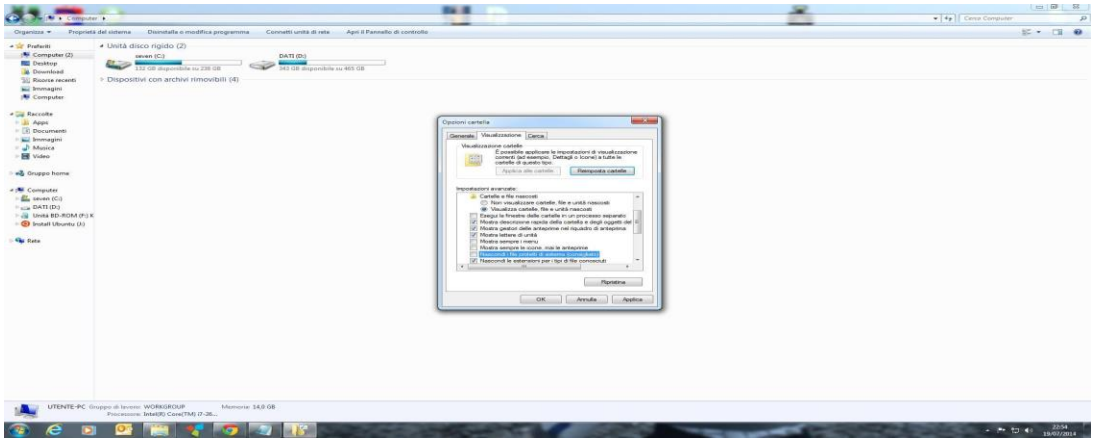
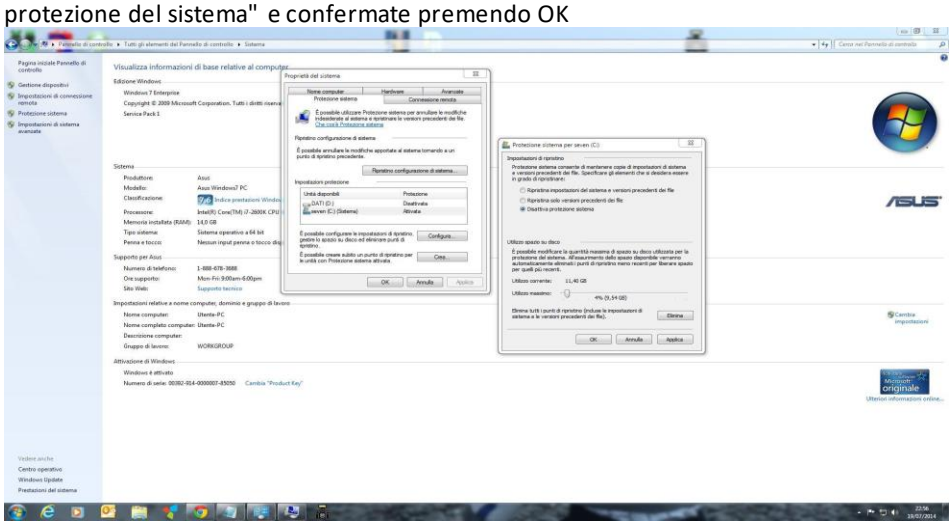
RIMOZIONE VIRUS UPDATER.VBE

Se improvvisamente vi scompaiono i files dalla pendrive ed al loro posto ci sono solo dei collegamenti, con molta probabilità siete stati infettati dal malware Updater.vbe
Se seguirete attentamente queste istruzioni potrete liberarvi del fastidiosissimo malware anche se non siete esperti. Ricordatevi di eseguire tutti i passi senza saltarne nemmeno uno. La procedura è valida per Windows 7 ma in linea di massima è applicabile anche sulle altre versioni di windows

1-) **Abilitare la visualizzazione dei file nascosti**
Andate sul pannello di controllo e cliccate su "Opzioni cartella", spostatevi sulla scheda "visualizzazione" e scorrendo sulle opzioni in basso mettere la spunta su "Visualizza cartelle, file e unità nascoste", poi togliete la spunta su "nascondi file protetti di sistema". Confermate con il tasto "OK" e rispondete di si se il sistema vi chiede nuovamente la conferma della scelta.

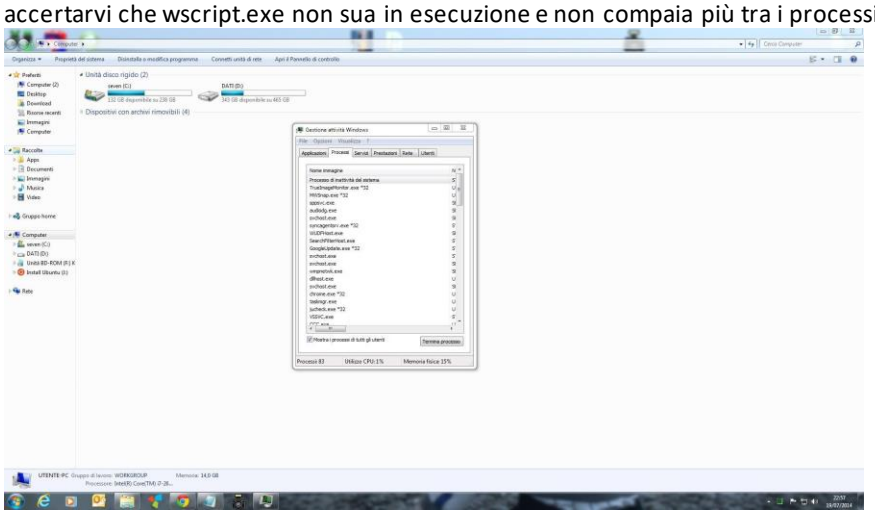


2-) **Disattivare punti di ripristino**
Sempre dal pannello di controllo cliccate su "sistema" e poi cliccate a sinistra su "Protezione sistema". Selezionate il disco C: e cliccate sul pulsante "Configura", nella finestra che segue spuntate la voce "disattiva protezione del sistema" e confermate premendo OK



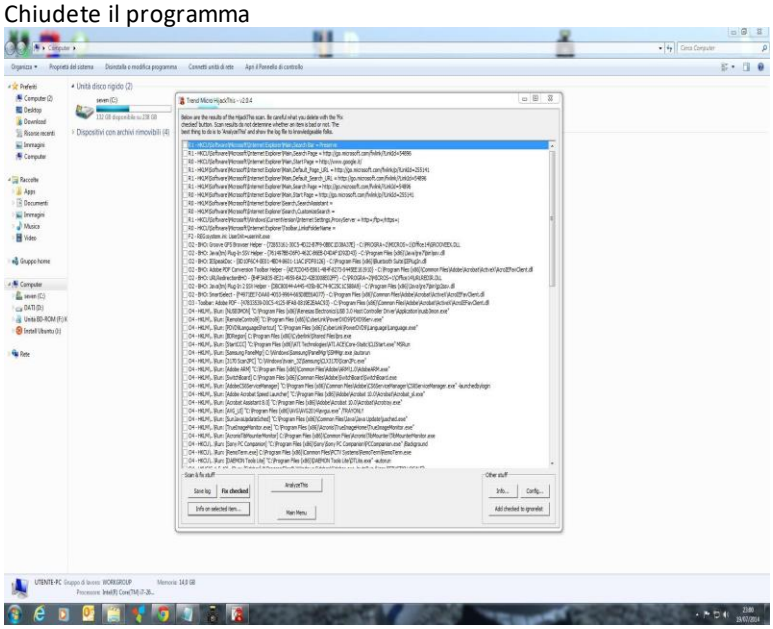
3-) **Terminare processo wscript.exe**
Premete contemporaneamente i tasti CTRL+ALT+CANC e cliccate su Avvia gestione attività". Nella finestra che appare selezionate la scheda "processi" in modo che possa comparire l'elenco dei processi attivi (elenco di file eseguibili in esecuzione). Tra questi dovrebbe comparire il processo legato al file "wscript.exe", se lo trovate

dovete selezionarlo e cliccare sul pulsante "termina processo". Attenzione!, wscript.exe esegue il codice virale ma non è il virus quindi terminatelo senza cancellare il file. Chiudete la finestra e rieseguite il punto 3 per accertarvi che wscript.exe non sua in esecuzione e non compaia più tra i processi attivi



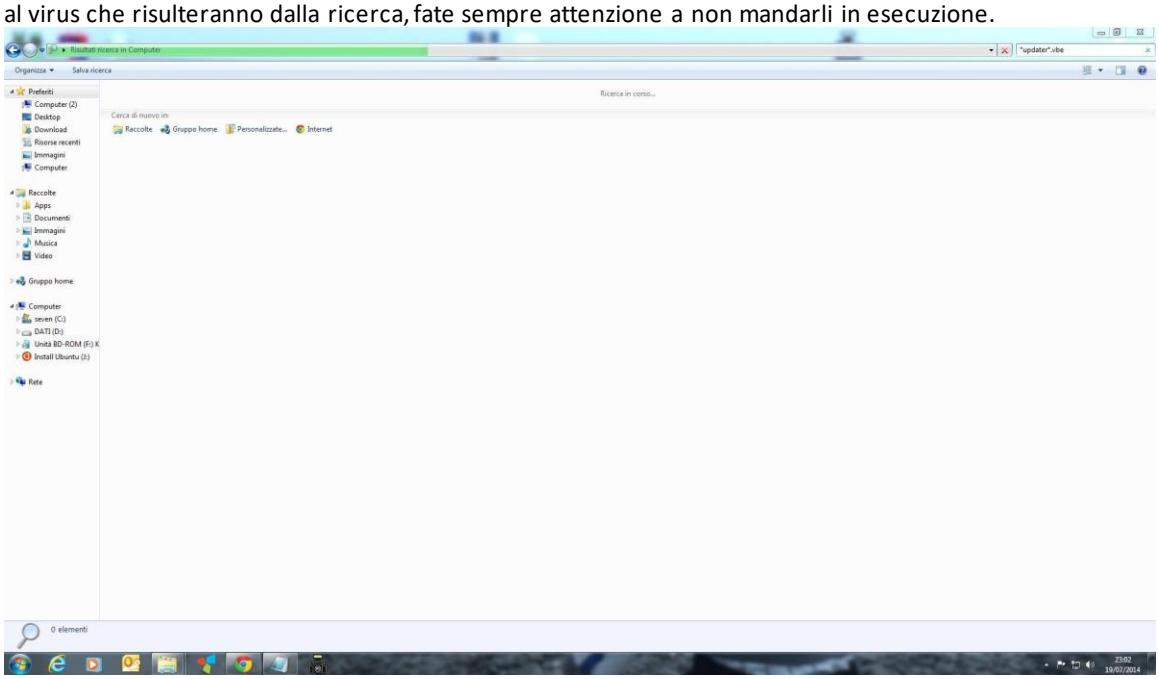
4-) Scaricate il software ccleaner dal link: http://www.piriform.com/ccleaner/download/standard ed installatelo spuntando solo le prime due voci nelle opzioni di installazione. Avviate ccleaner e cliccate su "pulizia" in alto a sinistra.
Selezionate tutte le caselle delle opzioni ad eccezione di: Password salvate, Password di rete, Collegamenti su Desktop, Installazione di windows obsoleta, Bonifica spazio libero. Ora cliccate su "Avvia pulizia" ed attendete il termine delle operazioni, poi chiudete il software

5-) Utilizzo di HijackThis
Scaricare HijackThis al link: http://www.ilsoftware.it/querydl.asp?id=754. Salvate il programma sul desktop ed eseguitelo come amministratore (tasto destro e poi "esegui come amministratore"). Cliccare su "I Accept" e poi su "Do a system scan only". Per comodità ingrandite la finestra in modo da vedere meglio l'elenco delle voci di registro riferite ai file che vengono caricati automaticamente all' avvio di windows. Selezionate tutte le voci in cui compare la chiamata al file updater.vbe, poi cliccate sul tasto "Fix checked" e confermare la scelta. Chiudete il programma



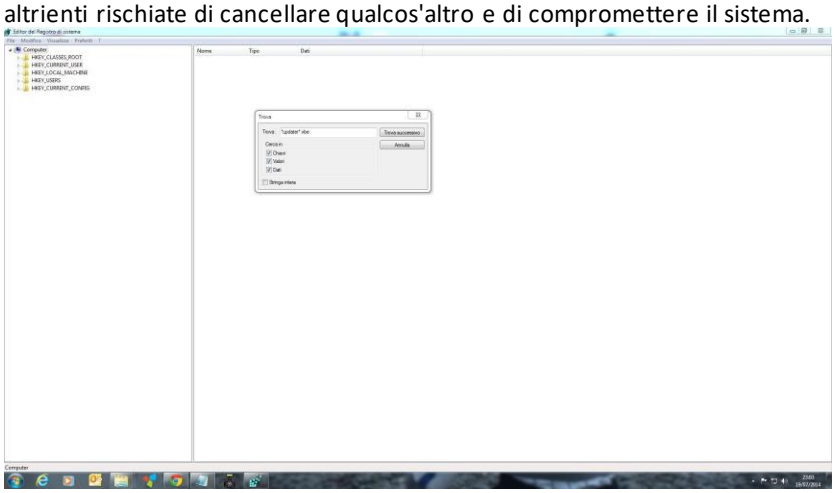
6-) Controllate che non sia presente la chiamata al virus updater.vbe in esecuzione automatica. (Cliccate sul pulsante di start e poi andate su "Tutti i programmi"e su "Esecuzione automatica". Se qui dentro trovate qualcosa che si riferisce a updater.vbe o a wscript.exe cancellatelo cliccandoci sopra con il tasto destro e poi con quello sinistro su "cancella". Attenzione a non cliccarci sopra con il tasto sx del mouse altrimenti lo manderete in esecuzione e dovrete ripetere la procedura da capo. **N.B.** : Non sempre il virus compare con il nome su citato ma potrebbe essere mascherato sotto qualche altra voce strana guardare attentamente se c'è qualche voce strana.

7-) Cliccate sempre sul pulsante di start e sul campo di ricerca file (a sx della lente di ingrandimento) scrivete *updater*.vbe (o la voce che avete trovato), poi cliccate subito sopra su "ulteriori risultati".Nella nuova finestra che apparirà cliccate su "computer" ed attendete il termine della ricerca. Ora cancellate i file correlati al virus che risulteranno dalla ricerca, fate sempre attenzione a non mandarli in esecuzione.



Poiché dovremo lavorare sul registro di sistema vi consiglio di riattivare il ripristino del sistema rifacendo il punto 2 al contrario. Vi consiglio anche di creare un punto di ripristino e poi di chiudere il tutto.
NOTA: Il virus potrebbe comparire con un nome diverso mediacandyphoto.exe o qualcosa di simile quindi attenzione a qualche voce strana qualora la individui elimina.

9-) Torniamo al pulsante di start e scriviamo nel campo di ricerca file "regedit" (senza virgolette) e premiamo in tasto invio sulla tastiera. Cliccare in alto su "modifica" e poi su "trova". Ora riscrivere la stringa: *updater*.vbe e cliccare sul tasto "trova". A questo punto bisogna cancellare tutti i risultati con il tasto DX del mouse e poi su "elimina", possiamo continuare la ricerca premendo il tasto F3 della tastiera e continuare così fino a quando non ci saranno più elementi trovati. Attenzione a scrivere correttamente la stringa da ricercare *updater*.vbe altrienti rischiate di cancellare qualcos'altro e di compromettere il sistema.



10) riavviare e controllare se il virus è ancora attivo ricontrollando i processi del sistema come al punto 3, in caso positivo ripetere dal punto 1, altrimenti proseguire

11) Durante il periodo in cui il vostro PC è stato infettato, tutti i dispositivi removibili (pennette, schede di memoria ecc.) in esso inseriti sono stati infettati, per cui bisogna ora pulirli. Inserite quindi la pendrive infettata ed apritela cliccandoci sopra con il tasto destro del mouse e poi su "Apri" (solo e soltanto su apri). Non fateci doppio click per nessun motivo e non apritela in nessun altro modo se non con quello appena descritto. Nella pendrive troverete il file updater.vbe, dovrete eliminarlo così come dovrete eliminare anche tutti i falsi collegamenti che ha creato il virus. (Il malware nasconde i file e li sostituisce con un falso collegamento) I collegamenti sono facilmente riconoscibili dalla freccetta in basso a sinistra

12a) Ora è venuta finalmente l'ora rendere visibili i vostri file. Come potrete notare sono ricomparsi i file sulla pennetta ma saranno visibili solo a chi a scelto di visualizzare i file nascosti come voi (infatti sono di un colore sbiadito). Per renderli definitivamente visibili vi basterà eseguire il file reset_attributi.bat disponibile in fondo all' articolo (solo per gli utenti registrati). Una volta scaricato il file sarà sufficiente scompattarlo ed eseguirlo come amministratore (tasto dx "esegui come amministratore). E' importante inserire prima la pendrive nel computer ed annotarsi la lettera ha cui è abbinata (di solito F ma potrebbe essere diversa). Il file è compatibile con versioni di windows successivi ad XP. Se avete qualche problema con il programmino passate pure al punto successivo, altrimenti saltate direttamente al punto 13

12b) Fate questa procedura solo se avete problemi con il punto 12a. Una volta inserita la pendrive avviate il prompt dei comandi con diritti di amministratore e dopo esservi portati dentro la pendrive digitate il comando: "attrib -R -S -H /s /d *.*" (senza virgolette) ed avrete finito la procedura con successo. Ricordatevi che il comando va eseguito dall' interno della pendrive, non digitatelo su C altrimenti renderete visibili i file nascosti e di sistema mettendo a rischio il sistema.

13) Reimpostare visualizzazione file invertendo le selezioni delle opzioni come al punto 1

14) Questo punto è facoltativo ma se vorrete approfittarne per ripulire il PC da altre infezioni potete scaricarvi il software combofix al link: http://www.bleepingcomputer.com/download/combofix/ (cliccate su download now), disattivate la connessione ad internet, disattivate momentaneamente il vostro antivirus ed eseguite Combofix. Al termine della scansione potrete riattivare tutto.

ATTENZIONE !!! AL FINE DI EVITARE DI BECCARVI NUOVAMENTE UPDATER.VBA ED ALTRE INFEZIONI SIMILI EVITATE SEMPRE DI FARE DOPPIO CLICK SELLE PENDRIVE O SU QUALSIASI DISPOSITIVO REMOVIBILE. IN QUESTO MODO NON VERRA' ELABORATO IL FILE AUTORUN.INF CHE SPESSO VIENE MODIFICATO DAL VIRUS PER MANDARSI IN ESECUZIONE. NEL CASO DI UPDATER NON BISOGNA CLICCARE ANCHE SUI COLLEGAMENTI ED E' FACILE CAPIRE SE SONO DEI FALSI COLLEGAMENTI POICHE' LA PENDRIVE CONTERRA' SOLO QUELLI (I FILE REALI SARANNO NASCOSTI).