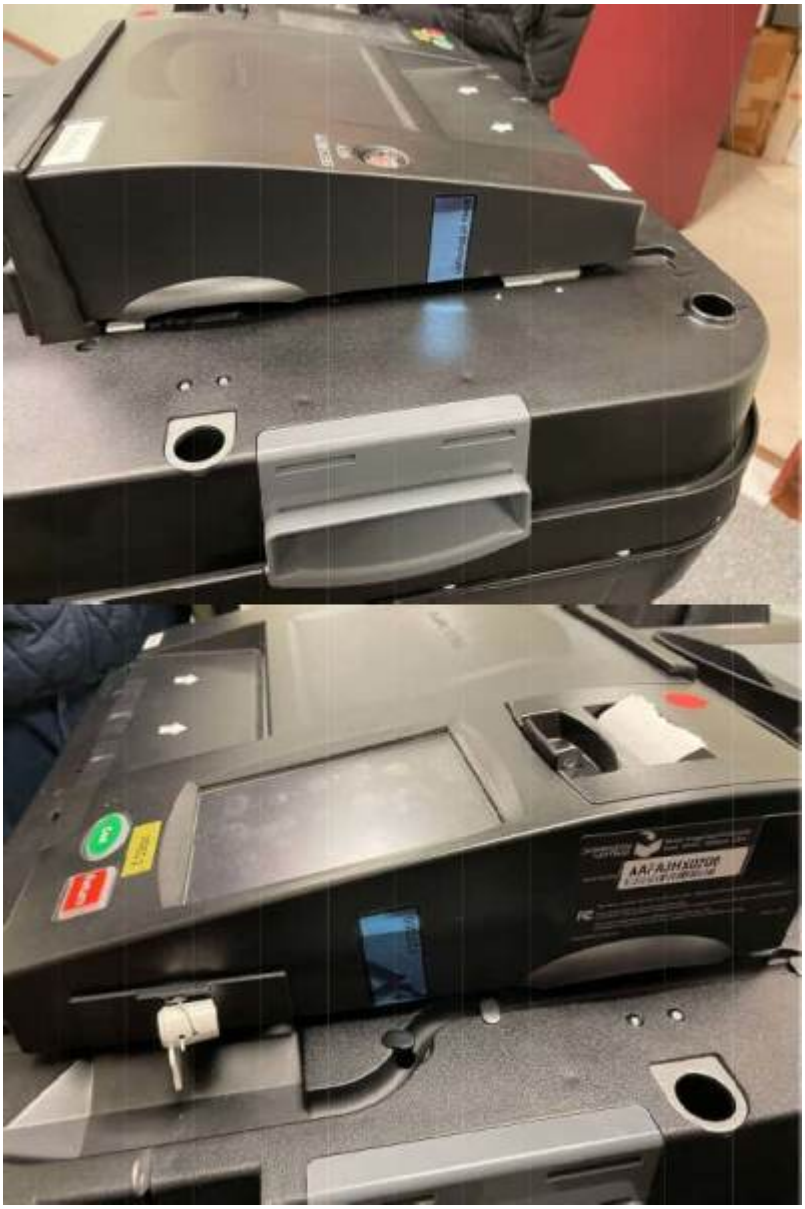
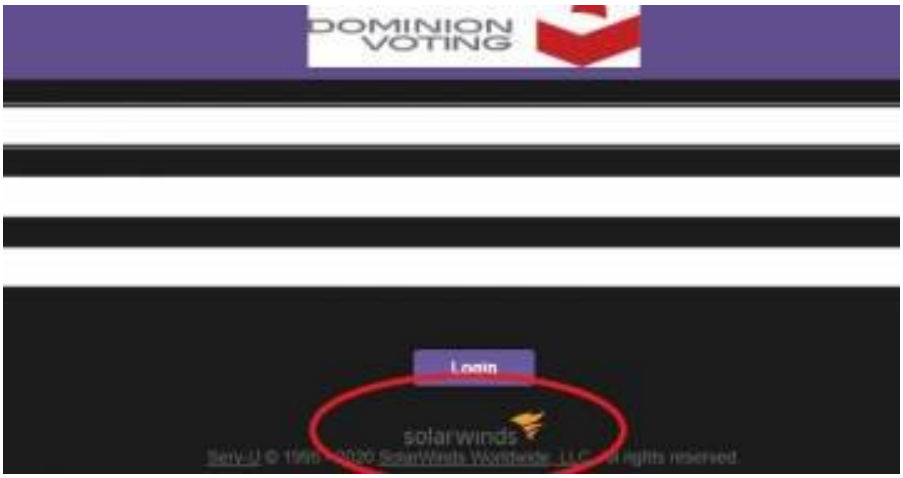
Dominion Voting Machines Are Trying to Hide Their Relationship with SolarWinds – Why's That?

By Joe Hoft
Published December 15, 2020 at 8:59am
530 Comments



Dominion is trying to hide their relationship with SolarWinds.

We reported yesterday that late Sunday night the Cybersecurity and Infrastructure Security Agency (CISA) issued a rare Emergency Directive 21-01, in response to a KNOWN COMPROMISE involving SolarWinds Orion products.



HUGE UPDATE: Dominion Voting Systems Uses SolarWinds — Same Company CISA in Rare Warning Reported Was Breached, Compromised and Should Be Disconnected!!

THIS IS A HUGE UPDATE! Last night the The Cybersecurity and Infrastructure Security Agency (CISA) issued a rare Emergency Directive 21-01, in response to a KNOWN COMPROMISE involving SolarWinds Orion products. This was only the fifth Emergency Directive issued by CISA under the authorities granted by Congress in the Cybersecurity Act of 2015. CISA reported ... Continue reading

GP The Gateway Pundit

It turns out that Dominion was trying to hide the fact that they were connected with SolarWinds:

Ron
@CodeMonkeyZ

Dominion deleted the reference and link to "SolarWinds"

Dominion deleted the reference and link to "SolarWinds" from their website, but we have the archive still.

Now you see it... now you dont.

dvsfileshare.dominionvoting.com/Web%20Client/M...
web.archive.org/web/2020121409...

9:14 AM · Dec 15, 2020

31.6K 16.5K people are Tweeting about this

One reader shared with us some thoughts about SolarWinds technology:

> *I work in IT and I am now left wondering if Solar Winds was used as a backdoor "jump host" to get into Dominion machines. If the machines each had a unique hostname and they were being connected to a central network it is a rational way to explain it. A "jumphost" is a server (which is very bad security practice, by the way) that contains all the hosts on a network with their hostnames and ip addresses so you can just "jump" to them or remote to them. If they did indeed put a backdoor in Solar Winds and connected these to a network, this is how they would do it: Solar Winds might be hacked to be a jumphost. I cannot say this is true for sure, but it is worth digging into. A "jumphost" is bad because it puts all your*

> *hosts and devices into one basket and if a hacker gets in there, you can only imagine what a nightmare they can create.*

Another IT professional shared this:

> *I am also an IT professional that uses SolarWinds. We use SolarWinds to manage network equipment, servers, etc. SolarWinds is a very powerful tool. SolarWinds has a scripting tool capable of automated task scheduling for configuration management. So say you had 1000 or more voting machines spread across the country. You could build scripts to download data from or upload data to rapidly in seconds. SolarWinds services and accounts are granted elevated permissions on equipment to perform these tasks. Hackers could take over a company's SolarWinds management server to use as a "zombie" and orchestrate attacks on voting machines from all over making it difficult to track.*

No wonder Dominion is trying to hide their connection to SolarWinds.