Data on the dark web

Derek Fisher
Securely Built LLC
Welcome

• Derek Fisher, CISSP, CSSLP
• Over 20 years of experience in hardware and software engineering.
• Last seven years in security as an architect and leader in the healthcare and financial sectors.
• Teaches Application Security at Temple University.
• Founded Securely Built for the purpose of providing security education to businesses and individuals.

• https://www.linkedin.com/in/derek-fisher-sec-arch/
How do we define data
Where is data collected
How is it collected

• Directly asking customers, by indirectly tracking customers, and by appending other sources of customer data to your own

• Location based

• Once captured, this information is regularly changing hands in a data marketplace of its own.

• Regulations like GDPR and CCPA show that governments and consumers are growing concerned over data collection.
Why is data collection and storage important?
How is it used

• IoT, AI, ML. Oh My!
  • Consumer behavior to predictive analytics
  • More targeted and predictive marketing
  • Improving customer experience
• More security?
  • Companies can use meta data or things like voice recognition to better secure your information.
• Make money
  • Data brokers buy and sell information on customers
The individual’s perspective

BREACHES – AUGUST 2019 ~114 M RECORDS IN 95 INCIDENTS

VARIATION OF ATTACKS – RANSOMWARE, MALWARE, INSIDER, AND MISTAKES

DATA IN BREACHES – FINANCIAL, HEALTHCARE, PERSONAL, CREDENTIALS
How are attackers using this data?
Maltego Demo
How attackers profit
What is your data worth?

securelybuilt.com
What’s behind the price
The Tor Network
High-Level Tor

- Originally called TOR (The Onion Router) now just called the Tor Network.
  - The EFF has been a major sponsor and funder.
  - Can run any protocol through it that runs over TCP and is resilient against man-in-the-middle.
- The software randomizes the network circuit.
  - This creates a layered approach, like an onion. Nodes have no knowledge of where the traffic came from. Only where it’s going.
  - Using PKI to encrypt and decrypt traffic between each node.
  - However, nodes are not controlled by a single entity.
Onion Services (formerly hidden services)

Using the Tor Browser you are able to access sites not normally visible on the internet.
Tor Demo
Tor Demo 1
Tor Demo 2
What can we do
Data Collection, Retention and Deletion

- Prepare for a continued march towards governance like GDPR and CCPA.
  - Know your regulations, governance and policies.
- Only collect the data you need to operate.
  - Know when you need granular data (project level) and general data (strategic level)
- Make data a strategic asset, similar to your hardware and people.
- Have the ability to forget people and a way to securely destroy data when it’s no longer needed.
- Be transparent about the data you are collecting.
  - Allow an option to opt out
Virus protection isn’t enough

- Know your system and where your critical data is
  - Separate sensitive data from non-sensitive
  - Only capture sensitive data when necessary and have a means to secure it.
- Practice least privilege and need-to-know when it comes to data access.
- Log access to data
  - Especially critical or sensitive data
- Raise your security IQ through awareness training
- Have a data backup and recovery plan
- Have a robust patch management program
- Encrypt
Public Service Announcement
Questions?

Derek Fisher
securelybuilt.com