

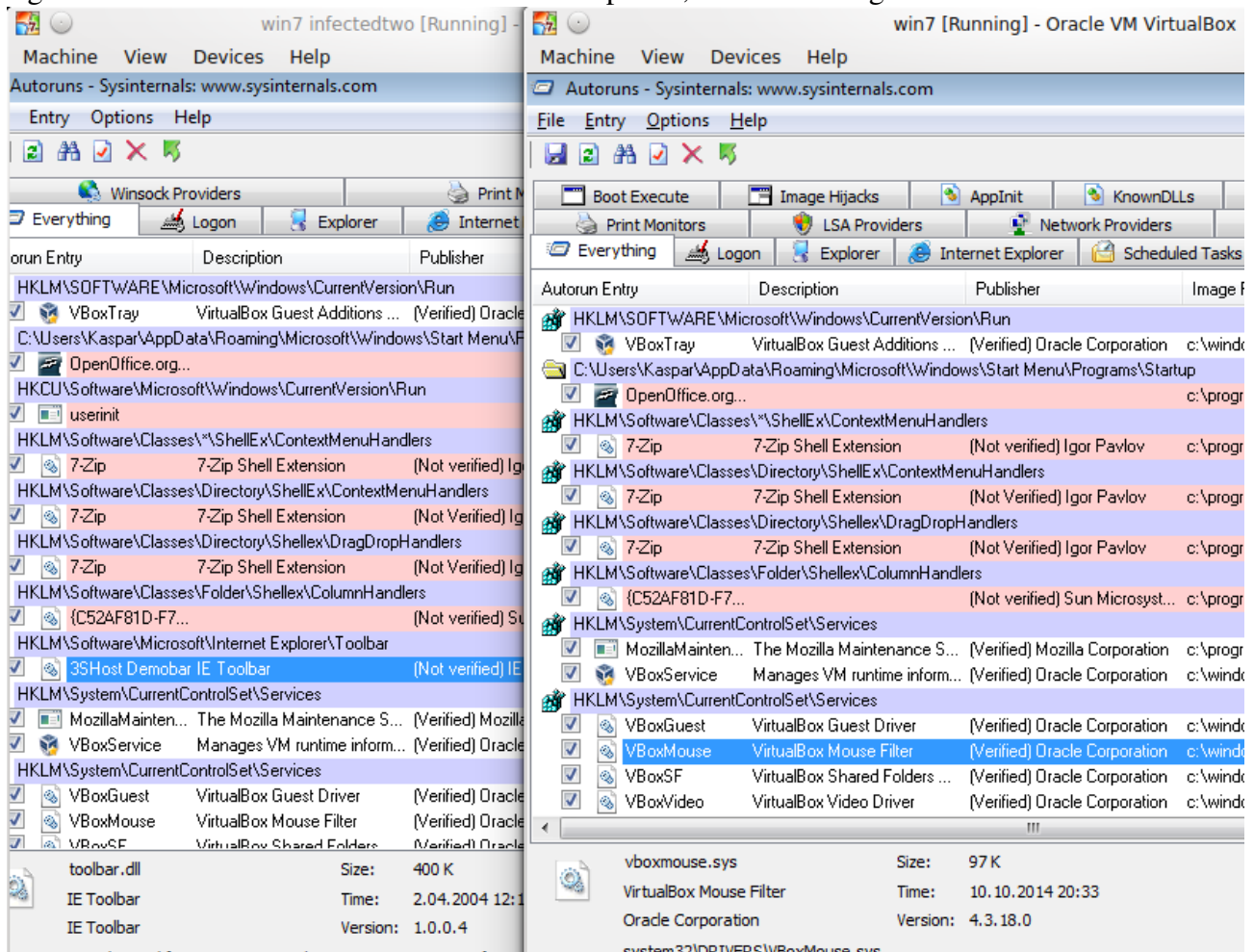
# Malware2 lab2

Chen Zhuge IVC132116

## 1. Finding Malware

### 1.1 Finding malware by using Autoruns.

Do cross-check between Win7 and Win7infectedtwo images, using Autoruns. Check Verify code signatures and Hide Microsoft entries in Filter Options, as shown in figure.



As result, 2 auto run entries are suspicious:

1) userinit, under HKCU\Software\Microsoft\Windows\CurrentVersion\Run, PATH c:\users\Kaspar\AppData\Roaming\ntos.exe

2) 3SHost Demobar, under HKLM\Software\Microsoft\Internet Explorer\Toolbar, PATH c:\program files\3shost demobar\toolbar.dll

### 1.2 Finding malware by using Processexplorer and Processmonitor.

Check Virus Total and Verified Singer in columns. Do the virus total and signature check. Currently every process seems normal, as shown in figure.

Is: www.sysinternals.com [FrendlyGost\Kaspar]

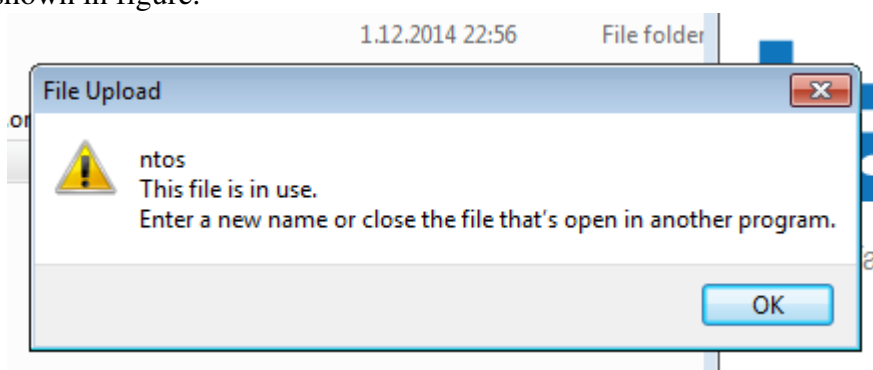
Find Users Help

	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer	VirusTotal
	95.98	0 K	24 K	0				
	0.24	44 K	520 K	4				
	1.06	0 K	0 K	n/a	Hardware Interrupts and DPCs			
		220 K	572 K	264				The system canno...
		1 156 K	2 452 K	340				The system canno...
		876 K	2 872 K	388				The system canno...
		4 044 K	4 964 K	484				The system canno...
		2 428 K	5 256 K	608	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...	0/55
	< 0.01	1 532 K	3 488 K	668				The system canno...
		2 176 K	4 516 K	732	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...	0/55
		12 796 K	9 852 K	820	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...	0/55
		14 944 K	13 720 K	1024				
		23 552 K	26 816 K	864	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...	0/55
	0.01	11 752 K	17 984 K	888	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...	0/55
	0.01	5 600 K	8 828 K	1080	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...	0/55
	0.03	11 420 K	9 996 K	1156	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...	0/55
		4 300 K	6 260 K	1296	Spooler SubSystem App	Microsoft Corporation	(Verified) Microsoft...	0/55
		9 428 K	6 904 K	1332	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...	0/55
		4 028 K	6 496 K	1572	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...	0/55
	0.01	15 584 K	9 536 K	1388	Microsoft Windows Search I...	Microsoft Corporation	(Verified) Microsoft...	0/55
		3 040 K	2 332 K	2372	Windows Media Player Netw...	Microsoft Corporation	(Verified) Microsoft...	0/55
		1 848 K	3 952 K	3900	Microsoft Software Protectio...	Microsoft Corporation	(Verified) Microsoft...	0/55
		112 240 K	17 400 K	3940	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft...	0/55
		2 592 K	5 968 K	500	Local Security Authority Proc...	Microsoft Corporation	(Verified) Microsoft...	0/56
		1 208 K	2 356 K	508				The system canno...
	0.28	1 280 K	3 904 K	400				The system canno...
		1 548 K	3 580 K	440				The system canno...
	0.51	39 028 K	38 148 K	1560	Windows Explorer	Microsoft Corporation	(Verified) Microsoft...	0/55
	1.87	10 252 K	18 660 K	3116	Sysinternals Process Explorer	Sysinternals - www.sysinter...	(Verified) Microsoft...	1/55
		9 388 K	15 884 K	2152				
		3 592 K	6 196 K	2184				

harge: 23.02% | Processes: 30 | Physical Usage: 29.15%

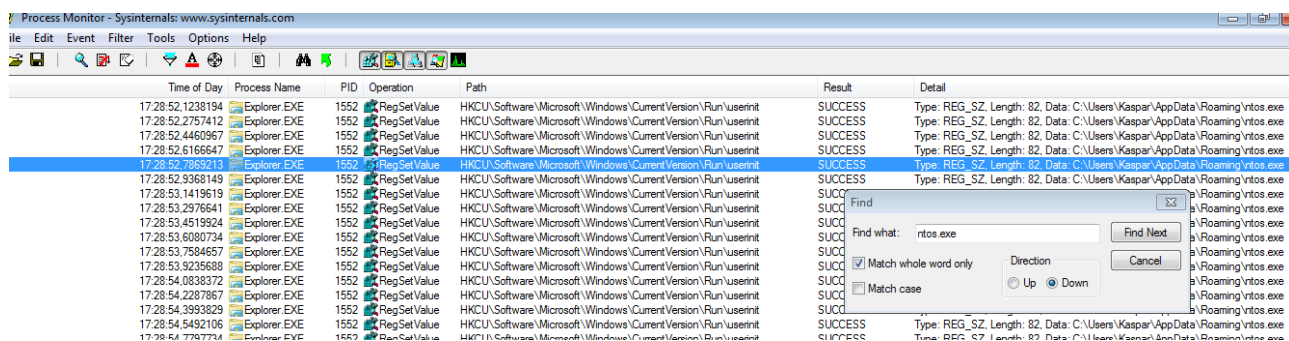
Maybe the malwares are not triggered yet.

Run `c:\users\Kaspar\appdata\roaming\ntos.exe` , but I was blocked by a dialog saying the application is already running. The same reason blocked me when I tried to submit `ntos.exe` to VirusTotal, as shown in figure.



Searched online, and `ntos.exe` was referred as a keylogger.

Try to find if `ntos.exe` is running in assistance of other processes, by using Processmonitor. Searching for `ntos.exe` in Find dialog. It's currently indeed running under explorer, as shown in figure.



However, when search 3SHost in Processmonitor, there is no sign of 3SHost. 3SHost is not running yet, I guess.

### 1.3 Finding malware by using Uninstall a program in Control Panel

As shown in figure, there are some suspicious software installed.

Program Name	Publisher	Installed On
3SHost Demobar		5.11.2014
7-Zip 9.20		4.11.2014
GoSave		5.11.2014
Mozilla Firefox 33.0.2 (x86 en-US)	Mozilla	4.11.2014
Mozilla Maintenance Service	Mozilla	4.11.2014
OpenOffice.org 3.1	OpenOffice.org	4.11.2014
Oracle VM VirtualBox Guest Additions 4.3.18	Oracle Corporation	4.11.2014

By submitting them into Virus Total, besides the already-known 3SHost Demobar, files under GoSave's folder were identified as malware. There was no sign of GoSave was running, according to Processexplorer and Processmonitor.

### 1.4 Finding malware by using Sigcheck.

My course mate Zhenyu Wu told me that another tool called Sigcheck is useful in finding malware. By running sigcheck -e -u -vr -s C:\, every executable, unsigned image will be submitted to Virus Total. It took 4 hours to finish this process, and some malware that have never showed up in previous procedures were detected by sigcheck. The new malwares' information are listed as below:

*c:\Users\Kaspar\Documents\temp\svchost.exe:*

*Verified: Unsigned*

*Link date: 9:59 12.10.2004*

*Publisher: n/a*

*Description: CCProxy Microsoft MFC Application*

*Product: CCProxy Application*

*Prod version: 2, 0, 0, 1*

*File version: 2, 0, 0, 1*

*MachineType: 32-bit*

*VT detection: 31/55*

*VT link: <https://www.virustotal.com/file/f2d3f793ad15d2ea40ebfdc431f3cbf4d436bcdbe6a4fd12c2088a9368b7357/analysis/>*

*c:\Users\Kaspar\Downloads\75WGsU05fiX4hx.exe:*

*Verified: Unsigned*  
*Link date: 18:27 18.11.2010*  
*Publisher: Igor Pavlov*  
*Description: 7z Setup SFX*  
*Product: 7-Zip*  
*Prod version: 9.20*  
*File version: 9.20*  
*MachineType: 32-bit*  
*VT detection: 34/55*  
*VT link: <https://www.virustotal.com/file/9526f11502ef2b21688b50ee4576896388da0f051a1e559f092c12d4da3404e3/analysis/>*

## 1.5 Summay

So far, there are 5 malwares that were detected.


c:\users\Kaspar\appdata\roaming\ntos.exe  
c:\program files\ 3shost demobar\toolbar.dll  
c:\program files\GoSave  
c:\Users\Kaspar\Documents\temp\svchost.exe  
c:\Users\Kaspar\Downloads\75WGsU05fiX4hx.exe

## 2. Removing malwares

### 2.1 Removing c:\users\Kaspar\appdata\roaming\ntos.exe

As it is running under explorer, in Processexplorer, kill the explorer.exe process.

Run cmd inside Processexplorer, force delete the file ntos.exe . The file was deleted, as shown in the figure.



```
C:\Windows\system32>del/f/s/q C:\Users\Kaspar\AppData\Roaming\ntos.exe
Deleted file - C:\Users\Kaspar\AppData\Roaming\ntos.exe
C:\Windows\system32>
```

In Autoruns, uncheck the box before ntos.exe , and delete the entry.

### 2.2 Removing c:\program files\ 3shost demobar\toolbar.dll

In Autoruns, uncheck the box before toolbar.dll .

In Control Panel, uninstall the program.

Delete the folder under c:\program files\ .

### 2.3 Removing c:\program files\GoSave

In Control Panel, uninstall the program.

Delete the folder under c:\program files\ .

### 2.4 Removing c:\Users\Kaspar\Documents\temp\svchost.exe

Delete the file.

### 2.5 Removing c:\Users\Kaspar\Downloads\75WGsU05fiX4hx.exe

Delete the file.