Assignment 2
Gunnar Yonker

1. InternetGetConnectedState

The InternetGetConnectedState function is used to determine if the computer is currently connected to the internet. This function will take two arguments, they are lpdwFlags and dwReserved. They are not directly related to a malware sample but are the arguments that will be taken by this function. The lpdwFlags argument is a pointer to a variable that receives the connection description such as if the connection is LAN. If the function call is successful, it will return a Boolean value in the form of TRUE or FALSE that will indicate if the computer is connected to the Internet or not. Malware can use this function to check if the infected system is online before it would attempt to communicate with any other system. Knowing if the system is online is important for malware because if it is, there are multiple ways that the malware can then spread to other systems. If the system is not connected, then the malware may delay communication or action until a connection is established.

2. InternetReadFile

The InternetReadFile is used to read data from a file or resource on the Internet. This function takes four arguments: hFile, IpBuffer, dwNumberOfBytesToRead, and IpdwNumberOfBytesRead. The hFile argument is a handle to the file or resource that is going to be read. The IpBuffer argument is a pointer to a buffer that receives the data that is read from the file. The dwNumberOfBytesToRead argument specifies the number of bytes that are going to be read from the file. The IpdwNumberOfBytesRead argument is a pointer to a variable that will receive the number of bytes read from the file. If the function call is successful, then it will return a Boolean value in the form of TRUE or FALSE that indicates if the read operation was successful or not. Malware can use this function to download data from the internet and to read any response from a server that can then be stored locally on the infected system.

3. InternetOpenUrlA

The InternetOpenUrlA function is used to open a connection to a file or resource on the Internet. This function takes a few different arguments: hInternet, IpszUrl, and IpszHeaders, dwHeadersLength, dwFlags. The hInternet argument is a handle that is returned by the InternetOpenA function. The IpszUrl argument is a pointer to a string that specifies the URL of the file or resource that the malware is attempting to open. The IpszHeaders argument is a pointer to a string that specifies any additional headers that are going to be sent with the request. dwHeadersLength si the size of the additional headers. The dwFlags argument can have different values based on the result of the function. If the function call is successful, it will then return a valid handle to the url or source or NULL if the connection fails. Malware can use this function to connect to a server and retrieve either instructions or to upload any stolen data that the malware has already gathered from the infected system. The malware could upload sensitive data such as any passwords found on the local system.

4. InternetOpenA

The InternetOpenA function is used to initialize a connection to the internet. This function takes 4 arguments: IpszAgent, dwAccessType, IpszProxy, dwFlags, and IpszProxyBypass. The IpszAgent argument is a pointer to a string that specifies the user agent string that is going to be used in the request. The dwAccessType argument specifies the type of access to the internet such as being INTERNET_OPEN_TYPE_DIRECT or INTERNET_OPEN_TYPE_PROXY among other options. The IpszProxyBypass argument and the IpszProxy argument are optional and can be used if the malware needs to use specific proxy server settings. The dwFlags argument contains options that can have a few different values such as INTERNET_FLAG_ASYNC. If the function call is successful, it returns a valid handle that can be used by other WinINet functions in the Internet API. Malware can use this function to establish a connection to the internet before trying to communicate with a server. This could then be used to download other malicious files from the internet that the malware wants to use on the system.

5. SetWindowsHookExA:

The SetWindowsHookExA function is used to install a hook procedure that monitors system events. This function takes three arguments: idHook, Ipfn, dwThreadID and hmod. The idHook argument specifies the type of hook procedure that is going to be installed, an example is WH_MOUSE would monitor mouse messages or WH_KEYBOARD would install a hook procedure that monitors keyboard messages. The Ipfn argument is a pointer to the hook procedure that is going to be installed. The dwThreadID argument is the identifier of the thread that the hood procedure is associated and identified with. The hmod argument is a handle to the DLL containing the hook procedure. If the function call is successful, then it will return a handle to the hook procedure in the type HHOOK. Malware can use this function to intercept and monitor system events. It could monitor events like keyboard input, mouse movement, or window messages and all of these could allow the malware to steal sensitive information from the infected system or allow the malware to take control of the system. An example of this would be a keylogger malware that would intercept and record the keyboard input to then gather sensitive information such as username and password combinations.