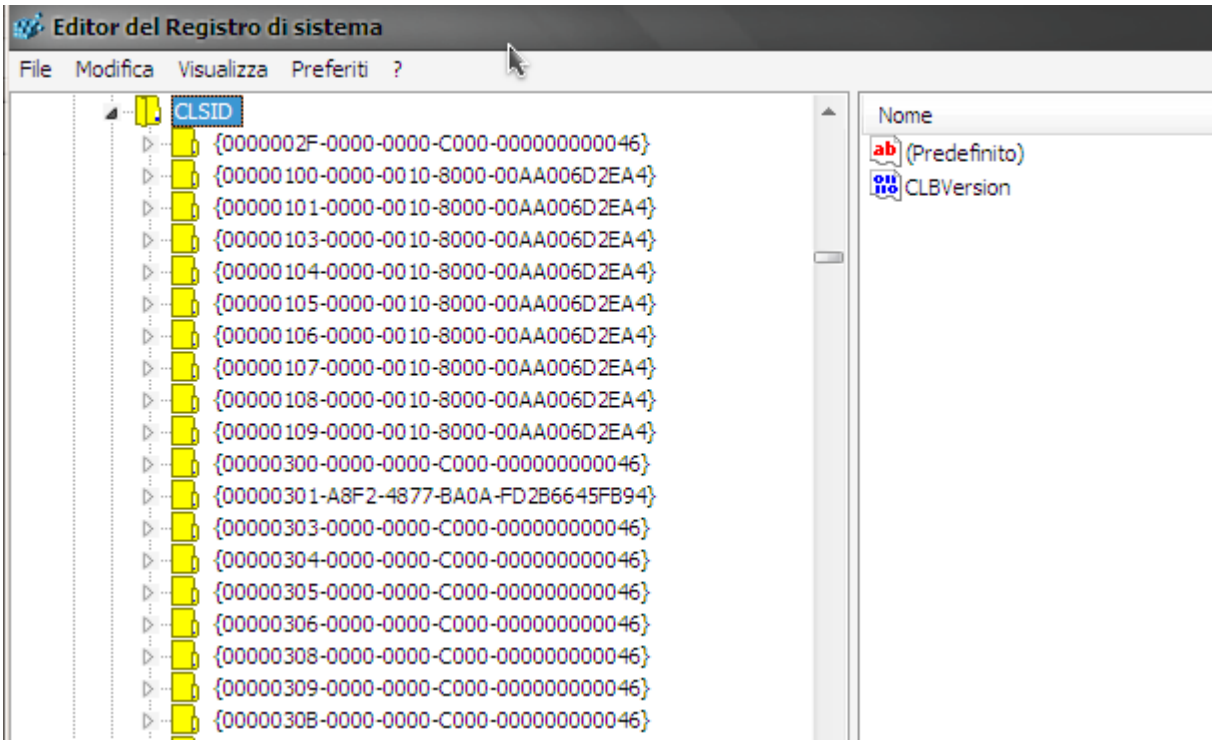
I CLSID e la GODMode di Windows 7

(I pericoli e le possibilità dei CLSID)

Augusto Scatolini (webmaster@comunecampagnano.it)
Ver. 1.0 Gennaio 2010



Il ClSID (Identificatore di Classe) è un codice di 128 bit, che viene utilizzato dal sistema operativo Microsoft Windows per riconoscere come maneggiare un file. Benché non molto famoso tra gli utenti medi, è il metodo più efficace e utilizzato per mascherare l'estensione di un file. Ciò può comportare un alto rischio per la sicurezza, poiché un file può essere mascherato da file immagine, mentre magari può essere un file eseguibile con codice ostile. Il problema che sta alla base dei rischi alla sicurezza derivati dall'utilizzo dei codici CLSID è che Microsoft Windows non visualizza mai i suddetti codici.

fonte: http://it.wikipedia.org/wiki/Clsid

Gli Identificatori di Classe CLSID sono un sottoinsieme degli Identificatori Unici Globali GUID i quali sono particolari identificatori usati nelle applicazioni software per permettere una referenza unica in ogni contesto.

fonte: http://en.wikipedia.org/wiki/Clsid

Alcuni esempi di codici CLSID (Class Identifier)

File audio Wav: {00020C01-0000-0000-C000-000000000046}
File di Word : {00020906-0000-0000-C000-000000000046}
Wordpad : {73FDDC80-AEA9-101A-98A7-00AA00374959}
File di Excel : {00020810-0000-0000-C000-000000000046}
Collegamento : {00021401-0000-0000-C000-000000000046}
File di Paint : {0003000A-0000-0000-C000-000000000046}
WM Player : {22D6F312-B0F6-11D0-94AB-0080C74C7E95}
Netscape : {481ED670-9D30-11ce-8F9B-0800091AC64E}
cestino win. : {645FF040-5081-101B-9F08-00AA002F954E}

i CLSID sono nel registro di Windows alla voce HKEY_CLASSES_ROOT\CLSID)

Per esempio per incorporare un file video in formato flash (quello più usato, quello di youtube per intenderci) su una pagina web (scritta quindi con codice HTML) è sufficiente incollare nella pagina il seguente codice:

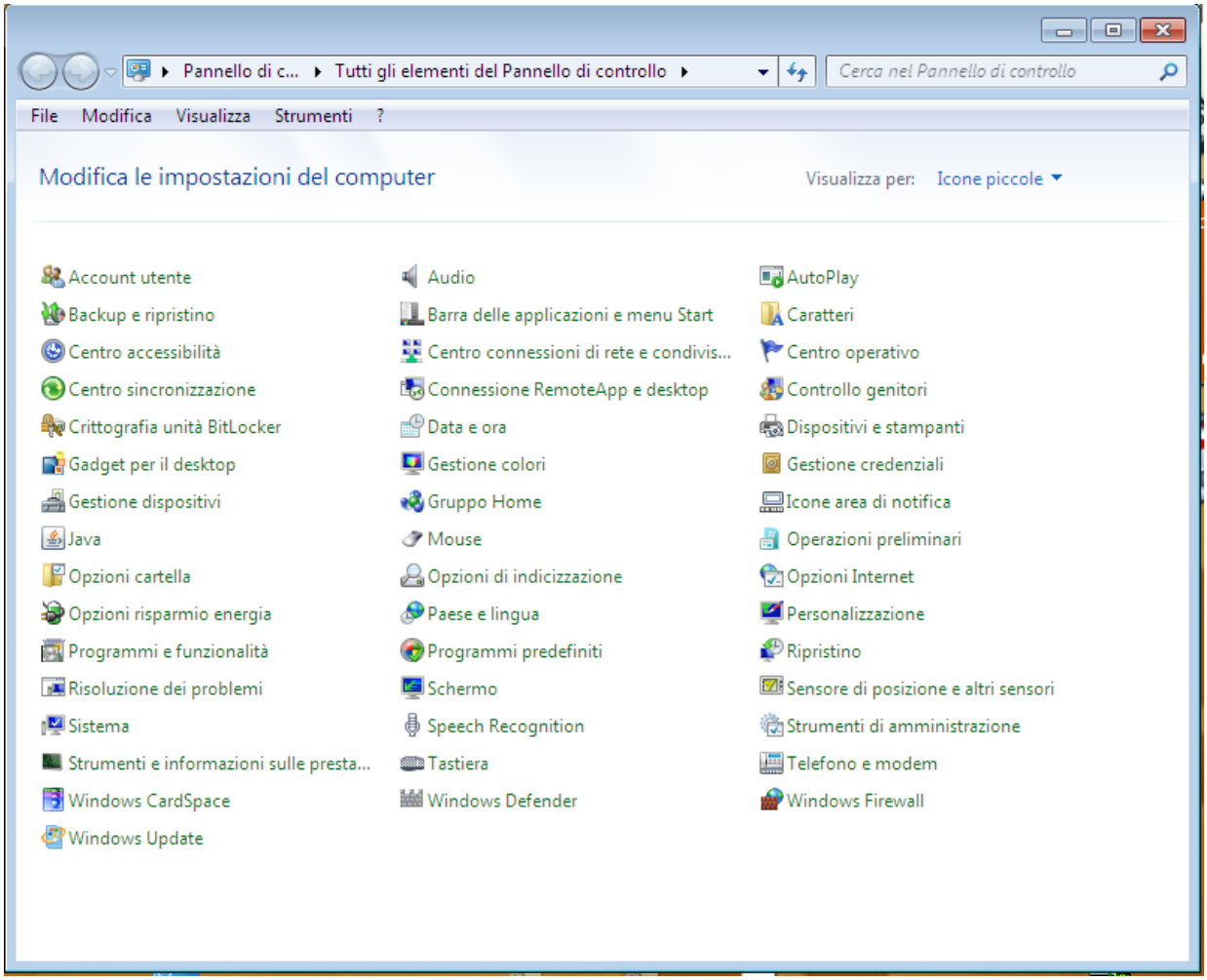
```
<OBJECT classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.ca
b#version=6,0,40,0" WIDTH="550" HEIGHT="400" id="myMovieName"><PARAM
NAME=movie VALUE="myFlashMovie.swf"><PARAM NAME=quality VALUE=high><PARAM
NAME=bgcolor VALUE=#FFFFFF><EMBED href="myFlashMovie.swf" quality=high
bgcolor=#FFFFFF WIDTH="550" HEIGHT="400" NAME="myMovieName" ALIGN=""
TYPE="application/x-shockwave-flash"
PLUGINSPAGE="http://www.macromedia.com/go/getflashplayer"></EMBED></OBJECT>
```

il CLSID D27CDB6E-AE6D-11cf-96B8-444553540000 è quello tipico di Shockwave Flash.
Quindi? Dove è il problema?
Il problema è che aprendo semplicemente una pagina web è possibile che il codice contenuto nella pagina attivi AUTOMATICAMENTE e senza alcun intervento da parte dell'utente il programma adatto alla visualizzazione del filmato in flash.
Dov'è il problema?
Il problema è che questo automatismo che senza dubbio è una facilitazione per l'utente può essere altrettanto automaticamente responsabile dell'apertura di qualsiasi file.
Inclusi quelli eseguibili.
Inclusi i virus.

Questa praticamente è una delle tecniche più utilizzate per diffondere virus, si confeziona una pagina web contenente un pezzo di codice simile a quello appena mostrato solo che invece del filmato il CLSID è quello di un programma “malevolo”. Poi si manda una mail formattata in HTML (quelle che vanno tanto di moda perché più carine di quelle classiche in ASCII” che già all'apertura potrebbe re-indirizzare alla pagina web contenente il virus, oppure potrebbe contenere un link alla pagina pericolosa oppure potrebbe avere la pagina pericolosa come allegato da aprire.

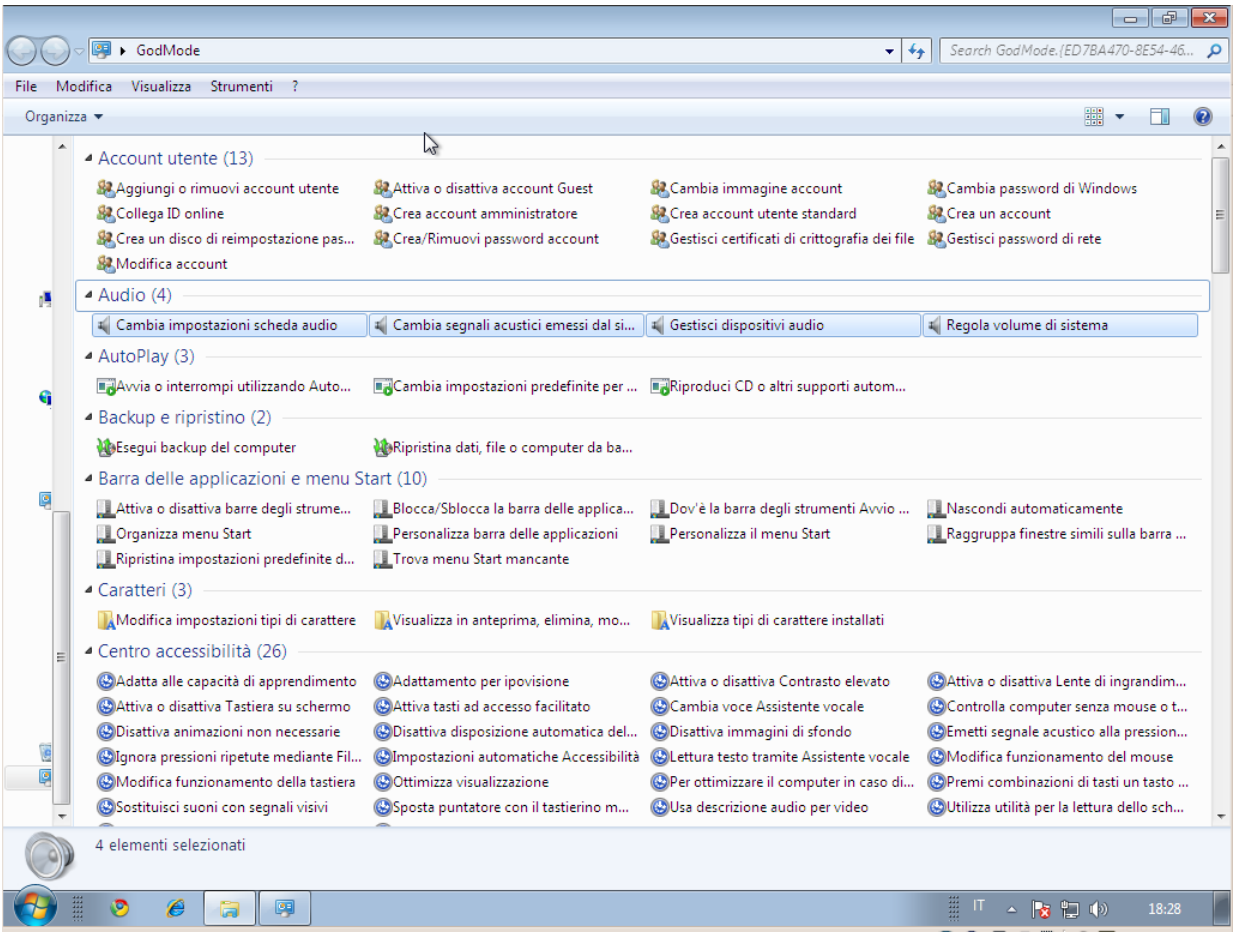
E' quello che succede ogni giorno.

Un'applicazione utile dei CLSID è quella per la quale si riesce ad attivare su Windows 7 (anche sul defunto Windows Vista) la cosiddetta modalità GODMODE che potrebbe essere tradotta in DIVINA.
E' stata chiamata così perché tramite una semplice procedura come la creazione di una cartella con estensione .{ED7BA470-8E54-465E-825C-99712043E01C} con qualunque nome si visualizza il contenuto della cartella di sistema “Pannello di Controllo” come una qualsiasi cartella e quindi molto più ricca e dettagliata.



Mentre aprendo la cartella

si vedrà



dove praticamente ogni voce del pannello di controllo è già esplosa nei rispettivi sottomenu. Tutto in unica e lunga pagina.

** attenzione – Il sistema è instabile (CRASH) su Vista Ultimate, Windows Server 2008 e Windows 7 a 64bit

FINE

altre miniguide
http://www.comunecampagnano.it/gnu/miniguide.htm