Kaveri 2.0 Hacked

Posted at: 19/02/2025

Kaveri 2.0 Hacked: How a DDoS Attack Disrupted Karnataka's Property Portal

What Happened?

In **January 2025**, Karnataka's **Kaveri 2.0** property registration portal stopped working, disrupting **essential citizen services**. At first, officials thought it was a **technical issue**, but later investigations revealed it was a **cyberattack** called a **Distributed Denial of Service (DDoS) attack**.

The **Kaveri 2.0 portal**, launched in **2023**, allows people to **register properties, search for land records, and get encumbrance certificates (ECs)** online. This attack shows how **government websites** are becoming targets for cybercriminals.

What is a DDoS Attack?

A **DDoS (Distributed Denial of Service) attack** is a way for hackers to **overload a website or online service** by sending **huge amounts of traffic**, making it **slow or completely unavailable**.

How Does a DDoS Attack Work?

1. **Hackers take control of many devices** (like computers or infected servers) and turn them into a "botnet."
2. **These devices send an overwhelming number of requests** to a website or server.
3. **The server gets overloaded** and **stops responding to real users**.

Types of DDoS Attacks

- **Flooding the network** – Too much traffic makes the system slow or crash.
- **Exploiting security flaws** – Hackers find weaknesses in a website's setup to cause problems.
- **Targeting a specific service** – Attackers overload certain functions, like searches or logins.

Examples of Major DDoS Attacks

1. Attack on X (Twitter) – August 2024

- **Elon Musk's X platform (formerly Twitter) faced a major DDoS attack.**

- It happened **just before a live conversation between Elon Musk and Donald Trump** (then a presidential candidate).
- The attack **slowed down the platform**, showing how cyberattacks can target important political events.

2. Attack on GitHub – 2015

- Hackers attacked **GitHub**, a website used by developers, using a **botnet linked to China**.
- The attack targeted projects that **helped users bypass internet restrictions in China**.
- Visitors' **browsers were unknowingly used to attack the website**, making it one of the **biggest cyberattacks** of that time.

Impact of DDoS Attacks

1. Websites and Services Stop Working

- People **cannot access important online services**, causing **delays and financial losses**.

2. Attackers Use It as a Distraction

- While people focus on fixing the **DDoS attack**, hackers may **steal data or launch other attacks** in the background.

3. Loss of Trust

- If **government or business websites** keep getting attacked, people **lose confidence** in their safety and reliability.

How Did the DDoS Attack Affect Kaveri 2.0?

The attack **overloaded the portal** by sending **huge numbers of fake search requests**, making it **slow or completely unusable**.

Key Facts About the Attack:

- **Hackers used 62 email accounts and 14 IP addresses** to launch the attack.
- The biggest problem was with the **Encumbrance Certificate (EC) search function**.
- The attack **increased traffic by 8 times the normal level**, overwhelming the system.
- Within **2 hours**, the system received **6.2 lakh fake requests**, preventing real users from accessing it.

Consequences of the Attack:

- **Property registrations were delayed**, causing issues for people buying or selling land.
- **Government services were disrupted**, affecting thousands of users.
- **The portal was fixed on February 5**, but the attack **exposed weaknesses** in its security.

How Can We Prevent DDoS Attacks?

1. Detect and Block Fake Traffic

- Use **advanced filters** to tell real users apart from bots.

2. Monitor Traffic in Real Time

- **Detect unusual activity early** and stop attacks before they cause damage.

3. Limit Requests Per User

- Stop users from **sending too many requests in a short time**.

4. Use CAPTCHA and Bot Detection

- Prevent bots from accessing key services.

5. Strengthen Security and Perform Regular Audits

- **Update security settings** and **check for vulnerabilities** regularly.

6. Work with Cybersecurity Experts

- Governments and businesses should **partner with cybersecurity firms** to improve protection.

7. Educate Users About Cyber Threats

- **Train employees and users** to recognize phishing and other cyber threats.

8. Have a Quick Response Plan

- If an attack happens, a **dedicated cybersecurity team** should **respond immediately** to minimize damage.

Conclusion

The **DDoS attack on Kaveri 2.0** is a **warning sign** about the **increasing risks of cyberattacks** on important government websites. As India continues to **go digital**, cybersecurity **must be a top priority**.

Stronger security measures, better monitoring, and public awareness are essential to **protect critical services** from future cyber threats.