|  |  |
| --- | --- |
| Student REGNO : 16BCE1053 | Student FIRSTNAME LASTNAME : RAHUL GUHA |

**Dynamic Malware Analysis Report**

Name of the Malware file: -→ VIRUS

**MD5 HASH :** → 8FB7A3B60B8A9BFC328AFB58D4A235A5

**SHA HASH** : → E762E16E6B693A5CA4A3FD0C05EEB0EF69EDCF74

**File Size** : → 559.71 kB

**File Info** → Microsoft Visual C++ 8

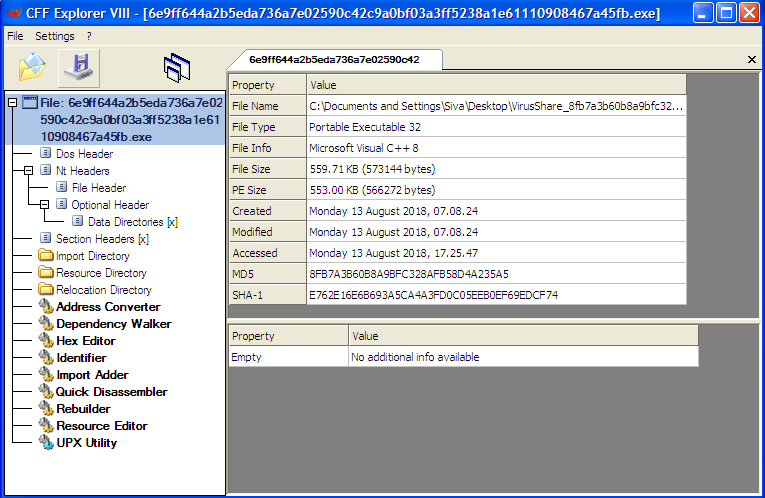
**File Type** → Portable Executable 32

**PE Size** : → 553.00 KB

**Company Name** : → NIL

**Legal Copyright :** → NIL

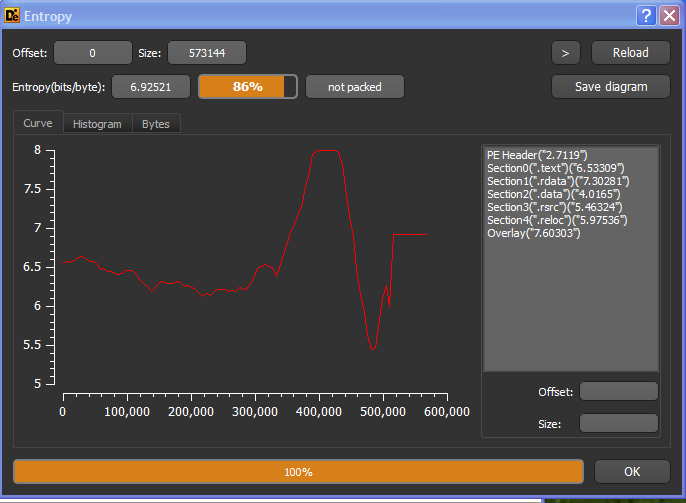
**FileName :** → Settings\Siva\Desktop\VirusShare\_8fb7a3b60b8a9bfc328afb58d4a235a5\6e9ff644a2b5eda736a7e02590c42c9a0bf03a3ff5238a1e61110908467a45fb.exe



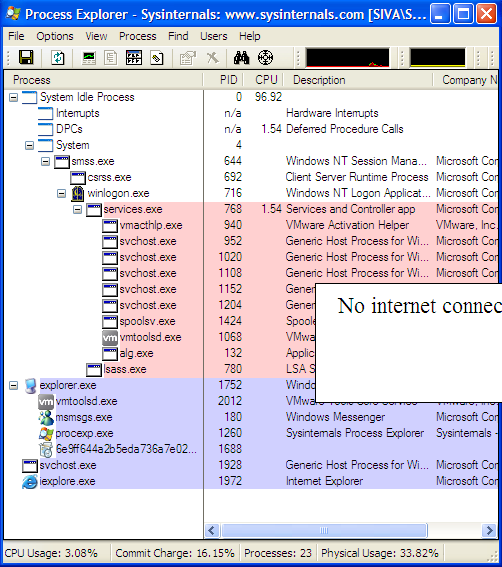
**UPX Utility** → NIL

**Entropy value** → 6.92521

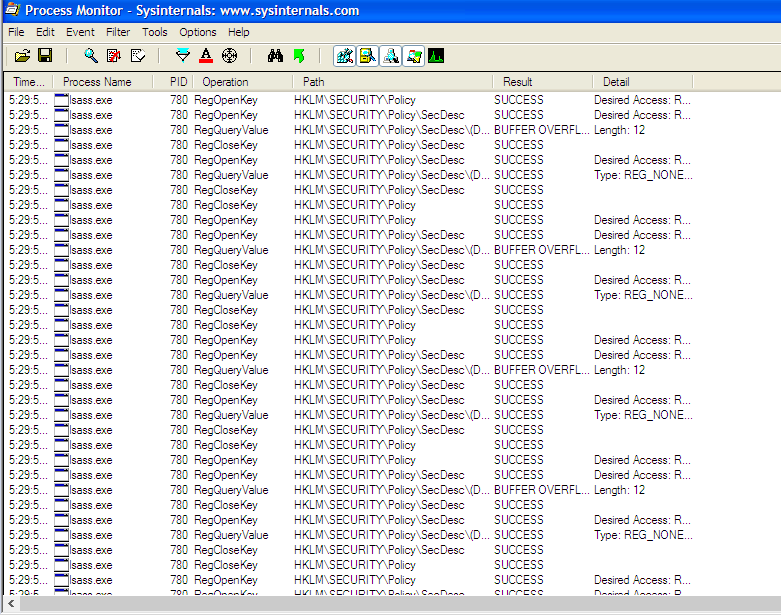
**Entropy Percentage** → 86%



**Any new Processes created** : -→NIL

**If yes, How many Processes are newly created ?** : -→ NIL

**Proc explorer running or closed**  -→ RUNNING



**Regshot Output :**

* **Keys Added: 2**
* **Keys deleted: NIL**
* **Values added: 5**
* **Values Modified: 9**
* **Values Deleted: NIL**
* **Files Added: 8**
* **Files Deleted: 1**
* **Files Modified: 7**
* **Folders added: 6**
* **Total Changes: 38**

**Whether the malware is trying to make network connections**: -→YES

**If yes, list the Websites/IPs/Domains that it is making connections**: -→

pyminifakeDNS:: dom.query. 60 IN A 192.168.116.1

Respuesta: remoteback.no-ip.biz. -> 192.168.116.1

Respuesta: dlg-configs.buzzrin.de. -> 192.168.116.1

Respuesta: mjed10.no-ip.info. -> 192.168.116.1

Respuesta: dlg-messages.buzzrin.de. -> 192.168.116.1

Respuesta: dlg-messages.buzzrin.de. -> 192.168.116.1

Respuesta: dlg-configs.buzzrin.de. -> 192.168.116.1

Respuesta: dlg-messages.buzzrin.de. -> 192.168.116.1

Respuesta: 1.116.168.192.in-addr.arpa. -> 192.168.116.1

Respuesta: 1.119.168.192.in-addr.arpa. -> 192.168.116.1

Respuesta: 1.56.168.192.in-addr.arpa. -> 192.168.116.1

Respuesta: 250.255.255.239.in-addr.arpa. -> 192.168.116.1

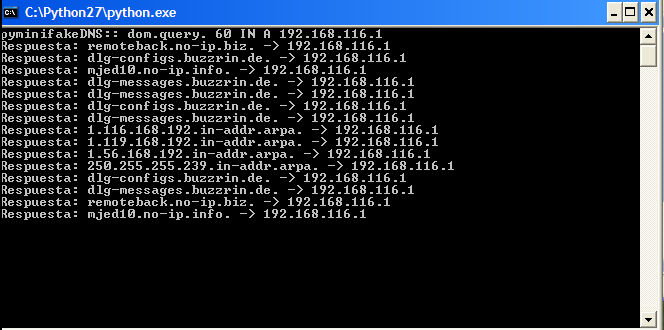
Respuesta: dlg-configs.buzzrin.de. -> 192.168.116.1

Respuesta: dlg-messages.buzzrin.de. -> 192.168.116.1

Respuesta: remoteback.no-ip.biz. -> 192.168.116.1

Respuesta: mjed10.no-ip.info. -> 192.168.116.1

**Total number of connections the malware is making:** -→ 16

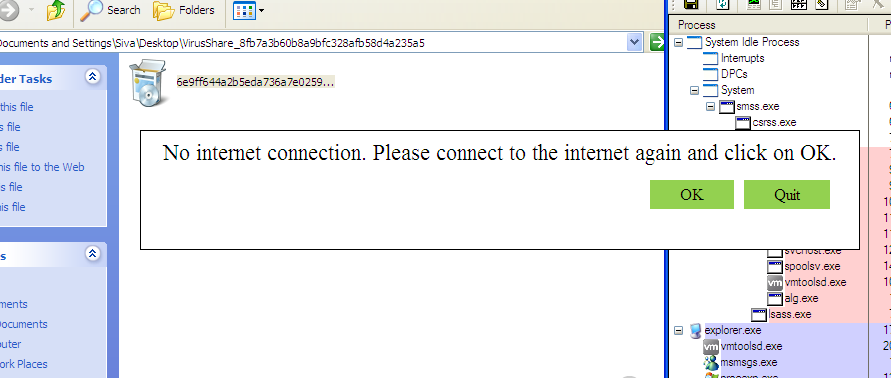


**Type of the Malware**: VIRUS

**List some unique behavior of the malware** : → Gives notification requesting for network connection. Notification cannot be minimized. all other filles moved behind the notification box.

Virus tries to make network connections to export info.

it is making changes in internal files of the system.



**Suggest some removal procedures apart from VM Snapshots** : → Deleting source file and all affected files.

scan the computer using antivirus software and use antivirus toold to clean.