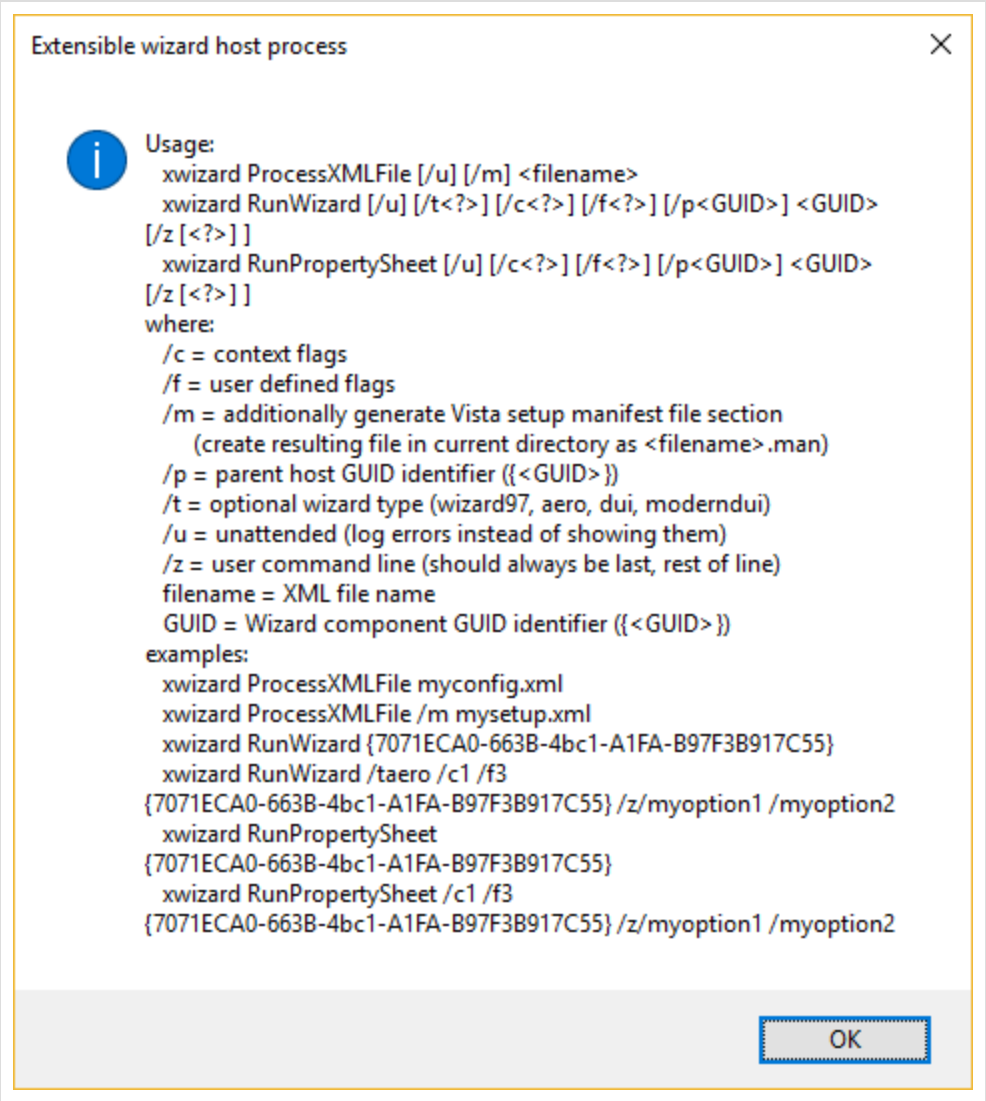
The Wizard of X – Oppa PlugX style

Xwizard is an 'Extensible wizard host process'. While I am not 100% sure what it is doing I know for certain that – whatever it is – PlugX guys would approve.

Why?

When you run it with a '/h' command line parameter, you will get this info:



Something about the unusual command line parameters described there caught my eye.

After a quick inspection I discovered why. The arguments are actually… names of functions exported from xwizards.dll!

Very nice!

And even nicer is the fact the LoadLibraryEx that loads that xwizards.dll finds its conveniently in the current path…

Ouch…

So… all you have to do is copy c:\WINDOWS\system32\xwizard.exe to your folder, drop your xwizards.dll DLL there and call xwizard.exe with at least two arguments.

And the Microsoft-signed xwizards.exe will load xwizards.dll of your choice…

This entry was posted in **Anti-***, **Compromise Detection**, **Forensic Analysis**, **Incident Response**, **Living off the land**, **Malware Analysis** by **adam**. Bookmark the **permalink**.