GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Introduction....3
Who are the Players?....4
Hackers....4
Crackers....4
Script Kiddies....4
Trojan Coders, Hacking Clubs....5
Mobman....5
Blade....9
Rezmond and Fraxx (BioNet)....10
Y3K....10
Dildog....10
Victims of Attack....10
What are Trojans?....11
Why Are Trojans So Effective?....11
How are Trojans Deployed?....12
How Are Trojans Operated?....13
Builder / Edit Server Considerations....13
Method 1, PACKING:....13
Method 2, BINDING:....14
Method 3, ICON CHANGING....15
Method 4, PORT CHANGING....15
Method 5: RENAMING .EXE and PROCESS RENAMING....16
Notification Options....16
Trojan Operations and Uses....19
Scanning....19
DoS, DDoS....19
Social Engineering....20
Password Extraction Techniques (PETs)....21
A Plan for a Lab-Demo of Sub Seven....23
Trojan Detection....24
Trojan Detection and Removal Software....24
TFAK (Trojan First Aid Kit)....24
TCP View Pro....24
Inzider....25
EASY REGISTRY....25
TDS-3 (Trojan Detection Suite)....25
RegistryProt....25
Server Sniper....25
Online Web Site Scanners....26
AVX....26
Trend Micro Housecall....26
Quick Inspector....26
Shields Up....27
Secure Me....27
IT.SEC....27
Host Base Lining....27

© SANS Institute 2000 - 2002 Author retains full rights.

Anti-Trojan Site Links.....27
Trojan Detection and Removal Summary.....28
References:.....30

© SANS Institute 2000 - 2002, Author retains full rights.

Trojan Warfare Exposed

By Scott Scheferman

Introduction

This paper is designed to uncover some of the mysteries surrounding the Trojan phenomenon currently taking place. Written under the premise that the best way to understand a practice is to engage in it from the first person point of view, it aims to illuminate the following aspects of Trojan Warfare:

WHO: Who are the parties involved? We will look at Mobman, Blade, and a few others.
WHAT: What are Trojans, and what are some examples? We will define, give examples and differentiators.
WHY: Why are Trojans so effective and preferred? We will demonstrate the power and versatility of Trojans, and uncover some of the motivations different users have to use them.
HOW: How are Trojans used, how are they spread, how do we detect them, how do we remove them, and how do we prevent future infections? This is to comprise the bulk of this paper. By the end of the paper, the student should feel comfortable with and knowledgeable about choosing, configuring, deploying, detecting and removing Trojans, all from a typically 'black hat' perspective. It is believed that by fully understanding Trojan warfare, the reader will be better able to think like and defend against the wily Internet hacker.

Lastly, the resources, links and references in this paper should serve as an excellent reference for future investigation into the world of Trojan Warfare.

© SANS Institute 2000 - 2002 Author retains full rights.

Who are the Players?

Hackers

The most popular term in the media today is 'hacker'. However, it was originally used to refer to a self-taught computer expert who is highly skilled in technology, programming, and hardware. Many hackers employ these skills to test the integrity and strength of computer systems for a wide variety of reasons: to prove their own ability, to satisfy their curiosity about how different programs work, or to improve their own programming skills by looking at how others have written programs. The term hacker has been adopted by the media to refer to all people who hack into computer systems, regardless of motivation; however, in the media the term hacker is often associated with people who hack illegally for criminal purposes. Many in the Internet security community strongly disagree with this use of the word hacker. In fact, it is often the highest compliment one can pay to an engineer's skill set. Hacking is also known affectionately as 'kung fu' within the security community. (Adapted from Jenkins)

Crackers

The term 'cracker' is rarely used in the media, yet it actually describes much more accurately the behavior of those, which the media highlights. Over the last few years, the term 'cracker' has been used less and less due to the media's influence in the industry. Most people within the Internet community tend to refer to people who engage in unlawful or damaging hacking as 'crackers', short for 'criminal hackers'. The term cracker generally connotes a hacker who uses his or her skills to commit unlawful acts, or to deliberately create mischief. Unlike hackers whose motivations may be professional, the motivation of crackers is generally to cause mischief and damage or to pursue illegal activities, such as data theft, or vandalism. Certainly all Denial of Service (DOS) attacks are performed by Crackers and not Hackers. (Adapted from Jenkins)

Script Kiddies

Some of the most highly publicized Internet security breaches, like corporate web site defacement acts, are committed by middle class teenagers, who seem to perpetrate chaos in order to make a name for themselves. Security experts often refer to these individuals as "script kiddies." Legends in their own minds, script kiddies are generally ego-driven, unskilled crackers who use information and software – or scripts – that they download from the Internet to inflict damage upon targeted sites. Script kiddies are generally looked upon with disdain by members of the hacking community and by law enforcement authorities because they are generally unskilled individuals with a lot of time on their hands that wreak havoc, usually in order to impress their friends. (Adapted from Jenkins)

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Often, script kiddies are described as having the following traits:

- Adolescent
- Bored
- Ego-Driven
- Possess much free time
- Irresponsible
- Ignorance of the severity of their actions
- Enjoy quick satisfaction with little preparation (impatient)

Trojan Coders, Hacking Clubs

Mobman

Mobman is the author of the now-famous trojan named SubSeven. Sub seven gained popularity quickly due to its excellent configurability, overall capability, and its relative small size. This propelled Mobman to the spotlight quickly, and led to the formation of Mobman's crew. Mobman's extensive skills overwhelmed many in both the hacking and security community. The following is a testimony to his skills, demonstrating his ability to incorporate many modules in a small package well under .5 Mb. These are the many features of SubSeven, all of which run with a high degree of stability:

2.1 features
features added in 2.1
Address book
WWP Pager Retriever
UIN2IP
Remote IP scanner
Host lookup
Get Windows CD-KEY
Update victim from URL
ICQ takeover
FTP root folder
Retrieve dial-up passwords along with phone numbers and usernames
Port redirect
IRC bot.
File Manager bookmarks
Make folder, delete folder [empty or full]
Process manager
Text 2 speech
Clipboard managerEDITSERVER CHANGES
Edit Server for 2.1 changes
Customizable colors

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Change server ICON
Pick random port on server startup
IRC bot configuration
Features added in 2.0
Restart server
AOL Instant Messenger Spy
Yahoo Messenger Spy
Microsoft Messenger Spy
Retrieve list of ICQ uins and passwords
Retrieve list of AIM users and passwords
App Redirect
Edit file
Perform clicks on victim's desktop
Set/Change Screen Saver settings [Scrolling Marquee]
Restart Windows [see below]
Ping server
Compress/Decompress files before and after transfers
The Matrix
Ultra Fast IP scanner [thanks to Blade's TH]
IP Tool [Resolve Host names/Ping IP addresses]
Get victim's home info [not possible on all servers]:
- Address
- Business name
- City
- Company
- Country
- Customer type
- E-Mail
- Real name
- State
- City code
- Country code
- Local Phone
- Zip code

Configure Client colors
Configure menu options [add/delete pages, change names]
Automatically Display Image when downloaded [jpg, bmp]
Automatically edit files when downloaded [txt, bat]
Change port numbers for The Matrix, Keylogger and Spies
Retrieve "SubSeven message of the day"
Edit Server for 2.0 new features:
Protect server's Port and Password once installed
Melt server when executed
Protect server settings with a password

1.9 or older features:

© SANS Institute 2000 - 2002 Author retains full rights.

Open Web Browser to specified location.
Restart Windows [5 methods]:
- Normal shutdown
- Forced Windows shutdown
- Log off Windows user
- Shutdown Windows and turn off computer
- Reboot System

Reverse/restore Mouse buttons.
Hide/Show Mouse Pointer.
Control Mouse.
Mouse Trail Config.
Set Volume.
Record Sound file from remote mic.
Change Windows Colors / Restore.
Hung up Internet Connection.
Change Time.
Change Date.
Change Screen resolution.
Hide Desktop Icons / Show
Hide Start Button / Show
Hide taskbar / Show
Open CD-ROM Drive / Close
Beep computer Speaker / Stop
Turn Monitor Off / On
Disable CTRL+ALT+DEL / Enable
Turn on Scroll Lock / Off
Turn on Caps Locl / Off
Turn on Num Lock / Off
Connect / Disconnect
Fast IP Scanner
Get Computer Name
Get User Name
Get Windows and System Folder Names
Get Computer Company
Get Windows Version
Get Windows Platform
Get Current Resolution
Get DirectX Version
Get Current Bytes per Pixel settings
Get CPU Vendor
Get CPU Speed
Get Hard Drive Size
Get Hard Drive Free Space
Change Server Port
Set/Remove Server Password
Update Server

© SANS Institute 2000 - 2002, Author retains full rights.

Close Server
Remove Server
ICQ Pager Connection Notify
IRC Connection Notify
E-Mail Connection Notify
Enable Key Logger / Disable
Clear the Key Logger Windows
Collect Keys pressed while Offline
Open Chat Victim + Controller
Open Chat among all connected Controllers
Windows Pop-up Message Manager
Disable Keyboard
Send Keys to a remote Window
ICQ Spy
Full Screen Capture
Continues Thumbnail Capture
Flip Screen
Open FTP Server
Find Files
Capture from Computer Camera
List Recorded Passwords
List Cached Passwords
Clear Password List
Registry Editor
Send Text to Printer
Show files/folders and navigate
List Drives
Execute Application
Enter Manual Command
Type path Manually
Download files
Upload files
Get File Size
Delete File
Play *.WAV
Set Wallpaper
Print .TXT\.RTF file
Show Image
List visible windows
List All Active Applications
Focus on Window
Close Window
Disable X (close) button
Hide a Window from view.
Show a Hidden Window
Disable Window

© SANS Institute 2000 - 2002, Author retains full rights.

Enable Disabled Window
Set Quality of Full Screen Capture
Set Quality of Thumbnail Capture
Set Chat font size and Colors
Set Client's User Name
Set local 'Download' Directory
Set Quick Help [Hints]
Edit Server for 1.9 or older features:
Pre Set Target Port
Pre Set server Password
Attach EXE File
Pre Set filename after installation
Pre Set Registry Key
Pre Set Auto start Methods:
- Registry: Run
- Registry: Run Services
- Win.ini
- Less known method
- Not known method

Pre Set Fake error message
Pre Set Connection Notify Username
Pre Set Connection Notify to ICQ#
Pre Set Connection Notify to E-Mail
Pre Set Connection Notify to IRC Channel or nickname

As can be seen, these features are both plentiful and powerful. Because of this, Mobman has gained a reputation for his clean code among even those in the white-hat community. Some legitimate companies have even employed Mobman for his skills to do work on remote access programs. The names of these companies have been intentionally left out.

Blade

Blade has been around for a number of years in the hacking community and has more than earned the respect of many. Blade is primarily known for an extremely small and well-used trojan called 'the tHing'. This trojan, although only 8kb, allows a hacker to upload and run a file remotely, as well as notify the hacker via ICQ page notification. Blade's trojan is often used to gain initial access into a system due to its small size.

Recently, blade has been working on a project known as R3X, which is an advanced scanning tool leveraging some of the functionality of the famous NMAP program. Blade's site, **http://www.come.to/soul4blade**, has recently been taken down by the hosting company, but should be back up soon.

© SANS Institute 2000 - 2002, Author retains full rights.

Rezmond and Fraxx (BioNet)

These two are famous in the UK for their trojan, known as BioNet. BioNet is extremely powerful, similar to Sub Seven, but with some key differentiators as well, such as super-fast encrypted file-transfer capability, and CGI notification options. BioNet's web page is http://www.bionet.org.uk

Y3K

A strong group dedicated to producing a rival to Sub Seven. Many believe code from SubSeven is what was used to create the Y3K trojan. The website for this group is http://www.y3knetworks.org

Dildog

Dildog is part of the CDC clan. His contributions to both the black and white hat community are extensive, although some believe he leans more to the anti-Microsoft black hat community. An excellent paper on Dildog and his famous trojan, Bo2K, is available at the SANS reading room at:
http://www.sans.org/infosecFAQ/hackers/dildog.htm

Others

This group is only a minute portion of the many trojan authors in the field today. As more and more people have access to the Internet worldwide, so too, are more and more black hat programmers finding their way into the world of trojans. Expect to see both the quantity and quality of trojans to increase proportionate to the Internet's growth as a whole.

Victims of Attack

The following types of users are victims of attack from trojan warfare:

- Home Users
- Corporate Mobile Users
- Enterprise Networks
- Universities
- Small Businesses
- Worldwide DUN users

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Targeted Individuals: VIPs, Millionaires, Executives
- Any Microsoft Windows User

Trojans can be used to attack just about any windows machine that is connected to a network. Some user-types are affected more than others, however. While many will fall victim to random attack, others will be the targets of a pre-meditated attack.

Victims are such due to many different reasons. More and more users are now enjoying 'always-on' Internet connections. These high-bandwidth services are prime targets for hackers, as they sit exposed to the Internet around the clock. The Internet itself, at the end of 1999 had approximately 200 million users online. By 2003, it is estimated that the number will grow to well over 1 billion users. (Jenkins) This greatly increases the number of 'hackers' that arrive every month to the hacking scene. Moreover, the technologies used on the Internet today are insecure by default. This leaves security up to the end-user, which more often than not is wholly uneducated in the area.

What are Trojans?

Trojan Horse: A program that appears to serve one purpose, but it reality performs an unrelated (and often malicious) task. Trojans are named after the famous Trojan Horse of Greek mythology in which Greek soldiers snuck into the city of Troy in the belly of a wooden horse that was made to appear to be a gift for the Trojans. (Adapted from Jenkins) While trojans can be any type of electronic code that comes unsolicited, this paper focuses entirely on remote access trojans, a.k.a., RATs.

Why Are Trojans So Effective?

Trojans allow a cracker to deploy many functional tools onto the victim's computer in a short amount of time, and in a very small package. Modern trojans add the convenience of being stable and easy to configure. Windows trojans have GUIs that are at once both intuitive and forgiving. Overall, the trojan is the straightest arrow into a victim's system, combining both stealth and power in one tiny package. Tomorrow's trojans may not listen on a certain port or run as a particular process. Instead, they mail use SMTP or use push technology at pre-determined times (off hours), and may destroy themselves immediately after. The future holds an ever-increasing risk of infection, and the battle to detect and remove trojans in a short enough amount of time will continue to be on the side of the cracker. Some of the reasons trojans are so effective are summarized as follows:

- Easy form of social engineering.
- Easy to install without suspicion
- Powerful, customizable, efficient
- Hard to detect and uninstall
- Useful for (D) DOS attacks

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Least Path of Resistance for attack
- Bypass firewall to access network
- Powerful tools used by relatively novice users

How are Trojans Deployed?

One of the most important aspects of trojan technology is its ability to be deployed in so many different ways. This allows the attacker to peel away the layers of a target's defense, by systematically testing it until an opening is found. Many networks today have a strong firewall in place. However, very few networks today have defense in depth enough to counter a targeted trojan attack. The cracker has numerous avenues available to deploy a trojan, and if one fails, there is always another.

For example, if a cracker is unable to send an attached trojan in an email because the target mail server strips off all .exe files, then the cracker may decide to send an email that has malicious code imbedded into the html of the message itself. If the mail server's AV program catches that attempt, then the cracker might turn to the end-user themselves, and hand someone a floppy that has a legitimate program that is bonded to a trojan application. If all of those attempts fail, the cracker may send an AIM chat message to the victim, and request a file transfer using AIM. The cracker may also send the victim a hyperlink to a URL that contains malicious java. If all of these fail, a hacker can perhaps leverage the lack of security in Microsoft's Netbios protocol, and simply connect to the C$ share with an easily guessed, known, or brute-forced password. He then places the trojan installer .exe into the victim's startup folder, and a short cut on the victim's desktop that says, "click me!" Or, if all else fails, the hacker can literally break in, or walk in (as the case may be) to the victim's premise, and quickly insert a floppy, or pop in a CD-ROM disk that utilizes the auto run feature to execute a .bat file that installs an entire army of various trojans!

As we can see, getting a trojan on a victim's computer is only a matter of time and determination. In addition, time, it seems, is always on the side of a cracker.
To summarize, here are some outlined ways a trojan may be deployed:

Via Email
- An attachment
- As embedded HTML script (using Java)
- As a reference to a link that serves malicious code

Physical Drive Access
- Floppy Boot
- Start Up Folder
- Zip Drive
- Auto-Run CD Rom Drive

Web Sites
- Wrapped with legitimate software downloads
- Embedded within the HTML code itself

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

•Links to other apparently legitimate sites that are mirrored, but with malicious code
•Greeting card sites

Chat Rooms

•IRC, ICQ, AIM, ISP Chat Rooms

How Are trojans Operated?

Most RATs have an architecture that employees two or more modules. Almost all RATs have a basic schema of client software, and server software. The Client is the GUI or command line interface the hacker uses to control the Server. The Server is the software that runs on the 'victim' system and 'serves' up the various services the particular trojan features. Many modern trojans are highly configurable and hence employ a third element, the Editor, or Builder component, which is used to configure and/or create the Server component, respectively. There are other miscellaneous bits of code that are often 'plugged in' to the server module, which give it additional functionality.
The range of these 'plugins' is quite extensible.

In summary,

•Client: The remote control portion of the trojan that the hacker uses.
•Server: The hidden code on the compromised box that serves up the goods.
•Builder: The software the hacker uses to generate and configure the server.
•Editor: The software the hackers use to configure and customize the server.
•Plugins: The extra modules that add additional functionality to the server component.

Builder / Edit Server Considerations

In order to successfully infect a host or network, a cracker must first configure a trojan server such that it gets through the front door successfully. In effect, a cracker must 'trojanize' the code in order to have it go undetected by humans, anti-virus software, and IDS systems. A cracker may deploy one or more of the following techniques to accomplish this:

- PACKING
- BINDING
- ICON CHANGING
- PORT CHANGING
- RENAMING .EXE FILE
- PROCESS RENAMING

Method 1, PACKING:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

All servers must be packed, either by the coder himself, or by the hacker using the trojan. The advantage of a hacker packing his/her own version of the trojan is two-fold: The size of the trojan can be even smaller than the original. If a non-standard, lesser-known packer is used; the trojan may escape AV programs, which look for common known signatures.

Taken right from Mobman's website (http://subseven.slak.org), the following is an excerpt in the FAQ regarding the use of a packer and SubSeven. Please note that English is a second language for Mobman. One might say he speaks better Delphi than English:

"Q: What is the 'unpacked server' for? How can I pack it?
A: Since a lot of AV's pick up the sub7 server within 2-3 days of release, so unpacked versions of the servers are released. Pack the unpacked server with an exe packer like Aspack, UPX, Neolite etc and have your OWN custom version. Therefore, here is how to do it: first, let me explain something. All the settings in Edit Server are appended at the end of server.exe. When ran, the server will look for it. If it cannot find it, then it _won't_ work. So you cannot just pack the server with an exe-packer, you are going to have to add that info at the end. Here is how to do it systematically:

1. First, find an exe-packer on the net. there are a _lot_ of them out there. Check out:

http://protools.cjb.net for a HUGE collection of packers

2. Use the exe-packer on the server.

3. Then open up Edit Server with the command: "EditServer.exe /noread". Set all the options [as usual] in there, and at the end click "update server with the new settings". After that, you can use the server as the original.

NOTE: If you want to be able to change the icon of the server, then do not pack the _resources_. All exe-packers should have an option to compress or not the resources. Of course, that will result in a bigger server. It is up to you. Well, that is it, you have no idea what I'm talking about here, then don't try anything with it. Use the original server. Do not e-mail US about it, we WONT help you. Use an exe packer that is _less_ known. The less known it is, the less people will use it to pack the server, which means more time for the AVs to catch it."

The point is well made: Using a lesser-known .exe packer means there is less chance the AV companies will discover the unique version the hacker has just created. Many trojans stay in the wild for several months before any AV dat files are able to catch them. By that time, the damage has been done, and the AV program local to the infected computer has been modified to use old .dat files or simply not run anymore.

Method 2, BINDING:

© SANS Institute 2000 - 2002, Author retains full rights.

A great way to emphasize the word 'trojan' is to bind the server with another legitimate program, so that the victim does not know he/she is running (installing) the trojan server. Instead, the victim only sees the legitimate program install (e.g., AIM, Aventail, etc.). This is the most effective way of infecting a victim: a simple email that suggests the victim start using a new chat program, and the cracker has attached an installer program that works. Meanwhile, the trojan installs silently and is running upon next reboot (which has to happen anyway after the legitimate program installs, usually).

Many trojan packages now come with their own server binders that are very easy and intuitive to use. This is why script kiddies are still very dangerous: They will learn just enough to get into real trouble, and/or open up trojan holes in legitimate corporate or academic networks, ones which real crackers can use to deploy larger attacks.

Method 3, ICON CHANGING

It is easy for a cracker to change the icon of the infected trojan installer, even after it is bound to the legitimate program, or after it has been repacked. A program called MicroAngelo, allows anyone to fully manage and manipulate all the icons on their system. This is one more layer of social engineering a cracker will use to trick the victim into never even second-guessing the program he/she just ran. After all, seeing is believing, and conversely, NOT seeing is trusting. Therefore, when the victim sees the familiar icon, but does not see anything else, they are already falling prey to the cracker's intentions. MicroAngelo can be downloaded from:
http://download.cnet.com/downloads/0-1476516-108-17056.html?bt.dl-10015.ImpactSoftware.Microangelo.1476516-108-17056

Method 4, PORT CHANGING

Most new trojan servers can be re-configured to use something other than their default ports. Crafty crackers will change the port the server listens on to something that is unsuspicious, and that they know may already be allowed through the victim network's firewall. Ports like 80, 21, 25, 110, 1024, 8000, 5190, etc. are all common ports that don't look suspicious to most administrators. Some crackers, after learning that the administrators play Quake3 Arena after hours on the LAN, and host a Quake server even worse, will configure the trojan server to listen on the same ports that Quake3 uses, and the firewall lets all traffic in. Worse yet, the administrators may choose not to log any activity on that port for fear of being caught playing Quake! Some crackers will also play a game of reverse psychology, and install multiple trojans on some PCs with standard obvious trojan ports (27374, 1243, etc). Then stage a stealthier attack from other hosts with innocuous ports. Meanwhile, the administration staff is in a panic removing all those known trojans (all of which would have false configuration data, such as notification email and ICQ addresses that are those of their enemies or of the victim's computer). In war, this is simply called a mass diversion. In Cracking, it's called "sit back and laugh while your spying web cam shows the victim running around like chickens with their heads cut off". Meanwhile, the cracker is off to bigger, better, and badder things…

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Method 5: RENAMING .EXE and PROCESS RENAMING

Simple, but effective, a cracker will rename the name of the installer .exe program to something innocuous or deceiving, like 'antivirus2000.exe'. The victim runs it, and nothing happens as far as he/she can tell. When the victim reports back to the cracker that gave him/her the file, the cracker simply says, "Oh man, I'm sorry, I didn't check it out myself. It's supposed to be a freeware trojan detector… but maybe it doesn't run on your OS." Everything goes back to normal, until the cracker one day makes a connection to the trojan listening on port 1024.

If, however, the victim is a Systems Administrator who knows how to hit CTRL-ALT-DEL to check for processes, the cracker will employ yet another layer of deception by renaming the server process to something that looks 'Microsofty', like "DHCP32", or "winlog.exe", or "MacAfee.dll.exe" or whatever. This makes it that much more gutsy of a move for a System Administrator to kill that process, and if anything, buys the cracker more time. Crackers must take care not to name the trojan server process something the same as a legitimate process that already is running, however, as this has been known to cause system instability. For example, if they name it "IEXPLORE.exe", certain instability will arise.

Notification Options

The notification options of modern trojans are exceptional. Without much knowledge, even a script-kiddie can configure the trojan server to send notification upon successful infection of the victims' system(s). The types of notification are:

- SMTP (email)
- ICQ pager
- IRC pager
- Traditional Pager
- IP broadcast to listening clients
- Telephone / Modem notification
- CGI script notification
- IP unicast to selected address

The types of information that the trojan may send out in its notification message are devastating. Armed with this data, the cracker can quickly connect to his victims in a matter of seconds. The data types are:

- IP address of victim
- Port number server is listening on
- Keystrokes since last bootup
- Victim's name (both real name and cracker's 'nick' that he has configured)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- The name and version number of the trojan server
- AIM, ICQ, POP3 usernames and passwords of the victim
- Anything else the cracker is 1) able to script and pull off, and 2) aware of on the victim's computer

The newest version of SubSeven to come out (v2.2) by Mobman will incorporate newer methods of notification still. A quote taken from his website, http://subseven.slak.org:

"…2.2 will NOT require a smtp server. All you need for email notification is your email, and it is 99.9% reliable. This is very important, since you'll be able to configure 2.2 to email you pretty much everything [logged keys, ras passwords, icq passwords, etc]. You can also use the email notification with icq email express [instead of wwp notification; basically using email: [uin]@pager.icq.com]."

This means one of the challenges most script kiddies face, that is, finding an SMTP server that will relay the notification message to them, will no longer be an issue. There is no documentation suggesting how this process will work at the time of this writing (1-23-00).

© SANS Institute 2000 - 2002, Author retains full rights.

The main issue from a cracker's point of view is that if the trojan server is detected, an advanced user can easily discover the cracker's notification data by reverse-engineering the trojan server with a tool such as SubSeven Sniper. (http://www.backdoored.org) This tool allows for a system administrator or power user to inspect the trojan server file itself, and read the configuration settings the cracker has used. If the cracker configured the server to notify him via email, then his email address will be exposed, as well as his ICQ number, IRC channel info, and the server he chooses to relay his mail off. Ironically, this information can quickly be turned against the cracker.

Ways crackers counter this potential danger, is by cycling through multiple ICQ accounts, all of which are set up anonymously in the first place. Advanced crackers will chose not to use the email notification, and if they do, they will most likely forge the email address and spoof someone else's, if only to distract any investigation. A cracker will do everything he can to keep time on his side, even after being caught. Using the IRC notification option, crackers can hang out in IRC channels using anonymous connections, and simply wait for notification messages to filter through. This is more tedious, but is the safest method over all. In fact, one might say that if a server is configured with only an IRC notify option, that the chances are higher that the cracker is more advanced in skill level. This alone would not necessarily divulge the cracker's skill level, however combined with other hints; it can be a strong sign in the subtle world of trojaning.

If a cracker wants to cause harm to an organization, he may infect it's network with trojans, all of which are configured to notify a commonly-visited IRC channel, such as #SubSeven. This invokes an immediate response from numerous script kiddies who wait impatiently for an open trojan server to play with. Many of these script kiddies do not know how to infect other systems, and thus must 'steal' or 'vulch' other people's efforts. Advanced hackers, knowing this, will configure all their servers with no passwords, letting the script kiddies play around and do all the dirty work, such as DoS attacks, file deletion, and general mayhem. The original cracker will never be caught, while teenagers that know just enough to get in trouble, do so. It is a classic case of the big fish eating the little fish.

Overall, the notification options trojans leverage provide the cracker with the uncanny ability to connect to victim repeatedly. Prior to notification options, victims using dial-up Internet accounts were relatively safe from a repeated connection attempt by the cracker, if only because of the dynamically assigned IP addresses. A cracker had no way of knowing the new IP address of the victim, unless he scanned entire subnets for open trojan ports, and did so continually in order to catch the victim when the victim was online. This deterred crackers, as ISPs began listening for scans on specific ports.

Nowadays, however, all of that has changed: The ports are variable, the IP address is mailed instantly to the cracker, and the scanning techniques the crackers use make it hard

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

to see patterns in the their activity. trojan Warfare is a classic example of how hacking will always stay ahead of Network Security.

trojan Operations and Uses

Scanning

One of the many advantages of using trojans is the ability to scan networks from the victim's computer. This allows the cracker to avoid ever being caught while scanning entire subnets for specific ports. Some of the things a cracker would want to scan for are:

- For other trojans
- For other known RC programs
- For IDS signature ports
- For Web Servers (target of defacement)
- For a given port on a given network subnet
- For FTP servers (port 21)
- For Telnet servers (port 23)
- For any other application port or authentication port

This ability can cause problems for cable and DSL ISPs. For example, it is not uncommon for an innocent victim to get shut down by their ISP because of the numerous scans taking place from his IP address. It also creates a culture of script-kiddies countering script-kiddies, where one thinks he's being scanned by 24.x.x.x host, and therefore retaliates with a port scan of his own, which of course yields a listening trojan port. The first script-kiddie counters with an attack of his own against the apparently aggressive IP, not realizing that the scans were coming from the SubSeven server process, and were not originated by the owner of that IP / hostname. Both the victim and the ISPs suffer while these script kiddies do battle. ISP's are finally starting to catch on, however, and have set up honeypots on every other subnet with services like 80, 21, 23 and other common trojan ports. The ISP does a scan (it's allowed to scan whatever it wants on its own network), and scans for port 27374 (the default sub-seven port). When the first script-kiddie retaliates, a packet filter catches all his actions, and logs them. Even though he may not have attempted any malicious activity, the script-kiddie is sent a warning letter, or immediately gets his account cancelled. Generally, it takes malicious activity for an ISP to cancel an account worth $45/month to them, but make no mistake, most cable ISPs know what activities hackers are up to, and choose to turn the other cheek all the while.

DoS, DDOS

Not only do trojans have the ability to scan from the victim's computer, they are also adept at conducting DoS attacks. Many trojans have the ability to target specific IP address with IGMP or SYN flood attacks. (BioNet has this capability built in). Other

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

trojans can be controlled in unison, to deploy Distributed Denial of Service (DDOS) attacks against corporate web servers from the Internet, or against key servers within the corporate firewall. Again, the possibility of being caught is thus minimized greatly. Typically, immediately following a DDOS attack, the cracker will melt and remove all traces of the trojan used on each of the targeting 'zombie' machines, so as to further obscure his identity.

Future trojans, incorporating the same peer-to-peer file sharing protocols that Napster and other software use, will be able to mount attacks with hundreds or thousands of zombie machines at once. Imagine what a group of 20 crackers could do, each armed with access to hundreds of zombie machines at once! That day is fast approaching.

Social Engineering

Although trojans' ease of use makes them ideal for script-kiddies to use, they are far too powerful of tools not to be used by elite crackers as well. Outside of their normal functions, trojans provide an extremely useful medium from which to launch social engineering attacks. These attacks can yield just enough (or more than enough) information about a company's people, network, resources and security practices for a cracker to launch a strategic attack.

In it is most basic form; a trojan is social engineering put into application code. In fact, the premise behind trojans is that they are revealing information unbeknownst to the owner of that information; much like social engineering itself.

There are many ways trojans give way to social engineering attacks. Some of the things they are used to gain are:

- Passwords from end users
- Network layout information
- Application Version Numbers
- Physical layout information
- Corporate Culture information
- Information on key individuals / habits
- Black mail, bribery, trickery, fear
- Impersonate FBI, Supervisors, Family

Of particular importance is the ability to gain access to passwords via numerous methods, almost all of which involve some form of Social Engineering. Passwords are the keys to authentication, and once gained, provide access to deep within a network.

By sending emails from a legitimate victim's host computer to an administrator of the compromised network, a cracker may be able to obtain information about that network's architecture, applications, managers themselves, their habits, the network's security, and so on. All the cracker has to do is simply change the return address on the email to an

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

account of his own. Alternatively, he can send the email at a calculated time and estimate when the reply will reach the victim's computer again. This way, he can intercept it upon arrival, and pull it off the victim's hard drive, destroying all traces of the thread in the process.

In general, trojans can be used to gain whatever information the cracker is looking for, as they take advantage of any network is weakest link: the end user. As most companies do not have proper policies in place, much less policies that are enforced, crackers can manipulate end users sometimes for weeks before they ever catch on. Imagine if a cracker could send the administrator of a remote branch office an email directly from his CIO's laptop connected to a cable modem at home, and request that the administrator send him all the network diagrams, passwords, and usernames of that branch's network. The cracker first finds out that the CIO will be playing golf all weekend, and thus shoots the email to the branch office administrator late on Friday. He then pages the administrator telling him to check his email and reply as soon as possible, signed by the CIO. All the cracker has to do now is stay connected to the CIO's laptop, and wait for the response. He can use similar techniques to cover his tracks after the information is obtained, and even if the Administrator and CIO catch on, it will most likely be too late: Their corporate website is vandalized while the CIO plays golf (that would be a distraction, while the cracker gains more important customer information, financial data, etc.)

Password Extraction Techniques (PETs)

As stated previously, the most important thing a cracker can social engineer out of an end user is their password(s). The following is a list of technologies and techniques that trojans provide to the hacker:

- Fake Windows Logon Script
- Key-Loggers that send strokes to hacker's email
- The Matrix
- Intimidation (do it or else)
- Fake Help Desk message box
- Simple trojan Chat box
- Web Cam Spy
- Microsoft Text-to-Speech engine manipulation.
- AIM/ICQ/MSIM spies, and/or impersonation
- File download from PC into a customized dictionary attack.
- Passwords stored in registry, DUN account settings, etc.
- Remote Network Sniffers

Crackers may employ a fake windows logon script that tricks the end user into re-entering their password. The password is then stored as a pre-named file on the victim's hard drive and can be encrypted and sent to the cracker's email address as well.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The Matrix is a program imbedding into many trojans (sub seven, BioNet, etc) that turns the victim's screen into a virtual 'matrix' screen, just like the movie. It allows the cracker to chat with the victim and scare them into giving up all sorts of information, the least of which can be a password. Although this sounds like something out of a movie, and somewhat hokey at that, The Matrix is both intimidating and effective against a majority of end users.

Most trojans have a generic chat box program that can be used instead of The Matrix. This vanilla-looking box can be effective in tricking the end user into thinking that it is being used by their Help Desk as part of a beta testing program, after which point most convinced victims will provide their password without question. Crackers that are more aggressive can use the chat box to simply frighten and threaten the end user into performing some action.

The Web Cam Spy allows a cracker to view the images produced by a victim's web cam, and can be used to gain access to passwords that are taken from posters, post-its, tee-shirts, or any other object with writing on it. I was actually at a large client that had a huge flipchart along the east wall that was flipped every Monday, upon which the words were written, "THE PASSWORD FOR THE WEEK IS: carrot", etc. I leave the rest up to your imagination.

Often used for fun, but occasionally used for social engineering, is the Microsoft Text-to-Speech engine component that trojans as SubSeven can leverage. By typing the words the cracker wants to say into the trojan client software, he can remotely force the victim's computer to speak aloud to the victim. When done right, the cracker can actually train the victim over time to associate the voice with, say, a particular website. In this way, the victim enjoys going to that website for the interactive experience, and yet the cracker can speak 'on behalf' of the website to either upset the victim, or even to open an online account at that site (whatever it may be). Chances are that the victim will use the same password he uses for his corporate logon, or his bank account. Either one is valuable to the cracker. This technique is reserved for the home user, as most pc's in corporate environments do not have soundcards installed.

Imagine how much information a cracker could gain, if he were able to impersonate someone else in an AIM, ICQ or IRC chat conversation? trojans provide everything necessary to accomplish this. A smart cracker will simply spy on the normal conversations between victim and friend/co-worker/etc., and learn the mannerisms, personalities and chatting style (no caps, emoticons, etc) before he impersonates one of them. He may choose to impersonate the victim, or he may choose to impersonate the victim's friend/co-worker/etc. in order to learn more about the victim. It is startling how easy this is to accomplish.

Just as interesting, the cracker may use files and registry entries on a victim's computer to draw upon for dictionary attacks against a user's remote logon prompt or POP3 account. This is done by finding files that relate to hobbies, etc. that can be converted into a customized dictionary file for use during the attack. Passwords for other apps, stored in

© SANS Institute 2000 - 2002, Author retains full rights.

the registry, will often match or be similar to passwords that the victim uses for network logon.

Hackers that really know what they are doing are now able to leverage a powerful tool in the form of a network sniffer, which will sniff traffic on the victim's wire and email or push the results to the cracker. This has tremendous impact on the internal network's security and forces us to think critically about employing segmented networks with strong access controls. This functionality will soon be available in the next release of SubSeven v2.2, available at http://subseven.slak.org.
Ultimately, passwords are the prime target of social engineering. trojans maximize every potential avenue from which to extract them.

A Plan for a Lab-Demo of Sub Seven

A live lab demonstration of Sub Seven is, of course, beyond the scope of this writing. However, in order to gain familiarity with this trojan, one might follow the following outline for a lab demonstration. For any how-to's and other FAQ's visit: http://subseven.slak.org

- Run Editserver.exe to configure the server.exe component.
- Experiment with different methods of Infection, as described earlier in this document.
- Configure notification options as described earlier in this document.
- Delete/replace Netstat.exe
- Kill AV Processes
- Pilfer Files (eg. SAM)
- Grab Passwords for DUN, or cached web pw's
- Optional: Scan their network, DoS attack, Web Cam, Network Sniffer
- Reconfigure Notification Options (ICQ, IRC, SMTP)
- Enable Keylogger
- Uninstall AV software, re-install with older, or modified DATs
- Use the chat, the Matrix, and / or other social engineering plugins.
- Cover Tracks

© SANS Institute 2000 - 2002 Author retains full rights.

trojan Detection

trojans are, by design, hard to detect. Discovering them in the first place, however, is the most important first step of defense after you have been infected. Oftentimes, the signs are subtle. They go unnoticed by the vast majority of end users. A large part of the problem is that the Windows environment is already relatively unstable, which makes noticing 'anomalies' that much more difficult. The following are common indicators of trojan activity:

- Hard Drive Activity
- Screen Flashes
- Any Abnormal Behavior
- AV Disabled
- Netstat –n 5, Netstat –A (save another copy of Netstat in another directory!)
- People sending you email replies to messages you don't remember sending, but are from you
- Browsers opening to pages you haven't requested
- Chat buddies not behaving / speaking the way they normally do
- Desktop colors, mouse pointers, fonts, etc changed
- Icons moved or missing

trojan Detection and Removal Software

After deciding you have been infected with a trojan, there are a number of resources you can use to further identify and remove the trojan. Some of the tools described below are not commercial tools and should only be used if you trust the author of the tools *as well as* the source from which you download them. They are listed below for you reference in the event you choose to use them.

TFAK (trojan First Aid Kit)

•www.kryptocrew.de/snakebyte/
•Used to detect and remove trojans, detect listening ports, etc.

TCP View Pro

• http://www.winternals.com/products/monitoringtools/tcpviewpro.shtml
•It shows for each IP connection src/dest address/port and which process built the connection.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Inzider

•http://ntsecurity.nu/toolbox/inzider/
•Lists processes in your Windows system and the ports each one listen on
•Can cause system instability on NT systems, and should not be used on online production systems.

EASY REGISTRY

•http://www.dark-e.com/
•Easy to use registry editor, to find programs that startup in the registry, etc.
•Also has other security features that are very useful in securing a host.

TDS-3 (trojan Detection Suite)

•http://www.diamondcs.com.au
•Grand daddy of all trojan Detection / Removal Suites. 30-day Trial.
•Clumsy interface, takes some time to get used to.
•Offers other networking tools incorporated into the software.

RegistryProt

•http://www.diamondcs.com.au
•Free! Detects changes, real-time in registry start-up values.
•Can be used to baseline a host's registry!

Server Sniper

•Email the detected server to Submit@diamondcs.com.au
•They will email back hacker information from the following server-types:
–Subseven
–Win Trinoo
–BO 2k
–DRAT
•Software available at www.diamondcs.com.au (many excellent utilities for detecting, removing and reverse engineering trojans)

© SANS Institute 2000 - 2002, Author retains full rights.

Online Web Site Scanners

Many excellent resources are already available on the web for free use. Some online sites offer a vulnerability assessment primarily based on open service ports on your host. Others utilize the powerful functions of the browser to actually perform ant virus scans and other such audits. Below you will find some useful examples:

AVX

- http://www.avx.com/scan
- Although new, this site has a nice detection-rate for viruses and backdoor files.
- Sample AVX output:

Memory ok
Master Boot Record 80 ok (Windows 95 B20 - Windows 98)
Partition Boot 1 (primary) (active) ok (Windows NT 2000 FAT32)
Partition Boot 2 ok (Windows NT 2000 NTFS)
Partition Boot 3 ok (Windows NT 2000 FAT32)
Master Boot Record 81 ok (Windows 95 B20 - Windows 98)
Partition Boot 1 (primary) (active) ok (Win95 OSR2, Win98 FAT32)
C:\Documents and Settings\schefe_s\Local Settings\Temporary Internet Files\Content.IE5\CDERGTIF\s721d[1].zip/EditServer.exe infected: Backdoor.SubSeven.214.Defcon
C:\Documents and Settings\schefe_s\Local Settings\Temporary Internet Files\Content.IE5\CDERGTIF\s722b[1].zip/sub7.exe infected: Backdoor.Subseven.22.b1
C:\Documents and Settings\schefe_s\Local Settings\Temporary Internet Files\Content.IE5\CDERGTIF\s722b[1].zip/capture.dll infected: Backdoor.Subseven.22.b1
C:\Documents and Settings\schefe_s\Local Settings\Temporary Internet Files\Content.IE5\CDERGTIF\s722b[1].zip/server.exe infected: Backdoor.Subseven.22.b1

(Truncated to save space)

Trend Micro Housecall

http://housecall.antivirus.com
Decent antivirus scanner using your browser.

Quick Inspector

http://www.shavlik.com/security/Registration.asp
Working with Microsoft…

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Shields Up

https://grc.com/x/ne.dll?bh0bkyd2
The granddaddy of online scanners

Secure Me

http://www.secure-me.net/r3/dsl
Runs actual hacker tools against your host

IT.SEC

http://www.it-sec.de/vulchke.html
Looks for known NETBIOS and BO vulnerabilities

Host Base Lining

The easiest way to tell if you have been infected with a trojan is to have already base lined your host system first. This allows you to compare today's configuration with yesterday's. Without this base lining, it is very hard to tell what has changed on your system. It is also hard to differentiate between legitimate changes and unsolicited ones. To begin base lining your windows system, use a program called WhatChanged, available at: http://www.net-security.org/various/software This program takes a snapshot of the following settings and allows for easy comparison later on:

- Users
- Groups
- Registry
- Directories
- Files

Anti-trojan Site Links

The Internet offers access to perhaps hundreds of online sites that offer information on countering trojans and fighting the battle against them. These sites vary in quality and accuracy of information, but for the most part, all are useful to some degree. The ones below are a few of the personalized, dedicated sites whose sole purpose is to offer counter-trojan information. They are by no means the best sources on the web for detecting, removing and preventing trojan activity.

- http://roocoocoo.cjb.net
- http://go.to/protect20000.com
- http://come.to/bchicken
- http://www.dark-e.com

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Pro-Trojan Site Links

Although the purpose of this paper is not to promote the mis-use of trojans, the following links are provided for academic and research purposes only. There are hundreds of sites readily available to educate on and provide users examples of various trojans. These are here as starting points only.

http://subseven.slak.org
http://backdoored.org
http://www.bionet.org.uk/

Trojan Detection and Removal Summary

Detecting trojans is cumbersome. Each trojan is unique and affects a victim's system differently. While some run as infamous known processes, others run in stealth mode and change identity with every boot up. If you know what trojan you are infected with, the best way to remove it usually is with the client portion of the trojan software itself. However, this may not work if the server is protected with a password. In these cases, your options are two-fold: 1) rebuild the entire system, starting with fdisk.exe, or 2) use a program like server sniper that is able to decrypt and unlock the server's configuration. Some believe the only real way to disinfect is to rebuild the system from scratch. It is this author's experience, however, that trojans can be effectively removed and/or sufficiently disabled to not warrant a complete rebuild.

Key in detecting and identifying trojans is an up-to-date anti virus software. While many hackers find ways around this layer of defense, the effectiveness of the anti-virus software cannot be minimized against the large majority of script-kiddies and amateurs. Anti-virus software is also very useful for discovering ways to manually remove a given RAT. The homepages of these anti-virus manufacturers usually have detailed instructions on the removal of each particular RAT.

It is a good idea to keep a second copy of netstat.exe in a non-standard directory for system-monitoring use. Watch for suspicious high-level ports that are listening, and for unsolicited tcp/ip connections.

Lastly, follow your gut instinct and be slightly more paranoid than you normally feel comfortable being. The crackers that are hardest to detect are usually the ones that know what they are doing, and have a focused reason for being on your host machine and /or network. Make sure if you are using a product like Zone Alarm that its security settings are what you want them to be, and have not been altered by a trojan's installer process. Personal firewalls can be very effective against trojan attack if they are configured properly. However, if they are not, the end user is most likely operating under a false sense of security, and may easily fall victim to attack.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

After reading this document, it is my hope that you have a greater understanding and familiarity with trojans and trojan activity. This document's purpose is to help prepare you against trojan attack. It is written under the premise that knowledge is power: without understanding the enemy, you cannot defend against nor defeat him. Onward!

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References:

Internet Security and Your Business - Knowing the Risks
by Joe Jenkins (joe@nowalls.com)
last updated Nov. 6, 2000
http://www.nowalls.inc

Mobman
http://subseven.slak.org/faq

Dildog
http://www.sans.org/infosecFAQ/hackers/dildog.htm
http://www.bo2k.com/indexnews.html

Who is Scanning Your Computer?
Andrew Daigle

An Overview of Internet Security
Jefferson Ogata
Eric Ogata
Joseph Shirley
http://www.antibozo.net/ogata/security/overview/

http://www.fortunecity.es/consola/dragon/403/mysite-index.html
EuYuLi0 sub7 CLIENT help section
By Euyulio

© SANS Institute 2000 - 2002, Author retains full rights.