Les objets connectés s'attaquent à Internet

PAR JÉRÔME HOURDEAUX
ARTICLE PUBLIÉ LE JEUDI 27 OCTOBRE 2016

Depuis plusieurs semaines, des chercheurs alertent sur la propagation d'un *malware*, un programme informatique installé dans les objets connectés (caméras de surveillance, enregistreurs vidéo) afin d'en prendre le contrôle. Le week-end dernier, un réseau de machines infectées a lancé une attaque de grande envergure ayant mis hors ligne de nombreux sites tels que Twitter ou Spotify.

Internet a connu, le week-end dernier, une attaque informatique historique : pour la première fois, des attaques lancées depuis des objets connectés ont réussi à mettre hors ligne certains des plus grands sites mondiaux. Une attaque rendue possible par la propagation sur « l'Internet des objets » d'un *malware* d'un nouveau type, tout aussi simple qu'inquiétant, et baptisé « Mirai ».

C'est au cœur de l'été que ce petit programme informatique aurait fait ses premières apparitions. Il est pour la première fois identifié dans une note **publiée sur le site Malware Must Die** le 31 août dernier. Ce collectif de chercheurs en sécurité informatique y expliquait avoir été alerté, au début du même mois, par des amis responsables de système informatique de l'existence d'un nouveau *malware* s'attaquant spécifiquement aux objets connectés. Celui-ci était baptisé « Mirai » et serait une variante d'autres virus du même type, Gafgyt, BASHLITE et Torlus.

L'information passe dans un premier temps inaperçue. Mais il ne faudra qu'un mois pour que « Mirai » se transforme en menace mondiale. Le mardi 20 septembre dans la soirée, Brian Krebs – journaliste américain spécialisé dans la cybersécurité – constate une étrange activité sur son site internet, KrebsonSecurity. Celui-ci est la cible d'un nombre inhabituel de requêtes qui, très vite, saturent ses serveurs et mettent son site hors ligne. En clair, Brian Krebs est victime d'une « attaque DDoS », encore appelée **« attaque par déni de service distribuée »**, consistant à rendre un site indisponible, généralement en le submergeant de requêtes.

Immédiatement, le journaliste contacte la société Akamai qui assure la sécurité de son site. En quelques heures, Brian Krebs comprend qu'il est confronté à une attaque hors du commun. Et ce, pour deux raisons. Tout d'abord, selon les premières investigations d'Akamai **publiées dès le lendemain de l'attaque** sur KrebsonSecurity, l'attaque DDoS lancée contre le site était d'une ampleur phénoménale, jamais vue chez la société de sécurité. Ses analyses font état d'un trafic d'environ 620 gigabits par seconde. À titre de comparaison, le précédent « record » constaté par Akamai était une attaque DDoS générant un trafic presque deux fois moins important, à 363 gigabits.

Mais ce qui interpelle le plus les experts en sécurité, c'est la simplicité de l'attaque. Ses auteurs ont en effet utilisé un « *botnet* », littéralement un « réseau de robots », c'est-à-dire un ensemble de programmes informatiques injectés dans des machines afin d'en prendre le contrôle. Ces dernières deviennent autant de « machines zombies » que l'auteur de l'attaque peut utiliser pour surcharger la cible de requêtes. Mais généralement, et encore plus dans le cadre d'une attaque de l'amplitude de celle menée contre KrebsonSecurity, les pirates utilisent différentes techniques pour l'amplifier en démultipliant le nombre de requêtes envoyées.

Or, selon Akamai, aucun des artifices connus n'a cette fois été employé. Les attaquants n'ont utilisé, selon les mots de Brian Krebs, que des méthodes *« pourries »*. La seule explication possible est que ceux-ci aient réussi à infecter un nombre sans précédent de machines, *« peut-être des centaines ou des milliers de systèmes »*. *« Quelqu'un a un* botnet *avec des capacités que nous n'avons jamais vues »*, expliquait alors au journaliste un responsable de la sécurité d'Akamai, Martin McKeay. *« Nous avons regardé le trafic provenant des systèmes attaquant et ils n'étaient pas dans une seule région du monde ou dans un petit sous-ensemble de réseaux – ils étaient partout. »*

Brian Krebs précisait déjà qu'il y a *« quelques indications que cette attaque ait été lancée avec l'aide d'un* botnet *ayant asservi un grand nombre d'appareils de ce que l'on appelle l'"Internet des objets" – routeurs, caméras de surveillance IP et enregistreurs vidéo numériques (DVR) exposés à Internet et protégés par des mots de passe faibles ou codés en dur »*, c'est-à-dire intégrés au code source du logiciel. Le site KrebsonSecurity restera quasiment inaccessible durant plusieurs jours. Au cours de cette période, la société Akamai informe le journaliste que, débordée par la situation, **elle n'assurera plus sa sécurité informatique**.

Si la mésaventure de Brian Krebs est largement relayée par la presse spécialisée, ce n'est que quelques jours plus tard que le lien avec « Mirai » est évoqué. La société américaine Level 3 communications, l'un des principaux opérateurs de réseaux internet au monde, annonce avoir étudié l'attaque menée contre KrebsonSecurity. **Selon ses conclusions**, entre 500 000 et 980 000 appareils auraient pu être infectés pour constituer deux « *botnets* ». De son côté, la société BackConnect, spécialisée dans la protection contre les attaques DDoS, confirme que le *malware* utilisé est bien « Mirai ».

Le vendredi 30 septembre, un utilisateur **du site communautaire Hackersforums** y publie le code source du *malware*, c'est-à-dire son ADN, permettant ainsi à n'importe qui de le dupliquer. Et *« garantissant virtuellement »*, commente alors Brian Krebs, *« qu'Internet sera bientôt inondé d'attaques provenant de nombreux nouveaux* botnets *alimentés par des routeurs, des caméras de surveillance IP, des enregistreurs vidéo numériques non sécurisés et d'autres appareils facilement piratables »*.

Les jours qui suivent donnent raison au journaliste. Avec son code source rendu public, les chercheurs peuvent se pencher plus en profondeur sur Mirai : le lundi suivant, **les chercheurs du site Malware Tech** mettent en ligne une carte de l'évolution de l'épidémie, illustrée par une vidéo résumant, en moins de 3'30, 18 minutes de propagation du *malware* dans le monde.

Un peu plus d'une semaine après la mise en ligne du code source, Level 3 faisait état **d'un doublement du nombre d'appareils infectés**, passant de 213 000 à 493 000 « *bots* » en quelques jours. Des chiffres purement indicatifs du fait d'une *« vue incomplète de l'infrastructure »*, précisait la société. Les objets impliqués dans les attaques étaient quant à eux répartis dans quasiment le monde entier, mais en priorité aux États-Unis (29 %), au Brésil (23 %) et en Colombie (8 %).

Le vendredi 21 octobre, Mirai fait la démonstration de son potentiel destructeur. Dans la matinée, la société américaine Dyn, fournissant divers services de gestion à certains des sites les plus importants au monde, est à son tour victime d'une attaque DDoS sans précédent. Durant toute la journée, plusieurs sites parmi lesquels Twitter, Reddit, Github ou Spotify sont régulièrement inaccessibles. Très vite, les *botnets* de Mirai sont identifiés. Et selon Level 3, seules 10 % de ses capacités auraient été utilisées durant l'attaque.

Cette fois, ce n'est plus le site d'un journaliste spécialisé qui est tombé. Pour la première fois, des objets connectés ont été utilisés pour lancer une attaque massive ayant mis hors ligne quelques-uns des sites les plus importants du Web. Beaucoup d'éléments, cependant, restent encore inconnus. Les évaluations du nombre total d'objets infectés, notamment, varient fortement dans le temps. Il est également très difficile de déterminer le degré de préparation et de coordination des attaques. S'agit-il d'une opération soigneusement élaborée et planifiée par un groupe ou un État ? Ou la propagation de Mirai, et la diffusion de son code source, ont-elles simplement donné des idées à quelques groupes de hackers et ouvert la voie à une attaque plus spontanée ?

Les suppositions vont bon train. Certains soupçonnent des groupes de hackers déjà connus, Poodel Corp et Lizards Squad, en raison de **deux étranges et très vagues messages** postés ces derniers mois et évoquant un événement pour la date du 21 octobre. WikiLeaks a également ajouté à la confusion en postant, quelques heures après le début de l'attaque, **un tweet** dont on ne sait s'il relève de la blague : *« M. Assange est*

toujours en vie et WikiLeaks continue à publier. Nous demandons à nos supporters d'arrêter de faire tomber l'internet US. Vous avez fait vos preuves. »

Des hackers se réclamant de la mouvance Anonymous vont même jusqu'à revendiquer l'attaque **auprès du site Politico**, affirmant avoir agi en soutien avec WikiLeaks. Tout comme un autre groupe de hackers, New World, qui publie même **un communiqué sur Twitter** se terminant par *« PS : WikiLeaks sont de bons amis »*.

Il faut préciser que l'attaque du 21 octobre intervenait quelques jours après **un incident particulièrement gênant** pour l'organisation. Quelques jours plus tôt, Julian Assange a été pour la première fois lâché par l'État qui, jusqu'à présent, assurait sa protection : l'Équateur. Peu après la publication de nouveaux mails de l'équipe de campagne de la candidate démocrate à l'élection présidentielle américaine Hillary Clinton, le fondateur de WikiLeaks, qui vit retranché dans l'ambassade équatorienne de Londres, avait vu sa connexion internet coupée. Une décision totalement assumée par Quito et justifiée, dans un communiqué, par le respect du *« principe de non-intervention dans les affaires internes d'autres États »* et par le fait que *« ces dernières semaines, WikiLeaks avait publié une quantité de documents impactant la campagne électorale américaine »*.

D'autres ont également cru voir, dans la propagation de Mirai, une nouvelle bataille de la *« cyberguerre »* entre grandes puissances. Et à ce titre, la Chine, et bien entendu la Russie, font figure de suspects idéaux. Mais pour l'instant, aucune de ces hypothèses n'a été vérifiée. Dans une note publiée le mardi 25 octobre, la société de sécurité informatique Flashpoint – l'une des premières à s'être penchée sur Mirai – affirmait même que toutes ces théories et revendications étaient *« probablement fausses »*.

Selon son analyse, l'attaque n'aurait été organisée ni par un État, ni par un groupe de hackers. Elle aurait tout simplement pris forme sur les forums du site Hackersforum, où le code source du *malware* avait été publié. Et les motivations ne seraient autres que le plaisir de l'exploit en lui-même. *« Les indicateurs techniques et sociaux de cette attaque la rapprochent plus des attaques de la communauté de Hackersforum que d'autres types d'acteurs tels que les criminels de haut rang, les hacktivistes, les États et les groupes terroristes »*, expliquait Flashpoint qui souligne que, parmi les victimes de l'attaque, figurait une société de jeux vidéo. Or *« les participants de la communauté de Hackersforum sont connus pour avoir lancé des attaques DDoS contre des sociétés de jeux vidéo en vue de faire étalage de leurs talents de hackers ou pour "troller" et attirer l'attention »*.

Il n'en reste pas moins que l'attaque du 21 octobre a été un électrochoc, une prise de conscience de la menace que fait peser « l'Internet des objets » sur la sécurité informatique mondiale. Le fait que Mirai ne soit qu'un *malware* « pourri », selon les mots de Brian Krebs, est sans doute bien plus inquiétant que s'il avait été secrètement développé par les meilleurs informaticiens de la NSA. Aujourd'hui, quelques hackers peuvent, avec quelques lignes de code, prendre le contrôle de centaines de milliers d'objets connectés et organiser sur les pages d'un forum des attaques capables de mettre hors ligne les plus gros sites mondiaux.

Dans une note publiée peu après avoir récupéré son site en intégralité, le 25 septembre, Brian Krebs avait ainsi dénoncé **le risque d'une *« démocratisation de la censure »***. Comme le souligne **sur son blog l'expert en sécurité informatique Bruce Schneier**, au début du mois de septembre, le journaliste avait **publié une enquête** sur des hackers louant leurs services pour mener des attaques DDoS. Et celle-ci avait permis l'arrestation de deux personnes. Sans que l'on puisse formellement établir un lien avec l'attaque dont il a été victime, Brian Krebs dénonçait le risque d'une censure à la portée de tous. *« Sur Internet, n'importe qui ayant envie d'en découdre et la volonté d'apprendre un peu de technologie peut devenir en un instant un censeur global autodésigné. »*

L'autre enseignement de « Mirai » est bien entendu le manque de sécurité flagrant des objets connectés. Sans entrer dans les détails techniques, ce *malware* est en effet d'une simplicité enfantine. Chaque

objet connecté est protégé par des identifiants (nom d'utilisateur et mot de passe). Le premier problème est que ceux-ci sont la pupart du temps très difficilement modifiables par les utilisateurs qui, bien souvent, ignorent même leur existence. De plus, ceux entrés par défaut par le fabricant sont généralement d'une simplicité enfantine – par exemple, 1234 pour un mot de passe. En réalité, Mirai se contente de scanner l'Internet des objets pour tester une série de mots de passe et repérer les appareils auxquels il peut accéder. Le code source publié à la fin septembre, par exemple, comprenait la liste des mots de passe testés par le *malware*. Et **ceux-ci n'étaient qu'au nombre de 61**… ce qui a pourtant été suffisant pour lancer une attaque de grande envergure.

Une société chinoise, notamment, s'est retrouvée au centre des critiques : XiongMai Technologie. Des identifiants utilisés par Mirai (nom d'utilisateur : Root, et mot de passe : xc3511) sont en effet configurés par défaut sur une bonne partie de ses appareils. Le 24 octobre, XiongMai a reconnu sa responsabilité et **annoncé le rappel de près d'un million de ses produits**, principalement des caméras.

Mais faire reposer la responsabilité de ces attaques sur un seul fabricant serait trop facile. Tout d'abord parce que d'autres ont été touchés par Mirai et que ce *malware* n'est sans doute que la partie émergée de l'iceberg. D'autres réseaux de *botnets* ont été utilisés, dans les attaques du 21 octobre ou même dans d'autres inconnues du grand public. Le 22 septembre, Octave Klaba, patron de l'hébergeur français OVH, a par exemple **annoncé sur Twitter** que sa société avait également fait l'objet d'une attaque DDoS menée par un *botnet* composé d'objets connectés, sans que l'on sache si celle-ci était liée à celle menée contre KrebsonSecurity.

L'affaire a en tout cas pris un tournant politique. Aux États-Unis, où se situent les principales victimes, les autorités ont annoncé avoir ouvert une enquête et l'autorité compétente, la Federal Communications Commission (FCC), a été officiellement **interpellée par un parlementaire**. En Europe, **la Commission européenne a annoncé**, au début du mois, avoir lancé une réflexion qui devrait déboucher sur une nouvelle législation visant à renforcer les obligations de sécurité des objets connectés.

En attendant que les fabricants se décident à renforcer la sécurité de leurs appareils, ou que les politiques les y contraignent, l'Internet des objets reste donc le nouvel eldorado des pirates.

Directeur de la publication : Edwy Plenel
Directeur éditorial : François Bonnet
Le journal MEDIAPART est édité par la Société Editrice de Mediapart (SAS).
Durée de la société : quatre-vingt-dix-neuf ans à compter du 24 octobre 2007.
Capital social : 28 501,20€.
Immatriculée sous le numéro 500 631 932 RCS PARIS. Numéro de Commission paritaire des publications et agences de presse : 1214Y90071 et 1219Y90071.
Conseil d'administration : François Bonnet, Michel Broué, Laurent Mauduit, Edwy Plenel (Président), Sébastien Sassolas, Marie-Hélène Smiéjan, Thierry Wilhelm. Actionnaires directs et indirects : Godefroy Beauvallet, François Bonnet, Laurent Mauduit, Edwy Plenel, Marie-Hélène Smiéjan ; Laurent Chemla, F. Vitrani ; Société Ecofinance, Société Doxa, Société des Amis de Mediapart.
Rédaction et administration : 8 passage Brulon 75012 Paris
Courriel : contact@mediapart.fr
Téléphone : + 33 (0) 1 44 68 99 08
Télécopie : + 33 (0) 1 44 68 01 90
Propriétaire, éditeur, imprimeur : la Société Editrice de Mediapart, Société par actions simplifiée au capital de 28 501,20€, immatriculée sous le numéro 500 631 932 RCS PARIS, dont le siège social est situé au 8 passage Brulon, 75012 Paris.
Abonnement : pour toute information, question ou conseil, le service abonné de Mediapart peut être contacté par courriel à l'adresse : serviceabonnement@mediapart.fr. ou par courrier à l'adresse : Service abonnés Mediapart, 4, rue Saint Hilaire 86000 Poitiers. Vous pouvez également adresser vos courriers à Société Editrice de Mediapart, 8 passage Brulon, 75012 Paris.