

# redpill Agent

## What is redpill Agent?

redpill Agent is spy software that allows you to monitor a computer anywhere in the world that you don't have access to. The spy software can be remotely installed.

Alternatively you can install the monitoring software directly at the computer using a USB drive. It will take less than 5 seconds and no setup or registration is required at the target computer.

You will receive hourly key logs of everything that was typed including all usernames and passwords. You will also receive a picture (screenshot) of what the target was doing every time any one of your alert words is typed.

You will be able to monitor any number of computers with one license.

## Is it legal?

The software itself is legal but it is possible to use it for illegal purposes. redpill does not encourage the illegal use of any of its products. Legal uses of the software might include the following:

- Penetration Testing by White Hat / Ethical Hackers.
- Parents wanting to monitor a child that might be overseas.
- Private detectives or authorities with the needed authorization.

redpill (the developer) are not liable for any type of damage, litigation, or legal predicaments that may arise due to use or abuse of redpill Agent.

Please use redpill Agent with restraint and visit our blog (<http://blog.redpill.co.za>) to see discussions on legal and moral issues.

## How it works / What you need to do:

**Step 1:** Open a gmail account.

You will need to open a gmail account as redpill Agent will send all the information to your gmail email. Gmail is free. To open an account go to [www.gmail.com](http://www.gmail.com). If you already have an account it is suggested that you open a new account specifically for redpill Agent.

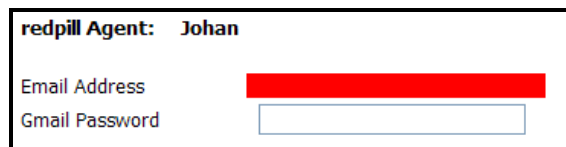
**Step 2:** Purchase a license and email the gmail email address you want to use to [register@redpill.co.za](mailto:register@redpill.co.za). We will create an account for you and email you your username

and password for redpill Agent (this might take up to 12 hours after we received confirmation of your payment).

To purchase a license go to <http://www.redpill.co.za> and click on Purchase.

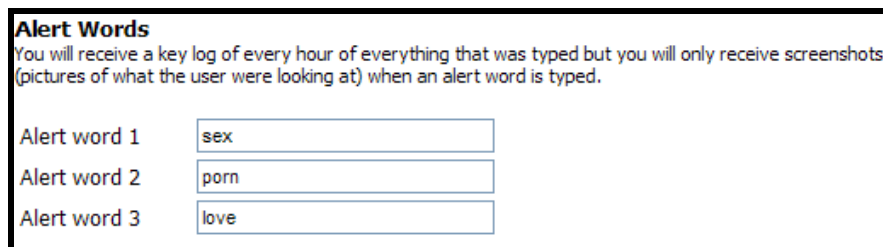
**Step 3:** Login to redpill Agent. Go to <http://www.redpill.co.za> and click on redpill Agent Login.

Enter your gmail password (see image below). Your gmail password **will not** be stored in our database. The password is encrypted and stored within the file that you will download. The email address and password is needed as your gmail account will be used to send the data and not the email server or account of the target.



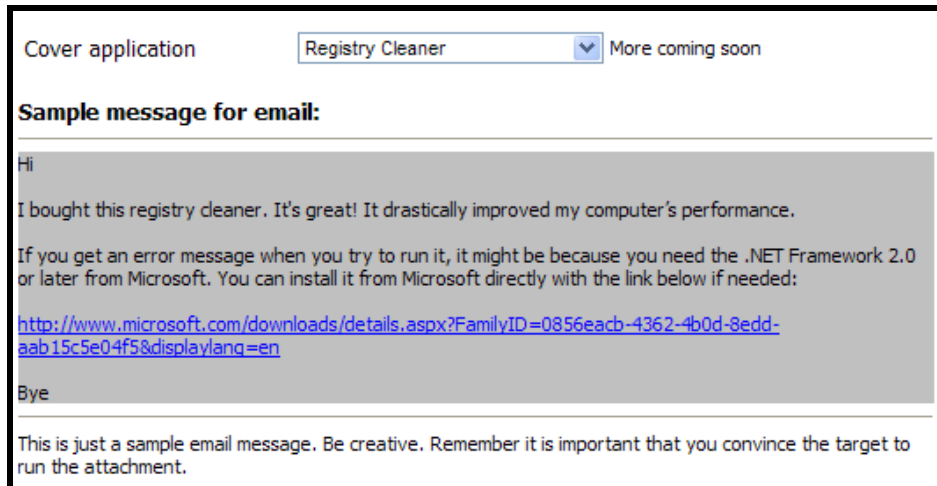
<b>redpill Agent: Johan</b>	
Email Address	<input type="text"/>
Gmail Password	<input type="password"/>

Choose your alert words. You will receive a key log email every hour (when there was activity) but you will only receive a screenshot when an alert word was typed ... so choose your alert words carefully.



<b>Alert Words</b>	
You will receive a key log of every hour of everything that was typed but you will only receive screenshots (pictures of what the user were looking at) when an alert word is typed.	
Alert word 1	<input type="text" value="sex"/>
Alert word 2	<input type="text" value="porn"/>
Alert word 3	<input type="text" value="love"/>

Choose a cover application. The cover application will be the attachment that you will email to the target. When you select a cover application a sample email message that you could use with that application will be provided.

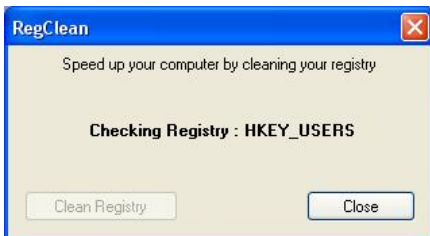


Remember that it is important that the target will run the attachment. It will give the target the impression of doing something else (or do something else) while it is actually busy installing redpill Agent in the background without the target's knowledge.

Cover applications include the following (more will be added over time):



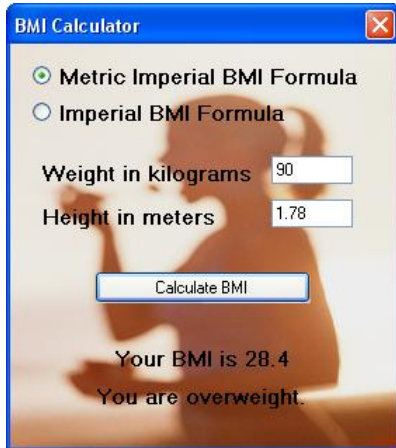
A Virus Removal Tool. Convince the target that there is a dangerous new virus that is not detected by standard anti-virus software but that you found this tool that detects and removes it



RegClean – A registry cleaner. Convince the target that this application drastically improves your computer's performance by cleaning your registry.



If you have physical access to the target computer (only a few seconds is needed), you can use this application to install or remove an installation.



The BMI calculator is a useful application that calculates your Body Mass Index and then tells you if you are underweight, normal, overweight or obese.

This cover application really works and is using scientific formulas.

You will be tempted to use this one but remember that each time it is opened it will check if redpill Agent is monitoring the computer, and if not it will secretly install redpill Agent.

After you selected the cover application click on 'Download'. When prompted select Save (not Run).

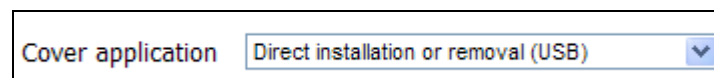


Save the file on your computer (make sure you know where it is saved).

**Step 4:** Test the cover application. The data is only sent to your gmail address and remember that your gmail password is not stored in our system ... so it's safe to test it on your own computer. Run the file that you downloaded on your own computer. After you ran the file (just double click on it) type one of your alert words, log into your gmail account and make sure you got the email message with the attachment.

If you didn't receive it contact us at [support@redpill.co.za](mailto:support@redpill.co.za).

Remember to uninstall it from your computer using the redpill agent removal program. To get the removal program select 'Direct Installation or removal' (see figure below).



### Step 5: Install on the target computer.

#### If you have physical access to the computer:

Choose 'Direct Installation' and save it on a USB drive (Flash drive), insert it in the computer you want to monitor and then just double click on the cover application. The installation will take less than 5 seconds and no setup or registration is required at the target computer.

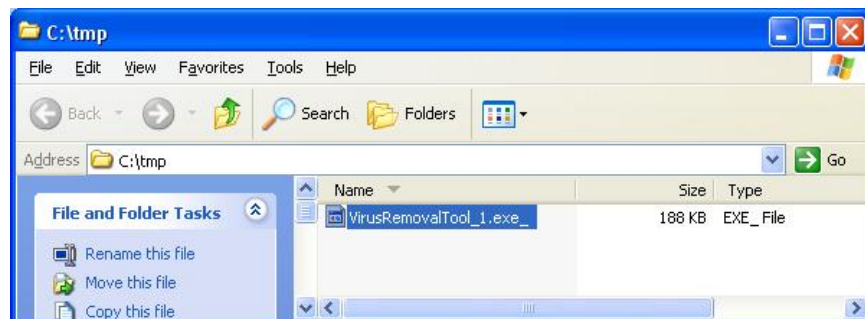
#### If you don't have physical access to the computer:

If you need to install remotely you need to email the target the cover application that you downloaded. Remember to 'convince' the target to run the application. Have a look at the sample email message that was provided with the cover application but as you probably know the target you will be able to come up with a much more convincing email (be creative). The target will not know that redpill Agent is being installed and will think that the program (cover application) is doing what it promises.

When you email the message don't use gmail as gmail will block any email message that has an application (exe) as attachment. If you don't have an email server that you can use you could create a Yahoo email account and use that account to send the message as Yahoo don't block applications as attachments if they are zipped. If you don't have a zip program try winzip or winrar (free or trials are available).

If the target has a gmail email address (or another email server that blocks exe's even when they are zipped) you could do the following:

Rename the cover application by adding a '\_' at the back.



You then don't have to zip the file. Just explain to the target that he will need to save the attachment on his computer and rename it back by removing the '\_' at the back. Remember that if your wording in your email was convincing the target would want to run the application.

If you have problems renaming the file it might be because the extension is hidden. In windows explorer (or my computer) click on Tools -> Folder Options -> View and uncheck the 'Hide extensions of know file types'.

**Step 6:** Wait for the target to run your cover application. Remember that the target will think he/she is running a virus removal tool or a registry cleaner to speed up his/her computer and will not know that redpill Agent is secretly being installed.

**Repeat steps 3 – 6 as many times as you want to install on any number of computers.** You can log into your redpill Agent account from any computer at any time when you need to install on another computer.

### **To stop monitoring a computer:**

To uninstall redpill Agent you need to run the redpill Agent removal program on the target computer. Log into your account and select 'Direct installation or removal'.

Cover application

Save the file to a USB drive and run it on the target computer.

### **Please note**

No remote installation can be guaranteed. The installation might fail due to one of the following reasons:

- The target might choose not to run the attachment.
- The target computer might not have the minimum requirements (see below).
- The target computer might have special firewall software blocking emails.
- The user on the target computer might not have administrative rights on the computer (needed for a successful installation).

As there is no way for us to confirm that an installation succeeded **we cannot give any refunds for redpill Agent. For a safer guaranteed installation have a look at redpill Spy at <http://www.redpill.co.za>** (also includes a free edition).

### **Target computer minimum requirements for redpill Agent:**

Windows XP or Windows Vista with the .NET Framework 2.0 or later.

The .NET Framework is already included with Microsoft Vista and is available as a download from Microsoft. You could also include a link to the .NET Framework on Microsoft's website in your email (sample email will be provided).

### **Examples and tips**

## **An example of using redpill Agent with Social Engineering**

redpill Agent allows you to remotely and covertly install spy software on a computer anywhere in the world. It allows you to choose from a list of cover applications (a program that gives the impression of doing something else while it secretly installs the spy software) that you can email to a target.

Just emailing the target the file and hoping for the best is not a good idea. Remember that if your first attempt is unsuccessful you will need to wait a few days or weeks before trying again to avoid making the target suspicious.

To improve your chances of success you will need to do some social engineering.

Example:

1. Find out as much as possible about the target (interests, hobbies, etc).
2. Create an alias with an email address and try to befriend the target using email, facebook (or any other social networking site).
3. At some stage, not at the beginning, mention how you managed to get rid of your computer performance problems using a great tool to clean up your registry.
4. When the target asks about the tool, email him/her your registry cleaner (one of the cover applications in redpill Agent).
5. The target will now be eager to run the application and will probably even contact you if he/she has any problems running it.
6. While the target is busy typing you an email to thank you for your help, every key will be recorded and secretly emailed to you!

From that point on the computer will be monitored and you will receive key logs and screenshots.