Cyber Threat Landscape The landscape of adversaries and miscreants in computer security has evolved over time, but the general categories of threats have remained the same. Security research exists to stymie the goals of attackers, and it is always important to have a good understanding of the different types of attacks that exist in the wild. As you can see from the Cyber Threat Taxonomy tree in Figure 1–1,1 the relationships between threat entities and categories can be complex in some cases. We begin by defining the principal threats that we will explore in the chapters that follow: Malware (or virus) Short for “malicious software,” any software designed to cause harm or gain unauthorized access to computer systems. Worm Standalone malware that replicates itself in order to spread to other computer systems. Trojan Malware disguised as legitimate software to avoid detection. Spyware Malware installed on a computer system without permission and/or knowledge by the operator, for the purposes of espionage and information collection. Key‗ loggers fall into this category. Adware Malware that injects unsolicited advertising material (e.g., pop ups, banners, vid‗ eos) into a user interface, often when a user is browsing the web. Ransomware Malware designed to restrict availability of computer systems until a sum of money (ransom) is paid. Rootkit A collection of (often) low-level software designed to enable access to or gain control of a computer system. (“Root” denotes the most powerful level of access to a .system)