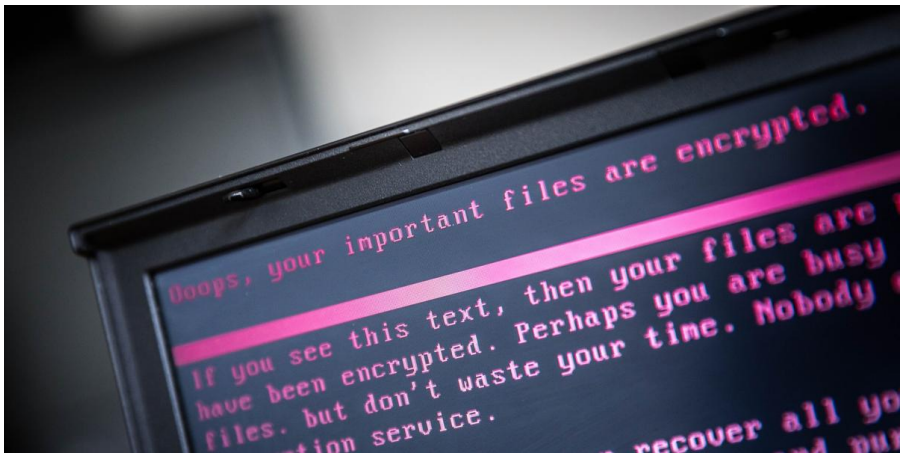
Comment fonctionne Petya, le virus qui a touché de nombreuses très grandes entreprises ?



Comment fonctionne Petya, le virus qui a touché de nombreuses très grandes entreprises ?

Il s'est répandu à très grande vitesse, et est plus évolué que son prédécesseur, WannaCry.

Après WannaCry, Petya. Pour la deuxième fois en quelques semaines, un « rançongiciel » (*ransomware*, en anglais) s'est largement propagé sur Internet, rendant inutilisable de nombreux ordinateurs et perturbant lourdement le fonctionnement de plusieurs grandes entreprises.
Le code de ce rançongiciel a été disséqué par de nombreux experts et entreprises de sécurité informatique ces dernières heures, permettant de mieux comprendre la manière dont il fonctionne.

Que fait-il exactement ?

Petya est un rançongiciel visant les systèmes Windows : il rend indisponibles les données d'un ordinateur, qui ne peuvent être déverrouillées qu'en versant une rançon. Il s'agit d'une variation très modifiée d'une souche apparue au printemps 2016.
A la différence de WannaCry, Petya commence par s'attaquer à la toute petite partie du disque dur – qui recense tous les fichiers présents dans la mémoire d'un ordinateur – et la chiffre, les rendant inutilisables. Ensuite, il s'en prend à la partie du disque dur qui permet de lancer le système d'exploitation, le logiciel qui fait fonctionner l'ordinateur. Cette partie est modifiée de manière à ce que l'ordinateur ne puisse plus démarrer en utilisant le système d'exploitation prévu. Lorsqu'on allume l'ordinateur, c'est Petya qui se lance, et le rançongiciel fait son travail. Un message s'affiche alors, réclamant que soient envoyés 300 dollars en bitcoin, la monnaie électronique, pour obtenir la clé de déchiffrement.
Il est extrêmement déconseillé de verser la rançon : outre le fait que payer entretient les réseaux mafieux qui se cachent souvent derrière les rançongiciels, l'adresse e-mail qui servait aux auteurs de Petya à rentrer en contact avec les victimes a été désactivée par le fournisseur de messagerie, rendant tout versement parfaitement inutile.

Comment se propage-t-il ?

Les développeurs de ce logiciel ont mis beaucoup de soin aux fonctionnalités d'infection de Petya, qui utilise plusieurs méthodes de propagation dites « *latérales* », vers les ordinateurs appartenant au même réseau que la machine infectée.
Une fois installé sur un ordinateur, Petya va chercher à y obtenir les plein pouvoirs et repérer les autres appareils branchés sur le même réseau. Le rançongiciel va ensuite fouiller dans l'ordinateur qu'il a infecté pour récupérer des identifiants et des mots de passe qu'il va pouvoir ensuite réutiliser dans le réseau pour prendre le contrôle de davantage d'appareils et démultiplier sa propagation. Ensuite, à l'aide de fonctionnalités classiques de Windows utilisées pour gérer les réseaux, il va se transférer vers d'autres machines.
Outre cette fonctionnalité, il utilise aussi deux outils – EternalBlue et EternalRomance – volés à la NSA, la puissante agence de renseignement américaine, qui, en exploitant une faille dans un protocole permettant aux ordinateurs de se « parler » au sein d'un même réseau, permettent sa propagation de machine en machine. EternalBlue était d'ailleurs déjà utilisé par WannaCry.
L'utilisation de plusieurs méthodes d'infection expliquerait pourquoi certaines machines pourtant immunisées contre EternalBlue et EternalRomance, car ayant installé les mises à jour de sécurité correspondantes de Microsoft, soient quand même infectées par Petya.
Son mécanisme de propagation à l'intérieur d'un réseau d'une entreprise fait que les postes de travail classiques ne sont pas les seuls à succomber à Petya. Des ordinateurs plus centraux, plus sensibles, sont aussi atteints, comme les serveurs sur lesquels fonctionnent les sites Web. C'est pour cette raison que plusieurs sites du groupe Saint-Gobain étaient inaccessibles mercredi 28 juin au matin, selon une source interne…[lire la suite]

Réagissez à cet article

Source : *Comment fonctionne Petya, le virus qui a touché de nombreuses très grandes entreprises ?*