

Dealing with mIRC Script Worms (SCRIPT.INI) and mIRC Trojans

[The RIMC Project] [RIMC ITW Statistics/Hot List]
[Infected?] [How to protect from scripts] [How to remove scripts]
[The DMSetup Worm/Trojan] [JeepWarz Analysis]

A Virus or Trojan via IRC?

There's currently a threat that you should be aware of -if you use the mIRC program- to chat over the Internet. mIRC is a popular program used to access the IRC (Internet relay Chat). mIRC supports a script language that is interpreted by the mIRC program; the mIRC scripts and can be sent as files from one user to another. This script language can automatically execute commands and can perform specific commands triggered on predefined words that someone types during the chat.

Beside that, if your IRC client is able to receive files there is the possibility that someone send you a Trojan via IRC (or E-mail or ICQ etc.). A very popular Trojan is DMSetup. This Trojan installs itself and manipulates mIRC in that way that copies of this Trojan are send out using the mIRC script language.

There are currently a number of worms that can be spread to your PC. We define these as worms not as viruses since they do not modify existing programs on your PC but rather simply transfer themselves from PC to PC. The worms travel via a file named SCRIPT.INI that must be transferred into the mIRC program directory in order to execute. Versions of the mIRC program prior to version 5.3 will transfer a downloaded SCRIPT.INI file into the same directory with the mIRC program. This allows the SCRIPT .INI file to automatically be executed. (This serious flaw was promptly fixed by the author with version 5.3 where all downloads go into a separate download directory by default.)

The worm is very simple. It is based on the assumption that when mIRC (versions before 5.3) is first installed on a computer, it by default is set up to load a script called SCRIPT.INI in the mIRC directory. When mIRC is first set up, there is no SCRIPT.INI file, so nothing happens. However, if somebody sends you a SCRIPT.INI file, and you save it into your mIRC directory, then the next time you run mIRC, it will follow its default behaviour of loading SCRIPT.INI if the SCRIPT.INI happens to contain malicious code, it will be executed by mIRC!

How does you become "infected" with the SCRIPT.INI worm? You will get infected when somebody sends a SCRIPT.INI file via DCC (Direct Client-to-client Connection; a way of transferring files and conducting chats, bypassing the IRC network.) You can only be infected if you accept the DCC request! However, many people will go ahead and accept the file without knowing what it is. Worse, some people will have turned on a feature in mIRC called Auto Get; this will cause mIRC to automatically accept any DCC request! Once the SCRIPT.INI is in your mIRC directory, it will be loaded by mIRC the next time it is started. The script will then perform whatever functions it was programmed to perform (which will be discussed later).

What the worm does

There are several variants of this worm, all of which do different things. Some variants will send all your channel and private messages to a certain channel or person. This compromises both your privacy and security. It will allow people to listen in on your conversations, and even get secret passwords that you might be /MSG'ing. Some will listen in for trigger words that will allow somebody to take control of your mIRC client; and through you take over your channels! Most versions will send themselves to other people via DCC, without your knowledge! Some versions will even go so far as to damage the files on your computer, and even tamper with your Windows system files! Finally, the more advanced versions will override some of mIRC internal commands in an attempt to prevent you from removing them.

How to tell if you're infected?

The most obvious sign that you are infected with the SCRIPT.INI worm is that there is a SCRIPT.INI file in your mIRC directory. However, this is not a telltale sign. The SCRIPT.INI file could be harmless. The only way to tell for sure is to look at the file and see if it contains malicious code (if you have any code reading skills.) However, if you're not sure, the safest thing to do is to simply delete it.

It is also conceivably possible for a script other than SCRIPT.INI to be a worm. Don't assume that you're not infected because there is no SCRIPT.INI file. Also, don't assume that you are if you do see one.

Another way to tell if you are infected is if somebody tells you that you're sending a SCRIPT.INI file to him or her, and you know for certain that you're not. This worm will spread itself by DCC sending itself to other people without your knowledge.

Some variants of this script will echo all your channel and private messages to a certain channel or person, so you may see a bunch of error messages saying something to the effect of "can't send to channel" or "can't send to nick". This is another sign that you're infected.

How to remove the worm

First of all, don't try to remove the worm from within mIRC. It's much safer, and more effective, to remove it externally. If mIRC is up and running, shut it down.

The first thing to do is to look at the folder containing mIRC and look at the SCRIPT.INI file. Open it up in the Notepad and examine it for any code that DCC sends the script to other people, or sends MSG to people or channels with the text you type, or anything else suspicious. If you're not familiar with mIRC scripting, simply delete the file.

You should also examine other .INI files for similar code. If you're not sure what files are scripts, open up the MIRC.INI file and look for a section called [rfiles]. This section will contain a list of all scripts loaded by mIRC. If in doubt, delete them all. You're playing with fire if you're using any script without knowing what it does.

Another file to check is ALIASES.INI. Check it for any aliases that try to override internal commands, particularly overridden commands that would

allow you to remove the worm. If in doubt, delete this file also. You'll lose any aliases that you've defined, but this will ensure that no aliases created by the worm are left behind.

Once you start up mIRC again, all scripts should be cleared (unless you've left some behind that you've checked and found clean). To be sure, press ALT+R to bring up the remote script window, and then open the View menu. This will list any scripts that are opened by mIRC. Either the list will be empty (unless, as stated above, you deliberately left some behind), or any scripts that are in the list will be blank when you select them. Also look at the Aliases tab; it should contain no aliases, unless you manually checked it and found it clean, rather than simply delete it.

Several web sites covering this topic go through a song-and-dance routine, giving you a string of commands to remove the virus. This procedure is (in my expert opinion) not as secure (or as simple) as simply going through and deleting any suspicious files. If the file's not there, it can't do anything to you!

A final note; if you think you've been infected, I would appreciate it if you e-mail me a copy of it before you delete it; I would like to analyze the various versions of these scripts. PGP keys are available from PGP key servers as well as you can find them in the file "ROSEBBS.TXT" (included in ROSE SWE distributions).

How to protect yourself

Here are some simple steps to take to protect you from the worm:

- Don't accept a DCC file if you don't know what it is, especially if it's a .INI file.
- Check and make sure that the Auto Get option is turned off in mIRC. To check, go to DCC menu and select Options. In some versions the entire DCC Options dialog is all in one window; in later versions the Auto Get options is under the "Send" tab. In either case, look for the "On Send request:" option, and make sure it's not set to "Auto get file".
- Change your default download directory to somewhere other than your mIRC directory. Again, this is somewhere in the DCC Options dialog. In later versions of mIRC, these is under the "Dirs" tab. Select the "(Default)" entry from the selection box, click "Edit", and change the directory.
- Upgrade to mIRC 5.4x. It will automatically take the above precautions.
- Use F_MIRC or RHBVS and scan your mIRC directory

The DMSetup Trojan/Worm

What is DMSetup?

The "DMSetup.exe" file is a worm which passes itself from one mIRC user's computer to the next by infecting the MIRC.INI file and other files in their computers. It does this by changing mIRC remote scripts and thereby sending itself to anyone joining the channel the infected mIRC user is in. This is done with the IRC file transfer protocol DCC. You should be suspicious of any file you are sent with a .Exe extension. The chances are it is "DMSetup.exe" which has been renamed or some other kind of malware.

The original DMSetup worm uses the filename "DMSetup.exe". There are a lot of different filenames being used by the DMSetup.B-H worms to circulate the "DMSetup.exe" worm. This newer variants change their own name with every infection. Names for DMSetup2.exe are any two of these words joined together with .Exe and/or .INI :

**buny love sex toe pee inst god fun ICQ IRC
mIRC powr jnk nuke udp lim set cfg hell pussy
tit dik 69 101 yes arm 311 bud fuck eat**

So BunyLove.exe, BunySex.exe, LoveBuny.exe, LoveSex.exe, SexBuny.exe and SexLove.exe are all possible etc.

In this document the worm will only be referred to as DMSetup. This worms are between 40 and 90 KB. Their length vary, because sometimes the file is cutted by a broken connection. Nevertheless those truncated files are still executable, because the main worm is only about 35 KB long, the rest is appended trash to make him survive better!

RHBVS & VSP currently scans the DMSetup worms as DMSetup.??? Trojan

Indications of infections

There are some obvious clues.

- Your pop-up and scripts have changed.
- You are unintentionally sending files to people.
- Your user name has changed, and now you have a user name of "s": for example, your /whois address used to be myname@internet.provider.com and now it's s@internet.provider.com

When you run a file containing DMSetup.A, the file will...

- Edit AUTOEXEC.BAT so that the infected file is run every time you start the PC.
- Create a CONFIG.SYS file that says NI! (the file is 5 bytes)
- Copy itself to C:\, c:\windows\, c:\mIRC\ and c:\program files\
- Edit SCRIPT.INI to auto send himself on joins to channels.
- Edit remote.ini to quit a channel leaving a message behind.
- Create a new MIRC.INI, which will load mircrem.ini
- Disable fserve warnings
- Displays error type 0 (so that you think the download is broken).
- It enables listening for fserve, send and chat, and sets port to 59

The new MIRC.INI installed by DMSetup.exe will

- overwrite your old settings, remove notify & channel lists, etc.
- Window fonts will be back to default Fixedsys
- your nick will be "a", user ID and full name field "s".
- the dccserver will be enabled for chat, send, and fserve,
- this will allow outsiders to access your hard drive
- fserve warning will be disabled, and the root directory will be c:\mIRC\
- cause you to send the DMSetup.exe file to other people
- cause you to quit IRC if sent a /MSG with the word "goawaysilly"
- quit message will be "'tis to I who seem so sad"
- some versions will allow others to run executables on your computer
- some versions will disable you from going to channels #nohack, #mirchelp, #mirchelp, #operhelp, #help, #helpdesk, #help-desk, #helpcenter and #dalnethelp
- some versions will cause you to quit if you are /noticed with "I hate your guts with a passion"
- some versions will cause you to say silly things on the channel.

In rare cases, if the DMSetup worm can't install properly it will do a rather destructive action. It will show a display of multicoloured rings and circles in a screen saver like fashion. While it does this, it fills the hard disk with directories that have garbage names and are difficult to remove again

How do I remove DMSetup from my PC?

Unload mircrem.ini by typing /UNLOAD -RS MIRCREM.INI in any mIRC- window. Open C:\AUTOEXEC.BAT and remove the DMSetup line - save and exit. Delete the following files:

C:\DMSETUP.EXE
C:\CONFIGG.SYS

Assuming, you have installed mIRC into C:\MIRC
C:\MIRC\DMSETUP.EXE
C:\MIRC\MIRCREM.INI
C:\MIRC\BACKUP0412.INI

C:\WINDOWS\DMSETUP.EXE
C:\PROGRAM FILES\DMSETUP.EXE
C:\MIRC.INI

mIRC Worm analysis - "JeepWarz"

This is an analysis of "JeepWarz", one of the mIRC SCRIPT.INI worms. This analysis comes from analyzing the script code, but "live testing" (taking an infected client online; isolated in a private room, for safety; for testing.) has not been carried out yet. JeepWarz is named after the name of the channel that it sends all console inputs to.

This script is apparently disguised as a script that does some useful functions. The script is the most ingenious one I've seen yet; it actually performs a few useful functions, but buried within some of them is security compromising code. The code is hidden by being located starting well past the 300th column in the file, so it can't be seen unless you scroll a long distance horizontally.

The worm performs the following functions

- When it first loads, it:
 - Turns on remote listening
 - Puts all DCC send requests on auto ignore
 - It places the words "(Not connected)" in the status bar
- When mIRC is first connecting to a server, it places the words "(Connecting to server name)" in the title bar
- When mIRC connects to a server, it places the words "(Connected to server name)" in the title bar, and then sends a message to the channel #JeepWarz giving your IP address, and server name and port
- When mIRC disconnects from a server, it places the words "(Not connected)" in the title bar.
- Whenever you type anything in mIRC, the script:
 - If you enter something in the status window without a /, it executes the command as if you had typed it with a /
- When you ping someone, the script sends a message to them giving them their lag time
- When you get pinged by someone, it sends a ping back to him or her. If there is a hidden command in the ping request (in the 3rd parameter, which will be empty in a legitimate ping request), it will execute the command
- If you are banned, but have ops, it will unban you
- When someone besides you joins a channel, it sends itself to the person that joined. If they are in more than two channels that you are in, it will send a message saying, "Following me?"
- When you join a channel, it echoes the topic into the channel window. If the topic contains the words "SCRIPT.INI" in the topic, it will immediately exit the channel.

Final analysis: This worm is quite capable of compromising security. It sends all input that the user types to a hidden channel, possibly transmitting passwords and private information to (presumably) the people that created the script.

The ROSE IRC Malware Collector - RIMC

The RIMC is a set of scripts and tools that try to download from IRC malware (viruses, Trojans and script worms). RIMC consists of a IRC robot, some DOS batches, AWK scripts and a few self written tools. RIMC has logging and statistics functions as well as it will warn users that are infected. The used scanner is ROSE SWE's Heuristic Based Virus Scanner (RHBVS) which was enhanced for this task.

The RIMC "Hot List"

[illegible]

RIMC Cummmulated Statistics

This web page requires Java Script! None of the materials from this site may be reproduced without prior consent of the copyright owner.
Document \$Id: f_mirc.htm.v 1.21 2020/12/21 15:34:41 ralph Exp \$