For those that say “I trust the computers”

August 21, 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

August 21, 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*

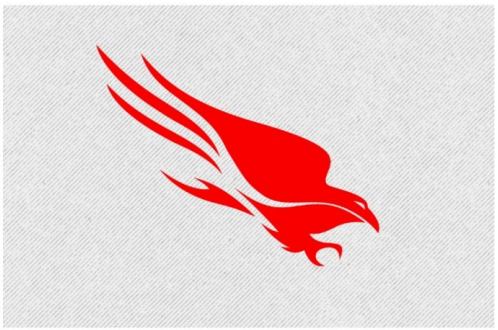
pic.twitter.com/qFLxuYvDHV

— Maricopa County Elections (@MaricopaVote) July 19, 2024

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

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.

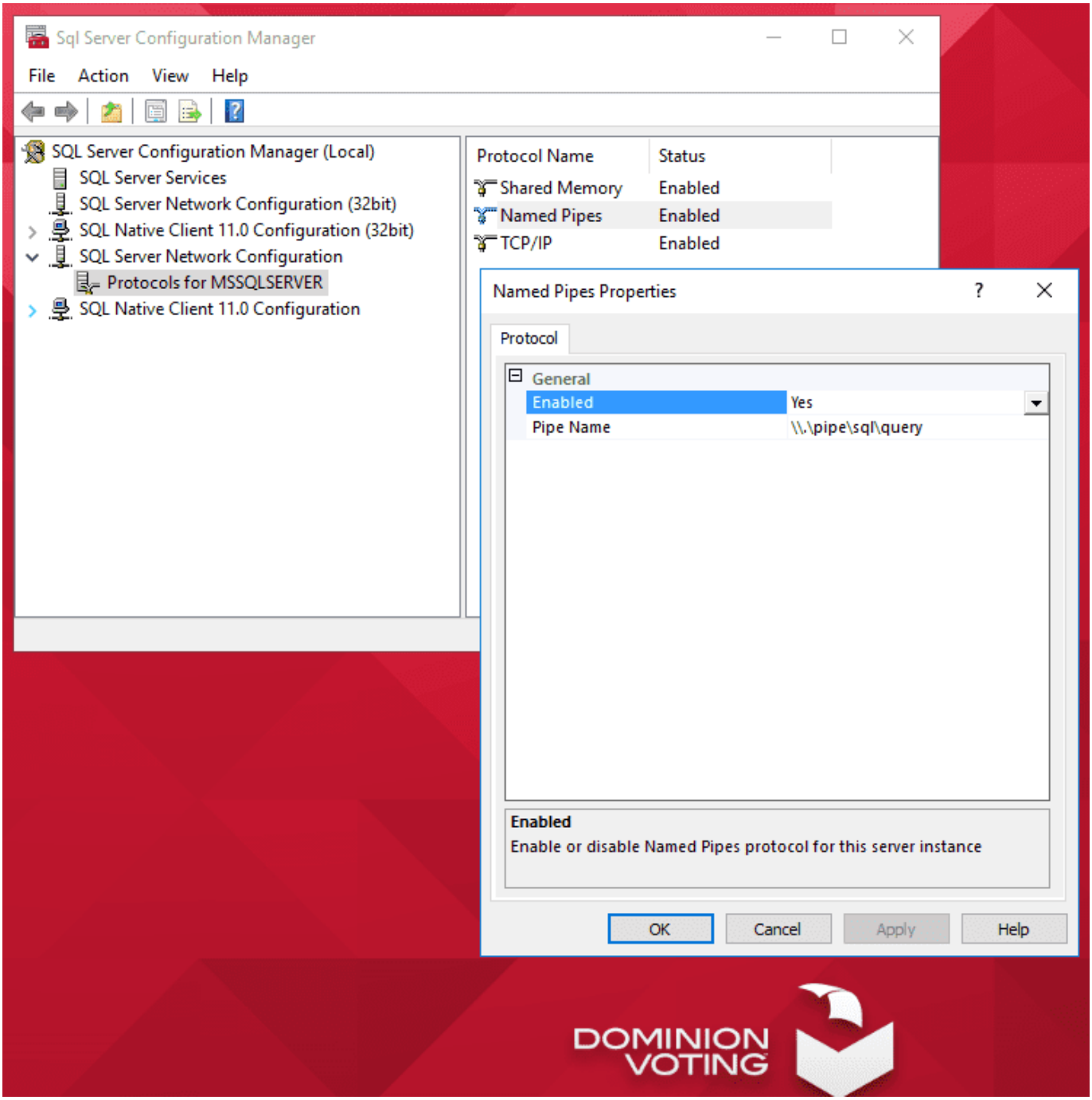
Root Cause Analysis

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/)

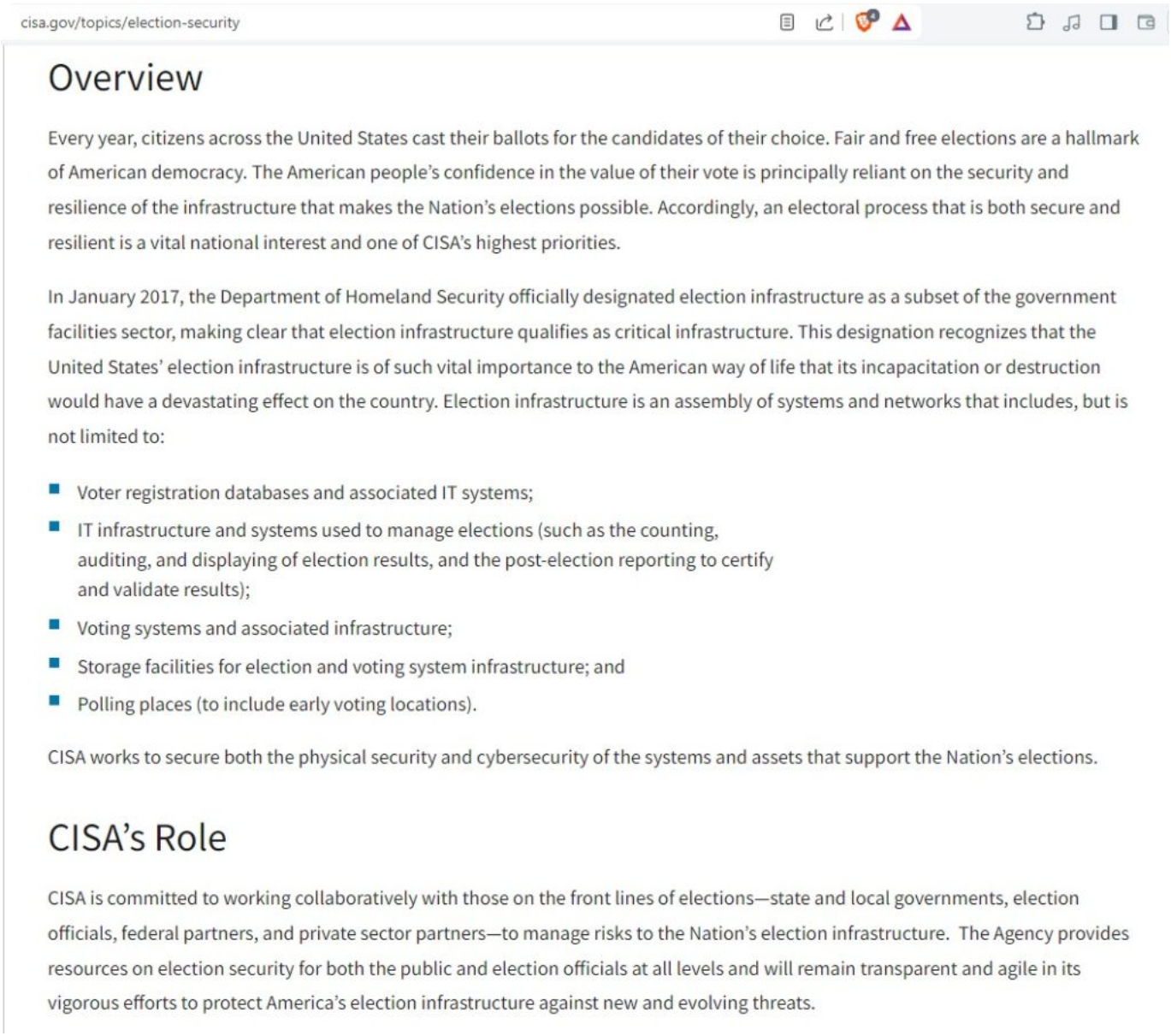
Speaking of Elections…let's not leave out Dominion just yet…

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:



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

August 21, 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.**

Bank-Your-Vote and Early Voting Scam

August 21, 2024

"Only an idiot would fall for ballot banking or early voting! Don't be that idiot! Vote ONLY on Election DAY, and vote in HUGE NUMBERS! Peacefully STAND YOUR GROUND. Do not leave until you CAST YOUR BALLOT!"

2 U.S. Code § 7 – Time of election: The Tuesday next after the 1st Monday in November, in every even numbered year, is established as the day for the election, in each of the States and Territories of the United States, of Representatives and Delegates to the Congress commencing on the 3d day of January next thereafter. (R.S. § 25; Mar. 3, 1875, ch. 130, § 6, 18 Stat. 400; June 5, 1934, ch. 390, § 2, 48 Stat. 879.)

There are two groups of people pushing Early Voting and Vote By Mail. Group 1 is benefiting from election manipulation. Group 2 has fallen for the con because they don't understand it. We can't do anything about Group 1. But we CAN educate Group 2.

How much more is your vote worth if you vote on the first day of early voting versus voting on Election Day? EXACTLY THE SAME, right? Well, exactly the same to YOU, yes. But to someone that would want to manipulate the election, you voting early is worth MUCH more to THEM. Why is that?

First, let’s identify some facts:

- If someone knew your party affiliation, they probably know how you will vote.
- If they didn’t know your affiliation or you are PND (party-not-designated, or independent), there is still an incredible amount of information that is already collected about you from your social media posts, products you buy, websites you visit, clubs you’re in, email lists you’re in, terms you search for, contents of your emails, etc. With that information, it would be easy for an algorithm to determine how you will vote.
- Notice how those committing election fraud aren’t trying to stop the voice of those pushing early voting. Why do you think that is? Think hard…

So then, if someone didn’t have access to look at the actual ballots, but wanted to build a estimate of the election results, the only other thing they would need to know is who has voted so far, right? But HOW could they monitor that? Do they follow people around and watch them drop ballots in mailboxes/dropboxes or sit and watch them go vote in person? No, of course not, they don’t need to!

Some very smart and devious people got us to pay for two systems that allow them to build a model of the election results before a single ballot is even tabulated. You’ve probably heard of and used one of these systems without even knowing. What are they?

- Mail-in Ballot Tracking – We were told that this is so we can track our mail-in ballot so we feel more CONfident in using mail-in ballots. (Did you know that CON in CON-artist stands for ‘confidence’?) The mail-in Ballot

Tracking isn't for US. It's for THEM. It's for THEM to know when we have voted and what precinct we are in. They just feed that right into their estimation without needing to look at our ballot. You might be thinking "well, they won't know when I vote, because I'm smart enough to vote in person!". Well, you aren't that smart…and here's why:

- Electronic Poll Books – We were told this was to make checking in to vote more convenient. Well, another thing it does is allow certain people to know when you vote (and of course what your voting precinct is). And they get this data in realtime as well, and they can add it to their election result model before you even finish filling out your ballot! How smart do you feel now?

So what good does a model of the election results do for someone? Well, I'm going to put on my 'BAD GUY' hat and speak to you from that perspective:

"Now that I have conned all these idiots and have a system that allows me to know what the election results are within a high likelihood, and I know what I WANT them to be, all I have to do is subtract the two, and I now exactly how many ballots need to be injected to COUNTER the real votes.

But how would I ever get them into the system? Well, that's EASY! With mail-in ballots and drop-boxes, I can just have ballot mules drop them off and nobody would know. And obviously I wouldn't have them put in just one precinct, I'd scatter them all around to stay under the radar so nobody notices. And because I already have all this data, I know exactly where to spread them out.

But this would take a lot of time to do on a large scale, wouldn't it? It definitely would. And it would be nearly impossible to do all that across a country in only one day. So,

as a bad guy, I'm going to change the voting laws to allow EARLY VOTING! That gives me plenty of time to scatter and inject the ballots. The only problem is some people procrastinate, not leaving me much time to do my magic. So, I'm going to concoct the BANK YOUR VOTE initiative to try to con the people into voting as early as possible so I have PLENTY of time to manipulate things! I might even do some things to scare people away from voting on election day or make it really inconvenient for them and channelize them to vote as early as possible! Haha, these people are so stupid, they'll buy it hook, line, and sinker.

But what do I do about the stubborn people that are on to my scam and therefore vote on election day? I've got that covered too, don't worry. I'll just push election laws that allow mail-in ballots to show up for another week after the polls close. That will give me plenty of time to do the cleanup and tie up all the loose ends, so I'm sure to get the predetermined results I want.

I love cheating elections this way, because if we ever do let the peasants have access to the ballots, they can count them to their little hearts content and they'll always get the same result! Even the county election officials wouldn't be able to catch this, so they'll be telling all their citizens that there was no manipulation in the election, lying to them for me! And my entire corrupt industry gets to make billions of dollars from these idiot taxpayers who are paying us to be able to override their will so they merely think their vote counts. Stupid people are just so easy to fool, that if I wasn't a total psychopath I might feel bad, lolol"

So how do we BREAK their control? Well, if we all VOTE IN PERSON ON ELECTION DAY, we break most of this feedback loop they created, and if they want to cheat, they have to cheat out in

the open where we can see them instead of the dark where we couldn't. This is what they did in Maricopa County AZ during the 2022 election. Yes, I know they still cheated, but at least WE CAUGHT THEM and now we have confirmation of the feedback loop. Can you imagine what's going to happen when far more people vote in person on election day that it completely crushes their ability to cheat on that kind of a large scale? VICTORY FOR THE PEOPLE! The real vote will far overwhelm the injected votes and the bad guys will have to think of some other way to cheat. If we all can spread the word fast and wide enough, we the people will finally have a massive win against the psychopath globalists.

> *"But Scott Presler, Charlie Kirk, and Lara Trump say to vote early!"*

Lara Trump has bad advisors around her. I have ZERO doubt of her integrity or intentions. I do hope she will contact me so I can walk her through this. However, Scott Presler told me directly face-to-face "Every expert has told me the same thing you're telling me, and I DON'T CARE. I'm not stopping." Why would Scott purposely mislead the people he claims to be helping? Charlie refuses to even listen to any of the experts. Isn't that foolish to ignore people that actually studied the mechanics? Why would Charlie refuse to even listen? It's bizarre at the least.

JP Sears does a **fantastic** job explaining it from a high level:

Share this video EVERYWHERE! Seriously, share it to everyone you know on every platform you can and ask every person to do the same. (and share this webpage as well, so everyone has the full detailed explanation)

If you cannot vote on election day, vote AS CLOSE TO ELECTION DAY AS POSSIBLE, and of course, IN PERSON. Remove as much time

and space between events in an election, and you will reduce the opportunities for induction of fraud.

For more details, see #RightWayVoting.