SamSam, le plus petit des grands ransomwares, analysé

Hier, nous nous étions fait l'écho d'une recrudescence de campagne de rançongiciels visant le monde hospitalier. Les noms de Locky, Maktub et de SamSam ont été mis en avant comme responsable du verrouillage des ordinateurs de plusieurs hôpitaux à l'étranger, mais aussi en France. Arrêtons-nous un moment sur SamSam qui dispose de quelques particularités.

Ce ransomware a été découvert par l'équipe de Cisco Talos. Craig Williams, responsable technique, souligne que « *par le passé des ransomwares comme CryptoLocker ou TeslaCrypt nécessitaient que quelqu'un ouvre un fichier joint ou visite un site. SamSam, lui, cible les serveurs vulnérables* ». Une manière de répondre à un double objectif selon les experts en sécurité : être indétectable et provoquer un maximum de dégâts via le réseau. Un changement de paradigme aussi en passant de l'exécution de code à distance et non plus à l'interaction avec l'utilisateur.

Pour Craig Williams, SamSam est capable de pénétrer le réseau d'un hôpital en testant des vulnérabilités connues sur des serveurs non mis à jour. En cas de succès, l'attaquant va gagner un accès au réseau et découvrir des données clés du système pour les chiffrer. *« On n'est pas dans le cadre d'un ordinateur verrouillé par un ransomware. Ce que cherche à faire SamSam, c'est bien de bloquer les serveurs et in fine tout le système IT de l'hôpital »*, constate le responsable.

Un chiffrement offline

Sur la partie technique, l'équipe de Cisco Talos a décortiqué SamSam et a donné quelques explications sur un blog. On apprend ainsi que les attaquants se sont servis de l'outil Open Source JexBoss pour tester et gérer les serveurs d'applications JBoss. Pour la partie communication, ils ont adopté un autre outil Open Source, REGeorg et plus spécifiquement un composant, tunnel.jsp. Une fois dans le système, SamSam part donc à la recherche des fichiers systèmes Windows pour les chiffrer.

Après, SamSam se charge de trouver d'autres fichiers (dont la liste est fournie dans le blog) pour « *les chiffrer avec Rijndael (AES) et crypte la clé en RSA-2048* ». Petite spécificité et non des moindres, SamSam est capable de chiffrer en mode déconnecté (offline), c'est à dire sans solliciter des actions du serveur de commande et contrôle.

Dans l'échantillon analysé par Cisco Talos, les spécialistes ont observé que le processus de chiffrement a cessé si le système fonctionne sur une version de Windows antérieure à Vista, probablement pour des raisons de compatibilités.

Un paiement de rançon en temps réel

Autre point souligné par Cisco Talos, le paiement de la rançon pour déverrouiller le système. Les cyberattaquants sont capables d'interagir directement et en temps réel avec les victimes pour leur demander de l'argent. Dans un premier temps, 1 puis 1,5 et, dans certains cas, 1,7 Bitcoin pour

débloquer un ordinateur du système. Au total, sur leur échantillon, 275 Bitcoins étaient demandés représentant une somme de 115 000 dollars. Des tests pour connaître les capacités des victimes à payer.

Des expérimentations qui expliqueraient pourquoi le monde hospitalier est en première ligne dans les campagnes de ransomwares. *« Les cybercriminels ont trouvé un coffre au trésor »*, explique Ben Johnson co-fondateur de Carbon Black, une société de sécurité à nos confrères de *SCMagazine*. Les hôpitaux contiennent des informations à forte valeur pour des pirates. « *Ils sont malheureusement plus vulnérables que les banques et cela ne devrait pas s'arrêter* », précise Mr Johnson. Pour Craig Williams, le secteur hospitalier est le premier sur la liste, mais les pirates ont déjà d'autres cibles en vue. Un tour d'échauffement !

A lire aussi :

Ransomware, haro sur le monde hospitalier

Un outil gratuit pour bloquer les ransomwares comme Locky

Crédit Photo : Carlos Amarillo / Shutterstock