A BUSY DAY FOR THE BEARS

Yesterday, there were three arguably big events associated with stolen records alleged to have ties to Russia's GRU.

Simon Biles treats her ADHD

The first is the leak, by a group explicitly calling itself Fancy Bear (though the hack was once tied to Polish Anonymous), of anti-doping agency records showing the Williams sisters and Simone Biles all got approval for and took drugs on a list of otherwise banned substances. While there are no allegations of impropriety — indeed, Biles explained that in her case the exception involved treating ADHD — the story got covered by the major international press, including the Beeb, NBC, and NYT.

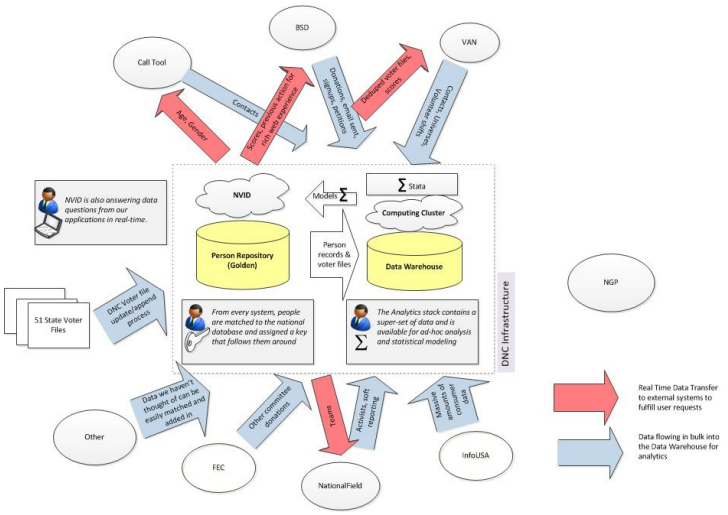
Colin Powell rants

The second alleged-Bear event is the release of Colin Powell emails, obtained by DC Leaks, to The Intercept, BuzzFeed, and Politico. The emails include quite recent ones, including one from August 26. Powell now uses GMail, suggesting his emails should be harder to hack than (for example) his State emails on AOL or emails run on a private server. Whether you worry about Russian influence or not, this hack is quite newsworthy.

There are embarrassing emails with Powell asserting that "Everything HRC touches she kind of screws up with hubris," as well as emails with Powell complaining about Trump's racism and the press' stoking of it.

The emails are not limited to election-related ones, either. They also include correspondence between Powell and Jack Straw and how the Chilcot report got buried in all the Brexit news.

Guccifer 2 goes mainstream



Finally, there was the "appearance" at a security conference by Guccifer 2.0, the guy who has released the DNC emails that gave the Democrats an excuse to force Debbie Wasserman Schultz's to resign, though they had been looking for an excuse for some time.

In point of fact, Guccifer 2.0 didn't appear in person at the conference. Rather, he sent a speech which got read at the conference, with the transcript released to journalists. The speech focused on the negligence of software companies in security. Guccifer went on for several paragraphs about the power and sloppiness of tech companies, arguing they were to blame for hacks.

> The next reason, and the crucial one, is software vulnerability. Tech companies hurry to finish the work and earn money. So they break development cycle very often omitting the stage of testing. As a result, clients have raw products installed on their systems and networks with a great number of bugs and holes.
>
> Fourth. It's well known that all large companies look forward to receiving governmental contracts. They develop governmental websites, communication systems, electronic voting systems, and so on and have their products installed to critical infrastructure objects on

> the national level.
>
> They are aggressively lobbying their interests. You can see it at the diagram that they spent millions of dollars for lobbying. That doesn't mean they will produce better software. That means they will get even more money in return.

Then he returned to a claim he has made on two earlier occasions: that he hacked DNC via a vulnerability in VAN.

> So, what's the right question we should ask about cyber crime?
>
> Who hacked a system?
>
> Wrong. The right question is: who made it possible that a system was hacked? In this regard, what question should you ask me?
>
> How I hacked the DNC???
>
> Now you know this is a wrong question. Who made it possible, that I hacked into the DNC? This is the question. And I suppose, you already know the answer. This is NGP VAN Company that operates the DNC network. And this is its CEO Stu Trevelyan who is really responsible for the breach.
>
> Their software is full of holes. And you knew about it even before I came on stage.
>
> You may remember Josh Uretsky, the national data director for Sander's presidential campaign. He was fired in December, 2015 after improperly accessing proprietary data in the DNC system. As it was agreed, he was intentionally searching for voter information belonging to other campaigns.
>
> However, he is not to blame. The real

> reason voter information became available for non-authorized users was NGP VAN's raw software which had holes and errors in the code. And this is the same reason I managed to get access to the DNC network. Vulnerabilities in the NGP VAN software installed on its server which they have plenty of. Shit! Yeah?
>
> This scheme shows how NGP VAN is incorporated in the DNC infrastructure.

One of two schemes released with the speech appears above.

Now, Guccifer's allegation — tying vulnerabilities in the VAN software to his own hack — could be newsworthy. Recall, after all, that one excuse the Bernie staffer gave for nosing around Hillary's side of VAN was that Sanders' own data had been compromised earlier that year. Importantly, Guccifer's persistent focus on VAN, which was a signature moment in Sanders' voters disillusionment with the DNC conduct in the election, would provide an alternative motive for this hack rather than just a Putinesque plot to tamper with Hillary's election.

Thing is, there's nothing in the materials released on VAN that indicates any particular vulnerability (though the dump does include some dated information on DNC's computer security): effectively Guccifer makes an allegation but — at least from what I've seen and heard from a few people who know security better — doesn't deliver the goods.

Indeed, while there are documents acknowledging the kind of pay-to-play appointments for big donors that both parties practice, and some other financial data that I suspect may prove more interesting with further scrutiny, there's nothing really newsworthy in this dump. It seems to be interesting primarily to Bernie diehards, not the press generally, which is rightly more interested by the Powell emails.

Which, again, emphasizes how much Guccifer has been feeding Bernie diehards, either out of his own motivation or his handler's. It is worth noting that while Guccifer claims to oppose Trump's policies, he did say this about Sanders: "I have nothing to say about Bernie Sanders. It seems he never had a chance to win the nomination as the Democratic Party itself stood against him!"

Why stomp on the Bears other big blasts?

Which has me wondering about yesterday generally. If someone is orchestrating all these leaks, why have Guccifer "give a speech" on the same day as two highly managed releases, especially given that Guccifer failed to deliver the goods? Indeed, why invite Guccifer to, or have him accept an invitation from, a pretty staid security conference at all?

And what is the role of Darren Martyn, a LulzSec Irish hacker who was indicted along with Jeremy Hammond but apparently never extradited. He's apparently the one who read Guccifer's speech. Which raises all sorts of questions about Guccifer's ties to the Anon group of hackers, or maybe also to what Martyn has been doing since he was indicted in the US.

Let me just close with an observation.

The Democrats have, rightly, been worried about what Guccifer will release closer to the election; I've heard specific concerns from connected Dems that he will release far more damning financial documents. The FBI, too, appears uncertain whether the set of documents Guccifer has is the same that the GRU-related hackers are believed to have spied on at the DNC. Thus, both the DNC and FBI would love to do something to make Guccifer show more of his hand.

Before this hack, we were all just waiting to see what Julian Assange, who is clearly maximizing damage to Hillary, will drop next.

And instead, by inviting Guccifer to appear at a conference, someone got Guccifer to drop an additional 700 MB of files while everyone is busy looking at the Powell emails.