FireEye iSIGHT Intelligence

ATTACKING THE BALLOT BOX

THREATS TO ELECTION SYSTEMS

APRIL 2018

EXECUTIVE SUMMARY

- State and local election infrastructure is increasingly at risk for targeting by a range of threat actors, in particular state-sponsored cyber espionage actors.
- FireEye iSIGHT Intelligence has identified threat vectors affecting voter registration, polling place identification, ballot submission, and vote counting that could be at risk.
- Actors utilizing information operations campaigns may target or mimic state and local officials' social media accounts directly to sow fear and mistrust.
- Aggressive campaigns to disrupt the electoral process may leverage tools such as ransomware and DDoS attacks to destabilize state and local IT networks and mimic cyber crime activity.

APRIL 2018

FireEye

CONTENTS

INTRODUCTION

Information technology now provides citizens convenient ways to take part in one of the most fundamental democratic processes, casting their vote. However, without the proper security mechanisms, this technology is vulnerable to attack by cyber threat actors.

The ability to vote and the integrity of the elections process is the foundational element in a successful democracy. The adoption of voting technology has streamlined many election processes, but it's not without risk. By conducting technological attacks, or falsely claiming them, adversaries can subtly change election outcomes or cause long-lasting loss of legitimacy and damage to US elections systems.

The US election system is complex and de-centralized, with states and counties using a wide variety of software and machinery to coordinate and conduct elections. Therefore, a nation-wide coordinated attack would require extensive resources, precise planning, intelligence on county and state-specific election processes, and high technical sophistication. Following Russian intent to interfere in the 2016 US general election, securing infrastructure prior to the midterm elections in 2018 will require insight into adversary intentions and evolving tools, tactics, and procedures (TTPs).

This report follows the voting process, from registering to vote to vote tabulation to provide an overview of cyber threat attack methods and their potential impact against US election systems, covering:

- Electronic voter registration
- DDoS against state elections websites
- Attacks against Voting Machines
- Attacks against Election Management Systems

Additionally, it examines other ways in which state and local infrastructure may be targeted to interfere with or cause a loss of confidence in the election process.

ATTACKING THE BALLOT BOX
Threats to US Elections Technology

Public officials seek to apply information technology to the foundational element of democracy – the right to vote. But adoption of elections technology is not without risk. By conducting technological attacks, or falsely claiming them, adversaries may influence particular races and delegitimize elections.

FireEye iSIGHT Intelligence analysts identified the following threat vectors affecting voter registration, polling place identification, ballot submission, and vote counting.

REGISTER TO VOTE

Registration Websites and Databases

Blocked access to online voter registration systems impedes voters from registering before the deadline.

Corrupted data disqualifies voters whose information no longer matches registration records.

Voters whose records are deleted from the database **may not be able to vote at all.**

A 2016 **intrusion into the Illinois voter registration** database signals adversary interest.

GOING TO THE POLLS

State Elections Websites

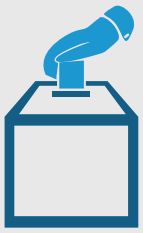
DDoS attacks against official elections websites **prevent voters** from finding their polling location.

DDoS of "where to vote" web sites occurred in the run up to **Russian elections in 2016** and during the **Seoul mayoral elections of 2011.**

These attacks can **diminish voter turnout.**

SUBMITTING A BALLOT

Electronic Voting Machines and Ballot Counters



Electronic voting machines are generally not connected to the Internet, but do require programming, meaning that **adversaries could gain access** through programmer computers.

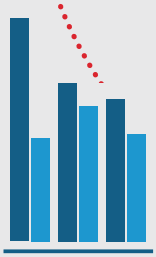
Removable media ports make voting machines **susceptible to tampering** before or during an election.

Most voting machines **exhibit weak authentication, limited encryption, and numerous software vulnerabilities.**

Inadequate auditing systems **facilitate false claims** of cyber-attack when voting technology fails for other reasons.

COUNTING THE VOTES

Election Management Systems



Election Management Systems (EMS) are **software that aggregate votes** from individual voting machines across counties or even states.

EMS are **susceptible to remote, network-based attacks,** such as from a voting machine, programmer machine or even the Internet.

PCs running EMS are **often outdated and unpatched.**

EMS **seldom follow recommended security** practices for authentication or encryption.

REGISTERING TO VOTE: THREATS TO ELECTRONIC VOTER REGISTRATION

Voter registration enables those eligible to vote to exercise that right while blocking illegitimate voters. As of March 2018, 31 states now offer online voter registration, with another seven having passed legislation to implement the online option. Along with online registration portals , many states also store voter information in databases accessible via the internet, in order to allow voters to check their voter status . However, as states transition their voter registration processes online, the databases and registration websites become targets for cyber threat activity.

Attacks against voter registration systems could have major disruptive potential for voters in the US. Actors who gain illicit access to registration databases can delete or modify information of voters. This could deter them from voting altogether, force them to use provisional ballots, or change their polling location. These attacks could also prevent voters from registering before the deadline.

RISK

RECYCLED INFORMATION

Since the beginning of 2016, millions of US voters have had their information leaked publically or sold on crime forums. Databases of voter information, which often includes names, dates of birth, and social security numbers, poses a direct threat to voter registration as malicious actors can log in directly using that information to change or delete key information for a group or individuals.

- In July, 2016, the actor DataDirect offered to sell US voter registration records for all 50 states on a crime forum.
- In March, 2016, the actor peace_of_ mind offered to sell information on 620,000 Pennsylvania voters.
- In January, 2016, the actor NSA shared four databases of voting information from Ohio, Rhode Island, Delaware, and Washington, with information on a total of 17,685,000 voters.
- In October, 2015, a reputable Russian-speaking actor “xors” offered to sell information on 190 million US persons allegedly taken from the website of the US Elections Commission.

SPEAR-PHISHING

Spear-phishing can also be used by malicious actors to gain access to databases servers through individuals working for the Board of Elections or state secretary of state offices. These attacks, utilizing infected attachments or spoofed websites, could be targeted at individuals in these offices on their personal or professional email accounts to gain access to credentials or place malware onto the machine of a board of elections employee.

WEBSITE VULNERABILITIES

Unpatched or poorly maintained voter registration websites pose a risk to the registration process. Actors seeking to gain unauthorized access to these databases without access to legitimate credentials may scan and exploit vulnerabilities in voter registration websites to gain access to the databases.

- These attacks can include SQL injection, cross-site scripting, remote file inclusion, and brute forcing, among others. Insufficient input validation and access control may allow SQL injection, in which attackers would be able to execute arbitrary SQL commands, including add, modify and delete records in the voter database.
- Other attacks like cross-site scripting, remote file inclusion, and brute forcing may not give the attackers access to the database, but may be used to prevent voters from using the website.
- In July, 2016, the state of Illinois voter registration database was compromised by actors that identified a SQL injection vulnerability in the state Board of Elections website, and used three penetration testing tools, Acunetix, SQLMap, and DirBuster, to gain access to 200,000 voter records. Illinois maintains that no data was altered; however, it is possible that the actors had the ability to the modify or delete data.

DDOS

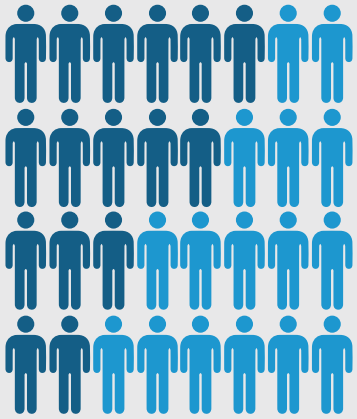
Another attack vector on voter registration is through distributed denial-of-service (DoS). These attacks could take a website offline for a number of hours, or days depending on the scale of the attack. These attacks could prevent voters from registering by the deadline.

MITIGATIONS

Many of the security issues in online voter registration systems can be solved by merely following common security practices. However, some additional mitigations could include:

- Keep a regular back-up of the voter database in a secure location.
- Track for large-scale changes to voter databases.
- Maintain and regularly patch voter registration websites.
- Deploy backup websites to show polling locations in the case of a DDoS attack.
- Implement spear phishing mitigation best practices, including employee awareness training.

GOING TO THE POLLS: THREATS AGAINST ELECTION WEBSITES



Limiting access to the polls is a well-known method of changing election outcomes. Cyber threat actors have their own method: using DDoS or defacement to prevent voters from finding their polling locations.

Voters use their county website to find their polling location, which often stores other important information regarding the elections. If these websites are taken offline, voters can be deprived of key information about their polling location, or alerts and last minute changes about the election.

Malicious actors targeting these websites could drastically reduce voter turnout for certain localities, create confusion and distrust, and reduce the legitimacy of the election outcome.

RISK

DDoS: With the rise of for-hire DDoS services, the threshold of sophistication for a successful DDoS attack can simply be how much an actor is willing to pay. Actors can also rally support for a participatory DDoS attack using publically available tools, or use their own tools and botnets to conduct the attack. A DDoS attack against a state elections website could take it offline anywhere from seconds to days. While a couple of seconds may not affect voter's abilities to reach the polls, if the elections-related information is offline for longer periods of time, it could prevent individuals from knowing their specific polling location, thereby reducing voter turnout.

- In September 2016, before the elections of the lower house of the Russian Federal Assembly, FireEye iSIGHT Intelligence believed that dozens of Russian websites, including media, research, transparency and election monitoring, and election commission websites were targeted with DDoS.
- In Sept. 2015, in the run up to the Russian local elections, cyber threat actors conducted low-impact DDoS attacks against at least eight Russian websites, including the Russian president's website, the Central Election Commission (CEC) website, and four opposition news websites. A non-profit website that promoted election transparency, the Open Alliance of Observers, was also targeted. We surmise that this activity was due to actors seeking to disrupt the Russian political process.
- In Oct. 2011, a DDoS attack against the South Korean National Election Commission (NEC) took parts of the website offline during the Seoul mayoral election, which prevented some voters from finding the polling location.

In the US, we have observed hacktivist actors using DDoS attacks to take state and local websites offline in several participatory operations, particularly in #OpFlint, #OpFerguson, and #OpBaltimore. While these campaigns did not consist of highly sophisticated actors or tools, they were still successful in taking them offline.

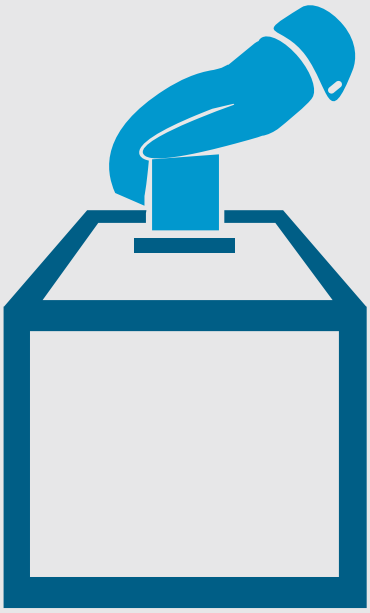
DEFACEMENT

By leveraging website vulnerabilities to deface state and county websites, malicious actors could change or block key information that voters need to find their polling locations. Hypothetically, these actors could fabricate a news announcement on the county front page announcing changes in polling locations, or create unrest by defacing the website with hacker-related imagery.

MITIGATIONS

- Ensuring that the security organization behind the state websites have established DDoS mitigation protocols, both within their own servers and with their ISP.
- These include backup servers, rate limits and filters to drop packets, and heightened monitoring of website traffic.
- Maintain and regularly patch election information websites.

CASTING THE BALLOT: VOTING MACHINES



Voting machines have become deeply integrated into the US elections process, but the inherent convenience of these systems does not come without some risk. If these machines are compromised by malicious actors, they take control of the votes of thousands of US citizens.

Voting machines record the votes of US citizens as well as tabulate, communicate, and audit those results. It's important to note that due to the US's de-centralized and unstandardized voting system, a nation-wide coordinated attack on voting machines would require high technical sophistication, lengthy planning, and extensive resources.

- The US uses 53 types of voting machines, which are sold by 17 different vendors. Each of these vendors creates a product ecosystem of voter-facing machines, optical scanners for absentee ballots, and an Election Management System. Most states use a number of different voting ecosystems, which vary county by county; however, 83% of the US votes are tabulated by machines coming from the top three vendors, ES&S, Dominion, and Hart Intercivic.
- Voter-facing voting machines require physical access to compromise. No voting machines in the US are required to be connected to external or public networks, therefore remote attacks are not currently possible. Some voting machines maintain the ports to be connected to external networks, however no states currently authorize the use of those ports. This limits the abilities of remote adversaries to compromise the voting machines unless they have an insider.
- Depending on the practices established by each county, there are central vote tabulating machines that may be connected to an Intranet or the public Internet. It may be possible for remote adversaries to attack those machines.

The security and ability to audit voting machines varies by the type of voting machine, and the settings used by each county. The following are the types of voting machines used in the US:

- **Optical Scanners (OS):** These devices, used by both poll workers and voters alike, scan physical ballots marked with a pen to tabulate votes.
- **Ballot Marking Devices (BM):** These machines use buttons to mark or punch holes in a physical ballot, and some store the information on a memory card or flash drive.
- **Direct-Recording Electronic (DRE):** These machines use touch screens or physical buttons to directly record votes onto a memory card, flash drive, or other external device.

RISKS

As the US employs 57 different types of voting machines, each machine and the system of hardware and software used around it has different security flaws. However, we identified key themes in their security flaws, namely that voting machines are particularly vulnerable to malware introduced through removable hardware. This is due to the generally weak security on the voting machines themselves, as well as similar basic security flaws and challenges as many Industrial Control Systems.

- Weak authenticity checks
- Lack of or weak integrity checks
- Lack of input validation
- Weak password security
- Lack of or poorly executed encryption
- Software vulnerabilities

MALWARE ATTACKS WITH REMOVABLE HARDWARE

More specifically to voting machines, the insecure removable hardware is one of the most prominent ways that an actor can introduce malware onto these machines. Since there is no easy way to check for malware introduced into a voting machine, it is difficult to prove that vote tampering occurred.

Actors introducing malware onto these machines would need to have high technical sophistication as they would need to create malware specifically for the voting machine that they intended to compromise, have an understanding of the types of voting machines and processes used in the location they intended to infiltrate, and have access through a registered voter or malicious insider in that specific location.

ATTACKS BY REMOVABLE MEDIA:

Memory cards, access cards, PEBs, and flash drives for these machines can be purchased online through legitimate vendors for under $200 USD. Therefore, finding the correct hardware would not be an issue for a malicious actor. Each type of removable hardware infects the machine differently, but the actors

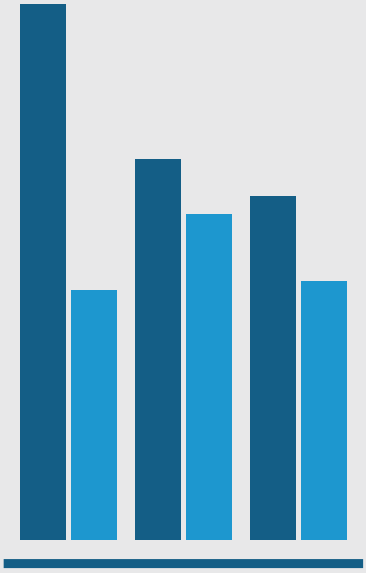
- **Memory Cards:** Most machines use memory cards to store data from the voting machine. These memory cards are stored behind locked doors in the voting machine itself. A memory card loaded with malware is then inserted, the machine automatically reboots, and the original memory card is reloaded into the machine to restore the originally tabulated votes.
  - For example, on the Diebold Accuvote TS, a security team at Princeton University found that after gaining physical access to the machine, they could install malicious code in the machine through the memory card in as little as one minute.
- **PEBs:** Personalized electronic ballots (PEBs) are required to access the iVotronic DRE. They are both purchasable online and relatively easy to emulate using other devices.
  - A team of security researchers at the University of California, Berkeley, successfully used a Palm Pilot PDA to emulate a PEB and take control of the iVotronic through an internal buffer overflow bug.
- **Flash Drives:** Many voting machines use external flash drives instead of memory cards, which are more easily accessible by malicious actors and could be replaced with flash drives containing malicious code.
- **Access Cards:** Access cards, also called Smart Cards or Voter Access cards, give a voter access to the voting machine and allows them to vote. We were unable to find definitive evidence that these could contain malware.
- **Exposed Ports:** Many voting machines have exposed ports that actors can use to connect their own devices and interact with the software on the machine.

As very few voting machines have strong authentication or integrity checks, these external devices could execute arbitrary code on the machines immediately, without any protocols checking if the code was non-malicious.

MITIGATIONS

- Specific mitigations vary from machine to machine
- Enforce strict password security
- Ensure that voting machines are fully patched and up to date
- Implement poll worker training to maintain vigilance against odd behavior and overt tampering with the machines. Insider threat is also a major risk to voting machines.
- Leave polling booth curtain partially open so poll workers can be vigilant for signs of odd voter behavior.
- Asking individuals to check their bags, cell phones, and large coats at the poll worker's desk may also prevent physical tampering.

COUNTING THE VOTES: VOTING MACHINES



When the votes are taken back to the county headquarters, poll workers aggregate the data from each polling station on an Election Management System (EMS). These systems are the software that aggregate data from the disparate voting machines and create readable outputs. EMS are housed on PCs and operated by supervisors or election officials. These machines are a particularly valuable target as EMS are vulnerable from both a software and hardware standpoint.

EMS provide greater incentives to attackers as they control data from the entire county, municipality, city or precinct, rather than the votes on a single voting machine. Attackers that gain access to these systems could flip votes, delete data, crash systems, or infect machines for future elections.

RISKS

EMS can have a larger attack surface than the voting machines themselves as they can be connected to public or private networks, have interactions with hardware from voting machines, and are housed on PCs running very old operating systems with potentially unpatched vulnerabilities. This leaves the system open to compromise via malware or potential remote system takeover.

EMS are run on specially configured PCs, however they often run on older operating systems such as Windows 98 or Windows XP, or outdated versions of Linux. These PCs have no or very basic firewalls or anti-virus software. Therefore, vulnerabilities in older operating systems could be exploited by malicious actors.

Similar to voting machines, we observed the following security flaws:

- Weak authenticity checks
- Weak password security
- Lack of or poorly executed encryption
- Software vulnerabilities

MALWARE FROM VOTING MACHINES:

Removable hardware from voting machines is often directly introduced into the PC that runs the EMS. An actor could plausibly introduce malware into a single voting machine that would pass between types of removable media until it was introduced into the EMS. Once introduced into the EMS, the malware would execute and could take full control of the system.

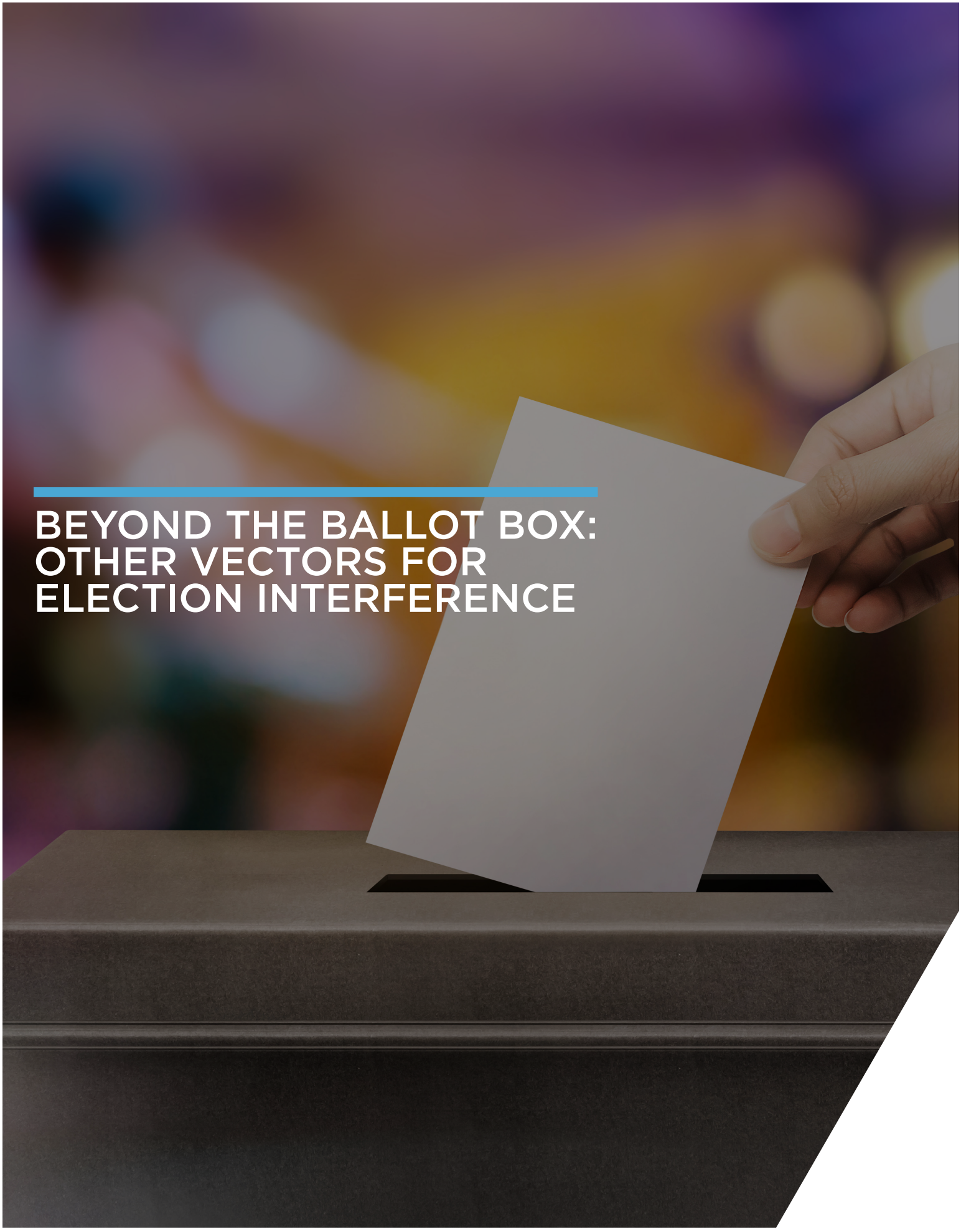
NETWORK-BASED ATTACK:

If the PC is connected to the internet or an Intranet that is connected to the Internet, the EMS is vulnerable to remote attack by malicious actors. If an actor can gain access to the Intranet or find the server on the Internet, it is possible that actors could conduct DDoS attacks or attempt to exploit the server that holds the data.

- It has been noted by security researchers that a number of EMS rely on SQL or other database formats that are vulnerable to exploitation.

MITIGATIONS

- Ensuring that the PC and the EMS are fully patched and up to date is vital to the security of these systems.
- Keeping all PCs unconnected to the Internet or even private Intranets can prevent remote attacks.



BEYOND THE BALLOT BOX: OTHER VECTORS FOR ELECTION INTERFERENCE

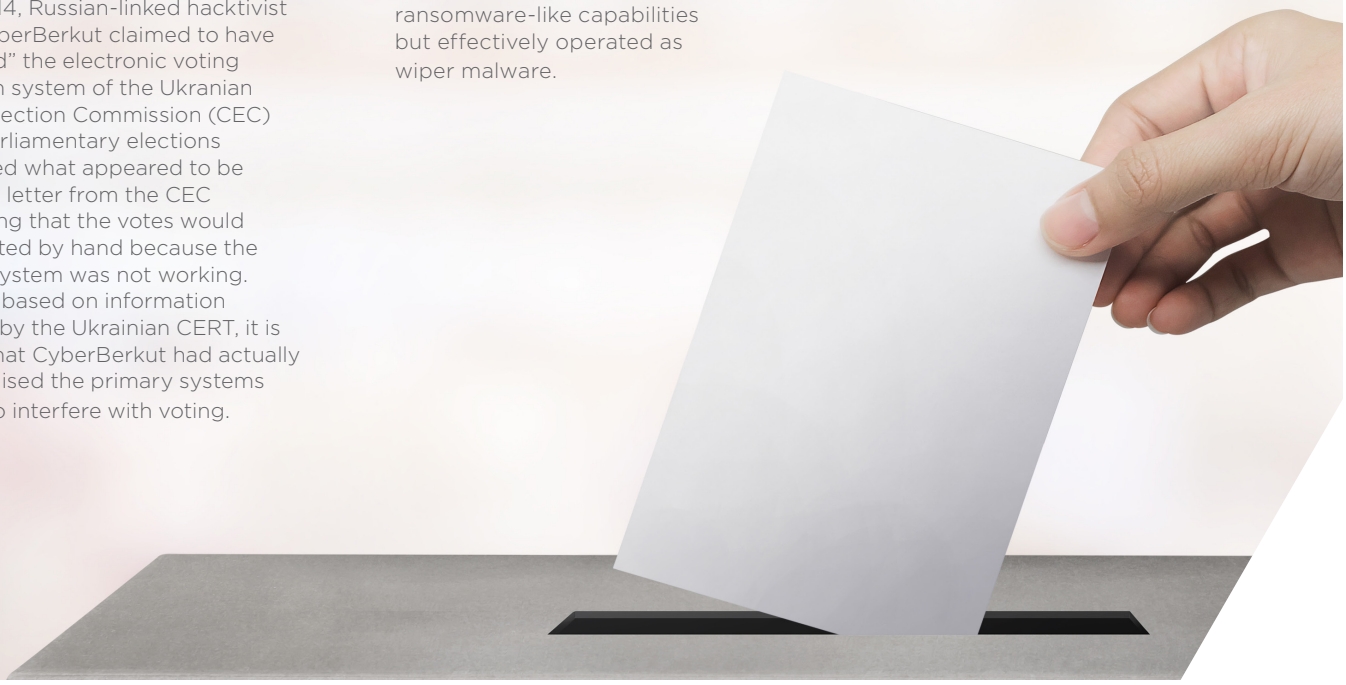
Beyond targeting of the voting process directly, enterprising adversaries may seek to cause disruption and loss of confidence by targeting broader state and local infrastructure, including official social media accounts and government IT systems.

- **Disinformation Campaigns:** During the 2016 general election in the US and subsequent elections in Europe, FireEye iSIGHT Intelligence witnessed the weaponization of data through leaks to social media. Outside of seeking to manipulate public opinion, the demonstration of this as a useful tactic could be expanded to include other malicious activity.
  - Actors could compromise—or spoof—legitimate state and local officials' social media accounts to sow confusion and distrust, announcing fraudulent results or closures at specific polls.
  - To further call into doubt the legitimacy of the election process, actors could circulate claims of election infrastructure compromise. In late 2014, Russian-linked hacktivist group CyberBerkut claimed to have "disrupted" the electronic voting tabulation system of the Ukranian Central Election Commission (CEC) during parliamentary elections and posted what appeared to be an official letter from the CEC announcing that the votes would be tabulated by hand because the election system was not working. However, based on information provided by the Ukrainian CERT, it is unlikely that CyberBerkut had actually compromised the primary systems needed to interfere with voting.
- **Disruptive Attacks:** Should actors seek to obstruct or hamper the process of conducting elections—or raise the prospect that they have been successful in compromising election infrastructure—they may result in targeting broader state and local IT infrastructure, using disruptive tools. In addition to the DDoS attacks mentioned above, deploying ransomware to impact state and local internal networks can create coordination, communication, and response problems for election officials.
  - Recent ransomware attacks on the city of Atlanta have highlighted how local municipalities face dangers from disruptive tools.
  - While in most cases actors deploy ransomware for financial gain, it is possible that state-sponsored actors could conduct targeted ransomware campaigns against state or municipal IT infrastructure without an intent to decrypt upon payment of the ransom. Additionally, actors may utilize wiper malware masquerading as ransomware to further confuse incident responders as to the actors intent, and cast suspicion on criminal actors.
  - Similar TTPs may have been used in January 2017 by Russian-nexus Sandworm Team, deploying WHITEROSE malware against targets in Ukraine that possessed ransomware-like capabilities but effectively operated as wiper malware.

OUTLOOK AND IMPLICATIONS

Following concerns about foreign adversary interference in the 2016 general election and with the upcoming midterm elections in 2018, increased attention is being paid to the security of the voting process. Many states are still using voting machines over a decade old. As such, technical failures are very likely to occur, and may be leveraged by social media-based disinformation campaigns to create fear of a cyber-based attack and de-legitimize the results of the election.

Although we have not observed attacks against elections infrastructure as of March 2018, malicious actors and nation states likely already have an understanding of the flaws in the US elections infrastructure and will seek to exploit opportunities where they can. Ensuring a holistic approach to security that considers adversary intent and TTPs will allow forward-leaning states and municipalities to reduce their risk exposure and preserve the integrity of the election process.



FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye