Malware Persistence

Windows malware exercise:

- Describe how the malware obtains persistence, highlighting the assembly code where the related instructions and function calls are executed.
- Identify the client software used by the malware to connect to the Internet.
- Identify the URL to which the malware attempts to connect and highlight the function call that allows the malware to connect to a URL.
- **BONUS**: What is the meaning and functioning of the assembly command "lea"?

Solution:

To analyze the malware code from the provided assembly snippets, let's answer the questions step by step:

1. **Describe how the malware obtains persistence, highlighting the relevant assembly code instructions and function calls**.

The malware obtains persistence by adding a new entry to the Windows registry key that controls programs that start automatically when Windows starts. This is typically done by modifying the "Run" registry key.

In the first code snippet, the relevant instructions are:

```
0040286F push 2
00402871 push eax
00402873 push offset SubKey ; "Software\\\\Microsoft\\\\Win
dows\\\\CurrentVersion\\\\Run"
00402878 push 80000002h ; HKEY_LOCAL_MACHINE
0040287D call ds:RegOpenKeyExW
```

```
...
0040288A push eax
0040288B push offset ValueName ; lpValueName
00402890 push ecx ; hKey
00402891 call ds:RegSetValueExW
```

This sequence of instructions does the following:

- Opens the "Run" registry key.
- Adds a new value to this key, which specifies a program to be run at startup.

2. **Identify the client software used by the malware for the connection to the Internet.**

In the second code snippet, the malware uses the Internet functions from the Windows API. The client software specified here is "Internet Explorer 8.0".

The relevant instruction is:

```
00401158 push offset szAgent ; "Internet Explorer 8.0"
0040115F call ds:InternetOpenA
```

3. **Identify the URL to which the malware attempts to connect and highlight the function call that allows the malware to connect to a URL.**

The URL the malware attempts to connect to is "http://www.malware12.com".

The relevant instructions are:

```
00401177 push offset szUrl ; "<http://www.malware12.com>"
0040117E call ds:InternetOpenUrlA
```

4. **BONUS: Explain the meaning and functioning of the assembly command "lea".**

The `lea` (Load Effective Address) instruction **is used to load the address of a memory operand into a register.** It computes the address of the operand and stores it in the specified register, rather than the actual value at that address. This can be used for various purposes, such as calculating offsets or pointers without performing an actual memory access.

For example:

```
lea ecx, [esp+428h+Data]
```

This instruction calculates the effective address of the memory location at `[esp+428h+Data]` and loads this address into the `ecx` register. It is commonly used for pointer arithmetic and to obtain the address of local variables or parameters.

In conclusion:

- The malware obtains persistence by adding an entry to the "Run" registry key.
- The malware uses "Internet Explorer 8.0" for Internet connectivity.
- The malware attempts to connect to "http://www.malware12.com".
- The `lea` instruction is used to load effective addresses into registers.