

[TOOL] StMichael – LKM Rootkit Detector

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0003.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/01/05

To: list@securiteam.com

Date: 1 Nov 2005 16:27:27 +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>

StMichael – LKM Rootkit Detector

SUMMARY

DETAILS

StMichael is a LKM that attempts to provide a level of protection against kernel-module rootkits. It provides this protection by monitoring various portions of the kernel, and optionally the entire kernel text itself, for modifications that may indicate the presence of a malicious kernel module.

If rootkit-like activity is detected, StMichael will attempt to recover the kernel's integrity by rolling back the changes made to a previously known-good state.

The following is a brief list of the capabilities of the StMichael kernel module:

- * Can generate and check MD5, and optionally SHA1, checksum of various kernel data structures, such as the system call table, and filesystem call out structures
- * Can checksum (md5 only) the base kernel, and detect modifications to the kernel text such as would occur during a silvo-type attack.
- * Can backup a copy of the kernel, storing it in a weekly encrypted form, for later restoration if a catastrophic kernel compromise is detected.
- * Can detect the presence of simplistic kernel rootkits upon loading.

Securiteam: [TOOL] StMichael – LKM Rootkit Detector

- * Can modify the Linux kernel to protect immutable files from having their immutable attribute removed.
- * Can disable write-access to kernel memory through the /dev/kmem device.
- * Can conceal the Stmichael module and its symbols.
- * Can monitor kernel modules being loaded and unloaded to detect attempts to conceal the module and its symbols, and attempt to 'reveal' the hidden module.

StMichael works on Linux kernel, and can be downloaded at:

<http://prdownloads.sourceforge.net/stjude/StMichael_LKM-0.12.tar.gz?download>
http://prdownloads.sourceforge.net/stjude/StMichael_LKM-0.12.tar.gz?download

ADDITIONAL INFORMATION

The information has been provided by <<mailto:rodrigo@kernelhacking.com>>
Rodrigo Rubira Branco.

To keep updated with the tool visit the project's homepage at:

<<http://sourceforge.net/projects/stjude>>
<http://sourceforge.net/projects/stjude>

=====

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.