

Hacked?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2003-07/0086.html>

From: Mike MacDonald (*mike.macdonald_at_lmts.net*)

Date: 07/02/03

Date: Wed, 2 Jul 2003 12:45:09 -0400

We are running IIS5.0 on a W2K SP3 machine and recently experienced what seems to be an odd problem. First, the machine is stand-alone and not part of a domain. In addition it is in a DMZ behind a firewall and has been hardened. Only port 80 is open from the Internet. Front Page extensions are loaded and Front Page is used to create several of the pages.

Yesterday at 7:00AM an authorized user was publishing some content got locked out and called for assistance. When we got to the box we found that the administrator account (renamed) and some other accounts belonging to administrators were unable to logon. We checked the firewall logs and noticed no unusual activity. We then used a password recovery utility to unlock the administrator account. When we got in we noticed several events, including the one at the exact time the problem started:

Event Type: Success Audit
Event Source: Security
Event Category: Account Management
Event ID: 643
Date: 7/1/2003
Time: 7:01:49 AM
User: NT AUTHORITY\SYSTEM
Computer: CODPAF01
Description:
Domain Policy Changed: Password Policy modified
Domain: CODPAF01
Domain ID: CODPAF01\
Caller User Name: CODPAF01\$
Caller Domain: DMZGROUP
Caller Logon ID: (0x0,0x3E7)
Privileges: -

After reading up on this event it seems it is normal when Group Policies are applied successfully to the box that would make such a change. The problem there is that this machine is in its own workgroup in the DMZ and no group policies are being applied to the box. My assumption is that the same event would be triggered if it was a local security policy change, however according to the logs no one with authority to make such a change was logged

microsoft.public.inetserver.iis.security: Hacked?

in at the time. The only other log entry of concern came at the same time from the app log:

Event Type: Information

Event Source: SceCli

Event Category: None

Event ID: 1704

Date: 7/1/2003

Time: 7:01:49 AM

User: N/A

Computer: CODPAF01

Description:

Security policy in the Group policy objects are applied successfully.

Again, the problem here is that this machine is not in a domain and does not have GPO's being applied to it, all security policies are local and no one with privilege to change local security policies was logged in at the time.

Thanks in advance,

Mike MacDonald, MCSE, CCA