

[TOOL] Hook Explorer

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00090.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 30 Mar 2006 13:17:35 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Hook Explorer

SUMMARY

DETAILS

This is a small application designed to scan a single process looking for IAT or detours style hooks.

HookExplorer gives the user several scanning and display options.

When first run, HookExplorer will enumerate all of the loaded dlls in the process and scan their import tables for hijacked function pointers in the import address table (IAT). The first instruction for each function pointer is then disassembled and examined to try to detect standard detours style hooks which may be in place.

If the "scan all exports" checkbox was selected, then HookExplorer will also scan every function found in the images export table for detours style hooks. For dynamically loaded dlls, this may be the only test we can perform on them. Note that this option can take some extra time to perform, and cannot be added to an existing scan on the fly. Once you

[TOOL] Hook Explorer

check this option the current scan will not be updated and you will have to rescan the target process.

HookExplorer also supports 4 data display modes to help you examine the data. These options can be applied on the fly and will simply re-display the collected scan data.

Internally hooks are stored in 3 collections. The first collection saves references to all functions, the second only cross module hooks, and finally the third which applies a user defined filter list to the results.

The display options that relate to these collections are termed:

- 1) Standard
 - displays cross module and same module hooks
- 2) Use Ignore List
 - displays filtered cross module hooks only
- 3) Hide hooks from same module
 - displays cross module hooks (no filter)
- 4) Show All
 - same as standard mode except also displays all entries per dll, hooked or not

These options are represented by radio buttons and can be applied on the fly once a scan has finished.

The IgnoreList is loaded from the file IgnoreList.txt found in the applications home directory. This file lists the dlls which you trust and do not want displayed in the results when using the IgnoreList display option. It is recommended to use the full dll path to your trusted dlls in this file.

The ignorelist can be edited in notepad and can be updated on the fly to an existing scan. The edit button on the main interface will launch notepad on the file allowing you to edit it. Once you have made your updates, save your changes and hit the reload button which will reload the file and apply the filter to the current display results.

ADDITIONAL INFORMATION

The information has been provided by ideo defense labs.
To keep updated with the tool visit the project's homepage at:
<<http://labs.ideodefense.com/labs-software.php?show=19>>
<http://labs.ideodefense.com/labs-software.php?show=19>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.