Cyberint

Impactful Intelligence

RANSOMWARE RECAP 2023

January 2024

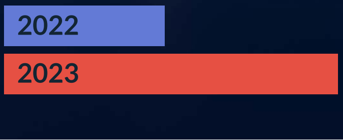
TABLE OF CONTENTS

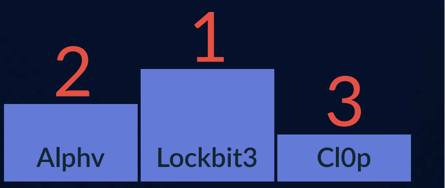
EXECUTIVE SUMMARY

In 2023, ransomware groups saw unprecedented success, with a 55.5% surge in victims, totaling 5,070 a̅ stark rise from the previous year. Q2 and Q3 alone claimed more victims than the entire 2022, with 2903 victims. Ransomware leaders remain the veterans, LockBit3.0, ALPHV and Cl0p. Without a doubt, the MOVEit campaign will be remembered as the most successful campaign this year, teaching us the importance of supply chain attacks, version control and the importance of understanding our attack surface. The USA was the most targeted country (49.8%, up from 38% in 2022) followed by the U.K. and Canada. The most targeted sector was business services, with 1265 cases, followed by retail and manufacturing.

5,070
VICTIMS

55.5%
VICTIMS RISE





LEADING RANSOMWARE GROUPS

MOVEit
MOST SEVERE CAMPAIGN

Law authorities succeeded in shutting down several major cybercrime groups, such as hive.

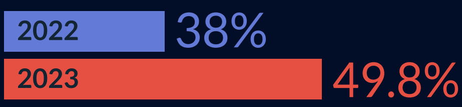
MOST TARGETED SECTORS

BUSINESS SERVICES	RETAIL	MANUFACTURING
1265 CASES	649 CASES	457 CASES

MOST TARGETED COUNTRY

USA | UK | CANADA

USA VICTIMS



2024

Ransomware groups will climb to new heights in 2024, targeting supply chain infrastructures while still sticking to "old habits" by applying phishing, leaked credentials, and social engineering techniques.

Q4 STATS

In the fourth quarter of 2023, we documented 1,309 ransomware incidents globally. As illustrated in the graph below, the **LockBit** group continues to dominate ransomware group attacks, recording a total of 243 successful incidents. Following closely in second place is the **PLAY** group, which executed ransomware attacks on 110 different organizations. Notably, nearly 40% of their attacks were carried out in the fourth quarter alone.

It is worth mentioning that the CLOP gang did not make it to the top 10 list for the quarter despite being among the top 3 in the year's overall totals. Since the notable MOVEIt breach orchestrated by the CLOP gang, there has been no observed activity from the group. However, despite missing an entire quarter, Cl0p is the third most active group in 2023, which shows us the scale of the MOVEit campaign.

Figure 1 //

TOP 10
ACTIVE RANSOMWARE GROUPS IN Q4

Lockbit3	243
Play	109
Alphv	109
8Base	71
Noescape	58
Akira	48
Medusa	46
Incransom	46
Bianlian	28
Blackbasta	28

Figure 2 //

TOP TARGETED INDUSTRY DISTRIBUTION IN Q4

Business Services	287
Retail	178
Manufacturing	119
Healthcare	66
Finance	63
Government	60
Education	56
Construction	46
Transportation	42
Technology	36

2023 STATS VS 2022

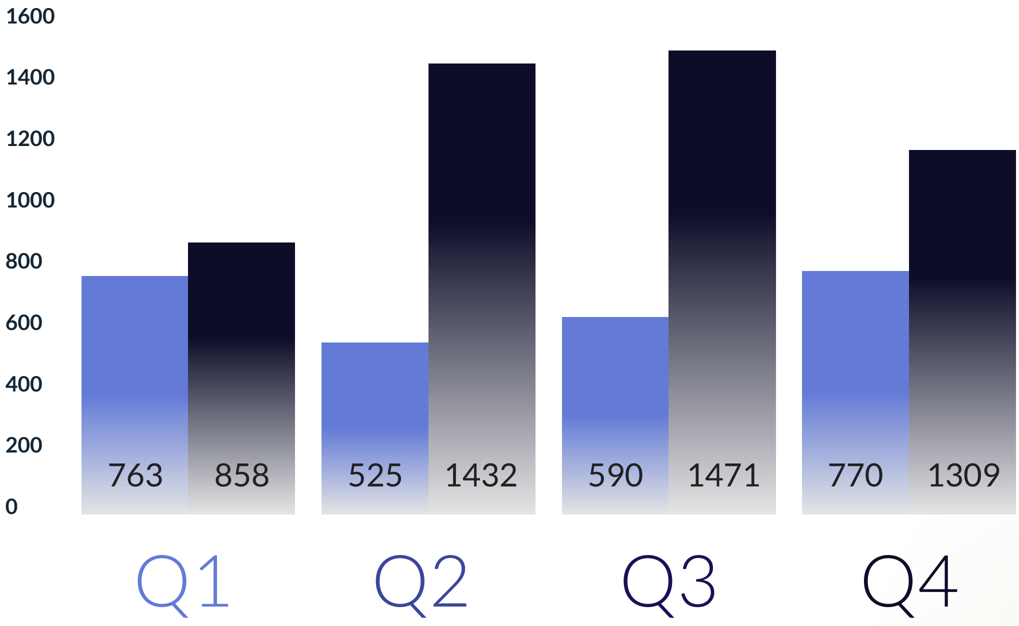
TOTAL NUMBER OF RANSOMWARE ATTACKS

In the year 2022, a total of 2,809 ransomware attacks were recorded globally. However, in 2023, there has been a significant surge, with the total number of ransomware attacks reaching 5070, marking a substantial increase of >55%.

This significant shift is spearheaded by established cybercrime groups like LockBit and Clop, with additional momentum coming from emerging ransomware gangs such as 8Base, BianLian, Play, Akira, and others. The substantial increase can be largely attributed to the CLOP group, which executed attacks at a higher frequency compared to the previous year, rapidly securing a position among the top three ransomware groups by attack count.

Figure 3 //

YEAR OVER YEAR VICTIMS PER QUARTER



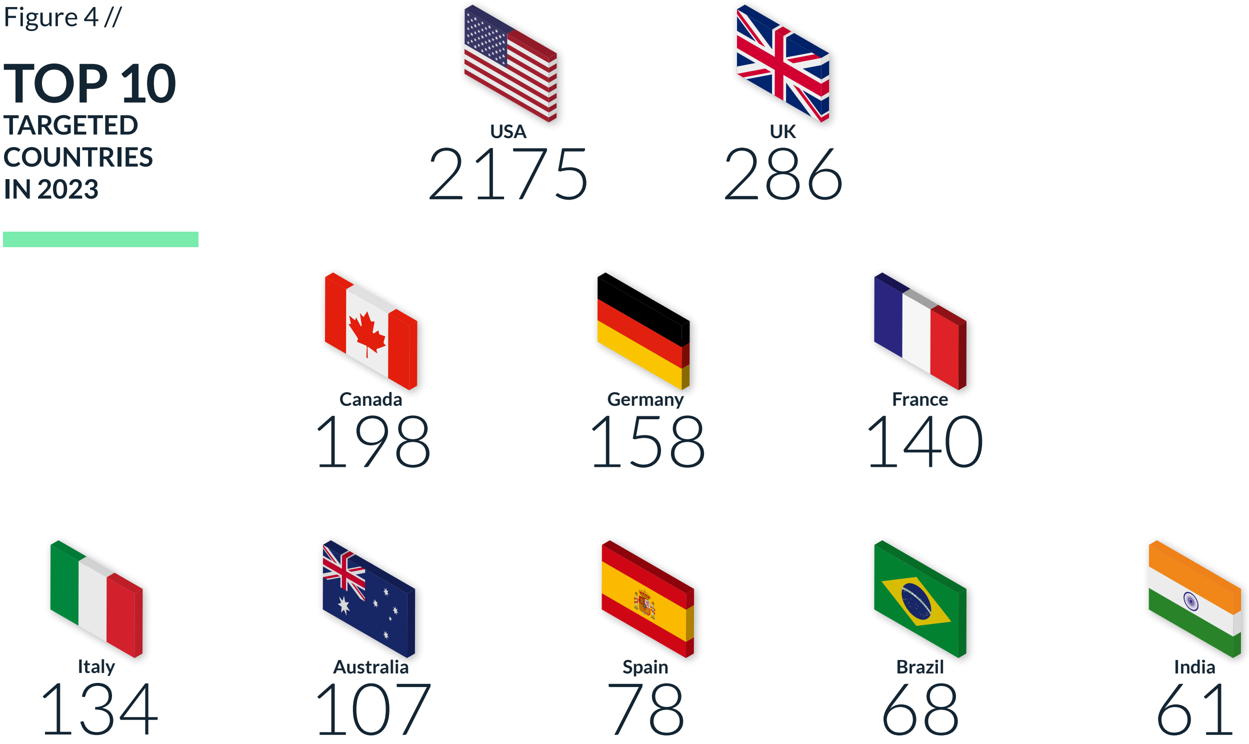
TARGETED COUNTRIES

When examining the Top 10 Countries most impacted by ransomware attacks, notable shifts are not apparent. The United States maintains its leading position, accounting for approximately 49.8% of all ransomware attacks. Following a pattern similar to the previous year, the United Kingdom, Canada, France, and Germany secured the next positions in the Top 5, with a considerable gap from the United States.

In a noteworthy change, India has unfortunately entered the top 10, displacing Russia from the previous year. This change could be attributed to the ongoing conflict between Russia and Ukraine, which garnered significant attention last year and involved ransomware groups from both sides, resulting in an escalation of attacks on the Russian front. With a relative de-escalation in cyber warfare activities between the two nations this year, India has taken Russia's side, experiencing increased ransomware attacks on its behalf.

Figure 4 //

TOP 10
TARGETED COUNTRIES IN 2023



TOP RANSOMWARE FAMILIES IN 2023

Figure 5 //

TOP 10 RANSOMWARE GROUPS IN 2023

Lockbit3	1047
Alphv	445
Clop	384
Play	304
Bianlian	281
8Base	281
Akira	174
Malas	172
Medusa	145
Noescape	123

Figure 6 //

TOP 10 TARGETED SECTORS IN 2023

Business Services	1265
Retail	649
Manufacturing	457
Finance	346
Education	245
Healthcare	226
Construction	198
Government	190
Transportation	177
Technology	153

TOP 3

LOCKBIT

Emerging in September 2019, the LockBit Ransomware Group claimed the title of the most active ransomware group in 2022 following the shutdown of Conti. Throughout 2023, LockBit maintained its prominence as the most active ransomware group. This year, LockBit achieved successful attacks on approximately 1047 victims, contributing to over 24% of the total ransomware attacks monitored by Cyberint in 2023.

Figure 7 //

LOCKBIT3.0 TOP 3 TARGETED COUNTRIES IN 2023

USA	UK	France
400	58	51

ALPHV

On December 19, 2023, the FBI successfully dismantled one of the ALPHV/BlackCat ransomware sites. The main page now bears the customary FBI banner, while other sites linked to the cybercrime gang remain operational. Although the FBI's action disrupted ALPHV, it is unlikely to completely halt the ransomware gang. Financially robust players like ALPHV can endure idle periods, and ransomware groups facing shutdown often resurface as entirely new entities or collaborate with existing groups. The comeback occurred swiftly when the group targeted two organizations at the end of December.

This year, ALPHV achieved successful attacks on approximately 445 victims, accounting for over 10% of the total ransomware attacks monitored by Cyberint in 2023.

Figure 8 //

ALPHV TOP 3 TARGETED COUNTRIES IN 2023

USA	UK	Canada
247	18	17

CLOP

Since February 2019, Clop attacks have been on the rise, persistently harming organizations worldwide in 2023. This year, Clop achieved successful attacks on approximately 384 victims, representing over 8.7% of the total ransomware attacks monitored by Cyberint in 2023.

Figure 9 //

CLOP TOP 3 TARGETED COUNTRIES IN 2023

USA	UK	Canada
227	26	18

FAMILIES WORTH NOTING

At the end of 2022, new ransomware families emerged and older ones intensified their attacks in 2023. Notable among them were the 8base and Play ransomware families.

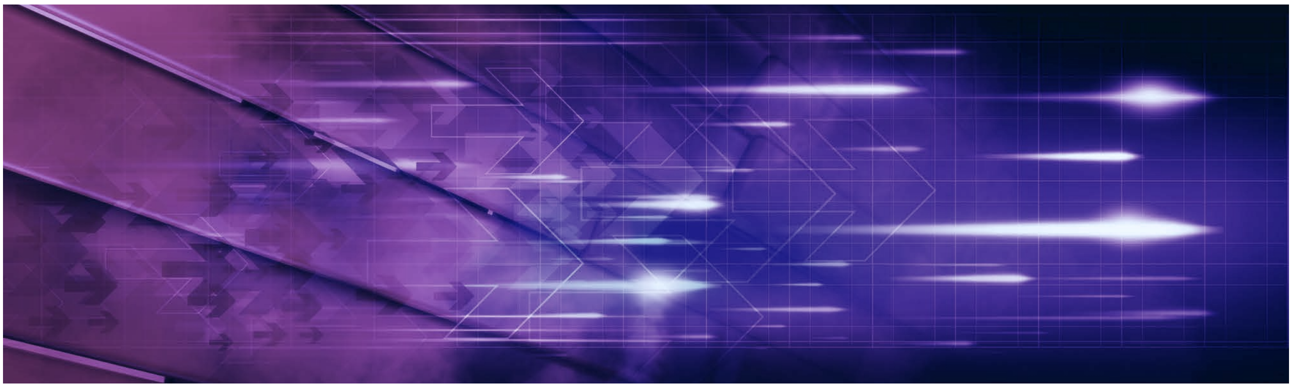
8BASE

Initiating operations in April 2022, 8Base is a ransomware collective that swiftly gained a reputation for its forceful strategies and a substantial volume of victims despite its relatively short time in the cyber landscape. In 2023, the group achieved significant milestones, conducting attacks on 281 organizations, with 40% of their focus on the United States.

PLAY

First observed around June 2022, the Play ransomware gang, responsible for devastating attacks on major American cities, allegedly launched more than 300 successful incidents since June 2022. In this year alone, the group executed 304 attacks, with more than 50% targeting organizations in the United States.

NEW COMERS



RHYSIDA

The Rhysida ransomware group came into the spotlight around May-June 2023 when they introduced a victim support chat portal accessible through the TOR (.onion) site. The group portrays itself as a “cybersecurity team,” claiming to be acting in its victims’ best interests by targeting their systems and drawing attention to the purported security vulnerabilities and their potential consequences.

The Rhysida ransomware group has gained notoriety due to a series of attacks on healthcare institutions, prompting government agencies and cybersecurity firms to intensify scrutiny of the group’s activities. In June, Rhysida first garnered attention when it publicly disclosed documents stolen from the Chilean Army (Ejército de Chile) on its data leak site.

In 2023, the Rhysida ransomware group made headlines with multiple significant attacks. They targeted high-profile entities, including the British Library, where they conducted a cyber-attack, causing a major technology outage and selling stolen personal information online. In the US, Rhysida attacked Prospect Medical Holdings, impacting the healthcare sector, and compromised Insomniac Games, a Sony-owned video game developer, showcasing their broad reach across diverse industries.

MALASLOCKER

MalasLocker emerged in March 2023 and adopted an unconventional approach by promising a charitable donation in exchange for providing decryption tools and preventing data leaks. This departure from typical ransom demands casts them as digital activists against corporate entities and economic inequality. Despite their claims, it’s unclear if they follow through on decryption after receiving proof of donations.

Focusing primarily on the Business Services, Software, and Manufacturing sectors, with a significant emphasis on Professional, Scientific, and Technical Services, MalasLocker targets companies mainly located in Italy, Russia, and the United States. Their attacks involve breaching Zimbra servers, encrypting data, and uploading suspicious JSP files to specific directories.

AKIRA

Akira is offered as a ransomware-as-a-service and was discovered in March 2023. Preliminary research suggests a connection between the Akira group and threat actors associated with the notorious ransomware operation Conti.

This ransomware, identified as having an impact on both Windows and Linux systems, operates by exfiltrating and encrypting data, coercing victims into paying a twofold ransom to regain access and restore their files. The collective responsible for this ransomware has already directed its attention towards numerous victims, primarily focusing on those in the U.S. Furthermore, the group operates an active leak site for the Akira ransomware, where they publish information, including their latest data breaches.

BLACKSUIT

BlackSuit, a newly identified ransomware group resembling the notorious Royal ransomware, has posed a significant threat to the Healthcare and Public Health (HPH) sector since its emergence in May 2023. Exhibiting strong connections to Royal and the now-defunct Conti, known for aggressive targeting in this sector, BlackSuit's affiliation raises concerns. While their victim count is limited, their attacks have impacted the United States, Canada, Brazil, and the United Kingdom across industries like healthcare, manufacturing, business technology, retail, and government. Notably, a U.S.-based medical services provider to numerous hospitals faced severe disruptions, reflecting potential widespread consequences. Employing a double extortion method, BlackSuit encrypts sensitive data and demands ransoms, with detections in various sectors, highlighting it's evolving threat. Operating independently, BlackSuit's distribution methods include infected email attachments, torrent websites, malicious ads, and Trojans.

3AM

3AM, a recently surfaced ransomware discovered in August 2023, has seen limited usage but showcased a noteworthy incident where it was employed as an alternative to LockBit after the latter was blocked. Coded in Rust, marking it as a distinct malware family, 3AM follows a distinct sequence, targeting services before encrypting files and attempting to delete Volume Shadow copies. The group behind 3AM publicly revealed leak sites, listing victims from the United States and Malaysia, a move that raises speculation about their intentions.

NOTABLE CAMPAIGNS

2023 provided us with some notable campaigns that, unfortunately, caused major damage to organizations worldwide. While MOVEit was the most devastating one, some other campaigns are worth mentioning.

MOVEIT CAMPAIGN

The ongoing MOVEit campaign remains a prominent fixture in headlines, continually ensnaring new victims as it unfolds. This expansive campaign is a stark illustration of the potency of a supply chain attack, impacting many global companies. MOVEit, an instrumental managed file transfer (MFT) software employed widely across healthcare, finance, technology, and government sectors, touts its security through encryption and robust file transfer protocols for safe data exchange within and between teams and organizations.

However, within this seemingly secure software lie discovered vulnerabilities, exposing a path to remote code execution and potential data breaches. These loopholes have been exploited by the Cl0p ransomware group, tracing back to their exploitation of the MOVEit vulnerability since 2021, with evident attempts to extract data in 2022.

Cl0p, renowned for their adeptness at zero-day exploits such as the Accellion File Transfer Appliance (FTA) attacks in 2020 and 2021 and the targeting of GoAnywhere MFT servers in early 2023, has disclosed various compromised victims through the MOVEit flaw. Noteworthy companies like Norton, EY, and Zellis fell prey to this assault.

This extensive cyber incursion caused a ripple effect, impacting major entities to such an extent that the US government has offered a substantial reward for any information that links Cl0p's actions to a foreign government. Despite Cl0p's claims of data deletion from specific sectors such as governments, the military, and children's hospitals, their breach affected several US federal government agencies. The scale and repercussions of this attack continue to reverberate, with the Cl0p gang's actions drawing widespread attention and scrutiny, signifying the severity and depth of the MOVEit ransomware breach.

ROYAL RANSOMWARE HITS CITY OF DALLAS

The City of Dallas fell victim to a ransomware attack orchestrated by the Royal gang on May 3, triggering extensive network disruptions that compelled Dallas courts to remain shuttered until May 31. The Royal operators initially infiltrated the city's network by pilfering service account credentials, maintaining a persistent presence for a month before deploying the ransomware. Restoration efforts commenced on May 9 and concluded by June 13.

In the wake of this disruptive attack, the Dallas City Council sanctioned an $8.5 million budget for mitigation and recovery endeavors. Expenditures encompassed external cybersecurity expertise, identity theft and fraud protection, and breach notification services.

The City of Dallas publicly acknowledged the ransomware intrusion in May, highlighted by the unusual printing of ransom notes from network printers, unequivocally attributed to the Royal ransomware group. In their blog post, the Royal ransomware gang threatened to expose sensitive information, encompassing employee details, court cases, prisoner data, medical records, client information, and governmental documents.

The ramifications were far-reaching, affecting various city services and departments, including the Dallas police department, 311 customer service app, courts, water utilities, code compliance services, animal services, secretary's office, and development services. Subsequent reports from the Attorney General's office in August indicated that 26,212 individuals bore the brunt of the breach, exposing personal details such as names, addresses, social security numbers, and medical and health insurance information. Further investigation pushed the tally of affected individuals to 30,253, amplifying the gravity and scope of the breach.

LAS VEGAS HOTEL GIANTS HIT BY SCATTERED SPIDER

In September 2023, two major hotel and casino giants in Las Vegas, MGM Resorts International and Caesars Entertainment, fell victim to ransomware attacks. MGM Resorts encountered a "cybersecurity issue" that led to the shutdown of U.S. systems, impacting numerous MGM hotels and disrupting vital services like the company's website, app, reservations, ATMs, slot and credit card machines. While sensitive financial data remained secure, personal information, including names, contact details, driver's license and Social Security numbers, and passport details of pre-March 2019 customers were compromised, with a projected cost of around US$ 100 million. In contrast, Caesars Entertainment saw limited service disruption but suffered data theft from its loyalty program database, affecting 41,397 Maine residents. Scattered Spider ransomware group claimed responsibility, absconding with 6 terabytes of data. MGM declined ransom payment, working on recovery, while reports indicated Caesars paid 15 US$ million of the demanded 30 US$ million ransom for data protection.

BLACKCAT RANSOMWARE HIT WESTERN DIGITAL

In March, Western Digital encountered a ransomware attack linked to the ALPHV/BlackCat ransomware group, which they disclosed on April 3. Responding swiftly, they activated their protocols, restoring affected services and engaging law enforcement. The aftermath involved data theft and service disruptions affecting platforms like SanDisk and My Cloud, impacting customer access. BlackCat, a notable ransomware group in 2023, claimed responsibility for leaking alleged stolen data publicly on April 28, employing aggressive tactics such as sharing purported footage from a Western Digital video conference. Western Digital acknowledged the leaked data on May 5 and confirmed an ongoing investigation into these claims.

LOCKBIT ATTACK ROYAL MAIL

In early 2023, Royal Mail experienced a significant ransomware attack orchestrated by the LockBit group. The attack, involving LockBit's encryptors, severely disrupted Royal Mail's international shipping capabilities for approximately six weeks. LockBit initially demanded a ransom of £65.7 million ($79.85 million) for the return of stolen data.

Royal Mail, however, chose not to comply with these ransom demands, which were considered "absurd" by its directors. In response, LockBit published 44 gigabytes of Royal Mail's stolen data on the dark web in an attempt to extort money. Despite this pressure, Royal Mail maintained its stance against paying the ransom.

The financial impact on Royal Mail was significant, with substantial costs incurred for recovery from the attack. Meanwhile, LockBit continued its extortion attempts, reducing the ransom demand to £33 million, a decrease from the original £65 million. Royal Mail maintained its stance against paying the ransom. The company's decision not to comply with the ransom demands led to LockBit publishing the stolen data on the dark web

RANSOMWARE PREDICTIONS FOR 2024

With a rise of more than 50% in ransomware cases in 2023, there is no doubt that the ransomware industry is one of the most profitable and growing cybercrime industries today.

As this industry grows, it draws new and bold groups that want to make a name for themselves by developing high-quality ransomware services and tools.

The ransomware threat in 2024 should look even more intimidating for organizations worldwide as the veteran groups consistently compromise growing numbers of victims, and the newer groups, such as Akira, 8Base and Play, will improve and become more dominating in the industry.

It is important to understand ransomware groups' rise and fall every day, and given that some newcomers "survived" a whole year in this industry, it says a lot about their ambitions and intentions to become a permanent player in this game.

CONCLUSIONS

2023 is a new all-time high for the ransomware industry. With permanent families such as LockBit ALPHV and Cl0p, this industry caused severe damage to organizations worldwide.

In addition to that, the newcomers this year were introducing quality tools and products that helped them become permanent threats as well.

Although law authorities worldwide are still doing their best to stop this menace from continuing to evolve, the industry is still growing rapidly.

The Cyberint Research Team assessment that as much as 2023 was very successful for the ransomware groups; unfortunately, 2024 will be even better.

Cyberint

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
6 The Broadway, Mill Hill NW7 3LL, London

USA – TX

Tel: +1-646-568-7813
7700 Windrose Plano, TX 75024

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

USA - MA

Tel: +1-646-568-7813
22 Boston Wharf Road Boston, MA 2210

JAPAN

Tel: +81 080-6611-7759
27F, Tokyo Sankei Building, 1-7-2 Otemachi,
Chiyoda-ku, Tokyo 100-0004

ABOUT CYBERINT

Cyberint's impactful intelligence solution fuses real-time threat intelligence with bespoke attack surface management, providing organizations with extensive integrated visibility into their external risk exposure.

Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, the solution allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier.

Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities, and more, ensuring continuous external protection from cyber threats.