Un colpo affollato

Informazioni su Crowdstrike e le permetterò analisi IT

#CrowdStrike #DNC #Clinton #FBI

Le aquile sono cacciatori incredibilmente graziosi. Le loro capacità di identificare anche l'animale più piccolo dall'alto nei cieli sono leggendarie. Chiunque abbia mai avuto la possibilità di osservare un'aquila che passa alla modalità di attacco, accendendo la loro rapida ma decisa picchiata a terra, difficilmente dimenticherà quella vista. La coincidenza vuole che proprio un'aquila del genere faccia parte del logo di Crowdstrike, una società che fornisce software e servizi IT relativi alla sicurezza di rete . L'azienda è stata fondata nel 2011 da George Kurtz, ex CTO del provider di sicurezza per personal computer McAfee, e Dimitri Alperovich, un esperto di sicurezza IT di origine russa ed ex VP di McAfee. Nel 2012, un ex funzionario dell'FBI di nome Shawn Henry è entrato a far parte dell'azienda, altri 12 mesi dopo la società ha lanciato il suo primo prodotto chiamato Crowdstrike Falcon.

Simile ai veri falchi, il software è stato creato per sorvegliare costantemente le reti di computer e il loro immenso traffico di dati per gli intrusi che miravano a rubare informazioni sensibili, indirizzi IP e altro in quella rete. Dopo che la società ha potuto identificare una serie di attacchi a varie reti aziendali e industriali presumibilmente provenienti da Cina, Corea del Nord e Russia nel 2014 e 2015, Crowdstrike ha ricevuto finanziamenti su larga scala da Google, per un totale di oltre $ 480 milioni entro il 2019. La società ha anche ricevuto una valutazione di oltre $ 3 miliardi nel 2018 con ricavi di vendita annuali di soli $ 100 milioni ed è stata quotata al NASDAQ nel 2019.

Gli attuali tre principali azionisti di Crowdstrike elencano due grandi investimenti nella Silicon Valley società e - stranamente - Allianz Asset Management GmbH con sede a Monaco, Germania. L'azienda ha attualmente una capitalizzazione di mercato di oltre $ 15 miliardi con poco più di 2000 dipendenti, è priva di debiti e aveva oltre $ 800 milioni in contanti nell'ottobre 2019 - non male per essere "solo" una società di software.

All'interno di tutto questo indiscusso successo alle stelle è apparso un incidente piuttosto strano nel 2016, quando Crowdstrike ha pubblicato un rapporto stravagante e colorato su come un gruppo russo denominato "Fancy Bear" avrebbe violato un'app militare ucraina denominata "ArtOS", un software che può essere installato su Tablet PC e che viene utilizzato per il controllo del fuoco "per apportare modifiche alle condizioni di fuoco dei sistemi balistici e meteorologici", quindi il sviluppatore dell'App, Yaroslav Sherstuk. Crowdstrike ha fatto una serie di valutazioni politiche di alto livello e ha affermato che l'esercito ucraino aveva subito "pesanti perdite" nell'artiglieria, principalmente a causa dell'hacking russo.

> Durante il periodo di sviluppo proposto, si sono verificati numerosi eventi significativi tra l'Ucraina, la Russia e la comunità internazionale. In particolare, i tentativi russi di influenzare le relazioni ucraino-UE hanno portato al movimento di protesta su larga scala Maidan, che alla fine ha portato alla cacciata dell'allora presidente Victor Yanukovich, all'invasione e all'annessione della penisola di Crimea da parte della Russia e al prolungato conflitto armato nell'Ucraina orientale. Pertanto, la creazione di un'applicazione [App] che prenda di mira alcune delle forze di prima linea fondamentali nella difesa ucraina sul fronte orientale sarebbe probabilmente una priorità assoluta per gli sviluppatori di malware avversari russi che cercano di ribaltare le sorti del conflitto a loro favore. Per le truppe ucraine, anche le

> forze di artiglieria hanno sostenuto un pesante costo ... (Crowdstrike Report "Uso di Fancy Bear e malware Android nel monitoraggio delle unità di artiglieria da campo ucraine")

Stranamente, le principali conclusioni di Crowdstrike furono rapidamente respinte. Ad esempio dall'International Institute for Strategic Studies (IISS), che ha rilasciato la seguente dichiarazione:

> Il rapporto Crowdstrike utilizza i nostri dati, ma le inferenze e le analisi tratte da tali dati appartengono esclusivamente agli autori del rapporto. La conclusione che fanno che le riduzioni delle disponibilità di artiglieria D-30 ucraina tra il 2013 e il 2016 siano state principalmente il risultato di perdite in combattimento non è una conclusione che ci siamo mai suggeriti, né una che riteniamo accurata. (Dichiarazione IISS del 2017)

Un altro ricercatore IISS ha affermato che la riduzione delle unità militari è stata principalmente attribuita a una riallocazione delle sue unità ad altri comandi militari. L'esercito ucraino ha riferito che le perdite di artiglieria dovute ai combattimenti in corso con i separatisti sono state "molte volte inferiori al numero riportato da Crowdstrike e non sono associate alla causa specifica" dell'hacking. Lo sviluppatore dell'App ha rilasciato una dichiarazione sui risultati di Crowdstrike in Ucraina su Facebook , definendoli "deliranti". Tuttavia, ha ammesso che le sue e-mail erano state compromesse.

È interessante anche che abbia spiegato un alto funzionario statunitense a una conferenza in Danimarca nel 2018 su come gli Stati Uniti hanno continuato a sostenere esplicitamente gli sforzi di sicurezza informatica dell'Ucraina con un totale di $ 10 milioni - si è quasi tentati di prendere in considerazione per ripulire il caos di Crowdstrike:

> Durante quel viaggio - penso sia stato nel settembre dello scorso anno [2017] - abbiamo annunciato che stavamo aumentando i nostri finanziamenti per l'assistenza all'Ucraina di 5 milioni di dollari, concentrati specificamente sulla sicurezza informatica. E poi, quando il sottosegretario Mitchell si è recato in Ucraina questa primavera [2018], ha annunciato altri 5 milioni di dollari in assistenza per la sicurezza informatica degli Stati Uniti in Ucraina. (Jorgan K. Andrews, Vice Segretario aggiunto, Bureau of International Narcotics and Law Enforcement Affairs, giugno 2018 a Kopenhagen, Danimarca)

Solo pochi mesi prima della debacle ucraina di Crowdstrike, la società ha ricevuto il permesso dal Comitato nazionale democratico (DNC) nel 2016 per indagare sui server di computer presumibilmente hackerati dalla Russia. La campagna di Hillary Clinton ha affermato che non solo migliaia delle sue e-mail sono state rubate - pubblicate da Wikileaks pochi mesi prima delle elezioni presidenziali statunitensi del 2016 - ma anche la sua intera presidenza.

Ci sono dichiarazioni ed eventi ancora più contraddittori che circondano le successive indagini di DNC Server di Crowdstrike - non limitate ad alcune confuse affermazioni di Crowdstrike riguardo a date di assegnazione, personale e metodi - che nella contorta storia di hacking militare ucraina. Il 28 aprile 2016 il DNC ha scoperto ufficialmente che i suoi server erano stati "violati". Nonostante il primo pagamento di DNC a Crowdstrike il 5 maggio 2016, entrambi non sono riusciti a impedire che le email di Clinton fossero ottenute prima dall'hacker "Guccifer 2" e persino pubblicate su Wikileaks quasi due mesi dopo, con il 75% di questi messaggi di posta elettronica che indicava una data di creazione successiva rispetto alla prima settimana di maggio 2016.

Afferma il CEO di Crowdstrike Alperovitchche i gruppi collegati alla Russia hanno utilizzato un cosiddetto comando software "Powershell.exe" o "X-Agent" con parametri criptici che si trasformavano in codice di programma quando eseguito, in grado di controllare il software di gestione Windows. La prova che tali comandi siano stati effettivamente impiantati da hacker russi è difficile se non impossibile da provare e potrebbe benissimo essere stata inserita da alcuni dei tanti addetti ai lavori del governo occidentale che abbiamo visto in passato , per 'distruggere Trump'.

> Alperovitch ha una significativa esperienza lavorando come esperto in materia con tutti i livelli delle forze dell'ordine statunitensi e internazionali su analisi, indagini e profilazione di attività criminali organizzate transnazionali e minacce informatiche da parte di terroristi e avversari di stati-nazione. Viene spesso citato come una fonte esperta in pubblicazioni nazionali, tra cui Associated Press, NBC, New York Times, USA Today e Washington Post. (Dmitri Alperovitch, Senior Fellow del Consiglio Atlantico)

Un'analisi forense indipendente del file zip contenente un'apparente sottoinsieme di tutte le e-mail di Clinton ottenute dall'hacker "Guccifer 2" è giunta alla conclusione che i singoli file ottenuti da lui - non Wikileaks - sono stati salvati l'ultima volta nel 2015 principalmente, esfiltrati il 16 aprile , 2016 utilizzando una connessione Internet lenta, probabilmente satellitare, quindi salvata su una pen drive, copiata da questa pen drive a un computer con fuso orario degli Stati Uniti orientali e infine compressa su questo computer in un unico file zip il 20 giugno 2016, se le informazioni sulla data di tutti i singoli file non erano state alterate dall '"hack". Inoltre, il presidente di CrowdStrike e lo stesso CSO Shawn Henry hanno dichiarato di fronte al Comitato di intelligence il 5 dicembre 2017 (a pagina 32) che "non avevamo prove concrete che i dati fossero stati esfiltrati dal DNC, ma abbiamo gli indicatori che siano stati esfiltrati".

> **Sig. Henry**: "L'avvocato mi ha appena ricordato che, per quanto riguarda il DNC, abbiamo indicatori che i dati sono stati esfiltrati. Non avevamo prove concrete che i dati fossero esfiltrati dal DNC, ma abbiamo indicatori che sono stati esfiltrati". (p. 32)
> ...
> **Sig. Henry**: "Sì, signore. Quindi, ancora una volta, è stato messo in scena, il che, voglio dire, non c'è - l'analogia che ho usato con il signor Stewart prima era che non abbiamo video di sta accadendo, ma ci sono indicatori che è successo. Ci sono momenti in cui possiamo vedere i dati esfiltrati e possiamo dire in modo definitivo. Ma in questo caso, sembra che sia stato impostato per essere esfiltrato, ma semplicemente non abbiamo il prove che dicono che effettivamente se n'è andato." (p. 32)
> ...
> **Sig. Henry**: "Quindi alcuni dei dati che abbiamo visto messi in scena ma non avevamo indicazione che fosse stato espulso, ma era stato messo in scena - sembravano essere messi in scena per l'esfiltrazione,

che era associato a ricerche condotte dal DNC sui candidati dell'opposizione". (p. 49)
...
Sig. Stewart dello Utah: "Va bene. Hai detto qualcosa, e voglio ribadirlo - e dimmi se sbaglio - se potessi. Hai detto, credo, parlando del Computer DNC, avevi indicazioni che i dati erano pronti per essere esfiltrati, ma nessuna prova che effettivamente ha lasciato. L'ho annotato correttamente ?"
Sig. Henry: "Sì"
Sig. Stewart dello Utah : "E, in questo caso, i dati che presumo tu"stai parlando dell'e-mail e di tutto ciò che potrebbero aver cercato di prendere."
Sig. Henry: "C'erano file relativi alla ricerca sull'opposizione che era stata condotta."
Sig. Stewart dello Utah: "Okay. E le e-mail di cui tutti sono così a conoscenza? C'erano anche indicatori che fossero preparati ma non prove che fossero effettivamente esfiltrati ?"
Sig. Henry: "Non ci sono prove che siano stati effettivamente esfiltrati. Ci sono prove circostanziali -"
Sig. Stewart dello Utah : "Okay"
Sig. Henry: "- ma nessuna prova che siano stati effettivamente esfiltrati. Ma lasciatemi anche affermare che se qualcuno stava monitorando un server di posta elettronica, potrebbe leggere tutta la posta." (p.74/75)

Trascrizioni dell'intervista di Shawn Henry alla House Committee on Intelligence il 5 dicembre 2017

Inoltre, Hillary Clinton aveva utilizzato un server di posta elettronica privato nel suo ufficio privato a Chappaqua, New York per questioni ufficiali del Dipartimento di Stato e aveva persino invitato Google nel 2012 - coprendo la cronologia degli attacchi dell'ambasciata degli Stati Uniti a Bengasi - per gestire il suo account di posta elettronica ufficiale personale, molto probabilmente per aggirare l'obbligo di sostenere e rendere disponibili al pubblico le sue conversazioni ufficiali del governo. Il suo server privato a Chappaqua eseguiva un software di gestione della posta elettronica di Windows.

Oltre a tutto ciò, non è necessario avere gli occhi di un'aquila per vedere le parole chiaramente discutibili dell'ex direttore dell'FBI James Comey quando nel gennaio 2017 al Senato degli Stati Uniti è stato chiesto sui server DNC e Crowdstrike:

Comey: "Preferiamo avere accesso al dispositivo o al server originale coinvolto, è la prova migliore."
Senatore: "Le è stato concesso l'accesso per fare indagini legali su quei server?"
Comey: "Non lo eravamo, una compagnia privata molto rispettata [Crowdstrike] alla fine ha avuto accesso e ha condiviso con noi quello che vedeva lì".
Senatore: "È questo il modo in cui l'FBI preferirebbe fare la scientifica o preferiresti sentire e vedere tu

> stesso il server?"
> **Comey**: "Preferiremmo sempre avere le mani di accesso su noi stessi, se possibile."
> **Senatore**: "Sai perché ti è stato negato l'accesso ai server?"
> **Comey**: "Non lo so per certo.Non lo so per certo."
> **Senatore**: "C'era una o più richieste?"
> **Comey**: "Molteplici richieste a diversi livelli e, in ultima analisi, ciò che è stato concordato è che la società privata condividesse con noi ciò che ha visto".
>
> (L'ex direttore dell'FBI James Comey durante un'audizione al Senato degli Stati Uniti il 10 gennaio 2017)

Sembra che nel 2016 il DNC fosse a capo dell'FBI, non del Dipartimento di Giustizia o del Congresso degli Stati Uniti e / o del Senato degli Stati Uniti. L'intera saga di DNC potrebbe essere archiviata nella cartella 'Massive Corruption', se non ci fosse la famosa telefonata del presidente degli Stati Uniti Donald Trump con il neoeletto presidente ucraino Zelensky il 25 luglio 2019, in cui il presidente degli Stati Uniti ha menzionato Crowdstrike in particolare:

> Vorrei però che ci faceste un favore perché il nostro paese ne ha passate tante e l'Ucraina ne sa molto. Vorrei **che scoprissi** cosa è successo con l'intera situazione con l'Ucraina, **dicono Crowdstrike**... Immagino che tu abbia una delle tue persone benestanti ... **Il server, dicono che l'Ucraina ce l'ha**. Sono successe molte cose, l'intera situazione ... Vorrei che il Procuratore generale chiamasse te o la tua gente e vorrei che arrivassi fino in fondo. Come hai visto ieri, tutta quella sciocchezza si è conclusa con una prestazione molto scarsa di un uomo di nome Robert Mueller, una prestazione incompetente, ma dicono che gran parte sia iniziata con l'Ucraina. (Il presidente statunitense Donald Trump in una conversazione telefonica del 25 luglio 2019 con il presidente dell'Ucraina, Zelensky)

Poco dopo, l'inferno è scoppiato tra i politici democratici per lo più statunitensi al Congresso degli Stati Uniti e che intendevano seriamente mettere sotto accusa il presidente degli Stati Uniti per queste parole piccanti - e per quanto riguarda alcune relative alla corruzione di Joe Biden in Ucraina - nella sua altrimenti appropriata e regolare telefonata con Zelensky. Il teatro dell'impeachment non è durato a lungo, è stato infine respinto dal Senato degli Stati Uniti all'inizio del 2020 e ha reso uno sforzo supra-partigiano quando tutti i repubblicani nel Congresso degli Stati Uniti lo hanno respinto anche lì.

Potrebbe non esserci altra spiegazione se non che l'Ucraina ha effettivamente una copia speculare digitale di quel server DNC da qualche parte. Con materiali potenzialmente contagiosi su di esso.

Le aquile possono vederlo chiaramente dall'alto e da lontano.

https://www.sun24.news/it/un-colpo-affollato-informazioni-su-crowdstrike-e-le-permettero-analisi-it.html