Sandy CERRATO
BTS SIO

HACKERS

Les différents types de malwares

Sommaire

I. Les différents types de malware.
II. Cybersécurité : tour d’horizon des types d’attaques informatiques.
III. Différents profils de Hackers.
IV. Arborescence : Les 10 virus les plus répandus en France en 2020 et leurs catégories.
V. Les cyber attaques les plus courantes contre les entreprises.
VI. Quelques grosses entreprises Françaises touchées par les cyberattaques.
VII. Coût d’une cyber attaque.
VIII. Arborescence : Les coûts des Cyber-attaques les plus courantes en France par an.
IX. Quelques chiffres.
X. BONUS ! TOP 5 des ransomwares les plus insolites du monde.

GLOSSAIRE

- **Spoofing** : Usurpation d'identité électronique.

- **Phishing** : L'hameçonnage (*phishing* en anglais) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance.

- **Attaque DDoS :** Une attaque DDoS vise à rendre un serveur, un service ou une infrastructure indisponible. L'attaque peut prendre différentes formes : une saturation de la bande passante du serveur pour le rendre injoignable, un épuisement des ressources système de la machine, l'empêchant ainsi de répondre au trafic légitime.

- **Cryptojacking** : Le cryptojacking est aussi appelé en anglais bitcoin mining malware (ou minage de cryptomonnaie malveillant en français). C'est une menace qui se cache sur n'importe quel appareil informatique (ordinateur de bureau, ordinateur portable, smartphone ou tablette tactile). Il utilise les ressources de la machine pour miner de la cryptomonnaie c'est-à-dire fabriquer de la monnaie virtuelle.

I. Les différents types de Malware

1- Le ransomware

Apparus pour la première fois en 2012, ces chevaux de Troie sont redoutables. Ils infectent votre ordinateur et cryptent vos fichiers. Sans la clé de décryptage, vos fichiers sont pris en otage.
Vous recevez ensuite une demande de rançon à verser contre l'obtention de la clé de décryptage qui vous rendra vos données. Il va sans dire que, même si c'est tentant, vous ne devez pas payer ! D'une part, rien ne certifie que vous allez récupérer vos fichiers si vous payez, et d'autre part, si plus personne ne paie, cela découragera le cybercriminel de faire de même chez d'autres victimes.

2- Les Fileless Malware

Ce que nous appelons les logiciels malveillants sans fichier n'installent rien au départ : pas de virus, mais ils modifient les fichiers natifs du système d'exploitation.
Et puisque les systèmes d'exploitation reconnaissent les fichiers modifiés et les considèrent comme légitimes, cette attaque n'est pas détectée par un logiciel antivirus.

3- Les Spiwares ou logiciels espions

Les logiciels espions ou « espiogiciels » permettent de connaitre et de collecter toute l'activité de l'utilisateur sur son ordinateur les informations à son insu ou sans son consentement.
Mots de passe, épingles, informations de paiement ou messages, tout est passé au crible.
Les logiciels espions sont regroupés en 2 grandes familles :

a. Keyloggers ou Enregistreurs de frappe

Un enregistreur de frappe surveille l'activité des utilisateurs. Il est souvent utilisé par un patron désirant surveiller l'activité en ligne de ses employés ou par des parents pour surveiller leurs enfants. Mais lorsqu'il est utilisé à des fins malveillantes, il peut vous voler vos mots de passe ou vos codes de carte bancaire.

b. Aware

L'adware n'est pas un virus très agressif. Il se contente de suivre l'activité de navigation d'un utilisateur pour déterminer les annonces à diffuser et de modifier la page de démarrage de votre navigateur internet ou d'installer un plug-in de recherche sur internet. Son but étant de vous faire venir sur un site web pour vous montrer de la publicité et vous voler des informations personnelles afin de les vendre à des annonceurs.

4- Le cheval de Troie

Un cheval de Troie est un logiciel malveillant, souvent téléchargé par mégarde par l'utilisateur qui clique sur la pièce jointe d'un email piégé, qui a pour but de faire profiter à un tiers les ressources de votre ordinateur.

5- Les vers

Les vers ciblent les vulnérabilités des systèmes d'exploitation pour s'installer dans les réseaux. Plus faciles à programmer qu'un virus, ils utilisent internet sous toutes ses formes pour se propager via des emails, des sites web ou des serveurs FTP.
Une fois en place, les vers peuvent être utilisés par les cybercriminels pour lancer des attaques DDoS, voler des données sensibles ou mener des attaques de ransomware.

6- Les virus

Un virus est un morceau de code, un programme qui s'insère dans une application et s'exécute lorsque celle-ci est ouverte. Il a la particularité de s'auto-reproduire en infectant d'autres programmes. Une fois à l'intérieur d'un réseau, il peut être utilisé pour voler des données sensibles, lancer des attaques DDoS ou mener des attaques de ransomware.

7- Les Rootkits

Les rootkits sont des logiciels qui permettent au cybercriminel de contrôler à distance l'ordinateur d'une victime avec des privilèges administratifs complets.

8- Les Botnets ou Bot

Un bot est un logiciel qui exécute des tâches automatisées sur commande. Utilisés à des fins malveillantes, ils se propagent automatiquement et peuvent se reconnecter à un serveur central.
Les bots sont utilisés en très grand nombre pour créer un botnet (un réseau de bots) pour lancer des attaques de grande envergure à distance comme les attaques DDoS.

9- Les logiciels malveillants sur mobiles

Les attaques d'appareils mobiles ont augmenté de 50% en un an ! Elles incluent autant de menaces que sur les ordinateurs de bureau : ransomwares, fraude aux clics publicitaires, vers…

II. Cybersécurité : tour d'horizon des types d'attaques informatiques

- Le cryptojacking, minage de cryptomonnaie malveillant.
- Les ransomwares, rançongiciels.
- Les intrusions sur les objets connectés.
- Les attaques géopolitiques.
- Les scripts intersites ou cross-site scripting (XSS)
- Les malwares sur mobile.
- Le phishing.
- Le spoofing.

III. Différents profil de hackers

Les « white hat hacker »

Un « white hat hacker » peut être considéré comme étant un gentil hacker. Ces experts en informatiques mettent leurs capacités à des fins honnêtes et éthiques. Ils aident les victimes de cybercriminalité en leur assurant une sécurité informatique. Le plus souvent, on trouve ce type de hackers au sein des grandes entreprises et organisations pour sécuriser leurs réseaux et leurs systèmes. Ils contribuent aussi à la création de nouvelles infrastructures et à l'amélioration des celles déjà créées pour de bonnes causes. C'est pour cela qu'ils sont appelés également les hackers éthiques.

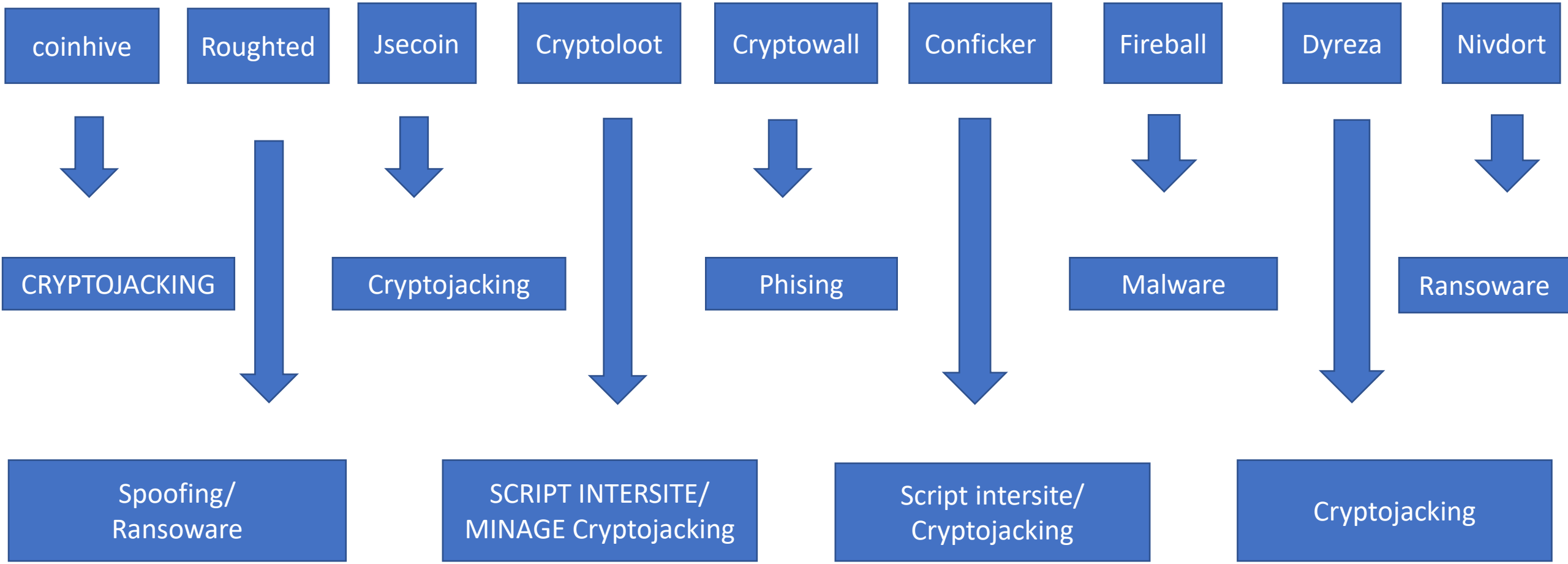
Le « black hat hacker »

Au white hat hackers oppose le « black hat hacker ». Ce dernier est comme un pirate d'internet et est connu pour des œuvres de cybercriminalité. Ce hacker au chapeau noir vole des données, s'introduit illégalement dans les systèmes de grandes entreprises et pirate leurs données ou leurs comptes. Ils gagnent souvent leur vie en vendant les informations personnelles qu'ils volent sur le darknet.

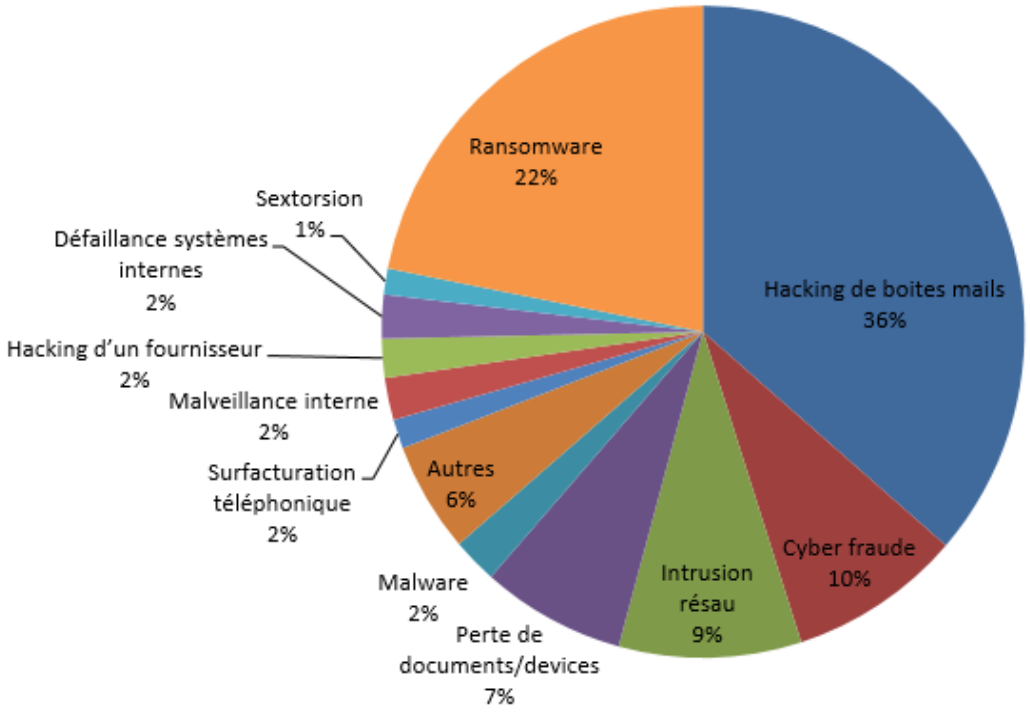
Les « grey hat hackers »

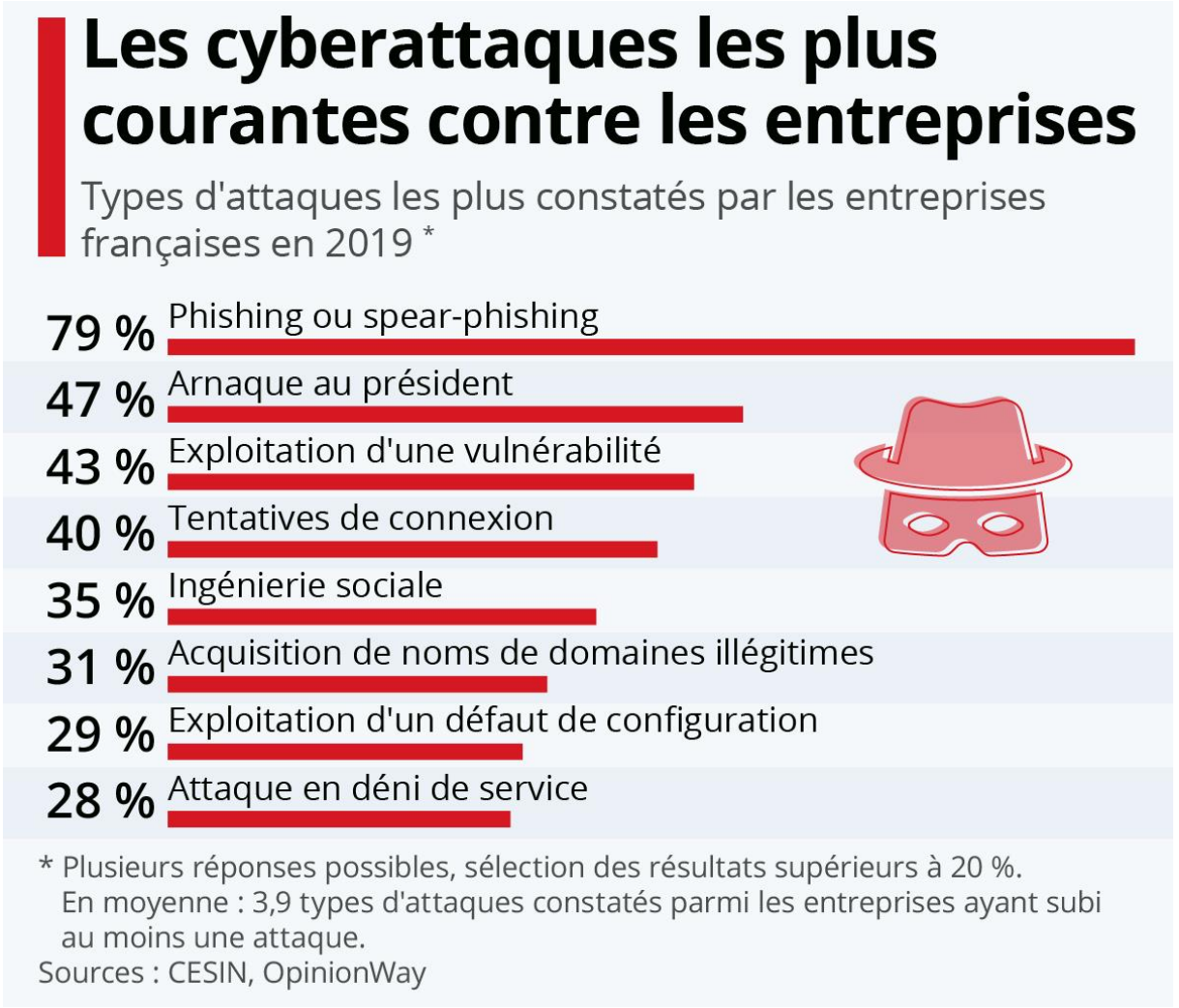
Le hacker au chapeau gris se situe entre le white et le black hacker. Il peut à la fois commettre des délits et des actes de cybercriminalité et agir de façon éthique. Par exemple, il peut s'infiltrer dans un système informatique sans autorisation, et n'avertir l'organisation des failles qu'après le fait accompli et résoudre le problème plus tard. C'est un acte à la fois honorable, mais tout à fait illégal.

IV. Les 10 virus les plus répandus en France en 2020 et leurs catégories



V. Les cyberattaques les plus courantes contre les entreprises





En France en 2020, le coût moyen des cyberattaques s'élève à 35 000€ contre 9 000€ en 2019, soit une augmentation de 290% !

Pour les grandes entreprises (+1000 employés), la moyenne des pertes culmine à 458 000€.

VI. Quelques grosses entreprises Française touchées par les cyberattaques :

- Le laboratoire Expanscience
- Le restaurateur NewRest
- Le « *transporteur* » d'énergie Oviance.
- SPIE groupe
- Sopra Stevia
- Faro technologie
- CHU de Rouen
- Econocom
- MMA
- MisterFly
- CPM

Pour n'en citer que quelleques une …
En effet depuis 2019, les cyberattaques sont en hausse constante, avec des rentabilités qui peuvent atteindre 400%, voire 800% pour les pirates !

CHIFFRES CLÉS	FRANCE
Individus ayant été confrontés à la cyber criminalité depuis un an - Nombre - Pourcentage	19,3 millions 42 %
Coût total de la cyber criminalité depuis un an	€6,1 milliards
Temps moyen passé à gérer les conséquences d'un acte de cyber criminalité	16 heures
Type de cybercrime le plus rencontré depuis un an	Infection par malware 45 %
Type de cybercrime le plus coûteux depuis un an	Fraude à la carte bancaire 1 212€
Pourcentage de cyber victimes ayant déjà partagés au moins un de leurs mots de passe de comptes en ligne • Vs non-victimes	41 % 21 %
Pourcentage de cyber victimes utilisant le même mot de passe pour tous leurs comptes en ligne • Vs aux non-victimes	23 % 12 %
Pourcentage de victimes de ransomware ayant payé leur rançon sans retrouver l'accès à leurs fichiers	22 %
Pourcentage d'individus déclarant qu'un cyber crime doit être traité comme toute autre acte criminel	80 %
Pourcentage d'individus qui jugent les actes suivants comme parfois acceptables : • Lire les e-mails d'une autre personne sans son accord • Partager des informations que l'on sait fausses sur les réseaux sociaux • Dérober les informations personnelles d'un tiers	 29 % 22 % 15%
Pourcentage de cyber victimes qui, après une cyber attaque, ont confiance en leur capacité à protéger leurs données personnelles	43%
Pourcentage d'individus pensant que les informations qu'ils postent sur les réseaux sociaux peuvent aider les cyber criminels	75 %
Pourcentage d'individus considérant que les organisations législatives et entreprises du Web devraient mieux protéger les consommateurs	82 %

VII. Coûts d’une cyber attaque

Afin de me faire une idée des coûts réels d’une cyberattaque, je suis allée sur le site «Cyber calculator» .

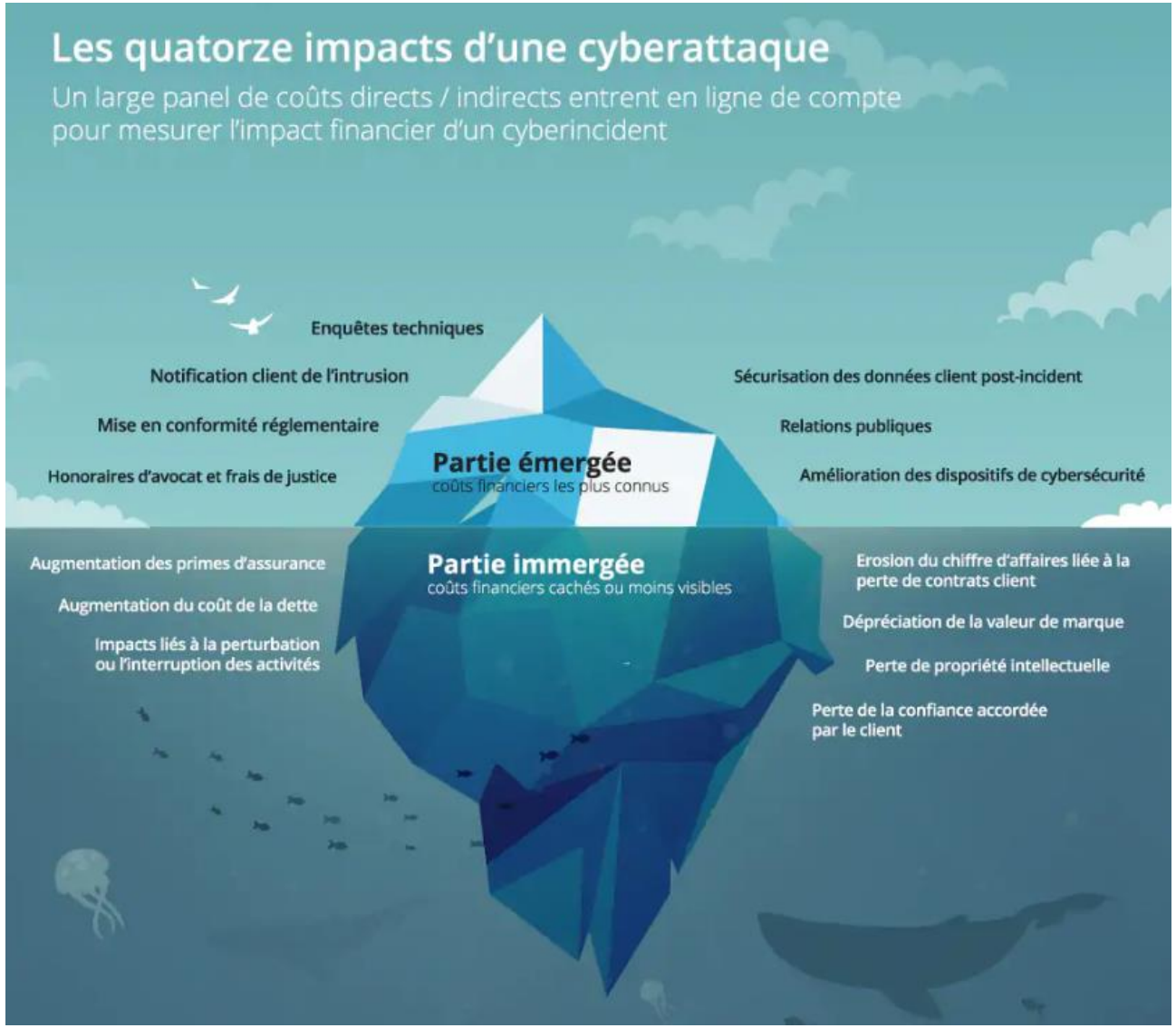
J’ai choisi une PME avec comme secteur d’activité la construction et un revenu de 250K€ par an.

Résultat édifiant, en cas de piratage informatique la perte estimée serait de 52.3K€ !!

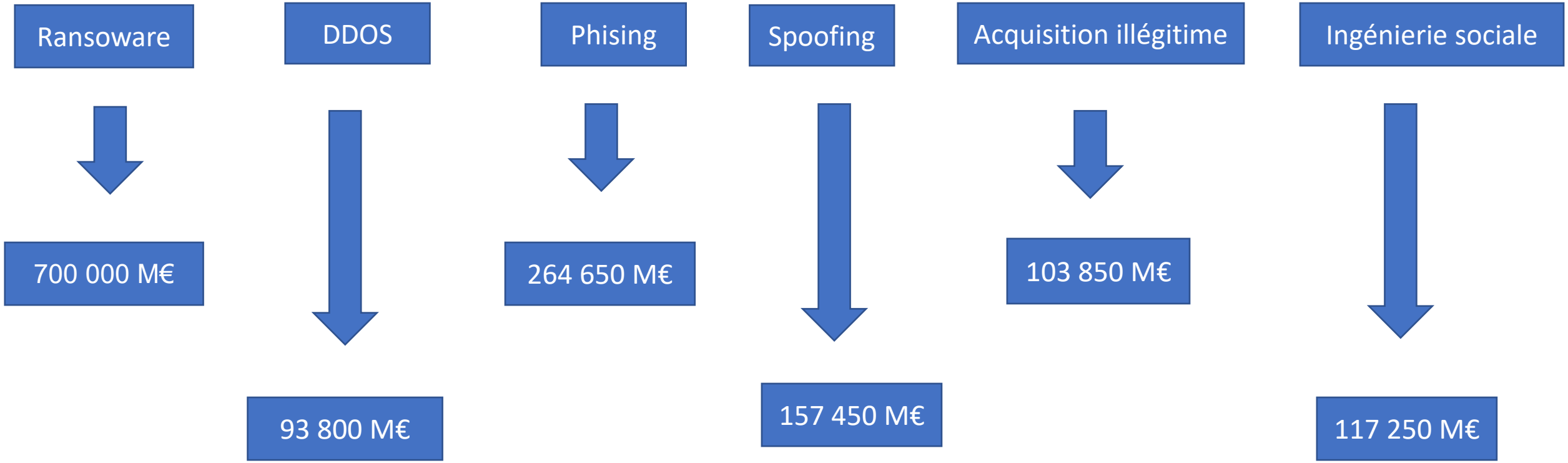
Expérience n°2 : avec cette fois le secteur service publique et réseaux et un revenu de 1M€ par an.

Résultat : 144.8K€ !

Mieux vaut donc protéger son entreprise au maximum.



VIII. Les coûts des Cyber-attaques les plus courantes en France par an



Seulement 3 % des dossiers d'une entreprise sont protégés

IX. Quelques chiffres

- 3 minutes pour pirater un nouvel objet connecté

- 1,1 million de victimes de fraude à la carte bancaire par an

- 41 % : le taux de succès d'un ransomware

- 201 jours pour découvrir une cyberattaque

- 140 attaques de phishing par heure

- Une entreprise subit 29 cyberattaques par an

- 65 vols de données par seconde

- Les entreprises qui ont endigué une fuite de données en moins de 30 jours ont économisé plus d'1 million de dollars par rapport à celles qui ont mis plus de temps

- 88 % des entreprises qui détiennent plus d'1 million de dossiers ont 100 000 dossiers accessibles à tous les employés

Le nombre d'entreprises françaises ayant déclaré des cyberattaques est en baisse cette année : 65 % ont déclaré avoir subi au moins une attaque au cours des douze derniers mois (en janvier 2020), contre 80 % l'année précédente. Ce qui est quand même une bonne nouvelle !

X. BONUS ! TOP 5 des ransomware les plus insolites du monde

Jigsaw (angoissant, sur le principe du film, toutes les heures des données sont effacées et la rançon augmente)

Cryptmix (ransomware caritatif, les fonds sont reversés à diverses associations)

Spora (sur le principe du marketing ! En effet, plusieurs options de rançon possible : chiffré, déchiffré, promesse de ne plus être infecter... Et en plus les 2 premiers fichiers sont restitués gratuitement ! Beau geste)

Popcorn time (le principe est social. Il faut tenter d'infecter plusieurs de ses connaissances et attendre qu'au moins deux d'entre elles payent la rançon. Les fichiers vous seront alors restitués)

Rensenware (Pour déchiffrer et récupérer ses fichiers, rien de plus simple : terminer un jeu. En théorie, car dans la pratique, le jeu était configuré en mode hardcore)