FIC 2020 : la cybergendarmerie fait l'autopsie de l'anéantissement d'un réseau de botnets

À Lille, sur le Forum International de la Cybersécurité, Futura a rencontré le cybergendarme en charge de la neutralisation de l'un des plus grands réseaux de botnets au monde. Il dévoile les dessous de ce fait d'armes. RV

ANSSI, ministère des Armées, ministère de l'Intérieur... ! l'État français et ses services spécialisés en cyberdéfense et cybersécurité disposent de stands imposants sur le Forum International de Cybersécurité (FIC). Du côté des gendarmes, se trouvent les représentants du Centre de lutte contre les criminalités numériques (C3N), et c'est un maréchal des logis-chef tenant à rester anonyme qui accueille Futura. Le militaire a participé à l'un des plus grands faits d'armes de la cybergendarmerie française. Il fut même le chef de l'équipe de cybercombattants qui a neutralisé l'un des plus importants botnets de la planète en août dernier.

Pour Futura, il a pris le temps de décortiquer ce qu'il s'est vraiment passé durant cette enquête et cette neutralisation qui n'a pas toujours bien été interprétée par les médias.

Retadup, c'est d'abord le nom d'un malware qui a contaminé plus d'1,3 million d'ordinateurs sur la planète pour constituer un botnet géant. Le vecteur de contamination reposait essentiellement par une transmission *via* les clés USB. Et, selon le militaire, « *le malware servait surtout à réaliser des opérations de cryptominage pour générer des Monero »*. Pour expliquer sa dangerosité, le sous-officier emploie un langage guerrier en qualifiant le botnet de *« véritable arme de destruction massive cyber »* en raison de sa puissance de feu. Sa taille est largement supérieure à celle du botnet qui génère 70 % du trafic de spams et le malware *Retadup* pourrait servir à réaliser bien d'autres exactions bien pires que de générer de la cryptomonnaie.

Un rapprochement inédit

Ce botnet a été découvert par Avast en début d'année 2019. L'éditeur de solution de sécurité a constaté que 200.000 de ses clients avaient été infectés par ce virus. Mais c'est surtout le rapprochement inédit entre Avast et la gendarmerie qui fait que ce fait d'armes est une première. Deux ans auparavant, lors de la Botconf, une conférence de cybersécurité où se trouvait le colonel en charge du C3N, celui-ci avait annoncé qu'il souhaitait que les éditeurs d'antivirus collaborent avec la gendarmerie en cas de détection d'un réseau de botnet. Une déclaration dont s'est souvenu Avast.

Par chance, alors qu'il se déplaçait de pays en pays régulièrement, le serveur de *Command & Control* (C&C) qui pilotait le botnet se trouvait justement hébergé en France. Le parquet a donc saisi les experts pour qu'ils mènent une perquisition. C'est ainsi qu'ils ont pu faire un clone du C&C pour l'analyser sans perturber le fonctionnement du Botnet. « *Nous avons ainsi pu constater que les ordinateurs infectés se connectaient toutes les 30 secondes au C&C pour recevoir de nouvelles instructions. S'il n'y avait pas de mise à jour, ils reprenaient alors leur tâche précédente »,* explique le gendarme.

« Nous n’avons pas désinfecté »

« J'ai procédé à l'analyse criminologique et j'ai trouvé 11 versions du malware sur le serveur. Seule, la dernière était active, mais notre cellule technique a découvert que toutes disposaient d'une faille de conception, ajoute le militaire. *Nous avons donc trouvé une ruse à laquelle les concepteurs de Retadup n'avaient pas pensé. Pour reprogrammer le virus, un fichier contenant les nouvelles instructions était envoyé par le C&C. Nous avons donc eu l'idée de faire croire au malware, qui se connectait donc toutes les 30 secondes, qu'un fichier était disponible et il s'est mis en mode de mise à jour. Le souci, c'est que le fichier en question était vide »,* détaille notre interlocuteur. Après des tests poussés, les gendarmes ont remplacé le serveur malveillant avant qu'il ne soit déplacé dans un autre pays avec l'autorisation du procureur et le stratagème a fonctionné.

“

Nous ne nous somme pas mis dans l'illégalité […]. Nous avons juste envoyé un fichier de mise à jour vide

Sans nouvelles instructions, le malware est devenu inoffensif et cette mise à jour s'est répandue progressivement à presque toutes les machines du botnet. Le sous-officier tient à souligner que, contrairement à ce qui est souvent dit, « *nous ne nous somme pas mis dans l'illégalité, car nous n'avons pas désinfecté les ordinateurs. D'ailleurs, le parquet nous avait bien expliqué que, pour agir, l'utilisation d'un script était illégale pour neutraliser le réseau. Nous avons juste envoyé un fichier de mise à jour vide ».* Pour ce qui est des C&C, ils ont aussi été neutralisés, car les noms de domaine ont été redirigés dans ce que l'on appelle un *Sinkhole*, autrement dit, les limbes du Web. Ceci dit, les ordinateurs portent toujours en eux ce malware devenu une coquille vide.

Un gel douche, pas comme les autres

Juste à côté du maréchal des logis, se trouve un capitaine entouré de différents objets du quotidien : un gel douche, un désodorisant, une peluche et un répéteur Wi-Fi. Ces accessoires sont ici pour présenter un nouveau service spécialisé baptisé « Plateau d'Investigations des Objets Connectés » (PIOC). Comme son nom l'indique, il est exclusivement dédié aux objets connectés utilisés à des fins criminelles. Ainsi, lors d'investigations pour n'importe quelle affaire, cette équipe spécialisée peut être appelée afin de chercher ce qui est susceptible de provenir d'un accessoire connecté.

Ces produits du quotidien renfermaient tous des objets connectés utilisés pour nuire. Dans les exemples qu'il livre, le gel douche logeait une dashcam Wi-Fi servant à filmer sous la douche l'ex-compagne d'un prévenu. L'électronique de la peluche avait été modifiée pour émettre à plus de 4 Km. Elle devait permettre au père d'un enfant de prouver la maltraitance de son enfant pour en récupérer la garde. Mal lui en a pris... Enfin, le déodorant enfermait une clé USB comprenant des images pédophiles. En plus de chercher ces gadgets connectés détournés dans les objets les plus improbables, l'équipe dispose d'outils permettant de les détecter sur les sites, même lorsqu'ils ne sont pas actifs. Des outils sur lesquels le capitaine refuse d'en dire plus. Encore une fois, ce FIC vient montrer que la cyber reste l'univers du secret.

Ce qu'il faut retenir

- Le virus *Retadup* a infecté 850.000 ordinateurs à travers le monde.
- Les cybergendarmes du C3N ont désactivé le serveur de commande.
- Les cybergendarmes ont également neutralisé le virus sur les ordinateurs infectés.