HIGH-TECH &MEDIAS

pixels

Olivier Gerolami prend la tête de « Midi Libre »

Olivier Gérolami a été nommé président-directeur général de la société du quotidien « Midi Libre », en remplacement d'Alain Plombat. Olivier Gérolami est, depuis 2012, à la tête du groupe Sud-Ouest, qui détient les Journaux du Midi (« Midi Libre », « L'indépendant », « Centre Presse »).

AFP

Fin 2015, date butoir pour Maurice Lévy

Le président du directoire de Publicis Groupe, Maurice Lévy, a indiqué au « Wall Street Journal », en marge du Festival de la publicité, qu'il ne chercherait pas à prolonger son mandat à la tête de l'entreprise au-delà de la fin 2015. Il pourrait néanmoins continuer de jouer un rôle au sein du groupe. Le chantier de sa succession démarrera fin 2014.

AFP

555

MILLIONS DE DOLLARS

Nest, le fabricant de thermostats et de détecteurs de fumée intelligents, va débourser 555 millions de dollars pour acquérir Dropcam, une start-up spécialisée dans la télésurveillance pour la maison, a indiqué vendredi le site Re/code.

Les demandes de rançon, une mode très prisée des cyberpirates

● Les cyberpirates pratiquent l'extorsion sur les particuliers et entreprises.
● Au menu : kidnapping de données et menaces sur des infos sensibles.

CYBERSÉCURITÉ

Sandrine Cassini
scassini@lesechos.fr

« Si vous êtes un client de Domino's Pizza, sachez que nous leur avons proposé de ne pas publier vos données en échange de 30.000 euros. » Tel est le message publié sur Twitter la semaine dernière par le « collectif » pirate Rex Mundi. La firme de restauration rapide a refusé de se plier au chantage des cyberpirates, qui se vantaient d'avoir dérobé les données de 600.000 clients.

Cet épisode illustre l'une des tendances actuellement en vogue chez les cybercriminels : l'extorsion de fonds. *« D'habitude, les demandes ne sont pas publiques. Là, les pirates grillent leurs dernières cartouches »*, explique Gérôme Billois, consultant en sécurité chez Solucom, qui estime que Rex Mundi aurait gagné plus d'argent en revendant les données au marché noir. Une ligne client vaut entre 50 centimes et 2 euros la ligne, soit entre 300.000 euros et 1,2 million d'euros pour un cas comme Domino's Pizza. *« Mais les données perdent très vite de leur valeur »*, modère-t-il.

En vogue, surtout, les « rançongiciels », qui consistent à bloquer le fonctionnement d'un ordinateur et à réclamer à son propriétaire entre 300 et 1.000 euros pour lui donner les clefs de cryptage. *« Parfois, le pirate fait passer la rançon pour une amende, en envoyant un message officiel qui semble provenir d'une autorité infligeant une amende »*, précise Loïc Guézo, de Trend Micro. Selon Europol, des millions d'ordinateurs ont été infectés ces deux dernières années, générant un business de plusieurs millions d'euros.

Le même phénomène touche les entreprises. Discrétion oblige, les demandes de rançon se font en bitcoin, cette monnaie virtuelle intraçable. Premier mode opératoire : le kidnapping de données. *« Nous avons eu chez un client le cas de pirates ayant mis la main sur une base de données ressources humaines et qui menaçaient de révéler les salaires des grands dirigeants en interne et sur la place publique »*, raconte Michel Van Den Bergue, directeur général d'Orange Cyberdéfense. La menace a produit son effet : l'entreprise a payé.

Imagination sans limites

Deuxième option : les cyberpirates paralysent un système d'information ou mettent sous séquestre une base de données sensibles (fichier clients, e-mails de dirigeants…) qu'ils peuvent menacer de détruire. Ils peuvent aussi menacer l'entreprise de saturer son réseau ou son système. *« Des cyberpirates ont paralysé la salle de marché d'une banque pendant quarante-cinq minutes, engendrant des pertes colossales. La banque a accepté de payer plusieurs centaines de milliers d'euros aux demandeurs de rançon »*, raconte Laurent Combalbert, un ancien officier du Raid reconverti dans la gestion de crise et la négociation de rançon. Si les montants ne paraissent pas élevés au regard des préjudices subis, c'est pour encourager les victimes à payer.

Comment les entreprises doivent-elles réagir ? *« On leur suggère de révéler l'affaire et, surtout, de ne pas payer, sinon c'est l'engrenage »*, souligne Laurent Combalbert. Dans les cas extrêmes, les négociations ont lieu – uniquement par e-mails, les pirates ayant dématérialisé la négociation –, l'objectif ultime étant quand même de persuader l'escroc de renoncer au butin.

Dernier phénomène : les faux ordres de virement. En se renseignant sur les réseaux sociaux, les pirates se font passer pour des dirigeants, mettant la pression sur un comptable ou une assistante. *« Sur LinkedIn, vous pouvez facilement accéder à tout l'organigramme d'une entreprise et à ses projets stratégiques. On a vu certains de nos clients accepter de faire des virements de 100.000 ou 200.000 euros »*, indique Jean-Michel Orozco, directeur général cybersécurité chez Airbus Defence and Space, qui conseille les entreprises. Les banques – en particulier la Société Générale, BNP Paribas, et la CDC – prendraient le phénomène très au sérieux. La Banque de France aurait également inscrit le problème à son agenda.

Encore plus malin, le virement par intrusion. *« J'ai eu le cas d'un client qui s'est fait dérober 1,5 million d'euros »*, explique Gérôme Billois. Le pirate s'est introduit dans le système d'information de l'entreprise, et a fait effectuer plusieurs virements à la place du service comptable. ■

La firme Domino's Pizza, victime d'un chantage utilisant Twitter, a refusé de se plier aux volontés des cyberpirates. *Photo Michel Gaillard/Réa*

Dans le maquis judiciaire de la cybercriminalité

Malgré la pléthore de services dédiés au cybercrime, le taux d'élucidation des affaires reste faible.

Que fait la police ? Les affaires en matière de cybercriminalité se multiplient, mais *« les taux d'élucidation ne sont pas très importants »*, admet l'avocat Olivier Itenau. Une situation paradoxale dans la mesure où la France dispose d'une panoplie de services spécialisés. La Brigade d'enquête sur les fraudes aux technologies de l'information (Befti) – 25 enquêteurs –, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) – 60 policiers – et un service de cybergendarmes enquêtent sur le cybercrime. En parallèle, l'Agence nationale de sécurité des systèmes d'information (ANSSI) qui porte assistance aux entreprises sensibles (opérateurs télécoms, banques…), transfère les dossiers à la DCRI.

Une pléthore d'alternatives qui n'est pas synonyme d'efficacité. *« Il y a un grand flou dans le rôle de chacun. Des entreprises se retrouvent à ne pas savoir où aller »*, indique l'avocate Isabelle Renard. Les victimes ont recours au système D : on appelle de manière informelle le policier que l'on connaît pour savoir si l'affaire en question les intéresse. Tout dépend de l'engorgement des services. La situation est pire pour le particulier et pour les petits préjudices portant sur quelques milliers d'euros.

> « Ce qui manque, c'est un office qui centralise les plaintes. »
> **ISABELLE RENARD**
> Avocate

Classement vertical

« La victime va au commissariat du coin, et là, c'est directement le classement vertical », indique un juriste. Face à cette situation, la police judiciaire vient de créer une sous-direction dédiée à la cybercriminalité, dont le patron – le nom de la commissaire Catherine Chambon circule – devrait être nommé le 1er juillet. En parallèle, le ministre de l'Intérieur, Bernard Cazeneuve, a annoncé la nomination d'un cyberpréfet. *« Ce qui manque, c'est un office qui centralise les plaintes »*, tranche Isabelle Renard. La faute n'est pas uniquement à chercher du côté des autorités juridiciaires. Les entreprises rechignent à porter plainte, craignant la mauvaise publicité.

Les victimes se heurtent aussi au manque d'efficacité de la justice. *« L'arsenal judiciaire existant, qui comprend l'usurpation d'identité numérique, la collecte déloyale de données ou les tentatives d'accès à un système d'information, est encore très peu utilisé »*, explique Bénédicte Graulle, avocate chez Jones Day. *« Ni les magistrats ni les juges ne le connaissent. Il y a donc très peu de jurisprudence. »* Plus grave, les auteurs des méfaits sont souvent basés hors d'Europe. L'entraide judiciaire internationale est donc un maillon essentiel. Or, le ministère de la Justice, qui ne s'est jamais doté d'un responsable en matière de cybercriminalité, ne pousse pas vraiment dans ce sens. — ***S. C.***

Plongée au cœur du nouveau laboratoire de tests de SFR

TÉLÉCOMS

L'opérateur teste la voix sur la 4G, qui sera disponible sur son réseau début 2015.

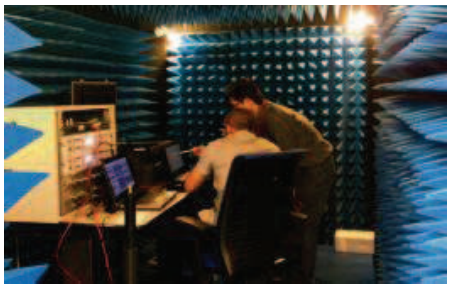
Romain Gueugneau
rgueugneau@lesechos.fr

C'est un bâtiment assez quelconque, à la façade claire, situé dans le quartier de bureaux de Vélizy, en banlieue parisienne. Pas d'imposant dispositif de sécurité à l'entrée. Pas de logo apparent ou d'affichage spécifique. La discrétion est de mise. Et pour cause. C'est ici que SFR a installé son nouveau laboratoire de tests. L'endroit est stratégique : l'opérateur télécoms a reconstitué sur cet espace de 7.800 m², dont 2.000 m² de « data centers », une réplique miniature de ses réseaux fixe et mobile, qui renferme 5.000 machines et permet de réaliser des tests de compatibilité et de performance dans des conditions semblables à la réalité du terrain. Une centaine d'employés de SFR, auparavant disséminés sur divers sites, travaillent dans ce laboratoire, opérationnel depuis le mois d'avril, et traitent environ 4.000 anomalies par an.

C'est ici que sont testés tous les smartphones commercialisés par SFR (100 terminaux par an). Quelques mois avant leur introduction sur le marché, les téléphones – ou du moins ce que les fabricants veulent bien en dévoiler – sont passés au crible par les ingénieurs. Voix, data, connexion, performance… ils subissent toute une batterie de tests dans le laboratoire. Pour effectuer ces tests dans les meilleures conditions, les ingénieurs s'enferment dans des cages de Faraday, des pièces totalement hermétiques, afin de ne pas être pollués par les ondes extérieures.

Ultrasécurisé

Pour éviter toute fuite, les fabricants veillent au grain et imposent leurs conditions. *« Seule une poignée de collaborateurs sont au courant des smartphones en test. Et ils n'ont en aucun cas le droit d'en parler »*, explique Pierre-Alain Allemand, le patron des réseaux et du système d'information chez SFR. A l'intérieur du laboratoire, certaines salles sont dotées d'un dispositif de sécurité particulier, avec code d'accès et caméra à l'entrée. Les constructeurs eux-mêmes viennent s'assurer sur place une à deux fois par an que les règles de confidentialité et de sécurité sont respectées. A Vélizy, les ingénieurs de SFR travaillent sur les dernières technologies mobiles. C'est dans le laboratoire que sont actuellement testés les appels voix sur la 4G (VoLTE), qui permettront d'améliorer la qualité audio (haute définition) et de réduire considérablement le temps d'établissement de la connexion (1 à 2 secondes). Actuellement, en France, lorsque l'on passe un appel sur un réseau 4G, on bascule automatiquement sur de la 3G, car les équipements en place ont été conçus en priorité pour faire passer de la data. Après des tests concluants, SFR va progressivement équiper son réseau très haut débit pour pouvoir offrir la voix sur LTE « *sans surcoût, dès le début 2015* ». Bouygues Telecom s'est aussi engagé à fournir cette technologie à partir de l'an prochain.



Pour pratiquer les tests, les ingénieurs du labo s'enferment dans des cages de Faraday. *Photo Romain Gueugneau/Les Echos*

C'est aussi dans ce laboratoire que sont conduits les travaux sur la mutualisation des réseaux mobiles des deux opérateurs, signée début février – et que le rachat de Numericable n'a pour l'instant pas remise en cause.

Accueillant mais pas trop

Dans une même salle cohabitent ainsi des antennes de SFR (Nokia et Huawei) et de Bouygues (Ericsson). *« Chacun teste ses équipements sur les fréquences de l'autre,* commente Jean-Michel Bradfer, patron du laboratoire. *Les ingénieurs de Bouygues Telecom viennent également ici pour travailler. Mais ils ont un accès très restreint au bâtiment. On fait très attention. »* Alors que la concurrence fait rage entre opérateurs, il serait regrettable de laisser un rival filer avec les plans des futures innovations…

À NOTER

L'accord définitif scellant le rapprochement entre SFR et le câblo-opérateur Numericable a été signé vendredi.