

Une entreprise touchée toutes les 40 secondes par une attaque par Ransomware en 2016

✖	Une entreprise touchée toutes les 40 secondes par une attaque par Ransomware en 2016
---	--

Entre janvier et septembre 2016, la fréquence des attaques de ransomware contre les entreprises a triplé, passant d'une toutes les deux minutes une toutes les 40 secondes. Pour les particuliers, cet intervalle s'est réduit de 20 à 10 secondes. Avec l'apparition de plus de 62 nouvelles familles de logiciels rançonneurs au cours de l'année, le ransomware est la menace désignée comme fait marquant de l'année 2016. La rubrique Story of the Year fait partie de l'édition annuelle du Kaspersky Security Bulletin retraçant les principales menaces et statistiques de l'année écoulée et établit des prévisions sur ce que nous réserve 2017.

Le ransomware est devenu un réel business

Entre autres choses, 2016 a révélé à quel point le modèle RaaS (Ransomware as a Service) séduit désormais les criminels qui ne possèdent pas les compétences ou les ressources nécessaires pour développer leur propre malware ou n'en ont tout simplement pas envie. Le principe consiste pour les créateurs du code malveillant à offrir celui-ci « à la demande », en se bornant à vendre des versions modifiées à leurs clients qui les diffusent via du spam ou des sites web et reversent une commission à l'auteur, le principal bénéficiaire financier. « Le modèle classique de l'affiliation paraît aussi efficace pour le ransomware que pour les autres types de malware. Les victimes paient souvent la rançon, de sorte que l'argent coule à flots. Inévitablement, cela a conduit à l'apparition quasi quotidienne de nouveaux logiciels de cryptage », commente Fedor Sinitsyn, analyste senior en malware chez Kaspersky Lab.

L'évolution du ransomware en 2016

En 2016, le ransomware a poursuivi ses ravages à travers le monde, devenant de plus en plus élaboré et diversifié pour renforcer son emprise sur les données, les appareils, les particuliers et les entreprises :

- Les attaques sur les entreprises ont nettement augmenté. Selon l'étude Kaspersky Lab, une entreprise sur cinq au niveau mondial a subi un incident de sécurité informatique à la suite d'une attaque de ransomware et une petite entreprise sur cinq n'a jamais récupéré ses fichiers, même après avoir versé une rançon.
- Si certains secteurs d'activité ont été plus durement touchés que d'autres, notre étude indique que personne n'est véritablement épargné par le risque : le plus fort taux d'attaques frappe l'enseignement (de l'ordre de 23 %) et le plus faible, la grande distribution et les loisirs (16 %).
- Le ransomware « éducatif », conçu pour donner aux administrateurs système un outil permettant de simuler des attaques de ce type, a été rapidement et impitoyablement exploité par des criminels, donnant notamment naissance à Ded_Cryptor et Fantom.
- Parmi les méthodes de rançonnage observées pour la première fois en 2016 figure le cryptage de disque, consistant pour les auteurs des attaques à bloquer l'accès, non pas à quelques fichiers, mais à la totalité d'entre eux simultanément. Petya Dcryptor, alias Mamba, va encore plus loin en verrouillant l'ensemble du disque dur, grâce à des attaques de mots de passe par force brute pour accéder à distance aux appareils des victimes.
- Le ransomware Shade a montré sa capacité à changer d'approche vis-à-vis d'une victime si l'ordinateur infecté s'avère appartenir à des services financiers, pour télécharger et installer un spyware au lieu de crypter les fichiers.
- Les codes malveillants ont sensiblement perdu de leur qualité : c'est ainsi que de simples chevaux de Troie rançonneurs, présentant des erreurs de programmation et des fautes grossières dans les demandes de rançon, multiplient les risques pour les victimes de ne jamais récupérer leurs données...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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 : Kaspersky Lab recense une attaque toutes les 40 secondes contre les entreprises en 2016 – Global Security Mag Online