MINISTRY OF
COMMUNICATIONS AND DIGITAL

CyberSecurity
MALAYSIA

MID-YEAR REPORT

THREAT LANDSCAPE

2023

SECURING
OUR
CYBERSPACE

COPYRIGHT AND CONFIDENTIALITY STATEMENT

Registered office:
Level 7, Tower1, Menara CyberAxis Jalan Impact,
63000 Cyberjaya, Selangor.

Registered in Malaysia – Company Limited by Guarantee
Company No. 726630-U

Disclaimer

This Mid-Year Threat Landscape report has been meticulously prepared by CyberSecurity Malaysia. The research is based on the latest technical reports generated over the past months. It should be noted that the statistics and risk summary provided in this report may have evolved over time.

CyberSecurity Malaysia unreservedly endorses the contents of this report, recognizing its alignment with the most up-to-date findings and analysis. However, it is essential to acknowledge that certain aspects of the management report may require further clarification from CyberSecurity Malaysia in order to ensure a comprehensive understanding.

CONTENT

Executive Summary

This report is produced in reporting the cyber threat landscape of Malaysia in the first half of the year 2023. The works begin in early month of January 2023 where we collected threat feeds related to Malaysia up to at the end of June 2023. Our sources for data aggregation in order to meet the objectives of our research are various – from social medias, online news, Cyber Threat Intelligent Platforms (or CTIPs), and from Darkweb forums.

What we learn in this first half of the year observation is Malaysia, and neighboring ASEAN countries are experiencing a noteworthy surge in cyber threats, primarily involving data breaches across diverse sectors. Both industrial entities and governmental bodies have been victims of escalating cyber-attacks, credited to the cybercriminals growing sophistication in term of tactics, techniques and procedures. With new innovations on cyber-attacks such as Infostealer MaaS (Malware as a Service) and better weaponizations of RaaS (Ransomware as a Service), even giants corporations with good cybersecurity infrastructures falls victims to these cybercriminals. Furthermore, they are no longer bound by secrecy and have been on several channels on social medias and Telegrams instead of on darkweb forums and channels.

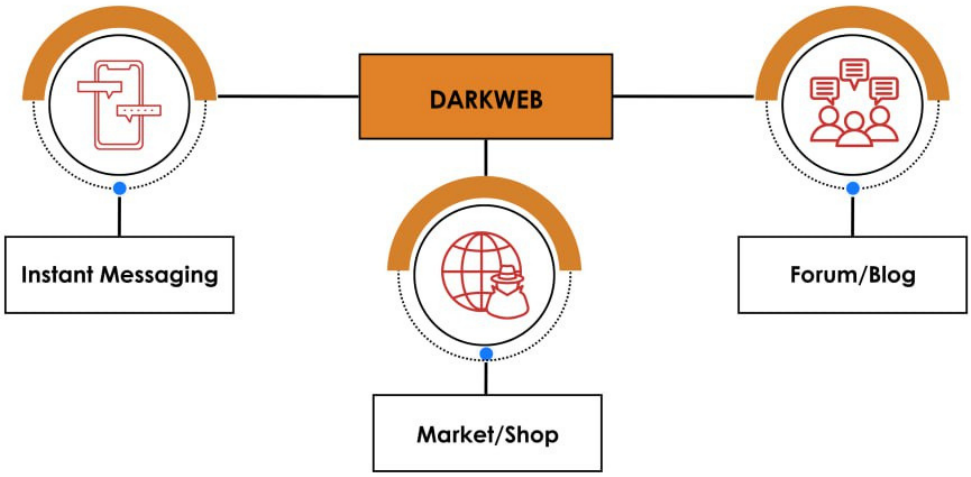
From the data we gathered and analyzed, we can see a smaller but significantly disruptive subsets of these incidents that point out to large-scale ransomware attacks. These ransomware groups have primarily targeted sectors like education, automotives, logistics, and others. The scale and impact of these attacks signify a shift in cybercriminal tactics, focusing on sectors that were traditionally less targeted before but could lead to considerable number of damages and higher ransom returns.

Parallel to these developments, there's been a rise of activities in darkweb forums relating to data breaches specifically targeting SEA nations including Malaysia. Such activities underline the lucrative values of stolen data via these forums marketplaces. Furthermore, the data we gathered from these forums indicates the willingness of these threat actors in exploiting these region's digital vulnerabilities.

However, on March 2023 a huge development took place as the closure of a prominent darkweb forum Breached.vc disrupted the cybercrime landscape indefinitely. With the detention of the forum founder Conor Brian Fitzpatrick (who is known with his darkweb monicker Pompompurin), we found a considerably decelerated of forums activities related to data breaches. This event sparked a ripple effect among cybercriminal communities, leading to exodus of these threat actors to other forums. The exodus also resulted in subsequent cyber-attacks among themselves on these new platforms in gaining dominance. Consequently, this has resulted in a temporary shutdowns and slowdowns, and even disarray within their networks.

In conclusion, the cyber threat landscape in Malaysia in circa midyear of 2023 has grown more intricate and also becoming more treacherous. While law enforcement interventions would offer temporary respites, it is imperative to acknowledge the underlining urgency for robust cybersecurity measures, given the heightened threat level and the evolving tactics of cybercriminals. Strengthening cybersecurity infrastructures, continuous monitoring, trainings, and best practices must be put a top priority to counter these escalating threats effectively.

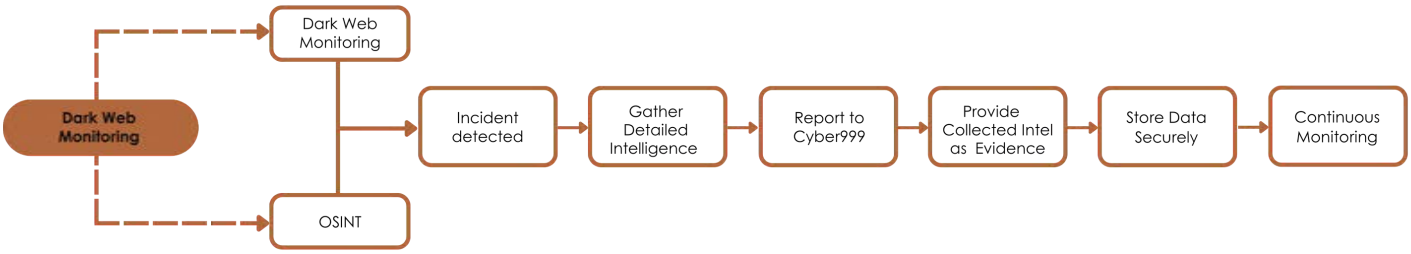
THE METHODOLOGY OF THREAT LANDSCAPE ANALYSIS



Our methodology for monitoring, data collection and analysis is depicted in the above chart, detailing the process and sources of our surveillance. The first step in our methodology is to identify the source. We begin by identifying the primary sources of information. These are categorized into three main sections:

- **Instant Messaging**: Channels like Telegram act as real-time communication platforms, often used for rapid information exchange.
- **Markets/Shops**: Dark web marketplaces are hubs for illegal transactions, ranging from drug sales to weapon trade.
- **Forums/Blogs**: These platforms host discussions, blogs, and posts, providing insights into users' intents and upcoming trends.

Once the sources are identified, we initiate continuous surveillance over these sources. With 45 forums, 7 markets, and 87 Telegram channels currently under watch, we capture a vast amount of data daily. Given the extensive data that we amassed, it's crucial to narrow down the information. We filtered down our information based on keywords, e.g. "Malaysia" to target specific content, ensuring that the data becomes manageable and relevant to the research scope. Post filtering, the filtered data is analyzed for potential threats, trends, or insights. Key findings are then compiled and reported to relevant stakeholders.



1. **Source of Monitoring**:
   - Dark Web Monitoring: This refers to the surveillance of hidden parts of the internet, often associated with illegal activities and unindexed by traditional search engines.
   - OSINT (Open-Source Intelligence): This involves gathering information from publicly available sources. It can include everything from news websites to public records, providing a contrast to the covert nature of the dark web.
2. **Incident Detection**:
   - Once the monitoring tools detect a potential security incident or any suspicious activity related to the target (e.g., an organization, individual, or country), the process moves to the next phase.
3. **Gather Detailed Intelligence**:
   - At this stage, in-depth research and intelligence gathering are conducted. This could involve understanding the nature of the threat, its origin, the entities involved, and potential impacts.
4. **Report to Cyber999**:
   - Our Cyber999 service is then alerted about the incident. The team is provided with initial findings and intelligence to take appropriate action.
5. **Provide Collected Intel as Evidence**:
   - The intelligence gathered can serve as evidence, useful for both internal investigations and potential legal actions. This data can help in understanding the threat actor's motives, methods, and potential future actions.
6. **Store Data Securely**:
   - All the information and intelligence gathered are securely stored to ensure the information CIA triad (confidentiality, integrity, and availability). This is crucial to prevent any unauthorized access or potential data breaches.
7. **Continuous Monitoring:**
   - After the incident has been addressed, continuous monitoring is maintained. This ensures that any subsequent suspicious activities or threats are detected promptly, ensuring the security and safety of the target.

INTRODUCTION

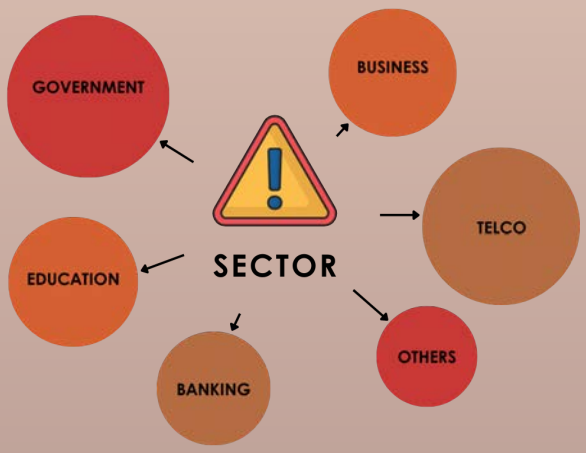
In this report we lay out the threat landscape of Malaysia from January into the mid-year of 2023. We map out this landscape in order to understand types of attacks occurred and where defenses need to be strengthened. We've drawn information from an array of sources to make this report as inclusive as possible, encompassing everything from Surfaceweb to Darkwebs. Additionally, we also made use of various Threat Intelligence Platforms (TIPs), to aggregate and analyze information about potential cyber threats.

With the information we have gathered, we categorized the affected entities by sectors, and start looking at the types of cyber-attacks that have been affecting them. We then delve further into the analysis by looking into the Threat Actors - the individuals or groups behind these attacks. We identified the Threat Actors who are targeting Malaysia in their campaigns, collecting the data on them from various darkweb forums, and figuring out the objectives they may pursuing. Whether they are highly organized hacking groups seeking financial gain, or individuals with a personal vendetta, understanding the Threat Actors is crucial in piecing together the cybersecurity puzzle. This knowledge not only helps in identifying patterns and anticipating potential future attacks but also plays an instrumental role in devising effective counterstrategies to safeguard the sectors under threat.

SECTORS MONITORED

Malaysia Sectors mostly affected by incidents within the half-year of 2023.

The monitoring are based on the numbers of incidents happened on entities within the enclave of each sector.



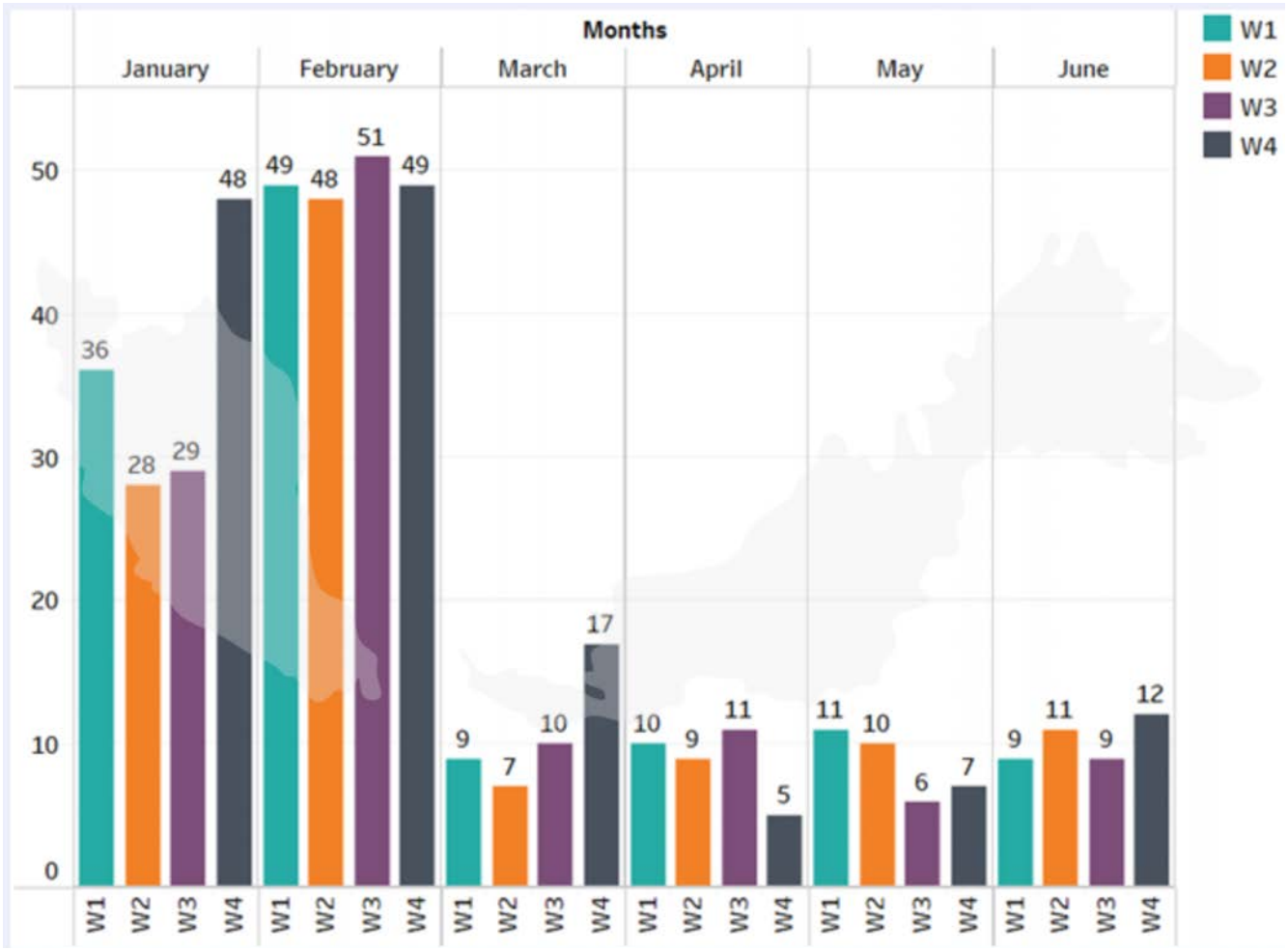
TYPES OF THREATS

From the incidents on these sectors, we found out the threats can be grouped into these five categories.

The incidents by these type of threats were recorded into weekly and into our monthly reporting.

The following visualization demonstrates the incidents reported by weekly and monthly.

WEEKLY-MONTHLY INCIDENTS REPORT



In the following section, we present a chronology of incident reports spanning the designated timeframe. What captures our attention is the notable concentration of incidents in January to February period, in stark contrast to a dramatic tapering off in the succeeding months through June.

Ordinarily, one might expect a gradual escalation in the tally of incidents. Contrary to this, the figures plummeted from an initial 309 incidents in the first two months to just 153 incidents over the course of the next four months - an astounding reduction of 50.49%.

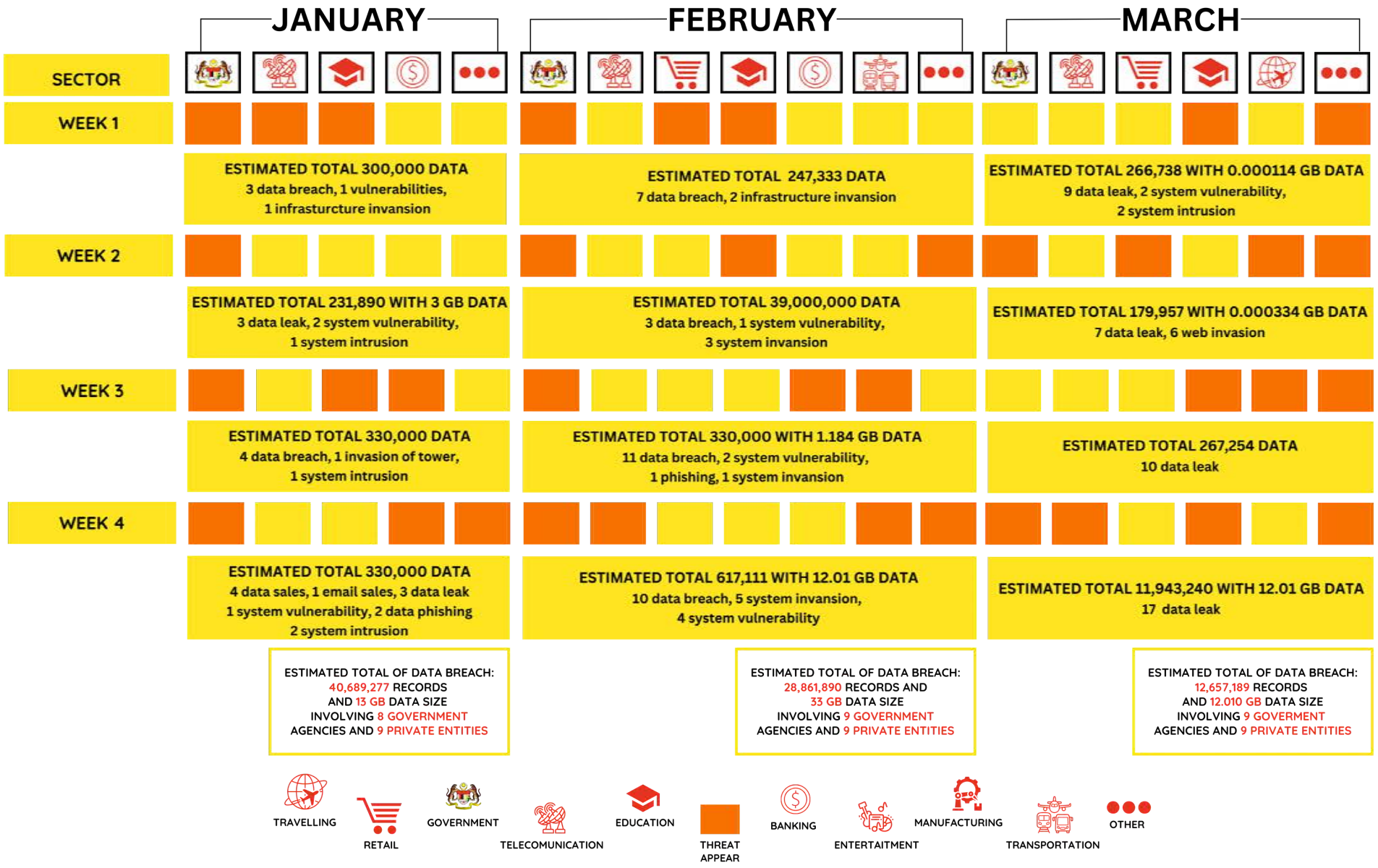
We identified the disruptive factors that lead to this pattern by aggregating intelligence data, in which we will uncover in this report.

CYBER INCIDENTS ON QUARTER 1

- In this segment, we'll be putting the spotlight on monthly cyber incidents for Quarter 1 of the year 2023.

- We are breaking them down week by week to get a more detail understanding of the trends and patterns in the reports of incidents.

CYBER INCIDENT QUARTER 1

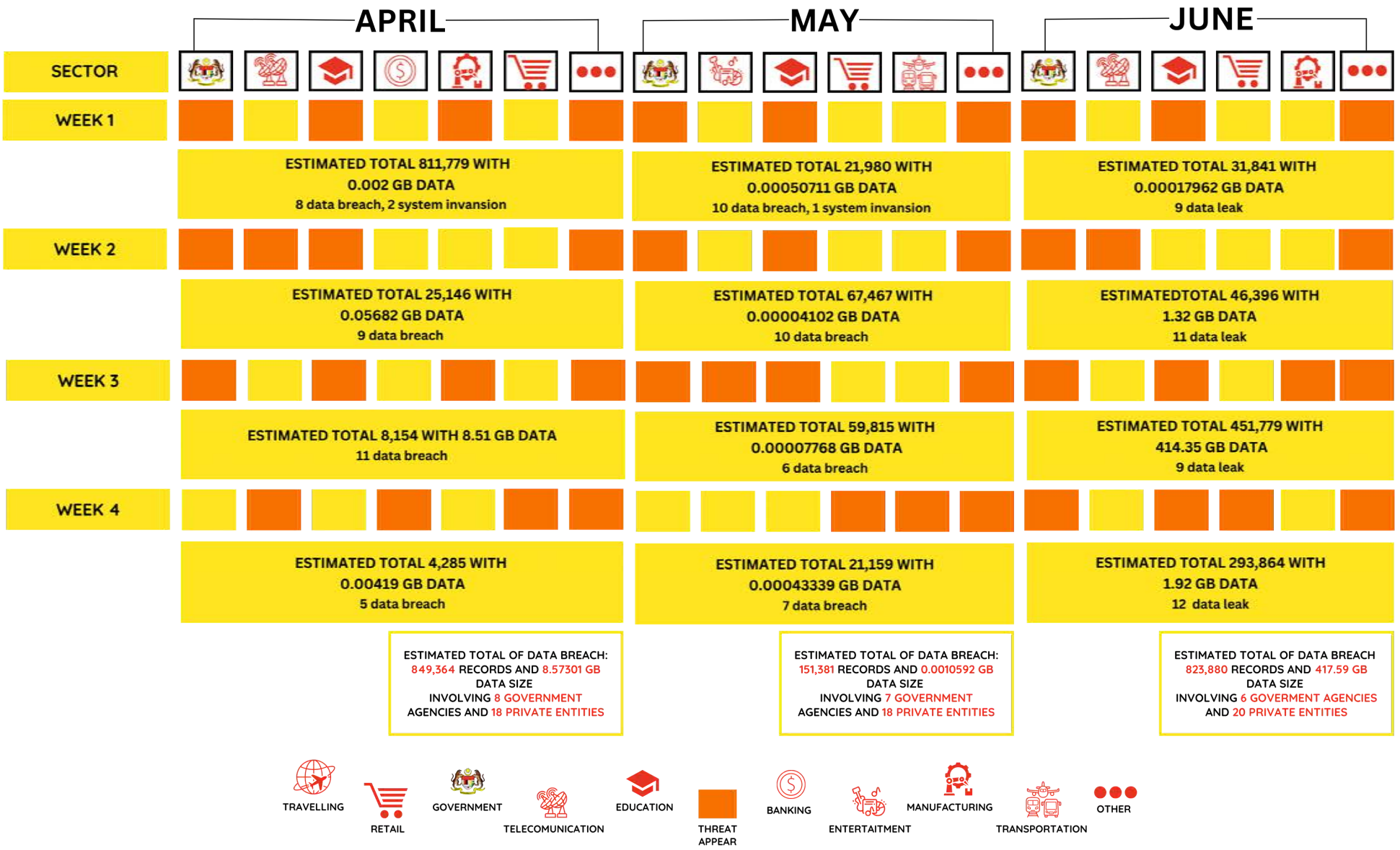


CYBER INCIDENTS ON QUARTER 2

- In this next segment, we'll be putting the spotlight on monthly cyber incidents for Quarter 2 of the year 2023.

- Just like before, we are breaking the reported incidents down by weekly to get a more detail understanding of the trends and patterns in the reports of incidents.

CYBER INCIDENT QUARTER 2

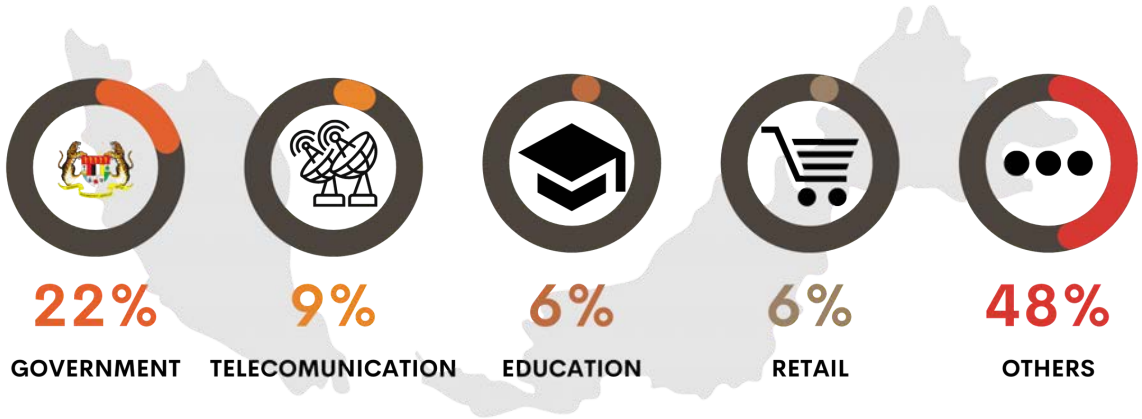


DATA BREACH INCIDENT

- In this portion, we will unpack an analytical exploration of data breach incidents that are centering on Malaysia.

- The analysis will look into sectors most vulnerable, the Threat Actors motives, and the volumes of digital assets affected.

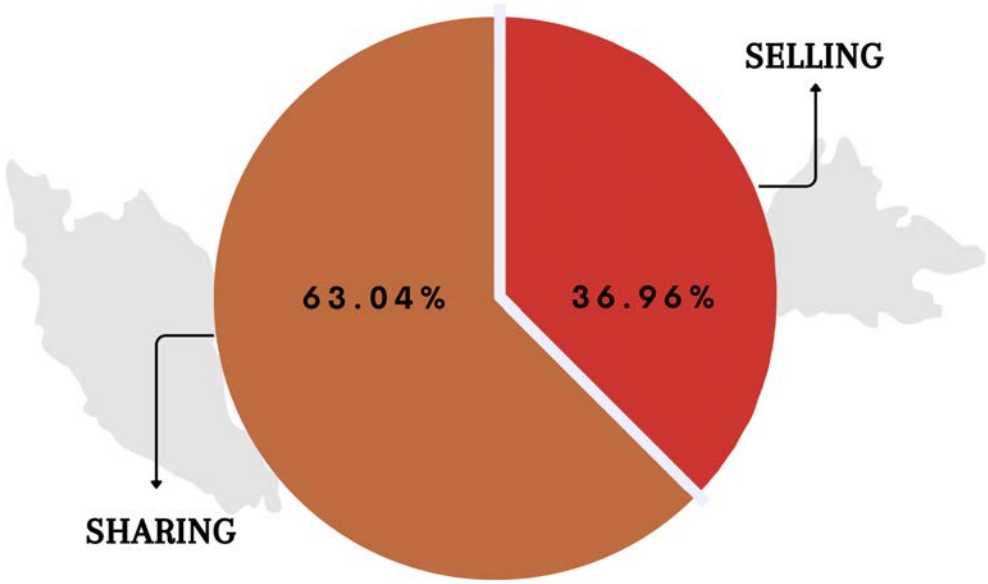
TOP 5 SECTOR AFFECTED BY THREAT



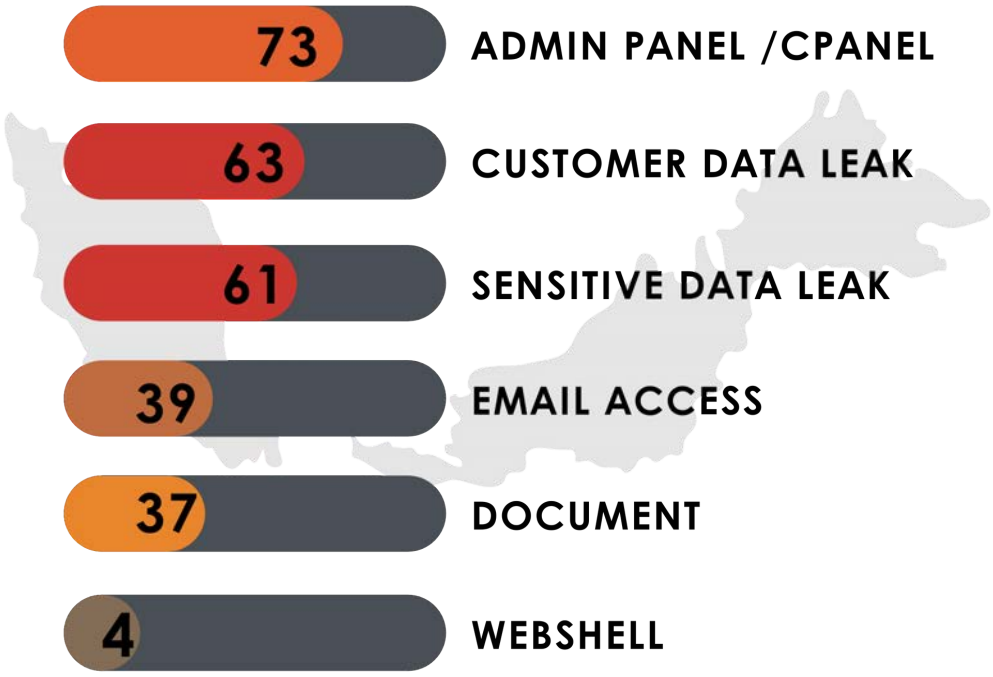
From the data breaches landscape reports across various sectors, it is intriguing to note that government sectors tops the list, accounting for 22% of the breaches. Telecommunication follows at 9%, highlighting the significance of safeguarding the sectors. Educations and retails are at tied, each comprising at 6% of Malaysia's data breach records. A diverse assortment of other sectors collectively make up the remaining 48%, illustrating that data breaches are a widespread concern.

TAG THREAT ACTOR

Following the sectorial analysis, it is imperative to highlight the behavioral of the Threat Actors (or TA) in these data breaches record. Alarmingly, 36.96% of the TAs are engaged in selling the leaked data. Even more concerning, is the fact that 63.04% of these TAs are into this fray to share the data. This could imply a range of subsequent scenarios – from public leaks that are meant to damage reputations, to sharing among TA networks for more extensive exploitation. This underscores the urgency for more robust cybersecurity frameworks to combat the evolving tactics of the TAs.



TYPES OF DATA AFFECTED, BY CASES

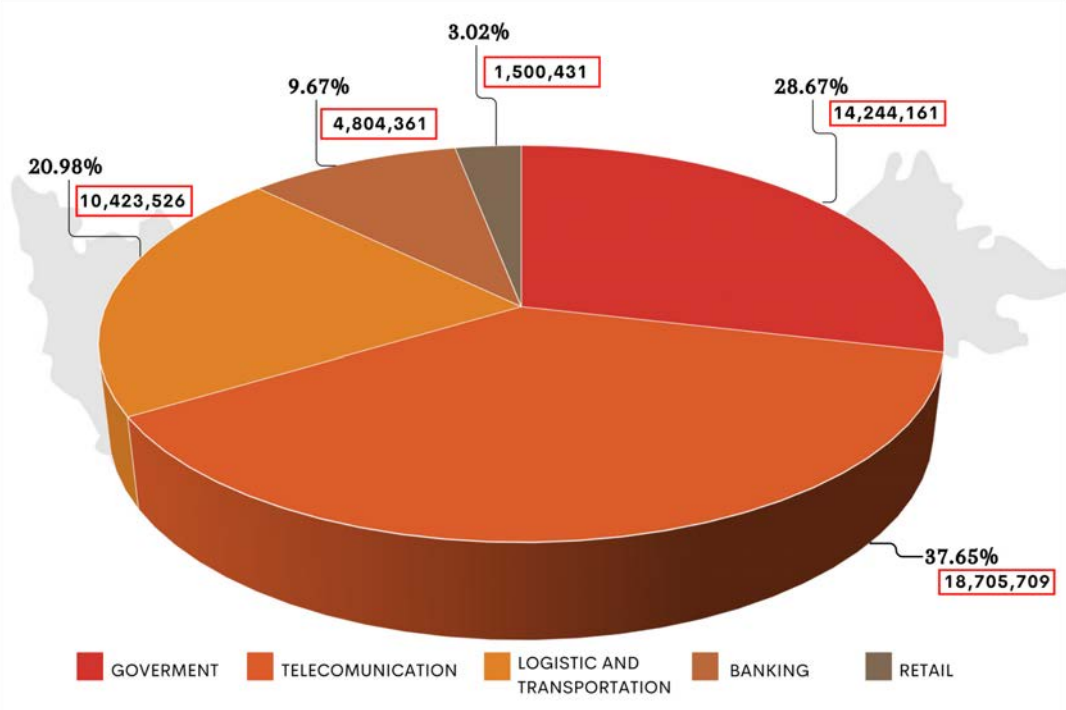


The following is the types of data being leaked within the context of reported cases of data leak in Malaysia from January to June 2023. From the data we can see that 71% of these incidents are related to Admin Panel/CPanel, Customer data and Sensitive Data leaks.

The cases related to email access and documents leak takes up 27% of the cases, while compromised webshell takes up 1.4% of the cases.

These data shows that the TA campaigns are highly popular on the tags related to data leaks within the half-year of 2023. Now, on to the question of how much data from Malaysia is affected. Subsequently, we need to know of which sectors in Malaysia are affected based on these cases. Finally, we ought to uncover who are these threat actors that are targeting our country's data.

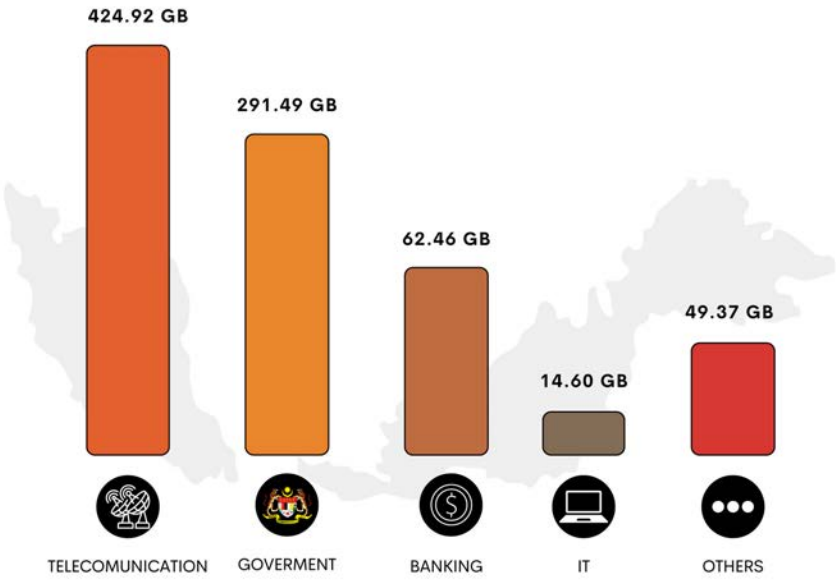
TOTAL DATA LEAKED BY SECTOR



The data spanning a period of 6 months unveils the landscape of data breaches within sectors in Malaysia. Out of these sectors, we see four sectors that are the most vulnerable – telecommunication(37.65%), government(28.67%), logistic and transportation(20.98%) and banking(9.67%). These sectors are seen as lucrative by TAs, as these sectors' data are seen as more impactful in term the level of sensitivity of the data and in term of the volume of these data.

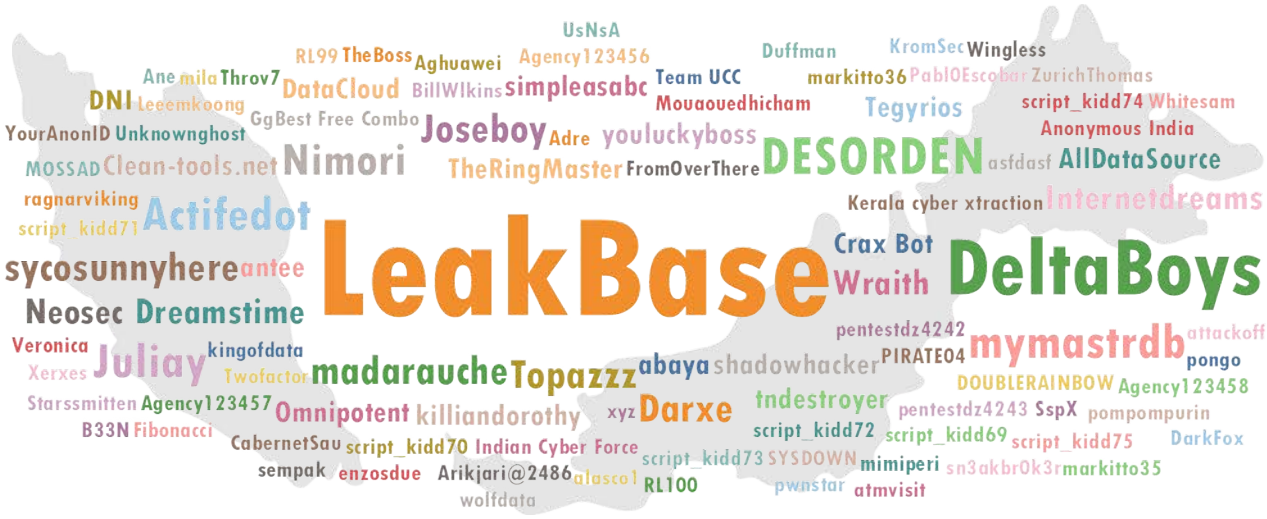
SIZE OF DATA LEAKED BY SECTOR

As per the volume of the data leaked, the number of Gigabytes leaked speak for themselves – a staggering amount of 842.84 Gigabytes with telecommunication sector tops the charts as the highest volumes of data leaked, followed with government sectors, and banking sectors.



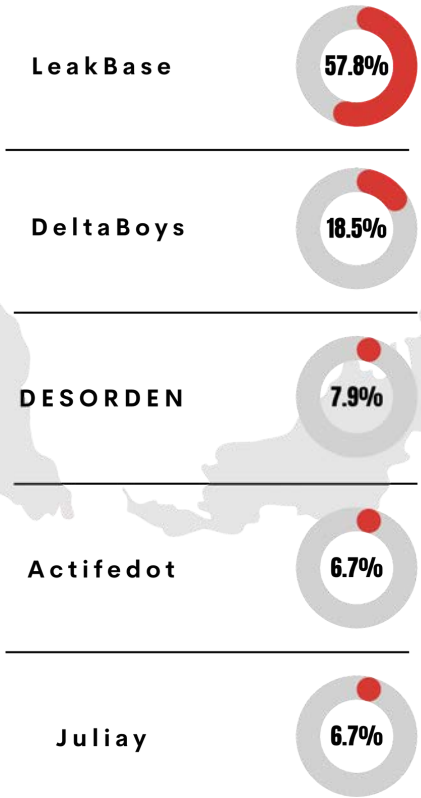
THREAT ACTOR

LIST OF THREAT ACTOR



The visualisation above is a word cloud that showcases Threat Actor individuals or group that have connections to the compromising of sensitive data from Malaysia via darkweb forums. In this graphic, the prominence of a name reflects the extent of activity these Threat Actors engage in within the forums; the more sizable the name, the higher their involvement in marketing, distributing, and exchanging the data. In total, there are 89 TAs involved in the breaching of Malaysia's data.

TOP 5 THREAT ACTOR THAT LEAKED MALAYSIA SENSITIVE DATA

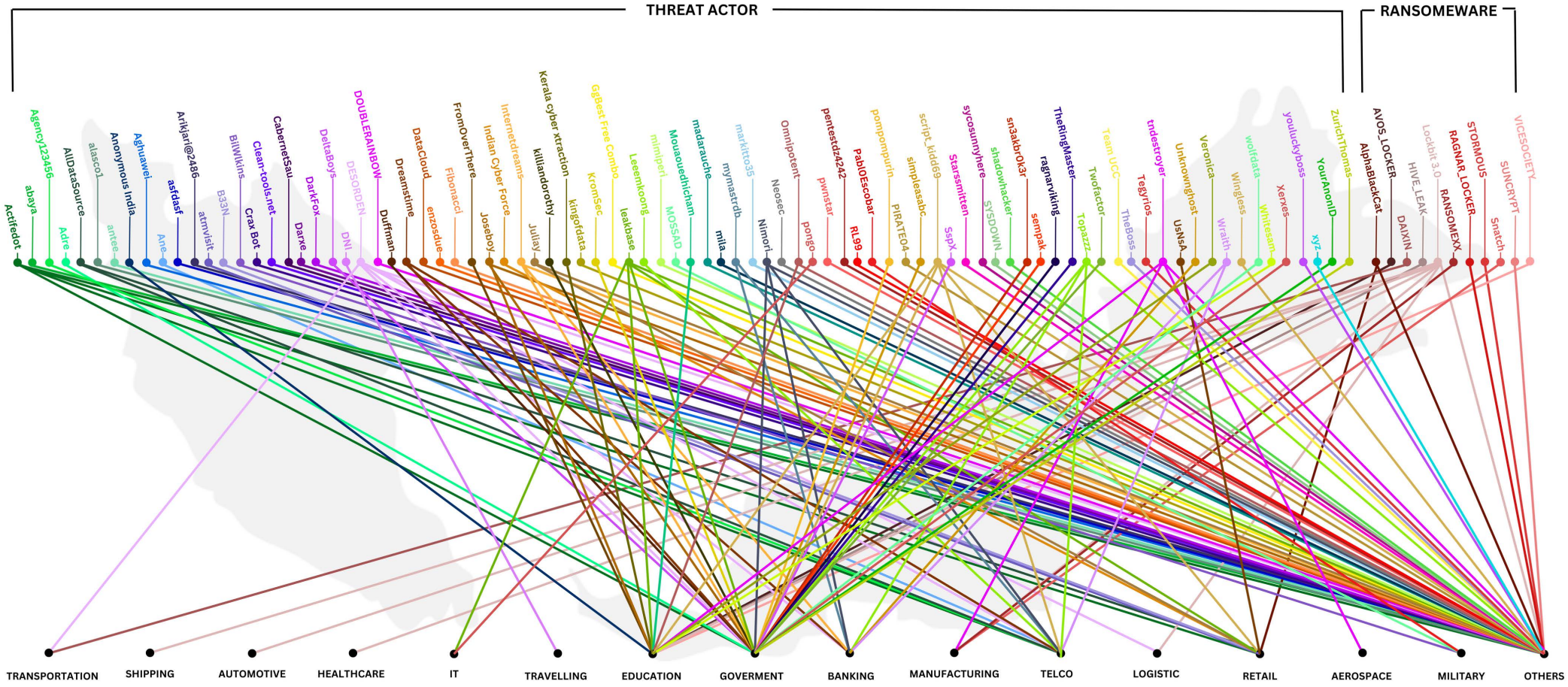


What follows here are the top 5 TAs most active and have high reputations in data breach of Malaysia.

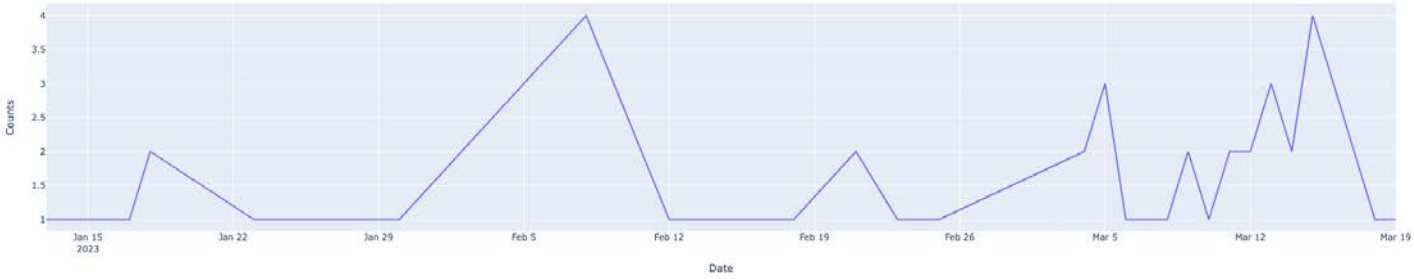
The following (in the next page) is the relational graphs based on the data we collected from darkweb forums during the six months from January to June 2023.

The graphs describe the relations between Threat Actors with Malaysia sectors they targeted. The data that they leaked are being promoted or shared within the forums. The information on ransomware groups is also included in the graphs, as their MO will leak sensitive data belongs to their victims.

THREAT ACTORS RELATIONAL GRAPH

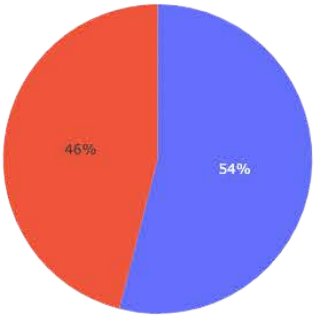


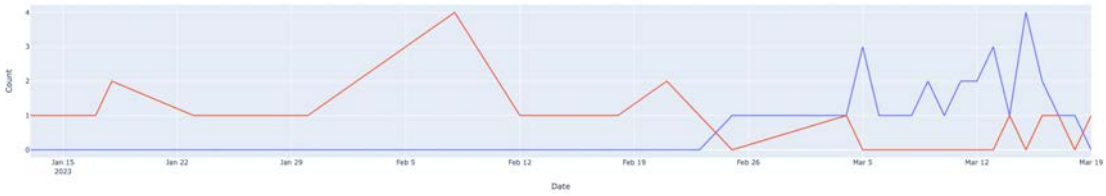
A LOOK INTO THREAT ACTOR PROFILE - LEAKBASE



TA active timeline

The graph show the active timeline of the threat actor Leakbase from January to June 2023. The group is seen to be active in darkweb forums from February to mid-March. They were active on Breached.vc, but with the closure of this forum, they took the initiative to form a new one called Leakbase.cc, overseen by an admin referred to as "Chucky"





TA activities timeline

The above pie chart and line graphs depict the TA activities monitored based on two activities – their postings and replies. The blue denotes their postings on forums while the red denotes of their replies. In the early 2023, their activities were mainly replying to posts on forums, until early March where they started to actively posting.

TA profiling

The graph show the radar plot on activity tags the Leakbase group are actively on darkweb.

ORGANIZATION AFFECTED BY LEAKBASE

Within the two months, the group has gain notoriety at the top in leaking Malaysia data with 52 cases recorded involving data from Malaysia's government, retails, education, and IT sectors. There are also 36 cases recorded, in which irrelated to any category of critical sectors in Malaysia.

From these 5 sectors, 50 activities of this group are related to the TA share the leaked data and 7 activities related to selling the data.

A LOOK INTO THREAT ACTOR PROFILE - DELTABOYS

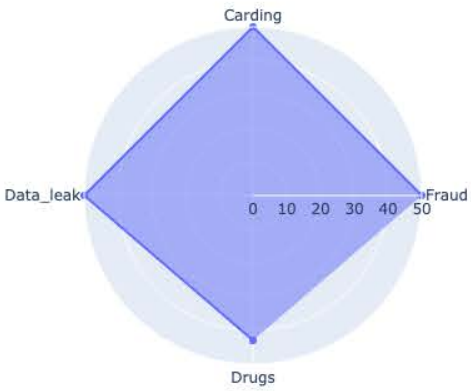
Now we are directing our attention to another Threat Actor that is Deltaboys which is at the top 5 most active on darkweb forums on topics related to leaked Malaysian data.

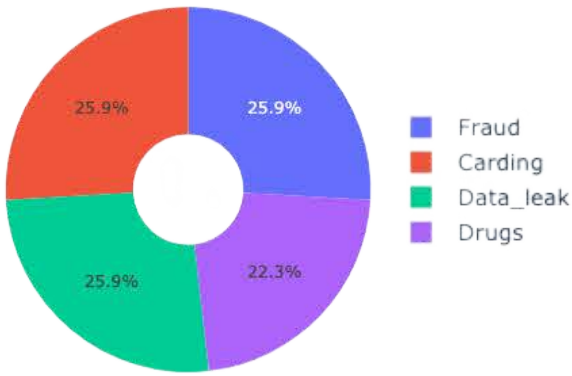
TA active timeline

Deltaboys was first seen actively this year on the data breach scene started on April 2023. However, unlike majority of other threat actors on the same interest, Deltaboys are not on any darkweb hacker forums, but they reach out their campaigns to the public via their Telegram channel and Twitter account. Our observation also shows that they are active on their platforms on early April and at the end of May 2023.

TA activities timeline

The following is the activities timeline of Deltaboys group. Their activities on forums were entirely on creating topics for discussions for their Telegram channel.

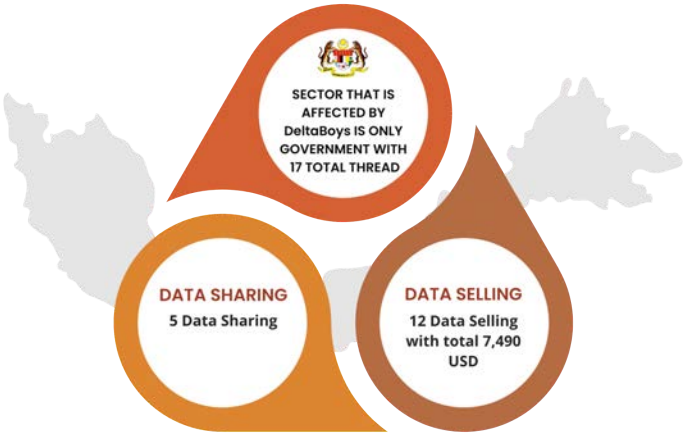




TA profiling

The graph show the radar plot on activity tags the Deltaboys group are actively on darkweb.

A LOOK INTO THREAT ACTOR PROFILE - DELTABOYS



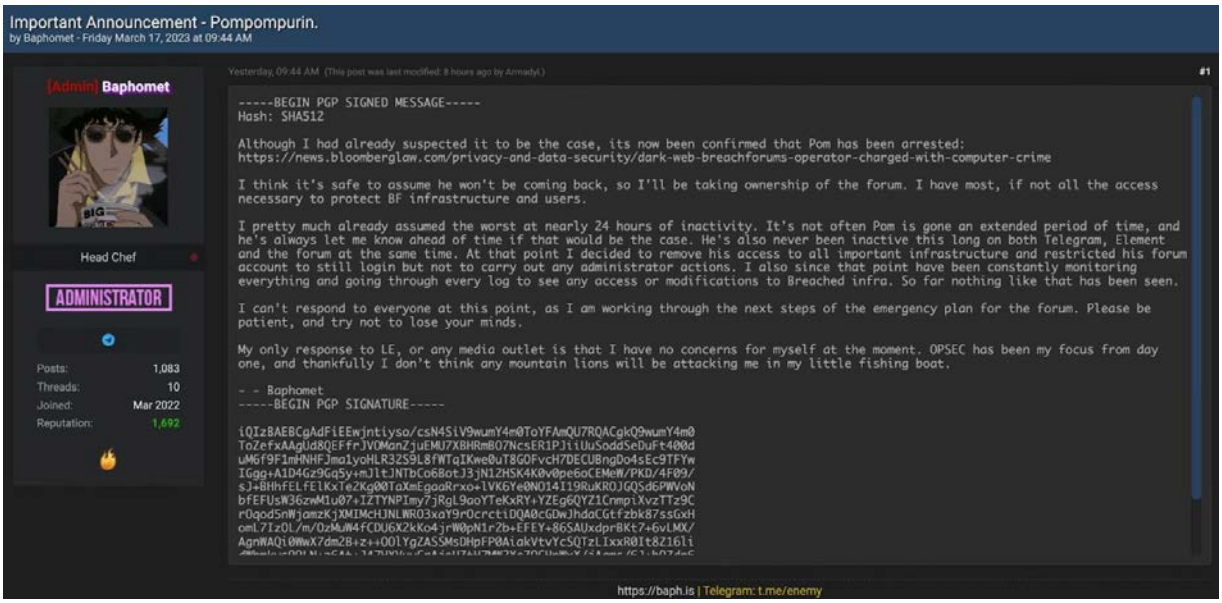
Deltaboys group specifically targeted governments sectors, with a record of 5 instances of data leaks and 12 instances of data sales of Malaysia government over the past half year. This group is perceived as a significant threat due to their focus on sensitive government information. It's not merely the numbers of data shared and selling that raises the alarm, but the strategic focus of this group on data is considered sensitive. These attacks pose a considerable risk to the integrity and security of government operations and the sensitive information of governments and rakyats. It is clear that the action of this threat actor group is not random but instead a targeted effort, designed to disrupt, to extract value, and to achieve strategic advantage. This makes them a formidable and a continuing threat to Malaysia security landscape.

DELTABOYS GROUP MOTIVATIONS

Mostly political. According to an interview by Cyfrima* with Deltaboys, their primarily aim, over nearly two decades of operation, has been to expose governmental corruption, with their activities mostly confined to underground operations until they emerge as Deltaboys a year ago. They claim to have infiltrate government bodies and publishing sensitive information to disrupt perceived justice. Their motivation for staging these attacks and the subsequent publicization they received, as they mentioned in the interview gave them the sense of satisfaction of being able to make people happy and this further fueled their motivation to intensify their efforts. Their key technical specialization lies in the penetration testing and vulnerability detection. Despite their secretive nature, they do share that they utilize zero-day vulnerabilities and exploit human errors within target organizations to successfully breach their systems. While their operations aren't driven by financial gains, they did say in the interview that they earn significant income from selling data and government and financial access. Looking ahead, their ambition is to form a powerful global group standing against corruption and defending human rights.

*https://www.cyfirma.com/outofband/unveiling-deltaboys-interview-about-their-past-and-motivation/

NEWS HIGHLIGHT: THE CLOSURE OF BREACH FORUM

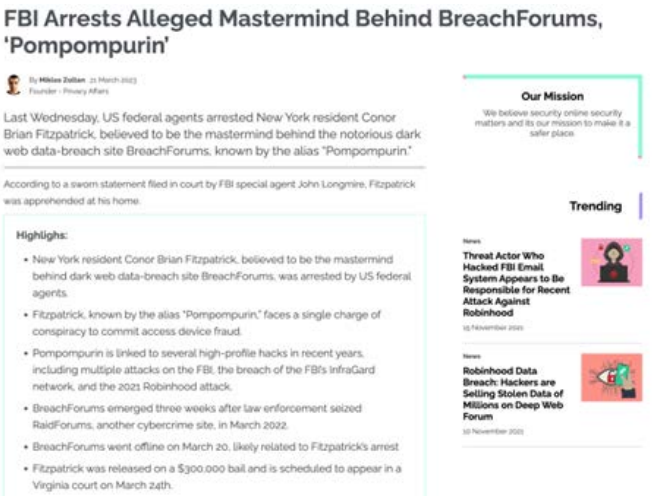


On 17th March 2023, a news reported that the mastermind behind the largest darkweb forum **Breached.vc,** an individual known as Conor Brian Fitzpatrick, or Pompompurin (his darkweb monicker) was arrested by FBI. This subsequently call for the closure of the forum by his associate, a TA with the Admin right "Baphomet".

The closure of the forum gave a huge impact to the data breach activities on the darkweb, where a lot of trades and sharing halted. The following is the strings of events that ensues dramas of scuffles between Threat Actors who are trying to regroup into new different forums.

The following timeline graphs shows the events since the closure of Breached.vc

- https://www.privacyaffairs.com/pompompurin-arrested-breach-forums/
- https://www.bloomberg.com/news/articles/2023-03-17/dark-web-breachforums-operator-charged-with-computer-crime


FBI Arrests Alleged Mastermind Behind BreachForums, 'Pompompurin'

Last Wednesday, US federal agents arrested New York resident Conor Brian Fitzpatrick, believed to be the mastermind behind the notorious dark web data-breach site BreachForums, known by the alias "Pompompurin."

According to a sworn statement filed in court by FBI special agent John Longmire, Fitzpatrick was apprehended at his home.

Highlighs:

- New York resident Conor Brian Fitzpatrick, believed to be the mastermind behind dark web data-breach site BreachForums, was arrested by US federal agents.
- Fitzpatrick, known by the alias "Pompompurin," faces a single charge of conspiracy to commit access device fraud.
- Pompompurin is linked to several high-profile hacks in recent years, including multiple attacks on the FBI, the breach of the FBI's InfraGard network, and the 2021 Robinhood attack.
- BreachForums emerged three weeks after law enforcement seized RaidForums, another cybercrime site, in March 2022.
- BreachForums went offline on March 20, likely related to Fitzpatrick's arrest
- Fitzpatrick was released on a $300,000 bail and is scheduled to appear in a Virginia court on March 24th.

Our Mission

Trending

Threat Actor Who Hacked FBI Email System Appears to Be Responsible for Recent Attack Against Robinhood

Robinhood Data Breach: Hackers are Selling Stolen Data of Millions on Deep Web Forum


Dark Web 'BreachForums' Operator Charged With Computer Crime

Pompompurin's profile on the BreachFourms website.

By Bob Van Voris, and William Turton
March 17, 2023 at 5:26 PM EDT
Updated on March 17, 2023 at 7:18 PM EDT

Federal agents have arrested a Peekskill, New York, man they say ran the notorious dark web data-breach site "BreachForums" under the name "Pompompurin."

Conor Brian Fitzpatrick was arrested by a team of investigators at his home around 4:30 p.m. Wednesday, an FBI agent said in a sworn statement filed in court the next day. Fitzpatrick is charged with a single count of conspiracy to commit access device fraud.

THE IMPACT OF THE CLOSURE

The aftermath of the Breached.vc closure is impactful to the community of Threat Actors. Major Threat Actors have been seen migrated to other forums or newly formed forums. The visualization above shows the list Threat Actors who were active in Breached.vc (on the left) have made their way to other forums, which are depicted on the forums list on the right.

TIMELINE OF EVENTS FROM THE CLOSURE OF BREACHED.VC TO PRESENT DAY

The following is the timeline of events post-closure of Breached.vc, a popular darkweb forum among threat actors with similar interest in breached/leaked data. The closing down of the forum by the FBI has given rise to a new drama between forums. On the last of our observation on 27th June 2023, we observed the BreachForums was on 2 hours downtime as announced by the admin of the forum Baphomet in their Telegram channel. The BreachForums however is still running as usual until now.

RANSOMWARE GROUP

MALAYSIA SECTORS AFFECTED WITH RANSOMWARE

The heatmap shows the number of incidents of sectors in Malaysia which fall victim to ransomware. It is profoundly alarming to discover that our education sector is with the highest number of ransomware victims. This also signify the dire needs to fortify this sector in terms of cybersecurity at both infrastructure and education against this threat.

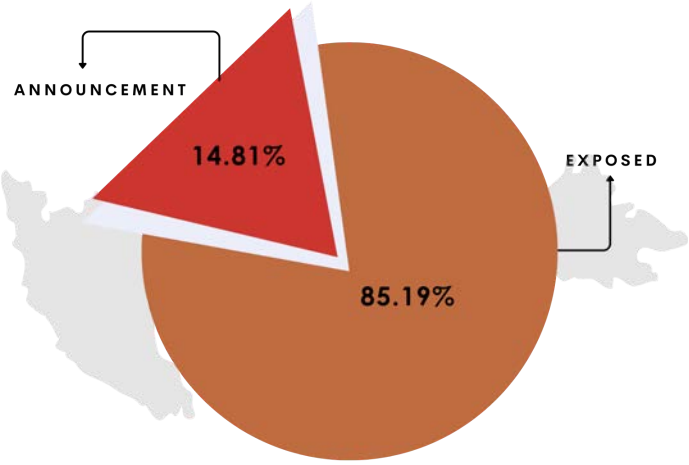
Ransomware stands out as a cyber threat that has gained infamy and notoriety. This malicious software, known for holding data hostage in exchange for a ransom, has etched its name in the annals of cyber threats due to its crippling effects on systems and the audacity of its demands.

Even though the incidents involving ransomware in this country may appear to be few in number, it's vital to note that the variety of sectors being impacted is surprisingly diverse. This suggests that ransomware perpetrators are not particularly choosy, casting a wide net to ensnare various types of organizations.

The scale or frequency of ransomware attacks, whether large or small, should not cause us to underestimate the gravity of this threat. Even the seemingly smallest ransomware issue should command our utmost attention and vigilance. These attacks, no matter the scale, can have far-reaching consequences that ripple through not only the targeted entity but also the broader community and economy.

RANSOMWARE TAG

The ransomware groups' campaigns landscape is dominated by a staggering 85.20% of cases involving the exposure of victim companies' data, as depicted in the pie chart. In contrast, a much smaller 14.8% represents ransomware groups merely making announcements, likely as intimidation tactics or public posturing without actual data exposure.

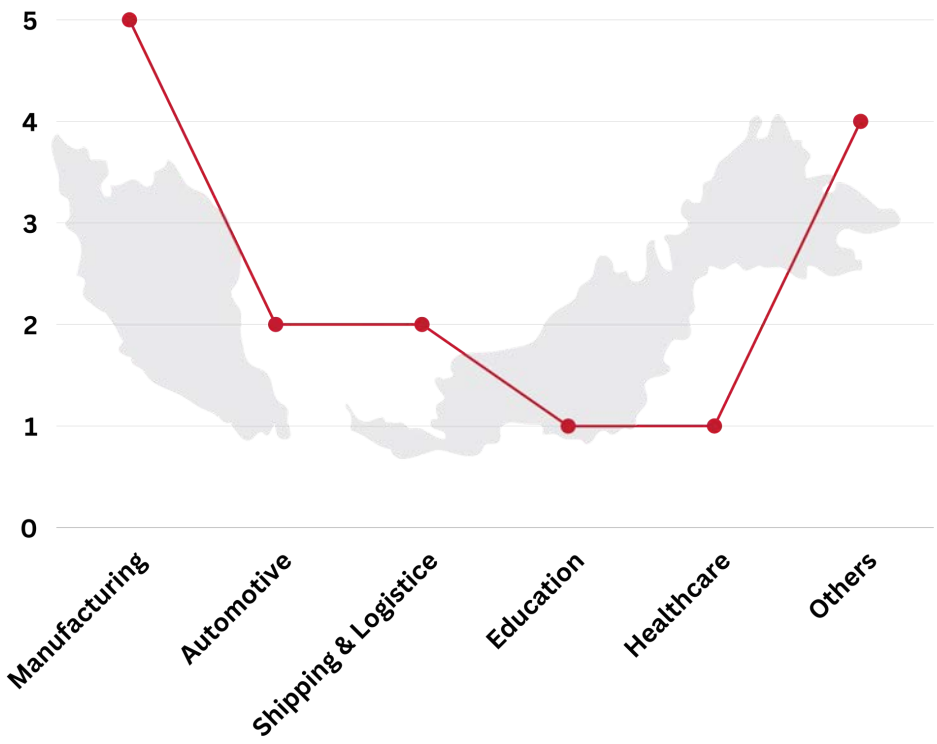


WORDCLOUD OF RANSOMWARE GROUP

The word clouds here depicting the ransomware groups that are targeting Malaysia. From January to June 2023, we observed only eleven ransomware groups which locked their targets on to Malaysian governments and companies. In this word cloud, the size of the group name indicates the number of campaigns they did – the more substantial the size of the group's name, the higher the number of campaigns they spearheaded. This gives an immediate visual cue on which groups were the most aggressive in their pursuit.

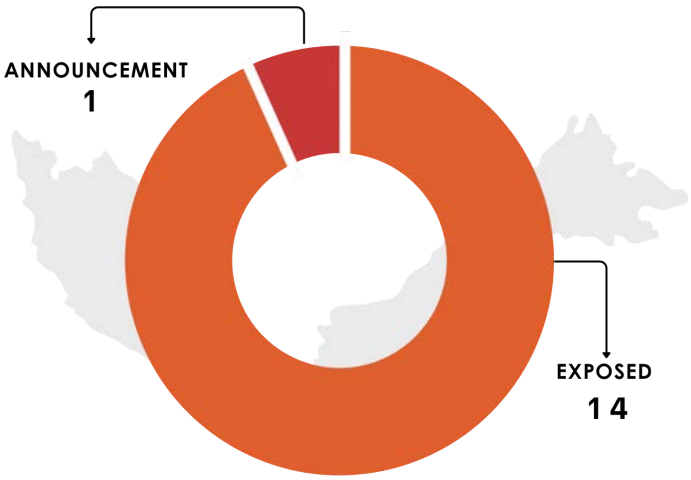
The second word cloud is the logos that are being used for each of the ransomware group. Some of the groups operated without logo to represent them, for instance Snatch, Daixin, and Ransomexx.

SECTORS AFFECTED BY LOCKBIT



As majority of the cases recorded on ransomware incidents in Malaysia are related to Lockbit, therefore we are diving into their campaigns on this country in the first half of this year. The above graph shows the affected six sectors by Lockbit's campaigns. It seems during this period their campaigns are targeting sectors related to industries, education, and healthcare but none are targeting the government sectors.

LOCKBIT BY TAGS



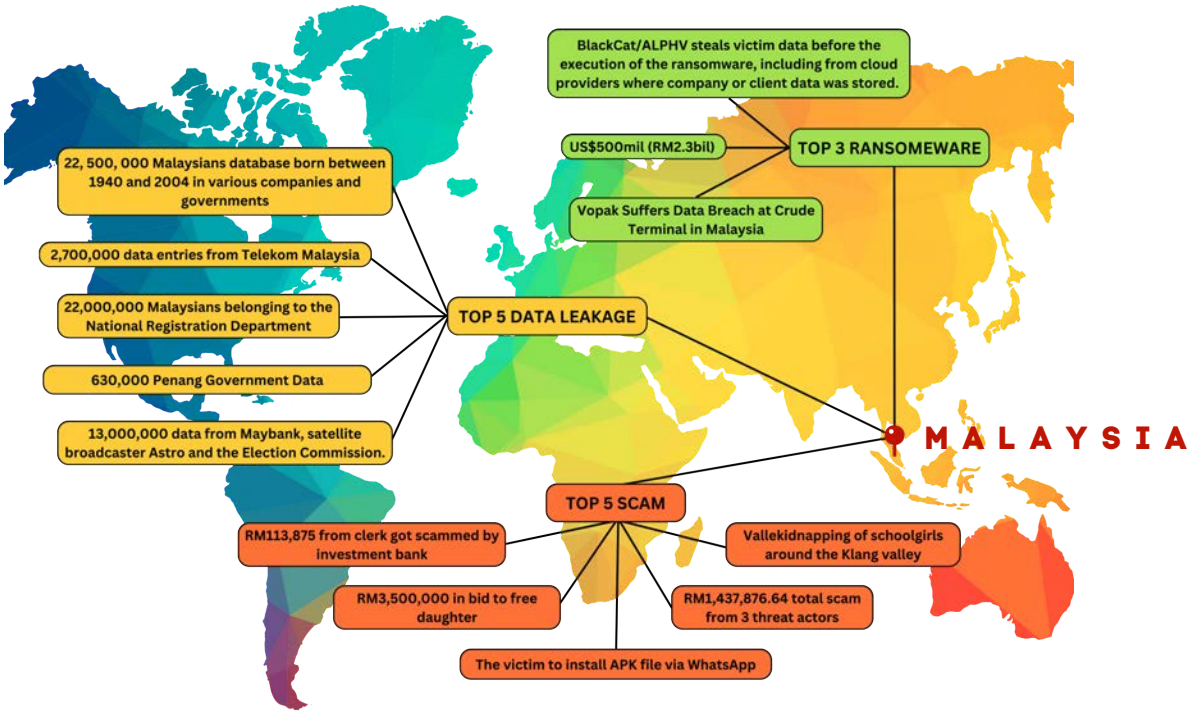
When looking further into the tags related to ransomware campaigns, the Lockbit group has been associated with 14 instances of data exposure and 1 instance related to announcement. Their modus operandi (or MO) involves in making public declarations about their victims on their website, in which hosted on dark-webs.

To further details their MO, the group uses their website as a platform to broadcast their targets by giving them the deadlines to settle the ransom before they expose the victim's data. This tactic is not only intimidating but also can potentially damaging the victims' reputations.

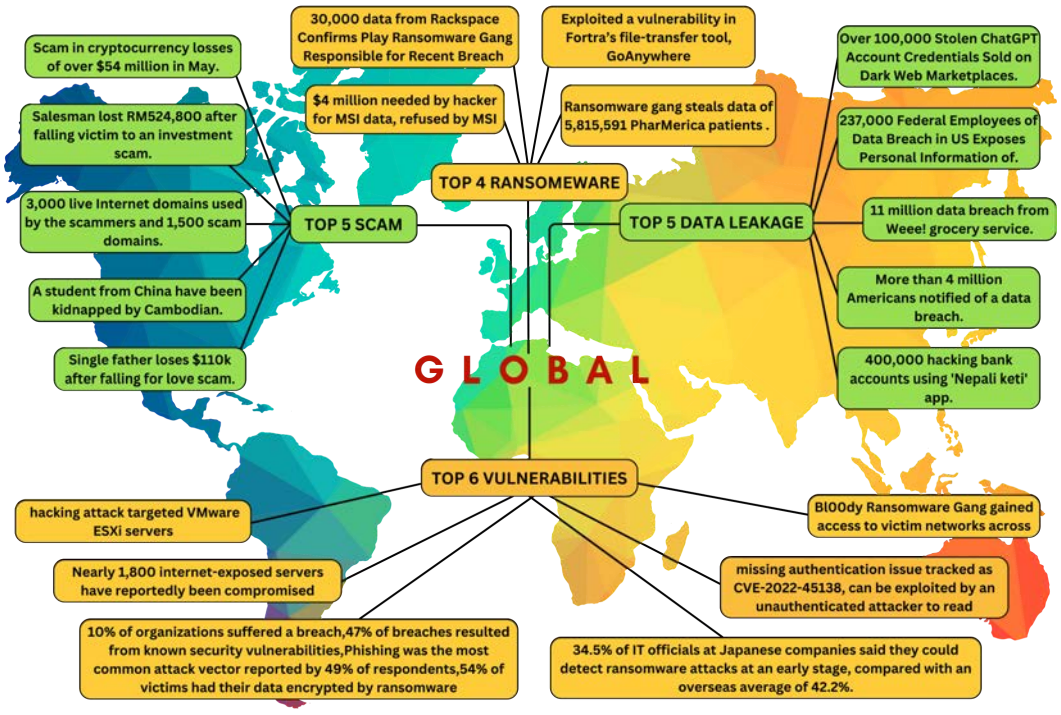
CYBER THREAT LANDSCAPE

- In this segment, we explore the cyber threat scenario in Malaysia through the lens of mainstream medias - the information platforms accessible to those who primarily use the surface web. The data represented in the graphs may not be entirely accurate, as they are extracted from search engines relying on particular keywords. The objective of these visualizations is to offer a broad understanding of the cyber threat information that the average internet user might gather from the surface web. For this analysis, we tracked frequently used search engines for keywords linked to cyber threats. We then categorized and illustrated this gathered data where the focal of the analysis would be on two perspectives – Malaysia and Global.
- Subsequently, we amassed data regarding the cyber threat environment in Malaysia through our Cyber Threat Intelligence platforms. This data is compiled from a variety of cybersecurity channels that contribute to shared threat feeds and offer a holistic view of the threats present. This approach ensures we have the most up-to-date and relevant information necessary for accurately depicting the cyber threat scenario in Malaysia.

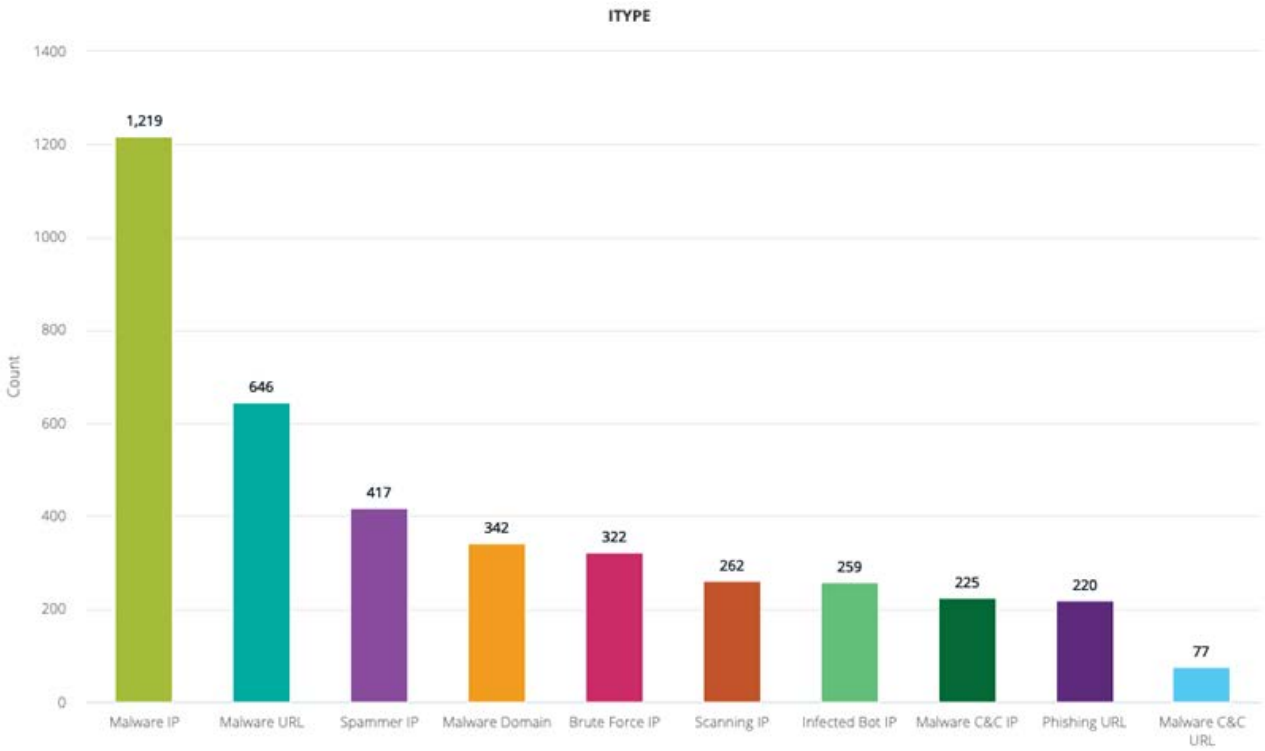
TOP REPORTED CYBER THREATS FROM MALAYSIA MASS MEDIA



TOP REPORTED CYBER THREATS FROM MALAYSIA MASS MEDIA GLOBALLY

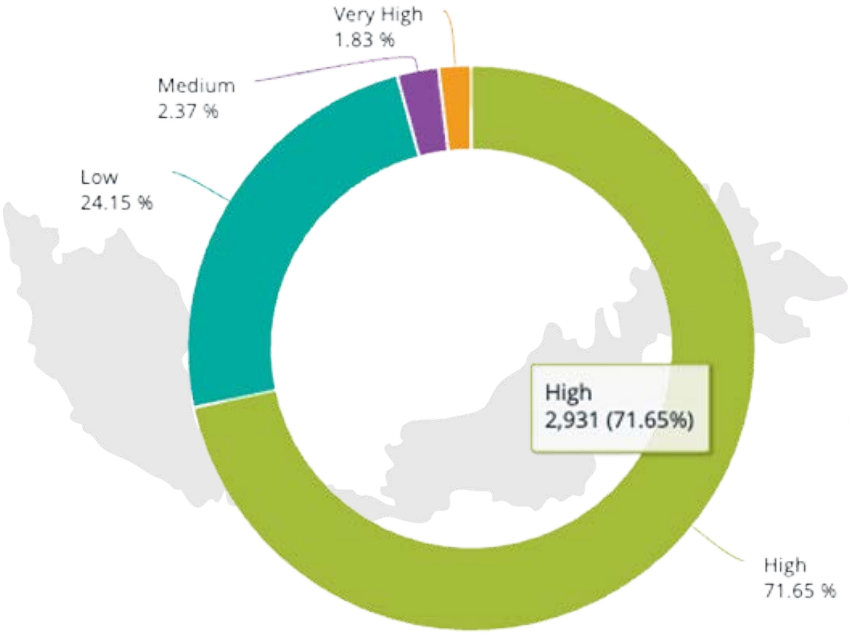


OUTBOUND THREATS MALAYSIA BY TYPES

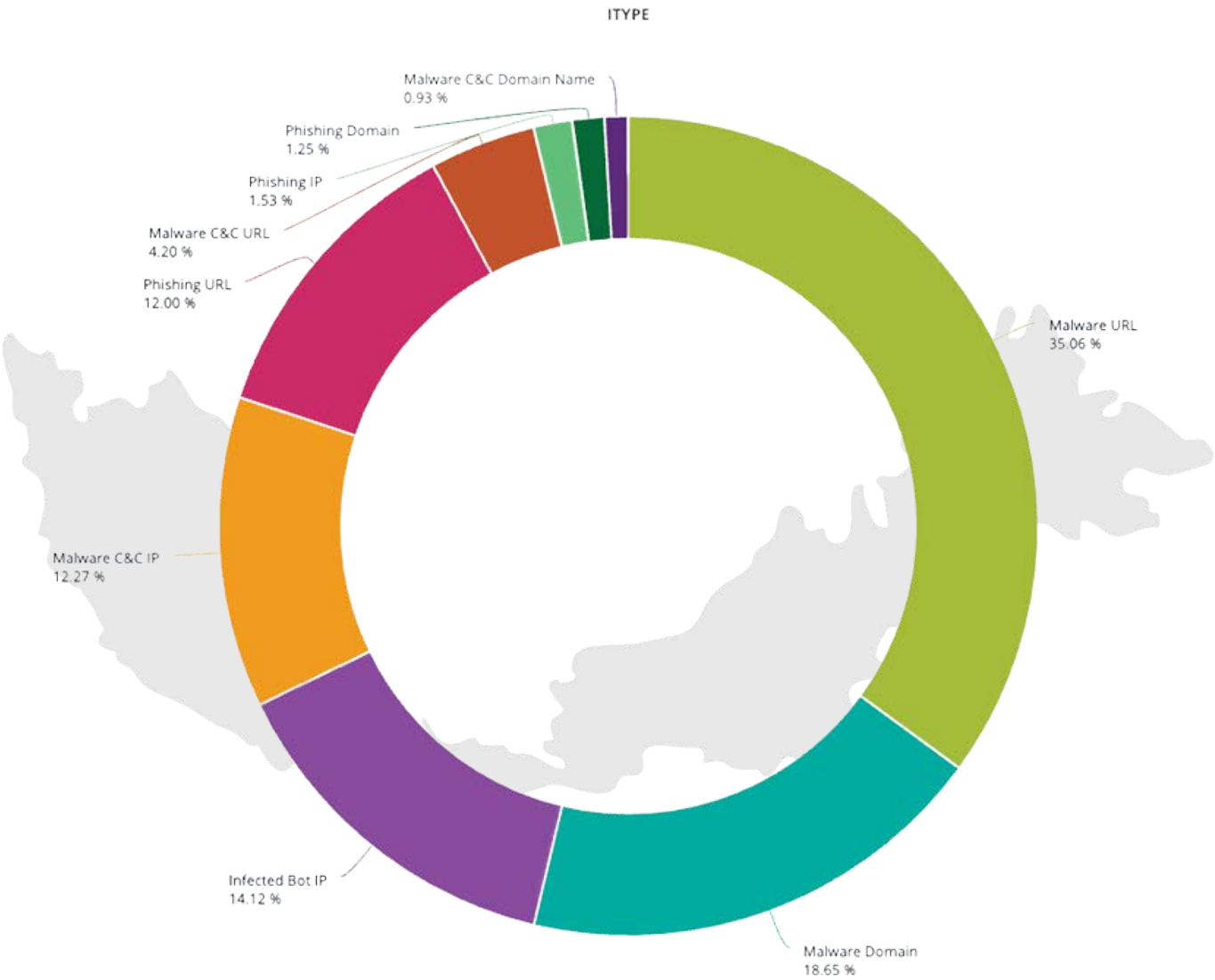


From the data aggregated by our Cyber-Threat Intelligence Platform on Malaysia, we visualize the outbound threats from Malaysia. Within 6 months of our observation, 3989 incidents information are gathered by our platform, in which is shown in the first visualization above. A closer look at the data reveals an overwhelming predominance of malware and phishing attacks, indicating these to be the primary areas of concern.

OUTBOUND THREATS MALAYSIA BY SEVERITY



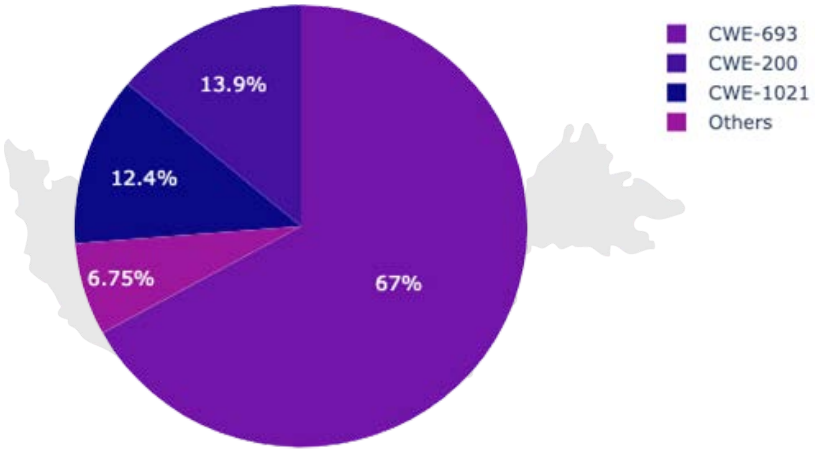
What follows are the distribution of the severity of these incidents. It is alarming to learn that 71.65% of these cyber issues are in High rate of severity



Taking a deeper dive into the issues at hand, we observed that a substantial 85.23% of the threat feeds related to Malaysia are occupied by malware concerns. This implies that most of the cyber threats in this context are related to malicious software designed to infiltrate or damage systems. Looking at another perspective, this number of outbounds malware issues detected is signifying the potential use of Malaysia infrastructures as hub for cyber-attacks.

Conversely, the remaining 14.77% encompasses phishing-related elements, including phishing URLs, IP addresses, and domains. This segment is indicative of deceptive tactics aimed at tricking individuals into revealing sensitive data, often by masquerading as a trustworthy entity. The data underscores the urgent need for robust defenses against malware, while also not underestimating the significance of fortifying against phishing attempts.

CWE COUNTS OBSERVED



On Common Weakness Enumeration of Malaysia governments, our Cyber Threat Intelligence Platform reveals the overall weaknesses. Most of our government ministries and agencies observed have three major CWEs. The following is pie chart depicting the distribution of CWE codes and explanation of each CWE code.

CWE EXPLAINATION

CWE-CODE	DESCRIPTION	EXTEND DESCRIPTION
CWE-693	The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product.	This weakness can be categorized into three situations: "missing," "insufficient," and "ignored" protection mechanisms. A "missing" mechanism refers to the absence of any defense against a particular type of attack. An "insufficient" mechanism offers partial protection, usually against common attacks, but fails to cover all intended threats. Lastly, an "ignored" mechanism exists within the product but is not implemented in certain sections of the code by the developer.
CWE-200	The web application does not restrict or incorrectly restricts frame objects or UI layers that belong to another application or domain, which can lead to user confusion about which interface the user is interacting with.	To ensure user safety, a web application should enforce limitations on its rendering within frames, iframes, objects, embed, or applet elements. Failure to implement these restrictions can lead to user manipulation and unintended interactions with the application.
CWE-1021	The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.	Mistakes resulting in information exposures can have varying levels of severity, depending on the context and type of sensitive information involved. This includes personal data, system status, business secrets, network configuration, code, metadata, and indirect information. Different parties, such as users, data subjects, administrators, and developers, may have their own expectations for protecting sensitive information. Information exposures can occur through explicit or indirect insertion of sensitive data into accessible resources, or unintentional accessibility of sensitive resources. It is important to differentiate information exposures from generic confidentiality breaches. CWE-200 and its subcategories specifically focus on mistakes related to the management, storage, transfer, or cleansing of sensitive information.

- https://cwe.mitre.org/

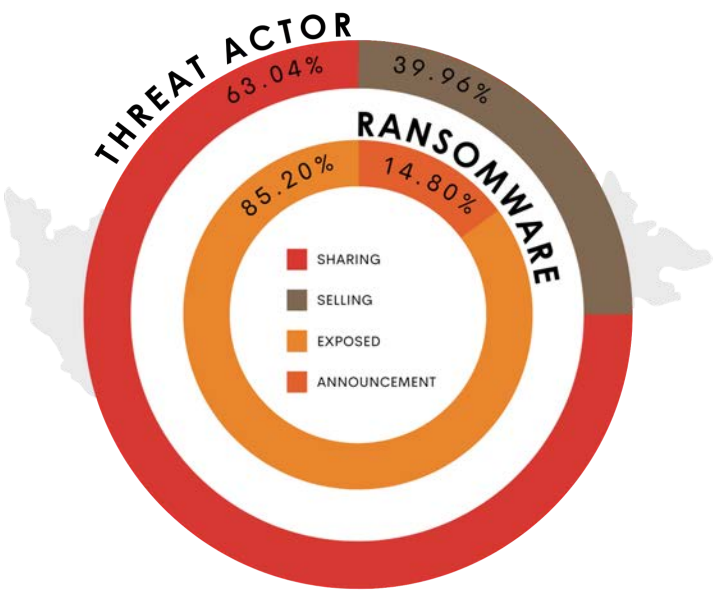
MITIGATION AND WAY FOWARD

- In this segment we will draw a conclusion to the 6 months observation into Malaysian Threat Landscape of the mid-year 2023.

- From the conclusion we will formulate possible mitigation plan, suggestion for continuous monitoring and improvement, and recommendations.

CONCLUSION

In drawing the conclusions to our 6 months observation, we would like to recap the overall situation regarding the data breaches in Malaysia, and the associated Threat Actors that are targeting Malaysia sensitive data.



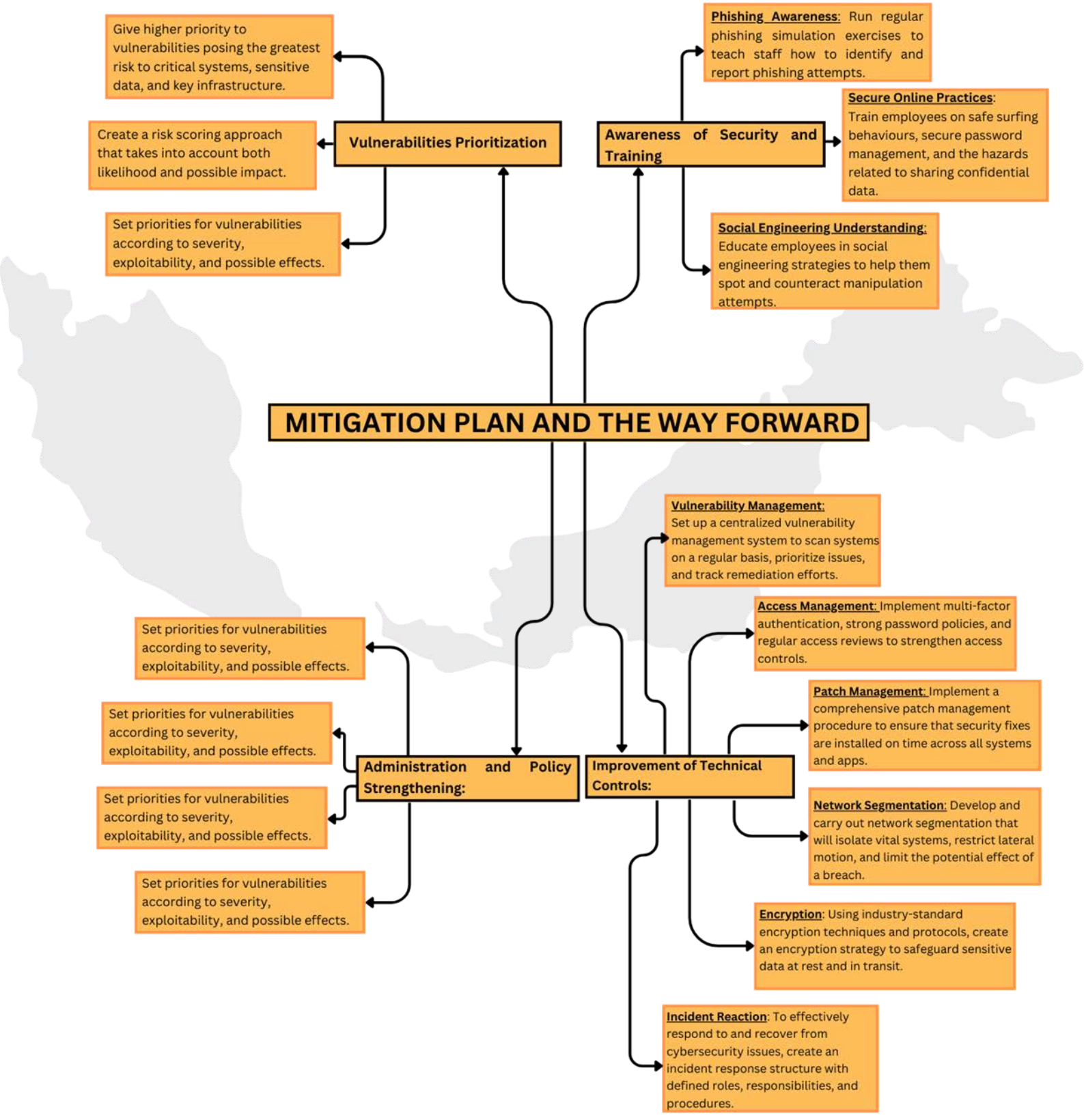
The above chart depicts the summarized activities of Threat Actors on data breach/leak and the prevalence of ransomware groups. A significant 63.04% of Threat Actors are found to be sharing leaked data, which indicates a willingness to disseminate information potentially for strategic or malicious purposes. Conversely, 36.96% of Threat Actors are engaged in selling and promoting this data, likely for financial gain. Regarding ransomware, the overwhelming 85.2% of cases involve the exposure of victims' data, which can have devastating consequences for both individuals and organizations.

The remaining 14.8% is constituted by announcements, which may be intended as warnings or intimidations. This data emphasizes the critical need for comprehensive cybersecurity measures to combat the multi-faceted threats posed by Threat Actors and ransomware, which not only for seeking financial profit but also to exploit and to share sensitive information with potentially wide-ranging ramifications.

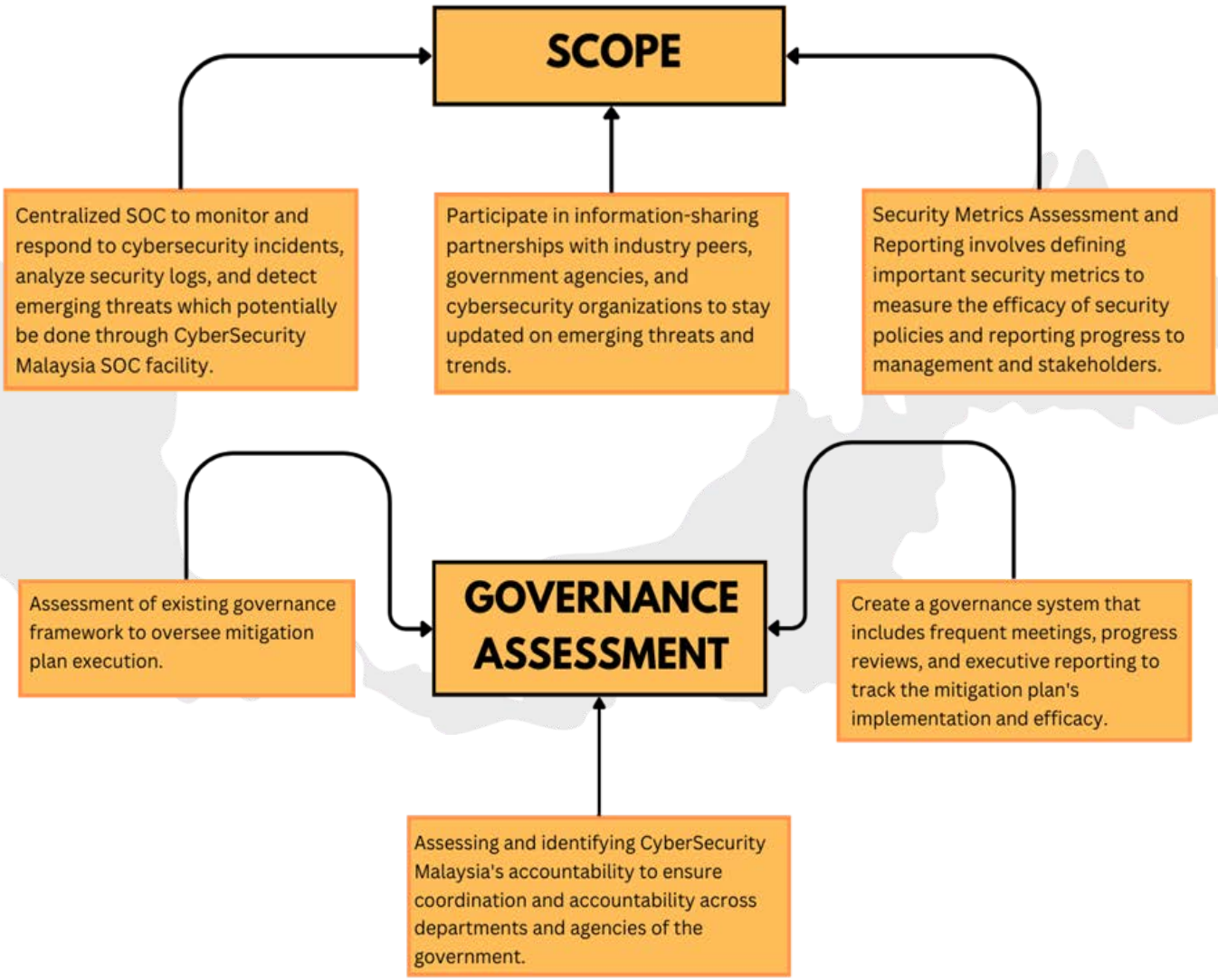
We also covered the threat landscape from the perspective of mainstream medias on both Malaysia locally and internationally, in order to identify the gaps between what our cyber threat intelligence data and what the public might know from the coverage of the journalism.

Finally, we covered the Malaysia threat landscape from the Cyber Threat Intelligence Platform standpoint. From the threat feeds aggregated on Malaysia threat landscape, we identified phishing and malware related cyber issues are still prevalent in the first half-year of 2023.

In this section, we proposed the mitigation and the way forward in lessening the issues in the future. For the mitigation plan, we are looking at four prospects, for in each we elaborated the suggestions for improvement, strengthening, prioritization, and knowledge and skills enrichments.



CONTINUOUS MONITORING AND IMPROVEMENT

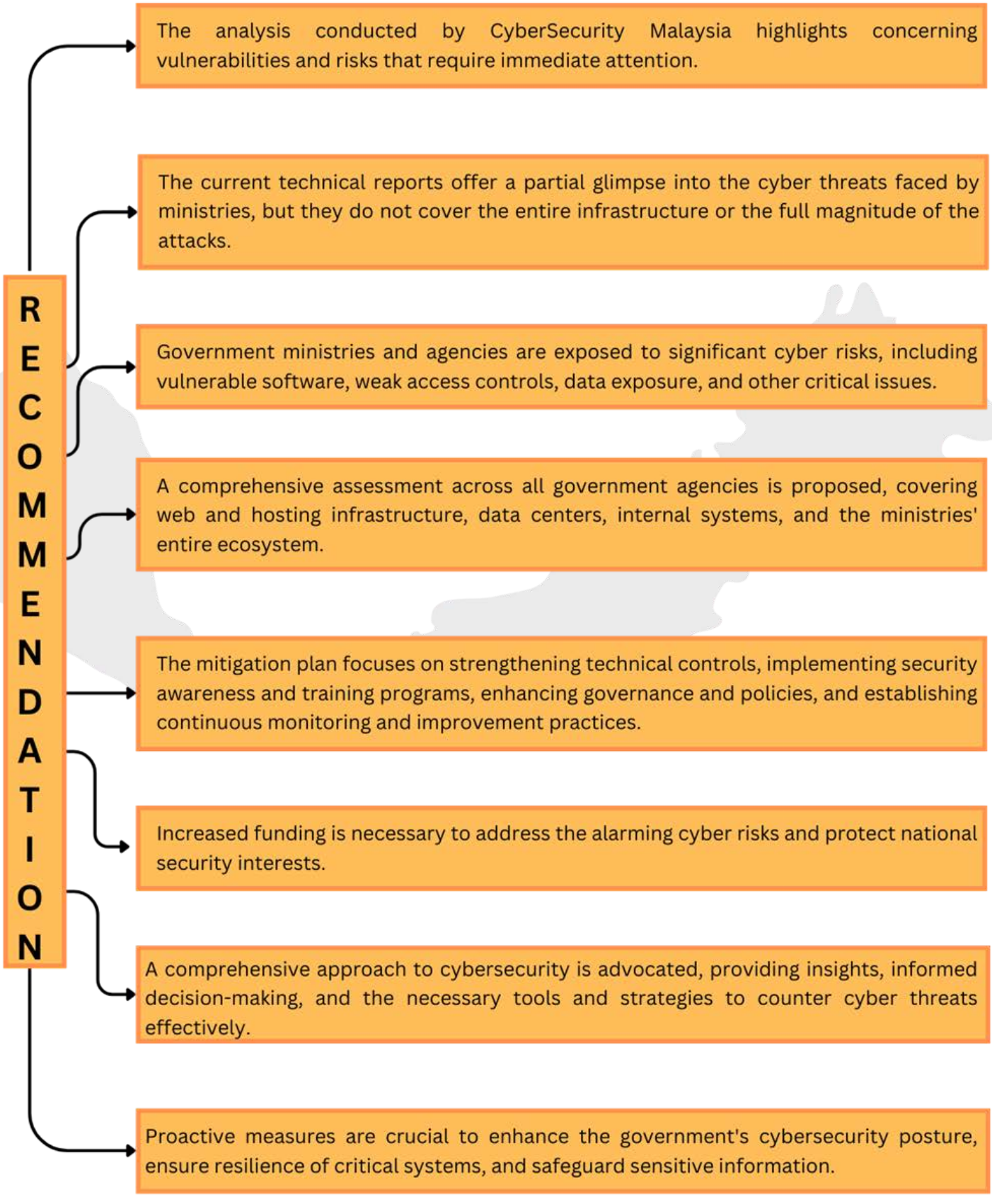


As data breaches and ransomware looming large in our countries, it essential for us to proactively enhancing our cybersecurity capabilities through continuous monitoring and improvements. It is imperative to adhere the scopes for such monitoring via centralized SOC, establishing threat feeds sharing partnerships, and develop security metrics and reporting.

Beyond these technical considerations, an in-depth governance assessment is crucial. The assessment would help in pinpointing gaps in policies, procedures, and accountability measures, enabling us to fortify our governance system against potential cyber threats.

In conclusion, it is critical to perceive this continuous monitoring and assessment as a core part of cybersecurity strategy as strengthening defenses is integral to safeguards digital assets and maintaining trusts of stakeholders.

In this section, we propose recommendations in a way forward to further strengthening our cyber defends against the evolving cyber threats that our country is facing.



CyberSecurity Malaysia
Level 7, Tower 1, Menara Cyber Axis
Jalan Impact, 63000 Cyberjaya
Selangor Darul Ehsan
Malaysia

Tel: +603 8800 7999
Fax: +603 8008 7000
Email: info@cybersecurity.my
Customer Service Hotline: 1 300 88 2999
www.cybersecurity.my

@cybersecuritymy
CyberSecurityMalaysia
cybersecurity_malaysia
CyberSecurityMy

MINISTRY OF
COMMUNICATIONS AND DIGITAL