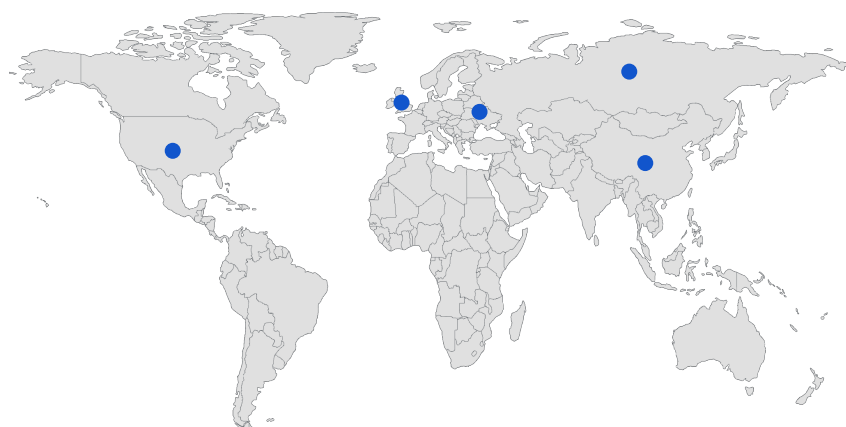


2024 Threat Intelligence Recap

Top 5 Tagged Countries of 2024



Top Tags of 2024

Government

Financial Services

Healthcare

DDoS

Malware

As we close out 2024, this special edition of our cyber threat intelligence report takes a comprehensive look back at the year's key developments. Drawing insights from the reports published throughout the year, we've identified significant trends and recurring themes that shaped the cybersecurity landscape. From evolving attack methods to the surge in ransomware campaigns and supply chain vulnerabilities, this analysis offers a unique perspective on the most pressing threats organizations faced in 2024. Use this roundup to better understand the challenges and prepare for what's ahead in 2025.

Top CVEs of 2024

Top CVEs of the past year, and their impact on our customers.

[CVE-2023-30185](#) | 19 million attacks | CVSS 9.8

- CRMEB v4.4 to v4.6 was discovered to contain an arbitrary file upload vulnerability via the component `\attachment\SystemAttachmentServices.php`.

[CVE-2024-27199](#) | 17 million attacks | CVSS 7.3

- In JetBrains TeamCity before 2023.11.4, path traversal allowing to perform limited admin actions was possible.

[CVE-2023-35082](#) | 10 million attacks | CVSS 10.0

- An authentication bypass vulnerability in Ivanti EPMM 11.10 and older, allows unauthorized users to access restricted functionality or resources of the application without proper authentication.

2024 Themes

Key cybersecurity trends and insights from 2024 reports.

Exploitation of Authentication Bypasses and Account Takeovers

→ Seen 15 Times in Threat Intelligence Reports

The past year has witnessed a significant uptick in cybercriminals exploiting authentication bypass vulnerabilities and conducting account takeover (ATO) attacks. These threats enable unauthorized access to sensitive systems, compromising critical data and disrupting services. Attackers frequently leverage authentication flaws to bypass security protocols, access privileged accounts, and deploy malware or conduct financial fraud. These trends underscore the importance of robust authentication mechanisms, patch management, and proactive monitoring to mitigate such risks.

Examples:

- **GoAnywhere MFT Vulnerability:** An authentication bypass in GoAnywhere MFT ([CVE-2024-0204](#)) allowed attackers to create administrative accounts using path traversal techniques, demonstrating the critical nature of securing web applications.
- **API Authentication Bypass in Telecommunications:** [Cox Communications](#) had a critical API authentication bypass vulnerability that exposed millions of modems to potential cyberattacks. The flaw allowed attackers to gain unauthorized control over modems, posing significant risks of data interception, service disruption, and privacy breaches.
- **Authentication Bypasses in MOVEit:** Multiple authentication bypass vulnerabilities were found in [MOVEit Transfer and MOVEit Gateway](#), which could allow attackers to gain unauthorized access to the systems. These flaws, tracked as CVE-2024-5806 and CVE-2024-5805, are critical as they can be exploited to access sensitive data without proper credentials.
- **GitLab ATO Vulnerability:** [GitLab](#) issued security updates for a critical vulnerability, CVE-2023-7028, which allows account takeover without user interaction. This flaw, rated 10.0 in severity, stems from a bug in the email verification process and affects various versions of GitLab Community Edition and Enterprise Edition.

Targeted Ransomware Campaigns on Critical Infrastructure

→ Seen 22 Times in Threat Intelligence Reports

Over the past year, ransomware campaigns have increasingly targeted critical infrastructure, especially utilities. These attacks often disrupt essential operations, compromise sensitive data, and demand substantial ransom payments. Threat actors are leveraging sophisticated tactics, including double-extortion and exploiting vulnerabilities in critical systems, to maximize their impact. The consequences of such campaigns extend beyond financial losses, often affecting public services and raising national security concerns.

Examples:

- **LockBit Ransomware on Southern Water:** The Black Basta ransomware gang targeted [Southern Water](#), a major UK water utility, claiming to have stolen 750 GB of sensitive data.
- **Trans-Northern Pipelines Ransomware Attack:** The AlphV ransomware group attacked [Trans-Northern Pipelines](#), stealing 183 GB of data. Despite no operational disruptions, the breach underscored the susceptibility of critical energy infrastructure to data theft.
- **Schneider Electric Breach:** The Cactus ransomware group targeted [Schneider Electric](#), affecting their Resource Advisor cloud platform and allegedly stealing terabytes of corporate data. This attack showcased the risks to industrial automation and energy management.
- **Solar Power Security Flaw:** Researchers uncovered a security flaw that allowed them to gain unauthorized access to [solar power systems](#) capable of generating enough energy to power the entire United States. By exploiting this vulnerability, attackers could potentially disrupt or control large-scale energy production, highlighting significant security risks within critical infrastructure sectors.

Persistent Focus on Financial and Healthcare Sector Attacks

→ Seen 106 Times in Threat Intelligence Reports

Cybercriminals have persistently targeted the financial and healthcare sectors, exploiting their critical role in society and their repositories of sensitive data. These sectors face a growing range of cyber threats, including ransomware, account takeovers (ATO), and data breaches. Attackers exploit vulnerabilities in systems, steal sensitive information, and disrupt services, often causing significant operational and financial damage. The frequency and sophistication of these attacks highlight the need for targeted cybersecurity measures in these high-risk industries.

Examples:

- **Grandoreiro Banking Trojan:** The [Grandoreiro](#) banking trojan has launched a widespread campaign targeting major financial institutions across Latin America and Europe. The trojan employs advanced social engineering tactics, including phishing emails and malicious macros, to steal credentials and financial information.
- **LoanDepot and Prudential Financial Breaches:** The [ALPHV](#) ransomware group targeted LoanDepot and Prudential Financial, exposing personal and financial data. LoanDepot's breach affected over 16.6 million individuals, while Prudential Financial suffered employee and contractor data exposure.
- **Viamedis Cyberattack:** A cyberattack on [Viamedis](#), a healthcare payment manager covering 20 million individuals, exposed sensitive data of policyholders and healthcare professionals in France.
- **Trinity Ransomware:** The U.S. Department of Health and Human Services has issued an alert warning healthcare providers of a growing threat from the [Trinity](#) ransomware group. This group specifically targets hospitals and other healthcare facilities, encrypting patient data and demanding ransom payments.

Increasing Exploitation of Software Supply Chain Vulnerabilities

→ **Seen 7 Times in Threat Intelligence Reports**

A growing number of cyberattacks in 2024 focused on exploiting vulnerabilities in software supply chains. Threat actors targeted dependencies, development tools, and third-party software to infiltrate systems. By compromising trusted software and services, adversaries can deploy malware, steal sensitive data, and disrupt operations on a large scale. These attacks highlight the critical need for organizations to secure their software supply chains and implement robust validation processes to protect against malicious exploitation.

Examples:

- **MavenGate Supply Chain Attack:** Attackers hijacked abandoned Java and Android libraries in [Maven](#)-based projects, injecting malicious code into applications.
- **PyPI Malware Distribution:** Malicious [PyPI](#) packages, including those deploying [WhiteSnake](#) malware, targeted developers and end-users by embedding malware into Python libraries, posing significant risks to software integrity.
- **Acemagic PCs with Pre-installed Malware:** Consumer PCs were discovered to contain pre-installed [malware](#) like Bladabindi and Redline, compromising systems before they even reached customers. This raised serious concerns about vetting supply chain partners in hardware manufacturing.
- **TensorFlow CI/CD Pipeline Vulnerability:** Misconfigurations in [TensorFlow's](#) CI/CD pipeline allowed attackers to inject malicious uploads to GitHub and PyPI, potentially compromising machine learning models and associated applications.

DDoS Attacks as a Weapon for Targeting Critical Industries

→ **Seen 41 Times in Threat Intelligence Reports**

Distributed Denial of Service (DDoS) attacks have emerged as a powerful weapon for disrupting critical industries, including finance, healthcare, and energy. These attacks often aim to overwhelm systems, disrupt operations, and demand ransom, posing significant challenges to targeted organizations. The use of large-scale and sophisticated multi-vector DDoS campaigns underscores the growing capability of threat actors to exploit this method, causing financial damage, reputational harm, and operational downtime for critical services.

Examples:

- **Monobank DDoS Attack:** [Monobank](#), Ukraine's largest mobile-only bank, suffered a massive DDoS attack generating 580 million requests, disrupting essential financial services amid ongoing geopolitical tensions.
- **DDoS Attack on Healthcare Systems:** Healthcare institutions in [Romania](#) faced disruptions due to a DDoS campaign that targeted the Hipocrate Information System, exacerbating operational challenges in critical healthcare services.

- **DDoS on Japanese Government:** Following military exercises between Japan and the U.S., Russian threat actor NoName057(16) launched a series of [DDoS](#) attacks on Japanese government and infrastructure websites. The attacks appeared to be politically motivated, disrupting services and signaling Russia's discontent with Japan's military collaboration.

Misconfigured Cloud and IoT Services Expose Organizations to Threats

→ Seen 8 Times in Threat Intelligence Reports

The increasing reliance on cloud and IoT services has brought significant efficiency and scalability benefits to organizations. However, misconfigurations in these services have emerged as a major vulnerability, exposing organizations to data breaches, unauthorized access, and malware attacks. Threat actors exploit these weaknesses to infiltrate networks, steal sensitive data, and disrupt operations. The growing prevalence of such incidents highlights the urgent need for stringent configuration management and continuous security monitoring.

Examples:

- **Public Elasticsearch Database in Brazil:** An unsecured Elasticsearch instance leaked 223 million records of Brazilian citizens, exposing nearly the entire population's personal data and highlighting the dangers of poor cloud security practices.
- **2FA Codes Leaked:** [YX International](#), a company specializing in SMS routing, inadvertently exposed a database containing one-time security codes for accounts on platforms such as Facebook, Google, and TikTok. Discovered by security researcher Anurag Sen, the database was accessible without a password, revealing text message contents including two-factor authentication codes and password reset links. The exposure raises concerns about the security of SMS-based two-factor authentication and the risks associated with database misconfigurations.
- **125 Million Records Exposed:** A study reveals a widespread [Firebase](#) misconfiguration, leading to the exposure of approximately 125 million user records across 900 sites. The exposed data includes plaintext passwords and sensitive billing information, highlighting the risks of cloud storage misconfigurations.
- **Google Drive Misconfiguration:** [Ateam](#), a Japanese game developer, exposed sensitive information of nearly one million people due to a Google Drive misconfiguration. The exposed data included full names, email addresses, phone numbers, and device identification numbers. The issue, which lasted for over six years, highlights the risks associated with cloud storage misconfigurations and the importance of securing cloud services.

Emerging Threats In AI and Advanced Technologies

→ Seen 18 Times in Threat Intelligence Reports

The rapid advancement of artificial intelligence and related technologies has introduced new vulnerabilities and attack surfaces. Threat actors are exploiting AI-driven systems, machine learning platforms, and advanced tools to conduct sophisticated cyberattacks. From hijacking AI models to leveraging malware-as-a-service in emerging platforms, the integration of these technologies presents challenges in securing their usage and development environments. These threats underscore the necessity for organizations to adopt robust security practices tailored to the unique risks posed by AI and advanced technologies.

Examples:

- **Hugging Face AI Model Hijacking Vulnerability:** A critical vulnerability in [Hugging Face's](#) model conversion service allowed attackers to hijack AI models, posing significant risks to supply chain security and the integrity of AI-based solutions.
- **ChatGPT Manipulated:** Security researchers demonstrated a method to manipulate ChatGPT into outputting malicious code by encoding it as [hexadecimal](#), effectively bypassing OpenAI's content filters. Using this approach, they were able to have ChatGPT generate potentially harmful code snippets that evade detection by traditional filtering mechanisms.
- **AI Health Bot Vulnerable:** Security researchers have uncovered critical vulnerabilities in Microsoft's Azure [AI Health Bot](#), which is widely used in the healthcare industry. These flaws could allow attackers to gain unauthorized access to patient data, manipulate bot responses, or disrupt healthcare services. The discovery

underscores the importance of securing AI-driven applications, particularly those handling sensitive health information.

- **Prompt Injection Enables RCE:** Security researchers have uncovered a prompt injection vulnerability in [Vanna AI](#), enabling remote code execution (RCE). Attackers can manipulate AI prompts to execute arbitrary commands, potentially compromising the systems using this AI model. The vulnerability affects applications integrating Vanna AI, necessitating immediate updates and improved prompt sanitization to mitigate risks.

Imperva Protection

Imperva provides comprehensive digital security solutions, including protection against threats to web applications and APIs— including security vulnerabilities, fraud, and bad bots, data security solutions, and security against disruptive network- and application-level DDoS attacks.