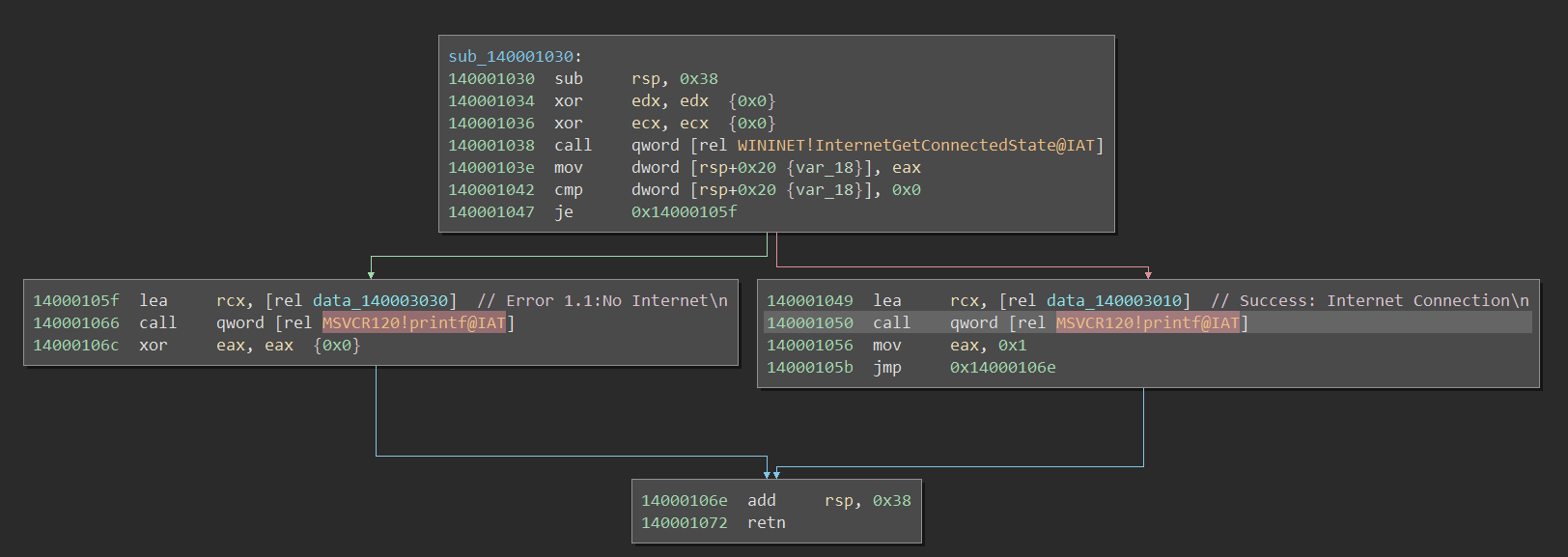
**Lab 6-1**

1. What is the major code construct found in the only subroutine called by main?
   1. The major code construct is an if statement.
2. What is the being called at 0x140001066 and 0x140001050?
   1. Printf is being called at these addresses. The string printed is loaded into rcx before the call
3. What is the purpose of this program?
   1. This program checks for an active Internet connection. If there is a successful connection then the string “Success: Internet Connection\n” is printed, otherwise "Error 1.1:No Internet\n" is printed

**Detailed Analysis**



**Lab 6-2**

1. What operation does the first subroutine called by main perform?
2. What is called at 0x14000103B?
3. What does the second subroutine called by main do?
4. What type of code construct is used in this subroutine?
5. Are there any network-based indicators for this program?
6. What is the purpose of this malware?

**Lab 6-3**

1. Compare the calls in main to Lab 6-2’s main method. What is the new function called from main?
2. What parameters does this new function take?
3. What major code construct does this function contain?
4. What can this function do?
5. Are there any host-based indicators for this malware?
6. What is the purpose of this malware?

**Lab 6-4**

1. What is the difference between the calls made from the main method in Labs 6-3 and 6-4?
2. What new code construct has been added to main?
3. What is the difference between this lab’s parse HTML function and those of the previous labs?
4. How long will this program run? (Assume that it is connected to the Internet.)
5. Are there any new network-based indicators for this malware?
6. What is the purpose of this malware?