

Ghiribizzo's Cracking Tutorial

Lazy Cracking 1 : Re-cracking ClipMate 4.5

Re-cracking ClipMate 4.5

Lazy cracking is an art. It is for the times when you think to yourself: "I don't give a damn". When you couldn't care less how the target program works, or just want to get it cracked as quickly as possible. The quickest, most brutal and unrefined 'cracks' of this type are by far the most satisfying and amusing.

PGP and Signed Tutorials

My tutorials and programs should be signed electronically using PGP. PGP 5 supports DSS/Diffie-Hellman keys. These keys are not supported by previous versions of PGP.

You should check the signature to make sure that the tutorial and especially its program files have not been tampered with. All cracks, tutorials and zip files I release will be signed. This will prevent tampering and will hopefully reduce the chances of viral infection.

My signature will also be the only way you can identify me as my email address will often change.

My Web Site:	http://www.geocities.com/Athens/3407
My Email:	Ghiribizzo@geocities.com
My Backup Email:	Ghiribizzo@hotmail.com

This document is Copyright © 1997 by Ghiribizzo. This document may be distributed non-commercially, provided that is it not modified in any way. This publication may not be sold or packaged, in whole or in part, as a service, or with a product for sale in any form without the prior written permission of the author. This document is presented with no warranties or guarantees of any kind including fitness for any particular purpose. If you use the information contained herein, you do so at your own risk.

Re-cracking ClipMate 4.5

What is it?

ClipMate 4.5 is a program which extends the functionality of the clipboard by allowing multiple objects to be placed in the clipboard. As a lazy cracker, your first objective should be to evaluate the program and see if it is worthy of cracking. Maybe there are better programs that do the same thing. ClipMate is a hugely bloated program clipmt45.exe takes just under 1MB of hard disk space (the whole lot taking around 3MB) but what's worse is that it takes up around 2.7MB of RAM! Now I consider this excessive and would look for a better program or write a leaner one myself - after all, 4.5 has added "*an industrial strength printing engine*" and other junk which isn't what you really want anyway. But, if you can't program, are too lazy to search for another program or actually like the program then read on.

OK. Let's crack it... quickly.

ClipMate 4.2 has been cracked to death with many serial/password combinations flying though the newsgroups. The easiest way to get on with your life is to simply use the serial you had from the 4.2 version either your own or one stolen from the newsgroups. I hear sharp intakes of breath from some crackers aghast at such a suggestion. We'll discuss the 'ethics' of laziness later but let's continue. So, you've got your old serial and want to use it. You'll be glad to know you can - unless...

Oh, my God, I don't believe they could be *so stupid*!

.. you happened to give out your serial to the world or are using a stolen serial. Why? Because the author has been a moron and decided to hardwire some of the most common serials into the program so that they can't be used (why has he bothered to do this? The 'new' serials will be out as soon as he publishes his program). You will notice this if you are upgrading (the program gives an error on loading) or when you enter the stolen serial (it registers OK but then has the same problem as upgrading when you try to start the program again).

Stupid, stupid!

You want to register it as quickly as possible. Obvious quick lines of attack are to examine the program. Get a raw listing of the program i.e. examine it using a hex editor. Search for some serial owners: PROMETHEUS, THATDUDE AND DJPAUL all show up in there without even a vague attempt at obfuscation. The author's attempt to protect his work is, in fact, a liability. Quick answer? We assume that ClipMate will read the serial owner from the ini file and then check to see if they match with the above and if they do, give an error. So the blunt way to do it would be to damage these strings, a single bit in each one should do it. So we quickly alter one byte in the specific one. And try again...

Hmm. Still no joy.

Unfortunately, that didn't do it. We'll assume then that the serial code is also checked. So we examine clipmt45.exe again. Searching on the string doesn't reveal anything. But look! Near the serial names are several 8 byte long strings. Only they are obviously (if you're into cryptography) encrypted strings. Now, it would be easy just to decode the strings there and then but we want to do it quicker than that even. So let's just hack each one again. We alter one or more bits in each of the strings, save and reload.

Cracked it

And there we have it. You can now use a bloated and buggy program. It works and what's more we cracked it in less than a minute - slightly more if you're a slow typist or were silly enough to quit windows to run the hexeditor. Admittedly it was no huge intellectual feat, nor was there that buzz you get when you finally 'beat' a protection scheme. However that buzz has been replaced by a buzz of another sort - a buzz you get when you realise that you actually managed to get away with such a crude hex hack and saved some of your valuable time.

'Ethics'?

There are always those who will turn their noses up at such a poor 'crack' in fact, I myself am reluctant to call it a crack. It isn't really a crack in that it relies on you're previous cracking work, but it saves you from doing it all again. Looking over what we actually did. You could have performed the above steps *with absolutely no knowledge of 'cracking'*. Good, eh?

I don't think these shortcuts should be overlooked. Of course you don't gain the cracking experience you would get had you actually done the job properly; nor can you make a key generator. But if you're just after some software, you get the same results a hell of a lot quicker. I admit that I am the lazy type; that's because I value my time highly. I waste enough time writing this rubbish. If you don't mind wasting your time sitting in front of a computer or pouring over pages of disassembled code then fair enough - you have my sympathy. There's a *real* world out there, you know.

By the way, if you *are* just after software, think. There are better ways of getting it free than cracking and I'm not talking about warez. Just a little time thinking can save you both time and money. Don't even bother emailing me. You've got a brain - use it or buy your software.

Other Tutorials

Not all of my tutorials are on the web. That's because I haven't written most of them yet. However, when I do, you can be sure I will make them freely available to everyone. After all, why else would I bother to write these things in the first place.