TWO (THREE, FOUR?) DATA POINTS ON DNC HACK: WHY DOES WIKILEAKS NEED AN INSURANCE FILE?

Actually, let me make that three data points. Or maybe four.

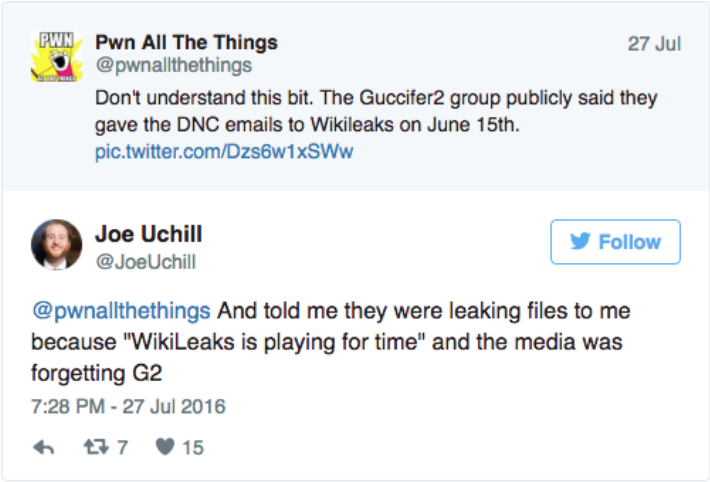
First, Reuters has reported that the DCCC has also been hacked, with the hacker apparently believed to be the same entity (APT28, also believed to be GRU). The hackers created a spoof version of ActBlue, which donors use to give money to campaigns.

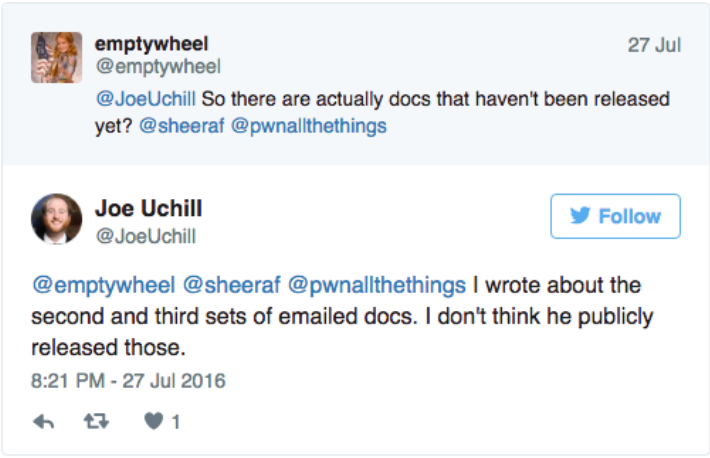
> The intrusion at the group could have begun as recently as June, two of the sources told Reuters.
>
> That was when a bogus website was registered with a name closely resembling that of a main donation site connected to the DCCC. For some time, internet traffic associated with donations that was supposed to go to a company that processes campaign donations instead went to the bogus site, two sources said.
>
> The sources said the Internet Protocol address of the spurious site resembled one used by Russian government-linked hackers suspected in the breach of the DNC, the body that sets strategy and raises money for the Democratic Party nationwide.

That would mean hackers were after either the donations themselves, the information donors have to provide (personal details including employer and credit card or other payment information), or possibly the bundling

information tied to ActBlue.

Second, Joe Uchill, who wrote one of the stories — on two corrupt donors to the Democratic Party — that preceded both publication at the Guccifer 2 site and Wikileaks, said Guccifer gave him the files for the story because Wikileaks was dawdling in publishing what they had.





Guccifer posted some of the documents Uchill used here.

This detail is important because it says Julian Assange is setting the agenda (and possibly, the decision to fully dox DNC donors) for the Wikileaks release, and that agenda does not perfectly coincide with Guccifer's (which is presumed to be a cut-out for GRU).

As I've noted, Wikileaks has its own beef with Hillary Clinton, independent of whom Vladimir Putin might prefer as President or any other possible motive for Russia to do this hack.

Now consider this bizarre feature of several

high level leak based stories on the hack: the claim of uncertainty about how the files got from the hackers to Wikileaks. This claim, from NYT, *seems* bizarrely stupid, as Guccifer and Wikileaks have both said the former gave the latter the files.

> The emails were released by WikiLeaks, whose founder, Julian Assange, has made it clear that he hoped to harm Hillary Clinton's chances of winning the presidency. It is unclear how the documents made their way to the group. But a large sampling was published before the WikiLeaks release by several news organizations and someone who called himself "Guccifer 2.0," who investigators now believe was an agent of the G.R.U., Russia's military intelligence service

The claim seems less stupid when you consider these two cryptic comments from two equally high level sourced piece from WaPo. In a story on FBI's certainty Russia did the hack(s), Ellen Nakashima describes that the FBI is less certain that Russia passed the files to Wikileaks.

> What is at issue now is whether Russian officials directed the leak of DNC material to the anti-secrecy group WikiLeaks — a possibility that burst to the fore on the eve of the Democratic National Convention with the release of 20,000 DNC emails, many of them deeply embarrassing for party leaders.
>
> The intelligence community, the officials said, has not reached a conclusion about who passed the emails to WikiLeaks.
>
> "We have not drawn any evidentiary connection to any Russian intelligence service and WikiLeaks — none," said one U.S. official. Doing so will be a challenge, *in part because the material*

> *may not have been passed electronically*. [my emphasis]

The claim appears this way in a more recent report.

> The bureau is trying to determine whether the emails obtained by the Russians are the same ones that appeared on the website of the anti-secrecy group WikiLeaks on Friday, setting off a firestorm that roiled the party in the lead-up to the convention.
>
> The FBI is also examining whether APT 28 or an affiliated group passed those emails to WikiLeaks, law enforcement sources said.

Now, the doubts about whether the files were passed electronically is thoroughly fascinating. I assume the NSA has Assange — and potentially even the Wikileaks drop — wired up about 100 different ways, so the questions about whether the files were passed electronically may indicate that they didn't see them get passed in such a fashion.

Add in the question of whether they're even the same emails! We know the DCCC hack is targeting donor information. The Wikileaks release included far more than that. Which raises the possibility GRU is only after donor information (which is part of, but just one part of, what Guccifer has released).

But then there's this detail. On June 17, Wikileaks released an insurance file — a file that will be automatically decrypted if Wikileaks is somehow impeded from releasing the rest of the files. It has been assumed that the contents of that file are just the emails that were already released, but that is almost certainly not the case. After all, Wikileaks has already released further documents (some thoroughly uninteresting voice mails that nevertheless further impinge on the privacy of

DNC staffers). They have promised still more, files they claim will be more damaging. ~~Indeed, Wikileaks claims there's enough in what they have to indict Hillary, though such claims should always be taken with a grain of salt.~~ Correction: That appears to have been a misunderstanding about what Assange said about the previously released State emails.

But here's the other question.

There's no public discussion of Ecuador booting Assange from their Embassy closet (though I'm sure they're pretty tired of hosting him). His position — and even that of Wikileaks generally — seems pretty stable.

So why does Assange believe they need an insurance file? I don't even remember the last time they issued an insurance file (update: I think it was when they released an insurance file of Chelsea Manning's documents). So is there someone else in the process that needs an insurance file? Is there someone else in the process that would use the threat of full publication of the files (which presumably is going to happen anyway) to ensure safety?

I'll leave that question there.

That said, these data point confirms there are *at least* two players with different motivations: Wikileaks, and the Russian hackers. But the FBI isn't even certain whether the files the Russians took are the same that Wikileaks released, which might suggest a third party.

Meanwhile, James Clapper (who thankfully is willing to poo poo claims that hacks that we ourselves do are unique) seems very interested in limiting the panic about this hack.

Update: Oh! I forgot this fifth data point. This absolutely delightful take-down of Debbie Wasserman Schultz includes this claim that Wikileaks has malware in its site, which I've asked around and doesn't seem to be true.

> Staff members were briefed in a Tuesday

> afternoon meeting in Washington that their personal data was part of the hack, as were Social Security numbers and other information for donors, according to people who attended. Don’t search WikiLeaks, they were told — malware is embedded throughout the site, and they’re looking for more data.

Who told the DNC Wikileaks is releasing malware, and why?

Update: here’s what the malware claim is about: When it posted the “AKP emails,” WL either added or did not remove a bunch of malware included in those emails, and as a result, that malware is still posted at the site. That is, the malware is associated with a separate set of documents available at the site.