CrowdStrike was behind Guccifer 2.0 Persona

CrowdStrike CTO Dmitri Alperovitch probably personally operated Guccifer 2.0

Guccifer 2.0

Guccifer 2.0 (G2) was not a persona created by Russian intelligence because Russian intel had nothing to do with the exfiltration and the publication of the internal documents of the DNC, DCCC, and John Podesta. Furthermore, Dmitri Alperovitch, co-founder and the chief technological officer of CrowdStrike, was probably (but not certainly) behind G2. CrowdStrike was a cybersecurity contractor hired by the DNC/DCCC law firm Perkins-Coie to assist it and/or its client DNC on cybersecurity matters in late April 2016. The fact that Perkins-Coie hired CrowdStrike to aid it in the contentious representation of the DNC was not known until very recently. The untruthful but publicly disseminated version of the events was that the DNC hired CrowdStrike in early May 2016 to remediate the DNC network breach. The CrowdStrike misattributed the breach to Russian intelligence and provided alleged "forensic evidence" to the FBI. G2 was not a Romanian hacker, and not a hacker at all.

Dmitri Alperovitch can be identified as the single individual behind the G2 persona by the classic combination of means, motives, and opportunities. Additionally, G2's linguistic and cultural traits are a match to Alperovitch. G2 persona shows affinity with CrowdStrike.

CrowdStrike Inc. wholly owned CrowdStrike Services, Inc. Shawn Henry, an executive assistant to the FBI Director Robert Mueller, has been President of CrowdStrike Services since he resigned from the FBI.

Contents

Means

As CrowdStrike's CTO, Dmitri Alperovitch had access to all the documents that G2 published. Further, Alperovitch was an expert in cyber-security and the internet, and he might have used that expertise and tools of the trade to copy those documents, to insert the "Russian fingerprints" onto some of the copied documents, and to create and operate the G2 personality without detection. In his first post on WordPress, G2 published some DNC documents intentionally modified using the Cyrillic template, which is well within Alperovitch means.

Motive

The DNC, its law firm Perkins-Coie, and their cyber-contractor, CrowdStrike, wanted to manufacture evidence that the DNC network had been hacked by Russian intelligence.

Opportunity

Since May 2016, Alperovitch knew almost everything that the DNC knew about the DNC's network breach or leak, the transfer of documents to WikiLeaks, and many related developments. The DNC coordinated with CrowdStrike all public relations related to the alleged breach. On June 14, 2016, CrowdStrike published a paper about the alleged breach just a few hours after Ellen Nakashima's article on the subject appeared in *The Washington Post*. Alperovitch had plenty of time to create accounts on WordPress and Twitter, to leave the "Russian fingerprints" on the documents, and to prepare the WordPress post.

Traits

Language

Based on http://g-2.space/guccifer2_corpus_raw.html, although there might be errors in attribution.

i. Alperovitch was born in the Soviet Union in 1980 and emigrated to the US around 1994-95. He is a native Russian speaker. G2 is a native Russian speaker.

ii. G2 and Alperovitch have a very good command of English.

iii. G2 and Alperovitch have an excellent command of business English.

iv. G2 claimed to be Romanian while leading an observer to believe that he was Russian. Maintaining consistency was hard; therefore, G2 writing exhibited two styles, causing people to believe that multiple individuals were behind G2.

The cultural and linguistic traits

The cultural and linguistic traits of G2 are consistent with those of Alperovitch, and they are inconsistent with most Americans and Russians.

v. In his first batch of documents, intentionally tainted with Cyrillic metadata, G2 applied a user name *Felix Edmundovich* [Dzerzhinsky] -- founder of the infamous NKVD, the predecessor of the KGB. Most people in the US don't even know that name. A Russian intelligence officer would not use it. But Alperovitch did know and might have used it to show off. G2 went through unusual steps to insert Cyrillic metadata, excluding the possibility it got there by accident[1]. It is hard to believe that Russian intel made such an obvious mistake, and it is even harder to think that anybody in Russia had such a user name.

vi. G2 made references to Rambo and Terminator – cultural icons in Russia of the early 1990s when Alperovitch was an impressionable 10-14 years old. Nobody thinks of them today.

vii. G2 used some expressions from British English, as was taught in the schools of the Soviet Union/Russia in the 1980's - early 1990's: an old-fashioned greeting "*How do you do?*" and saying "*a pupil at [middle] school*" instead of *a student*. Alperovitch attended middle school in Russia. Russian intelligence officers and younger people probably learn the American and do not use these expressions.

viii. G2 and Alperovitch[2] frequently use the word *cool*, especially when referring to technological subjects, and infrequently use other adjectives.

G2 & Insider's Knowledge

ix. It is not seriously disputed that G2 was not the hacker. G2 provided no evidence that he had hacked the DNC, no other hacker's credentials, and his statements about hacking suggest that he was not a hacker at all. Alperovitch is not a hacker, either.

x. In a FAQ posted on June 30, G2 twice mentioned the network clean-up operation, performed by CrowdStrike for the DNC on the weekend of June 12[3]. But this information was not public at that time. Thus, G2 was an insider. It is also remarkable how he wrote about it:

> "[Q] *And when did you get kicked out?*

[1] As admitted by ThreatConnect, CrowdStrike's partner and reseller (https://threatconnect.com/blog/guccifer-2-0-dnc-breach/)

[2] https://twitter.com/search?q=(from:DAlperovitch)%20cool&src=recent_search_click&f=live , https://twitter.com/search?q=(from:DAlperovitch)%20cool%20since:2015-09-01%20until:2017-06-01&src=typed_query&f=live

[3] http://www.esquire.com/news-politics/a49902/the-russian-emigre-leading-the-fight-to-protect-america/

> *[A] June 12, when they rebooted their system."*

It appears that Alperovitch forgot that the G2 persona has a huge ego and doesn't use self-deprecating humor. The G2 persona would have never written that he *got kicked out*. There is a pattern – G2 thought like Alperovitch and knew what Alperovitch knew.

No intelligence organization or group working for national intelligence would have announced to the world when the adversary terminated its operation!

xi. In communication with reporters, **G2 used the same IP addresses that CrowdStrike had earlier attributed to the putative hacker group**! A lot has been made from the fact that G2 communicated from a VPN in France, owned by the Russian company Elite VPN. This association, combined with the determination that G2 was not a hacker, was used by the CrowdStrike/DNC supporters to claim that G2 was a persona used by Russian intelligence. But Russian intelligence and any sophisticated hacking group are unlikely to re-use the same IP addresses[4] that they have used earlier. Russian intelligence wouldn't have used a Russian company's services when there are hundreds of alternatives. But Alperovitch had access to virtual machines with the same IP addresses and SSH fingerprints, because Elite VPN provided its services to anybody, and used it to reinforce the CrowdStrike/DNC narrative.

G2's Fondness of CrowdStrike

xii. The first G2 post on WordPress[5] shows amazing interest in and knowledge of CrowdStrike – unnatural for a foreign intelligence or hacking group targeting the DNC, but natural for Alperovitch. That post contains less than 300 words but mentions CrowdStrike four times! The post starts with "*Worldwide known cyber security company CrowdStrike announced …*" -- although CrowdStrike was an unknown little startup at that time[6]. It sounds like a promotion of CrowdStrike.

xiii. G2 used phrases and thoughts, unique to CrowdStrike at that time, like "*I had to pass from one machine to another inside the network to stay stealth*." This is not how hacking works. This imagery of Russian or Chinese hackers having a physical presence on the network and acting like real-world intruders or spies was a marketing gimmick unique to CrowdStrike.

[4] Or the same small range of IP addresses, or virtual machines with the same SSH fingerprints

[5] June 15th, https://guccifer2.wordpress.com/2016/06/15/dnc/

[6] "In 2016, CrowdStrike wasn't even in the Gartner Magic Quadrant for the EndpointProtection Platforms (pdf), meaning that it trailed well behind 18 included vendors. In 2017, CrowdStrike was included (pdf) only because "*The company grew its installed base rapidly in 2016 due to the publicity from high profile incident response work* [mentioned misattribution], *and the attractiveness of the CrowdStrike Overwatch service*", but not among the top 10 vendors. CrowdStrike Falcon was among 29 unranked vendors in the 2015-2016 Gartner Market Guide for Endpoint Detection and Response Solutions (pdf), which stressed that EDR solutions are not replacement for endpoint protection platforms." - https://defyccc.com/crowdstrike-crooked-and-shrill/

CrowdStrike also compared its activity on the DNC network to hand-to-hand combat with network "intruders." Thus, G2 was a CrowdStrike insider.

xiv. G2 praised CrowdStrike and used its imagery again in the interview with VICE: "*I had to go from one PC to another every week so CrowdStrike couldn't catch me for a long time. I know that they have cool intrusion detection system*"[7]. CrowdStrike had a crappy intrusion detection system. CrowdStrike was not even among the 18 top vendors included in the Gartner's Magic Quadrant for 2016[8]. Anyway, hackers do not care much about intrusion detection systems. And no Russian intelligence officer would engage in such chit-chat during an operation.

xv. G2 claimed that he had penetrated the DNC network through a vulnerability in NGP VAN – a rare voters database software, used only by a few Democrat/Socialist organizations. The use of NGP VAN software was a subject of conflict between the DNC and Bernie Sanders' campaign since December 2015. To analyze technical evidence and to help resolve the dispute, they invited CrowdStrike! CrowdStrike finished its work in April 2016, finding in favor of the DNC -- just a few weeks before being hired by Perkins-Coie. This is yet further evidence indicating a CrowdStrike insider (i.e., Alperovitch) was behind G2.

@DAlperovitch on Twitter

@DAlperovitch is a verified Twitter handle of Alperovitch. All the times below are CST.

- Alperovitch tweeted at 10:59 AM, June 16, 2016[9]: *'Vice: Guccifer 2.0' Is Likely a Russian Government Attempt To Cover Up Their Own Hack https://motherboard.vice.com/read/guccifer-20-is-likely-a-russian-government-attempt-to-cover-up-their-own-hack*[10] – his reaction to the article is too quick for somebody who has learnt about G2 existence less than 24 hours ago! Especially for a cyber-expert, who must be extra careful to maintain his reputation. The article's author replied to this tweet at 12. The article show time 12:25 PM, possibly the time of the latest update. The article claims are not evidence-based.
- Tweeted on August 10, 2016[11]: *"American intelligence agencies have virtually no doubt that the Russian government was behind the theft" #DNCLeak* -- and posted a link to a New York Times article; the quotes are in the original tweet. The NYT was not so sure: "*American intelligence*

[7] https://motherboard.vice.com/en_us/article/yp3bbv/dnc-hacker-guccifer-20-full-interview-transcript

[8] https://www.inisi.com/documents/magic-quadrant-for-endpoint-protection-platforms.pdf

[9] https://archive.fo/elXL7

[10] https://archive.fo/sA1Cd

[11] https://archive.fo/KXqIS

agencies have said they have 'high confidence' that the attack was the work of Russian intelligence agencies."[12]

- Replied to McFaul on December 29, 2016[13]: *Guccifer 2.0 actually admitted it providing the emails to Wikileaks. Shouldn't we take them at their word?* – another a **dead giveaway**! If Alperovitch believed that G2 was a front for Russian intelligence, why would he suggest taking G2's word on anything?

There is no alternative explanation

The official version that Russian intelligence was behind G2 is wrong for many reasons, only a few of which are stated above. G2 is not a Romanian hacker, as he claimed. G2 appears to be a Russia-born American and a CrowdStrike technical officer and stakeholder. Everything matches Alperovitch.

DCLeaks.com

The website DCLeaks.com hosted documents, covertly obtained from both Democratic and Republican parties. *The Smoking Gun* (https://thesmokinggun.com/documents/investigation/tracking-russian-hackers-638295, August 12, 2016) wrote:

> *And while Democrats may appear to be the only crime victims, TSG has learned that numerous prominent Republicans and GOP groups have also been targeted. These hacking victims include John McCain, Lindsey Graham, Michele Bachmann, various state Republican parties, as well as assorted GOP candidates, PACs, and consultants. …*
>
> *Since it seemed unlikely that hackers would target such a wide array of individual Republican web sites and email servers, TSG reviewed the DC Leaks "portfolio" in search of a common thread. That analysis revealed that the victimized campaigns, state parties, PACs, and businesses all contracted with the same Tennessee web hosting outfit. The firm, Smartech, and its parent, AirNet Group, are major providers of data services, call centers, and web hosting for scores of Republican clients. ...*
>
> *A review of the domains on a single Smartech server in Chattanooga shows that nine of the sites whose emails were compromised are housed on that server.*

The AirNet Group is located in **Chattanooga, TN**. When Dmitri Alperovitch immigrated to the US, he and his family settled in **Chattanooga, TN**. That might be a coincidence, although **Chattanooga, TN,** is a small town with a population of about 170,000.

[12] https://archive.fo/pREV0
[13] https://archive.fo/S76f1

Remarks

The FBI acknowledged that all the information it received about the alleged DNC breach it received from CrowdStrike.

The FBI had been warning the DNC of network intrusion by "CozyBear" or "FancyBear" long before the alleged discovery of the intrusion by CrowdStrike. See https://www.intelligence.senate.gov/sites/default/files/documents/FBI%20Response%20to%20Committee%20Questions%20for%20the%20Record.pdf.

Podesta email hack was likely unrelated from the DNC server emails exfiltration. The bulk of the emails, published by Wikipedia on the eve of the Democratic National Congress (late July 2016) were copied locally by a person familiar with the internal machinery of the DNC, possibly by Seth Rich.

On June 10-12, the DNC and CrowdStrike performed what looks like destruction of evidence on the computers in the main DNC office.

The G2 persona guccifer2.wordpress.com and @Guccifer_2 on Twitter is the same. Other putative G2 identifiers (such as guccifer20@aol.fr) might have been operated by other persons.

This paper adds to the information published by the author and other sources. Other useful sources of information:

https://defyccc.com/category/crowdstrike/

https://defyccc.com/category/dnc-leaks/

https://climateaudit.org/?s=dnc

https://g-2.space

https://theforensicator.wordpress.com/

https://krebsonsecurity.com/2017/08/blowing-the-whistle-on-bad-attribution/

https://loadedforguccifer.wordpress.com

Scott Ritter, a former Marine intelligence officer:

> https://medium.com/@HFINetwork/dumbstruck-how-crowdstrike-conned-america-on-the-hack-of-the-dnc-ecfa522ff44f
>
> https://medium.com/@scottritter/the-slam-dunk-that-isn-t-the-cia-russia-and-the-hacking-of-the-2016-presidential-election-82d2131b60af
>
> https://medium.com/@scottritter/exposing-the-man-behind-the-curtain-3b39472d28cc

Leo Goldstein

contact@defyccc.com

Texas, USA

July 2020