A DEEP DIVE ON THE OBAMA RESPONSE TO RUSSIAN DNC HACK (AND THEFT AND HARASSMENT)

I was still with family when the White House rolled out its retaliation against Russian hacks of the election the other day, so I didn't have a chance to unpack what they released. I'll do that here.

The actions — which retaliate not just for the DNC hack — consist of a package that includes:

- A "Voxsplainer" telling you "everything you need to know" about the package
- An Obama statement
- An expansion of cyber sanctions to include both our elections and those of our allies and partners
- State Department retaliation against Russia for harassing our personnel
- Two documents about Russian hacking: A Joint Analysis Report and an introduction to it

The Voxsplainer

In addition to promising to tell us "What You Need to Know" about "The Administration's Response to Russia," the Voxsplainer provides links to all the other pieces. There are two significant details.

First, the “response” is not just to “cyber operations aimed at our election” but also to “the Russian government’s aggressive harassment of U.S. officials.” Some of the most showy retaliation was actually specifically retaliation for the latter.

The other key detail is that, in describing Russia’s motive for the hack, the Voxsplainer steers very, very clear of the two more controversial motives (to retaliate for perceived and real covert operations against Russia, and to get Trump elected). Instead, the Voxsplainer provides the most wishy-washy description of Russia’s purpose.

> Russia’s cyber activities were intended to influence the election, erode faith in U.S. democratic institutions, sow doubt about the integrity of our electoral process, and undermine confidence in the institutions of the U.S. government.

“Faith, integrity, and confidence” are pretty squishy things that don’t require much proof.

Obama’s statement

Obama’s statement is basically a description of what he ordered (here, he admits some of the individual sanctions are for cyber-crime, not the hack). The most important part of the statement is the last paragraph.

> These actions are not the sum total of our response to Russia’s aggressive activities. We will continue to take a variety of actions at a time and place of our choosing, some of which will not be publicized. In addition to holding Russia accountable for what it has done, the United States and friends and allies around the world must work together to oppose Russia’s efforts to undermine established international norms of behavior, and interfere with democratic

> governance. To that end, my Administration will be providing a report to Congress in the coming days about Russia's efforts to interfere in our election, as well as malicious cyber activity related to our election cycle in previous elections.

As I'll show in this and a follow-up post, some of what Obama ordered is silly or downright counterproductive. But the actions took place alongside a claim that there would also be covert retaliation we won't see. So we've got silly and counterproductive overt retaliation, with the promise of covert retaliation that may be less silly.

Obama also stated what the presumed goal of these actions are, to prevent Russia from undermining democratic norms, norms which the President-Elect has expressed intent to violate.

New Cyber-Sanctions

Obama extended the application of an EO he signed in April 2015 to apply to election related hacking. The Voxsplainer doesn't explicitly describe what's new about the cyber-sanctions, leaving that to a separate fact sheet and an annex to the Executive Order extending the sanctions. Instead, the Voxsplainer describes what the original EO 13964 had done, which basically permitted the President to sanction entities that hacked critical infrastructure or big money.

Curiously, the White House doesn't appear to have issued a new version of EO 13964, relying solely on the fact sheet to explain the newly expanded scope.

Just as interesting there's a subtle difference in the way the attached fact sheet describes the addition, and how Obama did in his statement. The fact sheet does not specify whether these sanctions only apply for the targeting of our

own election processes or institutions, or for others.

> The increasing use of cyber-enabled means to undermine democratic processes at home and abroad, as exemplified by Russia's recent activities, has made clear that a tool explicitly targeting attempts to interfere with elections is also warranted. As such, the President has approved amending Executive Order 13964 to authorize sanctions on those who:
>
> - *Tamper with, alter, or cause a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions.*

But Obama's statement says the EO "provides additional authority for responding to certain cyber activity that seeks to interfere with or undermine our election processes and institutions, or those of our allies or partners." [my emphasis] That Obama would extend such sanctions to protect our allies' elections make sense, as there's real concern about Russia's plans for the upcoming French and German elections. But it's also really funny given that the NSA and CIA have targeted the election institutions and processes of our allies Pakistan and Mexico. Does that mean we have to sanction the NSA and CIA now? This is so confusing.

As to the sanctions themselves, they target the following:

> 1. Main Intelligence Directorate (a.k.a. Glavnoe Razvedyvatel'noe Upravlenie)

> (a.k.a. GRU); Moscow, Russia
> 2. Federal Security Service (a.k.a. Federalnaya Sluzhba Bezopasnosti) (a.k.a FSB); Moscow, Russia
> 3. Special Technology Center (a.k.a. STLC, Ltd. Special Technology Center St. Petersburg); St. Petersburg, Russia
> 4. Zorsecurity (a.k.a. Esage Lab); Moscow, Russia
> 5. Autonomous Noncommercial Organization "Professional Association of Designers of Data Processing Systems" (a.k.a. ANO PO KSI); Moscow, Russia Individuals
>
> 1. Igor Valentinovich Korobov; DOB Aug 3, 1956; nationality, Russian
> 2. Sergey Aleksandrovich Gizunov; DOB Oct 18, 1956; nationality, Russian
> 3. Igor Olegovich Kostyukov; DOB Feb 21, 1961; nationality, Russian
> 4. Vladimir Stepanovich Alexseyev; DOB Apr 24, 1961; nationality, Russian

As I noted the other day, I find it particularly interesting that Obama included FSB in these sanctions, given that the public record only reflects them doing the kind of data collection that we also do all the time (and that China and others have done against us in the past). Perhaps that means there's evidence they did more, or perhaps this is just gratuitous sanctioning. It will be interesting to see how seriously this part of the sanctions gets taken, given that we need to cooperate with Russian intelligence on things like bombing ISIS.

There has been some befuddlement about why Zorsecurity got included on the list, as its owner, Alisa Esage Shevchenko, claims she doesn't work for the Russian state and has been celebrated for her security research in the past, though one anonymous source claims she has.

> "I'm just trying not to freak out," she told me over email. "My company never

> worked with the government. It never had the necessary licenses to do so in the first place. And I personally tried to stay as far away as possible from anything remotely suspicious, as I'm naturally a cosmopolitan person, and an introverted single woman. I wouldn't want any job that would put me in danger or restrictions."
>
> Talking about the defunct state of the company, she added: "This is fixed in the public registry, and should be well known to any foreign intelligence that bothered to do any research." A search on the public registry showed ZorSecurity as still active, however — Shevchenko said the firm stopped submitting any tax statements, which should be visible in the registry.
>
> [snip]
>
> One Russian hacker who claimed knowledge of Esage Lab's business, and who asked to remain anonymous, said the company sold software exploits and hacking tools, and had worked with the Russian government. "Esage do exploits and offensive software," said the well-connected Moscow source. "Esage worked with government customers … but I'm really not sure if they related to the DNC hack."

That same anonymous Russian hacker also doesn't see why the US sanctioned the two other Russian companies.

> The anonymous Moscow source told me the list of organizations named in the sanctions — which also included the St. Petersburg-based Special Technology Center and the Autonomous Noncommercial Organization's Professional Association of Designers of Data Processing Systems — did "not look

> professional at all." "It looks like the U.S. government does not know who is behind this DNC thing," they added.

So it's possible the US just sanctioned some companies for the sake of sanctioning some companies. As MalwareJake notes in a critique of the sanctions, these companies don't do business in the US so it's not like the sanctions will have any effect anyway.

Four of the individuals sanctioned are top GRU officials (making this the equivalent of the post-Sony sanction on North Korean officials).

> Sanctioned individuals include Igor Valentinovich Korobov, the current Chief of the GRU; Sergey Aleksandrovich Gizunov, Deputy Chief of the GRU; Igor Olegovich Kostyukov, a First Deputy Chief of the GRU; and Vladimir Stepanovich Alexseyev, also a First Deputy Chief of the GRU.

The Voxsplainer also notes that Treasury added two Russian criminals to its sanction list.

> In addition, the Department of the Treasury is designating two Russian individuals, Evgeniy Bogachev and Aleksey Belan, under a pre-existing portion of the Executive Order for using cyber-enabled means to cause misappropriation of funds and personal identifying information.
>
> - *Evgeniy Mikhailovich Bogachev is designated today for having engaged in significant malicious cyber-enabled misappropriation of financial information for private financial*

> *gain. Bogachev and his cybercriminal associates are responsible for the theft of over $100 million from U.S. financial institutions, Fortune 500 firms, universities, and government agencies.*
> - *Aleksey Alekseyevich Belan engaged in the significant malicious cyber-enabled misappropriation of personal identifiers for private financial gain. Belan compromised the computer networks of at least three major United States-based e-commerce companies.*

Note, however, that at least Bogachev has been implicated in surveillance in the past. So it's possible these sanctions are designed to nod towards related activity, the sanctioned (heh) permission of cybercrime by entities willing to help out the Russian government.

Diplomatic retaliation

As noted above, this package of actions actually responds not just to the election (and Bogachev and Belan's crimes), but also to harassment of US personnel in Russia.

The beginning of the Voxsplainer says that the diplomatic measures were in retaliation for

harassment that has gone on in the last year. “Moreover, our diplomats have experienced an unacceptable level of harassment in Moscow by Russian security services and police over the last year.”

The part of the Voxsplainer that explains the actual actions says it responds to two years of harassment.

> Over the past two years, harassment of our diplomatic personnel in Russia by security personnel and police has increased significantly and gone far beyond international diplomatic norms of behavior. Other Western Embassies have reported similar concerns. In response to this harassment, the President has authorized the following actions:
>
> Today the State Department declared 35 Russian government officials from the Russian Embassy in Washington and the Russian Consulate in San Francisco “persona non grata.” They were acting in a manner inconsistent with their diplomatic status. Those individuals and their families were given 72 hours to leave the United States.
>
> In addition to this action, the Department of State has provided notice that as of noon on Friday, December 30, Russian access will be denied to two Russian government-owned compounds, one in Maryland and one in New York.

I find the temporal inconsistency interesting, especially since neither period extends back to the post-Boston Marathon period when numerous CIA officers, most notably Randy Fogle, were getting expelled from Russia. It does, however, cover incidents that have been reported since at least July, including this apparent attempt to detain someone who just barely made it into the US embassy, with ABC providing more detail in October.

In any case, the closure of the two recreational facilities had the excellent effect of getting journalists scurrying to the sites, one of which US officials misidentified:

> Articles on Friday about the Obama administration's decision to close two Russian-owned compounds in the United States misidentified one of the compounds, using information from the White House and F.B.I. officials. The administration ordered the closure of Norwich House in Upper Brookville, N.Y., owned by Russia — not the nearby Killenworth Mansion in Glen Cove, N.Y., also owned by the Russians. An accompanying picture that showed Killenworth Mansion should have been of Norwich House.

Every outlet was able to highlight pictures of big mansions and interview neighbors about weird interactions with Russians. All perfectly scripted just like the Americans.

Putin, of course, threatened to retaliate by kicking out 35 diplomats, but instead invited the children of American diplomats to a party at the Kremlin. Also perfectly scripted.

Two documents on Russian hacking

Finally, the government released two documents on Russian hacking: a document introducing a Joint Analysis Report and the Joint Analysis Report itself. It appears the introductory document served mostly to get FBI, ODNI, and DHS all listed on one document — so there's no doubt that this comes from the entire IC, as there was of the October 7 report that FBI declined to sign off on. It has this odd endorsement of many — but not all — claims made by a number of — but not all — security industry reports.

> 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.

I guess we'll just have to guess which parts the security firms got right and which they did not.

As for the Joint Analysis Report (JAR), it purports to be an alert to make everyone more vigilant against Russian hacks. A number of tech experts have criticized the contents. Robert Graham calls them a "political tool, to prove they have evidence pointing to Russia. They have limited utility to defenders, or those publicly analyzing attacks." Robert M Lee says the report "reads like a poorly done vendor intelligence report stringing together various aspects of attribution without evidence." Jerry Gamblin notes that a fifth of the IP addresses included were Tor exit nodes, meaning they could be used by anyone. Wordfence analyzes one malware sample and finds that it "is old, widely used and appears to be Ukrainian. It has no apparent relationship with Russian intelligence." Ultimately, the tech folks are complaining that the report is not very useful for defensive purposes, which is ostensibly what it is supposed to do.

But several of the reports also include some version of this conclusion from Lee: "the indicators are not very descriptive and will have a high rate of false positives for defenders that use them."

That is, we may see more of what we saw Friday, when a Vermont utility did as instructed with the report — searched for the indicators included in the report — reported a positive hit, only to have anonymous sources immediately blow it up to mean Russia had hacked our grid.

That find might turn out to be a Russian probe, or it might not; there's little doubt that Russia can hack our electrical system. But what it did do is feed a panic.

And even though the report is supposed to only address defense (with the report to Congress designed to report on the actual attacks) there is an odd detail in the narrative about the attack. After describing APT 29 (associated with FSB) and APT 28 (associated with GRU) generally, the report includes these two paragraphs.

> 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.

Of FSB's attack (APT29), the report states that at least one person clicked a bad link. After infesting (not a technical term!) the DNC server, the report describes, FSB "exfiltrated email from several accounts through encrypted connections."

That is, the government is saying it (or someone else) watched FSB steal documents.

Now compare that to the GRU description (APT 28). I guess the narrative vaguely suggests that recipients changed their passwords after being phished, though there's nowhere near the exactitude of at least one user clicking a bad link as used with FSB. And on the critical issue — whether any data was exfiltrated — the report only says it was "likely" that the information was exfiltrated. There's no claim here, as there was with FSB, to have watched the documents be exfiltrated.

That's important because GRU is the presumed source for the dump to Wikileaks (as the "assessment" that follows states). We've long known that the government wasn't certain how the documents got from GRU to Wikileaks, but here, they seem to go further and say they only believe it "likely" that the documents were exfiltrated.

And note what's *not* in the report? Any mention of John Podesta, whose leaked emails took up the final month of the campaign.

Maybe I'm overreading this (wouldn't be the first time). But after going out of its way to include a narrative that isn't necessary to the point of the report, the report stops short of making certain statements about the issues we most care about, that GRU stole the documents that Wikileaks got.

I'll have a bit more on this report later. But

it just seems odd from both the technical side and the narrative side.