REVUE DE L'U.KA

Volume 10, n. 20 (décembre 2022)

A l'ère du numérique

Université Notre-Dame du Kasayi
KANANGA

Les liens malicieux et leurs effets néfastes chez les internautes

Bernard KABUATILA KABUATILA
Assistant à l'Université Notre-Dame du Kasayi (U.KA)

Introduction

Les menaces provenant de l'Internet comme : *Spam, virus, spyware, pharming* ou autres chevaux de Troie, sont toujours plus nombreuses et insidieuses. Si certaines de ces attaques informatiques existent depuis plusieurs années déjà, les motivations qui les engendrent sont aujourd'hui bien différentes et par là même beaucoup plus pernicieuses et difficiles à contrer. Le piratage informatique était auparavant réalisé pour la gloire. Actuellement, il s'agit surtout de se faire de l'argent, ternir l'image d'une personne, faire du *buzz*, etc. Les pirates sont déterminés à rançonner l'argent de leurs victimes. Pour ce faire, les *hackers* appartiennent désormais à des bandes de crime organisé pour le compte desquelles ils mettent en place des attaques visant à faire de l'argent facilement et avec moins de dangers que le trafic de drogue ou la prostitution[1].

Généralement, les attaques sont discrètes, et le pirate ne veut surtout pas se faire repérer. C'est la genèse de la nouvelle technique d'attaque sur internet utilisant les liens malicieux comme outils. Par exemple un lien de type phishing peut très bien ne durer que deux heures, laissant le temps au pirate de récupérer quelques données utiles, tout en l'assurant de ne pas se faire repérer. Or jadis, les attaques étaient massives et destinées à faire le maximum de dégâts dans le maximum de réseaux possibles. « *I Love You* » constitue un bon exemple de virus destiné à affecter le plus grand nombre[2].

Les liens malicieux qui font l'objet de notre étude constituent l'ensemble des attaques permettant aux cybercriminels de prendre le contrôle

1 J. STERN, *La Science du secret*, Paris, Odile Jacob, 2011, p. 23.
2 https://www.cisco.com/web/FR/documents/pdfs/solutions/borderless/doc1_internet_threats.pdf, consulté le 13/04/2022.

des périphériques des internautes (Ordinateur, tablette, smartphone, etc.) connectés à l'Internet. *Phishing, spyware* et attaques de redirection de messages d'erreur en sont des exemples. Toutes ces attaques et menaces prennent désormais pour cible tout internaute non avisé qui tombe dans lepiège de cliquer sur n'importe quel lien qu'il reçoit sur la toile mondiale.

N'étant pas le premier à aborder ce thème, nous nous sommes référés à certains chercheurs qui nous ont précédés dans ce domaine[3]. La différence réside en ce que les études menées par nos prédécesseurs se limitaient à l'approche théorique, mais la nôtre va partir de l'approche théorique en passant par un scenario de déroulement de ce type d'attaque, pour chuter sur les recommandations à observer afin de se protéger de ces menaces sur la toile mondiale.

Cela étant, notre étude comprendra trois parties. Alors que la première et la deuxième se pencheront respectivement sur le contour théorique et le déroulement d'une attaque par lien malicieux, la troisième partie portera sur comment se protéger contre les liens malicieux.

1. Contour théorique

Dans le monde numérique actuellement, même le système de sécurité le plus complet peut être mis en échec si on réussit à déjouer son gardien. Les attaques sur la toile mondiale deviennent une monnaie courante, les cybercriminels formalisent les liens à apparence légitime comprenant un lien malveillant vers un site Web connu comme Facebook, Amazon, etc. En cliquant sur le lien, les victimes sont dirigées vers un faux site Web identique au site original où elles sont encouragées à confirmer ou à mettre à jour les informations de leur compte. Cette montée en puissance des cyberattaques nous oblige à informer notre entourage sur les risques qui y sont liés et les moyens de prévention.

1.1. Terminologies

1.1.1. L'attaque

L'attaque informatique se présente comme toute action qui vise à nuire au système informatique[4]. C'est une action volontaire et malveillante menée au moyen d'un réseau informatique visant à causer un dommage aux informations et aux personnes qui les traitent

3 Ch. DAISAY, *Phishing : le Puy du Fou victime d'une arnaque* ; R. ONGEMBA YALLO, *Passe sanitaire. Attention à ce faux mail de la police, c'est une arnaque*.

4 P. ATELIN, *Cryptographie Moderne*, Bruxelles, ENI, 2014, p. 69.

(particuliers, entreprises, hôpitaux, institutions...). Une attaque peut être le fait d›une seule personne (*hacker*), d'un groupe de pirates, d'un État ou d'une organisation criminelle. Les attaques sont facilitées par la quantité croissante d'informations mises en ligne (*cloud*) et par des failles de sécurité dans les systèmes.

1.1.2. Le maliciel

Un logiciel malveillant ou maliciel aussi dénommé logiciel nuisible ou programme malveillant ou pourriciel est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté. De nos jours, le terme « virus » est souvent employé, à tort, pour désigner toutes sortes de logiciels malveillants. En effet, les maliciels englobent les virus, les vers, les chevaux de Troie, ainsi que d'autres menaces.

1.1.3. La cyberattaque

Une cyberattaque est tout type d'action offensive qui vise des systèmes, des infrastructures ou des réseaux informatiques, ou encore des ordinateurs personnels, en s'appuyant sur diverses méthodes pour voler, modifier ou détruire des données ou des systèmes informatiques[5].

1.1.4. Le cybercrime

Un cybercrime est une « infraction pénale susceptible de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau ». Il s'agit donc d'une nouvelle forme de criminalité et de délinquance qui se distingue des formes traditionnelles en ce qu'elle se situe dans un espace virtuel, le « cyberespace ». Depuis quelques années la démocratisation de l'accès à l'informatique et la globalisation des réseaux ont été des facteurs de développement du cybercrime[6].

1.1.5. La cybercriminalité

La cybercriminalité est une activité criminelle qui cible ou utilise un ordinateur, un réseau informatique ou un appareil mis en réseau. Elle se définit aussi comme toute activité criminelle réalisée au travers du cyberespace et par le réseau Internet. Par extension, elle intègre toute

5 O. SALEM, *La protection des réseaux contre les attaques*, Paris, 3è éd., Eyrolles, 2012, p. 79.

6 R. ANDERSON, *Security Engineering : A Guide to Building Dependable Distributed Systems*, London, 2è éd., Wiley, 2018, p. 25.

forme de malveillance électronique effectuée à l'aide des technologies informatiques et de télécommunication (téléphonie, cartes à puces…). Qu'il s'agisse de fraude, d'escroquerie, d'extorsion, de vandalisme ou de harcèlement, les comportements malveillants ou criminels exploitent les caractéristiques d'Internet et portent préjudice aux internautes, aux organisations et à la société.

1.2. Les liens malicieux

Les liens malicieux se présentent comme l'ensemble de liens hypertexte conçus par les cybercriminels afin d'infiltrer un ordinateur et des appareils mobiles, d'y effectuer des activités non autorisées et de voler ainsi les renseignements personnels. Un seul clic sur ce lien, un seul URL pirate, suffisent pour que l'ordinateur ou le smartphone soit infecté, le mot de passe exposé, les données bloquées ou volées. Ainsi cette partie de notre réflexion étalera quelques types de ces attaques[7].

1.2.1. Le canular informatique

Un canular informatique (en anglais : *hoax*) est un contenu produit en ligne ou hors ligne par une personne puis divulgué à d'autres personnes au moyen d'un hyperlien, d'un courriel ou d'une lettre-chaîne[8]. À la différence des spams, qui sont la plupart du temps envoyés de manière automatisée à une liste de destinataires, ces types de messages sont relayés « manuellement » par des personnes de bonne foi à qui on demande de renvoyer le message à toutes leurs connaissances, ou à une adresse de courrier électronique bien précise ce qui inonde le serveur avec le réseau et des requêtes inutiles et rend le trafic réseau lent. Ce type de lien est trop fréquent sur les réseaux sociaux ; la figure suivante illustre un exemple de canular informatique relayé sur facebook messenger demandant à chaque internaute de partager le message avec 50 amis de sa liste. La question que chaque internaute devrait se poser c'est de connaitre l'origine du message mais malheureusement comme on cite Dieu dans l'attaque, les internautes se contentent de partager oubliant que ce message cacherait une attaque de saturation du réseau.

7 U. MARTIN, *Initiation au cybercrime*, London, Wiley, 2014, p. 46.
8 R. KAUFFER, *Histoire mondiale des services secrets*, Paris, Eyrolles, 2018, p. 22.

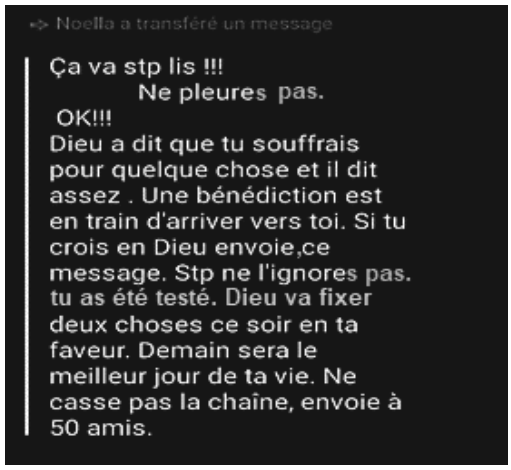


Fig. 1. Le canular informatique

1.2.2. L'appâtage

C'est un type de lien malicieux où l'attaquant fait aux internautes une offre alléchante et tente de les convaincre d'aller de l'avant avec une transaction ou de lui fournir des renseignements qui lui donnent accès à leurs comptes. Avec ce genre d'arnaque le responsable de l'attaque cherche probablement à accéder au système pour y introduire un programme malveillant[9]. Nous présentons sur la figure ci-dessous une attaque par appâtage où l'attaquant se fait passer pour le ministère de l'emploi de la RDC qui offre des subventions aux fonctionnaires de l'Etat ; l'attaquant crée un lien qu'il partage sur les réseaux sociaux incitant ainsi les gens à suivre le lien pour fournir les informations qu'il va utiliser pour poursuivre son attaque.

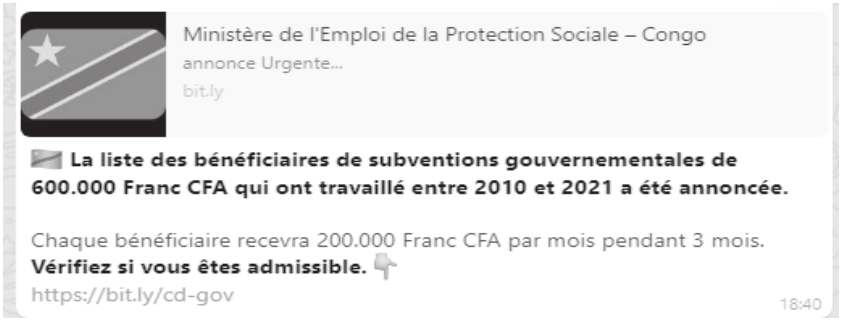


Fig. 2. L'exemple d'un lien appâtage

9 G. BERRY, *Pourquoi et comment le monde devient numérique ?,* Paris, Eyrolles, 2010, p. 16.

Ainsi une fois que l'internaute clique sur le lien, il est redirigé vers le site de pirate comme le montre la figure suivante. Sur le site tout est prévu pour séduire l'internaute à continuer à fournier ses informations confidentielles. Or comme on le remarque en RDC nous avons le franc congolais comme monnaie mais déjà le site propose le franc CFA, et même la structure de l'URL du site ne correspond à aucun site de la RDC, par extension. Nous savons que le domaine parent de notre pays c'est le ***.cd***. Partant de ces éléments il devient facile de détecter directement l'attaque que cache le lien ouvert.

Fig. 3. L'exemple d'un site pirate

1.2.3. L'hameçonnage

L'hameçonnage est une escroquerie qui consiste à tromper les gens pour qu'ils partagent des informations sensibles, telles que des mots de passe et des numéros de carte bancaire. Tout comme il existe plusieurs types d'hameçon, il existe plusieurs façons d'attraper une victime, mais une tactique d'hameçonnage spécifique a le vent en poupe. Les victimes reçoivent un e-mail ou un SMS qui imite (ou « usurpe l'identité de ») une personne ou une organisation à laquelle elles font confiance, comme un collègue, une banque ou un bureau gouvernemental. Quand la victime ouvre l'e-mail ou le SMS, elle y trouve un message inquiétant qui joue sur la peur pour l'empêcher de raisonner[10]. Ce message demande à la victime de se rendre sur un site Internet et d'exécuter immédiatement une action ou, dans le cas contraire, d'en subir des conséquences.

Si les utilisateurs mordent à l'hameçon et cliquent sur le lien, ils sont envoyés sur un site imitant un site légitime. Là, on leur demande de se connecter avec leur nom d'utilisateur et leur mot de passe[11]. S'ils sont

10 J.-P. ARNAUD, *Sécurité Réseaux*, Paris, Dunod, 2003, p. 135.
11 https://softwarelab.org/fr/maliciel.html, consulté le 12/03/2022.

assez crédules pour accepter, les informations de connexion sont transmises au malfaiteur, qui les utilise pour voler les identités, piller les comptes en banque et vendre des informations personnelles sur le marché noir. Sur les lignes suivantes nous présentons deux types d'attaque par phishings.

1.2.3.1. Arnaque sur Whatsapp

Des tentatives d'hameçonnage (ou phishing) envahissent actuellement les détenteurs de smartphones, via l'application de messagerie Whatsapp. Le mode opératoire n'est pas récent mais, bien rodé, il continue de sévir et de faire des victimes. L'attaquant incitera la cible à cliquer sur le lien inséré conduisant vers un faux site de l'enseigne usurpée. Après avoir répondu à une série de questions, on annonce à la cible qu'il est éligible pour remporter ou obtenir un cadeau[12]. Mais, avant de l'obtenir, elle devra envoyer le message reçu à vingt de ses contacts via Whatsapp, afin de propager l'arnaque. Voici un exemple de ce type de phishing.

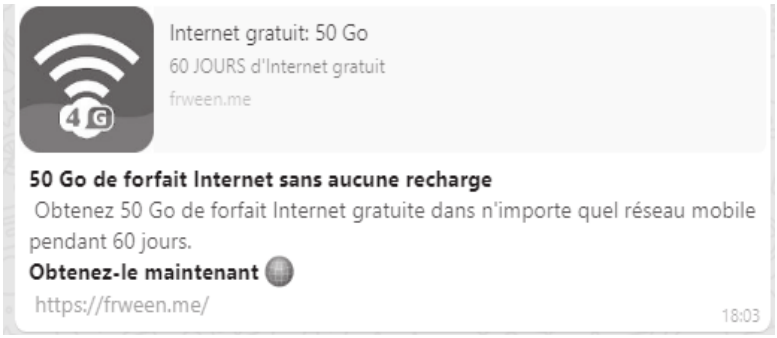


Fig.4. L'exemple d'un lien phishing

1.2.3.2. Les arnaques à l'héritage

Les escrocs diffusent un message électronique proposant de mirobolantes commissions, en échange de l'utilisation d'un compte bancaire pour effectuer des virements d'un montant très élevé. Il s'agit en général de prétendus fonds qui se trouveraient bloqués dans une banque au nom de prétendus héritiers ne pouvant récupérer leurs avoirs sans l'intervention d'un tiers[13]. Les escrocs excellent dans l'art d'instaurer un doute dans l'esprit des personnes qui se font duper en usurpant le nom des personnes réelles et de vraies banques en créant des adresses élec-

12 G. PUJOLLE, *Sécurité et cryptographie*, Paris, 6é éd., Eyrolles, 2019, p. 245.
13 Y. LESCOP, *Les attaques informatiques*, Paris, Hermès, 2016, p. 56.

troniques évocatrices, mais fausses. L'objectif des escrocs consiste soit à obtenir le numéro du compte bancaire et un exemplaire de la signature pour donner de faux ordres de virement à la banque, soit à faire payer à la cible de prétendus « frais de dossier » préalables, qui se succèderont ensuite en cascade.

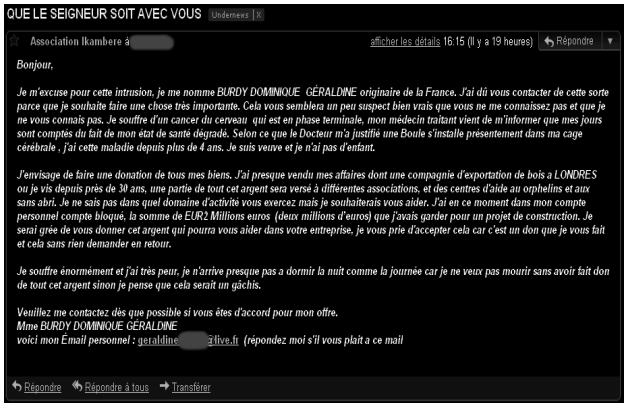


Fig. 5. Un message d'arnaque

2. Déroulement d'une attaque par lien malicieux

Nous venons de présenter quelques types d'attaques par lien malicieux. Cette deuxième partie de notre étude se charge d'étaler le scenario de l'un de ce type d'attaque. Nous partons de la génération du lien, son partage sur le réseau pour finir par l'exploitation de l'équipement de notre victime. Dans le cadre de ce scenario, nous allons utiliser l'outil *Metasploit* de Kali linux pour la génération de lien malicieux ; ce même outil nous servira d'interface d'espionnage de notre victime.

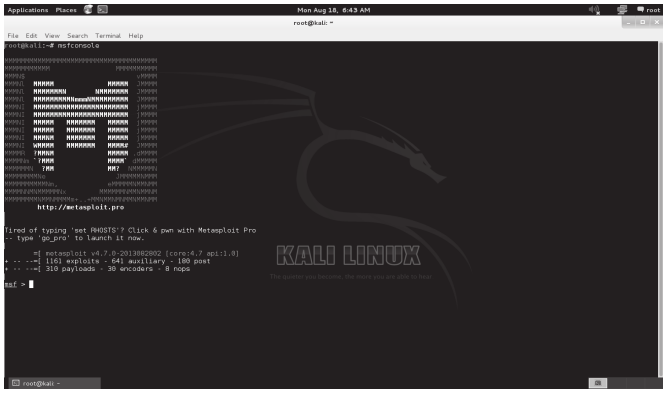


Fig. 6. L'interface principale de Metasploit

2.1. Génération de lien arnaque

Il y a plusieurs environnements que les pirates utilisent pour développer leurs attaques, le *Metasploit* que nous utilisions ici est l'un des outils puissants de la distribution Kali linux de l'environnement libre qualifié dans la sécurité informatique et piratage. En effet, nous présentons la génération de lien avec Kali Linux ; le lien généré sera envoyé sous forme de message à un smartphone.

Fig. 7. la génération de lien pirate

2.2. Prise de contrôle d'un smartphone victime

Ce processus commence une fois que la victime clique sur le lien piégé, et que son smartphone est toujours connecté au réseau. Du côté Kali Linux un message signale la présence d'une victime connectée en fournissant quelques éléments (Type, Marque, Numéro de port d'écoute et l'adresse Ip) de l'équipement comme l'illustre la capture ci-dessous.

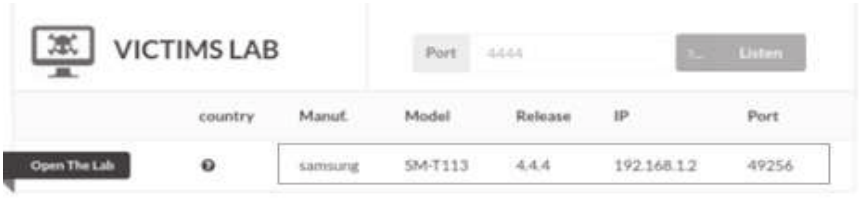


Fig. 8. La détection d'une victime

2.3. Espionnage du smartphone victime

Un clic sur la cible nous donne la possibilité de parcourir les informations dont dispose le smartphone victime. Il ne reste qu'à cliquer sur l'onglet correspondant aux informations que nous avons besoin d'explorer[14]. La capture suivante présente le gestionnaire de fichiers de notre cible.

14 https://summarynetworks.com/securite-des-reseaux-informatique-et-telecom/pirater-et-controler-un-telephone-portable-via-metasploit-sous-kali-linux-2020/, consulté le 04/02/2022.

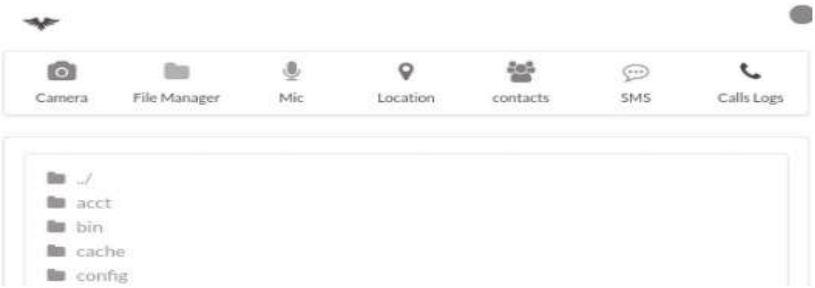


Fig. 9. L'exploitation des fichiers de la victime

Il faut souligner ici que le nombre croissant de *Sextape* sur les réseaux sociaux n'est surtout pas l'œuvre du concerné, le pirate passe par de tels mécanismes en activant la caméra de la victime à distance, ce qui lui donne la possibilité de surveiller tout mouvement de sa cible. Il peut même démarrer l'enregistrement de la vidéo qu'il utilisera en échange d'une somme d'argent. Au cas contraire il la balancera sur la toile pour ternir l'image de la victime.

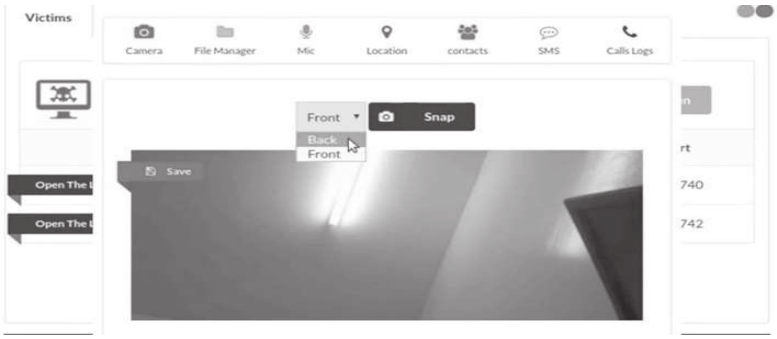


Fig. 10. La prise de contrôle de la caméra de la victime

2.4. Comment savoir si mes appareils sont infectés

Parfois, il n'est pas évident de savoir qu'un appareil ait été infecté. Le maliciel peut très bien fonctionner secrètement. Parfois aussi, certains signes vous avertiront que votre appareil a été infecté par un maliciel :

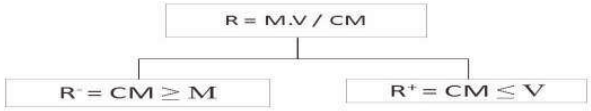
- ✓ Votre ordinateur pourra ralentir, tomber en panne ou figer.
- ✓ Des changements à la barre d'outils de votre navigateur pourront s'opérer et vous pourrez vous retrouver sur des sites Web que vous n'avez pas demandés.
- ✓ L'usage de données sur votre cellulaire monte en flèche.
- ✓ Vous remarquez une application sur votre cellulaire que vous n'avez pas téléchargée.

3. Se protéger des liens malicieux

Il est vrai que dans le monde informatique il n'y a pas une sécurité absolue, mais il est préferable de minimiser les risques d'attaques en difinissant un seuil de protection car si le niveau de failles de votre équipement est élévé vous êtes exposé à tout moment à des attaques de diverses formes. C'est pourquoi nous commençons par présenter cette formule simple de calcul de risque pour évaluer combien nous sommes tous exposés quand nous sommes connectés à la toile mondiale[15].

$$Risque = \frac{\text{Menace x Vulnerabilite}}{\text{Contre mesure}}$$

- ✓ ***Risque :*** c'est la probabilité qu'une menace exploite une vulnérabilité. Autrement dit, c'est une possibilité qu'un fait dommageable se produise.
- ✓ ***Vulnérabilité :*** c'est une faiblesse inhérente à un système (software ou hardware). Appelée parfois faille ou brèche, elle représente le niveau d'exposition face à la menace dans un contexte particulier.
- ✓ ***Menace :*** c'est le danger (interne ou externe) tel qu'une attaque, un virus, etc.
- ✓ ***Contre-mesure*** : c'est un moyen permettant de réduire le risque dans une organisation.



Le risque est d'autant plus réduit que les contre-mesures sont nombreuses. Le risque est plus important si les vulnérabilités sont nombreuses. Ainsi nous devons observer les règles suivantes pour minimiser les risques de tomber victime d'attaque quand nous surfons sur le Net.

- ➲ Disposer toujours d'un logiciel antivirus et anti-espion à jour ;
- ➲ Éviter de télécharger des applications, des fichiers, des programmes et des logiciels gratuits ;
- ➲ Ne jamais répondre aux messages contextuels qui apparaissent sur les sites ou les applications vous demandant vos informations confidentielles ;

15 C. LIORENS, *Tableaux de bord de la sécurité réseau*, Paris, 2è éd., Eyrolles, 2008, p. 65-68.

- Prendre tout le temps et ne pas laisser des messages d'urgence impressionner. Prendre toujours le temps d'examiner soigneusement les détails et les faits avant d'agir ;
- Ne jamais partager les informations, être prudent lorsqu'on partage des informations personnelles ou professionnelles ;
- Bien observer l'URL du lien, toute faute d'orthographe ou irrégularité doit attirer l'attention ;
- Vérifier que le site est sécurisé : un cadenas doit être présent dans l'URL et l'adresse du site doit commencer par HTTPS (et non HTTP) ;
- Saisir le nom d'utilisateur et mots de passe uniquement quand on utilise une connexion sécurisée.

Conclusion

Les cybercriminels sont devenus des experts dans l'utilisation de techniques sophistiquées pour amener les victimes à partager des informations personnelles ou financières. Mais la meilleure façon de nous protéger reste la mise en pratique des règles listée plus haut car autant nous cherchons à nous mettre à l'abri autant les pirates recherchent continuellement à développer des attaques malveillantes qui seront difficiles à différencier des vrais e-mails et des communications authentiques. Ainsi, à travers cette étude, nous avons voulu informer sur les différentes attaques qui ne cessent de monter en puissance sur la toile mondiale avec l'utilisation innovante et croissante de l'Internet des objets (IoT) et des appareils portables.