HACKED!

Recent Trends and Incidents

HACKED!

- The world is increasingly computer & smart phone reliant
- Cyber criminals are global
  - Freelancers
  - Contractors
  - Government sponsored

HACKED!

- Fortune magazine recently did a special issue on the topic of hacking. The original articles can be found at:
- http://fortune.com/2017/06/22/cybersecurity-business-fights-back/
- http://fortune.com/2017/06/23/google-project-zero-hacker-swat-team/

HACKED!

- Many companies are reluctant to publish information on hacking incidents
- Hacking incidents are getting more frequent, larger and bolder
- Hacking software and/or hacking consultants are readily available for purchase or hire

Who Hacks?

- Data Breach Perpetrators – 2016*
  - Outsiders 75%
  - Organized Criminal Groups 51%
  - Internal Actors 25%
  - State-affiliated Actors 18%
  - Involved Partners 2%

* Data Source: Verizon data from Fortune magazine, July 1, 2017 issue

How Do They Hack?

- Tactics used in data breaches – 2016
  - Hacking 62%
  - Malware 51%
  - Involving stolen or weak passwords 81%
  - Social attacks 43%
  - Errors being causal events 14%
  - Involving privilege misuse 14%
  - Involving physical actions 8%

  * Data Source: Verizon data from Fortune magazine

State Affiliated Hacker Groups

- Fancy Bear & Cosy Bear – Russian
- Lazarus Group – North Korea
- Equation Group – U. S. National Security Agency
- Comment Crew – China
- Sandworm – Russian
- Shadow Brokers - Russian

Hacks Attributed to State Groups

- Fancy Bear – European elections
- Cozy Bear – U.S. Think Tanks
- Lazarus Group – 2009-> denial of service to US & South Korean sites, 2015 -> Sony Entertainment, 2016 -> Bangladesh Central Bank & SWIFT Financial Network, May 2017 -> WannaCry ransomware work

Hacks Attributed to State Groups

- Equation Group – Iranian nuclear program
- Shadow Brokers – Stole and are using Equation Group hacking tools
- Comment Crew – hacked Google in 2009
- Sandworm – intelligence gathering on NATO and the Ukraine government, critical infrastructure (shut down Ukranian power grid)

Recent Major Corporate Attacks

- 2012 – LinkedIn
  - In 2012, LinkedIn said 6.5 million accounts had been hacked
  - In 2016, they admitted hackers were selling name and password info for more than 117 million accounts

Recent Major Corporate Attacks

- 2013 – Target
  - 110 million U.S. customers' personal and financial information was exposed

Recent Major Corporate Attacks

- 2014 – JP Morgan
  - One server hacked and data about millions of the banks accounts stolen
  - Data used in fraud schemes yielding about $100 million

Recent Major Corporate Attacks

- 2014 – Home Depot
  - E-mail and credit card info of more than 50,000,000 customers stolen
  - Retailer offered to pay for credit score monitoring for affected customers for a year
  - Settlements with customers and banks cost Home Depot at least $179 million.

Recent Major Corporate Attacks

- 2014 – Sony
  - Internal servers rampaged by hackers believed to be from N. Korea in retaliation for a film comedy showing North Korean leader Kim Jong-un's face being melted off.

Recent Major Corporate Attacks

- 2015 – Hilton Hotels
  - Credit card data stolen from dozens of Hilton and Starwood chains across the U.S.

Recent Major Corporate Attacks

- 2016 – SWIFT Payment System
  - $81 million stolen from the Bangladesh Central Bank's account at the New York Federal Reserve

Recent Major Corporate Attacks

- 2015 – NYC Law Firms
  - Information about upcoming corporate mergers stolen
  - Information used to make stock trades, allegedly netting $4 million in stock trade profits

Recent Major Corporate Attacks

- 2016 – Tesco Bank
  - Tesco is a giant grocery chain that also runs a bank
  - $3.2 million was stolen from more than 9000 accounts
  - Tesco was forced to reimburse customers for the stolen money

Recent Major Corporate Attacks

- 2017 – Chipotle
  - Credit card information of millions of customers
  - Part of a larger scam targeting restaurants

Recent Major Corporate Attacks

- 2016, 2015, 2014, 2013 – Yahoo
  - Hack revealed in 2016
  - Involved over 1 billion accounts
    - 2013 > 1 billion
    - 2014 – 500,000 accounts
    - 2015 & 2016 – numbers not readily found
  - Names, e-mails, phone numbers, encrypted passwords, security questions
  - Includes Flickr and Tumblr accounts

Recent Major Corporate Attacks

- 2017 – Equifax
  - Data for 143 million US customers & some Canadian & UK accounts
  - Names, SIN numbers, birth dates, addresses & some driver's license numbers, 209,000 credit card numbers plus some other personal info
  - Largest ever hack of SIN numbers
  - Equifax waited 6 weeks before going public
  - Problems with Equifax's Consumer Response site

What Does this Tell Us?

- No one is too big to fall
- Monitor cards and balances carefully
- Maintain virus protection
  - Computers
  - Smart phones
- Don’t use the same passwords on multiple accounts
- Change passwords frequently

Questions & Discussion