

CYBER SWACHHTA BHARAT

INDIA'S ANSWER TO THE BOTNET AND MALWARE ECOSYSTEMS?

साइबर स्वच्छता केन्द्र

CYBER SWACHHTA KENDRA

Botnet Cleaning and Malware Analysis Centre

The Botnet and Malware Ecosystems Fighting Conference - BOTCONF 2023

11-14th April

Presentation on 12th April 2023



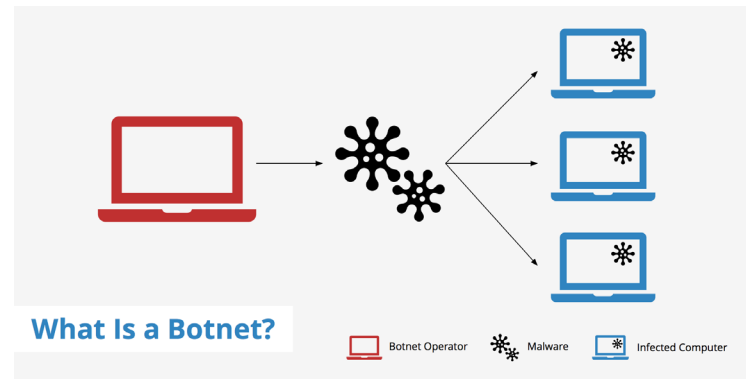
Pratiksha Ashok
UCLouvain, PhD Researcher
pratiksha.ashok@uclouvain.be

OVERVIEW

- Malware and Botnet
- Research question and methodology
- *Cyber Swachhta Kendra*
- Governmental response to malware and botnet
- Arguments for and against such a governmental response
- Takeaway from the Case Study of India

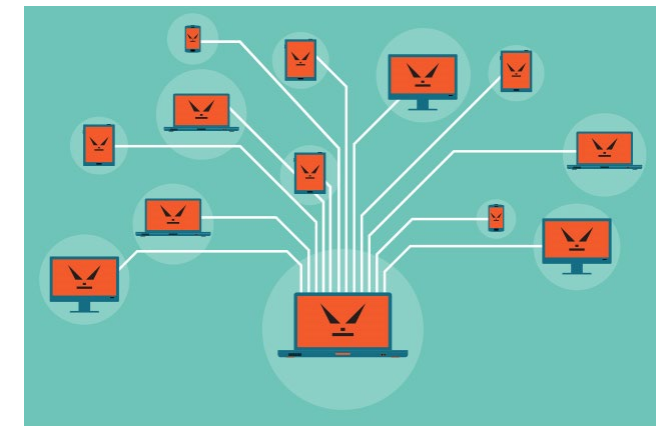


- Malware and Botnet



- Research question and methodology

- Governmental solutions to malware and botnet - should/should not governments resolve such issues?
- Descriptive and Normative analysis- From Economic, Technological and Legal Perspectives



CYBER SWACHHTA KENDRA

- Ministry of Electronics and Information Technology
- Indian Computer Emergency Response Team – 2004
- Swachh Bharat Abhiyan, Clean India Mission - 2014
- *Cyber Swachhta Kendra* – 2017



CYBER SWACHHTA KENDRA

- Reporting Incidents
 - Alerting Users
 - Listing of threats
 - Providing tools for resolving issues
-
- <https://www.csk.gov.in/alerts.html>





साइबर स्वच्छता कन्द्र

CYBER SWACHHTA KENDRA

Botnet Cleaning and Malware Analysis Centre



Ministry of Electronics and
Information Technology
Government of India

- Home
- About Us
- CERT-In
- Security Tools
- Alerts
- Security Best Practices
- Announcements
- Partners
- FAQ's
- Contact Us

Security Tools

Free Bot Removal Tool - For Microsoft Windows

You may use any of the following Bot Removal Tool for your digital device.

Note: To identify, the architecture of your computer system whether it is 32-bit or 64-bit, right click on "My computer"/ "This PC" -> Properties-> Check your system architecture

- eScan Antivirus



The antivirus company **eScan Antivirus** is providing the free bot removal Tool. Click the below mentioned link to download the tool.

<https://www.escanav.com/en/escanav-cert/escanav-cert-intoolkit.asp>

Download

- K7 Security



The antivirus company **K7 Security** is providing the free bot removal Tool. Click the below mentioned link to download the tool.

<https://www.k7computing.com/in/k7-bot-removal-tool>

Download

- Quick Heal



The antivirus company **Quick Heal** is providing the free bot removal Tool. Click the below mentioned link to download the tool.

<https://www.quickheal.co.in/bot-removal-tool>

Download



Free Bot Removal Tool - For Android



The antivirus company **eScan Antivirus** is providing the Smartphone Safety Toolkit. **Click** the below mentioned link or **Scan QR Code** to download the tool.

<https://play.google.com/store/apps/details?id=com.eScanAV.certin>



Free Mobile Security Application - For Android



C-DAC Hyderabad has developed M-Kavach 2 with the support of MeitY. **C-DAC Hyderabad** is providing the Android Mobile Security Application. **Click** the below mentioned link or **Scan QR Code** to download the tool.

https://play.google.com/store/apps/details?id=org.cdac.updatemkavach&hl=en_IN&gl=US



Other Relevant tools:

1. USB Pratirodh

This tool is a desktop security solution, which controls the usage of removable storage media like pen drives, external hard drives, cell phones, and other supported USB mass storage devices.

Download Link:

[USB Pratirodh - \(End point USB mass storage device control solution\)](#)

2. AppSamvid

This tool AppSamvid is a desktop based Application Whitelisting solution for Windows operating system. It allows only preapproved set of executable files for execution.

Download Link:

[AppSamvid - an application whitelisting software](#)

3. Browser JSGuard

This tool is a browser extension which detects and defends malicious HTML & JavaScript attacks made through the web browser based on Heuristics. It alerts the user on visiting any malicious web pages and provides the detailed analysis threat report of the web page. For more details, [click here](#)

Download Link:

- **For Firefox Web Browser:**
<https://addons.mozilla.org/en-US/firefox/addon/browser-jsguard/>
- **For Google Chrome Web Browser:**
<https://chrome.google.com/webstore/detail/browserjsguard/ncpkigeklafkopcelcegambndlhkcbhb>



Alerts

Current Cyber security threats and security measures

Current Threats

- ["MalVirt" Malware Loader](#) NEW
- [Vidar Malware](#)
- [Zerobot](#)
- [Panchan Botnet](#)
- [BlackCat Ransomware](#)
- [SOVA Android Trojan](#)
- [India Ransomware Report \(H1-2022\)](#)
- [Ransomware Advisory](#)
- [Autolykos Malware](#)
- [Black Basta Ransomware](#)
- [Hive Ransomware](#)
- [Escobar Android Malware](#)
- [LockBit 2.0 Ransomware](#)
- [Diavol Ransomware](#)
- [BotenaGo malware](#)
- [REvil aka Sodinikibi Ransomware](#)
- [Crackonosh Cryptocurrency Miner](#)
- [Siloscape Malware](#)
- [Sarbloh Ransomware](#)

ARGUMENTS FOR AND AGAINST A GOVERNMENTAL RESPONSE

Arguments for governmental response

- Economic- healthy digital economy
- Technical- governmental knowhow to resolve issues
- Legal – protect the privacy and prevent misuse of data of users; Paternalistic

Arguments against governmental response

- Economic- Burden on the economy
- Technical- Keep up with the recent developments
- Legal- suggested tools could create monopolies, making governments responsible for actions that are not their own and could be conducted by ISP

TAKE AWAY FROM THE CASE STUDY OF INDIA

- Large and diverse country like India
- The future of Digital India
- Provides options for people who cannot afford private solutions
- Like acts of war- a country should respond



QUESTIONS AND FURTHER INTERACTIONS!

- <https://www.linkedin.com/in/pratiksha-ashok-65b45567/>
- https://twitter.com/Pratiksha_Ashok
- pratiksha.ashok@uclouvain.be

