BotConf 2018 : les dilemmes de la sécurité informatique

Le dilemme du défenseur, qui se doit de protéger une surface d'attaque considérable, hétérogène et parfois difficile à contrôler. De son point de vue, la moindre intrusion sur un élément quelconque de son infrastructure représente à minima l'équivalent d'une brèche dans un barrage, et plus probablement l'ouverture des portes de la ville de Troie au cheval du même nom…

Les stratégies de sécurité ont pour but de répondre à ce dilemme. Ainsi le cloisonnement par (micro)segmentation physique ou virtuelle, la gestion des autorisations, l'homogénéisation des niveaux de sécurité, la supervision et la réponse à incident, etc… ne visent au final qu'à réduire la surface d'attaque et à contenir l'intrusion dont tout bon spécialiste de sécurité sait qu'elle est inévitable.

L'attaquant quant à lui, doit affronter un dilemme symétrique. Il sait qu'il sera à même de prendre pied par un moyen ou par un autre dans le Système d'Information cible. En revanche, il va être confronté à un arsenal de techniques de détection qui sauront tirer profit de la moindre erreur, de la moindre anomalie, du moindre détail qui pourrait s'avérer suspect. Se déclencheront alors les opérations de réponse à incident visant d'une part à colmater la faille (ou à brûler la statue de bois), et d'autre part à lancer d'éventuelles procédures pénales.

Cette approche peut paraître systémique; elle reste néanmoins assez proche de la réalité, comme nous avons pu le constater lors de la BotConf 2018. Cette conférence (dont la 6ème édition se tenait la semaine dernière à Toulouse) vise essentiellement à mettre en évidence, tant les techniques de compromissions et de contrôle massives mises en œuvre dans les botnets, que leur analyse et les actions menées avec succès contre ces réseaux. Une illustration sans ambiguïté des dilemmes évoqués plus haut.

Ainsi, quand il s'agit du défenseur, ce dernier se trouve confronté à des trésors de technologie et d'ingéniosité. Ainsi certains malwares sont véhiculés par de vrais documents (word ou pdf) précédemment « volés » sur d'autres systèmes. Ils répondent donc aux critères de cohérence, de langage ou de pertinence de la personne ciblée et semblent entièrement légitimes. L'exploitation rapide et massive de nouvelles failles dans les applications populaires reste un moyen simple mais terriblement efficace de prendre la main sur un ensemble conséquent de systèmes, avec lesquels la communication s'effectue maintenant via des protocoles peer-to-peer.

Cette technique offre la performance et la flexibilité nécessaires à des opérations plus « lourdes » telles que la récupération de données, le téléchargement de nouveaux modules (voire de mises à jour du malware), ou le travail collaboratif de validation et de crackage de mots de passe ou le minage de monnaie électronique.

Dans ce dernier domaine, des mécanismes de blockchain adaptés aux opérations malveillantes ont même été développées afin de les protéger et de les optimiser. Nous trouverons donc des systèmes de chiffrement asymétrique ou des « proof of work » indépendants du matériel afin de lisser les consensus. Dans ce dernier cas l'IoT apparait clairement comme la prochaine cible…

Enfin les techniques d'évasion et de « reprise après incident », entendez par là « rétablissement après blocage par les défenseurs » s'améliorent notablement. Et si, il y a quelques années, il fallait encore deux semaines pour qu'un botnet se rétablisse et corrige les failles ayant conduit à son démantèlement, le dernier délai observé pour Kelihos.D était de vingt minutes. Une résilience à faire pâlir de jalousie certains responsables de production…

Toutefois, le travail de l'attaquant n'est pas non plus toujours simple. Et le premier facteur d'erreur est la complexité accrue des composants mis en œuvre dans le cadre d'une attaque. C'est particulièrement le cas des mécanismes de chiffrement, dont la fréquente faiblesse est à l'origine de nombreuses opérations d'identification des différents composants. Il peut s'agir de la liste des pairs, qui peut ensuite être altérée et conduire à « l'extinction » du réseau; du protocole de communication qui sera ensuite analysé puis bloqué; voire des adresses des serveurs maîtres…

La complexité est également présente dans l'architecture, dans la mesure où plusieurs niveaux de relais sont mis en œuvre, non seulement pour offrir des capacités de mise à l'échelle dans le cadre des botnets les plus conséquents, mais également pour masquer le niveau principal des serveurs maîtres. Et dans ce cas encore, l'évolution de ces architectures donne lieu à des erreurs (ou oublis) explosant généralement un des serveurs de premier niveau.

Enfin, un autre travers de la complexité et de la richesse des botnets est la réutilisation de parties de code existantes, parfois achetées sur le marché noir. Une analyse des appels aux API et des DLL utilisées permet ainsi de distinguer certaines familles et variantes encore inconnues, et de mettre en place les contre-mesures de manière assez triviale.

Viennent les problèmes de sécurité des composants du botnet. Nous avons ainsi le cas d'une erreur d'un serveur lors de l'analyse d'un message erroné. Les chercheurs ont ainsi pu prendre la main sur un serveur maître et en mener une analyse poussée dont une conséquence sera détaillée un peu plus loin. L'absence de chiffrement de certains codes malicieux en permet également une analyse simple, qui révèle parfois des informations utiles, telles que les adresses des serveurs du botnet…

Enfin les erreurs d'étourderie, comme l'archive d'un malware contenant encore des répertoires au nom de son auteur, ou -et c'est la conséquence de la prise de contrôle du serveur vulnérable auquel nous avons fait allusion plus haut- les captures d'écran de test du malware affichant la page Facebook de son auteur !

Ainsi, les dilemmes de la sécurité informatique sont une réalité largement mise en évidence lors de la dernière BotConf, dont la conclusion reste toutefois que nous sommes confrontés à des individus présentant les mêmes faiblesses, mais pour lesquels l'échec se traduit généralement par de longues périodes de prison ferme…