Une faille JBoss ouvre la porte des serveurs au ransomware SamSam

Talos, la branche de recherche en sécurité de Cisco, a approfondi ses travaux sur la prolifération des ransomwares. Fin mars, l'expert en sécurité se penchait particulièrement sur les méthodes de propagation et d'attaque du rançongiciel SamSam, qui vise l'ensemble du parc informatique des entreprises plus que les seuls PC de bureau, en s'appuyant sur des failles de JBoss pour pénétrer les serveurs d'applications.

Aujourd'hui, après avoir scanné l'ensemble des serveurs JBoss connectées à Internet, Cisco Talos a dénombré pas moins de 3,2 millions de machines potentiellement vulnérables à SamSam. Parmi celles-ci, plus de 2□100 sont aujourd'hui compromises avec l'installation de backdoors depuis 1□600 adresses IP qui n'attendent plus que le chargement de SamSam (ou d'un autre ransomware). Lequel, une fois actif, entreprend de chiffrer tout ou partie des données des disques durs des PC et serveurs. Seule le paiement d'une rançon permettra de délivrer les données ainsi prises en otage. Ces dernières semaines, plusieurs organisations, dont des hôpitaux, en ont été victimes. Cisco a alerté les différentes organisations cibles de ces attaques en devenir. On y retrouve des établissements scolaires mais aussi des Gouvernements, des compagnies aériennes, notamment.

Des systèmes compromis à plusieurs reprises

Plus précisément, nombre de systèmes affectés embarquent le logiciel Destiny de l'éditeur Follet. Il s'agit d'un gestionnaire de bibliothèque notamment utilisé par les collèges à travers le monde entier. Selon Cisco, Follet a déployé un patch qui comble les failles de sécurité des systèmes des versions 9.0 à 13.5 mais supprime également tous les fichiers non relatifs à Destiny, ce qui devrait aider à supprimer les backdoors potentielles.

Dans son enquête, Talos a constaté la présence de plusieurs webshell sur les serveurs affectés (mela, shellinvoker, jbossinvoker, zecmd, cmd, genesis, sh3ll et probablement Inovkermngrt et jbot). Rappelons que les webshell sont des scripts qui permettent d'interagir sur les serveurs via le protocole HTTP. Donc, de potentiellement pouvoir prendre le contrôle à distance des serveurs (comme l'indique cette alerte de l'US Cert). La présence de nombreux webshell *« implique que bon nombre de ces systèmes ont été compromis à plusieurs reprises par les différents acteurs »*, rapporte la division sécurité de Cisco dans son blog. Et qu'il est urgent de les éradiquer.

Lire également
SamSam, le plus petit des grands ransomwares, analysé
Le ransomware Jigsaw lance son compte à rebours
Ransomware Locky : la France parmi les deux principaux pays ciblés

crédit photo © Carlos Amarillo – Shutterstock