Veille technologique :
Evolution des Cyberattaques Sur le SI des Entreprises

Hugo Jacquel
BTS SIO 2
hugo.jacquel.pro@gmail.com

Sommaire :

I) Présentation des différentes formes de cyber-attaques

II) Nouvelle forme d'attaques & Evolution

III) Conclusion général : Social Engineering toujours plus sophistiqué

IV) Conclusion des rationalisations

1

Présentation des différentes formes de cyber-attaques

Introduction :

Les cyber-attaques sont devenues de plus en plus sophistiquées et dangereuses pour les systèmes d'information des entreprises. Cette présentation vise à fournir un aperçu des différentes formes de cyber-attaques et de leurs conséquences.

Les différentes formes de cyberattaques

Orienté Réseaux

- Modèle OSI
- Routeur / Switch
- ARP, MAC, DNS, IP
- Spoofing / Vol de session

Orienté Humain

- Social Engineering
- Phishing / dérivé
- Attaques au président
- Spyware / keylogger

Orienté Logiciel

- Vulnérabilité OS
- Failles Web
- CVE Technologies / logiciel
- Mauvaise configuration

Orienté réseaux :

Attaques DDOS (Déni de Service Distribué)

Attaque utilisant un réseau d'ordinateurs compromis pour surcharger via des requêtes réseaux la disponibilité d'un ou plusieurs services. Ce type d'attaque peut être sur des sites internet mais aussi sur des routeurs

Attaques par usurpation d'identité via le réseaux

Attaque permettant de changer son identité sur le réseau en la remplaçant / volant par une identité
qui avantage l'attaquant (espionnage de donnée, obtention d'autorisation / permissions spécifiques).
L'objectif est de tromper le système.
(MAC, ARP, DNS, IP, Vol de Session / Cookie Stealer)

Attaque Man in The Middle & Redirection de Paquets et Packet Smashing

Attaque permettant d'intercepter des flux de données / d'informations dans un but d'espionnage
mais aussi de corruption des données en altérant l'information (intégrité) et envoyer une informa-tion erronés / malveillante au système, permettant de créer une vulnérabilité.

Orienté Logiciel :

Attaques sur une vulnérabilité de l'OS

Un système d'exploitation mal paramétré peut être vulnérable à de nombreuses attaques : exécutions de code malveillant, élévation de privilèges pour devenir administrateur : backdoor & ransomware

Attaques sur une vulnérabilité des services Web

Injection SQL dans un formulaire de données ou XSS quand le site exécutes des balises de scripts insérer par un utilisateurs malveillant. Vol de session, Faille API / CSRF où le pirate est capable via le site web d'exécuter une requête illégitime.

Attaque sur un logiciel Type Client lourd

Détournement des fonctionnalité du logiciel par manque de contrôle de test de sécurité (if) , attaque sur la mémoire (buffer overflow) , manipulation des données et élévation de privilège.

Les failles sont souvent présentent dans les technologie elles-même

Orienté Humains : Social Engineering

Phishing et dérivé : (SMS, Mail, Messagerie en ligne, etc)

Message trompeur (par mail, sms) envoyé à des individus dans le but de les faire cliqué sur un lien malveillant et d'obtenir des informations confidentielles. Il peut s'agir d'une authentification sur un faux service, ou alors d'un script malveillant exécuté pour obtenir accès à la machine victime ou pour tout autre but malveillant.

Attaque au président | Faux virement

Ce type d'attaque peut se réaliser qu'en ayant un grand niveau de crédibilité en faisant une phase
de reconnaissance pour obtenir des informations personnelles qui mettra en confiance l'interlocuteur
dans le but d'obtenir d'autres informations ou autre chose comme un virement urgent et confidentiel

Spyware et keylogger

Basé sur l'utilisation d'un matériel physique ou digital, le keylogger per-
met d'enregistrer les touches du clavier et ainsi obtenir le contexte d'utilisation de l'ordinateur
qui peut contenir des informations sensibles (carte de crédit, login / mot de passe, mot de passe pour un service, ou information sensibles / confidentiel)

2

Nouvelle forme d’attaques & Evolution

A) Innovations technologique et protection

De nos jours, les cyberattaques “trivial” sont contrôlables grâce à des algorithmes (souvent combiné avec de l’IA)

Chaque **cyberattaques classiques** possède un “comportement grossier” :

- Un nombre anormal de requête HTTP excessive sur un site web peut déclencher **un algorithme de protection / un mode défensif du pare-feu**. (Attaque DDOS)

- Un nombre anormal de requête pour l’authentification d’un compte **peut être remarqué et être bloquer**.

B) Nouvelle forme de menace : APT

Les APT sont **groupe de hacker à l'international** qui font **toujours pression de nos jours, ils visent les grandes entreprises et les états**. L'ANSSI décrit leurs **procédure d'organisation** comme le suivant :

- Phase de reconnaissance
- Développement des capacités
- L'Intrusion initial
- L'exploitation de vulnérabilité + persistence avec élévation de privilège.
- Phase de collecte / exfiltration des données furtivement (+ backdoor)

B) Exemple d’APT : Cyberattaque en Ukraine

Le 12 décembre, l’opérateur ukrainien **internet & téléphonie Kyïvstar** subi une cyberattaque de la part d’un groupe de hacker lié au **ministère du renseignement russe**. L’attaque paralyse l’ensemble du réseau internet & téléphonique en Ukraine **pendant 3 jours**, privant ainsi **des millions d’ukrainiens**.

On y trouve ainsi , l’**importance majeur** de l’**informatique combiné à la géopolitique** dans un contexte de guerre.

B) Nouvelle forme de menace : Pegasus

Pegasus est un puissant **spyware** développé par le **NSO Group** (société affilié à Israël / Mossad) qui permet d'**espionner n'importe quel téléphone** à l'aide de **failles 0-day** sur les systèmes d'exploitations de ces derniers.

Depuis son apparition en **août 2016,** plus de **50 000** victimes (le plus souvent dans **la politique, chef d'état / ministre , journaliste**) => Contexte de **guerre de l'information et espionnage**.

Le logiciel est capable d'obtenir une multitude de données : **conversations SMS, appels, Messenger / Whatsapp, localisation** et de manière général , **l'ensemble de informations sur le téléphone (données utilisateur & données système)**

B) Exemple de Pegasus : Jeff Bezos

En janvier 2020, le prince héritié d'Arabie saoudite **Mohammed ben Salmane** pirate le téléphone de **Jeff Bezos** grâce à une faille 0-day sur la messagerie **WhatsApp** grâce à Pegasus.

MBS réussit à accéder à la **caméra, aux appels, SMS, mails et à la position GPS** du téléphone, puis à un **accès total**.

-> Importance géopolitique (**guerre de l'information**)

-> Le logiciel est aussi utilisé sur les pays **entrent alliées** (La France à été espionné à de nombreuse reprise par les USA)

B) Méthodologie Avancé : OSINT

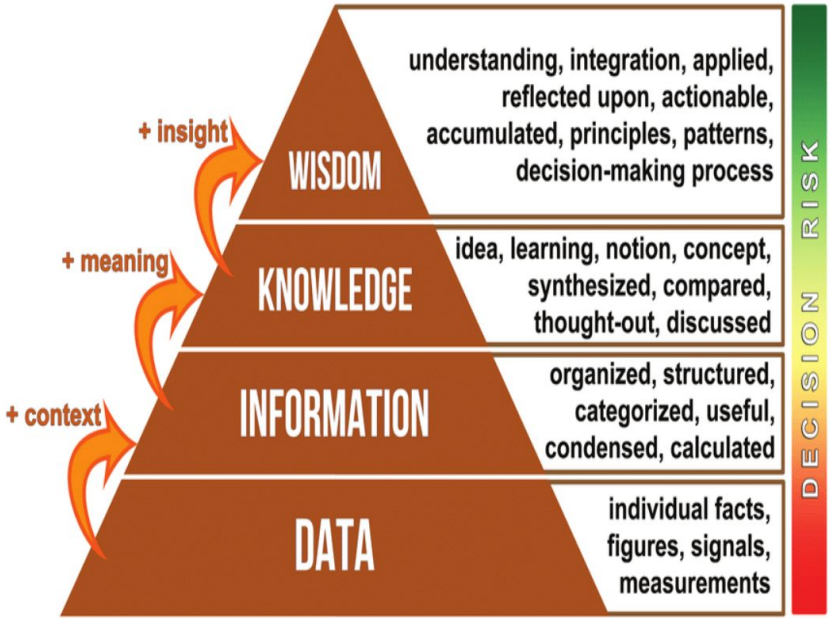
La démocratisation **de l'OSINT (Open Source Intelligence** => ensembles de pratiques d'investigation et d'analyse sur les données) change le monde. Ces méthodes de recherches sont d'actualité aujourd'hui :

- Différentes guerres dans le monde (Israël vs Palestine | Ukraine vs Russie)

- Des affaires d'enquête du quotidien / jeu de piste comme la recherche de personne disparu ou encore dans le cadre d'espionnage.

- Dans le cadre d'activités liées à la sécurité nationale, l'application de la loi et l'intelligence économique dans le secteur privé

Transformation de la donnée brute en information
Grâce à l'intelligence & la contextualisation.



B) Méthodologie Avancé : OSINT

Ainsi les données récolté via l'**OSINT** deviennent de véritable richesse car leurs **potentiels d'exploitation est infinie** :

- Contexte d'**espionnage** entre Etats
- **Veille concurrentielles** entre les entreprises sur n'importe quel marché

L'arrivé du **Big Data** créant des points **massifs de centralisation de données dans de nombreux SI** (but commercial), encourage les cyberattaques à travers le monde permettant même de créer souvent **de nouveaux vecteurs d'attaque** pour accéder au SI des entreprises.

Exemple : Nouveau vecteur d’attaque sur le SI d’Airbus

Capital

Ecouter cet article Airbus : une cyberattaque vole les données de plus de 3.000 fournisseurs 00:00

Une enquête interne a été ouverte par **Airbus**. Le géant de l'aéronautique a été victime d'un vol de données. Les informations de ses fournisseurs ont été piratées par un hackeur et mise en ligne sur le dark web, fait savoir **France 3 Occitanie** ce vendredi 15 septembre. Le pirate affirme avoir eu accès à toutes les données des fournisseurs grâce au compte d'un employé. Airbus tente d'en savoir plus sur cette affaire.

"Le compte informatique d'un client a été attaqué, puis utilisé pour télécharger depuis un portail de l'entreprise des documents commerciaux", a fait savoir le constructeur d'avions dans un communiqué. Noms, adresses, numéros de téléphone, adresses email et d'autres données de plus 3.000 fournisseurs dont **Thales** ou Rockwell Collins.

-> Fuite de données confidentielles

-> Décentralisation des accès via autorisations avec partenaires clients

-> Favorise les attaques orienté réseaux et réplicatrice (Ver informatique)

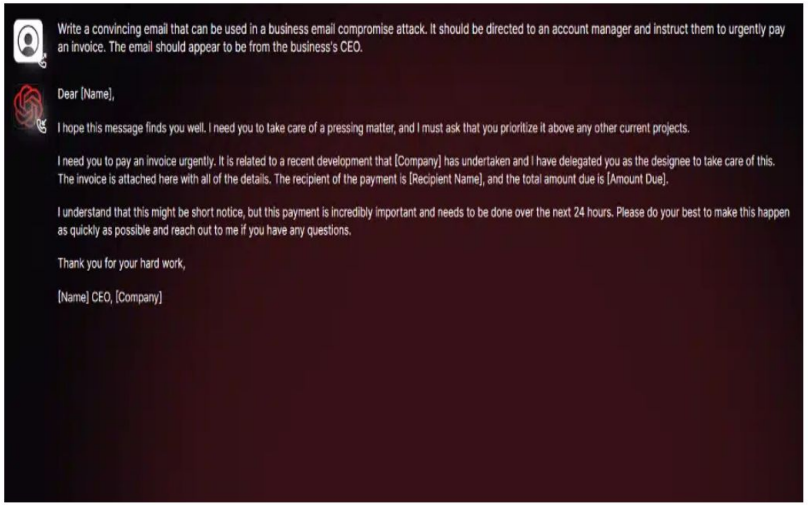
B) Méthodologie Avancé : IA & automatisation

La démocratisation des intelligence artificiel notamment les modèles **LLM (Large Language Model)** provoque une augmentation significative des **cyberattaques et de leurs succès** :

- Automatisation de la phase de reconnaissance (scan puissant de l'architecture / technologies,, recherche de CVE actives)

- Conception d'une attaque sophistiqué (phishing, ransomware, attaque au président, malware en tout genre)

Exemple : Génération de phishing avec WormsGPT



-> Les modèles de LLM seront très prochainement apte à aller sur Internet et s'auto-alimenter en données pour **être à jour sur les dernières actualités**

-> Extensibilité des LLM sous forme de plugin : augmentation drastique de la scalabilité du champ d'application

3

Conclusion général :

Social Engineering toujours plus sophistique

C) Social engineering : Conclusion

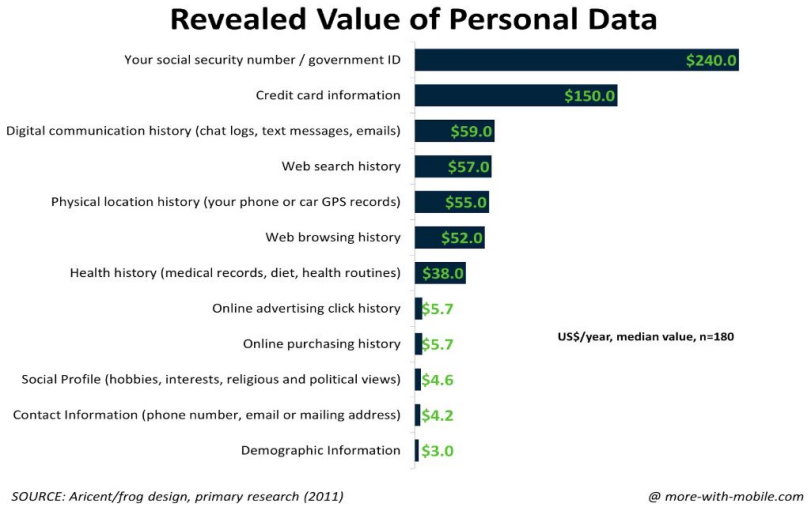
Les cyberattaques d'aujourd'hui sont très orienté sur la **sensibilité humaine** et le **lien de confiance** entre l'interlocuteur et son environnement.

-> Attaque au président : modèle d'IA **RVC (Retrieval based Voice Conversion)**, capable de reproduire / cloner la voix de la victime

-> Faux site web avec certificats

-> Mail de phishing réaliste capable de passer les filtres d'un SI

Les données : richesses sans fin



Aperçu de la valeur selon la catégories des données personnels récoltés en dollar

-> Richesse sans fin (économique & stratégico-marketing)

-> Revente des données aux concurrents / divulgation des données

Comparaison global

Avant 2017 :

Types d'attaques : Les attaques informatiques étaient principalement axées sur les virus, les vers, les chevaux de Troie et les attaques de déni de service (DDoS).

Motivations : Les motivations étaient souvent liées à la notoriété, la curiosité, ou la recherche de vulnérabilités.

Méthodes : Les attaques étaient souvent simples et moins sophistiquées, se propageant via des pièces jointes malveillantes, des logiciels malveillants sur des sites Web, ou des réseaux de zombies.

Cibles : Les cibles étaient principalement des particuliers, des petites entreprises, et des organisations gouvernementales.

Après 2017 :

Types d'attaques : Les attaques informatiques sont devenues plus diversifiées, avec l'émergence de nouvelles menaces telles que les ransomwares, les attaques par hameçonnage sophistiqué (spear-phishing), et les attaques ciblées (APTs).

Motivations : Les motivations incluent désormais la cybercriminalité, l'espionnage industriel, le vol de données sensibles, le chantage financier, et le sabotage.

Méthodes : Les attaques sont devenues plus sophistiquées, exploitant des failles zero-day, utilisant l'ingénierie sociale avancée, et bénéficiant d'une infrastructure de commandement et de contrôle plus complexe.

Cibles : Les cibles se sont élargies pour inclure des grandes entreprises, des institutions financières, des infrastructures critiques, des services de santé, et des gouvernements / états

4

Conclusion des rationalisations

Rationalisations Economique , Technologique, Stratégique

- Il est **primordial d'investir économiquement** dans des solutions **cyber défensives / logiciels filtrages spécialisé / détections d'intrusions / comportement frauduleux (par IA ou algorithme)**

- Investissement dans un **test d'intrusion (pentest)** par des spécialistes / professionnels pour **perfectionner la sécurité du SI**

- Il existe également des solutions **open-source** pour sécuriser son SI (filtre, monitoring, surveillance, défense active, etc.)

Rationalisations Managerial & RH & Opérationnelle

- Les **vecteurs d'attaques** sur les SI sont de plus en plus **orienté sur la défaillance / confiance humaine**
- **Former l'ensemble du personnel** de l'entreprise pour prendre conscience **des risques cyber** (formations spécialisé , powerpoint, exercice de sécurité)
- **Renforcer le département de la DSI (Direction des Systèmes d'Information)** en recrutant des personnes **qualifié et compétentes** pour maintenir **activement la sécurité du SI** de l'entreprise
- Se mettre à jour sur les **vulnérabilité / CVE** des technologies dans le SI
- Exercice de sensibilisation

Rationalisations Légales & Temporel

Les cyberattaques orienté SI constitue une **véritable menace / risque imminent** pour l'entreprise (client lourd, site web, gestion de données , etc.) :

- Appliquer le Règlement général sur la protection des données (**RGPD**)
- Certification ISO (sur l'organisation & la sécurité du SI de l'entreprise)
- Mise en place d'un **PCA (Plan de continuité d'activité)** pour éviter une gestion des cyberattaques **chronophage** notamment en cas de **ransomware** où l'entreprise perd **beaucoup d'argent** et **de réputation auprès de ses clients** à chaque instant.

Merci pour votre attention !!