

[NEWS] Evading the Norman SandBox Analyzer

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-03/msg00008.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 1 Mar 2007 18:44:46 +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>

Evading the Norman SandBox Analyzer

SUMMARY

The Norman SandBox Analyzer runs malicious code samples in an emulated environment while logging their actions. In practice it is more or less impossible to make an emulated environment perfectly similar to the real thing. It is possible to write malicious code that does not behave maliciously when run in the Sandbox Analyzer.

DETAILS

A sample evasion technique:

The following code creates the file c:\donothing.txt according to the Sandbox Analyzer, while it creates the file c:\breakstuff.txt on a real computer running a real copy of Windows.

```
unsigned char idt[6];
```

```
__asm  
{  
  sidt idt  
}  
if ((0x00 == idt[0]) && (0x08 == idt[1]))
```

[NEWS] Evading the Norman SandBox Analyzer

```
{  
fp = fopen("c:\\donothing.txt", "w");  
fclose(fp);  
}  
else  
{  
fp = fopen("c:\\breakstuff.txt", "w");  
fclose(fp);  
}
```

The problem in this particular case is the limit of the IDT. According to the Intel documentation: "Because IDT entries are always eight bytes long, the limit should always be one less than an integral multiple of eight (that is, $8N-1$).". However, the Sandbox Analyzer incorrectly uses a limit of 800h, which is not an integral multiple of eight minus one. Therefore it is trivial to create a piece of malware that does one thing in the Sandbox Analyzer and another thing completely in a real computer (or even in a virtual machine like VMware for that matter).

ADDITIONAL INFORMATION

The information has been provided by <<mailto:arne.vidstrom@xxxxxxxxxxxxxx>>
Arne Vidstrom.

The original article can be found at:
<<http://www.ntsecurity.nu/onmymind/2007/2007-02-27.html>>
<http://www.ntsecurity.nu/onmymind/2007/2007-02-27.html>

=====

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

=====
=====

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.