Cyberint

Impactful Intelligence

Q1 RANSOMWARE REPORT

April 2024

TABLE OF CONTENTS

EXECUTIVE SUMMARY

2024 began with a decline in the frequency of ransomware attacks worldwide. However, these attacks still continues to pose the leading threat to both businesses and individuals.

While the numbers skyrocketed in Q4 2023 with 1309 cases, in Q1 2024, the ransomware industry was down to 1,048 cases. This is more than a 22% decrease in ransomware attacks compared to Q4 2023.

Two reasons for this drop could be the intervention of law enforcement, as observed with LockBit and ALPHV gangs, and the decrease in ransom payments, prompting ransomware groups to retire and seek alternative sources of income.

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

There is no doubt that the new faces that were introduced to the industry, along with the ongoing attacks on businesses around the world, were able to claim many victims even though the number decreased. Combined with the consistency of the industry leader - LockBit3.0 - we saw devastating results for companies worldwide, such as **Hyundai Motor, Duvel Beers**, and others.

Furthermore, during this quarter, there numerous new ransomware groups emerged, a cautionary warning to businesses worldwide, as they could rise to prominence in the ransomware industry in the future.

STATISTICS

As noted, the ransomware sector recorded 1,048 victims this quarter, marking a decrease of approximately 22% compared to the fourth quarter of 2023.

TOP FAMILIES

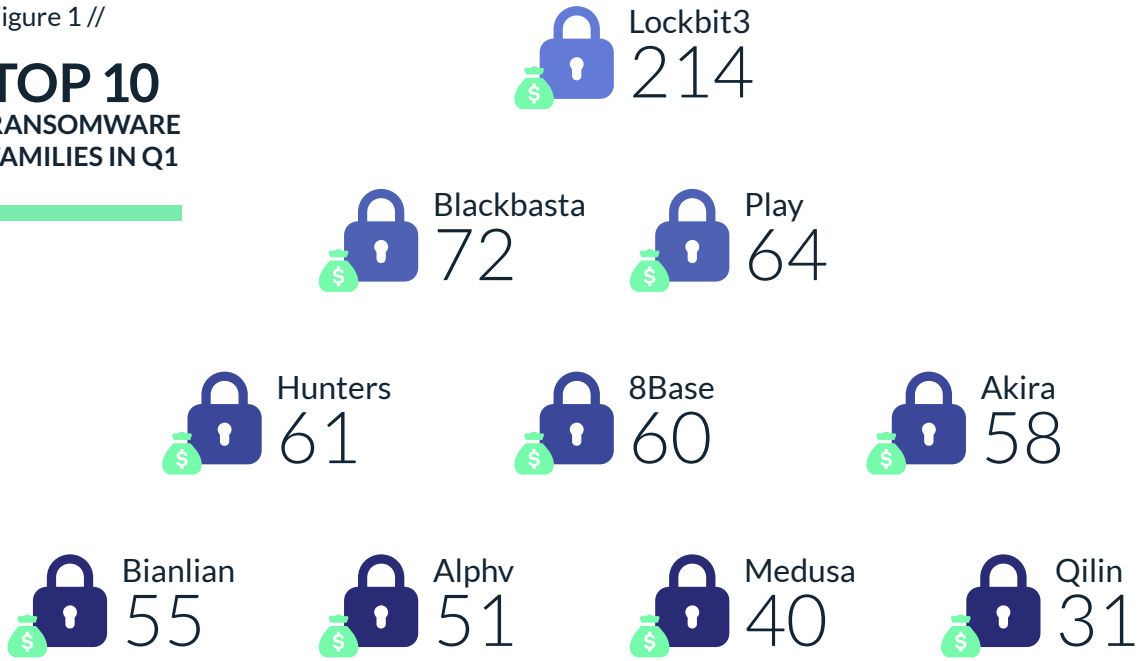
While it was a successful quarter for the entire ransomware industry, three families stood out. As expected, **LockBit3.0** remains the most dominant ransomware group, with, they claim, 213 new victims, 20.6% of all ransomware cases.

Coming in second is the **Blackbasta** group, which was able to claim a significant 75 victims.

In the current landscape, where ransomware groups are closing down their operations at a much quicker rate than previously observed, a group that consistently executes dozens of successful ransomwares attacks every month and has sustained its activities for over a year can rightfully be deemed a veteran. And the third place spot goes to another veteran – The **Play** group – with 74 victims this quarter.

Figure 1 //

TOP 10
RANSOMWARE FAMILIES IN Q1



LOCKBIT3.0

In February, an international operation culminated in the arrest of at least three associates of the infamous LockBit ransomware syndicate in Poland and Ukraine. Despite these arrests, the group continued its global onslaught against organizations, maintaining its position as a dominant force in the realm of ransomware operations. This resilience underscores the group's formidable power and capabilities, as well as the robust security measures surrounding its operations that ensurs its continued viability and potentially promising future, as evidenced by quarterly trends over recent years

Figure 2 //

TOP 3
ATTACKED COUNTRIES BY LOCKBIT3.0

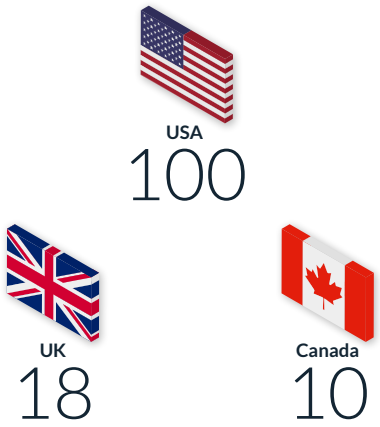


Figure 3 //

TOP 3
ATTACKED SECTORS BY LOCKBIT3.0

BLACKBASTA

BlackBasta is a ransomware operator and criminal enterprise offering Ransomware-as-a-Service (RaaS), which surfaced in early 2022 and swiftly became one of the most prolific threat actors in the global RaaS landscape. Last month, the group successfully targeted automotive giant Hyundai, encrypting a significant volume of internal files. With ransom payments amounting to at least $107 million since its inception, the BlackBasta cybercrime syndicate shows no signs of slowing down, indicating its enduring presence and formidable status in the cybercriminal realm.

Figure 4 //

TOP 3
ATTACKED COUNTRIES BY BLACKBASTA

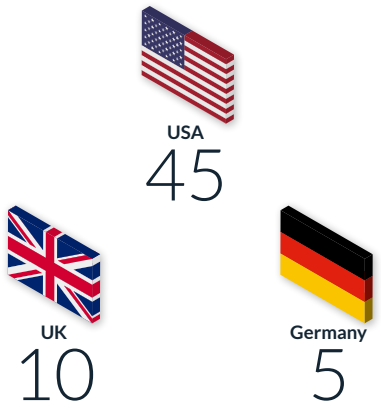


Figure 5 //

TOP 3
ATTACKED SECTORS BY BLACKBASTA

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 methodical group intends to halt its operations. An interesting point to note is that in January 2024, the group only managed to attack 3 victims, which is the lowest number in the past 2 years.

Figure 6 //

TOP 3
ATTACKED COUNTRIES BY PLAY

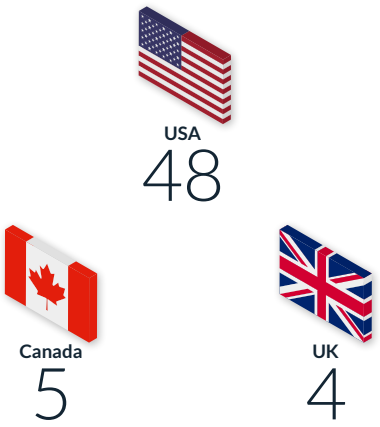


Figure 7 //

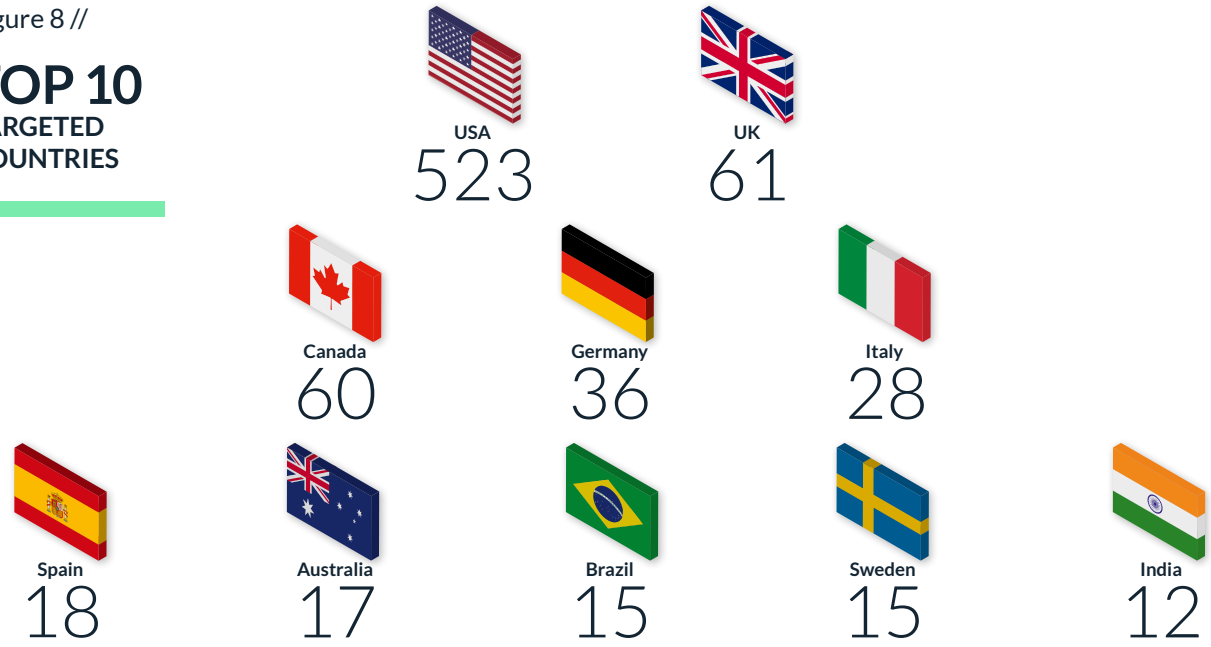
TOP 3
ATTACKED SECTORS BY PLAY

TOP COUNTRIES

Regarding the most targeted countries (Figure 8), the U.S. remains the number one targeted country globally, with good reason. The number one economy in the world was the victim of ransomware attacks this quarter in 50.8% of the cases, amounting to 523 cases.

Figure 8 //

TOP 10
TARGETED COUNTRIES



The second most targeted country this quarter is the United Kingdom, with 61 cases, far behind the U.S. Finally, Canada is in third place with 60 ransomware cases this quarter.

Even when focusing on the top three countries, we can see that there is no doubt that the U.S. is the most lucrative country for threat actors.

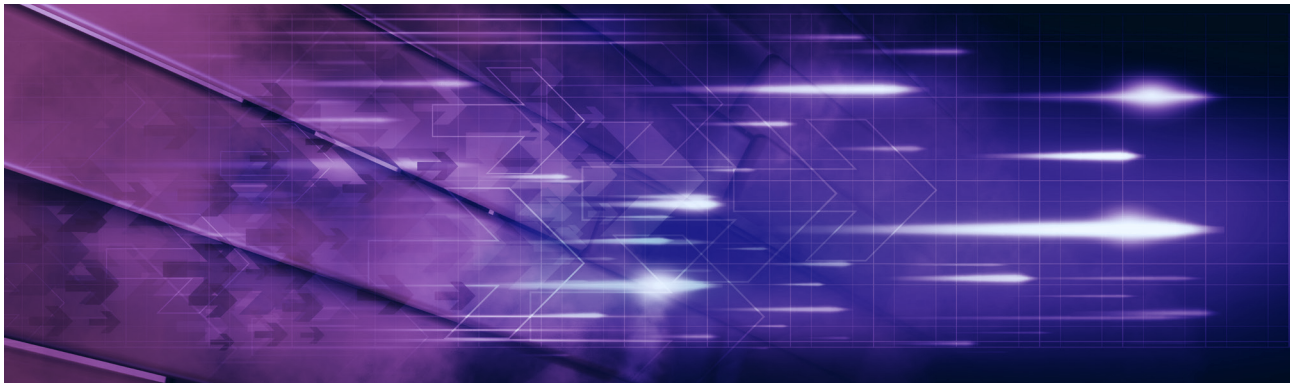
TOP SECTORS

As expected, the business services sector is the most targeted sector in Q1, with 23.5% of the ransomware cases, followed by the retail and manufacturing sectors, with 16% and 14%, respectively (Figure 9).

Figure 9 //

TOP 10
TARGETED SECTORS

NEWCOMERS



MOGILEVICH

The emergence of the Mogilevich group seemed sudden, as they promptly asserted control over major organizations including Epic Games, DJI, Shein, Kick, and others within a mere two weeks of their appearance. Despite their claims, both we and fellow researchers are doubtful about their successes due to the absence of evidence supporting these alleged breaches. None of the organizations mentioned reported any cybersecurity incidents, and there was a glaring lack of ransom notes, samples, analyses, or any public acknowledgment of such breaches or ransomware. In essence, there was a total absence of substantiation.

On March 2, 2024, doubts surrounding the group were confirmed when they revisited Epic Games, this time purportedly providing a data sample as evidence of a breach. However, this "data sample" turned out to be a confession admitting that the group were impostors rather than a legitimate Ransomware-as-a-Service (RaaS) entity (see their confession in the Ransom Notes section below). The individual(s) orchestrating this scheme, under the alias Pongo, confessed to fabricating false breaches to quickly garner attention and redirect victims to a scam.

RANSOMHUB

On their "About" page, RansomHub identifies itself as a global team of hackers primarily motivated by financial gain. While this motive isn't particularly surprising, the group claims to refrain from targeting certain entities.

On February 25, 2024, RansomHub made its debut with an attack on YKP, a Brazilian accounting and management firm, marking its first observed victim. Since then, four more victims fell prey to their ransomware in February, followed by an additional 13 victims in March.

Unlike the now-discredited Mogilevich scam, RansomHub provides data samples extracted by its affiliates, and in one instance, began releasing substantial volumes of data.

TRISEC

Trisec, a ransomware faction, announced its presence on the dark net leak site on February 17, declaring its initial victim: Cogans Toyota Cork, an Irish dealership. To date, the group has targeted a total of three victims.

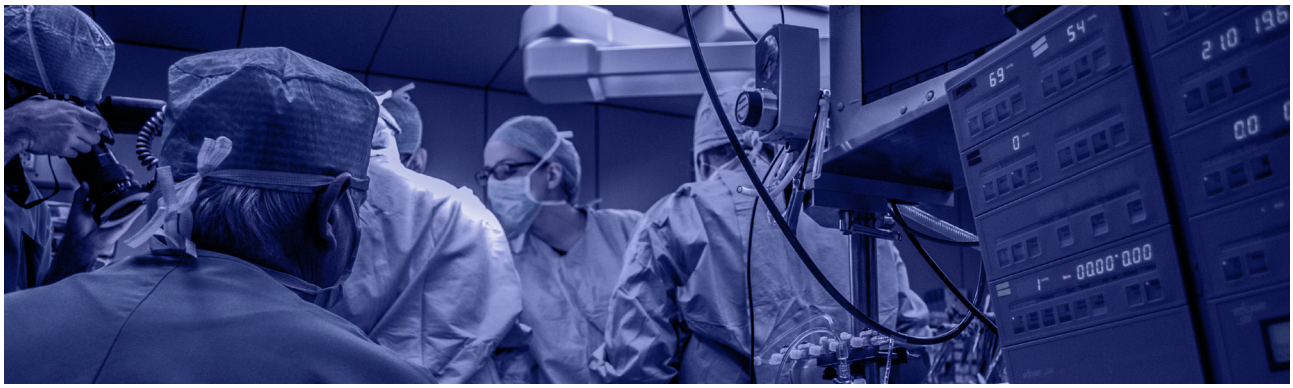
Trisec diverges from conventional ransomware groups by openly aligning itself with a nation-state, notably, Tunisia, rather than Russia or China. The Tunisian flag prominently features in the group's Telegram channels, and their leak site specifies a preference for hiring Tunisians.

SLUG

A ransomware collective known as Slug has claimed responsibility for infiltrating and targeting AerCap as its inaugural public victim. According to cybersecurity analysts at Hackmanac, the perpetrators claim to have absconded with 1TB of AerCap's data.

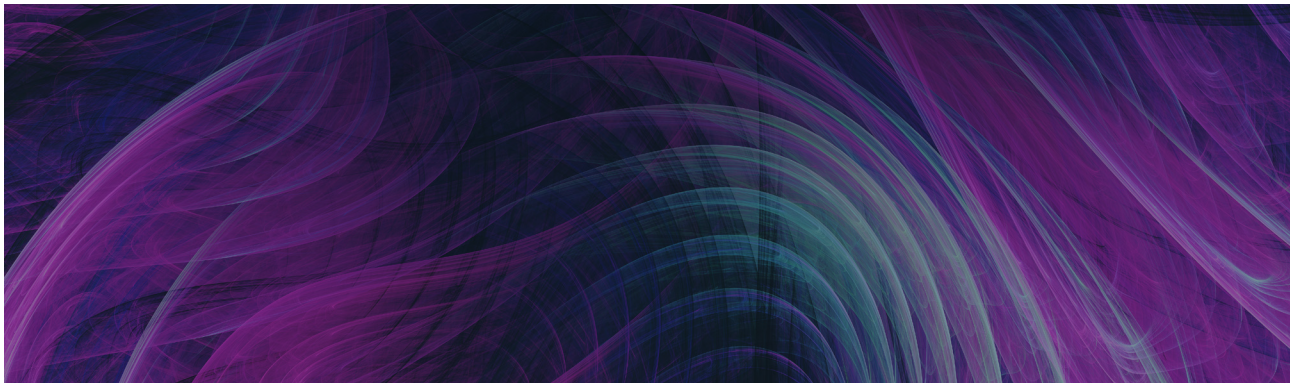
MYDATA

A new player in the ransomware arena, MyData / Alpha Locker, has emerged. An examination of their data leak site uncovers several companies victimized by the group, including Mike Ferry, A24Group, Accolade Group and its subsidiary Levelwear, Gadot Biochemical Industries, CARRI Systems, and Integrity. The exfiltrated data, dated 2023, points to the group's ongoing activity.



BLACKOUT

Another ransomware entity, Blackout, has recently emerged. Its initial target was the '**Centre Hospitalier d'Armentières**', where the group claims to have encrypted over 100 servers and workstations in the French medical institution's local network, as well as exfiltrated a database containing records of over 900,000 patients. Additionally, Groupe M7 in Quebec fell victim to Blackout's second attack, resulting in the extraction of 10 GB of internal documents and financial reports, alongside the encryption of several servers. The ransom demand for this incident expired on March 3rd.



DONEX

Enterprises in the United States and Europe are on high alert due to the emergence of a new ransomware strain known as “DoNex,” actively compromising companies and claiming victims.

This new threat has cybersecurity experts scrambling to comprehend its full extent and devise countermeasures.

The DoNex ransomware group has unveiled several companies as its victims on their dark web portal, accessible via the Onion network.

Employing a double-extortion method, the group not only encrypts files, appending them with a unique VictimID extension, but also exfiltrates sensitive data, using it as leverage to coerce victims into paying the ransom.

Affected companies discover ransom notes named Readme.VictimID.txt on their systems, directing them to initiate contact with the DoNex group via Tox messenger, a peer-to-peer instant messaging service known for its security and anonymity features.

INSANE

In January 2024, Insane, or Going Insane, surfaced suddenly, targeting a victim in Thailand before vanishing just as quickly. The only information available about this “group” was posted on their data leak site. They claim to utilize AES encryption for their ransomware and purport to possess malware capable of stealing information. Researchers from Clipeus Intelligence suggest the creator may be of Russian origin.

ARRESTS

LOCKBIT CYBERCRIME NETWORK FACES GLOBAL CRACKDOWN THROUGH INDICTMENTS AND ARRESTS

A multinational operation targeting the notorious LockBit ransomware gang has resulted in the apprehension of at least three affiliates in Poland and Ukraine.

The announcements of these arrests followed the shutdown of LockBit's darknet platform, utilized by the group for issuing threats to victims and releasing compromised data unless ransom demands were met.

Ukrainian cyber police disclosed on Wednesday that they had detained a "father and son" duo allegedly affiliated with LockBit, whose activities purportedly impacted individuals, businesses, governmental entities, and healthcare establishments in France.

During searches of the suspects' residences in Ternopil, Ukraine, law enforcement seized mobile phones and computer equipment suspected to have been utilized in cyberattacks.

In Poland, authorities arrested a 38-year-old individual in Warsaw, suspected of being associated with LockBit. He was brought before the prosecutor's office and charged with criminal offenses.

As evident, these occurrences did not impede the largest existing ransomware operation, as the attacks continue at the same pace. The significance of the LockBit gang likely extends beyond just three arrests, indicating that stopping their operations will demand considerable effort.

NEW TRENDS

RECORD LOW RANSOMWARE PAYMENTS REPORTED AS VICTIMS REJECT RANSOM DEMANDS

In the last quarter of 2023, the proportion of ransomware victims complying with ransom demands plummeted to a historic low of 29%, as per data from ransomware negotiation firm Coveware.

Coveware attributes this continuous decline to several factors, including enhanced preparedness among organizations, skepticism towards cybercriminals' assurances to not disclose pilfered data, and legal constraints in regions where ransom payments are prohibited.

Not only has there been a decrease in the number of ransomware victims making payments, but there has also been a notable decline in the monetary value of such payments.

Coveware notes that in Q4 2023, the average ransom payment amounted to $568,705, marking a 33% decrease from the preceding quarter, with the median ransom payment standing at $200,000.

MAJOR INCIDENTS

DUVEL MOORTGAT BREWERY TARGETED IN BLACKBASTA RANSOMWARE ATTACK

The Duvel Moortgat Brewery, renowned for its iconic Belgian beer brand, including the celebrated strong and fruity golden pale ale of the same name, fell victim to a BlackBasta ransomware assault.

On March 7, a spokesperson for the company informed local media that their automated threat detection systems had flagged the ransomware attack.

Ellen Aarts, communications manager at Duvel Moortgat, stated, “At 1:30 AM last night, alarms went off in Duvel’s IT department because ransomware was detected. Consequently, production was promptly halted. The timeline for its resumption remains uncertain. We are aiming for a restart either today or tomorrow.”

Aarts also mentioned that despite not having an accurate estimate for the return to normal production operations, their warehouses are adequately stocked, ensuring minimal impact on distribution.

The company did not specify whether the cyberattack affected production at Duvel’s primary brewery in Breendonk only or extended to other facilities in Antwerp, Oudenaarde, and Achouffe as well.

HYUNDAI MOTOR EUROPE TARGETED BY BLACKBASTA RANSOMWARE ASSAULT

Hyundai Motor Europe, the European division of car manufacturer Hyundai Motor Company based in Germany, fell victim to a BlackBasta ransomware attack, with threat actors asserting possession of three terabytes of corporate data.

According to reports, in an image obtained by BleepingComputer, the attackers disclosed lists of folders purportedly pilfered from multiple Windows domains, including those associated with KIA Europe.

While the exact nature of the stolen data remains undisclosed, the folder names suggest its affiliation with various departments within the company, encompassing legal, sales, human resources, accounting, IT, and management.

FULTON COUNTY, GEORGIA, TARGETED BY LOCKBIT RANSOMWARE GROUP

The LockBit ransomware syndicate has taken responsibility for the recent cyber assault on Fulton County, Georgia, issuing threats to disclose “privileged” documents unless a ransom is paid.

With a population exceeding one million, Fulton County is Georgia’s largest county and houses the state capital, Atlanta.

Over the last weekend in January, hackers infiltrated the county’s systems, causing extensive IT disruptions affecting telecommunications, judiciary proceedings, and taxation services.

Nearly three weeks after the breach, the county’s official website continues to display an initial alert regarding the system outage, redirecting visitors to the latest update from February 5.

Telephony services have been partially restored, but the property tax system remains offline, hindering payment processing and other transactions. Residents encounter challenges in water billing due to the unavailability of electronic payments, although penalties for delays are waived.

Officials have noted delays in justice system services, while affirming that email services remain unaffected.

CONCLUSIONS

The ransomware industry remains the number one threat to organizations worldwide.

As this quarter ended, supply chain attacks became a solid technique for the mature and experienced ransomware groups.

In addition, this quarter showed us the faces of new ambitious groups that look to put their mark on the ransomware industry. More than usual, we saw more than 10 new Ransomware groups!

LockBit3.0 remains the ruler of the industry, far ahead of the other groups, in spite of the arrests that affected the group in February.

Although we have seen increased activity by law authorities worldwide this quarter, this industry keeps on thriving despite their efforts.

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

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

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

UNITED KINGDOM
Tel: +44-203-514-1515
3rd Floor, Great Titchfield House, 14-18 Great Titchfield Street, London, W1W 8BD

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

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.