Introduction générale

Les progrès fulgurants des Technologies de l'Information et de la Communication(**TIC**) et le bésoin de faire collaborer des objets ont conduit à un concept moderne qui est « Internet of Things [1]» (**IoT**). L'IoT nous offre une nouvelle opportunité de croissance nous permettant délimiter la perte de temps, de ressource, améliorant ainsi nos vie quotidiennes.De nos jours, il existe de nombreuses plateformes et applications pour l'IoT conduisant à fournir de nouveaux services et automatiser de nombreux processus dans l'industrie(smart industry), la santé(smart health), le ménage, les transports(smart transport) et de nombreux autres secteurs etc.

Il existe plusieurs définitions sur le concept de l'IoT, mais nous adoptons celle proposée par Weill et Souissi qui ont défini l'IoT comme « une extension de l'Internet actuel envers tout objet pouvant communiquer de manière directe ou indirecte avec des équipements électroniques eux-mêmes connectés, à l'Internet. Cette nouvelle dimension de l'Internet s'accompagne avec de forts enjeux technologiques, économiques et sociaux tout en assurant la protection des données des utilisateurs » [Zhang Hang, 2013]. Quasiment n'importe quel appareil doté d'un bouton marche/arrêt peut se connecter à l'Internet aujourd'hui, intégrant ainsi la catégorie des objets de l'IoT [kaspersky,]
En ce qui concerne l'IoT, Les objets connectés peuvent être des objets physiques ou virtuelles (smartphones, ordinateurs, data centers, réseaux Wi-Fi, réseaux cellulaires, puces RFID , capteurs, équipement ménager, montres, serrures, véhicules, drones, etc) pouvant être identifiés et intégrés dans la communication des réseaux.
D'après la plateforme statisca [statista, 2020] aujourd'hui le nombre d'objets connectés est estimé à **30.73 milliards** d'objets connectés dans le monde et ce nombre atteindrait les **75.44 milliards** d'objets connectés en 2025.

Cependant assurer la confidentialité, la disponibilité et l'intégrité des objets connectés ainsi que les données qui y transitent sont les principales préoccupations concernant l'adoption de ce nouveau concept l'IoT. Une fois que les appareils sont connectés à Internet, ils deviennent vulnérables à d'éventuelles d'attaques informatiques. l'IoT étant la prochaine génération d'Internet [Dave, 2011] avec de plus en plus d'objets connectés allant des villes connectés aux vaches connectées. Dans ce réseau les objets connectés s'échangent des informations pour répondre à un but bien défini. Cette collaboration des objets ouvre des portes d'attaques aux hackers qui effectuent des attaques de plus en plus sophistiquées.

Selon 451 Research [Buckley,] beaucoup d'entreprises sont toujours retissant dans l'adoption de l'IoT à cause sa gestion de la sécurité de ce nouveau qui est encore en état embryonnaire, mais 55% des entreprises qui ont adoptées l'IoT classent la gestion de la sécurité IoT comme

[1]Nous utilisons tout le long de notre mémoire l'abréviation IoT pour « Internet of Things », qui se traduit en français par l'Internet des objets

leur priorité absolue lors des déploiements de projets IoT au sein de leurs organisations. Les systèmes vulnérables des objets connectés peuvent être compromis de n'importe où et utilisés pour cibler n'importe qui raison pour laquelle la sécurité IoT est une préoccupation mondiale.

Les objets connectés font faces à plus types de menaces. ces types de menaces sont classées en quatre(4) types [infosec,] :

- **Déni de Service :** Cette menace vise la disponibilité d'un service ou d'une ressource en la saturant de requête indésirable empêchant ainsi ses utilisateurs légitimes de l'utiliser. cette indisponibilité du service ou d'une ressource est mise en œuvre avec par l'attaque de types DDoS. C'est probablement l'une des ménaces les plus courantes et les plus dangereuses .

- **les logiciels malveillants** Un auteur de malware conçoit spécifiquement ses codes pour compromettre les architectures utilisées par les appareils IoT. Un code malveillant pourrait être utilisé pour infecter les ordinateurs utilisés pour contrôler un réseau d'appareils intelligents ou pour compromettre le logiciel qui y est exécuté. Dans ce deuxième scénario, les attaquants peuvent exploiter la présence d'une faille dans le micrologiciel exécuté sur les appareils et exécuter leur code arbitraire, transformant les composants IoT en utilisation non planifiée [infosec,]

- **Violation de données (Data Breaches) :** C'est une menace visant l'intégrité et la confidentialité des données. les attaquants peuvent utiliser des attaques de type homme du milieu pour intercepter les communications des objets connectés.

- **Affaiblissement des périmètres :** Les appareils de l'Internet des objets ne sont généralement pas conçus pour la sécurité. Bien qu'il s'agisse d'appareils connectés à Internet, la majorité des appareils ne disposent pas de mécanismes de sécurité réseau. Prenons, par exemple, un compteur intelligent. Si l'attaquant est en mesure de le compromettre, il pourrait avoir accès à notre réseau domestique, nous espionner ou causer des dommages physiques à notre environnement domestique. Le problème est tout aussi grave si nous considérons l'utilisation d'appareils IoT dans n'importe quelle industrie.[infosec,]

Nous nous focaliseront dans ce mémoire sur la menace « déni de service [2](**DoS**)», notamment l'attaque par « Déni de Service Distribué[3](**DDoS**)». une attaque par déni de service est une attaque qui empêche l'accès à une ressource ou à un service internet. Elle obtenue en saturant avec des centaines de milliers voire des millions de connexions(requêtes) un serveur ou un objet connecté jusqu'à le bloquer.

À titre d'exemple :

- En 2007 l'Estonie [Jégo, 2007] a été victime de la première plus grande attaque DDoS de l'histoire. l'attaque visait le système informatique du pays notamment ses sites gouvernementaux, ses banques et ses médias créant la panique et déclenchant de vaste d'émeute au sein de la population et force de l'ordre.

[2]Nous utilisons tout le long de notre mémoire l'abréviation DoS pour « Denial of Service », qui se traduit en français par déni de Service

[3]Nous utilisons tout le long de notre mémoire l'abréviation DDoS pour « Distributed Denial of Service », qui se traduit en français par déni de service distribué

- En octobre 2016 [Strawbridge,] Dyn un important fournisseur de service de noms de domaine a été victime d'une vague d'attaque par déni de service distribuée. l'attaque était orchestrée à l'aide d'un logiciel malveillant appelé Mirai, les pirates se sont servis de ce programme pour créer un énorme botnet[4] de 100000 objets connectés pour lanceur leur attaque. L'attaque a été extrêmement perturbatrice et a fait tomber les sites Web de plus de 80 de ses clients, notamment Amazon, Netflix, Airbnb, Spotify, Twitter, PayPal et Reddit. Les dommages causés par cette attaque auraient coûté 110 millions de dollars ainsi que la dégradation de la réputation du fournisseur.
- En 2018 github, une plateforme de développement à son tour était visée d'attaque DDoS qui a été. l'attaque a été maitrisée 10 min après [Strawbridge,] grâce à la présence système de protection d'attaque DDoS dans la plateforme.

Nous proposons dans ce mémoire *la mise en place d'un système de détection d'intrusion dans le réseau IoT contre les attaques de types DDoS.* afin d'assurer la disponibilité d'un service ou d'un objet connecté dans le réseau IoT.

Notre choix du DDoS s'explique du fait que le DDoS utilise les objets connectées non sécurisés pour sa mise œuvre et du fait qu'elle est actuellement considérée comme l'attaque la plus dangereuse visant l'IoT [Adat et al., 2017] [Perakovic et al., 2015].

Ce document est organisée en 2 parties :

La première partie : présente l'état de l'art sur les différents domaines entrant en jeu dans le cadre de ce mémoire à savoir la sécurité informatique et la cybersécurité, l'attaque par déni de service distribué (**DDoS**), l'Internet des objets(**l'IoT**) ——— A COMPLETER PAR LA SUITE ———

La seconde partie : ——— PRESENTERA LES CONTRIBUTIONS APPORTEES———

[4] un botnet est un réseau d'objet connectés contrôlé par un hacker

Bibliography

[Adat et al., 2017] Adat, V., Gupta, B. B., and Yamaguchi, S. (2017). Risk transfer mechanism to defend ddos attacks in iot scenario. pages 37–40.

[Buckley,] Buckley, K. Survey finds security continues to be top priority in deploying iot projects.

[Dave, 2011] Dave, E. (2011). The internet of things how the next evolution of the internet is changing everything. *Cisco Internet Business Solutions Group (IBSG)*.

[infosec,] infosec. Internet of things: How much are we exposed to cyber threats?

[Jégo, 2007] Jégo, M. (2007). L'estonie tire les leçons des cyberattaques massives lancées contre elle pendant la crise avec la russie. *Journal Le Monde*.

[kaspersky,] kaspersky. Internet des objets : qu'est-ce que l'iot ? iot security.

[Perakovic et al., 2015] Perakovic, D., Periša, M., and Cvitić, I. (2015). Analysis of the iot impact on volume of ddos attacks. page 1.

[statista, 2020] statista (2020). Internet of things (iot) connected devices installed base worldwide from 2015 to 2025.

[Strawbridge,] Strawbridge, G. 10 biggest ddos attacks and how your organisation can learn from them. *metacompliance*.

[Zhang Hang, 2013] Zhang Hang, H. M. (2013). Business intelligence architecture based on internet of things. *Journal of Theoretical and Applied Information Technology*.