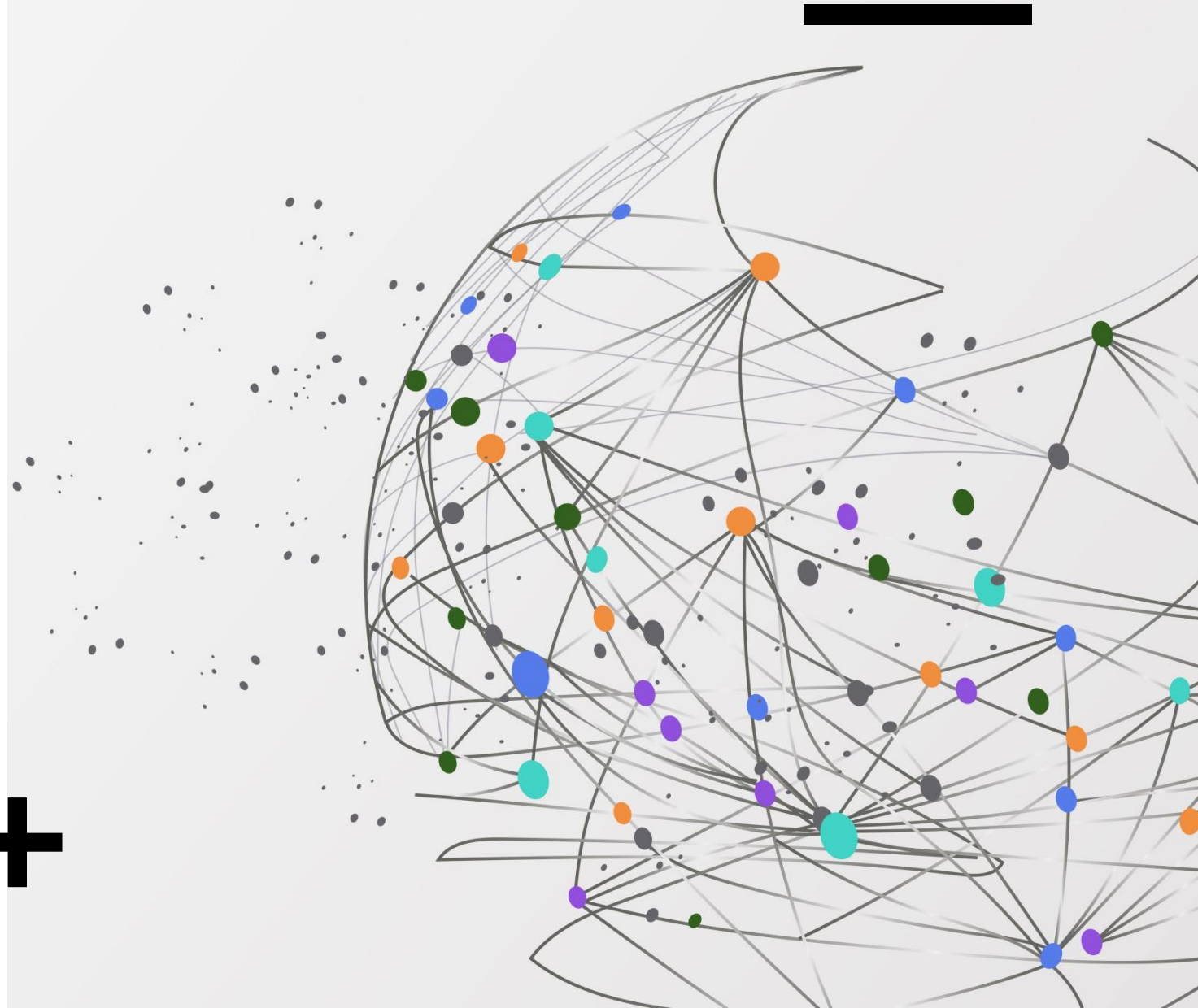
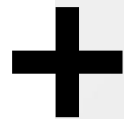


First American Financial Data Leak

By Jared Andraszek



Overview

Background prior to the leak

What happened

Who did it

How it could have been prevented



Prior to the data leak



What is First American?

- A title insurance and settlement service provider for primarily the real estate industry

Why was their data important?

- They were in possession of millions of documents that had personal information such as SSNs, bank account numbers, driver's licenses etc.

What Happened?



There was an authentication error

- If you had the web URL to a PDF page, you could have immediate access to that PDF.

Insecure Direct Object Reference (IDOR) Examples


- https://website.com/info_variable?info_value=11111
- <https://website.com/filename.pdf>



Who did it?

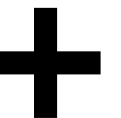
EVERYONE!!!

Because it was no authentication
many were able to get access to
years' worth of personal information
and financial statements



How could it have been prevented?

- Enforce more secure authentication
 - Multi-layer authentication
 - Require passwords to view documents





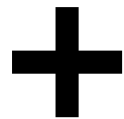
Summary

- Background prior to the attack
- What happened
- Who did it
- How it could have been prevented

Sources

- <https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/>
- <https://www.firstam.com/title-insurance-and-settlement-services/index.html>
- <https://portswigger.net/web-security/access-control/idor>





Thank You