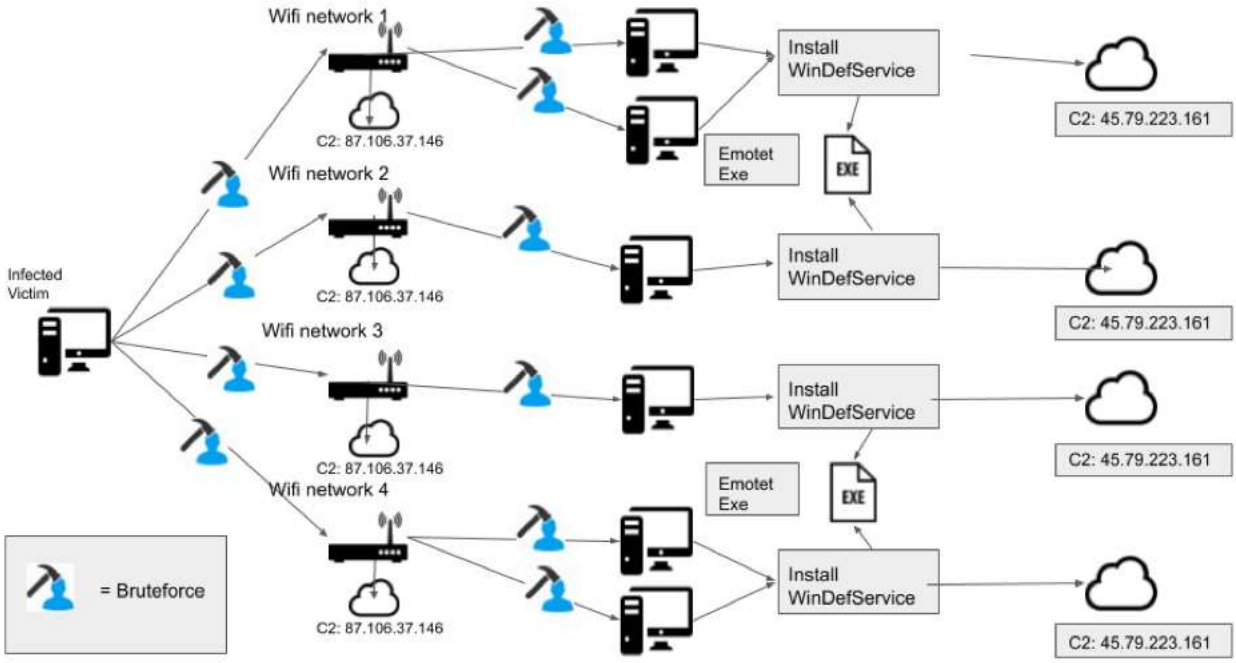
Analysis of Wi-Fi Spreading Worm

Emotet has a malicious new worm module, first seen this year, which connects and travels across Wi-Fi networks, we will do a deep-dive analysis looking at its main components and how they work.

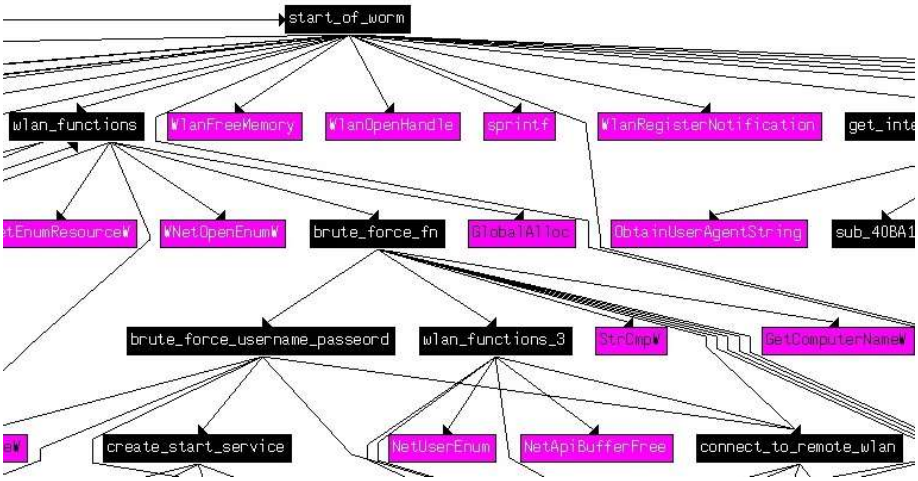
Spreading Mechanism



A new Emotet Wi-Fi worm module was discovered earlier this year. Emotet can spread to new victims connected to nearby unsecure wireless networks.

Deep Analysis

After downloading the executable, importing it into IDA PRO, renaming the functions, the logic of the infection can be clearly understood.



In Ghidra I was able to reverse engineer, many of the functions, allowing me closer inspection of the code. Upon start-up this worm's first action is to take up a copy of "service.exe" to a string buffer what will be used during the worm spreading.

```
void string_copy_function(void)

{
  code *pcVar1;

  StrCpyW((LPWSTR)&ExistingFileName,L"service.exe");
  start_of_worm();
  ExitProcess(0);
  pcVar1 = (code *)swi(3);
  (*pcVar1)();
  return;
}
```

Stage 1: Worm

Information Gathering

Its next step is to enter the main loop and begins searching the wireless network using wlanAPI.dll functions, with the intention of gaining access to any close by Wi-Fi networks.

```
loc = 0x40187f;
hClient = (HANDLE)0x0;
pIfList = (PWLAN_INTERFACE_INFO_LIST)0x0;
pIfInfo = (PWLAN_AVAILABLE_NETWORK_LIST)0x0;
WlanOpenHandle(1,(PVOID)0x0,&dwCurVersion,&hClient);
if (hClient == (HANDLE)0x0) {
  dwResult = 0xffffffff;
}
else {
  wResult = WlanEnumInterfaces(hClient,(PVOID)0x0,&pIfList);
  if ((wResult == 0) && (pIfList->dwNumberOfItems != 0)) {
    buffer[25] = pIfList->InterfaceInfo[0].InterfaceGuid.Data1;
    dwResult = WlanGetAvailableNetworkList(hClient,(GUID *)&buffer[25],1,(PVOID)0x0,&pIfInfo);
    if (dwResult != 0) {
      return 0xfffffffd;
    }
```

The client's session handle, obtained by a call to the WlanOpenHandle function. The worm goes on to call WlanEnumInterfaces collect all Wi-Fi devices enabled on the computer. The information returned is about the Wi-Fi device relating to the devices GUID and description, etc.

SSID: %s

SIGNAL: %d

SECURITY: [WPA|WPA2|UNKNOWN|WEP|OPEN]

encryption: [UNKNOWN|WEP104|CCMP|TKIP|WEP40|NONE]

Note: [Current Connecting| OR

WLAN_AVAILABLE_NETWORK_HAS_PROFILE| OR

WLAN_AVAILABLE_NETWORK_CONSOLE_USER_PROFILE]

Stage 2: Brute Force Wi-Fi Networks

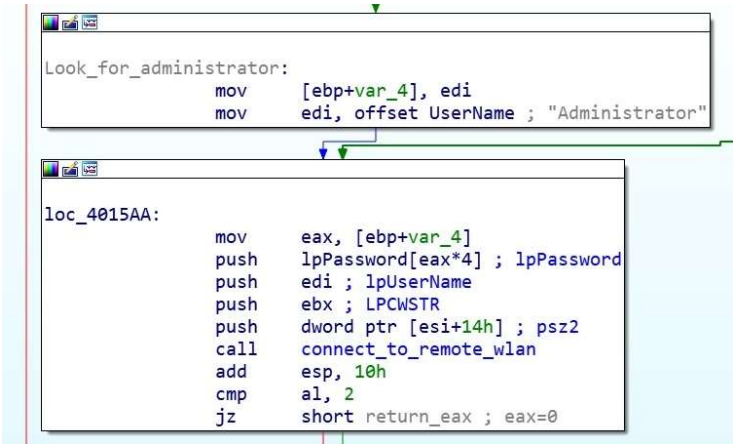
When the information about each Wi-Fi network is obtained, the malware enters into the connection state using brute-forcing loops to gain access.

A network profile is created for each Wi-Fi network, used from information already gathered. A password is obtained from an internal password list buffer, usually with common and standard password types.

Once a profile is set an attempt is made to get connected to a Wi-Fi network, if a connection is not made, the password list is looped through and another attempt is made. If a connection is successful, the malware connects to its Command and Control server, and sends the connected password.

Stage 3: Brute Force Network Users

Once a connection is made to the Wi-Fi network, the next stage is to brute-force all users on the network. The malware uses a second password list to attempt to get user password, again using common and known password types. If unable to get a user password, it attempts to brute-force the Administrator



Stage 4: Spreader Function

With passwords successfully obtained, the worm now attempts to spread service.exe to other systems. It does this by dropping service.exe as my.exe in the C drive of the remotely connected computer. This binary adds a new service called WinDefService with the following information:

Binary Path Name: C:\\my.exe

Desired Access: SERVICE_ALL_ACCESS

Display Name: WinDefService

Service Name: Windows Defender System Service

Stage 4: Create A Service

After successfully getting access to the victims account the worm drops a malicious binary called service.exe on the remote device.

```
result = 0;
hSCManager = OpenSCManagerW(lpMachineName,(LPCWSTR)0x0,2);
if (hSCManager == (SC_HANDLE)0x0) {
  result = 0;
}
else {
  hService = CreateServiceW(hSCManager,L"Windows Defender System Service",L"WinDefService",0xf01ff
                            ,0x10,2,0,L"C:\\my.exe",(LPCWSTR)0x0,(LPDWORD)0x0,(LPCWSTR)0x0,
                            (LPCWSTR)0x0,(LPCWSTR)0x0);
  if (hService != (SC_HANDLE)0x0) {
    serviceStarted = StartServiceA(hService,0,(LPCSTR *)0x0);
    if (serviceStarted != 0) {
      result = 1;
```

The installed service runs a new service called “Windows Defender System Service” used to gain persistence on the new infected system

Stage 5: Infect New System

Worm.exe is the spreader while Service.exe is the infector which installs the payload on the remote computer. Service.exe drops the embedded Emotet binary onto the remote computer.