Global Information Assurance Certification Paper

Nancy L. Feder
Version 1.2d
SADMIND/IIS Worm

Introduction

According the C|Net's News.Com, a list of 8,800 internet addresses were sent to attrition.org in the first three weeks in May of 2001.[1] These computers had been compromised by the sadmind/iis worm. This worm begins as an exploit on a Solaris server. The sadmind daemon is installed by default on certain Solaris operating systems, and on systems with Sun Solstice AdminSuite installed.[2] Sadmind is "installed in /usr/sbin and can be used to coordinate distributed system administration programs remotely."[3]

Once the Solaris server is compromised, the worm travels the Internet looking for other vulnerable Solaris systems and susceptible computers running Microsoft's IIS servers.

When a vulnerable IIS server is identified, the home page on the server is replaced by an anti-US government webpage.

This paper will outline some of the ways in which this exploit can be identified, prevented, and in the event of infection, dealt with.

Prevention

Both Microsoft and Sun Microsystems have identified the respective exploits and released patches for them. To immediately protect a PC running IIS 4.0 and IIS 5.0, disable the webserver.

If you do not need to use the administrative functions of sadmind, remove or comment out the sadmind line in /etc/inetd.conf. This will disable the daemon.

Alternatively, you can apply patches to both servers to solve the problem. Patches are available to all Sun Microsystems customers at:

http://susolve.sun.com/pub-cgi/show.pl?target=patches/patch-license&nav=pub-patches

The Microsoft patch for the "Web Server Folder Traversal" vulnerability is available at:

http://www.microsoft.com/technet/security/bulletin/fq00-078.asp

[1] http://news.cnet.com/news/0-1003-200-5893631.html
[2] For further information on the OS versions that are vulnerable, see http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/191&type=0&nav=sec.sba
[3] http://www.cert.org/advisories/CA-1999-16.html

This patch is for both IIS 4.0 and IIS 5.0. Alternatively, Microsoft released a patch on May 14, 2001 that rolls all the IIS patches that they have released since Service Pack 5 for IIS 4 and to date for IIS 5 (for Windows 2000) into a single cumulative patch. If you are not sure exactly which patches you have applied to your servers, this cumulative patch is a good way to insure that you are up-to-date. The cumulative patch is available for IIS 4 here:

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29787

And for IIS 5 here:

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29764

This exploit is almost always preceded by a scan of the network that would report that a certain IP address was performing http accesses on the network looking for exploitable webservers.

Detection

This exploit can be detected by packet sniffers or intrusion detection software. Once the initial Solaris system is exploited, this worm travels the Internet looking for more Solaris unpatched IIS servers to attack. The worm starts checking each system on your network searching for IIS Servers susceptible to the vulnerability. Using Etherpeek, the logs reveal an unsuccessful attempt to compromise an IIS server:

05/11/2001 16:27:10
http://xxx.xxx.xxx/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir from
05/11/2001 16:27:10
http://xxx.xxx.xxx/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir from
05/11/2001 16:27:10
http://xxx.xxx.xxx/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir from
05/11/2001 16:27:10
http://xxx.xxx.xxx/scripts/..%e0%80%af../winnt/system32/cmd.exe?/c+dir from
05/11/2001 16:27:10
http://xxx.xxx.xxx/scripts/..%f0%80%80%af../winnt/system32/cmd.exe?/c+dir
from
05/11/2001 16:27:10
http://xxx.xxx.xxx/scripts/..%f8%80%80%80%af../winnt/system32/cmd.exe?/c+d
ir from
05/11/2001 16:27:10
http://xxx.xxx.xxx/scripts/..%fc%80%80%80%80%af../winnt/system32/cmd.exe?
/c+dir from
05/11/2001 16:27:10
http://xxx.xxx.xxx/msadc/..%e0%80%af../..%e0%80%af../..%e0%80%af../winnt/s
ystem32/cmd.exe?/c+dir from

One can see from the speed with which this hammering of the system is occurring that this is not a manual process. The worm is attempting a buffer overflow to gain root access to the attacked system so that it can replace the home page with the hacked home page. One can also see that the string that is forced into the web browser gets longer and longer before the worm finally gives up and progresses to the next victim.

What follows is the EtherPeek log for a successful attempt where the worm gains root access to the IIS Server on the Windows NT system:

05/11/2001 16:27:10 http://xxx.xxx.xxxx from
05/11/2001 16:27:10
http://xxx.xxx.xxx/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir from
05/11/2001 16:27:10
http://xxx.xxx.xxx/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+..\ from
05/11/2001 16:27:10
http://xxx.xxx.xxx/scripts/..%c0%af../winnt/system32/cmd.exe?/c+copy+\winnt\system32\cmd.exe+root.exe from
05/11/2001 16:27:10
http://xxx.xxx.xxx/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>.././index.asp from

The worm then goes on to replace any of the following pages it finds with the hacked page:

index.htm, default.asp, default.htm, index.asp, index.htm

It places the hacked page into the root of the inetpub directory, and then into the subdirectories, if available: wwwroot, ftproot, webpub, scripts, and IISsamples. Addditionally, it places an executable called root.exe in the scripts subdirectory to provide a back door.

If you are lucky enough to catch this exploit when it is happening, you can block the IP address from access to your network, thus minimizing the damage of this particular attack. If this happens after hours, or if your intrusion detection has not informed you in a timely manner, it is recommended that you have a way of detecting the presence of rogue webpages on your webservers across the network. If you have some identifying text (i.e. you know what the hacked page says) you can write a script to troll through your entire network and use lynx (a text-based browser) to download every default webpage in your domain and search them for words in the hacker's substitution page.

Another preemptive course of action is to scan your network looking for vulnerabilities in your web servers. There are a number of free scanners that do varying levels of network auditing – among them SARA, SAINT, and Nessus. Be sure you have permission to scan before you do so.

If You Are Hacked

The first thing to do upon discovering a hacked system is to remove it from the network. This prevents the worm from moving on to another system if it is replicating.

At this point, you must notify the ISSO of your organization, or another responsible party. You should have a checklist of people to notify along with alternates. Ideally, this should be done by someone who is not involved in cleaning up the systems as this may be time consuming and can take place while clean up efforts are ongoing. In a large organization, it is helpful to have a list that identifies all the machines in an organization and the corresponding support person who is responsible for the machine. In most cases email is used to notify the appropriate people – it is helpful if information concerning a hack is coming from only one person. Otherwise, there is mass confusion.

Take a snapshot of the attacked system so that you can preserve what happened. Spin the snapshot to tape and put it in a safe place. In a large organization, where many people may be involved in cleaning up individual machines, it is helpful to have one person who issues instructions for how to clean up after any attack. Instructions should be clear and easy to follow.

Luckily, the damage caused by this hack does not necessitate a complete rebuild of the hacked system, although if you have those resources in place you can restore the systems to a pre-hacked state from tape. In many instances this hack goes unnoticed for a while especially on desktops that have personal web server installed by default. By checking the security event logs on NT systems you can see when the hack occurred and restore to a day prior to the attack.

To clean up an attacked computer, copy the contents of the inetpub directory to another part of the harddrive and reinstall the web server. Reinstall the inetpub directory to a drive that is not the system drive. Delete the IISsamples directory. Restore legitimate files to the new inetpub directory and save the hacked directory to a zip drive or cdrom. Delete the hacked directory from your computer. Consider the necessity of running a webserver on your desktop. If you can get web space on a professionally managed server, do so.

If it is not possible to disable the web server, apply the cumulative patch to IIS 4.0 or IIS 5.0 referred to above. Consider restricting access to your webserver to IP addresses inside your network through the Microsoft Management Console. To do this, right click on the virtual directory your web site resides in. Choose properties and then click on the Directory Security tab. Edit IP Address and Domain Name Restrictions and deny access from all except IP addresses within your network. Take this opportunity to make sure

you are up-to-date on operating system service packs and hotfixes as well. If you are not running SP6a on your NT machines, install this upgrade. Go to http://www.microsoft.com/security and click on Bulletins in the left panel. Enter your operating system and the service pack you are currently using. The list that is returned are all the hotfixes published since the release of your service pack level. Apply all the hotfixes for your operating system and the cumulative patch for your version of IIS.

Get permission to do so, but scan the machine you have just patched to make certain it is protected from this and other vulnerabilities. Continue patching until the machine scans clean. Resolve to keep up with security patches and updates in the future and make a case for the commitment of additional resources to security in your organization.

All actions concerning the hacking incident should be logged. In a large organization it is a good idea to open a ticket on each infected system so that those who work on it can log their actions. It is a good idea to conduct a post-mortem of the incident that reviews actions taken during the incident and make suggestions as to how things might have been handled differently. The lessons learned from a successful attack can sometimes more easily be worked into a policy statement if one did not exist before the incident.

Conclusion

Both the Solaris and the IIS exploits used by the sadmind worm were old. This was not something new that could have taken everyone by surprise. It was old news, and the fixes for combating it were in place. In this case, the successful defense was a boring defense – to keep up with OS and software fixes. It is dull work but if it is done properly and consistently it will help protect your organization along with other defensive mechanisms such as a complete auditing policy, a backup strategy and a firewall.

Resources

Lemos, Robert. “Fast-spreading code is weapon of choice for Net vandals.” C|Net News.com. March 15, 2001.
http://news.cnet.com/news/0-1003-201-5125673-0.html

University Computing and Communications Services. Georgia State University. “Solaris Security (Solstice AdminSuite Applications)” September 27, 2000.
http://www.gsu.edu/~wwwccs/docs/solaris.htm

CERT Coordination Center. “CERT Advisory CA-1999-16 Buffer Overflow in Sun Solstice AdminSuite Daemon sadmind.” March 2, 2000.
http://www.cert.org/advisories/CA-1999-16.html

U.S. Department of Energy, Computer Incident Advisory Center. “K-013: Buffer Overflow in Sun Solstice AdminSuite Daemon sadmind.” December 30, 1999.

http://ciac.llnl.gov/ciac/bulletins/k-013.shtml

Microsoft Technet. "Microsoft Security Bulletin (MS00-78) Patch Available for "Web Server Folder Traversal" Vulnerability." October 17, 2000
http://www.microsoft.com/technet/security/bulletin/MS00-078.asp

Jesper M. Johansson, Ed. SANS Windows Security Digest Archives. "1.10 MS00-78 – Patch Available for "Web Server Folder Traversal" Vulnerability." Vol. 3 No. 10. p. 7 October 31, 2000.
http://www.sans.org/newlook/digests/ntarchives/103100.htm

Unknown. "Solaris sadmind remote buffer overflow vulnerability" April 1, 2000.
http://www.securiteam.com/exploits/3P5Q1Q0QAO.html

Russ Rogers. "Solaris sadmind Buffer Overflow." April 4, 2000.
http://www.securityhorizon.com/whitepapers/sadmind.html