Nellie Ohr

From: Nellie Ohr
Sent: Wednesday, January 25, 2017 11:59 AM
To: (b)(6) [redacted]; bruce.g.ohr@usdoj.gov
Subject: Re: Big arrests

Additional notes on the articles below: (from my text threads with colleagues)
Note: Mikhaylov and Stoyanov were arrested

[The Kommersant article:]
They're citing Chronopay's Vrublevskiy (without describing him as a criminal)

Looks like Group-IB/Vrublevskiy are winning a battle against Kaspersky!

it's Mikhaylov, Gerasimov's subordinate [at FSB's Center for Information Security], who was arrested. Gerasimov was rumored to be stepping down because he had failed to prevent (or cover up) what was going on.

[9:52]
Kommersant says Mikhaylov heads "one of the subdivisions" of the FSB's Information Security Center

[9:54]
The FSB's Information Security Center aka Center 18, was accused by the Ukrainians

[9:54]
of spreading false messages on social media and hacking into Ukrainian officials' mailboxes.

[9:55]
Let me pull together some stuff I had written elsewhere and throw up a stub TG for the FSB

[9:55]
Some subdivisions of Center 18 inclue

[9:55]
include

[9:55]
Division of Information Technologies—Expert Subunit; and Operational Divisions.

[9:56]
Vrublevskiy was also prosecuted by then (sweet revenge now eh?)

[9:56]
by them

that is very interesting

[9:57]
isn't Vrublevskiy close to Ivanov?

nohr [9:57 AM]
Sergey Ivanov?

[9:57]
I've been thinking this was all tied with the "yellow rain dossier"

[9:57]
Gerasimov stepped down because couldn't cover up the FSB-led operation in the US

[9:58]
Ivanov already had to step down—according to the dossier—because the operation was becoming too public

[9:59]
Ah, I finally got to see the securityaffairs.co article . ""This case is not related to Kaspersky Lab. Ruslan Stoyanov is under investigation for a period predating his employment at Kaspersky Lab," reported Forbes citing a Kaspersky spokesperson's statement. "We do not possess details of the investigation. "

nohr [10:05 AM]
I wonder where Stoyanov worked in between 2006 and when he joined Kaspersky

Not that this is relevant, but Jan 13, when Kommersant reported Gerasimov might step down, was the same date as the arrest of Lisov (Neverquest) in Spain and 3 days after the arrests of the Occhioneros in Italy, and days after the publication of the "Yellow showers" dossier

[10:10]
That came out on Jan 10

nohr [10:18 AM]
"Before joining Kaspersky in July 2012, Stoyanov's LinkedIn profile lists him as the deputy director of 'Indrik' - Indrik being the name of a mythical beast in Russian mythology. However, Stoyanov has also had stints at telecoms company RTComm.ru and in the Ministry of Interior Moscow Cyber Crime Unit, where he was a Major." according to http://www.theinquirer.net/inquirer/news/3003238/kaspersky-lab-manager-arrested-over-treason-allegations-in-russia

On FSB Center 18 chief Gerasimov's ouster and possible connection with the dossier, see
http://foreignpolicy.com/2017/01/13/head-of-fsb-cyber-unit-may-soon-be-dismissed-russia-putin-trump/
Foreign Policy emilytamkin
Head of FSB Cyber Unit May Soon Be Dismissed
The man who oversaw the KGB successor's cybersecurity since 2009 may soon be out of a job.

[11:34]
https://meduza.io/en/news/2017/01/13/fsb-s-cybersecurity-supervisor-may-soon-be-sacked
Meduza
FSB's cybersecurity supervisor may soon be sacked — Meduza
The head of the FSB's Information Security Center Andrei Gerasimov could soon be dismissed, reported newspaper Kommersant, citing a source close to the FSB, as well as the top managers of IT-companies working with the Center. (61KB)

"The Center is now being investigated over its relations with commercial companies, specializing in cybercrimes, such with Kaspersky and Group-IB."

Interpretermag gets some things wrong. http://www.interpretermag.com/russia-update-january-25-2017/

However, they do summarize an article by a man close to the security services who is very involved in IT and cybersecurity policy in Russia
Pasted below

However, one of his critiques may be wrong. He and Soldatov (a widely respected expert on Russian special services) think the dossier mixes up Department K of the MVD and Department K of the Fsb.

However, as I understand it, Department K of the FSB is responsible for counterintelligence in the Financial industry, and therefore would be a pretty good candidate for listening in on Hillary. Whereas MVD Department K does cybercrime, but they're not investigating Hilary for cybercime

"Another aspect to the Trump dossier and its possible fall-out West and East is suggested in an interesting

article by Yevgeny Krutikov, an admitted former spy himself, in the pro-Kremlin *Vzglyad*, featured in Johnson's List by a blogger.

The headline of Krutikov's piece is "Kompromat on Trump May Be Regarded as Discreditation of Russian Counterintelligence".

This is an angle that has not been covered in the West, where media and officials have been preoccupied with whether or not the claims in the dossier are true, and the nature of the relations the dossier's author, who was revealed to be the ex-spy Christopher Steele, had with the FBI. The media has been busy trying to check the allegations in the dossier, and some have pointed out that the story is more about the *use* of the dossier made by a group of American intelligence agencies investigating Trump's associates and their connections to Russia.

But this Russia ex-spy -- although no spy is ever a former spy as Vladimir Putin himself will tell you -- is indignant about an issue that stands out for Russians. If the list of top figures mentioned in the dossier who are in the Russian government, oil and gas business and other sectors is true, then that means foreign espionage has been easily able to penetrate to the very top of Russian political and business leadership. It's an insult then to Russian counter-intelligence which should have prevented or exposed such a thing -- and also grounds for severe punishment in Russia. (And for all we know, what is happening now with the release of the dossier and its discreditation is Russian damage control.)

Krutikov lists all the supposed sources of the dossier and finds it improbable that any spy or spies in the West acting unofficially could have obtained that high and wide an access. That is indeed a point to marvel about in this dossier.

But since some of the aspects of the report fell apart upon close examination, or the people in the report vigorously denied their involvement and seemed to have alibis. Krutikov's article is

rather about how the Western intelligence agencies discredited themselves by buying this "fake." His headline promises an article of remorse or anger about "discreditation" of the valiant Russian organs, but it's really about discrediting Western spies.

Steele is a "decoy duck", says Krutikov, and whether this was planned, leaked to the press, or invented by editors who had read too many spy stories wasn't important. Says Krutikov:

> *"Such a figure [as Steele] does not look very convincing and is hardly dangerous But on the whole, there is no certainty that such a personage exists at all, at least in those existential categories that are ascribed to him. Moreover, it is hard to imagine, that this is one person, and not an abstract compilation of knowledge."*

To obtain access simultaneously to "five sources in the Russian government and the presidential administration," you would have to be at a minimum a deputy director for operational work in a Western spy shop, reasons Krutikov. And it would be nonsense to be retired in this case, as if you had left the service, you would no longer have access to the "most secret" material in MI6 or "top secret" in the CIA. Even if you could still maintain contact with an old agent, you wouldn't have access to his file any more; this is basic intelligence folk wisdom.

So looking at the dossier, reasons Krutikov, we would have to imagine that all five sources were still accessible by the report's compilers, even from the days of the USSR. "But that isn't possible by dint of the fact that the Russian elite has changed since then at a minimum three times, practically from the foundation up."

Krutikov analyzes the five sources, and notes about source B, who was said to have *kompromat* on Hillary Clinton. This source is

said to have contacted a certain "Department K" which as we know exists in the Interior Ministry. As Andrei Soldatov pointed out, the dossier mentions "Department K of the FSB," but that's a mix-up.

Department K in the FSB is involved in 'supervising' the banking and financing system," notes Soldatov and its officers were recently involved in a scandal "that ended with an Interior Ministry official jumping out of a window during interrogation."

It's the Department K in the Interior Ministry, not the FSB, that does the cyber investigations, he explains.

So isn't the connection between the individuals related to Department K in the Trump dossier (even identified incorrectly) and the Department K where Stoyanov and others at Kaspersky once worked rather tenuous? Of course it is.

But Krutikov's musings, which include a frank assessment of Western intelligence agencies' work "at the worst level it has been in a quarter of a century" and a knock on Western spies as amateurish, still contained a concern lurking underneath that the dossier -- *if true* -- could mean only one thing: somebody inside Russian intelligence was turned, and helping an effort to expose Trump -- and Putin's operation to promote him.
Again, if true, the high-level nature of the sources and the alleged nature of the information -- involving the very candidates of the US election, one of whom became president -- mean that Russian defense was penetrated. Maybe it wasn't, but if it were, we would expect to see heads roll.

We'd also expect to see lesser figures hung out to dry, in keeping with every scandal in Russia. There have been arrests of some Russian hackers in the West, and we don't know if they are related to the DNC hack or not. And the arrests announced today may not be the droids we are looking for. But if true, there will be

arrests in Russia -- for treason -- and we need to be on the look-out for them.

Even if the dossier is fake, unless Russian intelligence is fully behind it themselves, they can't be sure that in fact Steele's fact-finders really did have some Russian sources and they need to worry that their people have been turned. Then Russian counter-intelligence would believe they were penetrated even if they weren't -- a whole other aspect of the dossier which would indicate its fabrication was done in the West.

-- Catherine A. Fitzpatrick

Published in Press-Stream Russia Update: January 25, 2017 in Publication Russia Update

---

-----Original Message-----
From: Nellie Ohr (b)(6)
To: bruce.g.ohr <bruce.g.ohr@usdoj.gov>
Sent: Wed, Jan 25, 2017 11:49 am
Subject: Big arrests

A top FSB Information Security subdivision head, Mikhaylov, arrested for treason.

Supposedly received money from foreign organizations via Ruslan Stoyanov of Kaspersky

Kaspersky claims this all happened before Stoyanov came to work there in 2013

http://securityaffairs.co/wordpress/55675/cyber-crime/russia-arrested-ruslan-stoyanov.html

"Before joining Kaspersky in July 2012, Stoyanov's LinkedIn profile lists him as the deputy director of 'Indrik' - Indrik being the name of a mythical beast in Russian mythology. However, Stoyanov has also had stints at telecoms company RTComm.ru and in the Ministry of Interior Moscow Cyber Crime Unit, where he was a Major." according to http://www.theinquirer.net/inquirer/news/3003238/kaspersky-lab-manager-arrested-over-treason-allegations-in-russia

Will send more notes in a sec