Qui se cache derrière Anna-Senpai, l'auteur du botnet IoT Mirai

Mirai a été le nom de la fin de l'année 2016. Ce botnet a mis en lumière la faiblesse des objets connectés en les enrôlant pour mener des attaques violentes en déni de service. Brian Krebs, chercheur en sécurité, a été une des premières victimes de Mirai, avec OVH. Piqué au vif par le niveau des offensives DDoS, Brian Krebs a mené l'enquête pour en savoir un peu plus sur le ou les auteurs. Il vient de publier les résultats de ses investigations.

Il est parti du moment où l'auteur de Mirai a publié le code source du botnet sous le pseudonyme Anna-Senpai (un personnage d'un dessin animé japonais Mirai Nikki, qui a donné son nom au botnet par la même occasion). Tout d'abord, Brian Krebs souligne que Mirai n'est pas né avec Anna-Senpai, « *sa création a duré 3 ans* ». Pendant cette période, il a pris plusieurs noms « Bashlite », « Gafgyt », « Qbot », « Remaiten » et « Torlus ». Chacun de ces botnets IoT concourait au même objectif, trouver des failles dans les objets connectés, les infecter et mener des attaques par saturation. Une des cibles privilégiées par les attaquants était les serveurs Minecraft.

Quand ProTraf apparaît pour la première fois

En 2014, un groupe baptisé « Lelddos » s'en était fait une spécialité. Brian Krebs a interrogé Roberto Coehlo, patron de ProxyPipe, société chargée de protéger les serveurs Minecraft et qui a subi une attaque DDoS de 300 Gbit/s en juin 2014. Le responsable se rappelle avoir été contacté et menacé à la mi-2015 par un jeune homme, Christopher "CJ" Sculti, Jr, propriétaire d'une société de protection contre les DDoS Datawagon dont les serveurs étaient hébergés chez ProTraf Solutions. Ce dernier souhaitait attirer les clients de ProxyPipe sur ses solutions. Or, ProxyPipe a été attaqué massivement au même moment où Christopher "CJ" Sculti, Jr a réussi à désactiver les comptes Skype de l'entreprise. Elle a perdu des clients et donc de l'argent dans cette histoire. Plus tard, le jeune homme a eu une conversation avec Brian Krebs où il se vantait d'avoir scanné le web et avoir découvert de nombreux objets connectés vulnérables. Pour Roberto Coehlo, il ne fait aucun doute que Sculti et ProTraf Solutions étaient les principaux membres de l'organisation Lelddos.

Le Far West des forums underground

En dénouant un peu plus la pelote de laine, Brian Krebs tombe sur un autre nom, celui d'un employé de ProTraf Solutions, Josiah White, spécialiste dans l'atténuation des attaques DDoS. Il serait à l'origine de deux botnets IoT, Bashlite et Qbot, et était connu sous le pseudonyme LiteSpeed. Une implication reconnue à demi-mot lors d'un entretien avec le chercheur, qui a toutefois tenté de se dédouaner d'avoir voulu vendre et publier leur code source. Selon lui, il y aurait été contraint par un membre d'un forum underground (hackforums.net), baptisé Vypor, sous peine de voir des détails de sa vie privée dévoilés et sous la pression de menaces sur sa famille. Il explique aussi que ses « amis » revendaient en douce ses exploits. Un vrai panier de crabes.

Jha Paras = Anna-Senpai = Dreadiscool ?

Poursuivant son enquête, Brian Krebs constate que ProTraf Solutions comprend un autre employé, Jha Paras. Ni plus ni moins que le président de la société. Sur son profil Linkedin (cf image ci-dessous), il est indiqué qu'outre sa connaissance de l'environnement Minecraft, ses compétences en informatique sont étoffées, « C#, Java, Golang, C, C++, PHP, x86 ASM, sans parler des langages des navigateurs web comme Javascript et HTML/CSS ». Un CV aux accents de déjà-vu pour le chercheur en sécurité. En effet, il a retrouvé les mêmes compétences sur HackForums chez un membre nommé Anna-Senpai. De fil en aiguille, l'étau se resserre.

Mais ce n'est pas tout, en creusant l'historique de Jha Paras, Krebs a découvert un autre nom, Dreadiscool. Ce dernier est à l'origine d'un projet Open Source sur GitHub pour les plateformes de jeux vidéo. Une recherche sur Google montre un compte lié à une dizaine de forums sur la programmation informatique et Minecraft. Sur ces forums, ce profil critique les attaques contre les serveurs Minecraft et demande des conseils pour s'en prémunir. Brian Krebs indique : « *à un moment, il a pensé qu'il serait moins frustrant et plus rentable de protéger les serveurs Minecraft* ». D'où la création de ProTraf. Autre élément qui laisse à penser que Jha Paras, Dreadiscool et Anna-Senpai ne font qu'un, l'avatar utilisé par Dreadiscool. On voit une scène de Pulp Fiction avec John Travolta et Samuel L Jackson dont les têtes ont été modifiées. Le visage de John Travolta est celui de Vypor (membre qui a forcé Josiah White à publier le code source de botnet) et Samuel L. Jackson voit son visage remplacé par celui de Tucker Preston, cofondateur de BackConnect Security, société spécialisée dans la protection des attaques DDoS. Dans l'image, on voit également un personnage féminin d'un film d'animation japonais, B Gata H Hei. Or, Dreadiscool est aussi un compte utilisateur sur le site MyAnimeList.net où les membres indiquent les dessins animés qu'ils ont vus. Dreadiscool en a vu 9 dont B Gata H Hei, mais surtout un certain Mirai Nikki (qui a donné son nom au botnet et à Anna-Senpai).

Une lutte d'influence pour les contrôles des botnets IoT

La suite de l'histoire est une lutte d'influence pour être le botnet IoT le plus puissant et le plus rémunérateur. Anna-Sempai s'est servi d'une technique qui a d'abord été utilisée contre Mirai par Roberto Coehlo, patron de ProxyPipe : les plaintes contre les hébergeurs. Une de ses plaintes a permis de débrancher un serveur C&C de Mirai réduisant ainsi sa nocivité.

Le pirate a donc envoyé plusieurs plaintes à des hébergeurs leur demandant de supprimer des serveurs soupçonnés d'être des serveurs de commandes & contrôle de botnets concurrents à Mirai. Si les hébergeurs ne répondaient pas aux exigences, la sanction était une attaque DDoS massive. Brian Krebs révèle l'histoire de l'hébergeur FranTech dont le dirigeant a ignoré les menaces de Anna-Senpai qui, pour l'occasion, a encore changé de nom pour devenir « jorgeMichaels ». Il avait sollicité l'hébergeur pour supprimer des serveurs liés à Qbot. Refus de l'hébergeur qui a subi une attaque DDoS massive.

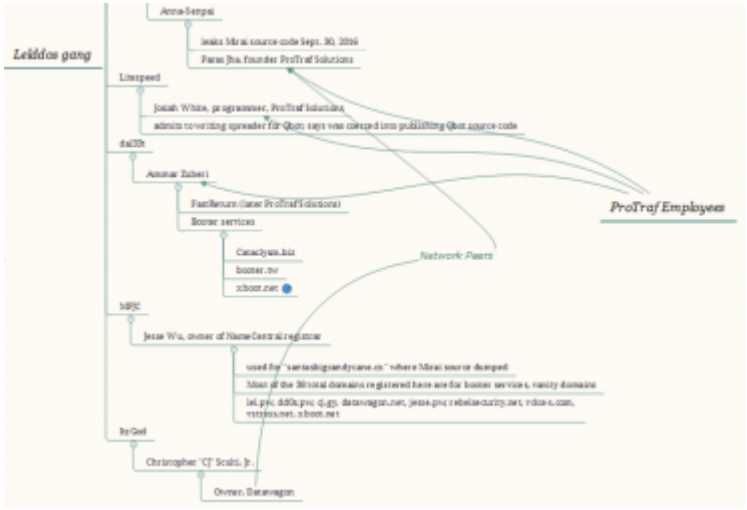
Une bascule du côté obscur

En croisant les différents codes de Mirai et ceux postés par Dreadiscool sur GitHub, Roberto Coehlo s'est rappelé avoir sympathisé en ligne avec Jha Paras il y a 4 ans de cela, quand le jeune homme travaillait pour Minetime, qui était protégé contre les attaques DDoS par ProxyPipe. Le dirigeant se rappelle avoir « *beaucoup communiqué et avoir programmé plusieurs projets communs* ». Et de se vanter de lui « *avoir enseigné presque tout* ». Mais avec le temps, cette relation s'est dégradé : « *il est devenu de plus en plus arrogant. Il a besoin de reconnaissance auprès des autres* ». Roberto Coehlo constate qu'après une attaque DDoS contre Minetime en 2013, Jha Paras a rejoint HackForums et n'a plus donné de nouvelles depuis.

La confession d'un employé de ProTraf

A la fin de sa longue enquête, Brian Krebs a eu un entretien avec un ancien employé de ProTraf, Ammar Zuberi, qui a lui confié que Jha Paras était le responsable de Mirai. Le code source du botnet a été rendu public sur le site santasbigcandycane.cx enregistré via Namecentral. Cet obscur registrar n'était connu que de 5 personnes : Ammar Zuberi, CJ Sculti, Paras Jha, Josiah White et le propriétaire de Namecentral Jesse Wu. En voyant la publication du code source de Mirai via Namecentral, Zuberi affirme avoir demandé à Jha Paras s'il était derrière cette manœuvre. Ce dernier a souri et lui a répondu oui.

Brian Krebs termine en notant que Jha Paras n'a pas souhaité faire de commentaires sur les différentes allégations que renferme le billet du journaliste. Ni le FBI qui a dû analyser avec intérêt le travail d'investigation du chercheur en sécurité. Ci-dessous un récapitulatif des connexions d'Anna-Senpai avec ProTraf



A lire aussi :

Leet : un botnet IoT plus effrayant que Mirai arrive

A louer : un botnet Mirai de 400 000 objets pour lancer des DDoS

Photo credit: aha42 | tehaha via Visualhunt.com / CC BY-NC