AIM-Europe CTAG

IT Security Report

Dateline: May 2005
Issue: 0505
General Distribution

Editorial

Well after a relatively quiet start to the year, things have started to pick-up on the vulnerability front. A new worm variant, *W32_Sober.s* has been detected spreading on the Internet as of 2nd May, which the Anti-Virus vendors have rated as a medium threat.
For the week ending Friday April 29th over one hundred vulnerabilities had been listed! It should be noted that over seventy of these were for exploits against various web servers, and that Microsoft had only one vulnerability listed against them for the week. Having said that, Microsoft has been fairing well lattely, averaging about one vulnerability a week, a better average over the last two months than Apple!

This does not mean users should become complacent about patching and updating Anti-Virus and anti-spy ware applications. All users of Windows XP operating system should be running with Service Pack Two (SP2), on their systems.

Critical Alerts

On the 18th April a Security announcement detailed flaws in the Mozilla Suite and Firefox browser which could allow the installation of malicious code or the theft of personal data.

Microsoft's April security update includes fixes for eight vulnerabilities, five of which are rated as critical.

Instant messaging malware attacks, see our web-site for details.
http://ctag.info

Feature: The Good Old Days…

For the feature article this month, we thought it would be nice to get away from all the technology, Spam and nastiness of the present Internet and step back in time.

Back in the days when the Internet was young, the Internet started in 1969, around the 1980's, people used to use email, ftp (File Transfer), Telnet (to login in to other Servers or BBS's Bulletin Boards) and Gopher.
A large number of people on the Internet today do not realise that until very recently the Internet was all Text based using consoles (CRT or Green screens).

Unless one worked at a University or Government institution, access to the Internet was expensive. UK phone charges coupled with modems running at 300 Baud (a modem modem runs at 56K Baud). Many 'home' users connected to the BBS network, most large towns had a BBS, which meant a local rate phone call. Some of these BBS's were just self-contained communities, but more and more had onward connectivity to the Internet, often via the Fidonet network. This facilitated Internet e-mail, thought not at the speeds users are accustomed to today. The BBS's used store and forward mail systems that would up-load and down-load the users email over-night on discount rate leased night-lines.

If one only had access to a local BBS and the software or files (information etc) the user wanted was not held on the BBS, the user could use e-mail to request the files. This could be a laborious task, first an e-mail was sent to the Server which help the files requesting a file list. The returned file list would list the directories on the Server and the file name. A second e-mail would then be sent requesting the file giving it's full local on the Server (a bit like UNC file shares under Windows). If all went well the file would then be sent, often split into multiple parts if it was large. This meant, that for large files or programs, it could take a week to get it using the store and forward BBS systems.

Access to the BBS was often via the Telnet protocol, now frowned upon as in-secure due to the transmission being in clear text (no encryption).
A few Telnet BBS system still run on the net today and make an interesting diversion from the flash web-forums and blogs so prevalent now.

To try out a Telnet BBS, enter the search phrase "telnet bbs" in to google and follow the links. Be patient as many of the links are probably dead. Try the following link, as this lists BBS systems live in the last 30 days,
http://www.dmine.com/telnet/newbbs.asp

Once you find a board, take it slow as they will seem a little quirky, but with luck and perseverance you may find some interesting nuggets.

One of the best known BBS systems was/is called "The Well", (Whole Earth 'Lectric Link) based in San Francisco it was 'populated by many intellectual people, members of the Grateful Dead Rock Group and pioneers of the 'Electric Frontier'.
For a taste of the modern Well, point your browser at
http://thewell.org

This brings us on to another old BBS system still thriving on today's Internet, sdf-lonestar (**http://sdf.lonestar.org**) which is the descendant of "the Killer" BBS, an old American Apple Mac BBS.
SDF now runs on 64 bit NetBSD box's and offers telnet shell accounts, web space, email, IRC and also Gopher space. SDF also has it's own conferencing system called bboard for use by the local user population.

Both The Well and the Killer BBS are mentioned in the excellent book, the Hacker Crackdown by Bruce Sterling (available free on the Internet in most e-book formats as well as HTML and text).

One other long running BBS system is called Grex. As with SDF, they offer free shell accounts and web space but the user is more limited than on SDF. You can create a free account by telnet'ing to grex.org and going through the new account procedure. If you do not want to keep the account, just do not bother to log back in, as they delete old un-used accounts after about 90 days.

Both SDF and Grex ofer a selection of old Unix console games, which are worth playing. Two that stand out are *adventure* the first real computer text adventure game and *rogue* or *hack* which are a bit like dungeons and dragons and are the fore-runner of the still popular *Nethack* (also available on both systems), see **www.nethack.org**.

These BBS systems also offer Text based web browsing in the form of the *lynx* browser, and in the case of SDF, a gopher client as well.

Gopher is a document search and retrieval system that pre-dates the Web (http) by many years. Gopher (the name given to both the client, Server and protocol) can deliver text, graphics, audio, multimedia and binary files to clients. The Gopher protocol has less over-head than http and has a cleaner interface. In today's world of media-rich content, Gopher can be a refreshing change, and works well on dial-up links or broadband!

Much of the historical content is still available on Gopher archives; SDF, TheWell and Quux hold information still.
Gopher Servers are still being developed and there are an increasing number of people on the Internet now 'playing' with Gopher. One of it's strong points is that the links are uniform and it does not matter if the link is on a local system or a server on the other side of the world.

The big problem is how to view Gopher pages on a Microsoft Windows machine, as Internet Explorer does not support the protocol without hacking the registry.
Firefox uses can dip into Gopher space with little problem, as can Netscape users. Just enter **gopher://thewell.org** in the URL bar and away you go.
One alternative is to create an account on SDF or Grex and then use the Gopher client on SDF or the Lynx browser on Grex. As Gopher is textual, these text browsers work very well.
One final option is to try our friend in Americas Gopher site, which includes a telnet/browser that does not require you to set-up an account or master the Unix command line! To use the service telnet to Chris's site as follows
telnet hal3000.cx 8080
the login name and password are both wildbill

Have fun till next time.

Vulnerabilities this Issue:

Microsoft:

Microsoft ASN.1 Vulnerability

Exploit code for this vulnerability is circulating in the wild. This issue, Decoding Heap Overflow was detailed in Microsoft's security notice MS04-007 last year. The issue affects systems running Windows NT/2000/XP/2003. Systems with the current security patches are not at risk.

Microsoft Internet Explorer Content Rating Overflow

The following systems are affected, Windows 2000 SP3 and SP4 Windows XP SP1 and SP2 Windows 2003 Windows 98/ME/SE Internet Explorer 5.01, 5.5 and 6.0

As with the issue, exploit code is available on the Internet. Apply the patch referenced in the Microsoft Security Bulletin MS05-020 as this exploit is being used to install malware on users systems.

Apple:

OS X Cumulative Security Update

On 15th April, Apple announce a security update for the OS X operating system which fixes a vulnerability in Safari browser that can be potentially exploited to execute arbitrary JavaScript code with the privileges of the logged-on user.

Tcpdump:

Tcpdump is a packet sniffing program used on Unix/Linux/Mac OSX and Windows systems. It also forms the core of the Shadow IDS.

Several security issues have been exposed in version prior to 3.9.X, please upgrade your tcpdump installations.

Current web application vulnerabilites

Vulnerabilities in the following applications;

CartWiz
BEA Weblogic
MetaCart2
Horde
Black Knight Forum
MediaWiki
ProfitCode
ASPNuke
PayProCart

Please see your vendor's site for full details.

Below is a list of the Top Ten Worms or Viruses as of week 18

1. HTML_NETSKY.P
2. JAVA_BYTEVER.A
3. HKTL_BRUTFORCE.A
4. WORM_NETSKY.P
5. TSPY_SMALL.SN
6. TSPY_LINEAGE.GEN
7. SPYW_GATOR
8. SPYW_DASHBAR.300
9. SPYWARE_GATOR.D
10. TROJ_BAGLE.BH

Current network port scanning is still centered heavily around TCP port 445, (approx 35% malicious activity for Europe). The Instant Messaging worm is using this port!
Other ports under attack are TCP 135 (Microsoft RPC).

Un-patched system survival time on the Internet is 16 Minutes!

E-mail: team@ctag.info Issue: 0505