3 questions sur l'attaque cyberjihadiste de TV5 Monde (MAJ)

Ce matin la France s'est réveillé avec une cyberattaque importante sur le média TV5 Monde. Plusieurs éléments ont été ciblées : les réseaux sociaux, page Facebook et compte Twitter. Et, plus original, l'outil de diffusion qui a été touché privant ainsi plusieurs millions de personnes dans le monde des programmes de la chaîne. Cette attaque a été revendiquée par Cyber Caliphate, un groupe de hackers se réclamant de Daesh. Reste qu'au-delà de l'émotion suscitée, des questions restent en suspens. Nous les avons posées à des spécialistes de la sécurité informatique.

1 – Comment les pirates ont-ils procédé ?

Plusieurs hypothèses sont possibles pour expliquer le *modus operandi* des pirates. Mais selon les experts en sécurité, le processus reste classique. *« Il respecte les 5 étapes traditionnelles d'une cyberattaque »*, explique Laurent Heslault, directeur de la stratégie sécurité chez Symantec. Ces différents points sont : la reconnaissance avec la collecte d'informations pour connaître les points de vulnérabilité d'une entreprise ; une incursion via plusieurs techniques ; la prise de contrôle des machines en restant indétectable ; l'attaque en elle-même et la sortie sans se faire repérer. Dans le cas de l'attaque sur TV5 Monde, les experts trouvent des similitudes avec celle menée contre le quotidien *Le Monde* le 20 janvier dernier par l'armée électronique Syrienne. Pour Laurent Heslault, « *il faut quand même du temps et de la patience pour monter une telle opération. Surtout pour pénétrer aussi profondément dans le réseau* ».

Le site Internet Breaking3zero donne une version de ce qui a pu se passer. Selon lui, le processus aurait démarré par l'exploitation d'une faille Java qui a permis l'installation d'un virus au format VBS (Visual Basic Script) nommé ISIS. Le site publie une capture d'écran du script. « *Nous avons analysé ce script en laboratoire et on retrouve sa trace jusqu'en 2006. Il est très peu sophistiqué et toucherait des anciennes versions de Windows* », indique Guillaume Lovet, expert en cybercriminalité chez Fortinet.

Sur la diffusion du virus, le site émet plusieurs hypothèses : l'envoi de faux e-mails, la réception de faux communiqués de presse et, enfin, le piratage de l'adresse IP de compte Skype, outil souvent utilisé par les journalistes en déplacement. Ce dernier point est jugé peu crédible par les experts en sécurité sollicités. « *Le spearphishing semble la méthode la plus probablement employée par les pirates* », explique l'expert de Fortinet.

2 – Quels sont les dégâts ?

Le plus visible et le plus symbolique est sans conteste l'arrêt de la diffusion des programmes de la chaîne. « *A l'inverse de ce que nous connaissions tel le* defacement *de sites ou de piratage de comptes sur les réseaux sociaux, les pirates font maintenant de véritables opérations de saccage et de vandalisme comme dans le cas de Sony Pictures* », explique Thierry Karsenty de CheckPoint. Les cyberjihadistes ont effectivement réussi à remonter jusqu'au serveur de diffusion. Est-ce que cela aurait pu aller jusqu'à la prise de contrôle de l'antenne de la chaîne ? « *Mon intime conviction est que cet aspect-là est*

plutôt un dommage collatéral de l'attaque des cyberjihadistes et non un but en soi. Les cibles principales étaient la récupération de mots de passe pour les réseaux sociaux », analyse Guillaume Lovet.

Il n'en demeure pas moins que la remise en état s'avère difficile et longue. Yves Bigot, directeur général de TV5 Monde, a indiqué dans un communiqué que « *nos systèmes ont été extrêmement détériorés par cette attaque d'une puissance inouïe. Le retour à la normale va prendre des heures, voire des jours* ». Le rétablissement des comptes des réseaux sociaux a pu se faire rapidement, ainsi que celui du site Web. Par contre, la remise en route des équipements de la partie diffusion est plus problématique notamment sur le flux en direct. « *En général, les grands médias disposent d'un équivalent de PRA (plan de reprise d'activité), mais la question se pose quand il faut redémarrer sur un environnement propre sans virus* », estime Thierry Karsenty.

Les équipes de TV5 Monde vont pouvoir compter sur l'aide des experts techniques de l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) pour rétablir le service et mener l'enquête afin de découvrir les traces et les indices de l'attaque. Devant l'ampleur de la tâche, le nombre d'experts de l'ANSSI a été renforcé en passant de 4 à 13 personnes selon *Le Figaro*. Elles seront épaulées par la Direction générale de la sécurité intérieure (DGSI), la Sous-direction antiterroriste et les cyber-policiers de la Direction centrale de la police judiciaire. Le parquet de Paris a quant à lui ouvert une enquête pour « *accès, maintien frauduleux et entrave au fonctionnement d'un système de traitement automatique de données* » ainsi qu'« *association de malfaiteurs en relation avec une entreprise terroriste* ».

3- Le broadcast est-il suffisamment sécurisé ?

Si la question de l'identité des auteurs de l'attaque ou plutôt de ses commanditaires reste toujours en suspens, d'autres interrogations sur la sécurité des médias restent posées. Ainsi, comment des pirates ont-ils pu avoir accès à la plateforme de broadcast de TV5 Monde. Depuis 2006, la chaîne travaille avec Ericsson (via le rachat de Technicolor en 2012) pour l'exploitation de sa plate-forme de production, diffusion et post-production. Ce partenariat a été renouvelé en 2012 et court jusqu'en février 2018. Sollicitée, la firme suédoise nous a indiqué qu'elle ne gérait pas l'IT de TV5 Monde mais uniquement la partie audiovisuelle.

Une telle attaque ne surprend pas un spécialiste du broadcast que nous avons sollicité, mais qui préfère rester anonyme. « *Dans ce type de plateforme, il y a des serveurs Windows qui gèrent des serveurs médias en NAS pilotés par des cartes spécialisées* », explique-t-il. Il ajoute que « *habituellement, ces plateformes sont déconnectées d'Internet, mais il y a des cas particuliers* ». De même, il pointe du doigt, « *le problème de la mise à jour des OS pour des questions d'incompatibilité* ». Un brin provocateur, un tweet d'Olivier Laurelli alias Bluetouff s'interrogeait : « *est-ce que ne pas isoler son infra de diffusion du frontal est un acte terroriste ?* ».

Des politiques de sécurité à revoir donc. Un point que reconnaît le spécialiste du broadcast que nous avons interrogé et qui explique que, dans son entreprise, un plan de renforcement de la sécurité est à l'étude. *« Il faut voir le côté positif de l'affaire, à savoir une prise de conscience de la vulnérabilité des grands médias aujourd'hui. C'est le moment de se poser les questions sur la gestion du risque, sur les outils de détection ou sur le système de backup de la partie technique »*, constate Laurent Heslault. « *Tous les médias sont visés, il faut avoir des politiques de sécurité cohérentes. Si l'utilisation de*

vieux OS est encore active, il s'agit d'une faute grave de sécurité », souligne Guillaume Lovet. Pour Thierry Karsenty, « *l'attaque en janvier sur* Le Monde *a provoqué beaucoup d'échanges sur la question de la sécurité des médias, mais élever le niveau en la matière ne se fait pas du jour au lendemain* ».

Une démarche qui s'inscrira dans les récentes annonces sur la sécurité des OIV (opérateur d'importance vitale). Une liste non publique, mais on peut supposer que les grands médias y trouvent leur place. En tous cas, les dirigeants des grands groupes de médias ont été invités par Fleur Pellerin, ministre de la Culture, à *« s'assurer des points de vulnérabilité ou de risque qui peuvent exister et de la manière de les traiter au mieux ».* Du pain sur la planche sans aucun doute…

A lire aussi :

Manuel Valls intensifie la lutte contre le cyberterrorisme
Cybersécurité : la France dans le Top 5 des puissances du mal