Malware Types by Propagation

Malware Type

Classification of malware families into groups with similar behavior or intent

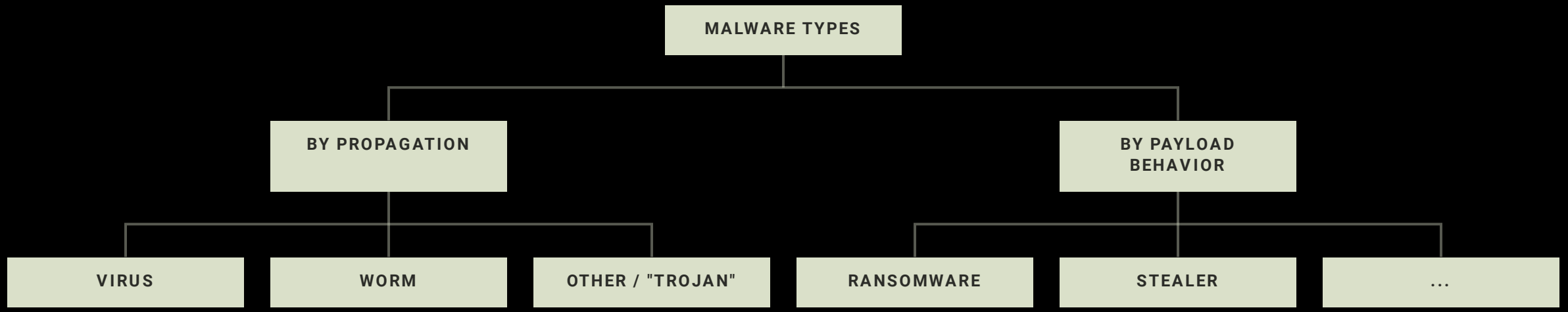
Most important characteristic/common behavior in one word

Malware Type

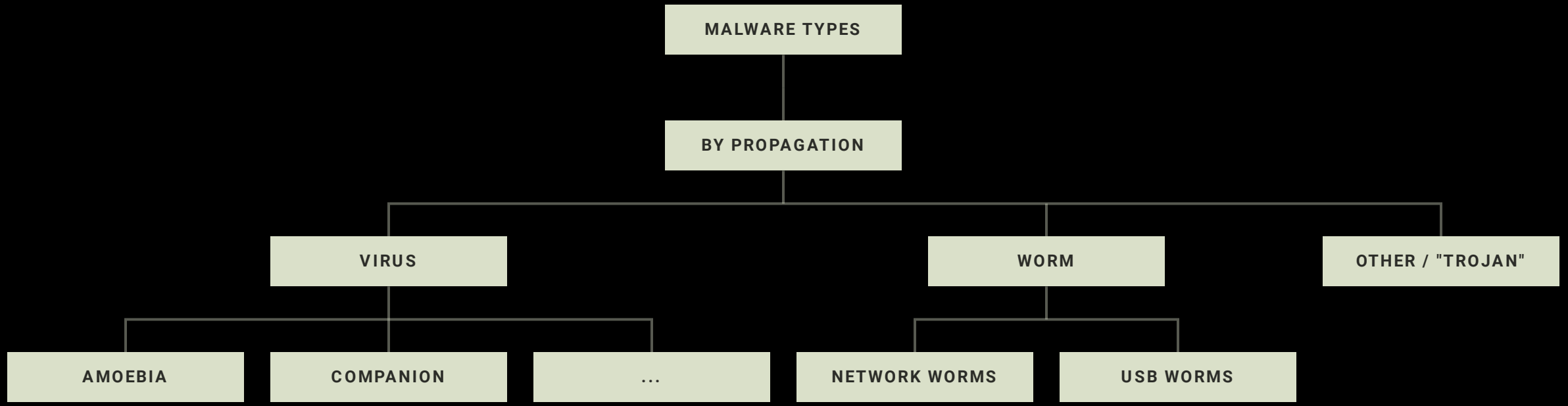
Communicate severity

If several types fit, the most severe is used.

Malware Types



Malware Types by Propagation



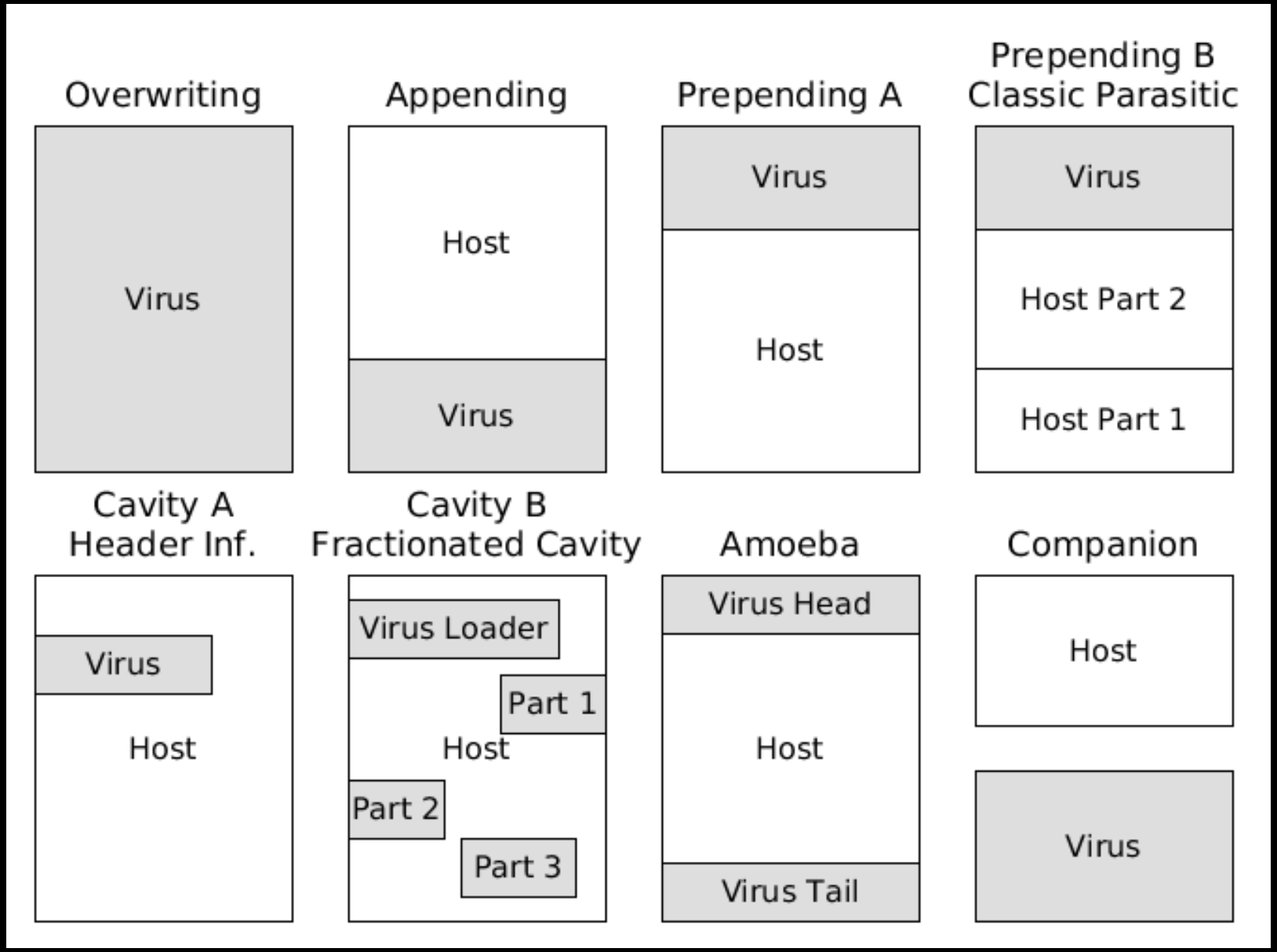
Virus

- aka "file infector"
- common media: "virus" == "malware"
- malware analysts: "virus" == "file infector"

Virus

- replicates itself
- infects other files (aka host files)
- those files are infectious themselves

File Infection Strategies by Peter Szor



Worm

Self-replicating either via the network or removable media.

Other / "Trojan"

All malware that is neither worm nor virus.

Better described by payload behavior

Beware of the term "Trojan"

The different meanings of "Trojan"

CLASSICAL TROJAN HORSE

- useful application is inherent part of malware family
- e.g. AIDS ransomware

INFECTION VECTOR

- using tools to bind legitimate program with malware
- or using legitimate seeming filename, icon, version info, ...
- no inherent characteristic of family

SYNONYM FOR MALWARE

- especially in news articles
- e.g. in the term "Remote Access Trojan" (RAT)

MALWARE WITH NO SELF-PROPAGATION

- neither worm nor virus