

Forum:[Hack Forums](#)

Thread: [Basics of Remote Administration Tools](#)

`Ninja - July 3, 2013, 2:00 pm

Contents:[Introduction](#)
[Free and Paid R.A.Ts](#)
[No-IP + Portforwarding](#)
[Member Tutorials and Help Desks](#)
[Spreading Methods](#)
[Crypters](#)

Thanks:

[Wackerboo](#) for post reservations and help!

`Ninja - July 4, 2013, 12:16 am

Introduction

What is a R.A.T?

A remote access tool (a RAT) is a piece of software that allows a remote "operator" to control a system as if he has physical access to that system. While desktop sharing and remote administration have many legal uses, "RAT" software is usually associated with criminal or malicious activity. Malicious RAT software is typically installed without the victim's knowledge, often as payload of a Trojan horse, and will try to hide its operation from the victim and from security software.

Source: [wikipedia](#)

Main Features of a R.A.T:Screen/camera capture or image control
File management (download/upload/execute/etc.)
Shell control (from command prompt)
Computer control (power off/on/log off if remote feature is supported)
Registry management (query/add/delete/modify)

Source: [wikipedia](#)

Why use a R.A.T?:

Many people use R.A.Ts for different reasons. Some use it to help their friends when they are stuck, some use it to watch their children's computer to keep them safe, then some use it to infect random people and fuck with them.

Words:

Many people use rats that are shortened or is just related to the topic while setting up rats or asking for help.

R.A.T(RAT) - Remote Administration Tool

FUD - Fully Undetectable File (No anti-viruses can detect it)

UD - Undetectable File (Some anti-viruses can detect it)

A/V(AV) - Anti-Virus

Crypter - Makes a file UD/FUD.

JDB - Java Drive-By

`Ninja - July 4, 2013, 12:17 am

Free and Paid R.A.Ts

Free:

[img]http://unremote.org/images/logo.png[/img]

Download: [Here](#)

Most people have used Darkcomet by now and really love it. Darkcomet is a user friendly, very stable R.A.T. It contains all of the basic features that a R.A.T contains and it also contains more. As Darkcomet is R.A.T it does have false positives so its a good idea to disable your A/V before you begin downloading Darkcomet. Also this R.A.T is not good to ddosing so don't complain and if you do get infected by Darkcomet some how, there is a Darkcomet remover. The Darkcomet coded (DarkCoderSc) left the scene of R.A.Ts about 1 - 2 weeks ago.

[img]http://www.cyber-software.org/site/wp-content/uploads/2012/12/logo5.png[/img]

Download: [Here](#) (Thanks [Plutonium](#))

I think this is the only free version of Cybergate (1.07.5). Anyway this version of the R.A.T is known to be quite unstable which is a bad thing if you want to keep quite a lot of slaves on the R.A.T. I suggest that you do not use this R.A.T if you are going to put a whole lot of slaves on it.

Paid:

Purchase Link: [Here](#) (Price: \$30)

jRAT is a java R.A.T, coded by redposi0n. As this R.A.T is coded in java, you will need java to be installed before using the R.A.T. Also this R.A.T used to be free but people abused it power so the owner made it paid. Most people use jRAT because it is FUD and has a very simple set-up.

[img]http://www.bshades.eu/images/top2.png[/img]

Purchase Link: [Here](#) (Price: 40€ Lifetime)

Blackshades is a very well known for all of the products their do. Their R.A.T is very good and stable and they do try their best to help out their customers even though they do take quite long to reply but they always try to give a detailed answer so that you can get fixed straight away.

Purchase Link: [Here](#) (Price: \$35)

I have been using emissary for like 6 months now and they have not let me down. Their R.A.T is amazing and is very simple to set-up. Emissary has all the great features that you will probably want to have. Very good support which responds very fast, never had a problem with them. It also comes with a lot of commands that are very good! The R.A.T is very stable and just nice to use overall.

`Ninja - July 4, 2013, 12:17 am

No-IP

You will need the No-IP so that the slaves can connect to you on different computers/laptops. However if you are using a different computer you will have to re-download the Dynamic Updater Client and install it. then it should start working after you selected the hosts again. The function that the updater does is to update your ip with the no-ip so that you wont loose slaves if your ip keeps changing.

1. Go to [No-IP](#).

2. Click sign up which is at the top of the page. You will need to enter a username, password and a valid email. You will need these for ever mostly. Enter a hostname that you will remember.

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

3. When you have entered all the details press Signup which is at the bottom (Not Get Enhanced).
Signup [\(Click to View\)](#)

4. Once you have signed up, you will need to go to your email and activate the code that you will receive.
5. Once your account is activated, go to the page where you will download the client to update the no-ip. Download: [Here](#)
Dynamic Client [\(Click to View\)](#)
[img]http://i1328.photobucket.com/albums/w525/Mob_Iliz/Screenshot_9_zps6a3e44b7.png[/img]
6. Once the Dynamic Update Client has downloaded, install it then login to the client when asked. Login [\(Click to View\)](#)
7. Once you have logged in, press edit hosts and check the box which is your no-ip address. Select Hosts [\(Click to View\)](#)
8. You are now done and you will use this no-ip in the IP/DNS boxes in the builders on R.A.Ts.

Portforwarding

I will be using sky to show how to portforward.

We need portforwarding so that the install/slave that we have just infected/helped (depends on which you do) can connect to your R.A.T Client.

1. Go to your start menu, type in cmd and start the app then type in "ipconfig" without the ".
cmd [\(Click to View\)](#)
2. Next go to your browser and type in the default gateway IP (Which for me is 192.168.0.1)
3. You will be asked to login into your router for sky the default user and pass is:
Code admin
skyfor others it might be:
Code admin
passwordCode admin
passCode admin
(no password)
Login [\(Click to View\)](#)
4. Once you have logged into your router, go to the security tab then to the services part (if different router: advanced tab then virtual servers/portforwarding for other routers)
Services [\(Click to View\)](#)
5. Click Add Custom Service and name it to what you want and the ports you want to portforward. Also make sure it is TCP not UDP then click Apply. (For other routers you will need to type in your IPv4 Address which is on the cmd (ipconfig) then click apply and you will be done.).
Custom Service [\(Click to View\)](#)
6. Next thing you need to do is go to Firewall Rules where you will need to add an Outbound and Inbound service.
Firewall Rules [\(Click to View\)](#)
7. For the Outbound service click Add (below) then select the service you will be using and change Block Always to Allow always (Leave everything else alone) then click Apply.

Outbound Services ([Click to View](#))

8. Now for the Inbound service press Add (below) then select the service you will be using and change Block Always to Allow always and enter your IPV4 Address which is on the cmd (ipconfig). Then finally click Apply.

Inbound Services ([Click to View](#))

Firewall Done ([Click to View](#))

9. You will need to be listening to the port on the R.A.T which you have just forwarded.

Listen ([Click to View](#))

10. Go to canyouseeme.org and type the port in you just forwarded and see if it has worked.
[canyouseeme](#) ([Click to View](#))

If you still need help vist: <http://portforward.com/> or PM me and I will portforward for you.

`Ninja - July 4, 2013, 12:18 am

Member Tutorials and Help Desks

Darkcomet:

[Lakai](#) - ? | [Terror](#) | [How to setup Darkcomet - Lakai's Way \(Noob Friendly\) | ?](#)

[Plutonium](#) - [\[TuT\]How To Setup DarkComet RAT 5.3.1 ||Portforwarding & With Pictures\[TuT\]](#)

Cybergate:

[Plutonium](#) - [\[TuT\] How To Setup Cybergate RAT 1.07.5 - Port Forward - Noob Friendly -UPDATE28thFeb](#)

jRAT:

[Prefix](#) - [\[Tutorial\] How to set-up jRAT \[Tutorial\]](#)

[Flaming Vls](#) - [jRAT Tutorial! Detailed! Pictures](#)

Emissary:

[Coding4Noobs](#) - [Emissary NET 1.0+ Setup Tutorial + Help Desk](#)

[Prefix](#) - [\[Tutorial\] How to set-up Emissary NET \[Tutorial\]](#)

legacyLink:

[Prefix](#) - [\[Tutorial\] How to set-up legacyLink \[Tutorial\]](#)

Misc Tutorials:

[Lakai](#) - ? [The Empire ? How to change icons of your stubs/.exe's ? The Empire ?](#)

[MyStErIoUs-87](#) - [\[TuT\] how to keep the slave for as long as possible \[Easy Steps \]](#)

[IIMachavelli](#) - [\[Infamous\] How to make money via Rat slave](#)

Help Desks:

[Prefix](#) - [Prefix R.A.T Desk || Free || Setting up || Test installs \(TEMP\) || Portforwarding](#)

[Frostix](#) - [\[FREE\] | ? | R.A.T Setup Service | ? | \[SUPPORT\] - \[DarkComet\] \[BlackShades\] \[jRAT\]](#)

I'm looking for a lot more help desks to add, please PM me if you got any I can add!

`Ninja - July 4, 2013, 12:18 am

Spreading

Everything going to need spreading at the end of the day so they can get some installs. So I have

just provided some ways that you can spread.

Omegle

This method is known to be very saturated as no one does it anymore. But all you got to do is find an omegle bot and make sure you have a good comment followed by your link then start the bot up.

Chat-Avenue

Quite an easy but saturated way. You just go to the chat, you can either spam a chat with your link or pretend you're a girl and say pics but ofc the file won't look legit but it does work most of the time.

Youtube Spreading

You will need to have a youtube account ofc. Upload a video about a software like either runescape account cracker or just money hacks for some games and slot your FUD server in the description. They will most likely download it and try to run it.

Torrent Spreading

This way does take time to make it fully work. You will have to make a torrent again on one of the sites and become legit at first. When you made like 5 - 10 legit uploads, just slide your server into one and upload it (Make sure it does look legit or is binded to legit software). Then you have to upload more legit torrents after that.

I have missed out quite a lot of spreading methods I think but if you have any suggestions on what to add just PM me.

This post has been hold for prefix guide.

Note: If you look around HF there is so much spreading tutorials.

Ninja - July 4, 2013, 12:21 am

Crypters

Everyone needs a crypter to either make a paid non-fud R.A.T FUD or just a free R.A.T like darkcomet FUD. Crypters are the reason that they world today has so much installs on their R.A.T clients.

Settings for R.A.Ts + Crypters:

If the R.A.T does not have a in-built crypter then don't enable start-up and persistence because when you are about to crypt your server you will select those options on the crypter. If you did have start-up and persistence on the R.A.T + Crypters, it would go badly and probably break your server so it won't work anymore.

Why use paid crypter and not free:

It is always a good idea to buy a crypter instead of using a free one because the paid ones always get updated daily and when they are only UD they normally get updated back to FUD. The free ones don't really get updated as much times and most people upload them to virustotal which ruins the FUD of the crypter. Also paid crypters are a lot more reliable!

Paid Crypters:

[img]http://razorhf.com/sig.png[/img]

Purchase: [Here](#)

I did use this crypter once before, I wouldn't say that it is that good as it just froze my pc from time to time but it is good and the price is cheap. I wouldn't say it is the best idea to buy but as I said it is good and the price is cheap and good. RazorCrypt has been running for about 1 year which is very good and makes it quite reliable. The crypter should still be FUD. Good support but kinda slow.

[img]http://i.minus.com/ibqjXpO4gFEx34.gif[/img]

Purchase: [Here](#)

I'm not quite about this crypter but what I know about it is that it has been going on for quite a while and by the looks of it is doing very well. It seems that quite a lot of people have purchased it before and really think it is a very nice crypter. The coder is very kind and respectable and is a great support.

Impress. - July 4, 2013, 1:24 am

Really nice thread we need more HQ members like you?

SickdudePW - July 4, 2013, 1:26 am

I love the thread, but I think that Crypting/Crypters should be a subject too.

`Ninja - July 4, 2013, 7:35 am

Thanks for the comments. I would add crypting/crypters but I only have one more post on this thread where I can make it into what I need.

Ad?m - July 4, 2013, 7:52 am

Great thread. Thanks for including legacylink

times558 - July 4, 2013, 9:06 am

Great thread man, you are really HQ!

`Ninja - July 4, 2013, 10:54 am

Thanks for the positive comments everyone.

Primarys4Reason - July 4, 2013, 12:40 pm

I try this method maybe my RAT will work now :/

E V O - July 4, 2013, 1:49 pm

Amazing thread mate.

We feel honoured for mentioning us. ;)

`Ninja - July 4, 2013, 2:41 pm

Thanks E V O.

@Everyone: Added crypter section.

Coding4Noobs - July 4, 2013, 3:41 pm

nice HQ Thread. It turned out nice.

`Ninja - July 5, 2013, 12:19 am

Thanks Coding4Noobs for the comment.

redi - July 5, 2013, 5:29 am

Thanks for this Simple Guide. Pretty cool, Gonna try it.

Burn3diC3 - July 5, 2013, 5:32 am

Nice guide. Though you could explain more on how a crypter works (dependencies, runtime/scantime, cryptography etc.), not only that you will need one.

`Ninja - July 5, 2013, 5:57 am

(Jul 5, 2013 05:32 AM)Burn3diC3 Wrote: [\[CITE\]](#) Nice guide. Though you could explain more on how a crypter works (dependencies, runtime/scantime, cryptography etc.), not only that you will need one.

Yeh will improve it soon, very busy atm trying to do something stuff.

Slyx - July 5, 2013, 11:43 am

Nice give me some good tipps this therad

`Ninja - July 5, 2013, 2:39 pm

Thank you very much Slyx and to everyone else that likes this guide.

marcmax5 - July 5, 2013, 3:03 pm

Very nice Hq Thread, great for anyone!

`Ninja - July 5, 2013, 3:47 pm

Merged No-ip + Portforwarding together. Put a members tutorials in replacement.

IIMachavelli - July 5, 2013, 7:46 pm

This thread has been added to the list

<https://hackforums.net/showthread.php?tid=3525922>

Good tutorial Prefix.

`Ninja - July 6, 2013, 1:39 am

(Jul 5, 2013 07:46 PM)IIMachavelli Wrote: [\[CITE\]](#) This thread has been added to the list

<https://hackforums.net/showthread.php?tid=3525922>

Good tutorial Prefix.

Thank you for adding me to the list.

clark.dll - July 7, 2013, 1:56 am

Extremely well put together guide. Vouch for Prefix, he know what he's talking about and has years of experience to back it up.

Darc - July 7, 2013, 2:39 am

Great thread. This will be very helpful to members who are new to RATS.

`Ninja - July 8, 2013, 9:14 am

Anyone got some more links for the Member Tutorials and Help Desks part?

Also: Thanks for the positive comments everyone!

M0dy - July 8, 2013, 9:33 am

Great thread, well organized and easy to follow. Thanks Prefix

bobby24 - July 8, 2013, 10:27 am

Very nice and well written, best for beginners.

Thanks OP

Deep Web - July 8, 2013, 11:35 am

very hq thread especially for the beginners thumbs up

`Ninja - July 8, 2013, 1:36 pm

Always glad to make threads for beginners!

JayBoss - July 10, 2013, 7:58 am

Vouch for Prefix, he is really known on the rat scene.
Thanks for sharing some knowledge.

`Ninja - July 10, 2013, 11:55 am

Thank you ??Dynasty for the vouch.

Master Oromis - July 12, 2013, 8:08 am

Thank you very much for this. :) It will be used.

`Ninja - July 12, 2013, 9:20 am

Taken down. FML FML FML FML FML FML

Elixine - July 12, 2013, 9:25 am

(Jul 12, 2013 09:20 AM)Prefix Wrote: [\[CITE\]](#) Taken down. FML FML FML FML FML FML
May I ask why you took it down? o.o

`Ninja - July 12, 2013, 9:26 am

Blame legacyWARE for this (Adam). Shittest R.A.T on the planet!

Ad?m - July 12, 2013, 9:28 am

(Jul 12, 2013 09:27 AM)?ETRO Wrote: [\[CITE\]](#) Ok, I think Prefixs account has been hacked.
It hasn't.

I told him I no longer want him as support staff on legacyware projects because he has scam reports on him. So he flips

`Ninja - July 12, 2013, 9:30 am

(Jul 12, 2013 09:28 AM)Ad?m Wrote: [\[CITE\]](#) It hasn't.

I told him I no longer want him as support staff on legacyware projects because he has scam reports on him. So he flips

I told you I got hacked but hey you don't believe anything as your shit legacyWARE support because I was the one who was doing set-ups and just ignored those idiots.

KVVS - July 12, 2013, 9:37 am

(Jul 12, 2013 09:28 AM)Ad?m Wrote: [\[CITE\]](#) It hasn't.

I told him I no longer want him as support staff on legacyware projects because he has scam reports on him. So he flips

Agreed,
He scammed someone for 300bucks, and now he wants to make it look like he's been hacked or something along those lines

Ad?m - July 12, 2013, 9:39 am

(Jul 12, 2013 09:37 AM)kvvs Wrote: [\[CITE\]](#) Agreed,
He scammed someone for 300bucks, and now he wants to make it look like he's been hacked or something along those lines
Wait, He scammed you too? That's 4x scams then. Why didn't you post a scam report on this kid?

KVVS - July 12, 2013, 9:42 am

(Jul 12, 2013 09:39 AM)Ad?m Wrote: [\[CITE\]](#) Wait, He scammed you too? That's 4x scams then. Why didn't you post a scam report on this kid?

Not me, i meant the guy in the deal dispute's forum

<https://hackforums.net/showthread.php?tid=3614451>

`Ninja - July 12, 2013, 9:43 am

(Jul 12, 2013 09:39 AM)Ad?m Wrote: [\[CITE\]](#) Wait, He scammed you too? That's 4x scams then. Why didn't you post a scam report on this kid?

Idiot he said someone not him, N1 Idiot here!

Noxler - July 12, 2013, 10:39 am

Lol wut?

FML FML FMI FMI FMI FML FML

Nobyl - July 12, 2013, 11:13 am

Wtf, this kid acts like he's five; i guess this is proof that humans can evolve backwards.

Master Oromis - July 12, 2013, 2:14 pm

Ouch.. alright, so he got exiled. No more tutorial. I wasn't finished reading it - ___ -

1337 - July 12, 2013, 8:54 pm

Great thread helped me thanks. ?

kamika\$e - July 12, 2013, 10:08 pm

If you did happen to get hacked, I hope you get your account back.

If you didn't get hacked and you're just making this whole story up then fuck you.

FireLook - July 13, 2013, 1:17 am

(Jul 12, 2013 10:08 PM)#LulzVex Wrote: [\[CITE\]](#) If you did happen to get hacked, I hope you get your account back.

If you didn't get hacked and you're just making this whole story up then fuck you.

Its me Prefix. Yeh yeh I been hacked appertantly, anyway, I don't want my account back anymore, Got really bad rep now because of all this.

Judgeit. - July 13, 2013, 1:31 am

This is the HQ'nes people I have ever seen. Shit, LQ uber member..

`Ninja - July 21, 2013, 5:27 am

Sorry people had problems with my account. Fixed everything on the thread.

`Ninja - July 22, 2013, 5:30 am

Fixed some problems that I forgot to update.

times558 - July 22, 2013, 6:28 am

(Jul 22, 2013 05:30 AM)Prefix Wrote: [\[CITE\]](#) Fixed some problems that I forgot to update.

Your DarkComet download isnt working. Replace it with this:

<http://ge.tt/api/1/files/6kymJ7I/5/blob?download>

From Nitohs thread found here:

<https://hackforums.net/showthread.php?tid=2632776>

Tricorn - July 22, 2013, 6:29 am

(Jul 4, 2013 12:21 AM)Prefix Wrote: [\[CITE\]](#) Crypters

Everyone needs a crypter to either make a paid non-fud R.A.T FUD or just a free R.A.T like

darkcomet FUD. Crypters are the reason that they world today has so much installs on their R.A.T clients.

Settings for R.A.Ts + Crypters:

If the R.A.T does not have a in-built crypter then don't enable start-up and persistance because when you are about to crypt your server you will select those options on the crypter. If you did have start-up and persistance on the R.A.T + Crypters, it would go badly and probably break your server so it won't work anymore.

Why use paid crypter and not free:

It is always a good idea to buy a crypter instead of using a free one because the paid ones always get updated daily and when they are only UD they normally get updated back to FUD. The free ones don't really get updated as much times and most people upload them to virustotal which ruins the FUD of the crypter. Also paid crypters are a lot more reliable!

Paid Crypters:

[img]http://razorhf.com/sig.png[/img]

Purchase: [Here](#)

I did use this crypter once before, I wouldn't say that it is that good as it just froze my pc from time to time but it is good and the price is cheap. I wouldn't say it is the best idea to buy but as I said it is good and the price is cheap and good. RazorCrypt has been running for about 1 year which is very good and makes it quite reliable. The crypter should still be FUD. Good support but kinda slow.

[img]http://i.minus.com/ibqjXpO4gFEx34.gif[/img]

Purchase: [Here](#)

I'm not quite about this crypter but what I know about it is that it has been going on for quite a while and by the looks of it is doing very well. It seems that quite a lot of people have purchased it before and really think it is a very nice crypter. The coder is very kind and respectable and is a great support. I purchased byte crypter before and was 100% not impressed.

Same with razor crypter I could the stub size was massive.

`Ninja - July 22, 2013, 2:33 pm

Thanks, retro.

@Tricorn: I will see and update that part then, thanks for info.

M@ddox - July 23, 2013, 11:09 am

good job Prefix !!!! this is good information

`Ninja - July 23, 2013, 12:47 pm

Thanks maddox for the positive comment.

Adorable - July 23, 2013, 12:52 pm

Thanks for the guide! This does really help people that are new to the Ratting business!

Coding4Noobs - July 23, 2013, 12:59 pm

welcome back prefix.

this is a really nice thread you have put together.

Ad?m - July 23, 2013, 3:28 pm

"(P.S: legacyLink was claimed to be backdoored as a member on HF said."

Could you link me to this so called member or even better a thread. Or are you holding a grudge because I told you I no longer want you working for us as you are a scammer.

`Ninja - July 24, 2013, 1:40 am

(Jul 23, 2013 03:28 PM)Ad?m Wrote: [\[CITE\]](#) "(P.S: legacyLink was claimed to be backdoored as a member on HF said."

Could you link me to this so called member or even better a thread. Or are you holding a grudge because I told you I no longer want you working for us as you are a scammer.

Dude you said you aint going to talk to me, so stop viewing my threads and shit yeh?

Second: I got told by a UB3R here which I'm not going to say his name because you will probably just neg gang rep him. So that stays on my thread.

Ad?m - July 24, 2013, 7:04 pm

(Jul 24, 2013 01:40 AM)Prefix Wrote: [\[CITE\]](#) Dude you said you aint going to talk to me, so stop viewing my threads and shit yeh?

Second: I got told by a UB3R here which I'm not going to say his name because you will probably just neg gang rep him. So that stays on my thread.

So you got told from a source that we are backdooring? lol At least provide proof of this so called "Backdoor" You can't just say that and have nothing to back it up with. We both know this is your way of trying to get back at us which is immature. Oh btw did you resolve that \$300 scam report on you?

I'm out.

`Ninja - July 25, 2013, 2:38 am

(Jul 24, 2013 07:04 PM)Ad?m Wrote: [\[CITE\]](#) So you got told from a source that we are backdooring? lol At least provide proof of this so called "Backdoor" You can't just say that and have nothing to back it up with. We both know this is your way of trying to get back at us which is immature. Oh btw did you resolve that \$300 scam report on you?

I'm out.

Yes the \$300 got resolved. Which I can provide proof.

And the log probably is on steam of saying its backdoored, so I will provide a screenshot when I get on my laptop.

paewand sahd - July 25, 2013, 3:25 pm

Really nice thread we need more HQ members like you Thumbsup

`Ninja - July 26, 2013, 3:38 am

Thanks paewand sahd for the comment.

times558 - July 26, 2013, 11:21 am

Can I just confirm that LegacyWARE is NOT backdoored. Thanks.

`Ninja - July 26, 2013, 11:36 am

You said that it was retro. Just tell the truth.

times558 - July 26, 2013, 11:42 am

(Jul 26, 2013 11:36 AM)Prefix Wrote: [\[CITE\]](#) You said that it was retro. Just tell the truth.

I didnt really say it was, I just told you that there was a thread about it but it got deleted so im not sure. Even look in the Steam/Skype logs. You probably didnt read it right or get what I was saying properly. Most likely its not backdoored and I really doubt that it is. Anyway, we should speak more on skype/steam about this, this is not the place.