MENACES SUR LA SECURITE DES DONNEES INFORMATIQUES DANS LES ORDINATEURS
(Enquête menée à Kindu de Mars à Décembre 2021)

OMOKENDE OTSHUDI Albert[1]

RESUME

Les menaces des données informatiques dans les ordinateurs sont bel et bien ressenties par les usagers des ordinateurs au sein des organisations tant publiques que privées.

Les types de menaces évoquées par nos enquêtés sont multiples et se manifestent dans des proportions différentes. Cependant, les virus représentent la menace la plus ressentie et ils représentent 36% des opinions de nos enquêtés.

Mots clés : Menaces, sécurité données, informatique, ordinateur.

ABSTRACT

The threats of computer data are well and truly felt by users working in both publics and privates organisations in Kindu.

The types of mentioned by our respondents are multiple and manifest themselves in different proportions. Howerver, viruses represent 36% of the opinions of our respondent.

Keywords: Threats, security, data, informatics, computeur

0. INTRODUCTION

L'adoption massive de systèmes informatiques multiples et variés dans les entreprises et dans les foyers a profondément changé les activités humaines exacerbant par là même les problématiques de sécurité. En effet, si auparavant le système d'information était cloisonné au sein des murs de l'entreprise et uniquement accessible aux employés au travers d'équipements propres à l'entreprise, la situation est bien différente aujourd'hui. Les entreprises s'allient pour répondre plus efficacement à des opportunités métier et donc désirent partager des ressources facilement mais de manière contrôlée. Les services informatiques se sont dématérialisés et externalisés. Les usages des employés ont aussi évolué. Le télétravail s'est développé et les employés veulent utiliser leurs équipements personnels pour accéder aux actifs de l'entreprise. En même temps l'informatique a pénétré les habitations domestiques[2].
D'un simple ordinateur connecté par le modem, le réseau domestique est aujourd'hui constitué d'une multitude d'équipements. Les objets du quotidien étant devenus de véritables ordinateurs, les contours même des réseaux informatiques domestiques ont aussi largement dépassé les murs des habitations. En parallèle, la vie des usagers s'est numérisée et les transactions électroniques se sont généralisées.

La Nouvelle Technologie de l'Information et de la Communication (NTIC) intègre le quotidien de la plupart des entreprises, organisations basées à Kindu. Elles permettent d'effectuer un travail en réseau et simplifient la communication. Le recours à ces nouvelles technologies est à l'origine de problèmes inconnus auparavant. Alors qu'auparavant on doutait de l'existence des virus informatiques, ils sont aujourd'hui répandus dans le monde entier et créent toutes sortes de menaces pour la sécurité informatique (Manuel Suter, 2006).

La criminalité sur Internet est apparue le jour où l'ordinateur a pris le relais du stylo et du papier. Son essor a été foudroyant dans le contexte de la globalisation des réseaux d'information.
La sécurité de donnés informatiques est donc une garantie d'authentification, de l'intégrité, de la confidentialité des informations d'une société à une autre. Mais malgré une assurance et garantie totale de données, celle-ci est

[1] Assistant à l'Institut Supérieur de Commerce de Kindu.
[2] Romain Laborde, *contribution à la gestion de la sécurité des infrastructures virtuelles,* Université de Toulouse 3 Paul Sabatier, 2016.

encore mal considérée, sous-exploitée dans la ville de Kindu par les acteurs du monde de la communication, du transfert de données et par ceux de la sphère informatique.
Spontanément, le premier facteur explicatif est que la question des outils sécuritaires demande une certaine information et formation, la veille sur l'actualisation, la bonne application régulière ainsi que la bonne gestion.

La sécurité informatique est de nos jours devenue un problème majeur dans la gestion des réseaux d'entreprises ainsi que pour les particuliers, toujours plus nombreux à se connecter à Internet. Ainsi, la transmission d'informations sensibles et le désir d'assurer la confidentialité de celles-ci est devenue un point primordial dans la mise en place de réseaux informatiques.

La sécurité d'un système informatique fait souvent l'objet de métaphores. En effet, on la compare régulièrement à une chaîne en expliquant que le niveau de sécurité d'un système ou d'une entreprise est caractérisé par le niveau de sécurité du maillon le plus faible. Ainsi, une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue (Suter, *Op. cit.*, 2006). Cela signifie que la sécurité doit être abordée dans un contexte global et notamment prendre en compte les aspects techniques ou organisationnels.

Dans le cadre de la présente recherche, nous nous intéressons exclusivement l'identification et l'analyse des menaces qui dérangent la sécurité des informations dans les ordinateurs à Kindu. De ces préoccupations découlent les questions suivantes :

1) Quelles sont les principaux types de menaces qui affectent la sécurité des données informatiques dans les ordinateurs à travers la ville de Kindu ?
2) Ces menacent se manifestent-elles dans les mêmes proportions ?

Faisant face à plusieurs menaces de sécurité informatique, les investigations menées dans les organisations tant publiques que privées de la place nous ont permis de répondre provisoirement aux questions posées ci-haut en ces termes :

1) Les principaux types de types de menaces qui affectent la sécurité des données informatiques dans les ordinateurs sont, entre autres : les Virus, les Espiogiciel (spayware), les Chevaux de Troie, l'Attaque par déni de service, les Intrusion dans le système (hacking) et vol de données, la Défiguration de site les Abus des réseaux sans fil,
2) Ces menaces ne se manifestent pas dans les mêmes proportions.

Ces deux réponses provisoires sont les hypothèses que nous avons tenté de vérifier à travers cette recherche, nos objectifs étant :

1) d'identifier les principaux types de menaces qui affectent la sécurité des données informatiques dans les ordinateurs utilisés au sein des organisations tant publiques que privées à travers la ville de Kindu.
2) D'évaluer, en termes de pourcentages les opinions des usagers des ordinateurs à travers la ville de Kindu sur la manifestation de chacune des menaces identifiées.

Vu aussi la multiplicité des ordinateurs dans la ville, l'apparition de beaucoup d'entreprises et institutions traitant les données avec l'ordinateur, de nombreux centres informatiques, l'utilisation aveugle et inconsciente des outils de sécurité et même l'ignorance des outils de la bonne sécurité de données informatiques nous ont intéressés de mener une étude afin de maintenir dans le bon sens le niveau de compréhension d'infection et de la bonne maitrise de notion de sécurités de ceux-ci ; raison pour laquelle les données relevant de ce travail serviront même à sa connaissance élémentaire aux utilisateurs et informaticiens à bien maintenir une sécurité et à bien gérer les outils informatiques qui les épargneraient désormais aux pertes des données dans les ordinateurs.

Un travail qui se veut scientifique exige à tout chercheur l'usage des méthodes et techniques qui peuvent lui permettre d'atteindre l'objectif qu'il s'est assigne. C'est ainsi que pour atteindre nos objectifs et vérifier les hypothèses que nous nous sommes fixées, nous avons recouru à une méthode, appuyée par une technique pour la collecte des données et une autre pour leur traitement.

Selon Pinto et Grawitz (2000, p.49), la méthode est l'ensemble d'opérations intellectuelles par lesquelles une discipline cherche à atteindre les vérités qu'elle poursuit, les démontre et les vérifie. Tandis que les techniques sont des outils mis à la disposition du chercheur pour lui permettre de bien mener ses études.
Une technique est un ensemble des procédés mis en œuvre dans le but d'obtenir un résultat bien déterminé à l'avance. Une technique est aussi un rassemblement des procédés propres à un art (Petit Larousse 2009). C'est pourquoi, l'étude sur la sécurité de données informatiques nécessite les méthodes de recherche et des différentes techniques.

En ce qui concerne la présente recherche, nous avons recouru à la méthode inductive, car les résultats tirés de cet échantillon ont été généralisés à toute la population.

La collecte de nos données a nécessité l'élaboration d'un questionnaire, que nous avons administré aux utilisateurs des ordinateurs dans les organisations tant publiques que privées opérationnelles à Kindu, qui forment la population à travers laquelle nous avons tiré notre échantillon, dont la taille est 50.

La statistique nous a permis de traiter les données issues du dépouillement de nos protocoles d'enquête dans un tableau indiquant les différentes menaces évoquées, leurs effectifs et leurs pourcentages respectifs.

Tout travail scientifique doit être délimité thématiquement, dans l'espace et dans le temps. La présente étude n'a pas fait exception à cette règle, c'est ainsi que, thématiquement, nos investigations portent les menaces sur la sécurité des données informatiques dans les ordinateurs.

La ville de Kindu est la délimitation spatiale de cette étude ; alors que dans le temps, elle correspond à la période pendant laquelle nos enquêtes ont eu lieu sur terrain (de mars à décembre 2021).

La présente recherche est subdivisée en trois parties, hormis l'introduction et la conclusion. Ces différents chapitres, à savoir : les généralités sur les types de menaces qui affectent la sécurité des données informatiques, la présentation du milieu d'étude et la présentation, l'analyse et les résultats interprétés à la lumière de nos objectifs fixés.

Comme il n'y a pas de rose sans épines, dit-on, nous avons été buté à des difficultés d'ordres multiples. Cependant, nous avons retenu les deux qui nous ont semblé être les plus importantes. Il s'agit de la réticence de certains usagers des ordinateurs dans les organisations tant publiques que privées à répondre à notre questionnaire d'enquête, d'une part, réduisant ainsi la taille de notre échantillon à 50 enquêtés. Et la remise tardive des protocoles d'enquêtes pour des motifs qui leurs sont propres, d'autre part.

I. GENERALITES SUR LES TYPES DE MENACES SUR LA SECURITE DES DONNEES INFORMATIQUES DANS LES ORDINATEURS

La sécurité des données informatiques, est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mise en place pour conserver, rétablir et garantir la sécurité du système d'information.

A. ENJEUX DE LA SECURITE DES DONNEES

Assurer la sécurité du système d'information est une activité du management du système d'information.
Le système d'information représente un patrimoine essentiel de l'organisation, qu'il convient de protéger. La sécurité informatique consiste à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. Plusieurs enjeux se présentent comme suit :

1. L'Intégrité : les données doivent être celles que l'on s'attend à ce qu'elles soient, et ne doivent pas être altérées de façon fortuite ou volontaire.
2. La confidentialité : seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché ;
3. La disponibilité : le système doit fonctionner sans faille durant les plages d'utilisation prévues, garantir l'accès aux services et ressources installées avec le temps de réponse attendu.
4. La non répudiation et l'imputation ; aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur
5. L'authentification : l'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

La sécurité informatique est un défi d'ensemble qui concerne une chaine d'éléments : les infrastructures matérielles de traitement ou de communication, les logiciels (systèmes d'exploitation ou applicatifs), les données, le comportement des utilisateurs. Le niveau global de sécurité étant défini par le niveau de sécurité du maillon le plus faible, les précautions et contre-mesures doivent être envisagées en fonction des vulnérabilités propres au contexte auquel le système d'information est censé apporter service et appui.

B. OBJECTIF DE LA SECURITE DES DONNEES

Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise permettant de les stocker ou de les faire circuler. Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger. La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

I.1. LES VIRUS

Le terme de virus informatique, né en 1984, est désormais bien connu du grand public. L'informatique, omniprésente dans le milieu professionnel et, de plus en plus, dans les foyers, l'utilisation d'internet et plus généralement des réseaux ont confronté, au moins une fois, une importante majorité des utilisateurs au risque viral. Cependant, il s'avère que dans les faits, la connaissance de ces derniers (au sens le plus large du terme) en matière de virologie informatique présente encore beaucoup de lacunes, au point d'augmenter les risques plutôt que de les diminuer. Le terme de virus, lui-même, est en fait improprement utilisé pour désigner une classe plus générale de programmes qui n'ont rien à voir avec les virus : vers, chevaux de Troie, bombe logique, leurres… Les virus, de plus, recouvrent une réalité bien plus complexe qu'il n'y paraît. De nombreuses sous-catégories existent, de nombreuses techniques virales s'y rapportent, toutes impliquant des risques différents, qui doivent être connus en vue d'une protection et d'une lutte efficaces.

En informatique, un « Virus » est un logiciel malveillant qui se propage en se cachant dans d'autres logiciels. On appelle virus, tout programme d'ordinateur capable d'infecter un autre programme d'ordinateur en le modifiant de façon à ce qu'il puisse à son tour se reproduire. Lorsque le logiciel infecté est activé, le virus s'active aussi. Il tente alors de se multiplier et commence son travail de destruction dans l'ordinateur infecté. Et à la suite modifie ou supprime des données dans l'ordinateur infecté et aussi provoque une panne matérielle non réparable (destruction de l'ordinateur), ralentissement ou bloque l'ordinateur infecté (le virus occupant toute la capacité de travail du PC), provoque l'extinction de l'ordinateur à l'intervalle régulier.

Afin d'illustrer l'importance du risque viral, Eric FILIOL (2008) le résume par quelques chiffres particulièrement pertinents : le ver I Love You a infecté en 1999 plus de 45 millions d'ordinateurs dans le monde. Plus récemment, le ver Sapphire/Slammer a infecté plus de 75000 serveurs sur toute la planète, en dix minutes environ. Le virus CIH dit Chernobyl a obligé des milliers d'utilisateurs, en 1998, à changer la carte mère de leur ordinateur après avoir détruit le programme BIOS.

Le même auteur nous a révélé que les dégâts provoqués par ces virus sont estimés à près de 250 millions d'euros pour la seule Corée du Sud tandis que ce chiffre atteint plusieurs milliards d'euros pour un ver informatique. La menace représentée par les BotNets depuis 2002-2003 concerne, selon le FBI, un ordinateur sur quatre dans le monde, soit près de deux cent millions de machines infectées à l'insu de leurs propriétaires. Enfin, l'attaque Storm Worm, durant l'été 2007, a frappé en moins d'un mois plus de 10 millions de machines à travers le monde. Ces chiffres montrent avec force l'importance d'une prise en compte sérieuse de la menace virale.

I.1.1. Types de virus

En effet, il existe de nombreux types de virus selon les systèmes d'exploitation et les données informatiques ; ceci ne veut pas dire que chaque Système d'exploitation a un type de virus, néanmoins la facilité de multiplication de virus dans un système d'exploitation et dans une certaine donnée informatique.

- **Les Virus Mutants (**virus ayant été réécrits par d'autres utilisateurs afin d'en modifier leur comportement ou leur signature)
- **Les virus polymorphes** (mot provenant du grec signifiant «*qui peut prendre plusieurs formes*»).
- **Les Rétrovirus** « virus flibustier » (en anglais *bounty hunter*) un virus ayant la capacité de modifier les signatures de l'antivirus afin de les rendre inopérants.
- **Les virus de secteur d'amorçage** (ou *virus de boot*), un virus capable d'infecter le secteur de démarrage d'un disque dur.
- **virus BadTrans :** Le virus BadTrans est un ver se propageant à l'aide du courrier électronique. Il exploite également un autre mode de propagation : **C'est quoi un Hoax ?** On appelle **hoax** (en français *canular*) un courrier électronique propageant une fausse information et poussant le destinataire à diffuser la fausse nouvelle à tous ses proches ou collègues.

Ainsi, de plus en plus de personnes font suivre des informations reçues par courriel sans vérifier la véracité des propos qui y sont contenus. Le but des hoax est simple :

- Provoquer la satisfaction de son concepteur d'avoir berné un grand nombre de personnes
- Les conséquences de ces canulars sont multiples :
- L'**engorgement des réseaux** en provoquant une masse de données superflues circulant dans les infrastructures réseaux ;
- Une **désinformation**, c'est-à-dire faire admettre à de nombreuses personnes de faux concepts ou véhiculer de fausses rumeurs (on parle de *légendes urbaines*) ;
- L'**encombrement des boîtes aux lettres électroniques** déjà chargées ;
- La **perte de temps**, tant pour ceux qui lisent l'information, que pour ceux qui la relayent ;
- La **dégradation de l'image** d'une personne ou bien d'une entreprise ;
- L'**incrédulité** : à force de recevoir de fausses alertes les usagers du réseau risquent de ne plus croire aux vraies.

Ainsi, il est essentiel de suivre certains principes avant de faire circuler une information sur Internet.

I.1.2. Détection des virus

Les virus se reproduisent en infectant des « *applications hôtes* », c'est-à-dire en copiant une portion de code exécutable au sein d'un programme existant. Or, afin de ne pas avoir un fonctionnement chaotique, les virus sont programmés pour ne pas infecter plusieurs fois un même fichier. Ils intègrent ainsi dans l'application infectée une suite d'octets leur permettant de vérifier si le programme a préalablement été infecté : il s'agit de la **signature virale (**www.securited'information.co, page consultée le 25 février 2021).

Les antivirus s'appuient ainsi sur cette signature propre à chaque virus pour les détecter. Il s'agit de la méthode de **recherche de signature** (*scanning*), la plus ancienne méthode utilisée par l'antivirus. Cette méthode n'est fiable que si l'antivirus possède une base virale à jour, c'est-à-dire comportant les signatures de tous les virus connus. Toutefois cette méthode ne permet pas la détection des virus n'ayant pas encore été répertoriés par les éditeurs d'antivirus. De plus, les programmeurs de virus les ont désormais dotés de capacités de camouflage, de manière à rendre leur signature difficile à détecter, voire indétectable : il s'agit de "**virus polymorphes**"(www.css.ethz.ch, page consultée le 25 février 2021).

Certains antivirus utilisent un **contrôleur d'intégrité** pour vérifier si les fichiers ont été modifiés. Ainsi le contrôleur d'intégrité construit une base de données contenant des informations sur les fichiers exécutables du système (date de modification, taille et éventuellement une somme de contrôle). Ainsi, lorsqu'un fichier exécutable change de caractéristiques, l'antivirus prévient l'utilisateur de la machine.
La méthode heuristique consiste à analyser le comportement des applications afin de détecter une activité proche de celle d'un virus connu. Ce type d'antivirus peut ainsi détecter des virus même lorsque la base antivirale n'a pas été mise à jour. En contrepartie, ils sont susceptibles de déclencher de fausses alertes.

I.2. LES VERS

Un **ver informatique** (en anglais *worm*) est un programme qui peut s'auto-reproduire et se déplacer à travers un réseau en utilisant les mécanismes réseau, sans avoir réellement besoin d'un support physique ou logique (disque dur, programme hôte, fichier, etc.) pour se propager; un ver est donc **un virus réseau**.

I.2.1. Le fonctionnement d'un ver dans les années 80

La plus célèbre anecdote à propos des vers date de 1988. Un étudiant (Robert T. Morris, de Cornell University cité par Mbole, 2019) avait fabriqué un programme capable de se propager sur un réseau, il le lança et, 8 heures après l'avoir lâché, celui-ci avait déjà infecté plusieurs milliers d'ordinateurs. C'est ainsi que de nombreux ordinateurs sont tombés en pannes en quelques heures car le « ver » (car c'est bien d'un ver dont il s'agissait) se reproduisait trop vite pour qu'il puisse être effacé sur le réseau. De plus, tous ces vers ont créé une saturation au niveau de la bande passante, ce qui a obligé la NSA à arrêter les connexions pendant une journée (Suter, 2006, p.7).
Voici la manière dont le ver de Morris se propageait sur le réseau :

- Le ver s'introduisait sur une machine de type UNIX ;
- Il dressait une liste des machines connectées à celle-ci ;
- Il forçait les mots de passe à partir d'une liste de mots ;
- Il se faisait passer pour un utilisateur auprès des autres machines ;
- Il créait un petit programme sur la machine pour pouvoir se reproduire ;

- Il se dissimulait sur la machine infectée ;
- Et ainsi de suite.

I.2.2. Les vers actuels

Les vers actuels se propagent principalement grâce à la messagerie (et notamment par le client de messagerie *Outlook*) grâce à des fichiers attachés contenant des instructions permettant de récupérer l'ensemble des adresses de courrier contenues dans le carnet d'adresse et en envoyant des copies d'eux-mêmes à tous ces destinataires (Suter, Op. cit., p.6).
Ces vers sont la plupart du temps des scripts (généralement VB Script) ou des fichiers exécutables envoyés en pièce jointe et se déclenchant lorsque l'utilisateur destinataire clique sur le fichier attaché.

I.3. LES CHEVAUX DE TROIE

On appelle « **Cheval de Troie** » (en anglais *trojan horse*) un programme informatique effectuant des opérations malicieuses à l'insu de l'utilisateur. Le nom « Cheval de Troie » provient d'une légende narrée dans l'*Iliade* (de l'écrivain *Homère*) à propos du siège de la ville de Troie par les Grecs.
La légende veut que les Grecs, n'arrivant pas à pénétrer dans les fortifications de la ville, aient l'idée de donner en cadeau un énorme cheval de bois en offrande à la ville en abandonnant le siège.

Les troyens (peuple de la ville de Troie), apprécièrent cette offrande à priori inoffensive et la ramenèrent dans les murs de la ville. Cependant le cheval était rempli de soldats cachés qui s'empressèrent d'en sortir à la tombée de la nuit, alors que la ville entière était endormie, pour ouvrir les portes de la cité et en donner l'accès au reste de l'armée…

Un cheval de Troie (informatique) est donc un programme caché dans un autre qui exécute des commandes sournoises, et qui généralement donne un accès à l'ordinateur sur lequel il est exécuté en ouvrant une **porte dérobée** (en anglais *backdoor*), par extension il est parfois nommé **troyen** par analogie avec les habitants de la ville de Troie.

A la façon du virus, le cheval de Troie est un code (programme) nuisible placé dans un programme sain (imaginez une fausse commande de listage des fichiers, qui détruit les fichiers au-lieu d'en afficher la liste).
Un cheval de Troie peut par exemple :

- Voler des mots de passe ;
- Copier des données sensibles ;
- Exécuter tout autre action nuisible ;
- Etc.

Pire, un tel programme peut créer, de l'intérieur de votre réseau, une brèche volontaire dans la sécurité pour autoriser des accès à des parties protégées du réseau à des personnes se connectant de l'extérieur.
Les principaux chevaux de Troie sont des programmes ouvrant des ports de la machine, c'est-à-dire permettant à son concepteur de s'introduire sur votre machine par le réseau en ouvrant une **porte dérobée**. C'est la raison pour laquelle on parle généralement de *backdoor* (littéralement *porte de derrière*) ou de backorifice (terme imagé vulgaire signifiant "*orifice de derrière*").

Un cheval de Troie n'est pas nécessairement un virus, dans la mesure où son but n'est pas de se reproduire pour infecter d'autres machines. Par contre certains virus peuvent également être des chevaux de Troie, c'est-à-dire se propager comme un virus et ouvrir un port sur les machines infectées (www.scoci.ch, Page consultée le 26 mars 2020).

I.4. LES BOMBES LOGIQUES

Sont appelés bombes logiques les dispositifs programmés dont le déclenchement s'effectue à un moment déterminé en exploitant la date du système, le lancement d'une commande, ou n'importe quel appel au système.
Ainsi ce type de virus est capable de s'activer à un moment précis sur un grand nombre de machines (on parle alors de *bombe à retardement* ou de *bombe temporelle*). Les bombes logiques sont généralement utilisées dans le but de créer un déni de service en saturant les connexions réseau d'un site, d'un service en ligne ou d'une entrepris.

I.5. LES ESPIOGICIELS

Un **espiogiciel** (en anglais **spyware**) est un programme chargé de recueillir des informations sur l'utilisateur de l'ordinateur sur lequel il est installé (on l'appelle donc parfois *mouchard*) afin de les envoyer à la société qui le diffuse pour lui permettre de dresser le profil des internautes (on parle de *profilage*).
Les récoltes d'informations peuvent ainsi être :

- La traçabilité des URL des sites visités ;
- Le traquage des mots-clés saisis dans les moteurs de recherche ;
- L'analyse des achats réalisés via internet ;
- Voire les informations de paiement bancaire (numéro de carte bleue / VISA) ;
- Ou bien des informations personnelles.

Les spywares s'installent généralement en même temps que d'autres logiciels (la plupart du temps des freewares ou sharewares). En effet, cela permet aux auteurs des dits logiciels de rentabiliser leur programme, par de la vente d'informations statistiques, et ainsi permettre de distribuer leur logiciel gratuitement. Il s'agit donc d'un modèle économique dans lequel la gratuité est obtenue contre la cession de données à caractère personnel.

Les spywares ne sont pas forcément illégaux car la licence d'utilisation du logiciel qu'ils accompagnent précise que ce programme tiers va être installé ! En revanche étant donné que la longue licence d'utilisation est rarement lue en entier par les utilisateurs, ceux-ci savent très rarement qu'un tel logiciel effectue ce profilage dans leur dos.

Par ailleurs, outre le préjudice causé par la divulgation d'informations à caractère personnel, les spywares peuvent également être une source de nuisances diverses :

- Consommation de mémoire vive ;
- Utilisation d'espace disque ;
- Mobilisation des ressources du processeur ;
- Plantages d'autres applications ;
- Gêne ergonomique (par exemple l'ouverture d'écrans publicitaires ciblés en fonction des données collectées).

On distingue généralement deux types de spywares :

- Les **spywares internes** (ou *spywares internes* ou *spywares intégrés*) comportant directement des lignes de codes dédiées aux fonctions de collecte de données.
- Les **spywares externes**, programmes de collectes autonomes installés Voici une liste non exhaustive de spywares non intégrés :
  Alexa, Aureate/Radiate, BargainBuddy, ClickTillUWin, Conducent Timesink, Cydoor, Comet Cursor, Doubleclick, DSSAgent, EverAd, eZula/KaZaa Toptext, Flashpoint/Flashtrack, Flyswat, Gator / Claria, GoHip, Hotbar, ISTbar, Lop, NewDotNet, Realplayer, SaveNow, Songspy, Xupiter, Web3000 et WebHancer

II.6. LES KEYLOGGERS

Un **keylogger** (littéralement *enregistreur de touches*) est un dispositif chargé d'enregistrer les frappes de touches du clavier et de les enregistrer, à l'insu de l'utilisateur. Il s'agit donc d'un dispositif d'espionnage.
Certains keyloggers sont capables d'enregistrer les URL visitées, les courriers électroniques consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute l'activité de l'ordinateur !

Dans la mesure où les keyloggers enregistrent toutes les frappes de clavier, ils peuvent servir à des personnes malintentionnées pour récupérer les mots de passe des utilisateurs du poste de travail ! Cela signifie donc qu'il faut être particulièrement vigilant lorsque vous utilisez un ordinateur en lequel vous ne pouvez pas avoir confiance (poste en libre accès dans une entreprise, une école ou un lieu public tel qu'un cybercafé).
Keyloggers : logiciel ou matériel

Les keyloggers peuvent être soit logiciels soient matériels. Dans le premier cas il s'agit d'un processus furtif (ou bien portant un nom ressemblant fortement au nom d'un processus système), écrivant les

informations captées dans un fichier caché ! Les keyloggers peuvent également être matériel : il s'agit alors d'un dispositif (câble ou dongle) intercalé entre la prise clavier de l'ordinateur et le clavier.

II. PRESENTATION DU MILIEU D'ETUDE

Kindu, anciennement kindu-Port-Empain (d'après le nom du baron Edouardn Louis Joseph Empain), est une ville de la République Démocratique du Congo, capitale de la province du Maniema. Elle se situe au Nord de Kasongo et à l'Ouest de la ville de Baraka.

II.1. COORDONNEES GEOGRAPHIQUES

La ville de Kindu est située sur les rives du fleuve Congo à 2°57'Sud, 25° 55'Est sur les élévations approximatives de 450 mètres, elle est desservie par la route RP508 à 1.820 kilomètres à l'Est de la capitale Kinshasa.

II.2. HISTOIRE

La ville de Kindu est composée d'une population hétérogène comprenant les Bantous, les Mongos, les Basonges… Ces populations ont envahi la ville à la suite des mouvements migratoires qu'a connu la province du Maniema au XVe siècle. Vers 1860, les commerçants arabes-swahilis s'installent dans la ville et y apportent ainsi leur culture. Le 5 décembre 1876, Henri Merton Stanley arrive dans la ville et la décrit comme étant remarquablement longue avec une large rue de trente pieds de large et deux milles de longueur, et derrière la ville de bananes et des palmiers.

La mission est ouverte par les Pères du Saint-Esprit qui font construire une église, puis une école tenue par les filles de la Croix.

II.3. ADMINISTRATION

Chef-lieu provincial de 148.086 électeurs enrôlés pour les élections de 2018, elle a le statut de ville constituée de trois communes urbaines de moins de 80.000 électeurs :

- Alunguli (29.176 électeurs, 7 conseillers municipaux) ;
- Kasuku, (63.207 électeurs, 7 conseillers municipaux) ;
- Mikelenge, (55.703 électeurs, 7 conseillers municipaux).

III. RESULTATS

La question à laquelle tout nos enquêtés ont répondus est la suivante :
Parmi les principaux types de menaces sur la sécurité des données informatiques énumérées ci-dessous, encerclez celle qui est la plus fréquente dans les machines utilisées au sein de votre organisation (publique ou privée) :

1. Les virus
2. Les vers
3. Les chevaux de troie
4. Les bombes logiques
5. Les espiogiciels
6. Les keyloggers

Nous présentons à travers le tableau qui suit les résultats issus du dépouillement de notre questionnaire d'enquête ; notamment les opinions de nos enquêtés sur les types de menaces sur la sécurité des données informatiques dans les ordinateurs.

Tableau n°1 : Opinions de nos enquêtés sur les types de menaces sur la sécurité des données informatiques dans les ordinateurs utilisés par leurs organisations

MENACES	Fréquences	Pourcentages
Les virus	18	36
Les vers	10	20
Les chevaux de troie	5	10
Les bombes logiques	6	12
Les espiogiels	4	8
Les keyloggers	7	14
Autres	0	0
Total	**50**	**100%**

Source : nos protocoles d'enquête et nos propres calculs.

Il ressort des résultats présentés au tableau ci-haut que les principaux types de menaces qui affectent la sécurité des donnes informatiques dans les ordinateurs à travers la ville de Kindu sont : les virus (opinion exprimée par 36% de nos enquêtés), les vers (opinion exprimée par 20% de nos enquêtés), les chevaux de troie (opinion exprimée par 10% de nos enquêtés), les bombes logiques (opinion exprimée par 12% de nos enquêtés), les espiogiels (opinion exprimée par 8% de nos enquêtés) et les keyloggers (opinion exprimée par 14% de nos enquêtés).

CONCLUSION

Au terme de cette recherche intitulée : menaces des données informatiques dans les ordinateurs (enquête menée à Kindu de Mars à Décembre 2021), nous nous permettons de confirmer que ces menaces sont bel et bien ressenties par les usagers des ordinateurs au sein des organisations tant publiques que privées.

Les types de menaces évoquées par nos enquêtés sont principalement : Les virus, les vers, les chevaux de troie, les bombes logiques, les espiogiciels et les keyloggers. Ces menaces se manifestent dans des proportions différentes ; cependant, les virus représentent la menace la plus ressentie, car ils représentent 36% des opinions de nos enquêtés.

Nous avons atteint nos objectifs parce que, d'une part, nous avons réussi à identifier les principaux types de menaces qui affectent la sécurité des données informatiques dans les ordinateurs utilisés au sein des organisations tant publiques que privées à travers la ville de Kindu ; et à évaluer en termes de pourcentages les opinions des usagers des ordinateurs à travers la ville de Kindu sur la manifestation de chacune des menaces identifiées, d'autre part.
Il ressort de ces résultats que celle la première hypothèse est confirmée.

REFERENCES

- Eric FILIOL, Virus informatiques*, in Laboratoire de virologie et de cryptologie de l'Ecole Supérieure d'Application des Transmissions à Rennes,* 2008.
- Manuel Suter (2006). S*écurité informatiques dans les entreprises suisse*. sl : se.
- Mbole, M. (2019). Problématique des virus dans les ordinateurs à travers la ville de Kisangani. In Mwalimu wetu. Kisangani : ISP/Kis.
- Pinto, R. et Grawitz, M. (2000) Méthodes de recherche en sciences sociales. Paris : Dalloz.
- Romain Laborde, *contribution à la gestion de la sécurité des infrastructures virtuelles,* Université de Toulouse 3 Paul Sabatier, 2016.
- Petit Larousse 2009
- www.securited'information.com.
- www.css.ethz.ch.
- www.scoci.ch.