CYBERSECURITY INTERNSHIP

Task 1 – Threat Intelligence Report

By: Akanksha Mane

Abstract:

The rapid digital transformation of global industries, accelerated cloud adoption, and the increasing use of AI-driven technologies have significantly expanded the modern cyberattack surface. As a Cybersecurity Analyst Intern, this Threat Intelligence Report examines five major cyber threats dominating the 2024–2025 landscape ransomware, phishing and social engineering, supply chain attacks, advanced persistent threats (APTs), and cloud security vulnerabilities. The report provides an in-depth analysis of their operational, financial, and national security impacts, supported by real-world case studies such as the Change Healthcare attack, XZ Utils backdoor incident, Cloudflare intrusion attempt, Snowflake data breaches, and supply chain compromises affecting critical infrastructure.

Additionally, the report highlights how these threats continue to evolve through advanced techniques such as double extortion, AI-driven phishing, and exploitation of misconfigured cloud environments. Comprehensive preventive measures are outlined, including Zero Trust security models, MFA deployment, vendor risk management, threat intelligence integration, and cloud-native security controls. The report concludes with insights into future trends such as quantum-resistant encryption, AI-enabled defense systems, and global cybersecurity collaboration which will shape the next generation of cyber resilience. This work underscores the urgent need for proactive, multilayered defense strategies to safeguard digital ecosystems in an increasingly complex threat landscape.

TABLE OF CONTENTS

INTRODUCTION TO CYBERSECURITY

1.1. What is Cybersecurity?

Cybersecurity refers to the collection of technologies, processes, and practices designed to protect digital systems, networks, devices, and data from unauthorized access, disruption, damage, or misuse. It encompasses multiple layers of defense across information technology environments, including hardware, software, cloud systems, and user interfaces. As modern societies increasingly rely on interconnected digital infrastructures ranging from critical services such as transportation, healthcare, and finance to personal communication and e-commerce, the importance of cybersecurity has grown significantly. Cybersecurity aims to ensure the confidentiality, integrity, and availability of information, commonly known as the CIA triad, by mitigating threats such as malware, ransomware, phishing, data breaches, and insider attacks. It integrates disciplines such as cryptography, network, security, application security, incident response, and risk management to provide comprehensive protection. Moreover, cybersecurity is not limited to technical safeguards; it also involves organizational policies, regulatory compliance, continuous monitoring, and user awareness to build a holistic security posture. In essence, cybersecurity plays a critical role in maintaining trust in digital systems, safeguarding sensitive information, and ensuring the resilience of modern technological ecosystems against an evolving landscape of cyber threats.

1.2. Why is it important for individuals and businesses?

Importance for Individuals:

Cybersecurity is essential for individuals because it protects their personal information, digital identity, and online activities in an increasingly connected world. As people rely heavily on online banking, shopping, social media, and cloud storage, the risk of exposure to cyber threats such as phishing, identity theft, ransomware, and fraudulent transactions has grown significantly. A lack of cybersecurity awareness or protective measures can lead to severe consequences, including financial losses, compromised personal data, and long-term identity misuse. Therefore, strong cybersecurity practices enable individuals to maintain privacy, ensure safe online interactions, and protect themselves from evolving cyber risks.

Importance for Businesses

For businesses, cybersecurity is a critical component of opertional resilience and long term sustainability. Organizations manage large volumes of sensitive data such as customer records, intellectual property, financial details, and strategic plans which makes them prime targets for cyberattacks. A single breach can result in catastrophic outcomes, including financial loss, service outages, reputational damage, legal penalties, and loss of stakeholder trust. As companies increasingly adopt digital technologies, cloud platforms, and remote work environments, their attack surface expands, requiring robust security strategies and continuous monitoring. Cybersecurity ensures the confidentiality, integrity, and availability of business systems, enabling organizations to operate securely, comply with legal standards, and safeguard their digital assets.

1.3. Current Relevance (2024 – 2025 trends)

In 2024 and 2025, cybersecurity has gained heightened importance globally as cyber threats have surged in frequency, sophistication, and impact driven by technological changes (such as cloud migration and widespread use of generative AI), evolving attacker strategies, and the increasing value of digital data. Several recent trends illustrate why cybersecurity remains not only relevant but essential for individuals, businesses, and critical infrastructure.

- **Ransomware & Malware Attacks Rising:** In 2024, about 59% of organizations globally experienced a ransomware attack. Ransomware continued to escalate in 2025 with early year data showing a sharp uptick in incidents year-over-year.

- **Data Breach Costs at Historic Highs:** The average cost of a data breach globally reached approximately US $4.88 million in 2024 – the highest recorded thus far, representing a marked increase over previous years. Data breaches are no longer rare or minor events, but major risks with financial, legal, and reputational consequences.

- **Human & Social Engineering Threats Escalating:** A significant portion of breaches now stern from human error, credential theft, or social engineering rather than purely technical exploits. As organizations and individuals increasingly rely on cloud services, remote access, and online collaboration tools, vulnerabilities related to identity and access management have become more pronounced.

- **New Attack Surfaces from Cloud, Remote Work, and AI:** The shift to cloud-native architectures and remote work accelerated by global digital transformation has

expanded the attack surface for many organizations. Cloud-targeted attacks, API vulnerabilities, misconfigurations, and insecure remote access have become common entry points. At the same time, the rise of generative AI tools has introduced both new threats (e.g., deepfakes, AI-driven phishing, automated vulnerability exploitation) and new defense opportunities.

- **Widespread Recognition of Cyber Risk Among Organizations:** According to a recent global survey, about 72% of organizations report that cyber risk has increased — a clear sign that cybersecurity is no longer a niche IT concern but a core part of strategic risk management and business continuity planning. Many companies have begun prioritizing security, adopting advanced frameworks (e.g., zero-trust models), and diversifying their security strategies to avoid relying on a single vendor or outdated tools.

- **Growing Talent Gaps and Need for Skilled Cybersecurity Professionals:** As threats evolve rapidly, there is a global shortage of skilled cybersecurity professionals estimated to be in the millions making it harder for organizations to build and maintain strong security postures. The scarcity of qualified personnel increases the risk of misconfiguration, undetected vulnerabilities, and delayed incident response — all of which amplify the consequences of cyberattacks.

Given these developments, cybersecurity in 2024–2025 is not a theoretical or optional concern it is a real, pervasive, and evolving necessity. With cyberattacks becoming more frequent, varied, and damaging, robust cybersecurity strategies are vital to protect data integrity, maintain trust, ensure business continuity, and safeguard national infrastructure.

FIVE MAJOR MODERN CYBER THREATS

1. Ransomware Attacks

Ransomware remains one of the most significant threats to organizations, targeting sensitive data and critical infrastructure. Attackers encrypt files and demand ransom, often in cryptocurrency, to restore access. Modern ransomware campaigns are highly sophisticated, using social engineering and exploiting unpatched vulnerabilities.

- Exploits vulnerabilities in outdated software and operating systems.
- Delivered via phishing emails, malicious attachments, and compromised websites.
- Can halt critical operations in healthcare, transportation, and government sectors.
- Double extortion: attackers exfiltrate data before encryption to threaten leaks.
- Defense: Regular backups, endpoint detection, security awareness training, and timely patch management.

2. Phishing & Social Engineering

Phishing attacks manipulate users into revealing sensitive information, such as login credentials of financial data. These attacks have evolved to include sophisticated spear-phishing campaigns targeting specific individuals or departments.

- Often delivered through email, instant messaging, or social media
- Spear-phishing uses personal information for higher success rates
- Can lead to credential theft, financial fraud, and unauthorized network access
- Defense: Multi-factor authentication (MFA), employe training, anti-phishing solutions, and email filtering.

3. Supply Chain Attacks

Supply chain attack compromise third-party software, hardware, or service providers to infiltrate the main organization. These attacks have grown due to the interconnectedness of modern IT ecosystems.

- Exploit vulnerabilities in trusted vendors systems
- Can remain undetected for months, impacting multiple organizations simultaneously
- Examples include compromised software updates or third-party libraries
- Defense: Vendor risk assessment, code integrity verification, continuous monitoring, and strict access controls

4. Advanced Persistent Threats

APTs are prolonged and targeted attacks, usually conducted by well-funded cybercriminal groups or nation-states. They aim to steal intellectual property, sensitive data, or disrupt operations without immediate detection.

- Often involve multiple stages: reconnaissance, intrusion, lateral movement, and exfiltration
- Use zero-day vulnerabilities and custom malware to avoid detection
- Target critical sectors like defense, finance, and energy
- Defense: Network segmentation, threat intelligence sharing, continuous monitoring, and anomaly detection systems

5. Cloud Security Threats

With widespread cloud adoption, attackers increasingly exploit misconfigured cloud services and insecure APIs to access sensitive data. Cloud environments require specialized security strategies due to shared responsibility between providers and clients.

- Common issues include misconfigured storage, insecure endpoints, and weak authentication
- Attacks can lead to data breaches, service disruption, and financial loss
- Insider threats and third-party access also increased risk
- Defense: Strong identity and access management, encryption, continuous security audits, and cloud security posture management (CSPM) tools.

IMPACT ANALYSIS

Cyber threats in 2024–2025 have grown more sophisticated, targeting critical infrastructure, cloud environments, and global supply chains. Their impact is not limited to financial loss but extends to operational disruption, legal consequences, and reputational damage. Below is a detailed impact analysis of the five major cyber threats.

1. Impact of Ransomware Attacks

Ransomware attacks can cripple an organization within minutes by locking up essential systems and demanding ransom payments. Modern double and triple-extortion techniques increase the pressure on victims and reduce recovery options.

Key Impacts:

- Operational Shutdown: Critical services (healthcare, energy, public transport) face downtime ranging from hours to weeks.
- Financial Losses: Costs include ransom payments, system restoration, forensic analysis, and lost revenue
- Data Breaches: Exfiltrated data may be leaked or sold on darknet markets.
- Reputational Damage: Loss of customer trust and long-term brand damage.
- Regulatory Penalties: Failure to protect data may result in fines under GDPR, CCPA, etc.

2. Impact of Phishing and Social Engineering

Phishing remains the most common entry point for cyberattacks because it exploits human error rather than technical flaws. Successful phishing can expose sensitive data or serve as the initial step in larger attacks like ransomware.

Key Impacts:

- Credential Theft: Unauthorized access to email, banking, and corporate systems.
- Financial Fraud: Direct monetary losses through fraudulent transactions.
- Business Email Compromise: Attacker impersonate executives to authorize fake payments.
- Unauthorized Network Access: Attackers gain footholds for deeper intrusions (APTs).
- Privacy Violations: Personal information exposure leads to identity theft.

3. Impact of Supply Chain Attacks

Supply chain attacks compromise trusted vendors, allowing attackers to bypass strong internal security. As organizations increasingly rely on third-party software and services, the impact becomes widespread and difficult to detect.

Key Impacts:

- Large Scale Breaches: A single compromised vendor can affect thousands of organizations.
- Loss of Software Integrity: Attackers can inject malicious code directly into software updates.
- Long Term Undetected Presence: Attackers may remain in the network for months (like SolarWinds)
- Financial & Legal Risks: Companies are liable for breaches caused by third-party providers.
- Disruption of Critical Infrastructure: Impacts in sectors like government energy, logistics, and finance.

4. Impact of Advanced Persistent Threats (APTs)

APTs are extremely dangerous because they are stealthy, persistent, and often backed by nation-states. Their goal is long-term access, espionage, or disruption.

Key Impacts:

- Intellectual Property Theft: Loss of trade secrets, R&D data, and proprietary methods.
- National Security Risks: Defense, aerospace, and energy sectors are frequently targeted.
- Prolonged Data Exfiltration: Continuous theft of sensitive information over months or years.
- System Manipulation: Attackers may alter data or compromise system integrity without detection.
- Large-Scale Geopolitical Impact: Cyber-espionage influences global political tensions.

5. Impact of Cloud Security Threats

Cloud environments store massive amounts of corporate data, making them prime targets. Misconfigured settings and insecure APIs result in breaches affecting millions of users globally.

Key Impacts:

Mass Data Exposure: Millions of records leaked due to misconfigured cloud buckets (S3, Azure Blob).

Service Downtime: Attacks on cloud resources disrupt SaaS operations and business continuity.

Financial Impact: Unexpected computer charges from unauthorized resource usage (e.g., crypto mining).

Compliance Failures: Breaches led to audits, legal action, and regulatory fines.

Insider Threat Amplification: Employees or vendors with cloud access can misuse privileges.

REAL WORLD CASE STUDIES

1. Ransomware Attack on CHANGE Healthcare (2024)

In February 2024, Change Healthcare – one of the largest U.S. healthcare payment processors was hit by a ransomware attack by the Black Cat/ALPV group. The attack shut down nationwide prescription processing and healthcare billing systems.

What Happened:

The attackers infiltrated the system using stolen credentials and deployed ransomware, encryption critical systems, and stealing 6TB of data.

Impact:

- Disruption in medical claims processing across the U.S.
- Pharmacies unable to process prescriptions for weeks
- Estimated financial loss: $872 million
- Sensitive patient data compromised
- Hospitals temporarily switches to manual operations

Relevance:

Shows how ransomware can cripple critical public infrastructure.

2. XZ Utils Backdoor Supply Chain Attack (2024)

In March 2024, a critical backdoor was discovered in XZ Utils, a widely used Linux compression tool. A malicious contributor had been adding the backdoor slowly over multiple updates.

What Happened:

The attacker tried to insert a remote code execution backdoor into the tool, which would have allowed attackers to hijack Linux systems globally.

Impact:

- Potential compromise of millions of Linux servers.
- Threat detected *just before* mass deployment.
- Considered one of the most sophisticated supply chain attacks ever discovered.
- Revealed how open-source ecosystems can be manipulated.

Relevance:

Highlights the risk of trust-based software development and large-scale supply chain vulnerabilities.

3. Cloudflare Cloud Outage Attack Attempt (2024)

Cloudflare reported multiple sophisticated attack attempts targeting its internal Atlassian environment in 2024. The attack originated from a compromised third-party vendor system linked to the Okta breach.

What Happened:

Attackers gained access to limited Cloudflare systems using session tokens stolen from Okta. Cloudflare detected unusual activity and contained the breach.

Impact:

- No customer data leaked, but internal systems were accessed.
- Demonstrated the interconnected threat of identity-based attacks.
- Showed how a compromise of a security vendor can affect high-value targets.

Relevance:

Cloud-focused identity attacks are rising sharply due to remote work and cloud adoption.

4. Snowflake Database Breach (2024 – 2025)

Between late 2024 and early 2025, multiple companies using Snowflake (a major cloud data warehouse service) suffered severe data breaches. Threat actors used stolen credentials from infostealer malware to access customer databases.

What Happened:

Attackers sold data from companies like Santander Bank and Ticketmaster on dark web forums.

Impact:

- 560+ million Ticketmaster customer records stolen.
- Sensitive bank customer data exposed.
- Attackers leveraged misconfigured Snowflake instances and lack of MFA.
- Companies faced financial penalties and customer lawsuits.

Relevance:

Shows how cloud misconfigurations + stolen credentials can lead to massive data breaches.

5. UK Ministry of Defense Data Leak (2024)

In May 2024, the UK Ministry of Defense faced a major data breach involving personal and payroll information of British military personnel.

What Happened:

The breach originated from a compromised third-party payroll contractor.

Impact:

- Potential exposure of sensitive data of 270,000 military members.
- Heightened national security risks.
- Investigation into potential foreign nation-state involvement.
- Forced rapid shutdown and restructuring of payroll systems.

Relevance:

Shows the severe consequences of third-party vendor compromise on national security.

6. MGM Resorts Cyberattack (Late 2023 – 2024)

While the attack started in 2023, its operational and financial impacts extended well into 2024. Scattered Spider hackers infiltrated MGM through social engineering.

What Happened:

Attackers impersonated an employee during a helpdesk call and gained network access.

Impact:

- Slot machines, hotel check-ins, and digital room keys stopped working.
- MGM lost over $100 million.
- Customer data exposed.

Relevance:

Demonstrates how simple human manipulation can compromise large corporations.

7. Critical Infrastructure Attack on Denmark's Power Grid (2024)

In late 2024, Denmark reported a cyberattack targeting parts of its power infrastructure.

What Happened:

Hackers exploited vulnerabilities in industrial control systems (ICS).

Impact:

- Temporary disruption of grid services.
- Forced system shutdowns to prevent equipment damage.
- Government attributed attack to nation-state actors.

Relevance:

Shows increasing threat to critical infrastructure worldwide.

PREVENTIVE MEASURES

To counter the rapidly evolving cyber threats of 2024 – 2025, organizations must adopt a multi-layered security strategy that includes technology, processes, and human awareness. Preventive measures ensure resilience reduce attack surfaces and enable faster detection and response. The following are comprehensive preventive measures aligned with modern threat landscapes.

1. **Strengthening Ransomware Defenses**
   Ransomware attacks continue to rise in sophistication, using zero-day exploits, phishing, and double extortion. Preventive measures must focus on proactive detection and backup strategies.
   Key Preventive Measures:
   - Regular Data Backups: Maintain offline and immutable backups following the 3-2-1 rule.
   - Patch & Vulnerability Management: Apply updates for OS, applications, and firmware promptly.
   - Endpoint Detection & Response (EDR): Deploy advanced behavioral detection tools.
   - Network Segmentation: Isolate critical systems to prevent lateral movement.
   - Email Security: Filter malicious links and attachments using secure email gateways.
   - Zero Trust Architecture: Enforce least privilege and verify every access request.

2. **Mitigating Phishing & Social Engineering Attacks**
   Human error remains the biggest vulnerability. Attackers rely on psychological manipulation to steal credentials or deploy malware.
   Key Preventive Measures:
   - Multi-Factor Authentication (MFA): Prevents unauthorized access even if credentials are stolen.
   - Security Awareness Training: Regular simulations to train employees to detect phishing attempts.
   - Email Authentication Protocols: Implement SPF, DKIM, and DMARC.
   - Password Policies: Enforce strong, unique passwords and password managers.
   - Browser Isolation: Protects users from malicious websites.

3. **Securing the Supply Chain**

   Modern attacks target trusted vendors, open-source libraries, and third-party service providers. Zero visibility into the supply chain increases organizational risk.

   Key Preventive Measures:

   - Vendor Risk Assessment: Evaluate the security posture of all third-party suppliers.
   - Software Bill of Materials (SBOM): Track all dependencies and open-source components.
   - Code Integrity Tools: Use signed updates and integrity checks.
   - Continuous Monitoring: Monitor third-party access, API calls, and unusual behavior.
   - Strict Access Controls: Use the Principle of Least Privilege (PoLP) for vendors.
   - Incident Reporting Contracts: Ensure vendors follow mandatory breach disclosure rules.

4. **Defending Against Advanced Persistent Threats (APTs)**

   APTs require long-term, stealthy detection methods as they target critical infrastructure and sensitive data.

   Key Preventive Measures:

   Threat Intelligence Integration: Use real-time threat feeds and IOC updates.

   - Network Behavior Analytics (NBA): Detect anomalies in traffic and user behavior.
   - Deception Technologies: Deploy honeypots to identify intrusions early.
   - Strong Identity Security: Enforce privileged access management (PAM).
   - Zero Trust Network Access (ZTNA): Replace VPNs with continuous authentication models.
   - Air-Gapped Systems: Protect critical systems in high-risk industries (energy, defense).

5. **Enhancing Cloud Security**

   With rapid cloud migration, misconfigurations and weak IAM practices lead to large-scale breaches.

   Key Preventive Measures:

   - Cloud Security Posture Management (CSPM): Automated detection of misconfigured resources.
   - Identity & Access Management (IAM): Enforce least privilege, role-based access, and MFA.
   - Secure API Gateways: Protect APIs from injection and unauthorized access.

- Encryption: Encrypt cloud data at rest and in transit.
- Logging & Monitoring: Enable audit logs like AWS CloudTrail, Azure Monitor, GCP Cloud Logging.
- Data Loss Prevention (DLP): Detect sensitive data leaving cloud systems.

6. Improving Cyber Hygiene Across the Organization

Cyber hygiene refers to essential security practices needed to maintain a baseline protective posture.

Key Preventive Measures:

- Asset Inventory: Maintain updated lists of hardware and software assets.
- Regular Security Audits: Conduct vulnerability scans and penetration testing.
- Access Revocation: Immediately remove access for departed employees or vendors.
- Secure Configuration Management: Use tools like CIS Benchmarks.
- Incident Response Planning (IRP): Prepare playbooks for ransomware, phishing, and cloud breaches.

7. Regulatory & Compliance – Based Measures

Adhering to regulations ensures organizations follow global standards in data protection and cybersecurity.

Key Preventive Measures:

- GDPR, HIPAA, PCI-DSS Compliance: Ensure legal protections for sensitive data.
- ISO 27001 Implementation: Strengthens the overall information security management system (ISMS).
- Regular Audits & Documentation: Maintain proper logs, records, and governance structures.
- Data Classification Policies: Prioritize protection of critical and sensitive data.

FUTURE SCOPE

As cyber threats continue to evolve, organizations must adopt a forward-looking strategy to strengthen their defense posture. Future developments in cybersecurity are expected to focus on:

1. **AI Driven Cyber Defense**
   - Use of machine learning to detect anomalies in real-time.
   - Automated threat hunting and incident response systems.
   - AI-based phishing detection and malware classification.

2. **Quantum Resistant Cryptography**
   - Transition toward post-quantum encryption algorithms.
   - Preventing future decryption of stored sensitive data by quantum systems.

3. **Advanced Cloud Security Solutions**
   - Increased adoption of Cloud-Native Application Protection Platforms (CNAPP).
   - Automated misconfiguration detection across multi-cloud environments.
   - Enhanced API security with behavioral analytics.

4. **Integrated Supply Chain Security**
   - Broader implementation of Software Bill of Materials (SBOM).
   - Mandatory supply chain audits and real-time vendor risk scoring.
   - Secure-by-design development practices.

5. **Zero Trust Expansion**
   - Wider deployment in critical infrastructure.
   - Identity-centric access validation across all network layers.
   - Integration of passwordless authentication methods.

6. **Global Cyber Policy & Collaboration**
   - Stronger international laws against cybercrime.
   - Increased intelligence-sharing among governments and enterprises.
   - Collective response frameworks for large cyber incidents.

CONCLUSION

The cybersecurity landscape of 2024–2025 is marked by rapidly evolving threats such as ransomware, supply chain attacks, cloud vulnerabilities, social engineering, and advanced persistent threats. These modern attack techniques increasingly target critical infrastructure, cloud ecosystems, and interconnected digital services, making organizations more vulnerable than ever.

This report highlights how these cyber threats impact business operations, financial stability, national security, and public trust. Through real-world case studies, it becomes clear that no sector is immune and attackers are continuously improving their capabilities using automation, AI, and credential-based exploitation.

Preventive measures such as Zero Trust architecture, multi-factor authentication, continuous monitoring, cloud security posture management, and robust employee training—are essential to building a resilient cybersecurity framework. Ultimately, reducing cyber risk requires a combination of strong technical defenses, updated policies, informed personnel, and proactive threat intelligence.

REFERENCES

- IBM Security. “Cost of a Data Breach Report 2024.” IBM Corp., 2024.
- CrowdStrike. “2024 Global Threat Report.” CrowdStrike Intelligence, 2024.
- Palo Alto Networks Unit 42. “Ransomware and Extortion Report 2024.” Unit 42 Threat Intelligence, 2024.
- Verizon. “2024 Data Breach Investigations Report (DBIR).” Verizon Enterprise, 2024.
- U.S. Department of Health and Human Services. “Update on Change Healthcare Cybersecurity Incident.” HHS Cybersecurity Program, 2024.
- CERT Coordination Center. “XZ Utils Backdoor Analysis (CVE-2024-3094).” Carnegie Mellon University, 2024.
- Cloudflare, Inc. “Cloudflare Security Update: Investigation of Unauthorized Access Attempt.” Cloudflare Security Blog, January 2024.
- Snowflake Inc. & Mandiant. “Joint Security Alert on Credential-Based Attacks Targeting Snowflake Accounts.” Mandiant Threat Intelligence, 2024–2025.
- UK Ministry of Defence. “MOD Statement on 2024 Payroll System Data Exposure Incident.” Government of the United Kingdom, 2024.
- European Union Agency for Cybersecurity (ENISA). “Threat Landscape Report 2024.” ENISA Publications, 2024.
- Microsoft Threat Intelligence. “Nation-State Activity Trends 2024.” Microsoft Security, 2024.
- National Institute of Standards and Technology (NIST). “Zero Trust Architecture – Special Publication 800-207.” U.S. Department of Commerce, 2023–2024 Updates.
- World Economic Forum. “Global Cybersecurity Outlook 2025.” WEF Centre for Cybersecurity, 2025.
- Okta Security. “Analysis of 2023–2024 Identity Compromise Events.” Okta Security Response Team, 2024.
- Kaspersky Global CERT. “Advanced Persistent Threat Activity Report 2024.” Kaspersky Labs, 2024.