Whitepaper on NetBIOS Firewall - Preventive Technologies for a Secure Future

MicroWorld Technologies Inc.

http://www.mwti.net

How many times do you hear Network Administrators scream at the top of their voice, "I have spent millions of dollars' buying expensive and best Antivirus software solutions and yet every two months, when a new virus strikes, I have my entire network go down!!!" This is a common complaint you will get to hear from one and all Network Administrators, primarily because most security vendors today concentrate more on a "reactive" approach to stop virus attacks, than a "preventive" approach!

How reactive approach works:

- New virus gets discovered;
- Manages to enter one of the workstations inside customer's Network;
- Vendor releases patch within 24-hours of getting a sample of the new virus;
- Customer downloads patch;
- Updates entire network.

But the 24-hour (or less) gap is enough for most viruses to spread & cause maximum damage.

How preventive approach works:

- New virus gets discovered;
- Manages to enter one of the workstations inside customer's Network;
- Virus tries to infiltrate other systems, but unsuccessful;
- Vendor releases patch;
- Customer downloads patch;
- Cleans up the "one" machine which has been affected;
- Updates entire network.

In the 2nd case, we have contained the infection to a single machine on the network, thereby preventing a huge outbreak! As we all know and will agree, major costs of an outbreak comes because of loss of productive time & cleaning up of the mess, created by a virus coming in through a single machine and spreading across the network.

This is the new generation of intelligent and extremely malignant viruses that can compromise poorly protected shared resources on windows network to infiltrate and spread. The networks typically have weak (or NULL) passwords and viruses are able to break them. This white paper provides information about how such viruses compromise your network and suggests an important feature that a good anti-virus should have to combat such threats.

About Shared Networks

In a network, there maybe shared drives, directories or resources like printers. The core protocol on which Windows file sharing runs is called SMB or Server Message Block. In older versions of Windows (e.g. 95, 98, Me, and NT), SMB shares ran on NetBIOS over TCP/IP (NBT) on ports 137/tcp and udp, 138/udp, and 139/tcp. However, in later versions of Windows (e.g., 2000 and XP), it is possible to run SMB directly over TCP/IP on port 445/tcp.

Windows file shares with poorly chosen or Null passwords are a recurring security risk for both corporate networks and home users. There are multiple ways for SMB clients (your Windows redirector) and also viruses to reach the server depending on what combination of protocol stacks you decide to bind your SMB client and server to.

It has often been the case that these poorly configured shares were exposed to the Internet. Intruders have been able to leverage poorly protected Windows shares by exploiting weak or Null passwords to access user-created and default administrative shares. This problem is exacerbated by another relevant trend: intruders specifically targeting Internet address ranges known to contain a high density of weakly protected systems.

Let me explain this with a simple example. Assume there are two computers A and B in a Local Area Network (LAN). Each of these computers has a “client component” and a “server component”. You can enable or disable, either or both of these components. If you wonder, why both A and B should be a server, here is the reason why. If A wants to access files on B, the “client” on A requests for a file from B, and the “server component” on B picks up the file and gives to A. Similarly, if B wants files from A, the “client” on B requests for files from the “server” on A.

Hence, if you disable the “server” component on A, no computer on the network can request any files from A. And if you disable the “client” component on A, A cannot request for any files from other computers on the same network.

In practical cases, many users in a corporate environment normally share their folders or local drives, in order to give access to their local documents or in order for other users to keep a backup of their local files!

How Viruses compromise weak networks

Since the past few months, a new breed of Windows worms known as Share Crawler has arrived. The W32/Opaserv share crawler attempts to discover new hosts to infect by scanning the current IP subnet for the presence of SMB (Server Message Block) servers listening on well-known network endpoints.

Once it is aware of the presence of a server, it will send some specially crafted SMB request packets to the server, which will allow it to copy and modify some critical files on the server’s file

system. This can happen even if your share is password protected. The worm is now able to put a copy of itself, (subsequently) run on the newly infected system and will continue it's search for further systems to infect.

The self-propagating W32/Deloder malicious code is another example of the intruder activity described above. It begins by scanning the /16 (i.e., addresses with the same first two high-order octets) of the infected host for systems listening on 445/tcp. When a connection is made, W32/Deloder attempts to break the *Administrator* account by using a list of pre-loaded passwords. Variants may include different or additional passwords, but reports indicate that the following have appeared thus far:

```
[NULL] 0 000000 00000000 007 1 110 111 111111 11111111 12 121212
123 123123 1234 12345 123456 1234567 12345678 123456789 1234qwer
123abc 123asd 123qwe 2002 2003 2600 54321 654321 88888888 Admin
Internet Login Password a aaa abc abc123 abcd admin admin123
administrator alpha asdf computer database enable foobar god
godblessyou home ihavenopass login love mypass mypass123 mypc
mypc123 oracle owner pass passwd password pat patrick pc pw pw123
pwd qwer root secret server sex super sybase temp temp123 test
test123 win xp xxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
yxcv zxcv
```

On successful compromise of the *Administrator* account, W32/Deloder copies itself to the victim's computer, placing multiple copies in various locations on the system. Additionally, it adds a registry key that will cause the automatic execution of virus. The victim will begin scanning for other systems to infect after it has restarted.

W32/Deloder also opens up backdoors on the victim system to allow attackers further access. It does this in two ways:

1. Attempting to connect to one of a number of pre-configured IRC servers
2. Installing a copy of VNC (http://www.uk.research.att.com/vnc/) (Virtual Network Computing), an open-source remote admin tool from AT&T, listening on 5800/tcp or 5900/tcp

Other viruses (like NIMDA or Klez, for instance) may use simpler methods to copy themselves by detecting network drives or using well-known share names.

Stopping the share crawler involves a deeper understanding of its propagation methods irrespective of the nature of the payload. It is like a virus scanning all local drives to check for open shares & if it finds one, immediately starts infecting all the files on the shared drive!

How do we stop such viruses

Some of the common methods outlined to stop the infiltration involve:

Disable File Shares:

If a given computer is not intended to be a server (i.e., share files with others), "File and Printer Sharing for Microsoft Networks" should be disabled or shares to be made read-only (read access given but write access disabled). Alternatively, if the computer is part of the Internet and the Local Area Network (LAN), sharing should be disabled on NetBT or TCP/IP on the Internet interface.

For computers that export shares, ensure that user authentication is required and that each account has a well-chosen password.

By default, Windows NT, 2000, and XP create certain hidden and administrative shares. Users can read the article HOW TO: Create and Delete Hidden or Administrative Shares on Client Computers (http://support.microsoft.com/default.aspx?scid=kb;en-us;Q314984&sd=tech) for further guidelines on managing these shares.

But Disabling file shares (or making it read only) is hardly the solution, because users in a large environment, certainly keep the sharing open, in order to backup their own files or for purposes of using a common document across groups. Imagine the nightmarish experience for an administrator tasked with the job of implementing a safe sharing policy on any large network!

Use strong passwords:

The various tools described above exploit the use of weak or null passwords in order to propagate, so using strong passwords can help keep them from infecting your systems.

But using the strongest password is also sometimes not enough, because shares on a system are normally persistent. This means that once you use the password to open the share, the resource “remains” shared till the time you restart your machine!

Do not run programs of unknown origin:

Never download, install, or run a program unless you know it to be authored by a person or company that you trust. Users of IRC, Instant Messaging (IM), and file-sharing services should be particularly wary of following links or running software sent to them by other users, as this is a commonly used method among intruders attempting to build networks of DDoS (Distributed Denial of Service) agents.

In corporate networks, such policy enforcements have never been too successful! After all, there’s a factor called as Human Weakness, which is far too complex to understand. I have personally seen very intelligent and knowledgeable users, click on an attachment by the name NudeJennifer.EXE, in spite of knowing that such attachments can carry destructive elements!

Deploy a Firewall:

Firewall products may be able to alert users to the fact that their machine has been compromised. Furthermore, they have the ability to block intruders from accessing backdoors over the network.

However, no firewall can detect or stop all attacks and it is never a practical approach to install Firewall software on all of your workstations on your network since, given the way the Windows LAN Manager operates, you would come up with an amazing number of false positives!

Some implementations try to quarantine the infected systems from the rest of the network as soon as detection occurs, to try and stem the spread of the virus. This may not be very reliable though.

Remote Access Detection (also called Remote Access File Rights / NetBIOS Firewall)

A radical and very effective approach could be used if we exploit the very method that is used by these worms to propagate. The method suggests use of a filter layer above the file system that is used to detect the creation and modification of certain files in different parts of the directory tree.

For example, the user could allow complete access to all folders on the local drive and still disallow the modification of important System files from a remote system or prevent the creation of any file having an .EXE, .COM, .BAT and .DLL extension in the Windows system folder.

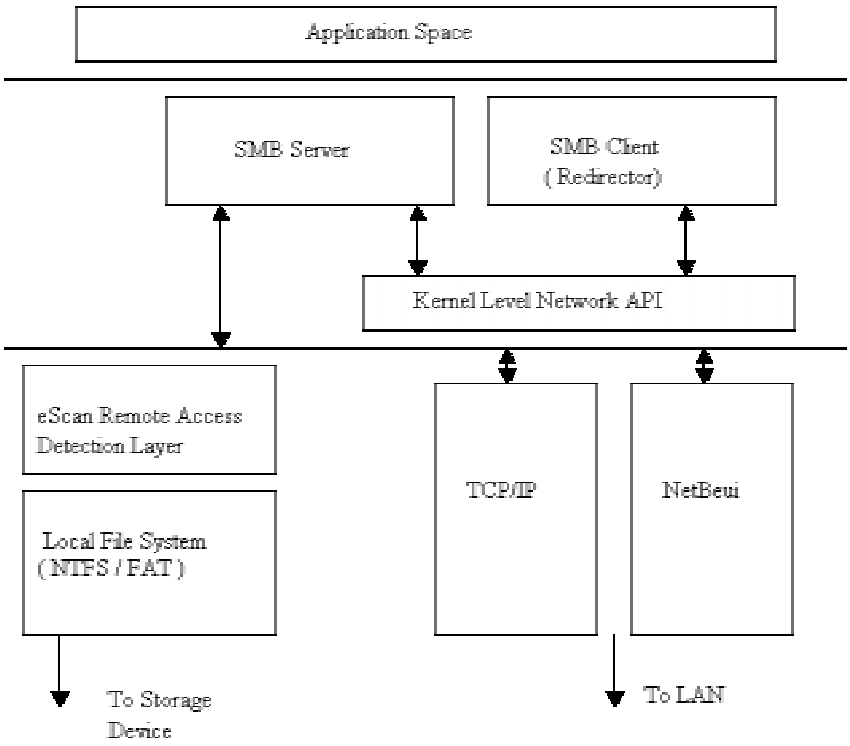
This method has several advantages since it acts a general purpose screening mechanism to prevent not only worms like Opaserv but also your colleague from inadvertently copying infected files to your system. You can also look at it like an Intrusion Detection System (IDS) for Local Area Networks.

Current security on Windows Operating Systems allows you to specify a share as read only or set per user permissions on a file. It does not provide much flexibility in allowing certain files to be accessed while generally protecting the entire share.

Secondly this method is based on the prevention principle and does not rely on the detection of an infected system on the network. Using this feature, it is sufficient for a network administrator to merely know about the way the worm infects the system and it's method of propagation. He can then proceed to block the creation or modification of the files that the worm uses by making appropriate changes in the filter list. She is now assured that the worm cannot spread across her network while she waits for the critical anti virus update from her vendor.

Taking the same example of the W32/Deloder above, assume you some of the systems having null password. If the deloder virus compromises one of the systems, it might be successful in hacking into those systems with the null password, but **cannot** copy itself on to them, if Remote Access File Rights is enabled. Effectively, what we have now achieved is systems getting sand-boxed and remaining safe from any **future** intrusions.

Following line drawing gives an illustration of this concept (eScan Remote Access Detection Layer).



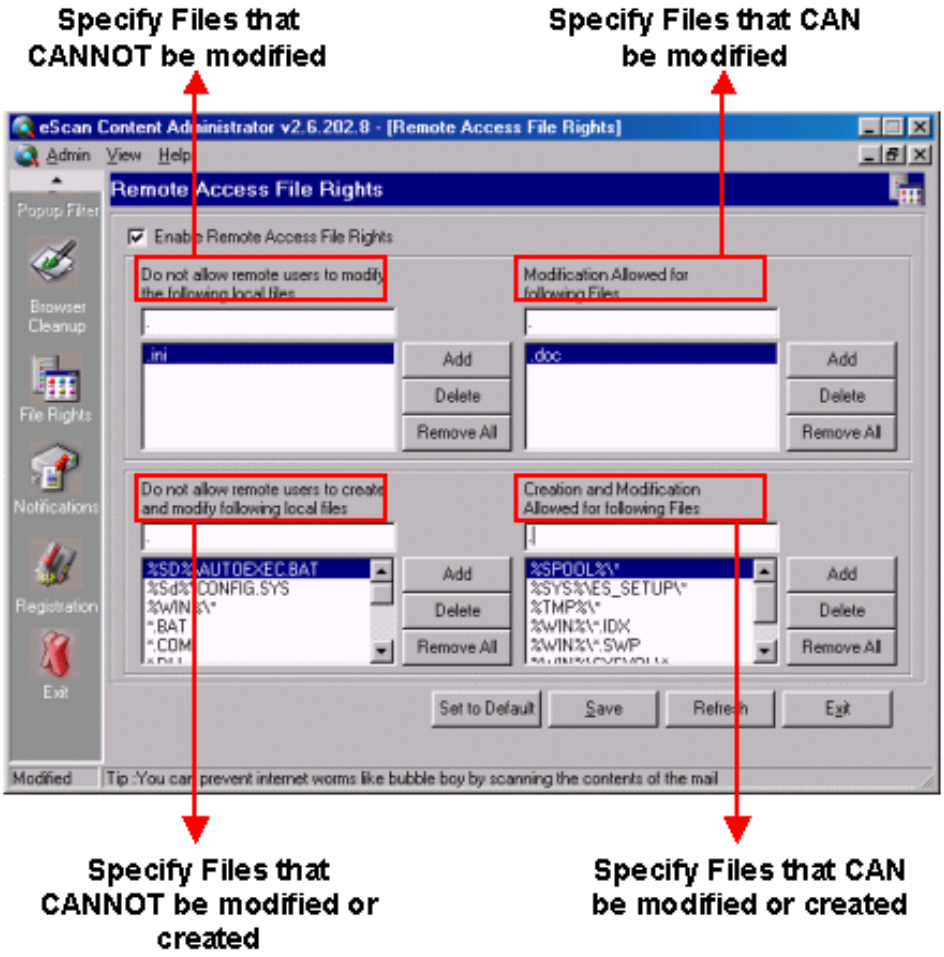
Filtering remote file activity just above the file system and below the SMB server also means that this method is independent of the transport protocol being used between two hosts on the network. Remember that the worm could use NetBeui, NetBT or TCP/IP to copy itself to your system. By using this method you can stop worrying about what protocol the worm would try and use next.

Example of a good software

Good anti-virus software should allow you to specify the file types that remote users CANNOT create or modify. This ensures that file, prone to attacks by viruses are not allowed to replicate on the server. The software should also ensure that sensitive folders, like for instance the startup folder, are never given access to for a remote user.

At the same time, the software should allow you to specify file types that users CAN create or modify. This ensures that your normal network activity remains unaffected.

Following figure shows a feature from eScan 2003, leading anti-virus software that allows you to assign file rights to remote users.



How eScan has an edge over others

The fight against viruses should be pre-emptive rather than reactive. The Assign File Rights feature of eScan prevents viruses from creating infected files and replicating, by denying them the means they need. This is important. Other software's, allow viruses to infect the server and rage through the network, then expect you to shut down the network and indulge in hectic firefighting. They may occasionally be successful but they often are not. You end up entertaining the office staff and lose valuable time and invaluable data.

Decide what you want. Now.

About MicroWorld Technologies Inc.

MicroWorld Technologies Inc is one of the fastest growing software companies in the Computer Software Security areas, and currently doing path-breaking research on preventive technologies. Its MWL Technology and Remote Access Rights, are the first of its kind and being used in its products eScan and MailScan. For more information, on how our world-class product suites, eScan and MailScan can help your organization, please visit http://www.mwti.net.