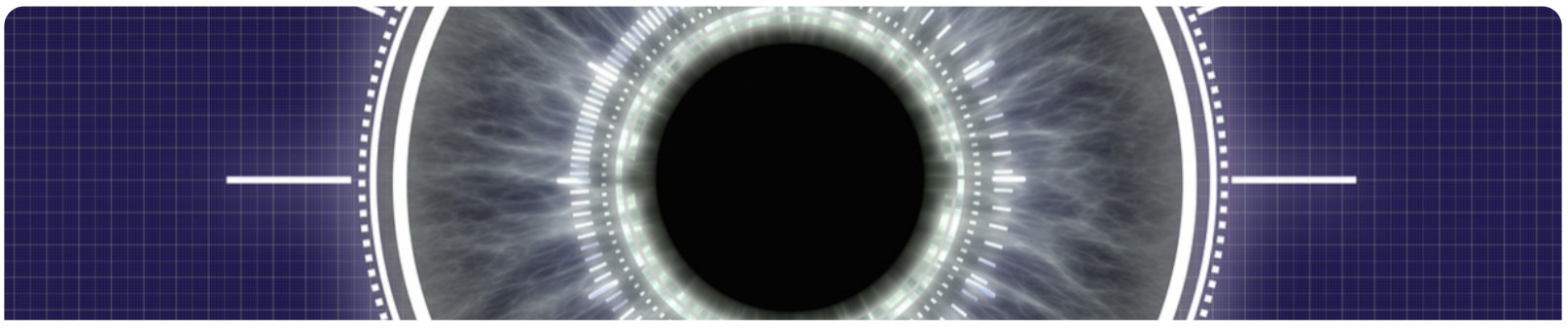
all posts prev | next

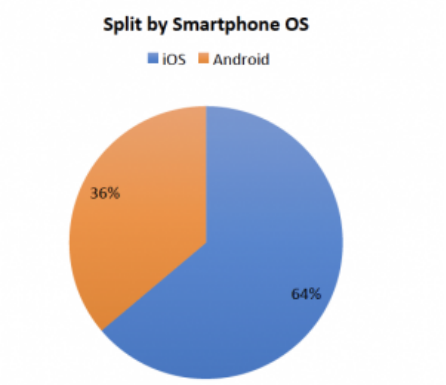


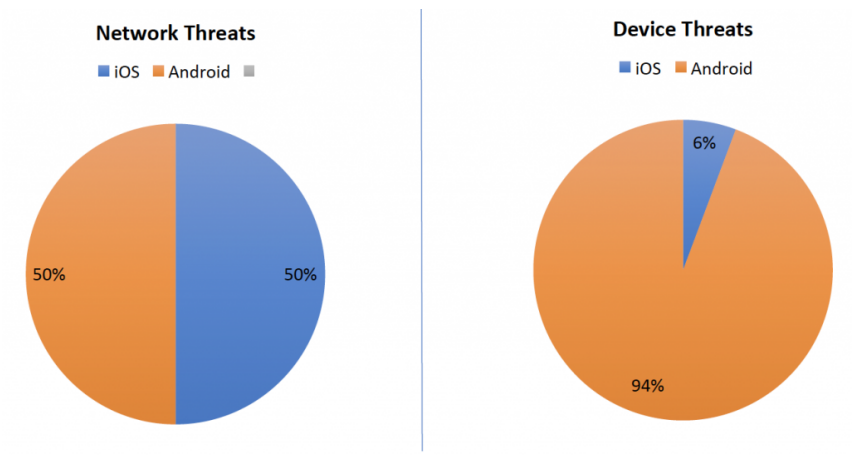
State-of-the-Art Security Performs First-Rate Threat Mitigation in Largest Mobile Voting Exercise

A few weeks ago, nearly 7,000 votes were submitted using the Voatz mobile voting platform. During the election, our advanced security threat detection mechanisms were able to detect, mitigate and thwart a handful of smartphones 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, we combine widely-used threat detection software with our 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.

Threat Mitigation

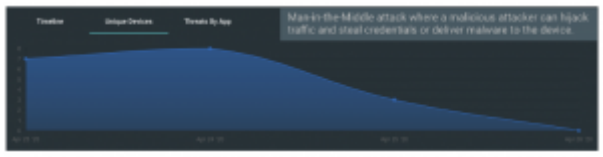
In the election, a handful of voters had compromised devices and were prevented from voting until their device threats were mitigated. In some instances, voters were asked to remove malware on their devices. In others, some voters were asked to delete certain applications or functions they had installed which made their smartphones insecure. These voters were unable to vote until they did so. These cases reveal important, cutting-edge data that indicates the system is capable and successful in both detecting threats at a very granular level, and mostly, ensuring a secure vote. Below includes compelling statistics around the types of malware or applications detected, along with the device type. First, what's interesting to note is that despite far more voters voting from an iPhone, far more threats were detected at the Android level:



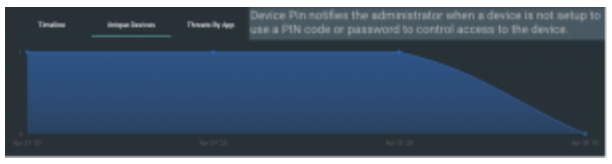


Mitigated Threat: Network Security Threats

A network security threat means that a device is operating on a WiFi network that isn't safe. Voatz doesn't allow

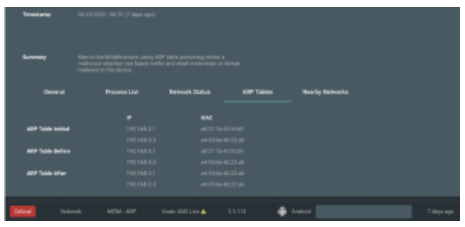


# of iOS devices detected with a network threat, over time



# 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 insecure 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.

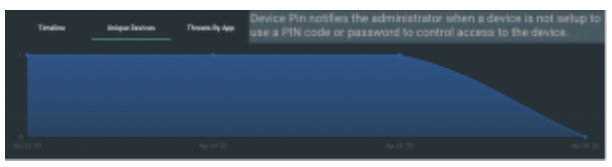


1 Android device threat detected with ARP poisoning

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 appliance that was interfering with the network traffic). *Mitigation:* After this cause was discovered, the voter was asked to remove the offending network appliance from the network and then was able to proceed.

Mitigated Threat: Device Pin Not Set

If a smartphone doesn't have a device PIN set, that means that the person who owns the smartphone hasn't yet setup their smartphone's PIN or activated their biometrics to keep the phone secure (i.e. when they go into the phone, as a safety measure they have to enter the device PIN or use their biometrics to get inside). Voatz doesn't allow voters to vote from a device that doesn't have a PIN set, because it leaves the device susceptible to easier access if an outside bad actor were to obtain physical access to the device. If a voter tries to sign up with Voatz and doesn't have their 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

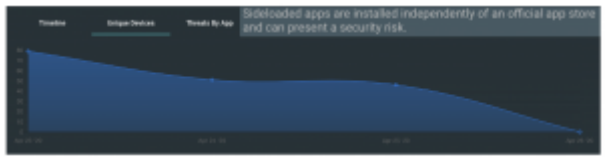
Threat detected: Voatz detected (3) iOS devices and (89) Android devices that had not yet set their device pin. *Mitigation*: They were requested to activate their device pin or biometrics and after, were able to proceed with voting.

Mitigated Threat: Sideloaded Apps

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

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). *Mitigation:* After investigation, the apps were deemed to be benign and the voters were able to proceed.

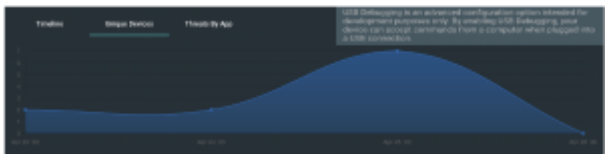
Mitigated Threat: Sideloaded Apps with Malware

Malware detected on Android devices

Threat detected: Voatz detected (2) Android devices with sideloaded apps that contained malware. *Mitigation*: Voters 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.
[Data provided by Voatz Security Operations]

Elections, Technology

all posts

prev | next

Voatz