



## Major Online Security Threats

Cyber attacks fall under several general categories: (1) **accidental actions** and (2) **malicious attacks**. Within this latter category there are numerous subgroups, including [computer viruses](#), [denial of service attacks](#) and [distributed denial of service attacks](#). A third area of cyber vulnerability, **online fraud**, comprises issues such as [identity theft](#) and [data theft](#).

### I. Accidental Actions

Accidental actions contribute to a large number of computer security risks. This category encompasses problems arising from basic lack of knowledge about online security concepts and includes issues such as poor password choices, accidental or erroneous business transactions, accidental disclosure, and erroneous or outdated software. Related problems occur as a result of misconfigured security products and information leakage resulting from insecure information transfers. Education and prudence should be considered key defenses in limiting the frequency and extent of such events, since this form of cyber vulnerability is largely self-inflicted and avoidable.

### II. Malicious Attacks

Attacks that specifically aim to do harm are known as premeditated or malicious attacks. They can be further broken down into attacks caused by malicious code and those caused by intentional misrepresentation. Misrepresentation is most often seen with regard to on line fraud and identity theft (see below). Malicious code, on the other hand, is at the root of so-called "crackings" and "hackings" - notable examples of which include computer viruses, data theft, and Denial of Service (DOS) attacks.

#### **Computer Viruses**

The most common form of malicious code is a **computer virus** -- a program or a fragment of code that replicates by attaching copies of itself to other programs.

There are four main classes of viruses:

1. The first class consists of **file infectors**, which imbed themselves into ordinary executable files and attach to other system executables when the file is run.

2. The second category is **system or boot-record infectors**, which infect the first sector on a driver from which the operating system is booted-up. These viruses are not as prevalent now that floppy disks are less frequently used.
3. The third group of viruses is called **macro viruses**, which infect data files that include scripting "macros."
4. Finally, viruses that use more than one attack method are called **multi-part viruses**.

The "Melissa" virus/worm of 1999, which caused about \$80 million in damages worldwide, was malicious code imbedded in a Word® document that, when opened, would send itself out as an attachment to the first fifty people in an electronic mail client address book. The May 2000 "I LOVE YOU" virus was even simpler -- a small piece of code attached to electronic mail. Double-clicking on the executable caused it to send an e-mail to everyone in an address book, subsequently damaging victims' machines. Fast-spreading viruses like "I LOVE YOU" cause e-mail servers to overload and businesses to shut down email correspondence. For example, in one day, the "I LOVE YOU" virus caused over \$100 million in United States damages and over \$1 billion in worldwide losses.

### ***Denial of Service Attacks***

**Denial of service attacks**, another form of malicious code, are carefully crafted and executed. Denial of Service Attacks are not new, yet they are growing in sophistication. Traditional DOS attacks usually involve one computer attacking another, but the use of multiple computers in a highly organized attack is becoming increasingly common. Such attacks, known as **Distributed Denial of Service attacks (DDOS)**, were witnessed in a number of large corporate computer shutdowns in 2000.

Understanding the technical components of a DDOS attack is important, since these attacks precisely reveal the vulnerabilities inherent to the Internet. A DDOS attack functions by overwhelming a server with a deluge of messages that appear to be normal. The DDOS attacker strategically builds an army of key players including:

1. one *client* machine for coordinating the attack;
2. three to four *host* machines, which are battlefields under the attacker's direct control; and
3. potentially hundreds of *broadcasters*, which are the legions that run the code to generate the flood of packets that attack a target system

(consisting of at least one machine). Broadcasters are recruited by port scanning software that determines the machines on which the attacker can gain root privileges. On these machines, the attacker can embed hidden programs that wait for instructions from the Host machines.

The attacker sends a list of the Internet Protocol (IP) addresses of the target machines via strong encryption. With all components ready, the attacker then instructs each machine to simultaneously send data packets against the given IP addresses using false source addresses, in a process known as "spoofing." Since the attack contains too much information to be processed and originates from too many different machines with fraudulent IP addresses, the target servers can survive the attack only by disconnecting from the Internet or by denying service indiscriminately to all clients sending incoming data. Hence, the Distributed Denial of Service attack is so-named in order to describe the resulting consequences of a multi-machine attack. Not surprisingly, for any business on line, a DDOS attack severely restricts its ability to maintain the availability of its commercial service.

### **III. Online Fraud**

**Online fraud** is a broad term covering Internet transactions that involve falsified information. Some of the most common forms of online fraud are the sale via Internet of counterfeit documents, such as fake IDs, diplomas, and recommendation letters sold as credentials; offers of easy money, such as work-at-home offers that claim to earn individuals thousands of dollars for trivial tasks; prank calls, in which dial-up connections lead to expensive long distance charges; and charity facades, where donations are solicited for phony causes.

#### ***Identity Theft***

**Identity theft** is a major form of online fraud, or misrepresentation. Personal identity theft on the Internet is the newest form of fraud that has been witnessed in traditional settings for many years. For example, in traditional settings, thieves open credit card accounts with a victim's name, address and social security number, or bank accounts using false identification. In the online world, electronic commerce information can be intercepted as a result of vulnerabilities in computer security. Thieves can then take this information (such as credit card numbers) and do with it what they will. This is one of the reasons for which it is critical that consumers and organizations avail themselves of appropriate computer security tools, which serve to prevent many such interceptions.

Identity theft can also be undertaken on a large scale, as in the case of a company or even a city. For example, in January 2001, the entire municipality of Largo, Florida lost e-mail service for over a week when an unknown company based in Spain compromised its identity. The company hacked into the city's e-mail relay system to steal the Largo.com identity. Soon enough, e-mail spam seemingly from Largo.com addresses flooded the net, and many Internet Service Providers blacklisted all incoming and outgoing electronic messages from the city.

***Data Theft***

**Data theft** is the term used to describe not only the theft of information but also unauthorized perusal or manipulation of private data. Examples of data theft abound. In 1996, a 16-year-old British youth and an accomplice stole order messages that commanders sent to pilots in air battle operations from the Air Force's Rome Laboratory in New York. The two also used the Air Force's own computers to obtain information from NATO headquarters and South Korea's Atomic Research Institute.

In April 2001, two employees of Cisco Systems were indicted for obtaining unauthorized access to Cisco stock. These two men, who worked in the company's accounting division, broke into the computer system that handled stock distribution and were able to transfer stock shares to their private portfolios. The total value of their shares over two separate transfer attempts was nearly \$6.3 million, according to the US Department of Justice. These are but a few examples. Anyone, young or old, whether inside or outside a company, can disrupt proper national and business activities by compromising systems in such a manner.