

Diese Tools zerlegen Originale in Programm-Codes



Cracker knacken mit Disassembler und Hex-Editor fast jeden unverschlüsselten Kopierschutz.

Interview führte Daniel Schröder

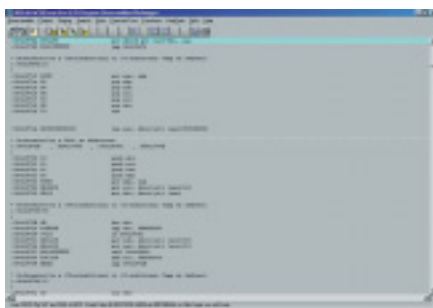
Neben Programmierkenntnissen müssen professionelle Cracker spezielle Programme einsetzen, um Kopierschutzmechanismen zu knacken. Benötigt wird in der Regel ein Disassembler, der die ausführbaren Dateien

der zu knackenden Software in die Assembler-Sprache übersetzt. Außerdem benutzt unser Informant Hex-Editoren, um die Änderungen am Code der Software speichern zu können. Das letzte nötige Tool ist die so

genannte Patch-Engine. Sie kompiliert den eigentlichen Crack der Datei, der im Internet verbreitet werden kann. „Entgegen dem, was ihr Name verspricht, entfernt sie aber den Kopierschutz nicht automatisch.“

1

Disassembler



W32Dasm 8.93 liest die Programmstruktur aus



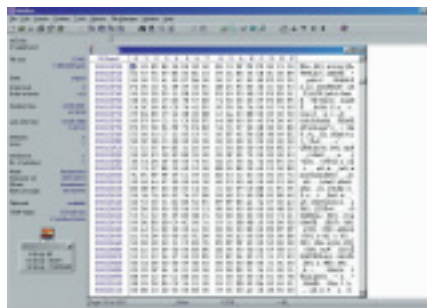
☹ konnte nicht ermittelt werden
☹ konnte nicht ermittelt werden
☹ konnte nicht ermittelt werden

Preis
unbekannt

Ein Disassembler wie W32Dasm von UR-Soft übersetzt den Maschinencode der ausführbaren Datei in die Assembler-Sprache. Aus diesem Code kann man den Ablauf des gesamten Programms nachvollziehen. Außerdem zeigt W32Dasm sämtliche im Programm erscheinenden Texte an. Fehlermeldungen, die fehlende CDs oder abgelaufene Testzeiträume melden, finden Profis so mit einem Mausklick im String-References-Fenster.

2

Hex-Editor



WinHex 9.92 öffnet und speichert jeden Dateityp

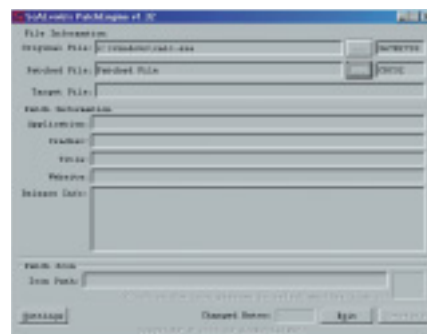


☹ Stefan Fleischmann
☎ (02 21) 3 10 88 20
🌐 www.winhex.com

Mit dem Disassembler kann die geladene Datei weder geändert noch gespeichert werden. Deswegen ist ein Hex-Editor wie WinHex nötig. Speicheradressen, die der Disassembler ausgibt, kann man im Hex-Editor schnell finden. Der große Vorteil von WinHex gegenüber den meisten anderen Editoren ist die unglaublich hohe Geschwindigkeit. Ohne Zeitverlust stehen dem Anwender sämtliche Hex-Codes der geöffneten Datei zur Verfügung.

3

Patch-Engine



ScAEVoLa's PatchEngine 1.32 erstellt Profi-Cracks

Fast jede Cracker-Crew hat ihre eigene Patch-Engine, doch einige stehen auch zum freien Download bereit. ScAEVoLa's PatchEngine ist leicht zu konfigurieren und kann kostenlos unter www.ebolavirusXXXX.de in der Sektion Tools heruntergeladen werden. Der Cracker gibt bei so einem Tool nur die unveränderte Originaldatei sowie die gecrackte Version an. Die Patch-Engine kompiliert dann den eigentlichen Crack, also eine ausführbare Datei, die verbreitet werden kann. Dieser Patch ändert die Originalversion der Software nach den Vorgaben des Crackers ab.

Mit diesen Assembler-Codes knackt unser Informant alles

Befehl	Bedeutung	Übersetzung	Hex-Wert	Ersetzen durch
jmp	jump	immer springen	EB	nop
nop	no operation	nichts ausführen, Achtung: den ganzen Befehl ersetzen	90	
je	jump if equal	Springe, wenn gleich	74 oder 0F84	jne, jmp, nop
jne	jump if not equal	Springe, wenn ungleich	75 oder 0F85	je, jmp, nop
ja	jump if above	Springe, wenn höher	77 oder 0F87	jna, jmp, nop
jna	jump if not above	Springe, wenn nicht höher	0F86	ja, jmp, nop
jae	j. if above or equal	S., wenn höher o. gleich	0F83	jnae, jmp, nop
jnae	j. if not above or e.	S., wenn nicht höher o. gl.	0F82	jae, jmp, nop
jb	jump if below	Springe, wenn niedriger	0F82	jnb, jmp, nop
jnb	jump if not below	Springe, wenn n. niedriger	0F83	jb, jmp, nop
jbe	j. if below or equal	Springe, wenn niedr. o. gl.	0F86	jnbe, jmp, nop
jnbe	j. if not below or e.	S., wenn nicht niedr. o. gl.	0F87	jbe, jmp, nop
jg	jump if greater	Springe, wenn größer	0F8F	jng, jmp, nop
jng	jump if not greater	Springe, wenn nicht größer	0F8E	jg, jmp, nop
jge	j. if greater or e.	S., wenn größer o. gl.	0F8D	jnge, jmp, nop
jnge	j. if not greater or e.	S., wenn nicht größer o. gl.	0F8C	jge, jmp, nop
jl	jump if less	Springe, wenn kleiner	0F8C	jnl, jmp, nop
jnl	jump if not less	Springe, wenn nicht kleiner	0F8D	jl, jmp, nop
jle	jump if less or e.	Springe, wenn kleiner o. gl.	0F8E	jnle, jmp, nop
jnle	j. if not less or e.	S., wenn nicht kleiner o. gl.	0F8F	jle, jmp, nop

Hauptsächlich drehen Cracker Entscheidungen eines Programms einfach um. Würde ein Programm etwa abbrechen, wenn keine CD im Laufwerk ist, ändert ein Cracker diese Abfrage so, dass es abbrechen würde, wenn die CD eingelegt ist, oder so, dass das Programm immer startet. In der Regel reicht es aus, wenn nur der Hex-Wert des Befehls ausgetauscht wird. Lediglich um eine Funktion komplett zu deaktivieren (Befehl nop), ersetzt unser Informant die gesamte vom Disassembler gezeigte Zeile.