Karate

TODO

Was alles mit der Paseudografik möglich war, zeigt eindrucksvoll das Programm KARATE von M.Geißler und W. Franze.

Hacking Karate

Wie schon der Turbo Loader von Sven Huth ist auch Karate kein Programm, was leicht zu hacken ist. Diverse Verschlüsselungen machen es dem Angreifer schwer[1)].

Karate besteht aus zwei Teilen: Einem Loader (in normalem KC-Format gespeichert) und dem Hauptprogramm, mit eigenem Turbo gespeichert.

1. Der Loader ist ist mit einer Passphrase XOR-verknüpft
2. Der Speicher wird komplett gelöscht, so dass Debugger etc. keine Chance haben
3. EOR wird verändert; Tastur und alle Interruptquellen werden blockiert
4. Eine OS-Erweiterung wird installiert, die nach Reser ein Info-Bild bringt und den Speicher löscht
5. Bei Ladefehlern wird der Speicher verschoben und gelöscht
6. Das Hauptprogramm beginnt auf Adresse 0000 !!!!
7. Das Programm belegt den kompletten Speicher 0000-BFFF
8. Die Turbo-Aufzeichnung erfolgt byteweise, auch hier sind die Bytes einzeln mit ihrer Position sowie einem Code XOR-verschlüsselt
9. Die Startadresse ergibt sich aus dekodierten geladenen Bytes und einem Offset, ers gibt keine OS-Rahmen, die Karte starten.

[1)]

aber nicht unmöglich. Ich habe es mit viel Mühe geschafft!