

Les pirates informatiques recrutent des complices chez les opérateurs télécoms

✕	Les pirates informatiques recrutent des complices chez les opérateurs télécoms
---	---

Un rapport de Kaspersky détaille les nombreuses menaces qui ciblent les opérateurs de télécommunications, réparties en deux catégories : celles qui les ciblent directement (DDoS, campagnes APT, failles sur des équipements, ingénierie sociale...) et celles qui visent les abonnés à leurs services. Parmi les premières, le recrutement de complicités internes, sous la menace ou par appât du gain, progressent, même si elles restent l'exception.

Les opérateurs de télécommunications constituent une cible de choix pour les cyberattaques. Ils gèrent des infrastructures de réseau complexes utilisées pour les communications téléphoniques et la transmission de données et stockent de grandes quantités d'informations sensibles. Dans ce secteur, les incidents de sécurité ont augmenté de 45% en 2015 par rapport à 2014, selon PwC. Dans un rapport intitulé « Threat intelligence report for the telecommunications industry » publié cette semaine par Kaspersky, l'éditeur de logiciels de sécurité détaille les 4 principales menaces qui visent les opérateurs de télécommunications et fournisseurs d'accès Internet (FAI) : les attaques en déni de service distribué (en hausse), l'exploitation de failles dans leur réseau et les terminaux clients, la compromission d'abonnés (par ingénierie sociale, phishing ou malware) et, enfin, le recrutement de personnes capables d'aider les cyber-criminels en interne, au sein même des entreprises attaquées.

☒ Lorsque les attaques passent par des collaborateurs contactés par les cybercriminels, il est difficile d'anticiper ces risques car les motivations sont diverses : appât du gain, collaborateur mécontent, coercition ou tout simplement négligence. Certains de ces relais internes agissent de façon volontaire, d'autres y sont forcés par la menace ou le chantage. Chez les opérateurs de télécoms, on demande principalement à ces « insiders » de fournir un accès aux données, tandis que chez les fournisseurs d'accès Internet (FAI), on les utilise en appui à des attaques contre le réseau ou des actions de type man-in-the-middle (MITM). Même si le recours à des collaborateurs indélébiles reste rare, cette menace progresse, selon Kaspersky, et ses conséquences peuvent être extrêmement critiques car elle peut ouvrir une voie directe vers les données ayant le plus de valeur. Le chantage est l'un des vecteurs de recrutement le plus efficace. A ce sujet, le spécialiste en technologies de sécurité remet en mémoire l'intrusion sur le site de rencontres extra-conjugales Ashley Madison, l'été dernier. Celle-ci a permis le vol de données personnelles que les attaquants ont pu confronter à d'autres informations publiquement accessibles pour déterminer où les personnes travaillaient et les compromettre.

Même des pirates inexpérimentés peuvent mener des attaques DDoS

D'une façon générale, Kaspersky répartit en deux catégories l'ensemble des menaces visant les opérateurs télécoms à tous les niveaux : d'une part, celles qui les ciblent directement (DDoS, campagnes APT, failles sur des équipements, contrôles d'accès mal configurés, recrutement de complicités internes, ingénierie sociale, accès aux données), d'autre part celles qui visent les abonnés à leurs services, c'est-à-dire les clients des opérateurs mobiles et des FAI. Les attaques en déni de service distribué ne doivent pas être sous-estimées, rappelle Kaspersky, car elles peuvent être un signe précurseur d'une deuxième attaque, plus préjudiciable. Elles peuvent aussi servir à affecter un abonné professionnel clé, ou encore à ouvrir la voie à une attaque par ransomware à grande échelle. Le 1er cas a été illustré par l'intrusion subie en 2015 par Talk Talk, l'opérateur de télécoms britannique, résultant dans le vol d'1,2 millions d'informations clients (noms, emails, dates de naissance, données financières...). L'enquête a montré que les pirates avaient dissimulé leurs activités derrière l'écran de fumée d'une attaque DDoS. L'un des éléments préoccupants de ces menaces, c'est que même des attaquants inexpérimentés peuvent les organiser de façon relativement efficace, rappelle Kaspersky.

Des équipements vulnérables et des malwares difficiles à éliminer

Les vulnérabilités existant dans les équipements réseaux, les femtocells (éléments de base des réseaux cellulaires) et les routeurs des consommateurs ou des entreprises fournissent aussi de nouveaux canaux d'attaques, de même que les logiciels exploitant des failles dans les smartphones Android. Ces intrusions mettent en œuvre des malwares difficiles à éliminer. En dépit des nombreux vols de données perpétrés au cours des 12 derniers mois, les attaques se poursuivent, exploitant souvent des failles non corrigées ou nouvellement découvertes. En 2015, par exemple, le groupe Linker Squad s'est introduit chez Orange en Espagne à travers un site web vulnérable à une injection SQL et a volé 10 millions de coordonnées sur les clients et les salariés. Par ailleurs, dans de nombreux cas, les équipements utilisés par les opérateurs présentent des interfaces de configuration auxquelles on accède librement à travers http, SSH, FTP ou telnet et si le pare-feu n'est pas configuré correctement, ils constituent une cible facile pour des accès non autorisés, explique encore Kaspersky.

En résumé, les menaces visant les opérateurs de télécommunications existent à de nombreux niveaux – matériel, logiciel, humain – et les attaques peuvent venir de différentes directions. Les opérateurs doivent donc « regarder la sécurité comme un processus englobant tout à la fois la prédiction, la prévention, la détection, la réponse et l'enquête », conclut Kaspersky.

Article de Maryse Gros



Réagissez à cet article

Original de l'article mis en page : Les pirates recrutent des complices chez les opérateurs télécoms – Le Monde Informatique