Economic view

- Human operated attacks:
    - In this cased, for every tactic (of the MITRE ATT&CK), human operators execute all the steps
    - Actions can be tailored to the specific environment
    - They can be very effective, these attacks are extremely dangerous and costly (so also less frequent)

Automated attacks

- Automated tools executes all the steps, actions cannot be tailored to the specific environment
- It is very hardly effective: circumventing a broad variety of different defenses and environments with one tool is not easy
- Are much more less dangerous than the human operated, but they are also much more cheaper (so quite frequent)
- Sometimes automated attacks can be effective
- There are attack tools indeed able to execute all the steps automatically, with high probability of success and quickly
- It is a huge problem: fast propagation across and within organizations
- A few examples
    - Petya (2017): example of high effectiveness in automation
    - NotPetya@Maerks (2017): example of fast propagation within organization
    - WannaCry (2017): example of fast propagation across different organizations
    - NotPetya (2017): example of high damage done
- Persistence: in all the examples attacks has a visible impact, attacks may aim at hidden initial access and persistence → backdoors for later human operated exploitation (these attack tools may be a critical issue worldwide even for national security)
- Fact: exploit E with injection remote/no user action
    - Injection attempt on the entire IPv4 space: feasible in less than 10 min
    - The predominant cost is for developing E, the injection attempt on the entire IPv4 space costs almost nothing
- Consequence: a device D with public IP address and exposed on the internet
    - You become aware that D has RCE vuln, exploitable remote/no user action, with cheap and reliable exploit → you should assume that D is already under the control of an attacker that is because
        - If it is a public vuln: the attacker has to develop exploit and start injection scan, usually takes a few days (the defender process is certainly much longer)
        - If it is a zero day vuln: full injection scan has probability occurred already
- High risk organizations: depending on the risk for your organization, the most sensible action may be disconnect the device immediately, irrespective to he operational cost
- Example: CISA has observed (January 2024) widespread and active exploitation of vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure solutions. CISA has determined these conditions pose an unacceptable risk to Federal Civilian Executive Branch (FCEB) agencies and require emergency action. This determination is based on the high potential for a compromise of agency information systems, the impact of a successful compromise and the complexity of the proposed mitigations → required actions: as soon as possible disconnect all instances of Ivanti Connect Secure and Ivanti Policy Secure solution products from agency networks
    - It is not enough, you then have to evict (D3FENSE) → continue threat hunting on any systems connected to-or recently connected to the affected Ivanti device
    - To bring a product back to service, agencies are required to perfume export configuration setting, complete a factory reset per Ivanti's instructions, rebuild the device per Ivanti's instructions and upgrade to the one of the following supported software versions through Ivanti's download portal
- Example: SolarWinds → all the SolarWinds Orion products has to be disconnected or powered down
- Very high risk organizations: any organization with very tight security requirements should have people able to pull the plug purely on their own authority
    - Software company that develops security tools, highly sensitive government agencies, control room of banks…
    - Risk/cost analyses require bypassing of normal processes

Attack economics

- Attack campaign on a predefined set of targets: $Gain \approx Takings - AttackCost$
- We want to estimate the attack cost for human operated attacks vs automated attacks
- Takings estimate
    - Assumptions: failed attack on a target = zero taking, successful attack on a target = always the same taking
    - $Takings \approx TakingsPerTarget \cdot NumberTargets \cdot ProbSuccess$, it is linear in the number of targets
- Attack cost and gain estimate for human operated attacks
    - Assumptions: the initial cost is independent from the number of targets (reconnaissance + resource development, how you execute the attack and collect takings), there is an additional cost for each target (same additional cost)
    - $AttackCost \approx FixedCost + CostPerTarget \cdot NumberTargets$, linear in number of targets, the slope is the cost per target
    - The target must be worth the effort, because an human operated attack is attractive only when $TakingPerTarget \cdot ProbSuccess >> CostPerTarget$
    - In this case attacking targets of little value is not rational
- Attack cost and gain estimate for automated attacks
    - There is no additional cost for each target (per il resto, stesse ipotesi di prima)
    - Counterintuitive fact: for many automated attacks, additional costs are negligible → attacking 100 targets cost like attacking 10000
        - Examples
            - Phishing: assume that the initial cost is independent from the number of targets (ti basta costruire una mail generica), una volta che hai fatto reconnaissance e resource development, poco cambia se mandi 1000, 10000 o 100000 email, il costo rimane praticamente lo stesso
            - Large scale injection: contacting 1000, 10000 or 100000 IP addresses has the same cost, the predominant cost is developing the exploit
    - $AttackCost \approx FixedCost$, independent from the number of targets
    - This kind of attacks is attractive when $TakingPerTarget \cdot ProbSuccess \cdot NumberTargets >> FixedCost$, a questo punto il taking per target e il prob of success possono anche essere piccoli, tanto posso aumentare a piacere il numero dei target
    - In this case attacking targets of little value may be rational → this explain why single users are almost always infected by automated attacks (Phishing is still a huge problem)
- Automated attacks are extremely frequent: there is only one fixed and known investment to make, there are a lot of taking opportunities (linear with the number of free attempts) → it is a fantastic economic opportunity

Attack categories

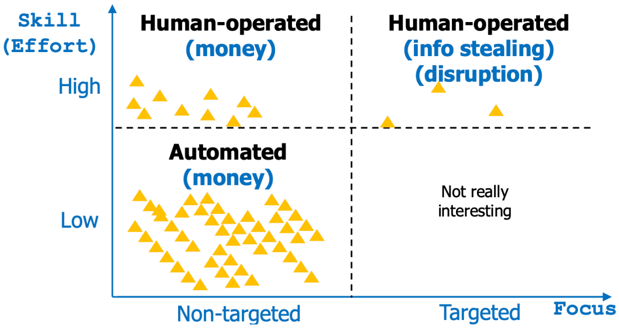
- The attacks can be categorized in many possible ways, we will see a very useful categorization in 4 classes (Steve Bellovin) and reason about how many attacks there are in each category, which category is more relevant for a defender?
- Prof said: is a seemingly trivial topic, but it has an huge impact on his understanding of cybersecurity
- Financially motivated attackers:
    - Real scenario (attacker point of view): plentiful of targets, many of them have bad defenses (so success requires not an high attack effort). While attacking a certain target you know that whether you succeed in the attack and what investment you will need for that target
    - These attackers are interested only in money, it is clearly a large part of the attackers → money is all that matters, so they are not fixated on any specific target, all targets are equivalent

NB this is the most common attacker mindset

- If you are a financially motivated attacker and you are attacking a certain target: your early attack steps are costly, prevention and detection appears not bad, the rational behavior is to change target (sicuramente l'attaccante non si mette a investire denaro su un target, se il suo obiettivo sono solo soldi) → in a large population of attackers, the prevalent behavior is the most rational one

NB se nelle fasi iniziali di un attacco fanno pensare all'attaccante che il target ha una buona difesa, l'attaccante cambia target

Economic view



- Threat matrix:
  - High effort - not targeted: frequent, the reason is money and it is sophisticated crime
    - Opportunistic
  - Low effort - not targeted: extremely frequent, the reason is money and it occurs in crime groups
    - Opportunistic
  - High effort - targeted: rare, the reason is info stealing/distruption and it is managed by National Intelligence Agencies, State groups
    - Advanced Persistent Threat (APT)

Strategic Framework: defender mindset

- How to defend:
  - For low effort attacks apply basic security hygiene usually suffices, these attacks are extremely frequent and practically unavoidable → there are no excuses for lack of basic security hygiene
  - For high effort - non targeted attacks
    - Opportunistic (manual)
    - These attacks are the most dangerous → they are relatively frequent, and it is very unlikely that $DefenseResources > AttackResources$
- The costs of attackers and defenders are highly asymmetric
  - Attacker: may concentrate the resources on a few points in a few moments
  - Defender: must dilute resources everywhere and always
  - So, with comparable resources, attacker wins
- Example: initial access, the defender has to consider that
  - There are hundreds of PCs/notebooks
  - end of life web frameworks
  - Networks printers that are forgotten by anyone
  - Webcams
  - Heating/cooling systems
  - …
- **Opportunistic attacks: the key defender strategy is to encourage the attacker to change target**
  - Defense must appear good
  - Penetration / lateral movement should be expensive for the attacker
  - Defense in depth → multiple independent layers
- Example: Tight Wks Firewall:
  - Not leave it in default configuration (accept inbound connections from any machine), but use a stricter configuration that do not accept any inbound connection, except from the very few designated remote maintenance wks → in this way the attacker cannot make lateral movement easily because he cannot connect to other workstations, so he changes target
- For high skill - targeted attacks (APT attacks) (quello che mancava prima): it is very unlikely that $DefenseResources > AttackResources$, but they are not frequent attacks
- Key defense strategy for APT Attacks: cross your fingers
  - If a highly skilled attacker is firmly interested in you, then it is very unlikely that you will be able to resist and it will not change target
  - Prof's suggestion: focus on opportunistic attackers (almeno lì c'è qualche speranza)

Understanding Cybersecurity

- Every major incident implies some recommended defensive actions, it is not rocket science, there are always the same boring recommendations, but why is necessary to recommend them always and they are not implemented?

Economic view

- In the real world we do not have to look at the technical issues, we have to focus on the incentive structure of our environment
- How the CEO think: unless you are a company like google, whose cybersecurity is a competitive advantage, you don't want to excel in cybersecurity. You want to be average, or at most, slightly above average. You want to do what your peers are doing
- It doesn't matter that this costs a lot of money due to data breaches, as long as the cost is no more than your competitors, then you are still competitive in your market (ragionamento totalmente sensato)
- Enter a tradeoff mindset: cybersecurity is not about preventing attacks, is about tradeoffs
    - The defensive budget has to be distributed the best you can
- We have to think in economical terms: to understand cybersecurity we have never to think only in technical terms, but always think in economical terms (what is the cost for attack, defense, incident? Who pays?)
- Money drives the world 2.0