**Ransomware tracer**

A REPORT

Submitted by

**Prathiksha**

**200970108**

UNDER THE GUIDANCE OF

**Mr. Akshay Bhat**

**Asst. Professor Senior Scale**

**Department of Computer Applications**

**Text

Description automatically generated**

**Manipal Institute of Technology**

**ABSTRACT**

* This report attempts to discover the surreptitious features of ransomware and to address it in information systems security research.
* It intends to elicit attention with regard to ransomware, a newly emerged cyber threat using such encryption technology as RSA, and to help both academic researchers and IT practitioners understand the technological characteristics of ransomware, along with its severity analysis.
* As ransomware infections continue to rise and attacks employing refined algorithm become increasingly sophisticated, data protection faces serious challenges.

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| **Sn.** | **Title** | **Page** |
| **1** | Introduction | **4** |
| **2** | Protect against Ransomware | **5** |
| **3** | Installation and configuration | **7** |
| **4** | Snapshots of tool | **4** |
| **5** | References | **16** |

**Introduction**

What it is?

Ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it. Ransomware variants have been observed for several years and often attempt to extort money from victims by displaying an on-screen alert.

How does it work?

* Ransomware is often spread through phishing emails that contain malicious attachments and through drive-by downloading. Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without the user’s knowledge.
* Crypto ransomware, a malware variant that encrypts files, is spread through similar methods and has also been spread through social media, such as Web-based instant messaging applications. Additionally, newer methods of ransomware infection have been observed. For example, vulnerable Web servers have been exploited as an entry point to gain access to an organization’s network.

**What do I do to protect against Ransomware?**

Infections can be devastating to an individual or organization, and recovery can be a difficult process that may require the services of a reputable data recovery specialist.

US-CERT recommends that users and administrators take the following preventive measures to protect their computer networks from ransomware infection:

* Employ a data backup and recovery plan for all critical information. Perform and test regular backups to limit the impact of data or system loss and to expedite the recovery process. Note that network-connected backups can also be affected by ransomware; critical backups should be isolated from the network for optimum protection.
* Keep your operating system and software up-to-date with the latest patches. Vulnerable applications and operating systems are the targets of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.
* Maintain up-to-date anti-virus software, and scan all software downloaded from the internet prior to executing.
* Restrict users’ ability (permissions) to install and run unwanted software applications, and apply the principle of “Least Privilege” to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network.
* Avoid enabling macros from email attachments. If a user opens the attachment and enables macros, embedded code will execute the malware on the machine.
* Do not follow unsolicited Web links in emails. Refer to the [Phishing](https://security.berkeley.edu/resources/phishing) resources found on this website for more information.

Individuals or organizations are discouraged from paying the ransom, as this does not guarantee files will be released.  However, the FBI has advised that if Cryptolocker, Cryptowall or other sophisticated forms of ransomware are involved, the victim may not be able to get their data back without paying a ransom.

What to do if you believe your system has been infected with ransomware

### 1. Disconnect From Networks

* Unplug Ethernet cables and disable wifi or any other network adapters.
* Put your device in Airplane Mode
* Turn off Wi-Fi and Bluetooth

This can aid in preventing the spread of the ransomware to shared network resources such as file shares.

### 2. Disconnect External Devices

Immediately disconnect:

* USB drives or memory sticks
* Attached phones or cameras
* External hard drives
* Or any other devices that could also become compromised

### 3. Report the Incident

It is important that incidents are reported as early as possible so that campus can limit the damage and cost of recovery.

* If you have access to the internet on another system see: [Reporting an Incident.](https://security.berkeley.edu/quick-links/report-security-incident)

**Installation and configuration**

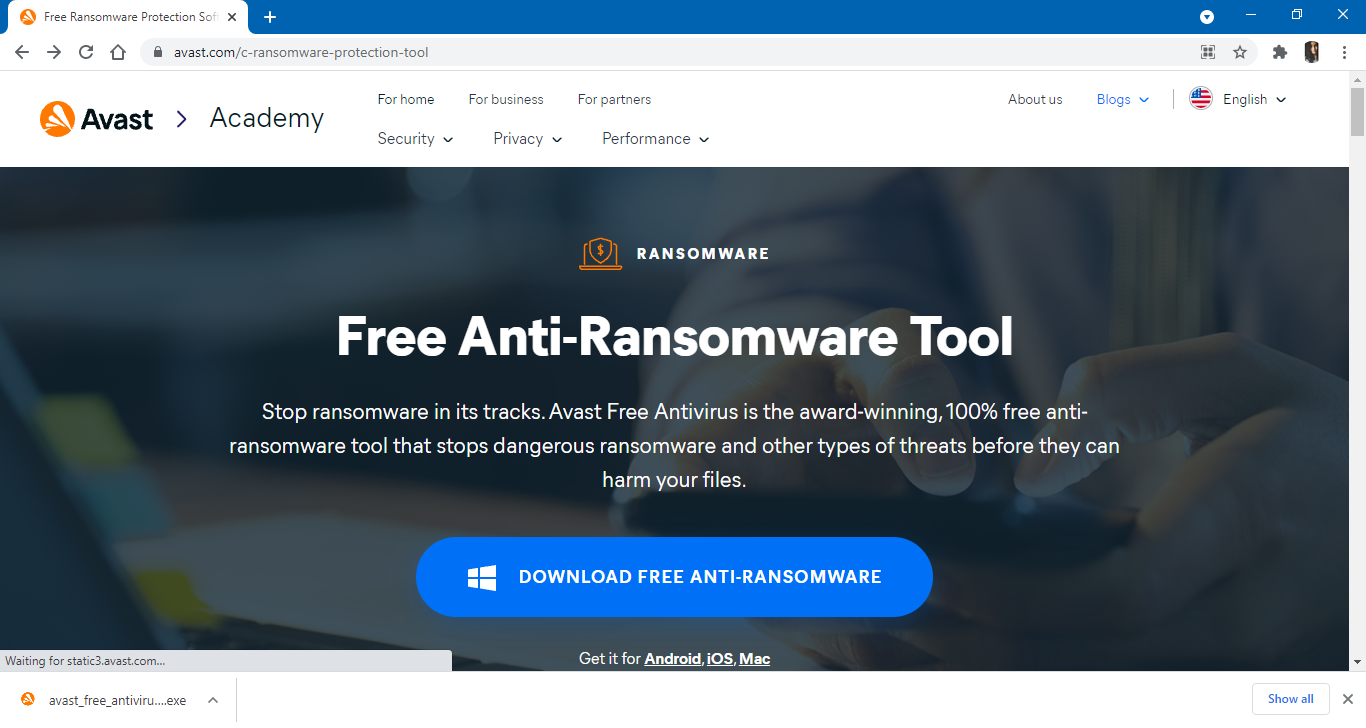
Step:1

Visit following URL

<https://www.avast.com/c-ransomware-protection-tool>

Step:2

Click on **“**[DOWNLOAD FREE ANTI-RANSOMWARE](https://www.avast.com/download-thank-you.php?product=FAV-ONLINE-ACADEMY)”.



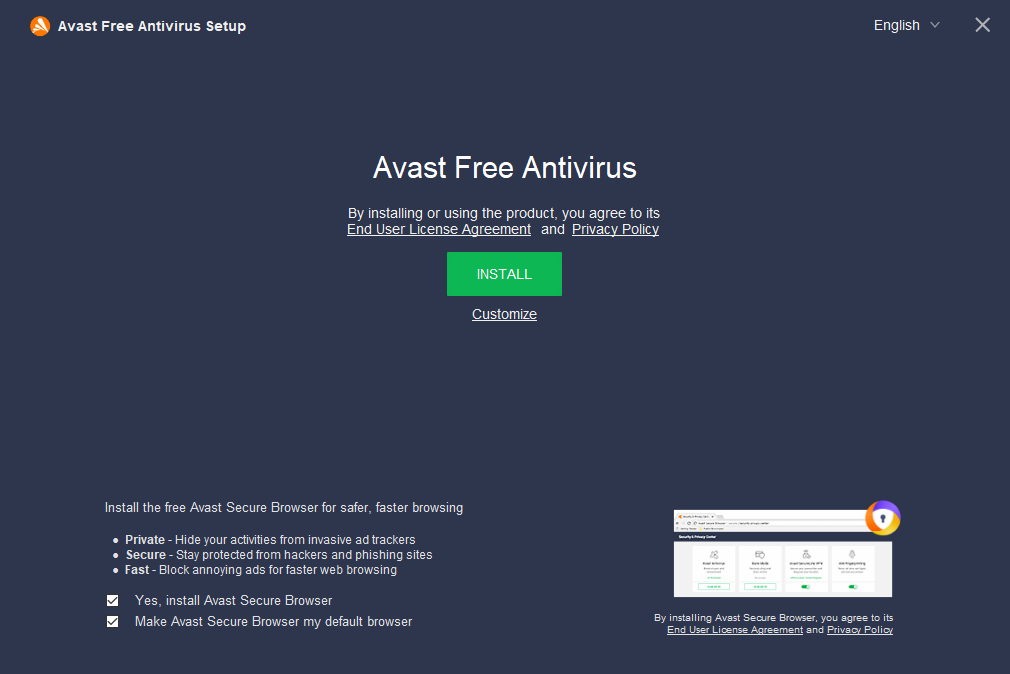
Step:3

After downloading double click on downloaded .exe file.



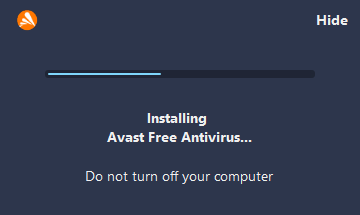
Step:4

Click on “Install”, and let it download.

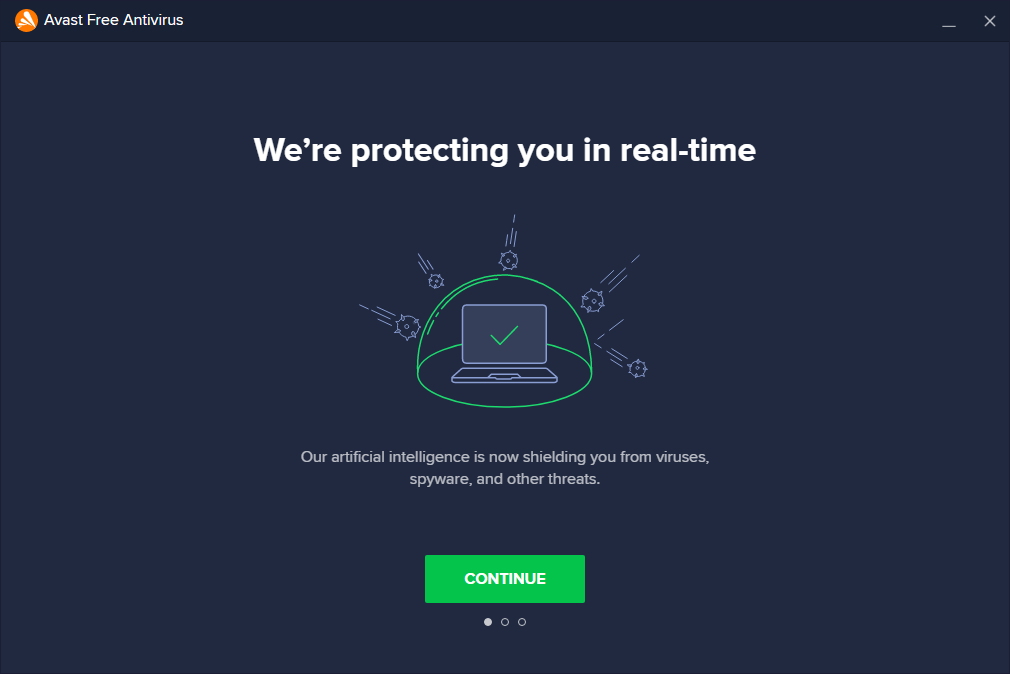


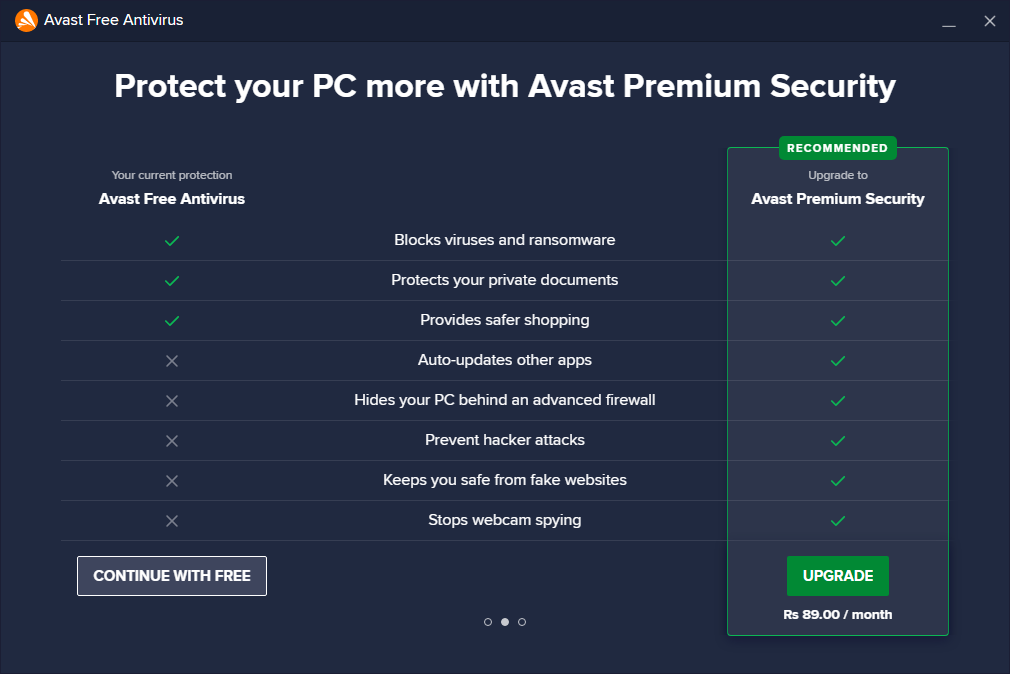
Step:5

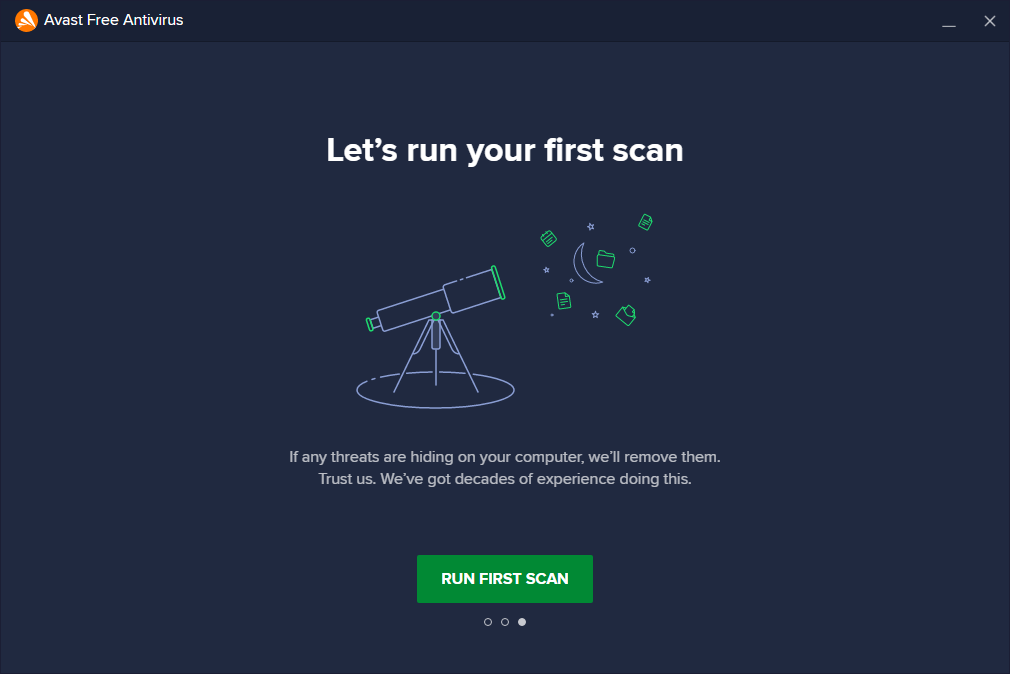
Wait for few minutes to complete installation.

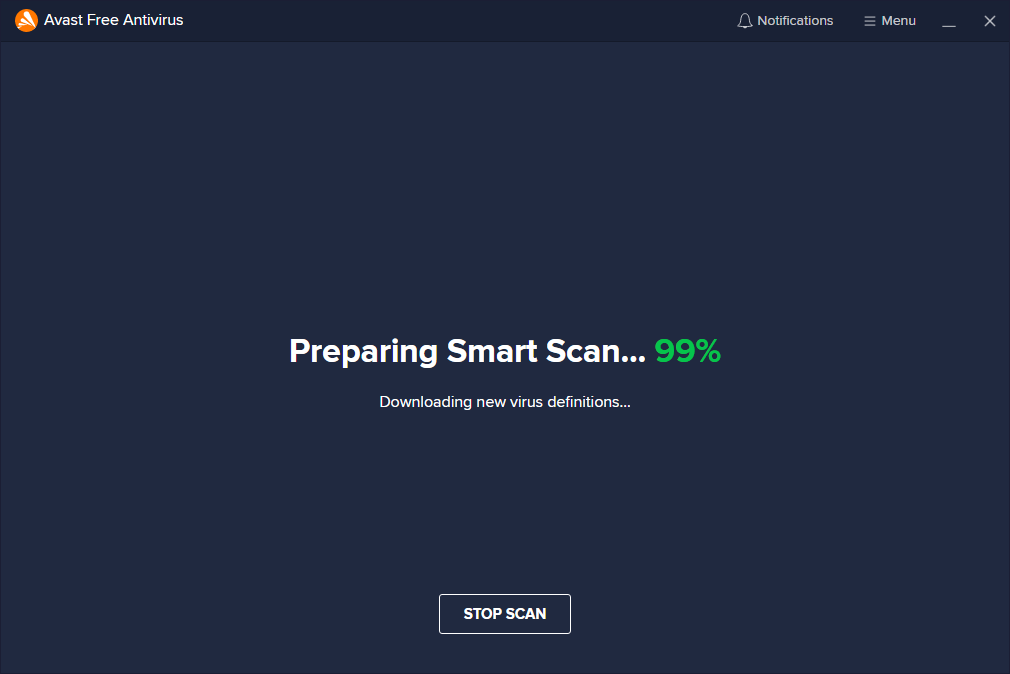


**Snapshots of tool**

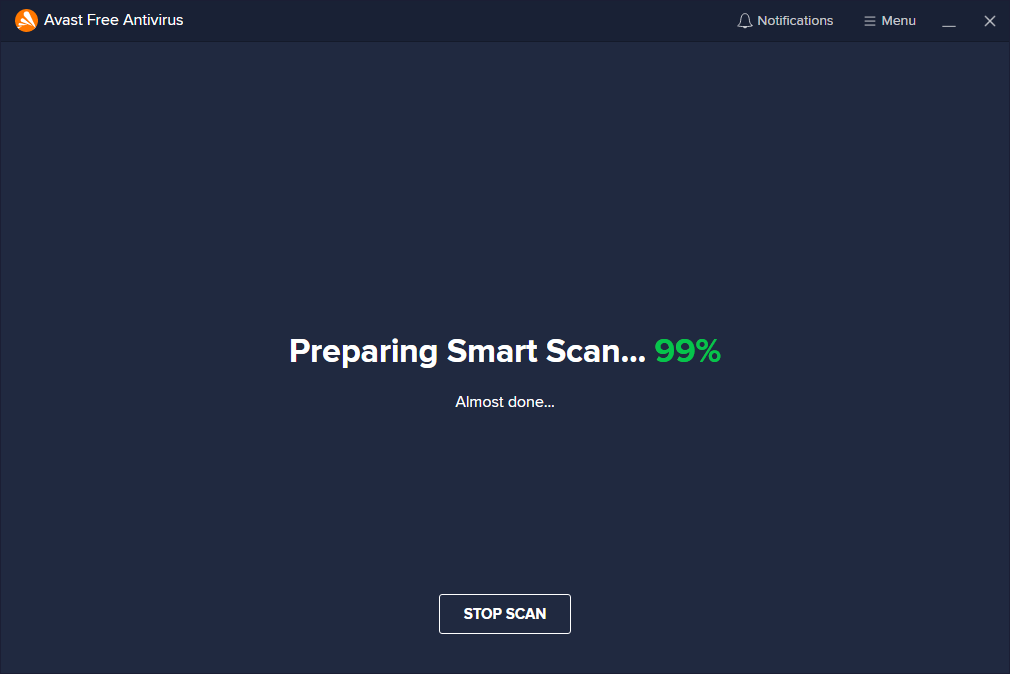


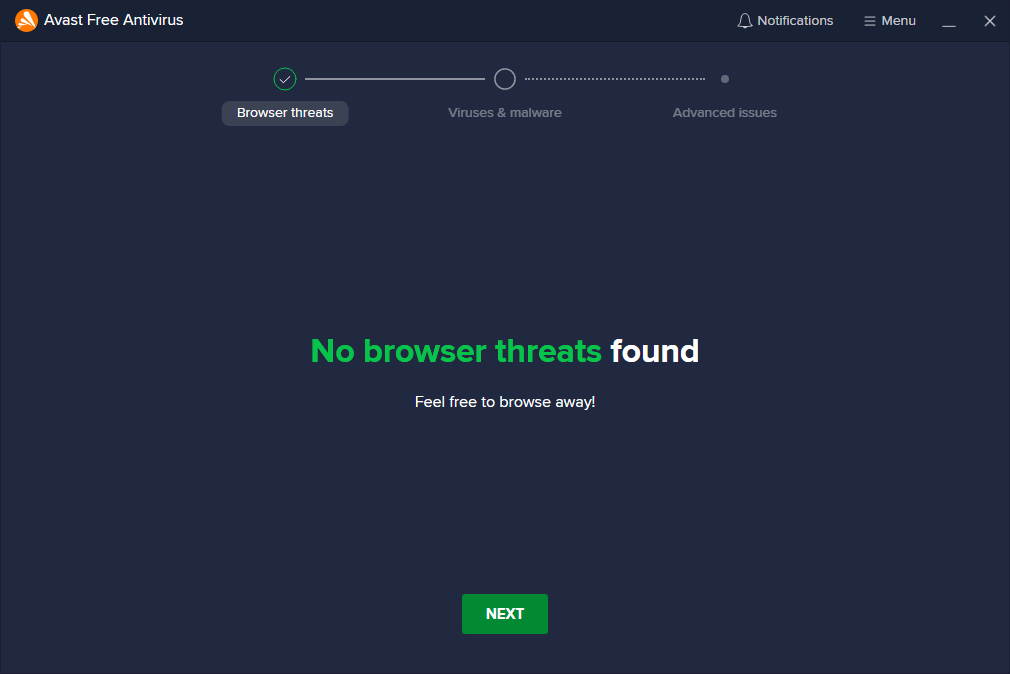




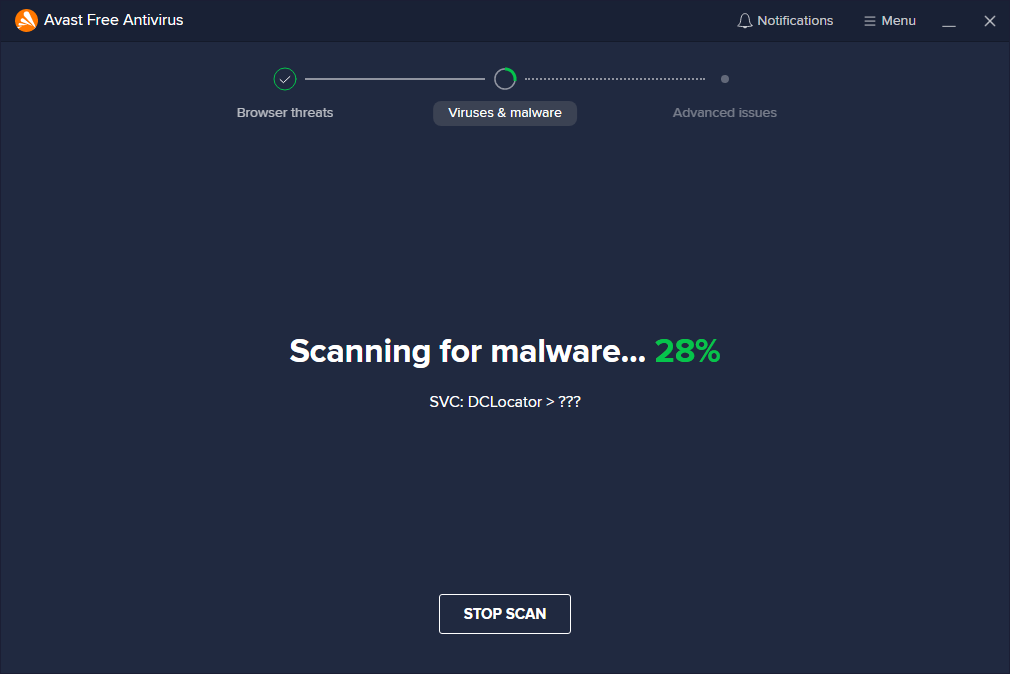


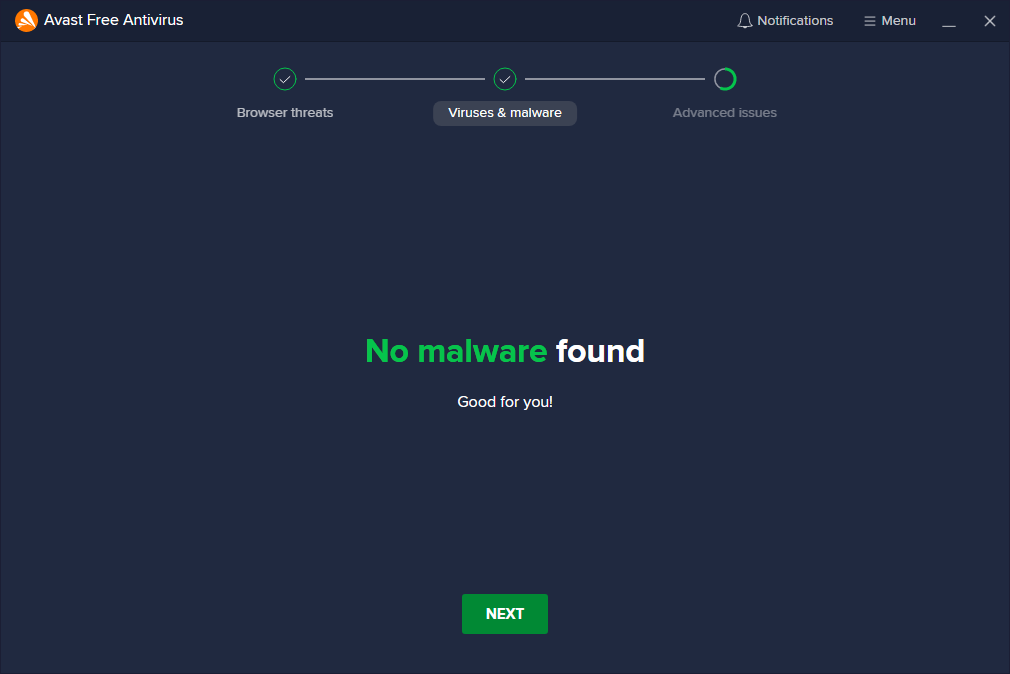
**Checking browser threats:**



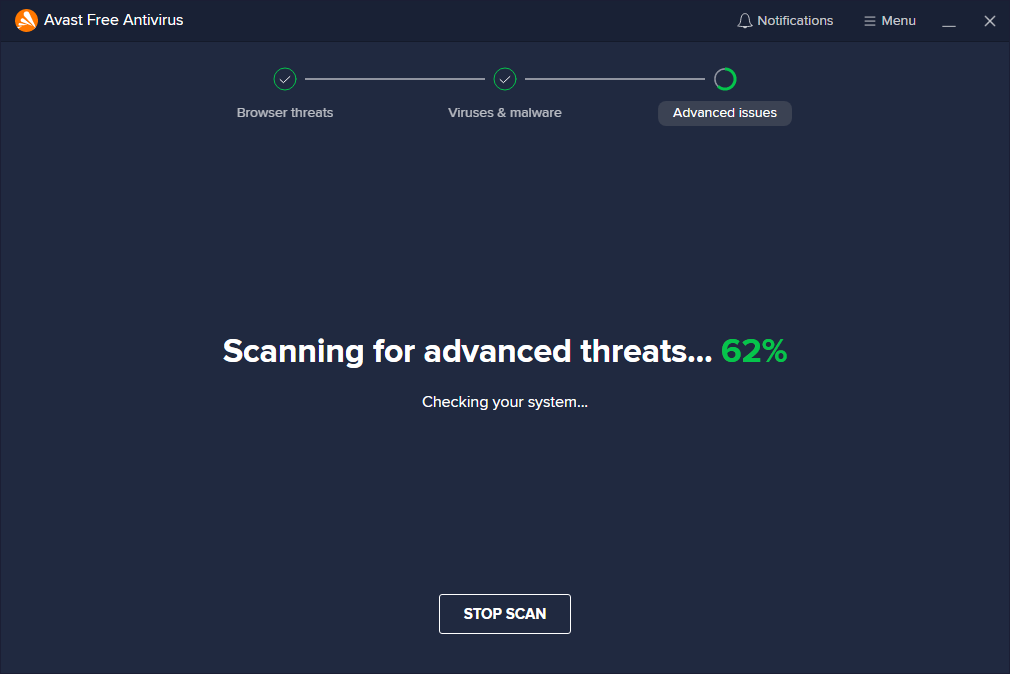


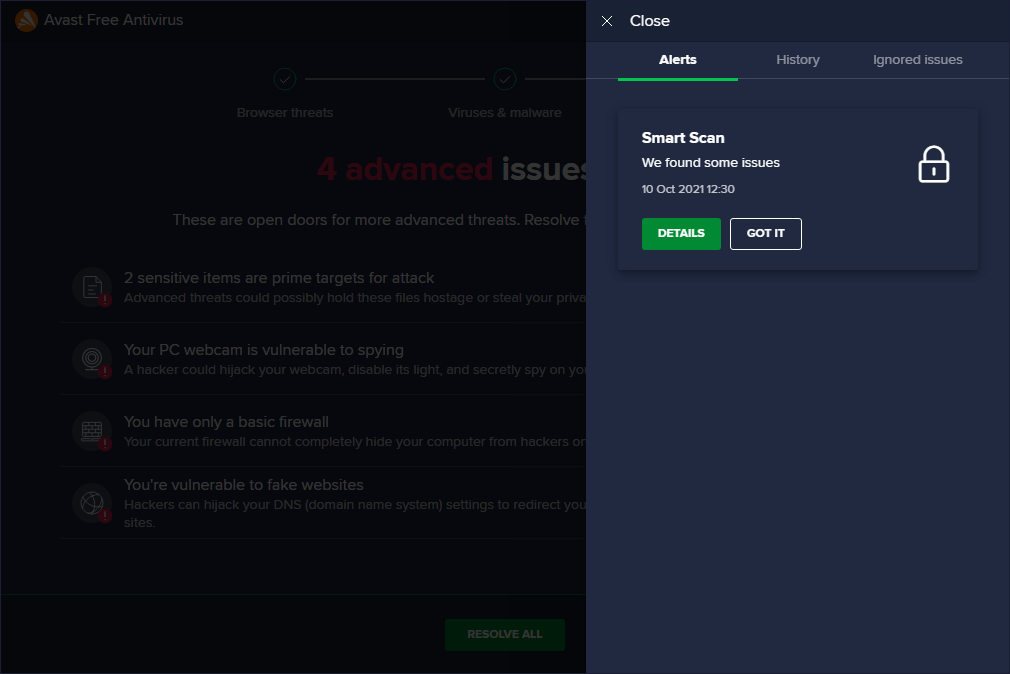
**Scanning for Viruses and Malware:**

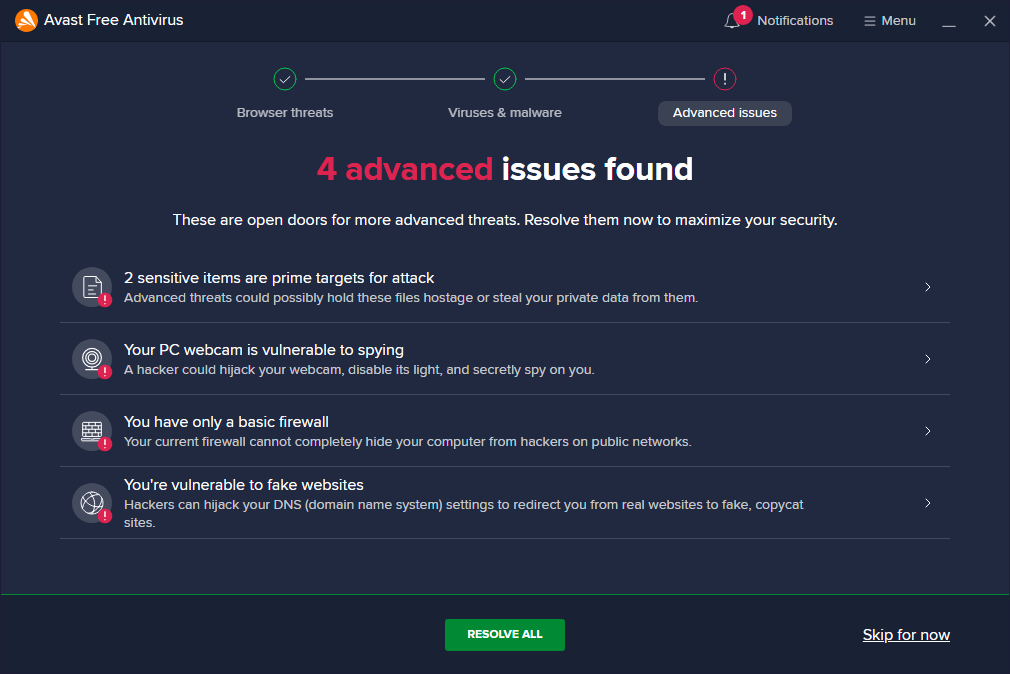


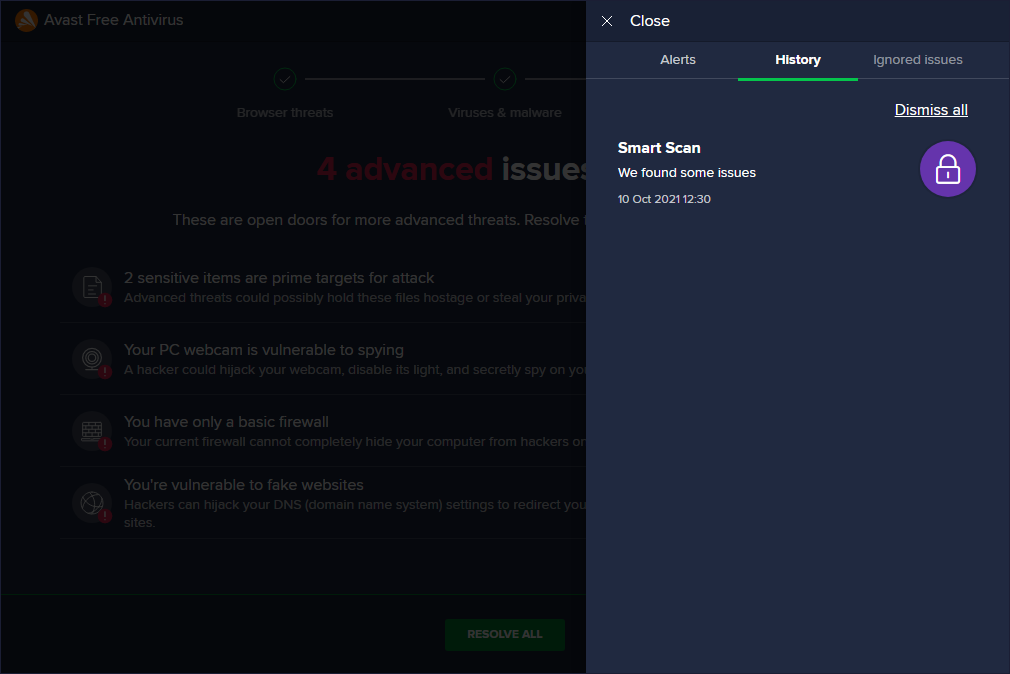


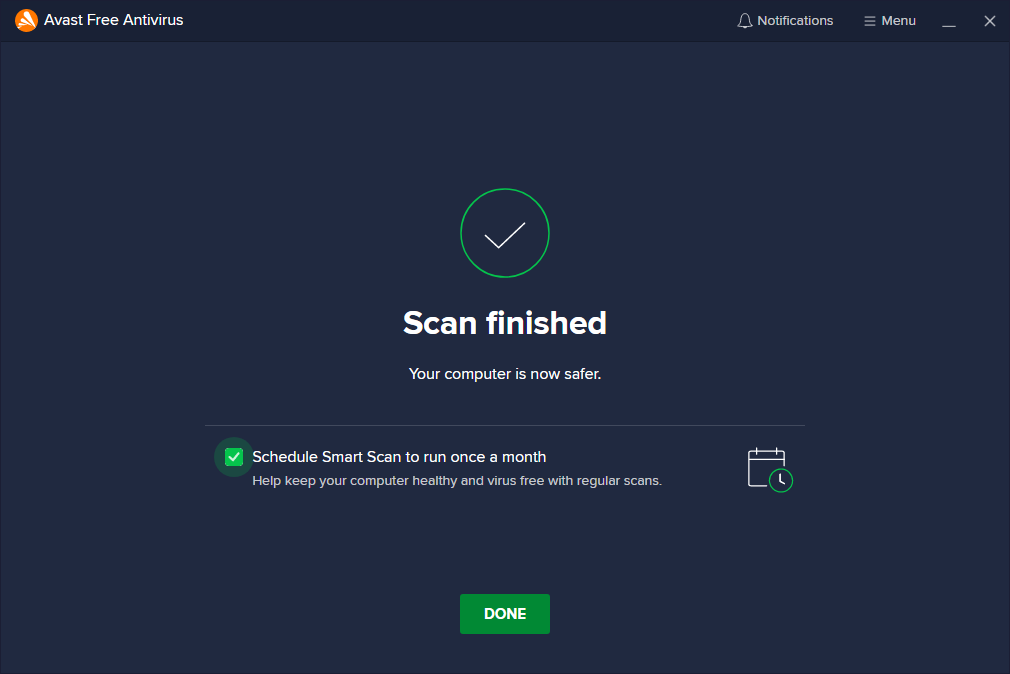
**Scanning for Advanced issues:**











**Reference**

* <https://www.dictionary.com/browse/ransom>[14/10/2021]
* https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time[14/10/2021]
* https://www.mcafee.com/enterprise/en-in/security-awareness/ransomware.html[14/10/2021]
* https://www.datto.com/blog/common-types-of-ransomware[14/10/2021]
* https://umbrella.cisco.com/ransomware-defense-dummies-2nd-edition[14/10/2021]
* https://www.statista.com/statistics/701020/major-operating-systems-targeted-by-ransomware/[14/10/2021]