



<http://www.lockless.com>

proudly presents

Krypton the Krypter

version 0.5

for Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP

Created by Yado

Official user's guide

END-USER LICENSE AGREEMENT FOR KRYPTON THE KRYPTER

Important - read carefully:

This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and the mentioned author of this Software for the software product identified above, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the SOFTWARE PRODUCT.

SOFTWARE PRODUCT LICENSE

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE.

This EULA grants you the following rights:
Installation and Use. You may install and use an unlimited number of copies of the SOFTWARE PRODUCT.

Reproduction and Distribution. You may reproduce and distribute an unlimited number of copies of the SOFTWARE PRODUCT; provided that each copy shall be a true and complete copy, including all copyright and trademark notices, and shall be accompanied by a copy of this EULA. Copies of the SOFTWARE PRODUCT may be distributed as a standalone product or included with your own product.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

Limitations on Reverse Engineering, Decompilation, and Disassembly. You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

Separation of Components.

The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one computer.

Software Transfer.

You may permanently transfer all of your rights under this EULA, provided the recipient agrees to the terms of this EULA.

Termination.

Without prejudice to any other rights, the Author of this Software may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the SOFTWARE PRODUCT and all of its component parts.

Distribution.

The SOFTWARE PRODUCT may not be sold or be included or used in a product or package which intends to receive benefits through the inclusion of the SOFTWARE PRODUCT. The SOFTWARE PRODUCT may be included in any free or non-profit packages or products.

3. COPYRIGHT.

All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and "applets" incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by the Author of this Software. The SOFTWARE PRODUCT is protected by copyright laws and international treaty provisions. Therefore, you must treat the SOFTWARE PRODUCT like any other copyrighted material except that you may install the SOFTWARE PRODUCT on a single computer provided you keep the original solely for backup or archival purposes.

LIMITED WARRANTY**NO WARRANTIES.**

The Author of this Software expressly disclaims any warranty for the SOFTWARE PRODUCT. The SOFTWARE PRODUCT and any related documentation is provided "as is" without warranty of any kind, either express or implied, including, without limitation, the implied warranties or merchantability, fitness for a particular purpose, or noninfringement. The entire risk arising out of use or performance of the SOFTWARE PRODUCT remains with you.

NO LIABILITY FOR DAMAGES.

In no event shall the author of this Software be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this product, even if the Author of this Software has been advised of the possibility of such damages.

REGISTRATION

The SOFTWARE PRODUCT is freeware software. You can use it for free, no registration is required. You must contact the author if you mean to use it for commercial purposes.

Table of contents

Introduction.....	5
History of changes.....	5
Usage notes.....	6
What is Krypton the Krypter.....	7
Requirements.....	7
 Getting started.....	 8
How does it work.....	8
Encrypting executables.....	9
ID Generator for Shareware Programmer.....	9
 KCD-Lock.....	 12
What is KCD-Lock.....	12
How does it work.....	12
 FAQ.....	 16
 Final notes.....	 17
Bug reports.....	17
Disclaimer.....	17
Thanks.....	17

Introduction

History of changes

v0.5

- Improved compatibility (it is now Delphi compatible)
- Improved K-Execution, you now have 5 levels of K-Exec. maybe your executable won't support all levels so try some of them
- K-Execution can be added to K-Protect to improve Api Protection
- Added KCD-Lock, you can now protect your CD-ROMs (see the help file)
- Added ID Generator for Shareware Programmer (see help)
- Added code for manual K-Execution (see help)
- Removed Level of Krypt, now Krypton will auto set itself
- Improved debug detection 9x/NT
- Improved loder and IAT destruction
- Fixed problem krypting executables with no resources

v0.4

- Fixed bugs (again)
- Improved K-Execution, you now have 3 levels of K-Execution, maybe your executable won't support all levels so try to decrease them if it crashes
- Added compression, with the High-Pack you can increase a lot the compression but you lose a bit (just a bit) of security
- Added Shell Ext.
- Added save config file

v0.3

- Fixed bugs =)
- Improved K-Execution
- Structure slightly changed (again)

v0.2

- Fixed a lot of bugs =)
- Added K-Execution
- Structure slightly changed

v0.1.1

- Fixed bugs thx to -alx :)

v0.1

- Added bogus opcodes
- First public release

v0.05 beta

- Some bugs fixed
- Added simple API wrapper
- Added some tricks

v0.02 beta

- Some minor fixes
- Added anti-trace
- Added smc

v0.01 beta

- First version, not public

Usage notes

Krypton the Krypter is freeware, this means you are free to use it for any non-commercial purposes, you are not allowed in any way to sell or distribute shareware or commercial programs or CD-ROMs protected with Krypton the Krypter. This program is freely distributable unless the whole package is kept exactly "as is" and no contents are modified. You must contact the author if you mean to use it for commercial purposes.

Krypton the Krypter works on the following operating systems: Windows 98, Windows 98 Second Edition, Windows Millennium Edition, Windows NT, Windows 2000, Windows XP Home & Professional. It does not work on Windows 95.

It has been tested on as many executables types as possible, if you should find any incompatibility you're welcome to report us the problems you found to: krypton@lockless.com.

You can always get the latest version of Krypton the Krypter at <http://www.lockless.com>.

You're always welcome to send your comments, critics, suggestions to krypton@lockless.com or leave a message on our forum at <http://forum.lockless.com>.

What is Krypton the Krypter

Krypton the Krypter encrypts sections of a PE-File and adds decryption code, to leave the file in (at least in most cases ;) an executable state. It's just another simple PE-Crypter.

Currently implemented features:

- Anti-debugging code
- Anti-tracer code (ProcDump, etc.)
- Anti-FrogsICE code
- Encryption of the decrypter
- Smc decrypt routine
- Bogus opcodes, making it harder to reverse the decrypter
- K-Execution
- KCD-Lock
- Compression
- ID generator for Shareware programmer

Not yet supported:

- Advanced K-Execution (coming with Krypton the Krypter v0.6)
- Api Emulator (coming with Krypton the Krypter v0.6)

Additional Info:

From 0.2 you can only make 1 layer of krypt.

Now Krypton the Krypter is a bit more compatible, it's been tested with a lot of executables, if your executable works after being crypted with no options selected you can try to add them, but be careful and deeply test it after encryption!

Requirements

To use Krypton the Krypter on your system you need the following configuration:

- Any Intel or AMD processor with at least 75MHz
- 16MB of RAM
- Windows 98 or later
- CD-R RAW DAO mode capable (if you mean to use KCD-Lock)
- CD Burning software (if you mean to use KCD-Lock)

Getting started

How does it work

Once loaded Krypton the Krypter looks this way:



Figure 2-1. Krypton the Krypter main form

The available options are the following:

Enable K-Exec: K-Execution is a technique to create a crypted executable which never resides fully decrypted in memory, this is possible with a combination or methods based on the substitution of several opcodes with wrappers or emulators which decrypt and execute the original code during the execution of the executable itself but always without fully decrypting it. Thus you'll be provided a better security because the executable will never be fully decrypted.

K-Exec Levels: number of opcodes and methods of wrap/emulation can be increased.

K-Exec on Api: enable K-Execution on Api adding itself to K-Protect on Api.

K-Protect on Api: enable a wrapper on Api calls avoiding an easy rebuilt of the IAT & IT.

High Pack Ratio: increase compression but decreases security! It should be used only if size is more important than security.

KCD-Lock: enable KCD-Lock, see next chapter for details.

Make Backup: make a backup of the target file before krypting it.

Encrypting executables

Encrypting your executables it's an easy procedure, just select the target file, enable the options you selected and press Krypt!

Test the krypted executable then, if it shouldn't work try to disable some of the features you selected, we suggest to try until you'll find a suitable configuration for your needs. If your executable should keep on refusing to run you're welcome to send it to us and we'll try to fix the next version of Krypton the Krypter to be compatible with it.

It is warmly suggested to deeply test the executable you just krypted especially before using KCD-Lock otherwise you won't be able to run the program and your CD-ROM will result in a coaster.

Beware: when krypting Delphi executables you won't be able to enable K-Exec Level 3 while the High Pack Ratio must always be active.

ID Generator for Shareware Programmer

Krypton the Krypter creates a registry value under:
HKEY_LOCAL_MACHINE / SOFTWARE / KRYPTON

the value will contain the path to the file, e.g.:
C:\Program Files\Krypton\Krypton.exe

but with the - symbol instead of \ , it will then be:
C:-Program Files-Krypton-Krypton.exe

and creates for each value the K-Key key as REG_BINARY containing 8 bytes, e.g.: 13 dc 6d 76 16 e4 33 aa

which is a value which creates a dependency between the executable and the machine. It changes if the executable is moved, this way the programmer will be able to open the registry key by simply knowing the path of the file (GetCommandLineA) and replacing each \ with a -. The K-Key must then be read to get the value to send to the executable and generate a serial number using an algorithm created by the programmer, if the user will move the file or copy it to another machine the K-Key will change therefore the key won't be valid any longer.

```
; -----  
Programmer code for manual K-Execution :  
; -----
```

```
db 0ebh,0eh  
db 'KDES'  
db 00,00,00,00,00  
db 00,00,00,00,00
```

```
db 0ebh,0eh  
db 'KDEE'  
db 00,00,00,00,00  
db 00,00,00,00,00
```

The KDES code indicates the beginning of the K-Execution, it means that this part once executed will be deleted.

The KDEE code must be placed at the end of the routine which shall be included into the K-Execution.

```
; -----
```

```
db 0ebh,0eh  
db 'KEES'  
db 00,00,00,00,00  
db 00,00,00,00,00
```

```
db 0ebh,0eh  
db 'KEEE'  
db 00,00,00,00,00  
db 00,00,00,00,00
```

The KEES code indicates the beginning of the K-Execution, it means that this part of the code once executed will NOT be deleted (it can be used more than once then).

The KEEE code must be placed at the end of the routine which shall be included into the K-Execution.

This function can be used only by the programmer and must be inserted into the code before compiling of the program (the program will work anyway even without krypting it), it's up to the programmer to choose which parts to krypt and eventually make them self-destroy if they're not needed anymore.

KCD-Lock

What is KCD-Lock

KCD-Lock is one of the most important new features implemented in Krypton the Krypter, it allows you to protect your home made CD-ROMs against copy protection.

Rather than what happens with many other famous and commercial CD protections, like SafeDisc or Securom, CDs protected with KCD-Lock cannot be copied performing a RAW data reading with programs such as CloneCD or CD-Mate.

Once the CD is protected the program will require the medium to be on any of the CD drives of the system (it can be read by any kind of CD drives, no special support is required), please remember that each copy is unique so a protected program will work only with its own protected CD inserted.

As described within our license agreement CD-ROMs protected with KCD-Lock cannot be distributed for commercial purposes.

How does it work

Note: KCD-Lock has been tested with Nero - Burning ROM versions 5.5.7.8 and later, if you had any problem with prior versions or other programs please refer to the ones mentioned.

IMPORTANT: during all the burning processes mentioned hereafter you will always have to start a new session ("Start Multisession Disk") and not continue a multisession disk ("Continue Multisession Disk").

The volume label must be the same in all burning processes and must be used during all operations.

To make a KCD-Lock protected CD please follow these steps exactly as described below, if something shouldn't work please review all the steps and look for something you missed or did in a wrong way. If you still can't succeed please refer to the FAQ section in the next chapter.

How to create a KCD-Lock CD:

1. Once encryption of the target executable is completed two files will be created in the same directory where the original file resides:
Kry00.dat
Kry01.dat

Remember to try crypting the executable without KCD-Lock enabled and check if it runs properly before start using KCD-Lock.

2. Burn the file Kry00.dat as data track to an empty CD, you can use the maximum writing speed allowed by your CD-R drive. Remember: do not finalize the CD and define a volume label for it.
3. Burn the file Kry01.dat as data track to the same CD, you can use the maximum writing speed allowed by your CD-R drive. Beware: start the multisession CD as if it was empty, do not continue importing the previous section. Use exactly the same label used when burning the first session.
4. Make a hole with a thin pin on the surface of the bottom part of the CD (where the CD is written), it must be done within the first burnt track. Distance between the edge of the center CD-hole and the point where you have to pierce has to be 19mm, as shown in the picture below:



Figure 3-1. Correct distance of the hole

Press firmly as to make the hole almost viewable from the upper side of the CD, beware not to bore the surface from side to side or the CD will result unreadable.

Try to get a result as closer as the following:

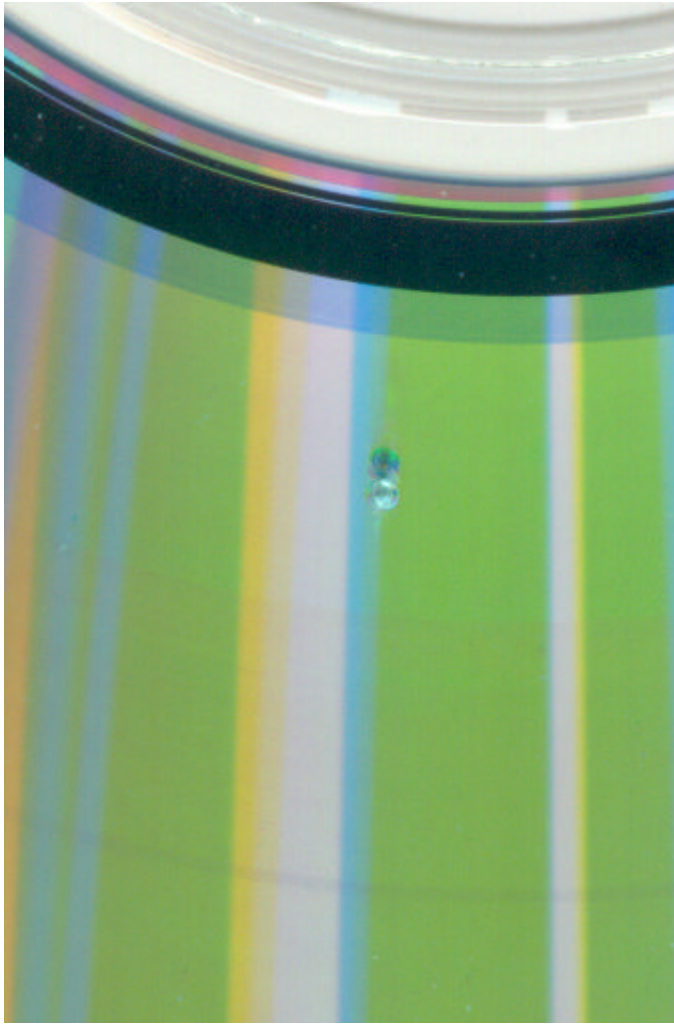


Figure 3-2. Detail of KCD-Lock hole

5. Once the hole is done put back the CD-ROM into the CD drive and press OK. When finished you will find another new file in the same directory of the crypted executable named Kry02.dat and the crypted executable itself.
6. Burn the file Kry02.dat as data track to the same CD, you can use the maximum speed allowed by your CD-R drive. Once again remember to start a multisession CD as if it was empty and use always the same volume label as before. Do not finalize the CD yet.
7. The protection is completed, you can now burn your contents on a new session including the crypted executable (always start a new multisession CD). This time you have to finalize the CD to avoid any further writing, do not forget to always define the same volume label as the beginning.

8. Delete all the data tracks and files you don't need any longer from your hard disk. You now have a KCD-Lock protected CD-ROM.

FAQ

Q: I get a "KCD-Lock can not found the CD-ROM with the 'hole'" error message

A: Two main reasons may cause this kind of error: you didn't make enough pressure to make the hole "viewable" by the CD recorder or the distance between the center of the CD is not correct. Try again making the hole deeper or making a new one adjusting the distance. If the error message says to try again but the program quit after some tries you can still use the same CD, just repeat the steps before (of course you won't have to burn again the kry00.dat and kry01.dat tracks to the CD) until you reach the CD krypting phase and try again.

Q: I get a "A FATAL ERROR stop the process. Cause: Wrong Hole Position"

A: Krypton has been able to see the hole on the CD but unfortunately it has been made in a wrong position. In this case the CD-ROM cannot be used anymore and must be replaced with a new one. Of course you can still use the CD as a normal empty media but it can't be used with KCD-Lock anymore.

Q: When I put back the CD-ROM into the CD-R drive after making the hole the program hangs

A: The most likely cause of this behaviour is due to the fact that your CD-R drive doesn't support RAW DAO mode. A RAW DAO mode CD-R capable is needed to create protected CD-ROMs with KCD-Lock. Once created instead the protected CD-ROMs can be used with any CD-ROM reader or writer drive.

Final notes

Bug reports

If you should experience any bugs using Krypton the Krypter or incompatibilities with one or more executables you can send your issues to: krypton@lockless.com or get in touch with the author at: yado@lockless.com.

Disclaimer

This software is provided "AS IS" and without warranties. Lockless cannot be held responsible for any damages or loss of data which may occur from its use. You can use it at your solely own risk. Please refer to the EULA included in this document for further informations about program's usage license and terms of use.

Thanks

Krypton staff:

Coder:	Yado
Scrambler Coder:	iNX
Main Support:	Lord Anshar
Beta testers:	Lord Anshar , AndreaGeddon , LittleLuk , -[alx]

Special Thanks go to:

GioCrack:	Thanks a lot for making the official Yado's Krypton Logo & icon :)
Kill3xx:	Thanks a lot for helping me to understand and realize my crazy ideas =)

My personal greetz to:

SirioKD , Boba Fett , PPinker , BuG, Capatosta ;) , Manonera , Scratch , Kriosman , ALT255 , LittleLuk , NikDH , Quequero , PhObos , EVC-IF and all Lockless Members !

This program is dedicated to my wife Elisa.

If i forgot someone write me and I'll add you.