

# [REVS] GDI+ JPEG Exploit Mutations Can Bypass Antivirus Tests

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0067.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 10/18/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 18 Oct 2004 14:52:13 +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>

-----

GDI+ JPEG Exploit Mutations Can Bypass Antivirus Tests

---

## SUMMARY

It seems that most Antivirus software is unable to detect variants of the JPEG exploit. An analysis of how this is accomplished is given below, outlining the general guidelines needed in order to create a variant that can slip by the Antivirus software.

## DETAILS

Changing some bytes in the known exploit

Most Antivirus vendors issue virus definitions for the publicly and well known JPEG exploit code which uses the string `\xFF\xFE\x00\x01` for the buffer overflow. When inspecting the relevant SNORT rule that detects the exploit, one can learn that there are in fact up to 7 mutations to the well known JPEG exploit. The SNORT rule can be found at

<http://www.snort.org/snort-db/sid.html?sid=2705>

<http://www.snort.org/snort-db/sid.html?sid=2705>.

Simply changin the `\xFE` byte to one of the following – `\xE1`, `\xE2`, `\xED` it is possible to evade many Antivirus software. In addition, variants exist with a `\x00` instead of `\x01` in the known pattern therefore it is

## Securiteam: [REVS] GDI+ JPEG Exploit Mutations Can Bypass Antivirus Tests

reasonable to assume that such a modification will help evade detection by an Antivirus.

Changing the location of the buffer overflow string

The original public exploit code uses a buffer overflow string near the beginning of the image file (after \xFF\xE0 , \xFF\xEC and \xFF\xEE markers). Apparently it is quite possible to create a malicious JPEG with a buffer overflow string located in different parts of the file, namely in the middle.

Using combinations of the above two techniques to certain degrees and on certain bits and pieces of data, many Antivirus scanners will fail to detect the modified JPEG exploit code, even though essentially it is the same. Andrey has provided two demonstration JPEG image files which are variants of the original and are based on combinations of modifications to the original file. The scan results on those files is shown below.

For 1.jpg:

This is the report of the scanning done over "1.jpg" (see Demo section) file that VirusTotal processed on 10/13/2004 at 18:54:56.

Antivirus Version Update Result

BitDefender 7.0 10.12.2004 –

ClamWin devel-20040922 10.12.2004 –

eTrust-Iris 7.1.194.0 10.13.2004 –

F-Prot 3.15b 10.13.2004 –

Kaspersky 4.0.2.24 10.13.2004 –

McAfee 4398 10.13.2004 Exploit-MS04-028

NOD32v2 1.893 10.13.2004 –

Norman 5.70.10 10.12.2004 –

Panda 7.02.00 10.13.2004 –

Sybari 7.5.1314 10.13.2004 –

Symantec 8.0 10.12.2004 Backdoor.Roxe

TrendMicro 7.000 10.12.2004 Exploit-MS04-028

For 2.jpg:

Results of a file scan

This is the report of the scanning done over "2.jpg" file that VirusTotal processed on 10/13/2004 at 18:56:32.

Antivirus Version Update Result

BitDefender 7.0 10.12.2004 –

ClamWin devel-20040922 10.12.2004 –

eTrust-Iris 7.1.194.0 10.13.2004 –

F-Prot 3.15b 10.13.2004 –

Kaspersky 4.0.2.24 10.13.2004 –

McAfee 4398 10.13.2004 Exploit-MS04-028

NOD32v2 1.893 10.13.2004 –

Norman 5.70.10 10.12.2004 –

Panda 7.02.00 10.13.2004 –

Sybari 7.5.1314 10.13.2004 –

Symantec 8.0 10.12.2004 Bloodhound.Exploit.13

TrendMicro 7.000 10.12.2004 Exploit-MS04-028

Securiteam: [REVS] GDI+ JPEG Exploit Mutations Can Bypass Antivirus Tests

A SANS GCIH paper will be published soon by Andrey with a full analysis of the evasion techniques on this matter.

ADDITIONAL INFORMATION

The information has been provided by <mailto:andrey@hiddenbit.org> Andrey Bayora.

=====

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.