Les utilitaires de déchiffrement fonctionnent contre toutes les versions de TeslaCrypt

	Les utilitaires de déchiffrement fonctionnent contre toutes les versions de TeslaCrypt

Il y a un mois environ, la clé principale de TeslaCrypt a été divulguée, ce qui a mis un terme à cette escroquerie qui marchait bien jusque là. Au cours de cette période, plusieurs utilitaires de déchiffrement capables de récupérer les fichiers endommagés par TeslaCrypt ont été créés.

Ainsi, Kaspersky Lab a actualisé son utilitaire Rakhni en y ajoutant un utilitaire de déchiffrement pour Bitman (TeslaCrypt) version 3 et 4. La semaine dernière, Cisco a réalisé une mise à jour similaire. Son outil est désormais capable de récupérer les fichiers chiffrés par l'ensemble des 4 versions existantes de ce ransomware.

D'après Earl Carter, analyste en chef chez Cisco Talos, la clé principale publiée le 19 mai était utilisée pour récupérer les fichiers chiffrés par TeslaCrypt version 3 et 4. Il ajoute : « Nous ne savons pas si cette clé principale fonctionne pour les versions antérieures. La version 2 était défectueuse et elle a pu être facilement déchiffrée et nous dispositons de l'utilitaire de déchiffrement pour la version originale. L'utilisateur devait d'abord identifier la version du ransomware qui l'avait infecté avant de pouvoir choisir l'utilitaire de déchiffrement adéquat. Nous avons actualisé l'utilitaire d'origine afin qu'il puisse s'occuper de toutes les versions existantes. »

Pour l'instant, les raisons qui ont poussé les opérateurs de TeslaCrypt à mettre un terme à leur projet sont inconnues. Les attaques de ransomwares contre des entreprises ou des particuliers ne faiblissent pas. D'après les estimations du FBI, au cours du premier trimestre seulement, les auteurs de ces attaques ont empoché plus de 200 millions de dollars américains sous la forme de rançons payées. D'ici la fin de l'année, ce chiffre pourrait atteindre 1 milliard. Ceci étant, TeslaCrypt, en tant qu'acteur sur ce marché juteux, n'était pas parfait. Il affichait des défauts qui avaient permis aux chercheurs, presque dès le début, de trouver dans le code les clés de déchiffrement et de créer des outils pour venir en aide aux victimes.

Le jeu du chat et de la souris pouvait commencer : les individus malintentionnés ont renforcé le chiffrement tandis que les chercheurs ont réalisé des analyses plus en profondeur pour trouver l'antidote. « Certains ransomwares utilisent le chiffrement symétrique et dans ce cas, il est possible de trouver la clé sur l'ordinateur et de déchiffrer les fichiers » explique Earl Carter. « D'autres privilégient l'infrastructure PKI et dans ce cas, il est plus difficile de récupérer les fichiers, principalement parce que la clé n'est pas enregistrée sur l'ordinateur infecté. »

Dès qu'un utilitaire de déchiffrement a été réalisé pour une des versions, d'autres chercheurs commencent également à fournir des efforts dans ce sens. Il est tout à fait possible que cela soit la raison pour laquelle les opérateurs de TeslaCrypt ont tué le projet.

« Les ransomwares sont très rentables et tout le monde veut sa part » signale Earl Carter. « Dans la mesure où toutes les versions [de TeslaCrypt] avaient été déchiffrées, on pourrait croire qu'elles n'étaient pas aussi rentables que le souhaitaient les opérateurs. Ceci n'est qu'une hypothèse car nous ne disposons pas des preuves concrètes. Mais à première vue, on dirait bien que c'est cela qui s'est passé. Le malware était toujours déchiffré, les revenus récoltés ne correspondaient pas aux attentes et à la fin, ils ont décidé de faire une croix sur le projet.

La clé principale de TeslaCrypt a été publiée sur le forum d'assistance technique du ransomware après qu'un chercheur de l'ESET avait repéré des indices qui laissaient entendre que le projet allait être abandonné et il a demandé la clé aux auteurs. TeslaCrypt pourrait être remplacé par CryptXXX qui, d'après BleepingComputer, est déjà diffusé via des kits d'exploitation répandus. Certaines sociétés spécialisées dans la sécurité de l'information, comme Kaspersky Lab, surveillent attentivement le développement de CryptXXX et ont même créé des outils de déchiffrement pour ses premières versions.

Le système de chiffrement adopté par TeslaCrypt était actualisé fréquemment afin que les chercheurs ne puissent pas le déchiffrer. Au début de cette année, ce malware se propageait via des redirections WordPress et Joomla ainsi que via le kit d'exploitation Nuclear. Au mois d'avril, des chercheurs de chez Endgame ont découvert deux nouveaux échantillons du ransomware dotés d'outils d'obfuscation et de dissimulation supplémentaires ainsi que d'une liste d'extensions plus longue. A ce moment, TeslaCrypt se propageait déjà via des campagnes de spam.

« Les kits d'exploitation ont commencé à charger des ransomwares au lieu d'enregistreurs de frappe ou de malware de fraude au clic ». L'association du kit d'exploitation et de la publicité malveillant a considérablement simplifié la tâche des attaquants » résume Earl Carter.

Article original de Securelsti

Réagissez à cet article

Original de l’article mis en page : Les utilitaires de déchiffrement fonctionnent contre toutes les versions de TeslaCrypt – Securelist