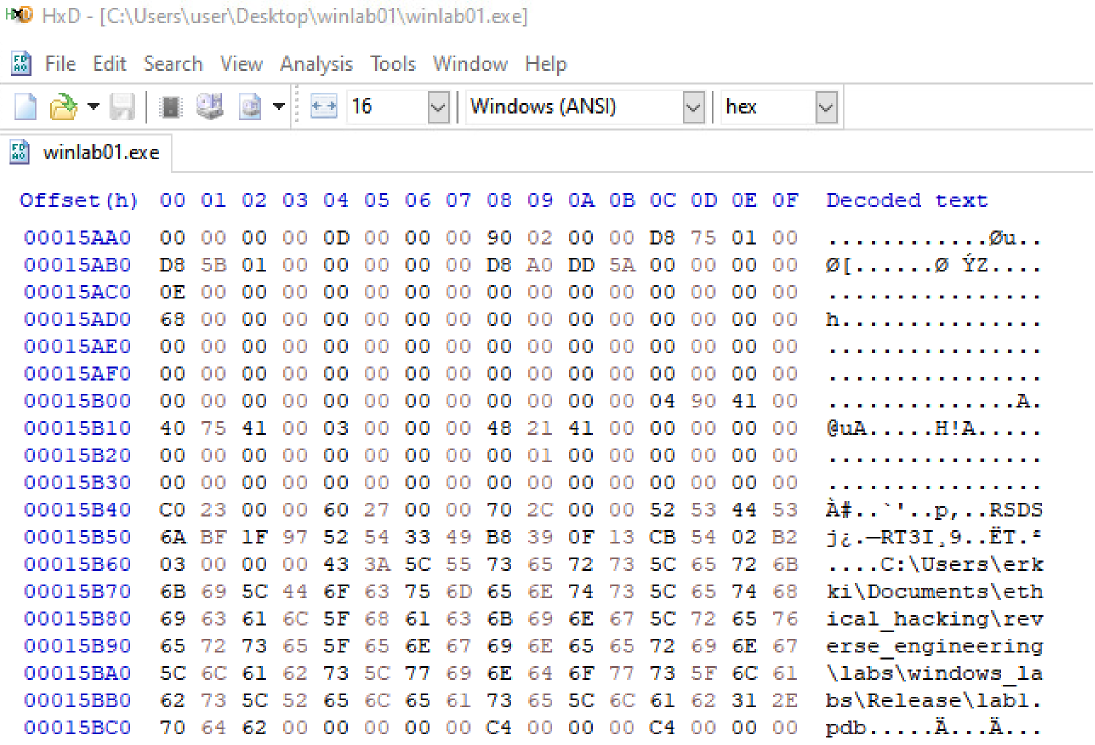
Kalle Jalkanen AB8822
winlab01

Summary

This malware connects 3 different servers and uses lots of .dll files. It also detects is it being debugged. After while it disconnects internet, I think it has something to do with running fakenet. I did get lot of information using static analyzing but with dynamic analyzing I did not get anything relevant approval to what I found earlier. Time used for this exercise is about 6 hours.

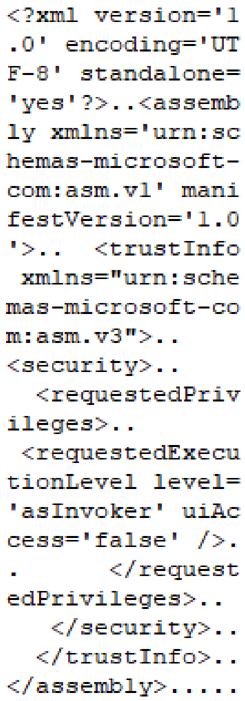
Static analyzing

From hex view we can see that there is path to user 'erkki' that does not exist in this machine even after running winlab01.exe, so maybe it is path where this .exe was originally created.


HxD - [C:\Users\user\Desktop\winlab01\winlab01.exe]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
hex
winlab01.exe

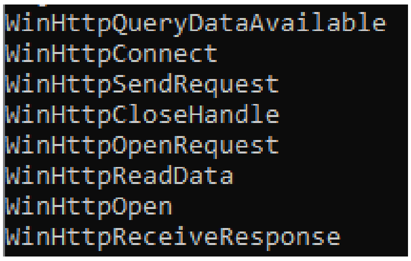
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00015AA0  00 00 00 00 0D 00 00 00 90 02 00 00 D8 75 01 00  ............Øu..
00015AB0  D8 5B 01 00 00 00 00 00 D8 A0 DD 5A 00 00 00 00  Ø[......Ø ÝZ....
00015AC0  0E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00015AD0  68 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  h...............
00015AE0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00015AF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00015B00  00 00 00 00 00 00 00 00 00 00 00 00 04 90 41 00  ..............A.
00015B10  40 75 41 00 03 00 00 00 48 21 41 00 00 00 00 00  @uA.....H!A.....
00015B20  00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00  ................
00015B30  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00015B40  C0 23 00 00 60 27 00 00 70 2C 00 00 52 53 44 53  À#..`'..p,..RSDS
00015B50  6A BF 1F 97 52 54 33 49 B8 39 0F 13 CB 54 02 B2  j¿.—RT3I¸9..ËT.²
00015B60  03 00 00 00 43 3A 5C 55 73 65 72 73 5C 65 72 6B  ....C:\Users\erk
00015B70  6B 69 5C 44 6F 63 75 6D 65 6E 74 73 5C 65 74 68  ki\Documents\eth
00015B80  69 63 61 6C 5F 68 61 63 6B 69 6E 67 5C 72 65 76  ical_hacking\rev
00015B90  65 72 73 65 5F 65 6E 67 69 6E 65 65 72 69 6E 67  erse_engineering
00015BA0  5C 6C 61 62 73 5C 77 69 6E 64 6F 77 73 5F 6C 61  \labs\windows_la
00015BB0  62 73 5C 52 65 6C 65 61 73 65 5C 6C 61 62 31 2E  bs\Release\lab1.
00015BC0  70 64 62 00 00 00 00 00 C4 00 00 00 C4 00 00 00  pdb.....Ä...Ä...
```

From there I also found xml file. It's requesting to run with the execution level of 'asInvoker', which means it will run with the same privileges as the parent process and not require elevated privileges. The uiAccess attribute is set to 'false,' indicating that the application does not require UI access privileges.



```
<?xml version='1
.0' encoding='UT
F-8' standalone=
'yes'?>..<assemb
ly xmlns='urn:sc
hemas-microsoft-
com:asm.v1' mani
festVersion='1.0
'>..  <trustInfo
 xmlns="urn:sche
mas-microsoft-co
m:asm.v3">..
<security>..
  <requestedPriv
ileges>..
 <requestedExecu
tionLevel level=
'asInvoker' uiAc
cess='false' />.
.       </request
edPrivileges>..
   </security>..
  </trustInfo>..
</assembly>.....
```

Looking from ‘strings’ it looks like the program is making HTTP connection to somewhere. There was also **WINHTTP.dll** which provides functions and components for making HTTP and HTTPS requests. It also allows applications to perform HTTP communication, such as downloading web pages, sending, and receiving data from web servers, and interacting with web services.

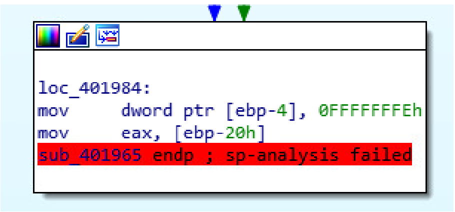


```
WinHttpQueryDataAvailable
WinHttpConnect
WinHttpSendRequest
WinHttpCloseHandle
WinHttpOpenRequest
WinHttpReadData
WinHttpOpen
WinHttpReceiveResponse
```

There was two more .dll files that sounded interesting. Firstly, there was **ADVAPI32.dll** which contains security functions, it can install, start, stop, and control system services, also it has user, and group management and much more but these sounds most interesting right now. Also, there was **USER32.dll** which might be used for tracking user inputs or maybe allows winlab01.exe to make these inputs? It also can for example make phishing dialogs etc.

From strings I also found ‘IsDebuggerPresent’ which can be used to detect analyzing or debugging of the malware. With this information program can change its behavior to make it more difficult to analyze.

I tried to use IDA but I did not get any point what this program does. And it looks like program blocks full analyzing with IDA.

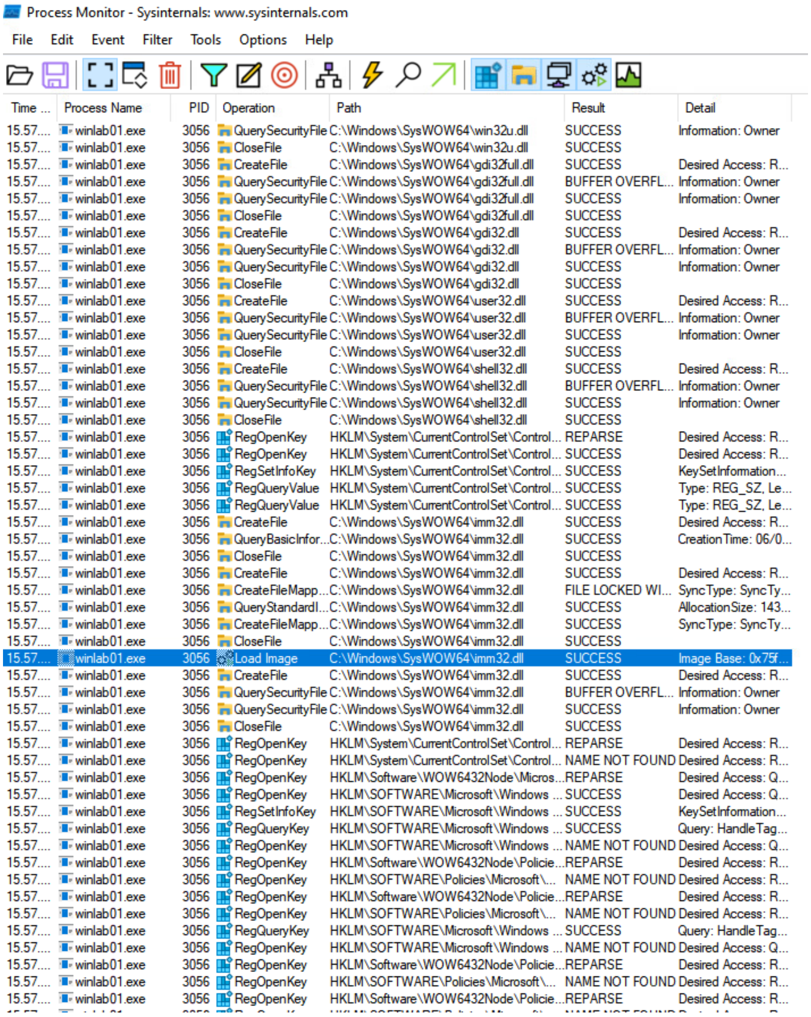


```
loc_401984:
mov     dword ptr [ebp-4], 0FFFFFFFEh
mov     eax, [ebp-20h]
sub_401965 endp ; sp-analysis failed
```

Then I used HashCalc and get md5 ‘e3d948329c3c96013706a8270cf52853’ I put it to google and found web page https://www.hybrid-analysis.com/sample/a02dbb5186eb38947a798357260ea0ed45c9e84c20d9179acdb73ad310f38ca4/5ae8ac117ca3e128ab7f0b44 .
From there I found that it contacts to three different servers 216.58.213.132:80, 216.58.213.142:80 and 216.58.213.142:443 and it read computer name.

Dynamic analyzing

Winlab uses some .dll files and part of them was found when running strings to winlab01.



Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail
15.57....	winlab01.exe	3056	QuerySecurityFile	C:\Windows\SysWOW64\win32u.dll	SUCCESS	Information: Owner
15.57....	winlab01.exe	3056	CloseFile	C:\Windows\SysWOW64\win32u.dll	SUCCESS	
15.57....	winlab01.exe	3056	CreateFile	C:\Windows\SysWOW64\gdi32full.dll	SUCCESS	Desired Access: R...
15.57....	winlab01.exe	3056	QuerySecurityFile	C:\Windows\SysWOW64\gdi32full.dll	BUFFER OVERFL...	Information: Owner
15.57....	winlab01.exe	3056	QuerySecurityFile	C:\Windows\SysWOW64\gdi32full.dll	SUCCESS	Information: Owner
15.57....	winlab01.exe	3056	CloseFile	C:\Windows\SysWOW64\gdi32full.dll	SUCCESS	
15.57....	winlab01.exe	3056	CreateFile	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Desired Access: R...
15.57....	winlab01.exe	3056	QuerySecurityFile	C:\Windows\SysWOW64\gdi32.dll	BUFFER OVERFL...	Information: Owner
15.57....	winlab01.exe	3056	QuerySecurityFile	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Information: Owner
15.57....	winlab01.exe	3056	CloseFile	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	
15.57....	winlab01.exe	3056	CreateFile	C:\Windows\SysWOW64\user32.dll	SUCCESS	Desired Access: R...
15.57....	winlab01.exe	3056	QuerySecurityFile	C:\Windows\SysWOW64\user32.dll	BUFFER OVERFL...	Information: Owner
15.57....	winlab01.exe	3056	QuerySecurityFile	C:\Windows\SysWOW64\user32.dll	SUCCESS	Information: Owner
15.57....	winlab01.exe	3056	CloseFile	C:\Windows\SysWOW64\user32.dll	SUCCESS	
15.57....	winlab01.exe	3056	CreateFile	C:\Windows\SysWOW64\shell32.dll	SUCCESS	Desired Access: R...
15.57....	winlab01.exe	3056	QuerySecurityFile	C:\Windows\SysWOW64\shell32.dll	BUFFER OVERFL...	Information: Owner
15.57....	winlab01.exe	3056	QuerySecurityFile	C:\Windows\SysWOW64\shell32.dll	SUCCESS	Information: Owner
15.57....	winlab01.exe	3056	CloseFile	C:\Windows\SysWOW64\shell32.dll	SUCCESS	
15.57....	winlab01.exe	3056	RegOpenKey	HKLM\System\CurrentControlSet\Control...	REPARSE	Desired Access: R...
15.57....	winlab01.exe	3056	RegOpenKey	HKLM\System\CurrentControlSet\Control...	SUCCESS	Desired Access: R...
15.57....	winlab01.exe	3056	RegSetInfoKey	HKLM\System\CurrentControlSet\Control...	SUCCESS	KeySetInformation...
15.57....	winlab01.exe	3056	RegQueryValue	HKLM\System\CurrentControlSet\Control...	SUCCESS	Type: REG_SZ, Le...
15.57....	winlab01.exe	3056	RegQueryValue	HKLM\System\CurrentControlSet\Control...	SUCCESS	Type: REG_SZ, Le...
15.57....	winlab01.exe	3056	CreateFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Desired Access: R...
15.57....	winlab01.exe	3056	QueryBasicInfor...	C:\Windows\SysWOW64\imm32.dll	SUCCESS	CreationTime: 06/0...
15.57....	winlab01.exe	3056	CloseFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	
15.57....	winlab01.exe	3056	CreateFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Desired Access: R...
15.57....	winlab01.exe	3056	CreateFileMapp...	C:\Windows\SysWOW64\imm32.dll	FILE LOCKED WI...	SyncType: SyncTy...
15.57....	winlab01.exe	3056	QueryStandardI...	C:\Windows\SysWOW64\imm32.dll	SUCCESS	AllocationSize: 143...
15.57....	winlab01.exe	3056	CreateFileMapp...	C:\Windows\SysWOW64\imm32.dll	SUCCESS	SyncType: SyncTy...
15.57....	winlab01.exe	3056	CloseFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	
15.57....	winlab01.exe	3056	Load Image	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Image Base: 0x75f...
15.57....	winlab01.exe	3056	CreateFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Desired Access: R...
15.57....	winlab01.exe	3056	QuerySecurityFile	C:\Windows\SysWOW64\imm32.dll	BUFFER OVERFL...	Information: Owner
15.57....	winlab01.exe	3056	QuerySecurityFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Information: Owner
15.57....	winlab01.exe	3056	CloseFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	
15.57....	winlab01.exe	3056	RegOpenKey	HKLM\System\CurrentControlSet\Control...	REPARSE	Desired Access: R...
15.57....	winlab01.exe	3056	RegOpenKey	HKLM\System\CurrentControlSet\Control...	NAME NOT FOUND	Desired Access: R...
15.57....	winlab01.exe	3056	RegOpenKey	HKLM\Software\WOW6432Node\Micros...	REPARSE	Desired Access: Q...
15.57....	winlab01.exe	3056	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows ...	SUCCESS	Desired Access: Q...
15.57....	winlab01.exe	3056	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows ...	SUCCESS	KeySetInformation...
15.57....	winlab01.exe	3056	RegQueryKey	HKLM\SOFTWARE\Microsoft\Windows ...	SUCCESS	Query: HandleTag...
15.57....	winlab01.exe	3056	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows ...	NAME NOT FOUND	Desired Access: Q...
15.57....	winlab01.exe	3056	RegOpenKey	HKLM\Software\WOW6432Node\Policie...	REPARSE	Desired Access: R...
15.57....	winlab01.exe	3056	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Desired Access: R...
15.57....	winlab01.exe	3056	RegOpenKey	HKLM\Software\WOW6432Node\Policie...	REPARSE	Desired Access: R...
15.57....	winlab01.exe	3056	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Desired Access: R...
15.57....	winlab01.exe	3056	RegQueryKey	HKLM\SOFTWARE\Microsoft\Windows ...	SUCCESS	Query: HandleTag...
15.57....	winlab01.exe	3056	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows ...	NAME NOT FOUND	Desired Access: Q...
15.57....	winlab01.exe	3056	RegOpenKey	HKLM\Software\WOW6432Node\Policie...	REPARSE	Desired Access: R...
15.57....	winlab01.exe	3056	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Desired Access: R...
15.57....	winlab01.exe	3056	RegOpenKey	HKLM\Software\WOW6432Node\Policie...	REPARSE	Desired Access: R...

For little while after running winlab01.exe internet connection losts. This happened 3 different times and all of them was after launching fakenet.

I also tried to use Wireshark and other programs, but I did not find anything relevant.