

Virtualizzazione UAC

Concetti di base

Certi percorsi di programma di Windows 10 (di principio già a partire da Windows VISTA) potrebbero non essere scritti coi normali diritti di utente. Questa restrizione che, in pratica, implica che questi file possano essere modificati solo se si dispone dei diritti di amministratore, fa parte del concetto di sicurezza di Windows ed è chiamato UAC (User Account Control = Controllo Account Utente)

Ciò riguarda in particolare i seguenti percorsi

- C:\Windows
- C:\Program Files
- C:\Program Files (x86)

e forse altri percorsi critici del sistema.

Alcuni tipi di file potrebbero inoltre essere modificati solo coi diritti di amministratore, vale a dire

- EXE
- VBA
- BAT

fra gli altri, che sono per la maggior parte file eseguibili e che, nel peggiore dei casi, potrebbero contenere codici dannosi. Per informazioni più dettagliate si prega di voler consultare il documento di Mark Russinovich.

Il problema

In base a questo concetto, non è possibile trarre vantaggio dalla prassi ormai consolidata di salvare i dati utente come settaggi e opzioni di base nel percorso di programma se il programma non è stato avviato con i diritti di amministratore. Questa soluzione tampone ampiamente utilizzata per salvare i settaggi nel registro risente del medesimo principio. A volte non è sufficiente neanche essere loggati come amministratore del programma; quest'ultimo deve essere esplicitamente avviato con diritti molto alti, cliccando col tasto destro del mouse e poi su "Esegui come amministratore".

Il programma Metric non riesce ora a salvare i settaggi di base, quali i sistemi di misura, la calibrazione, il tempo di esposizione o il collegamento delle tavole di misura o dei comandi motore – Salva tutto come Metric.opt nel percorso del programma – con un'eccezione: il programma deve essere avviato con diritti elevati. Tuttavia, se l'utente normale potesse avviare il programma coi diritti di amministratore, ciò abbatterebbe il muro di sicurezza del sistema.

Per eliminare questo problema Microsoft ha creato la tecnica conosciuta come "Virtualizzazione UAC". Se un programma non dispone dei diritti necessari a scrivere o modificare un file nel percorso desiderato, una copia di questo file viene memorizzata in una posizione particolare e questa copia (o anche file non esistente nella directory di destinazione) viene mostrata a livello virtuale nella directory di destinazione.

Esempio: siete loggati come "YouAsAUser", con normali diritti di utente e desiderate salvare le impostazioni in Metric.opt. Dal momento che non è possibile farlo in "C:\Program files (x86)\Metric\Metric.opt", Windows salva una copia del file in

C:\Users\YouAsAUser\AppData\Local\VirtualStore\Program Files (x86)\Metric\Metric.opt

La virtualizzazione UAC salva il file in una posizione completamente differente.

Non fa alcuna differenza che l'amministratore abbia modificato il vostro permesso di scrittura in "C:\Program files (x86)\Metric". Windows riconosce automaticamente il percorso critico ed effettua la virtualizzazione per in vece

vostra. Come detto in precedenza, l'unica eccezione è quando si avvia Metric esplicitamente con diritti elevati, cosa vietata per motivi di sicurezza.

Se si prosegue e si carica il file da "C:\Program files (x86)\Metric\Metric.opt", Windows carica questo file dal virtual store.

Quali utenti singoli, la cosa risulta estremamente pratica. Da una parte c'è l'alto livello di sicurezza della virtualizzazione UAC e dall'altra è possibile mantenere la solita prassi e salvare i file e i settaggi nella directory di installazione.

Se, in questo caso, un altro utente si logga come "YourColleague", accadranno due cose:

1. al primo avvio di Metric, il vostro collega leggerà il file originariamente installato Metric.opt,
2. in fase di salvataggio, il vostro collega creerà un nuovo Metric.opt nel suo VirtualStore e questa copia sarà visibile solo a lui.

Ora esistono tre Metric.opt differenti: quello installato dal CD, la vostra copia privata e quella privata del vostro collega, anche se ognuno di voi vedrà solo un singolo Metric.opt nel percorso dell'applicazione. L'unica differenza sarà probabilmente la dimensione e la data di creazione.

Inoltre sussiste il vantaggio che il vostro collega non è in grado di modificare le vostre impostazioni. Comunque, se fosse necessario modificare le impostazioni di base come la calibrazione, l'azione deve essere effettuata separatamente per ogni collaboratore, il che potrebbe comportare molto lavoro qualora molti collaboratori eseguissero il loro lavoro su questa macchina.

Qualora la virtualizzazione UAC fosse un problema, è possibile aggirarla nel seguente modo.

La soluzione Escludi file UAC

Come detto in precedenza ci sono dei tipi di file che non vengono virtualizzati dall'UAC. Se si aggiunge OPT alla lista di questi tipi di file non si assisterà più alla virtualizzazione di Metric.opt (e tutti gli altri file aventi l'estensione opt).

Un utente con diritti normali ora non deve più cambiare le impostazioni. Solo l'amministratore può modificarli avviando il programma Metric con diritti elevati. Se questa è la soluzione desiderata, allora si è terminato il tutto. Il file "uac opt exclusion.reg" contiene la voce di registro che fa il lavoro in vece vostra e aggiunge l'estensione del file OPT alle estensioni escluse.

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\luafv\Parameters]
"ExcludedExtensionsAdd"=hex(7):6f,00,70,00,74,00,00,00,00,00
```

Questi caratteri esadecimali effettuano la codifica per la stringa "OPT" in formato DBCS e una stringa vuota. Cliccando due volte su questo file ed accettando tutte le richieste di UAC, questa voce entra a far parte del registro per cui, dopo aver effettuato un reboot finale, tutti gli effetti entreranno in atto.

La soluzione estesa "permesso di scrittura"

Se ai normali utenti fosse permesso modificare i settaggi di Metric, dovrebbero ottenere il permesso di scrittura nel percorso di installazione di Metric ("C:\Program files (x86)\Metric"). In questo caso "modifica/cambia" sarebbe sufficiente poiché non sarebbe più necessario salvare un nuovo set completo di impostazioni in un file differente. In questo modo, l'amministratore potrebbe garantire un minimo di diritti e non dovrà garantire l'accesso completo al percorso.