State-of-the-Art Security Performs First-Rate Threat Mitigation in Convention Elections

Philip Andreae,
Advisor, Voatz

Hilary Braseth,
Chief of Staff, Voatz

Nimit Sawhney,
Co-founder and CEO, Voatz

Abstract

The COVID-19 pandemic has changed our world, touching every aspect of our lives. Elections are no exception. In the midst of the pandemic, and with the advent of new technologies in the last five years, many election officials are turning to remote voting options. Smartphone-app based remote voting systems have demonstrated the ability to remotely verify a voter's identity, detect threats at both the network and device level, prevent vote submissions from any compromised device, and finally, the ability to conduct a rigorous post-election audit to ensure the integrity of the results.

In the midst of a pandemic, political party conventions offered a unique opportunity to test and learn about the resiliency of remote options. This paper explores the emerging security datasets around the performance of the Voatz remote voting system while conducting virtual conventions in April 2020. During this time, the Voatz system processed a record 7,000 votes on its platform during a single election period. As a result, Voatz was able to collect a rich dataset of device and network level threat detection and mitigation events. This paper will analyze this dataset, the implications of the insights, and considerations for the applicability of mobile security for high-stakes industries, whether governmental, financial, or critical infrastructure related.

Introduction

In mid-March, when businesses and public spaces across the United States were forced to close, political parties began to investigate how to transition to the new reality as the election season kicked off. Political party conventions[1] were a particular challenge because virtual conventions had never been done before—historically, parties had grown accustomed to gathering in a large arena or gymnasium for a weekend and conducting in-person voting, often through hand-counted paper ballots. After careful deliberation, party leaders turned to remote voting platforms, advised by election officials who had successfully piloted them in governmental elections.

One of the earliest examples of a political party using remote voting for its convention in the midst of the pandemic was the Utah Republican Party[2]. The success at their early convention became the roadmap[3] for political parties on both sides of the aisle adopting these remote voting options throughout the remainder of the summer and leading up to the November election.

Context: Political Party Convention Voting

Political party conventions are unique opportunities to test and learn about the resiliency of remote voting options. Convention voting holds the same rigor and demands of governmental elections, with certain parties requiring real-time auditability. The convention experience itself is also important: it plays a critical role in creating enthusiasm within the party and rallying support. Party leadership must ensure trust and integrity in results, security, and access to avoid headlines like the ones emerging from conventions in Iowa[4] and Texas[5]. Any misstep can mean questioning the party leadership.

Every election system is under the constant threat of attacks. Political parties are especially vulnerable because conventions are run by volunteers under loosely constructed security systems. Even Presidential campaigns could be hacked despite security teams in place, like the 2016 hack into the DNC.

[1] Jeff Greenfield, POLITICO, How Coronavirus Will Blow Up the 2020 Campaign No conventions. No rallies. No get-out-the-vote. Insiders are starting to rethink how politics is even going to work. April 12, 2020

[2] Utah GOP Sets the Standards for Mobile Voting in Groundbreaking Virtual Convention (April 30, 2020)

[3] Utah State Convention Events https://utgop.org/nominees/

[4] Audrey Mcnamara, CBS News, Confusion and embarrassment in Iowa: What went wrong, and what happens next? (February 4, 2020)

[5] Patrick Svitek and Cassandra Pollock, Texas Tribune Texas GOP convention chaos prompts delegates to create a second gathering for unfinished business (July 20, 2020)

The stakes are high, especially in a polarized political environment. Any platform used must demonstrate that the system can run smoothly while simultaneously mounting rigorous defenses against any potential vulnerabilities or attacks.

With this background, Voatz worked closely with party officials to ensure a seamless voting process with the conventions. Delegates voting in the Utah GOP conventions, for example, expressed satisfaction about the experience voting[6] through their mobile devices, with enthusiastic support for its continued application during future elections.

Through these party conventions, Voatz was able to collect the largest threat dataset on mobile elections in the U.S., providing insights and solutions for future conventions and elections.

This threat detection data contains implications and applications beyond elections and could be applicable to the types of threats that enterprises and governments might see in an increasingly virtual world.

Situation Analysis

Coronavirus aside, the current voting landscape contains significant gaps and obstacles[7]. The "traditional" means of remote voting for disabled voters, overseas military, and citizens—mail-in ballots, fax, and email—are not reliable, accessible, or secure. Email[8], without end-to-end encryption and vulnerable to ransomware, is not a private or secure mode of transmission. Using these channels means that these voters revoke their right to a private ballot, or their ballot cannot arrive in a timely manner to be counted.

As per the National Conference of State Legislators[9] on email ballot returns: Privacy: Because election officials are able to identify the person who sent a ballot via electronic transmission, ballots are not fully anonymous. Privacy of the ballot is a value for voters and for society as a whole.

The pandemic has exacerbated this situation and exposed the missing pieces in the current systems of voting.

Given elections' status as critical infrastructure[10], security is an integral part of this conversation. The U.S. faces potential attacks from nation-states and nefarious actors, and it is important that every American has full confidence in the integrity of election infrastructure, particularly in critical election years.

Remote Voting Systems

In view of challenges to the current voting systems, over the past decade, a handful of companies have worked to develop accessible remote voting options to make voting more convenient and secure for the most disenfranchised voters. Each company differs in its approach, leveraging a different combination of technologies to build its platform.

Voatz is the first voting platform to pioneer a smartphone app-based system that leverages the recent advancements and advantages of mobile security, remote identity verification and other technologies to both secure the identity of the voter and the vote. The company has taken the steps necessary to build an integrated cybersecurity strategy that takes a layered defense-in-depth approach, covering the security of the platform from multiple points of contact and allowing for the reporting necessary to deliver lessons learned.

When considering any remote voting system, remotely accessing a ballot presents unique advantages in access and privacy, and with it, increased variability in the potential types of threats. As such, a critical touchpoint for security is to secure the device via which the voter votes.

Smartphone App-Based Systems

In the case of the Voatz remote voting system, a voter can only access their vote using a mobile device (e.g. a smartphone or tablet). Smartphone app-based systems[11] contain unique security features that distinguish them from web browser-based platforms. These distinct features allow unprecedented levels of threat detection at both the network and device level, ensuring that a compromised device cannot submit a vote.

This ability for advanced threat detection makes breaking into smartphones without physically connecting to the device resource intensive. For example, an untethered hack of an iOS is referred to as the "million-dollar hack[12], and according to Wired -- a zero-day hack of an Android system could cost up to $2.5mn dollars[13]".

In addition, smartphone app-based systems allow the ability to remotely verify a voter's identity, offer enhanced accessibility features, and the ability to conduct a rigorous post-election audit to ensure integrity in the results.

---

[6] Bridgett A. King, Casting Voatz in Utah: An Analysis of the 2020 Utah Republican Convention (June 2020)

[7] Katie Pyzyk - SmartCities - Dive Virus vs. voting: Behind the high-risk presidential primary elections (June 6, 2020)

[8] Danny Palmer - ZDnet Phishing attacks: Why is email still such an easy target for hackers? (October 24, 2018)

[9] National Conference of State Legislators https://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx

[10] IF10677.pdf Congressional Research Service (September 18, 2019)

[11] 10 Reasons Why Smartphone App Voting is better than Web Browser Voting (July 23, 2020)

[12] Danny Davies, Dave - NPR - Journalist Who Helped Break Snowden's Story Reflects On His High-Stakes Reporting (May 20, 2020)

[13] Andy Greenberg - The Wired - https://www.wired.com/story/android-zero-day-more-than-ios-zerodium/ (August 3, 2019)

Voatz

10 Reasons why Smartphone App-Based Remote Voting is better than Web Browser-Based Remote Voting

Criteria	Smartphone App Voting (SAV)	Web Browser Voting (WBV)	Reference
1 **Secure Enclave**	SAV takes advantage of secure enclaves on compatible mobile devices to create an extra layer of security for your private keys.	There is no known WBV system that offers this capability without requiring the user to connect additional hardware to the computer.	1a 1b 1c
2 **Remote Identity Verification**	SAV supports NIST 800-63 compliant remote identity verification to determine the eligibility of remote voters.	There is no known WBV system that offers this level of compliance for remote identity verification.	2a
3 **Device Threat Detection**	SAV can detect device tampering, malware and a whole range of device level threats.	There is no deployed WBV system that offers native device threat detection.	3a
4 **Network Threat Detection**	SAV can detect various network level threats and provide mitigations.	There is no deployed WBV system that offers native network threat detection.	4a
5 **Tamper Resistant Storage and Distributed Ledgers**	SAV uses tamper resistant storage based on distributed ledger technology to ensure ballot data cannot be tampered with in an undetectable manner.	Most of the deployed WBV systems don't make use of tamper resistant storage with or without distributed ledger technologies.	5a 5b 5c
6 **Voter Verifiable Receipts**	SAV provides secure voter verifiable receipts to ensure voter intent is honored.	There is no deployed WBV system that supports voter verifiable receipts.	6a
7 **End-to-End Citizens Audits**	SAV supports end-to-end citizens audits to ensure unprecedented levels of transparency and auditability.	There is no deployed WBV system that offers the end-to-end audit capabilities to remote voters.	7a 7b
8 **Accessibility and ADA Compliance**	SAV offers unprecedented levels of access for voters with disabilities and enables them to vote privately without needing assistance from a proxy.	Most WBV systems are unable to take full advantage of the modern accessibility features to ensure a private vote for voters with disabilities.	8a
9 **Automated eFax Support**	SAV offers remote accessible ballot return via automated eFax.	There is no known WBV system that offers automated eFax support for ballot return.	9a
10 **One Device One Vote**	SAV enforces the principle of one voter per smartphone device for extra security.	There is no known WBV system that offers this security capability.	10a

The term **deployed implies actual usage in an official government, public election*

LAST UPDATED: JULY 19, 2020

Finally, smartphone app-based systems incorporate multiple layers of security to provide defense-in-depth, or at every layer of the platform. These include system-level security, network-level security, application-level security, and transmission-level security. If one layer is penetrated, the threat is detected and stopped at additional levels. In addition, the system employs malware detection and end-to-end encryption to detect whether an operating system has been tampered with, and to prevent a compromised device from submitting a ballot. In the landscape of all remote voting systems, security is still and always an ongoing journey and not a destination. It remains vital to continually test and identify possible vulnerabilities to ensure a comprehensive defense.

The Data: Threat Detection In Convention Voting

In April 2020, Voatz implemented remote voting for a number of virtual conventions. The data presented here is from a convention that marks a milestone in processing a record number of mobile vote submissions. During the election, Voatz's advanced security threat detection mechanisms were able to detect, mitigate and thwart a number of smartphones from voting that had malware, were operating on insecure networks, or had insecure applications installed.

The ability to detect, log and mitigate these types of threats is unique to the Voatz mobile voting platform. To do this, the Voatz platform combines widely-used threat detection software with its own technology to safeguard the voting process. This ensures that only voters with secure smartphones are permitted to cast a ballot, and if the system detects any threats on the smartphone, a voter will not be able to vote.

In short, if a voter has a compromised device—whether they know about it or not —they'll receive an error and will not be able to vote.

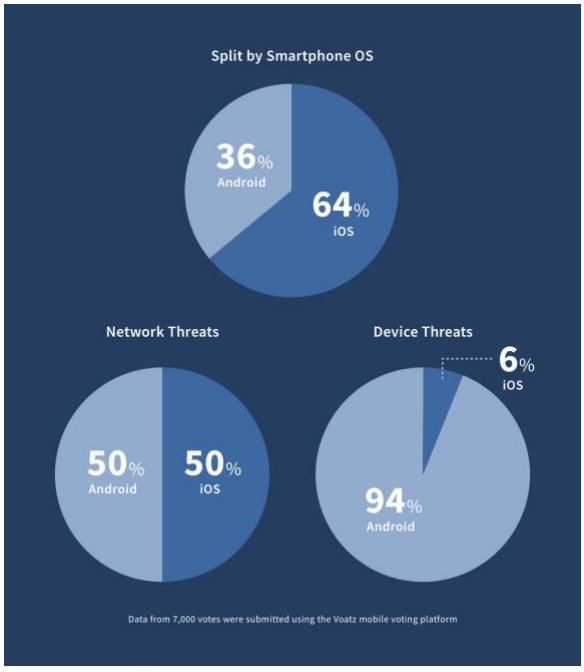
The threat detection behavior gathered at this large election produced a rich dataset that holds compelling insights for the applicability of mobile security for high-stakes industries, whether governmental, financial, or critical infrastructure. What Voatz found is reflective of potential on-the-ground vulnerabilities in both Android and iOS infrastructure, with additional potential lessons for broader cybersecurity concerns.

Threat Detection During the Election

During the election, a handful of voters were shown to have compromised devices and were prevented from voting until their device threats were mitigated. In some instances, voters were asked to remove malware on their devices. In others, some voters were asked to delete certain applications or functions they had installed which made their smartphones insecure. These voters were unable to vote until they did so. These cases not only reveal real-time device usage and the threat landscape but also indicate the system is capable and successful in both detecting and mitigating threats at a very granular level. This is required to ensure a secure vote.

The analysis below includes compelling statistics around the types of malware or applications detected, along with the device type.

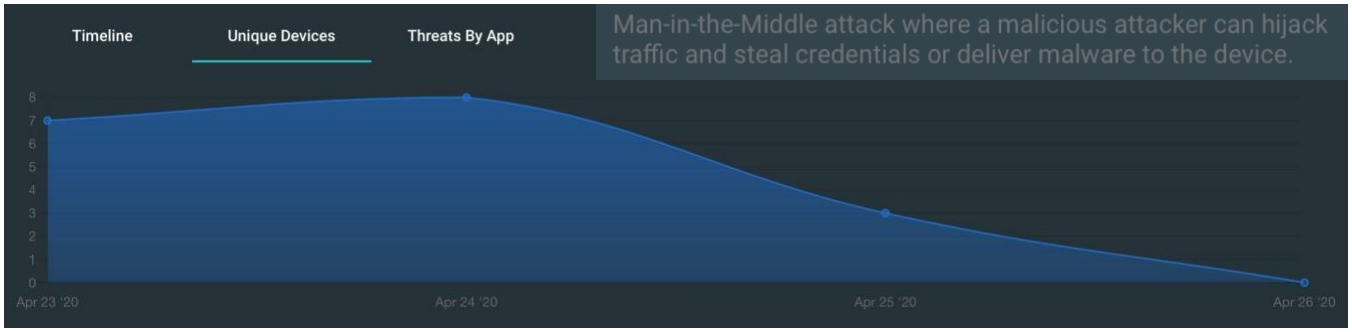
First, the majority of voters voted using an iPhone rather than an Android. However, far more threats were detected at the Android level:



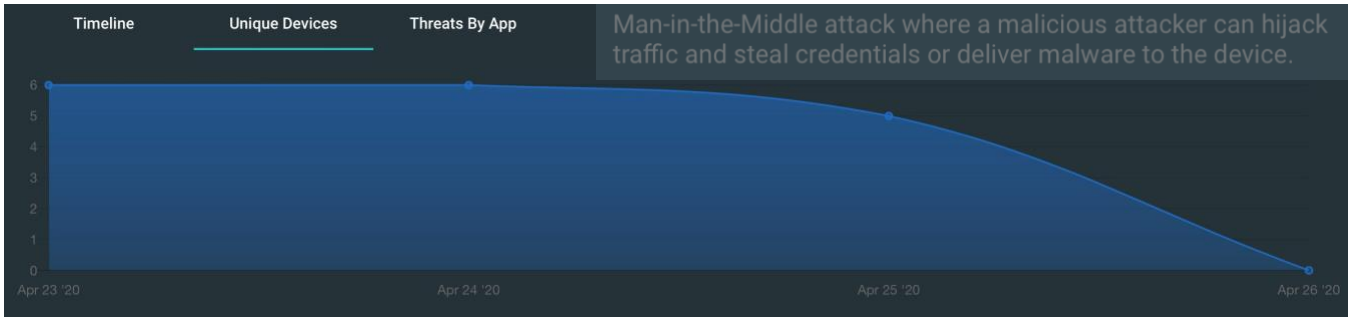
Mitigated Threat: Network Security Threats

A network security threat means that a device is operating on a WiFi network that is not safe. The platform was designed to bar voters from voting using an unsafe WiFi network because it could lead to a "Man-in-the-Middle" attack, or a malicious attacker hijacking traffic, stealing credentials, or delivering malware to the device. If a voter tries to vote on an unsafe WiFi network, they receive error messages and are asked to switch to a different network in order to vote.

# of iOS devices detected with a network threat, over time

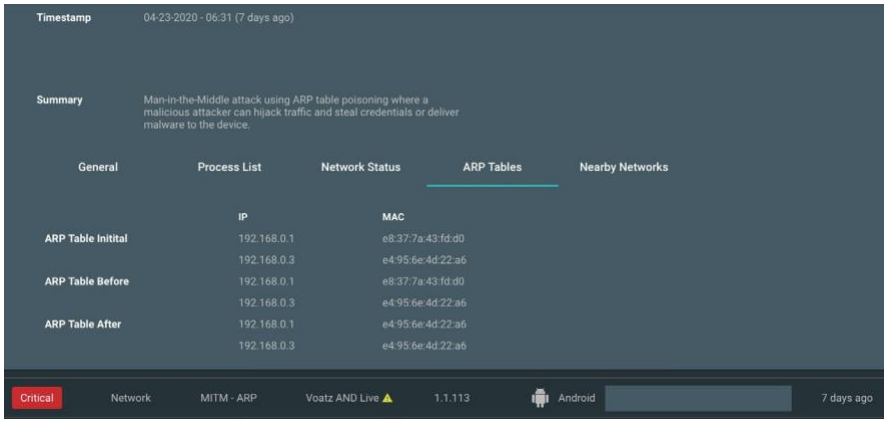


# of Android devices detected with a network threat, over time



Threat detected: Voatz detected (18) iOS devices and (17) Android devices to be operating on unsecured WiFi networks. These voters were unable to submit their ballots as a result.

Mitigation: These voters were asked to switch to a more stable cellular or WiFi network, reboot their device, and then they were able to submit their ballots.



Threat detected: Voatz detected (1) Android device to be susceptible to ARP Poisoning (meaning the device was operating in an insecure network environment, perhaps with an application that was interfering with the network traffic).

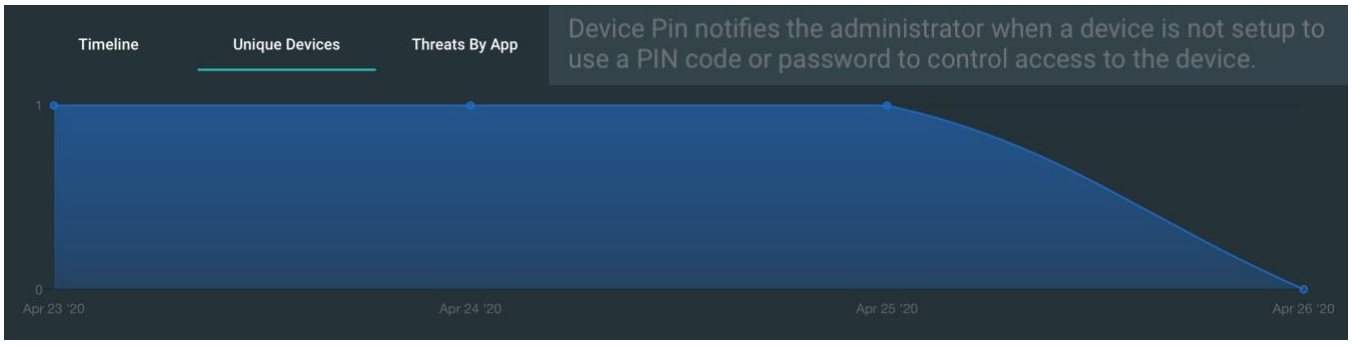
Mitigation: After this cause was discovered, the voter was asked to remove the offending network application from the network and then was able to proceed.

Mitigated Threat: Device Pin Not Set

The platform detects if the user does not have a device PIN set, meaning that either the smartphone's PIN or the biometric feature allowing secure entry into the smartphone has not been activated.

The Voatz platform is designed to block voters from voting with a device that does not have a PIN because it leaves the device susceptible to easier access if an outside attacker were to obtain physical access to the device. This closes a potential vulnerability; if a voter attempts to sign up to receive a ballot through the Voatz platform and does not have a device PIN set, the voter will receive an error until they set their device PIN or enable biometrics.

# of iOS devices detected with PIN not set, over time



# of Android devices detected with PIN not set, over time

Threat detected: Voatz detected (3) iOS devices and (89) Android devices that had not yet set their device pin.

Mitigation: Voters were requested to activate their device pin or biometrics and after, were able to proceed with voting.

Mitigated Threat: Sideloaded Apps

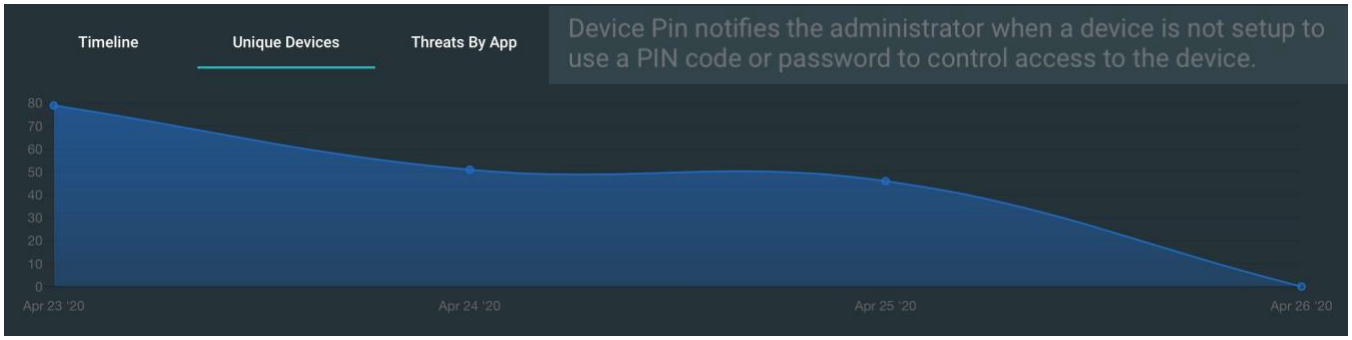
Sideloaded apps are applications that have been installed on a device, typically by bypassing the device's security protocols.

Voatz detects any time a device has a sideloaded app installed because some sideloaded apps can contain malware. Even if the sideloaded app is benign, as an extra precaution Voatz detects this and then analyzes whether or not it is benign. If it is deemed benign, then the voter is able to proceed.

If the sideloaded app contains malware, the voter is requested to remove the application from their device before they are able to proceed and vote.

# of iOS sideloaded apps detected, over time

# of Android sideloaded apps detected, over time



Threat detected: Voatz detected (15) iOS devices and (173) Android devices with sideloaded apps (apps that could potentially introduce a security threat on the device) that were deemed to be benign; Voatz detected (2) Android devices with sideloaded apps that contained malware.

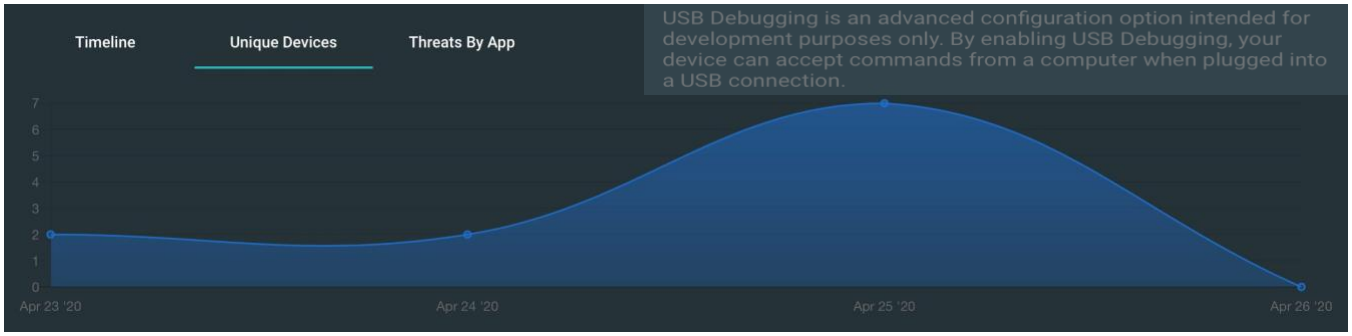
Mitigation: After investigation, the voters with sideloaded apps that were deemed to be benign were able to proceed. Voters who had sideloaded apps with malware were asked to delete the offending apps and reboot their phones, or to use a different device in order to proceed.

Mitigated Threat: USB Debugging Enabled

USB debugging enablement is a threat only associated with Android devices. It lets the device communicate with a computer, and allows access to specialized areas of the phone otherwise inaccessible.

Voatz detects if a device has USB debugging enabled and whether or not that device is connected to a computer. If the device is connected to a computer, the Voatz system will not let a vote be submitted and the voter will receive an error.

# of Android devices detected with USB debugging enabled, over time



Threat detected: Voatz detected (11) Android devices with USB debugging enabled (which allows a smartphone to communicate with a computer).

Mitigation: Because the mobile device was not connected to a computer at the time of voting, voters were able to proceed.

Conclusions

As election and political party officials alike reckon with remote needs for the future voting, it will continue to be important to evaluate the security mechanisms in place for that system's components, and specifically, the difference between the security profile of browser-based versus smartphone app-based systems.

Voatz's layered threat detection mechanisms and their execution during a live election is reflective of a system security that could serve as a model for future election platform pilots: a layered defense system that detects, identifies, and mitigates potential points of entry for the election platform. It reinforces the advantages of the security features of a smartphone, primarily on its ability to detect and prevent tampering or entry through third-party malware. It also provides a real-time breakdown of possible and distinct vulnerabilities at the device level for the two operating systems that are compatible with the Voatz platform.

As expected, network vulnerabilities are not limited to any one device; both Android and iOS devices encountered potential threats at similar volumes and were subsequently not allowed to vote until they joined a secure network.

Overall, Apple devices were shown to perform better on device-level security. The touchpoints necessary for secure ballot delivery, such as device PIN setting, were more likely to be in place, correlated with fewer incidents. Additionally, there were fewer incidents across the board on iOS for sideloaded apps and USB debugging.