A Crowded Strike

About Crowdstrike and ill-led IT analyses

#CrowdStrike #DNC #Clinton #FBI

Eagles are incredibly gracious hunters. Their abilities to identify even the smallest animal from high above in the skies are legendary. Anyone who had ever had the chance to observe an eagle switch into attack mode, igniting their velocious yet determined dive to the ground, will hardly forget that sight. Coincidence has it that just such an eagle is part of the logo of Crowdstrike, a company providing IT software and services surrounding network security. The company was founded in 2011 by George Kurtz, a former CTO of personal computer security provider McAfee, and Dimitri Alperovich, a Russian-born IT security expert and former VP of McAfee. In 2012, a former FBI official named Shawn Henry joined the firm, another 12 months later the company launched its first product named Crowdstrike Falcon.

Similar to real falcons, the software was created to constantly surveil computer networks and their immense data traffic for intruders who aimed at stealing sensitive information, IP addresses, and more in that network. After the company could identify a number of attacks on various corporate and industry networks allegedly from China, North Korea and Russia in 2014 and 2015, Crowdstrike received large scale funding from Google, totalling to more than $480 millions by 2019. The company also received a valuation of more than $3 billion in 2018 with annual sales revenues of only $100 million and was listed on NASDAQ in 2019.

Crowdstrike's current top three shareholders list two large Silicon Valley investment companies and - strangely - Munich, Germany based Allianz Asset Management GmbH. Crowdstrike has currently a market capitalisation of more than $15 billion with little more than 2000 employees, is debt-free and had over $800 million in cash at hand in October 2019 - not bad for being "only" a software company.

Within all this undisputed skyrocketing success appeared a rather strange incident in 2016, when Crowdstrike issued a fancy and colorful report about how a Russian group named "Fancy Bear" allegedly had hacked a Ukrainian military App named "ArtOS", a software that can be installed on Tablet PC's and that is used for fire control "to make adjustments to the firing conditions of ballistic and meteorological systems", so the developer of the App, Yaroslav Sherstuk. Crowdstrike made a number of high-level political assessments and claimed the Ukrainian military had suffered "heavy losses" in artillery, mainly because of the Russian hacking.

> During that proposed development timeframe, a number of significant events unfolded between Ukraine, Russia, and the international community. Most notably, Russian attempts to influence Ukrainian-EU relations resulted in the large-scale, Maidan protest movement, eventually resulting in the ouster of then-president Victor Yanukovich, the invasion and annexation of the Crimean Peninsula by Russia, and the protracted armed conflict in eastern Ukraine. Therefore, the creation of an application [App] that targets some of the front line forces pivotal in Ukrainian defense on the eastern front would likely be a high priority for Russian adversary malware developers seeking to turn the tide of the conflict in their favor ... For Ukrainian troops, artillery forces have also shouldered a heavy cost...

> (Crowdstrike Report 'Use of Fancy Bear and Android malware in tracking of Ukrainian field artillery units')

Strangely, Crowdstrike's major conclusions were quickly dismissed. For example by the International Institute for Strategic Studies (IISS), which issued the following statement:

> The Crowdstrike report uses our data, but the inferences and analysis drawn from that data belong solely to the report's authors. The inference they make that reductions in Ukrainian D-30 artillery holdings between 2013 and 2016 were primarily the result of combat losses is not a conclusion that we have ever suggested ourselves, nor one we believe to be accurate.
>
> (Statement by IISS from 2017)

Another IISS researcher stated that the reduction in military units were mainly attributed to a reallocation of its units to other military commands. The Ukrainian military reported that the artillery losses from the ongiong fighting with the separatists were "several times smaller than the number reported by Crowdstrike and are not associated with the specific cause" of the hacking. The App developer issued a statement about Crowdstrike's Ukraine findings on Facebook, calling them "delusional". He admitted that his emails were compromised, however.

Interestingly also that a high ranking US official explained at a conference in Denmark in 2018 about how the US continued to explicitly support Ukraine's cyber security endeavours with a total of $10 million - one is almost tempted to consider for cleaning up the Crowdstrike mess:

> During that trip – I think it was in September of last year [2017] – we announced that we were increasing our assistance funding to Ukraine by $5 million, focused specifically on cyber security. And then when Assistant Secretary Mitchell traveled to Ukraine this spring [2018], he announced an additional $5 million in U.S. cyber security assistance to Ukraine.
>
> (Jorgan K. Andrews, Deputy Assistant Secretary, Bureau of International Narcotics and Law Enforcement Affairs, June 2018 in Kopenhagen, Denmark)

Only a few months prior to Crowdstrike's Ukraine debacle, the company was given permission by the Democratic National Committee (DNC) in 2016 to investigate their allegedly Russian-hacked computer servers. Hillary Clinton's campaign claimed that not only thousands of her emails were stolen - published by Wikileaks a few month before the 2016 US presidential elections - but also her entire presidency.

There are even more contradictory statements and events surrounding Crowdstrike's subsequent DNC Server investigations - not limited to quite a few confusing Crowdstrike claims regarding assignment dates, personel and methods - than in the twisted Ukraine military hacking story. The DNC officially found out on April 28, 2016 that its servers had been 'hacked'. Despite DNC's first payment to Crowdstrike on May 5, 2016, both failed to prevent Clinton's emails from being obtained first by hacker "Guccifer 2" and even published at Wikileaks almost two months later, with 75% of these email messages indicating a creation date later than the first week of May 2016.

A DOJ purchase order from July 2016, issued to CrowdStrike, is worth taking a look at as well.

Crowdstrike CEO Alperovitch claims that the Russia-linked groups used a so-called 'Powershell.exe' or 'X-Agent' software command with cryptic parameters that transformed into program code when executed, able to control Windows Management software. Evidence that such commands were actually implanted by Russian hackers is difficult if not nearly impossible to prove and could very well had been inserted by some of the many Western government insiders we have seen in the past, out to 'destroy Trump'.

> Alperovitch has significant experience working as a subject matter expert with all levels of US and international law enforcement on analysis, investigations, and profiling of transnational organized criminal activities and cyberthreats from terrorist and nation-state adversaries. He is frequently quoted as an expert source in national publications, including the Associated Press, NBC, the New York Times, USA Today, and the Washington Post.
>
> (Dmitri Alperovitch, Senior Fellow of the Atlantic Council)

An independent forensic analysis of the Zip-File containing an apparent subset of all Clinton emails obtained by hacker 'Guccifer 2' came to the conclusion that the individual files obtained by him - not Wikileaks - were last saved in 2015 mainly, exfiltrated on April 16, 2016 using a slow - probably satellite - Internet connection, then saved to a thumb drive, copied from this thumb drive to a computer with US Eastern timezone and finally compressed on this computer into a single Zip-File on June 20, 2016, if the date information of all the individual files had not been altered by the 'hack'. Also, CrowdStrike's President and CSO Shawn Henry himself stated in front of the Committee of Intelligence on December 5, 2017 (on page 32) that "we did not have concrete evidence that data was exfiltrated from the DNC, but we have indicators that it was exfiltrated".

> **Mr. Henry**: "Counsel just reminded me that, as it relates to the DNC we have indicators that data was exfiltrated. We did not have concrete evidence that data was exfiltrated from the DNC, but we have indicators that it was exfiltrated." (p. 32)
> ...
> **Mr. Henry**: "Yes, Sir. So that, again, staged for, which, I mean, there's not - the analogy I used with Mr. Stewart earlier was we don't have video of it happening, but there are indicators that it happened. There are times when we can see data exfiltrated, and we can say conclusively. But in this case, it appears it was set up to be exfiltrated, but we just don't have the evidence that says it actually left." (p. 32)
> ...
> **Mr. Henry**: "So some of the data that we saw staged but we didn't have indication that it was exfil'd,

but it was staged - appeared to be staged for exfil, that it was associated with research that had been conducted by the DNC on opposition candidates." (p. 49)
...
Mr. Stewart of Utah: "Okay. You said something, and I want to restate it - and tell me if I'm wrong - if I could. You said, I believe, talking about the DNC computer, you had indications that data was prepared to be exfiltrated, but no evidence it actually left. Did I write that down correctly ?"
Mr. Henry: "Yes"
Mr. Stewart of Utah: "And, in this case, the data I am assuming you're talking about is the email as well as everything else they may have been trying to take."
Mr. Henry: "There were files related to opposition research that had been conducted."
Mr. Stewart of Utah: "Okay. What about the emails that everyone is so, you know, knowledgeable of ? Were there also indicators that they were prepared but not evidence that they actually were exfiltrated ?"
Mr. Henry: "There's not evidence that they were actually exfiltrated. There's circumstantial evidence --"
Mr. Stewart of Utah: "Okay"
Mr. Henry: "- but no evidence that they were actually exfiltrated. But let me also state that if somebody was monitoring an email server, they could read all the email." (p. 74 / 75)

Interview transcripts of Shawn Henry at the House Committee on Intelligence on December 5, 2017

In addition, Hillary Clinton had used a private email server in her private office in Chappaqua, New York for official State Department matters and even had invited Google in 2012 - covering the US embassy in Benghazi attacks timeline - to manage her personally official email account, most likely in order to circumvent the obligation to have her official government conversations backed up and available to the public. Her private server in Chappaqua was running a Windows email management software.

On top of all that, one does not need to have the eyes of an eagle to see the clearly questionable words of former FBI Director James Comey when asked in January 2017 in the US Senate about the DNC Servers and Crowdstrike:

Comey: "We prefer to get access to the original device or server that's involved, it's the best evidence."
Senator: "Were you given access to do forensics on those servers ?"

> **Comey**: "We were not, a highly respected private company [Crowdstrike] eventually got access and shared with us what they saw there."
> **Senator**: "Is that typically the way the FBI would prefer to do the forensics or would you prefer to feel and see the server yourself?"
> **Comey**: "We'd always prefer to have access hands on ourselves if that's possible."
> **Senator**: "Do you know why you were denied access to the servers ?"
> **Comey**: "I don't know for sure. I don't know for sure."
> **Senator**: "Was there one request or multiple requests ?"
> **Comey**: "Multiple requests at different levels and, ultimately, what was agreed to is that the private company would share with us what they saw."
>
> (Ex-FBI Director James Comey at a hearing in the US Senate on January 10, 2017)

It seems as if the DNC was in charge of the FBI in 2016, not the Department of Justice or the US Congress and/or the US Senate. The entire DNC saga could be filed under the folder 'Massive Corruption', if there would not be US President Donald Trump's famous phone call with the newly elected Ukrainian President Zelensky on July 25, 2019, in which the US president mentioned Crowdstrike in particular:

> I would like you to do us a favor though because our country has been through a lot and Ukraine knows a lot about it. I would like you to find out what happened with this whole situation with Ukraine, **they say Crowdstrike**... I guess you have one of your wealthy people... **The server, they say Ukraine has it**. There are a lot of things that went on, the whole situation...I would like to have the Attorney General call you or your people and I would like you to get to the bottom of it. As you saw yesterday, that whole nonsense ended with a very poor performance by a man named Robert Mueller, an incompetent performance, but they say a lot of it started with Ukraine.
>
> (US President Donald Trump in a phone conversation from July 25, 2019 with the President of the Ukraine, Zelensky)

Soon after, hell broke out among mostly US Democratic politicians in the US Congress and who seriously intended to impeach the US president over these spicy words - and regarding some related to Joe Biden's corruption in the Ukraine - in his otherwise appropriate and regular phone call with Zelensky. The impeachment theatre did not last long, it was finally dismissed in the US Senate in early 2020 and rendered a supra-partisan endeavour when all Republicans in the US Congress rejected it there as well.

There may be no other explanation than that the Ukraine indeed has a digitally mirrored copy of that DNC server somewhere. With possibly contagious materials on it. Eagles can see that clearly from high above and far away.