

[REVS] Antidebugging For (M)asses – Protecting the Environment

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0081.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/17/05

To: list@securiteam.com

Date: 17 Mar 2005 11:53:43 +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>

Antidebugging For (M)asses – Protecting the Environment

SUMMARY

The whitepaper linked here provides a few examples for antidebugging techniques that can be used under the Windows operating system.

DETAILS

Introduction:

The number of computer hackers/crackers have reached a very high level recently. It is very hard to develop a product that will be secure against reverse engineering attacks, to be const-stricto it is surely impossible.

However, if we can, why not make their dirty work harder?

The paper discusses several techniques:

- * Open CSRSS.EXE to detect SEH debugger
- * Use the CheckRemoteDebuggerPresent API provided by Windows XP
- * Protect ExitProcess to detect Softice/D*

The whitepaper can be found at:

<<http://pb.specialised.info/all/articles/antid.txt>>

<http://pb.specialised.info/all/articles/antid.txt>

ADDITIONAL INFORMATION

The information has been provided by <mailto:bania.piotr@gmail.com> Piotr Bania.

The original article can be found at:

<<http://pb.specialised.info/all/articles/antid.txt>>

<http://pb.specialised.info/all/articles/antid.txt>

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.