Arnaques entre cybercriminels !

	Arnaques entre cybercriminels !

Les chercheurs de Kaspersky Lab ont découvert PetrWrap, une nouvelle famille de malware exploitant le module d'origine du ransomware Petya et distribuée via une plate-forme RaaS (Ransomware as a Service) pour mener des attaques ciblées contre des entreprises. Les créateurs de PetrWrap ont produit un module spécial qui modifie le ransomware Petya existant « à la volée », laissant les auteurs de ce dernier impuissants face à l'utilisation non autorisée de leur propre malware. Ce pourrait être le signe d'une intensification de la concurrence sur le marché souterrain du ransomware.

En mai 2016, Kaspersky Lab avait découvert le ransomware Petya, qui non seulement chiffre les données stockées sur un ordinateur mais écrase aussi le secteur d'amorce (MBR) du disque dur, ce qui empêche le démarrage du système d'exploitation sur les machines infectées. Ce malware est un modèle de RaaS (Ransomware as a Service), c'est-à-dire que ses créateurs proposent leur produit malveillant « à la demande », afin de le propager via de multiples distributeurs en s'octroyant un pourcentage des profits au passage. Pour s'assurer de recevoir leur part du butin, les auteurs de Petya ont inséré certains « mécanismes de protection » dans leur malware de façon à prévenir un usage non autorisé de ses échantillons. Les auteurs du cheval de Troie PetrWrap, dont les activités ont été détectées pour la première fois au début de 2017, sont parvenus à contourner ces mécanismes et ont trouvé un moyen d'exploiter Petya sans verser de redevance à ses auteurs.

Le mode de diffusion de PetrWrap reste à éclaircir. Après infection, PetrWrap lance Petya afin de chiffrer les données de sa victime, puis exige une rançon. Ses auteurs emploient leurs propres clés de chiffrement privées et publiques en lieu et place de celles fournies avec les versions « standard » de Petya. Cela leur permet d'exploiter le ransomware sans avoir besoin de la clé privée d'origine pour décrypter la machine de la victime, dans le cas où cette dernière paie la rançon…[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 d'expertises, d'audits, de formations et de sensibilisation 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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *PetrWrap : des cybercriminels volent le code de ransomware d’autres criminels Le nouveau ransomware mène des attaques ciblées contre des entreprises – Global Security Mag Online*