TLP:WHITE

ÉTAT DE LA MENACE LIÉE AUX BOTNETS

Version 2.0.4

04/11/2019

TLP:WHITE

Sommaire

1 Synthèse

Les botnets, réseaux de machines infectées et contrôlées à l'insu de leurs propriétaires légitimes, peuvent être utilisés comme outil afin de mener différents types attaques informatiques. Il apparait cependant que la finalité lucrative est la principale motivation au déploiement de botnets. Les attaques par déni de service distribuées (DDoS) correspondent à une utilisation caractéristique des botnets, mais ceux-ci sont également utilisés à des fins d'anonymisation, de distribution de pourriels, de diffusion de codes malveillants, de fraude, de découverte d'identifiants ou pour miner des cryptomonnaies. Pour mener les attaques, les botnets tirent notamment profit des nombreux points d'accès au réseau et/ou exploitent la puissance de calcul usurpée aux machines infectées.

Les codes malveillants à l'origine des infections des machines rattachées à un botnet sont très nombreux. Ceux-ci n'ont cependant pas nécessairement été développés par les mêmes acteurs que les opérateurs des botnets qui les utilisent. Ces codes font régulièrement l'objet de modifications ou de mises à jour, dans une logique de concurrence entre des acteurs qui en sont à l'origine. En effet, le caractère lucratif de l'utilisation de botnet pourrait expliquer l'environnement hautement concurrentiel dans lequel évoluent leurs opérateurs. Une surface toujours croissante d'appareils connectés est ainsi ciblée.

Une caractéristique fondamentale des botnets est la capacité pour leurs opérateurs de faire exécuter des instructions par les machines infectées. Le maintien des communications avec les machines compromises semble ainsi être la priorité de nombreux botnets. Des mécanismes de redondance de plus en plus complexes ont ainsi été observés comme l'utilisation d'algorithmes de génération de noms de domaines, des architectures en pair-à-pair ou l'utilisation du réseau d'anonymisation TOR. Cette complexification des méthodes de communication nuit ainsi grandement aux efforts de démantèlement. Ainsi des coopérations internationales entre acteurs institutionnels et privés sont généralement nécessaires pour permettre de démanteler les botnets les plus sophistiqués.

2 Définition d'un Botnet

Au sens le plus large, un botnet, ou « réseau zombie », est défini comme un ensemble de ressources informatiques capable d'exécuter des opérations ordonnées, via un réseau informatique, par une infrastructure de commande et de contrôle. Une acception plus restreinte, utilisée dans cette production, désigne **un réseau d'un grand nombre de machines contrôlées à l'insu de leurs propriétaires, capables de mener des actions offensives coordonnées.**

Le contrôle du réseau de machines composant un botnet se fait généralement via un code malveillant permettant un accès à distance. Si, par métonymie, le premier réseau découvert faisant usage d'un nouveau logiciel se voit habituellement attribuer le même nom que le logiciel, **c'est le contrôle des machines depuis une infrastructure commune qui fait l'unité d'un botnet**. Ainsi, des réseaux reposant sur un même code malveillant et une organisation identique composeront des botnets distincts s'ils ne sont pas opérés de manière unifiée. Inversement, le contrôle unifié de machines infectées par des codes malveillants distincts ne forme qu'un botnet.

Les machines infectées faisant partie d'un botnet sont parfois qualifiées de « zombies », alors que celles utilisées pour contrôler un botnet sont désignées comme machines, serveurs ou infrastructure « de commande et de contrôle », abrégé « C2 ». Suivant les cas, le terme "*bot*" peut désigner les machines-zombies ou le code malveillant permettant leur contrôle [1]. Les machines zombies peuvent être des ordinateurs, mais également tout type de machine disposant d'une connexion réseau : des serveurs web, des routeurs, des téléphones, des caméras de surveillance, des terminaux GPS avec gestion du trafic... et plus largement tout objet connecté (voir « l'Internet des objets » 5.1).

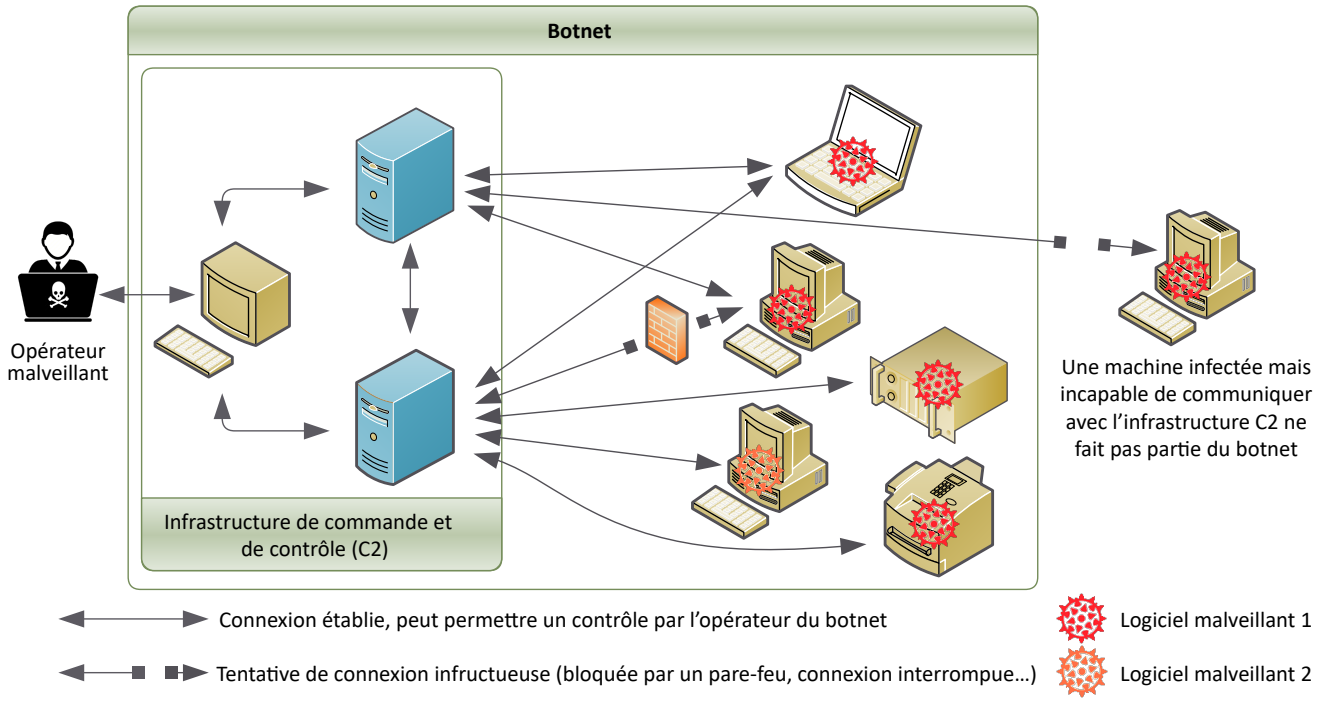


Fig. 2.1 : Schéma d'un botnet impliquant deux logiciels malveillants et infectant divers types de matériels.

La mise en place d'un botnet n'est généralement pas une fin en soi, mais **une manière de créer un outil destiné à mener des attaques informatiques**. Le contrôle distant de machines-zombies donne aux opérateurs de botnets l'accès à **deux ressources cruciales : des points d'accès distincts au réseau et de la puissance de calcul**. Un attaquant disposant d'un grand nombre de points d'accès au réseau peut en faire usage pour saturer les ressources de ses victimes et contourner certaines mesures défensives, en particulier les mesures de filtrage par adresse IP. L'usurpation de la puissance de calcul permet quant à elle d'en profiter sans avoir à en assumer les dépenses liées. De plus, les logiciels de contrôle de ces machines-zombies ont généralement la capacité d'installer des codes malveillants additionnels sur celles-ci, ce qui permet de mener des campagnes d'infection.

Selon de nombreux rapports publics [2, 3], les botnets sont considérés comme l'une des principales sources de me-

naces en cybersécurité. En effet, des articles universitaires estiment que près d'un ordinateur sur cinq connecté à internet pourrait faire partie d'un ou plusieurs botnets [4]. De plus, les plus grands botnets auraient rassemblé plusieurs millions de machines-zombies.

Commentaire: L'administration par une entité unique d'un grand nombre de comptes utilisateurs sur des services en ligne, par exemple Twitter, afin de simuler des actions d'internautes distincts est parfois appelée « botnet ». Le contrôle de multiples comptes sur un service en ligne est de nature trop éloignée du contrôle à l'insu de leurs utilisateurs de machines compromises et ne sera pas traité dans ce document.

3 Principales utilisations des botnets

La mise en place et le contrôle d'un botnet peut permettre, faciliter, accélérer ou amplifier la conduite de nombreux types d'attaque, dont une partie est détaillée ici.

3.1 Déni de service distribué (DDoS)

Les attaques par déni de service (*Denial of Service* - DoS) ont pour but de rendre indisponible une ressource pour son audience légitime en saturant ses capacités de réponse aux demandes. Lorsque les origines de ces requêtes sont multiples et coordonnées, comme dans le cas d'une attaque depuis un botnet, l'attaque est alors qualifiée de déni de service distribué (DDoS).

L'ampleur des attaques DDoS est généralement mesurée par le débit de données reçues par les cibles lors des attaques. Il est par ailleurs à noter que les canaux de transport des communications vers la cible peuvent également être victime d'une saturation, engendrant alors des dommages collatéraux.

3.1.1 DDoS contre paiement

Une attaque DDoS peut avoir pour objectif un enrichissement aux dépens de la victime ciblée.

Chantage au DDoS

Cette méthode consiste à menacer une cible d'attaques DDoS si celle-ci refuse de payer une rançon. Cela peut faire suite à une première attaque, mais des demandes de paiement par des attaquants n'ayant pas démontré leurs capacités . Les secteurs du jeu vidéo et des paris en ligne seraient les principaux secteurs touchés par ces attaques [5].

Vente de protection anti-DDoS frauduleuse

La proposition de vente de protection face à une menace créée de toute pièce est un mode opératoire utilisé par de nombreux acteurs malveillants, en particulier des groupes mafieux. À l'instar d'acteurs légitimes proposant des services de mitigation face aux attaques DDoS, certains acteurs malveillants proposent des services, présentés comme légitimes, mais ne consistant effectivement qu'en un arrêt de leur propre attaque. Les auteurs du botnet Mirai (voir 5.1) ont ainsi reconnu avoir eu recours à de telles pratiques [6].

3.1.2 Exposition médiatique ou démonstration de force

L'interruption d'un service peut avoir pour but une exposition médiatique, afin de faire passer un message ou de démontrer une capacité. La motivation peut être idéologique, comme dans le cas des attaques DDoS à l'encontre de sites institutionnels autrichiens entre septembre et février 2017, revendiquées par un groupe dénonçant la diplomatie autrichienne à l'égard de la Turquie et des musulmans. D'autres attaques peuvent avoir pour but de démontrer le pouvoir de nuisance de leur auteur. Ainsi, selon le journaliste américain spécialisé dans la cybersécurité Brian Krebs, la réussite d'une attaque DDoS contre son site Internet aurait été requise pour accéder à un forum Internet d'attaquants informatique [7].

Dans une dimension plus stratégique, certains analystes ont considéré que les DDoS ayant ciblé l'Estonie en 2007 avaient aussi pour objectif la démonstration des capacités offensives des acteurs à leur origine, le gouvernement russe étant largement pointé du doigt en source ouverte [8].

3.1.3 Dissimulation d'une autre attaque

Les attaques DDoS peuvent avoir pour but de masquer une autre attaque. La saturation du système d'information ciblé rend plus difficile la détection de marqueurs de compromission parmi les nombreuses alertes générées et surtout peut détourner l'attention des équipes de sécurité. De plus, ce type d'attaque peut être utilisé afin d'évaluer les capacités de réaction de leurs cibles.

3.1.4 Création d'un avantage concurrentiel

La forte concurrence entre les acteurs opérant sur Internet permet aux clients de se reporter rapidement sur des concurrents en cas d'indisponibilité ou de lenteur d'un service en ligne. Des attaques DDoS peuvent ainsi avoir pour objectif de réorienter les utilisateurs éventuels vers un service concurrent.

Le ciblage particulièrement important du secteur de l'industrie pornographique, des jeux en ligne [9] et des sites spécialisés dans la vente ou l'échange de cryptomonnaies [5] semble ainsi être lié à cet objectif.

3.1.5 Censure

L'indisponibilité d'un site Internet pourrait aussi être recherchée pour restreindre l'accès à une source d'information. Le journaliste Brian Krebs dit avoir été victime de nombreuses attaques par DDoS. Cette expérience l'a entrainé à considérer ce type d'attaque comme des sources possibles de censure à l'encontre de sites d'information [10]. Par ailleurs, certains sites ayant fourni des informations à même de contourner les restrictions d'accès imposées aux internautes chinois ont été victimes d'afflux soudain et massif de trafic en provenance de la Chine. L'indisponibilité qui en a résulté a été interprétée par certains comme une forme de censure ou de représailles provenant d'entités liées au gouvernement chinois [11]. **L'hypothèse de telles attaques à l'encontre de grands médias, en particulier lors de situations de crise, pourrait favoriser des campagnes de désinformation. Des attaques à l'encontre de systèmes de vote en ligne pourraient également avoir de graves conséquences sur le déroulement d'une élection.**

3.1.6 Vengeance

Enfin, dans certains cas, la volonté de nuire par vengeance peut être à l'origine de l'attaque. Ainsi, un rapport de Kaspersky décrit le cas d'un DDoS déclenché par un individu mécontent à l'encontre de son ex-employeur [12].

3.2 Infrastructure d'anonymisation

3.2.1 Recherche de vulnérabilités

De nombreux botnets intègrent des fonctions de reconnaissance de vulnérabilités utilisées afin d'infecter des machines zombies supplémentaires et ainsi agrandir le botnet. L'intégration de machines d'intérêt lors de ces reconnaissances massives permet de noyer les vulnérabilités recherchées et les objectifs ciblés dans la masse des requêtes. Les informations sur les machines vulnérables identifiées peuvent alors être transmises aux opérateurs afin de permettre une attaque ciblée. Le botnet prend alors un rôle de plateforme d'anonymisation et d'automatisation de ces recherches.

3.2.2 Infrastructure d'anonymisation des communications

Dans d'autres cas, le botnet peut être utilisé comme un vaste réseau de serveurs mandataires[1]. Le botnet Black aurait ainsi déployé des serveurs mandataires sur plus de 100 000 machines en 2018 [13, 14].

3.2.3 Contournement de mesures de limitation ou blocage

Les botnets peuvent également être utilisés pour contourner des mesures de blocage ou de limitation destinées à limiter les abus sur des services Internet légitimes. En cas de blocage de l'adresse IP utilisée pour accéder au service, la sélection d'une autre machine compromise permet de contourner la mesure.

Un cas d'usage notable est l'utilisation d'un botnet pour contourner les mesures de blocage mises en place par des sites d'actualité ou de réseaux sociaux pour lutter contre « l'astroturfing », une pratique consistant à simuler des réactions issues de personnes indépendantes, afin de laisser croire à une prise de position de la part d'une population [15].

3.3 Envoi de pourriels

L'envoi de courriels non sollicités, à caractère publicitaire ou dans le cadre d'une campagne d'hameçonnage[2], est une autre activité particulièrement répandue des botnets. En effet, de nombreux services de protection contre les pourriels fonctionnent par l'ajout sur liste noire des principales sources de pourriels. Ainsi, les opérateurs chargés de leur envoi chercheraient à profiter du grand nombre d'adresses IP fournies par les botnets afin d'éviter de telles mesures de blocage. Les botnets spécialisés seraient capables de n'utiliser qu'une partie des machines pour une campagne donnée, afin de compliquer le décompte et l'identification des machines infectées à un moment donné. L'envoi de pourriels semble se concentrer sur quelques botnets spécialisés. Ainsi, un rapport de la société Talos de janvier 2018 [16] affirme que certaines campagnes du botnet Necurs seraient responsables de près de 90% des envois de pourriels observés par l'éditeur en une journée.

Les botnets peuvent aussi être utilisés pour parcourir le web afin de collecter des adresses de messagerie publiquement accessibles (pages de commentaires, pages de coordonnées des sites web, réseaux sociaux, forums...). Les adresses collectées peuvent alors être ajoutées aux listes de diffusion des pourriels.

3.4 Diffusion de codes malveillants

3.4.1 Exécution de codes malveillants sur les machines-zombies

Les botnets peuvent être utilisés comme vecteur de distribution de codes malveillants supplémentaires. C'est en particulier le cas lorsque les machines infectées sont des postes de travail ou des téléphones mobiles multifonctions. **Un contrôle distant des machines peut permettre une très large palette de possibilités.** Les codes malveillants installés peuvent avoir pour but d'afficher des publicités, de modifier le comportement des navigateurs (en particulier lors de la visite de sites web bancaires), d'enregistrer les frappes sur le clavier, d'exfiltrer[3] des données à caractère personnel, d'altérer des données présentes sur la machine... Le cas particulier du cryptominage est décrit en 3.7.

Ce type de codes a tendance à modifier le comportement de la machine infectée et peut alerter son utilisateur légitime d'une probable compromission. Cette perte de furtivité peut indiquer un botnet en fin de vie dont l'opérateur cherche à maximiser les profits au risque de perdre plus rapidement des machines.

[1] Un serveur mandataire (*proxy*) joue un rôle d'intermédiaire, relayant des requêtes. Cela a pour effet de remplacer, pour ses interlocuteurs, l'adresse de l'utilisateur du service par celle du serveur mandataire.

[2] Attaque par courriel, reposant souvent sur l'ingénierie sociale, incitant la cible à télécharger une pièce jointe ou cliquer sur un lien malveillant. Généralement, le courriel usurpe l'identité d'une personne ou d'un service en ligne légitime.

[3] Dans les cas d'exfiltration de données des victimes, les données peuvent être envoyées via les canaux de communication permettant de contrôler le botnet ou via un canal distinct.

3.4.2 Hébergement de codes malveillants

Les machines infectées peuvent également être utilisées comme plateforme d'hébergement représentant autant de sources potentielles d'infections, contournant les mesures de défenses qui reposent sur des listes d'adresses IP associées aux menaces.

3.5 Fraude aux clics

La publicité en ligne est généralement rémunérée en fonction des affichages dont elle fait l'objet et des visites générées lors des clics. En simulant des visites d'internautes, le contrôle d'un botnet peut augmenter artificiellement le nombre d'affichages et de clics effectués sur des sites web complices [17]. Des techniques plus indirectes comme l'épuisement des budgets publicitaires d'un concurrent, des campagnes visant à faire accuser un concurrent de fraude au clic ou des gains en tant qu'intermédiaire lors de transactions publicitaires ont été rapportées. **Les montants concernés par la fraude aux clics ont été estimés à plusieurs milliards de dollars** [3, 17].

3.6 Compromission d'accès

3.6.1 "Brute force" hors-ligne

Un attaquant disposant d'informations chiffrées ou de condensats[4] de mots de passe peut essayer de les découvrir en essayant successivement un grand nombre de mots de passe. Ce type d'attaque, par dictionnaire ou par « brute force[5] », nécessite une grande puissance de calcul. En exploitant les machines-zombies de botnets de grande taille, il est possible de développer des puissances comparables à celles de supercalculateurs [4].

3.6.2 "Brute force" direct

Une autre approche consiste à essayer des mots de passe directement sur les pages web d'authentification. Comme de nombreux services limitent le nombre de tentatives par machines, l'utilisation d'un botnet pour des essais successifs et coordonnés de mots de passe semble s'être développée. Les interfaces d'administration de sites utilisant des systèmes de gestion du contenu (CMS) répandus, comme WordPress, semblent être particulièrement ciblées. Afin de rester le plus discret possible et ainsi éviter de voir ses machines bloquées, le botnet Sathurbot, spécialisé dans ce type d'attaques, ne ferait qu'une seule tentative de connexion par machine zombie selon ESET [18].

3.7 Cryptominage

La majorité des cryptomonnaies reposent sur un registre[6] chiffré et public, dont les modifications doivent être validées de manière cryptographique par la résolution de problèmes mathématiques complexes. Dans les modèles décentralisés, la puissance de calcul nécessaire à cette validation est mise à disposition par des acteurs indépendants contre une rémunération en cryptomonnaie. La rémunération de ces opérations, dites de cryptominage, se fait (indirectement) en fonction de la puissance fournie. Cependant, le coût de la consommation électrique élevée requise pour le cryptominage, ainsi que l'investissement dans le matériel informatique nécessaire sont deux facteurs déterminants pour la rentabilité de cette pratique.

Lors d'une récupération frauduleuse de puissance de calcul, les acteurs malveillants peuvent se procurer des cryptomonnaies sans avoir à en assumer les couts. .

Les revenus générés dépendent de la puissance de calcul cumulée des machines zombies, mais surtout des choix de l'opérateur du botnet quant à la fraction de la puissance qui est usurpée. Il semblerait en effet que de nombreux

[4] Résultat d'une fonction mathématique, dite de hachage, qui attribue à n'importe quel type de données une valeur unique de longueur constante. Deux condensats identiques correspondent ainsi à des données d'entrées (des mots de passe par exemple) identiques. Il est cependant impossible d'inférer les données d'origine à partir du condensat. Idéalement, les mots de passe sont stockés sous la forme de condensats.

[5] Approche consistant à essayer successivement toutes les combinaisons de mots de passe possibles.

[6] Ce registre est appelé « Chaine de bloc » ou "*blockchain*". Les modifications y sont enregistrées par blocs et chaque bloc dépend du bloc précédent, à la manière d'une chaine.

botnets n'exploitent qu'une partie limitée de la puissance de calcul des machines infectées afin de minimiser les risques de détection.

4 Cycle de vie d'un botnet

La mise en place d'un botnet, son maintien en conditions opérationnelles et son utilisation pour mener des attaques informatiques requièrent la réalisation de plusieurs étapes successives. Chacune de ces étapes représente une opportunité dans la lutte contre les botnets malveillants.

4.1 Définition des objectifs

Selon les utilisations prévues d'un botnet, divers compromis de conception doivent être effectués et ceux-ci conditionneront le fonctionnement du botnet.

Ces choix découlent des objectifs prioritaires des opérateurs (furtivité des infections, vitesse de compromission, capacité à monter en charge, résistance aux efforts de démantèlement, réactivité, possibilité de louer les accès, finesse de la gestion du botnet, type de propagation...).

Par exemple, l'intégration de mécanismes d'infections de type ver[7] risque de faire perdre en furtivité ce code malveillant, peut conduire à des infections de machines isolées du C2 et nécéssite un dimensionnement de l'infrastructure de contrôle capable de gérer des variations imprévisibles du nombre de machines victimes.

La sélection des machines ciblées aura également un impact. En effet, un code malveillant ciblant des routeurs de fibre optique disposera généralement de meilleures performances de communication qu'un code ciblant des téléphones mobiles.

La principale caractéristique qui devra ainsi être déterminée est le modèle économique développé.

4.1.1 Modèle économique

Les opérateurs de botnets peuvent avoir pour objectifs de réaliser des opérations pour leur propre compte (compromission d'identifiants, DDoS contre rançon, cryptominage...). Pourtant, il apparait qu'une grande partie des modèles économiques employés consistent à proposer des services (Envoi de pourriel, fraude au clic, DDoS, infrastructure d'anonymisation ...) ou à louer une partie de leur outil à d'autres acteurs malveillants.

Certains services peuvent être proposés sous une apparence légitime, notamment sous la forme de *stress testers*[8]. D'autres opérateurs proposent directement leurs services sur le marché noir en ligne. Les services de DDoS, de diffusion de pourriels et de fraude aux clics semblent être parmi les plus répandus. Des services d'infection d'un nombre déterminé de postes avec des logiciels malveillants ont aussi été décrits [19].

La location de botnet semble être une méthode particulièrement répandue pour tirer profit d'un botnet. Les montants demandés seraient compris entre 50 $ et plusieurs milliers de dollars par jour selon la taille et les capacités du botnet. Ce modèle économique peut permettre des gains importants pour les utilisateurs comme pour les opérateurs [20].

Certaines publications mentionnent également la vente de botnets de petite taille. Les acheteurs sont alors en charge de les faire croître [4].

[7] Un ver informatique est un code malveillant capable d'infecter de nouvelles machines de manière autonome.

[8] Les *stress testers* sont des services d'évaluation de la résistance d'infrastructures à des afflux massifs de requêtes. Ils peuvent être utilisés de manière légitime afin d'évaluer les capacités d'une infrastructure à résister à une attaque DDoS. Cependant, une part non négligeable des recours à ces services serait elle-même utilisée à des fins malveillantes pour mener des attaques DDoS (voir 3.1).

4.2 Développement du code

Les machines zombies qui composent un botnet doivent être infectées par un (ou plusieurs) code(s) malveillant(s) permettant le contrôle à distance par l'opérateur du botnet. Ces codes malveillants sont développés en fonction des objectifs recherchés et conditionnent l'organisation du réseau ainsi que les modes de communication au sein du botnet. Les développeurs réutilisent couramment certains codes existants afin de les adapter au contexte d'utilisation voulu.

Le développement logiciel nécessaire à la mise en place d'un botnet peut représenter un investissement important. Il a par exemple été estimé que 3 ans de travail ont été nécessaires à son développeur pour mettre au point le programme malveillant Zeus. Cependant, des copies de ce logiciel semblent pouvoir être obtenues sur le marché noir à partir de 700 $ pour des versions de base et à plus de 3000 $ pour des versions plus avancées [20].

Commentaire : Ce type de transaction est doublement préjudiciable. En effet, il rend potentiellement rentable une spécialisation de certains acteurs dans le développement de codes malveillants complexes et entraine leur dissémination auprès d'acteurs n'ayant pas les compétences de les développer.

Ainsi, les acteurs ayant développé les codes malveillants ne sont pas nécessairement les opérateurs des botnets. Le code peut avoir été vendu ou rendu disponible à titre gratuit[9] et réutilisé.

Du fait de la dissémination des codes malveillants, il est ainsi important d'avoir à l'esprit que deux machines infectées par un code malveillant similaire peuvent être associées à deux botnets distincts. Inversement, le botnet Sopelka [21] aurait été composé de machines zombies infectées par 3 codes malveillants différents se connectant à une même infrastructure de commande et de contrôle.

4.3 Déploiement

4.3.1 Infection initiale

Les méthodes d'infection utilisées varient : certains botnets utilisent les machines-zombies comme vecteur d'infection (propagation type ver) tandis que d'autres reposent sur un vecteur d'infection indépendant. Les vecteurs indirects les plus utilisés semblent être les campagnes d'hameçonnage, la compromission de copies gratuites de logiciels payants, la mise en place de point d'eau et les compromissions ciblées.

Bien qu'une propagation de type ver puisse permettre une croissance exponentielle d'un botnet, la recherche de cibles à partir des machines victimes rend l'infection moins furtive.

Dans de nombreux cas, le vecteur d'infection initial a pour unique fonctionnalité de conduire la machine victime à télécharger un ou plusieurs codes malveillants supplémentaires chargés de prendre le contrôle de la machine. Cette installation par étape peut ainsi permettre d'utiliser des vecteurs d'infection plus légers et éventuellement de sélectionner les codes malveillants installés en fonction des machines victimes.

Pour la plupart des botnets décrits, les serveurs délivrant les codes malveillants des différentes étapes étaient distincts des infrastructures C2, ce qui semble être une mesure de cloisonnement entre les activités d'infection et de contrôle.

4.3.2 Ralliement à l'infrastructure C2

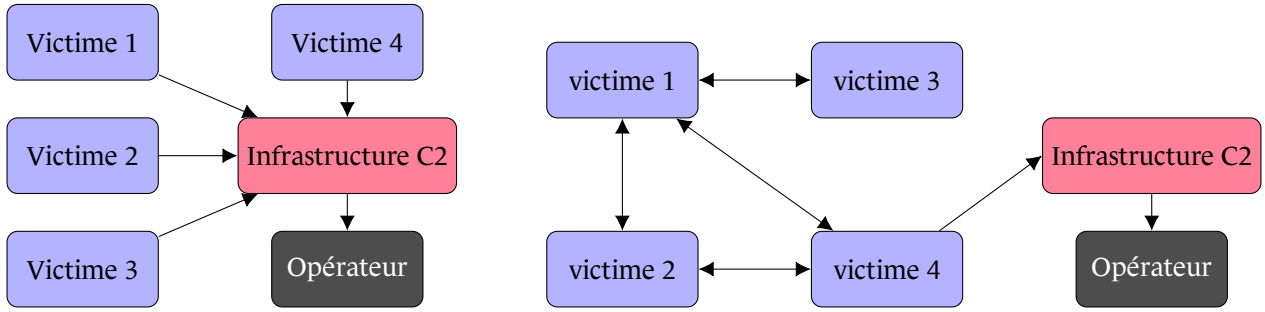
Une fois infectées, les machines vont chercher à communiquer avec les C2 du botnet afin de s'y rallier.

Un identifiant unique ainsi que des informations concernant la machine compromise sont généralement transmis lors des premières communications vers le C2 afin de répertorier la machine. L'ouverture de la connexion permet au C2 de donner ses premières instructions à la machine zombie qui fait alors partie du botnet.

[9] Les familles de codes malveillants Mirai (voir 5.1) et Gafgyt, parmi les plus utilisées [9], sont ainsi issues de codes disponibles en source ouverte.

Architecture pair-à-pair de botnet

Certains botnets reposent sur une infrastructure pair-à-pair. Dans les botnets utilisant cette architecture, les machines zombies ne communiquent pas directement avec l'infrastructure C2, mais avec d'autres machines zombies définies dans une liste de pairs évolutive. Ainsi, seul un petit nombre de machines est en contact avec l'infrastructure C2 opérée directement par l'attaquant. Ces machines relaient ensuite les informations transmises par le C2 aux autres machines infectées présentes dans leur liste qui feront de même. Cette technique est utilisée afin de compliquer la découverte de l'infrastructure C2 et de contourner les défenses centrées sur l'utilisation de pare-feu bloquant les adresses IP ou les domaines connus pour être rattachés à une infrastructure C2 de botnet.



Architecture client-serveur

Architecture pair-à-pair

Fig. 4.1 : Comparaison entre les architectures de communication client-serveur et pair-à-pair de botnet

Utilisation du réseau TOR

Le contact avec l'infrastructure C2 peut être effectué en utilisant le réseau d'anonymisation TOR. L'utilisation d'une adresse en .onion rend alors virtuellement impossible d'identifier les machines destinataires des communications. Cependant les communications avec le réseau TOR peuvent être bloquées depuis certains systèmes d'information. De plus, la relative lenteur du réseau peut compliquer la gestion de botnets comprenant un trop grand nombre de pairs.

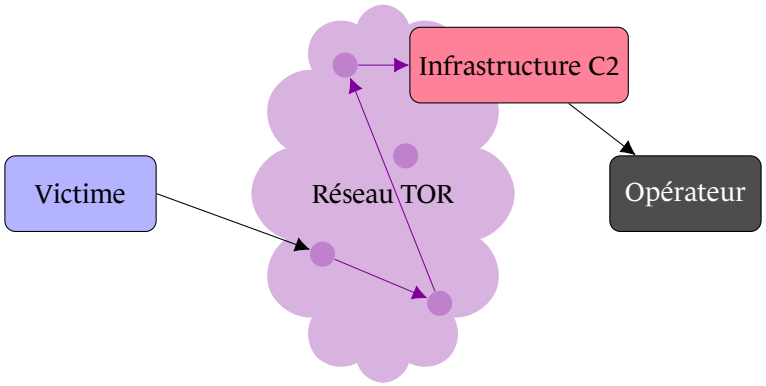


Fig. 4.2 : Utilisation du réseau Tor pour les communications

4.4 Exploitation

4.4.1 Maintien du contrôle

Le bon fonctionnement d'un botnet repose sur sa capacité à contrôler les machines zombies qui le composent. Ceci requiert le maintien d'un canal de communication avec les machines infectées ainsi que la persistance d'outils

d'accès à distance permettant le contrôle des machines par les opérateurs.

Maintien des communications vers le C2

Le maintien de la communication entre les machines zombies et le C2 est un élément crucial pour le fonctionnement du botnet, son interruption s'apparenterait à un démantèlement.

Selon leurs modalités d'accès au réseau Internet, les machines zombies peuvent changer d'adresses IP ou être placées derrière des routeurs ou des pare-feux, rendant difficile un contact initié par le C2. Ainsi, le modèle qui semble être le plus utilisé actuellement est celui d'un contact initié par les machines zombies vers le C2[10]. Le canal de communication peut être maintenu de manière continue ou renouvelé à un intervalle prédéfini.

Des modes de communication alternatifs sont généralement configurés pour pallier une coupure du mode de communication habituel. Cela peut consister en une liste d'adresses IP ou de noms de domaines contactés successivement en cas d'échec de la communication avec les entrées précédentes. Cela peut également passer par des algorithmes de génération de noms de domaine (DGA), conçus pour permettre aux opérateurs du botnet d'utiliser des noms de domaine spécifiques en cas de perte des communications.

Commentaire : Le recours aux DGA présente des vulnérabilités. En effet, un acteur cherchant à prendre le contrôle du botnet pourrait analyser cet algorithme, acheter certains noms de domaine avant l'attaquant et décider de faire pointer ceux-ci vers sa propre infrastructure, configurée de manière à simuler le C2 habituel. Des chercheurs auraient ainsi pris le contrôle du botnet Torpig durant 10 jours en 2011 en utilisant cette approche [22].

Exécution des instructions par les machines compromises

La coupure des canaux de communication n'est pas la seule cause possible d'une perte de contrôle des machines victimes. Un code malveillant capable de maintenir les communications et d'exécuter les instructions est nécessaire.

Certains codes malveillants utilisés par des botnets ne disposent pas de mécanismes de persistance en cas de redémarrage de la machine [23, 24]. C'est notamment le cas pour les codes ciblant des serveurs ou des objets connectés. Les codes disposant de mécanismes de persistance peuvent également être rendus inopérants par des mises à jour de sécurité ou des logiciels antivirus.

Une caractéristique plus spécifique des botnets réside cependant dans la concurrence qui s'opère entre les différents opérateurs de botnets [25]. En effet, de nombreux botnets cherchent à exploiter les mêmes vulnérabilités et ciblent ainsi les mêmes machines (voir 5.3). On observe ainsi qu'une grande partie des botnets mettent en place des protections sur leurs machines zombies afin de les protéger contre l'intrusion de botnets concurrents[11]. En particulier, les vulnérabilités exploitées par le code malveillant pour infecter les machines zombies sont très fréquemment corrigées suite à leur exploitation. Ces actions peuvent paradoxalement rendre les machines zombies plus sécurisées qu'elles ne l'étaient avant l'infection.

4.4.2 Mises à jour

À l'instar de la plupart des logiciels, les codes malveillants des machines zombies peuvent généralement être mis à jour, par exemple pour ajouter des fonctionnalités, modifier les modalités de communications ou augmenter la furtivité de l'infection. Lorsque la communication est établie, le C2 peut envoyer l'ordre à la machine zombie de télécharger et d'installer une mise à jour.

Ces mises à jour consistent souvent à ajouter des codes d'exploitation de vulnérabilités supplémentaires aux machines infectées, en particulier dans les cas de propagation de type ver. Ce type de mise à jour, qui augmente la quantité de machines vulnérables, peut conduire à des augmentations rapides du nombre de machines infectées

[10] Un mode de communication appelé "beaconing" en anglais

[11] Un entretien publié par NewSky Security [26] rapporte même le cas d'un opérateur de botnet ayant mis en place un « pot de miel » afin de collecter des informations sur des botnets concurrents afin de mieux les combattre.

au sein d'un botnet. La concurrence entre les différents opérateurs de botnets semble conduire à des courses à l'intégration de ces codes d'exploitation (voir 5.3).

La prise de contrôle d'une infrastructure de mise à jour des codes malveillants peut permettre d'usurper ou de démanteler un botnet [27]. En effet, une modification du code malveillant envoyé aux machines zombies permettrait de supprimer les communications ou de les rediriger vers une autre infrastructure C2. De plus, afin de déployer une mise à jour d'un grand nombre de machines zombies, une infrastructure de mise à jour devra disposer d'une connexion internet rapide et fiable, ce qui tend à la rendre plus facilement détectable.

4.4.3 Exécution des attaques

Plusieurs approches sont possibles pour la gestion des attaques, selon le type d'attaques mené et le niveau de discrétion recherché.

Certains opérateurs de botnets prennent soin de compartimenter leurs botnets et de ne lancer des attaques qu'à partir d'une fraction de celui-ci afin de rendre plus difficile une identification des machines zombies qui le composent ou des recherches sur leur nombre. Ainsi, la société de cybersécurité Talos a rapporté des écarts de plusieurs mois entre deux campagnes pour la majorité des adresses IP associées à des machines contrôlées par le botnet Necurs [16].

4.5 Démantèlement

Le cycle de vie d'un botnet se termine avec son éventuel démantèlement. Il peut être consécutif à l'intervention des forces de l'ordre et/ou d'acteurs privés, ou encore provoqué par son opérateur, afin d'effacer ses traces.

S'il existe des services destinés à diminuer l'impact de certaines attaques permises par les botnets, ceux-ci ne représentent pas une réponse satisfaisante, en particulier vis-à-vis des botnets de grande taille. Des opérations de démantèlement sont ainsi régulièrement entreprises par les acteurs de la sécurité informatique.

Les opérations de démantèlement cherchent généralement à couper les communications à destination du C2.
La désinstallation des codes malveillants présents sur les machines infectées, via une instruction ou mise à jour par un code inoffensif, n'est généralement pas utilisée par les acteurs légitime par crainte des effets de bords liés à l'envoi de code sur les machines victimes. Cependant, en août 2019, le Centre de lutte contre la criminalité numérique de la Gendarmerie nationale (C3N) a remplacé le serveur C2 du botnet Retadup par un serveur configuré pour déclencher une désinstallation du code malveillant des machines victimes. Cette opération de démantèlement a permis de désinfecter de plus de 850 000 machines victimes avec une approche alors indédite à cette échelle [28].

Plusieurs contraintes compliquent la lutte contre de telles menaces :

Une première contrainte est de nature technique. Afin de neutraliser un botnet, il faut parvenir à en comprendre le fonctionnement. Si de nombreuses structures privées ou étatiques disposent de personnel à même de réaliser de telles analyses, la mise en place d'architectures complexes et de techniques d'obscurcissement par l'opérateur du botnet peut rendre cette phase de compréhension fastidieuse et coûteuse.

Une deuxième contrainte est d'ordre juridique. La saisie de serveurs est parfois nécessaire pour étudier le fonctionnement du botnet ou pour rediriger les connexions vers une infrastructure légitime. Cela peut nécessiter des procédures judiciaires et l'intervention des forces de l'ordre. Pour pouvoir mettre en place de telles procédures dans un délai suffisamment bref pour suivre le rythme d'évolution des botnets, des efforts importants doivent être fournis. Il semble que de telles procédures ne soient mises en place que dans le cas de menaces dont l'ampleur a entrainé une attention particulière.

Enfin, les attaquants utilisent généralement des machines localisées dans plusieurs pays. Une coopération internationale peut alors être nécessaire pour mener à bien les opérations de démantèlement. Cela est particulièrement problématique lorsque les machines sont localisées dans des pays n'ayant pas établi d'accords de coopération judiciaires.

À titre d'exemple, un résumé de l'opération « Tovar », destinée à démanteler le botnet Gameover ZeuS, est disponible en annexe 6.1.

5 Évolutions et tendances

5.1 Extension à l'Internet des Objets

Les attaques du botnet Mirai de septembre 2019 ont entrainé une prise de conscience des risques associés aux botnets reposant sur l'Internet des objets (Internet of Things, IoT). En effet, avec un code malveillant relativement simple, exploitant les faiblesses des mots de passe par défaut des équipements, le botnet Mirai s'est montré capable d'attaques DDoS d'un débit proche de 1 Tbps, le double des records précédents.

Depuis la publication, le 30 septembre 2016, du code source du logiciel malveillant responsable de l'infection, de nombreux autres botnets reposant sur ce même code, plus ou moins modifié, ont été développés. En effet, selon les estimations, il y aurait plusieurs milliards d'objets connectés qui sont autant de cibles potentielles pour les attaquants.

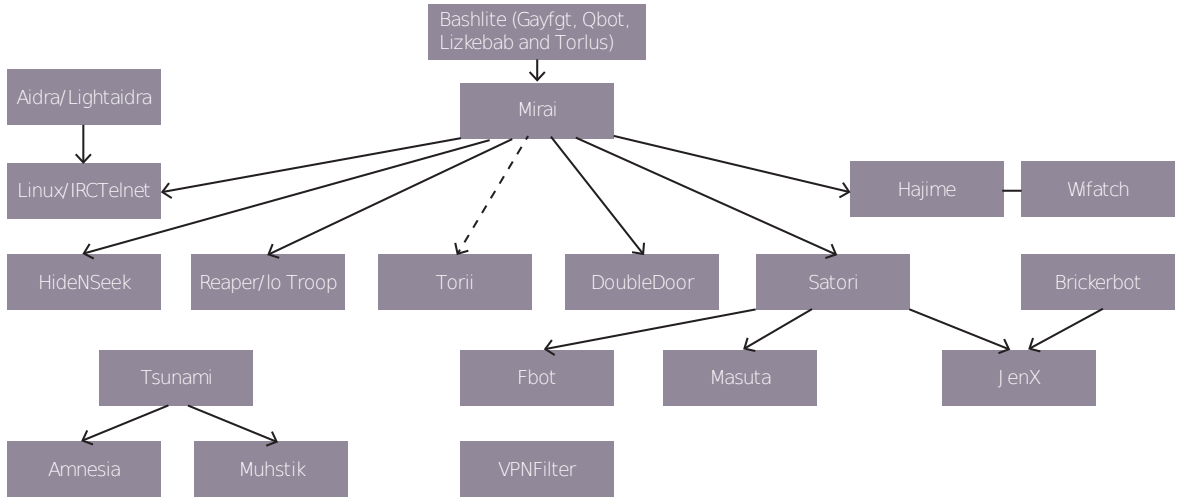


Fig. 5.1 : Évolution de codes malveillants utilisés par des botnets ciblant l'Internet des objets. Source : Nokia [29]

Plusieurs raisons peuvent expliquer le ciblage fort de l'IoT, observable depuis l'automne 2016 :

- Une sécurisation très faible de certains équipements, facilitant les infections ;
- Un nombre de machines existantes élevé et en forte croissance, permettant le déploiement de botnets de grande taille ;
- La disponibilité d'une base de code gratuite, facilitant la production de variantes ;
- La disponibilité généralement continue des machines ;
- Bien que disposant généralement d'une puissance de calcul très faible par rapport à d'autres machines, la puissance moyenne des objets connectés est en augmentation et a un potentiel d'utilisation qui se rapproche progressivement de celui des ordinateurs personnels.

La recherche de machines vulnérables supplémentaires par les opérateurs de botnets utilisant des codes malveillants ciblant l'IoT a conduit à une sophistication des codes malveillants utilisés. Ces modifications peuvent ainsi consister en une intégration de codes d'exploitation de vulnérabilités présentes sur des objets connectés. Plusieurs codes d'exploitations peuvent être combinés, une variante aurait ainsi compris plus de 50 codes d'exploitation [30]. Des variantes ont également été adaptées pour fonctionner sur une plus grande gamme de machines [31, 32]. Il y aurait ainsi plus de 20 000 variantes du code malveillant Mirai en 2019 [9, 33].

Selon Nokia, les activités liées aux botnets ciblant l'IoT auraient représenté 78 % des détections de codes malveillants sur des réseaux d'opérateurs télécoms [29].

Face au manque de sécurisation de certains objets connectés et des dégâts que peuvent causer leur enrôlement dans un botnet, un individu a déclaré avoir déployé entre 2016 et 2017 un botnet ayant pour objectif de rendre inutilisables les objets connectés non protégés, dans le but annoncé de prévenir leur exploitation à des fins malveillantes [34].

5.2 Cryptominage

En aout 2011, un rapport de Kaspersky [35] décrivait déjà une utilisation d'un botnet comme vecteur d'installation de logiciels de cryptominage. L'augmentation massive (supérieure à 1 000 % pour la majorité des cryptomonnaies représentatives) du prix des cryptomonnaies au cours de l'année 2017 semble avoir eu pour effet une réorientation des botnets à but lucratif vers des activités de cryptominage. Cependant, la baisse suite au pic de 2017 et la forte volatilité des prix ont fortement modéré ces migrations depuis 2018.

Ces activités représentent en effet plusieurs avantages :

Discrétion de l'attaque
: La majorité des types d'attaques à but lucratives menées par des botnets ont un impact visible sur leurs victimes. Inversement, un botnet ayant des objectifs de cryptominage et n'utilisant qu'une faible partie de la puissance de calcul des machines sur lequel il est présent peut ne pas être détecté et continuer à générer des revenus.

Pas d'interaction nécessaire avec d'autres acteurs malveillants
: Une part importante des utilisations lucratives d'un botnet (envoi de pourriels, location de botnet, fraude aux clics, revente d'informations exfiltrées…) impliquent de la part de l'opérateur de procéder à des transactions avec d'autres acteurs malveillants afin de leur vendre un service. Les injonctions à faire la publicité du service, induites par ces modèles économiques, entrent ainsi en contradiction avec les injonctions de la sécurité opérationnelle à garder le réseau le moins visible possible. De plus, la nécessité de maintenir des relations avec d'autres acteurs malveillants peut induire des conséquences indésirables. Bien que des activités de minage aient elles aussi à interagir avec des entités tierces (*pools* de minage[12] , plateformes d'échange de cryptomonnaies), la position de client à des services légitimes ne pose pas de telles contraintes.

Des revenus stables et prévisibles
: La puissance de calcul d'un botnet dans un *pool* de minage est relativement stable et prévisible. Cela permet des estimations des montants de rémunération à venir en cryptomonnaies. La forte volatilité du prix des cryptomonnaies entraine néanmoins de fortes variations de ces revenus lorsqu'ils sont exprimés avec une monnaie traditionnelle.

Une cryptomonnaie semble être privilégiée par les logiciels malveillants de cryptominage : Monero (XMR). Deux raisons peuvent expliquer ce choix : la première est due au fait que, contrairement à de nombreuses autres cryptomonnaies, il est très difficile de développer des machines spécialisées dans le minage de cette cryptomonnaie. Il en résulte une plus grande compétitivité des processeurs classiques, présents sur la majorité des machines susceptibles d'être intégrées dans un botnet ; la deuxième est due au plus grand anonymat permis par cette cryptomonnaie, qui

[12] Pour la plupart des cryptomonnaies, la rémunération n'est attribuée qu'au compte ayant validé un bloc, ce qui comporte une part de chance et donc une rémunération irrégulière. Des instances de mutualisation des calculs, appelées « *pool* de minage », permettent cependant à leurs membres de rendre de facto la rémunération proportionnelle au travail fourni. Le recours aux *pools* de minage est *quasi* systématique pour les cryptomonnaies majeures.

offre notamment la possibilité de dissimuler origine et destination des fonds transférés.

Les cryptomonnaies sont des actifs aux prix particulièrement volatils. Les revenus générés par leur minage peuvent largement varier à travail fourni constant. Ainsi, depuis 2018, plusieurs éditeurs [36, 37] ont rapporté une corrélation entre les prix des cryptomonnaies et la popularité des opérations de minage par des botnets.

5.3 Course au déploiement des codes d'exploitation de vulnérabilités

L'intégration de nouveaux codes d'exploitation de vulnérabilités dans les codes malveillants à l'origine des botnets permet à leurs opérateurs de cibler une plus grande quantité de machines et ainsi d'accroitre les capacités de leur botnet. Comme indiqué précédemment, une forte concurrence existe entre les différents opérateurs de botnets. L'ajout d'un code d'exploitation inutilisé par la concurrence permet la compromission de nouvelles machines, n'étant pas contrôlées par un autre botnet, ce qui procure un avantage compétitif notable. Il semble cependant que très peu de codes malveillants à l'origine de botnets aient déployé des codes d'exploitation n'ayant pas été rendus publics auparavant [38]. Cela est probablement dû à une maturité plus faible des développeurs de ces codes ou à une concentration sur d'autres aspects du code.

Lors de la publication par d'autres acteurs de codes d'exploitation de vulnérabilités, une course à leur intégration au sein des codes malveillants à l'origine des botnets semble se dérouler, en particulier pour les codes ciblant l'IoT. Des intégrations particulièrement rapides de codes d'exploitation ont ainsi été rapportées. Les vulnérabilités CVE-2018-10561 et CVE-2018-10562, affectant des routeurs Dasan, ont été rendues publiques le 1er mai 2018. L'exploitation de cette vulnérabilité étant triviale une fois celle-ci connue, au moins 5 familles de codes malveillants[13] avaient été mis à jour dans les 10 jours suivants afin de l'exploiter [39, 40, 41]. Autre exemple, la vulnérabilité CVE-2019-2725, affectant les serveurs WebLogic d'Oracle, aurait été exploitée 4 jours après avoir été rendue publique [42], et 1 jour après la publication d'un code d'exploitation en ligne.

[13] Les familles de codes malveillants mentionnées sont Mettle, Muhstik, Mirai, Hajime et Satori.

6 Annexe

6.1 Exemple de l'opération Tovar contre le botnet GameOver ZeuS

Le 30 mai 2014, de nombreux acteurs, sous la direction du FBI, ont lancé l'opération Tovar contre le botnet GameOver ZeuS. Cette opération, l'une des plus importantes de ce type, fait suite à deux tentatives infructueuses menées en 2011 et 2013. Ce botnet utilisant une version largement modifiée du logiciel malveillant ZeuS, reposait sur une infrastructure pair-à-pair (voir 4.3.2) et utilisait un algorithme de génération de domaine (DGA, voir 4.4.1) en cas de coupure de communication via le réseau de pair-à-pair. Trois niveaux indépendants de contrôle du botnet avaient par ailleurs été mis en place.

Bien que peu de détails aient été communiqués concernant la campagne de reconnaissance et d'infiltration du réseau pair-à-pair, l'objectif semble avoir été de rediriger les communications des machines zombies vers un serveur hors du contrôle des opérateurs malveillants (une pratique appelée "*sinkholing*"). Parallèlement aux opérations de reconnaissance et d'infiltration du réseau pair-à-pair du botnet, le FBI aurait demandé aux registraires[14] concernés d'enregistrer tous les noms de domaines possibles générés par le DGA de GameOver ZeuS plusieurs mois à l'avance. Cependant, afin de ne pas alerter les opérateurs du botnet, ces domaines n'étaient pas publiquement répertoriés comme ayant été achetés avant le lancement de l'opération. Dans les cas des domaines en « .ru », rattachés à un registraire russe n'ayant pas désiré collaborer à l'opération, les redirections vers les serveurs de FBI furent mises en place au niveau des opérateurs de serveurs DNS.

Le jour du lancement de l'opération, les deux principaux serveurs de commande et de contrôle, localisés au Canada et en Ukraine, ont été mis hors ligne par les forces de l'ordre de ces deux pays. Parallèlement, tous les domaines enregistrés se mirent à pointer vers des serveurs contrôlés par le FBI, lui donnant effectivement le contrôle progressif du botnet. Afin d'éviter une éventuelle reprise en main du botnet par ses opérateurs malveillants, une campagne de sensibilisation des victimes aurait été menée pour encourager la détection puis la suppression des logiciels malveillants sur les machines infectées [3].

[14] Bureau d'enregistrement gérant la réservation de noms de domaine Internet.

7 Bibliographie

[1] Éric Freyssinet. “Lutte contre les botnets : analyse et stratégie”. Paris : Université Pierre et Marie Curie, 12 nov. 2015. 206 p. URL : https://www.theses.fr/2015PA066390/document.

[2] Malewarebytes labs. *The Facts about Botnets*. 30 mar. 2016. URL : https://blog.malwarebytes.com/cybercrime/2015/02/the-facts-about-botnets/.

[3] Department of Homeland Security. *Taking down Botnets*. 15 juil. 2014. URL : http://www.judiciary.senate.gov/hearings/watch?hearingid=e4cdf730-5056-a032-5290-ddd9c65ff093.

[4] Nathan Goodman. “A Survey of Advances in Botnet Technologies”. 15 jan. 2017. In : *Arxiv preprint* (15 jan. 2017). URL : https://arxiv.org/abs/1702.01132.

[5] Kaspersky SecureList. *DDoS Attacks in Q3 2017*. 6 nov. 2017. URL : https://securelist.com/ddos-attacks-in-q3-2017/83041/.

[6] Krebs on security. *Mirail IoT Botnet Co-Authors Plead Guilty*. 13 déc. 2017. URL : https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/.

[7] KrebsOnSecurity. *Cowards Attack Sony PlayStation, Microsoft xBox Networks*. 26 déc. 2014. URL : https://krebsonsecurity.com/2014/12/cowards-attack-sony-playstation-microsoft-xbox-networks/.

[8] Rain Ottis. “Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective”. In : *Proceedings of the 7th European Conference on Information Warfare*. Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2 mar. 2018, p. 163. URL : https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

[9] NSFOCUS. *2018 Botnet Trend Report*. 17 juin 2019. URL : https://nsfocusglobal.com/2018-botnet-trend-report/.

[10] Krebs on security. *The Democratization of Censorship*. 25 sept. 2016. URL : https://krebsonsecurity.com/2016/09/the-democratization-of-censorship/.

[11] Citizen Lab, Bill Marczak et Nicholas Weaver. “China’s Great Cannon”. 10 avr. 2015. In : *Citizen Lab* 10 (10 avr. 2015). URL : https://citizenlab.ca/2015/04/chinas-great-cannon/.

[12] Securelist. *DDoS Attacks in Q4 2017*. 6 fév. 2017. URL : https://securelist.com/ddos-attacks-in-q4-2017/83729/.

[13] Check Point. *Ramnit’s Network of Proxy Servers*. 5 août 2018. URL : https://research.checkpoint.com/ramnits-network-proxy-servers/.

[14] Akamai. *UPnProxy : Blackhat Proxies via NAT Injections*. 5 avr. 2018. URL : https://www.akamai.com/us/en/multimedia/documents/white-paper/upnproxy-blackhat-proxies-via-nat-injections-white-paper.pdf.

[15] Masarah Paquet-Clouston et Olivier Bilodeau. “The Industry of Social Network Manipulation : From Botnets to Hucksters”. RSA Conference 2019 (San Francisco). 3 mar. 2019. URL : https://published-prd.lanyonevents.com/published/rsaus19/sessionsFiles/13529/SEM-M03C-The-Industry-of-Social-Network-Manipulation-from-Botnets-to-Hucksters.pdf.

[16] Cisco Talos. *The Many Tentacles of the Necurs Botnet*. 18 jan. 2018. URL : http://blog.talosintelligence.com/2018/01/the-many-tentacles-of-necurs-botnet.html.

[17] Google & White Ops. *The Hunt for 3ve*. 27 nov. 2018. URL : https://services.google.com/fh/files/blogs/3ve_google_whiteops_whitepaper_final_nov_2018.pdf.

[18] ESET WeLiveSecurity. *Sathurbot : Distributed WordPress Password Attack*. 6 avr. 2017. URL : https://www.welivesecurity.com/2017/04/06/sathurbot-distributed-wordpress-password-attack/.

[19] Sophos. *An Analysis of the Pay-per-Install Underground Economy*. 7 sept. 2011. URL : https://nakedsecurity.sophos.com/2011/09/07/an-analysis-of-the-pay-per-install-underground-economy/.

[20] C.G.J Putman et Lambert JM Nieuwenhuis. “Business Model of a Botnet”. In : 2018 26th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP). IEEE, 28 avr. 2018, p. 441-445. DOI : 10.1109/PDP2018.2018.00077. URL : http://arxiv.org/abs/1804.10848.

[21] S21sec. *Sopelka Botnet : Three Banking Trojans and One Banking Panel*. 17 oct. 2012. URL : https://www.s21sec.com/en/blog/2012/10/sopelka-botnet-three-banking-trojans-and-one-banking-panel/#.

[22] Brett Stone-Gross et al. "Analysis of a Botnet Takeover". 2 sept. 2010. In : *IEEE Security Privacy* 9.1 (2 sept. 2010). ISSN : 1540-7993, 1558-4046. DOI : 10.1109/MSP.2010.144. URL : http://ieeexplore.ieee.org/document/5560627/.

[23] Kaspersky SecureList. *New Trends in the World of IoT Threats*. 18 sept. 2018. URL : https://securelist.com/new-trends-in-the-world-of-iot-threats/87991/.

[24] MalwareTech. *Tracking the Hide and Seek Botnet*. 9 jan. 2019. URL : https://www.malwaretech.com/2019/01/tracking-the-hide-and-seek-botnet.html.

[25] ZDNet. *Two Botnets Are Fighting over Control of Thousands of Unsecured Android Devices*. 2 nov. 2018. URL : https://www.zdnet.com/article/two-botnets-are-fighting-over-control-of-thousands-of-unsecured-android-devices/.

[26] NewSky Security. *Understanding the IoT Hacker—A Conversation With Owari/Sora IoT Botnet Author*. 13 avr. 2018. URL : https://blog.newskysecurity.com/understanding-the-iot-hacker-a-conversation-with-owari-sora-iot-botnet-author-117feff56863.

[27] David Dittrich. "So You Want to Take Over a Botnet..." In : *Presented as Part of the 5th {USENIX} Workshop on Large-Scale Exploits and Emergent Threats*. San Jose, CA : USENIX, 24 avr. 2012. URL : https://www.usenix.org/conference/leet12/so-you-want-take-over-botnet.

[28] Avast. *Putting an End to Retadup : A Malicious Worm That Infected Hundreds of Thousands*. 28 août 2019. URL : https://decoded.avast.io/janvojtesek/putting-an-end-to-retadup-a-malicious-worm-that-infected-hundreds-of-thousands/.

[29] Nokia. *Nokia Threat Intelligence Report – 2019*. 6 déc. 2018. URL : https://onestore.nokia.com/asset/205835.

[30] Security Affairs. *The Number of Exploits in the Echobot Botnet Reached 59*. 7 août 2019. URL : https://securityaffairs.co/wordpress/89576/hacking/echobot-botnet-56-exploits.html.

[31] Arbor networks. *The ARC of Satori*. 18 jan. 2018. URL : https://www.arbornetworks.com/blog/asert/the-arc-of-satori/.

[32] Palo Alto Networks Unit42. *Mirai Compiled for New Processors Surfaces in the Wild*. 8 avr. 2019. URL : https://unit42.paloaltonetworks.com/mirai-compiled-for-new-processor-surfaces/.

[33] Netlab 360. "How Many Mirai Variants Are There ?" Botconf 2018 (Toulouse). 7 déc. 2018. URL : https://www.botconf.eu/wp-content/uploads/2018/12/2018-Y-Liu-H-Wang-HowManyMiraiVariantsAreThere_public.pdf.

[34] BleepingComputer. *BrickerBot Author Retires Claiming to Have Bricked over 10 Million IoT Devices*. 11 déc. 2017. URL : https://www.bleepingcomputer.com/news/security/brickerbot-author-retires-claiming-to-have-bricked-over-10-million-iot-devices/.

[35] Kaspersky SecureList. *The Miner Botnet : Bitcoin Mining Goes Peer-To-Peer*. 19 août 2011. URL : https://securelist.com/the-miner-botnet-bitcoin-mining-goes-peer-to-peer-33/30863/.

[36] NSFOCUS. *2018 DDoS Attack Landscape*. 10 avr. 2019. URL : https://nsfocusglobal.com/2018-ddos-attack-landscape/.

[37] Kaspersky SecureList. *DDoS Attacks in Q2 2019*. 5 août 2019. URL : https://securelist.com/ddos-report-q2-2019/91934/.

[38] TrendMicro. *New Mirai Variant Uses Multiple Exploits to Target Routers and Other Devices*. 23 mai 2019. URL : https://blog.trendmicro.com/trendlabs-security-intelligence/new-mirai-variant-uses-multiple-exploits-to-target-routers-and-other-devices/.

[39] Netlab 360. *GPON Exploit in the Wild (III) - Mettle, Hajime, Mirai, Omni, Imgay*. 21 mai 2018. URL : https://blog.netlab.360.com/untitled-3gpon-exploit-in-the-wild-iii-mettle-hajime-mirai-omni-imgay-en/.

[40] Netlab 360. *GPON Exploit in the Wild (II) - Satori Botnet*. 17 mai 2018. URL : http://blog.netlab.360.com/gpon-exploit-in-the-wild-ii-satori-botnet-en/.

[41] Netlab 360. *GPON Exploit in the Wild (I) - Muhstik Botnet Among Others*. 10 mai 2018. URL : https://blog.netlab.360.com/gpon-exploit-in-the-wild-i-muhstik-botnet-among-others-en/.

[42] SECURITYWEEK. *Muhstik Botnet Exploits Recent Oracle WebLogic Vulnerability*. 2 mai 2019. URL : https://www.securityweek.com/muhstik-botnet-exploits-recent-oracle-weblogic-vulnerability.

Version 2.0.4 - 04/11/2019

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
www.cert.ssi.gouv.fr / cert-fr.cossi@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN