



Il s'avère que la déclaration du Washington Post sur des hackers russes est une fausse information.



Depuis 2016, l'année de la campagne électorale américaine il est toujours question de cyber-attaques russes sur des objectifs américains.

Depuis 2016, l'année de la campagne électorale américaine il est toujours question de cyber-attaques russes sur des objectifs américains. Dans un communiqué de la dernière semaine de décembre, les services secrets américains pour l'étranger la CIA et la police fédérale des Etats-Unis le FBI, affirment avoir trouvé assez de preuves qui montrent que la Russie s'est immiscée de manière inadmissible dans la campagne présidentielle américaine par le biais de cyber-attaques. Avec ces prétendues preuves, le président américain en exercice a décrété des sanctions contre la Russie : ainsi 35 diplomates russes ont été expulsés du pays.

Le président russe Vladimir Poutine a toujours démenti : Moscou ne s'occupe pas de cyber-attaques au niveau du gouvernement et il n'a rien à voir avec ces attaques. Un des exemples les plus récents montre avec quelle précaution il faut considérer les accusations en matière de cyber-attaques russes :

Le 30 décembre 2016 le quotidien américain « The Washington Post » a écrit que des pirates informatiques russes avaient réussi à s'introduire dans le réseau d'un fournisseur d'électricité de l'Etat fédéral américain du Vermont. Dans le système du fournisseur d'électricité on aurait trouvé un « malware » – un logiciel « malveillant », qu'on pourrait attribuer à une cyber-attaque russe nommée « Grizzly Steppe ». C'est ce qu'a affirmé le journal en s'autorisant d'organismes publics américains qui n'étaient pas nommément précisés.

Ce message diffusé par le Washington Post et l'agence de presse Reuters a rapidement fait son chemin jusqu'aux médias principaux de langue allemande. Des médias établis comme le « SPIEGEL », le FAZ, DIE WELT, DER STANDART et aussi les journaux suisses NZZ et le TAGES-ANZEIGER, pour n'en citer que quelques-uns, l'ont répété à l'identique – sans l'avoir vérifié le moins du monde. Des politiciens également, comme le sénateur américain Patrick J. Leahy, se sont montrés inquiets : Il s'agit selon eux d'une expérience probablement destinée à couper le réseau d'électricité du pays en plein hiver.

Mais le lendemain, la rectification suivante du rédacteur en chef a paru dans le Washington Post :

« Une première version de cette histoire a prétendu de façon incorrecte que des pirates informatiques russes s'étaient introduits dans le réseau d'électricité américain. Des organismes publics disent qu'il n'y a pas d'indice qui le prouve. L'ordinateur de Burlington Electric n'était pas connecté au réseau. »

Au lieu de « pirates informatiques qui s'étaient introduits dans le réseau électrique américain... » on a dit le lendemain qu'il s'agissait seulement d'un malware russe sur un ordinateur de service du Vermont, ce qui prouverait que le réseau d'électricité américain est menacé.

Mais cette affirmation non plus n'a pas résisté longtemps. Le 3 janvier le Washington Post a annoncé en s'autorisant d'experts et de représentants des organismes publics, que des enquêteurs n'auraient pas trouvés d'indices qui permettent d'imputer l'incident au gouvernement russe. Entre-temps quelques médias principaux de langue allemande – pas tous les médias, loin de là – avaient également relayé cette rectification. Ainsi le quotidien autrichien « Der Standard » a écrit textuellement le 3 janvier :

« Selon le rapport (le plus récent) (du Washington Post) il s'est avéré maintenant qu'un collaborateur de Burlington Electric Department aurait simplement ouvert ses mails Yahoo sur son ordinateur portable. Ceci aurait déclenché l'alarme, parce que le réseau électrique avait reconnu une adresse IP suspecte. De par tout le pays il a également été fait appel à cette adresse supposée défectueuse à de nombreuses reprises. C'est pourquoi les enquêteurs seraient partis du principe que le fournisseur d'électricité n'a pas été la cible de pirates informatiques russes. »

Il semble que les enquêteurs ont trouvé des outils de malware, que des criminels aiment utiliser pour des cyber-attaques, sur l'ordinateur. Mais il n'y avait aucune trace de pirates informatiques russes.

En ce qui concerne le malware, nommé par le ministère pour la sécurité intérieure américaine « Grizzly Steppe », les experts informatiques sont d'accord pour dire que celui-ci serait accessible à tout le monde dans le réseau et pas seulement aux Russes. « The Intercept », un site web d'informations qui travaille avec des journalistes indépendants, a cité un expert en informatique. Celui-ci a comparé l'accusation selon laquelle le malware « Grizzly Steppe » aurait quelque chose à voir avec des Russes, avec l'hypothèse selon laquelle une kalachnikov trouvée sur les lieux d'un crime signifierait que le tueur serait russe. Tout le monde peut se procurer une kalachnikov et en outre dans d'autres Etats il y a un grand nombre de productions sous licence et de copies de kalachnikov.

Cet exemple de prétendus pirates informatiques russes, qui ciblent des objectifs américains, montre clairement une fois de plus :

1. que des informations fausses des médias établis américains comme le Washington Post sont publiées, volontairement ou involontairement, avec beaucoup de légèreté.
2. avec quelle vitesse et quel manque de vérification ces informations fausses en provenance des Etats-Unis sont reprises par les médias principaux européens.

C'est pourquoi on ne peut pas prendre des affirmations passées et également celles à venir au premier degré. Il faudrait plutôt les vérifier minutieusement, et voir si elles ne sont pas à classer parmi les fausses informations ciblées de la guerre d'information contre la Russie.

de s.

Sources:

www.welt.de/politik/article160741870/Russische-Hacker-in-Stromversorger-Netzwerk-eingedrungen.html
www.srf.ch/news/international/trump-preist-putins-reaktion
<http://alles-schallundrauch.blogspot.ch/2017/01/die-medien-verbreiten-wieder-fake-news.html>
<http://derstandard.at/2000050193323/Doch-keine-Spur-nach-Russland-nach-Angriff-aufStromversorger>
<http://www.broeckers.com/2017/01/01/hardware-der-grizzly-steppe-entdeckt/>
<https://deutsch.rt.com/international/44939-washington-post-fakenews-russland/>

Cela pourrait aussi vous intéresser:

Il s'avère que la déclaration du Washington Post sur des hackers russes est une fausse information.

Kla.TV – Des nouvelles alternatives... libres – indépendantes – non censurées...



- ce que les médias ne devraient pas dissimuler...
- peu entendu, du peuple pour le peuple...
- des informations régulières sur www.kla.tv/fr

Ça vaut la peine de rester avec nous!

Vous pouvez vous abonner gratuitement à notre newsletter: www.kla.tv/abo-fr

Avis de sécurité:

Les contre voix sont malheureusement de plus en plus censurées et réprimées. Tant que nous ne nous orientons pas en fonction des intérêts et des idéologies de la système presse, nous devons toujours nous attendre à ce que des prétextes soient recherchés pour bloquer ou supprimer Kla.TV.

Alors mettez-vous dès aujourd'hui en réseau en dehors d'internet!

Cliquez ici: www.kla.tv/vernetzung&lang=fr

Licence:  *Licence Creative Commons avec attribution*

Il est permis de diffuser et d'utiliser notre matériel avec l'attribution! Toutefois, le matériel ne peut pas être utilisé hors contexte. Cependant pour les institutions financées avec la redevance audio-visuelle, ceci n'est autorisé qu'avec notre accord. Des infractions peuvent entraîner des poursuites.