FAITS DIVERS

« La prise de conscience est récente mais réelle »

Christophe Bianco, PDG d'Excellium services, une société de cybersécurité installée au Luxembourg : « Un parc informatique vieillissant est plus vulnérable. » Photo Gilles WIRTZ

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 ?

Christophe BIANCO, PDG d'Excellium services : 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 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

Cybercriminalité : deux fois rançonné

En 2014, un virus a infecté le système informatique de l'entreprise Insmatel à Maxéville. Son patron a payé deux fois une rançon en bitcoins pour récupérer une clé de décryptage. Il raconte.

La cyberattaque qui a touché le monde entier ce week-end a réveillé chez Christian Bestron un très mauvais souvenir. Quand il revient sur l'épisode « douloureux » qu'il a vécu en 2014, le PDG de l'entreprise d'électricité Insmatel, implantée à Maxéville (54), en a encore froid dans le dos.

Tout commence un samedi matin d'avril : « J'étais passé au bureau pour finaliser quelques devis », raconte-t-il. « En ouvrant certains fichiers, ils étaient totalement cryptés. J'essaie une fois, deux fois, trois fois... Je pense à un problème sur mon ordinateur et ne vais pas plus loin. »

Le PDG décide d'attendre le lundi matin. Et là, c'est « alerte rouge » : tous les salariés de la PME se trouvent confrontés à la même situation, victimes d'un virus. À l'origine : l'ouverture d'une pièce jointe dans un mail frauduleux.

Christian Bestron va alors avoir le sentiment de vivre un mauvais film : il reçoit un message de demande « de rançon, 500 dollars US, à payer en temps voulu si je veux recevoir une clé de décryptage ». Et en bitcoins, monnaie virtuelle particulièrement difficile à tracer, dont le PDG ignore alors tout. Tout comme ses banquiers. « C'est Google qui me le dira. Je vais passer des jours à chercher comment en acheter. »

Quand il réussit enfin à ouvrir un compte auprès d'un organisme parisien et fait le virement des 1.16 bitcoin demandés (au cours de l'époque), le délai imparti est largement dépassé. Il ne recevra pas de clé mais un second message lui intimant de verser cette fois-ci la somme de 1 000 dollars US, soit 2.17 bitcoins.

Une clé de décryptage

Son entourage estime qu'il s'agit d'une « folie ». Lui se sent « prisonnier », ne voit pas d'autre solution que « payer ». Il a fait appel à la cybercriminalité à Paris : « On m'a répondu : si cela avait été le cryptage d'il y a un an, on aurait l'antivirus. Il n'y a plus qu'une chose à faire, c'est payer la rançon. »

Le 24 avril, soit 16 jours après l'attaque, 16 jours d'angoisse, de « nuits agitées », de mails à n'en plus finir auprès de contacts souvent tout aussi désemparés, Christian Bestron reçoit la fameuse clé de décryptage. Les soucis n'en sont pas pour autant terminés. Si tous les fichiers ont été cryptés en 5 minutes, il aura fallu trois machines et au moins trois semaines pour rendre lisibles l'essentiel des dossiers.

Aujourd'hui encore, « quand l'entreprise a besoin d'une recherche historique, on décrypte au cas par cas ». Sur une machine « totalement isolée du réseau », précise le patron. Pour l'installateur électricien qui effectue de très gros chantiers, ce virus n'a pas eu d'impact sur la production proprement dite. En revanche, il aurait pu anéantir toutes les études lancées, qui se traduisent souvent en mois voire en année de travail.

Depuis 2014, l'entreprise a instauré des procédures de sauvegarde rigoureuses. « Un mal pour un bien », se console Christian Bestron, qui confie : « Cela m'affole de voir que même des géants » puissent se faire attaquer.

Marie-Hélène VERNIER

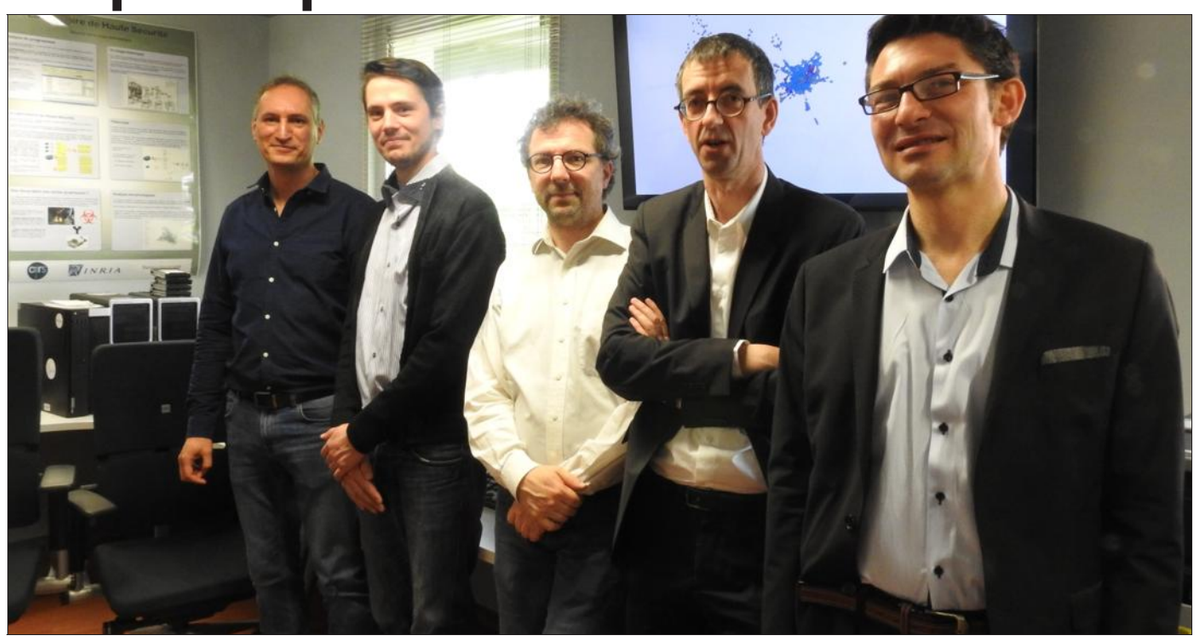
La cyberattaque dont Christian Bestron, PDG de l'entreprise Insmatel, a été victime en 2014 demeure un souvenir « douloureux ». Photo ER/Alexandre MARCHI

Match Microsoft contre 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 », commente Christophe Bianco, PDG d'Excellium services, société de cybersécurité au Luxembourg. Entre-temps, les données tenues secrètes auraient été volées ! 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.

L. S.

A Nancy, l'antivirus le plus puissant du monde !



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

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 touché. On craint cette semaine 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

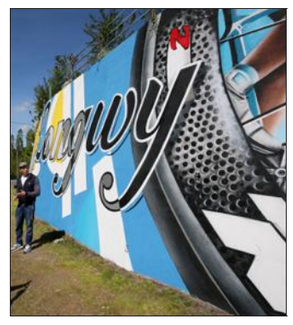
« Tous les fichiers qui entrent dans un système protégé par Cyber Detect passent par une machine virtuelle qui leur fait croire qu'ils sont arrivés au cœur du système », précise Laurent Werner. « Cyber Detect fait alors une analyse morphologique », explique Stéphane Gégout, président du conseil de surveillance, « 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

lorraine

Longwy : le Tour fait le mur



Pierre Bertolotti devant sa fresque. Photo René BYCH

Le 3 juillet, Longwy accueillera l'arrivée de la troisième étape du Tour de France. Pour marquer cette date attendue, la municipalité a décidé de mettre en place une série de rendez-vous. Ainsi, après le traçage symbolique de la ligne d'arrivée le 3 janvier, les visites de Bernard Hinault et Jean-Paul Ollivier, une fresque en l'honneur du passage du Tour a été réalisée au niveau du belvédère, entre les cités basse et haute.

L'œuvre picturale a été inaugurée hier, en présence de l'artiste, le local Pierre Bertolotti, et d'un aréopage d'élus. « Je me suis attaché à dessiner les symboles du patrimoine de Longwy : un sabot lorrain en émaux, les remparts et la porte de France. J'ai évidemment dessiné des vélos, la foule et des visages heureux, des ballons... Le tout avec des couleurs, de la gaîté », détaille le graffeur. Et ce sur une surface de 50 m de long et 4 m de haut en dégressif.

Metz : les 150 ans du Botanique

Les serres du Botanique vont être réhabilitées à partir de cet été. Photo Karim SIARI

Le jardin botanique de Metz fête cette année ses 150 ans et l'événement sera décliné en trois temps sur une année glissante : le week-end de la Pentecôte, en octobre puis en juin 2018 avec l'inauguration des serres du Botanique qui d'ici là seront réhabilitées.

Pour célébrer l'anniversaire, la Ville de Metz a mis en place un programme étoffé d'expositions, d'animations, de spectacles, de collections temporaires de plantes, etc. pour fêter le renouveau du site.

Ainsi, dès le week-end inaugural, le samedi 3 juin, la Ville annoncera la labellisation du Botanique de Metz en "Jardin botanique de France et des pays francophones".

Ce qui signifie que le jardin au parfum Belle époque va retrouver sa vocation première. C'est-à-dire scientifique et de préservation des espèces.