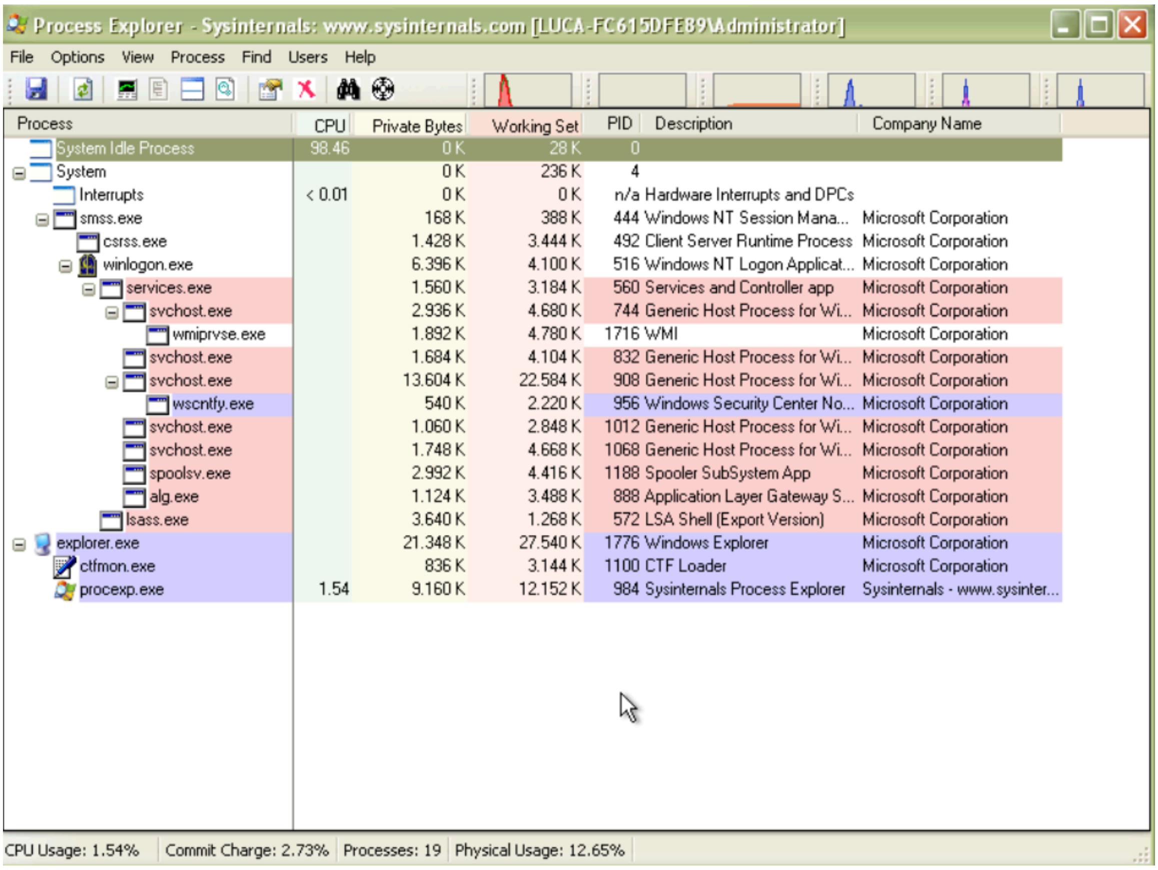
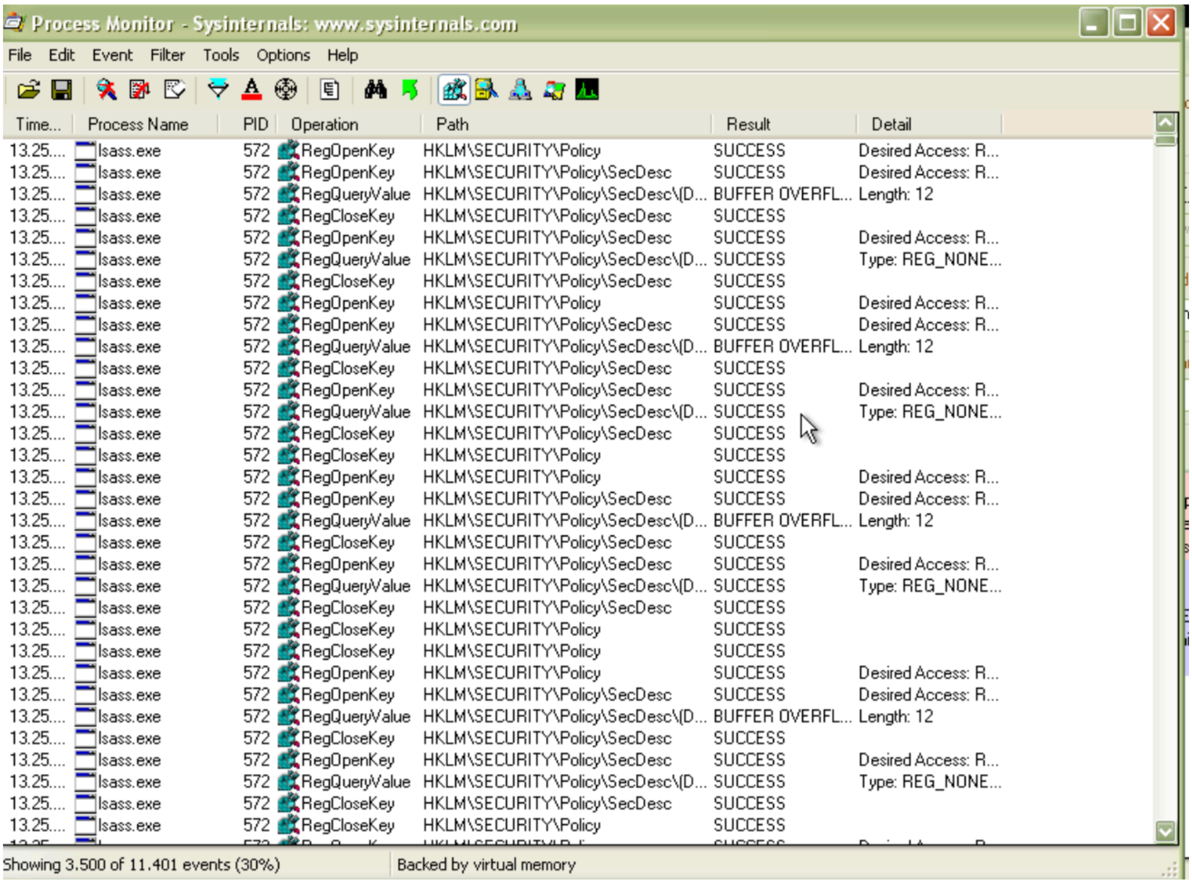
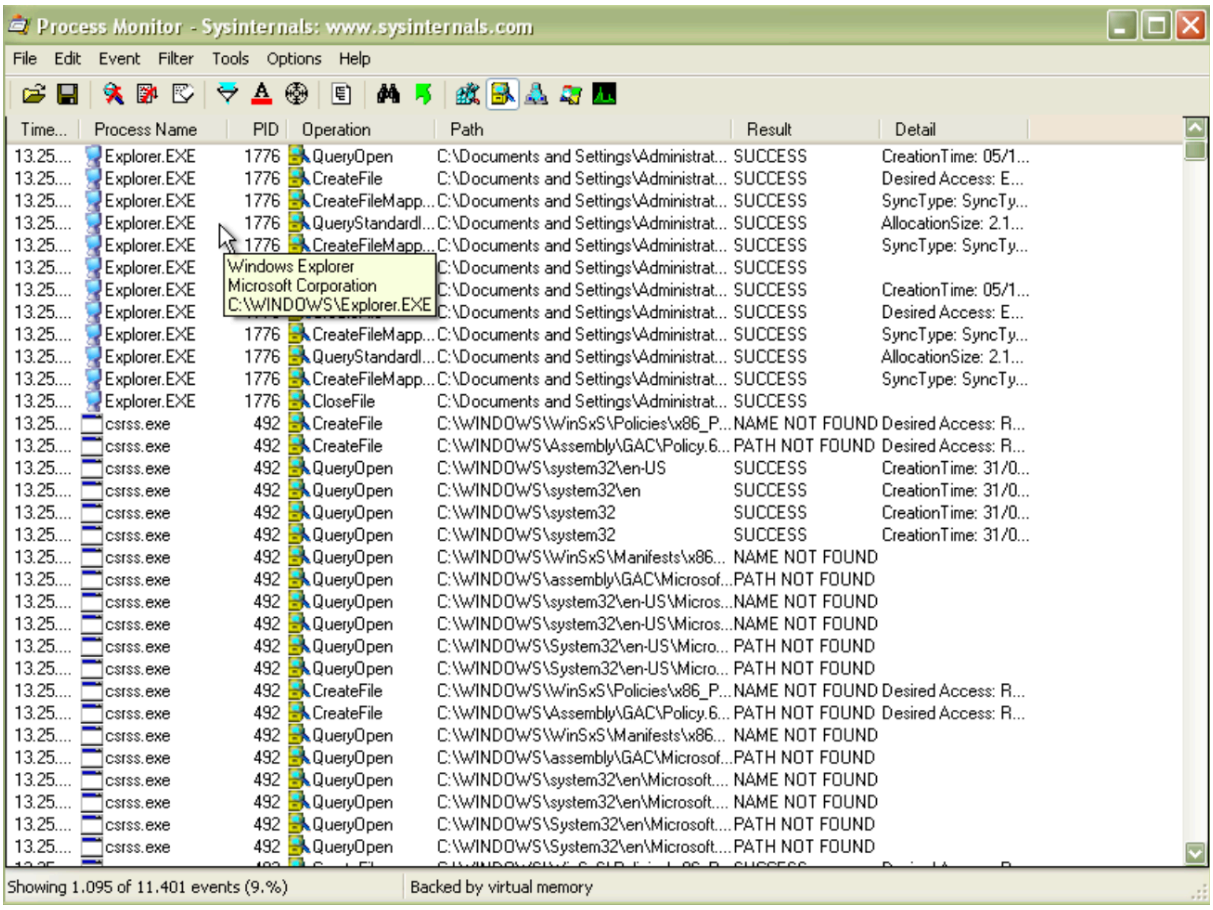
ANALISI DINAMICA BASICA

COME PRIMA COSA SIAMO ANDATI A MONITORARE I PROCESSI PRIMA DELL' AVVIO DEL MALWARE COME IN FOTO SOTTO







DOPO ABBIAMO FATTO USATO IL TOOL REGSHOT PER PARAGONARE DUE ISTANTANEE DELLE CHIAVI DI REGISTRO.

IL PRIMO SHOT E' STATO EFFETTUATO PRIMA DI AVVIARE IL MALWARE MENTE IL SECONDO SHOT E' STATO EFFETTUATO DOPO L'AVVIO DEL MALWARE, DOPO AVER FATTO TUTTO CIO' ANDIAMO A COMPARE I DUE FILE IL RISULATO VIENE MOSTRATO NELLE FOTO QUI DI SEGUITO

~res-x86.txt - Notepad

File Edit Format View Help

```
-----------------------------------
Valore modificato:17
-----------------------------------
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  8B 35 C2 04 BE 18 B6 74 2F 8B 99 8C 47 CE 26 2E F7 64 9C 7C 5B 70 FD 18 92 5F 0E 52 55 8D D3 A8 A7 4B FE B7
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  DC AF EC A1 E9 92 BD BB E1 D7 0E 5A B6 AB 6B EA 81 57 15 12 44 04 BC AE 62 2E 90 C5 BD 80 0C 48 C4 37 BA 24
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*\MRUList: "ajihgfedcb"
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*\MRUList: "bajihgfedc"
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*\b: "C:\Documents and Settings\Adm
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*\b: "C:\Documents and Settings\Adm
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\hivu\MRUList: "cba"
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\hivu\MRUList: "dcba"
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage\ProgramsCache:  09 00 00 00 0B 00 56 00 00 00
```


```
 00 6F 00 72 00 65 00 72 00 5C 00 69 00 65 00 78 00 70 00 6C 00 6F 00 72 00 65 00 2E 00 65 00 78 00 65 00 00 00 00 00 1C 00 00 00 01 DC 00 00 00 DA 00 32 C
20 00 41 00 73 00 73 00 69 00 73 00 74 00 61 00 6E 00 63 00 65 00 2E 00 6C 00 6E 00 6B 00 00 00 40 43 3A 5C 57 49 4E 44 4F 57 53 5C 73 79 73 74 65 6D 33 32
0 00 4D 00 65 00 64 00 69 00 61 00 20 00 50 00 6C 00 61 00 79 00 65 00 72 00 5C 00 77 00 6D 00 70 00 6C 00 61 00 79 00 65 00 72 00 2E 00 65 00 78 00 65 00
 33 32 2E 64 6C 6C 2C 2D 32 32 30 31 37 00 1C 00 66 00 00 00 0B 00 EF BE 00 00 00 00 00 00 00 00 43 00 3A 00 5C 00 50 00 72 00 6F 00 67 00 72 00 61 00 6D C
00 4E 6F 74 65 70 61 64 2E 6C 6E 6B 00 42 00 03 00 04 00 EF BE 1F 55 61 8C 1F 55 61 8C 14 00 2C 00 4E 00 6F 00 74 00 65 00 70 00 61 00 64 00 2E 00 6C 00 6E
0 0B 00 EF BE 00 00 00 00 00 00 00 00 00 00 00 00 1C 00 00 00 01 C0 00 00 00 BE 00 32 00 EF 05 00 00 1F 55 97 8B 20 00 53 59 4E 43 48 52 7E 31 2E 4C 4E 4B
 75 72 73 74 61 72 74 2E 65 78 65 2C 2D 31 00 1C 00 5C 00 00 00 0B 00 EF BE 00 00 00 00 00 00 00 00 25 00 53 00 79 00 73 00 74 00 65 00 6D 00 52 00 6F 00 6
03 00 04 00 EF BE 1F 55 61 8C 1F 55 6C 8C 14 00 26 00 50 00 72 00 6F 00 67 00 72 00 61 00 6D 00 73 00 00 00 40 73 68 65 6C 6C 33 32 2E 64 6C 6C 2C 2D 32 31
E 64 6C 6C 2C 2D 32 32 30 34 31 00 1C 00 58 00 00 00 0B 00 EF BE 00 00 00 00 00 00 00 00 25 00 53 00 79 00 73 00 74 00 65 00 6D 00 52 00 6F 00 6F 00 74 00
 04 00 EF BE 1F 55 61 8C 1F 55 61 8C 14 00 42 00 4F 00 6E 00 2D 00 53 00 63 00 72 00 65 00 65 00 6E 00 20 00 4B 00 65 00 79 00 62 00 6F 00 61 00 72 00 64 C
6D 00 33 00 32 00 5C 00 75 00 74 00 69 00 6C 00 6D 00 61 00 6E 00 2E 00 65 00 78 00 65 00 00 00 00 00 1C 00 00 00 00 0E 01 00 00 54 00 31 00 00 00 00 00 1F
9 4E 44 4F 57 7E 31 2E 4C 4E 4B 00 00 48 00 03 00 04 00 EF BE 1F 55 61 8C 1F 55 6C 8C 14 00 00 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 20 00 4D 00 65
 33 55 07 57 14 00 2C 00 41 00 63 00 63 00 65 00 73 00 73 00 6F 00 72 00 69 00 65 00 73 00 00 00 40 73 68 65 6C 6C 33 32 2E 64 6C 6C 2C 2D 32 31 37 36 31 C
65 00 72 00 5C 00 69 00 65 00 78 00 70 00 6C 00 6F 00 72 00 65 00 2E 00 65 00 78 00 65 00 00 00 00 00 1C 00 00 00 02 16 00 02 00 00 00 00 00 01 FE 00 00 0C
E 4C 4E 4B 00 00 52 00 03 00 04 00 EF BE 1F 55 97 8B 1F 55 97 8B 14 00 3C 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 20 00 43 00 61 00 74 00 61 00 6C 00
 47 51 1F 55 4E 8B 14 00 26 00 50 00 72 00 6F 00 67 00 72 00 61 00 6D 00 73 00 00 00 40 73 68 65 6C 6C 33 32 2E 64 6C 6C 2C 2D 32 31 37 38 32 00 18 00 00 C
00 00 00 00 00 00 00 43 00 3A 00 5C 00 50 00 72 00 6F 00 67 00 72 00 61 00 6D 00 20 00 46 00 69 00 6C 00 65 00 73 00 5C 00 4D 00 53 00 4E 00 5C 00 4D 00 53
F 55 4E 8B 20 00 57 49 4E 44 4F 57 7E 32 2E 4C 4E 4B 00 00 70 00 03 00 04 00 EF BE 1F 55 4E 8B 1F 55 4E 8B 14 00 44 00 57 00 69 00 6E 00 64 00 6F 00 77 00
 55 28 8B 11 00 41 43 43 45 53 53 7E 31 00 00 2E 00 03 00 04 00 EF BE 1F 55 D9 8A 1F 55 49 8B 14 00 00 00 41 00 63 00 63 00 65 00 73 00 73 00 6F 00 72 00 6
2C 2D 32 32 30 35 34 00 18 00 58 00 00 00 0B 00 EF BE 00 00 00 00 00 00 00 00 25 00 53 00 79 00 73 00 74 00 65 00 6D 00 52 00 6F 00 6F 00 74 00 25 00 5C 0C
5 00 78 00 65 00 00 00 00 00 1C 00 00 00 01 DA 00 00 00 D8 00 32 00 6F 03 00 00 1F 55 0B 8B 20 00 57 6F 72 64 50 61 64 2E 6C 6E 6B 00 42 00 03 00 04 00 EF
 1F 55 28 8B 11 00 41 43 43 45 53 53 7E 31 00 00 2E 00 03 00 04 00 EF BE 1F 55 D9 8A 1F 55 49 8B 14 00 00 00 41 00 63 00 63 00 65 00 73 00 73 00 6F 00 72 C
7A 00 2E 00 65 00 78 00 65 00 00 00 00 00 1C 00 00 00 00 FC 00 00 00 54 00 31 00 00 00 00 00 1F 55 4E 8B 11 00 50 72 6F 67 72 61 6D 73 00 00 3C 00 03 00 04
0 65 00 72 00 54 00 65 00 72 00 6D 00 69 00 6E 00 61 00 6C 00 2E 00 6C 00 6E 00 6B 00 00 00 40 73 68 65 6C 6C 33 32 2E 64 6C 6C 2C 2D 32 32 30 33 31 00 1C
 6F 00 74 00 25 00 5C 00 65 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 00 2E 00 65 00 78 00 65 00 00 00 00 00 1C 00 00 00 01 E8 00 00 00 E6 00 32 00 68 06 C
00 77 00 20 00 43 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 69 00 6F 00 6E 00 20 00 57 00 69 00 7A 00 61 00 72 00 64 00 2E 00 6C 00 6E 00 6B 00 00 00 40 43 3A
```


~res-x86.txt - Notepad

File Edit Format View Help

```
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings:  46 00 00 00 3
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings:  46 00 00 00 3
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{2559A1F4-21D7-11D4-BDAF-00C04F60B9F0} {C
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{2559A1F4-21D7-11D4-BDAF-00C04F60B9F0} {C
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{2559A1F5-21D7-11D4-BDAF-00C04F60B9F0} {C
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{2559A1F5-21D7-11D4-BDAF-00C04F60B9F0} {C
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\Shell\Bags\1\Desktop\ColInfo:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\Shell\Bags\1\Desktop\ColInfo:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\Shell\Bags\1\Desktop\ItemPos1280x720(1):  00 00 00 00 00 00 00 00 00 00 00 00 0C
```

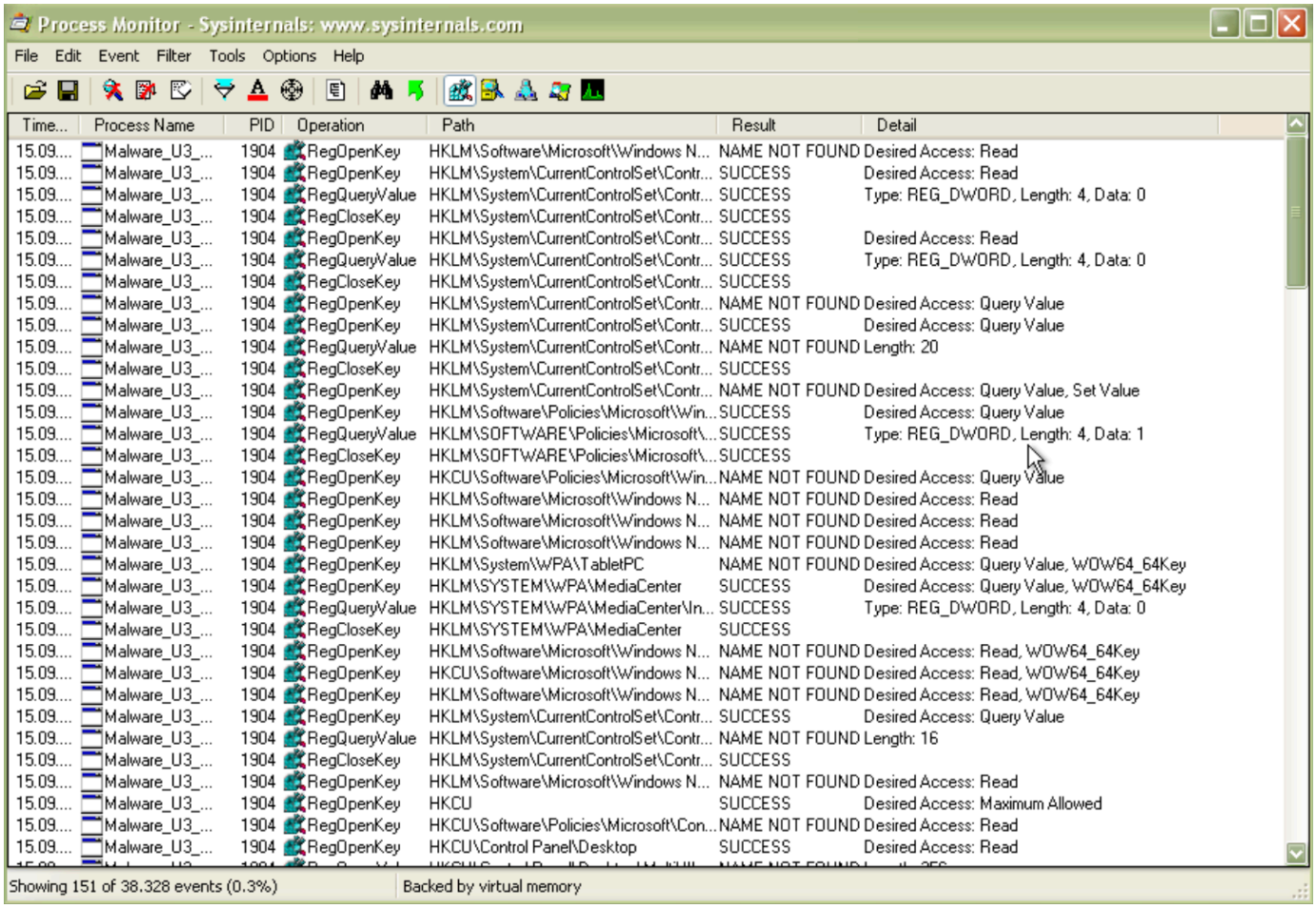

```
9 00 7A 00 69 00 6F 00 5F 00 50 00 72 00 61 00 74 00 69 00 63 00 6F 00 5F 00 55 00 33 00 5F 00 57 00 32 00 5F 00 4C 00 31 00 00 00 18 00 15 00 00 00 CA 01
 50 00 72 00 61 00 74 00 69 00 63 00 6F 00 5F 00 55 00 33 00 5F 00 57 00 33 00 5F 00 4C 00 32 00 00 00 18 00 60 00 00 00 4E 00 00 00 64 00 31 00 00 00 00 C
55 0C 5D 34 55 D4 96 14 00 00 00 6D 00 64 00 35 00 64 00 65 00 65 00 70 00 2D 00 34 00 2E 00 33 00 00 00 1A 00 60 00 00 00 7E 01 00 00 3C 00 31 00 00 00 0C
2 00 00 00 18 00 AB 00 00 00 02 00 00 00 4C 00 31 00 00 00 00 00 33 55 06 5D 10 00 50 52 4F 43 45 53 7E 32 00 00 34 00 03 00 04 00 EF BE 33 55 06 5D 34 55
 73 00 00 00 18 00 AB 00 00 00 32 01 00 00 52 00 31 00 00 00 00 00 33 55 0B 5D 10 00 53 59 53 49 4E 54 7E 31 00 00 3A 00 03 00 04 00 EF BE 33 55 07 5D 34 5
55 C4 8E 14 00 00 00 64 00 6F 00 77 00 6E 00 6C 00 6F 00 61 00 64 00 2E 00 65 00 78 00 65 00 00 00 1C 00 AB 00 00 00 16 02 00 00 54 00 32 00 92 02 00 00 34
4 55 C9 0D 20 00 57 49 52 45 53 48 7E 31 2E 4C 4E 4B 00 00 32 00 03 00 04 00 EF BE 34 55 C9 0D 34 55 45 98 14 00 00 00 57 00 69 00 72 00 65 00 73 00 68 00
```


```
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\Shell\Bags\1\Desktop\ItemPos1280x720(1):  00 00 00 00 00 00 00 00 00 00 00 00 0C
```


```
9 00 7A 00 69 00 6F 00 5F 00 50 00 72 00 61 00 74 00 69 00 63 00 6F 00 5F 00 55 00 33 00 5F 00 57 00 32 00 5F 00 4C 00 31 00 00 00 18 00 15 00 00 00 CA 01
 50 00 72 00 61 00 74 00 69 00 63 00 6F 00 5F 00 55 00 33 00 5F 00 57 00 33 00 5F 00 4C 00 32 00 00 00 18 00 60 00 00 00 4E 00 00 00 64 00 31 00 00 00 00 C
55 0C 5D 34 55 D4 96 14 00 00 00 6D 00 64 00 35 00 64 00 65 00 65 00 70 00 2D 00 34 00 2E 00 33 00 00 00 1A 00 15 00 00 00 4E 00 00 00 40 00 31 00 00 00 0C
E 00 31 00 00 00 00 00 33 55 06 5D 10 00 50 52 4F 43 45 53 7E 31 00 00 36 00 03 00 04 00 EF BE 33 55 05 5D 34 55 A7 95 14 00 00 00 50 00 72 00 6F 00 63 00
 00 00 E6 00 00 00 48 00 31 00 00 00 00 00 33 55 07 5D 10 00 53 44 4C 2D 41 50 7E 31 00 00 30 00 03 00 04 00 EF BE 33 55 07 5D 34 55 A7 95 14 00 00 00 73 C
00 72 00 6F 00 6D 00 70 00 74 00 2E 00 6C 00 6E 00 6B 00 00 00 1C 00 15 00 00 00 9A 00 00 00 4C 00 32 00 E0 A8 97 02 33 55 82 58 20 00 64 6F 77 6E 6C 6F 61
A 52 89 10 34 55 47 8F 14 00 00 00 50 00 72 00 6F 00 63 00 65 00 73 00 73 00 20 00 48 00 61 00 63 00 6B 00 65 00 72 00 20 00 32 00 2E 00 6C 00 6E 00 6B 00
```

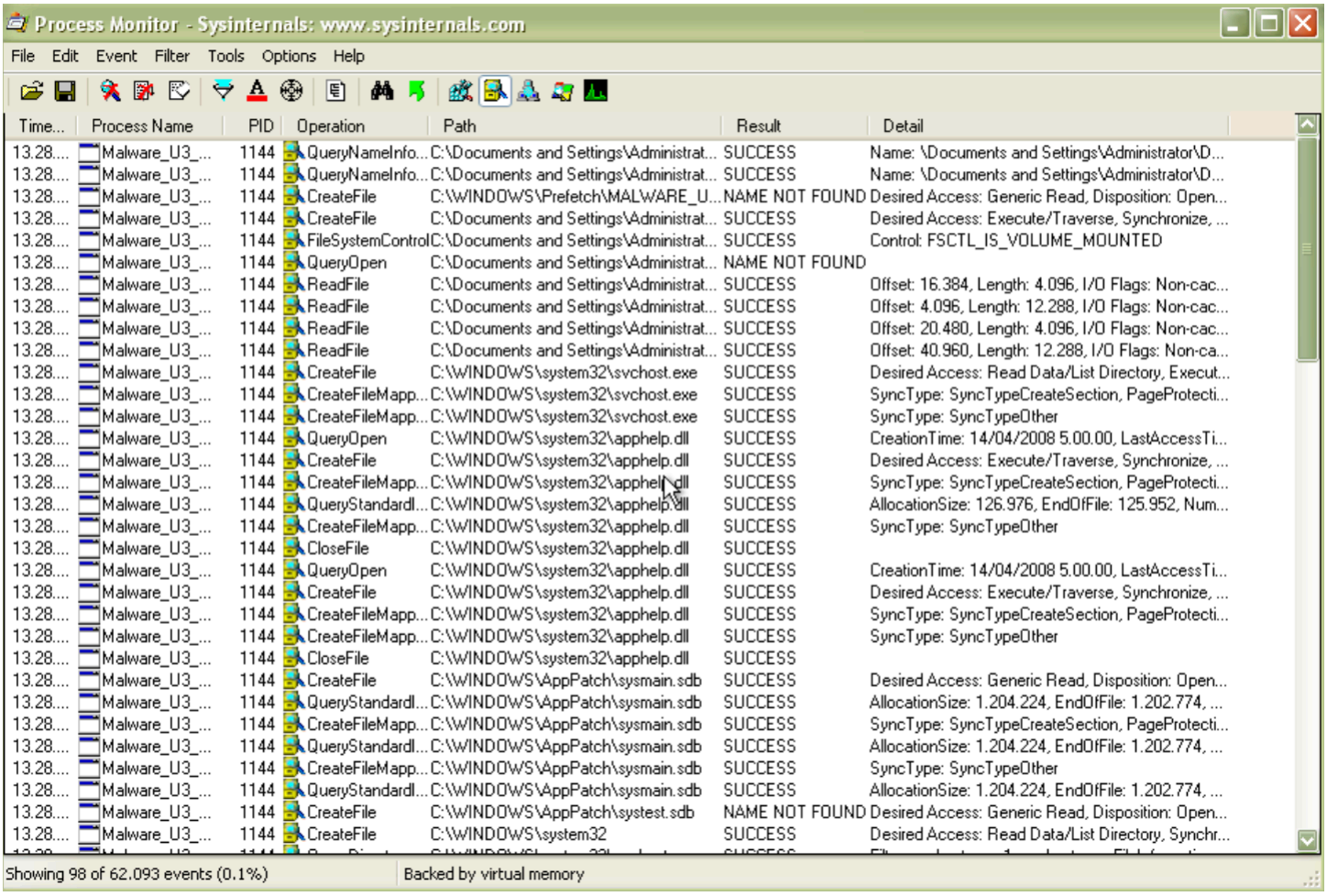

```
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx:  0A 00 00 00 09 00 00 00 00 00 00 00 0B 00 00 00 C
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx:  06 00 00 00 0A 00 00 00 05 00 00 00 09 00 00 00 C
HKU\S-1-5-21-1644491937-484763869-299502267-500\SessionInformation\ProgramCount: 0x00000003
HKU\S-1-5-21-1644491937-484763869-299502267-500\SessionInformation\ProgramCount: 0x00000005

-----------------------------------
Variazioni totali:35
-----------------------------------
```

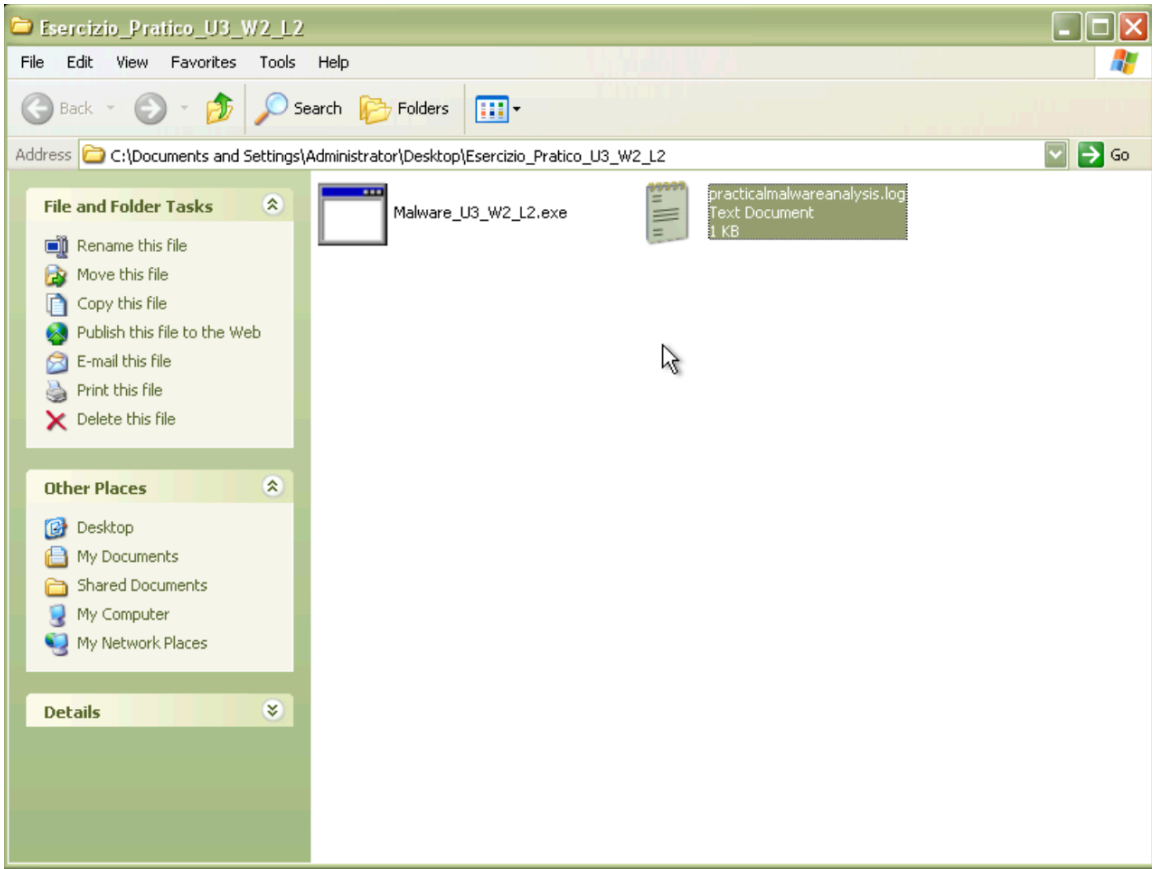
DOPO AVER EFFETTUATO QUESTE OPERAZIONI POSSIAMO AVVIARE IL MALWARE



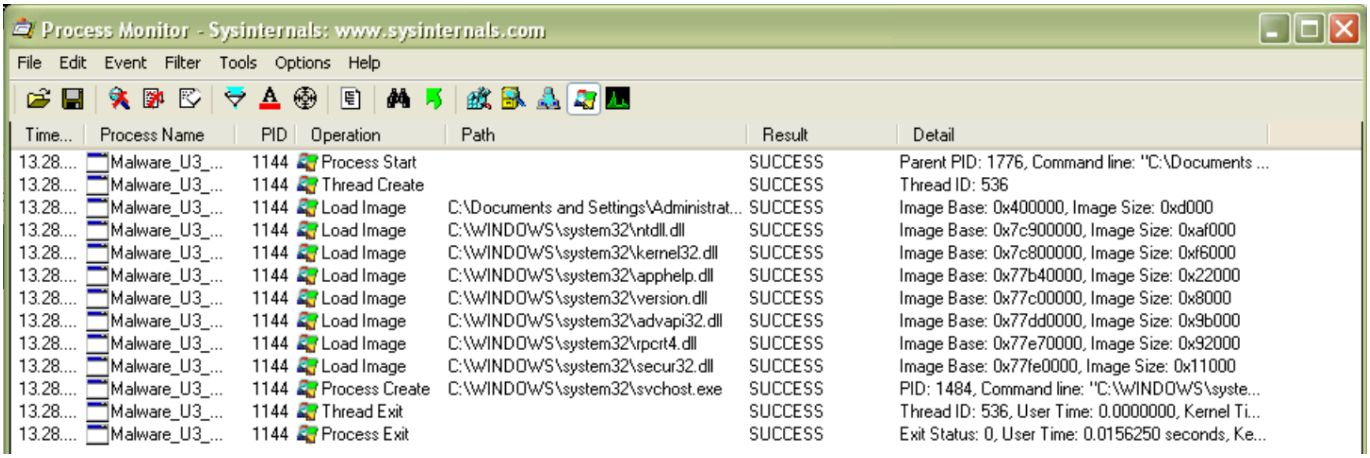
COME POSSIAMO VEDERE DALLA FOTO SOPRA QUI IL MALWARE STA PROVANDO AD APRIRE (REGOPENKEY) UNA CHIAVE DI REGISTRO E QUINDI IL MALWARE STA FACENDO UNA CHIAMATA AD UNA FUNZIONE CONTENUTA IN UNA DATA LIBRERIA

NELLA FOTO QUI DI SEGUITO POSSIAMO VEDERE COME MALWARE VA AD INTERAGIRE CON IL FILE SYSTEM, NEL NOSTRO CASO IL MALWARE CREA UN FILE

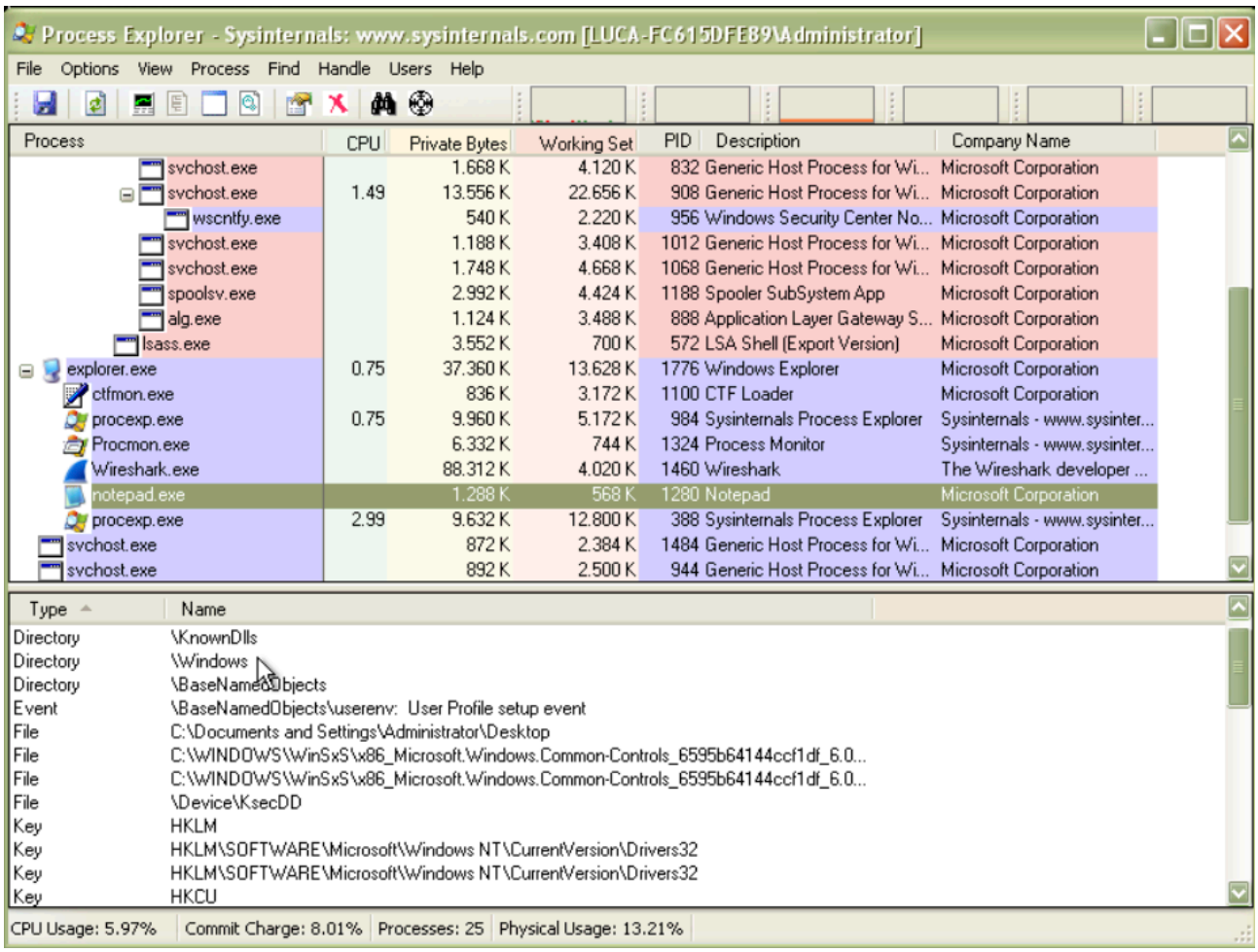




DA QUESTA FOTO POSSIAMO VEDERE COME IL MALWARE INTERAGISCE SUI PROCESSI E THREAD



COME POSSIAMO NOTARE QUI IL MALWARE VA A CREARE DELLE FUNZIONI (LOAD IMAGE) CHE SERVONO PER CARICARE ESEGUIBILI E LIBRERIE PER ESECUZIONE IN MEMORIA E ATTIVITA' SUI PROCESSI E THREAD COME CREATE PROCESS, CREATE THREAD



SECONDO ME IL MALWARE VA A COMPROMETTERE IL SITEMA OPERATIVO IN MODO TALE DA NON PERMETTE IL NORMALE FUNZIONAMENTO