Acteurs, vecteurs et ressources OSINT

Acteurs malveillants

Script Kiddies

- Pirates relativement nouveaux et inexpérimentés
  - essaient de voir ce à quoi ils réussissent à accéder illégalement, souvent par pur défi
  - a priori pas en lien avec des groupes cybercriminels
  - en général, peu d’argent à disposition
- Les *script kiddies* commencent en utilisant des programmes dont ils ne comprennent pas le fonctionnement mais qui sont suffisamment dangereux pour provoquer des dégâts s’ils sont correctement utilisés

Hacktivistes

- Pirates motivés par une idéologie, une cause sociale ou politique
  - expérimentés
  - ressources financières
- Actions typiques :
  - *defacing*
  - vol d’informations pour divulgation
  - DDoS
- Les actions sont en général brutales et peu discrètes

Crime organisé

- Motivés par l’appât du gain
  - hautes capacités techniques
  - ressources financières importantes
  - patients, persistents
- Développent et améliorent sans cesse des outils/techniques permettant de gagner de l’argent rapidement :
  - ingénierie sociale (hammeçonnage…)
  - vol de données personnelles ou propriété intellectuelle pour revente ou réutilisation
  - rançongiciels
  - …

Menaces avancées persistentes (APT)

- Pirates très doués et expérimentés
  - cyber-guerre / cyber-espionnage entre états
  - pénétration de systèmes commerciaux ou industriels importants
  - sabotage
- prennent potentiellement des mois/années pour constituer une attaque ciblée, développer des logiciels malveillants efficaces, découvrir des vulnérabilités…
- De gros efforts sont faits pour éviter de se faire découvrir

Attaques internes

- Collaborateur de l’organisation travaillant ou offrant ses services à un acteur malveillant externe (concurrence…), ou juste par vengeance
- 70 % des vols de propriété intellectuelle impliquent des attaques internes
- Les politiques de sécurité de l’organisation doivent notamment inclure dans les procédures de recrutement RH des vérifications des candidatures permettant d’évaluer le risque associé à chaque candidat

Concurrence

- La concurrence cherche à gagner un avantage compétitif sur l’organisation cible
  - attaque interne sur la cible
  - vol de propriété intellectuelle (projets futurs, prototypes…)
  - sabotage
- Peut aussi viser à décrédibiliser pour détruire la confiance des investisseurs et des clients :
  - *defacing*
  - divulgation publique de données
  - DDoS…

Type	Int/Ext	Compétence	Ressources	Motivations
Scripts Kiddies	externe	faible	faible	curiosité
Hacktivistes	externe	moyen/élevé	moyen/ élevé	idéologie
Crime organisé	externe	élevé	élevé	argent
APT	externe	élevé	élevé	cyber-guerre
Attaques internes	interne	faible à élevé	faible à élevé	vengeance, argent
Concurrence	externe	faible à élevé	faible à élevé	avantage compétitif, argent

Vecteurs d’attaques

On revient ici, pour synthétiser, sur différents vecteurs d’attaques déjà vus et les contre-mesures globales possibles

Vecteurs d’attaque - Accès direct

- Accès physique
- Sur site
- Ingénierie sociale
- Vol / destruction
- Contre-mesures :
  - sécurité physique
  - sensibilisation/formation **régulière** des usagers

Vecteurs d’attaque - Sans-fil

- Portails captifs
- Jumeaux malveillants
- Sniffing réseau
- Contre-mesures :
  - VPN/chiffrement
  - sensibilisation/formation **régulière** des usagers

Vecteurs d’attaque - Email

- Pièces jointes (malwware)
- Hammeçonnage, *whaling*…
- Liens malveillants
- Contre-mesures :
  - examens automatiques d’emails et de sources (SPF, DKIM…)
  - sensibilisation/formation **régulière** des usagers

Vecteurs d’attaque - Supply Chain

- Maillon faible dans la chaîne
- Contre-mesures :
  - Contrats de service incluant les mesures de sécurité à respecter pour pouvoir travailler ensemble à tous les niveaux de la chaîne

Vecteurs d’attaque - Réseaux sociaux

- Liens malveillants
- Phishing
- *Prepending*
- Consensus / acceptation sociale
- Contre-mesures :
  - sensibilisation/formation **régulière** des usagers

Vecteurs d’attaque - Périphériques externes

- USB, SD Card, CD/DVD…
- Malwares de tous types
- Contre-mesures :
  - politique de sécurité interdisant ces médias (ou alors utilisation sous contrôle)
  - sensibilisation/formation **régulière** des usagers

Vecteur d’attaque - Cloud

- Vulnérabilités des fournisseurs de cloud
- Partage de ressources ⇒ dommages collatéraux en cas d’attaque sur autre cible
- Mauvaise configuration / politique d’accès
- Contre-mesures :
  - bien examiner les contrats en place avec les services cloud
  - expertise dans le domaine de la configuration cloud

OSINT

- *Open Source Intelligence*
- Nombreuses ressources (légales) disponibles pour récolter des informations
- Les outils et techniques OSINT existent sous forme de :
  - sites webs
  - extensions navigateurs
  - applications

Quelques outils d’OSINT

- Maltego
- Metagoofil
- Shodan
- GHDB
- FOCA
- EXIF Data Viewers
- BackTrack Linux
- Buscador Linux
- Social Engineering Toolkit
- PeekYou
- Lullar
- Wayback Machine
- YouGetSignal
- Metasploit
- Spokeo

BDD de vulnérabilités

- Google Hacking DB : exploit-db.com
- VirusTotal : virustotal.com
- NVD (*National Vulnerability Database*) : nvd.nist.gov
- MITRE *CVE Database* : cve.mitre.org