HOW WAS KARIM BARATOV PAID?

The indictment accusing two FSB officers and two hackers of compromising Yahoo in 2014-2016 is remarkably detailed. It describes how Alexsey Belan accessed individual Yahoo accounts (though not how he broke in the first time). It provides lists and lists of who got hacked, in enough detail that any victims who didn't already know would learn they had been targeted — as would anyone else in Moscow who might find these details of interest.

I want to look closely, though, at what it tells us about how one of the hackers, Karim Baratov, got paid.

The question is not that interesting as it pertains to Belan. In his case, the indictment describes a number of ways he profited off the hack — with marketing commissions for erectile dysfunction drugs, with spam targets based off millions of hacked Yahoo accounts, and with credit and gift card numbers stolen from specific accounts. Moreover, any additional payment to Belan would be internal to Russia — a cinch to pull off without attracting the attention of the FBI or Department of Treasury.

But Baratov, the phisher that broke into Google and (presumably) Yandex accounts for the FSB men after they were identified via Yahoo metadata, is in Canada, meaning financial transfers would be international.

The indictment explains that he demanded payment of about $100 via online payment system per successful phish, and that FSB officer Dmirty Dokuchaev had to pay before obtaining the credentials.

> During the conspiracy DOKUCHAEV tasked BARATOV with obtaining unauthorized access to at least 80 identified email accounts, including at least 50 identified Google accounts.

> [snip]
>
> When BARATOV successfully obtained unauthorized access to a victim's account, he notified DOKUCHAEV and provided evidence of that access. He then demanded payment-generally approximately U.S. $100-via online payment services.
>
> Once DOKUCHAEV sent BARATOV a payment,' BARATOV provided DOKUCHAEV with valid, illicitly obtained account credentials permitting DOKUCHAEV, SUSHCHIN, and others known and unknown to thereafter access the victim's account without further assistance from BARATOV.
>
> [snip]
>
> Upon successfully gaining the credentials for a tasked account, BARATOV informed DOKUCHAEV thathe could be paid for his work in Russian rubles, U.S. dollars, Ukrainian hryvnia, or Euros through online payment services. DOKUCHAEV then paid BARATOV using these means.

Altogether, Baratov provided access to upwards 80 accounts, for a total profit of not much more than $8,000 for crimes that expose him to decades in prison.

At least once (though I believe just this once), the indictment actually records Dokuchaev paying Baratov.

> On or about November 17, 2015, BARATOV sent DOKUCHAEV the password for ****ov@gmail.com, to which account DOKUCHAEV had tasked BARATOV to gain unauthorized access.
>
> On or about November 17, 2015, DOKUCHAEV paid BARATOV U.S. $104.20.

We also learn that — in addition to seizing

Baratov's Aston Martin and Mercedes — the government will be seizing the contents of a Paypal account in his name.

> All funds which constitute proceeds that are held on deposit in PayPal account number xxxxxxxxxxxxxx9844, held by BARATOV in the name of "Elite Space Corporation";

Brian Krebs pointed to one of Baratov's hacker for hire sites that also accepted payment in WebMoney and YandexMoney.

According to this G&M article, the documents filed in support for extraditing Baratov say the Paypal account was tied to a Royal Bank checking account. (It also says Dokuchaev communicated with Baratov via a Yahoo account!)

> The payments are alleged to have travelled through Web accounts including a PayPal account that links to a Royal Bank chequing account in Mr. Baratov's name. Between February, 2013, and October, 2016, Mr. Baratov received more than $211,000 via that PayPal account, the court records say, adding, however, that the amounts he is alleged to have earned from the Yahoo scheme are smaller.

And the indictment also lists a Dokuchaev Paypal account for forfeiture.

> All funds which constitute proceeds that are held on deposit in PayPal account number xxxxxxxxxxxxxx2639, held by DOKUCHAEV;

So we have a pretty good idea of how the Paypal payments got to Baratov: from Dokuchaev's account to Baratov's to Baratov's Royal Bank checking account.

But we don't know where the money in Dokuchaev's account came from — and whether it made the FSB

tie clear.

Jeffrey Carr has asked whether this operation was an official or rogue operation from the FSB side – a question which has merit and which I'll return to. That question certainly raises the stakes on where the money in Dokuchaev's Paypal account came from.

There's also the other question. Baratov clearly made more than the $211,000 that came into his Royal Bank account. $211,000 would barely cover his fancy cars, much less the ability to throw $100 bills at trick or treaters. So where is the rest of Baratov's hacking income coming from?

Incidentally, according to the G&M, Baratov was put under surveillance by the RCMP around March 7. His $900K house was put on sale on March 13, but then delisted after the indictment. The indictment was actually dated February 28.