

Forum:[Hack Forums](#)

Thread: [What Does PEB Patching Do?](#)

Demoralise - November 21, 2014, 6:54 pm

Can somebody explain the purpose of PEB patching?

IAmNotHere - November 22, 2014, 1:37 am

If you PEB patch an internet connection will open a google search engine webpage, fills in the word "PEB patch" and give you the search results with an answer to your question.

Just kidding: As far as I know this is to access paths which aren't accessible normally.

salmoneus - November 22, 2014, 12:46 pm

PEB patching refers to any manipulation (patching) of values in the [Process Environment Block](#) (PEB) structure.

I am assuming the context to be that of a crypter.

It is necessary to preface the actual answer with a cursory overview of how a RunPE works. It starts a foreign process with the `CREATE_SUSPENDED` flag. Each process has a unique PEB, with specific environmental and contextual values that interact with the windows PE loader (not to mention, the actual application will use many of these values as well).

So if the application needs to access a field which corresponds to the hollowed process, the value retrieved from the PEB will not be what it would be if the process was running in its own context - therefore functionality will be lost. In order to correct many of the anomalies which occur when using process hollowing, some crypters will patch the relevant fields of the PEB in order to prevent loss of functionality and correct heuristic analysis.

The most common fields patched are located in the `RTL_USER_PROCESS_PARAMETERS` structure (ImagePathName + CommandLine), but there are many other fields that can be patched by a crypter. Note that the two fields mentioned are `UNICODE_STRING`s and should be treated as such.

Hope this helps, any further questions just ask. ?

©**Ratatouille™** - November 22, 2014, 12:50 pm

(Nov 22, 2014 01:46 PM)salmoneus Wrote: [CITE](#) PEB patching refers to any manipulation (patching) of values in the [Process Environment Block](#) (PEB) structure.

I am assuming the context to be that of a crypter.

It is necessary to preface the actual answer with a cursory overview of how a RunPE works. It starts a foreign process with the `CREATE_SUSPENDED` flag. Each process has a unique PEB, with specific environmental and contextual values that interact with the windows PE loader (not to mention, the actual application will use many of these values as well).

So if the application needs to access a field which corresponds to the hollowed process, the value retrieved from the PEB will not be what it would be if the process was running in its own context -

therefore functionality will be lost. In order to correct many of the anomalies which occur when using process hollowing, some crypters will patch the relevant fields of the PEB in order to prevent loss of functionality and correct heuristic analysis.

The most common fields patched are located in the RTL_USER_PROCESS_PARAMETERS structure (ImagePathName + CommandLine), but there are many other fields that can be patched by a crypter. Note that the two fields mentioned are UNICODE_STRINGS and should be treated as such.

Hope this helps, any further questions just ask. ?wow great reply man :)
you know what you're talking + 1 for you