No es la primera vez que CrowdStrike se ve envuelta en una polémica

RAY MCGOVERN :: 22/07/2024

La empresa con vínculos con el FBI fue responsable de una interrupción masiva de las computadoras que afectó a casi todo el mundo, luego de su dudoso papel en el asunto Russiagate

La empresa de seguridad cibernética CrowdStrike, que estaba en medio del falso escándalo Russiagate, sufrió un duro golpe a partir del jueves por la noche cuando una actualización defectuosa de su software de seguridad que envió causó que las computadoras de Microsoft se apagaran, afectando gravemente a los viajes aéreos y ferroviarios; bancario; radiodifusión, atención sanitaria y otras industrias.

El devastador episodio fue costoso para compañía: ha perdido el 12 por ciento de su valor en bolsa. Aún no se ha calculado la cantidad de dinero que perdieron las empresas afectadas. No es la primera vez que la firma de 13 años se ve envuelta en una polémica.

Reproducimos aquí un artículo escrito en 2020 por el exanalista de la CIA Ray McGovern que expone un testimonio a puerta cerrada del ejecutivo de CrowdStrike, Shawn Henry ante el comité de inteligencia de la Cámara de Representantes de EEUU, en el que dice que no hay pruebas definitivas de que los correos electrónicos del Partido Demócrata hayan sido pirateados desde sus servidores.

Ese explosivo testimonio, que permaneció en secreto durante casi tres años, destruyó el mito de que Rusia había pirateado el Comité Nacional Demócrata y había entregado sus correos electrónicos a WikiLeaks.

Los pilares gemelos del Russiagate se desmoronan

Durante dos años y medio, el Comité de Inteligencia de la Cámara de Representantes supo que CrowdStrike no tenía información cierta sobre el Russiagate. Ahora el público también lo sabe.

Los documentos del Comité de Inteligencia de Rusia publicados el jueves revelan que hace dos años y medio se le dijo al comité que el FBI no tenía pruebas concretas de que Rusia pirateara las computadoras del Comité Nacional Demócrata (DNC por sus siglas en inglés) para robar los correos electrónicos del Comité Nacional Demócrata publicados por Wikileaks en julio 2016.

El testimonio a puerta cerrada, hasta ahora enterrado, llegó el 5 de diciembre de 2017 de Shawn Henry, un protegido del ex director del FBI Robert Mueller (de 2001 a 2012), para quien Henry se desempeñó como jefe de la unidad de investigaciones de delitos cibernéticos de la Oficina.

Henry se jubiló en 2012 y ocupó uno de los puestos de más alto nivel en CrowdStrike, la empresa de seguridad cibernética contratada por el Comité Nacional Demócrata y la campaña de Clinton para investigar las intrusiones cibernéticas que ocurrieron antes de las elecciones presidenciales de 2016.

Las siguientes extractos del testimonio de Henry hablan por sí solos. El diálogo no es un modelo de claridad; pero si se lee con atención, incluso los ciberneófitos pueden entender:

Miembro de mayor rango [Adam] Schiff: ¿Sabe usted la fecha en que los rusos extrajeron los datos del Comité Nacional Demócrata? ... ¿cuándo habría sido eso?

Henry: El abogado acaba de recordarme que, en lo que se refiere al Comité Nacional Demócrata, tenemos indicadores de que se extrajeron datos del Comité, pero no tenemos indicadores de que se hayan extraído (sic). ... Hay ocasiones en las que podemos ver datos filtrados y podemos decirlo de manera concluyente. Pero en este caso, parece que fue preparado para ser exfiltrado, pero simplemente no tenemos la evidencia que diga que realmente así fue.

[Chris] Stewart de Utah: Bueno. ¿Qué pasa con los correos electrónicos que todo el mundo conoce? ¿Hubo también indicadores de que estaban preparados pero no pruebas de que realmente fueron exfiltrados?

Henry: No hay evidencia de que realmente hayan sido exfiltrados. Hay pruebas circunstanciales... pero no hay pruebas de que realmente hayan sido exfiltrados. ...

Stewart: ¿Pero tiene un grado de confianza mucho menor en que estos datos realmente salieron que el que tiene, por ejemplo, en que fueron los rusos quienes violaron la seguridad?

Henry: Existe evidencia circunstancial de que esos datos fueron extraídos de la red.

Stewart: Y lo circunstancial es menos seguro que las otras pruebas que ha indicado...

Henry: No teníamos un sensor que detectara la salida de datos. Dijimos que los datos salieron en base a la evidencia circunstancial. Esa fue la conclusión a la que llegamos.

En respuesta a una pregunta de seguimiento, Henry pronunció este clásico: "Señor, solo estaba tratando de ser objetivamente preciso, que no vimos que los datos desaparecieran, pero creemos que desaparecieron, según lo que nosotros vimos."

Sin darse cuenta, resaltando el tenue fundamento de la "creencia" de CrowdStrike de que Rusia pirateó los correos electrónicos del Comité Nacional Demócrata, Henry agregó: "Hay otros estados-nación que recopilan este tipo de inteligencia con seguridad, pero lo que llamaríamos las tácticas y técnicas eran consistentes con lo que habíamos visto asociado con el estado ruso".

No transparente

Por más que se intente hacer luz, algunos de los testimonios siguen siendo opacos. Parte del

problema es la ambigüedad en la palabra "exfiltración".

La palabra puede denotar (1) transferir datos desde una computadora a través de Internet (piratería) o (2) copiar datos físicamente a un dispositivo de almacenamiento externo con la intención de filtrarlos.

Como ha estado informando Veteran Intelligence Professionals for Sanity (VIPS) durante más de tres años, los metadatos y otras pruebas forenses contundentes indican que los correos electrónicos del Comité Nacional Demócrata no fueron pirateados, ni por Rusia ni por nadie más.

Más bien, fueron copiados en un dispositivo de almacenamiento externo (probablemente una memoria USB) por alguien con acceso a las computadoras del DNC. Además, es casi seguro que cualquier piratería en Internet habría sido descubierta por la cobertura de la Agencia de Seguridad Nacional y sus servicios de inteligencia extranjeros cooperantes.

Henry testifica que "parece que [el robo de correos electrónicos del DNC] fue preparado para ser extraído, pero simplemente no tenemos la evidencia que demuestre que realmente así fue".

Esto, desde el punto de vista de VIPS, sugiere que alguien con acceso a las computadoras del DNC "configura" correos electrónicos seleccionados para transferirlos a un dispositivo de almacenamiento externo (una memoria USB, por ejemplo). No se necesita Internet para dicha transferencia. Se habría detectado el uso de Internet, lo que habría permitido a Henry identificar una "exfiltración" a través de esa red.

Bill Binney, ex director técnico de la NSA y miembro de VIPS, presentó una declaración jurada en el caso de Roger Stone. Binney dijo: "WikiLeaks no recibió datos robados desde el gobierno ruso. Los metadatos intrínsecos de los archivos disponibles públicamente en WikiLeaks demuestran que los archivos adquiridos por WikiLeaks se entregaron en un medio como una memoria USB".

La llamada evaluación de la comunidad de inteligencia

No hay mucho bueno que decir sobre la Evaluación de la Comunidad de Inteligencia (ICA, por sus siglas en inglés), vergonzosamente empobrecida, del 6 de enero de 2017, que acusa a Rusia de piratear el Comité Nacional Demócrata.

Pero el ICA sí incluyó dos pasajes que son alta y demostrablemente cierto:

(1) En las observaciones introductorias sobre la "atribución de incidentes cibernéticos", los autores del ICA hicieron un comentario muy pertinente: "La naturaleza del ciberespacio hace que la atribución de operaciones cibernéticas sea difícil, pero no imposible. Todo tipo de operación cibernética, maliciosa o no, deja un rastro".

(2) "Cuando los analistas usan palabras como 'evaluamos' o 'juzgamos', [éstas] no pretenden implicar que tengamos pruebas que demuestren que algo es un hecho. ... Las evaluaciones se basan en información recopilada, que a menudo es incompleta o fragmentaria... Un alto

nivel de confianza en un juicio no implica que la evaluación sea un hecho o una certeza; tales juicios podrían estar equivocados". [Y se podría agregar que comúnmente están equivocados cuando los analistas sucumben a la presión política, como fue el caso de la ICA.]

Sin embargo, los medios corporativos favorables a la CIA otorgaron inmediatamente el estatus de Sagrada Escritura a la mal llamada "Evaluación de la comunidad de inteligencia" (fue un esfuerzo final preparado por "analistas cuidadosamente seleccionados" de la CIA, el FBI y la NSA únicamente), y optaron por pasar por alto las advertencias banales y de divulgación total incluidas en la propia evaluación.

El entonces director de Inteligencia Nacional, James Clapper, y los directores de la CIA, el FBI y la NSA informaron a Obama sobre la ICA el 5 de enero de 2017, el día antes de que se la entregaran personalmente al presidente electo Donald Trump.

El 18 de enero de 2017, en su última conferencia de prensa, Obama consideró oportuno utilizar un lenguaje jurídico sobre la cuestión clave de cómo llegaron los correos electrónicos del Comité Nacional Demócrata a Wikileaks, en un aparente esfuerzo por cubrir su propio trasero.

Obama: "Las conclusiones de la comunidad de inteligencia con respecto al hackeo ruso no fueron concluyentes en cuanto a si WikiLeaks fue consciente o no al ser el conducto a través del cual nos enteramos de los correos electrónicos del Comité Nacional Demócrata que se filtraron".

Así que terminamos con "conclusiones no concluyentes" sobre ese punto ciertamente crucial. Lo que Obama estaba diciendo es que la inteligencia estadounidense no sabía -o afirmaba no saber- exactamente cómo se produjo la supuesta transferencia rusa a Wikileaks, ya sea a través de un tercero o de un robo interno, y enturbió las aguas al decir primero que era un truco y luego una fuga.

Desde el principio, en ausencia de pruebas contundentes por parte de la NSA o de sus socios extranjeros de un hackeo en Internet de los correos electrónicos del DNC, la afirmación de que "los rusos entregaron los correos electrónicos del Comité Nacional Demócrata a Wikileaks" descansaba sobre bases débiles.

En noviembre de 2018, en un foro público, le pedí a Clapper que explicara por qué Obama todavía tenía serias dudas a fines de enero de 2017, menos de dos semanas después de que Clapper y los otros jefes de inteligencia informaran detalladamente al presidente saliente sobre su "alta confianza" en las recomendaciones.

Clapper respondió: "No puedo explicar qué dijo [Obama] ni por qué. Pero puedo decirles que estamos bastante seguros de que sabemos, o sabíamos en ese momento, cómo Wikileaks recibió esos correos electrónicos". ¿Bastante seguro?

El director del FBI, James Comey, informa a Obama en junio de 2016.

Una empresa de ciberseguridad "muy respetada"

CrowdStrike ya tenía una reputación de credibilidad empañada cuando el Comité Nacional Demócrata y la campaña de Clinton lo eligieron para hacer el trabajo que el FBI debería haber estado haciendo para investigar cómo se fugaron los correos electrónicos del Comité Nacional Demócrata. Anteriormente había afirmado que los rusos piratearon una aplicación de artillería ucraniana, lo que provocó grandes pérdidas de obuses en la lucha de Ucrania contra los separatistas apoyados por Rusia. Un reporte de Voz de América explicó por qué CrowdStrike se vio obligado a retractarse de esa afirmación.

¿Por qué el director del FBI, James Comey, no insistió simplemente en el acceso a las computadoras del Comité Nacional Demócrata? Seguramente podría haber obtenido la autorización correspondiente. A principios de enero de 2017, en reacción a los informes de los medios de comunicación de que el FBI nunca solicitó acceso, Comey le dijo al Comité de Inteligencia del Senado que había "múltiples solicitudes en diferentes niveles" de acceso a los servidores del DNC.

"En última instancia, lo que se acordó es que la empresa privada compartiría con nosotros lo que vieron", dijo. Comey había descrito a CrowdStrike como una empresa de ciberseguridad "muy respetada".

Cuando el presidente del comité, Richard Burr (R-NC), le preguntó si el acceso directo a los servidores y dispositivos habría ayudado al FBI en su investigación, Comey dijo que sí. "Nuestra gente forense siempre preferiría tener acceso al dispositivo o servidor original involucrado, que es la mejor evidencia", dijo.

Cinco meses más tarde, después de que despidieran a Comey, Burr le dio un apoyo en forma de unas cuantas preguntas triviales, claramente bien ensayadas:

> BURR: Y el FBI, en este caso, a diferencia de otros casos que usted pudo investigar, ¿alguna vez tuvo acceso al hardware que fue pirateado? ¿O tuvo que confiar en un tercero para que le proporcionara los datos que habían recopilado?
>
> COMEY: En el caso del Comité Nacional Demócrata... no teníamos acceso a los dispositivos en sí. Obtuvimos información forense relevante de un privado, una empresa de alto nivel, que había hecho el trabajo. Pero no obtuvimos acceso directo.
>
> BURR: ¿Pero sin contenido?
>
> COMEY: Correcto.
>
> BURR: ¿No es el contenido una parte importante de la ciencia forense desde el punto de vista de la contrainteligencia?
>
> COMEY: Lo es, aunque lo que me informaron mis superiores, las personas que eran mis superiores en ese momento, es que habían obtenido de la parte privada la información que necesitaban para comprender la intrusión para la primavera de 2016.

En junio del año pasado fue revelado que Crowdstrike nunca produjo un informe forense final para el gobierno porque el FBI nunca se lo exigió, según el Departamento de Justicia.

Según cualquier estándar normal, el ex director del FBI Comey estaría ahora en serios problemas legales, al igual que Clapper, el ex director de la CIA John Brennan, et al. Cada semana parece surgir evidencia adicional de la mala conducta del FBI bajo Comey, ya sean los abusos de la FISA, la mala conducta en el caso contra el general Michael Flynn o el engaño a todos sobre el hackeo ruso del Comité Nacional Demócrata. Si yo fuera fiscal general, declararía que Comey corre riesgo de fuga y le quitaría el pasaporte. Y haría lo mismo con Clapper y Brennan.

Schiff: toda la confianza, pero ninguna evidencia

Ambos pilares del Russiagate (la colusión y el hackeo ruso) se han derrumbado prácticamente.

La divulgación del testimonio ante el Comité de Inteligencia de la Cámara de Representantes muestra que su presidente Adam Schiff mintió no sólo sobre la "colusión" entre Trump y Putin [que el informe Mueller no pudo probar y cuyas acusaciones se basaron en investigaciones de la oposición financiadas por el DNC y Clinton] sino también sobre la una cuestión aún más básica: el "pirateo ruso" del DNC.

Cinco días después de que Trump asumiera el cargo, tuve la oportunidad de confrontar personalmente a Schiff sobre la evidencia de que Rusia "pirateó" los correos electrónicos del Comité Nacional Demócrata. En repetidas ocasiones le había dado a esa mentira la pátina de un hecho sin dudas durante un discurso en el antiguo "grupo de expertos" de Hillary Clinton/John Podesta, el Center for American Progress Action Fund.

Afortunadamente, las cámaras todavía estaban encendidas cuando me acerqué a Schiff durante la sesión de preguntas y respuestas: "Tiene toda la confianza pero no hay pruebas, ¿verdad?". Le pregunté. Su respuesta fue un presagio de lo que vendría.

consortiumnews.com. Traducción revisada por La Haine.

---

https://www.lahaine.org/mundo.php/no-es-la-primera-vez