BEHIND THE ARREST OF PUTIN'S PEN-TESTER, VLADISLAV KLYUSHIN

There's a gratuitous passage in the March 20, 2021 complaint charging Vladislav Klyushin, Ivan Yermakov, Igor Sladkov, Mikhail Irzak, and Nikolay Rumyantev with conspiracy to violate the Computer Fraud and Abuse Act. It describes that Klyushin — the guy just extradited to the US on the charges — possessing a picture of Alexander Borodaev and Sergey Uryadov posing in front of Scotland Yard in London.

[21] I am aware based on documents and communications I have reviewed that KLYUSHIN, ERMAKOV, Varshavskiy, and Uryadov are friendly with one another and travel together. For example, I have reviewed photographs in KLYUSHIN's possession of Varshavskiy and Uryadov standing across the street from the headquarters of New Scotland Yard, in London, England, and of himself with Uryadov in front of the United Kingdom Ministry of Defense building. KLYUSHIN has also shared photographs of ERMAKOV with Varshavskiy.

Thus far, it's unclear who the guys in the picture are, other than customers of M-13's "investment services," for which they paid extortionate 60% commissions to benefit from the insider trading scheme allegedly run by Klyushin and Yermakov. But, in addition to alerting Klyushin to how many of his personal files the FBI has obtained, folks back in Russia will have a taste of the kind of information at risk now that Klyushin is in US custody.

That is, this passage, and a host of others in the charging documents, appear designed to maximize the discomfort of a number of people involved, as much as justifying the arrest and extradition of the guy who led a company that provided services that amount to information operations to Vladimir Putin. As the DOJ presser explained,

> M-13's website indicated that the company's "IT solutions" were used by "the Administration of the President of the Russian Federation, the Government of the Russian Federation, federal ministries and departments, regional

> state executive bodies, commercial companies and public organizations." In addition to these services, Klyushin, Ermakov and Rumiantcev also allegedly offered investment management services through M-13 to investors in exchange for up to 60 percent of the profit

The insider trader scheme works like this: Klyushin (the guy in US custody) and Yermakov (a key person involved in the 2016 DNC hack, described in DOJ's press release as a "former" GRU officer), along with one other guy from M-13, area accused of hacking at least two US filing agents to obtain earnings reports before they were officially released. They conducted trades for a handful of clients — along with Borodaev and Uryadov, Boris Varshavskiy is mentioned. Klyushin also conducted trades for himself. The three M-13 figures were indicted on conspiracy, hacking, wire fraud, and securities fraud charges on April 6, 2021, an indictment that formalized the extradition request for Klyushin, who had already been arrested in Switzerland.

Then there are two apparent private citizens who live in St. Petersburg, Michail Irzak and Igor Sladkov. They were indicted on May 6, 2021 on conspiracy to hack and hacking charges, along with securities fraud. That indictment (like the complaint) focuses on some different trades than the Klyushin one (and because neither is likely to be extradited anytime soon, the second indictment may shield some portion of evidence from discovery).

	Yermakov	Sladkov	Complaint
February 5, 2018: Snap	X	X	X
April 27, 2018: Nanometrics			X
May 9, 2018: Cytomx	X		X
July 24, 2018: Grubhub & 6 others		X	X
October 12, 2018: Equity Bancshares & 2 others			X
October 22, 2018: Capstead	X	X	
October 24, 2018: Tesla	X	X	
November 4, 2018: Nevro			X
November 28, 2018: Box			X
February 25, 2019: Tandem		X	X
May 20, 2019: Kohl's		X	X
July 22, 2019: 8 companies			X
July 28, 2019: SS&C	X	X	X
October 22, 2019: Manhattan Associates			X
November 1, 2019: Roku	X		
November 11, 2019: Datadog			X
November 25, 2019: Beacon			
January 21, 2020: Avnet	X		
January 21, 2020: IBM			X
May 27, 2020: Box		X	

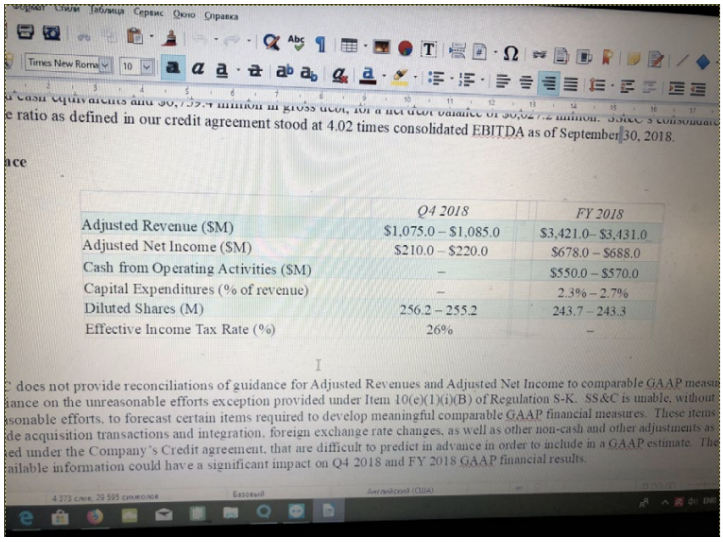
Actions attributed elsewhere to Yermakov are attributed to Co-Conspirator 1 in that indictment, and it is on that basis that Irzak and Sladkov are exposed to the hacking charges. Irzak and Sladkov don't appear to have been paying the extortionate 60% fees that the other M-13 clients were, which makes me wonder whether Yermakov was helping buddies get rich on the side. Worse still, Sladkov had some epically bad operational security; the indictment describes he had in his possession pictures showing:

- A picture of a black Acer computer, with a blue Russian Olympic Committee sticker over the camera, showing a press release with Snap's 2017 earnings that was not released publicly until 8 hours later.
- A picture showing the same Acer computer with the same blue sticker showing his own trading activity on BrokerCreditService on May 2, 2018
- A picture taken on July 24,

2018 at 2:05PM (ET) showing himself and Irzak sitting at a brown table; Irzak had Facebook running at the time, which showed him to be in the vicinity of Sladkov's house

- A picture dated July 25, 2018 showing him trading in a bunch of shares the earnings reports of which had been illegally accessed the day before
- A picture dated October 14, 2018 showing a hand-written note instructing to "short" three shares, which Irzak did short two days later

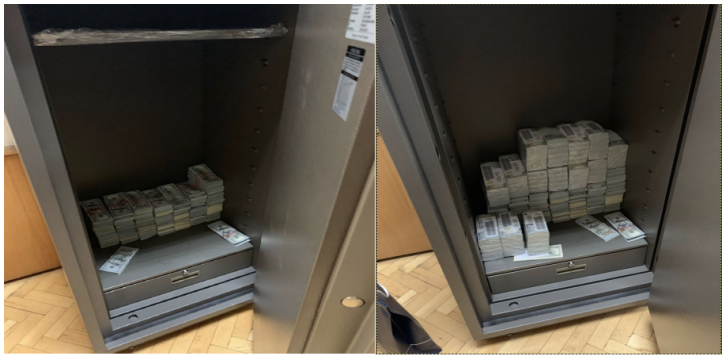
In other words, Sladkov *documented much of his insider training in photographs* (perhaps to share the instructions with Irzak), and left all those photographs somewhere accessible to the US government.



If Yermakov was sharing this information with these guys without permission, then Sladkov's role in providing the US government really damning information that would form the basis

for an arrest warrant for Klyushin, then things might get really hot.

But it's not like Klyushin or Yermakov did much better. In addition to the pictures of the clients, above, and some screencaps that got sent showing trading activity (though with less obvious evidence of insider trading), there's a bunch of messaging from both, including an oblique reference to messages Yermakov and Borodaev sent on November 19, 2020 that have nothing to do with the context of the indictment but happens to be after the US election. There are even pictures Klyushin shared with Yermakov, "showing a safe that contained growing stacks of U.S. one hundred dollar bills."



Yermakov appears to have used one of his messaging accounts via multiple devices, because on December 3, 2018, when he "forgot telephone at work," he was still able to message Klyushin about closing out a trade. Using the same messaging app across platforms would offer one means of compromise, especially if the FBI had gotten into Yermakov's device updates. The indictment doesn't mention a warrant for such messaging that you would expect if it took place on Facebook.

Again, this indictment seems to aim to cause discomfort and recriminations based on information in US possession.

But then there's the question of how it came about, how it landed in Massachusetts rather than DC (where the lead FBI agent is from) or NY (where the trades get done) or Pittsburgh, where one of the prior indictments against Yermakov was done.

The indictments and complaint base the MA jurisdiction on the fact that the culprits used a VPN that used a server in MA on several occasions. At a presser the other day, Acting US Attorney Nathaniel Mendell suggested the case had been assigned to MA because of its good securities prosecution teams.

As to how it came about, purportedly, the story starts in January 2020, when two filing agents allegedly hacked by the men, FA1 and FA2, reported being hacked at virtually the same time. Someone had used an FA1 employee's credentials on January 21, 2020 to access the earnings data for IBM, Steel Dynamics, and Avnet before those results were publicly announced the following day, but no similar transaction noted with respect to F2 (indeed, a list of accesses involving F2 have a gap from November 2019 through May 2020). The investigation determined that FA1 had first been hacked by November 2018 and that FA2 had first been hacked by October 2017.

FA1 and FA2 discovered this compromise just months after the third M-13 employee, Rumyantev, was blocked by his Russian-based brokerage account for suspicious transactions. Months after FA1 and FA2 reported their compromise, Rumyantev and Klyushin lied to a Denmark bank that they were working entirely off of public information. By that point, in other words, banks in at least two countries were onto them.

Then, the story goes, the FBI investigated those hacks — through domains hosted by Vultr Holdings to a hosting company in Sweden to a user account under the name Andrea Neumann. From there, the FBI tracked back through some Bitcoin transactions made in October and November 2018 to the IP address for M-13 where they just happened to discover one of the very same hackers that was behind the 2016 hack of the DNC was also behind this hack. Mendell sounded pretty sheepish when he offered that explanation at the press conference.

Perhaps it's true, but another key piece of

evidence dates to actions Yermakov took on May 9, 2018, when he was under very close scrutiny as part of the twin investigations into his role in the hacks of the DNC and doping agencies, but before the first indictment against him was obtained.

> Based on a review of records obtained from a U.S.-based technology company (the "Tech Company"), I have learned that on or about May 9, 2018, at 3:44 a.m. (ET), an account linked to ERMAKOV received an update for three native applications associated to the Tech Company. Records show that the May 9, 2018 application updates were associated to IP address 119.204.194.11 (the "119 IP Address").
>
> Based on my review of a log file from FA 2, I learned that on or about that same day, May 9, 2018, starting at 3:46 a.m. (ET)—approximately two minutes after ERMAKOV received application updates from the Tech Company—the FA 2 employee's compromised login credentials were used to gain unauthorized access to FA 2's system from the same 119 IP Address, and to view and/or download earnings-related files of four companies: Cytomx Therapeutics, Horizon Therapeutics, Puma Biotechnology, and Synaptics.7 All four companies reported their quarterly earnings later that day.

It would be rather surprising if the FBI agents investigating the DNC hack had not at least attempted to ID the IP associated with Yermakov's phone (or other device) back in 2018. Whether or not they watched him engage in insider trading for years after that — all the while collecting evidence from co-conspirators flaunting the proof of their insider trading — we may never learn. The discovery on this case, featuring evidence explaining how the FBI tracked the insider trading of Putin's pen-tester, will certainly feature a number of law

enforcement sensitive techniques that Klyushin would love to bring back to Putin.

But it's possible these techniques were what the FBI used to target these guys four years ago now, and the insider trading that Yermakov was doing in addition to whatever he spent the rest of his time doing has now provided a convenient way to bring Putin's pen-tester to the United States for a spell.

Update: Included the pictures of the safe included with his detention memo, as well as earnings reports from Sladkov's computer. Note the detention memo says the latter came from an ISP.