Sample Pretexting Scenario

Amy Devine

09/30/2021

Abstract

1 Research

For this effort, I chose Drew Barrymore for my target.

Using Maltego 4.2 Community Edition inside Kali Linux as primary tool for collection of data evaluation of that data. The target selected was a famous person.

Initially, the target's name was entered into Maltego and all transforms ran against it. No results were returned.

From Google, one of their online aliases was found (@drewbarrymore). A new graph in Maltego was created with the seed entity as an Alias with @drewbarrymore.

This alias was found at all the social media sites, which seems reasonable given that they are a famous person with a brand to maintain.

I picked tumbler to validate the link. Turns out that the tumbler page (found in the properties of the returned entity for the target) is a fan page that is maintained by someone else.

I'm a fan of spotify so checked that out next. The same handle has only 5 followers and 1 public playlist. Might not be the same person. Github also has the alias registered but 0 contributions. This could be a marketer just buying up the accounts for brand management purposes.

From the Maltgeo graph, I cut: Spotify Blogspot Github Disqus Steam Soundcloud Wordpress

Let's find one that seems active.

From the initial Google search for the target, Instagram was a top result. I don't see Instagram on Maltego nor Facebook in Maltego CE but it looks like an added transform for the pay versions. Easy enough to login and search FB and IG manually.

At this point, I switched from primarily using Maltego to using other OSINT tools out there. I found socialbearing which gives me a dashboard of tweets for a user.[3]

We can see that the target has an iPhone. Verified with a few photos off of IG as well. This could be useful in determining how we might deliver SMS or other cellphone based content, or as a pretext topic.

Figure 1: Social Media transforms for alias @drewbarrymore

From IG, we were able to find out that the target has a new book out Rebel Homemaker produced her own magazine DREW. FB resulted in the target being a vintner and partnered with Carmel Road to produce a Rose, Pinot Grigio and Pinot Noir.

I wanted to personalize the corresponence of the pretext. To do so, I needed a reasonable person to impersonate. I know I can get more information from instagram. This video was helpful in giving other ideas for searching IG.

I went back to Instagram. I found an IG Follwer Extract tool extension for chrome. Using that, I can download who follows Drew. I was thinking I could find her good friends this way but she has over 14 million followers. The list of who she's following is also very long as well. I would like to have found a way to import those people into Maltego (again probably in the pay versions) and then overlap with other projects of hers. Ideally, I wanted to find a person and their boss, as recommended by Kevin Mitnick: add in authority.

I started to look for her kids. Kids Olive (8) and Frankie (6.5) Barrymore Kopelman, in 2021. They are kept mostly out of the spotlight.[1] This feels like a dead end.

facebook.com/DrewBarrymore, recently spoke at the FastCompany Innovation Festival this year. Drew owns: Flower Beauty, Flower Films, Barrymore Wines, The Drew Barrymore Show,

At the FC festival, she spoke on "The Case for Optimism: A Conversation With Drew Barrymore". In the month of September, she announced on FB that she was now the Chief Mom Officer for Quorn using #quornpartner.

t 

Figure 2: Chief Mom Officer

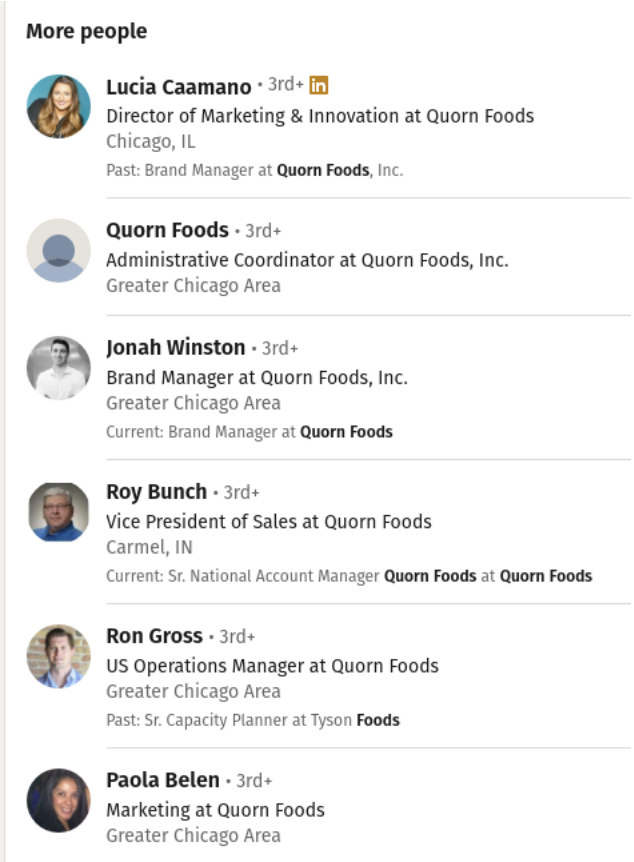

Figure 3: Marketing people at Quorn

September 24, 2021 - Drew announces on FB that she's a QuornPartner. Drew was raised as vegetarian till age 27 and is now a flexitarian. Given her green and holistic views on lifestyles, this seems like a good angle to start with. It's a recent partnership from the FB posting.

Looking at LinkedIn, we can find the CEO and the Director of Marketing and Innovation and someone who probably works for the Director of Marketing.

2 PreText

Dear Ms. Barrymore,

Thank you for being our Chief Mom Officer! We are so thrilled to have you and your platform behind our mission to provide healthy food for people and the planet. My boss, Lucia Cammano Director of Marketing & Innovation at Quorn Foods, has asked me to share some of our upcoming holiday marketing content. We hope it will resonate with your audience as we head into the holiday season!

I have attached a link to our online store of creative content. Please use the password: QuornPartner when you click online. I cannot wait to get your feedback!

Sincerly, Paola Belen Marketing at Quorn Foods Greater Chicago Area

References

[1] https://people.com/parents/valentines-day-2021-drew-barrymore-rare-photos-daughters-frankie-olive-will-kopelman/

[2] https://www.youtube.com/watch?v=DV8hUcdK2Bk

[3] https://socialbearing.com/search/user/drewbarrymore

[4] https://www.quorn.us/