Analysis Report

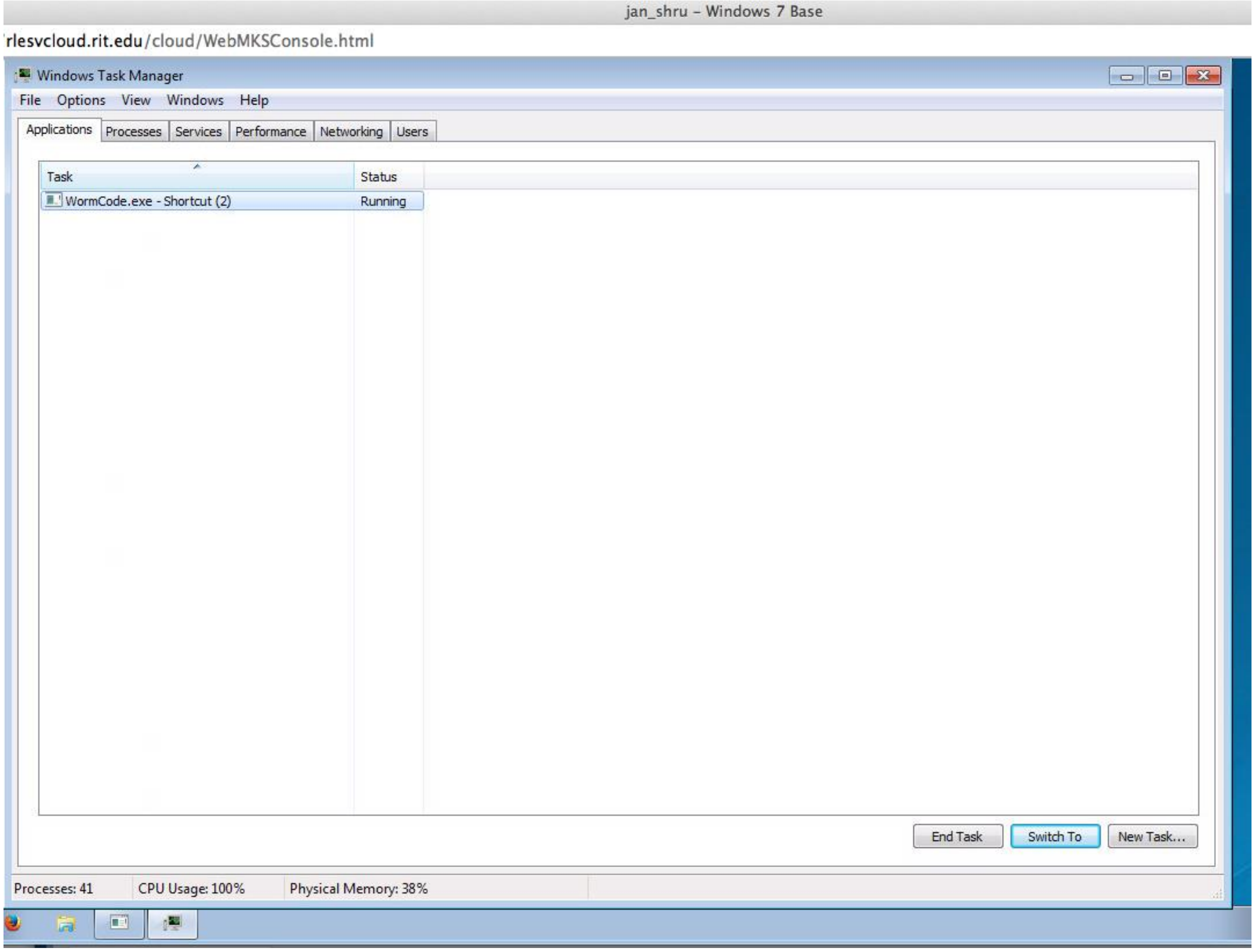
by

Team 6 (Dhivya Govindarajan, Sushant Murdeshwar, Ashish Pandit)

This report is the analysis report of **Team 7** malware (Janani Neelamekam, Shruthi Prakash). The malware identified is a Worm which replicates itself by creating 1000 NewFolders in Program Files folder and it also corrupts the files downloaded in the downloads folder. The following section provides the detailed analysis performed to detect the malware.

1. When we restarted the VM, we observed that a **console window** shortcut named 'WormCode.exe' **was open on desktop**. This console window seemed unusual, so we went to the task manager to see which processes are running and the CPU usage.

2. In the **Task Manager** under the **Applications** section, we saw that there was just one application running i.e. 'WormCode.exe' as shown in the figure below. So, this observation helped us to narrow down our attention to 'Wormcode.exe'.

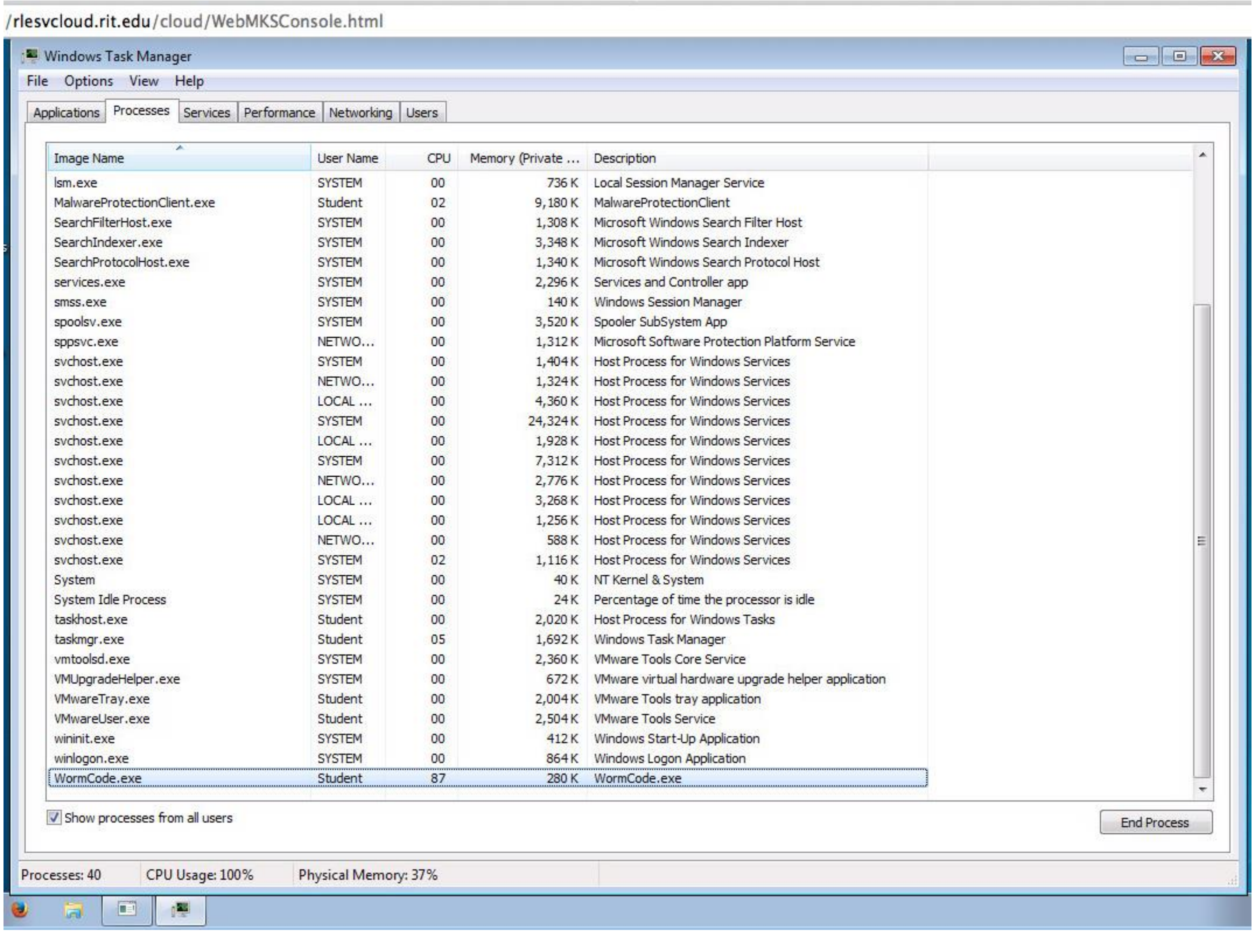


Task	Status
WormCode.exe - Shortcut (2)	Running

Processes: 41 CPU Usage: 100% Physical Memory: 38%

Figure 1 : Applications running in Task Manager

3. Then, we further checked the **Processes section** to see which processes were open and running; and how much percentage of CPU usage each process was using. We found out that ‘WormCode.exe’ was using significant amount of resources. As shown in the figure below, ‘Wormcode.exe’ consumes CPU usage of 87%. All other resources were consuming less amount of CPU usage and they were mostly the system files of windows. This observation further helped us to conclude that the malware is ‘WormCode.exe’.



/rlesvcloud.rit.edu/cloud/WebMKSConsole.html

Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users

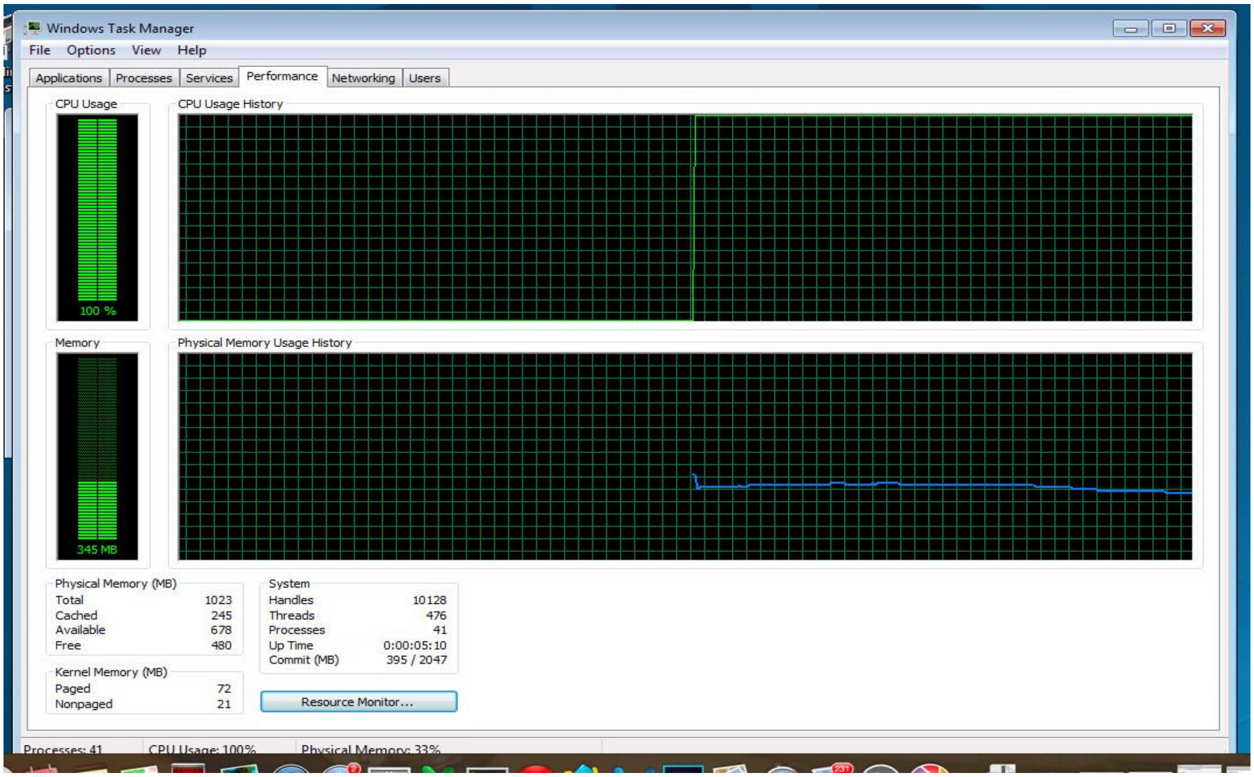
Image Name	User Name	CPU	Memory (Private ...	Description
lsm.exe	SYSTEM	00	736 K	Local Session Manager Service
MalwareProtectionClient.exe	Student	02	9,180 K	MalwareProtectionClient
SearchFilterHost.exe	SYSTEM	00	1,308 K	Microsoft Windows Search Filter Host
SearchIndexer.exe	SYSTEM	00	3,348 K	Microsoft Windows Search Indexer
SearchProtocolHost.exe	SYSTEM	00	1,340 K	Microsoft Windows Search Protocol Host
services.exe	SYSTEM	00	2,296 K	Services and Controller app
smss.exe	SYSTEM	00	140 K	Windows Session Manager
spoolsv.exe	SYSTEM	00	3,520 K	Spooler SubSystem App
sppsvc.exe	NETWO...	00	1,312 K	Microsoft Software Protection Platform Service
svchost.exe	SYSTEM	00	1,404 K	Host Process for Windows Services
svchost.exe	NETWO...	00	1,324 K	Host Process for Windows Services
svchost.exe	LOCAL ...	00	4,360 K	Host Process for Windows Services
svchost.exe	SYSTEM	00	24,324 K	Host Process for Windows Services
svchost.exe	LOCAL ...	00	1,928 K	Host Process for Windows Services
svchost.exe	SYSTEM	00	7,312 K	Host Process for Windows Services
svchost.exe	NETWO...	00	2,776 K	Host Process for Windows Services
svchost.exe	LOCAL ...	00	3,268 K	Host Process for Windows Services
svchost.exe	LOCAL ...	00	1,256 K	Host Process for Windows Services
svchost.exe	NETWO...	00	588 K	Host Process for Windows Services
svchost.exe	SYSTEM	02	1,116 K	Host Process for Windows Services
System	SYSTEM	00	40 K	NT Kernel & System
System Idle Process	SYSTEM	00	24 K	Percentage of time the processor is idle
taskhost.exe	Student	00	2,020 K	Host Process for Windows Tasks
taskmgr.exe	Student	05	1,692 K	Windows Task Manager
vmtoolsd.exe	SYSTEM	00	2,360 K	VMware Tools Core Service
VMUpgradeHelper.exe	SYSTEM	00	672 K	VMware virtual hardware upgrade helper application
VMwareTray.exe	Student	00	2,004 K	VMware Tools tray application
VMwareUser.exe	Student	00	2,504 K	VMware Tools Service
wininit.exe	SYSTEM	00	412 K	Windows Start-Up Application
winlogon.exe	SYSTEM	00	864 K	Windows Logon Application
WormCode.exe	Student	87	280 K	WormCode.exe

☑ Show processes from all users

Processes: 40 CPU Usage: 100% Physical Memory: 37%

Figure 2 : Processes running in Task Manager

4. We continued our analysis by checking the **Performance section** in the task manager. The Performance section showed that the CPU usage was 100% as shown below. We also observed that the CPU spike remains constant at 100%. This is because the ‘WormCode.exe’ application is continuously running in the system and consuming the resources.



Physical Memory (MB)	
Total	1023
Cached	245
Available	678
Free	480

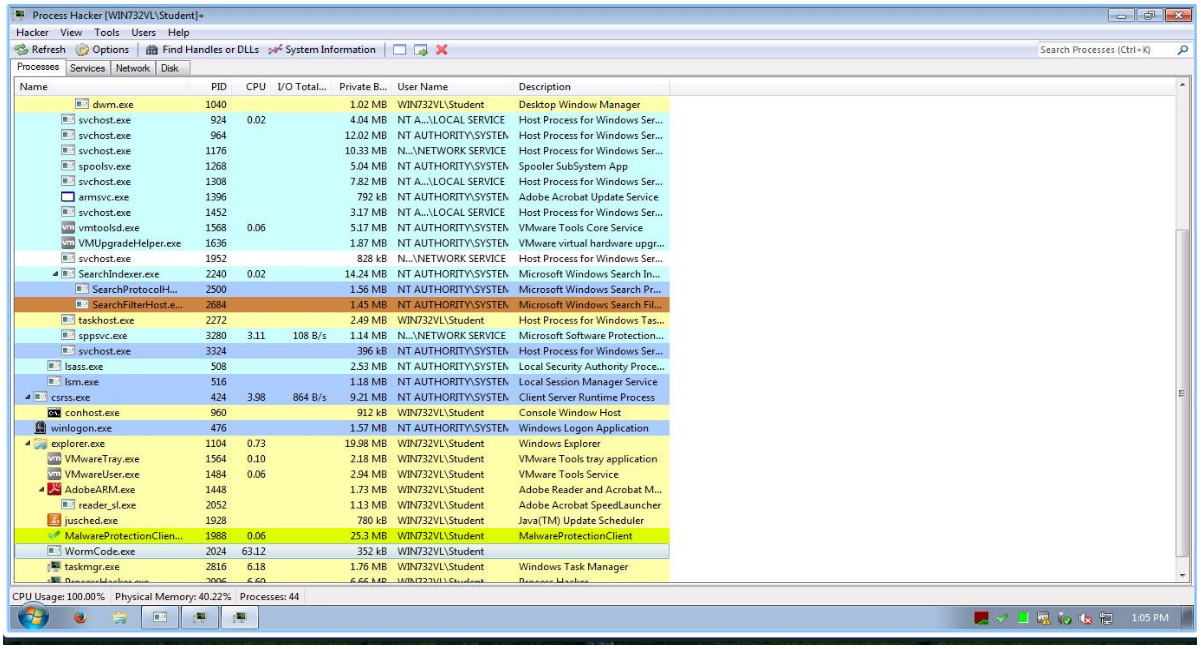
Kernel Memory (MB)	
Paged	72
Nonpaged	21

System	
Handles	10128
Threads	476
Processes	41
Up Time	0:00:05:10
Commit (MB)	395 / 2047

Processes: 41 CPU Usage: 100% Physical Memory: 33%

Figure 3 : CPU usage of the system

5. We then used the **Process Hacker tool** to confirm that ‘WormCode.exe’ was doing something malicious because of which it was consuming significant amount of resources. We then traced the location of the ‘WormCode.exe’ using the Process Hacker tool as shown below.

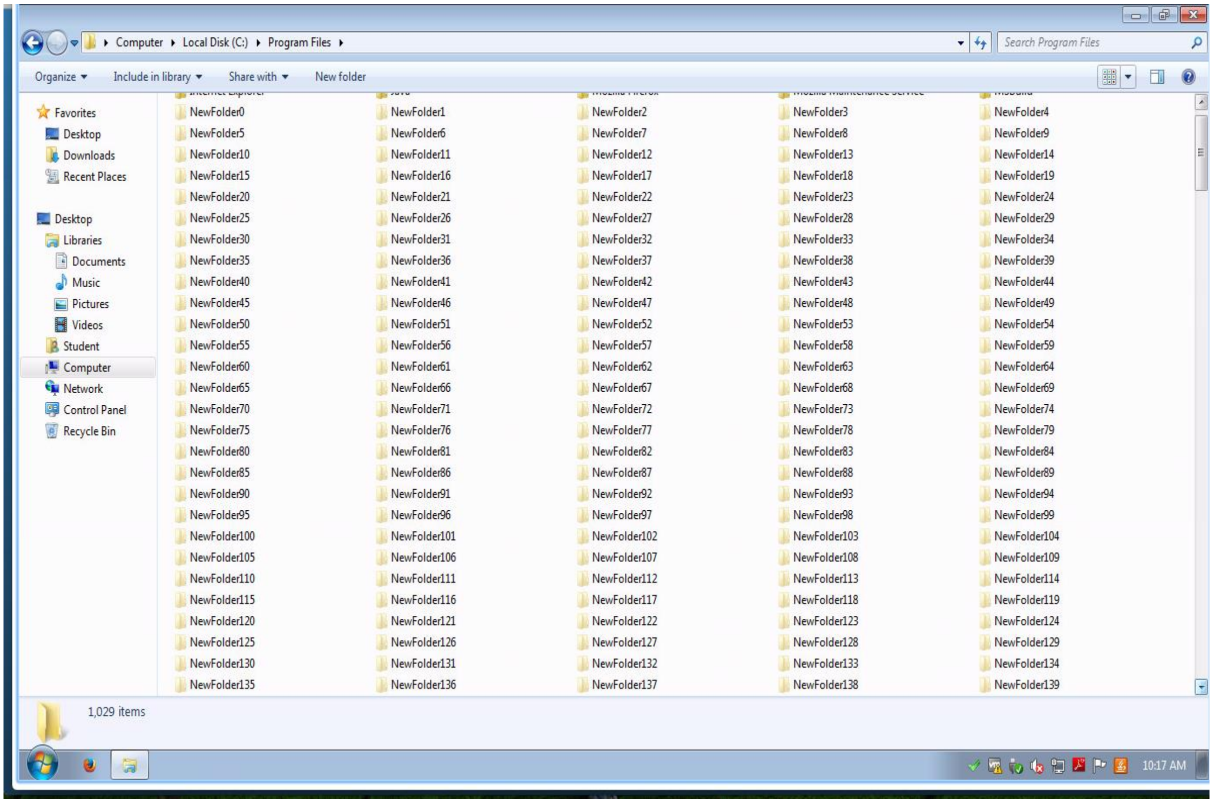

Process Hacker [WIN732VL\Student]+
Hacker View Tools Users Help
Refresh Options Find Handles or DLLs System Information
Search Processes (Ctrl+K)
Processes Services Network Disk
1:05 PM

Name	PID	CPU	I/O Total...	Private B...	User Name	Description
dwm.exe	1040			1.02 MB	WIN732VL\Student	Desktop Window Manager
svchost.exe	924	0.02		4.04 MB	NT A...\LOCAL SERVICE	Host Process for Windows Ser...
svchost.exe	964			12.02 MB	NT AUTHORITY\SYSTEN	Host Process for Windows Ser...
svchost.exe	1176			10.33 MB	N...\NETWORK SERVICE	Host Process for Windows Ser...
spoolsv.exe	1268			5.04 MB	NT AUTHORITY\SYSTEN	Spooler SubSystem App
svchost.exe	1308			7.82 MB	NT A...\LOCAL SERVICE	Host Process for Windows Ser...
armsvc.exe	1396			792 kB	NT AUTHORITY\SYSTEN	Adobe Acrobat Update Service
svchost.exe	1452			3.17 MB	NT A...\LOCAL SERVICE	Host Process for Windows Ser...
vmtoolsd.exe	1568	0.06		5.17 MB	NT AUTHORITY\SYSTEN	VMware Tools Core Service
VMUpgradeHelper.exe	1636			1.87 MB	NT AUTHORITY\SYSTEN	VMware virtual hardware upgr...
svchost.exe	1952			828 kB	N...\NETWORK SERVICE	Host Process for Windows Ser...
SearchIndexer.exe	2240	0.02		14.24 MB	NT AUTHORITY\SYSTEN	Microsoft Windows Search In...
SearchProtocolH...	2500			1.56 MB	NT AUTHORITY\SYSTEN	Microsoft Windows Search Pr...
SearchFilterHost.e...	2684			1.45 MB	NT AUTHORITY\SYSTEN	Microsoft Windows Search Fil...
taskhost.exe	2272			2.49 MB	WIN732VL\Student	Host Process for Windows Tas...
sppsvc.exe	3280	3.11	108 B/s	1.14 MB	N...\NETWORK SERVICE	Microsoft Software Protection...
svchost.exe	3324			396 kB	NT AUTHORITY\SYSTEN	Host Process for Windows Ser...
lsass.exe	508			2.53 MB	NT AUTHORITY\SYSTEN	Local Security Authority Proce...
lsm.exe	516			1.18 MB	NT AUTHORITY\SYSTEN	Local Session Manager Service
csrss.exe	424	3.98	864 B/s	9.21 MB	NT AUTHORITY\SYSTEN	Client Server Runtime Process
conhost.exe	960			912 kB	WIN732VL\Student	Console Window Host
winlogon.exe	476			1.57 MB	NT AUTHORITY\SYSTEN	Windows Logon Application
explorer.exe	1104	0.73		19.98 MB	WIN732VL\Student	Windows Explorer
VMwareTray.exe	1564	0.10		2.18 MB	WIN732VL\Student	VMware Tools tray application
VMwareUser.exe	1484	0.06		2.94 MB	WIN732VL\Student	VMware Tools Service
AdobeARM.exe	1448			1.73 MB	WIN732VL\Student	Adobe Reader and Acrobat M...
reader_sl.exe	2052			1.13 MB	WIN732VL\Student	Adobe Acrobat SpeedLauncher
jusched.exe	1928			780 kB	WIN732VL\Student	Java(TM) Update Scheduler
MalwareProtectionClien...	1988	0.06		25.3 MB	WIN732VL\Student	MalwareProtectionClient
WormCode.exe	2024	63.12		352 kB	WIN732VL\Student	
taskmgr.exe	2816	6.18		1.76 MB	WIN732VL\Student	Windows Task Manager
ProcessHacker.exe	2096	6.60		6.66 MB	WIN732VL\Student	Process Hacker

CPU Usage: 100.00% Physical Memory: 40.22% Processes: 44

Figure 4 : Identified WormCode.exe using the Process Hacker Tool

6. We tried to search the different folders in the C:\ drive to check if the ‘WormCode.exe’ has made any changes to any files. We then found that this worm replicated itself by creating **NewFolder in ‘Programs Files’** folder. It created 1000 NewFolder as shown below.



NewFolder0	NewFolder1	NewFolder2	NewFolder3	NewFolder4
NewFolder5	NewFolder6	NewFolder7	NewFolder8	NewFolder9
NewFolder10	NewFolder11	NewFolder12	NewFolder13	NewFolder14
NewFolder15	NewFolder16	NewFolder17	NewFolder18	NewFolder19
NewFolder20	NewFolder21	NewFolder22	NewFolder23	NewFolder24
NewFolder25	NewFolder26	NewFolder27	NewFolder28	NewFolder29
NewFolder30	NewFolder31	NewFolder32	NewFolder33	NewFolder34
NewFolder35	NewFolder36	NewFolder37	NewFolder38	NewFolder39
NewFolder40	NewFolder41	NewFolder42	NewFolder43	NewFolder44
NewFolder45	NewFolder46	NewFolder47	NewFolder48	NewFolder49
NewFolder50	NewFolder51	NewFolder52	NewFolder53	NewFolder54
NewFolder55	NewFolder56	NewFolder57	NewFolder58	NewFolder59
NewFolder60	NewFolder61	NewFolder62	NewFolder63	NewFolder64
NewFolder65	NewFolder66	NewFolder67	NewFolder68	NewFolder69
NewFolder70	NewFolder71	NewFolder72	NewFolder73	NewFolder74
NewFolder75	NewFolder76	NewFolder77	NewFolder78	NewFolder79
NewFolder80	NewFolder81	NewFolder82	NewFolder83	NewFolder84
NewFolder85	NewFolder86	NewFolder87	NewFolder88	NewFolder89
NewFolder90	NewFolder91	NewFolder92	NewFolder93	NewFolder94
NewFolder95	NewFolder96	NewFolder97	NewFolder98	NewFolder99
NewFolder100	NewFolder101	NewFolder102	NewFolder103	NewFolder104
NewFolder105	NewFolder106	NewFolder107	NewFolder108	NewFolder109
NewFolder110	NewFolder111	NewFolder112	NewFolder113	NewFolder114
NewFolder115	NewFolder116	NewFolder117	NewFolder118	NewFolder119
NewFolder120	NewFolder121	NewFolder122	NewFolder123	NewFolder124
NewFolder125	NewFolder126	NewFolder127	NewFolder128	NewFolder129
NewFolder130	NewFolder131	NewFolder132	NewFolder133	NewFolder134
NewFolder135	NewFolder136	NewFolder137	NewFolder138	NewFolder139

1,029 items

Figure 5 : Identified the New Folders created

7. We also searched the downloads folder and found that we had downloaded some files like the ProcessHacker, TCPView initially. When we checked these installation files again, we found that these installation files were already corrupted by the worm. Some of the image files in the download folder were also corrupted by the malware.

<u>Conclusion</u>

Based on the observations that we found, we could conclude that the malware was a worm. This is because, worms normally have the characteristics to replicate itself and corrupt some of the files in the system.