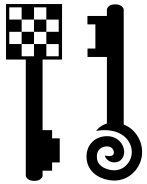
"Retour vers le futur : bienvenue en 1984 ?"
JSSI 2016

Retour d'expérience sur la lutte contre le cyber-espionnage (étatique ?)

Laurent OUDOT
Directeur de TEHTRIS



1) PLAN ET INTRODUCTION

Objectif de cette présentation

- Partager quelques éléments d'une expérience liée à la lutte contre le cyber-espionnage (étatique ?)
  - Dans la plupart des cas, il est difficile de positionner l'élément « étatique » avec certitude
- Proposer des exemples d'affaires traitées par les membres de TEHTRIS dans ce contexte
  - Essayer d'éviter les histoires déjà connues sur le cyber, etc
  - Participer au débat, humblement contribuer à des réflexions sur comment lutter et se défendre

Intervenant

- Laurent Oudot
  - Carrière étatique
    - Ancien ingénieur-chercheur au CEA
    - Ancien expert opérationnel de la DGSE
  - Speaker & Instructeur
    - Blackhat, Cansecwest, Defcon, HITB, Syscan…
  - Directeur de la société TEHTRIS
    - Lutte technique contre le cyber-espionnage
      - Glaive : Pentests…
      - Bouclier : Surveillance… ➔ eGambit

Avis

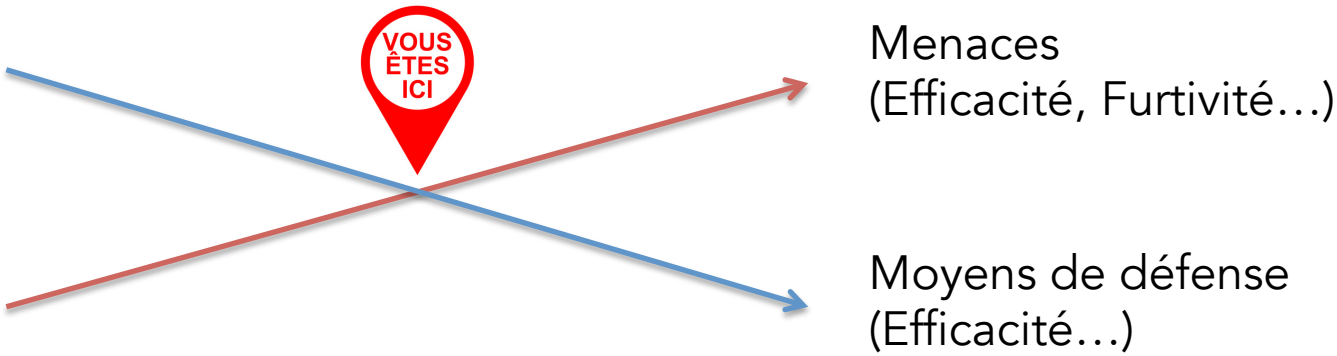
- Aucun lien entre cette présentation et mon ancienne carrière étatique
  - Merci de ne pas faire de raccourcis enfantins ☺
- Certaines informations sont modifiées / adaptées pour des raisons de confidentialité
- Pas d'expertise juridique
  - Ne pas tenir compte des aspects légaux éventuels, ceci n'est qu'une présentation, dans un contexte et dans un temps imparti

Réalité des menaces

- Dépendance sans limite aux mondes numériques, avec perte du contrôle technologique et évolution des menaces
  - « La sécurité est un échec © » et les exemples sont nombreux !
    - Il est très facile de construire un outil d'attaque invisible (un temps) pour l'ensemble (ou presque) des antivirus dans le monde
      - Simplicité du piratage des Endpoints, etc
    - Il est très facile de pirater un réseau (local), car en général les bases de la sécurité ne sont pas en place
      - Dhcp snooping, DAI, IPSG, 802.1X/NAC, Flux chiffrés, IPv6, Netbios, WPAD, déplacements latéraux en tous genres, exploits…

Réalité des menaces

- Les menaces sont réelles
  - Espionnage, Sabotage, Criminalité Organisée
- La violence est en pleine croissance
  - Tendance 2015 → 2016



« *Shall we play a game ?* »

Plan

- 1) Plan et introduction
- 2) Exemples de lutte contre des risques de type cyber-espionnage
  - Attaques/Visites/Vols physiques et impacts associés, Fraudes avancées…
- 3) Se protéger ? Principes simples et postures humaines
  - Comment (essayer de) (rêver qu'on puisse) (réellement) s'en sortir ?

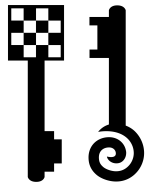
2) Exemples de luttes contre des risques de type cyber-espionnage

c2f3792eee213f0515eb9b4fe3cc6a8a[illegible]f65f8c0dac8f6c5d66eb8fd3d919

ATTAQUE DE « HACHES » ?

Attaque de haches

- *Hashes* != Haches
- Description
  - Pays étranger en pleine crise
  - Attaque dans une ville. Troubles forts.
    - Machettes et haches
  - Panique générale : sécurité physique == 0
  - Infiltration totale dans une entreprise sensible
  - Datacenter compromis physiquement
  - Serveur « AD » compromis ?
    - Récupération des disques puis autopsie TEHTRIS
  - Réflexions intéressantes sur les menaces
    - Limites de la sécurité physique & logique



Bombes analogiques ?!

- Sujet immédiat « naturel »
  - Sur le sujet des VMs dans des hyperviseurs « compromis » localement, peut-on détruire à distance tout ou partie d'un centre de données déployé dans une zone potentiellement instable ?
    - Le chiffrement peut ne pas suffire s'il est potentiellement connu en local (passwords, boot autorisé, attaque de la RAM…)
- Avantages
  - Meilleure certitude sur le devenir des informations localement présentes
- Inconvénients
  - Quid du risque d'avoir une bombe logique en permanence dans ses machines ?
- Autres pistes moins critiques
  - Avoir une cryptographie liée à des éléments distants, accédés par le réseau ou d'autres solutions techniques

Et dans un Cloud ?

- Peu de solutions qui soient simples à déployer et à manager, avec une forte compatibilité quelque soit le matériel
- Exemple de problème : mémoire vive
  - Si une infrastructure Cloud était piratée (un opérateur Cloud)
    - fortement attaquée physiquement, etc
  - Comment réussir à tenir ou à être (plus ou moins) certain qu'un intrus local ne pourra pas remonter à la totalité de la machine ?
    - Idée: éteindre à distance la machine si possible, mais quid de la situation où l'accès communication serait perdu ?
      - L'option « si PING error, alors KILL » ne marche pas ☺
        - » Exemple: Tempêtes de sable
      - L'option communication alternative se pratique visiblement parfois
        - » Exemple: Modem avec un numéro précis...

Mémoire vive du Cloud ?

- Mission presque impossible sur un Hyperviseur standard (?)
- Quelques exemples de solutions +/- publiques
  - « PrivateCore »
    - RAM chiffrée (AES) ←→ Hyperviseur dans le cache CPU
      - Racheté par Facebook en 2014
  - Intel SGX / Software Guard Extensions : Enclaves
    - https://software.intel.com/en-us/blogs/2013/09/26/protecting-application-secrets-with-intel-sgx
      - Quid de l'utilisation des enclaves par un malware, afin de se cacher ? Quid des i/o entre processus dans les enclaves ? …
  - …

Réflexions

- Bel exemple où la sécurité physique ne marche plus (#FAIL) et sur l'impact associé
- Serveurs, Mémoire, Cloud, etc
  - Pas de superbes solutions simples
  - Suivre les recommandations des constructeurs
  - Faire confiance à des tiers ? (déporter le risque)
- Ne pas déporter la totalité des informations dans les sous-zones à risque
  - Exemple tous les comptes informatiques au niveau monde, ne devraient pas être en local dans une sous entité
- Ne pas habiller une zone trop exposée ou à risque avec des informations sensibles non protégées de manière forte
  - Utiliser des outils de chiffrement pour ralentir les agresseurs
    - Les attaques sur des données en mode « offline » sont freinées
- Avoir des procédures pour traiter ces situations de crises
  - Mais en pratique, cela n'est plus suffisant, et le facteur humain est globalement imprévisible en cas de danger physique

VISITE DU WIFI

De gentils visiteurs

- Usine ultra sensible
  - Secrets industriels
  - Environnement technique complexe
- Négociations internationales
  - Visiteurs « contrôlés »
    - Identités demandées à l'avance
      - Intégration d'une personne au dernier moment : impossible / complexe de refuser « commercialement »
    - Surveillances et déclarations diverses, criblages…
    - Règles et conduites à suivre sur site
      - Sécurité physique liée à l'environnement
      - Autres aspects sécurité (laisser son "matos" à l'entrée)

Téléphone Maison

- Pendant la visite
  - Nouvelle adresse MAC vue sur un réseau Wifi ouvert (non sensible) en plein cœur du site
    - A priori un téléphone
    - Client DHCP classique
  - Puis, passage en mode « funky »
    - Scan automatique des adresses IP dans la plage des adresses IP associée (ICMP, TCP plusieurs ports…)
    - Arrivée automatique sur un honeypot de TEHTRIS
  - Alerte TEHTRIS en direct : escalade "Sûreté"
    - Visite mise en pause. Re-fouille des visiteurs (au risque hélas, de froisser commercialement). Un téléphone portable est trouvé. Excuses polies fournies ☺
    - Téléphone ramené à l'accueil le temps de la visite

Réflexions

- Les visites/passages en milieux sensibles sont de vraies opportunités pour glaner de l'information (au minimum)
- Ne pas hésiter à travailler avec les services étatiques qui peuvent éventuellement assister sur des contacts à risque
  - Ministères de l'Intérieur et de la Défense
- Ne pas hésiter à mettre en place des mesures de surveillance (& cloisonnement) de tout ordre, en particulier sur les zones sensibles et/ou exposées
  - Honeypots, Logs, NIDS, Netflow…
- Ne pas hésiter à avoir des procédures claires sur la gestion de ces situations
  - Rôles et responsabilités définis à l'avance

MIELLEUSE RENCONTRE

Collaboration

- Collaborations commerciales nécessitant la présence de plusieurs ingénieurs
  - Avec leur propre équipement informatique
  - Proposition de prêt de laptops pour éviter d'introduire des machines externes
    - Refus divers : clavier, outils « maisons », data, etc
  - Zonage terrain avec prise en compte des visiteurs
    - Aspects humains
      - La vigilance chute dans le temps, voire, la vigilance devient mal vue en local (être suspicieux = être méchant ?)
    - Aspects techniques
      - Bâtiment, salle, accès au réseau pour échange de rapports

Détection

- Observation par l'entreprise de trafic sortant non commun et non identifié en provenance de la zone
- Demande d'intervention de TEHTRIS
  - Découverte : le zonage réseau n'est pas nominal
    - Imperfections techniques, avec risque de rebond sur des réseaux a priori non connectés directement
    - Soucis de sécurité physique
      - Imprimantes & VLANs, sécurité logique, etc.
  - Problème : « on ne peut plus interdire l'accès au réseau, et les visiteurs ont au moins un accès officiel pour sortir qu'on ne peut pas leur changer »
  - Urgence: actions de nuit → reconfiguration de la matrice
    - Création d'un faux réseau complet, avec des centaines de machines ayant le même profil que le réseau normal avec pour objectif d'étudier voire de réagir

Surveillance

- Comportement normal le matin
  - TEHTRIS laisse le faux réseau en place, avec émulation de faux paquets comme sur le faux réseau (présence des copains windows, etc) et émulation du trafic d'inventaire qui vient régulièrement voir toutes les IP en ICMP + SNMP
- Puis un des postes des visiteurs se met à agir d'une manière différente
  - Sortie sur le proxy avec deux types de « User-Agent » principaux différents (OS) depuis un même laptop
  - Quelques paquets sont envoyés sur le réseau vers des machines locales. Assez simple, a priori pas offensif (UDP/TCP Windows), et difficile de déterminer que ce soit une action offensive.
  - La surveillance passive continue.

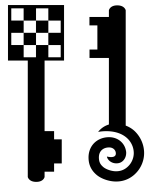
Sniff ☹

- Puis, brusquement, ce poste se met à répondre à des paquets ICMP envoyés à son IP, mais avec une légère erreur d'adresse MAC dedans
  - Résultat obtenu par le faux inventaire actif.
    - Faux exemple avec scapy() pour 00:3C:59:C0:FF:34
      - » ans,unans=srp(Ether(dst="00:3C:59:C0:FF:33")/IP(dst="192.168.1.26")/ICMP(), timeout=0.1, retry=0)
      - » ans.summary()
  - A priori : il s'agit d'une carte passée en mode « promiscuous » ou d'un effet de bord particulier
  - Discussion avec les équipes de « Sureté »
    - Décision d'envoyer de faux flux sur le réseau
      - Comportement changeant sur un des visiteurs
      - S'il(s) voulai(en)t de la data (ou pas), ce fut le cas (ou pas)
        - » Quand « /dev/urandom » devient ton meilleur ami
  - Suite en dehors de la zone (…)

Réflexions

- Il est clairement évident que les affaires de cyber espionnage les plus simples, avec des acteurs pas forcément trop forts, sont celles effectuées à distance
  - Moins risquées, relativement furtives, peu chères
- Néanmoins, dans certains cas, et/ou pour certains pays/acteurs, il peut être plus simple de se déplacer pour mener une agression
  - Sécurité physique basique
    - En général il n'est pas difficile de rentrer quelque part
  - Sécurité logique minimaliste
    - Attaques ARP, ICMP, DHCP, IPv6… Admins… Credentials… Patch Management… Zonage réseau… Rebonds partout…
    - Utilisation d'un premier point simple comme source de rebond vers un grand réseau mondial
      - Exemple: un point perdu dans le monde mais connecté au reste…

VOL DE LAPTOP

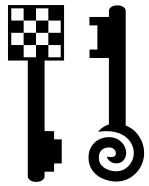


Intrusion physique

- Multinationale
- Sécurité physique réelle (et correcte)
- Un jour, un laptop disparaît dans une zone à accès réellement limité
- Visionnage vidéo-surveillance
  - Identification d'une personne assez fourbe
    - En train de téléphoner (?), visage jamais visible directement et/ou parfaitement sur la plupart des caméras (reconnaissance effectuée auparavant), etc
      - La personne ressort pas longtemps après, avec quelque chose
  - Forces de l'ordre contactées, etc

Gourmandise

- Puis : la même personne recommence la même opération (!) pour voler un autre laptop, toujours sur une zone ultra sensible
  - Interception physique
  - Garde à vue : /dev/null (!)
- TEHTRIS est mandatée pour étudier les risques d'espionnage sur récupération d'un laptop interne
  - Pas de chance : pas de FDE, et services Windows avec l/p et autres éléments/impuretés techniques laissant penser que posséder le laptop permettrait d'avoir des éléments pour simplifier une attaque



Réflexions

- Physique / Logique
  - Il peut exister (parfois) un lien évident entre la sécurité logique et la sécurité physique
  - La sécurité physique est parfois occultée dans le monde des « g33ks » et pourtant…
  - La « micro » faille de sécurité physique a été corrigée rapidement
  - Certaines failles de sécurité logiques sont parfois plus complexes à supprimer

LES CARTES AUX TRÉSORS

Fraude complexe

- Pays étranger
- Affaire très sensible
- Immense fraude organisée
  - Clonage de cartes bancaires, etc
  - Nombreuses pistes possibles
- Acteurs de différents mondes
  - Services de renseignement du pays impliqué
  - Banques concernées
  - …

Point Of Sales (POS)

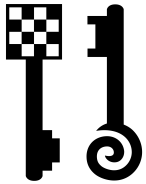
- Analyse des logs
  - Pas grand chose de trouvé
- Autopsies de machines sous Windows qui auraient pu être agressées
  - Découverte de sorte de « caches » sur le disque dur, avec des zones contenant des données sensibles censées être temporairement présentes puis détruites du disque dur
    - Eléments de type bancaires
    - Eléments techniques liés aux cartes bancaires (piste magnétique, « track 2 »)
  - Découverte de malwares capables de lire ces zones
    - Gros bug de conception au niveau « POS »
- Pentest à distance
  - Pas mal de « POS » sont connectés directement à Internet et il suffit de trouver leurs adresses IP (modems, etc) pour se nourrir d'informations

Remontée

- Analyses techniques
- Identifications de candidats
- Découverte d'autres attaques informatiques
- Décision prise au niveau bancaire
  - Création de « leurres bancaires » avec de fausses informations
  - Objectif : se faire voler ces informations, et traquer les achats effectués, tenter de remonter aux sources
  - Complexité juridique et administrative

Réflexions

- Sécurité ridicule type « pousse-au-crime »
  - Windows de base (XP, XP Embedded)
  - Pas d'audit des machines
  - Pas de protection au niveau infra
  - Pas toujours de chiffrement de bout en bout sur certains échanges et/ou dans les machines
    - Back-office / Front-office, Wifi…
- Importance réelle pour les individus et les entreprises
  - Achats (restaurants, hôtels, …)
- L'appel du gain à outrance fait parfois oublier la sécurité informatique et les conséquences peuvent être terribles



AUTRES EXEMPLES

Autres « affaires »

- « Dark Hotel » ?
  - Forensics suite à des suspicions d'espionnage
- IP Spoofing (ciblé ?) sur Internet
  - Quand personne ne comprend rien…
- Attaques externes
  - Mots de passe « internes » vus sur des honeypots positionnés dans les DMZ
- Attaque interne depuis l'étranger
  - Analyses des logs, des flux, d'outils malveillants
    - Affaire non résolue, mais stoppée
- Recherche d'APT/Ransomware/… à l'échelle d'un parc au niveau mondial
- …

3) Se protéger ? Principes simples et postures humaines

Des exemples de postures positives et négatives observées par TEHTRIS, qui ont un impact sur le pouvoir d'une entité pour tenir à des menaces de type cyber-espionnage

A PROPOS DES POSTURES

Postures négatives

- Exemples de postures classiques perdantes observées, qui ont contribué au succès potentiel d'opérations de cyber-espionnage
  - Acheter des outils sans les éprouver techniquement, juste parce qu'ils sont connus et/ou que les vendeurs étaient efficaces
  - Ne pas faire appel à des experts techniques sur des questions à risques
  - Croire que l'on a fait appel à des experts mais se faire avoir et croire que l'on est en sécurité
  - Attendre et/ou garder ses failles connues en place en se justifiant : coûts, héritage, organisation, susceptibilité…
  - …

Postures gagnantes

- Exemples de postures gagnantes qui peuvent contribuer à perturber, endiguer, couper les opérations de cyber-espionnage
  - Toujours continuer de refuser l'inadmissible
  - Rechercher la vérité technique
  - Rester humble face aux menaces
  - Se remettre en question, se former, être en veille
  - Agir régulièrement
  - …

L'appel du Cloud

- La Crise économique pousse les investisseurs à des rationalisations au niveau de toutes les dépenses
  - Certains pensent que le passage au Cloud permet de ne plus avoir certains soucis de sécurité chez soi, car le Cloud est mieux protégé
- En pratique, TEHTRIS a observé
  - Des destructions totales d'entreprises
  - De l'espionnage simplifié dans certains cas
    - Pas de suivi des logs ☺ …
  - C'est un déport des problèmes, mais le Cloud n'a jamais réellement vendu que tout serait résolu

SOLUTIONS TECHNIQUES

Attaques étatiques

- Talk de Rob Joyce (TAO, NSA), 28/1/16, où il annonce qu'il suffit
  - d'une première faille non traitée (même une paraissant de moindre impact),
  - d'un protocole en clair,
  - de mots de passe faibles ou en dur dans des produits,
  - de BYOD,
  - de GTC bâtiments
  - ou sinon d'armes avancées (Quantum Insert)

Connaître son infrastructure

- Inventaire des ressources communicantes
  - Découvrir / Suivre les nouveaux équipements
    - Un pirate pourrait néanmoins y penser au niveau furtivité mais on lui rajoute une couche de danger potentiel
      - Adresses MAC
      - Applications DHCP (« udhcp »)
      - Nom de la machine via DHCP (« bt », « kali »…)
      - …
    - NSA : « *You know the technologies you intended to use in that network. We know the technologies that are actually in use in that network. Subtle difference. You'd be surprised about the things that are running on a network vs. the things that you think are supposed to be there.* »
- Auditer techniquement son infrastructure
  - Audits ponctuels/réguliers, automatiques/manuels, actif/passif, distants/agents...
    - NSA: « *Accès à privilèges, cloisonnement des réseaux et des données, mises à jour, whitelisting d'applications, mots de passe en dur et/ou en clair* »

Protéger son infrastructure

- Suivre et enregistrer les activité
  - Systèmes et applications
    - Qui accède à quoi, quand, comment, que se passe-t-il en permanence…
  - Réseaux
    - Qui parle à qui, quand, comment…
  - NSA: « *Another nightmare for the NSA? An "out-of-band network tap"— a device that monitors network activity and produces logs that can record anomalous activity —p lus a smart system administrator who actually reads the logs and pays attention to what they say.* »
- « Interagir » avec les intrus (ripostes / détections)
  - Systèmes et applications
    - Endpoint Security…
  - Réseaux
    - Honeypots…

Gérer les incidents

- Nombreux outils à utiliser
  - Forensics, Sandboxes, Threat Intelligence, Bases…
- Posture : l'attrition ou le secret ?
  - Secret : ne rien publier, ne rien partager, pour ne pas prévenir les attaquants car cela pourrait les aider, etc
    - Exemple: « Hacking Team » sur VirusTotal
    - Mais, peur classique == la vengeance du pirate
      - Il faut donc comprendre son niveau, ses besoins, ses outils, ses motivations, son style, etc
  - Attrition : publier, partager, et faire comprendre qu'on n'est pas le bienvenu
    - Exemple: « coût » d'un outil malveillant et/ou d'un 0day
    - Pas de « cocooning » avec vos pirates

Il serait impossible de traiter ce vaste sujet en une simple intervention de type conférence, mais voici néanmoins quelques éléments pour conclure cette introduction globale à ce sujet complexe générant souvent des mythes complètement éloignés de la réalité

ELÉMENTS DE CONCLUSIONS

Conclusions

- Nous savons tous que nous sommes tous vulnérables
  - Tous les experts SSI constatent une amélioration des techniques offensives et une diminution de l'efficacité des moyens défensifs
  - Les politiques, stratégies et les organisations actuelles ne servent pas à grand chose quand la technologie est non maitrisée
  - Le cyber-espionnage est une réalité et il n'est pas limité à des aspects étatiques (concurrence, idéologie, etc)
- Certains ont le courage de lutter, d'autres espèrent tenir ou ne pas devenir des cibles
  - Les raisons pour ne pas agir efficacement sont souvent très nombreuses (refus du changement, budgets mal utilisés, méconnaissances, dénis de la réalité, historique, choix affectifs, interférences politiques, etc)

Conclusions

- Il est crucial d'écouter et de transformer sa posture pour limiter son exposition aux risques techniques
  - Instinct de survie individuel et collectif
  - Choix de la posture (subir ou agir) → sincérité associée
  - Principes technologiques
    - Détecter, limiter, contenir les intrusions
    - Avoir des outils qui marchent contre ce type de menaces en adéquation avec les besoins et les moyens internes
      - Oui, on peut (essayer de) tenir face à des APT, des 0days…
- De ces combats asymétriques naitront de nouvelles méthodes, techniques, comportements et usages, où ceux qui s'adapteront le mieux seront ceux qui survivront le mieux aux menaces de cet environnement

N'hésitez pas à poser vos questions

MERCI POUR VOTRE ATTENTION ☺