# Augmentation de 30% des demande de rançon informatique en 3 mois

| | |
|---|---|
|  | **Augmentation de 30% des demande de rançon informatique en 3 mois** |

**Le #ransomware a dépassé les attaques de type APT (menaces persistantes avancées) pour devenir le principal sujet d'actualité du trimestre. 2900 nouvelles variantes de malwares au cours de ces 92 jours.**

Selon le rapport de Kaspersky Lab sur les malwares au premier trimestre, les experts de la société ont détecté 2900 nouvelles variantes de malwares au cours de cette période, soit une augmentation de 14 % par rapport au trimestre précédent. 15 000 variantes de ransomware sont ainsi dorénavant recensés.

**Un nombre qui va sans cesse croissant.**
Pourquoi ? Comme j'ai pu vous en parler, plusieurs kits dédiés aux ransomwares sont commercialisés dans le blackmarket. Autant dire qu'il devient malheureusement très simple de fabriquer son arme de maître chanteur 2.0.
Au premier trimestre 2016, les solutions de sécurité de l'éditeur d'antivirus ont empêché 372 602 attaques de ransomware contre leurs utilisateurs, dont 17 % ciblant les entreprises. Le nombre d'utilisateurs attaqués a augmenté de 30 % par rapport au 4ème trimestre 2015. Un chiffre à prendre avec des pincettes, les ransomwares restant très difficiles à détecter dans leurs premiéres apparitions.

**Locky , l'un des ransomwares les plus médiatisés et répandus au 1er trimestre**
Le ransomware Locky est apparu, par exemple, dans 114 pays. Celui-ci était toujours actif début mai. Un autre ransomware nommé Petya est intéressant du point de vue technique en raison de sa capacité, non seulement à crypter les données stockées sur un ordinateur, mais aussi à écraser le secteur d'amorce (MBR) du disque dur, ce qui empêche le démarrage du système d'exploitation sur les machines infectées.
Les trois familles de ransomware les plus détectées au 1er trimestre ont été Teslacrypt (58,4 %), CTB-Locker (23,5 %) et Cryptowall (3,4 %). Toutes les trois se propagent principalement par des spams comportant des pièces jointes malveillantes ou des liens vers des pages web infectées. « Une fois le ransomware infiltré dans le système de l'utilisateur, il est pratiquement impossible de s'en débarrasser sans perdre des données personnelles. » confirme Aleks Gostev, expert de sécurité en chef au sein de l'équipe GReAT (Global Research & Analysis Team) de KL.

**Une autre raison explique la croissance des attaques de ransomware** : les utilisateurs ne s'estiment pas en mesure de combattre cette menace. Les entreprises et les particuliers n'ont pas conscience des contre-mesures technologiques pouvant les aider à prévenir une infection et le verrouillage des fichiers ou des systèmes, et négligent les règles de sécurité informatique de base, une situation dont profitent les cybercriminels entre autres. Bref, trop d'entreprise se contente d'un ou deux logiciels de sécurité, se pensant sécurisées et non concernées. L'éducation du personnel devrait pourtant être la priorité des priorités… [Lire la suite]

Article de Damien BANCAL

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybersécurité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Ransomware: +30% d'attaques en 3 mois – Data Security BreachData Security Breach*