# THE MACRON HACK: SOMETIMES THE METADATA IS (PART OF) THE MESSAGE

After he claimed he hadn't been hacked, 4Chan released documents from some of Emmanuel Macron's associates (along with a whole lot of crap) last night, just minutes before by French law the candidates and press have to stop talking about the election. Given that the hacking group believed to be associated with Russia's military intelligence GRU had been trying to phish Macron's campaign, it is widely assumed that these files came from GRU. That's a safe starting assumption but it has not been proven.

Here's one review of what we know about the documents so far. Here's advice for France on how to avoid having this become the centerpiece of the next few days.

Thus far, the most remarked aspect of individual documents from the dump (which I haven't started reading yet) is the metadata. For example, a good number of the Microsoft documents have Russian names or metadata in them. In addition, some people are claiming that metadata associated with forgeries in the dump point to specific equipment.

As a result, a number of people have uncritically said that this makes the dump just like the DNC dump, which is further proof that the same sloppy Russians did it.

Except in doing so, most reveal untested assumptions from that DNC dump.

Back when the DNC documents came out, a number of (these very same) people noted that there was Russian metadata in those documents, as well as the name Felix Drzezhinsky, the founder of the Soviet secret police. This was described,

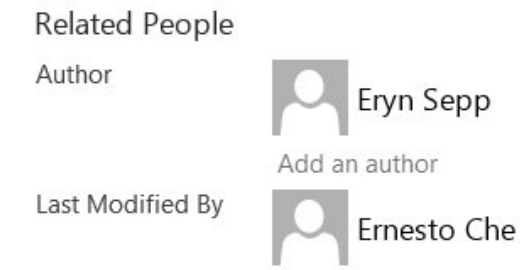
persistently, as an accident.

> The metadata in the leaked documents are perhaps most revealing: one dumped document was modified using Russian language settings, by a user named “Феликс Эдмундович,” a code name referring to the founder of the Soviet Secret Police, the Cheka, memorialised in a 15-ton iron statue in front of the old KGB headquarters during Soviet times. The original intruders made other errors: one leaked document included hyperlink error messages in Cyrillic, the result of editing the file on a computer with Russian language settings. After this mistake became public, the intruders removed the Cyrillic information from the metadata in the next dump and carefully used made-up user names from different world regions, thereby confirming they had made a mistake in the first round.

I noted, even at the time, the claim that someone who deliberately adopted the name of Iron Felix just accidentally saved the document with cyrillic characters made zero sense.

> Particularly with regards to the Russian metadata, you don’t both adopt a notable Russian spook’s ID while engaging in a false flag but then “accidentally” leave metadata in the files, although the second paragraph here pertains to Guccifer 2 and not the Crowdstrike IDed hackers.

Moreover, Guccifer 2 himself pointed out what Sam Biddle had already reported: the identity metadata was not limited to Iron Felix, but included Che Guevara and (I’ve been informed) Zhu De.




O secundă, vă rog [A second, please]


Since then, some folks have looked closer and compellingly argued that the Russian metadata "accidentally" left in the documents was actually made at significant effort by opening a word document, putting some settings onto Russian language, and then copying one after another document into that document.

That said, that doesn't mean — as some of the same folks suspect — that a Hillary staffer made the documents. This post provides five alternative possibilities.

And one thing that those arguing the Guccifer figure was created to obfuscate Russia's role didn't connect that claim that — as I've heard and Jim Comey recently confirmed — this second DNC hacker was obnoxiously loud in the DNC servers.

> COMEY: The only thing I'd add is they were unusually loud in their intervention. It's almost as if they didn't care that we knew what they were doing or that they wanted us to see what they were doing. It was very noisy, their intrusions in different institutions.

Effectively, then, the second DNC hacker (usually attributed to GRU) was leaving graffiti inside the DNC servers and Guccifer 2 effectively left graffiti on the documents he released.

In any case, the same rush to interpret the metadata is happening now on the Macron hack as it did with the DNC hack, with repeated claims the hackers — whom people assume are the same as the ones that targeted DNC — are sloppily leaving metadata again.

If they are the same hackers (which has not yet been proven) then we sure as hell ought not assume that the metadata is there accidentally. Again, that doesn't mean this isn't GRU. But it does mean the last time people made such assumptions they ended up arguing ridiculously that someone trying to obscure his ties to Russia was at the same time paying tribute to them.

Sometimes, it turns out, the metadata is the message.