Un ataque lleno de gente

Acerca de Crowdstrike y voy a dejar que los análisis de TI

#CrowdStrike #DNC #Clinton #FBI

Las águilas son cazadoras increíblemente amables. Sus habilidades para identificar incluso al animal más pequeño desde lo alto de los cielos son legendarias. Cualquiera que haya tenido la oportunidad de observar a un águila cambiar al modo de ataque, encendiendo su veloz pero decidida zambullida al suelo, difícilmente olvidará esa visión. La casualidad dice que ese águila es parte del logotipo de Crowdstrike, una empresa que ofrece software y servicios de TI relacionados con la seguridad de la red.. La empresa fue fundada en 2011 por George Kurtz, un ex director de tecnología del proveedor de seguridad de computadoras personales McAfee, y Dimitri Alperovich, un experto en seguridad de TI de origen ruso y ex vicepresidente de McAfee. En 2012, un exfuncionario del FBI llamado Shawn Henry se unió a la firma, otros 12 meses después la compañía lanzó su primer producto llamado Crowdstrike Falcon.

Al igual que los halcones reales, el software se creó para vigilar constantemente las redes de computadoras y su inmenso tráfico de datos en busca de intrusos que buscaran robar información confidencial, direcciones IP y más en esa red. Después de que la compañía pudo identificar una serie de ataques a varias redes corporativas e industriales supuestamente de China, Corea del Norte y Rusia en 2014 y 2015, Crowdstrike recibió financiación a gran escala de Google., con un total de más de $ 480 millones para 2019. La compañía también recibió una valoración de más de $ 3 mil millones en 2018 con ingresos por ventas anuales de solo $ 100 millones y fue incluida en NASDAQ en 2019.

Los tres principales accionistas actuales de Crowdstrike enumeran dos grandes inversiones en Silicon Valley empresas y, curiosamente, Allianz Asset Management GmbH con sede en Munich, Alemania. La compañía tiene actualmente una capitalización de mercado de más de $ 15 mil millones con poco más de 2000 empleados, está libre de deudas y tenía más de $ 800 millones en efectivo en octubre de 2019, lo que no está mal por ser "solo" una empresa de software.

Dentro de todo este indiscutible éxito vertiginoso apareció un incidente bastante extraño en 2016, cuando Crowdstrike publicó un informe elegante y colorido sobre cómo un grupo rusollamado "Fancy Bear" supuestamente había pirateado una aplicación militar ucraniana llamada "ArtOS", un software que se puede instalar en Tablet PC y que se utiliza para el control de incendios "para realizar ajustes en las condiciones de disparo de los sistemas balísticos y meteorológicos", por lo que desarrollador de la aplicación, Yaroslav Sherstuk. Crowdstrike hizo una serie de evaluaciones políticas de alto nivel y afirmó que el ejército ucraniano había sufrido "grandes pérdidas" en artillería, principalmente debido a la piratería rusa.

> Durante ese período de desarrollo propuesto, se desarrollaron una serie de eventos importantes entre Ucrania, Rusia y la comunidad internacional. En particular, los intentos rusos de influir en las relaciones entre Ucrania y la UE dieron como resultado el movimiento de protesta a gran escala de Maidan, que finalmente resultó en la destitución del entonces presidente Victor Yanukovich, la invasión y anexión de la península de Crimea por parte de Rusia y el prolongado conflicto armado. en el este de Ucrania. Por lo tanto, la creación de una aplicación [App] que se dirija a algunas de las fuerzas de primera línea fundamentales en la defensa ucraniana en el frente oriental probablemente

> sería una alta prioridad para los desarrolladores de malware rusos que buscan cambiar el rumbo del conflicto a su favor. . Para las tropas ucranianas, las fuerzas de artillería también han asumido un alto costo ... (Crowdstrike Report 'Uso de malware Fancy Bear y Android en el seguimiento de unidades de artillería de campaña ucranianas')

Curiosamente, las principales conclusiones de Crowdstrike fueron rápidamente descartadas. Por ejemplo, por el Instituto Internacional de Estudios Estratégicos (IISS), que emitió la siguiente declaración :

> El informe Crowdstrike utiliza nuestros datos, pero las inferencias y el análisis extraídos de esos datos pertenecen únicamente a los autores del informe. La inferencia que hacen de que las reducciones en las existencias de artillería D-30 ucranianas entre 2013 y 2016 fueron principalmente el resultado de pérdidas en combate no es una conclusión que hayamos sugerido nunca, ni que creemos que sea precisa. (Declaración del IISS de 2017)

Otro investigador del IISS afirmó que la reducción de unidades militares se atribuyó principalmente a una reasignación de sus unidades a otros comandos militares. El ejército ucraniano informó que las pérdidas de artillería de los combates ongiong con los separatistas fueron "varias veces menores que el número informado por Crowdstrike y no están asociadas con la causa específica" del ataque. El desarrollador de la aplicación emitió una declaración sobre los hallazgos de Crowdstrike en Ucrania en Facebook , calificándolos de "delirantes". Sin embargo, admitió que sus correos electrónicos estaban comprometidos.

Curiosamente también que un funcionario estadounidense de alto rango explicó en una conferencia en Dinamarca en 2018 sobre cómo EE. UU. continuó apoyando explícitamente los esfuerzos de seguridad cibernética de Ucrania con un total de $ 10 millones, uno está casi tentado de considerar para limpiar el desastre de Crowdstrike:

> Durante ese viaje, creo que fue en septiembre del año pasado [2017], anunciamos que íbamos a aumentar nuestra financiación de asistencia a Ucrania en $ 5 millones, centrados específicamente en la seguridad cibernética. Y luego, cuando el subsecretario Mitchell viajó a Ucrania esta primavera [2018], anunció $ 5 millones adicionales en asistencia de seguridad cibernética de Estados Unidos a Ucrania. (Jorgan K. Andrews, Subsecretario Adjunto, Oficina de Asuntos Internacionales de Narcóticos y Aplicación de la Ley, junio de 2018 en Kopenhagen, Dinamarca)

Solo unos meses antes de la debacle de Crowdstrike en Ucrania, el Comité Nacional Demócrata (DNC) le dio permiso a la compañía en 2016 para investigar sus servidores informáticos presuntamente pirateados por Rusia. La campaña de Hillary Clinton afirmó que no solo se robaron miles de sus correos electrónicos, publicados por Wikileaks unos meses antes de las elecciones presidenciales de EE. UU. De 2016, sino también toda su presidencia.

Hay incluso más declaraciones y eventos contradictorios en torno a las investigaciones posteriores de DNC Server de Crowdstrike, que no se limitan a bastantes afirmaciones confusas de Crowdstrike con respecto a las fechas de asignación, el personal y los métodos, que en la retorcida historia de piratería militar de Ucrania. El DNC descubrió oficialmente el 28 de abril de 2016 que sus servidores habían sido 'pirateados'. A pesar del primer pago de DNC a Crowdstrike el 5 de mayo de 2016, ambos no pudieron evitar que los correos electrónicos de Clinton fueran obtenidos primero por el hacker "Guccifer 2" e incluso se publicaran en Wikileaks casi dos meses después, y el 75% de estos mensajes de correo electrónico indicaron una fecha de creación posterior. que la primera semana de mayo de 2016.

El CEO de Crowdstrike, Alperovitch, afirmaque los grupos vinculados a Rusia utilizaron un comando de software llamado 'Powershell.exe' o 'X-Agent' con parámetros crípticos que se transformaron en código de programa cuando se ejecutaron, capaces de controlar el software de administración de Windows. La evidencia de que tales comandos fueron realmente implantados por piratas informáticos rusos es difícil, si no casi imposible, de probar y podría muy bien haber sido insertada por algunos de los muchos miembros del gobierno occidental que hemos visto en el pasado , con la intención de 'destruir a Trump'.

> Alperovitch tiene una experiencia significativa trabajando como experto en la materia con todos los niveles de la aplicación de la ley estadounidense e internacional en análisis, investigaciones y elaboración de perfiles de actividades delictivas organizadas transnacionales y amenazas cibernéticas de adversarios terroristas y de estados-nación. Con frecuencia se le cita como fuente experta en publicaciones nacionales, como Associated Press, NBC, New York Times, USA Today y Washington Post. (Dmitri Alperovitch, miembro principal del Atlantic Council)

Un análisis forense independiente del archivo zip que contiene un subconjunto aparente de todos los correos electrónicos de Clinton obtenidos por el hacker 'Guccifer 2' llegó a la conclusión de que los archivos individuales obtenidos por él, no Wikileaks, se guardaron por última vez en 2015 principalmente, exfiltrados el 16 de abril. , 2016 usando una conexión a Internet lenta, probablemente satelital, luego guardada en una memoria USB, copiada de esta memoria USB a una computadora con zona horaria del este de EE. UU. Y finalmente comprimida en esta computadora en un solo archivo Zip el 20 de junio de 2016, si la información de fecha de todos los archivos individuales no había sido alterada por el 'hack'. Además, el presidente y OSC de CrowdStrike, Shawn Henry, declaró ante el Comité de Inteligencia el 5 de diciembre de 2017 (en la página 32) que "no teníamos evidencia concreta de que los datos fueran exfiltrados del DNC, pero tenemos indicadores de que fueron exfiltrados".

> **Sr. Henry**: "El abogado me acaba de recordar que, en lo que se refiere al DNC, tenemos indicadores de que los datos fueron exfiltrados. No teníamos evidencia concreta de que los datos fueron exfiltrados del

DNC, pero tenemos indicadores de que fueron exfiltrados". (p. 32)
...
Sr. Henry: "Sí, señor. Así que, de nuevo, organizado para, lo cual, quiero decir, no existe - la analogía que usé con el Sr. Stewart antes es que no tenemos video de está sucediendo, pero hay indicadores de que sucedió. Hay momentos en los que podemos ver datos exfiltrados, y podemos decir de manera concluyente. Pero en este caso, parece que fue configurado para ser exfiltrado, pero simplemente no tenemos la evidencia que dice que realmente se fue ". (pág.32)
...
Sr. Henry: "Así que algunos de los datos que vimos se organizaron, pero no teníamos indicios de que fueran exfilados, pero estaban organizados, parecían estar organizados para exfil, que estaban asociados con una investigación realizada por el DNC. sobre los candidatos de la oposición ". (p. 49)
...
Sr. Stewart de Utah: "Está bien. Usted dijo algo, y quiero reafirmarlo - y decirme si me equivoco - si pudiera. Usted dijo, creo, hablando del Computadora DNC, tenía indicios de que los datos estaban preparados para ser exfiltrados, pero no hay evidencia de que realmente quedaran. ¿Lo escribí correctamente?
Sr. Henry: "Sí"
Sr. Stewart de Utah: "Y, en este caso, los datos que estoy asumiendo usted 'estamos hablando es el correo electrónico, así como todo lo demás que pueden haber estado tratando de tomar."
Sr. Henry: "Había expedientes relacionados con la investigación de la oposición que se había realizado".
Sr. Stewart de Utah: "Está bien. ¿Qué pasa con los correos electrónicos de los que todo el mundo está tan, ya sabes, bien informado? ¿Hubo también indicadores de que estaban preparados pero no evidencia de que en realidad fueron exfiltrados?"
Sr. Henry: "No hay evidencia de que realmente fueron exfiltrados. Hay evidencia circunstancial -"
Sr. Stewart de Utah: "Está bien"
Sr. Henry: "- pero no hay evidencia de que realmente fueron exfiltrados. Pero permítame también decir que si alguien estaba monitoreando un servidor de correo electrónico, podría leer todo el correo electrónico ". (pags.74/75)

Transcripciones de la entrevista de Shawn Henry en el Comité de Inteligencia de la Cámara el 5 de diciembre de 2017

Además, Hillary Clinton había utilizado un servidor de correo electrónico privado en su oficina privada en Chappaqua, Nueva York para asuntos oficiales del Departamento de Estado e incluso había invitado a Google en 2012 , cubriendo la cronología de los ataques de la embajada de Estados Unidos en Bengasi, para administrar su cuenta de correo electrónico oficial personal. muy probablemente para eludir la obligación de tener sus conversaciones oficiales con el gobierno respaldadas y disponibles para el público. Su servidor privado en Chappaqua estaba ejecutando un software de administración de correo electrónico de Windows.

Además de todo eso, uno no necesita tener los ojos de un águila para ver las palabras claramente cuestionables del exdirector del FBI James Comey cuando se le preguntó en enero de 2017 en el Senado de los Estados Unidos sobre los servidores DNC y Crowdstrike:

> **Comey**: "Preferimos tener acceso al dispositivo o servidor original involucrado, es la mejor evidencia".
> **Senador**: "¿Le dieron acceso para hacer análisis forenses en esos servidores?"
> **Comey**: "No lo éramos, una empresa privada muy respetada [Crowdstrike] finalmente obtuvo acceso y compartió con nosotros lo que vieron allí".
> **Senador**: "¿Es esa la forma típica en que el FBI preferiría hacer los análisis forenses o preferiría sentir y ver el servidor usted mismo?"
> **Comey**: "Siempre preferiríamos tener acceso a nosotros mismos si es posible".
> **Senador**: "¿Sabe por qué se le negó el acceso a los servidores?"
> **Comey**: "No lo sé con seguridad.No lo sé con certeza ".
> **Senador**: "¿Hubo una solicitud o varias solicitudes?"
> **Comey**: “Múltiples solicitudes a diferentes niveles y, en definitiva, lo que se acordó es que la empresa privada compartiera con nosotros lo que veían”.
>
> (El ex director del FBI James Comey en una audiencia en el Senado de los Estados Unidos el 10 de enero de 2017)

Parece como si el DNC estuviera a cargo del FBI en 2016, no del Departamento de Justicia o del Congreso de los Estados Unidos y / o del Senado de los Estados Unidos. Toda la saga del DNC podría archivarse bajo la carpeta 'Corrupción masiva', si no hubiera la famosa llamada telefónica del presidente estadounidense Donald Trump con el recién electo presidente ucraniano Zelensky el 25 de julio de 2019, en la que el presidente estadounidense mencionó a Crowdstrike en particular:

> Sin embargo, me gustaría que nos hicieras un favor porque nuestro país ha pasado por mucho y Ucrania sabe mucho al respecto. Me gustaría que averiguaras qué pasó con toda esta situación con Ucrania, **dicen Crowdstrike**... Supongo que tienes a una de tus personas adineradas ... **El servidor, dicen que Ucrania lo tiene**. Pasaron muchas cosas, toda la situación ... Me gustaría que el Fiscal General lo llamara a usted oa su gente y me gustaría que llegara al fondo del asunto. Como viste ayer, toda esa tontería terminó con una actuación muy pobre de un hombre llamado Robert Mueller, una actuación incompetente, pero dicen que muchas de ellas comenzaron con Ucrania. (El presidente estadounidense Donald Trump en una conversación telefónica del 25 de julio de 2019 con el presidente de Ucrania, Zelensky)

Poco después, estalló el infierno entre los políticos demócratas estadounidenses en el Congreso de los Estados Unidos y quienes tenían la intención seria de acusar al presidente de los Estados Unidos por estas palabras picantes, y con respecto a algunas relacionadas con la corrupción de Joe Biden en Ucrania , en su llamada telefónica regular y apropiada con Zelensky. El teatro de juicio político no duró mucho, finalmente fue desestimado en el Senado de los Estados Unidos a principios de 2020 y se convirtió en un esfuerzo suprapartidista cuando todos los republicanos en el Congreso de los Estados Unidos también lo rechazaron allí.

Puede que no haya otra explicación que el hecho de que Ucrania tiene una copia duplicada digitalmente de ese servidor DNC en alguna parte. Con materiales posiblemente contagiosos.

Las águilas pueden ver eso claramente desde lo alto y muy lejos.

https://www.sun24.news/es/un-ataque-lleno-de-gente-acerca-de-crowdstrike-y-voy-a-dejar-que-los-analisis-de-ti.html