Architecture d'un BOTNET

Batany David

2019

1. Présentation de la menace

1.1 Définition

Le terme **botnet**, contraction de l'anglais **robot+net**, se définit par l'ensemble des programmes, machines, serveurs connectés à internet ayant un ou plusieurs processus commun de communication. Placé sous le contrôle d'un opérateur humain, appelé botmaster, le botnet recrute des machines en exploitant les vulnérabilités, failles, infections afin d'étendre son réseau à travers l'utilisation de canaux de Command and Control(C&C).
Avec l'IoT[1], et ses appareils connectés, le réseau s'étend de plus en plus au sein de notre société. L'actuelle faiblesse en terme de sécurité lié aux objets connectés représente une menace majeure et croissante dans notre environnement.

1.2 Historique

Le concept, inventé en 1988 à l'université de Oulu en Finlande, fut développé à l'origine pour gérer les services associés au protocole IRC[2].
Le premier bot "<GM"> assistait ainsi l'utilisateur dans la gestion des connections IRC. Cette gestion automatisée, permettant via un accès à distance, de contrôler et de réaliser des opérations a très vite montré un haut pouvoir malveillant.
En Mai 1999, Pretty Park, un malware de forme trojan horse se propageant sur le net permettait de voler les mots de passe.
Les premières dérives furent notamment l'affrontement de botnet IRC (Eggdrop en décembre 1993, puis GTbot en avril 1998).

1.3 Motivations liées à la menace botnet

1. L'aspect lucratif représente l'intérêt majeur pour l'utilisateur de botnet. L'automatisation d'une tâche contrôlée à distance permettant de rapporter facilement des revenus (revente d'information, fraude au clic, spam), surtout si celle-ci est réalisée de manière anonyme(réseau TOR[3]).
2. La motivation idéologique, comme par exemple, lors du conflit entre la Georgie et la Russie en 2008 ou de nombreux sites étatiques faisait l'objet de cyberattaques massives paralysaient les infrastructures.
3. La motivation personnelle, à travers la vengeance ou le chantage, est également une finalité grâce notamment au caractère anonyme de l'attaque.

1.4 Les type de menaces

Les botnets représentent les outils de diffusion des attaques. Cet outil permet aux cybercriminels de disposer d'un grand nombre de services développé dans un environnement collaboratif. Vendus sur le web, ils instrumentalisent l'attaque quelque soit le but recherché.
Liste des menaces possibles :

1. Internet of Things
2. Internet Relay Chat, un protocole de communication textuel
3. The Onion Routing, un réseau d'anonymisation

— Relayer du spam pour du commerce illégal ou pour de la manipulation d'information (par exemple des cours de bourse)
— Réaliser des opérations d'hameçonnage
— Identifier et infecter d'autres machines par diffusion de virus et de programmes malveillants (malwares)
— Participer à des attaques groupées de déni de service (DDoS)
— Générer de façon abusive des clics sur un lien publicitaire au sein d'une page web (fraude au clic)
— Capturer de l'information sur les machines compromises (vol puis revente d'information) ;
— Exploiter la puissance de calcul des machines ou effectuer des opérations de calcul distribué notamment pour cassage de mots de passe
— Voler des sessions utilisateurs par credential stuffing ;
— Mener des opérations de commerce illicite en gérant l'accès à des sites de ventes de produits interdits ou de contrefaçons via des techniques de fast flux, simple ou double-flux ou RockPhish
— Miner des cryptomonnaies, telles que le bitcoin1.

1.5 Cycle de vie d'une attaque :

Pour la compréhension,il est nécessaire de comprendre les différentes étapes depuis l'infection jusqu'au fonctionnement complet du botnet.

1.5.1 Infection de la machine

Cette première étape a généralement pour but de télécharger la charge virale sur un serveur. Elle peut être initiée via les vecteurs suivants :

— Par spam(existence de spambot)
— Exploitation de faille lié à la navigation sur un site web(malvertising [4], waterholing [5])
— P2P
— Spear phishing [6]
— SMS, MMS
— Bluetooth
— TDS [7]
— Exploit kits [8]

1.5.2 Activation

Après téléchargement, l'installation du malware peut établir un premier contact avec le botnet(serveur dédié, servant-bot) ayant une fonctionnalité de C&C. Le téléchargement de rootkit d'installation ou de DLL complémentaire finalise la mise en place du botnet sur la machine infectée.

1.5.3 Mise à jour

Les échanges permettent l'ajout de fonctionnalité, de configurations afin que le botnet puisse identifier et s'adapter à son environnement. Il peut, par exemple, vouloir modifier son hash [9] afin de conserver une certaine furtivité pour la continuité de l'attaque.

1.5.4 Auto-protection

La persistance et la dissimulation sont les facteurs clés de cette étape. L'installation de rootkit de protection, la modification du système, etc permettent de masquer l'action du botnet.

4. exploitation de pop-up publicitaires
5. ciblage de sites web fréquentés
6. hameçonnage ciblé pour récupérer données ou identifiants
7. Traffic Distribution Service, outil et service de redirection de trafic
8. plate-forme d'exploitation supporté par un site web permettant de tester une liste d'exploits
9. signature numérique, ici on parle de signature virale

1.5.5 Propagation

Cette phase d'extension est à la fois locale par du scan et distante par diffusion virale (mail avec lien ou pièce jointe).

1.5.6 Phase opérationnelle

Cette dernière phase vise à accomplir les actions souhaitées de l'attaquant. Déclenchées, synchronisées ou persistantes ces attaques s'adaptent aux cibles désignées.Ordonné par le C&C elles peuvent être activées ou mises en sommeil afin de ne pas attirer l'attention.

1.6 Les attaques

Liste des attaques utilisable par les botnets :

- Déni de service distribué (DDoS [10])
- DDoS contre paiement
- Récupération des identifiants
- Exposition médiatique ou démonstration de force
- Dissimulation d'une autre attaque
- Création d'un avantage concurrentiel
- Censure par attaque de serveurs
- Vengeance par cryptolocker
- Infrastructure d'anonymisation
- Recherche de vulnérabilités
- Infrastructure d'anonymisation des communications
- Contournement de mesures de limitation ou blocage
- Envoi de pourriels
- Diffusion de codes malveillants
- Exécution de codes malveillants sur les machines-zombies
- Hébergement de codes malveillants
- Fraude aux clics
- Compromission d'accès
- Brute force hors-ligne
- Brute force direct
- Cryptominage

2. Architecture du botnet

2.1 Architecture centralisée

2.1.1 Définition

Un ou plusieurs nœud de communication permettent aux bots d'échanger des données via un canal de communication. Les nœuds représentent un serveur ou serveur relais avec comme fonction le C&C.

2.1.2 Liste des protocoles utilisés par le botnet

- IRC [11]
- HTTP [12]
- IRC modifié

10. Distributed Denial of Service
11. Internet Relay Chat
12. HyperText Transfer Protocol

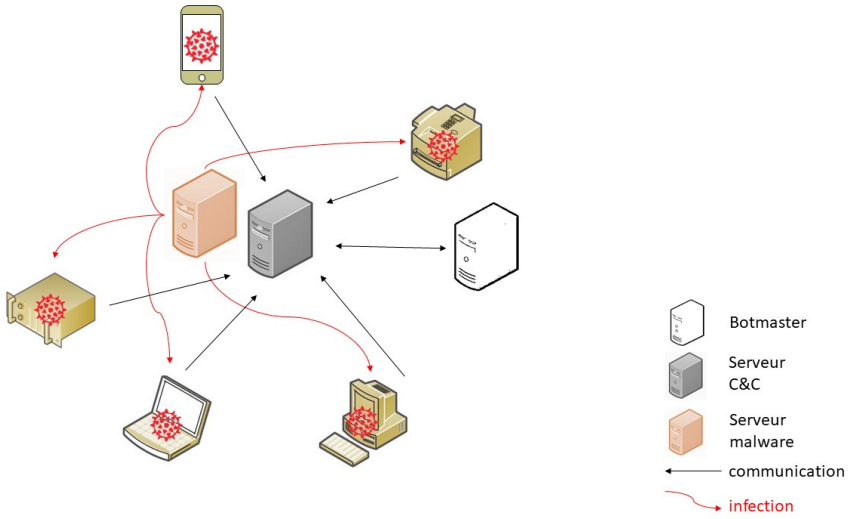

FIGURE 1 – Architecture centralisée

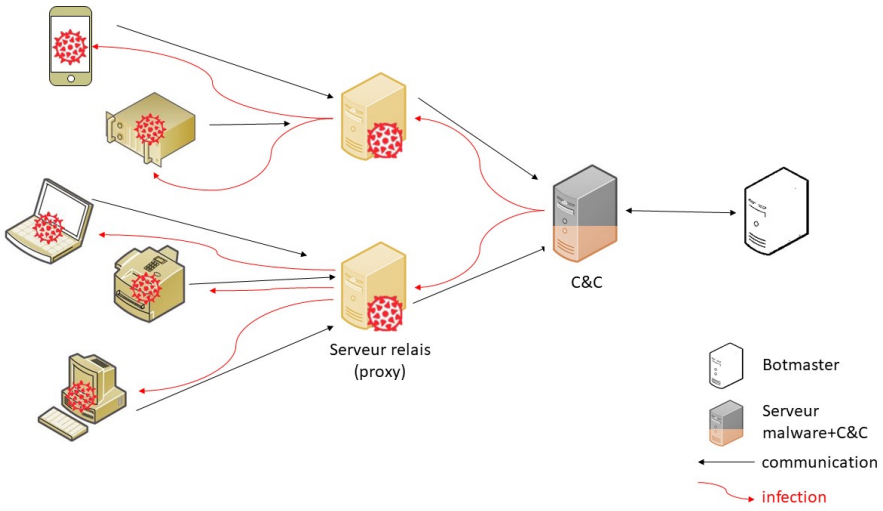

FIGURE 2 – Architecture centralisée répartie par utilisation d'une batterie de serveurs relais

2.1.3 Avantages

- Architecture centraliséee
- Simplicité de mise en oeuvre (mIRC, ...)
- Utilisation des canaux IRC (topics, messages) pour l'envoi des commandes vers les botsPerformance (non gourmant en bande passante)
- Connexions régulières entre les bots et le C&C (non-permanente)
- Recherche des ordres dans des forums, avec des mots clés ou même dans des images (stéganographie)

2.1.4 Inconvénients

- Vulnérabilité du botnet (serveur central)
- Connexion en permanence
- Facile à détecter (filtrage du flux IRC)

2.1.5 exemples

Nom du botnet	BEBLOH
Infection	Trojan
type de menace	Banking
type d'attaque	Spam
présence d'obfuscation	oui
Hash	54303e5aa05db2becbef0978baa60775858899b17a5d372365ba3c5b1220fd2e
Hash	03fe36e396a2730fa9a51c455d39f2ba8168e5e7b1111102c1e349b6eac93778
Hash	2b277c411944cb25bf454ad5dc38d32e8eed45eac058304982c15646720990cf
Domaines/URL	hxxps ://images2.imgbox(.)com/ca/88/A2ZSlW6S_o(.)png
Domaines/URL	(BEBLOHC&Cserver)hxxps ://oaril(.)com/auth/
Domaines/URL	hxxp ://lersow(.)com/images/beckky(.)exe

Nom du botnet	¯Kraken-Bobax
nombre de bots	400 000
Infection	worm
type de menace	¯DDos
type d'attaque	spam
présence d'obfuscation	oui
Hash	2dc0928de11577ed5ccf3679f4bd041a56a09494895d33462b02c873dd376515
Hash	c851d4bf3a939030fe8f5820042c98677b3472f36545dfff895e25645b0f9999
Hash	ac0558cfa97935e4dd1612e4f4a221c27bdba431aa5cc8f9696d83e7e4c5be77
Hash	b1deddb172b35a10160b1ba5f21be2071cd9d0c8b4312408bf408f79c010d836
Hash	ffced695fffc547abb70cd926f8d877a4e9326fa4c87415edb1d50d411871b50
Hash	00537fa963b668e5011c1166a6d418ec36d04d2b788f464e6e0f24d8a43b851b
Domaines/URL	.mooo.com
Domaines/URL	.dynserv.com
Domaines/URL	.dyndns.org
Domaines/URL	.yi.org
Domaines/URL	eoxjsnvzuh.mooo.com
Domaines/URL	jmyyptoo.dynserv.com
Domaines/URL	hrlgrh.dyndns.org
Domaines/URL	uvjvvqpjl.yi.org
Domaines/URL	20X.X9.34.132
Domaines/URL	1X3.2X5.15.189

2.2 Architecture décentraliséee

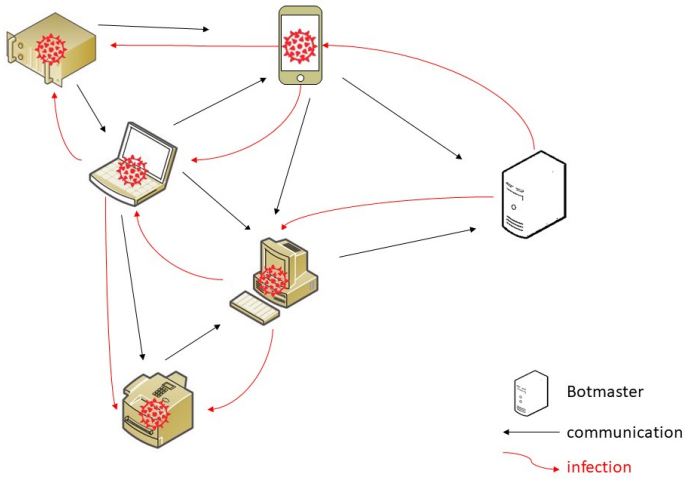

FIGURE 3 – P2P non structuré

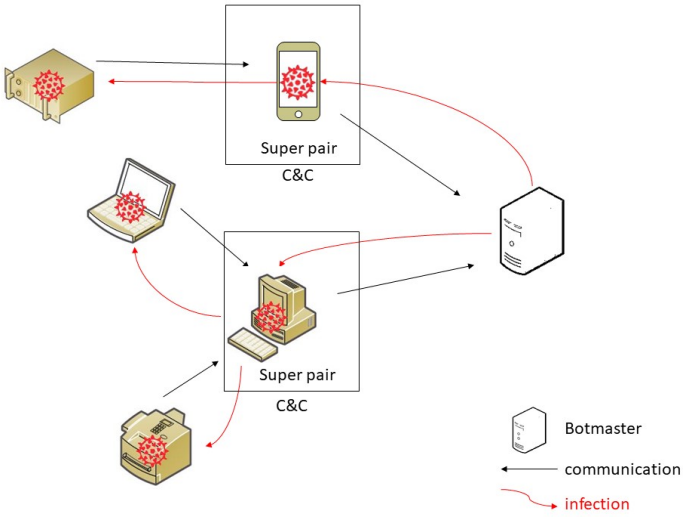

FIGURE 4 – P2P avec super-pairs

2.2.1 Définition

En utilisant des réseaux peer-to-peer, on s'affranchit d'un point central de communication.Chaque bot, selon ses caractéristiques, apporte les ressources pour élaborer le système de C&C. Il existe plusieurs typologies de réseau overlay [13] :

- **overlay P2P non-structuré** : les topologies sont aléatoires (loi de puissance, aléatoire uniforme,...)
- **overlay P2P par super-pairs** : tous les pairs du réseau ne sont pas égaux, certains d'entre eux étant automatiquement sélectionnés pour servir temporairement le rôle de serveur pour les recherches ou le contrôle du réseau (comme FastTrack ou Gnutella)
- **overlay P2P structuré** : une cartographie établissant le lien entre le contenu et son emplacement ; ce type de réseau implémente en général – mais pas systématiquement une table de hachage distribuée (DHT) ; on retrouve dans cette catégorie les protocoles P2P Chord, Tapestry et Kademlia (utilisé par le logiciel eMule).

2.2.2 Liste des protocoles utilisés par le botnet

- TCP/IP
- UDP

2.2.3 Avantages

- Architecture dé centraliséee
- Indépendant de l'architecture DNS
- difficile à repérer
- Connexions régulières entre les bots et le C&C (non permanente)
- Le botmaster donne les informations comme un bot faisant partie du réseau
- L'information transite de voisin en voisin
- très difficile à neutraliser

2.2.4 Inconvénients

- Pas de vision globale du réseau par un bot
- Connexion en permanence
- Facile à détecter (filtrage du flux IRC)

13. réseau logique de recouvrement

2.2.5 exemples

Nom du botnet	Storm
nombre de bots	85000
Infection	social engineering
type de menace	manipulation d'informations
type d'attaque	Spam DDoS
présence d'obfuscation	oui(XOR)
Hash	modification par la date du jour+checksum(32 combinaisons possibles / jour)
Domaines/URL	P2P

Nom du botnet	Qakbot
nombre de bots	
Infection	trojan banker(mutant)
type de menace	¯vol de renseignement personnel
type d'attaque	mail piégé
type d'attaque	brute force
présence d'obfuscation	
Hash	2E6AC2290F1E3D80ABC8D0D6F736D965
Hash	651EF2DBA96011F47EED9B72BE7B4B8C
Hash	F3CAA54DDE4056FADD52A024CF6B82ED
Domaines/URL	hxxp ://css.kbaf.myzen.co(dot)uk/TealeafTarget.php
Domaines/URL	hxxp ://projects.montgomerytech(dot)com/TealeafTarget.php
Domaines/URL	hxxp ://n.abcwd0.seed.fastsecureservers(dot)com/TealeafTarget.php

2.3 Architecture hybride

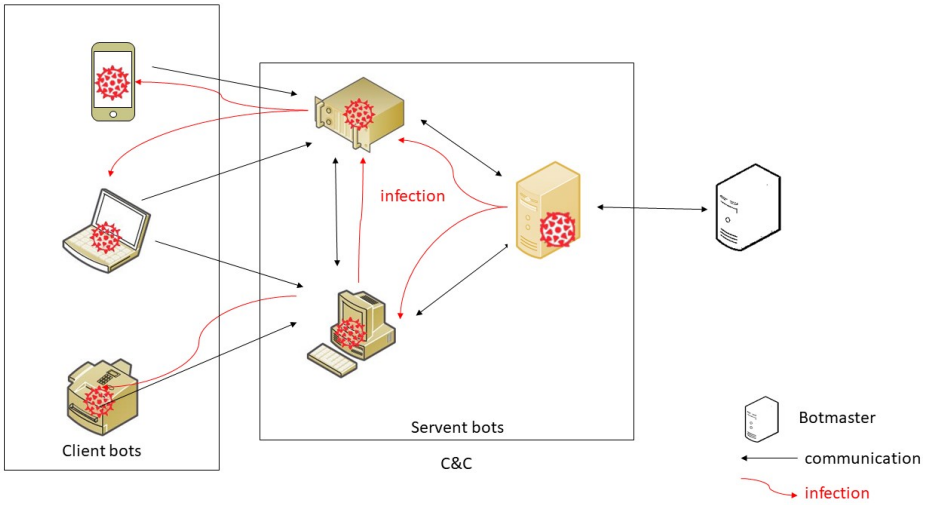

FIGURE 5 – Structure hybride P2P

2.3.1 Définition

Une architecture hybride intègre une solution de repli, comme à l'aide d'un DGA [14] ou de plusieurs niveaux successifs entre le P2P et le C&C.Cette hiérarchie permet de masquer une partie des adresses IP utilisées afin de rendre plus complexe l'analyse du botnet. L'association de bot clients et de bots servent [15] met en évidence l'organisation du réseau par le botmaster. Ces niveaux intermédiaires permettent de solidifier l'architecture du réseau.

14. Domain Generation Algorithm
15. serv-**eur** et cli-**ent**

2.3.2 Liste des protocoles utilisés par le botnet

Reprenant les protocoles présentés dans les architectures précédentes, L'efficacité, la furtivité et la complexité des méthodes de communication ont pour objectif de nuire aux efforts de démantèlement. Ainsi, les coopérations internationales entre acteurs institutionnels et privés sont généralement nécessaires pour permettre de démanteler les botnets les plus sophistiqués.

2.3.3 Avantages

— Nombre important de domaines

— masquage de l'adresse IP

2.3.4 Iconvénients

— tributaire de la bande passante

2.3.5 exemples

Nom du botnet	GameOver Zeus
nombre de bots	1 000 000
Infection	trojan et Cryptolocker
type de menace	vol de mot de passe/données bancaires et ransomware
type d'attaque	spam
présence d'obfuscation	
Hash	5e5e46145409fb4a5c8a004217eef836
Hash	ddc013410b944092c1eeb39699504dbfc6a90146632c93b0a6085b16aa65e802
Hash	30e2024f544fe8d904502cafd614d1fbfb30d428367a23757f2639dee0aa3cc6
Hash	6c8a03895665575619a6193d342cdc79500680971ff4398c62a2d6e84188f49a
Domaines/URL	P2P(1000 par jour)
Domaines/URL	cfs50p1je5ljdfs3p7n17odtuw.biz

Nom du botnet	Mirai
nombre de bots	300 000
Infection	brute force login d'IoT
type de menace	DDos
type d'attaque	envoi de paquets de données
présence d'obfuscation	
Hash	modification du hash(32000 variantes)
Domaines/URL	kankerc.queryhost.xyz 192.69.89.173 C2 server
Domaines/URL	kankerc.queryhost.xyz 154.16.199.34 C2 server
Domaines/URL	report.queryhost.xyz 192.69.89.173 report server
Domaines/URL	report.queryhost.xyz 45.32.186.11 report server
Domaines/URL	dongs.disabled.racing 93.158.200.126 malware distribution

2.4 Architecture aléatoire

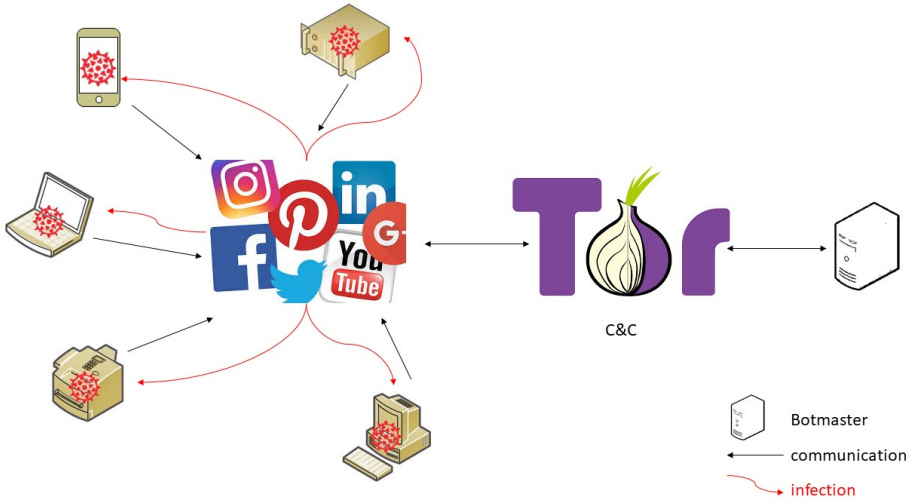

FIGURE 6 – Architecture aléatoire

2.4.1 Définition

Ce concept représente une variante de l'architecture centraliséee et peut se retrouver dans une variété de malware connue sous le nom de RATs [16].Ces chevaux de Troie fonctionnent sur un principe de client/serveur parfois mis en place avec des techniques de social engineering (exemple : un fichier d'installation récupéré sur un site douteux). Ils exécutent la partie client à l'insu de l'utilisateur pour se connecter au serveur.
Cette architecture tire profit de l'exploitation de plate-formes existantes supportant le protocole HTTP comme Facebook, Twitter, Yahoo, Evernote, Google, etc. et de réseau permettant de camoufler les échanges comme TOR, Hornet, etc.

2.4.2 Liste des protocoles utilisés par le botnet

- HTTP
- protocole propriétaire (exemple XMPP [17])
- IRC

2.4.3 Avantages

- Architecture déjà existante
- Réseau important en terme d'utilisateurs
- Utilisation des canaux existants (exemple : messagerie instantanée)
- utilisation des fonctionnalités du réseau (exemple :Le réseau anonymisation TOR)
- Difficulté de démanteler son propre réseau

2.4.4 Inconvénients

- Vulnérabilité du botnet face aux mécanismes de défense
- Connexion en permanence
- bloqué par le filtrage de liens de la plate-forme

16. Remote Access Trojan
17. Extensible Messaging and Presence Protocol de MSN Messenger

2.4.5 exemples

Nom du botnet	Cutwail via Pushdo
nombre de bots	125000
Infection	Trojan(mutant)
type d'attaque	¯spam
présence d'obfuscation	oui (XOR)
Hash	5F8FCC9C56BF959041B28E97BFB5DB9659B20A6E6076CFBA8CB2D591184C9164
Domaines/URL	4darabians.nl 4dbenelux.be accords-bilateraux.ch
Domaines/UR	4elementos.cl 4-elements.ch 4elements.de accounting.ee
Domaines/UR	4elements.hu 4-elements.se 4emails.de 0daymusic.biz
Domaines/UR	wellesley.ca 8zsmost.cz 4enerchi.nl 0handicap.at
Domaines/UR	4entertainmentgroup.tv 4ernila.de 4e-solutions.ch

Nom du botnet	carna
nombre de bots	420 000
Infection	Scan
type de menace	challenge personnel
type d'attaque	RAT (Telnet)
présence d'obfuscation	non
Hash	système de floutage et du modification du hash (32000 variantes trouvées)
Domaines/URL	kankerc.queryhost.xyz 192.69.89.173 C2 server
Domaines/URL	kankerc.queryhost.xyz 154.16.199.34 C2 server
Domaines/URL	report.queryhost.xyz 192.69.89.173¯report server
Domaines/URL	report.queryhost.xyz 45.32.186.11 report server
Domaines/URL	dongs.disabled.racing 93.158.200.126 malware distribution

3. Les méthodes de lutte adaptées au réseau

Lutter contre les botnets est possible à travers 4 étapes :

3.1 La détection

Recherche d'anomalie, comparaison de signatures, pots-de-miel, toutes ces techniques basées sur l'activité du réseau reposent sur l'inspection des flux et des paquets.

3.1.1 La détection passive

L'identification et l'analyse passive des flux (adresses IP,port source et destination, étiquette MPLS [18], etc.) permettent de classifier les protocoles suspects et les serveurs de C&C.
BotFinder, par exemple, permet de décomposer un flux (durée moyenne des connexions, nombre d'octets transférés, etc.) et de le comparer à l'activité normale du réseau.
L'observation des DNS [19] permet aussi d'identifier les domaines malveillants afin de caractériser le botnet suspecté. BotGad, un système d'exploitation permettant d'analyser le trafic DNS sur un réseau local, utilise un algorithme basé sur l'apprentissage afin de définir la stratégie de groupe du botnet.
EXPOSURE, un autre système d'exploitation déployé au sein de l'ISP [20], permet d'analyser à large échelle mais sur une durée de plusieurs mois le trafic DNS. Produisant une liste de domaines malveillants, il permet, par exemple, d'identifier un volume conséquent de requêtes pour un même domaine.
Enfin le recours aux pots-de-miel et l'analyse des journaux d'activité sont les éléments de base d'une recherche d'activité liée aux botnets. Suivant cette idée, le SIEM [21], une solution de gestion de la sécurité, représente un outil précieux et novateur afin d'optimiser la veille du trafic et d'automatiser les processus de sécurité en cas de comportement anormal.

18. MultiProtocol Label Switching
19. Domain Name Server
20. Internet Service Provider
21. Security Information and Event Management

3.1.2 La détection active

Différentes techniques existent comme le sinkholing [22] redirigeant le trafic vers des serveurs afin de simuler le comportement du C&C et de diminuer la puissance du réseau du botnet.
L'infiltration, fonction de l'architecture du botnet, consiste à simuler le comportement d'un botnet contrôlé à l'aide de drones IRC ou de script afin de capturer le trafic et de remonter jusqu'au botmaster. Le projet Pebbletrace reprend cette idée d'identification du botmaster en piégeant les équipements infectés avec une charge défensive afin de retourner le trafic contre le botnet.

3.2 L'analyse

3.2.1 L'analyse statique

Réalisée en sandbox, sur une machine virtuelle ou une machine dédiée avec des outils préinstallés comme InetSim,FakeNet ou Mozzle, elle débute par une analyse statique pour identifier les éléments et la composition du malware. L'examen du code et des fonctions appelées permettent d'évaluer les capacités du botnet.

3.2.2 L'analyse dynamique

Cette étape est relativement utile pour la compréhension de la menace car elle présente la machine infectée sous plusieurs états à l'aide de snapshots [23]. Ces captures instantanées situent l'avancement de l'infection lors de l'attaque. Il est souvent nécessaire en présence d'algorithme chiffré d'utiliser cette méthode pour désobfusquer le code et comprendre la structure du malware.

3.3 La défense et le blocage

Au même titre que la protection contre les malwares, les recommandations en terme de SSIrecommandations ANSSI, applicables localement, doivent s'inscrire dans nos habitudes et augmentent ainsi la probabilité de bloquer l'étape initiale de l'infection (spam, navigation non-sécurisée,etc.).
Les mises à jour logicielles et système sont essentielles pour bloquer l'exploitation de CVE [24] Common Vulnerabilities and Exposures.
Au niveau du FAI, les notifications en cas de connexions malveillantes et la surveillance des adresses IP sont un frein à l'extension du botnet.
Enfin la détection d'un appel de fonctions anormal par l'antivirus, l'autorisation et l'identification des flux sortants par le firewall permettent le blocage de l'activité malveillante. Les fonctionnalités recherchées de l'antivirus dans ce cadre sont un firewall bidirectionnel, une protection contre le phishing, la vérification de la certification, la lutte contre le tracking, la vérification du téléchargement, le blocage des pop-ups et pages WEB malveillantes,etc.

3.4 Le démantèlement

Les méthodes de détection impliquent parfois des actions offensives visant à entraver le développement du botnet. Il est cependant nécessaire d'avoir un support juridique et judiciaire pour mener à bien des actions adaptées au type et à la taille du botnet. Celles-ci sont généralement menées en coopération avec les industriels (Microsoft,Level 3, Cisco,etc.) et la communauté scientifique.

4. Conclusion

Les botnets font maintenant partie d'une économie souterraine sous forme de services payants. Le harcèlement, le vol, les attaques par déni de service, etc figurent comme des produits de vente accessibles, moyennant finances, pour n'importe quel criminel.
D'après l'ENISA [25] les prix varient suivant la fiabilité, la durée et le type de service requis. Par exemple une heure de DDoS est disponible pour 38$. Les différentes architectures permettent de mieux comprendre l'organisation du botnet et l'importance du C&C.

22. également appelé serveur gouffre, gouffre Internet ou Blackhole DNS
23. copie des données/modifications apportées à un système
24. Common Vulnerabilities and Exposures
25. European Union Agency for Cybersecurity, anciennement European Network and Information Security Agency

Les notions de veille technologique et de partage d'informations sur la menace sont essentielles du fait de l'implication du botnet dans les réseaux publiques et privés.
Dans le cadre du renseignement lié aux menaces, les constructeurs de smartphone fournissent les informations (recherches,cible des attaques, menaces associés aux mobiles, vulnérabilités des objets IoT) issues de leurs Threat Intelligence Center [26].

Selon Nokia (Nokia's Threat Intelligence Report, l'activité des botnet sur l'IoT représente 78% des événements de détection de malware en 2018.
La menace omniprésente de ces objets connectés (santé, domotique, médias, électroménager,...) n'est aujourd'hui pas assez prise en considération par notre société de consommation. Le manque de sécurité accrue de ces appareils faits apparaître ces objets connectés comme des acteurs potentiels constituant le réseau d'un botnet.
L'arrivée prochaine de la 5G [27] sera, dans ce domaine, un vecteur majeur pour la diffusion de l'infection du malware et le nombre d'attaques associés au botnet (exemple attaques DDoS).

FIGURE 7 – Figure 1

26. Centre de renseignements liés aux menaces cyber
27. prévisions en moyenne 100Mbit/S en download et 50 Mbit/s en upload