TESTHOOK manual

This document has been compiled on 2023-09-03.

Contents

Section 1: Online help

```
TESTHOOK - Install test hooks not discoverable via AMIS
Free software by C. Masloch

Parameters:
        NN      Operate on interrupt number NNh
        x       (Literal 'x') Alias for switch /L=x
Switches:
        /N      Insert NOPs before ieStart
        /I      Make iHPFS style uninstalled header
        /L=x    Patch letter x into ieSignature
        /C      Update current installed handler (must be reachable)
        /U      Uninstall handler (must be reachable)
```

Section 2: Parameters

NN

A single interrupt number, consisting of one or two hexadecimal digits. Default if not specified is interrupt 21h. This can be specified with all switches, including `/C` and `/U`.

x

The literal letter ‘`x`’. This is an alias for the switch `/L=x`.

Section 3: Switches

3.1 Switch /N - Insert NOPs before ieStart

This switch, when specified without the `/U` switch, causes the program to modify the IISP-style header of the currently installed or to-be-installed hook. It will modify the entrypoint from 10EBh to 0EEBh and insert two NOP instructions (9090h) into the last two bytes (reserved) of the header. This makes for a non-standard IISP header. It also makes it so the indirect far jump instruction cannot be reached directly by following the short jump branch.

If both this switch and the `/I` switch are specified, the latter takes precedence.

3.2 Switch /I - Make iHPFS style uninstalled header

This switch, when specified without the `/U` switch, causes the program to modify the IISP-style header of the currently installed or to-be-installed hook. It will modify the entrypoint from 10EBh to EA90h. This makes for a non-standard IISP header, specifically an iHPFS-style uninstalled IISP header.

If both this switch and the `/N` switch are specified, this one takes precedence.

3.3 Switch /L=x - Patch letter x into ieSignature

This switch, when specified without the `/U` switch, causes the program to modify the IISP-style header of the currently installed or to-be-installed hook. It will change the IISP signature (usually "KB") by changing the first letter to the specified letter. For instance, `/L=A` would change the signature to "AB". Specifying a capital "K" as in `/L=K` will reset the signature to "KB", making it an IISP header again. Any other letter makes the header not recognised as an IISP header.

3.4 Switch /C - Update current installed handler

This switch causes the application to search for an existing hook. The interrupt number is parsed as usual, and must be specified to operate on another interrupt than the default interrupt 21h. The existing interrupt hook is searched by loading from the IVT, and then following IISP headers if any. (The full advanced deinstallation method of ecm TSRs is not used.)

Every handler encountered is compared in three ways to detect our hook:

- Offset matches 102h.
- Letter "B" of the IISP header signature matches. (The letter "K" can be changed by the user, so it need not match.)
- At the segment one paragraph below the handler segment, the MCB name "TESTHOOK" matches.

If the handler is found, it is updated according to the currently specified parameters and switches. Particularly, the switches /N, /I, and /L= are used.

If both this switch and the /U switch are specified, the latter takes precedence.

3.5 Switch /U - Uninstall handler

This switch causes the application to search for an existing hook. The interrupt number is parsed as usual, and must be specified to operate on another interrupt than the default interrupt 21h. The existing interrupt hook is searched in the same way as described for the /C switch.

If the handler is found, it is uninstalled by updating either the IVT or the IISP header that has the handler in its downlink. The lDebug debugger's Update IISP Header function is used if not writing to the IVT and the "ecm" "lDebug" AMIS multiplexer is detected. Finally, the memory block matching the segment of the handler is freed.

If both this switch and the /C switch are specified, this one takes precedence.

3.6 No switch - Install handler

If neither the /C switch nor the /U switch are specified, the application will install a hook. The interrupt number is parsed as usual, and must be specified to operate on another interrupt than the default interrupt 21h.

The handler is updated according to the currently specified parameters and switches. Particularly, the switches /N, /I, and /L= are used.

The application will free its environment block, and zero the PSP field referencing this block. It will also close all Process Handles up to the amount of PHT entries of the process. The MCB name of the PSP block is forced to "TESTHOOK". The application will then terminate with the int 21h function 31h, leaving resident 120h (288) Bytes plus the MCB.

Source Control Revision ID

hg 18bdec492f06, from commit on at 2023-09-03 12:44:56 +0200

If this is in ecm's repository, you can find it at https://hg.pushbx.org/ecm/testhook/rev/18bdec492f06