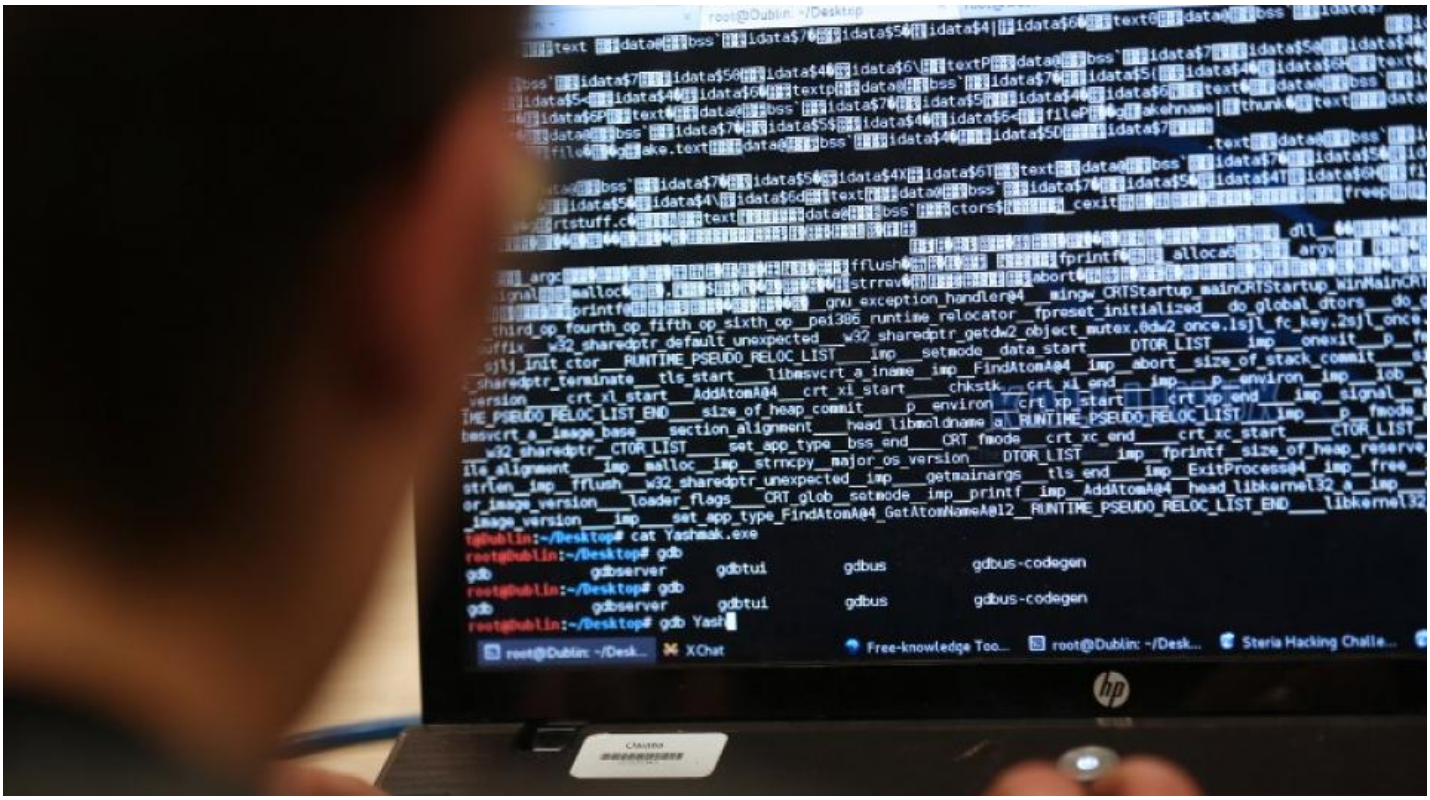
20 septembre 2020

Piratage automne hiver 2020/21

Voilà les techniques les plus utilisées par les escrocs en ligne et autres pirates informatiques



Le spectre des cyberattaques et des cybermenaces est particulièrement vaste. Nos conseils pour ne pas y succomber.

Avec Thierry Berthier

Atlantico : Quelles sont les types d'attaques les plus répandues sur Internet et quelles sont les méthodes et les techniques les plus utilisées par les pirates informatiques en cette période automne hiver 2020-21 visant des internautes ?

Thierry Berthier : En 2020, le spectre des cyberattaques et des menaces cyber est particulièrement étendu, tout comme celui des cibles. Les particuliers sont principalement touchés par les campagnes de phishing avec la réception de messages malveillants contenant un lien toxique. L'internaute imprudent clique sur le lien en pensant avoir affaire à une page légitime alors qu'il déclenche l'exécution d'un logiciel malveillant (malware) qui va s'installer sur sa machine, à son insu. Ce mode opératoire est extrêmement répandu. Le malware déployé peut avoir plusieurs fonctions : si c'est un rançongiciel (ransomware), il va chiffrer tout ou partie des données présentes sur le disque dur de la victime puis demander une rançon payable en bitcoin contre la restitution des données. L'internaute peut choisir de payer la rançon s'il estime que la valeur de ses données perdues dépasse cette rançon ou d'accepter de les perdre définitivement. L'attaquant peut alors tenter d'autres mécanismes de chantage s'il estime que le disque contient des données sensibles ou gênantes pour la cible. Il faut avoir conscience que tous les moyens de pression seront utilisés, même les plus « dégueulasses » car la victime a bien affaire à de la cyberdélinquance. En dehors des rançongiciels, le logiciel malveillant peut avoir des fonctions d'espionnage ou de simple vol et exportation de données. D'autres malwares prendront le contrôle de la webcam de la cible pour collecter de l'information dans le cadre de la préparation d'une autre attaque. Les objets connectés de l'internaute peuvent aussi constituer des cibles que l'attaquant va recruter et « zombifier » au sein d'un Botnet (un réseau d'objets connectés dont il a pris le contrôle). Cette « armée » d'objets connectés sous contrôle de l'attaquant sont ensuite utilisés pour envoyer une multitude de requêtes à un serveur ciblé et le paralyser. On parle alors d'attaque par DDoS (déni de service distribué). Certains DDoS peuvent atteindre 2,3 Tbps (TeraBit par seconde) comme cela a été le cas en février 2020 lors d'une attaque contre AWS. L'ordinateur de l'internaute peut aussi être ciblé par un logiciel crypto-mineur : un lien malveillant sur lequel vous avez cliqué installe un logiciel mineur de cryptomonnaies qui va travailler en tâche de fond sur votre machine en abaissant fortement ses performances (ralentissements, interruption de service, diminution du temps de batterie disponible, etc…). Enfin, l'internaute (le particulier) peut être cible par une multitude de tentatives de fraudes aux faux virements, fausses factures, faux remboursements, faux supports… Là aussi, l'imagination de l'attaquant est sans limite. Le niveau de complexité des attaques de type FOVI (Faux ordres de virements) augmente très régulièrement. L'escroquerie FOVI s'appuie souvent sur l'usurpation d'identité qui aujourd'hui peut être facilitée par l'intelligence artificielle (réseaux antagonistes génératifs, GAN).

Toutefois, les cibles privilégiées des groupes de hackers restent les entreprises, administrations, collectivités territoriales, organisations gouvernementales pour lesquelles l'attaquant peut espérer collecter de la donnée sensible (secrets et process

industriels, base de clients, de produits, de services, de sous-traitants, etc… Ces données ont toujours une valeur à la revente sur les marchés spécialisés du Darknet. Quand il touche une entreprise, un rançongiciel peut provoquer de lourdes pertes (en millions d'euros) et parfois même mettre en danger sa survie. De nombreuses organisations impactées choisissent de payer la rançon en espérant récupérer une partie des données. Ce n'est pas toujours le bon choix mais c'est ainsi. Les autres types d'attaques s'appliquent aux entreprises avec, à la clé, des gains faciles et presque sans risque pour l'attaquant.

Connaît-on une recrudescence des cas d'attaques informatiques menées par des pirates informatiques visant des institutions ou ciblant des lieux ou des bâtiments particuliers ? Ces attaques ont-elles évolué dans leur méthode ?

On observe que lorsqu'un conflit, une crise, un scandale survient dans l'espace physique, cet évènement est systématiquement projeté sur l'espace numérique avec des opérations contre les protagonistes. Les conflits du Moyen-Orient possèdent une composante cyber en général très active (cyber-renseignement, influence, contre-influence, déception et leurrage, désanonymisation). Les périodes d'élections suscitent des vagues de cyberattaques sur les partis politiques en compétition. La crise sanitaire du Covid-19 n'échappe pas à cette règle. Les campagnes de phishing liées au Coronavirus se sont multipliées durant la période du confinement. De janvier 2020 à avril 2020, plus de 907 000 campagnes de spam-covid ont été recensées. 737 nouveau malwares associés au Covid ont été déployés sur des cibles diverses. Plus de 48 000 url de sites malveillants « lutte contre la Covid-19, masques, traitements » ont été mis en ligne. Des dizaines de milliers d'internautes ont été trompés et ont perdu de l'argent, du temps et de la confiance dans des arnaques opportunistes. C'est la triste réalité. Encore une fois, la cyberdélinquance fait feu de tout bois, exploite toutes les failles cognitives et profite de tous les contextes dégradés pour s'enrichir. Au niveau mondial, les campagnes de spam en 2020 ont été multipliées par 220 par rapport à la même période en 2019. Le nombre d'url malveillantes Covid a quant à lui augmenté de 260 %. Actuellement, l'industrie pharmaceutique et les laboratoires travaillant sur un futur vaccin Covid sont particulièrement ciblés par des cyberattaques très agressives. Notons que ces attaques ralentissent parfois sensiblement les activités de ces organisations.

Une patiente qui devait être opérée en urgence à la clinique universitaire de Düsseldorf est morte lors de son transfert vers un autre hôpital, rendu nécessaire par une attaque informatique ayant paralysé le fonctionnement de la clinique. Ce drame révèle-t-il une gradation, une étape supplémentaire dans la stratégie des pirates informatiques ? Après la crise du Covid-19 et suite à ce drame faut-il s'attendre à une stratégie plus "agressive" et de plus grande ampleur de la part des pirates informatiques dans leurs méthodes d'attaques à l'avenir ?

Effectivement, cela faisait des années que la communauté cyber mondiale se posait cette question : une cyberattaque a-t-elle déjà provoqué une mort directe ? Dans un contexte de guerre (lors du conflit Syrien par exemple), la réponse était positive. Dans un contexte de paix et civil, c'était moins clair jusqu'à ce premier cas référencé. Il s'agit d'un rançongiciel qui paralyse les activités d'un hôpital allemand et qui provoque le décès d'une patiente non prise en charge. La forte connectivité des infrastructures industrielles, de secours, des transports, fait augmenter le risque de décès provoqués par une cyberattaque. On imagine les effets d'une cyberattaque sur le système de navigation d'un avion de ligne ou sur un poste de contrôle aérien. Ce risque est pris très au séreux par les autorités et par toutes les agences de sécurité du monde. Une attaque sur le système de signalisation d'un réseau de trains ou sur les feux tricolores d'un réseau routier pourrait elle aussi provoquer des accidents mortels. Certains dispositifs pacemaker connectés implantés dans la poitrine de malades présentaient des failles de sécurité qui les rendaient potentiellement vulnérables. Le liste des victimes cyber commence aujourd'hui. Nous devons tout faire pour qu'elle ne s'allonge pas.

La France est-elle suffisamment préparée pour faire face à des attaques informatiques à l'issue de la crise sanitaire ?

Aucun Etat ne doit avoir l'arrogance de penser qu'il est à l'abri de cyberattaques massives. Cela dit, la France fait partie des très bons élèves. Elle a choisi, il y a plus de dix ans, de se doter d'une Agence Nationale dédiée à la sécurité des infrastructures critiques civiles : l'ANSSI.

L'ANSSI a joué un rôle à la fois silencieux et actif dans la résilience des systèmes d'information des OIV français (Opérateurs d'Importance Vitale). Sans cette protection et cette veille constante de très haut niveau, de nombreuses administrations, grandes entreprises et organisations sensibles auraient été régulièrement impactées par les campagnes référencées depuis dix ans. C'est une certitude. Le rôle de l'ANSSI est aussi d'éduquer aux bonnes pratiques de la sécurité numérique et parfois de contraindre les organisations qui auraient tendance à négliger le risque cyber. La France a pris toute la mesure des menaces et a fait ce qu'il fallait en 2010. Il faut poursuivre l'effort « d'évangélisation » à la sécurité en l'appliquant aux plus petites structures (non OIV) qui subissent des attaques destructrices. Les mentalités et les bonnes pratiques progressent dans le bon sens mais le niveau de complexité des attaques monte en puissance également. Nous sommes engagés dans une course sans fin entre l'attaquant et le défenseur avec de nouvelles surfaces et vecteurs d'attaques (IoT, Cloud, 5G, Robotique, IA, mobilités, …). Les enjeux sont importants. Au niveau mondial, les attaques informatiques coûtent 6000 Milliards de dollars par an ! Nous devons former des experts en cybersécurité. La pénurie est inquiétante puisqu'elle concerne 3,8 millions de postes non pourvus à l'échelle mondiale. Il faut donc attirer les talents vers la cybersécurité et les former correctement. Tout cela a un coût et demande une prise en compte dans les plans de formation de l'enseignement supérieur.