What Types of Spyware Exist?

All forms of spyware can be divided into the following five categories:

1. **Infostealers**
   As the name suggests, infostealers are programs that have the ability to scan infected computers and steal a variety of personal information. This information can include browsing histories, usernames, passwords, email addresses, personal documents, as well as media files. Depending on the program, infostealers store the data they collect either on a remote server or locally for later retrieval.
   In most cases, infostealers exploit browser-related security deficiencies to collect your private data. They sometimes also use the so-called injection scripts to add extra fields to web forms. When you type in the requested information and hit “Submit”, instead of going to the website owner, the information will go directly to the hacker, who can then potentially use it to impersonate you on the internet.

2. **Password Stealers**
   Password stealers are very similar to infostealers, the only difference being that they are specially designed to steal login credentials from infected devices. First detected in 2012, these pieces of spyware don’t steal your passwords as you type them. Instead, they attach themselves to the browser to extract all your saved usernames and passwords. In addition, they can also record your system login credentials.
   Most password stealers are routinely removed by reliable security software, but some types still manage to avoid detection by changing their file hashes before each attack. As with infostealers, the creators of password stealers can choose whether they want to store the collected data on a remote server or in a hidden file on your hard drive.

3. **Keyloggers**
   Sometimes referred to as system monitors, keyloggers are spyware programs that record the keystrokes typed on a keyboard connected to an infected computer. While hardware-based keyloggers record each keystroke in real time, software-based keystroke loggers collect periodic screenshots of the currently active windows. This, in turn, allows them to record passwords (if they are not encrypted on-screen), credit card details, search histories, email and social media messages, as well as browser histories.
   While keyloggers are mostly used by hackers to gather sensitive data from unsuspecting victims, they have also found a more practical use in recent years. Namely, some business owners utilize them to monitor the activity of their employees, while concerned parents may install them on their children’s computers to ensure that they are safe online. Some law enforcement agencies in the United States have also used keyloggers to arrest notorious criminals and crack down on drug dealers.

4. **Banker Trojans**
   Banker Trojans are programs that are designed to access and record sensitive information that is either stored on or processed through online banking systems. Often disguised as legitimate software, banker Trojans have the ability to modify web pages on online banking sites, alter the values of transactions, and even add extra transactions to benefit the hackers behind them. Like all other types of spyware, banker Trojans are built with a backdoor, allowing them to send all the data they collect to a remote server.
   These programs usually target financial institutions ranging from banks and brokerages to online financial services and electronic wallet providers. Due to their sophisticated design,

banking Trojans are often undetected even by the state-of-the-art security systems of some financial institutions.

5. **Modem Hijackers**
   With the gradual shift from dial-up to broadband in the last decade, modem hijackers have become a thing of the past. They are perhaps the oldest type of spyware that would attack its victims while they were browsing the internet. As a rule, a pop-up ad would appear, prompting the user to click on it. When they did, it would initiate a silent download of a file that would then take control of their dial-up modem.
   Once in charge of the computer, the modem hijacker would disconnect the phone line from its current local connection and instead connect it to an international one. Most hackers would premium-priced phone numbers (usually intended for adult chat lines) that were registered in countries with insufficient cybercrime legislation like China, Russia, and some South American countries. The victims would usually only become aware of the problem when they saw their $1,000+ phone bill early next month.

Examples of Spyware

With the development of cybersecurity technologies over the years, many spyware programs have disappeared, while some other, more sophisticated forms of spyware have emerged. Some of the best-known examples of spyware include the following:

- **CoolWebSearch** – This program would take advantage of the security vulnerabilities in Internet Explorer to hijack the browser, change the settings, and send browsing data to its author.
- **Gator** – Usually bundled with file-sharing software like Kazaa, this program would monitor the victim's web surfing habits and use the information to serve them with better-targeted ads.
- **Internet Optimizer** – Particularly popular in the dial-up days, this program promised to help increase internet speeds. Instead, it would replace all error and login pages with advertisements.
- **TIBS Dialer** – This was a modem hijacker that would disconnect the victim's computer from a local phone line and connect them to a toll number designed for accessing pornographic sites.
- **Zlob** – Also known as Zlob Trojan, this program uses vulnerabilities in the ActiveX codec to download itself to a computer and record search and browsing histories, as well as keystrokes.