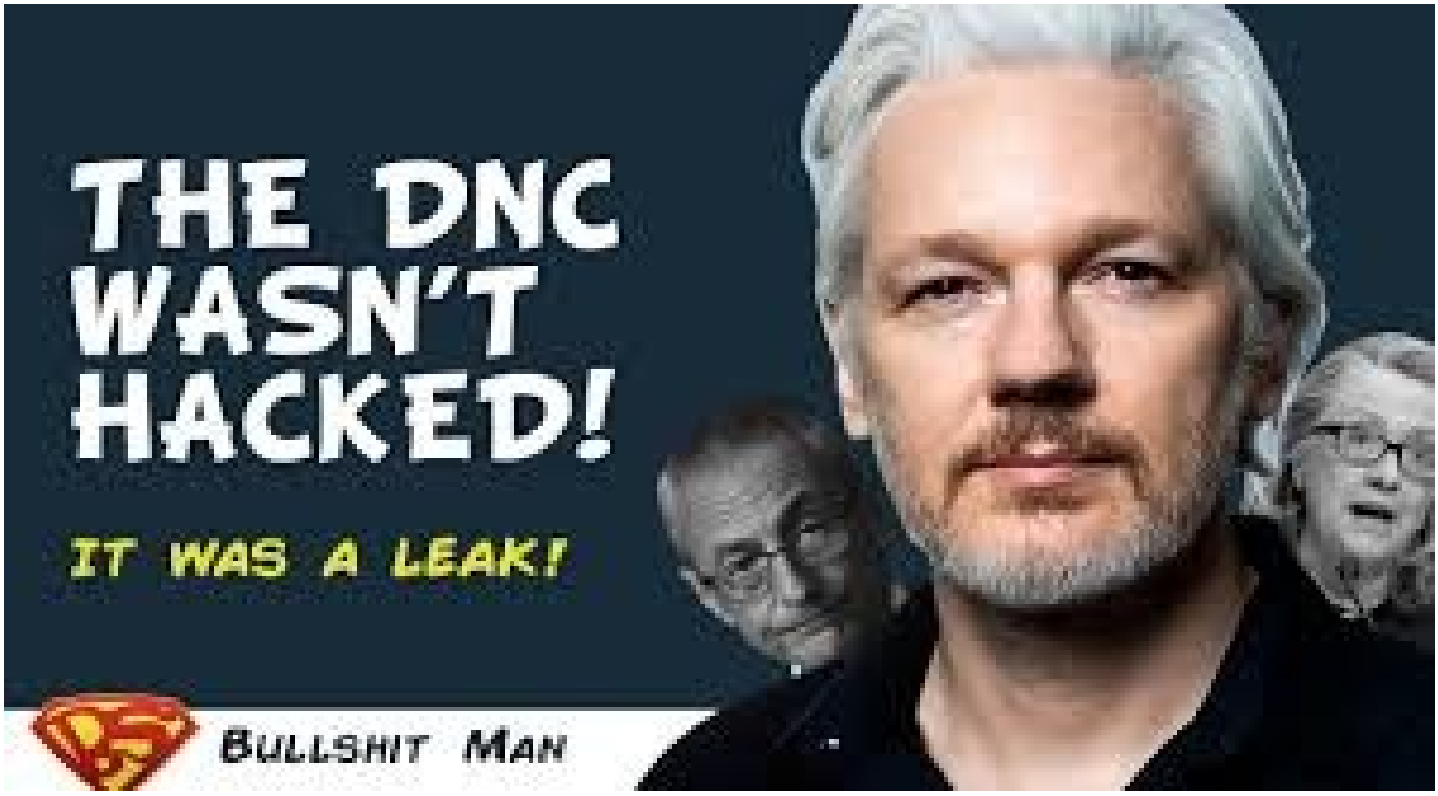
Non, les russes ne sont pas à l'origine du piratage du DNC: voilà pourquoi

par Binney et Johnson [DNC = Comité National Démocrate NdT] .

Par William Binney, ancien directeur technique de la NSA [Agence Nationale de Sécurité NdT]
Larry Johnson, ancien agent du Département d'État, du Contre terrorisme et de la CIA
https://turcopolier.typepad.com/sic_semper_tyrannis/2019/02/why-the-dnc-was-not-hacked-by-the-russians.html

Le FBI, la CIA et la NSA affirment que les courriels du DNC publiés par WIKILEAKS le 26 juillet 2016 ont été obtenus via un piratage russe, mais plus de trois ans après le prétendu "piratage", aucune preuve légale n'a été produite pour étayer cette affirmation. En fait, les preuves disponibles contredisent le communiqué officiel qui attribue la fuite des courriels du DNC à une "intrusion" russe sur Internet. Les preuves existantes plaident pour une autre explication - les fichiers eux même du DNC piratés entre le 23 et le 25 mai 2016 et copiés sur un périphérique de stockage de fichiers, tel qu'une clé USB.



Si les Russes avaient été responsables du piratage du réseau informatique du DNC, les preuves de cette attaque auraient été enregistrées et stockées par la NSA. Les systèmes techniques pour y arriver sont en place depuis 2002. Lorsqu'elle a signé l'"Intelligence Community Assessment" de janvier 2017 concernant l'interférence russe dans l'élection présidentielle de 2016, la NSA a clairement indiqué que les Russes avaient influencé l'élection présidentielle de 2016, si il y avait eu le moindre doute quant au piratage du DNC elle avait l'occasion d'indiquer clairement qu'il y avait des preuves irréfutables.

Nous estimons également que Poutine et le gouvernement russe souhaitaient favoriser l'élection du candidat désigné Trump autant que possible en discréditant la Secrétaire d'État Clinton et en la présentant publiquement de façon défavorable à l'opposé de ce qui se passait pour Trump. Les trois

agences soutiennent cette hypothèse. La CIA et le FBI ont une grande confiance dans ce diagnostic; la NSA une confiance plus modérée.

Dans le milieu du renseignement, l'expression "confiance modérée" veut dire "nous n'avons aucune preuve sérieuse". Grâce aux fuites d'Edward Snowden, nous savons avec certitude que la NSA était tout à fait en capacité d' examiner et analyser les courriels du DNC. Elle a très régulièrement "aspiré" le trafic de courriels transitant par les USA en utilisant des systèmes de collecte tout à fait performants (savoir si quelqu'un de la NSA a choisi ou non de collecter ces données est une toute autre question).

Si ces courriels avaient été piratés depuis internet, la NSA aurait également été en mesure de suivre le chemin électronique emprunté. Ce type de données aurait permis à la NSA de déclarer sans ambiguïté ni restriction que les Russes sont coupables.Cela aurait pu se faire par un document non confidentiel sans compromettre les sources et les méthodes. Au lieu de cela, la NSA a prétendu n'avoir qu'une confiance modérée dans l'affirmation d'ingérence russe. Si la NSA disposait d'informations solides à l'appui de son verdict, la conclusion aurait été présentée comme de "totale confiance".

Nous pensons que le conseiller spécial Robert Mueller risque d'être extrêmement embarrassé s'il décide, pour le piratage du DNC, de persévérer dans ses poursuites contre 12 militaires Russes du GRU [service de renseignement militaire de la Russie NdT].ainsi que d'une entité nommée Guccifer 2.0 - car les preuves légales indiquent que les mails ont été copiés sur un système de stockage.

Selon un communiqué de presse du Département de la Justice concernant l'inculpation des Russes, Mueller estime que les mails ont été obtenus grâce à une attaque de type "hameçonnage" [Spearfishing : technique de fraude sur Internet visant à obtenir des renseignements confidentiels (mot de passe, informations bancaires…) afin d'usurper l'identité de la victime NdT].

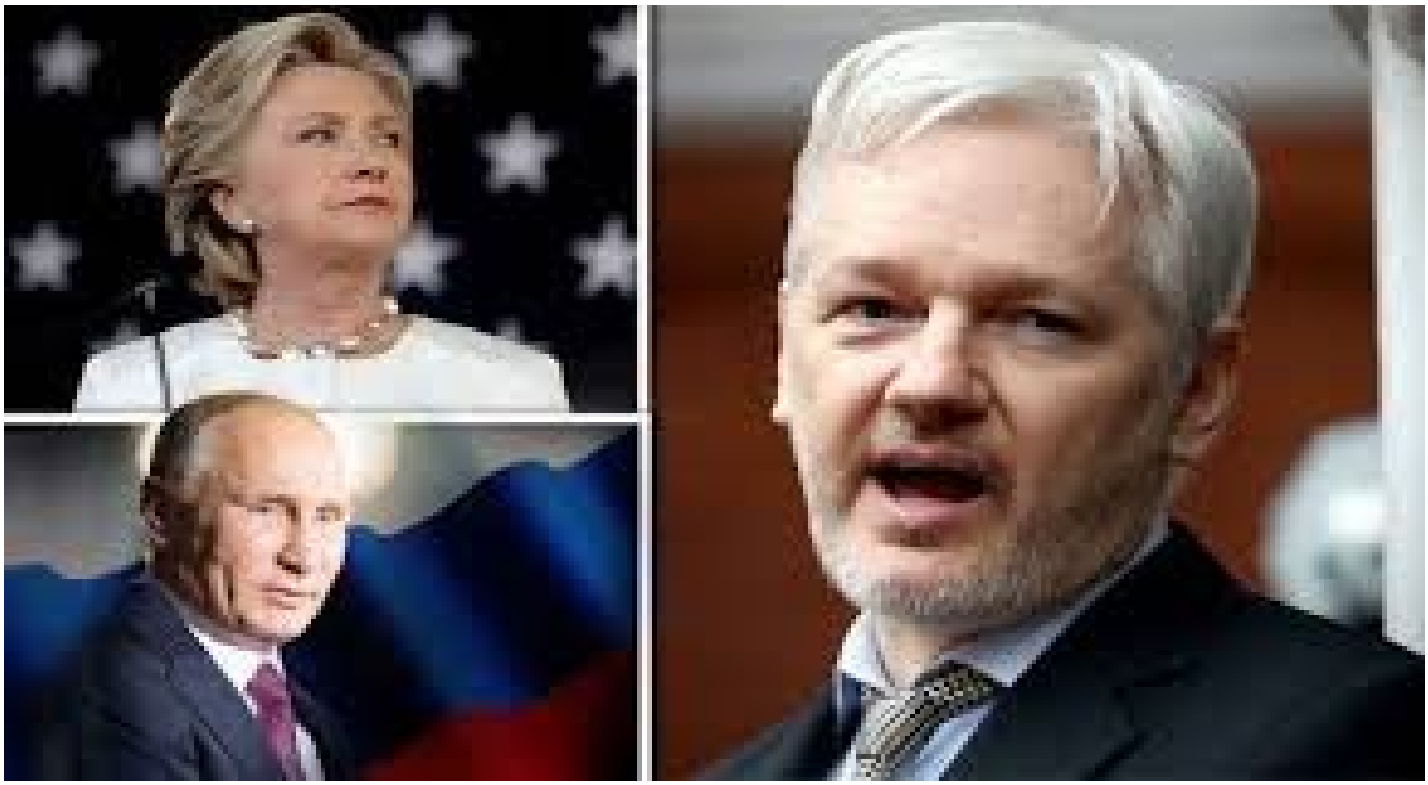
En 2016, les responsables de l'unité 26165 ont commencé à harceler les volontaires et les employés de la campagne présidentielle d'Hillary Clinton, y compris le président de cette campagne. C'est ce processus qui a permis aux fonctionnaires de cette unité de voler les noms d'utilisateur et les mots de passe de nombreuses personnes afin d'utiliser ces informations d'identification pour voler le contenu des courriels et pirater d'autres ordinateurs.

Ils ont également pu pirater les réseaux informatiques du Democratic Congressional Campaign Committee (DCCC)[Comité de campagne démocrate pour le Congrès NdT] et du Democratic National Committee (DNC) en utilisant ces techniques de hameçonnage pour voler des courriels et des documents, surveiller secrètement l'activité informatique de dizaines d'employés et implanter des centaines de fichiers malveillants de code informatique pour voler des mots de passe et conserver l'accès à ces réseaux.

Les responsables de l'unité 26165 et ceux de l'unité 74455 ont conjugué leurs efforts pour planifier la divulgation des documents volés afin d'interférer avec l'élection présidentielle de 2016. Les inculpés ont enregistré le domaine DCLeaks.com et ont par la suite utilisé théâtralement ce site web pour publier des milliers de courriels et de documents volés. Sur ce site, ils prétendaient être des "hacktivistes américains" et utilisaient des comptes Facebook aux noms fictifs et des comptes Twitter pour le promouvoir.

Suite aux accusations publiques visant le gouvernement russe quand au piratage des ordinateurs DNC et DCCC, les accusés ont créé le personnage fictif de Guccifer 2.0. Afin de saper les allégations de participation russe, le soir du 15 juin 2016, entre 16h19 et 16h56, prétendant être un pirate roumain isolé responsable des piratages, les accusés ont utilisé leur serveur basé à Moscou

pour effectuer une recherche de mots et de phrases en anglais, le résultat de ces recherches est apparu plus tard dans le premier billet du blog de Guccifer 2.0.(https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election)



Craig Murray, qui travaille maintenant avec Julian Assange, Hillary Clinton, Vladimir Poutine

En dépit du communiqué de presse du Ministère de la Justice, l'examen des fichiers DNC de Wikileaks ne corrobore pas l'affirmation selon laquelle les courriels auraient été obtenus par hameçonnage.

Au lieu de cela, les preuves montrent très clairement que les courriels affichés sur le site Wikileaks ont été copiés sur un support électronique, tel qu'un CD-ROM ou un disque dur, avant d'être affichés sur Wikileaks. Les courriels affichés sur Wikileaks ont été sauvegardés à l'aide de l'architecture du système de fichiers informatique File Allocation Table (alias FAT) [système de fichiers devenu un standard de l'industrie NdT].

Un examen des fichiers DNC de Wikileaks montre qu'ils ont été créés les 23, 25 et 26 mai respectivement. Le fait qu'ils apparaissent dans un format de système FAT indique que les données ont été transférées à un dispositif de stockage, tel qu'une clef USB.

Comment on sait ça ? On trouve la vérité dans la chronologie de "dernière modification" des fichiers Wikileaks. Chacun des derniers chiffres de ces données est pair. Si on n'est pas familier avec le système de fichiers FAT, il faut savoir que lorsqu'une date est stockée dans ce système, les données arrondissent l'heure à la seconde paire la plus proche.

500 fichiers de courriels DNC stockés sur Wikileaks ont été examinés et tous se terminent par un chiffre pair - 2, 4, 6, 8 ou 0. Si un système autre que FAT avait été utilisé, il y aurait une probabilité égale que la chronologie se termine par un chiffre impair. Mais ce n'est pas le cas en ce qui concerne les données stockées sur le site Wikileaks qui toutes se terminent par un chiffre pair.

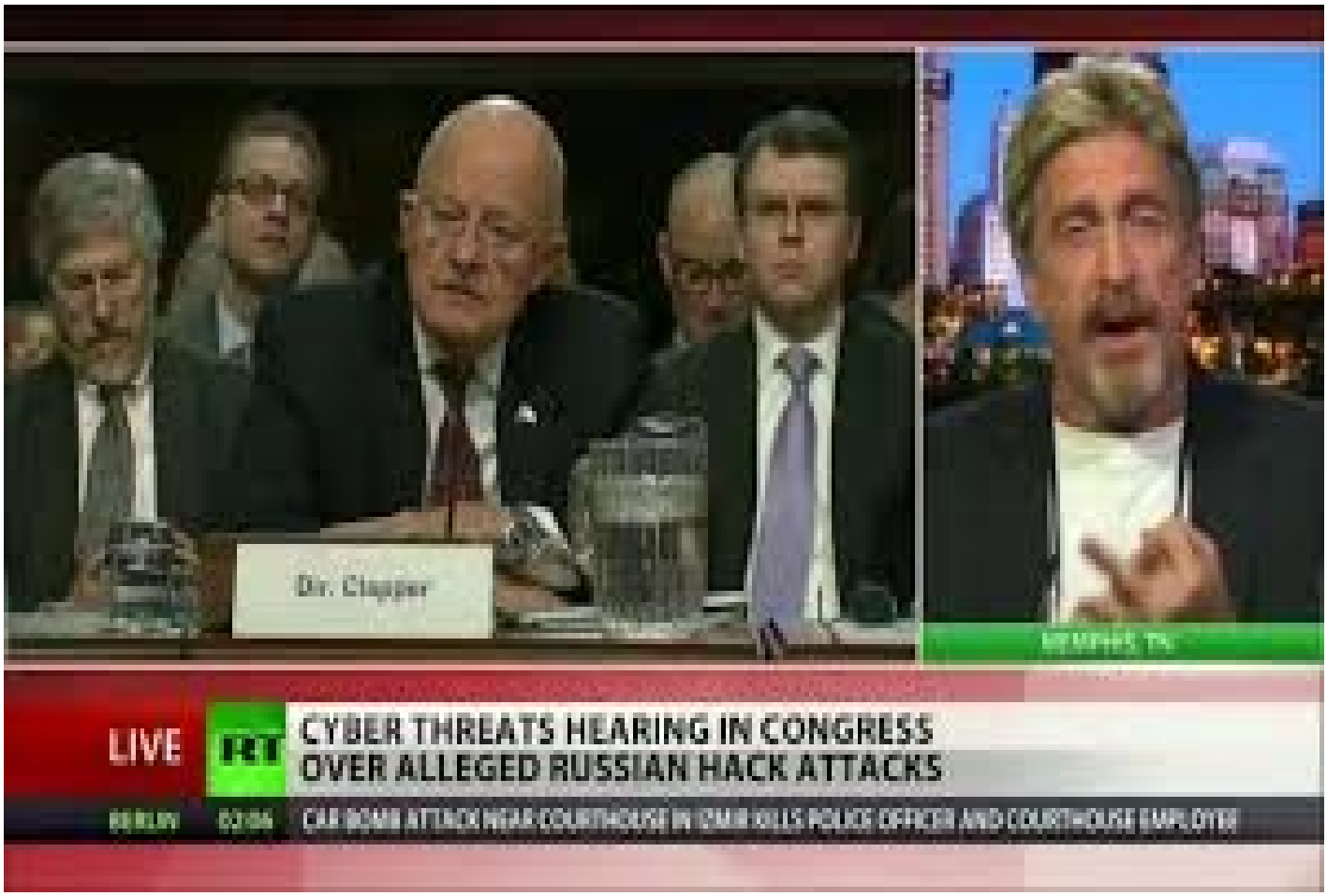
Les emails de la DNC se répartissent en trois séries (heures GMT)

Date	Count	Min Time	Max Time FAT	Min Id Max Id
2016-05-23	10520	02:12:38	02:45:42 x 3800	14319
2016-05-25	11936	05:21:30	06:04:36 x 1	22456
2016-08-26	13357	14:11:36	20:06:04 x 22457	44053

La probabilité statistique qu'un autre système que FAT ait été utilisé est de 1 chance sur 2 à la puissance 500 ce qui est à peu près 1 chance sur 10 à la puissance 150 - en d'autres termes, une chance infinitésimale.

Ce résultat ne prouve pas que les enregistrements aient été faits au quartier général de la DNC. Cependant cela prouve que les données et courriels postés sur Wikileaks sont passés par un périphérique de stockage comme une clef USB avant que Wikileaks n'affiche les courriels sur la toile internet.

Ce seul fait suffit à soulever des doutes raisonnables sur l'acte d'accusation de Mueller à l'encontre de 12 soldats russes éventuels coupables de la fuite des e-mails du DNC sur Wikileaks. Un avocat de la défense astucieux soutiendra, et à juste titre, que quelqu'un a copié les fichiers DNC sur un périphérique de stockage (par exemple, une clé USB) et les a transférés à Wikileaks.



Une autre hypothèse a été tentée : par une comparaison des fichiers de courriels DNC avec les courriels Podesta (alias fichier Larter) publiés le 21 septembre 2016, était-il possible à Wikileaks de manipuler ces fichiers pour générer un résultat FAT ? Le format de fichier FAT n'est PAS utilisé dans

les fichiers Podesta. Si Wikileaks a utilisé un protocole standard pour le traitement des données/emails reçus de sources inconnues, on devrait s'attendre à trouver une structure similaire pour les fichiers/ emails DNC et celle des courriels Podesta. Or, ce n'est pas le cas, les preuves sont là.

D'autres preuves techniques convaincantes viennent contredire l'allégation selon laquelle les courriels DNC proviendraient d'une attaque par hameçonnage. Bill Binney, ancien directeur technique de l'Agence Nationale de Sécurité ainsi que d'autres ex-experts du Renseignement ont examiné les mails posté par Guccifer 2.0 et découvert qu'ils n'ont pas pu être téléchargés depuis le net suite à un hameçonnage. C'est une simple affaire de mathématiques et de physique.

C'est peu après que Wikileaks ait annoncé qu'il avait reçu les courriels du DNC que Guccifer 2.0 est apparu sur la scène publique, affirmant qu'"il" avait piraté le DNC et qu'il avait les courriels du DNC. Fin juin 2016, Guccifer 2.0 a commencé à publier des documents prouvant qu'"il" avait piraté le DNC.

Prenant Guccifer 2.0 au pied de la lettre - c'est-à-dire que ses documents ont été obtenus par une attaque sur Internet - Bill Binney a procédé à un examen légal des métadonnées de ces documents affichés en fonction de la vitesse de connexion Internet aux États-Unis. Cette analyse a montré que le taux de transfert le plus élevé était de 49,1 mégaoctets par seconde, ce qui est bien plus rapide que n'importe quelle connexion à distance. La vitesse de 49,1 mégaoctets correspond à la vitesse de téléchargement d'une clé USB.

M. Binney, assisté par d'autres collègues ayant une expertise technique, est allé plus loin et a effectué divers tests depuis les Pays-Bas, l'Albanie, Belgrade et le Royaume-Uni. Le débit le plus rapide obtenu - depuis un centre de données du New Jersey vers un centre de données au Royaume-Uni - a été de 12 mégaoctets par seconde, moins du quart du débit nécessaire pour transférer les données, tel qu' indiqué par Guccifer 2.

Les conclusions de l'examen des données de Guccifer 2.0 et de Wikileaks ne nous donnent pas l'identité de la personne qui a copié l'information sur la clef USB, mais elles offrent une explication empirique alternative qui vient mettre à mal l'affirmation du Conseiller Spécial selon laquelle le DNC a été piraté. Selon les preuves légales concernant les données de Guccifer 2.0, les courriels du DNC n'ont pas été obtenus depuis internet par une attaque de hameçonnage. C'est localement que la violation des données s'est produite. Il s'agit d'une copie depuis le réseau.

D'autres preuves circonstancielles viennent corroborer cette conclusion. L' atteinte à la protection des données a été une manœuvre locale de copie de données.

Tout d''abord, il y a l'information Top Secret divulguée par Edward Snowden. Si les courriels DNC avaient été piratés par hameçonnage (comme le prétend Mueller), la NSA aurait saisi les données grâce au programme Upstream (Fairview, Stormbrew, Blarney, Oakstar) et les preuves scientifiques n'auraient pas modifié les heures - les données seraient présentées telles qu'envoyées.

Nous avons également les rapports publics sur le DNC et Crowdstrike, et là, on obtient une chronologie bizarre pour un piratage présumé russe.

Le 29 avril 2016, le DNC prétend avoir eu connaissance du piratage de ses serveurs. (https://medium.com/homefront-rising/dumbstruck-how-crowdstrike-conned-america-on-the-hack-of-the-dnc-ecfa522ff44f). Aucune déclaration sur d'éventuels responsables à ce stade.

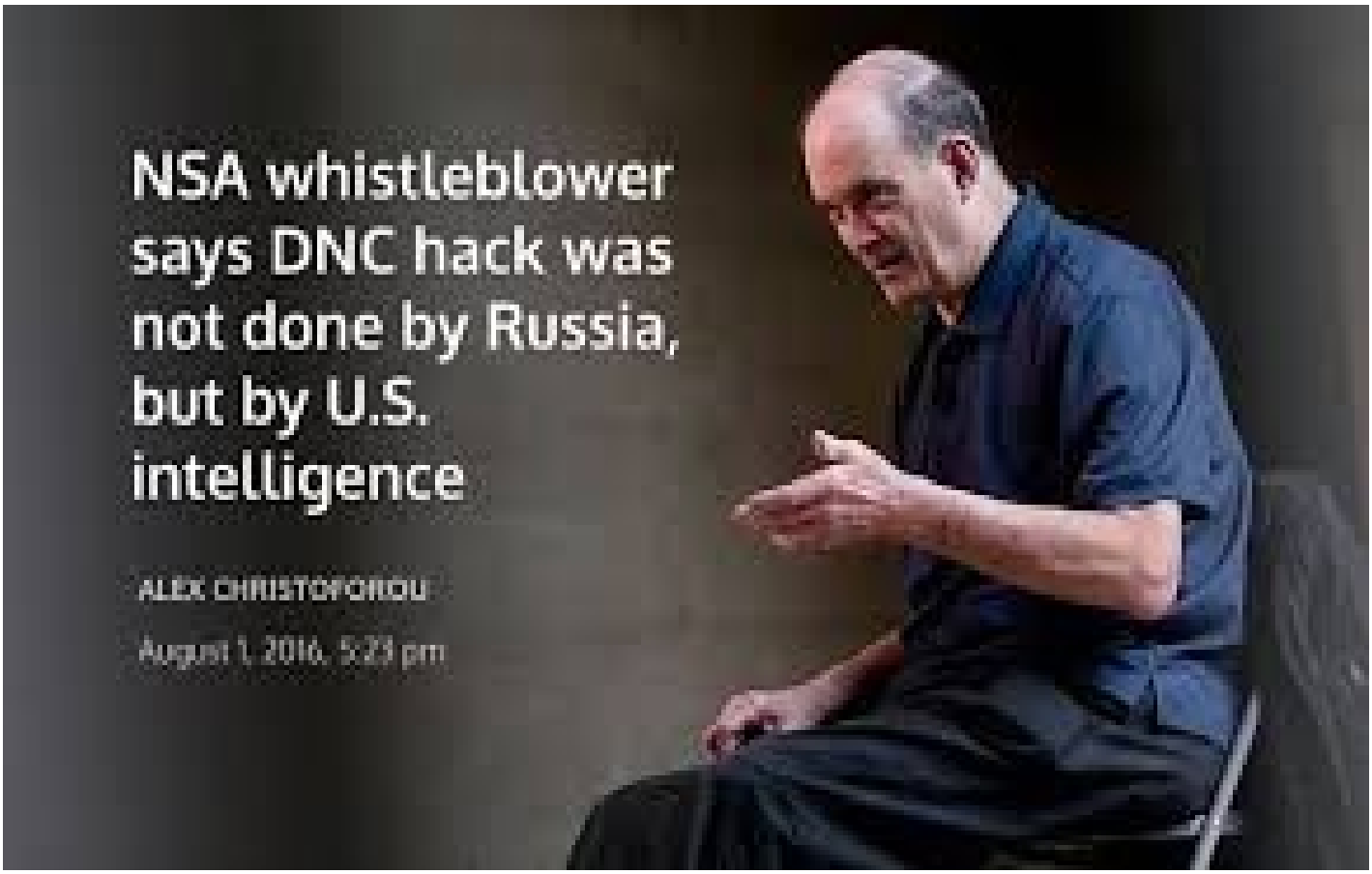
Selon le fondateur de CrowdStrike, Dimitri Alperovitch, c'est le 6 mai 2016 que sa société a détecté

pour la première fois la présence des Russes à l'intérieur du serveur DNC. Un analyste du renseignement de CrowdStrike aurait dit à Alperovitch :

Ce n'est pas un, mais deux intrus russes qui ont été identifiés par Falcon : Cozy Bear, un groupe d'experts affiliés au FSB selon CrowdStrike, la réponse de la Russie à la CIA ; et Fancy Bear, associé au GRU, le renseignement militaire russe.[Le FSB ou Service fédéral de sécurité de la fédération de Russie est un service secret de la Russie, chargé des affaires de sécurité intérieure, successeur du KGB NdT] (https://www.esquire.com/news-politics/a49902/the-russian-emigre-leading-the-fight-to-protect-america/)

Et quelle a été la réponse de CrowdStrike ? Rien, aucune réponse. Pour Michael Isikoff : Selon CrowdStrike, ce manque de réaction entrait dans un plan délibéré afin d'éviter d'avertir les Russes qu'ils avaient été "découverts". C'est n'importe quoi. Si une entreprise de sécurité découvrait qu'un voleur est entré par effraction dans une maison et l'avait cambriolée, quelle entreprise saine d'esprit conseillerait au client de ne rien faire pour éviter d'alerter le voleur ?

L'examen des données Wikileaks nous donnent la preuve que le dernier message copié depuis le réseau DNC date du mercredi 25 mai 2016 à 08:48:35. Aucun courriel du DNC n'a été envoyé à Wikileaks après cette date.



Un lanceur d'alerte de la NSA l'affirme: le piratage du Comité du Parti Démocrate n'était pas le fait de la Russie mais du renseignement américain Alex Christoforou

CrowdStrike a attendu le 10 juin 2016 pour prendre des mesures concrètes afin de nettoyer le réseau DNC. Alperovithc a déclaré à Vicky Ward d'Esquire que : «Finalement, les équipes ont décidé qu'il fallait remplacer les logiciels de chaque ordinateur DNC. Le secret était crucial jusqu'à ce que le réseau soit propre. Dans l'après-midi du vendredi 10 juin, tous les employés du DNC ont reçu l'ordre de laisser leurs ordinateurs portables au bureau.» https://www.esquire.com/news-

politics/a49902/the-russian-emigre-leading-the-fight-to-protect-america/

Pourquoi une société de cybersécurité attend-elle 45 jours après avoir prétendument découvert une attaque massive de la Russie contre le serveur DNC pour prendre des mesures concrètes afin de protéger l'intégrité des informations sur ce serveur ? Cela n'a aucun sens.

Il est beaucoup plus vraisemblable qu'on savait que les mails avaient été chargés et copiés depuis les serveurs sur une clé USB. Par contre le responsable du piratage n'avait pas encore été identifié. Par contre il y a une chose dont on est sûr - ce n'est que 18 jours après que le dernier courriel ait été copié depuis le serveur que CrowdStrike a pris des mesures pour fermer et réparer le réseau DNC.

Finalement, le plus curieux est qu'à aucun moment le DNC n'a fourni l'accès de ses serveurs au FBI dont les techniciens qualifiés auraient pu faire un examen légal complet. S'il s'était agi d'un véritable piratage via Internet, la NSA aurait très facilement pu identifier le moment du vol de l'information et l'itinéraire suivi après le piratage depuis le serveur.

La NSA avait mis en place des systèmes techniques de collecte permettant aux analystes de savoir la date et l'heure des messages. Mais cela n'a pas été fait.Si on considère la question dans son ensemble, ces points de données disparates se combinent pour brosser un tableau qui disculpe les présumés pirates russes et met en cause des membres de notre communauté policière et du renseignement participant à une campagne de désinformation, de duperie et d'incompétence. Ce n'est pas bien joli.