Salty Hurricanes

Quentin Barnes
CUCUG
12/19/2024

Two Big Recent News Items

- National Public Data breach (August)
- Salt Typhoon (earlier this month)

National Public Data Breach

- NPD is a data broker company
- DB had information on most adults in the US
  - Full names, birthdates, SSNs, phone numbers and addresses for the last few decades
- Check for yourself

Salt Typhoon

- Nation state threat actor, odds are China
- Intercepted internet traffic
  - Reconfigured and tapped ISPs' Cisco routers
- Compromised CALEA
  - Using law enforcement's own backdoor for wiretapping
  - Gives them access to the contents of all text messages, voice communications, and their metadata
  - Infiltration has not stopped

Why It Matters

- NPD breach gave enough information out for anyone to impersonate others
- Salt Typhoon is giving a nation state full access of any telecommunications in this country they want
  - Personal, commercial, or government

I Have Nothing to Hide!

Why Should I Worry?

Protecting is Different than Hiding

- Your identity with others
- Your bank accounts and credit history
- Your government assets
  - Social Security and unemployment benefits, tax refunds, property, being flagged for suspicious activity, travel
- Your employment
- Your reputation

What Should I Do?

- Create accounts with credit reporting agencies and freeze them
  - Equifax, Experian, TransUnion, Innovis, ChexSystems
- Create accounts with federal government agencies
  - login.gov, SSA, IRS
  - May take a few weeks
- Check credit reports often, up to weekly
  - AnnualCreditReport.com
- All free!
  - If anything asks for a credit card # or bank information, wrong place!

What Else?

- Never reuse passwords or similar passwords
- Use strong passwords
  - Correct Horse Battery Staple
    - Dice word list
    - Raid a Yahtzee game or “d20 Calc” app (Apple)
- Use password managers
  - Bitwarden
- Use Two Factor Authentication (2FA)
  - Avoid SMS 2FA, SIM Swap Attack
  - 2FAS Auth (Apple or Android)
  - Google Authenticator (Apple or Android)

Addn Recommendations from FBI

- Use end-to-end encryption for everything
  - Yes, FBI has flipped from anti-e2e to pro-e2e!
- Avoid plaintext methods (SMS or Email)
  - iMessage / Google Messages
  - Signal (Desktop, Apple, or Android)
  - Whatsapp
- Use https:// (TLS), not http://