McAfee Labs:
Combating Aurora

By Rohit Varma, McAfee Labs™

Contents

Combating Aurora

Overview

"Operation Aurora," released the week of January 11, exploits the recent Microsoft Internet Explorer vulnerability. The attack was initially targeted at several large companies, including Google. It is now public and is available on the web. The public release significantly increases the possibility of widespread attacks exploiting the vulnerability, putting Internet Explorer users at potentially serious risk.

Microsoft is aware of the targeted attacks and lists the following combinations as vulnerable: Internet Explorer 6 Service Pack 1 on Microsoft Windows 2000 Service Pack 4, and Internet Explorer 6, Internet Explorer 7 and Internet Explorer 8 on supported editions of Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2.

http://www.microsoft.com/technet/security/advisory/979352.mspx

Below we have a summary of McAfee's assessment of Internet Explorer and platform risks:

Platform	IE 6 Vulnerable	IE 7 Vulnerable	IE 8 Vulnerable
Windows 2000	High Risk	N/A	N/A
Windows XP	High Risk	High Risk	Medium Risk (DEP* Enabled w/ SP3)
Windows 2003	Medium Risk (DEP* Enabled)	Medium Risk (DEP* Enabled)	Medium Risk (DEP* Enabled)
Windows Vista	N/A	High Risk	Medium Risk (DEP* Enabled w/ SP1)
Windows 2008	N/A	N/A	Medium Risk (DEP* Enabled)
Windows 7	N/A	N/A	Medium Risk (DEP* Enabled)

* DEP

Data Execution Prevention (DEP) is a set of hardware and software technologies that perform additional checks on memory to help prevent malicious code from running on a system. In Microsoft Windows XP Service Pack 2 (SP2) and Microsoft Windows XP Tablet PC Edition 2005, DEP is enforced by hardware and by software.

The primary benefit of DEP is to help prevent code execution from data pages. Typically, code is not executed from the default heap and the stack. Hardware-enforced DEP detects code that is running from these locations and raises an exception when execution occurs. Software-enforced DEP can help prevent malicious code from taking advantage of exception-handling mechanisms in Windows.

McAfee detection names for Aurora

Exploit-Comele

This maliciously crafted script attempts to exploit the vulnerability when Internet Explorer handles certain DOM operations.

An attacker may exploit this issue to execute remote code.

http://vil.nai.com/vil/content/v_253210.htm

Roarur.dr

This Trojan drops further malicious files onto the victim's computer.

http://vil.nai.com/vil/content/v_253415.htm

Roarur.dll

This Trojan is dropped by the roarur.dr Trojan.

The dll creates an additional service on the victim's computer and checks for certain files on the system. The files it looks for are

- acelpvc.dll (presence of this file does not necessarily imply an infection) . acelpvc.dll is used to stream live desktop feeds to the attacker

- VedioDriver.dll (presence of this file does not necessarily imply an infection)- Helper dll for acelpvc.dll

http://vil.nai.com/vil/content/v_253416.htm

Aliases

Trojan.Hydraq

Symptoms

Outbound network connections to “hxxp://demo[remove].jpg”

The presence of the following files:

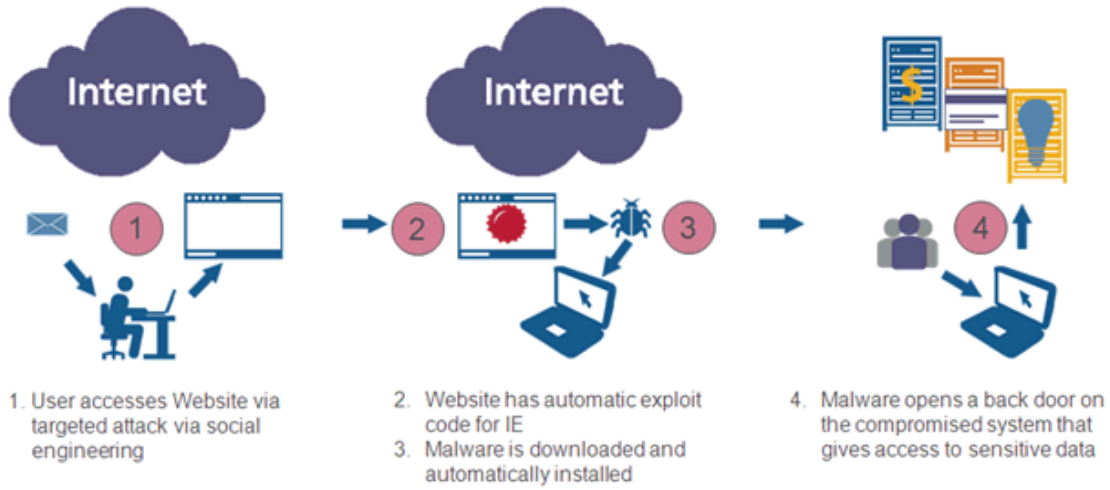
%SystemDir%\Rasmon.dll
%SYSDIR%\DFS.bat

The presence of the following registry keys:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RaS[% random 4 chars %]
  "ImagePath" = %SystemRoot%\svchost.exe -k netsvcs
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RaS[% random 4 chars %]
  "Start"= 02, 00, 00, 00
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RaS[% random 4 chars %]\Parameters "ServiceDll" = %SystemRoot%\rasmon.dll

Characteristics

Aurora demonstrates these four infection characteristics:



Common filenames and hashes

```
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

wuauclt.exe
69BAF3C6D3A8D41B789526BA72C79C2D

jucheck.exe
79ABBA920201031147566F5418E45F34

AdobeUpdateManager.exe
9A7FCEE7FF6035B141390204613209DA

zf32.dll
EB4ECA9943DA94E09D22134EA20DC602
```

* This data is subject to change.
* For the latest data, please visit McAfee Aurora site
  http://www.mcafee.com/us/threat_center/operation_aurora.html

McAfee product coverage for Aurora

The McAfee Labs Aurora Stinger tool

The Aurora Stinger tool detects and removes threats associated with "Operation Aurora" attacks.

http://download.nai.com/products/mcafee-avert/aurora_stinger.exe

Extended McAfee product coverage details:

McAfee Web Gateway. TrustedSource has coverage for domains and IP addresses that the malware contacts. Coverage for associated malware was released January 15 (as "BehavesLike.JS.Obfuscated.E"). Proactive coverage existed for some components (as "Trojan.Crypt.XDR.Gen").

McAfee Application Control. All versions of McAfee Application Control protect against infection, without requiring updates, and will prevent all versions of the Aurora attack witnessed to date.

McAfee Firewall Enterprise. TrustedSource has coverage for domains and IP addresses that the malware contacts. The embedded McAfee anti-virus scanning engine in Firewall Enterprise Version 7.0.1.02 and later provides coverage for supported protocols via standard McAfee DAT updates. Coverage for known exploits and associated malware is provided as Exploit-Comele, Roarur.dr, and Roarur.dll in the 5862 DATs, released January 15.

McAfee SiteAdvisor, SiteAdvisor Plus, SiteAdvisor Enterprise. TrustedSource has coverage for domains and IP addresses that the malware contacts.

McAfee Email and Web Security Appliances. TrustedSource has coverage for domains and IP addresses that the malware contacts.

Aurora coverage in McAfee point products:

Exploit-Comele Trojan

DAT files	Coverage is provided as Exploit-Comele in the 5860 DATs, released January 13, for known exploits.
VSE BOP	Out of scope
Host IPS	Out of scope
McAfee Network Security Platform	The UDS release of January 14 contains the signature "UDS-HTTP: Microsoft Internet Explorer HTML DOM Memory Corruption," which provides coverage.

McAfee Vulnerability Manager	Coverage not warranted at this time
MNAC 2.x	Coverage not warranted at this time
McAfee Remediation Manager	Malware coverage is out of scope.
McAfee Policy Auditor SCAP	Out of scope
MNAC SCAP	Out of scope

Roarur.dr Trojan

DAT files	Coverage is provided as Roarur.dr in the 5862 DATS, released January 15.
VSE BOP	Out of scope
Host IPS	Out of scope
McAfee Network Security Platform	McAfee Network Security Platform versions with Artemis enabled (6.0.x) provide coverage for this malware. Out of scope for prior versions.
McAfee Vulnerability Manager	Coverage not warranted
MNAC 2.x	Coverage not warranted
McAfee Remediation Manager	Malware coverage is out of scope.
McAfee Policy Auditor SCAP	Out of scope
MNAC SCAP	Out of scope

Roarur.dll Trojan

DAT files	Coverage is provided as Roarur.dll in the 5862 DATs, released January 15.
VSE BOP	Out of scope
Host IPS	Out of scope
McAfee Network Security Platform	McAfee Network Security Platform versions with Artemis enabled (6.0.x) provide coverage for this malware. Out of scope for prior versions.
McAfee Vulnerability Manager	The FSL/MVM package of January 15 includes a vulnerability check to assess if your systems are at risk.
MNAC 2.x	The MNAC release of February 10 will include a vulnerability check to assess if your systems are at risk.
McAfee Remediation Manager	Malware coverage is out of scope.
McAfee Policy Auditor SCAP	Out of scope
MNAC SCAP	Out of scope

Microsoft Internet Explorer DOM Operation Memory Corruption Vulnerability

Threat Identifier(s)	CVE-2010-0249
Threat Type	Vulnerability
Risk Assessment	High
Main Threat Vectors	E-Mail; Web
User Interaction Required	No
Description	A memory corruption vulnerability in some versions of Microsoft Internet Explorer may lead to remote code execution or an application crash. The flaw lies in Internet Explorer's handling of certain DOM operations. Exploitation can occur via a maliciously crafted file or a maliciously crafted web page and allow an attacker to execute arbitrary code. Failed exploit attempts may result in an application crash (denial of service).
Importance	High. On January 14 Microsoft publicly disclosed this vulnerability. Active exploitation has been observed in the wild.
McAfee Product Coverage *	
DAT files	Coverage for known exploits and associated malware is provided as Exploit-Comele, Roarur.dr, and Roarur.dll in the 5862 DATs, released January 15.
VSE BOP	Generic buffer overflow protection is expected to cover some, but not all, exploits.
Host IPS	Generic buffer overflow protection is expected to cover some, but not all, exploits.
McAfee Network Security Platform	Extended coverage is provided in the **January 18 UDS release via the signature "Microsoft Internet Explorer HTML DOM Memory Corruption III."** Coverage was originally provided in the UDS release of January 14.
McAfee Vulnerability Manager	The FSL/MVM package of January 14 includes a vulnerability check to assess if your systems are at risk.
MNAC 2.x	Under analysis
McAfee Remediation Manager	Remediation Manager provides mitigation for this issue by elevating Internet Explorer settings in the Internet and Local Intranet zones. A remedy for this issue will be provided upon release of an official vendor patch.

Cleaning and Repair

A full on-demand scan must run to completely clean an infected host. In some cases, it may also be necessary to run the on-demand scan in Safe Mode, as well as run a second scan after a reboot. It is critical that the on-demand scan be configured properly.

The proper configuration:

- Scan All Local Drives
- Memory for Rootkits
- Running Processes
- Registry
- First “Action” set to “Clean”

The full, recommended process:

- Launch a full on-demand scan with the prior-documented configuration
- Allow the scan to run to completion
- Reboot
- Launch a second on-demand scan and allow it to run to completion to verify that the system has been cleaned

Common URLs accessed

The following domains need to be blocked at the firewall:

```
360.homeunix.com
69.164.192.4
alt1.homelinux.com
amt1.homelinux.com
aop1.homelinux.com
app1.homelinux.com
blogspot.blogsite.org
filoups.info
ftp2.homeunix.com
ftpaccess.cc
google.homeunix.com
members.linode.com
sl1.homelinux.org
sl1.homelinux.org
tyuqwer.dyndns.org
update.ourhobby.com
voanews.ath.cx
webswan.33iqst.com:4000
yahoo.8866.org
ymail.ath.cx
yahooo.8866.org
sl1.homelinux.org
360.homeunix.com
ftp2.homeunix.com
update.ourhobby.com
connectproxy.3322.org
csport.2288.org
```

* This data is subject to change.
* For the latest data, please visit McAfee Aurora site
  http://www.mcafee.com/us/threat_center/operation_aurora.html

Appendix A: Useful URLs related to Aurora

http://www.mcafee.com/us/local_content/reports/how_can_u_tell.pdf
http://www.mcafee.com/us/threat_center/aurora_enterprise.html
http://newsroom.mcafee.com/article_display.cfm?article_id=3613
http://www.mcafee.com/us/threat_center/operation_aurora.html
http://www.avertlabs.com/research/blog/
http://www.microsoft.com/technet/security/advisory/979352.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0249
http://podcasts.mcafee.com/audioparasitics/AudioParasitics-Episode80-01-2010.mp3
http://community.mcafee.com/groups/operation-aurora