Written 2/6/2021 by Ryan Hartwig

On Friday February 5th, 2021 I, Ryan Hartwig was already this week speaking to many volunteers in a group chat about the issue of possible irregular behavior in the audit being performed of the ballots at the Maricopa County Tabulation Center and Election Center (MCTEC), located at 510 S 3rd Ave, Phoenix, AZ 85003.

Several members of our volunteer group have a background in IT and were concerned about the Nest cams not functioning properly during the audit. Staci Burk who resides in Arizona, and Matt Van Bibber, an IT professional from Pennsylvania, both witnessed irregularities with regards to the public Nest cams not working properly and also of employees looking at the cameras for inordinate periods of time, using smartphones while inside the tabulation center, etc. In a separate document they will submit their notarized statements.

Around 9:45pm on Friday February 5th, 2021, the volunteers in our group agreed we needed someone on the ground in Phoenix to do a public scan of the public WiFi being used at the election center. I called Aaron Wagner who I've known for at least 7 years, to assist me with this, as a volunteer. He has done IT consulting for family members in the past. Aaron Wagner holds an active CISSP certification, which stands for Certified Information Systems Security Professional (CISSP).

Aaron Wagner, CISSP
NET CONCEPTS AZ
3241 E. Shea Blvd., 179
Phoenix, AZ 85028
602.404.1520
https://ncarizona.net/

I drove to the MCTEC and arrived around 10:20pm. Aaron arrived shortly thereafter. Staying on public property, Aaron scanned the public wifi and assessed the vulnerabilities. He did NOT attempt to hack into or penetrate the hidden networks whatsoever and confirmed this multiple times with me. I also opened an app on my android phone named Wifi Analyzer and saw that there was a network with the name of MCPublic that was an open network.

Based on Aaron's scan, he saw an Apple TV, Xbox, and Nintendo Switch on the public county WiFi Network. At our location, there were no other buildings nearby except the election center, and there was an empty lot to our southwest and an electrical substation to our southeast.

Aaron also scanned and saw a 3Com SuperStack 3 Switch device on the network, which is an outdated piece of equipment from 2014, very vulnerable to manipulation by cyber attacks because of EOL (end of life). There was mention of whether or not it was a managed switch.

Generally speaking, Aaron saw vulnerabilities related to DoS attacks (Denial of Service). Port 80 and 443 were open, but not tested due to that would require authorization.

At one point, we believe someone inside realized we were there doing a public scan because one of the networks changed names to “fuckyou”. The WiFi Analyzer scan on my phone showed that that there were other networks, presumably inside the Maricopa County Election Center, in very close proximity to the “fuckyou” network.

Other observations and questions from Aaron Wagner that he conveyed to me are the following:

1. There are a large amount of wireless networks. A corporate network should not be “Netgearxx”. There were two “Mcxx” networks (Maricopa County).
2. Who created the “fuckyou” SSIDI wifi network name?
3. Who would control APs (Access Points) during an audit? Is that network still up? Who would create a network like that in a county building or business
4. The issue of the old equipment from 2014 (3Com superstack)
5. Why would gaming systems be connected to a network at a tabulation center? It’s likely the networks are on HP equipment (3com being acquired by HP). Why are Foreign APs (access points) allowed to be installed?
6. Consumer Routers are notorious for having vulnerabilities. Consumer routers appear to be in use along with “main” network. Old un-patched wireless access points are vulnerable. Corporate wireless products can suffer the same issues. https://routersecurity.org/bugs.php
7. Aaron is very confident they are not just using the HP equipment. He is fairly certain those other wireless networks were coming from the tabulation center.
8. All networks were encrypted aside from guest and one hidden. It isn't likely tabulation machines on those networks. Getting into those networks would not be legal. Network accessed was public and open for anyone and everyone. Network isolation not configured. Point is, are there wireless networks? YES

Other insights from Aaron Wagner, CISSP:

Something else to consider, USB sticks don't have to be storage. A USB stick could also be a wireless card. I could bring a router and plug it into a hot ethernet port and blam I have a network where data can be sent to the cloud. With so many wireless networks bleeding through you don't have an "air gapped" network. With a public WiFi that was strong enough to bleed through the walls and connected across the street, they could connect the machines easily. They use consumer printers, there was a printer on that network. Not having network isolation means options.

It’s a tabulation center that’s supposed to be air-gapped. You can’t have a public wifi. Those tabulation machines run windows. It’s not a handicapped operating system that can’t use network cards. You could make a really scaled back version of linux that has no capabilities of talking to a network card. We’re dealing with Windows machines that we know have the capability of acting as a full windows desktop.

Myself, Ryan, and Aaron Wagner left the area surrounding the Maricopa County Elections and Tabulation Center around 11:30pm and each drove home separately.

Sincerely,

Ryan Hartwig
Resident of Phoenix, Arizona
BA Spanish Linguistics, Arizona State University