Cybersecurity Threat Intelligence Report (2024–2025)

Internship Program: Cybersecurity Analyst Intern (Simulation)

Task: Threat Intelligence Report – Task 1

Name: Anusmita Majhi

INTRODUCTION TO CYBERSECURITY

Cybersecurity is the discipline dedicated to defending computers, networks, and data from unauthorized access, attacks, and damage.

As global dependence on digital systems grows, cybersecurity becomes crucial for protecting financial data, privacy, intellectual property, national security, and business continuity.

The relevance of cybersecurity has surged in 2024–2025 due to AI-generated attacks, sophisticated malware, supply chain exploitation,

cloud adoption, and the explosive growth of IoT devices. Attackers are now leveraging automation and deepfake tools, reducing the skill barrier and increasing threat frequency.

MAJOR MODERN CYBER THREATS (2024–2025)

1. AI-POWERED PHISHING ATTACKS

These attacks use artificial intelligence to craft highly convincing phishing emails, cloned websites, and deepfake audio/video.

AI gathers information from social media, breached data, and public records to create personalized messages that bypass human suspicion.

2. RANSOMWARE-AS-A-SERVICE (RaaS)

RaaS is a subscription-based cybercrime model where attackers rent ransomware kits. It allows even unskilled criminals to launch attacks.

The economic impact of RaaS has grown sharply, targeting hospitals, banks, and government systems.

3. CLOUD SECURITY MISCONFIGURATIONS

Misconfigured storage buckets, weak IAM policies, open ports, publicly exposed databases, and incorrect firewall rules lead to massive data leaks.

Rapid cloud migration has created gaps between deployment and security governance.

4. IoT VULNERABILITIES

IoT devices often ship with weak default passwords, outdated firmware, hardcoded credentials, and insecure communication protocols.

Attackers exploit these weaknesses to gain control of smart home devices, CCTV systems, and industrial IoT machinery.

5. ZERO-DAY EXPLOITS

Zero-days are vulnerabilities unknown to software vendors. Attackers exploit them before patches exist, making them extremely dangerous.

Zero-days are often used in espionage operations and supply-chain attacks.

IMPACT ANALYSIS

Impact on Individuals:

- Identity theft through stolen credentials.

- Unauthorized bank transactions and financial loss.

- Personal photos, chats, and location data leaked.

- Extortion through hacked accounts.

Impact on Organizations:

- Large-scale data breaches and financial penalties.

- Loss of intellectual property and trade secrets.

- Operational downtime, frozen systems, and halted services.

- Violations of compliance laws (GDPR, HIPAA, PCI-DSS).

REAL-WORLD CASE STUDIES

AI Phishing Case (2024):

A European company lost $25 million after deepfake voice phishing convinced an employee to transfer money.

AI-generated audio mimicked the CFO’s voice with high accuracy.

WannaCry Ransomware (2017):

Used NSA-leaked EternalBlue exploit, infected 230,000 devices, and disrupted hospitals, telecom networks, and transport systems.

Capital One Cloud Breach (2019):

A misconfigured AWS firewall exposed data of 100 million users, including SSNs and bank account numbers.

Mirai IoT Botnet (2016):

Compromised thousands of IoT devices and launched a historic DDoS attack that shut down major websites.

SolarWinds Zero-Day Attack (2020):

Hackers inserted malicious code into SolarWinds Orion updates, compromising U.S. government systems and global corporations.

PREVENTIVE MEASURES

AI Phishing Defenses:

- MFA to block account takeover.

- AI-based anomaly detection.

- Employee phishing simulation training.

RaaS Defenses:

- Frequent patching of systems.

- Offline, encrypted data backups.

- Network segmentation to contain infection.

Cloud Security Measures:

- Automated vulnerability scanning.

- Zero Trust Architecture.

- Strong IAM with least-privilege access.

IoT Security Strategy:

- Change default credentials immediately.

- Regular firmware updates.

- Isolated IoT network separate from main network.

Zero-Day Defense:

- Deploy IDS/IPS for anomaly detection.

- Threat hunting teams within SOC.

- Continuous monitoring of attack indicators.

DIAGRAMS (TEXT-BASED)

1. Zero Trust Architecture (Simplified)

User → Authentication → Authorization Check → Micro-Segmented Resource Access

2. Cloud Misconfiguration Attack Path

Misconfigured Bucket → Unauthorized Access → Data Exfiltration → Public Leak

3. Ransomware Infection Flow

Phishing Email → Malware Execution → File Encryption → Ransom Demand

CONCLUSION & FUTURE SCOPE

Cyber threats are evolving rapidly, driven by AI, automation, and expanding digital ecosystems.

A proactive security strategy is essential to protect individuals and organizations from catastrophic impacts.

Future cybersecurity will rely heavily on AI-driven defense, Zero Trust models, continuous monitoring, and workforce upskilling.

Continuous learning is critical because attackers constantly change tactics. Organizations that invest in cybersecurity awareness,

modern security tools, and strong governance will remain resilient in the ever-evolving threat landscape.

REFERENCES

- CISA Cyber Alerts

- OWASP Official Documentation

- IBM Security Intelligence Reports

- KrebsOnSecurity Articles

- Public breach reports and verified security case studies