

Pascal Code Untuk ngePatch WinRAR 3.41

Selasa, 20 Desember 05 - by : [Reporter](#)

WinRAR tool compression dan decompression yang memiliki banyak sekali feature dan support archive file. (<http://www.rarlab.com/>)

Mungkin anda pernah mempelajari bahasa pascal disekolah ataupun kuliah, bukankah gampang? berikut adalah cara membuat patch dengan menggunakan pascal yang pasti tidak pernah diajarkan disekolah ataupun kuliah, seperti di UNDIP ataupun POLINES, mungkin kalo di TI diajarkan yah? Tapi untuk menjadi seorang cracker tidak perlu harus kuliah atau sekolah mahal-mahal, it's just for fun...

Pertama-tama sediakan WinRar.exe (original) tentunya..
Tool-tool yang diperlukan disassembler, debugger, hex editor, compiler, dan beberapa buku referensi..
Secangkir kopi tentunya, kalo ga susu boleh juga.. apalagi sekalian sumbernya... heheheee...
terus cemilan & sebungkus rokok, bagi yang ngrokok....

Ok, disini aku hanya mau mbahas tentang source code yang aku pake buat bikin patch buat WinRAR versi 3.41, sebenarnya sih ini bisa di pake buat ngepatch program2 yg laen tinggal diganti aja data2nya..

Source ini butuh dicompile pake pascal 7 tentunya yang udah di patch..
tapi di pascal 5 juga tetep bisa dicompile kok so don't worry..

yoi, disini aku kaga' nerangin darimana dapat byte yang mau kita patch, soalnya catetanku yang winRAR versi lama ilang terus juga lagi banyak - banget tugas numpuk.. Kalo pengen tau darimana byte-byte tersebut di dapet coba aja debug sendiri tuh winrar, disarankan pake Soft-ICE..
aku udah ngomong ke ropiX supaya bisa download softICE di sini..

Sebenarnya sih untuk ngepatch bisa pake HexEditor untuk ngubah nilainya aja tapi kemudian sulit kalo mau menDistribusikan crack yang kita buat..

ok,mulailah debug atau disassembling itu winrar.exe...

Disini patch yang dibuat adalah untuk mengalihkan program winrar ini untuk membaca kode registrasi (pada file RARREG.KEY) dari kode yang sebenarnya- dengan membypassnya untuk membaca kode registrasi yang kita buat sendiri tanpa perlu menggunakan pengacakan kode yang bikin pusing....

ToDo:

Configure out the Restoring Procedure to restore patched program to original one.
caranya: kembalikan nilai bytes yang di ubah menjadi nilai aslinya.

Disini aku cuman nampilin ada apa di kode tersebut:

nilai byte asli:

```
00002C3Bh 01 add [bx+si],ax
```

-> add register ax to [bx+si]
-> ax = -> it's bad -> original regkey (mungkin...)

0000D3CBh 7F jg Short 0000D3D7
-> jump if greather - ZF=0 and SF=OF

0000D3D7h 33 C0 xor ax,ax
-> hasil Xor ax = Nol

nilai byte patch:

----> kemudian byte2 tersebut kita ganti:

00002C3Bh 00 add [bx+si],al
-> add register al to [bx+si]
-> ga di add kan ke [bx+si]

0000D3CBh EB jmp Short 0000D3D7
-> Langsung ngeJump Short

0000D3D7h B0 01 mov al,01
-> mov 01 () ke al -> our regkey (mungkin juga... heeee)

keterangan tamabahan:

General Purpose Registers

AX (EAX) Accumulator

BX (EBX) Base

(Exx) indicates 386+ 32 bit register

Pointer Registers

SI (ESI) Source Index

8088/8086 Effective Address (EA) Calculation

Description Clock Cycles

Displacement 6

Base or Index (BX,BP,SI,DI) 5

Displacement+(Base or Index) 9

Base+Index (BP+DI,BX+SI) 7

Base+Index (BP+SI,BX+DI) 8

Base+Index+Displacement (BP+DI,BX+SI) 11

Base+Index+Displacement (BP+SI+disp,BX+DI+disp) 12

- add 4 cycles for word operands at odd addresses

- add 2 cycles for segment override

- 80188/80186 timings differ from those of the 8088/8086/80286

pusing juga yah.. saatnya ngupi.. dan nyalakan rokok.... enak juga sambil ngemil...

Semoga sedikit penjelasan tadi tidak salah yah... hiXss..

Catatan:

Untuk kode-kode patch tersebut diatas dapat digunakan untuk versi winRAR yang lain aku udah mencobanya pada beberapa versi winRAR, yang perlu diperhatikan hanyalah alamat dari byte-byte tersebut biasanya semakin baru versinya alamatnya akan semakin bertambah pula..

here the code

```
{-----cut here-----}
```

```
program NgapaX_patch_dinalova;
```

```
uses crt;
```

```
const a: array[1..4] of record {<-- 4 bytes to be patched}
a: longint;
b: byte;
end =
((a:$2C3B;b:$00),(a:$D3CB;b:$EB),(a:$D3D7;b:$B0),(a:$D3D8;b:01));
{ data yang akan di patchkan }
```

```
var x,ch:char; reg:text;
I:byte; buff,buff1:string[255];
F:file; FN:file of byte;
size:longint;
{ Declaration }
```

```
begin clrscr; writeln; writeln; textcolor(lightgreen);
writeln(' BÜÜÜ ° ÜÜÜÜÜÜÜÜ ÜÜÜ ');
writeln(' BBBÜÜÜÜÜÜÜÜÜ BÜÜÜÜÜÜÜÜ ÜB ÜÜ° ');
writeln(' PÜÜÜÜÜÜ B °ÜÜ²ÜÜÜ B Ü °ÜÜ² ÜÝ ');
writeln(' ²ÜÜ²ÜÜ ÜÜÜ²²² ÜÜÜÜÜÜ²² ÜÜ²² ÜÜÜ ° ÜÜÜÜÜÜÜ ');
writeln(' ÜÜÝBÜ²²²Ü BÜÜÜÜÜÜÜÜ Ü²ÜÜÜÜÜ²² ÜÜ ÜÜÜÜÜÜÜÜÜÜ²² B°ÜÜ²ÜBÜÜÜ ');
writeln(' ÜÜBB ÜÜÜÜBÜ²²²Ü ²ÜÜ B ÜÜ²²²Ü ÜÜ ²ÝP²ÜÜ Ü Ü ÜÜ²²ÜÜ BB ');
writeln(' B ÜP²ÜÜ²²²ÜÜ BÜ²²²Ü ÜÜ² ÜÜÜÜÜ ÜÜ²² ÜÜ B Ü²ÜÜ ° Ü °ÜÜ²ÜÜÜÜÜÜ ');
writeln(' °ÜÜÜÜÜÜ²²²²B BÜ²²²Ü 2 ²ÜÜ²²Ü Ü²P²² ÜÜ Ü²ÜÜ ²Ü °ÜÜ²²ÜÜBB ');
writeln(' ÜÜÜ²Ü²²²²²B Ü²²ÜÜ Ü²Ü° ²ÜÜ²²² Ü² ÜÜÜÜ ÜÜ² ÜÜ²²²° ');
writeln(' ÜÜÜÜÜÜÜÜÜÜ °ÜÜÜ ²Ü²° Ü² ²ÜÜÜÜÜ²Ü² ÜÜÜÜÜÜ ²ÜÜ ÜÜ²²²° ');
writeln(' BÜÜ²²²Ü° ° ÜÜÜB Ü²ÜÜP° °²Ü ²ÜÜÜÜÜ ÜÜÜ²ÜÜÜÜÜÜÜÜÜÜ °Ü²²²²Ü ÜÜÜ ');
writeln(' Ü°ÜÜÜÜ Ü²B BÜÜ°°Ü²Ü²Ü° Ü Ü ÜÜÜÜÜÜÜÜÜÜ °Ü ');
writeln(' BÜÜBÜÜ ÜBB B ²ÜÜÜÜÜÜÜÜ ° ° BBBBÜÜÜ B ');
writeln(' ÜBBÜÜ B BBB Ý ° BÜ ');
writeln(' B Bp ° ');
```

```

writeln;
textcolor(7);
gotoxy(20,2);writeln('Crack WinRAR 3.41 by : arie a.k.a " X-cUTe ');
gotoxy(20,20);write('Pencet sembarang tombol kanggo mulai ngePatch !');
gotoxy(1,24);textcolor(lightred);writeln('ÛÛÛ');
textcolor(white);write('ÛÛÛ');
write(' Republik Indonesia');
textcolor(7);x:=readkey;

assign(F,'xx.exe'); { <-- File yg akan di patch }
{$i-} reset(F,1); {$i+}
if IOResult 0 then { <-- syarat #1. Cek keberadaan file }
begin clrscr;
gotoxy(25,10);writeln('Nyuwun ngapunten, winRAR.exe ora bisa di bukak');
x:=readkey; { <-- exit jika file tidak ditemukan }
halt(1);
end;

size:= FileSize(F); { <-- syarat #2. Cek file Size }
if size<846848 then { <-- nek ora pada, metu }
begin clrscr;
gotoxy(25,10);writeln('Versi file ora pada utawane wis di patch...');
x:=readkey;
halt(1);
end;

for I:=1 to 4 do { <-- poses patching file nulis 4 byte }
begin
seek(F,a[I].a);
ch:=char(a[I].b);
blockwrite(F,ch,1);
end;

clrscr;
assign(reg,'RARREG.KEY');rewrite(reg);rewrite(reg); { <- awal pembentukan file rarreg.key }
writeln(reg,'Cracked by X-cute # ASSHOLES Inc #');
writeln(' File wis di patch saiki kari ngisi datamu');writeln;
writeln(' Tulisen Datamu ( Jeneng & Organisasi )');writeln;
write(' Jeneng : ');readln(buff); { <- masukkan nama dan company }
write(' Keterangan : ');read(buff1);
writeln(reg,buff);writeln(reg,buff1);writeln;writeln(reg,"");
writeln(reg,' --* Dedicated to : *--');writeln(reg,"");
writeln(reg,' Dina Yulianita Sari');writeln(reg,"");
writeln(reg,'Kiye hasil gaweane wong NgapaX');
writeln(reg,"");writeln;
writeln(reg,'Copyright (c) 2005 X-cute, ASSHOLES INC');writeln;
close(reg);clrscr; { <-- akhir pembentukkan file rarreg.key }

gotoxy(1,8);textcolor(lightred);writeln(' ÛÛÛ');textcolor(white);write(' ÛÛÛ');
write(' May NgapaX Force Always Be With You..');
textcolor(7);gotoxy(8,2);writeln('Winrar 3.41 terdaftar dumateng : ');writeln;

```

```
writeln(' Jenenge : ',buff);
writeln(' Organisasi : ',buff1);
gotoxy(20,15);writeln('Persembahan kanggo : Dina Yulianita Sari');

textcolor(14);gotoxy(15,24);write('Info, bukak file "RARREG.KEY", nganggo text editor!');
x:=readkey; clrscr;writeln;
textcolor(lightred);write('ÛÛÛ');
textcolor(white);write('ÛÛÛ');
write(' ma5_arie@yahoo.com');
delay(500);
end.
{-----end of code-----}
```

Note: on any instance, this tutorial is just for educational purposes and not for commercialized and should never be carried out.

I wrote this tutorial just to explain how easy it would be for some person break the shareware protection.

"If you want use this software, please buy it to support the author."

thats it for now... keep crackin' reverse engineering.

I hope you've learned something from this,and if you did, let me know.
If you didn't, good for you. Tell me how to improve this tutorial.

[The only reason why I indulge in "software re-engineering" is because I get pleasure out of it. The first time when I managed to registering a shareware freely my own way, I was so overwhelmed; I shouted out loud with triumph and I felt so good about myself. All boiled down to the "ummmph" that I get - it's addictive and I wanted more each time.]

- " X-cute " -

ma5_arie@yahoo.com
<http://arieloverina.f2g.net/>