Global Information Assurance Certification Paper

The Possible Dangers of a ATT Worldnet Internet Account
By James J. Ulanowski

We all install software on our machines but do we ever consider what security problems we might have just caused? Whether it was a glitch in the program or there by design, we must constantly monitor and scrutinize all software we install. This article covers the dangers from software that is never told to you. You may have stumbled across but not realized its importance. The security problem I am going to describe concerns ATT Worldnet Software.

First this problem may or may not effect you, this depends on your OS, how you use your system and whether or not you have file and print sharing enabled. How many users of ATT Worldnet Software realize that they could be sharing more than files? ATT Worldnet software installs a backup of all your account information on your computer! If you have File Sharing enabled you could be sharing all your account information! This file, account.txt file contains your login password, DNS address, e-mail name and password, POP server, SMTP server, NNTP server, location description (home, work, office, etc.), the primary and secondary access numbers and more. ATT Worldnet advises you to create a backup copy of this file on a diskette, label it as "Account.txt backup" and store it in a convenient safe place should you ever need it." This file the ACCOUNT.TXT file is stored in various locations depending on version and where you installed the software! But you are never warned of the implications during install. Here are the direction's from ATT Worldnet Help File," How to locate the account.txt file
The following are places you might locate the account.txt file or a backup copy:

Backup files you have created:
You have created a backup account.txt file on a diskette.
A backup file created by AT&T WorldNet Setup labeled account.txt.
A backup file created by earlier versions of AT&T WorldNet Software. These early versions did not create account.txt files; they had a separate "Account tool" that created a wnetacct.wna backup file from information stored in several different files on this system.

Automatic backups:
Each time your account file is modified, a backup copy is created and saved in the following path: c:\windows\wnbackup\account.txt

AT&T WorldNet Account files:
By default, the account currently used by AT&T WorldNet Software is saved in the following path: c:\program files\at&t\wns\user

Note: The location of the \at&t\wns\user directory and its contents may very depending on where the AT&T WorldNet Software was installed.

Netscape Navigator account files:
Older versions of AT&T WorldNet Software shipped with Netscape Navigator created a reg.ini file. By default, this file was saved in the following path:

c:\program files\worldnet\program\reg.ini

Note: The location of this directory and its contents may vary depending on where the AT&T WorldNet Software was installed."[1]

Did you realize this? Now how many people do you think have this information shared? All a hacker/cracker has to do is scan the ATT Worldnet address blocks looking for machines with shares, it's like shooting fish in a barrel. Once he finds machines with share it is a matter of connecting and looking for the account.txt file and copying it. Once the initial scan for shares has been done getting this file only takes a matter of seconds! Then the hacker/cracker can restore your account to his machine and not even need to know any of your information. I am not going to actually tell you how to go about restoring the account.txt file, but let me assure you this whole process can be done very quickly.

Here is ATT's response to file and printer-sharing (Netbios), "While NetBIOS (Microsoft Networking) over TCP/IP can present a **serious security risk** if you are careless, **hysteria** related to NetBIOS over TCP/IP is **unwarranted**. Some Internet sites are making matters worse spreading **bad advice (fiction/urban myths)**." [2]

Nice of them to tell you before hand not to share the folders where account.txt resides or provide any suggestions to eliminate these files in case you do share files and folders or even physically sharing the machine with someone. This is a big concern in a number of ways, especially if you pay for your account hourly. If you feel you could have fallen victim review your bills.

My suggestions:
Limit your shares (if you have to have file sharing), create a folder and put only the necessary files needed to share in it. Never share the entire hard drive.

Always use passwords for your shares.

If you have file and print sharing over TCP/IP use a strong Scope ID. The Scope ID option in the TCP/IP configuration provides a way to isolate a group of computers that only communicate with each other. The Scope ID is a character string value that is appended to the NetBIOS name and is used for all NetBIOS over TCP/IP communications from that computer. Other computers that are configured with an identical Scope ID are able to communicate with this computer, while TCP/IP clients with a different Scope ID disregard packets from any other Scope ID. [3]

Install some sort of personal firewall on your machine.

Keep detailed records of the time you spend online this way if you account has been stolen you might be able to realize it before it really costs you.

Use the commands:
Nbtstat –s: Displays your NetBIOS sessions.
Netstat –a: Displays all listening ports and connections
Net -? : Other useful net commands.

Even Microsoft recommends removing File and Printer Sharing component with Dial-Up Networking (Win98-ME) and disabling NetBios over TCP/IP (NT-2000). [4]

Information on ScopeID and Setting it:

- For **Windows 98** as well as **Windows 95**, see Q138271 "Windows 95 NetBIOS Scope ID Configuration".
- For **Windows NT**, use Control Panel » Network » Protocols » TCP/IP Protocol » Properties » WINS Address » Scope ID
- To avoid **compatibility problems**, all letters in the Scope ID should be **uppercase**. (See Q163112 "NetBIOS Scope ID All Uppercase in Windows NT 4.0") [3]
- Using and Troubleshooting the TCP/IP Scope ID - http://support.microsoft.com/support/kb/articles/Q138/4/49.asp

Further Reading:

File And Printer Sharing And The Internet - http://www.nwi.net/~pchelp/security/issues/sharing.html

Practical Recommendations for Securing Internet-Connected Windows NT Systems - http://support.microsoft.com/support/kb/articles/Q164/8/82.asp

Disable File and Printer Sharing for Additional Security - http://support.microsoft.com/support/kb/articles/q199/3/46.asp

Configuring NETBIOS for Maximum Security – http://www.symantec.com/ns-search/SecurityCheck/netbios.html?NS-search-set=/3a115/aaa03o836115218&NS-doc-offset=3&

Features / Douglas Toombs / December 1998 Common-Sense Security Suggestions - http://www.winntmag.com/Articles/Index.cfm

[1] ATT Worldnet Help File

[2][3] File and Printer Sharing (NetBIOS) Fact and Fiction
Part of the Navas Cable Modem/DSL Tuning GuideTM
Copyright 1999-2000 The Navas GroupSM, All Rights Reserved.

[4] Practical Recommendations for Securing Internet-Connected Windows NT Systems – © 2000 Microsoft Corporation. All rights reserved. Terms of Use.
http://support.microsoft.com/support/misc/cpyright.asp
http://support.microsoft.com/support/kb/articles/Q164/8/82.asp