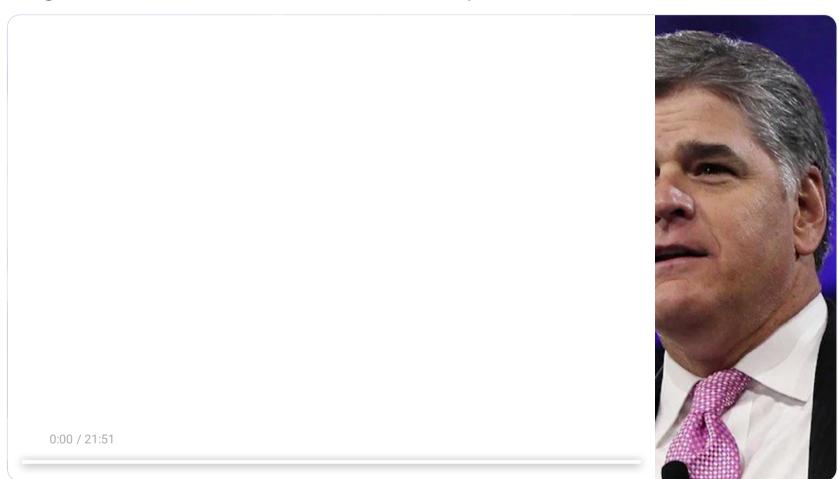
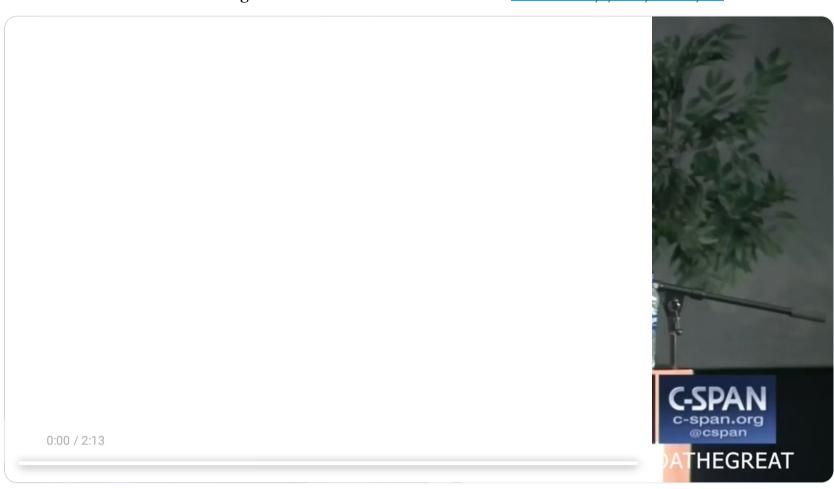


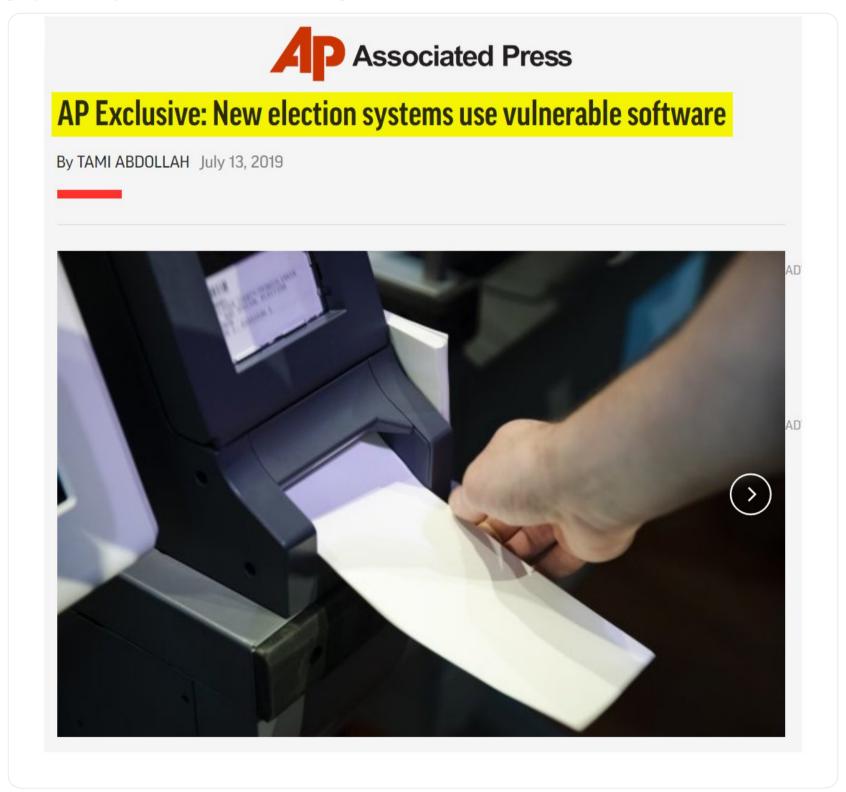
BREAKING: Explosive video surfaces of FOX News stars Tucker Carlson, Laura Ingraham, and Sean Hannity slamming Trump's "insane" voting machine fraud allegations as "absurd," "ridiculous," and "complete BS"!



#2 All electronic voting equipment can easily be hacked because all such equipment must receive programming before each election from memory cards prepared on election management systems which are computers often

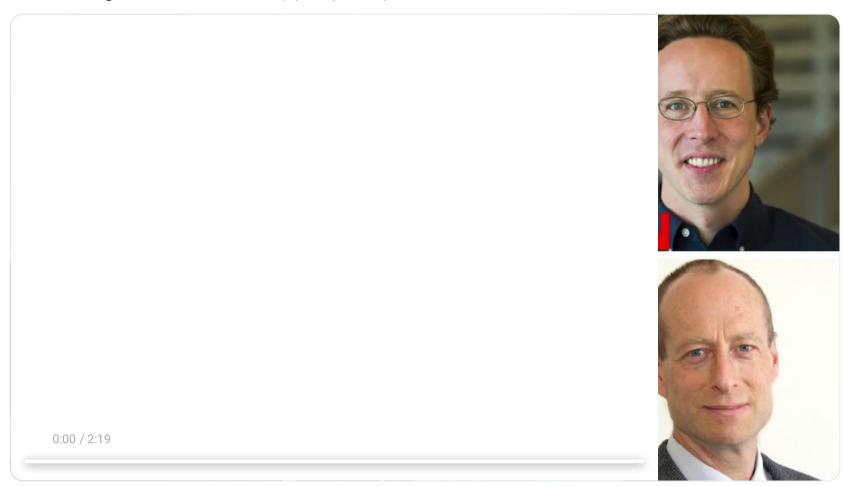


#3 In 2019, the Associated Press reported that the vast majority of 10,000 election jurisdictions nationwide, including numerous swing states, were still using Windows 7 or older operating systems to produce ballots, program voting machines, count votes, and report results.... twitter.com/i/web/status/1...



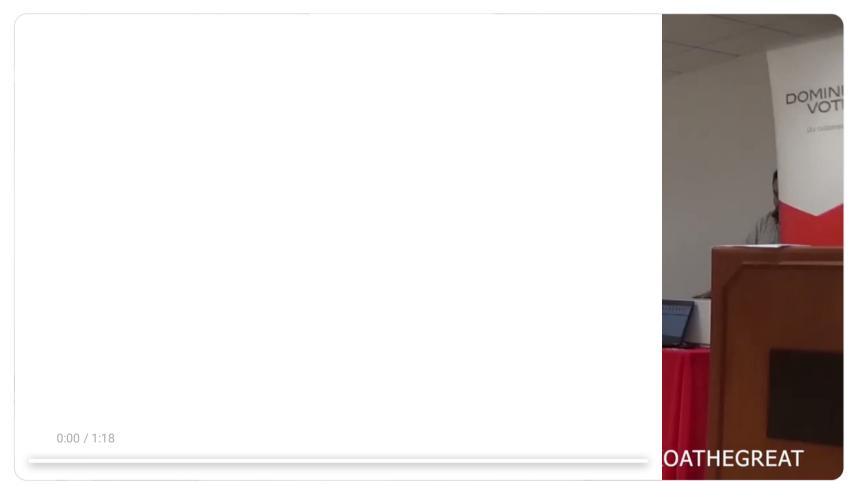
#4 Furthermore, not only are U.S. elections being programmed on computers running out-of-date software, but voting machine manufacturers have also installed remote-access software and wireless modems connecting voting

NBC News reported ten... twitter.com/i/web/status/1...



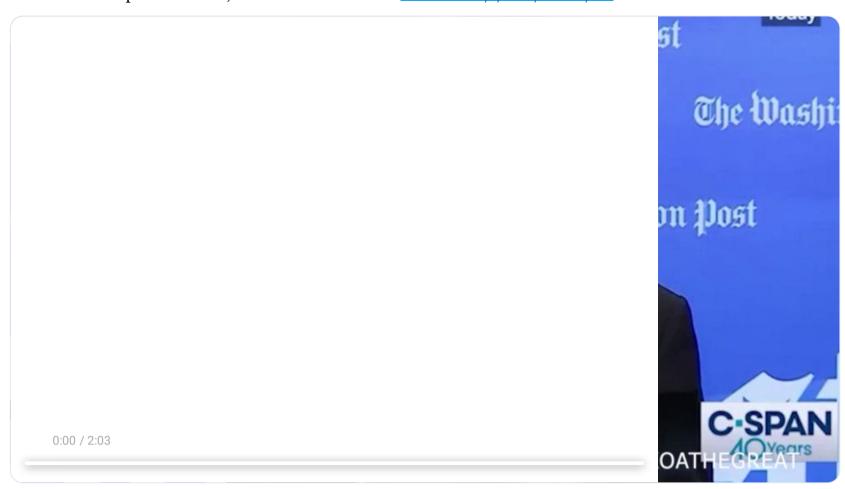
#5 Dominion Voting Systems, the second-largest U.S. election machine vendor, which has given public presentations acknowledging their use of modems in their voting machines, was also discovered to be running remote-access software during the 2020 election:

In Georgia, 20-year... twitter.com/i/web/status/1...



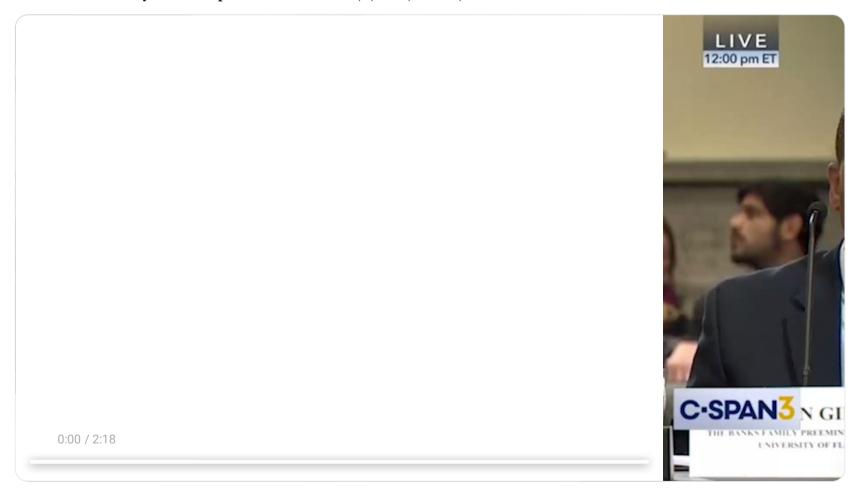
#6 This isn't a problem exclusive to elections — all computers are hackable — and that is why election security experts have always recommended the use of hand-marked paper ballots and rigorous post-election audits.

This also isn't a partisan issue; both Democrats and... twitter.com/i/web/status/1...



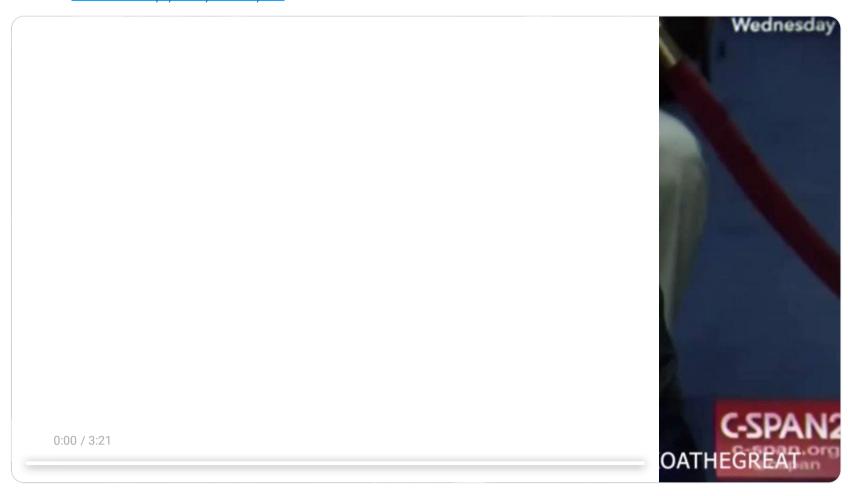
#7 Professor Matt Blaze of Georgetown University's Computer Science Department provided testimony on the vulnerabilities of the United States' election system during a congressional hearing titled "2020 Election Security" on January 9, 2020:

"I come here today as a computer... twitter.com/i/web/status/1...



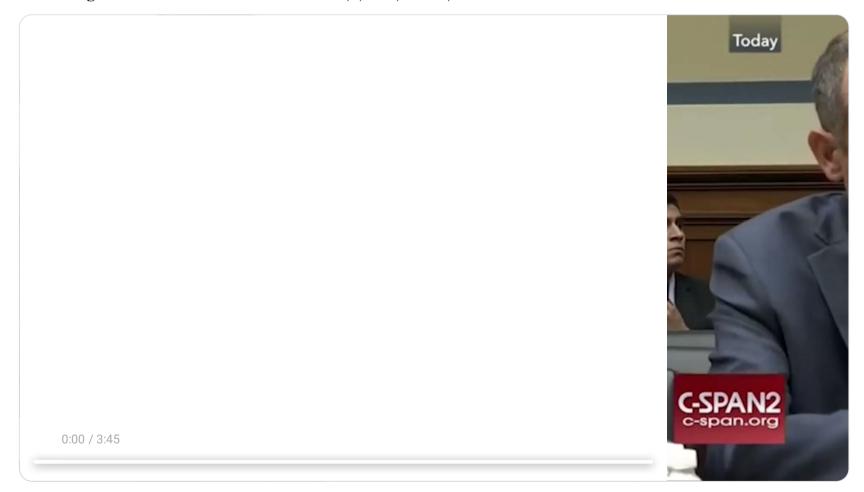
#8 Professor J. Alex Halderman of the University of Michigan's Computer Science Department provided testimony on the vulnerabilities of the United States' election system during a congressional hearing titled "Russian Interference in U.S. Elections" on June 21, 2017:

"I'm a... twitter.com/i/web/status/1...



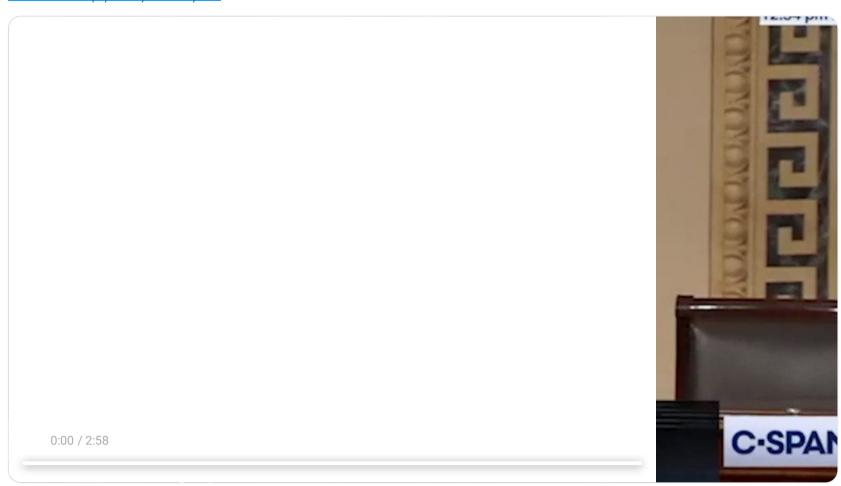
#9 Professor Andrew Appel of Princeton University's Computer Science Department provided testimony on the vulnerabilities of the United States' election system during a congressional hearing titled "Election Cybersecurity" on September 28, 2016:

"Installing new software is how... twitter.com/i/web/status/1...



#10 Senator Ron Wyden provided testimony on the vulnerabilities of the United States' election system during a congressional hearing titled "Election Security" on July 15, 2019:

"The vast majority of ten thousand election jurisdictions nationwide use election management systems...



#11 Senator Elizabeth Warren published an article on her website on the vulnerabilities of the United States' election system titled "Strengthening Our Democracy" on June 25, 2019:

"The harsh truth is that our elections are extremely vulnerable to attack: Forty-two states use... twitter.com/i/web/status/1...

#12 In Dec. 2019, Senators Elizabeth Warren, Amy Klobuchar, Ron Wyden, and Mark Pocan sent letters to the three private equity firms that own the largest voting machine companies in the US expressing their concern about the industry's "vulnerabilities" and "lack of transparency."... twitter.com/i/web/status/1...

#13 Following Hillary Clinton's defeat in the 2016 election, the corporate media dedicated the next four years to writing hundreds of articles about the extent to which the United States' election system is online, compromised, and vulnerable to hackers.



Hacking America's Computerized Voting System

110 Articles Affirm America's Computerized Voting System Is Online, Compromised, and Vulnerable To Hackers: Documented, Linked, and Quoted

https://kanekoa.substack.com/p/110-articles-affirm-americas-computerized

#14 The Guardian: Voting machine password hacks as easy as 'abcde' (April 15, 2015)

"Touchscreen WinVote voting machines used in numerous elections between 2002 and 2014 used "abcde" and "admin" as passwords and could easily have been hacked from the parking lot outside the... twitter.com/i/web/status/1...

#15 New York Times: Millions of Voter Records Posted, and Some Fear Hacker Field Day (Dec. 30, 2015)

#16 Wired: America's Electronic Voting Machines Are Scarily Easy Targets (Aug. 2, 2016)

"They are old, buggy, and insecure. If someone wanted to mess with the US election, these machines would be an easy way in. Most of these machines are running Windows XP, for which Microsoft...

twitter.com/i/web/status/1...

#17 Politico: How to Hack an Election in 7 Minutes (Aug. 5, 2016)

"Princeton professor Andrew Appel decided to hack into a voting machine... He summoned a graduate student named Alex Halderman, who could pick the machine's lock in seven seconds. Clutching a screwdriver, he deftly... twitter.com/i/web/status/1...

#18 CBS: Hacker demonstrates how voting machines can be compromised (Aug. 10, 2016)

"Concerns are growing over the possibility of a rigged presidential election. Roughly 70 percent of states in the U.S. use some form of electronic voting. Hackers told CBS News that problems with... twitter.com/i/web/status/1...

#19 ABC News: Yes, It's Possible to Hack the Election (Aug. 19, 2016)

"Slight meddling in some swing precincts in swing states could tip the scales. If it's a computer, it can be hacked... if sophisticated hackers want to get into any computer or electronic device, even one that... twitter.com/i/web/status/1...

#20 The Atlantic: How Electronic Voting Could Undermine the Election (Aug. 29, 2016)

"...computer-security experts think electronic voting is a very, very bad idea. For years, security researchers and academics have urged election officials to hold off on adopting electronic... twitter.com/i/web/status/1...

#21 FOX: Princeton Professor demonstrates how to hack a voting machine (Sept. 18, 2016)

"I have demonstrated how to hack the AVC Advantage voting machines that we use in New Jersey... The touch screen voting machine, the type used in about ten states, can be tampered with... By... twitter.com/i/web/status/1...

#22 Fortune: Watch This Security Researcher Hack a Voting Machine (Nov. 4, 2016)

"Researchers at cybersecurity startup Cylance said they were able to hack into the Sequoia AVC Edge Mk1, used to count votes in states including California, Florida, and New Jersey, and change the... twitter.com/i/web/status/1...

#23 Vox: Here's how hackers can wreak havoc on Election Day (Nov. 7, 2016)

"Voting machines are old and vulnerable, and voter databases are connected to the internet. Many voting machines are running software that's over a decade old, like Windows XP, which Microsoft hasn't... twitter.com/i/web/status/1...

#24 PBS: Here's how hackers might mess with electronic voting on Election Day (Nov. 8, 2016)

"...vulnerabilities in electronic ballots, make hacking a major possibility on Election Day... Five states — New

y Tweet **f** Share

#25 Slate: Now Is the Time to Replace Our Decrepit Voting Machines (Nov. 17, 2016)

"With antiquated voting devices at the end of their projected lifespans still in widespread use across the country, the U.S. is facing an impending crisis in which our most basic election... twitter.com/i/web/status/1...

#26 PBS: Recounts or no, U.S. elections are still vulnerable to hacking (Dec. 26, 2016)

"Pennsylvania is one of 11 states where the majority of voters use antiquated machines that store votes electronically, without printed ballots or other paper-based backups that could be used... twitter.com/i/web/status/1...

#27 Politico: U.S. elections are more vulnerable than ever to hacking (Dec. 29, 2016)

"America's political system will remain vulnerable to cyberattacks and infiltration from foreign and domestic enemies unless the government plugs major holes and commits millions of dollars in... twitter.com/i/web/status/1...

#28 ScientificAmerican: Our Voting System Is Hackable by Foreign Powers (March 1, 2017)

"It is entirely possible for an adversary to hack American computerized voting systems directly and select the next commander in chief. A dedicated group of technically sophisticated... twitter.com/i/web/status/1...

#29 Politico: Will the Georgia Special Election Get Hacked? (June 14, 2017)

"A 29-year-old former cybersecurity researcher with the federal government's Oak Ridge National Laboratory in Tennessee, Lamb, who now works for a private internet security firm in Georgia, wanted to... twitter.com/i/web/status/1...

#30 NPR: If Voting Machines Were Hacked, Would Anyone Know? (June 14, 2017)

"U.S. officials are increasingly worried about how vulnerable American elections really are... But even if most voting machines aren't connected to the Internet, says cybersecurity expert Jeremy Epstein,... twitter.com/i/web/status/1...

#31 HuffPost: Good News For Russia: 15 States Use Easily Hackable Voting Machines (July 17, 2017)

"Touch-screen machines can be programmed to change votes and are nearly impossible to audit, computer experts say... Manufacturers like Diebold touted the touch screens, known as... twitter.com/i/web/status/1...

#32 CNET: Defcon hackers find it's very easy to break voting machines (July 30, 2017)

"When the password for a voting machine is "abcde" and can't be changed, the integrity of our democracy might be in trouble. The Advanced Voting Solutions WinVote machine, dubbed "America's... twitter.com/i/web/status/1...

#33 CNN: We watched hackers break into voting machines (Aug. 11, 2017)

"These are supposed to be the latest machines, they're still used in elections, and they're running ancient software. I think that if somebody wanted to, it would be pretty easy to fake an election...So if you...

y Tweet **f** Share

#34 The Intercept: The U.S. Election System Remains Deeply Vulnerable (Oct. 3, 2017)

"The Harvard report, titled "Voter Identity Theft: Submitting Changes to Voter Registrations Online to Disrupt Elections," concludes that online attackers can alter voter registration... twitter.com/i/web/status/1...

#35 New York Times: The Myth of the Hacker-Proof Voting Machine (Feb. 2, 2018)

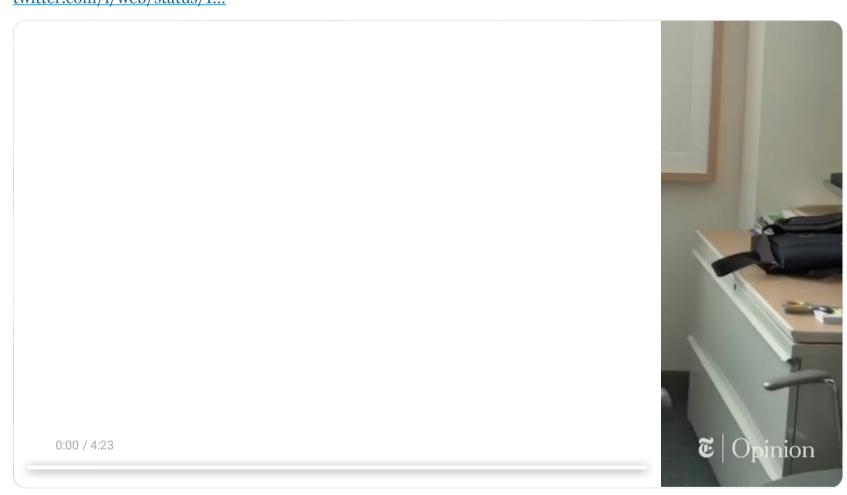
"Examining the election-management computer at the county's office — the machine used to tally official election results and, in many counties, to program voting machines — they found that... twitter.com/i/web/status/1...

#36 Slate: America's Voting Systems Are Highly Vulnerable to Hackers (Feb. 22, 2018)

"Did Russia shift the election's outcome by hacking registration rolls or voting machines? The fact is that it's impossible to say. In September, the Department of Homeland Security informed... twitter.com/i/web/status/1...

#37 New York Times: I Hacked an Election. So Can the Russians. (April 5, 2018)

"After the chaos of the 2000 election, we were promised a modern and dependable way to vote, Halderman says in the video. "I'm here to tell you that the electronic voting machines Americans got to... twitter.com/i/web/status/1...



#38 The New Yorker: America Continues To Ignore Risks of Election Hacking (April 18, 2018)

"America's voting systems are hackable in all kinds of ways. As a case in point, in 2016, the Election Assistance Commission, the bipartisan federal agency that certifies the integrity of... twitter.com/i/web/status/1...

#39 Reuters: Old voting machines stir concerns among U.S. officials (May 31, 2018)

"In 14 of the 40 most competitive races, Americans will cast ballots on voting machines that do not provide a paper trail to audit voters' intentions if a close election is questioned... These... twitter.com/i/web/status/1...

#40 Axios: There's more than one way to hack an election (July 2, 2018)

(which the voter registration process produces), voter records at polling places (known as poll... twitter.com/i/web/status/1...

#41 Newsweek: Election Hacking: Voting-Machine Supplier Admits It Used Hackable Software Despite Past Denials (July 17, 2018)

"One of the country's largest voting machine makers has admitted in a letter to a U.S. senator that some of its past election-management systems had... twitter.com/i/web/status/1...

#42 Salon: Remote-access allowed: Voting machine company admits installing vulnerable software (July 20, 2018)

"A letter sent to Congress reveals that, between 2000 and 2006, one of America's top voting machine companies installed remote-access software in their products that... twitter.com/i/web/status/1...

#43 BBC: Hacking the US mid-terms? It's child's play (Aug. 11, 2018)

"Bianca Lewis, 11, has many hobbies. She likes Barbie, video games, fencing, singing... and hacking the infrastructure behind the world's most powerful democracy...She's taking part in a competition organized by... twitter.com/i/web/status/1...

#44 PBS: An 11-year-old changed election results on a replica Florida state website in under 10 minutes (Aug. 12, 2018)

"An 11-year-old boy on Friday was able to hack into a replica of the Florida state election website and change voting results found there in under 10 minutes... twitter.com/i/web/status/1...

#45 The Guardian: Why US elections remain 'dangerously vulnerable' to cyber-attacks (Aug. 13, 2018)

"By mid-evening, Jon Ossoff, the leading Democrat, had 50.3% of the vote, enough to win outright without the need for a run-off against his closest Republican challenger. Then... twitter.com/i/web/status/1...

#46 The Guardian: Kids at hacking conference show how easily US elections could be sabotaged (Aug. 22, 2018)

"The risk of a hacker casting the validity of an election into question through one of any number of other entry points is huge, and the actual difficulty of such an... twitter.com/i/web/status/1...

#47 CBS: Why voting machines in the U.S. are easy targets for hackers (Sept. 19, 2018)

"Tens of thousands of voting machines in the United States are vulnerable to hacking. They have been successfully dismantled and attacked by security researchers for years to demonstrate their... twitter.com/i/web/status/1...

#48 New York Times: The Crisis of Election Security (Sept. 26, 2018)

The Illinois intruders had quietly breached the network in June and spent weeks conducting reconnaissance. After alighting on the state's voter registration database, they downloaded information on hundreds of... twitter.com/i/web/status/1...

#49 Politico: Attack on commonly used voting machine could tip an election (Sept. 27, 2018)

Follow Us on Twitter!

y Tweet **f** Share

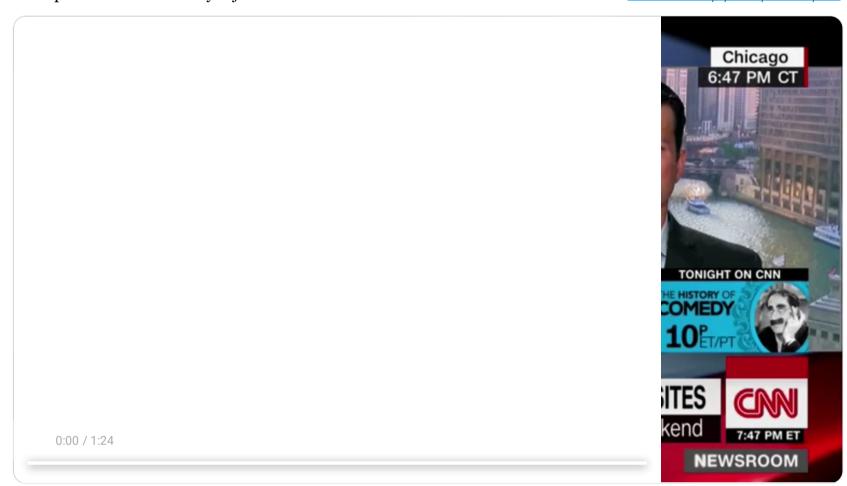
"A malicious hacker could alter the outcome of a U.S. presidential election by taking advantage of numerous flaws in one model of vote-tabulating machine used in 26 states, cybersecurity... twitter.com/i/web/status/1...

#50 WSJ: Voting Machine Used in Half of U.S. Is Vulnerable to Attack (Sept. 27, 2018)

"Election machines used in more than half of U.S. states carry a flaw disclosed more than a decade ago that makes them vulnerable to a cyberattack, according to a report to be delivered... twitter.com/i/web/status/1...

#51 CNN: Hackers Bring Stark Warning About Election Security (Sept. 27, 2018)

"The vulnerabilities in America's voting systems are "staggering," a group representing hackers warned lawmakers on Capitol Hill on Thursday – just over a month before the midterm elections. The... twitter.com/i/web/status/1...



#52 Wired: Voting Machines Are Still Absurdly Vulnerable to Attacks (Sept. 28, 2018)

"The report details vulnerabilities in seven models of voting machines and vote counters, found during the DefCon security conference's Voting Village event. All of the models are in active use... twitter.com/i/web/status/1...

#53 Slate: Can Paper Ballots Save Our Democracy? (Oct. 10, 2018)

"The machine was an AccuVote TSX used in 18 states, some with the same software version. Attackers don't need physical access--we showed how malicious code can spread from the election office when officials program... twitter.com/i/web/status/1...

#54 New York Times: America's Elections Could Be Hacked. Go Vote Anyway. (Oct. 19, 2018)

"In April, the nation's top voting machine manufacturer told Senator Ron Wyden of Oregon that it had installed remote-access software on election-management systems that it sold from 2000 to... twitter.com/i/web/status/1...

#55 Vox: The hacking threat to the midterms is huge. (Oct. 25, 2018)

"On a scale of 1 to 10, with 10 being the Pentagon's [security measures], elections have probably moved from a 2 to a 3... They laid out a number of scenarios that could exploit vulnerable election... twitter.com/i/web/status/1...

#56 Scientific American: The Vulnerabilities of Our Voting Machines (Nov. 1, 2018)

"This just isn't a good idea to have elections be conducted by, essentially, black box technology."...The voting machines themselves have received much, much, much less scrutiny post-2016 from...

twitter.com/i/web/status/1...

#57 Salon: Philly ignores cybersecurity and disability access in voting system selection (Feb. 16, 2019)

"According to computer science professor Richard DeMillo of Georgia Tech, the barcodes also can be manipulated to instruct the scanners to flip votes. Adding insult to... twitter.com/i/web/status/1...

#58 Politico: State election officials opt for 2020 voting machines vulnerable to hacking (March 1, 2019)

"Security experts warn, however, that hackers could still manipulate the barcodes without voters noticing. The National Academies of Sciences, Engineering, and Medicine has... twitter.com/i/web/status/1...

#59 TechCrunch: Senators demand to know why election vendors still sell voting machines with 'known vulnerabilities' (March 27, 2019)

"The letter, sent Wednesday, calls on election equipment makers ES&S, Dominion Voting, and Hart InterCivic to explain why they continue to sell... twitter.com/i/web/status/1...

#60 Salon: New "hybrid" voting system can change paper ballot after it's been cast (March 28, 2019)

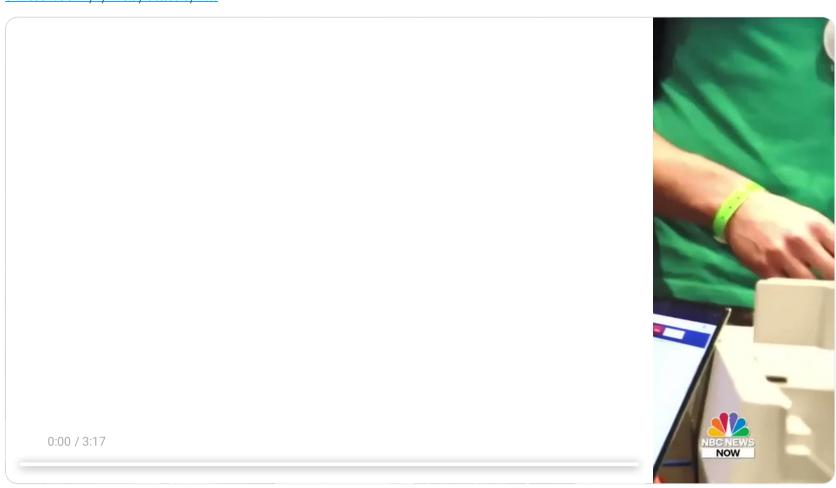
"Unfortunately, there is no universal definition of "paper ballot," which has enabled vendors and their surrogates to characterize machine-marked paper printouts from hackable... twitter.com/i/web/status/1...

#61 Vice: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials (Aug. 8, 2019)

"The top voting machine company in the country insists that its election systems are never connected to the internet. But researchers found 35 of the systems have been... twitter.com/i/web/status/1...

#62 NBC News: How Hackers Can Target Voting Machines (Aug. 12, 2019)

"They had assembled some of the most common voting machines in the country, both systems on the front-end that you and I use to register our vote and the back-end tabulators and so forth that you feed a paper...



#63 MIT Technology Review: 16 million Americans will vote on hackable paperless machines (Aug. 13, 2019)

"Despite the obvious risk and years of warnings, at least eight American states and 16 million American voters will use completely paperless machines in the 2020 US... twitter.com/i/web/status/1...

#64 Salon: Hackers can easily break into voting machines used across the U.S. (Aug. 14, 2019)

"Voting machines used in states across the United States were easily penetrated by hackers at the Def Con conference in Las Vegas on Friday...A video published by CNN shows a hacker... twitter.com/i/web/status/1...

#65 FOX News: Election machine keys are on the Internet, hackers say (Aug. 22, 2019)

"I may have the keys to open voting machines used in states across the country, and that is not a good thing. I am not an election official. I am not a voting machine expert, operator, or... twitter.com/i/web/status/1...

#66 The Hill: Voting machines pose a greater threat to our elections than foreign agents (Oct. 2, 2019)

"In 2017, the largest U.S. voting machine vendor, ES&S, exposed encrypted employee passwords online. Using those passwords, hackers could have planted malware on the company's... twitter.com/i/web/status/1...

#67 NPR: Cyber Experts Warn Of Vulnerabilities Facing 2020 Election Machines (Sept. 4, 2019)

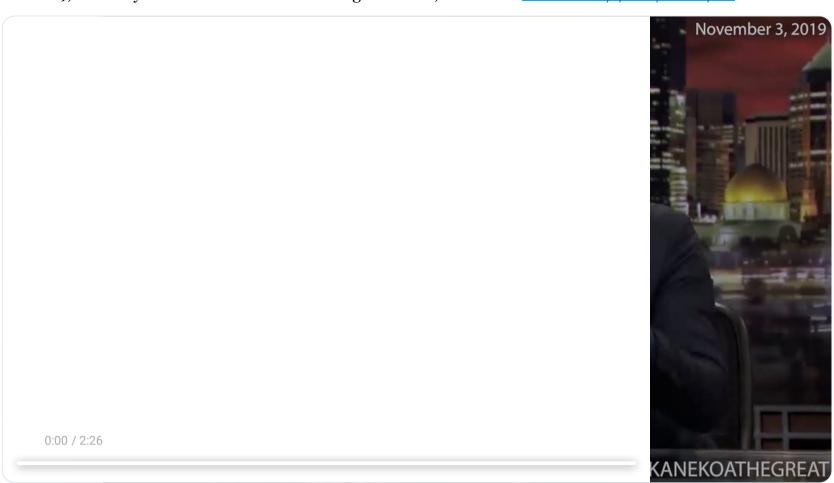
"The machine he's investigating is a ballot-marking device used to help people with physical impairments or language barriers vote, and it's running a version of Windows that is more... twitter.com/i/web/status/1...

#68 Wired: Some Voting Machines Still Have Decade-Old Vulnerabilities (Sept. 26, 2019)

"Today's report highlights detailed vulnerability findings related to six models of voting machines, most of which are currently in use. That includes the ES&S AutoMARK, used in 28 states in... twitter.com/i/web/status/1...

#69 John Oliver Breaks Down Faulty Voting Machine Security on Last Week Tonight (Nov. 3, 2019)

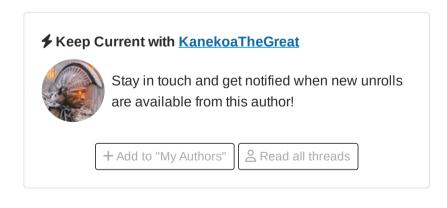
minutes), how easy it is to find unattended voting machines, and how... twitter.com/i/web/status/1...

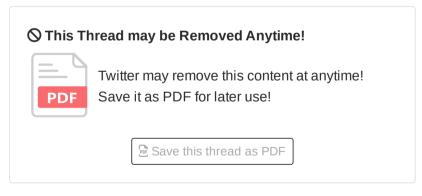


• • •

Missing some Tweet in this thread? You can try to force a refresh

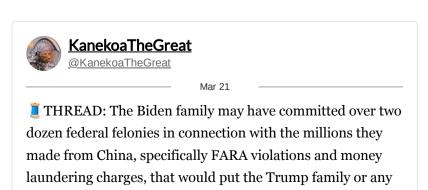




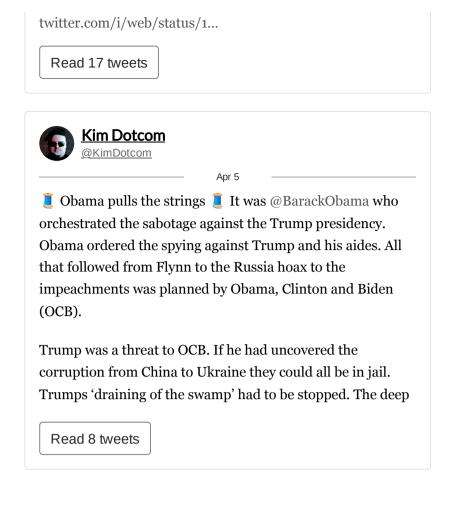


People who liked this thread also liked...

ordinary citizen behind bars for decades. For...





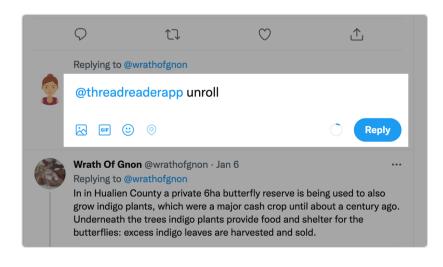




Read 16 tweets

they made it cost the US economy \$13 dollars. Quite the

Try unrolling a thread yourself!



- 1. Follow <u>@ThreadReaderApp</u> to mention us!
- 2. From a Twitter thread mention us with a keyword "unroll"

@threadreaderapp unroll

Practice here first or read more on our help page!

KanekoaTheGreat @KanekoaTheGreat Apr 20 Joe Biden falsely claimed that Hunter's laptop, which contains evidence of hundreds of crimes, was "Russian disinformation" just weeks before the 2020 election. The United States, led by President Biden, is now engaged in a proxy war with nuclear-armed Russia. Read 5 tweets	KanekoaTheGreat @KanekoaTheGreat Apr 18 THREAD: Tucker Carlson's Interview with Elon Musk starts with OpenAI's transition from the non-profit @elonmusk founded to ethically distribute the power of artificial intelligence to a closed-source for-profit partnered with Microsoft.
	KanekoaTheGreat @KanekoaTheGreat Apr 17 Washington Post reporter @joshrogin tells @glennbeck that the Pentagon's leaked documents reveal China's hypersonic glide missiles defeat our aircraft carriers and missile defense systems: "We spent thirty years building aircraft carriers and missile defense, and the Chinese twitter.com/i/web/status/1
Read 4 tweets	Read 7 tweets
KanekoaTheGreat @KanekoaTheGreat #1 @JoeRogan is shocked by a study that found ten rivers in Asia and Africa cause up to 95% of ocean plastic pollution: "If we stop using plastic straws, we're not going to put a f*ckin dent in it unless they do. We're not even close to #1. We're not even close to #6." #2 A 2017 study published in Environmental Science & Technology found that ten rivers are responsible for up to 95% of the plastic dumped into oceans. 1. Yangtze 2. Indus 3.	KanekoaTheGreat @KanekoaTheGreat Apr 3 THREAD: Joe Rogan and Michael Shellenberger discuss the censorship-industrial complex, the Twitter Files, the Biden laptop, the Election Integrity Project, and the US government officials, contractors, and NGOs using disinformation and propaganda against the American people twitter.com/i/web/status/1



Read 18 tweets

Read 6 tweets



Did Thread Reader help you today?

Support us! We are indie developers!

This site is made by just two indie developers on a laptop doing marketing, support and development! Read more about the story.

Become a Premium Member (\$3/month or \$30/year) and get exclusive features!



Don't want to be a Premium member but still want to support us?

Make a small donation by buying us coffee (\$5) or help with server cost (\$10)

P Donate via Paypal

Or Donate anonymously using crypto!

Ethereum

0xfe58350B80634f60Fa6Dc149a72b4DFbc17D341E



Bitcoin

3ATGMxNzCUFzxpMCHL5sWSt4DVtS8UqXpi



♥ ♥ Thank you for your support! ♥ ♥

9

Help | About | TOS | Privacy | Twitter Files