

15:39:	Malware_U3_...	572	RegOpenKey	HKCU\Software\Microsoft\Windows N...	SUCCESS	Desired Access: R...
15:39:	Malware_U3_...	572	RegSetInfoKey	HKCU\Software\Microsoft\Windows N...	SUCCESS	KeySetInformation...
15:39:	Malware_U3_...	572	RegQueryValue	HKCU\Software\Microsoft\Windows N...	SUCCESS	Type: REG_SZ, Le...
15:39:	Malware_U3_...	572	RegCloseKey	HKCU\Software\Microsoft\Windows N...	SUCCESS	
15:39:	Malware_U3_...	572	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
15:39:	Malware_U3_...	572	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
15:39:	Malware_U3_...	572	RegSetInfoKey	HKLMSYSTEM\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
15:39:	Malware_U3_...	572	RegQueryValue	HKLMSYSTEM\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 120
15:39:	Malware_U3_...	572	RegQueryValue	HKLMSYSTEM\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 120
15:39:	Malware_U3_...	572	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
15:39:	Malware_U3_...	572	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
15:39:	Malware_U3_...	572	RegSetInfoKey	HKLMSYSTEM\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
15:39:	Malware_U3_...	572	RegQueryValue	HKLMSYSTEM\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 16
15:39:	Malware_U3_...	572	RegCloseKey	HKLMSYSTEM\CurrentControlSet\Contr...	SUCCESS	
15:39:	Malware_U3_...	572	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
15:39:	Malware_U3_...	572	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
15:39:	Malware_U3_...	572	RegSetInfoKey	HKLMSYSTEM\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
15:39:	Malware_U3_...	572	RegEnumKey	HKLMSYSTEM\CurrentControlSet\Contr...	SUCCESS	Index: 0, Name: i:T
15:39:	Malware_U3_...	572	RegQueryKey	HKLMSYSTEM\CurrentControlSet\Contr...	SUCCESS	Query: HandleTag...
15:39:	Malware_U3_...	572	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
15:39:	Malware_U3_...	572	RegQueryValue	HKLMSYSTEM\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWO...
15:39:	Malware_U3_...	572	RegQueryValue	HKLMSYSTEM\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 12
15:39:	Malware_U3_...	572	RegCloseKey	HKLMSYSTEM\CurrentControlSet\Contr...	SUCCESS	
15:39:	Malware_U3_...	572	RegEnumKey	HKLMSYSTEM\CurrentControlSet\Contr...	NO MORE ENTRI...	Index: 1, Length: 5...
15:39:	Malware_U3_...	572	RegCloseKey	HKLMSYSTEM\CurrentControlSet\Contr...	SUCCESS	
15:39:	Malware_U3_...	572	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
15:39:	Malware_U3_...	572	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: R...
15:39:	Malware_U3_...	572	RegOpenKey	HKLMSYSTEM\Wow6432Node\Polici...	REPARSE	Desired Access: R...
15:39:	Malware_U3_...	572	RegOpenKey	HKLMSYSTEM\Software\Policies\Microsoft\...	NAME NOT FOUND	Desired Access: R...
15:39:	Malware_U3_...	572	RegOpenKey	HKCU	SUCCESS	Desired Access: M...
15:39:	Malware_U3_...	572	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
15:39:	Malware_U3_...	572	RegOpenKey	HKCU\Control Panel\Desktop\MuiCach...	NAME NOT FOUND	Desired Access: R...
15:39:	Malware_U3_...	572	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Contr...	REPARSE	Desired Access: R...

```
--res-x86 - Blocco note
```

File Modifica Formato Visualizza ?

Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2024/2/14 14:38:56 , 2024/2/14 14:41:19
Computer: USER-PC , USER-PC
Username: user , user

Keys deleted: 1


HKU\S-1-5-20\Software\Microsoft\MediaPlayer\Health\{8B537D52-4B21-4BD7-90CF-816B5C46B524}

Keys added: 27

HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{659a6cf-64cd-480b-843e-32c86e1ba19f}\##?#UMB#UMB#1&841921d&o&pPrinterBusEnumerator#\{659a6cf-64cd-480b-843e-32c86e1ba19f}\
HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{659a6cf-64cd-480b-843e-32c86e1ba19f}\##?#UMB#UMB#1&841921d&o&pPrinterBusEnumerator#\{659a6cf-64cd-480b-843e-32c86e1ba19f}\Printers
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Fax
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Fax\DspDriver
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Fax\Dspooler
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Fax\PrinterDriverData
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Microsoft XPS Document Writer
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Microsoft XPS Document Writer\DspDriver
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Microsoft XPS Document Writer\Dspooler
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Microsoft XPS Document Writer\PrinterDriverData
HKLM\SYSTEM\CurrentControlSet\Enum\USB\UMB\1&841921d&o&pPrinterBusEnumerator\Control
HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{659a6cf-64cd-480b-843e-32c86e1ba19f}\##?#UMB#UMB#1&841921d&o&pPrinterBusEnumerator#\{659a6cf-64cd-480b-843e-32c86e1ba19f}\
HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{659a6cf-64cd-480b-843e-32c86e1ba19f}\##?#UMB#UMB#1&841921d&o&pPrinterBusEnumerator#\{659a6cf-64cd-480b-843e-32c86e1ba19f}\Printers
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Fax
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Fax\DspDriver
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Fax\Dspooler
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Fax\PrinterDriverData
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Microsoft XPS Document Writer
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Microsoft XPS Document Writer\DspDriver
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Microsoft XPS Document Writer\Dspooler
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Microsoft XPS Document Writer\PrinterDriverData
HKLM\SYSTEM\CurrentControlSet\Enum\USB\UMB\1&841921d&o&pPrinterBusEnumerator\Control
HKEY_USERS\S-1-5-20\Software\Microsoft\MediaPlayer\Health\{727105F7-E781-4D48-9A4C-DEF58012237}
HKU\S-1-5-20-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\WHCIConStartup
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help



Time ...	Process Name	PID	Operation	Path	Result	Detail
15:39:...	Malware_U3_...	572	Process Profiling		SUCCESS	User Time: 0.0312...