

# Cyberattaque mondiale par le cryptovirus Wannacrypt. Pourquoi changer une équipe qui gagne ?



## Des dizaines de milliers d'ordinateurs dans une centaine de pays ont été infectés depuis vendredi par un rançongiciel ou ransomware appelé Wannacry.

Denis JACOPINI Interviewé par RFI et propos personnels

### De quoi s'agit-il ? comment ça marche ?

Depuis vendredi 12 mai 2017, une cyberattaque d'envergure mondiale a touché des dizaines de milliers d'ordinateurs. En fait, peut-être beaucoup plus d'ordinateurs ont été infectés car il ne s'agit qu'un nombre estimatif.

Les ordinateurs en question ont été infectés par un virus qui s'est introduit dans les systèmes informatiques au travers de la messagerie électronique et d'e-mails.

Ce type de virus, une fois introduit et activé bloque l'usage de votre ordinateur ou de votre système informatique en cryptant vos données. Une fois vos données cryptées, un message vous invite à payer une somme d'argent en échange du code qui vous permet de décrypter vos fichiers et de les rendre à nouveau utilisables.

Le virus crypteur de données auquel nous avons à faire face s'appelle **WannaCry** (probablement un nom de ransomware qui est la contraction de Want a cry).

### Quelles suites peut-on donner à ce type d'attaques d'un point de vue judiciaire ?

Dans un monde idéal, il vous suffirait d'aller porter plainte à la Police ou à la Gendarmerie avec les preuves techniques à votre disposition pour qu'une enquête soit ouverte, que l'auteur du piratage soit recherché, retrouvé, arrêté, puis que son matériel saisi.

Des cas précédents ont montré que grâce à ça, des enquêteurs ont réussi à retrouver des clés de décryptage pour les mettre à disposition des victimes sur des sites internet spécialisés comme nomoreransom.org.

Malheureusement, la réalité est bien différente. Il est essentiel de recueillir les preuves de cette attaque (ne serait-ce que pour votre assurance et porter plainte), mais une fois la plainte déposée il peut se passer plusieurs mois ou plusieurs années avant de retrouver un pirate.

Dans ce grand désarroi certains décident de payer la rançon aux pirates pour récupérer l'accès à leurs données mais malheureusement peu nombreux seront qui auront satisfaction.

Dans le cas de cette cyber attaque mondiale, vu que le parquet de Paris se saisit de cette affaire, les choses devraient bouger plus vite.

Les chefs d'accusation qui peuvent être retenus contre les auteurs de cette d'attaque sont ;

- « accès et maintien frauduleux dans des systèmes de traitement automatisé de données », (deux ans d'emprisonnement et 30 000 euros d'amende et trois ans d'emprisonnement et 45 000 euros d'amende lorsque l'accès ou le maintien a entraîné une altération du système),
- « entraves au fonctionnement » d'un système de traitement automatisé de données (cinq ans d'emprisonnement et de 75 000 € d'amende);
- et « extorsions et tentatives d'extorsions ».

### N'est-on pas protégé contre cette forme d'attaque ?

Depuis des dizaines d'années, pirates informatiques et forces de l'ordre jouent au chat et à la souris. La quasi totalité des victimes ayant fait les frais de telles attaques numériques se sont bien rendu compte qu'elle ne recevraient d'aide ni de la Police, ni de la Gendarmerie pour avoir réparation. Particuliers, entreprises, TPE, libéraux PME et même grandes entreprises ayant été piégées par de telles attaques informatiques devraient se poser des questions sur les compétences de leurs informaticiens.

Spécialisés pour être au service de leurs clients pour gérer des parcs informatiques, ils assurent l'assistance, la maintenance, l'infogérance, mais pas la sécurité !

Assurer la sécurité informatique et plus particulièrement la sécurité de vos données est un métier à part entière et doit couvrir aussi bien des domaines techniques que pédagogiques pour amener les utilisateurs à faire évoluer leurs réflexes face aux usages du numérique.

### Pourquoi changer une équipe qui gagne ?

Le premier virus qui a demandé une rançon date de 1989 et s'appelle PC Cyborg. Certes, il n'y avait pas encore l'Internet qu'on connaît aujourd'hui, mais déjà un mode opératoire habile destiné à tromper la vigilance de l'utilisateur était utilisé.

Depuis que l'Internet s'est répandu, les techniques de propagation sont désormais différentes et peuvent s'adapter au support infecté (smartphone, tablette, PC, Mac et aussi objet connecté) mais la techniques pour s'introduire dans le réseau est depuis toujours la même dans la très grande majorité des cas. Même les virus, ransomwares (rançongiciels) les plus perfectionnés utilisent le bon vieux e-mail piégé ou le site Internet piégé pour s'introduire dans un réseau informatique. Les techniques de camouflage, de dissimulation et de propagation vers les autres équipements du réseau peuvent par contre, elles, être extrêmement perfectionnées, mais les techniques pour pénétrer un système sont quant à elles quasiment systématiquement les mêmes.

Pourquoi faire autrement quand cette technique fonctionne encore !

### Comment alors contrer de telles attaques ?

La solution n'est pas seulement technique. Certes il faut utiliser des logiciels de sécurité adaptés, mettre en place (et suivre !) des procédures de gestion de sécurité de parc rigoureuses mais ce qui nous paraît essentiel est le changement de comportement des utilisateurs.

C'est pour cela que nous proposons des formations dans le but de changer les réflexes des utilisateurs face à un e-mail, un site internet ou un appel téléphonique suspect. Nous apprenons à nos stagiaires à quoi ressemble le loup afin qu'ils évitent à l'avenir de le faire rentrer dans la bergerie.

### Qui se trouve derrière ces attaques ?

Enquêteurs et experts informatiques internationaux sont lancés sur les traces des pirates informatiques à l'origine de cette cyberattaque. L'attaque est « d'un niveau sans précédent » et « exigera une enquête internationale complexe pour identifier les coupables », a indiqué l'Office européen des polices Europol, en précisant qu'une équipe dédiée au sein de son Centre européen sur la cybercriminalité avait été « spécialement montée pour aider dans cette enquête, et qu'elle jouera un rôle important ».

On évoque désormais « 200.000 victimes dans au moins 150 pays » (d'après Rob Wainwright, le directeur d'Europol) visés par les pirates informatiques et de nombreuses entreprises ou services publics reconnaissent avoir été touchés ou avoir fait l'objet d'attaques. Mais il faudra attendre lundi et la réouverture des entreprises pour dresser un bilan plus complet de cette attaque, a-t-il prévenu.

Selon nous, si la vague de cyberattaques lancée vendredi semble marquer le pas, de nouvelles offensives sont à craindre. Une version encore plus redoutable de **WannaCry** risque bien d'arriver. En espérant que les OIV ne soient pas cette fois touchés.

**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>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRETEP n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article