SANCTIONING GRU … AND FSB

While I was out and about today, President Obama rolled out his sanctions against Russia to retaliate for the Russian hack of Democrats this year. Effectively, the White House sanctioned two Russian intelligence agencies (GRU — Main Intelligence, and FSB —Federal Security Service), top leaders from one of them, and two named hackers.

In addition to sanctioning GRU, the White House also sanctioned FSB. I find that interesting because (as I laid out here), GRU has always been blamed for the theft of the DNC and John Podesta documents that got leaked to WikiLeaks. While FSB also hacked the DNC, there's no public indication that it did anything aside from collect information — the kind of hacking the NSA and CIA do all the time (and have done during other countries' elections). Indeed, as the original Crowdstrike report described, FSB and GRU weren't coordinating while snooping around the DNC server.

> 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.

Data provided by FireEye to War on the Rocks much later in the year suggested that the DNC hack was the only time both showed up in a server, which it took to mean the opposite of what Crowdstrike had, particularly high degree of 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.

The sanctioning materials offers only this

explanation for the FSB sanction: “The Federal Security Service (a.k.a. Federalnaya Sluzhba Bezopasnosti) (a.k.a FSB) assisted the GRU in conducting the activities described above.”

So I’m not sure what to make of the fact that FSB was sanctioned along with GRU. Perhaps it means there was some kind of serial hack, with FSB identifying an opportunity that GRU then implemented — the more extensive coordination that FireEye claims. Perhaps it means the US has decided it’s going to start sanctioning garden variety information collection of the type the US does.

But I do find it an interesting aspect of the sanctions.