Intelligence agents intercepted network traffic containing a password encrypted archive in “.rar” format. After receiving intelligence reports from field agents, they also believe the archive contains an additional password protected archive. They have managed to obtain a client binary which may authenticate with a remote server to access the passwords to decrypt the archive containing these files.

Field agents are currently working on obtaining a copy of the server binaries for further analysis. In the meantime, your mission, should you choose to accept it, is to try and derive as much information as possible from the binary to gain a stronger understanding of how the client and server communicate, and prepare the testbed for further analysis with the server binary once the agents can obtain the files.

**Your final goal is to identify the network parameters used to connect to the server.**

Intelligence agents provided the following binary:

<< Client.exe located on the desktop >>
Connectivity to the testbed

NOTE: Ensure the laptop’s wireless interface is turned off.

1. Connect the laptop to the testbed with the provided Ethernet cable.

Windows users:

2. Click on the Windows Logo > Control Panel > View Network status and tasks under Network and Internet. (Windows 10:  + “network status”)

3. In the new window, click on Local Area Connection.

4. Click on Details and make sure the IPv4 Address field is 192.168.1.x, where x is an integer (shown above).

5. Open Remote Desktop Connection on your computer by clicking on the Windows Logo > Search programs and files > type Remote Desktop Connection. (Windows 10:  + “remote desktop”)


a. Click on the **Show Options** drop down menu and under the **Display** tab select the following settings:

![Remote Desktop Connection](image1)

b. In the **Computer** field type in the Remote Computer address provided on your ticket.

   `<IP address>:<port>`

   Example: 192.168.1.x:xxxx

![Remote Desktop Connection](image2)

c. Click on **Connect**.

d. Click **Yes** on the security prompt.

e. After ~10 seconds you will see the desktop.
OSX users:

2. Click on the **Apple logo** on the top left corner > **System Preferences**.
3. Click on **Network**.
4. Verify that the Ethernet adapter IP Address matches **192.168.1.x**, where x is an integer (shown below).

5. Open **Microsoft Remote Desktop** (can be obtained from the **APP Store**) by holding **Command + Space** keys and typing **Microsoft Remote Desktop**.
6. Click on **New**.
7. Enter the **Remote Computer** address in the **PC name** field.

   \(<\text{IP address}>:\<\text{port}>\)

   Example: 192.168.1.x:xxxx

8. Close the window, double click the new entry under **My Desktops**.

9. After \(~10\) seconds you will see the desktop.
Analyzing the binary (It was a bright cold day in April, and the clocks were striking thirteen)

ID pro is a combination of disassembler and debugger, facilitating both static and dynamic analysis. It is a powerful tool commonly used by professionals to perform binary analysis and much more. This is an excellent asset to assist any cybersecurity professionals.

1. Locate the **IDA Pro icon** on the desktop, and double click the icon to start the project.

2. In the about screen click **OK**, close the *Welcome to IDA window*.
3. Reduce the size of the IDA window so you can see the icons on the desktop.
4. Locate the **Client** binary on the desktop, and **drag & drop** it into the **Drag a file here to disassemble** pane in IDA.

5. In the **Load a new file** pop up, ensure that **Portable executable for 80386** is highlighted and click **OK**. When prompted with a *please confirm* window click **No**.
6. **Maximize** IDA Pro. Then click on **Windows => Reset Desktop**.
7. Click on the node in **IDA View-A** and hit the **space bar**.

8. The view should toggle into a listing view.
9. **Scroll** all the way to the top of the listing view.
   a. What is the is the **MD5** hash for this executable?
   b. __________________________
   c. What is the **File Name** of the binary?
   d. __________________________
   e. What is the **Format** of the file?
   f. __________________________

The MD5 hash is utilized by anti-virus software to identify malicious software. It is also stored in online repositories such as [www.virustotal.com](http://www.virustotal.com)

PE Headers are common across all windows executables.
BINARY ANALYSIS (It’s my business to know what other people don’t)

One the best starting points for gathering information from an unknown binary is by sifting through the binary’s strings or names sections. This section will begin in the names section.

10. Navigate to the Names section in IDA.

11. Scroll through the Names and locate connect.

Dynamic Linked Libraries are useful for abstracting common functionality between multiple binaries.

12. Double click connect. IDA will jump into the listing view. IDA has identified that this call along with several other common calls are imported from another dll.

   a. What is the name of this dll? _________________ (HINT SCROLL UP)

   b. Name the complete list of imports from this DLL.
      i. __________________________________
      ii. __________________________________
      iii. __________________________________
      iv. __________________________________
      v. __________________________________
      vi. __________________________________
      vii. __________________________________
      viii. __________________________________
      ix. __________________________________
      x. __________________________________
Binary Analysis (The tiny white pebbles gleamed in the moonlight…)

IDA Pro offers various methods for traversing through binaries. This section will exploit the use of cross-references (XREF).

13. Locate \texttt{WSA\textit{Startup}} in the \textit{Imports from WS2\textunderscore 32.dll}.
   
a. Double click on the \texttt{sub\_411xxxx\_xxxx} next to the \textit{DATA XREF} located on the same line as \texttt{WSA\textit{Startup}}.
   
   ![Control Flow Graph](image)
   
   b. IDA should jump into a control flow graph (CFG) of the binary where \texttt{WSA\textit{Startup}} is called in the \textit{IDA View} window. If IDA is still in listing view (not in same view as seen below) click on the space bar to toggle views.

14. Follow the \textbf{green path} from the node to the next node \texttt{loc\_41160F}.
   
a. Arguments are pushed as parameters from right to left before a subroutine is called, what three arguments are pushed as parameters before the call for \texttt{socket}? 
   
i. \texttt{af}: 
   
   ii. \texttt{type}: 
   
   iii. \texttt{protocol}: 

*\textbf{Diagram} should be included as an image*
15. Follow the green path on the CFG to loc_41165A. A string is pushed as parameters before the inet_addr call is made.
   a. What is the value this string? _________________________________

   The string is the destination IP address for the remote server.

   b. What is the value assigned to mov [ebp_name.sa_family], ax? Hint a value is moved into the EAX register right before the mov instruction, ax is just the lower 16 bits of the 32 bit register EAX. _________________________________

16. Right before htons is called a hexadecimal value is pushed as parameters.

   a. What is this value in hex? _________________________________ (the h at the end of the value indicates it is in hex (ex: 9999h))

   b. Click on the hex value once, then click on View => Calculator…in the IDA Pro toolbar. What is the decimal value?

   The hex is the destination port on the remote server.
Binary Analysis (Follow the white rabbit)

17. Continuing onto loc_4116DF in the CFG, a string is check for length, and pushed as parameters before the send call.
   a. What is the value of this string? _________________________
   b. What is the value of flags before the send call? _________________________
      
      Hint: look at the auto-generated comments

      ```
      push 0 ; flags
      push offset _mkscHeap2 + 1;
      call j_strlen
      add esp, 4
      push eax ; len
      push offset _mkscHeap2 + 1;
      mov eax, [ebp+4] ; s
      call ds:send
      ```
      
18. Several values are pushed as parameters in loc_41173E. What are the four values pushed onto to stack before recv is called?
   a. Flags: _________________________
   b. len: _________________________
   c. buf: _________________________
   d. s: _________________________

19. Examine the recv call in loc_41173E:

   a. recv returns the number of bytes received, and receive buffer pointed to in the var_9D0 parameter will contain the data received.
   b. Give [ebp+var_9D0] a more meaningful name, what would you rename it?
      _________________________
      
      hint: this is the buffer that receives the data.
      
      c. Right click on [ebp+var_9D0] and rename the variable to the name specified in your previous answer.

      Notice IDA pro has changed subsequent calls to this variable on the stack to the name specified.
This concludes the static analysis workshop.

Based on your work so far:

List everything you know about the communications initialization of this binary and the external server (IP ADDRESS, PORT, etc…):