

Non, NotPetya n'est pas un ransomware... mais un logiciel de sabotage

✘	Non, NotPetya n'est pas un ransomware... mais un logiciel de sabotage
---	--

Le déchiffrement des machines impactées est impossible. La demande de rançon n'était donc qu'un leurre pour camoufler un cybersabotage. La piste d'un acte politique, probablement réalisé par une agence gouvernementale, émerge.

Mauvaise nouvelle pour toutes les victimes de NotPetya. Les dernières analyses des chercheurs en sécurité montrent que ce malware est en réalité un logiciel de sabotage déguisé en ransomware. Les victimes ne pourront donc retrouver leurs données, à moins qu'un expert arrive à détecter une faille dans le processus de chiffrement.

Plusieurs indices prouvent que les auteurs de NotPetya n'ont jamais eu l'intention d'envoyer une quelconque clé de déchiffrement. Le premier concerne l'identifiant unique affiché dans le message de rançonnage et que la victime doit envoyer aux pirates après avoir effectué le paiement en bitcoins. En théorie, cet identifiant doit permettre aux auteurs de NotPetya d'identifier la victime. Il doit, par conséquent, contenir des informations sur les clés de chiffrement utilisées sur la machine en question. Mais selon les chercheurs de Kaspersky, il s'avère que cet identifiant est totalement aléatoire. « *Les attaquants ne peuvent extraire une quelconque information de déchiffrement d'une telle suite de caractères aléatoire* », soulignent-ils dans une note de blog.



Kaspersky – L'identifiant unique affiché est totalement aléatoire

De son côté, le chercheur en sécurité Matt Suiche a découvert que les données de la zone d'amorçage ne sont sauvegardées nulle part, mais simplement remplacées par autre chose. Le système de fichier du disque serait donc de toute façon irrécupérable. « *La version actuelle de Petya a été réécrite pour être un wiper, et non un ransomware* », souligne l'expert... [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>



Réagissez à cet article

Source : *Non, NotPetya n'est pas un ransomware... mais un logiciel de sabotage*