Ransomware Petya : la déjà trop longue liste des victimes

En quelques heures et par des mécanismes d'infection qui restent encore discutés au sein de la communauté des experts en sécurité, le ransomware Petya a infecté des centaines, voire des milliers d'entreprises dans le monde. Voici une liste (provisoire) des principales victimes connues à ce jour, des cas révélés au grand jour notamment en raison des conséquences de l'infection sur le fonctionnement de ces entreprises.

En France :

Auchan

Le géant de la distribution français a été touché via sa filiale ukrainienne . « *Les systèmes informatiques touchés ont été isolés et pour le moment, le problème est contenu* », a indiqué une porte-parole du groupe à *20 Minutes*. Les terminaux de paiement que possède le groupe dans le pays de l'Est sont inactifs, en raison de l'attaque par Petya.

Saint-Gobain

L'infection de Saint-Gobain, connu depuis mardi 27 juin en début d'après-midi, a eu des conséquences opérationnelles, avec certains salariés forcés à prendre une journée de RTT. Le groupe industriel indique aujourd'hui que le fonctionnement de ses systèmes est en passe de revenir à la normale. Un porte-parole de l'entreprise a souligné que l'attaque n'avait touché ni ses clients, ni ses lignes de production.

BNP Paribas

La banque a reconnu que sa filiale immobilière a bien été frappée par le ransomware. BNP Paribas a ajouté avoir pris des mesures pour contenir l'infection.

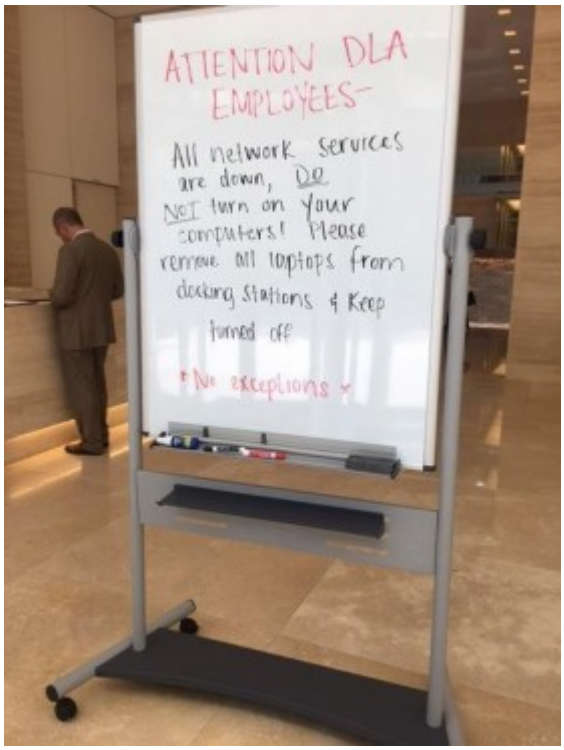
SNCF

Citée parmi les victimes, la SNCF indique avoir paré l'attaque, sans toutefois préciser combien de postes ont été pris en otage avant que le malware ne soit stoppé. La compagnie ferroviaire assure que cette attaque n'a pas eu de conséquence sur le fonctionnement des trains.

Les multinationales :

DLA Piper

La firme d'avocats a posté dans l'entrée de ses locaux à Washington un avertissement expliquant aux salariés que tous les services réseaux sont inactifs et leur demandant de ne pas allumer leur ordinateur (lire ci-contre).



Merck

Le géant de la pharmacie a confirmé dans un tweet que son réseau informatique avait été victime de Petya. Sans toutefois donner d'indication sur l'étendue de l'infection.

WPP

Le n°1 de la publicité a annoncé que plusieurs de ses agences, « *mais pas toutes* », ont été victimes du malware. Le groupe britannique indique travailler à limiter l'impact opérationnel de cette infection, qui a touché certains bureaux parisiens de WPP.

Mondelez

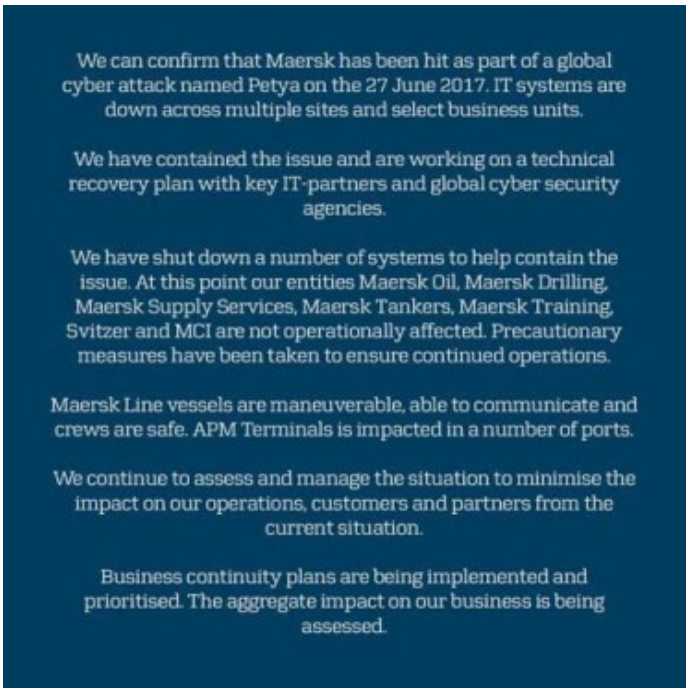
Le géant agroalimentaire a connu une panne informatique majeure hier, que la firme a reconnue sur Twitter. Sans établir toutefois un lien direct entre cette interruption de services et Petya.

Beiersdorf

Selon la chaîne de télévision régionale allemande *NDR*, « *plus rien ne fonctionne au siège* » de Beiersdorf, industriel qui fabrique notamment la crème Nivea. De nombreux salariés ont dû rentrer chez eux.

Maersk

Le n°1 du transport maritime, qui prend en charge un conteneur sur sept sur le globe, a reconnu que Petya a provoqué des pannes dans son système d'information global, sur de nombreux sites et diverses 'business unit'. Dans un message posté sur Twitter (ci-contre), le géant danois assure que les opérations de la plupart de ses activités ne sont pas affectées. Par contre, sa filiale APM Terminals, gérant des terminaux portuaires dédiés aux conteneurs, a été sévèrement touchée. Selon la télévision danoise, 17 terminaux ont été pris en otage par le ransomware.



En Ukraine :

Les banques ukrainiennes

L'hécatombe a démarré en Ukraine, aux environ de 10h45 hier. Plusieurs sources soupçonnent d'ailleurs que l'infection initiale par Petya résulte du détournement du système de mise à jour d'un éditeur métier de ce pays. Les banques du pays sont durement touchées, comme l'a confirmé la banque centrale de Kiev. « *Elles éprouvent des difficultés à prendre en charge leurs clients et faire des opérations bancaires* », a reconnu la banque centrale.

L'aéroport international de Kiev

Le directeur du Boryspil Airport de Kiev a expliqué sur Facebook que son organisation avait été touchée par Petya. « *Certains retards dans les vols ne sont pas à exclure* », a-t-il indiqué.

Ukrenergo

Le fournisseur d'électricité ukrainien, contrôlé par l'Etat, est lui aussi tombé dans les filets de Petya. Sans conséquence toutefois sur la fourniture d'électricité contrairement à la cyberattaque dont il a été victime en décembre 2016.

Centrale nucléaire de Tchernobyl

31 ans après l'accident nucléaire qui a rendu la ville ukrainienne tristement célèbre dans le monde entier, la centrale reste sous surveillance. Sauf que les ordinateurs de Tchernobyl ont été eux aussi touchés par la cyberattaque, forçant les techniciens de la centrale nucléaire chargés de contrôler la radioactivité du site accidenté à revenir à des mesures manuelles, avec des compteurs Geiger.

En Russie :

Rosneft

Victime de ce qu'il décrit comme une attaque « *puissante* », le groupe pétrolier russe précise que sa production, gérée par un système isolé, n'est pas affectée par le problème.

Des banques russes

Plusieurs établissements bancaires russes sont aussi victimes de Petya. En particulier toutes les filiales locales de Home Credit, un établissement de prêt aux particuliers, sont fermées ainsi que le centre d'appel russe de la firme.

Evraz

L'industriel russe de l'acier a confirmé avoir été touché par une cyberattaque, mais assure que sa production en est sorti indemne.

A lire aussi :

Un vaccin pour enrayer le ransomware Petya

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

Le ransomware GoldenEye infecte plusieurs entreprises, dont Saint-Gobain

Crédit photo © Carlos Amarillo – Shutterstock