IS YOUR DEVICE BOTNET FREE?

What is Botnet Attack and it's early sign?

A botnet attack is a large-scale cyber attack carried out by malware-infected devices which are controlled remotely. It turns compromised devices into **'zombie bots'** for a botnet controller. Attackers use botnets to compromise systems, distribute malware and recruit new devices to the attackers. This attack is mainly done for disruption and a means of setting a path to launch a deadly malware attack.

Early signs of a botnet attack can include unusual outbound network traffic, increase in spam emails, and increased number of failed login attempts, strange device behaviour, and unexplained online account lockouts. Monitoring for these indicators can help in early detection and prevention of botnet infiltration.

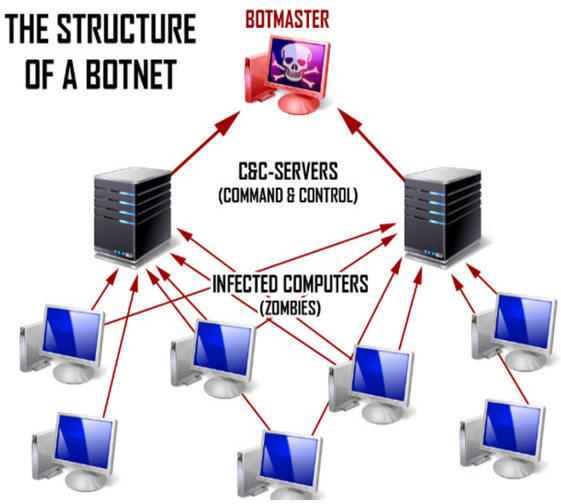

Fig 1. Botnet

Botnet cleaning tools

CERT-In under the Union Govt has released few free tools for monitoring and verification of bots related activities in the digital devices. By using these tools from individuals and organizations can ensure that they are employing reliable and government-approved solutions to safeguard their devices and digital infrastructure. The usage of botnet cleaning tools removes the cyber attack percentage and increases the security of device.

List of the Bot removal tool

*These tools are available in this link **(https://www.csk.gov.in/security-tools.html)** which provides softwares/solutions for below mentioned OS:*

- For Microsoft Windows
- For Android
- For Mobile M-Kavach 2, Developed by C-DAC, Hyderabad

Process of installing the Bot removal tool

- **The process of installing Bot removal for Machines(Desktop/Laptop/etc.)**

Click on the link given in the website => download => Open the file from download of the system => I Accept => Select any one of three type of scan => Select Corrupted file => clean.

➔ It is mandatory to done Complete scanning once in a week for better result and update the application on regular basis.

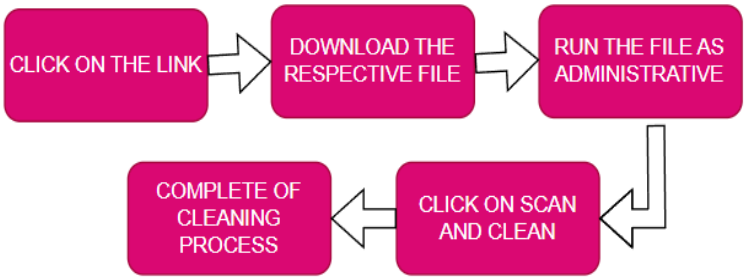

Fig 2. Installation Process

- **The process of installing M-Kavach 2 for Mobile**

M-Kavach 2 is a tool developed by C-DAC, promoted by the Indian Government. Install from Play store => Next(4 times) => Gives permission to the app => Get started => Click on red mark icon as given in fig 2 => scan completes and removal of botnet is automated done if presented in device. Mobile is used and surf a lot on network and can caught botnet from unwanted process too.

➔ For effective security management, it is crucial to ensure that M-Kavach 2 is regularly updated. This app let the user to custom the setting according to their need.

Prevention Techniques for Botnet Attacks

While botnet attacks are a major cybersecurity threat, the good news is that organizations can use many botnet attack prevention techniques, which includes but not limited to the following:

- Deploy sophisticated antivirus and anti malware tools and keep them updated.
- Regularly install updates and bug fixes for software and operating systems.
- Learn how to recognize suspicious emails and attachments and avoid clicking on them.
- Use strong passwords and multi-factor authentication to prevent unauthorized access.

- Impart cyber security training and education programs for employees to understand botnet attacks.

Some tips to prevent your IT environment from becoming the victim of a botnet attack:

- Install cyber security solutions such as firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention System(IPS).
- Monitor network traffic for suspicious activity and unexpected surges in requests.
- Use a DDoS protection tool such as DNS filtering that can help block malicious visits to a website or service.

References:

- https://www.csk.gov.in/security-tools.html
- https://www.k7computing.com/in/k7-bot-removal-tool
- https://www.escanav.com/en/escanav-cert/escanav-cert-intoolkit.asp
- https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/botnet-attack prevention/