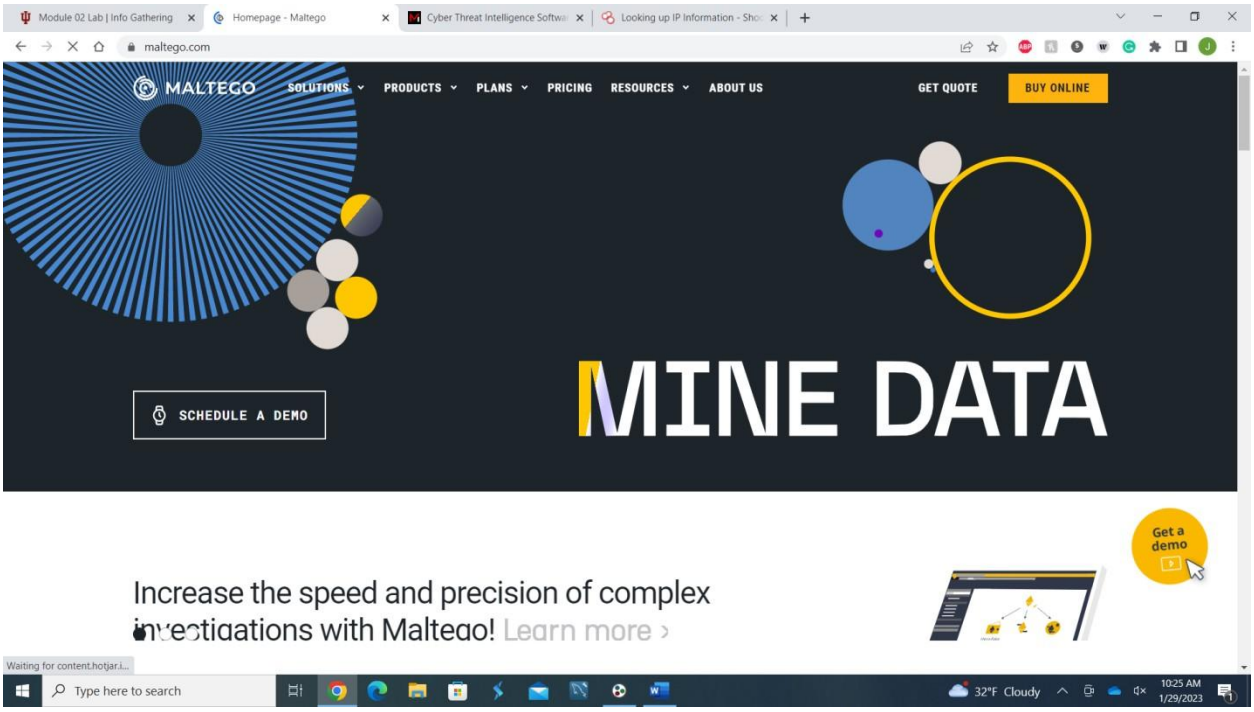
OVERVIEW:

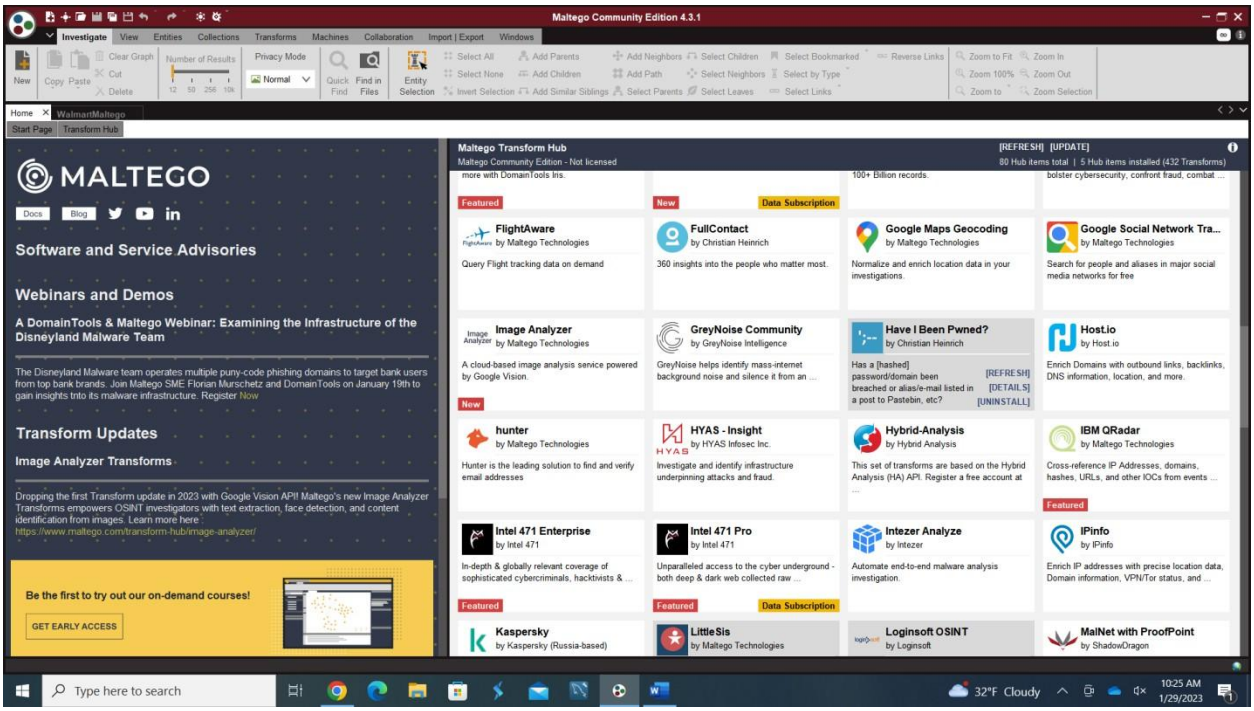
This lab focused on exploring the vast amount of publicly available data and utilizing tools like Maltego to visualize and analyze that information. Maltego CE, the free community edition of Maltego, enables data discovery from open sources. For this exercise, Walmart.com was selected as the target for information mining. Using Maltego CE, various publicly accessible details such as DNS names, IP addresses, phone numbers, and personnel could be uncovered. This process provided hands-on experience with reconnaissance, highlighting the extent of exposed data and underscoring the importance of better data protection.

ANALYSIS:

The first step that was taken was to install Maltego CE. This could be found on their website.

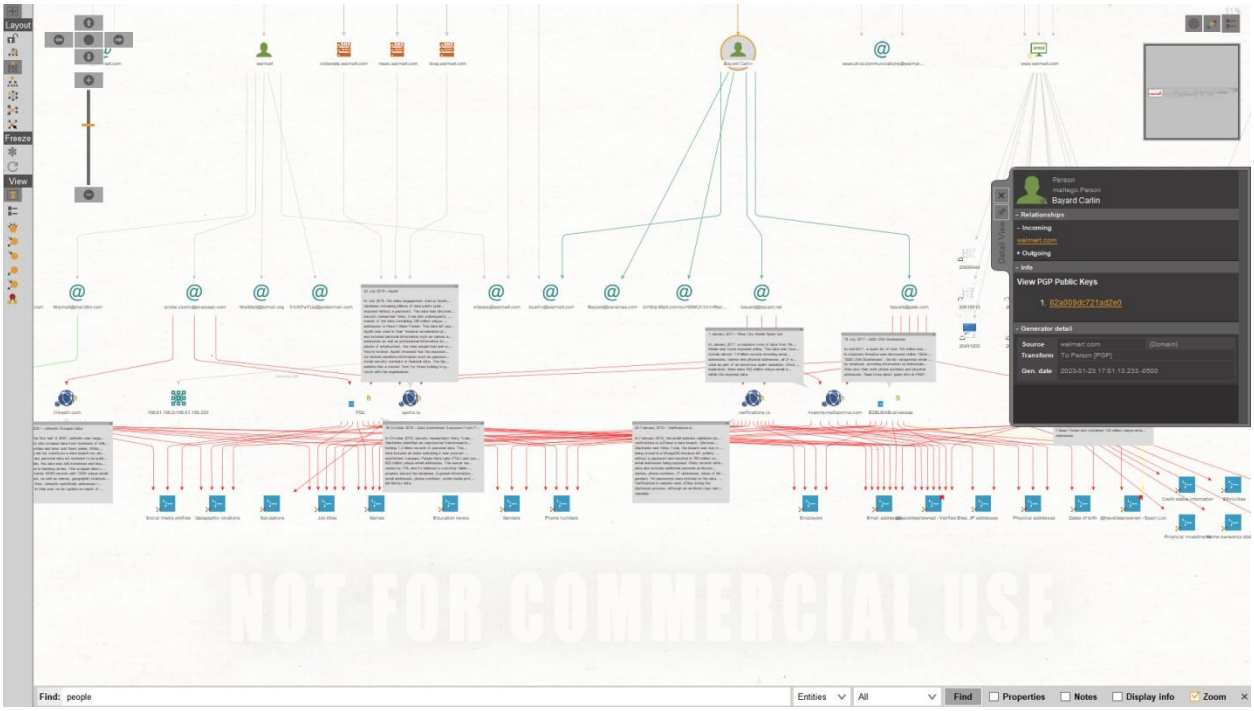


After downloading the Maltego CE it was installed on the system and then ran. Plugins were then installed to assist in the recon. For example, HaveIBeenPwned.

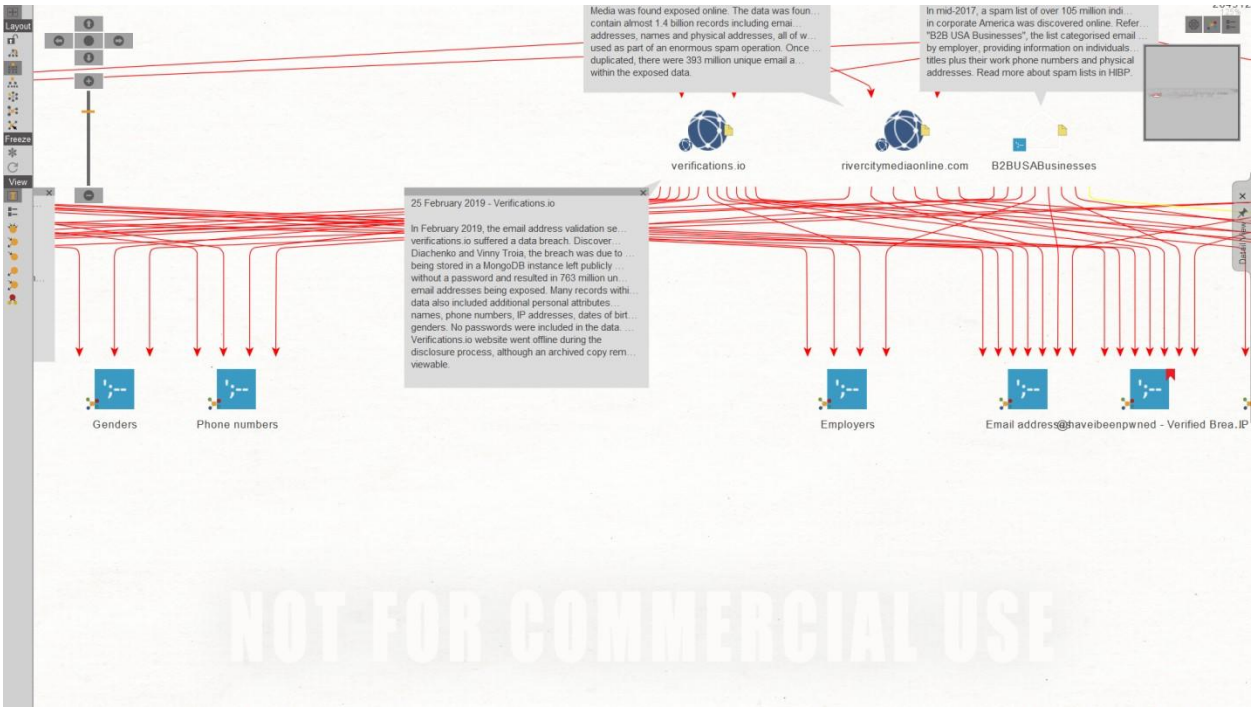


Walmart has then chosen as the target company that the recon was going to be used on. Using various different commands different public information was able to be pulled just based off of the Walmart.com domain. This includes phone numbers, ips, domains, personnel, emails, geolocations, and more.

Some interesting data that was able to be obtained was the fact that of the few employee emails that were pulled some of them have been pwned in the past. Using the HaveIBeenPwned tool you were able to see that employee Bayard Carlin has been pwned on multiple email addresses. Using that information, you could go the different breaches and look for his information.



It appears the most recent breach that affected him was the Verification.io breach of 2019. It was a massive breach that effected hundred of millions of accounts. If you wanted you could go the breach and find out more information like personal attributes, phone number, DOB, ip address, gender. No passwords were compromised in this breach. This doesn't mean the information isn't valuable. You could with this information use it in a social engineering attack, or an attack were you impersonate Bayard Carlin



Overall, a lot of good information was able to be pulled.

.