

[REVS] Polymorphic Shellcodes vs. Application IDS's

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0127.html>

From: support@securiteam.com

Date: 01/29/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 29 Jan 2002 21:27:21 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Polymorphic Shellcodes vs. Application IDS's

SUMMARY

An article on Polymorphic Shellcodes (shellcodes that utilize methods to hide the fact they are of binary form, and contain malicious code), and how IDSs can possibly detect them has been published by NGSec.

DETAILS

A document written by NGSec focuses on how IDS, under certain circumstances, can detect Polymorphic shellcodes. The document then goes through the three main parts of a polymorphic shellcode and analyzes IDSs' common problems to detect them.

ADDITIONAL INFORMATION

The document (white paper) can be downloaded from:

<<http://www.ngsec.com/whitepapers.html>>

<http://www.ngsec.com/whitepapers.html>

The information has been provided by <<mailto:labs@ngsec.com>> NGSEC Research Team.

Securiteam: [REVS] Polymorphic Shellcodes vs. Application IDS's

=====
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.

- **Previous message:** support@securiteam.com: "[EXPL] BadBlue Contains Multiple Security Vulnerabilities (Exploit code)"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)