RÉGION

FRANCHE-COMTÉ > *Economie*

Des cyberattaques de plus

Si la dernière offensive massive de virus informatique, vendredi, ne semble pas avoir eu d'impact sur les entreprises de la grande région, les tentatives de piratages, parfois avec demande de rançon, se multiplient.

« Ouf ! Cette fois nous n'avons pas été visés », respirait ce lundi matin Dominique, commercial à l'entreprise R. Bourgeois de Besançon. Son soulagement est d'autant plus grand que l'entreprise a été victime voilà trois mois d'une cyberattaque similaire avec à la clé un blocage temporaire total de l'entreprise.

Un coup dur pour ce fleuron franc-comtois de l'usinage, du découpage et de l'emboutissage employant 1080 salariés, dont 450 à Besançon, qui a vu son activité bloquée deux jours durant. Les ordinateurs étant tous en rideau, il a été impossible de facturer, de livrer, etc. « C'est venu de notre service commercial », poursuit Dominique. « L'un de nous a ouvert un document piégé et patatras… »

« Deux jours pour identifier et éradiquer le problème. Sans payer la rançon. »

La réaction des salariés, très sensibilisés aux consignes de sécurité, a heureusement permis de limiter les dégâts. « Dès que l'écran a commencé à devenir noir, nous avons tout éteint et débranché pour éviter la propagation du virus. Mais pendant deux jours, nos informaticiens ont dû faire le tour des ordinateurs pour identifier la source du problème et l'éradiquer. » Le tout sans payer la rançon qui était demandée par les pirates auteurs de l'attaque.

Depuis ? « Cela n'a fait que renforcer notre vigilance. Et nous conforter dans la pertinence des différentes procédures de sécurité informatique. Sachant que nous avons régulièrement, quasiment chaque semaine, des piqûres de rappel pour respecter les protocoles de sécurité. Ce matin encore nous avons reçu une remise à jour des procédures. »

Cette cyberattaque était-elle la première au sein de l'entreprise Bourgeois ? « De cette ampleur oui. En revanche notre pare-feu recense très régulièrement des attaques qu'il parvient heureusement à bloquer. »

Renseignements pris, ni Alstom Belfort et Ornans, ni des entreprises comme Parkeon ou Breitling à Besançon n'ont été atteintes cette fois. Pas plus manifestement que PSA Peugeot-Citroën à Sochaux où, si la direction ne communique pas « sur ce type de sujets » – elle est coutumière du fait dès lors qu'il s'agit de problèmes de sécurité–, l'activité du site, était ce lundi qualifiée de « normale ».

Seulement quelques ricochets dans les concessions Renault

« Mieux », ajoutait Eric Peultier (FO), secrétaire du comité d'établissement, « cela fait douze jours qu'il n'y a pas de modification des programmes de fabrication ». Le syndicaliste précisant simplement que des « consignes de prudence » ont été passées à l'ensemble des usagers de l'informatique au sein du groupe afin d'éviter les gros soucis rencontrés par le concurrent Renault Nissan.

En effet, hormis quelques ricochets de l'attaque nationale sur certaines concessions Renault, comme à Vesoul, les effets de cette cyberattaque sur l'économie de la grande région s'avèrent donc, sinon inexistants, du moins très limités. Un constat que confirmait hier après-midi le Medef de Franche-Comté : « Sur l'ensemble des entreprises contactées et qui nous ont répondu sur le sujet, aucune n'a rencontré de souci. Il semble que l'on ait été épargné cette fois. Du moins pour l'instant… »

Pierre LAURENT et Jacques BALTHAZARD

L'antivirus « le plus puissant du monde » développé par une start-up de Nancy

Là où il passe, les fichiers trépassent. WannaCrypt est un logiciel malveillant aussi redouté qu'Attila. Ce virus a infecté les systèmes informatiques de milliers d'entreprises à travers le monde, dont Renault en France, contraintes de payer une rançon en bitcoin pour récupérer leurs « fichiers ». Et une nouvelle vague d'attaques n'est pas exclue cette semaine quand les employés auront rallumé les ordinateurs…

« Si WannaCrypt passe aussi facilement entre les mailles des antivirus, c'est parce qu'il exploite une faille du système d'exploitation de Microsoft », explique Laurent Werner, le président de Cyber Detect, une start-up hébergée dans les murs du Loria (Laboratoire lorrain de recherche en informatique et ses applications), spécialisée dans la sécurité informatique. La nouvelle génération d'antivirus qu'elle a mise au point ne se serait pas laissé leurrer par WannaCrypt. Leur approche est si innovante que l'entreprise nancéienne, créée au début du mois, est déjà sollicitée par de nombreux grands comptes, tant publics que privés, à travers le monde.

« Les antivirus traditionnels fonctionnent comme des douaniers », explique Jean-Yves Marion, directeur du Loria et conseiller scientifique de la start-up, qui travaille sur cette solution avec Guillaume Bonfante, maître de conférences à l'École des Mines. « Ils doivent disposer du signalement d'une personne recherchée pour la repérer. Le problème, c'est qu'il lui suffit de se déguiser un peu pour passer inaperçue. Avec notre solution, elle aura beau enfiler une armure, on la reconnaîtra. Il nous suffit de repérer une petite partie de son corps pour l'identifier. Car nous analysons les fonctionnalités qui sont toujours similaires d'un virus à l'autre. »

Le vrai danger, les attaques ciblées

« Tous les fichiers qui entrent dans un système protégé par Cyber Detect passent par une machine virtuelle qui leur fait croire qu'ils sont arrivés au cœur du système », précise Laurent Werner. « Cyber Detect fait alors une analyse morphologique », explique Stéphane Gégout, président du conseil de surveillance, « ce qui permet une représentation du code informatique en 3D, afin de mettre en évidence certaines fonctionnalités ».

Cyber Detect est ainsi en mesure de dresser le « portrait » de n'importe quel virus. Et celui de WannaCrypt n'est pas si redoutable que ça. « Il y a des malwares beaucoup plus complexes », selon Jean-Yves Marion. « Le véritable enjeu de sécurité porte sur les attaques ciblées menées par des hackers travaillant pour le compte d'États », à l'instar des Russes d'APT28 accusés d'avoir piraté la messagerie du Parti démocrate en pleine campagne présidentielle américaine, selon le rapport du département à la Sécurité intérieure et le FBI. « Nous avons décortiqué et analysé une partie de cette attaque », précise Jean-Yves Marion qui est attendu fin mai à San Jose, en Californie, à la conférence internationale Security and Privacy, pour un « débriefing » avec les plus grands spécialistes mondiaux de la question.

Saïd LABIDI

1 575 €

c'était le cours hier, à 18 h, du bitcoin, monnaie virtuelle mais bien réelle dans laquelle les pirates exigent une rançon, en apparence modeste, en échange de leur clef de cryptage.

Fabrice Sabatier, Laurent Werner, Guillaume Bonfante, Jean-Yves-Marion et Stéphane Gégout, devant le portrait en 3D du virus WannaCry. Photo DR

L'antivirus le plus puissant du monde !

Là où il passe, les fichiers trépassent. WannaCry est un logiciel malveillant aussi redouté qu'Attila. Ce virus a infecté les systèmes informatiques de milliers d'entreprises à travers le monde qui sont contraintes de payer une rançon en bitcoins pour récupérer leurs « fichiers ». En France, c'est Renault qui a été particulièrement touchée. On craint une nouvelle vague d'attaques quand les employés auront rallumé les ordinateurs…

« Si WannaCry passe aussi facilement entre les mailles des antivirus, c'est parce qu'il exploite une faille du système d'exploitation de Microsoft », explique Laurent Werner, le président de Cyber Detect, une start-up hébergée dans les murs du Loria (Laboratoire lorrain de recherche en informatique et ses applications, CNRS, Inria et Université de Lorraine), spécialisée dans la sécurité informatique. La nouvelle génération d'antivirus qu'elle a mise au point ne se serait pas laissé leurrer par WannaCry. Leur approche est si innovante que l'entreprise nancéienne, créée au début du mois, est déjà sollicitée par de nombreux grands comptes, tant publics que privés, à travers le monde.

« Les antivirus traditionnels fonctionnent comme des douaniers », explique Jean-Yves Marion, directeur du Loria et conseiller scientifique de la start-up. « Ils doivent disposer du signalement d'une personne recherchée pour la repérer. Le problème, c'est qu'il lui suffit de se déguiser un peu pour passer inaperçue. Avec notre solution, elle aura beau enfiler une armure, nous, on la reconnaîtra. Il nous suffit de repérer une petite partie de son corps pour l'identifier. Car nous analysons les fonctionnalités qui sont toujours similaires d'un virus à l'autre. » L'homme travaille sur cette solution avec Guillaume Bonfante, maître de conférences à l'École des Mines (Université de Lorraine).

Le vrai danger, les attaques ciblées

« Tous les fichiers qui entrent dans un système protégé par Cyber Detect passent par une machine virtuelle qui leur fait croire qu'ils sont arrivés au cœur du système », précise Laurent Werner. « Cyber Detect fait alors une analyse morphologique », explique Stéphane Gégout, président du conseil de surveillance, « ce qui permet une représentation du code informatique en 3D, afin de mettre en évidence certaines fonctionnalités ».

Cyber Detect est ainsi en mesure de dresser le « portrait » de n'importe quel virus. Et celui de WannaCry n'est pas si redoutable que ça. « Il y a des malwares beaucoup plus complexes », selon Jean-Yves Marion. « Le véritable enjeu de sécurité porte sur les attaques ciblées menées par des hackers travaillant pour le compte d'États », à l'instar des Russes d'APT28 accusés d'avoir piraté la messagerie du Parti démocrate en pleine campagne présidentielle américaine, selon le rapport du département à la Sécurité intérieure et le FBI. « Nous avons décortiqué et analysé une partie de cette attaque », précise Jean-Yves Marion qui est attendu fin mai à San Jose, en Californie, à la conférence internationale Security and Privacy, pour un « débriefing » avec les plus grands spécialistes mondiaux de la question.

Saïd LABIDI

Questions à ?

Photo RL/G. WIRTZ

Christophe Bianco
PDG Excellium services, Luxembourg

« La prise de conscience est récente mais réelle »

Avec l'attaque par déni de service en septembre dernier – 147 000 caméras piratées pour empêcher des majors de l'économie de fonctionner – et le ransomware (rançongiciel) de ce week-end, les entreprises ont-elles pris la mesure du problème ?

Oui, dans la plupart des entreprises, la cybersécurité commence à être intégrée dans la gestion des risques. La prise de conscience est récente mais maintenant, les patrons savent clairement que ça peut leur arriver. Même si tout le monde n'a pas la même acceptation et sensibilisation au risque.

Clairement, en plein cœur de l'attaque, qu'avez-vous pu conseiller à vos clients ?

J'ai diffusé à mes 180 clients – aucun n'a été affecté – un premier bulletin samedi vers 16h, puis un autre le lendemain car on avait une meilleure visibilité sur la nature de ce malware. Dimanche, 50 % d'entre eux, dans les sept pays où je travaille, étaient au boulot pour se prémunir de tout risque de contamination.

Que devaient-ils faire ?

D'abord, nettoyer les boîtes aux lettres. Ensuite, je leur rappelais la liste de patchs Microsoft à déployer. Le patch, c'est un bout de code qui vient corriger les vulnérabilités du logiciel. Microsoft en sort régulièrement, mais les entreprises disent n'avoir jamais le temps de faire ces opérations. Là, elles l'ont trouvé ! Ensuite, c'est la mise à jour du système et le blocage des noms de domaine connus en lien avec le malware.

Et lorsqu'on est infecté ?

Il ne faut pas tout éteindre, car on perd alors toutes les informations sur le virus. Il faut couper sa connexion internet et son wifi. En fait, s'isoler des réseaux pour empêcher sa propagation. Les fichiers du poste concerné seront néanmoins vérolés.

Comment une entreprise comme Renault, des hôpitaux et tant d'autres géants de l'économie ont-ils pu être piégés ?

Ce type de virus peut plus facilement infecter la vieille économie. Dans l'industrie, le parc informatique est vieillissant, les logiciels peu actualisés. Microsoft ne fournit plus de patch pour les logiciels antérieurs à ses deux versions les plus récentes. Dans les hôpitaux, c'est compliqué de faire constamment des mises à jour et ça devient des établissements vulnérables.

Renault a communiqué sur le piratage, vous appréciez ?

À ce niveau, c'est une première et une très bonne chose. Ça doit être la posture d'un client mature. Le problème avec les cyberattaques, c'est qu'il n'y a pas de retour d'expérience. Chacun garde l'info, trouve sa parade et la garde pour lui. Alors qu'au contraire, il faut faire tourner l'info, échanger, informer, former de jeunes ingénieurs et éduquer la population à ces risques.

En cas de rançon demandée, que peut-on faire à part payer ?

Prier ! Tout dépend de la valeur de l'attaque. Mais généralement, vous n'avez pas d'autre choix que payer. C'est d'ailleurs pour cela que ça marche. Ce type d'attaque est extrêmement lucratif. Mais derrière, vous devez corriger rapidement. Plutôt que payer, je préconise d'investir en amont. Je sais que cette semaine, il va y avoir une vague de comité de direction pour lancer des plans de continuité. Car la cybersécurité ne doit jamais être une opération d'un jour. Elle doit être constante et réactualisée.

Propos recueillis par Laurence SCHMITT

Le match Microsoft vs NSA

La faille chez Microsoft avait été mise en évidence par la NSA, lors de l'affaire Snowden. Mais l'agence de sécurité américaine ne lui en a jamais fait part. Pourquoi ? « Pour s'en servir et pouvoir rentrer dans les systèmes. On n'est pas dans un monde de Bisounours », n'hésite pas à commenter Christophe Bianco, PDG d'une société de cybersécurité au Luxembourg, Excellium services. Entre-temps, les données tenues secrètes auraient été volées ! Étonnant. Inquiétant, surtout. Hier, Microsoft demandait des comptes à la NSA et parlait d'une « convention de Genève numérique ». « Renault pourrait demander des dédommagements à Microsoft. L'entreprise a subi de grosses pertes. » Europole exige plus de collaborations entre États. « Il faut absolument établir un protocole de retour d'expérience après ce type de pandémie », insiste le spécialiste. Comme le font les compagnies aériennes après un crash ou l'industrie nucléaire au moindre incident.

L. S.