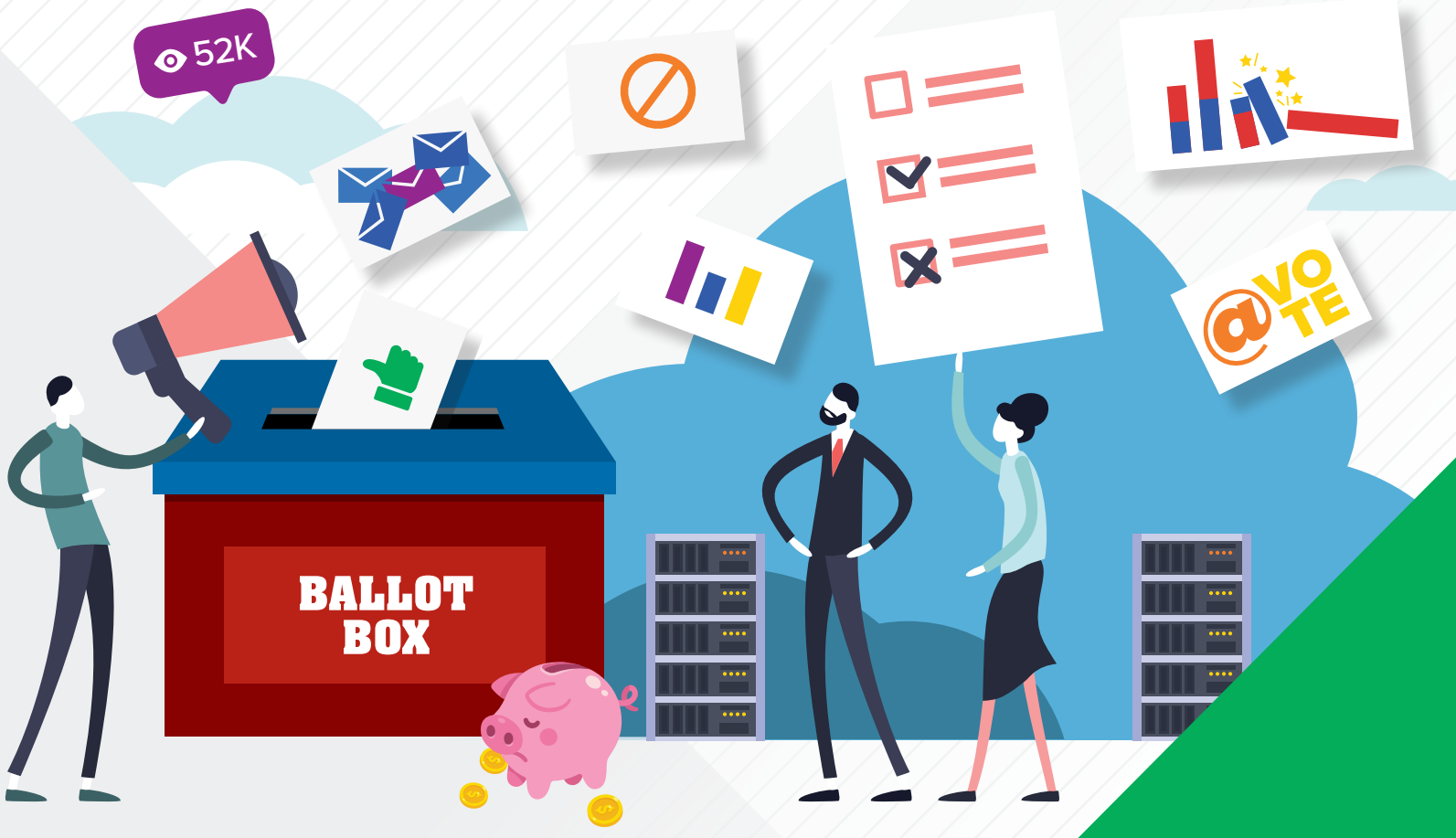
www.expel.io

The Election Supply Chain:
Where and how elections can be compromised

(and what *we* can do about it)



expel®

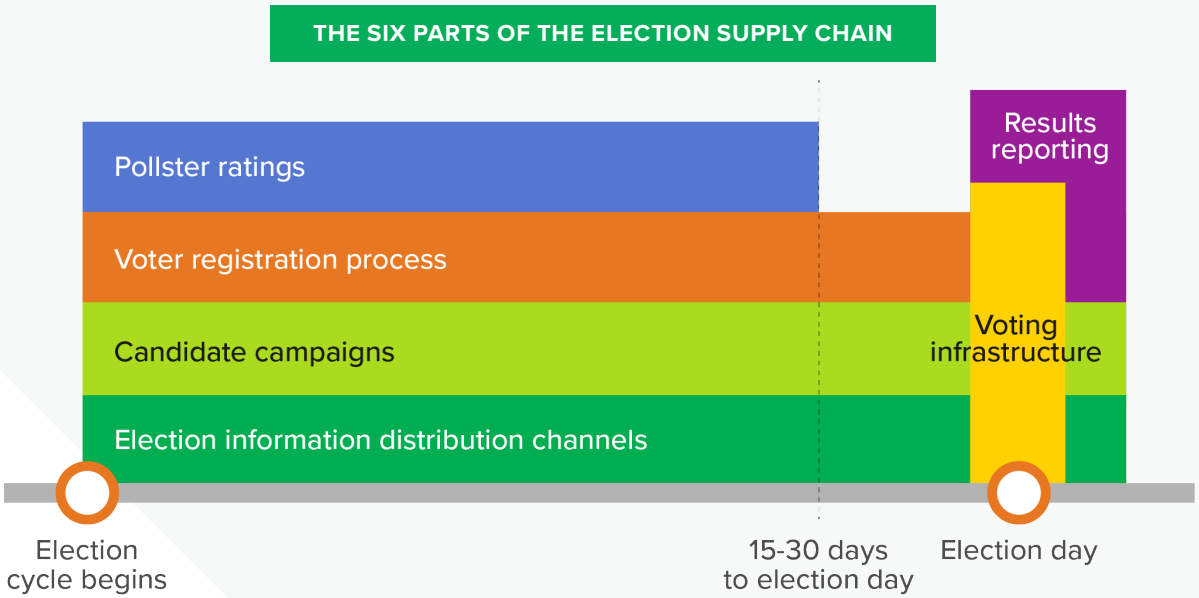
When you think about elections, most people think about that moment when you show up and cast your ballot. Think about election security and you're probably wondering just how secure that voting machine is.

But the system is more complex than that—**election security isn't about securing a single machine**. Consider voter registration efforts and election rolls or all of the information voters have digested leading up to voting day that have influenced their decisions. And don't forget what happens *after* you cast your vote and how the results are tallied.

To really understand election security you've got to consider the entire supply chain. There are plenty of opportunities for bad actors to influence votes and voters. And the adversary can be lurking almost anywhere, whether that's at a polling place or behind a Twitter account.

There are six distinct parts of the election supply chain (*see below*) and each has the potential to be compromised at different times (and in different ways) during the election cycle.

The potential for election compromise starts long before Election Day. We're going to look at potential points of compromise and how a crafty attacker could "hack" each piece along the chain. We also offer up ideas about how public and private sector organizations—even individual, well-informed citizens who are planning to vote—can better protect our elections from attacks.



Contents

1

Election information distribution channels

AT A GLANCE

Attackers become influencers using social media bots, fake photos and videos, and paid ads.

WHEN IT HAPPENS

- ELECTION CYCLE BEGINS
- ELECTION DAY
- AND BEYOND...

Why it matters

Say "election security" and the ballot box is probably the first thing that comes to mind. But long before a voter drops their ballot in the box, attackers are trying to hack their brains by compromising the information they consume to make their decisions.

Information about candidates, campaigns and issues is available everywhere you turn—from Twitter to the nightly news to your Facebook feed. The problem? Publishing and promoting content is so easy to do these days that anyone can be an influencer whether they're qualified to be one or not. In fact, political misinformation is so rampant that ***The New York Times*** asked its readers to send in examples of it...and they received over **4,000 submissions!**

HOW COMPROMISE HAPPENS

ATTACKER OBJECTIVE

Push false information to influence voters

HOW IT COULD HAPPEN AND REAL-WORLD EXAMPLES

Social media bots (or lots of people)

As much as we call them "bots" they're actually real people actively working to push specific messages. The Internet Research Agency has been implicated in extensive election meddling in the 2016 election.

Fake photos and videos

A video of U.S. House Speaker Nancy Pelosi was doctored to make it seem as though she was drunk and slurring her speech. The manipulated video was shared by thousands on social media.

Paid advertising

The IRA not only used bot accounts to push specific narratives, they also used ads to target certain individuals. Facebook released hundreds of ads that were paid for by outside interests to push different agendas around the time of the 2016 election.

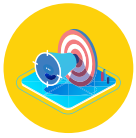
The impact

Whether it's deceptive claims about candidates or poorly labeled ads, all the election-related misinformation that's floating around out there makes it tough for voters to separate fact from fiction. The onus is on each voter to figure out the truth about candidates, campaigns and the issues they care about, and to be their own fact checker.

Why it's hard to fix

The same reasons why people love to use social media are the reasons that make it so hard to fix. It's cheap, anonymous and easy to reach hundreds of thousands of people. Information (real or fake) can travel like wildfire and it's highly dispersed.

HOW WE CAN PROTECT THE PROCESS



	VOTERS	CAMPAIGNS	FEDERAL GOVERNMENT
BEFORE **NOV 2020**	Fact check information before you believe it using sites like **snopes.com** (*and definitely before you share it*).	Actively call out misinformation, potentially through your own advertising campaigns.	Enforce laws that require campaigns to disclose when they buy ads on social media sites.
BEFORE **2024**	Ask social media companies to actively supply information to help with the fact checking process rather than relying on third-party sites.	Work with social media companies to get misinformation campaigns taken down before they spread.	Consider updating the **Communications Act of 1934** to empower all media companies to address information operations in political ads.

All the election-related misinformation that's floating around out there makes it tough for voters to separate fact from fiction.

2

Candidate campaigns

AT A GLANCE

When outside parties gain access to campaign strategy and voter targeting information, they can sway voters by sharing their discoveries in an unfavorable light.

WHEN IT HAPPENS

- ELECTION CYCLE BEGINS
- ELECTION DAY
- AND BEYOND...

Why it matters

Political campaigns are fast-moving, dynamic organizations. Campaign strategy, voter targeting information, canvassing, polling, you name it—they're constantly creating and communicating information about their strategies, messages and prospects for victory or defeat. When outside parties gain access to this information and use it for nefarious purposes, though, they can potentially sway voters by sharing their discoveries in an unfavorable light. Attackers could also focus disinformation campaigns on core voter segments for a given candidate, increasing the apparent credibility of their attacks by adding specifics or inside information about the candidate, their positions and strategies.

Campaigns are highly invested in data and technologies associated with communications, voter targeting and outreach. What they don't consistently invest in are effective measures for protecting their communications and data... and the results can be devastating.

HOW COMPROMISE HAPPENS

ATTACKER OBJECTIVES... AND HOW IT COULD HAPPEN	REAL-WORLD EXAMPLES
Disclose sensitive communications information to discredit candidates Compromising a candidate or campaign official's email account is easy if they don't use multi-factor authentication. Phishing is a low-tech, highly effective method. Once you compromise an individual, attackers can use their email account to more effectively target others, rapidly increasing the scope of a breach.	In March 2016, the personal Gmail account of John Podesta, a former White House chief of staff and the chair of Hillary Clinton's 2016 U.S. presidential campaign, was compromised. The spear-phishing attack exposed some of his emails, many of which were related to the campaign.
Impersonate a candidate or political organization to discredit them Beyond phishing, attackers use look-alike campaign or political social media or email accounts – something with a name close to an authentic account that appears credible–to spread disinformation.	In the 2016 election, a group claiming its efforts were paid for by Hilary Clinton's campaign targeted Democratic voters with social media ads urging them to "skip the lines" and vote by text message...which isn't possible.

The impact

Disclosure of sensitive communications can directly impact voter views of a candidate. Knowing which voters the candidate views as potential supporters allows an attacker to focus and potentially customize disinformation efforts, increasing their effectiveness. Directly impersonating a candidate, campaign or organization sows confusion, destroys voter trust and chips away at public confidence in the election process.

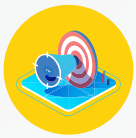
Why it's hard to fix

Political campaigns focus most of their people power and dollars directly on activities to get their candidate elected. There frequently aren't sufficient funds for security protections, and there isn't sufficient knowledge to provide awareness and training to campaign staff—which makes them vulnerable and ripe for an attack. Once an attack is successful, it's challenging if not impossible for a voter to be able to discern truth from lies or understand relevant context in the case of a sensitive information disclosure.

Once an attack is successful, it's challenging if not impossible for a voter to be able to discern truth from lies or understand relevant context in the case of a sensitive information disclosure.

HOW WE CAN PROTECT THE PROCESS

VOTERS



CAMPAIGNS

BEFORE NOV 2020

Fact check information before you believe it using sites like **snopes.com** (*and definitely before you share it*). **Sound familiar?**

Make staff aware of the risk their technology poses. Consider getting help with security basics for everyone on staff. (**pro tip:** Use Multi-Factor Authentication).

BEFORE 2024

Ask social media companies to actively supply information to help with the fact-checking process rather than relying on third-party sites. Furthermore, social media companies should consider more structured, accessible verified identity programs so it's possible to know if a given account is associated with a political figure, organization or campaign.

High-profile campaigns should consider spending funds on a CISO or equivalent; national political organizations like the RNC and DNC should consider providing shared security services for their party's campaigns.

3

Voter registration process

AT A GLANCE

Online registration opens up opportunities to tamper with voter rolls.

WHEN IT HAPPENS

- ELECTION CYCLE BEGINS
- ELECTION DAY
- AND BEYOND...

Why it matters

It's pretty simple: If you show up to vote and your name isn't on the registration list, you won't get to cast your ballot.

Today, thirty-eight states plus the District of Columbia offer online voter registration. While registering on the internet is convenient for voters, it offers an increasing array of opportunities for attackers to tamper from afar, or at least stir up doubt and confusion which can call the results of any election into question.

There's a second problem with voter registration: it's hard for voters to verify and update their voter registration information, especially when they move. There've been many contentious situations in the last few years between state governments and various political groups around the integrity of voter registration rolls in several states. This results in confusion and is yet another opportunity for some to call into question the overall integrity of the voter registration process.

HOW COMPROMISE HAPPENS

ATTACKER OBJECTIVES... AND HOW IT COULD HAPPEN	REAL-WORLD EXAMPLES
Delete or add voters An attacker could steal credentials of an administrator can add or change voter registration data.	Unless you're living under a rock, you probably know that the Russians targeted 21 states during the 2016 election cycle. They weren't successful in every case, but this was still a major wake up call for everyone involved in the election ecosystem.
Falsify absentee ballots Another tactic is to request absentee ballots on behalf of registered voters. Then, one could change their votes under the guise of helping others complete the absentee ballots.	North Carolina, we're looking at you. In 2018, a political operative coordinated an unlawful absentee ballot scheme where he paid workers to collect absentee ballots, and then filled out blank or incomplete ones. Not a good look.

The impact

Once someone gains access to a voter registration database, it's easy for an attacker to modify the data. The result? Voter registration rosters are, at best, not correct, or at worst they include fake voter records. This means that there's a risk of legitimate voters not being able to vote come Election Day, along with illegitimate voters suddenly being able to cast a vote.

Why it's hard to fix

While protecting against these kinds of simple, well-known attacks may sound straightforward, it's not. States and municipalities don't follow a standardized way to process voter registrations. Every state, city and county uses their own systems and has unique processes. Sure, organizations like the National Conference of State Legislatures and the Brennan Center offer guidelines and best practices for securing the voter registration process, but there are no hard and fast rules that states, cities and counties *have* to follow. This lack of standardization represents a potential field day for a crafty attacker who discovers a way to exploit the system. Add to that the fact that most state and local governments' budgets are under pressure, which makes for an attractive playing field for attackers.

HOW WE CAN PROTECT THE PROCESS

Fixing this challenge takes a broad-based, concerted effort—but the good news is that many of the resilience recommendations are things that can be kicked off now and can continue through 2024.

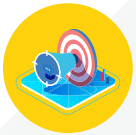
VOTERS

Check your registration status with your local government. Print out proof of your registration and take it with you to the polling place.

STATE AND LOCAL GOVERNMENTS

BEFORE **NOV 2020**
Make sure basic security precautions are in place (remember, two-factor authentication is your friend).

BEFORE **2024**
Develop more user-friendly mechanisms to assist voters in registering and keeping registrations current.

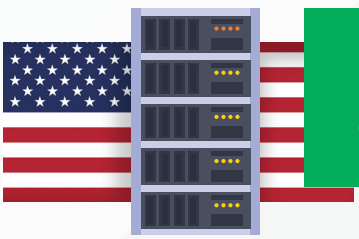


CAMPAIGNS

Launch education initiatives designed to assist voters in checking their voter status.

FEDERAL GOVERNMENT

Authorize election security funding for state and local governments.



Once they gain access to a voter registration database, it's easy for attackers to modify the data.

4

Pollster ratings

AT A GLANCE

Manipulating poll results can create confusion and sway or suppress votes.

WHEN IT HAPPENS

- ELECTION CYCLE BEGINS
- 15-30 DAYS TO ELECTION DAY
- ELECTION DAY
- AND BEYOND...

Why it matters

Leading up to a vote, all eyes are on the polls. Who's up? Who's down? Who's expected to win? What the polls say means a lot because it can have a material impact on who people vote for. If one voter's candidate has a big lead and it's snowing on Election Day, maybe they decide not to vote. Or maybe another voter simply decides their candidate doesn't "need" their vote and casts a protest vote instead.

HOW COMPROMISE HAPPENS

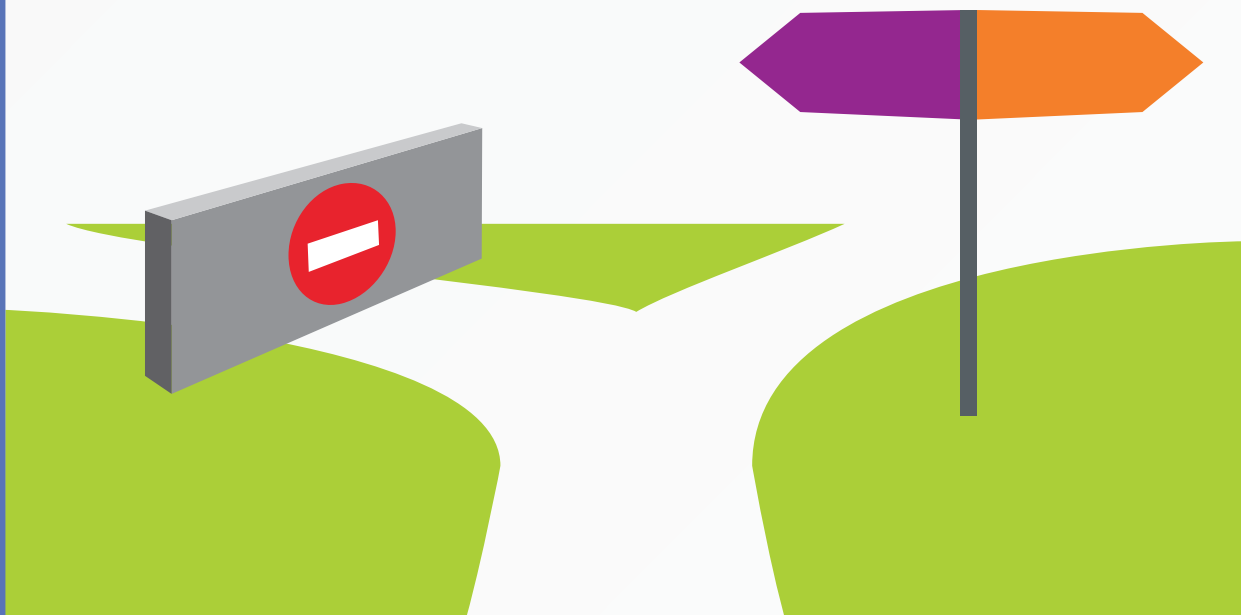
ATTACKER OBJECTIVE... AND HOW IT COULD HAPPEN

Suppress the vote on Election Day

Early exit polling data (real or fake) could be leaked on Election Day, affecting whether those who haven't voted yet decide to venture out to the polls.

REAL-WORLD EXAMPLE

Let's rewind to 2004—that's when exit poll data erroneously showed that former Senator John Kerry was headed to the White House. While the data itself was real, there are plenty of limitations to exit poll data, meaning that voters shouldn't take it as the ultimate source of election truth.

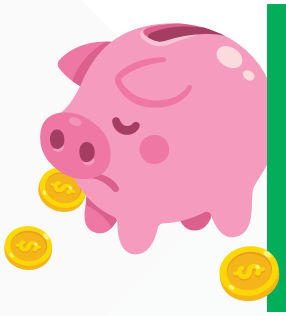


The impact

Leading up to Election Day, polling data is everywhere—on the TV, on social media, on your favorite podcast. False polling data can swing votes toward or away from candidates.

Why it's hard to fix

Organizations that conduct polls are privately held and comparatively small when it comes to other parts of the election supply chain. Most of them don't have big security teams or budgets. This makes it hard to keep determined attackers out. Plus, the attacker's ultimate target here is voter opinion. A low-tech compromise of polling data combined with social media promotion that goes viral can achieve an attacker's objective.



Organizations that conduct polls are privately held and comparatively small when it comes to other parts of the election supply chain. Most of them don't have big security teams or budgets.

HOW WE CAN PROTECT THE PROCESS

	VOTERS	POLLSTERS
BEFORE **NOV 2020**	Fact check the polling data you're reading. Also, compare polling results from multiple sources—don't rely on just one.	"With great power comes great responsibility." Pollsters are in a position of power when it comes to influencing public opinion about elections. Validate poll results as they're reported and flag and report anomalies both internally and to voters.
BEFORE **2024**	Educate others! Fact check the data you consume and encourage others to do the same.	Pollsters need to understand the critical role they play in this ecosystem and enact fundamental security measures commensurate with their role in the process. This includes things like having a CISO, implementing multi-factor authentication and making staff aware of security risks.

5

Voting infrastructure

AT A GLANCE

When a bad actor tampers with voting machines, they can control the outcome of an election.

WHEN IT HAPPENS

- ELECTION CYCLE BEGINS
- **ELECTION DAY**
- AND BEYOND...

Why it matters

According to the Brennan Center for Justice, as of 2019, 12 states still used primarily electronic polling methods in at least some of its municipalities; and four states—Delaware, Louisiana, Georgia and South Carolina—used these systems statewide, often foregoing paper backups. Many security experts argue that ditching paper backups is an unnecessary security risk to the integrity of elections.

Whether we like it or not, we're putting a lot of trust in the voting infrastructure, much of which is antiquated. If a bad actor can change the results on the electronic voting machines themselves, or if the machines are easy to hack into because the patching and software is outdated, then attackers can easily control the outcome of an election.

HOW COMPROMISE HAPPENS

ATTACKER OBJECTIVES... AND HOW IT COULD HAPPEN	REAL-WORLD EXAMPLES
Raise doubts about the integrity of results An attacker compromises one machine in a swing district. When authorities compare the paper trail they acknowledge the reported results are wrong.	At the 2019 DefCon cybersecurity conference, held annually in Las Vegas, ethical hackers showed us just how easy it is to break into a voting machine at the event's 'Voter Village.' The group purchased a variety of voting machines on eBay and after a few days of tinkering, broke into every single one.
Build security vulnerabilities into voting machines Voting machines aren't designed to be online—but if they accidentally get connected to the interwebs, it's easier than ever for an attacker to build a vulnerability right into a machine.	In January 2020, an independent team of cybersecurity researchers at the National Election Defense Coalition examined multiple voting machines and found at least 35 of them were connected to the internet.

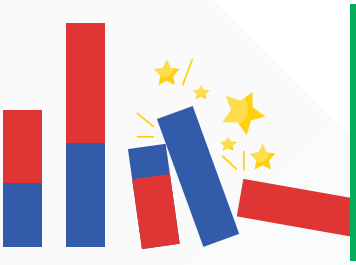
The impact

This is where everyone's mind goes first when they think about election security—to compromised voting machines. The impact is pretty straightforward: a bad actor can effectively "stuff" (or suppress) the ballot box in favor of his or her chosen candidate.

Why it's hard to fix

The biggest problem? Finding money to purchase new voting infrastructure. According to a recent study from the **Brennan Center for Justice**, two-thirds of local election officials said they don't have adequate funding to replace their aging voting infrastructure.

Beyond budget challenges, the lack of consistency in what voting infrastructure states and localities use makes it tough to enforce security standards at the ballot box. And a limited number of voting machine vendors means states are dependent on how good a vendor's security is (or isn't).

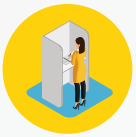


If a bad actor can change the results on the voting machines themselves, then they can control the outcome of an election.

HOW WE CAN PROTECT THE PROCESS

STATE AND LOCAL GOVERNMENTS

FEDERAL GOVERNMENT



ELECTION EQUIPMENT MANUFACTURERS

BEFORE NOV 2020

Ask election equipment manufacturers for guidance on securing infrastructure. Get new training materials to share with election officials and poll staffers.

Press election equipment manufacturers to offer more security-focused education programs and resources to municipalities so that they can protect themselves as election day approaches.

Provide training and security best practices to those officials and staffers who'll be using the manufacturer's machines on election day.

BEFORE 2024

Band together to make demands of election equipment suppliers to provide more secure machines.

Provide adequate funding for municipalities to upgrade antiquated voting machines, and mandate training among municipalities so that officials and poll workers will be well-versed in election security best practices.

Create stronger training programs for municipalities that purchase election tech. Address known vulnerabilities in equipment.

6

Results reporting

AT A GLANCE

The activity of hundreds of precincts reporting results within a matter of hours creates a rush of activity that can make crafty attackers hard to spot.

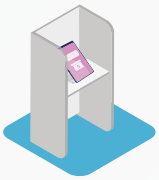
WHEN IT HAPPENS

- ELECTION CYCLE BEGINS
- ELECTION DAY
- AND BEYOND...

Why it matters

In a criminal trial there are detailed rules designed to protect the chain of custody for key evidence. Imagine if someone tampered with the fingerprints on a murder weapon. This might cause a judge to throw out a guilty verdict. In elections, the ballots are evidence. Preserving that evidence, including how it's reported, can impact election results and—equally important—the perception of an election's results.

HOW COMPROMISE HAPPENS



Change electronic voting results

An attacker can compromise the way the election results are uploaded to the central server.

Years ago, when the election board in Pennsylvania's Venango County examined its voting machines, officials discovered that remote-access software was installed on them. While a compromise never occurred, any voting machines that aren't disconnected from the internet are vulnerable to attackers tampering with the results.

ATTACKER OBJECTIVES

HOW IT COULD HAPPEN...

REAL WORLD EXAMPLES

Cast doubt on election results

An attacker can hack state and local websites where results are posted, tampering with the reporting.

It's so simple, even an 11-year old can do it. And at a past DefCon hacking conference, that's exactly what happened. A participant hacked into a replica of a website used to report election results, and successfully changed them.

The impact

If an attacker were successful at changing voting results, public trust in the elections process would take a nosedive. Candidates would demand recounts and would be left wondering if the reported results were actually accurate.

The scarier thing is that it doesn't take a crafty attacker to wreak havoc and cloud the election results reporting process. As Iowa recently showed us, sometimes a wonky app combined with untrained elections officials is enough to botch the results. Whether it's a hacker or a honest mistake, neither is a good look for a municipality.

Why it's hard to fix

Everyone is in a rush to report results on election day. Like a thief trying to shake surveillance in a busy train station, the activity of hundreds of precincts reporting results within a matter of hours creates a rush of activity that can make crafty attackers and their activities hard to spot.

HOW WE CAN PROTECT THE PROCESS

STATE AND LOCAL GOVERNMENTS

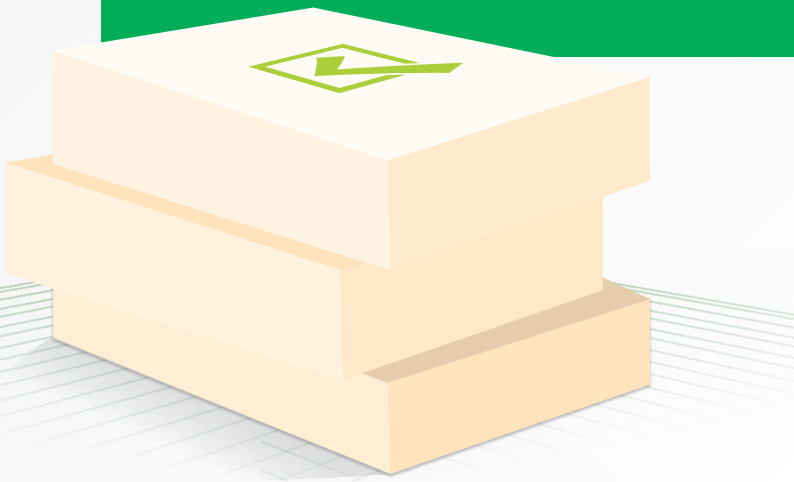
BEFORE **NOV 2020**

Double check your security protocols used for vote tallying and recording, along with the security of the systems involved in those activities.

BEFORE **2024**

Increase the integrity of the vote tallying and recording process through training for those involved in the process and more secure technology.

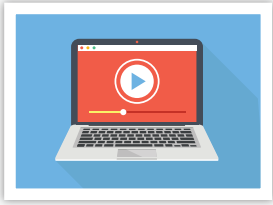
In elections, the ballots are evidence. Preserving that evidence, including how it is reported, can impact election results and—equally important—the perception of an election's results.



What happens next?

These potential points of compromise—along with a boatload of attack vectors that could be applied to each—might feel daunting to even the most seasoned security professional. But the truth is that by focusing on even a few key proactive security measures, our election security supply chain would be far better protected than it is today.

There are some easy things that all players in the supply chain can do right now to improve their security posture, such as:



Take advantage of education and training opportunities. Whether you're making sure your election officials know how to transfer election results to a website (*ahem*, Iowa) or sending your security analysts to relevant training sessions or conferences, educating the *people* who impact each part of the election supply chain is paramount. Having people on staff who know to look around the corners and can jump in quickly when something goes awry... that's one of your best defenses against threats.

Learn about (and implement) security best practices and frameworks. If you've worked in security for any length of time, chances are good that you've heard of the NIST Cyber Security Framework (CSF). It's a useful tool for helping organizations increase their overall resilience and response to cyber threats. The NIST CSF is just one of the many frameworks out there that can help you gauge your effectiveness when it comes to security and think about how you want your efforts to change or grow. So whether it's NIST or something else, pick a framework and use it to understand where and how you can get better.

Pressure test your systems. You know what helps when bad things start happening? Having a plan and knowing who needs to do what when something goes sideways. Create an incident response plan—better yet, create a plan, emulate an incident and practice what you might do if that bad thing happened in real life.

Expel provides transparent managed security. It's the antidote for companies trapped in failed relationships with their managed security service provider (MSSP) and those looking to avoid the frustration of working with one in the first place.

To learn more, check us out at **www.expel.io**.