Cybersecurity Threat Intelligence Report (2024–2025)

Threat Report – Awareness & Research Project (Task-1)

Internship Program: Cybersecurity & Ethical Hacking

Prepared By: *Vishvjeet*

Role: Cybersecurity Analyst Intern

Organization: Maincrafts Technology

Year: 2025

Table of Contents

1. Introduction to Cybersecurity
2. Major Modern Cyber Threats
    2.1 AI-Powered Phishing Attacks
    2.2 Ransomware-as-a-Service (RaaS)
    2.3 Cloud Security Misconfigurations
    2.4 IoT Vulnerabilities
    2.5 Zero-Day Exploits
3. Impact Analysis
4. Real-World Case Studies
5. Preventive Measures
6. Conclusion & Future Scope
7. References

1. Introduction to Cybersecurity

What is Cybersecurity?

- Cybersecurity refers to the practice of protecting computer systems, networks, applications, and data from digital attacks. These attacks are often intended to access, change, or destroy sensitive information, extort money from users, or disrupt normal business operations.

Why is Cybersecurity Important?

- In today's digital world, individuals and businesses heavily depend on technology for communication, banking, healthcare, education, and operations. Cyberattacks can lead to financial losses, identity theft, data breaches, reputational damage, and legal penalties. Strong cybersecurity ensures confidentiality, integrity, and availability of information.

Current Relevance (2024–2025)

- Cybercrimes are increasing rapidly due to digital transformation, cloud adoption, remote work, and AI-driven technologies. Attackers now use automation, artificial intelligence, and sophisticated tools to bypass traditional security controls. Therefore, understanding modern threats and defence strategies is critical.

---

2. Identify 5 Major Modern Cyber Threats

2.1 AI-Powered Phishing Attacks

- AI-powered phishing uses artificial intelligence to craft highly convincing emails, messages, voice calls, and deepfake videos. These attacks impersonate trusted individuals or organizations to steal credentials and financial information.

Key Characteristics:

- Personalized phishing emails
- Deepfake voice/video scams
- Social engineering using AI chatbots

2.2 Ransomware-as-a-Service (RaaS)

- RaaS allows cybercriminals to purchase or rent ransomware tools without technical knowledge. Attackers encrypt victims' data and demand ransom for decryption keys.

Key Characteristics:

- Subscription-based ransomware kits
- Double extortion (data theft + encryption)
- Targeting enterprises and healthcare sectors

2.3 Cloud Security Misconfigurations

- Cloud platforms like AWS, Azure, and GCP can be misconfigured, exposing sensitive data to the public internet. This is one of the leading causes of data breaches.

Key Characteristics:

- Publicly accessible storage buckets
- Weak access control policies
- Improper identity and access management (IAM)

2.4 IoT Vulnerabilities

- Internet of Things (IoT) devices such as smart cameras, routers, wearables, and home appliances often lack proper security controls, making them easy targets.

Key Characteristics:

- Default passwords
- Outdated firmware
- Poor encryption

2.5 Zero-Day Exploits

- Zero-day exploits target unknown or unpatched software vulnerabilities. Since no fix exists initially, attackers can exploit systems before detection.

Key Characteristics:

- No available security patch
- High-value targets
- Used in advanced persistent threats (APTs)

---

3. Impact Analysis

Impact on Individuals

- Identity theft and financial fraud
- Loss of personal data and privacy
- Unauthorized access to accounts

Impact on Organizations

- Business downtime and financial losses
- Reputation damage and customer trust loss
- Legal and compliance penalties
- Intellectual property theft

4. Real-World Case Studies

AI-Powered Phishing – Deepfake Scams (2024)

- In 2024, attackers used AI-generated voice deepfakes to impersonate company executives, tricking employees into transferring large sums of money.

Ransomware – WannaCry Attack

- The WannaCry ransomware attack affected over 200,000 systems globally by exploiting unpatched Windows systems, causing massive disruption.

Cloud Misconfiguration – Capital One Breach

- In 2019, Capital One suffered a data breach due to a misconfigured cloud firewall, exposing sensitive customer data stored in AWS.

IoT Attack – Mirai Botnet

- The Mirai malware exploited insecure IoT devices to launch massive DDoS attacks, disrupting major websites and services.

Zero-Day Exploit – SolarWinds Attack

- In 2020, attackers exploited a zero-day vulnerability in SolarWinds software, compromising multiple government and private organizations.

5. Preventive Measures

Against AI-Powered Phishing

- Multi-Factor Authentication (MFA)
- Employee security awareness training
- Email filtering and AI-based detection tools

Against Ransomware

- Regular data backups
- Patch management
- Endpoint Detection and Response (EDR)

Against Cloud Misconfigurations

- Secure IAM policies
- Regular cloud security audits
- Cloud Security Posture Management (CSPM)

Against IoT Vulnerabilities

- Change default credentials
- Regular firmware updates
- Network segmentation

Against Zero-Day Exploits

- Intrusion Detection Systems (IDS/IPS)
- Threat intelligence feeds
- Zero Trust security model

6. Conclusion & Future Scope

Cybersecurity threats are evolving rapidly with advancements in AI, cloud computing, and automation. Organizations must adopt proactive security strategies, continuous monitoring, and regular training to defend against modern cyber threats. Continuous learning and adaptation are essential, as attackers constantly innovate new attack techniques.

Future cybersecurity professionals must stay updated with emerging technologies, threat intelligence, and security best practices to protect digital assets effectively.

---

7. References

- OWASP Top 10 – https://owasp.org
- CISA Cyber Alerts – https://www.cisa.gov
- IBM Security Blog – https://www.ibm.com/security
- Krebs on Security – https://krebsonsecurity.com
- Verizon Data Breach Investigations Report