LES DÉQODEURS
déQodons l'info, ensemble

DÉVOLUTION 6

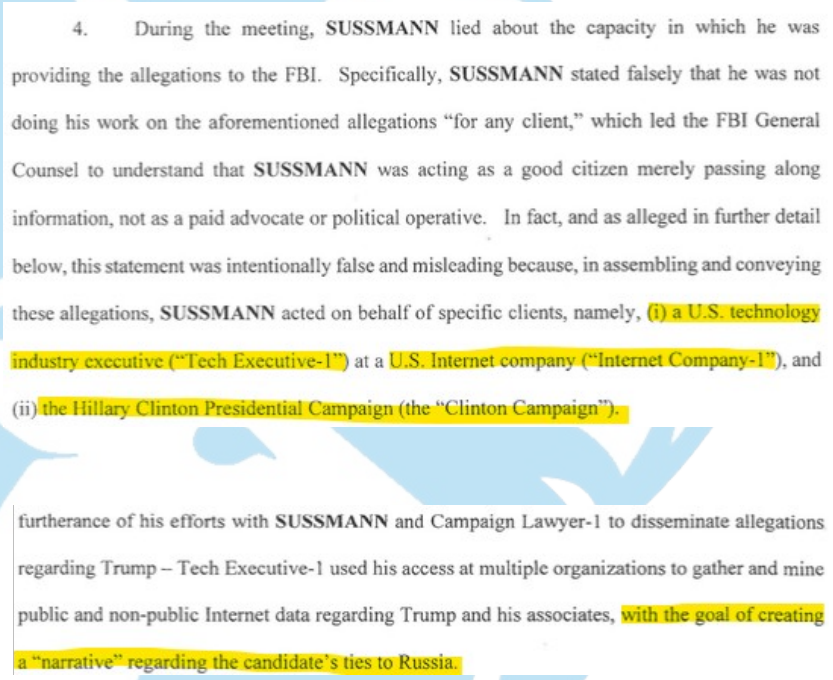
Devolution 11 : CrowdStrike

Petit rappel sur le Spygate :

https://lesdeqodeurs.fr/spygate-obamagate-fisagate-ou-le-plus-gros-scandale-politique-de-lhistoire-americaine/

https://lesdeqodeurs.fr/pilule-rouge-lenquete-durham-obamagate-fisagate-spygate/

Retour sur le rapport Durham :



4. During the meeting, **SUSSMANN** lied about the capacity in which he was providing the allegations to the FBI. Specifically, **SUSSMANN** stated falsely that he was not doing his work on the aforementioned allegations "for any client," which led the FBI General Counsel to understand that **SUSSMANN** was acting as a good citizen merely passing along information, not as a paid advocate or political operative. In fact, and as alleged in further detail below, this statement was intentionally false and misleading because, in assembling and conveying these allegations, **SUSSMANN** acted on behalf of specific clients, namely, (i) a U.S. technology industry executive ("Tech Executive-1") at a U.S. Internet company ("Internet Company-1"), and (ii) the Hillary Clinton Presidential Campaign (the "Clinton Campaign").

furtherance of his efforts with **SUSSMANN** and Campaign Lawyer-1 to disseminate allegations regarding Trump – Tech Executive-1 used his access at multiple organizations to gather and mine public and non-public Internet data regarding Trump and his associates, with the goal of creating a "narrative" regarding the candidate's ties to Russia.

[...]En fait, et comme allégué plus en détail ci-dessous, cette déclaration était intentionnellement fausse et trompeuse car, en rassemblant et en transmettant ces allégations, **SUSSMANN a agi pour le compte de clients spécifiques, à savoir (i) un cadre de l'industrie technologique américaine (« Tech Executive- I *') dans une société Internet américaine (« Internet Company-I »), et (ii) la campagne présidentielle d'Hillary Clinton (la « campagne Clinton »).**

Tech Executive-I a utilisé son accès à de multiples organisations pour recueillir et exploiter des données Internet publiques et non publiques concernant Trump et ses associés **dans le but de créer un « narratif » concernant les liens du candidat avec la Russie.**

Le rapport Durham complet est disponible ici

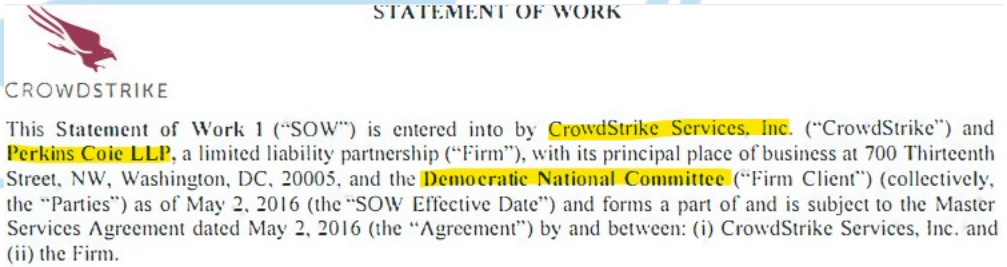
L’hypothèse de Patel Patriot

Tech Executive-1 = **Shawn Henry**

Internet Company-1 = **CrowdStrike**

L’hypothèse de Patel Patriot

Contrat de travail entre Perkins Coie et CrowdStrike :



STATEMENT OF WORK

CROWDSTRIKE

This Statement of Work 1 ("SOW") is entered into by CrowdStrike Services, Inc. ("CrowdStrike") and Perkins Coie LLP, a limited liability partnership ("Firm"), with its principal place of business at 700 Thirteenth Street, NW, Washington, DC, 20005, and the Democratic National Committee ("Firm Client") (collectively, the "Parties") as of May 2, 2016 (the "SOW Effective Date") and forms a part of and is subject to the Master Services Agreement dated May 2, 2016 (the "Agreement") by and between: (i) CrowdStrike Services, Inc. and (ii) the Firm.

Perkins Coie LLP a engagé CrowdStrike pour des services dont avaient besoin le DNC et le DCCC. Sussman et son cabinet d’avocats, Perkins Coie, agissaient essentiellement comme des intermédiaires.

Le rapport Mueller

Le supposé piratage des serveurs du Comité Nationale Démocrate était encore une autre histoire utilisée pour faire avancer le récit selon lequel la Russie s'ingérait activement pour faire élire Donald Trump à la présidence en 2016. **C'était un des éléments essentiels du rapport Mueller.**

- **Des agents du renseignement militaire russe ont piraté et divulgué des documents embarrassants du Parti démocrate,**
- Une équipe de trolls liée au gouvernement russe a orchestré une campagne de médias sociaux sophistiquée et de grande envergure qui a dénigré Hillary Clinton et promu Trump.

Le piratage du DNC

La lecture de cet article de RealClearNews apporte des éléments très intéressants sur la question :

Le rapport [Mueller] affirme [...] :
- ses enquêteurs ne savent pas vraiment avec certitude ***si des agents des services de renseignement russes ont volé des courriels du parti démocrate, ni comment ces courriels ont été transférés à WikiLeaks.***

- Les responsables du renseignement américain ne peuvent pas tirer de conclusions définitives sur le piratage des serveurs informatiques du Comité national démocratique, ***car ils n'ont pas analysé ces serveurs eux-mêmes. Au lieu de cela, ils se sont appuyés sur les analyses de CrowdStrike***

- En outre, ***le gouvernement a autorisé CrowdStrike et le conseiller juridique du parti démocrate à soumettre des documents expurgés****, ce qui signifie que c'est CrowdStrike et non le gouvernement qui a décidé de ce qui pouvait être révélé ou non concernant les preuves de piratage.*

Une chronologie bancale

Selon le rapport Mueller :

- **Mars 2016 :** des agents de la principale agence de renseignement russe, le GRU, ont pénétré dans les courriels du président de la campagne Clinton, John Podesta.

- **Avril 2016**: Ils ont dérobé les identifiants de Podesta et les ont utilisés pour pirater les serveurs du DNC et du DCCC (Democratic Congressional Campaign Committee).

- **Juin 2016:** le GRU créé deux avatars en ligne, « DCLeaks » et « Guccifer 2.0 » pour commencer à diffuser les documents volés. Plus tard, Guccifer 2.0 aurait transmis les documents à Wikileaks. Le rapport Mueller indique la date du **14 juin** pour le premier contact supposé entre Assange et les «hackers russes ».

- **22 juillet 2016** : Wikileaks publie le premier lot de documents avant la Convention Nationale Démocrate.

Une chronologie bancale

Selon Mueller, Wikileaks aurait eu son premier contact avec les hackers DCLeaks et Guccifer 2.0 en date du **14 juin** 2016. Or, le **12 juin** 2016, Assange faisait la déclaration suivante (source):

Julian Assange

This article is more than 5 years old

WikiLeaks to publish more Hillary Clinton emails - Julian Assange

New release likely to fan controversy and provide further ammunition for Republican presidential rival Donald Trump

Mark Tran

@marktran

Sun 12 Jun 2016 15.50 BST

Julian Assange says it was unlikely the US attorney general would indict Clinton. Photograph: Dominic Lipinski/PA

« Julian Assange, le fondateur de WikiLeaks, a déclaré que son organisation s'apprêtait à publier davantage d'e-mails envoyés et reçus par Hillary Clinton lorsqu'elle était secrétaire d'État américaine. »

Ce qu'en dit Assange

Il est intéressant de constater que Mueller n'a jamais accepté d'entendre les déclarations d'Assange dans cette affaire, alors qu'il est LE témoin principal sur le piratage du DNC (**source**) :
Nous avons également reproché à Mueller ***de ne pas avoir interrogé des témoins volontaires ayant une connaissance directe de la situation, comme Julian Assange de WikiLeaks.***

Qui plus est, dés 2017, Assange affirmait que les documents du DNC ne lui étaient pas parvenus par le biais du gouvernement russe (source)

AFP

Assange hits back after US intelligence hack report

Le fondateur de WikiLeaks, Julian Assange, a insisté lundi sur le fait que les fuites de documents du parti démocrate publiées avant l'élection présidentielle américaine ne provenaient pas du gouvernement russe.

Focus sur Crowdstrike

Le FBI n'a jamais eu accès aux serveurs du DNC

- "Nous n'avons jamais eu un accès direct aux machines elles-mêmes", a déclaré M. Comey, ajoutant que la société que le DNC a engagée [CrowdStrike] *pour examiner les données forensiques a transmis ces informations au FBI vers le mois de juin de l'année dernière. (source)*

- M. Comey a souligné sa confiance dans les informations fournies par CrowdStrike, qu'il a qualifiée de « société privée très respectée » et d' « entité de haut niveau ».(source)

CrowdStrike ment et doit se rétracter

Quelques jours après le témoignage de Comey, CrowdStrike a été contraint de retirer son affirmation selon laquelle un logiciel russe avait été utilisé pour pirater du matériel militaire ukrainien. L'erreur de CrowdStrike est d'autant plus pertinente qu'elle avait accusé le GRU d'avoir utilisé ce même logiciel pour pirater le DNC.*(source)*

Focus sur Crowdstrike

Shawn Henry, cadre de CrowdStrike, qui a dirigé l'équipe d'experts qui a fini par imputer la responsabilité de la violation du DNC à la Russie, a été **directeur adjoint du FBI sous la direction de Mueller**. (source)

Dmitri Alperovitch, est un membre senior non résident de l'Atlantic Council, le principal groupe de réflexion de Washington qui promeut agressivement une attitude belliciste envers la Russie.(source)

Dmitri Alperovitch, executive chairman at Silverado Policy Accelerator and co-founder of CrowdStrike, **Katie Nickels,** director of intelligence at Red Canary and nonresident senior fellow at the Atlantic Council's Cyber Statecraft Initiative, **Matthew Rojansky**, director of the Wilson Center's Kennan Institute, and **Dr. Louise Shelley,**

Résumons...

- Liens avérés entre CrowdStrike et Perkins Coie
- Informations expurgées par CrowdStrike sans supervision gouvernementale
- Une chronologie étrange
- Mueller refuse d'interroger Assange
- Le rapport Mueller emploie des conditionnels qui interrogent :

«Les agents de l'unité 26165 semblent avoir volé des milliers d'emails et de pièces jointes, qui ont ensuite été publiés par WikiLeaks en juillet 2016 »

Unit 26165 officers appear to have stolen thousands of emails and attachments, which were later released by WikiLeaks in July 2016.[136]

- Assange nie que les documents viennent de Russie
- Les serveurs du DNC ne seront jamais examinés par le FBI, seulement par CrowdStrike
- Gigantesque conflit d'intérêt entre CrowdStrike et Mueller

Résumons...

- Shawn Henry déclare **sous serment, devant le congrès** en 2020 au sujet du piratage du DNC : *Il n'y a pas de preuve qu'ils [NDLR :les documents du DNC] ont été réellement exfiltrés. Il y a des preuves circonstancielles mais aucune preuve qu'elles ont été réellement exfiltrées.*(source)

-Bill Binney, ancien directeur technique de la NSA déclare (source):

« *S'il s'agissait vraiment d'un piratage interne,* ***la NSA pourrait facilement nous dire quand les informations ont été prises et le chemin qu'elles ont emprunté après avoir été retirées du serveur du DNC*** *». Mais compte tenu des réserves émises par M. Mueller et de l'utilisation répétée de l'expression « vers le ou autour du » au lieu d'indiquer des dates précises, à la seconde près, que la NSA pourrait fournir, M. Binney doute que les renseignements de la NSA aient été inclus dans l'acte d'accusation et le rapport du GRU.*

- Bill Binney déclare également sous serment : « *Les principales conclusions indiquent que les données du DNC ont été copiées* ***sur un dispositif de stockage à une vitesse qui dépasse de loin la capacité d'Internet pour un piratage à distance****. Il est tout aussi important de savoir que la copie et le traitement ont été effectués sur la côte Est des États-Unis. ».* L'enquête Mueller a complètement écarté cette possibilité

Seth Rich

La déclaration de Binney selon laquelle les données du DNC pourraient avoir été dérobées sur une clé USB et non sur Internet renvoie directement au meurtre de Seth Rich. Des «théories » prétendent qu'il serait à l'origine de la fuite d'information du DNC :

- Il travaillait au DNC(source)
- Il a été assassiné 5 jours après le hack du DNC
- La police a conclut à une tentative de vol, mais ni son portefeuille, ni son téléphone, ni sa montre n'ont été dérobés
- Julian Assange a offert 20000$ de récompenses pour des informations sur sa mort
- Assange a également laissé ici entendre que Rich pourrait être une source.

Annonce : Wikileaks a décidé d'offrir une récompense de 20 000 dollars pour toute information menant à une condamnation pour le meurtre de Set Rich, membre du personnel du DNC.

Seth Rich

Et par hasard, très certainement, on apprend que le laptop professionnel de Seth Rich, lorsqu'il travaillait au DNC a été fourni au FBI par nul autre que… **Michael Sussmann**

[redacted]

b6 -1
b7C -

From: [redacted]
Sent: Tuesday, June 26, 2018 10:24 AM
To: LRA
Cc: JSR
Subject: Seth Rich work laptop

b6 -1, -4
b7C -1, -4
b7D -3
b7E -6

Rush,
In May 2017 [redacted] with Perkins Coie provided San Francisco FBI with a copy of Seth Rich's DNC laptop.
The FBI submission document says the laptop was given to the FBI voluntarily so I am assuming that there is no Search Warrant for the laptop.

San Francisco provided [redacted] for us at SCO. [redacted]

[redacted]

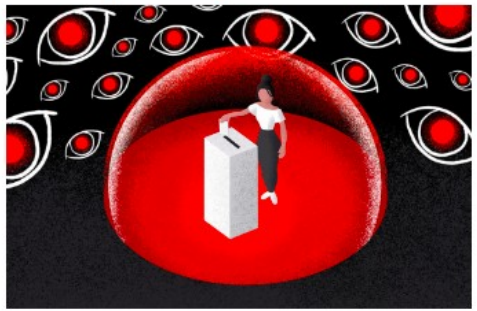
Thank you,
[redacted]

CrowdStrike et les élections

CROWDSTRIKE | BLOG

Securing Elections Globally: How CrowdStrike Is Helping

July 30, 2020 Shawn Henry Executive Viewpoint

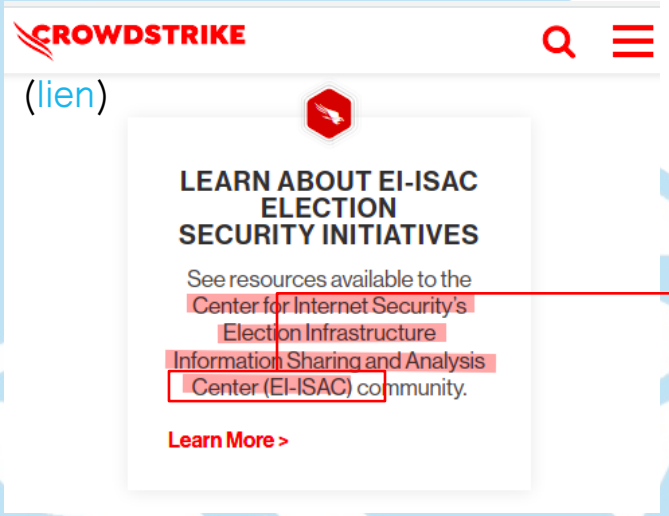


(source)

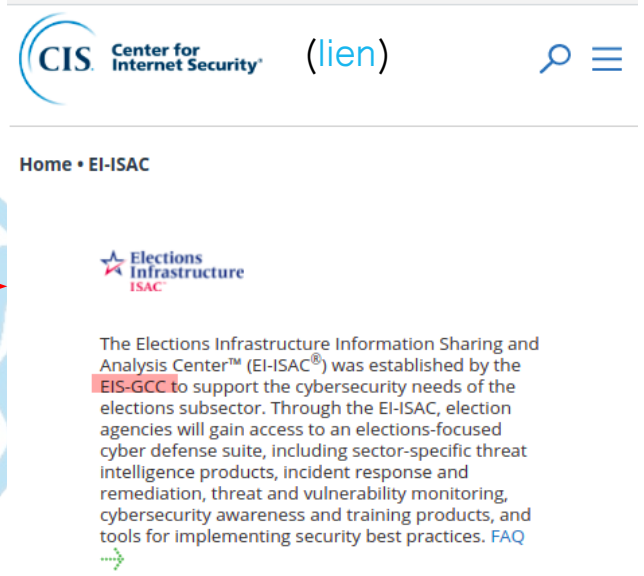
***En tant que leader mondial de la protection des élections**, nous souhaitons expliquer notre point de vue sur les questions de sécurité électorale et partager quelques ressources avec la communauté électorale. **Les élections libres et équitables sont la pierre angulaire des démocraties partout dans le monde, et elles sont de plus en plus menacées par des adversaires étrangers qui cherchent à manipuler ou à saper leurs processus ou leurs résultats**. Nous pensons que ceux qui sont en mesure de contribuer à la sécurité des élections ont la responsabilité de le faire, et dans cet esprit, nous sommes ravis de lancer un nouveau site web dédié à l'expertise, aux conseils et au soutien.[...]*

*À cette fin, nous annonçons aujourd'hui **le lancement du centre de ressources CrowdStrike sur la cybersécurité et la sécurité des élections**. Ce site met en évidence certaines des entités avec lesquelles nous nous sommes associés et les programmes que nous soutenons,[...]*

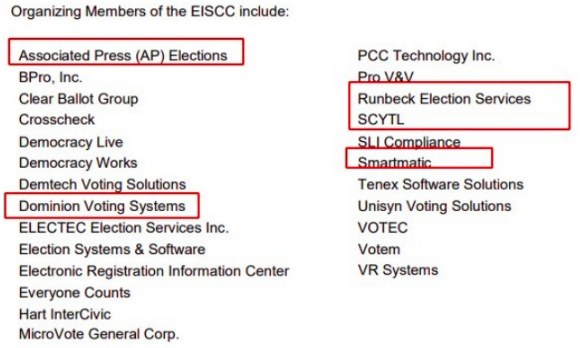
CrowdStrike et les élections



(lien)



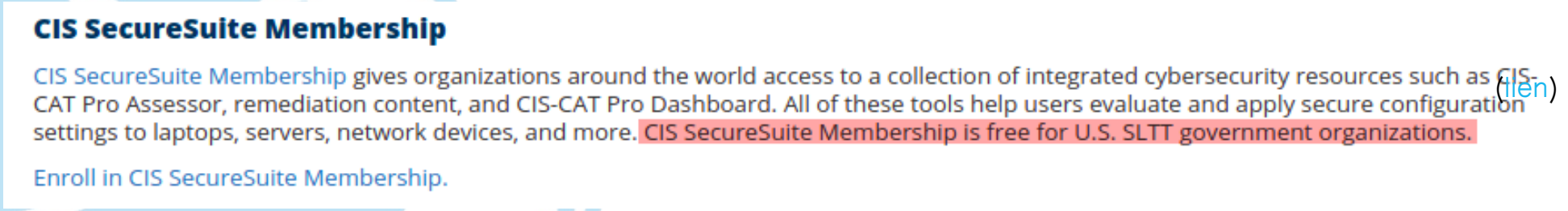
(lien)



L'EIS-GCC est le nouveau nom de l'EISCC dont on a parlé dans Dévolution 2 (ici et ici slide 8 et suivants)

Donc l'EI-ISAC a été créé par l'EIS-GCC pour « soutenir les besoins en cybersécurité du sous-secteur des élections ». Le même conseil dont Dominion Voting Systems était membre a créé l'EI-ISAC. CrowdStrike s'est associé à l'EI-ISAC et lui fournit des **ressources**. De quelles ressources est-il question?

CrowdStrike et les élections



CIS SecureSuite Membership

CIS SecureSuite Membership gives organizations around the world access to a collection of integrated cybersecurity resources such as CIS-CAT Pro Assessor, remediation content, and CIS-CAT Pro Dashboard. All of these tools help users evaluate and apply secure configuration settings to laptops, servers, network devices, and more. CIS SecureSuite Membership is free for U.S. SLTT government organizations.

Enroll in CIS SecureSuite Membership.

(lien)

L'adhésion à CIS SecureSuite est gratuite pour les organisations gouvernementales américaines SLTT (NDT : collectivités locales, des tribus et des territoires).

Pour votre édification personnelle, je vous invite à cliquer sur ce lien pour voir la liste des organisations adhérant à l'EI-ISAC. (Sur cette page seule, il y a plus de 1000 occurrences du terme « election »)

Conclusion sur CrowdStrike

Vous voyez maintenant où je veux en venir. Notre gouvernement fédéral a passé un contrat avec le **Center for Internet Security** (CIS) pour assurer la cybersécurité de centaines, voire de milliers, d'organisations SLTT américaines. **Le CIS utilise CrowdStrike pour assurer cette cybersécurité** :

- Le même CrowdStrike qui a des liens avec l'administration Obama.
- Le même CrowdStrike qui a menti et couvert le piratage du DNC qui a été l'une des bases de lancement de l'intox Trump-Russie.
- Le même CrowdStrike qui, je crois, a fabriqué les données derrière l'histoire d'Alfa Bank.
- Le produit de cybersécurité de CrowdStrike comprend « un composant téléchargeable en code objet (« composant logiciel »). » Cela signifie que tout État ou gouvernement local qui a utilisé le CIS pour assurer la cybersécurité, a autorisé le logiciel de CrowdStrike à être téléchargé directement dans ses machines et systèmes.

Peut-être que ce n'est que moi, mais je penserais que si un acteur malveillant (comme la Chine) voulait pirater l'ensemble de notre système électoral, y accéder par le biais de quelques entités comme Perkins Coie et CrowdStrike pourrait être le moyen idéal pour le faire.

Malgré une longue liste de conflits d'intérêts au nom de ces deux entités, on a dit à notre nation, à plusieurs reprises, de simplement ignorer ces conflits et de « croire » que rien de néfaste ne s'est produit lors de l'élection de 2020 - alors que CrowdStrike lui-même avait un accès direct aux machines à voter dans tout le pays.