REUTERS CONFIRMS KREBS' SUPPOSITION ON RUSSIAN TREASON CHARGES

Earlier this month, I noted Brian Krebs' supposition on the source of the Russian treason charges against some FSB officers. He suggested the charges arose from an old grudge that spam businessman Pavel Vrublevsky had against two of the guys who got charged. Vrublevsky has long wanted to prove that they leaked information on his operations.

> [T]he 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."
>
> As it happens, an email that Vrublevsky wrote to a ChronoPay employee in 2010 eerily presages the arrests of Mikhaylov and Stoyanov, voicing Vrublevsky's

> suspicion that the two men were closely involved in leaking ChronoPay emails and documents *that were seized by Mikhaylov's own division* — the **Information Security Center** (CDC) of the Russian **Federal Security Service** (FSB).

Today, Reuters confirms Vrublevsky's role in the arrest (as well as identifies the fourth person, Georgy Fomchenkov, arrested in the case).

> The source connected to the investigation said the arrests were a result of accusations first made in 2010 by Pavel Vrublevsky, a Russian businessman and founder of ChronoPay, an online payments company. Vrublevsky told Reuters he had also learned that the arrests were a response to his allegations: that Stoyanov and Mikhailov had passed secrets on to American firms.

This makes a lot of sense. Notably, it explains why Kaspersky attributes Ruslan Stoyanov's charges to actions that precede his time at the firm.

Reuters does not, however, pursue the other connection Krebs made — the long-term association between the operator of King Servers, Vladimir Fomenko, who has been named in association with the hack — and Vrublevsky.

My suspicion is that the King Servers connection identified other associations that were far more sensitive for Russia than just an old spam business grudge. And that's why Vrublevsky is finally getting his revenge.

Update: Just to add two bits to this, because people are reading the Reuters story to suggest there's no tie to the DNC hack. Not even Reuters states that. On the contrary, a source "connected to the investigation" states sometimes Russia uses old charges to go after people on new ones (actually we do this too, especially where the old charges can be

prosecuted without exposing classified information).

> Neither Vrublevsky nor the source connected with the investigation offered an explanation as to why they believe the Russian authorities would resurrect such an old case seven years after the allegations were first made.
>
> However, the source said he believed *the case may not be the sole reason why Russian authorities had decided to arrest the men now*: in his experience, he said, Russian authorities at times use old cases as a way of charging people suspected of later crimes.

And Krebs made the connection to Vrublevsky because his company translated the denial for King Servers.

> Fomenko issued a statement in response to being implicated in the ThreatConnect and FBI reports. Fomenko's statement — written in Russian — said he did not know the identity of the hackers who used his network to attack U.S. election-related targets, but that those same hackers still owed his company USD $290 in unpaid server bills.
>
> A English-language translation of that statement was simultaneously published on **ChronoPay.com**, Vrublevsky's payment processing company.
>
> "The analysis of the internal data allows King Servers to confidently refute any conclusions about the involvement of the Russian special services in this attack," Fomenko said in his statement, *which credits ChronoPay for the translation*. "The company also reported that the attackers still owe the company $US290 for rental services and King Servers send an invoice for the payment to Donald Trump

> & Vladimir Putin, as well as the company reserves the right to send it to any other person who will be accused by mass media of this attack.” [italics mine]

Krebs suggested the complaint about unpaid bills sounded like Vrublevsky humor.