# Petya : une vraie cyberarme, teintée de ransomware

Après la vague d'attaques du ransomware Petya (autrement appelé NotPetya, Petna, ExPetr) qui a chiffré et verrouillé des milliers de PC et de serveurs à travers le monde, les experts en sécurité se sont penchés sur cette opération. Et les premières conclusions de Comae Technologies et Kaspersky Lab, montrent que cette opération, sous couvert d'un ransomware, avait pour objectif de saboter et détruire des ordinateurs.

Premier élément donné par les experts pour qualifier cette offensive de cybersabotage, Petya fonctionne comme un ransomware, mais des indices cachés dans son code source révèlent que les utilisateurs ne pourront jamais récupérer leurs fichiers. Ils expliquent que Petya génère une ID aléatoire d'infection pour chaque ordinateur. Le malware n'utilise pas de serveur de commandes et contrôle, il s'appuie sur une ID d'infection pour stocker des informations sur chaque victime et la clé de chiffrement. Comme les données sont aléatoires pour chaque ID, le processus de déchiffrement est impossible, selon l'expert de Kaspersky, Anton Ivanov . « *Cela signifie tout d'abord que c'est le pire cas pour les victimes, même si elles paient la rançon, elles ne récupéreront pas les données. Ensuite, cela renforce la théorie selon laquelle l'objectif principal de Petya n'était pas financier, mais de destruction.* »

## MFT irrécupérable et un maigre butin récolté

En complément de l'analyse de Kaspersky, Matt Suiche, chercheur de Comae Technologies, a trouvé un autre élément aboutissant à la même conclusion. Dans son rapport, il montre que la récupération du fichier MFT original est impossible, malgré différentes opérations de recouvrement. Ce fichier gère l'emplacement des fichiers sur le disque dur, mais en restant chiffré, il n'y a aucun moyen de connaître où chaque fichier est situé sur un PC. « *La version originale de Petya modifiait le disque d'une façon à revenir sur ces changements. Le Petya actuel provoque des dommages permanents et irréversibles sur le disque* », indique Matt Suiche.

La finalité du Petya version 2017 est donc clairement de provoquer des dégâts en se masquant sous la couverture de ransomware. Une spécialiste de la threat intelligence, Grugq, a indiqué que « *le vrai Petya est une entreprise criminelle pour gagner de l'argent, mais cette version de Petya n'est certainement pas conçue pour gagner de l'argent. Elle est élaborée pour se diffuser rapidement et causer des dégâts, sous la couverture d'un ransomware* ». En appui de ses propos, il suffit d'aller voir sur le portefeuille bitcoin lié à l'opération pour s'en convaincre. Il affiche 45 transactions pour un montant d'environ 10 000 dollars. Wannacry avait réussi à faire mieux.

**A lire aussi :**

Un vaccin pour enrayer le ransomware Petya

Petya : 5 questions pour comprendre le ransomware qui terrorise les entreprises

**crédit photo © GlebStock – Shutterstock**