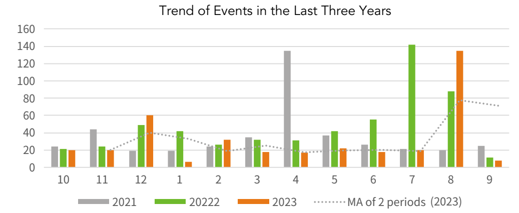
NSFOCUS

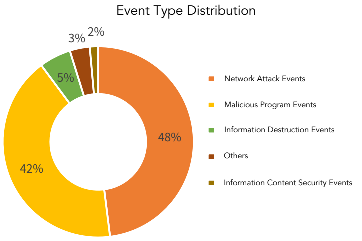
2023 ANNUAL SECURITY INCIDENT OBSERVATION REPORT

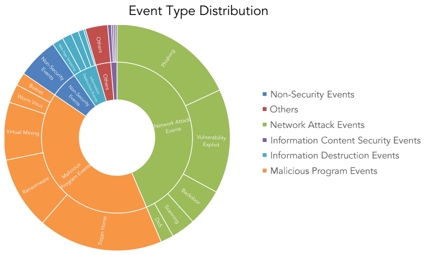
NSFOCUS, Inc

2023 Cybersecurity Landscape

In 2023, the overall security incident data showed a stable trend, with no significant fluctuations. NSFOCUS received and recorded 376 security incidents in 2023, a decrease of 33.2% from 2022. The total number of incidents in the first quarter of 2023 was 100, which increased from 2022. Since the second quarter, the number of incidents each quarter was lower than the same period in 2022. In August 2023, the number of incidents reached the highest of the year, with 135 incidents, an increase of 34.8% compared to the same period of 2022, and an increase of 85.2% compared to July.

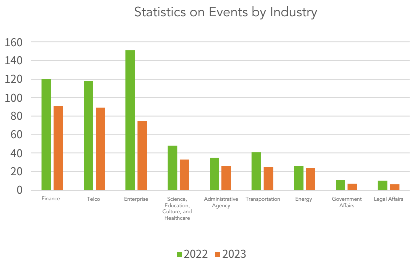




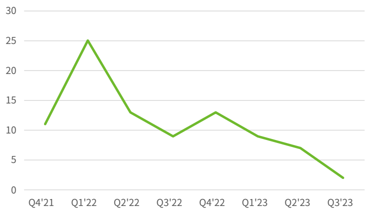


Observations of Security Incidents in 2023

The financial services and the telcos have become the main targets of attacks. According to the statistics and analysis of industry incident data in the recent two years, finance, enterprises, and telcos have always been the key targets for threat actors. However, compared with 2022, the number of emergency events from enterprises in 2023 has decreased by nearly 50%, while the financial industry and telcos have become the primary targets of attack. This to a certain extent reflects the improvement of defense capabilities and security awareness of enterprise customers, and the change in the targets of attackers.



The trend of crypto mining incidents continues to slow down, with ransomware incidents having the highest proportion. In recent years, with the improvement of security protection capabilities at the endpoint and traffic levels, mining programs have become increasingly difficult to persist long-term, making it challenging for attackers to sustain effective profits over an extended period. Statistics show that the number of mining incidents has been declining in recent years. Starting from the first quarter of 2023, the number of mining incidents has dropped to single digits.



Data Security Risks in Enterprises and Healthcare Sectors are Increasing

With the widespread use of the internet and the accelerated digitization of businesses, the number of data security incidents continues to grow. Statistics reveal that threat actors primarily target enterprises and the healthcare industry, accounting for 58% and 27% of data security incidents, respectively. Among corporate data security events, ransomware is the predominant form of attack. The surge in data ransom incidents further contributes to the proportion of enterprise data security events. The healthcare sector, characterized by large data volumes, numerous users, and weak security defenses, also becomes a prime target for attackers. Given the frequent occurrence of data security incidents due to network vulnerabilities and password security issues, organizations should prioritize vulnerability monitoring and remediation while enhancing user and corporate security awareness.

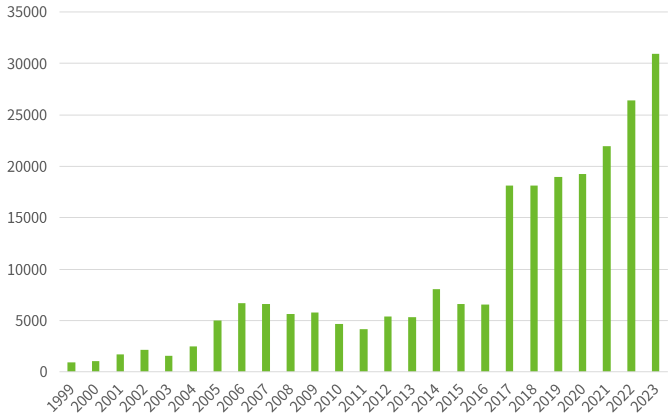
Data Security Regulations are Becoming More Robust

In March 2023, the White House released the National Strategy to Advance Privacy-Preserving Data Sharing and Analytics (PPDSA). In addition, EU legislators adopted the Data Governance Act (DGA) in September, and the European Parliament adopted the Data Act in November 2023. Both Acts are important legislative measures to implement the European Data Strategy.

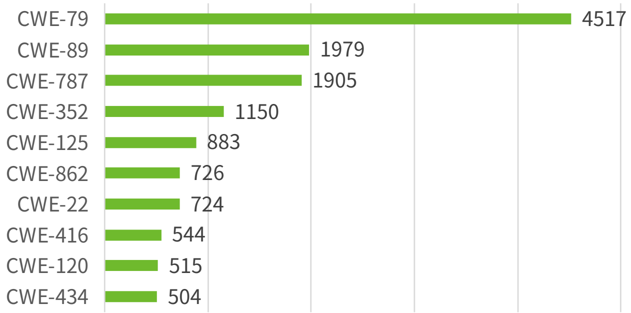
Trends in Security Vulnerabilities

In 2023, the monthly addition of vulnerabilities ranged from 2100 to 3000, exacerbating the severity of the security vulnerability landscape. High-risk vulnerabilities continue to grow. According to the National Vulnerability Database (NVD), the number of newly added vulnerabilities in 2023 reached 30,947, representing a 14.59% increase compared to the previous year. Among the vulnerabilities recorded in 2023, 27,856 were assigned with CWE IDs. The most prevalent type of vulnerability was Cross-Site Scripting (CWE-79), followed by SQL Injection (CWE-89).

Trends in Vulnerability Counts Over the Years



Top 10 Vulnerability Type in 2023



Decade-old Vulnerabilities Remain Active

According to monitored alerts from 2023, among attack events related to vulnerability exploitation, some decade-old vulnerabilities remain active, with alert counts exceeding three hundred thousand. For example:

- CVE-2014-6271: GNU Bash Environment Variable Remote Code Execution Vulnerability. Alert count: 336,279

Additionally, vulnerabilities with alerts exceeding one million include:

- CVE-2016-3324: Microsoft Internet Explorer and Edge Remote Memory Corruption Vulnerability. Alert count: 6.2 million
- CVE-2017-0146: Windows MS17-010 Series Vulnerability Scanning Attack. Alert count: 1.54 million

0-Day Vulnerability Exploitation on the Rise

As threat actors enhance their attack techniques, the number of zero-day vulnerabilities and their exploitation has significantly increased. Numerous threat actors exploit undisclosed and unpatched vulnerabilities to gain unauthorized access, steal data, or engage in other malicious activities. Exploiting such vulnerabilities is often highly covert and aggressive, making security defense and response more challenging. NSFOCUS's monitoring indicates that in 2023, attackers actively exploited several zero-day vulnerabilities, including (but not limited to):

- CVE-2023-20269: Unauthorized Access Vulnerability in Cisco ASA and FTD Software
- CVE-2023-41064: RCE Vulnerability in Apple ImageIO
- CVE-2023-41061: RCE Vulnerability in Apple Wallet Frameworks

Key Vulnerabilities

Office systems remain a core risk area. The complexity, diverse functionality, and widespread use of office software provide ample attack surfaces for potential vulnerabilities. Within office systems, sensitive data, business information, and employee details are stored, making them high-value targets for attackers.

Windows, as a widely adopted operating system, continues to face security challenges due to its large user base and intricate system structure, resulting in a considerable number of vulnerabilities.

Cybersecurity Trends

01 Java Applications and ESXi as Ransomware Hotspots

- Java applications have become a primary attack surface for ransomware.
  In May 2023, the TellYouThePass ransomware group launched large-scale attacks, and NSFOCUS CERT received multiple reports of ransom attacks with the ".locked1" file extension.
- ESXi caught the attention of more ransomware groups.
  As VMware ESXi becomes one of the most popular virtualization platforms, numerous ransomware groups are now targeting ESXi platforms with encryption programs. Interestingly, these ESXi encryptors often exhibit high similarity across different ransomware groups.

02 Malware Tactics Evolve and Social Engineering Attacks Remain a Concern

- Increased Abuse of Cloud Infrastructure Services
  While cloud services offer convenience, they also provide opportunities for attackers to conduct highly covert phishing attacks leveraging the cloud's high credibility.
- Rise of Phishing via Social Software Channels
  Emergency event statistics from 2023 indicate a noticeable increase in attackers using instant messaging apps for phishing. Common attack methods include resume delivery, remote technical guidance, and forwarding of superior notifications.

03 Cybersecurity Risks Amid the AI Wave

- AI-based social engineering attacks are becoming increasingly rampant.
  With the development of large language models and widespread use of generative AI, incidents of AI-driven voice alteration and deepfake-based online fraud are on the rise.
- Emerging risks of data leakage and misuse.
  As AI applications expand, issues related to data misuse, leaks, and securing large models reveal significant risks and vulnerabilities.

04 Automotive Electrification, Connectivity, and Smart Systems Introduce More Cybersecurity Risks

- Enhanced security is needed for smart cars.
  The adoption of "cloud-edge-device" automotive IoT architectures exposes both vehicle-side and cloud-side risks.
- Smart cars urgently need to strengthen data protection.
  Unorganized management of massive connected vehicle data and user personal information directly impacts public safety and property.

05 Cloud Security Awareness Must Improve When Kubernetes Gains Prominence

- Security of the K8S cluster console requires special attention.
  The web console for Kubernetes clusters provides access and management capabilities for the entire cluster or multiple clusters. Any password leaks or loss of control over permissions in the console could jeopardize the entire cluster's security and expose critical information to threat actors.
- Insecure container configurations have become a weak point in cloud security.
  Kubernetes cluster security risks often stem from inadequate cluster or container configurations.

06 Direct and Common Attack Techniques in Geopolitical Cyber Conflicts

- DDoS attacks are the primary method of cyber warfare.
  From the 2022 Russia-Ukraine conflict to the 2023 Israel-Palestine conflict, cyberattacks closely correlate with physical warfare. One prevalent form of cyberattacks is Distributed Denial of Service (DDoS) attacks.
- Critical infrastructure is the main target of cyber warfare.
  Since the start of the Israel-Palestine conflict, threat actors have extensively targeted critical infrastructure in large-scale network attacks.