Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.482 – 487

RESEARCH ARTICLE

Remote Administrative Trojan/Tool (RAT)

Manjeri N. Kondalwar [1], Prof. C.J. Shelke [2]

[1]M.E. [C.S.E.] Ist year, P. R. Patil College of Engineering, Amravati

[2]Head of the Department, Information Technology, P. R. Patil College of Engineering, Amravati

[1] manjerikondalwar13@gmail.com [2] chetanshelke7@gmail.com

Abstract- Remote Administration Tool (RAT) allowing a potentially malicious user to remotely control the system. A Remote Administration Tool is remote control software that when installed on a computer it allows a remote computer to take control of it. A Remote Administration Trojan (RAT) allows an attacker to remotely control a computing system and typically consists of a server invisibly running and listening to specific TCP/UDP ports on a victim machine as well as a client acting as the interface between the server and the attacker. The most common means of infection is through email attachments. The developer of the virus usually uses various spamming techniques in order to distribute the virus to unsuspecting users. Malware developers use chat software as another method to spread their Trojan horse viruses such as Yahoo Messenger and Skype. Remote Administration Trojans (RATs) are malicious pieces of code often embedded in lawful programs through RAT-sanction procedures. They are stealthily planted and help gain access of victim machines, through patches, games, E-mail attachments, or even in legitimate-looking binaries. Once installed, RATs perform their unexpected or even unauthorized operations and use an array of techniques to hide their traces to remain invisible and stay on victim systems for the long haul.

Keywords- Remote Administration Tool; Trojan; email attachments; malicious; Compromised System

---

I. INTRODUCTION

Remote administration refers to any method of controlling a computer from a remote location. Remote administration is becoming increasingly common and is often used when it is difficult or impractical to be physically near a system in order to use it, or in order to access web material that is not available in one's location. Any computer with an Internet connection, TCP/IP or on a Local Area Network (LAN) can be remotely administered. Remote administration can be used for any cluster of activities and can span multiple categories of servers, such as database servers, middleware servers, etc.

Today, providing remote and mobile workers with secure remote access to corporate networks is no longer luxury; it has become a business necessity. Letting employees tap into the office local area network "LAN" from customer sites, hotels, internet cafe and airport kiosks can greatly increase business efficiency, productivity and job satisfaction. But mobile empowerment has a price, measured in IT administration and network security. As more Information Technology departments centralize and consolidate to reduce cost, many remote sites are left with no on-site IT support. Remote administration of computers is common because of the significant cost benefits; many tasks can be automated, and the administrator does not have to physically visit each computer. Remote control software provides businesses the ability to login and access computers remotely. Utilizing remote control software enables personnel to transfer files or folders quickly and easily, and communicate by instant message, text chat, or voice intercom from any PC, cell phone, wireless PDA. This fast, reliable, easy-to-use pc remote control software saves you hours of running up and down stairs between computers. The remote administrator software allows you to take control of another PC on a LAN, WAN or dial-up connection so you see the remote computer's screen on your monitor and all your mouse movements and keystrokes are directly transferred to the remote machine. These softwares provide fast secure access to remote PC's on Windows platforms. Many remote administrator tools exist in the market and it is difficult to choose what you need. As you are an IT support, you need to choose the software which leads your IT skills. After you determine how much you want to manage remotely, the next step is to select the tools and supporting components you need to accomplish your remote management tasks.

II. REMOTE ADMINISTRATION PROGRAMS (TOOL)

It is used to remotely connect and manage a single or multiple computers with a variety of tools, such as:

1.Screen/camera capture or control
2. File management (download/upload/execute/etc.)
3. Computer control (power off/on/log off)
4. Registry management (query/add/delete/modify)
5. Shell control (usually piped from command prompt)

We have two kind of connection:

1. Direct Connection

A direct-connect RAT is a simple set-up where the client connects to a single or multiple servers directly. Stable servers are multi-threaded, allowing for multiple clients to be connected, along with increased reliability.

2. Reverse Connection

A few advantages of a reverse-connection:

1. No problems with routers blocking incoming data, because the connection is started outgoing for a server
2. Allows for mass-updating of servers by broadcasting commands, because many servers can easily connect to a single client

III. CHARACTERISTICS OF RATS

As RATs can essentially capture every screen and keystroke, intruders may obtain account information, passwords, and sensitive computing system data. RATs can also spawn arbitrary numbers of processes on specific TCP/UDP ports, impersonate victims, redirect traffic for specific services to other systems, and launch distributed denial of service (DDoS) attacks.

RAT Trojans can generally do the following:

1. Download, upload, delete, and rename Files.
2. Format drives
3. Open CD-ROM tray
4. Drop viruses and worms

5. Log keystrokes
6. Hack passwords, credit card no.
7. View, kill, and start tasks in task Manager.
8. Print text, Play sounds
9. Randomly move and click mouse

Some RAT Trojans are pranks that are most likely being controlled by a friend. RATS are generally not harmful, and won't log keystrokes or hack. They usually do whimsical things like flip the screen upside-down, open the CD-ROM tray, and swap mouse buttons.

IV. **FUNCTIONALITIES OF** RATS

RATs typically provide attackers with comprehensive command repertoires for file management, process scheduling, and system configuration manipulation. File management features include potentially destructive operations such as delete/move a file or directory on victim systems. The process scheduling component in a RAT permits intruders to create, view, and/or terminate running processes at will. The configuration manipulation element allows RATs to alter the behavior of the victim system by for instance disabling its security features after modifying the Windows Registry. RATs can often operate as device controllers being able to open/close CD-ROMs, disable the mouse and network cards, intercept keystrokes and/or screen snapshots, flip the victim's screen or change its resolution, monitor password dialog boxes and clipboards, capture audio/video of the victim's environment, and finally, crash the victim.
The re-direct feature of RATs allows an attacker to chain various services together and ultimately forward the results to a specified destination, making it trivial for intruders to hijack network connections, intercept private data, and inject fake messages. By functioning as packet sniffers, RATs can also monitor a victim's network activities and determine its topology. Furthermore, by scanning the entire system of the victim machine, including its garbage bin, a number of RATs can collect personal information such as user accounts, passwords, credit cards, and Email addresses.

V. **DIFFERENT TECHNIQUES USED IN REMOTE ADMINISTRATION TOOLS**

The purpose of this section is to present the different methods and tools frequently used to administer remote Windows systems, and which let you able to access a command prompt and perform basic system administration, such as view and/or start/kill processes or services, reboot machines and view system logs, observe what is happening on the display, and even run GUI based programs all remotely, that depends on each features of these remote administrator softwares

A. MSRPC "Win32 legacy management APIs" The traditional method to administer remote Windows systems is to use Win32 legacy management APIs. These APIs can be easily identified because they take a server name as one of their parameters, when the server name is empty "NULL", the API operates on the local server, and when a server name is specified, the API operates on the specified remote server. For instance, all APIs with names starting with Net such as NetShareEnum() belong to this class of APIs. When used to administer a remote server, these APIs use the MSRPC protocol, "Microsoft implementation of the DCE RPC standard" with the SMB transport. SMB is the core protocol of Windows networks and operates on both port 139/tcp and 445/tcp. When used as a transport for MSRPC, named pipes inside the IPC$ share are used as RPC services endpoints. Microsoft Remote Procedure Call "RPC" is an interprocess communication "IPC" mechanism that enables data exchange and invocation of functionality residing in a different process. That process can be on the same computer, on the local area network "LAN", or across the Internet. The Microsoft RPC mechanism uses other IPC mechanisms, such as named pipes, NetBIOS, or Winsock, to establish communications between the client and the server. With RPC, essential program logic and related procedure code can exist on different computers, which is important for distributed applications.

B. WMI "Windows Management Instrumentation"
WMI "Windows Management Instrumentation" is the management framework available in recent Windows systems. WMI is built on the COM "Component Object Model" infrastructure and can thus operate remotely, using DCOM "Distributed COM". In addition, several WMI-based administration tools are available by default on Windows systems to administer remote systems using WMI. Windows Management Instrumentation is an infrastructure that enables you to access and modify standards-based

information about objects, such as computers, applications, and network components, in your enterprise environment. Using WMI, you can create powerful administration applications to monitor and respond to specific events in your environment. For example, you can create applications to check CPU usage on your Windows Server 2003, based servers and warn you when it exceeds a specified level. Although WMI is a powerful tool for building customized applications, it does require a certain amount of developing time and expertise. Windows Management Instrumentation Command-line "WMIC" provides a simplified interface to WMI. By using WMIC, you can access WMI based information using the command line or scripts. You can use WMIC from any computer where WMIC is enabled to manage any remote computer. WMIC does not have to be available on the remote computer.
Currently, testers of the Windows Management Instrumentation "WMI" conduct tests through a proprietary GUI interface, which does not allow for negative testing or the logging of events and methods.

C. GUI-oriented tools build in windows

Many Windows system administrators tend to use graphical remote administration tools that allow access to Windows GUI. Recent Windows systems "Windows 2000, Windows XP, Windows Server 2003" natively support Terminal Services, the feature of Windows NT that allow multiple concurrent interactive logon sessions. The network protocol used by Terminal Services is RDP, Remote Desktop Protocol, and operates by default on TCP port 3389.
Terminal Services rely on Windows authentication to authenticate users establishing remote sessions. In addition, applicative permissions are supported by Terminal Services to restrict the category of users allowed to establish Terminal Services sessions, Permissions tab in the Properties of the RDP-Tcp transport in Terminal Services Configuration MMC snapin.
Remote Desktop, included with Windows XP Professional, enables you to connect to your computer across the Internet from virtually any computer, Pocket PC, or Smartphone. Once connected, Remote Desktop gives you mouse and keyboard control over your computer while showing you everything that is happening on the screen. With Remote Desktop, you can leave your computer at the office without losing access to your files, applications, and e-mail. Your sales force will be able to access the latest pricing sheet from on the road by using Remote Desktop in Windows XP Professional. With Remote Desktop, you can connect to your work computer from home and access all of your programs, files, and network resources as though you were actually sitting in front of your computer at work.

D. CLI-oriented tools

CLI "Command Line" remote administration tools are sometimes needed, for instance to execute non-interactively system administration scripts. PsExec is a convenient tool for Windows systems administrators because it allows to execute processes on a remote system, provided the server service is available "TCP ports 445 or 139" and that you have local administrator credentials on the remote system.
PsExec first copies its executable, psexesvc.exe, contained in the psexec.exe binary, using SMB, under %systemroot%\System32\, installs the service and starts it. These steps require administrator credentials. If you are logged on with local credentials that also correspond to local administrator credentials, with a domain administrator account or with an account with username and password identical to a local administrator account on the remote system, additional credentials are not needed. Rcmd is a Windows NT 4.0 Resource Kit tool composed of a Windows service and a command line client that supports remote process execution.
The Rcmd service opens a named pipe, \pipe\rcmdsvc. The Rcmd client establishes an SMB session to the IPC$ share, authenticated with an account that needs to have the SeInteractiveLogonRight logon right "Allow log on locally".

E. Web based tools

One of the major issues confronting information systems "IS" managers today is how to provide secure access to corporate IS resources to people who are physically located outside of the corporate network. In today's increasingly connected society, traveling salespeople, telecommuters and staff working extra hours all need real-time access to resources on corporate networks. For security reasons, these resources, such as databases, sales tools and email are usually protected by firewalls so that users outside the corporation cannot access them. Companies are looking for ways to provide cost-effective network access to their remote and mobile employees. Many Remote-control solutions are one way to provide this access. The Web based remote administration tools like GoToMyPC is a hosted service that enables secure browser-based access to any Internet-connected Microsoft Windows-based PC. Features include a screen-sharing Viewer, drag-and-drop File Transfer, Remote Printing, Guest Invite and Chat.
Corporate administrators have access to extensive management and reporting tools that enable central control over these remote-access services. While choosing a Windows remote administration tool, the following characteristics have to be considered the TCP ports required to use the remote administration feature the supported authentication mechanisms, system authentication implemented by Windows, application level authentication only.

VI. WORKING MECHANISMS OF RATS

Before their installation, RAT-servers can be customized via RAT-provided configuration packages termed binders. This customization includes the setting of the default TCP/UDP ports utilized by RAT servers, definition of auto-start methods, encryption algorithms and designation of initial login passwords. For instance, EditServer and bo2kcfg are the binders for SubSeven v2.2 and Back Orifice 2000 (BO2K) respectively. Prior to being delivered, RAT-servers may be named as software patches or games with the corresponding binders, tricking users into downloading, un-bundling, and finally, executing such malicious programs.

During their installation, RAT-servers may piggyback themselves to other legitimate programs, termed hosts, so that they are executed every time their hosts are invoked. In this way, a BO2K-server can install itself as a thread to the host programIEXPLORE.EXE. RAT-servers typically run in the background and listen on designated network ports waiting for attacker-issued instructions, leaving victims unaware of their damaging activity.

There is a multitude of avenues to spread Trojans to victim machines; the most notable for the time being are Instant Messengers (IM) and peer to- peer (P2P) systems. With the help of either MSN-messenger or KaZaA, an attacker may freely visit chat-rooms, scan buddy-lists, or even randomly select candidate victims among encountered active users, and subsequently deliver RATs to victims. Additional delivery options include HTTP servers especially created to disseminate Trojans along with regular web-pages, opening Email attachments, execution of malware and distributions for software patches, freewares, and/or games. Hence, anti-Trojan systems are easily defeated if their RAT-detection methods cover only a small portion of such propagation channels. The IP addresses, TCP/UDP ports, access passwords, and other information of RATservers can be obtained by intruders through feedback channels. IM/P2P systems, Email services, and shared folders can even provide auto-notifications between RAT-servers and clients. In Guptachar for example, an attacker may set up an IRCserver via its IRCBOT function by providing a login account nickname; every time a compromised system is activated, it connects to the above IRC-server using nickname to upload the victim's IP-address and port number. Furthermore, most RATs resort to multiple methods to outlive system crashes or reboots and evade AVs/IPSs/IDSs. By editing Registry entries, modifying system files such as win.ini, system.ini and autoexec.bat as well as inserting items on the startup folders, RATs can easily "hide" and be transparently triggered on every reboot. In this regard, host-based detection methods are inferior to their network-based counterparts as far as RAT detection is concerned.

On Windows computers, three tools commonly used by intruders to gain remote access to your computer are

1. BackOrifice

Back Orifice (often shortened to BO) is a controversial computer program designed for remote system administration. It enables a user to control a computer running the Microsoft Windows operating system from a remote location. The name is a pun on Microsoft BackOffice Server software.

2. Netbus

NetBus or Netbus is a software program for remotely controlling a Microsoft Windows computer system over a network. It was created in 1998 and has been very controversial for its potential of being used as a backdoor.

3. Sub Seven (help to hack other pc's).

Sub7, or Sub Seven, is the name of a popular Trojan or backdoor program. It is mainly used by script kiddies for causing mischief, such as hiding the computer cursor, changing system settings or loading up pornographic websites. However, it can also be used for more serious criminal applications, such as stealing credit card details with a keystroke logger.

These back door or remote administration programs, once installed, allow other people to access and control your computer.

Check if any unwanted program found in your system using the process monitor from **remote administration programs Tools**, you will see whether any foreign programs are running on your computer. If you find some unwanted program, you can terminate it by clicking the 'Terminate Process' button on the Toolbar, so you can find out what programs are started behind your back.

VII. CONCLUSION

Using remote administrator tools for remote administration of computers running can greatly reduce the administrative overhead. Administrators can access the servers from anywhere, be it inside the computer room. They can start time-consuming administrative jobs, disconnect, a later time to check the progress. Server application and operating system upgrades can be completed remotely, as well tasks that are not usually possible unless the administrator is sitting at the console. Server file system tasks such as copying large files and virus scanning are much more efficient when performed within a remote tools session, rather than using utilities that are executed on a PC client. Remote administrator tool is an affordable tool that any small business owner can purchase without

having to consult his accountant. Companies offer very flexible licensing policies for Remote administrator tool that cover multiple computers at minimal expense. Remote administrator tool has no special hardware requirements. Even if your old home computer is what you use for running your business, it's fast enough for Remote administrator tool. If the computer runs Windows, Remote administrator tool will run on it, and it will run faster than any other remote control software you can buy. An evaluation is being built on existing remote administrator tools of the availability of features and is expected to be one of the important evaluations used by major high-energy research. This evaluation let customers choose their need of remote administrator tools carefully.

REFERENCES

[1]. Remote administration tools: A comparative study Anis Ismail, Mohammad Hajjar, Haissam Hajjar Department of Computer Network andTelecommunications Engineering University Institute of Technology – Saida, Lebanese University.
[2] A Single Interface Remote Administration Tool: Rajesh Ratnala July 2011
[3]. Catching Remote Administration Trojans (RATs) by Zhongqiang Chen , Peter Wei and Alex Delis.
[4]. Trojan Horse program Back door and remote administration programs: Ibrahim Al qarout New York Institute of Technology Institute (NYIT)-Jordan.

