REPORT

Global Third-Party Cybersecurity Breaches

In-depth analysis of the most significant third-party cyber risks and incidents in 2023

SecurityScorecard

Foreword

As organizations become more complex, risks have become more interconnected.

The first edition of the SecurityScorecard Global Third-Party Cybersecurity Breach Report comes at a time when top organizational risks, such as supply chain, cybersecurity, and third-party risks cut across large parts of all organizations.

Stopping supply chain attacks requires understanding their causes and the variables that contribute to them. SecurityScorecard threat researchers assist in that effort by helping organizations gauge their overall risk levels and set priorities for vendor vetting.

Introduction

Cybercriminals continue to exploit the trusted relationships between companies and their third-party suppliers and vendors, resulting in damaging attacks. As cited by the new SEC cybersecurity incident disclosure requirements, SecurityScorecard research discovered that 98% of organizations have a relationship with a third party that has been breached.

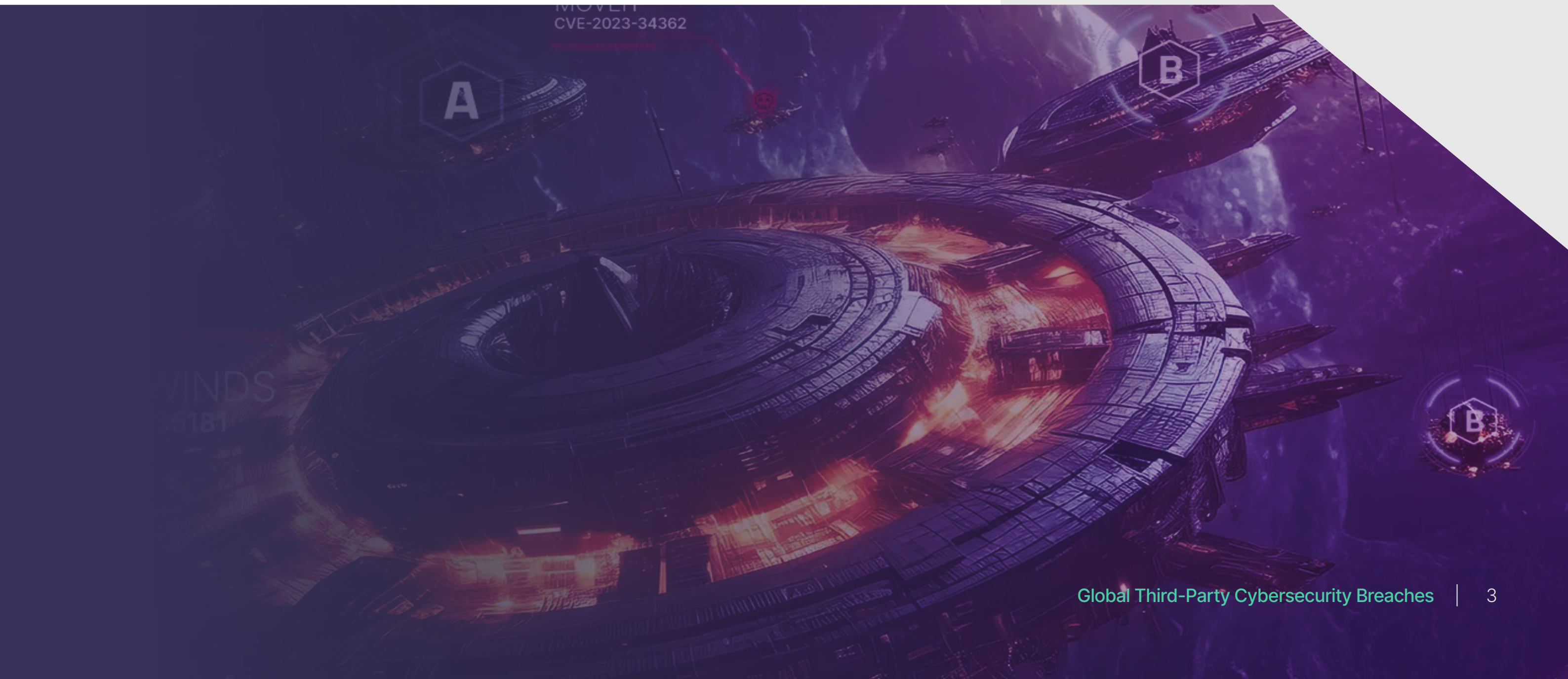
Against that backdrop, this SecurityScorecard research sheds light on third-party breaches in support of third-party risk management (TPRM). Threat researchers examine the frequency of third-party breaches within the overall threat landscape and identify variations in that frequency by industry and geography. It enumerates those external relationships that enable third-party breaches more frequently. It highlights those threat actor groups most active in this arena, as well as the most frequently exploited software vulnerabilities.

BREACH LIKELIHOOD

Companies with an F rating have a

13.8X GREATER

likelihood of a data breach than companies with an A.



Key Findings:

1 **At least 29% of breaches have third-party attack vectors.**

2 The criminal threat group **C10p** (also known as FIN11, TA505, Graceful Spider, Gold Tahoe, SectorJ04, Hive0065, and G0092) **stood out by wide margins as the most prolific perpetrator of breaches in general and even more so for third-party breaches in particular.**

3 The preeminence of C10p was due in large part to its large-scale exploitation of **a zero-day vulnerability in MOVEit file transfer software, which was also the most frequently mentioned vulnerability.**

4 **The healthcare and financial services industries experienced the highest volume of third-party breaches.** Third-party breaches in those two industries constituted the largest and second-largest shares of third-party breaches within our sample, respectively.

5 Third-party breaches in the **technology & telecommunications** vertical were a smaller share of third-party breaches within our sample. This vertical nonetheless had the **highest internal percentage (43%) of third-party breaches.**

6 **75% of external relationships that enabled third-party breaches involved software or other technology products and services.** The remaining 25% of third-party breaches involved non-technical products or services.

7 The frequency of third-party breaches did not appear to vary significantly by country or geographic region, **with the exception of Japan.**

8 **The complex ecosystem of third-party relationships in healthcare,** in which many highly specialized vendors contribute to various phases of the care cycle, **may be one of several reasons why this industry is such a common victim in general and for third-party breaches in particular. Having more third parties creates more third-party risk.** A similar factor may be at work in Japan, whose supply chains have diversified away from its traditional form of vertical integration.

9 Third-party compromises of software or other technology products and services often enable threat actors to scale their operations with minimal effort, **making those actors more prolific than others.**

Methodology

Our sample for this report came from a new, internally developed feed that collects publicly available reporting on breaches. We limited the time frame of our inquiry to reporting collected during Q4 2023, the first full quarter in which our feed has operated. We note that many of the reported incidents occurred earlier in the year. It often takes months or longer for breaches to become public knowledge. It may have taken victims weeks or months to discover a breach, which may not appear in public reporting for weeks or months thereafter (if it ever appears at all). We thus chose to include incidents that occurred earlier in the year to account for this common lag/latency in breach reporting and to avoid discarding otherwise useful data points. Our sample is thus a snapshot of breaches from throughout 2023, with an emphasis on Q4.

29%

of all breaches were attributable to a third-party attack vector.

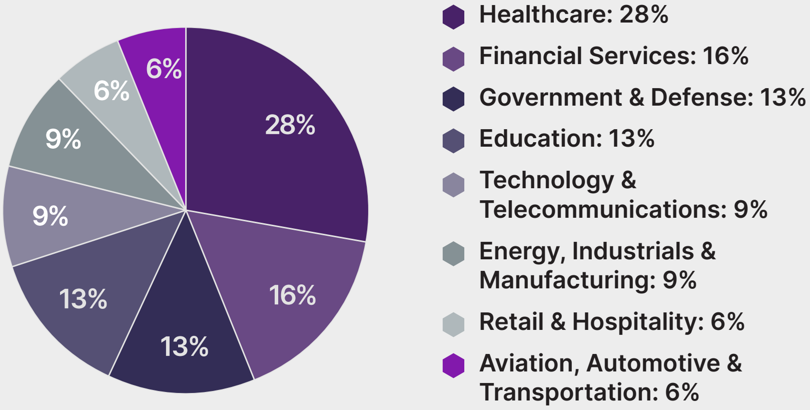
What percentage of breaches are attributable to third-party risks?

Quantitative analysis of our sample indicated that approximately 29% of all breaches were attributable to a third-party attack vector. This figure is nonetheless conservative; the actual percentage of breaches occurring via third parties was probably higher. Many breaches for which the reporting did not mention a third-party attack vector did not specify any attack vector at all. It stands to reason that many incidents with no identified cause could have had third-party origins that the reporting did not mention.

BREACHES
BY INDUSTRY

This pie chart illustrates the distribution of breaches in our sample by industry.

How do breaches vary by industry?



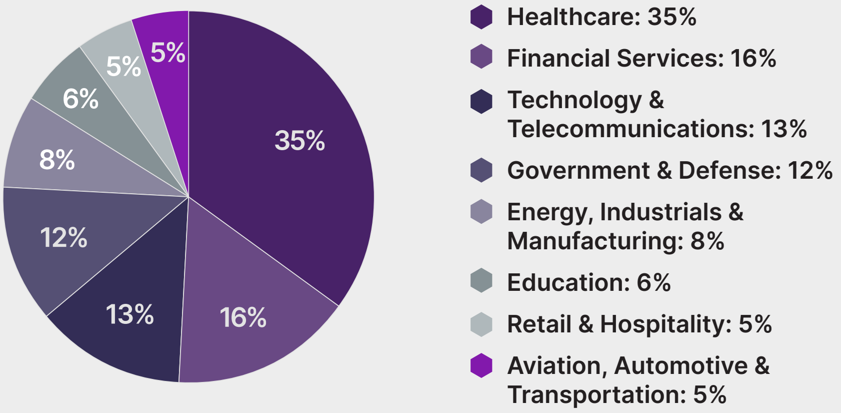
This distribution is not surprising. More than one-quarter of all reported breaches affected healthcare organizations, exceeding the "market share" of all other industries by a wide margin. Healthcare organizations are popular targets for criminals, particularly ransomware operators, for a variety of reasons. The below section on third-party relationships that enable breaches may shed more light on the high volume of breaches in this industry. Financial institutions are another popular target for criminals because they hold the wealth that criminals seek. Financial institutions tend to have stronger defenses, which might explain why they came so far behind healthcare.

National governments and the defense contractors that support them hold highly sensitive information of potentially great value to threat actors. By the same token, their typically stronger defenses make them harder targets than local or state/provincial governments. The latter often lack resources for more robust security programs and are thus perceived by criminals (particularly ransomware operators) as easier targets. Criminals (particularly ransomware operators) may perceive educational institutions as "soft targets" for similar reasons, hence the salience of victims from that industry.

More than one-quarter of all reported breaches affected healthcare organizations, exceeding the "market share" of all other industries by a wide margin.

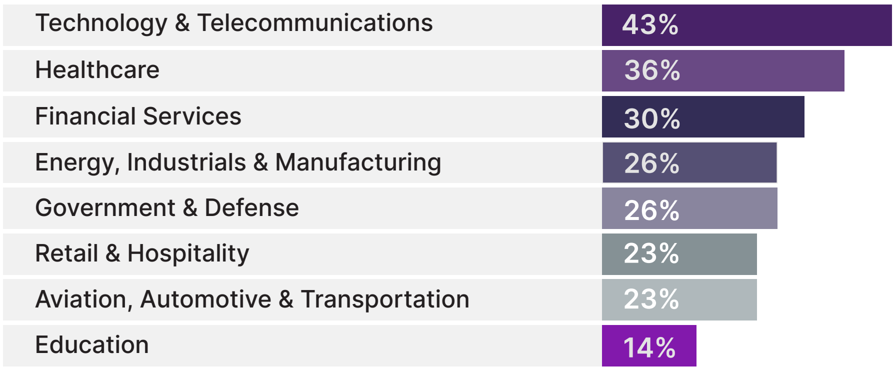
THIRD-PARTY BREACHES BY INDUSTRY

This pie chart illustrates the distribution by industry in the subset of our sample that the reporting identified as third-party breaches.



The above percentages in the pie charts reflect each industry's share of a) the overall sample; and b) and the subset of the sample that reporting identified as third-party breaches, respectively. In contrast, the bar graph below indicates the percentage of attacks within each industry that the sample subset identified as third-party breaches. The rates at which the reported breaches within a given industry had a discernible third-party attack vector are illustrated in the bar graph below. Compare these percentages with the general cross-industry percentage of 29% in the overall sample.

PERCENTAGE OF THIRD-PARTY BREACHES IN EACH INDUSTRY



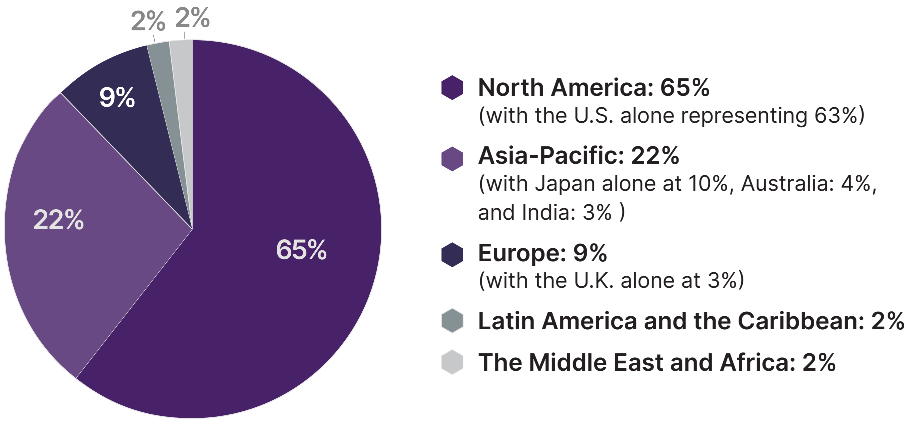
Three industries were the most noteworthy targets of third-party breaches. Once again, healthcare stood out by wide margins. Its 35% share of all incidents with an identifiable third-party attack vector dwarfed those of all other industries. The 36% rate at which breaches within this industry had an identifiable third-party attack vector was well above the general cross-industry rate of 29% and the second-highest in our sample.

The industry with the highest internal rate of third-party breaches was technology & telecommunications at a whopping 43%, exceeding the cross-industry rate of 29% by a wide margin. Technology & telecommunications organizations also had a somewhat larger share (13%) of all reported third-party breaches than their share of all breaches (9%), but not by much. In other words, this industry's share of third-party breaches may have been smaller than those of the healthcare and financial services industries. Still, third-party vectors were a more frequent cause of the less voluminous breaches in this industry than in any other. The below discussion of third-party relationships proposes possible explanations for this distribution.

Financial services stood out in that its share of all reported third-party breaches was the same as its share of all breaches in general (16%) and came in second place in both rankings. Furthermore, the rate at which breaches affecting financial services institutions were attributable to third-party attack vectors (30%) was the closest to the overall cross-industry rate of 29%. Third-party breaches of financial institutions thus represent a large share of the third-party threat landscape but do not seem to affect this industry markedly more or less than other industries or organizations in general.

How do third-party breaches vary by geography?

Geographic variations may be harder to detect due to the overwhelming focus of news media and security vendors on breaches in the U.S. and other English-speaking countries. SecurityScorecard diversified the languages of our sources to provide a more representative sample that gives due consideration to other countries. A disproportionate share of U.S. data points is still unavoidable, given the huge U.S. share of the world economy and the geopolitical prominence of the U.S. Government.

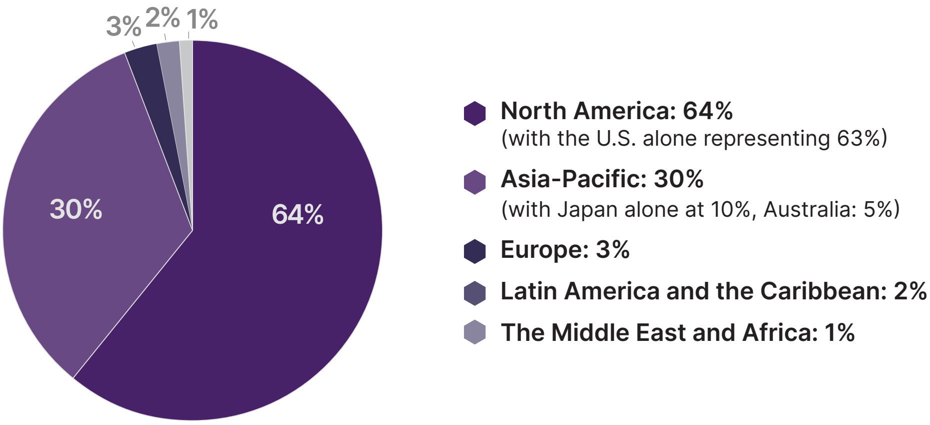


BREACHES BY GEOGRAPHIC REGION

A geographic breakdown of our overall sample, by region and country.

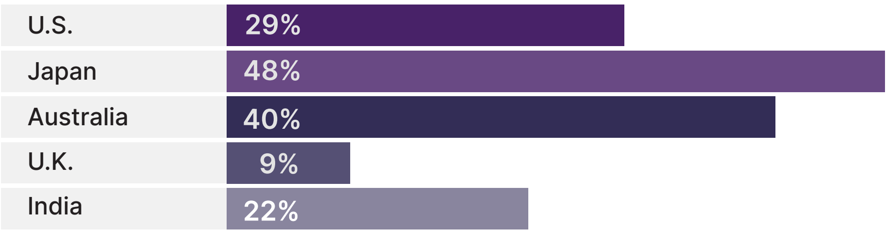
When limiting the data pool to the subset of breaches with identifiable third-party attack vectors, the geographical distribution remained similar.

THIRD-PARTY BREACHES BY GEOGRAPHIC REGION



The respective distribution of third-party breaches for each region and country did not vary much from that of the overall sample, except for the somewhat larger share of third-party breaches in the Asia-Pacific region. That region's larger share of third-party breaches was largely due to Japan and Australia, which is clearer when one considers the percentages of third-party breaches within the top countries' overall breach count.

PERCENTAGES OF BREACHES WITH THIRD-PARTY ATTACK VECTORS IN TOP COUNTRIES



The rate at which breaches were attributable to third-party attack vectors is well above the global rate (29%) in Japan and Australia, representing nearly half of all incidents in Japan. In contrast, the rate at which incidents were attributable to third-party vectors in the U.S. matches the global rate; that may be simply because the U.S. breaches represent such a huge share of the whole sample. The below discussion of third-party relationships responsible for breaches may shed light on Japan's salience in this regard.

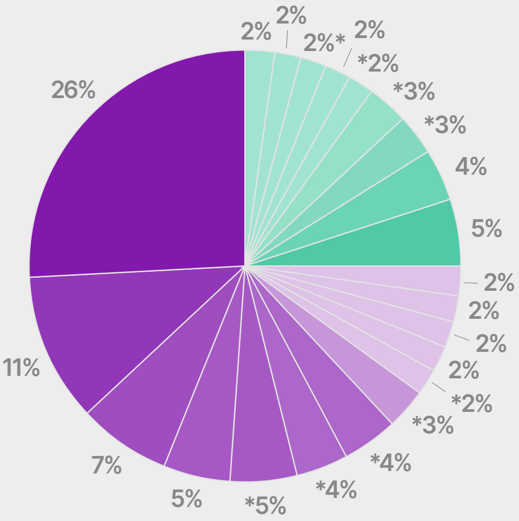
What types of relationships are responsible for third-party breaches?

It is worth asking what types of business-to-business (B2B) relationships enable third-party breaches and the varying frequency with which they do so. If nothing else, it helps TPRM teams set priorities when evaluating vendors. Furthermore, a review of the third-party relationships that enabled breaches in our sample may shed light on why they might affect certain industries or geographic areas more than others.

We divided the B2B relationships that enabled third-party breaches into 22 different categories. The most significant finding was that three-quarters (75%) of these relationships were technical in nature, involving the provision of software or other information technology (IT) products and services. A variety of non-technical relationships were the source of the remaining 25% of third-party breaches.

B2B RELATIONSHIPS RESPONSIBLE FOR THIRD-PARTY BREACHES

The high proportion of breaches attributed to file transfer software reflects C10p's 2023 MOVEit campaign, which is covered in greater detail below. Nonetheless, even if one factors out that potentially anomalous example, the preponderance of technical relationships in third-party breaches is still quite clear from both quantitative and qualitative perspectives. The technical relationships are not only greater in number but also more diversified and often highly specific.



75%
Technical relationships

File transfer software: 26%
Miscellaneous software/technology: 11%
Cloud services/software: 7%
Hosting provider/external platforms: 5%
Doctor/patient communication apps: 5%*
Financial services software/technology: 4%*
Medical transcription services: 4%*
Miscellaneous healthcare software: 3%*
Hospital/EMS/first responder software: 2%*
Human Resources (HR) software: 2%
Security software: 2%
Outsourced software development: 2%
Facilities & connected home management: 2%

25%
Non-Technical relationships

Law firms & other professional services: 5%
Miscellaneous: 4%
Banking services: 3%*
Healthcare billing: 3%*
Healthcare records management: 2%*
Miscellaneous healthcare: 2%*
Automotive supply chain: 2%
Telemarketing services: 2%
Subsidiaries: 2%

** Denotes B2B relationships specific to the healthcare and financial services industries.*

Technology & Telecommunications

The nature and distribution of these third-party relationships may also shed light on why three industries, in particular, stood out in our sample of third-party breach victims. For example, the preponderance of technical relationships may explain why such a high percentage of breaches in the technology & telecommunications industry had third-party attack vectors. The very nature of their work puts them in the most direct and extensive contact with the very same ecosystem of technical B2B relationships that enable a large majority of third-party breaches in the first place. It thus makes sense that organizations in this industry would experience third-party breaches at a higher rate.

Healthcare

The number, diversity, and specialized nature of the healthcare-specific relationships in this sample, technical or otherwise, is striking. Healthcare-specific relationships constitute 7 of the 22 categories, and those 7 categories account for 21% of the relevant relationships. As with the general cross-industry figures, the technical healthcare relationships (14%) outweigh the non-technical healthcare relationships (7%) by a wide margin of 2/1 - less than the cross-industry norm, but still high.

This complex ecosystem of third-party relationships may shed light on why healthcare experiences so many breaches in general and third-party breaches in particular. The healthcare industry has many other distinctive risk factors that may account for its frequent breaches, such as: vulnerable medical devices; a perceived vulnerability to ransomware extortion; the greater usefulness of more detailed PHI for fraud; and so on. We propose that the above ecosystem of more numerous, specialized, and diversified third-party relationships is another distinctive risk factor for this industry. **Simply put, one has more third-party risk if one has more third-party relationships.** The more extensive division of healthcare labor among a greater number of more highly specialized organizations creates more third-party relationships and, thus, more risk.

Third parties like those in our sample participate in a patient's care throughout the process. A patient calling an ambulance may appear in software that a third-party vendor designed for hospitals and EMS. A doctor's notes on the patient may go through a third-party medical transcription service, and another third party may manage those healthcare records. A third-party radiologist or anesthesiologist may participate if the patient needs diagnostic imaging services or surgery. The doctor may use a third-party app for follow-up communications with the patient. A doctor or hospital may retain the services of a third-party medical billing specialist to analyze or collect payment from the patient or insurer. And the patient's insurance provider is, of course, another third party.

Financial Services

The only other industry that is even remotely worth comparing to healthcare in this regard is financial services, which had 2 of the 22 industry-specific relationships in our sample, accounting for 7% of the total. The preponderance of technical relationships in third-party breaches is also clear in this industry, with the majority of this activity being attributed to specialized financial services software or technology.

Japan

The above insights into the healthcare industry may also shed light on Japan's high rate of third-party breaches. For decades, keiretsu networks of Japanese companies, based on long-standing relationships of mutual trust, goodwill, and investment, provided a degree of vertical integration for the Japanese economy and its supply chains. This model remains key to Japanese business culture to this day. Still, since the 1990s, many Japanese companies have shifted toward more competitive, market-driven, and contractual B2B relationships with organizations with whom they may have had little or no prior connection. This point raises the question: do Japanese third-party breaches originate more frequently from within traditional keiretsu alliances, from more "impersonal" outsourcing contracts with relatively new vendors, or from both?

A review of the Japanese third-party relationships that enabled breaches in our sample did not provide a clearer answer, which may come to light with further research.

> "The cost of a third-party cyber breach is typically 40% higher than the cost to remediate an internal cybersecurity breach."[1]

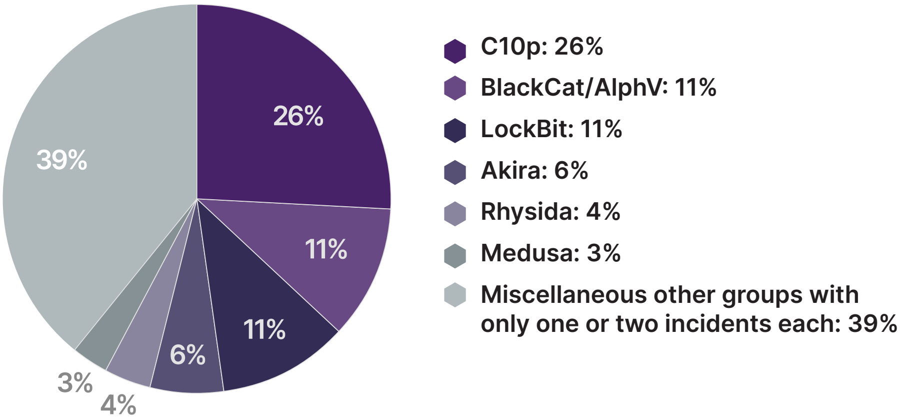
[1] Gartner, "4 Third-Party Risk Principles That CISOs Must Adopt," Luke Ellery, Sam Olyaei, April 11, 2022

PERCENTAGES OF BREACHES ATTRIBUTABLE TO SPECIFIC THREAT GROUPS

PERCENTAGES OF THIRD-PARTY BREACHES ATTRIBUTABLE TO SPECIFIC THREAT GROUPS

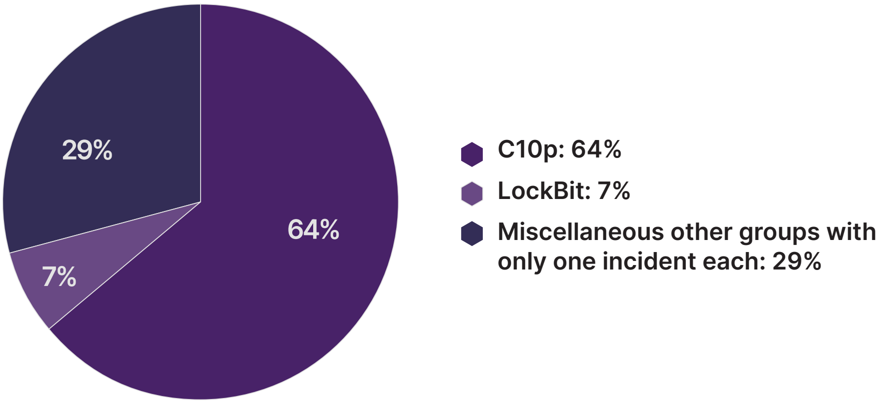
What specific threat groups were responsible for third-party breaches?

Only 29% of the breaches in our overall sample of reporting were attributable to specific threat actor groups. The six most frequently mentioned groups were responsible for more than half (61%) of those breaches attributable to any group. The remaining 39% of breaches attributable to a specific group were attributed to miscellaneous groups that appeared only once or twice in our sample and thus did not warrant further comparison.



Note the vast disparities amongst the various groups, creating an inverted pyramid of market share. C10p's market share was more than twice as large as that of the second-most prolific groups, BlackCat/ALPHV and LockBit. By the same token, the market share of Akira, the third-most prolific group, was just over half that of the two second-most prolific groups. At the very "bottom" of this inverted pyramid are miscellaneous groups responsible for just one or two incidents each.

This disproportionality becomes clearer when limiting the pool to third-party breaches.



One group, C10p, was responsible for almost two-thirds of breaches that both had an identifiable perpetrator and involved a third-party attack vector. Its market share of this subset of breaches was more than nine times as large as that of the next-most prolific perpetrator of third-party breaches, LockBit. None of the other miscellaneous groups - including those that figured far more prominently above in the overall sample - were held responsible for more than one third-party compromise each.

This growing disproportionality in the distribution of breaches among groups makes sense when one considers why threat actors choose common third-party attack vectors in the first place. These methods often enable attackers to compromise large numbers of victims at once, giving their operations far greater scalability. For example, compromising one managed service provider (MSP) could enable an actor to compromise dozens or even hundreds of its customers with relatively minimal effort. It thus makes sense that threat actors using third-party attack vectors more frequently would be responsible for a disproportionately large share of victims.

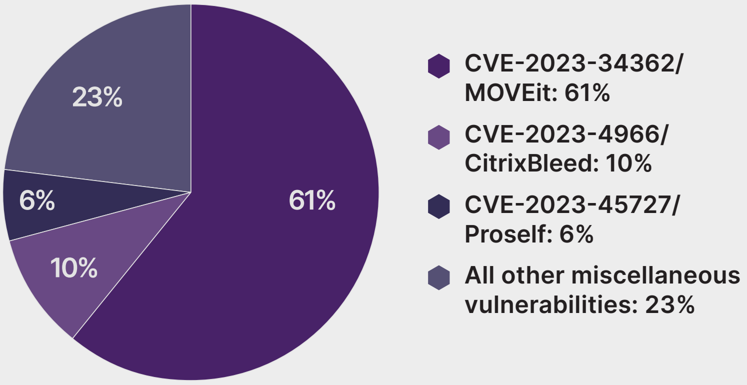
What vulnerabilities did threat actors exploit most frequently?

The above preeminence of C10p is attributable to its mid-2023 campaign, in which it exploited a zero-day SQL injection vulnerability in Progress Software's MOVEit managed file transfer solution (CVE-2023-34362). Newly identified victims of this massive campaign continued to surface in reporting months after the original attacks. The number of breaches involving the exploitation of this vulnerability dwarfed all others in our sample, constituting 61% of those breaches involving a specified vulnerability. Remarkably, new identifications of this campaign's victims continued to represent a significant share of breach reporting in our sample months after the campaign.

Coming in a distant second, at 11%, was "CitrixBleed" (CVE-2023-4966), a buffer overflow zero-day vulnerability in Citrix NetScaler web application delivery control (ADC) and NetScaler Gateway appliances. The exploitation of this vulnerability has been associated with both LockBit and BlackCat/AlphV ransomware attacks.

Coming in a distant third, at 6%, was CVE-2023-45727, an XML external entity reference (XXE) zero-day vulnerability in Proself, an online file storage software for Japanese businesses. All of the reported breaches involving this vulnerability, which received relatively little coverage in English-language sources, occurred in Japan.

None of the other vulnerabilities referenced in our sample appeared frequently enough to warrant comparison with the three above. The three most widely exploited vulnerabilities were involved in 77% of all breaches involving a specified vulnerability; the other miscellaneous vulnerabilities were responsible for the remaining 23%.



One reason for the widespread impact of the MOVEit zero-day was that it not only enabled third-party attacks on Progress Software customers but also enabled “fourth-party” or even “fifth-party” compromises of other organizations. A vendor experiencing such a compromise could affect a large number of its customers, or even customers of its customers, in one fell swoop. It is not a coincidence that all of these examples below involved healthcare organizations in one way or another.

- A MOVEit breach of the professional services firm Westat compromised data for many of its customers, including the U.S. Government’s Office of Personnel Management, as well as healthcare organizations in North Carolina, South Carolina, and Pennsylvania for which Westat managed healthcare data.
- A MOVEit breach of healthcare SaaS provider WellTok compromised the data of 8.5 million patients of healthcare organizations across the U.S., including at least two organizations in Michigan and others in Arkansas, Oregon, and Tennessee.
- A MOVEit breach of Arietis Health, which provided billing and revenue cycle management for NorthStar Anesthesia, affected the PHI of patients of more than 50 U.S. healthcare organizations for which both organizations provided services.
- A MOVEit compromise of Nuance Communications, which provides AI-enabled automatic transcription of clinical notes for U.S. healthcare providers, affected data from at least 13 different U.S. healthcare organizations, including two organizations in North Carolina and one in West Virginia.
- A MOVEit compromise of ESO Solutions, which provides software for hospitals, EMS, and other first responders, affected at least 14 different healthcare organizations in Texas, Alaska, Florida, Mississippi, and other U.S. states.
- A MOVEit compromise of Cadence Bank, which provided treasury management services to healthcare organizations, enabled the compromise of data from healthcare organizations in at least Louisiana and Mississippi.

Recommendations

We present the below recommendations for TPRM teams or other security professionals evaluating their third-party risk landscapes.

- Make TPRM an integral component of your security program and vendor selection processes. SecurityScorecard's platform facilitates and enhances this effort, providing ratings to evaluate prospective vendors and monitor existing vendors and hold them accountable.
- Use our findings to set priorities for your TPRM program. For example, software and other technology providers warrant higher-priority consideration and closer scrutiny than their non-technical counterparts, since they are responsible for a much higher proportion of third-party breaches.
- Healthcare organizations that do not already have TPRM programs should establish them immediately. These programs should cover the complex ecosystem of third parties through which patients and their data progress to receive care and billing, as well as providers of specialized healthcare software.
- Immediately apply patches for CVE-2023-34362, CVE-2023-4966, and CVE-2023-45727, if you use the affected software and have not already done so.
- Do not pay ransoms to ransomware operators or attackers threatening to sell or disclose your compromised data if you fail to pay. Even if you do pay, these criminals might not keep their word; they might be unable or unwilling to decrypt your encrypted files, or they might sell your data to other criminals anyway. Furthermore, paying a ransom suggests to threat actors that you are vulnerable to extortion attempts and, thus a more desirable target for future attacks.

To learn more and create your free account, visit SecurityScorecard.com

ABOUT SECURITYSCORECARD

Funded by world-class investors, including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings, response, and resilience, with more than 12 million companies continuously rated.

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight.

SecurityScorecard makes the world safer by transforming how companies understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors. SecurityScorecard achieved the Federal Risk and Authorization Management Program (FedRAMP) Ready designation, highlighting the company's robust security standards to protect customer information, and is listed as a free cyber tool and service by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Every organization has the universal right to its trusted and transparent Instant SecurityScorecard rating. For more information, visit **securityscorecard.com** or connect with us on **LinkedIn**.

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.io