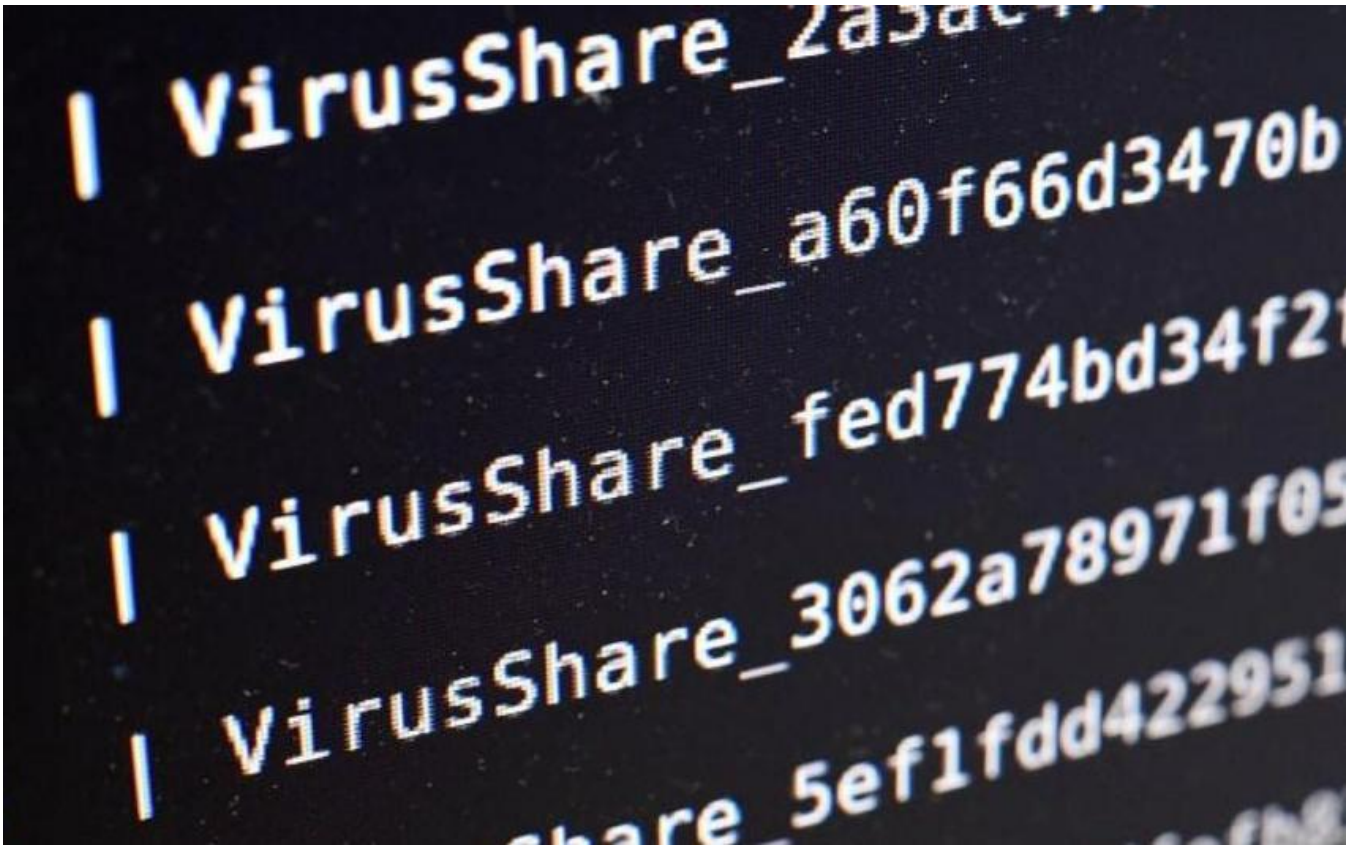
CYBERCRIMINALITÉ **28 Juin 2017**

# Comment se protéger contre les cyberattaques de type «Petya» ?

PAR STEVEN MEYER* Les fonctionnalités de Petya, qui attaque des entreprises du monde entier, sont très inhabituelles. L'analyse et les conseils de Steven Meyer, CEO de la compagnie genevoise spécialisée en cyber-protection ZENData.




Contrairement au ransomware classique, Petya ressemble davantage à une cyber-attaque de grande envergure. (Crédits: AFP)

15

15

Une nouvelle souche de ransomware surnommée «Petya» se déploie dans le monde à une vitesse alarmante, immobilisant des centaines d'entreprises telles que La SNCF, Merck, Maersk, Mondelez, WPP Group, Rosneft, Evraz et DLA Piper. Le logiciel malveillant se répand, entre autres, à l'aide de la même vulnérabilité existant dans Windows que WannaCry, le ransomware qui a infecté plus de 300'000 ordinateurs le mois dernier.

Depuis que la NSA a vu ses cyber-armes volées et publiées par les Shadow Brokers, de nombreux criminels les utilisent pour mener des attaques. La vulnérabilité en question « Eternel Blue » a déjà été corrigée par Microsoft en mars dernier, mais de nombreuses entreprises restent réticentes à mettre à jour leurs systèmes par peur de perdre des fonctionnalités, les poussant à ignorer ce correctif.

Les organisations et les personnes n'ayant pas encore appliqué la mise à jour de Windows pour cette vulnérabilité doivent le faire dès que possible. Il existe cependant des indications laissant à penser que Petya pourrait avoir plus d'un tour dans son sac pour se propager malgré tout à travers les réseaux.

### Prise de contrôle à distance

En effet, Petya aurait la fonctionnalité de recueillir des mots de passe et des données d'identification sur des ordinateurs Windows et des contrôleurs de domaine pour ensuite prendre le contrôle à distance d'autres systèmes.

Le vecteur d'infection initial et le patient zéro n'ont pas encore été découverts, mais plusieurs signes indiqueraient que l'attaque ait été amorcée par un mécanisme de mise à jour logicielle intégré dans M.E.Doc, qui est un programme de comptabilité que les entreprises travaillant avec le gouvernement ukrainien doivent utiliser.

### Un gouvernement pourrait être derrière

Contrairement au ransomware classique, Petya ressemble davantage à une cyber-attaque de grande envergure, cherchant plus à perturber, saboter et interrompre le bon fonctionnement d'un système informatique, qu'à extorquer de l'argent. On

pourrait éventuellement envisager qu'un gouvernement soit derrière cette attaque (WannaCry par exemple a été attribué à la Corée du Nord).

Plusieurs fonctionnalités de ce ransomware sont très inhabituelles. Ce dernier crypte le disque tout entier, empêchant la victime d'utiliser son ordinateur pour payer la rançon. Il comprend aussi la même adresse Bitcoin pour chaque victime, alors que la plupart des ransomware créent une adresse de paiement Bitcoin personnalisée pour chacune, afin de pouvoir attribuer le transfert. Finalement, Petya demande aux victimes de communiquer avec les hackeurs via email, tandis que la majorité des ransomwares exigent aux victimes de payer ou communiquer avec eux via Tor (un réseau mondial anonyme et décentralisé).

À l'heure de l'écriture de cet article, personne n'a confirmé avoir réussi à décrypter son ordinateur, et ce, même après avoir payé la rançon. L'adresse email utilisée par les hackeurs pour communiquer a été saisie par les autorités empêchant tous paiements futurs de rançons

## Comment se protéger contre cette attaque ?

Si vous allumez votre ordinateur et voyez un écran noir avec un message indiquant que vos documents ont été cryptés, il est malheureusement trop tard pour vous. Mais si un message indiquant la réparation de votre disque apparaît, ceci indique que vous avez été infecté, mais que vos données ne sont pas encore cryptées.

Nous vous recommandons donc d'éteindre votre ordinateur immédiatement, car vos données sont encore récupérables. En effet, le processus de cryptage ne commence que lorsque ce message s'affiche et vous pouvez donc récupérer vos documents si vous l'interrompez rapidement. (Il est aussi possible de détecter si un ordinateur a été infecté en vérifiant l'existence de ce fichier : C:/Windows/dllhost.dat)

Pour empêcher et prévenir toute infection, vous devez absolument maintenir votre système à jour, notamment en installant MS17-010.

Il vous faut aussi un antivirus (de préférence nouvelle génération qui n'utilise pas de signatures) qui peut détecter les activités d'un ransomware et empêcher l'infection.

Finalement, nous recommandons de façon systématique d'avoir une bonne hygiène informatique, en appliquant des préceptes de base, comme faire attention avant de cliquer sur un lien ou ouvrir un document, désactiver les services non utilisés ou obsolètes (tel que WMI et SMB1), mettre en place une segmentation du réseau informatique et toujours avoir un backup au cas où vos protections n'auraient pas suffi.

**CEO de la compagnie genevoise spécialisée en cyber-protection ZENData*