

Versione Stampabile della Discussione

[Clicca qui per visualizzare questa discussione nel suo formato originale](#)

WinInizio _ Altri problemi legati alla Sicurezza _ Dangerous Viruses Detected In Your System

Inviato da: nerdone il 08/09/08, 01:13

Salve 🙌 mi sono da poco registrato, e ho da pochi giorni un grandissimo problema ora mi spiego meglio:

navigando nel web ho trovato un programmino utile, allora l'ho scaricato e quando l'ho avviato non è apparso nulla e poi da lì ho dubitato...poco dopo apro una cartella dentro il disco rigido ed ecco che viene fuori una finestra con titolo: " **Dangerous error!** " e poi vi è scritto : " **Attention , seguito dal nome del mio pc,! Some dangerous viruses detected in your system. Micorsoft Windows XP Files corrupted.This may lead to the destruction of important files in c:\Windows. Download protection software now! Click OK to download the antispyware.(Reccomended)**

Poi ci sono 2 pulsanti ovvero SI o NO..e in qualsiasi dei 2 clicchi ti indirizzano a questa pagina:htxtp://checksystem-online.com/id/4912933/4/1/" dove ti obbligano a scaricare altri porgrammi ecc... 🤔🤔🤔🤔

Insomma so benissimo il significato di questo messaggio e credo che nn sia affatto un virus (dato che provando a fare scansioni con l'antivirus non lo rivela) ..il problema e che innanzitutto ogni volta che riapro cartelle esce questo messaggio e in più dopo un pò mi si crasha explorer.exe(il

desktop)...



Ho bisogno di questo grande aiuto..se mi potete aiutare ve ne sarò molto grato



Un Saluto a tutti!

Inviato da: thesorow il 08/09/08, 01:22

Benvenuto/a!

Ciao e Benvenuto/a nel forum, **nerdone**.

Perché non personalizzi la tua presenza in WinInizio aggiungendo una firma e un'immagine al tuo profilo personale ? se non sai come fare, [clicca qui](#).

Se sei una ragazza e vuoi essere aggiunta al gruppo delle **WinGirls** non dovrai fare altro che presentarti in [questo thread](#) o contattare un membro dello staff; se invece hai meno di 18 anni potresti far parte degli **Juniores**, per farlo [presentati qui](#) o contatta un membro dello staff.

Il gruppo WinGirls e Juniores offrono alcuni vantaggi speciali, scopriili nell'apposito thread di presentazione!



Ricordati, infine, che un titolo appropriato per dare visibilità alle tue nuove discussioni è essenziale: chiamare una discussione "Aiuto" o "Consiglio" non permette di capire subito la tua richiesta e rende più difficili le ricerche per gli altri utenti.

Link utili:

- [Regolamento](#)
- [Netiquette](#)
- [Glossario](#)
- [Thread di Benvenuto](#)
- [Guida all'uso di WinInizio](#)

Posta un <http://www.wininizio.it/forum/index.php?showtopic=21584> e vediamo di cosa si tratta.

Inviato da: nerdone il 08/09/08, 01:34

ok! appena posso personalizzo il mio profilo! comunque grazie per la tempestività della risposta
thesorrow 😄

Ascolta io hijackthis non l'ho ancora installato credo che lo si scarichi da
<http://forum.wininizio.it/index.php?showtopic=21584> 😊 appena posso lo installo e ti posto il log..grazie ancora ora vado a dormire... good night!!!!

Inviato da: thesorrow il 08/09/08, 01:48

Si lo scarichi da li, ma visto che non l'hai ancora installato ti consiglio prima di fare altre 2 o 3 operazioni preliminari domattina appena ti svegli 😊

1. Scarica <http://www.ccleaner.com/download/downloading>, durante l'installazione togli la spunta da Yahoo Toolbar. Poi apri il programma, vai su Opzioni - Avanzate e togli la spunta da "cancella file in windows temp solo se più vecchi di 48 ore". Ora chiudi internet explorer e/o firefox quindi avvia la pulizia e conferma la richiesta.

2. Scarica <http://download.bleepingcomputer.com/sUBs/ComboFix.exe>, disconnettiti da internet, disabilita e chiudi antivirus, antispyware e firewall. Manda in esecuzione il programma. Digita 1 e premi invio poi attendi il termine degli stage di scansione. Posta il log che troverai alla fine in C:\Combofix.txt.

3. Scarica poi http://www.download.com/Malwarebytes-Anti-Malware/3000-8022_4-10804572.html, aggiornalo e avvia una scansione completa. A fine scansione elimina tutto ciò che trova e posta il report che ti visualizza.

Scarica HijackThis e allega ora anche il suo log.

Inviato da: nerdone il 08/09/08, 01:49

ecco fatto..almeno domattina avrò qualche risposta 😊 :

```
Logfile of Trend Micro HijackThis v2.0.2
Scan saved at 2.43.14, on 08/09/2008
Platform: Windows XP SP2 (WinNT 5.01.2600)
MSIE: Internet Explorer v7.00 (7.00.6000.16705)
Boot mode: Normal
```

Running processes:

```
C:\WINDOWS\System32\smss.exe
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\system32\services.exe
C:\WINDOWS\system32\lsass.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\System32\svchost.exe
C:\WINDOWS\system32\ZoneLabs\vsmon.exe
C:\WINDOWS\system32\spoolsv.exe
C:\PROGRA~1\Grisoft\AVGFRE~1\avgamsvr.exe
C:\PROGRA~1\Grisoft\AVGFRE~1\avgupsvc.exe
C:\WINDOWS\system32\DRIVERS\CDANTSRV.EXE
C:\WINDOWS\system32\gearsec.exe
C:\WINDOWS\system32\nvsvc32.exe
C:\WINDOWS\System32\svchost.exe
```

C:\WINDOWS\ALCXMNTR.EXE
 C:\Programmi\Hewlett-Packard\HP Software Update\HPWuSchd.exe
 C:\Programmi\Hewlett-Packard\Digital Imaging\bin\hpotdd01.exe
 C:\WINDOWS\system32\spool\drivers\w32x86\3\hpztsb09.exe
 C:\Programmi\File comuni\Microsoft Shared\Works Shared\WkUFind.exe
 C:\Programmi\File comuni\Real\Update_OB\realsched.exe
 C:\PROGRA~1\Grisoft\AVGFRE~1\avgcc.exe
 C:\PROGRA~1\Grisoft\AVGFRE~1\avgemc.exe
 C:\WINDOWS\system32\RUNDLL32.EXE
 C:\Programmi\Zone Labs\ZoneAlarm\zlclient.exe
 C:\Programmi\Windows Live\Messenger\MsnMsgr.Exe
 C:\WINDOWS\system32\ctfmon.exe
 C:\Programmi\VisualTaskTips\VisualTaskTips.exe
 C:\Programmi\Vidalia Bundle\Privoxy\privoxy.exe
 C:\Programmi\MessengerDiscovery\MessengerDiscovery Live.exe
 C:\Programmi\Windows Live\Messenger\usnsvc.exe
 C:\Programmi\Mozilla Firefox\firefox.exe
 C:\Programmi\Winamp\winamp.exe
 C:\Programmi\Free Download Manager\fdm.exe
 C:\WINDOWS\system32\drwtsn32.exe
 C:\WINDOWS\system32\drwtsn32.exe
 C:\WINDOWS\explorer.exe
 C:\Programmi\Mozilla Thunderbird\thunderbird.exe
 C:\HiJackThis\HijackThis.exe

R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page = http://www.google.it/
 R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL =
 http://go.microsoft.com/fwlink/?LinkId=69157
 R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL =
 http://go.microsoft.com/fwlink/?LinkId=54896
 R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page = http://go.microsoft.com
 //fwlink/?LinkId=54896
 R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Start Page = http://go.microsoft.com/fwlink
 /?LinkId=69157
 R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName = Collegamenti
 O2 - BHO: Supporto di collegamento per Adobe PDF Reader - {06849E9F-C8D7-4D59-
 B87D-784B7D6BE0B3} - C:\Programmi\File comuni\Adobe\Acrobat\ActiveX\AcroIEHelper.dll
 O2 - BHO: (no name) - {7E853D72-626A-48EC-A868-BA8D5E23E045} - (no file)
 O2 - BHO: AFS plugin - {8EF40C36-293F-4749-8EA0-94FB3AD83FA1} - C:\WINDOWS\system32
 \dfax32x.dll
 O2 - BHO: Guida per l'accesso a Windows Live - {9030D464-4C02-4ABF-8ECC-5164760863C6} -
 C:\Programmi\File comuni\Microsoft Shared\Windows Live\WindowsLiveLogin.dll
 O2 - BHO: Windows Live Toolbar Helper - {BDBD1DAD-C946-4A17-ADC1-64B5B4FF55D0} -
 C:\Programmi\Windows Live Toolbar\msntb.dll
 O2 - BHO: FDMIECookiesBHO Class - {CC59E0F9-7E43-44FA-9FAA-8377850BF205} -
 C:\Programmi\Free Download Manager\iefdm2.dll
 O3 - Toolbar: Windows Live Toolbar - {BDAD1DAD-C946-4A17-ADC1-64B5B4FF55D0} -
 C:\Programmi\Windows Live Toolbar\msntb.dll
 O4 - HKLM\..\Run: [AlcxMonitor] ALCXMNTR.EXE
 O4 - HKLM\..\Run: [NeroFilterCheck] C:\WINDOWS\System32\NeroCheck.exe
 O4 - HKLM\..\Run: [HP Software Update] "C:\Programmi\Hewlett-Packard\HP Software
 Update\HPWuSchd.exe"
 O4 - HKLM\..\Run: [DeviceDiscovery] C:\Programmi\Hewlett-Packard\Digital Imaging\bin
 \hpotdd01.exe
 O4 - HKLM\..\Run: [HPDJ Taskbar Utility] C:\WINDOWS\system32\spool\drivers\w32x86
 \3\hpztsb09.exe
 O4 - HKLM\..\Run: [Microsoft Works Update Detection] C:\Programmi\File comuni\Microsoft
 Shared\Works Shared\WkUFind.exe
 O4 - HKLM\..\Run: [TkBellExe] "C:\Programmi\File comuni\Real\Update_OB\realsched.exe"
 -osboot
 O4 - HKLM\..\Run: [AVG7_CC] C:\PROGRA~1\Grisoft\AVGFRE~1\avgcc.exe /STARTUP
 O4 - HKLM\..\Run: [AVG7 EMC] C:\PROGRA~1\Grisoft\AVGFRE~1\avgemc.exe
 O4 - HKLM\..\Run: [NvCplDaemon] RUNDLL32.EXE C:\WINDOWS\system32\NvCpl.dll,NvStartup
 O4 - HKLM\..\Run: [NvMediaCenter] RUNDLL32.EXE C:\WINDOWS\system32
 \NvMcTray.dll,NvTaskbarInit
 O4 - HKLM\..\Run: [ZoneAlarm Client] "C:\Programmi\Zone Labs\ZoneAlarm\zlclient.exe"
 O4 - HKCU\..\Run: [msnmsgr] "C:\Programmi\Windows Live\Messenger\MsnMsgr.Exe"
 /background

04 - HKCU\..\Run: [ctfmon.exe] C:\WINDOWS\system32\ctfmon.exe
 04 - HKCU\..\Run: [VisualTaskTips] C:\Programmi\VisualTaskTips\VisualTaskTips.exe
 04 - HKUS\S-1-5-19\..\Run: [CTFMON.EXE] C:\WINDOWS\System32\CTFMON.EXE (User 'SERVIZIO LOCALE')
 04 - HKUS\S-1-5-19\..\Run: [AVG7_Run] C:\PROGRA~1\Grisoft\AVGFRE~1\avgw.exe /RUNONCE (User 'SERVIZIO LOCALE')
 04 - HKUS\S-1-5-20\..\Run: [CTFMON.EXE] C:\WINDOWS\System32\CTFMON.EXE (User 'SERVIZIO DI RETE')
 04 - HKUS\S-1-5-18\..\Run: [CTFMON.EXE] C:\WINDOWS\System32\CTFMON.EXE (User 'SYSTEM')
 04 - HKUS\DEFAULT\..\Run: [CTFMON.EXE] C:\WINDOWS\System32\CTFMON.EXE (User 'Default user')
 04 - Global Startup: Microsoft Office.Ink = C:\Programmi\Microsoft Office\Office\OSA9.EXE
 04 - Global Startup: Privoxy.Ink = C:\Programmi\Vidalia Bundle\Privoxy\privoxy.exe
 08 - Extra context menu item: &Windows Live Search - res://C:\Programmi\Windows Live Toolbar\msntb.dll/search.htm
 08 - Extra context menu item: Scarica con Free Download Manager - file://C:\Programmi\Free Download Manager\dllink.htm
 08 - Extra context menu item: Scarica i video con Free Download Manager - file://C:\Programmi\Free Download Manager\dlfvideo.htm
 08 - Extra context menu item: Scarica selezionati con Free Download Manager - file://C:\Programmi\Free Download Manager\dlselected.htm
 08 - Extra context menu item: Scarica tutto con Free Download Manager - file://C:\Programmi\Free Download Manager\dlall.htm
 09 - Extra button: Messenger - {FB5F1910-F110-11d2-BB9E-00C04F795683} - C:\Programmi\Messenger\msmsgs.exe
 09 - Extra 'Tools' menuitem: Windows Messenger - {FB5F1910-F110-11d2-BB9E-00C04F795683} - C:\Programmi\Messenger\msmsgs.exe
 016 - DPF: {1F831FA9-42FC-11D4-95A6-0080AD30DCE1} (InstaFred) - file://C:\Programmi\AutoCAD 2002 Ita\InstFred.ocx
 016 - DPF: {78AF2F24-A9C3-11D3-BF8C-0060B0FCC122} (Controllo AcDc oggi) - file://C:\Programmi\AutoCAD 2002 Ita\AcDcToday.ocx
 016 - DPF: {AE563729-B4F5-11D4-A415-00108302FDFD} (NOXLATE-BANR) - file://C:\Programmi\AutoCAD 2002 Ita\InstBanr.ocx
 016 - DPF: {F281A59C-7B65-11D3-8617-0010830243BD} (Controllo AcPreview) - file://C:\Programmi\AutoCAD 2002 Ita\AcPreview.ocx
 017 - HKLM\System\CCS\Services\Tcpip\..\{A516A343-BD71-4FAD-9F1E-3180C0921772}: NameServer = 62.211.69.150 212.48.4.15
 018 - Protocol: skype4com - {FFC8B962-9B40-4DFF-9458-1830C7DD7F5D} - C:\PROGRA~1\FILECO~1\Skype\SKYPE4~1.DLL
 020 - AppInit_DLLs: C:\PROGRA~1\Google\GOOGLE~2\GOEC62~1.DLL
 023 - Service: AVG7 Alert Manager Server (Avg7Alrt) - GRISOFT, s.r.o. - C:\PROGRA~1\Grisoft\AVGFRE~1\avgamsvr.exe
 023 - Service: AVG7 Update Service (Avg7UpdSvc) - GRISOFT, s.r.o. - C:\PROGRA~1\Grisoft\AVGFRE~1\avgupsvc.exe
 023 - Service: C-DillaSrv - C-Dilla Ltd - C:\WINDOWS\system32\DRIVERS\CDANTSrv.EXE
 023 - Service: gearsec - GEAR Software - C:\WINDOWS\system32\gearsec.exe
 023 - Service: GFI LANguard N.S.S. 8.0 Attendant Service (gfi_Inss8_attservice) - GFI Software Ltd. - C:\Programmi\GFI\LANguard Network Security Scanner 8.0\Inssatt.exe
 023 - Service: Google Desktop Manager 5.7.712.18632 (GoogleDesktopManager-121807-210419) - Google - C:\Programmi\Google\Google Desktop Search\GoogleDesktop.exe
 023 - Service: Google Updater Service (gusvc) - Google - C:\Programmi\Google\Common\Google Updater\GoogleUpdaterService.exe
 023 - Service: InstallDriver Table Manager (IDriverT) - Macrovision Corporation - C:\Programmi\File comuni\InstallShield\Driver\1150\Intel 32\IDriverT.exe
 023 - Service: NVIDIA Display Driver Service (NVSvc) - NVIDIA Corporation - C:\WINDOWS\system32\nvsvc32.exe
 023 - Service: Remote Packet Capture Protocol v.0 (experimental) (rpcapd) - CACE Technologies - C:\Programmi\WinPcap\rpcapd.exe
 023 - Service: TrueVector Internet Monitor (vsmon) - Zone Labs, LLC - C:\WINDOWS\system32\ZoneLabs\vsmon.exe
 --
 End of file - 8244 bytes

Spero di essere stato utile...Buona notte ci vediamo domani 🙌!!!

Inviato da: thesorrow il 08/09/08, 09:36

Ok esegui le operazioni che ti ho descritto sopra.

Inviato da: nerdone il 08/09/08, 10:44

Va bene..l'unico problema è che dovrai appettare un pochino dato che qui dove sono ancora arriva l'adsl quindi navigo ancora con la vecchia 56 kpbs 🙄🙄🙄🙄🙄🙄

Finalmete Problema RISOLTO ALLA GRANDE 🙌🙌🙌 !!!!

Grazie ancora, devo dire che questi software sono davvero utili...conoscevo solo **ccleaner** 😊

thank you very much 🙄🙄🙄 !!!

Allego comunque i log che mi avevi chiesto;

...Sicuramente ora saprai il mio vero nome 😄😄😄

-  [ComboFix.txt](#) (19.43k) : 10
-  [mbam_log_2008_09_08_14_23_42_.txt](#) (1.33k) : 3
-  [hijackthis.log](#) (7.7k) : 4

Inviato da: thesorrow il 08/09/08, 17:00

Purtroppo ancora non è finita.

Ora scarica The Avenger (dalla mia firma) e incolla il seguente script nel box bianco, poi premi Execute, e dai la conferma:

Files to delete:

C:\WINDOWS\system32\lpax32i.dll

C:\WINDOWS\system32\dfax32x.dll

C:\Documents and Settings\Computer\Dati applicazioni\wklnhst.dat

C:\Documents and Settings\Fabio\Dati applicazioni\wklnhst.dat

Fai di nuovo la scansione con MalwareBytes e stavolta seleziona ed elimina tutto quello che trova.

A fine operazioni esegui una scansione completa con <http://forum.wininizio.it/index.php?showtopic=36981> e posta il report.

Inviato da: nerdone il 09/09/08, 16:42

CITAZIONE

Ora scarica The Avenger (dalla mia firma) e incolla il seguente script nel box bianco, poi premi Execute, e dai la conferma:

Files to delete:

C:\WINDOWS\system32\lpax32i.dll

C:\WINDOWS\system32\dfax32x.dll

C:\Documents and Settings\Computer\Dati applicazioni\wklnhst.dat

C:\Documents and Settings\Fabio\Dati applicazioni\wklnhst.dat

Dopo il riavvio tutto ok mi è uscito il file.txt con la conferma dell'eliminazione dei file !!!

CITAZIONE

Fai di nuovo la scansione con MalwareBytes e stavolta seleziona ed elimina tutto quello che trova.

Terminata la scansione non mi ha trovato nulla di malvagio 😊 !
ecco il log:

CITAZIONE

Malwarebytes' Anti-Malware 1.27
Versione del database: 1128
Windows 5.1.2600 Service Pack 2

09/09/2008 15.24.51
mbam-log-2008-09-09 (15-24-51).txt

Tipo di scansione: Scansione completa (C:\|F:\|)
Elementi scansionati: 129816
Tempo trascorso: 1 hour(s), 13 minute(s), 20 second(s)

Processi della memoria infetti: 0
Moduli della memoria infetti: 0
Chiavi di registro infette: 0
Valori di registro infetti: 0
Elementi dato del registro infetti: 0
Cartelle infette: 0
File infetti: 0

Processi della memoria infetti:
(Nessun elemento malevolo rilevato)

Moduli della memoria infetti:
(Nessun elemento malevolo rilevato)

Chiavi di registro infette:
(Nessun elemento malevolo rilevato)

Valori di registro infetti:
(Nessun elemento malevolo rilevato)

Elementi dato del registro infetti:
(Nessun elemento malevolo rilevato)

Cartelle infette:
(Nessun elemento malevolo rilevato)

File infetti:
(Nessun elemento malevolo rilevato)

Per questo:

CITAZIONE

fine operazioni esegui una scansione completa con <http://forum.wininizio.it/index.php?showtopic=36981> e posta il report.

avrei dei problemi in quanto la mia connessione è lentissima (figurati 56 kbps 😞) e dato che mi serve anche il software java..anche per scaricare quello ho problemi dato che il software si installa

mentre si scarica.....



Inviato da: thesorrow il 09/09/08, 17:02

Se non hai altri problemi allora fai una scansione con <http://www.tgsoft.it/italy/download.htm> e

poi disinstallalo se non ti trova niente.

Se vuoi essere sicuro allora scarica la versione di prova di Kaspersky, però prima devi disinstallare l'antivirus che hai. Poi scaduta la versione di prova puoi tranquillamente rimettere l'antivirus gratuito. Questo procedimento è per fare una scansione completa con Kaspersky, altrimenti segui il consiglio di Virit.

Inviato da: angelique il 09/09/08, 20:12

Puoi anche provare con KASPERSKY VIRUS REMOVAL TOOL (non richiede l'installazione)

<http://downloads5.kaspersky-labs.com/devbuilds/AVPTool/>

- scarica la versione del tool più aggiornata rispetto alla data di pubblicazione
 - crea una apposta Cartella sul Desktop ed al suo interno posiziona il file
 - lancia il tool
 - imposta le aree che intendi scansionare (non è possibile eseguire la scansione di specifiche cartelle)
 - al termine della scansione sarà possibile rimuovere e/o mettere in quarantena i file infetti rilevati
- Salva ed allega, il log che verrà rilasciato

(Il tool è incompatibile se si hanno già prodotti Kaspersky installati e non possiede una funzione di aggiornamento automatico delle firme)

Procedura di disinstallazione di KASPERSKY VIRUS REMOVAL TOOL

- clicca sull'icona per lanciare il tool
- nella finestra principale, in basso, clicca sulla voce Complete Virus Protection
- verrà visualizzato un messaggio: clicca su Ok
- chiudi la pagina web che verrà aperta
- nel messaggio successivo, clicca su SI per avviare la disinstallazione
- al termine, verrà richiesto di riavviare il P.C.



Inviato da: nerdone il 10/09/08, 11:20

Grazie a tutti e due 😊 😊 !!!

Al momento credo che per quanto riguarda la versione di prova di Kaspersky, non la metterò dato che se installo e disinstallo il mio antivirus avrò un sacco di aggiornamenti da fare e immaginate un pò..sempre lo stesso problema...

La cosa più sbrigativa al momento è VirIt (dato che è grande 2.4 MB 😊);

per quanto riguarda KASPERSKY VIRUS REMOVAL TOOL anche se è grande una 20 di Mb, appena posso lo scarico (dato che una volta su questa linea così lenta ho scaricato 700 MB 😞)....

Ancora Grazie!!

Al prossimo aggiornamento 😊 ...!!!

Inviato da: angelique il 10/09/08, 11:28

Solo una piccola precisazione:

Se usi Virit non hai bisogno di usare il tool Kaspersky e viceversa...

La scansione online con Kaspersky puoi anche eseguirla disconnesso dalla rete

leggi > <http://www.wininizio.it/forum/index.php?s=&showtopic=36981&view=findpost&p=495435>

<



Inviato da: nerdone il 10/09/08, 16:27

CITAZIONE(angelique @ 10/09/08, 12:28) ☒

Solo una piccola precisazione:

Se usi Virit non hai bisogno di usare il tool Kaspersky e viceversa...

😊 Può darsi che hai perfettamente ragione... ma ti spiego:

Usando Virit dopo la scansione non ha trovato nulla di anomalo.. 😊 !!!

Dopo aver scaricato Kaspersky ..sta a guardare il file log 😊 (naturalmente manca tutto il resto):

CITAZIONE

Scan

Scanned: 337478

Detected: 4

Untreated: 0

Start time: 10/09/2008 14.08.15

Duration: 02.33.53

Finish time: 10/09/2008 16.42.08

Detected

Status Object

deleted: riskware not-a-virus:Client-IRC.Win32.mIRC.621 File: C:\Downloads\Software
\mirc621.exe//stream//data0008

deleted: riskware not-a-virus:Client-IRC.Win32.mIRC.631 File: C:\Downloads\Software
\mirc631.exe//stream//data0001//stream//data0014

deleted: riskware not-a-virus:Client-IRC.Win32.mIRC.621 File: C:\Programmi\mIRC\mirc.exe

deleted: Trojan program Trojan-Downloader.VBS.Small.dn File: C:\Programmi\Norton
AntiVirus\Quarantine\3A640B49.htm//CryptFF

-----mancano gli eventi!!!-----

Statistics

Object Scanned Detected Untreated Deleted Moved to Quarantine Archives

All objects 337478 4 0 4 0 4606 606 10 21

System memory 0 0 0 0 0 0 0 0

Startup objects 706 0 0 0 0 1 20 0 0

Disk boot sectors 5 0 0 0 0 0 0 0

Disco Locale (C:) 309745 4 0 4 0 4173 562 10 21

Dati (F:) 27022 0 0 0 0 432 24 0 0

Settings

Parameter Value

Security Level Recommended

Action Prompt for action when the scan is complete

Run mode Manually

File types Scan all files

Scan only new and changed files No

Scan archives All

Scan embedded OLE objects All

Skip if object is larger than No

Skip if scan takes longer than No

Parse email formats No

Scan password-protected archives No

Enable iChecker technology No

Enable iSwift technology No
Show detected threats on "Detected" tab Yes
Rootkits search Yes
Deep rootkits search No
Use heuristic analyzer Yes

Quarantine

Status Object Size Added

Backup

Status Object Size

Inviato da: angelique il 10/09/08, 16:44

I primi riskware not-a-virus:Client-IRC.Win32.mIRC.621 File: C:\Downloads\Software
\mirc621.exe//stream//data0008
sono falsi positivi (non virus)
l'ultimo è nella quarantena di Norton, quindi innoquo

direi che sei a posto così 😊



Inviato da: nerdone il 10/09/08, 21:52

si lo sapevo grazie cmq per l'aiuto che mi avete dato in questi giorni 🙌🙌 !!!

un'ultima domanda: ma qui in questo forum come funziona, chi scrive molti messaggi sale di livello 😄 ?

saluti 😊 !!

Inviato da: B4D il 23/09/08, 16:40

We anche io ho lo stesso prob. (cacchio nn so come fare a continuare ad usare il pc) ogni volta che apro 1 cartella mi da errore e mi manda sul sito 🤖 htxtp://sc.videofreeforonline.com/id/4912933/4/1/ per farmi vedere 1 video dimostrativo. Ho provato a scaricarlo il file ma dentro c'è veramente 1 virus (che mi ha bloccato nod) Aiutooooooo plz!

Inviato da: angelique il 24/09/08, 14:27

Benvenuto/a!

Ciao e Benvenuto/a nel forum, **B4D**.
Perché non personalizzi la tua presenza in WinInizio aggiungendo una firma e un'immagine al tuo profilo personale ? se non sai come fare, [clicca qui](#).



Se sei una ragazza e vuoi essere aggiunta al gruppo delle **WinGirls** non dovrai fare altro che presentarti in [questo thread](#) o contattare un membro dello staff; se invece hai meno di 18 anni potresti far parte degli **Juniores**, per farlo [presentati qui](#) o contatta un membro dello staff.

Il gruppo WinGirls e Juniores offrono alcuni vantaggi speciali, scopriili nell'apposito thread

di presentazione!

Ricordati, infine, che un titolo appropriato per dare visibilità alle tue nuove discussioni è essenziale: chiamare una discussione "Aiuto" o "Consiglio" non permette di capire subito la tua richiesta e rende più difficili le ricerche per gli altri utenti.

Link utili:

- [Regolamento](#)
- [Netiquette](#)
- [Glossario](#)
- [Thread di Benvenuto](#)
- [Guida all'uso di WinInizio](#)

Ciao **B4D**,
hai provato a seguire la procedura descritta in questa discussione?

- log hijackthis
- log combofix
- Malwarebyte



Inviato da: nerdone il 24/09/08, 16:40

CITAZIONE(B4D @ 23/09/08, 17:40)

We anche io ho lo stesso prob. (cacchio nn so come fare a continuare ad usare il pc) ogni volta che apro 1 cartella mi da errore e mi manda sul sito  [htxtp://sc.videofreeforonline.com/id/4912933/4/1/](http://sc.videofreeforonline.com/id/4912933/4/1/) per farmi vedere 1 video dimostrativo. Ho provato a scaricale il file ma dentro c'è veramente 1 virus (che mi ha bloccato nod) Aiutooooooo plz!

Si guarda..è davvero facile , tanto facile che mi domando come diavolo ho fatto a non arrivarci..  (non conoscevo i programmi ) ... a questo punto per te deve essere ancora più facile..segui passo passo i topic 

Inviato da: pinzer il 01/11/08, 19:42

Anche io ho avuto lo stesso problema. Con un semplice scan con Malwarebytes ho risolto tutto. Mi avete salvato la vita...grazie   

Inviato da: angelique il 01/11/08, 20:22

Benvenuto/a!

Ciao e Benvenuto/a nel forum, **pinzer**.
Perché non personalizzi la tua presenza in WinInizio aggiungendo una firma e un'immagine al tuo profilo personale ? se non sai come fare, [clicca qui](#).

Se sei una ragazza e vuoi essere aggiunta al gruppo delle **WinGirls** non dovrai fare altro che presentarti in [questo thread](#) o contattare un membro dello staff; se invece hai meno di 18 anni potresti far parte degli **Juniores**, per farlo [presentati qui](#) o contatta un membro dello staff.



Il gruppo WinGirls e Juniores offrono alcuni vantaggi speciali, scopriili nell'apposito thread di presentazione!

Ricordati, infine, che un titolo appropriato per dare visibilità alle tue nuove discussioni è essenziale: chiamare una discussione "Aiuto" o "Consiglio" non permette di capire subito la tua richiesta e rende più difficili le ricerche per gli altri utenti.

Link utili:

- [Regolamento](#)

- [Netiquette](#)
- [Glossario](#)
- [Thread di Benvenuto](#)
- [Guida all'uso di WinInizio](#)

Ciao **pinzer**, sono contenta che ti siamo stati di aiuto, se hai bisogno di un controllo siamo qui.



Inviato da: illya_xp il 02/11/08, 14:25

Ciao ragazzi. anch'io ho stesso problema... come procedo? segue gli stessi passi di Nerdone poi posto i log? grazzzzzie

Inviato da: angelique il 02/11/08, 14:28

Benvenuto/a!

Ciao e Benvenuto/a nel forum, **illya_xp**.
Perché non personalizzi la tua presenza in WinInizio aggiungendo una firma e un'immagine al tuo profilo personale ? se non sai come fare, [clicca qui](#).

Se sei una ragazza e vuoi essere aggiunta al gruppo delle **WinGirls** non dovrai fare altro che presentarti in [questo thread](#) o contattare un membro dello staff; se invece hai meno di 18 anni potresti far parte degli **Juniores**, per farlo [presentati qui](#) o contatta un membro dello staff.

Il gruppo WinGirls e Juniores offrono alcuni vantaggi speciali, scopriili nell'apposito thread di presentazione!



Ricordati, infine, che un titolo appropriato per dare visibilità alle tue nuove discussioni è essenziale: chiamare una discussione "Aiuto" o "Consiglio" non permette di capire subito la tua richiesta e rende più difficili le ricerche per gli altri utenti.

Link utili:

- [Regolamento](#)
- [Netiquette](#)
- [Glossario](#)
- [Thread di Benvenuto](#)
- [Guida all'uso di WinInizio](#)

Ciao **illya_xp**,
segui <http://forum.wininizio.it/index.php?showtopic=98111> dal punto 1 al punto 8 ed allega i report di Combofix e Malwarebytes



Inviato da: illya_xp il 02/11/08, 14:31

OK. seguiro' la guida=) (se siete veloci a rispondere!!!!=)

Inviato da: illya_xp il 02/11/08, 15:59

Ecco fatto. Posto i report di Combofix, Malwarebytes e log di hijackthis. spero ke riuscirete ad aiutarmi.

-
- [hijackthis.log](#) (9.76k) : 1
 - [ComboFix.txt](#) (21.92k) : 4
 - [mbam_log_2008_11_02_13_57_57_.txt](#) (2.23k) : 2

Inviato da: Luke57 il 02/11/08, 19:22

Ciao, adesso apri un file di testo e copiaci questo script all'interno:

CODICE

```
File::
C:\WINDOWS\system32\ifsndu.dll

Folder::
C:\Documents and Settings\All Users\Dati applicazioni\
{3276BE95_AF08_429F_A64F_CA64CB79BCF6}

Registry::
[-HKEY_LOCAL_MACHINE\~\Browser Helper Objects\{3A303EF6-2598-4D2D-B4DA-DEFA7CD0DC51}]
```

salva il file di testo, chiamandolo obbligatoriamente **CFScript.txt** nella stessa direzione di combofix, trascinalo con il puntatore del mouse sull'icona di combofix per una nuova scansione e riavvio del computer. Allega nuovo report se prodotto.

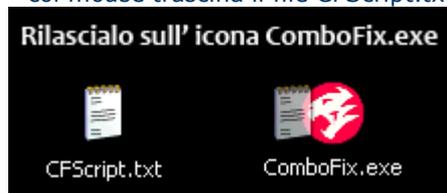
Inviato da: illya_xp il 02/11/08, 22:47

dice che C:\WINDOWS\system32 non è un programma e non e' un percorso valido...

Inviato da: angelique il 03/11/08, 09:35

Ciao **illya_xp**,
lo script è giusto, te l'ho allego...

- col mouse trascina il file CFScript.txt sull'icona rossa di combofix



riavvia il computer

Esegui una <http://www.wininizio.it/forum/index.php?showtopic=99707> (su "my computer") ed allega il report



 [CFScript.txt](#) (245byte) : 4

Inviato da: illya_xp il 03/11/08, 13:33

mi pare ke il problema si è stato risolto=)

Inviato da: angelique il 03/11/08, 15:10

Meglio così 😊 ...quando hai un pò di tempo esegui la scansione online 🙄

Inviato da: Mr Guerra il 06/11/08, 16:15

Salve a tutti. Purtroppo ho anche io lo stesso problema degli altri utenti in questo thread; la differenza è però che non riesco ad eseguire alcune applicazioni, fra le altre anche ccleaner, combofix, the avenger, hijackthis, avast... mentre Malwarebytes' anti-malware, advanced windows care e qualcos'altro funziona. Sapete dirmi come procedere? Non so più che pesci prendere...

Inviato da: Duca Bianco il 06/11/08, 16:35

Ciao **Mr Guerra**

segui una di <http://forum.wininizio.it/index.php?showtopic=93833> procedure e posta i log



Inviato da: Mr Guerra il 06/11/08, 16:40

Ok, lo faccio, grazie 1000!

EDIT:

Perfetto, ho risolto con la II procedura, quella valida anche per Vista.

Ho dovuto reinstallare Avast, Ccleaner, Messenger ecc.

Grazie!

Inviato da: angelique il 06/11/08, 22:20

Benvenuto/a!

Ciao e Benvenuto/a nel forum, **Mr Guerra**.

Perché non personalizzi la tua presenza in WinInizio aggiungendo una firma e un'immagine al tuo profilo personale ? se non sai come fare, [clicca qui](#).

Se sei una ragazza e vuoi essere aggiunta al gruppo delle **WinGirls** non dovrai fare altro che presentarti in [questo thread](#) o contattare un membro dello staff; se invece hai meno di 18 anni potresti far parte degli **Juniors**, per farlo [presentati qui](#) o contatta un membro dello staff.

Il gruppo WinGirls e Juniors offrono alcuni vantaggi speciali, scopriili nell'apposito thread di presentazione!



Ricordati, infine, che un titolo appropriato per dare visibilità alle tue nuove discussioni è essenziale: chiamare una discussione "Aiuto" o "Consiglio" non permette di capire subito la tua richiesta e rende più difficili le ricerche per gli altri utenti.

Link utili:

- [Regolamento](#)
- [Netiquette](#)
- [Glossario](#)
- [Thread di Benvenuto](#)
- [Guida all'uso di WinInizio](#)

Sono contenta che hai risolto!



Fornito da Invision Power Board (<http://www.invisionboard.com>)
© Invision Power Services (<http://www.invisionpower.com>)