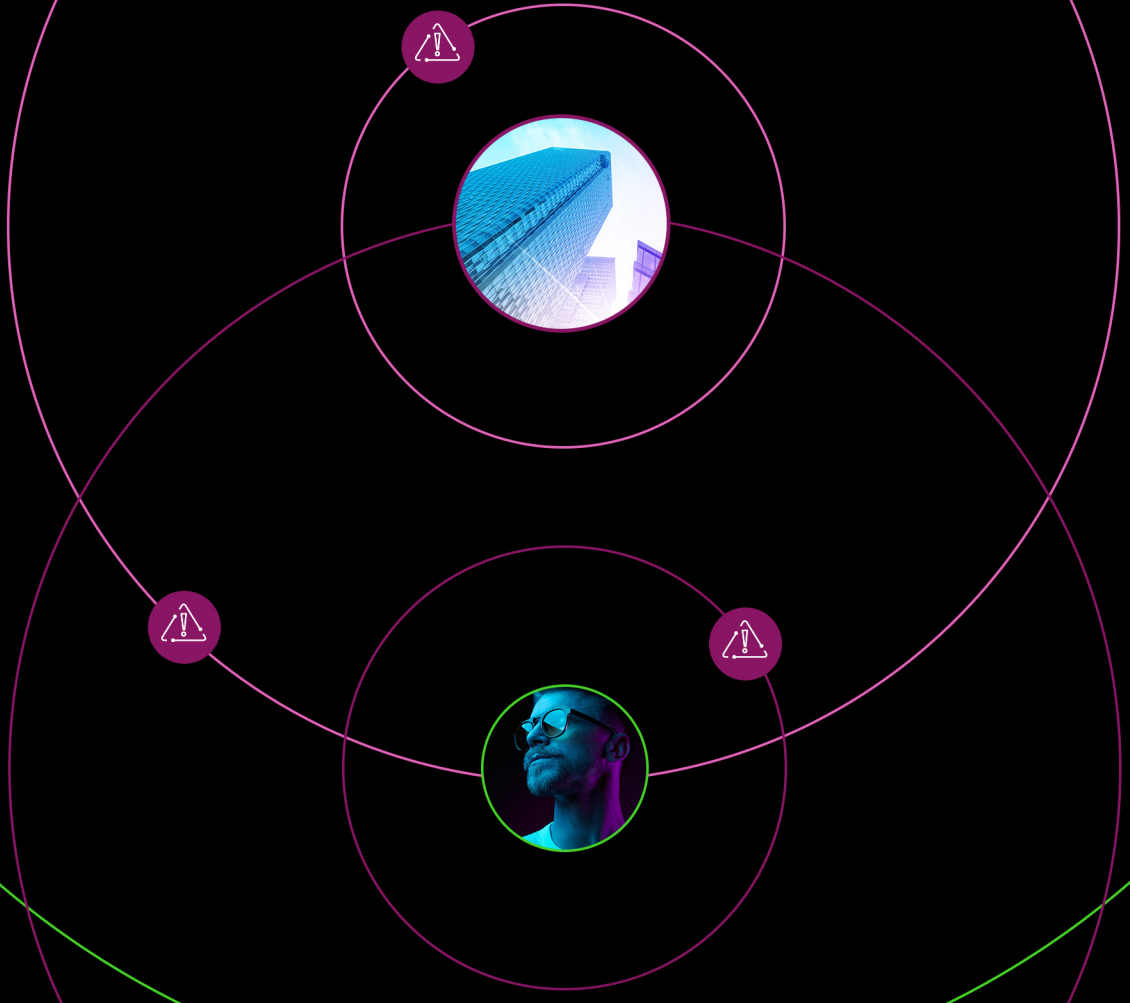
BLACK KITE

2024

THIRD-PARTY BREACH REPORT



ZERO-DAYS CREATED A THIRD-PARTY BREACH YEAR

EXECUTIVE SUMMARY

In the rapidly evolving world of cyber threats, 2023 has unfolded a complex tapestry of third-party data breaches, underscoring the critical vulnerabilities businesses face in their extended networks. Black Kite's comprehensive analysis of these incidents offers invaluable insights, charting the contours of an increasingly intricate cyber threat landscape.

The past year witnessed 81 third-party security breaches, impacting 251 companies—a stark reminder of the pervasive risks associated with third-party vendors. Despite a slight decrease in the total number of affected companies compared to 2022, the data reveals a significant trend: the average number of companies impacted per vendor incident has dropped from 4.76 to 3.1. This shift suggests a growing awareness and perhaps an improved response to mitigating the spread of breaches through vendor networks.

A critical finding from our analysis is the predominance of unauthorized network access as the leading cause of breaches, accounting for over half of the incidents. This trend not only highlights the persistent threat of network penetration but also the sophistication with which attackers exploit vulnerabilities. Notably, the exploitation of MOVEit and GoAnywhere vulnerabilities marked significant breach events, emphasizing the need for rigorous software security practices.

In an era where ransomware attacks have become a common headline, 2023 saw a relative decrease in ransomware-related third-party breaches. However, the impact of such attacks remains substantial, with the ransomware group CL0P emerging as a notably successful exploiter of network vulnerabilities.

The report also sheds light on the sectors most at risk, with technical services vendors leading the breach statistics for the fourth consecutive year. Despite this, a silver lining emerges as a significant portion of these vendors demonstrated improvements in their cyber ratings post-breach. The healthcare sector continues to bear the brunt of these incidents, reinforcing the need for heightened security measures within this critical industry.

One of the more encouraging trends of 2023 is the improvement in breach response and disclosure. The time taken to disclose breaches has significantly decreased, with companies now reporting incidents within 76 days on average, compared to 108 days in the previous year. This progress indicates a positive shift towards transparency and promptness in addressing cyber threats.

As businesses navigate the challenges posed by third-party breaches, the insights from 2023 offer a roadmap for enhancing cybersecurity resilience. The data underscores the importance of vigilant software security, the potential for recovery and improvement post-breach, and the critical need for rapid breach disclosure.

In conclusion, the landscape of third-party breaches in 2023 reveals a complex interplay of risks, responses, and resilience. For businesses, the lessons are clear: enhance vigilance, foster transparency, and continuously improve cybersecurity practices. As we look ahead, these insights will be pivotal in shaping strategies to protect against the ever-evolving cyber threats of the digital age.

ABOUT THIS REPORT

This document presents a detailed analysis and aggregation of third-party data breaches that occurred in 2023. Black Kite's 2023 Third-party Report particularly emphasizes the evolving strategies of cyber attacks, the profiles of threat actors involved, the sectors most affected, and a comprehensive review of the most significant breaches of the year.

This report's statistics have been meticulously gathered from a variety of sources, including cybersecurity news platforms, the dark web, Telegram channels, and resources exclusive to Black Kite. To ensure accuracy and coherence, these data have undergone curation and rounds of expert review. It is important to acknowledge that the actual count of data breaches caused by third parties could exceed what is publicly disclosed. Consequently, the figures presented in this report should be regarded as a representative sample, encompassing both the publicly known and undisclosed cyber attacks.

This analysis encompasses 81 distinct third-party incidents over the previous year, which collectively impacted 251 companies. When considering affected victims in a specific incident in the education sector the breaches amount to 1,150. The report encapsulates key insights gleaned and ongoing lessons from these events.

2022

In 2022, 63 attacks on vendors caused third-party breaches: from those 63 attacks, 298 data breaches occurred across impacted companies. In conclusion: 63 hits and at least 298 victims

63

Third-Party Breaches

298

Cascading Data Breaches

2023

81

Third-Party Breaches

251

Cascading Data Breaches

3.1 Victims Per Breach

We consider the 890 schools impacted by a vendor in a single incident as one victim to avoid skewing the numbers.

2023-Spotlight:

CASCADING DATA BREACHES IN THE EDUCATION SECTOR

81

Third-Party Breaches

1150

Cascading Data Breaches (Including 890 schools)

14.1 Victims Per Breach

Table of Contents

Key Findings

As software vulnerabilities take the stage, companies are now more vigilant in breach disclosures!

By comparison, 2022 has seen 63 vendor-related attacks, resulting in data breaches at 298 companies. Although this number of breaches didn't fluctuate greatly from the previous year, the average number of affected companies per vendor decreased from 2022 onwards, dropping the ratio from **4.76 to 3.1.**

In 2023, unauthorized network access continued to be the leading cause of third-party cyber attacks, a trend consistent with previous years. However, this year marked a notable increase, with such breaches constituting 53.6% of the third-party incidents analyzed. *While this term frequently appears in breach disclosures, the specific techniques used in these unauthorized access incidents often remain undisclosed or undiscovered.*

Numerous breaches were initiated by exploitation of software vulnerabilities, with notable breaches caused by the exploitation of MOVEit and GoAnywhere vulnerabilities. Although these are not classified as third-party breaches, these vulnerabilities considerably impacted the number of breaches observed this year.

Ransomware continued to significantly impact vendors, leading to notable data breaches for their clients in 2023.

An interesting point from 2023 is that unauthorized network access caused the majority of the breaches, with the ransomware group CL0P benefiting more from this than other groups through ransomware attacks. This implies that many companies are not aware of how they are being infiltrated.

In 2023, breaches caused by **81 vendors affected a total of 251** companies.

Once again, the **healthcare sector was the most common victim** of third-party data breaches, accounting for 33% of the cases in 2023.

Vendors in technical services remained the predominant source of third-party breaches for the fourth consecutive year, comprising 35% of incidents. Additionally, software providers continued to be the second most common vendor type of such breaches.

This year marked a new trend in which types of vendors experienced the most breaches. Despite the fact that technical service providers experienced the majority of breaches, more of these vendors improved their cyber ratings by more than 11 points (60%). **The next industry with improved cyber ratings over 11 points was Healthcare Services (20%).**

Once again, the healthcare sector was the most common victim of third-party data breaches, accounting for 33% of the cases in 2023. This trend has been consistent for several years in a row.

Despite the consequences of these incidents and breaches there was a positive result as well. **A significant percentage of the vendors (40%) increased their cyber scores following the attacks.** We also saw an improvement in breach disclosure. In 2023, the breach disclosure period decreased to 76 days from 108 days in 2022. Black Kite has been tracking this statistic since 2021.

Continuing the annual trend, in 2023, the majority of companies impacted by these incidents were once again predominantly based in the United States.

Countries of Companies Experiencing Third-Party Breaches in 2023

U.S. corporations consistently face breaches caused by vendors. The appeal to cyber attackers is driven by U.S. companies' high digital presence (e.g., data assets, cloud use, etc.) and significant financial resources. Additionally, the rigorous data protection and cybersecurity regulations in the United States require detailed breach reporting, which further amplifies the visibility of these incidents.

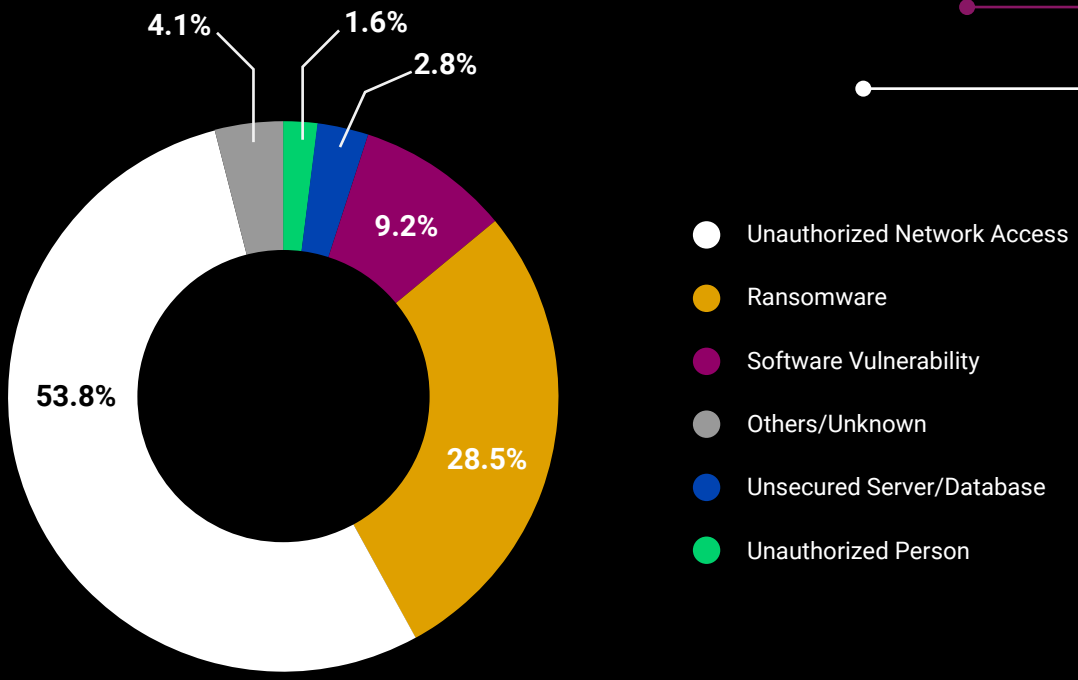
The Evolution of Third-Party Data Breaches

In 2023, there was a marked increase in the number of companies falling victim to data breaches through third-party providers. Although there was a decrease in breaches via third-party providers compared to the previous year, the impact of these incidents on businesses intensified.

A key difference in the cyber threat landscape between 2023 and 2022 was the dramatic rise in ransomware attacks. The exploitation of publicly known vulnerabilities primarily fueled this surge. While unauthorized network access continued as the most commonly reported entry point for breaches, ransomware was the most frequently used attack vector for these breaches – especially through exploiting known vulnerabilities. This trend highlights the tactic of threat actors in leveraging existing vulnerabilities to orchestrate and execute ransomware attacks effectively.

40% of companies that suffered from a data breach caused by a vendor were indirectly affected by CL0P's mass exploitation of vulnerabilities in MOVEit and GoAnywhere. The vulnerabilities in these products were used by vendors, leading to a data breach for these companies. **The average annual revenue of these affected companies is approximately $10 billion.**

The Root Causes of Breaches



Unauthorized Network Access

Over the past three years, unauthorized network access has consistently been the most prevalent reason of data breach as disclosed by the companies, a trend that persisted in 2023. This predominance in breach disclosures is often attributed to companies' reluctance to divulge detailed information regarding the breach's specifics.

In 2023, unauthorized network access was responsible for over 53.8% of all third-party breaches, representing a 26% increase from 2022. The prevalence of unauthorized network access breaches is especially true for companies with revenues over $6.10 billion.

Nevertheless, these incidents, originating from unauthorized network access, underscore the existing vulnerabilities within the network security protocols of third-party vendors. Despite concerted efforts to enhance cybersecurity measures, attackers continue to adeptly exploit gaps in network access controls, thereby gaining unauthorized entry into systems.

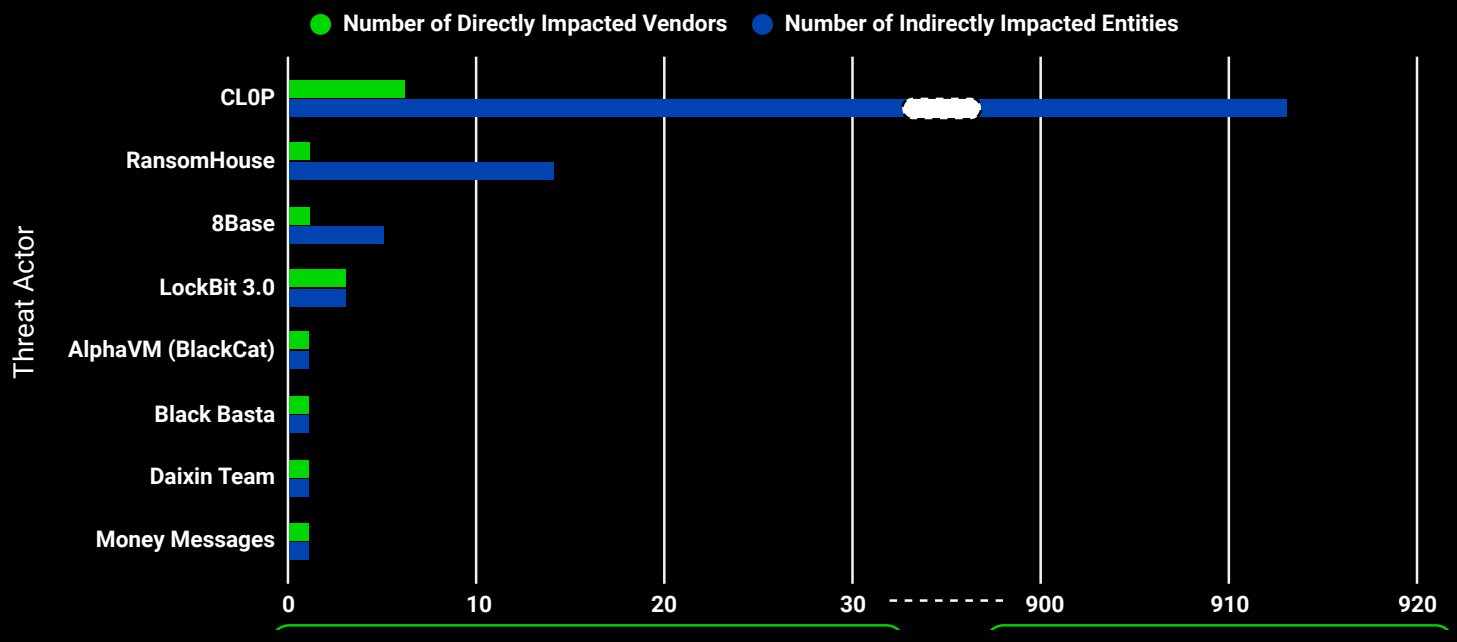
53.8% of all third-party breaches, representing a 26% increase from 2022.

Ransomware

This year, ransomware maintained its position as the second most common cause of third-party breaches, constituting 28.5% of such incidents. Despite a decrease in the overall number of ransomware attacks linked to third parties compared to 2022, threat actors, notably CL0P, have realized more significant gains this year. Companies with revenues exceeding $10 billion have been particularly impacted, suffering substantial losses due to these ransomware attacks.

The CL0P ransomware group executed cyber attacks, primarily targeting prominent companies and institutions. The group encrypted sensitive data (PII/PHI/PCI, etc.) and demanded ransoms. Utilizing security flaws and advanced penetration methods, CL0P infiltrated networks, capturing crucial information. These attacks impacted not only the direct targets but also their clients, affiliates, and entire supply chains. These incidents underscored the severity and far-reaching consequences of zero-day vulnerabilities and ransomware in the realm of cybersecurity.

This year, ransomware maintained its position as the second most common cause of third-party breaches, constituting 28.5% of such incidents.



Software Vulnerabilities

In the past year, software vulnerabilities have significantly contributed to data breaches caused by third partiess, representing more than 9% of the primary causes.

2023 has seen a notable uptick in these incidents, with the infamous CL0P group exploiting every vulnerability they could discover. This group's activities have resulted in substantial data leaks across numerous companies, highlighting the ongoing struggle against cyber threats.

The rise in software vulnerabilities has notably facilitated cybercriminals' ability to penetrate systems and exfiltrate sensitive information. Among these, zero-day vulnerabilities — flaws unknown to the public and unpatched by developers — stand out as particularly perilous. These vulnerabilities enable attackers to circumvent established security protocols and access vital data. Because these vulnerabilities tend to be present in many applications, it allows cyber criminal groups to easily create a single exploit that can be used by several companies — amplifying the impact of a single vulnerability on the overall security landscape. Although software developers routinely release updates to address security weaknesses, the prompt application of these patches by organizations is crucial for effective cyber defense.

The MOVEit data breach exemplifies the cascading impact of such cyber incidents. Originating from the National Student Clearinghouse (NSC), this breach extended its effects to an extensive network, ultimately impacting 890 educational institutions as fourth-party entities.

Another cascading effect of the data breaches due to MOVEit vulnerability started with Welltok, a subsidiary of Virgin Pulse. The breach created a domino effect, impacting 20 healthcare institutions and hospitals.

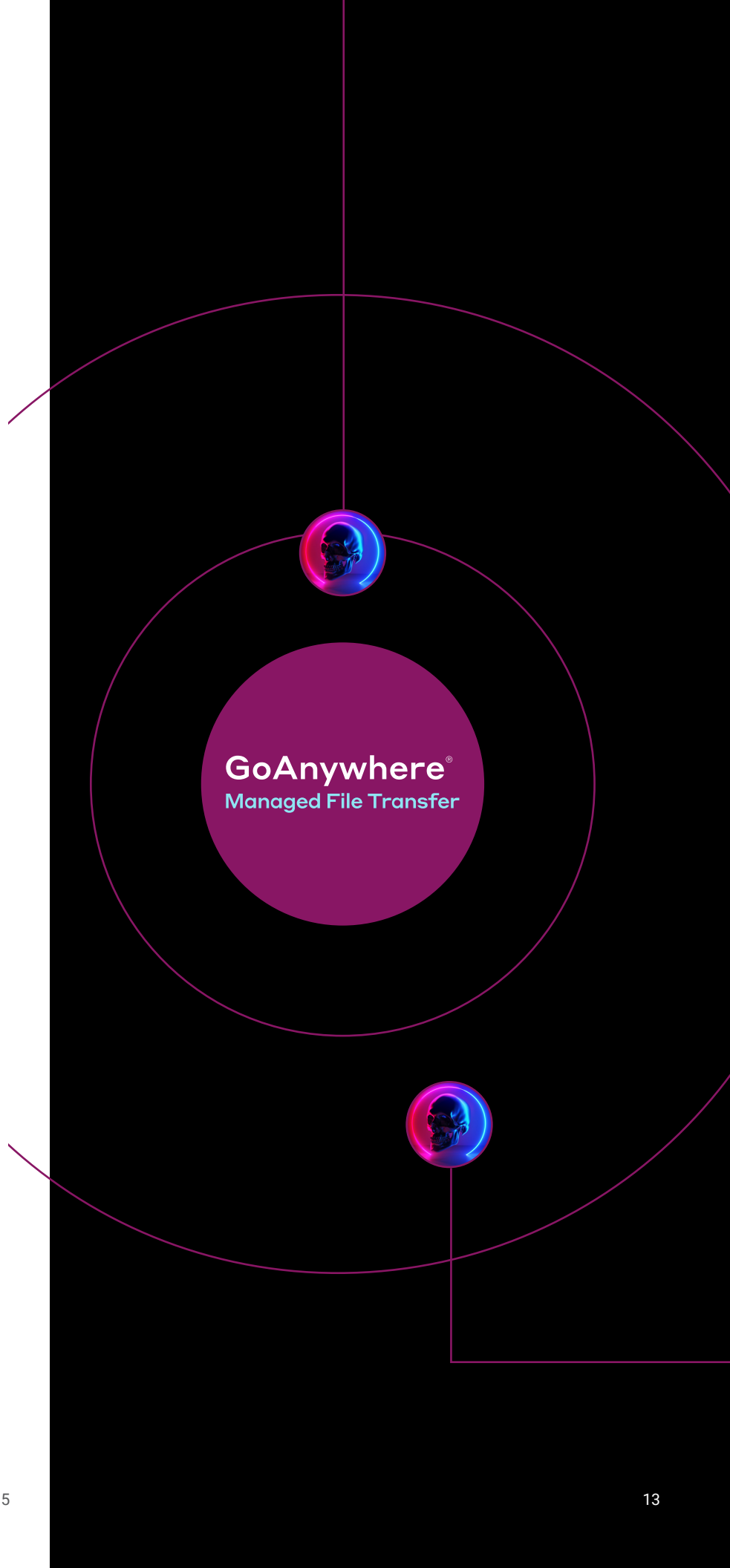
GOANYWHERE

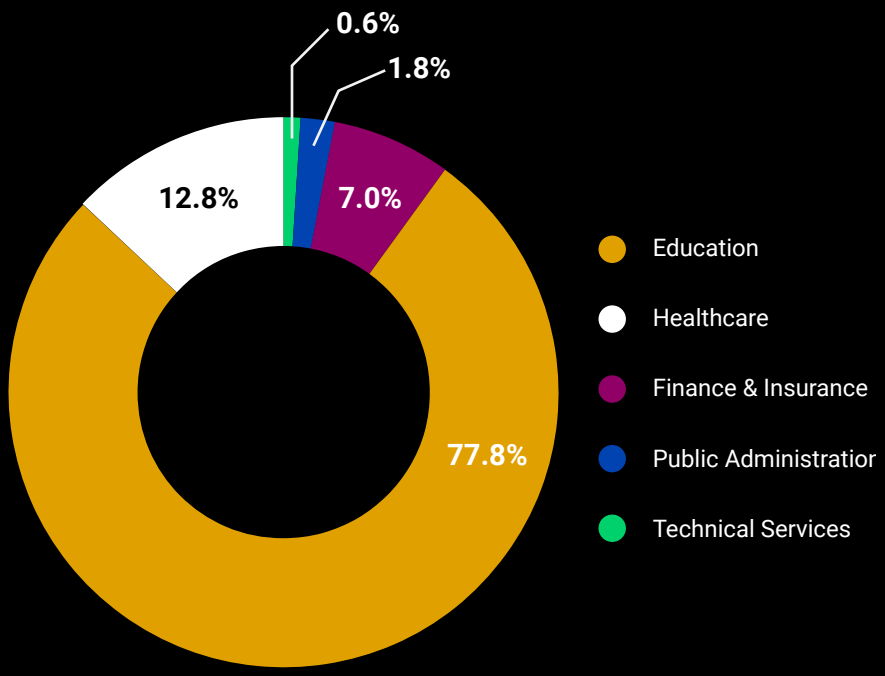
A critical zero-day vulnerability, CVE-2023-0669, was found in Fortra's GoAnywhere Managed File Transfer (MFT) solution in 2023.

This vulnerability allowed for remote code execution, enabling unauthorized access to the system. The CL0P cybercriminal group discovered and exploited this vulnerability in the GoAnywhere software, which is used mostly by large/high-revenue companies and institutions.

CL0P leveraged the vulnerability to gain access to the management console, create unauthorized user accounts in the MFT environments, and engage in malicious activities. These activities included stealing sensitive data like personal, customer, and financial information and installing additional tools such as Netcat and Errors.jsp to infiltrate further and control the systems.

CL0P exploited this vulnerability in hundreds of organizations. In a rapid response, Fortra issued patches and updates to the affected customers to reduce the risk. Nevertheless, the security of numerous companies' data was already compromised. Following reporting the vulnerability, Black Kite promptly integrated GoAnywhere vendors into its monitoring system, reflecting the cybersecurity community's quick action in response to this significant threat.





MOVEit

In May 2023, MOVEit, the file transfer software, formed the basis of a massive breach due to a critical security vulnerability in its software.

This vulnerability, which allowed SQL injection, enabled attackers to access MOVEit's database and steal vast amounts of data by deploying web shells within minutes. The impact was notable due to the diversity and size of the affected organizations, including many large companies with average revenues exceeding $27.96 billion.

The National Student Clearinghouse

The education sector faced the most substantial data loss in recent years due to MOVEit vulnerability. The National Student Clearinghouse (NSC), a non-profit organization for reporting in the education sector, was particularly an interesting party in this attack. The breach further cascaded into 890 more education institutes through this vendor.

The breach further cascaded into 890 more education institutes through this vendor.

Brightline Health

Brightline Health, a provider of virtual coaching and therapy services for children, was part of a large-scale attack by the CL0P ransomware group, stemming from a vulnerability in the MOVEit transfer software. The attack affected more than 130 companies, including Brightline Health, and leaked data from their GoAnywhere systems. This incident affected more than 36 companies that provide healthcare services specifically for children.

This incident affected more than 36 companies that provide healthcare services specifically for children.

What Did Black Kite Do?

Brightline Health

hellobrightline.com

- Data Breach (90+ days)
- Ransomware (90+ days)
- MOVEit

Capespan

capesapan.com

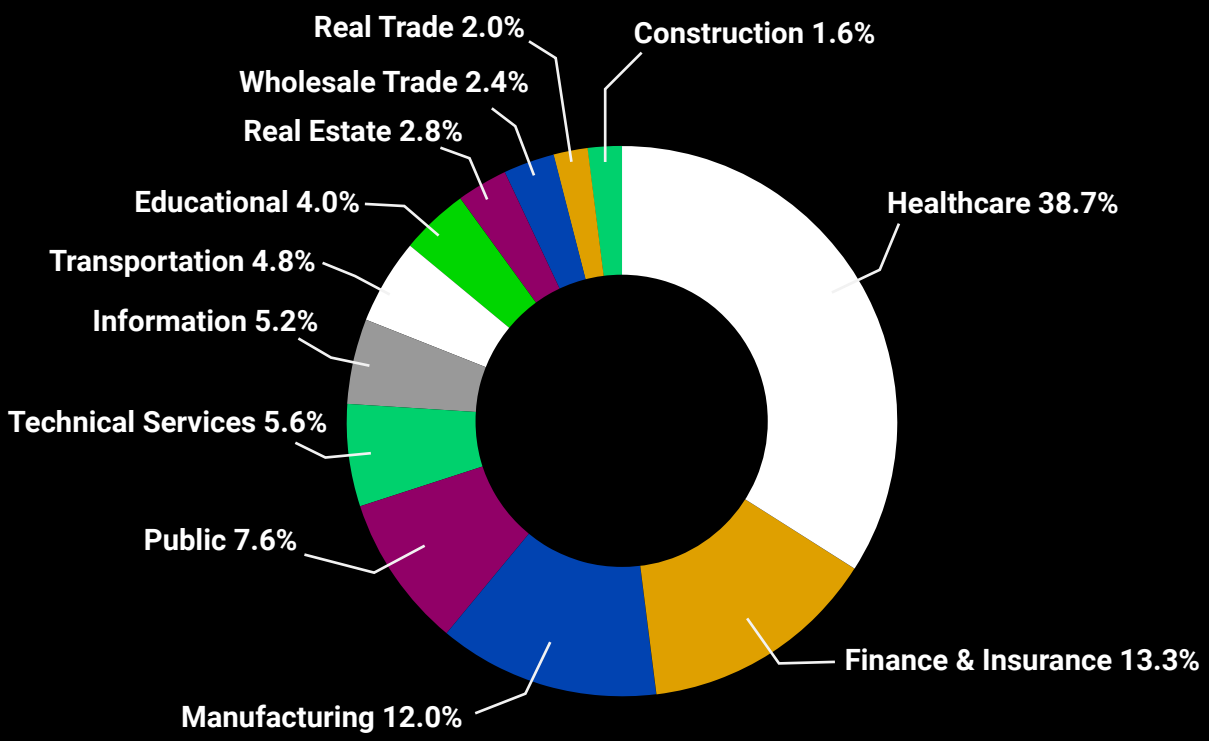
- Data Breach
- Ransomware
- MOVEit

Black Kite detected an announcement made by the CL0P ransomware group claiming responsibility for attacks exploiting the MOVEit vulnerability and was able to provide a Focus Tag™ on this topic. Black Kite identifies companies that have suffered a Data Breach or Ransomware attack using tags. Companies are tagged based on curated information in public sources (public announcements, disclosures, cybersecurity reports, posts on community forums, etc.). Some of the tags related with breaches are:

Data Breach: Company suffered from a data breach.

Ransomware: Company became a victim of ransomware.

Industries Most Affected by Third-Party Data Breaches



Education and healthcare industries rely on tools like MOVEit due to the need to manage large data sets and sensitive information. These industries are highly regulated to protect personal information and health records. Therefore, breaches may have more devastating consequences in these areas.

Third-party providers' security vulnerabilities can also have knock-on effects on their customers' customers. The MOVEit attack exposed their security implications.

Educational Services

In 2023, More than 890 educational institutions experienced third-party breaches due to the National Student Clearinghouse. Third-party attacks had a serious impact on the education sector caused by the MOVEit vulnerability. In particular, ransomware attacks and data breaches targeted schools and universities. These attacks led to the leakage of student and staff information, interruption of educational processes, and damage to corporate reputation. These events, which emphasize the need for educational institutions to increase cyber security measures, also reveal the difficulties in protecting the personal data of students and education personnel. These attacks made it clear that the education sector needs to be better prepared against cyber threats.

Healthcare

In 2023, 32.7% of attacks targeted the healthcare sector. Threat actors managed to leave major wounds in the health sector in 2023.

In 2023, the healthcare industry was seriously affected by ransomware attacks. At least 141 hospitals were directly affected as a result of ransomware attacks on 46 hospital systems, the information of which Black Kite researchers were able to access. These attacks resulted in loss of access to hospitals' IT systems and patient data, caused emergency services to be diverted to other facilities, and caused delays in diagnosis and treatment. Additionally, the cost of data breaches in the healthcare industry has reached a record high in 2023, rising to an average of $11 million. Although these attacks were not directly linked to patient deaths, an increase in post-attack medical complications and death rates was observed. This situation highlights the urgency of increasing cybersecurity measures in the healthcare sector.

Finance And Insurance

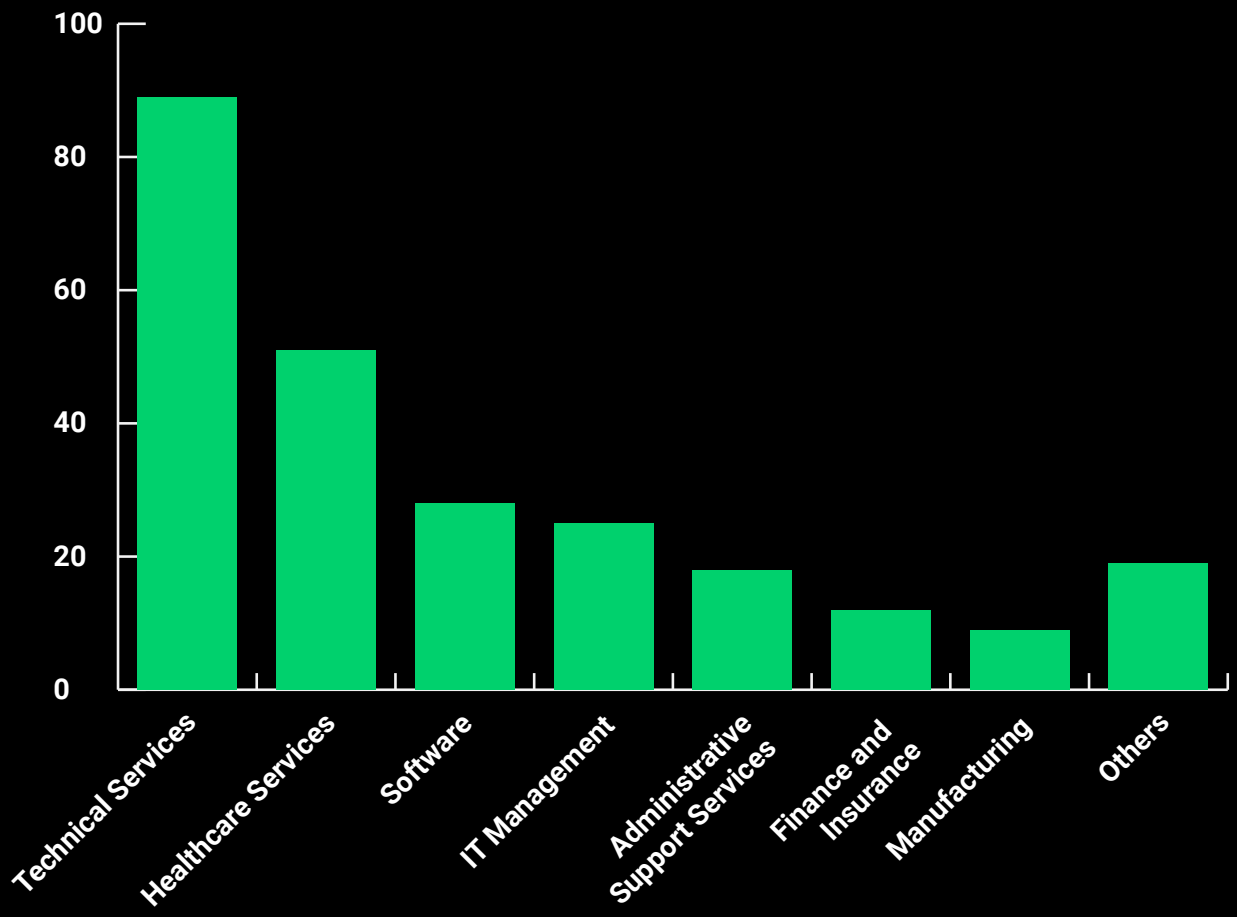
In 2023, 13.3% of attacks targeted the Finance And Insurance sector.

A significant portion of third-party data breaches in the finance and insurance industry have affected millions of people. For example, the largest data breaches experienced by financial services companies affected customers ranging from 10,000 to 37 million people. The attacks were carried out using methods such as system hacking, phishing, malware, and ransomware.

In particular, targeting the MOVEit file transfer system by the CL0P ransomware group affected many companies in the financial services and insurance sectors. These attacks led to companies leaking sensitive information about their customers and also caused companies in the financial and insurance industries to re-evaluate their cybersecurity measures.

These attacks highlight the need to manage third- and especially fourth-party risks and constantly update security systems.

The Most Affected Vendor Industries



2023 was a tiring and devastating year for vendors in technical services.

They were the vendors most at risk in terms of third-party breaches. Technical services typically serve a broad customer base. This means that a single vulnerability can affect multiple organizations. Therefore, it offers cybercriminals the chance to achieve maximum impact through a single target. The rapid digital transformation, especially after the COVID-19 pandemic, has caused many companies to switch to digital solutions quickly. This has led to the adoption of new technologies without adequate integration of security measures. Even though security measures increased with developing technologies, threat actors did not remain idle.

Most Destructive Third-Party Breaches of 2023

PERRY JOHNSON & ASSOCIATES, Inc.

In March 2023, Perry Johnson & Associates (PJ&A) came to the fore with a significant data breach. PJ&A is a company that provides medical transcription services to healthcare organizations and physicians. This breach affected 8.95 million patients' names, dates of birth, addresses, medical records, and hospital account numbers, admission diagnoses, and dates and times of service. Also included were some Social Security numbers and insurance and clinic information.

This information was obtained from medical transcription files and included information such as laboratory and diagnostic test results, medications, treatment facility names, and healthcare providers.

This breach had a particularly serious impact on large healthcare systems like Northwell Health. Northwell Health confirmed that 3.89 million of its patients were affected by this data breach. PJ&A's customers include Cook County Health in Illinois, which said the breach affected 1.2 million of its patients.

PJ&A's customers include Cook County Health in Illinois, which said the breach affected 1.2 million of its patients.

CREDIT CONTROL CORPORATION

The attackers first obtained an employee's credentials with a phishing attack and used this information to infiltrate the systems.

Credit Control Corporation (CCC) is a large company in the financial services field. In May 2023, a vulnerability was detected in CCC's API interface. This vulnerability allowed attackers to infiltrate systems and access sensitive data. The attackers first obtained an employee's credentials with a phishing attack and used this information to infiltrate the systems. They then accessed the database using a weak API (Application Programming Interfaces) endpoint and stole customers' names, addresses, Social Security numbers, credit card information and other financial details.

The company has reviewed its cybersecurity policies and procedures and strengthened security measures such as firewalls, monitoring systems and regular penetration testing. It has also increased awareness of phishing and other cyber threats by investing more in employee training programs. Unfortunately, the regret that comes later does not bring losses.

ESO SOLUTIONS

In 2023, ESO Solutions, Inc. suffered a significant data breach. ESO Solutions is a company that provides software solutions for hospitals, healthcare systems, emergency medical services, and fire departments. The breach occurred as a result of a ransomware attack on the company's systems and affected approximately 2.7 million individuals.

As a result of the ransomware attack, some of ESO's computer systems were encrypted, and sensitive patient information was captured in the process. The breach leaked information such as patients' names, dates of birth, types of injuries, dates of treatment, types of treatments, and, in some cases, Social Security numbers.

This incident also affected some hospitals and healthcare institutions. Some healthcare organizations affected by the breach include Ascension Providence Hospital (Waco), Alaska Regional Hospital, CaroMont Health, Desert View Hospital, ESO EMS Agency, Forrest General Hospital, Manatee Memorial Hospital, Gulfport Memorial Hospital, Merit Health Biloxi, Merit Health River Oaks, Mississippi Baptist Medical Center, Alaska Providence Medical Center, Kodiak Island Providence Medical Center, and Tallahassee Memorial.

The breach occurred as a result of a ransomware attack on the company's systems and affected approximately 2.7 million individuals.

Attackers infiltrated the system by targeting weak authentication mechanisms and inadequate data encryption.

PBI

PBI provides business intelligence and analytics services to various companies. The breach was caused by a security vulnerability in a third-party service provider of PBI. This vulnerability allowed unauthorized persons to access sensitive data, compromising thousands of users' personal and corporate information.

At the heart of the breach were security deficiencies in the APIs and data storage systems used by the service provider. Attackers infiltrated the system by targeting weak authentication mechanisms and inadequate data encryption. This led to data leakage via APIs.

OKTA

In 2023, Okta, a company that specializes in identity and access management, suffered a cybersecurity breach which impacted around 5,000 employees along with one of its customers.

And after that Okta experienced a serious data breach. In this attack on Okta's support systems, all customers' data was affected. A hacker accessed the support case management system using a stolen credential and stole session tokens uploaded by customers, Okta announced in October. These tokens were used to infiltrate Okta customers' networks. Okta initially stated that only 1% of its customers were affected, or approximately 134 organizations.

Upon further analysis, Okta revealed that it had run and downloaded a report containing data on customer support system users. This data included full name, email address, phone number, username and the roles of some employees. Okta stated that for 99.6% of its customers only full names and email addresses were accessed, but in some cases phone numbers, usernames, and details of some employee roles were also accessible.

Okta advised its customers to use multi-factor authentication (MFA) and use authenticators that are resistant to phishing attacks, such as physical security keys. It also noted that Okta's government customers were not affected by this breach and that its Auth0 support case management system was not affected.

99.6% of its customers only full names and email addresses were accessed, but in some cases phone numbers, usernames, and details of some employee roles were also accessible.

Notable Breach

This breach was particularly notable for its technical details, so how did it happen?

It confirmed that in October a hacker accessed the support case management system using a stolen credential and stole session tokens uploaded by customers.

On September 28, a hacker ran and downloaded a report containing data on Okta's customer support system users. This data included full name, email address, phone number, username and the roles of some employees.

The breach involved customers' HTTP Archive (HAR) files. These files are used to record browser activity and contain sensitive data, such as session tokens and cookies. Threat actors can use this information to impersonate users or hijack their accounts. **So, will threat actors be able to obtain this information in the future?**

The Aftermath of an Attack

There was a noticeable improvement in breach reporting times in 2023. The disclosure period in 2022 was 108 days, which was 50% more than in 2021. In 2023, the breach disclosure period decreased to 76 days.

Black Kite started tracking this statistic in 2021, and for the first time since 2021, the time it takes for vendors to notice/disclose their attacks has shortened. **What caused the decrease in response and disclosure time?**

In 2023, companies have made significant progress in detecting data breaches faster. This progress can be attributed to advances in cybersecurity solutions and companies being more motivated to discover breaches because of the increasing costs of data breaches. Companies have become more proactive due to increasing concerns about the financial losses, reputational damage, and legal sanctions of cyber attacks. This fear has led them to invest in advanced threat detection systems and incident response capabilities. Artificial intelligence and machine learning technologies are rapidly identifying anomalies, and companies have improved their processes to comply with regulatory pressure and compliance requirements. These advances have helped detect data breaches at earlier stages and reduce their impact.

Although companies disclosed more quickly, threat actors accelerated even more and launched attacks on hundreds of different companies thanks to a single breach.

We have been attacked. What now?

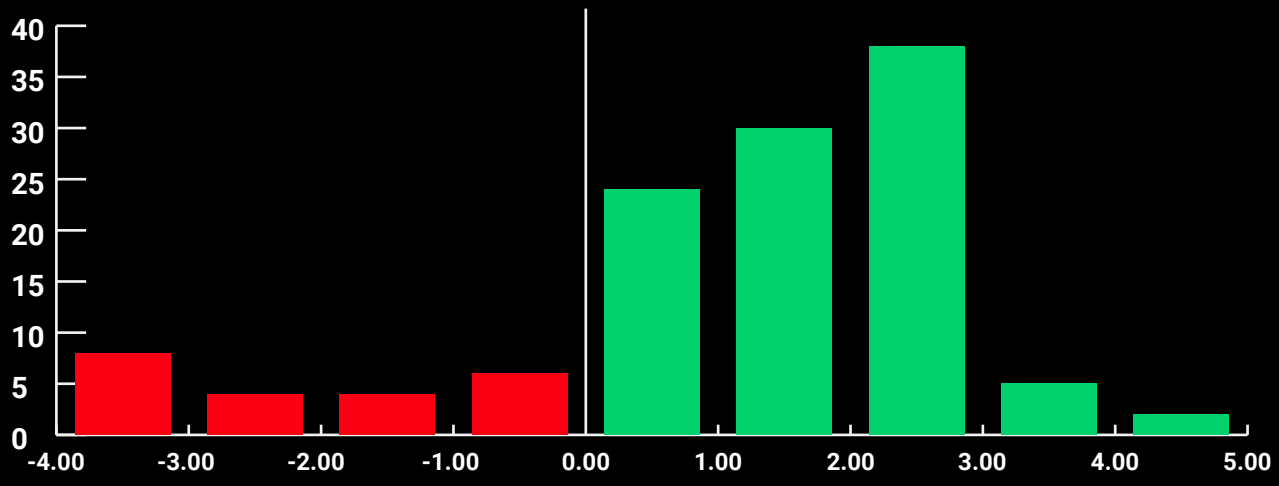
A cybersecurity researcher is always curious about what happens after a cyberattack. Did the company take enough new measures to prevent this in the future? Did they learn their lesson? Could they have taken the measures preemptively?

In 2023, there was an average increase of 1.30 in cyber ratings.

Score Improvers in Post Attack (Top 5)

Score Reduction in Post-Attack (Bottom 5)

Vendor Grade Shifts in Post-Attack



Lessons Learned

1 The collapse of the software provider has had a domino effect on all sectors.

The failure of a software provider has had far-reaching effects on a variety of industries. Recently, there has been a trend among companies to collaborate with more than one software vendor. While this diversification was beneficial for business processes, it also created a weak spot in terms of creating shared data. Attackers exploited this weakness by using the compromised data as a stepping stone to access the information of other companies, including those operating in more critical and sensitive areas. This highlights the increasing complexities and risks associated with data management and the need for robust cybersecurity strategies in an interconnected business environment.

2 Vultures don't just exist in the wild. They also exist in the threat actors

Threat actors, especially CL0P, exploited every vulnerability they found this year. They hovered over the companies like vultures, waiting for them to run a deficit.

3 Companies are quicker to disclose attacks, but threat actors are like Flash!

Although statistics show us that there is an improvement in the time it takes for companies to disclose attacks, unfortunately, we have seen that threat actors act faster than companies before they close their vulnerabilities.

Additional Advice

4 Do not skip on your cyber security while investing in artificial intelligence.

Especially with the development of artificial intelligence, companies spent most of their budgets on this area, but they forgot one important thing. The more they attract the attention of threat actors, the more vulnerable they become to cyber attacks.

BLACK KITE

Conclusion

The insights from 2023's third-party breaches crystallize a crucial lesson for businesses: Continuous monitoring of third-party vendors is indispensable. Point-in-time assessments simply cannot keep pace with the rapidly evolving cyber threat landscape. As the nature and frequency of these breaches reveal, vulnerabilities can emerge and be exploited swiftly, leaving companies at significant risk. The dynamic nature of cyber threats necessitates a vigilant, ongoing approach to third-party risk management.

By prioritizing continuous monitoring, businesses can detect potential vulnerabilities early, respond to threats more effectively, and safeguard their operations against the unpredictable tide of cyber risks. This proactive stance is not just a strategy—it's a necessity for securing the future of digital business integrity.

Black Kite provides security and business experts with the industry's most accurate, timely, comprehensive, and operational cyber risk intelligence.

Insights gained from the award winning-platform ease the stress of the unknown in your cyber ecosystem by automating the process of providing real-time and accurate risk intelligence. With Black Kite, you get more than a simple risk score, you get instant access to reliable qualitative data and detailed remediation prioritization around business, threat and risk scenarios so you can make informed risk decisions about business resilience while continuously monitoring your entire ever-changing cyber ecosystem.