



# Vista system restore rootkit

Principle and protection

**Edward Sun**

**HIT Conference 2008**

# About speaker

- u **Network ID : CardMagic**
- u **Author of DarkSpy anti-rootkit**
- u **Posted several articles on rootkit.com**
- u **R&D of some world famous kernel level products in global companies**
- u **Experienced in Windows kernel mode research and programming**
- u **Now is a researcher of Trend Micro threat solution team**

**HIT Conference 2008**

# What will be introduced

- u **Internals of Vista system restore**
- u **A user-mode rootkit to hide arbitrary file or registry key from Windows Vista system restore**
- u **A new way to bypass modern HIPS**
- u **Detection and protection of the threat**

HIT Conference 2008

# Agenda

- u **Vista system restore (VSR) introduction**
- u **VSR internals**
- u **VSR rootkit**
- u **A new way to bypass HIPS**
- u **Protect & detect VSR**
- u **Demo**

**HIT Conference 2008**

# Vista system restore (VSR) introduction

- u **VSR allows user to use restore point to return their system files and settings to an earlier point in time**
- u **System restore in Vista has been enhanced a lot and use new architecture & implementation which is different from XP's**
- u **System Restore can make changes to Windows system files, registry settings, and programs installed on your computer. It also can make changes to scripts, batch files, and other types of executable files on your computer**

**HIT Conference 2008**

# VSR internals

- u **But how does VSR work? Microsoft hasn't provided detail document about how it works .**
- u **We will introduce the whole process in three phases**
  1. **Create restore point (when you click "Create" button)**
  2. **Serve a restore request (when you click "Restore" button)**
  3. **Shutdown & Startup (when the system shuts down after you clicking "Restore")**

**HIT Conference 2008**

## u Create restore point

**Rely on shadow copy mechanism to create a volume shadow copy, see the call stack of SRSetRestorePoint**

```
VSSAPI!CreateVssBackupComponents  
SPP!CSpp::_CreateGroupHelper+0x2a7  
SPP!CSpp::_CreateGroupNoEnum+0xde  
srclient!SetSRStateAfterSetup+0xc58  
srclient!SetSRStateAfterSetup+0xd55  
srclient!SetSRStateAfterSetup+0xff0  
srclient+0x2ae0  
srclient!SRSetRestorePointW+0x29  
TMVEManager!CVirtualEnvironment::_CreateRestorePoint+0x7f  
TMVEManager!CSystemProtectionDlg::_OnBnClickedCreatevirtualenvironment+0xb4  
TMVEManager!_AfxDispatchCmdMsg+0x43  
TMVEManager!CCmdTarget::_OnCmdMsg+0x118  
TMVEManager!CDialog::_OnCmdMsg+0x1b  
TMVEManager!CWnd::_OnCommand+0x90  
TMVEManager!CWnd::_OnWndMsg+0x36  
TMVEManager!CWnd::_WindowProc+0x22  
TMVEManager!AfxCallWndProc+0x9a  
TMVEManager!AfxWndProc+0x34  
USER32!GetMessageW+0x6e  
USER32!GetMessageW+0x146
```

**HIT Conference 2008**

# Shadow copy

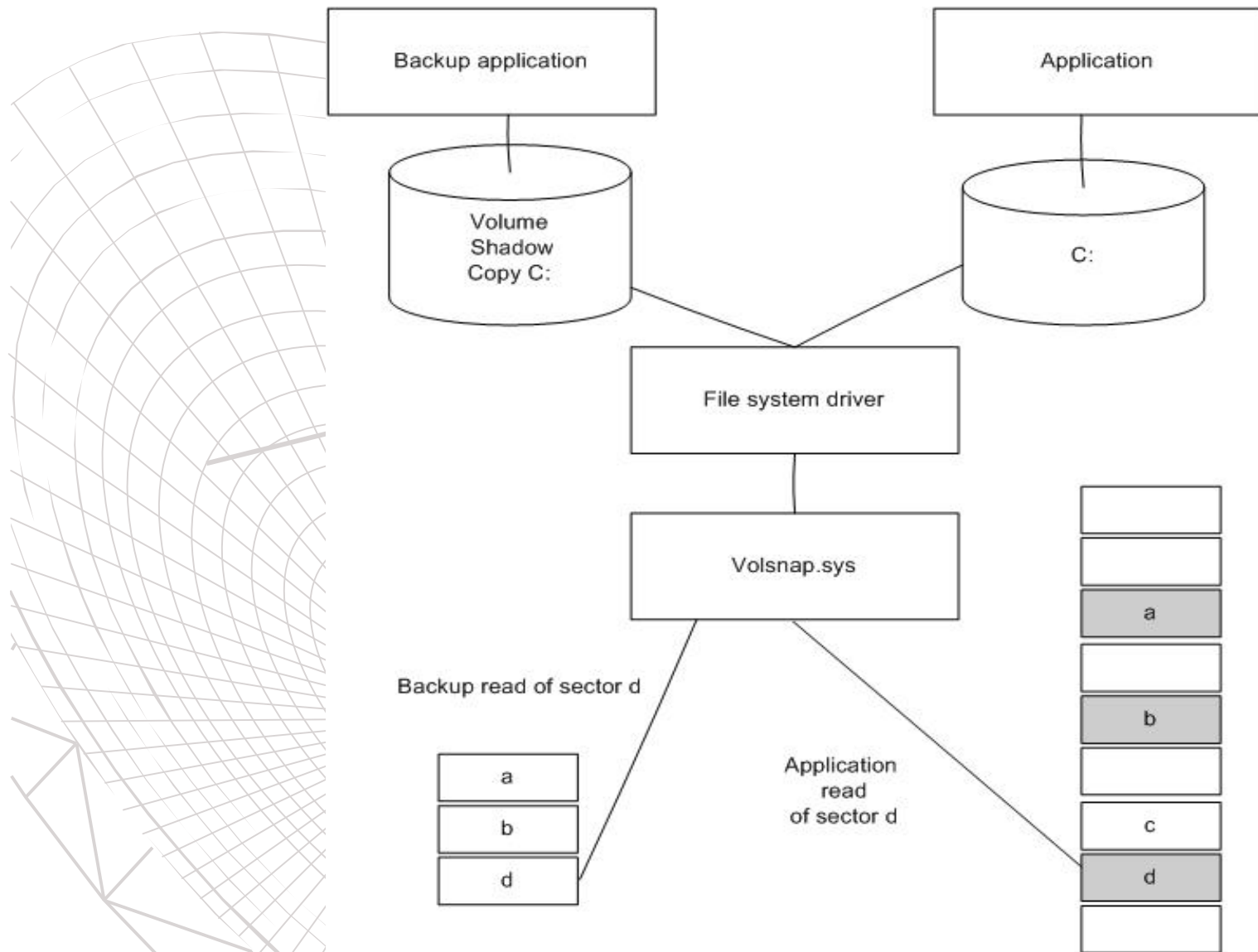
**Implemented with disk filter -- Volsnap.sys**

**It can back up original sector when it finds any writer's modification action and provide backup application a point in time view of a volume**

**E.g. if application(writer) has written a,b,d, the original copy of these sectors are kept by shadow copy service in storage. When backup application accesses the three sectors, shadow copy service will route the request to original copy. However, when c is requested, the service will direct the request to real volume.**

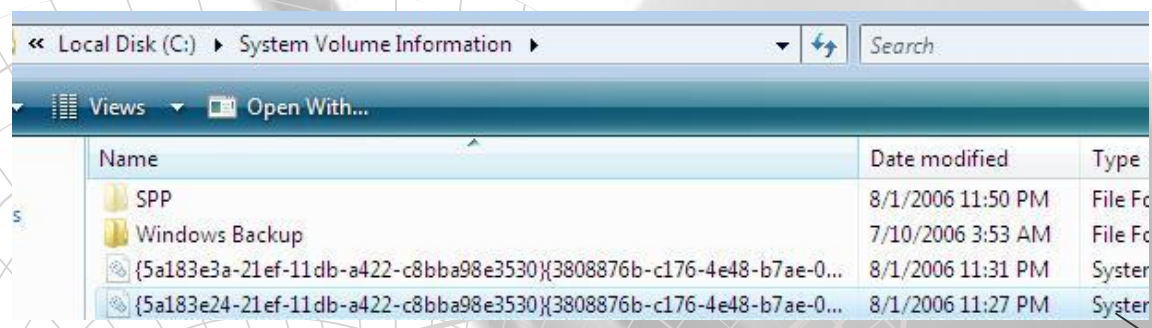
**HIT Conference 2008**





HIT Conference 2008

# Associated shadow copy files located here:



Local Disk (C:) > System Volume Information

Name	Date modified	Type
SPP	8/1/2006 11:50 PM	File Folder
Windows Backup	7/10/2006 3:53 AM	File Folder
{5a183e3a-21ef-11db-a422-c8bba98e3530}{3808876b-c176-4e48-b7ae-0...}	8/1/2006 11:31 PM	System Volume Shadow Copy
{5a183e24-21ef-11db-a422-c8bba98e3530}{3808876b-c176-4e48-b7ae-0...}	8/1/2006 11:27 PM	System Volume Shadow Copy

- HarddiskVolumeShadowCopy8
- HarddiskVolumeShadowCopy9
- HarddiskVolumeShadowCopy{5a183e24-21ef-11db-a422-c8bba98e3530}
- HarddiskVolumeShadowCopy{5a183e36-21ef-11db-a422-c8bba98e3530}
- HarddiskVolumeShadowCopy{5a183e3a-21ef-11db-a422-c8bba98e3530}

Backup file id matches the name of shadow volume device name

HIT Conference 2008

## u Serve a restore request

When backup program calls restoration method, two processes will be launched :  
**WmiPrvSE.exe**( to hold srwmi.dll) , **dllhost.exe**(to hold srcore.dll)



services.exe	544	1.49	Services and Controller app
svchost.exe	736		Host Process for Windows Services
WmiPrvSE.exe	3180		WMI Provider Host
dllhost.exe	4092		COM Surrogate
levelhost.exe	796		Host Process for Windows Services

HIT Conference 2008

Then the control transferred to srwmi.dll --  
**CSrWMIProvider::Restore**

**This method will involve score.dll:**

CreateInstance here

Clsid

```

push offset __GUID_b653f1e0_17d7_4ac6_9b18_f84b61dbc1a2 ; riid
push 10004h ; dwClsContext
push ebx ; pUnkOuter
push offset _CLSID_SrControl ; rclsid
mov [ebp-34h], ebx
mov word ptr [ebp-30h], 2D0h
call ds: __imp__CoCreateInstance@20 ; CoCreateInstance(x,x,x,x,x)

```

```

38 ; CLSID CLSID_SrControl
38 _CLSID_SrControl db 0FCh ; Q
38
39 db 0F1h ; Q
3A db 3Fh ; ?
3B db 88h ; Q
3C db 0E1h ; Q
3D db 9
3E db 0E5h ; Q
3F db 48h ; H
40 db 8Eh ; Q
41 db 54h ; T
42 db 0E2h ; Q
43 db 46h ; F

```

; D  
; C

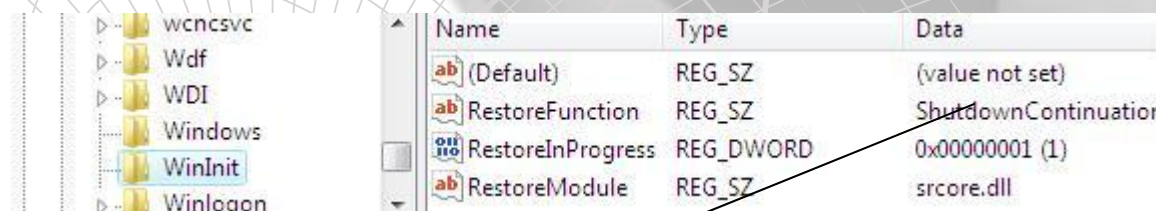
Corresponding  
Registry key

{8833BC41-DC6B-34B9-A799-682D}	Name	Type	Data
{883FF1FC-09E1-48e5-8E54-E2469A}	(Default)	REG_EXPAND_SZ	%systemroot%\system32\score.dll
InprocServer32	ThreadingModel	REG_SZ	Both
ProgID			

HIT Conference 2008

srcore.dll will do some preparation and configuration work and then call its internal interface `_RegisterForShutdownContinuation`.

This routine will create WinInit key and register a callback function for Windows shutdown. And the key looks like



The screenshot shows the Windows Registry Editor with the 'WinInit' key selected in the left pane. The right pane displays a list of registry values:

Name	Type	Data
(Default)	REG_SZ	(value not set)
RestoreFunction	REG_SZ	ShutdownContinuation
RestoreInProgress	REG_DWORD	0x00000001 (1)
RestoreModule	REG_SZ	srcore.dll

The routine will be called for shutdown restoration logic

HIT Conference 2008

## u Shutdown & Startup

### The Shutdown Call back:

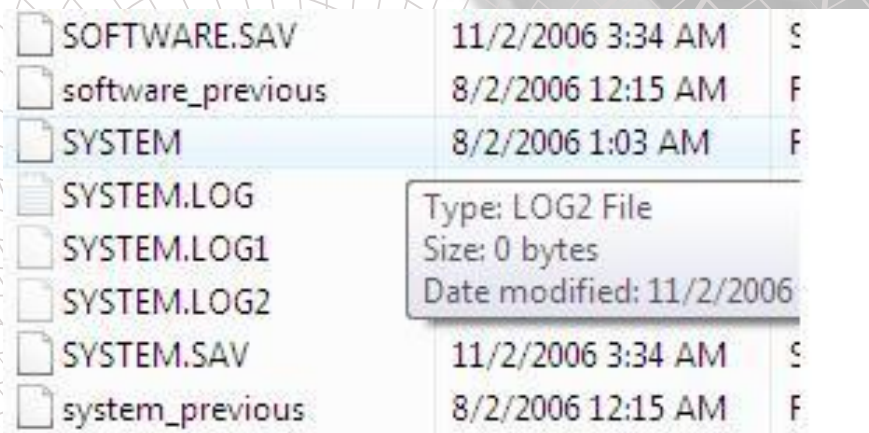
When system shuts down, the ShutdownContinuation will be called, and this callback routine is exported by srcore.dll. In this routine, it will parse shadow volume information and restore various system elements. The main restore logic include two parts :

HIT Conference 2008

## a. Registry restore :

The registry restore is based on hive file:

srcore will firstly rename the original hive file and then copy the backed hive file from volume shadow copy. The original hive file will be renamed as xxxx\_previous, and after reboot system will use the backed hive file.



SOFTWARE.SAV	11/2/2006 3:34 AM	S
software_previous	8/2/2006 12:15 AM	F
SYSTEM	8/2/2006 1:03 AM	F
SYSTEM.LOG		
SYSTEM.LOG1		
SYSTEM.LOG2		
SYSTEM.SAV	11/2/2006 3:34 AM	S
system_previous	8/2/2006 12:15 AM	F

Type: LOG2 File  
Size: 0 bytes  
Date modified: 11/2/2006

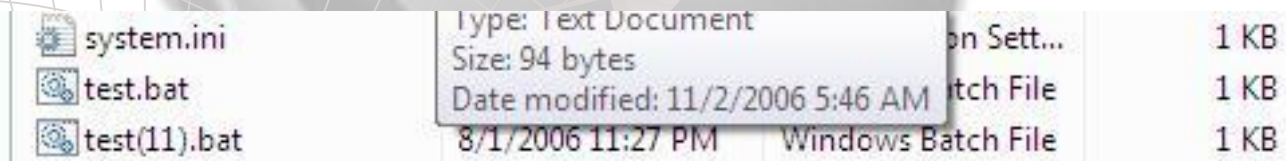
HIT Conference 2008

## b. File restore:

Modified file will be restored immediately, excepted inaccessible file.

For inaccessible file :

srcore will firstly copy the old version file to the restore folder and name it like :



system.ini	Type: Text Document	on Sett...	1 KB
test.bat	Size: 94 bytes	atch File	1 KB
test(11).bat	Date modified: 11/2/2006 5:46 AM	Windows Batch File	1 KB
	8/1/2006 11:27 PM		

Then it will register an autorun program called srdelayed.exe which will be executed when system starts up, and meanwhile log the operations which will be done by srdelayed.exe in <System volume information>\systemrestore\DelayedOperations. srdelayed.exe will overwrite the inaccessible file later with the copied file.

Show result :

Finally,srcore will register an autorun entry under <RunOnce> key to execute rstrui.exe to show the restore status when user enter system next time.

HIT Conference 2008



## Startup :

In the startup, Windows will run `srdelayed.exe` to do some remaining post actions (e.g. move the copied file to overwrite the file which is inaccessible in previous restore). And then run `rstrui.exe` to show restore result to user.

HIT Conference 2008

# VSR rootkit

u **Purpose :**

**survive after the system restore**

**hide following items from system restore:**

- 1. registry items**
- 2. executables**

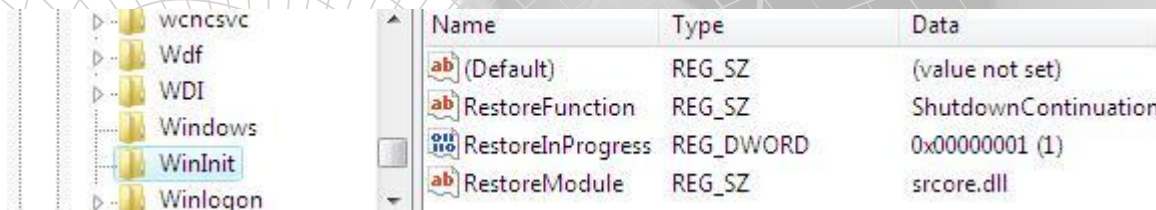
**HIT Conference 2008**

## u Approach :

### 1. How this rootkit intercept the restore process:

#### Thru shutdown call back hooking :

Microsoft has passed the restore function name and module under WinInit as described before :



The image shows a screenshot of the Windows Registry Editor. The left pane displays a tree view with the following folders expanded: wcnscvc, Wdf, WDI, Windows, WinInit (selected), and Winlogon. The right pane shows the values for the WinInit key:

Name	Type	Data
(Default)	REG_SZ	(value not set)
RestoreFunction	REG_SZ	ShutdownContinuation
RestoreInProgress	REG_DWORD	0x00000001 (1)
RestoreModule	REG_SZ	srcore.dll

HIT Conference 2008

**This key will be set when the system requests a restore. If rootkit dynamically modifies this key to point to its module and routine when after system sets this key, guess what will happen ?**

**Yes, the rootkit's module will be loaded, Microsoft has no checking on the module.**

## **2. How can it continue the system restore:**

**It loads sscore.dll internally ,and call ShutdownContinuation exported by sscore itself.**

**HIT Conference 2008**

### 3. How can it make file survive?

It loads file in memory before calling ShutdownContinuation exported by sscore.dll, and restore the files from memory to disk after the calling. (because all files and registry items are restored in the calling)

### 4. How can it make registry item survive?

This is relatively difficult, but still easy for a rootkit author. As described before, OS will rename original hive to a new name ,and copy restored hive to the location.

However, after these operations in calling of ShutdownContinuation exported by sscore.dll, both the restored hive file and renamed hive file will be locked.

**What VSR does to solve the locking problem is to hook IAT of srcore.dll to intercept the call : RegLoadKeyW**

**In its hooking procedure of RegLoadKeyW, it will follow the below steps :**

**For registry hive it wants to hide items in:**

- a. load the key ourselves to a temp key before calling the real RegLoadKeyW**
- b. do recovery (write rootkit protected registry items to registry) under temp key**
- c. unload the key**
- d. pass the call control to real RegLoadKeyW and return**

**For registry hive it doesn't want to hide any item in, just simply pass the call control to real RegLoadKeyW and return.**

**HIT Conference 2008**

# A new way to bypass HIPS

- Malware author might benefit from shutdown call back hook to bypass commercial HIPS

- The theory :

1. Malware initiates a restore from any restore point, and modify restore module and routine to point to malicious ones.

2. When user shuts down his computer, malicious module will be called, and malware can do anything they want (E.g. create malicious autorun key) without popup of HIPS in its module.

HIT Conference 2008

u **But there might be some concerns:**

**1. Will user notice if the shutdown takes long time to complete? (Because the restoration will happen during system shuts down)**

**No, because malware will not need to call original ShutdownContinuation for any restore actions. This will make the shutdown very quick.**

**2. How malware solves Vista's popup for restore error next time when user logs on if it doesn't call original ShutdownContinuation ?**

**This can be done by deletion of run key rstrui.exe under <RunOnce>**

**HIT Conference 2008**

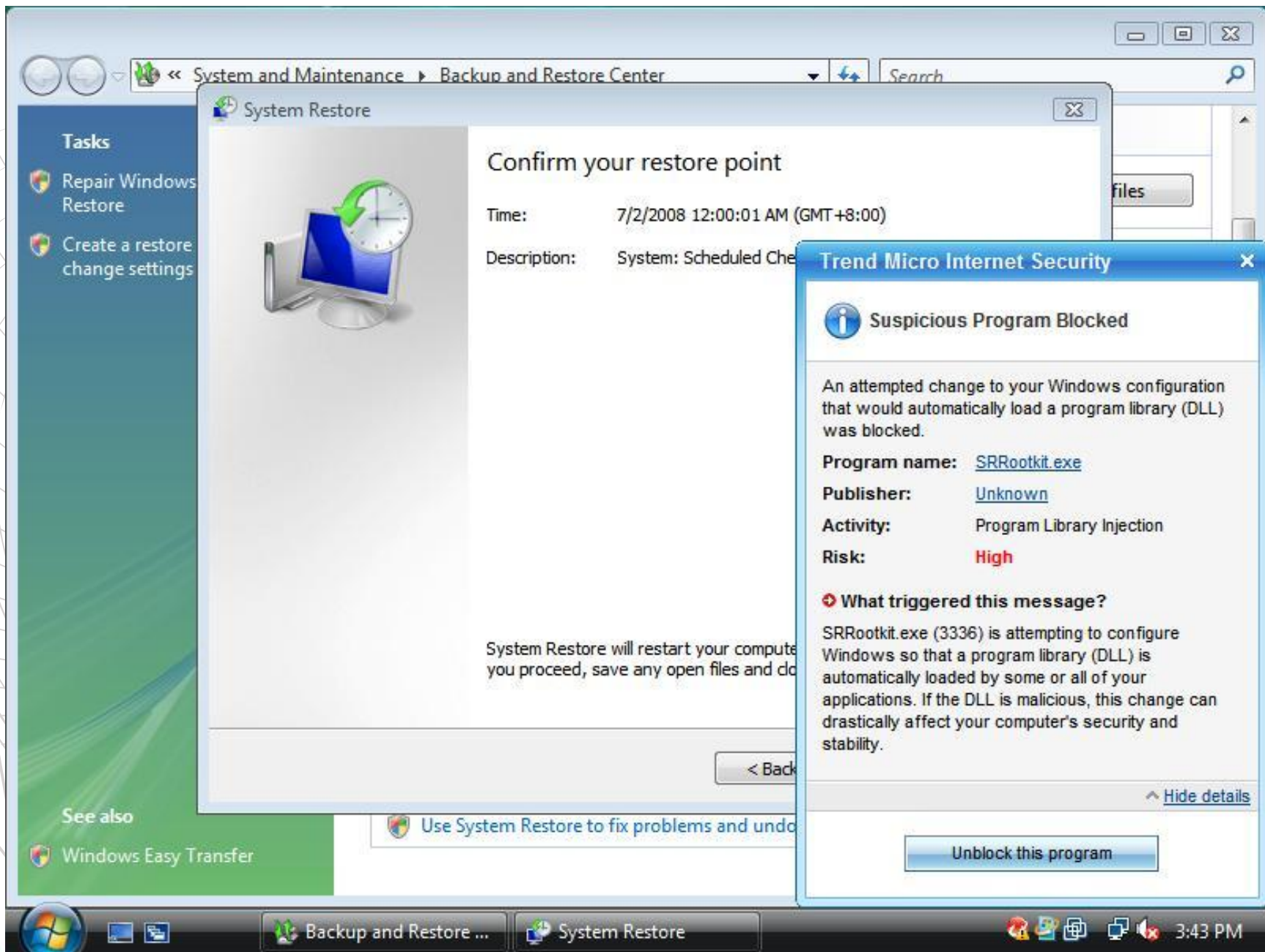


# Protect & detect VSR

- Microsoft needs to use more secure parameter passing method (e.g. do signature verification for calling module)
- For commercial HIPS to protect VSR intrusion , they need to monitor the WinInit modification by a malware.

**But the challenge is : Microsoft might still leaves some other places to implement VSR.**

HIT Conference 2008



HIT Conference 2008

**For detection of the VSR, security providers can use the cross-compare technology for rootkit detection.**

**In order to get the real view of files & reg keys that system restore should restore, they can access the volume shadow copy to enumerate the files & reg keys in restore point.**

**How can they access ?**

**Just use Win32 API (e.g. FindFirstFile), but pass the path parameter like:**

**\\.\HarddiskVolumeShadowCopy2\Windows\system32**

**(But the media is just read-only)**

**HIT Conference 2008**



Thanks

Q & A

**HIT Conference 2008**