Cost of Insider Risks

GLOBAL REPORT

2023

Independently conducted by Ponemon INSTITUTE | DTEX

Study snapshot

309
Organizations that experienced one or more insider incidents

1,075
IT and IT security practitioners

7,343
Total number of insider incidents

24
Incidents per company

In the context of this research, insider risks are defined as:

Malicious
An insider who seeks to cause harm

Non-malicious
An insider who does not seek to cause harm

NEGLIGENT
An insider who causes harm through carelessness or inattentiveness

MISTAKEN
A non-malicious insider who causes harm through a genuine mistake that cannot be attributed to carelessness

OUTSMARTED
A non-malicious insider who causes harm through being reasonably outmaneuvered by an attack or adversary

EXAMPLES

- Espionage
- IP threat
- Unauthorized disclosure
- Sabotage
- Fraud
- Workplace violence

Ignore warnings

Pressing the incorrect button in a very noisy and stressful environment

Being phished by a new, advanced phishing attack that has not previously been seen in the wild

* This table is based on **MITRE Corporation's Insider Threat Types**

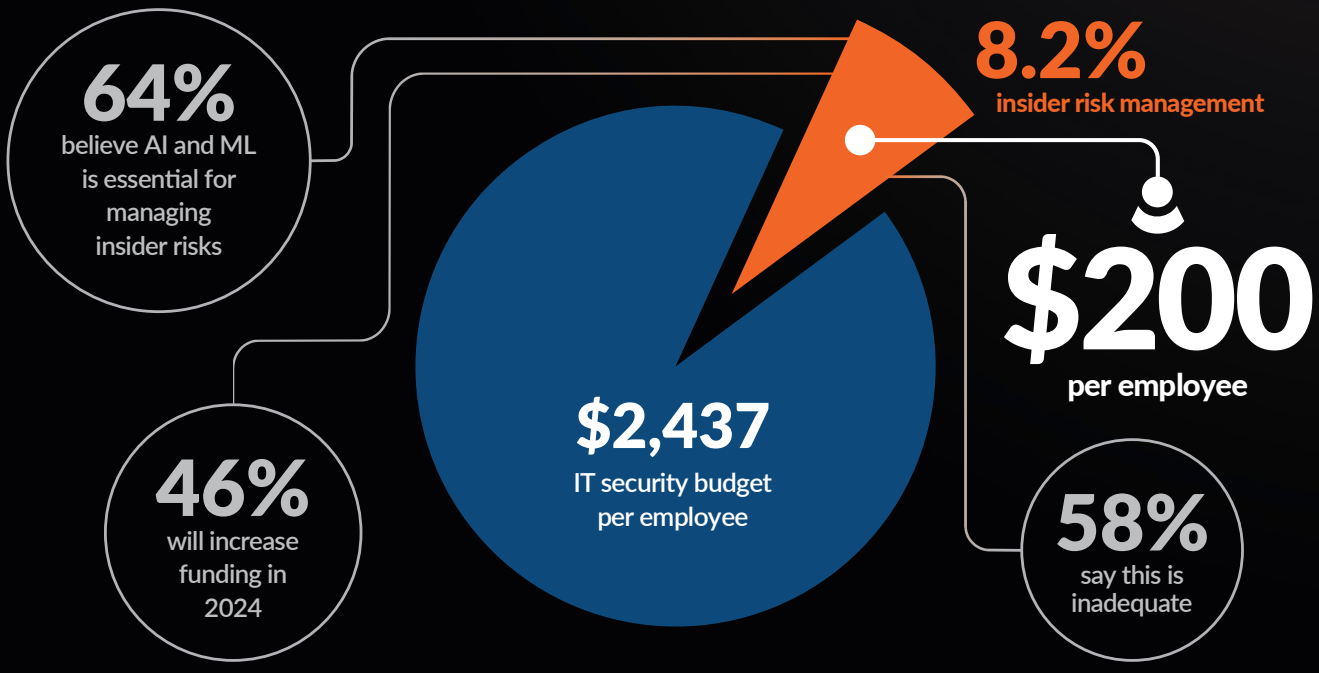
So what?

The upward trends associated with incident costs, frequency, and time to contain demonstrate that current approaches to insider risk are simply not working. In fact, the numbers clearly show we are going backwards.

Funding is being inadvertently misdirected due in part to a widespread misunderstanding of insider risks and how they manifest based on early warning behaviors. A whole-of-industry approach is required to educate and find common ground on how we define and discuss insider risks with enterprise and government entities.

On a positive note, more and more organizations are building insider risk programs and seeking budget and executive buy-in to fund and champion them.

Our research echoes similar findings from other leading analysts and research organizations, notably Forrester, Gartner, MITRE Corporation and Verizon. The human is unquestionably at the center of most data breaches — and increasingly, that human risk is an insider, right under our noses. By homing in on insider risk management, organizations have a powerful opportunity to proactively identify and mitigate insider risks well before a costly incident occurs.



Based on the average number of organizations surveyed. This aligns with other industry studies, including Deloitte Insights: Reshaping the cybersecurity landscape

It pays to be proactive

The time to contain an insider incident has increased to an average of 86 days.

As revealed in this research, the highest cost burden happens after an incident has occurred. Organizations spend far more money reacting to insider incidents than they do on preventative measures. The longer it takes to respond, the higher the cost ($18.33 million for incidents that take longer than 91 days to contain).

OPPORTUNITY VS COST

77%
of organizations have started or are planning to start an insider risk program

$16.2M
average annual cost of insider-related incidents (USD)

7,343 INCIDENTS

Malicious	25% - $4.8M
Outsmarted	20% - $4.2M
Negligent/Mistaken	55% - $7.2M

Incident
Day Zero

LEFT OF BOOM
Proactive detection and prevention of insider risks

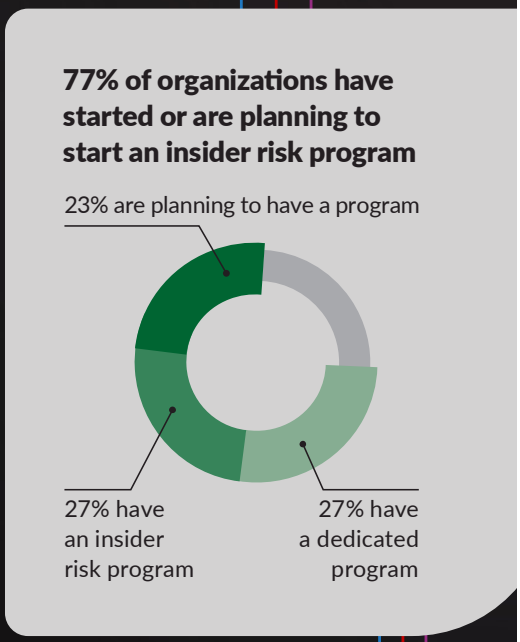
Time is money
Organizations that took more than 91 days to respond had costs exceeding
$18.3M

PRE-INCIDENT		POST-INCIDENT	
$0.87M	Monitoring	Investigation	$3.03M
$0.77M	Ex-post	Escalation	$0.77M
		Incident response	$2.93M
		Containment	$4.63M
		Remediation	$3.23M

All monetary values mentioned on this page are in US dollars (USD).

Key findings

For the first time, we asked about how organizations are funding and governing their insider risk management programs and strategies. Our research revealed the following insights.



Organizations are spending less than 10% of their IT security budget per year trying to solve a $16.2 million (and growing) problem.

Organizations had an average IT security budget of $2,437 per employee, yet only 8.2% (equivalent to $200 per employee) was allocated specifically to insider risk management programs and policies.

Most organizations agree this level of funding is not enough.

Fifty-eight percent of organizations said current funding levels for insider risk management are inadequate. This lack of funding has likely put insider risk programs on the back foot, causing many organizations to be reactive instead of proactive.

Most insider risk budget is spent after an insider incident has occurred.

Only 10% of insider risk management budget (averaging $63,383 per incident) was spent on pre-incident activity cost centers: $33,596 on monitoring and surveillance, and $29,787 on ex-post analysis (this includes activities to minimize potential future insider incidents and steps taken to communicate recommendations with key stakeholders). The remaining 90% (averaging $565,363 per incident) was spent on post-incident activity cost centers: $179,209 on containment, $125,221 on remediation, $117,504 on investigation, $113,635 on incident response, and $29,794 on escalation.

Nearly half of organizations expect insider risk management funding will increase.

Thirty percent expect a mild increase (3-10%) in funding, while 16% expect a significant increase (10% or more).

Most organizations have started or are planning to start an insider risk program.

Seventy-seven percent of organizations have started or are planning to start an insider risk program. Of those organizations, 23% are planning to have a program, 27% have an insider risk program as part of their cybersecurity program, and 27% have a dedicated program that sits outside of the cyber function.

Having top-down support is the most critical element of a successful insider risk program.

Fifty-two percent of organizations that have or are planning to have a dedicated insider risk program selected top-down support as a key feature of the program. Having a dedicated team (from legal, HR, lines of business and security) was also selected as a key feature of an insider risk program (51%). The selection of these features is indicative of many organizations' acceptance that insider risk requires a human-centric solution.

Most organizations put insider risk management outside of IT security.

The department most commonly responsible for insider risk management was legal (34%) followed by IT (23%), and risk and compliance (21%). Only 6% of organizations said IT security was responsible for insider risk management, while only 7% said no one function was more responsible.

More key findings

The negligent/mistaken insider causes the most incidents.

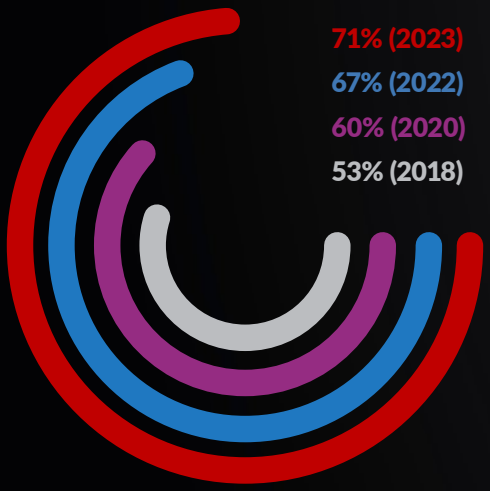
In 2023 there were 4,019 insider incidents related to employee negligence or employee mistakes. This equates to 55% of all incidents experienced by organizations represented in this research, costing on average $505,113 per incident. The average annual cost to remediate these incidents was $7.2 million – up from $6.6 million in 2022. Examples include not ensuring devices are secured, not following the company's security policy, or forgetting to patch and upgrade.

Malicious insiders are less common but cost the most.

Malicious insiders accounted for 1,874 incidents (25%), costing an average of $701,500 per incident. The average annual cost of an incident by malicious insiders was $4.8 million, up from $4.1 million in 2022. Malicious insiders are employees or authorized individuals who use their data access for harmful, unethical, or illegal activities. By virtue of their wider available access to information, malicious insiders are generally harder to detect compared with external attackers or hackers.

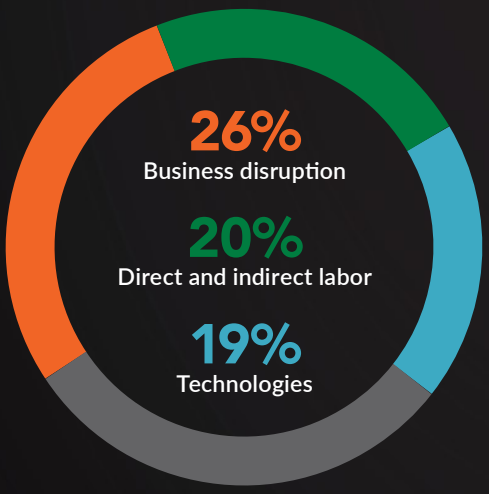
Credential theft incidents average $679,621 per incident.

The outsmarting of insiders via social engineering is a go-to tactic for many external attackers looking to steal credentials to get access to critical data and information. In 2023, 1,450 20%) of outsmarted insider incidents involved stolen credentials, at an average annualized cost of $4.2 million – down from $4.6 million in 2022..



More organizations are having more than 21 incidents per year.

According to the 2023 findings, 71% of companies are experiencing between 21 and more than 40 insider incidents per year. This is an increase from 67% in 2022 of companies having between 21 and more than 40 incidents.



Disruption or downtime and direct and indirect labor represent the most significant costs when dealing with insider risks.

The three largest costs are the impact of business disruption due to diminished employee productivity (26% of total cost), direct and indirect labor (20% of total cost) and technology (19% of total cost), which includes the amortized value and the licensing for software and hardware that are deployed in response to insider-related incidents.

Organizational size affects the cost per incident.

The cost of incidents varies according to organizational size. Large organizations with a headcount of more than 75,000 spent an average of $24.60 million over the past year to resolve insider-related incidents. To deal with the consequences of an insider incident, smaller organizations with a headcount below 500 spent an average of $8 million.

Companies spend the most on containment of the insider security incident.

An average of $179,209 is spent to contain the consequences of an insider risk. The least amount of average cost is for escalation at $29,794 and monitoring and surveillance at $33,596. Incidents that took less than 31 days to contain had the lowest average total cost of activities at $11.92 million. In contrast, average activity costs for incidents that take more than 91 days is $18.33 million – up from $17.19 million in 2022.

North American companies are spending more than the average cost on activities that deal with insider risks.

The total average cost of activities to resolve insider risks over a 12-month period is $16.2 million. Companies in North America experienced the highest total cost at $19.09 million. European companies had the next highest cost at $17.47 million.

Financial services and service organizations have the highest average activity costs.

The average activity cost for financial services is $20.68 million and services is $19.63 million. Service organizations include accountancy, consultancy, and professional service firms.

Interviews with participants in this research revealed the following insights into insider risks.

In addition to determining the cost of insider risks for companies in this research, we interviewed participants about their experiences with the risk and what they are doing to reduce risks.

The non-malicious insider risk continues to pose the greatest risk to organizations. Seventy-five percent of respondents say the most likely cause of insider risk is non-malicious: a negligent or mistaken insider (55%), or an outsmarted insider who was exploited by an external attack or adversary (20%).

Sales and customer service are the roles or functions that pose the greatest insider risks (48% and 47%, respectively). Functions that pose the least risk are IT and legal third-party contractors at 23% and 29%, respectively.

Malicious insiders are most likely to email sensitive data to outside parties (67%). They are also very likely to access sensitive data not associated with the role or function (66%) and scan for open ports and vulnerabilities (63%).

Cloud and IoT devices are most likely to be the channels where insider-driven data loss occurs (59% and 56%, respectively). Less likely are corporate-owned endpoints (41%) and BYOD endpoints (43%). The channels organizations are most concerned about are IoT (65%) and cloud (61%).

Malware and social engineering attacks were most likely to cause a non-insider attack that led to a data breach, at 56% and 53%, respectively. In the past 12 months, 58% of organizations had a minimum of two non-insider attacks that caused a data breach. Malware is considered the most important attack to prevent (65% of organizations).

Advanced technologies are considered essential to reducing insider risks. User-behavior-based tools for detecting insider risks are considered essential (31%) or very important (33%). Sixty-four percent of respondents believe AI and machine learning is essential (33%) or very important (31%) to preventing, investigating, escalating, containing and remediating insider incidents. Sixty-one percent say automation is essential (38%) or very important (23%) to managing insider risks.

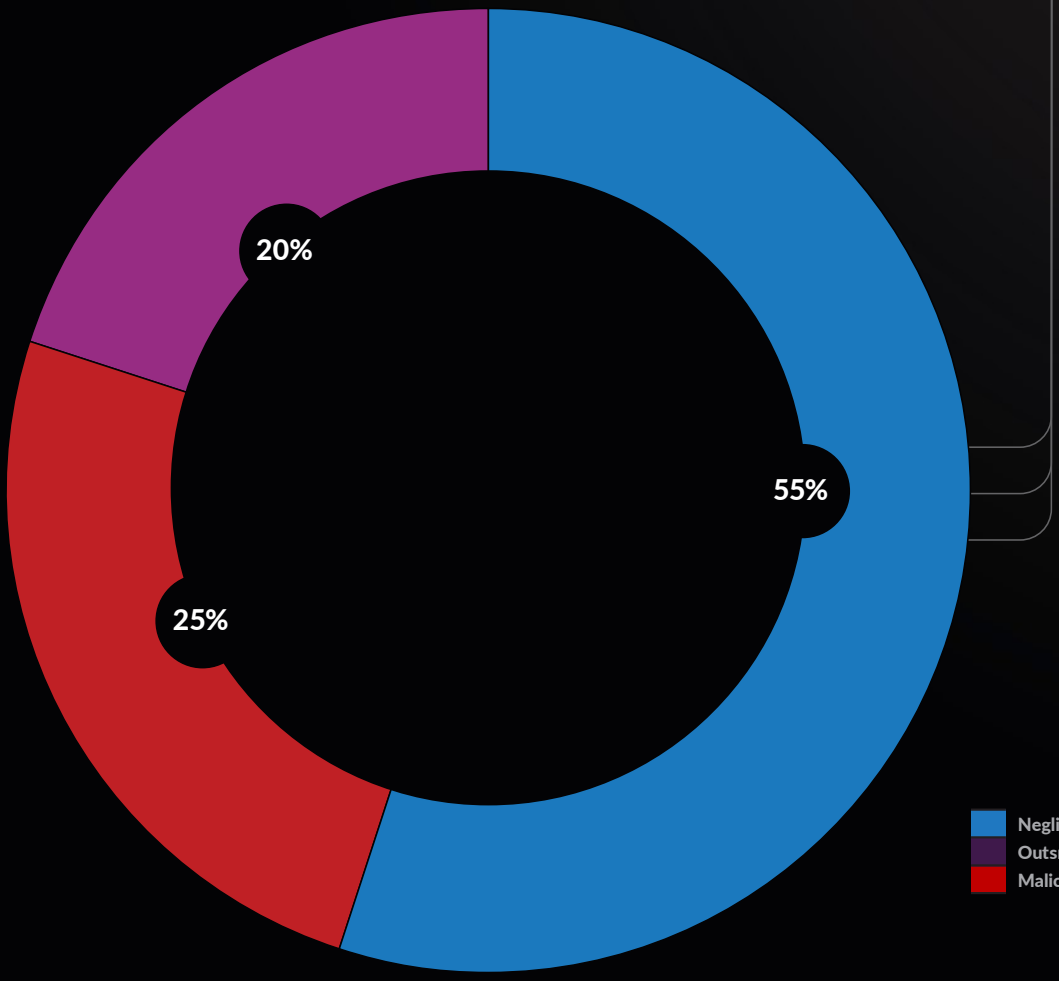
Reduction in incidents is the top metric for measuring the success of insider risk efforts and programs (50%). This is followed by assessment of insider risks (40%) and length of time to resolve the incident (38%).

Cost analysis

Employees or contractors continue to be the primary source of an insider risk.

Figure 1. Frequency of 7,343 incidents for three insider profiles

Figure 1 shows the distribution of 7,343 reported attacks analyzed in our sample. A total of 4,019 attacks (or 55%) were caused by employee or contractor negligence/mistakes. Malicious insiders caused another 1,874 attacks (or 25%) and there were 1,450 credential thefts caused by outsmarted insiders (20%).



4,019
Negligent or mistaken insiders

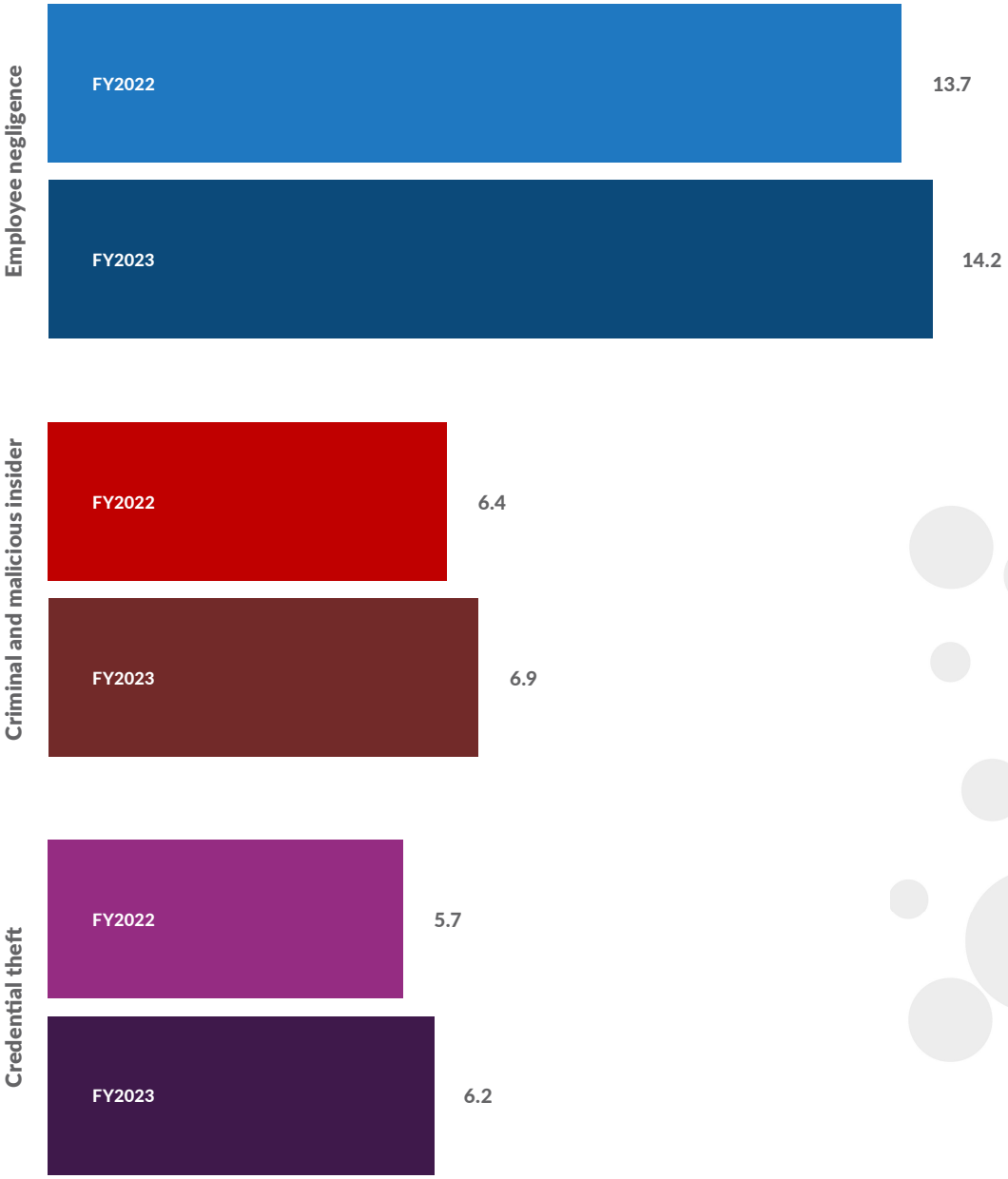
1,874
Malicious or criminal insiders

1,459
Outsmarted insiders (credential theft)

Figure 2. Frequency for three profiles of insider incidents

Employee negligence or employee mistakes are the most frequent insider incidents.

As shown in Figure 2, employee or contractor negligence/mistakes increased slightly from 13.7 to 14.2. Credential theft has increased from an average of 5.7 incidents in 2022 to 6.2 incidents in this year's study. Criminal and malicious insider incidents increased from 6.4 to 6.9.



The 2022 data includes North America, Europe, Middle East and Africa and Asia-Pacific. We believe the data is comparable because US companies represented in the 2016 report are multinationals.

Figure 3. Frequency of insider-related incidents per company over a four-year period

Organizations having more than 40 incidents increased only slightly.

Figure 3 shows the average consolidated frequency of employee or contractor negligence/mistakes, malicious/criminal insider and credential theft incidents per company. According to the 2023 research, 71% of companies (30% + 22% + 19%) are experiencing between 21 and more than 40 incidents per year. This is an increase from 67% in 2022 of companies having between 21 and more than 40 incidents.

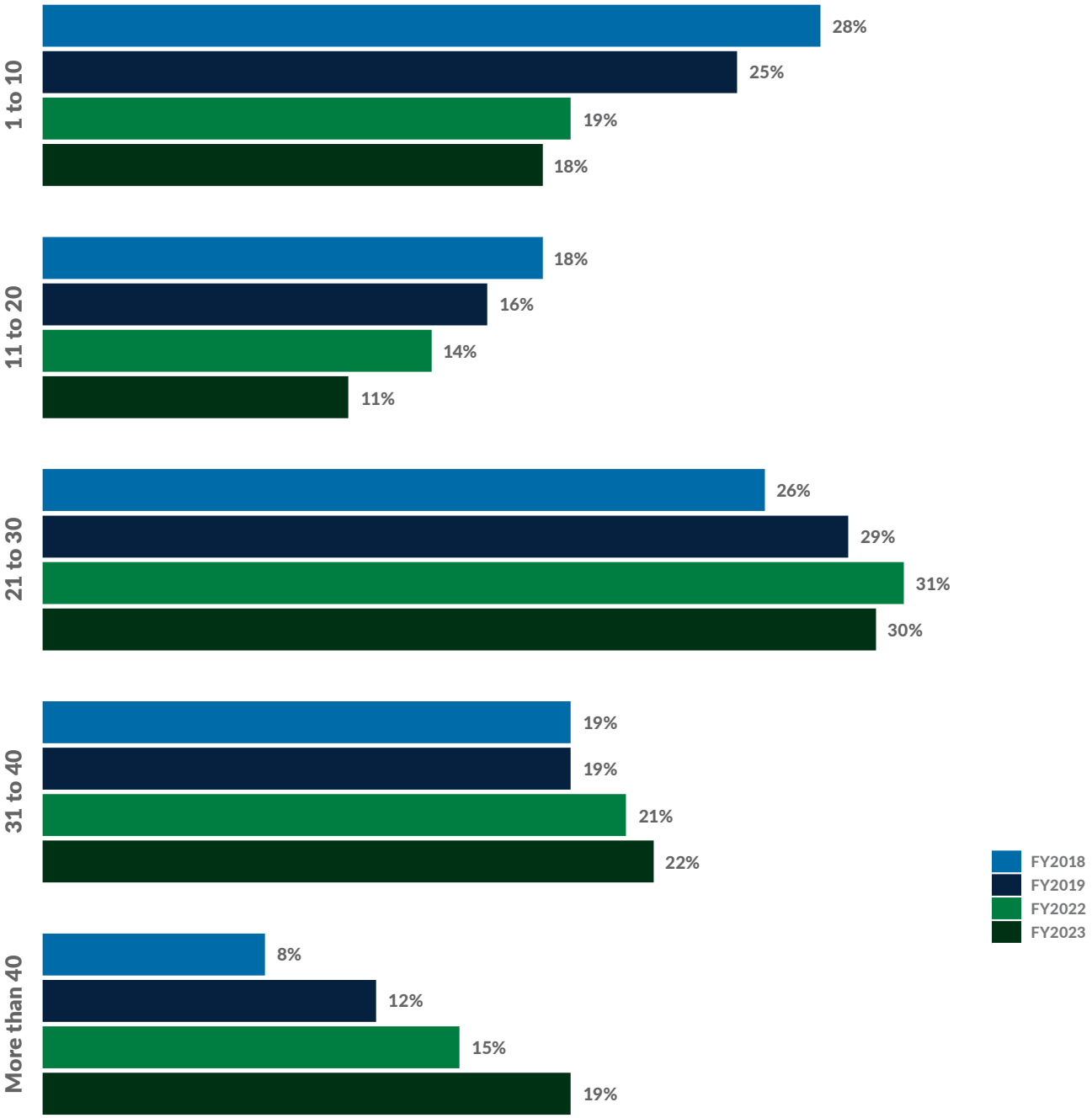
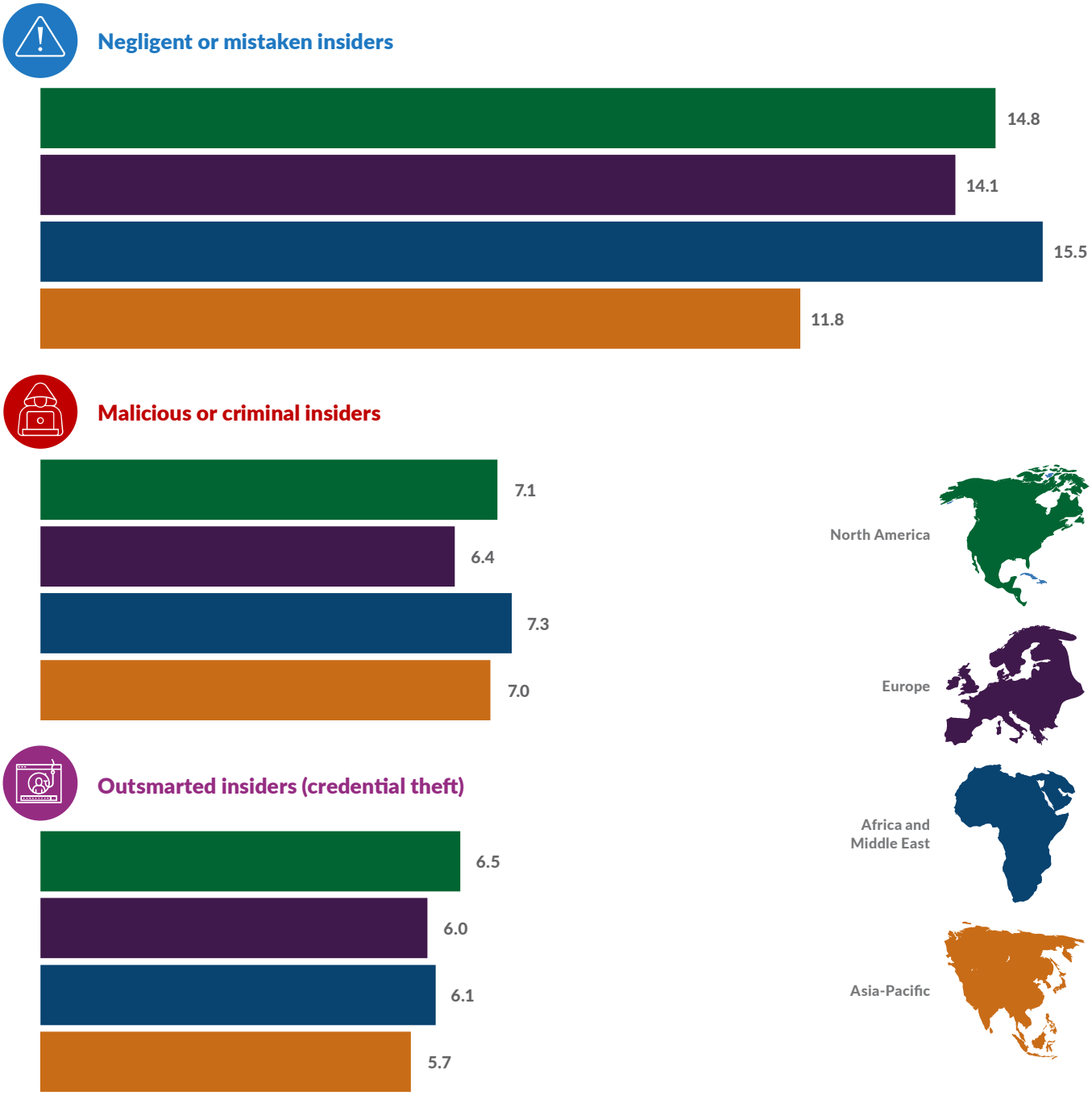


Figure 4. Average incident frequency for three profiles by geographic region

Organizations in the Middle East experienced the most insider incidents, and Asia-Pacific had the least number of incidents.

Figure 4 presents the frequency of insider incidents in the four regions represented in the research. In all regions, employee or contractor negligence incidents occurred the most frequently. North America and the Middle East are most likely to experience credential theft, which is a costly source of insider risk.



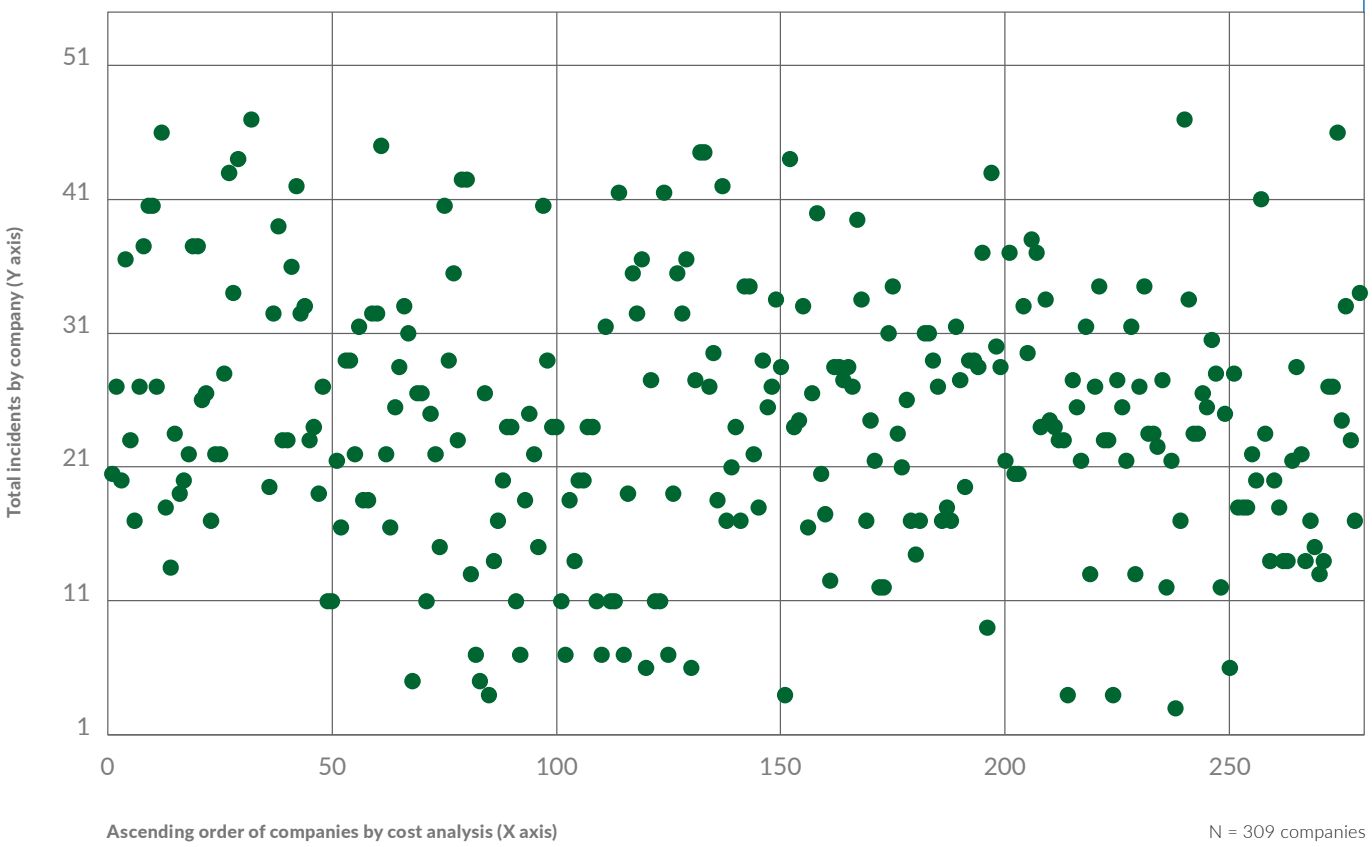


Figure 5. Scattergram of insider-related incidents by company

Figure 5 shows a scattergram of insider incidents per company.

Of the 309 participating companies, 161 (52%) of companies had an average total cost at or below the mean of $16.2 million over the past 12 months. The remaining 148 companies (48%) are above the average of $16.2 million. This finding suggests that the distribution is slightly skewed.

Figure 6. Percentage distribution of insider-related incidents based on the time to contain

Companies are spending an average of 86 days to contain one insider security incident.

According to Figure 6, the time to contain insider-related incidents in our benchmark sample took an average of 86 days to contain the incident. Only 13% of incidents were contained in less than 31 days.

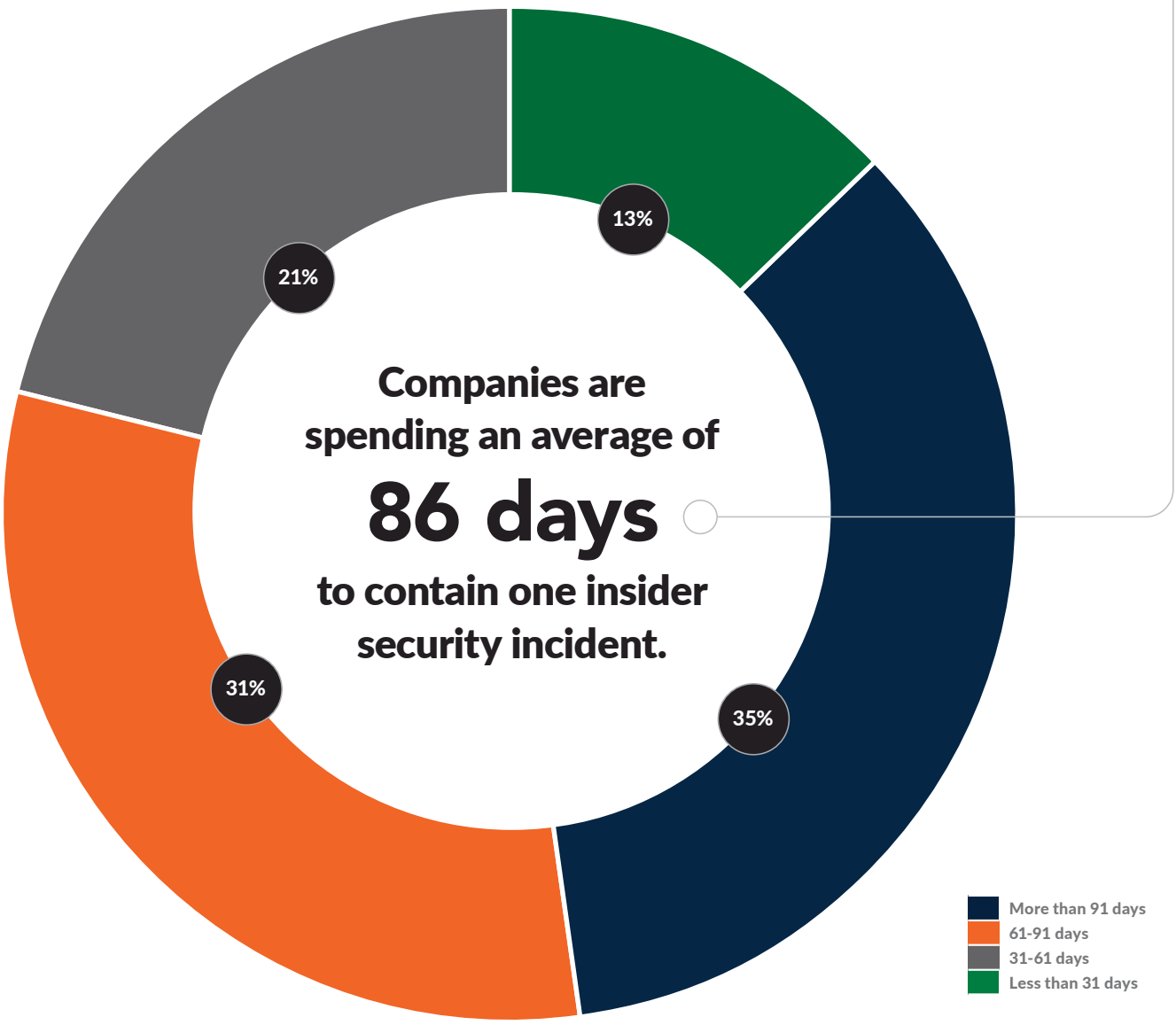
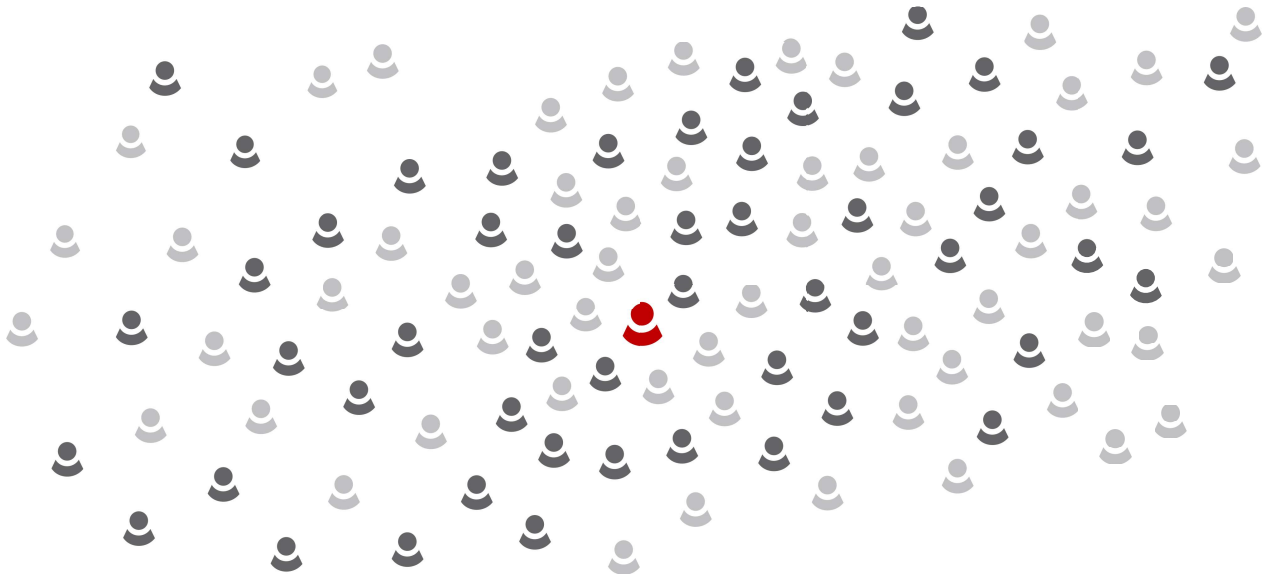


Table 1. Percentage frequency in the use of tools and activities

Most participating companies (72%) are conducting training and awareness programs to reduce insider risks.

Fifty-seven percent of organizations deploy data loss prevention solutions and 56% use SIEM and PAM solutions.

FY2023 Tools and activities that reduce insider risks	Percentage of companies
User training and awareness	72%
Data loss prevention (DLP)	57%
Security incident and event management (SIEM)	56%
Privileged access management (PAM)	56%
User behavior analytics (UBA)	54%
Insider risk management (IRM)	43%
Strict third-party vetting procedures	39%
Employee monitoring and surveillance	38%
Risk intelligence sharing	36%
Network traffic intelligence	27%



The cost of insider risks

Figure 7. Percentage of insider cost by consequence to business organization

Disruption or downtime and direct and indirect labor costs represent the most significant costs when dealing with insider incidents.

Figure 7 reports the percentage of insider cost for careless or negligent employees, malicious insiders and outsmarted employees (credential theft) according to the seven cost categories: Disruption cost (downtime), direct and indirect labor, technology, cash outlays, process/workflow changes, revenue losses and overhead.

The three largest cost categories are the impact of business disruption due to diminished employee/user productivity (26% of total cost), direct and indirect labor (20% of total cost) and technology (19% of total cost), which includes the amortized value and the licensing for software and hardware that are deployed in response to insider-related incidents.

Process costs (11%) include governance and control system activities in response to risks and attacks. Overhead (4%) includes a wide array of miscellaneous costs incurred to support personnel as well as the IT security infrastructure.

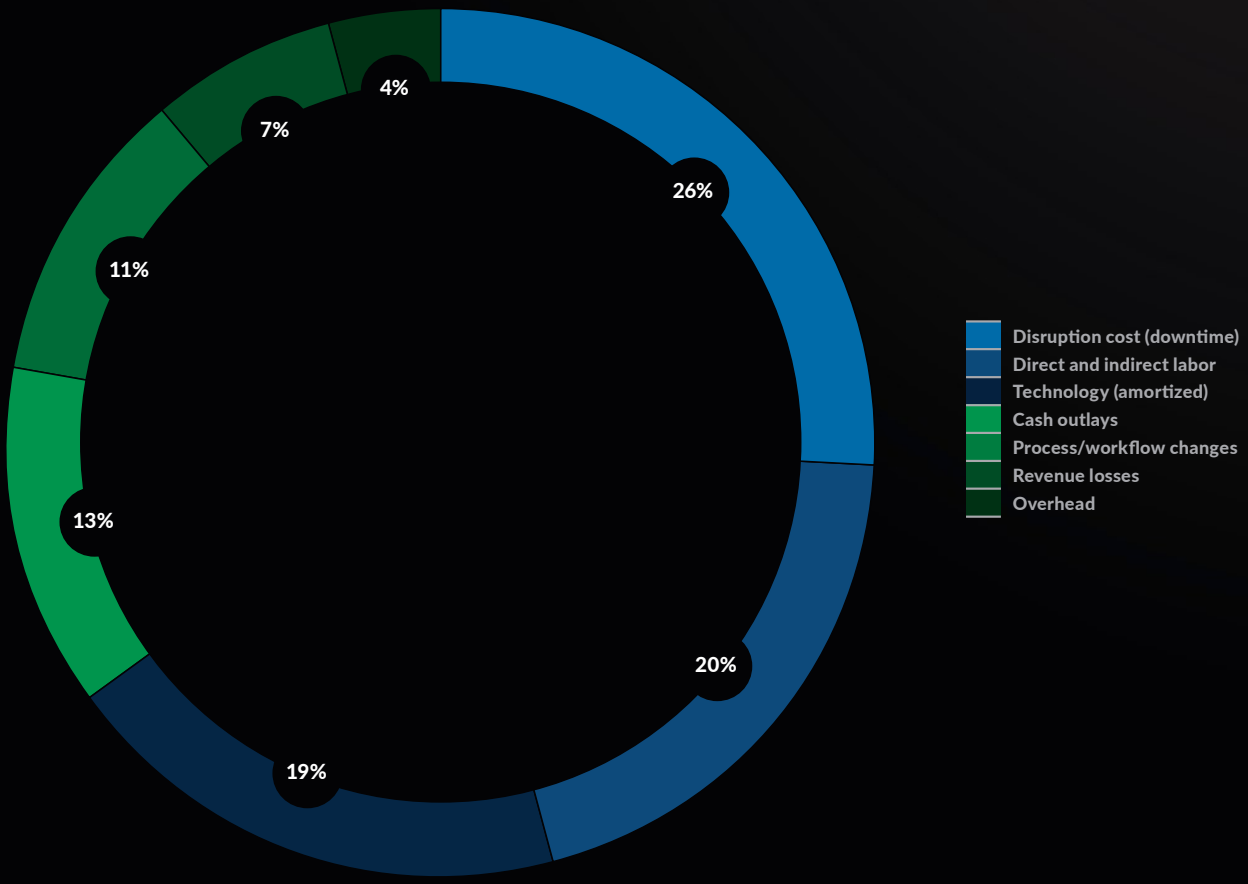


Table 2. The average annual cost per incident for the three types of incidents

Malicious and criminal insider and credential thief incidents continue to be more costly per incident than employee or contractor negligence.

Table 2 presents the average cost per incident, the average number of incidents and the average annualized cost per year. As shown, employee or contractor negligence is most frequent (14 incidents). However, the average cost for this type of incident is less than credential theft and malicious insider incidents.

The cost of malicious insider incidents steadily increased between 2018 and 2019 from $614,192 to $755,761 but declined to $701,500 in 2023. The average number of credential thefts has increased since 2018 and the average cost for remediating these incidents is $679,621 in this year's research.

FY2018 CASE PROFILES	Average cost per incident	Mean number of incidents per year	Average annualized cost
Non-malicious insider (negligent/mistaken)	$277,557	13.2	$3,663,752
Malicious and criminal insider	$614,192	4.6	$2,825,283
Outsmarted insider (credential theft)	$672,112	2.7	$1,814,702
			$8,303,737

FY2019 CASE PROFILES	Average cost per incident	Mean number of incidents per year	Average annualized cost
Non-malicious insider (negligent/mistaken)	$317,111	14.9	$4,724,954
Malicious and criminal insider	$755,761	5.4	$4,081,109
Outsmarted insider (credential theft)	$871,686	3.2	$2,789,395
			$11,595,458

FY2022 CASE PROFILES	Average cost per incident	Mean number of incidents per year	Average annualized cost
Non-malicious insider (negligent/mistaken)	$484,931	13.7	$6,643,555
Malicious and criminal insider	$648,062	6.4	$4,147,597
Outsmarted insider (credential theft)	$804,997	5.7	$4,588,483
			$15,378,635

FY2023 CASE PROFILES	Average cost per incident	Mean number of incidents per year	Average annualized cost
Non-malicious insider (negligent/mistaken)	$505,113	14.2	$7,172,605
Malicious and criminal insider	$701,500	6.9	$4,840,350
Outsmarted insider (credential theft)	$679,621	6.2	$4,213,650
			$16,226,605

Table 3. Average trend in activity cost for seven activity centers

Companies spend the most on containment of the insider security incident.

As discussed, the average time to contain an incident is 86 days in this year's research. Table 3 summarizes the average cost of insider-related incidents for the three types of incidents and seven activity centers. As shown, containment and remediation of the incident represent the most expensive activity centers at $179,209 and $125,221, respectively. Least expensive are ex-post analysis and escalation at $29,787 and 29,794, respectively.

Activity cost centers	FY2016	FY2018	FY2019	FY2022	FY2023
Monitoring and surveillance	$9,620	$12,634	$22,124	$35,080	$33,596
Investigation	$41,461	$78,398	$103,798	$128,056	$117,504
Escalation	$8,919	$12,542	$21,805	$32,228	$29,794
Incident response	$66,371	$91,263	$118,317	$120,391	$113,635
Containment	$122,796	$173,161	$211,553	$184,548	$179,209
Ex-post analysis	$8,498	$11,491	$19,480	$26,563	$29,787
Remediation	$91,397	$138,532	$147,776	$119,131	$125,221
Overall	**$349,060**	**$517,921**	**$644,853**	**$645,997**	**$628,745**

Figure 9. Percentage net increase in average cost from FY2016 to FY2023

Since 2016, it has become far more costly to respond to an insider risk incident.

As shown in Figure 9, ex-post analysis and monitoring and surveillance have increased the most since 2016, 111%. Importantly, these are the only pre-incident activities. This finding suggests attempts have been made to take a proactive approach to managing insider risks.

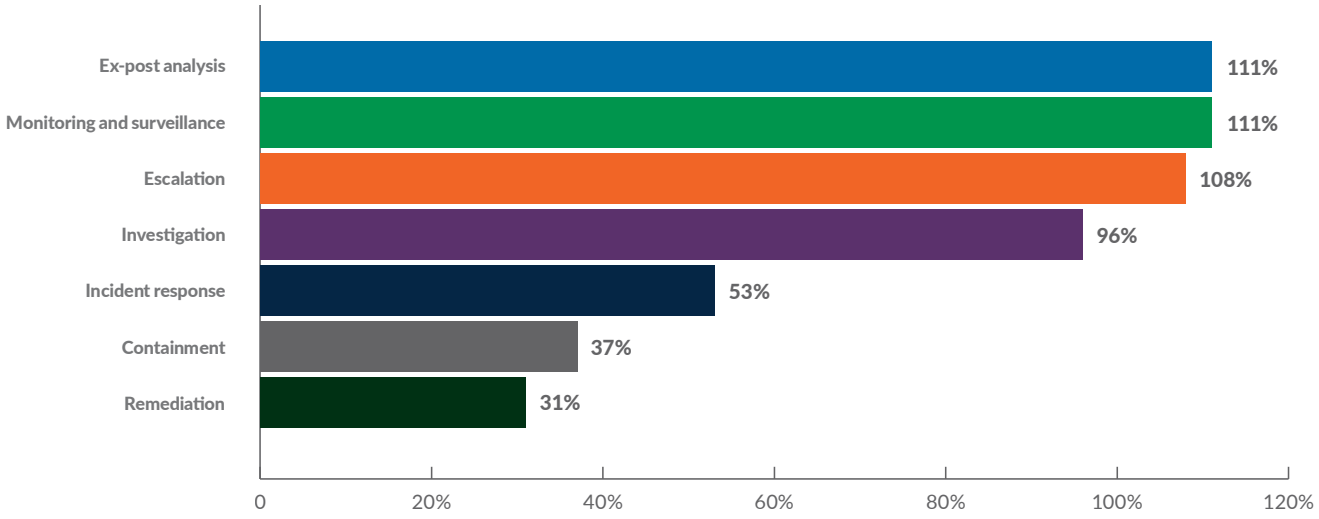


Table 4. 2023 cost of seven activities by the type of incident

Containing the insider incident is most costly for malicious or criminal insider and credential theft incidents.

Table 4 presents the average annualized cost for the seven activities according to the type of incident.

FY2023 activity cost centers	Negligent or mistaken	Malicious or criminal	Outsmarted (credential theft)	Average cost
Monitoring and surveillance	$21,869	$38,420	$40,499	$33,596
Investigation	$103,388	$136,096	$113,026	$117,504
Escalation	$24,337	$41,552	$23,492	$29,794
Incident response	$105,941	$133,330	$101,635	$113,635
Containment	$140,312	$198,545	$198,769	$179,209
Ex-post analysis	$19,834	$28,349	$41,176	$29,787
Remediation	$89,433	$125,208	$161,023	$125,221
Total	**$505,113**	**$701,500**	**$679,621**	**$628,745**

Figure 10. 2023 average activity cost per incident for the three types of incidents

The average activity cost is highest for malicious or criminal insiders.

Figure 10 demonstrates the significant difference in activity cost between employee or contractor negligence and credential theft.

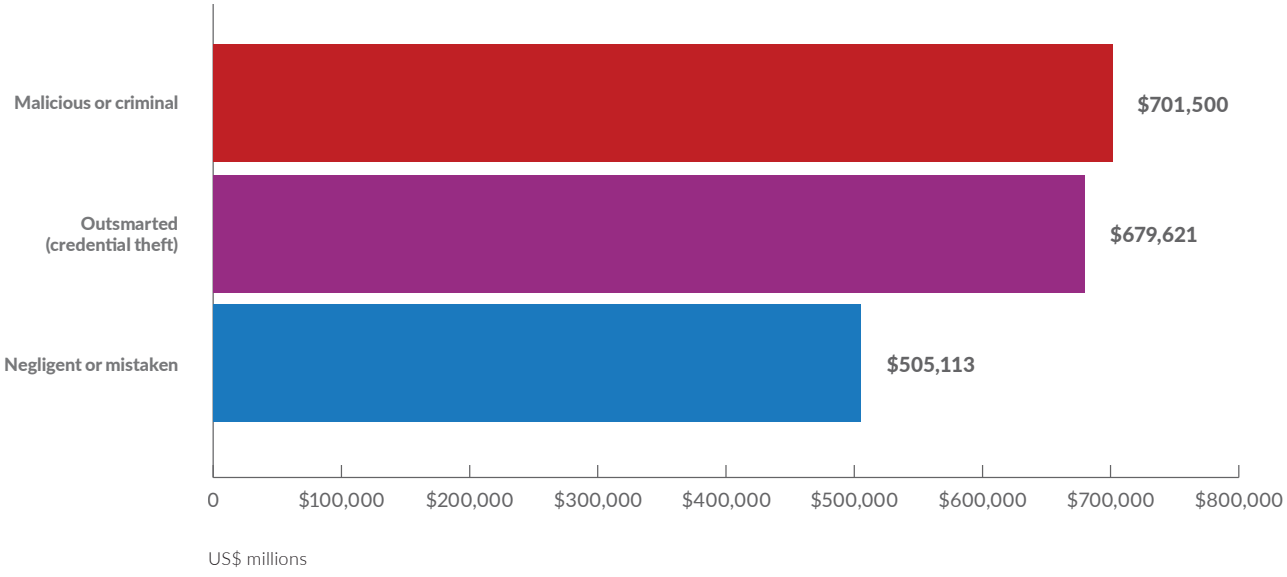


Figure 11. Average activity cost by global region

North American companies are spending significantly more than the average cost on activities that deal with insider risks.

The total average cost of activities to resolve insider risks over a 12-month period is $16.2 million. As shown in Figure 11, companies in North America experienced the highest total cost at $19.09 million. European companies had the next highest cost at $17.47 million. Asia-Pacific had an average cost much lower than average total cost for all 309 companies ($12.17 million).

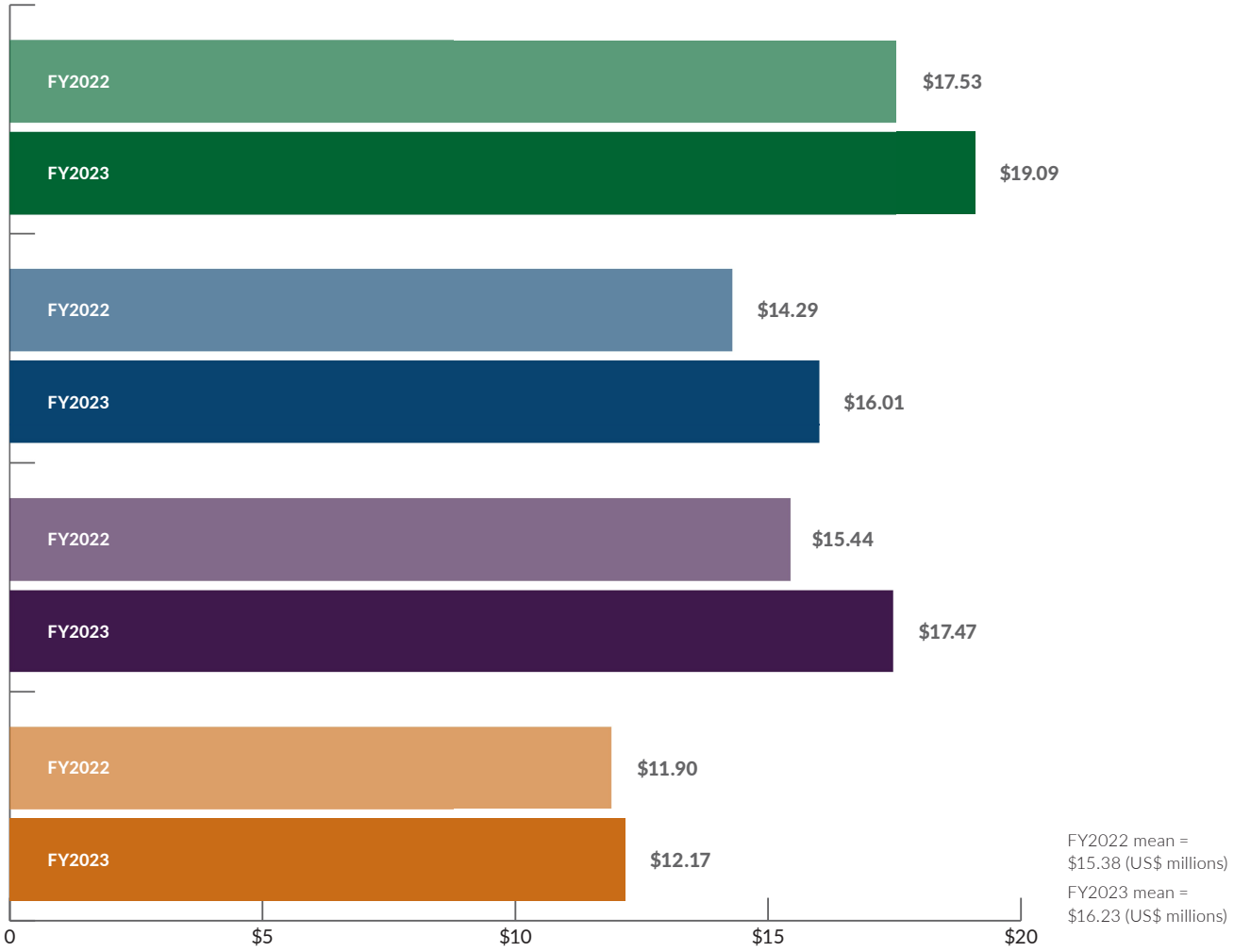


Figure 12. Average activity cost by headcount

Larger organizations spend the most on the activities to resolve an insider risk incident.

As shown in Figure 12, organizations with a headcount of between 25,000 and 75,000 are spending significantly more on activities needed to resolve the incident, an average of $19.70.

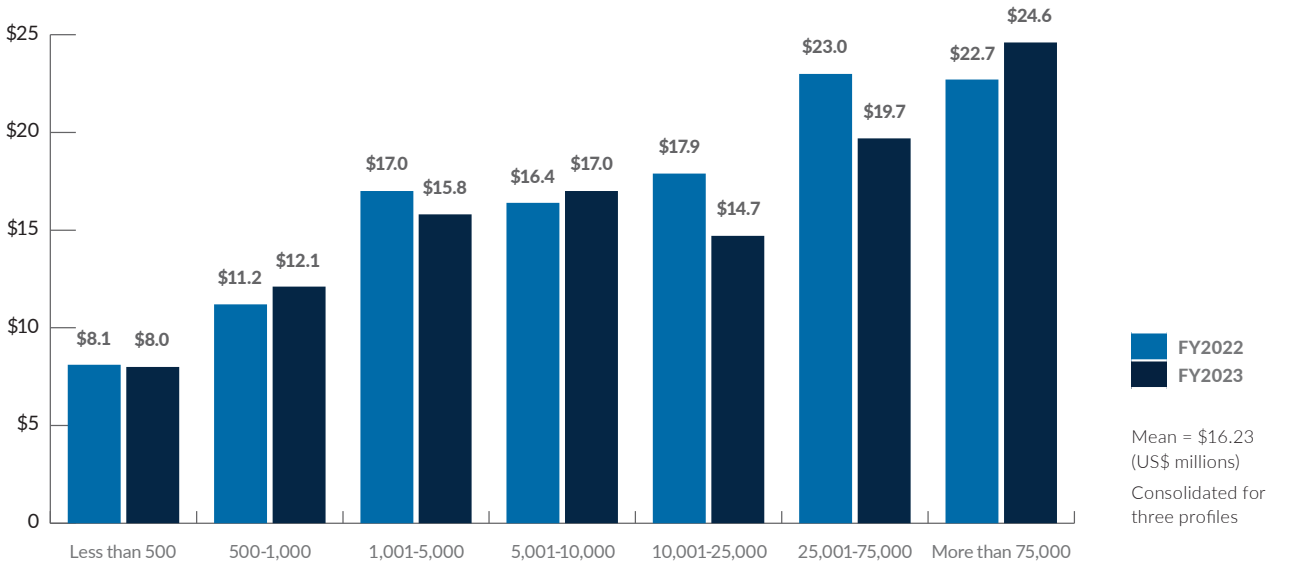


Figure 13. Average activity cost by days to contain the incidents

The faster containment occurs, the lower the activity cost.

The total annualized cost appears to be positively correlated with the time to contain insider-related incidents. As shown in Figure 13, incidents that took more than 91 days to contain had the highest average total cost per year ($18.33 million). In contrast, incidents that took less than 31 days to contain had the lowest total cost. ($11.92 million). The average annual cost is $16.23 million.

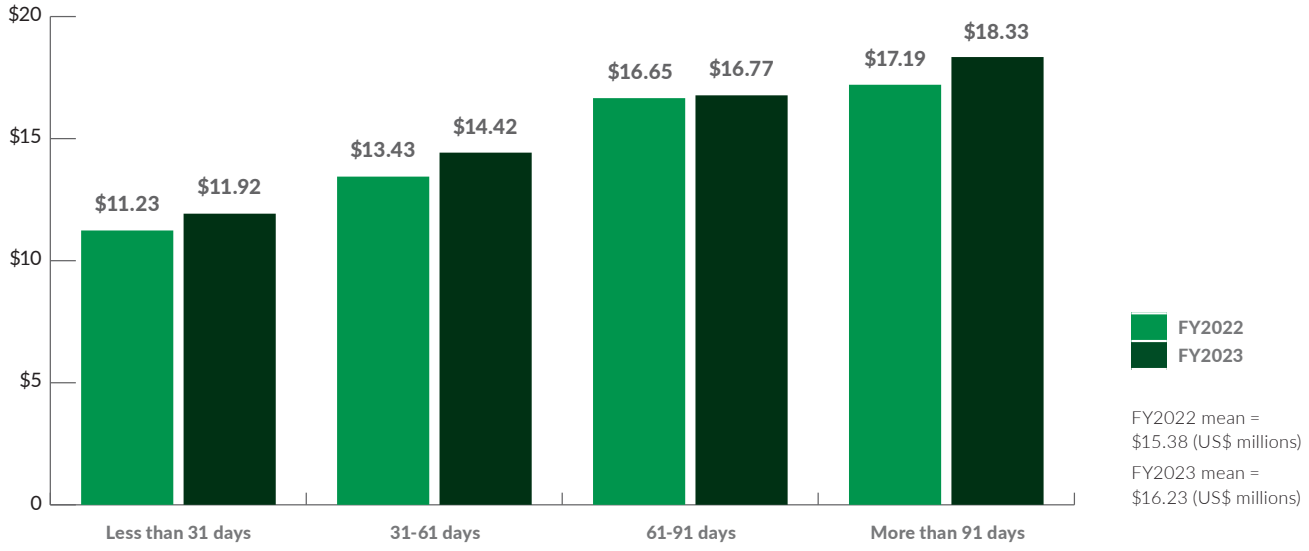


Figure 14. Percentage cost of insider incidents by activity center

Containment accounts for one-third of all costs.

The following pie chart shows the percentage cost for seven activity centers. According to Figure 14, containment represents 28% of total annualized insider-related activity costs. Activities relating to investigation and incident response represent 20% of total cost, respectively.

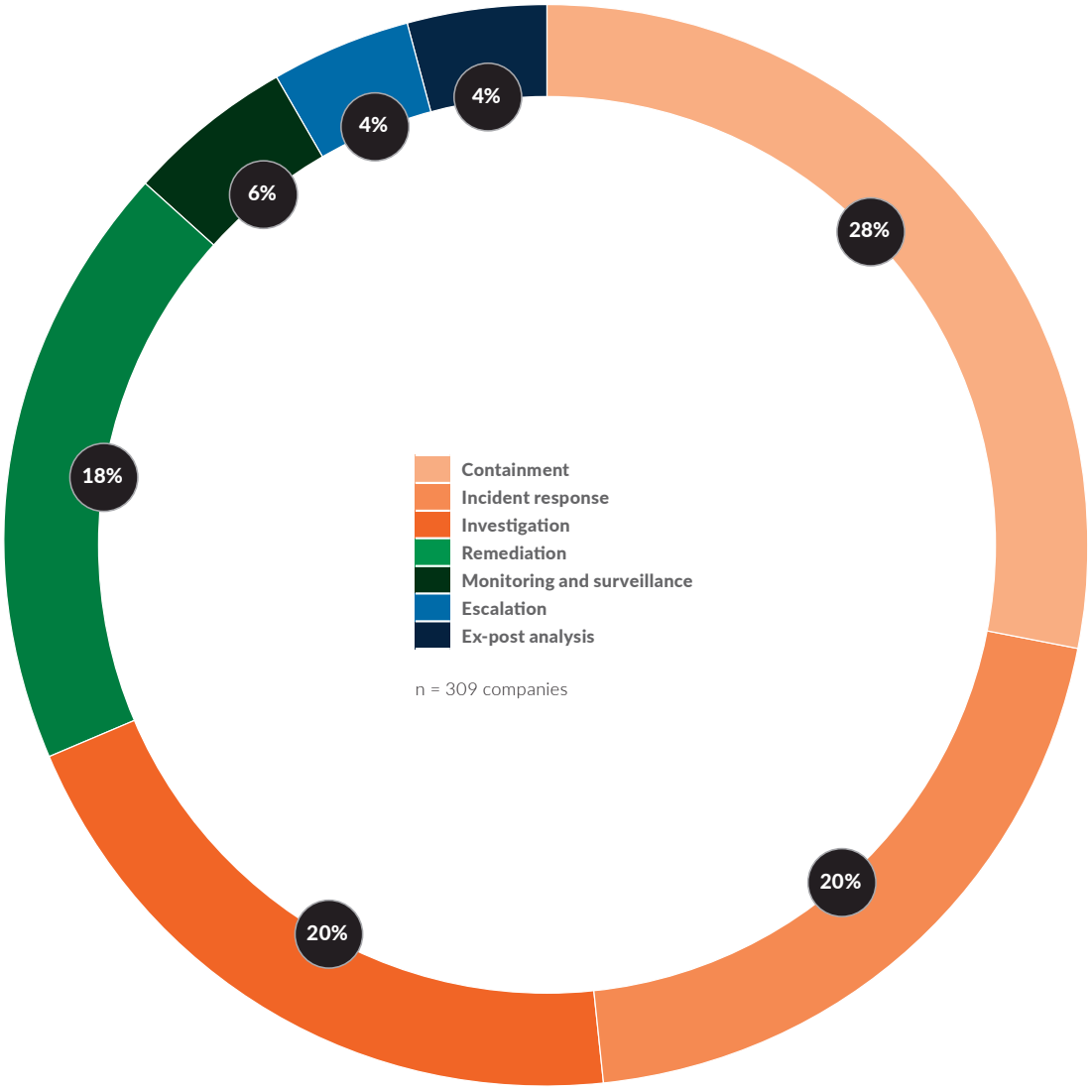


Figure 15. Annualized activity cost by industry

Activity costs are higher for financial services and services.

According to Figure 15, the average activity cost for financial services is $20.68 million and services is $19.63 million, much higher than the average of $16.2 million. Services includes such companies as law, consulting and accounting firms.

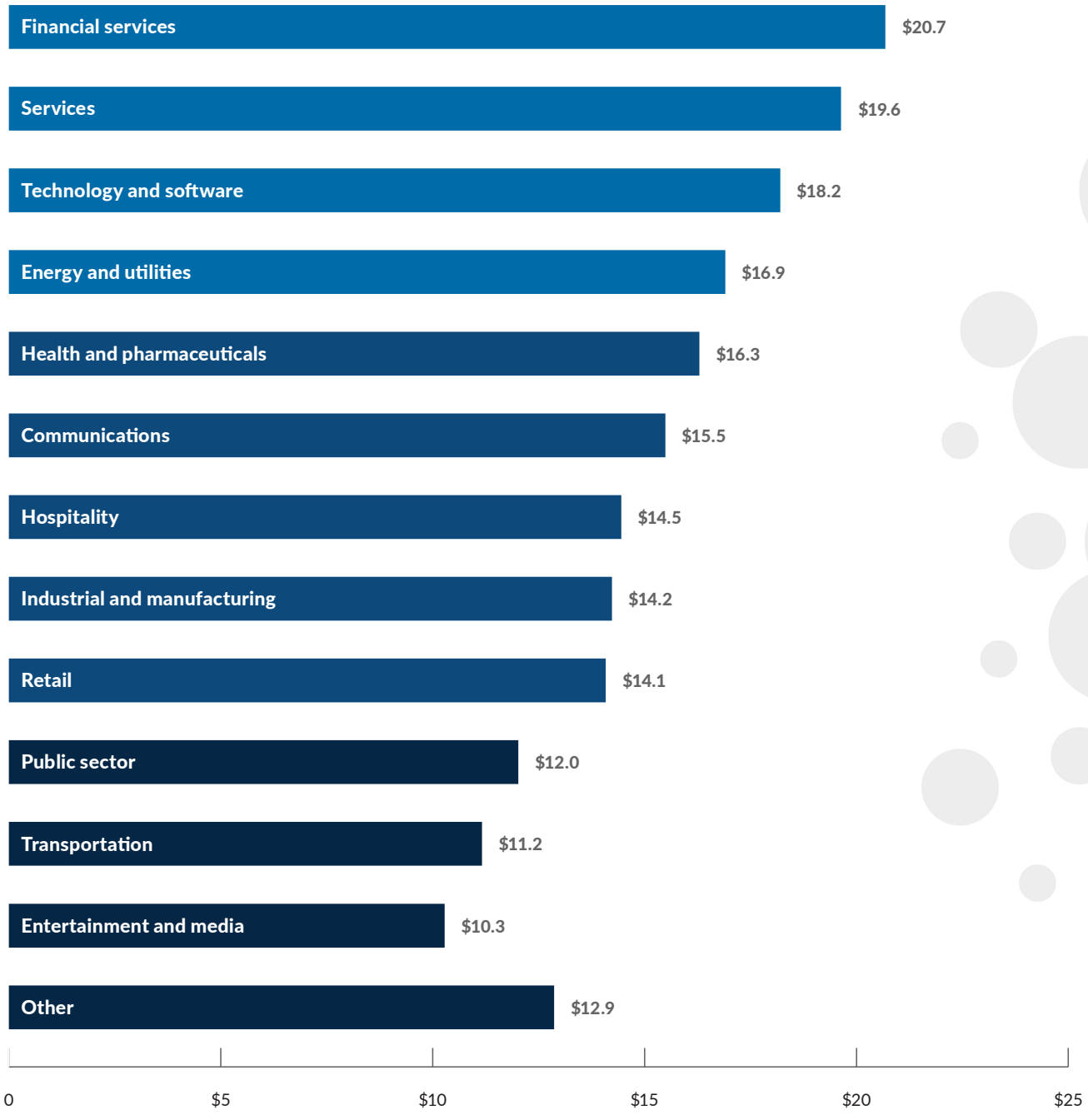
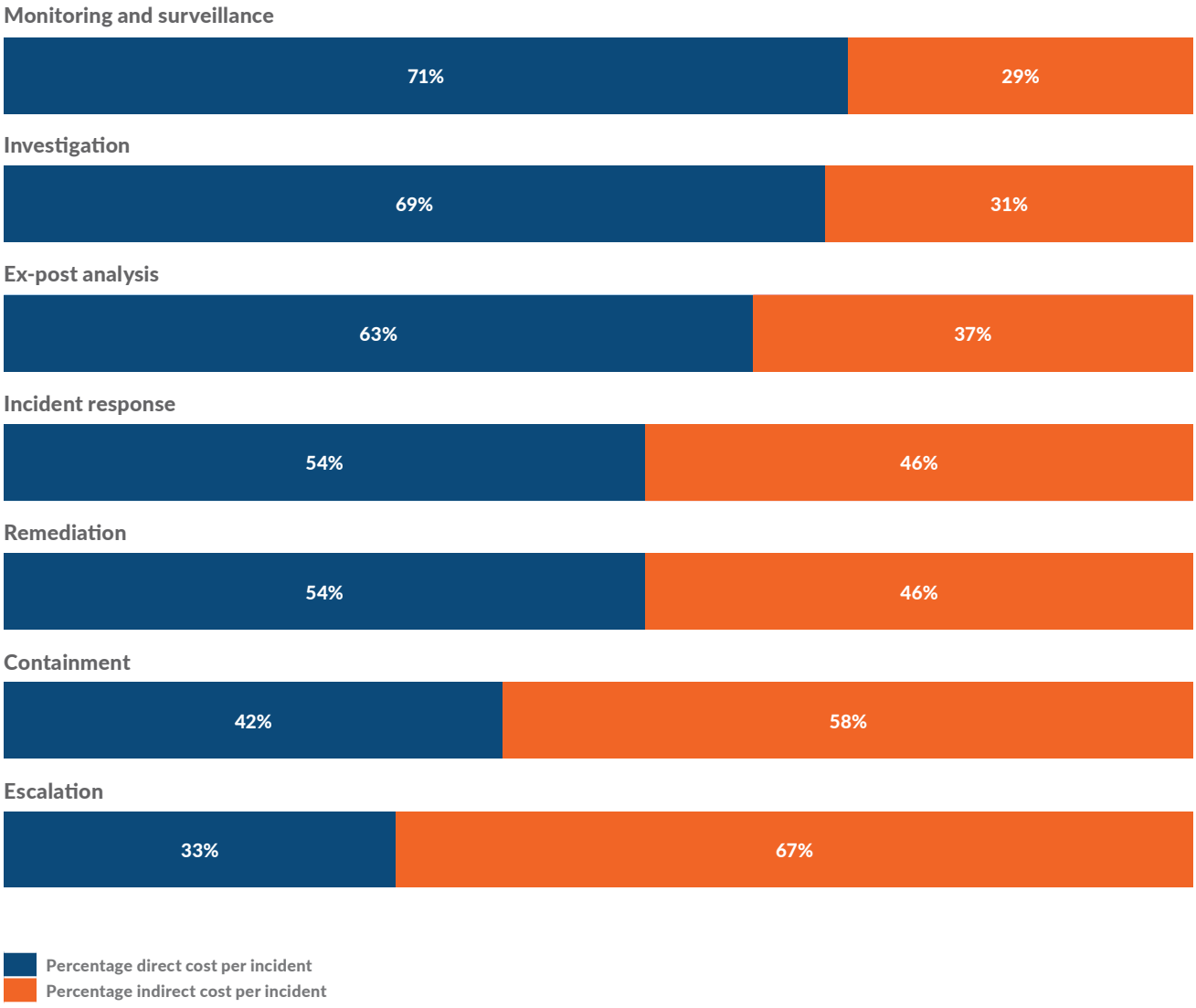


Figure 16. Percentage of direct vs. indirect costs for activity centers

Companies were asked to estimate the direct and indirect costs spent to accomplish a given activity.

Direct costs are the direct expense outlay to accomplish a given activity and indirect costs are the amount of time, effort and other organizational resources spent, but not as a direct cash outlay.

Figure 16 shows the proportion of direct and indirect costs for seven internal activity cost centers. As can be seen, the cost for monitoring and surveillance and investigation has the highest percentage of direct cost (71% and 69%, respectively). The highest percentage of indirect cost for activities are for containment (58%) and escalation (67%).



The direct cost is what is spent to accomplish a given activity and indirect costs are the amount of time, effort and other organizational resources spent to resolve the incident.

Managing insider risks

In addition to determining the cost of insider risks, we interviewed study participants about their ability to manage malicious and non-malicious insider risks.

Figure 17. Which insider incidents are you most concerned about?

Of all insider risks, organizations are most concerned about malicious or criminal insiders.

This is despite that 75% of insider incidents were non-malicious in nature (55% of incidents were attributed to negligence, while 20% were attributed to credential theft).

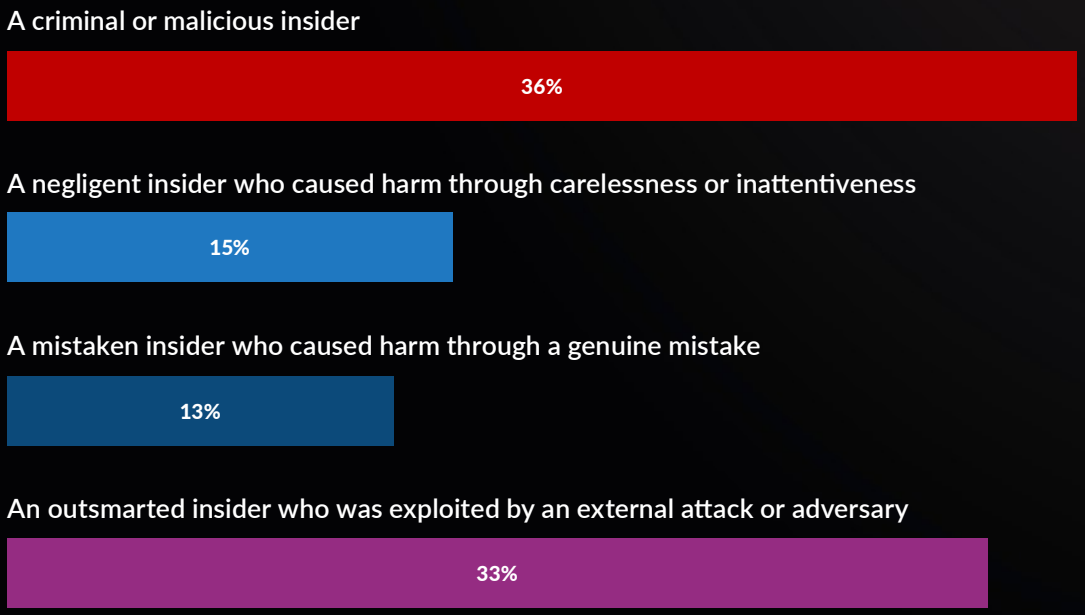
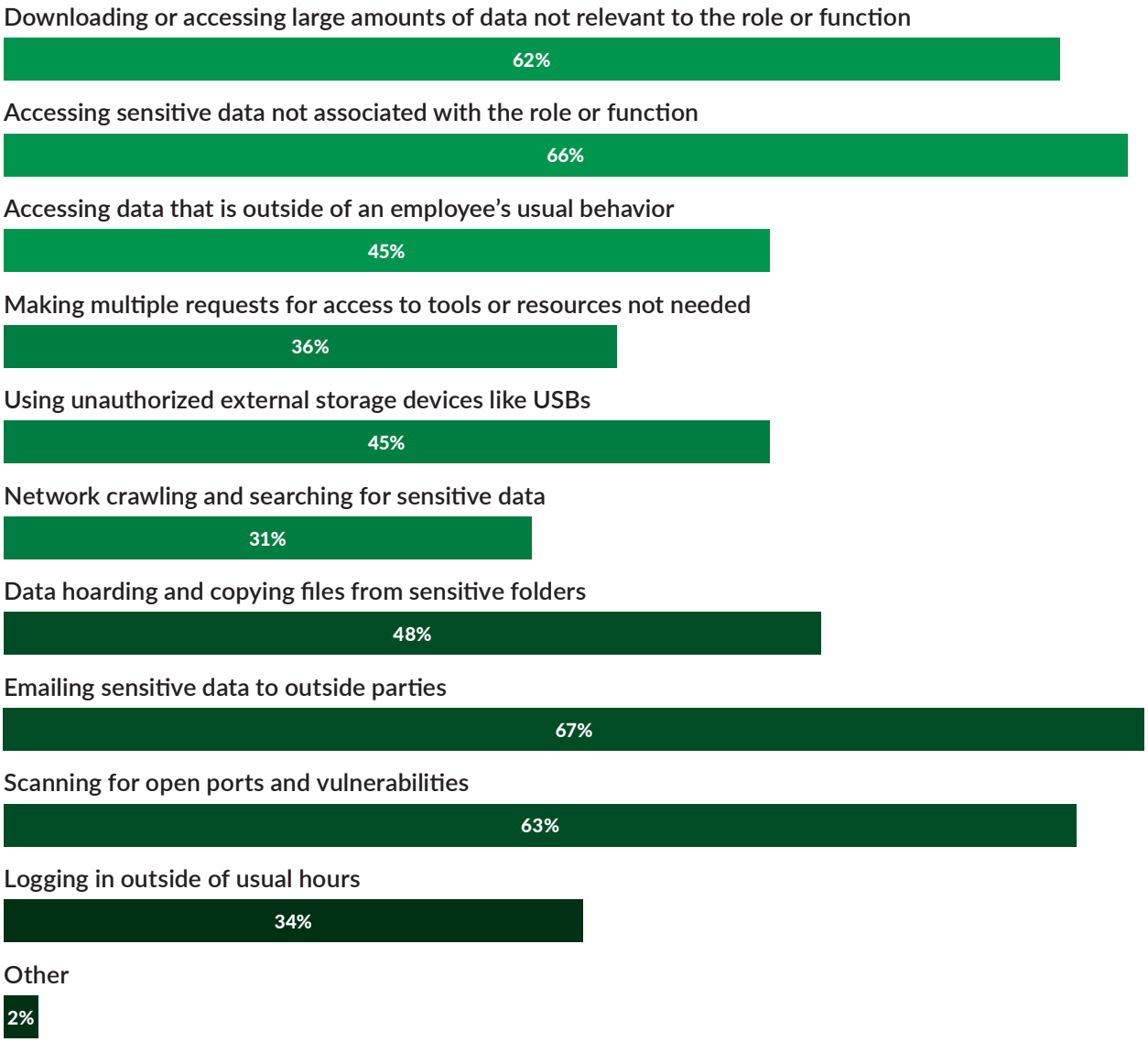


Figure 18. Did malicious insiders do any of the following in your organization?

Malicious insiders were likely to access and share sensitive data unrelated to their job role or function, often in large volumes.

Volume and frequency, data sensitivity and job function have all been validated as early warning indicators for malicious insider risk. This was made evident in two Pentagon incidents in 2023: the Discord leaks and the 'critical compromise' of Air Force communications. While these indicators might seem harmless in isolation, the risk profile is elevated when the indicators are aggregated and correlated, especially with psycho-social data via HR feeds.

More than one response permitted.



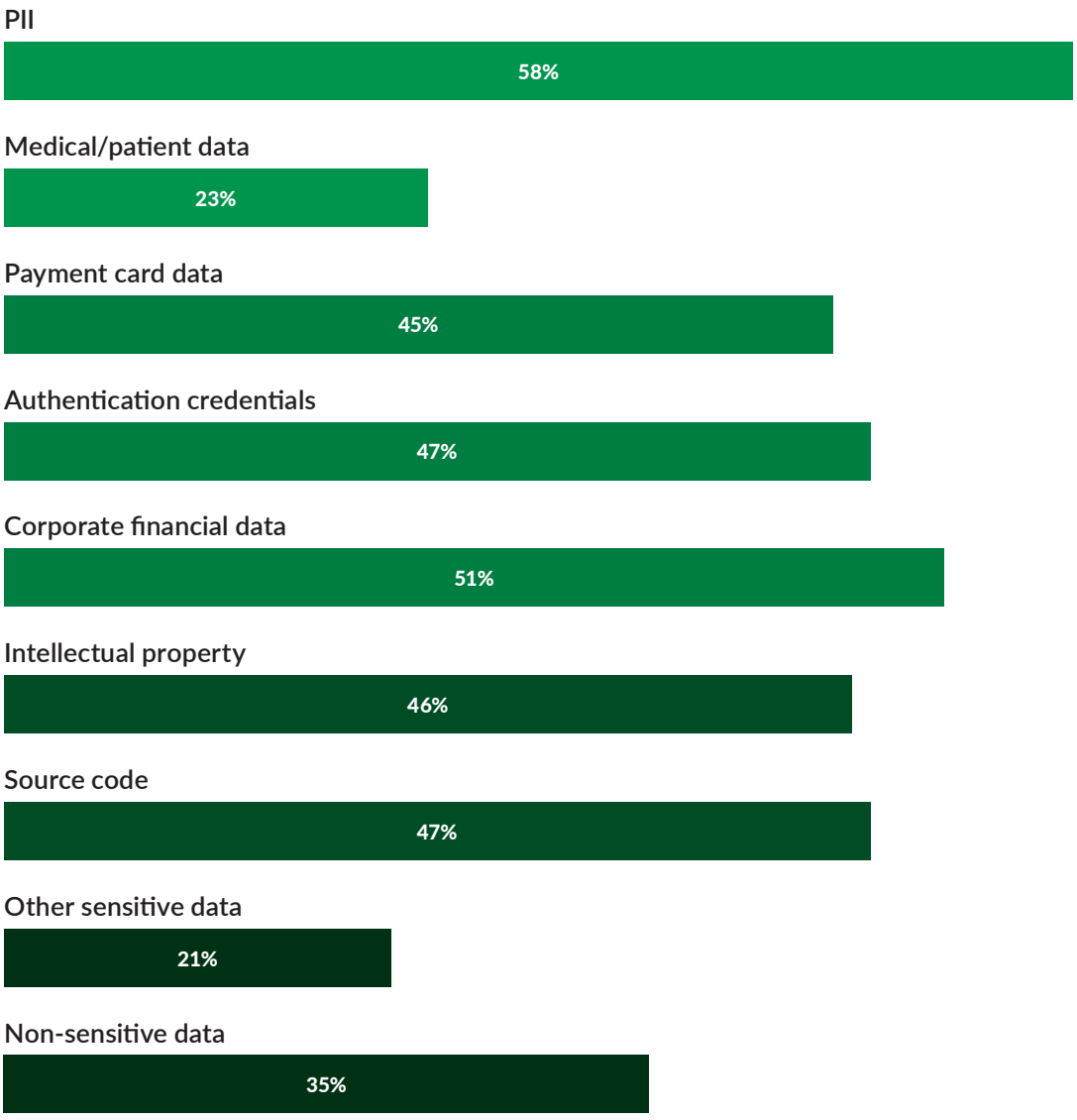
Total (FY2023) = 499%

Figure 19. Which data types were involved in the insider incidents?

Intellectual property (IP) holds the most value for organizations and is involved in nearly half of all insider incidents.

Intellectual property can be sensitive or non-sensitive. Sensitive IP can include customer data, employee data, health records, sales contracts and more, often via clipboard and device sync capabilities, while non-sensitive IP can include corporate presentations and templates.

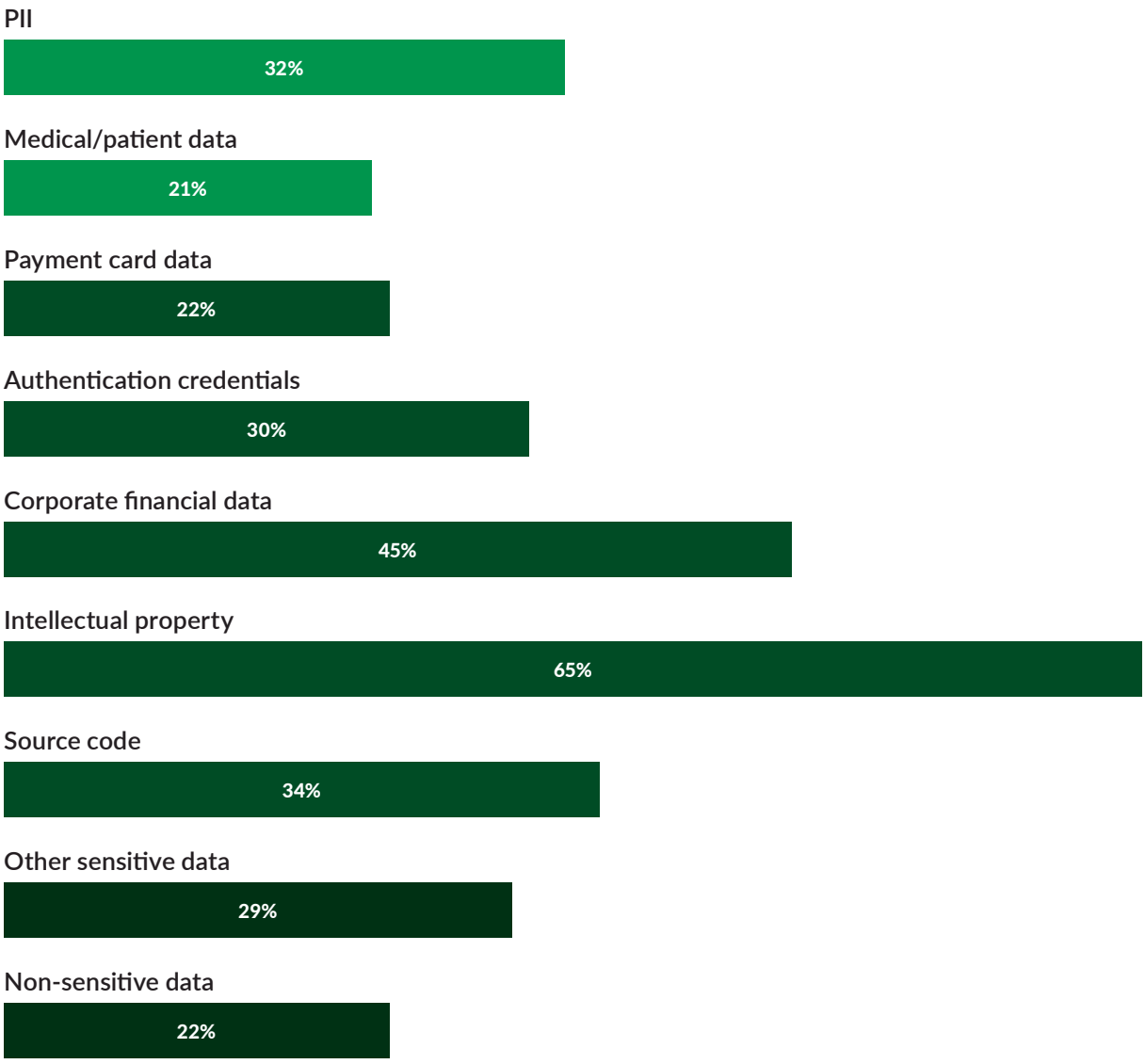
More than one response permitted.



Total (FY2023) = 373%

Figure 20. Which data types are the most valuable to your organization?

Three responses permitted.

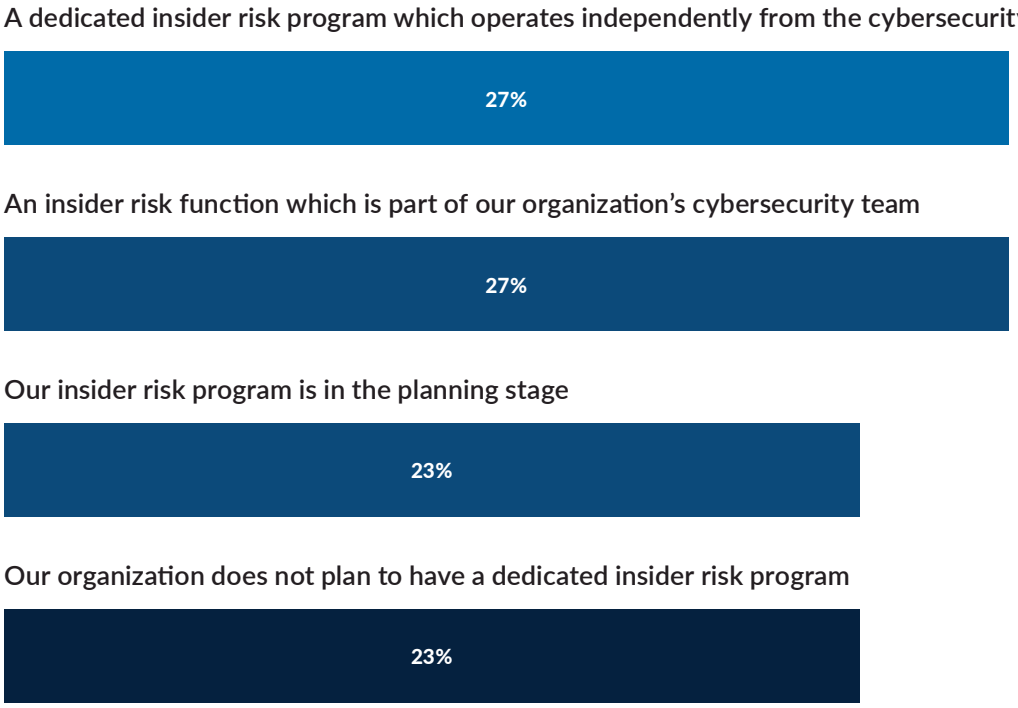


Total (FY2023) = 300%

Figure 21. Does your organization have a dedicated insider risk program?

Having a human-centric insider risk program has become a top priority for most organizations.

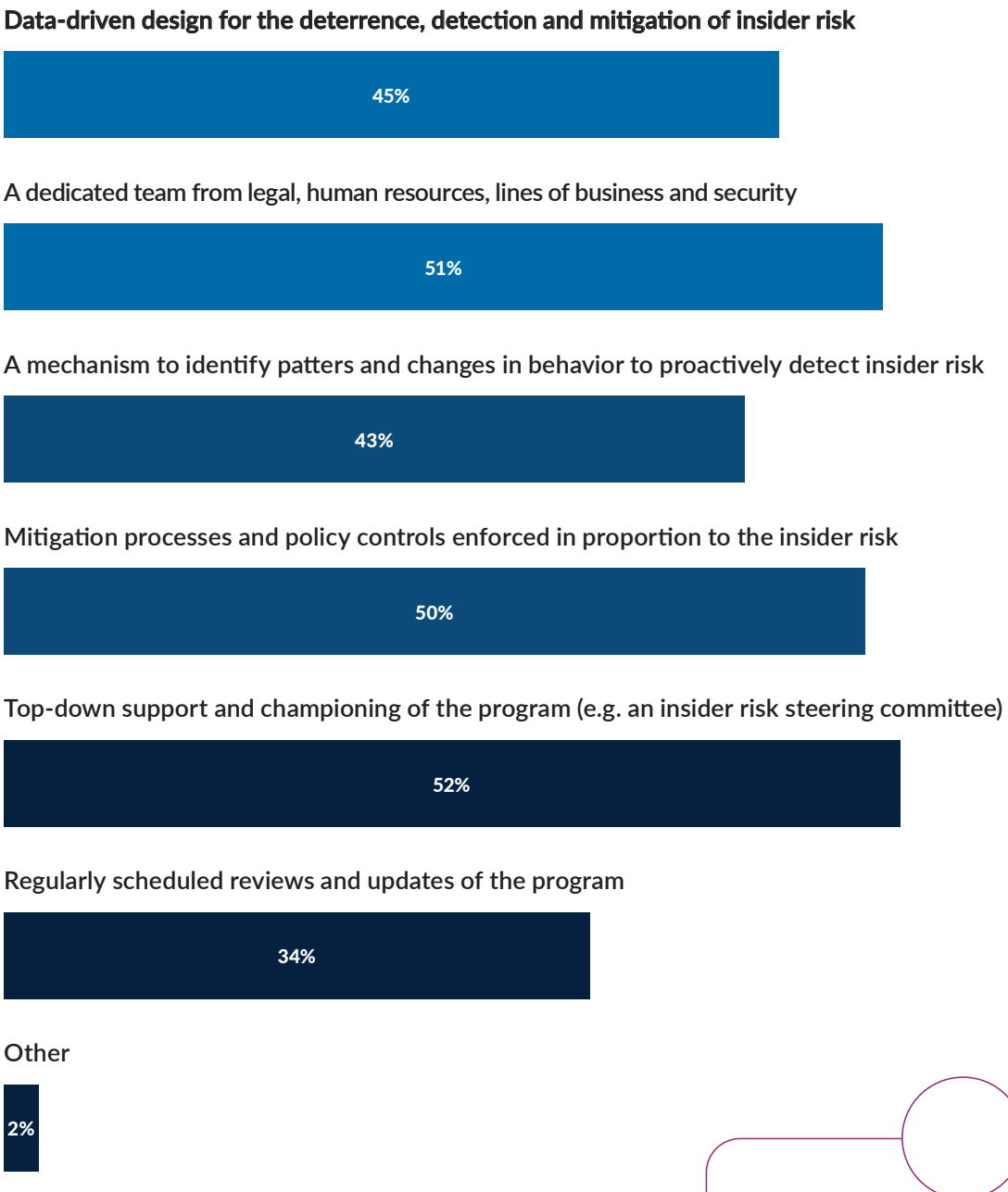
Seventy-seven percent of organizations are planning or have started an insider risk program. More than half (52%) believe top-down support is a key feature of an insider risk program, while 51% believe the program should include a cross-functional dedicated team.



Total (FY2023) = 100%

Figure 22. If your organization has or will have a dedicated insider risk program, what features are/will be included?

More than one response permitted.



Total (FY2023) = 277%

Figure 23. What are the primary business reasons for having an insider risk program?

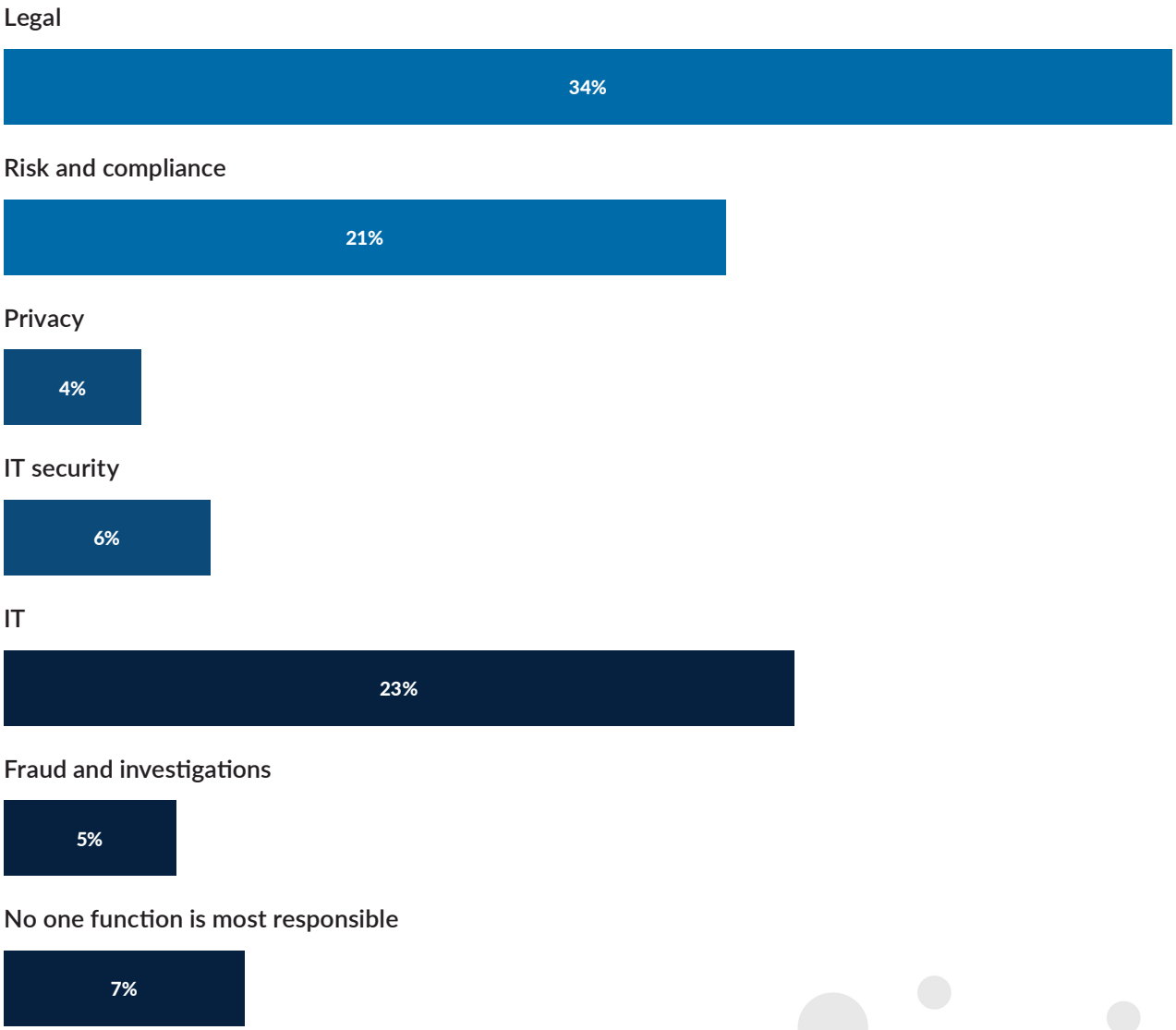
Customer and partner requirements, the demands of a hybrid workforce and industry regulations are the primary business reasons for having an insider risk program.

More than one response permitted.

Total (FY2023) = 261%

Figure 24. Which department is most responsible for insider risk management in your organization?

Legal (34%), IT (23%) and risk and compliance (21%) typically bear the most responsibility for insider risk management.

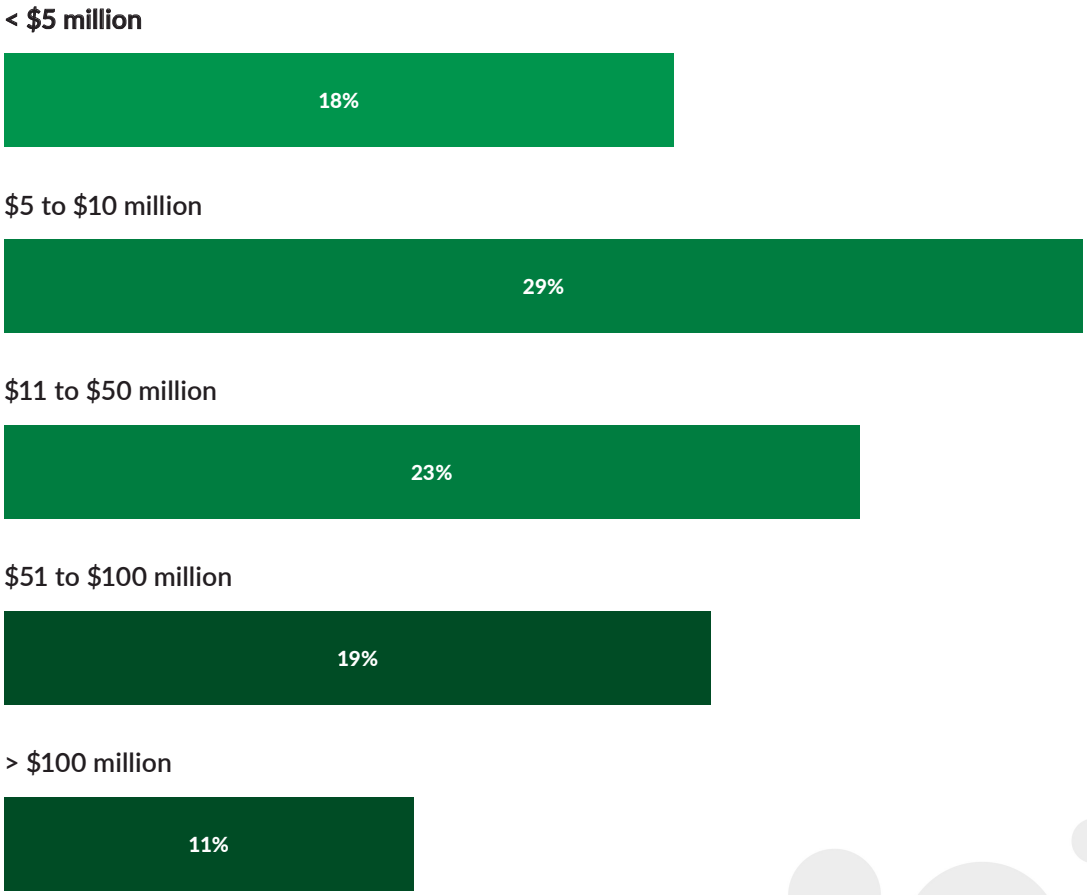


Total (FY2023) = 100%

Figure 25. Approximately, what is the dollar range that best describes your organization's IT security budget this year?

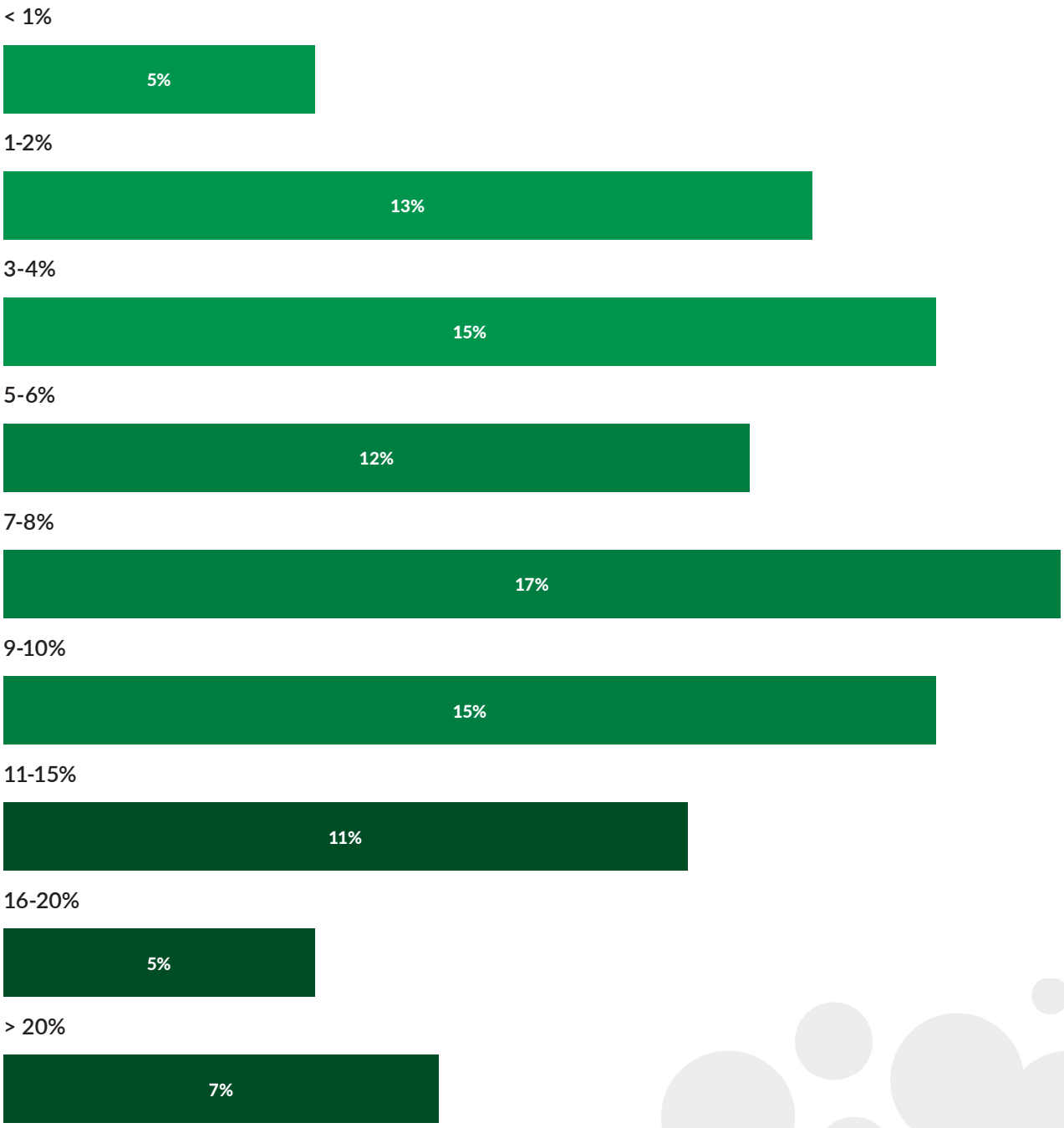
Organizations are trying to fix a $16.2 million problem with just 8.2% of their overall IT security budget.

Organizations had an IT security budget of $2,437 per employee, yet only 8.2% ($200 per employee) was allocated specifically to insider risk management programs and policies.



Total (FY2023) = 100%

Figure 26. What percentage of your organization's IT security budget is allocated to insider risk management?



Total (FY2023) = 100%

Conclusions

If the findings from our study reveal anything, it's that more energy is required to fund and drive proactive insider risk management.

To stop insider risks from escalating into costly incidents, organizations must prioritize a proactive and human-centric approach that cuts across people, processes, technology, and systems. Having an insider risk program can no longer be perceived as a "nice to have", but rather the backbone from which all preventative insider risk mitigation efforts flow.

To date, most budgets have been pivoted on post-incident activities. In fact, of the 8.2% budget allocated to insider risk management, 91.2% is spent reacting to the incident.

This has to change.

To get left of boom, organizations must focus their energy on activities that are specifically designed to prevent insider incidents from occurring in the first place. This is where artificial intelligence (AI) offers great potential.

Figure 27. Insider risk: Cost vs budget

The power of AI

It is encouraging that most organizations (64%) consider AI and machine learning (ML) "essential" to preventing insider incidents. Understanding why people become insider risks means understanding human behavior and why people do the things they do — and AI can help achieve this in spades.

Using AI and ML, analysts can capture early warning signals and apply analysis quickly, easily and at scale. In the case of non-malicious insiders, AI can also help drive automated education and awareness communications to provide "teachable moments" to risky employees in near real time. Given non-malicious insiders are behind most incidents (75%), this is a powerful way for organizations to proactively exercise proportionality when resolving insider risks in a way that is both cost effective and fair.

May 2023

MARKET REPORT

2023 spear-phishing trends

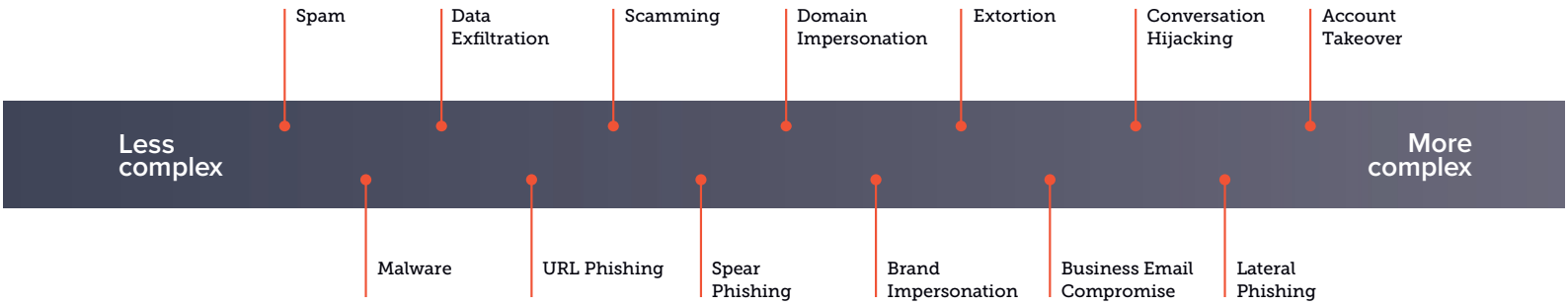
Key findings about the impact of attacks and the challenges of threat detection and response »

Barracuda®
Your journey, secured.

Designed to evade traditional email security, including gateways and spam filters, spear-phishing attacks are often sent from high-reputation domains or already-compromised email accounts. Spear-phishing emails do not always include malicious links or attachments. Since most traditional email-security techniques rely on blocklists and reputation analysis, these attacks get through. Attacks typically use spoofing techniques and include "zero-day" links — URLs hosted on domains that haven't been used in prior attacks or that have been inserted into hijacked legitimate websites — so they are unlikely to be blocked by URL-protection technologies.

Cybercriminals also take advantage of social-engineering tactics, including urgency, brevity, and pressure, in their spear-phishing attacks in order to increase the likelihood of success.

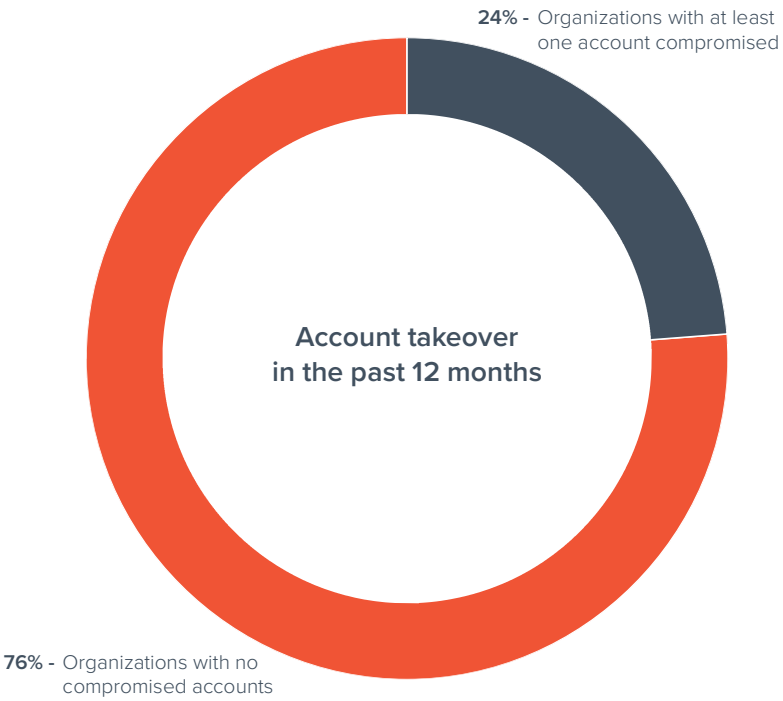
13 email threat types



Account compromise or account takeover is often the result of phishing attacks. Hackers use social engineering tactics to trick users into disclosing their login credentials, which are then used to get inside an organization's network. Once inside, hackers can spread laterally within an organization, compromising more valuable accounts or using compromised accounts as launch pads for further attacks.

In 2022, based on Barracuda's data and analysis, nearly one in four organizations (24%) had at least one email account compromised through account takeover. Hackers sent an average of 370 malicious emails from each compromised account.

The rest of this report looks at the experience of spear-phishing around the world, the impact of attacks, detection and response challenges, and a variety of related issues.



The impact and costs of spear-phishing attacks

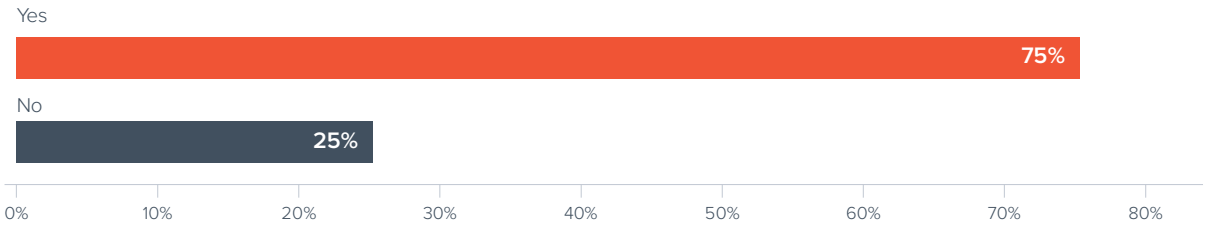
While spear-phishing attacks are low volume, they are widespread and highly successful compared to other types of email attacks.

The success of spear-phishing attacks

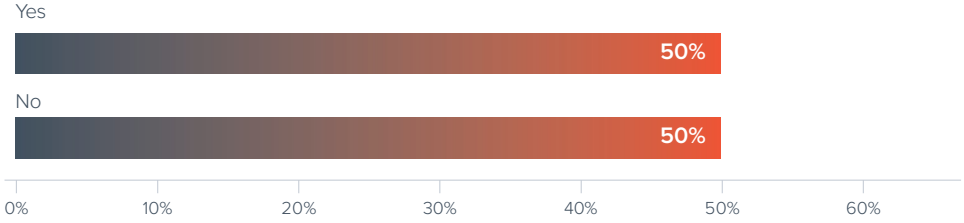
Three-quarters of respondents surveyed said they fell victim to an email attack in the last 12 months. Half said they were the victims of spear phishing. That means 2 out of 3 successful email attacks are spear-phishing attacks that use personalized messages, social engineering, and other tactics.

This is significant because these attacks make up only 0.1% of all email-based attacks according to Barracuda's data but are responsible for 66% of all breaches. On the other hand, high-volume attacks such as spam and malware, make up 16% of emails but are only responsible for one-third of breaches. Spear-phishing protection is critical because even just one successful attack can be devastating.

Has your organization faced any successful email-based attacks in the past year? (n=1,350)

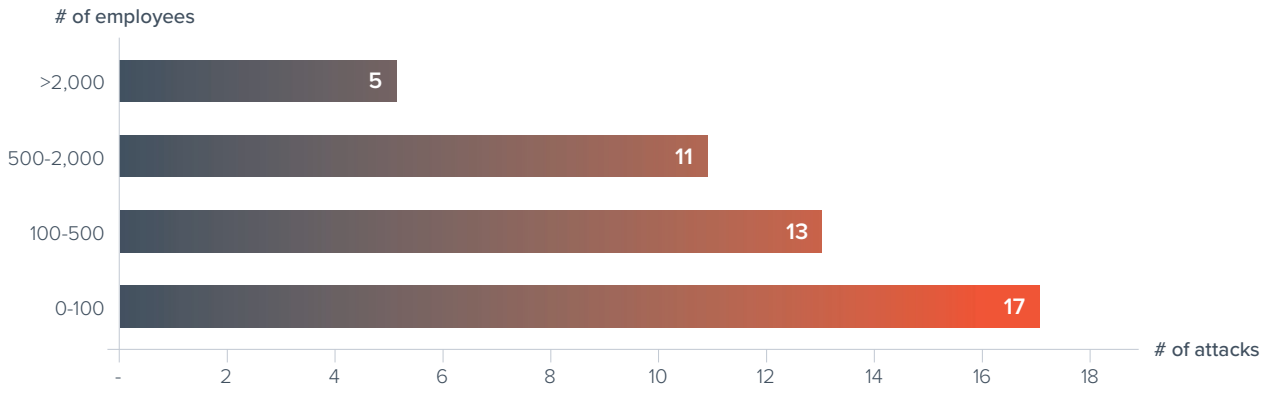


Was your organization a victim of spear phishing in the past 12 months? (n=1,350)



While smaller organizations report fewer successful email attacks caused by spear phishing (42%), Barracuda's 2022 report, Spear Phishing: Top Threats and Trends (Volume 7), showed that smaller businesses are being disproportionately attacked, with a higher average number of social engineering attacks per mailbox. Smaller organizations don't often have the tool necessary to identify and block sophisticated attacks or even identify and respond to attacks in progress. Many may not be aware of the volume of threats already in their users' inboxes.

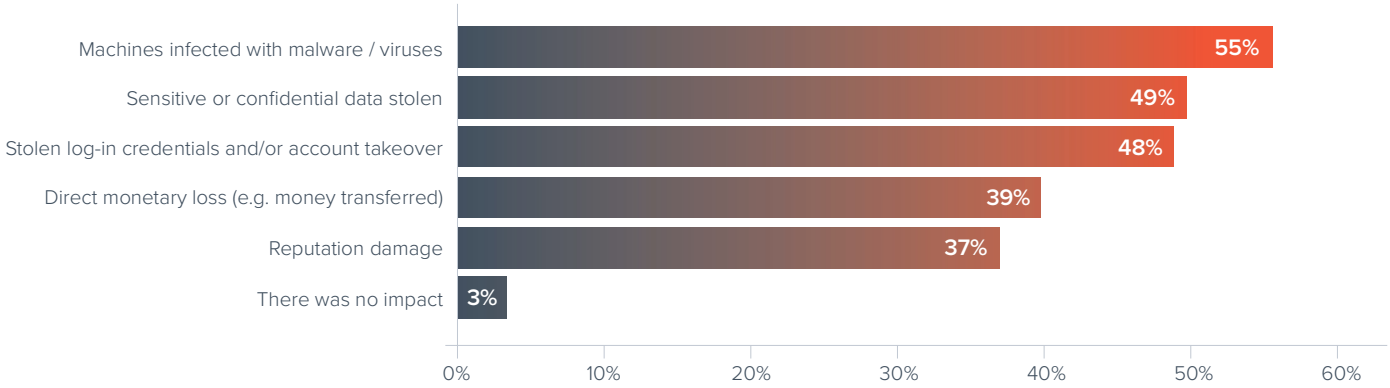
Average number of social engineering attacks per mailbox



According to our recent market survey, organizations using Gmail are more likely to report falling victim to spear-phishing attacks than those using Microsoft 365 — 57% of organizations using Gmail reported a successful spear-phishing attack, compared to 41% for those using Microsoft. In the Microsoft environment, there are many security options available to layer on, which provides better protection.

The impact of spear-phishing attacks

What was the imapct of the spear phishing attacks that occured in your organization in the past 12 months? (n=678)

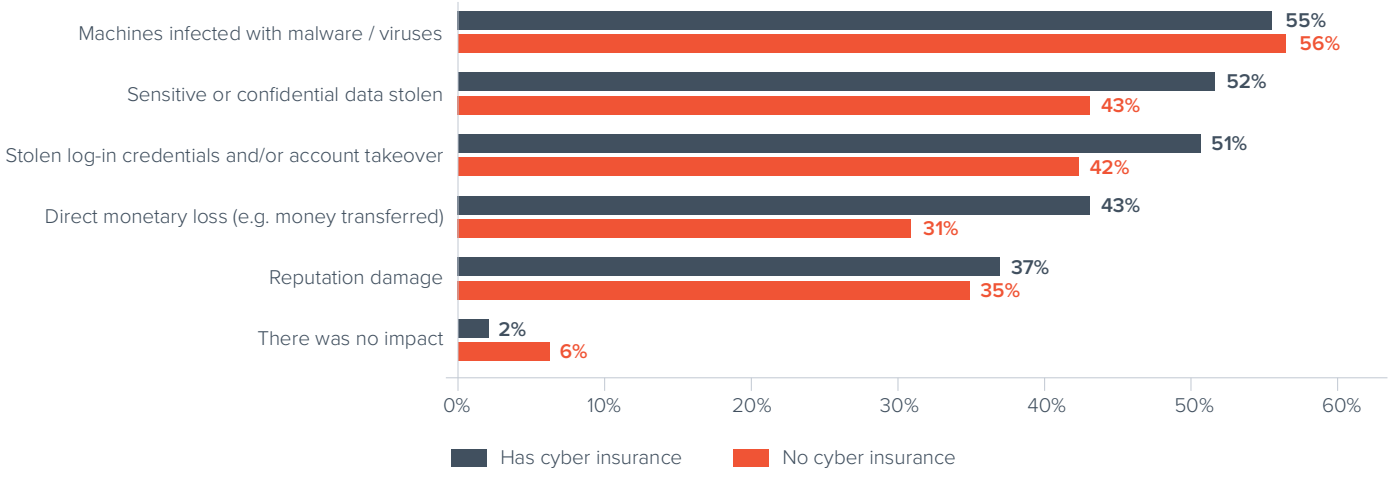


Nearly every victim of a spear-phishing attack in the last 12 months saw impacts on their organization, including malware infections, stolen data, and reputational damage. While a direct monetary loss is one of the effects, all the other impacts could also result in some financial damage for an organization as a result of an attack.

Hackers looking to launch malware attacks, such as those involving ransomware, often rely on phishing to get inside an organization. Stealing credentials is also a common goal of these attacks, as scammers are increasingly relying on spear-phishing tactics to gain access and then execute account takeover attacks. Of those who reported being a victim of a spear-phishing attack in the last 12 months, nearly half said they were the victims of stolen log-in credentials and/or account takeover.

For organizations with no cyber insurance in place, infected machines were the most frequently cited impact of spear-phishing attacks. While those that have cyber insurance also experienced this impact, they were more likely to experience other effects, including stolen information, stolen credentials, and direct monetary losses. The difference could be that only companies with sensitive information to steal would cite that as an impact. It's also possible that companies aren't aware of these problems and aren't looking for impacts, like the loss of sensitive information or stolen credentials.

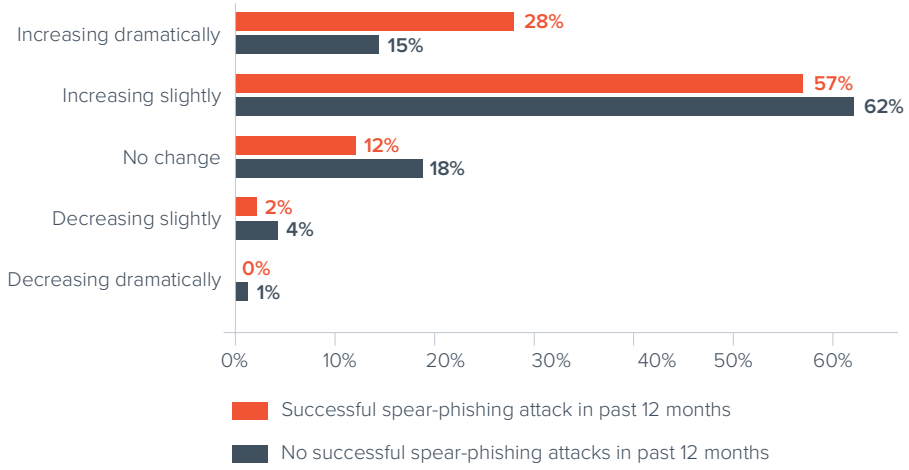
What was the impact of the spear phishing attacks that occured in your organization in the past 12 months? (n=678)



The costs of spear-phishing attacks

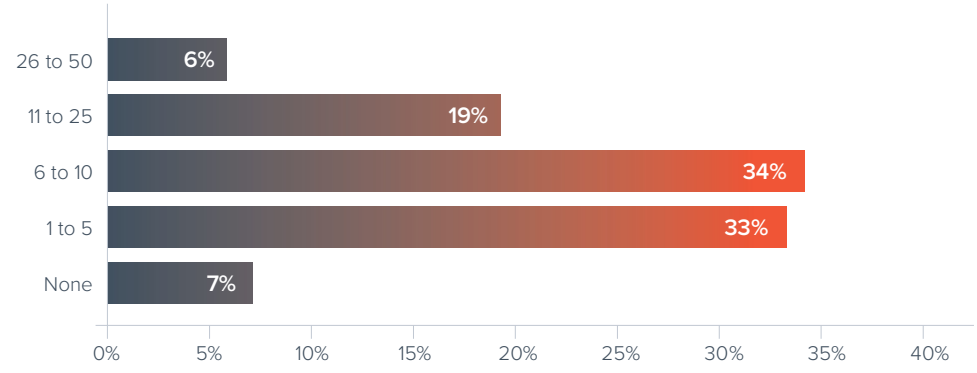
Organizations hit with a spear-phishing attack were more likely to say the costs associated with an email security breach had increased dramatically in the last year — 28% versus 15% of those who hadn't been victims of spear-phishing. These organizations are also more likely to have higher overall recovery and impact costs for the most expensive attack they suffer — an average of $1.1 million compared to $760,882 for those who were the victims of other types of email-based attacks.

How has the total cost of email security breaches changed over the past 12 months? (n=1,003)



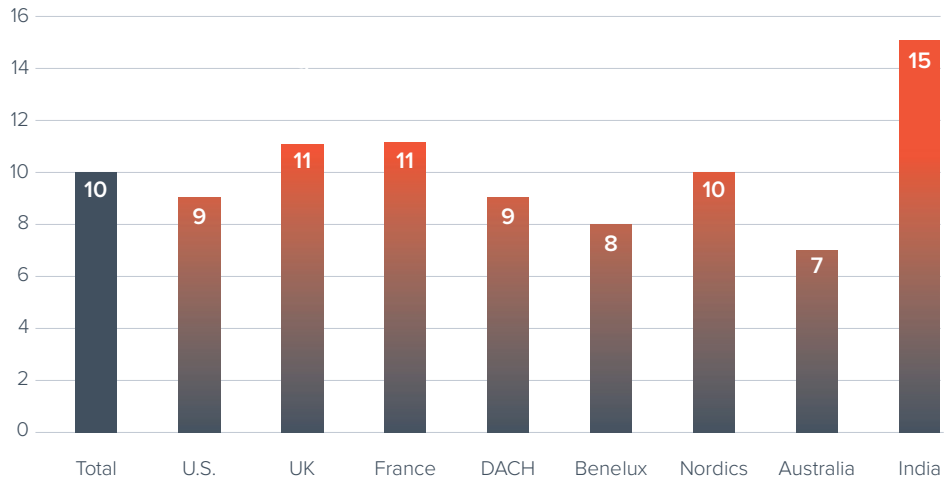
93% of organizations had users report suspicious messages post-delivery

Approximately how many suspicious emails are reported to your organization's IT on a typical work day? (n=1,350)



An average of 10 suspicious emails are reported to IT on a typical workday

Approximately how many suspicious emails are reported to your organization's IT on a typical work day? (n=1,350)



By region, users in India report the highest average number of suspicious emails per day — 50% more than the global average. This could be evidence that organizations are struggling to prevent email-based attacks or that organizations in India are placing a higher focus on suspicious emails and are discovering and reporting a higher average as a result. However, a large number of messages being reported is not always a good thing; it could also mean users are reporting a lot of gray mail or unwanted messages rather than malicious emails.

7% of organizations worldwide don't have any emails being reported by their users. In DACH and Australia, the numbers are particularly high, with 14% saying no emails are reported. These regions also have below-average levels of adoption of computer-based security awareness training. While the global average is 42%, in Australia, it's 28%, and in DACH, it's 37%. Lower investment in security awareness may have contributed to users being less vigilant or less able to recognize a potential email threat.

Based on the highly personalized nature of spear-phishing emails and the potentially severe impacts of a successful attack, every organization, regardless of size and location, should take the appropriate precautions to prevent these attacks.

Proportionately, users in larger organizations report fewer suspicious emails

The number of attacks being reported by users isn't proportionate to the size of their organizations. Organizations with 100-249 employees have an average of 7 suspicious emails reported per day, while at businesses with 1,000-2,500 employees, users report an average of 12 per day. As we have seen previously, smaller organizations actually receive a larger volume of spear-phishing attacks proportionate to their size.

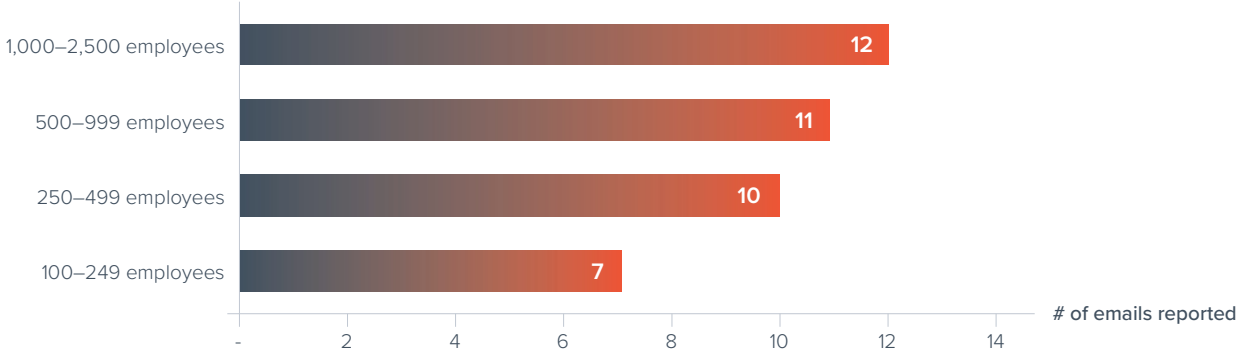
This larger volume of attacks and some potentially overzealous reporters could mean that IT teams need to process a larger number of messages. Unfortunately, smaller organizations have smaller IT teams, so they don't always have enough tools and resources to process all potential incidents.

Larger organizations are more likely to leverage tools and resources to help prioritize incidents that need to be addressed and quickly determine the difference between benign and malicious emails.

Users in companies with more than a 50% remote workforce report higher levels of suspicious emails — 12 per day on average, compared to 9 per day for those with less than a 50% remote workforce. Due to the dispersed nature of their employees, organizations with larger remote workforces are more sensitive to potential threats. Given that they are more likely to fall victim to a spear-phishing attack, they may welcome some overreporting from their users.

At organizations hit with multiple ransomware attacks, employees also report higher levels of suspicious emails — a daily average of 17 suspicious emails for businesses hit with three or more ransomware attacks. Security awareness among users in organizations is likely to increase after ransomware attacks, possibly leading to users overreporting

Approximately, how many suspicious emails are reported to your organization's IT on a typical work day? (average) (n=1,350)



Threat detection and response challenges

No security is effective 100 percent of the time. When a threat gets through, security teams need to act fast to identify and respond before it spreads and causes extensive damage. Faster detection and response times lower the risk of a security breach.

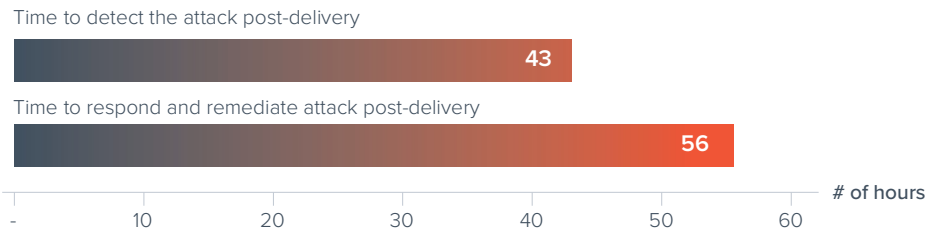
On average, organizations take nearly 100 hours to identify, respond to, and remediate a post-delivery email threat

With an average detection time of 43 hours and an average response and remediation time of 56 hours for post-delivery email threats, organizations take almost 100 hours to deal with an email security incident.

For 1 in 5 organizations (22%), it takes longer than 24 hours to identify an email attack. This long period gives users ample time and opportunity to click on a malicious link or respond to an email. When that happens, hackers are able to use the compromised account to get inside the network and potentially compromise additional accounts. If long detection times aren't concerning enough, 38% of respondents reported taking more than 24 hours to respond to and remediate attacks once they become aware of them.

Detection, response, and remediation times are shorter on average for larger organizations, which typically have more resources available and can respond more quickly. While the larger size has the potential to make the company susceptible to more threats, a larger team is likely available to help with efforts to detect, respond to, and remediate any impacts from attacks.

Thinking about your detection and response times of post-delivery or reported email incidents, aproximately how long does it take for your organization to do the following? (hours) (n=1,350)

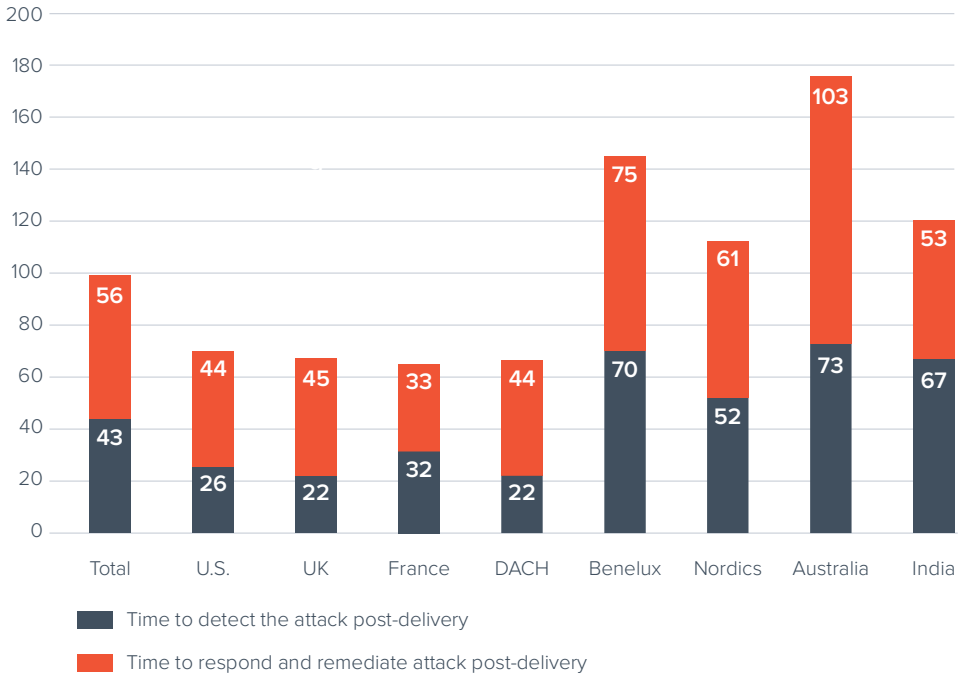


Investment in automation and security training cuts response times

Australia's low adoption rate (24%) for automated incident response may very well be a factor for their long response times. Australia also has the lowest adoption rates of computer-based security awareness training. The responsibility to uncover and respond to post-delivery threats falls mostly on IT, which takes too long without the necessary tools — 175 hours on average in Australia.

On the other hand, 36% of organizations in the United States use automated incident response, and 45% use computer-based security awareness training. They also report faster response times on average, which means they are using fewer IT resources and those resources can focus on other tasks.

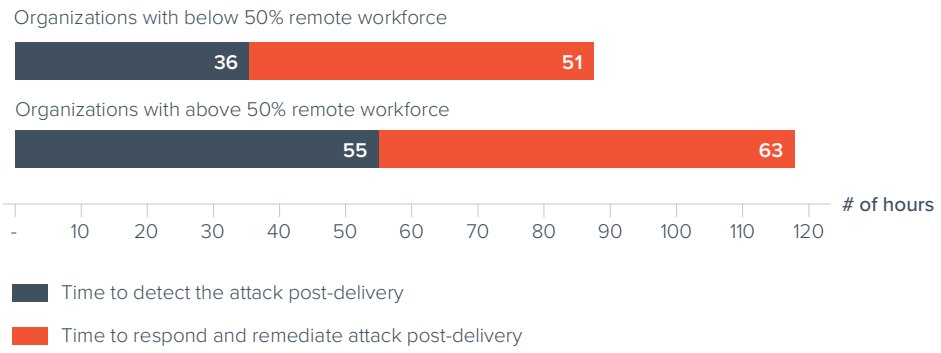
Thinking about your detection and response times of post-delivery or reported email incidents, aproximately how long does it take for your organization to do the following? (hours) (n=1,350)



Having more remote workers slows detection and response time

It takes organizations with more remote workers longer to both detect and respond to email security incidents. Organizations with less than a 50% remote workforce had average detection times of 36 hours, while those with more than a 50% remote workforce took an average of 55 hours to detect an email security incident. Likewise for remediation: Those with less than a 50% remote workforce had an average response and mitigation time of 51 hours, while those with more than a 50% remote workforce took an average of 63 hours to respond to and mitigate an email security incident.

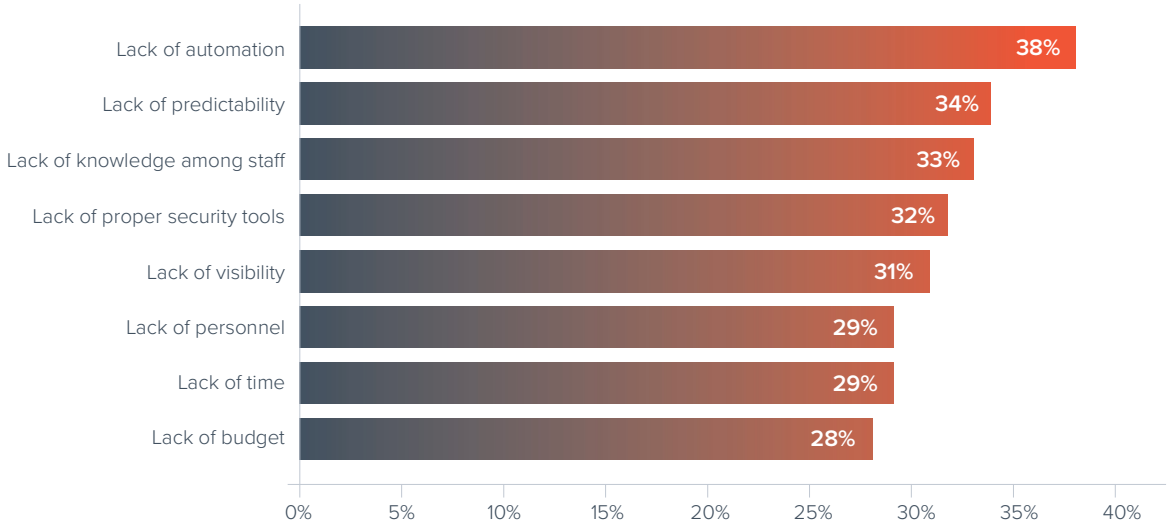
Thinking about your detection and response times of post-delivery or reported email incidents, aproximately how long does it take for your organization to do the following? (hours) (n=1,350)



Lack of automation is a top obstacle

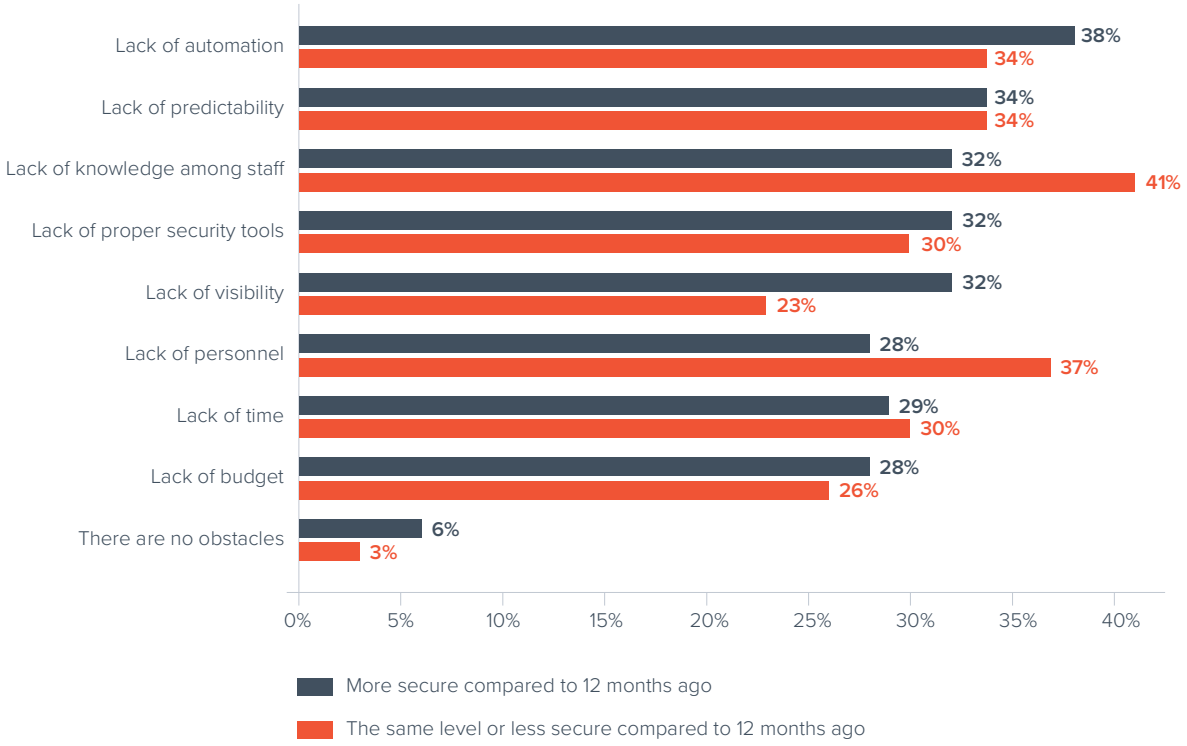
Larger organizations cite lack of automation as the most likely obstacle preventing a rapid response to an incident — 41% for organizations with more than 250 employees, compared to 28% for organizations with 100–249 staff. These smaller companies cite additional reasons almost equally, including the lack of predictability (29%), knowledge among staff (32%), and proper security tools (32%). Smaller companies appear to be still in the process of adopting appropriate tools and appear to have difficulty hiring and retaining knowledgeable staff. Once organizations have the right people, processes, and technology in place, they can take advantage of accelerators available to expedite response work, including automation.

What are the main obstacles that prevent fast detection and response to post-delivery email threats in your organization? (n=1,350)



Companies that feel more secure also say lack of automation is the most likely obstacle to fast incident response. In contrast, companies that feel less secure cite a lack of knowledgeable staff. Having knowledgeable staff is a prerequisite to having a strong incident response program, and automation can help significantly accelerate that response.

What are the main obstacles that prevent fast detection and response to post-delivery email threats in your organization? (n=1,350)



Best practices to defeat spear phishing

As email attacks evolve and become more sophisticated, organizations are facing serious threats from targeted spear-phishing attacks. The impact of just one successful attack can be devastating. To protect your business, you must invest in technology that blocks attacks and in training that helps people act as the last line of defense.

Technology

- **Take advantage of artificial intelligence.** Scammers are adapting email tactics to bypass gateways and spam filters, so it's critical to have a solution in place that detects and protects against spear-phishing attacks, including business email compromise, impersonation, and extortion attacks. Deploy purpose-built technology that doesn't solely rely on looking for malicious links or attachments. Use machine learning to analyze normal communication patterns in your organization and to spot anomalies that may indicate an attack.

- **Deploy account-takeover protection.** Ensure scammers aren't using compromised accounts in your organization to launch spear-phishing attacks. Use technology with artificial intelligence to recognize when accounts have been compromised and that remediates in real time by alerting users and removing malicious emails sent from compromised accounts.

- **Monitor inbox rules and suspicious logins.** Use technology to identify suspicious activity, including logins from unusual locations and IP addresses, a potential sign of a compromised account. Be sure to also monitor email accounts for malicious inbox rules, as they are often used to hide or delete emails sent as part of an account-takeover attack.

- **Use multifactor authentication.** Provide an additional layer of security above and beyond username and password, such as an authentication code, thumb print, or biometric authentication.

- **Implement DMARC authentication and reporting.** This helps defeat domain spoofing, one of the most common techniques used in impersonation attacks. Stop domain spoofing and brand hijacking with DMARC authentication and enforcement. Accurately set enforcement rules for your organization with the help of DMARC reporting and analysis.

- **Automate incident response.** With an automated incident response solution, you can quickly clean up any threats found in inboxes and make remediation more efficient for all messages going forward.

- **Train staffers to recognize and report attacks.** Educate users about spear-phishing attacks by making it a part of security awareness training. Ensure staffers can recognize these attacks, understand their fraudulent nature, and know how to report them.

- **Maximize data-loss prevention.** Use the right combination of technologies and business policies to ensure emails with confidential, personally identifiable, and other sensitive information are blocked from leaving the company.

About Barracuda

At Barracuda, we strive to make the world a safer place.

We believe every business deserves access to cloud-first, enterprise-grade security solutions that are easy to buy, deploy, and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey.

More than 200,000 organizations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level

Get more information at barracuda.com.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research in the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision-makers across technical and business functions in all business sectors and all major markets.

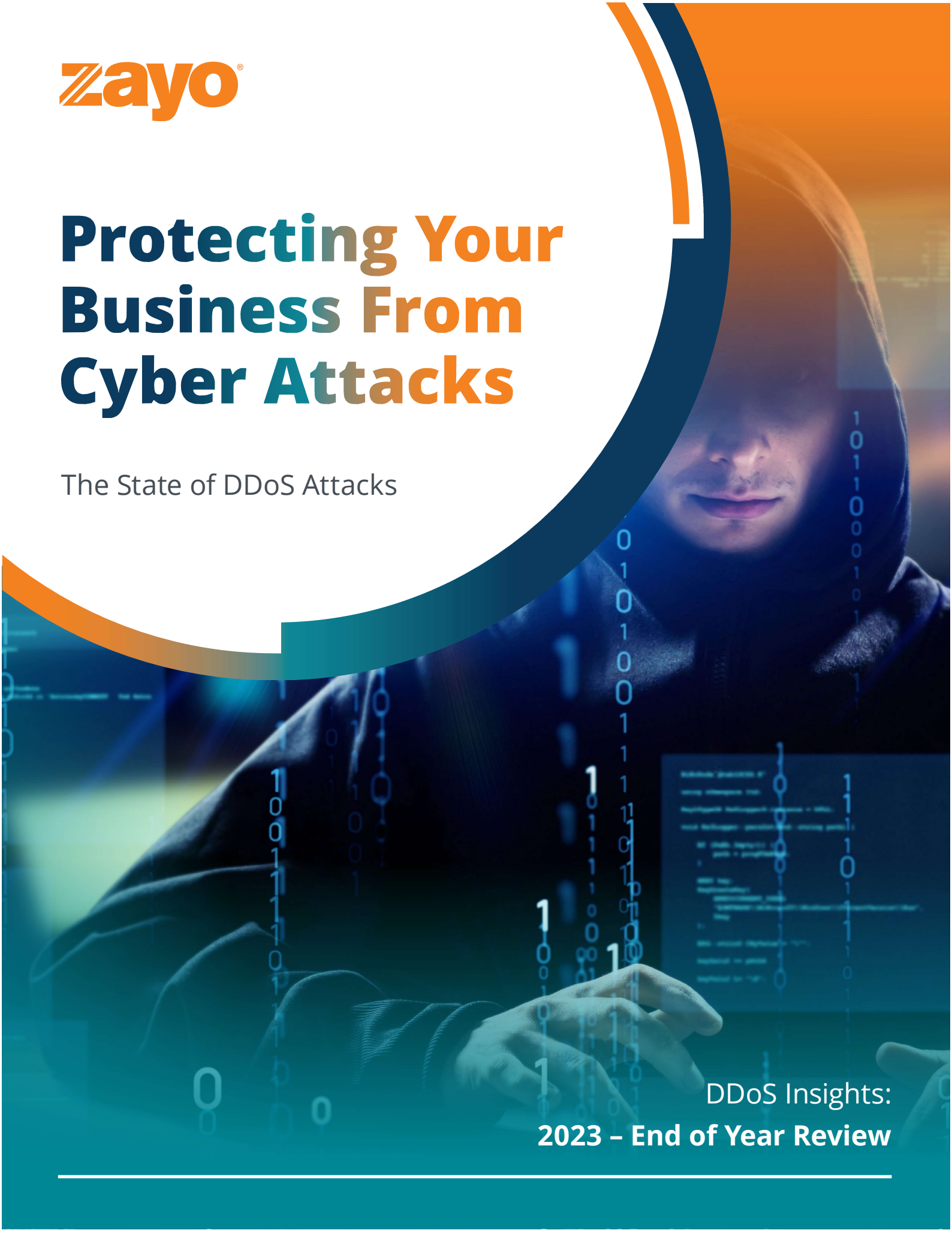
For more information, visit vansonbourne.com.

Barracuda®
Your journey, secured.

zayo

Protecting Your Business From Cyber Attacks

The State of DDoS Attacks



DDoS Insights:

2023 – End of Year Review

Executive Summary

Large fluctuations in DDoS attack activity quarter over quarter through 2023 still point to a **16% overall increase** over the course of the year. Telecom, retail, healthcare, and government were hit especially hard.

In the second half of 2023, once again **telecommunications** companies experienced the **most frequent attacks**, comprising about 40% of total attack volume with nearly 13,000 attacks over the course of these 6 months.

An astonishing second quarter of attacks (up 387% from Q1), seems to have leveled in the second half of the year. Across all industries comparing Q4 to Q1 2023, companies saw a 16% increase in attack activity.

In the second half of 2023, **government** once again experienced the **longest attacks** with the average attack duration increasing from 4 hours in the first half of the year, to **18 hours** in the second half, representing an increase of 322%.

Across all industries, attackers are launching more persistent, longer attacks. The average duration of attacks increased by over 400% from Q1 to Q4 2023, from an average of 24 minutes per attack in Q1, to 121 minutes per attack in Q4.

Retail and **healthcare** companies experienced the **largest attacks** in the second half of the year, with an average attack size of **2.5 Gbps** across companies in these two industries.

Across all industries in the second half, attack size has dropped. However, even the smallest attack can cause business reputational – and financial – harm. Plus the drop in attack size points to a troubling emerging trend: the increasing use of multi-vector attacks.

Across all industries, organizations experienced 110 attacks on average over the 6 month time frame - **4 attacks every week.**

The Cost of Exposure: No matter the attack frequency, duration, or size, unprotected organizations experienced an average cost of $6,000 per minute of each DDoS attack.

Factors such as lost revenue, the cost of detection and recovery, legal fees, reputational harm, customer churn, opportunity costs during downtime, and many other factors, can easily surpass **$150,000 for a single 20-minute attack**.

DDoS 101

A Distributed Denial of Service (DDoS) attack is a deliberate cyber attack against an organization's online presence.

A DDoS attack, launched simultaneously from multiple systems, floods a victim's Internet circuit with fake or illegitimate traffic to prevent true user traffic from passing. DDoS attacks are more common than phishing, spoofing, insider threats and DNS tunneling attacks.

DDoS attacks are **always** deliberate.

In the second half of 2023, DDoS attackers targeted:

Enterprises across all industries | Very large to very small companies | Airports, hospitals, utilities, and other critical infrastructure | Federal, state, and local governments – including schools | Telecom and cloud companies | Many more

And they attack organizations multiple times.

One example: in Q4 2023, Zayo mitigated **over 140 individual DDoS attacks** launched against a single consulting firm. The firm was protected by Zayo, so their business was unimpacted.

This report contains insights, analysis, and conclusions about each industry under attack. Further, it provides you the steps to take to ensure your business isn't harmed by the DDoS attacks heading your way.

Conclusion

DDoS attacks are here to stay. Year over year we're seeing growth in their frequency, length, and bandwidth power. Further, they're becoming more sophisticated, more automated, stealthier, and harder for attacked organizations to detect. DDoS Protection has largely kept pace, itself evolving to be able to protect organizations against attacks in real-time, and now, **proactively**.

Methodology

This report analyzed more than 103,000 threat detections and mitigations experienced by Zayo customers in 2023. The data, spanning 14 industries and regions across North America and Western Europe, covers the period from January 1 to December 31, 2023. Notably, 72,000 of these attacks occurred in the first half of 2023, and 31,000 occurred in the second half.

"Most people on the Internet aren't plotting a DDoS attack. But the Internet is a big place, and Dark Web crime is the fastest growing business on earth. **Attackers are leveraging sophisticated technologies and cutting edge techniques to** innovate the ways they **deceive**, **disrupt** and **destroy our most critical data.**"

- Eric O'Neill, National Security Strategist, Carbon Black

Table of Contents

Executive Summary ii

DDoS 101 iii

Let's Begin 1

The Frequency of DDoS Attacks 4

The Duration of DDoS Attacks 12

The Time of DDoS Attacks. 19

The Size of DDoS Attacks. 21

The Future of DDoS Attacks 27

Time to Exhale. 30

Let's Begin

Welcome to Zayo's DDoS Insights Report for year end 2023.

This report reviews DDoS attack data collected from Zayo's network-based DDoS protected customers. Within this report, we illustrate who is being attacked, how frequently the attacks occur, when attacks occur, how long each attack lasts, and the size of the attacks.

The insights provided within this report illustrate the DDoS attack landscape across the businesses Zayo protects.

Ups and Downs - But Ultimately Up

For the customers Zayo protects, we've seen significant fluctuations in DDoS activity through 2023:

387% increase
in DDoS attacks
From Q1 to Q2

74% drop
in DDoS attacks
From Q2 to Q3

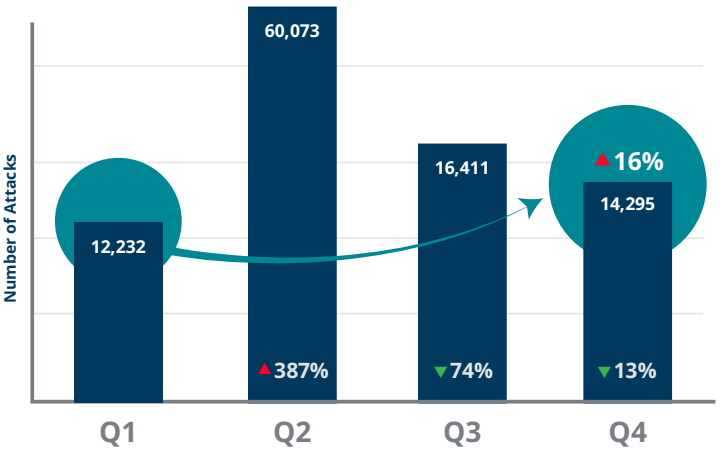
13% increase
in DDoS attacks
From Q3 to Q4

Comparing Q4 to Q1, 2023, there was a **16% increase** in attack activity across industries.

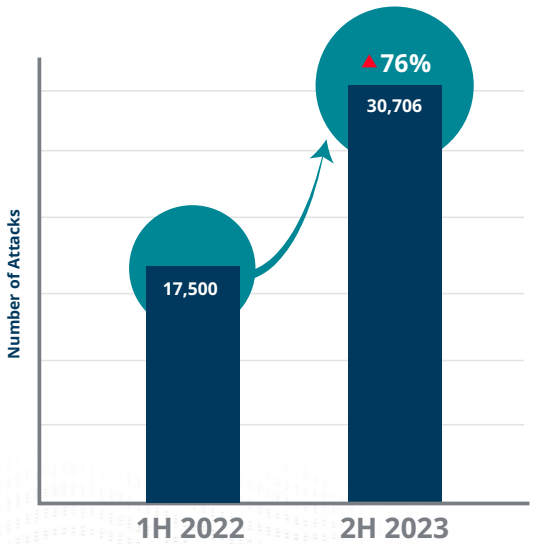
Past evidence and current environmental factors both point toward the inevitability of future increases in DDoS attacks in the years to come:

- Since early 2021, there has been a 150% increase in DDoS attacks globally.
- A new cyber attack occurs every 39 seconds.
- Some say there are approximately 23,000 DDoS attacks every day globally. Others claim over 40,000.
- DDoS attacks can be costly to any business, but unprotected businesses experience an average cost of $200K per attack. This too is rising.
- DDoS attack frequency rose 200% YoY from 1H22 to 1H23, and still managed to rise 76% from 1H22 to 2H23.

Number of Attacks Detected by Zayo Scrubbers (2023)

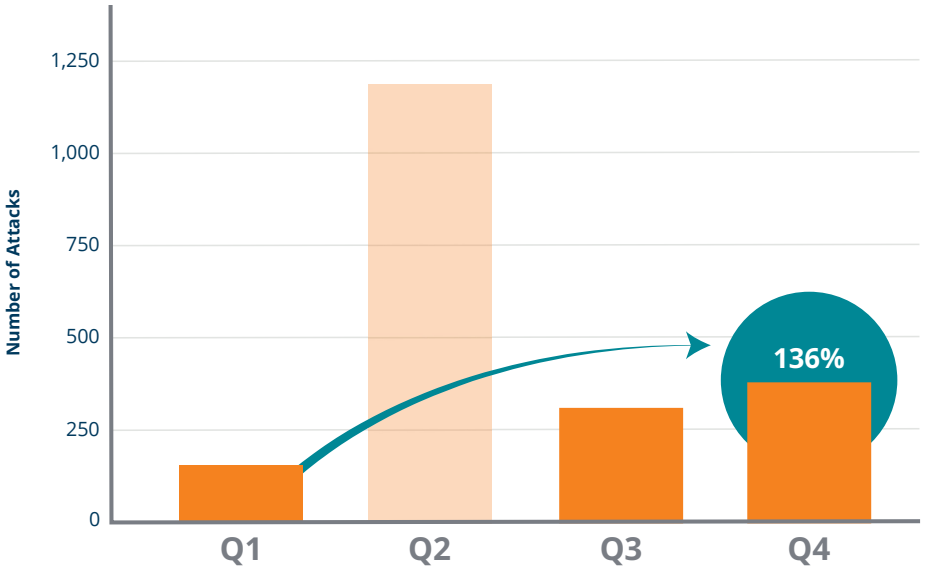


Number of Attacks Detected (Previous 24 Months)



Healthcare

Healthcare Total Number of Attacks (QoQ 2023)

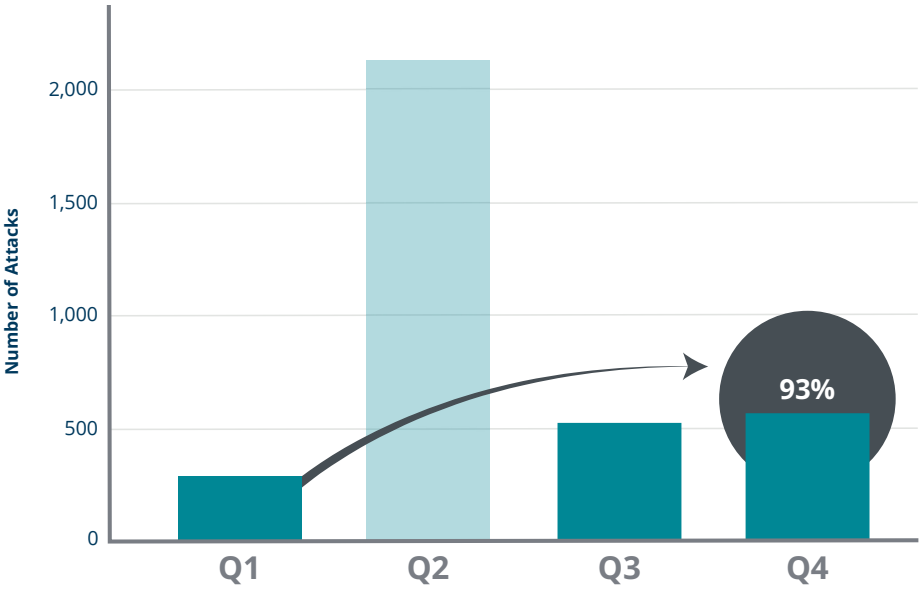


Healthcare continues to be a favorite target for DDoS attacks. DDoS attacks **increased 136%** from Q1 to Q4 2023. Healthcare continues its journey toward a full digital transformation. By 2027, healthcare companies will spend an estimated $974.5 billion on IT alone. DDoS attacks on healthcare aim to disrupt services, compromise patient data, or advance hacktivist agendas.

This sector must prioritize investing in security measures to safeguard both patients and digital assets.

Finance

Finance Total Number of Attacks (QoQ 2023)

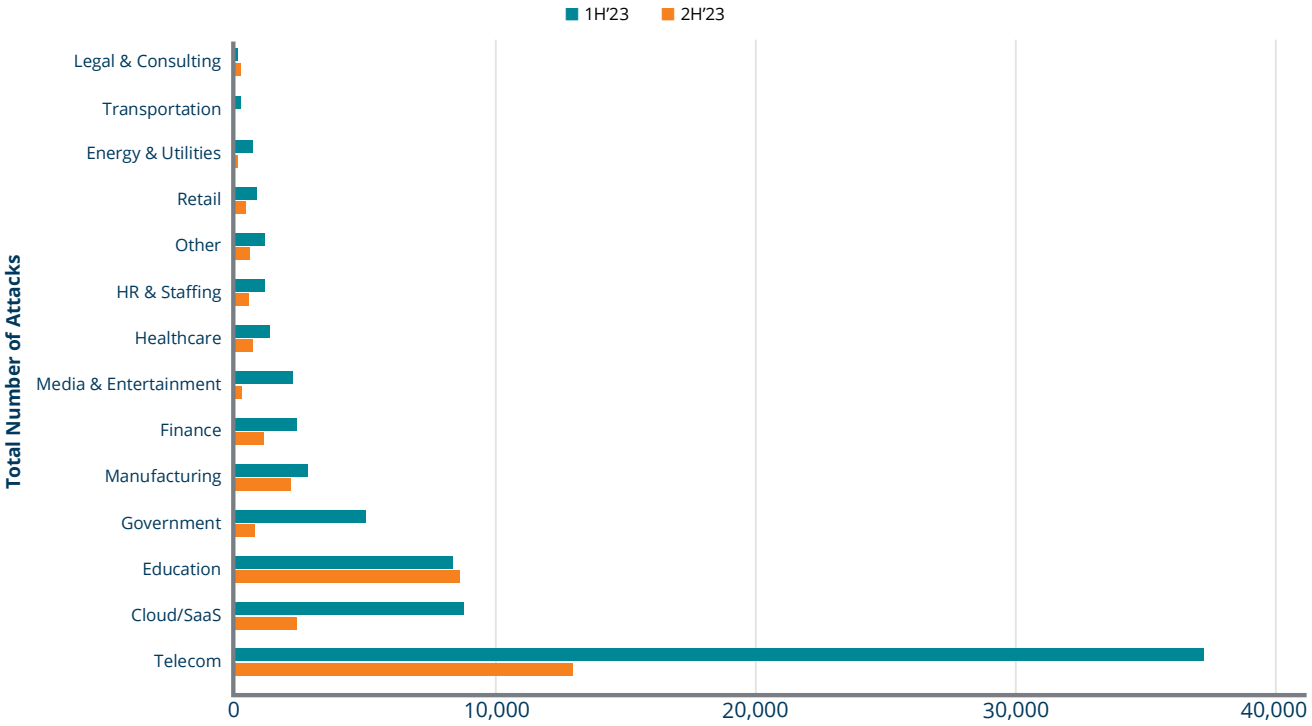


The finance industry is a high-value target for DDoS attackers. While it's never easy to divine the motive of an attacker, these companies could offer attackers an opportunity for financial gain through extortion, operational disruption, chaos, market manipulation, theft of sensitive customer data, and the advancement of hacktivist agendas.

"Law firms are pretty far from being attractive victims for cybercriminals. However, their clients — namely, secrets of their clients — make law firms a magnet for all kinds of cybercriminals."

- Ilia Kolochenko, Chief Architect at application security firm ImmuniWeb. **Source**

Total Number of Attacks Per Industry (1H 2023 vs 2H 2023)



The industries that experienced the most frequent attacks throughout 2023:

Telecommunications 49% of all attacks

Telecom accounted for almost half of all the DDoS attacks in 2023 (51% in the first half of the year, 42% in the second). Threat actors are targeting Internet providers directly, with destructive impact to their operations and their customers.

A devastating second quarter across all industries was especially bad for telecom. This industry was attacked 1,175% more in Q2 than in Q1. Why Telecom?

- The prize of sensitive information belonging to millions of users
- The possibility of disrupting communication for political purposes
- The vast attack surface of their (often outdated) digital assets

Whatever the motive and means, telecom is clearly not immune to DDoS attack disruption.

Education 17% of all attacks

The ease and affordability of botnet-for-hire services, combined with frequent gaps in the cybersecurity of educational institutions, make education an easy target.

"Fully 17% of all DDoS attacks targeted educational institutions. A DDoS attack on education not only disrupts the pursuit of knowledge, but often shuts down operations and can cost institutions a lot of money. DDoS attacks can also serve as distractions, tying up limited resources and introducing vulnerabilities to other cybercrimes that represent even greater safety threats for our students."

- Gayle Nelson, VP, Education Sales, Zayo

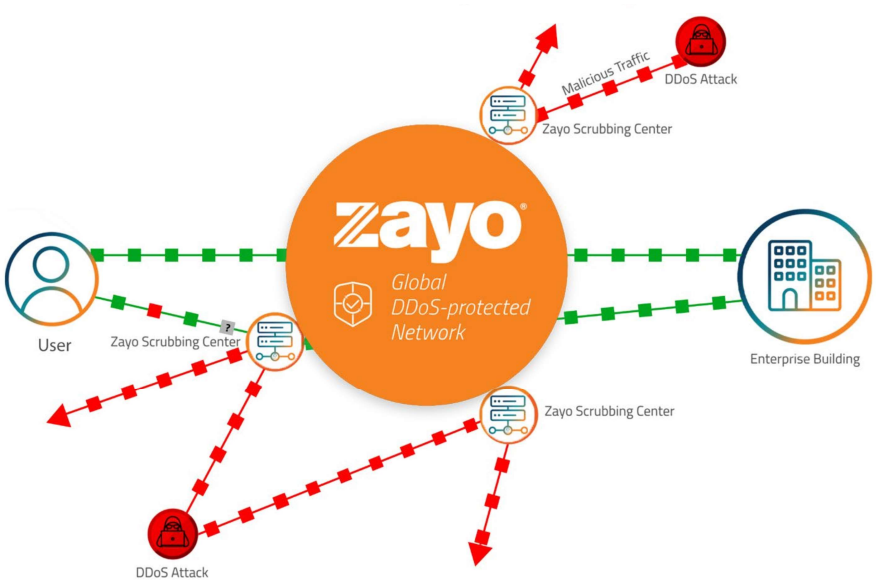
Cloud/SaaS 11% of all attacks

Why do attackers target Cloud and SaaS providers with such frequency? First, attackers can cause widespread damage to cloud and SaaS providers' intricately interconnected core infrastructures. A quick ransom payment stops the attack. Attackers could also be fishing for vulnerabilities - searching for security weaknesses where they can target larger attacks later.

DDoS Protection is Everyone's Force Field:

If your business is protected, the number of attacks directed toward you doesn't matter. With automated DDoS Protection from Zayo, none of the attacks will reach your network, leaving your online traffic flowing as usual and your business operations impervious to the attack.

Zayo has taken a unique approach. A single DDoS subscription immediately protects all of your IP addresses across your whole network, rather than paying on a per-circuit basis. This aggregate protection **costs less** and **scales based on your usage**.



We analyze, redirect and scrub **each individual IP address** attacked, without the collateral damage of latency caused by touching your healthy traffic.

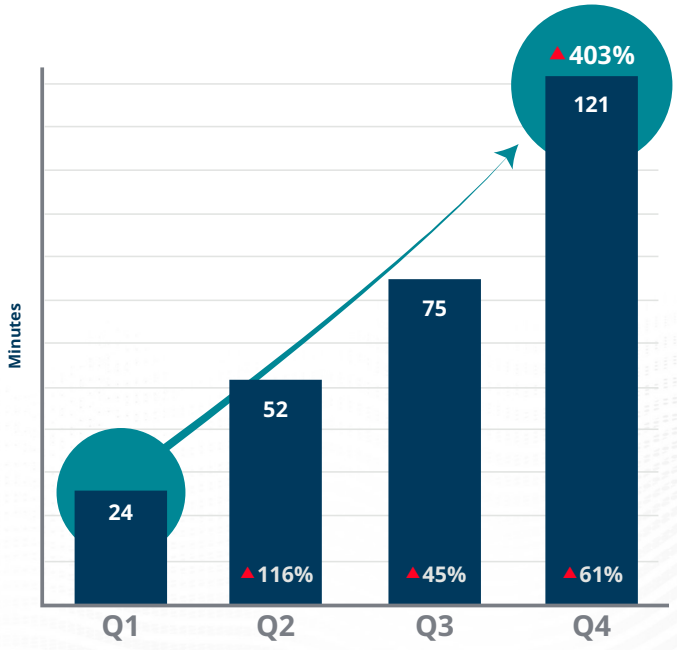
The Duration of DDoS Attacks

In the second half of 2023, short burst attacks – those lasting less than 10 minutes – still represent the vast majority of attacks.

Specifically, **over 72% of all attacks during this period were of this short duration**. However, this percentage represents a decrease from the first half of the year, when 83% of attacks were under 10 minutes in length.

This represents a **worrying trend**. As attack frequency has dropped, attack duration has lengthened. Overall, attacks are more sustained, lasting much longer:

How Long Do Average Attacks Last? (QoQ 2023)



The duration of an attack has a real impact on an unprotected business:

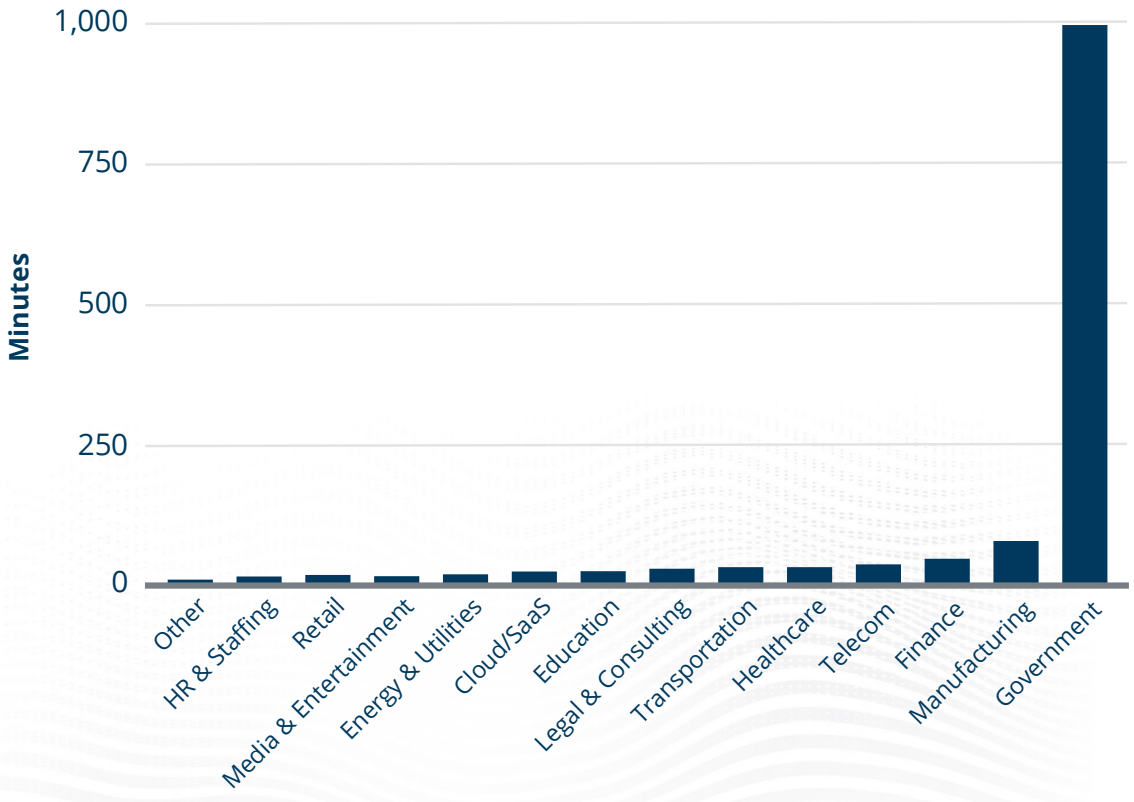
Customer experience:
Customers can't interact with you if they can't connect to your network. Downtime hurts your reputation and hinders future business.

Employee experience:
Employees can't work remotely or in an office if they are not connected to your network. How long can you afford to be offline?

Financial impact:
What is the cost of fixing the network? Of regaining lost business? Of paying a ransom to the attacker? Of mending a damaged reputation?

The longest attack in 2H lasted for **17 days**, 2 hours, 36 minutes, 55 seconds. Even when attacks last for weeks, **protected businesses are unimpacted**.

Average Duration of Attack by Industry (2H 2023)



And once again, **finance** companies experienced longer-than-average attacks as well, at over 30 minutes per attack.

Finance institutions have highly valued and sensitive information that proves irresistible for attackers seeking identity theft or financial fraud. Attackers may be more persistent in their efforts to extract data or cause disruption, leading to more prolonged DDoS attacks.

Aside from manufacturing and finance, the industries whose average attack duration increased the most from Q1 to Q4 2023 were:

- **Education** (23 minutes per attack - a **206% increase**)
- **Media and Entertainment** (16 minutes per attack - a **111% increase**)
- **Telecommunications** (33 minutes per attack - a **104% increase**)

Other notables:

- **Cloud & SaaS** companies experiences an **increased attack duration of nearly 350%** from Q2 to Q3, and another 11% from Q3 to Q4
- **Healthcare** companies experienced a **158% increase** in attack length from Q2 to Q3.

Across all industries, average attack duration increased 138% from 1H to 2H, and 403% when we compared Q4 to Q1.

"A 30-second spurt attack would lead to a full hour loss"

- Billy Russell, Technology Director at North Judson-San Pierre Schools in North Judson, Indiana

Protect Your Business

You can shorten the duration of an attack (indeed, make it nearly **imperceptible**) with an automated redirect of attack traffic from your network ingress to scrubbers that will ensure only legitimate traffic passes.

With automated DDoS Protection, attack length does not matter. An attack of hours – or even weeks – would have zero impact on a protected business.

The truth of the matter is that being a digital business exposes you to network risks. Every business in every industry has confidential information to protect.

DDoS attacks can occur in the background, quietly disrupting your business while you remain largely unaware. According to IBM, it takes a company 197 days to discover a breach and up to 69 days to contain it. Companies that contained a breach in fewer than 30 days saved more than $1 million compared to those that took more than 30 days.

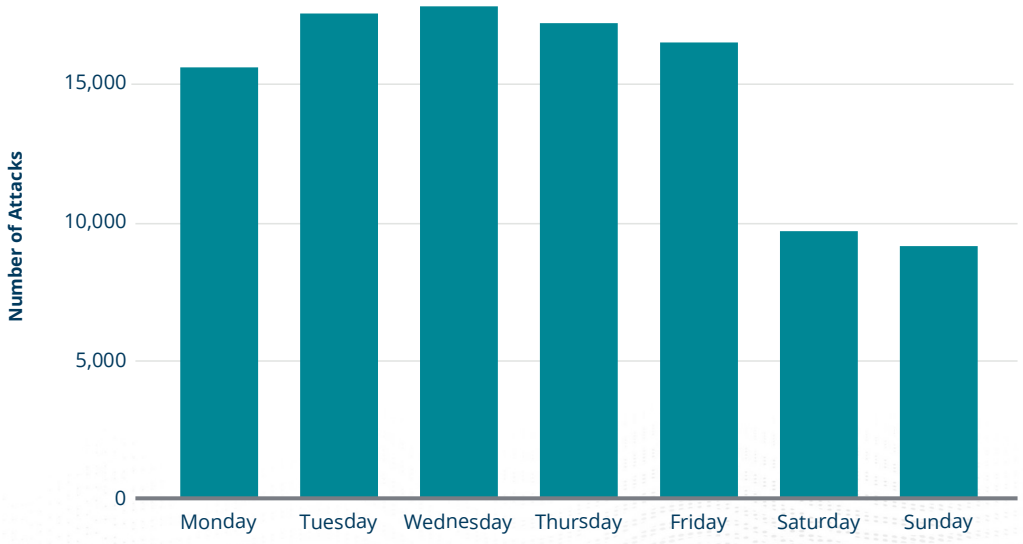
DDoS Protection can't stop DDoS attacks, but will stop them from impacting your business.

The Time of DDoS Attacks

When can you expect an attack? **The timing is strategic.**

Similar to the first half of 2023, attacks in the second half also occurred during the most disruptive times – within the business week and specifically during business hours. Even hackers from overseas synchronize their attacks to coincide with the busiest periods of the business day when your network is crucial for both employees and customers.

When Attacks Occurred During the Week (2023)

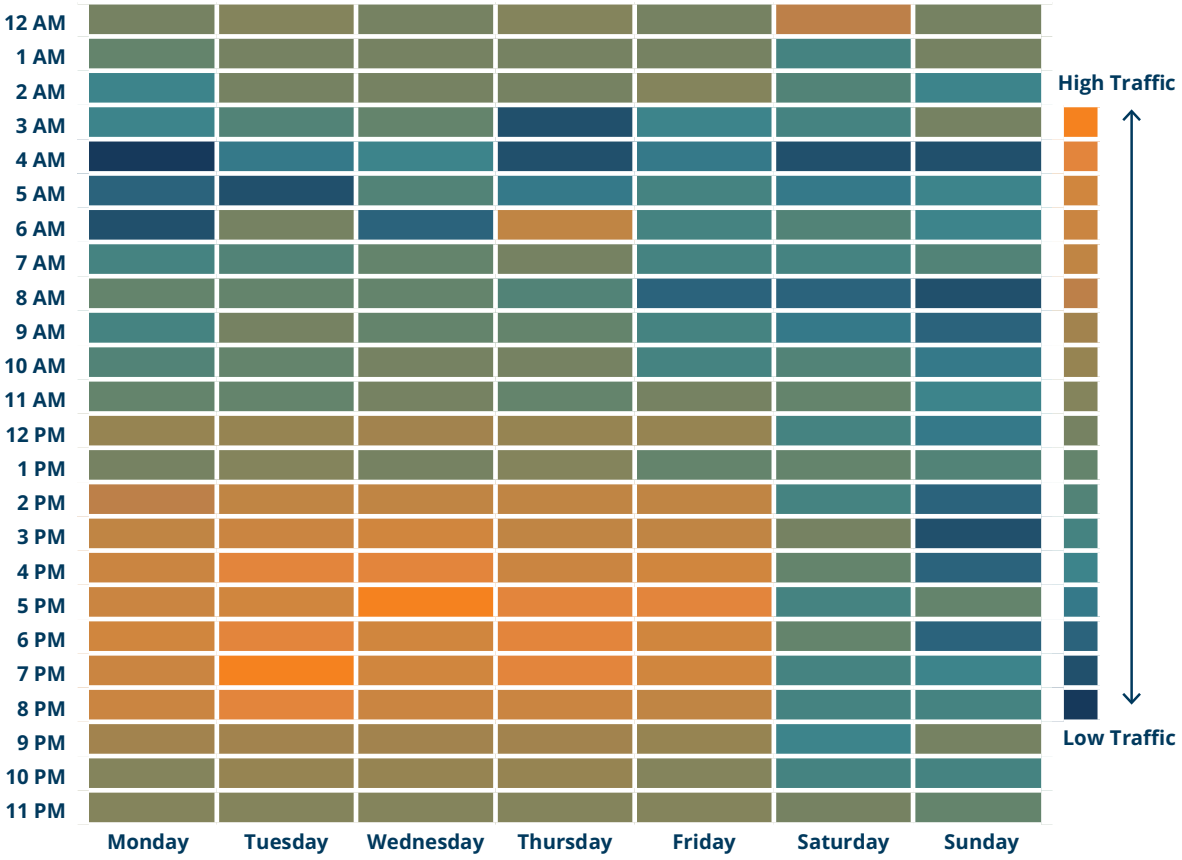


The middle of the work week saw the most traffic. **57% of attacks** in 2023 happened on a **Tuesday and Wednesday**.

The timing of attacks in Q3 and Q4 mirrored those in Q1 and Q2.

Attacks occurred most consistently during the U.S. business day. Yet, with continuous online presence, consumer activity on the Internet may lead to outlier attacks occurring beyond the usual business hours.

When Attacks Occurred During the Day, Eastern Time (Q3 and Q4, 2023)



The timing of attacks in Q3 and Q4 mirrored those in Q1 and Q2. Attacks occurred most consistently during the U.S. business day. Yet, with continuous online presence, consumer activity on the Internet may lead to outlier attacks occurring beyond the usual business hours.

Zayo is proactive. We **monitor** your network to establish normal traffic patterns, **identify** malicious traffic at the onset, and **protect** you during an attack, ensuring only legitimate traffic passes through. After the attack is over, and traffic has remained clean, Zayo will **restore** traffic to its original path.

The Size of DDoS Attacks

How big will this battle be?

Like frequency and duration, the size of a DDoS attack (measured by the amount of bandwidth used by the attack) can affect how long it takes to stop it and how damaging its effects are to your organization.

Like in the first half of the year, retail organizations continued to face the largest DDoS attacks, with healthcare companies following. Customers in these two industries experienced the weightiest attacks on average, while the top 10% of attacks by size continued to focus on telecom.

Average Attack Size per Industry (Gbps)

Industry	1H2023	2H2023	Δ
Retail	3.1	2.9	▼8.0%
Healthcare	2.2	1.8	▼18.2%
Telecom	3.0	1.7	▼42.8%
Energy & Utilities	2.4	1.7	▼28.5%
Manufacturing	2.2	1.7	▼24.5%
Government	1.9	1.4	▼24.2%
Media & Entertainment	3.5	1.3	▼62.6%
Legal & Consulting	0.6	1.3	▲117%
Cloud/SaaS	2.0	0.9	▼56.8%
Transportation	0.8	0.9	▲17.4%
Finance	1.3	0.7	▼49.6%
Education	0.7	0.4	▼36.1%
Other	0.5	0.4	▼17.9%
HR & Staffing	2.4	0.0	▼100.0%
Average	**1.9**	**1.3**	▼33.1%

It should be noted that Zayo did not see the increase in size of attacks other organizations are reporting.

Notably, across all industries, the overall size of DDoS attacks detected by Zayo dropped, by a lot, from the first half to the second half of 2023. The average attack in the first half of the year was 1.9 Gbps, dropping to an average of 1.3 Gbps in the second half of the year.

This is not the good news story it seems to be

This 33% decrease in attack size is a symptom of a larger disturbing trend. Volumetric type attacks are declining. Volumetric attacks are typically the largest and most visible attacks, the ones that are easiest to mitigate because they're easiest to spot.

However, **they're being replaced by "multi-vector" attacks**. If we think of a "vector" as a means of entry to your systems or network, a multi-vector attack spreads its destructive power more widely (albeit: thinly), targeting individual IP addresses, email systems, databases, or web browsers with just a few megabytes of probing traffic. These "feeler" attacks are much harder to detect.

Multi-vector attacks can employ the following attack types simultaneously:

- Carpet-bombing attacks, where the attacker targets its malicious traffic from multiple sources toward multiple targets simultaneously
- DNS water torture attacks, also known as DNS flood attacks, where the attacker targets the DNS infrastructure, usually with a botnet-generated flood of requests
- TCP attacks, where the attacker searches for vulnerabilities or weaknesses in the TCP protocol stack and exhausts the server's resources or disrupts the TCP communication path between clients and the server
- HTTP/HTTPS attacks, achieved by flooding the server with a massive volume of HTTP requests, such as GET or POST requests, consuming bandwidth, processing power, and memory

This **33% decrease** in attack size is symptom of a larger disturbing trend. Large attacks are being replaced by multi-vector attacks.

Why did attackers direct their largest attacks toward these industries?

Usually, the larger the target, the larger the brute force needs to be to match the size of the server traffic running applications. Large scale attacks are also easy to launch; since servers don't allocate resources to applications equally, attacking a single server resource heavily can take the whole server down.

Telecommunications (1.7 Gbps average attack size)

Telecommunications companies are the source of the Internet. They provide the bandwidth all companies rely on to reach their customers. If an attacker can cripple a telecommunication company, the effect ripples through the information chain, impacting thousands of users, with a significant overall impact.

Manufacturing (1.7 Gbps average attack size)

A combination of business and networking practices have made manufacturing an increasingly valuable target for cyber attacks. Manufacturers have a broad digital supply chain and often connect to their partners using APIs. Additionally, they've adopted, perhaps more than other industries, IoT, robotics and AI within their facilities. Each digital connection exposes manufacturers to potential vulnerability. And the second half of any year ramps up production in preparation for the holiday season - a prime time for ransom-motivated attacks.

Healthcare (1.8 Gbps average attack size)

In 2023, the Department of Health and Human Services (HHS) division of cybersecurity reported 568 separate instances of cybercrime directed toward healthcare organizations. Most of these incidents reported hacking, unauthorized access, theft and loss. Further, the Russian Killnet DDoS attacks that occurred earlier in the year - attacks that so disrupted the healthcare industry - are evolving into a new attack-for-hire service.

What motivates attackers to disrupt healthcare organizations, especially with such large attacks? A large DDoS attack is a major obstruction to patient care, and is often used to distract a security organization while the attacker feels for vulnerabilities and plots a larger theft. Sensitive patient data is valuable. As discussed earlier, ransom attacks are especially prevalent in healthcare, and the growing use of Electronic Health Records (EHRs) and other digital technologies has rendered the healthcare industry more exposed to DDoS attacks.

Education (410 Mbps average attack size)

DDoS attacks are easier than ever to implement and launch. With little cyber knowledge or expertise, almost anyone can find a way to purchase a DDoS attack online, inexpensively. And schools are especially vulnerable; whether instruction is remote or in person, a single attack can disrupt an entire day of education.

The largest attack Zayo saw in Q3 2023 was a **404 Gbps** attack directed toward a **telecommunications company**. In Q4 2023, the largest attack was 399 Gbps - whose target was the same company. A large attack aimed at the source of online communications can impact the thousands of companies using that service.

Organizations of All Sizes

In many ways, the smaller the business, the more vulnerable. Small companies generally have limited resources and weaker security measures than larger organizations, making them easier targets for attackers looking to test their mettle. DDoS attacks disrupt business operations, causing financial losses, brand reputation damage, and customer loss.

The cost of exposure far outweighs the cost of protection. Companies of all sizes, but especially those with limited in-house expertise, should invest in DDoS mitigation services and create a response plan to protect themselves.

It's Inevitable

We protect thousands of companies from DDoS attacks, so we know when and where attacks occur, how long they last, and who's being attacked most. Utilizing our extensive network and DDoS Protection data, we decipher the underlying narrative within the data, presenting our informed conclusions for your consideration.

"It's not hard to see that a key security trend coming up in 2024 - one that is going to adversely affect our customers - **is the rapid rise in DDoS attacks.**"

- Anna Claibourne, Senior VP of Packet and Product Software, Zayo

Will you be attacked?

Yes.

DDoS attacks are increasing in frequency, duration, size, automation, sophistication, and therefore, **inevitability**. It's a profitable model for attackers, so, big or small, expect your business to be targeted one day.

Zayo protected our customers from an average of nearly **170 DDoS attacks per day** in the second half of 2023.

Why will you be attacked?

It depends.

Attackers have their own agendas:

- To discover vulnerabilities in an organization's online security
- To distract while the attacker captures confidential information
- To debilitate or damage the reputation of a company
- To extort a ransom to stop the attack
- To exact revenge, to make a political statement, or simply to troll
- To cover up secondary style attacks such as extortion or data theft

2024 is a federal election year in the United States. We expect an increase of attack activity, from both domestic and global sources to target government, education, and critical infrastructure.

What does a DDoS attack do?

It inflicts digital chaos.

Your customers, staff, and associates can no longer access your information online. Your website isn't responding. Your files aren't loading. Your customers are receiving error notices. Your business stands still.

Time to Exhale

We've provided a dire DDoS attack outlook in this report.

But know that **Zayo stays one step ahead**. With Zayo's network-based DDoS Protection service, you can protect your online presence, data, and customers from DDoS attacks.

Zayo stops DDoS attack traffic **before** it reaches your network and impacts your business.

Our DDoS Protection service is network-based, so you can put our network to work for you. A single DDoS Protection subscription from Zayo will stop any DDoS attack aimed at any of your IP addresses. Learn more about the uniqueness of our service in our DDoS Ebook.

The relative investment in DDoS Protection is tiny compared with the inevitable cost of DDoS attacks.

From Real-Time to Proactive

Zayo's DDoS Protection service already operated in real-time, automatically preventing the effects of an attack from impacting the targeted business.

Now, we're **proactively** protecting our customers, preventing attacks from occurring in the first place.

We've enhanced our DDoS Protection with a new **Intelligence Feed**. With this enhancement, we dynamically ingest data of DDoS attacks occurring worldwide, identify the source IP addresses, and then automatically block traffic from those malicious source IPs.

It's proactive.

It's adaptive.

It stops attacks before they start.

In today's digital landscape, the stakes have never been higher.

Protecting your organization from DDoS attacks isn't just an option; it's a critical necessity to safeguard your operations, reputation, and bottom line.

"We're in an attackers' market - very fertile soil for undetected cyber criminal activity. To stop the attackers from gaining the upper hand, we need DDoS protection that is as easy and effective as turning a switch."

- Eric O'Neill, National Security Strategist, Carbon Black

Secure Your Business With Zayo Today

Learn more about protecting your business from a DDoS attack.

Contact us for immediate support.

SONICWALL®

2024

SONICWALL CYBER THREAT REPORT

NAVIGATING THE RELENTLESS SURGE IN CYBERCRIME

sonicwall.com | @sonicwall

Small Cracks Lead to Big Payouts

Cyberattacks are big news. Reports of attacks at large, well-known companies or local government offices make headlines on a seemingly constant basis. For those following cybersecurity a bit more closely, the view isn't too different, with cybersecurity news outlets' coverage of top breaches dominated by household names like Mailchimp, MGM, Activision and 23andMe.

Based on what gets reported, it wouldn't be unreasonable to assume that cybercrime is a far bigger problem for Wall Street than for Main Street. Unfortunately, nothing could be further from the truth. In a 2023 blog, CISA reported that **small businesses are three times more likely to be targeted by threat actors** than larger organizations. And these SMB attacks represent billions of dollars in losses each year.

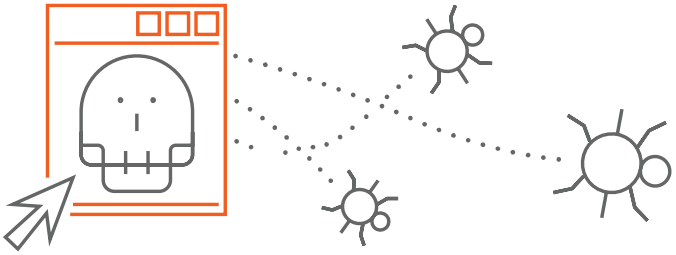
That's a key reason why SonicWall is so committed to researching and publishing the latest threat intelligence. With SMBs making up 80% of our end users, our data presents a view of the threat landscape unlike what you'll find anywhere else — one centered less around large multinational conglomerates, and more on businesses just like yours.

2023's Top Trends

Perhaps the biggest trend we observed in the 2023 landscape was acceleration. SonicWall Capture Labs threat researchers noted increased attack volumes nearly across the board. **Malware jumped 11% year-over-year, with encrypted threats up 117% and cryptojacking up 659%**. This trend bore out on a regional basis as well, with attack volume increases outpacing decreases nearly 3 to 1.

Rather than the relentless push and pull of outside forces we've seen at work over the past several years, we saw threat actors in 2023 sticking with tried-and-true methods. While one would expect increasing malware attack volumes and persistently high phishing levels to be accompanied by high rates of new malware, we found the opposite to be true: Never-before-seen malware detections actually *fell* 38% year over year.

But this doesn't mean threat actors weren't refining their craft. SonicWall researchers observed the emergence of Microsoft OneNote files as an initial threat vector, as well as massive campaigns targeting vulnerabilities in WinRAR and MOVEit.



Our data continued to reflect vulnerabilities as the most common ransomware vector — and this will likely remain the case as the number of vulnerabilities continues to climb. **A record 28,834 CVEs were published in 2023**, a 15% increase over 2022's numbers. In December, SonicWall's threat researchers **discovered and responsibly disclosed CVE-2023-51467**, a vulnerability affecting ApacheOFBiz. Large numbers of exploitation attempts have since been observed.

Other campaigns displayed a similar level of innovation. Novel phishing campaigns driving targets to highly convincing Microsoft Outlook and American Express login pages were observed, along with phishing campaigns utilizing QR codes to bypass file scanning technology. Cybercriminals took advantage of inflation and uncertain economic conditions to launch fraudulent loan apps packed with spyware functionalities and credential-theft capabilities. And Google scripts embedded in PDFs were weaponized to commit cryptocurrency theft, demonstrating the need for heightened vigilance even in seemingly trusted environments.

From SMB to the Enterprise, Today and Tomorrow

We're already looking toward a future threat landscape much different from today's, as threat actors continue adopting ChatGPT and other generative AI technology to refine phishing attempts, carry out highly convincing Business Email Compromise (BEC) attacks, and quickly write malicious code.

But AI also holds great promise for the world's defenders. SonicWall was an early adopter of AI and machine learning, with Capture ATP and RTDMI already capable of detecting many of these types of attacks. But in coming years, we'll begin to see the true potential of AI as a defensive tool.

MALWARE

Highest Since 2019

In 2023, SonicWall Capture Labs threat researchers recorded 6.06 billion malware attacks — a year-over-year increase of 11%. This marks the highest global attack volume for any year since 2019, indicating that malware levels have risen back to their pre-pandemic levels as threat actors continue to become more plentiful, resourceful and active.

But while global malware was up, this was the combination of two opposing trends. Malware in Asia and Europe actually *dropped* by 2%, but this was easily offset by larger increases in North America (+15%) and LATAM (+30%).

This divergence also appeared in our industry-specific data. Education, which saw by far the most malware in 2022, experienced 3% less in 2023. Malware targeting healthcare and retail, on the other hand, rose 20%, and attacks targeting government spiked 38%. But the hardest-hit were customers in finance—malware attacks on these businesses *doubled*. This increase was enough to make finance the hardest-hit industry we studied in 2023, up from the bottom of the list in 2021 and the middle of the pack in 2022.

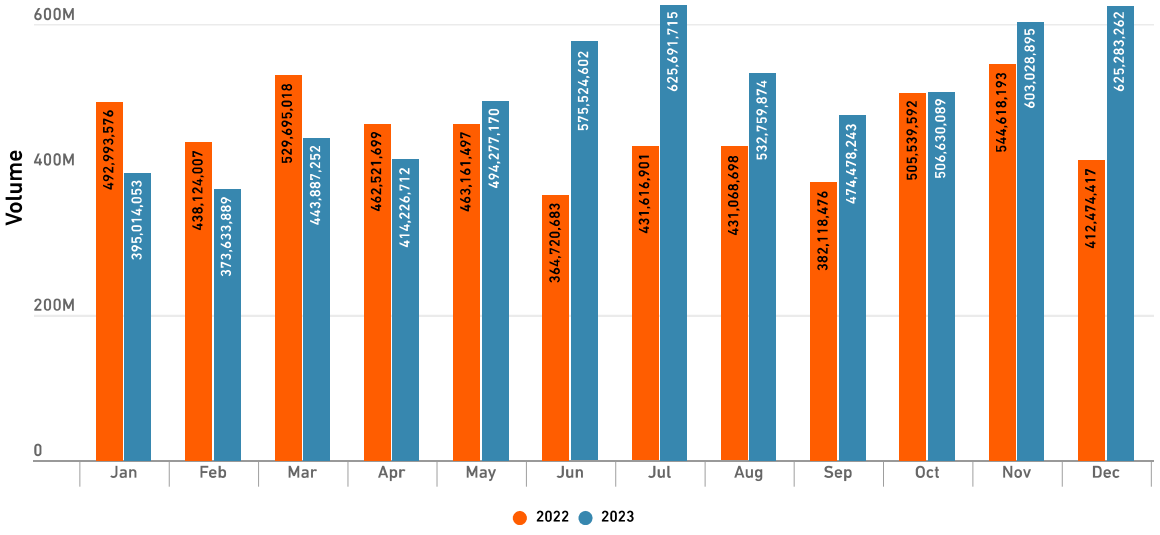
One and Done: Malicious OneNote Files

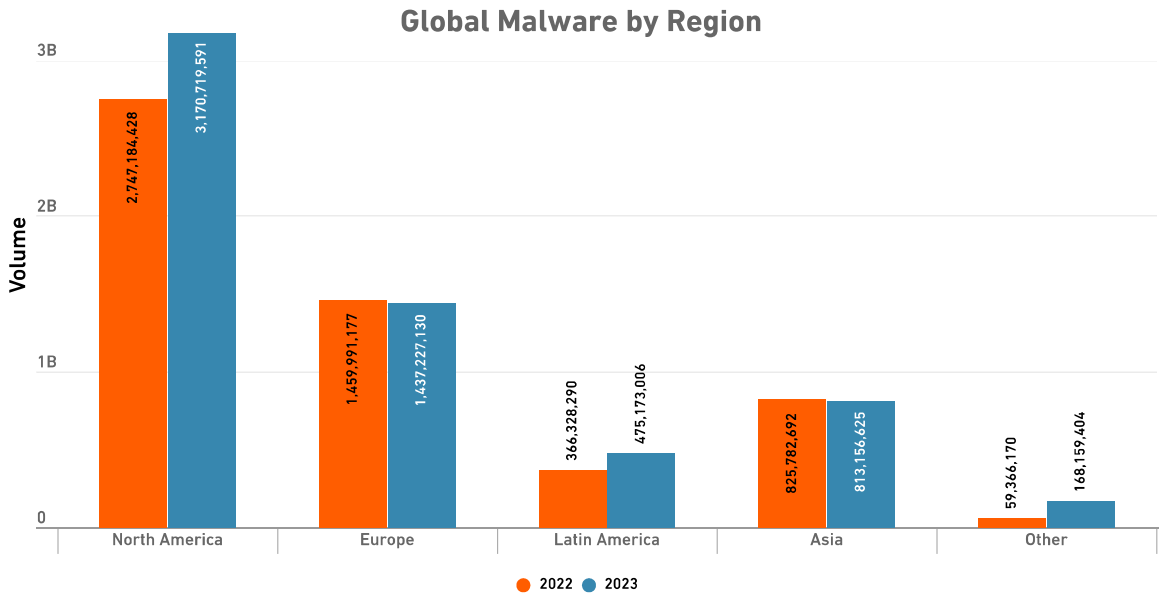
In early 2023, SonicWall researchers observed threat actors leveraging a new initial vector to infect systems: the use of Microsoft OneNote files. These weaponized attachments were being sent via email, accompanied by a variety of social engineering techniques designed to maximize the odds the attachments would be opened and the target would click on the hidden malicious files tucked inside, triggering the payload execution.

But as security vendors quickly wised up, they began triggering detections based on those attached payload files. Then threat actors pivoted to using a URL that, when clicked, would point to the payload. At the same time, attackers began bloating their code with repeated null bytes at the end of the OneNote files, pushing the file size above 500 MB in an attempt to bypass many AV scanning solutions.

By March, however, the use of these files had already begun to fall dramatically, likely due to Microsoft releasing an Office update that blocked embedded files with dangerous extensions from opening in OneNote. But even though this trend was short-lived, it was widespread enough to make malicious OneNote files the most popular type of malicious Office file for all of 2023, with Qakbot, AsyncRat, AgentTesla and others all using OneNote attachments as an initial entry point.

Global Malware Volume





Malicious PDFs Are Prevalent

Using malicious PDFs has long been a preferred tactic of threat actors. But their use increased dramatically in 2023, growing from roughly a fifth of all new malicious filetype detections to nearly a third—a clear sign that this tactic continues to succeed.

As these attacks grew, so did the innovation, leading to the creation of many notable variants. SonicWall observed several instances of PDFs containing QR codes in 2023, with one example threatening the user with the expiration of a Microsoft password if the target failed to scan the code.

Another PDF featured a malicious URL created by using Google Script in an attempt to evade detection. This complex scam came complete with a fabricated Bitcoin transaction record and a fake "mining progress" bar, enticing targets to enter financial information in order to receive their fictitious funds.

As we've seen in past years, threat actors have gone to extremes in 2023 to replicate well-known and trusted brands — and they're getting better at it all the time. Some examples include malicious PDFs masquerading as iTunes receipts, warnings about multiple login attempts to a Wells Fargo account, and even the login page for collaboration platform RingCentral.

Top Tactics by Threat Actors

Portable Executable (PE) Files Reign Supreme

PE files continue to be the most-used final payload due to delivery simplicity, use of general tools, and ease of execution. But in 2023, we noted an increase in PE malware written in .NET. Likely due to its accessibility and rich functionality, we observed the majority of PE malware is now being written in .NET, including prominent malware families such as RedLine, AgentTesla and AsyncRAT.

Fortunately, PE malware are red-flagged file types, which are examined thoroughly for malicious intent. And while some malware authors use script files as initial vectors for other malware, or write complete malicious code using JavaScript, VBScript, PowerShell or others, SonicWall customers are protected: RTDMI's exceptional script emulation capability provides excellent detection of malicious scripts.

WinRAR Offers Easy Win for Attackers

Threat actors began exploiting a new vulnerability in popular Windows file archiver tool WinRAR in early 2023. By the second half of the year, multiple stealer malware families — including AgentTesla, Remcos, Rhadamanthys and Guloader — were implicated in a variety of campaigns exploiting CVE-2023-38831, which allows attackers to execute arbitrary code within zip archives. Due to the widespread use of WinRAR in enterprises, these campaigns quickly proliferated globally, targeting the U.S., the Middle East and Asia. They've now been linked to state-sponsored hackers from Russia and China, including Sandworm, APT28, APT 30 and others.

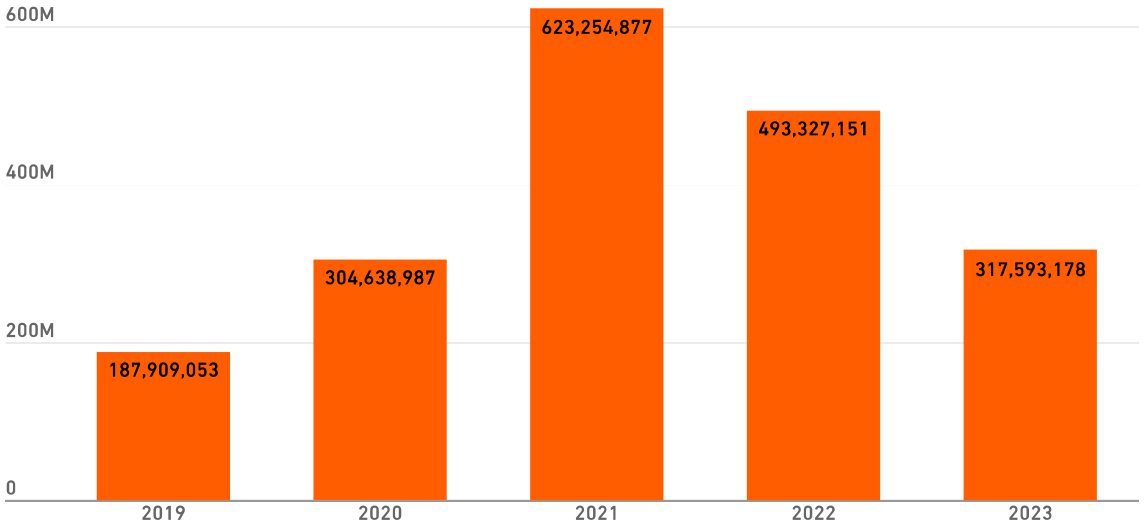
RANSOMWARE

Still a Force to be Reckoned With

The ransomware attack landscape continued to evolve in 2023. SonicWall Capture Labs threat researchers recorded 317.6 million ransomware attacks, a decrease of 36% year-over-year — but the third-highest total on record. This trend was reflected across several regions: North America and Europe each saw ransomware fall by a third, and in LATAM, attacks fell by 52%.

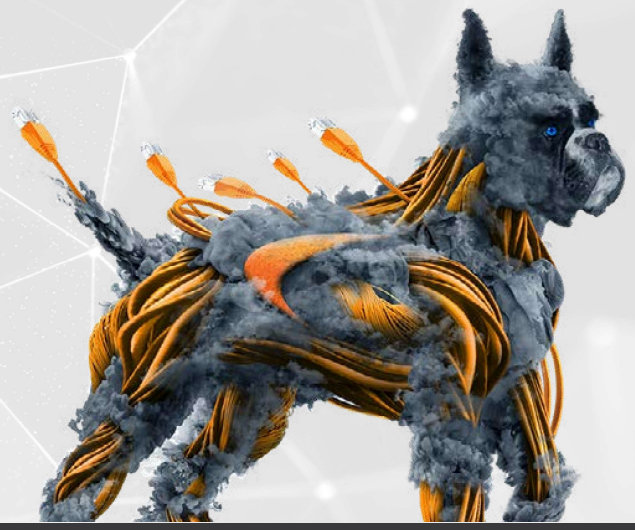
A notable exception was Asia. Ransomware volumes hit a record high in 2023, rising to 17.5 million — a 1,627% increase since 2019. This increase was spearheaded by attacks on the financial sector. In May, the LockBit ransomware group stole 15 million customer records and 1.5 terabytes of internal data from Bank Syariah Indonesia. In November, the Industrial and Commercial Bank of China (ICBC), the world's largest bank by assets, was also attacked by Lockbit. And according to an IDC report released in September 2023, roughly three-quarters of enterprises in India were hit by ransomware in 2022 — a number that has likely continued to climb since.

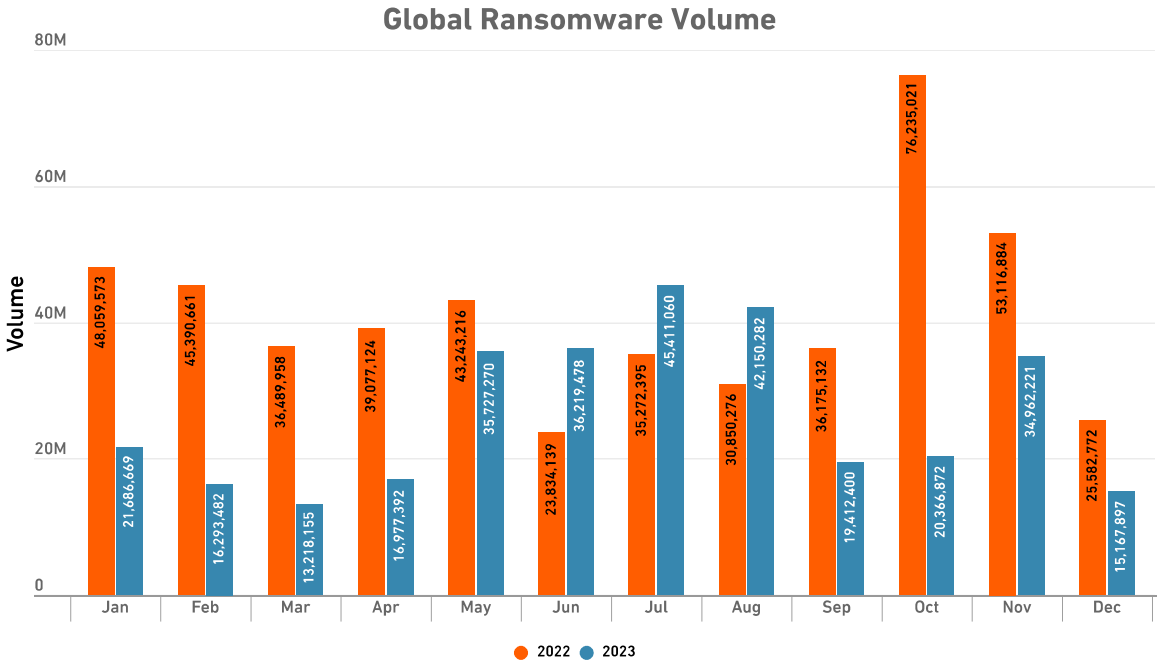
Global Ransomware Volume by Year



2023's Top Ransomware: LockBit

The arrest of two affiliates barely made a dent in LockBit's numbers: It remained the leading ransomware group in 2023. This is likely due to consistent innovations, such as bug bounty programs to enhance "product" quality, marketing efforts, and the regular release of updated toolkit versions with improved capabilities. After the leak of LockBit 3.0/ "Black," SonicWall engaged the threat actors, who then made a staggering ransom demand (You can see the details here.)





Still Top of Mind: Why it Matters Today

Assuming you don't live in one of the rising ransomware hotspots, how concerned should you be about ransomware?

In our 2023 SonicWall Threat Mindset Survey, we asked customers which types of cyberattack they're most concerned about. Once again, ransomware topped the list at 83%, beating out phishing, encrypted threats, fileless malware, IoT attacks and more.

Despite a decrease in ransomware attack volume amongst our SMB customers, we believe these respondents are on the right track.

Some historical context may be useful here. A 36% decrease sounds like a lot — until you consider ransomware's growth between 2020 and 2022. Even after this drop, 2023 still had enough ransomware to be the third-highest year on record. **And with 27% more ransomware in the second half of 2023 than the first half, ransomware is trending in the wrong direction to meaningfully undo 2021 and 2022's meteoric spikes**.

When cybersecurity vendors like SonicWall measure ransomware and other threats, they can only see what's happening across their own ecosystem. While SonicWall (with its large partner and MSP customer base) noted a decline in ransomware over 2023, some other vendors recorded increases over the same period. With increased law enforcement efforts making each attack riskier, and SMBs no longer being "easy pickings" for threat actors deploying spray-and-pray-style attacks, there seems to be a shift toward focusing on fewer, more highly targeted attacks with a bigger potential payday.

But this doesn't mean there aren't easy pickings to be had. Organizations are increasingly moving data and workflows to the cloud, but often aren't ensuring these instances have the same protection as on-prem. As threat actors continue refining ransomware attacks on SaaS, failing to ensure sufficient security in the cloud could have disastrous results.

There are also still plenty of huge ransomware campaigns being run. In late May, SonicWall observed the exploitation of a critical-rated, zero-day SQL injection vulnerability within MOVEit Transfer. The popularity of this file transfer tool — and its widespread adoption by enterprises — made it a target of the Cl0p ransomware gang. It leveraged CVE-2023-34362 to conduct a supply chain attack that affected about 2,000 organizations across financial, insurance, healthcare, education and government, with data theft impacting more than 62 million people.

It's important to note that vulnerabilities such as this one were the most common vector SonicWall observed for ransomware in 2023 — and those campaigns contributed to ransomware payments surpassing $1 billion for the first time in 2023.

INTRUSIONS

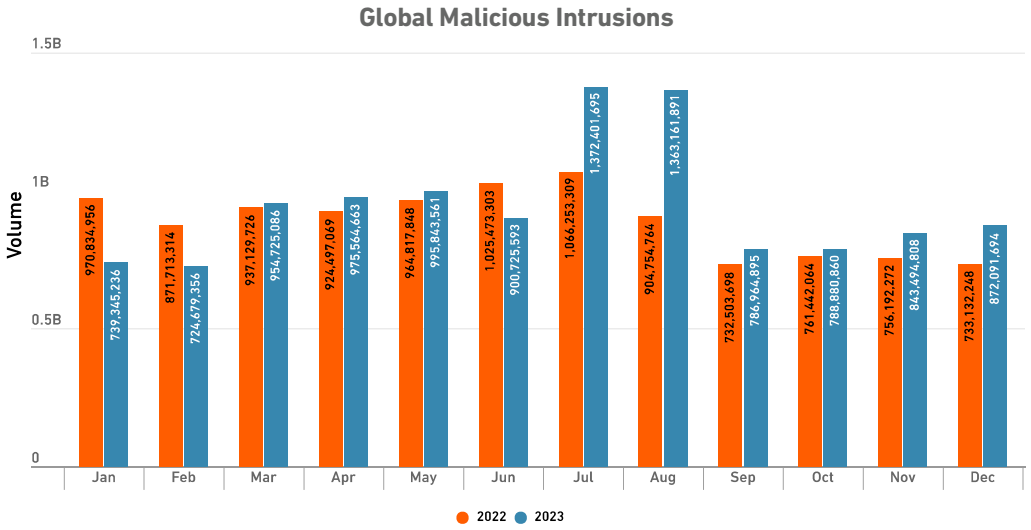
Attempts Up 20%

Overall intrusion attempts continued to climb in 2023, rising to 7.6 trillion, a 20% increase over 2022's total. Since SonicWall began reporting this metric in 2013, the number of intrusion attempts has increased each year — and over the past decade, the number of intrusions has risen 613%.

While some of this increase can be attributed to low-severity hits associated with pings and other typically benign actions, there's also been an uptick in moderate- to high-severity hits — otherwise known as "malicious intrusions." These intrusion attempts increased to 11.3 billion in 2023, a 6% increase year over year.

Malicious intrusion volumes were also up across every industry we studied. Moderate and high-severity hits rose 19% for education customers, 34% for retail customers, 36% for healthcare, 46% for government, and 47% for finance customers.

These attempts set off alerts that must be reviewed by SOC analysts, or MSPs with SOC analysts, contributing to alert fatigue and taking valuable time away from other critical initiatives. And when an intrusion is successful, threat actors are free to exfiltrate data, execute malicious code, encrypt systems and more — potentially grinding operations to a halt and costing these organizations thousands or millions in remediation costs and compliance fines.



What is an Intrusion Attempt?

A malicious intrusion attempt is a security event in which a threat actor tries to gain unauthorized access to a system or resource by exploiting a vulnerability. While the exploit of unpublished "zero-day" vulnerabilities make the most headlines, the most commonly exploited vulnerabilities are generally public and published as CVEs. But because not everyone patches at the same rate, attackers have an opportunity to use unpatched software or appliances as an entry point into a network.

Once threat actors are inside the network, vulnerability exploitation continues as attackers attempt to gain network persistence and lateral movement using other vulnerabilities in unpatched systems within the network.

SonicWall tracks the detection and prevention of exploits coming from both external and internal sources. When a piece of code that constitutes a vulnerability passes a firewall with Intrusion Prevention enabled, and the firewall detects and neutralizes that code, an intrusion attempt is counted.

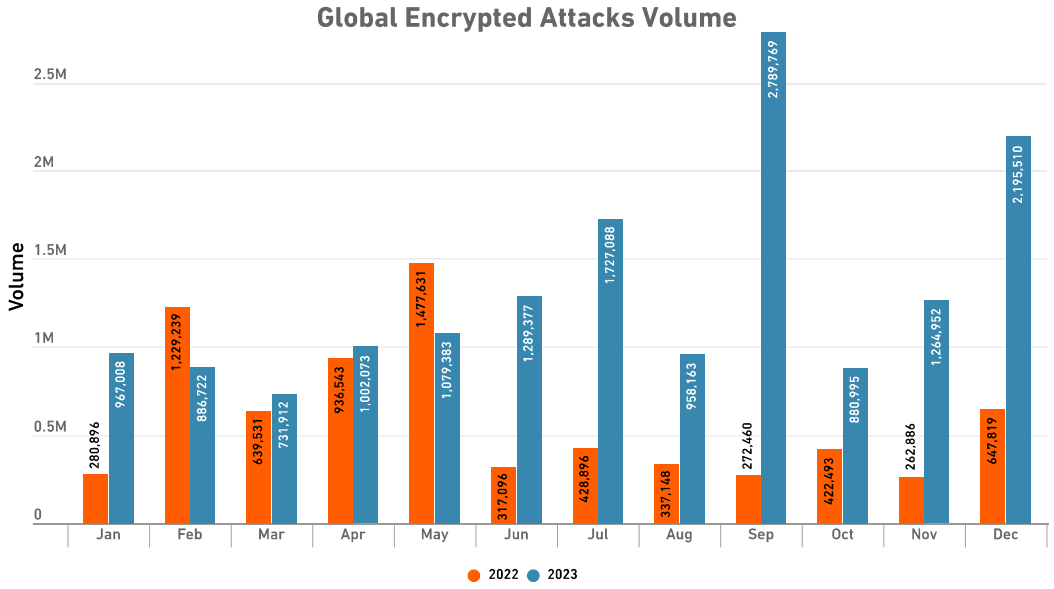
ENCRYPTED THREATS

Encrypted Attacks More Than Double

In 2023, SonicWall Capture Labs threat researchers observed 15.7 million encrypted attacks. This is the most it's been since we began reporting on this threat metric, and we've seen an increase of 117% year over year.

While North America saw a more modest increase of 30%, triple-digit jumps were recorded in Europe, Asia and LATAM, where encrypted attacks rose 182%, 462% and 527% respectively.

Even sharper increases were observed in some of the industries we studied — all of which experienced triple-digit spikes. Finance saw the smallest increase: attacks on these customers "only" doubled. But healthcare (252%), education (429%), government (629%) and retail (680%) all saw encrypted threats skyrocket in 2023.



What Are Encrypted Threats?

Most industry analyst firms conclude that between 80-90 percent of network traffic is encrypted today, requiring you to scan encrypted traffic. While TLS (Transport Layer Security) provides added security for web sessions and internet communications, attackers increasingly use this encryption protocol to hide malware, ransomware, zero-day attacks and more.

Legacy firewalls and other traditional security controls lack the capability or processing power to detect, inspect and mitigate threats sent over HTTPs traffic, making this a highly successful avenue for threat actors to deploy and execute attacks.

CRYPTOJACKING

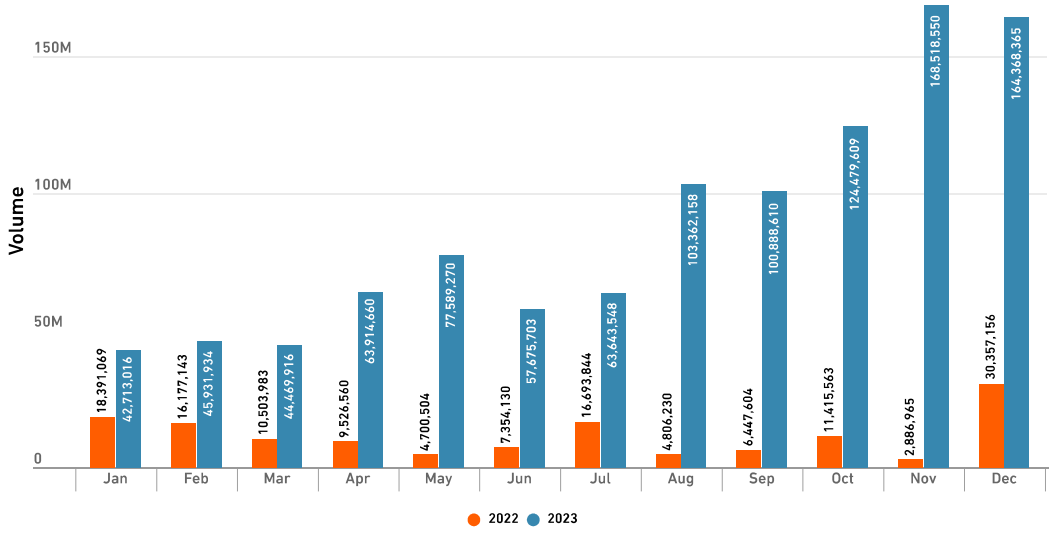
Why It's Dangerous (And Why It's Climbing)

In last year's threat report, we noted a concerning milestone: The number of cryptojacking hits, which had remained fairly low since we began tracking in 2018, surpassed 100,000 for the first time.

But as it turned out, cryptojacking's ascent was only beginning. In 2023, the number of cryptojacking hits had sailed past 2022's full-year total by early April, and continued to pick up steam from there. By the end of the year, SonicWall Capture Labs threat researchers had recorded *1.06 billion* cryptojacking hits—a 659% increase over 2022's totals. This total was fueled by unprecedented attack volumes in November and December—which each had more cryptojacking hits than were noted for the entire year in 2022.

Large increases were also observed across every region. In APAC and LATAM, cryptojacking hits rose 87% and 116% respectively. But truly massive increases were recorded in NOAM (+596%) and Europe (+1,046%).

Global Cryptojacking Volume



What Is Cryptojacking?

Cryptojacking is a type of cyberattack where threat actors hijack a victim's computing resources to mine cryptocurrencies without their consent or knowledge. It involves the installation of malware, often delivered via phishing emails or compromised websites, that secretly runs in the background on a victim's computer, smartphone or server. This malware uses the device's processing power and energy to solve complex mathematical problems ("proof of work"), generating cryptocurrency for the attacker.

paloalto NETWORKS | UNIT 42 BY PALO ALTO NETWORKS

MALWARE

2023

NETWORK THREAT TRENDS RESEARCH REPORT

VOLUME 2

Executive Summary

In this report, the Palo Alto Networks Unit 42 research team shares current trends in malware and the evolving threat landscape. This includes an analysis of the most common types of malware and their methods of distribution. With the growing volume and sophistication of today's threats, it's critical for network security professionals to understand the threat landscape and how to properly defend against it.

The insights provided in this report are intended to give you a better understanding of how the threat landscape is evolving and provide security recommendations for organizations to protect themselves.

Most findings are based on data and observations we gathered in 2022 and are a comparison to one year earlier. Data for AI was collected between November 2022 and April 2023. Here are some key highlights of the findings:

- We've seen a boom in traditional malware techniques taking advantage of interest in AI/ChatGPT.
- The ratio of malware impacting industries using Operational Technology (OT) has increased by 27.5%.
- Exploitation of vulnerabilities increased 55% compared to 2021.
- PDFs are the most popular file type for delivering malware as email attachments (66.6% of all attachments).
- While nearly 49% of network communication generated during sandbox analysis (including both malicious and benign files) uses encrypted SSL for its traffic, 12.91% of network traffic generated by malware (such as phoning home, getting time calibration) is encrypted with SSL.
- Cryptominer traffic has doubled in 2022.

We will also discuss emerging advanced threats that organizations should be aware of. Sophisticated multivector attacks are designed to elude detection using an array of evasion tools and camouflage techniques. The result is a significant strain on IT and security teams charged with strengthening the organization's security posture. Armed with expert knowledge and recommendations, you can make your organization a less tempting target.

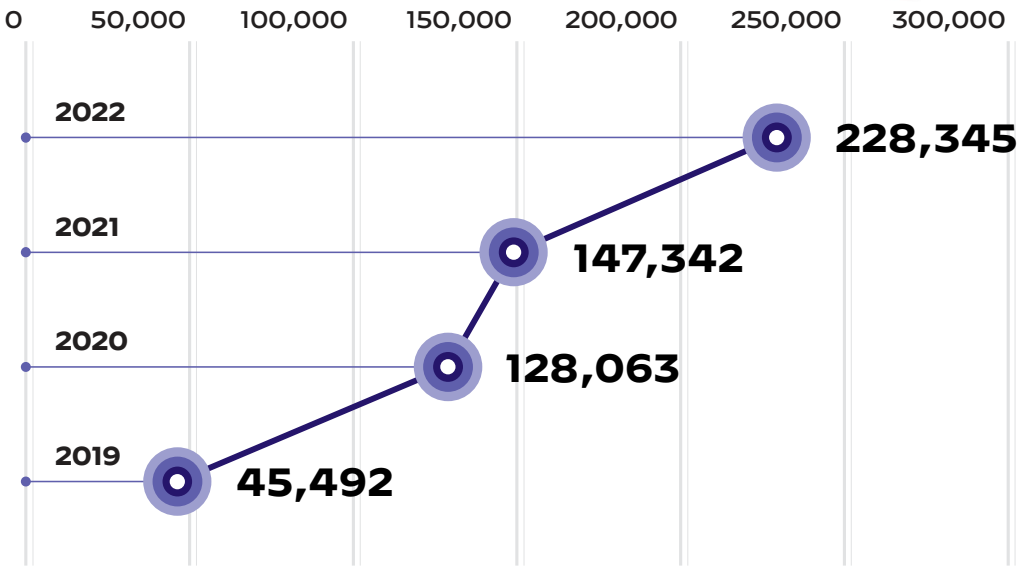


Figure 1. Vulnerability exploitation attempts

Attackers are using both vulnerabilities that are already disclosed and ones that are not yet disclosed. (aka exploiting zero-day vulnerabilities). We continue to find that vulnerabilities using remote code execution (RCE) techniques are being widely exploited, even ones that are several years old.

While using old vulnerabilities might seem counterproductive, they still have significant value to attackers. In some cases, vulnerabilities discovered years ago have not been patched. This could be either because the company failed to fix the issue, or they didn't provide the patch in a way that customers could easily find. In other cases, the product could lack a patch because the product is at the end of its supported lifespan.

But the full weight of responsibility is not just on the vendor supplying the product with a vulnerability. Organizations must also have appropriate processes in place for updating in a safe and timely fashion. For example, companies must have a policy in place for acquiring, testing and applying patches, as well as the bandwidth to apply them. Many companies could also lack awareness of available fixes, which effectively turns an old, known vulnerability into something as risky as a zero-day threat.

Threat actors know these problems exist, and they continue to try these old vulnerabilities because they're counting on organizations to fail at some point in the process of applying patches.

Email as Infection Vector

Email continues to be a popular infection vector for threat actors, but they have to pair it with social engineering tactics for it to be successful. Figure 2 shows that even though executables are the file type of choice for malware once on a victim's system, attackers are more likely to deliver malicious PDF files in email attachments.

PDFs are the primary malicious email attachment type being used 66% of the time to deliver malware via email. PDF files are commonly used in a business environment, and victims are less likely to be wary of an expected file type, versus unexpected file types like EXEs. They could also simply be unaware that this type of file could be used for nefarious purposes.

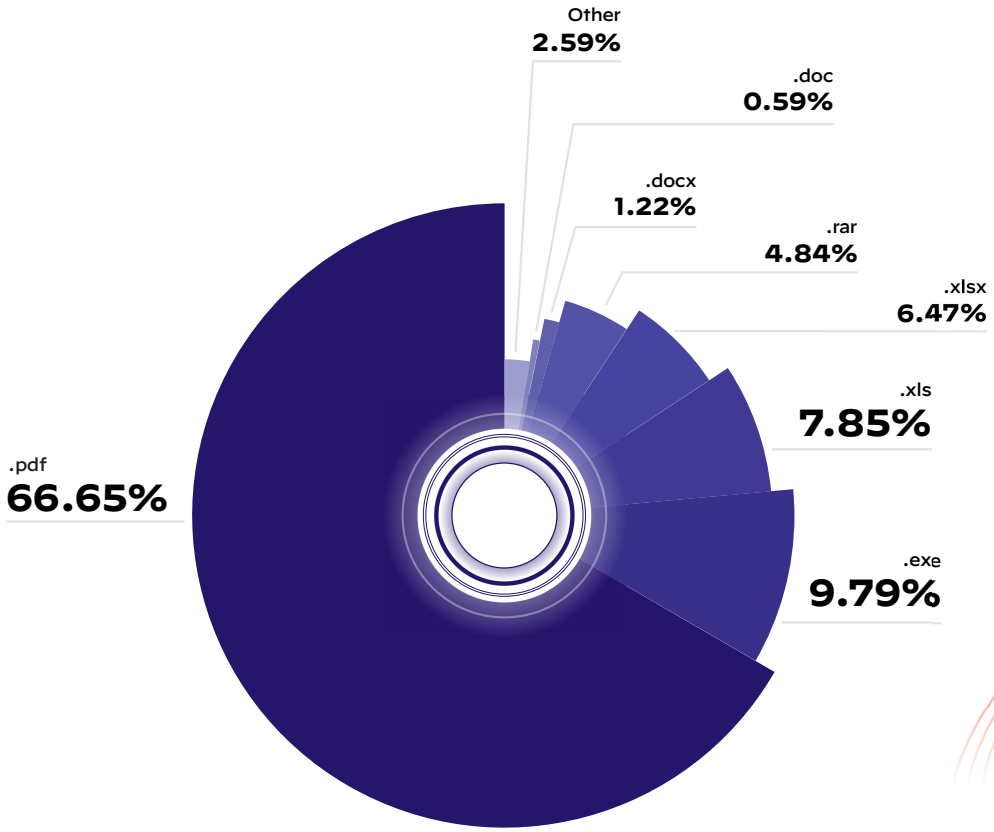


Figure 2. Malicious email attachment file types

Linux Threats Target Cloud Workloads and IoT Devices

While representing a relatively small number of attacks, Linux malware is on the rise. Attackers are looking for new opportunities in cloud workloads and IoT devices that run on Unix-like operating systems. The growing prevalence of this family of operating systems among mobile and "smart" devices could explain why some attackers are turning their eyes toward Linux systems.

Figure 7 shows that the most common type of threat against Linux systems is botnets. The malware families of choice for this type of operating system are Mirai (14.3%) and Gafgyt (4.7%).

The release of the Mirai source code in 2016 enabled attackers to create new variants with new exploits and new functionality. These variants usually spread by continuously updating their arsenal of exploits, looking for victims by actively scanning and then exploiting any vulnerable IoT device they can find on the internet.

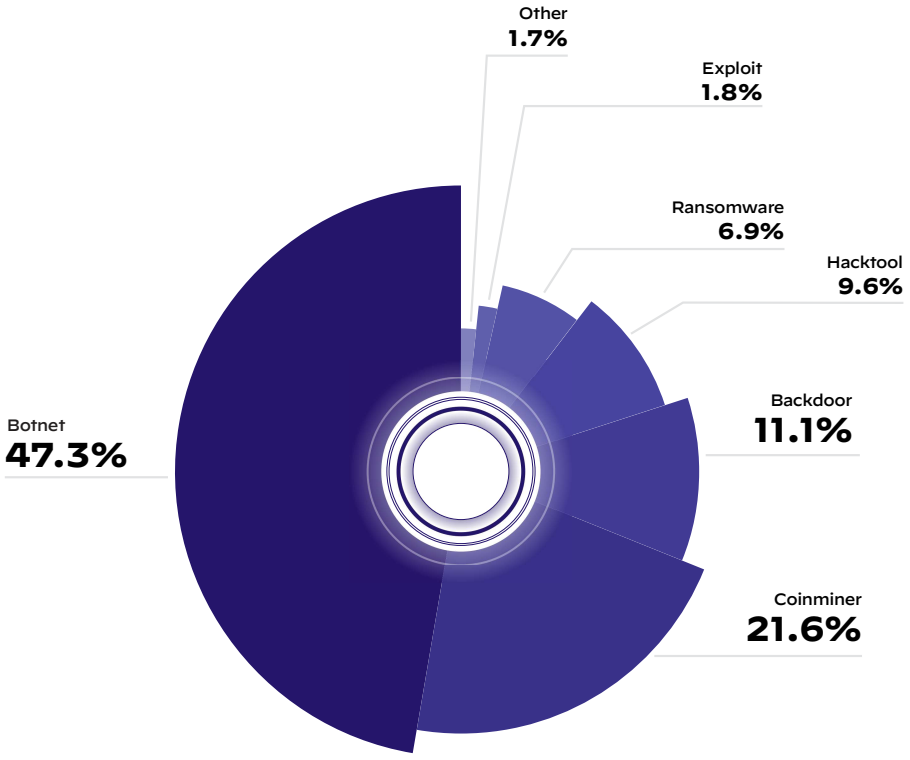


Figure 7. Malware type distribution in Linux systems

Observation From the Malware Network Traffic

More than 647 million command and control (C2) traffic sessions were detected during 2022.

We reviewed C2 traffic captured by Palo Alto Networks services to gain more insight into active malware activities. Here's what we found.

Decrypting Traffic Becomes Increasingly Important

We collected over 134 million network traffic sessions generated by samples during sandbox analysis and found SSL was the most common protocol for both benign and malicious samples, constituting 48.94% of traffic.

In the portion of this traffic generated by malware, 12.91% of sessions were SSL encrypted. To better understand the nature of the encrypted traffic, we also checked the reputation of the Server Name Indication (SNI) and IP addresses of each session. 3.6% of this SSL encrypted traffic was being received by endpoints with a bad reputation, meaning they could be C2 servers or other attacker-controlled devices.

SSL traffic is of particular concern because it's the same kind of encryption that legitimate web and email traffic uses to keep data secure. To determine whether this traffic is benign or malicious, enterprises should decrypt SSL traffic for security inspection.

The FormBook malware family uses SSL to pull down its second stage. Our sandbox can extract session keys from memory to decrypt SSL traffic so there's no need to use a meddler in the middle (MitM) to get this information.

In addition to monitoring SSL communications on the network, it's a good idea to check for malicious network activity in SSL tunnels. This technique is also useful for detection within malware sandboxing environments.

Growth in Cryptominer Traffic

Sifting through network traffic can help us identify trends in malware activity. Figure 8 shows how, by reviewing 647 million signature triggers, we were able to identify the distribution trend of different malware categories during each month in 2022.

There is one particularly notable point from the trend graph, which shows that cryptominer traffic has increased dramatically since April 2022. Within the subset of customers who have both a Cortex Data Lake (CDL) license and Threat Prevention license, 45% of sampled organizations had a signature trigger history that contains cryptominer-related traffic.

95.5% of the cryptominer traffic came from XMRig miners attempting to log in to its mining pool. This traffic includes both XMRig variants and malware incorporating XMRig.

Because XMRig is open-source software, its source code is publicly available. This makes it easy for malware authors to modify and integrate into their own code. XMRig is available on a variety of platforms including Windows, Linux and macOS. It can be customized to mine a variety of different cryptocurrencies and can be configured to use different mining algorithms and pools.

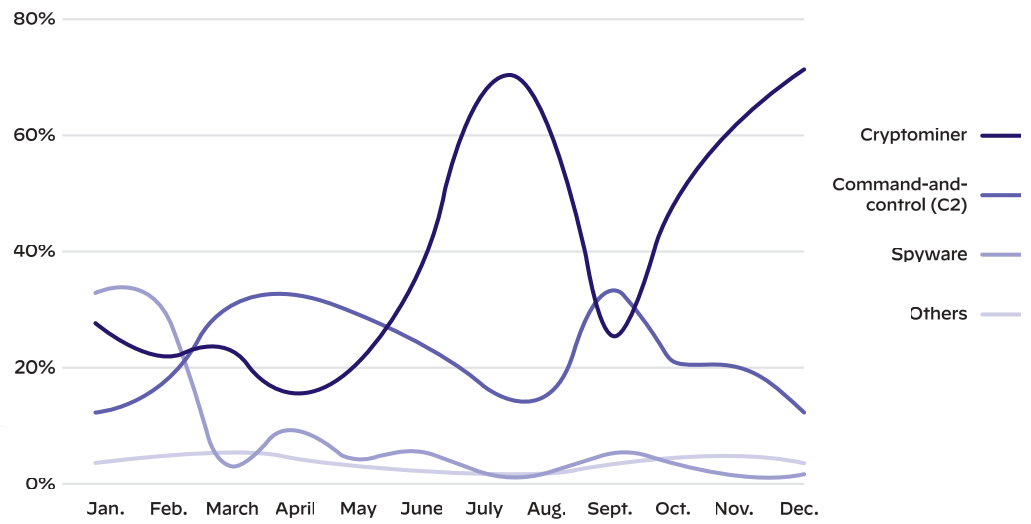


Figure 8. C2 traffic category distribution

Ac

Report
2023

Acronis Mid-Year Cyberthreats Report 2023

From Innovation to Risk: Managing the Implications of AI-driven Cyberattacks

2. Phishing and malicious emails remain the main vector of infection

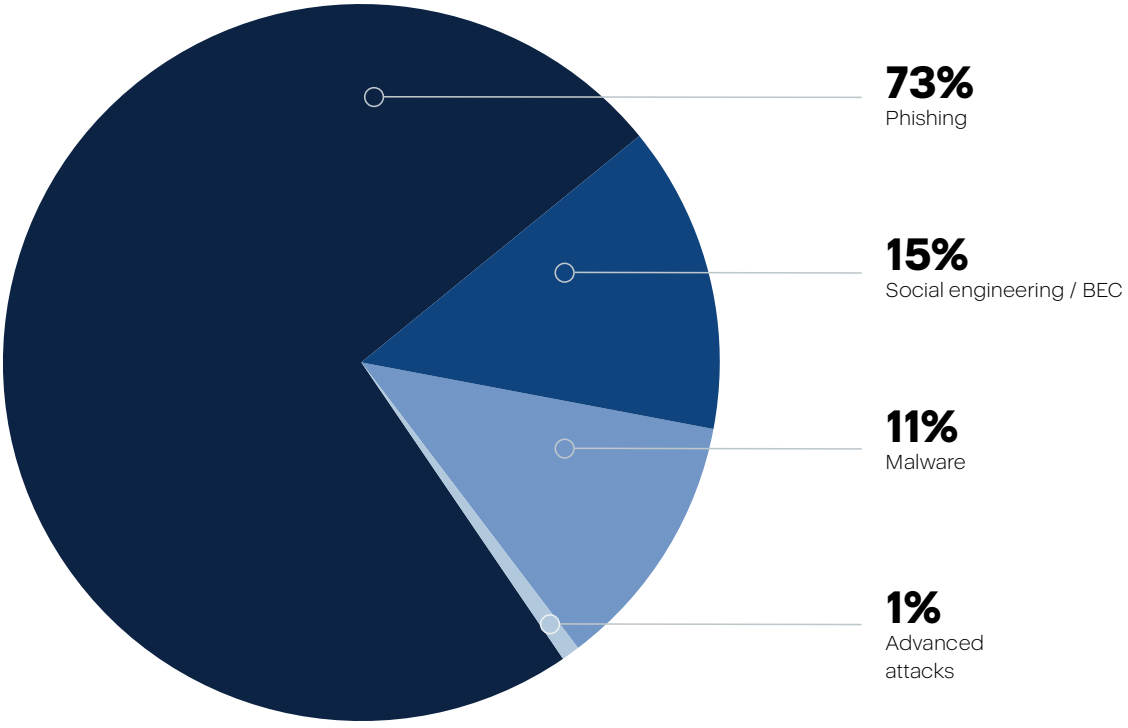
The following email and phishing statistics are from the Advanced Email Security pack for Acronis Cyber Protect Cloud, which is powered by Perception Point. Acronis and Perception Point work together to protect organizations and ensure they remain safe from email-borne threats. The data was gathered for the first half of 2023, and combined with Acronis telemetry data for malware and URL blocks on the endpoints. Later in this report, you'll find a dedicated section highlighting a collection of malicious websites that have been blocked.

There are two significant numbers to highlight. First, the number of email-based attacks seen thus far in 2023 has experienced a staggering 464% surge compared to the first half of 2022. Second, when considering the attacks per organization within the same time frame, there has been a notable increase of 24%. These numbers underscore the escalating threat landscape — with email being the main attack vector — and the urgency for organizations to fortify their defenses against malicious activities.

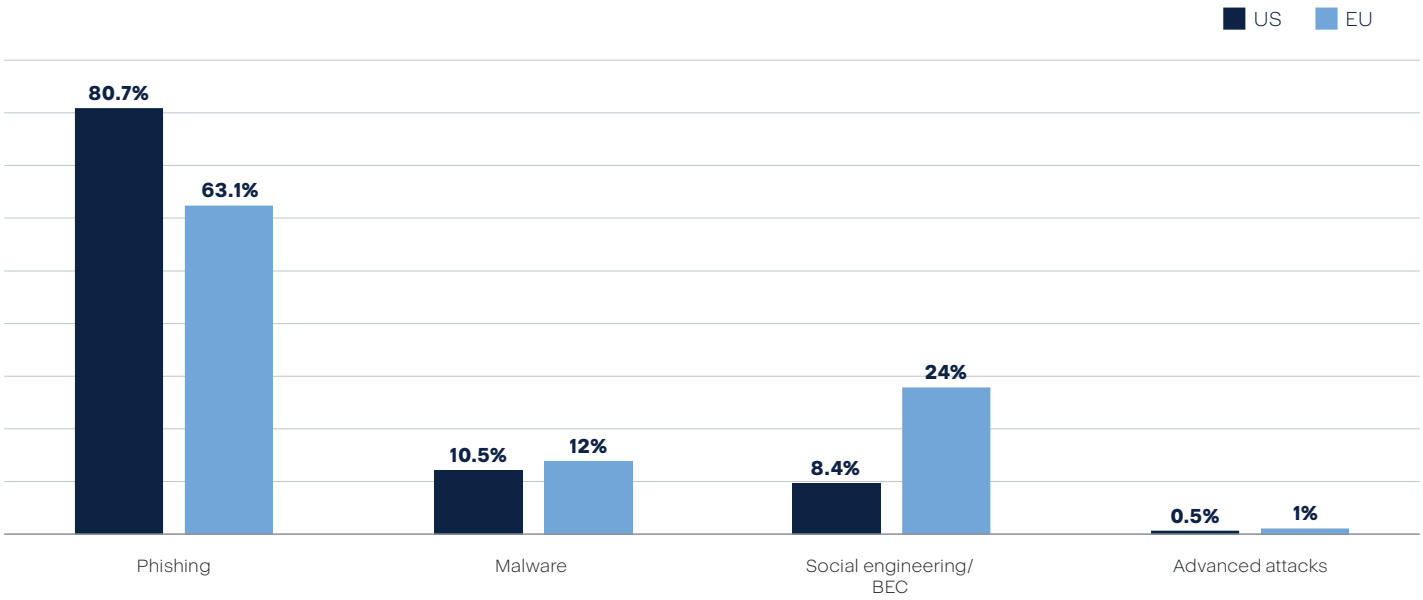
In 2022, each scanned email, contained, on average, 2.7 files and URLs. Any of these could potentially pose a threat to the organization. And as expected, in 2023 we've observed a 15% increase in the number of files and URLs per scanned email. This means that organizations now need to be even more vigilant, as the average number has risen to approximately three files and URLs per scanned email.

The Advanced Email Security pack for Acronis Cyber Protect Cloud is often deployed as a second layer of email filtering, on top of the basic filtering present in most email services. This makes it even more surprising that 30.3%, or about one-third, of emails that made it through were spam.

One out of 76, or 1.3%, of the received emails were malicious. Phishing remains the number one threat, with these attacks making up 73% of the total. However, the business email compromise (BEC)/social engineering category has increased by 7.5 times compared to the same period of time last year, and now takes second place, moving malware — which has dropped in percentage twice — into third.



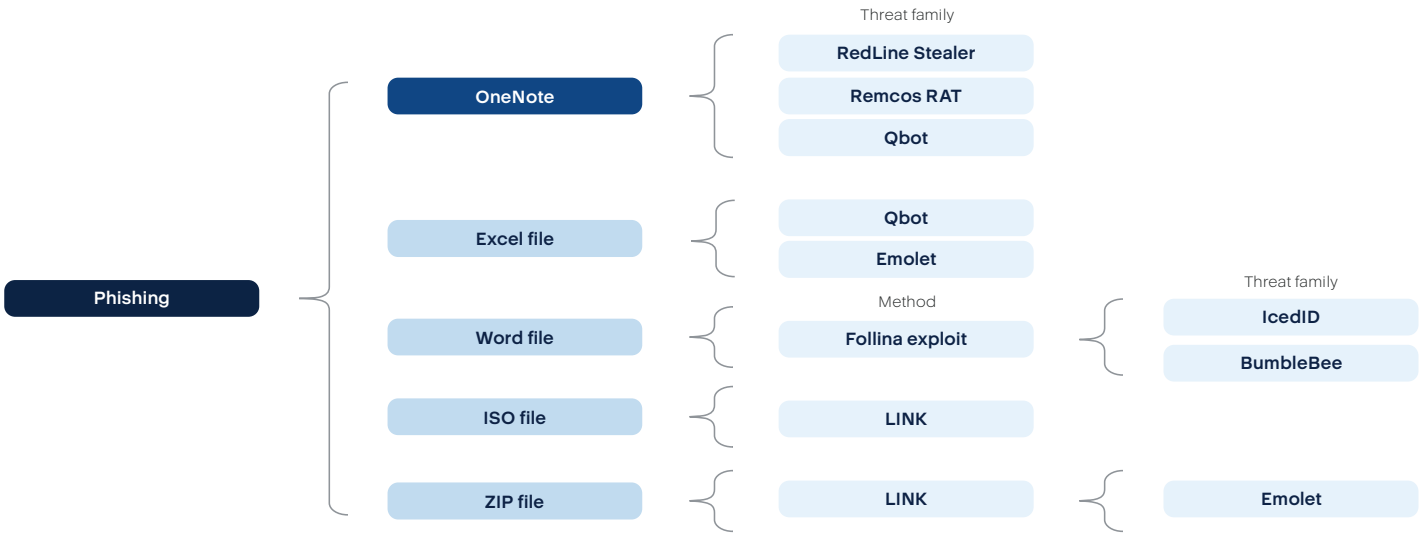
If we take a look at the regional impact and make a comparison for the categories between US and the EU, we will notice varying patterns of attack categories across the U.S. and EU regions. The trend reveals the following observations: Phishing attacks more commonly target the U.S., while BEC/social engineering exhibits a higher percentage of attacks in the EU region. Please refer to the table below for a detailed breakdown of these statistics:



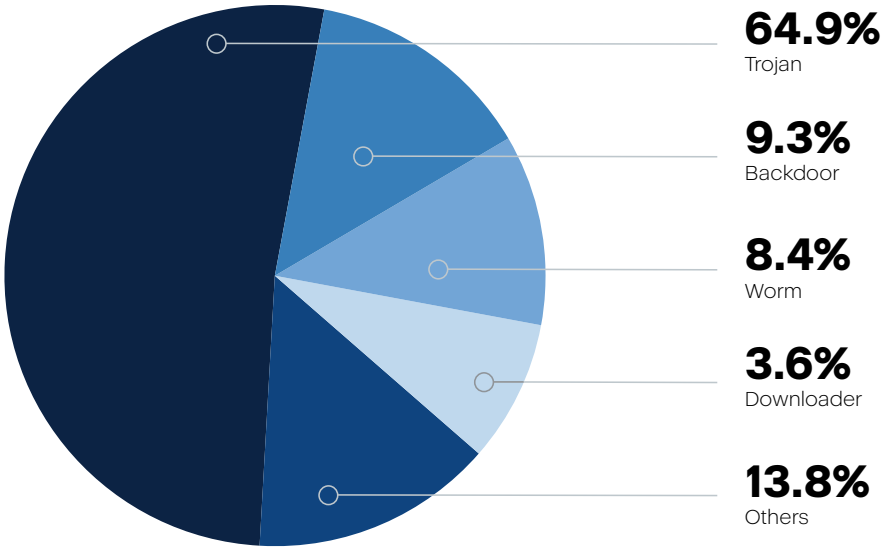
Big cases and phishing trends

Phishing continues to be one of the favorite tools of cybercriminal for penetrating systems. Let's take a look at some big cases discovered by Acronis and other cybersecurity researchers from January–May this year.

We observed a new phishing campaign that targets U.S. taxpayers by impersonating W-9 tax forms allegedly sent by the Internal Revenue Service and companies you work with. This campaign spreads Emotet, a malware threat that was previously distributed via malicious macros embedded in Microsoft Word and Excel documents, but now is delivered primarily via Microsoft OneNote files. Tax forms are usually sent as PDF documents. If the victim clicks the 'View' button in the received One Note file and continues, despite a system warning that the file might be malicious, a VBScript will be launched to download the Emotet DLL. The subsequently installed malware is capable of stealing emails and contacts, and downloading further payloads to the device.



In January, about 8.9% of our clients had at least one malware attack successfully blocked on their endpoints. The percentage peaked at 10.5% in March, returning to 8.9% in May. These high percentages suggest that, despite corporations' attempts at awareness training and patching, about one out of every 10 threats makes it to the endpoint. Furthermore, because these statistics are based on endpoint detections, any proxy or email protection applied earlier in the chain did not prevent these threats.



AV-TEST

Malware types detected in the last two weeks of May 2023 (source: av-test.org)

Month in 2023	Percentage of clients with blocked malware
January	8.9
February	9
March	10.5
April	8.5
May	8.9

Another prevalent trend in the first half of 2023 is the resurgence of malvertising, a well-established method utilized by cybercriminals to distribute malware. This time-tested technique involves leveraging Google Ads and SEO poisoning to promote widely-used software such as Zoom, Cisco AnyConnect, ChatGPT and Citrix Workspace, luring unsuspecting users into downloading malicious payloads.

The most common malware type are Trojan horses, making up more than half of the blocked threats. The most commonly seen malware families for H1 2023 were the following, showing again a clear focus on bots and information stealers:

- RedLine Stealer
- Agent Tesla
- FormBook
- njRAT
- Remcos
- Raccoon Stealer
- Emotet
- NanoCore
- AsyncRat
- IcedID

We've seen only a 4% decrease in the number of new malware samples appearing in the wild since Q4 2022. The independent malware testing lab AV-TEST recorded 219,741 new malware samples per day in Q1 2023, compared to 228,091 in Q4 2022.

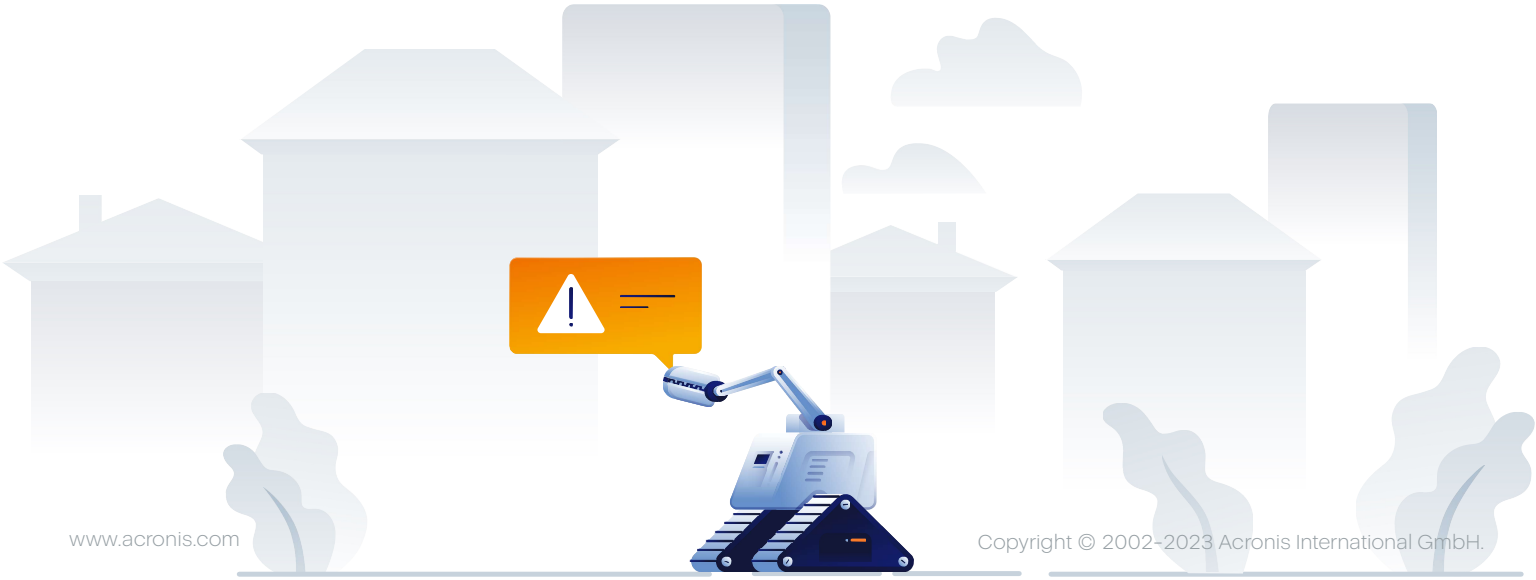
This proportion matches the number of new samples seen by the Acronis CPOCs. This decrease could be the result of some spikes at the end of last year as well as more targeted distribution methods of malware — for example, through malware droppers and distribution networks.

The average lifetime of a malware sample in June 2022 was a mere 2.3 days, after which it disappeared and was never seen again by us. In May 2023, this figure was down to 2.1 days. Malware is shorter-lived than ever as attackers use automation to create new and personalized malware at blazing speeds, in an effort to bypass traditional signature-based detection. Of all the samples observed, 73% were seen only once across our customer base.

The country with the most clients experiencing malware detections in May 2023 was the United States with 18.4%, followed by Brazil with 9.0% and Germany with 8.7%.

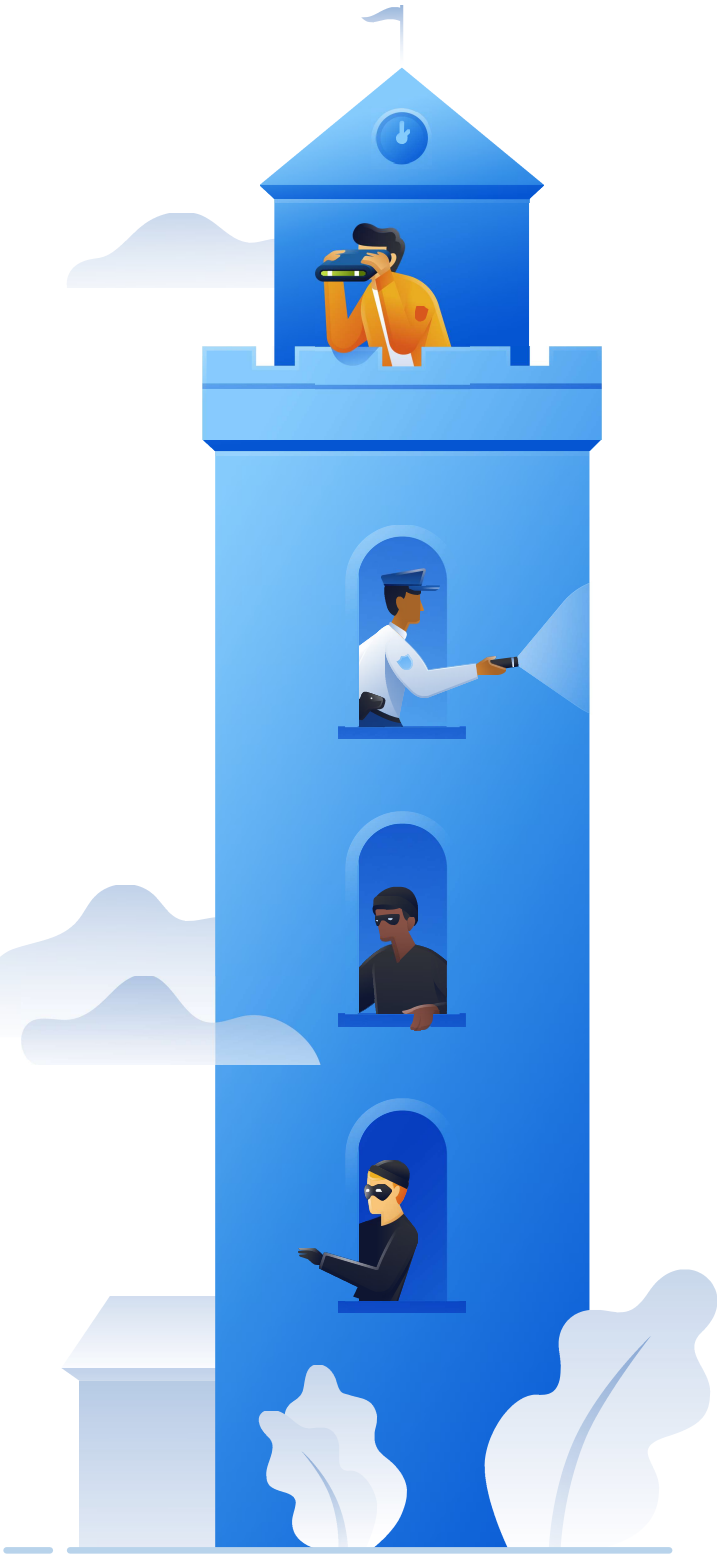
Monthly percentage of global detections by country

Country	Jan	Feb	Mar	Apr	May
United States	21.2	21	18.5	19.4	18.4
Brazil	6.6	6.6	7.1	7.9	9
Germany	9.2	8.5	9.3	8.9	8.7
Singapore	5.2	5.7	5	5.8	6.1
Canada	5.7	5.5	5.8	5.3	5.3
Italy	4.5	4.7	5.4	5	4.8
United Kingdom	5	4.9	5	4.6	4.1
Switzerland	3.4	4.8	4.2	4	4.1
Japan	3.7	3.9	3.3	4	3.7
France	3.3	2.9	3.3	3	2.9

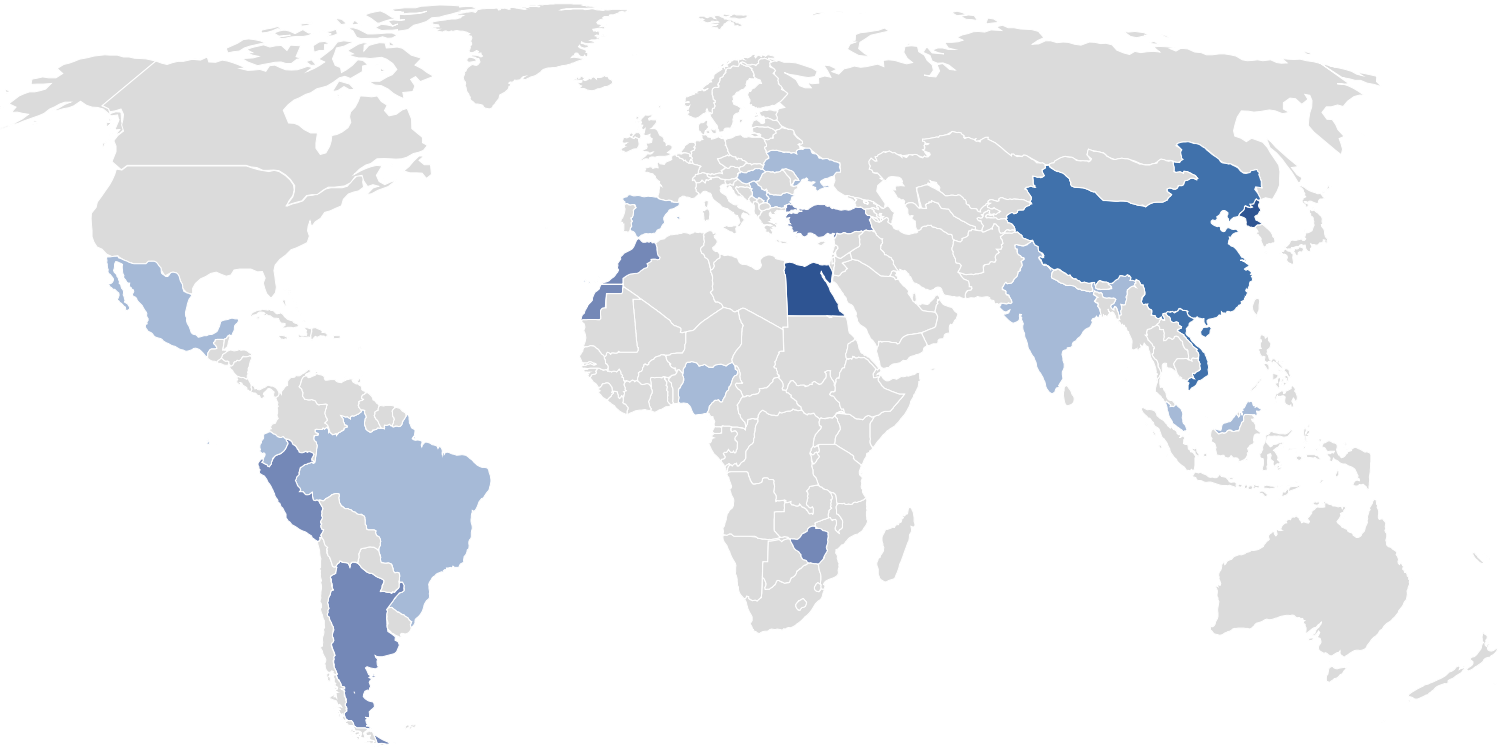


If we normalize the number of detections per active client per country, then we get a slightly different distribution. The following table shows the normalized percentage of clients per country with at least 25 malware detections per country in April 2023.

Rank	Country	Percentage of clients with malware detections in April 2023 (normalized)
1	South Korea	26
2	Egypt	25.7
3	Singapore	23.2
4	Taiwan	21.1
5	China	20.4
6	Vietnam	18.2
7	Morocco	17.1
8	Argentina	16.3
9	Turkey	15.7
10	Nigeria	14.5
11	Hungary	14.3
12	Zimbabwe	13.2
13	Bulgaria	13.1
14	Mexico	12.7
15	India	12.7
16	Serbia	12.6
17	Peru	12.1
18	Malaysia	12
19	Ukraine	11.9
20	Brazil	11.8
21	Dominican Republic	11.7
22	Spain	11.5
23	Israel	11.4
24	Hashemite Kingdom of Jordan	11.1
25	Ecuador	10.3



Top 25 countries: Normalized malware detections, April 2023



Regional normalized malware detection numbers

Top 10 countries: Normalized malware detection numbers by region

APAC

Rank	Country	Regional normalized malware detection percentage in April 2023
1	Taiwan	26
2	Vietnam	24.4
3	India	23.4
4	China	23.3
5	Singapore	22.6
6	South Korea	22.5
7	Philippines	19.4
8	Thailand	16.5
9	Indonesia	11.9
10	Malaysia	11.9

EMEA

Rank	Country	Regional normalized malware detection percentage in April 2023
1	Egypt	25.7
2	Morocco	17.1
3	Turkey	15.7
4	Nigeria	14.5
5	Hungary	14.3
6	Zimbabwe	13.2
7	Bulgaria	13.1
8	Serbia	12.6
9	Ukraine	11.9
10	Spain	11.5

Americas

Rank	Country	Regional normalized malware detection percentage in April 2023
1	Peru	20.1
2	Ecuador	17.9
3	Venezuela	17.6
4	Argentina	14.9
5	Mexico	14.2
6	Brazil	14.2
7	Colombia	12.2
8	Dominican Republic	12.1
9	Chile	10.7
10	United States	9.5

Prevalent malware in the spotlight

This time we focused our attention on the infostealers that are increasingly on everyone's radar, and pose a similarly significant threat as ransomware. Successful infostealing attacks can in fact lead to a breach that results in a huge ransom, so all these threats are interconnected.

We already reviewed an infostealing trend at the beginning of this report, and below you'll find a detailed analysis of an actual threat in this space.

Raccoon Stealer: One of the most popular and dangerous malware threats

Raccoon Stealer, also known as "Mohazo" or "Racealer," is an infostealer that first appeared in 2019 and is available as malware-as-a-service (MaaS). It can be obtained from cybercrime forums, and a subscription costs $200 per month.

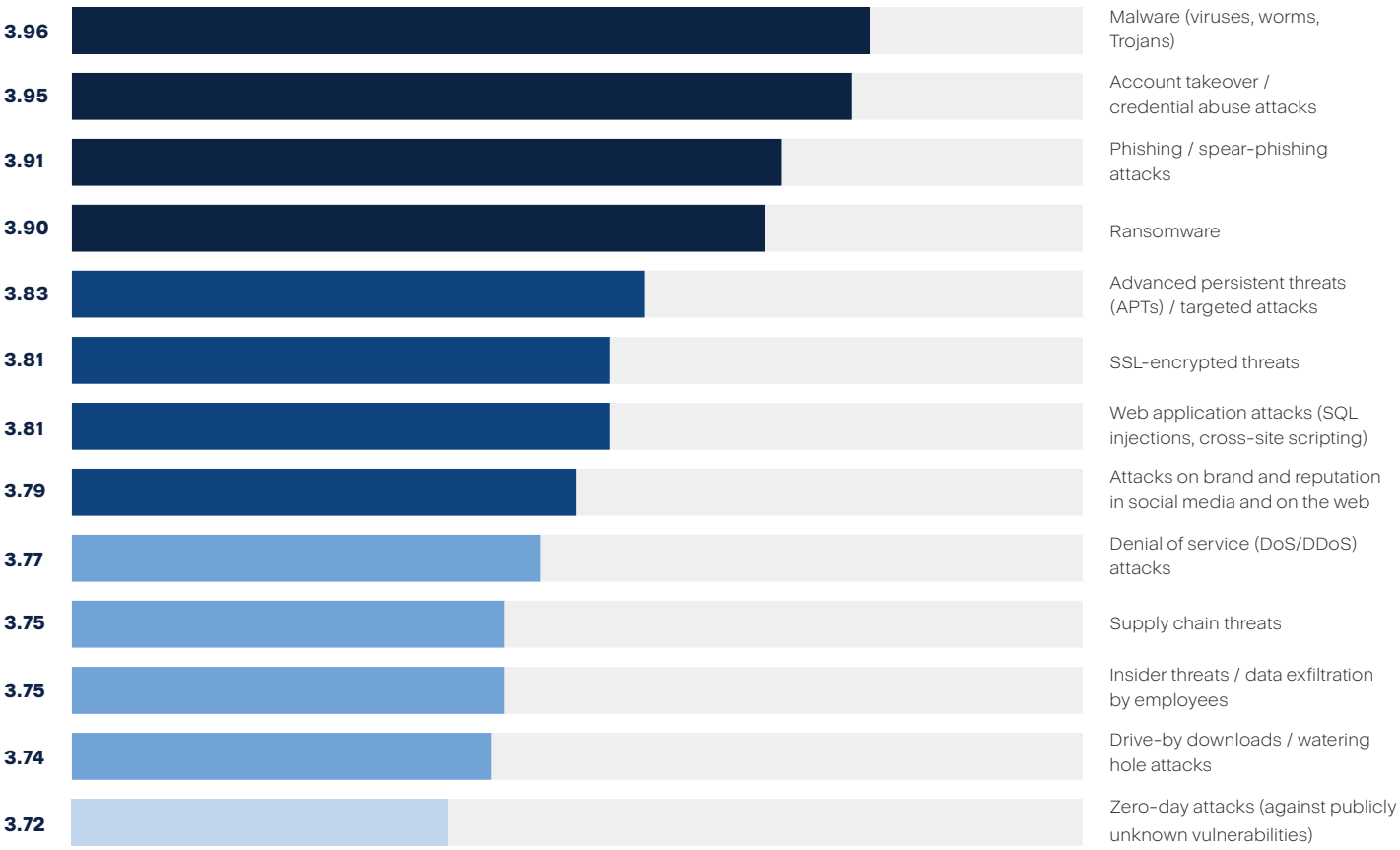
Raccoon Stealer has already infected over 100,000 devices in the wild, including both organizations and individuals, and is one of the most frequently mentioned threats on underground forums. This malware is used to steal data like credit card information, desktop cryptocurrency wallet contents, cookies and passwords. Raccoon Stealer performs SQL queries using sqlite3.dll in order to get the user's auto-login passwords, credit card information, cookies, and browser history.

It is delivered most often through exploit kits and phishing attacks, sometimes in combination with remote command-and-control servers. In the past, Racoon Stealer has been delivered via phishing emails with malicious macros embedded in an MS Excel file.

Ransomware threats

Falling victim to ransomware is among the greatest concerns for individuals and organizations globally.

On a scale of 1 to 5, with 5 being highest, rate your overall concern for each of the following types of cyberthreats targeting your organization.



Source: https://cyber-edge.com/wp-content/uploads/2023/04/CyberEdge-2023-CDR-Report-v1.0.pdf

And it's no wonder, as the number and frequency of ransomware attacks remains high.

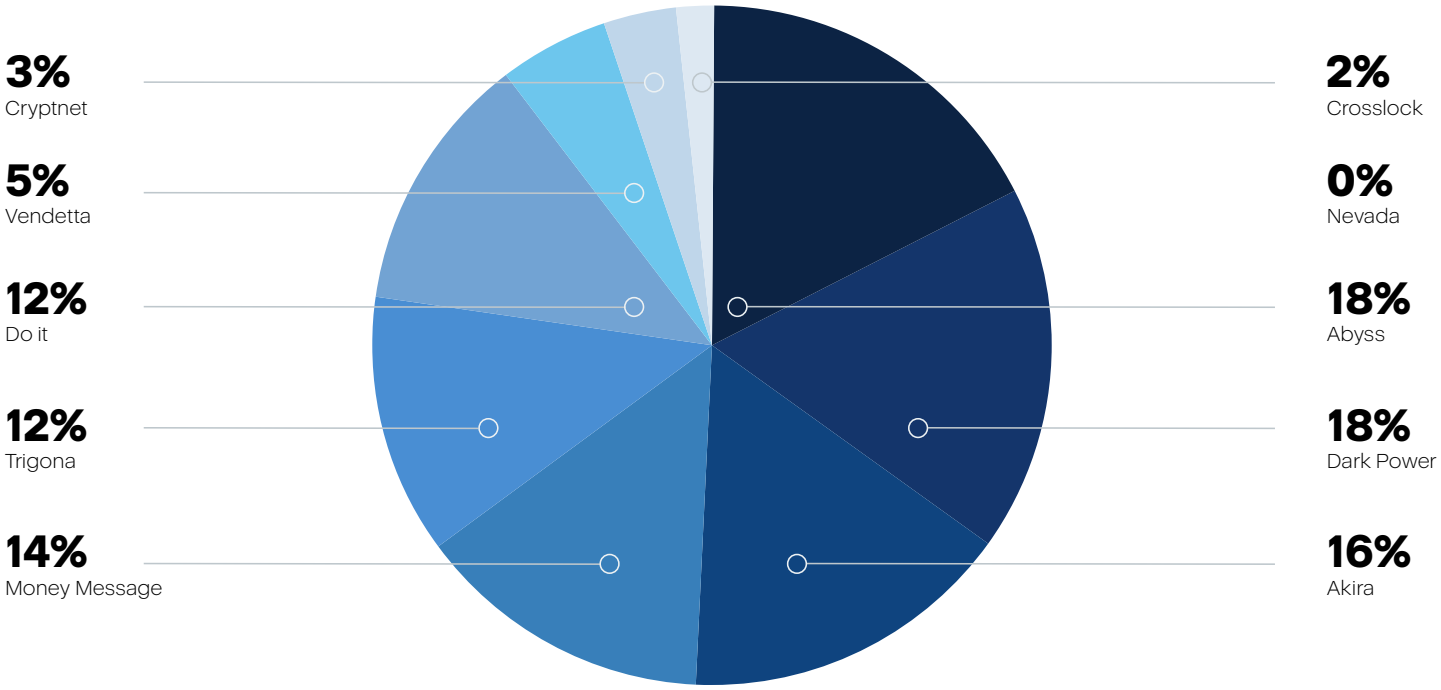
In this section we have reviewed data, spanning from January–April 2023, that was intercepted and safeguarded by our threat-agnostic Acronis Active Protection. We've also analyzed data that has been made public on the underground leak sites of ransomware operators.

While law enforcement has made several arrests and increased the pressure on ransomware groups, some attacks are being thwarted earlier in the process — such as at the email lure or malicious URL stage — resulting in the final ransomware not being downloaded. As a result, these attacks are not included in current statistics.

Despite these developments, the availability of large language models (LLM) like ChatGPT has enabled cybercriminals to increase the number of attacks further through automation and repetition. This has led to a growing number of players in the ransomware market.

In Q1 2023 we saw the appearance of 10 new groups, which together claimed 61 globally.

- Abyss → 10
- Akira → 9
- Trigona → 7
- Vendetta → 3
- Crosslock → 1
- Dark Power → 10
- Money Message → 8
- Do it → 7
- Cryptnet → 2
- Nevada → 0



Here are the top 10 most active ransomware families we observed and tracked in Q1 2023. Three highly active groups stand out as the primary contributors, collectively responsible for about 57% of the attacks. Among these groups, LockBit takes the lead, accounting for 34.6% of attacks, followed by Clop with 13.1% and ALPHV/BlackCat with 9.1%.

1. LockBit	3. BlackCat / ALPHV	5. Play	7. Medusa	9. Black Basta
2. Clop	4. Royal	6. BianLian	8. Vice Society	10. Stormous

We've seen 809 publicly mentioned ransomware cases in Q1 2023, with a 62% spike above the monthly average in March (270 cases). In April, the number increased again to 308 cases, and in May dropped to 275.

It should be noted that the mentioned statistics represent only a portion of the overall picture, as certain victims choose to negotiate with, and ultimately pay, their attackers to avoid public exposure. Unfortunately, paying a ransom does not provide any guarantee that the stolen data will be deleted on the attacker's end.

Historical cases have revealed that victims who complied with ransom demands were later targeted for additional extortion, witnessed their data being sold to other malicious actors or saw it leaked online.

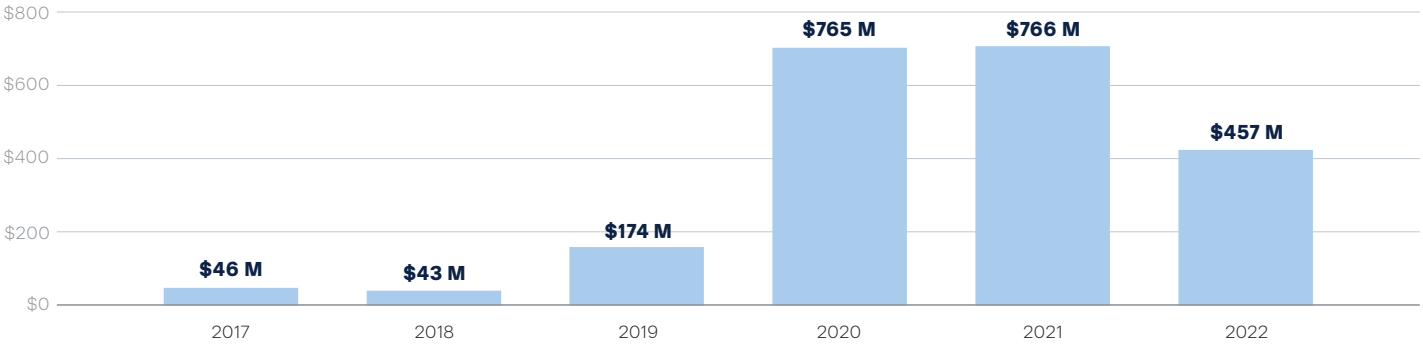


Figure 1: Total value received by ransomware attackers 2017-2022 (ChainAnalysis)

Daily ransomware detections

The number of ransomware detections has increased by 6% in Q1 over Q4 2022. Since then, the number of monthly ransomware detections has stayed relatively flat for 2023.

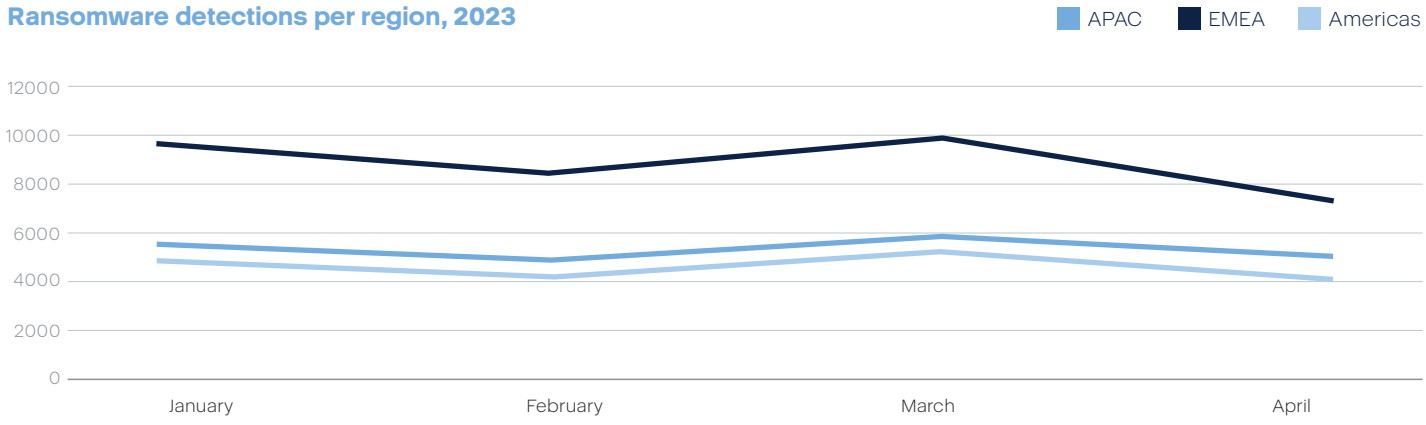
Increase in the number of ransomware detections percentage per region in comparison of Q1 2023 to Q4 2022

Quarter	EMEA	Americas	Asia	Global
Q1/2023 - Q4/2022	2	9	9	6

If we follow the changes from month to month in 2023, during the period from January to February globally, the number of detections has decreased by 8. The spike for all three regions was from February to March, with the highest in the Americas (16.9%) and a decline again from March to April, with the lowest being in EMEA with (-27.9%).

Period	EMEA	Americas	Asia	Global
January–February	-11	-4.1	-6.7	-8
February–March	12.5	16.9	14.7	14.3
March–April	-27.9	-17.6	-22.4	-23.5

Ransomware detections per region, 2023

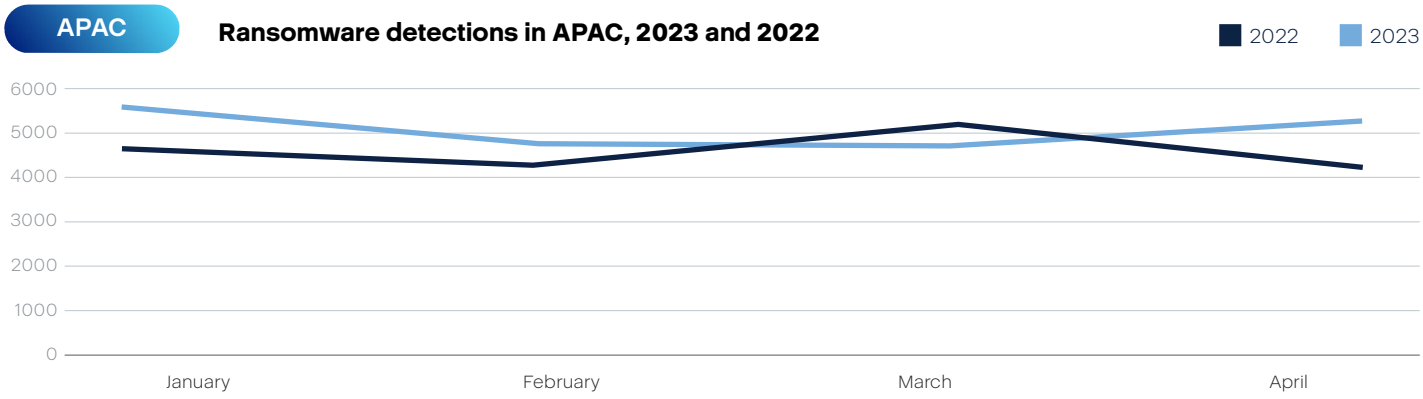


We've taken a closer look at the different regions and compared ransomware detections between January–April this year to those of the same period in 2022. Interestingly, even though we saw a decreasing trend from January to February in both years, the trends from February to April turned out to be the opposite of what we saw in 2022 for all three regions in comparison.

We can also see that EMEA and the Americas had a slight decrease in ransomware attacks that were blocked at the endpoint in 2023 compared to the previous year. This could be an indication that these regions were getting better at blocking threats earlier in the cyber kill chain.

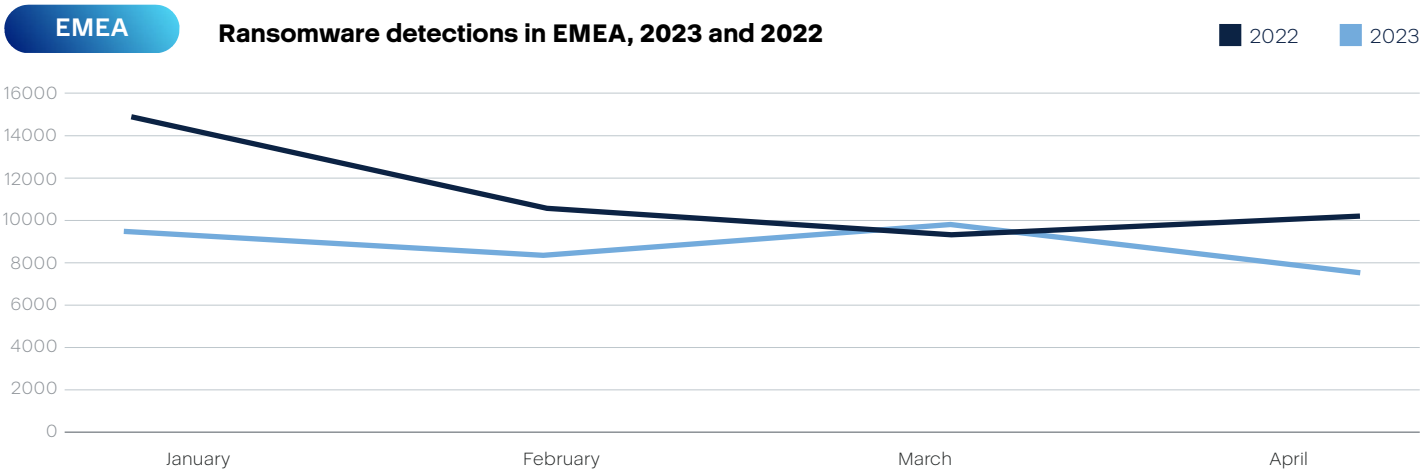
APAC

Ransomware detections in APAC, 2023 and 2022



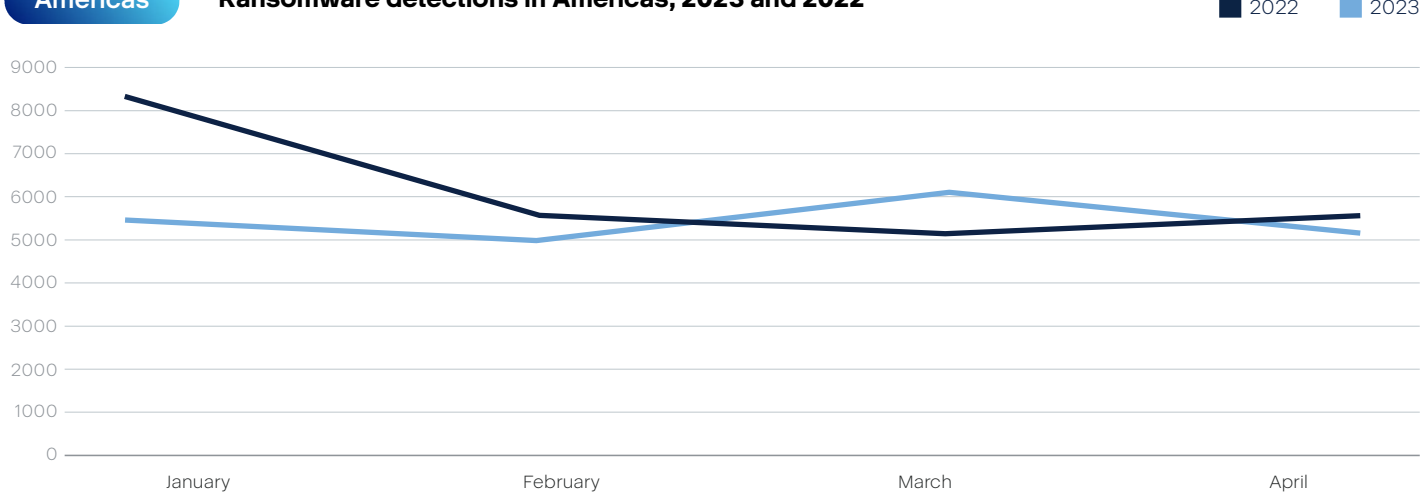
EMEA

Ransomware detections in EMEA, 2023 and 2022



Americas

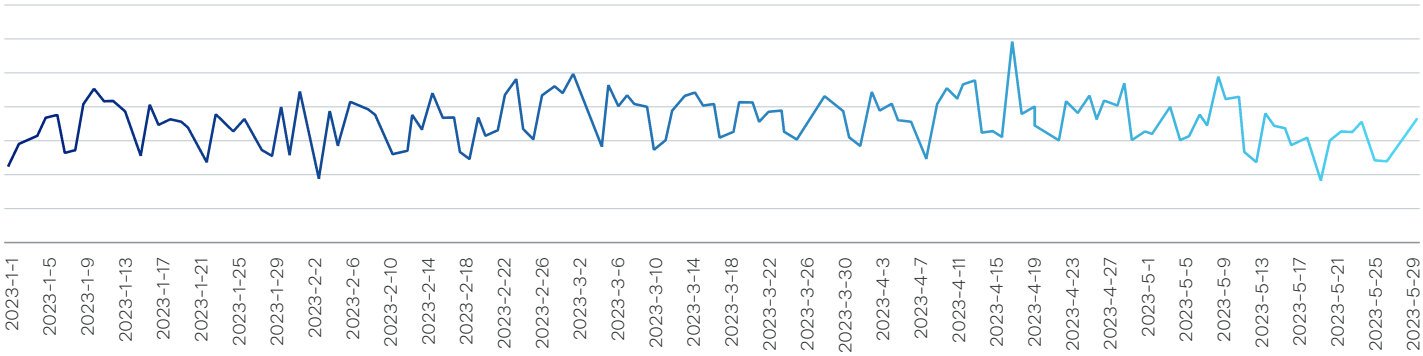
Ransomware detections in Americas, 2023 and 2022



The daily number of ransomware detections appears to be relatively stable, with no significant spikes recently and a slight upward trend overall. This reinforces the importance of maintaining high resilience through the implementation of a multi-layered cyber protection solution, as well as the frequent testing and adoption of an incident response plan. Such procedures are crucial for ensuring that companies are well-prepared to defend against, and respond to, ransomware attacks.

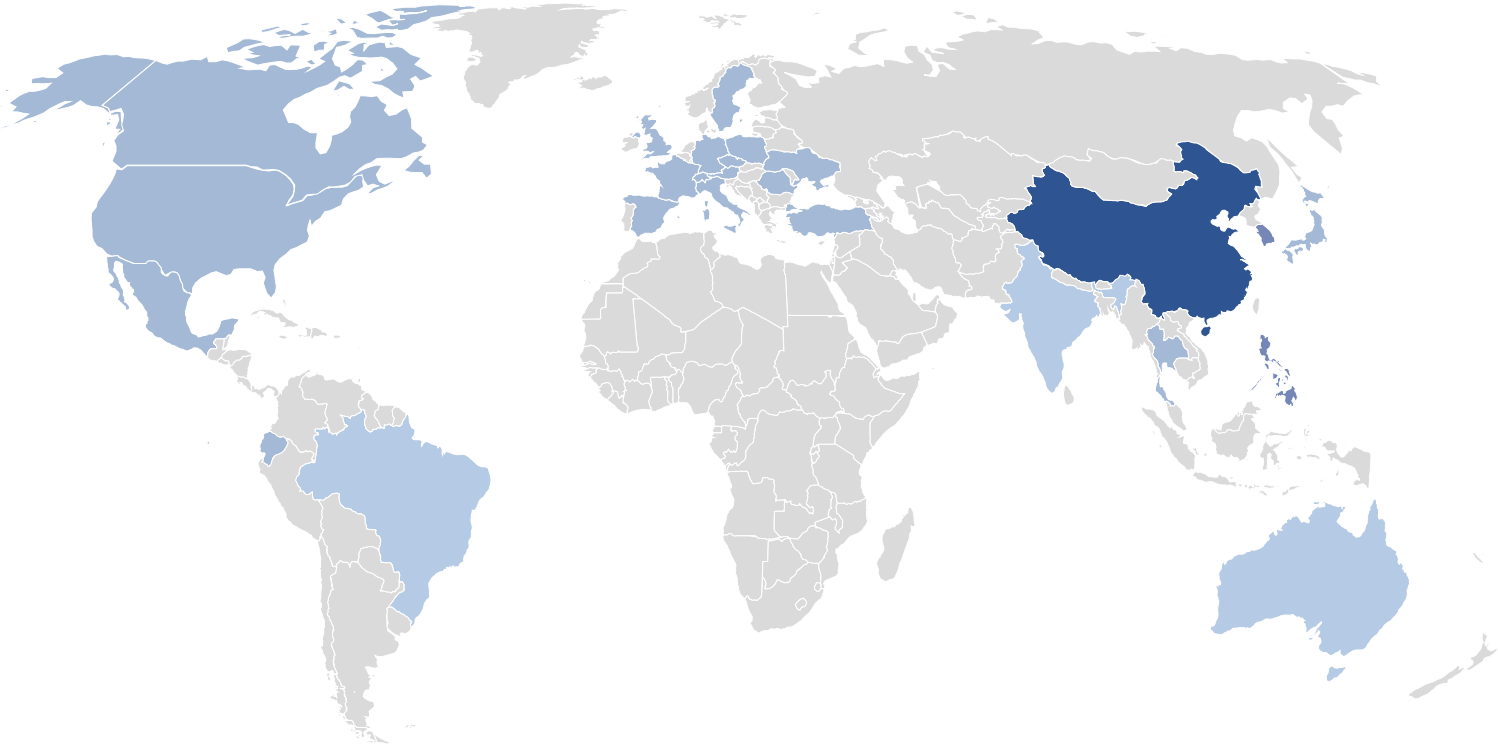
Daily ransomware detections globally

Daily ransomware detections



The peak day of ransomware detections in this period was April 18, and the lowest day of ransomware detections was May 21.

Ransomware detections, April 2023



Percentage

0.2% 63.3%

We've normalized the number of ransomware detections, considering only machines with more than 25 detections and countries where we have more than 150 installations.

Top 20 countries: Global ransomware detections by quarter normalized

Rank	Country	Global ransomware detection percentage in Q1 2023	Global ransomware detection percentage in Q4 2022
1	China	37.85	39.10
2	South Korea	34.07	34.41
3	Philippines	20.80	19.81
4	Vietnam	14.22	12.19
5	Egypt	12.70	10.13
6	Japan	12.64	11.45
7	Taiwan	11.17	13.19
8	Germany	8.60	9.10
9	Hungary	7.72	5.72
10	Thailand	7.65	5.90
11	Slovakia	7.28	8.23
12	Turkey	6.96	6.84
13	Peru	6.82	8.36
14	Hong Kong	6.20	7.67
15	Spain	5.80	5.26
16	Poland	5.65	6.31
17	Czechia	5.58	5.95
18	Ukraine	5.42	5.26
19	United States	5.26	4.82
20	Norway	5.12	3.72

Top five countries: Ransomware detections by quarter normalized

The leading top three countries in APAC were China (37.85%), South Korea (34.07%) and the Philippines (20.80%).

APAC

Country	Regional ransomware detection percentage in Q1 2023	Regional ransomware detection percentage in Q4 2022
China	37.85	39.10
South Korea	34.07	34.41
Philippines	20.80	19.81
Vietnam	14.22	12.19
Japan	12.64	11.45

The leading top three countries in EMEA were Egypt (12.7%), Germany (8.6%) and Hungary (7.72%).

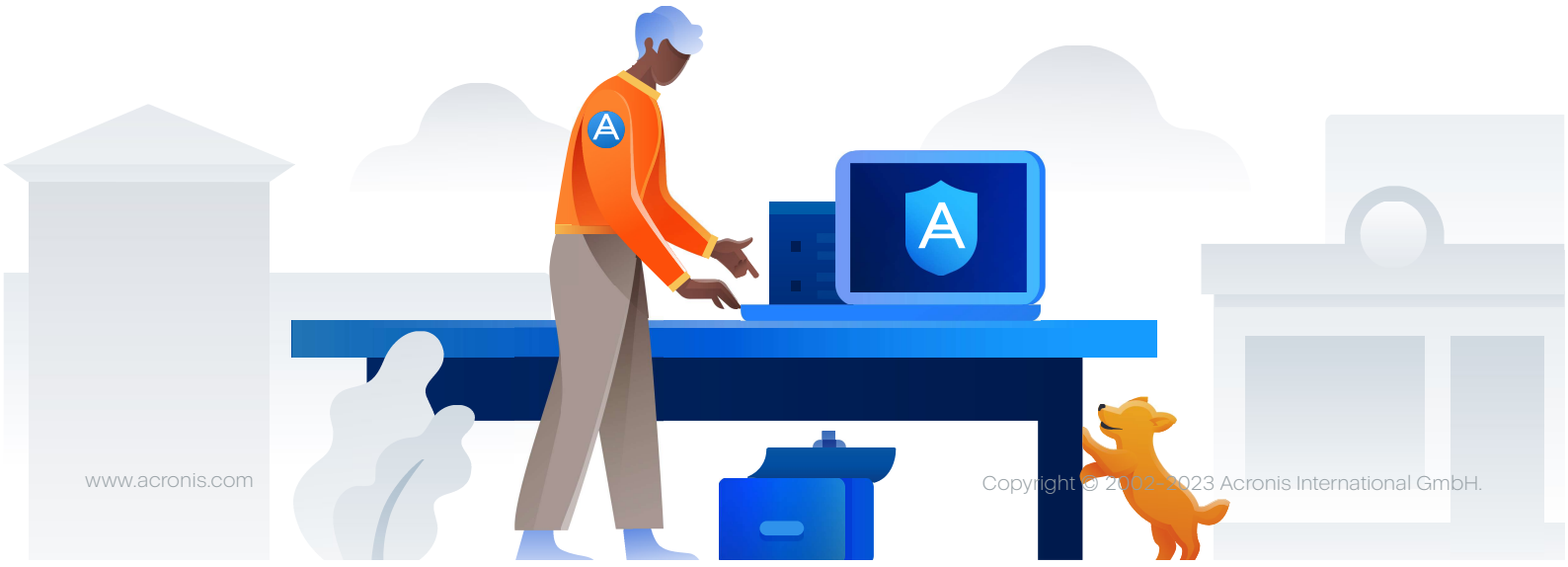
EMEA

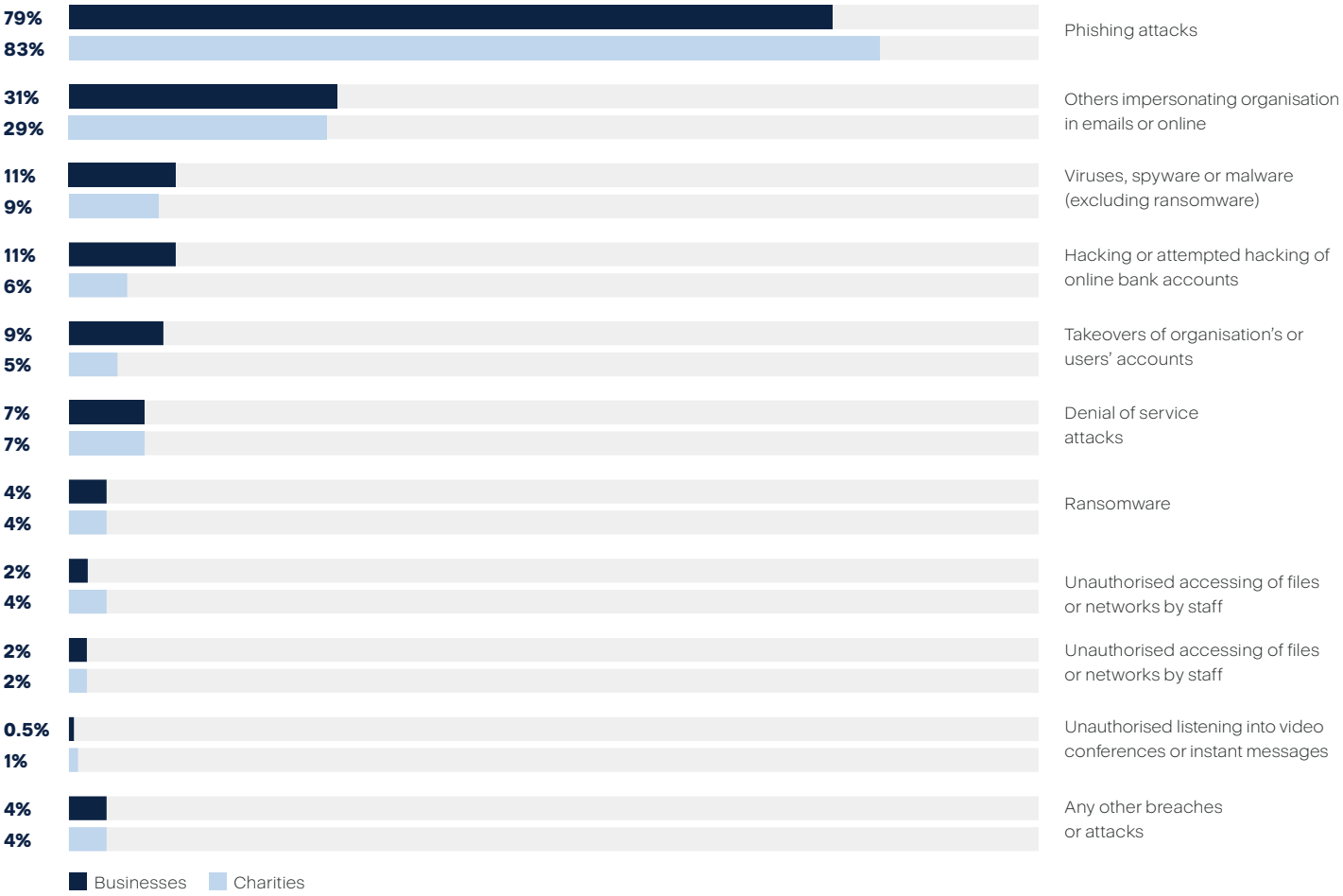
Country	Regional ransomware detection percentage in Q1 2023	Regional ransomware detection percentage in Q4 2022
Egypt	12.70	10.13
Germany	8.60	9.10
Hungary	7.72	5.72
Slovakia	7.28	8.23
Turkey	6.96	6.84

The leading top three countries in the Americas were Peru (6.82%), the United States (5.26%) and Argentina (4.92%).

Americas

Country	Regional ransomware detection percentage in Q1 2023	Regional ransomware detection percentage in Q4 2022
Peru	6.82	8.36
United States	5.26	4.82
Argentina	4.92	5.96
Mexico	3.75	3.27
Canada	3.05	2.96

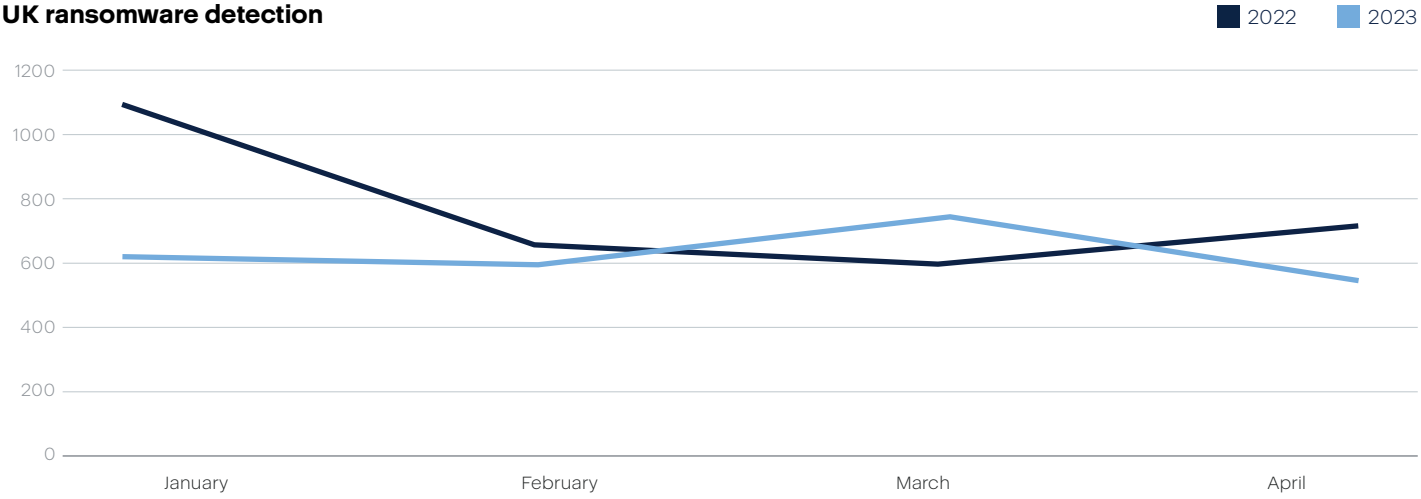




Source: Cyber security breaches survey 2023 - GOV.UK (www.gov.uk)

In January 2023, Royal Mail — the multinational postal service of Britain — fell victim to LockBit. The group demanded an unprecedented ransom of $80 million, claiming the title of largest ransom to date. Royal Mail swiftly dismissed the demand as 'absurd.' In response, LockBit publicly released stolen files from the company and provided an illuminating transcript documenting the negotiation process between the two entities.

UK ransomware detection



Similar to the U.S. education sector's situation in the early months of 2023, the BBC covered a series of attacks on 14 U.K. schools carried out by Vice Society in the previous year.

The Clop ransomware victims list was updated with entities including British multinational conglomerate Virgin's rewards club, Virgin Red; Procter & Gamble; and the U.K.'s Pension Protection Fund. Some retail businesses, like Yum! Brands and car dealer Arnold Clarke, also fell victim.

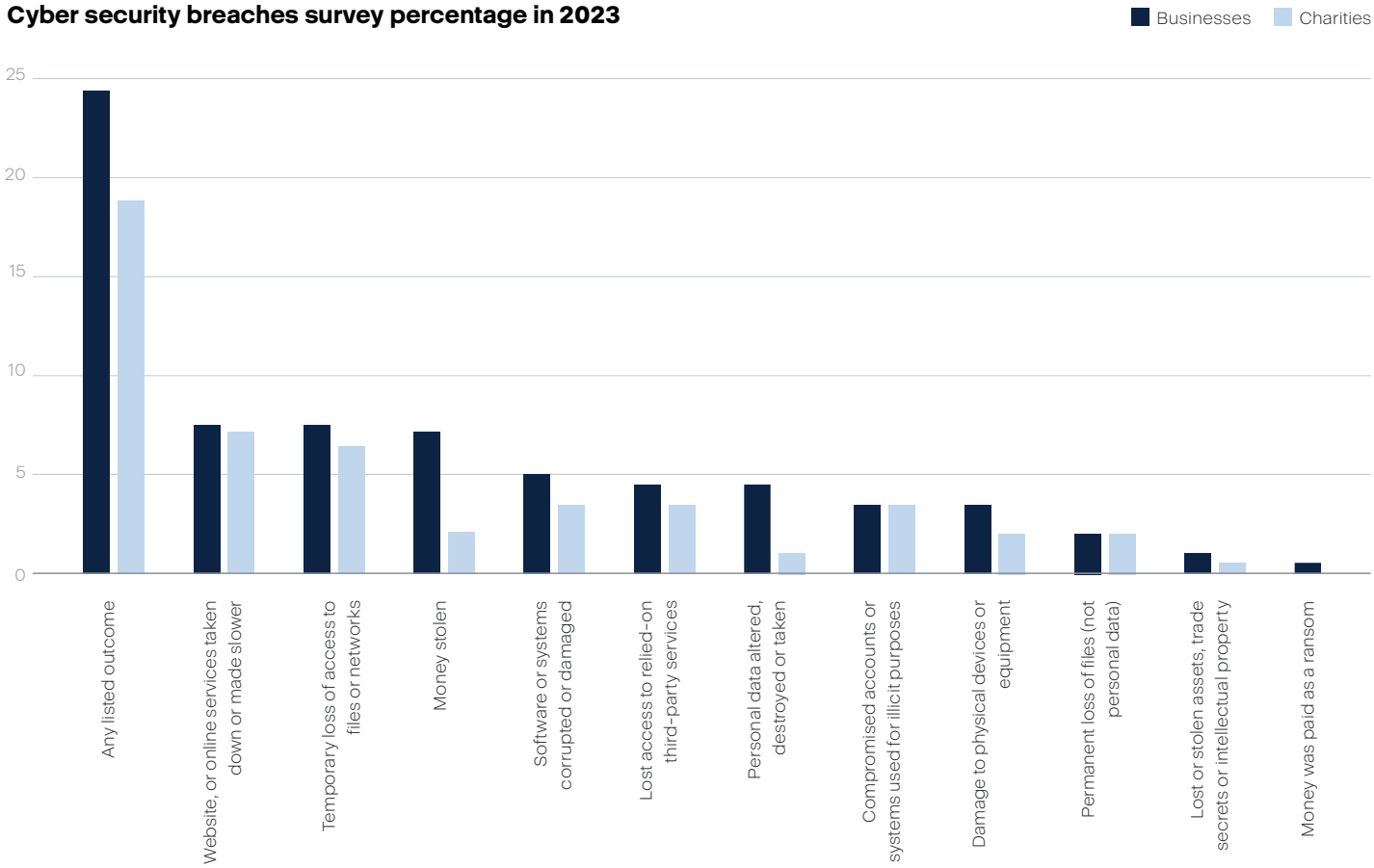
The U.K. Criminal Records Office (ACRO) encountered a cyber incident that led to the temporary closure of its customer portal, causing significant disruptions to various operations over an extended duration. ACRO informed users via email about the situation, acknowledging that they were informed of a cybersecurity incident that occurred on their website from January 17 to March 21. However, they stated that there was no definitive evidence to suggest that personal data had been compromised.

Another example from Q1 2023 is Vesuvius, a U.K.-based molten metal flow engineering company with an annual revenue of $2.2 billion and more than 10,000 employees. The company was hit by a cyberattack, which they estimate will cost £3.5 million (approximately $4.6 million at the current exchange rate) in damages.

Earlier, ION Group, another U.K.-based company with a revenue of $273 million and over 1300 employees, suffered a cyber incident. The financial trading services firm was hit by the ransomware group LockBit. ION initiated an investigation of the attack, which affected 42 of their clients and forced a number of European and U.S. banks and brokers to process certain trades manually.

For companies, the most frequently reported outcomes of data breaches and attacks involve website disruptions and temporary loss of access to files or networks. These consequences have a direct impact on productivity and result in financial implications for the affected organizations.

Cyber security breaches survey percentage in 2023



Source: Cyber security breaches survey 2023 - GOV.UK (www.gov.uk)

SOTI

V10 ISSUE 02

10 YEARS
OF SECURITY INSIGHT

Fighting the Heat

EMEA's Rising DDoS Threats

Akamai

State of the Internet/Security

DDoS then and now

DDoS attacks, whether deployed by individuals or botnets, flood servers with requests and overwhelm them with traffic, which leads to the hosted services and sites being unavailable for users and visitors.

DDoS attacks have evolved from the period in which open-source tools were used by threat actors to conduct them. For this group, motivation was often simplistic — perhaps they were dissatisfied with the newest game feature, hoping to gain a competitive edge, or just looking for sport. In general, this group of threat actors did not dominate the attack landscape with trends of targeting critical infrastructure or hospitals, nor with aiming to severely damage networks or endanger human life.

Hacktivism changed the landscape dramatically, both in terms of the threat actors' identities and their motivation. While some hacktivist attacks may have only limited or nuisance-level impact, others target commercial industry for significant financial gain and may cause service outages that last for days. Attacks can have potentially life-threatening consequences, as seen in some healthcare center attacks.

The ability to conduct DDoS attacks has become simpler over the past few years, with the emergence of services such as DDoS booter services, that allow even the most unsophisticated adversary to launch an attack with just a click of a button and for a nominal fee — sometimes as low as €10. These simple attack launches then lead to a plethora of traffic, which forces entire websites and networks offline, harming businesses both financially and operationally and depriving customers and users of crucial services.

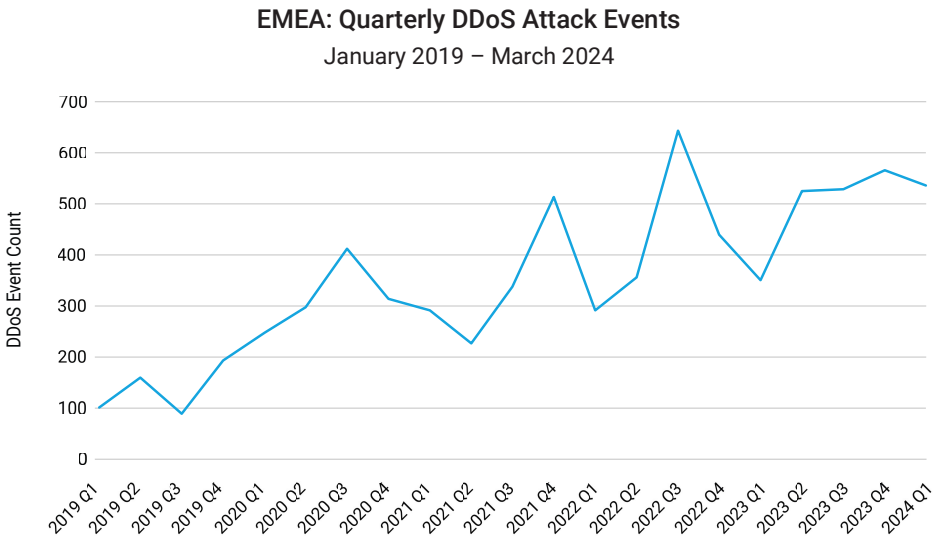


Fig. 1b: The growth of DDoS attacks in the EMEA region

Within the EMEA region, the United Kingdom (26%), Saudi Arabia (22.3%), and Germany (9.1%) lead the way for countries with the highest number of attack events. Also, Akamai's findings show that more than one-third of all DDoS attack events globally are in the EMEA region (Figure 2).

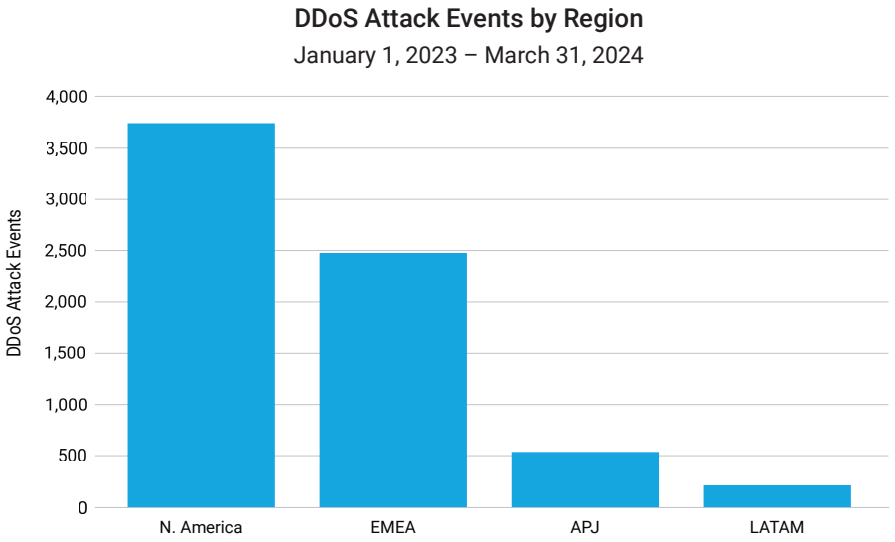


Fig. 2: The number of EMEA DDoS attacks climbed to nearly 2,500 from the beginning of 2023 to the first quarter of 2024 — more than three times as many as in the Asia-Pacific and Japan (APJ) and Latin America (LATAM) regions combined

In the financial services vertical, EMEA is the region with the most amount of DDoS Layers 3 and 4 attack event traffic (Figure 3). As mentioned earlier, Russian hacktivist groups declared their intention to launch DDoS attacks on the European banking system, and we surmise that the main reason for the rise in DDoS attack events in the financial services industry is this geopolitical hacktivism.

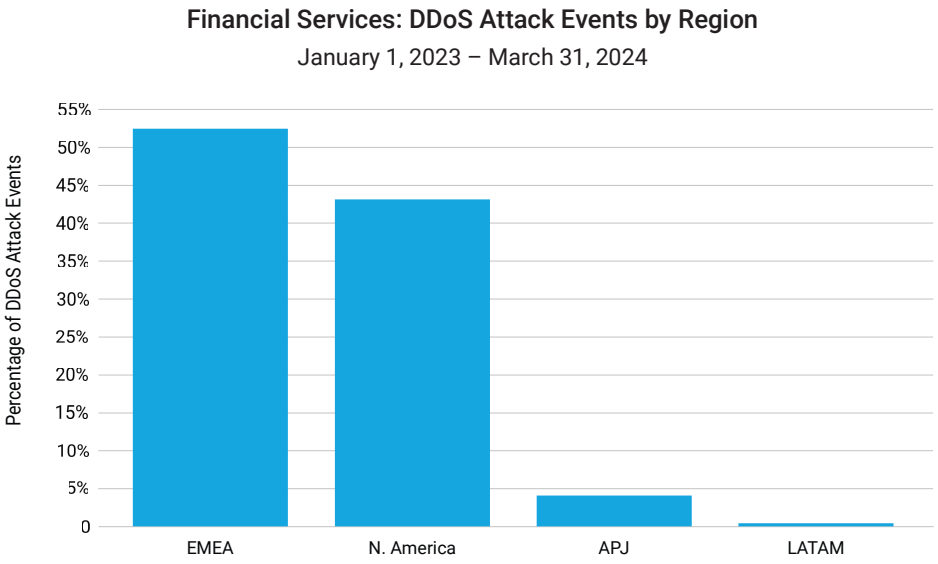


Fig. 3: EMEA experienced 52.5% of the regional DDoS Layers 3 and 4 attack event traffic in the financial services vertical

In addition to Layer 3 and 4 attacks, financial services applications are plagued by Layer 7 DDoS attacks. But the commerce vertical is seeing the largest increase in Layer 7 DDoS attacks in EMEA, experiencing almost 30% of all attacks in the region (Figure 4).

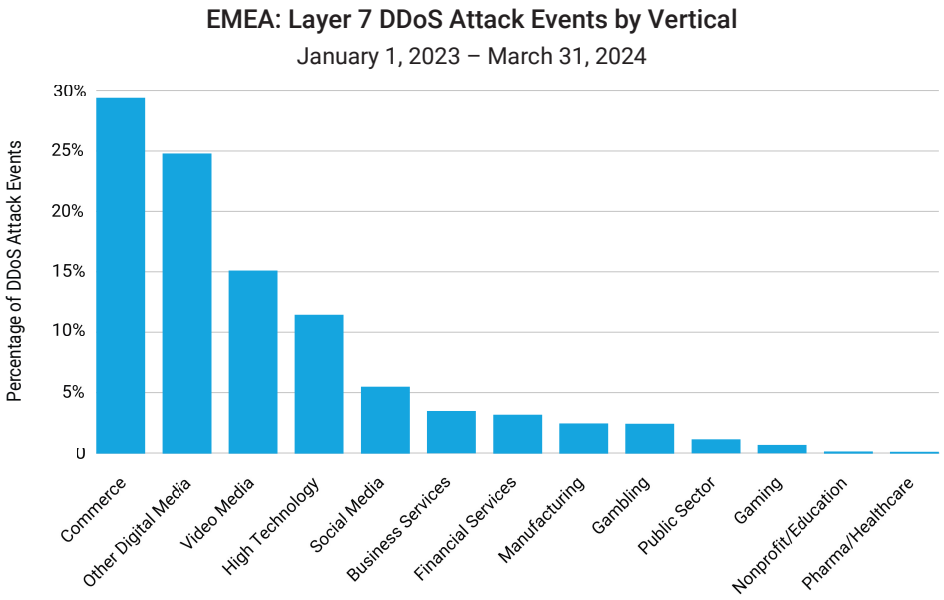
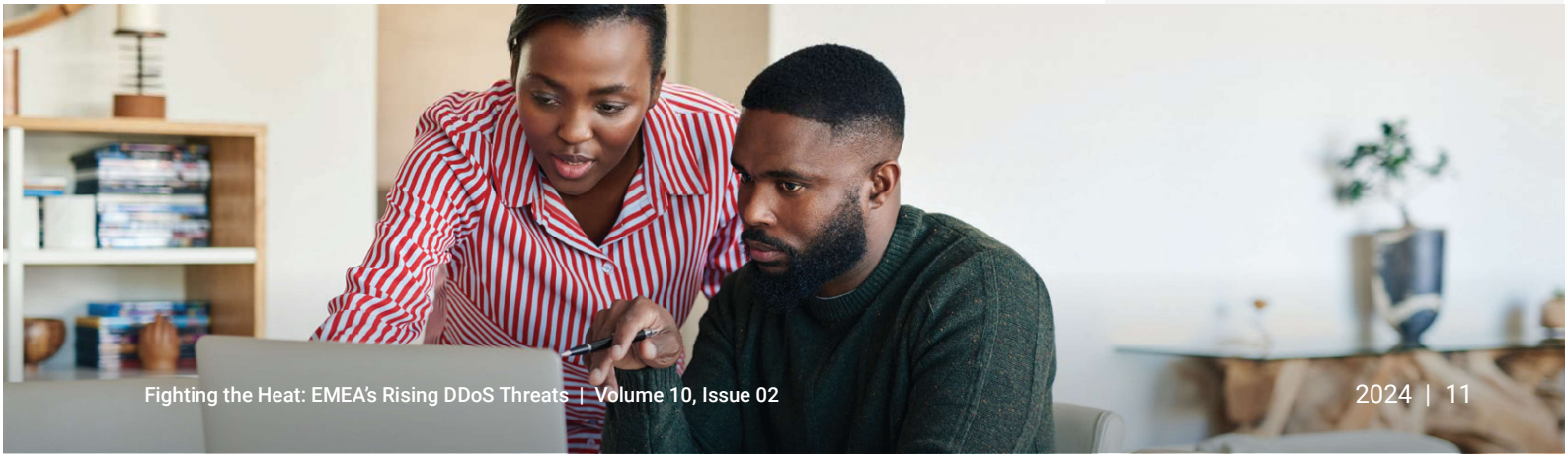


Fig. 4: The commerce vertical experiences 29.4% of the regional DDoS Layers 7 attack event traffic in EMEA

It is possible that application-layer DDoS attacks, like those that employ HTTP flooding, may be highest in the commerce vertical because of the significant revenue disruption opportunity these attacks offer to threat actors. These types of attacks are especially crippling for commerce organizations because they can make an online store inaccessible or a reservation system unavailable, leading to a significant revenue loss for the victim company. Additionally, they may be deployed as a distraction tactic to consume incident response resources, while attackers aim to steal lucrative customer data (such as payment card information) from other areas in the victim's network.



While DDoS attack event numbers have been on the rise, we have also observed that the number of vectors used to deploy DDoS attacks has increased sharply (Figure 5a). Those attack types include DNS Flood, UDP Fragment, and NTP Reflection (Figure 5b). Attacks have also been lasting longer.

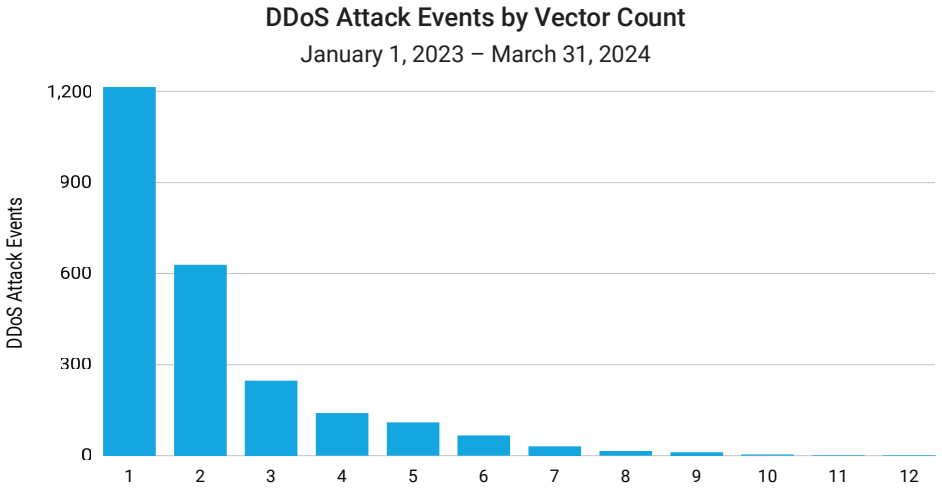


Fig. 5a: The number of vectors used to deploy DDoS attacks has increased sharply

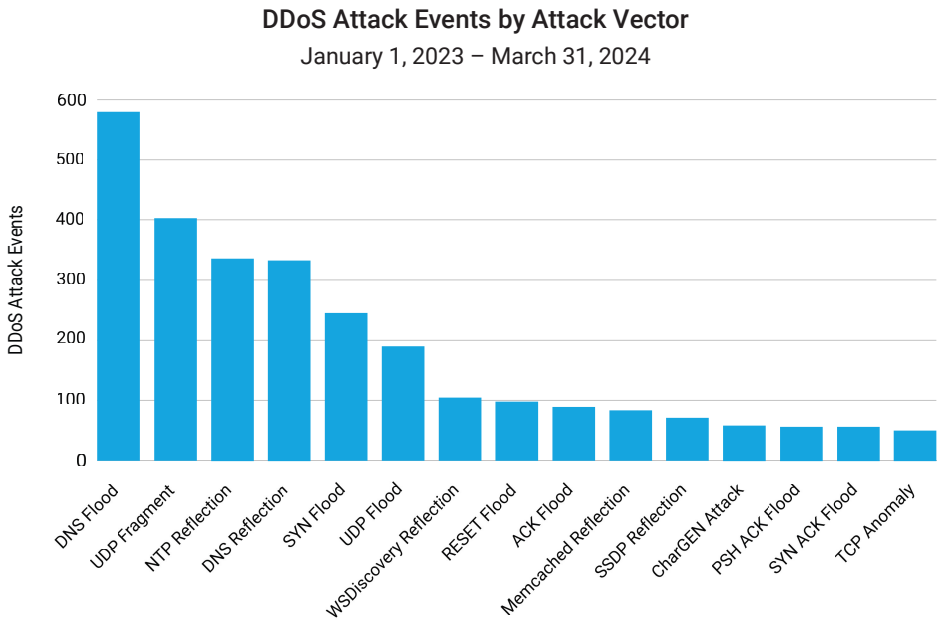


Fig. 5b: EMEA's DDoS attack types include DNS Flood, UDP Fragment, and NTP Reflection

Prolonged attacks hinder productivity and the ability of operations to preserve continuity when other threats are found and responsive action is needed. DDoS techniques involving longer-lasting attacks and the use of more DDoS attack vectors are effective strategies for attackers, allowing them to better achieve resource exhaustion and overwhelm businesses' network security teams.

The newly trending DDoS target: DNS

Of all the DDoS attack types, those targeting the Domain Name System (DNS) are among the most prevalent (Figure 6). DNS is a popular target for DDoS attacks because of the impact malicious traffic can have on this critical and foundational service. A successful DNS attack has the potential to literally erase a company's presence on the internet.

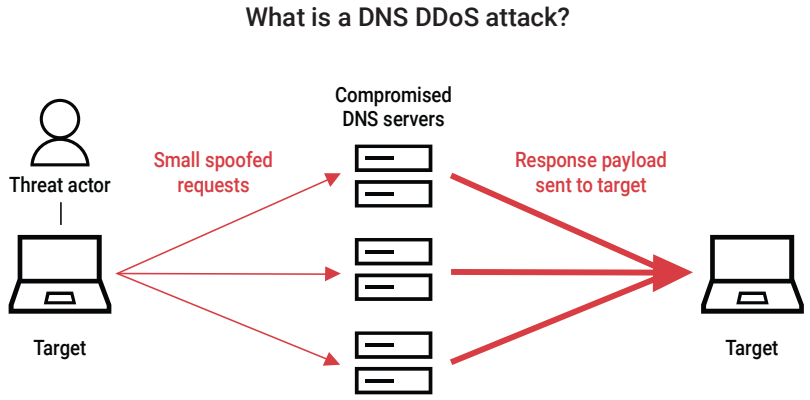


Fig. 6: A DNS DDoS attack compromises DNS servers with spoofed requests, causing an overwhelming response of payloads to the target

Specifically, the NXDOMAIN (nonexistent domain) attacks, also called Pseudo-Random Subdomain (PRSD) or DNS Water Torture attacks, have been observed flooding DNS infrastructure with requests for nonexistent domains. This type of attack aims to get to the origin name servers and cause high load on the systems — processing a request for a nonexistent domain is an involved task that consumes many processing cycles, ultimately exhausting the systems' ability to respond. We have seen many short attacks of this type, which typically are used to probe the victim's DNS infrastructure setup, only to return later with a refined attack in full force. According to research findings from our top 50 financial customers using Akamai Edge DNS, requests toward nonexistent domains made up almost 60% of their internet traffic in March 2024 (Figure 7).

Phishing Activity Trends Report

4th Quarter 2023

APWG

Unifying the
Global Response
To Cybercrime

Activity October-December 2023

Published 13 February 2024

Phishing Report Scope

The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org. APWG measures the evolution, proliferation, and propagation of identity theft methods by drawing from the research of our member companies and industry experts.

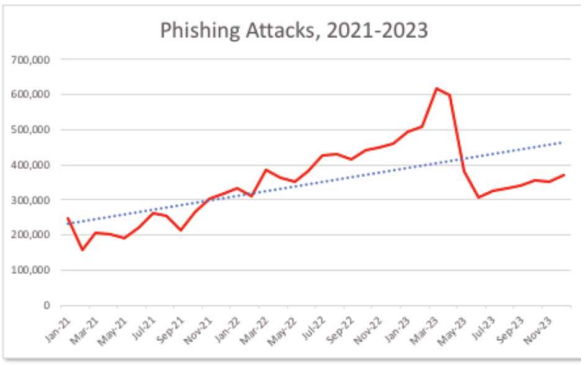
Phishing Defined

Phishing is a crime employing both *social engineering* and *technical subterfuge* to steal consumers' personal identity data and financial account credentials. Social engineering schemes prey on unwary victims by fooling them into believing they are dealing with a trusted, legitimate party, such as by using deceptive email addresses and email messages. These are designed to lead consumers to counterfeit Web sites that trick recipients into divulging financial data such as usernames and passwords. Technical subterfuge schemes plant malware onto computers to steal credentials directly, often using systems that intercept consumers' account usernames and passwords or misdirect consumers to counterfeit Web sites.

Table of Contents

Statistical Highlights	**3**
Most-Targeted Industry Sectors	**5**
Business Email Compromise	**6**
Free Webmail services used in BEC attacks	**8**
Registrars sponsoring BEC attack domains	**8**
APWG Phishing Trends Report Contributors	**9**
About the APWG	**9**

2023 Was Worst Year for Phishing on Record



Even after a dramatic decrease in the second quarter, phishing rose late in the year, and the APWG observed 1,077,501 phishing attacks in the fourth quarter of 2023

Phishing Activity Trends Summary

- The APWG observed 1,077,501 phishing attacks in the fourth quarter of 2023. APWG observed almost five million phishing attacks in 2023, the worst year for phishing on record. [pp. 3-4]
- Attacks against social media platforms exploded in late 2023, and were 42.8 percent of all phishing attacks. [p. 5]
- Phishing using phone calls — also known as voice phishing or "vishing" — is increasing every quarter. [pp. 5-6]
- The number of wire transfer BEC attacks in Q4 increased by 24% compared to the prior quarter. While the number of these attacks was up, the average dollar amount per attempt went down, to $56,195. [p. 6]

Statistical Highlights for the 4th Quarter 2023

APWG's contributing members study the ever-evolving nature and techniques of cybercrime. APWG has two sources of phishing data: phishing emails reported to it by APWG members and by members of the public, and phishing URLs reported by APWG members into the APWG eCrime eXchange.

The APWG tracks:

- **Unique phishing sites**.This is a primary measure of reported phishing across the globe. This is determined by the unique bases of phishing URLs found in phishing emails reported to APWG's repository. (A single phishing site may be advertised as thousands of customized URLs, all leading to basically the same destination.) Thus APWG measures reported phishing *sites*, which is a more relevant metric than URLs. A synonym for sites is *attacks*.
- **Unique phishing e-mails subjects**.This counts email lures that have different email subject lines. Some phishing campaigns may use the same subject line but advertise different phishing sites. This metric is a general measure of the variety of phishing attacks, and can be a rough proxy for the amount of phishing taking place.
- The APWG also counts the **number of brands attacked** by examining the phishing reports submitted into the APWG eCrime Exchange, and normalizing the spellings of brand names.

	October	November	December
Number of unique phishing Web sites (attacks) detected	356,538	350,776	370,187
Unique phishing email campaigns	22,750	24,621	20,642
Number of brands targeted by phishing campaigns	477	442	420

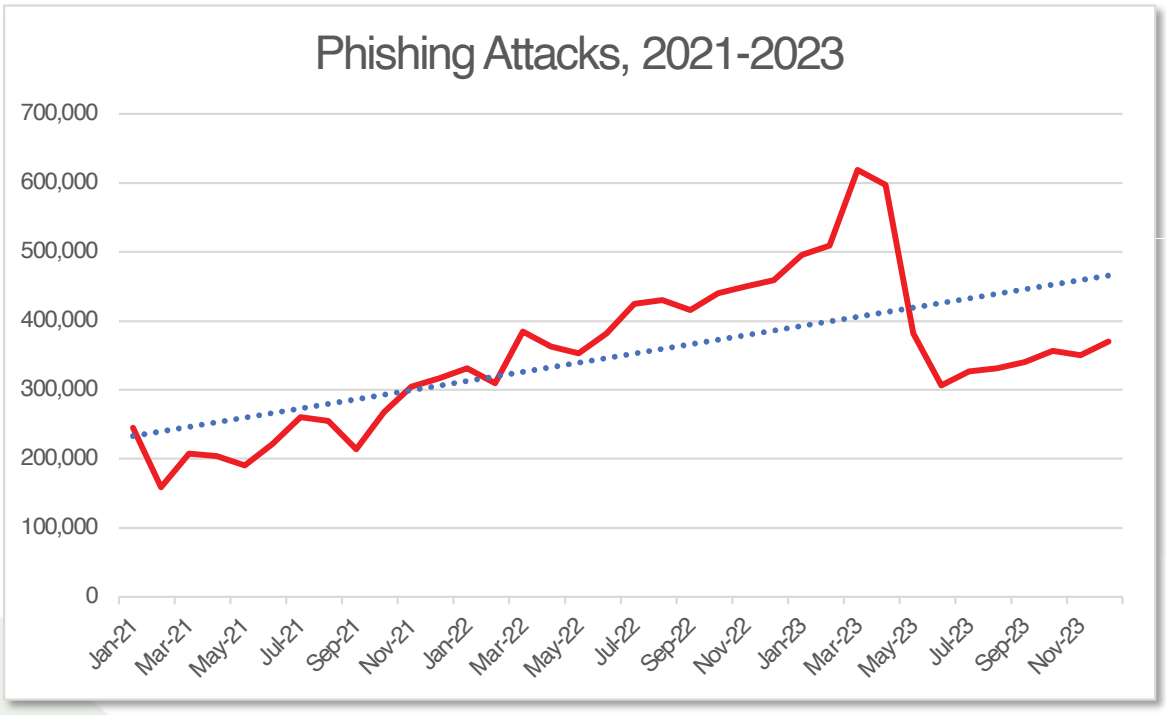
The APWG observed almost five million phishing attacks over the course of 2023 — 4,987,809 attacks in all. This made 2023 the worst year for phishing on record, ecliping the 4.7 million attacks seen in 2022.

In the fourth quarter of 2023, APWG observed 1,077,501 phishing attacks. This was up slightly from the 999,956 seen in Q3, but down from the 1,286,208 seen in Q2, and far below the 1,624,144 attacks seen in Q1 2023, which was the record high quarter in APWG's historical observations.

Phishing attacks fell in the second quarter of 2023 in part due to the shut-down of the Freenom free domain name program. Freenom offered free domain name registrations in five repurposed country top-

level domains (.TK, .ML, .GA, .CF, and .GQ), and this free service was used extensively by phishers for many years. In past years Freenom domains had been used for 14 percent of all phishing attacks worldwide, and Freenom was responsible for 60 percent of the phishing domains reported in all ccTLDs in November 2022. Freenom stopped offering free registrations in January 2023, and phishing in its ccTLDs died out as phishers used up their free domain inventories in mid-2023.[1] In February 2024, Freenom announced its complete exit from the domain name business, and that it had settled a lawsuit brought by Meta, which alleged that Freenom had ignored abuse complaints about phishing websites while monetizing traffic to those abusive domains.[2]

After the notable decrease in Q2 2023, phishing levels began creeping up again, and reached the levels observed in early 2022:



In Q4 2023, the number of unique email subjects (campaigns) received by the APWG dropped slightly from the previous quarter. The number of total email reports that APWG received was flat between Q3 and Q4.

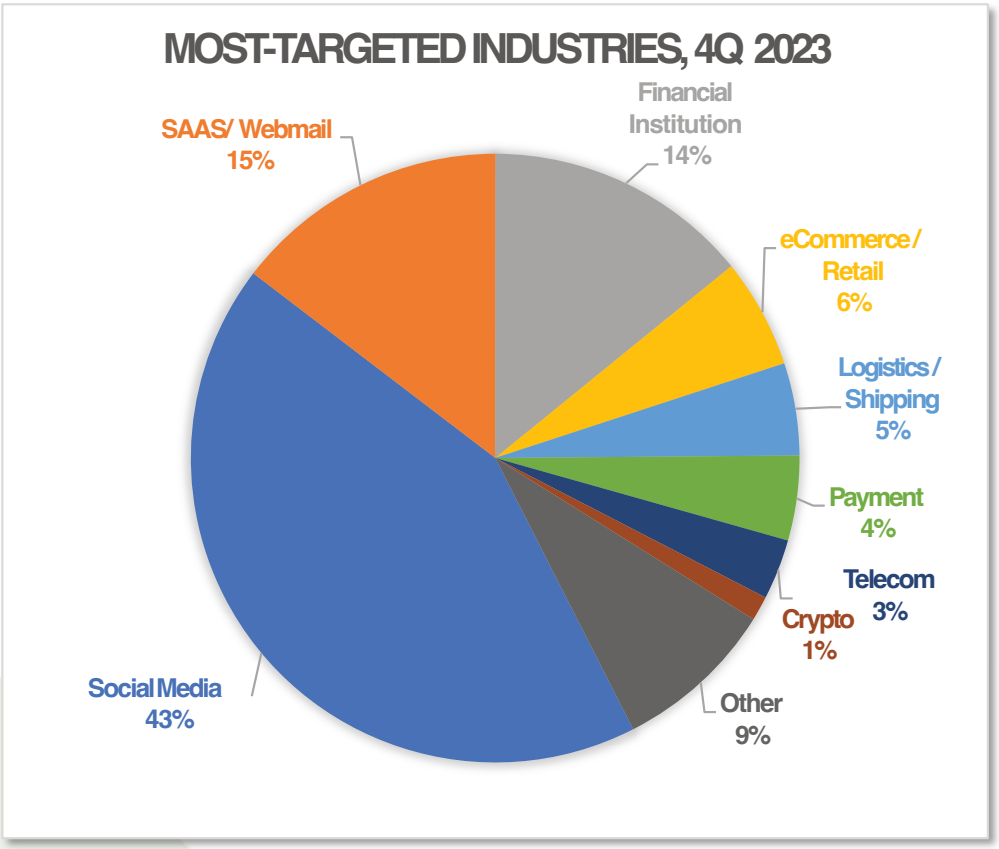
[1]For an in-depth look at the Freenom decrease, see "Phishing Landscape 2022" by Interisle Consulting and APWG members Greg Aaron and David Piscitello: https://www.interisle.net/PhishingLandscape2023.pdf
[2]https://www.freenom.com/en/freenom_pressstatement_02122024_v0100.pdf

Most-Targeted Industry Sectors – 4th Quarter 2023

In the fourth quarter of 2023, APWG founding member OpSec Security found that phishing attacks against social media platforms comprised 42.8 percent of all phishing attacks, exploding from 18.9 percent of all attacks in Q3. Phishing against the Financial Institution segment fell, from 24.9 percent of all attacks in Q3 to 14 percent in Q4. Attacks against online payment services were another 4 percent of all attacks.

"Continuing a trend we've previously observed, OpSec is tracking a strong increase in phone-based fraud, or voice phishing," said Matt Harris, Senior Product Manager, Fraud at OpSec. "Vishing incidents increased more than 16 percent over Q3, and represented a nearly 260 percent increase over the Q4 2022 volume."

OpSec Security offers world-class brand protection solutions.



Business e-Mail Compromise (BEC), 4th Quarter 2023

APWG member Fortra tracks the identity theft technique known as "business e-mail compromise" or BEC, which was responsible for $51 billion dollars in losses between October 2013 and December 2022 according to the FBI's Internet Crime Complaint Center (IC3). In a BEC attack, a threat actor impersonates an employee, vendor, or other trusted party in an email communication and attempts to trick an employee into sending money, privileged information, or some other asset. Fortra examined thousands of BEC attacks attempted during Q4 2023. Fortra protects organizations against phishing, BEC scams, and other advanced email threats.

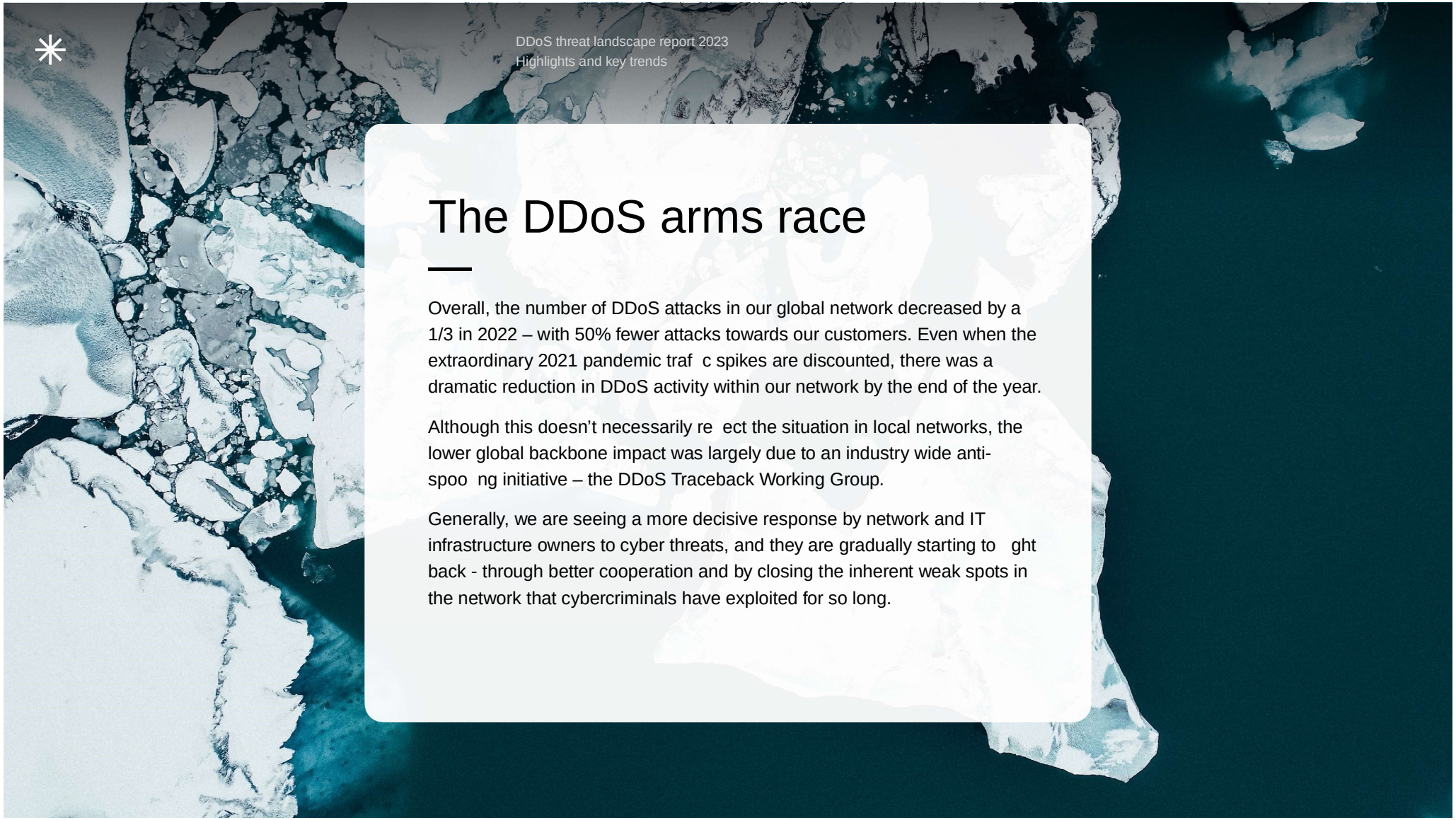
Fortra found that when criminals asked victims to send money by wire transfer, the average amount requested in Q4 2023 was $56,195, down 64 percent from Q3's average of $157,422. The number of wire-transfer BEC attacks in Q4 increased by 24 percent compared to the prior quarter. This suggests bad actors behind BEC wire transfer conducted more attacks but requested smaller amounts of money in each attack.

During the fourth quarter of 2023, gift card scams were the most popular scam type, and were 37.6 percent of all scams. At number two were advance fee fraud scams, at 30.6 percent. Payroll diversion remained a popular attack type, making up 9.2 percent of Forta's engagements.

Hybrid vishing is phishing in which the attacker uses both email and telephone to communicate with the victim. Fortra rarely saw hybrid vishing before 2023, but these made up 6.1 percent of the attacks Fortra recorded in the fourth quarter of 2023.

"The hybrid vishing attacks we track typically begin with an email, which tells the recipient that he or she has been charged for a product or service," said John Wilson, Senior Fellow, Threat Research at Fortra. "The messages instruct the recipient to call a phone number if they wish to cancel their order and obtain a refund. Geek Squad was the most common brand used as a lure in these attacks, accounting for 32.2 percent of the Q4 2023 attacks. This was followed by Norton/LifeLock with 30.4 percent, McAfee at 20 percent, and PayPal with 11.3 percent."


Key Internet backbone security trends
DDoS threat landscape report 2023
Arelion



The DDoS arms race

Overall, the number of DDoS attacks in our global network decreased by a 1/3 in 2022 – with 50% fewer attacks towards our customers. Even when the extraordinary 2021 pandemic traf c spikes are discounted, there was a dramatic reduction in DDoS activity within our network by the end of the year.

Although this doesn't necessarily re ect the situation in local networks, the lower global backbone impact was largely due to an industry wide anti-spoo ng initiative – the DDoS Traceback Working Group.

Generally, we are seeing a more decisive response by network and IT infrastructure owners to cyber threats, and they are gradually starting to ght back - through better cooperation and by closing the inherent weak spots in the network that cybercriminals have exploited for so long.

Attack distribution & intensity

The size of the largest attacks keeps growing. In 2022, peak attack traf c (Mpps) was up 19% from 2021. This trend is not only a re ection of overall Internet traf c growth, but also the continuing shift towards fewer, but more spectacular attacks.

> The average size of attacks experienced by our DDoS customers increased in 2022, both in terms of bits and packets.

Whilst there has been an increase in the number of large attacks, the vast majority of attacks are still small. These are mostly driven by free tier stress-test or DDoS-as-a-Service attacks instigated by amateur cybercriminals.

We saw the biggest increase in the 5-20 & 20-50 Gbps attack ranges, mainly as a result of DNS and NTP attacks, but also memcache due to its high ampli cation factor.

Network impact – peak attack size

The size of the largest attacks keeps growing. In 2022, peak attack traf c (Mpps) was up 19% from 2021.

This trend re ects overall Internet traf c growth and is also evidence that there is a continuing shift towards fewer, but more spectacular attacks.

Peak attack Gbps

813

Peak attack Mpps

854

Average attack size and duration

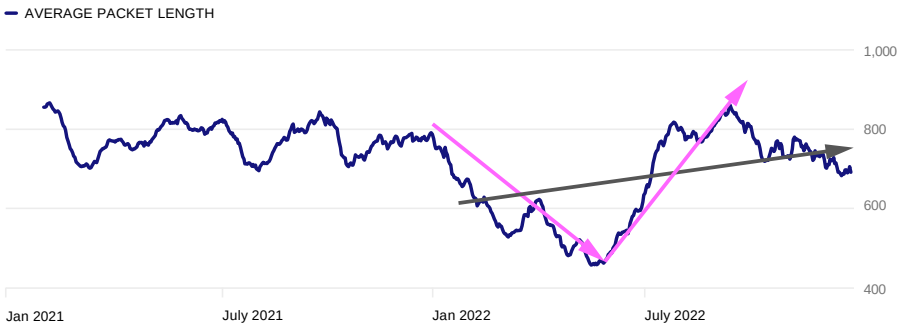
The average size of attacks experienced by our DDoS customers increased in 2022, both in terms of bits and packets. Packet intensity has uctuated throughout the year, but the general trend is upwards. The average duration of attacks has increased marginally since 2021. Looking at the bigger picture, the increase in average size is driven by a shift towards a greater number larger and fewer mid-sized attacks.

DDoS attack avg.
Duration +3%
11 min

DDoS attack average size +10%
11 [illegible]bps

DDoS attack average size +61%
6 Mpps

Attack average packet length per day

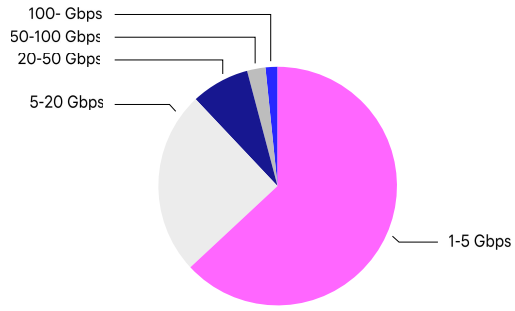


Overall size distribution

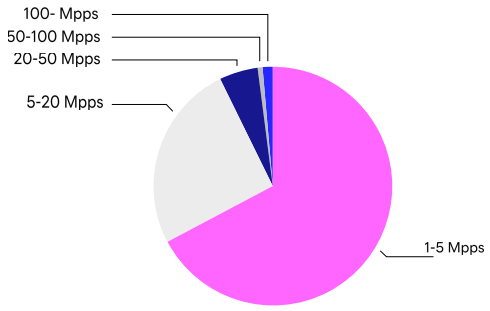
When looking at the overall size distribution of attacks in our backbone, we see that while there has been an increase in the number of large attacks, the vast majority of attacks are still small. These are mostly driven by free tier stress test or DDoS-as-a-Service attacks instigated by amateur cybercriminals. We saw the biggest increase in the 5-20 & 20-50 Gbps attack ranges.

This is because NTP and memcache attacks (the main DDoS drivers) have a much larger ampli cation factor and are more effective as a result (NTP 556x, memcache 10-51,000x and DNS 28-54x). All of this reinforces the need for a basic level of customer protection to mitigate the abundant smaller attacks, together with a solid insurance policy (a capable provider with effective DDoS protection services) for the larger ones.

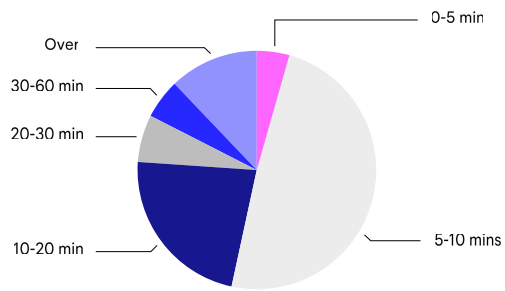
DDoS attack size Gbps



DDoS attack size Mpps



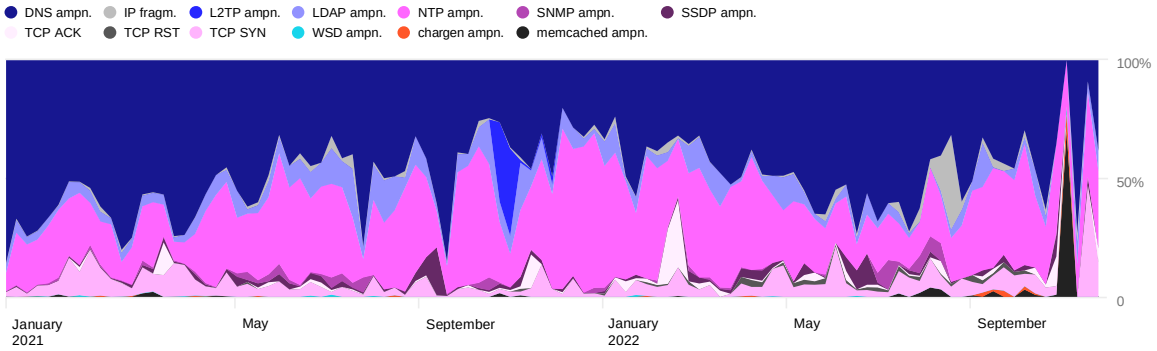
DDoS attack duration



Attack vectors towards our customers

There was a noticeable trend towards larger (bps) attacks targeting our customers at the end of the year. In terms of distribution, DNS & NTP are still the two most common attack vectors, with NTP decreasing slightly during the year. We also noticed a decline in UDP-based spoo ng attacks as servers are slowly being secured throughout the internet and are consequently used less frequently for such attacks. As a result, the underlying threat from re ection attacks is slowly but surely being reduced.

Alert types DDoS customer per week



Attack ampli cation

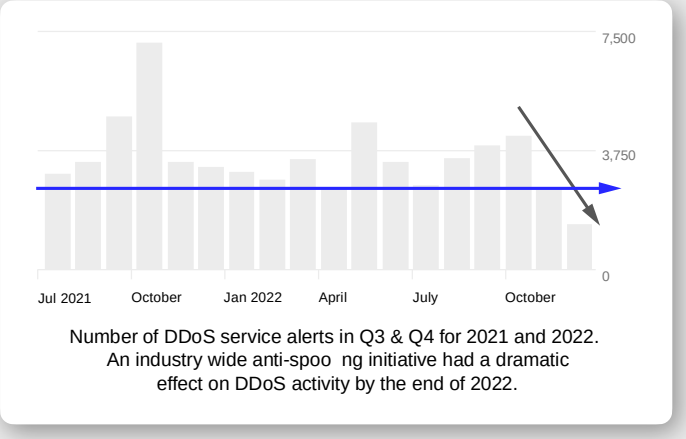
UDP-BASED PROTOCOL	SCALING MULTIPLE
DNS	28-54 x
NTP	556 x
SNMP	6.3 x
CharGEN	358 x
Memcached	10,000 - 51,000 x

Because of the effectiveness of a high ampli cation factor, our customers are still facing a signi cant threat from memcache.

Monthly attack distribution

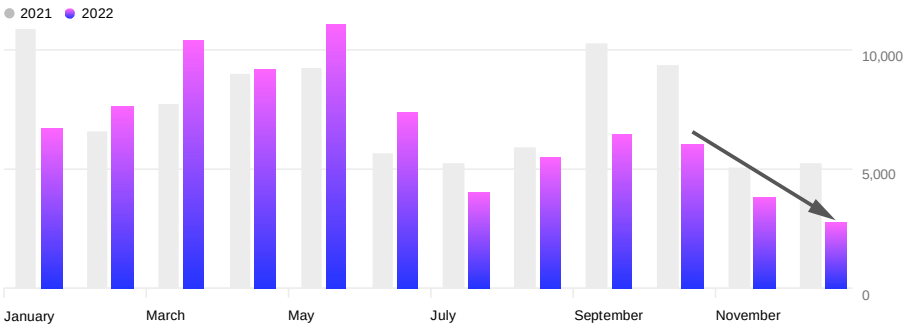
The number of DDoS attacks in our global network decreased by a 1/3 in 2022, with 50% fewer attacks towards our customers. However, it is worth noting that we observed an exceptionally high amount of pandemic-related DDoS activity during Q1 & Q2 2021, but activity in Q3 & Q4 for both 2021 and 2022 were comparable.

There was a dramatic reduction in DDoS activity within our network during the nal months of the year. This was largely due to an industry wide anti-spoo ng initiative – the DDoS Traceback Working Group – between backbone providers (see the following pages).

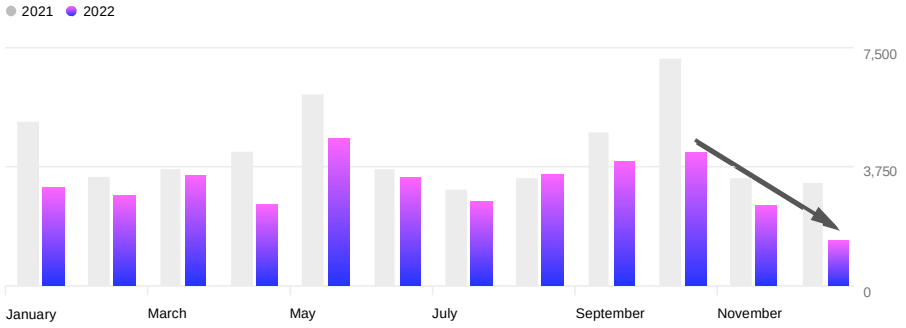


Number of DDoS service alerts in Q3 & Q4 for 2021 and 2022. An industry wide anti-spoo ng initiative had a dramatic effect on DDoS activity by the end of 2022.

All alert



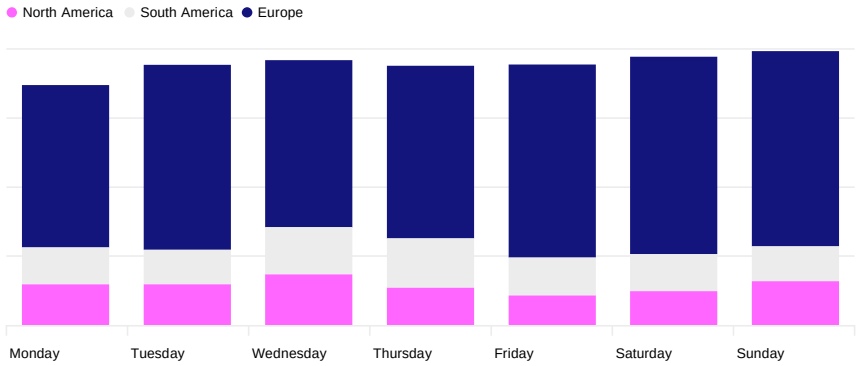
DDoS service alert



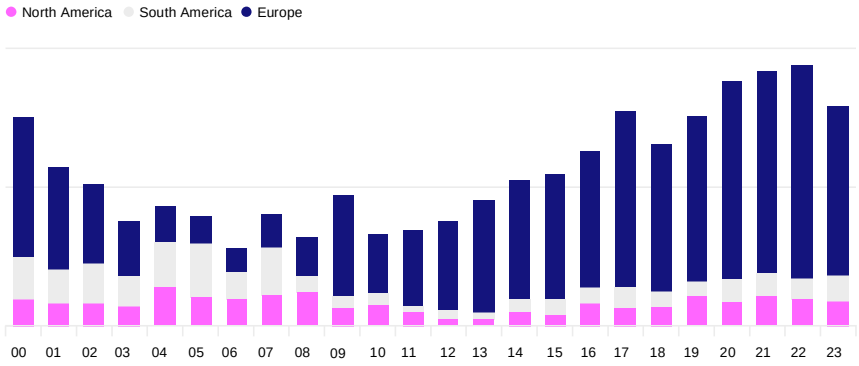
DDoS day-to-day

Attacks continue to follow the sun and DDoS doesn't take the weekend off – they are a constant threat every day of the week.

DDoS customer continent weekday



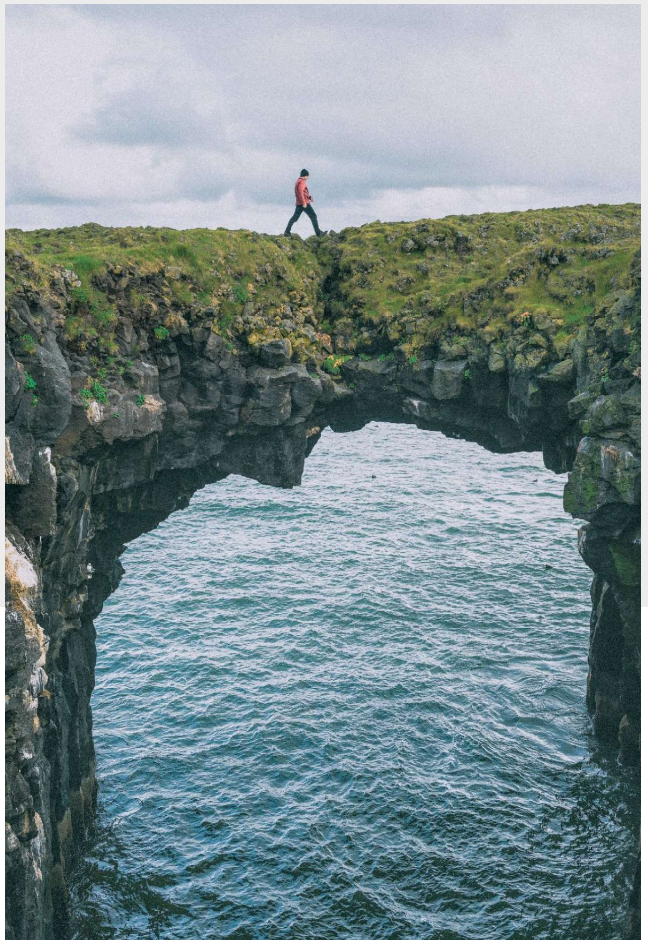
DDoS customer continent hour CET



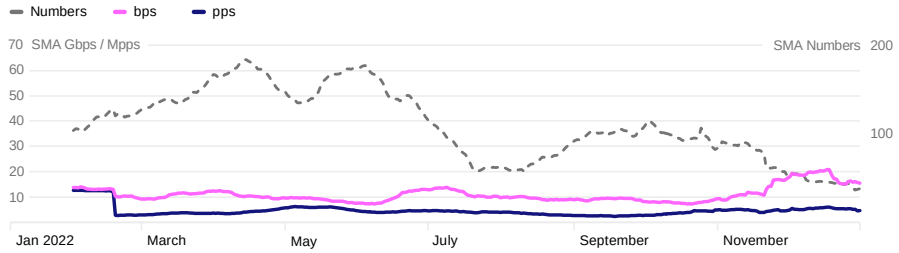
Could DDoS Traceback be a game changer?

During 2022, we started working together with a number of other major backbone networks in the DDoS Traceback Working Group, an initiative to actively track spoo ng-friendly networks, and by encouraging customers to implement anti-spoo ng mechanisms and/or shutdown bad client networks. Spoo ng is a key component of the ampli cation/re ection attacks that we've seen in recent years. This work proved to be effective and has made it much more dif cult for the DDoS attack providers (Stresser/Booter services) to operate.

While this has resulted in a drop in the overall number of attacks, we are seeing an increase in direct-path attacks from botnets, – albeit it to a lesser extent. These are more expensive to purchase since bots are a valuable asset for cyber criminals and if exposed, they risk being shut down when used extensively. Also, proxies are being used more – as a smoke screen to protect the bots from being exposed.



Attack size (all) per day, simple moving avg. 28 days (>1 Gbps, >1 Mpps)




Key backbone security trends
DDoS threat landscape report 2024
Arelion

The big attacks just get bigger

Peak attacks continue to grow

—

Peak attacks reached 960Gbps in 2023. This demonstrates the continued importance of volumetric protection.

Attacks of this size are enough to bring down many larger networks, let alone an on-prem device, which even if mitigated, would most likely break the network it is attached to.

Global decrease in large volumetric DDoS attacks

—

Although we've seen a global decrease in large volumetric DDoS attacks of late, we've also noticed an increase in these locally – on a national level. This we think is the combination of many factors.

Large amplification attacks are now harder to carry out successfully, especially in view of recent cooperation across our industry. Enabling anti-spoof ing filters has forced the attacker to use a "direct-path" when exploiting their botnets. This limitation makes detection easier and these attacks much more vulnerable to take-down initiatives. As a result, cyber criminals need to be more careful and choose wisely when using attack resources.

Overall decline in packets-per-second

—

It seems that hackers are increasingly working "smarter not harder". As DNS amplification has improved, fewer packets-per-second are needed for an effective attack, which is one less thing that could trip the existing defences of an organization.

Attack duration is down

—

But this doesn't mean attacks are less serious. Larger, more intensive attacks over slightly shorter periods ultimately cause the same damage overall. From the data we've observed, it appears that average duration is being dragged down by unsuccessful attacks being called off quicker, and the resources reassigned to alternate, unprotected targets. This reaffirms the notion that some DDoS protection is definitely much better than none at all.

The DDoSnetwork impact: peak attack traf c

The largest volumetric attack in 2023 peaked at 960 Gbps (up 18% from 2022). This came from a UDP-based attack in Europe.

At 343 Mpps, the largest pps attack came from a multi-vector TCP SYN, SSDP Ampli cation attack in North America.

Largest volumetric attack

Peak size

+18%

Peak attack Gbps

960

Peak attack Mpps

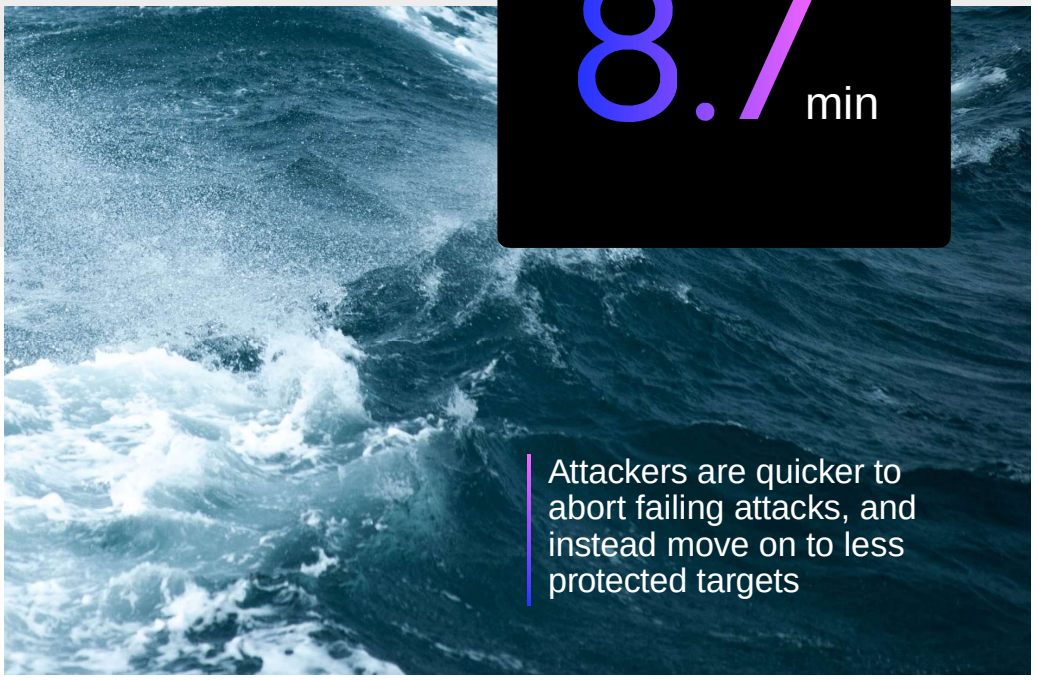
343

Average attack size and duration

Attack duration is down, but this doesn't mean attacks are less serious. Larger, more intensive attacks over slightly shorter periods ultimately cause the same damage overall.

From the data we've observed, it appears that average duration is being dragged down by unsuccessful attacks being called off quicker, and the resources reassigned to alternate, unprotected targets.

DDoS attack avg. ↘
Duration -12%
8.7 min



Attackers are quicker to abort failing attacks, and instead move on to less protected targets

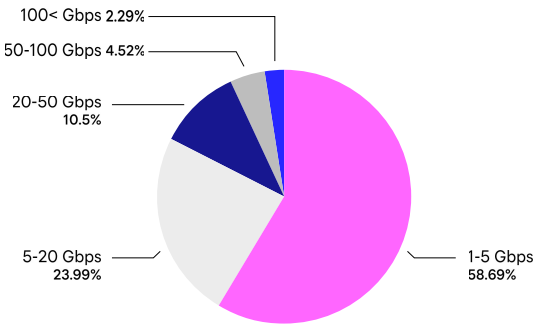
DDoS attack average size (2Y) ↗ +6%
11.7 Gbps

DDoS attack average size (2Y) -16%
5 Mpps

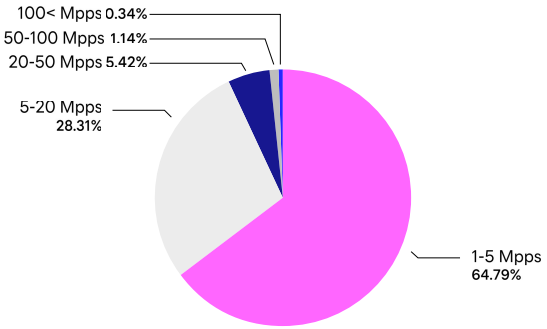
Attack size distribution

Generally, attack size distribution in 2023 was fairly similar to that in 2022. The vast majority of attacks are still small and mostly driven by free-tier stress test or DDoS-as-a-Service attacks instigated by amateur cybercriminals.

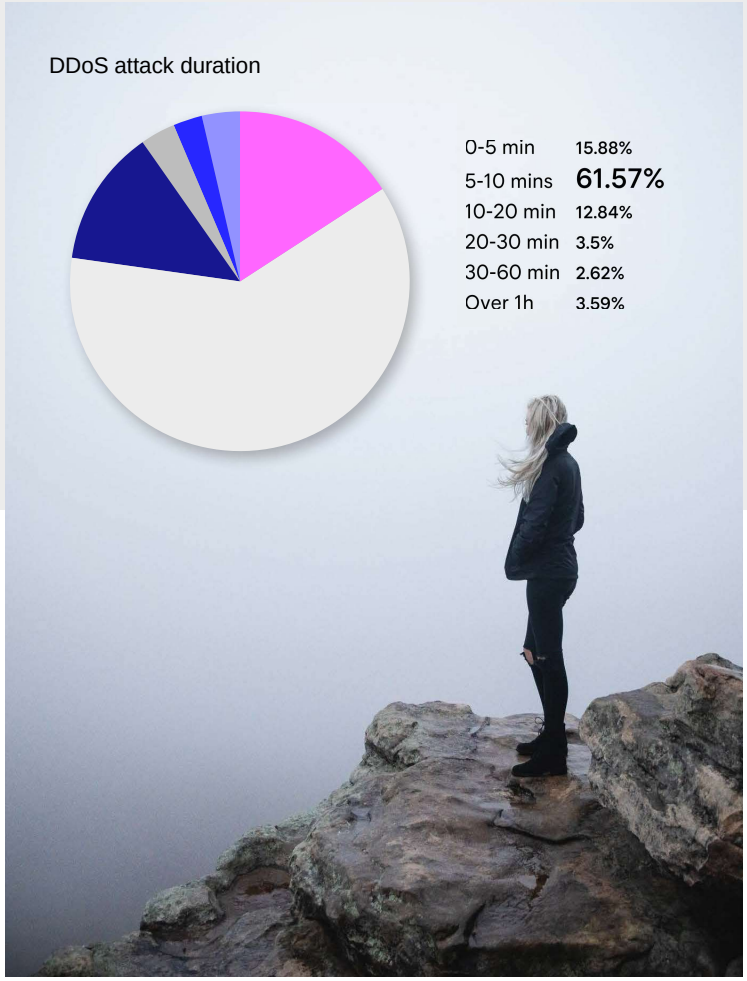
DDoS attack size Gbps



DDoS attack size Mpps



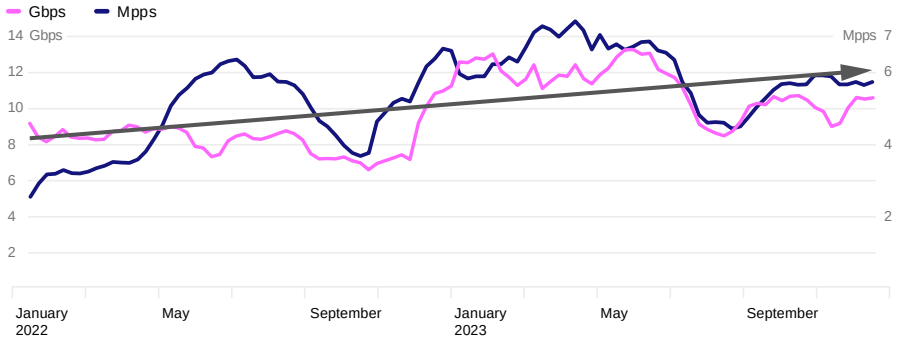
DDoS attack duration



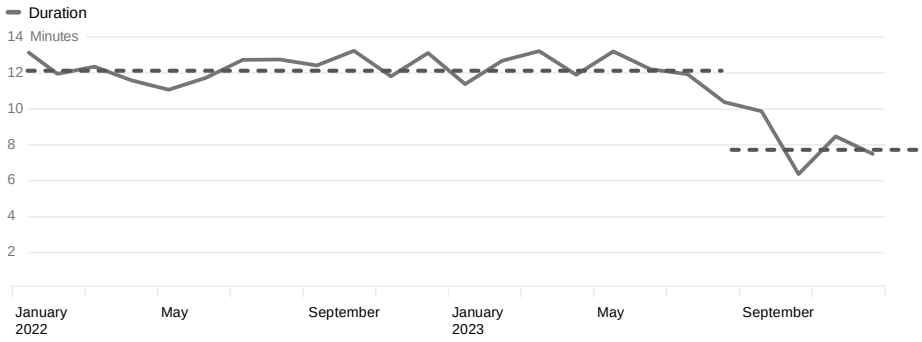
Attack strength and duration over time

Year-on year, attack strength (in terms of both Gbps and Mpps) is increasing. This is predominantly driven by DNS ampli cation attacks. Average attack duration fell from a consistent level towards the end of 2023 – largely as a consequence of the increase in DNS ampli cation.

Average DDoS attack size Gbps and Mpps



Average DDoS attack duration



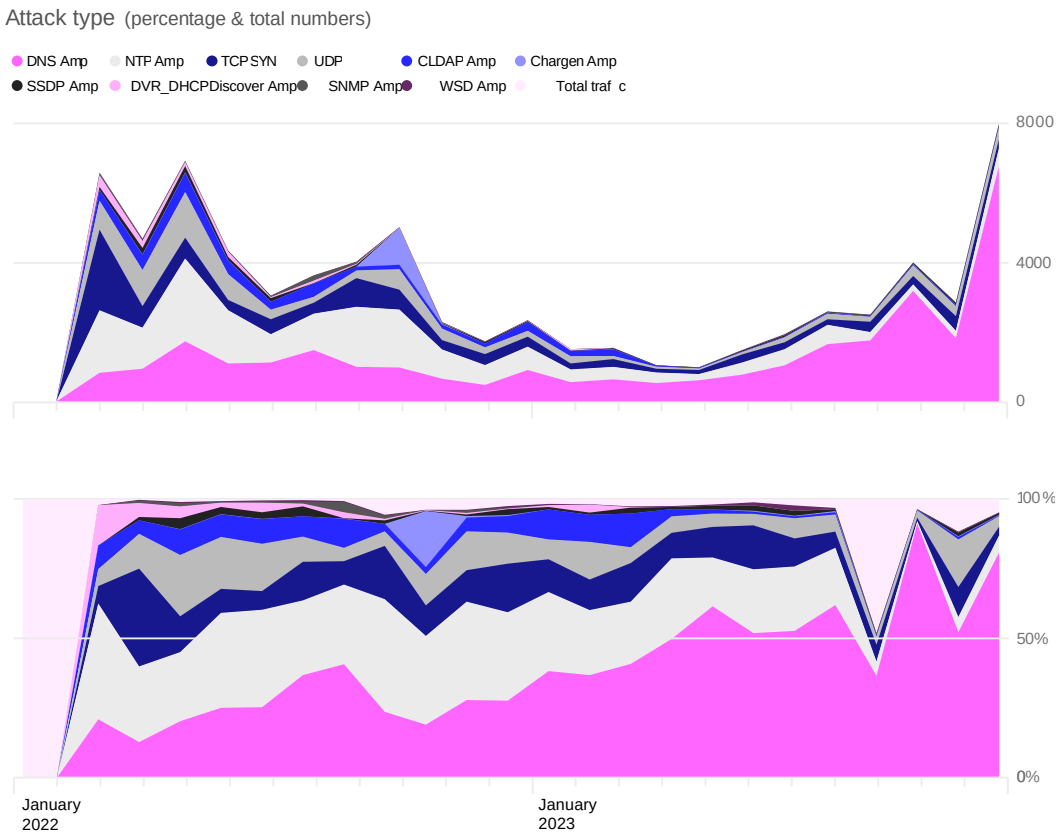
How our DDoS customers are being attacked

Following steady growth over the past four years, DNS Ampli cation was the most common type of attack in 2023, and by the end of the year, it constituted 80% of all attacks.

The most common attack vector in 2023 was UDP over HTTP (port 80) and HTTPS (port 443). The increasing popularity of the QUIC protocol makes it an easy target for ampli cation attacks, posing a greater challenge to defend against than attacks using TCP as the data transport layer.

Attackers are now mainly exploiting compromised or acquired virtual machines (VMs) and virtual private servers (VPS). Unlike compromised IoT device botnets, virtual servers offer more bandwidth and computational resources.

Additionally, there is a rising trend in bulletproof hosting over the past two years.



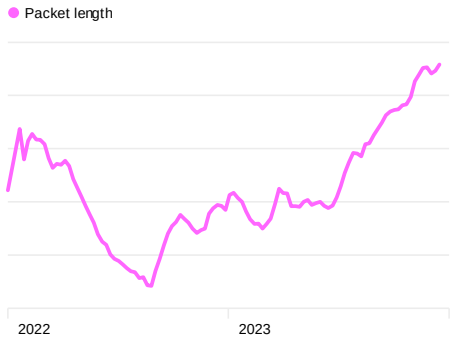
Average packet length and ampli cation

With improved DNS ampli cation, attackers are achieving larger and more effective responses with the re ection packet. There is a growing trend towards more multi-vector ampli cation attacks, where different re ection UDP services are combined within the same attack.

> Attackers are constantly evolving their tactics - often changing their vectors mid-attack

The cat-and-mouse game continues, and attacks continue to evolve with advanced DDoS vectors such as TCP/Syn in combination with mixed UDP ampli cation. We've also observed attackers adapting and changing vectors more frequently, even during ongoing attacks.

Attack average packet length



DNS AMP attack average packet length