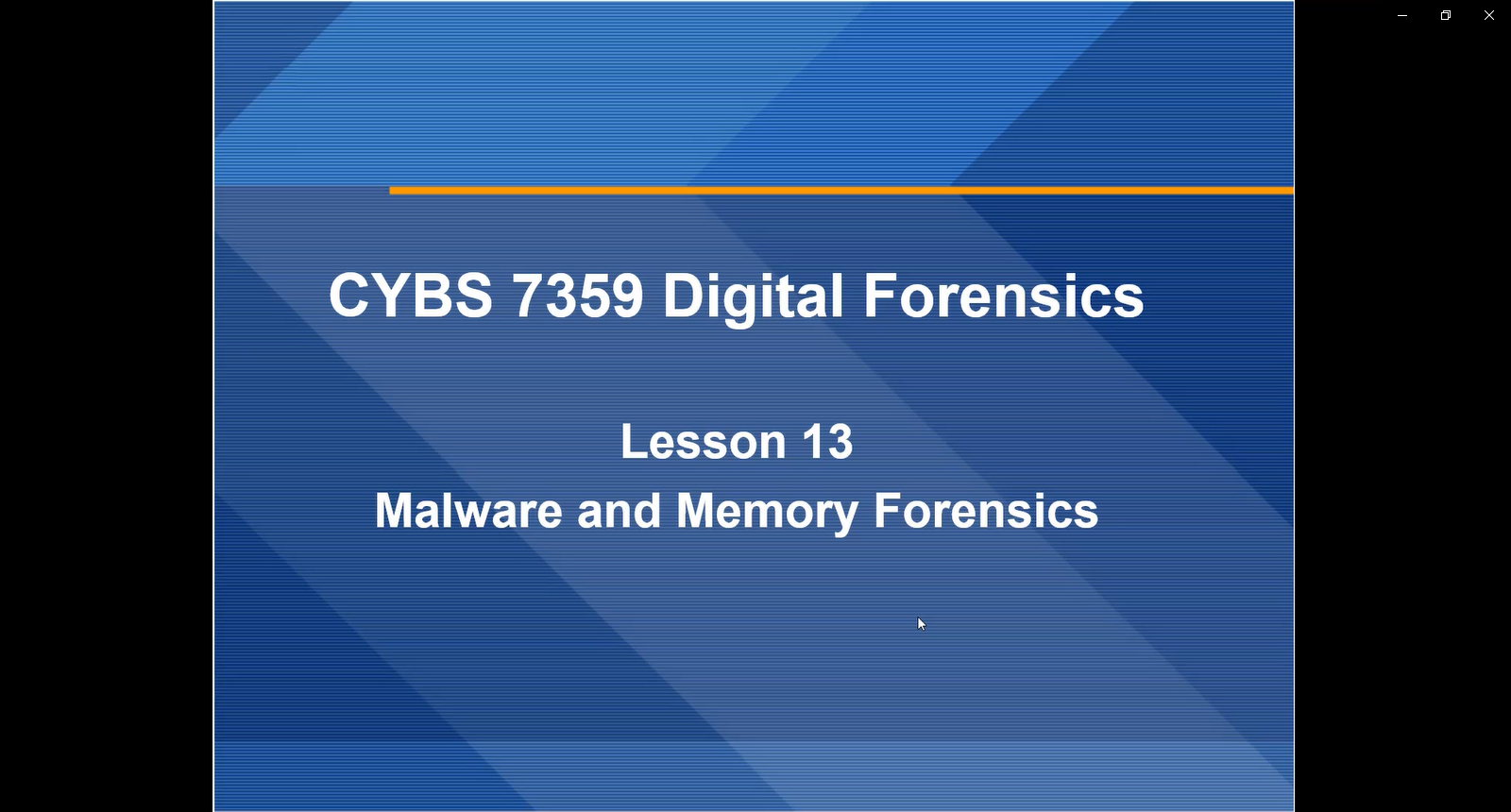
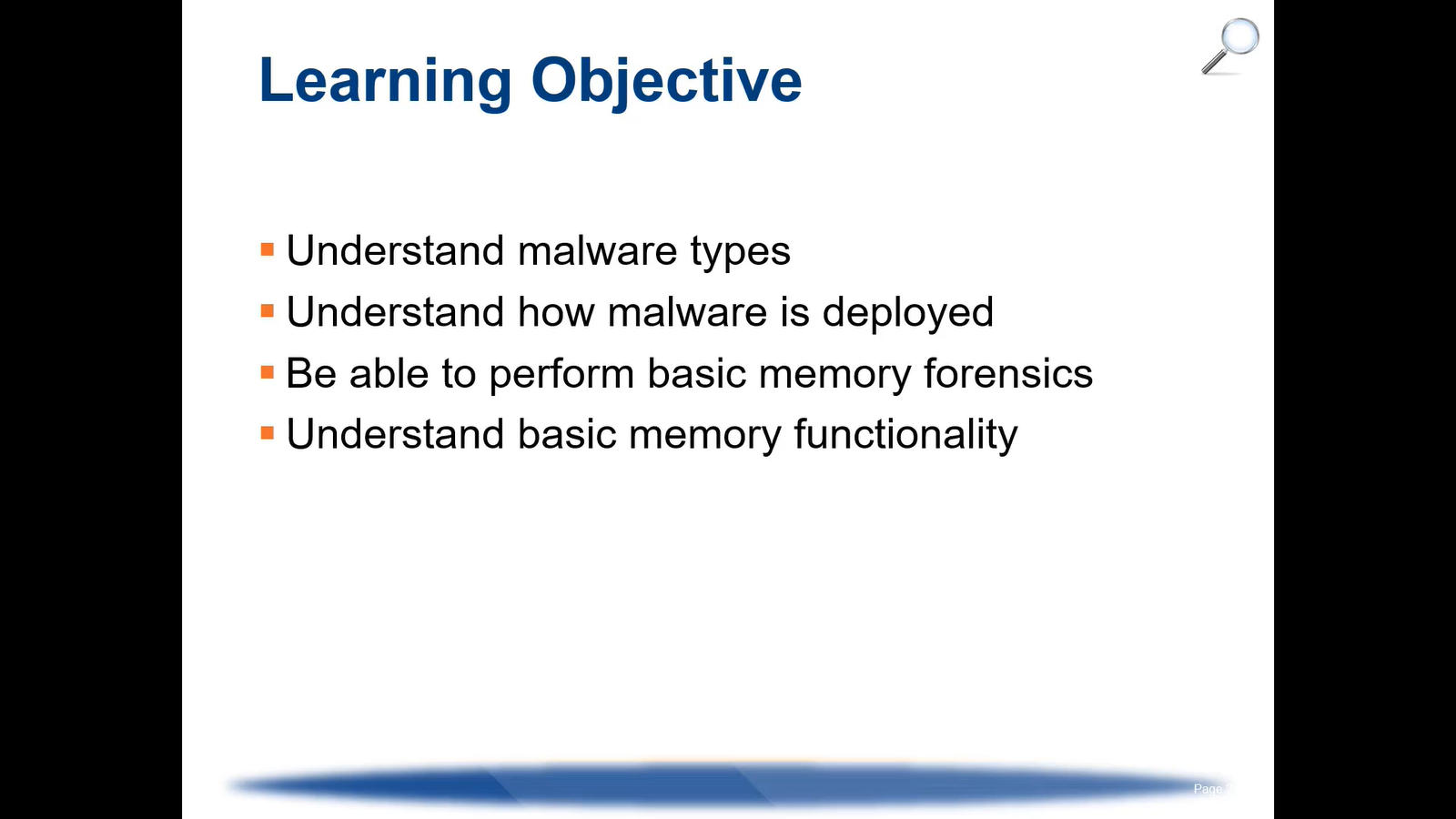
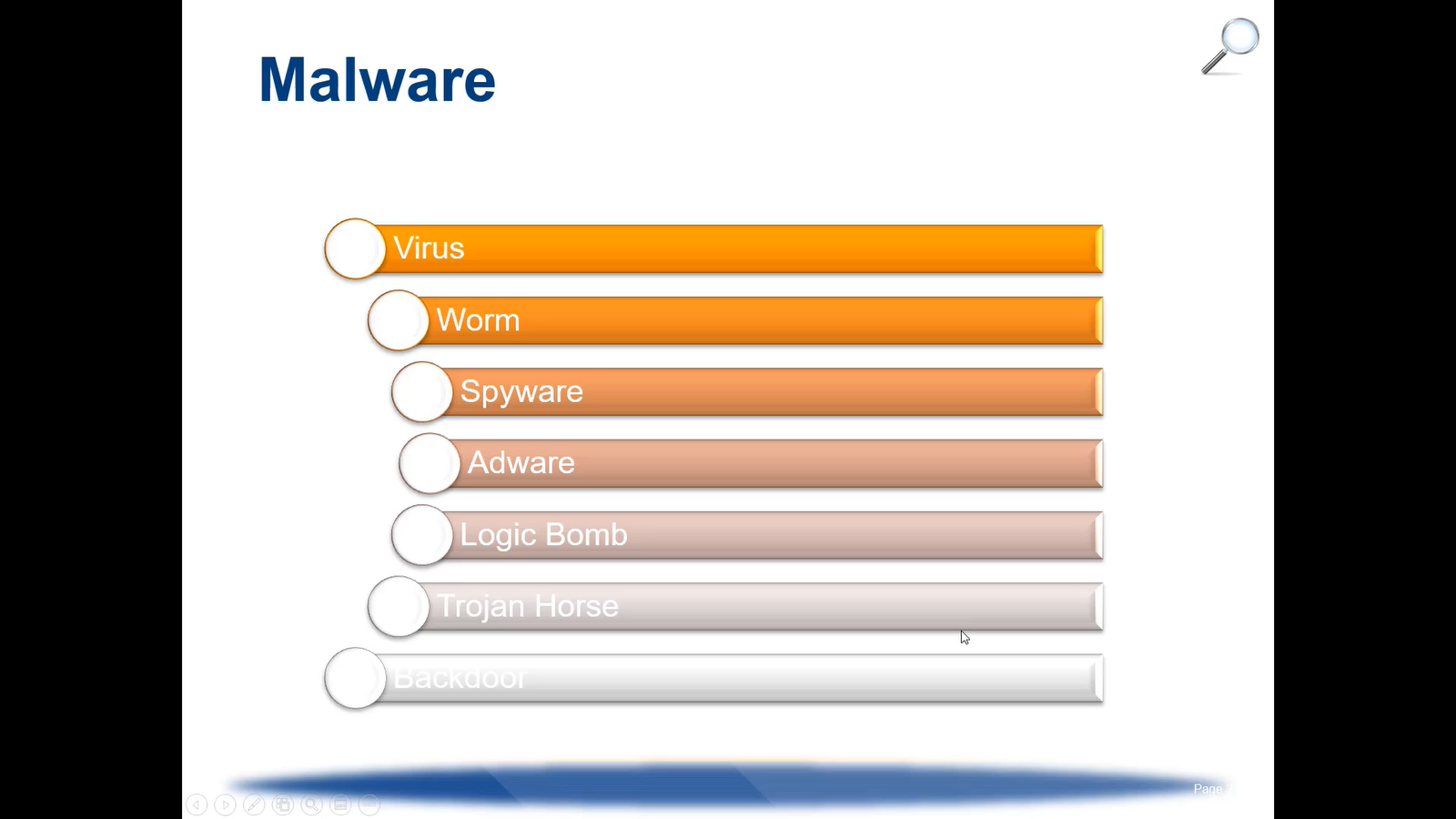
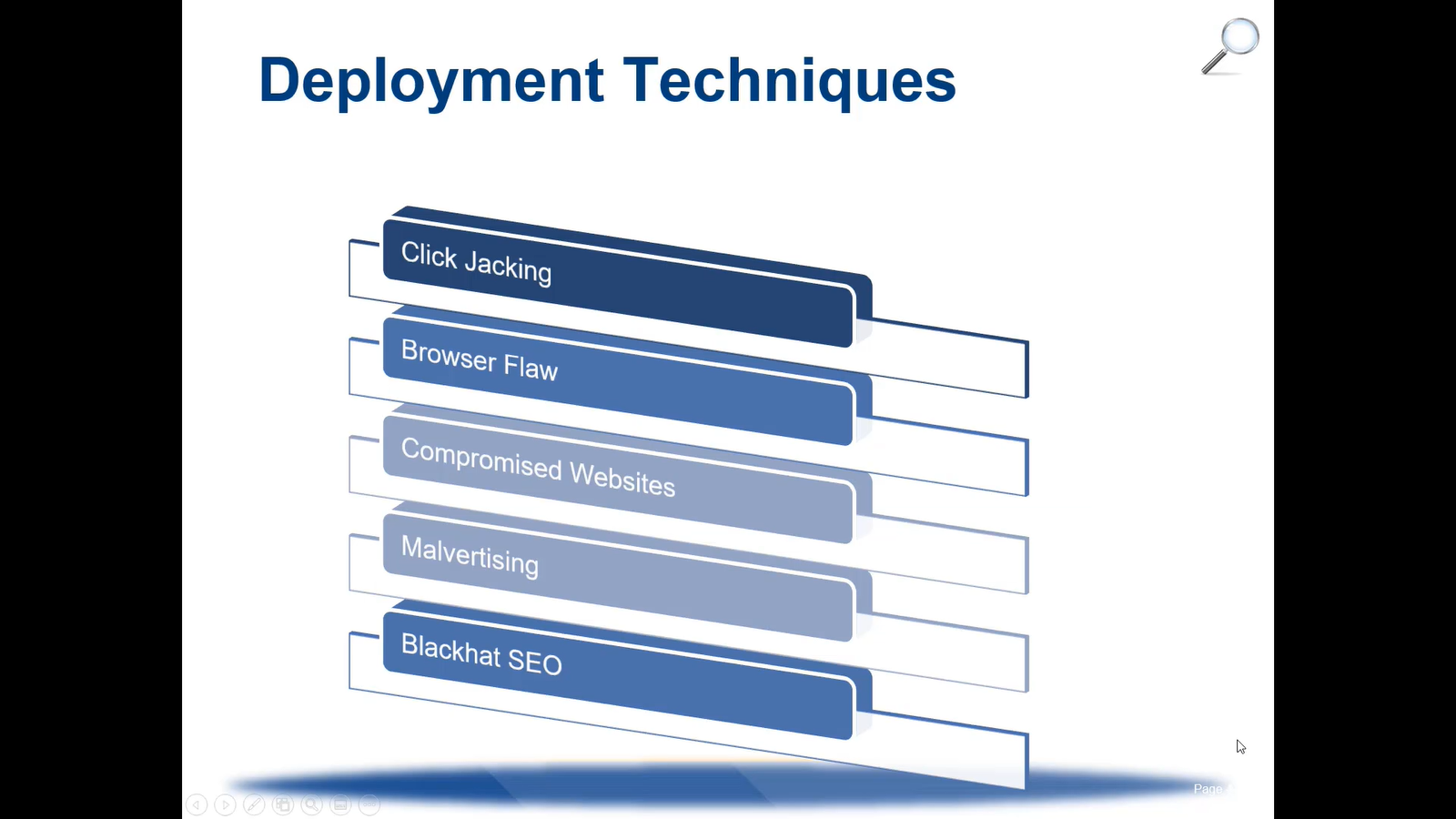
Malware and Memory Forensics Notes

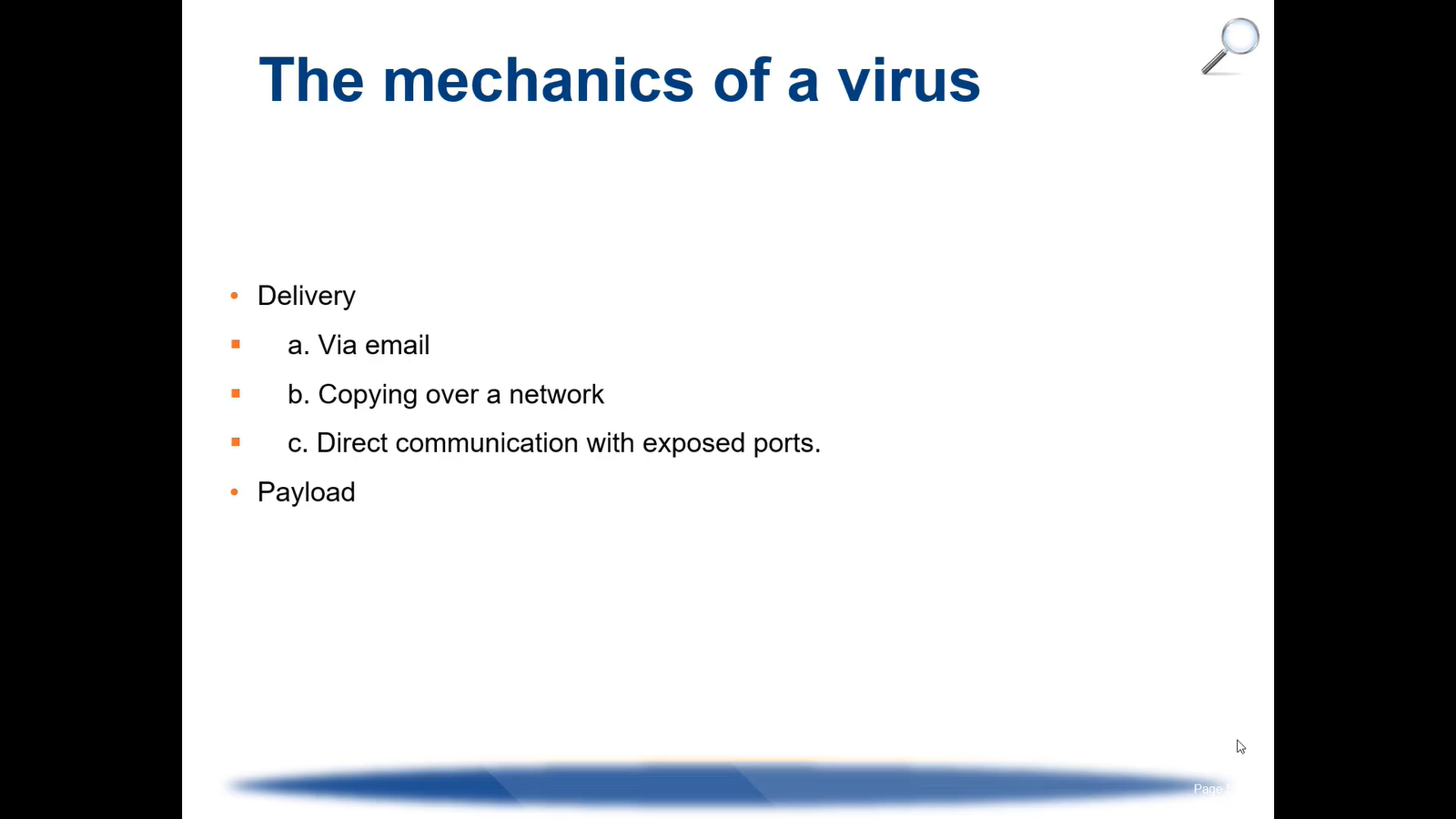


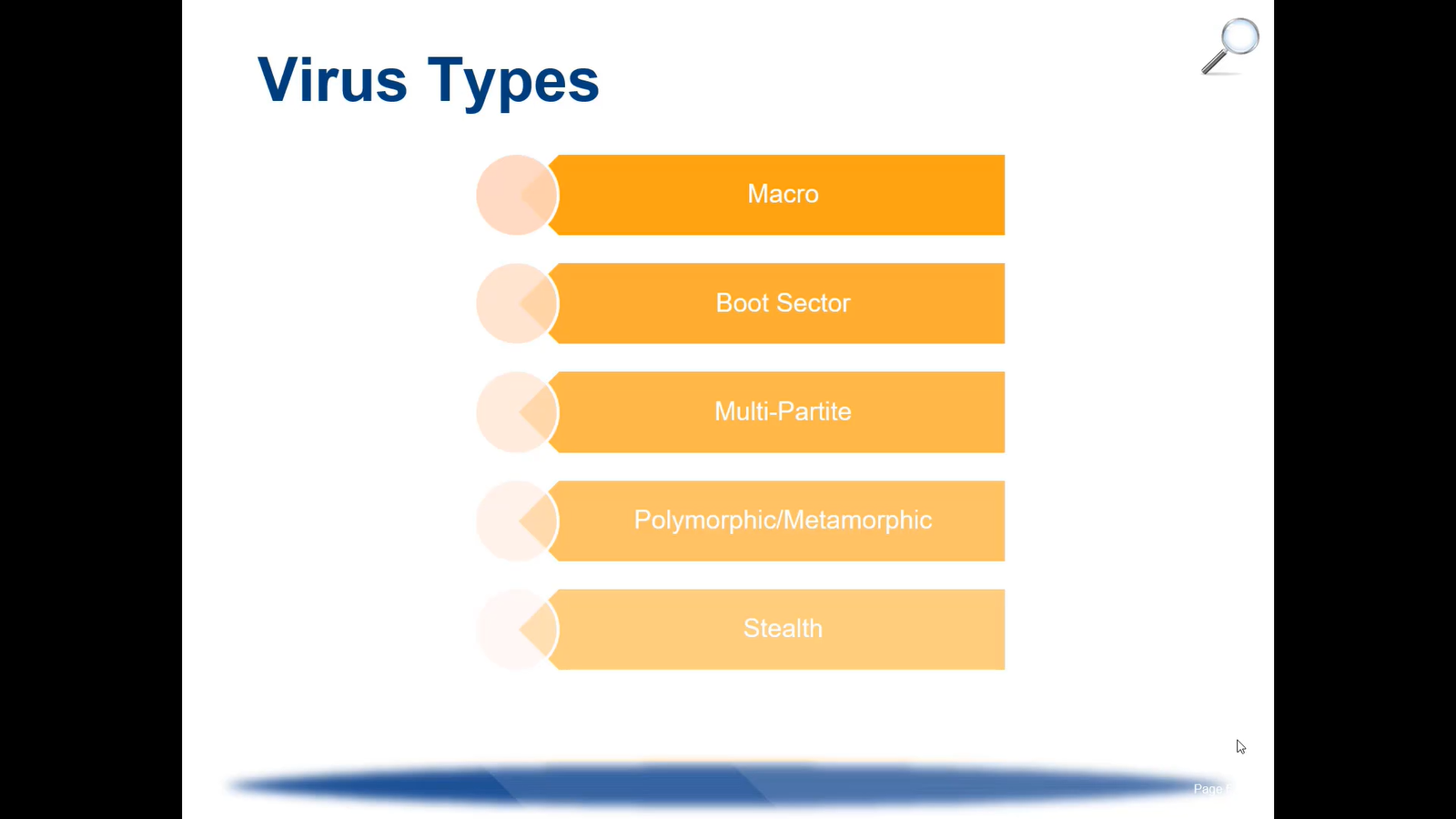






Malvertising and Blackhat SEO: Designed to get traffic (have users access) to sites that are infected.



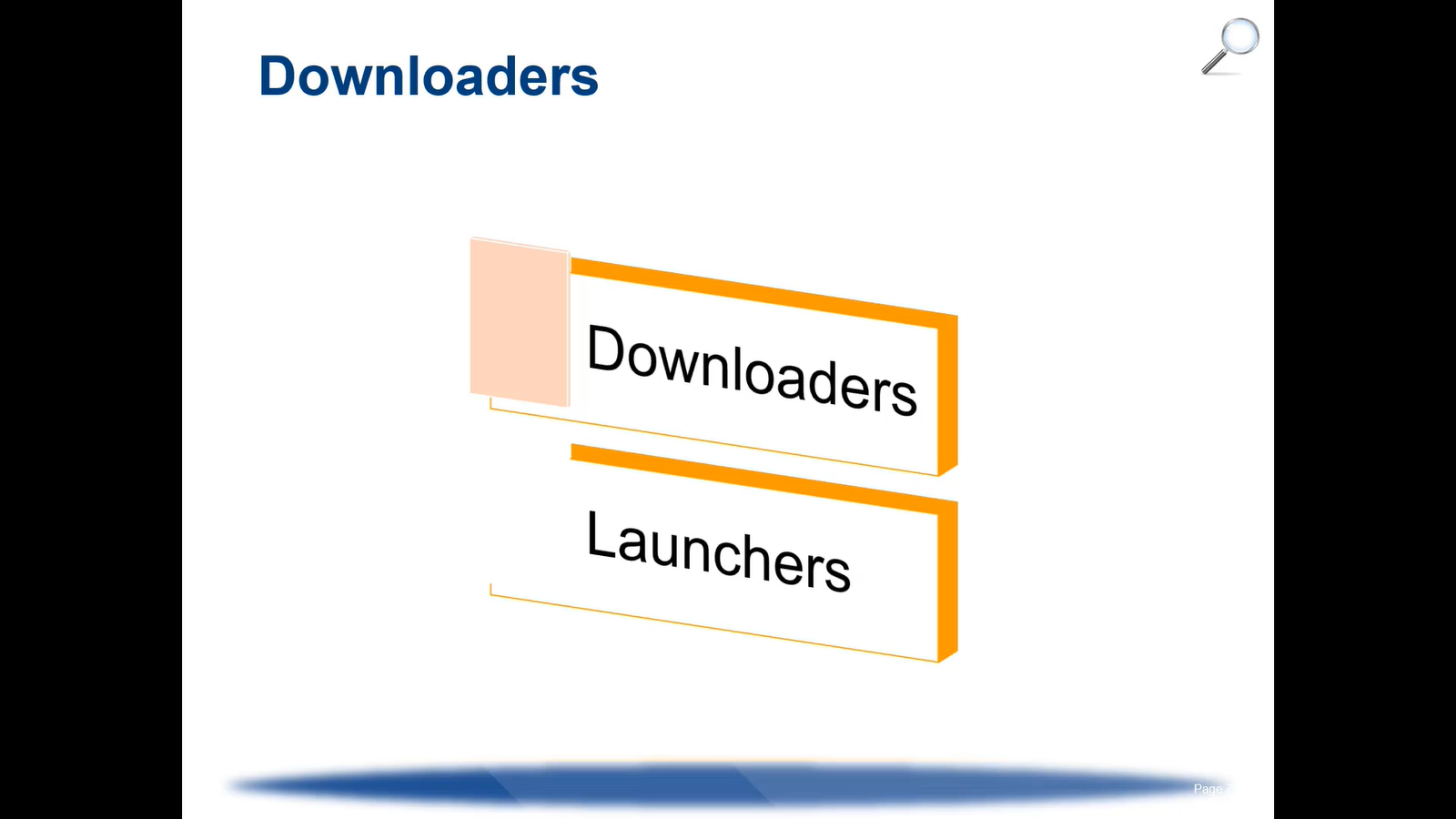


Multi-Partite: Infect both the boot sector and the OS.

Polymorphic: Change small parts of themselves when they replicate.

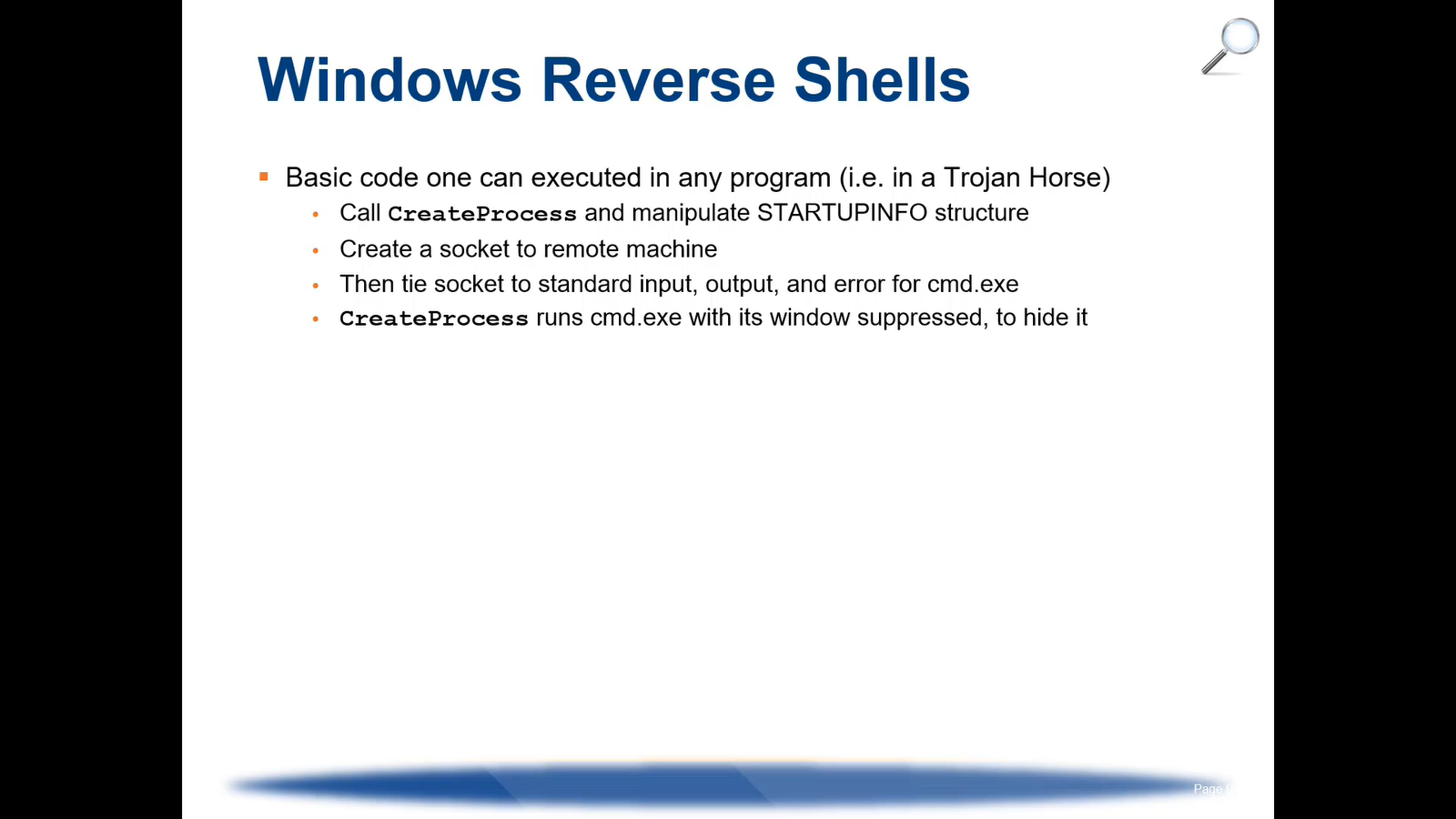
Metamorphic: Completely re-write themselves periodically, making themselves almost impossible to detect.

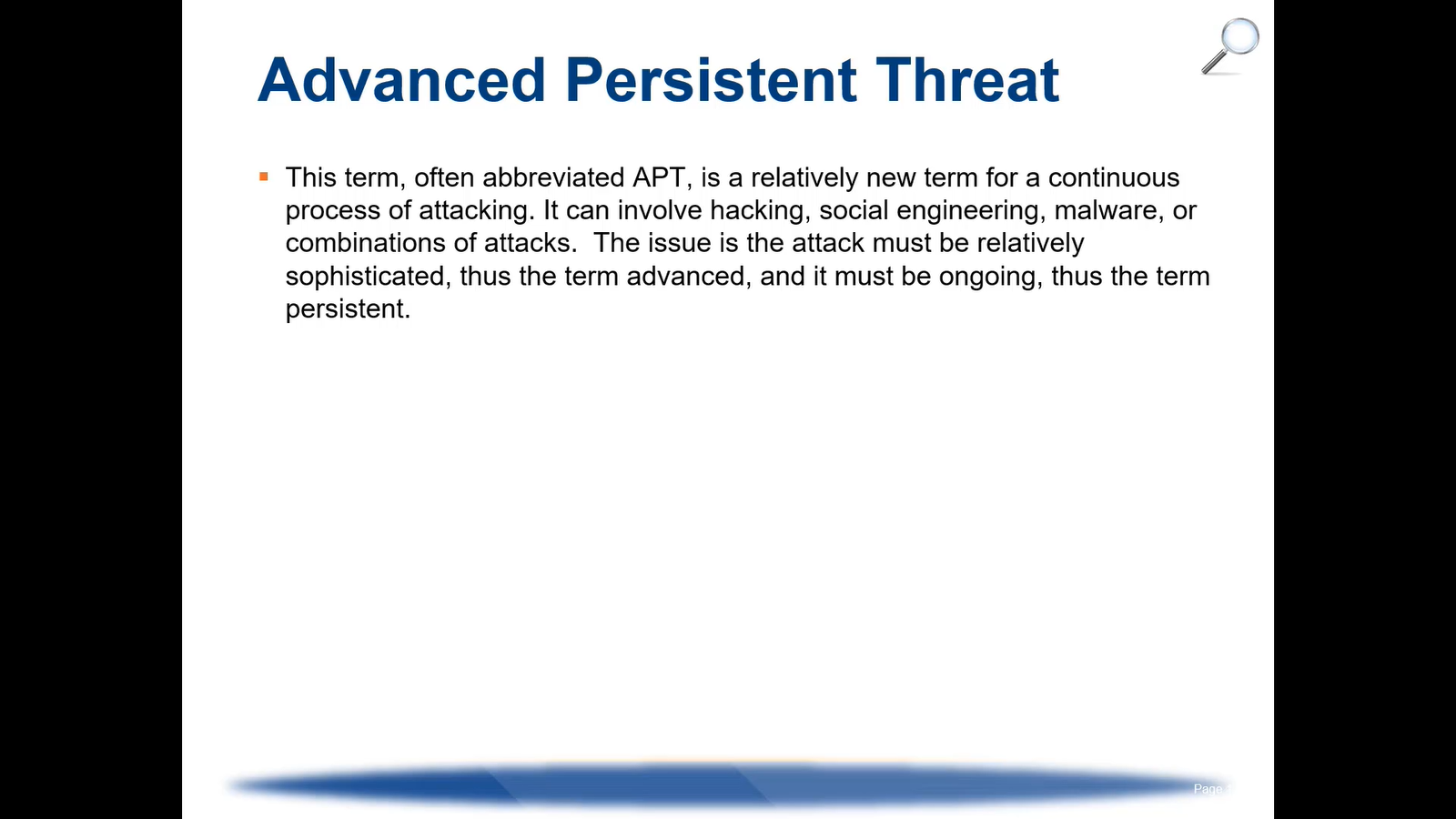
Stealth: Take some steps to be hidden using a variety of steps.

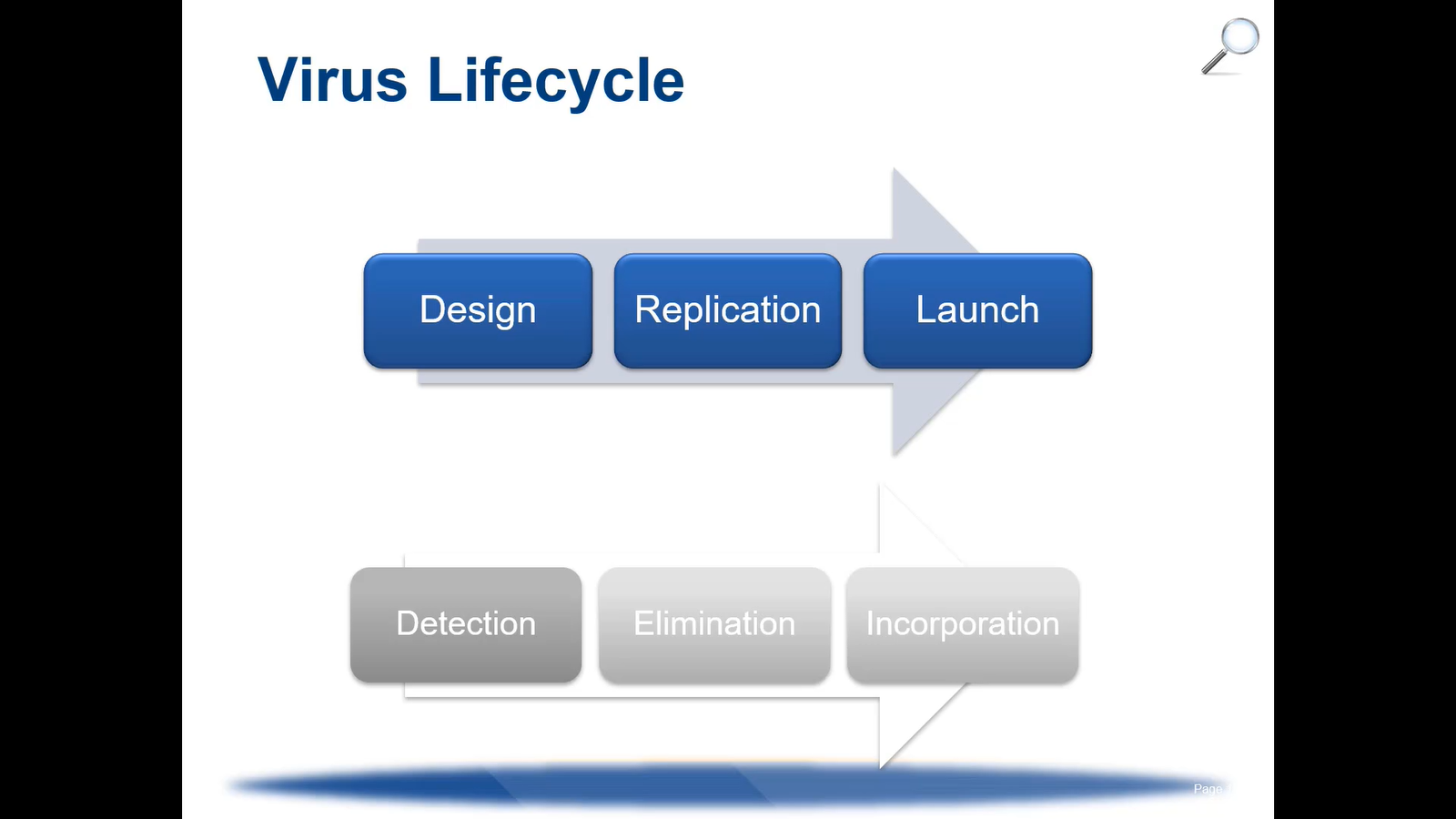


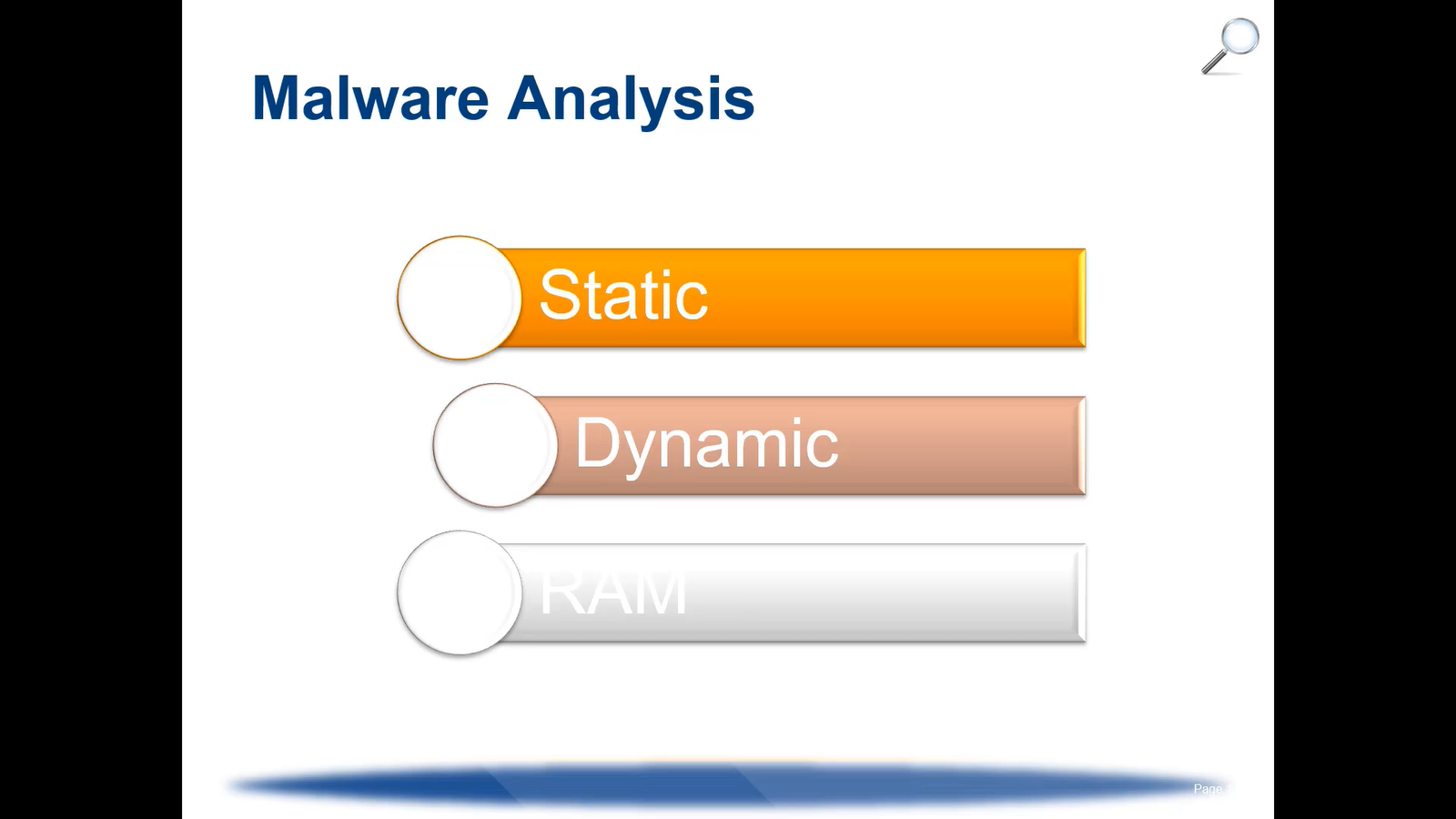
Downloaders goal is to download malicious software to the target while the launcher actually starts the attack.











Static Analysis: Looking at the code of the malware. If you can reverse engineer the virus, you can look at the code and see what it does.

Dynamic Analysis: Involves executing the malware in a test enviroment and seeing what it does.

RAM Analysis: Capturing the RAM and doing memory forensic analysis.

