

SpiritCat

spiritxcat@yahoo.com

- Describe your malware lab.

x86 with 2 gigs of ram and 80 gb HD, no net access, Debian Etch base OS. VMware Workstation 6 with various OS images. For this challenge I used:

Windows XP VM

software: IDApro, OllyDBG, PEInfo, Sniff_hit, FakeDNS, Procmon, procexp, bintext, regshot, stud_PE, Peid, ImportREC.exe.

Debian Etch VM

software: snort, irssi IRC client & ircd

- What information can you gather about the malware without executing it?

Running strings on the .exe file indicates that it is an executable that has possibly obfuscated in some manner.

- Is the malware packed? If so, how did you determine what it was?

Yes, the executable is packed with a version of UPX. Examining the .exe with Stud_PE revealed sections labeled: ABC0, ABC1 & ABC2. This is similar to UPX's standard sections of UPX0, UPX1, UPX2. The .exe would not unpack using UPX but following the SOP for unpacking UPX with Olly the unpacked executable was recovered.

- Describe the malware's behavior. What files does it drop? What registry keys does it create and/or modify? What network connections does it create? How does it auto-start, etc?

The malware checks its current location and if not located in [C:\Windows](#) it creates a file named Winsec32.exe in this location and runs this new executable. Md5sum shows this new executable to be the same as the original. This file's attributes are set so that the file is hidden in the default folder view settings. However the process Winsec32 is visible in the task manager as well as in procexp.

Reg Changes as recorded by regshot:

Keys added:6

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\Microsoft\OLE

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\Sysinternals\Process Explorer\ProcessComments

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\JavaSoft

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\JavaSoft\Java Update

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\JavaSoft\Java Update\Policy

Values deleted:2

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\kmixer\Enum\0: "SW\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}"

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kmixer\Enum\0: "SW\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}"

Values added:12

HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Update\Policy\VisitorId: "5292a48f-db6b568c"

HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Update\Policy\UpdateSchedule: 0x00000011

HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Update\Policy\Frequency: 0x011C0000

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Microsoft Svchost local services: "Winsec32.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Microsoft Svchost local services: "Winsec32.exe"

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU*b: "C:\secure\10-21-08-11-07.hiv"

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\hiv\b: "C:\secure\10-21-08-11-07.hiv"

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Zvpxrl\Qrfxgbc\znyjner\znyjner.rkr: 05 00 00 00 06 00 00 00 D0 C6 14 99 6C 33 C9 01

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Documents and Settings\Mickey\Desktop\malware\malware.exe: "malware"

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\Microsoft\OLE\Microsoft Svchost local services: "Winsec32.exe"

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\JavaSoft\Java Update\Policy>LastUpdateBeginTime: "Tue, 21 Oct 2008 11:02:20 GMT"

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\JavaSoft\Java Update\Policy>LastUpdateFinishTime: "Tue, 21 Oct 2008 11:02:20 GMT"

Values modified:17

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG\Seed: C4 75
BA 2C B5 B1 17 AD 51 50 43 44 22 31 9F 74 A5 15 F5 B1 11 E1 41 A6 C0 4A 7A 4E
A9 9F B8 60 75 22 F1 0B 7E DA 75 9F 29 53 DB E1 70 22 7E 89 BB 40 39 EE 3F 6C
2B E2 5E 82 7A 44 8D 19 5D F7 3D 0A 91 DD 54 92 6D 67 8F C8 46 E9 42 34 80 B9

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG\Seed: C1 32
F3 7A E4 BA 57 0A 6C 41 2B 76 C1 40 E2 7F 59 40 4E C8 72 7B A9 BE E3 A3 5F 6B
06 D9 2D 98 92 63 EF 81 F1 96 15 7D BC 94 FF A7 A7 BA 60 C1 08 8C E5 8F 57 CB
7B 1C 4E 75 78 60 9D 8B 0A 82 62 20 67 57 CC A7 14 5A C6 C9 19 14 EF E9 9C 58

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\kmixer\Enum\Count:
0x00000001

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\kmixer\Enum\Count:
0x00000000

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\kmixer\Enum\NextInst
ance: 0x00000001

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\kmixer\Enum\NextInst
ance: 0x00000000

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kmixer\Enum\Coun
t: 0x00000001

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kmixer\Enum\Coun
t: 0x00000000

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kmixer\Enum\Next
Instance: 0x00000001

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kmixer\Enum\Next
Instance: 0x00000000

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\Microsof
t\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU\a: 72 00 65 00 67 00
73 00 68 00 6F 00 74 00 2E 00 65 00 78 00 65 00 00 00 43 00 3A 00 5C 00 44 00 6F 00
63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 20 00 61 00 6E 00 64 00 20 00 53 00 65 00
74 00 74 00 69 00 6E 00 67 00 73 00 5C 00 4D 00 69 00 63 00 6B 00 65 00 79 00 5C 00
44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 64 00 61 00 74 00 61 00 00 00

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\Microsof

als\Process Explorer\Windowplacement: 2C 00 00 00 00 00 00 00 01 00 00 00 00 00 00
00 00 00 00 FF FF FF FF FF FF FF FF 64 00 00 00 32 00 00 00 BC 02 00 00 26 02
00 00

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\Sysintern
als\Process Explorer\Windowplacement: 2C 00 00 00 00 00 00 00 01 00 00 00 00 83 FF
FF 00 83 FF FF FF FF FF FF FF FF 64 00 00 00 32 00 00 00 BC 02 00 00 26 02
00 00

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\Sysintern
als\Process Explorer\ProcessSortColumn: 0xFFFFFFFF

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\Sysintern
als\Process Explorer\ProcessSortColumn: 0x00000003

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\Sysintern
als\Process Explorer\ShowProcessTree: 0x00000001

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\Sysintern
als\Process Explorer\ShowProcessTree: 0x00000000

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\Sysintern
als\Process Explorer\SymbolWarningShown: 0x00000000

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\Sysintern
als\Process Explorer\SymbolWarningShown: 0x00000001

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\Sysintern
als\Process Explorer\DefaultProcPropPage: 0x00000000

HKEY_USERS\S-1-5-21-1004336348-492894223-839522115-1003\Software\Sysintern
als\Process Explorer\DefaultProcPropPage: 0x00000006

Files Modified as recorded by regshot:

Files added:5

C:\Documents and Settings\Mickey\Local Settings\Temp\jusched.log

C:\Documents and Settings\Mickey\Local Settings\Temporary Internet
Files\Content.IE5\2XGFUD6L\10_21_08-11_07[1]

C:\WINDOWS\Prefetch\MALWARE.EXE-1CE26A6C.pf

C:\WINDOWS\Prefetch\WINSEC32.EXE-090839CD.pf

C:\WINDOWS\Winsec32.exe

Files deleted:1

C:\WINDOWS\SoftwareDistribution\DataStore\Logs\tmp.edb

Files [attributes?] modified:11

C:\Documents and Settings\Mickey\Cookies\index.dat

C:\Documents and Settings\Mickey\Local Settings\History\History.IE5\index.dat

C:\Documents and Settings\Mickey\Local Settings\Temporary Internet Files\Content.IE5\index.dat

C:\Documents and Settings\Mickey\NTUSER.DAT.LOG

C:\WINDOWS\Prefetch\JAVA.EXE-0539FACC.pf

C:\WINDOWS\SoftwareDistribution\DataStore\DataStore.edb

C:\WINDOWS\SoftwareDistribution\DataStore\Logs\edb.chk

C:\WINDOWS\SoftwareDistribution\DataStore\Logs\edb.log

C:\WINDOWS\system32\config\SECURITY.LOG

C:\WINDOWS\system32\config\software.LOG

C:\WINDOWS\WindowsUpdate.log

The following two registry keys ensures that the malware autostarts on system startup:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Microsoft Svchost local services: "Winsec32.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Microsoft Svchost local services: "Winsec32.exe"

- What type of command and control server does the malware use? Describe the server and interface this malware uses as well as the domains and URLs accessed by the malware.

Once started, the malware attempts to resolve the URL "tirc1.sh1xy2bg.net". Once this address is resolved it attempts to log into an IRC server on port 6667. Upon successful login to the IRC server it creates a custom nickname in the format <country>[operating system]<random 7 digit number> with a random user name. The malware, which is now obviously a bot, looks up user information on the IRC server then joins the channel #challenge, note the misspelling of challenge, with the password happy12. It then sets it's user mode to +i (invisible) -x (no squelch) +s (receive server messages). It also attempts to set the mode of the channel to +m (moderated) n (no external messages) s (secret channel) t (only ops can change the topic). It then attempts to set the channel topic to .acs vnc 100 0 0 -r -b . This message causes the bot to

start scanning the local subnet for VNC clients on port 5900. Examination of the recoverable strings in IDApro indicates the inclusion of a password dictionary that could possibly be used in a brute force attempt. The bot lists itself as REALMBOT which is a bot used to control characters in World of Warcraft. However, examination of the unpacked executable through virustotal.com identifies it as a modified version of sdBot which is a common IRC bot. Trying to login with the command `.login <pass>` gets a response from the bot indicating that this is indeed sdbot.

- What commands are present within the malware and what do they do? If possible, take control of the malware and run some of these commands, documenting how you did it.

Using IDApro and Olly I was able to identify the login mechanism for the bot program and obtain the required password. This was done by searching for the string “login” and then examining the calls to strcmp that followed. I passed an incorrect passwords to the bot and examined the output of the strcmp command by setting breakpoints with Olly. This showed that the bot was expecting the password “gemp123”. By using this password I was able to get past the password authenticate however the bot requires a form of two factor authentication to take control. Further analysis of the executable with Olly determined that the user has to be logged in from the domain “legalize.it” before the bot will authenticate you. This is easily bypassed by patching the executable with Olly. I changed the jnz to a jmp after the strcmp command used to check the login domain to ensure that the jump was always taken. Once the executable was patched I was able to take control of the bot. It responds to the usual sdBot commands: `.status`, `.id`, `.die`, etc.

- How would you classify this malware? Why?

This is a fairly common IRC bot that is set to scan for machines using VNC. It is dangerous, but easily detectable since it does not attempt to hide its existence or actions. The two factor authentication was a nifty change however. The fact that it uses IRC for C&C is the determining factor in its classification.

- What do you think the purpose of this malware is?

To locate machines with weak VNC passwords.

Bonus questions: (These questions are not required to be answered but could be used to break a tie for prizes.)

- Is it possible to find the malware's source code? If so, how did you do it?

Yes by searching the internet. SdBot is fairly common and the source is available on the net.

- How would you write a custom detection and removal tool to determine if the malware is present on the system and remove it?

This malware does not attempt to hide itself. You could detect it on the local machine by searching for the executable name or the md5sum of the executable. For network detection you could look for communication destined for port 6667. Look for nick changes in the form of `<country>[OS]<7 digit #>` is also a good way of detecting these sort of bots. A custom snort rule could be developed to alert on this pattern.