TV5 Monde, une attaque prévisible

Après l'attaque dont TV5 Monde a été victime mercredi soir, la chaîne a seulement pu recommencer à diffuser normalement jeudi après-midi. Selon plusieurs experts, cette attaque était prévisible. D'après le politologue Abdelasiem El Difraoui, *« la question était de savoir quand elle surviendrait parce que cela fait cinq ans que les chercheurs la sentaient venir comme la suite inéluctable de la stratégie que les islamistes mettent en œuvre depuis longtemps sur internet »*.

Du côté des spécialistes en informatique, on explique qu'une faille informatique sur un simple ordinateur de bureau serait à l'origine de l'attaque. ■

L'attaque djihadiste était attendue, mais pas la cible

▶ De nombreuses zones d'ombre persistent après le piratage de TV5 Monde.
▶ Cela fait plusieurs années déjà que les spécialistes s'attendaient à ce type d'action.
▶ La RTBF a développé des procédures de sécurité renforcées pour réduire au maximum les risques d'une telle attaque.

TV5 Monde a pu reprendre totalement sa diffusion jeudi en fin d'après-midi, après la cyberattaque dont elle a été la cible, dans la soirée de mercredi. Mercredi, vers 22 heures, des pirates qui se revendiquaient de l'organisation de l'Etat islamique (EI) avaient paralysé le système informatique de la chaîne pour s'emparer, d'abord, de ses comptes Facebook, Twitter et de son site internet, puis de tout son réseau. La chaîne, dont l'écran est resté noir pendant plusieurs heures, a rétabli progressivement ses programmes ce jeudi.

Cette cyberattaque, sans véritable précédent dans l'histoire de la télévision, a suscité une kyrielle de réactions scandalisées, dont celle du Premier ministre français Manuel Valls qui, dans un tweet, a dénoncé *« une atteinte inacceptable à la liberté d'information et d'expression »*.

Pourquoi TV5 Monde ? Cette question, Yves Bigot, le directeur général de la chaîne aura probablement été le premier à se la poser. *« Mais j'ignore encore si nous avons été la cible ou le moyen »*, expliquait-il, ce jeudi.

Difficile, aussi, de dire si les pirates ont voulu s'en prendre à la chaîne française – TV5 Monde est une société de droit français installée à Paris – pour dénoncer la part prise par la France sur divers théâtres d'opération face à l'Etat islamique ou à ses satellites, ou à l'opérateur francophone qui, via ses onze chaînes, diffuse sur tous les continents *« des valeurs qui sont à l'exact opposé de celles qu'entendent promouvoir les radicaux islamistes »*, comme le rappelle Alain Gerlache, le secrétaire général de la Communauté des télévisions francophones.

Des documents présentés comme des pièces d'identité et des CV de proches de militaires français impliqués dans les opérations contre l'EI, ont été postés sur le compte Facebook de TV5 Monde durant l'attaque. *« La teneur de ces messages incline à penser que c'est à la chaîne française que les pirates entendaient s'en prendre, de la même façon qu'on visait les journaux durant les guerres coloniales,* estime l'historien Fabrice d'Almeida, professeur à Paris II, spécialiste de la propagande par l'image et de la manipulation, et auteur de l'ouvrage *Une histoire mondiale de la propagande* (La Martinière). *Ce qui traduirait dans le chef des pirates une certaine méconnaissance de la mission de la chaîne et des contenus qu'elle diffuse. On ne peut pas non plus exclure que l'attaque a visé le maillon faible du paysage audiovisuel : une chaîne dont la cyber-sécurité présente sans doute d'autant plus de failles qu'elle met à contribution des télévisions francophones du monde entier »*.

« Cette attaque est la transposition numérique du concept de la guerre asymétrique »
ABDELASIEM EL DIFRAOUI

Pour le politologue Abdelasiem El Difraoui, auteur de l'ouvrage *Al-Qaïda par l'image* (PUF), il n'est pas douteux que *« TV5 Monde a été attaquée parce qu'elle est très regardée en Syrie, au Liban et dans plusieurs pays d'Afrique »*. Pour lui, une attaque de ce type était hautement prévisible, même si la cible était inconnue : *« La question,* dit-il, *était de savoir quand elle surviendrait parce que cela fait cinq ans que les chercheurs la sentaient venir comme la suite inéluctable de la stratégie que les islamistes mettent en œuvre depuis longtemps sur internet. Cette attaque, c'est la transposition numérique du concept de la guerre asymétrique, propre au terrorisme : causer un maximum d'effets en mobilisant un minimum de ressources. »*

Dans une interview aux *Echos*, le directeur informatique de TV5Monde, Jean-Pierre Verines, raconte que l'Agence nationale de sécurité des systèmes d'information (Anssi), en charge de la sécurité des systèmes informatiques les plus sensibles, avait récemment prévenu la chaîne qu'au moins une partie de ses serveurs n'était pas suffisamment bien sécurisée et avait déjà été compromise. L'Anssi avait découvert que l'un de ces serveurs avait été utilisé pour réaliser une attaque, sans doute dirigée vers une autre cible. Il est assez courant, en effet, que des pirates utilisent des serveurs vulnérables pour servir de relais aux attaques qu'ils organisent, masquant ainsi l'origine exacte de l'agression.

Que l'attaque soit survenue au moment même où TV5 Monde lançait dans les pays du Maghreb et du Moyen-Orient une nouvelle chaîne thématique dédiée à « l'art de vivre à la française » n'est probablement qu'une coïncidence, selon Yves Bigot. ■

STÉPHANE DETAILLE

RÉACTION

Yves Bigot : « Ça fait froid dans le dos »

Yves Bigot, le patron de TV5 Monde, a passé une nuit blanche agitée. Au *Soir*, il confie son désarroi : « *Quand tu fais de la télé et que tu as onze chaînes en écran noir, en matière de diffusion et de ton métier, il ne peut rien se passer de pire. C'est ce que tu cherches à préserver. Après, le sentiment qui vient quand on lit sur nos sites et réseaux sociaux les messages postés, ça fait froid dans le dos.* »

Une réunion avec tous les principaux médias de France (TF1, M6 et l'AFP par exemple) a été organisée en fin d'après-midi au ministère de la Culture. « *On a expliqué à tous nos collègues comment on avait géré la situation. Ils vont bénéficier des services spécialisés de l'Etat pour voir s'ils n'ont pas déjà été infiltrés par des attaques dormantes. C'est presque comme si on mettait du désinfectant partout, mais le risque zéro n'existe pas.* »

La chaîne travaille d'arrache-pied pour retrouver un rythme normal de diffusion de ses programmes, mais Yves Bigot craint que des « *mines* » aient été laissées par les pirates et déclenchent une nouvelle attaque.

MAXIME BIERMÉ

sécurité Les télés, victimes prévisibles d'une cyberguerre

Comment l'un des plus grands réseaux audiovisuels au monde peut-il être mis sur les genoux en quelques minutes par un attaquant déterminé ? La réponse à cette question épineuse ne se posera pas uniquement au sein de TV5 Monde. Tous les opérateurs devront sérieusement interroger la sécurité de leurs infrastructures.

Mais comment pirate-t-on une télé ? « *L'une des méthodes les plus fréquentes dans les tentatives d'attaques, c'est de cibler les équipements de programmation de la diffusion*, explique un spécialiste contacté par *Le Soir*. *C'est le système qui détermine quelle séquence audiovisuelle passe à tel moment précis. Pour des raisons pratiques, ces équipements sont souvent connectés au réseau général de l'entreprise.* »

Selon le site *Breaking3zero*, une faille informatique sur un simple ordinateur de bureau serait à l'origine de l'attaque. Elle aurait permis l'infection par un virus qui se serait rapidement répliqué pour atteindre les serveurs par lesquels sont diffusés les programmes. En quelque sorte, il s'agit du « *centre de dispatching de TV5 Monde* ».

Les ordinateurs compromis auraient également permis aux attaquants de s'emparer des mots de passe nécessaires pour prendre le contrôle des comptes Twitter et Facebook de TV5 Monde. A ce stade, rien n'a cependant été confirmé par les responsables de l'entreprise.

Sur son site web, RTL France affirme que l'attaque serait partie de France. Elle aurait transité par un réseau qui emploierait, d'après les services de renseignement américains, une quinzaine de pirates chevronnés dans le monde. Un tel scénario pourrait-il se dérouler en Belgique ? « *Nous avons pris d'importantes précautions de longue date*, explique l'administrateur délégué de RTL Belgique, Philippe Delusinne. *Mais l'on sait que si des personnes sont déterminées à faire tomber des protections à n'importe quel prix, il ne sera pas facile de les arrêter. Nous n'avons pris aucune mesure particulière liée à ce qui s'est passé chez TV5 Monde, ce ne sont pas des choses qui s'improvisent. Mais après le piratage dont avait été victime Sony, il y a quelques mois, nous avions revu en profondeur chacun des paramètres de protection de notre réseau, que nous avons voulu particulièrement costaud.* » ■

A.Je.

en Belgique « La RTBF n'est pas totalement à l'abri »

ENTRETIEN

Directrice générale des technologies à la RTBF, Cécile Gonfroid n'a pas attendu le piratage de TV5 Monde pour blinder la sécurité de la chaîne publique.

Mais comment se prémunir contre de telles menaces ? Elle répond à nos questions.

Le piratage de TV5 Monde pose la question de la sécurité des chaînes belges. Un tel scénario est-il envisageable à la RTBF ?

A ce stade, on ne sait pas encore avec précision comment les pirates ont pu commettre leurs actes. On parle d'un ordinateur personnel qui se serait connecté sur le réseau de l'entreprise. A la RTBF, ce type de connexion n'est pas autorisé. Une personne qui vient dans nos locaux avec son équipement personnel peut se connecter au wi-fi, pour lire ses messages. Mais elle ne pourrait pas utiliser nos applications.

L'un des ordinateurs internes de la RTBF pourrait cependant être un jour infecté…

C'est vrai. Mais le personnel de l'entreprise n'a pas les permissions d'administration nécessaires pour installer des logiciels sur son poste de travail. Si de nouveaux programmes sont nécessaires, ils sont d'abord testés par l'équipe informatique. C'est un peu plus compliqué à gérer, mais je suis rassurée, aujourd'hui, d'avoir imposé ces règles qui augmentent le degré de protection.

Si l'on en croit les spécialistes,

l'un des talons d'Achille de la sécurité de nombreux opérateurs audiovisuels, c'est que le réseau qui est utilisé par l'ensemble des employés n'est pas distinct de celui sur lequel se trouvent les serveurs de diffusion. C'est le cas à la RTBF ?

Chez nous, ce sont deux réseaux séparés. Mais il y a des interconnexions. On n'est donc pas totalement à l'abri.

Est-ce qu'il y a des mesures de sécurité particulières qui ont été prises pour se protéger contre des cyberattaques ?

Nous avons multiplié les initiatives pour renforcer la sécurité du réseau. On a mis en place un monitoring du réseau qui fonctionne vingt-quatre heures sur vingt-quatre. C'est une société spécialisée qui se charge de ces opérations. Dès qu'il y a une activité anormale, l'alerte est déclenchée.

Que se passerait-il si votre serveur de diffusion était piraté ?

Nous avons des copies de sauvegarde de tous nos serveurs à l'extérieur de la RTBF, y compris de tous ceux sur lesquels se trouvent nos productions. En quelques heures, tout pourrait être restauré.

La RTBF a-t-elle préparé un plan de reprise d'activité en cas de désastre ?

On y travaille. Plusieurs volets ont déjà été traités même si tout n'a pas encore été validé par le comité de direction. Nous avons des réunions régulières avec les responsables pour envisager le scénario du pire pour toutes nos activités. Comment reprendre la diffusion en utilisant d'autres antennes. La priorité sera donnée à l'info. Nous voulons nous donner les moyens de relancer rapidement un JT ou de réalimenter nos sites web en informations. Tout le monde dans l'entreprise a pris conscience du risque. ■

Propos recueillis par ALAIN JENNOTTE

les auteurs Une revendication opportuniste d'un Daesh affaibli

Jeudi, le site d'investigation *breaking3zero.com* affirmait avoir identifié deux des pirates responsables de l'attaque, l'un basé en Algérie et l'autre en Irak, où il combattrait au sein de l'Etat islamique. Information qui, à l'heure actuelle, n'est confirmée par aucune autre source, ni aucune autorité.

Si on ignore donc encore qui, précisément, se cache derrière l'attaque de TV5, il semblait communément admis ce jeudi que ce piratage-là est d'une puissance inédite et qu'il n'est pas l'œuvre d'amateurs. Certains experts doutent pourtant que Daesh puisse être le commanditaire de l'attaque... Plutôt l'heureux bénéficiaire.

« Il est vrai que c'est un piratage tout à fait inédit. Mais je serais très étonné qu'un organisme de terrain comme Daesh puisse mener ce type d'attaque, même si l'objectif me semble plus évident : montrer aux mécréants de quoi Daesh est capable », estime André Jacob, spécialiste du terrorisme et ancien commissaire à la Sûreté de l'Etat.

« Internet est plutôt le terrain d'Al-Qaïda. Ça ne cadre pas avec la stratégie de l'Etat Islamique, qui, pour le dire platement, a autre chose à faire en ce moment. »

Une théorie qui semble également crédible aux yeux de Rik Coolsaet, professeur de relations internationales à l'Université de Gand. *« Le problème avec ce genre de cyberattaques, c'est que beaucoup d'hypothèses circulent mais que l'on dispose au final de très peu de faits. Ce qui, par contre, me semble plus évident, c'est que le piratage de TV5 ne correspond pas aux nécessités actuelles de l'Etat islamique – bien que l'organisation ait besoin en ce moment de redonner une image de gagnant qui va de l'avant, surtout après la défaite de Tikrit. Il est par contre vrai que Daesh compte, dans ses rangs, des hommes ayant appartenu à la garde de Saddam Hussein et qui sont dotés de compétences en génie militaire ou en électronique et qui connaissent les ficelles de la propagande. Donc, à ce stade, je dirais que toutes les hypothèses, y compris celle-là, sont valables. »*

« En difficulté, Daesh n'a probablement plus les moyens financiers de commanditer une telle attaque » RIK COOLSAET

Mais le spécialiste du terrorisme miserait davantage sur une récupération purement opportuniste de la part de Daesh. *« Les auteurs pourraient être des sympathisants de Daesh qui voudraient en faire partie mais qui ne parviennent pas à se rendre sur le terrain. Ce qui ne signifie pour autant pas que Daesh est le commanditaire de l'attaque. Il est même tout à fait possible que l'organisation n'ait pas été informée des projets des pirates, mais qu'elle saute sur l'occasion pour la revendiquer. »*

Si « sous-traiter » une telle opération en faisant appel à des pirates de haut vol, des hackers de la pointure de ceux qui agissent pour le compte d'Anonymous, semble au-dessus des moyens de l'organisation terroriste, qui consacre l'essentiel de ses ressources financières (lesquelles auraient d'ailleurs tendance à s'épuiser) à l'entretien de ses combattants et à la gestion des villes comme Raqqa qui sont encore sous son contrôle, la revendiquer après coup ne coûte rien. En termes d'image, par contre, c'est bingo ! *« Là est tout le problème »*, déplore Rik Coolsaet. *« Je crains qu'après cette attaque, on ne surestime à nouveau la capacité de Daesh. Que l'on offre à ces combattants le statut de super-guerriers alors qu'ils en sont loin. »* ■

LUDIVINE PONCIAU

TV5 Monde est p

Si les pirates visaient
fausse route, du moin
France 24 incarne à 1
Elle est présente dans
tionnariat de TV5 Mo
de 200 pays, est qua
français. France Télév
détient 11,11 % des pa
Radio-Canada (6,67 %
(3,29 %), l'Institut de
Médias Monde (12,64
diale et Monte Carlo
complètent le tableau

L'UE pour un ren

La Commission europ
cybersécurité en Euro
mier vice-président d
que face à ces *« terro*
dernes (...), nous devro
source européenne, o
la fin du mois un *« ag*
ment à la lutte contre

TV5 Monde est présente dans 200 pays

Si les pirates visaient la France à travers TV5 Monde, ils faisaient fausse route, du moins au niveau symbolique. Une chaîne comme France 24 incarne à 100 % la représentation de la France à l'étranger. Elle est présente dans 253 millions de foyers à travers 177 pays. L'actionnariat de TV5 Monde, qui touche 260 millions de foyers dans plus de 200 pays, est quant à lui réparti entre huit acteurs dont quatre non français. France Télévisions est le principal actionnaire (49 %), la RTBF détient 11,11 % des parts tout comme la SSR suisse. Les Canadiens de Radio-Canada (6,67 %) et Télé-Québec (4,44 %), Arte France (3,29 %), l'Institut des archives françaises l'INA (1,74 %) et France Médias Monde (12,64 % répartis entre France 24, RFI, la radio mondiale et Monte Carlo Doualiya, la radio universaliste en langue arabe) complètent le tableau. (M.B.)

L'UE pour un renforcement de la cybersécurité

La Commission européenne a plaidé jeudi pour un renforcement de la cybersécurité en Europe, après l'attaque contre TV5 Monde. Le premier vice-président de la Commission, Frans Timmermans, a déclaré que face à ces *« terroristes »* qui *« ont des instruments numériques modernes (...), nous devrons continuer à renforcer notre cybersécurité »*. De source européenne, on a souligné que la Commission devait adopter à la fin du mois un *« agenda sur la sécurité »* qui sera consacré notamment à la lutte contre les attaques informatiques. (afp)