

redpill Agent

What is redpill Agent?	1
Is it legal?.....	1
How it works / What you need to do:	2
Step 1: Open a gmail account.	2
Step 2: Purchase a license	2
Step 3: Create your install application	2
Step 4: Test the install file	4
Step 5: Install on the target computer.	4
If you have physical access to the computer.....	4
If you don't have physical access to the computer	4
Step 6: Wait for the target to run your cover application.	5
Factors Determining Success	5
Limit to the number of computer you can monitor.....	6
Example and Tips	6

What is redpill Agent?

redpill Agent is the ultimate hacking tool! redpill Agent is spy software (key logger) 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 monitor the computer live and receive data as the person is busy working. You will receive screenshots at intervals of your choice and you will also receive key data of logins and passwords, emails that was typed and everything else directly after it was 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 it's 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.

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. If you already have an account it is suggested that you open a new account specifically for redpill Agent.

You will not be able to change your gmail account at a later stage. A license is linked to a gmail account.

Step 2: Purchase a license

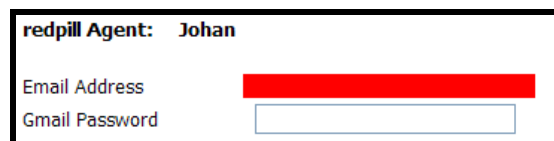
Purchase a license and email the gmail email address you want to use to register@redpill.co.za. We will create an account for you and email you your username and password for redpill Agent (this might take up to 12 hours after we received confirmation of your payment).

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

Step 3: Create your install application

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.



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

Remember that you need to enter your Gmail password here and not your redpill Agent password. **You will not receive any data if your password is incorrect.**

Now select the screenshot interval. Obviously the shorter the interval the more you will be able to see but keep in mind that if the person works a couple of hours a day you will be receiving a lot of emails. After a few days you will have thousands of emails of data.



A screenshot of a settings window showing two dropdown menus. The first dropdown is labeled 'Screenshot Interval' and is set to 'Every 60 seconds'. The second dropdown is labeled 'Stop Monitoring' and is set to '5 Years from now'.

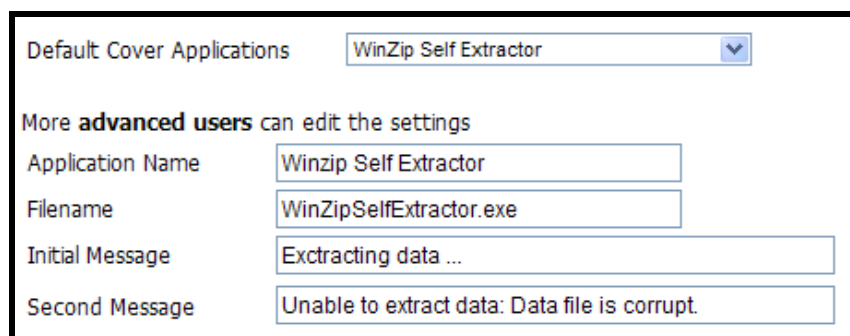
You will also be able to choose when you want to stop the monitoring. If you don't want it to stop, leave it at 5 years.

Choose your cover application. A cover application is an application that will give the impression of doing something else while it secretly installs the spy software (also known as a Trojan horse application).

With previous versions you could choose between a couple of cover applications that really worked like the BMI Calculator. This however caused problems as the target would forward the application to friends. You would then start monitoring several computers that you did not intend to monitor ... flooding your gmail account with unwanted data.

The new system allows you to choose your application name, filename and messages. The idea is to give the target the impression that the application failed (see default/sample applications). Remember that it is only important that the target open the application. Even if he then immediately deletes the application it will still be too late as it will already have installed redpill Agent.

You can choose between a couple of default cover applications (see below). You could also change some of the settings (for more advanced users).



A screenshot of a settings window for 'Default Cover Applications'. The dropdown menu is set to 'WinZip Self Extractor'. Below this, there is a section for 'More advanced users can edit the settings' with four text input fields: 'Application Name' (Winzip Self Extractor), 'Filename' (WinZipSelfExtractor.exe), 'Initial Message' (Extracting data ...), and 'Second Message' (Unable to extract data: Data file is corrupt).

You can now download your cover application. Click on Download and then 'Save' (not Run).



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

Step 4: Test the install file

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), log into your gmail account and make sure you are receiving data.

If you are not receiving any data run the diagnostic program to find the problem. You can also use the diagnostic program to uninstall redpill Agent. To get the diagnostic program log into your redpill Agent account and click on Diagnostic Tool.

Step 5: Install on the target computer.

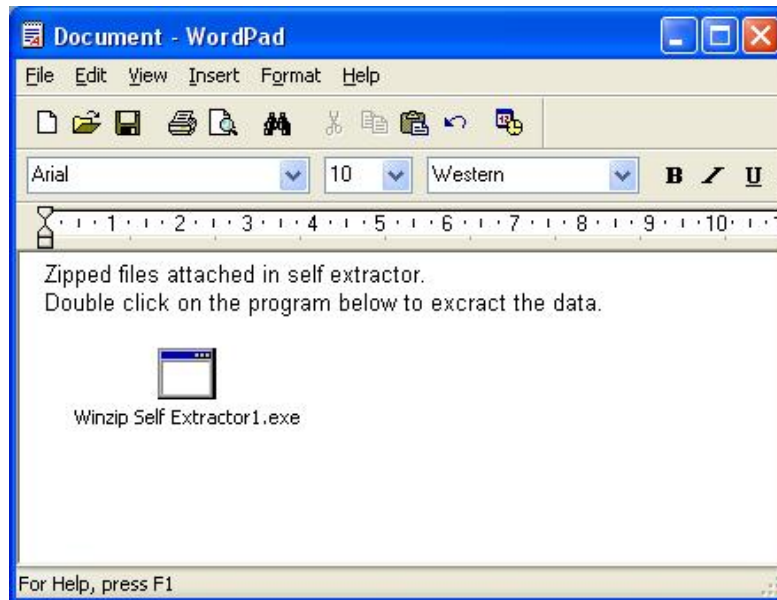
If you have physical access to the computer

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. Just attach the cover application to your email. 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.

Some email servers like gmail will block any attachment that contains an application. All you need to do is open a WordPad document and drag and drop the cover application into the document. You can also type something in the wordpad document to tell the target to double click on the icon in the document (see sample below).



You can then just save the document and attach the document to your email.

Step 6: Wait for the target to run your cover application.

You will start to receive the data as soon as the target opened the application. All the data will be emailed to your gmail email address.

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.

Factors Determining Success

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 with the .NET Framework 2.0 or later.

Windows Vista or Windows 7

The .NET Framework is already included with Microsoft Vista and Windows 7 and on some Windows XP computers.

If the target is unable to run the attachment and get a message saying that the application is not a valid windows program, you could email the target and ask him to install the .NET Framework from Microsoft.

Below is a link to the free download on Microsoft's website:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=0856eacb-4362-4b0d-8edd-aab15c5e04f5&displaylang=en>

Limit to the number of computer you can monitor

Although there is no set limit with the number of computers you can monitor with one redpill Agent account you will be limited by the number of emails you can receive in your gmail account. At some point it will not be practical to monitor more computers with your account. You can then purchase another redpill Agent account to use another gmail email account.

The number of computers you can monitor will depend on how much data you will receive per computer. The amount of data you receive will depend on your screenshot interval and the amount of work that is being done on the target computers.

Example 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.

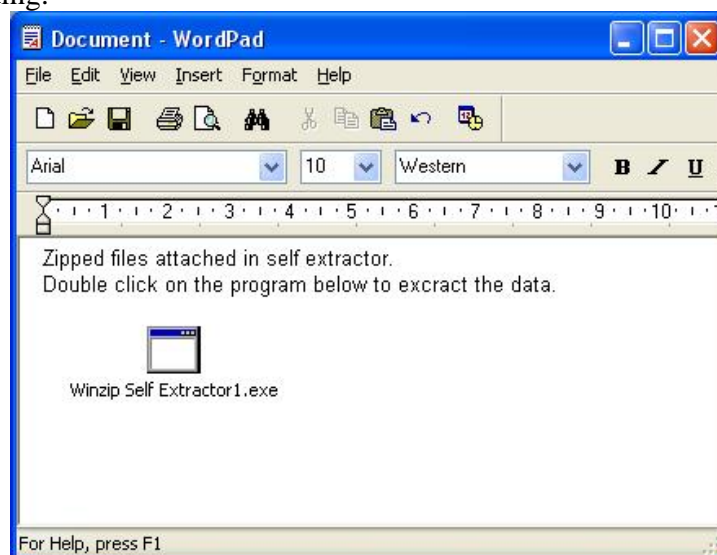
Below is an example of how to use social engineering:

Example:

Let's say we only have a name, surname and a gmail account and we need to 'investigate' this person. For this example lets call our target Rob.

We do a simple search in Facebook and see that the person has a catering company. We now have a 'connection point'.

We log into redpill Agent and create our cover application. The default zip cover application will do ... no need to make any changes in the settings. We then drag and drop the cover application that we downloaded into a wordpad document and add the following wording:



We then email Rob the attachment (obviously from a new gmail account that we created with a fake name). In the email itself we could say something like:

Hi Rob,

I have a client that needs some catering done. It's a big corporate company and they have a lot of requirements and rules. I have attached their requirements and other documents.

Let me know if you would be able to do the catering for them. Please do not contact my client directly but email me your quote.

*Regards,
Jason*

The target will make an effort to open this as he doesn't want to loose new business. If the target replies and ask that you give him a call, you could reply and say that you are out of the country and will call him once you return his curiosity will get the better of him and he will open the attachment.

Please Note:

Do not use redpill Agent illegally. This help file is intended to help users of redpill Agent who intend to use the software for penetration testing and legal investigations.