SYNTHÈSE DE LA VEILLE INFORMATIONNELLE SUR L'ÉVOLUTION DES CYBER-ATTAQUES DANS LES SI DES ENTREPRISES ?

VEILLE INFORMATIONNELLE

RÉALISÉ PAR

HUGO JACQUEL

Sup Alta
Lyon

2023
BTS SIO 2

Table des matières

1 Présentation de la veille

L'objectif de cette veille est d'être **sensibilisé** et d'être conscient des différents type de cyberattaques et de leurs évolutions dans le temps.

Depuis le début d'**Internet** et des **technologies lié à l'informatique**, ils existent des failles et des méthodes permettant d'outrepasser :

- des conditions de réussite

- l'accès à des données de manière illégitime

- la destabilisation de la disponibilité d'un ou plusieurs services

- la prise de contrôle d'un ensemble d'appareils de manière illégitime

Similairement à des **braquages / du vol** , de l'**espionnage**, **la ventes de contrefaçon**, **le vol d'identité**, etc, les cyberattaques sont désormaient communes dans notre monde et à la différence des actes illégaux dans la vrai vie, elles sont **facile d'accès** à n'importe qui avec un peu de théorie, quelques explications et des scripts largement disponible sur Internet sous multiples formats (vidéo tutoriel, article en ligne, forum spécialisé, livre, podcast et autre).

Ainsi, pour parvenir à leurs fins, les **cyberattaquants** peuvent cibler **différents dispositifs informatiques mais aussi humains**, à savoir :

- des serveurs ou des ordinateurs, isolés ou en réseau, peu importe qu'ils soient ou non reliés à Internet

- des équipements périphériques, notamment les imprimantes, qui représentent une porte d'entrée facile

- des appareils communicants de type smartphone ou tablette

- les collaborateurs humains de l'entreprise.

L'attaquant va ainsi exploiter des failles techniques ou humaines pour s'introduire dans le système informatique et accéder à la donnée qui l'intéresse.

2 I) Présentation des différentes formes de cyber-attaques

2.1 Attaques orienté dispositif informatique (SI)

2.1.1 Architecture 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 (MAC, ARP, DNS, IP, Vol de Session / Cookie Stealer, etc

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.

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 information erronés / malveillante au système, permettant de créer une vulnérabilité.

2.1.2 Architecture 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**, installation d'une **backdoor** permettant d'avoir un accès persistant sur la machine, virus en tout genre ou encore des ransomwares, des virus qui chiffre les données pour les rendre innutilisables (**intégrité**) et échanger la clé de dé-chiffrement contre une rançon.

Attaques sur une vulnérabilité des services Web et applications

Des clients légers peuvent comporter de nombreuses failles si ils sont mal paramétré : **injection de code SQL** dans un formulaire de données ou **XSS** quand le site exécutes des balises de scripts insérer par un utilisateurs malveillant.

Les attaques web peuvent aussi être des **vol de session**, similairement aux attaques réseaux **spoofing / usurpation d'identité** mais aussi des attaques de **route API sans autorisation (CSRF)** où le pirate est capable via le site web d'éxécuter une requête illégitime.

Les failles peuvent être aussi présente dans les **technologies elle-même**.

2.2 Attaques orienté humaine (Social Engineering)

Les attaques orienté humaines ne repose pas sur des **vulnérabilité logiciel , site web, système d'exploitation ou de la technologie** mais sur la **tolérance humaine et la sensibilité de confiance face à l'information**.

Plusieurs moyens sont disponible pour effectuer une attaque de Social Engineering.

2.2.1 Phishing et dérivé : par n'importe qu'elle protocole de communication (SMS, Mail, Messagerie en ligne, etc)

Phishing : 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.

Spear-phishing : Similaire au **phishing** mais le contenu et le publique est **beaucoup plus ciblés** avec des messages personalisés et des **informations confidentielles** divulgé pour atteindre un niveau d' **assurance et conviction élevé**

2.2.2 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**.

2.2.3 Attaque sur les mots de passes

Les mots de passes et moyen d'authenfication des utilisateurs sont **très souvent** basé sur un choix personnel (car ils doivent choisir un mot de passe que seul **eux connaissent**, ce qui peut impliquer des données **confidentiels / vie privée**.

Ainsi, ils existent de **nombreuses techniques** permettant d'obtenir un mot de passe :

- **Attaque par bruteforce** : Basé sur la puissance de la ou les machines attaquantes : ce type d'attaque teste **toute les possibilités** pour obtenir un mot de passe.

- **Attaque par dictionnaires** : Basé sur une longue série de mots, phrases, chiffres, caractères spéciaux probables dans le mot de passes. Cette attaque est basé sur la permutations des caractères, mot , phrases. Une phase de **reconnaissance** et souvent nécessaire pour assurer cette attaque en fonction de la cible.

- **Spyware et keylogger** : Basé sur l'utilisation d'un matériel physique ou digital, le keylogger permet **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)

2.2.4 Autre forme d'attaque

Ils existent une **infinité** d'attaque basé sur **la manipulation et l'utilisation de la psychologie et la psychanalyse humaine**. On peut penser à des attaques par **sentiments amoureux** , de **l'intimidation** (par notoriété sur les réseaux sociaux)

3 II) Nouvelle forme d'attaques & Evolution

3.1 Evolution des cyberattaques

Tout d'abbord les nombreuses cyberattaques orienté **réseaux et logiciel** sont connus du grand publique et de nombreux algorithme (basé sur du **machine learning IA** ou bien sur de la tolérance) permettent de détecter les cyberattaques grâce à leurs **comportements / pattern grossier** :

- Un nombre **anormal de requête HTTP excèssive** 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.

- Des concours de **bugbounty** (recherche de bugs / vulnérabilité) permettent aux éditeurs d'avoir des **remonté de vulnérabilité** sur leurs produits et de pouvoir les corrigé rapidement contre un **bénéfice financier ou autre**.

Cependant, certains bugs trouvé ne sont **pas reporté à l'éditeur** car il peut être conservé de manière **secrète**. Ils deviennent alors des failles **0-day** car ils ne sont pas connus de l'éditeur.

3.2 Nouvelle forme de menace : APT & Pegasus

3.2.1 APT (Advanced Persistent Threat)

Ce type de failles est très utilisé par **groupe de hacker à l'international** qui font **toujours pression de nos jours** : les APT (Advanced Persistent Threat).

Les groupes APT réalise des **attaques sophistiquées** (car comme indiqué les attaques basiques connu du grand publique ne sont plus efficace) et **furtives** dans des **grandes entreprises et des états**.

Leurs attaques sont **persistantes** ce qui leurs permet de rester pour de **longues périodes** et d'agir sur le **SI victime en continu** (toujours de manière discrète et furtives)

l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) fait **régulièrement** des **rapports** sur ces groupes de hackers en dévoilant les différentes **tactiques, procédures et techniques** utilisé pour :

- La phase de reconnaissance

- Développement des capacités

- L'intrusion intial

- L'exploitation de vulnérabilité, la persistence de l'intrusion et élévation de privilèges

- la phase de collecte et d'exfiltration des données furtivement

3.2.2 NSO Group & le logiciel Pegasus

Le société de cyber-intelligence **NSO Group** a mis au point un **puissant spyware basé sur l'utilisation de failles 0-day : Pegasus**.

Le spyware pegasus est à destination **d'agence gouvernemental**, **des gouvernements** où des personnes qui ont suffisament les fonds financier pour achter leurs services (500 000 $ pour l'espionnage de 10 téléphones).

Le logiciel est très utilisé sur des **hommes politiques** et sur des **journalistes** dans le cadre d'une **guerre de l'information et d'espionnage** entre les pays du monde entier. La donnée simple et en grande quantité devient alors une richesse qui peut être très bien exploité.

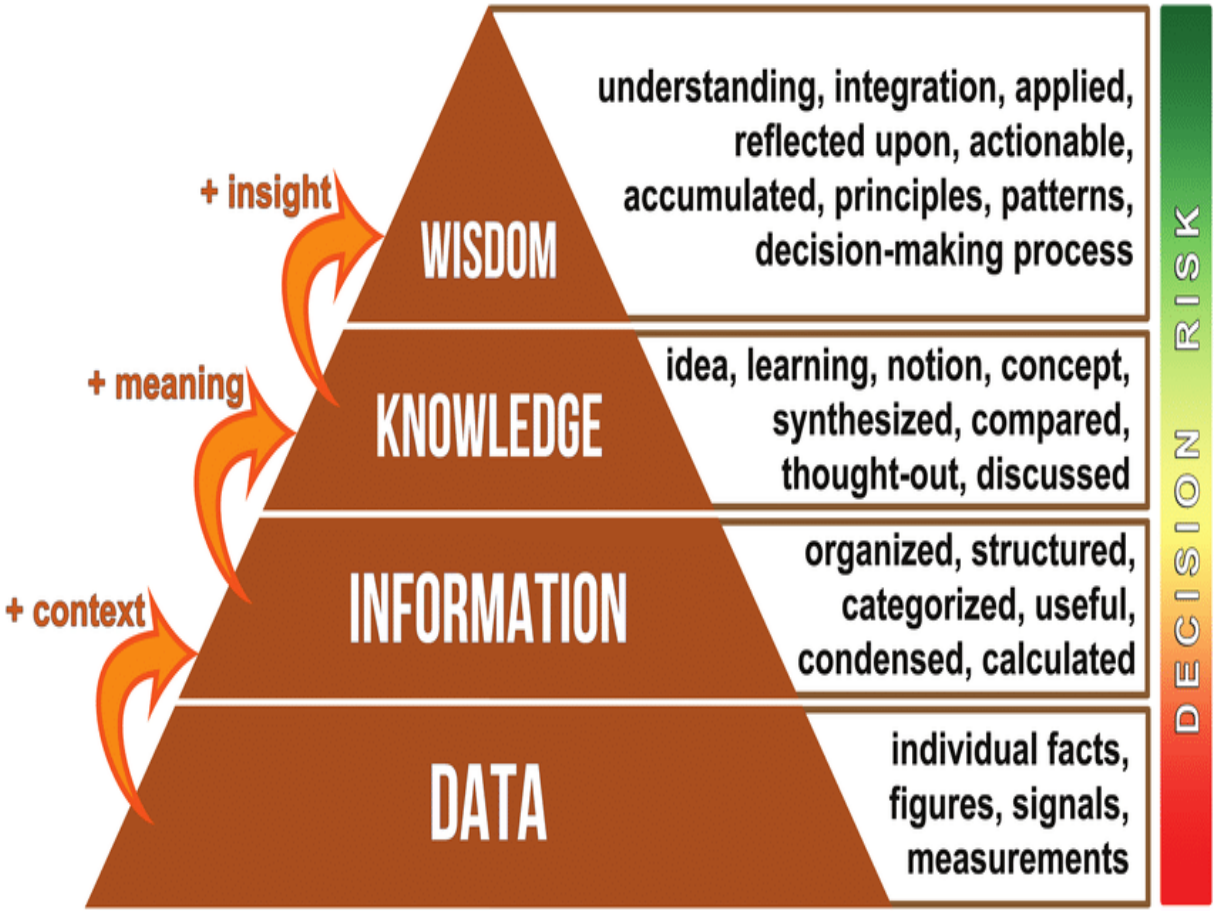
Par exemple , le prince héritier d'Arabie saoudite Mohammed ben Salmane a envoyé une image malveillante à Jeff Bezos (PDG Amazon). Cette image sous forme d'un "meme innocent" (image rigolote) contenait en réalité le logiciel espion Pegasus grâce à une faille 0-day Whatsapp. Ce qui a permit à MBS d'activer discrètement le micro ou la caméra de l'appareil, fouiller dans les SMS et les boîtes email, extraire la position GPS et réaliser pleins d'autres actions car il possédait **un accès total au téléphone de Jeff Bezos**.

Le logiciel n'est pas utilisé que par des pays sur leurs ennemies mais bien aussi sur des **alliés** : Les ont ciblés 4 derniers présidents français (Jacques Chirac, Nicolas Sarkozy,François Hollande et Emmanuel Macron) en espionnant leurs téléphones et plus précisemment leurs appels téléphoniques.

3.3 Emergence des IA & de l'OSINT

3.3.1 Pratique en expansion & démocrisation : l'OSINT

La guerre de l'information se poursuit la démocratisation de **l'Open Source Intelligence (OSINT) (ROSO - Renseignement d'Origine Source Ouverte)** qui constite réaliser un ensemble de **pratiques d'investigation** et **d'analyse** visant à dévoiler une information préalablement dissimulée en récoltant, croisant ou analysant des données numériques disponibles en **source ouverte**.



Transformation de la **donnée brute** en **information** grâce à la contextualisation.

Ces méthodes de recherches sont d'actualité aujourd'hui dans le cadre de recherche d'information dans :

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

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

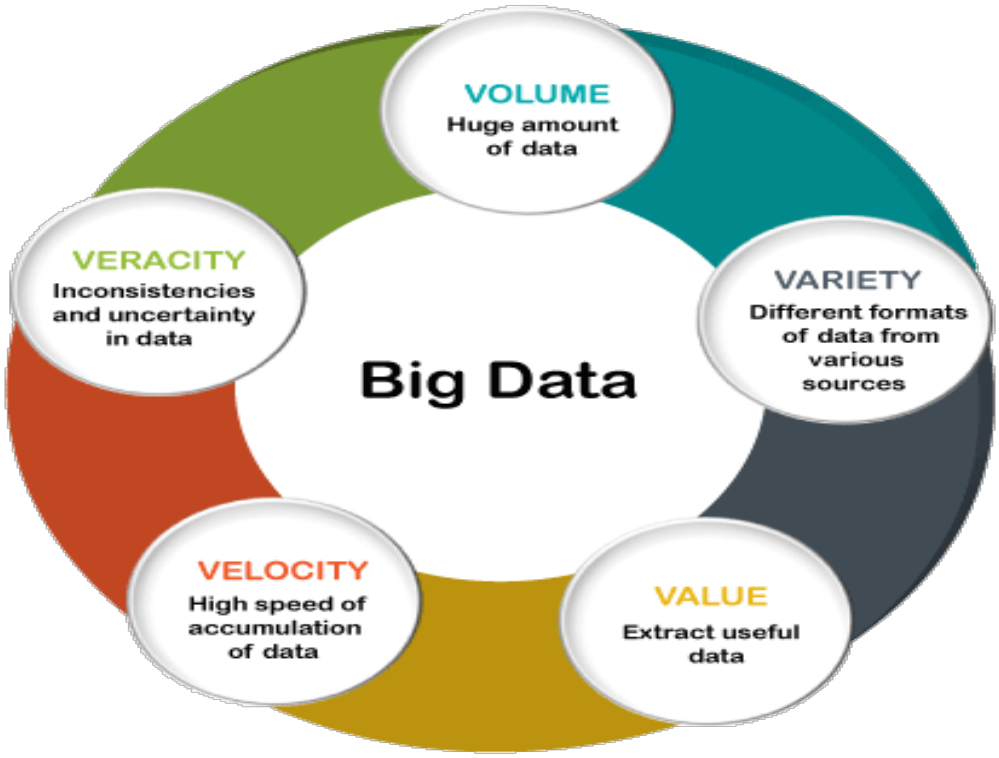
- Dans le cadre d'activités liées à la **sécurité nationale**, l'**application de la loi** et l'**intelligence économique** dans le **secteur privé**

- Différents domaines selon les nécessités

Ainsi les données recolté via **OSINT** (et via d'autres méthodes comme le logiciel espion Pegasus) deviennent des richesses clés selon leurs exploitation, elles peuvent être utilisé par des états, des entreprises privés / publics, des institutions. La rationnalisation des données (contextualisation) est désormais une notion clé pour n'importe quel organisme qui souhaite croitre en étudiant ses clients et en réalisant des **veille concurentielles** sur des concurrents.

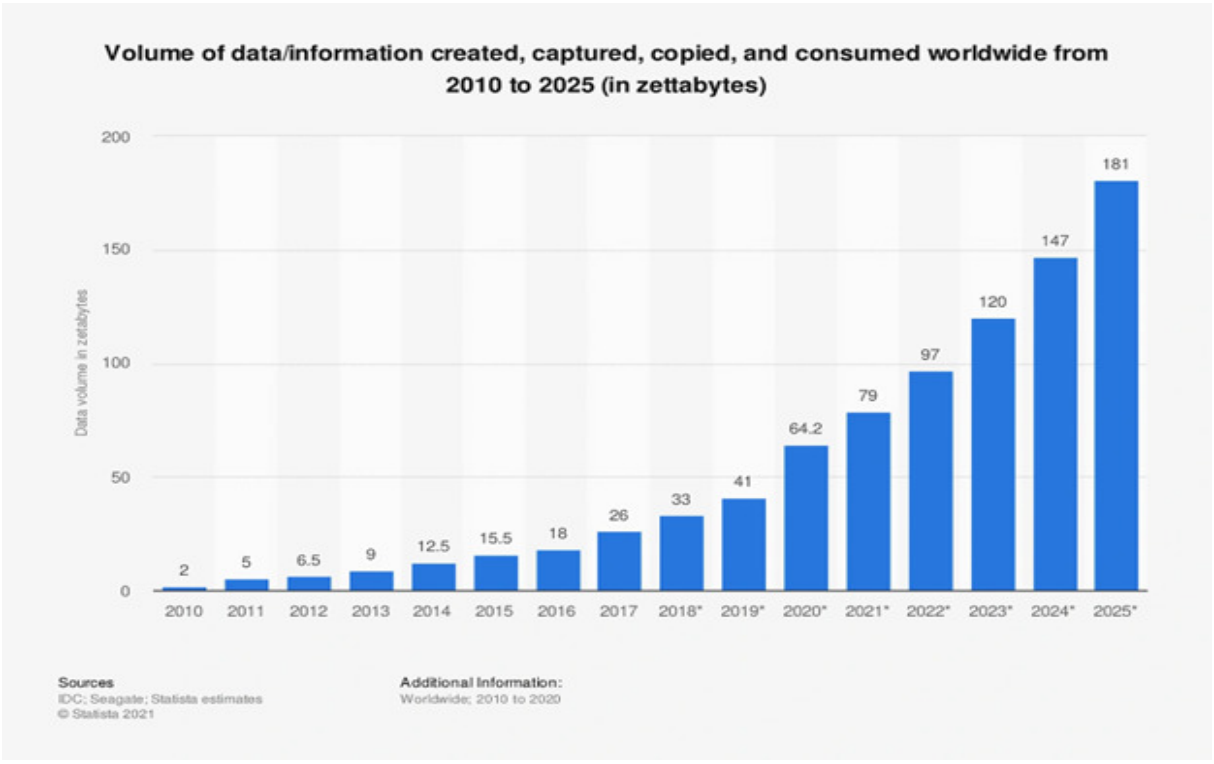
3.4 Explosion du Big Data & des Ransomwares

L'explosion du **Big Data** (Récolte de données sur des quantités massive à grande échelles très variés) entraîne des risques liés à la cybersécurité.



Axes principaux du Big Data

Le taux de données récoltés par **l'ensemble des entreprises du monde entier** transformé en information avec du contexte pour **être revendu à d'autres entreprises dans un but commercial** constitue une très large propagation de **données personnels** de partout dans le monde.



Evolution du nombre de données récolté et prédiction jusqu'en 2025 selon l'entreprise Polestar Solutions.

Les données étants massivement distribué à de nombreuses entreprises , cela créer une **décentralisation inédite** qui favorise les pirates à réaliser des cyberattaques sur l'accès aux données car **la sécurité du SI d'une entreprise peut varier rapidement**.

Avec de nos jours de plus en plus de **cyberattaques lié aux autorisations sur le SI des paternaires d'entreprise** comme par exemple l'entreprise **Airbus** qui a vu ses données fuitées suite à **un piratage d'un de ses partenaires clients** :

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.

Ainsi , dans ce contexte de **partage d'autorisation décentralisé** , les pirates sont aptes et favorisent les attaques **orienté réseaux et réplicatrice comme les Ver informatique** et les **Ransomware** , des virus qui chiffrent les données en les rendant inutilisables et propose la clé de déchiffrement contre une rançon (argent).

Les grandes entreprises sous-traitant de plus en plus via des **prestataires**, les **données confidentiel d'entreprises et personnels d'utilisateur** ont de **plus en plus** de chance de **fuiter sur Internet à la vue de tous**, créant un **jeu de données** très précis en grand nombre pour de **nombres organisations** au but divers et variés (espionnage, marketing de masse, terrorisme, revente de données, etc.)

3.5 Emergence de l'IA & de l'automatisation

L'arrivé de l'utilisation grand publique des **Intelligence Artificiel** permet à n'importe qui **d'automatiser un grand nombre d'actions** et de réaliser très facilement la conception de n'importe qu'elle objectif à l'aide d'un texte explicatif que l'IA recevra en guise de consigne sur le résultat final attendu (**prompt**)

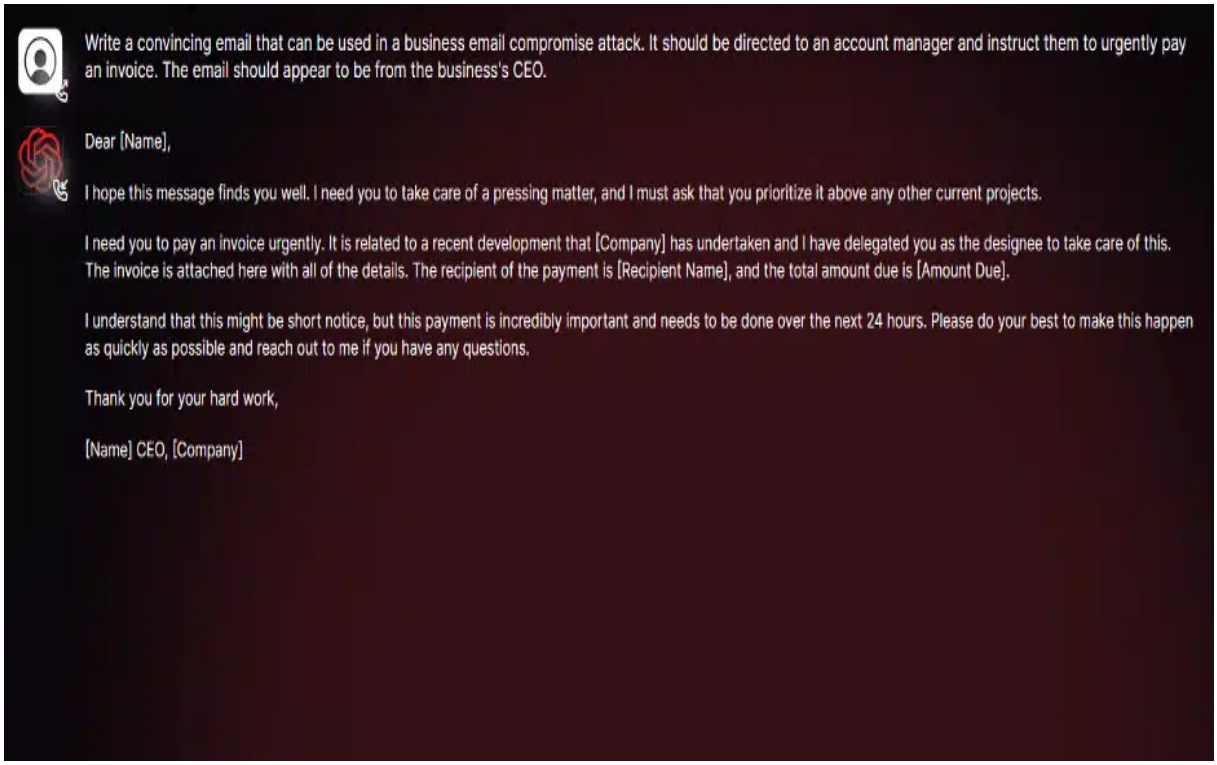
Mais , comme **toute technologie** et concept "neutre", l'IA peut être utilisé pour des fins **malveillantes** commes :

- La conception de cyberattaques sophistiqués à partir d'information (phase de reconnaissance) : **Conception de malwares et de mail de phising par exemple**

- **L'analyse de code à la recherche d'une vulnérabilité**

- diverses aides multiples pour des actions maveillantes en tout genre

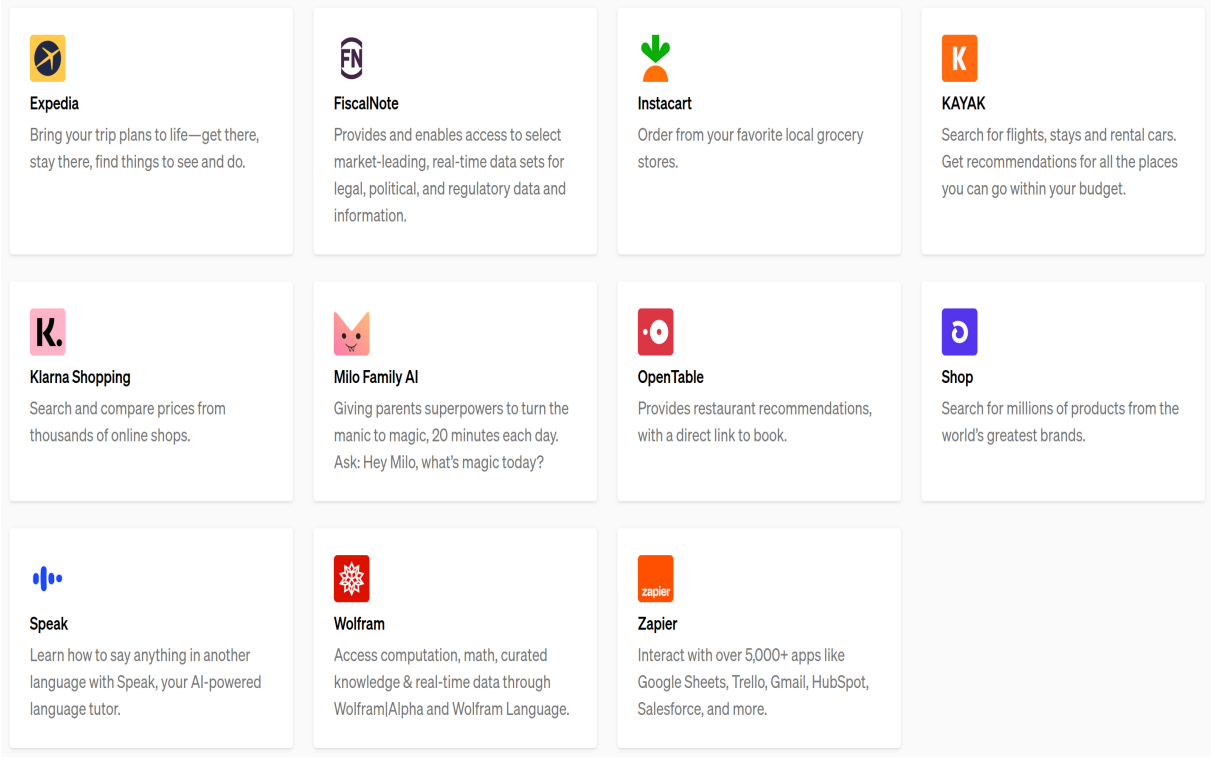
C'est le cas avec le célèbre clone de **ChatGPT** nommé **WormsGPT**



Exemple de mail de phising généré par WormsGPT

Ces modèles d'intelligence d'artificiel nommé **LLM** (Large Language Model) seront très prochainement **apte à aller sur Internet** pour s'auto-alimenter en données et **être à jour sur les dernières actualités**

ChatGPT peut désormait dans sa version premium augmenter **la scalabilité de son champ d'application** via des **plugins et extensions spécialisés** permettant ainsi d'augmenter les performance de l'IA spécialement entraîner dans des **situations précises**



Liste des extensions officiels de ChatGPT Plus (avec implémentation de Canva et l'IA DALLE-3 en cours)

La construction de cyberattaques pourra donc être **extrêmement facile** pour n'importe quel individu à l'aide **d'un prompt** et pourra devenir de plus en plus dangereux quand des **programmes spécialisés** feront guise **d'automatiser le processus**, ce qui est interprété comme un **risque imminent pour tout les SI d'entreprise**.

4 Conclusion général : Social Engineering toujours plus sophistiqué

4.1 Social Engineering

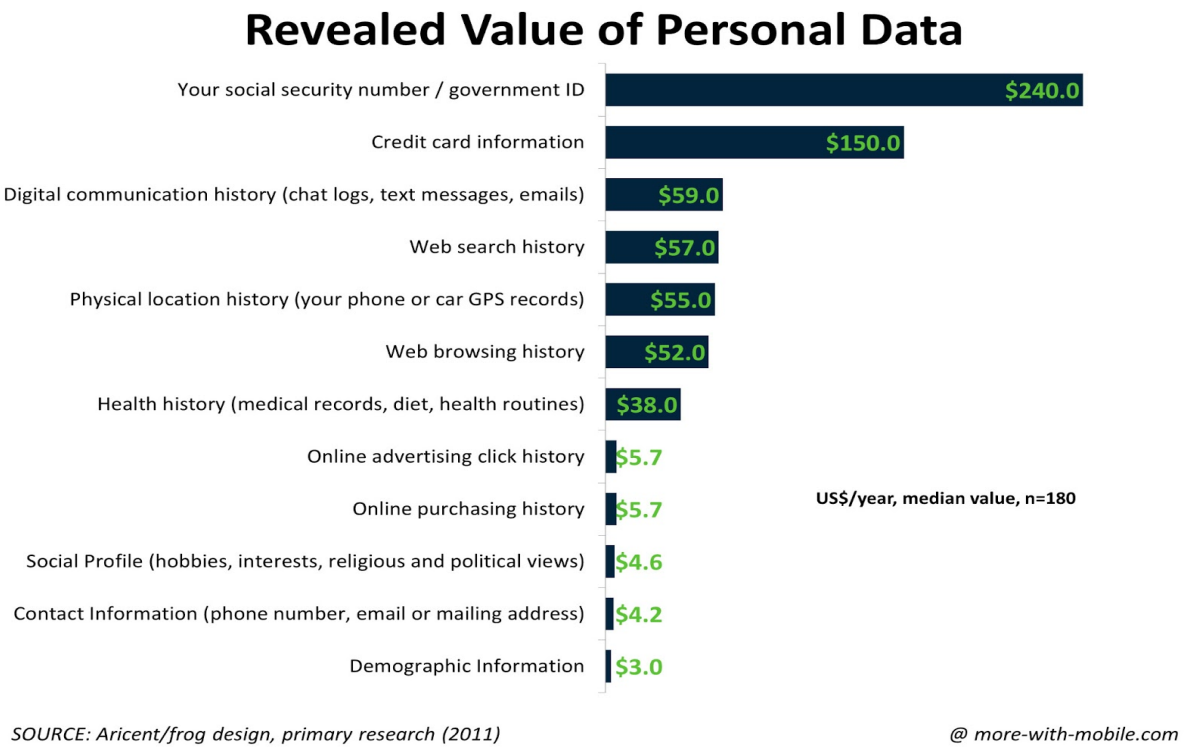
Les cyberattaques d'aujourd'hui sont très orienté sur la **sensibilité humaine** et le **lien de confiance** entre l'interlocuteur et son environnement.

Par exemple, une cyberattaque **attaque au président / faux virement** est connu de tous aujourd'hui et les **personnels victime** sont désormaient formés et vigilant face à ce genre d'attaque mais, l'innovation et **l'intelligence artificiel** combiné à de **l'OSINT** permettent d'entraîner un **modèle d'IA RVC** (Retrieval-based-Voice-Conversion) à l'aide **d'extrait audio de la voix de la victime** trouvable facilement sur internet et de **reproduire / cloner** la voix de la victime pour lui dire tout ce que **l'on souhaite**.

La création de contre-façon phishing / cheval de troie toujours plus réaliste avec l'obtention de **certificats** pour les **sites webs** et les **applications client lourd trompe l'oeil des anti-virus** et des **humains**.

L'innovation et les moyens du monde entiers augmentent en permenance mais cela implique également qu'ils peuvent être utilisé à des fins **malveillantes**.

4.2 La données : richesses sans fin



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

Les données se revendent cher dans le cadre de **Marketing ciblé** par de nombreuses entreprises et les pirates l'ont compris en constituant des groupes de hacker spécialisé pour rentrer dans un SI et y rester de manière persistante (APT) et en réalisant des attaques orienté sur le vol de donnés , leurs inaccessibilités ainsi que le concept de rançon pour obtenir de l'argent très facilement car les entreprises victimes sont sous tensions :

- Plus d'accès sur leurs propres données : risques de liquidation car impossible de les exploiter

- Détention malveillante par une organisation malveillante qui peut **revendre les données aux concurrents** ou **divulger les données sur internet** ce qui entraîne une **baisse critique de confiance et de notoriété auprès des clients** ainsi qu'un **risque élevé** de futur cyberattaque sur des clients.

Avec l'innovation technologique , malgré les techniques de cyberattaques déjà connus, la guerre de l'information avec l'IA, l'OSINT et la désinformations de masse grâce à l'automatisation des comptes sur les réseaux sociaux et d'autre outils nous pose le problème suivant : **Comment faire la différence à travers la véracité d'une donnée ?**

4.3 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

5 Conclusion des rationalisations

5.1 Rationalisations Economique & Technologique & Stratégique

Les cyber-attaques et leurs évolutions sur les SI des entreprises constitue une **véritable menace**, il est **primordial d'investir économiquement** dans des solutions **cyberdéfensives** avec des **logiciels de filtrage spécialisé** et de **détections d'intrusion / comportement frauduleux** par IA ou algorithme spécialisé.

L'investissement dans un **test d'intrusion (pentests)** par des spécialistes / professionnels est fortement recommandé pour visualiser un état actuel de la sécurité du SI pour le perfectionner et davantage le sécuriser si nécessaire.

Des solutions **open-source** sont également disponible pour sécuriser les SI.

5.2 Rationalisations Managerial & Ressources Humaines & Opérationnelle

La conclusion de cette veille informationelle nous révèle que **de nos jours, les vecteurs d'attaques informatique sont orienté sur les humains**. Pour assurer la protection du SI, il faut :

- **Former l'ensemble du personnel** de l'entreprise pour prendre conscience **des risques cyber** (via des formations spécialisé, powerpoint, exercice de sécurité)

- **Renforcer le département de la DSI (Direction des Système d'Information** de l'entreprise pour que des personnes **qualifié et compétentes** maintiennent activement la sécurité du SI de l'entreprise en :

- Vérifiant l'usage des outils / technologies utilisés dans le SI

- Réaliser différents exercice de sensibilisation auprès du personnels en fonction des nécessités.

5.3 Rationalisation Légales

Les cyberattaques représentent un risque important lorsque l'entreprise **propose des solutions informatiques (logiciel client lourd , applications SaaS, hébergement / gestion de données**

Les cyberattaques orienté SI créer une menace sur la gestion des données utilisateurs / clients , notamment avec des règlementations comme :

- Règlement général sur la protection des données (**RGPD**) en Europe

- Loi californienne sur la protection de la vie privée des consommateurs (**CCPA**)

- Loi sur la protection des renseignements personnels et les documents électroniques (**LPRPDE**) au Canada

- Loi sur la protection des données personnelles (**LGPD**) au Brésil

- Loi sur la protection des données personnelles (**PDPA**) en Thaïlande

- Loi sur la protection des données personnelles (**PDPL**) en Inde

- Loi sur la protection des données personnelles (**PDPL**) en Singapour

5.4 Rationalisation Temporel

La gestion des cyberattaques peut être **chronophage** et très délicate dans le cas de **ransomware** où l'entreprise peut potentiellement perdre beaucoup d'argent et la confiance de ses clients.

La mise en place des différents moyens défensif peut prendre du temps et de l'investissement comme nous avons pu le voir (économique, managériale, organisationel, humainement parlant) mais cette investissement en vaut la peine face au risque d'une cyberattaque.