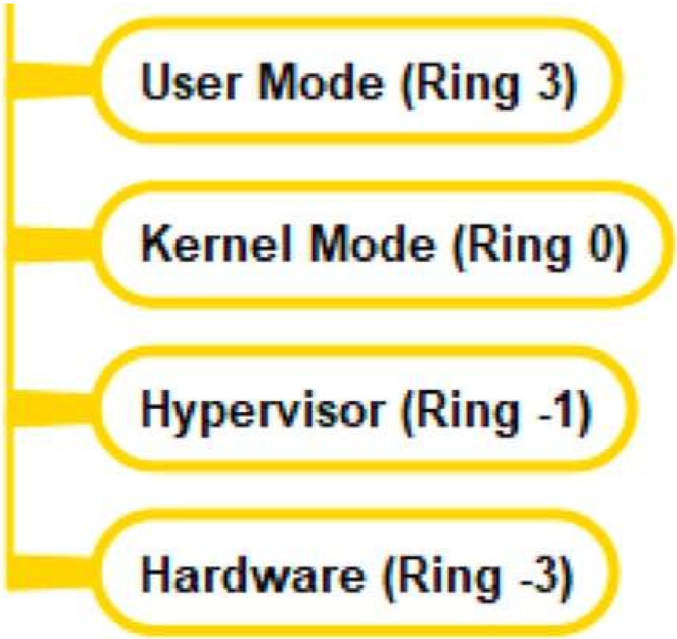
# Classification of Malware by Privilege
## (Protection Rings)



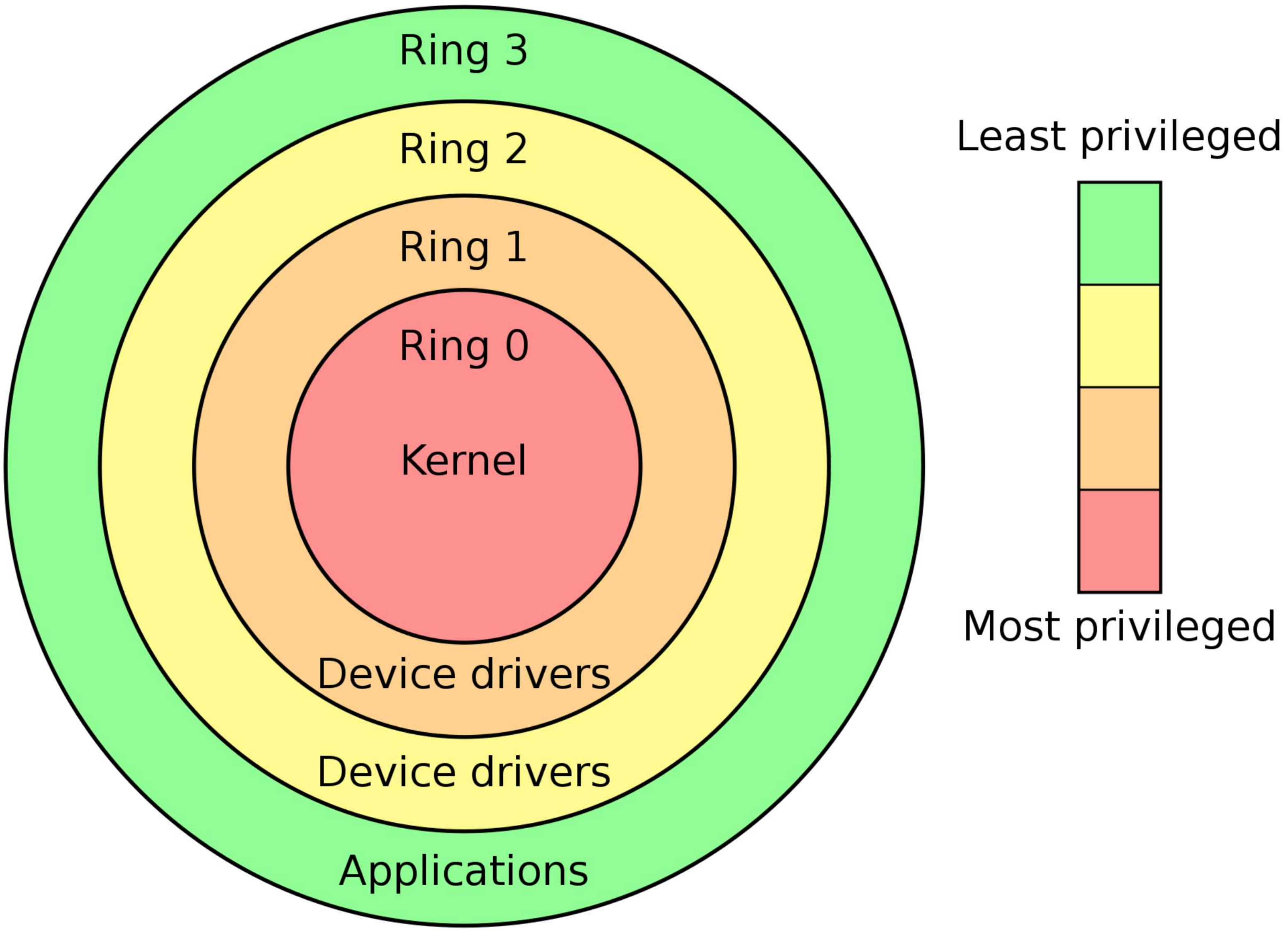
User Mode (Ring 3)

Kernel Mode (Ring 0)

Hypervisor (Ring -1)

Hardware (Ring -3)

**A protection ring** is one of two or more hierarchical *levels* or *layers* of privilege within the architecture of a computer system.



# Protection Rings

- Code running at a lower protection rings has more privileges (e.g., read/write permissions) over code running at higher ones.
- Rings 1 and 2 are not used by Windows.
  - User mode (Ring 3)
  - Kernel mode (Ring 0)
  - Hypervisor (Ring -1)
  - Hardware (Ring -3)

# User mode (Ring 3)

- When a new process is started, its code is loaded into the RAM with user mode privileges.
- Any code that does not require more than user mode privileges is considered user mode code.
- In Windows operating systems, this includes any software installed by the user, as well as large parts of the operating system itself (even the Administrator account has only user mode privileges).
- When analyzing **user-mode malware**, *the infection can be cleaned easily by undoing the changes made by the malware or by reformatting the system completely.*

# Kernel mode (Ring 0)

- The **kernel** is the part of the operating system responsible for handling the system resources.
- It provides functionality for communicating with the hardware, and it is responsible for managing all aspects of the system (memory, networking, process priorities, CPU time, etc.).
- The kernel runs at Ring 0 with kernel mode privileges (aka root privileges).
- **Ring 0** is reserved only for the OS kernel and system drivers.

# Kernel mode (Ring 0)

- It allows the operating system to control the physical devices, manage resources such as CPU time or memory allocation, and control user mode code.
- Kernel mode code can load new code into the kernel when necessary, for example when new hardware is connected to the system (like a camera or USB storage device).
- This type of code is called a driver, and it provides the necessary functions to allow interaction with the new device.
- Malware might gain access to the system’s kernel to perform operations with root privileges, and thus this type of malware is also called a rootkit

# Hypervisor (Ring -1)

- Hypervisor technology enables the execution of several virtual operating systems simultaneously on the same physical hardware.
- A hypervisor runs with more privileges than kernel mode; thus, is said to be running in Ring -1, even though this is not an actual protection ring.
- There are two types of hypervisors:
  1. **Type 1 hypervisors** support multiple operating systems running in parallel.
  2. **Type 2 hypervisors** allow the execution of a virtual machine.

# Hypervisor (Ring -1)

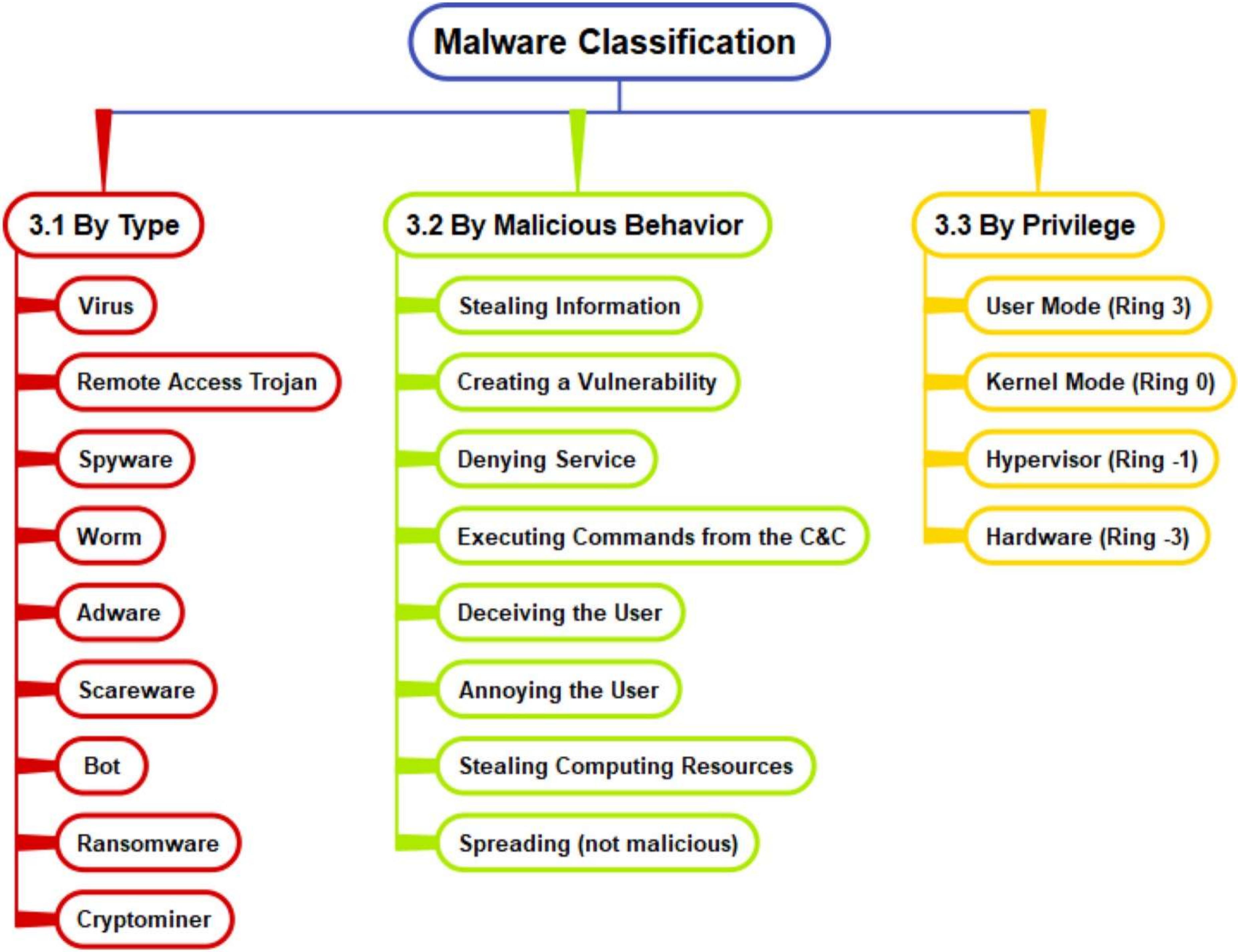
- Malware authors try to exploit the potential of hypervisors.
- A malicious hypervisor can be installed to trap the operating system in a virtual machine (VM) and take away its root privileges, hence gaining superiority over the kernel, effectively giving it control of the operating system.
- Any analysis tool installed on the OS will be unaware of code executed by the hypervisor.
- Malware that installs a malicious type 1 hypervisor is called a virtual machine-based rootkit (VMBR).

# Hardware (Ring -3)

- Infecting a hardware device means that the malware can run freely without fear of detection, and launch attacks against other devices from outside the CPU (aka Ring-3 Rootkit).
- Malicious firmware update is a common attack to achieve hardware privileges.
- Every hardware component includes code (firmware) that operates the device.
- The firmware can be updated from time to time to fix bugs and patch security vulnerabilities.

# Hardware (Ring -3)

- However, if a vulnerability in the update process is discovered by an attacker, then the vulnerability could be used to install malicious firmware that is hidden from the CPU and can be used to launch an attack on the system.
- Such hardware infection is common in USB, IoT, and medical devices.



Malware Classification

3.1 By Type

- Virus
- Remote Access Trojan
- Spyware
- Worm
- Adware
- Scareware
- Bot
- Ransomware
- Cryptominer

3.2 By Malicious Behavior

- Stealing Information
- Creating a Vulnerability
- Denying Service
- Executing Commands from the C&C
- Deceiving the User
- Annoying the User
- Stealing Computing Resources
- Spreading (not malicious)

3.3 By Privilege

- User Mode (Ring 3)
- Kernel Mode (Ring 0)
- Hypervisor (Ring -1)
- Hardware (Ring -3)