Antimalware Doctor removal

Antimalware Doctor is a fake antivirus used by malevolent persons to infect computer users for various purposes:

- immediate financial gain by tricking the innocent user to buy a license to remove the infections found– of course fake detections;

- stealing of your credit card details if a naïve user falls into the trap and follows the instructions to buy the activating license for this fake antivirus;

- continuous display of pop up advertisements;

By distributing this malware, the "cyber-criminals" can hide other malicious intentions aswell, it has an uninterrupted connection to an IP address(malicious domain), listening for commands. In my test this IP address was :

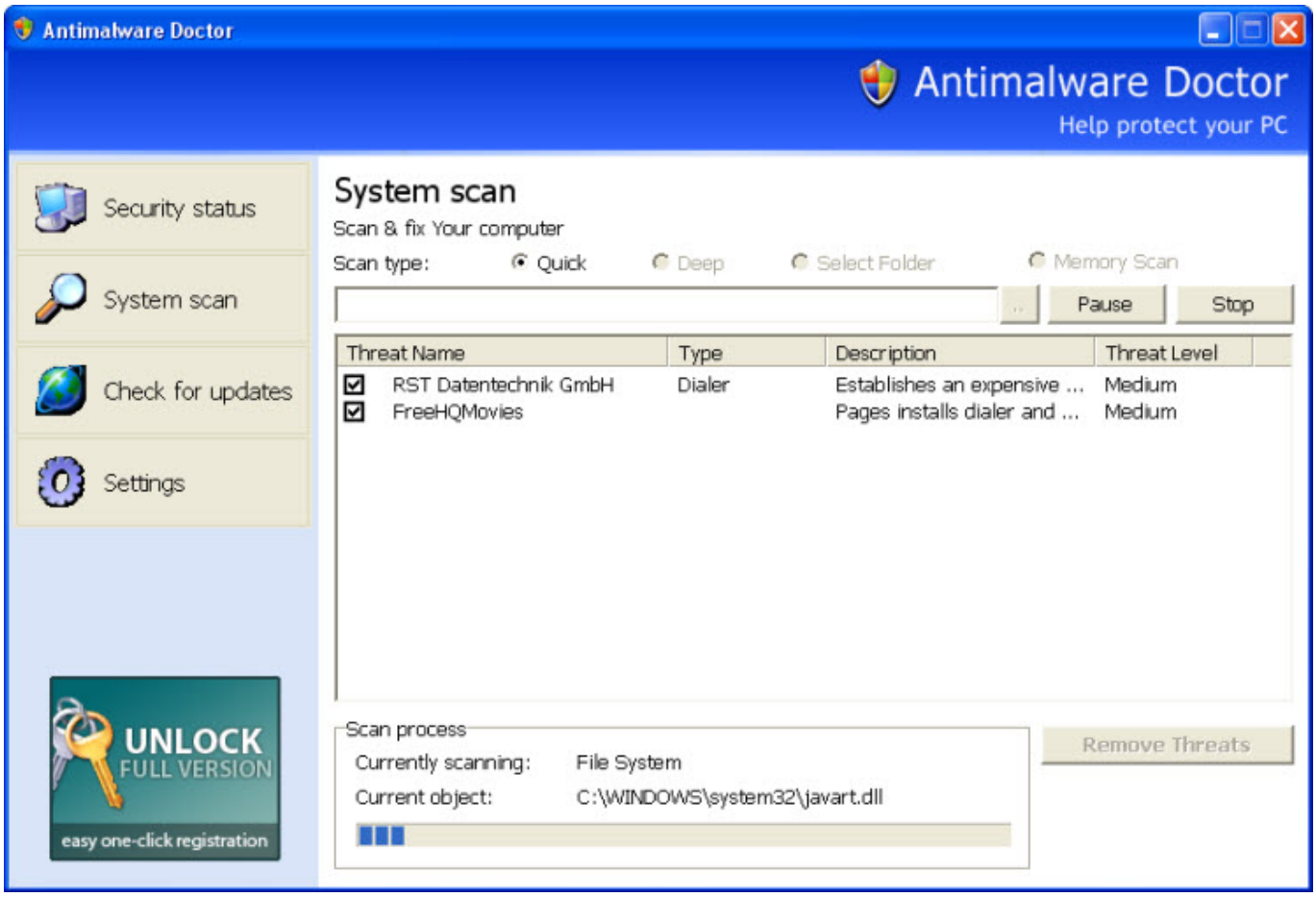
> 93.186.170.62(*kgbtoe.in* malware domain) on port 80, the request was :
>
> GET /install.php?do=1&coid=011ACB248A9E2992401570F2DFB7A229&fff=7070010100&IP=192.168.0.2&lct=AUT&v=X240
>
> and response from the server:
>
> 200 "OK"

Maybe at the first look it seems that *Antimalware Doctor* does not do many harms to the computer, maybe you will think: "Just another fake antivirus, the prejudice occurs only if somebody buy it" but this continuous connection to the above IP address posses a huge risk for your computer and to an end to your most important informations as credit card details or online accounts.

Even if *Antimalware Doctor* trojan virus does not appears to attack the sensitive data in the first stages after its installation, it keeps communicating with the Command & Control server and the evil person who is behind it can anytime upload and execute in the victim's computer other malware, trojan, viruses much more advanced and with a much more sinister purpose than only to take your money for a license for this rogue antivirus.

This malware infects computers by tricking the users to use malicious online scanners very often offered in pop-ups from dubious websites or it comes bundled in warez programs, keygens or cracks. It has the capacity to avoid the debugging procedures, the process running in virtual machines or sandboxes is obstructed, its author were very careful to not reveal the inside code so the only solution to see it in action was to infect my computer with it and to track the changes made to the system and the network connections. Its messages and windows looks very credible and legitimate, the author made considerable efforts to imitate the Windows Security Center or Automatic Updates, here are a few examples :


Automatic Updates
System Security Pack Upgrade
Update
System Security Pack 2010.78.932 (Antimalware Doctor Upgrade; KB952746)
Details
Thank you for your interest in obtaining updates from our site.
To use this site, you must be running Microsoft Internet Explorer 5 or later.
To upgrade to the latest version of the browser, go to the Internet Explorer Downloads
<http://go.microsoft.com/fwlink/?linkID=24748> website.
If you prefer to use a different web browser, you can obtain updates from the Microsoft
Download Center <http://go.microsoft.com/fwlink/?linkid=10678> or you can stay up to
date with the latest critical and security updates by using Automatic Updates. To turn on
Automatic Updates:
Click Start, and then click Control Panel.
Install
Remind Later


Antimalware Doctor
Antimalware Doctor
Help protect your PC
Security status
System scan
Check for updates
Settings
System scan
Scan & fix Your computer
Scan type:
Quick
Deep
Select Folder
Memory Scan
Pause
Stop
Threat Name
Type
Description
Threat Level
RST Datentechnik GmbH
Dialer
Establishes an expensive ...
Medium
FreeHQMovies
Pages installs dialer and ...
Medium
Scan process
Currently scanning:
File System
Current object:
C:\WINDOWS\system32\javart.dll
Remove Threats
UNLOCK
FULL VERSION
easy one-click registration

The *Antimalware Doctor* installation folder was %Application Data%\F730125D34AE47F98F6C006FB04FC690 this is a random name of course and contains 3 files:

- k70ccreloc.exe(random name as you see) which is actually the virus.

Size: 1MB; MD5: 181D67052C0C55A3375B262103F14545

- enemies-names.txt which contains the name of fake detections, see examples :

> [UnderageHost]
> Threat=Browser hijacker
> Description=Silently sets itself as IE start- and search pages (furthermore done by a file on every system start), and adds some favourites. Anyone visiting the site that installs it is sick!
> [SuperSexPass]
> Threat=(Unverified) Browser hijacker
> Description=Redirects MSN search for URLs that could not be resolved.
> [Amircivil]
> Threat=Malware
> Description=
> [DeskMate.Tahni]
> Threat=Trojan
> Description=This trojan horse adds itself to systemstart and connects without user consent to the internet.It also downloads other trojan horses and malware like Zlob , SurfSideKick, Smitfraud-C.

[CastGen]
Threat=Trojan
Description=This trojan horse downloads other malware and trojans like ClimaxBucks.InternetOptimizer, Avenue Media and Media-Motor without user consent.
[Win32.Downloader.Wzip32]

- local.ini file is a configuration file and contains data used by the program, examples;

[ThankYouPage]
formCaption={APPNAME}
lHeader={APPNAME} has been successfully activated!
bContinue=OK
mInfo=Thanks for purchasing and registration {APPNAME}.%NEWLINE%%NEWLINE%All the neccessary information will be send to Your email. %NEWLINE%Please, SAVE them into secure location in case you need to reinstall the software.%NEWLINE%Feel free to contact Customer Support Service if You have any questions.%NEWLINE%%NEWLINE%Useful advices from {APPNAME} Team:%NEWLINE%%NEWLINE%- Scan your computer once ot twice a day and remove all the viruses and security threats.%NEWLINE%- Maximal protection of your computer is enabled ONLY if You turn ON all the Security Status services.%NEWLINE%- Do not use {APPNAME} together with other antivirus softwares.%NEWLINE% It may result some software conflicts between them.%NEWLINE%- If you have any question, please, contact Customer Support Service.%NEWLINE%%NEWLINE%Please, press “OK” button and wait while {APPNAME} will eliminate threats. Please, be patient.%NEWLINE%

This configuration file introduced me to the idea that this program is highly “customizable”, it can be used by the hackers with different names and different text messages. At installation time it added also shortcuts on the Desktop and in the Internet Explorer Quick Launch folder : Antimalware Doctor.lnk

In the registry the value “k70ccreloc.exe” was added in

“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run”

a key added:
“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Antimalware Doctor”

and another key
“HKEY_USERS\S-1-5-21-839522115-261903793-1417001333-500\Software\Antimalware Doctor Inc”

The *Antimalware Doctor removal* instructions are simple in this stage(immediately after installation) when other infections did not occured yet:

- kill the Antimalware Doctor process in Task Manager, be aware of its name, in my case it was: k70ccreloc.exe, this is a random name;

- delete the registry keys and values associated with it, especially the values under the *“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run”* and *“HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\Run”* are the ones

responsible for automatic start at boot time of this virus. You can delete these values by accessing regedit.exe, click Start>Run>type regedit.exe and hit Enter or click OK, navigate to these keys and delete them via context menu(right-click);

- delete the virus installation folder specified above. Again be aware because the folder name is a random one, a long string formed from letters and ciphers. In my case it was F730125D34AE47F98F6C006FB04FC690. The %Application Data% folder is default hidden, you must modify in the *Folder Options* the setting to *Show hidden files and folders.*

Removing this virus is an emergency in the first moments when you see it in your computer, it must not have enough time to run and do any other damages to the computer like causing other more serious infections. Following the Antimalware Doctor removal instructions provided above, it can not be difficult to remove it even for a not so savvy computer user.

Continuing the analysis of this fake antivirus if an user click “Activate now” or Remove threats” button, it is seen connecting to the “sales” page using an Internet Explorer frame, the URL address is :

https://srv102.cyberhost.com on port 443.

Looking inside the program code, another URL address is found for sales page, take a look:

http://iters.in/purchase.php?aaa=csp&fff=7070010100&sbb=X240-9-aftscann&lct=USA&ttt=1&tns=4&sss=2&nocashe=10

and another one:

https://secure.realfastpayplus.com/payment/?sku_name=AMDOCT_EN_02,AMDOCT_EN_01,AMDOCT_EN,AMDOCT_EN_00,ACTF_EN_00&aid=csp&affid=7070010100&nid=USA&sub=X240-9-aftscann&lid=4&p=1&sku_checked=2

The installer of this rogue antivirus was scanned at http://anubis.iseclab.org online scanner, see the report. In conclusion, Antimalware Doctor virus is *only apparently* not so sophisticated in doing computer damages, it presents a huge potential risk and must be removed from the computer as soon as possible.

Keep safe !