Palantir Presentation

Howdy! How's everyone doing tonight?

(audience)

Who here has heard of Palantir?

(audience)

Palantir is a startup founded by these guys in 2003.

I shit you not they named their company after the evil all-seeing-eye stone from the Lord of the Rings.

And to go along with that they do a lot things like uhhh spy software for federal government or spy software for the military or even spy software for private companies. They're really a jack-of-all-trades.

And I'm only being a little bit facetious there.

Here is a leaked document for their program XKEYSCORE Helper, which you'll remember an NSA tool used to sort through the vast amounts

of data collected from the mass surveillance program XKEYSCORE.

I first really started paying attention to them earlier this year when the Trump admin tapped them to centralize all federal government data on U.S. citizens.

Though I should say, they're really big players in the stock market so I found out from this comically-evil ass article.

Basically every article you'll find about them looks like this by the way.

Now, with Palantir playing such a big role in the government's ability to spy on you, it's pretty damn important that we have an idea on what the hell they're doing and what they're like.

They're a very secretive so it's not really possible to just ask what they're doing.

I mean you can try but I don't think they'd like that.

So the next best thing would be to analyze their products and the tools they use to build them.

This will allow us to get a sense of the type of company that Palantir is.

Sort of like a negative image of Palantir.

Oh! That's the name of the talk.

I had a couple of choices for which product I could look into for this.

There's the government data analysis software, Gotham but information about it is quite hard to find so that's gonna have to be for another day.

There's the military and CIA spy software, AIP but I'd like to keep my nuts disconnected from a car battery and being waterboarded doesn't sound fun. So that one's out.

But then there's this one, Palantir Foundry.

It's main purpose is data analysis for private corporations.

That one seems like a safe bet.

So we've got our target, how do we go about researching it?

There's very little on Palantir's website; certainly no URL or anything.

I tried checking for subdomains, enumerating directories; everything you could think of against the Palantir.com domain.

Nothing. Nada. I was SOL.

If I couldn't find anything on Palantir.com, I looked elsewhere.

I did some google dorking—that's an advanced hacker technique also known as "googling it"—and with this query, I got an interesting result.

This is a technical onboarding document for Palantir Foundry and on page 10, bingo.

Palantirfoundry.com

Going to that domain doesn't get me anything but, like the document suggests, if I go to a subdomain, I get a response.

It redirects me back to Palantir.com for this error page but this is still very good news.

We have a lead.

By the way that error page just reflects whatever you put in the URL.

I just thought that was funny.

Okay, so, now that we know that subdomains are the key, I went about fuzzing them.

In case anyone's curious, this is the command I used.

I used a program called “ffuf”; it’s a really good and simple web fuzzing tool.

Anyways, when it finished, I had 170 responses.

And to my surprise, only a few of them sent me to that “Network Blocked” page from earlier.

Most of them sent me to a login page that looks like this.

I didn’t try very hard to login or anything because that can get into some legally grey areas and I do not want to see the inside of a cell.

Though I did notice something.

I’m gonna use Wal-Mart’s Foundry portal as an example here.

If I put in some dummy email like test@walmart.com, it redirects me to a Microsoft login page.

And this only works if you use a Walmart.com email. It doesn’t work with any other email domain.

So under the hood it's probably checking against some backend SSO service.

Which means that, hypothetically, if you wanted to get in, all you would need is some stolen credentials from a company on this list.

Though you really shouldn't hack Palantir. It's generally a bad idea to hack into a company with a CEO like this.

But that's beside the point.

We can see by looking some of these domains up on Shodan that quite a lot about these servers can change.

On the left hand side we've got Samsung's subdomain and on the right we have Walmart's subdomain.

Notice how these are hosted on opposite sides of the world and have competing server providers.

This suggests that the domain points to servers controlled by the client or at least operating in

the same environment as the client’s other servers.

So let's be clear about what this evidence is telling us.

We have client-specific authentication, client-specific hosting providers, and client-specific server locations.

This isn't a one-size-fits-all software service.

This is a deliberate architectural choice.

Okay, with all that in mind, what did our negative image reveal about Palantir.

I think it shows that Palantir is not some monolithic fortress unable to be penetrated, but rather they’re likely integrated in their client’s environments.

This means that they’re only as strong as their weakest client.

We can also take a reasonable guess that their more government focused products do the same.

They're probably also directly in the environment of whatever government agency they're servicing.

Hell, they might even share vulnerabilities.

With that said, I think I've done enough speculation for one night.

All of my notes are on this github repository in case you wanted to use them.

And I believe I have enough time for questions.

(Answer questions from the audience to the best of my ability)