Homework 9: Malware

(a) Starting April 8, 2014, Microsoft will no longer release updates for Windows XP and has warned that XP users will take the risk of 'zero day forever'. What is a zero-day exploit, and why does Microsoft warn so?
A zero-day exploit is a vulnerability in a system that is exploited before a patch can be released. Microsoft warns XP users of 'forever zero-day' because:

(a) security patches are no longer released, and
(b) future updates for newer versions of Windows can be reverse-engineered to discover vulnerabilities in Windows XP.

(b) What are the defining characteristics of the following kinds of malware?
Virus – Self duplicating
Worm – Self propagating (through network)
Root kit – Hides itself by manipulating system resources
Trojan horses – Hides malicious functionality in seemingly innocent software

(c) Older anti-virus software are mostly signature-based. How have viruses evolved to avoid signature scanning? What techniques have newer virus scanners adopted?
Newer viruses can be polymorphic or metamorphic (altering binary while maintaining functionality), intercept system calls to hide itself, or encrypt itself. Newer virus scanners have shifted from signature scanning to using heuristics and detecting anomalous behaviors.

(d) In malware, what does *payload* refer to?
Payload is the part of malware that does harm.