

THE PROXY STEP IGNORED IN THE NGP/VAN ANALYSIS

I'm working on a longer post on the two reports that went into this VIPS letter and in turn this even more breathless Nation article.

One of two underlying reports those pieces rely on to raise doubts about the Intelligence Community's conclusion that Russia hacked the DNC was written by a pseudonymous person under the name The Forensicator. It argues that data "published by a persona named Guccifer 2" on September 13, 2016 was first copied, probably in Linux, locally on July 5, 2016. On September 1, 2016, the data was then transferred on a Windows system. Both those events probably took place in the Eastern Timezone. The derivative reporting on this analysis claims, unjustifiably, that because the first event happened locally and both happened in the Eastern Timezone, they couldn't have been done by people associated with Russia.

The analysis of the data is worth reviewing, though some people quibble with the analysis that claims the first event had to have happened "locally" (that is, over a LAN or similar direct access rather than over the Internet). Even there, there's no reason to believe that that event happened involving a DNC (or other Democratic) computer; the files could (and according to the IC's narrative about the hack, would) have been moved to a second server before July. Nor is there any reason to assume events that took place in the Eastern Timezone could not involve people tied to Russia.

But even with those ready explanations that could align this forensic analysis with the IC's analysis, there's a step of the analysis that is entirely missing.

The Forensicator explains that the files were "published by a persona named Guccifer 2" and

“disclosed by Guccifer 2.0 on 9/13/2016.” But that’s not true. Instead, the files were posted during a speech given in London by another hacker as a proxy for G2.0 on that day. The Forensicator relies on a copy posted by NatSecGeek. And while on Twitter G2.0 pointed to the speech the day before it was given, he never actually pointed back to the data on his WordPress site.

It’s true that the “speech” that was read for G2.0 relied on and posted a link to these files at the conference.

This scheme shows how NGP VAN is incorporated in the DNC infrastructure. It’s for detailed examination, if you are interested. And here are a couple of NGP VAN’s documents from their network. If you r interested in their internal documents, you can have them via the link on the screen. The password is usual. It’s also on the screen. You may also ask the conference producers for them later.

But at the very least, it seems any analysis of these forensics needs to account for the hand-off and proxy involved.

One person I spoke to about these forensics described that they looked like a skilled Linux user followed by an unskilled Windows user (because the latter copied the files via drag and drop). Perhaps. But given that we know there was a proxy step involved in the release, it seems any analysis of why this several step process took place would have to account for the fact that other people were involved in the release of the files.