Cyberint

Ransomware Q2 2024 Report

July 2024

Table of Contents

Executive Summary 4
Statistics 4
Top Families 5
Lockbit3.0 6
Top 3 Countries Attacked by Lockbit3.0 6
Top 3 Sectors Attacked by Lockbit3.0 6
Play 7
Top 3 Countries Attacked by Play 7
Top 3 Sectors Attacked by Play 7
RansomHub 7
Top 3 Countries Attacked by RansomHub 8
Top 3 Sectors Attacked by RansomHub 8
Top Countries 8
Top Sectors 9
Newcomers 10
Underground 10
SpaceBears 10
Flocker 11
Embargo 11
DarkVault 12
dAn0n 13
APT73 13
Quilong 14
HelloGookie 14
Apos 15
ArcusMedia 15
Zerotolerance 16
Brain Cipher 16

Table of Contents

Arrests 17

Massive police operation across Europe dismantles ransomware networks and results in 4 arrests 17

LockBitSupp Identity Revealed - $10 million reward for his arrest 17

Threat actor linked to the Scattered Spider group arrested in Spain 18

Police arrest Conti and LockBit ransomware crypter specialist 18

New Trends 19

Fall of Major Ransomware Groups Sparks Rapid Rise of New Threats 19

Major Incidents 20

Keytronic confirms data breach after Black Basta gang leaks stolen files 20

London hospitals have postponed over 800 operations following a ransomware attack attributed to the Qilin Ransomware group 20

The city of Wichita shuts down its IT network after a ransomware attack 21

Indonesian National Data Center Breach 22

Conclusions 23

Contact us 24

About **Cyberint** 24

Executive Summary

Although 2024 began with a Q1 decline in the frequency of ransomware attacks, the second quarter was underscored by a return to a much more intimidating world of ransomware attacks globally.

While the number of ransomware attacks decreased in Q1 2024 to 1,048 cases, in Q2 2024, it increased to 1,277 cases. This is almost a 21.5% increase compared to Q1 2024.
One reason could be the intervention of law enforcement, as demonstrated by LockBit arrests and the identity reveal of group admins and other cybercriminals' infrastructure seizure. As a result, big ransomware operations were split into smaller ones, creating more competition between ransomware gangs.

The emergence of new ransomware groups in 2024, as evidenced by the emergence of 27 new groups by the second quarter, suggests a sustained and evolving threat landscape. These groups, such as **ArcusMedia**, **APT73**, **dAn0n**, and **DragonForce**, pose fresh challenges to cybersecurity professionals and organizations worldwide.
Interestingly, this quarter, the top 10 ransomware groups were responsible for 60% of all attacks. Compared to previous quarters, this highlights the significant influence of new ransomware groups and the highest number of active groups on record, indicating a decline in dominance by specific groups in the ransomware landscape.

Nevertheless, it is no surprise that the U.S. continues to be the country most targeted by ransomware, while business services is the most targeted sector, similar to last year's stats.

There is no doubt that the new faces introduced to the industry, along with ongoing attacks on businesses around the world, claimed many victims. This, combined with the consistency of the industry's leaders - LockBit3.0, Play, RansomHub, IncRansom, and Medusa - led to devastating results for companies worldwide, such as **Keytronic**, **London hospitals**, and others.

Statistics

As noted, the ransomware sector recorded 1,277 victims this quarter, marking an increase of approximately 21.5% compared to the first quarter of 2024.

Top Families

While it was a successful quarter for the entire ransomware industry, three families stood out. As expected, ***LockBit3.0*** remains the most dominant ransomware group, with 211 new victims as they claim 16.5% of all ransomware cases.

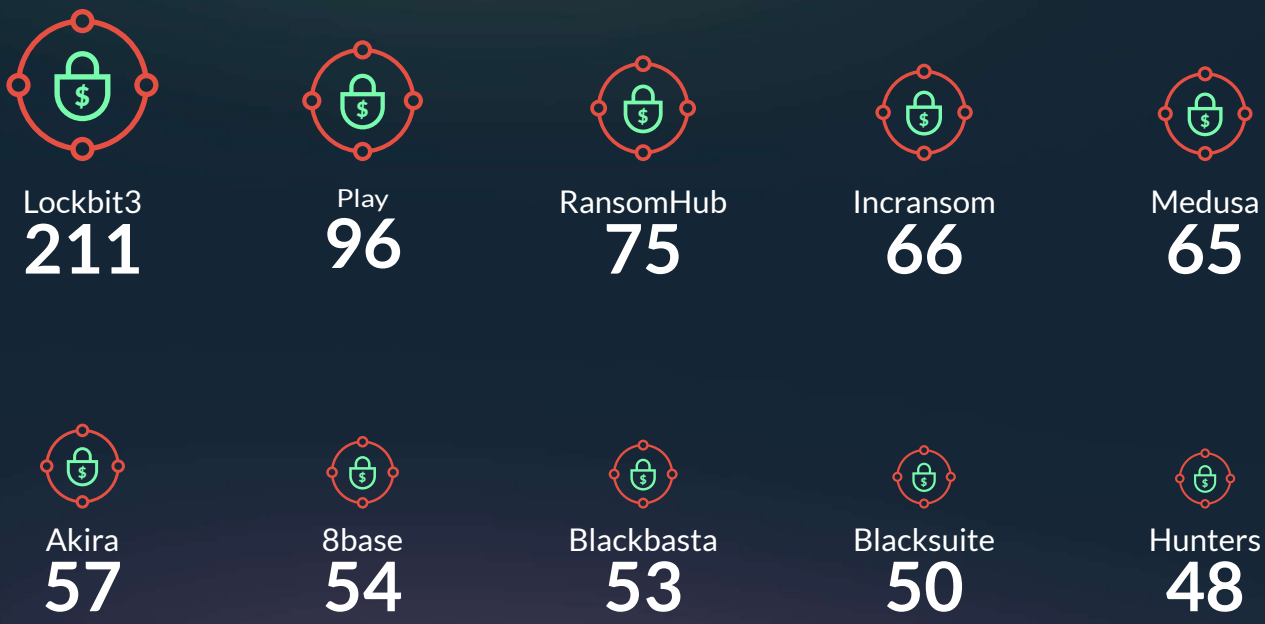
Coming second is the ***Play*** ransomware group, which claimed a significant 96 victims, 7.5% of all ransomware cases. Play continues to be a dominant power in the ransomware landscape.

Ransomware as a Service (RaaS) is a business model where affiliates pay to use ransomware attacks developed by operators. It mirrors the Software-as-a-Service (SaaS) model. This approach is significant in the global proliferation and persistence of ransomware attacks. The rise of RaaS models has notably impacted the ransomware landscape, exemplified by the ***RansomHub*** group, which recently claimed the third spot with 75 victims this quarter.

In the current landscape, where ransomware groups are closing their operations much faster than previously observed, a group that consistently executes dozens of successful ransomware attacks every month and sustains its activities for over a year can be considered a veteran. Therefore, the fourth and fifth places are also reserved for other veteran groups: the ***IncRansom*** group, which had 66 victims this quarter, and the Medusa group, which had 65 victims.

Figure 1

Top 10 Ransomware Families in Q2



Lockbit3.0

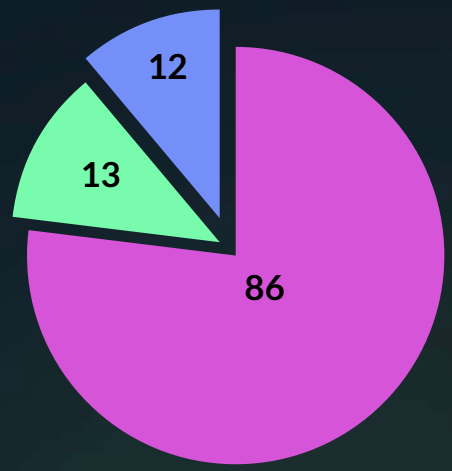
On Feb. 19, 2024, Operation Cronos, a targeted law enforcement action, caused outages on LockBit-affiliated platforms, significantly disrupting the notorious ransomware group's operations.

The UK, US, and Australia have revealed the identity of Dmitry Khoroshev, a Russian national and the leader of the once-notorious LockBit ransomware group, following an international disruption campaign led by the National Crime Agency (NCA).

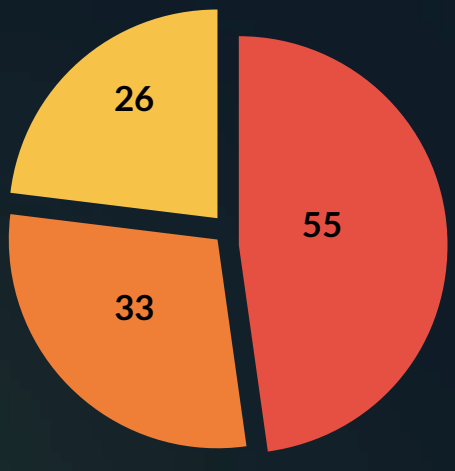
Dmitry Khoroshev, also known as LockBitSupp, who previously operated in secrecy and offered a $10 million reward to uncover his identity, is now facing sanctions announced by the FCDO in coordination with the US Department of the Treasury's Office of Foreign Assets Control (OFAC) and the Australian Department of Foreign Affairs.

Over the past three months, the group has made efforts to regroup; however, according to the NCA's assessment, their operations are currently running at limited capacity due to this investigation, resulting in a substantial decrease in the global threat posed by LockBit. LockBit has launched a new leak site where they have exaggerated their activity by listing victims targeted before the NCA gained control of their services in February, and have also claimed responsibility for attacks carried out using other ransomware strains. Despite these major operations against the group, LockBit continued its global onslaught against organizations, maintaining its position as a dominant force in ransomware operations.

Top 3 Countries Attacked by Lockbit3.0

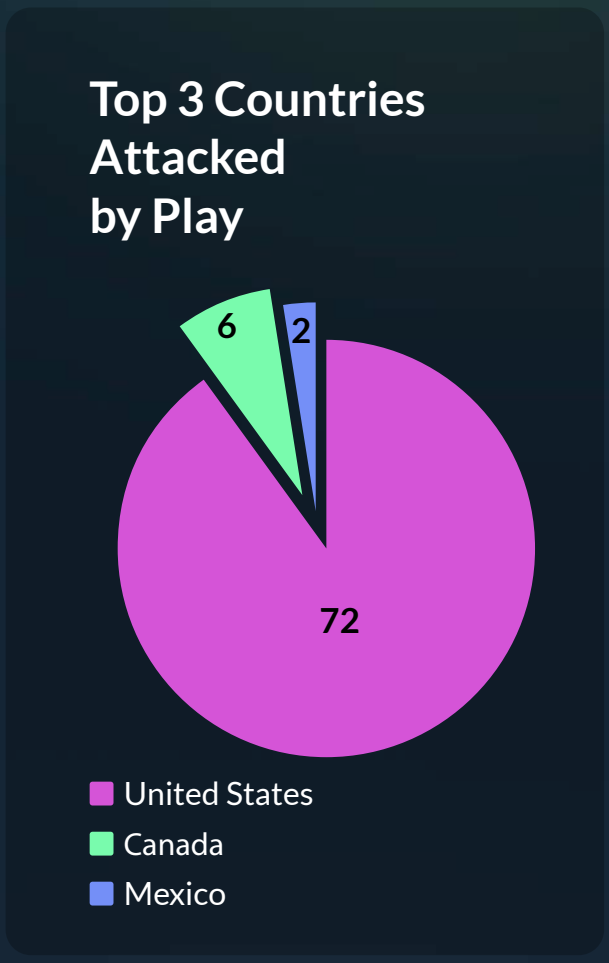


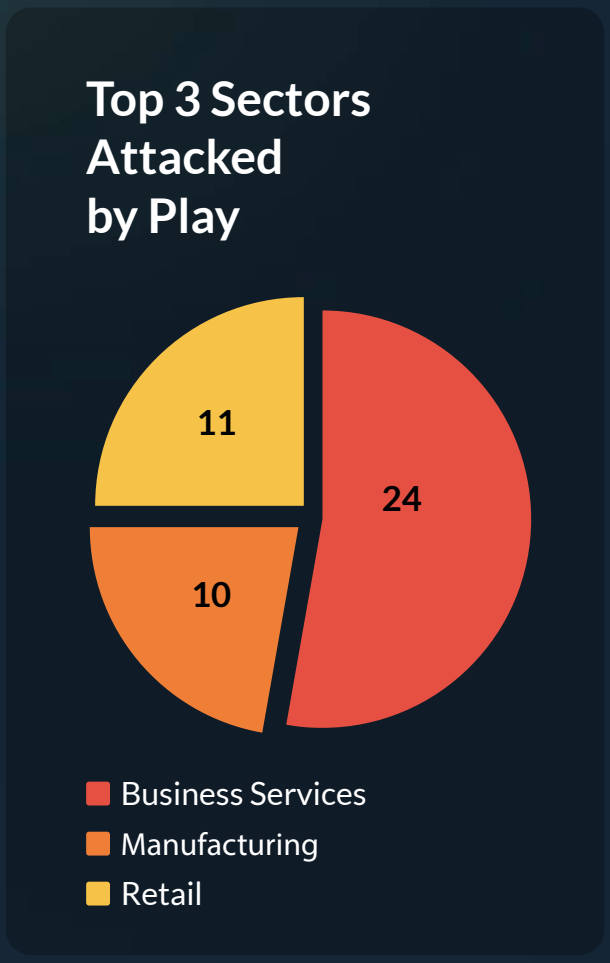
Top 3 Sectors Attacked by Lockbit3.0



Play

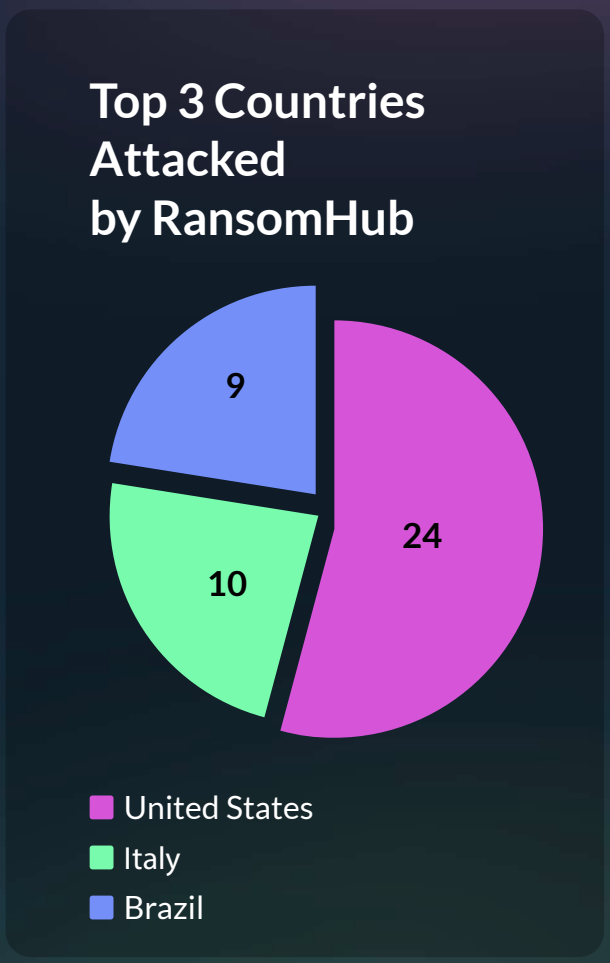
The ransomware syndicate responsible for numerous destructive assaults on significant American municipalities purportedly executed over 300 successful incidents since June 2022. Among the notable attacks, this quarter was the breach targeting the Swiss government, where approximately 65,000 files were pilfered by the Play ransomware gang during an assault on an IT vendor. Like BlackBasta, there are no indications that this systematic group intends to halt its operations. An interesting point is that in January 2024, this group only managed to attack 3 victims, which is the lowest number in the past 2 years.

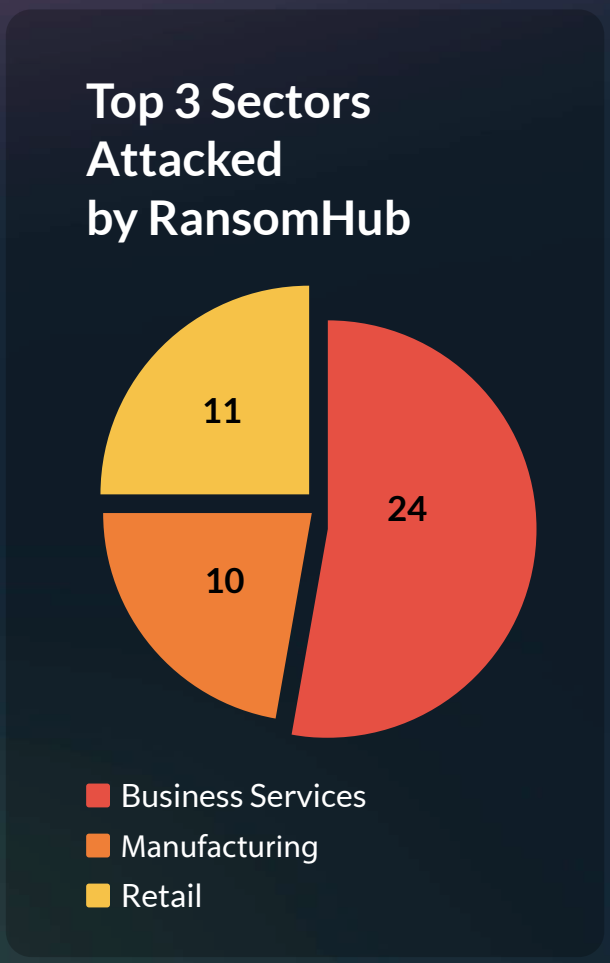




RansomHub

The RansomHub ransomware group has emerged as a significant player in the ransomware landscape, making bold claims and substantiating them with data leaks. In February 2024, RansomHub posted its first victim, the Brazilian company YKP. The group has since successfully attacked over 100 organizations worldwide. RansomHub offers affiliates a 90% commission rate, which is higher than the typical 80-90% range seen in the RaaS market. This lucrative rate is likely to attract seasoned affiliates from other platforms, leading to a surge in RansomHub-related infections and victims, as we've seen in this quarter, where they successfully attacked 75 victims worldwide.





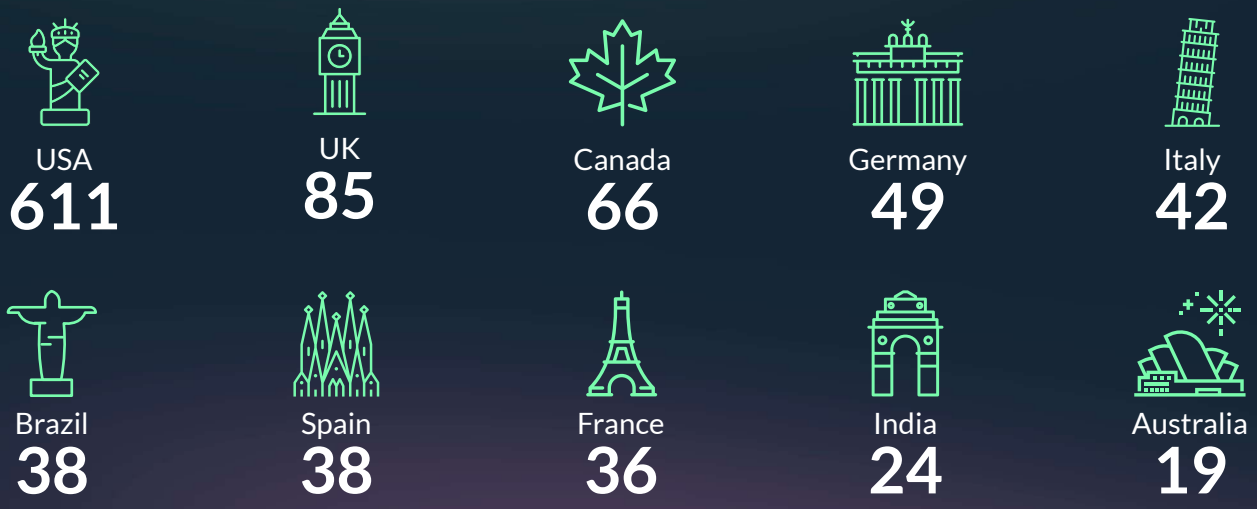
Top Countries

Regarding the most targeted countries (Figure 2), the U.S. remains the number one targeted country globally, with good reason. The world's number one economy was the victim of ransomware attacks this quarter in 47.8% of total cases, i.e., 611 cases.
The second most targeted country this quarter is the United Kingdom, with 85 cases, lagging far behind the U.S.

Finally, Canada is in third place with 66 ransomware cases this quarter.
Even when focusing on the top three countries, there is no doubt that the U.S. is the most profitable country for threat actors.

Figure 2

Top 10
Most Targeted Countries



Top Sectors

As expected, the business services sector was the most targeted in Q2, with 28.5% of the ransomware cases, followed by the retail and manufacturing sectors, with 17% and 11.5%, respectively (Figure 3).

Figure 3

Top 10
Targeted Sectors by Ransomware in Q2 2024

Newcomers

Underground

The Underground ransomware group surfaced in May 2024, quickly posting 13 victims on its official Data Leak Site (DLS). In contrast, June saw fewer victims, with only 2 reported. 6 of the victims are from the United States, two from South Korea, and the rest from Germany, Slovakia, UAE, Taiwan, Singapore, Spain, and Canada.

SpaceBears

Within the cybersecurity community, it is believed that SpaceBears, a ransomware group reportedly based in Moscow, Russia, has recently claimed responsibility for several high-profile cyberattacks, showcasing their advanced tactics in the cyber threat landscape.

The group provides detailed instructions for visitors to their Data Leak Site (DLS) on what to do if they believe their data has been compromised. They claim that upon receiving payment, they will remove the published data, delete it from their servers, and provide a decryption tool for the encrypted files. Additionally, they offer guidance on how to prevent similar attacks in the future.

SpaceBears lists 20 organizations on their DLS, most of which are medium to small-sized enterprises. The organizations are spread across several countries: 7 in the US and the others in Portugal, Canada, Germany, Norway, Morocco, Singapore, Ecuador, and Fiji. Sector-wise, the victims include manufacturing companies, small technology solutions providers, and healthcare-related companies.

Flocker

The Flocker (aka Fsociety) ransomware group emerged at the end of April, listing four victims on its official DLS in just two days. The group continued to operate and listed more victims on its DLS in June.

Embargo

Embargo ransomware, created using the Rust programming language, is a new group that emerged in April 2024. The threat actors (TAs) behind this ransomware employ double extortion tactics, exfiltrating sensitive information from the victim's systems before encrypting the data. One notable victim, "Aussie lender Firstmac," has garnered significant media attention.

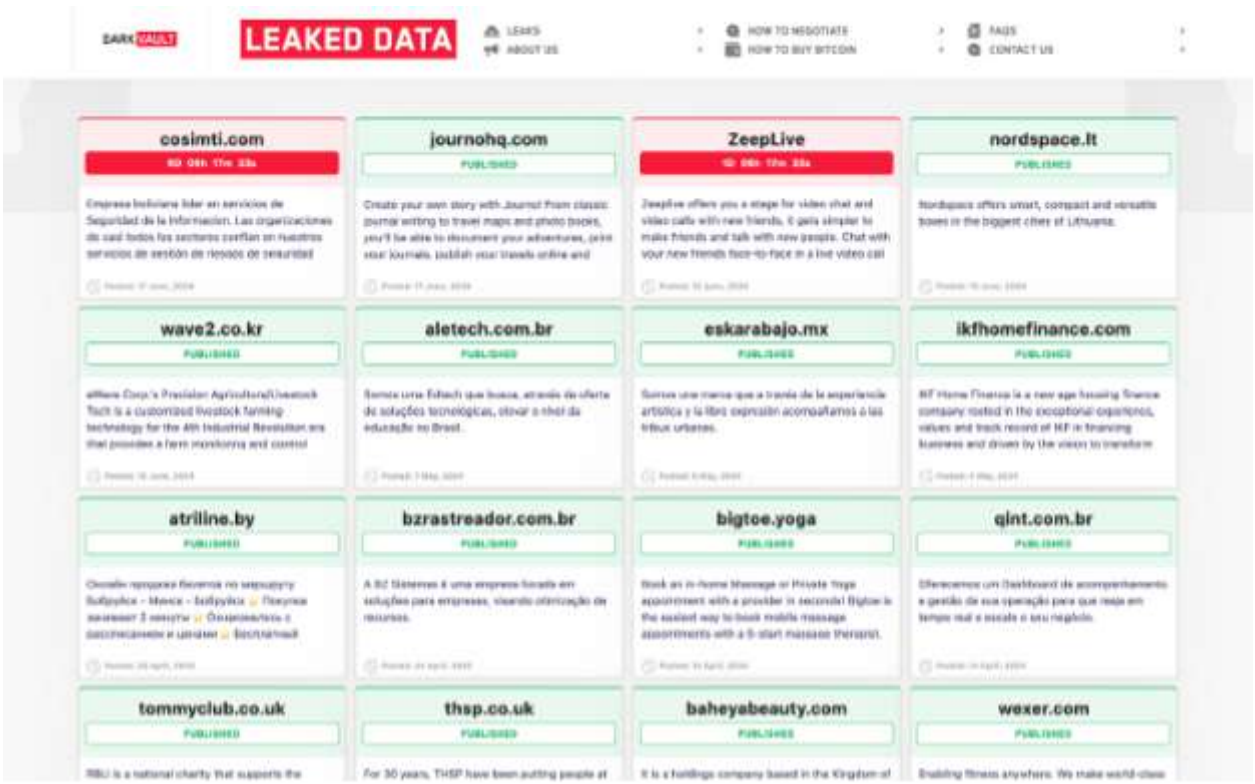
According to Embargo, the group stole over 500 gigabytes of data, including "full databases, source codes, and sensitive customer data."

DarkVault

DarkVault recently published data from 19 victims on its leak site in April 2024. This rapid publication rate indicates either previously undisclosed activities or a well-coordinated team capable of quickly executing multiple attacks. Their targets are diverse, spanning industries such as surveillance systems, fitness, fashion, and healthcare insurance, and are located in countries including the US, India, Sri Lanka, and the UK.

Among their notable victims are the UK-based charity Tommy Club, which raises funds for various divisions of the Royal British Legion, and Sandip University in Nashik, India. Despite their brief history, DarkVault's ability to compromise significant targets has raised concerns within the cybersecurity community.

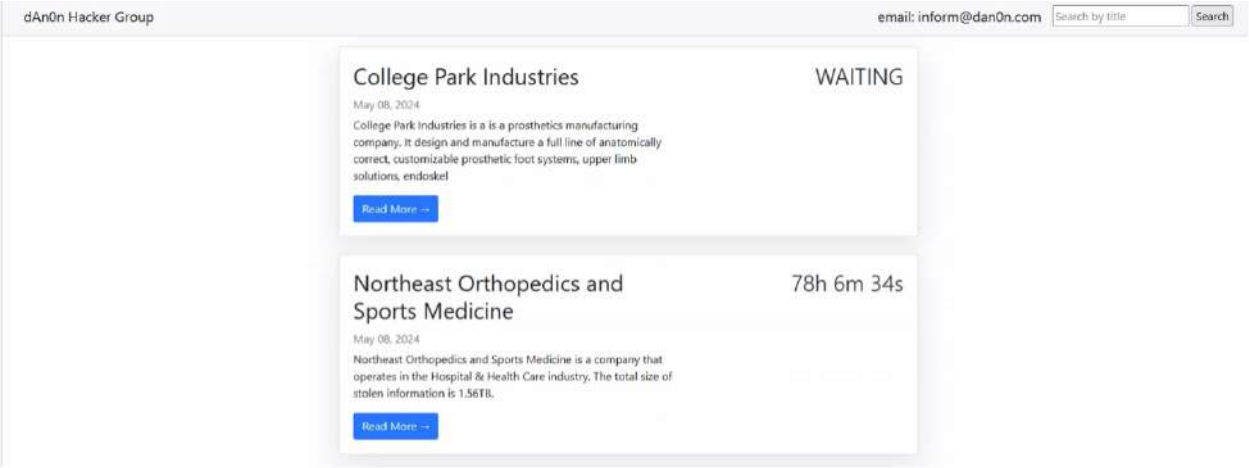
There has been speculation about DarkVault's connection to LockBit due to similarities in their activities and site design. However, no concrete evidence supports this theory, and it is equally plausible that DarkVault is a new entity or a rebranding effort by experienced cybercriminals seeking to capitalize on LockBit's notoriety.



dAn0n

This group surfaced at the end of April and has since posted information about 14 victims on their data leak site. Of these victims, 10 are based in the United States, with business services as the primary sector targeted.

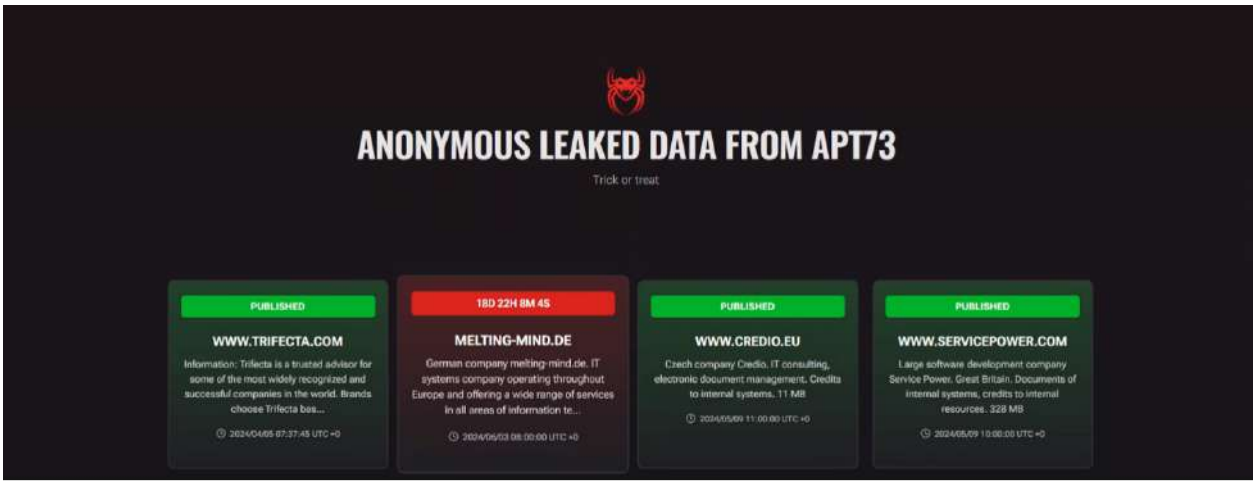
A notable observation from their data leak site is the apparent lack of emphasis on design or a visible logo, which may suggest that the group prioritizes attack methodologies over branding and has a smaller team.



APT73

In contrast to other naming conventions that researchers use to identify threat actors, this group has chosen to refer to themselves as "APT" (Advanced Persistent Threat) followed by a number, specifically APT73, a ransomware group modeled on LockBit. This was observed through similarities in their "Contact Us," "How to Buy Bitcoin," and "Web Security & Bug Bounty" pages, which closely resemble the layout of the LockBit Data Leak Site (DLS). The content on these pages mirrors that of LockBit, indicating that this is essentially a LockBit-style Ransomware Data Leak Site (DLS). One notable difference is the "Mirrors" section, which lacks any active mirrors, unlike LockBit, highlighting a level of amateurism within this group.

To date, the group has targeted a total of 12 victims in various locations worldwide, including Germany, Canada, the Czech Republic, and the United States (twice). Their attacks have been exclusively focused on the business services sector.



Quilong

The Qiulong ransomware gang, a new cyber threat actor, has emerged, targeting Brazilian victims. The group announced its presence by compromising two entities in Brazil: Dr. Lincoln Graca Neto and Rosalvo Automoveis.

The attackers created a website for posting data breaches, including summaries of the compromised targets and mocking content directed at Dr. Lincoln Graca Neto. Dr. Neto either rejected the ransom demand or negotiated in bad faith, as he has not paid the ransom.

Although this is the first known exploit of the Qiulong gang, their technical capabilities are evident in their ability to target multiple victims and potentially compromise sensitive data. These attacks suggest that the Qiulong gang aims to become a significant player in the ransomware threat landscape.

So far, the group has posted 8 victims on their DLS; 7 of them are from Brazil, and one from Canada.

HelloGookie

The rebranding of ransomware operation HelloKitty to HelloGookie coincided with the publication of internal Cisco network data exfiltrated from a 2022 attack, exfiltrated source code for several CD Projekt Red games from a 2021 attack, and four private decryption keys for other intrusions that involved an older iteration of its ransomware encryptor.

HelloGookie, which has not yet touted any new victims, noted on its data leak site that it had a list of Cisco NTLM hashes that were exfiltrated during a breach, which was believed to be conducted by the Yanluowang ransomware attack.

Meanwhile, more than 400GB of uncompressed information was included in the exposed CD Projekt Red data, which included source code for the company's "The Witcher 3," "Cyberpunk," and "Gwent" titles, as well as numerous console SDKs and build logs, said Sventek, one of the developers who compiled Witcher 3 from the leaked data.

Apos

The Apos ransomware gang emerged on April 2024. They listed 4 victims on their DLS, other than which, it looks like the group hasn't been active over the last 2 months. This could indicate a one-time operation or a relation to another group. Two of the victims are from Brazil, one from India and one from France.

ArcusMedia

The Arcus Media ransomware group, active since May 2024, is a relatively new threat actor known for its direct and double extortion methods. They gain initial access through phishing emails, deploy custom ransomware binaries, and use obfuscation techniques to evade detection.

Their tactics include phishing emails with malicious attachments, obfuscated scripts for executing payloads, and privilege escalation using tools like Mimikatz.

The group attacks various sectors and countries; Brazil is the most targeted country to date, with 6 notable attacks. The most targeted sector is business services.

The group admin is a threat actor who manages his account in the Exploit Russian hacking forum. This information, along with the actor's name, could indicate the group's location or political position in Russia.

Zerotolerance

According to our resources, this individual attacked the Republic Bank of Argentina only once, in May 2024.

Brain Cipher

Brain Cipher is a recently launched ransomware operation that launched attacks on organizations globally earlier this month, June 2024.

On June 20, 2024, Brain Cipher attacked Indonesia's National Data Center (Pusat Data Nasional or PDN), disrupting various government services. This ransomware significantly impacted public services, including immigration processing at Jakarta's Soekarno-Hatta International Airport, causing long queues and delays.

The attackers demanded a ransom of $8 million to decrypt the compromised data. Over 210 institutions, including national and local government offices, were affected.

The encryptor is based on the leaked LockBit3.0 encryptor, which has been thoroughly analyzed. Unless Brain Cipher has modified the encryption algorithm, there are no known methods to recover files for free.

Arrests

Massive police operation across Europe dismantles ransomware networks and results in 4 arrests.

THE HAGUE, Netherlands (AP) - In the largest international operation ever against ransomware, police coordinated by the European Union's justice and police agencies have dismantled computer networks responsible for spreading ransomware through infected emails.

The EU's judicial cooperation agency, Eurojust, announced on Thursday that police arrested four "high value" suspects, dismantled over 100 servers, and seized control of more than 2,000 internet domains.

This major operation, codenamed Endgame, involved coordinated efforts in Germany, the Netherlands, France, Denmark, Ukraine, the United States, and the United Kingdom. According to Europol, three suspects were arrested in Ukraine and one in Armenia, and searches were conducted in Ukraine, Portugal, the Netherlands, and Armenia.

LockBitSupp Identity Revealed - $10 million reward for his arrest

The UK, US, and Australia have revealed the identity of Dmitry Khoroshev, a Russian national and the leader of the once-notorious LockBit ransomware group, following an international disruption campaign led by the National Crime Agency (NCA). Dmitry Khoroshev, also known as LockBitSupp, who previously operated in secrecy and once offered a $10 million reward to anyone who could reveal his identity, is now facing sanctions announced by the FCDO in coordination with the US Department of the Treasury's Office of Foreign Assets Control (OFAC) and the Australian Department of Foreign Affairs.

These sanctions include asset freezes and travel bans. Additionally, the US has unsealed an indictment against Khoroshev and is offering a reward of up to $10 million for information leading to his arrest or conviction.

These actions are part of an extensive investigation into the LockBit group conducted by the NCA, FBI, and other international partners forming the Operation Cronos taskforce.

Threat actor linked to the Scattered Spider group arrested in Spain

A 22-year-old British national allegedly linked to the Scattered Spider hacking group and responsible for attacks on 45 U.S. companies has been arrested in Palma de Mallorca, Spain. The suspect is believed to be a leader of a cybercrime gang focused on stealing data and cryptocurrencies from organizations and extorting them to prevent the publication of sensitive data. Investigators report that the group stole $27,000,000 worth of cryptocurrencies using this scheme.

The arrest followed an investigation initiated by a tip from the FBI, which led to the issuance of an International Arrest Warrant (OID). The Spanish police arrested the suspect on May 31, 2024, at Palma airport as he was about to depart for Naples, Italy. During the arrest, his laptop and mobile phone were confiscated for forensic examination. Authorities have not yet disclosed details about the specific threat group, but VX-Underground alleges without confirmation that the suspect is "Tyler," a SIM swapping specialist from the notorious Scattered Spider group.

Scattered Spider is a loose-knit collective of English-speaking cybercriminals known for accessing their targets' networks through social engineering, phishing, multi-factor authentication (MFA) fatigue, and SIM swapping. Some members of this group have also acted as affiliates with the Russian-speaking BlackCat ransomware gang.

In September 2023, Scattered Spider breached entertainment giant MGM Resorts, deploying a BlackCat/ALPHV encryptor, stealing data, and causing significant operational disruption.

Police arrest Conti and LockBit ransomware crypter specialist

The Ukraine cyber police arrested a 28-year-old Russian man in Kyiv for collaborating with the Conti and LockBit ransomware operations. He specialized in making their malware undetectable to antivirus software and conducted at least one attack himself.

Supported by information from the Dutch police, the investigation linked the man to a ransomware attack on a Dutch multinational. He was arrested on April 18, 2024, as part of Operation Endgame, which targeted various botnets and their operators.

The suspect developed custom crypters to make ransomware payloads appear as safe files, selling these services to Conti and LockBit. The Dutch police confirmed his involvement in a 2021 ransomware attack using a Conti payload. During the arrest, authorities seized computer equipment, mobile phones, and handwritten notes. The investigation is ongoing, and the suspect, charged under Part 5 of Article 361 of the Criminal Code of Ukraine, faces up to 15 years in prison.

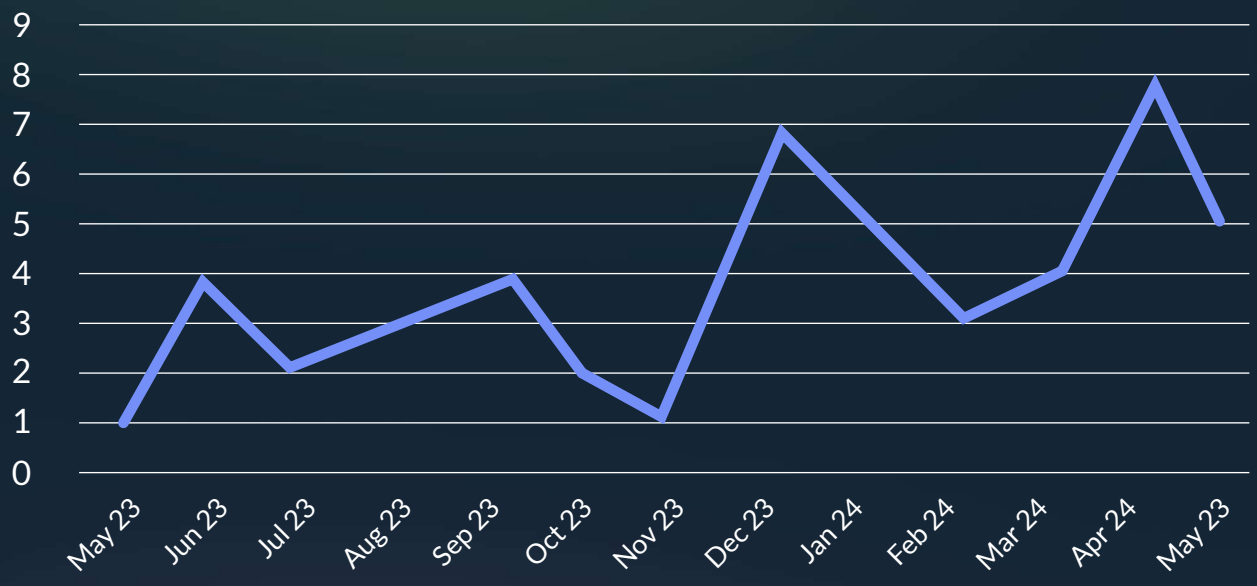
New Trends

Fall of Major Ransomware Groups Sparks Rapid Rise of New Threats

In 2023, international law enforcement agencies intensified their efforts against ransomware, resulting in the decline of groups such as Hive, Ragnar Locker, and the collapse of ALPHV (BlackCat). These actions underscore the growing challenges faced by ransomware groups. The significant February 2024 operation targeting LockBit, which included arrests and the seizure of data leak sites and servers, represents one of the largest law enforcement actions taken against a major ransomware operation.

Data from leak sites revealed the emergence of at least 25 new ransomware groups in 2023, highlighting the ongoing appeal of ransomware as a lucrative criminal activity. However, despite the appearance of new groups like Toufan, Darkrace, and CryptNet, many of these threat actors disappeared during the second half of the year.

New Emerging Ransomware Groups



We are only at the end of the second quarter of 2024, and we've already seen 25 new ransomware groups posting at least one victim on their data leak site.

Major Incidents

Keytronic confirms data breach after Black Basta gang leaks stolen files

Keytronic, a major manufacturer of printed circuit board assemblies (PCBA), has confirmed a data breach after the Black Basta ransomware gang leaked 530GB of stolen data. Initially known for making keyboards and mice, Keytronic revealed in an SEC filing that a cyberattack on May 6 disrupted their operations, halting domestic and Mexican operations for two weeks. The attack resulted in the theft of personal information, which the company is now notifying affected parties and regulatory agencies about.

The SEC filing highlighted that the cyberattack and subsequent production loss will significantly impact Keytronic's financial situation in the fourth quarter ending June 29, 2024. The company incurred approximately $600,000 in expenses to hire external cybersecurity experts, and this figure could continue to rise. While Keytronic did not name the perpetrators, Black Basta has claimed responsibility for leaking sensitive data, including employees' passports, social security cards, customer presentations, and corporate documents.

London hospitals have postponed over 800 operations following a ransomware attack attributed to the Qilin Ransomware group.

At the beginning of June NHS England announced that the Synnovis ransomware attack forced multiple London hospitals to cancel hundreds of planned operations and appointments. Synnovis, a partnership between SYNLAB UK & Ireland, Guy's and St Thomas' NHS Foundation Trust, and King's College Hospital NHS Foundation Trust, was locked out of its systems on June 3 by an attack linked to the Qilin ransomware group. This disruption significantly impacted procedures and operations, particularly blood transfusions and tests. Nevertheless, emergency services like A&E, urgent care centers, and maternity departments remained open.

The scale of the impact was revealed on Friday, with more than 800 planned operations and 700 outpatient appointments needing to be rescheduled across the two most affected trusts. Synnovis is working on restoring its IT systems, but full recovery will take time, causing ongoing disruptions in the coming months. Additionally, NHS Blood and Transplant (NHSBT) warned of blood shortages in London hospitals, urging O-positive and O-negative blood donors to help replenish reserves essential for urgent operations and procedures. Despite the distress caused by these delays, patients are advised to keep their appointments unless notified otherwise.corporate documents.

The city of Wichita shuts down its IT network after a ransomware attack

The city of Wichita, Kansas revealed that it had to close parts of its network following a ransomware attack over the weekend. With a population of 400,000, Wichita ranks among the top 50 largest cities in the United States.

In a rare act of transparency, city officials confirmed that the attack occurred on Sunday, May 5th, when ransomware encrypted IT systems. To prevent further spread, the city promptly shut down its computer network.

It remains unclear if any data was stolen, though ransomware groups typically exfiltrate data from compromised networks before encrypting it.

Officials on the city of Wichita's website stated, "We are conducting a thorough review and assessment, including evaluating any potential data impact. Such assessments take time."

BleepingComputer has confirmed that city services' online payment systems, including water bills and court citations, are offline. Despite this disruption, first responders continue to operate, and the police and fire departments are implementing business continuity measures as needed.
While the specific ransomware gang responsible for the attack has not been disclosed, the city has notified local and federal law enforcement agencies, who are assisting in the response.

Indonesian National Data Center Breach

On June 20, the National Data Center (PDN) in Jakarta Indonesia suffered a ransomware attack, resulting in delays for airport immigration services and new student registration. The attackers are demanding a ransom of $8 million, approximately Rp 131 billion, to return the stolen data.

The ransomware used in this incident, known as Brain Cipher, is a new development of the LockBit 3.0 ransomware. In 2023, the LockBit hacker group also disrupted the systems of Bank Syariah Indonesia (BSI).

The cyber attack caused significant disruptions to the immigration office's online services nationwide over the past week, as well as the online announcement of new student registration results (PPDB).

According to data from IT security company Vaksincom, by mid-2024, 10 major institutions had been victims of ransomware attacks, including both private and government entities. These victims come from various sectors such as logistics, shopping centers, consumer finance, banks, financial services, IT services, transportation, and stock brokerage firms.

Conclusions

The first half of 2024 has shown a dynamic and volatile ransomware landscape. After a brief decline in Q1, Q2 saw a significant resurgence, with a 21.5% increase in attacks, reaching 1,277 cases. This rise is partly due to law enforcement interventions that fractured large ransomware operations, leading to more competition among smaller groups.

The emergence of 27 new ransomware groups underscores the evolving threat environment, posing fresh challenges to cybersecurity professionals. Notably, the top 10 ransomware groups accounted for 60% of all attacks, indicating a significant yet diversified influence within the ransomware ecosystem. Despite ongoing efforts to combat these threats, the United States remains the most targeted country, and the business services sector continues to be the most affected.

Veteran groups like LockBit3.0, Play, and RansomHub continue to dominate, while new groups such as ArcusMedia and APT73 point to persistent and growing dangers. The significant disruptions caused by these groups to major organizations like Keytronic and London hospitals demonstrate the devastating impact on global businesses and infrastructure.

Arrests and law enforcement actions have led to temporary disruptions to major players, as seen with LockBit3.0. However, the continued rise of new groups suggests that ransomware remains a lucrative and persistent threat. The arrests of high-profile figures and significant police operations signal progress and highlight the ongoing challenge of dismantling these networks.

Overall, the first half of 2024 has reaffirmed the resilience and adaptability of ransomware groups. Continued vigilance, international cooperation, and innovative cybersecurity measures are crucial in addressing the ever-evolving threat landscape.

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
3rd Floor, Great Titchfield House
14-18 Great Titchfield Street,
London, W1W 8BD

USA – TX

Tel: +1-646-568-7813
7250 Dallas Pkwy STE 400
Plano, TX 75024-4931

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: +81-3-3242-5601
27F, Tokyo Sankei Building, 1-7-2 Otemachi,
Chiyoda-ku, Tokyo 100-0004

ABOUT CYBERINT

Cyberint, the Impactful Intelligence company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Cyberint Argos platform's patented technology provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: https://Cyberint.com.