RUSSIA HACKED THE DNC. BUT WHAT, SPECIFICALLY, DID GRU DO?

I'm working on a series of posts to point out existing holes in the claim that Russia hacked the DNC. None of them mean I am yet convinced it is someone besides Russia. But there are holes in the story that no one wants to acknowledge. And those who want to argue the case is solid would do well to at least answer them. In this one, I want to point to a curious piece of evidence in a necessary part of the evidence: how GRU is alleged to have hacked the DNC.

You need to separate attribution of FSB's hack of the DNC from GRU's hack of the DNC

One thing a lot of people don't realize about the Russian hack attribution is there's some slippage in the argument.

There are two groups in question: APT 29, which has been publicly associated with FSB, and APT 28, which has been publicly associated with GRU. As I laid out here, those two groups must be kept separate, because the story is that these two groups did different things: FSB hung around DNC's servers for months and stole a lot of information, but never leaked it. That's the kind of stuff intelligence services do all the time, including our own. Our government has no reason to make a case against that — which is unwanted but nevertheless normal espionage — because they do it too, such as when, in 2012, they stole communications between then Mexican presidential candidate Enrique Peña Nieto and his closest allies.

GRU, by contrast, was believed to have been in DNC's servers briefly — and John Podesta's Gmail account even more briefly — but to have, in that time, stolen the documents that ultimately made their way to Wikileaks. That's the action that was deemed newly beyond the pale (even if the US has probably had documents leaked to Wikileaks itself).

In a sense, then, only the APT 28 attribution matters, because that's the entity that is believed to have been involved in hacking *and* leaking; that's the entity believed to have done things that might have affected the outcome of the election.

But people have long either intentionally or unknowingly conflated the two, claiming that "Russia" hacked the DNC. If FSB hacked the DNC, the claim is true, but that doesn't prove that Russia is behind the tampering in the election, because unless you prove that GRU is APT 28, then the stuff you're bugged about hasn't been properly attributed.

I've come to distrust the claims of anyone who has paid close attention to this that doesn't assiduously maintain the distinction between the APT 29 and APT 28 hacks.

The Administration's creation of Grizzly Steppe conflates APT 29 and APT 28 more than ever before

So, reports on this hack should scrupulously avoid conflating the APT 29 hack and the APT 28 hack. But Obama's response last month did the opposite. Whereas every infosec outfit treats APT 28 (which CrowdStrike calls Fancy Bear) and APT 29 (which CrowdStrike calls Cozy Bear) as distinct entities (regardless of how confident they are that one or the other are

Russian intelligence), and even though within the reports the Administration retained this distinction, the materials released by the Obama Administration invented an entirely new entity: Grizzly Steppe.

Get it? This entity is not a soft and cuddly Cozy Bear or an entirely distinct suave Fancy Bear anymore. Put the two together and you get a Grizzly Bear!

RAWRRRRRRR!

Aside from just the fact *that* the Administration did this (which would permit them to say, correctly, that Russia hacked the DNC even if they were less certain about GRU, though I don't think they are), there are two other interesting aspects of this conflation in their package of sanctions.

First, as I noted here, the Administration sanctioned FSB as well GRU. That's weird because our intelligence community believes what FSB did is solidly within the norms of intelligence gathering. It's possible the IC has some evidence that FSB did something to facilitate this operation that is not yet public. But the only explanation the sanctioning document offers is that, "The Federal Security Service (a.k.a. Federalnaya Sluzhba Bezopasnosti) (a.k.a FSB) assisted the GRU in conducting the activities described above."

The other notable thing about the Obama package is the differential language the Joint Analysis Report uses to describe the APT 29 and APT 28 hacks, which I pointed out here.

> In summer 2015, an APT29 spearphishing campaign directed emails containing a malicious link to over 1,000 recipients, including multiple U.S. Government

> victims. APT29 used legitimate domains, to include domains associated with U.S. organizations and educational institutions, to host malware and send spearphishing emails. In the course of that campaign, APT29 successfully compromised a U.S. political party. At least one targeted individual activated links to malware hosted on operational infrastructure of opened attachments containing malware. APT29 delivered malware to the political party's systems, established persistence, escalated privileges, enumerated active directory accounts, and exfiltrated email from several accounts through encrypted connections back through operational infrastructure.
>
> In spring 2016, APT28 compromised the same political party, again via targeted spearphishing. This time, the spearphishing email tricked recipients into changing their passwords through a fake webmail domain hosted on APT28 operational infrastructure. Using the harvested credentials, APT28 was able to gain access and steal content, likely leading to the exfiltration of information from multiple senior party members. The U.S. Government assesses that information was leaked to the press and publicly disclosed.

I admit I may be over-reading these differences. But there is a difference in the certitude with which this report speaks of the APT 29 hack and the APT 28 hack. Regarding the former, the report describes how APT 29 stole the documents: it "exfiltrated email from several accounts through encrypted connections back through operational infrastructure." And whereas the report affirmatively says APT 28 "was able to gain access and steal content," it seems far less sure about how much data it stole, saying the hack "likely [led] to the exfiltration of

information from multiple senior party members." Maybe that means it's likely APT 28 stole documents from more than one person; maybe that means it is likely they exfiltrated documents period. But remember, matching precisely what documents GRU stole to those Wikileaks released was one of the things the FBI was still working on a month and a half after the DNC hack.

> 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.

That's just one of several piece of evidence that suggests they don't have (or at least didn't have) as clear forensics on.

One more note about the JAR report: It makes no mention of Podesta. Again, we should not draw any conclusions for that, as they may have just chosen to focus on the DNC (which people often forget is a distinct entity from Hillary's campaign). But, as I hope to show in a follow-up post, the IC may have either less information — or perhaps even some sheepishness — about the Podesta leak, which is remarkable because that's the actual hack for which there is the best evidence tying it to APT 28.

The Administration materials endorse some, but not all, of what infosec companies have

published

Which brings me to a point I've made before but deserves more focus. In the introduction to the JAR, the Administration has this to say about the great work infosec companies have done about this hack.

> A great deal of analysis and forensic information related to Russian government activity has been published by a wide range of security companies. The U.S. Government can confirm that the Russian government, including Russia's civilian and military intelligence services, conducted many of the activities generally described by a number of these security companies.

It confirms that Russia's intelligence services have indeed done "many of the activities" described by "a number of these security companies." That's not a confirmation that Russia's spooks have done all the things alleged by all the security companies. Indeed, it seems to suggest that the infosec reports are wrong on some (perhaps very minor) points. We just don't know which ones those are.

What were FSB and GRU doing hacking the same target anyway?

Which brings me to an important side discussion, one for which everyone has an answer but about which there is no agreement.

While FSB and GRU have been portrayed as adversarial intelligence agencies (perhaps in the way that FBI and CIA don't always get along, sometimes to spectacular effect), it's not actually normal for them to be hacking the same target. The original CrowdStrike report on the hack noted that the two groups of hackers appeared not to be coordinating as they rooted

around DNC's servers.

> At DNC, COZY BEAR intrusion has been identified going back to summer of 2015, while FANCY BEAR separately breached the network in April 2016. We have identified no collaboration between the two actors, or even an awareness of one by the other. Instead, we observed the two Russian espionage groups compromise the same systems and engage separately in the theft of identical credentials. While you would virtually never see Western intelligence agencies going after the same target without de-confliction for fear of compromising each other's operations, in Russia this is not an uncommon scenario. "Putin's Hydra: Inside Russia's Intelligence Services", a recent paper from European Council on Foreign Relations, does an excellent job outlining the highly adversarial relationship between Russia's main intelligence services – Федеральная Служба Безопасности (FSB), the primary domestic intelligence agency but one with also significant external collection and 'active measures' remit, Служба Внешней Разведки (SVR), the primary foreign intelligence agency, and the aforementioned GRU. Not only do they have overlapping areas of responsibility, but also rarely share intelligence and even occasionally steal sources from each other and compromise operations. Thus, it is not surprising to see them engage in intrusions against the same victim, even when it may be a waste of resources and lead to the discovery and potential compromise of mutual operations.

It explains this away by the competition between the agencies. Still: note that according to CrowdStrike, there were two groups of Russians sniffing through the DNC servers that appeared

unaware of each other's presence.

A competing infosec company, Fire Eye, has come up with a completely different explanation for the presence of FSB and GRU in the same servers. It deems that proof of superior coordination.

> According to data provided for this article by the private cybersecurity company, FireEye, two separate but coordinated teams under the Kremlin are running the campaign. APT 28, also known as "FancyBear," has been tied to Russia's foreign military intelligence agency, the Main Intelligence Agency or GRU. APT 29, aka "CozyBear," has been tied to the Federal Security Service or FSB. Both have been actively targeting the United States. According to FireEye, they have only appeared in the same systems once, which suggests a high level of coordination — a departure from what we have seen and come to expect from Russian intelligence.

Frankly, I'm agnostic about what the answer to this question might be, and find either one plausible. Or, it's possible we should pay more attention to how unusual it is to have FSB and GRU digging in the same holes and think about whether it might, instead, tell us something else about who did this hack. But it is a datapoint that any theory of the hack should at least acknowledge and try to explain. Most don't.

Why is GRU using open source tools?

All of which is my long-winded explanation for why I went back and re-read specifically what CrowdStrike said about APT 28 (at a time, we now know but didn't then, CrowdStrike only had "medium" confidence that the APT 28 hackers of DNC were GRU). It made me realize why the stakes on the APT 28 tool X-Agent — which is not the

only tool associated with APT 28 — are so high.

> FANCY BEAR adversary used different tradecraft, deploying X-Agent malware with capabilities to do remote command execution, file transmission and keylogging. It was executed via rundll32 commands such as:
>
> *rundll32.exe "C:\Windows\twain_64.dll"*
>
> In addition, FANCY BEAR's X-Tunnel network tunneling tool, which facilitates connections to NAT-ed environments, was used to also execute remote commands. Both tools were deployed via RemCOM, an open-source replacement for PsExec available from GitHub. They also engaged in a number of anti-forensic analysis measures, such as periodic event log clearing (via wevtutil cl System and wevtutil cl Security commands) and resetting timestamps of files.

So after a longer section describing APT 29's tools (which we now know, but which was not known then, were the less important part of the hack), Crowdstrike describes APT 28's use of X-Agent and X-Tunnel (the latter of which I may come back to), but then also explains that these hackers deployed the APT 28 tools via an open source tool available on GitHub.

I'm no tech wizard, but this detail seems to beg some explanation, as it is awfully curious to have GRU resorting to an outdated open source tool to hack an American political party.

None of this is definitive. None of it changes my inclination that Russia probably is behind the APT 28 hack of the DNC (and, even more convincingly, behind the hack of John Podesta). But these are some details that deserve more attention amid the claims that all the case against GRU (as distinct from Russia) is rock solid.