For Board of Elections

October 20, 2024

THE FOLLOWING IS JUST A SAMPLE AND IS NOT LEGAL ADVICE

[Your Name]
[Your Address]
[City, State, Zip Code]
[Email Address]
[Phone Number]
[Date]

To The [State] Board of Elections,[Address of the Board of Elections][City, State, Zip Code]

Subject: Legal Notice for Compliance with Election Resource Allocation and Voter Accessibility

Dear Members of the [State] Board of Elections,

This letter serves as an official notice regarding your statutory and fiduciary duties to ensure an adequately resourced and accessible election process for all citizens of [State]. As the entity charged with overseeing election administration at the state level, your compliance with both state and federal election laws is paramount.

Legal Obligations:

1. **Voting Rights Act of 1965:** This federal law ensures that all citizens have equal opportunity to participate in the electoral process without discrimination.

2. **Help America Vote Act (HAVA) of 2002:** Among other mandates, HAVA requires accessibility for voters with disabilities and improvements in election technology and procedures.
3. **[State Election Code, e.g., Title XX, Chapter YY]:** These statutes detail specific requirements for election resource allocation, including the number of voting machines per capita, staff training, and voter education efforts.
4. **Americans with Disabilities Act (ADA):** Requires that public services, including voting, be accessible to individuals with disabilities.

Required Measures:

- **Adequate Resource Deployment:** Ensure sufficient voting equipment, polling locations, and staff, as outlined in [State Election Statute], to manage voter turnout without excessive wait times.
- **Training Programs:** Implement rigorous training for all election workers to handle voting procedures, emergency protocols, and accessibility accommodations as per state directives.
- **Public Voter Education:** Execute a thorough campaign to inform voters of their rights, polling place changes, voter ID requirements, and other pertinent information.
- **Disaster and Emergency Planning:** Develop comprehensive strategies to address potential voting disruptions caused by unforeseen events.

Legal Ramifications of Non-Compliance:

- **Legal Challenges:** Failure to adhere to these laws could precipitate lawsuits alleging voter suppression or discrimination, potentially under Section 2 of the Voting Rights Act or state equivalents.

- **Regulatory Actions:** The Board could face investigations or corrective actions from state or federal election oversight bodies, potentially including fines or mandates for operational changes.
- **Public Trust:** Any failure in election administration can severely undermine voter confidence and could lead to questions regarding the legitimacy of election outcomes.
- **Court Mandates:** Courts might intervene with injunctions or consent decrees to enforce compliance with election laws, leading to direct judicial oversight.

This notice is intended to underscore the gravity of maintaining an election system that operates smoothly, fairly, and within legal bounds. It is crucial that your Board takes all necessary steps to meet these legal requirements to prevent any disenfranchisement or legal disputes.

Please consider this communication as a formal request for your attention to these critical issues, ensuring that every eligible voter in [State] can participate in the democratic process without undue hindrance.

Thank you for your cooperation and dedication to upholding our state’s election integrity.

Sincerely,

[Your Signature (if sending a hard copy)][Your Printed Name]

Ensure to verify all cited laws and regulations with an attorney or legal expert in election law for accuracy and to tailor the specifics to the laws of your state before sending this notice.

For Secretary of State

October 20, 2024

THE FOLLOWING IS JUST A SAMPLE AND IS NOT LEGAL ADVICE

[Your Name]
[Your Address]
[City, State, Zip Code]
[Email Address]
[Phone Number]
[Date]

The Honorable [Secretary of State’s Name]Secretary of State,[State Capitol Address][City, State, Zip Code]

Subject: Formal Legal Notice Regarding State Election Resource Management and Voter Accessibility

Dear Secretary [Last Name],

I am writing to formally address the critical responsibilities of your office in overseeing state elections, ensuring compliance with both federal and state election laws. This letter serves as a legal reminder of the obligations to provide adequate resources for the upcoming election to facilitate an efficient voting process for all eligible voters, ensuring they are not required to wait longer than one hour to cast their vote.

Legal Framework:

1. **The Voting Rights Act of 1965:** Requires that no voting qualification or prerequisite to voting be imposed or applied in a manner which results in a denial or abridgment of the right to vote on account of race or color.
2. **The Help America Vote Act (HAVA):** Mandates improvements to the administration of elections, including the accessibility and efficiency of the voting process.
3. **[State-specific Election Statutes, e.g., State Election Code Section XX]:** This includes regulations on voter wait times, the ratio of voting equipment to voters, and the accessibility of voting locations.
4. **Americans with Disabilities Act (ADA):** Requires that all public entities, including state election processes, ensure accessibility for individuals with disabilities.

Mandatory Election Preparations:

- **Resource Allocation:** Ensure there are enough voting machines, ballots, and polling staff as mandated by [State Law Reference], to prevent undue delays.
- **Staff Training:** All election officials and volunteers must be adequately trained in accordance with state guidelines to handle voter registration, machine operation, and accessibility accommodations.
- **Voter Information Dissemination:** Implement comprehensive outreach to inform voters about their rights, polling locations, and any changes in voting procedures, fulfilling the educational mandates of HAVA.
- **Emergency Preparedness:** Establish and communicate clear protocols for addressing potential disruptions to the voting process.

Legal Consequences for Non-Compliance:

- **Litigation:** Your office could face lawsuits for violations of the Voting Rights Act, ADA compliance issues, or state-specific election laws, potentially leading to court-mandated election oversight.
- **Administrative Penalties:** Non-compliance might attract sanctions or fines from federal or state election commissions or other regulatory bodies.
- **Public Accountability:** Failure to ensure an efficient election could lead to a significant erosion of public trust, potentially impacting future electoral participation and legitimacy of election outcomes.
- **Injunctive Relief:** Courts may issue injunctions requiring immediate action to rectify identified deficiencies in election preparation or execution.

This notice is not merely a formality but a call to ensure that the democratic process in [State Name] is accessible, fair, and efficient for all citizens. Your office's proactive engagement in addressing these concerns will be crucial in upholding the integrity of our electoral system.

Please treat this notice with the urgency and seriousness it warrants. Should there be any lapses identified on election day or in pre-election preparations, be advised that such could prompt legal scrutiny and action.

Thank you for your attention to this vital democratic matter.

Yours sincerely,

[Your Signature (if sending a hard copy)][Your Printed Name]

Please ensure all legal references are accurate and tailored to the specific laws of your state, and consider having this document reviewed by an attorney to maximize its legal efficacy.

For Election Departments Regarding Election Day

October 20, 2024

THE FOLLOWING IS JUST A SAMPLE AND IS NOT LEGAL ADVICE

[Your Name]
[Your Address]
[City, State, Zip Code]
[Email Address]
[Phone Number]
[Date]

To Whom It May Concern,

Subject: Legal Notice for Compliance with Election Resource Allocation and Voter Accessibility Laws

Dear Election Department Officials,

I am writing to formally remind your department of its legal obligations under federal, state, and local election laws to ensure that all eligible voters can exercise their right to vote within a reasonable time frame, specifically within no more than one hour, on election day. This letter serves to underscore the importance of compliance with these laws to avoid legal repercussions.

Legal Grounds:

1. **The Voting Rights Act of 1965, as amended:** This federal law prohibits racial discrimination in voting. Inadequate resources leading to long wait times can disproportionately affect minority voters, potentially constituting a violation.
2. **The Help America Vote Act (HAVA) of 2002:** Requires states to upgrade their election administration, including ensuring accessibility for individuals with disabilities and providing adequate voting systems.
3. **[State-specific Election Laws]:** Many states have laws specifying the maximum allowable wait times, the required number of voting machines per number of registered voters, and accessibility requirements. Please refer to [State Code or Statute Number], which mandates these provisions.
4. **Americans with Disabilities Act (ADA):** Polling places must be accessible to people with disabilities, ensuring that facilities are equipped to handle all voters.

Required Actions:

- **Adequate Staffing and Training:** Ensure sufficient and well-trained staff to manage voter turnout effectively, as per [Relevant State Law or Election Code Section].
- **Voting Machine Availability:** Per [State Election Law], there must be an adequate number of operational voting machines. Malfunctions or shortages could be considered non-compliance.
- **Voter Information and Accessibility:** Provide comprehensive voter education and ensure all polling locations meet

accessibility standards, adhering to both ADA and state requirements.
- **Contingency Plans:** Develop emergency plans for unforeseen circumstances, as failure to do so can lead to violations under emergency management statutes or implied duties of care.

Consequences of Non-Compliance:

- **Legal Actions:** Failure to comply with these legal standards could result in lawsuits under federal and state laws for voter suppression or disenfranchisement. This might include class-action lawsuits or actions by advocacy groups.
- **Fines and Sanctions:** Regulatory bodies or courts might impose fines or administrative sanctions against the election officials or the department for failing to uphold voter rights.
- **Corrective Orders:** Courts could issue mandates requiring immediate corrective actions, potentially overseeing election processes to ensure compliance.
- **Loss of Public Trust:** Beyond legal ramifications, there’s a significant risk of diminishing public confidence in the electoral process, which could lead to broader democratic issues.

This notice is intended to ensure that all necessary precautions are taken to uphold the integrity of our electoral system. It is crucial for your department to review and implement these requirements diligently.

Please consider this a formal demand for compliance to prevent any legal actions that might arise from neglect of these duties.

Thank you for your immediate attention to this critical matter.

Sincerely,

[Your Signature (if sending a hard copy)][Your Printed Name]

Note: Before sending this notice, it is imperative to verify all legal references and possibly consult with an attorney specializing in election law to ensure that all cited laws are current and applicable in your jurisdiction. This will make the notice as legally binding as possible within your specific legal context.

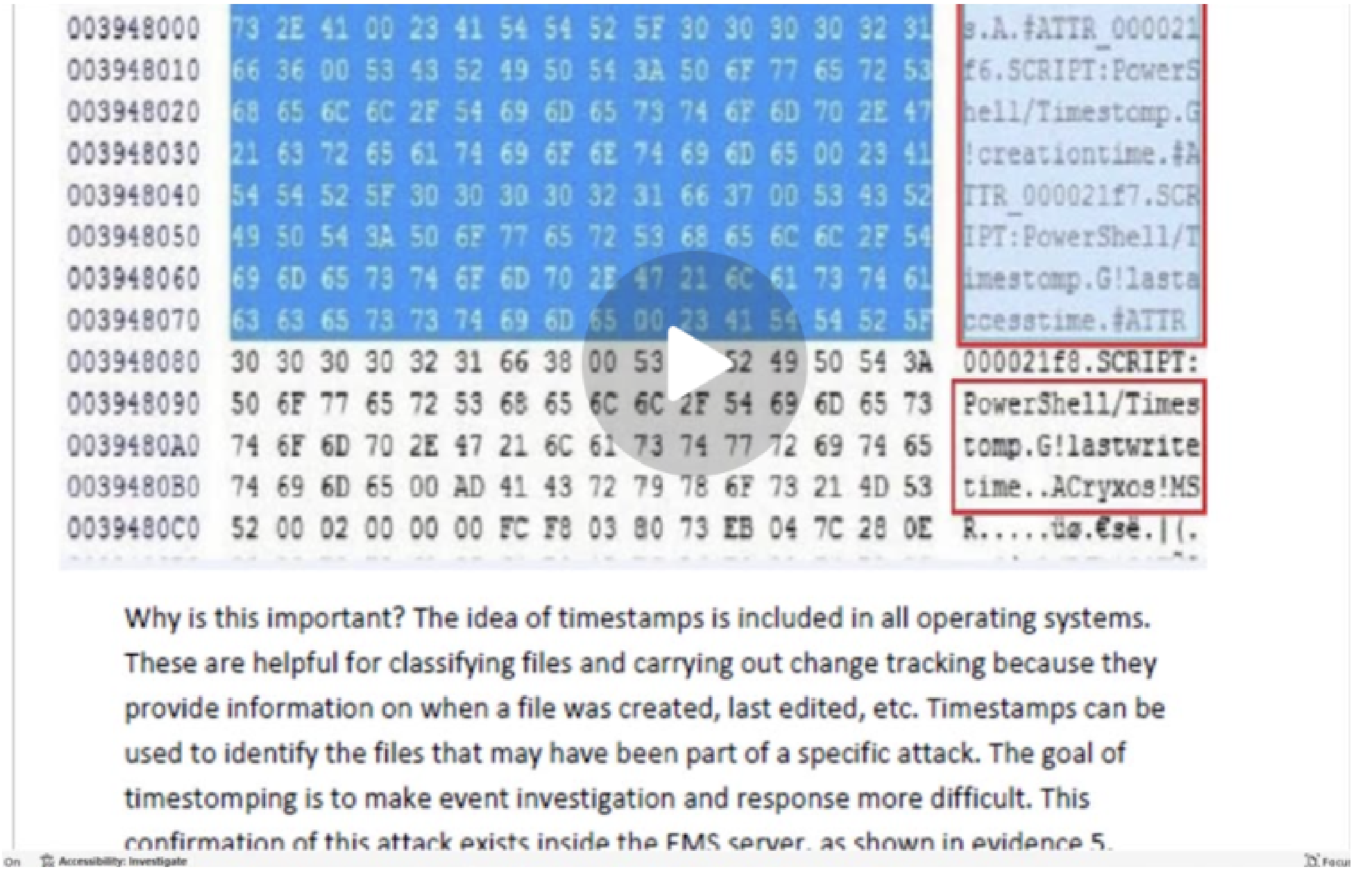
Good intentions can result in Big Problems

October 20, 2024

The claim from Jeff Boungiorno about there being a 'massive breach' Dominion's server is **NOT TRUE!!!** I'm trying to reach him to let him know. If you know him or you are him, please contact me! This is the kind of thing that happens when someone thinks they know more than they do, and jumps to conclusions without having it reviewed by people that have more knowledge. I certainly am not a fan of Dominion, and am perfectly happy to shine a light on what they do that is wrong, but in this case, I must defend Dominion on this because this claim being made is UNTRUE. The claim is that this an indication of a virus:

BOUNGIORNO: Palm Beach County Election Infrastructure Breach Proven

Staff Writer August 31, 2024 No Comments

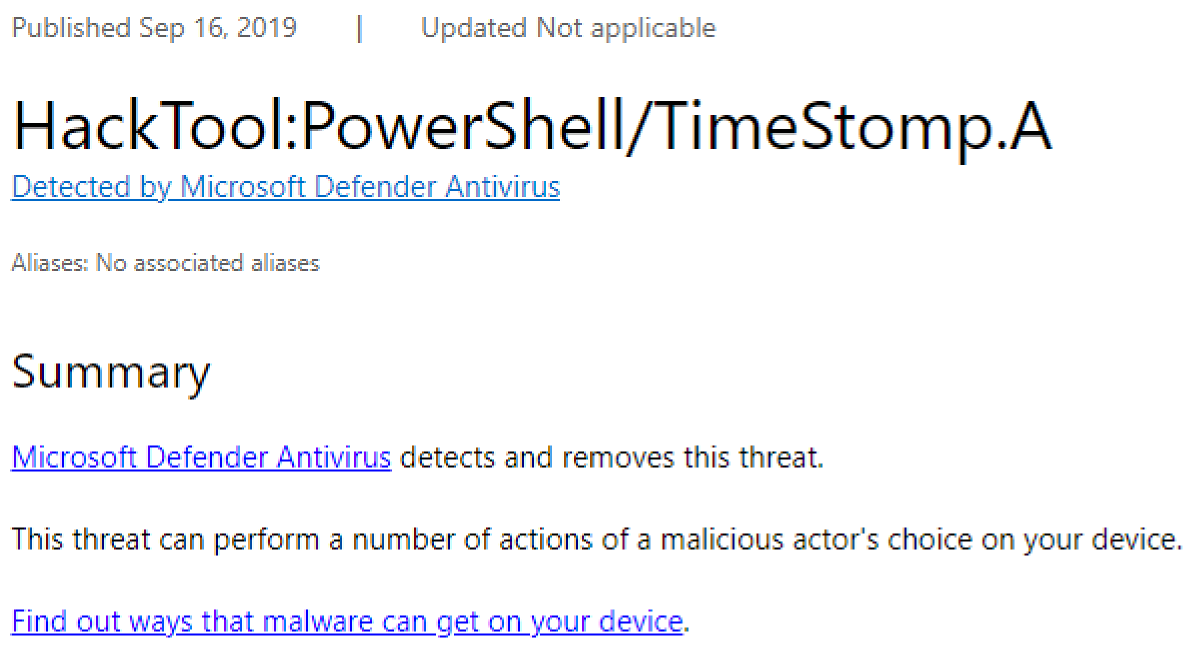


```
003948000  73 2E 41 00 23 41 54 54 52 5F 30 30 30 30 32 31  s.A.#ATTR_000021
003948010  66 36 00 53 43 52 49 50 54 3A 50 6F 77 65 72 53  f6.SCRIPT:PowerS
003948020  68 65 6C 6C 2F 54 69 6D 65 73 74 6F 6D 70 2E 47  hell/Timestomp.G
003948030  21 63 72 65 61 74 69 6F 6E 74 69 6D 65 00 23 41  !creationtime.#A
003948040  54 54 52 5F 30 30 30 30 32 31 66 37 00 53 43 52  TTR_000021f7.SCR
003948050  49 50 54 3A 50 6F 77 65 72 53 68 65 6C 6C 2F 54  IPT:PowerShell/T
003948060  69 6D 65 73 74 6F 6D 70 2E 47 21 6C 61 73 74 61  imestomp.G!lasta
003948070  63 63 65 73 73 74 69 6D 65 00 23 41 54 54 52 5F  ccesstime.#ATTR
003948080  30 30 30 30 32 31 66 38 00 53 [illegible] 52 49 50 54 3A  000021f8.SCRIPT:
003948090  50 6F 77 65 72 53 68 65 6C 6C 2F 54 69 6D 65 73  PowerShell/Times
0039480A0  74 6F 6D 70 2E 47 21 6C 61 73 74 77 72 69 74 65  tomp.G!lastwrite
0039480B0  74 69 6D 65 00 AD 41 43 72 79 78 6F 73 21 4D 53  time..ACryxos!MS
0039480C0  52 00 02 00 00 00 FC F8 03 80 73 EB 04 7C 28 0E  R.....üø.€së.|(.
```

Why is this important? The idea of timestamps is included in all operating systems. These are helpful for classifying files and carrying out change tracking because they provide information on when a file was created, last edited, etc. Timestamps can be used to identify the files that may have been part of a specific attack. The goal of timestomping is to make event investigation and response more difficult. This confirmation of this attack exists inside the FMS server, as shown in evidence 5.

Someone mistook uncompressed virus definitions in the pagefile as nefarious commands in the voting system. It is a **FALSE POSITIVE** and will serve only as a distraction and discredit vector for legitimate work and people. The part of the screen he shows is the part of the virus definitions for PowerShell/Timestomp.A and PowerShell/Timestomp/G viruses. Here are the Microsoft links on them:

https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=HackTool:PowerShell/TimeStomp.A&threatId=-2147224496



Published Sep 16, 2019 | Updated Not applicable

HackTool:PowerShell/TimeStomp.A

Detected by Microsoft Defender Antivirus

Aliases: No associated aliases

Summary

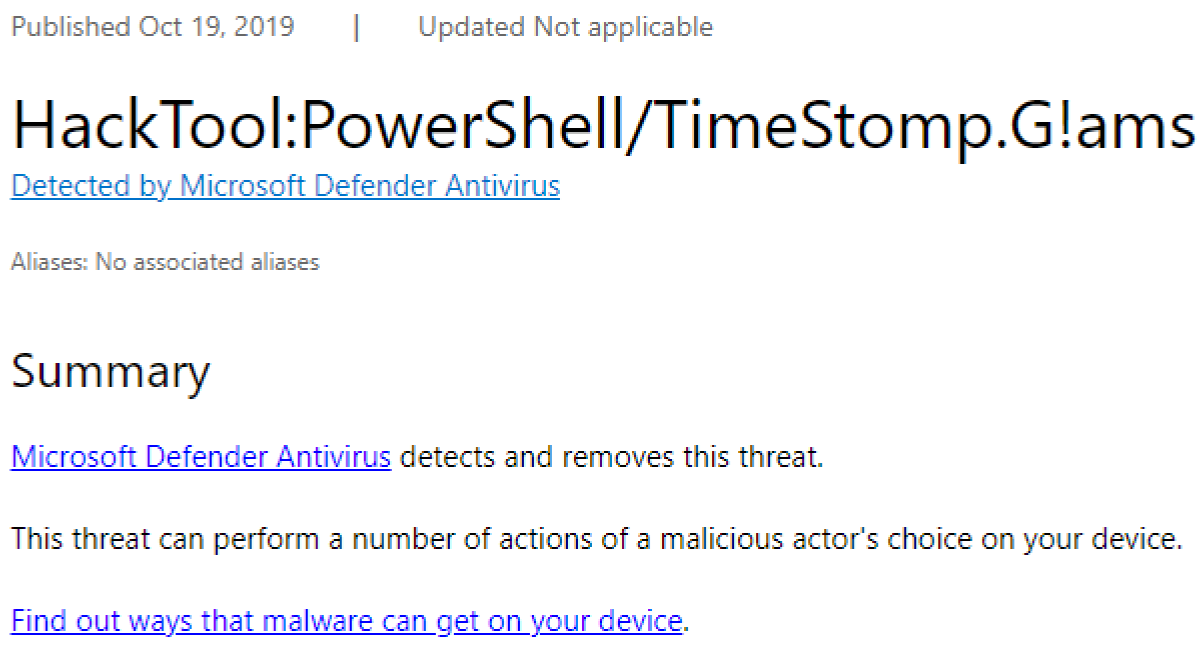
Microsoft Defender Antivirus detects and removes this threat.

This threat can perform a number of actions of a malicious actor's choice on your device.

Find out ways that malware can get on your device.

Here is the reference to PowerShell/TimeStomp.G

https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=HackTool:PowerShell/TimeStomp.G!ams&threatId=-2147223301



Published Oct 19, 2019 | Updated Not applicable

HackTool:PowerShell/TimeStomp.G!ams

Detected by Microsoft Defender Antivirus

Aliases: No associated aliases

Summary

Microsoft Defender Antivirus detects and removes this threat.

This threat can perform a number of actions of a malicious actor's choice on your device.

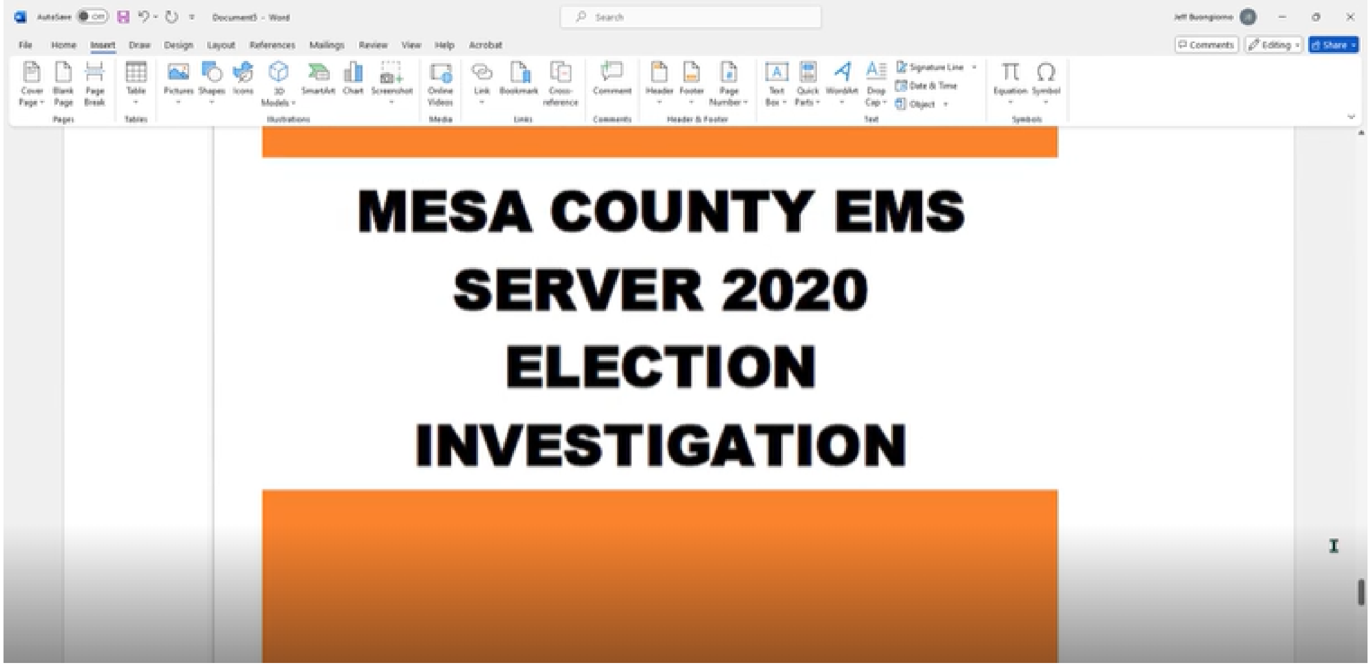
Find out ways that malware can get on your device.

Virus definitions are benign parts of a computer virus that the antivirus engine uses in order to detect the real virus. The names of the viruses are actually there in the screen shot, but someone that doesn’t have the proper knowledge/experience may not realize what they are looking at. I’m not saying he is lying to be malicious. I have no reason to believe it is anything other than an honest mistake at this time.

It is incredibly important that any claims are peer reviewed by people with the proper knowledge and experience to discern fact from fiction. We cannot afford the movement to secure our elections to be discredited, or anyone in our movement to be discredited.

Where did Jeff get this? Well, he got it from a previously-DEBUNKED ‘Mesa County EMS Server 2020 Election Investigation’ done by Josh Merritt. The report that Josh produced was full of assumptions and incorrect conclusions. That was communicated to Josh, but he refused to listen. I’m not sure why anyone with integrity would push something that is factually false and misleading unless they are attempting to discredit and distract people. I’m sorry to see that his work is still causing damage to people’s reputation.

Here is a screen shot from the video in the article, showing the same document that I already debunked in March 2023:



MESA COUNTY EMS SERVER 2020 ELECTION INVESTIGATION

DO NOT SHARE THE LINK BELOW BECAUSE IT IS NOT TRUE. I am including it only for reference.

https://miamiindependent.com/boungiorno-palm-beach-county-election-infrastructure-breach-proven/
I have already let Miami Independent know this and suggested they take it down. They have put a notice on their page with a reference to this page.

For those that say “I trust the computers”

October 20, 2024
Why? Why do trust them? Do you trust them because you are a programmer and have personally looked through the tens of thousands to millions of lines of code and examined exactly what it does, then compiled that to ensure that the resulting file

hashes match those that are running on each of the voting machines you are using? Or do you just blindly trust them because someone you perceive as smarter and more qualified than you are told you to trust them? And that person that told you to trust them…are THEY a programmer that personally looked through the tens of thousands to millions of lines of code and examined exactly what it does, then compiled that to ensure that the resulting file hashes match those that are running on each of the voting machines you are using? Or are they just blindly trusting the person above them? And is the person above them just blindly trusting the certification lab that never looked at the source code? Did the certification lab just blindly trust the testing lab that didn't even examine the logic of the source code, and has even missed blatant security requirements that the software has failed, yet they passed it in their testing despite that?

Or is your answer "I trust it because I tested it and it came out with the right answer!"? Do you realize that any programmer can program their software to detect it is being tested and behave perfectly in that instance, then do whatever they want it to do at any other time? No? Really? Did you hear about the Volkswagen Scandal in 2015?

> *Source: https://www.caranddriver.com/news/a15339250/everything-you-need-to-know-about-the-vw-diesel-emissions-scandal/*
>
> ***What happened?***
>
> *Volkswagen installed emissions software on more than a half-million diesel cars in the U.S.—and roughly 10.5 million more worldwide—that allows them to sense the unique parameters of an emissions drive cycle set by the Environmental Protection Agency. According to the EPA and the California Air Resources*

> *Board, which were **tipped off by researchers in 2014**, these so-called "defeat devices" detect steering, throttle, and other inputs used in the test to switch between two distinct operating modes.*
>
> *In the test mode, the cars are fully compliant with all federal emissions levels. But when driving normally, the computer switches to a **separate mode**—significantly changing the fuel pressure, injection timing, exhaust-gas recirculation, and, in models with AdBlue, the amount of urea fluid sprayed into the exhaust. While this mode likely delivers higher mileage and power, it also permits heavier nitrogen-oxide emissions (NOx)—a smog-forming pollutant linked to lung cancer—up to 40 times higher than the federal limit. That doesn't mean every TDI is pumping 40 times as much NOx as it should. Some cars may emit just a few times over the limit, depending on driving style and load.*

Do you realize that if a car manufacturer can do it, a voting system manufacturer can also do the same thing? The car manufacturer benefited by selling millions of vehicles. A voting system manufacturer can benefit by controlling all the money and power in every country that uses their systems. Which do you think is a higher value target for bad actors? And that 'voting system' can just as easily be a 'voter registration database', an 'electronic poll book', and an 'election night reporting tool'.

At some point, the citizens of America need to pull their heads out of their asses and realize that they will never have freedom again if they don't IMMEDIATELY stop using computers for their voter registration lists, poll books, tabulation, totals aggregation, and election night reporting. If they realize this is the NATIONAL EMERGENCY that it IS, 2024 may very well be the end of the United States of America experiment.

If we do lose our beloved Country, I would certainly not want be any of those individuals that decided to keep their heads up their asses and take part in indirectly destroying this country that over 300M people call their home. I can't imagine those 300M+ people are going to be too happy with them.

So the time to decide is right now. Will you keep your head up your ass? Or are you willing to pull it out and reconsider your actions? Do you want to be on the list of people that destroyed the United States of America, or do you want to be on the list that saved the United States of America? Tick, tock…

If you DO decide to make the sane decision, the next thing you need to read is https://handcountroadshow.org/the-early-voting-scam/

After that, watch my most recent presentation by clicking here. Don't forget to click on the slides just below the recording so you have those to flip through too!

CrowdStrike Falcon Worldwide Outage

October 20, 2024

What it is

CrowdStrike is a network security company. A Falcon Sensor is part of their Cloud-based endpoint protection platform. Think of

Endpoint Protection as a firewall on each device that is part of a network. The ‘cloud’ part of it is similar to a conductor in a orchestra, with the endpoints being those playing the instruments, and the instruments are the individual computers/servers.

What caused it

CrowdStrike sent out an update to their software that conflicted with Microsoft Windows, which caused a BSOD (blue screen of death – a ‘crash’ of the software). Following the software crash, the computer gets stuck during reboot and won’t load the operating system, leaving it dead in the water.

How this affects our elections

The idiots that implemented our cloud-based voter registration and poll-book systems have created a HUGE abuse vector in our election ecosystem and I’d be shocked if those election systems weren’t also affected by this. And there is nothing that can prevent their being another accidental (or intentional) abuse! Have you considered that this may just be cover for an election hack just prior to/during an election? It would be perfect cover.

Maricopa County Voting Locations Impacted – and they aren’t alone!

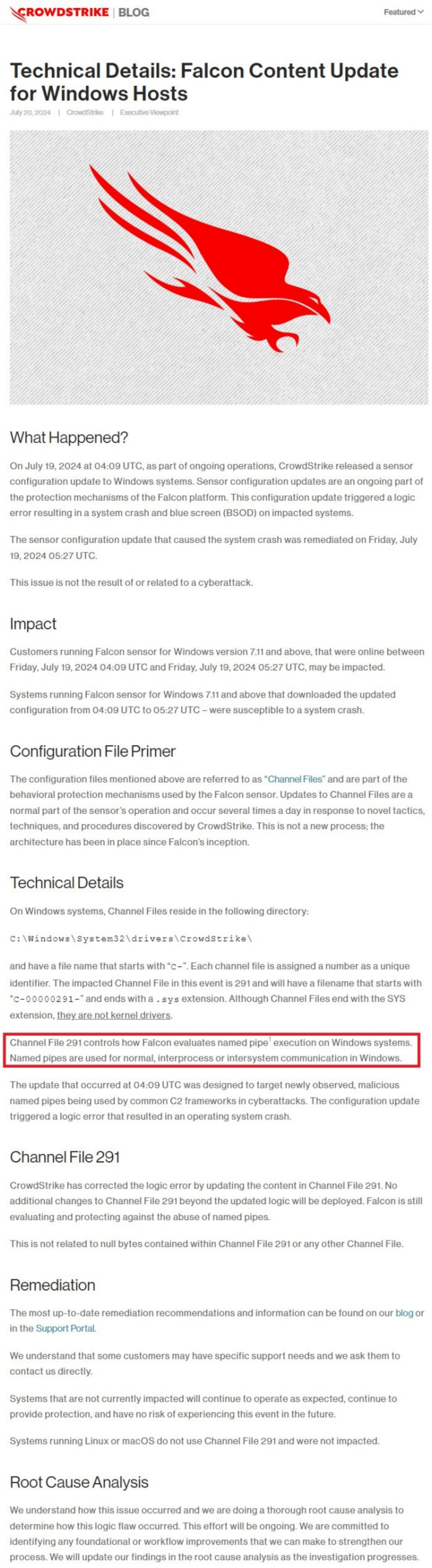
Outages locally have included Maricopa County voting locations, multiple Valley police dispatch centers, several airlines at Phoenix Sky Harbor International Airport and all flights to and from Mesa Gateway Airport.

Gov. Katie Hobbs said on social media that her team is “closely monitoring all services that have been impacted and is working to ensure that we continue delivering the critical services that Arizonans rely on.”

> *A worldwide IT outage has impacted some State of Arizona systems and agency operations.*
>
> *My team is closely monitoring all services that have been impacted and is working to ensure that we continue delivering the critical services that Arizonans rely on.*
>
> *As we work to address…*
>
> *— Governor Katie Hobbs (@GovernorHobbs) [July 19, 2024]*

> *[pic.twitter.com/qFLxuYvDHV]*
>
> *— Maricopa County Elections (@MaricopaVote) [July 19, 2024]*

But wait…There’s more! New update from CrowdStrike:



CROWDSTRIKE | BLOG

Featured

Technical Details: Falcon Content Update for Windows Hosts

July 20, 2024 | CrowdStrike | Executive Viewpoint

What Happened?

On July 19, 2024 at 04:09 UTC, as part of ongoing operations, CrowdStrike released a sensor configuration update to Windows systems. Sensor configuration updates are an ongoing part of the protection mechanisms of the Falcon platform. This configuration update triggered a logic error resulting in a system crash and blue screen (BSOD) on impacted systems.

The sensor configuration update that caused the system crash was remediated on Friday, July 19, 2024 05:27 UTC.

This issue is not the result of or related to a cyberattack.

Impact

Customers running Falcon sensor for Windows version 7.11 and above, that were online between Friday, July 19, 2024 04:09 UTC and Friday, July 19, 2024 05:27 UTC, may be impacted.

Systems running Falcon sensor for Windows 7.11 and above that downloaded the updated configuration from 04:09 UTC to 05:27 UTC – were susceptible to a system crash.

Configuration File Primer

The configuration files mentioned above are referred to as "Channel Files" and are part of the behavioral protection mechanisms used by the Falcon sensor. Updates to Channel Files are a normal part of the sensor's operation and occur several times a day in response to novel tactics, techniques, and procedures discovered by CrowdStrike. This is not a new process; the architecture has been in place since Falcon's inception.

Technical Details

On Windows systems, Channel Files reside in the following directory:

```
C:\Windows\System32\drivers\CrowdStrike\
```

and have a file name that starts with "`C-`". Each channel file is assigned a number as a unique identifier. The impacted Channel File in this event is 291 and will have a filename that starts with "`C-00000291-`" and ends with a `.sys` extension. Although Channel Files end with the SYS extension, they are not kernel drivers.

Channel File 291 controls how Falcon evaluates named pipe[1] execution on Windows systems. Named pipes are used for normal, interprocess or intersystem communication in Windows.

The update that occurred at 04:09 UTC was designed to target newly observed, malicious named pipes being used by common C2 frameworks in cyberattacks. The configuration update triggered a logic error that resulted in an operating system crash.

Channel File 291

CrowdStrike has corrected the logic error by updating the content in Channel File 291. No additional changes to Channel File 291 beyond the updated logic will be deployed. Falcon is still evaluating and protecting against the abuse of named pipes.

This is not related to null bytes contained within Channel File 291 or any other Channel File.

Remediation

The most up-to-date remediation recommendations and information can be found on our blog or in the Support Portal.

We understand that some customers may have specific support needs and we ask them to contact us directly.

Systems that are not currently impacted will continue to operate as expected, continue to provide protection, and have no risk of experiencing this event in the future.

Systems running Linux or macOS do not use Channel File 291 and were not impacted.

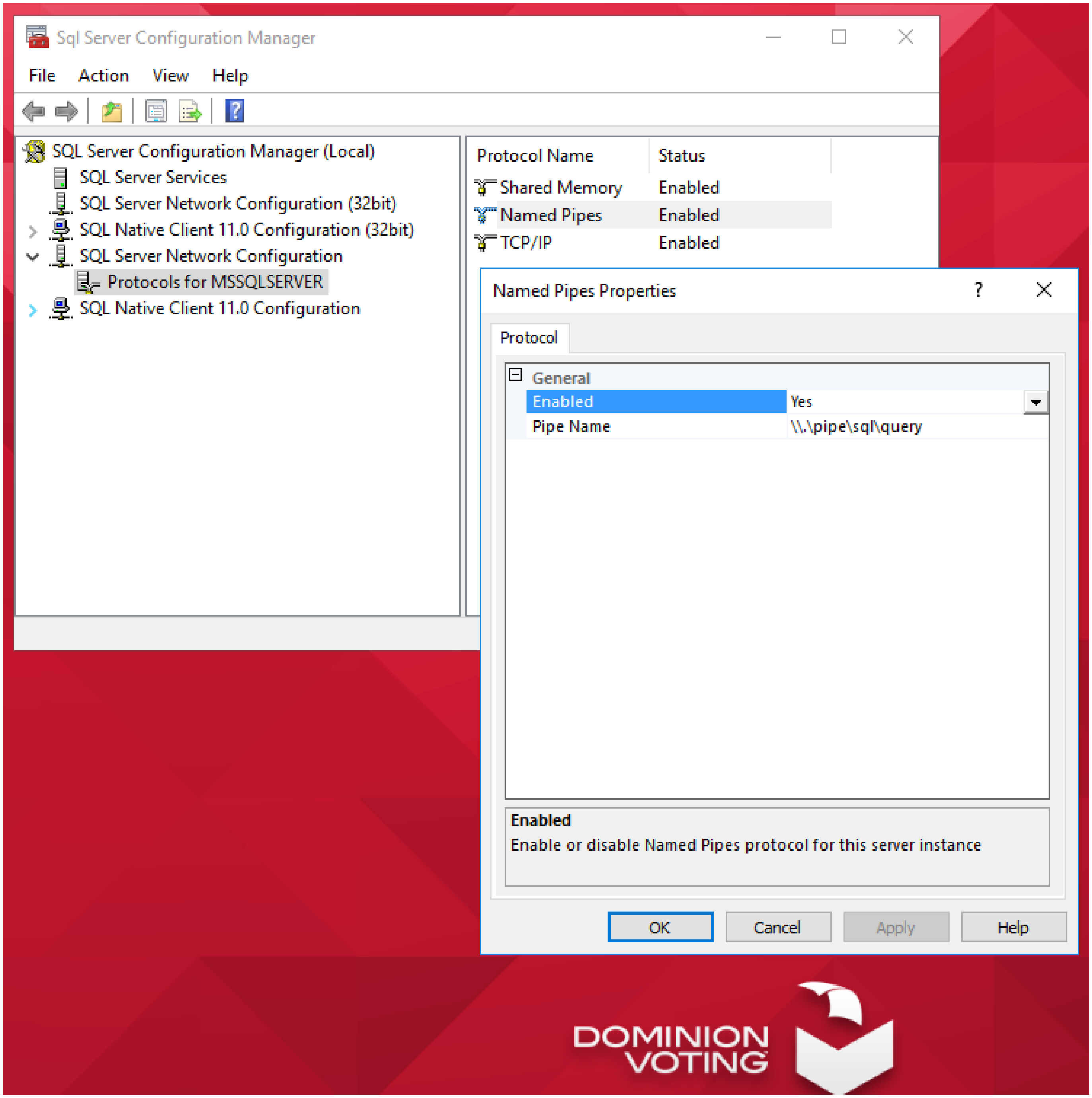
Root Cause Analysis

We understand how this issue occurred and we are doing a thorough root cause analysis to determine how this logic flaw occurred. This effort will be ongoing. We are committed to identifying any foundational or workflow improvements that we can make to strengthen our process. We will update our findings in the root cause analysis as the investigation progresses.

(Source: https://www.crowdstrike.com/blog/falcon-update-for-windows-hosts-technical-details/)

Speaking of Elections…let’s not leave out Dominion just yet…

The idiots at Dominion Voting Systems also leave their election management server database server open to Named Pipes (notice the red box above!):



SQL Server Configuration Manager (Local)
- SQL Server Services
- SQL Server Network Configuration (32bit)
- SQL Native Client 11.0 Configuration (32bit)
- SQL Server Network Configuration
  - Protocols for MSSQLSERVER
- SQL Native Client 11.0 Configuration

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Enabled
TCP/IP	Enabled

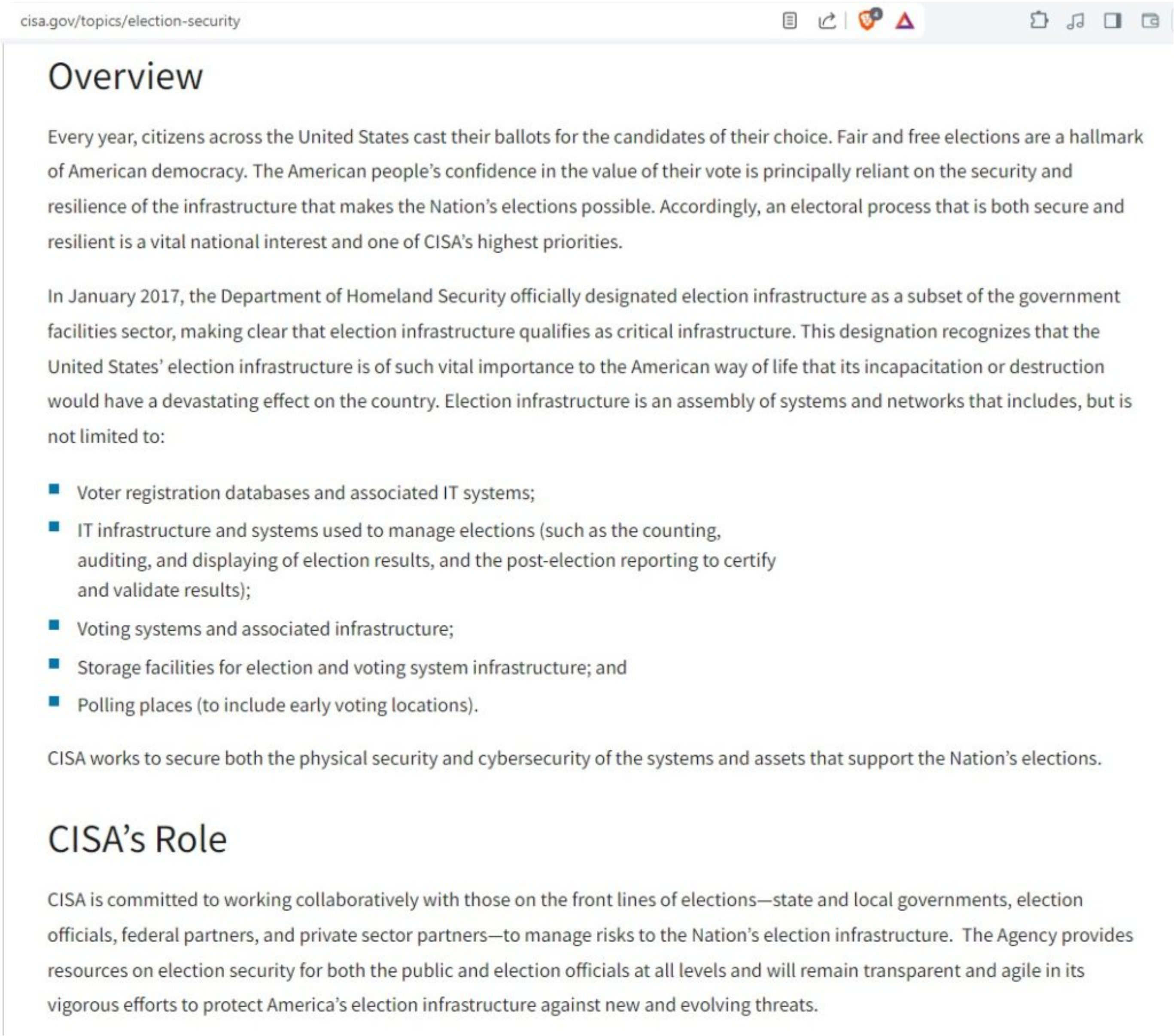
General

Enabled	Yes
Pipe Name	\\.\pipe\sql\query

Enabled
Enable or disable Named Pipes protocol for this server instance

Is this yet another example of their incredible incompetence? Or is it instead, intentional ‘incompetence’? And we trust them with WHAT? *(And yes of course, Named-Pipes is not the only problem showing there.)*

According to CISA:



Overview

Every year, citizens across the United States cast their ballots for the candidates of their choice. Fair and free elections are a hallmark of American democracy. The American people's confidence in the value of their vote is principally reliant on the security and resilience of the infrastructure that makes the Nation's elections possible. Accordingly, an electoral process that is both secure and resilient is a vital national interest and one of CISA's highest priorities.

In January 2017, the Department of Homeland Security officially designated election infrastructure as a subset of the government facilities sector, making clear that election infrastructure qualifies as critical infrastructure. This designation recognizes that the United States' election infrastructure is of such vital importance to the American way of life that its incapacitation or destruction would have a devastating effect on the country. Election infrastructure is an assembly of systems and networks that includes, but is not limited to:

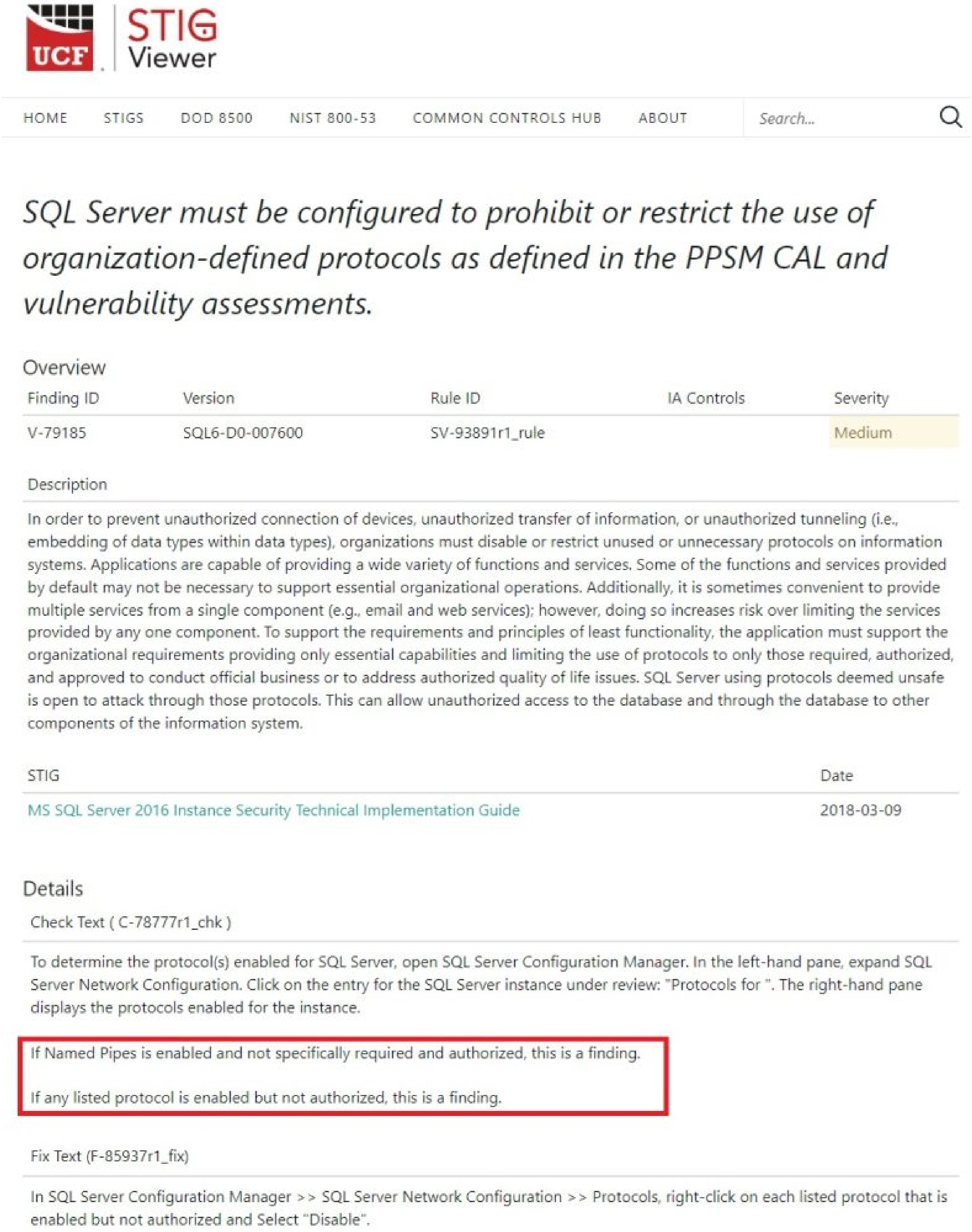
- Voter registration databases and associated IT systems;
- IT infrastructure and systems used to manage elections (such as the counting, auditing, and displaying of election results, and the post-election reporting to certify and validate results);
- Voting systems and associated infrastructure;
- Storage facilities for election and voting system infrastructure; and
- Polling places (to include early voting locations).

CISA works to secure both the physical security and cybersecurity of the systems and assets that support the Nation's elections.

CISA's Role

CISA is committed to working collaboratively with those on the front lines of elections—state and local governments, election officials, federal partners, and private sector partners—to manage risks to the Nation's election infrastructure. The Agency provides resources on election security for both the public and election officials at all levels and will remain transparent and agile in its vigorous efforts to protect America's election infrastructure against new and evolving threats.

For this system deemed CRITICAL INFRASTRUCTURE, how convenient for Dominion to not even follow standard STIGs. Here's V-79185:



SQL Server must be configured to prohibit or restrict the use of organization-defined protocols as defined in the PPSM CAL and vulnerability assessments.

Overview

Finding ID	Version	Rule ID	IA Controls	Severity
V-79185	SQL6-D0-007600	SV-93891r1_rule		Medium

Description

In order to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary protocols on information systems. Applications are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., email and web services); however, doing so increases risk over limiting the services provided by any one component. To support the requirements and principles of least functionality, the application must support the organizational requirements providing only essential capabilities and limiting the use of protocols to only those required, authorized, and approved to conduct official business or to address authorized quality of life issues. SQL Server using protocols deemed unsafe is open to attack through those protocols. This can allow unauthorized access to the database and through the database to other components of the information system.

STIG	Date
MS SQL Server 2016 Instance Security Technical Implementation Guide	2018-03-09

Details

Check Text (C-78777r1_chk)

To determine the protocol(s) enabled for SQL Server, open SQL Server Configuration Manager. In the left-hand pane, expand SQL Server Network Configuration. Click on the entry for the SQL Server instance under review: "Protocols for ". The right-hand pane displays the protocols enabled for the instance.

If Named Pipes is enabled and not specifically required and authorized, this is a finding.

If any listed protocol is enabled but not authorized, this is a finding.

Fix Text (F-85937r1_fix)

In SQL Server Configuration Manager >> SQL Server Network Configuration >> Protocols, right-click on each listed protocol that is enabled but not authorized and Select "Disable".

Did Dominion do anything else wrong?

Lol…oh boy. This is **barely even the tip of the iceberg**. But in Dominion's defense, it's not just Dominion that's the problem. Every company that electronically centralizes any aspect of our elections creates a superhighway of attack vectors leading into our Nation's entire foundation, our **Election System**. The shear incompetence and inability to protect any system in the industry from abuse is the elephant in the room. When you have a bad actor inside the company, you're done. For instance, look at this **very accurate** quote from an atsec source code review of Dominion that is applicable to ANY system:

> *"Backdoors are extremely hard to find because a seasoned programmer can obfuscate code to look benign. The atsec team would like to stress that, when facing a competent and sufficiently motivated maliciousdeveloper, it is extremely difficult to prove that all backdoors in a system have been identified. The famous Turing award lecture by Ken Thompson in 1984 entitled Reflections on Trusting Trust [TRUST] demonstrated how fundamentally easy it is to undermine all security mechanisms when the developers cannot be trusted. This voting system is no exception."*

Yes, I know CISA claims to secure our systems. Unfortunately, the same types of incompetence in these vendors exist in CISA as well. Not to mention, they are also lying right to our face about many things.

So what is the connection between

CrowdStrike and Dominion?

Well…it is interesting that CrowdStrike is intercepting Named-Pipes and Dominion also left their database connected to Named-Pipes. Coincidence? Possibly. Convenient as yet another possible attack vector? Absolutely!

So what are you trying to say?

Simply put, the people wielding this technology are wholly irresponsible (at best). At worst, what if there are **bad actors** at Dominion? Even worse (if that's even possible), what if there are **bad actors** at CrowdStrike? What do those **bad actors** now have access to? How many millions of computers around the world does CrowdStrike have LOW LEVEL control of? (8.5 Million at the last count according to David Weston, Microsoft VP, Enterprise and OS Security in a blog post Saturday). Who owns CrowdStrike? Who works there? THINK ABOUT ALL THAT…

Our election officials are sitting ducks and in no way knowledgeable enough to secure (nonetheless even understand) this threat landscape. How can any election official claim their system is secure when they don't know it to be such, and they are merely blindly believing what someone they trust tells them? What happens when those that they trust are LYING TO THEM? Our election officials need to accept the reality that is in front of their faces: They cannot control or secure that which they cannot fully see and do not fully understand. The solution is simple…boot all the electronic systems out of our elections and go back to a simple system with a much smaller and controllable threat model, then use technology to add transparency instead of obscurity.

How to fix this current CrowdStrike issue:

The affected file in the update is a particular ‘driver’ that was updated. A ‘driver’ is a program that runs on the computer that performs a task. This driver is the Falcon driver. To repair it, the affected ‘driver’ must be removed in order to allow the operating system to boot up, then the new fixed version of the driver must be installed. The huge complication here is that the driver must be removed MANUALLY. A further complication is for servers that have encrypted hard drives because extra steps must be performed to decrypt the hard drive in order for the repair to be implemented. For companies that didn’t follow best-practices on their encryption passwords, their systems will be permanently locked out and unrecoverable.

Details on repair

The morning of 2024-07-19, a content update was sent to some CrowdStrike Falcon clients on Windows devices which resulted in “Blue Screen” errors for those devices. If you have a Windows device stuck on a blue screen at boot, this issue is almost certainly the cause.

The fix for this issue requires booting the Windows device into Safe Mode or Recovery Mode and deleting a file. Instructions for doing this are below. This post and these instructions may be updated as the situation develops.

FIXING THE WINDOWS DEVICE PROBLEM

Direct link to CrowdStrike instructions: https://www.crowdstrike.com/blog/statement-on-falcon-content-update-for-windows-hosts/

If you are affected by this, we happen to know someone VERY good with solving these types of issues! Contact Mark Cook here.

Workaround Steps for individual hosts:

- Reboot the host to give it an opportunity to download the reverted channel file. If the host crashes again, then:
    - Boot Windows into Safe Mode or the Windows Recovery Environment
        - NOTE: Putting the host on a wired network (as opposed to WiFi) and using Safe Mode with Networking can help remediation. ***(** NOTE: This is the same type of backdoor that many of our electronic voting systems including electronic poll books have)***
    - Navigate to the %WINDIR%\System32\drivers\CrowdStrike directory
    - Locate the file matching “C-00000291*.sys”, and delete it.
    - Boot the host normally.

Workaround Steps for public cloud or similar environment including virtual:

Option 1:

- □□□□□□□Detach the operating system disk volume from the impacted virtual server
- Create a snapshot or backup of the disk volume before proceeding further as a precaution against unintended

changes ***(** NOTE: This type of backup is essentially same thing that [Clerk Tina Peters] had done to her election system before the SoS and Dominion showed up to remove the QR code feature, that they later attacked her for!)***

- Attach/mount the volume to to a new virtual server
- Navigate to the %WINDIR%\System32\drivers\CrowdStrike directory
- Locate the file matching “C-00000291*.sys”, and delete it.
- Detach the volume from the new virtual server
- Reattach the fixed volume to the impacted virtual server

Option 2:

- □□□□□□□Roll back to a snapshot before 0409 UTC.

AWS-specific documentation:

- To attach an EBS volume to an instance
- Detach an Amazon EBS volume from an instance
  - Note: Use a different OS version for the VirtualMachine used as the recovery VM to the Virtual Machine you are trying to recover.

Azure environments:

- Please see this Microsoft article

User Access to Recovery Key in the

Workspace ONE Portal

When this setting is enabled, users can retrieve the BitLocker Recovery Key from the Workspace ONE portal without the need to contact the HelpDesk for assistance. To turn on the recovery key in the Workspace ONE portal, follow the next steps. Please see this Omnissa article for more information.

Bitlocker recovery-related KBs:

- BitLocker recovery in Microsoft Azure (pdf) or login to view in support portal.
- BitLocker recovery in Microsoft environments using SCCM (pdf) or login to view in support portal.
- BitLocker recovery in Microsoft environments using Active Directory and GPOs (pdf) or login to view in support portal.
- BitLocker recovery in Microsoft environments using Ivanti Endpoint Manager (pdf) or login to view in support portal.

#RightWayVoting

October 20, 2024

EARLY vs ELECTION DAY voting

Best to Worst	When	Pros	Cons

Safest	Election Day	You may find out if your voting identity was previously stolen. Your ballot can’t get intercepted along the way to the polling location. Citizen Unity and Social Restoration, standing side-by-side your fellow citizens. Election Day Exit Polling is much easier to implement in order to compare the election-day results with the exit-polling results.	None
Safer	**Close to** Election Day	Convenience for those that are unable to vote on Election Day without showing hand early	Something could happen to your ballot before it makes it to tabulation day. Election results can be estimated before polls close, allowing last-minute **FEEDBACK LOOP** manipulation. Your envelope could be thrown out by someone and your ballot never counted.

Unsafe	Early	None	Something could happen to your ballot before it makes it to tabulation day. Election results can be estimated before polls close, allowing easy **FEEDBACK LOOP** manipulation. Your envelope could be thrown out by someone and your ballot never counted.

MAIL BALLOTS

Mass Mail Ballot State

- **Vote In-Person** – bring your unopened mail ballot with you
    - Pros
        - If you are told that you already voted by mail, you have real evidence to expose/address it and file an identity theft complaint with Sheriff prior to election day
        - You eliminate time/space between events, and therefore reduce the election abuse surface
    - Cons
        - None

- **Vote by Mail**
    - Pros
        - You can be lazy
    - Cons
        - You increase the election abuse surface
        - Bad actors know when you return your ballot using the mail ballot tracking system to feed their election model
        - Your identity is directly connected to your ballot (violates voter secrecy) via the barcode keep in mind that not all states use a secrecy sleeve, for instance, Colorado.
        - Your party affiliations is often shown on the envelope (sometimes covertly)
        - There is no guarantee that your ballot won’t be swapped out for another
        - There is no guarantee that your ballot will ever make it to be counted

Non-Mass Mail Ballot State

- **Vote In Person**
    - **NOT Request Mail Ballot**
        - Pros
            - You don’t give them data to substantiate use of mail ballots
            - Less mail ballots in circulation results in smaller attack surface
            - If a mail ballot is shown as having been

sent, you can expose/address it and file an identity theft complaint with Sheriff prior to election day

- If one or more mail ballot shows up anyway, you can expose/address it prior to election day (and bring with you on election day to PROVE you didn’t vote with it)
- If a mail ballot is shown as being received, you can expose/address it and file an identity theft complaint with Sheriff prior to election day
- County Mail in tracking database
    - If a mail ballot is recorded as having been sent that shouldn’t have been, election officials can see it and deal with it prior to election day
    - If a mail ballot is recorded as being received that shouldn’t have been sent, election officials can see it and deal with it prior to election day
    - When arriving on Election Day, if you are told you already voted and you bring your sealed mail ballot in your hand, you expose/address it and file an identity theft complaint with Sheriff

- Post-election voted lists
    - If a mail ballot is recorded as having been sent, you can expose it

            - If a mail ballot is recorded as being received, you can expose it

        - Exposed voter identity theft is great evidence to support not being able to certify an election

    - Cons
        - None

- **Opt-Out of Mail Ballot** (where possible)
    - Pros
        - You demonstrate that citizens don’t want mail ballots
        - Less mail ballots in circulation results in smaller attack surface
        - If one or more mail ballot shows up anyway, you can expose/address it prior to election day (and bring with you on election day to PROVE you didn’t vote with it)
        - Public-facing Mail in ballot tracking system (pre-election-day)
        - If a mail ballot is shown as having been sent, you can expose/address it and file an identity theft complaint with Sheriff prior to election day
        - If a mail ballot is shown as being received, you can expose/address it and file an identity theft complaint with Sheriff prior to election day
        - County Mail in tracking database

- If a mail ballot is recorded as having been sent, election officials can see it and deal with it prior to election day
- If a mail ballot is recorded as being received, election officials can see it and deal with it prior to election day
- When arriving on Election Day, if you are told you already voted and you bring your sealed mail ballot in your hand, you expose/address it and file an identity theft complaint with Sheriff

- Post-election voted lists
  - If a mail ballot is recorded as having been sent, you can expose it
  - If a mail ballot is recorded as being received, you can expose it

- Exposed voter identity theft is great evidence to support not being able to certify an election
- You may get assigned a higher voting propensity which would make your vote less attractive to abuse

- Cons
  - None

- **Request Mail Ballot** but still Vote in Person
    - Pros
        - If you don’t receive your mail ballot you know it has been ‘lost’
    - Cons
        - **If you go in to vote in person, but you have requested a mail ballot, you may be forced to vote a provisional ballot instead, which may not be tabulated.**
        - If you don’t receive your mail ballot, you have put another phantom ballot into circulation
        - Ballots lose chain of custody as soon as they are sent out
        - You put more mail ballots in circulation increasing election attack surface
        - You provide evidence that can be used to justify the receipt of a mail ballot in your name
        - You provide feedback to bad actors that raise your voting propensity score used to decide which records to use for ballot injection
        - You put yourself at risk being able to vote on a non-mail ballot on election day, and your in-person vote could end up provisional
        - Election staff may force you to use your mail ballot (less chain of custody and far more abuse vectors) to vote in person instead of depositing your non-identifiable ballot in a ballot box.

- **Vote by Mail**
    - Pros
        - You can be lazy
    - Cons
        - You increase the election abuse surface
        - Bad actors know when you return your ballot using the mail ballot tracking system to feed their election model
        - Your identity is directly connected to your ballot (violates voter secrecy) via the barcode keep in mind that not all states use a secrecy sleeve, for instance, Colorado.
        - Your party affiliations is often shown on the envelope (sometimes covertly)
        - There is no guarantee that your ballot won’t be swapped out for another
        - There is no guarantee that your ballot will ever make it to be counted

DROP BOXES

- **Isolated** – Not at your County polling place
    - Pros
        - None
    - Cons
        - No chain of custody

        - There is no guarantee that your ballot won’t be swapped out for another
        - There is no guarantee that your ballot will ever make it to be counted

- **At County Polling Place**
    - Pros
        - More secure than isolated
        - Better chain of custody than isolated
    - Cons
        - Less chain of custody than traditional voting on paper
        - You increase the election abuse surface
        - Bad actors know when you return your ballot using the mail ballot tracking system to feed their election model
        - Your identity is directly connected to your ballot (violates voter secrecy) via the barcode keep in mind that not all states use a secrecy sleeve, for instance, Colorado.
        - Your party affiliations is often shown on the envelope (sometimes covertly)
        - There is no guarantee that your ballot won’t be swapped out for another
        - There is no guarantee that your ballot will ever make it to be counted

Comparative Analysis

To determine the safest method, I compare the methods based on exposure to known and unknown vulnerabilities and the feasibility of exploitation, assuming typical U.S. safeguards (paper trails, audits, verification) are in place but could have gaps.

- **Exposure to Known Vulnerabilities:**
    - **Mail-In (Early or Election Day):** Most exposed due to multiple touchpoints (voters, postal services, drop boxes, processing centers). Interception, theft, or forgery is possible. Errors, small-scale fraud, and large-scale fraud are possible.
    - **In-Person (Early or Election Day):** Less exposed, as ballots are cast and stored in controlled environments. Electronic systems risk hacking, but paper backups and proper chain of custody and audits can limit impact. Insider fraud is possible.

- **Exposure to Unknown Vulnerabilities:**
    - **Mail-In:** Higher risk due to complexity (e.g., postal systems, drop boxes, voter databases). Hypothetical attacks like AI-driven forgery or coordinated theft could exploit undiscovered flaws in distributed processes.
    - **In-Person (Electronic):** Moderate risk due to potential software or hardware flaws in voting machines. Complex code or supply chain attacks could introduce undetectable issues.
    - **In-Person (Paper):** Lowest risk, as simple paper ballots avoid technological vulnerabilities. Unknown risks are limited to physical tampering or novel

social engineering.

- **Ease of Exploitation:**
    - **Mail-In:** Small-scale exploitation (e.g., stealing a few ballots) is easier but unlikely to affect outcomes. Large-scale fraud can significantly impact elections.
    - **In-Person (Early):** Extended timeline increases opportunities for tampering or hacking, though proper audits can catch some issues. Insider fraud needs coordination.
    - **In-Person (Election Day):** Short timeline limits exploitation windows, especially for outsiders. Insider fraud is possible but heavily constrained by immediate counting and oversight. ***(Count Where Cast!)***

- **Safeguard Effectiveness:**
    - All methods benefit from audits, paper trails, and verification, but in-person voting simplifies chain-of-custody and reduces external touchpoints (e.g., postal services).
    - Election Day in-person voting minimizes storage time, reducing risks of tampering or loss compared to early voting.

Safest Voting Method

Election Day In-Person Voting with Paper Ballots is the safest method against potential vulnerabilities and exploitation, for these reasons:

- **Minimized Exposure:** The single-day process reduces the time window for attacks, limiting opportunities for both known (e.g., hacking, tampering) and unknown exploits compared to early voting or mail-in systems.
- **Simpler System:** Paper ballots avoid technological vulnerabilities (e.g., software bugs, hardware tampering) that electronic systems face, reducing unknown risks. Hand-counting ensures accuracy.
- **Controlled Environment:** Voting and counting occur in supervised polling stations, minimizing external touchpoints (e.g., postal services) and simplifying chain-of-custody compared to mail-in voting.
- **Auditability:** Paper ballots provide a verifiable record, making it easier to detect and correct errors or fraud compared to electronic-only or distributed mail-in systems.
- **Unknown Risk Mitigation:** By avoiding complex technology and extended timelines, this method limits exposure to hypothetical flaws in software, hardware, or distributed processes.

Caveats

- **Assumption of Safeguards:** This conclusion assumes basic safeguards like voter ID, secure polling stations, chain of custody records, and audits are in place. Without them, no method is safe.
- **Local Variations:** Security varies by jurisdiction. A poorly managed polling station may be less secure, but the impact of issues is typically contained.
- **Access Trade-Offs:** Election Day in-person voting may reduce accessibility for some (e.g., those with work conflicts), but the prioritizes safety for all voters over convenience of some.

- **Unknown Unknowns:** No method is immune to completely unforeseen exploits (e.g., a novel attack on voter psychology). Paper-based, in-person voting minimizes technological risks but not human or physical ones.

Rankings

1. **Election Day In-Person (Paper Ballots):** Safest due to simplicity, short timeline, and minimal technological risks.
2. **Early In-Person (Paper Ballots):** Slightly less safe due to longer storage time, increasing tampering risks.
3. **Election Day In-Person (Electronic with Paper Trail):** Based on blind trust and vulnerable to technological abuse and flaws.
4. **Early In-Person (Electronic with Paper Trail):** Even more exposure due to extended timeline.
5. **Election Day Mail-In:** Distributed process increases touchpoints, but shorter window limits some risks.
6. **Early Mail-In:** Most vulnerable due to multiple touchpoints, longer timeline, and reliance on external systems.

Conclusion

Election Day in-person voting with paper ballots is the safest method, as it minimizes known and unknown vulnerabilities by using a simple, controlled, and auditable process with a short timeline. While no method is invulnerable, this approach reduces exposure to technological, distributed, or prolonged risks, making exploitation harder for both known and hypothetical attacks.

*** If you have any input on the above, PLEASE feel free to contact us directly.**

Mass Psychosis – Killing of the Mind

October 20, 2024

BOONE CUTLER | Surviving the Psyop: Military Intelligence Strategies for the Everyday American to Survive 2024

October 20, 2024

Take me to the books!

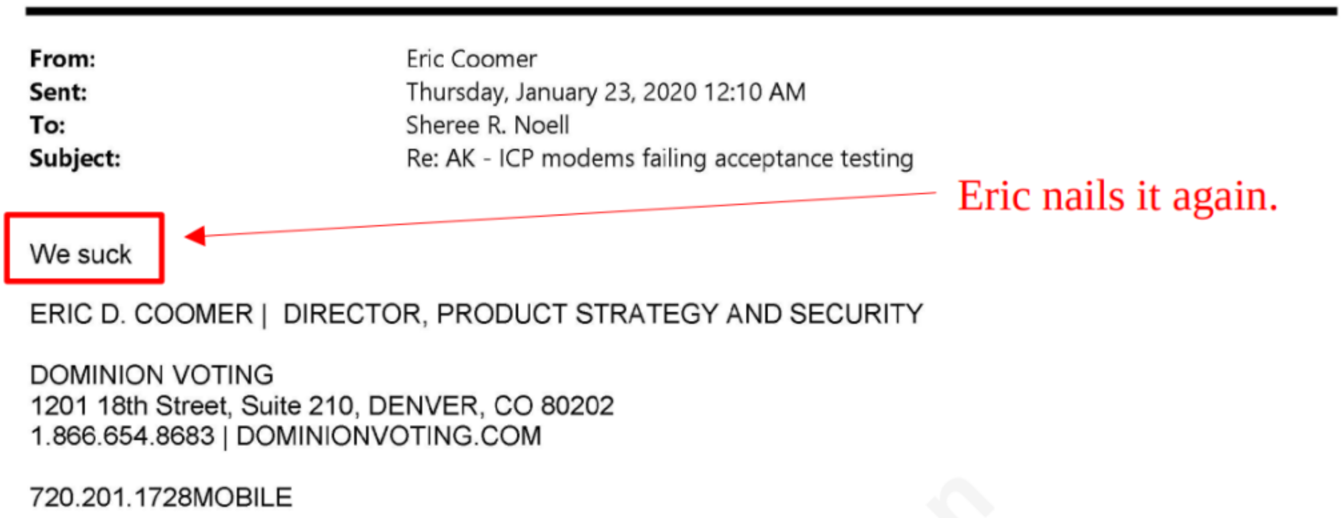
Dominion Serv-U Cover-Up

October 20, 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.



From: Eric Coomer
Sent: Thursday, January 23, 2020 12:10 AM
To: Sheree R. Noell
Subject: Re: AK - ICP modems failing acceptance testing

We suck

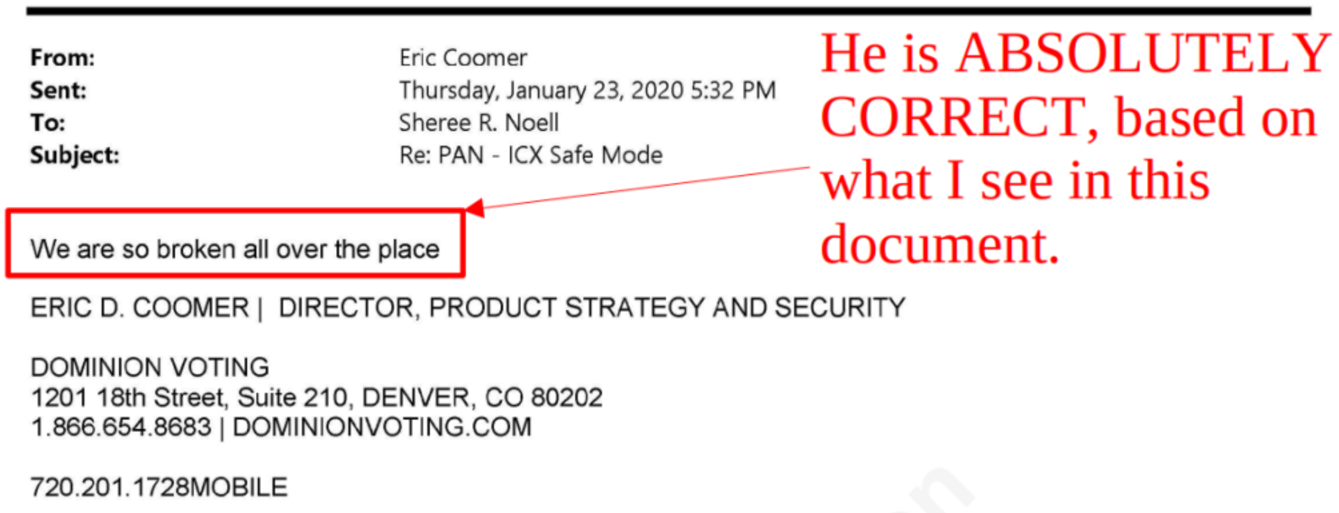
ERIC D. COOMER | DIRECTOR, PRODUCT STRATEGY AND SECURITY

DOMINION VOTING
1201 18th Street, Suite 210, DENVER, CO 80202
1.866.654.8683 | DOMINIONVOTING.COM

720.201.1728MOBILE

Eric nails it again.

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



From: Eric Coomer
Sent: Thursday, January 23, 2020 5:32 PM
To: Sheree R. Noell
Subject: Re: PAN - ICX Safe Mode

We are so broken all over the place

ERIC D. COOMER | DIRECTOR, PRODUCT STRATEGY AND SECURITY

DOMINION VOTING
1201 18th Street, Suite 210, DENVER, CO 80202
1.866.654.8683 | DOMINIONVOTING.COM

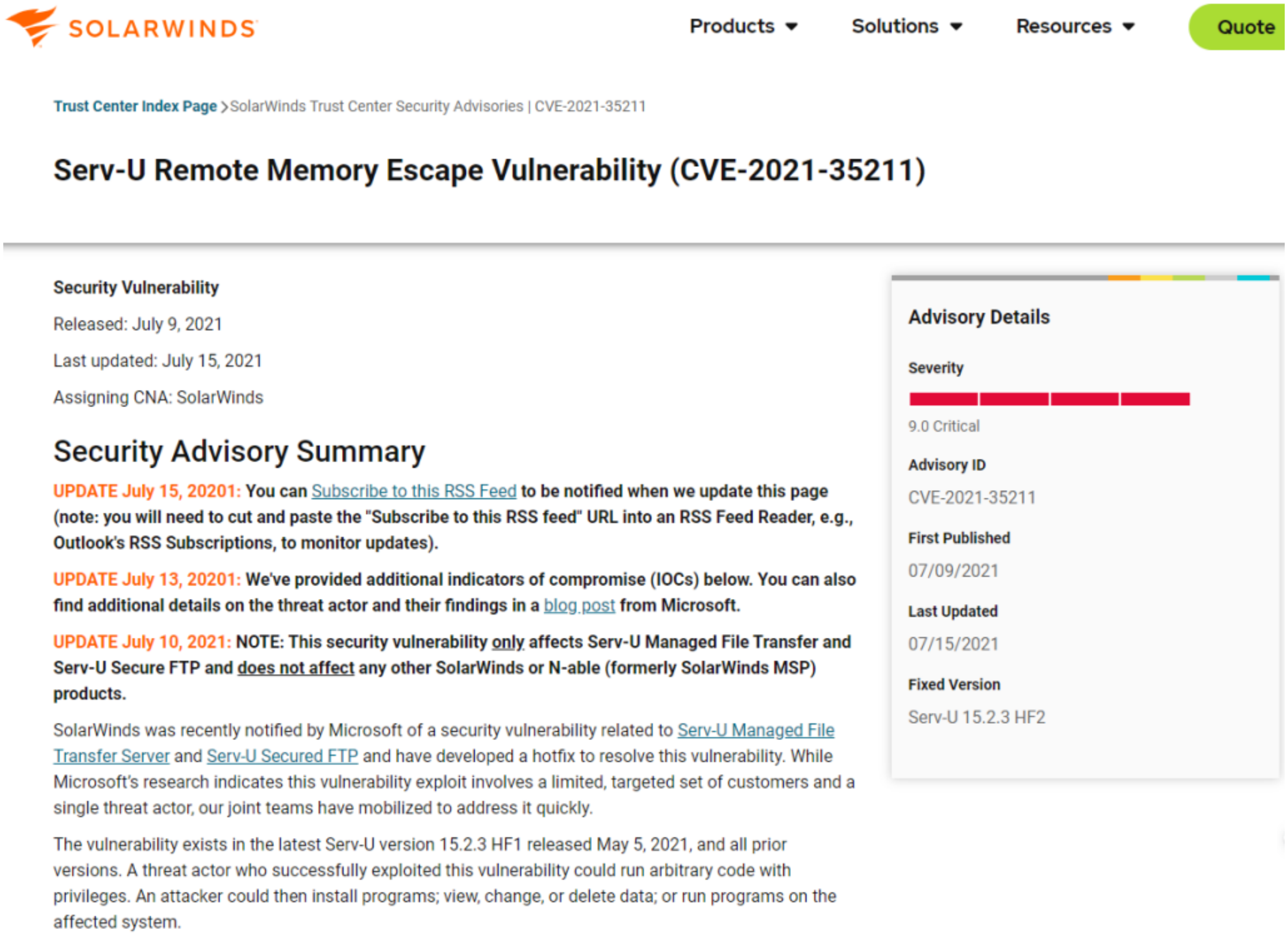
720.201.1728MOBILE

He is ABSOLUTELY CORRECT, based on what I see in this document.

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)



Trust Center Index Page > SolarWinds Trust Center Security Advisories | CVE-2021-35211

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

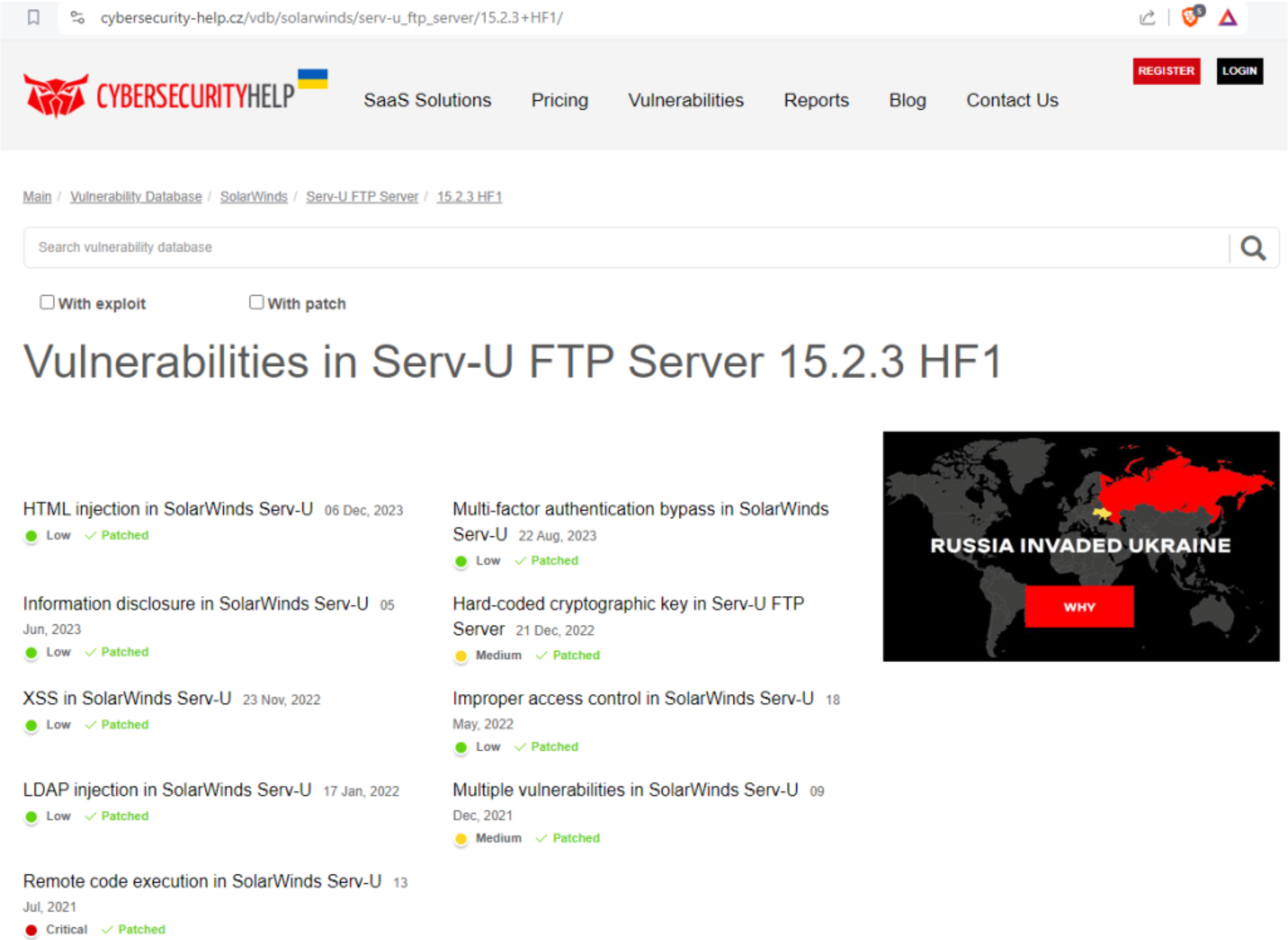
07/09/2021

Last Updated

07/15/2021

Fixed Version

Serv-U 15.2.3 HF2


cybersecurity-help.cz/vdb/solarwinds/serv-u_ftp_server/15.2.3+HF1/
CYBERSECURITYHELP
SaaS Solutions
Pricing
Vulnerabilities
Reports
Blog
Contact Us
REGISTER
LOGIN
Main / Vulnerability Database / SolarWinds / Serv-U FTP Server / 15.2.3 HF1
Search vulnerability database
☐ With exploit
☐ With patch
RUSSIA INVADED UKRAINE
WHY

Vulnerabilities in Serv-U FTP Server 15.2.3 HF1

HTML injection in SolarWinds Serv-U 06 Dec, 2023
● Low ✓ Patched

Information disclosure in SolarWinds Serv-U 05 Jun, 2023
● Low ✓ Patched

XSS in SolarWinds Serv-U 23 Nov, 2022
● Low ✓ Patched

LDAP injection in SolarWinds Serv-U 17 Jan, 2022
● Low ✓ Patched

Remote code execution in SolarWinds Serv-U 13 Jul, 2021
● Critical ✓ Patched

Multi-factor authentication bypass in SolarWinds Serv-U 22 Aug, 2023
● Low ✓ Patched

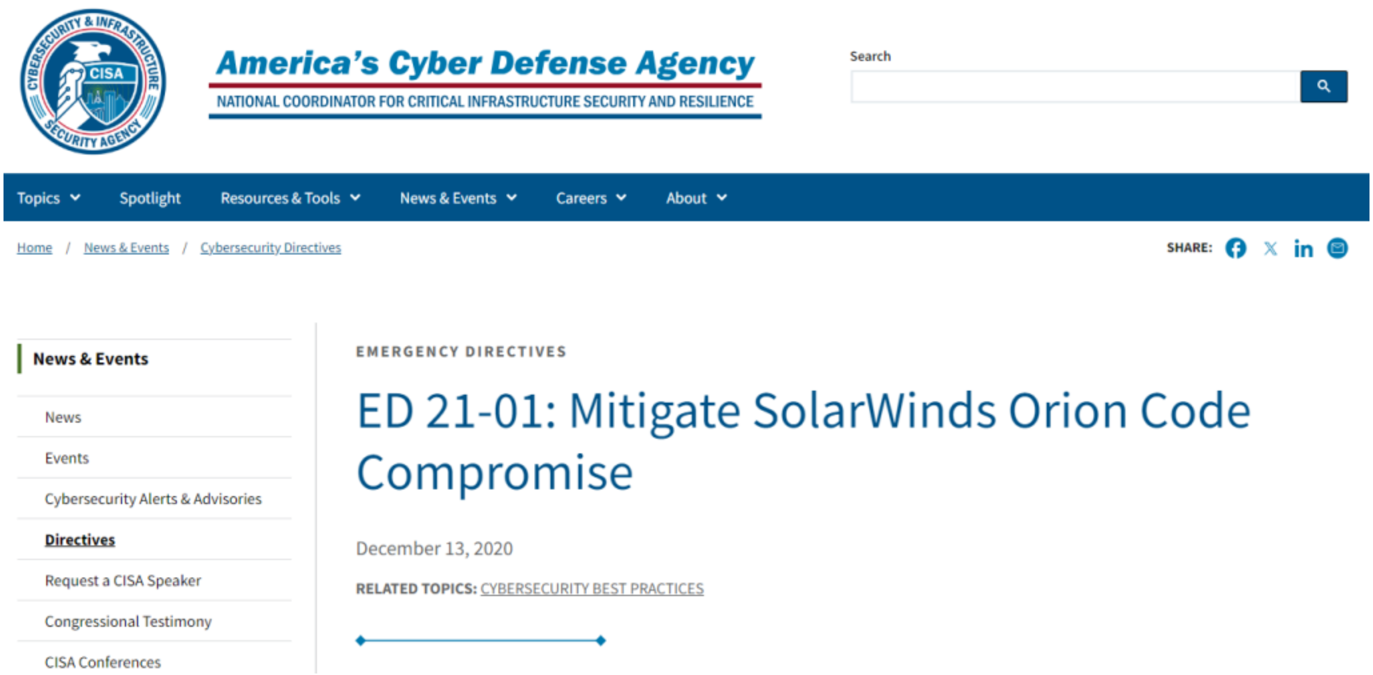
Hard-coded cryptographic key in Serv-U FTP Server 21 Dec, 2022
● Medium ✓ Patched

Improper access control in SolarWinds Serv-U 18 May, 2022
● Low ✓ Patched

Multiple vulnerabilities in SolarWinds Serv-U 09 Dec, 2021
● Medium ✓ Patched

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

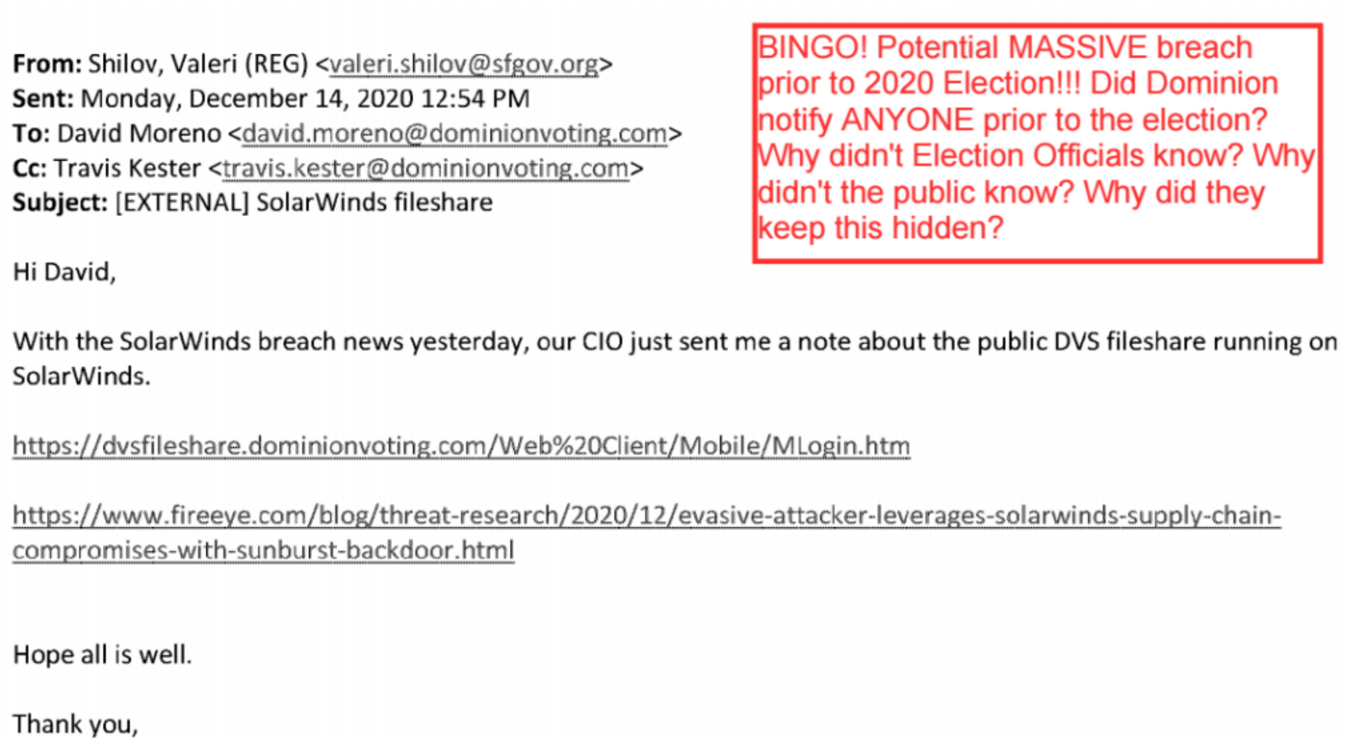
EMERGENCY DIRECTIVES

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

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

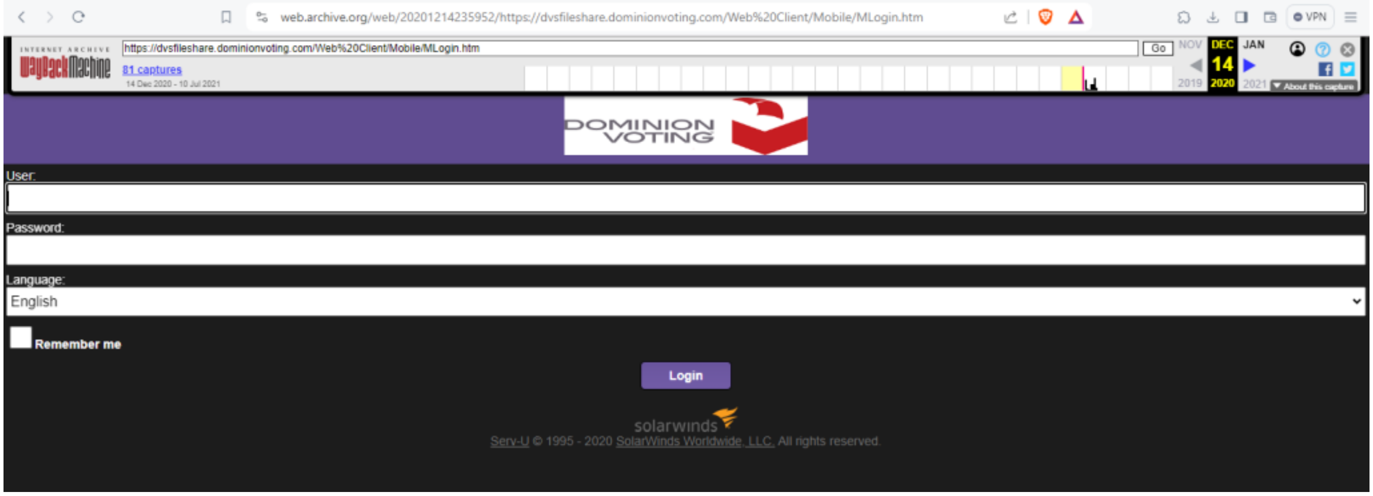
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Hope all is well.

Thank you,

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?

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



web.archive.org/web/20201214235952/https://dvsfileshare.dominionvoting.com/Web%20Client/Mobile/MLogin.htm

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

81 captures

14 Dec 2020 - 10 Jul 2021

User:

Password:

Language: English

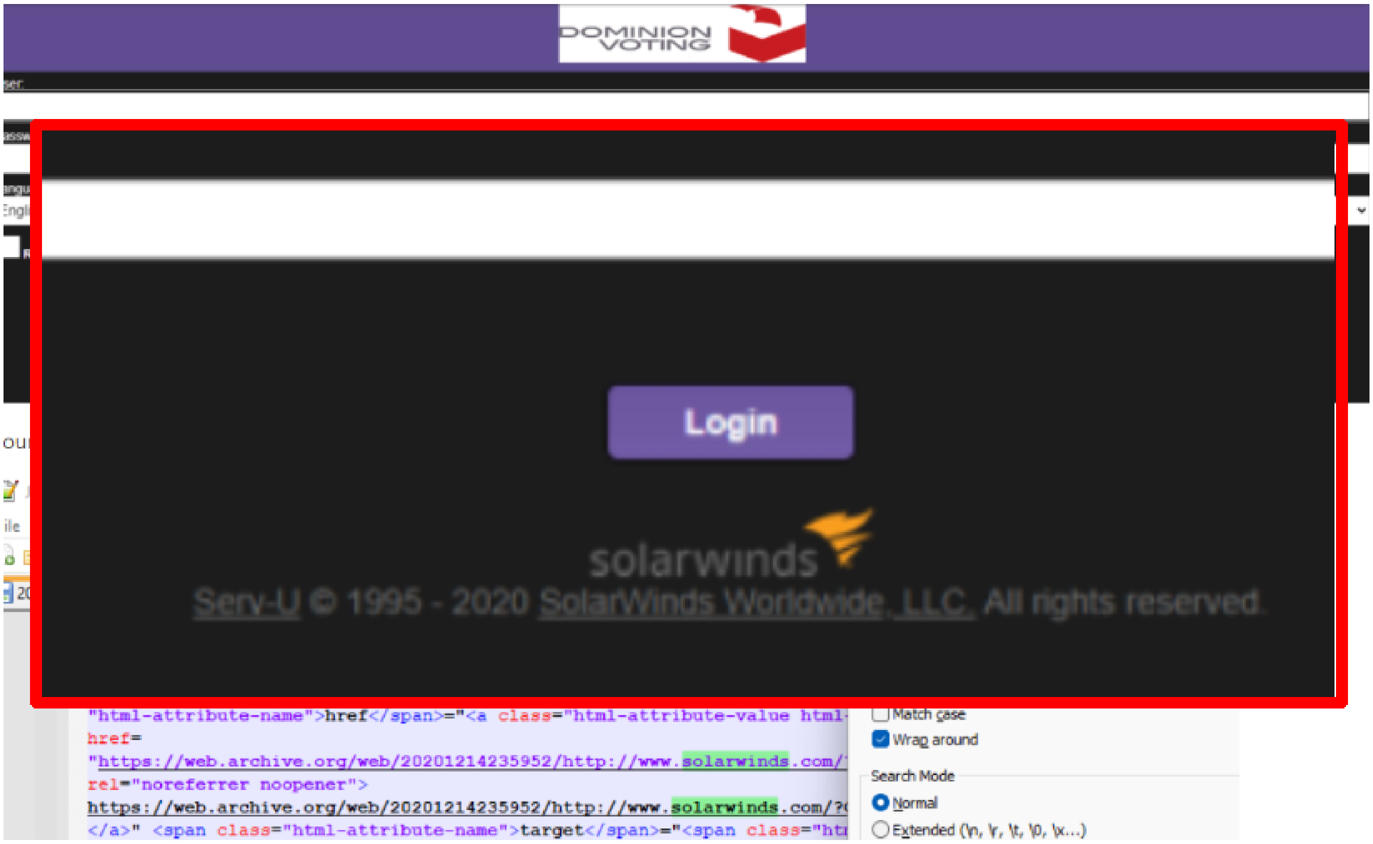
□ Remember me

Login

solarwinds

Serv-U © 1995 - 2020 SolarWinds Worldwide, LLC. All rights reserved.

I’ll zoom in for you:



Serv-U © 1995 - 2020 SolarWinds Worldwide, LLC. All rights reserved.

```
"html-attribute-name">href</span>="<a class="html-attribute-value html-
href=
"https://web.archive.org/web/20201214235952/http://www.solarwinds.com/
rel="noreferrer noopener">
https://web.archive.org/web/20201214235952/http://www.solarwinds.com/?
</a>" <span class="html-attribute-name">target</span>="<span class="htm
```

□ Match case

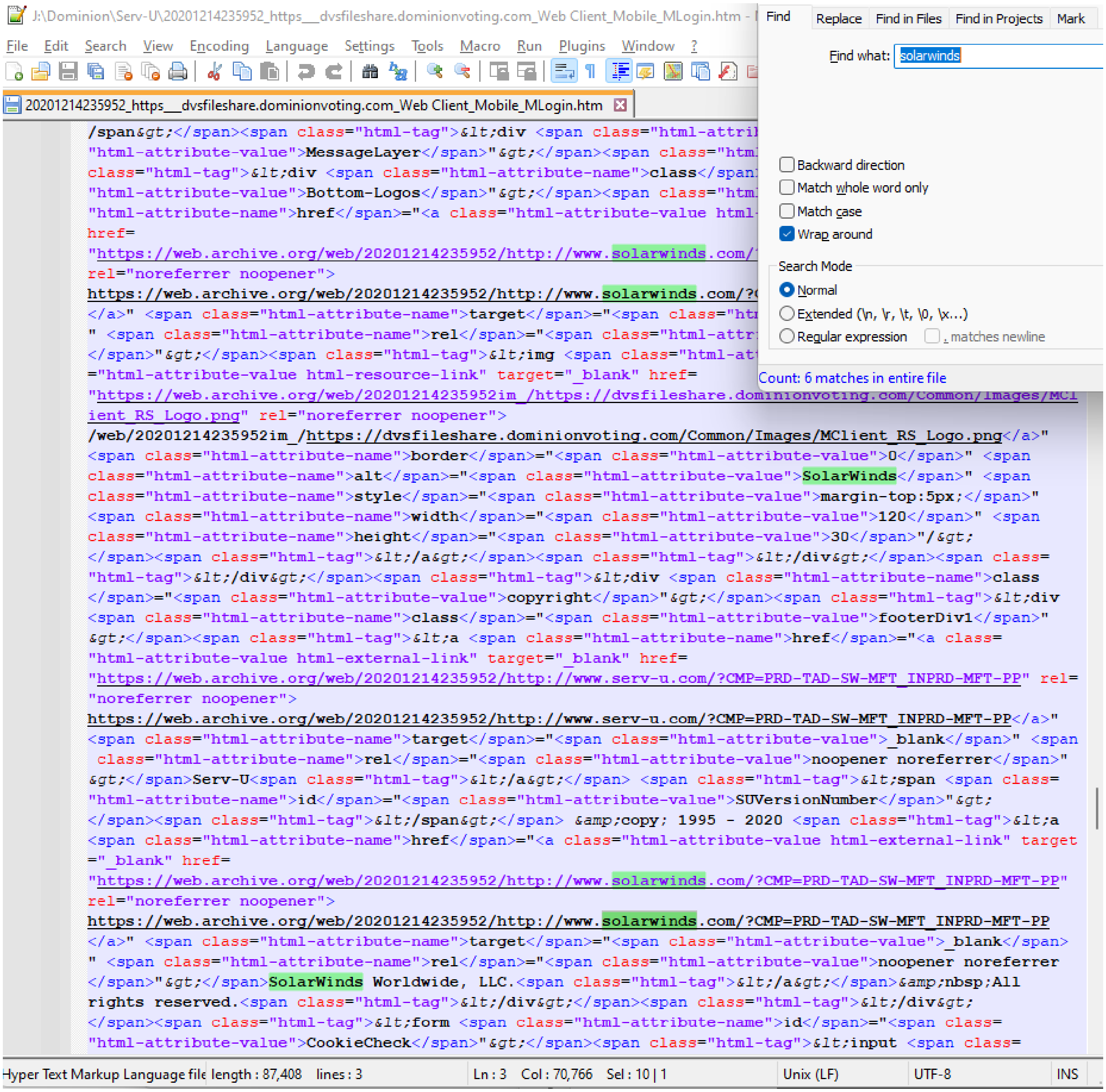
☑ Wrap around

Search Mode

● Normal

○ Extended (\n, \r, \t, \0, \x...)

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



J:\Dominion\Serv-U\20201214235952_https__dvsfileshare.dominionvoting.com_Web Client_Mobile_MLogin.htm -
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
20201214235952_https__dvsfileshare.dominionvoting.com_Web Client_Mobile_MLogin.htm
Find
Replace
Find in Files
Find in Projects
Mark

Find what: solarwinds

□ Backward direction
□ Match whole word only
□ Match case
☑ Wrap around

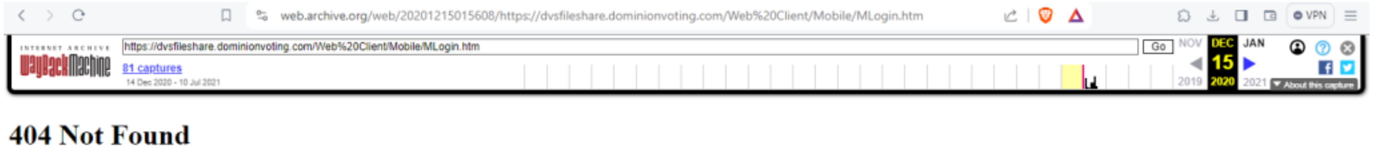
Search Mode
● Normal
○ Extended (\n, \r, \t, \0, \x...)
○ Regular expression □ . matches newline

Count: 6 matches in entire file

```
/span&gt;</span><span class="html-tag">&lt;div <span class="html-attril
"html-attribute-value">MessageLayer</span>"&gt;</span><span class="html
class="html-tag">&lt;div <span class="html-attribute-name">class</span
"html-attribute-value">Bottom-Logos</span>"&gt;</span><span class="html
"html-attribute-name">href</span>="<a class="html-attribute-value html-
href=
"https://web.archive.org/web/20201214235952/http://www.solarwinds.com/?
rel="noreferrer noopener">
https://web.archive.org/web/20201214235952/http://www.solarwinds.com/?C
</a>" <span class="html-attribute-name">target</span>="<span class="htr
" <span class="html-attribute-name">rel</span>="<span class="html-attr
</span>"&gt;</span><span class="html-tag">&lt;img <span class="html-at
="html-attribute-value html-resource-link" target="_blank" href=
"https://web.archive.org/web/20201214235952im_/https://dvsfileshare.dominionvoting.com/Common/Images/MCl
ient_RS_Logo.png" rel="noreferrer noopener">
/web/20201214235952im_/https://dvsfileshare.dominionvoting.com/Common/Images/MClient_RS_Logo.png</a>"
<span class="html-attribute-name">border</span>="<span class="html-attribute-value">0</span>" <span
class="html-attribute-name">alt</span>="<span class="html-attribute-value">SolarWinds</span>" <span
class="html-attribute-name">style</span>="<span class="html-attribute-value">margin-top:5px;</span>"
<span class="html-attribute-name">width</span>="<span class="html-attribute-value">120</span>" <span
class="html-attribute-name">height</span>="<span class="html-attribute-value">30</span>"/&gt;
</span><span class="html-tag">&lt;/a&gt;</span><span class="html-tag">&lt;/div&gt;</span><span class=
"html-tag">&lt;/div&gt;</span><span class="html-tag">&lt;div <span class="html-attribute-name">class
</span>="<span class="html-attribute-value">copyright</span>"&gt;</span><span class="html-tag">&lt;div
<span class="html-attribute-name">class</span>="<span class="html-attribute-value">footerDiv1</span>"
&gt;</span><span class="html-tag">&lt;a <span class="html-attribute-name">href</span>="<a class=
"html-attribute-value html-external-link" target="_blank" href=
"https://web.archive.org/web/20201214235952/http://www.serv-u.com/?CMP=PRD-TAD-SW-MFT_INPRD-MFT-PP" rel=
"noreferrer noopener">
https://web.archive.org/web/20201214235952/http://www.serv-u.com/?CMP=PRD-TAD-SW-MFT_INPRD-MFT-PP</a>"
<span class="html-attribute-name">target</span>="<span class="html-attribute-value">_blank</span>" <span
 class="html-attribute-name">rel</span>="<span class="html-attribute-value">noopener noreferrer</span>"
&gt;</span>Serv-U<span class="html-tag">&lt;/a&gt;</span> <span class="html-tag">&lt;span <span class=
"html-attribute-name">id</span>="<span class="html-attribute-value">SUVersionNumber</span>"&gt;
</span><span class="html-tag">&lt;/span&gt;</span> &amp;copy; 1995 - 2020 <span class="html-tag">&lt;a
<span class="html-attribute-name">href</span>="<a class="html-attribute-value html-external-link" target
="_blank" href=
"https://web.archive.org/web/20201214235952/http://www.solarwinds.com/?CMP=PRD-TAD-SW-MFT_INPRD-MFT-PP"
rel="noreferrer noopener">
https://web.archive.org/web/20201214235952/http://www.solarwinds.com/?CMP=PRD-TAD-SW-MFT_INPRD-MFT-PP
</a>" <span class="html-attribute-name">target</span>="<span class="html-attribute-value">_blank</span>
" <span class="html-attribute-name">rel</span>="<span class="html-attribute-value">noopener noreferrer
</span>"&gt;</span>SolarWinds Worldwide, LLC.<span class="html-tag">&lt;/a&gt;</span>&amp;nbsp;All
rights reserved.<span class="html-tag">&lt;/div&gt;</span><span class="html-tag">&lt;/div&gt;
</span><span class="html-tag">&lt;form <span class="html-attribute-name">id</span>="<span class=
"html-attribute-value">CookieCheck</span>"&gt;</span><span class="html-tag">&lt;input <span class=
```

Hyper Text Markup Language file length : 87,408 lines : 3 Ln : 3 Col : 70,766 Sel : 10 | 1 Unix (LF) UTF-8 INS

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


web.archive.org/web/20201215015608/https://dvsfileshare.dominionvoting.com/Web%20Client/Mobile/MLogin.htm

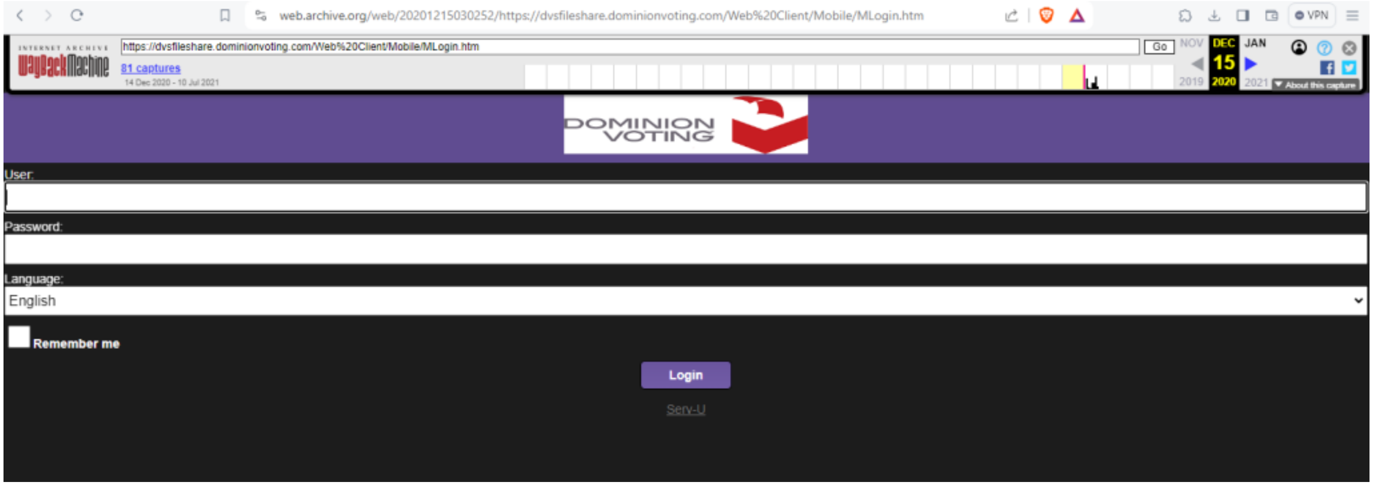
https://dvsfileshare.dominionvoting.com/Web%20Client/Mobile/MLogin.htm

81 captures

14 Dec 2020 - 10 Jul 2021

404 Not Found

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


web.archive.org/web/20201215030252/https://dvsfileshare.dominionvoting.com/Web%20Client/Mobile/MLogin.htm

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

81 captures

14 Dec 2020 - 10 Jul 2021

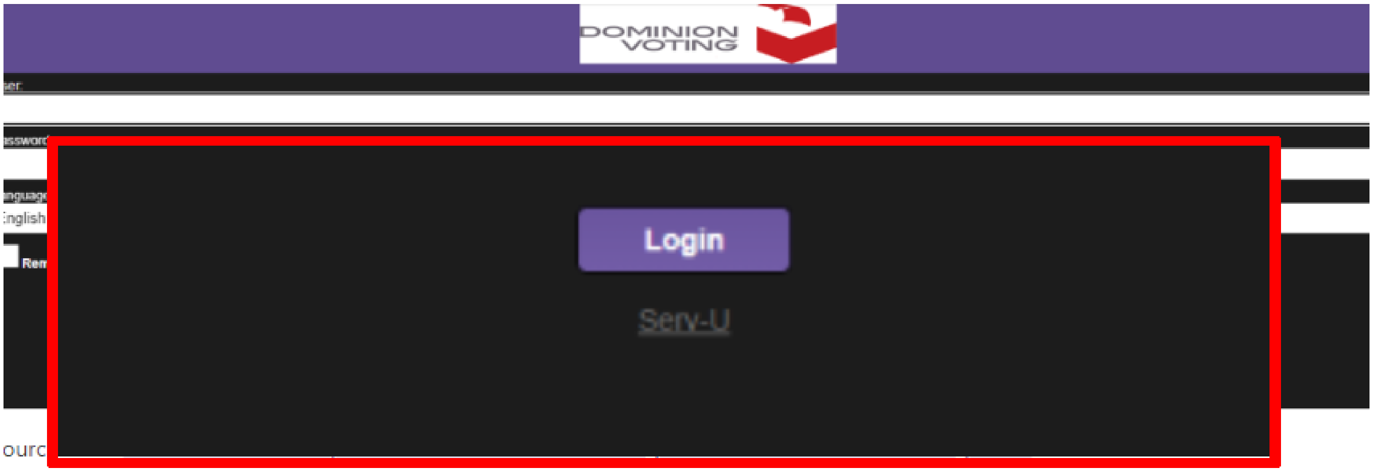
User:

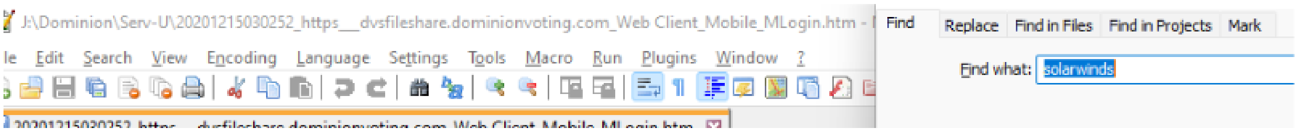
Password:

Language: English

□ Remember me

I’ll zoom in again:



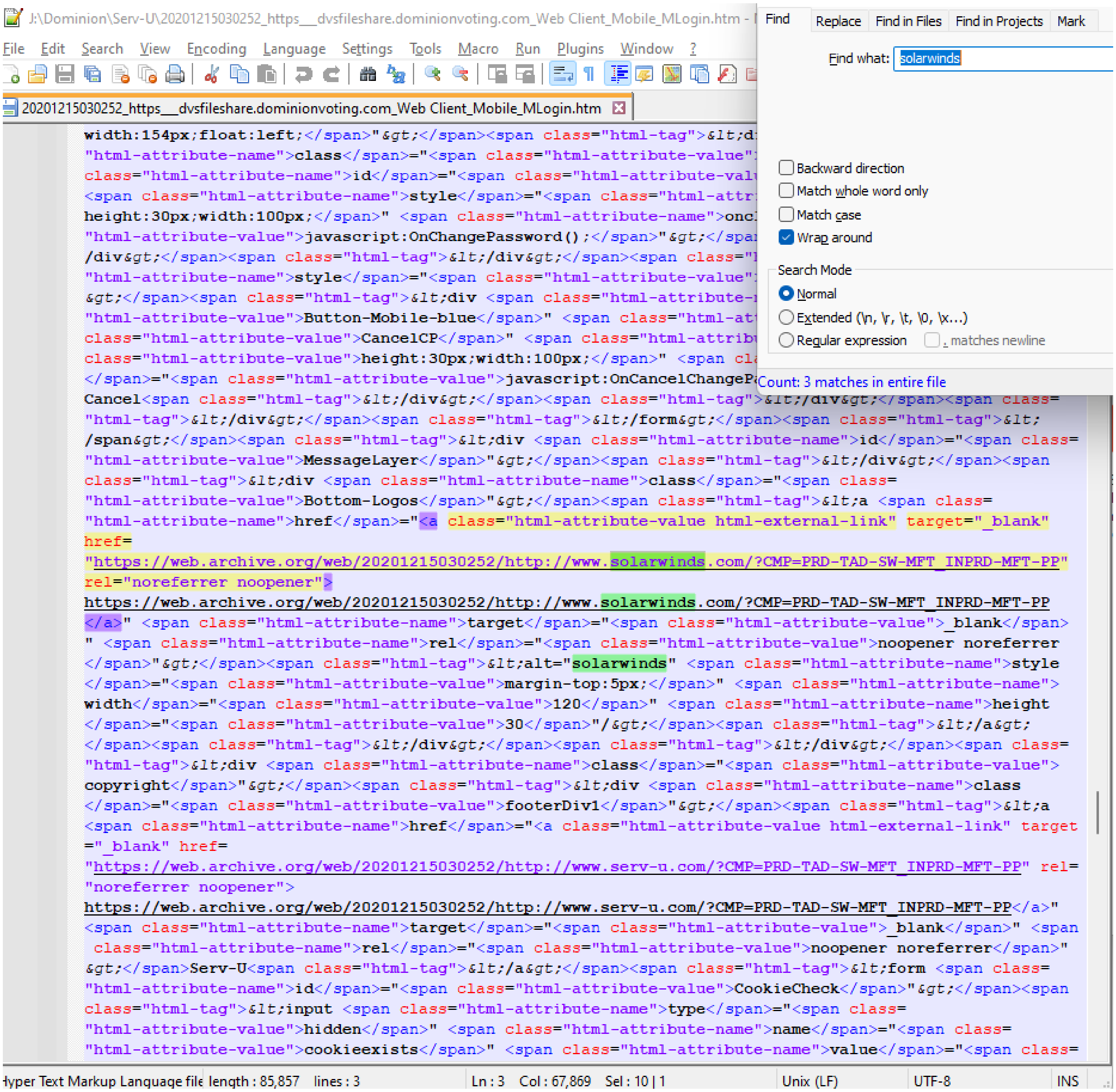

J:\Dominion\Serv-U\20201215030252_https__dvsfileshare.dominionvoting.com_Web Client_Mobile_MLogin.htm

Find what: solarwinds

le Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Find
Replace
Find in Files
Find in Projects
Mark
20201215030252_https__dvsfileshare.dominionvoting.com_Web Client_Mobile_MLogin.htm

Their website source code

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



J:\Dominion\Serv-U\20201215030252_https___dvsfileshare.dominionvoting.com_Web Client_Mobile_MLogin.htm -

20201215030252_https___dvsfileshare.dominionvoting.com_Web Client_Mobile_MLogin.htm

Find what: solarwinds

☐ Backward direction
☐ Match whole word only
☐ Match case
☑ Wrap around

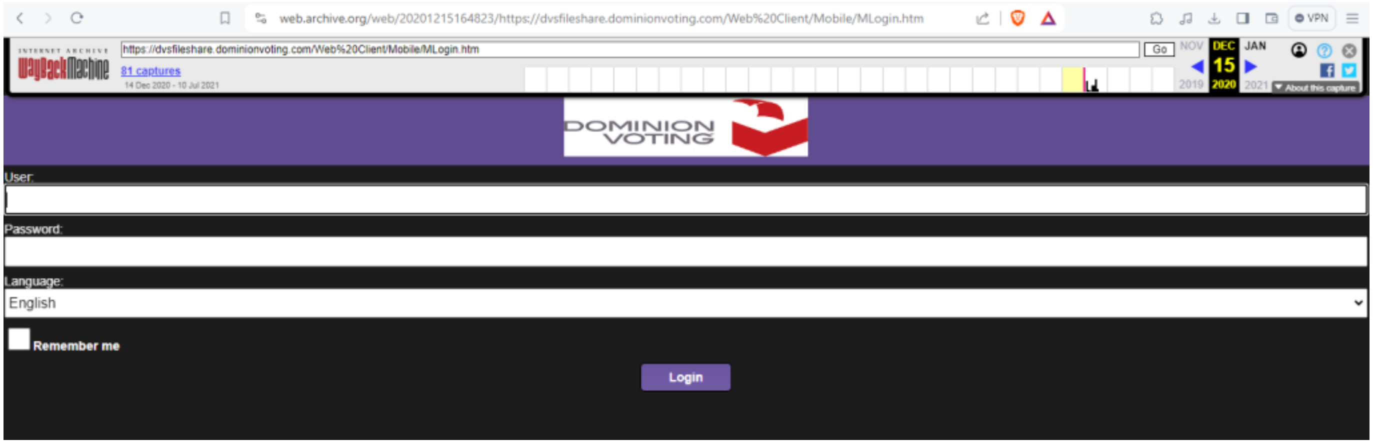
Search Mode
● Normal
○ Extended (\n, \r, \t, \0, \x...)
○ Regular expression ☐ . matches newline

Count: 3 matches in entire file

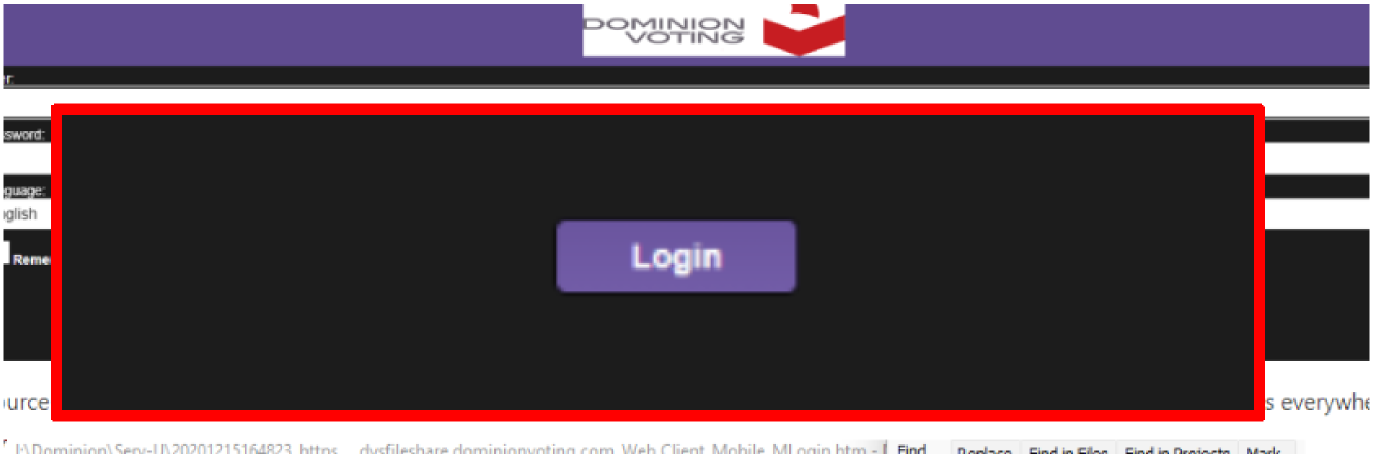
```
width:154px;float:left;</span>"&gt;</span><span class="html-tag">&lt;d
"html-attribute-name">class</span>="<span class="html-attribute-value"
class="html-attribute-name">id</span>="<span class="html-attribute-valu
<span class="html-attribute-name">style</span>="<span class="html-attr
height:30px;width:100px;</span>" <span class="html-attribute-name">oncl
"html-attribute-value">javascript:OnChangePassword();</span>"&gt;</spa
/div&gt;</span><span class="html-tag">&lt;/div&gt;</span><span class="
"html-attribute-name">style</span>="<span class="html-attribute-value"
&gt;</span><span class="html-tag">&lt;div <span class="html-attribute-
"html-attribute-value">Button-Mobile-blue</span>" <span class="html-at
class="html-attribute-value">CancelCP</span>" <span class="html-attrib
class="html-attribute-value">height:30px;width:100px;</span>" <span cla
</span>="<span class="html-attribute-value">javascript:OnCancelChangeP
Cancel<span class="html-tag">&lt;/div&gt;</span><span class="html-tag">&lt;/div&gt;</span><span class=
"html-tag">&lt;/div&gt;</span><span class="html-tag">&lt;/form&gt;</span><span class="html-tag">&lt;
/span&gt;</span><span class="html-tag">&lt;div <span class="html-attribute-name">id</span>="<span class=
"html-attribute-value">MessageLayer</span>"&gt;</span><span class="html-tag">&lt;/div&gt;</span><span
class="html-tag">&lt;div <span class="html-attribute-name">class</span>="<span class=
"html-attribute-value">Bottom-Logos</span>"&gt;</span><span class="html-tag">&lt;a <span class=
"html-attribute-name">href</span>="<a class="html-attribute-value html-external-link" target="_blank"
href=
"https://web.archive.org/web/20201215030252/http://www.solarwinds.com/?CMP=PRD-TAD-SW-MFT_INPRD-MFT-PP"
rel="noreferrer noopener">
https://web.archive.org/web/20201215030252/http://www.solarwinds.com/?CMP=PRD-TAD-SW-MFT_INPRD-MFT-PP
</a>" <span class="html-attribute-name">target</span>="<span class="html-attribute-value">_blank</span>
" <span class="html-attribute-name">rel</span>="<span class="html-attribute-value">noopener noreferrer
</span>"&gt;</span><span class="html-tag">&lt;alt="solarwinds" <span class="html-attribute-name">style
</span>="<span class="html-attribute-value">margin-top:5px;</span>" <span class="html-attribute-name">
width</span>="<span class="html-attribute-value">120</span>" <span class="html-attribute-name">height
</span>="<span class="html-attribute-value">30</span>"/&gt;</span><span class="html-tag">&lt;/a&gt;
</span><span class="html-tag">&lt;/div&gt;</span><span class="html-tag">&lt;/div&gt;</span><span class=
"html-tag">&lt;div <span class="html-attribute-name">class</span>="<span class="html-attribute-value">
copyright</span>"&gt;</span><span class="html-tag">&lt;div <span class="html-attribute-name">class
</span>="<span class="html-attribute-value">footerDiv1</span>"&gt;</span><span class="html-tag">&lt;a
<span class="html-attribute-name">href</span>="<a class="html-attribute-value html-external-link" target
="_blank" href=
"https://web.archive.org/web/20201215030252/http://www.serv-u.com/?CMP=PRD-TAD-SW-MFT_INPRD-MFT-PP" rel=
"noreferrer noopener">
https://web.archive.org/web/20201215030252/http://www.serv-u.com/?CMP=PRD-TAD-SW-MFT_INPRD-MFT-PP</a>"
<span class="html-attribute-name">target</span>="<span class="html-attribute-value">_blank</span>" <span
 class="html-attribute-name">rel</span>="<span class="html-attribute-value">noopener noreferrer</span>"
&gt;</span>Serv-U<span class="html-tag">&lt;/a&gt;</span><span class="html-tag">&lt;form <span class=
"html-attribute-name">id</span>="<span class="html-attribute-value">CookieCheck</span>"&gt;</span><span
class="html-tag">&lt;input <span class="html-attribute-name">type</span>="<span class=
"html-attribute-value">hidden</span>" <span class="html-attribute-name">name</span>="<span class=
"html-attribute-value">cookieexists</span>" <span class="html-attribute-name">value</span>="<span class=
```

Hyper Text Markup Language file length : 85,857 lines : 3 Ln : 3 Col : 67,869 Sel : 10 | 1 Unix (LF) UTF-8 INS

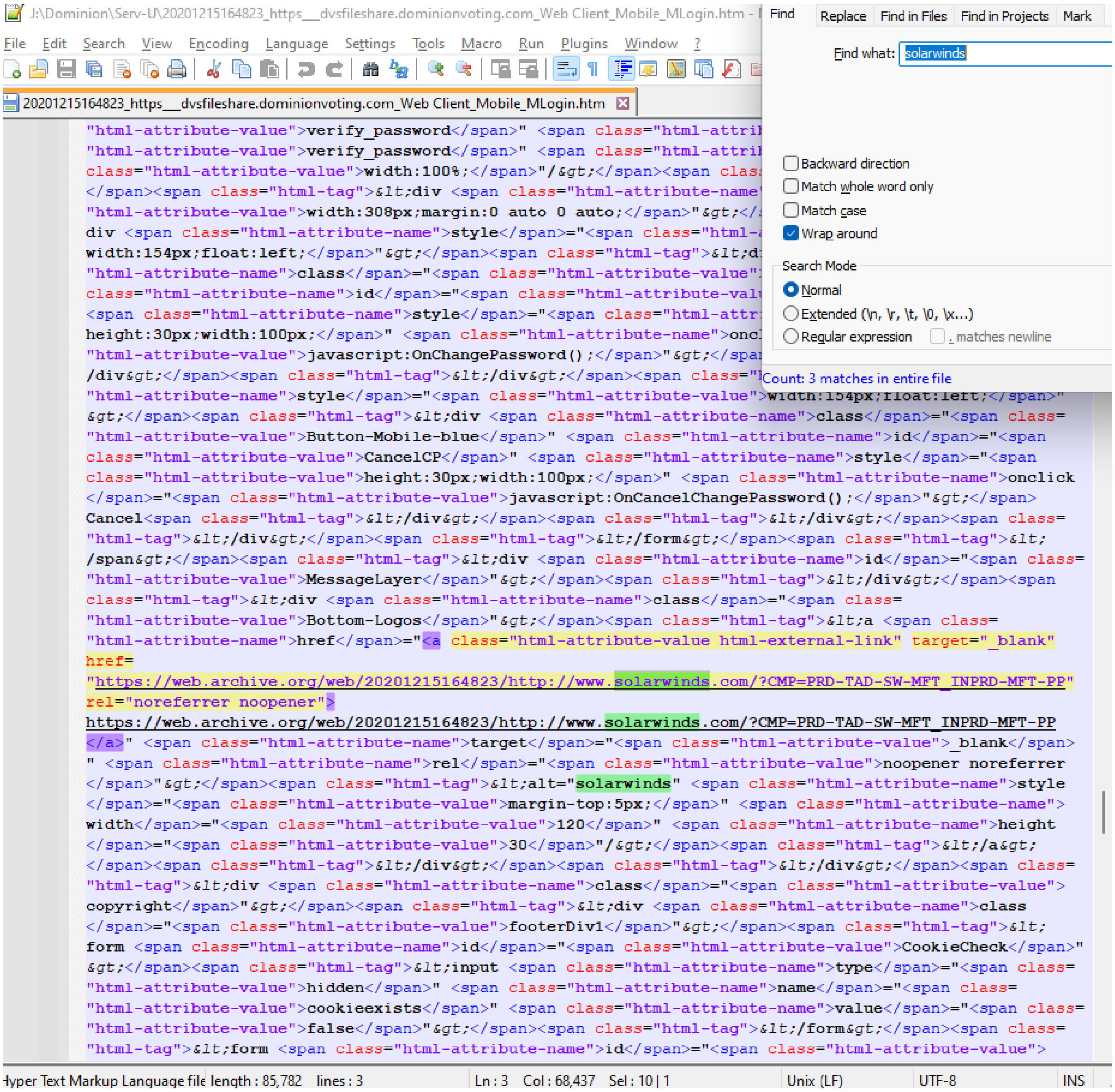
Then later in the same day at 16:48, they decide to remove Serv-U to try to cover that up as well:


web.archive.org/web/20201215164823/https://dvsfileshare.dominionvoting.com/Web%20Client/Mobile/MLogin.htm
INTERNET ARCHIVE
WayBackMachine
https://dvsfileshare.dominionvoting.com/Web%20Client/Mobile/MLogin.htm
Go
81 captures
14 Dec 2020 - 10 Jul 2021
NOV
DEC
JAN
15
2019
2020
2021
About this capture
DOMINION VOTING
User:
Password:
Language:
English
Remember me
Login

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:


J:\Dominion\Serv-U\20201215164823_https__dvsfileshare.dominionvoting.com_Web Client_Mobile_MLogin.htm - N
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
20201215164823_https__dvsfileshare.dominionvoting.com_Web Client_Mobile_MLogin.htm
Find Replace Find in Files Find in Projects Mark

Find what: solarwinds

□ Backward direction
□ Match whole word only
□ Match case
☑ Wrap around

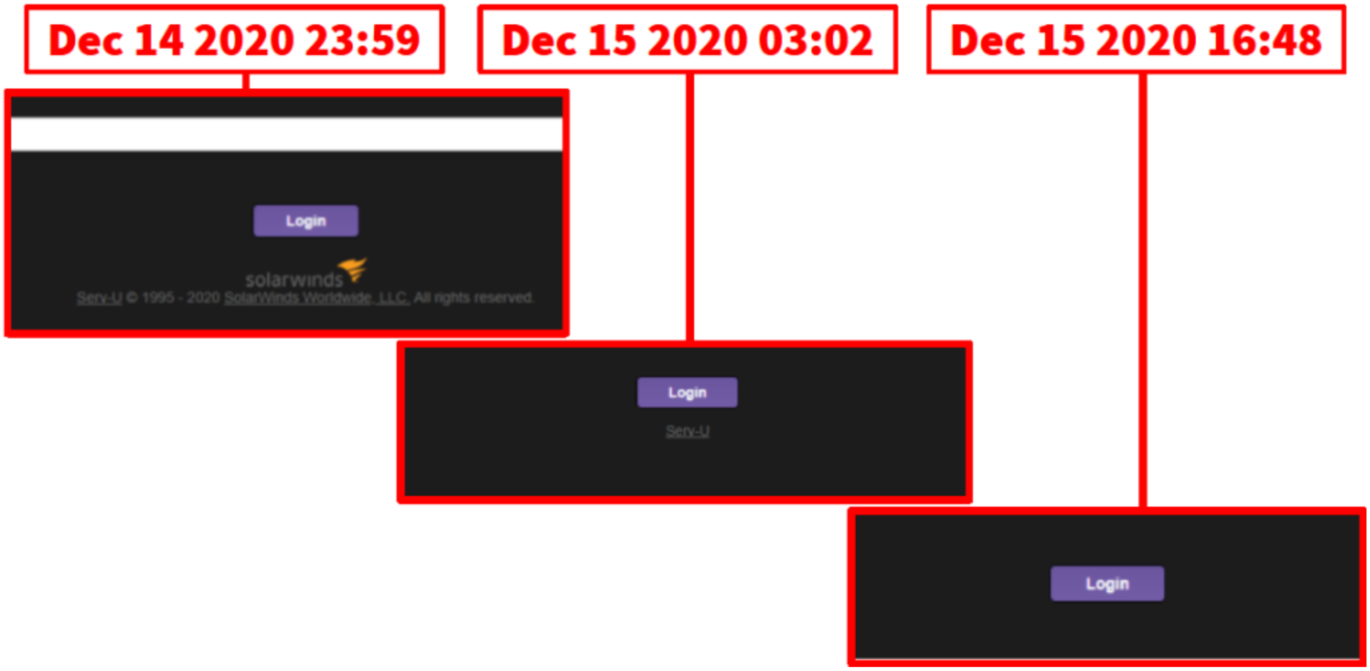
Search Mode
● Normal
○ Extended (\n, \r, \t, \0, \x...)
○ Regular expression □ . matches newline

Count: 3 matches in entire file

```
"html-attribute-value">verify_password</span>" <span class="html-attri
"html-attribute-value">verify_password</span>" <span class="html-attri
class="html-attribute-value">width:100%;</span>"/&gt;</span><span clas
</span><span class="html-tag">&lt;div <span class="html-attribute-name
"html-attribute-value">width:308px;margin:0 auto 0 auto;</span>"&gt;</
div <span class="html-attribute-name">style</span>="<span class="html-
width:154px;float:left;</span>"&gt;</span><span class="html-tag">&lt;d
"html-attribute-name">class</span>="<span class="html-attribute-value"
class="html-attribute-name">id</span>="<span class="html-attribute-val
<span class="html-attribute-name">style</span>="<span class="html-attr
height:30px;width:100px;</span>" <span class="html-attribute-name">oncl
"html-attribute-value">javascript:OnChangePassword();</span>"&gt;</spa
/div&gt;</span><span class="html-tag">&lt;/div&gt;</span><span class="
"html-attribute-name">style</span>="<span class="html-attribute-value">width:154px;float:left;</span>"
&gt;</span><span class="html-tag">&lt;div <span class="html-attribute-name">class</span>="<span class=
"html-attribute-value">Button-Mobile-blue</span>" <span class="html-attribute-name">id</span>="<span
class="html-attribute-value">CancelCP</span>" <span class="html-attribute-name">style</span>="<span
class="html-attribute-value">height:30px;width:100px;</span>" <span class="html-attribute-name">onclick
</span>="<span class="html-attribute-value">javascript:OnCancelChangePassword();</span>"&gt;</span>
Cancel<span class="html-tag">&lt;/div&gt;</span><span class="html-tag">&lt;/div&gt;</span><span class=
"html-tag">&lt;/div&gt;</span><span class="html-tag">&lt;/form&gt;</span><span class="html-tag">&lt;
/span&gt;</span><span class="html-tag">&lt;div <span class="html-attribute-name">id</span>="<span class=
"html-attribute-value">MessageLayer</span>"&gt;</span><span class="html-tag">&lt;/div&gt;</span><span
class="html-tag">&lt;div <span class="html-attribute-name">class</span>="<span class=
"html-attribute-value">Bottom-Logos</span>"&gt;</span><span class="html-tag">&lt;a <span class=
"html-attribute-name">href</span>="<a class="html-attribute-value html-external-link" target="_blank"
href=
"https://web.archive.org/web/20201215164823/http://www.solarwinds.com/?CMP=PRD-TAD-SW-MFT_INPRD-MFT-PP"
rel="noreferrer noopener">
https://web.archive.org/web/20201215164823/http://www.solarwinds.com/?CMP=PRD-TAD-SW-MFT_INPRD-MFT-PP
</a>" <span class="html-attribute-name">target</span>="<span class="html-attribute-value">_blank</span>
" <span class="html-attribute-name">rel</span>="<span class="html-attribute-value">noopener noreferrer
</span>"&gt;</span><span class="html-tag">&lt;alt="solarwinds" <span class="html-attribute-name">style
</span>="<span class="html-attribute-value">margin-top:5px;</span>" <span class="html-attribute-name">
width</span>="<span class="html-attribute-value">120</span>" <span class="html-attribute-name">height
</span>="<span class="html-attribute-value">30</span>"/&gt;</span><span class="html-tag">&lt;/a&gt;
</span><span class="html-tag">&lt;/div&gt;</span><span class="html-tag">&lt;/div&gt;</span><span class=
"html-tag">&lt;div <span class="html-attribute-name">class</span>="<span class="html-attribute-value">
copyright</span>"&gt;</span><span class="html-tag">&lt;div <span class="html-attribute-name">class
</span>="<span class="html-attribute-value">footerDiv1</span>"&gt;</span><span class="html-tag">&lt;
form <span class="html-attribute-name">id</span>="<span class="html-attribute-value">CookieCheck</span>"
&gt;</span><span class="html-tag">&lt;input <span class="html-attribute-name">type</span>="<span class=
"html-attribute-value">hidden</span>" <span class="html-attribute-name">name</span>="<span class=
"html-attribute-value">cookieexists</span>" <span class="html-attribute-name">value</span>="<span class=
"html-attribute-value">false</span>"&gt;</span><span class="html-tag">&lt;/form&gt;</span><span class=
"html-tag">&lt;form <span class="html-attribute-name">id</span>="<span class="html-attribute-value">
```

Hyper Text Markup Language file length : 85,782 lines : 3 Ln : 3 Col : 68,437 Sel : 10 | 1 Unix (LF) UTF-8 INS

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:



Dec 14 2020 23:59

Dec 15 2020 03:02

Dec 15 2020 16:48

Login
solarwinds
Serv-U © 1995 - 2020 SolarWinds Worldwide, LLC. All rights reserved
Login
Serv-U
Login

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.