VENEMY

A Collection and Intelligence Tool for Venmo

conINT 2020 | October 17 2020

root@ubuntu:~/conINT_2020# _

Michael - @mportatoes

- CEO and Lead Analyst at Amarok, Inc.
- Former Red Team Operator within the DoD, Threat Hunting at Deloitte
- Featured in the Raspberry Pi magazine (3x), has presented at Defcon 27 (Crypto & Privacy Village), Shmoocon XV, and many other conferences
- TraceLabs Missing Person CTF Winner (Layer8 2019, Team Cymru RISE 2019)
- OSCP, OSWP, CISSP, CEH, CRISC, Sec+, BS & MS from Auburn
- Enjoys video games, tinkering, board games with wife, and being a #GirlDad (2x)

Neal - @Shad0\\\`Rec0n

- Senior Analyst
- CISSP, Sec+, Net+, CEH
- Husband, Father, Recon Marine
- TraceLabs Missing Person CTF Winner (2x incl. Defcon 27), DerbyCon VIII SECTF 3rd Place

VENMO OVERVIEW

- Mobile app allowing P2P transactions with a social aspect
- Acquired by PayPal in 2015
- 52 Million users (2020) (~16% of the USA)
- $37 Billion net payment volume in Q2 2020 – 52% YoY growth
- 50 percent of users are between the ages 25 to 34

Source: https://www.businessofapps.com/data/venmo-statistics/

VENMO IN THE NEWS

- "Security Research of a Social Payment App" (2014) – MIT grads
- Vicemo (defunct, 2015) – Who is buying drugs, booze, and sex on Venmo
- publicbydefault.fyi – research on public transactions by Hang Do Thi Duc (2018)
- FTC throws down (Feb. 2018)
- Mozilla launched a campaign to make transactions private by default (2018)
- The EFF and Mozilla published an open letter to PayPal to fix Venmo's privacy holes (Aug. 2019)

VENMO VS ZELLE

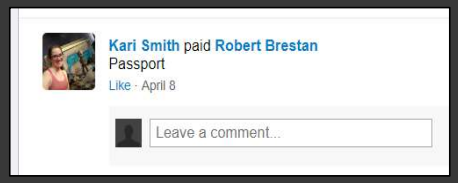
vs.

$75 $300

Per transaction

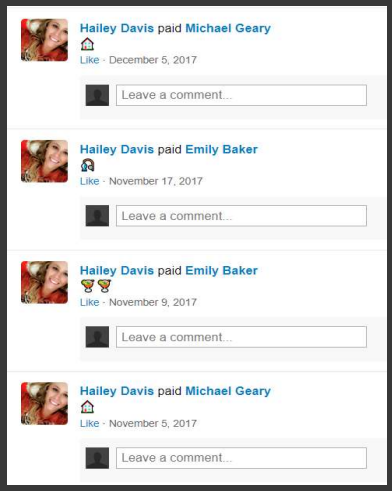
VENMO DATA TELLS STORIES

Travel?



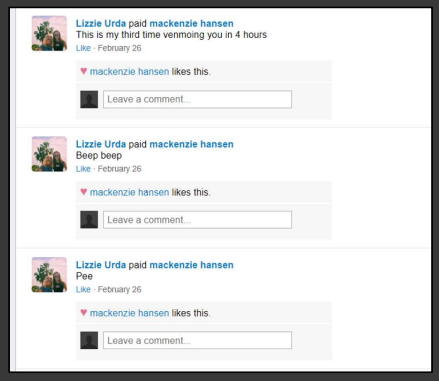
Birthday?

Roommates?

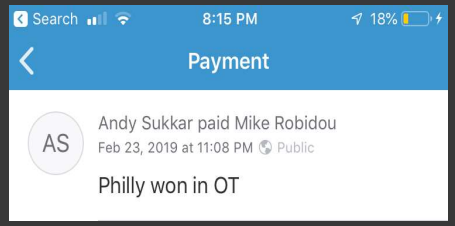


Getting Married?

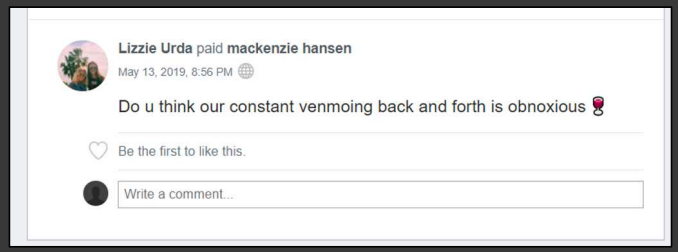
Besties?



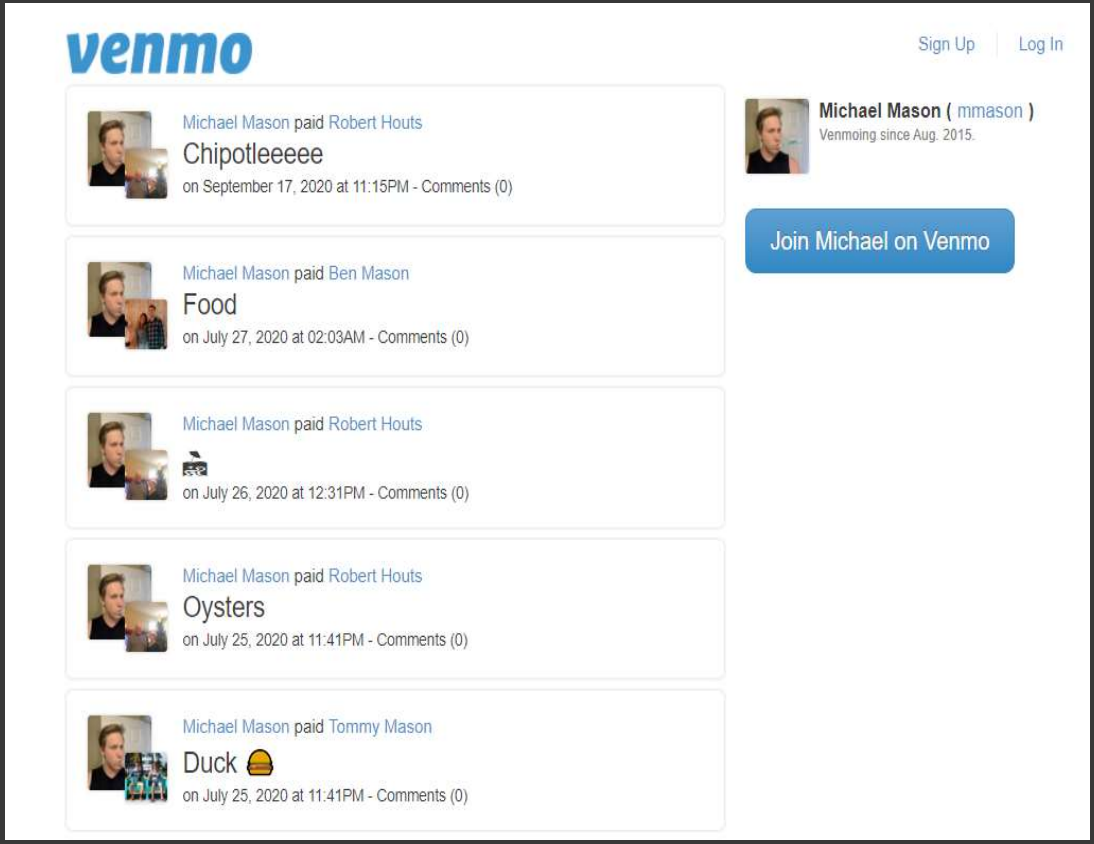
Gambling?



Wine Night?



VENMO DATA TELLS STORIES



Screenshot above is public profile available via normal web browsing

- What was he likely doing 06/25-06/27?
- Tommy Mason – Relative?
- Ben Mason – Relative?
- Hobby – Foodie?
- Pattern of Life – night owl?
- Likes Chipotle? Me too

Information ? Intelligence

INFOSEC USE CASES

- Red Teams:
  - Reconnaissance
  - Spear-phishing scenarios
- Blue Teams:
  - Pro-active defense, personnel exposure
- Counter-Intelligence/Law Enforcement:
  - Building a network of persons of interests
  - Identifying suspicious transactions
  - TraceLabs Missing Persons CTF
- Personal
  - Identifying scams

DISCLAIMER

- Please use this for being an infosec hero, not a zero
- Use at your own risk
- Not responsible for misuse
- Recommend the OSINT usuals:
  - VM
  - VPN
  - Common User Agents
  - Burner phone or service for 2FA
  - Sock Puppet Account
  - LXC for the super paranoid

TOOL OVERVIEW

- https://github.com/mportatoes/venemy
- Written in python3, native libraries
- Authenticated and Unauthenticated options
- Installation and sample analysis can be found in the repo
- Neo4j used for graph analysis but awesome alternatives exist!

WHAT CAN WE GET?

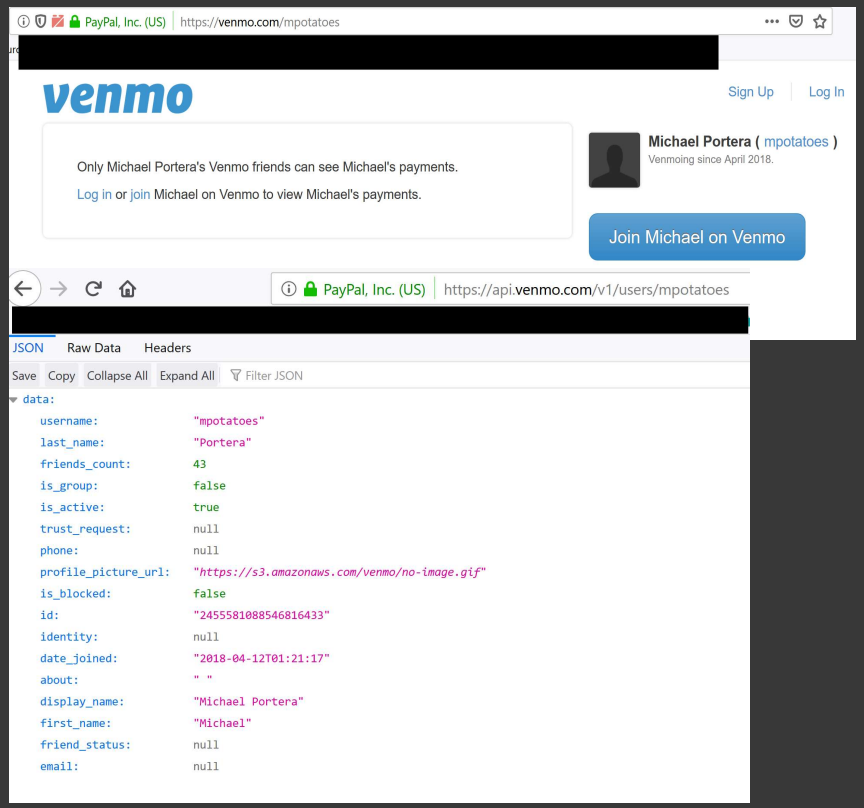
- Excellent APIv1 documentation for all endpoints and fields can be found here by mmohades
- Authenticated:
  - Friends list, friend of a friend (FOAF)
  - Access to more API endpoints
  - **All** previous transactions
- Unauthenticated:
  - Last five transactions
    - Timestamps, transaction ID, parties involved, item/description, profile pictures (w/possible link to Facebook), "Likes"/Comments

API IN 2020

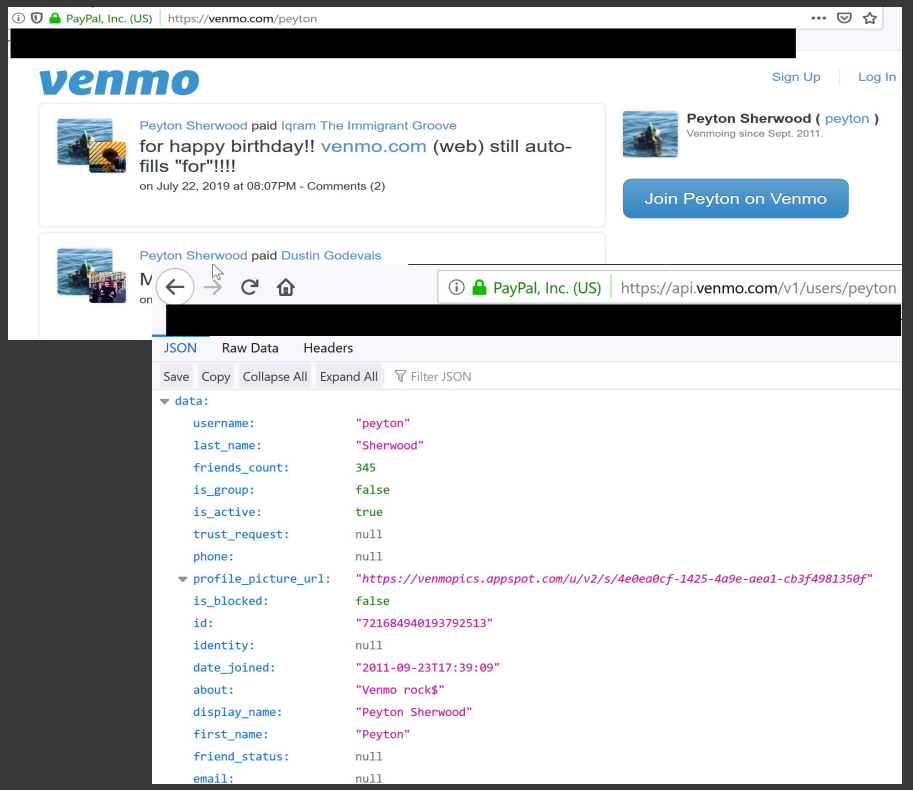
- Changed some time in 2020 to Oauth
- API keys available to any authenticated user, no signups or additional steps
- API key doesn't expire
- Process automated thanks to this code and integrated into Venemy

PRIVATE VS PUBLIC

Private Profile (Unauth)

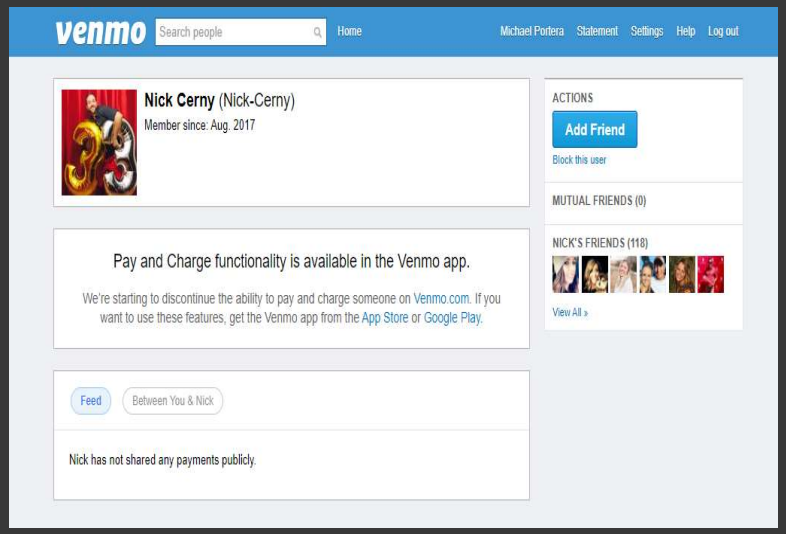


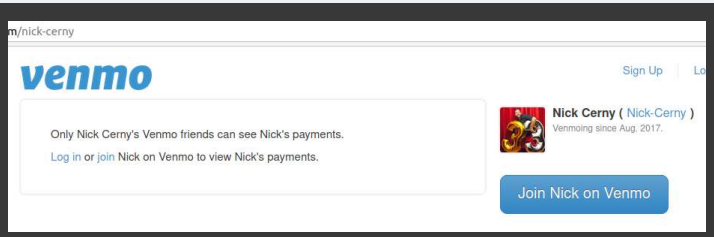
Public Profile (Unauth)



PRIVATE VS PUBLIC

Private Profile (Auth)

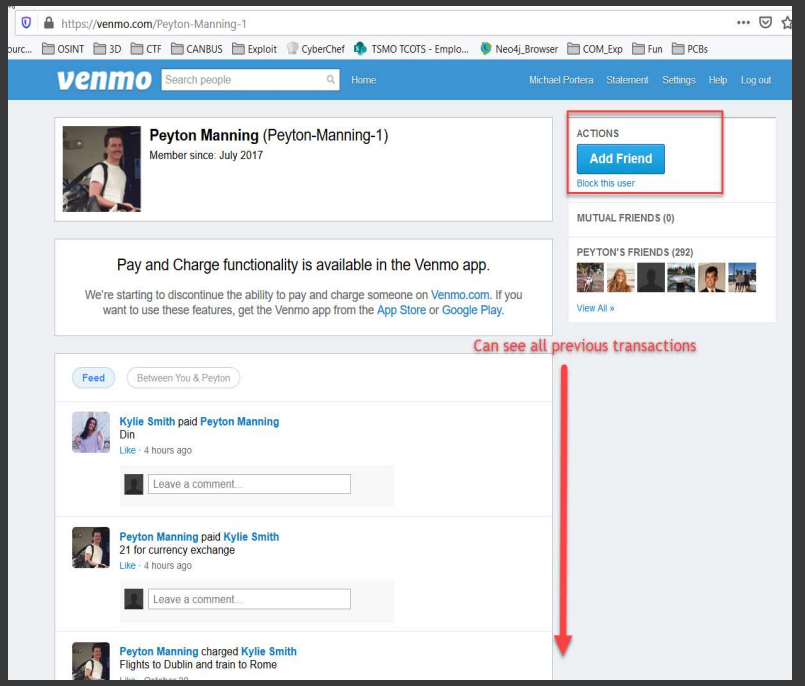




API calls reveal all of these details in formatted JSON.

This is for visual purposes only.

Public Profile (Auth)



FRIENDS LIST

- When setting up the mobile application, it will import your contacts and look up those users by their details
  - *"Venmo will use the names, phone numbers, and email addresses of your contacts to friend those that use Venmo, help you invite those that don't, improve your search results and as noted in our Privacy Policy."*
- If the other party has no social media but uses Venmo, your public profile will show a connection to you
  - Example: Person A isn't friends with shady character, Person B, on any social media but Venmo found his number when importing contacts and now they are connected online

ANALYSIS WITH NEO4J

- Neo4j Graph Database
- Neo4j community edition is fully-featured and FREE
- Free training materials and Free certification
- Cypher Query Language
- InfoSec projects:
  - Bloodhound
  - ODIN
  - Vulnerability and Exploit Research (Analyzing RPC w/ Ghidra and Neo4j)

ALTERNATIVES TO NEO4J

- Anaconda (python, pandas, numpy, jupyter lab, etc.)
- ArangoDB (this has become my go-to at work)
- Maltego Transform (never done one, looking into it)
- Any RDBMS
- Excel
- Note:
  - Venemy puts everything in a csv format to make any of the above easy

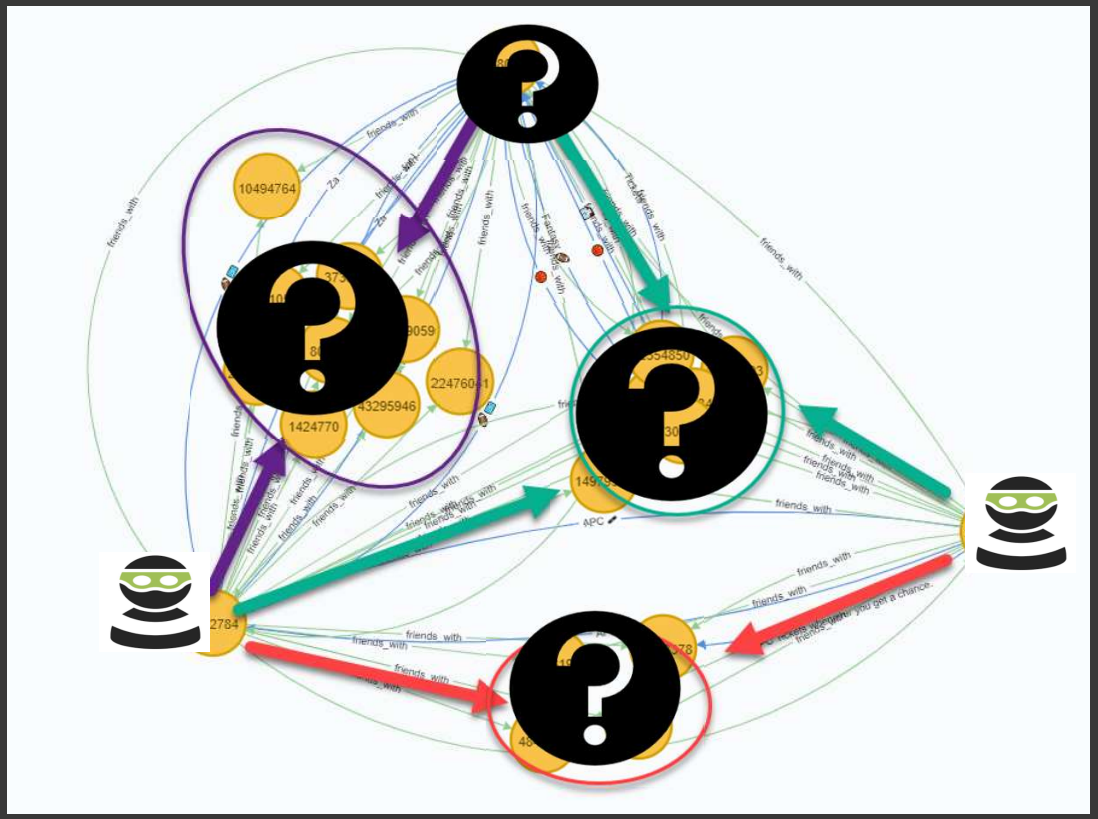
All depends on what's important to your investigation

CI/LE: TRACE LABS

- Find a target's profile on Venmo by (user)name, find their friends
- Find those friends on other social media and see if they uncover any new profiles pointing back to the person of interest
- Use different options in Venemy for identifying a profile and gathering all the things

Tip:
Usernames, aliases, friends, social media profiles, key items within pictures, timestamps, and locations can earn points in the TL CTF.

CI/LE: SUSPICIOUS ACTIVITY

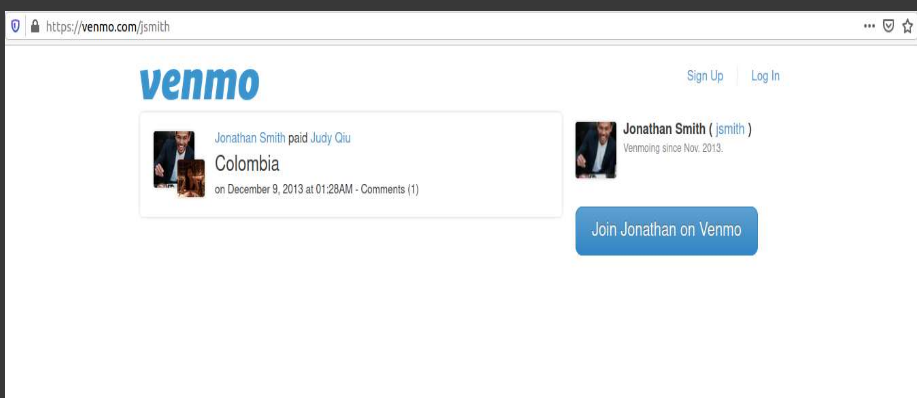


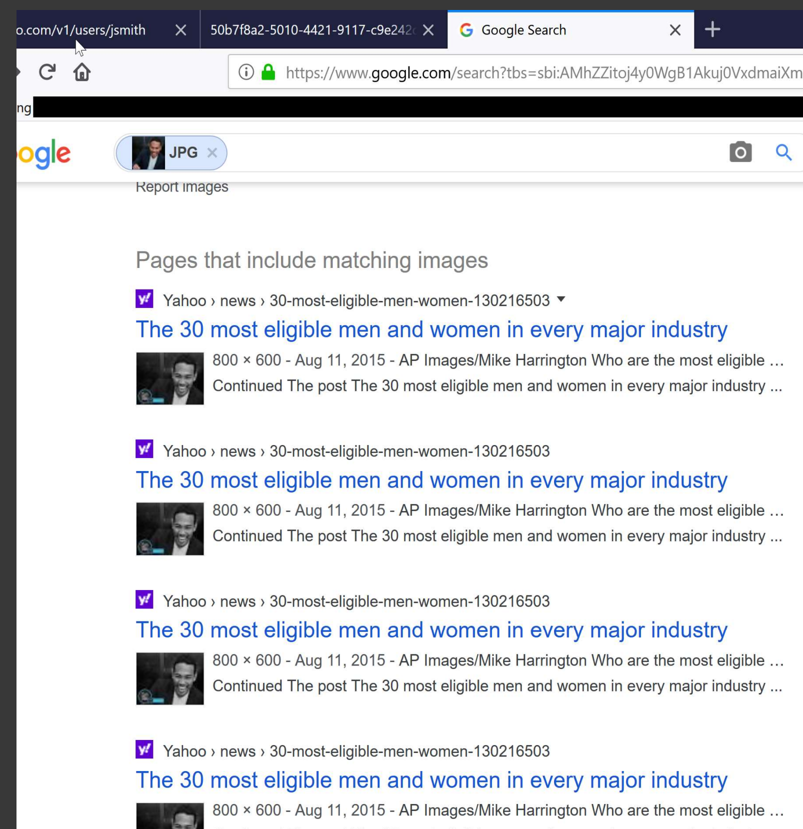
- Whose are the common contacts amongst the persons of interest?
- Are there different/new contacts from other social media outlets?
- Anybody that's not a "friend" but payments are being made?
- Are there recurring purchases or weird emojis?
- Is the time of day suspicious?
- Silly Millennials
- #FollowTheMoney

DEMO

EXPANDING OUR OSINT

- Reverse image search for more profiles (Google, Tineye, etc)

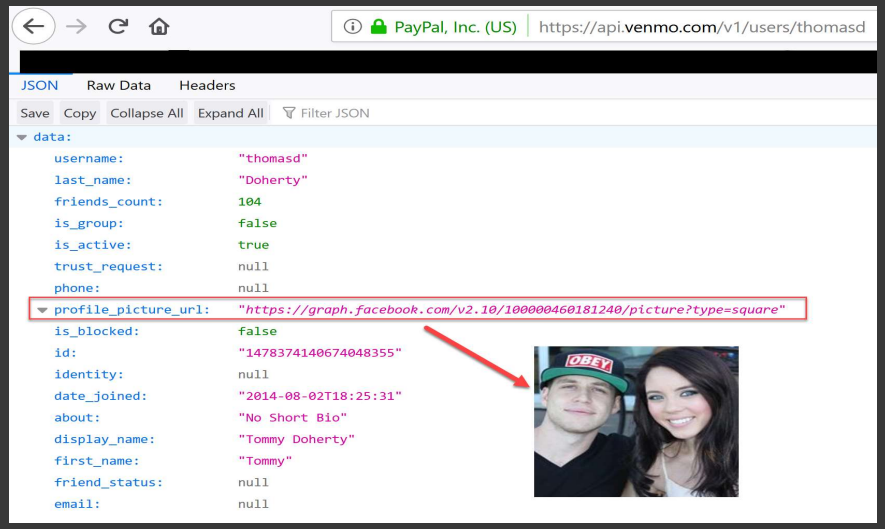


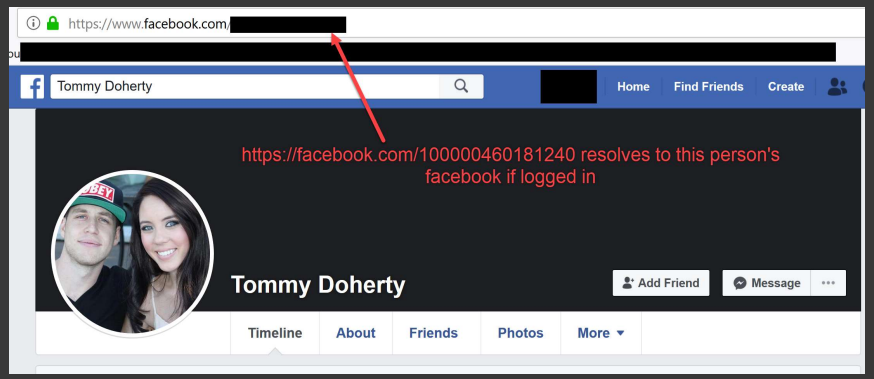


Use the –p flag to download images of friends profiles

EXPANDING OUR OSINT

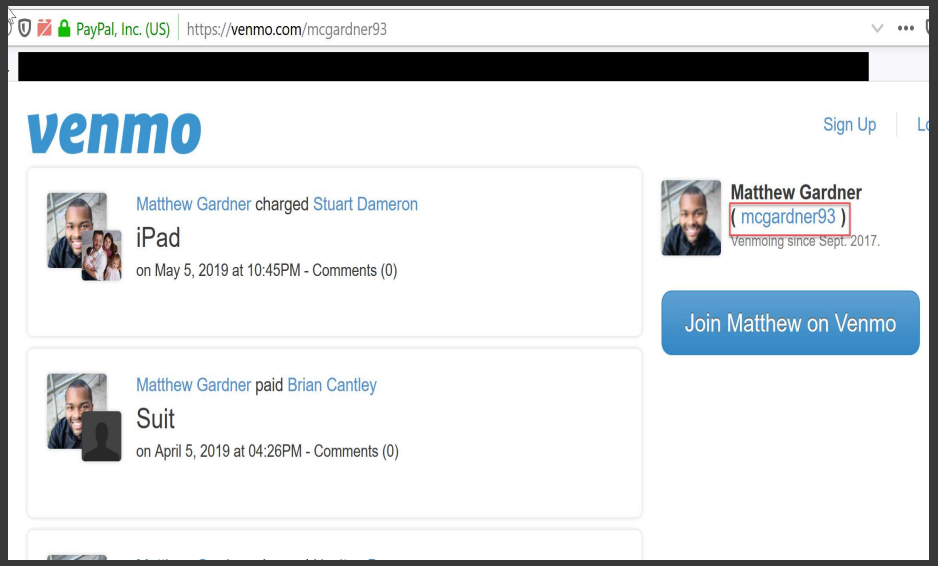
- Facebook UserID to Email
  - Can change picture size via ‘picture?type=[square,large,etc]’

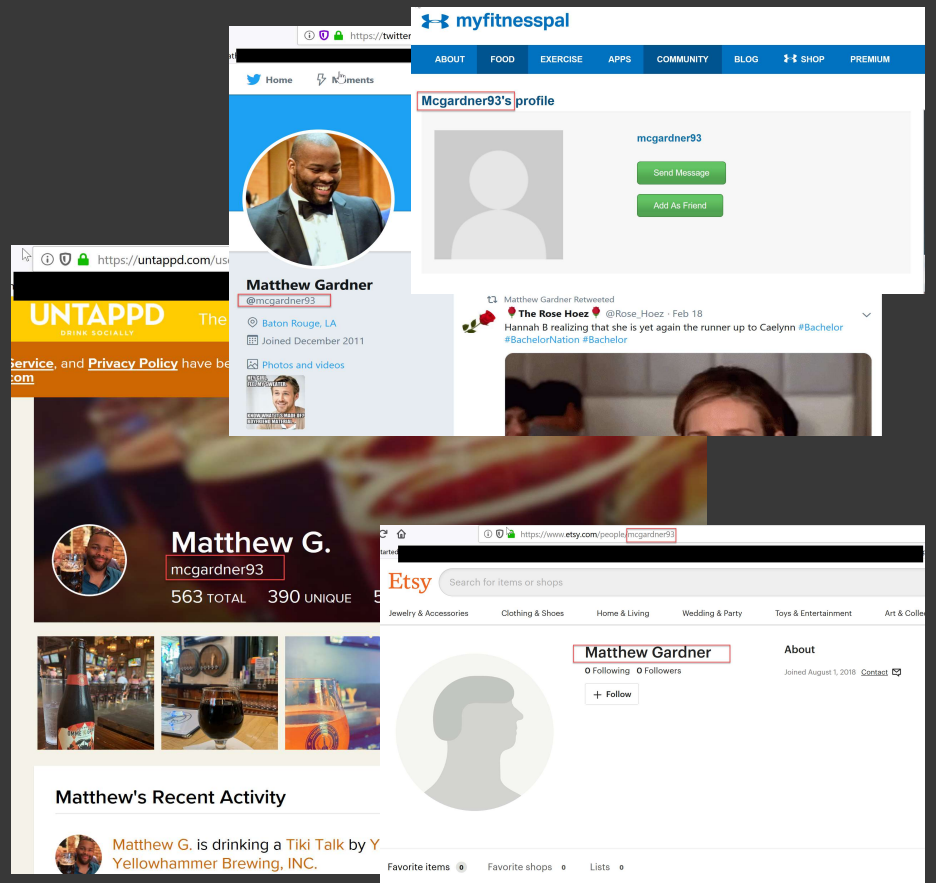




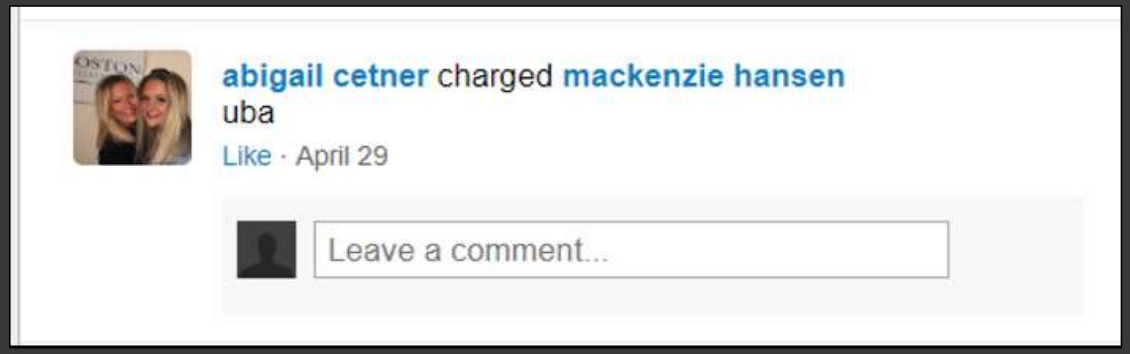
EXPANDING OUR OSINT

- Pivoting to other profiles
- Automated tools to expedite e.g. username sherlock, spiderfoot, awesome-osint





OFFENSE: SOCIAL ENGINEERING

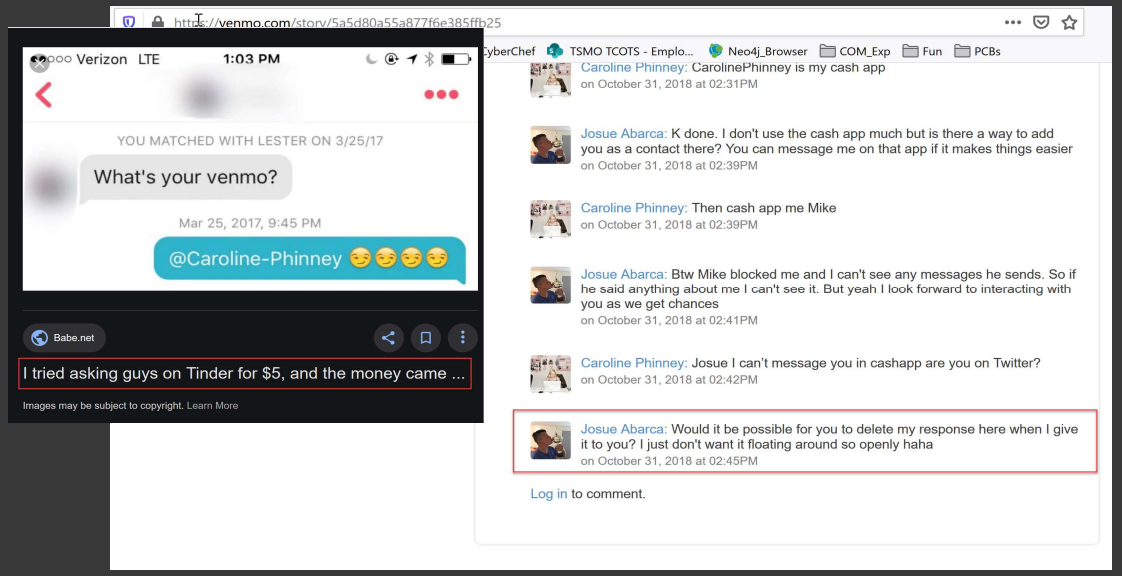


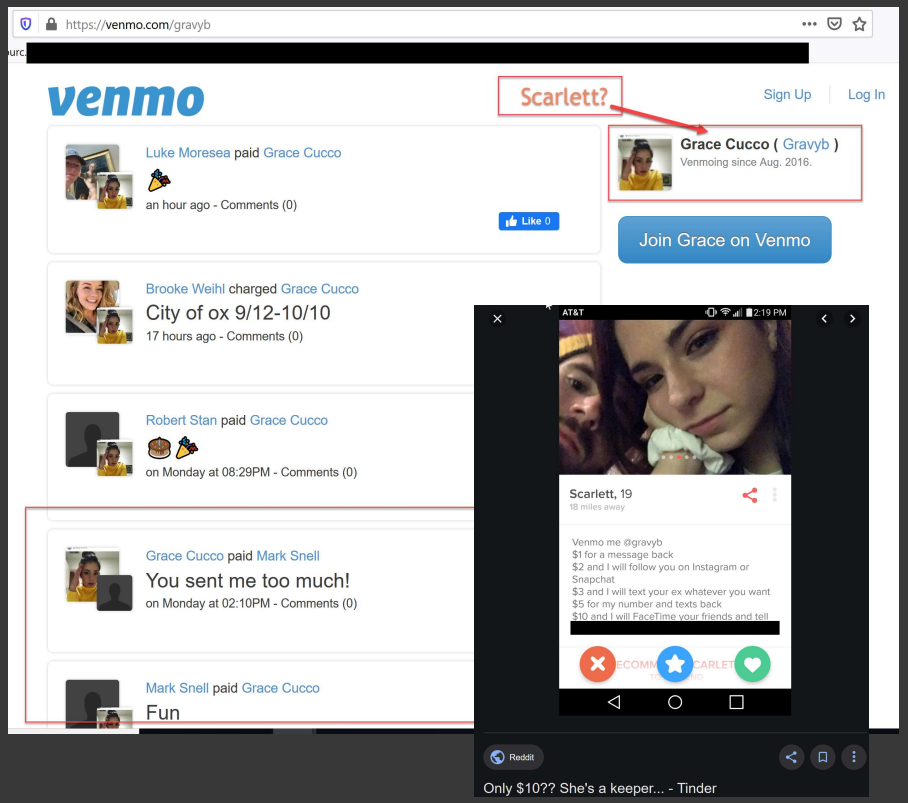
To: cetner@email.com
From: noreply@ubersupport.tech
"There was an issue with your transaction on April 29…please see the attached or visit <>"

To: hanzen@email.com
From: noreply@venmosupport.net
"There was an issue with your transaction, 1a2b3c4d, on April 29 with Abigail Cetner. Please <>"

PERSONAL/LE: SCAMS

- Personal Security: Detecting scams





TIPS

- Set Profile and Transactions to Private
- Set PAST transactions to private