

# Thanks For All The Cash 1

30

To access this challenge, ssh to  
volatility@forensics.5charlie.com using the  
attached private key.  
Challenge files are located in /data.  
What is the correct Volatility profile  
for cash.img?

Run vol.py -f cash.img imageinfo to get the flag

```
forensicator@c6dff0dc8a0d:/data$ vol.py -f cash.img imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO      : volatility.debug      : Determining profile based on KDBG search...
           Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
           AS Layer1           : IA32PagedMemoryPae (Kernel AS)
           AS Layer2           : FileAddressSpace (/data/cash.img)
           PAE type            : PAE
           DTB                  : 0x319000L
           KDBG                 : 0x80544ce0L
           Number of Processors : 1
           Image Type (Service Pack) : 2
           KPCR for CPU 0       : 0xffdff000L
           KUSER_SHARED_DATA    : 0xffdf0000L
           Image date and time  : 2010-08-15 19:17:56 UTC+0000
           Image local date and time : 2010-08-15 15:17:56 -0400
```

Flag: WinXPSP2x86

Thanks For All The  
Cash 2

30

How many active network connections are  
there in this sample?

vol.py -f cash.img --profile=WinXPSP2x86 connections

```
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Local Address      Remote Address      Pid
-----
forensicator@c6dffb0dc8a0d:/data$ vol.py -f cash.img --profile=WinXPSP2x86 connections
vol.py -f cash.img --profile=WinXPSP2x86 connections
```

Flag: 0

# Thanks For All The Cash 3

## 30

What IP address and port did this system  
previously connect to? FORMAT  
AAA.BBB.CCC.DDD:PPPPP

```
vol.py -f cash.img --profile=WinXPSP2x86 connscan
```

This will find previous connections

```
forensicator@c6dff0dc8a0d:/data$ vol.py -f cash.img --profile=WinXPSP2x86 connectionsvol.py -f cash.img --profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)  Local Address      Remote Address      Pid
-----
0x02214988 172.16.176.143:1054 193.104.41.75:80    856
0x06015ab0 0.0.0.0:1056        193.104.41.75:80    856
```

Flag: 193.104.41.75:80

# Thanks For All The Cash 5

## 50

What key is used by this malware to  
maintain persistence?

If we look at pid 632 handles and grep for key we can find registry keys called by the process

```
vol.py -f cash.img --profile=WinXPSP2x86 handles -p 856 | grep -i key
```

xel0bd930	856	0x180	0x10	Key	USER
xel0bd9b0	856	0x188	0xf003f	Key	MACHINE\SOFTWARE\MICROSOFT\COM3
xel0bd9e0	856	0x190	0xf003f	Key	MACHINE\SOFTWARE\MICROSOFT\COM3
xel0bd810	856	0x198	0xf003f	Key	MACHINE\SOFTWARE\CLASSES\CLSID
xel0bd740	856	0x1a0	0xf003f	Key	MACHINE\SOFTWARE\CLASSES
xel0bd670	856	0x1a8	0xf003f	Key	MACHINE\SOFTWARE\MICROSOFT\COM3
xel0bd5a0	856	0x1b0	0x10	Key	USER
xel0bd4d0	856	0x1b8	0xf003f	Key	MACHINE\SOFTWARE\MICROSOFT\COM3
xel0bd400	856	0x1c0	0xf003f	Key	MACHINE\SOFTWARE\MICROSOFT\COM3
xel0bd330	856	0x1c8	0xf003f	Key	MACHINE\SOFTWARE\CLASSES\CLSID
xel7dce70	856	0x22c	0xf003f	Key	MACHINE\SYSTEM\CONTROLSET001\CONTROL\TERMINAL SERVER\LICENSING CORE
xel7dce08	856	0x234	0xf003f	Key	MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON

The one of interest is winlogon being called. This should not be called by anything spawned after winlogon initially.

Next we will need to jump into the registry, so start off with listing the hives with hivelist

```
forensicator@c6d8f0dc9a0d:/data$ vol.py -f cash.img --profile=WinXPSP2x86 connectionsvol.py -f cash.img --profile=WinXPSP2x86 hivelist
Volatility Foundation Volatility Framework 2.6.1
Virtual Physical Name
-----
0xelc49008 0x036dc008 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xelc41b60 0x04010b60 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xela39638 0x021eb638 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xela33008 0x01f98008 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xel153ab60 0x06b7db60 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xel1542008 0x06c48008 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xel1537b60 0x06ae4b60 \SystemRoot\System32\Config\SECURITY
0xel1544008 0x06c4b008 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xel13ae580 0x01bbd580 [no name]
0xel101b008 0x01867008 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xel1008978 0x01824978 [no name]
0xle158c0 0x009728c0 \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xlda4008 0x00f6e008 \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
```

Verify that we have the correct offset of the hklm:\system: 0xe153ab60

Run the following to get to the winlogon directory:

```
vol.py -f cash.img --profile=WinXPSP2x86 printkey -o 0xe153ab60 -K "Microsoft\windows  
nt\currentversion\winlogon"
```

```

forensicator@fc6dfff0dc8a0d:/data$ vol.py -f cash.img --profile=WinXPSP2x86 connectionsvol.py -f cash.img --
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable (V) = Volatile

-----
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\software
Key name: Winlogon (S)
Last updated: 2010-08-15 19:17:23 UTC+0000

Subkeys:
(S) GPExtensions
(S) Notify
(S) SpecialAccounts
(V) Credentials

Values:
REG_DWORD      AutoRestartShell : (S) 1
REG_SZ         DefaultDomainName : (S) BILLY-DB5B96DD3
REG_SZ         DefaultUserName : (S) Administrator
REG_SZ         LegalNoticeCaption : (S)
REG_SZ         LegalNoticeText : (S)
REG_SZ         PowerdownAfterShutdown : (S) 0
REG_SZ         ReportBootOk : (S) 1
REG_SZ         Shell : (S) Explorer.exe
REG_SZ         ShutdownWithoutLogon : (S) 0
REG_SZ         System : (S)
REG_SZ         Userinit : (S) C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\system32\sdra64.exe,
REG_SZ         VmApplet : (S) rundll32 shell32,Control_RunDLL "sysdm.cpl"
REG_DWORD      SfcQuota : (S) 4294967295
REG_SZ         allocatedcdroms : (S) 0
REG_SZ         allocatedasds : (S) 0
REG_SZ         allocatefloppies : (S) 0
REG_SZ         cachedlogonscount : (S) 10
REG_DWORD      forceunlocklogon : (S) 0
REG_DWORD      passwordexpirywarning : (S) 14
REG_SZ         scremoveoption : (S) 0
REG_DWORD      AllowMultipleTSSessions : (S) 1
REG_EXPAND_SZ  UIHost : (S) logonui.exe
REG_DWORD      LogonType : (S) 1
REG_SZ         Background : (S) 0 0 0
REG_SZ         AutoAdminLogon : (S) 0
REG_SZ         DebugServerCommand : (S) no
REG_DWORD      SFCDisable : (S) 0
REG_SZ         WinStationsDisabled : (S) 0
REG_DWORD      HibernationPreviouslyEnabled : (S) 1
REG_DWORD      ShowLogonOptions : (S) 0
REG_SZ         AltDefaultUserName : (S) Administrator
REG_SZ         AltDefaultDomainName : (S) BILLY-DB5B96DD3

```

The item of interest here is under the Userinit key with sdra64.exe, there should only be the userinit.exe here.

Flag: hklm:\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON

# Thanks For All The Cash 5

50

What executable is ran from the  
persistence registry key?

```
forensicator@c6dff0dc8a0d:/data$ vol.py -f cash.img --profile=WinXPSP2x86 connectionsvol.py -f cash.img --
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable (V) = Volatile

-----
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\software
Key name: Winlogon (S)
Last updated: 2010-08-15 19:17:23 UTC+0000

Subkeys:
(S) GPExtensions
(S) Notify
(S) SpecialAccounts
(V) Credentials

Values:
REG_DWORD      AutoRestartShell : (S) 1
REG_SZ         DefaultDomainName : (S) BILLY-DB5B96DD3
REG_SZ         DefaultUserName : (S) Administrator
REG_SZ         LegalNoticeCaption : (S)
REG_SZ         LegalNoticeText : (S)
REG_SZ         PowerdownAfterShutdown : (S) 0
REG_SZ         ReportBootOk : (S) 1
REG_SZ         Shell : (S) Explorer.exe
REG_SZ         ShutdownWithoutLogon : (S) 0
REG_SZ         System : (S)
REG_SZ         Userinit : (S) C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\system32\sdra64.exe,
REG_SZ         VmApplet : (S) rundll32 shell32,Control_RunDLL "sysdm.cpl"
REG_DWORD      SfcQuota : (S) 4294967295
REG_SZ         allocatecdroms : (S) 0
REG_SZ         allocatedasd : (S) 0
REG_SZ         allocatefloppies : (S) 0
REG_SZ         cachedlogonscount : (S) 10
REG_DWORD      forceunlocklogon : (S) 0
REG_DWORD      passwordexpirywarning : (S) 14
REG_SZ         scremoveoption : (S) 0
REG_DWORD      AllowMultipleTSSessions : (S) 1
REG_EXPAND_SZ  UIHost : (S) logonui.exe
REG_DWORD      LogonType : (S) 1
REG_SZ         Background : (S) 0 0 0
REG_SZ         AutoAdminLogon : (S) 0
REG_SZ         DebugServerCommand : (S) no
REG_DWORD      SFCDisable : (S) 0
REG_SZ         WinStationsDisabled : (S) 0
REG_DWORD      HibernationPreviouslyEnabled : (S) 1
REG_DWORD      ShowLogonOptions : (S) 0
REG_SZ         AltDefaultUserName : (S) Administrator
REG_SZ         AltDefaultDomainName : (S) BILLY-DB5B96DD3
```

Flag: C:\WINDOWS\system32\sdra64.exe

# Thanks For All The Cash 6

## 30

What is the name of the computer this  
sample was taken from?

```
vol.py -f cash.img --profile=WinXPSP2x86 envvars | grep -i computername
```

This will pull the environmental variables from all the pids and display the computername for us

```
forensicator@c6dff0dc8a0d:/data$ vol.py -f cash.img --profile=WinXPSP2x86 connectionsvol.py -f cash.img --profile=WinXPSP2x86 envvars | grep -i computername
Volatility Foundation Volatility Framework 2.6.1
632 winlogon.exe 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
676 services.exe 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
688 lsass.exe 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
844 vmacthlp.exe 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
856 svchost.exe 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
936 svchost.exe 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
1028 svchost.exe 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
1088 svchost.exe 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
1148 svchost.exe 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
1432 spoolsv.exe 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
1668 vmttoolsd.exe 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
1788 VMUpgradeHelper 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
1968 TPAutoConnSvc.e 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
216 alg.exe 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
888 wscntfy.exe 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
1084 TPAutoConnect.e 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
1732 wuauclt.exe 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
1724 explorer.exe 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
432 VMwareTray.exe 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
452 VMwareUser.exe 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
468 wuauclt.exe 0x00010000 COMPUTERNAME BILLY-DB5B96DD3
```

Flag: BILLY-DB5B96DD3

# Thanks For All The Cash 7

## 50

How many processors exist on this  
system?

If we look at the envvars for a process we see our answer:

```
forensicator@c6dfff0dc8a0d:/data$ vol.py -f cash.img --profile=WinXPSP2x86 connectionsvol.py -f cash.img --profile=WinXPSP2x86 envvars -p 632
Volatility Foundation Volatility Framework 2.6.1
Pid      Process      Block      Variable      Value
-----
632 winlogon.exe 0x00010000 ALLUSERSPROFILE C:\Documents and Settings\All Users
632 winlogon.exe 0x00010000 APPDATA C:\Documents and Settings\Administrator\Application Data
632 winlogon.exe 0x00010000 CommonProgramFiles C:\Program Files\Common Files
632 winlogon.exe 0x00010000 COMPUTERTNAME BILLY-DB5B96DD3
632 winlogon.exe 0x00010000 ComSpec C:\WINDOWS\system32\cmd.exe
632 winlogon.exe 0x00010000 FP_NO_HOST_CHECK NO
632 winlogon.exe 0x00010000 LOGONSERVER \\BILLY-DB5B96DD3
632 winlogon.exe 0x00010000 NUMBER_OF_PROCESSORS 1
632 winlogon.exe 0x00010000 OS Windows_NT
632 winlogon.exe 0x00010000 Path C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
632 winlogon.exe 0x00010000 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
632 winlogon.exe 0x00010000 PROCESSOR_ARCHITECTURE x86
632 winlogon.exe 0x00010000 PROCESSOR_IDENTIFIER x86 Family 6 Model 23 Stepping 10, GenuineIntel
632 winlogon.exe 0x00010000 PROCESSOR_LEVEL 6
632 winlogon.exe 0x00010000 PROCESSOR_REVISION 170a
632 winlogon.exe 0x00010000 ProgramFiles C:\Program Files
632 winlogon.exe 0x00010000 SystemDrive C:
632 winlogon.exe 0x00010000 SystemRoot C:\WINDOWS
632 winlogon.exe 0x00010000 TEMP C:\WINDOWS\TEMP
632 winlogon.exe 0x00010000 TMP C:\WINDOWS\TEMP
632 winlogon.exe 0x00010000 USERPROFILE C:\Documents and Settings\Administrator
632 winlogon.exe 0x00010000 windir C:\WINDOWS
```

Flag: 1



# Thanks For All The Cash 8

## 30

What is the name of the currently logged  
on user?

We look at the Winlogon.exe process ID 632, we see the answer.

```
forensicator@c6dfff0dc8a0d:/data$ vol.py -f cash.img --profile=WinXPSP2x86 connectionsvol.py -f cash.img --profile=WinXPSP2x86 envvars -p 632
Volatility Foundation Volatility Framework 2.6.1
```

Pid	Process	Block	Variable	Value
632	winlogon.exe	0x00010000	ALLUSERSPROFILE	C:\Documents and Settings\All Users
632	winlogon.exe	0x00010000	APPDATA	C:\Documents and Settings\Administrator\Application Data
632	winlogon.exe	0x00010000	CommonProgramFiles	C:\Program Files\Common Files
632	winlogon.exe	0x00010000	COMPUTERNAME	BILLY-DB5B96DD3
632	winlogon.exe	0x00010000	ComSpec	C:\WINDOWS\system32\cmd.exe
632	winlogon.exe	0x00010000	FP_NO_HOST_CHECK	NO
632	winlogon.exe	0x00010000	LOGONSERVER	\\BILLY-DB5B96DD3
632	winlogon.exe	0x00010000	NUMBER_OF_PROCESSORS	1
632	winlogon.exe	0x00010000	OS	Windows_NT
632	winlogon.exe	0x00010000	Path	C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
632	winlogon.exe	0x00010000	PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
632	winlogon.exe	0x00010000	PROCESSOR_ARCHITECTURE	x86
632	winlogon.exe	0x00010000	PROCESSOR_IDENTIFIER	x86 Family 6 Model 23 Stepping 10, GenuineIntel
632	winlogon.exe	0x00010000	PROCESSOR_LEVEL	6
632	winlogon.exe	0x00010000	PROCESSOR_REVISION	170a
632	winlogon.exe	0x00010000	ProgramFiles	C:\Program Files
632	winlogon.exe	0x00010000	SystemDrive	C:
632	winlogon.exe	0x00010000	SystemRoot	C:\WINDOWS
632	winlogon.exe	0x00010000	TEMP	C:\WINDOWS\TEMP
632	winlogon.exe	0x00010000	TMP	C:\WINDOWS\TEMP
632	winlogon.exe	0x00010000	USERPROFILE	C:\Documents and Settings\Administrator
632	winlogon.exe	0x00010000	windir	C:\WINDOWS

Flag: Administrator

# Thanks For All The Cash 9

## 30

What malware family does McAfee report  
PID 856 as?

For this we will try malfind and dump this to a tmp directory

First create a folder in the tmp directory: `mkdir /tmp/malfind`

Then run the following: `vol.py -f cash.img --profile=WinXPSP2x86 malfind -p 856 --dump-dir /tmp/mal/`

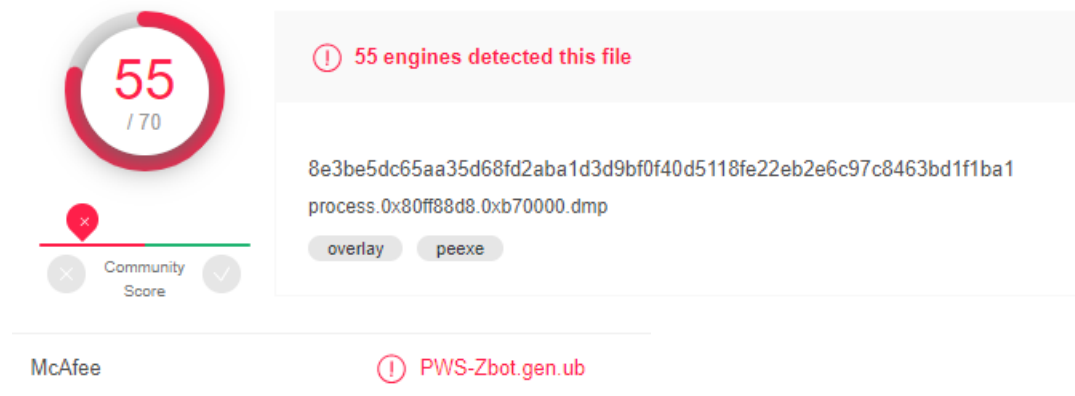
This will create two items in the directory

```
forensicator@c6dff0dc8a0d:/data$ ls /tmp/mal/  
process.0x80ff88d8.0xb70000.dmp  process.0x80ff88d8.0xcb0000.dmp  
forensicator@c6dff0dc8a0d:/data$
```

Sha1sum a file and throw it into virus total to see what comes back.

```
forensicator@c6dff0dc8a0d:/data$ sha1sum /tmp/mal/process.0x80ff88d8.0xb70000.dmp  
c38cad24055afaac806c94b2e380a406a55e277f  /tmp/mal/process.0x80ff88d8.0xb70000.dmp  
forensicator@c6dff0dc8a0d:/data$
```

Hash: c38cad24055afaac806c94b2e380a406a55e277f



55 / 70

55 engines detected this file

8e3be5dc65aa35d68fd2aba1d3d9bf0f40d5118fe22eb2e6c97c8463bd1f1ba1  
process.0x80ff88d8.0xb70000.dmp

overlay peexe

McAfee PWS-Zbot.gen.ub

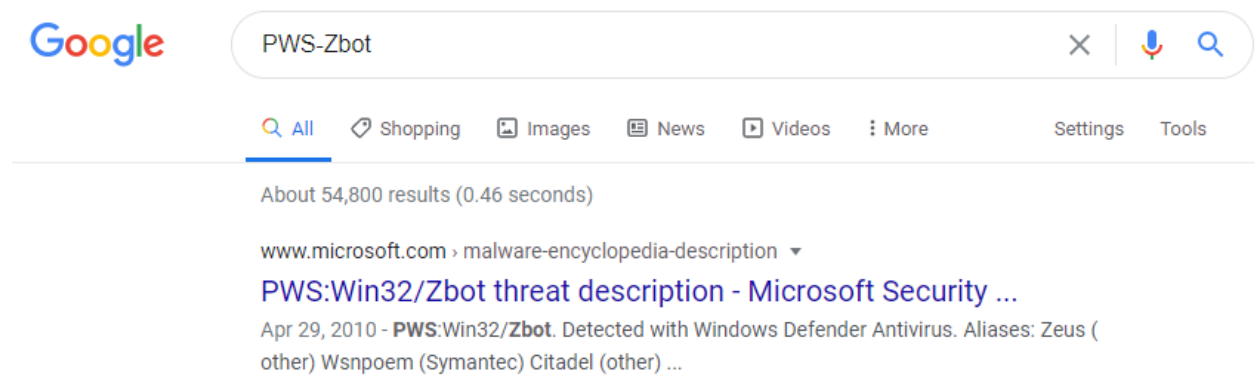
Flag: PWS-Zbot.gen.ub

Thanks For All The  
Cash 10

50

Based on the reports from Thanks For All  
The Cash 9, what (early version) malware  
are you likely looking at?

Do a google search for PWS-Zbot and we get the following results:



The screenshot shows a Google search interface. The search bar contains the text "PWS-Zbot". Below the search bar, the Google logo is on the left, and navigation links for "All", "Shopping", "Images", "News", "Videos", and "More" are in the center. On the right, there are links for "Settings" and "Tools". Below the navigation bar, it says "About 54,800 results (0.46 seconds)". The first search result is from "www.microsoft.com" with the title "PWS:Win32/Zbot threat description - Microsoft Security ...". The snippet below the title reads: "Apr 29, 2010 - **PWS:Win32/Zbot**. Detected with Windows Defender Antivirus. Aliases: Zeus (other) Wsnpoem (Symantec) Citadel (other) ...".

Flag: Zeus