Windows Administrators Meeting
December 10, 2004
Updated: December 13, 2004
Notes (taken by Steve Kunz)

Meeting Started (9:00)

Announcements

- On Monday, January 3, 2005, there will be electrical power work in Durham Center. No service outage is anticipated if all goes smoothly for the electricians. The UPS power supplies in the Durham machine room should handle the short outage anticipated. However, people should be aware that there is a remote possibility of a major service outage this evening if "things go wrong". See the following "Inside Iowa State" article for more information:

  http://www.iastate.edu/Inside/04/1210/upgrade.shtml

- Kunz announced that Windows infrastructure hardware upgrades for the SUS and WINS servers are planned in the coming months. In addition, a new WUS service (Windows Update Services, the next generation of SUS) is planned for production service as soon as the product is released and tested. More on schedules as the work progresses. The SUS server will be the first to be replaced (hardware is already on order).

MarketScore

Wayne Hauber (AIT) talked about a new security concern on campus called "MarketScore". MarketScore is "market analysis service" that installs software on a client computer under the guise of "speeding up your web browser". What the product actually does is configure the client system to use a "proxy server" at MarketScore. After the user gives permission to install the software, a program called "mkse.exe" and a root certificate (for MarketScore or NetSetter) and some DLLs are installed. The end result is that all SSL traffic is redirected to MarketScore systems via the Windows proxy mechanism (both to and from the final endpoint). MarketScore then claims it uses this data stream for "market analysis". Locally at ISU this means traffic for such things as WebMail and AccessPlus are redirected to MarketScore. Other SSL secure traffic (to your bank from a compromised home system, for example) is also redirected. The user sees little difference in their web-browsing (but all the traffic is going through MarketScore).

This is bad enough, but the real danger is that after decrypting the SSL traffic on the client system, the previously encrypted data steam is sent to MarketScore in clear text. This exposes items such as SSNs, passwords, bank account numbers, etc. to any listener over the public network (and at MarketScore).

Both AIT and ATS view this product as a serious concern. AIT is looking at blocking traffic to and/or from MarketScore systems. However, simply blocking MarketScore traffic without removing the product breaks network communication for that system (since it is configured to go to MarketScore's proxy servers). The product needs to be uninstalled (which can be a complex process).

Mike Bowman has list of systems by subnet (about 80 on-campus, about 160 residence hall systems) that are communicating with MarketScore systems. If you are concerned any of your systems may be compromised Mike can check the list (send email to mbowman@iastate.edu). For self analysis, you can look at the installed root certificates within your web-browser for certificates owned by "MarketScore" and "NetSetter". Hauber says "TCPview" is a good tool to see if mkse.exe connecting to the external MarketScore site.

AIT and ATS are working on procedures to detect and remove MarketScore. More information will be forthcoming as soon as it is available. This item will also be a topic at the next CCSG meeting (Dec 14).

Dave Orman (CNDE) asked if anyone was looking at legal aspects of what MarketScore was doing. Bowman indicated "not currently". It is felt that since the user actually gives permission for the use of the MarketScore proxy, legal arguments may be hard to apply.

Login Delays on XP SP2 Domain-Member Systems

Kunz and Wayne Hauber (AIT) reviewed the "lockup" issue on XP SP2 systems that are members of a domain. After installing XP SP2 and after a reboot, the system appears to "lock up" at the first login. The lockup appears after the username and password is entered but before the desktop is displayed. A CTRL-ALT-DEL will unfreeze the system, and subsequent logins will not exhibit the lockup.

We currently have a ticket open with Microsoft Premier Support on this issue. Several leads are being followed. OpenAFS (and the "loop-back adapter") seems to have been ruled out. One promising lead is that it may relate to the "Kerberos AutoLogon" application. [Note since the meeting: Kunz and Hauber have proven that this is not always the case]

One piece of information was learned during the analysis process that people may find useful. Using the Windows Security Center (in the Windows Control Panel on XP SP2) to disable the Windows Firewall does NOT totally disable the firewall. The only way to totally disable the firewall on an XP SP2 system is to disable the firewall service. This may be an option for people who are having trouble with the firewall and thought the only answer was to uninstall SP2. You should be able to leave SP2 on the system (and gain benefit from the other security fixes) and simply disable the firewall service.

VBS 15 Sec Delay Issue

Kunz brought up a very new issue that is still a "puzzler" and solicited help from the general community. On SOME systems, Visual Basic Script files take a very long time (15 secs) to terminate. For example, if you create a one-line file called "tryit.vbs", and make the following the only command on the single line:

```
wscript.quit(123)
```

and execute the file, it SHOULD take a very short amount of time (since all the script does is immediately quit with a return code of "123"). On many systems it indeed does work as expected. However, on other systems the script executes but takes about 15 seconds to actually exit and return the return code. This can be seen by launching the task manager and seeing how long it takes the "wscript.exe" process to complete (this is the process running the script). Normally, the wscript.exe process is in and out so fast you may miss it. However, on SOME (many?) systems it will "hang around" for the 15 second delay.

Why should you care? Because if these scripts are part of automated processes, logon scripts, etc. then suddenly processes that took sub-seconds now take many seconds to complete.

Kunz first started noticing this behavior on two of his systems about the same time he upgraded from VirusScan 7.1 to VirusScan 8.0i. However, other systems within AIT seem to not exhibit this problem even with VirusScan 8.0i. Changing VirusScan 8.0i settings in "program" related areas seem to have no effect. If anyone has an answer please email skunz@iastate.edu. We'll get the word out to everyone.

[UPDATE: 12/13/04, Kunz and Balvanz]
This behavior has been proven to be a result of VirusScan 8.0i. You don't have to uninstall all of VirusScan to get rid of the script execution delay. Go into the "Add/Remove Programs" Control Panel and modify VirusScan Enterprise. Remove the "ScriptScan" component. You won't be protected from hostile VBScripts and Javascripts, but your scripts will no longer take 10-15 seconds to complete. Oddly enough, just disabling ScriptScan in the "VirusScan On-Access Scan Properties" doesn't do it; you have to remove the "ScriptScan" component from the installation.

Windows Server 2003 SP1

Kunz went over the highlights of a November 11 presentation by Microsoft on Windows Server 2003 SP1 (to be released into production in 2005). The notes from this presentation are available at:

http://tech.ait.iastate.edu/win2000/admin/WinAdmin.12.10.04.2003SP1.pdf

As stated in a previous email to the WinAdmin and CCSG mailing lists, since that time Microsoft has offered a "release candidate" for Windows Server 2003 SP1 for testing. A good deal of documentation is also available at the download site. This is by far the best place to get information on this service pack. The location is:

http://www.microsoft.com/WindowsServer2003/downloads/servicepacks/sp1/default.mspx

Interest in AutoIt Demo for Next Meeting

Jacob Dekkenga (AIT) has considerable experience at this point using the AutoIt tool recommended in a previous WinAdmin meeting (see the "Open Discussion" section in http://tech.ait.iastate.edu/win2000/admin/WinAdmin.9.10.04.pdf). Jacob has found AutoIt scripts superior to "msi" installers for installing Windows products (including operating system installs). Kunz and Dekkenga asked for a show of hands to see if there was any interest in Jacob giving a presentation at the next WinAdmin meeting on his techniques. The majority of people in the room indicated they were interested. We will place this on the agenda for the next meeting.

Open Discussion

Little time was available (and no important items were brought by anyone)

Meeting Adjourned (about 10:05)

Next meeting is scheduled January 14.