Challenge Questions

Q: Record any observed symptoms of infection from initial detonation. What are the main symptoms of a WannaCry infection?

A:

- Desktop wallpaper changed
- Notification systems are infected, countdown timer and pay buttons
- Many files on the system are encrypted with the extension .WNCRY

Q: Use FLOSS and extract the strings from the main WannaCry binary. Are there any strings of interest?

A:

\\172.16.99[.]5\IPC$
\192.168.56[.]20\IPC$
http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
taskdl.exe
taskse.exe
C:\%s\%s
mssecsvc.exe
%s -m security
C:\%s\qeriuwjhrf
C:\%s\%s
tasksche.exe

Q: Inspect the import address table for the main WannaCry binary. Are there any notable API imports?

A: ReadFile, CreateFileA, InternetOpenA, Sleep, InternetOpenUrlA, GetAdaptersInfo, GetPerAdapterInfo, CreateServiceA, StartServiceA, OpenServiceA, OpenSCManagerA, CryptGenRandom, CryptAcquireContextA,.v.v.

Q: What conditions are necessary to get this sample to detonate?

A:

- Malware tries to connect a url: http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
- If connection is not established => ransomware payload is executed.
- If connection is established => the program exits
- In a lab environment, inetsim must be turned off

Q: Network Indicators: Identify the network indicators of this malware

A:

- Attempted access of the weird URL
- Flood of numerous SMB connection requests
- taskhsvc.exe opens port 9050 to a LISTENING state

Q: Host-based Indicators: Identify the host-based indicators of this malware.

A:

- New directory with a random character name is created in C:\ProgramData\
- Directory is set to hidden
- This directory contains many artifacts from Wanacry
- A new service is created to start tasksche.exe as a persistent executable

Q: Use Cutter to locate the killswitch mechanism in the decompiled code and explain how it functions.

A:

```
int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
{
  void *hInternetOpenA; // esi
  void *hInternetOpenUrlA; // edi
  CHAR kill_switch_url[57]; // [esp+8h] [ebp-50h] BYREF
  int v8; // [esp+41h] [ebp-17h]
  int v9; // [esp+45h] [ebp-13h]
  int v10; // [esp+49h] [ebp-Fh]
  int v11; // [esp+4Dh] [ebp-Bh]
  int v12; // [esp+51h] [ebp-7h]
  __int16 v13; // [esp+55h] [ebp-3h]
  char v14; // [esp+57h] [ebp-1h]

  strcpy(kill_switch_url, "http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com");
  v8 = 0;
  v9 = 0;
  v10 = 0;
  v11 = 0;
  v12 = 0;
  v13 = 0;
  v14 = 0;
  hInternetOpenA = InternetOpenA(0, 1u, 0, 0, 0);
  hInternetOpenUrlA = InternetOpenUrlA(hInternetOpenA, kill_switch_url, 0, 0, 0x84000000, 0);
  InternetCloseHandle(hInternetOpenA);
  if ( hInternetOpenUrlA )
  {
    InternetCloseHandle(hInternetOpenUrlA);
  }
  else
  {
    InternetCloseHandle(0);
    wanacry_entry_point();
  }
  return 0;
}
```