ON RUSSIAN TREASON

Yesterday, several reports revealed that a top Kaspersky employee, Ruslan Stoyanov, had been arrested in December on treason charges, along with a top FSB officer. The news has led many people to assume — as Paul Rosenzweig did here that Stoyanov was a source for the dossier on Donald Trump. And the timing of Stoyanov's arrest — reportedly some time in December — may coincide with the suspicious death of another person who might be tied to the dossier, Oleg Erovinkin.

That may well be the case. But perhaps not in an obvious way. Kaspersky, at least, claims that Stoyanov is under investigation for things that pre-date his start at Kaspersky, so 2012 or earlier.

> This case is not related to Kaspersky Lab. Ruslan Stoyanov is under investigation for a period predating his employment at Kaspersky Lab. We do not possess details of the investigation. The work of Kaspersky Lab's Computer Incidents Investigation Team is unaffected by these developments.

Moreover, there's not anyone in the dossier that obviously fits the description of Stoyanov.

That said, there is a tie between Kaspersky and what is assumed to be the DNC hack. On January 8, Shadow Brokers — the entity that dumped a bunch of NSA hacking tools and targets on the web — announced it would sell a bunch of tools targeting Windows. On January 12, it dumped a subset of Windows tools. It claimed, in doing so, it was just dumping the tools identified by Kaspersky. But in fact, not all of them were detected at that point by Kaspersky.

> They claim they only dumped the 58 tools that were detected by Kaspersky AV, but the dump contained 61 files. A little anonymous birdie told me that Kaspersky

> only detects 43 of these files as of mid-day on the 12th. I don't like Russian software on my machines so I can't confirm whether or not that's true.

At the time, a lot of US security people believed that Kaspersky was part of this plot. But it seemed to me, at the time, that this dump instead *targeted* Kaspersky for allowing vulnerabilities in Windows they knew about to remain unaddressed by the anti-virus (and perhaps by whatever other services they offered in Russia). The tools are dated, so they definitely could date to the period when Stoyanov was still at FSB.

Mind you, even if this connection explains why Stoyanov was arrested, it doesn't explain several other things, such as why Russia would arrest Stoyanov *before* any of these Windows tools were released. Nor does it explain who Shadow Brokers is, and why he'd be targeting Kaspersky.

But it is a known tie between events believed to be related to the DNC hack and Kaspersky.