Malware lab3

Chen Zhuge IVCM132116

Algorithm:
remnux@remnux:~$ echo $RANDOM
12984
My number1= 16 + 12984mod90 = 40
My number2= 40 + 9 = 49

1)Story of where I found malwares:

They were found in Kafan Forum, http://bbs.kafan.cn/thread-1778521-1-1.html. From this thread, I was redicted to download page http://pan.baidu.com/s/1mgxD1jy. The downloaded ZIP file conents totally 18 malware samples. These three were randomly picked out from those samples. (The password of the downloaded ZIP file: infected)

2)hashes:

1st file: ff11.exe
remnux@remnux:~/Pahadus$ sha256sum ff11.exe
dcc25f627c62089660dcfd0b2177b163b5c52f2b59521b4df7fea69f0af27884 ff11.exe
remnux@remnux:~/Pahadus$ md5sum ff11.exe
39ab9018a13e17072f8accb022c09a04 ff11.exe

2nd file: kl0309.exe
remnux@remnux:~/Pahadus$ sha256sum kl0309.exe
0dec5a0cc69fb8da33f70c10f5703545f62628e439dfae4efffb6ea3578c70ae kl0309.exe
remnux@remnux:~/Pahadus$ md5sum kl0309.exe
fe94fcd5d5d4779e361da62d006772fa kl0309.exe

3rd file: 7.exe
remnux@remnux:~/New$ sha256sum 7.exe
2b3455114241727073ded60ba196b1e527d864addd54f6d6f106633c5e9ac123 7.exe
remnux@remnux:~/New$ md5sum 7.exe
7754bdc106b475cd60c16214c62dce36 7.exe

4th file: FAC32E50B561AC30FDD7D0ADB709399E

remnux@remnux:~/New$ sha256sum FAC32E50B561AC30FDD7D0ADB709399E
3faba568344c624b1ae231d42720259ed989203a41d790f6246f5d3e652c099e
FAC32E50B561AC30FDD7D0ADB709399E
remnux@remnux:~/New$ md5sum FAC32E50B561AC30FDD7D0ADB709399E
fac32e50b561ac30fdd7d0adb709399e FAC32E50B561AC30FDD7D0ADB709399E

5th file: 3.scr

remnux@remnux:~/New$ sha256sum 3.scr
25edd357a04e455dc8a8027384e651da695436592f7d6f96983a47a58483bf14 3.scr
remnux@remnux:~/New$ md5sum 3.scr

3fe3af78a555966fdc948232ed41f7ac 3.scr

3)The most common names:

1st file: ff11.exe => Trojan.Generic.1771345
2nd file: kl0309.exe => Trojan.Refpron.M
3rd file: 7.exe => Trojan.GenericKD.1920395
4th file: FAC32E50B561AC30FDD7D0ADB709399E => Gen:Variant.Zusy.110458
5th file: 3.scr => Trojan.Injector.BAJ

4)Strings:

1st file: ff11.exe

.....
GetStringTypeW
ff.dll
ServiceMain
~~{~{zz
Userenv.dll
CreateEnvironmentBlock
SeDebugPrivilege
winsta0\default
wtsapi32.dll
WTSQueryUserToken
explorer.exe
ProcessIdToSessionId
kernel32
.....
/ffxikaishi/get.asp
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
www.luckffxi.com
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.....
InstallModule
SOFTWARE\INSTALLCOOL\%s
polcore.dll
pol.exe
memcpy
msvcrt
.....

Reason: Seems that ff.dll is called here, followed by sensitive words as "ffxikaishi" and "www.luckffxi.com".

2nd file: kl0309.exe

*messages***
%08x
riched32.dll

riched20.dll
COMCTL32.DLL
InitCommonControlsEx
....
SeSecurityPrivilege
SeRestorePrivilege
.....
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity
  version="1.0.0.0"
  processorArchitecture="X86"
  name="WinRAR SFX"
  type="win32"/>
<description>WinRAR SFX module</description>
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
  <security>
    <requestedPrivileges>
      <requestedExecutionLevel level="asInvoker"
      uiAccess="false"/>
    </requestedPrivileges>
  </security>
</trustInfo>
<dependency>
  <dependentAssembly>
    <assemblyIdentity
      type="win32"
      name="Microsoft.Windows.Common-Controls"
      version="6.0.0.0"
      processorArchitecture="X86"
      publicKeyToken="6595b64144ccf1df"
      language="*"/>
  </dependentAssembly>
</dependency>
</assembly>

Reason: Some suspicious words appeared. The following seems like another suspicious assembly script, for which I don't understand quite well, but still worth digging.

3rd file: 7.exe

.....
1#QNAN
1#INF
1#IND
1#SNAN
This is a compiled AutoIt script. AV researchers please email avsupport@autoitscript.com for support.
uxtheme.dll
IsThemeActive

kernel32.dll
IsWow64Process
GetNativeSystemInfo
AU3_GetPluginDetails
AU3_FreeVar
MARK
ACCEPT
.....

Reason: Some related dll-s and other interesting information.

4th file: FAC32E50B561AC30FDD7D0ADB709399E

.....
PAD<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
 <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
  <security>
   <requestedPrivileges>
    <requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
   </requestedPrivileges>
  </security>
 </trustInfo>
</assembly>PAPADDINGXXPADDINGPADDINGXXPADDINGBp

Reason: I tried, but only found one thing worth mentioning, the PAD assembly script.

5th file: 3.scr

.....
PA<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
 <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
  <security>
   <requestedPrivileges>
    <requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
   </requestedPrivileges>
  </security>
 </trustInfo>
</assembly>PA

Reason: Almost the same outcome as the 4th file.

5) Links to the dirty and quick analysis.

www.virscan.org
www.threatexpert.com/submit.aspx

6) Interesting features that I learned.

Many rare malwares don't have its record in many anti-malware organizations. Before deciding to open a suspicious file, I'd better upload it to analysis websites and check.