- Malware
    - Malicious software
    - Gather information
        - Keystrokes
        - Information on screen
    - Participate in a group
        - Controlled over the net and turn into a bot and then be in a bot net
        - Can be controlled and can be used for multiple purposes
            - DDoS
    - Show you advertising
        - Big money
    - Viruses and worms
        - Encrypt your data
        - Ruin your day
- Malware types and methods
    - Viruses
    - Crypto-malware
    - Ransomware
    - Worms
    - Trojan Horse
    - RootKits
    - Keylogger
    - Adware/Spyware
    - Botnet
- How you get malware
    - They tend to work together
        - A worm takes advantage of a vulnerability
        - Installs malware that includes a remote access backdoor
        - Botnet may be installed later
    - Your computer must run a program
        - Email link - don't click links
        - Web page pop-up
        - Drive-by download
        - Worm
    - Your computer is vulnerable
        - Keep you OS updated
        - Keep the applications up to date

- **Virus**
    - Malware that can reproduce itself
        - It needs you to execute a program
        - **Virus needs a human being, whereas a worm can jump from machine without human intervention**
        - Reproduces through file systems or the network

            - Just running a program can spread a virus
        - May or may not cause problems
            - Some viruses are invisible, some are annoying
        - Anti-virus is very common
            - Thousands of new viruses every week
            - Is your signature file updated?
- Virus Types
    - Program virus
        - Part of an application
    - Boot sector virus
        - Who needs an OS?
    - Script viruses
        - Operating system and browser based
    - Macro viruses
        - Common in Microsoft Office
    - Fileless virus
        - A stealth attack
            - Does a good job of avoiding antivirus detection
        - Operates in memory
            - But never installed in a file or application
            - Will exploit itself through Flash/Java/Windows vulnerabilities then launches powershell and downloads payload in RAM -> runs powershell scripts, and executables in memory -> adds an auto start to registry (automatically turns on when you boot)
    - Worms
        - Malware that self replicates
            - Doesn't need you to do anything
            - Uses the network as a transmission medium
            - Self-propagates and spreads quickly
        - Worms are pretty bad things
            - Can take over multiple systems at a time
        - Firewalls and IDS/IPS can mitigate many worm infestations
            - Does Not help much once the worm gets in
        - **Wannacry worm**
            - Started with infected computer -> another vulnerable is exploited with eternalblue

—---

- **Personal Data**
    - Family photos, pictures
    - Organization Data
        - **Employee personally identifiable information (PII)**
        - Financial information
        - Company private data
        - How much is it worth?

      - Theres always a number
- Ransomware
  - The want your money and will take your computer in the meantime
  - May be fake ransom
    - Locks your computer “by the police”
  - A newer generation of ransomware
    - Your data is unavailable until you provide cash
    - Uses **cryptography** to encrypt your information
    - Your OS remains available, they want you running but not working
    - You must pay the people to obtain the decryption key
      - Untraceable payment system
      - An unfortunate use of public key cryptography
  - Protecting against ransomware
    - Always have a good backup
    - An offline backup ideally
    - Keep your OS up to date to patch vulnerabilities
    - Aswell as applications up to date
    - Keep your anti-virus/anti-malware signatures up to date.
      - New attacks every hour
    - Keep everything up to date.

- **Trojan Horse**
  - Software that pretends to be something else
    - So it can conquer your computer
    - Doesn't really are much about replicating
    - Circumvents your existing security
      - Anti-virus may catch it when it runs
        - The better trojans are built to avoid and disable AV
    - Once its inside it has free reign
      - And it may open the gates for other programs
- **Potentially Unwanted Program (PUP)**
  - Identified by antivirus/antimalware
  - Undesirable software
  - Often installed along with other software
  - Overly aggressive browser toolbar
  - A backup utility that displays ads
  - Browser search engine hijacker
- Backdoors
  - Why go through normal auth methods?
  - Just walk in the back door
  - Often placed on your computer through malware
    - Some malware software can take advantage of backdoors created by other malware
  - Some software includes a backdoor

- Old linux kernel included a backdoor
- Bad software can have a backdoor as part of the app.

- **Remote Access Trojans (RATs)**
    - Remote Administration Tool
    - The ultimate backdoor
    - Administrative control of a device
    - Malware installs the server/service/host
        - Can be connected with a client software
    - Control a device
        - Key logging
        - Screen recording / screenshots
        - Copy files
        - Embed more malware
    - DarkComet Rat
    - Don't run unknown software
    - Keep AV/AM up to date
    - Always have a backup

—---

- **Rootkits**
    - Originally a Unix Technique
        - The “root” in rootkit
    - Modified core system files
        - Part of the kernel
    - Can be invisible to the operating system
        - Won't see it in task manager
    - Also invisible to traditional antivirus utilities
        - If you cant see it, you can't stop it
- Kernel drivers
    - Zeus/ZBot malware
    - Famous for cleaning out bank accounts
    - Now combined with Necurs rootkit
        - Necurs is a kernel level driver
    - Necurs makes you cant delete Zbot
        - Access denied
    - Trying to stop the software
        - Access denied
    - Use a remover specific to the rootkit
        - Usually built after the rootkit is discovered
    - Secure boot with UEFI
        - Security in the BIOS

—---

- **Adware**
    - Your computer is one big advertisement
    - Pop ups with pop ups

  - May cause performance issues
    - Especially over the network
  - Installed accidentally
    - May be included with other software
  - Be careful of software that claims to remove adware
- Spyware
  - Malware that spies on you
    - Advertising, identity theft, affiliate fraud
  - Can trick you into installing
    - Peer to peer, fake security software
  - Browser monitoring
    - Capture surfing habits
  - Keylogger
    - Capture every keystroke
- Why is there so much adware and spyware
  - Money, your eyeballs are incredibly valuable
  - Your computer time and bandwidth is valuable
  - Your bank account is valuable.
- Protecting against adware/spyware
  - Maintain your antivirus / antimalware
  - Always know what you’re installing
  - Where's your backup?
  - Run some scans

—--

- **Bots**
  - Once your machine is infected, it becomes a bot
  - How does it get on your computer
    - Trojan Horse, or running a program that you thought was legitimate
    - OS or application vulnerabilities
  - Sit round and check in with C2-Command and Control server and wait for instructions.
  - A group of bots working together
  - Distributed Denial of Service (DDoS)
    - The power of many
  - Relay spam, proxy network traffic, distributed computing tasks
  - Botnets are for sale
    - Rent time from bad guys
    - Not a long term business proposition
  - Stopping the bot
    - Prevent initial infections
    - OS and application patches
  - Identify an existing infection
    - On demand scans
  - Prevent C2

        - Block at the firewall
        - Identify the workstation with a host based firewall or host based IPS (intrusion prevention system)

—---

- **Logic bomb**
    - Waits for a predefined event
    - **Disgruntled employees.**
    - **Time bomb**
        - Time or date
    - User event
        - Logic Bomb
    - Difficult to identify
        - Difficult to recover if it goes off
        - Hard to find evidence because they'll delete themselves
- **Real World logic bombs**
    - March 19, south korea
    - Email with malicious attachment sent to organizations
        - Posed as ban
        - Trojan installs malware
    - March 20
        - Malware time based logic bomb activities
        - Storage and master boot record deleted, system reboots
    - Boot device not found
    - Please install OS on your hard disk
    - Kiev, Ukraine high voltage substation
        - Logic bomb begins disabling electrical circuits
            - Malware mapped out of the control network
    - Began disabling power at a predetermined time
    - Customized for SCADA networks
        - Supervisory Control and Data Acquisition

—---

- **Preventing a logic bomb**
    - Difficult to recognize
        - Each is unique
        - No predefined signatures
    - Process and procedures
        - Formal change control
    - Electronic monitoring
        - Alert on changes
        - Host based intrusion detection, Tripwire
    - Constant audisting
        - An administrator can circumvent these existing systems

—---

- **Plaintext / unencrypted passwords**
    - Some applications store passwords “in the clear”
        - No encryption. You can read the stored password.
        - This is rare, thankfully
    - Do not store passwords as plaintext
        - Anyone with access to the password file or database has every credential
    - What to do if your application saves passwords as plaintext:
        - Get a better application
- Hashing a password
    - Hashres represent data as a fixed length string of text
        - A message digest or “fingerprint”
    - Will not have a collision
        - Different inputs will not have the same hash
    - One way trip
        - Impossible to recover the original message from the digest
        - A common way to store passwords
- **Examples:**
    - SHA-256 Hash algorithm
- The password file
    - Different across operating systems and applications
- Spraying attack
    - Try to login with an incorrect password
    - Eventually you’re locked out
    - Using common passwords
    - Attack with an account with the top three passwords
        - If they dont work, move to the next account
        - No lockouts no alarms, no alerts
- Brute force
    - Try every possible password combination until the hash is matched.
    - This might take some time
        - A strong hashing algorithm slows things down
        - It is solvable through bruteforce by comparing all letters to the hash of the original password
    - Brute force attacks - online
        - Keep trying the login process
        - Very slow
        - Most accounts will lockout after a number of failed attempts
        - Brute force the hash - offline
            - Obtain the list of users and hashes
            - Calculate a password hash
            - Compare it to a stored hash
            - Large computational resource requirement

  - Dictionary attacks
    - Use a dictionary to find common words
      - Password are created by humans
    - Many common wordlists available on the net
      - Some are customized by language or line of work
    - The password crackers can sub letters
    - This takes time, distributed cracking and GPU cracking is common
    - Discover passwords for common words
      - This won't discover random passwords
  - Rainbow tables
    - An optimized, pre built set of hashes
      - Saves time and storage
      - Does Not need to contain every hash
      - Contains pre calculated hash chains
      - Remarkable speed increase
        - Especially with longer password lengths
      - Challenge; needs different tables for different hashing methods
        - Windows is different than MySQL
  - Salt
    - Random data added to a password when hashing
    - Every user gets their own random salt
      - The salt is commonly stored with the password
    - Rainbow tables wont work with salted hashes
      - Additional random value added to their original password
    - This slows things down the brute force process
      - It doesn't completely stop the revers engineering
  - Salting the hash
    - Each user gets a different random hash with each letter that is random
- When the hashes get out
  - Collection #1
    - A collection of email addresses and passwords
    - 12k files and 87 gb of data
    - 1.1 bil unique emails and passwords
    - 772k unique usernames
      - 773 million people
    - 21 unique passwords
      - You really need a password manager

—---

- **Malicious USB Cable**
  - It looks like a normal cable
  - Has additional electronics
  - Operating system identified it as a HID
    - Human interface device
    - It looks like you’ve connected a keyboard or mouse

    - Once connected, the cable takes over
    - Downloads and installs malicious software
    - Dont plug in any USB cable
        - Always use trusted hardware
    - **Malicious flash drive**
        - Plug it in and see whats on it
    - Older operating systems would automatically run files
        - This has now been disabled or removed by default
    - Could still act as a HID (Human Interface Device)/ keyboard
        - Start a command prompt and type anything without your intervention
    - Attackers can load malware in documents
        - PDF files, spreadsheet virus
    - Can be configured as a boot device
        - Infect the computer after a reboot
    - Acts as an ethernet adapter
        - Redirects or modified internet traffic requests
    - Never connect an untrusted USB device
- **Skimming**
    - Stealing CC info usually during a normal transaction
        - Copying data from the magnetic stripe: card number, expiration date, card holders name
    - ATM skimming
        - Includes a small camera to also watch your pin
    - Use the card information for other financial transactions
    - Always check before using card readers
- **Card cloning**
    - Get card details from a skimmer
        - The clone needs an original
    - Create a duplicate of a card
        - Often included the CVC (card validation code)
    - Can be used with magnetic cards
        - The chips cant be cloned
    - Cloned gift cards are common
        - A magnetic stripe tech

—--

- **Machine Learning**
    - Our computers are getting smarter
    - This recognizes a lot of training data
        - Face recognition requires analyzing a lot of faces.
    - This requires a lot of training data
        - Face recognition requires analyzing a lot of faces
        - Driving a car requires a lot of road time
    - In use everyday
        - Stop spam

        - Recommend products
        - What movie would you like to see
        - Prevent car accidents
    - Poisoning the training data
        - Confuse the Ai
            - Attackers send modified training data that causes the Ai to behave incorrectly
        - Microsoft AI Chatter Bot named Tay
            - March 23, 2016
            - Interacted with twitter users, didnt program anti offensive behavior or anti offensive behavior algo
            - Tay quickly became racist, sexist and inappropriate bot.
        - Evasion attacks
        - The Ai is only as good as the training
            - Attackers find the holes and limitations
            - Change the number of good and bad words in the message
    - Securing the learning algo
        - Check the training data
        - Cross check and verify
        - Constantly retrain with new data
            - More data and better data
        - Train the Ai with possible poisoning

—---

- **Supply Chain**
    - The chain contains moving parts
        - Raw materials, supplies, manufacturers
    - Attackers can infect any step along the way
        - Infect different parts of the chain without suspicion
    - One exploit can infect the entire chain
- Target supply chain
    - 40 million credit card stolen
    - Heating and AC firm in Penn was infected and they worked for target and VPN Credentials for HVAC techs was stolen.
    - Email with malware
    - Used to infect every cash register at 1,800 stores.
- **Supply Chain Security**
    - Can you trust your new server/router/switch/software
    - Use a small supplier base
    - Strict c ontrols over policies and procedures
    - Ensure proper security is in place
    - Security should be part of the overall design
        - There's no limit to security

—--

- **Attacks can happen anywhere**
  - Two categories for IT security
    - The on premises data is more secure
    - The cloud based data is more secure
  - Cloud based security is centralized and costs less
    - No dedicated hardware, no data center to secure
    - On premises puts the security burden on the client
    - Data center security and infrastructure costs
  - On-premises security
    - Customize your security posture
    - Full control
    - On site IT team can manage security better
      - The local team can ensure everything is secure
      - A local team can be expensive and difficult to staff
    - Local team maintains uptime and available
      - System checks can occur at any time
      - No phone call for support
    - Security changes can take time
      - New equipment, configs, and additional costs
  - Security in the cloud
    - Data is in a secure environment
      - No physical access to the data center
    - Cloud providers are managing large scale security
      - Automated signature security updates
      - Users must follow security best practices
    - Limited downtime
      - Extensive fault tolerance and 24/7/365 monitoring
    - Scale security options
      - One click security developments
      - This may not be as customizable as necessary

—---

- **Cryptographic Attacks**
  - You’ve encrypted data and send it to another person
    - Is it really secure?
    - How do you know?
  - The bad guy doesnt have the combination (the key)
    - So they break the safe (the cryptography)
  - Finding ways to undo the security
    - There are many potential cryptographic shortcomings
    - The problem is often the implementation
- **Birthday Attack**
  - In a classroom of 23 students, what is the chance of two students share a birthday

    - About 50%
    - For a class of 30, the chance is about 70%
    - In the digital world, this is a hash collision
        - A hash collision is the same hash value for different plaintexts
        - Find a collision through brute force
    - The attacker will generate multiple versions of plaintext to match the hashes
        - Protect yourself with a large hash output size
    - **Collisions**
        - Hash digests are supposed to be unique
        - Different input data should never create the same hash
        - MD5 hash
            - Message digest algorithm 5
            - First published in april 1992
            - Collision identified in 1996
        - Researchers created a CA certificate that appeared legitimate when MD5 was checked.
            - Built other certificates that appeared to be legit and issued by RapidSSL
- **Downgrade Attack**
    - Instead of using perfectly good encryption, use somethings thats not so great
    - Force the systems to downgrade their security
        - 2014 - TLS vulnerability
            - POODLE (padding oracle on downgraded legacy encryption)
            - On path attack
            - Force clients to fallback to SSL 3.0
            - SSL 3.0 has significant cryptographic vulnerabilities
            - Because of POODle, modern browsers wont fallback to SSL 3.0