Chad Ballay

CYBR 430-342N

11/29/2020

**Week 2 LAB**

**What is the domain name for Happy Accident Labs?**

<http://www.happyaccidentlabs.com/>

Performed a google search for the phrase "Happy Accident Labs" and verified content of site was in line with what I would expect given the information at hand. (Had to suspend disbelief since google also returned a few other results that are from other people's work on this project. I'm guessing this was created in conjunction with Douglas Rausch and Aurora Cybersecurity? <https://sites.google.com/a/auroracybersecurity.com/happyaccidentlabs/>)

**Who is the domain name provider?**

Godaddy.com is the Registrar. Ran this using the Sysinternals tool for whois. Confirmed the response when looking at this using some of the other web based whois tools.



**Do they have an email provider or do they provide this service internally? If external who is the provider?**

Did a MX Record lookup. Wanted to continue on trying to figure out local tools to use and found out how to use nslookup.



They use an external provider called mailgun. Researching them and it appears it's a mail as a service company. Mostly geared for programmaticlly being able to send mass emails but also for other scaling issues that a company would face. <https://www.mailgun.com/>

**Who might be a good technical point of contact?**

Their DNS record list this as the mechanism for getting a technical contact communication started. This pulls up a form that will mask who it is you are contacting with GoDaddy acting as the broker.



**What might be the address of their company? Phone number(s)?**

Address is listed on their homepage.



Decided to try using an automated tool for finding phonenumbers listed on the website but had some Python/pip setup issues. (<https://github.com/enjoys-sashimi/contact-scraper>) For now I eyeballed the phone numbers from the DNS record and the website itself. Only phone number I found was on the careers page.



**What type of building are they in?**

Multi-tennet, commercial building in an dense urban setting. Lots of brick and businesses. Starbucks and other type resteruants for daytime lunches or upscale evening meals. Not much for residential type activities. <https://goo.gl/maps/MqAShqdbMmFJqjkE6>

**What is the area like around their offices? Can you think of any opportunities for Social Engineering encounters?**

Multiple corporate offices and various ancillary type businesses. Starbucks would be a good initial point to observe the area from. To the east is a public library which could also serve as a base of sorts. The north has a multi story parking garage which could also be used for observation. Several resteruants are nearby. For an extended period Farnam Executive Suites is nearby for a more permenant operations point.

**Are there any email addresses you found?**



russells@happyaccidentlabs.com

**Do you know anything about their network or potential access to their network?**

With just passive tools at this point no. A road trip to walk the permiter would be worthwhile for gathering more information. With some research using one of the public datalakes like Skyhook, we might be able to identify their network SSID and start with that information. Enumerating DNS records for this IP block might provide us with some other sub domains. Same with brute forcing likely ones. ([ftp.happyaccidentlabs.com](ftp://ftp.happyaccidentlabs.com/))

**Did you find any other potentially useful information?**

Based on the footer it's being hosted/created using Google Sites. I don't know the relevance of that but it's a piece of information for later. Same with the job posting. On it's own it's not that relevant but it lets me know of a person in their system, technologies that they use, email userid formats in their system. Perhaps the use of a pfSense firewall based off of the job posting will be relevant.