

"Within 5 minutes I was hacked. . ."

In this report I'm going to show you:

- ✓ How dangerous file sharing programs are
- ✓ What they can do to your systems
- ✓ Why you need to control how your systems are being used

In many of my travels I speak with small business owners regarding their system security. Invariably, I mention how infectious file sharing programs are.

Well, more accurately, how infectious their use is. It's not necessarily the file sharing program that infects their systems but what is downloaded as a result of using a file sharing program.

As I talk with them I always offer, "If you have any file sharing programs installed on any of your systems, I will bet you a free vulnerability scan that you're infected with something".

If I'm wrong, they lose nothing, but they gain the knowledge that they're clean. If I'm right, they pay double for my time – I haven't lost yet.

What is file sharing?

File sharing programs, or as they're sometimes referred to as P2P (peer-to-peer), are used by many, many people for downloading music files, movie clips, jokes, "software updates" and many other types of files. These programs give people a sense of community. You're sharing programs with other people around the world with similar interests and after all, someone in your "group" wouldn't want to infect you right?

Some people I've talked with assume that the software provides some type of security. This, they believe, is their guarantee that the software is safe.

Nothing could be further from the truth.

In the remainder of this report, I'm going to prove to you how infectious using these programs really is. I will attempt to keep the "geek speak" to an absolute minimum. My attempt isn't to bore you with the *nitty-gritty* details but to educate you. You need to know how vulnerable you and your systems are.

I selected LimeWire for my test. I have nothing against them. I know it's one of the more popular P2P programs out there so I thought I would use them.

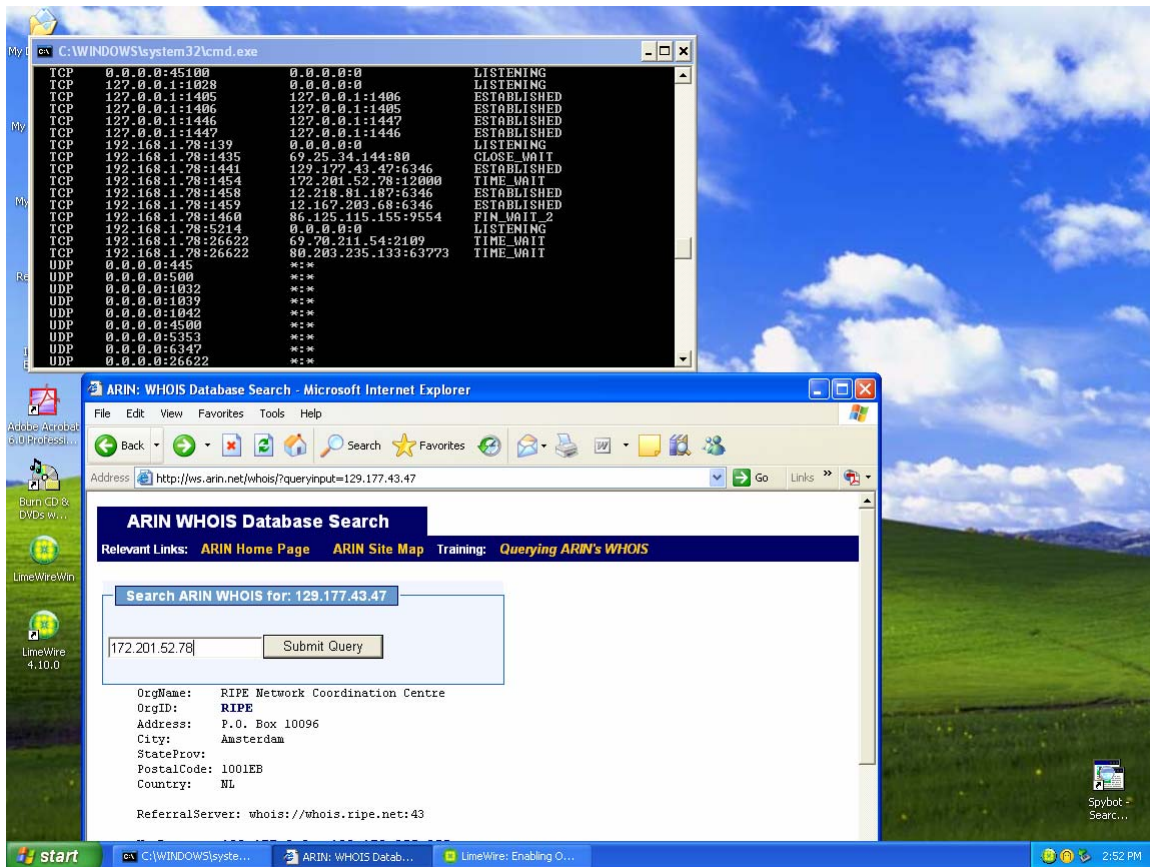
Let's get started.

I downloaded their software from their website:

<http://www.limewire.com/english/content/home.shtml>

How dangerous are file sharing programs?

I configured it safely only giving access to the restricted folder on my system. Shortly after installation I decided to check the outside connections to my system and I noticed this:



What I did here was: Start->Run->CMD and hit OK. Then at the black screen I typed in:

netstat -an

And hit Enter.

The black screen above shows the results of this command. Basically in the third column it's showing me all the IP addresses of the connections to my system. I then opened my browser and went to:

www.arin.net to track down these IP addresses.

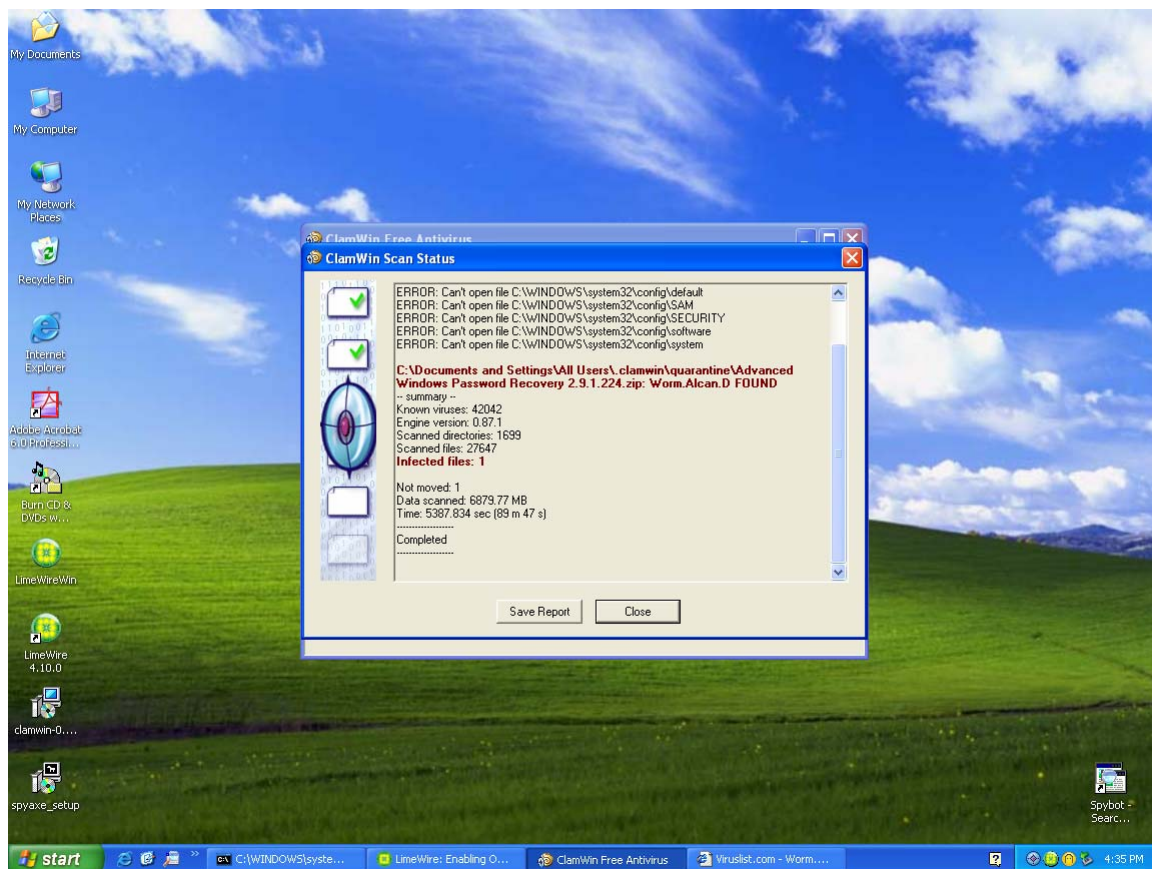
www.arin.net is a web site I use frequently. It keeps a large database of IP addresses and who controls or uses those IP addresses. It is generally considered to be very accurate.

You'll notice in the above browser window that the first IP address I checked is from somewhere in Amsterdam.

Within 5 minutes of installation, these are the connections from outside my network to my new PC!

So I thought I should download some files. I picked three; one video clip of two cats playing (fighting), one was a program claiming to recover Windows passwords, and the other was a Van Halen song. Note: I do own the CD with the song on it. Trust me, if I didn't already own the song I wouldn't be downloading it.

After downloading these files I decided to open them. They opened without any issue. However I then ran a virus scan. One of the files I downloaded was infected:



What can these downloads do to your systems?

To see what it does, I double-clicked the file. I had to. How boring would this report be if I just ended it here?

Nothing ventured, nothing gained.

Here's what happened:

1. It created a hidden folder in C:\Program Files called winupdates. To most people, even if they saw this folder, they would think it's probably safe.
2. It copies the following files to the C:\Windows\System32 folder:
 - a. Tracert.com
 - b. Tasklist.com
 - c. Taskkill.com
 - d. Regedit.com
 - e. Ping.com
 - f. Netstat.com
 - g. Cmd.com
 - h. Bzip.dll

3. Next it creates these files:
 - a. C:\Program Files\winupdates\winupdates.exe
 - b. C:\Program Files\winupdates\a.tmp
 - c. C:\Program Files\winupdates\bszd7349.tmp
4. It checks for the existence of LimeWire. If it finds it installed on the system, it modifies the limewire.props file and adds C:\Documents and Settings\Administrator\Complete to the line:

DIRECTORIES_TO_SEARCH_FOR_FILES

This gives them total access to my system despite the safe install I selected in the beginning.

5. The file: C:\Documents and Settings\Administrator\Complete\Windows XP Live Edition 2.zip is created. Notice it's in the folder that was added to the LimeWire properties file.
6. Don't think that this particular Trojan is picking on LimeWire. It also checks for other P2P programs:

```
C:\Program Files\eMule\Incoming\ PATH NOT FOUND
C:\Program Files\Kazaa\My Shared Folder\ PATH NOT FOUND
C:\My Shared Folder\ NOT FOUND
C:\Program Files\morphus\My Shared Folder\PATH NOT FOUND
C:\Program Files\LimeWire\Shared\ NOT FOUND
C:\Program Files\Edonkey2000\Incoming\ PATH NOT FOUND
C:\Program Files\gnucleus\downloads\ PATH NOT FOUND
C:\Program Files\shareaza\downloads\ PATH NOT FOUND
C:\Program Files\rapiigator\share\ PATH NOT FOUND
```

Notice the NOT FOUND or PATH NOT FOUND comments. That's this trojan's way of determining what other applications it can infect.

7. The Trojan creates a series of files to be shared across the P2P programs:

```
Universal Shield 3.3.zip
Acronis Bootable CD.zip
Advanced Administrative Tools 5.92.zip
Allok AVI Mpeg Converter 1.40.zip
Autodesk 3ds Max Plus.zip
Avalanche Plus.zip
Bejeweled 2 Deluxe Plus.zip
Best of David Lee Roth.zip
Blue - The Best Of.zip
Chuzzle Deluxe Plus.zip
Eminem - Curtain Call.zip
Eminem - Encore - Complete CD.zip
Empire Earth II.zip
EximiousSoft GIF Creator 2.40.zip
EzyPage Enterprise 9.22.zip
Feeding Frenzy Plus.zip
Harry Potter and the Goblet of Fire - Visions.zip
Insaniquarium Deluxe Plus.zip
Internet Explorer 7 Plus.zip
Isobuster 1.9.zip
ISS BlackICE PC ProtectionServer Prot.zip
Journey - The Essential Journey.zip
Koepe XviD 1.1.0.zip
Macromedia Flash Pro8 Plus.zip
MSN Messenger 8 Plus.zip
Nik Color Efex Pro 2.0 for Adobe Photoshop.zip
```

Nik Dfine 1.0 for Adobe Photoshop.zip
Outlaws.zip
Realize Voice 4.1.736.zip
Roxio Easy Media Creator 8 Suite Plus.zip
Suse Linux Professional 10.zip
The Chronicles of Narnia.zip
The Doobies Brothers - 9 Albums.zip
TweakNow Powerpack 2006 Pro.zip
TweakNT - Removes Windows Timebomb.zip
Universal Shield 3.3.zip
Vista Tranformation Pack 2 XP.zip
Windows XP Live Edition 2.zip
Zuma Deluxe Plus.zip

All of these were infected files as well. So my newly loaded PC just became a source for infected files.

8. Remember the files it downloaded in step #2? Well these files copied over the original Windows files. This means if I were to run the "netstat -an" command again, I wouldn't be using Microsoft's original version. I'd be using the one the hackers copied onto my system. Their version doesn't show any outside connections – go figure.

The other files:

- a. Tracert.com
- b. Tasklist.com
- c. Taskkill.com
- d. Regedit.com
- e. Ping.com
- f. Netstat.com
- g. Cmd.com
- h. Bzip.dll

prevent me from doing other system checking. I can no longer modify my registry because they replaced my regedit.com file, well I could use regedt32, but that's too much "geek speak". I can't ping and I can't trace IP addresses any longer. Okay I know I said earlier I would keep the "geek speak" to a minimum but these are all essential commands for someone trying to troubleshoot problems or to check on their system connections.

The malicious program made all of these changes to my system within a few minutes. Notice that my firewall did not block any of these files. It did not block access to my system either. I have three different anti-virus/anti-spyware programs running on this system and none of them alerted me about this infected file until *after* I ran a virus scan.

I decided to use ClamWin for the system scan as that is my choice. The other two anti-virus/anti-spyware programs installed on this system are two of the most popular packages available.

Note: My wife referred to this as the "Mother lode of dangerous code". It's nice being married to a fellow computer nerd.

If you go to LimeWire's web site:

<http://www.limewire.com/english/content/home.shtml>

You'll see the following:



Notice all of their attempts to make you feel comfortable in using their software.

They assure you with "Guaranteed clean install with no bundled software". They use terms like, "Firewall-to-firewall transfers" and "Proxy support". But then if you read further, "Directly connect to a computer" and "Browse host feature – even works through firewalls".

Does this really give you a sense of security?

Not me, that's for sure.

Proxy support means that if your security appliance, i.e., firewall, blocks access to a particular web site, you can first connect to a freely available proxy server, then from there go to the intended web site to view what your firewall tried to protect you from originally. In other words, they support people trying to circumvent their company's security measures.

Shameless plug inserted here: The Box blocks access to proxy servers. There is no circumventing the security provided by The Box. End of shameless plug.

Again, I'm not picking on LimeWire. It's the methods used by all P2P programs that I'm picking on. If you don't own the software or the music, don't think you can get it for free by downloading it or obtaining it through some file sharing service.

Enough of my rant.

Why you need to control how your systems are being used

By allowing people to install this software on your systems you're basically giving them the "okay" to not only "steal" software but you're also giving them your permission to open your systems up to many people with malicious intent!

These are your systems and you can do whatever you'd like to with them, however as a small business owner, I'm sure you'd much rather your resources were used for their intended purpose rather than a gathering ground for gigabit groupies.

Our strategy for preventing this type of user activity is to first detect the traffic, then block the traffic, then report the traffic.

The Box watches all traffic coming in and going out of your network. We won't look at what software is installed. Instead we'll look at the traffic the software generates. We block it so it can't do any harm to your system, such as download more malicious code, then alert the user and anyone else you so desire, including our staff.

Next our staff will work with you or someone you designate to remove the software and then we continually monitor the traffic to be certain that no other malicious traffic is **trying** to get out.

I'm not even going to get into the legal ramifications of having pirated software on your systems. It's illegal and there are groups of people like the **Business Software Alliance** that are offering rewards, or bounties if you will, for information that leads them to someone who is using pirated software. That is a matter for you to deal with on your own.

End of report wrap-up

Within 5 minutes of installing a P2P program and selecting the safe defaults when configuring it, my system was hacked. I'm sure if I would have left it online others would have been downloading files from my system and infecting their system and their system would have been another source for infectious files.

This proves my point that using P2P software is not safe! Notice I didn't say that P2P software itself was not safe, but using it sure is.

I hope this shows you how easily you can become infected. Hopefully you're now running to every PC in your office and checking for any type of P2P software and uninstalling it.

Unfortunately this won't help. You'll probably need to update all of your anti-virus software and verify that it's actually been updated and then run a full scan of each and every PC in your office. You see, this nasty stuff likes to spread. One of the ways it spreads itself is to seek out file shares, like on your server or other PCs connected together. It copies itself out to these shares and waits for someone else to connect in and then it continues spreading.

The reason you'll have to verify that your anti-virus software actually has updated is that many of these malicious programs like to disable your anti-virus software. This prolongs their stay on your system. They'll also block Internet access to websites that provide these updates.

Please be careful out there. It's a wicked world on the Internet.

If you have any questions regarding this report, please do not hesitate contacting me either via phone (866)838-6108 or via email at traef06@ebasedsecurity.com

Thank you for your time and attention.