THE TWO INTELLIGENCE AGENCY THEORY OF HANDING TRUMP THE ELECTION

There has been a lot written about Russian intelligence agencies allegedly hacking the DNC server and — by leaking it — attempting to influence the election. Some observers have, based on that assumption, called the hack an act of war.

I'm agnostic on whether Russian intelligence did one or both of the hacks, in part for reasons I'm still working through. I'm even more skeptical of some of the claims made about Russia's motivations in launching this attack to put Trump in the presidency (which is not to say Trump wouldn't be horrible for a whole slew of other reasons); on that topic, see this Josh Marshall piece and a fact-checking of it. And I'm frankly amused that, after using several other outlets for publicity and to release documents, the hacker(s') cooperation with WikiLeaks (which irresponsibly released credit card and social security information on Democratic donors, but which almost certainly had its donors investigated by DOJ with the heavy involvement of Clinton after Wikileaks published the State cables) itself is a sign of Russian involvement. Does Russia also run The Hill, the last outlet used by DNC hacker(s)?

In short, there are a whole bunch of claims being made, all serving a narrative that Putin is playing in our elections, with little scrutiny of how you get from one level (what have been described as two separate hacks) to another (to Guccifer 2, to help Putin) to another (with the help of Wikileaks). It's like the Rosetta stone of Cold War 2.0 paranoia. All may be true, but the case is thus far still fragile.

This post, from Thomas Rid, is the most sober analysis of the claim that Russian hackers hacked the DNC. Even still, there are some logical problems with the analysis (that are sadly typical of the underlying cybersecurity consultants). Take these two passages, for example.

> The DNC knew that this wild claim would have to be backed up by solid evidence. A*Post* story wouldn't provide enough detail, so CrowdStrike had prepared a technical report to go online later that morning. The security firm carefully outlined some of the allegedly "superb" tradecraft of both intrusions: the Russian software implants were stealthy, they could sense locally-installed virus scanners and other defenses, the tools were customizable through encrypted configuration files, they were persistent, and the intruders used an elaborate command-and-control infrastructure. So the security firm claimed to have outed two intelligence operations.
>
> [snip]
>
> The metadata in the leaked documents are perhaps most revealing: one dumped document was modified using Russian language settings, by a user named "Феликс Эдмундович," a code name referring to the founder of the Soviet Secret Police, the Cheka, memorialised in a 15-ton iron statue in front of the old KGB headquarters during Soviet times. The original intruders made other errors: one leaked document included hyperlink error messages in Cyrillic, the result of editing the file on a computer with Russian language settings. After this mistake became public, the intruders removed the Cyrillic information from the metadata in the next dump and carefully used made-up

> user names from different world regions, thereby confirming they had made a mistake in the first round.

They argue (based in part on CrowdStrike's claims of expertise) both that the hacker(s) were really sophisticated and that they deliberately adopted a Russian name but accidentally left Russian metadata in the files. Particularly with regards to the Russian metadata, you don't both adopt a notable Russian spook's ID while engaging in a false flag but then "accidentally" leave metadata in the files, although the second paragraph here pertains to Guccifer 2 and not the Crowdstrike IDed hackers.

If Guccifer were a true false flag, he might well be pretending to be Russian to hide his real identity.

Add to that this post (from June), which notes some confirmation bias in the way that FireEye first attributed APT 28 (which CrowdStrike believes to be GRU, Russia's military intelligence).

> I chose to look at Fancy Bear (APT28 in FireEye's ecosystem). The most comprehensive report on that threat actor was written by FireEye and released last October, 2014 so I started with that. To my surprise, the report's authors declared that they deliberately excluded evidence that didn't support their judgment that the Russian government was responsible for APT28's activities:
>
> > *"APT28 has targeted a variety of organizations that fall outside of the three themes we highlighted above. However,* ***we are not profiling all of APT28's targets with the same detail because they are not particularly indicative of a specific sponsor's interests****."*

> *(emphasis added)*
>
> That is the very definition of confirmation bias. Had FireEye published a detailed picture of APT28's activities including all of their known targets, other theories regarding this group could have emerged; for example, that the malware developers and the operators of that malware were not the same or even necessarily affiliated.

And even if you took the underlying report as definitive, APT 28 was primarily focused on military targets, which by itself ought to raise questions about why they'd go after the DNC.

Malware	Targeting	Russian Attributes
Evolves and Maintains Tools for Continued, Long-Term Use • Uses malware with flexible and lasting platforms • Constantly evolves malware samples for continued use • Malware is tailored to specific victims' environments, and is designed to hamper reverse engineering efforts • Development in a formal code development environment **Various Data Theft Techniques** • Backdoors using HTTP protocol • Backdoors using victim mail server • Local copying to defeat closed/air gapped networks	**Georgia & the Caucasus** • Ministry of Internal Affairs • Ministry of Defense • Journalist writing on Caucasus issues • Kavkaz Center **Eastern European Governments & Militaries** • Polish Government • Hungarian Government • Ministry of Foreign Affairs in Eastern Europe • Baltic Host exercises **Security-related Organizations** • NATO • OSCE • Defense attaches • Defense events and exhibitions	**Russian Language Indicators** • Consistent use of Russian language in malware over a period of six years • Lure to journalist writing on Caucasus issues suggests APT28 understands both Russian and English **Malware Compile Times Correspond to Work Day in Moscow's Time Zone** • Consistent among APT28 samples with compile times from 2007 to 2014 • The compile times align with the standard workday in the UTC + 4 time zone, which includes major Russian cities such as Moscow and St. Petersburg

To make the argument *based on targets* that APT 28 is GRU you need to do even more adjusting of motivation (though more recent APT 28 attributed attacks are more similar to this one).

But one reason I find the Rid piece sober and useful is it emphasizes something that has been ignored by much of the inflamed reporting. First, even CrowdStrike claims that DNC was hacked twice, by two different Russian entities, which did not appear to be coordinating during the hack. From the CrowdStrike report:

> 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.

And, as Rid points out, the proof that Guccifer is tied to Russia (it would be to GRU or APT 28 if the tie were real, so the less persistent of the two apparently unrelated hacks) is even less clear, though there still is a lot of circumstantial evidence.

> The evidence linking the Guccifer 2.0 account to the same Russian operators is

> not as solid, yet a deception operation—a GRU false flag, in technical jargon—is still highly likely. Intelligence operatives and cybersecurity professionals long knew that such false flags were becoming more common. One noteworthy example was the sabotage of France's TV5 Monde station on 9/10 April 2015, initially claimed by the mysterious "CyberCaliphate," a group allegedly linked to ISIS. Then, in June, the French authoritiessuspected the same infamous APT 28 group behind the TV5 Monde breach, in preparation since January of that year. But the DNC deception is the most detailed and most significant case study so far. The technical details are as remarkable as its strategic context.
>
> [snip]
>
> Other features are also suspicious. One is timing, as ThreatConnect, another security company, has pointed out in a useful analysis: various timestamps indicate that the Guccifer-branded leaking operation was prompted by the DNC's initial publicity, with preparation starting around 24 hours after CrowdStrike's report came out. Both APT 28 and Guccifer were using French infrastructure for communications. ThreatConnect then pointed out that both the self-proclaimed hacker's technical statements on the use of 0-day exploits as well as the alleged timeline of the DNC breach are most likely false. Another odd circumstantial finding: sock-puppet social media accounts may have been created specifically to amplify and extend Guccifer's reach, as UK intelligence startup Ripjar told me.
>
> Perhaps most curiously, the Guccifer 2.0 account, from the beginning, was not

> simply claiming to have breached the DNC network—but claiming that two Russian actors actually were *not* on the DNC network at the same time. It is common to find multiple intruders in tempting yet badly defended networks. Nevertheless the Guccifer 2.0 account claimed confidently, and with no supporting evidence, that the breach was simply a "lone hacker"—a phrasing that seems designed to deflect blame from Russia. Guccifer 2.0's availability to the journalists was also surprising, and something new altogether.
>
> The combative yet error-prone handling of the Guccifer account is in line with the GRU's aggressive and risk-taking organizational culture and a wartime mindset prevalent in the Russian intelligence community. Russia's agencies see themselves as instruments of direct action, working in support of a fragile Russia under siege by the West, especially the United States.

Now, again, I'm not saying the Russians didn't do this hack, nor am I dismissing the idea that they'd prefer Trump to Hillary. By *far* the most interesting piece of this is the way those with the documents — both the hackers and Wikileaks — held documents until a really awkward time for some awkward disclosures, with what may be worse to come.

But discussions that want to make the case should explain several things: Which of the two agencies alleged to have hacked DNC are behind the operation — or are they both, even though they weren't, at least according to the report that everyone is relying on without question, apparently cooperating? How certain can they be that the GRU is Guccifer, and if Guccifer is supposed to be a false flag why was it so incompetently done? What explains Guccifer's sort of bizarre strategy along the way, encompassing both Wikileaks (an obvious one) and

The Hill?

Again, I absolutely don't put this kind of thing beyond Putin. Russia has used hacking to influence outcomes of elections and authority in various countries in the past and the only thing new here is that 1) we wouldn't already be playing the other side and 2) we're big and can fight back. But the story, thus far, is more complex than being laid out.

Update: Here's an amusing debunking of a lot of the metadata analyses.

> Meanwhile, after the WaPo story hit the wires the "lone hacker" created his wordpress site and dropped dox as we say on the intertubes. Shortly after the drop people were inspecting, detecting, infecting, and making circles and arrows with captions on the back to describe what you were seeing! … And the conspiracy theory machine went into overdrive. Pwnallthethings made some good comments on the metadata in the dropped dox but really, concluding that this is a Russian disinformation operation from metadata stripped documents on the idea that the machine name was cyrillic for Felix Dzerzhinsky (Феликс Эдмундович) Really? Now that is fucking SOLID work man! Stellar! FUCK LET'S GO BOMB RUSSIA NOW!
>
> 
>
> **NAILED IT!**

> You know at least Crowdstrike has like actual data, ya know, C2's, malware, and shit like that. Anything else is totally speculative, I mean even more speculative than most attribution that these companies make with real data! Anyway, I took a look at the metadata on the documents and here is what I have found…
>
> - *Much of the data was stamped out in saving from format to format*
> - *Emails of users though were still embedded in the excel files*
> - *The word docs have no more metadata than the Iron Felix machine name save, which, gee, kinda leads one to wonder…*
> - *The image files have no metadata.. none.. niente clean.*
> - *Grizzli777 is just someone who pirates*
>
> Yep, not a lot to see there and people are hanging their collective hats on the deliberate placement of Феликс Эдмундович as the machine name to it's quite OBVIOUSLY being Mother Russia's exclusive secret services.
>
> *squint.. takes drag of cigarette*
>
> So here's my assessment…. Maybe Russia did it… OR Maybe this actor is the real thing and happens to want to take credit. The facts that this person(s) reads, writes, has, cyrillic on their machine and names it after the founder of the KGB is as reliable a means to

> saying it was Russia as it is to say that aliens built the pyramid because people just were fucking too stupid back then!