Lab 1.3: Dynamic Analysis

Analysis of FakeTrojan.exe

Fredrik Helgesson

DV2582 - Malware Analysis
Blekinge Institute of Technology
371 79 Karlskrona
September 11 2018

1 Introduction

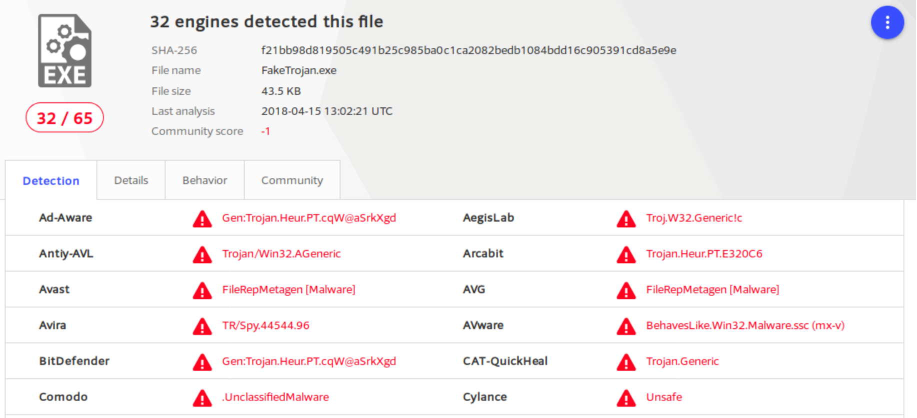
The objective of this lab is to gain skills in analysis of malicious programs. The analysis will be done in two different stages. Firstly a static analysis is done where information about the executable is gathered without running the file. Secondly a dynamic analysis is done by running the executable with and without a debugger. The goal of the analyze is to find indications that the executable is malicious, determine what the malware is doing to the machine and lastly instruct how to remove the malware from an infected system. The file analyzed is presented below.

Filename: FakeTrojan.exe
Filepath: ”C:/STUDENT_LABS/Lab3 - Dynamic Analys/FakeTrojan.exe”
SHA256 sum: f21bb98d819505c491b25c985ba0c1ca2082bedb1084bdd16c905391cd8a5e9e
Creation Time: 2008-09-25 14:12:00

2 Static Analysis

2.1 VirusTotal.com

According to VirusTotal.com this file is identified as malware by 32 different sources. Most of the sources has classified the malware as a trojan.



32 engines detected this file

SHA-256 f21bb98d819505c491b25c985ba0c1ca2082bedb1084bdd16c905391cd8a5e9e
File name FakeTrojan.exe
File size 43.5 KB
Last analysis 2018-04-15 13:02:21 UTC
Community score -1

Ad-Aware	⚠ Gen:Trojan.Heur.PT.cqW@aSrkXgd	AegisLab	⚠ Troj.W32.Generic!c
Antiy-AVL	⚠ Trojan/Win32.AGeneric	Arcabit	⚠ Trojan.Heur.PT.E320C6
Avast	⚠ FileRepMetagen [Malware]	AVG	⚠ FileRepMetagen [Malware]
Avira	⚠ TR/Spy.44544.96	AVware	⚠ BehavesLike.Win32.Malware.ssc (mx-v)
BitDefender	⚠ Gen:Trojan.Heur.PT.cqW@aSrkXgd	CAT-QuickHeal	⚠ Trojan.Generic
Comodo	⚠ .UnclassifiedMalware	Cylance	⚠ Unsafe

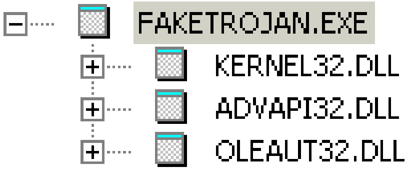
The image above only show a few of the antivirus engines that had analyzed the executable.

2.2 Packing

By examining the size of the virtual size and compare it to the size of raw data a conclusion could be made that the executable is not compressed. This conclusion was strengthened by that neither PEID nor VirusTotal could identify any packing. Lastly the possibility that packing was discarded considering that the code looked complete when the executable was disassembled in IDA Pro.

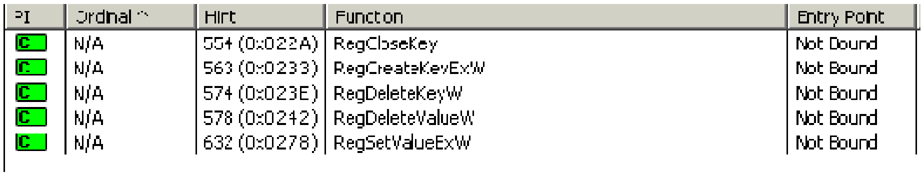
2.3 Imports

Through the use of the tool ”Dependency Walker” three DLLs could be identified that ”FakeTrojan.exe” is importing functions from.



```
⊟ FAKETROJAN.EXE
    ⊞ KERNEL32.DLL
    ⊞ ADVAPI32.DLL
    ⊞ OLEAUT32.DLL
```

None of the imports above can directly be connected to malicious activity but there are a couple of called functions from the imports that can be considered as indications of maliciousness. The strongest indication is the functions called from ”ADVAPI32.DLL” which are used to modify keys in the Windows Registry, the functions called are shown in the image below.



PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	554 (0x022A)	RegCloseKey	Not Bound
C	N/A	563 (0x0233)	RegCreateKeyExW	Not Bound
C	N/A	574 (0x023E)	RegDeleteKeyW	Not Bound
C	N/A	578 (0x0242)	RegDeleteValueW	Not Bound
C	N/A	632 (0x0278)	RegSetValueExW	Not Bound

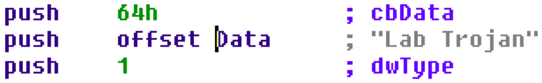
One example of registry modification often done by malware is creating new sub-keys which configures a malicious file to start on log-on or during system start-up. This is used by malware to create a persistent backdoor into the system.

Some of the functions used from the import ”KERNEL32.DLL” suggests that the executable modifies existing files in the system, which at some level can be interpreted as suspicious activity.

2.4 Strings

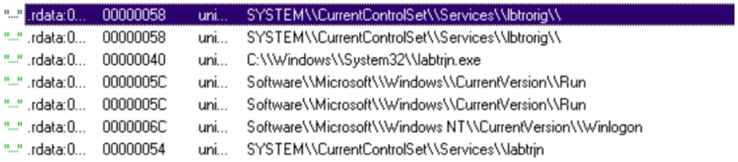
By examining the strings of the executable a number of indicators of compromise were discovered.

The program is creating a new file with the name ”labtrjn.exe” under ”C:/Windows/System32/”. The name of the file suggests that it is short for ”labtrojan.exe”. The string ”Lab Trojan” is also mentioned, seen in image below.



```
push    64h             ; cbData
push    offset Data     ; "Lab Trojan"
push    1               ; dwType
```

As expected when studying the functions called from ”ADVAPI32.DLL” the program does multiple modifications in Windows Registry.



```
"..." .rdata:0...  00000058  uni...  SYSTEM\\CurrentControlSet\\Services\\lbtrorig\\
"..." .rdata:0...  00000058  uni...  SYSTEM\\CurrentControlSet\\Services\\lbtrorig\\
"..." .rdata:0...  00000040  uni...  C:\\Windows\\System32\\labtrjn.exe
"..." .rdata:0...  0000005C  uni...  Software\\Microsoft\\Windows\\CurrentVersion\\Run
"..." .rdata:0...  0000005C  uni...  Software\\Microsoft\\Windows\\CurrentVersion\\Run
"..." .rdata:0...  0000006C  uni...  Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon
"..." .rdata:0...  00000054  uni...  SYSTEM\\CurrentControlSet\\Services\\labtrjn
```

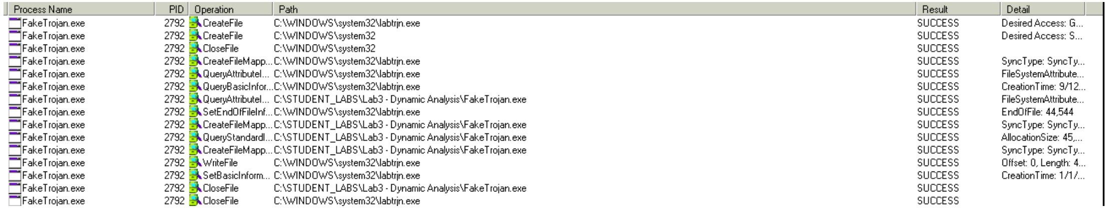
These modifications suggests that the malware is trying to create a persistent backdoor by configuring itself to start during system start-up and installing itself as a Windows Service.

3 Dynamic Analysis

The dynamic analysis of ”FakeTrojan.exe” is done by running the executable in a virtual machine while monitoring the now compromised system. The monitoring tools used were Wireshark, Process Monitor and Process explorer. Thereafter the executable is ran through the IDA Pro debugger to further analyze the behaviour of the program.

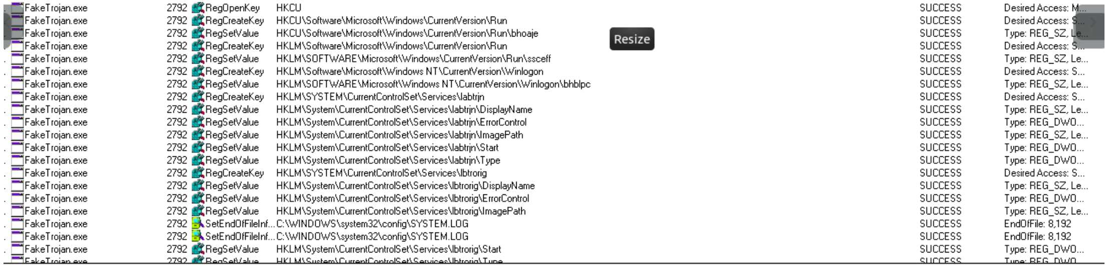
3.1 Process Monitor

By running the program and monitoring the actions in Process Monitor by applying the filter ”include FakeTrojan.exe”, many of the hypothetical actions discussed in the static analyze got verified. The image below shows a snippet of the actions of ”FakeTrojan.exe” monitored by Process Monitor.



Process Name	PID	Operation	Path	Result	Detail
FakeTrojan.exe	2792	CreateFile	C:\WINDOWS\system32\labtrjn.exe	SUCCESS	Desired Access: G...
FakeTrojan.exe	2792	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: S...
FakeTrojan.exe	2792	CloseFile	C:\WINDOWS\system32	SUCCESS	
FakeTrojan.exe	2792	CreateFileMapp...	C:\WINDOWS\system32\labtrjn.exe	SUCCESS	SyncType: SyncTy...
FakeTrojan.exe	2792	QueryAttributeI...	C:\WINDOWS\system32\labtrjn.exe	SUCCESS	FileSystemAttribute...
FakeTrojan.exe	2792	QueryBasicInfor...	C:\WINDOWS\system32\labtrjn.exe	SUCCESS	CreationTime: 9/12...
FakeTrojan.exe	2792	QueryAttributeI...	C:\STUDENT_LABS\Lab3 - Dynamic Analysis\FakeTrojan.exe	SUCCESS	FileSystemAttribute...
FakeTrojan.exe	2792	SetEndOfFileInf...	C:\WINDOWS\system32\labtrjn.exe	SUCCESS	EndOfFile: 44,544
FakeTrojan.exe	2792	CreateFileMapp...	C:\STUDENT_LABS\Lab3 - Dynamic Analysis\FakeTrojan.exe	SUCCESS	SyncType: SyncTy...
FakeTrojan.exe	2792	QueryStandardI...	C:\STUDENT_LABS\Lab3 - Dynamic Analysis\FakeTrojan.exe	SUCCESS	AllocationSize: 45,...
FakeTrojan.exe	2792	CreateFileMapp...	C:\STUDENT_LABS\Lab3 - Dynamic Analysis\FakeTrojan.exe	SUCCESS	SyncType: SyncTy...
FakeTrojan.exe	2792	WriteFile	C:\WINDOWS\system32\labtrjn.exe	SUCCESS	Offset: 0, Length: 4...
FakeTrojan.exe	2792	SetBasicInform...	C:\WINDOWS\system32\labtrjn.exe	SUCCESS	CreationTime: 1/1/...
FakeTrojan.exe	2792	CloseFile	C:\STUDENT_LABS\Lab3 - Dynamic Analysis\FakeTrojan.exe	SUCCESS	
FakeTrojan.exe	2792	CloseFile	C:\WINDOWS\system32\labtrjn.exe	SUCCESS	

The output above shows how a new file being created under ”C:/Windows/system32/” called labtrjn.exe which is then written to. By comparing the files ”FakeTrojan.exe” and ”labtrjn.exe” it is clear that ”labtrjn.exe” is a copy of the original malware. The copy is created to be persistent and somewhat hidden compared to the original ”FakeTrojan.exe”.



FakeTrojan.exe	2792	RegOpenKey	HKCU	SUCCESS	Desired Access: M...
FakeTrojan.exe	2792	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Desired Access: S...
FakeTrojan.exe	2792	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\bhoaje	SUCCESS	Type: REG_SZ, Le...
FakeTrojan.exe	2792	RegCreateKey	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Desired Access: S...
FakeTrojan.exe	2792	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ssceff	SUCCESS	Type: REG_SZ, Le...
FakeTrojan.exe	2792	RegCreateKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Desired Access: S...
FakeTrojan.exe	2792	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\bhblpc	SUCCESS	Type: REG_SZ, Le...
FakeTrojan.exe	2792	RegCreateKey	HKLM\SYSTEM\CurrentControlSet\Services\labtrjn	SUCCESS	Desired Access: S...
FakeTrojan.exe	2792	RegSetValue	HKLM\System\CurrentControlSet\Services\labtrjn\DisplayName	SUCCESS	Type: REG_SZ, Le...
FakeTrojan.exe	2792	RegSetValue	HKLM\System\CurrentControlSet\Services\labtrjn\ErrorControl	SUCCESS	Type: REG_DWO...
FakeTrojan.exe	2792	RegSetValue	HKLM\System\CurrentControlSet\Services\labtrjn\ImagePath	SUCCESS	Type: REG_SZ, Le...
FakeTrojan.exe	2792	RegSetValue	HKLM\System\CurrentControlSet\Services\labtrjn\Start	SUCCESS	Type: REG_DWO...
FakeTrojan.exe	2792	RegSetValue	HKLM\System\CurrentControlSet\Services\labtrjn\Type	SUCCESS	Type: REG_DWO...
FakeTrojan.exe	2792	RegCreateKey	HKLM\SYSTEM\CurrentControlSet\Services\lbtrorig	SUCCESS	Desired Access: S...
FakeTrojan.exe	2792	RegSetValue	HKLM\System\CurrentControlSet\Services\lbtrorig\DisplayName	SUCCESS	Type: REG_SZ, Le...
FakeTrojan.exe	2792	RegSetValue	HKLM\System\CurrentControlSet\Services\lbtrorig\ErrorControl	SUCCESS	Type: REG_DWO...
FakeTrojan.exe	2792	RegSetValue	HKLM\System\CurrentControlSet\Services\lbtrorig\ImagePath	SUCCESS	Type: REG_SZ, Le...
FakeTrojan.exe	2792	SetEndOfFileInf...	C:\WINDOWS\system32\config\SYSTEM.LOG	SUCCESS	EndOfFile: 8,192
FakeTrojan.exe	2792	SetEndOfFileInf...	C:\WINDOWS\system32\config\SYSTEM.LOG	SUCCESS	EndOfFile: 8,192
FakeTrojan.exe	2792	RegSetValue	HKLM\System\CurrentControlSet\Services\lbtrorig\Start	SUCCESS	Type: REG_DWO...
FakeTrojan.exe	2792	RegSetValue	HKLM\System\CurrentControlSet\Services\lbtrorig\Type	SUCCESS	Type: REG_DWO

The output above shows how ”FakeTrojan” creates further persistance by modifying the Windows Registry.

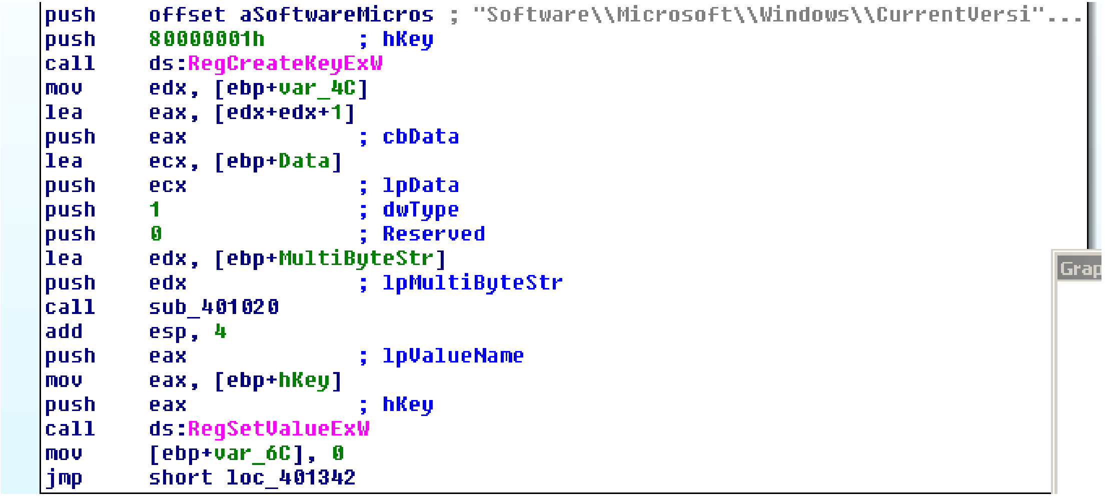
By creating the subkey called ”bhoaje” containing the path to the newly created ”labtrjn.exe” under the key:
HKCU/Software/Microsoft/Windows/CurrentVersion/Run
and the subkey called ”ssceff” containing the same path under the key:
HKLM/SOFTWARE/Microsoft/Windows/CurrentVersion/Run
the trojan is configured to be executed each time the system is powered on.

The same path is then added as data in a subkey called ”bhblpc” under the key:
HKLM/SOFTWARE/Microsoft/Windows NT/CurrentVersion/Winlogon
which configures the trojan to be executed each time a user is logged on or ”explorer.exe” runs.

Finally the two services ”labtrjn” and ”lbtrorig” are installed under the registry key:
HKLM/System/Microsoft/CurrentCOntrolSet/Services
The service ”labtrjn” contains an imagepath to ”C:/Windows/system32/labtrjn.exe”

while ”lbtrorig” (probably short for lab trojan original) contains the imagepath to the location of the original trojan, ”FakeTrojan.exe”.

The registry modifications mentioned above were done by ”FakeTrojan.exe”. The modification of ”HKCU/Software/Microsoft/Windows/CurrentVersion/Run” can be seen in the image below where the key is first accessed with the function ”RegCreateKeyExW” and is afterwards modificated by using the function ”RegSetKeyExW”.



```
push    offset aSoftwareMicros ; "Software\\Microsoft\\Windows\\CurrentVersi"...
push    80000001h       ; hKey
call    ds:RegCreateKeyExW
mov     edx, [ebp+var_4C]
lea     eax, [edx+edx+1]
push    eax             ; cbData
lea     ecx, [ebp+Data]
push    ecx             ; lpData
push    1               ; dwType
push    0               ; Reserved
lea     edx, [ebp+MultiByteStr]
push    edx             ; lpMultiByteStr
call    sub_401020
add     esp, 4
push    eax             ; lpValueName
mov     eax, [ebp+hKey]
push    eax             ; hKey
call    ds:RegSetValueExW
mov     [ebp+var_6C], 0
jmp     short loc_401342
```

All the modified registers are tampered with in a similar way.

3.2 Wireshark

The trojan does not seem to connect to any remote site considering that no outgoing traffic can be seen through Wireshark while the trojan is active. This result can be verified by the fact that no imports are made that supports network connections.

4 System Cleanup

4.1 Indicators of compromise

The indicators of compromise found during the analyze can be categorized in two different categories, paths and registry entries.

Paths:
C:/Windows/system32/labtrjn.exe
C:/STUDENT_LABS/Lab3 - Dynamic Analys/FakeTrojan.exe

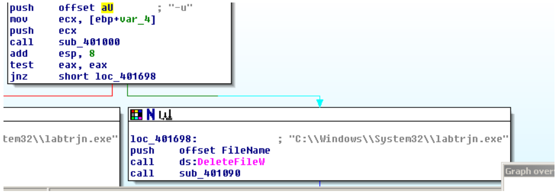
Registry Entries:
HKCU/Software/Microsoft/Windows/CurrentVersion/Run/bhoaje

HKLM/SOFTWARE/Microsoft/Windows/CurrentVersion/Run/ssceff
HKLM/SOFTWARE/Microsoft/Windows NT/CurrentVersion/Winlogon/bhblpc
HKLM/System/Microsoft/CurrentControlSet/Services/labtrjn
HKLM/System/Microsoft/CurrentControlSet/Services/tbtrorig

4.2 Cleaning instructions

To remove the trojan the files and registry entries mentioned above should be removed. To verify the cleanups success the system should be restarted. After the restart Process Explorer can be used to make sure that neither the ”labtrjn.exe” nor the ”FakeTrojan.exe” process is running.

During the analysis of ”FakeTrojan.exe” an uninstallation switch was discovered which can be used as an alternative to the manual cleaning instructions above. This switch made it possibly to delete ”labtrjn.exe”, all register modifications and terminating the malicious process. This switch was activated by passing the parameter ”-u” to the executable ”FakeTrojan.exe”. The uninstallation switch implementation can be seen in the image below.

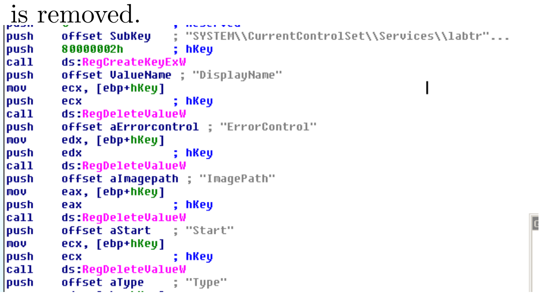


```
push    offset aU       ; "-u"
mov     ecx, [ebp+var_4]
push    ecx
call    sub_401000
add     esp, 8
test    eax, eax
jnz     short loc_401698
```

```
tem32\\labtrjn.exe"
```

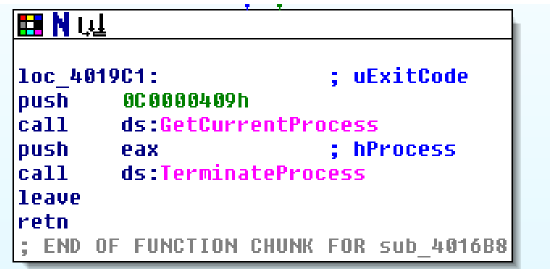
```
loc_401698:                 ; "C:\\Windows\\System32\\labtrjn.exe"
push    offset FileName
call    ds:DeleteFileW
call    sub_401090
```

The image shows how ”labtrjn.exe” is removed when the switch is activated but also a call to a subfunction. This function does further removal of register entries. Several register key deletions are made, the image below shows how the registry key and all the subkeys of ”HKLM/System/Microsoft/CurrentControlSet/Services/labtrjn
” is removed.



```
push    offset SubKey   ; "SYSTEM\\CurrentControlSet\\Services\\labtr"...
push    80000002h       ; hKey
call    ds:RegCreateKeyExW
push    offset ValueName ; "DisplayName"
mov     ecx, [ebp+hKey]
push    ecx             ; hKey
call    ds:RegDeleteValueW
push    offset aErrorcontrol ; "ErrorControl"
mov     edx, [ebp+hKey]
push    edx             ; hKey
call    ds:RegDeleteValueW
push    offset aImagepath ; "ImagePath"
mov     eax, [ebp+hKey]
push    eax             ; hKey
call    ds:RegDeleteValueW
push    offset aStart   ; "Start"
mov     ecx, [ebp+hKey]
push    ecx             ; hKey
call    ds:RegDeleteValueW
push    offset aType    ; "Type"
```

The last action after the uninstallation switch has been activated is that the ”labtrjn.exe”-service is terminated which can be seen in the image below.



```
loc_4019C1:              ; uExitCode
push    0C0000409h
call    ds:GetCurrentProcess
push    eax              ; hProcess
call    ds:TerminateProcess
leave
retn
; END OF FUNCTION CHUNK FOR sub_4016B8
```

This switch removes all malicious files and registry entries that "FakeTrojan.exe" has spawned but does not remove the file itself. "FakeTrojan.exe" has to be removed manually.

4.3 Questions and Answers

1. **What is Dynamic Analysis?**
   Dynamic analysis is done by observing the behaviour of the program while it is running on a host and thereby infecting the system. The dynamic analysis is often done in a sandbox environment such as a virtual machine to ensure that the possibly malicious program can't do any damage to the physical machine nor infect other systems over the network. The sandbox environment can then be rolled back to the state before the analysis and the infection is gone. The malware can also be ran through a debugger which means that the behaviour of the malware can be examined step by step.

2. **What ProcessExplorer can do?**
   The basic functionality in the process explorer is to list the currently active processes including information such as names, descriptions, company name, CPU demand and more. The list is built in a hierarchical tree structure and can show which process is a parent to another process. The list can also show which handles a particular process has and which DLLs are loaded into it. Process Explorer also has functionality to verify the signatures of processes against databases to ensure that the process is derived from the company it states. Finally every process can also be crosschecked towards the malware database VirusTotal to verify if the process has previously been analyzed and identified as malicious.

3. **What ProcessMonitor can do?**
   Process Monitor is a monitoring tool for Windows that shows modifications in the file system, registry and process/thread activity in real time. The information can easily be filtered to ensure that all data derived from for example an individual process can be examined.

4. **How to set up filters in ProcessMonitor?**
   The process monitor comes with a small set of predefined filters to eliminate information about a small set of windows events. Custom filters can

then easily be added by for example rightclicking an event that is interesting/uninteresting and include/exclude it from the currently used filters. The filters can be based on many different categories such as event type, time of the event and events concerning a certain process name.

5. **What are the Indicators-of-Compromise (IoCs) for the analyzed application?**
   The Indicators of compromise are listed in section 4.1 - Indicators of Compromise.