Ces attaques ne doivent pas être prises à la légère puisqu'en les privant d'informations parfois très sensibles, elles peuvent être très dommageables pour les entreprises. Leurs auteurs semblent être des informaticiens professionnels ou du moins des hackers dotés de compétences en cryptographie. «Le chiffrement créé est très puissant. Ce sont loin d'être des débutants». Demandant d'être payés en bitcoins, ces derniers sont très difficiles à identifier et localiser. Le Cirel conseille néanmoins aux organisations de porter plainte afin de pouvoir démarrer un processus d'investigation. «Cela crée une base de travail pour la police, même si la chance de retrouver les attaquants, généralement installés dans des pays éloignés, est très mince. Et quand bien même ils seraient tracés, les forcer à dévoiler les clés de déchiffrement resterait très compliqué».

Sauvegarder son travail

Pour se prémunir de ce genre de virus, la première chose est de fréquemment sauvegarder ses fichiers personnels, notamment sur des disques durs externes, pour pouvoir les restaurer sans problème en cas d'attaque. «Faire des back-up réguliers permet de prévenir certains dégâts. Bien sûr, il faut penser à stocker les fichiers ailleurs que sur le réseau local, lui aussi pouvant être touché en cas d'attaque. Il est aussi important de veiller à disposer d'une période de conservation adéquate. Une fois le virus dans les systèmes, il faudra réinstaller toutes les machines concernées, y compris et surtout si une entreprise paye la rançon. Les organisations déjà piratées font des victimes faciles».

D'autres précautions d'usages sont de mettre à jour ses logiciels et inclure les plug-in des navigateurs, par exemple Flash Player ou Java Silverlight, ainsi que de ne pas ouvrir des pièces jointes, ni cliquer sur des liens en provenance de mails non sollicités. Enfin, il importe aussi de vérifier que son anti-virus est bien à jour. «Plus que des solutions techniques, ce sont des solutions humaines dont on a besoin dans ce cas là. Communiquer est essentiel. Il est important de prévenir les équipes et de leur apprendre à être prudentes vis à vis des e-mails qu'elles reçoivent, et en particulier avec ceux issus de nouveaux comptes. En ce sens, le département IT doit se montrer proactif et être disponible pour les autres branches de l'entreprise», conseille encore Vinot.