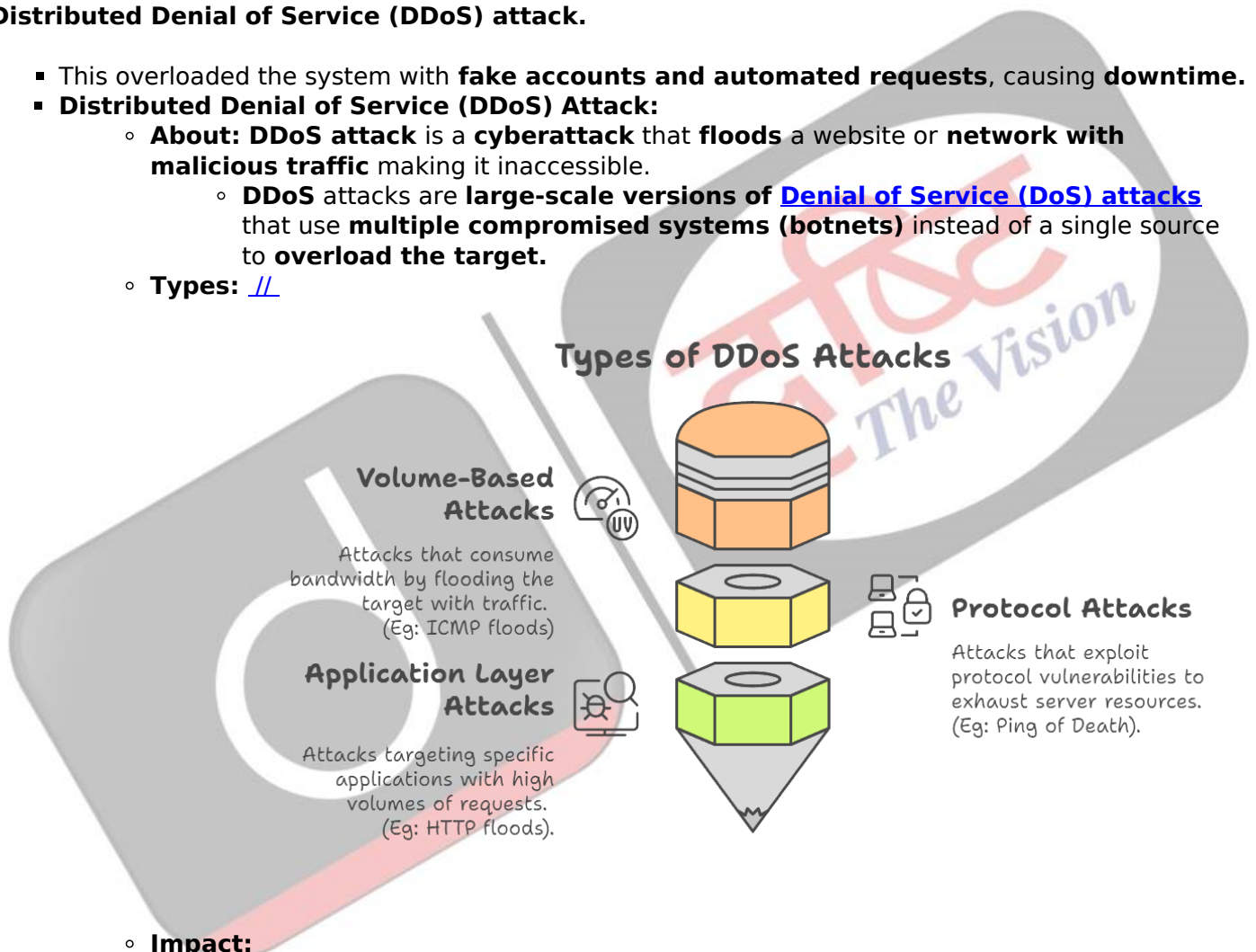# DDoS Cyber-Attack

**Source: TH**

**Karnataka's Kaveri 2.0 portal** that deals with property registration faced severe disruptions due to a **Distributed Denial of Service (DDoS) attack.**

- This overloaded the system with **fake accounts and automated requests**, causing **downtime.**
- **Distributed Denial of Service (DDoS) Attack:**
    - **About: DDoS attack** is a **cyberattack** that **floods** a website or **network with malicious traffic** making it inaccessible.
        - **DDoS** attacks are **large-scale versions of Denial of Service (DoS) attacks** that use **multiple compromised systems (botnets)** instead of a single source to **overload the target.**
    - **Types:** //

## Types of DDoS Attacks

**Volume-Based Attacks**

Attacks that consume bandwidth by flooding the target with traffic. (Eg: ICMP floods)

**Application Layer Attacks**

Attacks targeting specific applications with high volumes of requests. (Eg: HTTP floods).

**Protocol Attacks**

Attacks that exploit protocol vulnerabilities to exhaust server resources. (Eg: Ping of Death).
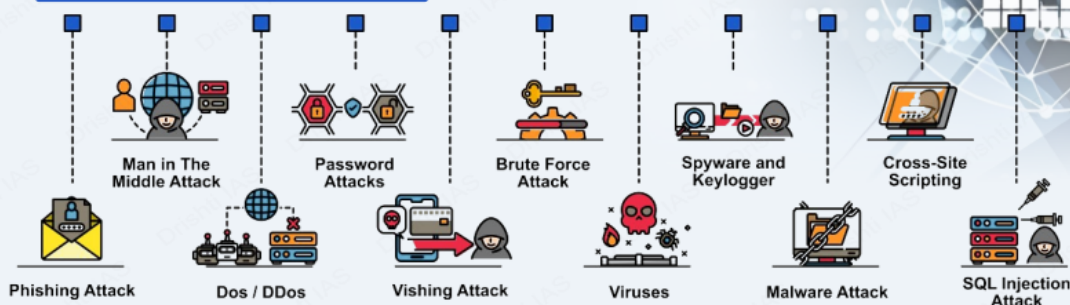
- **Impact:**
    - DDoS attacks **disrupt services, impact revenue,** and expose cybersecurity vulnerabilities, damaging an organization's reputation.
- **Mitigation Strategies**
    - **Traffic filtering, rate limiting, bot detection** (CAPTCHA, behavioral analysis), security audits, incident response plans, and **multi-factor authentication** enhance defense against DDoS attacks.

# CYBER SECURITY

**Cybersecurity refers to any technology, measure, or practice for preventing cyberattacks or mitigating their impact.**

## CYBER SECURITY ATTACKS

- Man in The Middle Attack
- Password Attacks
- Brute Force Attack
- Spyware and Keylogger
- Cross-Site Scripting
- Phishing Attack
- Dos / DDos
- Vishing Attack
- Viruses
- Malware Attack
- SQL Injection Attack

**'Crime in India' Report 2022 (NCRB) highlighted 24.4% surge in cybercrimes in India since 2021.**

## Common Cybersecurity Myths

- Strong passwords alone are adequate protection
- Major cybersecurity risks are well-known
- All cyberattack vectors are contained
- Cybercriminals don't attack small businesses

## Cyber Warfare

- Digital attacks to disrupt vital computer systems, to inflict damage, death, and destruction.

## CYBER THREAT ACTORS

| CYBER THREAT ACTOR | MOTIVATION |
| --- | --- |
| NATION-STATES | GEOPOLITICAL |
| CYBERCRIMINALS | PROFIT |
| HACKTIVISTS | IDEOLOGICAL |
| TERRORIST GROUPS | IDEOLOGICAL VIOLENCE |
| THRILL-SEEKERS | SATISFACTION |
| INSIDER THREATS | DISCONTENT |

## Types of Cybersecurity

- Critical infrastructure security (Robust access controls)
- Network security (Deploying firewalls)
- Application security (Code reviews)
- Cloud Security (Tokenization)
- Information security (Data masking)

## Recent Major Cyber Attacks

- WannaCry Ransomware Attack (2017)
- Cambridge Analytica Data Breach (2018)
- Financial data of 9M+ cardholders, including SBI, leaked (2022)

## Regulations & Initiatives

- **International:**
  - UN Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace
  - NATO's Cooperative Cyber Defense Centre of Excellence (CCDCOE)
  - Budapest Convention on Cybercrime, 2001 **(India not a signatory)**
- **India:**
  - IT Act, 2000 (Sections 43, 66, 66B, 66C, 66D)
  - National Cyber Security Policy, 2013
  - National Cyber Security Strategy 2020
  - Cyber Surakshit Bharat Initiative
  - Indian Cyber Crime Coordination Centre (I4C)
  - Computer Emergency Response Team-India (CERT-In)

## Steps Needed for Cyber Security

- Network Security
- Malware Protection
- Incident Management
- User Education and Awareness
- Secure Configuration
- Managing User Privileges
- Information Risk Management Regime

Drishti IAS

**Read More: Denial of Service (DoS) Attack**