TWO CAUTIONS ON THE RUSSIAN HACK OF RNC SERVERS

I followed the Senate Intelligence Committee Hearing on the Russian hacking via Twitter on the train.

From what I can tell, there was a big stink about the fact that Russia hacked, but did not release, information from Republicans (aside from Colin Powell, but he appears to have been kicked out of the Republican party as far as hacking victims go). In addition, there was some befuddlement about the fact that the Russians hacked an old RNC server. Here's WSJ's coverage of it.

There are two details in the public domain that may go some way to explain the discrepancy.

First, as I pointed out here, you should distinguish between FSB and GRU when discussing these things (something the head spooks have been really sloppy about doing, helped in part by combining two different hacking groups into one Grizzly Steppe). As far as we know, FSB hacked the DNC for months, but never released anything. Whereas GRU was only in the DNC server for a few months, but then passed on the documents they stole to be leaked.

From what I've read online (I'll check later) it's possible FSB hacked the RNC, but – as they are thus far believed to have done with the DNC too – simply sat on the documents.

In addition, this report from SecureWorks (which is one of the more measured security contractor reports on the hack), which tracked which entities and people were targeted by fake GMail links, reveals that key Republican entities don't use GMail and therefore would have had to have been hacked via other means.

> Republican party or the other U.S.

> presidential candidates whose campaigns were active between mid-March and mid-May: Donald Trump, Bernie Sanders, Ted Cruz, Marco Rubio, and John Kasich. However, the following email domains do not use Google mail servers and may have been targeted by other means:
>
> - *gop.com — used by the Republican National Committee*
> - *donaldjtrump.com — used by the Donald Trump campaign*
> - *johnkasich.com — used by the John Kasich campaign*
>
> Access to targets' Google accounts allows TG-4127 to review internal emails and potentially access other Google Apps services used by these organizations, such as Google Drive.

Of course, phishing is phishing, and if you can make an expert fake of a Gmail login, you can do the same for some other login. But one major source of information on the hack of Democrats (though not necessarily on the DNC, given that it was not using Gmail when the report was done) has a gap for the campaigns that didn't use Gmail.

Presumably, the IC has more than just a bunch of clicked fake Gmail links to go on, though, including awareness of other, non-Gmail phishing campaigns.

That said, details like this are one of the reasons top spooks would raise confidence in their Trust Us claims by being rigorous about what they're actually referring to.