Trojans and Backdoors

Shahram Monshi Pouri, Nikunj Modi

1. Introduction

In this paper we try to show what are Trojans and Backdoors and how an attacker can use them to have access to any victim system. We also talk about abilities which a Trojan or a backdoor gives to attacker and how we can protect our system against these kinds of attacks. In final, we use an open source backdoor to show how a backdoor works as a case study.

2. Trojans

You may remember the story of old Greek. Greeks attacked to one of the Troy's cities. After an unsuccessful attack, Greeks made a great plan to win. They made a big horse from wood and left it in front of the Troy's gate. The troy's civilians thought that it was a gift and brought that horse which is called Trojan into the city. In late night, Greek militaries came out of the horse and destroyed the whole city.

The applications works like this story and it is one of the most popular applications which is used for attacking computers. A new game, new free software or an electronic postal card can be a Trojan and it can harm your data or makes a backdoor and your system. Therefore we should be careful about what ever software, an unknown person offers to us.

3. Backdoors

As you can guess, a backdoor is an unusual way which an attacker can use it to get into the system. Normal users use login boxes and password protected ways to use the system. Even system administrator may add some security features to this system to make it more protect, but the attacker can easily use installed backdoor to get into system without any password or authenticating.

Most of attackers like to protect their backdoor on victim system. They do not like that some another attacker use the same vulnerability to get into victim system and change their configurations. That is why an expert attacker after getting access protects vulnerability which is used for getting access to the system. Although the system could be in a company and some body else use that for working, but attacker is the owner of system and can install any application or use stored infractions which is exists on that system.

Some times attacker makes a very secure backdoor even much safer than normal way to get into system. A normal user may use only one password for using the system but a backdoor may needs many authentications or SSH layer to let attacker use the system. Usually it is harder to get into the victim system from installed backdoor in compare with normal logging in.

3.1. Backdoor installation methods

At the most of times, after getting the control of victim system by an attacker, he installs a backdoor on victim system to keep his access in future. It is as easy as running a command on victim machine. But there are also some easier ways to install a backdoor. Most popular way is using Trojans. With sending a greeting card or a free game a backdoor can install on victim system and let attacker to control system.

Another way to install a backdoor is using ActiveX. Whenever a user visit a website, embedded ActiveX could run on system. Most of websites show a message about running ActiveX for voice chat, downloading applications or verifying the user. But the truth is they can easily install any thing on user machine with

only running ActiveX for once. There are several kinds of applications which are used to improve the abilities of websites, such as Java applets but Java applets have a limited access to the system but with ActiveX you can have a full control of machine which is running given ActiveX.

Microsoft made a security policy for protecting the system against this trick. Developers of ActiveX should sign their published ActiveX and the signature should be valid. If any user wants to run an ActiveX without a valid signature, the browser shows the alert about the security problems which may happen after running ActiveX. Unfortunately most of the users do not care to this alert and run any ActiveX which is embedded to browsing web page. It could be very dangerous to run any ActiveX without a valid signature from any unknown source.

4. Undetectable control

Attackers use different mechanisms to make their backdoors undetectable and untraceable. If system administrator sees an abnormal behavior in system, he can understand that it may because of some virus or backdoor, therefore he will find the backdoor and attacker can not access to the system anymore. If he can trace the destination of packets he also can find the attacker. That is why, expert attackers tries to hide their communication and backdoor tasks. There are several ways to do hiding which we shortly describe some of them.

4.1. Cryptography

In many situations attackers use cryptography to encrypt transferred data between victim system and attacker. They use different methods of encryption to make commands and transfer data between victim machine and attacker’s system transparent for system administrator during monitoring the network traffics and behaviors.

In most cases, there is no need to use a very powerful encryption technique, because attacker only use encryption algorithm for hiding the data during transmission. If attacker uses a very powerful technique like RSA, it may cause to increase the CPU usage of victim machine and makes transfer time longer.

In these cases, attackers usually use AES symmetric encryption methods. Serpent is one of popular methods which are used by backdoors. Although Serpent is very strong, still it can be broken with XSL attack but it is much stronger than other AES methods and attackers use that because they believe XSL could be an expensive attack for breaking an effective algorithm like Serpent.

SSH or VPN is another methods which attackers use for encrypting the traffic. Delivering packets using VPN or SSH is undetectable by firewalls and administrators and attacker can use standard services which are already installed on the network for encrypting the backdoor control packets.

4.2. Root kits

Although backdoors can be very dangerous but because they run like a normal application, they can be easily findable. Taking a look in system task list, services or registry may show the backdoor. Expert attacker use more powerful backdoors called Root kits. Root kits work as a part of operating system and do not let the users to see real tasks or services. Operating system will be under full control of attacker and he can hide everything he wants in system. Root kits have two main groups with different architectures, Classic Root kits and Kernel Root Kits.

4.2.1. Classic Root kits

Classic Root kits focused on UNIX based operating systems, like Linux and SunOS. Usually, in these Root kits attackers replace /bin/login file with another version which lets attacker to use his own user name and password to get into system. In this situation, if system administrator changes the root password or limit the access of root user to log into system remotely, attacker can logging in with his saved password. It can also use for saving the passwords of other users in attacker’s database.

Sometimes, Classic Root kits hide more things. For example they change ifconfig command to hide network card flags from administrator eyes. If they do not change the classic ifconfig file, during sniffing of attacker, administrator can see the PROMISC flag and he can understand that a sniffer program is running.

Other UNIX commands which usually changes by classic root kits for hiding are: du, find, ls, netstat and ps.

4.2.2. Kernel Root kits

Kernel root kits replace themselves with the kernel of operating system. In this case you can not trust anything in your system. Whenever an application wants to run on system, operating system reports the results which attacker wants. With Kernel root kits, all processes, tasks, network configurations, port numbers, content of files and any other things that you can believe can show themselves in another way and attacker can force operating system to lie about what ever the user or administrator wants to know.

With Kernel Root kits detection and tracing the backdoors is very hard and they can even stop antivirus or system monitors. It is the most powerful way of using backdoors.

4.3. Using different protocols and port numbers

Attacker may use a random port number instead of standard ports for running a service and victim machine. Unexpected running of SSH service on port 22 which is always monitored by administrator may cause to trace the attack by system administrator. That is why most of attackers use another port numbers to make it harder to detect the running service of the attacker.

Some of the backdoors works more professionally. They change port numbers or using protocol during attack. For example a good backdoor can change the connection protocol from TCP to UDP and even ICMP. If system administrator blocks a port or protocol on gateway, backdoor can switch to another protocol or port number and let attacker to reconnect into the system.

4.4. Reverse control

Most of firewalls or administrators block some connections to outside. They may just let local user to browse websites and not more. Even it can be harder with a NAT system and giving private IP addresses, it is impossible for attacker to connect to a system which is exists on a private LAN.

Backdoors can use another strategy in these situations. Attacker runs his own server on a specific IP address and in given time backdoor tries to connect to the server inside the firewall and ask from attacker's server for commands which should be run on victim machine. Backdoor can also use standard HTTP protocol to connect to attacker server and the server will give the command in HTTP format. It looks like a web browsing for firewall or administrator. This strategy can also work from behind of huge firewall system and it really hard to detect.

The only way which may case to detect these connections is to monitoring the number of requests which sends from a system to a special IP address. Sometimes attackers use chaining many servers on different IP addresses to connect randomly by victim system. This method is even harder to protect.

4.5. Backdoor timing
There are many services which are used for updating the systems during idle time. Cron command on UNIX machines or Schedule tasks on windows machines are samples of these services.

Attackers can use these services to use backdoors in given times. For example, using Cron table of an UNIX machine, a back door can start to work in 4 O'clock of morning and let attacker to connect to system, the time which there is no administrator in the office.

5. Protecting against Trojans and Backdoors
Now, this is a time to know how we can protect our systems from Trojans and Backdoors and how we can defend these kinds of attacks.

Several ways could be suitable for this defending. We discuss briefly about these methods.

5.1. Antivirus
Running an update antivirus on all client systems with Real-time protection can be a very good way against popular Backdoors and Trojans. Antivirus can easily find Backdoors or Trojans before running them on the system, but the important thing is to keep any antivirus update. If an attacker use a new backdoor or Trojan which is not exists in antivirus database, it can run on victim machine easily and without any warning.

5.2. Signatures
Before using software you should be in sure about the application which you want to run. Many of developers use MD5 algorithm to make a hash string from their final application. After downloading any application and before running you can calculate the hash string of executable application and compare it with given hash string which is exists on developer's website. If hash strings were same you can understand nobody changes executable file and you can execute it. But before execution you should have trust to developer.

There are many third-party companies, like verisign, which they give some keys for signing applications to the developers. If any application had this signature you can be in sure that the company is trusted and application is valid and safe for execution. If you do not know all of trusted software companies, you can trust to your trusted third-party company which guarantees the software company.

5.3. Training
It is very important to train the users about security problems which may happens in whole system. In most of times attackers use social engineering to deceit users. Users have to know what they should do and what they should not. If any user do something wrong, whole the corporation may become reachable for an attacker.

6. Case study
In this part, we use Back Orifice 2000 as a sample to show how a backdoor can work on a system. Back Orifice 2000 (also called Bo2k) is one of oldest and most

popular backdoors which is widely used for training issues on Windows machines. Bo2k is open source and it can be reachable from Source forge website.

6.1. Back Orifice and its history

Back Orifice is written by Dildog on of the members of 'Cult of the dead cow' group. It introduced in DefCon 7 conference in 1999.

After a while they made a more powerful version of Back Orifice in the name of Back Orifice 2000 or Bo2k as an open source project. They called this system a remote administration system but because it can be installed on client machine without any prompt, many of peoples used this application for bad reasons. Tht is why when ever you want to execute a Bo2k application on your system, your antivirus shows an alert. Bo2k is a tool which you can use it in both good and bad tasks. Many of companies use Bo2k as a cheap solution for managing their systems remotely.

6.2. Abilities of BO2K

Bo2k is very small but very complete in abilities. The client code of Bo2k is about 100 KB and it can be installed very easily even with old modems and limited bandwidth. You can also change the size of client with adding more features to it to have more control on remote machine. It can use different kinds of authentication, cryptography algorithms and protocols. In recent versions you can also run it as a reverse client or you can add kernel root kit features to hide the tasks. You can Improve the Bo2k abilities with adding some plug-ins to both client and server part of this application. Even you can develop your own plug-ins to work under Bo2k system.

Whenever you download a Bo2k application, you can use bo2kcfg (Bo2k Configuration Application) for configuration of Bo2k client. You can open Bo2k file and pre-configure it for using in future. In this step you can add TCP/UDP protocols for Communication, Authentication and Encryption mechanisms, and default port for using in future. After configuration this client, whenever you run it on any machine, you can connect to that machine using bo2kgui interface to control the client system remotely.

6.3. Making a Trojan using BO2K

You can use many binder applications to bind Bo2k client to any other program. After running the result program, Bo2k will start to work and user can not understand that bo2k is running in parallel. Elite Wrap, Saran Wrap and Silk Rope are some sample programs which is widely used for binding the Bo2k client to other applications.

7. Conclusion

This paper is written to have an overview on Trojans and Backdoors. It is good to know how Backdoors and Trojans work and how they can harm our systems. With studying their behaviors we can design more secure systems and we can protect our information against these attacks.

8. References

a. Counter Hack, Ed Skoudis, ISBN: 0130332739
b. Maximum Security, Anonymous, ISBN: 0672318717
c. Firewalls and Backdoors, Bob Rudis and Phil Kostenbader, Security Focus
d. Bo2k official website, http://www.bo2k.com, Last visit: October 24, 2006
e. Serpent (Cipher), Wikipedia, http://en.wikipedia.org/wiki/Serpent_(cipher), Last visit: October 24, 2006