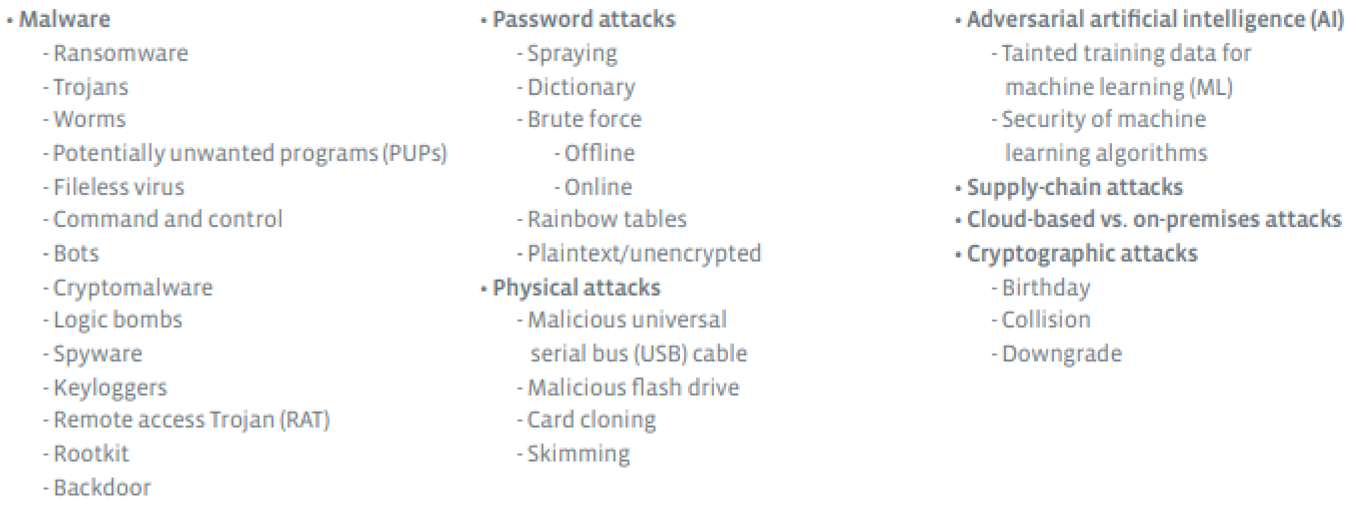
1.2 Given a scenario, analyze potential indicators to determine the type of attack



- Malware
  - Ransomware
  - Trojans
  - Worms
  - Potentially unwanted programs (PUPs)
  - Fileless virus
  - Command and control
  - Bots
  - Cryptomalware
  - Logic bombs
  - Spyware
  - Keyloggers
  - Remote access Trojan (RAT)
  - Rootkit
  - Backdoor
- Password attacks
  - Spraying
  - Dictionary
  - Brute force
    - Offline
    - Online
  - Rainbow tables
  - Plaintext/unencrypted
- Physical attacks
  - Malicious universal serial bus (USB) cable
  - Malicious flash drive
  - Card cloning
  - Skimming
- Adversarial artificial intelligence (AI)
  - Tainted training data for machine learning (ML)
  - Security of machine learning algorithms
- Supply-chain attacks
- Cloud-based vs. on-premises attacks
- Cryptographic attacks
  - Birthday
  - Collision
  - Downgrade

Created: 2021-07-25 16:53

Status: #malware #cryptography #password #AI

Malware

Malware: Malicious code that performs an unwanted function from the perspective of the legitimate user or owner of a computer system

Ransomware: Takes over a computer system, usually by encrypting user data, to hold data hostage while demanding payment.

- > Ransomware is often sophisticated enough to be able to encrypt files on internal and external storage devices, network shares, and even cloud storage services

Trojans: A means of delivering malicious software by distinguishing inside of a benign host file.

Worms: Self-contains applications that don't require becoming attached directly to a distribution (locally or across a network).

Potentially unwanted programs (PUPs): Any type of questionable software, such as sniffers, password crackers, network mappers, port scanners, keystroke loggers, and vulnerability scanners. (AKA: potentially unwanted applications (PUA) and potentially unwanted software (PUS))

Fileless virus: Resides in memory only and do not saves themselves to the local storage devices. They are injected into memory that then self-destructs leaving the virus living in memory. Rebooting a system can potentially rid of them from a system

Command and control: Intermediary serving as the locus of connection between an attacker and bots where commands are distributed and information is exchanged. C&C assists the attacker in remaining anonymous, while controlling botnet agents.

Botnet: Shortened form of the phrase "software robot network". Remotely controlled compromised systems most commonly known to be used to perform DoS flooding attacks.

Cryptomalware: Uses system resources to mine cryptocurrencies, such as Bitcoin or Monero.

Logic Bombs: Malicious code that remains dormant until a triggering event or condition occurs.

Spyware: Malicious code or even business/commercial code that collects information about users without their direct knowledge or permission.

Adware: Pop-ups or alternate advertisements to users based on their activities

Keyloggers: A PUP that records keystrokes

Remote Access Trojan (RAT): Malware that grants an attacker some level of remote control access to a compromised system. (Utilize reverse shells)

Rootkit: Malware that embeds itself deep within an OS. They can manipulate information seen by the OS and displayed to users. Rootkits are a type of invisibility shield used to hide itself and other malicious tools.

Backdoor: There are two types of backdoor attacks: a developer installed access method that bypasses any and all security restrictions, or a hacker-installed remote-access client

Password attacks

Spraying/Credential Stuffing: The attempt to log into a user account through repeated attempts of submitting generated or pulled-from-a-list credentials.

Dictionary attack: Performs password guessing by using a preexisting or precompiled list of possible passwords.

Brute Force attack: Tries every possible valid combination of characters to construct possible passwords

Offline password attack: One in which the attacker is not working against a live target but instead is working on their own independent computers.

Online password attack: Occurs against a live logon prompt (aka password spraying/credential stuffing)

Rainbow table: A form of pre-computed hash tables to increase speed of checking the stolen hash of a victim

Physical Attacks

Attempts to gain access into a facility, damage a facility, steal equipment, damage equipment, plant software or listening devices, clone data, and physical harm personnel

Malicious USB cable/Flash drive: A device crafted to perform unwanted activities against a device.

- Functioning as a hardware keystroke logger
- Function as a file copying device
- Function as an injector of malicious code
- Function as a remote access tool using a WiFi adapter
- Function as a false keyboard or mouse
- Destroy a connected system through electricity discharge
- Examples: Rubber ducky, Evilduino

Card Cloning: Duplication or skimming of data from a targeted source card and writing it onto a blank new card More info

Adversarial Artificial Intelligence (AI)

Training or programming technique where computational systems are set up to operate in opposition to automate the process of developing system defenses and attacks More info

Tainted training data for machine learning

Tainted training data for machine learning can result in poor, useless, or even harmful outcomes. It is extremely important to provide properly focused data as input to AL, ML, and GAN systems.

Supply Chain Attacks

Supply chain attacks could result in flawed or less reliable products or could allow for remote access or listening mechanisms to be embedding into otherwise functioning equipment

Cryptographic attacks

Cryptographic attacks are the means and methods by which hackers attempt to overcome the mechanisms of encryption to breach the security that such systems provide

Birthday attack:

Collision: Occurs when the output of two cryptographic operations produce the same result.

Downgrade attack: Attempts to prevent a client from successfully negotiating robust high-grade encryption with a server. If successful, the attacker is able to eavesdrop and manipulate the conversation even after the "encrypted" session is established (man in the middle)

- POODLE downgrade attack