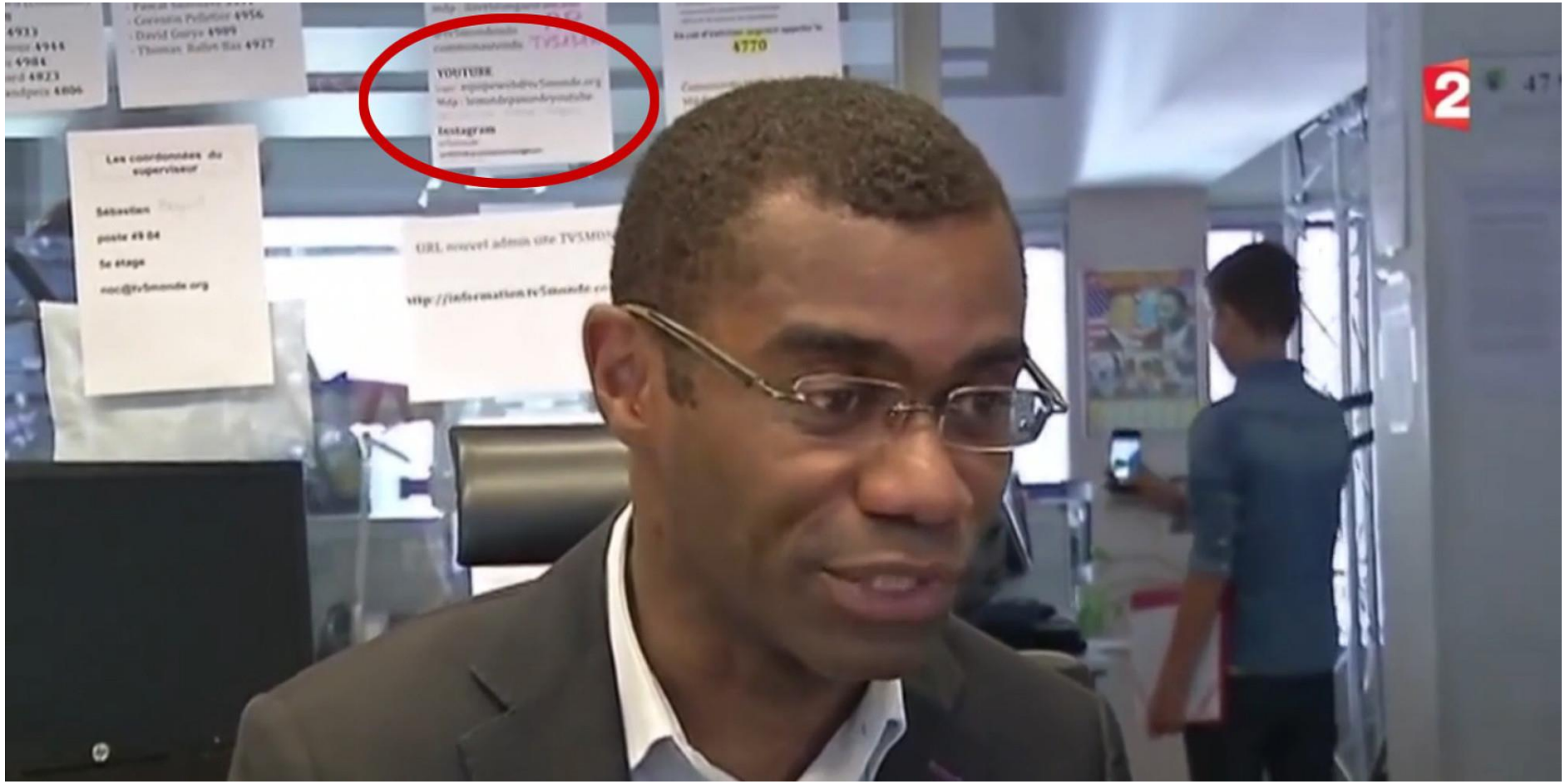
TV5 Monde
Déroulement de l'incident

- L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est appelée à la rescousse
- Simultanément tout le système informatique est arrêté
- Des informations sont supprimées :
  - Y compris certains firmwares : sabotage
- L'intervention permet le rétablissement du SI
  - Le 9 avril vers 5h, les 12 chaînes diffusent un programme unique
  - Vers 10h chaque chaîne retrouve sa programmation
  - Vers 18h le journal peut à nouveau être diffusé en direct
- L'intervention de l'ANSSI s'est terminée en juillet
  - Mais prise de relais par des entreprises privées

TV5 Monde
Raisons de l'incident

- Plusieurs erreurs :
  - Mots de passe des comptes de réseaux sociaux diffusés… sur TV5 Monde
  - Sensibilisation du personnel insuffisante (diffusion de malwares)
  - Vulnérabilités non corrigées présentes sur Internet
  - Absence de cloisonnement entre les réseaux de diffusion et de bureautique
- Mais :
  - Attaque d'envergure préparée longtemps à l'avance
  - Volonté de destruction de la chaîne

TV5 Monde
Comment ne pas stocker des mots de passe



TV5 MONDE
UN MALWARE SPÉCIFIQUEMENT CONÇU POUR L'ATTAQUE

```
on error resume next

'#########################################################################

'<[ Recoder : Security.Najaf (c) skype : Security.Najaf ]>

'<[ Credits : NjQ8 and Mr.Hacker ]>

'<[ Thanks For : JoHn.Dz ]>

'#########################################################################

' \\ Configuration ~
'_____________________________________
dim shell
set shell = WScript.CreateObject("WSCRIPT.SHELL")
dim fs
set fs = WScript.CreateObject("Scripting.filesystemobject")
dim installname
installname = "SecurityNajaf.vbs"
dim dir
dir = "Temp"
path = shell.ExpandEnvironmentStrings("%" & dir & "%") & "\"
```

TV5 Monde
Attribution de l'attaque

- L'attribution : jamais simple
  - Facile d'imiter un autre groupe pour brouiller les pistes
  - Facile de se cacher pour ne pas être découvert
  - Difficile de rassembler des preuves sur des équipements compromis
- Initialement : « Cyber Califate »
  - Diffusion de messages pro-daesh
  - Utilisation de malware à priori Irakien
- Résultats de l'enquête (non sûr) : « APT28 »
  - « Advanced Persistent Threat »
  - Groupe à priori Russe proche des services secrets
  - Possibles représailles des actions françaises en Ukraine

TV5 Monde
Coût de l'attaque

- Heures supplémentaires et coûts d'intervention: 4,6 M€
- Investissements dans la mise en place de sécurité :
  - 2016 : 3,1 M€
  - Années suivantes : 2,5 M€ / an
- Coûts indirects non inclus
- Problèmes récurrents :
  - Sous-investissements en sécurité (« pas productif »)
  - Décalage technologique entre le personnel et l'informatique
  - Simplification abusive dans le déploiement de réseaux

TV5Monde
Sources

- Rapport d'activité 2015 de l'ANSSI : https://www.ssi.gouv.fr/uploads/2016/09/rapport_annuel_2015_anssi.pdf
- Surcoût pour TV5 Monde : http://www.lemondeinformatique.fr/actualites/lire-cyber-attaque-un-surcout-de-4-6-meteuro-pour-tv5-monde-en-2015-64096.html
- Analyse du malware utilisé : https://www.bluecoat.com/security-blog/2015-04-09/visual-basic-script-malware-reportedly-used-tv5-monde-intrusion

TV5 Monde
Sources

- Lien avec APT28 : http://www.lemondeinformatique.fr/actualites/lire-piratage-de-tv5-monde-la-piste-russe-se-precise-61430.html

MIRAI BOTNET
CONTEXTE

- Fin septembre 2016 : le + gros DDoS de l'histoire
- Cible : l'hébergeur français OVH
- Débit : 1 Tbit/s
- Botnet utilisé : Mirai
  - Malware infectant les webcams non sécurisées
  - Création d'un réseau botnet avec une immense capacité en débit
- Nombre de caméras utilisées : plus de 145 000
- Conséquences : légers ralentissements du réseau OVH, une telle attaque était anticipée

- Le code source de Mirai libéré quelques mois après
- Nouvelle compréhension des enjeux envers les DDoS :
  - Utilisation de l'IoT
    - Relativement mal sécurisé
    - Objets très nombreux
    - Souvent directement connectés à Internet
  - Disponibilité d'une gigantesque bande passante
- Naissance de nombreuses problématiques de sécurité avec l'IoT

- La goutte DDoS n'a pas fait déborder le VAC : https://www.ovh.com/fr/blog/ovh-resiste-attaque-ddos-vac
- Mirai botnet linked to massive Dyn DDoS attacks : https://www.hackread.com/mirai-botnet-linked-to-dyn-dns-ddos-attacks/
- Mirai IoT botnet code release : http://www.computerweekly.com/news/450400311/Mirai-IoT-botnet-code-release-raises-fears-of-surge-in-DDoS-attacks

VAULT 7 ET SHADOWBROKERS
CONTEXTE

- 2 fuites de documents et outils de la CIA et la NSA :
  - Vault7 : documents et outils internes à la CIA
  - ShadowBrokers : groupe mystérieux ayant diffusé des outils de la NSA
- Vault7 :
  - Publication de documents par Wikileaks le 23 mars 2017
  - Comprend : malwares insérés à la production, espionnage par téléviseur Samsung, espionnage de téléphones
- ShadowBrokers :
  - Publication initiale de quelques exploits firewall le 13 août 2016
  - Prétend avoir piraté l'Equation Group (équivalent américain d'APT28)
  - Publication complète le 8 avril 2017 après des enchères ratées

- Rien de bien neuf depuis Snowden
- Mais :
  - Exploits non patchés (0days) dans la nature
  - Outils de guerre à disposition du public
  - Recrudescence d'attaques sur les environnements Windows
  - Patch en urgence de Microsoft, Oracle ou encore les différents constructeurs de firewalls
- Détermination formelle de l'identité de l'Equation Group

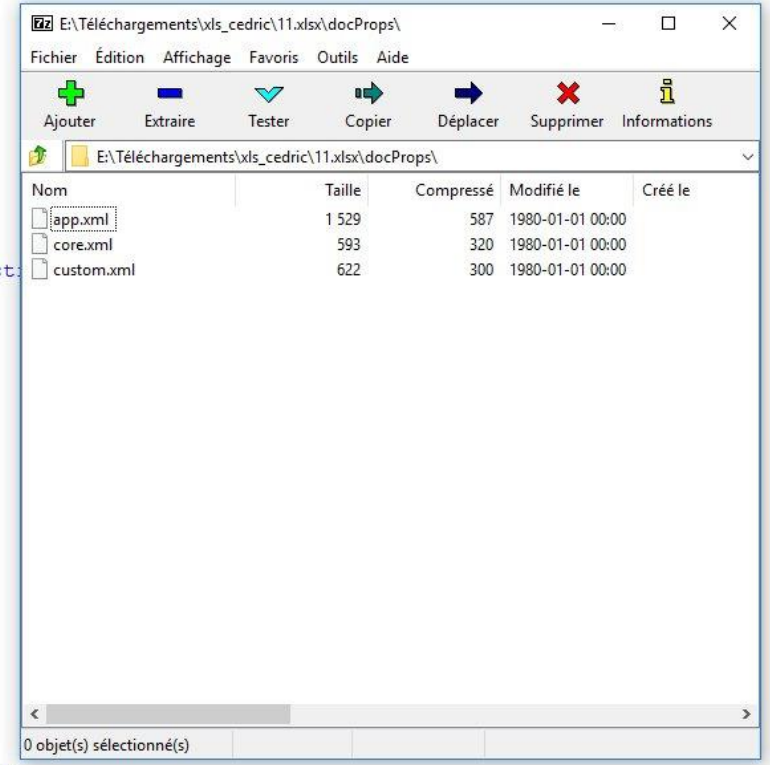
- Utilisation des malwares : https://www.nextinpact.com/news/104098-shadow-brokers-malwaredoublepulsarde-nsa-sur-nombre-croissant-machines.htm
- Deuxième vague des ShadowBrokers : http://www.lemonde.fr/pixels/article/2017/04/11/the-shadow-brokers-devoilent-de-nouveaux-outils-de-la-nsa_5109618_4408996.html
- Contenu de Vault7 : https://wikileaks.org/ciav7p1/cms/index.html

Macron Leaks
Contexte

- Elections présidentielles françaises de 2017
- Le 5 mai, une 20aine de minutes avant le silence des équipes de campagne
- Contenu de 6 boîtes mail de hauts responsables d'En Marche!
- Premières analyses :
  - Rien de compromettant pour E. Macron
  - Du faux si on se fie aux métadonnées des documents Office comprenant des noms russes (sociétés d'informatiques proches des services secrets)
  - Attention : pas d'attribution à la Russie à cette heure
- Exemple de tentative d'ingérence
- Attaque basique : phishing

MACRON LEAKS
MÉTADONNÉES RUSSES

```
<DocSecurity>0</DocSecurity>
<ScaleCrop>false</ScaleCrop>
<HeadingPairs>
    <vt:vector size="4" baseType="variant">
        <vt:variant>
            <vt:lpstr>Листы</vt:lpstr>
        </vt:variant>
        <vt:variant>
            <vt:i4>9</vt:i4>
        </vt:variant>
        <vt:variant>
            <vt:lpstr>Именованные диапазоны</vt:lpstr
        </vt:variant>
        <vt:variant>
            <vt:i4>7</vt:i4>
        </vt:variant>
    </vt:vector>
</HeadingPairs>
<TitlesOfParts>
    <vt:vector size="16" baseType="lpstr">
        <vt:lpstr>RECAP</vt:lpstr>
        <vt:lpstr>JAM</vt:lpstr>
        <vt:lpstr>Opérations</vt:lpstr>
        <vt:lpstr>Meetings</vt:lpstr>
        <vt:lpstr>Strat&amp;com</vt:lpstr>
        <vt:lpstr>Afgé</vt:lpstr>
        <vt:lpstr>déplacements</vt:lpstr>
        <vt:lpstr>vs 2012</vt:lpstr>
        <vt:lpstr>campagne</vt:lpstr>
        <vt:lpstr>Afgé!Область_печати</vt:lpstr>
        <vt:lpstr>JAM!Область_печати</vt:lpstr>
        <vt:lpstr>Meetings!Область_печати</vt:lpstr>
        <vt:lpstr>Opérations!Область_печати</vt:lpstr>
        <vt:lpstr>RECAP!Область_печати</vt:lpstr>
        <vt:lpstr>'Strat&amp;com'!Область_печати</vt:lpstr>
        <vt:lpstr>'vs 2012'!Область_печати</vt:lpstr>
    </vt:vector>
</HeadingPairs>
```



eXtensible Markup Language file | length : 1724 lines : 46 | Ln : 46 Col : 14 Sel : 0 | 0 | Dos\Windows | UTF-8 | INS

Macron Leaks
Sources

- Pourquoi les experts privilégient la piste russe : http://www.leparisien.fr/elections/presidentielle/piratage-de-l-equipe-macron-pourquoi-les-experts-privilegient-la-piste-russe-09-05-2017-6931416.php
- MacronLeaks Pollution Hackeuse : http://www.liberation.fr/france/2017/05/07/macronleaks-pollution-hackeuse_1567922
- Comment manipuler du PDF (Hors sujet mais intéressant) : https://lafibre.info/bistro-sujet-libre/metadonnees-pdf/

SE SÉCURISER

- Mettre en place une politique de la sécurité du SI
- Réaliser régulièrement des audits de sécurité
- Investir dans des équipements de sécurité
- Sensibiliser les utilisateurs
- Demander à l'ANSSI : https://www.ssi.gouv.fr/entreprise/guide/guide-des-bonnes-pratiques-de-linformatique/

SE SÉCURISER
PARTICULIER

- Ne pas réutiliser son mot de passe (utiliser un coffre-fort)
- Vérifier l'identité d'un site avant chaque action critique
- Se renseigner sur les techniques des attaquants
- Demander à l'ANSSI :

https://www.ssi.gouv.fr/particulier/precautions-elementaires/

SE SÉCURISER
PARTICULIER

POUR ALLER PLUS LOIN

POUR ALLER PLUS LOIN

- Développer ses compétences techniques :
  - Nourrir sa curiosité, rechercher
  - Participer à des challenges (Root-Me, CTF, etc…)
  - Participer à des Bug Bounties
  - Participer à des évènements (Nuit du Hack, ESE, GreHack, etc…)
- Se documenter (forums de hacking, TOR, etc…):
  - Penser à se protéger : VPN, TOR browser, etc…

POUR ALLER PLUS LOIN
PISTES…

- Root-Me : https://www.root-me.org
- Challenge du logo de l'ANSSI : http://blog.bienaime.info/2015/01/le-challenge-du-logo-anssi.html
- Exploit-DB : https://www.exploit-db.com
- Kali : https://www.kali.org

MERCI
DES QUESTIONS ?