Threat Actors & Attributes

- The entity responsible for an event that has impact on the safety of another entity
  - Also called a malicious actor
- Broad scope of actors
  - And motivations vary widely
- Advanced Persistent Threat (APT)
  - Attackers are in the network and undetected
  - 2018 FireEye report:
    - Americas: 71, EMEA: 177, APAC: 204
- Insiders
  - More than just passwords on sticky notes
    - Some insiders are out for no good reason
  - Sophistication may not be advanced, but the insider has institutional knowledge
    - Attacks can be directed at vulnerable systems
    - The insider knows what to hit
  - Extensive resources
    - Eating away from the inside
- Nation States
  - Governments
    - National security, job security
    - Always an external entity
  - Highest sophistication
    - Military control, utilities, financial control
    - US and Israel destroyed nuclear centrifuges with the Stuxnet worm
  - Constant attacks, massive resources
    - Commonly an Advanced Persistent Threat (APT)
- Hacktivist
  - A hacker with a purpose
    - Social change or a political agenda
    - Often an external entity
  - Can be remarkably sophisticated
    - Verify specific hacks
    - DoS, website defacing, release of private documents
  - Funding is limited
    - Some organizations have fundraising options
- Script Kiddies
  - Runs premade scripts without any knowledge of whats really happening
    - Not necessarily a youngster
  - Can be internal or external
    - But usually external
  - Not very sophisticated
  - No formal funding
    - Looking for low hanging fruit
  - Motivated by the hunt

        - Working the ego trying to make a name
- Organized crime
    - Professional criminals
        - Motivated by money
        - Almost always an external entity
    - Very sophisticated
        - Best hacking money can buy
    - Crime thats organized
        - One person hacks, one person manages the exploits, another person sells the data, another handles customer support
    - Lots of capital to fund hacking efforts
- Hackers
    - Experts with technology
        - Often driven by money, power, and ego
    - Authorized
        - An ethical hacker with good intentions
        - And permission to hack
    - Unauthorized
        - Malicious
        - VIolates security for personal gain
    - Semi authorized
        - Finds a vulnerability
        - Does Not use it
- Shadow IT
    - Going rogue
        - Working around the internal IT organization
    - Information Technology can put up roadblocks
        - Shadow IT is unencumbered
        - Use the cloud
        - Might also be able to innovate
    - Not always a good thing
        - Wasted time and money
        - Security risks
        - Compliance issues
        - Dysfunctional organization
- Competitors
    - Many different motivations
        - DoS, espionage, harmful reputation
    - High level of sophistication
        - Based on some significant funding
        - The competitive upside is huge
    - Many different intents
        - Shut down your competitor during an event
        - Steal customer lists

- Attack Vectors
    - A method used by the attacker
    - Gain access or infect to the target
    - A lot of work goes into finding vulnerabilities in these vectors
        - Some are more vulnerable than others
    - IT security professionals spend their career watching these vectors
        - Closing up existing vectors
        - Finding new ones
- Direct access attack vectors
    - Theses a reason we lock the data center
        - Physical access to a system is a significant attack vector
    - Modify the operating system
        - Reset the administrator password in a few minutes
    - Attach a keylogger
        - Collect usernames and passwords
    - Transfer files
        - Take it with you
    - Denial of service
        - This power cable is in the way
- Wireless attack vectors
    - Default login credentials
        - Modify the access point configuration
    - Rogue access points
        - A less secure entry point to the network
    - Evil twin
        - Attacker collects authentication details
        - Man-in-the-middle attacks
        - On path attacks
    - Protocol vulnerabilities
        - 2017 - WPA2 Key Reinstallation Attack (KRACK)
        - Older encryption protocols (WEP, WPA)
    - Email attack vectors
        - One of the biggest (and most successful) attack vectors
            - Everyone has email
        - Phishing attacks
            - People want to click links
        - Deliver the malware to the user
            - Attach it to the message
        - Social engineering attacks
            - Invoice scam
- Supply Chain attack vectors
    - Tamper with the underlying infrastructure
    - Or manufacturing process

- Gain access to a network using a vendor
    - 2013 Target credit card breach
- Malware can modify the manufacturing process
    - 2010 - Stuxnetwork disrupts Iran’s uranium enrichment program
    - Counterfeit networking equipment
        - INstall backdoors, substandard performance and availability
        - 2020 - Fake Cisco Catalyst 2960-X and WS-2960-X-48TS-L
- Social media attack vectors
    - Attackers thank you for putting your personal information line
        - Where you are, and when
        - Vacation pictures are especially telling
    - User profiling
        - Where were you born?
        - What is the name of your school mascot?
    - Fake friends are fake
        - The inner circle can provide additional information
- Removable media attack vectors
    - Get around the firewall
        - The USB interface
    - Malicious software on USB flash drives
        - Infect air gapped networks
        - Industrial systems, high-security services
    - USB devices can act as keyboards
        - Hacker on a chip
    - Data exfiltration
        - Terabytes of data walk out the door
        - Zero bandwidth used
- Cloud attack vectors
    - Publicly facing applications and services
        - Mistakes are made all the time
    - Security misconfigurations
        - Data permissions and public data stores
    - Brute force attacks
        - Or phish the users of the cloud service
    - Orchestration attacks
        - Make the cloud builds new application instances
    - Denial of service
        - Disable the cloud services for everyone

- Threat Intelligence
    - Research the threats
        - And the threat actors
    - Data is everywhere
        - Hacker groups profiles, tools used by the attackers, and much more

    - Make decisions based on this intelligence
        - Invest in the best prevention
    - Used by researchers
        - Security operations teams, and others
- Open Source Intelligence (OSINT)
    - Open source
        - Publicly available sources
    - Internet
        - Discussion groups, social media
    - Government data
        - Mostly public hearings, reports, websites
    - Commercial data
        - Maps, financial reports, databases
- Closed/proprietary intelligence
    - Someone else's has already compiled the threat information
        - You can buy it
    - Threat intelligence services
        - Threat analytics
        - Correlation across different data sources
    - Constant threat monitoring
        - Identify new threats
        - Create automated prevention workflows
- Vulnerability databases
    - Researchers find vulnerabilities
        - Everyone needs to know about them
    - Common Vulnerabilities and Exposures (CVE)
        - A common managed list of vulnerabilities
        - Sponsored by the US department of homeland security (DHS) and cybersecurity and infrastructure security agency (CISA)
        - US National Vulnerability Database (NVD)
            - A summary of CVE’s
            - Also sponsored by DHS and CISA
        - NVD provides additional details over the CVE list
            - Patch availability and severity scoring
- Public/Private information sharing centers
    - Public threat intelligence
        - Often classified information
    - Private threat intelligence
        - Private companies have extensive resources
    - Need to share critical security details
        - Real time, high quality cyber threat information sharing
    - Cyber threat alliance (CTA)
        - Members upload specifically formatted threat intelliegence
        - CTA scores each submission and validates across other submissions

        - Other members can extract the validated data
- Automated indicator sharing (AIS)
    - Intelligence industry needs a standard way to share important threat data
        - Share information freely
    - Structured Threat information eXpression (STIX)
        - Describes cyber threat information
        - Includes motivations, abilities, capabilities, and response information
    - Trusted Automated eXchange of Indicator Information (TAXII)
        - Securely shares STIX data
- Dark web intelligence
    - Dark web
        - Overlay networks that use the internet
        - Requires specific software and configurations to access
    - Hacking groups and services
        - Activities
        - Tools and Techniques
        - Credit card sales
        - Accounts and passwords
    - Monitor forums for activity
        - Company names, executive names
- Indicators of compromise (IOC)
    - An event that indicates an intrusion
        - Confidence is high
        - He's calling from inside the house
        - Change to file hash values
        - Irregular international traffic
        - Changes to DNS data
        - Uncommon login patterns
        - Spikes of read requests to certain files
- Predictive analysis
    - Analyze large amounts of data very quickly
        - Find suspicious patterns
        - Big data used for cyber security
    - Identify behaviors
        - DNS queries, traffic patterns, location data
    - Creates a forecast for potential attacks
        - An early-warning system
    - Often combined with machine learning
        - Less emphasis on signatures
- Threat maps
    - Identify attacks and trends
        - View worldwide perspective
- File/code repositories
    - See what the hackers are building

        - Public code repo
        - Github
    - See what people are accidentally releasing
        - Private code can often be published publicly
    - Attackers are always looking for this code
        - Potential exploits exist
        - Content for phishing attacks

- Threat research
    - Know your enemy
        - And their tools of war
    - A never-ending process
        - The field is constantly moving and changing
    - Information from many different places
        - You can't rely on a single source
- Vendor websites
    - Vendors and manufacturers
        - They wrote the software
    - They know when problems are announced
        - Most vendors are involved in the disclosure process
        - They know their product better than anyone
    - They react shen surprises happen
        - Scrambling after a zero day announcement
        - Mitigating and support options
- Vulnerability feeds
    - Automated vulnerability notifications
        - National Vulnerability Database (CVE’s)
        - CVE data feeds
    - Third party feeds
        - Additional vulnerability coverage
    - Roll up to a vulnerability management system
        - Coverage across teams
        - Consolidated view of security issues
- Conferences
    - Watch and learn
        - An early warning of things to ome
    - Researchers
        - New DDoS methods
        - Intelligence gathering
        - Hacking the latest technologies
    - Stories from the trenches
        - Fighting and recovering from attacks
        - New methods to protect your data
    - Building relationships

        - Forge alliances
- Academic journals
    - Research from academic professionals
        - Cutting edge security analysis
    - Evaluations of existing security technologies
        - Keeping up with the latest attack methods
    - Detailed post mortem
        - Tear apart the latest malware and see what makes it tick
    - Extremely detailed information
        - Break apart topics into their smaller pieces.
- Request for comments (RFC)
    - Published by the internet society (ISOC)
        - Often written by the internet engineering task force (IETF)
        - Internet society description is RFC (1602)
    - Not all RFC's are standards documents
        - Expiremental, Best current practice, standard track, and historic
    - Many informational RFC's analyze threats
        - RFC 3833 - Threat analysis of the domain name system
        - RFC 7624 - Confidentiality in the Face of Pervasive Surveillance:
            - A threat model and problem statement
    - Local industry groups
        - A gathering of local peers
        - Shared industry and tech
    - Geographical presence
        - Associations
        - Info systems security associations
    - Meet others in the area
        - Discuss local challenges
        - Industry user groups
            - Cisco, Microsoft, VMWare
    - Secure specific technologies
- Social Media
    - HAcking group convo
    - Monitor the chatter
- Honeypot monitoring on Twitter
- Identify new exploit attempts
- Threat feeds
    - Monitor threat announcements
- Sources
    - US DEpartment of homeland security
    - US FBI
    - SANS Internet Storm center
    - VirusTotal Intelligence
- TTP

- Tactics, Techniques, and procedures
  - What are adversaries doing and how are they doing it?
- Search through data and networks
  - Proactively look for threats
  - Signatures and firewall rules cant catch everything
- Different types of TTPS
  - Information on targeted victims (Finance for energy companies)
  - Infrastructure used by attackers (DNS and IP addresses)
  - Outbreak of a particular malware variant on a service type