1. Quelques éléments techniques des attaques

Afin d'illustrer les menaces et les attaques, je vous propose de présenter avec un peu de détails quelques éléments techniques utilisés dans le cadre d'attaques informatiques classiques comme.

- Botnet ;
- Banker ;
- Rançon-logiciel ;
- Techniques des malware ;
- Command and control.

toutefois, il est important de connaitre les grandes stratégies des attaquants. En particulier les mécanismes de Kill Chain. Issu de la terminologie militaire ces éléments caractérisent et décrivent les mécanismes d'attaques.

2. Botnet, des codes malveillants organisés

.

A titre d'illustration, je vous propose de découvrir les botnets avec les travaux de David Batany. Les Botnets font partis de ce que nous pourrions appeler des architectures techniques malveillantes. En effet, un Botnet en lui même est un code malveillant qui fonctionne dans une architecture informatique complexe avec des mécanismes de pilotage, de stockage, de réplication et d'activation spécialisées. Un Botnet est peut être considéré comme un système d'arme utilisable pour des attaques.

2.1 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 liée aux objets connectés représente une menace majeure et croissante dans notre environnement. **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.

1. Internet of Things
2. Internet Relay Chat, un protocole de communication textuel

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). **Motivations liées à la menace botnet**

- 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]).
- La motivation idéologique, comme par exemple, lors du conflit entre la Georgie et la Russie en 2008 ou de nombreux sites étatiques faisant l'objet de cyberattaques massives paralysaient les infrastructures.
- La motivation personnelle, à travers la vengeance ou le chantage, est également une finalité grâce notamment au caractère anonyme de l'attaque.

2.2 Les utilisations des Botnets

On peut citer les attaques classiques utilisant des techniques de botnets :

- Déni de service distribué (DDoS[4]) ;
- DDoS contre paiement ;
- Cryptominage ;
- 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 (Spam) ;
- 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 ...

3. The Onion Routing, un réseau d'anonymisation
4. Distributed Denial of Service

2.3 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.

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 [5], waterholing [6])
- P2P
- Spear phishing [7]
- SMS, MMS
- Bluetooth
- TDS [8]
- Exploit kits [9]

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 Dynamic Loads Library (DLL) complémentaire finalise la mise en place du botnet sur la machine infectée.

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 [10] afin de conserver une certaine furtivité pour la continuité de l'attaque.

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.

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

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.

2.4 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 développés dans un environnement

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

collaboratif. Vendus sur le web, ils instrumentalisent l'attaque quelque soit le but recherché.
Liste des menaces possibles :

- 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.

2.5 Architecture aléatoire

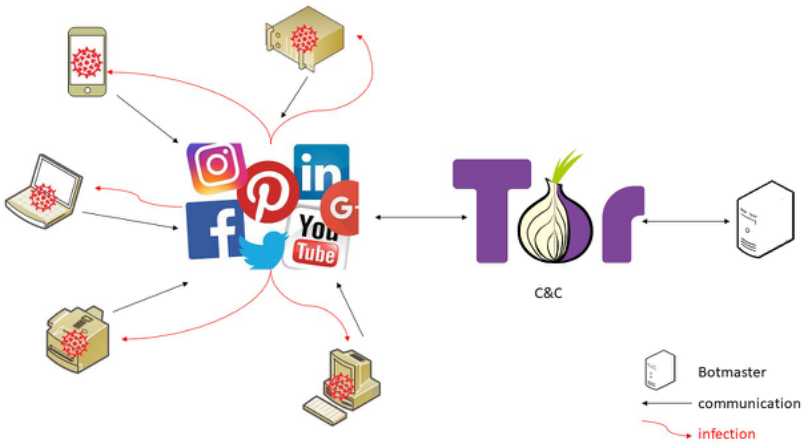

FIGURE 1. Architecture aléatoire

2.5.1 Définition

Ce concept représente une variante de l'architecture centralisée et peut se retrouver dans une variété de malware connue sous le nom de RATs [11].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.

2.5.2 Liste des protocoles utilisés par le botnet

- HTTP
- protocole propriétaire (exemple XMPP [12])
- IRC

2.5.3 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

11. Remote Access Trojan
12. Extensible Messaging and Presence Protocol de MSN Messenger

2.5.4 Inconvénients

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

2.5.5 exemples

2.6 Architecture centralisée

2.6.1 Définition

Un ou plusieurs nœuds 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.

2.6.2 Liste des protocoles utilisés par le botnet

- IRC [13]
- HTTP [14]
- IRC modifié

2.6.3 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)

2.6.4 Inconvénients

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

13. Internet Relay Chat
14. HyperText Transfer Protocol

2.7 Architecture décentraliséee

2.7.1 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 [15] :

- **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).

2.7.2 Liste des protocoles utilisés par le botnet

- TCP/IP
- UDP

2.7.3 Avantages

- Architecture décentralisée
- 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

2.7.4 Inconvénients

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

15. réseau logique de recouvrement

2.8 Architecture hybride

2.8.1 Définition

Une architecture hybride intègre une solution de repli, comme à l'aide d'un DGA [16] 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 [17] met en évidence l'organisation du réseau par le botmaster. Ces niveaux intermédiaires permettent de solidifier l'architecture du réseau.

2.8.2 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.

2.8.3 Avantages

- Nombre important de domaines
- masquage de l'adresse IP

2.8.4 Iconvénients

- tributaire de la bande passante

2.8.5 exemples

2.9 L'analyse

2.9.1 L'analyse statique

Réalisée en sandbox, sur une machine virtuelle ou une machine dédiée avec des outils pré-installés 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.

2.9.2 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 [18]. Ces captures instantanées situent l'avancement de l'infection lors de l'attaque. Il est souvent nécessaire en présence

16. Domain Generation Algorithm
17. serv-**eur** et cli-**ent**
18. copie des données/modifications apportées à un système

d'algorithme chiffré d'utiliser cette méthode pour désobfusquer le code et comprendre la structure du malware.

2.10 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 [19] 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 anormales 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.

2.11 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.

2.12 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.

2.12.1 La détection passive

L'identification et l'analyse passive des flux (adresses IP,port source et destination, étiquette MPLS [20], 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 [21] 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.

19. Common Vulnerabilities and Exposures
20. MultiProtocol Label Switching
21. Domain Name Server

EXPOSURE, un autre système d'exploitation déployé au sein de l'ISP [22], 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 [23], 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.

2.12.2 La détection active

Différentes techniques existent comme le sinkholing [24] 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.

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.

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, cibles 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 fait apparaître ces objets connectés comme des acteurs potentiels constituant le réseau d'un botnet.

22. Internet Service Provider
23. Security Information and Event Management
24. également appelé serveur gouffre, gouffre Internet ou Blackhole DNS
25. European Union Agency for Cybersecurity, anciennement European Network and Information Security Agency
26. Centre de renseignements liés aux menaces cyber

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).

3. Malware

3.1 Malware industriel : citadel

Les créateurs du malware Citadel ont adopté un modèle de développement Open Source qui leur permet de corriger collectivement les bugs et d'ajouter plus rapidement des fonctionnalités à leur logiciel malveillant. Citadel est basé sur ZeuS, l'un des plus anciens et des plus populaires Cheval de Troie mis au point pour pirater les services bancaires en ligne. Zeus a été abandonné par son créateur fin 2010, mais quelques mois plus tard, le code source de son malware a été diffusé sur le Net. Depuis la publication de son code source, Zeus a servi de base au développement d'autres Trojan comme Ice IX, et Citadel. « Le 17 décembre 2011, pour la première fois, un laboratoire de recherche (Seculert) a mis en évidence l'existence d'un botnet Citadel, » a déclaré le spécialiste de la sécurité dans un blog. « Le taux d'adoption et le développement de ce malware est en pleine expansion. » Seculert dit avoir identifié plus de 20 réseaux de zombies utilisant des versions différentes du Cheval de Troie. « Chaque version comporte de nouveaux modules et de nouvelles fonctionnalités, certaines proposées par les clients de Citadel eux-mêmes, » a indiqué l'entreprise de sécurité. L'aspect le plus intéressant de ce malware est sans aucun doute le processus adopté pour son développement. Les modalités de développement adoptées pour Citadel ressemblent à celles des communautés supportant des projets Open Source. « L'organisation est calquée sur le développement des logiciels courants : les créateurs de Citadel fournissent à leurs clients un manuel utilisateur, des avis donnant des détails sur les mises à jour et même un contrat de licence.

Acronymes

DLL Dynamic Loads Library. 3

27. prévisions en moyenne 100Mbit/S en download et 50 Mbit/s en upload

Table des matières

Table des figures