« La plupart des crypto virus viennent de Russie et d’Ukraine»

	« La plupart des crypto virus viennent de Russie et d’Ukraine»

Lors du salon Viva Technology, qui se déroulait à Paris du 15 au 17 juin, Ondrej Vlcek, directeur technique de la société Avast, l'un des antivirus les plus populaires du monde, animait une conférence sur «le commerce des malwares». Alors qu'une nouvelle attaque d'un logiciel malveillant appelé WannaCry a touché la planète en mai dernier, comment se prémunir d'une telle menace à l'avenir? Quelles sont les bonnes pratiques à adopter pour minimiser les risques?

Ondrej Vlcek : C'est le nom d'une catégorie de malwares («logiciels malveillants») qui réclament une rançon. Généralement, une fois qu'un rançongiciel est installé, le hacker s'empare du disque dur des victimes avec tous leurs fichiers personnels et demande de l'argent pour rendre les fichiers – sans quoi il les supprime. Une fois que l'ordinateur est infecté, le rançongiciel commence à chiffrer les fichiers, c'est-à-dire à les transformer afin qu'ils ne soient plus lisibles et que l'on ait besoin d'un mot de passe ou d'une clé de chiffrement pour y avoir accès. Il existe aujourd'hui de nouvelles variantes : en plus de crypter le disque dur, le rançongiciel peut aussi menacer l'utilisateur de faire fuiter les fichiers volés sur tout l'Internet.

Les vieux virus étaient beaucoup moins agressifs : ils détournaient votre ordinateur et l'utilisaient simplement pour envoyer des spams ou vous obliger à cliquer sur des pubs afin de générer de l'argent. Ils pouvaient aussi détourner votre ordinateur pour vous espionner et connaître vos mots de passe et identifiants. Là, une fois que la machine est infectée, vos fichiers personnels sont immédiatement modifiés et l'on vous réclame tout de suite de l'argent pour y accéder.

WannaCry est particulièrement inquiétant, car c'est un rançongiciel « auto-répliquant ». Qu'est-ce que cela signifie ?

Normalement, la plupart des logiciels malveillants aujourd'hui nécessitent l'action de l'homme : vous devez cliquer sur un lien, ouvrir une pièce jointe associée à un message électronique ou faire quelque autre exécution manuelle. Ici, tout est entièrement automatisé, c'est-à-dire que si vous avez un ordinateur vulnérable ou pas à jour, WannaCry peut l'infecter sans avoir besoin d'aucune interaction humaine, sans même que vous soyez devant votre ordinateur.

Quelles conséquences cela peut-il avoir sur l'ampleur de WannaCry ?

Cela rend sa propagation beaucoup plus rapide, car le fait de devoir cliquer sur un lien peut prendre des jours ou des semaines. Concernant WannaCry, le monde entier a été infecté en deux heures, le logiciel passant d'un ordinateur à l'autre.

Savons-nous aujourd'hui d'où viennent tous ces logiciels malveillants ? Et quelles sommes d'argent sont impliquées dans ces attaques ?

Pour ce qui concerne les rançongiciels, la plupart viennent de Russie et d'Ukraine (concernant WannaCry, la piste nord-coréenne semble la plus probable, ndlr). Nous avons des indications qui nous laissent penser que la majorité des rançongiciels aujourd'hui sont déployés de façon à ce qu'ils n'affectent pas les personnes vivant en Russie. La raison est qu'il existe en Russie une loi qui rend la création de rançongiciels illégale lorsqu'ils peuvent avoir un impact sur des citoyens russes, mais techniquement légale, d'une certaine manière, lorsqu'ils infectent des gens hors de Russie. L'année dernière, une estimation publiée par le FBI chiffrait le coût de ces cyberattaques à plus d'un milliard de dollars. Cette année, ce montant va probablement doubler et monter à plus de deux milliards de dollars.

Peut-on neutraliser ce type de logiciels malveillants ?

Il y a deux enjeux. Le premier, c'est la prévention. Très important : utiliser un système d'exploitation à jour afin de ne pas être trop vulnérable. Il faut aussi installer un logiciel antivirus de qualité. Enfin, il vaut mieux faire des sauvegardes régulièrement, car vous pouvez ainsi récupérer vos fichiers en cas d'attaque. Je fais des sauvegardes tous les jours et je recommande à tout le monde de faire de même.

La majorité des sauvegardes se font automatiquement, mais il faut être prudent sur ce point parce que, si le rançongiciel est installé sur l'ordinateur depuis un certain temps – un jour ou deux – la sauvegarde peut aussi enregistrer les fichiers infectés qui écraseront les anciennes versions saines.

Le second enjeu apparaît lorsque l'infection s'est produite : que peut-on faire ? En fait, quasiment la moitié des rançongiciels peuvent être supprimés et décryptés sans payer la rançon, car le chiffrement n'est pas bien installé, et possède des failles. Nous ou d'autres entreprises spécialisées dans la cybersécurité sommes capables d'accéder à l'algorithme de chiffrement et de décrypter les fichiers. Mais s'il est installé correctement, il n'y a aucune chance. Avec les ordinateurs d'aujourd'hui, décrypter les fichiers prendrait des centaines d'années.

Mon conseil : si vous êtes attaqué et qu'il n'y a pas de moyen de décrypter le disque dur aujourd'hui, ne supprimez pas vos fichiers infectés pour autant si vous en avez vraiment besoin. Bien que l'outil de décryptage pour ce rançongiciel en particulier ne soit pas disponible pour le moment, il peut l'être dans six mois, un mois ou même une semaine…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Cybercriminalité: «La plupart des rançongiciels viennent de Russie et d'Ukraine» – Technologies – RFI*