Testing Svchost: To Whom and Why?

Svchost.exe is the container that 'hosts' Microsoft's services. It has been involved in a number of different virus/trojan attacks, most notable of late is Conficker (***svchost.exe emphasized and underlined below)*** :

[From http://mtc.sri.com/Conficker/ :]

"**Figure 1** illustrates a flow diagram of the main thread for both variants of the Conficker agent, A and B. In both cases, the Conficker agent is distributed and run as a dynamically linked library. Its base code has been compiled as a DLL and its DLLMain function initiates the main thread represented by the diagram. The agent code proceeds by first checking the Windows version, and based on this result creates a remote thread in processes such as ***svchost.exe***. This is done by invoking LoadLibrary, where the copy of the DLL is passed as an argument. The malicious library then copies itself in the system root directory under a random file name. After initiating the use of Winsock DLL, the bulk of the malicious code logic is executed. "

From http://mtc.sri.com/Conficker/addendumC/index.html :]

"Conficker C installs itself into the user file system and configures the registry appropriately to invoke its DLL at host startup. It also inserts a variety of extraneous registry keys that are subsequently unused, presumably to cloak its presence (Obfuscating C's Installation and Its Presence). It copies itself into a randomly named DLL located in either the System32 directory, program files directory, or the user's temporary files folder. It deletes all restore points prior to its infection to thwart rollback. C then performs a simple validation of its DLL size, and suicides if this check fails. It sets the DLL's date to the same date as the local `kernel32.dll`, and sets NT File System (NTFS) file permissions on its stored file image to prevent write and delete privileges. Once installed, the DLL spawns a remote thread, which it attaches to the `netsvcs.exe` or ***svchost.exe*** process, depending on the OS version."

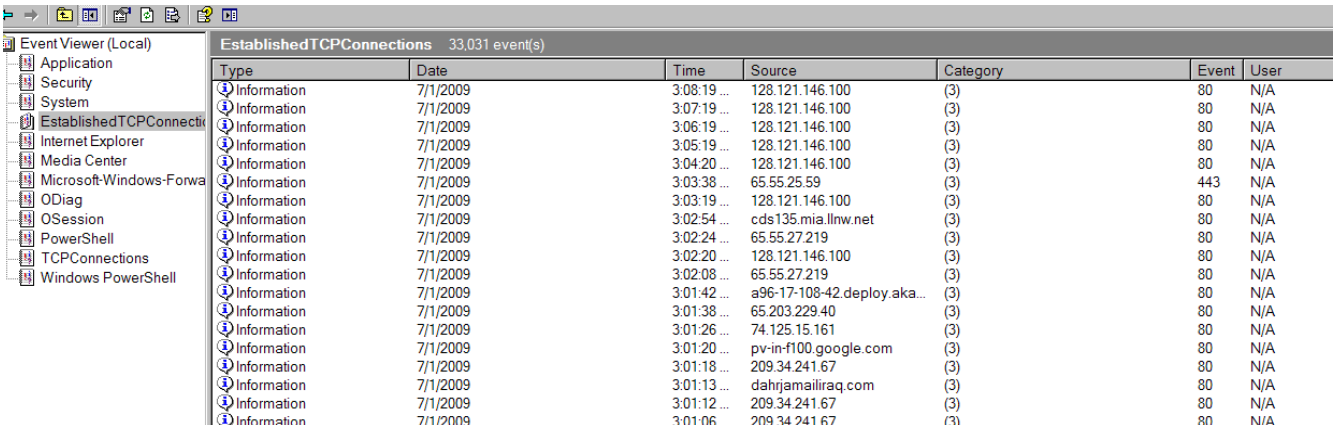
For some time, I have been running into Windows firewall generated messages like this in my event logs:

Event Type: Failure Audit
Event Source: Security
Event Category: Detailed Tracking
Event ID: 861
Date: 7/1/2009
Time: 3:02:03 PM
User: NT AUTHORITY\NETWORK SERVICE
Computer: RMFMEDIA
Description:
The Windows Firewall has detected an application listening for incoming traffic.

Name: -
Path: C:\WINDOWS\system32\svchost.exe
Process identifier: 1592
User account: NETWORK SERVICE
User domain: NT AUTHORITY
Service: Yes
RPC server: No
IP version: IPv4
IP protocol: UDP
Port number: 23691
Allowed: No
Usernotified:No

I have detailed tracking turned on in Auditing on my XP Pro SP3 installation, but since ICF (Windows Firewall) was blocking some of those connections, it was impossible for me to sniff what IP address to which svchost.exe was attempting a connect. A single svchost.exe instance can host multiple services,

making it difficult to segregate or map the application threads to individual processes. Because of this, I wrote a Powershell script to help me look at all established connections in Windows IP tables. Output looks something like below. Note the TCP established connections to a Microsoft IP (i.e. 65.55.25.59) and then to one of the 'CDN' (**C**ontent **D**elivery **N**etworks) that has close relationships with Microsoft: Limelight Networks (i.e. cds135.mia.llnw.net):



Event Viewer (Local)
- Application
- Security
- System
- EstablishedTCPConnecti
- Internet Explorer
- Media Center
- Microsoft-Windows-Forwa
- ODiag
- OSession
- PowerShell
- TCPConnections
- Windows PowerShell

EstablishedTCPConnections 33,031 event(s)

Type	Date	Time	Source	Category	Event	User
Information	7/1/2009	3:08:19 ...	128.121.146.100	(3)	80	N/A
Information	7/1/2009	3:07:19 ...	128.121.146.100	(3)	80	N/A
Information	7/1/2009	3:06:19 ...	128.121.146.100	(3)	80	N/A
Information	7/1/2009	3:05:19 ...	128.121.146.100	(3)	80	N/A
Information	7/1/2009	3:04:20 ...	128.121.146.100	(3)	80	N/A
Information	7/1/2009	3:03:38 ...	65.55.25.59	(3)	443	N/A
Information	7/1/2009	3:03:19 ...	128.121.146.100	(3)	80	N/A
Information	7/1/2009	3:02:54 ...	cds135.mia.llnw.net	(3)	80	N/A
Information	7/1/2009	3:02:24 ...	65.55.27.219	(3)	80	N/A
Information	7/1/2009	3:02:20 ...	128.121.146.100	(3)	80	N/A
Information	7/1/2009	3:02:08 ...	65.55.27.219	(3)	80	N/A
Information	7/1/2009	3:01:42 ...	a96-17-108-42.deploy.aka...	(3)	80	N/A
Information	7/1/2009	3:01:38 ...	65.203.229.40	(3)	80	N/A
Information	7/1/2009	3:01:26 ...	74.125.15.161	(3)	80	N/A
Information	7/1/2009	3:01:20 ...	pv-in-f100.google.com	(3)	80	N/A
Information	7/1/2009	3:01:18 ...	209.34.241.67	(3)	80	N/A
Information	7/1/2009	3:01:13 ...	dahrjamailiraq.com	(3)	80	N/A
Information	7/1/2009	3:01:12 ...	209.34.241.67	(3)	80	N/A
Information	7/1/2009	3:01:06 ...	209.34.241.67	(3)	80	N/A

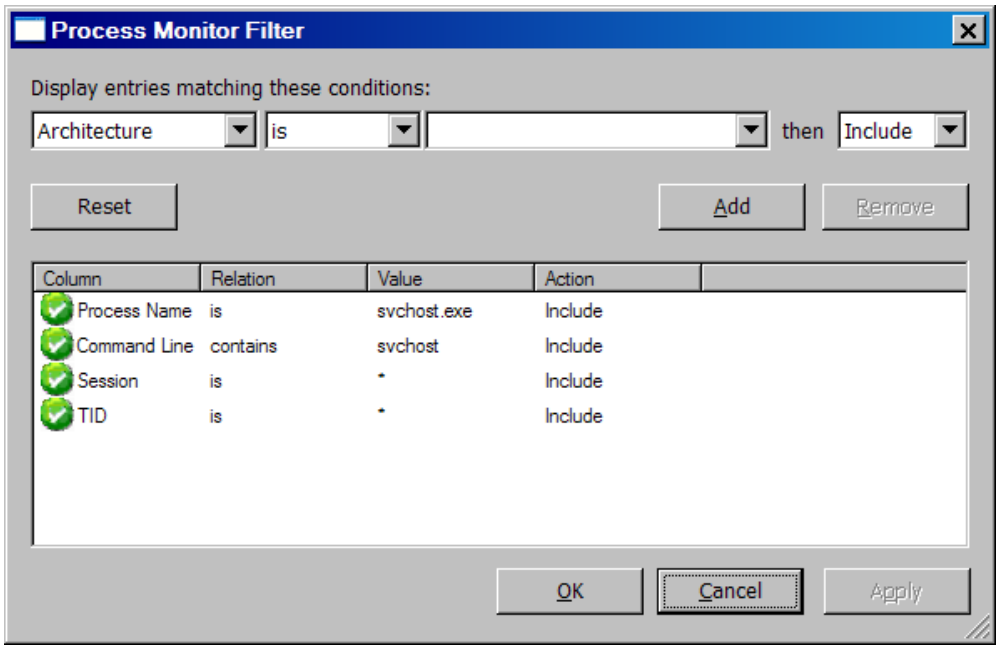
Among tools most helpful in examing svchost.exe from System Internals (from Microsoft) are Procmon, Procexplorer, Vmmap and the GWMI commands in Powershell. Some relatively simple Powershell code helps us understand the svchost processes. You will need a large screen to display this output:

```
$global:svchost = get-wmiObject win32_process -filter "name='svchost.exe'"
$global:win32_handle = $svchost | foreach { gwmi -query "Select * from win32_service where processID = $($_.handle)" }
$global:Sort_handle = $win32_handle | sort processID, Name
$global:Sort_svchost = $svchost | sort processID
$Sort_handle | format-table processID,name,state, startmode,Started,AcceptStop,Description -AutoSize
$Sort_svchost | format-table
ProcessID,ThreadCount,HandleCount,WS,VM,KernelModeTime,ReadOperationCount,ReadTransferCount,OtherTransferCount -Autosize
```

[Output]:

```
processID name state startmode Started AcceptStop Description
--------- ---- ----- --------- ------- ---------- -----------
840 SSDPSRV Running Manual True True Enables discovery of UPnP devices on your home network.
1168 stisvc Running Auto True True Provides image acquisition services for scanners and cameras.
1204 DcomLaunch Running Auto True False Provides launch functionality for DCOM services.
1292 RpcSs Running Auto True False Provides the endpoint mapper and other miscellaneous RPC services.
....
ProcessID ThreadCount HandleCount WS VM KernelModeTime ReadOperationCount ReadTransferCount OtherTransferCount
--------- ----------- ----------- -- -- -------------- ------------------- ------------------ -------------------
840 9 236 6078464 39940096 468750 369 48936 129130
1168 5 210 6574080 41291776 11093750 438 53831 32770
1204 5 209 6381568 43548672 3125000 383 53947 330048
1292 10 457 7004160 45506560 24375000 506 465380 63666
```

Procmon (sysinternals.com) is a powerful utility that allows us to filter processes in Windows for specific tracking. My Procmon filter looks like this:

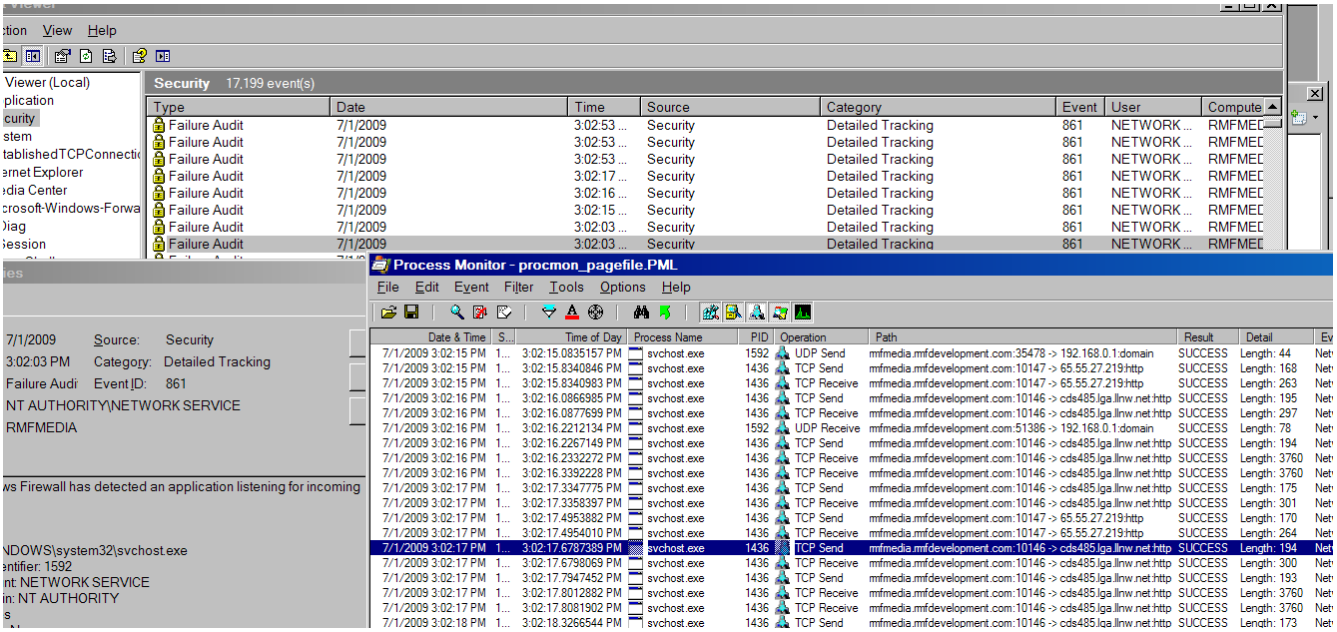


Output from this filter reveals when svchost.exe initiates a network connection. Some sample output:

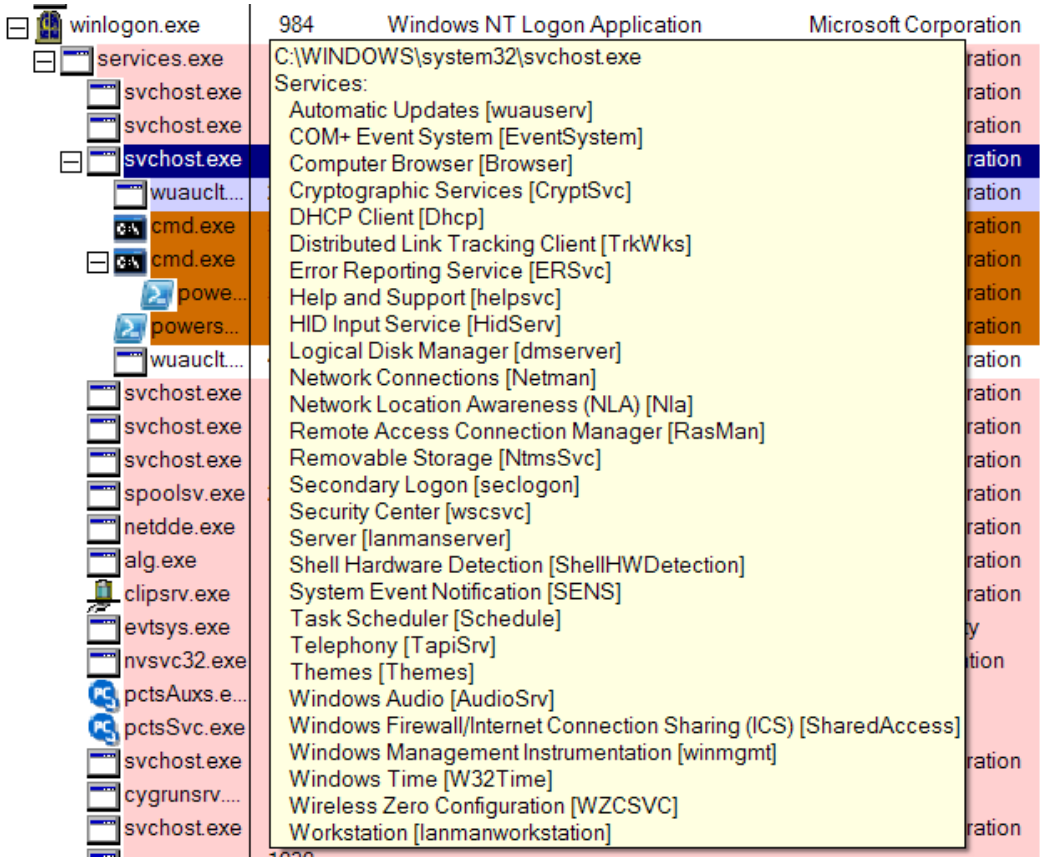
"7/1/2009 3:02:15 PM","n/a","3:02:15.8340983 PM","svchost.exe","1436","TCP Receive","rmfmedia.rmfdevelopment.com:10147 -> 65.55.27.219:http","SUCCESS","Length: 263","Network","C:\WINDOWS\System32\svchost.exe","NT AUTHORITY\SYSTEM","00000000:000003e7","1028","C:\WINDOWS\System32\svchost.exe -k netsvcs","","0","0"

"7/1/2009 3:02:16 PM","n/a","3:02:16.0866985 PM","svchost.exe","1436","TCP Send","rmfmedia.rmfdevelopment.com:10146 -> cds485.lga.llnw.net:http","SUCCESS","Length: 195","Network","C:\WINDOWS\System32\svchost.exe","NT AUTHORITY\SYSTEM","00000000:000003e7","1028","C:\WINDOWS\System32\svchost.exe -k netsvcs","","0","0"

The first communication by svchost.exe PID: 1436 is receiving data over port 80 (http) from 65.55.27.219 (Microsoft). The second communication is sending data to cds485.lga.llnw.net. (a 'CDN' Limelight networks) also on port 80. What data is my PC receiving and sending and why? We can certainly see from Procmon and Event viewer that svchost PID 1436 is sending and receiving data to and from various Microsoft and Limelight hosts.:



What can 'Process explorer' tells us about svchost PID 1436? This svchost.exe instance has an inordinate amount of services inside of it. :



But the process (**wuauclt.exe**) of the service (**wuauserv**) hosted by svchost.exe that is talking to Microsoft and Limelight networks runs as needed. Therefore, we only see this process if detailed

tracking is requesting via auditing. And generally we only see the procmon entries if we un-hibernate the computer with procmon previously running. However, I found I could re-initialize the update process and 'CDN' based connections from my PC with the following commands below (See http://technet.microsoft.com/en-us/library/cc720477(WS.10).aspx):

net stop wuauserv
net start wuauserv
wuauclt /detectnow

The **EventViewer** shows that at 8:13 AM the update service (**wuauclt.exe**) started and then finished/exited at 8:20 AM. In the event logs below, I had just 'un-hibernated' but had yet to log on:

Event Type: Success Audit
Event Source: Security
Event Category: Detailed Tracking
Event ID: 592
Date: 7/7/2009
Time: 8:13:04 AM
User: NT AUTHORITY\SYSTEM
Computer: RMFMEDIA
Description:
A new process has been created:
New Process ID: 5060
Image File Name: C:\WINDOWS\system32\wuauclt.exe
Creator Process ID: 1436
User Name: RMFMEDIA$
Domain: RMFDEVELOPMENT
Logon ID: (0x0,0x3E7)

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

Event Type: Success Audit
Event Source: Security
Event Category: Detailed Tracking
Event ID: 593
Date: 7/7/2009
Time: 8:20:39 AM
User: NT AUTHORITY\SYSTEM
Computer: RMFMEDIA
Description:
A process has exited:
Process ID: 5060
Image File Name: C:\WINDOWS\system32\wuauclt.exe
User Name: RMFMEDIA$
Domain: RMFDEVELOPMENT
Logon ID: (0x0,0x3E7)

Microsoft uses Limelight Networks (among others) to help them distribute update content. What I do not like about this is that when you enable Microsoft update you do not explicitly give Microsoft permission to use a third party CDN to send and receive data from your PC. But that is exactly what happens in the world of Edge Networks, 'CDNs', 'Software Ecosystems' and 'Cloud computing'. Data from my computer is sent elsewhere without my permission to network locations that are not local to the Pacific Northwest or necessarily controlled by the Software vendor of which I have service level agreements:

[**grepped/awked** output from ' *pcregrep cds July072009PMLSvchostOnly.CSV | gawk -F"," '{print $1","$7 "," $9}'* ']

"7/7/2009 8:13:54 AM","rmfmedia.rmfdevelopment.com:12344 -> cds423.dal.llnw.net:http","Length: 173"
"7/7/2009 8:13:54 AM","rmfmedia.rmfdevelopment.com:12344 -> cds423.dal.llnw.net:http","Length: 297"
"7/7/2009 8:13:55 AM","rmfmedia.rmfdevelopment.com:12344 -> cds423.dal.llnw.net:http","Length: 195"
"7/7/2009 8:13:55 AM","rmfmedia.rmfdevelopment.com:12344 -> cds423.dal.llnw.net:http","Length: 297"
"7/7/2009 8:13:55 AM","rmfmedia.rmfdevelopment.com:12344 -> cds423.dal.llnw.net:http","Length: 194"
"7/7/2009 8:13:55 AM","rmfmedia.rmfdevelopment.com:12344 -> cds423.dal.llnw.net:http","Length: 3760"
"7/7/2009 8:13:55 AM","rmfmedia.rmfdevelopment.com:12344 -> cds423.dal.llnw.net:http","Length: 3760"
"7/7/2009 8:13:55 AM","rmfmedia.rmfdevelopment.com:12344 -> cds423.dal.llnw.net:http","Length: 13746
"....

Procmon log [partial results from "TCP' grep]

"7/7/2009 8:13:36 AM","n/a","8:13:36.8479797 AM","svchost.exe","1436","TCP Send","rmfmedia.rmfdevelopment.com:12341 -> 65.55.184.27:http","SUCCESS","Length: 366","Network","C:\WINDOWS\System32\svchost.exe","NT AUTHORITY\SYSTEM","00000000:000003e7","1028","C:\WINDOWS\System32\svchost.exe -k netsvcs","","0","0"
"7/7/2009 8:13:36 AM","n/a","8:13:36.8479817 AM","svchost.exe","1436","TCP Send","rmfmedia.rmfdevelopment.com:12341 -> 65.55.184.27:http","SUCCESS","Length: 1607","Network","C:\WINDOWS\System32\svchost.exe","NT AUTHORITY\SYSTEM","00000000:000003e7","1028","C:\WINDOWS\System32\svchost.exe -k netsvcs","","0","0"
"7/7/2009 8:13:36 AM","n/a","8:13:36.8505359 AM","svchost.exe","1436","TCP Receive","rmfmedia.rmfdevelopment.com:12341 -> 65.55.184.27:http","SUCCESS","Length: 1072","Network","C:\WINDOWS\System32\svchost.exe","NT AUTHORITY\SYSTEM","00000000:000003e7","1028","C:\WINDOWS\System32\svchost.exe -k netsvcs","","0","0"
"7/7/2009 8:13:36 AM","n/a","8:13:36.8513039 AM","svchost.exe","1436","TCP Disconnect","rmfmedia.rmfdevelopment.com:12341 -> 65.55.184.27:http","SUCCESS","Length: 0","Network","C:\WINDOWS\System32\svchost.exe","NT AUTHORITY\SYSTEM","00000000:000003e7","1028","C:\WINDOWS\System32\svchost.exe -k netsvcs","","0","0"
"7/7/2009 8:13:54 AM","n/a","8:13:54.4318157 AM","svchost.exe","1436","TCP Send","rmfmedia.rmfdevelopment.com:12344 -> cds423.dal.llnw.net:http","SUCCESS","Length: 173","Network","C:\WINDOWS\System32\svchost.exe","NT AUTHORITY\SYSTEM","00000000:000003e7","1028","C:\WINDOWS\System32\svchost.exe -k netsvcs","","0","0"
"7/7/2009 8:13:54 AM","n/a","8:13:54.4327594 AM","svchost.exe","1436","TCP Receive","rmfmedia.rmfdevelopment.com:12344 -> cds423.dal.llnw.net:http","SUCCESS","Length: 297","Network","C:\WINDOWS\System32\svchost.exe","NT AUTHORITY\SYSTEM","00000000:000003e7","1028","C:\WINDOWS\System32\svchost.exe -k netsvcs","","0","0"
"7/7/2009 8:13:54 AM","n/a","8:13:54.8722381 AM","svchost.exe","1436","TCP Send","rmfmedia.rmfdevelopment.com:12345 -> 65.55.184.27:http","SUCCESS","Length: 168","Network","C:\WINDOWS\System32\svchost.exe","NT AUTHORITY\SYSTEM","00000000:000003e7","1028","C:\WINDOWS\System32\svchost.exe -k netsvcs","","0","0"
"7/7/2009 8:13:54 AM","n/a","8:13:54.8722499 AM","svchost.exe","1436","TCP Receive","rmfmedia.rmfdevelopment.com:12345 -> 65.55.184.27:http","SUCCESS","Length: 263","Network","C:\WINDOWS\System32\svchost.exe","NT AUTHORITY\SYSTEM","00000000:000003e7","1028","C:\WINDOWS\System32\svchost.exe -k netsvcs","","0","0"
"7/7/2009 8:13:55 AM","n/a","8:13:55.0042759 AM","svchost.exe","1436","TCP Send","rmfmedia.rmfdevelopment.com:12344 -> cds423.dal.llnw.net:http","SUCCESS","Length: 195","Network","C:\WINDOWS\System32\svchost.exe","NT AUTHORITY\SYSTEM","00000000:000003e7","1028","C:\WINDOWS\System32\svchost.exe -k netsvcs","","0","0"
"7/7/2009 8:13:55 AM","n/a","8:13:55.0051924 AM","svchost.exe","1436","TCP Receive","rmfmedia.rmfdevelopment.com:12344 -> cds423.dal.llnw.net:http","SUCCESS","Length: 297","Network","C:\WINDOWS\System32\svchost.exe","NT AUTHORITY\SYSTEM","00000000:000003e7","1028","C:\WINDOWS\System32\svchost.exe -k netsvcs","","0","0"
…..

Windows Firewall log

Because these TCP requests are initiated by Microsoft's update service (**wuauclt.exe)** on port 80 (http)**,** they are not blocked by Windows Firewall, although they are logged.

2009-07-07 08:13:35 OPEN TCP 192.168.0.8 65.55.184.27 12341 80 - - - - - - - - -
2009-07-07 08:13:36 CLOSE TCP 192.168.0.8 65.55.184.27 12341 80 - - - - - - - - -
2009-07-07 08:13:53 OPEN TCP 192.168.0.8 68.142.123.66 12344 80 - - - - - - - - -
2009-07-07 08:13:53 OPEN TCP 192.168.0.8 65.55.184.27 12345 80 - - - - - - - - -

To be continued...