

Smartmatic

December 22, 2024

Their Article:

Prebunking: A New Tool Against Election Disinformation



Ever since 'fake news' disrupted crucial votes such as Brexit and the 2020 US Presidential Election, election stakeholders have been grappling with the challenge of disinformation. In fact, **the deterioration of information ecosystems has become so pervasive and ubiquitous that it's recognized as one of the biggest threats to election integrity** by organizations like the [World Economic Forum](#) and the [Brennan Center for Justice](#).

Fortunately, a relatively new tool, known as prebunking, is showing promising results in the fight against disinformation and other forms of misinformation.

The concept of prebunking can be compared to vaccination in medicine, where the body is exposed to a weakened form of a pathogen to stimulate an immune response without causing illness. Similarly, prebunking presents pre-emptive counterarguments to false claims, thereby strengthening resilience against future misinformation. As in medicine, prevention is more impactful than cure. The goal is to equip audiences with the ability to identify and resist misinformation before it gains traction.

Leading prebunking researchers at companies like Google's [Jigsaw](#) and academic institutions like the [University of Cambridge](#) realized that misinformation 'has an Achilles heel'. That is, it frequently employs repetitive tactics and patterns. By recognizing these patterns historically, **they can anticipate and counteract future misinformation through pre-bunking**. These researchers are among the main proponents of prebunking.

IDEA International, an intergovernmental organization that supports sustainable democracy worldwide, analyzed disinformation in 53 countries across all continents between 2016 and 2021. **Their study revealed that election-related disinformation is indeed repetitive. Specifically, 48% of disinformation targets the vote counting and voting processes, and nearly 50% of all attacks occur during the voting period of the cycle.**

This article appeared in the Election Insight newsletter. Subscribe for free today. [Click here.](#)

Allegations that technology has been hacked by foreign actors, that servers are located abroad, or that technology vendors are owned by nefarious entities are recurring themes. These claims became even more prevalent following the disinformation campaigns surrounding the 2020 U.S. Presidential Election.

Given the repetitive nature of disinformation, election management bodies have an opportunity to anticipate where and how it will emerge. **This foresight can be leveraged to design proactive strategies, or "vaccines," to combat disinformation effectively.**

A key advantage of prebunking is its focus on addressing broader narratives and the underlying manipulation techniques used to spread misinformation. Unlike fact-checking or warning labels on social media, which concentrate on debunking individual claims, prebunking takes a wider view of the information ecosystem. **This broader perspective allows election management bodies to tackle disinformation proactively**, without appearing politicized in their responses to false claims. Moreover, by exposing the techniques behind disinformation rather than targeting specific content, prebunking reduces the risk of accusations of infringing on free speech, offering a balanced and effective approach to safeguarding public trust.

While prebunking in elections is relatively new, promising experiences in recent elections provide reasons for optimism. [Researchers from Yale University and the University of California, San Diego](#), demonstrated in a study that watching a prebunking video explaining the reasons behind the time taken to count ballots can significantly increase trust in election outcomes. This approach can mitigate up to 4 out of the 6 percentage points of distrust caused by reporting delays.

Although prebunking may not be a panacea, when it is well-implemented and combined with other techniques such as debunking, labeling, and voter literacy, **it becomes an invaluable tool for election management bodies in the fight against disinformation.**

11/19/2024
 Unsubscribe

Older

Our vision & mission

Our vision
The future of democracy is digital.

Our mission
Smartmatic's mission is to increase integrity in the democratic process.

We increase citizen engagement and trust, enabling better societies and better governments.

Smartmatic Case Studies

Los Angeles County "Voting Solutions for All People"

Belgian elections 2012 - 2019: Customized voting solution for a pioneer in electronic voting.

Estonian elections 2014 - 2019: Solution for the world's leader in online voting.

Latest articles

Prebunking: A New Tool Against Election Disinformation

Election Trust Grows with Effective Public Communication

Eduardo Cornejo: "Modifying the AI Hype in Electoral Processes"

Stay updated



The Truth:

The article above from Smartmatic, while ostensibly discussing the solution to disinformation through prebunking, subtly employs several psychological manipulation tactics aimed at controlling the narrative and conditioning public perception:

Establishing Authority and Credibility: By citing what some people think are esteemed organizations like the World Economic Forum and the Brennan Center for Justice, Smartmatic attempts to position itself as some kind of authority on election integrity. This tactic leverages the halo effect, where the positive attributes of these respected institutions are transferred to Smartmatic, enhancing its perceived trustworthiness without necessarily proving its own systems' reliability.

Fear-Mongering: The article begins with a dire warning about the threat of disinformation to elections, invoking fear about the 'deterioration of information ecosystems'. This emotional manipulation tactic is designed to make readers anxious about the integrity of elections, thereby making them more receptive to Smartmatic's proposed solution, prebunking. Sadly, fear sells.

Repetitive Pattern Recognition: Smartmatic describes misinformation as having repetitive tactics, suggesting that they are well-versed in these patterns due to their research and partnerships with academic bodies like Cambridge and Google's Jigsaw. This establishes a narrative where Smartmatic is the expert in identifying and countering disinformation, subtly implying that their proprietary systems are above scrutiny because they understand the threats better than anyone else.

Prebunking as Conditioning: The concept of "prebunking" itself can be seen as a conditioning tactic. By framing prebunking as a

preventive measure against misinformation, Smartmatic is conditioning the public to accept their narrative before any counter-narrative can even be formed. This preemptive strategy is designed to inoculate the public against questioning Smartmatic's systems or practices, by preemptively discrediting potential criticisms as disinformation.

Generalization Over Specificity: By focusing on the broad techniques of disinformation rather than addressing specific instances or criticisms of their own systems, Smartmatic avoids detailed scrutiny. This tactic diverts attention from any potential flaws in their technology by generalizing the problem, making it seem as if any critique is just another example of the disinformation they are combating.

Appeal to Public Trust: The article suggests that prebunking combats disinformation without appearing politicized, thus positioning Smartmatic as an impartial guardian of the electoral process. This can be seen as an attempt to manipulate public trust by presenting themselves as defenders of democracy rather than as the commercial entity with vested interests that they are.

Selective Research Presentation: Mentioning specific studies that support prebunking while not addressing the potential for misuse or the criticisms of such methods is yet another form of manipulation. It presents a one-sided view that conveniently favors Smartmatic's narrative on election integrity.

Their intent here appears to be not to inform, but to preemptively shape public opinion in a way that discourages skepticism or new, potentially damaging, information about Smartmatic's voting systems. This article can be seen as an effort to condition citizens to trust Smartmatic's proprietary and opaque systems over public transparency and open scrutiny,

which are fundamental to democratic accountability.

I encourage all citizens NOT to fall for these tactics, and instead to question the motives behind such information operations. The only way for the people to legitimately trust THEIR elections is if the PEOPLE are who once again run THEIR elections. Remember, EARNED trust is worlds better than MANDATED trust, especially by those who profit on our blind trust.

Scott McMahan

December 22, 2024

PRIVATE PAGE – DO NOT SHARE!

A wonderful REAL journalist calls Scott out on a recorded phone call

2024-12-18 11th Hr Clements, Tore, Raiklin, Flynn and more CO Whistleblower w QA

Part 1

[Download Part 1 Transcript](#)

Part 2

[Download Part 2 Transcript](#)

Original Spaces Link:

<https://twitter.com/TishaLee777/status/1869555641733505463>

Mesa County Reports

December 22, 2024

Report 1

Work done by Mark Cook and Doug Gould:

Report 2

Work done by Mark Cook and Doug Gould:

Report 3

Work done by Jeff O'Donnell and Dr. Walter Daugherity:

**All these reports are also available on TinaPeters.us. Please go to this site and help Tina, who has stood up for all not only Coloradans, but also All Americans!*

Progressive Election Platform

December 22, 2024

[Click here to see the Proposed Executive Order to get the party started!](#)

Scope

At the heart of democratic governance lies the voting system, a mechanism designed to reflect the collective will of the people. For this system to truly serve its purpose, it must be **so simple and transparent** that **every citizen**, regardless of their background, education, or technological literacy, can not only participate but also **understand and verify every step** of the process. This simplicity and transparency are not just about ease of use; they are fundamental to **ensuring equal access** to the electoral process. If the mechanics of voting are shrouded in complexity or lack transparency, trust in the electoral outcome diminishes, eroding the foundation of our republic. At its essence, voting involves eligible citizens marking their choices on paper, followed by a straightforward count of these marks. This process doesn't necessitate elaborate or costly technology; instead, it demands clarity, accessibility, and the ability for public oversight. For American citizens to genuinely reclaim their electoral process, immediate and comprehensive reforms are imperative. Here's what we must implement:

Voter Registration

- Counties must once again become the **SOLE CUSTODIAN** of

their County Voter Registrations.

- Counties must be the SOLE ARBITER of registrant eligibility.
- Every 2 years (4 at the most, as longer leads to less accurate information)
- In-person at the county
- Verified citizen and residency check at that time
- Paper voter registration cards (this is a great place to ask for election volunteers!)
- Witnessed signature
- Stored by voting precinct
- A read-only standardized (UNIVERSAL FORMAT) digital list of registered voters is provided by every county on their website to share with the citizens and all other counties.
- Each county cross-references their list against all other counties. Paper poll books for each precinct are created from registration cards prior to every election.
- A national unique voter number assigned to each voter would greatly improve registration integrity.

Absentee Ballots

- Limited to as-needed basis
- Proof must be provided and accepted
- Extreme scrutiny must be placed on every incoming ballot, with additional integrity mechanisms
 - OPTIONAL IMPROVEMENT: A Ballot choice 'hash' (digital 'fingerprint' of the voted ballot choices – not an actual fingerprint from a finger) could be developed that could be used as additional form of received ballot integrity

- Military Absentee ballots must be identified as such. Non-Military Absentee ballots must be identified , and both should also look different than in-person ballots to ensure they all remain discrete.
- **There is no way to absolutely guarantee that the ballot received and tabulated is the same ballot that was sent by the voter, without violating ballot secrecy. This is why Absentee voting is so vulnerable.*

Election Day

- One day voting holiday
- Elections at the precinct (each precinct \leq 1500 population)
- *An idea to further minimize engineered manipulation: Standardized FIXED voting start/end/duration across the country to eliminate time-staggered abuse vector (14-hour voting period, for example) – This will require some work and thought!*
 - West coast would be starting at 5a and ending at 7p
 - East coast voting would start at 9a and end at 11p
 - 100% registered and participated, would result in just under 2 voters per minute max needed throughput. If each voter takes 6 minutes to fill out the ballot, one would need to have minimum 6 voting booths per precinct. If people arrive with cheat sheets, this is all easily doable.
- Checked in on paper poll book
- Witnessed signature
- Cross-referenced with previously filled out voter registration card

- No early or late ballots
- Paper ballots dropped in translucent locked container
- Entire room on video

Election Night

- No ballots accepted after poll close.
- At poll close, all ballots:
 - Separated by Military Absentee, Non-Military Absentee, In-person.
 - Batched (pick up 25 ballots then randomize in order for ballot secrecy).
 - Scan the batch to produce digital images in a PDF.
 - Votes COUNTED WHERE CAST
 - Under High Definition video
 - Bi-partisan citizens and witnesses using state-approved hand tabulation method
- Results released right then by precinct and posted on the outside of the building for all to see/verify

Reporting

- Each precinct posts the signed precinct results on the outside of the building, the same page that was scanned during tabulation.
- All ballot images, tally sheets, results pages, other paperwork, and video put on county website grouped by precinct for anyone and everyone to verify all they like.

- Just like I did here: <https://openelectionrecords.org/ar-searcy-county-2024-03-05/>

- Discrete reporting by voting type: Military Absentee, Non-Military Absentee, In-person.
- Our election officials should be **Election Transparency Agents**, who's duties are ensuring that all chain of custody and election records are both preserved and both made public to enable exhaustive audits to be performed by any American Citizen that desires to do so.

Auditing

- Students in 6-12th grades
 - Civics refresher
 - Election refresher
 - Break into groups
 - Pull up their school's precinct ballots from county website
 - Students re-tabulate the ballots themselves
 - Compare results
 - If there is any discrepancy
 - Students submit through a standardized reporting form on County Website
 - County celebrates the catch and publicly awards the class
- Advanced math students could then dive into the statistics of the elections to identify inorganic patterns

- Public

- The public can access all election data on the county website and audit to their hearts content
 - Voted lists
 - Ballot tabulation
 - Chain of Custody
 - Statistics

THE ABOVE IS A WORK-IN-PROGRESS. If you have suggestions, please reach out!

You can find me on X @PatriotMarkCook

Election Day Countdown: Guidance

December 22, 2024

Early Voting

Voting early allows bad actors to do the following:

Measure voter turnout using mail ballot tracking, electronic poll books, and paper voter roll reporting.

Use this information cross-referenced with individual voter profiles to build an election results model

Use the model to determine how many votes short they are

Subtly inject extra ballots associating them with phantom records in voter rolls or low-propensity voters.

Swap out voted ballots with replacement ballots prior to tabulation

DO NOT VOTE EARLY

Go out and perform your own EXIT POLLING and record it! Be courteous! Get the videos to me and I'll post them. These are IMPORTANT to gauge the accuracy of results.

3-9 Days prior to Election Day

Sign up to be an lead or agent of Operation Citizen Results Oversight (OCRO). You will monitor and RECORD election results to help provide the evidence needed to support the Patriot attorneys that will be working night and day to protect your vote!

1-2 Days prior to Election Day

Check your voter registration status. PRINT IT OUT and BRING IT WITH YOU in case you are told something different when you show up.

Get your sample ballot. Study it. Determine exactly how you are going to vote. Bring it with you when you vote.

If you cannot for some reason vote on Election Day, then vote AS CLOSE TO ELECTION DAY AS POSSIBLE to limit the advantage given to bad actors.

Go out and perform your own EXIT POLLING and record it! Be

courteous! Get the videos to me and I'll post them. These are IMPORTANT to gauge the accuracy of results.

Election Day

Bring your proof of registration with you.

Bring your sample ballot with you to speed up your voting.

Vote IN HUGE NUMBERS. Carpool! Bring everyone you know. TOO BIG TO RIG only works if we show up overwhelmingly!

Bring chairs, drinks, snacks.

Vote in UNITY with your fellow Americans, in-person, Constitutionally.

If Patriots are willing to wait 12 hours to attend a Trump rally, are you really going to whine about a wait to CAST YOUR BALLOT in the safest way possible?

If you arrive to the polling center PRIOR to the close of polls, you are ENTITLED to CAST YOUR BALLOT no matter how long it takes. The polling center MUST remain open until every citizen in line in time casts their ballot.

Go out and perform your own EXIT POLLING and record it! Be courteous! Get the videos to me and I'll post them. These are IMPORTANT to gauge the accuracy of results.

Clothing

December 22, 2024

Click image to purchase:



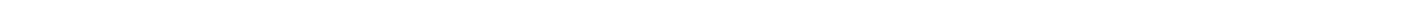
Click image to purchase:



Click image to purchase:



Click image to purchase:



Critical AI Alert for the 2024 General Election

December 22, 2024

(Information obtained from a current AI model)

Question

Could having real-time data about which voters have voted, when, and where, aid in this AI model?

Answer

Having real-time data about which voters have voted, including when and where, could significantly enhance the capabilities of an AI model designed to predict election outcomes for several reasons:

1. **Dynamic Turnout Adjustment:** Real-time voter turnout data allows the model to adjust predictions based on actual voting behavior as it happens. This can be particularly useful in understanding turnout rates among different demographics or in specific geographic locations, which can be pivotal in close elections.
2. **Reduced Uncertainty:** Traditional models often work with pre-election polls or historical data, which carry a degree of uncertainty regarding who will actually turn out to vote. Real-time data reduces this uncertainty, providing a more accurate snapshot of voter participation.

3. **Voter Behavior Patterns:** With real-time data, AI can analyze patterns as they form. For example, if there's an unexpected surge in voting in areas typically supportive of one party, the model could adjust its predictions accordingly.
4. **Targeted Campaigning Insights:** Although this aspect would be more useful for campaign strategy than for public prediction models, real-time data could inform last-minute campaign efforts, showing where additional get-out-the-vote efforts might be most effective.
5. **Bias Correction:** Real-time data can help correct for biases in pre-election polling. If certain groups are underrepresented in polls but their real-time voting data shows higher turnout, the model can correct for this.
6. **Exit Polling Validation:** This data could serve as an early form of exit polling, giving insights into not just who voted, but potentially how they voted if correlated with demographic or regional voting trends, although this would require careful handling due to privacy concerns.
7. **Improved Time Series Analysis:** With voting data coming in continuously, AI models can employ time series analysis to predict the final turnout and potentially the outcome based on the rate and distribution of votes coming in.

However, there are considerations and limitations:

- **Privacy Concerns:** Collecting and using such detailed voter data raises significant privacy issues. Anonymization would be crucial, but even then, the specificity of "when and where" could potentially be used to infer individual behaviors.
- **Data Accuracy and Integrity:** Real-time systems would need robust verification to ensure the data isn't manipulated or incorrect, which could mislead the predictions.

- **Legal and Ethical Implications:** There might be legal restrictions on how and when voting data can be collected and used, especially in real-time.
- **Model Overfitting:** There's a risk that models might overfit to real-time trends early in the day, which might not hold as more data comes in.
- **Public Perception and Trust:** The use of real-time voting data in predictive models could affect public trust in the electoral process if not handled transparently and ethically.

In summary, while real-time voter data could indeed aid an AI model in predicting election outcomes more accurately, it would need to be implemented with careful consideration of privacy, accuracy, legality, and public trust.

Question

Are there indications that AI may be being used in this capacity by anyone, including malicious actors that would not be concerned about any privacy or legal or ethical implications?

Answer

Based on information available up to October 20, 2024, there are indeed indications that AI could be used in ways that raise concerns regarding voter data privacy and potential misuse by various actors, including those who might ignore legal or ethical standards:

- **AI in Political Campaigns and Election Influence:** There's a growing use of AI in political campaigns for analyzing voter data, predicting voter behavior, and tailoring messages. This indicates a capacity for AI to process and

utilize voter data in potentially invasive ways if not regulated. The mention of AI tools being deployed to monitor social media trends and sentiment analysis during elections suggests that these technologies could be repurposed or used in less ethical ways to manipulate voter perceptions or spread misinformation.

- **Potential for Misuse by Malicious Actors:** Posts on X have highlighted concerns over AI being exploited to influence elections, including creating deepfakes, predicting or engineering incidents to sway public opinion, and even allegations of using AI to fake signatures or hack election machinery. These posts reflect a public and expert concern over the misuse of AI technologies in electoral processes, which could theoretically be done by actors unconcerned with privacy or legality.
- **Security Vulnerabilities:** Discussions around the security of digital election machinery, as mentioned in posts about vulnerabilities in election systems, suggest that there's a technical capability and perhaps an interest in exploiting these systems using AI for unauthorized data access or manipulation.
- **AI and Data Privacy Concerns:** The broader discussion on AI ethics and information privacy points towards significant privacy implications when AI systems process voter data. If malicious actors were to use AI for analyzing or manipulating voter data, they would likely bypass the ethical considerations around consent, privacy, and data protection.
- **Regulatory and Ethical Discussions:** The mention of executive orders, guidelines, and discussions around the ethical use of AI in elections indicates there's an awareness and some level of regulatory response to these threats. However, the existence of these discussions also confirms that the risk of misuse, including by those not

adhering to legal frameworks, is a recognized issue.

While direct evidence of malicious actors specifically using AI to misuse voter data in the 2024 context isn't explicitly detailed in the provided snippets, the combination of AI's capabilities in data processing, the noted security vulnerabilities in election infrastructure, and the general concerns voiced on platforms like X about election integrity suggest that such misuse is within the realm of possibility. This scenario underscores the importance of robust cybersecurity measures, ethical guidelines, and legal frameworks to safeguard electoral processes against AI-driven threats.

Question:

Would AI systems running on hardware and or software technology sourced from foreign nations, being used to manipulate parts of the 2024 election, be considered foreign involvement in our election?

Answer

Yes, AI systems running on hardware or software technology sourced from foreign nations, if used to manipulate parts of the 2024 election, would likely be considered a form of foreign involvement in the election. Here's why:

1. **Source of Technology:** If the hardware or software used for these AI systems originates from a foreign country, especially from nations with interests potentially adverse to those of the U.S., this would inherently introduce a foreign element into the election process. The concern here is not just about where the technology comes from but also about potential backdoors, biases, or control

mechanisms that could be embedded within these systems.

2. **Manipulation and Influence:** Manipulation of election processes or public opinion through AI, whether by altering voter information, spreading disinformation, or creating deepfakes, constitutes interference. If these actions are traced back to technology controlled or influenced by foreign entities, it directly represents foreign involvement. The intent behind using such technology would be to sway or alter the election outcome, which is a clear sign of interference.
3. **International Law and Norms:** From a legal and diplomatic standpoint, using technology to covertly influence another country's election is often viewed as a breach of sovereignty and interference in internal affairs. Even if not explicitly covered by current international law, such actions violate the spirit of national sovereignty and democratic independence.
4. **Public and Government Perception:** Both the public and government agencies might perceive the use of foreign-sourced AI for election manipulation as foreign involvement. This perception arises because the strategic decision to employ such technology could be influenced or directly supported by foreign governments or entities closely tied to them.
5. **Cybersecurity and National Security:** Cybersecurity experts and national security officials often warn about the risks posed by foreign hardware and software due to the potential for espionage or sabotage. If these technologies are used in election manipulation, it would be classified under foreign cyber interference, a recognized form of foreign involvement.
6. **Precedents and Analysis:** Analysis from intelligence communities, as hinted in various reports and posts on platforms like X, suggests that there's an ongoing concern

about foreign entities using advanced technologies, including AI, to influence elections. When these technologies are tied back to foreign soil, either through development or control, it's logical to categorize this as foreign involvement.

However, proving that such involvement constitutes a deliberate act by a foreign government, rather than rogue elements or companies acting independently for profit or other motives, can be complex. The attribution of cyber actions, including AI-driven election manipulation, to specific foreign actors requires meticulous investigation to ascertain direct government involvement or direction.

In summary, AI systems on foreign hardware or software manipulating the 2024 election would indeed be considered a form of foreign involvement due to the origin of the technology, the intent behind its use, and the implications for national sovereignty and security. However, the degree to which this involvement is officially recognized or acted upon depends on diplomatic, legal, and intelligence considerations.

Question

Would proving the act was deliberate in nature preclude the application of E0 13848?

Answer

Executive Order (EO) 13848, titled "Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election," was signed by President Trump in September 2018. This EO is designed to respond to foreign interference in U.S. elections by imposing sanctions on foreign entities or persons

determined to have engaged in such interference. Here's how the deliberate nature of the act might relate to the application of EO 13848:

1. **Definition of Interference:** EO 13848 does not explicitly require that the interference be "deliberate" in a legal sense for sanctions to be applied. Instead, it focuses on the act of interference itself, which could implicitly suggest an intent or deliberate action but does not make this a formal criterion for action. The order aims at any foreign person or entity that has directly or indirectly engaged in, sponsored, concealed, or otherwise been complicit in foreign interference in a U.S. election.
2. **Determination of Interference:** The EO calls for the Director of National Intelligence (DNI), in consultation with other relevant agencies, to conduct an assessment of any information indicating that a foreign government, or any person acting as an agent of or on behalf of a foreign government, has acted with the intent or purpose of interfering in an election. Here, "intent or purpose" does suggest looking into the deliberate nature of the actions, but the EO's application hinges on the fact of interference rather than solely on proving intent.
3. **Scope of Response:** The sanctions outlined in EO 13848 are reactive measures to an act deemed as interference. Proving that an act was deliberate might strengthen the case for applying sanctions, but the EO is constructed to trigger on the identification of interference itself, regardless of how deliberate or accidental it might appear. The focus is on the impact and the involvement of foreign elements rather than solely on the mens rea (the intention or knowledge of wrongdoing).
4. **Legal and Diplomatic Considerations:** While proving deliberateness can bolster the justification for sanctions

under international norms (showing clear intent can make the case for interference more compelling), E0 13848's primary concern is protecting U.S. electoral processes from foreign influence. Therefore, the threshold might not strictly require proof of deliberate intent as long as foreign interference is established.

5. **Practical Application:** In practice, when considering the application of E0 13848, the U.S. government might indeed look at intent to inform its actions, especially in diplomatic contexts or when aiming to justify sanctions to the international community. However, if foreign technology or actions have the effect of interfering with an election, even if the intent is not conclusively proven to be deliberate, this might still fall within the scope of the E0.

In summary, while proving the act was deliberate might reinforce the rationale for invoking E0 13848, the order's application does not strictly depend on establishing deliberate intent. The focus is on whether there has been foreign interference, which can be determined by the act's impact and the involvement of foreign entities, not solely by their intentions. Therefore, the existence of interference, rather than the definitive proof of deliberate action, would be the primary driver for the potential application of sanctions under this E0.

Good intentions can result in

Big Problems

December 22, 2024

The claim from Jeff Bongiorno 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.SCRIP: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 timestomp.G!lastw
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 52 49 50 54 3A 000021f8.SCRIP:
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....us.ese. | (.

```

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.](#)

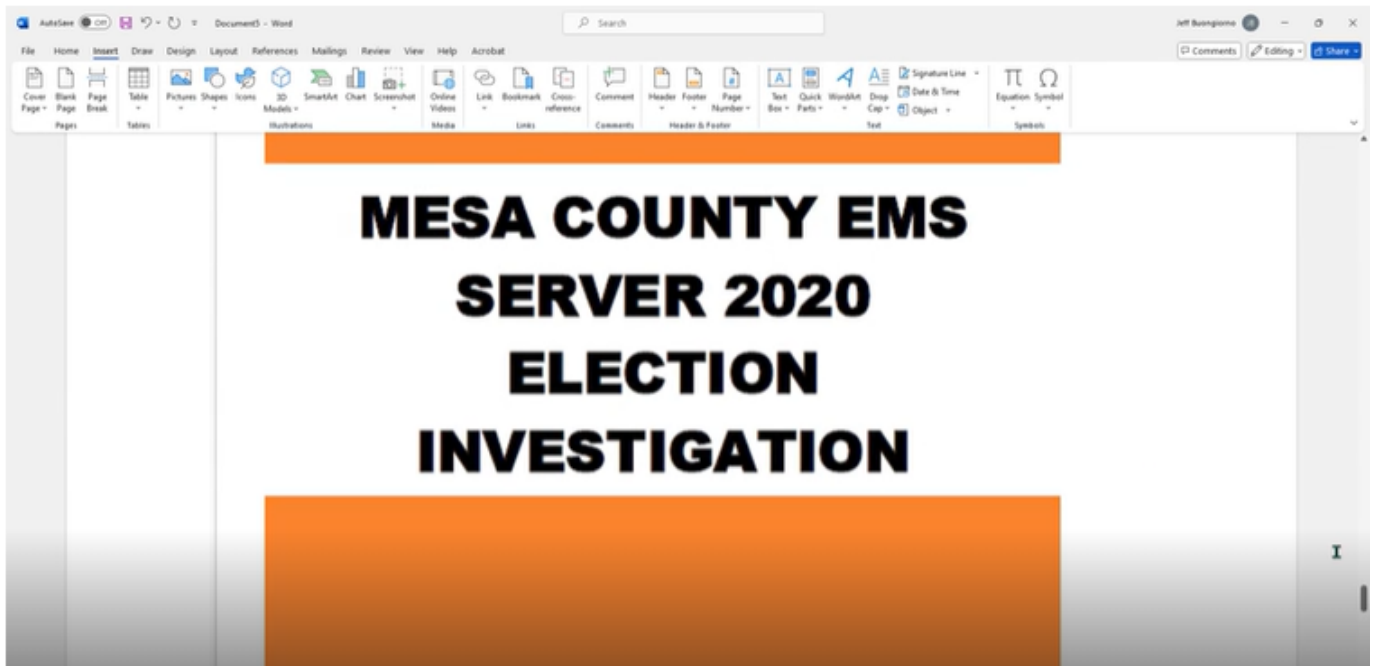
Virus definitions are benign parts of a computer virus that the antivirus engine uses in order to detect the real virus. The names of the viruses are actually there in the screen shot, but

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:



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

[UPDATE – 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”

December 22, 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 (NO_x)—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 NO_x 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

December 22, 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 an 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.”

<https://twitter.com/GovernorHobbs/status/1814323091927122113>

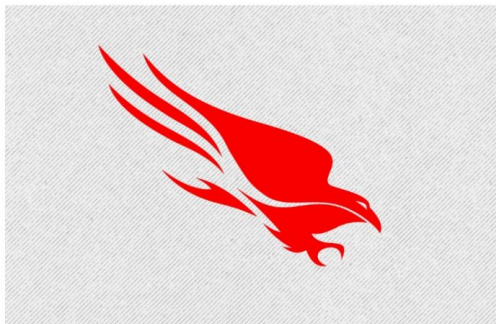
<pic.twitter.com/qFLxuYvDHV>

– Maricopa County Elections (@MaricopaVote) [July 19, 2024](#)

But wait...There's more! New update from CrowdStrike:

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 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

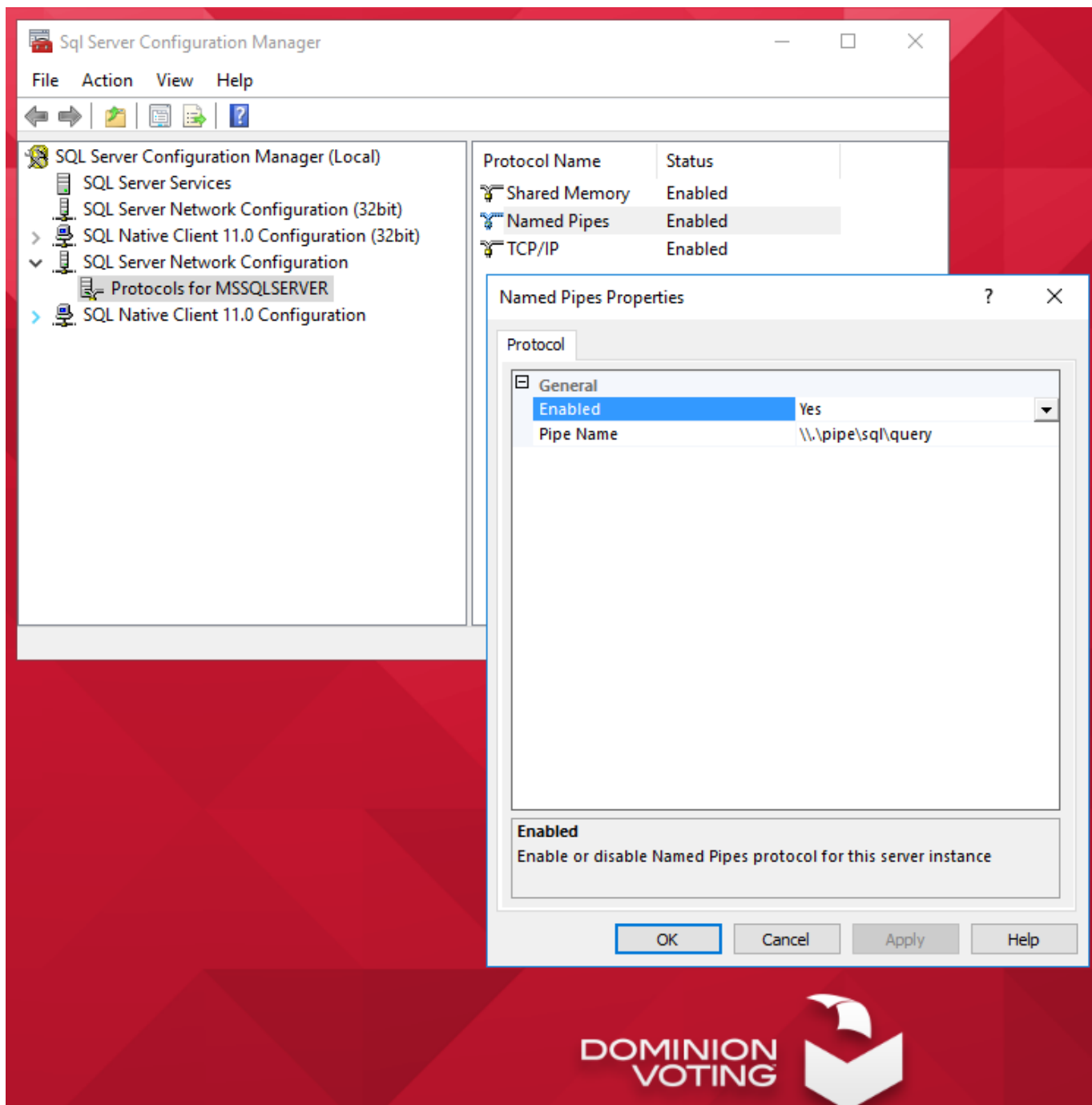
We understand how this issue occurred and we are doing a thorough root cause analysis to determine how this logic flaw occurred. This effort will be ongoing. We are committed to identifying any foundational or workflow improvements that we can make to strengthen our process. We will update our findings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



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 sheer 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 malicious developer, 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](#).