Tutorial

LanFiltrator Trojan

Security Through Hacking

# LanFiltrator – The "Reversed" Trojan

# (Free Gobo 2)

Straight forward, no nonsense Security tool Tutorials

SECURITY THROUGH HACKING

# LanFiltrator 1.0 Trojan

muts@SecureIT.co.il

http://www.SecureIT.co.il

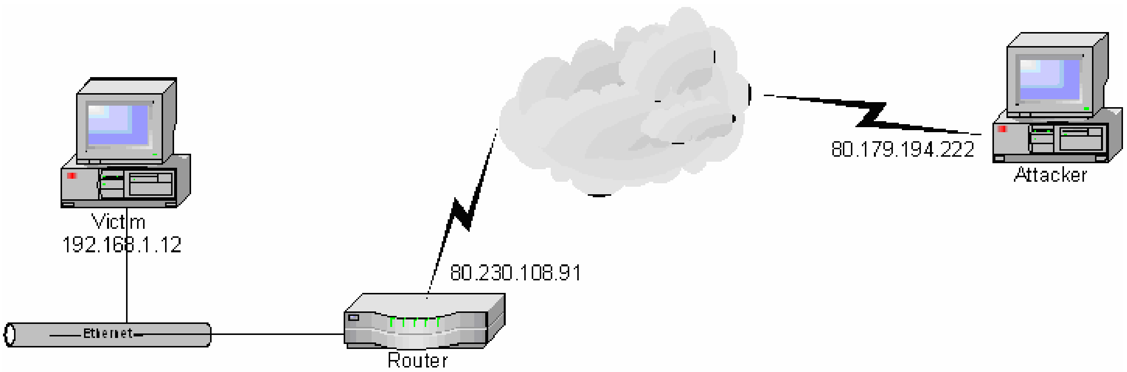
# LanFiltrator 1.0 - The reversed Trojan

## Description

**LANfiltrator is a remote access tool, designed to access a remote computer through a router, LAN or proxy server.** Remote Administration Tools (RAT's) generally work by connecting to the remote computer IP address. However, if this remote computer is behind a router or a proxy (or otherwise using an RFC 1918 address) it would be impossible for a normal RAT to connect to the remote computer (unless NAT would be preformed on the router - which is unlikely ☺).

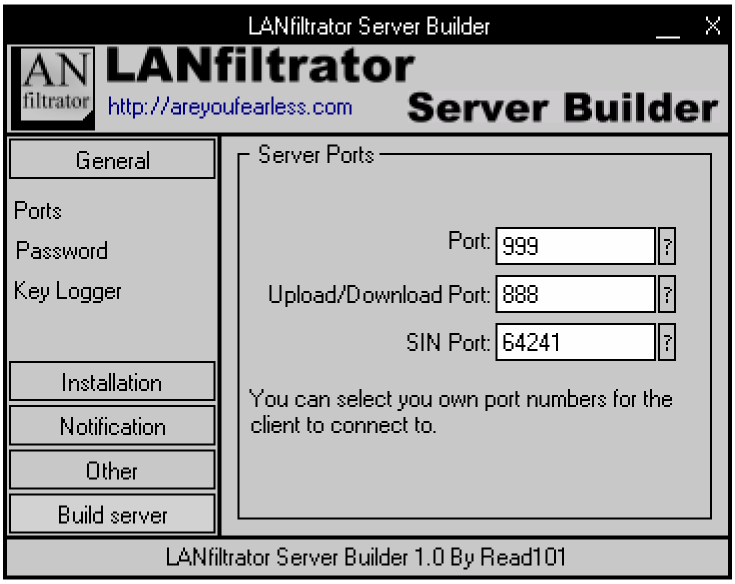
This is where LanFiltrator comes in handy. Think of this a Trojan where the traditional "client" and "server" roles have been reversed. The malicious file which infects the target machine does not *listen* for a client connection – it ***initiates*** a client connection with a listening "server" on the attacking machine. Thus, the initial connectivity is preformed by the victim, and not by the attacker. This would obviously require the server to know the IP of the attacking machine – in order to connect to it.

This might be a bit confusing at first, so here's a sample diagram to explain the tutorial environment. Since the victim does not have a public IP address, at can to be reached directly by the attacker. It can however, ***initiate*** a connection with the attacker – which is exactly how this Trojan works.



For more information, look at the Readme files that come with this Trojan.

1. We first need to edit our server file – the file that will be sent to the victim machine. The settings are rather plain and straight forward. In the "General" tab, edit port numbers and password (if required).



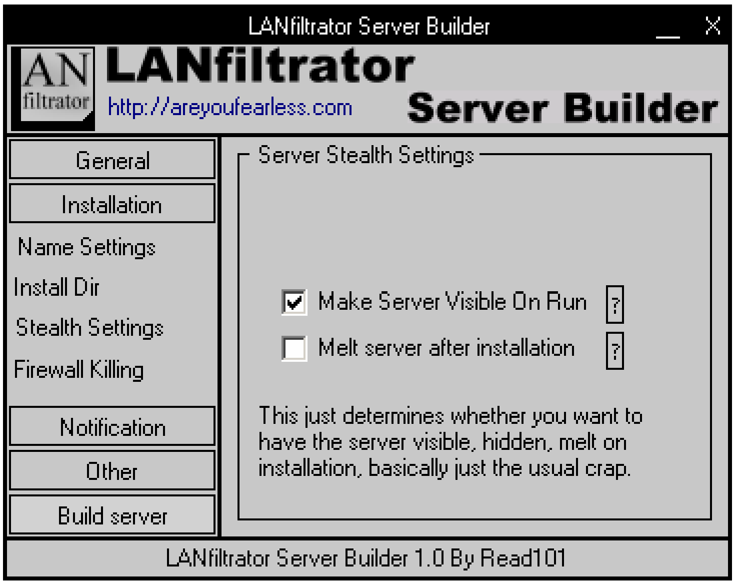
Port: 999

Upload/Download Port: 888

SIN Port: 64241

You can select you own port numbers for the client to connect to.

In the installation tab, you edit the server properties. Notice that the "stealth settings" tab you have the two installation options – "Make server Visible on Run" or "Melt server after installation". The first option is for testing purposes; i.e. – it does not actually install the Trojan, but runs it as an executable. The Trojan will not be restarted after a reboot. The second option actually infects the victim machine, and then deletes the installation file.

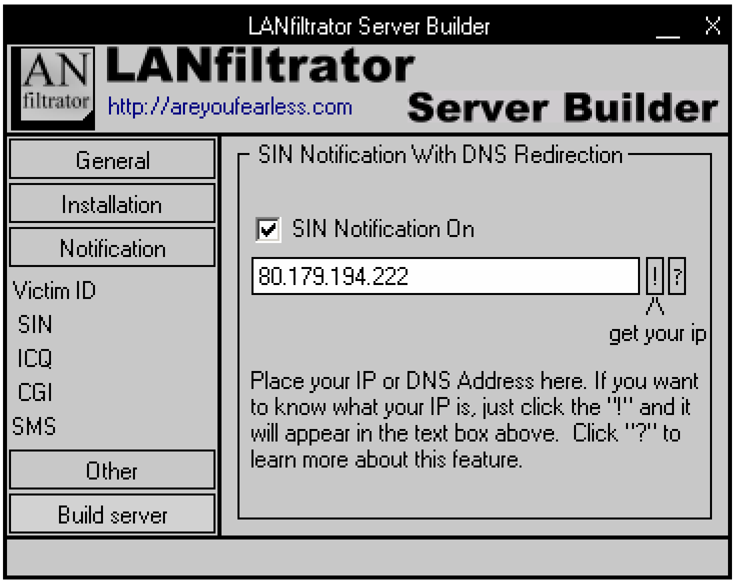


☑ Make Server Visible On Run

□ Melt server after installation

This just determines whether you want to have the server visible, hidden, melt on installation, basically just the usual crap.

2. The notification tab is very interesting… This is where we will be telling the Trojan to try to connect to the ***attacking*** computer after it is installed. We will be using the SIN Notification method. If you are using an ISP DHCP assigned IP (ADSL / Dialup / Cable), you might consider using a free dynamic DNS service, such as No-IP (www.no-ip.com) for name resolution.

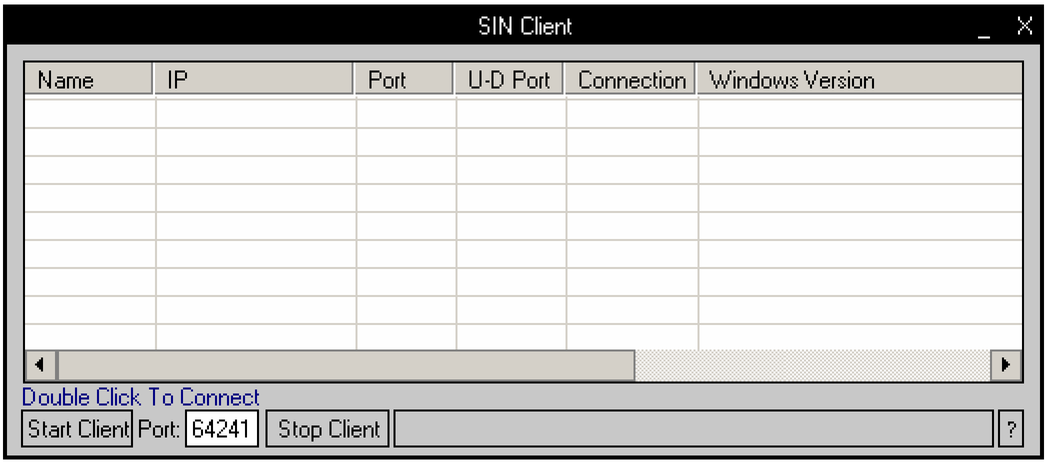


☑ SIN Notification On

80.179.194.222

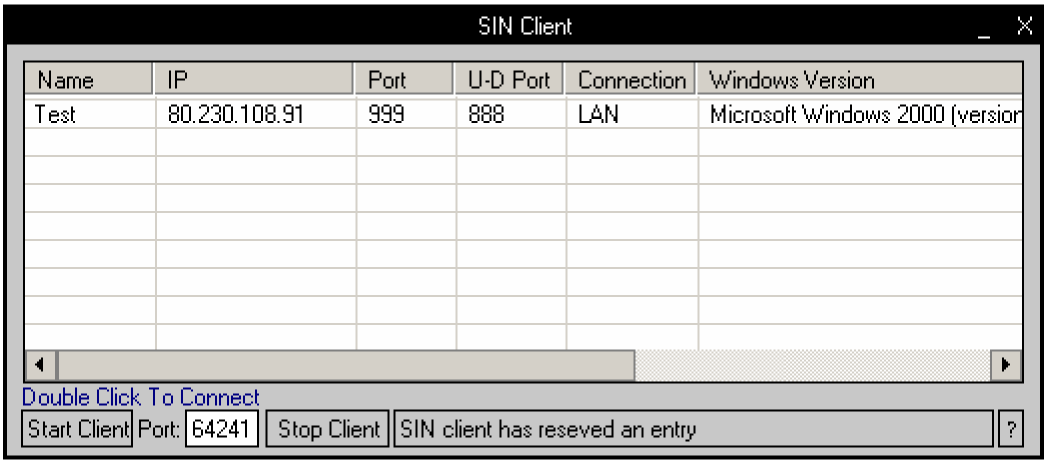
Place your IP or DNS Address here. If you want to know what your IP is, just click the "!" and it will appear in the text box above. Click "?" to learn more about this feature.

3. Once you have gone through all the configurations, you may build the server.
4. Once the Trojan is executed on the victim machine, it will send SIN notification packets to the attacking machine, alerting the attacking machine that it is ready for a connection – even though the victim machine is behind a router, or using a NAT 'ed IP address. After the Trojan is executed on the victim machine, we need to start our **client.exe** program in order to listen for these connections. Click on the "*SIN Client*" button, and the following window will open. Click on "Start Client" to start listening.



Port: 64241

5. After a while, we will notice our victim computer connecting to our attacking machine:



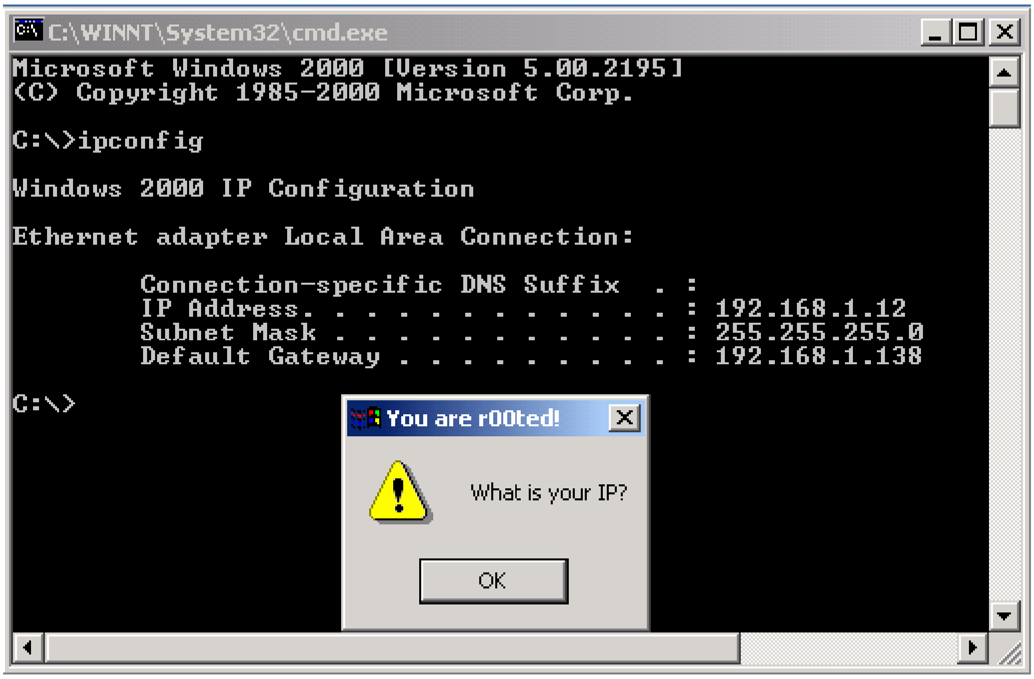
| Name | IP | Port | U-D Port | Connection | Windows Version |
|---|---|---|---|---|---|
| Test | 80.230.108.91 | 999 | 888 | LAN | Microsoft Windows 2000 (version |

Double Click To Connect

SIN client has reseved an entry

6. In case you opted for password protection on your Trojan, you will be prompted for it. Double click on the victim machine computer name, and the main admin panel opens up - you're ready to control the victim machine.

7. We now have a fully fledged Trojan with neat options, such as Web Cam capture, key logger and other features to control the victim machine with. The following is a capture of a message box sent to the victim machine, including an IPConfig – to show that the victim machine is indeed using a NAT'ed address.



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.12
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.138

C:\>
```

You are r00ted!

What is your IP?

## Conclusion and Counter measures

This is a difficult attack to stop, as the initial connection with the Trojan is preformed from *within* the attacked network. The best bet for identifying such an attack would be using a file integrity checker (such as Sentinel 2.0), in conjunction with a correctly configured IDS system (such as Snort) do detect anomalies both in the filesystem, and on the network.

For more information about RFC 1918 see: http://www.isi.edu/in-notes/rfc1918.txt
You can visit the AreYouFearless Team at : http://www.areyoufearless.com

**And for God's sake – Free GOBO!**

## The End