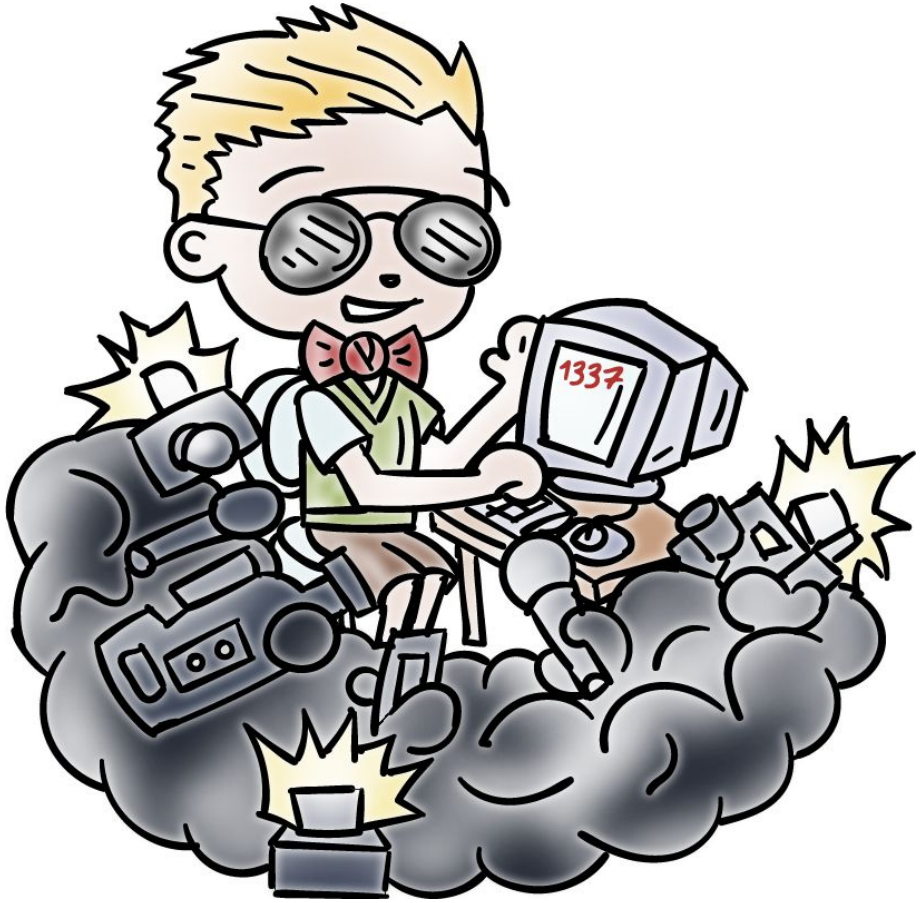
Modern Malware
Lesson Introduction

- What is “modern”
- Botnets and APTs
- Basic malware analysis and detection techniques

Past Malware



- In the past, often for "fame" and/or "fun"
  - E.g., defacing web pages
  - Fast and large-scale spreading

Modern Malware

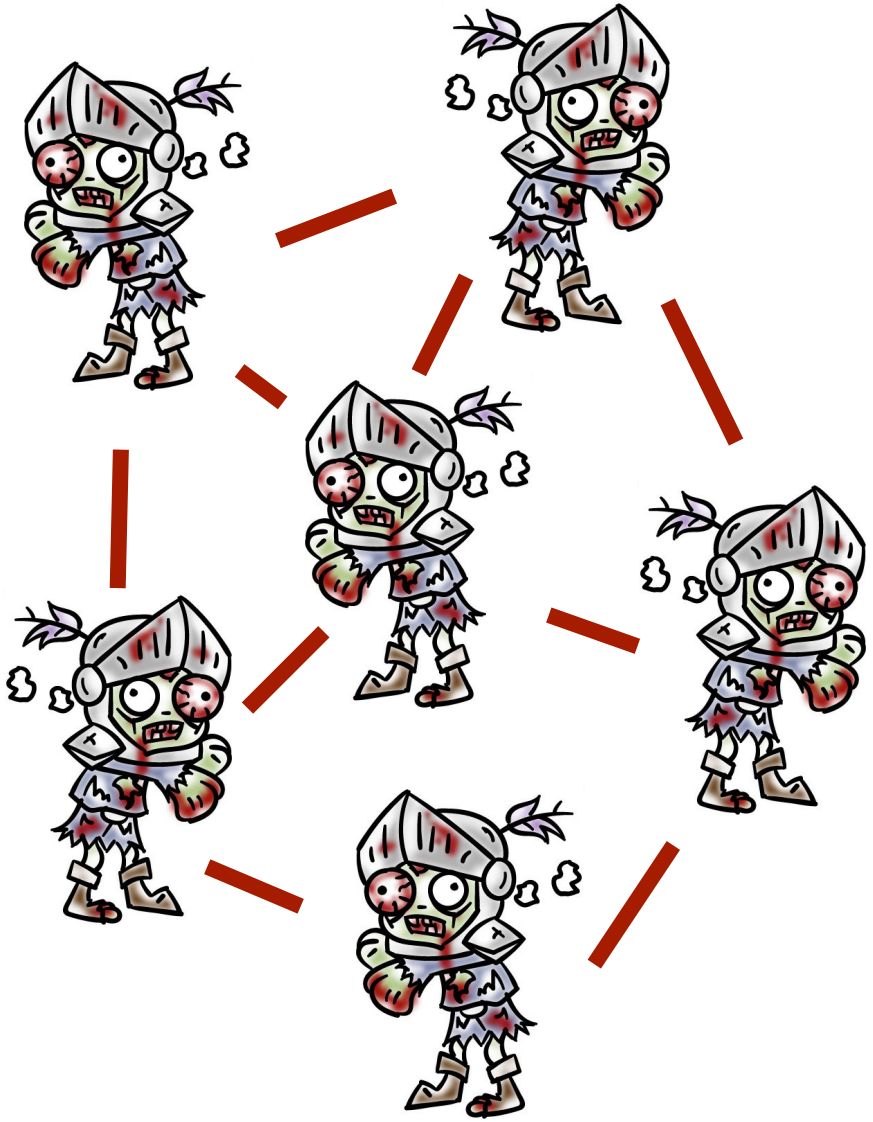
- Now, often for profit and political gains
- Technical sophistications based on the latest technologies
  - Efficiency, robustness, and evasiveness

Botnet

- **Bot (Zombie)**
  - A compromised computer under the control of an attacker
  - Bot code (malware) on the computer communicates with the attacker's server and carries out malicious activities per attacker's instructions

Botnet

- Botnet
  - A network of bots controlled by an attacker to perform coordinated malicious activities
  - Key platform for most Internet-based attacks and frauds



Bot Quiz

Match the bot with its definition by putting the correct letter in the box.

- ☐ Spamming
- ☐ Click Fraud
- ☐ Phishing

A. Used by botmasters to fraudulently increase revenue from advertisers.

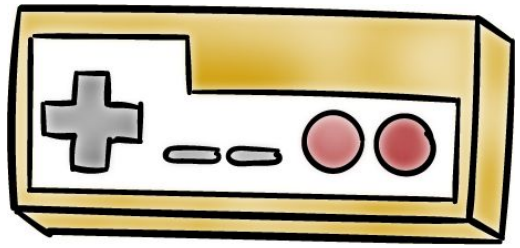
B. Used to gather valuable financial information.

C. Infected machines send out unsolicited emails.

Attacks and Frauds by Botnets

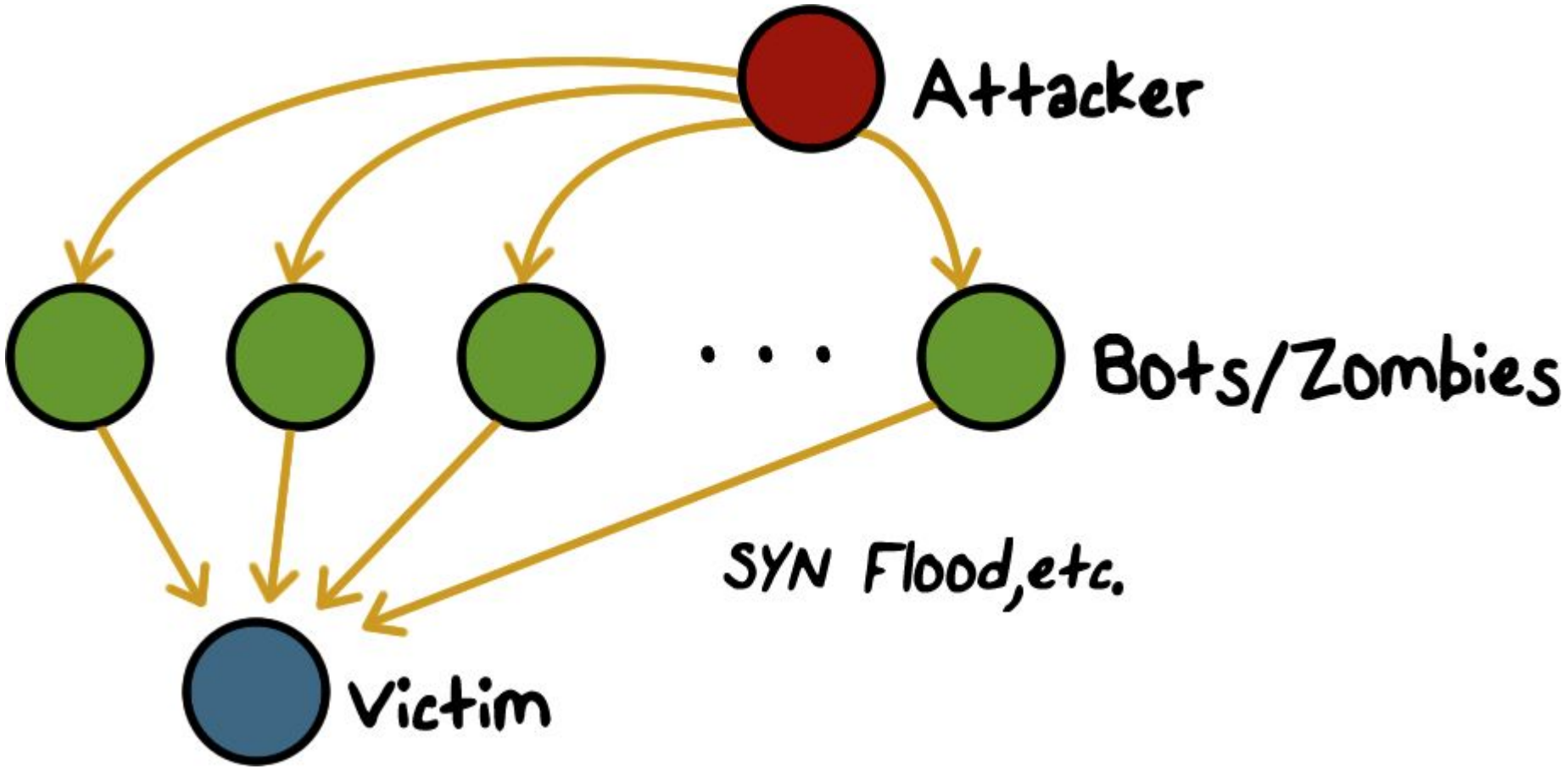
- Spam
- Distributed Denial of Service (DDOS) Attacks
- Clickfraud
- Phishing & Pharming

- Key Logging & Data/Identity Theft
- Key/Password Cracking
- ...

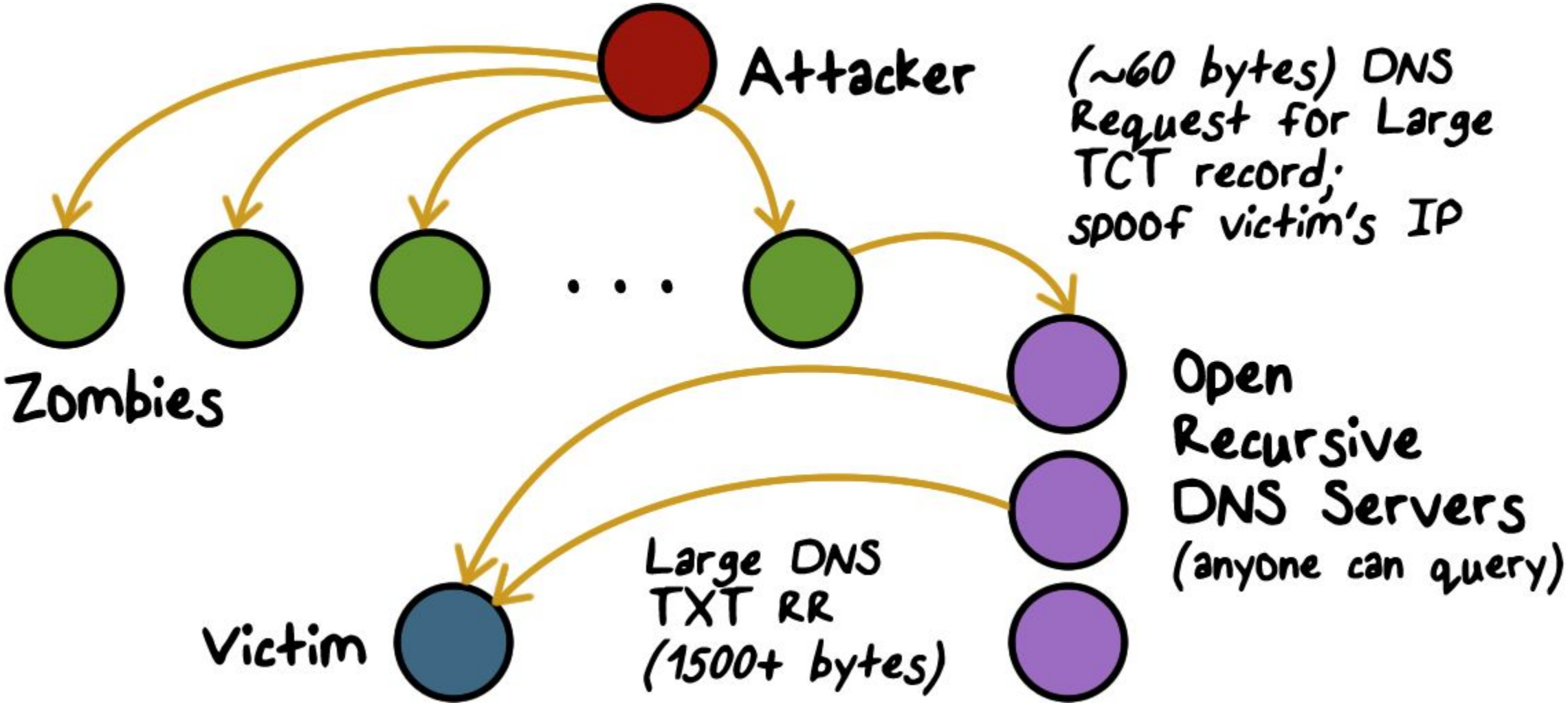


- Cheating in online games/polls
- Anonymized Terrorist & Criminal Communication

DDos Using Botnets



Amplified Distributed Reflective Attacks



DDoS Quiz

Put a check next to each of the following statements about DDoS that are true.

- ☐ The attacker does not have to use his own computer in the attack.
- ☐ Since there are so many computers involved in the attack it is difficult to distinguish legitimate from malicious traffic.
- ☐ The characteristics of DNS servers help mitigate the effect of DDos attacks.

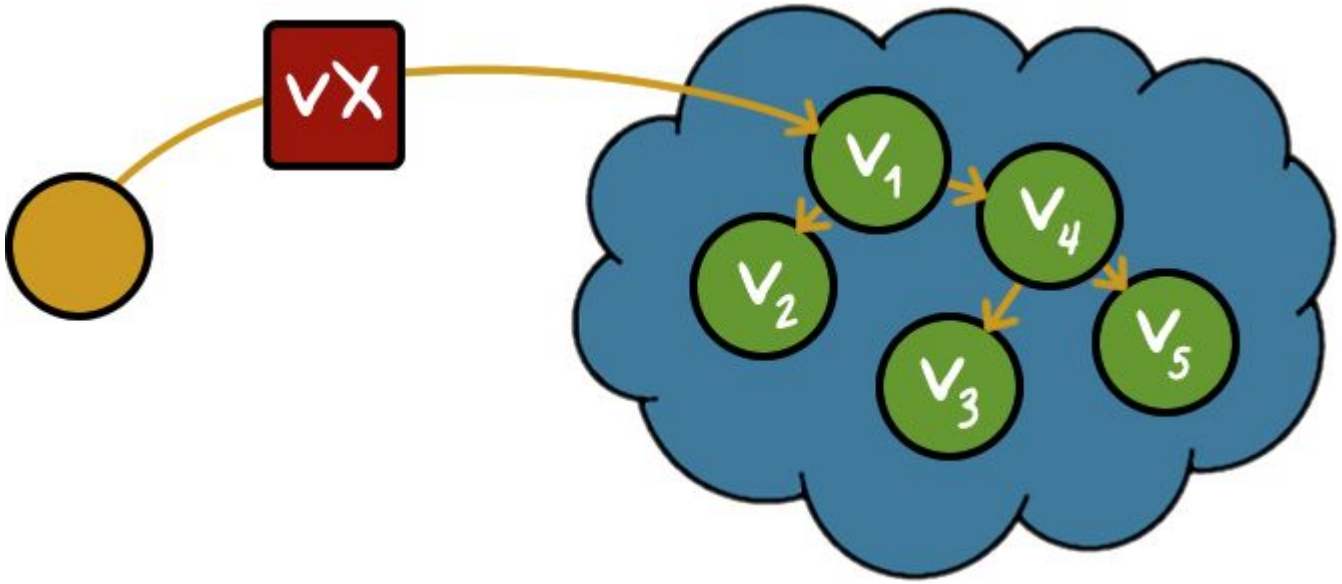
Botnet Command and Control

- Botnet is a network of compromised computers that the "botmaster" uses for malicious purposes

- There needs to be command & control (C&C) from the botmaster to the bots
  - Example: a bot reports to the botmaster its status, is directed to a site to download a malware (botcode) update, and/or receives instructions to spam/phish/DDoS, etc.

Botnet C&C Problem

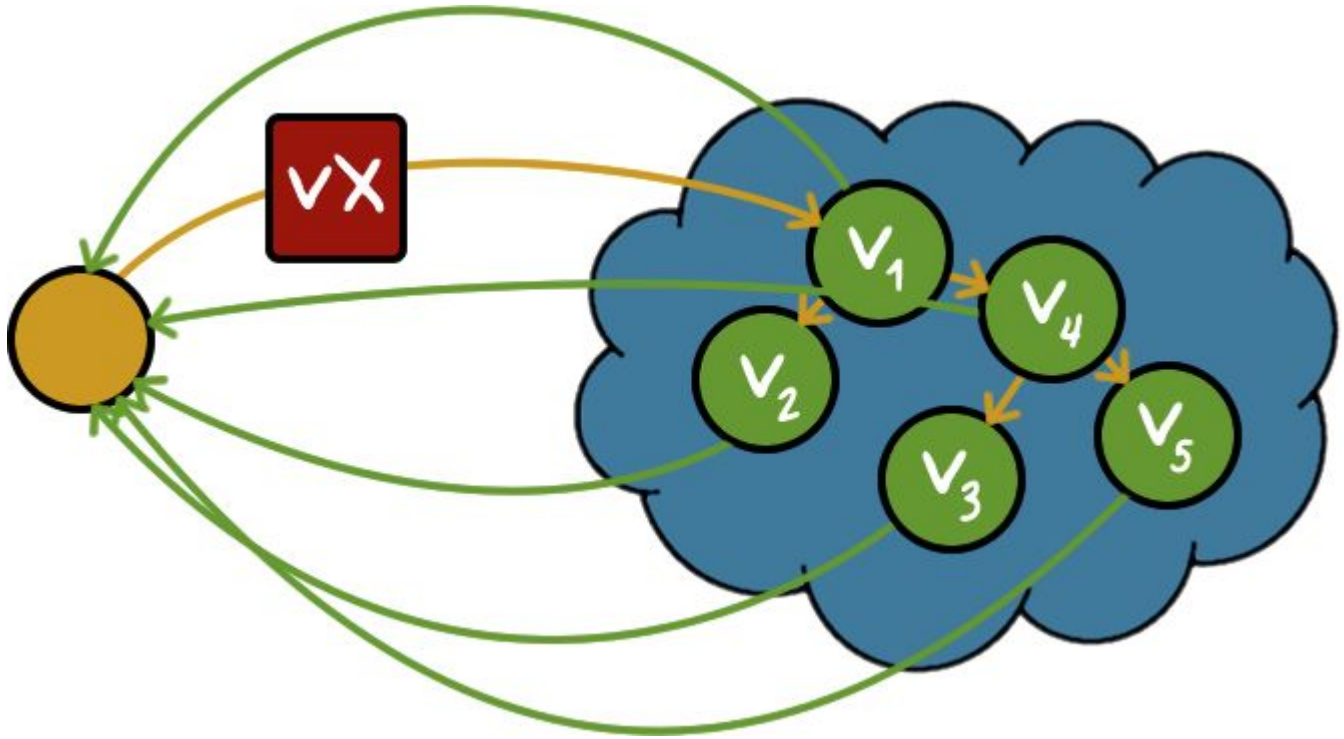
- Naively, we could have victims contact us...
  - Suppose we create malware (vx)
    - Download vx code; fiddle; compile
    - Uses email propagation/social engineering
  - We mail it...



Spreading is easy, but what if we want to use the compromised computers (victims)?

Botnet C&C- Naive Approach

- Naively, we could have victims contact us...



- Problems:
  - VX must include author's address (not stealthy)
  - Single rallying point (not robust)
  - VX has hard-coded address (not mobile)

Botnet C&C Design

- How can bots contact their master safely?
- Simple, naïve approach:
  - Victims contact single IP, website, ping a server, etc.
  - Easily defeated (ISP intervention, blackhole routing, etc.)
  - Still used by script-kiddies, first-time malware authors

Botnet C&C Design

Design considerations:

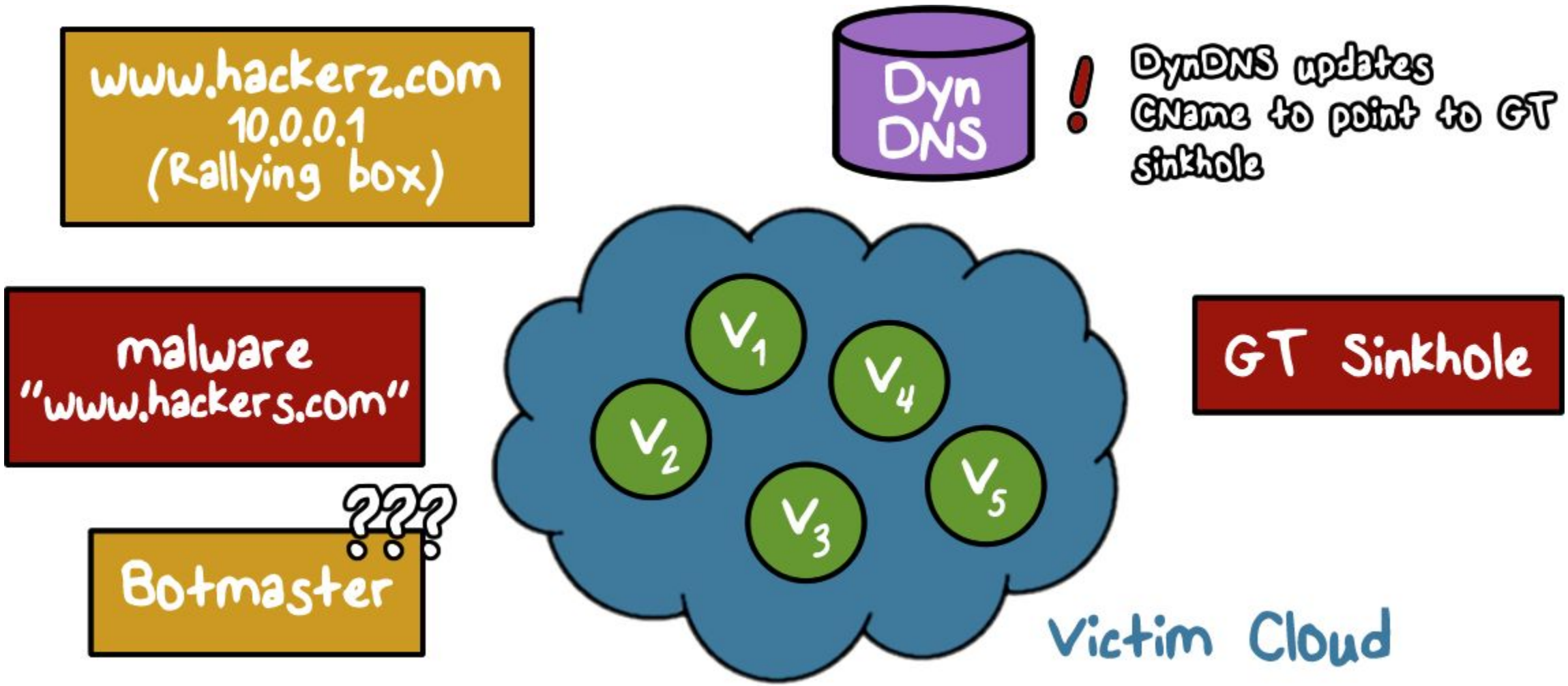
- Efficient and reliable
  - Able to reach to a sizable set of bots within a time limit
- Stealthy
  - Hard to detect (i.e., blended with normal/regular traffic)
- Resilient
  - Hard to disable or block

C&C Design Quiz

Mark the following statements as either true (T) or false (F):

- [ ] Bots have more sophisticated communication capabilities than worms and viruses
- [ ] Bots require direct communication with the C&C server before beginning an attack
- [ ] A botnet will be less likely to be found if it uses custom communication protocols

DNS-Based Botnet C&C



Botnet C&C Quiz

Which of the following C&C schemes provide:

- Efficient/reliable communications
- Stealth communications (hard to detect)
- Resilient communications (hard to disrupt)

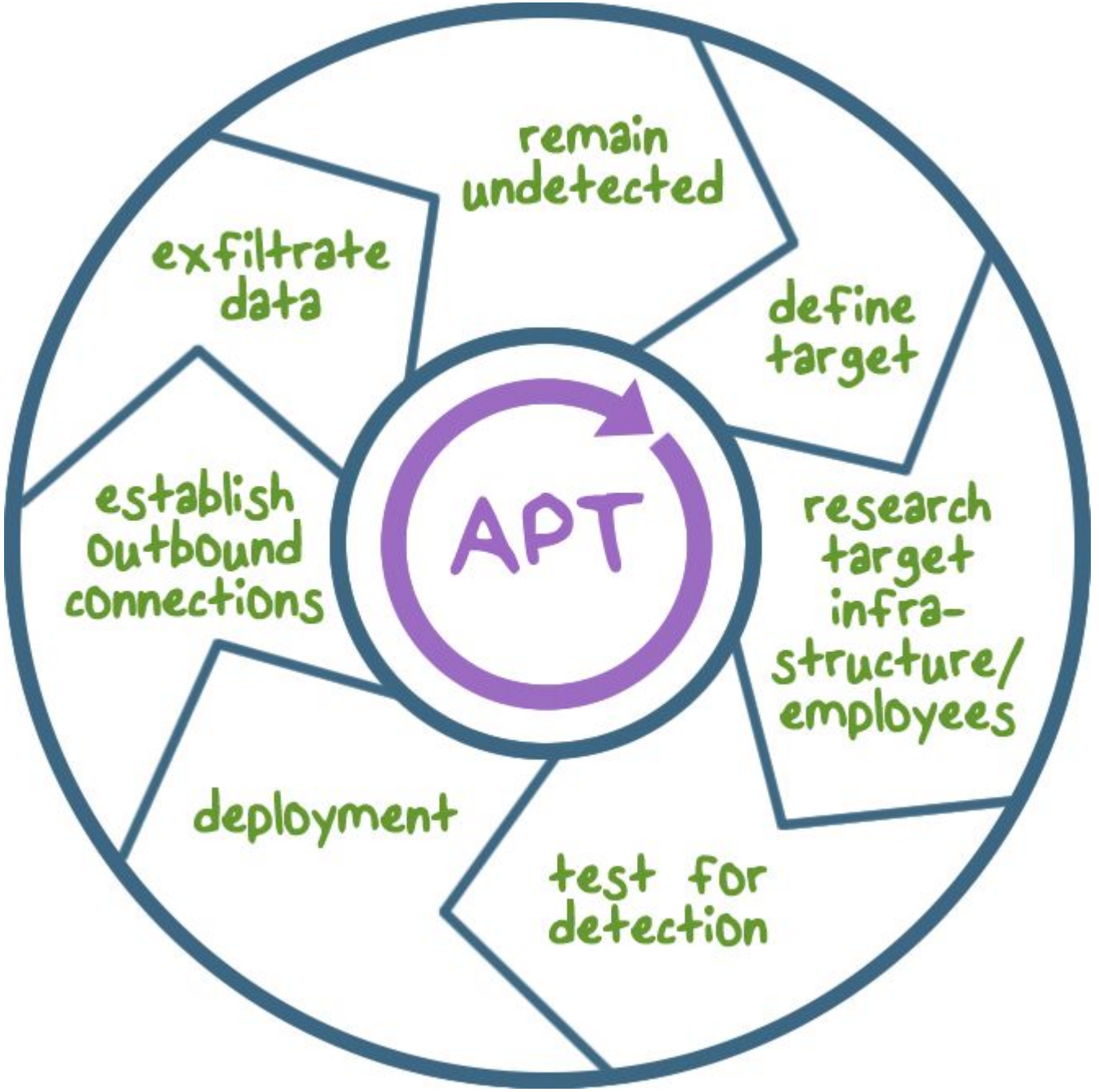
Check all that apply:

- ☐ A Gmail account is used for C&C, email address hardcoded in botcode
- ☐ P2P protocol is used for C&C, query string is hardcoded in botcode
- ☐ A "news" web site has been set up for C&C, i.e., commands can be "parsed" from news articles. Website and parsing logic hardcoded in botcode.

Advanced Persistent Threat (APT)

- **Advanced:**
  - (Special) malware
  - Special operation and operators
- **Persistent:**
  - Long-term presence, multi-step, "low-and-slow"
- **Threat:**
  - Targeted at high-value organization and information

APT Lifecycle



APT Characteristics

- **Zero-day exploit** or a specially crafted malware
  - No readily available signature for its detection

APT Characteristics

- Social-engineering to trick even the most sophisticated users. Example:
  - First compromise core internal network control elements such as routers and web servers to learn about the valuable targets;
  - Then play man-in-the-middle (MITM) on the compromised routers/server to make social-engineering attacks very convincing, e.g., to even forge answers to challenge or inquiry by suspecting users

APT Characteristics

- Carry out its intended mission, such as data tampering and exfiltration, in a low-and-slow fashion to completely blend in with normal activities
- Example:
  - Acts only when the targeted user is authoring and sending a document
  - Make repeated, small incremental change to data to accomplish the eventual attack goal
  - Not detectable anomaly by existing approaches

APT Characteristics

- APT is a persistent operation that involves multiple deliberate steps over time, rather than a single attack act

- Example:
  - Employ a combination of steps to move laterally through the network and target only the necessary systems and users at each attack step

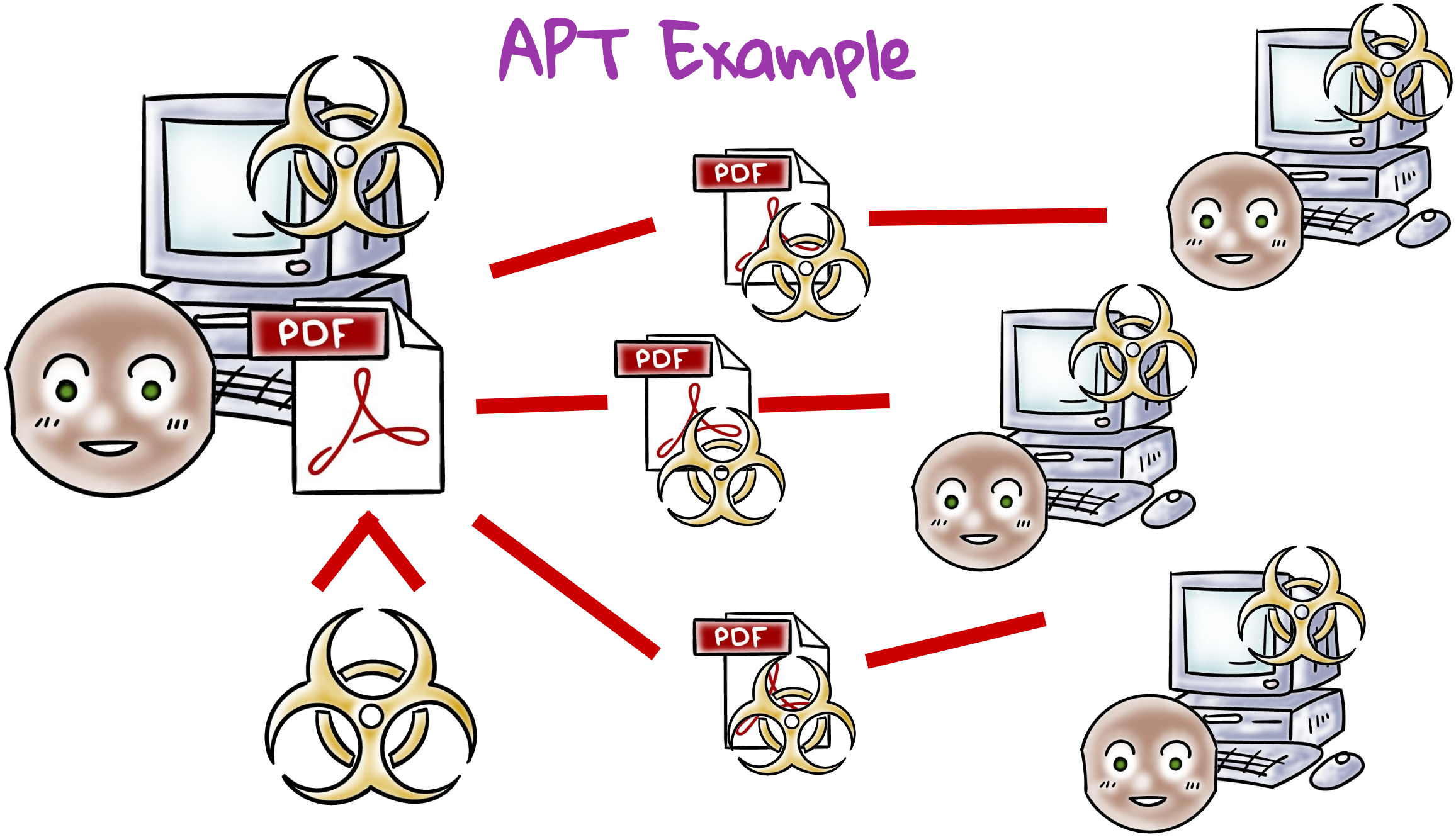
APT Quiz

Match the following by writing the corresponding letter in the boxes:

- ☐ Boy in the Middle
- ☐ Clickjacking
- ☐ Man in the Browser
- ☐ Man in the Middle
- ☐ Keyloggers

A. Eavesdrops
B. Modifies web pages covertly
C. Covertly records keystrokes
D. Covertly changes a computer's network routing
E. Web users unknowingly click on a something that is not as it is portrayed

APT Example

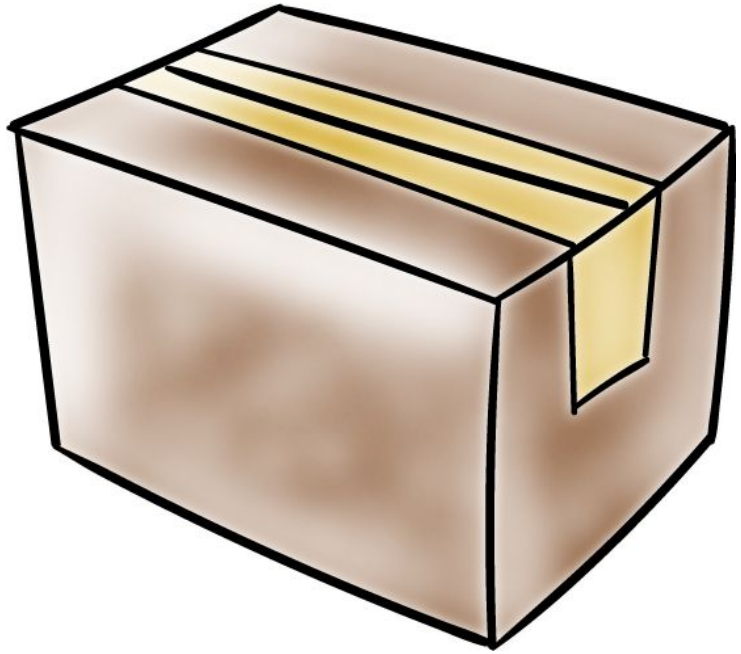


Malware Analysis

- Produce info for detection/response
- **Static Analysis:** Attempts to understand what a malware instance would do if executed
- **Dynamic Analysis:** Attempts to understand what a program does when executed
  - Different granularities
    - Fine-grained (e.g., automated unpacking)
    - Coarse-grained (e.g., system call tracing)

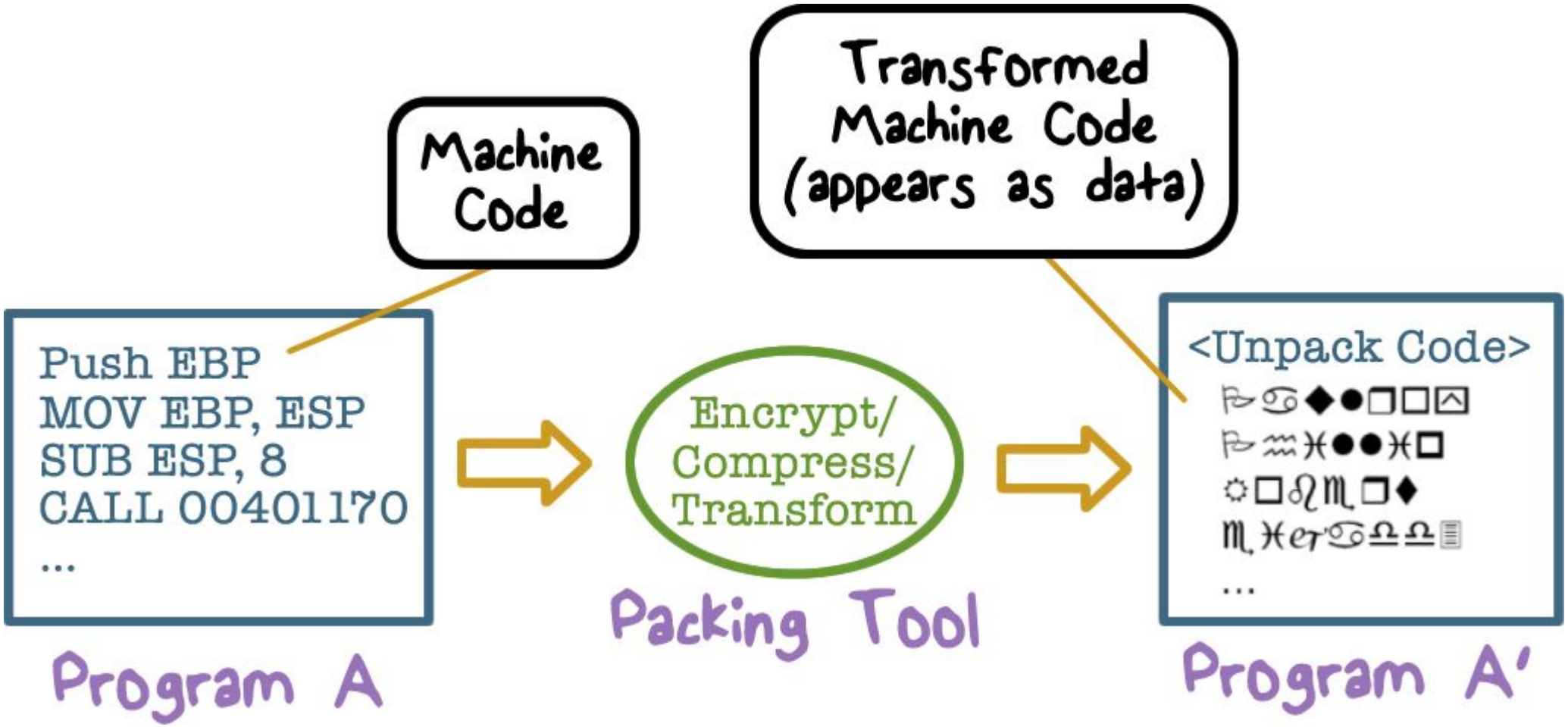
Malware Obfuscation

- **Packing:** a technique whereby parts or all of an executable file are compressed, encrypted, or transformed in some fashion

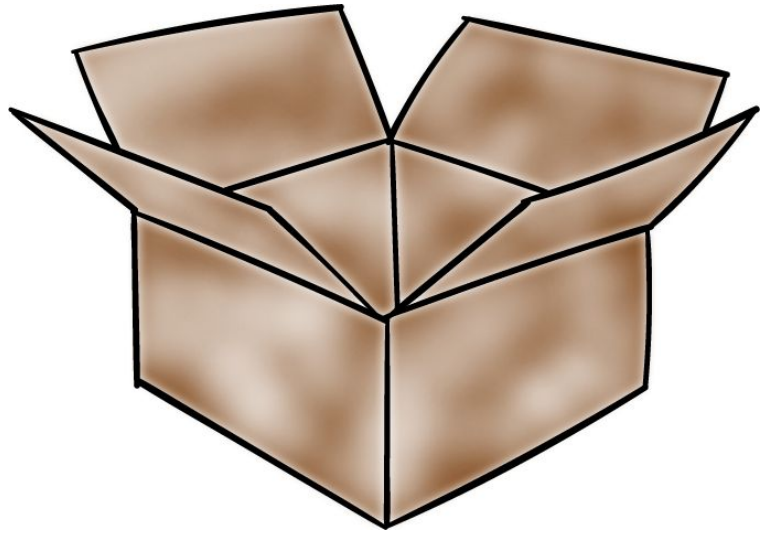


- Code that reverses the pre-runtime transformation is included in the executable

Malware Obfuscation



Unpacking



- Most modern malware comes packed
  - Thousands of packers, countless ways to obfuscate code
  - Volume of malware samples makes manual unpacking untenable
- Need for automated unpacking that does not require a priori knowledge
- Fine-grained tracing-based universal automated unpacking algorithms
  - =Detect the execution of code not in the static code model (i.e., the model of the packed program)

Malware Analysis Quiz

What approach(es) can be used to detect the example APT malware (the malicious browser extension)

- [ ] A network monitor that analyzes traffic to detect anomalies or known bad traffic (e.g., to known bad domains)
- [ ] A host monitor that examines operating systems activities (e.g., access to files)
- [ ] A malware analysis system that identifies malicious logic (e.g., running the browser in a sandbox & tracing its execution)

Modern Malware
Lesson Summary

- Botnets use command-and-control mechanisms
- APTs can hide tracks, and lay “low and slow”
- Need network monitoring, and static and dynamic analysis of malware