THE FSB PURGE: TWO NARRATIVES

I first mentioned the arrest of a Kaspersky researcher for treason last week. Since then, more of the American press has been focusing on it, often simply assuming that what are now reported to be up to six arrests must have some tie to the Russian hack of the DNC and other election-related targets.

> One way or another, the arrests—according to the Russian media accounts—are linked to the country's hacking of the US election.

Such assumptions don't even engage with some of the most obvious questions, such as what all these FSB-related arrests would have to do with the hack-and-leak of DNC and Podesta emails allegedly done by Russia's military intelligence GRU.

Obviously, the timing of the arrests would suggest there *might* be a connection, but the presumption has been downright sloppy. So in an effort to unpack this story, I'm going to lay out some of the known claimed details

Some of the better English language sources on the arrests are stories in Bloomberg, Guardian, FT, NYT, and Forbes (as well as the Brian Krebs story quoted in detail below).

Committing crimes pre-dating 2012

When news of Stoyanov's arrest was made public, Kaspersky released a statement saying the activity pre-dated his employment at the security firm, so before 2013. That would seem to rule out involvement in the DNC hack.

Exposing King Servers as key infrastructure in Russian hacks

A more public explanation behind the purge is that Stoyanov and Mikhailov served as sources for the FBI on the investigation into the probes of the state election sites.

On August 18, the FBI released a flash about two probes of US state election websites. Among the details, it released an IP address, 5.149.249.172, associated with the probe. “The FBI received information of an additional IP address, 5.149.249.172, which was detected in the July 2016 compromise of a state’s Board of Election Web site.” Why you would need two human sources for this information, I’m not sure, but the implication in this narrative is that it came from the Russians.

On September 2, ThreatConnect released a report analyzing the IP address, tying it to other suspected Russian hacks.

> However, as we looked into the 5.149.249[.]172 IP address within the FBI Flash Bulletin, we uncovered a spearphishing campaign targeting Turkey’s ruling Justice and Development (AK) Party, Ukrainian Parliament, and German Freedom Party figures from March – August 2016 that fits a known Russian targeting focus and modus operandi. As we explored malicious activity in the IP ranges around 5.149.249[.]172 we found additional linkages back to activity that could be evidence of Russian advanced persistent threat (APT) activity. This connection around the 5.149.249[.]172 activity is more suggestive of state-backed rather than criminally motivated activity, although we are unable to assess which actor or group might be behind the attacks based on the current evidence.

At the time, the guy who owns King Servers, which hosts that IP, Vladimir Fomenko, played dumb, claiming that the entities tied to the election website hacks owed him money and that the FBI had never contacted him but that he'd be happy to provide information.

More recently, Brian Krebs pulled up some of his old reporting to note that Fomenko has long-established ties to spam businessman Pavel Vrublevsky, including with these servers. Vrublevsky has been trying to implicate Mikhaylov and Stoyanov in leaking Russian investigative details to people in the west for years.

> Multiple Russian media outlets covering the treason case mention that King-Servers and its owner Fomenko rented the servers from a Dutch company controlled by Vrublevsky.
>
> Both Fomenko and Vrublevsky deny this, but the accusations got me looking more deeply through my huge cache of leaked ChronoPay emails for any mention of Mikhaylov or Stoyanov — the cybercrime investigators arrested in Russia last week and charged with treason. I also looked because in phone interviews in 2011 Vrublevsky told me he suspected both men were responsible for leaking his company's emails to me, to the FBI, and to Kimberly Zenz, a senior threat analyst who works for the security firm iDefense (now owned by Verisign).
>
> In that conversation, Vrublevsky said he was convinced that Mikhaylov was taking information gathered by Russian government cybercrime investigators and feeding it to U.S. law enforcement and intelligence agencies and to Zenz. Vrublevsky told me then that if ever he could prove for certain Mikhaylov was involved in leaking incriminating data on ChronoPay, he would have someone "tear him a new asshole."

Krebs' story would date Stoyanov's actions to before his ties with Kaspersky, which would explain that part. But it would also suggest this might be product of a long-standing feud — or that the long-standing feud provides cover for a fight for power within the FSB.

One thing that's interesting about all this is that, for some time, the US intelligence community did not attribute the probes of voter registration databases to Russian intelligence. A September 20 DHS alert attributed it to criminal hackers seeking identity theft data. The October 7 ODNI/DHS statement affirmatively declined to attribute it. It was not until the January 6, 2017 report on the hacks that the IC first blamed Russian intelligence (without specifying whether it was FSB or GRU) for the probes.

So if the FSB purge pertains to revealing details about the voter database probes to US intelligence, the first US public acknowledgment of that intelligence came after most people allegedly involved in exposing the tie had been arrested (though people like former Russian Ambassador Michael McFaul were yapping about such things in public statements, and the WaPo had gotten soft leaks about it). That is, in spite of complaints that US reporting might have set off this molehunt, for the registration databases, the molehunt preceded the IC's affirmative (public) use of the data.

Hack-and-leaking top Russians

The other major allegation against the Russians is that they were involved with a hacking group Shaltai Boltai (which translates as Humpty Dumpty from Alice in Wonderland). The group has blackmailed and/or exposed the emails of a number of top Russian leaders, including Prime Minister Dmitry Medvedev and his deputy Arkady Dvorkovich.

Reports claim that Anikeev started the group years earlier, and the FSB either tried to infiltrate it, but then got swept up, or always had ties to it. Ultimately, though, the implication is that FSB was working both sides, using an Anonymous-modeled hacking group to acquire materials on powerful Russians even while, perhaps, using such hackers for Russian ends.

In mid-to-late October, the group released the emails of Vladislav Surkov, the architect of Putin's Ukrainian policy. There wasn't much revealed, though it did make it clear planning for Russia's Ukrainian intervention went back some time. The understanding behind this narrative is that releasing these emails got too close to Putin, which led to the crack-down on the group.

Even when the emails got released, there was no *public* discussion of the possibility that this was US retaliation against Russia — not even after NBC published a really dick-wagging story on October 14 promising CIA retaliation. That's the public story, anyway, which was really weird, given that exposing Putin's plotting in Ukraine would be a really logical retaliation for the DNC hack (even if American exceptionalists like to pretend we would never do a hack and dump). The private story is different, but any private opinions I've heard don't describe who might have conducted such a hack.

It's also not entirely clear the timing works out. But it's not clear we've got all those details yet.

I'm still working through these issues — and warnings from Russian observers that *both* of these narratives may just be convenient front stories for something else and/or for pure power consolidation are well taken.

What has also gone unmentioned is that at a time when Russia and the US would be staring each other down on a "cyber" battlefield, Putin just

apparently took out a number of the key players in that field. No one has mentioned that, but even if these guys were working both sides in a manner that brought value to Putin, having them removed may leave holes in Russia's cyber offense for the near future.

Update: This FT piece, based off an interview with what is alleged to be the last remaining Shaltai Boltai member at large, would seem to confirm that that explains the arrests (it explains the SB got FSB handlers in early 2016). Though I'd ask why someone would return from Thailand to apply for asylum in Estonia if Putin were after them.

Known arrestees

Colonel Sergey Mikhailov, deputy head of the Information Security Center at the FSB

Major Dmitry Dokuchaev (AKA Forb), also with ISC

Ruslan Stoyanov, now with Kaspersky but with earlier with cybercrime investigation firm Indryk and before that Ministry of Interior's Cyber Crime Unit

Journalist Vladimir Anikeev, believed to have been in Ukraine and alleged to have led the hack ofVladislav Surkov

Known dates

August 18: FBI flash identifying new King Servers-related IP address used in probes of election related sites

September 2: ThreatConnect report implicating King Servers

September 5: Obama and Putin discuss hacks at G-20

September 20: DHS alert attributes voter registration probes to criminal hackers in search of PII

September 27: King Servers owner Vladimir

Fomenko claims FBI hasn’t contacted him

October 7: ODNI/DHS statement on Russian hacking declines to attribute voter database hacks to Russian state

October 14: CIA preparing possible cyber response on Russia

October 23-25: Hackers release emails of Vladislav Surkov, exposing Putin’s Ukrainian plans

October 31: Obama contacts Putin on red cyber phone for first time

November 9: Anikeev reportedly detained, begins cooperating

November 26: Anonymous White House statement affirms integrity of election

December 4: Arrests of Mikhailov and Stoyanov

December 9: CIA-based leaks (based off recent human intelligence) claim DNC hack designed to get Trump elected

December 13: Last date on (partial) dossier implicating Trump

January 6, 2017: In declassified Russian Hack Report, US Intelligence Community for the first time attributes probes of voter websites to Russian intelligence (not specifying FSB or GRU): “Russian intelligence obtained and maintained access to elements of multiple US state or local electoral boards.”

January 11: Partial anti-Trump dossier published by BuzzFeed; Christopher Steele flees his home

January 23: GCHQ head Robert Hannigan quits to spend more time with his family

January 25: Kommersant announces arrests