What is the strange garbage-looking string in the "command" value of a static verb?

devblogs.microsoft.com/oldnewthing/20140731-00

July 31, 2014

Raymond Chen

A customer from a major software vendor asked, “What is the significance of the `command` value that can be found under `HKCR\<progid>\shell\open\command`. It appears to be a copy of the default value, but with the program name replaced with apparent garbage. We’ve seen this both with Microsoft products as well as products by other companies. There is no mention of this value in the documentation on static verbs.”

Name	Type	Data
(Default)	REG_SZ	“C:\Program Files\Contoso\CONTOSO.exe” /NOLOGO “%1”
command	REG_MULTI_SZ	34GY`{XL?{Y)2S($,PP>c=@0l{Ja0N8KUwy@4JdO /NOLOGO “%1”

The customer didn’t explain why they were interested in this particular registry value. Maybe they thought it was enabling some super magical powers, and they wanted to get in on that action. (If that was the case, then they failed to notice that the same `command` value also existed in the verb registration *for their own program*!)

That strange garbage-looking string was placed there by Windows Installer (also known as MSI). It is the so-called Darwin descriptor that Windows Installer uses to figure out what program to run when the verb is invoked by the shell. For compatibility with programs that read the registry directly (because everybody knows that reading the registry is much cooler than using the API), the default value is set to something approximating the local executable’s path. That default value might be incorrect if the application has moved in the meantime, and it might be missing entirely if the application is marked as install-on-demand and has never been used, but at least it keeps those rogue programs working 99% of the time.

Raymond Chen

Follow