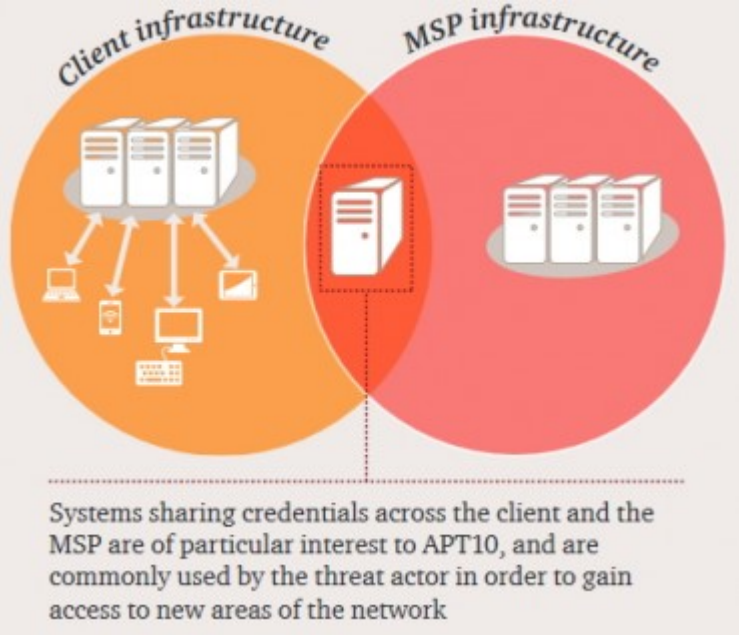
Des pirates chinois attaquent les entreprises via les services Cloud

La maturité des attaques ciblées contre les entreprises est montée d'un cran. *« Un groupe de piratage a mené l'une des campagnes d'espionnage les plus prolifiques depuis l'APT1 en 2013, employant de nouvelles tactiques pour atteindre une large audience »*, a alerté PwC (Pricewaterhouse Coopers) lundi 3 avril. En collaboration avec BAE Systems et le National Cyber Security Centre (NCSC) britannique, la branche réseau du cabinet d'audit a découvert ce qu'il considère comme *« l'une des plus importantes campagnes mondiales de cyber-espionnage jamais organisées »*. Pas moins.



De quoi s'agit-il ? Du piratage des infrastructures de fournisseurs de services managés à partir desquelles les cyber-attaquants remontent aux serveurs des organisations qui y ont recours. Une opération que PwC a baptisé 'Cloud Hopper'. Les cyber-criminels derrière ces agissements seraient le groupe de hackers chinois APT10. *« PwC et BAE Systems croient que le groupe de piratage largement connu sous le nom 'APT10' a mené la campagne d'espionnage en ciblant les fournisseurs de services informatiques externalisés comme une façon d'accéder aux organisations de leurs clients à travers le monde, leur conférant un accès sans précédent à la propriété intellectuelle et aux données sensibles »*, indique PwC dans son communiqué. APT10 est le nom donné par FireEye à un groupe de pirates chinois également référencé sous les appellations Red Apollo (par PwC UK), CVNX (par BAE), Stone Panda (par CrowdStrike), et menuPass Team (plus globalement).

Un grand volume de données exfiltrées

Les méthodes d'infection restent relativement classiques et s'appuient sur le spear-phishing, ou harponnage. Cette méthode de phishing ciblé fait appel à des techniques d'ingénierie sociale qui visent à tromper le destinataire d'un e-mail pour l'inciter à installer, à son insu, un malware ou visiter une page infectieuse, à partir desquels les pirates ouvrent une porte d'entrée sur le réseau. Objectif ici : prendre le contrôle des accès d'employés de prestataires Cloud, afin d'exploiter les canaux de communication existant entre les services managés de ces derniers et les serveurs des entreprises clientes. De la grande distribution aux technologies en passant par l'énergie, l'industrie manufacturière, le secteur public ou l'industrie pharmaceutique, tous les grands secteurs sont touchés par cette campagne.

PwC se garde de préciser les noms des fournisseurs de services managés touchés par les intrusions d'APT10. Les fournisseurs de services d'hébergement seraient particulièrement prisés du groupe de hackers identifié en 2009. Au total, *« le groupe a exfiltré un grand volume de données provenant de plusieurs victimes et a utilisé des réseaux compromis pour déplacer furtivement ces données dans le monde entier »*. Les entreprises d'Amérique du Nord, du Brésil, de France, de Suisse, du Royaume-Uni, du Nord de l'Europe, de la Corée du Sud, de l'Inde, de Thaïlande, d'Afrique du Sud ou encore d'Australie ont ainsi été la cible d'APT10, selon le rapport sur Cloud Hopper. Selon BAE, *« il est impossible de dire aujourd'hui combien d'organisations pourraient avoir été impactées »*. Si les chercheurs ont focalisé leurs travaux sur 2016, il est probable que les intrusions dans les systèmes des services managés aient débuté en 2014. Signalons qu'un certain nombre d'organisations japonaises, dont les noms ne sont pas précisés, ont également été visées au cours d'une seconde campagne d'attaques simultanée aux pénétrations des services Cloud.

Surveiller jusqu'à la chaîne d'approvisionnement

Sans surprise, les attaques se poursuivent en 2017. *« L'approche indirecte de cette attaque souligne la nécessité pour les organisations d'avoir une vision complète des menaces auxquelles elles sont exposées – y compris celles de leur chaîne d'approvisionnement*, souligne Kris McConkey, consultant sécurité chez PwC. *Les organisations du monde entier devrait travailler avec leurs équipes de sécurité et leurs fournisseurs pour surveiller les signes avant-coureurs de compromission de leur réseau et s'assurer qu'elles répondent et se protègent en conséquence. »*

Lire également

Un groupe de pirates menace de réinitialiser 200 millions d'iPhone

2016, l'année des vols de données massifs

Comment la Russie crée des unités d'élite de pirates informatiques