

Shareware ist in Minutenschnelle geknackt

Unser Informant erkennt Schwachstellen am Kopierschutz anhand von Jump-Befehlen im Disassembler.

Interview führte Daniel Schröder

Viele Shareware-Programme sind echt praktisch und damit ihr Geld wert. Doch teilweise ist die Software so stark eingeschränkt, dass ausreichendes Testen nicht möglich ist. „Gerade die Funktionen, wegen derer man das Programm überhaupt heruntergeladen hat, stehen in vielen Demoversionen nicht zur Verfügung. Manchmal ist die Zeitperiode schlecht – wer Software installiert und in den Urlaub fährt, hat eventuell Pech, wenn er zurückkommt. Auch wenn es ein Entgegenkommen des Programmierers ist, seine Software überhaupt zum kostenlosen Testen anzubieten, kauft man manchmal dennoch die Katze im Sack. Nur mit einem Patch kann man die Software testen, ohne unnötig Geld auszugeben.“ sagt unser Informant.

„Die meisten Shareware-Programmierer wissen nicht, wie sie ihre Programme vor Crackern wie mir schützen sollen. Deswegen können die meisten Programme innerhalb weniger Minuten komplett geknackt werden. Im Gegensatz zu professionellen Anwendungen und Spielen gibt es fast nie eine Verschlüsselung der ausführbaren Dateien, wie es etwa bei SafeDisc der Fall ist. Das macht es möglich, Patches zu kompilieren, da die Originaldatei und die geknackte Version gleich groß sind.“

Unser Informant zeigt uns hier am Beispiel von DatSave, wie leicht es wirklich geht. DatSave ist ein Verschlüsselungsprogramm, die Registrierung kostet lediglich 20 Mark – wer das Tool also wirklich einsetzt, sollte es auch bezahlen. Die Testversion zieht er unter www.uwe-schmidt.de.

1 Original disassemblieren



Der Cracker zieht eine Kopie der DatSave.exe, damit die Datei später problemlos vom Hex-Editor überschrieben werden kann. Danach öffnet er mit W32Dasm die Kopie und überprüft, ob als Schriftart Courier New in Größe 8 eingestellt ist, wenn nur unleserliche Zeichen zu sehen sind.

2 Programm analysieren



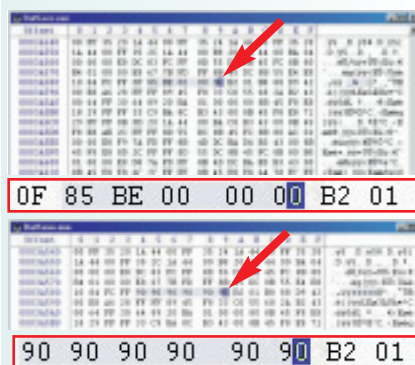
DatSave bringt beim Start eine Meldung, dass es noch 30 Tage oder maximal 100 Ausführungen läuft. Außerdem gibt es im Menü den Punkt Registrierung. Das bedeutet, dass DatSave durch Eingabe von Name und der dazu passenden Seriennummer zur Vollversion ohne Zeitbeschränkung und ohne nervige Fenster freigeschaltet werden kann.

4 Aufruf suchen



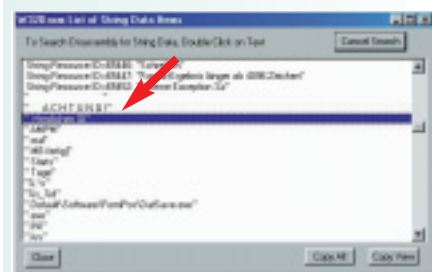
W32Dasm springt zu der Stelle, an der die Glückwunsch-Meldung ausgegeben wird. Aufgerufen wird die Meldung von Adresse 0043B228, das erkennt der Cracker an der darüberliegenden Zeile. Ein Doppelklick auf die rechte Maustaste springt zum Aufruf.

6 Hex-Wert ändern



Die DatSave.exe öffnet der Informant jetzt mit dem Hex-Editor und geht zur angegebenen Offset-Adresse 3A584. Die gesamte Zeile des Sprunges, also 0F 85 BE 00 00 00, wird jetzt komplett entfernt, also mit 90 90 90 90 90 überschrieben und die Datei gespeichert.

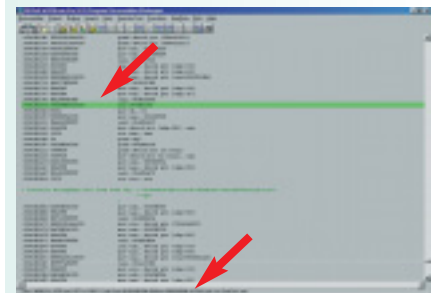
3 Registrierung suchen



ACHTUNG! Herzlichen Glückwunsch! AMPM

Unser Informant sucht bei W32Dasm im Menü Refs/String Data References nach der Meldung, die DatSave ausgibt, wenn die Registrierung erfolgreich war. Üblich sind Meldungen wie „Vielen Dank“ oder „Herzlichen Glückwunsch“, wie es bei DatSave der Fall ist. Mit einem Doppelklick gelangt er zur entsprechenden Stelle im Code.

5 Überprüfung suchen



4 @Offset 0003A584h in File:Kopie von D:

Der Cracker geht jetzt zeilenweise so lange weiter nach oben, bis er eine Überprüfung gefunden hat (siehe Assembler-Referenz Seite 70), in diesem Fall JNE. Bei einem Doppelklick auf diese Zeile verrät W32Dasm unten rechts die Offset-Adresse dieses Sprungs.

7 Programm registrieren



Nun wird DatSave jede Seriennummer akzeptieren, die aus Zahlen besteht. In jedem Fall ist das Programm dann vollständig freigeschaltet und tut seine Dienste ohne weitere nervige Shareware-Fenster. Doch wer es länger nutzt, muss es kaufen!