Department of Energy

CIAC

Computer Incident Advisory Capability

UCRL-ID-130898

IRC on Your Dime? What You Really Need to Know About Internet Relay Chat

CIAC-2318

Jerry Rayome

June, 1998

Lawrence Livermore National Laboratory

CIAC is the U.S. Department of Energy's Computer Incident Advisory Capability. Established in 1989, shortly after the Internet Worm, CIAC provides various computer security services to employees and contractors of the DOE, such as:

- Incident Handling consulting
- Computer Security Information
- On-site Workshops
- White-hat Audits

CIAC is located at Lawrence Livermore National Laboratory and is a part of its Computer Security Technology Center. CIAC is also a founding member of FIRST, the Forum of Incident Response and Security Teams, a global organization established to foster cooperation and coordination among computer security teams worldwide.

IRC on Your Dime?
What You Really Need to Know About Internet Relay Chat

UCRL-ID-130898

CIAC-2318

June 15, 1998

Jerry Rayome
CIAC/LLNL

With special thanks to
Steve Romig
Ohio State University

Introduction

The purpose of this paper is to describe recent trends CIAC has encountered while working with sites that have been compromised. Frequently, the intruders set up and run Internet Relay Chat (IRC) to exchange information and to show off their success at having compromised a site. Invariably, this protocol consumes bandwidth, uses CPU cycles and is a source of embarrassment for the site. This paper focuses on these negative aspects of IRC and concedes that one can cite numerous examples where IRC is used in a positive manner.

What is IRC?

Some individuals describe IRC as a "citizen's band radio for the Internet." The Request for Comments 1459 (RFC1459) documentation describes the technical details of the IRC protocol and various user commands. One can utilize a search engine to locate RFC1459.

In practical terms though, IRC allows users to chat with each other over what might be “great” distances without incurring the associated “long distance” and “conference call” charges typical of ordinary telephone services. Often times, Internet Service Providers (ISPs) provide this “chat” service in addition to their “Surfing the Web” services. Netscape Corporation and Microsoft Corporation both provide IRC services or chat rooms for their world wide web browsing customers. Some common IRC clients used by intruders are Eggdrop, mIRC and BitchX.

The IRC Protocol

IRC is implemented using the TCP/IP protocol in a client/server model. At the client’s request, a server establishes a socket for the client/server communications and then listens on that socket for client requests. Servers also establish and maintain server-to-server communications in an IRC network. Clients can query servers to gain information about other IRC servers and other IRC clients within the IRC network.

There are several publicly available IRC client and server applications to choose from. Once a client is chosen, installed and run by the user, the client carries out commands and actions on behalf of the user. User commands are those that the user executes by typing out the command. There are numerous actions that are carried out on behalf of the user in both an interactive and a background modes. Typically these actions handle the message passing responsibilities and maintain connectivity with the IRC server while the user is inactive or away from the terminal. However, it is the interactive use that we should be most concerned with.

How IRC is Used

As stated above the intended purpose for IRC is to provide a conference call environment. This is accomplished by the creation of a virtual channel or “chat room”. An IRC user can create a channel by being the first to join a non-existent channel; this user becomes the channel operator. The channel operator possesses special privileges that are not given to ordinary channel members. It is intended that these special privileges be only used for channel maintenance responsibilities. If they choose, channel operators can give these special privileges to other channel members. All too frequently though, these special privileges are abused. The privilege to remove someone from a channel is a special privilege. Naturally, this privilege should be used sparingly and under appropriate circumstances. And yes, this is one privilege that is most often abused.

Abuses and conflicts within channels give rise to “channel wars”. Often channel wars are the result of obnoxious channel members being either kicked off of the channel or banned from joining the channel again. Sometimes these rogue IRCers will circumvent their banned status by joining the channel as another user from a different source address; one that is not banned from the channel. This is one reason why intruders show up at your site. More frequently though, they create their own channel and flood the channel they are banned or “kicked” from with unsolicited network traffic like syn/ack or ping flooding.

Some people question whether IRC is a good thing. That depends on how it is used and who is incurring the charges for these services. Few would argue that legitimate IRC users pose a threat or do any harm. The operative word here

is “legitimate”. In this context, one can define “legitimate IRC users” as those individuals who’s CPU cycles, disk space, network traffic and Internet access is monetarily compensated for, by an appropriate entity like a commercial enterprise, an ISP, a government agency or a private individual who owns their own IP address.

Given the above definitions and the premise that an IRC user uses IRC for its intended purpose, then the answer to the question is...yes. IRC is a good thing. However, outside these confines, IRC quickly erodes into an unsavory mechanism for vulgarity, illegal and lascivious activity.

How Intruders Use IRC

Intruders frequently use IRC to share compromised passwords, warez, exploitable information, exploit tools, pornography and vulnerabilities associated with particular sites. Sites that have high-bandwidth Internet connections and muscle machines (high-speed systems with large disks and plenty of memory) are favorite targets for intruders. These sites have the local resources that are necessary to efficiently store and deliver warez to other warez consumers using the IRC server eggdrop.

IRC also provides the means for intruders to brag about their accomplishments. This is especially more convincing and therefore, rewarding if they can provide proof to back up their boasts. Often this is achieved by installing and running IRC on the compromised host so that the domain name itself supports their purported claims. Furthermore, an additional amount of personal gratification is acquired if the compromised host incurs the cost of operating the IRC activity. The degree of gratification varies depending on the degree of difficulty/risk associated with the effort required to compromise a host at a given site.

What precautions will an intruder take to avoid the risk of detection while attempting to compromise a hardened site?

- They will work stealthily to avoid detection while continually checking for signs that they are being monitored.
- If they do not already possess enough privileges, they will gain them by exploiting a vulnerability or through a previously installed backdoor.
- They will continually check to see if a system administrator is on-line.
- They will remove any evidence of their presence from log files.
- They will create a hidden directory just below the root of the file system.
- They will download their tools to this hidden directory.
- Finally they will install their Trojan binaries or Trojan runtime modules that hide their presence and the processes they are running.

If the intruder has not been detected by the time these tasks are accomplished, then the intruder will probably never be detected. At this point, all of the conventional utilities that would reveal information about the intruder are keeping this information from the system administrator. It is here that the stealthy intruder will essentially become invisible.

Now the intruder who seeks the notoriety for their accomplishments will set up and run IRC. Naturally, it will be an “invitation only” channel since outsiders are not welcome. Usually they will try to obtain a copy of the password file to be cracked off-line or they might distributed it among others so that they can help share the CPU intensive burden associated with password cracking. Cracked passwords and their associated logins are traded like baseball cards among the intruder community. Sharing them and information regarding site specific vulnerabilities promotes camaraderie and elevates one’s position among the intruder community.

Intruders occasionally have an escape plan in place in the event that they are detected. Escape plans vary widely. Some are as crude as simply bailing out of the system, while others are more sophisticated. More elaborate plans involve tricking the DNS server into caching a bogus hostname/address for their host so that it is difficult to trace the intruder back to their origin. A typical escape plan will be to remove any evidence of their activity, install a network sniffer, Trojan important system binary files and leave quietly. Often this involves creating an account for future use in case the vulnerability they used to compromise the host is removed. Frequently, they will Trojan the

login process so it will allow them to login the next time. This is the preferred method since it does not add an additional entry to the password file. Some system administrators routinely check for the presence of new or suspect accounts.

How to Detect IRC Activity

What else can a system administrator look for to determine if their site has been compromised? Look for the presence of IRC! If your site strictly prohibits IRC activities and you discover evidence of IRC activity on your network, then it is an EXTREMELY STRONG indication that your site has been compromised. Be careful though; do not gain a false sense of security by the absence of IRC activity at your site. The absence of IRC activity does not imply that your site has not been compromised. Some intruders are stealthy and will not risk detection by running IRC to impress others.

How can one detect the presence of IRC activity on their network? This can be done in two ways. The first method is to check for evidence of IRC activity on a host-by-host basis. The second method is to monitor network traffic.

First let us examine the host-based method. Here we look for suspicious hidden directories. Most often these are located just below the root of the file system; however, frequently they are found further down the file tree in directories like /dev. When one is found, look for the source code for exploit tools, well-known daemons or system commands that may be Trojaned. Frequently these are written in the "c" programming language and have the ".c" extension or they are executable shell script files. Also, be on the lookout for IRC files like Eggdrop, mIRC or BitchX and IRC support files that list servers, clients and channels. Look for a tool called datapipe.c that takes input from one port and outputs it from another port. Finally, since we are dealing with the intruder element, look for pornography.

A less useful method is to scan the semi-standard IRC ports 6666-6667. However, IRC is not bound to these ports and intruders often use higher port numbers in the 6555X range. To detect IRC activity using a port scanning method one would have to continually scan these, and possibly other ports, searching for an IRC response. For this to be successful two requirements must be satisfied. First, the IRC agent is listening on that port when the scan takes place. Secondly, the port scanner is able to identify the IRC service response. It is conceivable that an IRC response from a customized IRC server might incorporate a secret response mechanism. This mechanism would prelude its identification as being an IRC service by a standard or non-customized IRC port scanner.

Detecting IRC activity using the network monitoring method is probably more reliable than the host-based method. There are two strategies one might employ using this method. The first strategy is to analyze the network traffic, searching for patterns that resemble IRC activity. Remember that IRC is similar to a conference call environment. In that environment, a message sent to the channel by a client is dispersed to all of the members of that channel in real time. This does not hold for private messages between individual clients. In general, the IRC server is sending packets from a particular port to all of its channel clients. The network analyzer must keep track of packet header information regarding the source address, destination address, port number and packet type for this to be successful. Simultaneously the analyzer must sort through this information looking for patterns that match IRC activity. The pattern matching phase might be a non-trivial task to implement in real time. A scaled down version of the network monitoring method would detect IRC activity by looking for repeated or persistent unknown TCP sessions that are neither FTP nor Telnet sessions.

The second network monitoring strategy is more intrusive than the first strategy. Rather than simply use the packet header information to perform network analysis, this strategy looks at the contents of each packet and attempts to match the data against a set of user defined strings. A typical set of user defined strings will contain IRC specific strings like NICK for the client's nickname, USER for the user name, PASS for a password, JOIN for joining a channel, OPER that says a regular user wants to become a channel operator or PRIVMSG that says the message is a private message. This is just a sample of the types of user defined strings that should be searched for while attempting to detect IRC activity on a network using packet analysis. Implementing this strategy is fairly straight forward for most network intrusion detection software.

There have been several cases where the FBI has successful prosecuted computer criminals where IRC was used in the manner described throughout this paper. Recent trends suggest that intruders are not only using private channels

to communicate, but they are also using encryption as an additional means of securing their communications. Employing this technique within IRC effectively eliminates any hope for successful packet content analysis strategies, unless the encryption algorithm and passphrase are compromised. If the encryption algorithm and the associated passphrase were acquired, then the encrypted versions of the above clear-text strings would be temporarily added to the list of strings to match against.

Conclusion

It is important to note that the prohibited IRC activity does not just happen by itself. Intruders download, setup and run IRC after they have compromised a host. Therefore, the best defense against having IRC run on your network is to prevent intruders from compromising your systems in the first place. Adhering to good computer security practices and ensuring that all systems on your network have the latest patches installed, is the best way to prevent a system compromise. If intruders cannot compromise your system then they cannot install and run IRC on your systems.

APPENDIX A: CONTACTING CIAC

Phone	(925) 422-8193
Fax	(925) 423-8002
STU-III	(925) 423-2604
Electronic mail	ciac@llnl.gov
Emergency SKYPAGE	800-SKYPAGE pin# 855-0070
Anonymous FTP server	ciac.llnl.gov (IP 128.115.19.53)
BBS	(925) 423-3331 (9600 Baud) (925) 423-4753 (2400 Baud)

Reader Comments

CIAC updates and enhances the documentation it produces. If you find errors in or have suggestions to improve this document, please fill out this form. Mail it to CIAC, Lawrence Livermore National Laboratory, P.O. Box 808, Mail Stop L-303, Livermore, CA, 94551-9900. Thank you.

List errors you find here. Please include page numbers.

_____

_____

_____

_____

_____

_____

_____

_____

List suggestions for improvement here.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Optional:

Name _____ Phone _____

Stamp

Computer Incident Advisory Capability
Lawrence Livermore National Laboratory
P.O. Box 808, L-303
Livermore, CA 94551

Department of Energy

CIAC

Computer Incident Advisory Capability

Technical Information Department • Lawrence Livermore National Laboratory
University of California • Livermore, California 94551