

Des sites internet d'entreprises et de médias français perturbés par des attaques

Plusieurs sites web d'entreprises et de médias français ont été la cible d'attaques informatiques la semaine dernière. Selon Reuters, une «perturbation» a touché les sites de médias comme *Le Figaro*, *Le Monde*, *20 Minutes*, *L'Obs* ou France Télévisions, le mercredi 10 mai. Cette perturbation a pour origine une attaque par dénis de service (DDos) qui a ciblé l'entreprise Cedexis, spécialisée dans la distribution de contenu, «qui a perturbé nombre de sites français clients, dont ceux d'une partie de la presse». Cedexis a qualifié l'attaque DDos de «puissante». «Vers environ 14h GMT, l'infrastructure de Cedexis a été la cible d'une attaque par déni de service sophistiquée», selon un mail adressé par le P-dg de la société à Reuters. Selon *L'Obs*, les sites de grandes entreprises comme Airbus, Hermès, Longchamp, Pinterest ou Slack, ont également été rendus inaccessibles. Le ministère de l'Intérieur a également mentionné cette attaque dans la soirée mais pour indiquer que son «Système d'alerte et d'information des populations» (Saif) n'avait pas été affecté et fonctionnait normalement, affirme encore l'Agence. Le service était redevenu normal dans la soirée même. Aucune indication n'a été donnée sur la source de cette attaque informatique.

A l'approche des législatives, Facebook conseille les Britanniques contre les «fake news»

A l'approche des élections législatives du 8 juin au Royaume-Uni, Facebook a lancé une campagne publicitaire dans la presse britannique pour mettre en garde contre les «fake news». Le réseau social exhorte ses utilisateurs britanniques à mettre en doute les informations peu crédibles et à les vérifier avant de les partager, tout en promettant de supprimer les faux profils et de cesser de promouvoir les messages qui semblent peu plausibles, indique Reuters. «Nous avons développé de nouveaux moyens d'identifier et retirer les comptes factices qui pourraient propager des fausses nouvelles, de manière à nous attaquer à la racine du problème», explique Simon Milner, responsable du code de conduite de Facebook au Royaume-Uni. Le réseau social n°1 dans le monde a récemment supprimé des profils automatiques qui postent des messages à caractère commercial ou politique. Quelque 30 000 comptes ont été suspendus en France avant le premier tour de la présidentielle. Aussi, des mesures ont été prises contre des dizaines de milliers de faux comptes en Grande-Bretagne à l'activité inhabituelle, comme la répétition du même contenu. Facebook a annoncé son intention de recruter 3 000 personnes supplémentaires au cours de l'année pour faire la chasse aux fausses informations et pour supprimer des vidéos montrant des actes de violence.

Samsung Electronics va créer une division de fabrication de puces pour ses clients

Le géant sud-coréen Samsung Electronics a déclaré, vendredi dernier, qu'il a formé une nouvelle division dans son secteur des semi-conducteurs pour la fabrication de puces destinées à ses clients. La nouvelle division sera responsable de la fabrication de processeurs mobiles et d'autres puces non-mémoire pour des clients tels que Qualcomm Inc et Nvidia Corp, en concurrence avec des entreprises telles que Taiwan Semiconductor Manufacturing Co. Cette décision n'a pas surpris les analystes qui avaient prévu depuis quelque temps que l'entreprise finirait par diviser ses opérations de fabrication de puces pour les rendre plus efficaces et atténuer les inquiétudes des clients au sujet de fuites éventuelles. Bien que l'activité de fabrication de puces représente une petite partie des ventes globales de Samsung, ses revenus ont connu une forte croissance. La firme de recherche IHS estime que ces revenus ont augmenté de 86% pour s'établir à 4,7 milliards de dollars en 2016.

EUROPOL DÉNOMBRE PLUS DE 200 000 VICTIMES

Une cyberattaque touche plus de 150 pays, crainte d'un «cyberchaos»

● Une cyberattaque de portée mondiale «sans précédent» frappe plus de 200 000 victimes dans au moins 150 pays depuis vendredi 12 mai 2017. De la Russie au Mexique, en passant par l'Espagne, la France, l'Italie, la Grande-Bretagne, et l'Algérie, des centaines de milliers d'ordinateurs ont été infectés par un logiciel de rançon. Des pirates ont exploité une faille dans les systèmes Windows, divulguée dans des documents piratés de l'agence de sécurité américaine NSA, expliquent les autorités américaines et britanniques.

Par Rabah Rahmani

Celles-ci appellent depuis vendredi à ne pas payer ces pirates. «Payer la rançon ne garantit pas la restitution des fichiers», affirme le département américain de la Sécurité intérieure. Les deux autorités disent redouter un «cyberchaos» que devrait générer une recrudescence du virus lorsque des millions d'autres ordinateurs auraient été allumés au début de la semaine.

Ce logiciel malveillant, un rançongiciel nommé WannaCry (Littéralement, «vouloir pleurer») verrouille les fichiers des utilisateurs, sous Windows XP principalement et les oblige à payer 300 dollars pour en recouvrer l'accès à leurs données. La rançon est demandée en monnaie virtuelle bitcoin, difficile à tracer, explique l'Europol. Cette attaque a affecté plusieurs hôpitaux britanniques, le constructeur automobile français Renault, le système bancaire russe, le groupe américain de logistique FedEx, la compagnie de télécoms espagnole Telefonica ou encore des universités en Grèce et en Italie. Europol a

affirmé samedi que cette cyberattaque ne vise aucun pays en particulier. Cette institution a insisté sur la rapidité inédite de la propagation de ce virus, appelé «WannaCry», qui combine pour la première fois les fonctions de logiciel malveillant et de ver informatique. «Il a commencé par attaquer les hôpitaux britanniques avant de se propager rapidement à travers la planète. Une fois qu'une machine est contaminée, le virus va scanner le réseau local et contaminer tous les ordinateurs vulnérables», a expliqué le porte-parole d'Europol, Jan Op Gen Oorth, relayé par plusieurs agences de presse. Selon une carte réalisée par des chercheurs de la société spécialisée dans la sécurité informatique, Avast, l'Algérie figure bel et bien parmi les pays touchés par WannaCry. Toutefois, aucune société, publique ou privée ni administration algérienne n'a indiqué avoir été touchée par cette attaque.

Crainte d'un «cyberchaos»

Rob Wainwright, directeur d'Europol, a révélé à la chaîne de télévision britannique qu'il n'avait encore jamais rien vu

de tel». «Le dernier décompte fait état de plus de 200 000 victimes, essentiellement des entreprises, dans au moins 150 pays. Nous menons des opérations contre environ 200 cyberattaques par an, mais nous n'avons encore jamais rien vu de tel», a-t-il renchéri. Le même responsable a expliqué que les autorités britanniques et américaines craignent une augmentation du nombre de victimes. «WannaCry», lancé vendredi soir, pouvait effectivement toucher de nouveaux appareils lundi matin, «lorsque les employés allumeront leurs ordinateurs». «A partir du moment où l'échelle est très grande, on peut se demander si le but recherché est le cyberchaos», s'interrogeait Laurent Heslault, directeur des stratégies de sécurité chez la société de sécurité informatique Symantec. Rob Wainwright affirme qu'il y a eu étonnamment peu de paiements jusqu'à présent. La société de sécurité informatique Digital Shadows a fait état dimanche d'un montant total de 32 000 dollars versés. Mais le département américain de la Sécurité intérieure insiste et signe : «Payer la rançon ne garantit pas la restitution des fichiers», appelant ainsi à ne pas céder au chantage.

Microsoft met en garde les gouvernements

La compagnie Microsoft, qui reconnaît sa responsabilité de prévenir contre de telles attaques, a surtout averti les gouvernements deux jours après le lancement de WannaCry contre la tentation de cacher des failles informatiques qu'ils auraient repérées. Son directeur juridique Brad Smith a cité cette attaque comme exemple, puisque la brèche dans le système Windows XP, utilisée par les pirates, avait été décelée depuis longtemps par la NSA avant de tomber dans le domaine public via des documents piratés au sein de la NSA elle-

même. «Un scénario équivalent avec des armes conventionnelles serait comme si l'armée américaine se faisait voler des missiles Tomahawks», affirme-t-il. Il a rajouté que «c'est une tendance émergente depuis 2014. Nous avons vu des failles gardées par la CIA apparaître sur WikiLeaks et maintenant, cette faille volée à la NSA a affecté des clients autour du monde». Microsoft a émis plusieurs «patch correctifs exceptionnels» puisque les versions du système d'exploitation touchées par WannaCry ne sont plus concernées par les mises à jour ni les correctifs. Brad Smith a ainsi invité les Etats à une «prise de conscience» vu «les dégâts infligés à des civils». Selon la ministre britannique de l'Intérieur, Amber Rudd, dans une tribune au *Sunday Telegraph*, il faut désormais s'attendre à d'autres attaques. Et on ne «connaîtra peut-être jamais la véritable identité des auteurs» de celle en cours, a-t-elle ajouté. Mais le porte-parole d'Europol se veut plus optimiste, affirmant que «le nombre de victimes semble ne pas avoir augmenté et la situation semble stable en Europe». Jan Op Gen Oorth a souligné que de nombreux systèmes informatiques avaient été mis à jour au cours du week-end. «Il est encore un peu tôt pour dire qui est derrière tout ça mais nous travaillons sur un outil de décryptage» des fichiers affectés par le virus, a-t-il ajouté, cité par l'AFP. Ces autorités devraient surtout remercier un jeune chercheur britannique de 22 ans, qui a permis de ralentir la propagation du virus. Il a également prévenu que les pirates risquaient de revenir à la charge en changeant le code, et qu'il serait alors impossible de les arrêter. «Vous ne serez en sécurité que lorsque vous installerez le correctif le plus rapidement possible», a-t-il tweeté sur son compte @MalwareTechBlog.

R. R.

La cyberattaque mondiale «WannaCry»

Ce logiciel malveillant qui réclame une rançon après le blocage de fichiers a fait plus de 200 000 victimes dans 150 pays

