



The State of Ransomware

2024 ANNUAL REPORT





Since 2020, **BlackFog’s State of Ransomware blog** has tracked public ransomware attacks, earning recognition from major news outlets. In 2023, we expanded our research to **undisclosed attacks** on data leak sites and the dark web. This **2024 Annual Report** analyzes rising threats, key trends, and actionable insights to strengthen cybersecurity defenses.”



Contents

1	Introduction	PAGE 3
2	2024 In Review	PAGE 4
3	Top 5 Ransomware Attacks	PAGE 7
4	Variants	PAGE 9
5	Industry	PAGE 14
6	Geography	PAGE 17
7	Critical Infrastructure	PAGE 19
8	Data Exfiltration	PAGE 21
9	2025 Predictions from Dr. Darren Williams	PAGE 23
10	How to Prevent a Ransomware Attack	PAGE 25
11	About BlackFog	PAGE 27
12	Methodology	PAGE 28

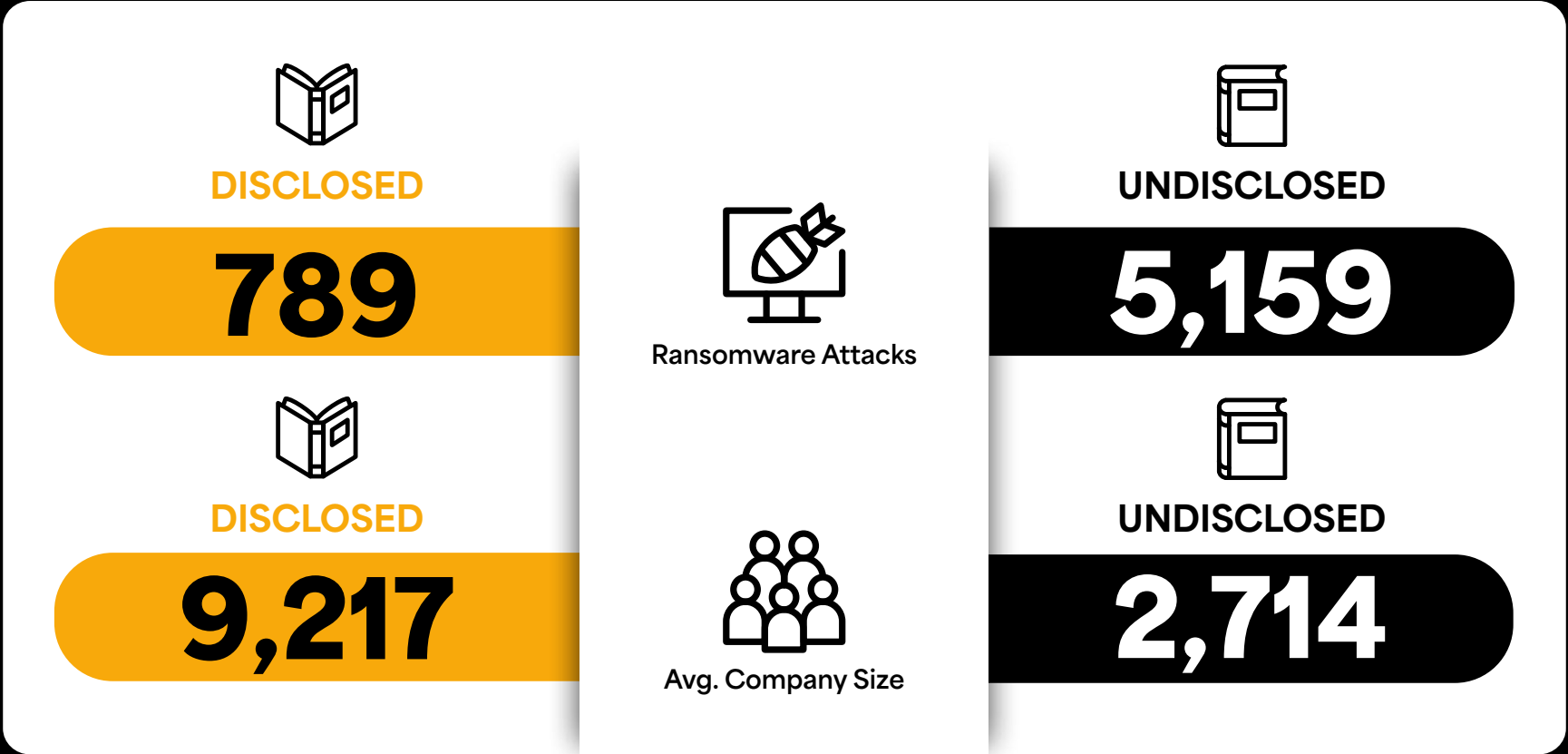
1

Introduction

Since 2020 BlackFog has been tracking and documenting publicly disclosed ransomware attacks in its award-winning State of Ransomware blog.

A trusted resource cited by news publications such as Associated Press, Yahoo, Forbes and Dark Reading to name a few, BlackFog also publishes a quarterly Ransomware Trend Report which is sent to thousands of subscribers globally. In 2023, we expanded the report to include undisclosed ransomware attacks listed on data leak sites and the dark web, enabling us to provide a more detailed picture of the ransomware landscape as a whole.

In this, our 2024 annual report, we delve into the alarming rise and severity of ransomware threats. The report not only highlights the key findings from 2024 but also compares them to previous years, revealing significant cybersecurity trends. Most importantly, it offers practical recommendations for organizations to enhance their defenses and better protect themselves against these evolving threats.



2

2024: A Record Breaking Year for Ransomware

2024 proved to be a landmark year for ransomware, with 789 disclosed attacks and 5,159 undisclosed attacks, reflecting year-over-year increases of 25% and 26%, respectively. The year began with a record breaking January, which saw 76 attacks, an eye-opening 130% rise compared to January 2023. This upward trend continued throughout the year, with seven months showing significant increases in disclosed attacks compared to the previous year.



94% of disclosed attacks use **Data Exfiltration**

The avg. **Data Exfiltration** per attack is **592GB** (undisclosed).

DID YOU KNOW?

November marked the peak of both disclosed and undisclosed attacks, contributing substantially to Q4's strong performance. In fact, Q4 accounted for 33% of all undisclosed attacks and 29% of disclosed attacks for the year.

LockBit remained the most active ransomware variant, while RansomHub, a newcomer to the scene in February 2024, secured second place. We'll dive deeper into the various ransomware variants later in the report.

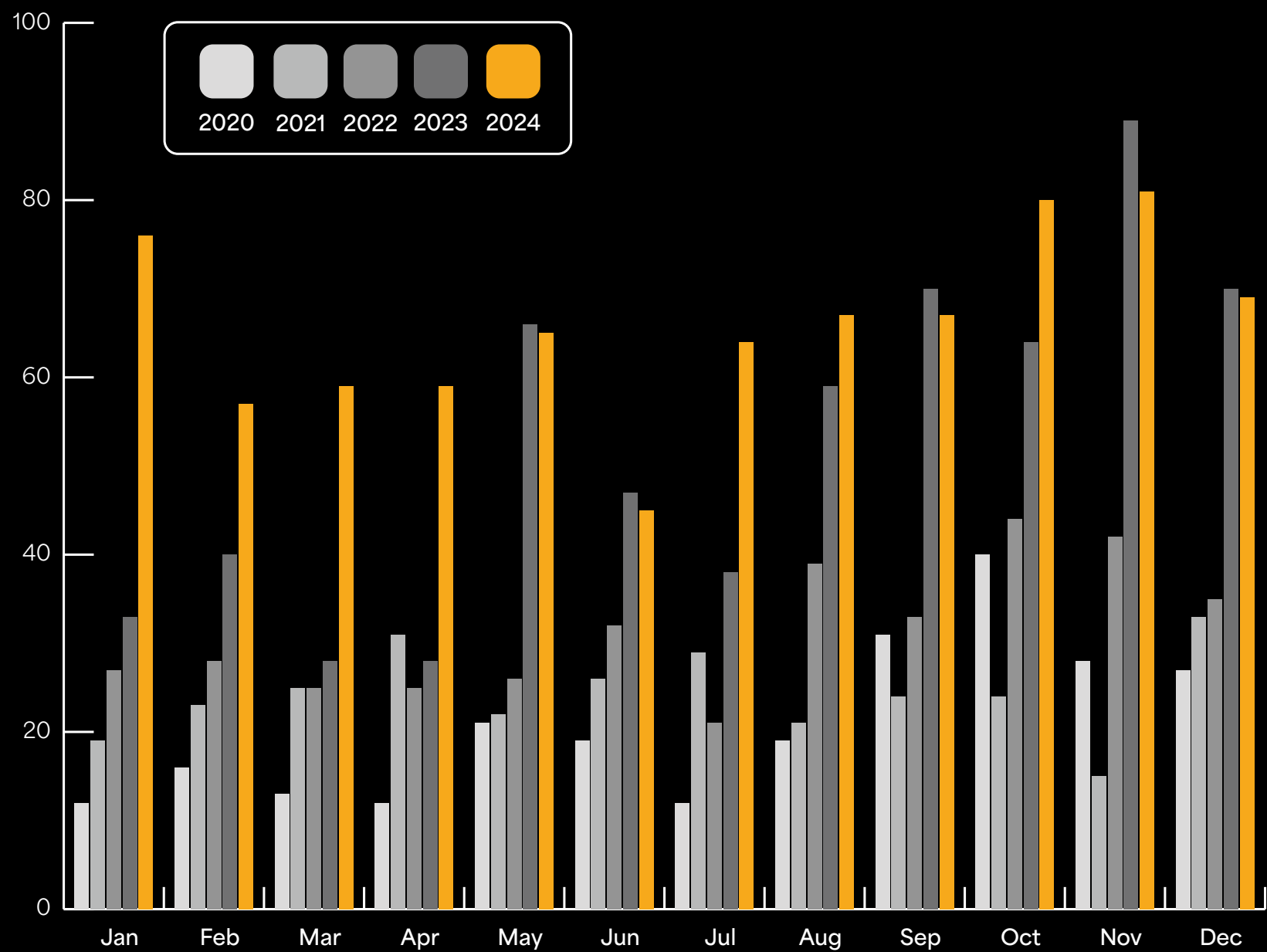
When it comes to targeted industries, a stark contrast emerged between publicly disclosed attacks and those that remained under the radar. Healthcare, government, and education were among the top

targets in the headlines, while the manufacturing, services, and technology sectors bore the brunt of the attacks that flew under the radar.

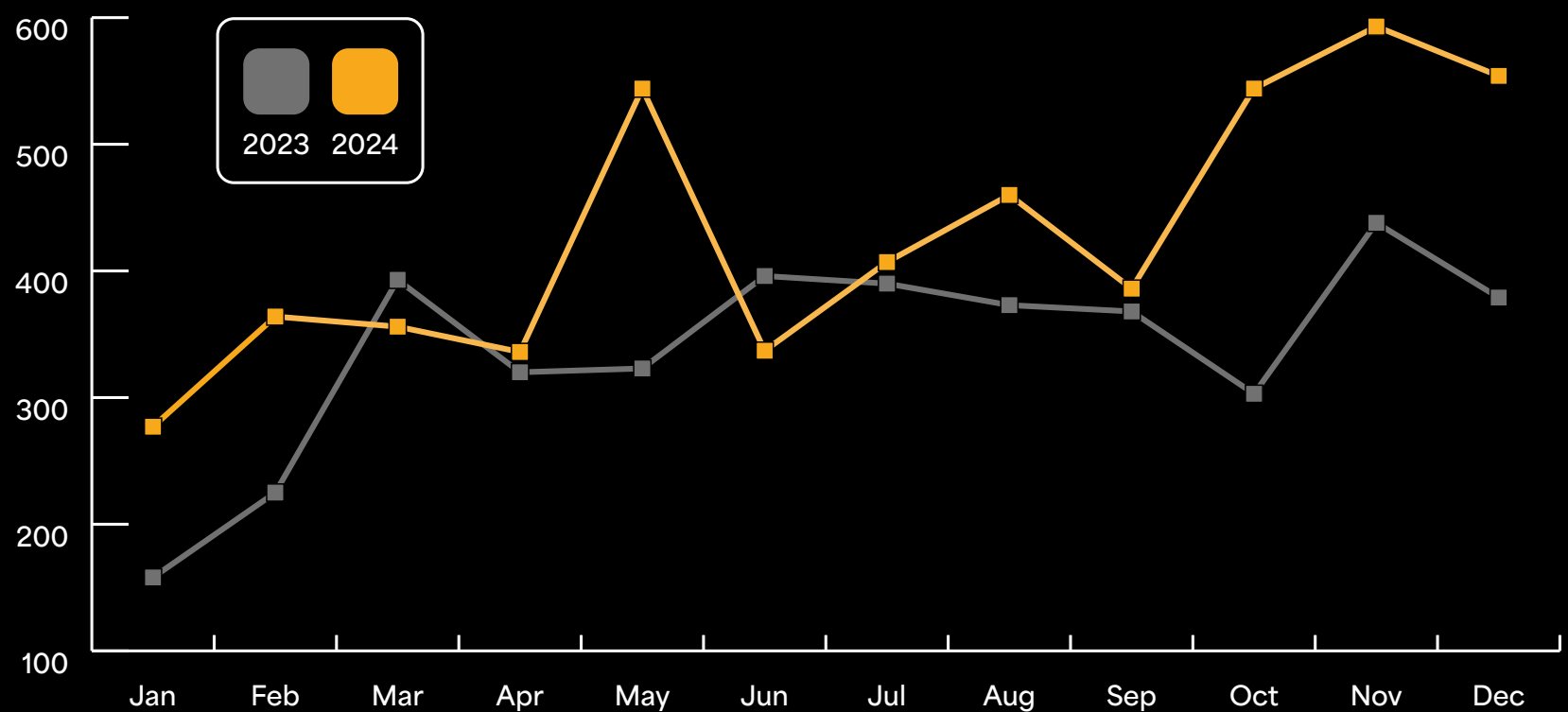
In 2024, PowerShell emerged as a significant tool in ransomware incidents, being utilized in 56% of all cases. This trend highlights a concerning tactic among attackers: leveraging legitimate tools and platforms to infiltrate networks, establish a presence, and exfiltrate data without triggering alarms from many endpoint protection platforms.

Notably, the level of data exfiltration surged to 94%, the highest we have ever recorded, providing evidence of the move from traditional encryption only tactics to extortion.

Disclosed ransomware attacks by month, 2020-2024



Undisclosed ransomware attacks by month, 2023 & 2024



3

Top 5 Ransomware Attacks of 2024

Ransomware headlines were filled with reports of major attacks, many of which caused lasting damage and disruption to the affected organizations. By tracking ransomware attacks, both disclosed and undisclosed, we are subject matter experts on this topic and have shortlisted the top 5 ransomware attacks of 2024:



Change Healthcare Ransomware Attack

On February 21, 2024, [BlackCat/ALPHV](#) launched a massive ransomware attack on [Change Healthcare](#), a division of UnitedHealth Group, affecting over 100 million people. This incident became the [largest healthcare breach](#) in American history to date.

The attackers initially gained access by exploiting a Citrix portal account that didn't have multi-factor authentication. Once inside, they spent nine days moving around undetected and stealing data before unleashing ransomware. This attack disrupted over one hundred applications across various healthcare services.

Even though UnitedHealth Group [paid a \\$22 million ransom](#) in cryptocurrency to try to resolve the situation, things got worse when the RansomHub group attempted another extortion. The overall financial impact was huge, with direct damages totalling over \$800 million and costs expected to [surpass](#) \$2.457 billion.



CDK Global Ransomware Attack

In June 2024, the [BlackSuit ransomware group](#) hit CDK Global, a well-established software provider for auto dealers with a serious attack. This caused disruptions for thousands of dealerships across North America, showing just how damaging ransomware can be to large-scale operations and important supply chains.

The attackers demanded 387 Bitcoin, which was about \$25 million [at the time](#), but the funds were never recovered. The collective losses for the affected dealerships were estimated to be around \$1 billion, making this one of the [most expensive](#) ransomware attacks of the year.



Kawasaki Motors Europe Attack

In September 2024, the [RansomHub ransomware group](#) leaked 487 gigabytes of data allegedly stolen from Kawasaki Motors Europe (KME). Kawasaki [initially disclosed](#) the attack themselves, claiming it had not been successful.

However, despite Kawasaki's preventive measures, including temporarily isolating servers and initiating a "cleansing process," RansomHub went ahead with the [data release](#). The leaked information included business documents, financial information, banking records, dealership details, and internal communications.

Exposed files were organized in directories titled "Dealer Lists," "Financing Kawasaki," "COVID," and "Trading Terms," with timestamps showing activity as recent as early September.



Starbucks Supply Chain Disruption

In late November 2024, Starbucks faced disruption when its third-party vendor, Blue Yonder, became the target of a [ransomware attack](#). The incident, attributed to the [Termite ransomware group](#) on December 9, 2024, severely impacted the company's internal systems, particularly those responsible for employee scheduling and payroll across 11,000+ stores in North America.

The attack left Starbucks' digital processes for managing staff schedules and payroll completely nonfunctional, forcing store managers to temporarily switch to manual processes. Shift planning and tracking work hours had to be done the old-fashioned way—pen and paper became the tools of the moment.

In response, Starbucks provided clear guidance to store leaders and managers on how to navigate the manual systems to ensure employees were paid accurately and on time. These interim solutions were key in keeping operations running and supporting staff during the recovery phase.

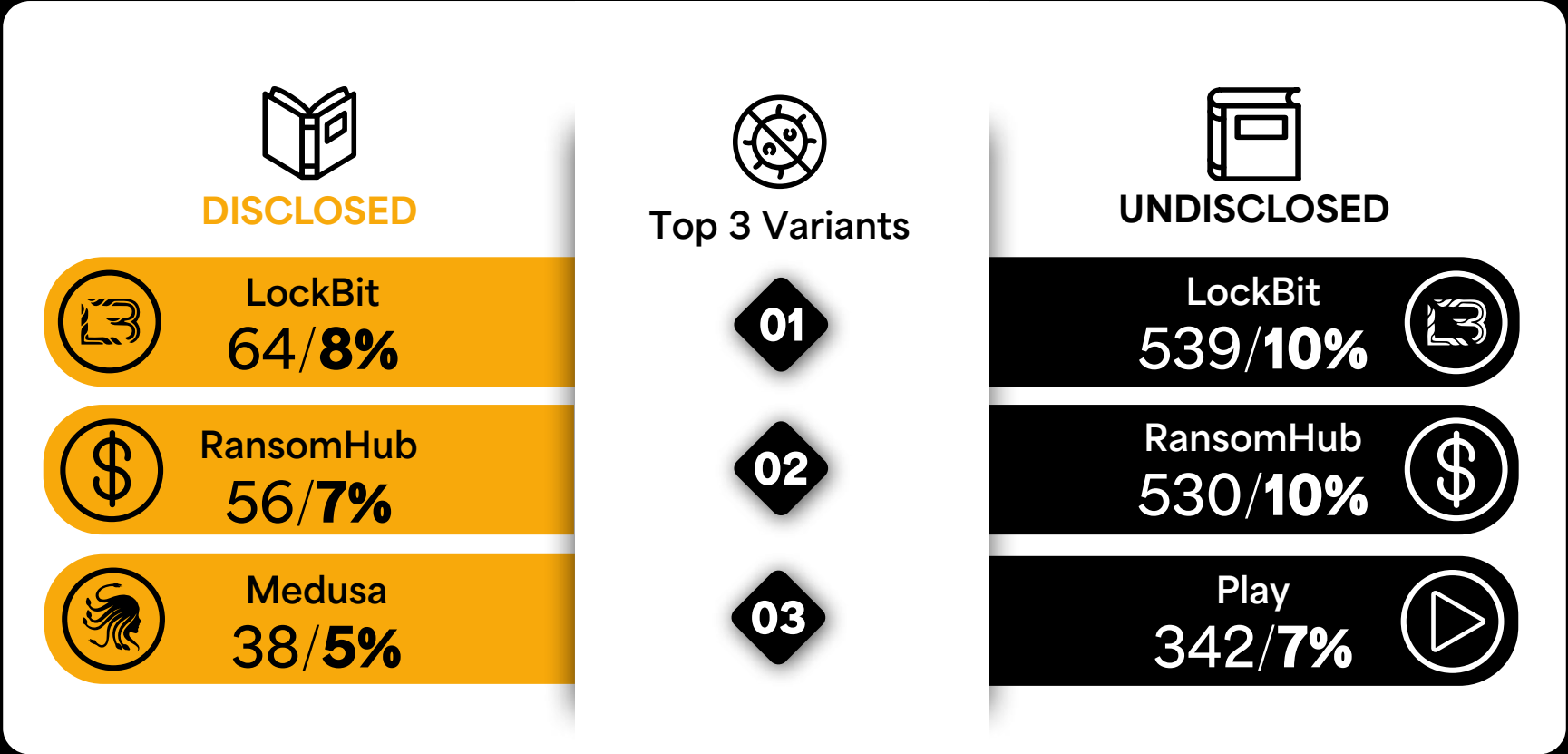


NHS London Ransomware Attack

In June 2024, the Qilin ransomware group [targeted NHS London](#), compromising the data of nearly one million National Healthcare System (NHS) patients. The attack severely impacted major London hospitals, including King's College Hospital, Guy's and St Thomas, the Royal Brompton, and Evelina London Children's Hospital.

The incident led to the cancellation of over eight hundred planned operations and seven hundred outpatient appointments in the first week alone. The attackers exploited vulnerabilities in [Synnovis](#), an NHS supply chain provider of laboratory services.

They not only encrypted vital information but also stole [sensitive patient data](#), including details about individuals with cancer and sexually transmitted diseases. The attack caused disruptions to blood transfusions and test results, forcing staff to resort to paper-based methods and slowing down operations considerably.



4

Smaller Players Also Made a Big Impact: Variants in 2024

While several well-established ransomware gangs have been causing significant disruptions for years, 2024 marked the rise of new variants, with [48 emerging](#) over the past 12 months. Not all of these variants made headlines, but their impact was certainly felt by their victims.

Focusing on the top three variants, LockBit and RansomHub were dominant, affecting 603 and 586 victims respectively across both disclosed and undisclosed attacks.

In third place, the leading players varied by category: Medusa accounted for 5% of disclosed incidents, while Play made up 7% of undisclosed ones.

Let's take a closer look at these gangs and some of their victims:



LockBit

In 2024, we closely [tracked LockBit's](#) attacks, given its notoriety as one of the most prominent ransomware gangs in recent years.

LockBit's attacks spanned several industries, though healthcare, education, and manufacturing appeared to be frequent targets in reported incidents. However, some high-profile attacks occurred outside these favored sectors, including:

[London Drugs](#): A cyberattack targeting the retailer led to the closing of 80 stores in late April. The company acknowledged that corporate head office files, some of which may have included employee information, was compromised during the incident. LockBit claimed the attack and demanded a massive \$25million ransom. Although the company maintained that it was not paying the ransom demand, the post relating to the attack disappeared from LockBit's dark web site, leading some to believe that London Drugs may have negotiated and made some sort of ransom payment.

[Clay County](#): Filed a Local Disaster Declaration following a "significant" LockBit ransomware attack in July. The county was unable to provide critical services required for the daily operation of all offices of the Clay County Courthouse, Community Corrections and County Probation. The government website was also down as a result of the attack. The ransomware group claimed to have stolen 3TB of data and posted six screenshots as proof of claims.

May was LockBit's busiest month, launching nearly 200 attacks, which accounted for 36% of all attacks that month. This surge followed news of the gang's disbandment after its leader was unmasked earlier in the year.



RansomHub

This is probably one of the most concerning gangs in the ransomware landscape currently, consistently making waves since its emergence in February.

While many of its attacks remain undisclosed, the group's influence in its debut year has been widely recognized within the cybersecurity community.

RansomHub made headlines with high-profile attacks on government entities such as the [Jędrzejów District](#) in Poland, the [Government of Mexico](#), and several municipalities across the USA, reinforcing its reputation as a serious threat to critical infrastructure.

The group also made its mark in the global manufacturing sector, claiming 78 victims including major players like [Kawasaki Motors](#) and Polaris.

Although these industries have been heavily targeted, RansomHub can't be pigeonholed when it comes to targeting specific sectors or company sizes. With its victims range from SMEs to large global corporations, this newcomer poses a significant threat to all organizations.



Medusa

Medusa’s dark web posts give us a bit of insight into this ransomware group with ransom demands appearing on the majority of claims. In 2024, ransom demands by the group exceeded \$40M, with over 26% of their disclosed attacks demanding a ransom of over \$1million.

This financially motivated gang made headlines during the year targeting organizations such as [Summit Pathology](#), an incident that impacted over 1.8million individuals, [Henry County](#) which suffered wide-ranging disruption to crucial services, and the [Kansas City Area Transportation Authority](#) which rendered its call centers across the state unavailable.



Play

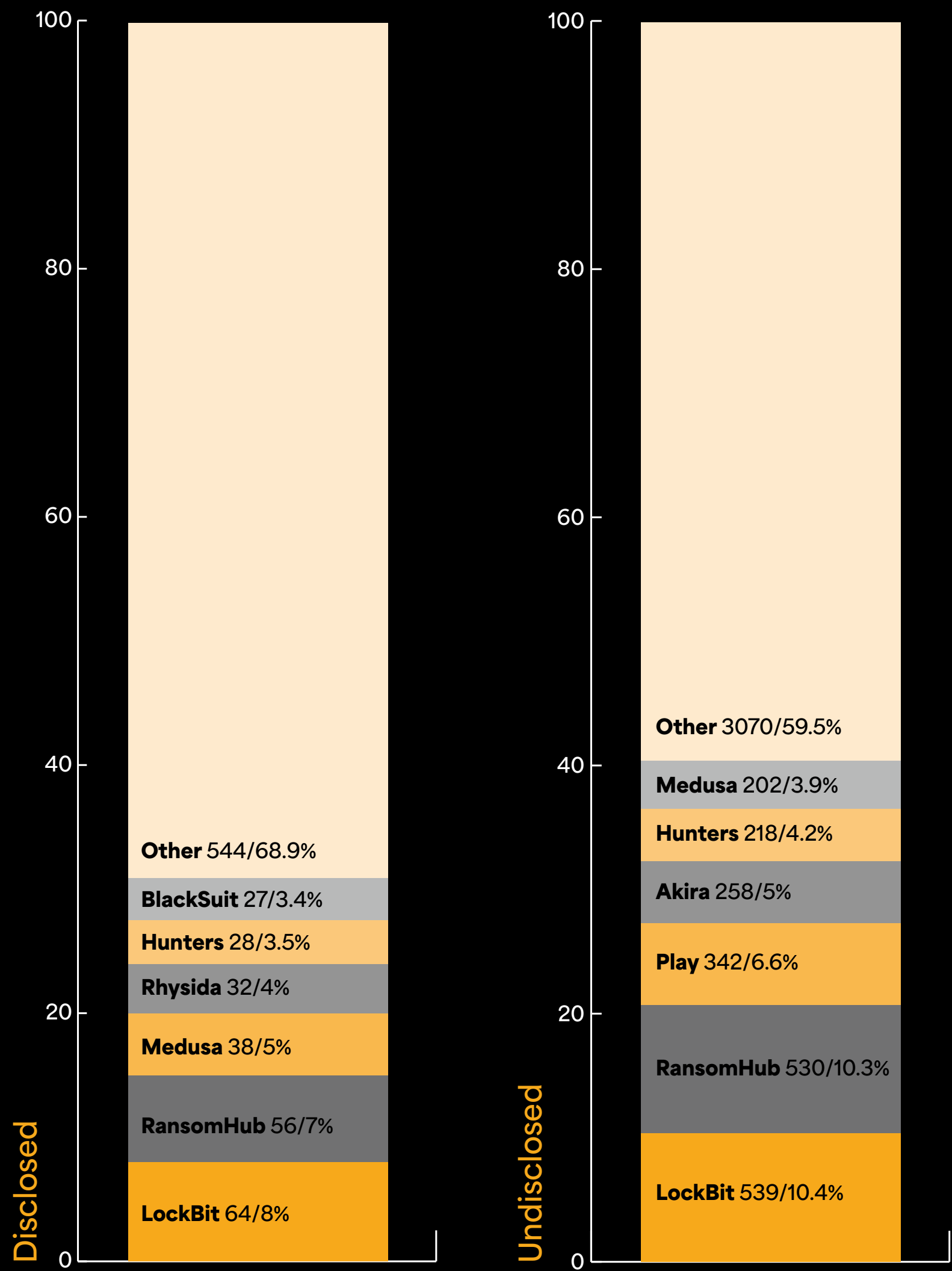
Although most of their attacks were only seen by those on the dark web, Play contributed significantly to the ransomware tally in 2024. Making up 7% of all undisclosed attacks with a total of 342, many countries and industries felt the brunt of their escapades.

Manufacturing seemed to be a key target for the group, but they also targeted a number of lesser favored industries such as food and drink and arts and entertainment. Donut lovers crumbled when [Krispy Kreme](#) fell victim to Play, and many event spaces across the US had their networks infiltrated by the group.

Now that we have addressed the most notable, it is only fair that we look into the new entries. They may not have racked up the big numbers during the year but they still managed to make an impact on their victims.



Ransomware attacks by variant, 2024





48 new
ransomware
variants were
recorded in
2024

2024 saw a **65%**
increase in the
number of **new**
variants vs 2023

DID YOU KNOW?

New Players in The Game

With **48 new groups emerging this year**, a huge 65% increase from the number of new variants in 2023, it is clear why ransomware is one of the biggest worries for cybersecurity professionals worldwide.

Only 4 out of 48 were one time attackers, meaning that between 44 new variants they were responsible for 32% of all undisclosed attacks in 2024. July saw

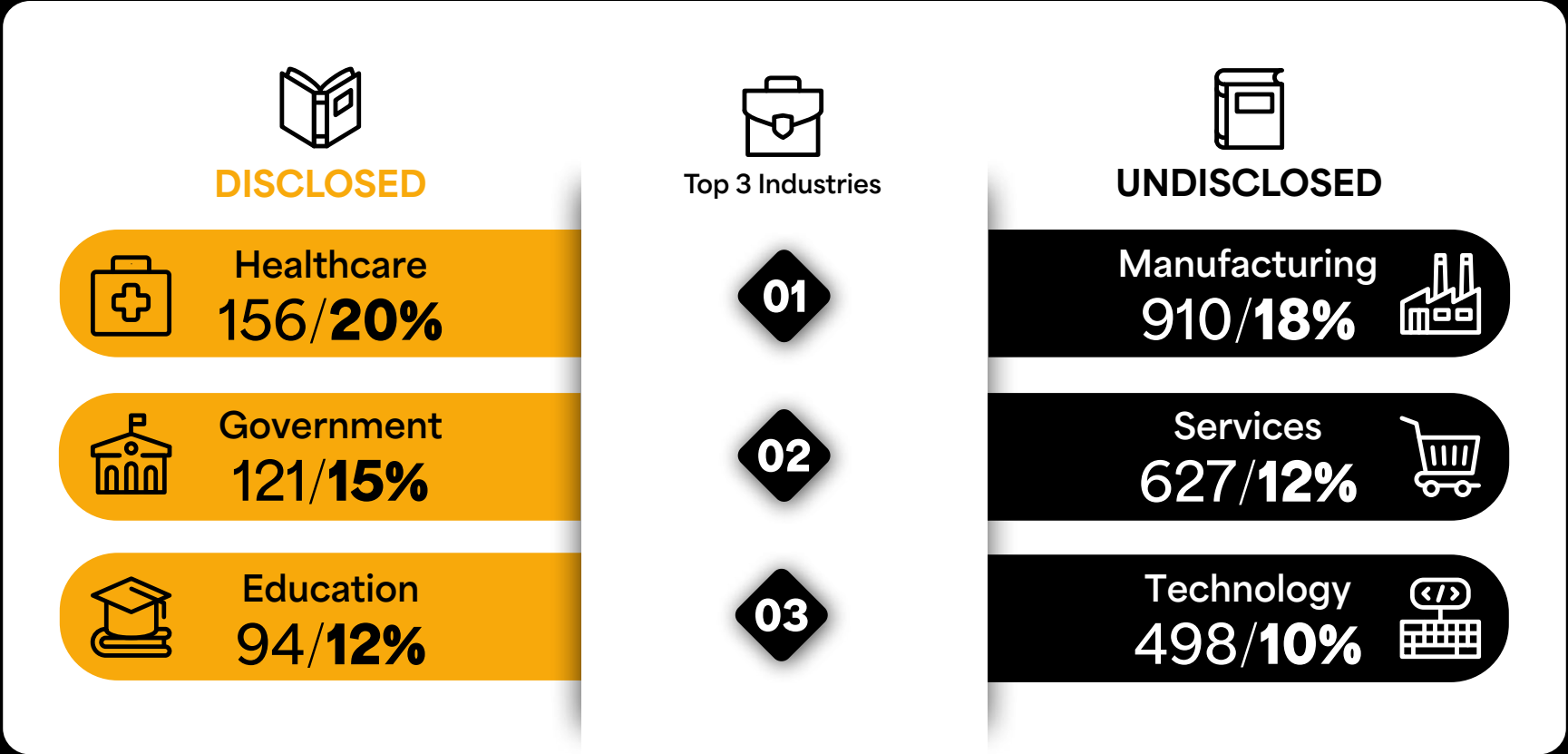
the highest number of new gangs emerge, with 8 in total claiming their first attacks during that month.

In November and December, gangs that debuted in 2024 accounted for more than 50% of the attacks in each of those months - another interesting statistic that tells an unnerving story about underestimating an unknown group.

Some new variants to mention are:

- **Funksec** only emerged in December but ended the year on 60 attacks - this could indicate increased prominence in 2025.
- **Kill** started emerging slowly in March but ramped up activity in Q3 (134 total)
- **El Dorado** and **APT73** who both claimed their first victims this year but who also changed their operating names to Blacklock and Bashe respectively. This shows that, even though they are new, these gangs will pivot to find new ways to target and extort companies.
- Top Israeli organizations and personnel were targeted by **Handala**, who went on a rampage of politically motivated attacks this year.

These new variants, and the volume in which they have appeared during the year, provides an insight into the ransomware landscape. **With the developments in RaaS and AI**, less cybercrime groups are building custom tools, instead using these readily available options to facilitate a cyberattack more quickly and easily.



5

Industry

No industry is safe from cyberattacks, and this was made abundantly clear in 2024. Industry and size don’t matter, if you have data, which all organizations do, you are at risk of falling victim to ransomware.

As has become the norm, the three top targeted industries for disclosed attacks were healthcare, government and education, which accounted for 47% of all 2024’s ransomware news headlines. Healthcare and government still experienced an

increase in attacks from 2023, but attacks on the education sector dropped by 10%. Industries like retail, services and finance all saw huge increases in the number of attacks in 2024, with 96%, 88% and 66% increases respectively.

This highlights the importance of cybersecurity in all industries, not just those that are seen as “most at risk.”

For undisclosed attacks, the favored industries were very different. Manufacturing, services and technology were named the top three, with 17.6%, 12.2% and 9.7% respectively. With these figures contrasting those of the attacks that are publicly disclosed, it brings to question, why are these industries not disclosing attacks as frequently or consistently as others?

Our research into undisclosed attacks also revealed that the legal sector was substantially impacted

this year and that logistics companies also felt the brunt of ransomware attacks. The reasons behind targeting these industries are clear; the legal sector has extremely sensitive data worth exfiltrating, whereas attacking a logistics company will cause significant disruption to operations.

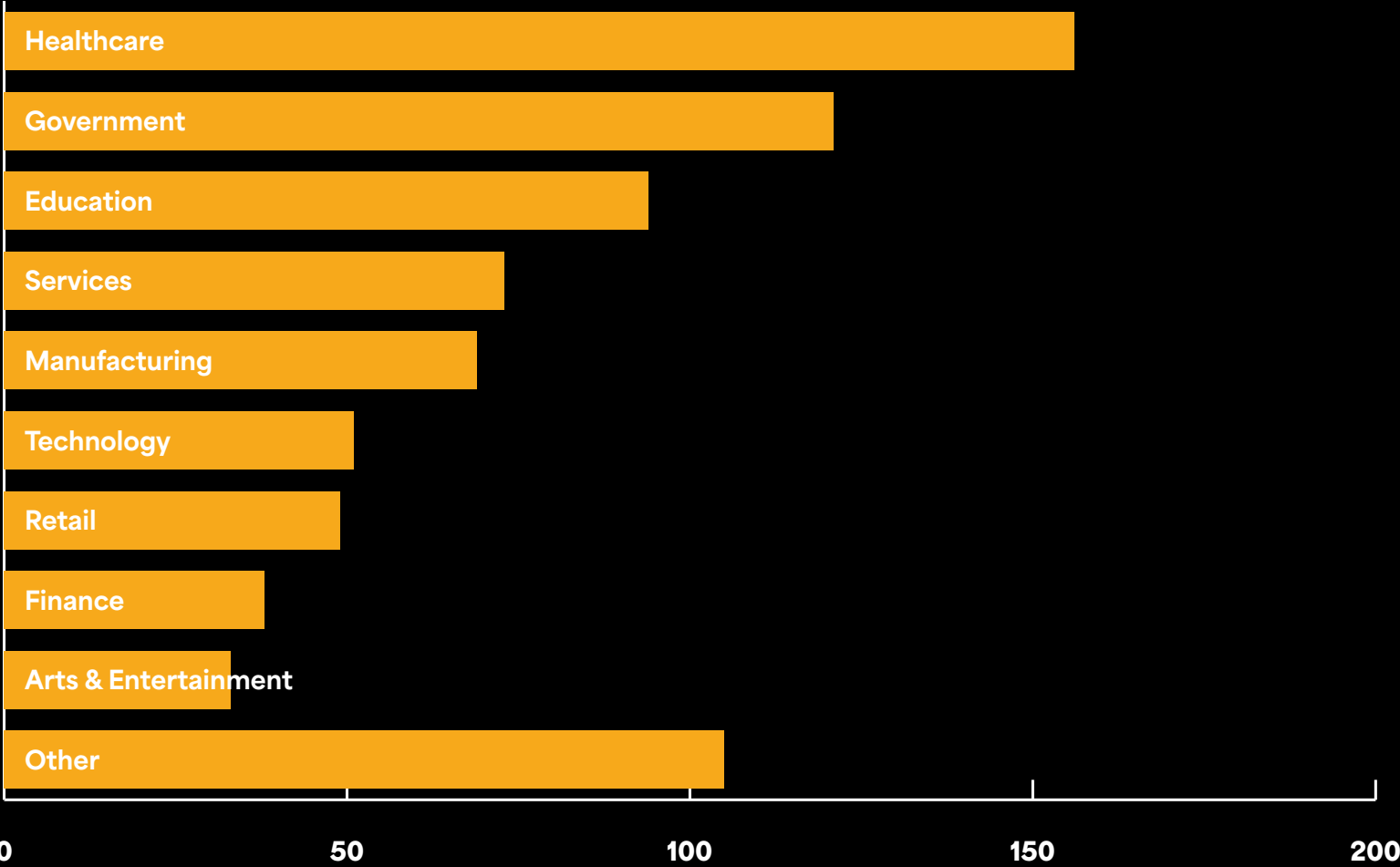
The news constantly reinforces the importance of protecting critical infrastructure, and in 2024 it was more important than ever. An example of this was the utilities industry, where 103 gas, electrical or other energy companies were targeted. Some of these included state owned companies such as Costa Rica’s [RECOPE](#), PT Pertamina in India and various United States based organizations.

18%

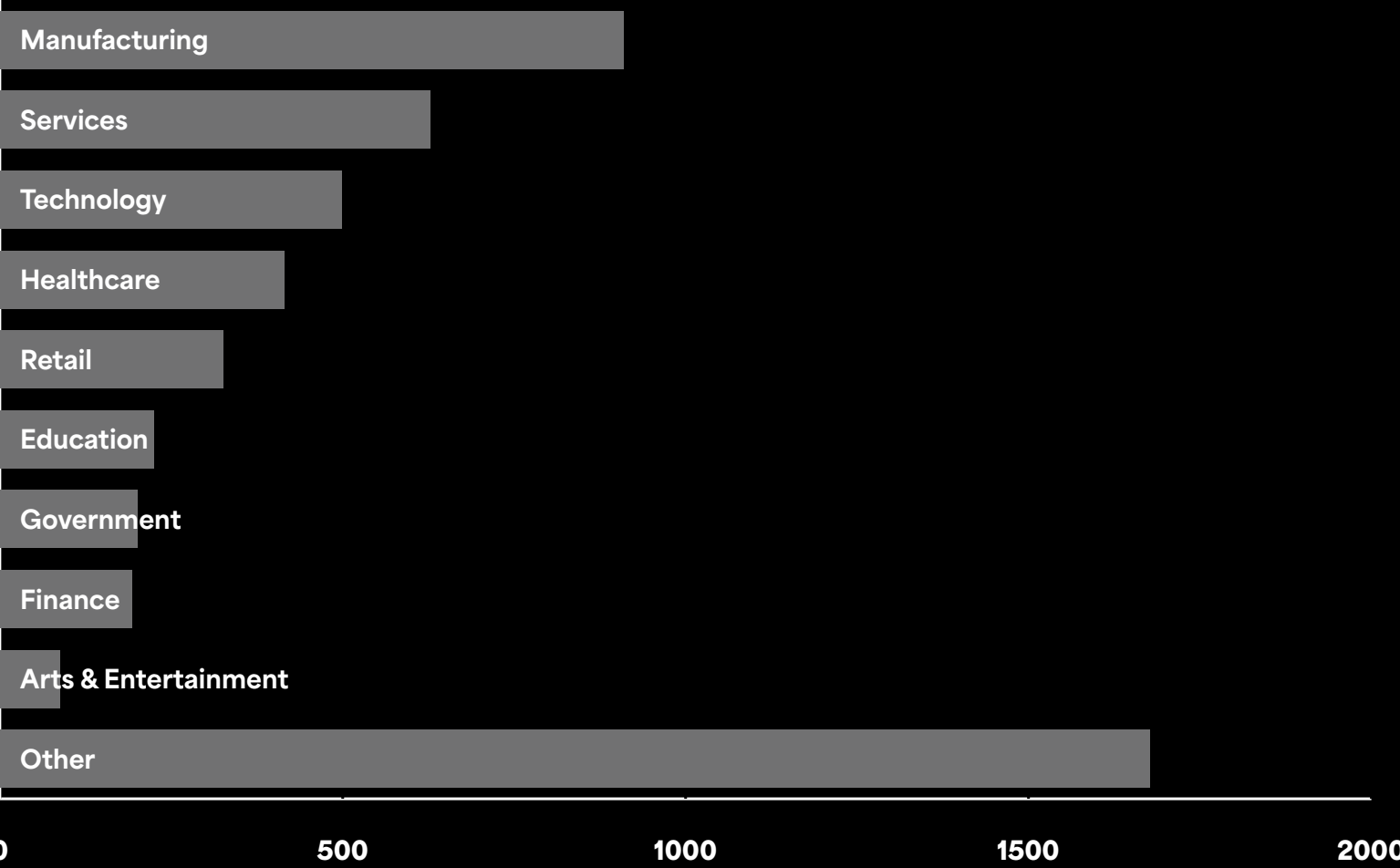
of all undisclosed ransomware attacks targeted the manufacturing industry

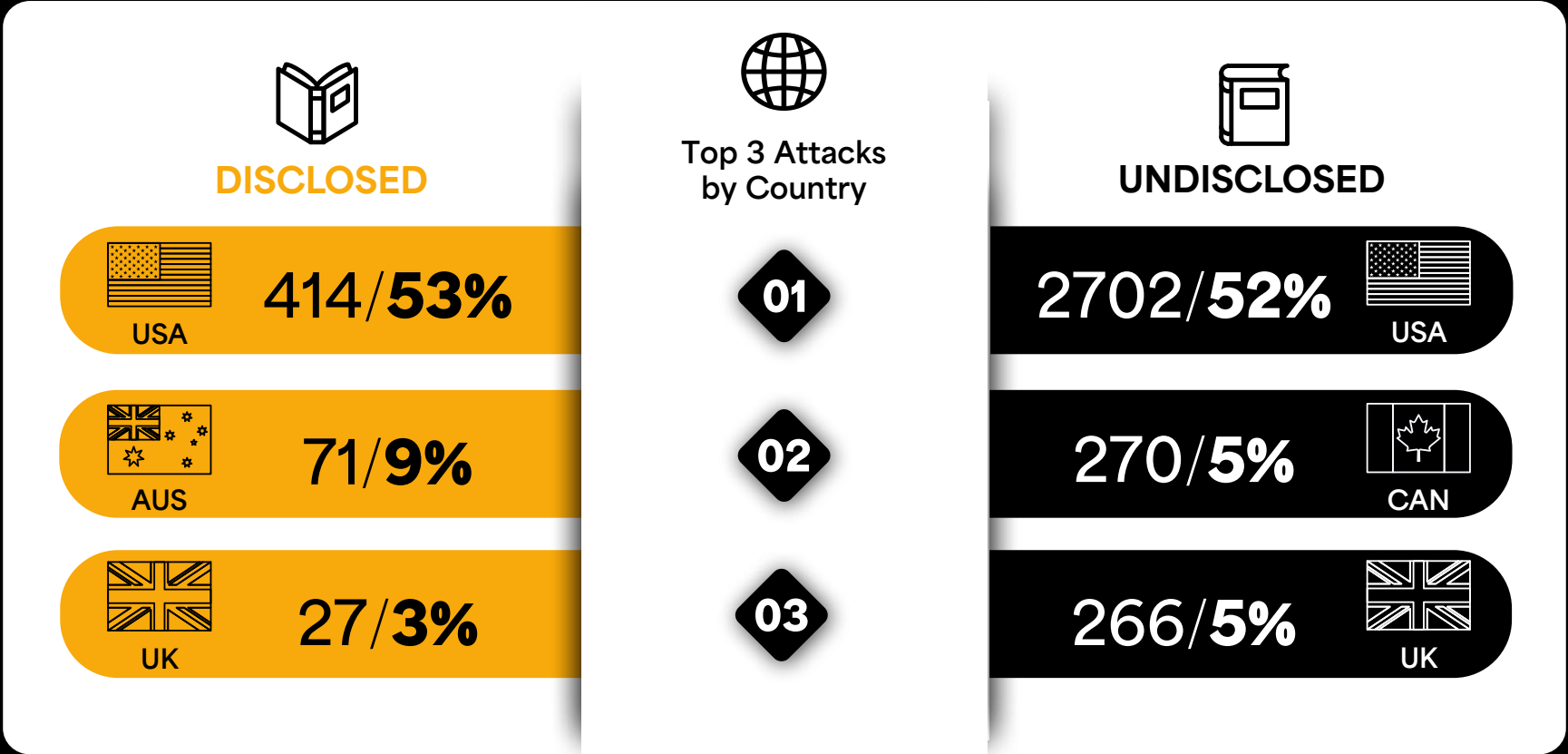


Disclosed ransomware attacks by industry, 2024



Undisclosed ransomware attacks by industry, 2024





6

Geography

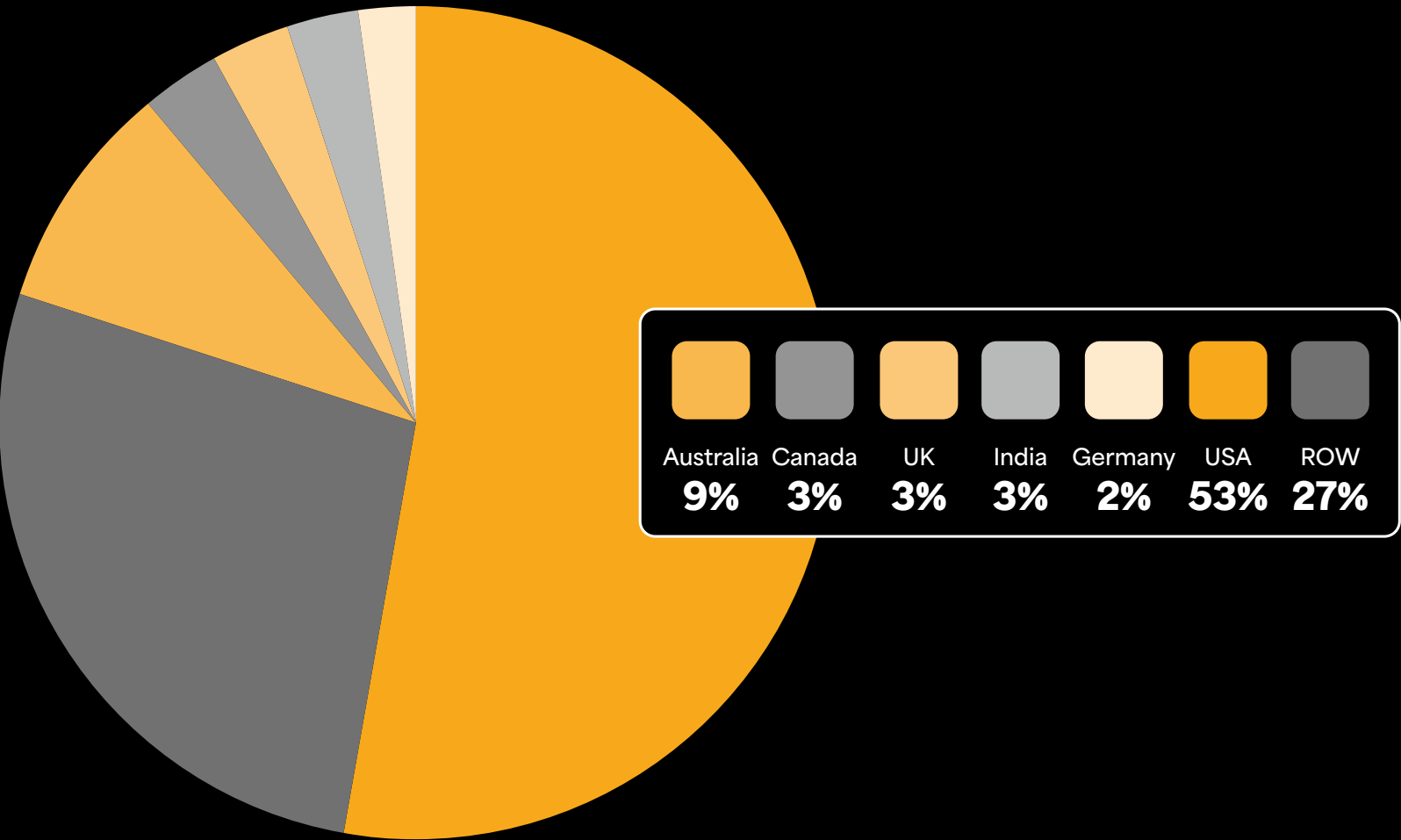
No country is off limits when it comes to ransomware, attackers pay little attention to borders when looking for their next victim.

Evident by the number of attacks targeting companies in smaller countries in recent years. In 2024 we recorded attacks in Congo, Fiji, Ghana, Costa Rica, Barbados and Philippines to mention a few, none of these being considered as typical targeted countries. Attacks within smaller countries, who may not have the financial support or infrastructure to defend against an attack, can result in much more detrimental attacks compared to other countries with stricter cybersecurity guidelines and regulations.

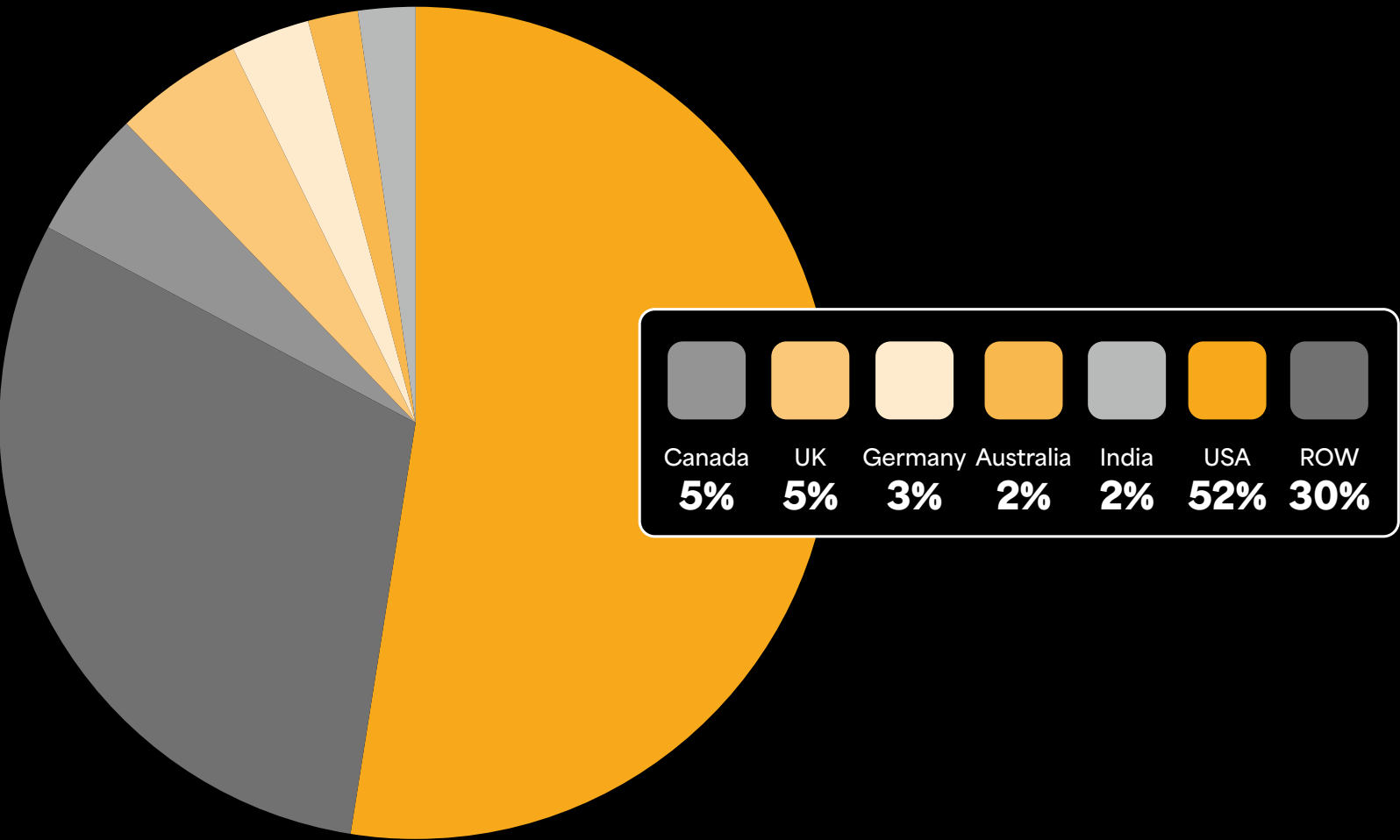
As expected, organizations in the United States faced the largest number of attacks, totalling 3116 throughout the year. All verticals we recorded faced attacks in the USA, with manufacturing suffering from 28% of the incidents.

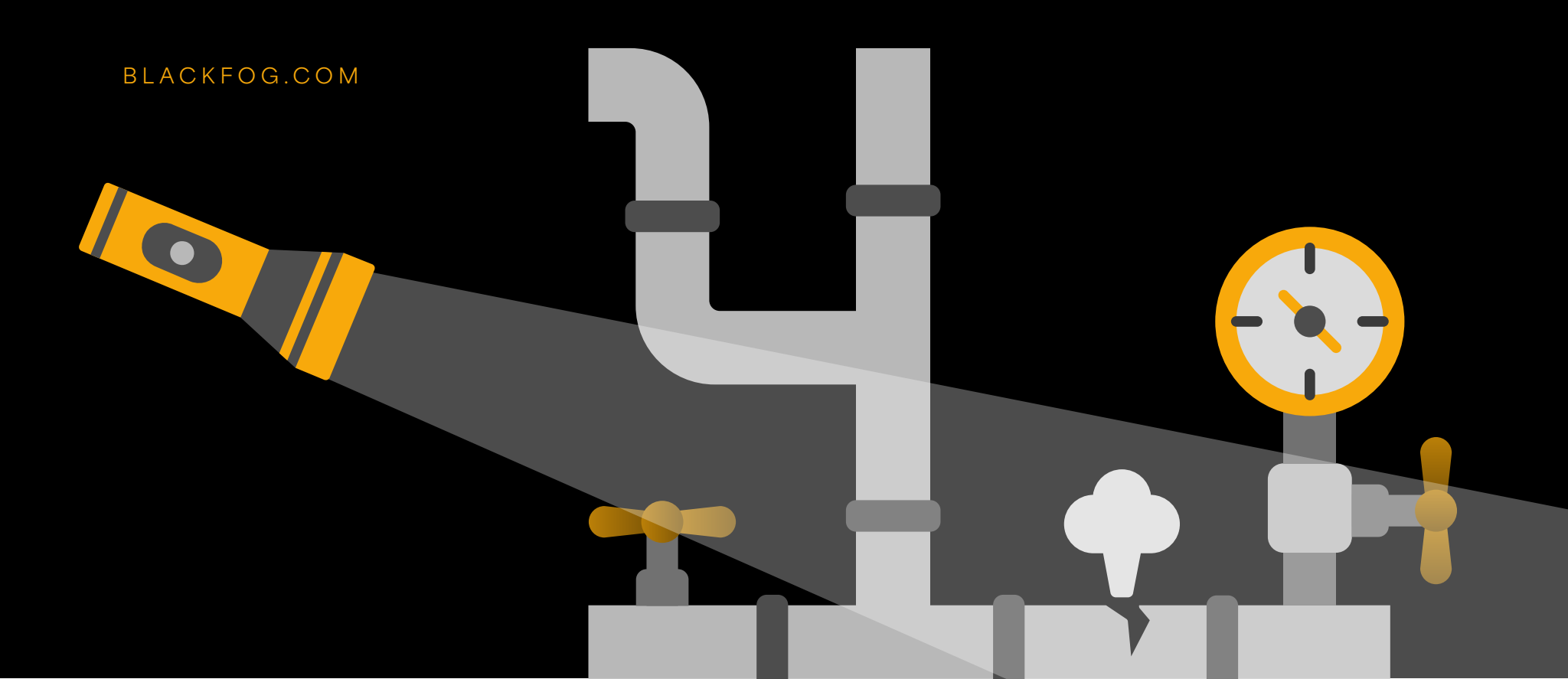
As previously mentioned, some attacks on certain countries are motivated by factors other than money. Cyberespionage and cyberwarfare was the motivation behind a number of attacks in 2024, most of them focused on the targets of [Handala](#).

Disclosed ransomware attacks by country, 2024



Undisclosed ransomware attacks by country, 2024





7

Critical Infrastructure

In 2024, the world faced an alarming rise in cyberattacks on critical infrastructure, revealing significant vulnerabilities across various sectors. From the United States to Europe and beyond, cybercriminals and state-sponsored actors launched sophisticated attacks on essential services like water, energy, healthcare, and transportation. As the frequency and severity of these attacks continue to rise, it is imperative for nations to bolster their defenses and protect their critical infrastructure from future cyber threats. Let’s dive into some of the incidents that marked this troubling trend.



U.S. Telecommunications Breach



In August 2024, Chinese hackers infiltrated major U.S. telecommunications firms, including AT&T, Verizon, Lumen Technologies, and T-Mobile. The attackers accessed metadata of calls and text messages from over a million users, including political figures. They also compromised wiretapping systems used for authorized surveillance. The breach was attributed to the “Salt Typhoon” group, linked to China’s Ministry of State Security.



Water Cyberattacks



American Water (USA): the largest regulated water and wastewater utility company in the U.S., suffered a cyberattack that led to a temporary halt in billing operations. While water services remained unaffected, the incident underscored the vulnerabilities in essential services and prompted calls for enhanced cybersecurity measures in the water sector.

Southern Water (UK): In February 2024, Southern Water reported a data breach that exposed personal and operational data. Hackers targeted the utility’s IT systems, gaining unauthorized access and compromising personal details of customers and employees.

Texas Water Facility (USA): A water facility in Texas was targeted in a cyberattack that attempted to manipulate processes, suspected to involve Russian-linked hackers. This incident underscored the vulnerability of water utilities to sophisticated cyber threats.

Arkansas City Water Treatment Facility (USA): In Kansas, a water treatment facility in Arkansas City suffered a cybersecurity incident and was switched to manual operations out of caution. This incident highlighted the need for robust cybersecurity measures in water utilities.



Healthcare Sector Ransomware Surge

The healthcare industry experienced a significant increase in ransomware attacks in 2024. These attacks disrupted hospital operations, leading to postponed procedures and compromised patient data. The surge highlighted the critical need for improved cybersecurity in healthcare systems to protect patient safety and confidentiality.



Transportation for London (TfL) Cyberattack



In 2024, Transport for London faced a cyberattack that disrupted its operations. The incident served as a stark reminder of the importance of safeguarding national infrastructure against digital threats, emphasizing the need for robust cybersecurity measures in public transportation systems.



Automotive Industry Cyberattacks

The automotive sector saw a significant rise in cyber incidents, with 409 new cases reported in 2024, up from 295 in 2023. Ransomware attacks targeting the mobility sector contributed notably to this increase, raising concerns about vehicle security and the broader implications for transportation infrastructure.



The average cost of a **ransomware attack** involving data exfiltration in 2024 was **\$5.21M**

DID YOU KNOW?

8

Extortion and Exfiltration – The New Age of Ransomware

Ransomware attacks continue to evolve, with criminals shifting from traditional encryption-only methods to a mix of different tactics. Extortion has become a widely used method by cybercriminals, who use data to blackmail organizations into paying ransom demands. But one of the most significant cybersecurity trends is the persistent rise in data exfiltration.

Data exfiltration is one of the most worrying tactics used – after infiltrating a company’s infrastructure and stealing the data, cybercriminals then threaten to leak the data to force organizations to pay up or face a PR nightmare. At BlackFog, we’ve tracked the rate of data exfiltration closely for the past four years, we’ve seen the level of data exfiltration rise in recent times but in 2024 it surged to an all-time high of 94%!

With the focus moving away from traditional encryption only attacks to data exfiltration based attacks, more information has become available on the true cost of data exfiltration. [IBM’s Cost of a Data Breach Report](#) stated that the average cost of a ransomware attack involving data exfiltration in 2024 was \$5.21M.

The aim of extortion is to pressure the company to pay the ransom demand to stop a data leak and avoid reputational damage as the result of being a publicly named victim of a ransomware attack. When a security team identifies a data security breach, the organization, on average, [saves around \\$1million](#), compare to an incident being disclosed by a cybercriminal group. This data highlights the importance of early detection in reducing the financial impact of a data breach. As expected, organizations in the United States faced the largest number of attacks, totalling 3116 throughout the year. All verticals we record faced attacks in the USA, with manufacturing suffering from 28% of the incidents.



Dr. Darren Williams,
Founder & CEO,
BlackFog Inc.



9

2025 Predictions – Cybersecurity Trends

With 2025 now underway our Founder & CEO [Darren Williams](#) shared his predictions on the top cybersecurity challenges organizations could face in 2025:



AI Driven Ransomware:

As threat actors’ use of AI continues to proliferate, their attack rate will allow them to work more efficiently and successfully than ever before. There’s no honor amongst thieves, and the trend of “gang-hopping” by individual cybercriminals between ransomware groups will further complicate attribution and containment efforts. Attackers will follow the money and choose financial gain over any allegiance to a group.

As threat actors evolve their tactics for maximum impact, they will continue to use advanced AI-driven tools to deploy highly tailored phishing attacks. AI is also ushering in a new generation of highly convincing deepfake technology that will introduce unprecedented risks for personal and corporate brands alike. Organized crime groups are aiming to cash in by creating increasingly convincing videos impersonating executives and public figures, such as Jeff Bezos and Elon Musk.



AI and Machine Learning: The New Frontier in Ransomware Prevention

The only way to truly fight modern ransomware attacks is with AI based technologies. Ransomware has evolved rapidly in the last two years and is more effective than it has ever been. This year has seen unparalleled success with the highest number of successful attacks in five years. Existing technologies have simply failed to have any impact. The importance of adopting AI-Driven solutions was highlighted by figures suggesting that extensively using [AI reduced the financial impact of data breaches by \\$1.88million](#).

Newer solutions based around AI and zero day based attacks have proved very effective against these new variants, which are often combinations of other variants cobbled together.

By leveraging AI, vendors are able to target vulnerabilities that haven't even been identified in real time. The challenge is for these emerging vendors to break through the noise of a crowded cybersecurity market to get attention from organizations. Strong solutions do exist, and they are only getting better.



Critical Infrastructure Under Siege: A Growing Threat

High-profile healthcare provider attacks in 2024, from Change Healthcare in the US to pathology services provider Synnovis in the UK, were notable not only for the significant data loss but also for their impact on services and, ultimately, patient wellbeing.

Ongoing issues with resources and legacy infrastructure, along with the wealth of valuable data across the healthcare sector, mean it is perceived as a “weak link” by cyberattackers and will likely continue to bear the brunt of serious cyberattacks. As criminal gangs leverage patients’ privacy, safety, and health in ransom demands, it is vital for providers across the sector to protect their most vulnerable points to safeguard patients and staff.



By **leveraging AI**, vendors are able to **target vulnerabilities** that haven't even been identified in real time.”





Battling Cyber Fatigue: Staying Vigilant in an Ever-Evolving Threat Landscape

As security stacks continue to grow, leaders in the field must also confront the escalating issue of alert fatigue. This challenge stems from teams managing a multitude of disconnected tools instead of relying on well-integrated solutions. I anticipate many security leaders will prioritize quality over quantity, focusing on unified security platforms, which aim to consolidate threat detection and response capabilities, reducing duplication and alleviating alert fatigue for overwhelmed teams.

Looking ahead to next year, it's clear that organizations will have a whole range of cybersecurity challenges to contend with. Ransomware will continue to be a thriving industry, with criminal gangs intent on developing new techniques and strategies to steal data, extort money and cause mass disruption.

As cybercriminals increasingly employ AI-powered advanced technology to target specific companies and even individuals, organizations must proactively prepare. Regardless of their size or sector, the reality is that they must assume they are a target and have the right policies, procedures and tools in place to safeguard their data and effectively recover from an attack.



Insider Threats: The Power of Employee Awareness in Preventing Ransomware Attacks

Awareness training should not be underestimated when it comes to reducing the impact of ransomware within any organization. The weakest link is always a human in our experience and the sophistication of phishing attacks has reached a new zenith with the use of AI to craft impactful, targeted attacks.

Ensuring users are well trained in identifying these types of techniques is critical as a first line of defense and for reducing human error. Many regulatory frameworks such as SOC 2 and ISO 27000 already mandate employees perform regular training to help foster a strong security culture with an organization.

Innovative methods to make this more interesting involve forms of gamification such as puzzles and other tests to see if users can be tricked, these often prove quite effective. Many systems also employ training with real time alerts warning them of the latest scams and techniques and when emails have been flagged, for example due to suspicious activity. Together these techniques can make training generally more engaging and more likely to be embraced as part of the company culture.



Ransomware will continue to be a **thriving industry**, with criminal gangs intent on developing **new techniques and strategies** to steal data, extort money and cause **mass disruption**.”





There was a
27%
increase in
the number of
ransomware victims
In 2024

DID YOU
KNOW?

10

How to Prevent Ransomware Attacks

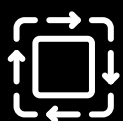
The last 18 months has seen ransomware around the world continue to set new, unwanted records. Both the frequency of recent ransomware attacks and the ransom amounts cybercriminals have demanded from businesses continue to rise, and it's clear that every company is a target, no matter its size or sector.

As a result, organizations unprepared to stop ransomware attacks are putting themselves at huge risk. Therefore, it's vital that enterprises appreciate the [scale of the ransomware threat in 2024](#) to better understand how to prevent ransomware attacks in 2025.

Understanding Ransomware attacks

Step one must be to ensure firms have a comprehensive understanding of what these attacks involve and why they are so dangerous. This includes knowing exactly what happens during a ransomware attack, how firms get infected and what can be done to both prevent and recover from these incidents.

4 Best Practices for how to Prevent a Ransomware Attack



Protect Beyond The Perimeter

While blocking attacks at the edge of the network before they have a chance to infiltrate the network is essential, techniques such as advanced firewalls, antimalware and email security alone aren't enough. Greater use of techniques such as fileless malware can easily bypass these defenses and, if left unchecked, can have free rein inside your network. Therefore, monitoring tools that can keep an eye on suspicious data traffic and other activity within your systems are a must.



Keep Systems Up To Date

Outdated software is another major cause of data loss - and breaches caused by unpatched systems cost firms **54 percent** more than incidents related to user actions. To avoid this, it pays to have a clear patching schedule for every system within the network. This can be a tedious job, but the right tools can help identify and alert security teams to potential issues and keep on top of this.



Train And Test Employees

Human error remains the number one cause of malware infections - with this at least partly responsible for **88 percent** of data breaches. Therefore, it's vital all employees are trained on what red flags to look for and how to alert security teams of suspicious activity. It's also not enough to lecture individuals on their responsibilities. Firms need to make sure messages are sinking in, so frequent testing of employees, such as with fake phishing emails, is also highly important.



Harden Every Endpoint

If hackers have been able to gain access to systems, they still won't be able to operate a successful ransomware attack unless they can actually exfiltrate data from the network. Therefore, tools to protect every endpoint on the system against this activity - from desktop PCs and servers to employee-owned smartphones - are essential. Dedicated, lightweight **anti data exfiltration (ADX)** software enables this by using machine learning to monitor every packet of data leaving the network, with the ability to automatically step in and shut down any suspicious activity.

11

About BlackFog

Founded in 2015, BlackFog is a global AI based cybersecurity company that has pioneered on-device anti data exfiltration (ADX) technology to protect organizations from ransomware and data loss.

With more than 94% of all attacks involving some form of data exfiltration, preventing this has become critical in the fight against extortion, the loss of customer data and trade secrets.

BlackFog recently won the “Best Threat Intelligence Technology” in the 2024 Teiss Awards, “AI-based Cybersecurity Innovation of the Year” award in the [CyberSecurity Breakthrough Awards](#), as well as the 2024 Fortress Data Protection award for its pioneering anti data exfiltration (ADX) technology.

BlackFog also won Gold at the Globee awards in 2024 for best Data Loss Prevention and the State of Ransomware report which recognizes outstanding contributions in securing the digital landscape.

Trusted by hundreds of organizations all over the world, BlackFog is redefining modern cybersecurity practices. For more information visit blackfog.com

12

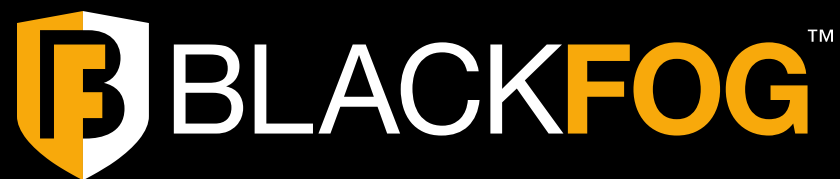
Methodology

This report was generated in part from data collected by BlackFog Enterprise over the specific report period January - December 2024. It highlights significant events that prevented or reduced the risk of ransomware or a data breach and provides insights into global trends for benchmarking purposes.

This report contains anonymized information about data movement across hundreds of organizations and should be used to assess risk associated with cybercrime.

Industry classifications are based upon the ICB classification for Supersector used by the York Stock Exchange (NYSE).

All recorded events are based upon data exfiltration from the device endpoint across all major platforms.



Follow Us



Award-winning Technology



Contact us for a demo

Start your free trial

Visit blackfog.com

All contents copyright © 2025 BlackFog, Inc. All rights reserved. The BlackFog logo and name are trademarks of BlackFog, Inc. All other trademarks are the property of their respective owners.

Except as specifically stated herein, none of the material may be copied, reproduced, distributed, republished, downloaded, displayed, posted, or transmitted in any form without authorized, prior written permission from BlackFog, Inc. Permission is granted for you to make a single copy of this document solely for informational uses within your organization, provided that you keep intact all copyright and other proprietary notices. No other use of the information provided is authorized.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners. The information contained in this document represents the current view of BlackFog, Inc. on the issues discussed as of the date of publication.