

Attackers and Type of attackers

Dr. Shahzada Khurram

Who are attackers

Attacker or hacker referred to a person who used advanced computer skills to attack computers.

- **Black hat** hackers were those attackers who violated computer security for personal gain (such as to steal credit card numbers) or to inflict malicious damage (corrupt a hard drive). Malicious hackers, trying to find flaws to exploit them (Crackers – they crack the code).
- **White hat** hackers were described as “ethical attackers”: with an organization’s permission they would attempt to probe a system for any weaknesses and then privately provide information back to that organization about any uncovered vulnerabilities.
- **Gray hat** hackers who would attempt to break into a computer system without the organization’s permission (an illegal activity) but not for their own advantage; instead, they would publically disclose the vulnerability in order to shame the organization into taking action.

Who are attackers

- **Cybercriminals** individuals who launch attacks against other users and their computers. They are a loose network of attackers, identity thieves, and financial fraudsters. "Cybercriminals often meet in online "underground" forums to trade information and coordinate attacks".
- **Script kiddies** they lack the knowledge of computers and networks needed to do so. Script kiddies instead do their work by downloading automated attack software (scripts) from websites and using it to perform malicious acts.
- **Brokers** In recent years several software vendors have started financially rewarding individuals who uncover vulnerabilities in their software and then privately report it back to the vendors so that the weaknesses can be addressed.
- **Insiders** Another serious threat to an organization actually comes from an unlikely source: its employees, contractors, and business partners, often sell insider information.
- **Cyberterrorists** Many security experts fear that terrorists will turn their attacks to a nation's network and computer infrastructure to cause disruption and panic among citizens.

- **Hactivists** can involve breaking into a website and changing the contents on the site as a means of making a political statement against those who oppose their beliefs. as a means of protest or to promote a political agenda.
 - Famous attacks: Anonymous – DDOS attack on Visa, Mastercard, PayPal to protest the arrest of Julian Assange (WikiLeaks). Google/Twitter/SayNow worked together to provide communication for the Egyptian people when the government orchestrated an internet blackout during the 2011 protests.
- **State-Sponsored Attackers** Instead of using an army to march across the battlefield to strike an adversary, governments are using for launching computer attacks against their foes.
 - Approximately 120 countries have been developing ways to use the internet as a weapon to target financial markets, government computer systems and utilities.
 - Famous attacks: US elections (Russia), Sony websites (N. Korea), Stuxnet (US/Israel), US Office of Personnel Management (China), ...

- **Outsiders:**

- Unauthorized individuals - Trying to gain access; they launch the majority of attacks but are often mitigated if the organization has good Defense in Depth.
- Interception, malicious code (e.g. virus, logic bomb, trojan horse), sale of personal information, system bugs, system intrusion, system sabotage or unauthorized system access.
- 48-62% of risks are from outsiders.

- **Insiders:**

- Authorized individuals - Not necessarily to the compromised system, who intentionally or unintentionally compromise the system or data.
- This could be: Assault on an employee, blackmail, browsing of proprietary information, computer abuse, fraud and theft, information bribery, input of falsified or corrupted data.
- 38-52% of risks are from insiders, another reason good Authentication and Authorization controls are needed.

Thank you