Ransomware : Locky active le mode pilotage automatique

Il n'y a pas que les voitures autonomes qui se pilotent toutes seules (parfois avec des conséquences dramatiques). Les malwares aussi (avec des conséquences moins dramatiques humainement mais qui peuvent s'avérer aussi ennuyeuses qu'onéreuses). Locky, l'un des ransomwares les plus actif et tristement célèbre, connaît une nouvelle évolution. Il vient de passer en mode d'auto-pilotage. Autrement dit, l'agent malveillant n'a plus besoin de se connecter à un serveur distant de contrôle et commandes (C&C) pour engager le chiffrement des fichiers victimes de son attaque. C'est du moins ce qu'ont découvert les chercheurs en sécurité de l'éditeur Avira.

Locky en mode furtif

L'autopilotage permet désormais à Locky d'opérer en mode furtif. *« Avec cette étape, [les attaquants] n'ont plus à jouer au chat et à la souris avec la mise en place incessante de nouveaux serveurs avant qu'ils ne soient blacklistés ou fermés »*, commente Moritz Kroll, spécialiste des logiciels malveillants au Protection Labs d'Avira. Il rappelle en effet que, précédemment, la configuration de Locky comprenait des URL pointant vers des serveurs de C&C ainsi qu'un algorithme de génération de domaines pour créer des liens supplémentaires vers des serveurs de commande et contrôle.

En se libérant de cette dépendance, le mode Autopilote du malware permet à ses auteurs (ou utilisateurs) d'économiser des coûts d'infrastructure et optimiser ainsi la rentabilité de leurs opérations. *« Les cybercriminels affinent le mode d'infection 'hors-ligne'*, ajoute le chercheur d'Avira. *En réduisant au minimum les activités en ligne de leur code, ils n'ont pas à payer pour autant de serveurs et de domaines supplémentaires. »* Et si ce mode de fonctionnement déconnecté ne leur permet plus de remonter les statistique des infections en cours, il présente l'avantage de se montrer plus discret aux yeux des responsables du réseau. *« Auparavant, les administrateurs systèmes pouvaient bloquer les connexions aux serveurs C&C et se prémunir des opérations de chiffrement de Locky. Ces jours sont désormais révolus*, prévient Moritz Kroll. *Locky a réduit les chances des victimes potentielles d'éviter une catastrophe de chiffrement. »*

Moins de deux minutes

Ce mode Autopilote n'est en fait utilisé qu'en dernier recours, lorsque Locky n'est pas parvenu à se connecter aux serveurs pré-programmés ou générés dynamiquement (jusqu'à 12 adresses par jour). Moins de deux minutes suffisent entre le début de l'infection et le démarrage du chiffrement en mode «offline», selon Avira. Qui plus est, le malware se montre toujours plus discret. *« Dans mon cas, alors qu'il continue de passer par les serveurs C&C, Locky a fait 3 pauses, d'une durée de 10 à 20 secondes*, poursuit le chercheur. *Ce n'est pas très pratique pour les administrateurs qui essaient de repérer les demandes [de connexion]. Même si les liens que Locky tente d'établir peuvent être observés, il chiffre les fichiers en cas d'échec. Donc, si un administrateur remarque ces connexions, il a très peu de temps pour éteindre l'ordinateur avant que les données ne soient endommagées. »*

En revanche, le mode opératoire de paiement de la rançon pour déverrouiller les fichiers chiffrés ne change pas, lui. La configuration de Locky contient toujours une adresse pointant vers le service de l'attaquant dans le réseau d'anonymisation Tor. A la différence que la clé de déchiffrement est potentiellement commune à toutes les victimes du mode Autopilote pour la même variante du malware, avance Avira. Ce qui laisse supposer qu'une entreprise pourrait utiliser la même clé pour déchiffrer l'ensemble des PC infectés par Locky Autopiloté au lieu de payer une clé pour chaque machine victime. *« Évidemment, le mieux est de prendre ses précautions, disposer d'une politique de sauvegarde, et ne pas être atteint du tout »*, rappelle Moritz Kroll. Évidemment !

Lire également

Une variante de Locky se fait passer pour un fichier système Windows
Comment un chercheur français a infecté des arnaqueurs avec Locky
Ransomware : Locky reprend du service