درس ۱۰

چگونه کراک کنیم، کراکینگ بعنوان یک هنر

BARCODE ها یا کدهای میله‌ای

قبل از هرچیز، برا همیت کراکینگ در زندگی روزمره‌تان تأکید میکنم. کراکینگ نه فقط در مورد نرم افزار، بلکه در مورد اطلاعاتی راجع به الگوهای زندگی می‌باشد. کراک کردن، یعنی امتناع ورزیدن از کنترل شدن، کراک کردن یعنی آزاد بودن .

باید یاد بگیرید تا وقایع مربوط به کراکینگ در اطراف خود را تشخیص دهید و باور کنید که با پیشرفت این جامعه مخوف، هر روز، کدها، محافظتها و مکانیسمهای جدید مخفی کردن عرضه میشوند.

بارکدها را بعنوان نمونه‌های جالب در نظر میگیریم، بارکدها خطوط کوچکی هستند که روی هر کتاب، بطری یا اجناسی که میخرید، مشاهده میکنید، آیا با کارکرد آنها آشنا هستید؟ اگر نمیدانید، اشکالی ندارد اما اگر هرگز حتی هوس یادگرفتن هم نکرده‌اید دیگر جای هیچ عذر و بهانه‌ای نیست. کراکرها ذاتاً کنجکاوند. واریشن نسل تقریباً منقرض محققانی که هیچ وجه تشابهی با بردگان تلویزیون و آدمهای مشهور ندارند در اطراف ما وجود دارند. کراکرها باید قدرتی فراتر از قدرت معمول و اطلاعاتی فراتر از اطلاعات دیگران داشته باشند.

تاریخچه BARCODE

حال میخواهیم تاریخچه مختصری از آن را عنوان کنیم. کد جامع محصول (UPC)، جهت استفاده تجاری در صنعت خوار و بار در آمریکا تعیین شده است. روش دقیق و سریع و مطمئن وارد شدن به اطلاعات موجوددر کامپیوتر و احتمال اخراج کردن تعدادی از کارگران و کسب سود بیشتر از جمله مزایای این روش است . این موفقیت منجر به توسعه سیستم شماره‌گذاری اقدام اروپایی (EAN) شد، سمبلی نظیر سیستم UPC که در اروپا و سایر کشورهای دنیا مورد استفاده می‌باشد. از آنجایی که ما خوشبختانه در این ایالات زندگی نمی‌کنیم، کراک کردن به این روش را به شما می‌آموزم. بهرحال به خاطر بسپارید که بارکدهای دارای سمبلهای مختلفی هستند که هریک الگوی مخصوص خود را دارد. کد UPC/EAN که روی محصولات خرده فروشی بکار میروند، یک کد کاملاً عددی است، بنابراین این کد، ۲ تا کد همراه شده از ۵ تا کد است. کد ۳۹ شامل حروف بزرگ، اعداد و چندتا سمبل است. کد ۱۲۸، هر کد کاراکتر قابل چاپ و غیرقابل چاپ ASCII را دربرمیگیرد. جدیدترین کد،کد شماره 2-D می‌باشد. این کدها، کدهای مستطیلی مخصوصی هستند که بارکدهای استاک شده یا کدهای ماتریسی نامیده میشوند . این کدها نسبت به بارکدهای استاندارد، اطلاعات بیشتری ذخیره میکنند. این کدها به خواننده‌های خاصی نیاز دارند که در مقایسه با اسکنرهای استاندارد، با ارزشتر باشند. محدودیت واقعی بارکدهای استاندارد به تعداد فاکتورها بستگی دارد در حالیکه ۲۰ الی ۲۵ کاراکتر، ماکزیمم مقدار است، در مواردیکه به اطلاعات و داده‌های بیشتری نیاز داشته باشیم از کدهای ماتریسی استفاده می‌شود، بعنوان مثال بسته‌ای را از یونایتدپارسل سرویس دریافت میکنید که برچسب روی آن به شکل مربع کوچکی با مدلی از نقاط و خالهای کوچکی در وسط به نظر میرسد. این برچسب Moxicode است و توسط سیستم UPS جهت جدا کردن اتوماتیک نمونه از سایر نمونه‌ها بکار میرود.

شماره شناسایی تولید کننـده روی بـارکد (Barcode) بـرای تشـخیص محصـولات منحصـر بفـرد میباشند. این شماره گذاریها توسط Chiform Code Council در دیتو، ایالت اوهیو، برای آمریکـا و کانادا و توسط مقامات EAN(انجمن بین المللی شماره گذاری اقـلام) در بروکسـل بـرای اروپـا و سایر کشورهای دنیا ترتیب داده شده‌اند. شماره شناسایی تولید کننده بـرای برخـی از ارقـام کـد در نظر گرفته شده‌اند، سایر ارقام دیگر، طبق خواسته تولید کننده مشخص میشوند. وی، نمـایندگیـهای خرده فروشیها را همراه با لیستی از محصولاتش و کدهای تعیین شده آنها تهیه می‌کند، بـه گونـه‌ای که بتوان آن کدها را وارد صندوق فروشگاه کرد. بسیاری از این کدها روی محصولات زده نشده‌اند و خود سوپرمارکتها با استفاده از طرح کدگذاری داخلی، آن را روی محصـول می‌زننـد. ایـن کدهـا غیرقابل استاندار هستند، خوب، برویم سرواغ کراک کردن.

بارکدها (Barcodes) تنها چیزهایی هستند که لازم است تا صندوقدار آن را روی محصول ببیند تـا بتواند قیمت کالا را حساب کرده و اتوماتیک وار، کالای فروخته شده را وارد فهرست کنـد. تصـور کنید (البته این کار کاملاً غیرقانونی است) کسی بر چسـب یـک جنـس خـانگی را مسـتقیماً بـالای برچسب سوپرمارکت، مرکز خرید یا فروشگاه خرده فروشی بچسباند. مثلاً روی یک بطر pomeral (کار خوبی است اما متأسفانه مشروب فرانسوی خیلی گران است).

مفهوم برچسب جدید برای صندوقدار می‌تواند این باشد: «مشروب ارزان از bardeaux فرانسـه بـه قیمت چنین و چنان، بد نیست، نگران نباشید. فکر می‌کند که کسی به این نتیجه خواهد رسید که یا این برچسب، اشتباهی است یا بطری یـا اینکـه شـما اشـتباه می‌کنیـد؟ مـن مدتـهای مدیـدی روی برچسبها، کدگذاری می‌کردم و با یک مشکل مواجه بودم و آن این بود که پرینتر من خالی از جوهر شده و اسکنر سوپرمارکت قادر به خواندن کد نبود ... برای چه؟ همیشه بدون اعتنا، ژاکتـهای مـدل بالا،پولیورهای بافته شده از پشم شتلند، کفشهای زیبا و گرانقیمت می‌پوشید...

(تمام اجناسی که با این روش، روی برچسبشان کدگذاری گردیده‌اند) . در جامعه فعلی، قیافه و ظاهر شخص بیشتر از ذات و معلومات او مورد توجه قرار می‌گیرد. ... بیایید به نفع خودمان کار کنیم! ممکن است هیچ کس باور نکند که واقعاً کار این برنامه را بلد هستید... کد روی برچسب، بسیار پیچیده و سخت بوده و بدون استثناء، عمومی هستند. در وب اطلاعات زیادی در این مورد وجود دارد، اما بیشتر این اطلاعات بی فایده هستند، در صورتیکه بدانید که چگونه اغلب اوقات آن را سرچ کنید جملاتی نظیر این جمله را خواهید یافت:

«رقم تست محاسبه شده، شماره ۱۲ و در واقع آخرین رقم. در کد UPC است.

این رقم بر اساس الگوریتم خاصی محاسبه شده و لازم است تضمین کند که عدد بطور صحیح خوانده شده و وارد می‌شود.

اما ORC + خوب، آنچه را که لازم است برای کراک کردن بدانید، برای شما توضیح خواهد داد:

BARCODهای ۱۳تایی.

هر برچسب بارکدی دارای ۱۳ مقدار است. از 0# تا 12# (این کد، EAN است، کد UPC آمریکایی دارای ۱۲ رقم است، از 0# تا 11#).

0# و 1# ، خاستگاه محصول را نمایش میدهند.

2# و 11#، کد کالای را نشان میدهند.

12# (و آخرین شماره یعنی 13#) مقدار Cheksum (جمع ارقام) را نشان میدهند که در نهایت ارزش سایر شماره‌های دیگر را تأیید می‌کند.

این ارقام چگونه محاسبه میشوند؟ 12# در چهار مرحله محاسبه می‌شود:

مقدار A: اعداد فرد را جمع کنید (10#+8#+6#+4#+2#+0#)

مقدار B: اعداد زوج را جمع کنید و ضربدر ۳ کنید (3*(11#+9#+5#+3#+1#)

مقدار C: مقدار A و B را جمع کنید.

مقدار D:، مقدار C را در نظر بگیرید. (آن را تقسیم بر ۱۰ کنید و مقدار باقیمانده را نگه دارید، طرح رایج تست نمودن که در بخش نرم افزار این درس خواهید دید).

چنانچه نتیجه حاصل، صفر نبود، این عدد را از ۱۰ کم کنید.

حال به برچسب بارکدها دقت کنید، یک سری کتابها یا سایر اقلام دارای برچسب کدگذاری شده تهیه کنید و به آنها نگاه کنید. ...

بارکدها. در هر دو طرف سمبل, دارای «نواحی آرامی» هستند. «نواحی آرام» نواحی سفیدی هستندکه چیزی روی آنها پر نیست یا علامتگذاری نشده و پهنایشان ۱۰ مرتبه باریکتر از فضای موجود در بارکد می‌باشد. ایجاد فضای کافی در هر طرف سمبل برای نواحی آرام اشتباه است، چون باعث می‌شود که بارکد خوانده نشود.

روی هر بارکد، دو «مرز» در طرف چپ و راست، و خط بزرگتری در میان آن وجود دارد. این سه خط بلندتر از سایر خطوط بوده و برای تنظیم کردن اسکنر بکار میرود تا بتوان برای بارکد، از هر طرف آن را مورد استفاده قرار داد.

0# در سمت چپ اولین مرز (سمت چپ) نوشته می‌شود و مفهوم خاصی دارد و دوازده عدد دیگر داخل کد، نوشته شده و توسط میله وسطی به دو گروه تقسیم می‌شود:

عدد از طریق هفت میله کدگذاری می‌شود: balck=1 و white=0

این میله‌ها از دو جفت میله چشمی تشکیل شده‌اند.

حال به قسمت «جادویی» میرسیم. به منظور گول زدن افراد ساده، بارکد از سه مجموعه کاراکتر مختلف برای نمایش دادن مقادیر ۰ تا ۹ استفاده می‌کند. این باعث می‌شود که نفهمید چکار باید

بکنید، در چنین جامعه‌ای لزومی ندارد برده‌ها نـگران عملکـرد واقعـی چنیـن چیزهـایی باشـند. در بخش ذیل، کدهای گرافیکی از سه مجموعه گرافیک نشان داده شده‌اند.

```
     CODE A             CODE B (XOR C)     CODE C (NOT A)
0:   0001101   (13)     0100111   (39)     1110010   (114)
1:   0011001   (25)     0110011   (51)     1100110   (102)

2:   0010011   (19)     0011011   (27)     1101100   (108)
3:   0111101   (61)     0100001   (33)     1000010   (066)
4:   0100011   (35)     0011101   (29)     1011100   (092)
5:   0110001   (49)     0111001   (57)     1001110   (078)
6:   0101111   (47)     0000101   (05)     1010000   (080)
7:   0111011   (59)     0010001   (17)     1000100   (068)
8:   0110111   (55)     0001001   (09)     1001000   (072)
9:   0001011   (11)     0010111   (23)     1110100   (116)

Borders:       101
Centre:        01010
```

ـ مجموعه گرافیکی C، مجموعه گرافیکی "NOT A" می‌باشد.

– مجموعه گرافیکی B، مجموعه گرافیکی "XOR C" می‌باشد.

- هر مقدار دارای دو جفت میله با عرض متفاوت می‌باشد.

- حال به برخی از برچسبهای خود توجه کنید. تفـاوتی بیـن اعـداد سـمت راسـت و چـپ می‌بینید؟

اولین نیمه این بارکد با استفاده از مجموعه‌های A و B کدگذاری شده‌اند. نیمـه دوم بـا اسـتفاده از مجموعه C کدگذاری شده است. در صورتیکه مجموعه کـافی وجـود نداشـته باشـد، از A و B در اولین «نیمه» بصورت ترکیبی استفاده می‌شود که تغییر کرده و به مقدار 0# بستگی دارد.

در این قسمت، ۱۰ الگوی متفاوت وجود دارد:

	#1	#2	#3	#4	#5	#6
0	A	A	A	A	A	A
1	A	A	B	A	B	B
2	A	A	B	B	A	B
3	A	A	B	B	B	A
4	A	B	A	A	B	B
5	A	B	B	A	A	B
6	A	B	B	B	A	A
7	A	B	A	B	A	B
8	A	B	A	B	B	A

9 A B B A B A

خریدار نادان هرگز به این موضوع توجه نمی‌کند که چرا مقادیر یکجـور، بارهـای متفـاوتی دارنـد.

حال به ذکر مثالی در مورد کدبار برای مارتینی درای می‌پرازیم:

BARCODE: 8 0 00570 00425 7

داریم (مشروب): 8 0 0 = booze

پـس عـدد عـدد 000570 بصـورت ABABBA و 004257 بصـــورت C جمــع اعــداد «فــرد»

8+0+5+0+0+2=15 (عدد فرد)

سپس 16=5+4+0+7+0+0 (حاصلجمع عدد زوج)و 48=3*16

سپس 63=48+15

63= = = 3

10-3=7=Checksum

(pattern) الگو =8=ABABBA CCCCCC

دانشجویان خوب،هدف از این همه کد چیست ؟ کسی که نمیداند . سوار بر قایق است ،کســی کـه میداند و یاد میگـرد می‌تواند از معلومایتش به منظور تلاش در مبارزه با هــر مشـکلی کـه بـر نظـام نفرت انگ‌یز ما حاکم است مبارزه کند، جامعه ای کــه مـا در آن بـه زور زنـدگی‌ی می‌کنیـم برنامـه کوتاهی است جهت پرینت کردن هر کد باری (کد میله‌ای) که دوست دارید (یا هــرچـه کـه مرکـز خرید شما استفاده می‌کند) با هر اندازه و هر نوع برچسبی کــه میخواهیـد (بیشـتر بـا هـدف مـورد نظرتان جور درمی‌آید). بنویسید . این برنامه سریعاً با برنامه visual basic و Delphy انجام می‌شود .. ما روی وب راه دیگ‌ری که بتوانید با آن در سیستم dos برنامه کوتاه C را بنویسید مشــکلی کـه من قبلاً با آن مواجه بودم. پس مجبورید برچسب بزنید. .. عبارت کوتاه اخطار...هر بــار فقـط یـک آیتم را کراک نموده و سعی کنید که به محصولات یکجور، برچسب یکجور بزنید. یعنی کد صحیح برای آن آیتم (قلم جنس) اما با برچسب انتخابی خودتان. اگـر این برنامــه، نتیجـه موفقیـت آمـیزی داشته باشد، و یا حتی اگـر نداشته باشد، هیچ کس نمیتواند که به شما ضرر بزنـد. بهرجـهت، هیـچ

اتفاقی نخواهد افتاد، هرگز: بارکد (کد میله‌ای) خواننده وسایل، تولرانس زیادی دارد پس اسکنرها باید بتوانند بارها کدهایی را تشخیص دهند که روی رسانه‌های مختلفی پرینت شده‌اند . شما باید برچسبهایی را انتخاب کنید که شبیه برچسبهای استفاده شده باشند، صرفاً به خاطر اینکه افراد به آنها شک نکنند، پس به خاطر اینکه تمام اسکنرها خودشان مراقب باشند. برچسب شما می‌تواند بصورت نوارهای صورتی یا سبز رنگ با شماره‌های دست نویس نارنجی رنگ انتخاب شود. بخاطر داشته باشید ما هنوز هم علمی در یک موقعیت فرضی قرار داریم، پس عمل کردن با چنین روش سنجیده‌ای،کلاً غیرقانونی است.

Cracking power (قدرت کراکینگ) این عبارت برای بارکدها ،فاکتورهای ارتباط از راه دور (مخابرات)، برای صورتحساب شبکه اصلی اطلاع رسانی، برای کارتهای شرکت amex و چکهای بانکی و برای شماره ثبتها واقعاً به جا و مناسب است. میدانید که MICR چیست؟ تشخیص کاراکتر جوهر، مغناطیسی ... چاپ کدهای کوچک در چکهای جدید، سمت چپ... یک مجموعه کراکینگ روی آن کار شده است). ... شما آن را نامگذاری میکنید. آنها آن را توسعه میدهند، ما آن را کراک می‌کنیم.

اول به سراغ بارکدها میرویم. ساده، راحت و مفید! همواره در رفاه، زندگی خواهید کرد، با شهرت و ثروتی که وجه تمایز کراکرهای واقعی از دیگران است، از این گذشته، شما باید مجموعه pomerals را در برنامه cave a-vin من ببینید.

دستیابی فوری

روتنیهای دستیابی فوری به C، طرح حفاظتی تجاری هستند که به منظور باز کردن کدهای کاملاً تجاری سری شده روی CD استفاده میشوند. ROMها که اغلب از طریق ارزیابی توزیع نشده‌اند، این هدف واقعی کراکینگ است. این نرم افزار، یک نرم افزار تجاری، کامل، کاراَ و با کیفیت نسبتاً

خوب می‌باشد که می‌توان تعداد زیادی از آن را با حداقل هزینه تهیه کرد. مسلماً این نوع محـافظت یک موضوع مناسب برای درسهای ما خواهد بود تا آنجا که من میدانم این نوع برنامه‌های محافظتی نسبتاً پیچیده، هنوز توسط شخصی کراک نشده ا ست. پس داوطلب ایــن طـرح، کـاندیدای خوبـی برای دانشگاه من خواهد بود. حال، کراک کردن آن را در سه درس C.3, C.2, C.1 به شما خواهـم آموخت.

به شما هشدار میدهم... آموزش کراکینگ این جلسه بسیار مشکل بوده و این طرح حفاظتی در واقع یک مبارزه فکری است . اما اگـر جداً به این کار ما علاقمند هستید، این جلسات و درســها، از هـر چیز دیگـر برای شما لذت بخشتر خواهد بود.

این روش کراکینگ بعنوان یک تکلیف برای دانشجویان دانشگاه کراکینگ HCV+ در نظر گـرفتــه شده است. شما میتوانید در درسهای C1 و C2، مقدمه نسبتاً کاملی در مورد کراکیــنگ بـا دسـتیابی فوری پیدا کنید. این روش، اطلاعات زیادی را به شما آموزش داده و اوقات بی حاصل شــما را پـر خواهد کرد و مستقیم به موضوع کراکینگ خواهید رسید! اما من بخش سوم این درس را همـراه بـا راه حـل کـامل آن (درس C3) در وب، صرفــاً در تــاریخ اکتــبر ۱۹۹٦ توضیــح داده‌ام. تمــامی دانشجویانی که به Higher Cracking University درخواست میدهند، طبق تاریخ شروع روی وب یعنی ۱۹۹۷ را باید سه ماه روی این تکلیف کار کنند یعنی ژوئیه. اوت و سپتامبر (سـه مـاه فرصـت کافی است). آنها باید طرح دستیابی فوری را کاملاً کراک کرده و راه حل خود را برای من تا قبل از ۱۹۹٦ / ۹ /۳۰ بفرستید (توجه کنید! میتوانید این طرح را حداقل به روش متفاوتی کراک کنید، دقت کنید و بهترین روش را انتخاب کنید. توجه کنیـد! برخـی از اطلاعـات موجـود در درس C1 و C2 یک سری اشکالاتی دارند، آنها را چک کنید.

چهار احتمال وجود دارد

۱)نامزدها (داوطلبها) برنامه کراک را پیدا نکرده یا راه حلشان به مقدار کافی مستدل یا عملی نیست. بنابراین قابلیت کراک کردن را ندارند و در دوره‌های HCV+ سال ۱۹۹۷ پذیرفته نمیشوند،شاید در سال ۱۹۹۸ شانس بهتری داشته باشند.

۲- راه حل کراکینگ پیشنهادی نامزد، به خوبی راه حل من نیست (میتوانید در ماه اکتبر خودتان در ای مورد قضاوت کنید). اما با وجود این، باز هم با همین روش عمل می‌کند...

او در دوره ۱۹۹۷ پذیرفته خواهد شد.

۳- روش کراکینگ نامزد ، کم و بیش مثل روش من است، او پذیرفته شده و شخصاً کنترل می‌شود و بدین ترتیب به تمام مطالبی که برای کراک کردن در سطوح بالاتر به آن نیاز دارد دست خواهد یافت.

٤- راه حل کراکینگ نامزد بهتر از راه حل من بوده و او پذیرفته می‌شود و هرگونه اطلاعاتی که بخواهد در اختیارش است و به ما آموزش داده و همراه با ما به تحقیق و مطالعه ادامه میدهد.

دستیابی فوری به کراکینگ

استفاده‌کننده‌ای که میخواهد برنامه نرم افزاری محافظت شده‌ای با دستیابی فوری C را باز کند باید قبل از هر چیز یک رشته اعداد Registration را وارد برنامه کند که بواسطه یک سری دستگاههای ریاضی که مخصوص محصول است شکل می‌گیرد. بر اساس این «کد محصول» از استفاده کننده خواسته می‌شود تا به محافظت کنندگان تجاری تلفن زده و به منظور بدست آوردن کد مخصوص رمزگشایی شده‌ای که به او اجازه میدهد تا نرم افزار مربوط را آشکار سازد، وجه پرداخت کند.

این موضوع روتینهای محافظتی «عدد رمز» برای نرم افزارهای باز شده، دستیابی به BBS، دستیابی به سرور (Server)، بازگشایی مخفیانه، و سایر طرحهای محافظتی مورد استفاده قرار می‌گیرند.

تاکنون کراکهای زیادی از کلمه رمز در دروس مختلف این دوره آموزشی (مخصوصاً درسهای ۳/۱ و ۳/۲ برای سیستم dos و درسهای ۸/۱ ، ۸/۲ و ۹/۱ برای ویندوز). بر مبنای سادهترین مقیاسها دیدهایم. پس چندان مهم نیست که شما چگونه این طرح محافظتی را رمزی میکنید:

در حالیکه آن را رمز دار میکنید، میتوانید به برنامه آن هم دست یابید، چنین چیزی در مورد دستیابی فوری به C وجود ندارد. با آن مواجه شوید، کمی خسته کننده است، اما مهم اینست که یاد بگیرید چگونه روتینهای محافظتی پیچیده را مغلوب سازید. (در سالهای آتی، زیاد با آنها روبرو خواهید شد). و من معتقدم که با عنوان کردن نمونه ذیل، روش صحیح کراکینگ را حس خواهید کرد.

در چنین وضعیتی، ما نه تنها باید این طرح حفاظتی را کراک کنیم بلکه باید به منظور رسیدن به اهداف مورد نظرمان، روی آن تحقیق و مطالعه کنیم: این تمرین بسیار خوبی است: برنامه Disassembling معکوس، به شما روشهایی را میآموزد که بتوانید از آن در جلسات آتی کراکینگ خود استفاده کنید.

دستیابی فوری به (C) یک طرح محافظتی رایج و کاملاً استثنایی است و روش نسبتاً سادهای برای جمع آوری برخی از نرم افزارهای سری شده است است که به این روش محافظت شدهاند. .. آن را به سرعت اجرا کنید. پس از آنکه وب این دروس را منشتر کرد (من درس c1 را در ۸ صفحه و ٤ گروه usenet در تاریخ ۲۵/٦/۱۹۹٦ خواهم فرستاد). این طرح حفاظتی هم مثل پرنده دود و نسلش منقرض شده است. طرفداران Accessor در صورتیکه بخواهند طرحهای حفاظتی را به تولید کنندگان نرم افزارهای بزرگ بفروشند چیزهایی بهتری طراحی میکنند.

اگر BTW را خوانده باشید و در برخی از کمپانیهای محافظت تجاری کـار کـرده باشـید میتوانیـد شانس ایستادن در جلو رؤسای خود را افزایش دهید. تمام پروژه‌هایی که میخواهیـد در آینـده روی آنها کار کنید را به من تحویل دهید! اینها مرا سرگرم خواهند کرد.

همانگونه که گفتم برنامه‌های بسیار بزرگی با این سیستم دستیابی فوری، محافظت میشوند. مـن حداقل ۷ یا ۸ تـا از برنامـه‌های دسـت دوم آن را بصـورت CD-ROM بسـته بنـدی شـده توسـط شرکتهای نرم افزاری Symantec, Norton, Lotus, Microsoft خریداری نموده‌ام . شما میتوانید آن را نامگذاری کنید. تمام برنامه‌ها به همیـن روش محـافظت شـده‌اند. قیمـت هرکـدام از ایـن CD-ROM ها، با قیمت یک بطر مارتینی درای یکجور است شاید هم کمتر. چنین نرم افزاری بصـورت باز شده به افراد نادان و هالو به خاطر پول کمتر فروخته شده است.

هرگز مجلات CD-ROM را در صورت باز شدن نخرید! خونسرد باشید! آنها را دو الـی سـه مـاه پس از تاریخ انتشارشان خریداری کنید! یا باقیمانده‌ها را بخرید و یا مجلات CD-ROM دست دوم را. خوب فکر کنید، هیچ وقت چیزی که بـاز شـده نخریـد، بـه خـاطر داشـته باشـید کـه روندهـا، گرایشها و مدها، اسامی مختلفی برای شلاق زدن و غل و زنجیر کردن برده‌های احمق این جامعـه نفرت انگیز هستند: «کراکرهای با هوش، خونسرد، ارزان کراک میکنند و خریدار را می‌فریبند».

روتین سه گانه محافظت کلمه رمز در برنامه دستیابی فوری به (C)، از دیدگاه یک کراکـر بسـیار جالب توجه است. این یک طرح فوق العاده پیچیده است. من به شما خواهم آموخت کـه آن را در دو مرحله کراک کنید: اول از همه شما باید کد ثبت مجاز را پیدا کنید. کدی که روی کد محصـول، تأثیر میگذارد. اگر بخواهیم مابقی کدها را کراک کنیم باید ابتدا این کد را کـراک نمـوده و کـاملاً بشناسیم. فقط برای رکوردها، من مدل ۱/۸ دستیابی فـوری عملکـرد (C) را اکـراک می‌کنیـم (CD-ROM یافت شده روی کپی قدیمی کامپیوترهای شخصی مربوط به ماه اوت ۱۹۹٤ است که توسـط

شرکتهای نرم افزاری Symantec, Lotus, Calris و کلمه پردازهای سریع بسته‌بندی شده‌اند. مطمئن باشید که من نتایج بدست آمده خود را با CD-ROM دیگری چک خواهم کرد که برنامه‌های محافظت شده‌ای بر اساس دستیابی به (C) دارد. اداره انتشار کامپیوترهای شخصی Progrom: طرح حفاظتی همیشه یکجور است). کانون توجه من در این درس، کراکینگ ساده، در اصل باید یک شماره را تایپ کنید (در این مورد، جاییکه ورودی، ۱۰ شماره میدهد از "-1212 1212-12 استفاده می‌کنیم). داخل حافظه را سرچ کنید S 30:0 1 ffffffff your string) و سپس نقاط توقف در حافظه را در تمام آدرسهای مربوط به حافظه مشخص کنید (میدانم، میدانم دوستان ... شیوه‌های مؤثرتری هم وجود دارد. اما شما روش خود را دنبال کنید. چون ما آنها را جزو روشهای خودمان محسوب میکنم. حال بیایید برای محافظت کنندگانی که این مطالب را میخوانند کمی جدی‌تر مسئله را دنبال کنیم.... بعلاوه: شیوه قدیمی بی عیب و نقص است).

پس از یافتن پنجره Registration روی صفحه، مراحل استاندارد Winice عبارت خواهند بود از :

```
:task                          ; how
 :heap IABROWSE                 ; where & what
 :hwnd IABROWSE                 ; get the Winhandle
 :bpx [winhandle] WM_GETTEXT    ; pinpoint code
 :bpx GetProcAddress            ; in case of funny routines
 :dex 0 ds:dx                   ;          let's see their name
 :gdt                           ; sniff the selectors
```

S 30:0 1ffffffff رشته ورودی شما ؛ ٤ گ‌یگا داده را بایت کنید.

Bpr: تمام دامنه حافظه برای رشته شما بیش از 80000000 و الی آخر می‌باشد.

خوب، اینها مطالب عمده این درس بودند، همه درسهای برنامه آموزشی من روی وب هستند.