WAS "COMPUTER NETWORK" "ANALYTICS DATA PROGRAM" HACKED AT HILLARY HQ VAN OR SOMETHING ELSE?

Several outlets have reported that Hillary's campaign — or rather, a network the Hillary campaign uses — got hacked along with the DNC and DCCC, presumably by the same APT 28 group presumed to be Russia's military intelligence GRU. But reports on this, coming after a day of equivocation about whether Hillary's campaign had been hacked at all, are unclear.

Reuters explains hackers accessed an "analytics program server" for five days (though doesn't provide a date for that access).

> A Clinton campaign spokesman said in a statement late on Friday that an analytics data program maintained by the DNC and used by the campaign and a number of other entities "was accessed as part of the DNC hack."
>
> [snip]
>
> Later, a campaign official said hackers had access to the analytics program's server for approximately five days. The analytics data program is one of many systems the campaign accesses to conduct voter analysis, and does not include social security numbers or credit card numbers, the official said.

KTLA (working off a CNN feed, I think) described the target as a "dynamic voter database — with voter participation, voter contact information and voter files all campaign organizations use."

> A person familiar with the Clinton campaign program described it as essentially a dynamic voter database — with voter participation, voter contact information and voter files that all campaign organizations use. It's a list — but a dynamic one with key voter data.
>
> A Clinton aide said the hackers had access to the analytics program's server for approximately five days. The analytics data program is among many systems accessed to conduct voter analysis. It does not include social security numbers or credit card numbers.
>
> The aide noted further that according to the campaign's outside cyber security expert, the hack of this analytics data program could not have resulted in access to Clinton campaign internal emails, voicemails, computers or other internal communications and documents. Those are completely independent systems.

Some, though not all, of those reports is based off this circumspect statement from Nick Merrill.

> An analytics data program maintained by the DNC, and used by our campaign and a number of other entities, was accessed as part of the DNC hack. Our campaign computer system has been under review by outside cyber security experts. To date, they have found no evidence that our internal systems have been compromised.

Meanwhile, the FBI sources in these stories seem hesitant to definitively tie this hack to the others.

I raise all this because the KTLA description of the program *sounds* a lot like VAN, the voter management program that has already made the news several times this election year. VAN is

dynamic and accessible to all Democratic campaigns so they can share data about voter participation, contacts, and enthusiasm for one or another candidate.

But if it were VAN it'd be of particular interest for two reasons. First, because a firewall between Hillary and Bernie's campaigns went down in December, just as Bernie's campaign finished up an utterly historic fundraising day. A few of Bernie's staffers accessed some of Hillary's data — they said to monitor the extent of the breach, which they claimed was the second time it had happened. Bernie sued the DNC over the insecurity of the VAN, but ultimately he ended up punishing several staffers.

In other words, by December, if not before, the DNC had warning that the VAN was unstable. If the hack was of VAN and if it was in any way associated with this time period — or if it was a response to DNC taking no action to force VAN to improve security — then it would be very damaging to the Democrats.

If this hack was of VAN, it would also be significant given that Guccifer 2's technically bogus explanation of how "he" hacked the DNC claimed he got in through VAN.

> ***How did you break into the DNC network? And are you still in?***
>
> These questions are also very popular. I've already said about the software vulnerabilities. The DNC had NGP VAN software installed on their system so I used the 0-day exploit and then deployed my backdoor. The DNC used Windows on their server, so it made my work much easier. I installed my Trojan like virus on their PCs. I just modified the platform that I bought on the hacking forums for about $1.5k.
>
> I've been inside the network for pretty long time, so I downloaded a lot of files. I lost access after they rebooted the system on June 12. But after all, if

> they'll carry on like this it won't be a problem to get in again and again.

I've worked with VAN (albeit in a county party office) and I can't think of a way it would be hooked up to more substantive computers (hmm—except perhaps within a computer and from there back up through a network). And the explanation appears bogus for a number of other reasons. But it would be interesting if Guccifer 2 had pointed to VAN weeks before the campaign decided to check whether VAN had been accessed (after having been proven to be unstable in the primary).

Finally, it would be interesting if it were VAN for one more reason: because after the December incident, Bernie moved off of VAN. Which means he has files protected from whatever the Russians or whoever else have been up to.