

Alerte : Le ransomware Locky passe en mode autopilote

 Alerte : Le ransomware Locky passe en mode autopilote

Une nouvelle variante de Locky ajoute un mode autopilote qui proscriit les connexions aux serveurs de commandes et contrôles. Un mode toujours plus discret.

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 actifs 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 statistiques 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. »...[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Original de l'article mis en page : Ransomware : Locky active le mode pilotage automatique