HACK YOURSELF DEFENSE

Eric DETOISIEN
SSTIC 2015

1 Introduction

Introduction

- Pas question ici des moyens à mettre en œuvre pour se protéger mais plutôt de la connaissance environnementale nécessaire pour choisir, maintenir et faire évoluer ces moyens
- Cela implique une maîtrise du milieu offensif, si possible plus avancée que celle de l’adversaire
- Une maitrise, par la suite, mise au service de la sécurisation pour lui permettre d’évoluer et de s’adapter

Introduction

- Cela passe par une mise à plat du contexte actuel entourant l’attaque et la défense
- Puis une proposition de solution qui pourrait être mise en place pour tenter de maîtriser et d’utiliser des moyens offensifs

Introduction

Limites

- Le contexte est principalement le contexte français
- Les attaquants considérés sont des individus ou des organisations criminelles (les méchants officiels)
- Les cibles considérées sont des organisations (entreprises ou administrations), les particuliers ne sont pas directement dans le périmètre
- Quelques zooms sur des sujets spécifiques plus par intérêt et expérience personnelle (aucune exhaustivité)
- Généralités sans pour autant exclure les exceptions

2 CONTEXTE

Contexte

Environnement

- Généralisation de l'équipement informatique et de la connectivité
- Dématérialisation systématique
- Valorisation de plus en plus élevée des données
- Emergence de points de concentration
  - ✓ Service en ligne regroupant des quantités massives de données
  - ✓ Technologies/applications très fortement répandues (web, sécurité, client side, mobile, ...)
  - ✓ Croisement et regroupement des environnements professionnels et privés (augmentation des points d'entrée)

Contexte

Environnement

- Apprentissage des techniques d’attaque plus rapide
- Augmentation du nombre d’attaques
- Méconnaissance des risques réels et par conséquent de la réelle efficacité des moyens de défense
- Capacité de traitement des équipes sécurité saturée
- Disproportion entre l’exposition aux risques et les ressources disponibles pour traiter ces risques

Contexte

Attaque

- Ressources humaines
  - ✓ Recrutement non limité (RH moins regardant, diplômes facultatifs, casier vierge optionnel, peu de problèmes de licenciement en cas de désaccord avec le salarié, ...)
  - ✓ Rémunération moins contrainte (droit, fiscalité, ...) et généralement plus attrayante
  - ✓ Les compétences et donc les résultats sont les critères principaux (la communication et le rédactionnel ne sont pas un pré-requis non plus)
  - ✓ Activité focalisée à 100% sur l'attaque (pas trop de consulting)
  - ✓ Mondialisation du recrutement (activité mondialisée)

Contexte

Attaque

- Ressources techniques
  - ✓ Outils automatisés pour la recherche de cibles et de failles
  - ✓ Framework d'exploitation / Kits d'exploitation client side
  - ✓ Malware avec infrastructure
  - ✓ Spécialisations : verticales (banque, webmail, login/password, données personnelles, CB, données métier, …), hacktivisme, …
  - ✓ Outils d'anonymisation et de post exploitation
  - ✓ Accès à des taupes (telecom, réseaux sociaux, ...)
  - ✓ Equipement testé, approuvé et éprouvé en conditions réelles
  - ✓ R&D directe ou indirecte incluant les 0days

Contexte

Attaque - Interlude

- 0days
  - ✓ De plus en plus utilisés dans la nature même si ce n'est pas indispensable
  - ✓ De plus en plus de sous en jeu
  - ✓ De plus en plus d'acteurs (chercheurs, intermédiaires, utilisateurs finaux)
  - ✓ De moins en moins de full disclosure (ou plus généralement d'informations publiques pertinentes)

Contexte

Attaque - Interlude

- 0days
  - ✓ Acteurs historiques : Zero Day Initiative, iDefense
  - ✓ Nouvelles plateformes : HackerOne, Bugcrowd
  - ✓ Concours : Pwn2Own, Google Pwnium
  - ✓ Indépendants et sociétés spécialisées
  - ✓ Editeurs : programme de récompense (Facebook, Mozilla, DropBox, …), équipe interne (Microsoft, Google, …)
  - ✓ Méchants : TheRealDeal (TOR), forums (antichat.ru)
  - ✓ Certains bugs terminent bien chez les éditeurs (et sont donc corrigés) d’autres terminent chez les attaquants - ou les deux

Contexte

Attaque

- Ressources financières
  - ✓ Système de financement opaque
  - ✓ Mutualisation des cibles donc rentabilité et efficacité plus élevées
  - ✓ Centre de profit
- Contraintes
  - ✓ Obligation de résultat
  - ✓ Anonymat
  - ✓ Vie sans doute un peu compliquée des fois

Contexte

Défense

- Ressources humaines
  - ✓ Manque de ressources
  - ✓ Ressources dispersées (privé, publique)
  - ✓ Recrutement contraint (droit du travail, diplômes, rejet, dénigrement et dévalorisation de l'expertise technique avec impact sur la rémunération et l'évolution professionnelle)
  - ✓ Conséquences : équipes internes spécialisées rares, faible connaissance de la réalité du terrain en général
  - ✓ Externalisation mais avec un report du problème : compétences variables, capacité de traitement limitée

Contexte

Défense

- Ressources techniques
  - ✓ Outils commerciaux et open source (grand public)
  - ✓ Outils internes spécifiques (plutôt chez les prestataires)
  - ✓ Vulnérabilités publiques (le reste n’intéresse pas ou n’est simplement pas connu/disponible)
  - ✓ Conséquences : pas ou peu de capitalisation ni de personnalisation (par métier, par pays), spectre des compétences trop limité, pas ou peu de R&D, audit/pentest trop contraint
  - ✓ Externalisation : simple transfert du problème

Contexte

Défense - Interlude

- Pentest
  - ✓ Indispensable
  - ✓ Contraintes du client : périmètre, horaires, portée des attaques (pas ou peu de post exploitation juste des preuves), temps et budget
  - ✓ Fréquence trop faible (valable à instant t, la seconde suivante le résultat peut être caduque)
  - ✓ Rarement de client side et quasiment jamais de 0days (ou équivalent)

Contexte

Défense - Interlude

- Pentest
  - ✓ Résultats variables en fonction des compétences de l'auditeur
  - ✓ Sur des périmètres trop larges (interne, centaines de sites web, ...) il est impossible de tout voir et de tout faire
  - ✓ Temps perdu sur le reporting et autres présentations
  - ✓ Les tarifs ne sont plus adaptés au périmètre et à une récurrence obligatoire

Contexte

Défense - Interlude

- Scanner de vulnérabilités
  - ✓ Fréquence plus réaliste (surveillance continue possible)
  - ✓ Rapports et alertes automatisés
  - ✓ Pertinence trop limitée (false positive et quasiment pas d'exploitation)
  - ✓ Pas du tout adapté aux spécificités d'un pays ou d'une verticale métier (industriel, télécom, banque, hospitalier, ...)
  - ✓ Nombre de plugins important mais toujours insuffisant
  - ✓ Peu de capitalisation et de personnalisation vis-à-vis des cibles
  - ✓ Pas d'équipes opérationnelles

Contexte

Défense

- Ressources financières
  - ✓ Budget limité (centre de coût)
  - ✓ Au mieux une obligation de moyens
- Contraintes
  - ✓ Périmètre à protéger de plus en plus diffus (et donc méconnu dans sa totalité)
  - ✓ Réglementation, législation, horaire, résilience de la production

3

Hack Yourself

Hack Yourself

Objectifs

- Confronter la sécurité de son SI à la réalité et à l'efficacité des attaquants
  - ✓ Connaissance de l'entreprise (métier, organisation, enjeux)
  - ✓ Fréquence élevée et évènementielle (évolution, nouveau bug, …)
  - ✓ Périmètre global (serveur, client side, …)
  - ✓ Ciblage (connaissance des applications spécifiques et propriétaires)
  - ✓ Opportunisme technologique

Hack Yourself

Objectifs

- Effectuer des attaques avec des outils, des techniques et des experts du plus haut niveau
  - ✓ Panoplie d'outils à jour (R&D, utilisation de 0days ou de jokers)
  - ✓ Compétences multi-domaines
- Faire ressortir les faiblesses pour focaliser les efforts sur les risques réels et avérés avec une réactivité optimale
  - ✓ Aucun false positive
  - ✓ Rapports et alertes en temps réel
  - ✓ Capitalisation sur la connaissance du SI
  - ✓ Suivi des corrections et des évolutions

Hack Yourself

Modèle

- Plateforme technique industrielle
  - ✓ Identification et gestion du périmètre
  - ✓ Scan de vulnérabilités automatisé et personnalisé (dynamique et statique)
  - ✓ Campagnes spécifiques : client side, phishing
  - ✓ Exploitation et post-exploitation
  - ✓ Analyse statique et dynamique
  - ✓ Rapports et alertes
  - ✓ Capitalisation et suivi

Hack Yourself

Modèle

- Equipe d’experts opérationnels
  - ✓ Personnalisation de la plateforme pour une cible
  - ✓ Revue et validation des résultats
  - ✓ Attaques complémentaires
- Equipe R&D
  - ✓ Développement et maintien de la plateforme
  - ✓ Veille, analyse et recherche de vulnérabilités
  - ✓ Mise en place des nouvelles techniques et des nouveaux outils

Hack Yourself

Modèle

- Service gérant tout type de technologie (web, serveur, client side, mobile, embarqué, …)
- Service opérationnel et disponible mondialement
- Service forensics à étudier car très intéressant pour alimenter la connaissance sur les attaques (et inversement)

Hack Yourself

Modèle

- Service de surveillance type détection de fuites d’informations à étudier car les canaux de diffusion sont similaires à ceux de la veille (oneworldlabs.com par exemple)
- Cela peut aussi devenir un excellent centre de formation (interne)

Hack Yourself

Modèle

- Ressources humaines
  - ✓ Sélection stricte à l'entrée par compétence (attention aux taupes)
  - ✓ Pas de limite à une nationalité particulière (attention aux taupes)
  - ✓ Mode de travail adapté (horaires, travail à distance, ...)
  - ✓ Reconnaissance de l'expertise (salaire)
- Ressources techniques
  - ✓ Celles des attaquants et des défenseurs
  - ✓ Celles décrites précédemment (plateforme)

Hack Yourself

Modèle

- Ressources financières
  - ✓ Nécessité d’un financement important
  - ✓ Des modèles similaires ou approchants existent déjà et montrent le niveau de financement demandé (Veracode, White Hat Security, Synack, High-Tech Bridge, …)
- Contraintes
  - ✓ En France, celles connues par tous les entrepreneurs
  - ✓ En France, celles liées à l’activité offensive

4 Self Defense

Self Defense

- La protection seule n’a jamais été suffisante pour éliminer un danger
- L’élimination du problème doit être étudié
- Contexte à rapprocher de celui de la légitime défense
- Contraintes et limites de la légitime défense
  - ✓ S’il n’y a pas d’autres alternatives
  - ✓ Avoir une probabilité élevée de frapper les attaquants réels
  - ✓ Garder un principe de proportionnalité

Self Defense

- Les moyens d’effectuer des contre-attaques sont identiques à ceux décrits pour le Hack Yourself
- Seule la capacité d’anonymat doit être ajoutée
- Ce type de structure existe déjà : Société Militaire Privée

5 Conclusion

Conclusion

- Création d'une Société Militaire Privée Virtuelle
  - ✓ Mutualisation des ressources et des compétences au sein d'une structure spécialisée et industrialisée
  - ✓ Investissements importants
- Mais :
  - ✓ On s'aperçoit que les grosses structures résistent bien
  - ✓ On ne travaille pas sur la vaccin contre le cancer
  - ✓ On peut changer de métier si on n'est pas content

Liens

- https://www.troopers.de/events/troopers15/288_keynote_information_security__the_hard_thing_about_the_hard_thing/
- http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
- http://www.leviathansecurity.com/wp-content/uploads/Value-of-Cloud-Security-Scarcity.pdf
- http://seanmason.com/2014/07/21/impact-on-company-stock-following-data-breaches/
- https://hackerone.com/news/the-wolves-of-vuln-street
- http://www.vulnerability-lab.com/list-of-bug-bounty-programs.php
- http://geer.tinho.net/geer.blackhat.6viii14.txt
- http://recode.net/2014/12/10/sony-pictures-tries-to-disrupt-downloads-of-its-stolen-files/
- http://www.bloomberg.com/news/2014-12-30/fbi-probes-if-banks-hacked-back-as-firms-mull-offensives.html
- http://trdealmgn4uvm42g.onion/
- https://angel.co/