THE NEW CYBER SANCTIONS

Even as Trump was working hard to get Russia admitted back into the G-7, Treasury was preparing new cyber sanctions against a number of "Russian" entities. This appears to be an effort to apply sanctions for activities exploiting routers and other network infrastructure (activities that the US and its partners engage in too) that US-CERT released a warning about in April.

> One of the designated entities in controlled by and has provided material and technological support to Russia's Federal Security Service (FSB), while two others have provided the FSB with material and technological support. OFAC is also designating several entities and individuals for being owned or controlled by, or acting for or on behalf of, the three entities that have enabled the FSB.
>
> [snip]
>
> Examples of Russia's malign and destabilizing cyber activities include the destructive NotPetya cyber-attack; cyber intrusions against the U.S. energy grid to potentially enable future offensive operations; and global compromises of network infrastructure devices, including routers and switches, also to potentially enable disruptive cyber-attacks. Today's action also targets the Russian government's underwater capabilities. Russia has been active in tracking undersea communication cables, which carry the bulk of the world's telecommunications data.

I've included the entire list of sanction targets below.

On paper, at least, it looks like Treasury is sanctioning:

- An entity, Divetechnoservices, that helps Russia tap into submarine cables along with three of its employees (another thing our spooks do, but one the US and especially UK have been increasingly worried about from Russia); the Treasury release notes that Divetechnoservices got the contract for a FSB submersible craft way back in 2011
- An entity, Kvant Scientific Research Institute, that has been a research institute for FSB since August 2015 and, since April 2017, the prime contractor on an FSB project
- An entity, Digital Security, that as of 2015 worked on a project that would expand Russia's offensive cyber capabilities; the sanctions also include two companies the release claims are Digital Security subsidiaries, both which have US and Israeli locations

All of these were sanctioned under E.O. 13694,

which, as amended, included attacks on election processes; given the dates, they might be implicated in the election year hacks, or might just be deemed a threat to national security. Just Kvant was *also* sanctioned under CAATSA, which is the more general sanctions program forced onto Trump by Congress. I've also put the language for the two of those below.

And, as Lorenzo F-B notes, the heads of two of the sanctioned alleged subsidiaries of Digital Security, ERPScan and Embedi, say they have nothing to do with the company.

> But one of the security companies named in the new sanctions, ERPScan, denied having anything to do with the Russian government in an email to Motherboard.
>
> "The only issue is that I and some of my peers were born in Russia, oh, cmon, I'm sorry but I can't change it," ERPScan's founder Alexander Polyakov told me. "We don't have any ties to Russian government."
>
> ERPScan is mostly known for its product that hunts for vulnerabilities in companies' systems provided by SAP, a popular German enterprise software maker. Cyber Defense Magazine gave ERPScan an award this year for "best product" in its artificial intelligence and machine learning category.
>
> [snip]
>
> Polyakov, however, claimed that as of 2014, ERPScan is a "private company registered in the Netherlands" and that it has no connections "with other companies listed in this document."
>
> [snip]
>
> "The news came to us as an unpleasant surprize. We never worked for Russian government, but indeed we have some former Russian researchers in our

> Research Team (some of them are former employees of Digital Security)," Alex Kruglov, Embedi's head of marketing, told Motherboard in an email. "It is the only reason we can figure out to be added to a sanctions list."

And they're both legit cybersecurity companies, which at the very least raises questions (as the Kaspersky targeting did) about whether this is just infosec protectionism. If these protestations are correct, however, it renews real questions about the accuracy of sanction claims made under Treasury Secretary Steve Mnuchin.

The first indication that Mnuchin's Treasury Department was offering bullshit to fulfill Congress' demand for sanctions came when Treasury released a list of Russian oligarchs in January that was basically just the Forbes list of richest Russians, including a number that oppose Putin.

> President Trump's Treasury Department releaseda list of prominent Russian political figures and business leaders who have prospered while Vladimir Putin has led Russia.
>
> The list features 210 people, including politicians such as Prime Minister Medvedev and Minister of Defense Sergey Shoygu. Also on the list are 96 "oligarchs." Within hours of the list's posting , media organizations began pointing out the similarity between the 96 billionaires listed and the Russians that appear on *Forbes*' 2017 list of the World's Billionaires.
>
> *Forbes* went through the lists and confirmed that indeed the Treasury Department's list is an exact replica of the Russians on the 2017 billionaires list.

For a bit, I thought the list released in March, which added a few new GRU officers, might have reflected new knowledge about GRU officers involved in the targeting of the DNC. Except it turned out those officers were just people readily identifiable off public GRU records. Treasury basically could have gotten them from a spook phone book.

Treasury did better with non-cyber Ukraine-related sanctions in April. It actually named several figures — most obviously Oleg Deripaska and Alexander Torshin — suspected of having played key roles in the election interference. Since then, Deripaska and his aluminum company Rusal have pursued financial games to shield Rusal from sanctions. He's doing this with the help of Mercury Public Affairs — the Vin Weber lobbying group that shows up in a lot of Manafort's indictments — and former Trump aide Brian Lanza, who now works there. So it's not clear whether Deripaska will be significantly impacted.

With that history in mind, it's worth asking whether Treasury simply can't do *cyber* sanctions well, both because it's hard to distinguish infosec from hacking (it would be equally difficult to do so for any of a number of contractors with close ties to FBI, the analogue of the companies that got sanctioned yesterday), and perhaps because Treasury doesn't have good intelligence on who is hacking for Russia. Or perhaps Mnuchin is just obstinate.

But thus far, the history of Treasury's selections on Russian related cyber sanctions leaves quite a bit to be desired.

Today's action includes the designation of five Russian entities and three Russian individuals pursuant to E.O. 13694, as amended, as well as a concurrent designation pursuant to Section 224 of CAATSA.

Digital Security was designated pursuant to E.O.

13694, as amended, for providing material and technological support to the FSB. As of 2015, Digital Security worked on a project that would increase Russia's offensive cyber capabilities for the Russian Intelligence Services, to include the FSB.

ERPScan was designated pursuant to E.O. 13694, as amended, for being owned or controlled by Digital Security. As of August 2016, ERPScan was a subsidiary of Digital Security.

Embedi was designated pursuant to E.O. 13694, as amended. As of May 2017, Embedi was owned or controlled by Digital Security.

Kvant Scientific Research Institute (Kvant) was designated pursuant to E.O. 13694, as amended, and Section 224 of CAATSA for being owned or controlled by the FSB. In August 2010, the Russian government issued a decree that identified Kvant as a federal state unitary enterprise that would be supervised by the FSB.

Kvant was also designated pursuant to E.O. 13694, as amended, for providing material and technological support to the FSB. As of August 2015, Kvant was a research institute with extensive ties to the FSB. Furthermore, as of April 2017, Kvant was the prime contractor on a project for which the FSB was the end user.

Divetechnoservices was designated pursuant to E.O. 13694, as amended, for providing material and technological support to the FSB. Since 2007, Divetechnoservices has procured a variety of underwater equipment and diving systems for Russian government agencies, to include the FSB. Further, in 2011, Divetechnoservices was awarded a contract to procure a submersible craft valued at $1.5 million for the FSB.

Aleksandr Lvovich Tribun (Tribun) was designated pursuant to E.O. 13694, as amended, for acting for or on behalf of Divetechnoservices. As of December 2017, Tribun was Divetechnoservices' General Director.

Oleg Sergeyevich Chirikov (Chirikov) was

designated pursuant to E.O. 13694, as amended, for acting for or on behalf of Divetechnoservices. As of March 2018, Chirikov was Divetechnoservices' Program Manager.

Vladimir Yakovlevich Kaganskiy (Kaganskiy) was designated pursuant to E.O. 13694, as amended, for acting for or on behalf of Divetechnoservices. As of December 2017, Kaganskiy was Divetechnoservices' owner. Previously, Kaganskiy also served as Divetechnoservices' General Director.

EO 13694 as amended

E.O. 13694 authorized the imposition of sanctions on individuals and entities determined to be responsible for or complicit in malicious cyber-enabled activities that result in enumerated harms that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States. The authority has been amended to also allow for the imposition of sanctions on individuals and entities determined to be responsible for tampering, altering, or causing the misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions.

CAATSA Section 224

IN GENERAL.—On and after the date that is 60 days after the date of the enactment of this Act, the President shall— (1) impose the sanctions described in subsection (b) with respect to any person that the President determines— (A) knowingly engages in significant activities undermining cybersecurity against any person, including a democratic institution, or government on behalf of the Government of the Russian Federation; or (B) is owned or

controlled by, or acts or purports to act for or on behalf of, directly or indirectly, a person described in subparagraph (A);

[snip]

SIGNIFICANT ACTIVITIES UNDERMINING CYBERSECURITY DEFINED.—In this section, the term ‘‘significant activities undermining cybersecurity’’ includes— (1) significant efforts— (A) to deny access to or degrade, disrupt, or destroy an information and communications technology system or network; or (B) to exfiltrate, degrade, corrupt, destroy, or release information from such a system or network without authorization for purposes of— (i) conducting influence operations; or (ii) causing a significant misappropriation of funds, economic resources, trade secrets, personal identifications, or financial information for commercial or competitive advantage or private financial gain; (2) significant destructive malware attacks; and (3) significant denial of service activities.
