Malicious Code

Thierry Sans

Outline

- Malware Taxonomy
- The Evolution of Malware Through History
- Anatomy of Modern Malware
  - **Payload** - What the malware does?
  - **Infection Vector** - how malware infects the system?
  - **Persistence Mechanisms** - how malware sticks to the system?
  - **Exfiltration and Control** - How the malware can be exfiltrate data and/or be controlled remotely?
  - **Evasion Technique** - How the malware stays undetectable and/or hard to analyze?
- [Bonus] A Malware Story (2014)