Sécurité : une solution made in France pour lutter contre les APT

Un travail de trois ans en sous-marin, hébergé par Armature Technologies. C'est ainsi que Philippe Gillet, le président de cette société de conseil en cybersécurité (à droite sur photo), décrit le développement de GateWatcher, une solution de lutte contre les menaces avancées (ou APT pour *Advanced Persistent Threat*) 100 % française. La première du genre, selon les fondateurs de cette jeune société, Philippe Gillet donc (le directeur technique de GateWatcher) et Jacques de La Rivière (le Pdg, à gauche sur l'image ci-dessus). Selon ces derniers, la solution est bâtie sur une approche originale, mêlant **recours aux signatures**, et – surtout – **approche Big Data**. Logique car les signatures ne sauraient suffire à lutter contre les APT. Quatre de ces menaces avancées sur cinq se basent en effet sur une ou plusieurs failles zero day, par définition absentes des bases de signatures.

Le principe de l'algorithme embarqué par les boîtiers GateWatcher ? Il se base sur une **inspection des binaires** des applicatifs présents dans le SI (fournie par l'éditeur pour les logiciels courants ou réalisée par l'entreprise elle-même sur ses solutions propres ou systèmes 'exotiques') et détecte les comportements suspects, sur la base d'analyses statistiques. « *Les systèmes, même les plus décriés, se sont durcis ces dernières années. Les vulnérabilités par dépassement de tampon (buffer overflow), c'est terminé. Mais, en face, les pirates ont aussi gagné en compétences ; ils emploient désormais des techniques bien plus furtives, comme le ROP (return-oriented programming) ou le JOP (jump-oriented programming), consistant à manipuler la mémoire des systèmes. Notre solution se base sur le fait que ces techniques ont un mode de fonctionnement assez prévisible.* » Bref, GateWatcher ne prédit évidemment pas où seront les failles zero day – ce qui est rigoureusement impossible – mais plutôt le comportement qu'auront les souches infectieuses. « *La solution effectue des comparaisons entre les événements suspects sur le réseau et une base de données statistiques d'exploitations potentielles.* »

Mieux que les sandbox ?

Une approche unique, selon Philippe Gillet. Même si la méthode employée par la société française n'est pas sans rappeler celle de DarkTrace, une start-up britannique qui analyse elle aussi les comportements suspects sur le réseau. DarkTrace est le nouveau bébé de Mike Lynch, l'ex-Pdg d'Autonomy, éditeur britannique vendu quelque 11 milliards de dollars à HP, dans des conditions décriées.

« *Nous ne prétendons dont pas détecter 100 % des APT, mais, contre ces menaces avancées, notre approche est bien plus pertinente que celle des bacs à sable (sandbox)* », affirme le directeur technique. Une pique adressée à l'éditeur américain FireEye, considéré comme un pionnier de la détection d'APT avec sa solution de sandbox. La solution de GateWatcher a notamment été développée par Jean-Marie Bourbon, un consultant d'Armature qui, en juillet 2014, avait dévoilé des techniques permettant de contourner les technologies de l'éditeur américain…

« *Au début des années 2010, la sandbox a connu un vrai engouement*, explique Philippe Gillet. *C'était le seul moyen qu'on avait trouvé pour détecter et étudier des malwares sans disposer de leurs signatures. Mais les concepteurs d'APT se sont adaptés et testent aujourd'hui leurs logiciels sur Cuckoo Box, une solution Open Source de bac à sable. Les attaquants utilisent donc des techniques de détection ou d'évasion de sandbox, rendant cette technologie inopérante. Raison pour laquelle les entreprises se détournent d'elle aujourd'hui, au moins en ce qui concerne la détection d'intrusion.* »

Tableaux de bord

L'outil de détection temps réel GateWatcher s'appuie sur des sondes (appelées G-Cap) et une intelligence collective (G-Center). Il fonctionne sur une dérivation du trafic, depuis un équipement télécoms ou réseau, et **supporte pour l'heure le 10 Gbit/s**. « *Nous travaillons sur une version 40 Gbit/s, correspondant à un cœur de réseau d'opérateur* », précisent les co-fondateurs de la société. La solution prend également en charge les flux chiffrés.

Conçu pour les SOC (Security Operation Center, centres opérationnels de sécurité) des grandes entreprises ou des prestataires spécialisés, GateWatcher propose quelques fonctions complémentaires à la détection, comme la capacité à **rejouer une attaque pour l'analyser**, des

tableaux de bord donnant une vue synthétique de l'état du réseau, des indices de sévérité permettant de qualifier les menaces… Développée en France, la solution a reçu un avis favorable de l'Anssi, et non une habilitation officielle pour l'instant. « *Tout simplement parce que l'habilitation n'existe pas encore pour la détection d'intrusion* », précise Philippe Gillet.

Selon la société, le prix d'entrée de la solution, pour la surveillance d'un réseau, se chiffre à **entre 50 000 et 60 000 euros** (maintenance non comprise). La solution du jeune éditeur hexagonal est actuellement en test chez Citya Immobilier (3ème administrateur de biens en France), au Crédit Agricole et dans d'autres organisations (banques, industriels et administrations).

A lire aussi :

Profession : chasseur de hackers
Le réseau de Kaspersky piraté par Duqu 2.0
Vol de données : la facture grimpe pour les entreprises françaises