VigiElabe
Vendredi 22 mai 2020

CYBER-CRIMINALITÉS : DES MENACES DÉCUPLÉES PAR LA CRISE

Plusieurs rapports publiés ces derniers jours font état d'une croissance sans précédent du nombre de cyber-attaques depuis le début de la pandémie. Une étude du spécialiste de la cyber-sécurité Kaspersky publiée le 23 avril affirme ainsi que les attaques informatiques cherchant « *à inciter les gens à ouvrir des liens ou des pièces jointes infectés ont progressé de 43% entre janvier et mars* », souvent « *sous couvert d'aides ou de conseils relatifs à la pandémie* ». Une autre étude du cabinet de cyber-sécurité Check Point publiée le 12 mai affirme pour sa part que « *plus de 192.000 cyber-attaques liées au coronavirus ont été découvertes par semaine en mai, soit une augmentation de 30% par rapport au mois précédent* ». Enfin, dans une étude publiée le 13 mai, la société informatique VmWare rapporte « *qu'entre le début février et la fin avril, les attaques informatiques visant le secteur financier ont augmenté de 238%* ». De fait, comme l'explique l'expert en sécurité informatique Stephen Burke, « *la crise actuelle crée une cyber-tempête parfaite nous rendant plus vulnérables que jamais* ». La mise en tension des entreprises et institutions ainsi que le bouleversement des modes de communication privés et professionnels créent en effet de nouvelles failles de sécurité aiguisant l'appétit des cybercriminels – tout comme celui des agences de renseignement étatiques.

Une crise marquée par trois « cyber-risques » spécifiques

« *Les crises ont toujours constitué des périodes propices à la cybercriminalité, et le Covid-19 ne fait pas exception* », affirme Shane Huntley, directeur du Threat Analysis Group de Google, qui détaille les stratagèmes cherchant à tirer parti de la situation : « *appels aux dons émanant d'organismes de bienfaisance, sites se faisant passer pour des pages institutionnelles, messages provenant d'agences de santé publique, etc.* ». Et ce risque pourrait aller croissant selon Darren Guccione, dirigeant de Keeper security, pour qui «*les mesures de relance des gouvernements pourraient à l'avenir constituer un catalyseur presque parfait pour inciter les fraudeurs en ligne à frapper* » : dans ce contexte, en effet, « *de simples campagnes de mails peu sophistiquées, proposant de fausses inscriptions à des programmes de subvention ou d'aide publique pourraient s'avérer très efficaces* ». Google affirme déjà bloquer chaque jour « *jusqu'à 18 millions de tentatives d'arnaques liées au Covid-19 sur Gmail* ».

> ***« Les mesures de relance des gouvernements pourraient à l'avenir constituer un catalyseur presque parfait pour inciter les fraudeurs en ligne à frapper.»***
> **Darren Guccione**

Cette crise se démarque toutefois par trois risques spécifiques, largement soulignés par les observateurs. D'abord celui lié aux applications de traçage. Les préoccupations viennent de ce qu'elles « *ont été conçues dans la précipitation* », si bien qu'elles « *comporteront nécessairement des bugs à leur sortie* » selon Jon Callas, ancien directeur de la cyber-sécurité chez Apple, qui s'attend « *à ce qu'au moins une chose horrible en matière de confidentialité ou de sécurité se produise* ». Ce risque est décuplé par le fait que « *les données médicales font partie des données les plus recherchées par les hackers, car ce sont celles vendues le plus cher sur le Dark Web* », explique Stephen Burke. Les pirates les utilisent en effet « *pour créer de fausses pièces d'identité, acheter des médicaments vendus sur ordonnance, ou exploiter la maladie des personnes pour les escroquer* ». Le deuxième facteur de risque spécifique à cette pandémie vient du bouleversement des pratiques de travail des entreprises et des institutions. Comme l'explique une analyse publiée récemment par le cabinet McKinsey, la situation actuelle impose « *aux responsables de la sécurité informatique de trouver un équilibre entre deux*

priorités : se protéger contre les nouvelles cyber-menaces et maintenir la continuité des activités ». Le principal risque souligné par McKinsey vient ici du télétravail : celui-ci « *favorise l'utilisation d'équipements informatiques personnels insuffisamment protégés, et notamment dépourvus de VPN efficace* » ; le « *manque de connaissance des comportements dangereux ainsi que le stress et les désorganisations causés par la situation augmentant encore les risques*. » Enfin, un troisième danger vient de la vulnérabilité spécifique de certaines structures en première ligne dans la lutte contre la pandémie. C'est particulièrement le cas des hôpitaux « *débordés de patients, qui n'ont ainsi ni le temps de se concentrer sur leur sécurité, ni de négocier avec les cyber-pirates* », comme l'explique Markus Holzbrecher-Morys, chef de la sécurité informatique à la Fédération hospitalière allemande. De fait, Interpol a mis en garde le mois dernier contre « *un pic massif d'attaques numériques contre les hôpitaux et d'autres organisations de santé clés* » - les cybercriminels utilisant des virus informatiques « *pour garder les hôpitaux et les services médicaux en otage numériquement, les empêchant d'accéder aux fichiers et systèmes vitaux jusqu'au paiement d'une rançon* ».

Le cyber-espionnage, au cœur de la « géopolitique pandémique »

Cette crise est également marquée par une forte augmentation des faits de cyber-espionnage. Comme s'en émeut l'expert en cyber-sécurité Justin Fier dans les colonnes du New York Times, « *il s'agit d'une pandémie à dimension globale qui n'est malheureusement pas traitée comme telle : tous les États mènent une collecte de renseignements à grande échelle pour leur propre compte, afin de voir qui fait quel progrès en matière de recherche pharmaceutique, de commande de matériel, etc.* ». Les laboratoires et instituts de recherche sont de fait au centre de toutes les attentions. En plus de leur caractère hautement stratégique, ils apparaissent également particulièrement vulnérables « *en raison de leur mode de travail en réseau, impliquant un grand nombre de laboratoires, universités et entreprises, et où les informations sont fréquemment échangées via des canaux non sécurisés* », comme l'explique Le Figaro.

> ***« Il s'agit d'une pandémie à dimension globale qui n'est malheureusement pas traitée comme telle : tous les États mènent une collecte de renseignements à grande échelle pour leur propre compte.»***
>
> **Justin Fier**

Les accusations d'attaques d'origine étatique se sont démultipliées ces dernières semaines et font apparaitre des objectifs variés – ainsi que d'évidents sous-jacents géopolitiques. En Israël, le Mossad s'est spécialisé « *dans la sécurisation des approvisionnements nécessaires pour lutter contre la maladie (masques, respirateurs, médicaments, etc.)* », selon le New York Times. En Corée du Sud, des pirates auraient ciblé l'OMS ainsi que des responsables nord-coréens, japonais et américains, toujours selon le New York Times. En Europe, le Royaume-Uni a dénoncé « *des tentatives d'intrusion russes et iraniennes dans ses institutions luttant contre le coronavirus* », et Angela Merkel s'est insurgée il y a quelques jours contre « *les tentatives scandaleuses de la Russie pour pirater [ses] systèmes informatiques* ». Mais la cyber-guerre la plus remarquée est sans conteste celle entre la Chine, accusée par l'administration Trump de vouloir « *cibler les universités américaines, les sociétés pharmaceutiques et autres entreprises de santé dans le but de voler la propriété intellectuelle liée aux traitements et vaccins contre les coronavirus* », comme le rapporte le Wall Street Journal, et les États-Unis, qui concentrent pour leur part leurs efforts de cyber-espionnage sur deux objectifs clefs, selon The Independent : « *démontrer que la Chine a initialement caché la pandémie, et prouver que le virus est d'origine humaine et s'est échappé du laboratoire de Wuhan* ». Toutes ces allégations de cyber-attaques ont pour trait commun d'être dénoncées sans preuve – ce que soulignent tous les responsables des États mis en cause, à l'instar de Zhao Lijian, ministre des affaires Étrangères chinois, pour qui il ne s'agit que de « *diffamations à caractère géopolitique* ».

Il reste que cette crise « *révèle de façon évidente l'ampleur de notre dépendance aux outils numériques et la vulnérabilité de certaines institutions, notamment dans le secteur de la santé* », comme l'explique Claire Landais, Secrétaire générale de la défense et de la sécurité nationale, qui conclue en réaffirmant « *l'importance pour les pays de travailler à l'émergence de solutions numériques souveraines* ».

LIENS DES ARTICLES :

Jonathan Chadwick, « Cyber criminals create a spoof copy of the NHS website in the midst of the coronavirus pandemic to trick users into downloading dangerous malware that can steal their passwords and credit card data », The Daily Mail

https://www.dailymail.co.uk/sciencetech/article-8250737/Kaspersky-detects-fake-NHS-site-steals-credit-card-data.html

« Coronavirus cyber-attacks update: beware of the phish », Check Point

https://blog.checkpoint.com/2020/05/12/coronavirus-cyber-attacks-update-beware-of-the-phish/

« 'Modern Bank Heists' Threat Report from VMware Carbon Black Finds Dramatic Increase in Cyberattacks Against Financial Institutions Amid COVID-19 », VmWare

https://www.vmware.com/company/news/releases/vmw-newsfeed.Modern-Bank-Heists-Threat-Report-from-VMware-Carbon-Black-Finds-Dramatic-Increase-in-Cyberattacks-Against-Financial-Institutions-Amid-COVID-19.0ccd81eb-8142-40a2-9ce9-d77307f15961.html

Dan Hall, « Perfect cyber-storm : How hackers could cause a cyber doomsday during coronavirus pandemic – from shutting down hospitals to crashing banks », The Sun

https://www.thesun.co.uk/news/11595563/hackers-cyber-doomsday-coronavirus-pandemic-shutting-down-hospitals-crashing-banks/

« Nation-backed Hackers Tune Attacks To COVID-19 Fears: Google », Barron's

https://www.barrons.com/news/nation-backed-hackers-tune-attacks-to-covid-19-fears-google-01587653997

Rob Clymo, « The Covid-19 crisis is resulting in a growing wave of small business cybercrime », TechRadar

https://www.techradar.com/news/the-covid-19-crisis-is-resulting-in-a-growing-wave-of-small-business-cybercrime

Joseph Marks, « The Cybersecurity 202: Coronavirus tracking apps spark security concerns », The Washington Post

https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/05/05/the-cybersecurity-202-coronavirus-tracking-apps-spark-security-concerns/5eb05603602ff15fb00246d2/

Catherine Stupp, « Coronavirus Tracking Apps Raise Questions About Bluetooth Security », The Wall Street Journal

https://www.wsj.com/articles/coronavirus-tracking-apps-raise-questions-about-bluetooth-security-11588239000

Jim Boehm, « Cybersecurity's dual mission during the coronavirus crisis », McKinsey

https://www.mckinsey.com/business-functions/risk/our-insights/cybersecuritys-dual-mission-during-the-coronavirus-crisis

Sophie Caulier, « Coronavirus : le télétravail met en danger la confidentialité des entreprises », Le Monde

https://www.lemonde.fr/emploi/article/2020/05/17/coronavirus-le-teletravail-met-en-danger-la-confidentialite-des-entreprises_6039942_1698637.html

Arthur Le Denn, « Phishing : Des pirates informatiques se font passer pour Zoom, Microsoft Teams et Google Meet », L'Usine Digitale

https://www.usine-digitale.fr/article/phishing-des-pirates-informatiques-se-font-passer-pour-zoom-microsoft-teams-et-google-meet.N963546

Adrien Jaulmes, « Coronavirus: Pékin accusé d'espionner les laboratoires de recherche américains », Le Figaro

https://www.lefigaro.fr/international/coronavirus-pekin-accuse-d-espionner-les-laboratoires-de-recherche-americains-20200517

Catherine Stupp, « Hackers Change Ransomware Tactics to Exploit Coronavirus Crisis », The Wall Street Journal

https://www.wsj.com/articles/hackers-change-ransomware-tactics-to-exploit-coronavirus-crisis-11589448602

David E. Sanger and Nicole Perlroth, « U.S. to Accuse China of Trying to Hack Vaccine Data, as Virus Redirects Cyberattacks », The New York Times

https://www.nytimes.com/2020/05/10/us/politics/coronavirus-china-cyber-hacking.html

Ronen Bergman, « Israel's Not-So-Secret Weapon in Coronavirus Fight: The Spies », The New York Times

https://www.nytimes.com/2020/04/12/world/middleeast/coronavirus-israel-mossad.html

Harry Cole, « Iran and Russia launch hacking attacks on British universities in attempt to steal coronavirus vaccine secrets », The Daily Mail

https://www.dailymail.co.uk/news/article-8281091/Iran-Russia-launch-hacking-attacks-British-unis-attempt-steal-vaccine-secrets.html

« US Security Agencies Reportedly to Warn of Chinese Hackers Seeking to Obtain COVID-19 Vaccine Data », Sputnik

https://sputniknews.com/world/202005111079267122--us-security-agencies-reportedly-to-warn-of-chinese-hackers-seeking-to-obtain-covid-19-vaccine-data/

« Cyberattaques : Merkel dénonce les « tentatives scandaleuses » de la Russie », AFP

https://www.lesechos.fr/monde/europe/cyberattaques-merkel-denonce-les-tentatives-scandaleuses-de-la-russie-1202659

Gordon Lubold, « U.S. Says Chinese, Iranian Hackers Seek to Steal Coronavirus Research », The Wall Street Journal

https://www.wsj.com/articles/chinese-iranian-hacking-may-be-hampering-search-for-coronavirus-vaccine-officials-say-11589362205

Kim Sengupta, « Covid intelligence: Who was responsible for the cyber-attacks on China? », The Independant

https://www.independent.co.uk/independentpremium/long-reads/coronavirus-china-cyber-attack-vietnam-israel-mossad-trump-lab-a9502136.html

Michel Cabirol, « Covid-19 : les hôpitaux français relativement épargnés par les cyberattaques », La Tribune

https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/covid-19-les-hopitaux-relativement-epargnes-par-les-cyberattaques-847164.html