DISTRIBUTED DENIAL OF SERVICE ATTACK : SCIENCE & TECHNOLOGY

NEWS: *What's a DDoS cyberattack that hit Karnataka's Kaveri 2.0 portal?*

WHAT'S IN THE NEWS?

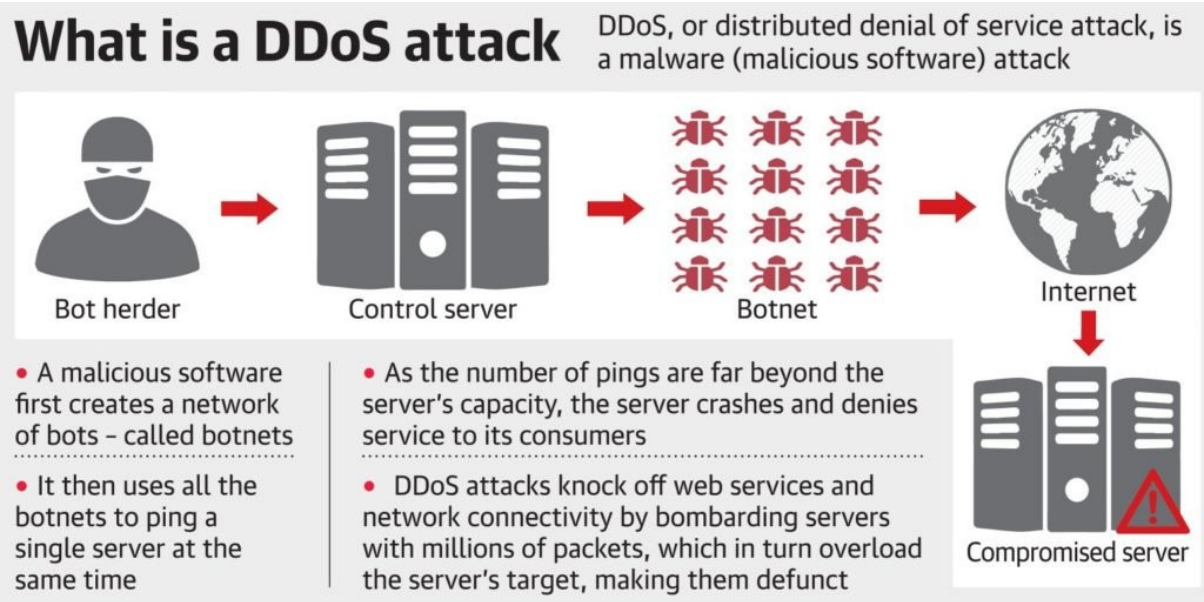
Introduction to the Incident In January 2025, the Kaveri 2.0 portal, Karnataka's revamped platform for property registrations, experienced significant disruptions due to a Distributed Denial of Service (DDoS) attack. This attack utilized automated tools or bots, leading to the creation of fake accounts and entries that overwhelmed the system.

Understanding DDoS Attacks

- **Definition**: A DDoS attack aims to disrupt the normal functioning of a targeted server, service, or network by flooding it with excessive internet traffic.
- **Mechanism**: Unlike single-source Denial of Service (DoS) attacks, DDoS attacks involve multiple compromised devices, known as a botnet, which are used to generate massive amounts of traffic.
- **Target and Tactics**: These attacks can saturate a website's bandwidth, exploit network protocol vulnerabilities, or target specific application weaknesses.

Implications of DDoS Attacks

- **Service Disruption**: Such attacks can cause significant downtime, rendering essential services unavailable and potentially leading to loss of revenue.
- **Secondary Attacks**: Often, DDoS attacks serve as a distraction for more invasive cyber attacks like data breaches.
- **Reputational Damage**: Organizations suffering from DDoS attacks may face reputational harm as stakeholders lose trust in their ability to safeguard against cyber threats.
- **Financial Impact**: The downtime associated with DDoS attacks can result in substantial financial losses, particularly for online-based businesses and services.



Mitigation Strategies

- **Traffic Filtering**: Implementing advanced traffic filtering can help distinguish between legitimate and malicious data packets.
- **Traffic Monitoring**: Utilizing monitoring tools can aid in identifying and mitigating unusual traffic patterns swiftly.
- **Rate Limiting**: This involves setting a cap on the number of requests a user can make within a certain time frame to prevent overload.
- **Bot Detection**: Technologies such as CAPTCHA and behavioral analysis help in detecting and blocking bots.
- **Security Audits**: Regular security checks and robust authentication methods are crucial to enhance the security frameworks of online portals.

Kaveri 2.0 Portal Details

- **Purpose and Launch**: Launched in 2023, Kaveri 2.0 is Karnataka's initiative to streamline the land registration process through a digital platform.
- **Features**: This portal provides users with access to critical information regarding stamp duties, property guidelines, and simplifies the data entry process for registrations, aiming for a quicker and more transparent property registration experience.

The DDoS attack on Kaveri 2.0 underscores the critical need for robust cybersecurity measures, especially for government-operated digital services, to protect against and mitigate the effects of such cyber threats.

Source: **https://www.thehindu.com/sci-tech/technology/whats-a-ddos-cyberattack-that-hit-karnatakas-kaveri-20-portal/article69228797.ece**