Une grève bondée

À propos de Crowdstrike et des analyses informatiques mal menées

#CrowdStrike #DNC #Clinton #FBI

Les aigles sont des chasseurs incroyablement gracieux. Leur capacité à identifier le moindre animal depuis le ciel est légendaire. Quiconque a eu la chance d'observer un aigle passer en mode attaque et plonger vers le sol avec vélocité et détermination n'oubliera jamais ce spectacle. La coïncidence veut qu'un aigle de ce type fasse partie du logo de Crowdstrike, une entreprise qui fournit des logiciels et des services informatiques dans le domaine de la sécurité des réseaux. L'entreprise a été fondée en 2011 par George Kurtz, ancien directeur technique du fournisseur de sécurité informatique McAfee, et Dimitri Alperovich, expert en sécurité informatique d'origine russe et ancien vice-président de McAfee. En 2012, un ancien fonctionnaire du FBI nommé Shawn Henry a rejoint l'entreprise, et 12 mois plus tard, la société a lancé son premier produit, Crowdstrike Falcon.

Semblable à de véritables faucons, le logiciel a été créé pour surveiller en permanence les réseaux informatiques et leur immense trafic de données à la recherche d'intrus visant à voler des informations sensibles, des adresses IP et bien d'autres choses encore dans ce réseau. Après que l'entreprise a pu identifier un certain nombre d'attaques sur divers réseaux d'entreprises et d'industries prétendument en provenance de Chine, de Corée du Nord et de Russie en 2014 et 2015, Crowdstrike a reçu un financement à grande échelle de Google, totalisant plus de 480 millions de dollars en 2019. L'entreprise a également été évaluée à plus de 3 milliards de dollars en 2018, avec un chiffre d'affaires annuel de seulement 100 millions de dollars, et a été cotée au NASDAQ en 2019.

Lestrois principaux actionnaires actuels de Crowdstrike sont deux grandes sociétés d'investissement de la Silicon Valley et, curieusement, Allianz Asset Management GmbH, basée à Munich, en Allemagne. Crowdstrike a actuellement une capitalisation boursière de plus de 15 milliards de dollars avec un peu plus de 2000 employés, n'a pas de dettes et disposait de plus de 800 millions de dollars de liquidités en octobre 2019 - pas mal pour être "seulement" une société de logiciels.

Au sein de tout ce succès incontesté et fulgurant est apparu un incident plutôt étrange en 2016, lorsque Crowdstrike a publié un rapport fantaisiste et coloré sur la façon dont un groupe russe nommé "Fancy Bear" aurait piraté une application militaire ukrainienne nommée "ArtOS", un logiciel qui peut être installé sur des tablettes PC et qui est utilisé pour le contrôle des tirs "pour faire des ajustements aux conditions de tir des systèmes balistiques et météorologiques", selon le développeur de l'application, Yaroslav Sherstuk. Crowdstrike a fait un certain nombre d'évaluations politiques de haut niveau et a affirmé que l'armée ukrainienne avait subi de "lourdes pertes" au niveau de l'artillerie, principalement à cause du piratage russe.

> Au cours de la période de développement proposée, un certain nombre d'événements importants se sont produits entre l'Ukraine, la Russie et la communauté internationale. Les tentatives russes d'influencer les relations entre l'Ukraine et l'Union européenne ont notamment débouché sur le mouvement de protestation à grande échelle Maidan, qui a finalement abouti à l'éviction du président de l'époque, Victor Yanukovich, à l'invasion et à l'annexion de la péninsule de Crimée par la Russie et au conflit armé prolongé dans l'est de l'Ukraine. Par conséquent, la création d'une application [App] ciblant certaines des forces de première ligne essentielles à la défense de l'Ukraine sur le front oriental serait

> probablement une priorité pour les développeurs de logiciels malveillants de l'adversaire russe qui cherchent à renverser le cours du conflit en leur faveur [...]. Pour les troupes ukrainiennes, les forces d'artillerie ont également payé un lourd tribut...
>
> (Rapport Crowdstrike "Use of Fancy Bear and Android malware in tracking of Ukrainian field artillery units"(Utilisation de Fancy Bear et de logiciels malveillants Android dans le suivi des unités d'artillerie de campagne ukrainiennes))

Curieusement, les principales conclusions de Crowdstrike ont été rapidement rejetées. Par exemple, l'Institut international d'études stratégiques (IISS), qui a émis la déclaration suivante:

> Le rapport Crowdstrike utilise nos données, mais les conclusions et l'analyse tirées de ces données appartiennent exclusivement aux auteurs du rapport. L'inférence qu'ils font selon laquelle les réductions des stocks d'artillerie D-30 ukrainiens entre 2013 et 2016 étaient principalement le résultat de pertes au combat n'est pas une conclusion que nous avons suggérée nous-mêmes, ni une conclusion que nous croyons être exacte.
>
> (Déclaration de l'IISS de 2017)

Un autre chercheur de l'IISS a déclaré que la réduction des unités militaires était principalement attribuée à une réaffectation de ses unités à d'autres commandements militaires. L'armée ukrainienne a indiqué que les pertes d'artillerie dues aux combats d'ongiong avec les séparatistes étaient "plusieurs fois inférieures au nombre rapporté par Crowdstrike et ne sont pas associées à la cause spécifique" du piratage. Le développeur de l'application a fait une déclaration sur les conclusions de Crowdstrike concernant l'Ukraine sur Facebook, les qualifiant de "délirantes". Il a toutefois admis que ses courriels avaient été compromis.

Il est également intéressant de noter qu'un haut fonctionnaire américain a expliqué lors d'une conférence au Danemark en 2018 comment les États-Unis continuaient à soutenir explicitement les efforts de cybersécurité de l'Ukraine avec un total de 10 millions de dollars - que l'on est presque tenté d'envisager pour nettoyer le gâchis de Crowdstrike :

> Au cours de ce voyage - je pense que c'était en septembre de l'année dernière [2017] - nous avons annoncé que nous augmentions notre financement d'assistance à l'Ukraine de 5 millions de dollars, axés spécifiquement sur la cybersécurité. Puis, lorsque le secrétaire adjoint Mitchell s'est rendu en Ukraine ce printemps [2018], il a annoncé une aide supplémentaire de 5 millions de dollars de la part des États-Unis.L'assistance des États-Unis en matière de cybersécurité à l'Ukraine.
>
> Jorgan K. Andrews, secrétaire adjoint adjoint, Bureau des affaires internationales en matière de stupéfiants et d'application de la loi, juin 2018 à Kopenhagen, Danemark.

Quelques mois seulement avant la débâcle de Crowdstrike en Ukraine, l'entreprise a été autorisée par le Comité national démocrate (DNC) en 2016 à enquêter sur ses serveurs informatiques prétendument piratés par la Russie. La campagne d'Hillary Clinton a affirmé que non seulement des milliers de ses courriels ont été volés - publiés par Wikileaks quelques mois avant les élections présidentielles américaines de 2016 - mais aussi l'ensemble de sa présidence.

Les déclarations et événements contradictoires entourant les enquêtes ultérieures de Crowdstrike sur le serveur de la DNC sont encore plus nombreux - sans compter quelques affirmations confuses de Crowdstrike concernant les dates d'affectation, le personnel et les méthodes - que dans l'histoire tordue du piratage militaire de l'Ukraine. La DNC a officiellement découvert le 28 avril 2016 que ses serveurs avaient été "piratés". Malgré le premier paiement de la DNC à Crowdstrike le 5 mai 2016, tous deux n'ont pas réussi à empêcher que les courriels de Clinton soient d'abord obtenus par le pirate "Guccifer 2" et même publiés par Wikileaks près de deux mois plus tard, 75 % de ces messages électroniques indiquant une date de création postérieure à la première semaine de mai 2016.

Un bon de commande du DOJ datant de juillet 2016, délivré à CrowdStrike, mérite également d'être examiné.

LePDG de Crowdstrike, M. Alperovitch, affirme que les groupes liés à la Russie ont utilisé une commande logicielle appelée "Powershell.exe" ou "X-Agent" avec des paramètres cryptiques qui, une fois exécutés, se transforment en code de programme capable de contrôler le logiciel de gestion de Windows. Il est difficile, voire impossible, de prouver que de telles commandes ont été implantées par des pirates informatiques russes et elles pourraient très bien avoir été insérées par certains des nombreux initiés des gouvernements occidentaux que nous avons vus par le passé, dans le but de "détruire Trump".

> M. Alperovitch a acquis une grande expérience en tant qu'expert en la matière auprès de tous les niveaux des forces de l'ordre américaines et internationales en matière d'analyse, d'enquête et de profilage des activités criminelles organisées transnationales et des cybermenaces émanant de terroristes et d'États-nations adverses. Il est fréquemment cité comme source d'expertise dans des publications nationales, notamment l'Associated Press, NBC, le New York Times, USA Today et le Washington Post.
>
> (Dmitri Alperovitch, Senior Fellow du Conseil Atlantique)

Une analyse médico-légale indépendante du fichier Zip contenant un sous-ensemble apparent de tous les courriels de Clinton obtenus par le pirate informatique "Guccifer 2" a permis de conclure que les fichiers individuels obtenus par lui - et non par Wikileaks - ont été sauvegardés pour la dernière fois en 2015, principalement, exfiltrés le 16 avril, 2016 en utilisant une connexion Internet lente - probablement par satellite -, puis sauvegardés sur une clé USB, copiés de cette clé USB sur un ordinateur avec le fuseau horaire de l'Est des États-Unis et enfin compressés sur cet ordinateur en un seul fichier Zip le 20 juin 2016, si les informations de date de tous les fichiers individuels n'ont pas été modifiées par le "piratage". Par ailleurs, le président et CSO de CrowdStrike, Shawn Henry, a lui-même déclaré devant la

commission du renseignement le 5 décembre 2017(à la page 32) que "nous n'avions pas de preuve concrète que des données avaient été exfiltrées de la DNC, mais nous avons des indicateurs qu'elles ont été exfiltrées".

> **M. Henry**: "L'avocat vient de me rappeler qu'en ce qui concerne la DNC, nous avons des indicateurs selon lesquels des données ont été exfiltrées. Nous n'avons pas de preuve concrète que des données ont été exfiltrées de la DNC, mais nous avons des indicateurs qu'elles ont été exfiltrées". (p. 32)
> ...
> **M. Henry**: "Oui, Monsieur. Je veux dire qu'il n'y a pas - l'analogie que j'ai utilisée avec M. Stewart tout à l'heure, c'est que nous n'avons pas de vidéo de ce qui s'est passé, mais il y a des indicateurs qui montrent que cela s'est passé. Il arrive que nous puissions voir des données exfiltrées et que nous puissions l'affirmer de manière concluante. Mais dans ce cas, il semble que les données aient été préparées pour être exfiltrées, mais nous n'avons pas de preuve qu'elles ont effectivement été envoyées." (p. 32)
> ...
> **M. Henry**: "Certaines des données que nous avons vues ont été mises en scène, mais nous n'avions pas d'indication qu'elles avaient été exfiltrées, mais elles ont été mises en scène - semblaient avoir été mises en scène pour être exfiltrées, et étaient associées à des recherches menées par le DNC sur des candidats de l'opposition." (p. 49)
> ...
> **M. Stewart de l'Utah**: "Vous avez dit quelque chose, et je voudrais le répéter - et me dire si je me trompe - si c'est possible. Vous avez dit, je crois, à propos de l'ordinateur de la DNC, que vous aviez des indications que des données étaient prêtes à être exfiltrées, mais qu'il n'y avait aucune preuve qu'elles étaient effectivement parties. Ai-je bien noté cela ?"
> **M. Henry**: "Oui"
> **M. Stewart de l'Utah**: "Et, dans ce cas, les données dont je suppose que vous parlez sont les courriels ainsi que tout ce qu'ils ont pu essayer de prendre."
> **M. Henry**: "Il y avait des fichiers liés aux recherches de l'opposition qui avaient été menées."
> **M. Stewart de l'Utah**: "D'accord. Qu'en est-il des courriels dont tout le monde est si, vous savez, au courant ? Y avait-il aussi des indices qu'ils avaient été préparés, mais pas de preuves qu'ils avaient été exfiltrés ?"
> **M. Stewart : "D'accord. Henry**: "Il n'y a pas de preuve qu'ils ont été exfiltrés. Il y a des preuves indirectes..."
> **M. Stewart de l'Utah**: "D'accord"
> **M. Henry**: "- mais aucune preuve qu'ils ont été réellement exfiltrés. Mais permettez-moi aussi de dire que si quelqu'un surveillait un serveur de messagerie, il pourrait lire tous les courriels." (p. 74 / 75)
>
> Transcription de l'entretien de Shawn Henry à la commission du renseignement de la Chambre des représentants le 5 décembre 2017.

En outre, Hillary Clinton avait utilisé un serveur de messagerie privé dans son bureau privé de Chappaqua, New York, pour les affaires officielles du département d'État et avait même invité Google en 2012 - couvrant la chronologie des attaques de l'ambassade des États-Unis à Benghazi - à gérer son compte de messagerie officiel personnel, très probablement dans le but pour contourner l'obligation de sauvegarder ses conversations officielles et de les mettre à la disposition du public. Son serveur privé à Chappaqua utilisait un logiciel de gestion de courrier électronique Windows.

Pour couronner le tout, il n'est pas nécessaire d'avoir les yeux d'un aigle pour voir les propos clairement contestables de l'ancien directeur du FBI James Comey lorsqu'il a été interrogé en janvier 2017 au Sénat américain sur les serveurs de la DNC et Crowdstrike :

> **Comey**: "Nous préférons avoir accès à l'appareil ou au serveur original qui est impliqué, c'est la meilleure preuve."
> **Sénateur**: "Avez-vous eu accès à l'expertise de ces serveurs ?"
> **Comey**: "Non, une société privée très respectée [Crowdstrike] a fini par y avoir accès et nous a fait part de ce qu'elle y a vu."
> Le**sénateur**: "Est-ce que c'est typiquement la façon dont le FBI préfèrerait faire les expertises ou préfèreriez-vous sentir et voir le serveur vous-même ?"
> **Comey**: "Nous préférons toujours avoir accès à nos propres mains si c'est possible."
> Le**sénateur**: "Savez-vous pourquoi on vous a refusé l'accès aux serveurs ?"
> **Comey**: "Je n'en suis pas sûr. Je n'en suis pas sûr."
> Le**sénateur**: "Y a-t-il eu une ou plusieurs demandes ?"
> **Comey**: "Plusieurs demandes à différents niveaux et, en fin de compte, ce qui a été convenu, c'est que la société privée partagerait avec nous ce qu'elle a vu."
>
> (James Comey, ancien directeur du FBI, lors d'une audition au Sénat américain le 10 janvier 2017)

Il semble que le DNC ait été en charge du FBI en 2016, et non du ministère de la Justice, du Congrès américain ou du Sénat américain. Toute la saga du DNC pourrait être classée dans le dossier "Corruption massive", s'il n'y avait pas le fameux appel téléphonique avec le président ukrainien nouvellement élu Zelensky le 25 juillet 2019, au cours duquel le président américain a mentionné Crowdstrike en particulier :

> J'aimerais cependant que vous nous fassiez une faveur parce que notre pays a traversé beaucoup de choses et que l'Ukraine en sait beaucoup à ce sujet. Je voudrais que vous découvriez ce qui s'est passé avec toute cette situation avec l'Ukraine, **ils disent Crowdstrike**.... Je suppose que vous avez un de vos riches... Le **serveur, ils disent que c'est l'Ukraine qui l'a**. Il y a beaucoup de choses qui se sont passées, toute cette situation... J'aimerais que le procureur général vous appelle, vous ou vos collaborateurs, et que vous alliez au fond des choses. Comme vous l'avez vu hier, toute cette absurdité s'est terminée par une très mauvaise performance d'un homme nommé Robert Mueller, une performance incompétente, mais ils disent que beaucoup de choses ont commencé avec l'Ukraine.

> (Le président américain Donald Trump lors d'une conversation téléphonique du 25 juillet 2019 avec le président de l'Ukraine, Zelensky)

Peu après, l'enfer a éclaté parmi les politiciens démocrates du Congrès américain, qui avaient sérieusement l'intention de mettre en accusation le président américain pour ces mots épicés - et certains liés à la corruption de Joe Biden en Ukraine - lors de son appel téléphonique, par ailleurs approprié et régulier, avec Zelensky. Le théâtre de l'impeachment n'a pas duré longtemps, il a finalement été rejeté par le Sénat américain au début de l'année 2020 et est devenu une entreprise supra-partisane lorsque tous les républicains du Congrès américain l'ont également rejetée.

Il n'y a peut-être pas d'autre explication que le fait que l'Ukraine possède une copie numérique du serveur du DNC quelque part. Avec des matériaux potentiellement contagieux. Les aigles peuvent le voir clairement de très haut et de très loin.

https://www.sun24.news/fr/une-greve-bondee-a-propos-de-crowdstrike-et-des-analyses-informatiques-mal-menees.html