

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Western District of Texas**FILED**

September 03, 2024

CLERK, U.S. DISTRICT COURT
WESTERN DISTRICT OF TEXASUnited States of America
v.BY: SL
DEPUTY

Case No.

1:24-mj-559-DHAubrey Cottle aka: Kirtaner*Defendant(s)***CRIMINAL COMPLAINT**

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of September 2021 in the county of Travis in the
Western District of Texas, the defendant(s) violated:*Code Section**Offense Description*

18 U.S.C. § 1028(7)(A)(C)



Identity Theft

This criminal complaint is based on these facts:

See attached Affidavit.

☒ Continued on the attached sheet.

- ☐ Sworn to before me and signed in my presence.
☒ Sworn to telephonically and signed electronically.

Date: 09/03/2024City and state: Austin, Texas
Complainant's signature , FBI Special Agent*Printed name and title*
*Judge's signature*U.S. Magistrate Judge, Dustin Howell*Printed name and title*

INTRODUCTION

I, [REDACTED], being first duly sworn, hereby state as follows:

1. I am employed as a Special Agent (SA) with the Federal Bureau of Investigation (FBI), assigned to the FBI's San Antonio Field Office, Austin Resident Agency (ARA). I have been an FBI Agent since January 9, 2005. During my FBI career I have investigated various violations of federal law, including but not limited to Cyber Intrusions and other Cyber related criminal activity, National Security matters, Domestic Terrorism crimes, and Weapons of Mass Destruction. As a Federal Agent, I am authorized to investigate violations of laws of the United States.

2. I make this affidavit in support of an application for an arrest warrant for Aubrey COTTLE for Identity Theft, in violation of 18 U.S.C. § 1028(7)(A)(C).

3. As detailed below, Aubrey COTTLE committed computer intrusion by gaining unauthorized access to EPIK Enterprise Solutions (EPIK)¹ computer network in order to deface and download a backup of the Republican Party of Texas also known as the Texas GOP² web server containing personal identifying information. The information was distributed and made available for download on a Torrent. COTTLE claimed responsibility for the attack on multiple social media platforms.

4. This Affidavit is based on my participation in the investigation, the participation of other law enforcement officers, my review of documents and digital data obtained or seized during the course of the investigation, and my training and experience. This affidavit is intended to show merely that there is sufficient probable cause for the requested arrest warrant. It does not set forth all of my knowledge about this matter. All statements are set forth in sum and substance and relevant part.

STATUTES VIOLATED

5. Title 18, United States Code, Section 1028(7) provides, in relevant part, that “[w]hoever knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.”

6. In Title 18, United States Code, Section 1028(7), the term “means of identification” means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any (A) name, social security number, date of birth, official State or government issued driver’s license or identification number, employer or taxpayer identification number; (B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (C) unique electronic identification number or address, or routing code; (D) telecommunications identifying or access device (as defined in section 1029(e)).

¹ EPIK Enterprise Solutions (EPIK) founded in 2009, is an American domain registrar and web hosting company.

² The Republican Party of Texas also known as the Texas GOP is a political organization based in the Western District of Texas. The Texas GOP is the affiliate of the United States Republican party in the state of Texas. The organization functions to reach new voters who share the same conservative values to elect new officials.

7. Cottle's violation of Title 18, United States Code, Section 1028(7) was done in connection with multiple felony violations of the Texas Penal Code, including:

"Section 33.02

(b-1) A person commits an offense if, with the intent to defraud or harm another or alter, damage, or delete property, the person knowingly accesses:

(1) a computer, computer network, or computer system without the effective consent of the owner;

(b-2) An offense under Subsection (b-1) is:

(6) a felony of the second degree if:

(C) the actor obtains the identifying information of another by accessing only one computer, computer network, or computer system."

According to Texas Code of Criminal Procedure (specifically, TX Code Crim Pro art 13A.263 (2023)), violations of Section 33 may be prosecuted in any Texas county "in which an individual who is a victim of the offense resides."

SUMMARY

8. Based on the facts set forth below, there is probable cause to believe that Aubrey COTTLE knowingly and intentionally gained unauthorized access to deface and downloaded a backup copy of the Texas GOP web server containing personal identifying information (PII). The information was then made available for download and distribution on a Torrent³. COTTLE claimed responsibility for the attack on multiple social media platforms.

STATEMENT OF FACTS

9. On September 11, 2021, the Texas GOP website (texasgop.org) was defaced by hackers claiming to be a group known as "Anonymous."⁴ The banner of the website was replaced with cartoon characters, a pornographic image, and a music video. The defacement was the result of an intrusion into the hosting provider EPIK. In addition to the defacement, the actors accessed and downloaded a Texas GOP Apache web-server that contained personal identifying information. The information was made available for download on a Torrent.

³ "Torrent" is a method of distributing files over the internet. Torrents operate over the BitTorrent protocol to facilitate what is called peer-to-peer (P2P) file-sharing.

⁴ [REDACTED]

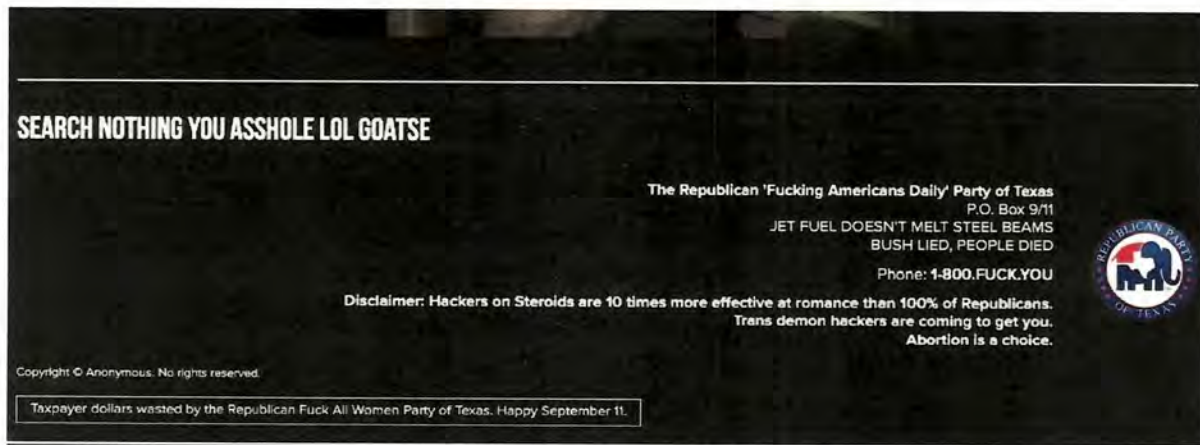


Figure 1: Defaced Texas GOP website

10. Following the attack, CNN published a news article titled, “Epik is a refuge for the deplatformed far right Here’s why its CEO insists on doing it.”⁵ In the article, EPIK CEO [REDACTED] alleged COTTLE was responsible for the breach.

11. Public open source information identified COTTLE claiming responsibility for the hack, including a screen capture of a Discord post by user “Kirtaner #0420” aka COTTLE. In the screen capture, COTTLE wrote, “OH I GAVE THE CHILDREN THE SQLI EXPLOIT VULN GAB CODE ALREADY.” Followed by, “when it hits you’ll never see it attributed to me but... epik hosting’s fucked.” Legal process later served to Discord confirmed these screen captures as COTTLE’s posts to Discord on “420chan,” an anonymous image-board founded by COTTLE in April 2005.

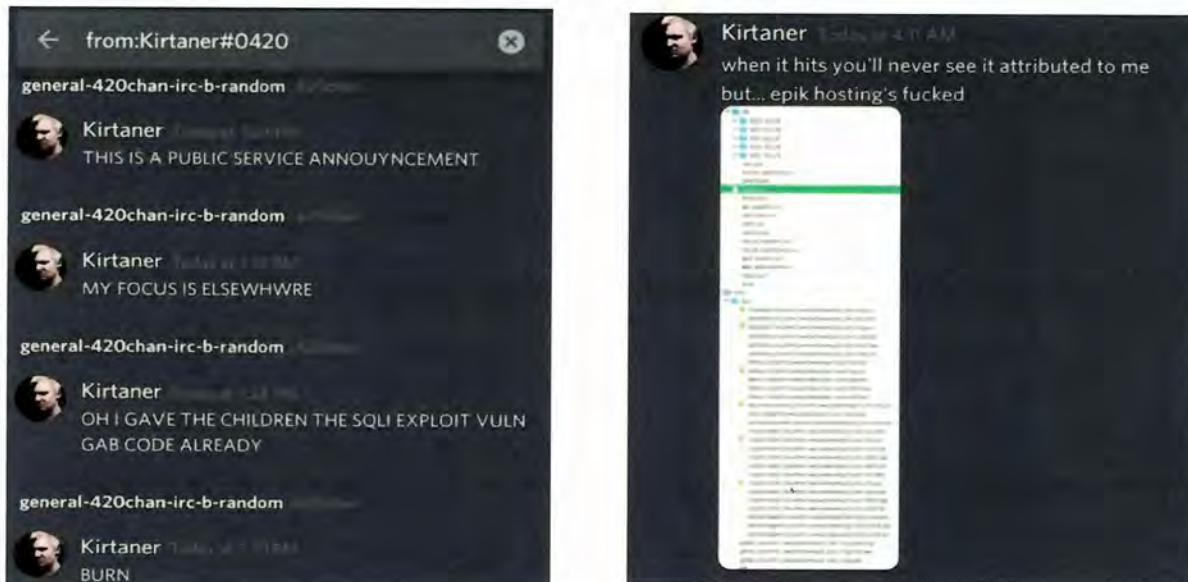


Figure 2: Screen captures of a Discord post by user “Kirtaner #0420

12. In September 2021, Anonymous released a press release announcement about the EPIK hack. In the press release a torrent file was linked containing over 180 gigabytes of stolen data ([REDACTED]). According to [REDACTED], a single source IP address was identified that downloaded

⁵ <https://www.cnn.com/2021/12/09/business/epik-hack-ceo-rob-monster-invs/index.html>

100% of the EPIK data when the file went live. A BitTorrent user utilizing IP address [REDACTED].173 downloaded the compromised Texas GOP data on Tue, Sep 14, 2021, at 2:32 PM CDT. An open-source check of the IP address [REDACTED].173 using WHOIS data identified the internet service provider as Bell Canada (residential). The FBI provided the IP address to OPP, who confirmed the IP address was assigned to COTTLE, [REDACTED], Ontario, and email address [acottle@\[REDACTED\]](mailto:acottle@[REDACTED]).

Address	Link	Flag	Bytes In	Bytes Out	Progress
[REDACTED].173	[Link Icon]	Canada	383 K	89.4 K	[Progress Bar]
[REDACTED]	[Link Icon]	USA	1.09 M	161 K	[Progress Bar]
[REDACTED]	[Link Icon]	Canada	441 K	187 K	[Progress Bar]
[REDACTED]	[Link Icon]	USA	275 K	205 K	[Progress Bar]
[REDACTED]	[Link Icon]	Canada	2.47 M	3.77 M	[Progress Bar]

Figure 2: EPIK screen capture of BitTorrent download screen.

13. I believe, based on my training and experience, as well as conversation with other law enforcement, that a person's IP address is visible to everyone when downloading or uploading a torrent. It is common for the person responsible for uploading and sharing information via BitTorrent to have their initial IP address displayed as completing the upload or download of a torrent. Therefore, I believe this BitTorrent information is evidence that COTTLE distributed the stolen Texas GOP data via BitTorrent.

14. On COTTLE's [REDACTED] page, [REDACTED], COTTLE listed his location as [REDACTED], Ontario, which is right next to [REDACTED], Ontario.

15. Through open-source research, law enforcement discovered a post on [REDACTED]⁶, which detailed information associated with COTTLE to include domain registration information for an address in [REDACTED], Ontario, Gmail account (Kirtaner@[REDACTED]) and phone number ([REDACTED]).

⁶ [REDACTED] is a company and entertainment website that hosts user-generated content.



Figure 3: [REDACTED] screen capture.

16. FBI agents located a TikTok user known as “kirtaner,” which was a public facing account containing videos that appear to be COTTLE. In one video, an individual believed by the FBI to be COTTLE based on his appearance and screen name, claimed ownership for the hack against EPIK.

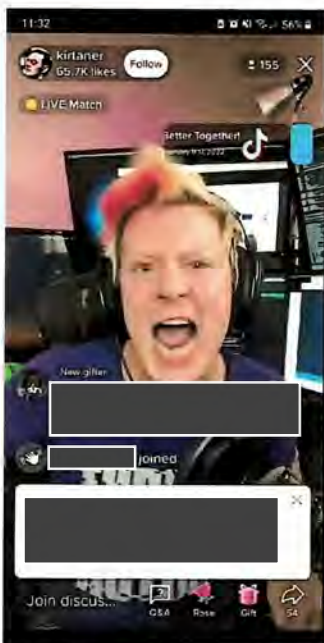


Figure 4: Screen captures of a “Kirtaner” TikTok video

17. In response to legal process, investigators received Discord Inc. information on accounts belonging to COTTLE (Kirtaner#0420). Messages directly related to the EPIK computer intrusion and the Texas GOP were discovered. The context in which the messages were shared suggested COTTLE was “bragging” about the Texas GOP intrusion and took

ownership for the attack. On January 18, 2022, COTTLE posted the following messages on Discord:

- a. 2022-01-18 05:38:21.941000+00:00 Kirtaner#0420:
i also did this to the texas GOP on 9/11.
- b. [REDACTED] 2022-01-18 05:40:17.861000+00:00
Kirtaner#0420: **to the fbi agents reading my discord logs: eat my ass i helped your sedition charges least you could do is pay for my therapy.**
- c. [REDACTED]
2021-09-26 16:02:54.981000+00:00 Kirtaner#0420: **The hack comprised more than 180 gigabytes of data from Epik, which is known for providing services to websites that host far-right, neo-Nazi, and other extremist content. The hack was described as "a Rosetta Stone to the far-right" because it has allowed researchers and journalists to discover links between far-right websites, groups, and individuals. Distributed Denial of Secrets (DDoSecrets) co-founder Emma Best said researchers had been describing the breach as "the Panama Papers of hate groups".**
- d. [REDACTED]
2021-09-26 16:03:19.686000+00:00 Kirtaner#0420: **Aubrey Kirtaner Cottle, a security researcher and co-founder of Anonymous, declined to share information about the hacks origins but said it was fueled by hackers frustrations over Epik serving as a refuge for far-right extremists.**


18. The Ontario Provincial Police (OPP), Canada served a judicially authorized search warrant on COTTLE's residence located at [REDACTED], Ontario, Canada. Approximately 20 terabytes data was seized. The following are a selection of examples of data found on a computer owned by COTTLE and found at his residence:

- a. Sender acottle@[REDACTED]
Recipient [REDACTED]
Message Sent Date/Time - UTC+00:00 2/26/2021 3:17:14 AM
Message: **I have root on Epik Networks. I have access to all of their customer VMs, their domains, their customer data. I can hijack Gab's domain. I am dumping 900GB of client VMs at this very moment. Delete this message after reading.**

[REDACTED]

- b. Sender acottle@[REDACTED]

Recipient [REDACTED]
Message Sent Date/Time - UTC+00:00 9/9/2021 10:30:02 AM
Message **oops i control the texas GOP**
Read Status Read



Stolen GOP data located on COTTLE's computer

19. Canadian law enforcement also seized a one terabyte Western Digital Solid State Drive at COTTLE's residence in Canada. A review of the drive revealed a file folder titled "EpikFailYouLostTheGame" located within a file folder titled "Dumps."

20. Within the folder "EpikFailYouLostTheGame" contained the following file names: [REDACTED].xz⁷, [REDACTED].xz, [REDACTED].xz, [REDACTED].tar⁸, [REDACTED].tar.gz⁹, [REDACTED].xz, [REDACTED].sql.gz¹⁰, and [REDACTED].sql.gz.

21. The file folder labeled "[REDACTED].tar.gz" contained a subfolder labeled "[REDACTED].tar", which contained additional subfolders. Based on my review of the subfolders, there were file folders labeled by two-digit numbers and four-digit years. With the subfolders were various legislative documents. For example, one document titled "[REDACTED].pdf" contained full names, county seat locations, email addresses, and phone numbers of individuals.

22. Additionally, the "[REDACTED].tar" contained the following documents:
- a. Applicant Resumes containing name, mailing address, contact number and email address.
 - b. Ballot Application Checklist for District Attorney and State Representatives.
 - c. [REDACTED].pdf (General Rules for All Conventions and Meetings).
 - d. Special Session Call Item: Strengthening Patient Protections Relating to Do-Not Resuscitate Orders.
 - e. Republican candidate endorsement letter
 - f. [REDACTED].pdf.
 - g. [REDACTED].doc (contains PII: date of birth).
 - h. County Court at Law, County Criminal Court, County Probate Court Ballot Application Checklist – 2020 Primary Candidate Application Review.
 - i. Emails routed through "[REDACTED].epik.com" to various @texasgop.org emails. [REDACTED]
 - j. Emails from info@texasgop.org to infor@texasgop.org, where new users entered their email address to sign up for Texas GOP updates (user email address shown in email field).

⁷ The "XZ" compression is a high-ratio data compression tool that is used to compress files in Linux environment.

⁸ "TAR" short for Tape Archive, a TAR file is used to store multiple files in one to send over the internet or for archiving purposes; a group of files, packaged as one file.

⁹ The "TAR.GZ" file extension is created when compressing archived TAR files with the GNU zip utility.

¹⁰ A file ending in ".sql.gz" is a compressed version of a MySQL database file; a compressed archive.

23. Based on my review of the digital evidence received from the OPP, COTTLE had a copy of the stolen EPIK data on digital devices in his possession and bragged about acquiring it before the public distribution via BitTorrent.

CONCLUSION

24. COTTLE gained unauthorized access to the computer servers operated by EPIK and leased by the Texas GOP and without authorization downloaded Texas GOP data that was stored on EPIK servers and defaced the Texas GOP website in violation of the above-referenced Texas state felony statute. Dozens of the email addresses and resumes containing PII within the stolen Texas GOP data were received from individuals located within the Western District of Texas, and the Texas GOP, were located in the Western District of Texas.

25. Based on the foregoing, I submit there is probable cause to believe Aubrey COTTLE committed violations of federal law within the Western District of Texas and elsewhere. Accordingly, I request the issuance of a warrant for his arrest.

E ic



FBI Special Agent

Subscribed and sworn to me via telephone pursuant to Federal Rule of Criminal

Procedure 4.1 on September 3, 2024.



HONORABLE DUSTIN HOWELL
UNITED STATES MAGISTRATE JUDGE
WESTERN DISTRICT OF TEXAS

UNITED STATES DISTRICT COURT

for the

Western District of Texas

United States of America

v.

Case No. **1:24-mj-559-DH**

Aubrey Cottle aka: Kirtaner

Defendant

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay*(name of person to be arrested)* Aubrey Cottle

who is accused of an offense or violation based on the following document filed with the court:

- ☐ Indictment
 ☐ Superseding Indictment
 ☐ Information
 ☐ Superseding Information
 ☒ Complaint
- ☐ Probation Violation Petition
 ☐ Supervised Release Violation Petition
 ☐ Violation Notice
 ☐ Order of the Court

This offense is briefly described as follows:

18 U.S.C. § 1028(7)(A)(C), Identity Theft



Date: 09/03/2024

City and state: Austin, Texas

Issuing officer's signature

U.S. Magistrate Judge, Dustin Howell

Printed name and title

Return

This warrant was received on *(date)* _____, and the person was arrested on *(date)* _____
 at *(city and state)* _____.

Date: _____

*Arresting officer's signature**Printed name and title*