ANNUAL THREAT PULSE REPORT

2024

DigitalXRAID

CYBER SECURITY EXPERTS

Executive Summary

2024 was a landmark year in cybersecurity, marked by the rising sophistication of cyber threats, a growing reliance on AI-driven attacks, and an intensifying focus on critical infrastructure and emerging technologies.

DigitalXRAID's Threat Pulse Reports provided monthly updates on the evolving threat landscape, highlighting key vulnerabilities, new attack methodologies, and targeted sectors. This annual report summarises the findings from these reports, offering further insights into trends, patterns, and actionable recommendations for organisations to bolster their defences in 2025 and beyond.

2024 was defined by innovation in cybercrime, the weaponisation of AI and automation, and the continued targeting of critical industries. With ransomware groups evolving, zero-days being exploited at scale, and cloud infrastructure becoming a prime target, 2025 will require a proactive, intelligence-driven approach to cybersecurity.

At DigitalXRAID, we remain committed to ensuring that the bad guys don't win. Our industry-leading security services, expert SOC analysts, and cutting-edge threat intelligence will continue to protect organisations against the ever-changing cyber threat landscape.

Key Findings

2024 was a pivotal year in cybersecurity, with threat actors evolving their tactics to exploit vulnerabilities across industries. DigitalXRAID's Threat Pulse Reports provided a detailed overview of the shifting threat landscape, highlighting trends, attack methodologies, and the most frequently targeted sectors.

Key Threat Trends in 2024

- Ransomware Evolution – New ransomware strains like Mallox, Kasseika, and SystemBC emerged, with attackers adopting stealthier, highly targeted techniques.
- Exploitation of Zero-Day Vulnerabilities – Threat actors leveraged unpatched CVEs in widely used platforms, with peak activity seen in June and November.
- AI-Powered Cybercrime – Attackers used AI for phishing, deepfake scams, and automated attacks, making social engineering more sophisticated and harder to detect.
- Cloud Services Under Attack – Misconfigurations in AWS, Microsoft Azure, and Google Cloud exposed businesses to data breaches and credential theft.
- Phishing-as-a-Service (PhaaS) Growth – Mamba 2FA enabled cybercriminals to bypass MFA, posing a high risk to Microsoft 365 and Google Workspace users.

Most Severe Threat of 2024

The most critical cyber threat of the year was the exploitation of Google Chrome's Zero-Day Vulnerability (CVE-2024-21412) by the Lazarus Group, allowing for remote code execution and widespread credential theft. This vulnerability affected millions of users worldwide, reinforcing the importance of rapid patching and proactive security measures.

Implications and Recommendations

The findings from 2024 highlight the increasing complexity and automation of cyberattacks, with AI-driven and zero-day exploitation becoming primary attack vectors. As cybercriminals adapt to new security measures, businesses must shift towards proactive, intelligence-led cybersecurity strategies.

Key Recommendations for 2025

- Strengthen AI-Driven Threat Detection – Automated SOC monitoring and anomaly detection will be crucial against evolving threats.
- Adopt a Zero Trust Model – Implement strong authentication, least privilege access, and network segmentation to limit attack surfaces.
- Improve Cloud Security Posture – Regular security audits and CSPM solutions are essential to prevent misconfigurations and API exploits.
- Enhance Cyber Resilience – Proactive threat hunting, security awareness training, and real-time incident response drills will mitigate risks.
- Invest in Ransomware Defences – Use EDR/SOC/XDR solutions, offline backups, and MFA hardening to minimise ransomware impact.

As 2025 approaches, businesses must prioritise adaptability, automation, and intelligence-driven defences to stay ahead of evolving cyber threats. DigitalXRAID remains at the forefront of cybersecurity, providing 24/7 threat monitoring and expert guidance to protect organisations worldwide.

Introduction to the 2024 Cybersecurity Landscape

2024 was a year of rapidly evolving cyber threats, with attackers leveraging automation, AI, and advanced evasion techniques to increase their success rates.

The cybersecurity landscape of 2024 has been marked by an unprecedented array of cyber threats that have challenged organisations globally. From sophisticated ransomware campaigns to covert state-sponsored espionage activities, the threats have not only grown in volume but have also significantly increased in complexity and sophistication.

Most Common Cyber Threats

2024 saw various threat types targeting businesses, with ransomware and phishing attacks remaining in the forefront. Analysing the last 12 months revealed recurring cyber threats that evolved and gained prominence throughout the year.

- Ransomware remained dominant, with new variants emerging nearly every month.
- Zero-day exploits peaked in June and November, aligning with a surge in cybercriminal activity.
- Phishing campaigns became more advanced, incorporating AI and automation to bypass security measures.
- Cloud-related breaches increased, particularly those linked to misconfigurations and credential theft.

Most Frequently Targeted Technologies

Throughout 2024, threat actors focused on exploiting vulnerabilities in widely used technologies. These are the most frequently mentioned technologies or companies in cyber threat reports.

- Cloud platforms (AWS, Microsoft Azure, Google Cloud) were prime targets due to misconfigurations and credential theft.
- Linux and IoT devices faced persistent attacks, particularly from malware designed for botnet expansion.
- Microsoft and Google products were frequently mentioned in security advisories, given their widespread adoption across enterprises.

Most Prevalent Attack Methods in 2024

Threat actors continuously refined their tactics, shifting towards stealthier and more efficient means of exploitation:

- Phishing & Social Engineering accounted for over 40% of major cyber incidents, making it the most prevalent attack vector. Platforms like Mamba 2FA were used to bypass Multi-Factor Authentication (MFA).
- Credential Theft & Token Exploitation surged due to weaknesses in cloud authentication systems.
- Zero-Day Exploitation remained a preferred method for advanced persistent threats (APTs) and nation-state attackers.
- Fileless Malware & Living Off the Land (LotL) Attacks gained traction, making traditional detection techniques less effective.
- Double Extortion Ransomware where attackers encrypt victim data and simultaneously exfiltrate sensitive files. Victims are threatened with public exposure of data if the ransom is not paid.
- DLL Sideloading exploited legitimate applications to load malicious DLL files. Attackers used this technique to evade detection and escalate privileges.
- Supply Chain Attacks exploited third-party dependencies or vulnerabilities in software supply chains to compromise multiple organisations simultaneously.
- Cloud Exploits and Misconfigurations exploited vulnerabilities in cloud services or misconfigured cloud storage to gain access to sensitive data or resources.
- AI-Driven Cyberattacks employed generative AI to automate tasks like crafting phishing emails, personalising malware, and evading detection.

Key Cyber Threat Trends of 2024

The cybersecurity landscape of 2024 was marked by rapid evolution in attack methodologies, increased automation, and an expanding threat surface.

Key trends included the rise of fileless malware, the growth of RaaS, the exploitation of zero-day vulnerabilities, and the targeting of critical infrastructure.

As we move into 2025, organisations must adopt proactive security measures, including enhanced threat intelligence, Zero Trust architectures, and AI-driven cybersecurity solutions to mitigate these growing risks.

Recurring & Evolving Threats Per Month

January:

- QakBot Malware – A long-standing banking trojan used for credential theft and network infiltration.
- Boldmove Linux Malware – A sophisticated backdoor specifically designed to target Fortinet appliances.

February:

- PureCrypter Malware – A loader malware distributing info-stealers and RATs.
- Beep Malware – Noted for its stealthy evasion techniques to bypass security solutions.

March:

- AlienFox Malware – Targeted cloud services, particularly misconfigured AWS instances.
- Elementor Pro Plugin Vulnerability – Exploited in widespread attacks affecting WordPress sites.

April:

- Fake Browser Updates Malware – Attackers lured victims into downloading malicious browser updates.
- Windows SmartScreen Exploitation – Used to deliver the DarkGate malware.

May:

- PHP Remote Code Execution Vulnerability – Allowed attackers to execute arbitrary code on Windows servers.
- ValleyRAT Trojan – A Chinese-linked malware with extensive evasion capabilities.

June:

- SpiceRAT Malware – Targeted government agencies across EMEA and Asia.
- Malvertising Campaigns – Used to deploy Oyster Backdoor malware.

July:

- North Korea-Linked Malware – Aimed at software developers across Windows, Linux, and macOS.
- VMware ESXi Flaws – Exploited to deploy ransomware.

August:

- Gafgyt Botnet – Exploited weak SSH passwords for crypto mining.
- AI-Driven Deepfake Scams – Used for financial fraud and identity theft.

September:

- LemonDuck Malware – Exploited SMB vulnerabilities for cryptojacking.
- Akira Ransomware – A highly active ransomware group using double extortion tactics.

October:

- Phishing-as-a-Service (Mamba 2FA) – Enabled cybercriminals to bypass MFA protections.
- Dragonfly 2.0 Cyber Campaign – Targeted energy infrastructure and industrial control systems.

November:

- Google Chrome Zero-Day (CVE-2024-21412) – Exploited by the Lazarus Group for credential theft.
- AI-Enhanced Ransomware – Attackers leveraged AI to enhance phishing and social engineering tactics.

December:

- Snowflake Data Breach – Impacted major organisations like Ticketmaster and AT&T.
- Midnight Blizzard Email Compromise – A Russian APT targeting Microsoft executives.

Key Observations & Emerging Threat Trends

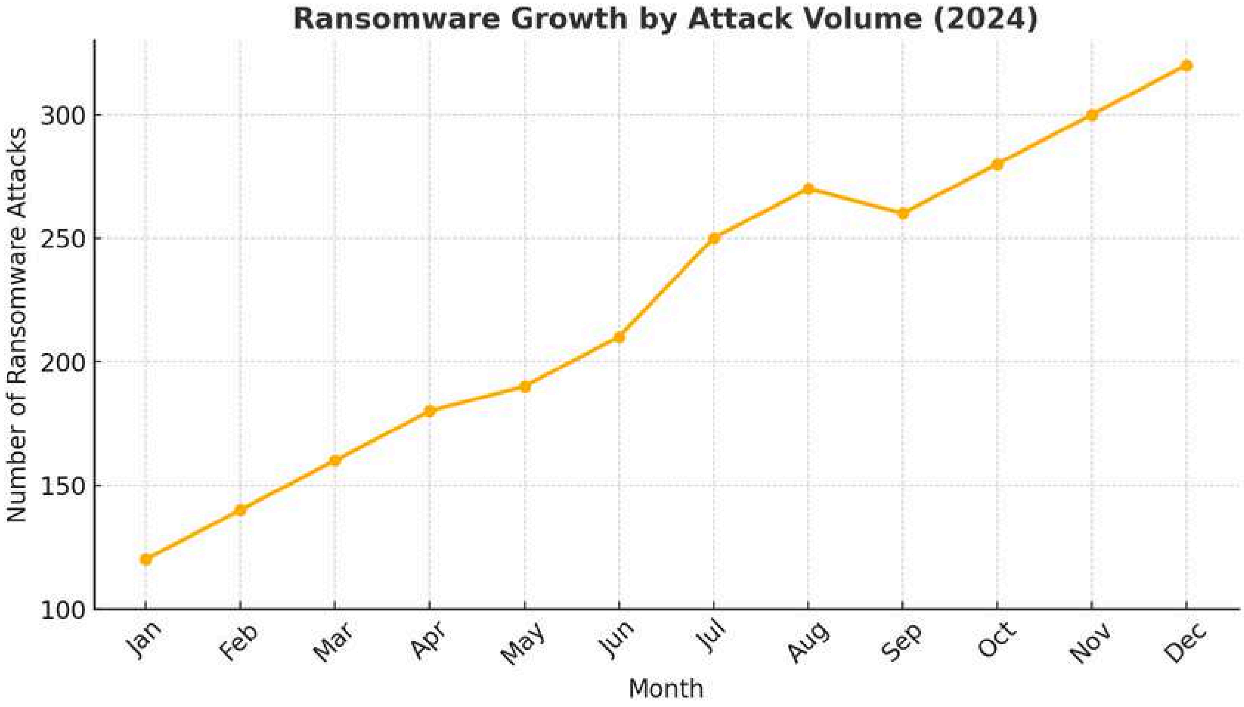
Rise of Fileless Malware

- Fileless malware attacks surged in 2024, leveraging system processes to execute malicious payloads without leaving traditional malware signatures. This method was seen in:
- LotL (Living off the Land) attacks – Used legitimate system tools such as PowerShell and Windows Management Instrumentation (WMI) for malicious activity.
- Stealthy malware like Beep and Fickle Stealer – Designed to evade traditional endpoint security.

Ransomware-as-a-Service (RaaS) Proliferation

Ransomware attacks continued to dominate the cyber threat landscape, with an increase in RaaS models making sophisticated ransomware tools accessible to low-skilled cybercriminals.

- New ransomware strains: Mallox, Kasseika, SystemBC, and Akira.
- Industries affected: Finance, healthcare, government agencies, and cloud service providers.
- Notable technique: Ransomware groups increasingly used data exfiltration and double extortion tactics, increasing pressure on victims to pay ransoms.



Key Insights:

- Steady Increase Throughout the Year – The data shows a consistent rise in ransomware attacks across 2024, with notable spikes in the latter half of the year.

- Peak Activity in Q4 – Attack volumes were highest in October, November, and December, coinciding with increased cybercriminal activity targeting businesses during the holiday season.

- Mid-Year Surge in July and August – A sharp increase in attacks during the summer months suggests cybercriminals exploited periods of lower IT staff availability, a known trend in ransomware campaigns.

- Overall Growth in Attack Volume – The number of ransomware incidents increased by nearly 167% from January to December, highlighting the growing threat of Ransomware-as-a-Service (RaaS) and the adoption of stealthier attack techniques.

Strategic Recommendations:

- Proactive Threat Intelligence & Monitoring – Implement 24/7 SOC services to detect ransomware attacks early.
- Regular Security Patch Management – Reduce attack surface by ensuring all systems, applications, and endpoints are regularly updated.
- Enhanced Backup Strategies – Maintain offline, immutable backups to mitigate data loss and recovery costs.
- Security Awareness Training – Strengthen user awareness against phishing and social engineering, which remain the primary ransomware delivery methods.

Critical Infrastructure as a Prime Target

Energy, water, and healthcare sectors faced growing attacks, with:

- Dragonfly 2.0 targeting power grids.
- Unitronics PLC Attacks disrupting US-based water and energy facilities.
- Healthcare ransomware incidents affecting hospitals and medical research institutions.

Exploitation of Zero-Day Vulnerabilities

Zero-day exploits saw an alarming rise, with attackers leveraging unpatched CVEs to gain initial access.

- CVE-2024-21412 (Google Chrome vulnerability) – One of the most severe threats of the year.
- CVE-2024-47575 (Fortinet vulnerability) – Allowed unauthorised command execution.
- CVE-2024-43572 (Microsoft Windows flaw) – Affected millions of devices globally.

AI-Driven Cybercrime

Threat actors increasingly utilised AI for:

- Phishing & social engineering – Automated and highly targeted attack campaigns.
- Deepfake scams – Used for financial fraud and identity theft.
- Malware obfuscation – AI-generated malware with adaptive evasion techniques.

Ransomware Evolution

Ransomware continued to evolve throughout 2024, becoming more targeted, sophisticated, and destructive.

The year saw an increase in double extortion techniques, greater exploitation of Linux and cloud-based systems, and the emergence of Ransomware-as-a-Service (RaaS) operators, lowering the barrier for cybercriminals to execute large-scale attacks.

This chapter explores the new ransomware strains identified in 2024, their impact, and key trends shaping the ransomware threat landscape.

New Ransomware Strains in 2024

Several new ransomware families emerged this year, targeting a broad range of industries and exploiting previously unseen techniques.

2024 saw the emergence of 8 new ransomware strains, demonstrating the continued evolution of ransomware as a preferred tactic for attackers. Below is an overview of the most notable strains:

- Akira – A RaaS operation that adopted double extortion tactics, stealing data before encrypting it. Akira was linked to attacks in North America, the UK, and Australia, often exploiting compromised credentials.
- Mallox – Expanded beyond Windows targets, now infecting Linux systems and cloud environments, particularly MS-SQL servers and weak SSH configurations.
- Nitrogen – Claimed responsibility for the SRP Federal Credit Union breach, stealing sensitive financial data and demanding high ransoms.
- SystemBC – Deployed as a malware-as-a-service tool, often in conjunction with other ransomware to enable stealthy data exfiltration and persistence.
- Black Basta – This variant continued evolving with advanced evasion techniques, heavily targeting healthcare and critical infrastructure.

These strains highlight the increasing diversification of ransomware targets, as well as the ongoing shift towards stealthier, highly persistent malware variants.

Ransomware Strains of 2024

Mimic Ransomware (January)

- Features: Leverages APIs from the Windows "Everything" search tool to locate files for encryption efficiently. It employs custom encryption techniques to lock data and leave a ransom note for the victim.
- Impact: Highly efficient at targeting and encrypting specific file types, disrupting organisational operations. Victims often face significant downtime and potential data loss if backups are unavailable.

Black Basta Linux Variant (March)

- Features: A Linux-focused variant of the Black Basta ransomware, capable of encrypting virtualised environments and disrupting server infrastructure. Employs double extortion tactics (data encryption and theft).
- Impact: Targeted cloud-based and virtualised environments, highlighting a growing trend in ransomware focusing on Linux systems. It severely disrupted business continuity for affected organisations.

EDRKillShifter (August)

- Features: An advanced tool used during ransomware attacks to disable endpoint detection and response (EDR) systems. Acts as a loader for malicious drivers to gain elevated privileges and bypass security measures.
- Impact: Facilitates the deployment of ransomware by neutralising security tools, making it difficult to detect or prevent attacks in real time. Increased the success rate of ransomware payload delivery.

WarmCookie Malware (September)

- Features: Often distributed through fake browser updates, WarmCookie is a modular ransomware strain designed to lock systems and exfiltrate sensitive information.
- Impact: Primarily affected users in France and spread through phishing campaigns, disrupting businesses by locking access to critical systems and demanding ransoms.

Mallox Ransomware Variant (September)

- Features: Expanded to target both Windows and Linux systems, with a specific focus on Microsoft SQL servers and SSH vulnerabilities. Employs encryption to lock files and exfiltrates data for double extortion.
- Impact: Increased the attack surface by targeting hybrid infrastructures, such as cloud and on-premises environments. Affected businesses experienced operational downtime and reputational damage due to exposed data.

Key Ransomware Trends in 2024

Several critical ransomware trends defined 2024, shaping the way cybercriminals operated and how businesses were impacted.

Dominance of Double Extortion

- Over 80% of ransomware attacks in 2024 used double extortion, meaning that attackers not only encrypted data but also exfiltrated sensitive information.
- Victims were threatened with public data leaks to pressure them into paying ransoms.
- High-profile cases included Akira and Black Basta, both of which used this method to devastating effect.

Expansion into Cloud & Linux Environments

- Ransomware operators shifted their focus to cloud-based storage, virtualisation platforms, and Linux servers.
- Mallox and Nitrogen were among the first ransomware families to explicitly target Linux-based systems and MS-SQL servers.
- Misconfigured cloud security settings were a primary attack vector, with exploits of cloud APIs and access control misconfigurations becoming common.

AI-Powered Ransomware & Social Engineering

- AI played an increasing role in automated spear-phishing campaigns designed to deliver ransomware payloads.
- Attackers used AI-generated phishing emails and deepfake social engineering to increase their success rates.
- AI was also leveraged to bypass traditional detection methods and improve encryption speed within ransomware payloads.

Ransomware-as-a-Service (RaaS) Proliferation

- The availability of RaaS operations made it easier for cybercriminals with limited technical expertise to launch ransomware attacks.
- Groups like Black Basta and Akira used RaaS models to scale their operations and increase the frequency of attacks.

Impact of Ransomware in 2024

The rise in ransomware activity had significant financial and operational consequences across industries:

- Healthcare Sector – Hospitals, telehealth services, and pharmaceutical companies faced ransomware attacks, disrupting critical operations and putting patient data at risk.
- Finance & Banking – Credential-stealing malware, such as Fickle Stealer, was deployed alongside ransomware, leading to severe financial losses.
- Government & Public Sector – Local councils, federal agencies, and critical infrastructure providers were increasingly targeted, leading to service disruptions.
- Cloud & SaaS Providers – Attacks on misconfigured cloud environments resulted in data breaches and ransom demands.

Strategic Recommendations for Ransomware Defence

Ransomware remains one of the most disruptive and financially damaging cyber threats globally. In 2024, the continued evolution of double extortion tactics, AI-driven attacks, and cloud-targeted ransomware demonstrated that attackers are becoming more sophisticated and harder to detect.

To mitigate these threats, organisations must invest in proactive defences, adopt intelligence-driven security strategies, and strengthen cyber resilience frameworks.

- Deploy Endpoint Detection & Response (EDR/XDR) – Advanced security solutions can detect ransomware behaviour and isolate infected systems before widespread encryption occurs.

- Regular Security Audits & Patching – Keeping software, cloud environments, and endpoints updated can prevent exploitation of known vulnerabilities.

- Implement Immutable Backups – Secure, offline backups ensure businesses can restore critical data without paying ransoms.

- Enhance Phishing & Social Engineering Awareness – Security training programs should focus on AI-generated phishing risks and MFA bypass attacks.

- Adopt Zero Trust Architecture (ZTA) – Limiting access privileges and implementing strict identity verification can reduce ransomware attack success rates.

Common Threats Across the Year

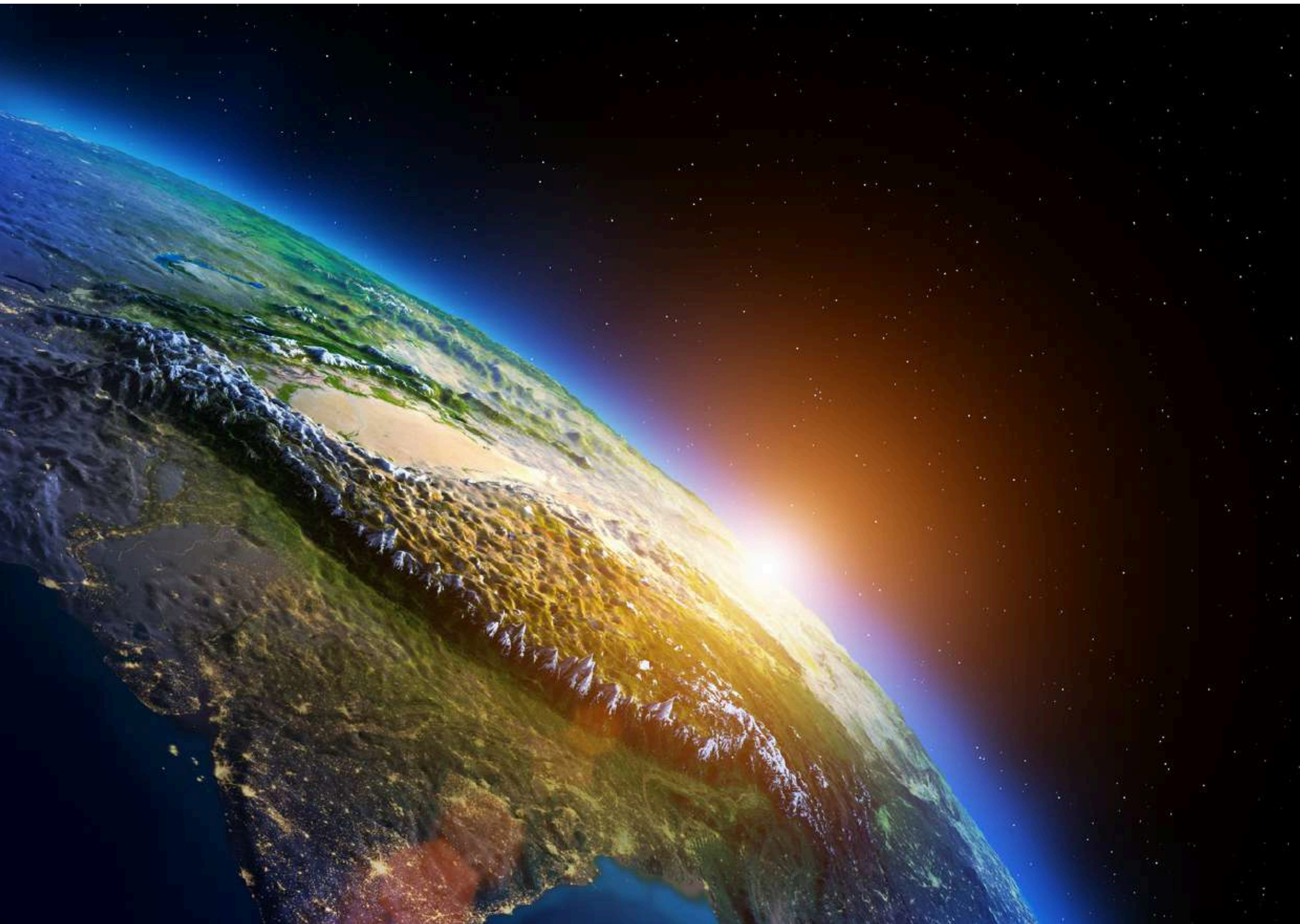
- January: Russian Cyber Espionage, jsonwebtoken Library Flaw, XLL Add-ins Infection, QakBot Malware, Boldmove Linux Malware, Mimic Ransomware, Python RAT, Titan Stealer
- February: PureCrypter Malware, Beep Malware, Trojanised PyPI Packages, HTML Smuggling, Stealc Info Stealer, Beep Malware Evasion, ESXi Servers Ransomware
- March: Microsoft OneNote Abuse, HiatusRAT Router Malware, Emotet Malware in OneNote, Microsoft Outlook Vulnerability, Elementor Pro Plugin Vulnerability, AlienFox Malware
- April: FakeBat Malware, DOS-to-NT Path Exploitation, Brokewell Android Malware, Line Runner and Line Dancer Attacks on Cisco ASA, Raspberry Robin Malware Evolution
- May: PHP Remote Code Execution Vulnerability, ValleyRAT Malware Updates, Windows Print Spooler Privilege Escalation, PyPI Crypto-Stealer Malware, TXZ File Malware Campaigns
- June: SpiceRAT Targeting EMEA and Asia, Oyster Backdoor in Malvertising Campaigns, Cisco Webex Exploitation via DLL Sideloading, GrimResource Exploitation in Microsoft MMC, P2PInfect Botnet Ransomware Module
- July: DEV#POPPER Malware Targeting Developers, SideWinder Cyberattacks on Maritime Facilities, VMware ESXi Exploitation by Ransomware Groups, OneDrive Pastejacking Phishing Campaign, Telegram EvilVideo Flaw Exploitation
- August: Voldemort Malware Using Google Sheets, Sedexp Linux Malware, Gafgyt Botnet Crypto Mining Campaign, EDRKillShifter in Ransomware Attacks, Deepfake Scams Promoting Fraudulent Investments
- September: LemonDuck Malware Exploiting SMB Vulnerabilities, Yoda Crypter Attacks via VirusTotal, Earth Lusca's KTLVdoor Backdoor, Akira Ransomware Expansions, Mallox Ransomware Targeting Linux Systems
- October: Mamba 2FA Phishing-as-a-Service Platform, BlackCat Ransomware Targeting Healthcare, Gelsemium Attacks on Real Estate Sector, LAURIONITE Exploitation of Oracle Systems, Dragonfly 2.0 Targeting Power Grids
- November: AI-Enabled Ransomware Campaigns, Zero-Day Exploitation in Google Chrome, Token Exploitation at the Internet Archive, Fileless Malware Surge in UK Businesses, Cloud Security Misconfigurations
- December: Snowflake Data Breach, Midnight Blizzard Email Compromise, BeyondTrust Software Breach in US Treasury, Ascension Health Ransomware Attack, Unitronics PLCs Attacked in Critical Infrastructure

Targeted Sectors and Geographical Focus

Cyber threats in 2024 were increasingly sector-specific and geographically diverse, reflecting the growing sophistication of threat actors and their strategic targeting of high-value industries.

This chapter explores the most targeted sectors, the geographical distribution of cyberattacks, and the broader implications for cybersecurity resilience.

2024 saw a major shift in cyber threat targeting, with a clear focus on critical infrastructure, financial institutions, and cloud services. The expansion of state-sponsored espionage and AI-driven cybercrime added new dimensions to the global threat landscape.



Most Targeted Sectors in 2024

Healthcare

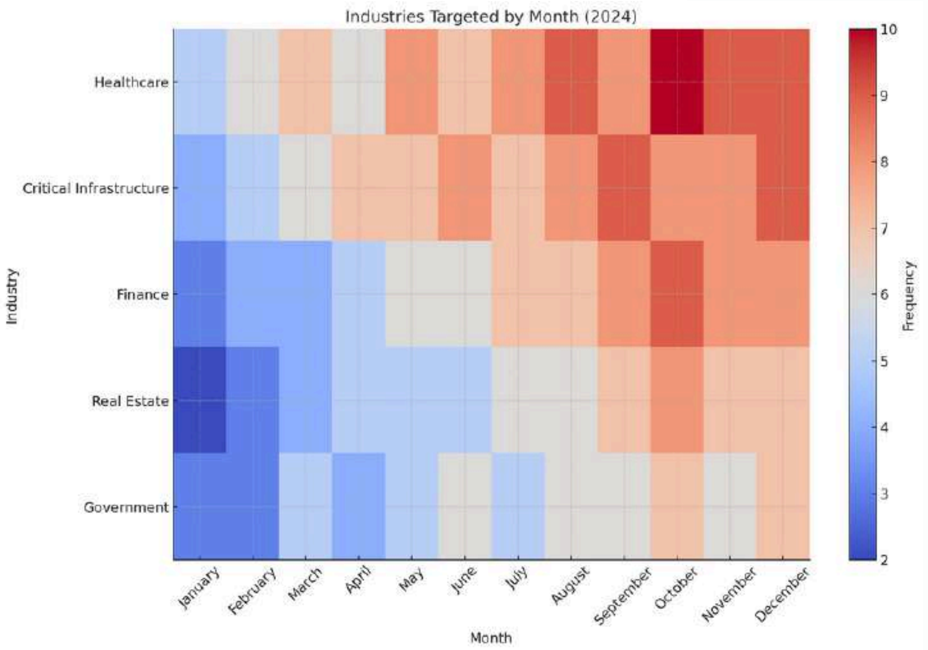
- Key Attack: Ascension Health Ransomware Attack
- Threat Actors Involved: BlackCat ransomware group, financially motivated cybercriminals
- Methods Used: Ransomware, data exfiltration, DDoS attacks
- Impact: Service disruptions, patient data breaches, ransom demands

The healthcare sector saw an alarming rise in ransomware attacks, with hospitals and medical service providers targeted due to their reliance on uninterrupted operations. The BlackCat ransomware group and other APT actors conducted double extortion attacks, disrupting patient care and demanding high ransoms.

Critical Infrastructure

- Key Attack: Dragonfly 2.0 targeting energy & water systems
- Threat Actors Involved: Dragonfly group, CyberAv3ngers
- Methods Used: Industrial Control System (ICS) exploitation, network infiltration, remote access malware
- Impact: Potential for operational shutdowns, data breaches, and infrastructure sabotage

Critical infrastructure—including energy grids, water systems, and industrial facilities—became a major target. The Dragonfly 2.0 campaign escalated its activities, shifting from reconnaissance to direct attacks on operational systems, particularly in power grids and water treatment facilities. Additionally, CyberAv3ngers exploited Unitronics PLC vulnerabilities, compromising at least 34 water treatment systems in the U.S.



Finance & Banking

- Key Attack: Evilnum targeting financial institutions
- Threat Actors Involved: Evilnum, Lazarus Group, AI-powered phishing campaigns
- Methods Used: Credential theft, deepfake fraud, token exploitation
- Impact: Stolen financial data, fraudulent transactions, regulatory challenges

The finance sector remained a prime target for cybercriminals, with Evilnum leading spear-phishing campaigns to steal customer records, payment information, and banking credentials. The rise of AI-driven fraud, such as deepfake impersonation and automated phishing, increased financial losses.

Government & Public Sector

- Key Attack: UK Council DDoS Attacks
- Threat Actors Involved: State-sponsored groups, hacktivists
- Methods Used: DDoS attacks, data exfiltration, system compromise
- Impact: Disruption of government services, exposure of citizen data

State-backed APTs and hacktivist groups ramped up attacks on government agencies, often in retaliation for geopolitical events. Several UK councils suffered major DDoS attacks, leading to temporary service disruptions for essential public services.

Cloud & SaaS Providers

- Key Attack: Volkswagen's Cariad Cloud Misconfiguration
- Threat Actors Involved: Cybercriminal syndicates
- Methods Used: Exploitation of misconfigured cloud environments, API abuses, credential stuffing
- Impact: Data exposure, regulatory fines, customer trust erosion

As businesses migrated to the cloud, attackers targeted misconfigured cloud environments. Volkswagen's Cariad suffered a cloud security breach, highlighting the risks of weak access controls and poor API security management.

Geographical Analysis of Cyber Threats in 2024

Cyberattacks in 2024 expanded beyond traditional hotspots, with threat actors shifting focus to emerging economies and previously under-targeted regions.

Expansion Beyond Europe & North America

- APT groups such as SideWinder and Evilnum increased attacks in the Middle East, Asia, and Australia.
- Cybercriminal syndicates exploited regional financial hubs, targeting banks and fintech startups in Canada and Southeast Asia.

State-Sponsored Espionage & Geopolitical Attacks

- China-linked group Gelsemium targeted web applications in real estate, finance, and government sectors.
- The Lazarus Group exploited a Google Chrome Zero-Day (CVE-2024-21412), conducting widespread espionage across multiple countries.

Critical Infrastructure Attacks Increasing in the Middle East & Asia

- Dragonfly 2.0 and CyberAv3ngers focused on energy grids and water facilities in the United States, Indonesia, and the Middle East.
- DDoS campaigns in the UK and Australia disrupted government services and telecommunications.

Emerging Technologies and Exploits

The rapid evolution of technology in 2024 introduced new attack surfaces and vulnerabilities. As organisations accelerated digital transformation, adversaries adapted their tactics to exploit weaknesses in emerging technologies, particularly cloud environments, artificial intelligence (AI), and hybrid IT infrastructures.

As adversaries continue to leverage automation, deepfake technology, and sophisticated zero-day exploits, organisations must shift towards proactive, intelligence-driven cybersecurity strategies.

Cloud Security: A Critical Attack Vector

The expansion of cloud adoption across enterprises brought with it a surge in cloud-targeted cyberattacks. Adversaries exploited misconfigurations, weak access controls, and API vulnerabilities to gain unauthorised access to sensitive data.

Misconfigurations: The Primary Entry Point

- Case Study: Volkswagen’s Cariad software division suffered a significant data exposure due to cloud misconfigurations.
    - Attackers exploited weak API authentication and mismanaged cloud storage permissions, leading to a high-profile data leak.
- Key Insight:
    - 75% of cloud security incidents in 2024 were attributed to human error and misconfigurations, highlighting the urgent need for stricter cloud security governance.

Hybrid IT Environments and Fragmented Defences

- Organisations increasingly operated in hybrid IT setups, combining on-premise data centres with multi-cloud environments.
- The lack of unified security controls across these environments led to data silos, policy inconsistencies, and an expanded attack surface.
- Attackers exploited API misconfigurations and weak IAM policies, often escalating privileges to infiltrate cloud-based assets.

AI-Driven Attacks: The Rise of Automated Cybercrime

Artificial intelligence (AI) played a pivotal role in both cyberattacks and cyber defences in 2024. While AI-enhanced threat detection helped security teams, cybercriminals leveraged AI for more sophisticated attacks, particularly in phishing, social engineering, and deepfake-enabled scams.

Deepfake Technology in Cybercrime

- Deepfake scams surged, with cybercriminals using synthetic media to impersonate executives, politicians, and financial authorities.
- A notable deepfake-driven fraud incident involved attackers impersonating a CEO's voice in a finance department phone call, leading to a multi-million-pound transaction fraud.
- AI-powered voice cloning and video manipulation were leveraged in fraud campaigns, bypassing traditional identity verification methods.

Generative AI: Automating Phishing and Malware

- Generative AI tools, were used to:
    - Craft highly convincing phishing emails that were nearly indistinguishable from legitimate communications.
    - Generate polymorphic malware that constantly evolved to evade traditional antivirus detection.
- Cybercriminals adopted AI-enhanced phishing kits, making social engineering attacks more scalable and effective.

The Evolution of Exploit Techniques in 2024

Zero-Day Exploitation: Attacking Unpatched Systems

- Zero-day vulnerabilities were a persistent and growing threat, with attackers frequently exploiting newly discovered flaws before vendors released patches.
- Google Chrome's Zero-Day Vulnerability (CVE-2024-21412) was the most severe of the year, allowing the Lazarus Group to execute remote code and steal credentials globally.
- Other high-profile zero-day exploits targeted:
  - Microsoft Defender (CVE-2024-6387) – Used to bypass endpoint security.
  - Fortinet FortiManager (CVE-2024-47575) – Exploited for privilege escalation and network compromise.

Fileless Malware and Living Off the Land (LotL) Attacks

- Attackers increasingly adopted LotL techniques, leveraging trusted system processes to execute malicious payloads.
- Fileless malware became one of the most difficult threats to detect, as it operated entirely in memory without traditional signatures.
- LemonDuck Malware was a notable example, targeting SMB vulnerabilities and Windows Defender evasion tactics.

API Exploitation in SaaS and Cloud Environments

- API vulnerabilities emerged as a key attack vector, with cybercriminals exploiting weak authentication mechanisms to:
- Bypass access controls in cloud applications.
- Exfiltrate sensitive customer data from SaaS platforms.
- The Snowflake Data Breach highlighted the risks of weak token security, leading to mass credential theft and cloud-based attacks.

Key Takeaways:

Securing Emerging Technologies

As cybercriminals rapidly adapted to the evolving technological landscape, businesses must proactively fortify their defences.

- **Cloud Security Prioritisation:**
  - Implement Cloud Security Posture Management (CSPM) to detect misconfigurations in real-time.
  - Enforce least privilege access and multi-factor authentication (MFA) for cloud applications.

- **Defending Against AI-Powered Threats:**
  - Develop deepfake detection mechanisms for executive communications and financial transactions.
  - Use AI-driven anomaly detection to flag AI-generated phishing campaigns.

- **Mitigating Zero-Day Exploits and Fileless Malware:**
  - Deploy Endpoint Detection and Response (EDR) solutions to monitor LotL attack techniques.
  - Prioritise vulnerability patching and implement virtual patching for unpatched software.

- **Enhancing API and Token Security:**
  - Enforce strict API authentication policies and regularly rotate API keys.
  - Implement real-time monitoring for abnormal API traffic to detect potential exploits.

Patterns in Vulnerability Severity (CVE Analysis)

Vulnerability management remained a cornerstone of cybersecurity strategy in 2024, as attackers increasingly exploited unpatched systems and zero-day vulnerabilities to infiltrate organisations.

Throughout the year, Common Vulnerabilities and Exposures (CVEs) played a crucial role in shaping the cyber threat landscape, with critical vulnerabilities making up the largest proportion of reported CVEs.

This chapter provides an in-depth analysis of vulnerability severity patterns, highlighting the distribution of CVEs by severity, the most notable exploits, and the key takeaways for improving security posture in 2025.

Categorisation of CVEs

The severity of a CVE is typically assessed using the Common Vulnerability Scoring System (CVSS), which provides a standardised way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity.

The CVSS scores range from 0 to 10, with higher scores indicating greater severity. CVEs are categorised into the following severity levels based on their CVSS scores.

- **Critical Severity (CVSS 9.0-10):**

Vulnerabilities that pose an immediate and severe risk, often allowing for remote code execution or complete system compromise without user interaction.

- **High severity (CVSS 7.0-8.9):**

Significant vulnerabilities that can still lead to substantial harm, such as data breaches or system disruption, but may require specific conditions to exploit.

- **Moderate severity (CVSS 4.0-6.9):**

Vulnerabilities with a moderate impact which could potentially lead to limited harm under certain circumstances.

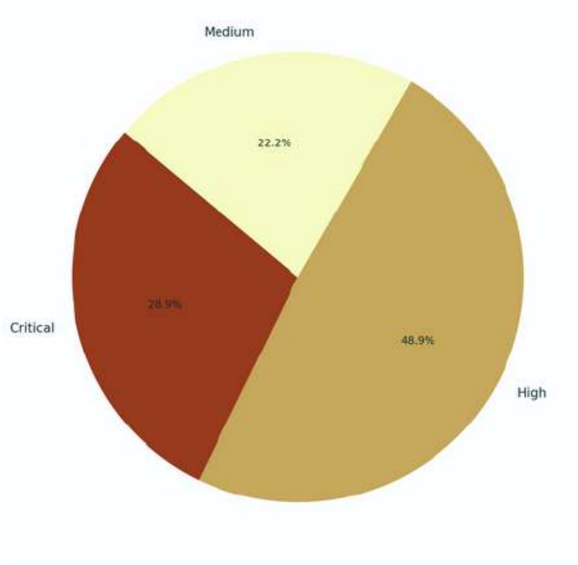
- **Low Severity (CVSS 0.1-3.9):**

Issues that pose a minimal risk, often requiring extensive user interaction to exploit or resulting in negligible impact.

Distribution of CVE Severities in 2023

Threat actors focused heavily on high and critical-severity vulnerabilities, exploiting weaknesses in widely used platforms such as Microsoft Windows, Google Chrome, Fortinet, and VMware.

This distribution underscores the prevalence of severe vulnerabilities, with nearly 80% of all CVEs categorised as High or Critical, reinforcing the urgency of patching and proactive threat mitigation.



Key Insights from CVE Severity Trends:

✅ Critical vulnerabilities dominated in high-value targets, such as financial institutions, government agencies, and critical infrastructure.
✅ Unpatched zero-day flaws were actively exploited before vendors released patches.
✅ Attackers leveraged high-severity vulnerabilities in widely used software, highlighting the risks of delayed patching cycles.

Notable CVEs of 2024

Throughout the year, several high-impact CVEs were exploited at scale, enabling ransomware campaigns, credential theft, and system compromise.

These include:

CVE-2024-47575 – Fortinet Zero-Day Vulnerability

- A critical flaw in Fortinet’s FortiManager and FortiAnalyzer.
- Exploited in the wild to bypass authentication and gain administrative control over network security configurations.
- Used in nation-state attacks to infiltrate enterprises and steal sensitive data.

CVE-2024-21412 – Microsoft Defender Exploit

- A critical vulnerability in Microsoft Defender’s SmartScreen security feature.
- Used to distribute ACR Stealer, Lumma, and Meduza malware.
- Attackers deployed booby-trapped LNK files to bypass SmartScreen warnings and execute malicious payloads.

CVE-2024-37085 – VMware ESXi Authentication Bypass

- A high-impact vulnerability in VMware ESXi, exploited by ransomware groups such as Akira and Black Basta.
- Allowed privilege escalation and lateral movement within virtualised environments.

CVE-2024-43047 – Synacor Exploit

- A zero-day vulnerability added to CISA’s Known Exploited Vulnerabilities (KEV) list.
- Attackers used this flaw to execute arbitrary code remotely on Zimbra email servers, exposing organisations to data breaches.

CVE-2024-45519 – Qualcomm Chipset Exploit

- A severe vulnerability in Qualcomm Snapdragon processors, affecting millions of Android devices.
- Exploited to enable remote code execution and privilege escalation, bypassing security restrictions on mobile devices.

Patterns in CVE Exploitation

A deep dive into CVE trends in 2024 revealed commonalities in exploitation techniques and targeted technologies.

Targeting of Widely Used Enterprise Software

- Attackers focused on vulnerabilities in Microsoft, VMware, Fortinet, and Google Chrome, knowing these platforms are widely deployed in businesses.
- Zero-day exploits in these systems allowed threat actors to maintain persistent access before patches were released.

Remote Code Execution (RCE) Dominated Exploit Chains

- A large proportion of CVEs allowed RCE, giving attackers control over systems without needing direct access.
- Exploited in:
    - Ransomware campaigns (e.g., Akira and Mallox ransomware).
    - Espionage and data theft (e.g., Lazarus Group using CVE-2024-21412).

Privilege Escalation as a Key Attack Vector

- Many CVEs were exploited to bypass authentication and gain elevated privileges.
- Example: Fortinet Zero-Day (CVE-2024-47575) enabled attackers to gain full administrative control over network environments.

Key Takeaways:
Strengthening Vulnerability Management

- **Implement Proactive Patch Management:**
  - Organisations must adopt a risk-based vulnerability management approach to prioritise patching for high-impact CVEs.
  - Zero-day vulnerabilities should be addressed through virtual patching and rapid remediation strategies.

- **Enhance Threat Intelligence Capabilities:**
  - Businesses must leverage real-time threat intelligence to stay ahead of exploited CVEs.
  - Collaborating with cybersecurity vendors and industry groups (e.g., CISA, MITRE ATT&CK) enhances defensive capabilities.

- **Deploy Security Controls to Mitigate CVE Exploitation:**
  - Implement Endpoint Detection & Response (EDR) solutions to detect exploit attempts in real-time.
  - Use Zero Trust Architecture (ZTA) and least privilege access to limit lateral movement within networks.

- **Conduct Continuous Security Testing:**
  - Regular penetration testing and vulnerability assessments help identify and patch potential weaknesses before attackers exploit them.

AI in Cyber Threats: A Game Changer

2024 marked a significant shift in the cybersecurity landscape, driven by the increasing weaponisation of artificial intelligence (AI) by cybercriminals.

Attackers leveraged machine learning models, automation, and AI-driven content generation to refine their tactics, scale attacks, and bypass traditional security defences.

This chapter examines how AI transformed cyber threats, highlighting key AI-driven attack vectors, their impact on cybersecurity, and the challenges organisations must address to defend against these evolving threats.

Computer security, cybersecurity
or information technology security
(IT security) is the protection of
computer systems and networks
frominformation disclosure,
theft of or damage to their
hardware, software, or electronic
data, as well as from
the disruption or misdirection of the
services they provide.[1]
Computer security, cybersecurity
or information technology security
(IT security) is the protection of
computer systems and networks
frominformation disclosure,
theft of or damage to their
hardware, software, or electronic
data, as well as from
the disruption or misdirection of the
services they provide.[1]
2 3 1 5 1 2 1 3 2 5 6 1 1 2 1
2 1 3 2 3 1 5 6 2 1 3 1 2

AI-Driven Cyber Threats in 2024

AI played a multifaceted role in cyberattacks throughout 2024, enabling threat actors to enhance attack efficiency, sophistication, and evasiveness.

AI-Powered Phishing Attacks

- AI-generated phishing emails became indistinguishable from legitimate communications, making detection harder.
- Attackers customised emails based on stolen personal data, business roles, and organisational context.
- Deepfake audio and video impersonations were used in business email compromise (BEC) scams, tricking victims into transferring funds or revealing credentials.

Automated Exploitation of Vulnerabilities

- AI-powered tools scanned the internet for vulnerable systems in real-time, allowing attackers to launch mass-scale zero-day exploits within hours of disclosure.
- Machine learning models were used to generate adaptive malware, capable of altering signatures to evade endpoint detection and response (EDR) solutions.

AI-Driven Malware and Ransomware

- AI-assisted ransomware strains (e.g., Mallox, Nitrogen, and SystemBC) used automated reconnaissance techniques to identify high-value assets before encryption.
- AI-powered evasion techniques made malware more resistant to signature-based detection.
- Self-learning ransomware could adapt to security controls and re-route attack paths if blocked.

AI-Powered Social Engineering and Deepfake Fraud

- Attackers used AI-generated deepfake content to conduct highly convincing social engineering attacks.
- Deepfake scams targeted:
    - Financial institutions – AI-generated voices used in fraudulent wire transfer requests.
    - Government agencies – Deepfake videos impersonating political figures for disinformation campaigns.
    - Enterprise executives – CEO fraud scams using deepfake voice cloning to instruct employees to make payments.

Impact of AI on Cybersecurity in 2024:

Increased Attack Volume and Speed

- AI-enabled attackers launched large-scale cyber campaigns faster than ever before.
- Mass automation of phishing emails, vulnerability scanning, and malware deployment significantly increased attack frequency.

Enhanced Attack Sophistication

- AI-generated malware evaded traditional security tools, forcing security teams to adopt behaviour-based detection techniques.
- AI-assisted polymorphic malware changed its structure after every infection, rendering signature-based detection ineffective.

Growing Challenges for Defenders

- Traditional cybersecurity tools struggled to keep pace with AI-powered attacks.
- Human analysts faced difficulties distinguishing between legitimate communications and AI-generated social engineering attempts.

Notable AI-Driven Cyber Attacks in 2024:

Mamba 2FA Phishing-as-a-Service (PhaaS)

- AI-generated phishing kits allowed cybercriminals to bypass multi-factor authentication (MFA).
- Used against Microsoft 365 and Google Workspace accounts, leading to data breaches in multiple industries.

AI-Powered Ransomware – The Mallox Expansion

- Mallox ransomware adapted its attack strategy using AI, automating network reconnaissance and prioritising high-value targets.
- Deployed against cloud environments and Linux systems, making it more dangerous to enterprises operating hybrid IT infrastructures.

AI-Generated Deepfake Scams in the Financial Sector

- Cybercriminals used deepfake voice technology to impersonate bank executives and authorise fraudulent transactions.
- Targeted high-profile financial institutions in the UK, US, and Australia, resulting in millions in financial losses.

AI-Enabled Cybercrime Trends to Watch in 2025:

Looking ahead, AI-driven cyber threats are expected to grow in sophistication and scale, presenting new challenges for cybersecurity teams.

AI-Augmented Malware Will Become More Adaptive

- Malware will use machine learning to adjust attack paths in real-time, avoiding detection.
- AI-assisted brute-force attacks will increase, accelerating credential theft and network infiltration.

Large-Scale Deepfake Fraud Will Increase

- Attackers will refine deepfake impersonations, making them harder to distinguish from real communications.
- AI-powered identity theft and fraud will become more frequent in business and government sectors.

AI-Driven Phishing Attacks Will Target More Sectors

- AI-generated phishing will be tailored for specific industries, using company-specific intelligence to increase success rates.
- Supply chain attacks will leverage AI-generated phishing emails to compromise software vendors and third-party service providers.

Key Recommendations:
Mitigating AI-Driven Cyber Threats

- **Invest in AI-Powered Threat Detection**
  - Organisations must deploy AI-driven security solutions capable of detecting anomalous behaviours instead of relying on traditional signature-based detection.
  - Behavioural analytics and machine learning-based security models will be crucial in detecting AI-driven attacks.

- **Enhance Employee Awareness Against AI-Generated Scams**
  - Conduct regular security awareness training to educate employees about AI-generated phishing, deepfake scams, and AI-driven fraud tactics.
  - Use real-world attack simulations to help employees recognise and respond to AI-powered threats.

- **Strengthen Email and Identity Security**
  - Implement phishing-resistant authentication, such as hardware security keys instead of SMS-based MFA, which AI-driven phishing campaigns can bypass.
  - Use email filtering and anti-impersonation tools to detect AI-generated phishing emails and deepfake attempts.

- **Deploy AI Against AI-Powered Threats**
  - Cybersecurity teams should leverage AI to defend against AI-driven attacks, using automated anomaly detection, deepfake detection models, and real-time monitoring.
  - Threat intelligence platforms enhanced with AI can help predict and counter AI-powered cybercrime tactics.

Recommendations for 2025

As cyber threats continue to evolve, organisations must adopt a proactive, intelligence-led security approach to mitigate risks effectively in 2025.

The findings from DigitalXRAID's 2024 Threat Pulse Reports indicate that AI-driven attacks, zero-day exploits, and ransomware will remain dominant threats. Meanwhile, cloud security vulnerabilities, phishing-as-a-service (PhaaS), and deepfake fraud will demand new security measures.

This chapter outlines key cybersecurity recommendations for 2025, focusing on proactive defence, cloud security, and resilience-building strategies to help organisations stay ahead of emerging threats.

Adopt a Proactive Defence Strategy

Why It Matters

2024 saw a sharp increase in AI-powered cybercrime, with attackers using automation, deepfake technology, and adaptive malware to breach defences. Organisations can no longer rely solely on reactive security measures—they must embrace proactive threat detection and anticipatory defence strategies.

Key Actions

✅ Invest in AI-Driven Threat Detection

- Deploy machine learning-based security tools that detect anomalies and emerging attack patterns in real-time.
- Use AI-powered Extended Detection and Response (XDR) solutions to analyse endpoint, network, and cloud threats dynamically.

✅ Implement Threat Intelligence Feeds

- Subscribe to real-time threat intelligence sources to identify and counter emerging attack tactics.
- Integrate threat hunting capabilities to proactively detect sophisticated attacks before they escalate.

✅ Enhance Network Segmentation

- Use micro-segmentation to isolate high-value assets and limit attack spread in case of breaches.

Enhance Incident Response and Resilience

Why It Matters

The speed and sophistication of modern cyberattacks mean that incident response (IR) plans must be continuously refined and tested. Ransomware incidents, cloud breaches, and zero-day exploits can escalate within hours—organisations need robust, tested response plans to mitigate damage.

Key Actions

✅ Conduct Regular Incident Response Drills

- Implement tabletop exercises and live attack simulations to evaluate team readiness.
- Include business continuity planning to ensure minimal operational disruption during attacks.

✅ Automate Incident Response Playbooks

- Use Security Orchestration, Automation, and Response (SOAR) tools to reduce manual effort in responding to threats.
- Automate alert triage, containment actions, and threat intelligence correlation.

✅ Establish 24/7 SOC Monitoring

- Engage a Managed Security Operations Centre (SOC) provider to ensure continuous visibility and rapid response.

Raise Cybersecurity Awareness and Training

Why It Matters

A significant percentage of cyberattacks in 2024 involved social engineering, phishing, and deepfake fraud. Employees remain one of the weakest links in cybersecurity, making security awareness training a critical investment.

Key Actions

✅ Implement Phishing Simulation Training

- Conduct regular phishing simulations to educate employees about evolving attack techniques.

✅ Educate Employees on Deepfake and Social Engineering Risks

- Train employees to detect AI-generated scams and fraudulent deepfake communications.
- Develop reporting mechanisms for suspected phishing and impersonation attacks.

✅ Establish a Culture of Cyber Vigilance

- Implement security champions programmes within departments to foster cybersecurity awareness at all levels.

Improve Patch and Vulnerability Management

Why It Matters

2024 saw zero-day vulnerabilities in major platforms like Google Chrome, Microsoft Defender, and Fortinet FortiOS being actively exploited before patches were released. The speed at which attackers weaponise new vulnerabilities means that organisations must strengthen their patch management strategies.

Key Actions

✅ Implement Automated Patch Management Solutions

- Deploy patch automation tools to apply critical updates without delay.
- Establish a risk-based patching approach, prioritising high and critical vulnerabilities.

✅ Conduct Regular Vulnerability Assessments

- Perform weekly vulnerability scans to detect and address exploitable weaknesses.
- Use penetration testing services to simulate real-world attack scenarios.

✅ Apply Virtual Patching for Zero-Days

- When vendor patches are unavailable, use virtual patching solutions to block exploits at the network level.

The 2024 threat landscape reinforced the reality that cyber threats are becoming more sophisticated, adaptive, and persistent.

Attackers continued to refine their tactics, techniques, and procedures (TTPs), leveraging artificial intelligence, automation, and emerging exploit techniques to evade detection and compromise critical systems. The weaponisation of AI in cybercrime, the expansion of ransomware capabilities, and the increased exploitation of cloud services and critical infrastructure defined the year's biggest challenges.

The insights shared in DigitalXRAID's Annual Threat Pulse Report serve as a reminder that as cyber adversaries continue to seek out and exploit vulnerabilities, organisations must remain vigilant - ensuring that their defences evolve in tandem with the threat landscape.

By prioritising the identification and remediation of high and critical severity vulnerabilities organisations can strengthen their cyber security posture and protect their vital digital assets against potential attacks.

Key Takeaways from 2024

- **AI-Powered Cybercrime:**
  - Attackers used AI for automated phishing, deepfake social engineering, and rapid vulnerability exploitation, making cyberattacks more effective and scalable.

- **Ransomware Evolution:**
  - Ransomware groups continued to refine double extortion tactics, incorporating stealthier delivery mechanisms and improved data exfiltration techniques.

- **Zero-Day Exploitation at Scale:**
  - The rapid exploitation of zero-day vulnerabilities in widely used software (e.g., Google Chrome, Microsoft Defender, Fortinet FortiOS) demonstrated the urgency of timely patching and proactive security monitoring.

- **Cloud and SaaS Exploits on the Rise:**
  - The increasing reliance on hybrid and multi-cloud environments exposed organisations to misconfigurations, insecure APIs, and unauthorised access attacks.

- **Phishing-as-a-Service (PhaaS) Proliferation:**
  - The emergence of Mamba 2FA and similar fraud-as-a-service platforms lowered the barrier for cybercriminals, increasing the volume and success rates of credential theft attacks.

- **Critical Infrastructure as a Prime Target:**
  - Attackers increasingly focused on energy, water, and healthcare systems, with incidents such as the Unitronics PLC breaches and Dragonfly 2.0 attacks on power grids signalling a growing cyber threat to national security and essential services.

DigitalXRAID

CYBER SECURITY EXPERTS

DigitalXRAID: Securing the Future

As cyber threats grow in complexity, DigitalXRAID remains at the forefront of cybersecurity innovation, offering 24/7 threat monitoring, advanced penetration testing, and industry-leading SOC services. Our expert security analysts, AI-powered threat detection, and intelligence-driven approach ensure that businesses can stay ahead of evolving cyber threats in 2025 and beyond.

Our mission remains clear:

- Protecting organisations from cybercriminals
- Ensuring business continuity despite evolving threats
- Delivering intelligence-led security solutions tailored to every industry

As we step into 2025, businesses must be prepared, proactive, and resilient. Cybersecurity is no longer just an IT function—it is a business-critical priority.

Stay Secure. Stay Resilient. Stay Ahead.

DigitalXRAID

CYBER SECURITY EXPERTS

Need the Best Defence
Against Cyber Threats?
Call us now on 0800 090 3734

info@digitalxraid.com digitalxraid.com

UKAS MANAGEMENT SYSTEMS ISO 27001 INFORMATION SECURITY MANAGEMENT

UKAS MANAGEMENT SYSTEMS ISO 9001 QUALITY MANAGEMENT

CYBER ESSENTIALS CERTIFIED PLUS

IASME CONSORTIUM

CREST

CHECK IT Health Check Service