YOUR WEEKLY ALARMING ANONYMOUS FRIDAY NIGHT WAPO DUMP: VERMONT ELECTRICAL GRID EDITION

It seems like every Friday this month, there has been an alarming Friday night news dump in the WaPo based off anonymous leaks. This time, it's a story claiming that,

> *Russian hackers penetrated U.S. electricity grid through a utility in Vermont*

The anonymous officials behind this story have just squandered the efforts of a slew of infosecurity professionals trying to get non-experts to take the attribution of the DNC hack seriously.

The story, which features WaPo White House bureau chief Julie Eilperin first on the byline (followed by the usually strong Adam Entous) but does not include WaPo's cybersecurity reporter Ellen Nakashima at all, claims that "a code" associated with the family of signatures associated with several Russian hacking groups that Obama dubbed Grizzly Steppe for the purposes of yesterday's CERT report was found "within the system of a Vermont utility." The language of the report — what do they mean by "code"??? — exhibited no certitude about what the report actually meant.

The original version of the story included no comment from Burlington Electric Department,

though added one after the Burlington Free Press revealed that the "code" was not actually in the grid at all, but in a laptop unattached to it. As the Free Press explained, there's really no reason to worry this would affect the grid.

> The utility found the malware Friday on a laptop after the Obama administration released code associated with the campaign, dubbed Grizzly Steppe, on Thursday.
>
> The aim of the release was to allow utilities, companies and organizations to search their computers for the digital signatures of the attack code, to see if they had been targeted.
>
> The computer on which the malware was found was not connected to the operation of the grid, Vermont Public Service Commissioner Christopher Recchia said.
>
> Based on his knowledge, Recchia said Friday night he did not believe the electrical power grid was at risk from the incident. "The grid is not in danger," Recchia said. "The utility flagged it, saw it, notified appropriate parties and isolated that one laptop with that malware on it."

So here's what appears to have happened.

Yesterday, along with all the sanction-related information, DHS released a US-CERT report attempting to draw together all the signatures from the two Russian related hacking groups accused of hacking the DNC. Numerous security experts have criticized it, noting that it reads like "a poorly done vendor intelligence report stringing together various aspects of attribution without evidence" and finding that "21% (191 of 876) of [IP addresses included in the report] were TOR exit nodes," meaning there are a lot of worse-than-useless details in the report.

That in and of itself was a problem. But then potential Russian targets, including utilities, started scanning their system for the malware included in the report and one of two Vermont utilities found one malware signature on a laptop and alerted the government. The other one is spending its Friday night insisting it was unaffected.

At which point multiple "US officials" (which can include Congressional staffers) and one Senior Administration Official (who, given Eilperin's involvement, is likely at the White House) ran to the press and insinuated that Russia had *hacked our grid*, even while admitting they don't really know what the fuck this is.

> American officials, including one senior administration official, said they are not yet sure what the intentions of the Russians might have been. The incursion may have been designed to disrupt the utility's operations or as a test to see whether they could penetrate a portion of the grid.
>
> Officials said that it is unclear when the code entered the Vermont utility's computers, and that an investigation will attempt to determine the timing and nature of the intrusion, as well as whether other utilities were similarly targeted.
>
> "The question remains: Are they in other systems and what was the intent?" a U.S. official said.

Of course, by the time this report was amended to make it clear the malware was not in the grid at all, the story itself had gotten picked up by other outlets, even in spite of the many many many security professionals mocking the report as soon as it came out.

So now a slew of people are convinced that Russia has hacked (a word that has lost all meaning in the last month) our electrical grid —

I've even seen some people assuming this occurred this week! — even though no actual analysis of what is going on has happened yet.

Here's the thing. Some of these security professionals are the same ones who've been saying for months that the DNC hack can be reliably attributed to the Russian state. I mostly agree (though I've got some lingering doubts). And while those of us who follow this closely can distinguish the two different kind of analyses, the general public will not. And — having been alarmed off a premature report here that was not sufficiently researched before publicized — they will be utterly justified in believing the government is making baseless claims to generate fear among the public.

As I said, I mostly agree with reports attributing the DNC hack to the Russians. But seeing inflammatory shit like this peddled anonymously to the press makes me far more inclined to believe the government is blowing smoke.