



UNCLASSIFIED//
FEDERAL BUREAU OF INVESTIGATION

Date of entry 11/09/2020

[REDACTED] ([REDACTED]), date of birth (DOB) [REDACTED], cellular telephone number [REDACTED], Email addresses [REDACTED], [REDACTED], Google Voice number [REDACTED], was interviewed at [REDACTED]. After being advised the identity of the interviewing Agents, SA [REDACTED] and SA [REDACTED], [REDACTED], provided the following information:

This interview was audio recorded. The below is an interview summary. It is not intended to be a verbatim account and does not memorialize all statements made during the interview. Communications by the parties were electronically recorded. After approximately 30 minutes into the interview, the audio recording stopped. Therefore, this interview summary captures information obtained from [REDACTED] with and without audio recording. Follow-up questions were asked of [REDACTED] several times throughout the interview to provided clarification. The recording captured some partial responses from [REDACTED], where he later provided more detailed answers after the recording stopped.

[REDACTED] and his wife, [REDACTED], DOB [REDACTED], lived in their residence since approximately 2018. [REDACTED] lived in [REDACTED] from 2008 - 2018 where he worked for himself fixing computers, viruses, installing cameras, and reprogramming programmable logic controllers (PLCs). After moving to Arizona, [REDACTED] obtained employment at [REDACTED] in technical sales and website support from the Fall of [REDACTED] - Spring [REDACTED]. [REDACTED] did not maintain full time employment after separating from [REDACTED]. However, he worked on technical repairs for customers and "moonlighting" projects where he earned roughly \$100 per week.

[REDACTED] utilized his community's Nextdoor app to share election and voting research. [REDACTED] used this site to provide accurate information on the voting process to include sharing county website URLs, statues, and Arizona

UNCLASSIFIED//
[REDACTED]Investigation on 11/05/2020 at [REDACTED], Arizona, United States (In Person)File # 288A-PX-3341832Date drafted 11/05/2020by [REDACTED]

UNCLASSIFIED// [REDACTED]

288A-PX-3341832

Continuation of FD-302 of (U// [REDACTED]) [REDACTED] Interview, On 11/05/2020, Page 2 of 4

records information. [REDACTED] copied this information directly from the Maricopa County website and pasted it into a boiler plate format used on the Nextdoor app. The Nextdoor app was used by more than 900 people and the content was maintained by about six moderators.

Around September 2020, [REDACTED] first discovered a vulnerability in the Maricopa County Recorder's Office website after entering his own voter registration information. He noticed his voter ID appeared in the URL. [REDACTED] tested the vulnerability by entering several seven-digit numbers into the URL path resulting in access to different voter registration information. [REDACTED] developed and tested a PowerShell script, which accessed and extracted the voter registration data from the Maricopa County Recorder's website. [REDACTED] initially grabbed a small amount of data, but decided to stop because the script was not working right. He started thinking of ways to improve on the script to make it better. [REDACTED] estimated that approximately 100 - 1,000 records were taken during this time and referred to this as the "trial run".

Around the beginning of October 2020, [REDACTED] improved his PowerShell script. He ran the script again up until around November 2, 2020, when Maricopa County fixed their firewall. [REDACTED] stated he probably would have continued this activity if the flaw went unfixed. [REDACTED] knew Maricopa County was aware of his activity because his script provided an error message and could no longer generate requests. Between 1,000,000 and 2,000,000 voter registration records were extracted to text files stored on [REDACTED]'s personal hard drives, which he estimated to be four gigabytes (GB) of data. Records were also saved to [REDACTED]'s Google Cloud account. [REDACTED] initially received an adrenaline rush, but realized he made a huge mistake with regrets and remorse. He did not intend to sell the information because it was publicly available. [REDACTED] could have purchased the records, but he wanted to obtain the information for free. [REDACTED] realized the gravity of the situation and became scared. [REDACTED] said he knew he would get a visit from [law enforcement].

[REDACTED] expressed that looking for vulnerabilities was a hobby and described himself as a hacker or tinkerer. [REDACTED] stated he has not conducted recent hacking activity in which he would like to confess. However, [REDACTED]'s first "highlight moment" happened while

UNCLASSIFIED// [REDACTED]

UNCLASSIFIED// [REDACTED]

288A-PX-3341832

Continuation of FD-302 of (U// [REDACTED]) [REDACTED] Interview , On 11/05/2020 , Page 3 of 4

attending [REDACTED] College in [REDACTED], when his hacking activity led to a "meeting with the Dean". [REDACTED] used several hacker tools and scripts, which were stored on USB drives to include Curl, Invoke-Webrequest, and Medaproducts Download Explorer.

[REDACTED] considered telling the news about his actions, but thought it was better kept a secret as it would have brought down a "shitstorm" during the elections. He did not tell anyone of his activity including his wife. [REDACTED] scrubbed and formatted the hard drives with stored records and deleted any stored files from his Google Cloud. [REDACTED] visited another county website, which he believed was Pinal County, to see if it had the same vulnerability. However, he was unable to test the website because he was not registered in that county. [REDACTED] did not scan Cochise County or any other counties for vulnerabilities. He did not visit any county websites after Maricopa County fixed their firewall.

[REDACTED] stored files to his Google cloud tied to the email addresses [REDACTED] and [REDACTED]. He initially believed his Google cloud account was tied to the email address [REDACTED].

[REDACTED] received a pension of approximately \$1300 a month from the City of [REDACTED], [REDACTED] where he worked for 13 ½ years. [REDACTED] stated that he later worked as a [REDACTED] officer, but could not remember an accurate time frame of his employment. He made approximately \$16 an hour plus commission while employed with [REDACTED]. [REDACTED]'s wife made between \$500 - \$700 per week working for [REDACTED].

[REDACTED] provided a final statement and said he was 100% accountable for his actions and was deeply regretful. [REDACTED] apologized and commented that he has to deal with the consequences of his actions.

[Agent note: [REDACTED] invited SA [REDACTED] and SA [REDACTED] to sit in his backyard for a non-custodial interview. Agents explained to [REDACTED] that he was not going to be arrested. Approximately 30 minutes into the interview, Agents advised [REDACTED] that a search warrant was issued for his residence. SA [REDACTED], SA [REDACTED], and [REDACTED] stepped outside of the residence to the driveway while agents cleared the home for safety precautions prior to executing the search warrant. The recording stopped while the search

UNCLASSIFIED// [REDACTED]

UNCLASSIFIED// [REDACTED]

288A-PX-3341832

Continuation of FD-302 of (U// [REDACTED]) [REDACTED] Interview , On 11/05/2020 , Page 4 of 4

warrant was being executed and failed to turn back on for the remainder of the interview. During the search, [REDACTED] was advised that he was free to leave and come back when the search was completed, at which time [REDACTED] chose to stay with Agents in his backyard until the remainder of the search.]

[Agent note: [REDACTED] provided two of his business cards which were placed into the 1a file along with the Agent notes.]

[REDACTED] provided the following personal account information:

Bank Accounts

[REDACTED]
[REDACTED] in [REDACTED]
[REDACTED]
[REDACTED]

Credit Cards

[REDACTED]
[REDACTED]

Social Media

Facebook: Inactive unknown profile name

LinkedIn: [REDACTED]

Indeed: [REDACTED]

UNCLASSIFIED// [REDACTED]