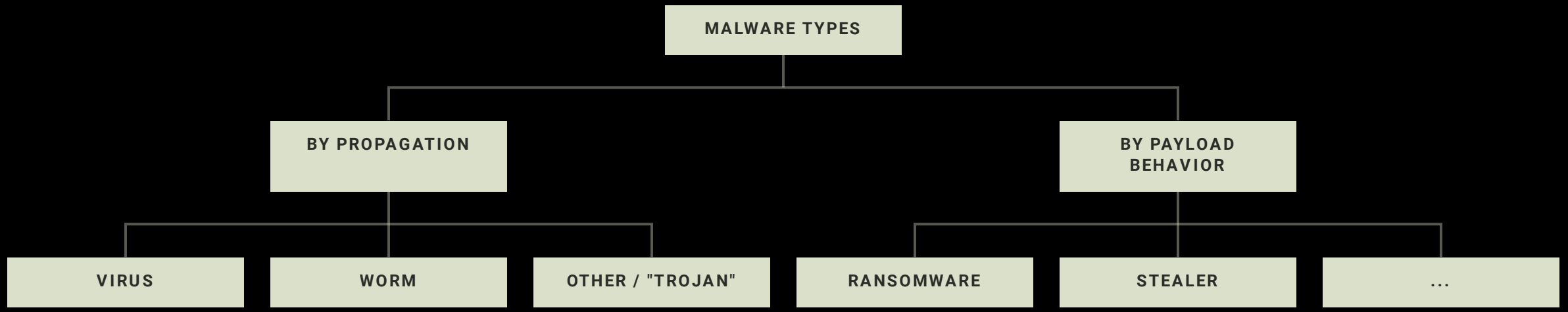
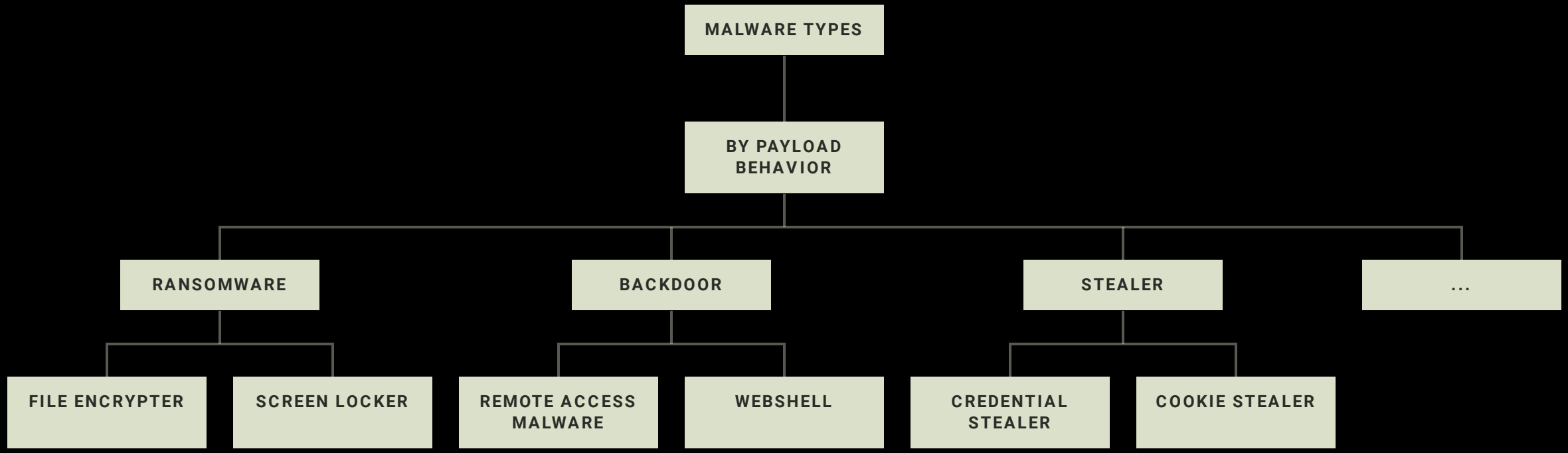
Malware Types by Payload Behavior

Malware Types



Malware Types by Payload Behavior



Dealing with Malware Type Overlaps

1. **MOST SEVERE TYPE FIRST**

   worm and virus > behavioral malware types

   backdoor > stealer, keylogger, ...

2. **FOCAL POINT OF MALWARE**

   remote access malware with stealing features --> backdoor

3. **MIXED TYPES**

   Worm + Ransomware = Ransomworm

Confusing Malware Types

Confusing Malware Types

1

DROPPER

carries other malware in its body

drops it to disk and executes it

2

DOWNLOADER

downloads other malware in from the Internet

and runs it

3

LOADER

loads other malware

that malware can either be downloaded or carried

Confusing Malware Types

1

BACKDOOR

provides unauthorized access to attacker

access may only be a shell

or full remote control

2

REMOTE ACCESS MALWARE

is a form of backdoor

attacker can control computer as if they sit in front of it

often also capabilities of: stealer, ransomware, keylogger, ...

Beware: These are **not** malware types

- **EXPLOIT**
  can be a technique for worm propagation or privilege escalation
  can be used by people (without malware)

- **REMOTE ACCESS TOOL**
  legitimate program to assist remotely
  can be abused by threat actors --> installed without consent
  riskware verdict if easily abusable