CYBER THREAT TREND ANAYSIS

Understanding Global Cybersecurity Threats (2015-2024)

About the Dataset: A Decade of Cyber Insights

Comprehensive Data

Over 3000 records of cyberattacks, malware types, and targeted industries.

Global Scope

Tracking incidents across various countries from 2015 to 2024.

Key Metrics

Includes data breached (GB), financial impact ($M), and response times.

Strategic Value

Enhances threat intelligence, trend forecasting, and ML model development.

KEY DATA POINTS FOR ANALYSIS

1. **Country**
   Geographic location of attacks.

2. **Year**
   Temporal distribution of incidents.

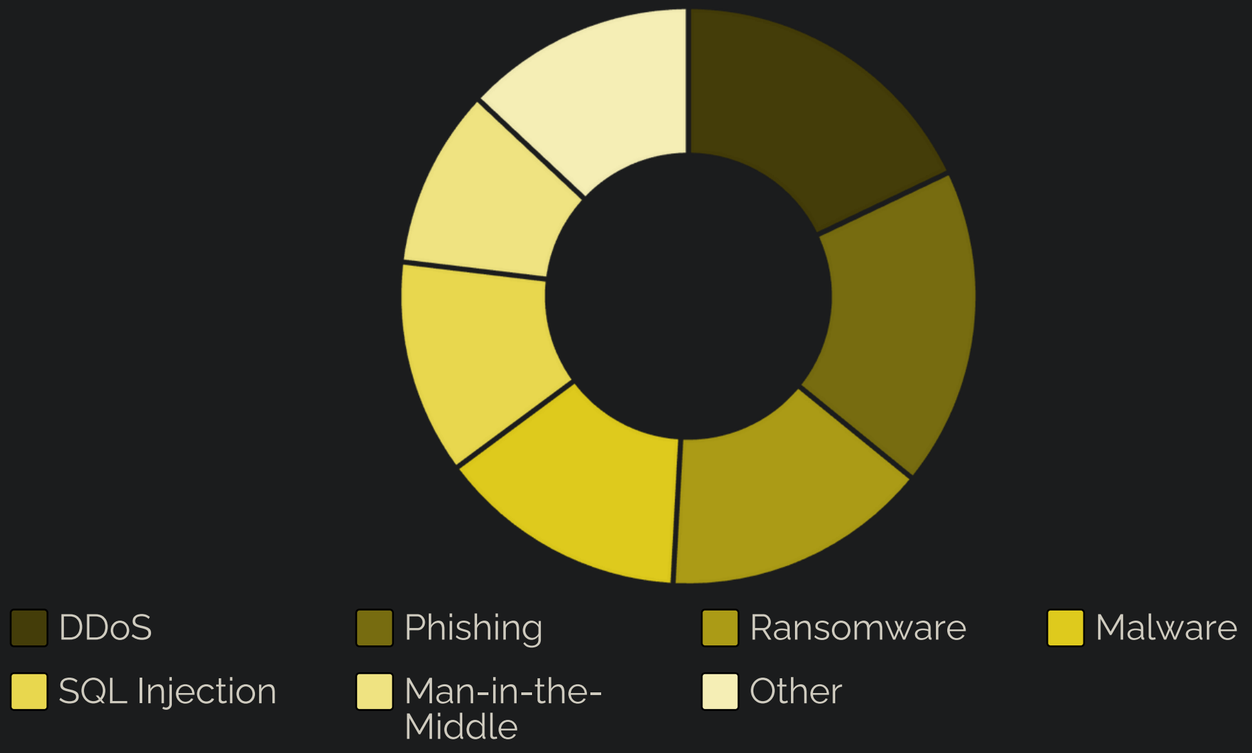
3. **Threat Type**
   Malware, DDoS, Phishing, Ransomware.

4. **Attack Vector**
   Methods like SQL Injection, Social Engineering.

5. **Affected Industry**
   Finance, Healthcare, IT, Retail, Government.

6. **Financial Impact**
   Estimated losses in millions of dollars.

Top Threat Types: A Closer Look



Distributed Denial of Service (DDoS)

Overwhelming systems to disrupt service availability.

Phishing

Deceptive communications to steal credentials.

Ransomware

Encrypting data for financial extortion.

INDUSTRIES UNDER SIEGE

Banking & Finance

High-value targets, sensitive data.

Information Technology

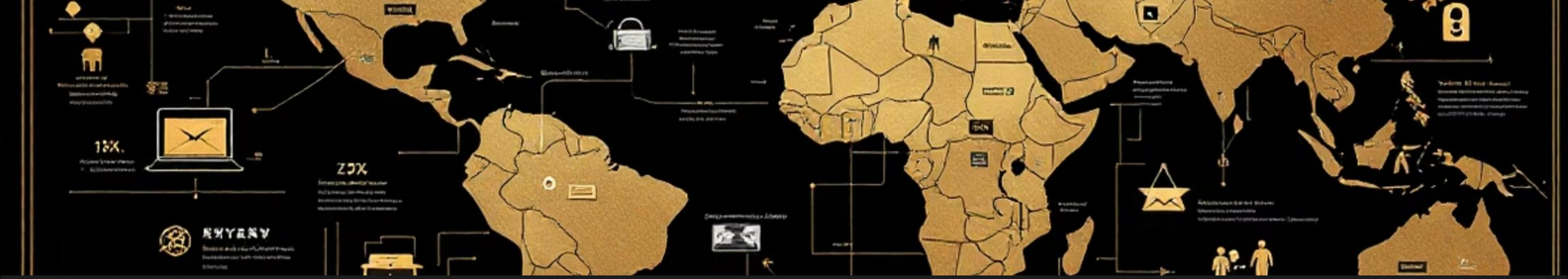
Critical infrastructure, intellectual property.

Healthcare

Personal health information, patient data.

Government

National security, citizen data.



Attack Sources & Vulnerabilities

Primary Attack Sources

- **Nation-state Actors:** 26% — Sophisticated, state-sponsored attacks.
- **Hacker Groups:** 20% — Organized criminal entities.
- **Insiders:** 15% — Threats from within the organization.
- **Unknown:** 26% — Undetermined origins, complex attribution.

Common Vulnerability Types

- **Zero-Day Exploits:** 26% — Unpatched, unknown vulnerabilities.
- **Social Engineering:** 25% — Manipulating individuals for access.
- **Weak Passwords:** 18% — Easily compromised authentication.
- **Unpatched Software:** 16% — Exploiting known security flaws.

Defense Mechanisms & Incident Response

Firewall Implementation

First line of defense against unauthorized access.

Antivirus Protection

Detecting and removing malicious software.

VPN Utilization

Securing network communications and data.

AI-Based Detection

Advanced threat identification and response.

Average incident resolution time: 1-72 hours, with continuous improvement efforts.

Looking Ahead: The Future of Cyber Resilience

The Global Cybersecurity Threats Dataset offers crucial insights for proactive defense.

1

Data-Driven Strategies

Leveraging historical data for predictive analytics.

2

Enhanced Collaboration

Sharing threat intelligence across sectors and nations.

3

Continuous Adaptation

Evolving defenses to counter emerging threats.