Dominion Serv-U Cover-Up

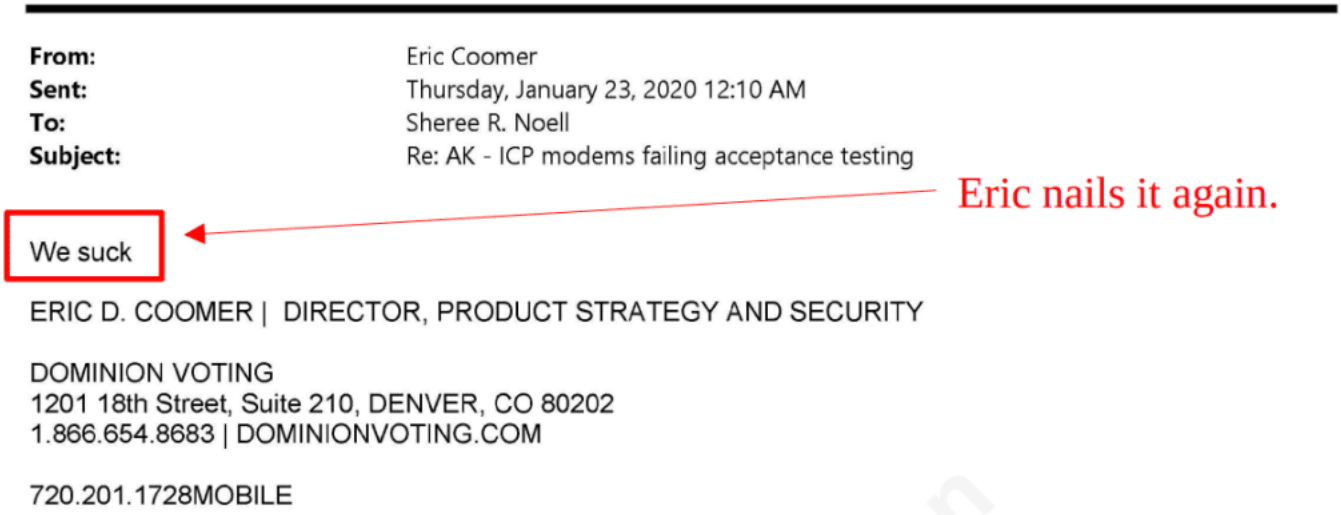
May 10, 2024

These lying idiots at Dominion were running an exploitable Serv-U FTP server on their public-facing dvsfileshare.dominionvoting.com IP address. When they got caught, they took place in a 17-hour cover-up operation. They initially took their page down, then edited it so it didn't show the SolarWinds name, just leaving Serv-U (but the morons left it in the page source code), then later they removed even the Serv-U portion, but still again left SolarWinds in the page source code (they weren't smart enough to remove it entirely). If they can't even figure out how to cover their tracks on something this simple, they have no business writing software to handle our elections. Not to mention, innocent people DO NOT TRY TO CONCEAL THINGS LIKE THIS!

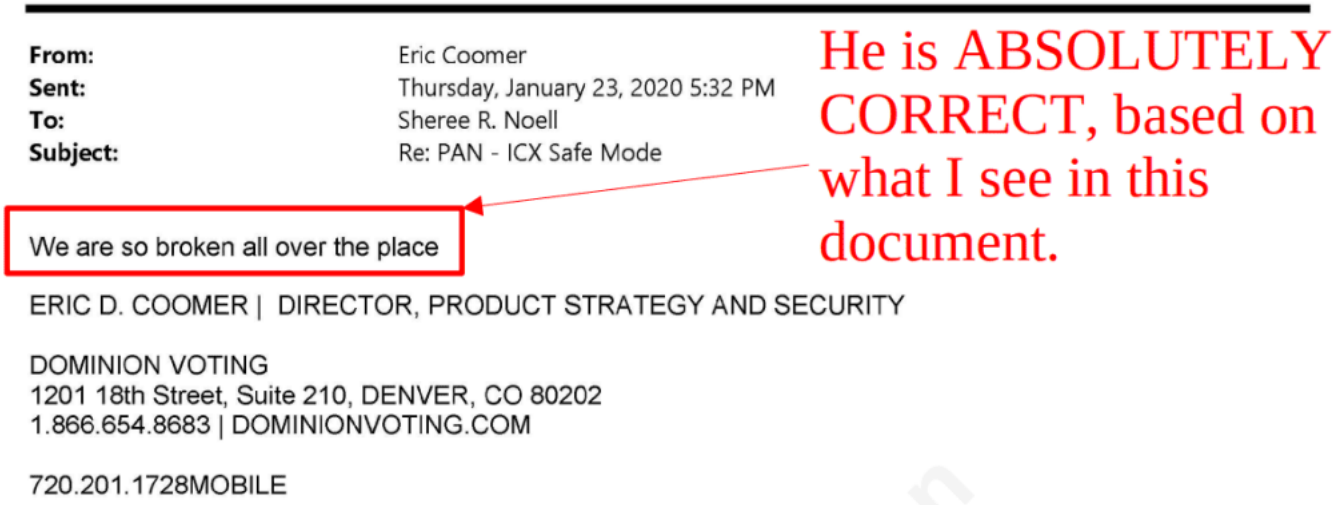


Then everyone freaked out because of the SolarWinds Orion Platform hack and Dominion misdirected all the pleebs at that and then claimed they don't use Orion. What the pleebs didn't realize is that there was ALSO a zero-day exploit on the Serv-U 'FTP' software that Dominion was using up until and at that time, and they bought the BS from Dominion, hook, line, and sinker. Nobody that falls for this should be using electronic voting systems (or much less, anything electronic). I don't mean to come down on those deceived by Dominion, but at some point they do need to take responsibility for not having enough knowledge to protect a domain that they claim to be responsible or making decisions for. It is UNFAIR to put them in these positions, but it is important to notify them that they ARE in these positions so they can't claim ignorance after being put on friendly notice.

So let's walk through it. First, sometimes people at Dominion are honest, and I am happy to point that out when I see it.



Eric is not a stupid person by any means. I do wish he used his intelligence to help his fellow man, though.



Based on the evidence I have seen that clearly Eric knows about, as he is listed as a sender and/or recipient of many of the emails that shed a bright light on what is going on inside Dominion that those who blindly trust them don't know about, Eric Coomer's conclusion in the above email is very accurate.

Let's begin with the information regarding this particular Zero-Day Exploit directly from SolarWinds themselves: https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211 (PDF Serv-U-Remote-Memory-Escape-Vulnerability.pdf)

Serv-U Remote Memory Escape Vulnerability (CVE-2021-35211)

Security Vulnerability

Released: July 9, 2021

Last updated: July 15, 2021

Assigning CNA: SolarWinds

Security Advisory Summary

UPDATE July 15, 20201: You can Subscribe to this RSS Feed to be notified when we update this page (note: you will need to cut and paste the "Subscribe to this RSS feed" URL into an RSS Feed Reader, e.g., Outlook's RSS Subscriptions, to monitor updates).

UPDATE July 13, 20201: We've provided additional indicators of compromise (IOCs) below. You can also find additional details on the threat actor and their findings in a blog post from Microsoft.

UPDATE July 10, 2021: NOTE: This security vulnerability only affects Serv-U Managed File Transfer and Serv-U Secure FTP and does not affect any other SolarWinds or N-able (formerly SolarWinds MSP) products.

SolarWinds was recently notified by Microsoft of a security vulnerability related to Serv-U Managed File Transfer Server and Serv-U Secured FTP and have developed a hotfix to resolve this vulnerability. While Microsoft's research indicates this vulnerability exploit involves a limited, targeted set of customers and a single threat actor, our joint teams have mobilized to address it quickly.

The vulnerability exists in the latest Serv-U version 15.2.3 HF1 released May 5, 2021, and all prior versions. A threat actor who successfully exploited this vulnerability could run arbitrary code with privileges. An attacker could then install programs; view, change, or delete data; or run programs on the affected system.

Advisory Details

Severity

9.0 Critical

Advisory ID

CVE-2021-35211

First Published

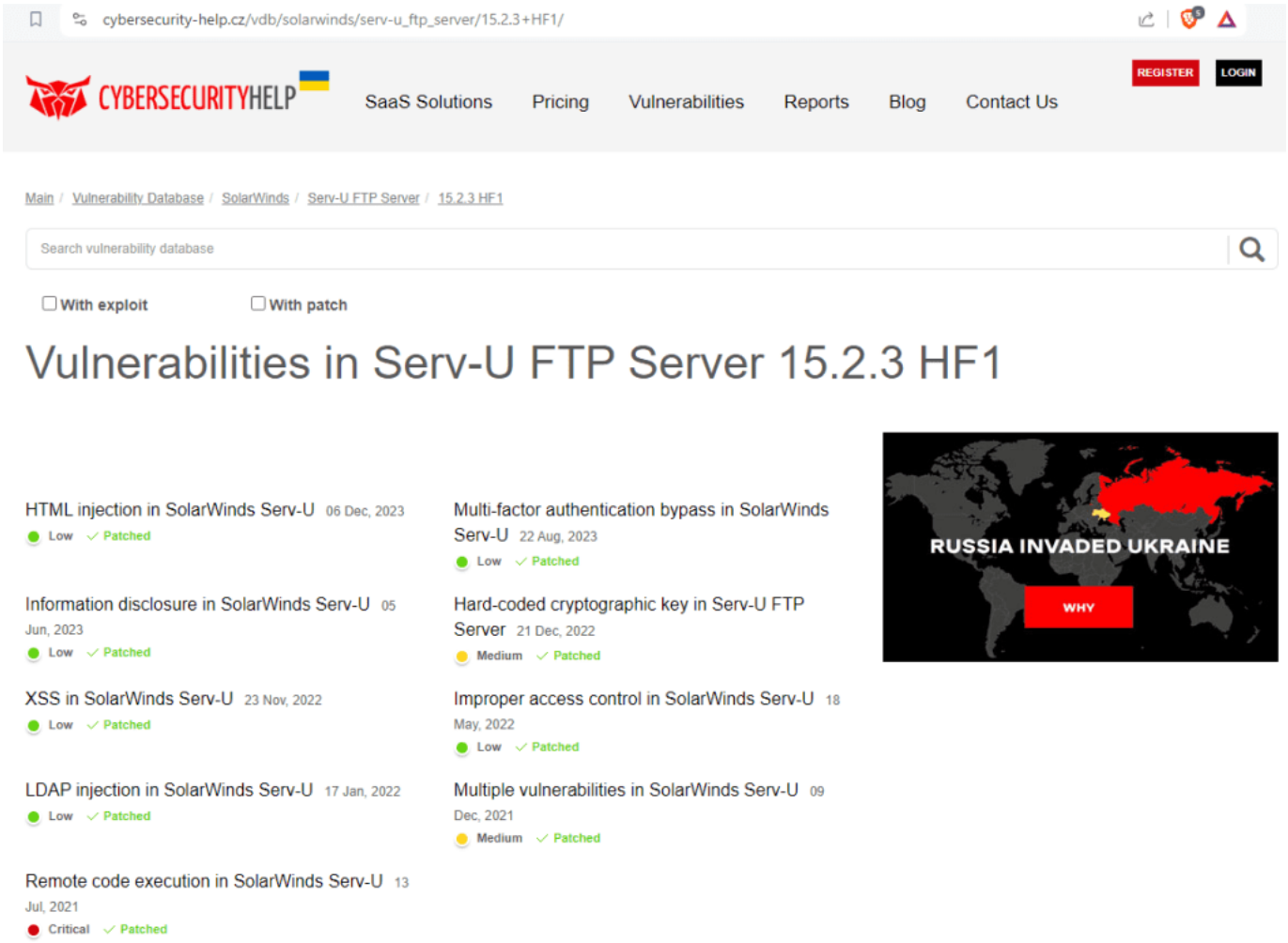
07/09/2021

Last Updated

07/15/2021

Fixed Version

Serv-U 15.2.3 HF2



Another site: [SolarWinds patches critical Serv-U vulnerability exploited in the wil_ – www.bleepingcomputer.com.pdf]

On December 13, 2020, [CISA] the Cybersecurity & Infrastructure Security Agency charged with keeping our elections secure, came out with this:

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / News & Events / Cybersecurity Directives

SHARE:

News & Events

- News
- Events
- Cybersecurity Alerts & Advisories
- **Directives**
- Request a CISA Speaker
- Congressional Testimony
- CISA Conferences

EMERGENCY DIRECTIVES

ED 21-01: Mitigate SolarWinds Orion Code Compromise

December 13, 2020

RELATED TOPICS: CYBERSECURITY BEST PRACTICES

Valeri Shilov (IT Operations Support in San Francisco CA) sent an email to David Moren and Travis Kester of Dominion Voting Systems regarding Dominion's public fileshare running on SolarWinds:

From: Shilov, Valeri (REG) <valeri.shilov@sfgov.org>
Sent: Monday, December 14, 2020 12:54 PM
To: David Moreno <david.moreno@dominionvoting.com>
Cc: Travis Kester <travis.kester@dominionvoting.com>
Subject: [EXTERNAL] SolarWinds fileshare

BINGO! Potential MASSIVE breach prior to 2020 Election!!! Did Dominion notify ANYONE prior to the election? Why didn't Election Officials know? Why didn't the public know? Why did they keep this hidden?

Hi David,

With the SolarWinds breach news yesterday, our CIO just sent me a note about the public DVS fileshare running on SolarWinds.

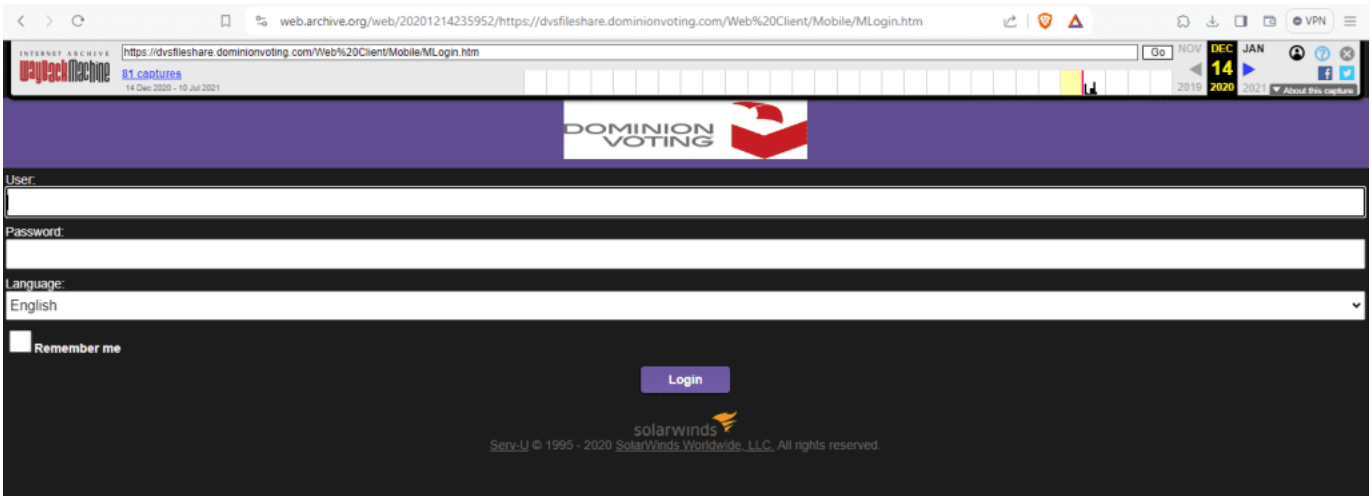
https://dvsfileshare.dominionvoting.com/Web%20Client/Mobile/MLogin.htm

https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

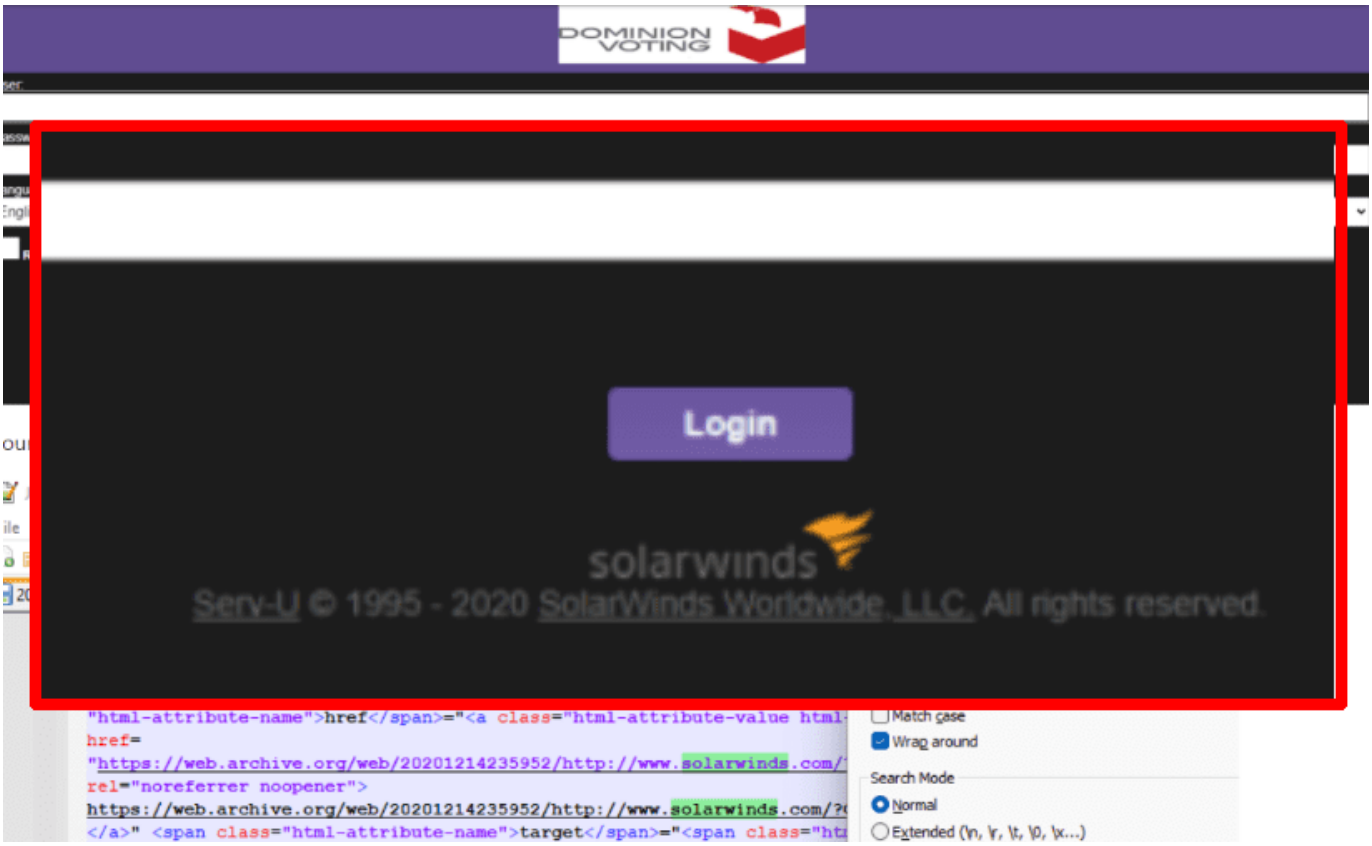
Hope all is well.

Thank you,

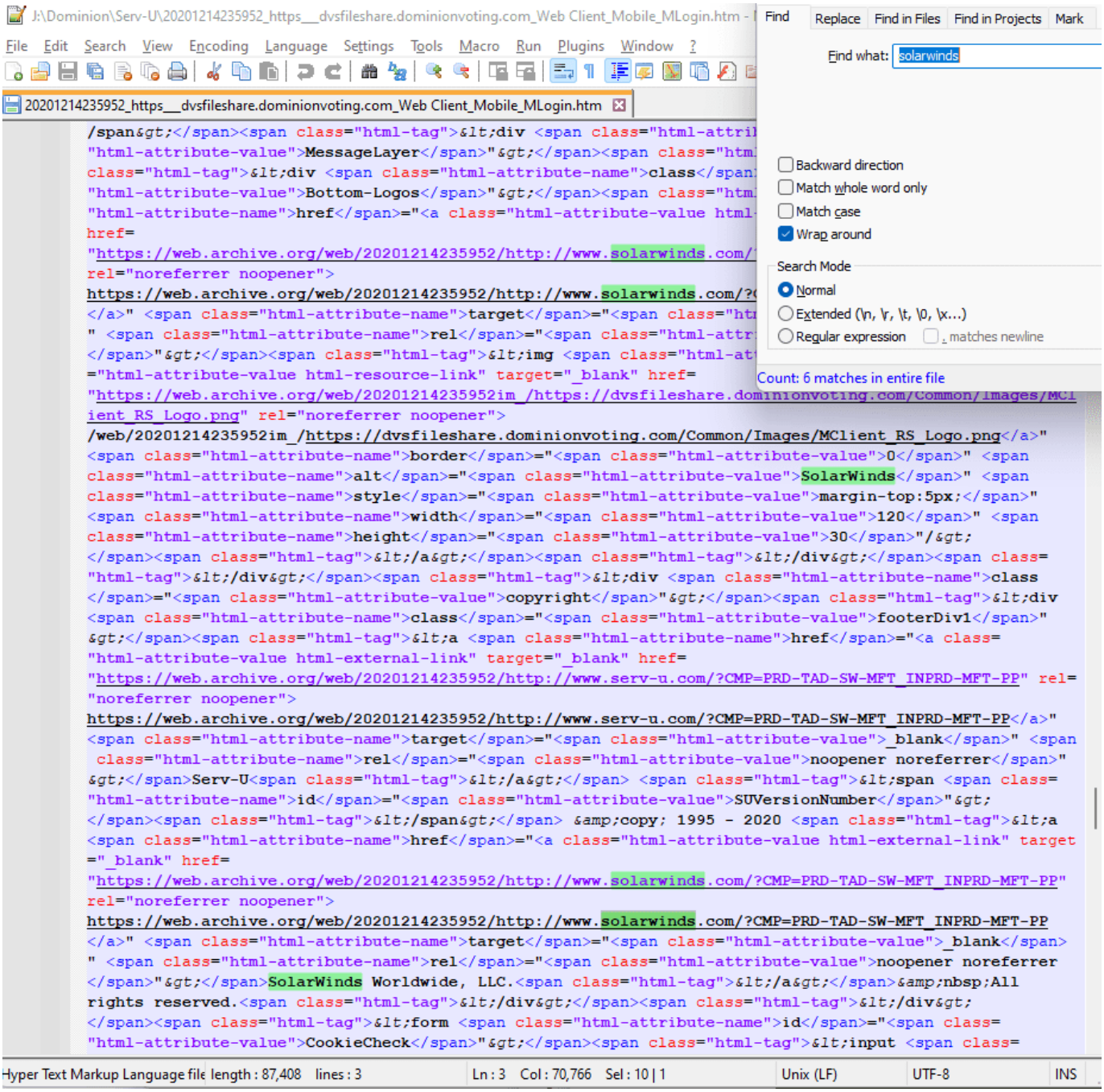
December 14, 2020 23:59, prior to the cover-up, their public file-sharing site looked like this:



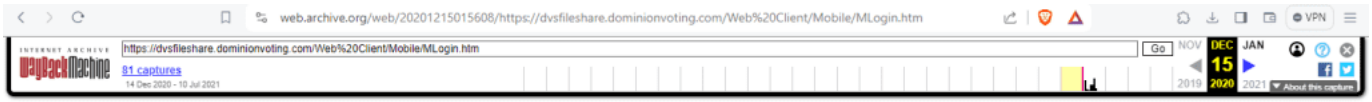
I'll zoom in for you:



The source code for their website (20201214235952_https___dvsfileshare.dominionvoting.com_WebClient_Mobile_MLogin.htm) also shows SolarWinds, which is responsible for being displayed in what you see just above:

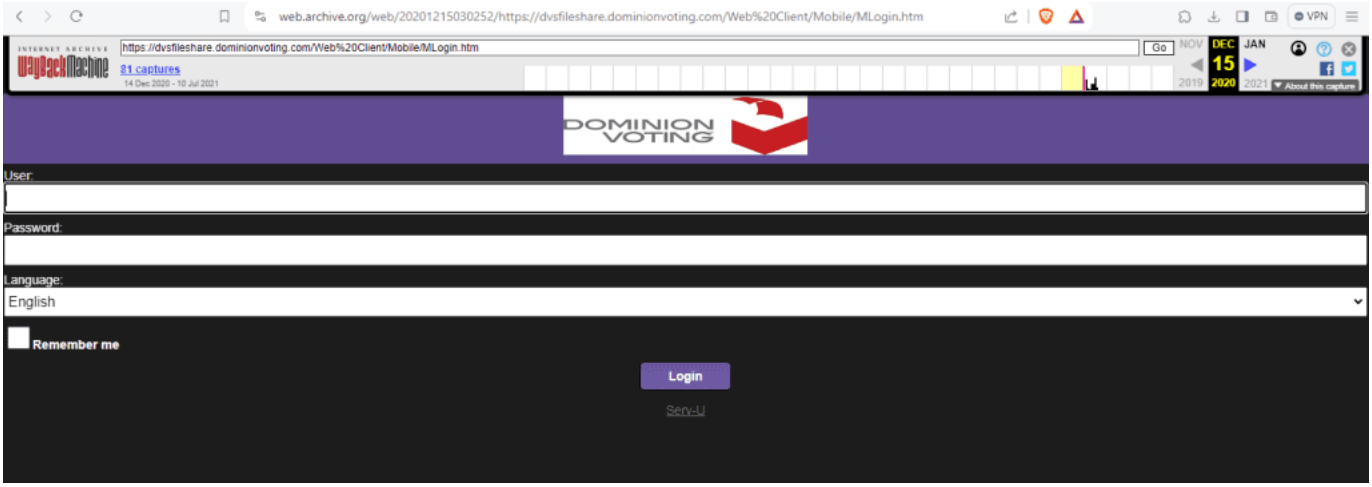


Then sometime before December 15, 2020 01:56, they take the page down:

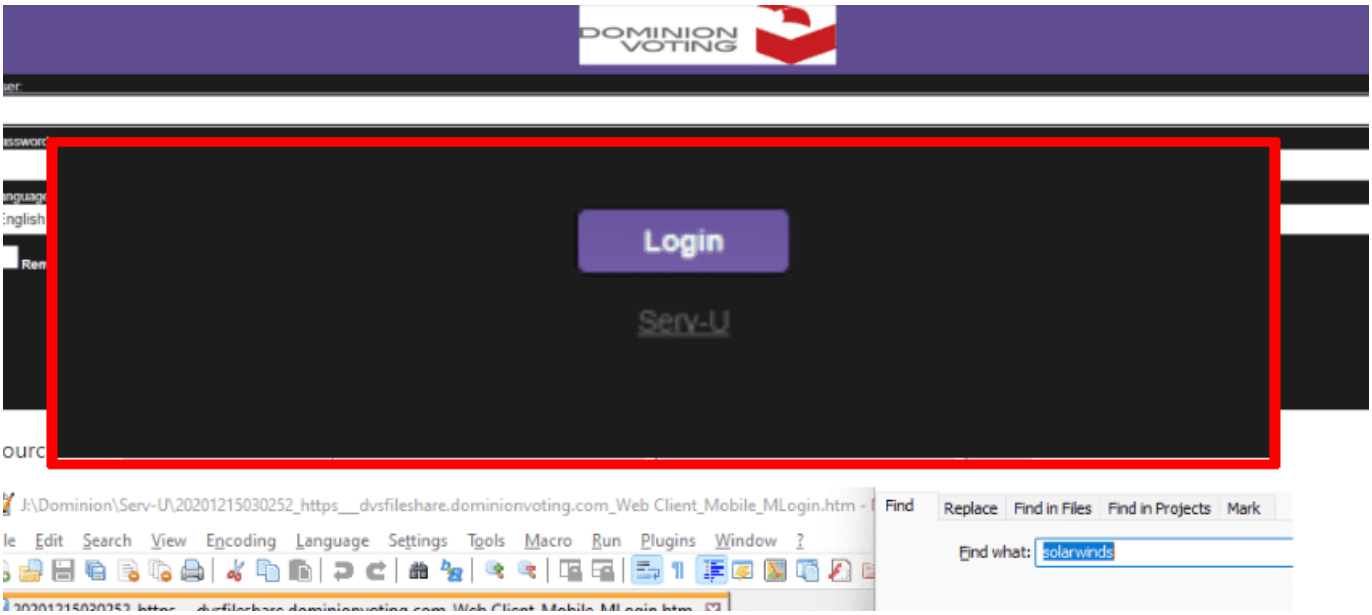


404 Not Found

Then sometime before December 15, 2020 03:02, they remove SolarWinds:

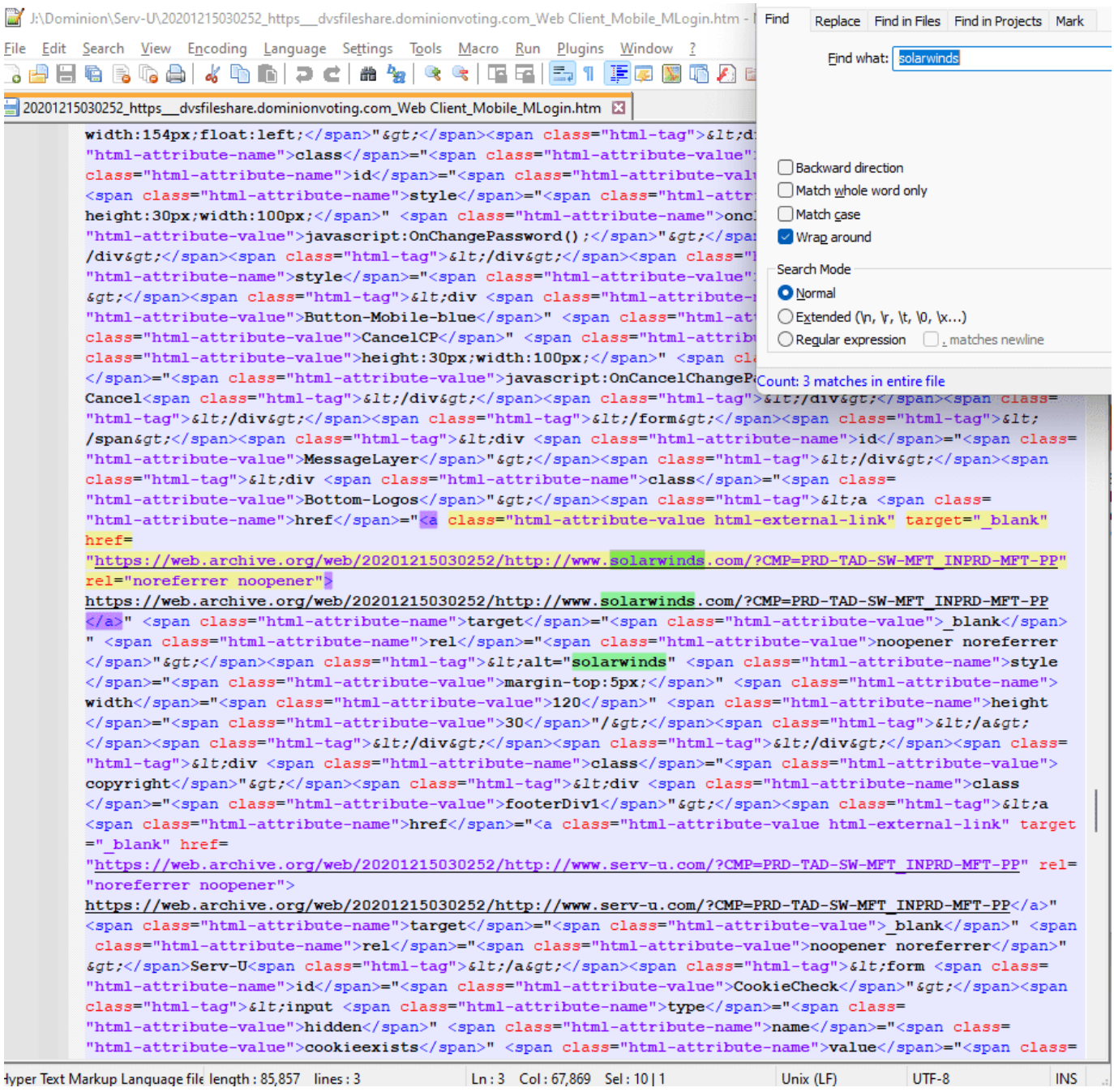


I'll zoom in again:

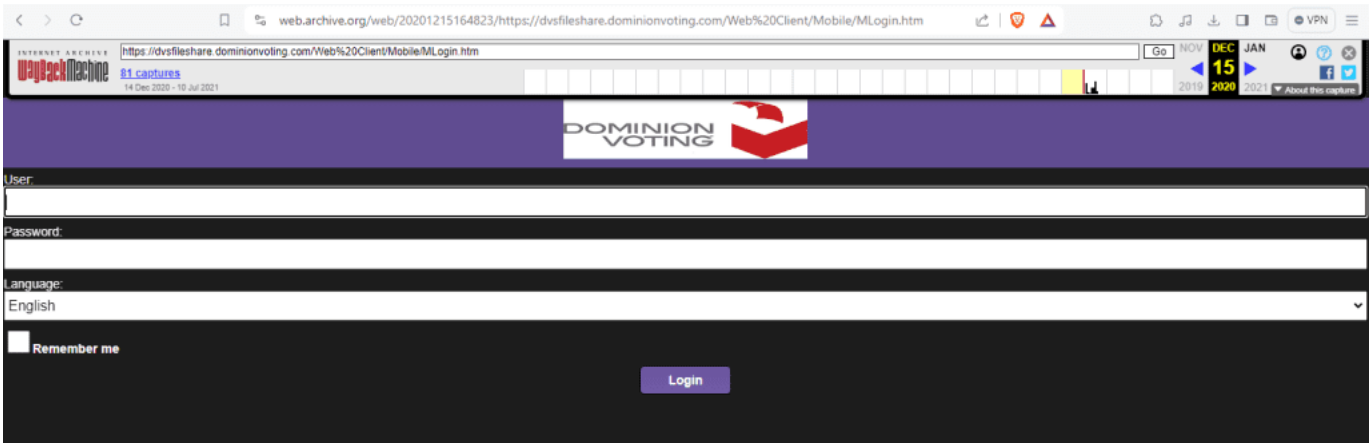


Their website source code

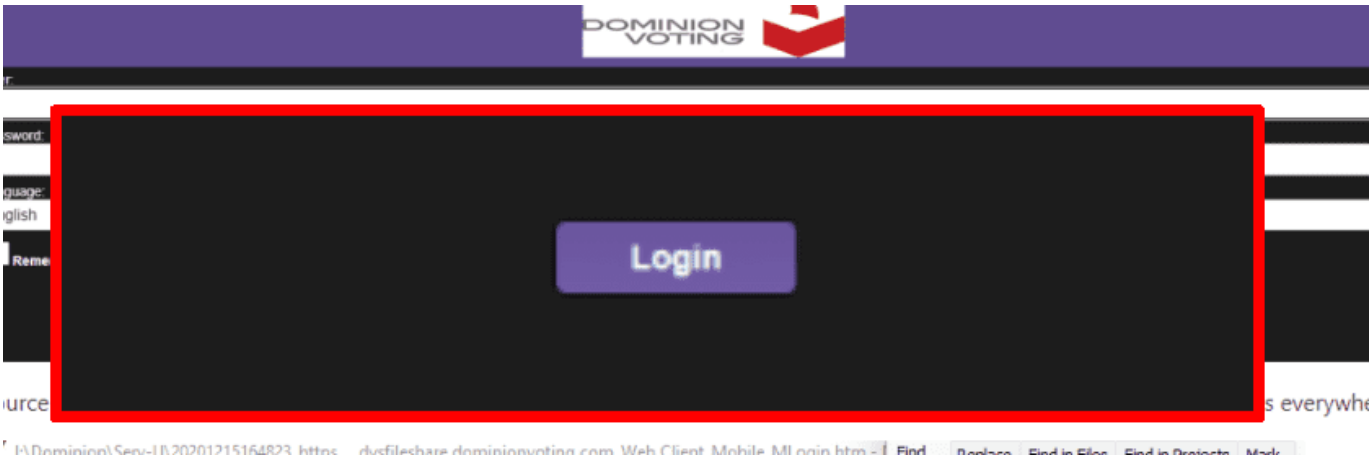
(20201215030252_https___dvsfileshare.dominionvoting.com_Web Client_Mobile_MLogin.htm) however, still has remnants of SolarWinds:



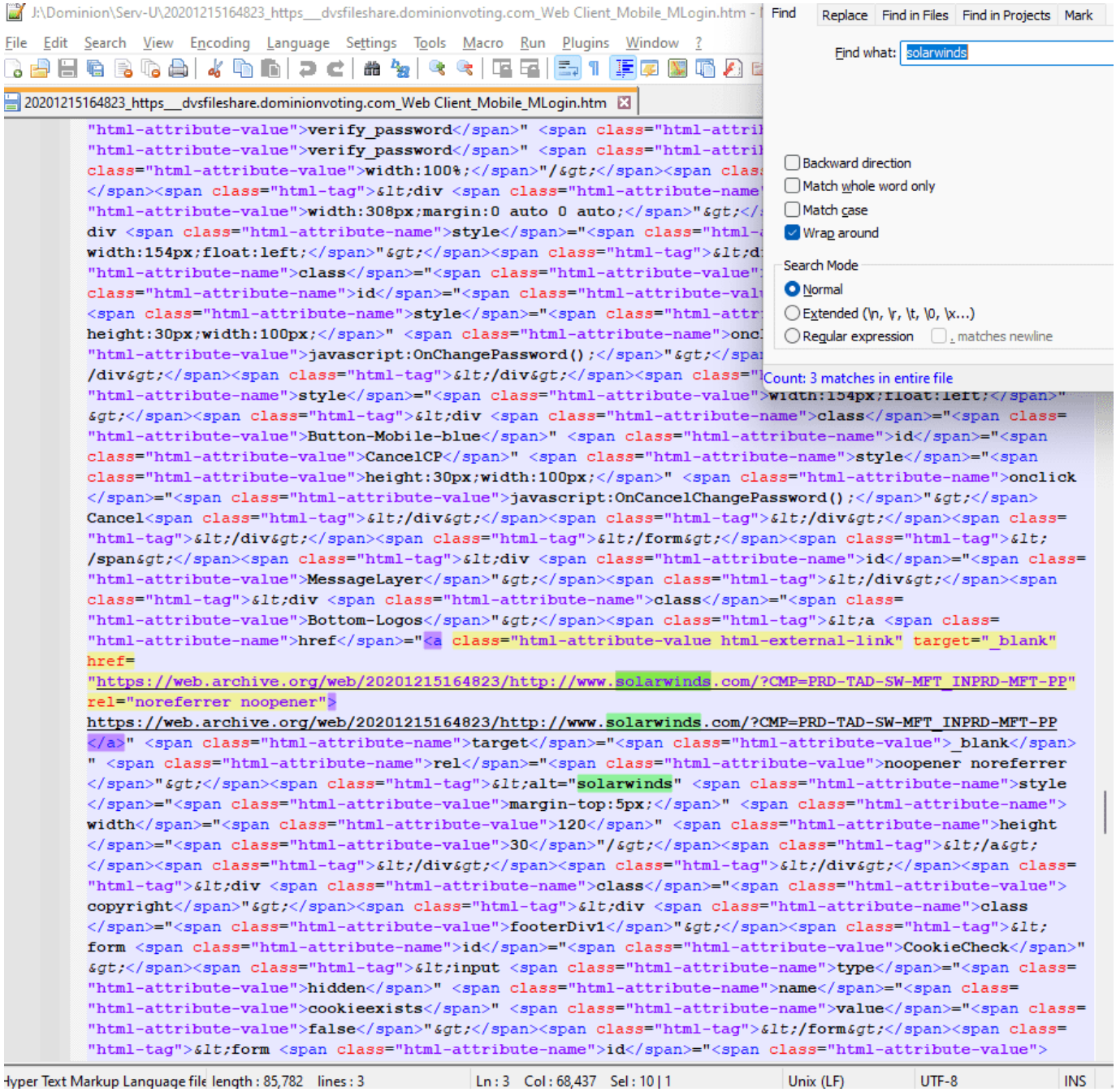
Then later in the same day at 16:48, they decide to remove Serv-U to try to cover that up as well:



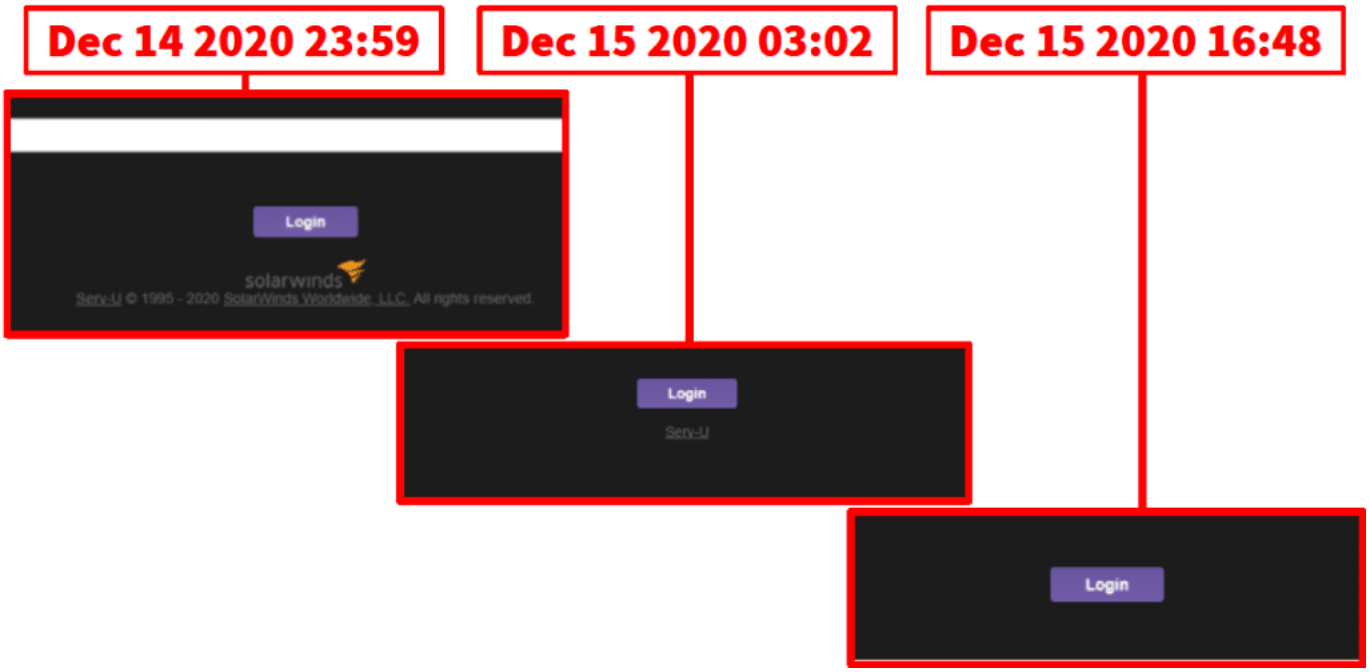
And again, I'll zoom in:



However, their website source code (20201215164823_https___dvsfileshare.dominionvoting.com_Web Client_Mobile_MLogin.htm) still shows SolarWinds everywhere:



I certainly hope it wasn't Eric Coomer that was responsible for trying to cover up the fact that they were using SolarWinds Serv-U from the public, because if it was, I guess Eric is including himself in the "we" he claims "sucks". So in summary, over a 17 hour period:



Dominion, in all the time you spent covering up your use of a compromised product on one of your public-facing file-sharing websites (and you know what files you shared on it), did you notify any government agencies about that? Did you notify any election officials? I would LOVE to ask you a lot more questions as well in a very public setting.