REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

UNIVERSITE SAAD DAHLEB DE BLIDA

FACULTE DES SCIENCES

DEPARTEMENT D'INFORMATIQUE

Mémoire de fin d'étude pour l'obtention

Du diplôme de Master

Spécialité : Sécurité des Systèmes D'informations

Thème

ANALYSE DYNAMIQUE AUTOMATISÉE DES RANSOMWARES : AVANTAGES, LIMITES ET UTILISATION POUR LA DÉTECTION

Encadreur :

PhD Mme BOUAISSA Djamila

Réalisé par :

SYLLA DJENEBA

SANGARE MOHAMED

Les membres du jury :

Mr Kamesh, président du jury

Mme Ferdi, examinatrice

Année universitaire 2020-2021

Remerciements

La réalisation de ce mémoire a été possible grâce au concours de plusieurs personnes à qui nous voudrions témoigner toute notre gratitude.

Nous voudrions tout d'abord adresser toute notre reconnaissance à notre encadreur, ***Madame BOUAISSA Djamila*** *pour sa patience, sa disponibilité et surtout ses judicieux conseils, qui ont contribué à alimenter notre réflexion.*

Nous désirons aussi remercier ***les professeurs de l'université Saad Dahleb de Blida****, qui nous ont fourni les outils nécessaires à la réussite de nos études universitaires.*

Nous tenons aussi à remercier spécialement ***Amadou DIARRA****, qui nous a été d'une grande aide en nous fournissant la documentation nécessaire pour avancer dans ce travail.*

Nous voudrions exprimer notre reconnaissance envers ***les amis et proches*** *qui nous ont apporté leur soutien matériel, moral et intellectuel tout au long de notre démarche.*

Que tous trouvent ici l'expression de notre franche et profonde reconnaissance.

Dédicaces

Je ne saurais exprimer toute ma gratitude envers ma famille qui m'a soutenu pendant toute cette aventure à travers leur confiance, affection, aide et conseil.
Je suis qui je suis grâce à vous.
Ce travail est une des preuves de l'effort consenti.
A toi mon père que je n'arrêterais jamais de regretter l'absence, j'aurais souhaité que tu me vois franchir ces étapes mais telle est la vie.
A vous mes mères dont je n'ai jamais su faire la différence, vous êtes la lumière qui guide mes pas partout où je me trouve.
A vous mes sœurs et frères qui me montrent chaque jour que la famille est ce qu'il y a de meilleur dans cette vie.
A mes amis qui de près ou de loin m'ont aidé et soutenu tout au long de ce mémoire.
Ce travail, je vous le dédie.

SANGARÉ Mohamed

À mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études,
A mes chères sœurs pour leurs encouragements permanents, et leur soutien moral,
A ma grand-mère, pour son infaillible présence,
A toute ma famille pour leur soutien tout au long de mon parcours universitaire,
Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fruit de votre soutien inébranlable,
Merci d'être toujours là pour moi.

SYLLA Djeneba

Table des matières

LISTE DES FIGURES

LISTES DES ABREVIATIONS

- **AES:** Advanced Encryption Standard
- **AIDS:** Anomaly Intrusion Detection System
- **API :** Application Programming Interface
- **C&C :** Command and Control
- **DDoS:** Distributed Denial of Service
- **DES :** Data Encryption Standard
- **DIDS:** Distributed Intrusion Detection System
- **DNS :** Domain Name service
- **GNU :** General Public License
- **HIDS :** Host Intrusion Detection System
- **HTTP :** HyperText Transfert Protocol
- **IDS :** Intrusion Detection System
- **IPS :** Intrusion Prevention System
- **MCFP:** Maya Fluid Cache Playback Format
- **NBNS :** NetBIOS Name Server
- **NIDS :** Network Intrusion Detection System
- **OSSEC:** Open Source HIDS SECurity
- **PCAP :** Packet Capture
- **RDP :** Remote Desktop Protocol
- **RSA :** Rivest, Shamir et Adleman
- **SIDS:** Signature Intrusion Detection System
- **TCP :** Transfert Control Protocol
- **VPN :** Virtual Private Network

RÉSUMÉ

Nous vivons à une époque où l'internet et les nouvelles technologies sont en constante évolution. Face à des hackers de plus en plus performants, nous devons impérativement assurer la sécurité des systèmes d'information tant au niveau physique que logique.
Les ransomwares, des logiciels malveillants utilisés par les cybercriminels pour crypter les données d'un ordinateur ou en bloquer l'accès connaissent eux aussi un essor croissant. Ils deviennent au fil du temps la plus grande menace des structures informatisées.
Face à ce danger croissant d'intrusion malveillante, l'utilisation d'outils de sécurité tel que les systèmes de détection d'intrusion s'imposent. Snort, logiciel libre, gratuit et l'un des logiciels les plus sollicités pour la détection est l'outil utilisé dans ce travail pour détecter la présence de ransomware sur un ordinateur.
A travers ce projet, nous avons pris en main l'outil Snort ainsi que sa configuration dans le but de détecter la présence d'exploits ou d'échantillons de ransomwares.

ABSTRACT

We live in an era where the Internet and new technologies are constantly evolving. Faced with increasingly powerful hackers, it is imperative that we ensure the security of information systems both physically and logically.
Ransomware, malicious software used by cybercriminals to encrypt computer data or block access to it, is also growing. Over time, they are becoming the greatest threat to computerized structures.
Faced with this growing danger of malicious intrusion, the use of security tools such as intrusion detection systems is essential. Snort, free software and one of the most requested software for detection is the tool used in this work to detect the presence of ransomware on a computer.
Through this project, we have taken in hand the Snort tool and its configuration in order to detect the presence of exploits or samples of ransomware.

Introduction générale

La sécurité des systèmes d'information qui n'a pas toujours été prisée dans le temps est de nos jours plus importante que jamais. C'est l'un des domaines de l'informatique nécessitant une constante mise à jour et un suivi en temps réel. Ce paramètre constitue un réel défi pour les éditeurs de solutions de sécurité qui doivent constamment se surpasser pour contrer des cybercriminels qui sont sans cesse à l'affût de la moindre occasion, développant de nouvelles techniques d'attaques de système.

Les ransomwares sont l'une des plus vieilles méthodes d'attaque mais néanmoins pas des moindres.

Avec de nombreuses victimes à travers le monde connaissant un nouvel essor avec la pandémie de COVID-19, ils sont devenus la cyber-menace la plus prolifique de ces dernières années.

Et le développement des nouvelles technologies telles que l'internet des objets, la venue d'un nouveau protocole d'adressage (IPv6) et l'expansion vers l'ordinateur quantique qui rendraient toutes d'une part l'avancée des attaques et une facilité à casser les systèmes de sécurité.

Pour y faire face, certaines entreprises ont opté pour l'utilisation de systèmes de détection d'intrusion capables de déceler la présence de la plupart des ransomware dans un système informatique.

Ce mémoire se divise en trois chapitres :

Le premier chapitre fait objet **de l'État de l'art,** qui décrit les ransomwares et quelques travaux de détection**. Les IDS** sont abordés dans **le chapitre II,** et la conception et l'implémentation de la solution pour **le dernier chapitre.**

Chapitre I : État de l’art

I. Introduction à la notion de ransomwares :

Les ransomwares (rançongiciel en français), des logiciels malveillants qui bloquent l'accès à l'ordinateur ou à des fichiers en les chiffrant et réclamant après le paiement d'une rançon pour en obtenir de nouveau l'accès, sont depuis quelques années, objets d'étude de plus en plus poussées. Selon vpnMentor, ils ont été de loin la cyber-menace la plus prolifique et la plus persuasive de ces dernières années. Et selon les chiffres du gouvernement américain, les attaques de ransomware sont depuis 2005 plus nombreuses en ligne que les violations de données. Elles n'ont pas toujours été d'échelle mondiale, ce qui leur a sûrement permis de rester sous les radars pendant très longtemps. **[1]**

Le premier type de ransomware est apparu en 1989. Il s'agit du **Trojan AIDS** aussi connu sous le nom de « PC Cyborg ». A cette époque, le sida faisant la une des journaux du monde entier, le docteur Joseph Popp en profita pour distribuer environ 20 000 disquettes contenant chacune un programme de renseignements sur le sida en surface et en arrière-plan un ransomware qui, après quelques jours, chiffrait les fichiers de l'ordinateur pour ensuite demander une rançon de 189 dollars afin de récupérer les fichiers chiffrés. **[2]**

Entre 2015 et 2016, il y'a eu une augmentation du nombre de familles de ransomwares qui n'ont pas été détectées comme malveillantes.

En Mai 2017, une attaque malware massive du nom de **WannaCry** a fait les gros titres du monde entier permettant ainsi de dévoiler au grand public la notion de ransomware. Touchant plus de 300 000 ordinateurs dans plus de 150 pays principalement en Inde, aux États-Unis et en Russie, WannaCry a réussi à atteindre de grosses institutions comme le National Health Service, les entreprises Vodafone, FedEx, Renault, Telefónica, le Centre hospitalier universitaire de Liège, le ministère de l'Intérieur russe ou encore la Deutsche Bahn. **[3]**

WannaCry est un raccourci de WannaCrypt, référence au fait que WannaCry est un crypto-ware. Plus spécifiquement, il s'agit d'un crypto Worm, capable de se reproduire et de se répandre automatiquement. **Pas d'arnaque phishing, pas de téléchargement depuis un site**

compromis. WannaCry a marqué une nouvelle phase chez le ransomware, en ciblant les vulnérabilités connues des ordinateurs.

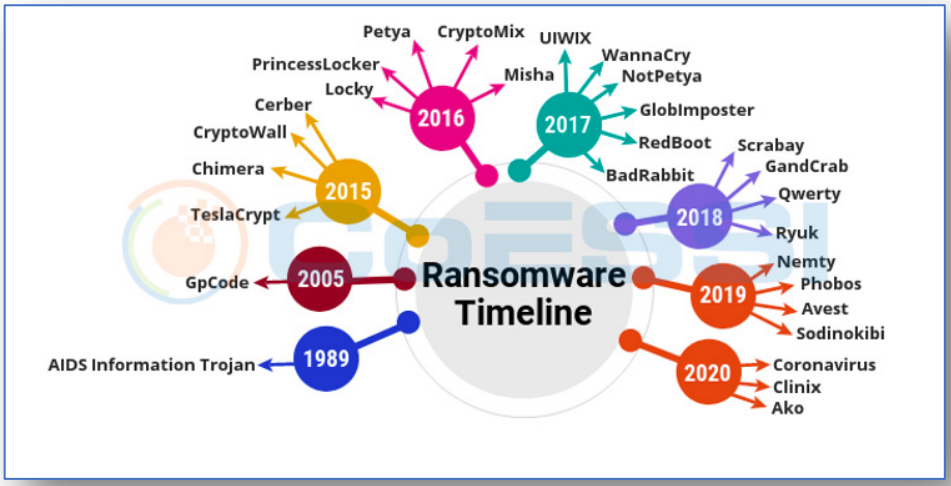


Figure 1 Timeline des différents ransomwares

Tirée de CoESSI.com

II. Les types de ransomwares :

Deux types de ransomwares sont notamment plus connus **[4]** :

1. Les ransomwares Lockers : qui ne ciblent pas les fichiers critiques mais cherchent à verrouiller l'ordinateur en bloquant les fonctions de base de celui-ci qui sera alors inutilisable. La victime se verra refusé l'accès au bureau par exemple, pendant que la souris et le clavier sont tous deux désactivés partiellement pour permettre l'interaction avec la fenêtre de demande de rançon pour rendre possible le paiement de cette dernière.
2. Les ransomwares Crypto : aussi reconnus comme les plus virulents et les plus agressifs. Dont l'objectif est de semer la panique chez les victimes en chiffrant des données importantes, comme des documents, des photos et des vidéos, sans verrouiller les fonctions de base de l'ordinateur contrairement aux ransomwares Locker. Ceux-ci peuvent voir leurs fichiers sans toutefois pouvoir y accéder. Ces ransomwares sont souvent accompagnés par un compte à rebours avec un message

de menace de suppression des fichiers en cas de non-respect du délai de paiement. Dans ce cas de figure, si les données n'étaient pas périodiquement sauvegardées sur le Cloud ou sur des appareils de stockage physique, il est très fort probable que les criminels aient gain de cause devant des victimes soucieuses de récupérer leurs fichiers. Il faut aussi comprendre que les ransomwares Crypto tentent de chiffrer n'importe quel fichier situé à la fois sur des lecteurs réseau mappés et non mappés, arrêtant ainsi un service ou l'ensemble de l'organisation en cas d'infection du système.

III. Les ransomwares sur la base du système cryptographique :

Les ransomwares cryptographiques sont divisés en trois types, basés sur le système cryptographique utilisé. **[5]**

1. Ransomwares à système cryptographique symétrique :

Utilise un algorithme de cryptage symétrique tel que DES ou AES pour crypter les fichiers de la victime, en utilisant la même clé pour le cryptage et le décryptage. Cela rend possible pour la victime la récupération de la clé secrète en appliquant des techniques d'ingénierie inverse ou d'analyse de la mémoire. La figure 1(a) illustre les activités de réseau impliquées dans ce type de ransomware.

2. Ransomwares à système cryptographique asymétrique :

Dans ce cas de figure, une clé publique, intégrée dans le fichier du ransomware ou téléchargée lors de la communication avec le serveur de commande et de contrôle (C&C) est utilisée pour crypter le fichier de la victime. La clé privée étant conservée uniquement chez l'attaquant, il est alors impossible pour la victime de l'obtenir sans payer la rançon. Cependant, cette technique consomme plus de ressources lors du chiffrement des fichiers. Les communications réseau correspondantes sont représentées sur la figure 1(b).

3. Ransomwares à système cryptographique hybride :

Qui utilise une clé symétrique générée dynamiquement pour crypter les fichiers de la victime et une clé publique pré-chargée pour crypter la clé symétrique elle-même, après l'avoir effacée de la mémoire. La plupart des familles modernes de ransomware crypto utilisent cette technique pour tirer parti des deux types de cryptage.

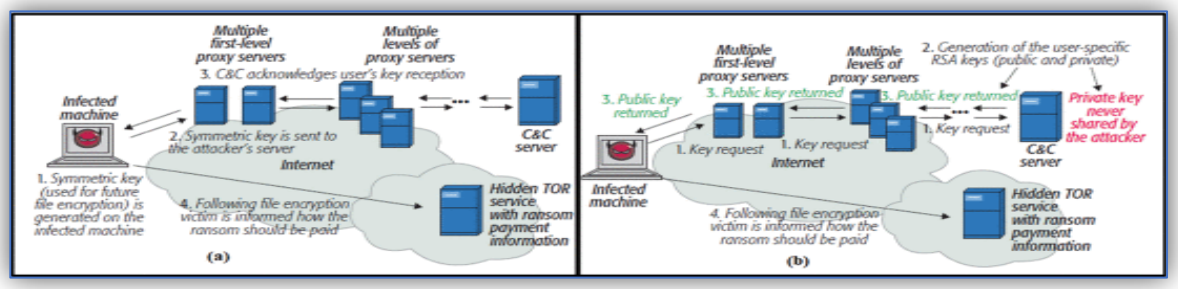


Figure 2 Communications réseau crypto ransomware (a) Cryptage symétrique, (b) Cryptage asymétrique.

Les familles de ransomwares crypto pour la plupart après l'infection tentent de se connecter au serveur C&C juste avant l'exécution de la charge utile. Dans ce cas de figure, l'analyse du trafic réseau peut donner des résultats significatifs dans la détection des ransomwares. Par ailleurs, les cryptolockers fonctionnent de différentes manières et sont en perpétuelle évolution, cette mutation constante est la cause de la complexité de leur détection pour les éditeurs de solutions de sécurité. **[2]**

IV. Statistiques sur les ransomwares :

Selon une enquête indépendante menée auprès de 5 000 responsables informatiques dans 26 pays différents menée par SOPHOS en 2020 **[6]** :

- **Environ 3/4 des attaques de ransomware aboutissent au chiffrement des données.**

  51 % des entreprises ont été touchées par un ransomware au cours de l'année passée. Les cybercriminels ont réussi à chiffrer les données dans 73 % de ces attaques.

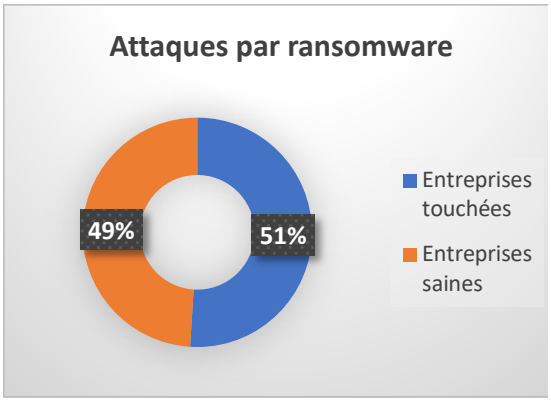


Figure 4 : entreprise attaquée par ransomware

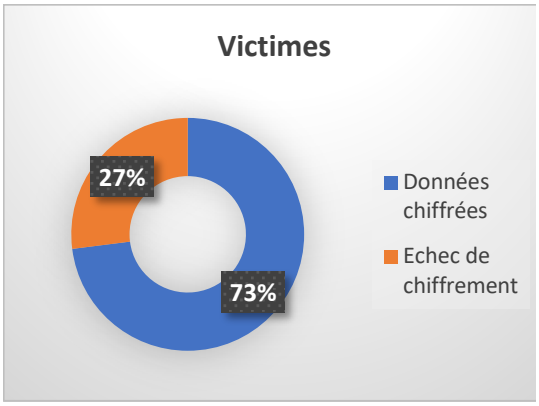


Figure 3 : taux de chiffrement

- **26 % des victimes dont les données ont été chiffrées les ont récupérées en payant une rançon.** 1 % a payé la rançon, mais n'a pas pu récupérer ses données.
- **94 % des victimes dont les données ont été chiffrées les ont récupérées.** Plus de deux fois plus de victimes les ont récupérées via des sauvegardes (56 %) plutôt qu'en payant une rançon (26 %).

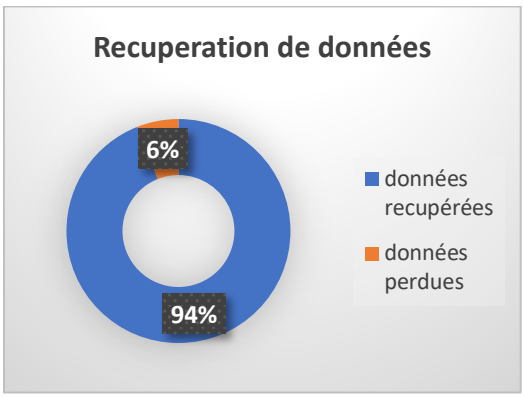


Figure 6 : taux de récupération de données

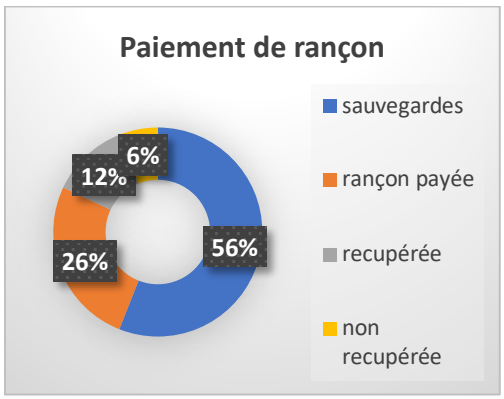


Figure 5 : taux de paiement de la rançon

- **Payer la rançon multiplie par deux le coût total d'un ransomware.** Le coût moyen que représente la gestion des dommages causés par les attaques de ransomware les plus récentes (en tenant compte des temps d'arrêt, des ressources humaines nécessaires, du coût des équipements et du réseau, du manque à gagner, de la rançon payée, etc.) est de 732 520 USD (environ 673 600 €) pour les entreprises qui ne paient pas la

rançon, et ce coût passe à 1 448 458 USD (soit à peu près 1 332 000 €) pour les entreprises qui la paient.

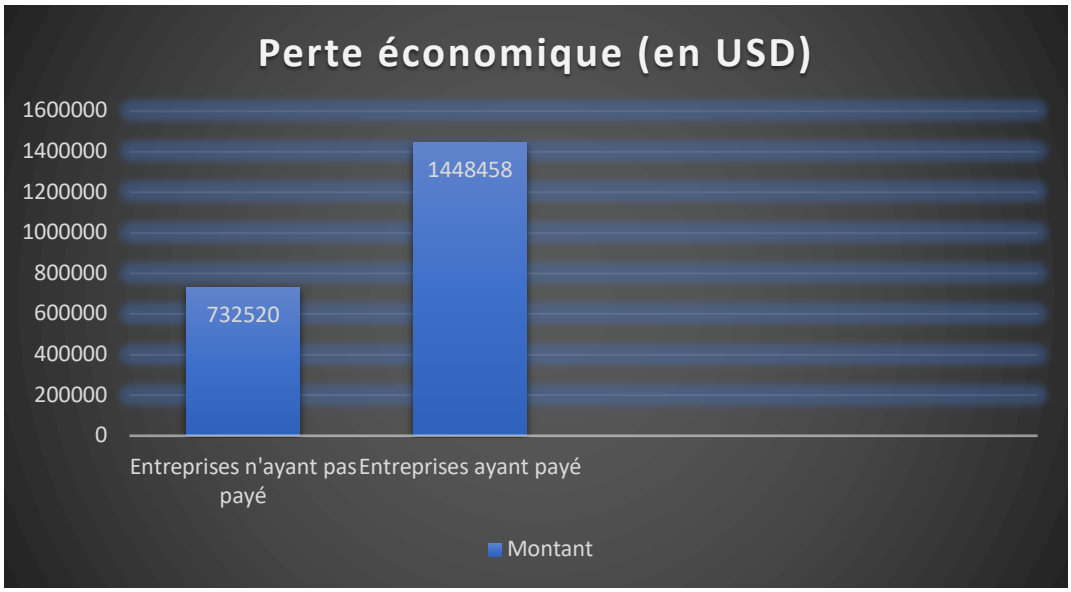


Figure 7 : Perte économique engendrée par ces attaques

- **Malgré le fait qu'il fasse souvent la Une de l'actualité, le secteur public est moins touché par les ransomwares que le secteur privé.** L'an dernier, 45 % des organismes du secteur public ont été touchés par un ransomware, contre une moyenne mondiale de 51 %, avec un maximum de 60 % dans le secteur des médias, des loisirs et du divertissement.
- **1 entreprise sur 5 n'est pas suffisamment protégée par son assurance cybersécurité.** 84 % des répondants ont une assurance cybersécurité, mais seulement 64 % couvrent les attaques de ransomware.
- **L'assurance cybersécurité paie la rançon.** Pour les entreprises bénéficiant d'une assurance couvrant les ransomwares, dans 94 % des cas, lorsque la rançon est payée pour récupérer les données, c'est la compagnie d'assurance qui la paie.
- **Les attaques de ransomware les plus efficaces ciblent les données dans le Cloud public.** 59 % des attaques où les données ont été chiffrées concernaient des données dans le Cloud public. Bien qu'il soit fort probable que les personnes interrogées aient interprété au sens large le terme 'Cloud public', en incluant notamment les services tels que Google Drive et Dropbox et des solutions de sauvegarde telles que Veeam, il

est clair que les cybercriminels ciblent les données, peu importe l'endroit où elles se trouvent.

V. Méthodes de détection des ransomwares :

Plusieurs méthodes de détections et de contre-mesures des ransomwares ont vu le jour et parmi lesquelles figurent **[7]** :

1. La protection basée sur l'analyse de fichiers c'est une méthode qui supervise quelques fichiers dans les machines des utilisateurs. Après modification, suppression ou mouvement de l'un de ces fichiers, le système déduit une activité de ransomware.
2. Une protection au niveau réseau contre certaines familles de ransomwares qui communiquent avec l'extérieur avant le chiffrement de fichiers. Cette méthode de détection repose sur l'analyse du trafic réseau généré par le programme, généralement la communication effectuée avec le centre de contrôle. Il a par exemple été proposé de découper le flot réseau en séquences sur lesquelles appliquer le modèle en comparant l'alignement avec du trafic malveillant témoin.
3. Une détection par l'analyse comportementale des ransomwares ou encore analyse dynamique désigne le processus d'observation comportementale du ransomware en provoquant volontairement son exécution au sein d'un environnement surveillé, isolé du reste du système (type « bac à sable »). L'analyse dynamique présente l'avantage d'être parfaitement robuste face aux méthodes de maquillage des fichiers statiques (obfuscation de code, chargement de code dynamique, chiffrement, packing...)
4. Une détection par l'apprentissage automatique et l'intelligence artificielle :

Les antivirus conventionnels se basent uniquement sur les signatures connues pour la détection. L'efficacité permanente de cette approche se discute car un ransomware d'une même famille peut avoir plusieurs variantes et par conséquent, différentes signatures (des

packers et des méthodes d'obfuscation sont souvent utilisés). Cependant, les familles de ransomware ont un comportement général immuable qui leur est propre, ce qui leur détection possible avec plus d'efficacité en utilisant une approche basée sur leurs comportements.

VI. Travaux connexes sur la détection des ransomwares :

AO Almashhadani et al. Se sont appuyés sur les recherches de pointes sur la détection de ransomware basée sur le réseau. Ils ont fourni une analyse en profondeur du trafic réseau avec le ransomware Locky en étude de cas. Pour ce faire, ils ont créé un environnement de banc d'essai dédié dans le but de capturer, collecter et analyser avec soin les fichiers PCAP (format de fichier de capture du trafic réseau) de l'ensemble de données MCFP de Locky.

Leur analyse indique que plusieurs activités réseau peuvent être utilisées pour relever des caractéristiques comportementales potentielles et a permis d'extraire en tout 18 fonctionnalités informatives pouvant différencier le trafic généré par un hôte compromis d'un trafic normal à l'aide du trafic TCP, HTTP, DNS et NBNS.

En outre, ils proposent une méthode et un prototype de détection de ransomware basée sur le réseau multi-classificateur, fonctionnant à deux niveaux différents : le niveau paquet et le niveau flux. Des analyses expérimentales détaillées démontrent clairement une précision de détection élevée pour chaque niveau : 97,92 % et 97,08 % respectivement validant l'efficacité des caractéristiques extraites. Leur découverte contribue largement à l'avancée des recherches sur la détection des logiciels malveillants sur un réseau. **[5]**

Une étude menée par **S.-J. Lee et al.** en 2021 a consisté à identifier en temps réel si les clients étaient infectés par un ransomware crypto open source, RAASNet, via Google Rapid Response (GRR), l'osquery de Facebook et Open Source hids SECurity (OSSEC) parmi les techniques de détection systématique de ransomware. Chacun de ces outils EDR utilise sa propre fonction pour envoyer une demande de détection d'infection de fichier causée par un ransomware. Le GRR peut détecter des fichiers et des répertoires via Flow, et osquery peut envoyer des requêtes pour déterminer les changements. De plus, OSSEC détecte les changements dans les fichiers à l'aide du contrôle d'intégrité, une fonction de surveillance en temps réel. Les résultats de la détection étaient affichés sous forme de notifications ou

de journaux lorsque tous les fichiers d'un répertoire spécifique étaient cryptés, indiquant que les trois outils EDR de l'environnement Linux sont capables de détecter les ransomwares. Grâce à cette détection des menaces open source, il est possible de déterminer à quel moment le ransomware a été exécuté et d'analyser la méthode d'attaque. Bien que cette étude n'ait pas été testée dans diverses conditions de changement environnemental, dans des travaux futurs. Néanmoins Grâce à cette elle, les auteurs sont parvenus à détecter les ransomwares en utilisant chaque fonctionnalité de ces trois outils EDR open source qui ne sont que représentatifs. **[8]**

S. Sheen et al. ont opté pour une détection des appels API utilisés par le ransomware et les fichiers bénins. Selon leur étude, les fonctions API et les appels système prennent en charge diverses opérations clés fournies par les systèmes d'exploitation, telles que le réseau, la sécurité, les services système, la gestion de fichiers, etc. Selon cette même une analyse détaillée d'un grand nombre de ransomwares montre qu'il existe des appels d'API qui sont plus importants dans le ransomware que dans les fichiers bénins. De plus, il est possible de déterminer si un fichier peut être malveillant par ses appels d'API, dont certains sont typiques pour certains types de ransomware. Les modèles d'appels de fonction API peuvent fournir des informations clés qui peuvent être utilisées pour détecter le mouvement du logiciel et pour représenter les comportements du logiciel. Ainsi, l'analyse des fonctions API et des appels système joue un rôle important dans l'analyse du comportement des ransomwares. **[9]**

U. Urooj et al. ont mené la toute première étude qui traite des concepts de pré-chiffrement et de dérive de population des ransomwares pour les crypto-ransomwares. Les travaux existants traitent soit d'un seuil fixe pour la définition des limites de pré-chiffrement, soit utilisent des données entières, ce qui n'est pas utile pour arrêter les attaques de crypto-ransomware et ne prennent pas non plus en compte l'évolution des variantes avancées. Dans leur article, ils ont proposé un modèle de détection précoce adaptatif de crypto-ransomware de pré-cryptage basé sur la littérature existante et destiné à être développé et validé. **[10]**

Étude comparative :

Les études mentionnées ci-dessus traitent toutes du concept de détection en temps réel. Néanmoins, elles présentent de grandes différences dans le fond.

La première, basée sur l'analyse du trafic du réseau peut relever les caractéristiques comportementales de certains types de ransomware, bien qu'elle ne puisse pas stopper certains types de ransomware elle se relève tout de même efficace pour la détection en général.

La détection grâce aux outils EDR mise en place dans la seconde étude utilise la lecture des fichiers grâce à ces derniers pour relever les activités suspectes.

La détection basée sur les appels API, est elle aussi une alternative qui n'est pas des moindres. Les fonctions API prenant en charge divers opérations clés du système d'exploitation.

La quatrième étude bien que n'étant une théorie, révolutionne la détection en temps réel car traitant du concept de pré-cryptage.

En sommes, nous ne saurions dire quelle étude est la meilleure. Elles ont toutes leur utilité dans la détection et ne traitent pas du même concept bien qu'étant toutes des moyens de détection en temps réel.

Chapitre II : les IDS

I. Contexte

L'expansion de l'internet et des nouvelles technologies s'est vue accompagnée de l'augmentation de la cybercriminalité, et surtout d'intrusions non autorisées dans les réseaux des entreprises. Pour protéger leurs données et leur intégrité contre les criminels du net, les entreprises et institutions ont opté pour l'utilisation de plusieurs outils de sécurité réseau, notamment les systèmes de détection d'intrusion ou IDS.

1. Définition

Les systèmes de détection d'intrusion plus connus sous le nom d'IDS (en anglais intrusion detection system) sont des outils d'écoute et de sécurité réseau qui ont pour fonction de détecter les activités anormales sur le réseau auquel ils sont rattachés ou sur lequel ils sont placés en générant des alertes. ¨

2. Historique des IDS

Selon Wikipédia le tout premier IDS nommé **IDES** et développé par Dorothy Denning est apparu en 1987, avant même l'usage d'internet ou des réseaux développés. Il s'agissait d'un **HIDS**. Apparaissent ensuite les **NIDS** au début des années 1990. Jusque-là, seule la détection à base de signature était en application. Avec le progrès des techniques de détection (découverte de patterns dans les communications réseaux), les IDS à base d'Anomaly detection (détection comportementale) commencent à apparaître. On note aussi l'apparition des DIDS (IDS distribués) en 1994 qui permettront de gérer un parc de machines.
Les IDS explosent à l'arrivée du cloud computing, avec l'apparition de nouvelles contraintes (apparition des IDS pour hyperviseurs, multiplication du parc de machines à surveiller...). Cela entraîne donc l'apparition des Hypervisor-based IDS. **[11]**

II. Méthodes de détection des IDS :

Les IDS utilisent 3 méthodes de détection des anomalies, à savoir **[12] [13] [14]** :

1. La détection basée sur les signatures :

C'est la méthode la plus simple car elle consiste en une comparaison des signatures des activités anormales à une liste de signature déjà établie des attaques connues pour

identifier les possibles incidents. Pour cela, la méthode utilise des opérations de comparaison de chaîne.

2. La détection basée sur les anomalies :

Compare les définitions d'une activité considérée comme normale avec les événements observés afin d'identifier les écarts significatifs. Cette méthode de détection peut se révéler très efficace pour repérer les menaces inconnues.

3. L'analyse dynamique des protocoles :

Quant à elle, compare les profils prédéterminés des définitions généralement acceptées de l'activité bénigne du protocole, pour chaque état du protocole, avec les événements observés, afin d'identifier les écarts de conduite.

A savoir que la détection basée sur les signatures et celle basée sur le comportement peuvent être utilisées simultanément dans un seul et même IDS

III. Les principales familles d'IDS et leur fonctionnement :

Il faut comprendre qu'il existe plusieurs familles d'IDS, mais les trois principales sont les suivantes **[15] [11]** :

1. Les NIDS (Network Based Intrusion Detection System):

En français, système de détection d'intrusion basé sur l'écoute du réseau Ceux-là assurent la sécurité au niveau du réseau en analysant en temps réel le trafic qu'ils aspirent à l'aide d'une sonde (carte réseau en mode "promiscuous"). Ce sont des outils très utiles pour l'administrateur réseaux qui va pouvoir, en temps réel, comprendre ce qui se passe sur son réseau et prendre des décisions en ayant toutes les informations.

Ils peuvent être placés à divers endroits sur le réseau, en amont ou en aval d'un pare feu ou encore sur chaque hôte, comme un anti-virus. Ces IDS vont analyser tout le trafic entrant et sortant du réseau afin d'y déceler des attaques. Cependant, un NIDS placé sur chaque hôte ne saura pas détecter toutes les attaques possibles comme les attaques par déni de service (DDoS) car il ne verra pas tout le trafic réseau, mais que celui qui arrive à l'hôte final.

Quand un NIDS est positionné en amont d'un pare feu **(Fig. 9),** il pourra alors générer des alertes pour le pare feu qui va pouvoir filtrer le réseau.

Placé en aval du pare feu **(Fig. 8),** le NIDS produira moins de faux positifs, car le trafic réseau qu'il analysera aura déjà été filtré par le pare feu.

Dès qu'une attaque est détectée, que ce soit par signature (SIDS) ou anomalies (AIDS), une alerte est remontée afin de pouvoir prendre une décision sur l'action à effectuer, soit par un IPS ou intrusion prevention system (Système de prévention d'intrusion), soit par l'administrateur.

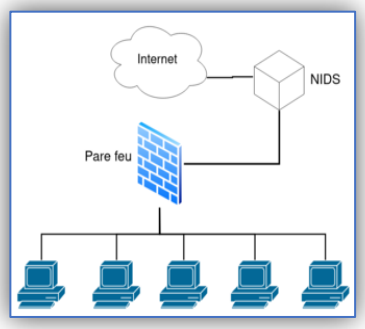


Figure 9 : placement d'un NIDS en amont du pare-feu

¨Tiré de https://fr.wikipedia.org¨

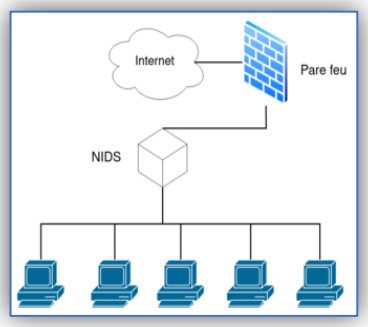


Figure 8 : placement d'un NIDS en aval du pare-feu

¨Tiré de https://fr.wikipedia.org¨

2. Les HIDS (HostBased Intrusion Detection System) ou système de détection d'intrusion basé sur l'écoute des hôtes :

Surveillent l'état de la sécurité au niveau des hôtes. Ils sont mis en place directement sur les hôtes à surveiller et analysent directement leurs fichiers, les différents appels système et aussi les événements réseaux. Les HIDS agissent comme des antivirus mais en plus poussé, car les antivirus ne sont intéressés que par les activités malveillantes du poste alors qu'un HIDS va pouvoir intervenir s'il détecte des attaques par dépassement de tampon et concernant les processus système par exemple.

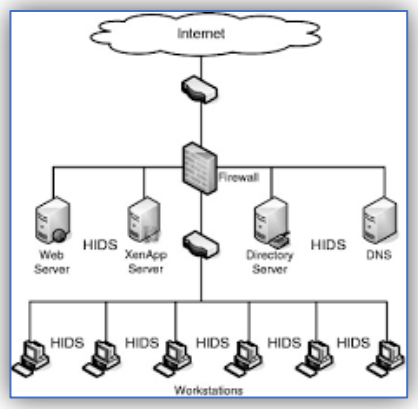


Figure 10 Schéma HIDS

¨Tiré de sciencedirect.com¨

3. Les IDS hybrides combinant les deux premières fonctionnalités :

Plus pertinentes au niveau des alertes car elles utilisent les NIDS et HIDS. Les HIDS sont particulièrement efficaces pour déterminer si un hôte est contaminé et les NIDS permettent de surveiller l'ensemble d'un réseau contrairement à un HIDS qui est restreint à un hôte.

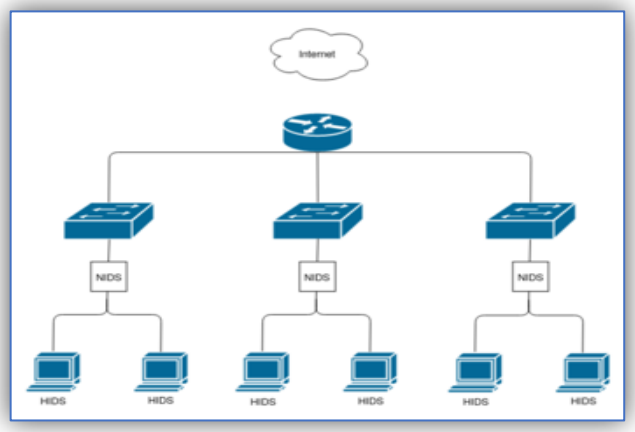


Figure 11 Réseau d'IDS hybride

Tiré de fr.wikipédia.org

IV. Logiciels de détection d'intrusion :

Il existe un panel de logiciels de détection d'intrusion qui sont divisés en deux types. Ceux qui sont destinés aux réseaux (NIDS) et ceux destinés aux postes (HIDS).

1. OSSEC :

C'est un IDS (système de détection d'intrusion) de type host(poste) qui analyse les trafics sur les ports pour détecter les anomalies. Le logiciel peut aussi jouer le rôle de système de prévention d'intrusion en se servant du système de réponse active. Il fonctionne sur de nombreux systèmes d'exploitation tels que : Windows, Linux et MacOs

Il assure principalement trois (3) fonctions :

- Surveille tout ce qui se passe sur l'hôte
- Stopper les attaques par brute-force
- Assurer les exigences de conformités PCI (Peripheral Componet Interconnect) liées à la surveillance. **[16]**

Figure 12 OSSEC

2. BRO :

Bro est un logiciel de détection d'intrusion de type réseau. De son nouveau ZEEK depuis 2018, il analyse tout le flux réseau. Il fonctionne sur les mêmes bases que Snort mais différents de par leur implémentation. Disponible pour le système UNIX, il travaille avec une base de données des signatures connues avec les comportements normaux**. [17]**

Figure 13 : Bro IDS

3. IDSNet :

C'est un logiciel de détection aussi de type réseau basé sur le Machine-Learning. Il a été créé à l'université technique du Danemark au sein du département " Informatics and Mathematics Modelling" ("Modélisation informatique et mathématique" en français). **[18]**

Figure 14 : IDSnet

4. SNORT :

Comme indiqué plus haut, Snort permet de détecter une intrusion en se basant à la fois sur les signatures connues et les comportements normaux. Il permet aussi d'établir un ensemble de règle pour gérer les entrées-sorties. **[18]**

Figure 15 : SNORT

Conclusion :

Les IDS sont d'aujourd'hui incontournable pour une bonne politique au niveau d'une infrastructure en complétant les antivirus et d'autres outils de sécurité.

Chapitre III : Conception et Implémentation.

I. Contexte :

Pour mettre en place notre solution, nous allons utiliser un IDS qui nous permettre de surveiller tous les trafics dans notre réseau. Pour cela nous configurons notre logiciel avec les chemins d'accès et en indiquant notre réseau sur lequel le test sera fait. Et pour finir le résultat des différents tests seront présentés dans un tableau.

II. Pourquoi Snort :

Le choix s'est porté sur le logiciel Snort car il est le plus utilisé dans le domaine et cela est dû à son efficacité en matière de détection d'intrusion.

Les avantages de l'utilisation du logiciel de détection Snort sont les suivants :

- Logiciel libre et mise à jour sous licence GNU
- Utilisable sur plusieurs systèmes d'exploitation (Windows, Linux, …)
- Analyseur du trafic réseau
- Il met à disposition un ensemble de règles à définir au besoin
- Les données sont stockées dans une base de données
- Définition des signatures pour la détection **[19]**

Son inconvénient est qu'il est particulièrement difficile à prendre en charge. Sa configuration et sa prise en main sont aussi très compliquées.

III. Principe de détection des ransomware

Les principales cibles des ransomwares sont les serveurs. Pour pouvoir contrer ces attaques, il faut d'abord qu'elles soient détectables.

Snort est principalement utilisé pour la détection d'intrusion des malwares dans un réseau. Il opère en combinant l'analyse des signatures et des comportements normaux et une analyse en temps réel du trafic réseau. De ce fait, une des meilleures manières de détecter un ransomware est de procéder à une détection comportementale.

Pour la détection comportementale, le plugin **SPADE** a été développé par Silicon Defense. Il détecte les paquets inhabituels et suspicieux. En cas de détection, SPADE est capable

d'envoyer deux types d'alertes. La première, « **spp_anomsensor : Anomaly threshold exceeded** » indiquant la présence d'un paquet anormal, la seconde qui est le message le message « **spp_anomsensor : threshold adjusted to T after X alerts (of N)** » indiquant un changement de seuil. Ce projet fut cependant abandonné.

Ensuite on a l'algorithme **PHAD** développé par Matthew V. Mahoney et Philip K. Chan. Cet algorithme analyse les entêtes des couches réseau, liaison de données et transport pour établir un schéma normatif qui sera réévalué à chaque fois qu'un nouvel évènement est traité. **[20]**

A défaut de l'obtention de ces plugins, pour établir notre solution, nous avons décidé de tester nos échantillons de ransomwares avec les règles de base de Snort pour attester de son efficacité. Notre objectif sera de déterminer si l'échantillon de ransomware établit une connexion avec un serveur distant car comme nous le savons, certains ransomwares pour chiffrer les données vont chercher la clé de chiffrement au niveau du serveur de l'attaque.

La détection de ce Trafic entraîne la possibilité de prévention rapide contre les exploits de ransomware utilisant ce processus.

- **Scenario d'attaque pouvant être détectée par notre solution** :

De nos jours, il existe plusieurs scenarios d'attaque par ransomwares :

- Le cybercriminel lance l'attaque, le logiciel pour s'exécuter envoie une requête de demande de clé de chiffrement pour crypter les données de la victime.
- Le cybercriminel lance l'attaque, avant le cryptage des données le logiciel malveillant copie ces données dans une base de données contrôlée par l'attaquants.

La figure suivante résume les deux scenarios attaques par ransomwares :

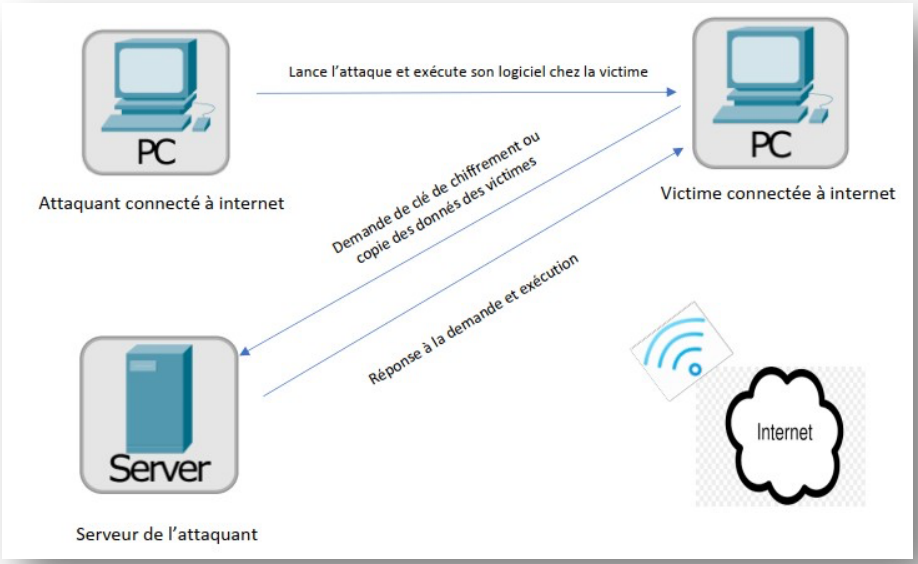


Figure 16 : Illustration d'une attaque par ransomware

Le diagramme d'activité ci-dessous montre comment l'attaque de ransomware détectable par notre solution se déroule dans le monde réel en ayant pour cible un utilisateur lambda.

Pour détecter cette attaque, nous allons nous mettre entre la machine victime et le serveur.

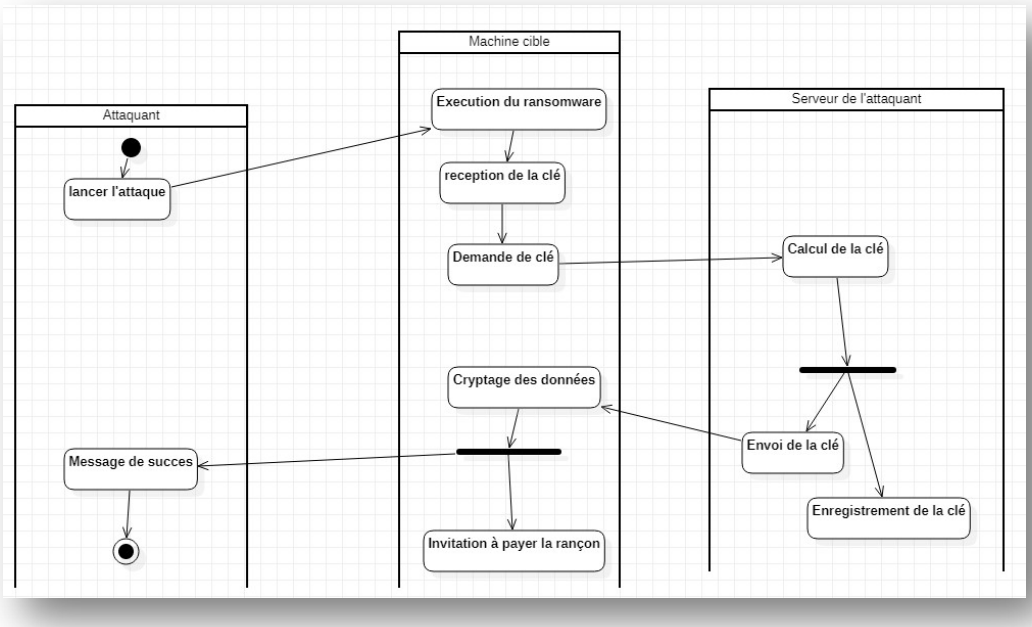


Figure 17 : diagramme d'activité présentant le ciblage d'un tiers sans protection ni système de détection

Dans le monde réel, la solution que nous déployons permet de collecter l'ensemble du trafic en tenant compte de son type afin de générer une alerte.

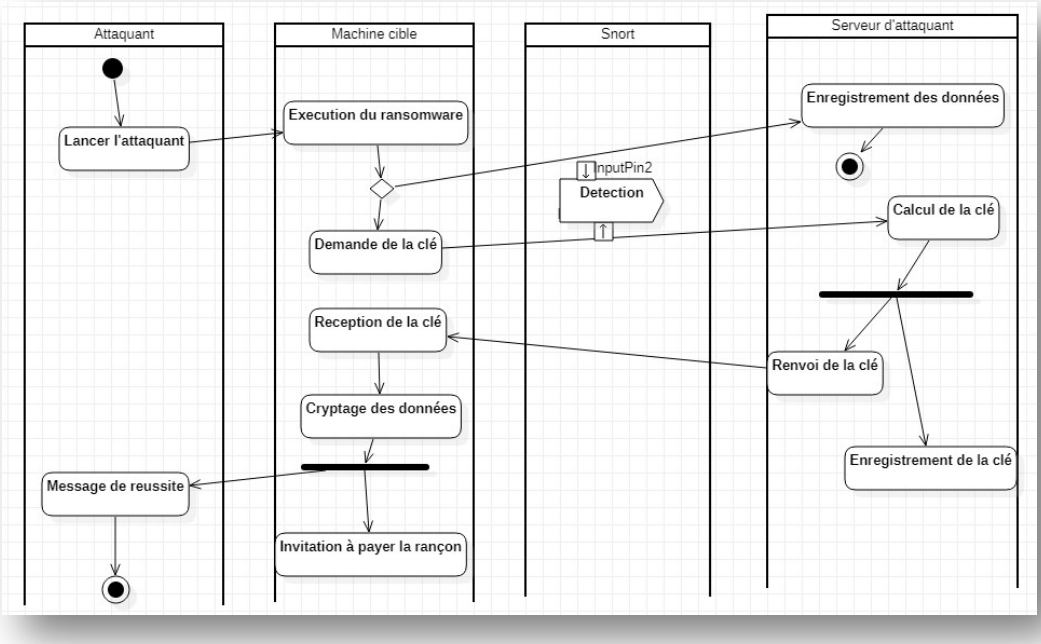


Figure 18 : déploiement de la solution dans le monde réel

- **Scenario de test :**

Notre architecture se présente comme suit :

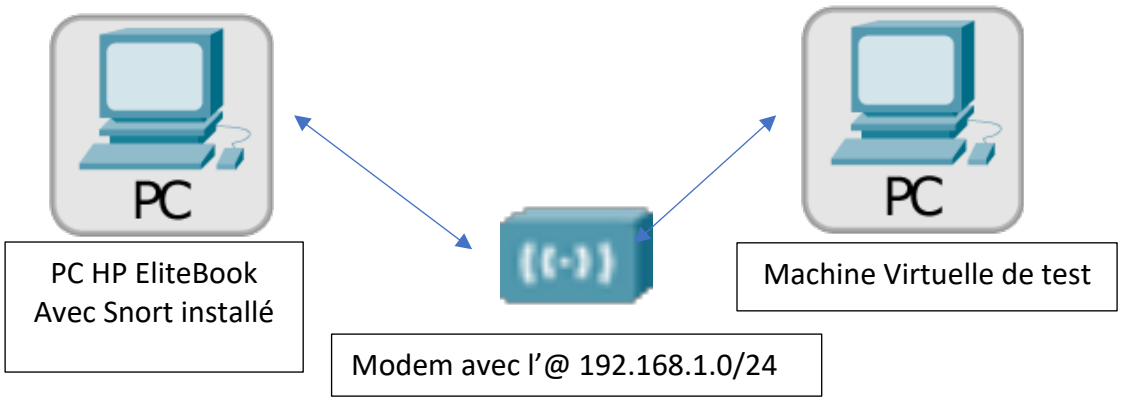


Figure 19 : Architecture de la mise en place de notre solution

Cette architecture est composée de trois (3) machines :

- Le PC HP qui accueille le logiciel Snort
- Sur notre PC, nous installons des machines virtuelles avec le système d'exploitation Windows 10. Et sur cette machine nous allons exécuter nos échantillons de ransomwares.
- Le Modem crée un réseau sur lequel les machines vont réagir entre elles permettant

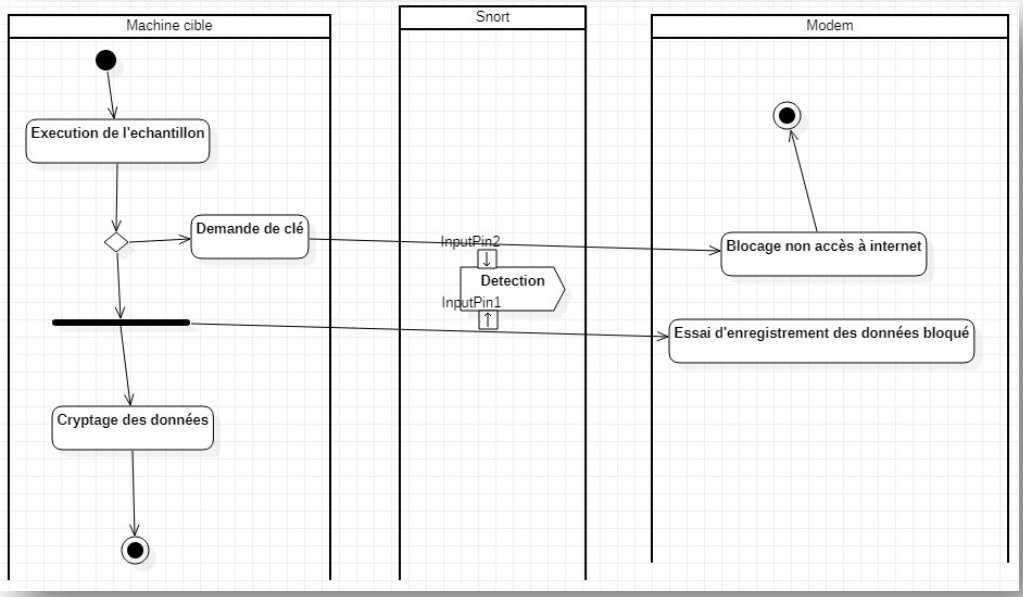


Figure 20 : diagramme de test

IV. Installation et configuration du logiciel Snort :

1. Installation :

La démarche à suivre pour l'installation de Snort se décrit comme suit :

Il faut d'abord se rendre sur le site officiel du logiciel à l'adresse www.snort.org et télécharger l'exécutable. Dans notre cas nous exécutons la version 2.9.18.

En plus de l'exécutable, nous téléchargeons aussi :

- Le fichier compressé ***snortrules-snapshot*** pour la version correspondante pour la configuration de notre logiciel.
- Le fichier compressé ***Community-Rules*** contenant un ensemble de règles.
- Et enfin le programme *WinPcap* pour gérer les logs en format *Pcap*.

A noter que la version que nous utilisons n'est pas la dernière à ce jour. C'est une version antérieure dont le choix se traduit par une plus grande flexibilité dans le travail à faire.

Enfin nous exécutons nos logiciels *Snort* et *WinPcap* de façon standard.

2. Configuration du logiciel :

Configurer Snort revient à modifier une bonne partie du fichier ***snort.conf*** du répertoire **c:\Snort\etc**. Il faut impérativement respecter les quelques étapes qui suivent pour la configuration de ce fichier :

- Étape 1 : Premièrement, l'adresse du réseau sur lequel la surveillance doit s'opérer sur la ligne 45 et l'adresse des machines externes qui peut être toute machine qui ne fait pas partie du réseau de surveillance doivent être toutes deux spécifiées.

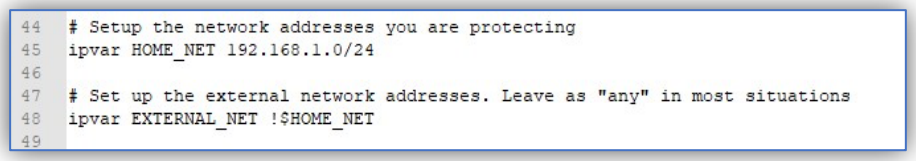


Figure 21 Spécification d'adresse réseau

- Étape 2 : Deuxièmement, les lignes à supprimer. Elles sont les lignes numéro 105, 253 et de 263 à 269 et la ligne 335.
- Étape 3 : Troisièmement les lignes à activer. Les lignes à activer sont les suivantes : 186, 418 et de 659 à 661. Sur la ligne 186, le chemin vers le dossier *log* doit être indiqué.
- Étape 4 : Pour terminer avec le fichier *snort.conf*, les chemins des dossiers indiqués sur les lignes 104 à 106, 113, 114, 247 et 250 doivent être modifiées en indiquant les chemins exacts.
- Étape 5 : Cette étape consiste à décompresser le dossier ***snortrules-snapshot*** et à remplacer les dossiers ***preproc_rules*** pour le préprocesseur et ***rules***.
- Étape 6 : La dernière étape est de décompresser le fichier ***community-rules*** et le copier dans le dossier ***rules***.

Nous mettons le logiciel Snort en marche et commençons à collecter les trafics au niveau du réseau. Snort contient un ensemble de règle se portant sur les différents protocoles UDP, TCP,

ICMP …. À chaque test nous devons réinstaller la machine virtuelle car nous exécutons directement nos échantillons sur celle-ci.

Les trafics collectés sont enregistrés dans le dossier log et ils sont décortiqués en utilisant le logiciel Wireshark. Tout trafic venant de la machine virtuelle vers le Modem différent d'un handshake (processus permettant de maintenir la connexion) est considère comme suspect et peut être une tentative de liaison à un serveur distant pour obtenir la clé de chiffrement.

3. Présentation de règle

Les règles Snort sont composées de deux parties séparées par une flèche écrites sur une seule ligne.

1ere partie : cette partie commence par le mot clé ALERT (ou log, …) suivi du type de paquet à vérifier (UDP, TCP ou ICMP) ainsi que l'adresse source et le port à surveiller.

Exemple : alert tcp $HOME_NET [21,25,443,465,636,992,993,995,2484] (ou any pour tous les ports)

Snort agit en fonction de l'action établie dans la règle. Ces actions sont au nombre de 5 :

- Alert : pour générer une alerte et journalisé le paquet
- Log : pour la journalisation du paquet
- Pass : sert à ignorer le paquet
- Activate : fait une alerte et active une règle dynamique
- Dynamic : passif jusqu'à activation d'une règle **activate** et puis agit comme une règle **log**.

2e partie : on indique l'adresse de destination et le port en notant un message d'alerte et un numéro identifiant la règle.

Exemple : $EXTERNAL_NET 445 (msg :" Alerte requête ICMP " ; sid = 1000001)

Pour une règle complète, on a :

- alert 192.168.10.0/24 8080 -> 172.16.10.0/24 8080 (msg : "Connexion http " ; sid = 1000000001).

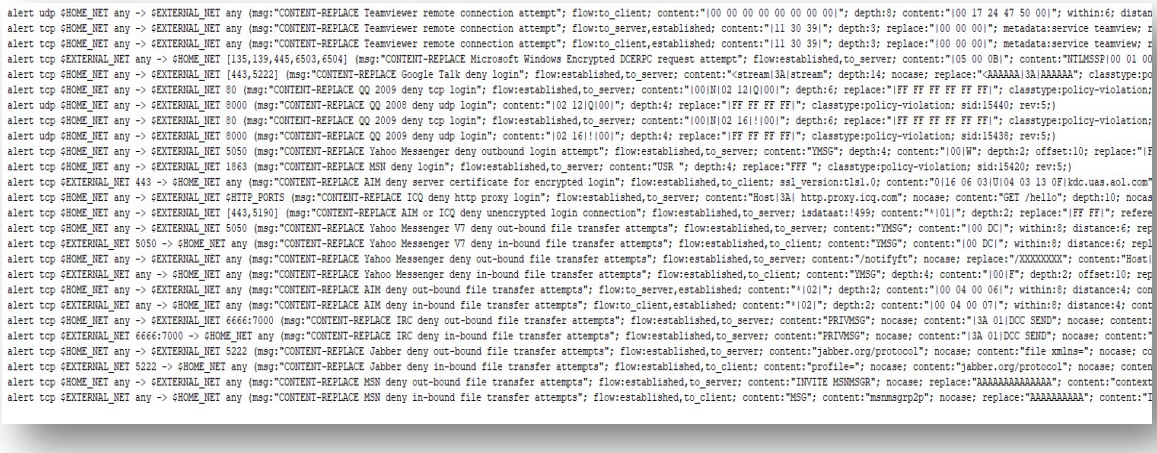
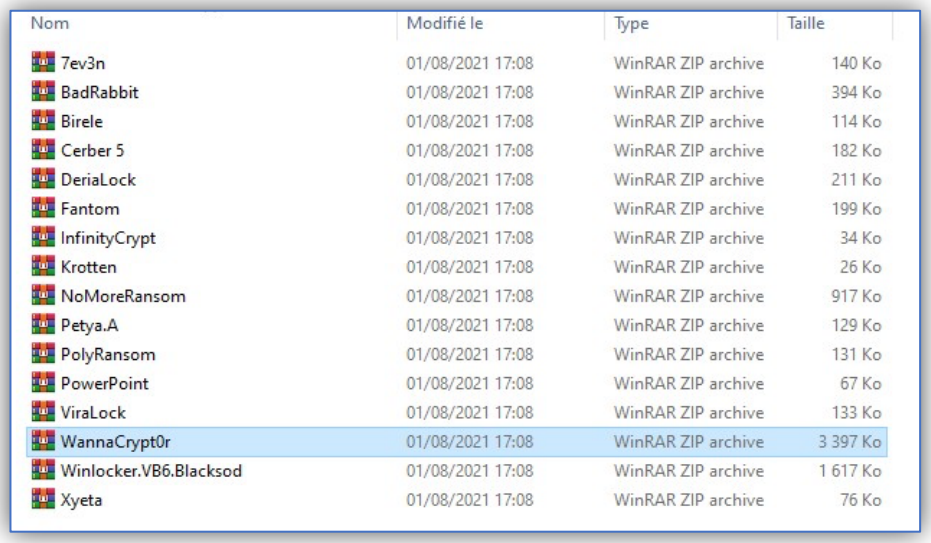


Figure 22 : exemple de règles

V. Test et résultat :

Les tests qui suivent ont été menés sur ordinateur portable **HP core i5** avec une **RAM de 8 Go** et un disque de **180 giga SSD.** Nous y installons notre outil de surveillance et le logiciel **VirtualBox** sur lequel nous installons des machines virtuelles, machines qui serviront pour l'exécution des ransomwares.

Le tableau suivant présente les résultats des différents tests avec chacun des échantillons suivants de ransomwares obtenus sur la base de données des malwares du site internet GitHub.



Nom	Modifié le	Type	Taille
7ev3n	01/08/2021 17:08	WinRAR ZIP archive	140 Ko
BadRabbit	01/08/2021 17:08	WinRAR ZIP archive	394 Ko
Birele	01/08/2021 17:08	WinRAR ZIP archive	114 Ko
Cerber 5	01/08/2021 17:08	WinRAR ZIP archive	182 Ko
DeriaLock	01/08/2021 17:08	WinRAR ZIP archive	211 Ko
Fantom	01/08/2021 17:08	WinRAR ZIP archive	199 Ko
InfinityCrypt	01/08/2021 17:08	WinRAR ZIP archive	34 Ko
Krotten	01/08/2021 17:08	WinRAR ZIP archive	26 Ko
NoMoreRansom	01/08/2021 17:08	WinRAR ZIP archive	917 Ko
Petya.A	01/08/2021 17:08	WinRAR ZIP archive	129 Ko
PolyRansom	01/08/2021 17:08	WinRAR ZIP archive	131 Ko
PowerPoint	01/08/2021 17:08	WinRAR ZIP archive	67 Ko
ViraLock	01/08/2021 17:08	WinRAR ZIP archive	133 Ko
WannaCrypt0r	01/08/2021 17:08	WinRAR ZIP archive	3 397 Ko
Winlocker.VB6.Blacksod	01/08/2021 17:08	WinRAR ZIP archive	1 617 Ko
Xyeta	01/08/2021 17:08	WinRAR ZIP archive	76 Ko

Figure 23 Échantillons de Ransomwares

1. Test :

- Exemple de test sans utilisation de snort

Le test suivant est mené pour voir l'exécution d'un de nos échantillons.

La figure ci-dessous représente notre machine virtuelle avant l'exécution de l'échantillon :

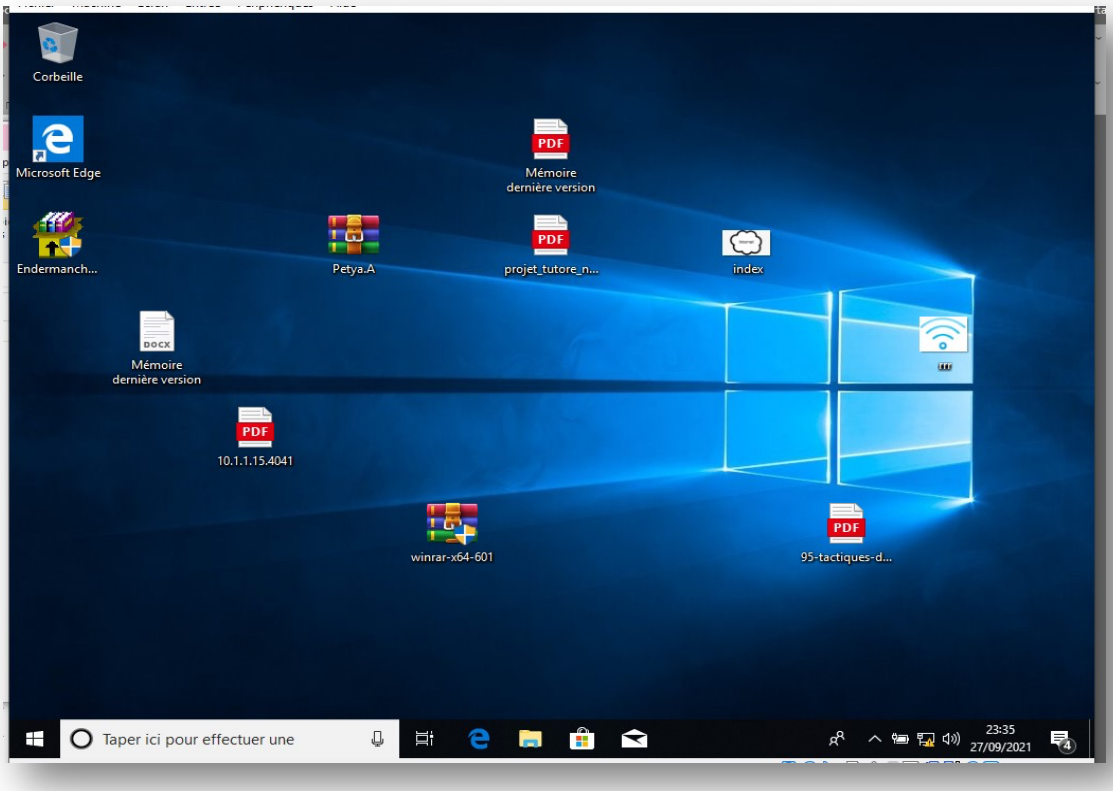


Figure 24 : capture d'écran avant exécution de l'échantillon

Nous voyons qu'il y a des photos, PDF et fichier exécutable sur le bureau de notre machine virtuelle. Nous avons décompressé notre échantillon nommé **PetyA** en prenant en compte la désactivation de la sécurité de Windows 10 (Windows defender, pare-feu …) pour pallier à toute interférence avec celle-ci.

La figure suivante donne une image après l'exécution de notre échantillon :

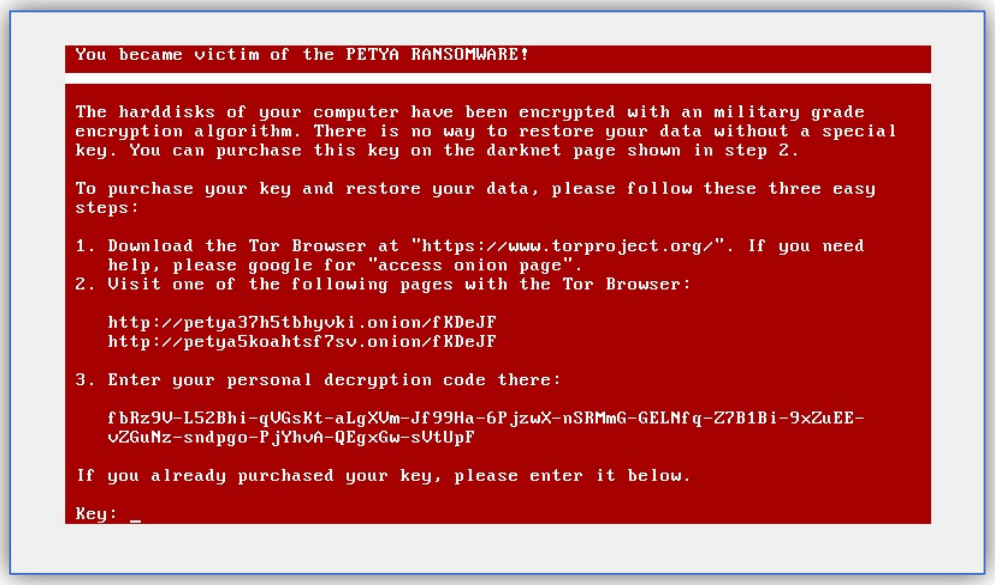


Figure 25 : capture d'écran après exécution de l'échantillon

Le logiciel entraine un blocage total de la machine, l'utilisateur ne peut rien faire sur celle-ci et doit obligatoirement payer la rançon afin de débloquer sa machine et l'utiliser ou réinstaller complètement son système d'exploitation s'il n'a pas de fichiers importants dans son disque.

- **Test avec Snort en marche**

Nous lançons Snort avec la commande « ***snort -A console -l c:\snort\log -c c:\snort\etc\snort.conf -ix*** *(x représentant notre interface de connexion au réseau)* ».

Le flux capté sera enregistré dans le dossier **log**. Et nous pouvons analyser ces fichiers enregistrés à l'aide du logiciel de sniffing Wireshark. Le tableau ci-dessous fait état du résultat des tests.

N°	Échantillons	Actif	Trafic détecté
1	BadRabbit	Oui	Il capte une tentative de fuite d'information
2	Birele	Non	-
3	WannaCry	Oui	Aucun Trafic
4	Cerber 5	Oui	Aucun Trafic
5	Fantom	Oui	Aucun Trafic

6	DeriaLock	Oui	Aucun Trafic
7	InfinityCrypt	Oui	Aucun Trafic
8	Krotten	Non	-
9	Xyeta	Non	-
10	Petya.A	Oui	Aucun Trafic
11	PolyRansom	Non	-
12	ViraLock	Non	-
13	Winlocker	Non	-
14	PowerPoint	Oui	Aucun Trafic
15	NoMoreRansom	Non	-
16	7ev3n	Non	-

2. Résultats :

Sur les **16 échantillons**, la moitié n'est pas actif. Et parmi ceux qui sont actifs, un seul communique avec un serveur distant ce qui fait qu'aucun Trafic n'a été détecté au reste. Ce qui nous donne un pourcentage de réussite de **12,5 %** avec les échantillons testés.

La figure ci-dessous montre la capture d'écran pour l'exécution du ransomware **BadRabbit** :

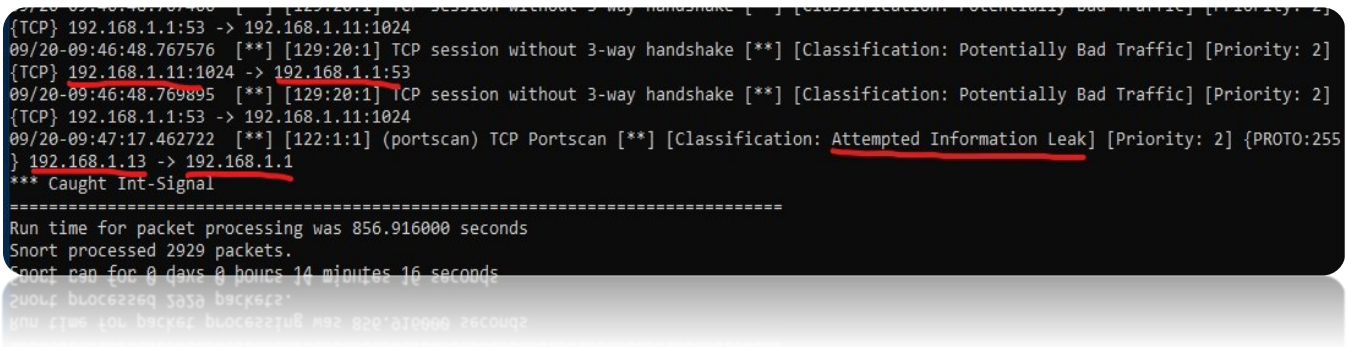


Figure 26 : capture d'écran de la requête venant de la machine virtuelle

Notre solution capte tout trafic dans le réseau donc il peut détecter tous les ransomwares qui cherchent d'abord leur clé à un serveur à l'extérieur du réseau ou essaient d'y copier les données. Et nous remarquons un type de requête venant de notre machine virtuelle d'adresse **192.168.1.13** qui est "**Attemped Information Leak**" ou une tentative de fuite d'information.

Nb : cette solution n'a pas pour but d'arrêter l'exécution des ransomwares mais de les détecter.

Conclusion :

La solution mise en place a été concluant car elle détecte effectivement les échantillons qui ont pour fonction d'établir une connexion avec un serveur externe afin de récupérer une clé de chiffrement ou de sauvegarder une copie des données de la victime.

Conclusion générale

Les pirates informatiques ont une avance considérable dans l'obstruction des systèmes informatiques. Leur limite n'est pas encore découverte et peut être qu'elle ne le sera jamais. Les seules connaissances se limitent aux logiciels dits **zero-day** qui ont été découverts.

C'est dans cette optique que les professionnels du monde de la sécurité informatique s'orientent vers de nouvelles méthodes qui ne dépendent ni de la signature des malwares ni d'une quelque autre caractéristique qui exige d'être connue au préalable.

Les nouvelles des méthodes sont basées sur le comportement des logiciels tels que la détermination des comportements normaux ou le machine Learning qui au fur et à mesure classifie les bons comportements des mauvais.
Les ransomwares comme son nom l'indique sont parmi les attaques les plus convoitées et les plus rentables de nos jours pour les cybercriminels. Et l'un des exemples les plus récents est l'attaque du **Colonial Pipeline** aux États-Unis d'Amérique.

Dans le but de mettre en place une méthode de détection des attaques par ransomware, notre travail consistait à la découverte des travaux existant et à élaborer une solution convenable. Nous nous sommes dirigés vers l'utilisation d'un IDS pour l'exécution de cet objectif. Notre choix s'est porté sur **l'IDS Snort** qui est l'un des plus utilisés dans le domaine et qui offre la possibilité de sniffer un réseau ou de détecter une attaque. Il surveille le
Trafic réseau et possède des plugins pour analyser les en-têtes des paquets.

A travers les thèses et travaux menés dans ce domaine, nous avons appris les multitudes de solutions proposées pour l'éradication des ransomwares. Et ce travail a été très bénéfique pour approfondir notre connaissance dans le domaine de la sécurité informatique.

Notre perspective est l'amélioration de cette solution afin de pouvoir détecter tout type de ransomwares et de bloquer leur exécution à temps.

Bibliographie

- **[1]** Renaud Dumont. *Cryptographie et sécurité informatique*. INFO0045-2. 2009-2010
- **[2]** MISINI Leutrim, **Étude des ransomware : Vecteur d'attaque, fonctionnement, économie et réponse légal ;**

- **[5]** A. O. Almashhadani, M. Kaiiali, S. Sezer and P. O'Kane, "**A Multi-Classifier Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware**," in IEEE Access, vol. 7, pp. 47053-47067, 2019, doi:10.1109/ACCESS.2019.2907485.

- **[6]** Sophos, Un livre blanc Mai 2020 << état des ransomwares 2020 >>;

- **[8]** S.-J. Lee, H.-Y. Shim, Y.-R. Lee, T.-R. Park, S.-H. Park et I. -G. Lee, "**Study on Systematic Ransomware Detection Techniques,**" 2021 23e Conférence internationale sur les technologies de communication avancées (ICACT), 2021, pp. 297-301, doi: 10.23919/ICACT51234.2021.9370472 ;

- **[9]** S. Sheen et A. Yadav, "**Ransomware detection by mining API call usage**," *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2018, pp. 983-987, doi: 10.1109/ICACCI.2018.8554938;

- **[10]** U. Urooj, M. Aizaini Bin Maarof et B. Ali Saleh Al-rimy, "**A proposé Adaptive Pre-Encryption Crypto-Ransomware Early Detection Model**," *2021 3rd International Cyber Resilience Conference (CRC)*, 2021, pp. 1-6, doi: 10.1109/CRC50527.2021.9392548;

- **[16]** NICOLAS ZIN. *OSSEC HOWTO THE QUICK AND DIRTY WAY*. REF: SLF-ED01. Page 9

- [18] Liran LERMAN. *LES SYSTEMES DE DETECTION D4INTRUSION BASES SUR DU MACHINE LEARNING*. Page 10

- [20] Michaël AMAND et Mohamed NSIRI. Rapport du projet tutoré. **Étude d'un système de détection d'intrusion comportemental pour l'analyse du trafic aéroportuaire.** Page 14

Webographie

- **[3] WannaCry** – Wikipedia , www.wikipedia.org ;

- **[4] kaspersky.fr, https://www.kaspersky.fr/resource-center/threats/ransomware-threats-an-in-depth-guide**

- **[7] Coessi.com : ransomware, comment les détecter** https://coessi.com/fr/news-technologie-20200604-ransomwares-comment-les-detecter--11.php#:~:text=%2D%20Une%20protection%20bas%C3%A9e%20sur%20l,d%C3%A9duit%20une%20activit%C3%A9%20de%20ransomware;

- **[11] Wikipédia .org, Système de détection d'intrusion,** https://fr.wikipedia.org/wiki/Syst%C3%A8me_de_d%C3%A9tection_d%27intrusion ;

- **[12] wikipedia.org, Principes et architecture des systèmes de détection d'intrusion,** https://fr.wikipedia.org/wiki/Principes_et_architecture_des_syst%C3%A8mes_de_d%C3%A9tection_d%27intrusion ;

- **[13] Juniper.net,** https://www.juniper.net/fr/fr/research-topics/what-is-ids-ips.html ;

- **[14] amazonaws.com, Les familles d'IDS,** https://shms-prod.s3.amazonaws.com/media/editor/143832/Types_of_IDS_Systems.pdf

- **[15]** igm.univ-mlv.fr**, IDS: Intrusion Detection Systems,**http://www-igm.univ-mlv.fr/~dr/XPOSE2004/IDS/IDSPres.html ;

- **[17] wikipedia.org,** https://fr.wikipedia.org/wiki/Bro_(IDS)

- **[19] github.com,** https://github.com/Endermanch/MalwareDatabase

Nb : les pages web ont été consultées entre Aout 2021 et septembre 2021.