L'IoT au profit de la montée en puissance des botnets-as-a-service

CORENTIN GARCIA, JIMMY FONTAINE, THOMAS SCOTTO-LOMASSESE, ENSIBS, France

En remarquant la corrélation entre l'augmentation des appareils IoT et la croissance exponentielle des attaques par botnets, cela a suscité notre curiosité quant au fonctionnement de ceux-ci. Nous nous sommes penchés sur la question de la sécurité des appareils IoT et nous nous sommes demandé pourquoi ces dispositifs étaient les cibles de prédilection dans le processus de création de botnets. En recueillant ces observations et ces questions, nous avons identifié le problème suivant : comment l'IoT profite à la montée en puissance des botnets-as-a-service ? Nos recherches ont mis en lumière des résultats inquiétants concernant la sécurité des appareils IoT. Nous avons également constaté une certaine négligence de la part des utilisateurs à cet égard. De plus, nous avons découvert l'existence de véritables armes de DDoS. Les botnets ont considérablement évolué et sont maintenant plus puissants que jamais. Par exemple, en mars 2023, le botnet HinataBot a été capable de lancer des attaques DDoS atteignant 3,3 Tbit/s. Il y a toutefois des nouvelles positives. Les solutions de protection et de détection des botnets sont en constante évolution. Nous aborderons des mesures de sécurité telles que l'EDIMA et d'autres mesures de protection qui peuvent être mises en place pour se prémunir contre ces menaces.

CCS Concepts: • **Networks** → **Botnets**; Network security; • **Computer systems organization** → **Internet of Things**; *Distributed architectures.*

Additional Key Words and Phrases: Cybersecurity, Distributed Denial of Service (DDoS), Machine Learning, Public Key Infrastructure (PKI), Network Traffic Analysis, Malware Detection

Author's address: Corentin Garcia, Jimmy Fontaine, Thomas Scotto-Lomassese, ENSIBS, Vannes, France.

1 INTRODUCTION

La prolifération des dispositifs connectés à l'Internet des objets (IoT) a apporté des avantages considérables dans des domaines variés, mais a également conduit à des conséquences indésirables. Parmi ceux-ci, les attaques de botnets qui ont augmenté de façon inquiétante, menaçant la sécurité et la confidentialité des systèmes informatiques ainsi que des données des utilisateurs. Il existe un véritable fossé entre Agobot (2002) et HinataBot (2023) en termes de performance d'attaque et de capacité d'infection. En 2022 on recense près de 13 millions d'attaques DDoS (Cloudflare), ce qui représente un nouveau record. Cette évolution est d'autant plus préoccupante avec l'émergence des botnets-as-a-service, qui facilitent leur déploiement et leur utilisation par des acteurs malveillants.

Nous avons constaté un lien étroit entre l'expansion des dispositifs IoT et l'évolution des botnets, ce qui a suscité notre intérêt pour leur fonctionnement et leur exploitation. Toutefois, pour comprendre le fonctionnement des botnets, il est indispensable de comprendre les mécanismes sous-jacents de l'Internet des Objets (IoT). Suite à ces observations, nous avons formulé la problématique de notre recherche comme suit : Comment l'IoT est au profit de la montée en puissance des botnets-as-a-service ?

Les résultats de nos recherches nous ont permis de confirmer cette corrélation entre évolution de l'IoT et évolution des botnets. En effet, nous avons remarqué que les appareils IoT étaient dotés de mesures de sécurité insuffisantes. Par ailleurs, ceux-ci connaissaient une certaine négligence de la part de leurs utilisateurs. D'autre part, les botnets devenaient de plus en plus contagieux et donc, indirectement, de plus en plus puissants. Au travers de ces recherches, nous nous sommes également penchés sur les objectifs recherchés par les détenteurs de botnets. Nous y avons alors trouvé un modèle économique rentable pour les créateurs de botnets tandis que les acheteurs cherchaient plutôt à mettre à mal la concurrence ou bien tout simplement à nuire à certains services. Cependant, face à cette évolution inquiétante, il y a aussi une évolution des solutions de protection face aux botnets. Certaines sont des solutions de détection préventive des botnets, d'autres sont des solutions pour apporter davantage de sécurité aux appareils IoT. Nous nous sommes particulièrement intéressés au protocole de sécurisation PKI4IoT ainsi qu'à la solution de détection EDIMA.

Nous commencerons par présenter les notions essentielles nécessaires à la compréhension de l'étude. Ensuite, nous détaillerons la méthodologie de recherche utilisée, ainsi que les critères de sélection des articles pertinents. Les résultats de nos recherches seront ensuite exposés, en mettant en évidence les systèmes économiques qui gravitent autour des botnets et en décrivant l'évolution de ces derniers au fil du temps. Nous analyserons ensuite en détail comment les botnets sont devenus de véritables armes redoutables, capables de causer des dommages considérables. Une attention particulière sera portée à la question de la maigre sécurité entourant l'IoT et aux lacunes qui permettent aux botnets de cibler les appareils embarqués de petite taille. Nous présenterons par la suite les différentes solutions de détection de botnets qui ont été mises en œuvre pour contrer cette menace croissante. De plus, nous étudierons les mesures de protection particulières de l'IoT qui peuvent être mises en place pour améliorer la sécurité des appareils connectés. La discussion des résultats nous permettra d'analyser en profondeur les implications de nos découvertes et de déterminer les futures pistes de recherche pour aborder l'évolution des botnets-as-a-service. Nous soulignerons aussi les limites de notre étude et reconnaîtront les domaines qui pourraient nécessiter d'autres recherches. Pour conclure, nous récapitulerons les principaux points abordés dans cet article et soulignerons l'importance cruciale de la sécurité dans le contexte de l'Internet des objets. Les références bibliographiques utilisées pour étayer notre étude seront également fournies.

2 GLOSSAIRE

Table 1. Glossaire des termes clés

Mot-clés	Définition	Justification
IoT	"Internet of Things" pour l'internet des choses. C'est une catégorie représentant les appareils intelligents, dispositifs médicaux connectés, ampoules…	Sujet principal de notre problématique qui est d'étudier la corrélation entre IoT et botnet
Botnet	Constitue un botnet, un réseau regroupant plusieurs machines compromises permettant un accès distant aux cybercriminels sur chacune des machines du réseau constitué.	Sujet principal de notre problématique qui est d'étudier la corrélation entre IoT et botnet
DDoS	Attaque informatique souvent associée aux botnets	Permet d'identifier les motivations à la création d'un botnet
Mirai	Mirai est un logiciel malveillant ayant pour but de contaminer les équipements numériques afin de les intégrer dans les divers Botnets	Un des premiers Software à avoir réellement eu un impact conséquent sur l'ensemble d'internet quant à la création de botnets
Security	Protéger l'intégrité des systèmes d'informations (ici l'IoT)	Sécurité de l'IoT
Opportunity	Une conséquence qui convient au moment	Ici, nous cherchons à montrer que l'IoT est devenu un vrai terrain d'opportunité aux acteurs malveillants d'Internet

3 MÉTHODOLOGIE DE RECHERCHE

Pour effectuer nos recherches nous nous sommes concentrés sur quatre bases de données distinctes dont nous avons extrait dix-huit articles. Le schéma ci-dessus récapitule notre méthode de recherche, explicite les mots clés que nous avons utilisés ainsi que le nombre d'articles trouvés. Ces articles extraient représentent la matière brute que nous avons travaillé afin d'écrire cet article qui a pour ambition d'être un état de l'art sur la problématique traitée.

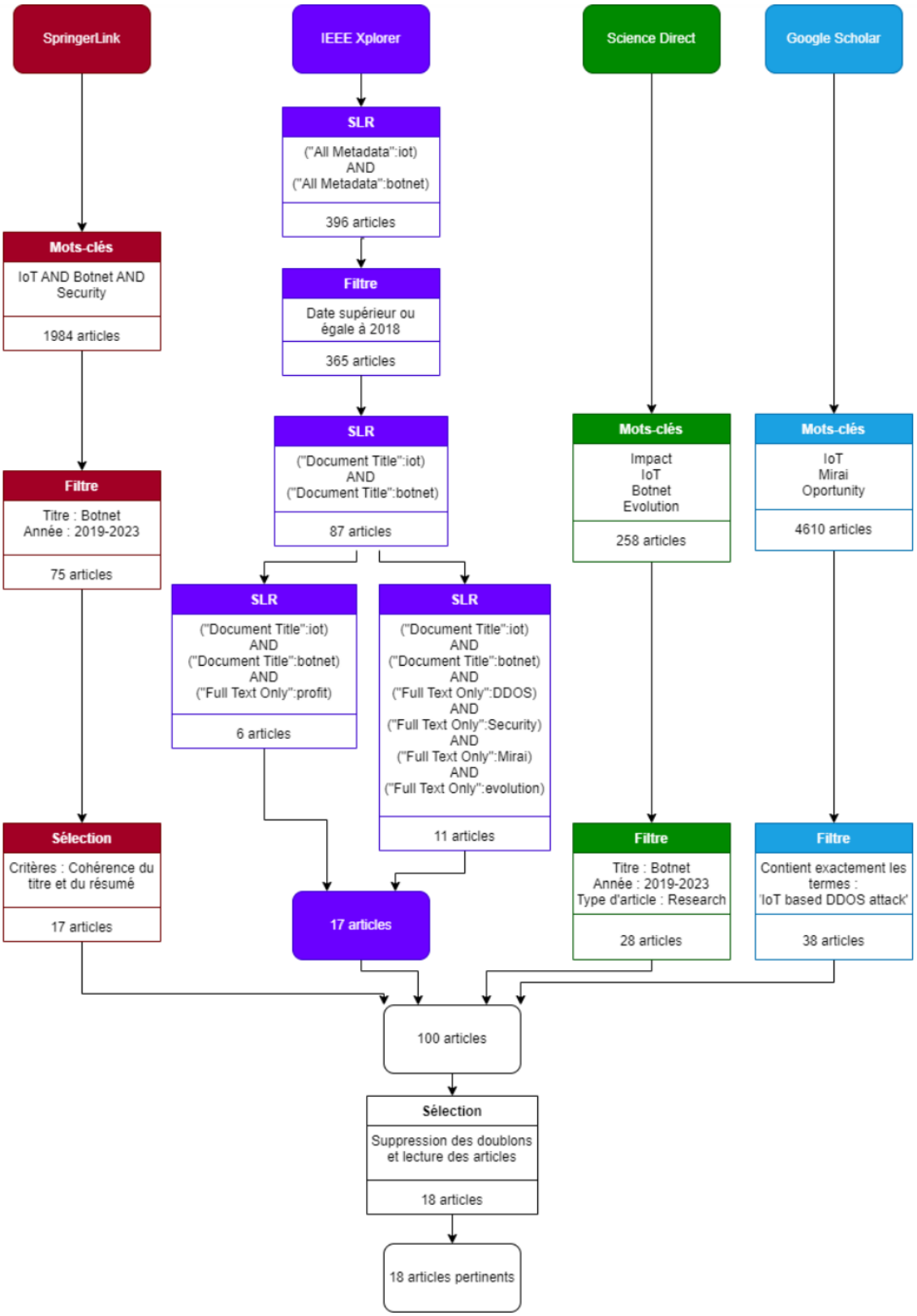

Fig. 1. Schéma récapitulatif de nos recherches

Bien que nous ayons sélectionné les articles les plus pertinents vis-à-vis de notre sujet dans ces bases de données, cela n'était pas suffisant. Nous nous sommes donc assurés que ces articles répondaient bien à notre problématique en définissant des critères de pertinence.

4 CRITÈRES DE SÉLECTION DES ARTICLES PERTINENTS

Afin de pouvoir filtrer les articles qui seraient les plus pertinents pour notre étude, nous avons dû établir un ensemble de critères clés pour évaluer chaque article. Le processus de définition de ces critères a été réalisé avec soin, en tenant compte de l'objectif et de la portée de notre recherche.

Ces critères, que nous avons finalement définis, sont présentés dans le tableau ci-dessus. Ils nous ont permis d'effectuer une évaluation précise de chaque article et de déterminer ceux qui pourraient contribuer de manière significative à notre étude. Après avoir appliqué ces critères de manière rigoureuse, nous avons pu sélectionner un total de neuf articles parmi les dix-huit que nous avions initialement trouvés.

Table 2. Résumé des articles

Titre de l'article	**Année de parution**	**Type de botnets**	**Moyen de défense**	**Type de performance**	**Environnement de tests**
IoT as a Land of Opportunity for DDoS Hackers	2018	Tous	-	Recherche	-
Weaponizing the internet of Things	2017	Tous	-	Recherche	-
DDoS in the IoT : Mirai and Other Botnets	2017	Tous	-	Recherche	Lab
Cyber espionage through Botnets	2019	Hybride	-	Espionnage	-
The Evolution of Bashlite and Mirai IoT Botnets	2018	Centralisée	-	?	Réels Honeypots
A Low-Cost Distributed Denial-of-Service Attack Architecture	2020	Hybride	-	Faible coût	Lab
Botnet Business Models, Takedown Attempts, and the Darkweb Market	2023	Tous	Démantèlement	-	-

Continue sur la page suivante

Table 2 – suite de la page précédente

Titre de l'article	Année de parution	Type de botnets	Moyen de défense	Type de performance	Environnement de tests
Machine learning-based early detection of IoT botnets using network-edge traffic	2022	-	Machine Learning	Botnet detection	Lab
PKI4IoT: Towards public key infrastructure for the Internet of Things	2019	-	PKI for IoT	IoT protection	Lab / IoT Device

Chacun des neuf articles sélectionnés apporte une partie de réponse à la problématique que nous nous sommes fixés. Nous avons donc répartis ces neufs articles et leurs résultats dans plusieurs catégories qui sont les suivantes:

(1) Évolution des botnets au fil du temps
(2) Systèmes économiques autour des botnets
(3) Comment les botnets sont-ils devenus de véritables armes
(4) La sécurité autour de l'IoT
(5) Les solutions de détection des botnets

En répartissant ainsi les articles dans ces catégories, nous sommes en mesure de couvrir un large spectre de perspectives et de réponses à la problématique : comment l'IoT contribue-t-il à la montée en puissance des botnets-as-a-service ? Cette approche multicritère nous permet d'appréhender le problème dans sa globalité, tout en soulignant les diverses facettes qui le constituent.

5 RÉSULTATS PAR CATÉGORIE

5.1 Évolution des botnets au fil du temps

Au fil du temps, les botnets ont considérablement évolué. Cette évolution est illustrée par l'étude de deux botnets importants dans l'article [6]. Ces deux botnets ont marqué l'écosystème des menaces IoT en raison de leur sophistication croissante et de leur capacité à infliger des dégâts importants.

Initialement, Bashlite était l'un des botnets IoT les plus notables, exploitant les vulnérabilités des appareils connectés pour créer un réseau d'appareils infectés. Cependant, au fil du temps, son successeur, Mirai, a émergé avec des fonctionnalités plus avancées et une plus grande capacité d'adaptation.

L'évolution de ces botnets a été étudiée à partir des données recueillies de 47 honeypots sur une période de 11 mois. Ils ont constaté que Mirai avait évolué pour utiliser une infrastructure d'hébergement et de contrôle plus résiliente et envoyait des attaques plus efficaces.

Le passage de Bashlite à Mirai illustre non seulement l'évolution des techniques d'attaque des botnets, mais aussi comment les opérateurs de botnets s'adaptent et se renouvellent face à l'évolution des défenses en matière de cybersécurité. Plus particulièrement, l'étude a montré que les logiciels malveillants, les opérateurs de botnet et les activités malveillantes deviennent de plus en plus sophistiqués.

Ainsi, l'évolution constante des botnets et l'adaptation rapide des opérateurs de botnets mettent en évidence l'importance d'une surveillance constante et de l'établissement de défenses robustes et évolutives. C'est dans ce contexte que nous examinerons dans la section suivante les systèmes économiques qui entourent les botnets, pour mieux comprendre comment ils sont vendus et exploités.

5.2 Systèmes économiques autour des botnets

Les botnets constituent une partie primordiale de la cybercriminalité, générant un flux économique important, en particulier, sur les marchés du darkweb. En parallèle, l'émergence des botnets "low-cost" a remodelé l'économie de ces menaces, rendant leur accès plus facile et moins coûteux.

D'après l'article [1], les acteurs malveillants vendent ou louent leurs botnets. Ces transactions ont lieu sur des marchés cachés dans le darkweb, loin de la surveillance des autorités (Figure 2). Dans cette économie souterraine, les botnets sont une ressource précieuse qui peut être exploitée de différentes manières. En particulier, les botnets sont souvent utilisés pour mener des attaques DDoS avec une grande facilité d'utilisation.

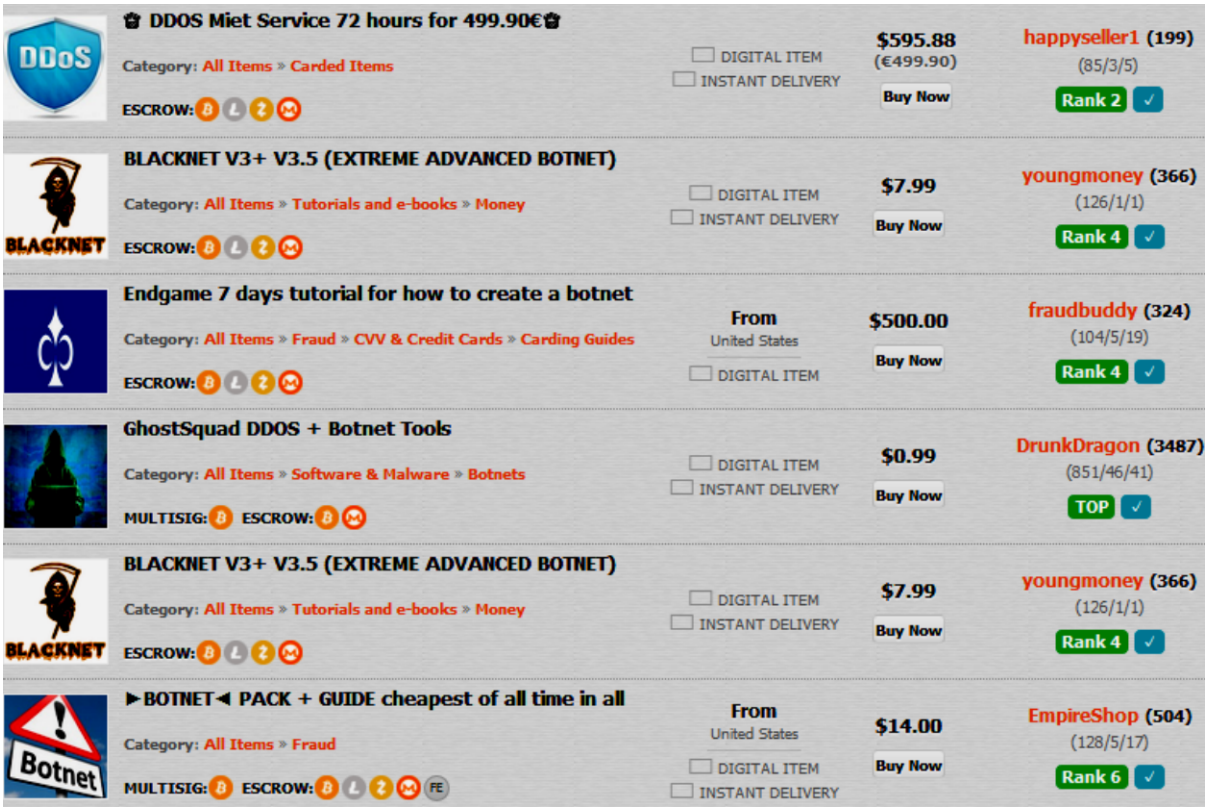

Fig. 2. Services de botnet sur le marketplace Torrez

L'article [2] décrit une architecture de botnet de type "low-cost" pour les attaques DDoS. Ces botnets sont conçus pour être bon marché à mettre en place et à maintenir, ce qui rend ces types d'attaques accessibles aux

acteurs malveillants avec des ressources limitées. Cela a donc augmenté le nombre d'acteurs capables de mener de telles attaques, et ainsi augmenter le nombre d'attaques. C'est un aspect important à prendre en compte lors de l'élaboration de stratégies de défense contre les botnets.

Pour résumer, la commercialisation des botnets sur le darkweb, couplée à leur facilité et à leur faible coût d'utilisation, présentent de nouveaux défis en matière de sécurité. Comprendre ces systèmes économiques peut nous aider à élaborer des stratégies plus efficaces pour lutter contre ces menaces et pour diminuer leur incidence économique. Les efforts futurs pourraient également se concentrer sur la perturbation de ces marchés souterrains, en rendant plus difficile l'accès aux ressources de botnet et en augmentant les coûts associés à leur utilisation car leur utilisation peuvent mener des attaques DDoS dévastatrices et c'est ce que nous explorerons dans la section suivante : "Comment les botnets sont-ils devenus de véritables armes ?".

5.3 Comment les botnets sont-ils devenus de véritables armes

Au fil du temps, les capacités techniques et la motivation des botnets ont évolué. Ils ont abandonné leurs objectifs de destruction (exemple Figure 3) pour se concentrer sur la recherche de gains financiers et d'autres bénéfices. Cela a entraîné une augmentation des violations de données, touchant particulièrement les informations personnelles telles que les comptes bancaires, les cartes de crédit et même le minage de crypto-monnaies sans le consentement des utilisateurs. Des botnets tels que Gemini en 2010 et AnserverBot en 2011 ont réussi à exploiter les smartphones pour exécuter leurs agents. En 2011, Ramnit a pu voler des comptes bancaires sans difficulté.

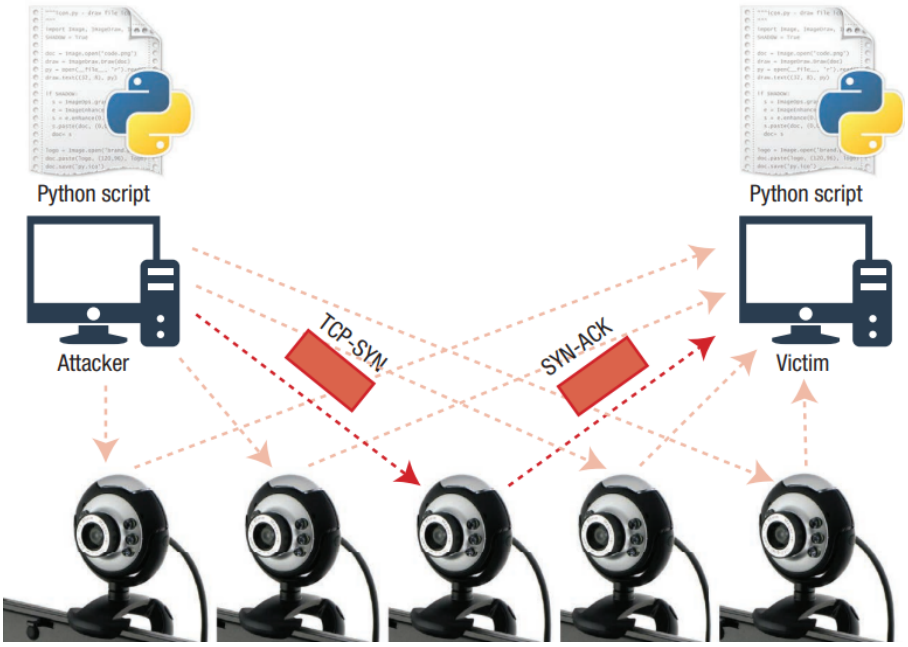

Fig. 3. Attaque DDoS par réflexion SYN-ACK à l'aide de webcams

Les réseaux sociaux ont également ouvert de nouvelles opportunités, avec l'utilisation de "socialbots" contrôlés par une infrastructure solide de serveurs de commandes et de contrôle fournie par les réseaux sociaux. Ces bots communiquent via des messages chiffrés ou dissimulés pour mener leurs activités.

L'importance croissante des botnets dans le domaine de l'espionnage cybernétique a été mise en évidence, en particulier dans le contexte de l'Internet des objets (IoT), où les "thingbots" jouent un rôle de plus en plus important. En 2018, le botnet VpnFilter, l'un des botnets modulaires à plusieurs niveaux, a bénéficié d'une mise à jour comprenant sept nouvelles fonctionnalités, telles que la découverte de réseaux et l'obfuscation de la source des attaques. De plus, il a été démontré que les dispositifs réseau étaient également vulnérables à ces attaques.

La montée en puissance des botnets s'explique par plusieurs points:

- **Évolutivité :** Les réseaux zombies peuvent être constitués de milliers ou même de millions d'ordinateurs infectés dans le monde. Cette échelle massive leur donne un pouvoir de frappe considérable et leur permet de réaliser des attaques de grande envergure comme le montre l'article [7].
- **Facilité de propagation :** L'article [7] montre également que les pirates utilisent souvent des techniques complexes pour infecter les ordinateurs et les intégrer dans un réseau de zombies. Ils exploitent les vulnérabilités dans les systèmes d'exploitation et les logiciels, se propagent au moyen de phising, de pièces jointes compromises ou de sites web compromis. Les ordinateurs infectés se transforment alors en esclaves numériques sous le contrôle de l'attaquant.
- **Anonymat :** Les botnets sont souvent conçus pour masquer l'identité réelle du pirate (article [7] et [3]). Les pirates utilisent des techniques telles que le rebondissement à travers des serveurs proxy ou le chiffrement des communications pour éviter d'être détectés et retrouvés.
- **Diversité des attaques :** L'article [5] nous montre que les botnets sont polyvalents et peuvent être utilisés pour différentes formes d'attaques. Ils peuvent être utilisés pour lancer des attaques DDoS massives, voler des informations sensibles, propager des logiciels malveillants, envoyer du spam ou même extraire des crypto-monnaies via le minage illicite et ceci par le biais d'appareils insoupçonnés.

Les articles [7], [5] et [3] nous ont permis de comprendre les méthodes d'infections des appareils ainsi que leur moyen de prolifération. De plus, les articles nous démontrent les diverses raisons de la prolifération des botnets par le biais des 4 points présentés ci-dessus.

5.4 La sécurité de l'IoT

Malgré les contraintes liées aux ressources limitées des appareils embarqués de l'IoT, certains chercheurs se sont engagés dans l'élaboration de protocoles de sécurité adaptés à ces dispositifs. Ces efforts visent à trouver des mesures de sécurité appropriées pour les objets embarqués, en prenant en compte leurs capacités restreintes.

Nous nous intéressons donc au protocole PKI4IoT qui a pour ambition d'adapter le protocole d'échange de clés (PKI) au monde de l'IoT. Le protocole PKI (Public Key Infrastructure) est un système de gestion de clés cryptographiques utilisé pour sécuriser les communications électroniques et les transactions en ligne. Il fournit un cadre pour la création, la distribution, la gestion et la révocation des certificats numériques, qui sont des éléments essentiels de l'infrastructure de sécurité. Cependant de nombreux petits dispositifs IoT alimentés par batterie sont limités en termes de ressources informatiques nécessaires.

La PKI4IoT est conçue pour permettre l'enrôlement initial, la réinscription et la vérification des certificats pour les dispositifs IoT de manière légère et automatisée, en utilisant des profils légers des protocoles web existants. Il

a été testé dans un environnement de laboratoire avec l'appareil Zolertia Fireflies (Figure 4).

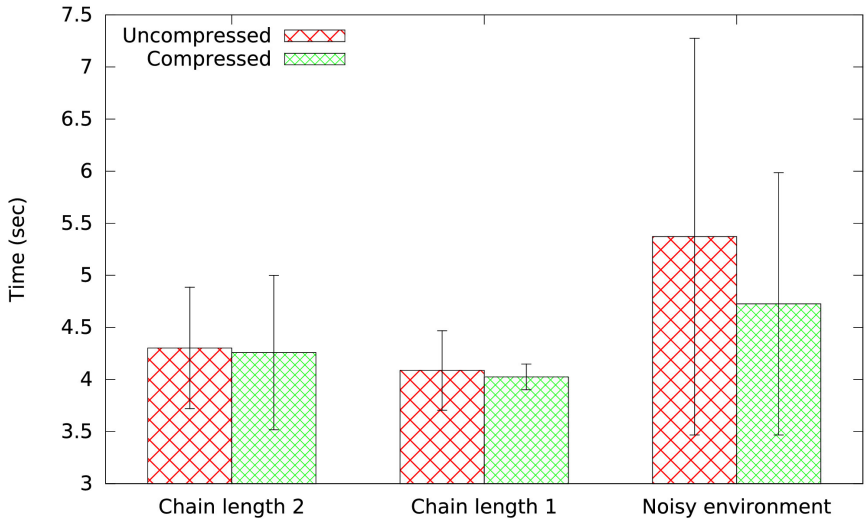

Fig. 4. Temps d'exécution de la négociation DTLS dans un appareil IoT Zolertia Firefly avec le Contiki

L'implémentation de la PKI4IoT présente des avantages en termes de réduction de la consommation d'énergie et de surcharge mémoire. Toutefois, il convient de remettre en question les résultats obtenus et de poursuivre les tests supplémentaires afin de valider les performances et la fiabilité de la PKI4IoT. De plus, l'évaluation des performances de la solution proposée a été effectuée sur un nombre restreint de périphériques, ce qui souligne la nécessité de réaliser des tests à plus grande échelle pour confirmer son efficacité dans des environnements réels.

5.5 Les solutions de détection des botnets

Détecter un botnet est une opération délicate et difficile à mettre en place. Cependant, avec l'évolution du machine learning, il existe aujourd'hui des solutions de détection de botnets. L'article [4] traite de la solution EDIMA (Early Detection of IoT Malware Scanning and CnC Communication Activity).

La méthode privilégiée par les auteurs afin d'évaluer les performances de la solution EDIMA a été la mise en place de la solution puis l'expérience de celle-ci sur deux types de trafics : un trafic sain ainsi qu'un trafic malsain. Le trafic de données dit "sain" est généré par des appareils non infectés tandis que le trafic de données dit "malsain" est lui généré par des appareils infectés.

Les résultats sont très concluants pour cette solution de détection. En effet, il y a un taux de détection de 93% pour cette solution comme l'indique le diagramme ci-dessous (Figure 5) :

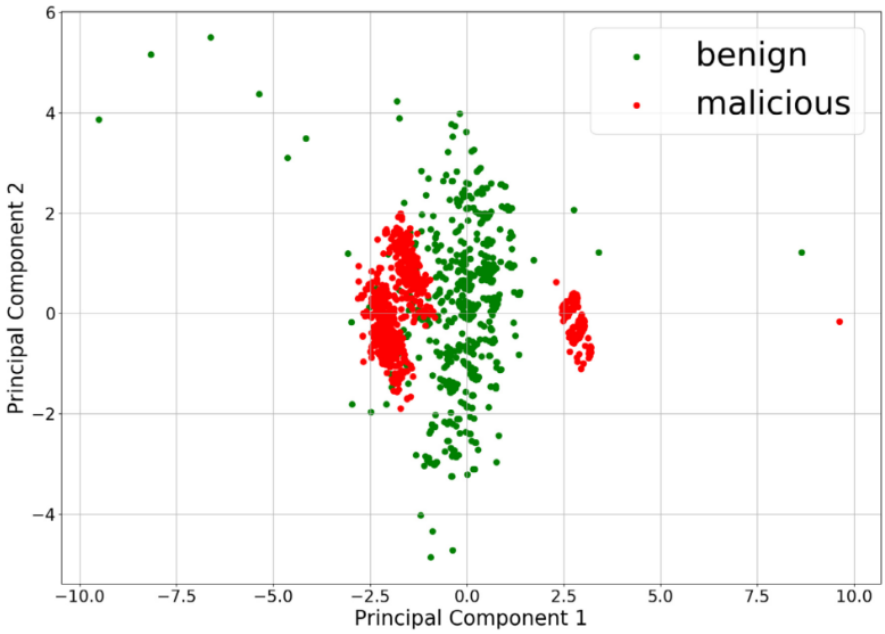

Fig. 5. Résultats de la détection et de la différenciation entre trafic sain et malsain par la solution EDIMA

Cependant, il est envisageable de considérer ces conclusions avec une certaine réserve. Il convient de noter que la solution proposée n'a pas été évaluée dans un contexte opérationnel, mais plutôt en laboratoire avec des données de trafic générées de manière artificielle. Par conséquent, il est essentiel de poursuivre les recherches en testant l'efficacité de la solution EDIMA dans un environnement réel, représentatif des conditions auxquelles elle sera confrontée dans le monde réel. Cette étape permettra d'obtenir des résultats plus concrets et de valider l'applicabilité de la solution dans des situations pratiques.

6 DISCUSSION DES RÉSULTATS, ANALYSE DE CEUX-CI ET DIRECTION DES FUTURES RECHERCHES

L'évolution constante des botnets, couplée à leur commercialisation croissante dans le darkweb, représente un défi de taille pour la cybersécurité. Les botnets, autrefois un outil de nuisance relativement simple, ont maintenant évolué en armes cybernétiques potentiellement dévastatrices, exploitables par quiconque ayant l'argent pour les acquérir et la malveillance pour les utiliser.

La sophistication croissante des botnets, illustrée par l'évolution de Bashlite à Mirai, souligne l'importance d'une défense robuste et évolutive face à ces menaces. Les acteurs malveillants continuent d'innover et d'adapter leurs techniques à mesure que les défenses se renforcent, nécessitant une vigilance constante de la part des défenseurs.

Parallèlement, l'économie souterraine des botnets a également évolué. Le darkweb est devenu une place de marché pour les botnets, avec des acteurs vendant ou louant leurs botnets à d'autres. L'émergence de botnets "low-cost" a rendu ces outils plus accessibles, augmentant le nombre d'attaques DDoS.

En ce qui concerne la sécurité de l'IoT, le protocole PKI4IoT présente un potentiel certain pour renforcer la sécurité des appareils IoT. Toutefois, des recherches supplémentaires sont nécessaires pour valider son efficacité et sa fiabilité dans des environnements réels et à grande échelle.

Enfin, les résultats des tests de détection de botnets tels que la solution EDIMA sont prometteurs, bien qu'ils aient été obtenus dans un environnement de laboratoire plutôt que dans un contexte opérationnel. Cela souligne l'importance de tester ces solutions dans des conditions réelles pour confirmer leur efficacité.

L'évolution rapide des botnets et leur rôle croissant dans la cybercriminalité soulignent l'importance de poursuivre les recherches dans ce domaine. Plusieurs directions peuvent être envisagées pour les futures recherches.

Tout d'abord, il est nécessaire de poursuivre l'étude de l'évolution des botnets et de leurs techniques d'attaque. Cela aidera à anticiper les futures menaces et à développer des défenses plus efficaces.

Ensuite, une analyse plus approfondie de l'économie des botnets pourrait fournir des informations précieuses sur la manière dont ces menaces sont vendues et exploitées. Les efforts pour perturber ces marchés souterrains pourraient être une stratégie efficace pour réduire l'incidence économique des botnets.

De plus, des recherches supplémentaires sur des protocoles de sécurité adaptés à l'IoT, comme le PKI4IoT, sont nécessaires. Ces recherches devraient se concentrer sur la validation de l'efficacité et de la fiabilité de ces protocoles dans des environnements réels et à grande échelle.

Enfin, le développement et le test de solutions de détection de botnets dans des conditions réelles sont une priorité. L'efficacité de ces solutions doit être confirmée dans un contexte opérationnel pour garantir qu'elles soient applicables dans le monde réel. La mise à l'épreuve des algorithmes de détection basés sur le machine learning dans des conditions d'utilisation réelles sera une étape cruciale pour renforcer nos défenses contre les botnets.

7 LIMITATIONS DE L'ÉTUDE RÉALISÉE

7.1 Environnement de laboratoire

La majeure partie de l'étude a été réalisée dans un environnement de laboratoire, ce qui peut ne pas refléter fidèlement les conditions réelles du monde cybernétique. Les botnets, par exemple, peuvent se comporter différemment dans un environnement contrôlé par rapport à un environnement réel, et les solutions de sécurité pourraient ne pas être aussi efficaces dans la pratique qu'en théorie. Il est donc nécessaire de confirmer les résultats de cette étude dans des conditions opérationnelles.

7.2 Limites de l'échantillonnage

L'analyse des botnets a été réalisée en se basant sur des données recueillies à partir de 47 honeypots, ce qui pourrait ne pas être représentatif de l'ensemble de l'Internet. De plus, l'évaluation des performances de la PKI4IoT et de la solution EDIMA a été effectuée sur un nombre restreint de dispositifs et de trafic de données générées de manière artificielle, ce qui souligne la nécessité de réaliser des tests à plus grande échelle pour confirmer leur efficacité.

7.3 Manque de données en temps réel

L'étude se concentre principalement sur l'analyse des botnets à partir des données passées, ce qui peut ne pas être indicatif des menaces actuelles. Les botnets évoluent rapidement et les données récentes pourraient donner un aperçu plus précis des menaces actuelles.

7.4 Limitation dans la compréhension des systèmes économiques du darkweb

Bien que l'étude analyse l'économie des botnets sur le darkweb, elle ne donne qu'un aperçu superficiel de ces systèmes complexes. Une analyse plus approfondie des mécanismes de prix, de la demande et de l'offre, et des facteurs influençant ces marchés souterrains pourrait être nécessaire pour une compréhension plus complète.

8 CONCLUSION

L'expansion de l'Internet des objets (IoT) a entraîné une augmentation alarmante des attaques par botnets, mettant en péril la sécurité des systèmes informatiques. Cette étude s'est intéressée à la corrélation entre l'évolution de l'IoT et l'émergence des botnets-as-a-service. Les résultats de nos recherches ont révélé plusieurs aspects préoccupants.

Tout d'abord, les botnets ont considérablement évolué au fil du temps, passant de simples outils de nuisance à des armes cybernétiques redoutables. Leur évolution a été marquée par des avancées techniques et des adaptations aux défenses de cybersécurité. Les botnets sont devenus polyvalents, capables de mener divers types d'attaques, tels que les attaques DDoS, le vol d'informations sensibles et le minage de crypto-monnaies.

En parallèle, les systèmes économiques autour des botnets ont également évolué. Les botnets sont désormais vendus ou loués sur le darkweb, ce qui les rend accessibles à un plus grand nombre d'acteurs malveillants. Les botnets "low-cost" ont également rendu ces attaques plus courantes, augmentant ainsi le nombre d'attaques DDoS.

La sécurité IoT pose de grands défis parce que de nombreux dispositifs connectés ne disposent pas de mesures de sécurité adéquates. Les utilisateurs sont négligents au sujet de la sécurité de leurs dispositifs, ce qui rend plus facile d'infecter et d'intégrer ces dispositifs dans les botnets. Toutefois, des efforts sont en cours pour développer des solutions de protection et de détection spécifiques à l'IoT, comme le protocole PKI4IoT et la solution EDIMA.

Des études supplémentaires sont nécessaires pour comprendre les mécanismes économiques entourant les botnets et pour perturber les marchés souterrains. De plus, des protocoles de sécurité adaptés à l'IoT doivent être développés et testés dans des environnements réels pour renforcer la protection des appareils connectés. Les solutions de détection des botnets, telles que la solution EDIMA, doivent également être évaluées dans des conditions réelles pour confirmer leur efficacité.

En conclusion, la montée en puissance des botnets-as-a-service est une préoccupation majeure dans le contexte de l'IoT. Il est essentiel de prendre des mesures pour renforcer la sécurité des appareils IoT, développer des stratégies de défense efficaces et poursuivre les recherches pour anticiper les futures menaces. La sécurité doit être une priorité absolue pour garantir la protection des systèmes informatiques et la confidentialité des utilisateurs dans un monde de plus en plus connecté.

REFERENCES

[1] Dimitrios Georgoulias, Jens Myrup Pedersen, Morten Falch, and Emmanouil Vasilomanolakis. 2023. Botnet Business Models, Takedown Attempts, and the Darkweb Market: A Survey. *Comput. Surveys* 55, 11 (2023), 219:1–219:39. https://doi.org/10.1145/3575808

[2] Kaifan Huang, Lu-Xing Yang, Xiaofan Yang, Yong Xiang, and Yuan Yan Tang. 2020. A Low-Cost Distributed Denial-of-Service Attack Architecture. *IEEE Access* 8 (2020), 42111–42119. https://doi.org/10.1109/ACCESS.2020.2977112 Conference Name: IEEE Access.

[3] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. 2017. DDoS in the IoT: Mirai and Other Botnets. *Computer* 50, 7 (2017), 80–84. https://doi.org/10.1109/MC.2017.201 Conference Name: Computer.

[4] Ayush Kumar, Mrinalini Shridhar, Sahithya Swaminathan, and Teng Joon Lim. 2022. Machine learning-based early detection of IoT botnets using network-edge traffic. *Computers & Security* 117 (June 2022), 102693. https://doi.org/10.1016/j.cose.2022.102693

[5] Steve Mansfield-Devine. 2017. Weaponising the Internet of Things. *Network Security* 2017, 10 (Oct. 2017), 13–19. https://doi.org/10.1016/S1353-4858(17)30104-6

[6] Artur Marzano, David Alexander, Osvaldo Fonseca, Elverton Fazzion, Cristine Hoepers, Klaus Steding-Jessen, Marcelo H. P. C. Chaves, Ítalo Cunha, Dorgival Guedes, and Wagner Meira. 2018. The Evolution of Bashlite and Mirai IoT Botnets. In *2018 IEEE Symposium on Computers and Communications (ISCC)*. 00813–00818. https://doi.org/10.1109/ISCC.2018.8538636 ISSN: 1530-1346.

[7] Natalija Vlajic and Daiwei Zhou. 2018. IoT as a Land of Opportunity for DDoS Hackers. *Computer* 51, 7 (July 2018), 26–34. https://doi.org/10.1109/MC.2018.3011046 Conference Name: Computer.