Alert
January 26, 2010

How Can I Tell if I Was Infected By Aurora?

McAfee Labs identified a zero-day vulnerability in Microsoft Internet Explorer that was used as an entry point for “Operation Aurora” to exploit Google and at least 30 other companies.

How can I tell if my systems were infected?

If you are a McAfee VirusScan Engine customer, verify that you are using .DAT 5864 released on January 18, 2010 (McAfee has provided protection to identify this as of release 5862 and is updating as we continue to debug the attack) and perform a full scan on all machines within your enterprise, starting with most sensitive servers. If you detect the following signatures triggered: Exploit-Comele, Roarur.dr or Roarur.dll, you very likely have an infected Aurora host and should reach out toMcAfee Foundstone, our vulnerability management and protection services division, for onsite Incident Response Services. You may also take advantage of McAfee’s free Stinger product, used to clean up an Operation Aurora-infected system.

If I’m not a McAfee customer…

If you are not a McAfee Virus Scan Engine customer and your anti-malware vendor does not provide comprehensive detection for Aurora binaries, you can perform filename and md5 hash searches on your servers to determine if you have any matches that way. You should ensure that the md5 hash matches along with the filename to avoid false positives, as the filenames themselves are not unique and are very common Windows OS and other legitimate program filenames. The list of files and hashes is as follows:

securmon.dll:
E3798C71D25816611A4CAB031AE3C27A

Rasmon.dll:
0F9C5408335833E72FE73E6166B5A01B

a.exe:
CD36A3071A315C3BE6AC3366D80BB59C

b.exe
9F880AC607CBD7CDFFFA609C5883C708

AppMgmt.dll
6A89FBE7B0D526E3D97B0DA8418BF851

A0029670.dll
3A33013A47C5DD8D1B92A4CFDCDA3765

msconfig32.sys
7A62295F70642FEDF0D5A5637FEB7986

VedioDriver.dll
467EEF090DEB3517F05A48310FCFD4EE

acelpvc.dll
4A47404FC21FFF4A1BC492F9CD23139C

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

Check for outbound Web communications

You can also check for outbound past or present Web communication or DNS resolutions of the following domains* known to be associated with the malware activity:

ftpaccess[dot]cc
360[dot]homeunix[dot]com
sl1[dot]homelinux[dot]org
ftp2[dot]homeunix[dot]com
update[dot]ourhobby[dot]com
ad01[dot]homelinux[dot]com
ads1[dot]homelinux[dot]org
ads1[dot]webhop[dot]org
aep[dot]homelinux[dot]com
aka[dot]homeunix[dot]net
alt1[dot]homelinux[dot]com
amd[dot]homeunix[dot]com
amt1[dot]homelinux[dot]com
amt1[dot]homeunix[dot]org
aop01[dot]homeunix[dot]com
aop1[dot]homelinux[dot]com
asic1[dot]homeunix[dot]com
bdc[dot]homeunix[dot]com
corel[dot]ftpaccess[dot]cc
ddd1[dot]homelinux[dot]com
demo1[dot]ftpaccess[dot]cc
du1[dot]homeunix[dot]com
fl12[dot]ftpaccess[dot]cc
ftp1[dot]ftpaccess[dot]cc
patch[dot]homeunix[dot]org
up1[dot]mine[dot]nu
hho1[dot]homeunix[dot]com
hp1[dot]homelinux[dot]org
i1024[dot]homeunix[dot]org
i1024[dot]homelinux[dot]com
ice[dot]game-host[dot]org
il01[dot]servebbs[dot]com
il01[dot]homeunix[dot]com
il02[dot]servebbs[dot]com
il03[dot]servebbs[dot]com
lih001[dot]webhop[dot]net
lih002[dot]webhop[dot]net
lih003[dot]webhop[dot]net
list1[dot]homelinux[dot]org
live1[dot]webhop[dot]org
patch1[dot]gotdns[dot]org
patch1[dot]ath[dot]cx
patch1[dot]homelinux[dot]org
ppp1[dot]ftpaccess[dot]cc
sc01[dot]webhop[dot]biz
temp1[dot]homeunix[dot]com
tor[dot]homeunix[dot]com
ttt1[dot]homelinux[dot]org
up01[dot]homelinux[dot]com
up1[dot]homelinux[dot]org
up1[dot]serveftp[dot]net
up2[dot]mine[dot]nu
update1[dot]homelinux[dot]org
update1[dot]merseine[dot]nu
jlop[dot]homeunix[dot]com
on1[dot]homeunix[dot]com
vm01[dot]homeunix[dot]com
vvpatch[dot]homelinux[dot]org
war1[dot]game-host[dot]org
xil[dot]homeunix[dot]com

*In the names above, "[dot]" is substituted for "." to protect users from accidentally clicking and launching malicious domains.

We recommend searching for outbound requests for, at minimum, the 12/10/09 to 1/6/10 timeframe. The above domains and file names and hashes may not be all inclusive of all those associated with Aurora but give a reasonable representation. If you see Web communication to any of the above sites you should analyze the origination machine immediately and reach out to McAfee Foundstone for onsite Incident Response Services.