



**Faculté d'Informatique**

**Département des Systèmes Informatiques (DSINF)**

# **Mémoire de Master**

**Spécialité : Sécurité des Systèmes Informatiques (SSI)**

**Thème**

Conception et Réalisation d'un outil d'analyse  
et de detection de ransomware

**Présenté par :**

— BOUSSOURA Mohamed Cherif  
— HOUANTI Narimene

**Encadré par :**

— ISSAD Adel (Ooredoo)  
— BOUACHI Farida (USTHB)

Binome N° : SSI 019/2023

# Résumé

Mots clés : ...

# Remerciements

Au terme de ce travail, je tiens à exprimer ma profonde gratitude à notre cher encadrant de la société M. ISSAD Adel pour son suivi et pour son énorme soutien, qu'il n'a cessé de nous prodiguer tout au long de la période du projet.

Je tiens à remercier également mon encadrant de l'université Mem BOUACHI Farida pour le temps qu'elle a consacré et pour les précieuses informations qu'elle m'a prodiguées avec intérêt et compréhension.

J'adresse aussi mes vifs remerciements aux membres des jurys pour avoir bien voulu examiner et juger ce travail. Mes remerciements vont à tout le personnel que j'ai contacté durant mon stage au sein de l'entreprise Ooredoo, auprès desquelles j'ai trouvé l'accueil chaleureux, l'aide et l'assistance dont j'ai besoin.

Je ne laisserai pas cette occasion passer, sans remercier tous les enseignants et le personnel de l'université, et particulièrement ceux de la spécialité Sécurité des systèmes informatiques (SSI) pour leur aide et leurs précieux conseils et pour l'intérêt qu'ils portent à ma formation.

Enfin, mes remerciements à tous ceux qui ont contribué de près ou de loin au bon déroulement de ce projet.

# TABLE DES MATIÈRES

<b>Table des Figures</b>	<b>4</b>
<b>Liste des Tableaux</b>	<b>5</b>
<b>Introduction générale</b>	<b>6</b>
<b>0 Présentation de l'organisme d'accueil</b>	<b>7</b>
0.1 Introduction . . . . .	8
0.2 Cadre du projet . . . . .	8
0.3 Présentation de Wataniya Télécom Algérie (WTA) . . . . .	9
0.4 Les valeurs d'Ooredoo . . . . .	9
0.5 L'architecture structurelle de l'entreprise . . . . .	10
0.6 Les directions d'accueil . . . . .	12
0.6.1 Directions IT Operations : . . . . .	12
0.6.2 Le sous système opération OSS . . . . .	13
0.6.3 La Direction de Sécurité . . . . .	14
<b>1 État de l'art</b>	<b>15</b>
1.1 Introduction . . . . .	16
1.2 Quelques notions . . . . .	16
1.2.1 Généralités sur la cybersécurité . . . . .	16
1.2.2 Types de cybersécurité . . . . .	16
1.2.3 Malware . . . . .	18
1.2.4 Ransomware . . . . .	23
1.2.5 Impact . . . . .	25
1.3 conclusion . . . . .	27
<b>2 Analyse des malwares</b>	<b>28</b>
2.1 Introduction . . . . .	29
2.2 Définition l'analyse de malware . . . . .	29
2.3 Objectifs de l'analyse de malware . . . . .	30
2.4 Exigences de l'analyse de malware . . . . .	31
2.5 Types et Techniques d'analyses de malwares . . . . .	32
2.5.1 Analyse Statique . . . . .	32
2.5.2 Analyse Dynamique . . . . .	40
2.5.3 Analyse Hybride . . . . .	44
2.6 Conclusion . . . . .	44

## TABLE DES FIGURES

1	Photo d'entreprise Ooredoo. . . . .	8
2	Ooredoo Algérie logo . . . . .	9
3	Organisation structurelle d'Ooredoo . . . . .	11
1.1	Types de cybersécurité . . . . .	17
1.2	Nombre annuel d'attaques de logiciels malveillants dans le monde de 2015 au premier semestre 2022 (en milliards) . . . . .	20
1.3	Types des malwares . . . . .	22
1.4	Païement de rançon par trimestre [1] . . . . .	26
2.1	Organigramme du processus de rétro-ingénierie . . . . .	30
2.2	La règle YARA a l'extension .yara . . . . .	33
2.3	Le classificateur de forêt aléatoire pour l'analyse statique. . . . .	35
2.4	Représentation simplifiée de la structure du format PE (Portable Executable). . . . .	36
2.5	Une partie des chaînes de caractères extraites d'un fichier suspect. . . . .	37
2.6	Le classificateur de forêt aléatoire pour l'analyse dynamique. . . . .	42
2.7	Logo de virustotal. . . . .	43
2.8	Logo de Scanii. . . . .	43
2.9	Logo d'Intezer. . . . .	43

LISTE DES TABLEAUX

1.1 Famille de malware . . . . . 21

1.2 Types des ransomwares . . . . . 24

2.1 Précisions des algorithmes . . . . . 35

## INTRODUCTION GÉNÉRALE

# CHAPITRE 0

## PRÉSENTATION DE L'ORGANISME D'ACCUEIL



## 0.1 Introduction

Dans ce chapitre, nous allons présenter notre projet ainsi que l'organisme d'accueil qui est Ooredoo Algérie, tout en précisant ses activités ainsi que ses objectifs. Ensuite nous allons faire une description de notre projet afin d'expliquer son contexte et son objectif.

## 0.2 Cadre du projet

Notre projet intitulé « Conception et implémentation d'un outil d'analyse et de détection de Ransomwares. » est réalisé dans le cadre de présentation du projet de fin d'études en vue de l'obtention du diplôme de master en Sécurité des Systèmes Informatiques (SSI) à l'université des sciences et de la technologie Houari-Boumédiène durant l'année universitaire 2022/2023.



FIGURE 1 – Photo d'entreprise Ooredoo.

### 0.3 Présentation de Wataniya Télécom Algérie (WTA)

**Ooredoo** est une compagnie internationale leader des télécommunications qui fournit les services de téléphonie mobile, fixe et l'Internet haut débit et les services entreprise adaptés aux besoins des particuliers et des entreprises à travers les marchés du Moyen Orient, d'Afrique du Nord et du Sud-est asiatique.

**Ooredoo Algérie** précédemment connu sous le nom Nedjma est le troisième opérateur (en termes de date d'entrée en vigueur) de téléphonie mobile en Algérie. C'est la marque commerciale mobile de Wataniya Télécom Algérie.

Présent en Algérie depuis le **23 décembre 2003**, date d'obtention de la licence de fourniture des services de téléphonie mobile en Algérie, la marque Nedjma a été commercialement lancée le **24 Août 2004**, en offrant aux Algériens, qu'ils soient clients particuliers ou entreprises, une gamme d'offres et de services novateurs, en respect avec les standards internationaux.

Premier opérateur multimédia de téléphonie mobile en Algérie, Nedjma, devenue Ooredoo le **21 Novembre 2013**, est la filiale algérienne du Groupe Ooredoo. Ce dernier s'est établi à plus de 14 millions à la fin de l'année 2016.



FIGURE 2 – Ooredoo Algérie logo

### 0.4 Les valeurs d'Ooredoo

Les valeurs de Ooredoo sont les principes sur lesquels elle se base pour évoluer dans son secteur et prendre ses décisions stratégiques, à savoir :

- **Caring** : pour le soutien, la confiance, le respect d'autrui et la responsabilité qu'Ooredoo incarne.
- **Connecting** : pour l'engagement d'Ooredoo à travailler dans un esprit collaboratif et en intégrant parfaitement la communauté algérienne.

- **La sécurité des données** : qui vise à protéger les données sensibles ou confidentielles contre les accès non autorisés, les vols ou les pertes.
- **Challenging** : pour le progrès auquel aspire Ooredoo et la recherche continue de l'amélioration et de la différence. Ooredoo dispose d'un réseau technique performant, couvrant 99% de la population algérienne, et d'un service regroupant un vaste réseau de boutiques réparti sur tout le territoire national, dont 107 Espaces Ooredoo, 3 VIP Shops (Centre de service), 74 City Shops, 9 Shops in Shop et 345 Espaces Services Ooredoo.

## 0.5 L'architecture structurelle de l'entreprise

L'entreprise est constituée de différentes directions tel que le Marketing, le RH et Technologie, etc. . . Notre projet de fin d'étude fait partie de la direction de technologie et spécialement au service information on security planning. Ce dernier est composé de trois directions qui sont reliés entre eux en effectuant les meilleures solutions dans le but d'amélioration du réseau , ils sont classées en trois catégories :

- Direction plannification (Engenering).
- Direction de sécurité.
- Direction d'opération.

La Figure 3 représente l'hierarchie global de l'entreprise ooredoo

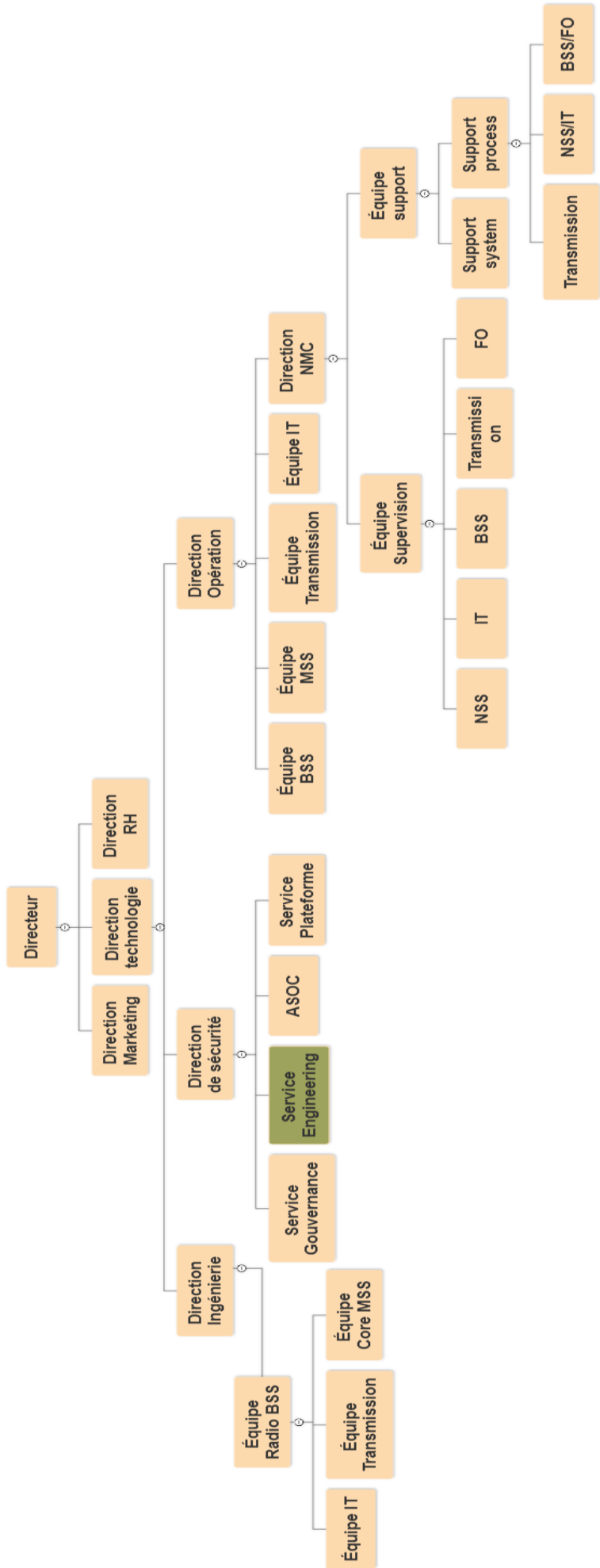


FIGURE 3 – Organisation structurelle d'Ooredoo

## 0.6 Les directions d'accueil

L'entreprise nous a accueillis au sein de son département de sécurité qui compte plusieurs équipes et un grand nombre d'employés.

### 0.6.1 Directions IT Operations :

Cette directions est composé de plusieurs petites équipes travaillant ensemble pour garantir une coordination efficace et une collaboration harmonieuse. Parmi ces équipes, on peut citer :

- a) **Équipe Project Management** : Cette équipe contribue au bon déroulement de tous les projets informatiques de son service en servant de lien entre les différentes équipes informatiques et en s'assurant qu'elles collaborent efficacement.
- b) **Équipe Automatisation des Tâches** : Ce groupe est chargé du développement des flux d'automatisation, également connus sous le nom de « workflows », qui sont demandés par les clients internes ou recommandés par l'équipe de gestion de projet.
- c) **Équipe Virtualisation Serveur** : Cette équipe assure la conversion des machines physiques en machines virtuelles (P2V) et veille au bon fonctionnement de l'ensemble des serveurs virtuels ainsi que de la plateforme de virtualisation.
- d) **Équipe Virtualisation Poste de Travail** : Ce groupe permet de :
  - L'objectif de cette équipe est de déployer une plateforme de postes de travail virtuels et de garantir le bon fonctionnement de l'infrastructure de la VDI (Virtual Desktop Infrastructure).
  - La mission de cette équipe est de fournir aux utilisateurs un accès à leurs postes de travail à partir de n'importe quel endroit et sur n'importe quel dispositif, conformément au principe "Any where, any time, any device".
- e) **Équipe Virtualisation d'application** : est chargé de rendre les applications disponibles de manière virtuelle, sans installation locale nécessaire, aux utilisateurs finaux via un magasin d'applications. Leur objectif est de permettre un accès transparent aux applications depuis n'importe quel endroit, à tout moment et sur n'importe quel appareil, en suivant le principe « Any where, any time, any device ».
- f) **Équipe OS et System Center** : consiste à assurer la gestion du parc informatique, des PC et des serveurs Windows, ainsi qu'à surveiller ces serveurs grâce à une fonctionnalité de « monitoring ».

g) **Équipe Network** : Cette équipe est chargée de :

- L'équipe est en charge d'attribuer et de gérer les accès réseau des clients connectés en Wifi ou par câble.
- Elle assure également l'attribution des accès réseau aux différents types de terminaux tels que les téléphones IP, les caméras, les imprimantes, etc.
- Enfin, l'équipe configure des solutions d'équilibrage de charge réseau pour les applications et portails web de l'entreprise.

h) **Direction NMC Supervision** La direction NMC (Network Management Center) surveille le réseau en continu (24h/7j) en recevant des alarmes de différents niveaux de gravité. En cas de dépassement de service, il envoie des messages instantanés (IMs) au service des opérations pour enquêter et résoudre les problèmes qui affectent les performances du réseau et des tâches.

D'autre part, ce service reçoit des demandes de changement du service d'ingénierie pour effectuer les changements nécessaires. La direction NMC est composé de plusieurs équipes, dont :

1. **Équipe process** : est chargée de superviser les alarmes et de détecter les anomalies au niveau des nœuds des différentes plates-formes. Elle est responsable de suivre les performances en définissant les indicateurs clés de performance (KPIs), en assurant un reporting au management et en définissant des processus pour encadrer les travaux d'instruction afin de décrire les processus de dépannage. Chaque élément de l'équipe assure également un support technique aux ingénieurs de supervision de chaque shift. Elle est composée de plusieurs sous-équipes spécialisées :

- Équipe ( NSS / IT) ;
- Équipe transmission ;
- Équipe (BSS /FO).

Un coaching continu est assuré pour garantir la passation efficace de nouveaux équipements, plates-formes ou changements sur le réseau.

2. **Équipe système** :L'équipe système prend en charge les demandes de l'équipe de supervision pour les problèmes logiciels liés aux outils de supervision, ainsi que pour les problèmes matériels liés aux machines et équipements.

### 0.6.2 Le sous système opération OSS

Le sous-système opérationnel OSS est utilisé par l'opérateur Ooredoo pour superviser son réseau de manière globale via le NMC. Les OSS utilisés sont

différents selon la technologie et l'équipement déployé par les fournisseurs tels que Ericsson, Nokia et ZTE. Les différents OSS utilisés par Ooredoo sont classés selon les plates-formes :

a) **La partie radio (BSS) :**

1. Netact Radio de la technologie NOKIA ;
2. OSS-RC Radio de la technologie ERICSSON ;
3. Net newmen de la technologie ZTE ;

b) **La partie core (NSS) :**

1. Netactcore de la technologie NOKIA (MSS, SGSN, SGGN...);
2. OSS-RC de la technologie ERICSSON ( soft ware, hard ware, MPLS....).

c) **La partie transmission :**

1. OSS-SOEM de la technologie ERICSSON ;
2. Net viewer de la technologie NOKIA ;
3. PNMSG ;
4. NMS5.

d) **La partie IT :**

1. NNRI-HP (Rt, soft ware, hard ware...);
2. OVO-HP (unix, linux...);
3. SCOM (windows...);
4. OSS-RC (plate-forme CBIO).

### 0.6.3 La Direction de Sécurité

Cette direction est chargée de préserver les actifs (à savoir l'infrastructure et les données) d'Ooredoo Algérie, ainsi que les données personnelles de ses clients.

- a) **Service Gouvernance :** Se charge de tous ce qui est process, audit workflow de l'entreprise.
- b) **Service Engineering :** Se charge de la planification, design, implementation des nouveaux projets cyber-sécurité ainsi que de données des recommandations cyber-sécurité au nouveau projet Technology.
- c) **ASOC :** Se charge de l'administration, support des plateformes de sécurité (AV, proxy, relais-smtp, SIEM).
- d) **Service Plateforme :** Se charge du monitoring de la sécurité 24/24, 7/7 elle se compose de 3 niveaux (Analyst N1, Analyst N2, Analyst N3 Threat Hunting and Incident Handling).

# CHAPITRE 1

## ÉTAT DE L'ART



## 1.1 Introduction

Les ransomwares sont l'un des types de logiciels malveillants les plus destructeurs et coûteux en termes de dommages pour les individus, les entreprises et les organisations gouvernementales. Dans ce chapitre nous allons présenter la cybersécurité, ses types, la politique de sécurité d'un système d'information, ainsi que les malwares, son historique, ses familles, son fonctionnement et ses objectifs. Par la suite nous définissons le ransomware, son fonctionnement, ses types, son impact et à la fin la protection.

Dans ce chapitre, nous allons définir les mots clés ainsi que les notions de base qui font l'objet de notre mémoire.

## 1.2 Quelques notions

### 1.2.1 Généralités sur la cybersécurité

#### 1.2.1.1 La cybersécurité

La cybersécurité consiste à protéger les ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données contre les attaques malveillantes. On l'appelle également sécurité informatique ou sécurité des systèmes d'information. [17]

### 1.2.2 Types de cybersécurité

Il existe différents types de cybersécurité, notamment :

- La sécurité des réseaux : qui comprend les mesures de protection pour les réseaux informatiques contre les attaques externes ou internes.
- La sécurité des applications : qui concerne la protection des applications et des systèmes contre les vulnérabilités connues ou inconnues.
- La sécurité des données : qui vise à protéger les données sensibles ou confidentielles contre les accès non autorisés, les vols ou les pertes.
- La sécurité physique : qui concerne la protection des infrastructures et des équipements physiques contre les dommages ou les pertes.
- La sécurité des utilisateurs : qui comprend la sensibilisation, la formation et la préparation des utilisateurs pour mieux gérer les risques de cybersécurité.

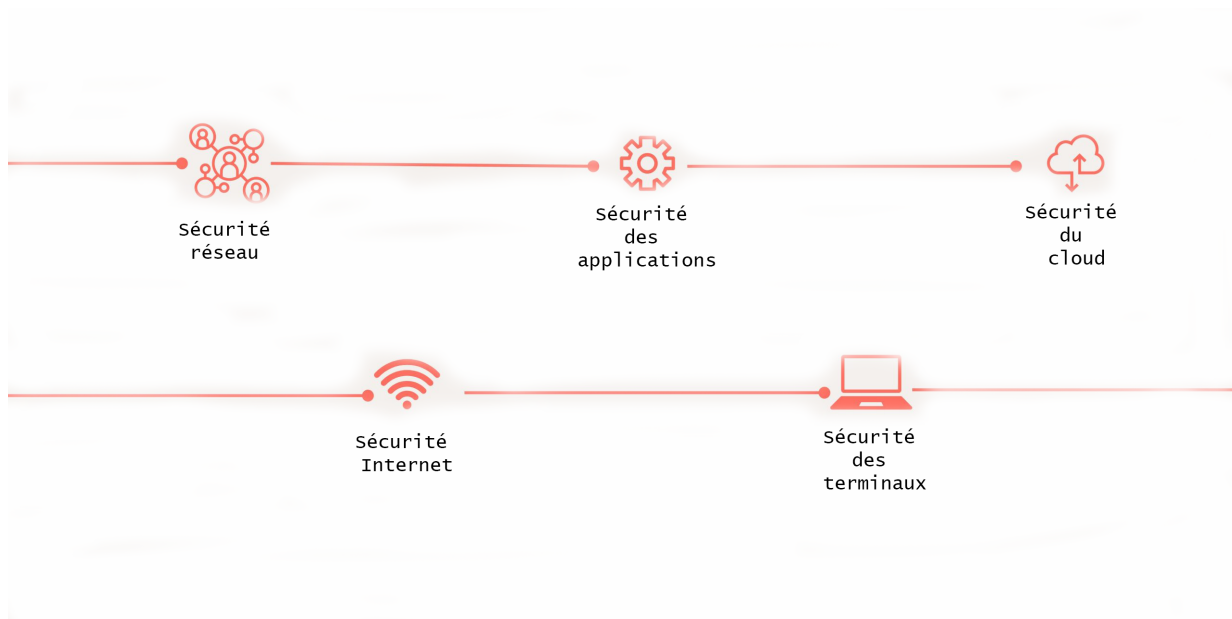


FIGURE 1.1 – Types de cybersécurité

#### 1.2.2.1 Les vulnérabilités, risques et menaces

Les vulnérabilités, les risques et les menaces sont tous des concepts liés à la cybersécurité.

- **Vulnérabilités** : il s'agit de vulnérabilités dans les systèmes informatiques, les réseaux ou les applications que les attaquants peuvent exploiter pour s'introduire dans les systèmes et provoquer la corruption ou la perte de données.
- **Risques** : Ce sont les conséquences possibles des vulnérabilités. elles peuvent inclure la perte de données, l'invasion de la vie privée, la fraude, le vol d'identité, etc. elles sont souvent classés en fonction de leur probabilité et de leur impact.
- **Menaces** : il s'agit d'attaques potentielles qui peuvent exploiter des vulnérabilités pour causer des dommages ou des victimes. ils peuvent être internes ou externes à l'organisation.

#### 1.2.2.2 La politique de sécurité d'un système d'information (PSSI)

La Politique de Sécurité du Système d'Information (PSSI) est un ensemble de politiques, de procédures et de règles visant à assurer la sécurité des informations du système d'information. Il assure la disponibilité, l'intégrité, la confidentialité et la traçabilité des données stockées et traitées par le système informatique. Les éléments clés de l'ISSP comprennent :

- **L'identification des actifs critiques** : Les données et les systèmes critiques sont identifiés et leur niveau de sensibilité est évalué.

- L'analyse des risques : Les risques potentiels sont identifiés et évalués, en prenant en compte leur impact sur les actifs critiques.
- Les mesures de sécurité : Les mesures de sécurité appropriées sont mises en place pour minimiser les risques identifiés.
- Les procédures de contrôle : Les procédures de contrôle sont établies pour surveiller et gérer la sécurité du système d'information.
- La sensibilisation à la sécurité : La sensibilisation à la sécurité est assurée pour les utilisateurs du système d'information.

Une PSSI bien conçue peut aider à atténuer le risque de violation de données et à assurer la continuité des activités en cas de panne ou d'incident de sécurité. C'est également un élément clé pour garantir le respect des réglementations en matière de sécurité de l'information.

### 1.2.3 Malware

#### 1.2.3.1 Définition

ou logiciel malveillant, est un type de logiciel conçu pour causer des dommages à un ordinateur, un réseau ou un système informatique, ou pour collecter des informations sensibles sans autorisation. Les malwares sont créés par des cybercriminels pour voler des informations, extorquer de l'argent, dégrader les performances des ordinateurs ou même prendre le contrôle de systèmes entiers.

#### 1.2.3.2 Historique

Il y a eu de nombreux malwares au fil des ans, et leur histoire remonte aux premiers jours de l'informatique. Voici quelques exemples de malwares notables et de leur histoire :

- Les années 80 : Le fondement théorique des « automates autoreproducteurs » (c'est-à-dire des virus) remonte à un article publié en 1949, et les premiers virus sont apparus sur les ancêtres des plateformes informatiques dans les années 1970. Cependant, l'histoire des virus modernes débute avec un programme appelé Elk Cloner, qui a commencé à infecter les systèmes Apple II en 1982. Disséminé par des disquettes infectées, ce virus n'était pas dangereux en soi, mais sa capacité à contaminer toutes les disquettes d'un système lui a permis de se propager si rapidement qu'il a été considéré comme la première infection par un virus informatique à large échelle de

l'histoire. On peut noter que ce virus a surgi avant le premier malware ciblant les ordinateurs Windows. Depuis, les virus et les vers se sont devenus monnaie courante.[11]

- Les années 90 : La plateforme Microsoft Windows est apparue au cours de cette décennie, en même temps que les macros flexibles de ses applications, qui ont incité les créateurs de malwares à écrire un code infectieux en langage macro de Microsoft Word ainsi que d'autres programmes. Ces macrovirus ont infecté des documents et des modèles, plutôt que des applications exécutables, bien que strictement parlant, les macros de documents Word soient une forme de code exécutable.[11]
- 2002 à 2007 : Des vers de messagerie instantanée (code malveillant qui se reproduit disséminé via un réseau de messagerie instantanée) exploitent les failles du réseau pour se propager à grande échelle, infectant le réseau AOL AIM, MSN Messenger et Yahoo Messenger, ainsi que des systèmes de messagerie instantanée d'entreprise.[11]
- 2005 à 2009 : Les attaques d'adware prolifèrent et affichent des publicités indésirables sur les écrans des ordinateurs, parfois sous la forme de pop-ups ou d'une fenêtre que les utilisateurs ne peuvent pas fermer. Ces publicités exploitent souvent des logiciels légitimes pour se propager, mais vers 2008, les éditeurs de logiciels se mettent à poursuivre les entreprises d'adware pour fraude. Il en a résulté des millions de dollars d'amendes, ce qui a entraîné la fermeture des entreprises d'adwares.[11]
- 2013 : Une nouvelle forme de malware, appelée ransomware, lance une attaque sous le nom de CryptoLocker, qui s'est étendue de début septembre 2013 à fin mai 2014, visant les ordinateurs sous Windows. Au dernier trimestre 2013, CryptoLocker était parvenu à forcer ses victimes à verser environ 27 millions de dollars. En outre, le succès de ce ransomware a donné naissance à d'autres ransomwares du même nom. Une variante imitatrice de CryptoLocker a soutiré plus de 18 millions de dollars à près d'un millier de victimes entre avril 2014 et juin 2015.[11]
- 2013 à 2017 : S'immisçant dans les chevaux de Troie, les exploits, le malvertising et les ransomwares sont devenus les rois des logiciels malveillants,

aboutissant en 2017 à de gigantesques attaques qui ont affecté des entreprises de toutes sortes. Les ransomwares cryptent les données des victimes puis exigent des paiements pour les libérer.[11]

- 2013 à 2017 : S’immisçant dans les chevaux de Troie, les exploits, le malvertising et les ransomwares sont devenus les rois des logiciels malveillants, aboutissant en 2017 à de gigantesques attaques qui ont affecté des entreprises de toutes sortes. Les ransomwares cryptent les données des victimes puis exigent des paiements pour les libérer.[11]

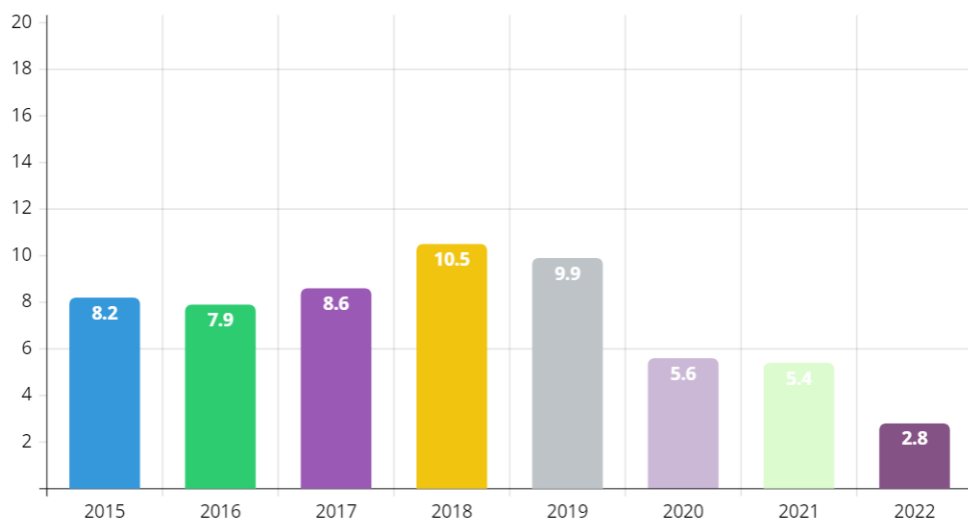


FIGURE 1.2 – Nombre annuel d’attaques de logiciels malveillants dans le monde de 2015 au premier semestre 2022 (en milliards)

**1.2.3.3 Famille de malware**

Type de malware	Définition
Les virus informatiques	sont des programmes ou des morceaux de code conçu pour endommager un ordinateur en corrompant ses fichiers système, en gaspillant ses ressources, en détruisant ses données ou en perturbant son fonctionnement. Lorsqu'un virus infecte un ordinateur, il se duplique et s'attache à d'autres fichiers ou documents.[16]
Les chevaux de Troie	sont des programmes malveillants qui se cache dans des programmes d'apparence inoffensive ou vous incite à les installer. On les appelle "chevaux de Troie" parce qu'ils procèdent de la même façon que le cheval de Troie classique pour infecter les ordinateurs.[14]
Les logiciels espions	sont des programmes informatiques qui sont conçus pour collecter des informations sur un ordinateur ou un réseau sans le consentement de l'utilisateur. Ils peuvent être utilisés pour voler des informations sensibles telles que des mots de passe, des numéros de carte de crédit et d'autres données personnelles. [9]
Les ransomwares	sont un type de logiciel malveillant qui verrouille les données ou l'appareil informatique d'une victime et menace de le garder verrouillé - ou pire - à moins que la victime ne paie une rançon.[26]
Les vers informatiques	un type de malware qui infecte un ordinateur, puis s'auto-réplique et se propage vers d'autres appareils tout en restant actif sur toutes les machines qu'il infecte.[15]
Les adwares	un type de logiciel malveillant qui affiche des publicités non désirées sur un ordinateur ou un appareil mobile. [21]
Les keyloggers	un type de malware qui enregistre toutes les frappes effectuées sur un clavier de pc.[24]

TABLE 1.1 – Famille de malware

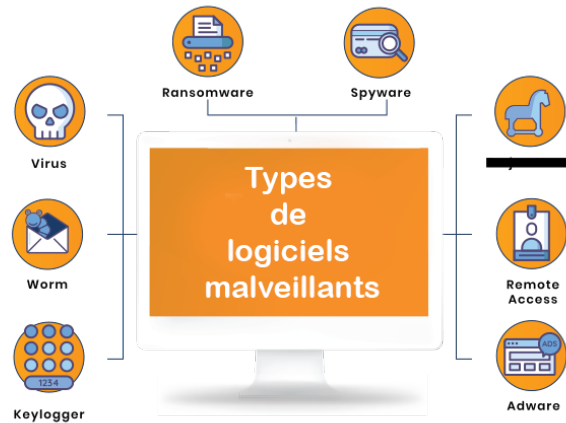


FIGURE 1.3 – Types des malwares

#### 1.2.3.4 Fonctionnement

dépend du type et de l'objectif du malware, mais les étapes typiques de ce fonctionnement est comme suit :

1. Infection : le malware doit pénétrer dans le système cible. Cela peut se faire par l'intermédiaire d'un e-mail de phishing, d'un téléchargement depuis un site Web malveillant, d'une clé USB infectée ou de toute autre méthode qui permet au malware de pénétrer dans le système.[6]
2. Installation : une fois que le malware a infecté le système, il s'installe. Il peut installer des fichiers supplémentaires sur le système, modifier les paramètres du système, s'ajouter aux processus en cours d'exécution ou effectuer d'autres actions pour s'assurer que le malware peut fonctionner en toute discrétion.[6]
3. Exécution : une fois que le malware est installé, il commence à exécuter son code malveillant. Cela peut inclure la collecte d'informations sur le système et l'utilisateur, l'envoi de données volées à un serveur distant, la modification de fichiers ou de paramètres, ou l'ouverture d'une porte dérobée pour permettre à un attaquant de prendre le contrôle de l'ordinateur à distance.[6]
4. Propagation : dans certains cas, le malware peut se propager à d'autres systèmes. Cela peut se faire en utilisant une fonctionnalité de réseau pour se propager automatiquement, ou en dupant l'utilisateur pour qu'il télécharge

et exécute le malware sur d'autres systèmes.

5. Dissimulation : le malware est souvent conçu pour se cacher sur le système cible, de sorte qu'il peut fonctionner en toute discrétion sans être détecté. Cela peut inclure des techniques telles que l'utilisation de noms de fichiers aléatoires, la modification des paramètres du système ou la suppression de fichiers de journalisation.[6]

#### **1.2.3.5 Les objectifs du malware**

L'objectif principal des logiciels malveillants est de gagner de l'argent. Pour faire du profit, les cybercriminels créent et distribuent des logiciels malveillants. Les logiciels malveillants sont capables de voler des identifiants bancaires, des numéros de carte de crédit et d'autres données financières sensibles. Les chevaux de Troie bancaires, par exemple, sont un type de malware qui cible les institutions financières et leurs clients. Ces chevaux de Troie volent les identifiants de connexion des victimes et d'autres données financières sensibles, qui sont ensuite utilisées pour commettre des fraudes ou vider des comptes bancaires. Le vol de données est un autre objectif des logiciels malveillants. Les logiciels malveillants sont capables de voler des informations sensibles telles que des informations personnelles, la propriété intellectuelle d'une entreprise et des secrets gouvernementaux. Le cyberespionnage est un type de vol de données dans lequel des informations sensibles sont volées à une entreprise ou à un gouvernement. Les attaquants peuvent ensuite revendre ou exploiter ces informations au plus offrant. Par exemple, les APT (Advanced Persistent Threats) sont un type de malware conçu pour rester non détecté pendant de longues périodes et voler des données sensibles.

### **1.2.4 Ransomware**

#### **1.2.4.1 Définition**

Consiste à relier le domaine d'informatique à des activités industrielles, de gestion ou de documentation. Le but est en effet d'organiser des informations, de les vérifier et de les collecter, de manière à être plus optimal tout en apportant un gain de temps.



#### 1.2.4.2 Fonctionnement

Le ransomware se propage via des e-mails de phishing, des téléchargements malveillants, des vulnérabilités logicielles ou des attaques par force brute. Une fois qu'il est installé sur un système, le ransomware se met à chiffrer les fichiers de l'utilisateur, généralement en utilisant un algorithme de chiffrement fort, afin qu'ils ne puissent plus être ouverts ou modifiés sans une clé de déchiffrement. Le ransomware affiche ensuite une notification à l'utilisateur, indiquant que les fichiers ont été chiffrés et qu'il doit payer une rançon pour récupérer l'accès à ses données. Les rançons sont généralement payées en bitcoins ou d'autres crypto-monnaies, ce qui rend la récupération des fonds difficile, voire impossible.

#### 1.2.4.3 Types

Type de ransomware	Définition
Ransomware de chiffrement	Ce type de ransomware utilise un algorithme de chiffrement pour chiffrer les fichiers de la victime. Les cybercriminels exigent ensuite une rançon pour fournir la clé de déchiffrement.
Ransomware de blocage	Ce type de ransomware bloque l'accès à l'ordinateur de la victime en affichant une fausse notification de la police ou d'un organisme gouvernemental. Les cybercriminels exigent ensuite une rançon pour débloquer l'ordinateur.
Ransomware de destruction	Ce type de ransomware détruit les fichiers de la victime sans possibilité de les récupérer. Les cybercriminels exigent ensuite une rançon pour empêcher la destruction d'autres fichiers.
Ransomware de fuite de données	Ce type de ransomware exfiltre les données de la victime et menace de les rendre publiques à moins que la rançon ne soit payée.
Le ransomware hybride	Ce type de ransomware combine plusieurs méthodes pour maximiser les profits des cybercriminels, par exemple en chiffrant les fichiers et en exfiltrant des données sensibles.
Ransomware en tant que service (RaaS)	Ce type de ransomware permet aux cybercriminels de louer ou d'acheter des kits de ransomware prêts à l'emploi pour attaquer des victimes. Les cybercriminels payent une commission aux développeurs du ransomware en fonction des rançons collectées.

TABLE 1.2 – Types des ransomwares

Il est important de noter que ces types de ransomware peuvent évoluer et

se combiner au fil du temps pour créer de nouvelles variantes et méthodes d'attaque.

### 1.2.5 Impact

Les ransomwares sont très dangereux car ils peuvent causer des pertes de données importantes et des coûts considérables pour les entreprises, les institutions et les particuliers. Voici quelques-unes des conséquences les plus courantes des ransomwares :

1. Perte de données : Si les fichiers sont chiffrés et que la victime refuse de payer la rançon, elle peut perdre définitivement ses données.[18]
2. Perturbation des activités : Les ransomwares peuvent causer des interruptions importantes des activités de l'organisation, car les utilisateurs ne peuvent plus accéder à leurs fichiers ou à leurs applications.[18]
3. Coût financier : Le coût de la rançon demandée peut être élevé, mais il y a également des coûts supplémentaires pour la récupération des données, la restauration des systèmes et la mise en place de mesures de sécurité supplémentaires pour éviter des attaques futures.[18]
4. Atteinte à la réputation : Les ransomwares peuvent causer une atteinte à la réputation de l'organisation, surtout si des données sensibles ont été divulguées ou si l'attaque est médiatisée.[18]
5. Risques de conformité : Les organisations peuvent être soumises à des obligations légales et réglementaires en matière de sécurité des données, et les ransomwares peuvent causer des risques de non-conformité.[18]

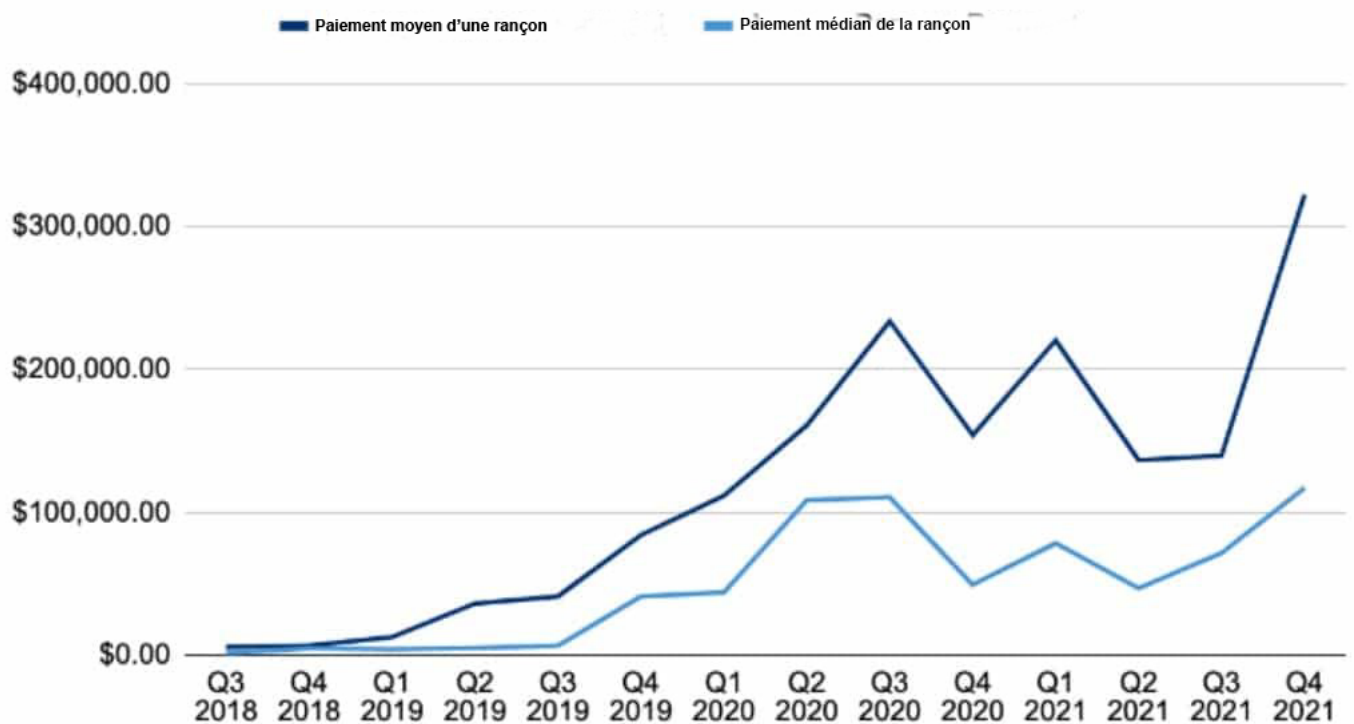


FIGURE 1.4 – Paiement de rançon par trimestre [1]

#### 1.2.5.1 Comment se protéger

Les ransomwares peuvent causer des dommages importants et perturber gravement les opérations d'une entreprise ou d'un utilisateur. Par conséquent, il est important de prendre des mesures de prévention et de protection pour réduire les risques d'attaque. Voici quelques-unes des mesures de prévention et de protection que vous pouvez prendre :

1. Effectuez régulièrement des sauvegardes de vos données importantes et stockez-les sur un support externe déconnecté du réseau.
2. Utilisez des outils de sécurité, tels que des programmes antivirus, des pare-feux, des logiciels anti-logiciels malveillants, et tenez-les à jour.
3. Éduquez les utilisateurs sur la sécurité informatique (attaque de l'ingénierie sociale), les risques des courriels non sollicités (phishing), les téléchargements douteux, et la navigation sur des sites web potentiellement dangereux.
4. Utilisez des outils de détection d'intrusion pour surveiller les activités ré-

seau, les tentatives d'attaques et les comportements malveillants.

5. Installez les dernières mises à jour de sécurité pour votre système d'exploitation, les applications, les navigateurs et les logiciels.
6. Utilisez des technologies de protection de la messagerie électronique pour filtrer les messages indésirables ou malveillants.
7. Configurez les autorisations d'accès aux fichiers et aux répertoires pour éviter que des utilisateurs non autorisés puissent accéder aux données.

### **1.3 conclusion**

Dans un premier temps, on a défini quelques notions qui représentent les mots clés de notre projet.

Suite à ça, on a abordé ....

Le chapitre prochain aura pour but la ...

# CHAPITRE 2

## ANALYSE DES MALWARES

## 2.1 Introduction

Dans le deuxième chapitre de ce mémoire consistera à fournir une définition de l'analyse de logiciels malveillants. Il tentera également d'établir un lien entre les objectifs de cette discipline et le contexte actuel de plus en plus menaçant, où la prolifération des logiciels malveillants est incommensurable.

Ensuite, ce même chapitre abordera les approches technique habituellement utilisées pour effectuer une analyse complète de logiciels malveillants, ainsi que les outils couramment utilisés pour chacune d'entre elles.

Enfin, ce chapitre présentera les techniques utilisées dans le cadre de cette pratique. [20]

## 2.2 Definition l'analyse de malware

Pour comprendre les actions et caractéristiques des programmes nuisibles, il est nécessaire de les analyser. L'analyse des logiciels malveillants est le processus de déterminer la fonctionnalité des logiciels malveillants et les réponses à questions suivantes[2], [20]. Comment fonctionnent les logiciels malveillants, qui machines et programmes sont affectés, quelles données sont endommagé et volé, etc. Il existe principalement deux techniques pour analyser les malwares : statiques et dynamiques [2]. Analyse statique examine le logiciel malveillant sans exécuter le code réel [7]. D'autre part, l'analyse dynamique examine les logiciels malveillants comportements lors de l'exécution de son code. L'analyse des logiciels malveillants commence avec analyse statique de base et finitions avec dynamique avancée analyse. Le logiciel malveillant est analysé à l'aide de l'ingénierie inverse [5] et d'autres outils d'analyse de logiciels malveillants pour représenter le malware dans un format différent. La Figure 2.1 illustre le processus de rétro-ingénierie.

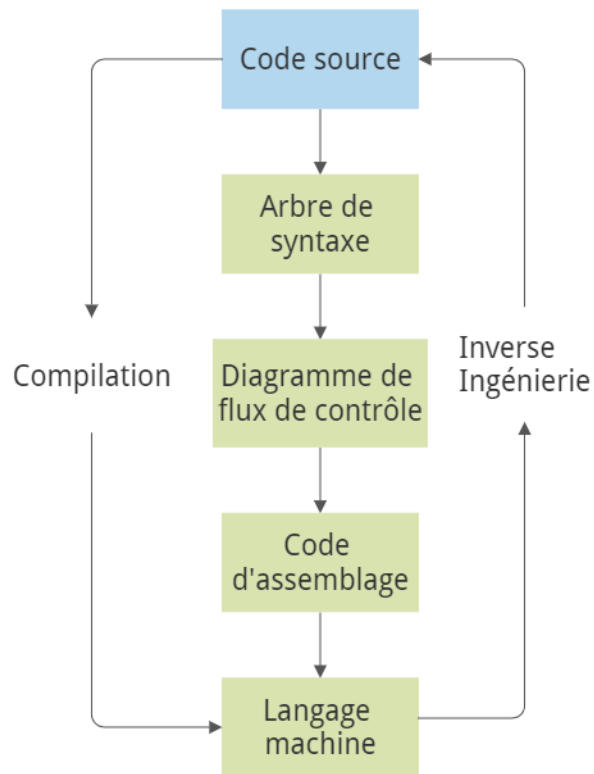


FIGURE 2.1 – Organigramme du processus de rétro-ingénierie

## 2.3 Objectifs de l'analyse de malware

La définition précédemment donnée souligne l'importance croissante des outils d'analyse de logiciels malveillants pour toute personne chargée de la sécurité des systèmes d'information et/ou de la gestion des incidents liés à la sécurité des données. Cela inclut les enquêteurs en informatique légale, les administrateurs système, les chercheurs en vulnérabilités, les testeurs d'intrusion, et d'autres encore. Ces outils sont devenus indispensables pour mener à bien ces tâches. [4]

La principale mission de cette discipline consiste à comprendre le fonctionnement des logiciels malveillants afin de les éliminer de manière optimale. Cependant, elle comporte également plusieurs objectifs secondaires, parmi lesquels les plus importants sont énumérés ci-dessous [25] :

1. La mission consiste à identifier le type d'infection causée par un logiciel malveillant générique ou une attaque ciblée contre une organisation donnée.
2. L'objectif est de stopper la propagation de l'infection le plus rapidement possible tout en cartographiant les secteurs touchés sur le réseau pour

déterminer son étendue.

3. Obtenir des indicateurs de compromission et créer des signatures d'attaques basées sur l'hôte et le réseau.
4. Automatiser la détection et l'élimination de l'infection au sein du réseau infecté en utilisant les indicateurs récupérés au préalable.
5. Identifier les familles spécifiques de ransomwares qui sont reconnues comme "les plus agressives".
6. Repérer et résoudre les vulnérabilités qui sont exploitées par une infection.
7. Le processus consiste à détecter les logiciels malveillants de type ransomware en utilisant des signatures basées sur le comportement qui sont préalablement échantillonnées manuellement.

## 2.4 Exigences de l'analyse de malware

Pour avoir une bonne connaissance de l'analyse de malwares, il est nécessaire d'avoir une compréhension avancée dans plusieurs domaines de l'informatique. Pour donner un exemple, voici quelques-uns des plus essentiels [12] :

- Le réseau et le protocole TCP/IP,
- Les composants internes des systèmes d'exploitation (Windows et Unix),
- La sécurité informatique,
- L'enquête médico-légale et la réponse aux incidents,
- La programmation (notamment en langages tels que C, C++, Python et Perl),
- Le rétro-ingénierie,
- La recherche de vulnérabilités,
- Les principes fondamentaux des logiciels malveillants.



## 2.5 Types et Techniques d'analyses de malwares

Il existe plusieurs types d'analyses de malwares qui peuvent être effectuées pour étudier le comportement d'un programme malveillant. Voici quelques exemples[25] :

### 2.5.1 Analyse Statique

L'analyse statique de malwares consiste à inspecter les fichiers potentiellement dangereux pour votre système, sans les exécuter activement. Cette méthode est considérée comme sûre car elle permet d'exposer les bibliothèques ou les fichiers malveillants empaquetés. Elle peut fournir des informations utiles sur la nature du malware, telles que les noms de fichiers, les hachages, les adresses IP, les domaines et les données d'en-tête de fichier. Pour observer le malware, divers outils tels que des analyseurs de réseau peuvent être utilisés.

#### 2.5.1.1 Scan base sur signature Yara

YARA est un outil open source utilisé pour la recherche et la détection de logiciels malveillants. Il utilise une approche basée sur des règles pour détecter les logiciels malveillants en fonction de modèles. Les règles sont créées de manière à détecter un logiciel malveillant avec un modèle et des indicateurs spécifiques. Une fois qu'une règle est créée, elle peut être analysée par rapport à différents fichiers pour identifier les activités malveillantes. De plus, les règles YARA sont incorporées dans Incident Response and Forensics pour rechercher des artefacts basés sur un modèle. [10] Pour comprendre les règles YARA et comment elles sont créées, nous devons d'abord comprendre la structure de fichier typique. En général chaque fichier comporte deux parties : [10]

- En-tête : qui identifie le type de fichier
- Corps : qui contient les données ou les chaînes réelles

Pour identifier un fichier Macro Enabled, nous utiliserons une simple règle YARA. Cette règle détectera tout document Word sur lequel les macros sont activées. Chaque règle YARA comprend le composant suivant : [10]

Rule <name> : le nom de la règle.

Meta : description de la règle telle que la date de création, l'auteur, etc.

String : La valeur réelle/les chaînes que nous voulons rechercher. Cela pourrait être Hex, String ou Regex.

Condition : Toute la logique de la règle.

Voici un exemple de l'utilisation de Figure 2.6 dans notre projet.



```
rule Cryptoshield
{
  meta:
    author = "kevoreilly"
    description = "Cryptoshield Payload"
    cape_type = "Cryptoshield Payload"
  strings:
    $a1 = "CRYPTOSHIELD." wide
    $a2 = "Click on Yes in the next window for restore work explorer" wide
    $a3 = "r_sp@india.com - SUPPORT"
  condition:
    uint16(0) == 0x5A4D and (all of ($a*))
}
```

FIGURE 2.2 – La règle YARA a l'extension .yara

#### 2.5.1.2 Scan base sur signature dans un fichier

L'utilisation de la détection basée sur les signatures dans l'analyse des logiciels malveillants offre des avantages significatifs par rapport à la simple correspondance de hachage de fichiers. En tirant parti des signatures qui identifient les points communs entre les échantillons de logiciels malveillants, les analystes peuvent cibler des familles entières de logiciels malveillants, plutôt que des instances individuelles. Cette approche offre une compréhension plus large et plus complète du paysage des menaces.

Les signatures sont hautement adaptables et peuvent être utilisées pour détecter divers types de logiciels malveillants basés sur des fichiers. Ils peuvent être personnalisés pour inclure ou exclure des formats de fichiers spécifiques, per-

mettant des capacités de détection polyvalentes sur différentes plates-formes et types de fichiers. Cette flexibilité garantit que la détection basée sur les signatures reste efficace dans divers environnements.[22]

### 2.5.1.3 Scan avec le machine learning

L'apprentissage automatique (ML) est un ensemble d'algorithmes qui estime les résultats des candidatures sans être explicitement programmé. Le but du ML est de convertir les données d'entrée dans des intervalles de valeurs acceptables à l'aide d'une analyse statistique. En utilisant ML, de nombreuses opérations peuvent être effectuées sur des données connexes telles que la classification, la régression et le regroupement. Les algorithmes ML ont été utilisés dans la détection de logiciels malveillants pour plusieurs années. Les algorithmes ML bien connus sont bayésiens réseau (BN), Bayes naïf (NB), variante d'arbre de décision C4.5 (J48), arbres modèles logistiques (LMT), arbre forestier aléatoire (RF), k-plus proche voisin (KNN), perceptron multicouche (MLP), régression logistique simple (SLR), machine à vecteurs de support (SVM) et l'optimisation minimale séquentielle (SMO). Ces les algorithmes sont utilisés en particulier dans la détection basée sur le comportement et certaines autres approches de détection. Bien que chaque algorithme ait ses propres avantages et inconvénients, il ne peut pas être conclu qu'un algorithme est plus efficace qu'un autre. Cependant, un algorithme peut être plus performant que d'autres algorithmes en termes de distribution des données, de nombre de fonctionnalités et de dépendances entre les propriétés. [19]

Dans cette étape, la classification du ransomware qui classe les données en ransomware, bénin et malveillant. Il contient 35 367 échantillons de ransomware et 27 117 échantillons de fichiers bénins. Il peut être classé comme rançongiciel et bénin en utilisant un algorithme d'apprentissage automatique, à savoir une forêt aléatoire, un algorithme de renforcement d'arbre à gradient et un algorithme de vecteur de support. Tableau 2.1 montre que la précision de l'algorithme. Il compare le résultat en utilisant la régression linéaire, Marines Bayes, l'algorithme Adaboost. En combinaison de l'algorithme combiné une meilleure précision. Il mesure un vrai taux positif (TPR), taux vrai négatif (TNR), taux faux positif (FPR), taux faux négatif (FNR). D'après les résultats précédents, dans le cadre

Algorithm	True Positive (TP) rate	False Positive (FP) rate	%
RF, GBTA	0.922	0.077	92
DT, LR	0.567	0.03	58.43

TABLE 2.1 – Précisions des algorithmes

de notre projet, nous avons utilisé l'algorithme de l'Arbre Forestier Aléatoire (Random Forest).

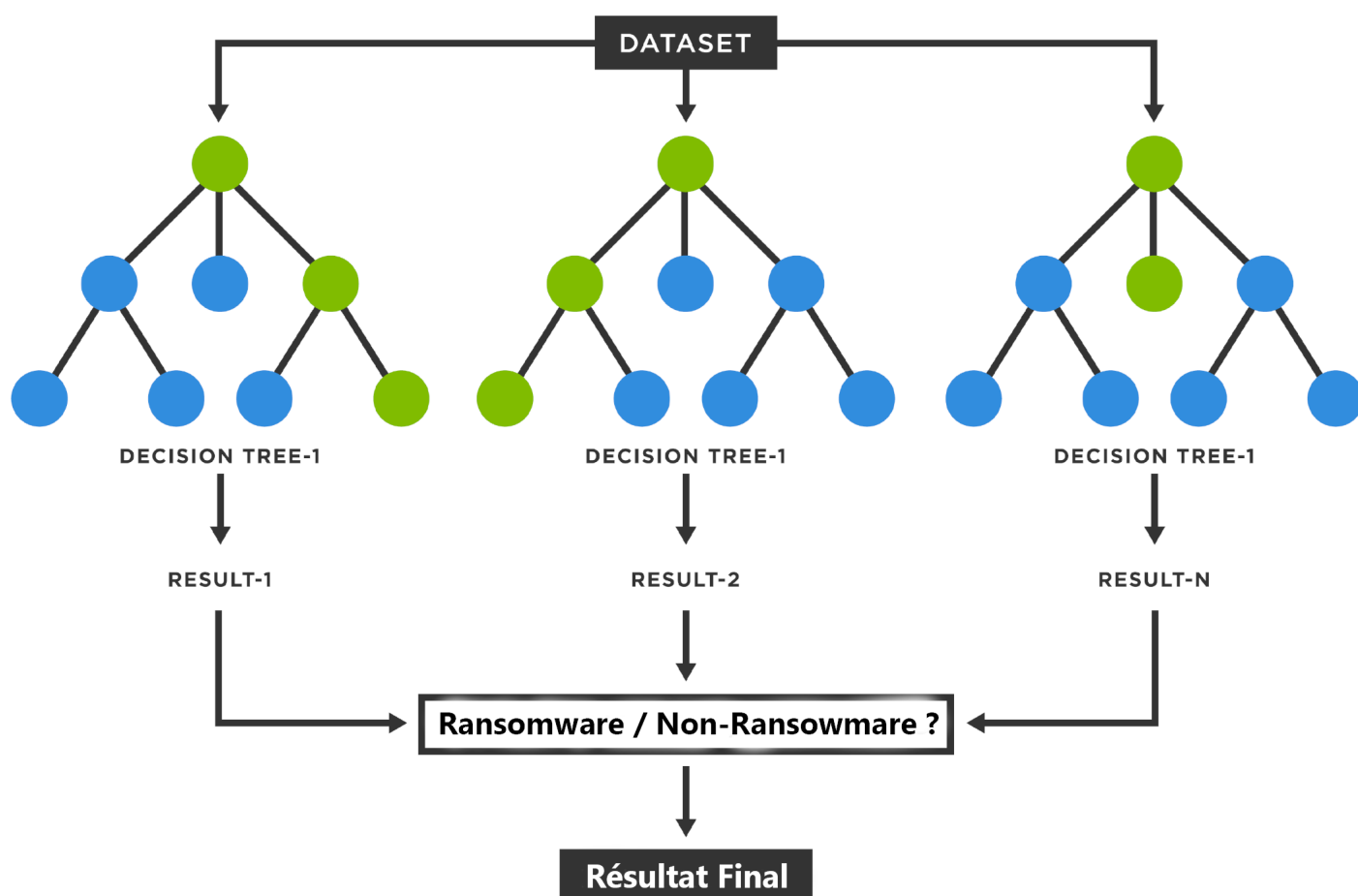


FIGURE 2.3 – Le classificateur de forêt aléatoire pour l'analyse statique.

Il sera basée sur l'analyse du format "Portable Executable", d'où le format Portable Executable est le format de fichier standard pour les exécutables, le code objet et les bibliothèques de liens dynamiques (DLL) utilisés dans les versions 32 et 64 bits des systèmes d'exploitation Windows. Les infecteurs de fichiers qui infectent ces exécutables sont détectés par Trend Micro en tant que PE\_malwarename. [13]

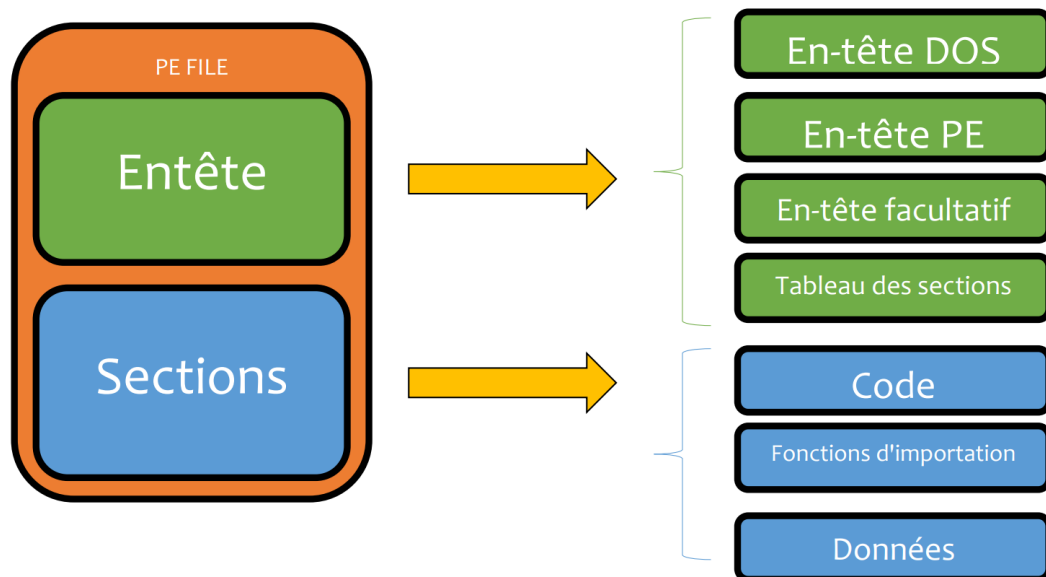


FIGURE 2.4 – Représentation simplifiée de la structure du format PE (Portable Executable).

#### 2.5.1.4 Identification par l'entropie

L'entropie est une mesure du degré de chaos ou de désordre dans un ensemble de données. Voici quelques exemples pour illustrer cela :

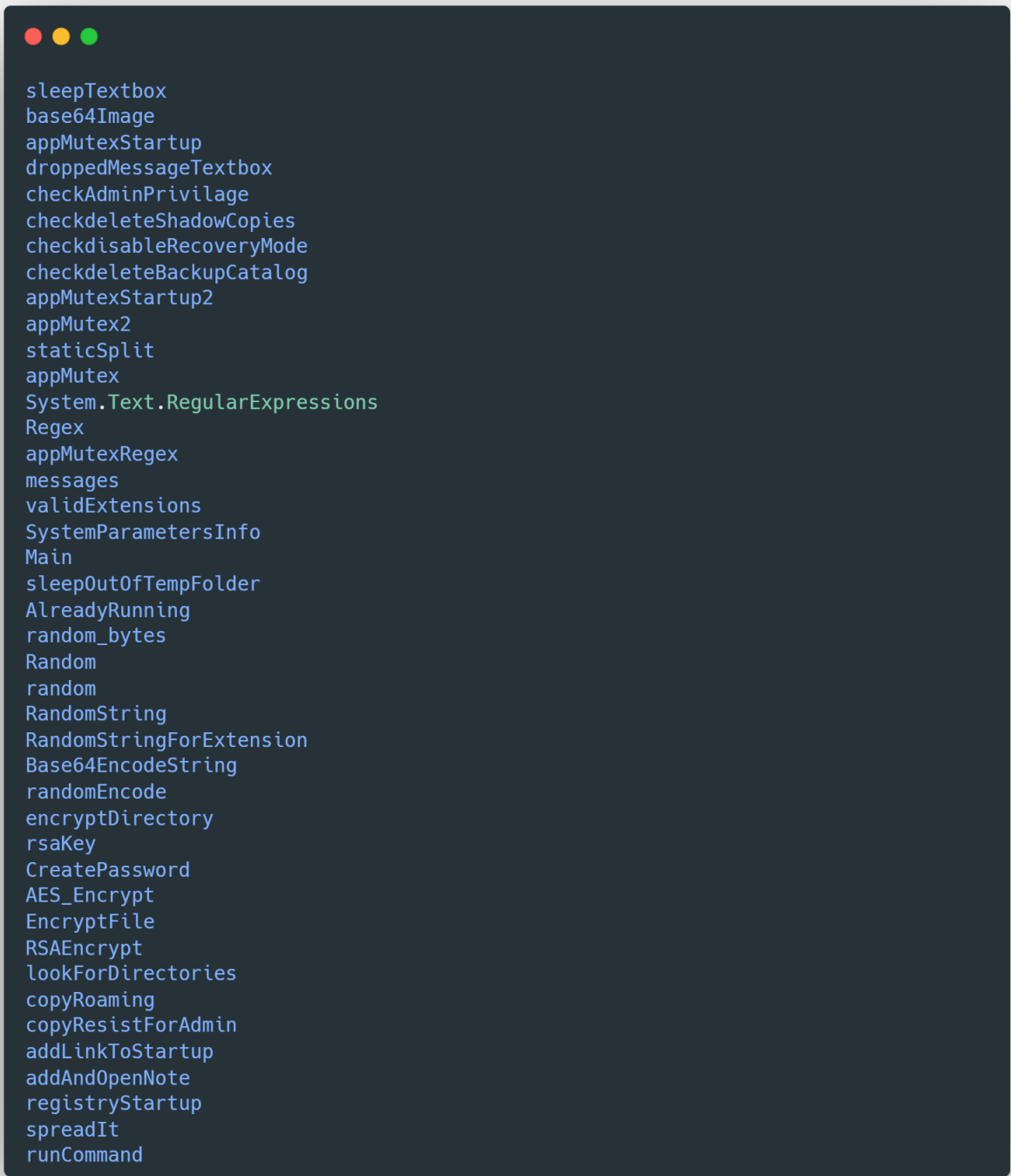
La séquence de caractères "01 01 01 03 03 01 01 05 06 06 01" présente une entropie faible, car elle suit une suite logique et semble ordonnée, laissant supposer une certaine signification.

En revanche, la séquence de caractères "99 15 03 78 54 36 70 08 42 46 87" présente une entropie élevée, car les chiffres semblent être disposés de manière aléatoire ou du moins désordonnée, sans logique apparente. [8]

Regrettamment, dans la pratique, l'analyse d'entropie a généré certains faux positifs difficiles à détecter et à corriger. De plus, elle ne peut pas être appliquée dans tous les cas. Par exemple, elle fonctionne assez bien pour les fichiers .exe et les fichiers texte, mais très mal pour les fichiers Java compilés.

#### 2.5.1.5 Identification les algorithmes de cryptage et de chiffrement

Lors de cette étape, le but est d'extraire les chaînes de caractères présentes dans les fichiers analysés. Cela se fait généralement à l'aide d'outils spécialisés conçus à cet effet, tels que l'utilitaire "Strings". [3]



```
sleepTextbox
base64Image
appMutexStartup
droppedMessageTextbox
checkAdminPrivilage
checkdeleteShadowCopies
checkdisableRecoveryMode
checkdeleteBackupCatalog
appMutexStartup2
appMutex2
staticSplit
appMutex
System.Text.RegularExpressions
Regex
appMutexRegex
messages
validExtensions
SystemParametersInfo
Main
sleepOutOfTempFolder
AlreadyRunning
random_bytes
Random
random
RandomString
RandomStringForExtension
Base64EncodeString
randomEncode
encryptDirectory
rsaKey
CreatePassword
AES_Encrypt
EncryptFile
RSAEncrypt
lookForDirectories
copyRoaming
copyResistForAdmin
addLinkToStartup
addAndOpenNote
registryStartup
spreadIt
runCommand
```

FIGURE 2.5 – Une partie des chaînes de caractères extraites d’un fichier suspect.

Une recherche rapide sur Internet concernant les chaînes de caractères découvertes révèle clairement la nature malveillante des échantillons (comme illustré dans la figure 2.5 où la présence des fonctions de chiffrement Windows AES, RSA, SHA1 laisse fortement penser à un ransomware, plus de détails seront ajoutés dans le prochain chapitre). En effet, certaines instructions, routines,

appels système ou messages d'erreur fictifs utilisés sont caractéristiques de certaines catégories de malwares.

#### **2.5.1.6 Identification les machines virtuels**

Les chercheurs en sécurité utilisent fréquemment des machines virtuelles pour exécuter et analyser des logiciels malveillants en raison de leur environnement isolé et contrôlé. Toutefois, les auteurs de logiciels malveillants cherchent à détecter si leur code est exécuté dans une machine virtuelle. Afin d'identifier les machines virtuelles lors de l'analyse de logiciels malveillants, différentes techniques sont employées. Celles-ci peuvent impliquer la recherche de signes spécifiques tels que des pilotes ou des services virtuels, la détection de composants d'hyperviseur ou l'observation de comportements caractéristiques des machines virtuelles. D'autres approches consistent à analyser les éléments laissés par l'environnement virtuel lui-même, tels que les registres ou les fichiers système. Ces techniques permettent aux chercheurs en sécurité de rester en avance sur les méthodes de détection utilisées par les auteurs de logiciels malveillants. Dans notre projet, nous nous appuyons également sur la bibliothèque `pefile`. En explorant la section `DIRECTORY_ENTRY_IMPORT` de fichier exécutable, nous sommes en mesure de détecter la présence d'une machine virtuelle sur le système.

#### **2.5.1.7 Identification les Anti debugging**

Lorsque les développeurs travaillent sur leur code, ils adoptent des bonnes pratiques pour assurer la protection de leur code et, en fin de compte, de l'application pour laquelle ils le développent. Les débogueurs leur permettent de tester leur code dans des environnements contrôlés, en l'exposant à des attaques connues, en modifiant certaines variables, en mettant à jour les configurations, etc. Cela leur permet de détecter et de corriger les bugs, les erreurs et les vulnérabilités de sécurité, garantissant ainsi la protection des données. Cependant, bien que ces débogueurs soient utiles aux développeurs, ils peuvent également être exploités par des attaquants pour observer l'application en cours de test dans des conditions spécifiques, ce qui leur permet d'améliorer leurs techniques d'attaque. Les techniques d'anti-debugging sont utilisées pour modifier le comportement des applications afin de se protéger et, dans la plupart des cas,

ralentir le processus de rétro-ingénierie. Différentes méthodes sont couramment utilisées dans ces techniques d'anti-debugging :

- L'analyse des données échangées entre les applications à l'aide d'un analyseur de paquets.
- La désassemblage du code binaire du logiciel pour le transformer en langage d'assemblage.
- La reconstitution du code source en décompilant le binaire ou le bytecode.

Dans notre projet, nous nous appuyons également sur la bibliothèque `pefile`. En explorant la section `DIRECTORY_ENTRY_IMPORT` de fichier exécutable, nous pouvons détecter la présence de fonctions potentiellement malveillantes.

#### **2.5.1.8 Conclusion**

En plus des connaissances techniques approfondies requises en programmation et en fonctionnement interne des systèmes d'exploitation, l'analyse de logiciels malveillants peut être laborieuse, en particulier lorsqu'il s'agit de programmes de grande taille, même avec l'aide d'outils automatisés.

De plus, ces techniques révèlent rapidement leurs limites qui sont les suivants :

1. La détection des techniques d'obfuscation : Les malwares ont souvent recours à des techniques d'obfuscation pour dissimuler leur code et rendre l'analyse statique plus complexe. Ces techniques peuvent comprendre le chiffrement, la compression et la fragmentation du code, ce qui complique l'identification des fonctionnalités malveillantes.
2. Polymorphisme et métamorphisme : Certains malwares utilisent des techniques de polymorphisme et de métamorphisme pour modifier leur code à chaque exécution ou lors de la propagation. Cela rend l'analyse statique inefficace, car les signatures et les modèles de comportement peuvent changer continuellement.
3. Dépendance aux données d'entrée : L'analyse statique ne prend pas en compte les données d'entrée dynamiques. Les logiciels malveillants peuvent se comporter différemment en fonction des entrées utilisateur ou de l'état



du système, ce qui rend difficile la détection de comportements malveillants uniquement à partir de l'analyse statique du code.

4. Analyse incomplète des interactions système : L'analyse statique se concentre principalement sur le code lui-même, mais ne prend pas en compte les interactions avec d'autres composants du système, tels que les appels système, les fichiers système, les registres, etc. Cela limite la capacité de détecter certains comportements malveillants qui se produisent uniquement lors de l'exécution réelle du programme.
5. Nouvelles variantes de malwares : Les auteurs de logiciels malveillants développent constamment de nouvelles variantes pour éviter la détection. L'analyse statique peut être inefficace pour détecter les nouvelles variantes, car elle repose souvent sur des signatures ou des modèles préexistants.

Ainsi, il peut s'avérer ardu de détecter de manière précise le comportement malveillant spécifique d'un malware en se basant uniquement sur une analyse statique.

### **2.5.2 Analyse Dynamique**

L'analyse dynamique de malwares se fait à l'aide d'un sandbox, qui est un environnement virtuel sécurisé et isolé permettant d'exécuter du code potentiellement dangereux. Les spécialistes de la sécurité peuvent ainsi surveiller de près les malwares dans cet environnement sans risque d'infecter le reste du système ou du réseau, ce qui leur permet de recueillir davantage d'informations sur les malwares.

#### **2.5.2.1 Usage de sandbox**

L'utilisation d'une sandbox pour l'analyse de malwares sur notre site présente de nombreux avantages en termes de sécurité. Une sandbox est un environnement isolé dans lequel les fichiers suspects peuvent être exécutés et analysés sans risque pour le système hôte.

En utilisant une sandbox, nous pouvons exécuter les fichiers malveillants dans un environnement contrôlé, ce qui permet de limiter les risques d'infection ou de propagation de ces malwares. La sandbox crée une barrière de protec-

tion entre les fichiers suspects et notre système, empêchant ainsi les éventuelles conséquences néfastes.

De plus, la sandbox offre la possibilité de surveiller et d'analyser le comportement des malwares en temps réel. Cela nous permet de détecter les actions malveillantes, telles que l'accès non autorisé aux fichiers, la modification du registre système ou la communication avec des serveurs de commande et de contrôle. En observant ces comportements, nous pouvons mieux comprendre le fonctionnement des malwares et prendre les mesures appropriées pour les contrer.

#### **2.5.2.2 La detection baser sur le machine learning**

L'analyse dynamique des fichiers de ransomware à l'aide de l'apprentissage automatique est une approche qui peut être utilisée pour déterminer et analyser le comportement des échantillons de ransomware dans un environnement contrôlé. En utilisant les techniques d'apprentissage automatique, il devient possible d'automatiser la détection et la classification des ransomware en fonction de leurs caractéristiques dynamiques. L'analyse se base sur le rapport generer dans la partie de sandboxing, d'où nous allons extraire les informations qui sont reliaer a notre dataset, et a la fin nous allons predire si le fichier analyser est un ransomware ou goodware. Dans notre cas d'etude, nous avons choisit le Ransomware Dataset for arXiv :1609.03020 est une dataset qui est telechargeable sur le github. Elle contient de 584 échantillons de ransomware et 942 échantillons de fichiers bénins et de 30970 colonne qui sera evaluer. Dans l'etape de classification, il peut être classé comme rançongiciel et bénin en utilisant un algorithme d'apprentissage automatique, à savoir une forêt aléatoire, un algorithme de renforcement d'arbre à gradient et un algorithme de vecteur de support. Dans le cadre de notre projet nous avons utiliser l'agorithme de l'Arbre Forestier Aleatoire (Random Forest), d'où les caractéristiques seront basee sur 30970 informations pour qu'il sera predire, parmi d'elle les appels système API, la suppression d'une certains extensions, clé de registre qui soit supprimer ou modifier, ou bien ouverte ou bien lire. La gestion des fichier et d'autre informations importante.

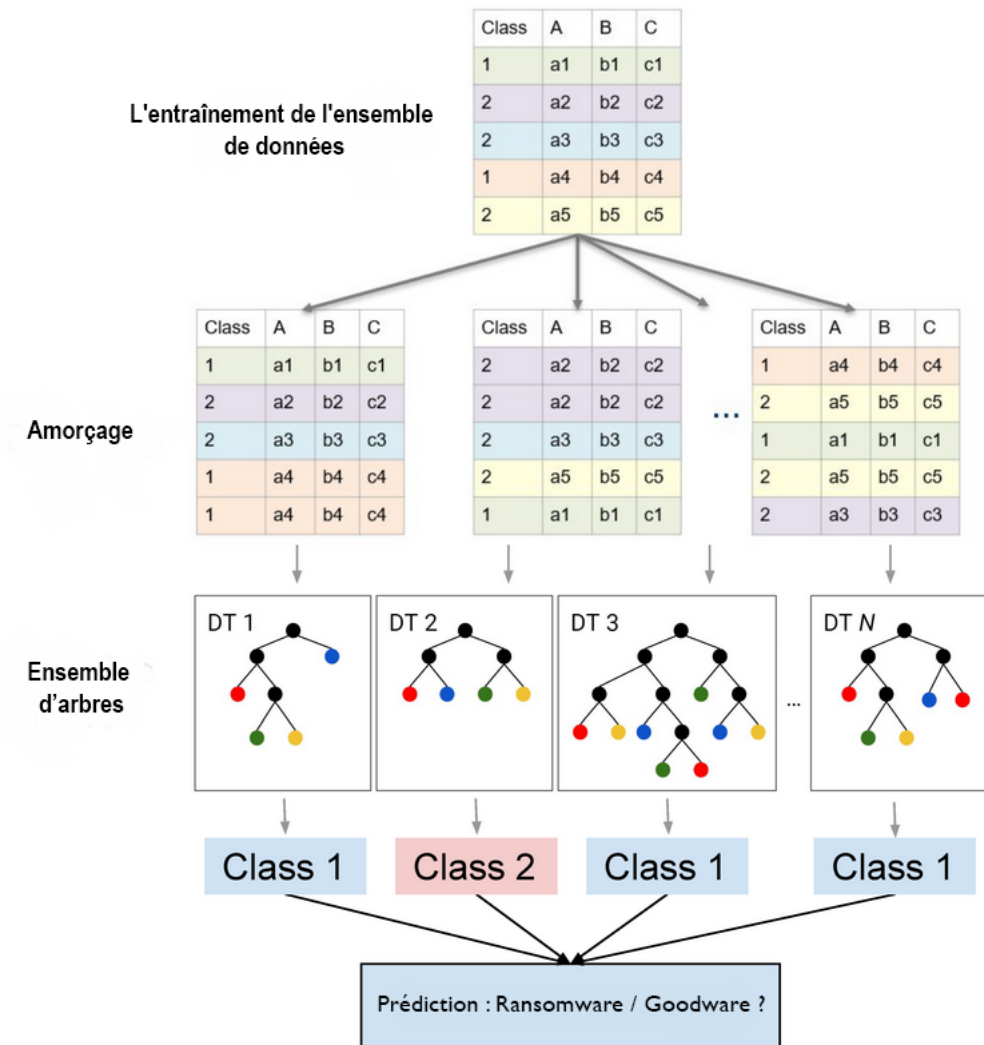


FIGURE 2.6 – Le classificateur de forêt aléatoire pour l'analyse dynamique.

### 2.5.2.3 Autres fournisseurs utilisés

Lorsqu'il s'agit d'effectuer des analyses de ransomwares à l'aide d'API, plusieurs fournisseurs peuvent être utilisés pour obtenir des informations et des services supplémentaires. Voici quelques-uns des fournisseurs couramment utilisés dans le cadre de l'analyse de ransomwares API :

- **VirusTotal** : un site Web qui vous permet d'analyser les fichiers suspects, domaines, IP et URL pour détecter les logiciels malveillants et autres violations. Vous pouvez l'utiliser pour analyser des fichiers de votre ordinateur ou de sources en ligne avec plus de 70 scanners antivirus et autres outils. [28]



FIGURE 2.7 – Logo de virustotal.

- **Sacanii End-point** : est un service d'identification de contenu qui identifie les logiciels malveillants, les images inappropriées et le langage. Il n'est pas directement lié à VirusTotal. Cependant, vous pouvez utiliser VirusTotal pour analyser des fichiers depuis votre ordinateur ou des sources en ligne avec plus de 70 scanners antivirus et autres outils. [27]



FIGURE 2.8 – Logo de Scanii.

- **Intezer** : est une société autonome d'opérations de sécurité qui fournit des solutions technologiques pour le triage des alertes, la réponse aux incidents et la chasse aux menaces. Il n'est pas directement lié à VirusTotal. Cependant, vous pouvez utiliser Intezer pour analyser les fichiers par SHA256, MD5 ou SHA1. Si l'échantillon n'existe pas déjà dans la base de données d'Intezer, le fichier peut être téléchargé depuis VirusTotal. [23]



FIGURE 2.9 – Logo d'Intezer.

### **2.5.3 Analyse Hybride**

L'analyse dynamique de malwares se fait à l'aide d'un sandbox, qui est un environnement virtuel sécurisé et isolé permettant d'exécuter du code potentiellement dangereux. Les spécialistes de la sécurité peuvent ainsi surveiller de près les malwares dans cet environnement sans risque d'infecter le reste du système ou du réseau, ce qui leur permet de recueillir davantage d'informations sur les malwares.

## **2.6 Conclusion**

## BIBLIOGRAPHIE

- [1] *70 MILLION Dollars RANSOMWARE DEMAND SHOCKS THE WORLD*. URL : <https://banyanhill.com/70-million-ransomware-demand/>.
- [2] Y. ALOSEFER. « Analysing Web-based malware behaviour through client honeypots ». In : (2012).
- [3] Michael Sikorski et ANDREW HONIG. « PRACTICAL MALWARE ANALYSIS ». In : (2012).
- [4] Dennis DISTLER. « Global Information Assurance Certification Paper ». In : (2007).
- [5] E. EILAM. « Reversing : Secrets of Reverse Engineering. Hoboken ». In : (2011).
- [6] *How Malware Works : Anatomy of a Malware Attack*. URL : <https://www.varonis.com/blog/how-malware-works/>.
- [7] N. IDIKA et P. MATHUR. « A survey of malware detection techniques ». In : (2007).
- [8] *Les différentes techniques de détection des virus et malwares*. URL : <https://www.securiteinfo.com/attaques/malwares-virus-spam-logiciels-indesirables/techniques-detection-malware.shtml>.
- [9] *Logiciel pour espionner*. URL : <https://espion-logiciel.com/>.
- [10] *Malware Analysis : Introduction to YARA*. URL : <https://medium.com/@ammadb/malware-analysis-introduction-to-yara-e11b89e02ba6>.
- [11] *Malwares*. URL : <https://fr.malwarebytes.com/malware/>.
- [12] Blake Hartstein MICHAEL LIGH Steven Adair et Matthew RICHARD. « Malware Analyst's Cookbook and DVD : Tools and Techniques for Fighting Malicious Code ». In : (2010).
- [13] *Portable executable (PE)*. URL : <https://www.trendmicro.com/vinfo/in/security/definition/portable-executable-pe>.
- [14] *Qu'est-ce qu'un cheval de Troie ? Est-ce un malware ou un virus ?* URL : <https://www.avg.com/fr/signal/what-is-a-trojan>.
- [15] *Qu'est-ce qu'un malware et comment s'en protéger ?* URL : <https://www.avast.com/fr-fr/c-malware>.
- [16] *Qu'est-ce qu'un virus informatique et comment ça fonctionne ?* URL : <https://www.avast.com/fr-fr/c-computer-virus>.
- [17] *Qu'est-ce que la cybersécurité ?* URL : <https://www.kaspersky.fr/resource-center/definitions/what-is-cyber-security>.
- [18] *Ransomware and Recent Variants*. URL : <https://www.cisa.gov/news-events/alerts/2016/03/31/ransomware-and-recent-variants>.

- [19] REFIK SAMET. « A Comprehensive Review on Malware Detection Approaches ». In : (2020).
- [20] M. SIKORSKI et A. HONIG. « Practical Malware Analysis : The Hands-On Guide to Dissecting Malicious Software. » In : (2012).
- [21] *Tout savoir sur l'adware*. URL : <https://www.kaspersky.fr/resource-center/threats/adware>.
- [22] *What Is A Malware File Signature (And How Does It Work) ?* URL : <https://www.sentinelone.com/blog/what-is-a-malware-file-signature-and-how-does-it-work/>.
- [23] *What is Intezer ?* URL : <https://support.intezer.com/hc/en-us/articles/360021345380-Analyzing-Files-or-Hashes>.
- [24] *What is Keylogger ?* URL : <https://www.techopedia.com/definition/1802/keylogger>.
- [25] *What is Malware Analysis ?* URL : <https://www.fortinet.com/resources/cyberglossary/malware-analysis>.
- [26] *What is ransomware ?* URL : <https://www.ibm.com/topics/ransomware>.
- [27] *What is Scanii ?* URL : <https://docs.scanii.com/article/99-v21>.
- [28] *What is VirusTotal ?* URL : <https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works>.