Describe a simple method used to create a polymorphic malicious software

**Polymorphic malicious software:**

A software or malicious code that spreads between computers and corrupts the system is known as a virus. It replicates itself and affixes it to a software file to spread. The viruses merely proliferate, display messages, and some may pass a segment of the hazardous code to a program that is capable of modifying software, erasing files, formatting the hard drive, and erasing crucial data.

Explanation

As the name implies, a polymorphic code in a computing system is a code that modifies while maintaining the original algorithm in tact. In other words, as the code is executed, it changes itself. The goal of the code remains constant, though. The code is always evolving, so after several attacks it becomes relatively complex, making it more challenging for upcoming attackers. In order to evade and outwit your computer's defences, a "shape-shifting" virus or threat creates dangerous code that repeatedly repeats and changes its features, eventually damaging your system.

Step 2 of 3

**How to Creates a Polymorphic Code?**

In addition to using polymorphic code, a mutation engine is also used. The mutation engine changes the file name of the polymorphic code and generates a randomly chosen decoding procedure for each infection.

The virus searches for new programs to infect and gives the new program a duplicate copy of its body as well as its mutation engine. This makes it possible for the polymorphic virus to spread throughout the system and cause its demise without being recognised and stopped by any antivirus utilizing the standard signature detection method.

Step 3 of 3

**Developing Polymorphic Code:**

When antivirus software finds a virus, it blocks it and immediately blocks any other bad code with similar features. However, with a polymorphic code, the virus's primary function remains the same even if the signature or decryption method changes with each mutation.

Antivirus software that depends on traditional signature-based detection fails to find and remove malicious code when the signature and decryption techniques change. As a result, both the virus and its mutation engine multiply.

The mutation engine is then turned on, and a brand-new decryption technique is created that has nothing to do with the initial decryption procedure. The virus then attaches the new decoding programme, encrypted virus, and mutation engine to the host before encrypting its body and mutation engine to the new program.

**Final Answer**

**Conclusion:**

A polymorphic virus is a sort of malicious software that may alter or "morph," making it challenging to find using antimalware solutions. Malicious code can evolve in a number of ways, including through filename changes, compression, and encryption using variable keys.

A mutation engine is frequently used by polymorphic code along with the underlying harmful code. The mutation engine creates fresh decryption procedures for the code rather than altering the underlying code itself. The polymorphic code's file names can also be changed by the mutation engine.