

RANSOMWARE THREAT LANDSCAPE REPORT FOR ASIA PACIFIC

TLP: WHITE

2022



GreyInt



GreyInt

RANSOMWARE THREAT LANDSCAPE REPORT FOR ASIA PACIFIC 2022

Under the All Rights Reserved to GreyInt 2022:

This publication may be reproduced in whole or in part and in any form for non-profit purposes without special permission from the copyright holder, provided acknowledgement of the source is made. GreyInt would appreciate receiving a copy of any publication that uses this publication as a source.

TABLE OF CONTENT

●	INTRODUCTION.....	4
●	RANSOMWARE INCIDENTS AS REPORTED IN THE MEDIA.....	7
●	STATISTICS	8
	EAST ASIA	11
	SOUTH ASIA	12
	SOUTHEAST ASIA	13
	OCEANIA	14
●	TOP THREAT ACTOR: LOCKBIT 2.0	15
	COUNTRIES AFFECTED	17
	SECTORS IMPACTED	17
	TACTICS, TECHNIQUES AND PROCEDURES	18
●	CASE STUDY: RANSOMWARE ATTACK ON BANGKOK AIRWAYS	19
●	OUTLOOK AND CONCLUSION.....	22





INTRODUCTION

INTRODUCTION



On 6 August 2021, a Singapore-based private medical center was hit by a cyberattack that impacted nearly 73,500 of its patients' data. Details including personally identifiable information (PII) such as names, addresses, identity card numbers, contact details and clinical information were affected. The unidentified threat actors reportedly deployed malware that locked up files in its clinic management systems and servers at one of its branches and demanded a ransom to be paid in order to unlock them. A month later, on 18 September, a Malaysia-based web hosting service provider was hit by a similar cyberattack, disrupting its services. According to reports, the threat actors demanded USD 900,000 in cryptocurrency in order to unlock their files. Both entities were impacted by a type of malware known as ransomware.

Ransomware is a form of malware that encrypts files in a system infected by it. These encrypted files are locked, preventing users from opening them until they are unlocked by a decryption key generally provided by the threat actor behind the ransomware. The decryption key would generally be provided after a ransom has been paid, though there is no guarantee. Depending on the type of ransomware and the threat actor operating it, victims have been threatened and demanded to pay ransom from as little as USD 30 to a staggering USD 70,000,000 in order to obtain the decryption key.

The delivery of ransomware differs, depending on the preferred tactics, techniques and procedures (TTPs) employed by ransomware operators or its affiliates. One of the most common techniques to deliver ransomware is via phishing, either in the form of an attachment or a malicious link in email messages. Threat actors have also masqueraded ransomware as legitimate or cracked software uploaded in file hosting sites where users would download either directly from the websites or via Torrents.

There is also a category of ransomware threat actors who deploy ransomware manually after breaching victims' networks. Commonly referred to as "human operated" ransomware, threat actors would gain access to victims' networks or servers in multiple ways, conduct lateral movement, exfiltrate data before detonating the ransomware. Actors who operated its operations in this manner have also been categorized as Big Game Hunting (BGH) ransomware actors.

BGH is a term first coined in 2019, referring to ransomware threat actors targeting victim organisations that typically generate millions in revenue, and can potentially yield a greater financial payoff for the threat actors. Threat actors in the BGH business tend to incorporate data exfiltration techniques and sometimes, use zero-day exploits. Many of these actors operate a site, commonly known as dedicated leak site (DLS), in the dark web where victim names are listed, along with details such as sample data. Those who refused to pay the ransom, had their entire data published on the DLS.

This report highlights the events and statistics of victims gathered from BGH ransomware groups operating a DLS (sometimes known as victim shaming portals) in the TOR network (dark web) throughout the year 2021.



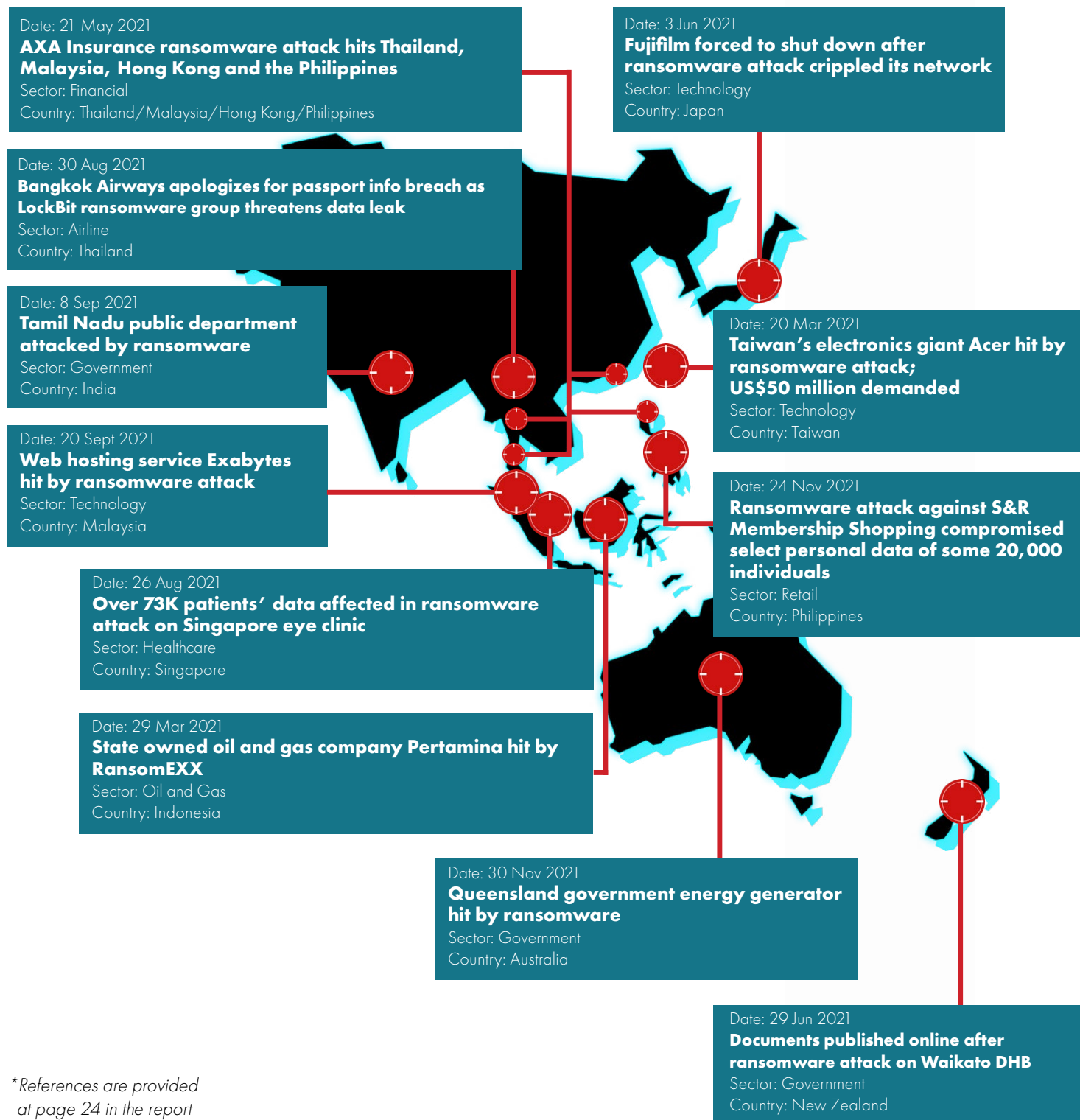


RANSOMWARE INCIDENTS **AS REPORTED IN THE MEDIA**

RANSOMWARE INCIDENTS AS REPORTED IN THE MEDIA



Organisations in Asia Pacific are not spared from ransomware attacks. Throughout the year 2021, almost every country in Asia Pacific were victims to ransomware. The map below highlights some of the headlines reported in the media.



**References are provided
at page 24 in the report*

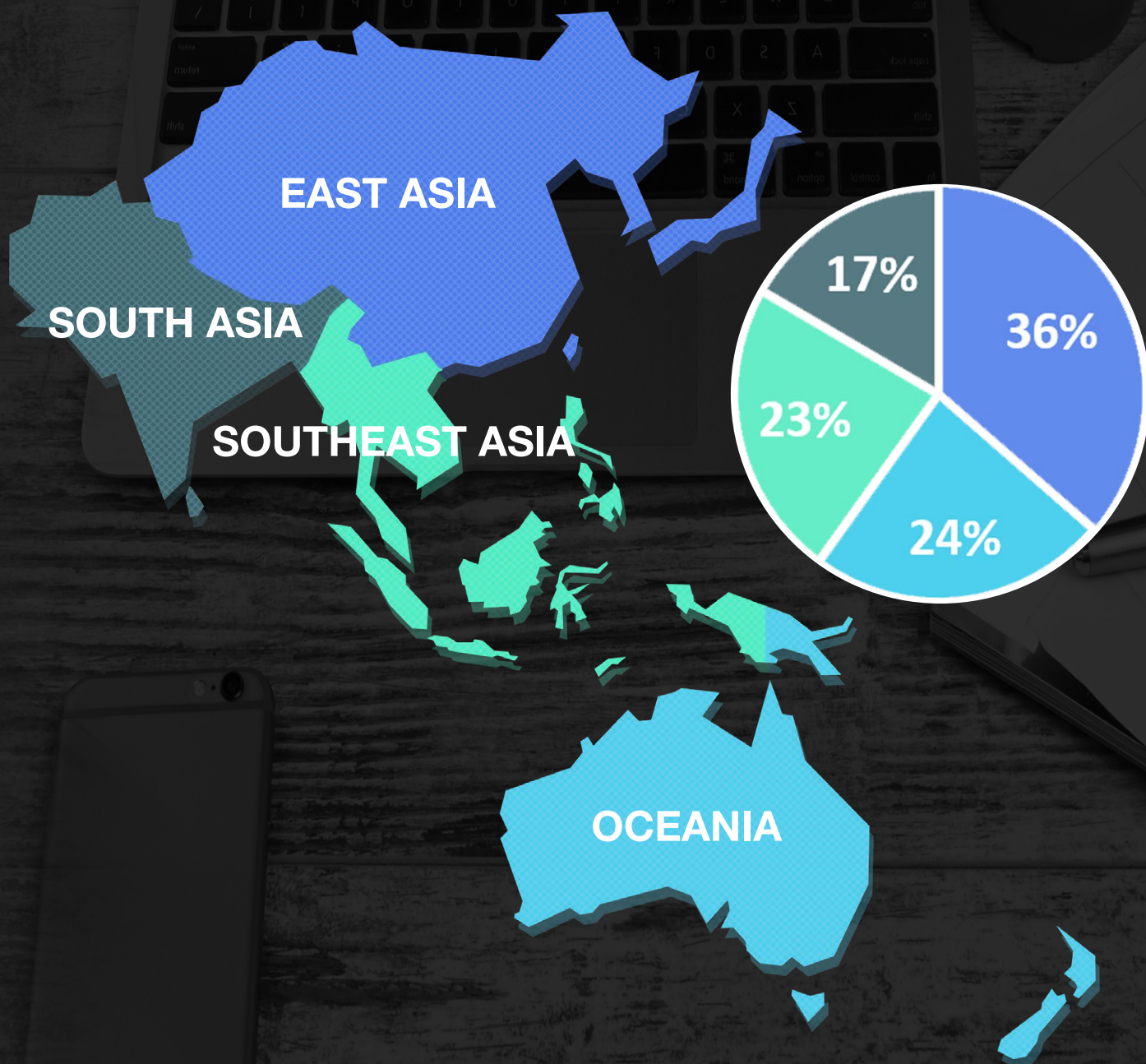


STATISTICS

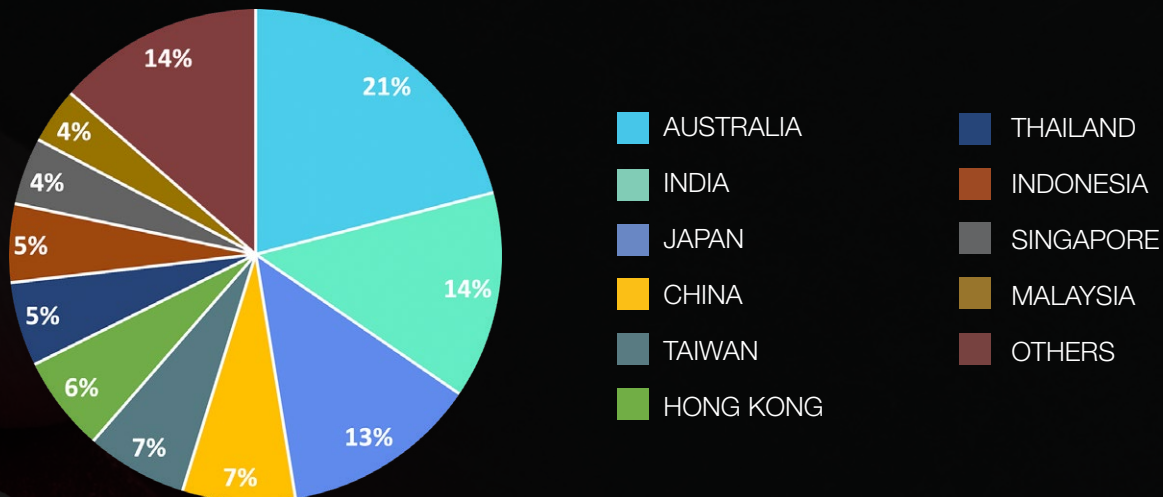
STATISTICS

In 2021, GreyInt identified more than 2800 victims listed in ransomware victim registry sites located in the dark web owned by BGH groups. This is a 103.9 per cent increase year-on-year from 2020. Out of the 2834 victims, close to 10 per cent were organisations and companies from APAC. The top 5 countries impacted in APAC were Australia, India, Japan, China and Taiwan while the top 5 sectors impacted in APAC were Manufacturing, Technology, Financial Service, Construction and Transportation. APAC were mainly hit by LockBit 2.0, Conti, Avaddon (inactive at time of writing), Sodinokibi (REvil) (inactive at time of writing) and LV.

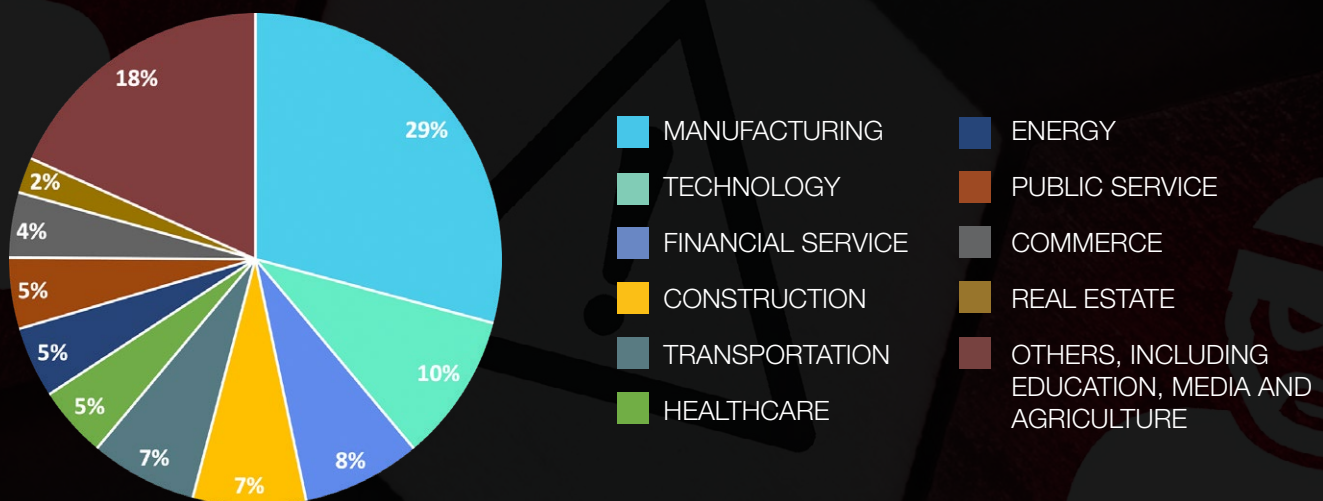
REGIONS



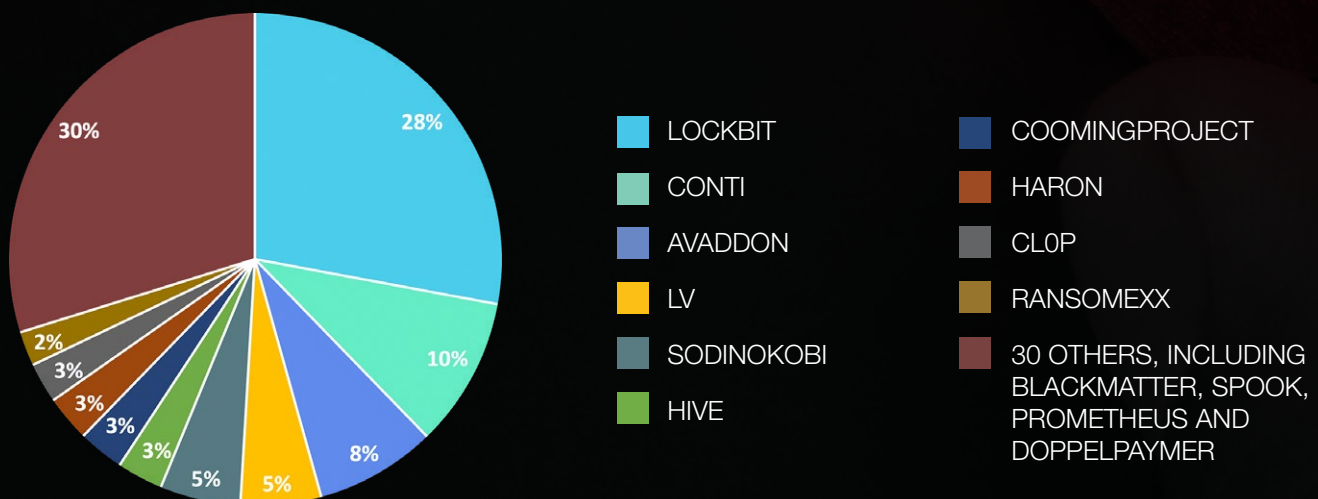
TOP 10 COUNTRIES IMPACTED



TOP 10 SECTORS IMPACTED



TOP 10 RANSOMWARE ACTORS

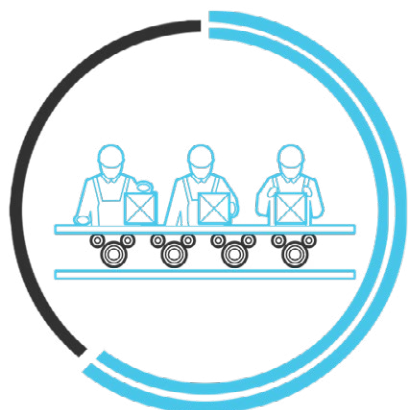


EAST ASIA

Three per cent of the overall victims globally comprises of East Asia-based organisations. This also constituted 36 per cent of the overall victims in APAC. The top 3 sectors impacted were Manufacturing, Technology and Transportation and the top 3 ransomware threat actors were LockBit, Sodinokibi (REvil) and Conti.



TOP 3 SECTORS



MANUFACTURING



TECHNOLOGY



TRANSPORTATION

TOP RANSOMWARE ACTORS



LOCKBIT



SODINOKIBI (REVL)



CONTI

SOUTH ASIA

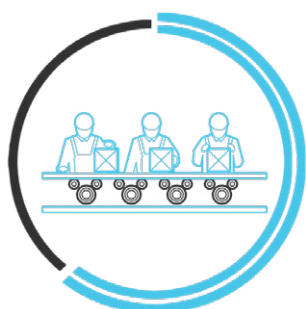
Two per cent of the overall victims globally comprises of South Asia-based organisations. This also constituted 17 per cent of the overall victims in APAC. The top 3 sectors impacted were Technology, Manufacturing and Energy and the top 3 ransomware threat actors were Conti, LockBit and CoomingProject.



TOP 3 SECTORS



TECHNOLOGY



MANUFACTURING



TRANSPORTATION

TOP RANSOMWARE ACTORS



CONTI



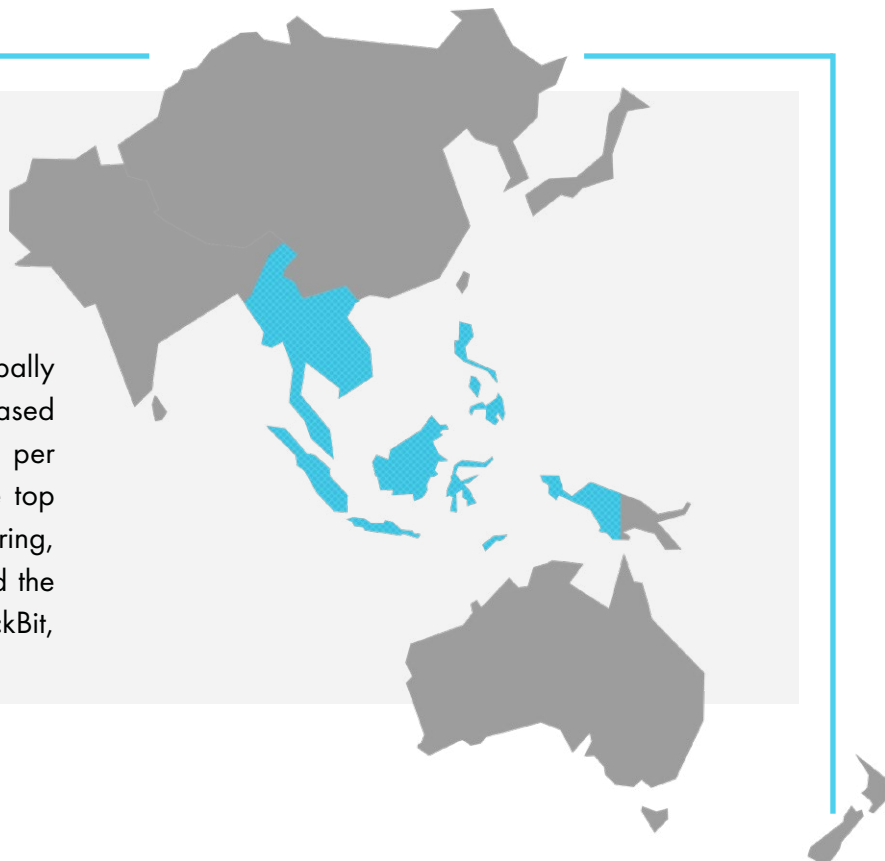
LOCKBIT



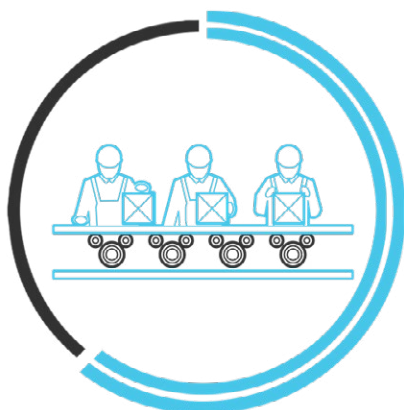
COOMINGPROJECT

SOUTHEAST ASIA

Two per cent of the overall victims globally comprises of Southeast Asia-based organisations. This also constituted 23 per cent of the overall victims in APAC. The top 3 sectors impacted were Manufacturing, Transportation and Financial Service and the top 3 ransomware threat actors were LockBit, Avaddon and Prometheus.



TOP 3 SECTORS



MANUFACTURING



TRANSPORTATION



FINANCIAL SERVICE

TOP RANSOMWARE ACTORS



LOCKBIT



AVADDON



PROMETHEUS

OCEANIA

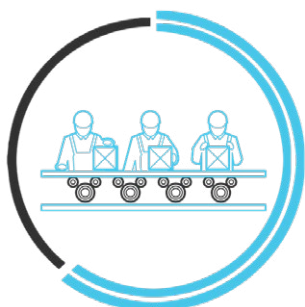
Two per cent of the overall victims globally comprises of Oceania-based organisations. This also constituted 24 per cent of the overall victims in APAC. The top 3 sectors impacted were Construction, Manufacturing and Healthcare and the top 3 ransomware threat actors were LockBit, Conti and LV.



TOP 3 SECTORS



CONSTRUCTION



MANUFACTURING



HEALTHCARE

TOP RANSOMWARE ACTORS



LOCKBIT



CONTI



LV



TOP THREAT ACTOR: **LOCKBIT 2.0**



LockBit 2.0

LockBit 2.0 (aka LockBit) is a financially motivated ransomware group first appeared in September 2019 and was initially known as 'ABCD' ransomware due to the '.abcd' extension appended to files it encrypted. The group operates a ransomware-as-a-service (RaaS) model relying on partnership and affiliates to use its ransomware payloads against targets. Members of LockBit 2.0 frequented the Russian-language forums such as XSS and EXPLOIT and used them to advertise their affiliate program, promote their ransomware capability and searching and purchasing compromised access to corporate networks.

In late June 2021, LockBit claimed to have developed "the fastest encryption software all over the world" and published this news to its revamped victim shaming site in the dark web. The revamped site suggests the group has rebranded themselves as LockBit 2.0. The group also offered a new data stealing tool called StealBit claiming to have the capability to automatically exfiltrate all files of a targeted company to its victim shaming site.

Tactics, techniques and procedures used by LockBit 2.0 vary as different affiliates may use different methods to gain initial access before delivering its ransomware. Besides gaining initial access through compromised credentials, VPN and RDP accounts, affiliates reportedly used phishing emails as well as exploiting a vulnerability in Fortinet devices tracked as CVE-2018-13379 to obtain VPN accounts.

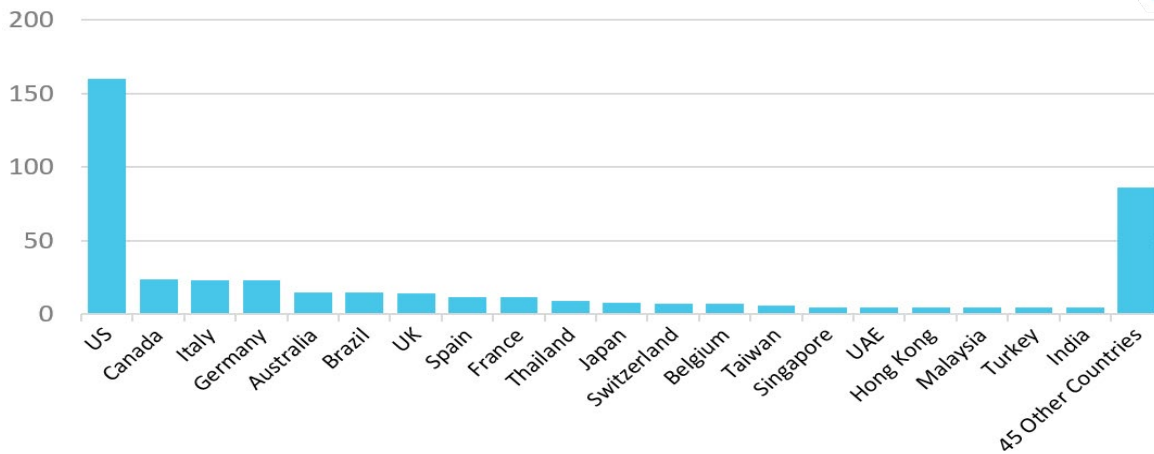
The group uses a double extortion technique where victims are demanded to pay ransom within a specific time frame. Victims refusing to pay will have their entire data leaked to the dark web, allowing its site visitors to download and access the stolen data freely.

LockBit 2.0 has impacted organisations and companies worldwide including UK rail network Merseyrail and consulting giant Accenture. In Asia Pacific, the group has targeted Press Trust of India and Thailand's airline company Bangkok Airways.

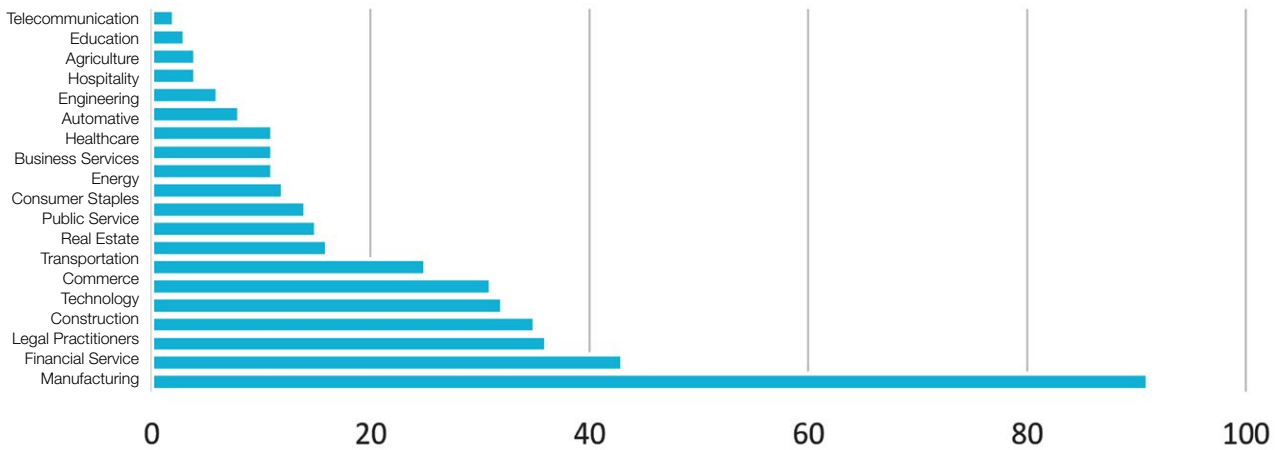




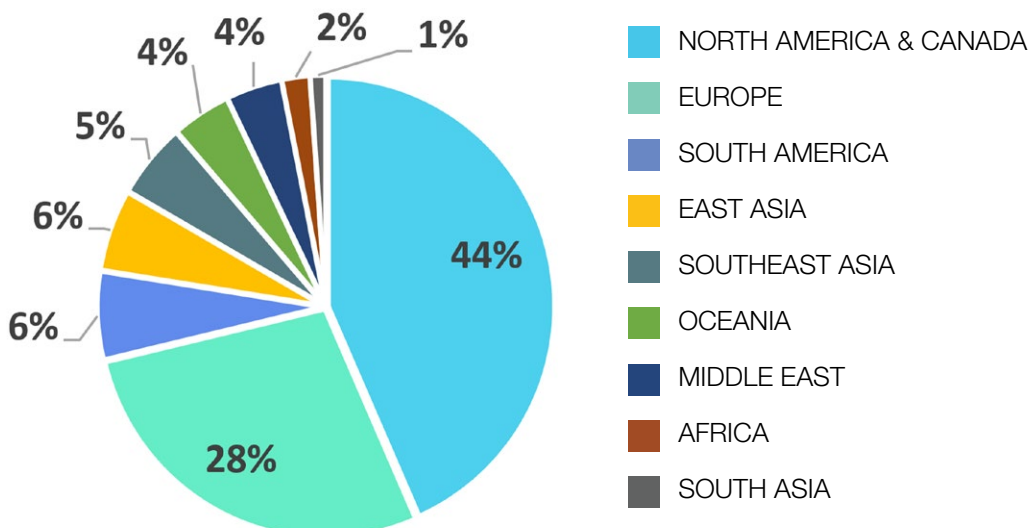
ORGANISATIONS IN COUNTRIES IMPACTED BY LOCKBIT 2.0



SECTORS IMPACTED BY LOCKBIT 2.0




REGIONS



LOCKBIT 2.0: TACTICS, TECHNIQUES AND PROCEDURES

TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1190: Exploit Public-Facing Application	T1059: Command and Scripting Interpreter	T1547: Boot or Logon Autostart Execution	T1562: Impair Defenses	T1003: OS Credential Dumping	T1087: Account Discovery	T1021: Remote Services	T1213: Data from Information Repositories	T1213: Data from Information Repositories	T1573: Encrypted Channel	T1041: Exfiltration Over C2 Channel	T1486: Data Encrypted for Impact
T1566: Phishing	T1059.001: PowerShell		T1562.001: Disable or Modify Tools		T1482: Domain Trust Discovery	T1021.001: Remote Desktop Protocol	T1039: Data from Network Shared Drive	T1039: Data from Network Shared Drive	T1219: Remote Access Software	T1567: Exfiltration Over Web Service	T1490: Inhibit System Recovery
T1566.001: Spearphishing Attachment	T1072: Software Deployment Tools		T1070: Indicator Removal on Host		T1046: Network Service Scanning		T1074: Data Staged	T1074: Data Staged			T1489: Service Stop
T1078: Valid Accounts	T1569: System Services				T1069: Permission Groups Discovery						
T1133: External Remote Services					T1069: Permission Groups Discovery						
			T1082: System Information Discovery								
					T1016: System Network Configuration Discovery						
					T1049: System Network Connections Discovery						
					T1033: System Owner/User Discovery						





CASE STUDY

RANSOMWARE ATTACK ON BANGKOK AIRWAYS



CASE STUDY: RANSOMWARE ATTACK ON BANGKOK AIRWAYS

On 26 August 2021, threat actors associated with LockBit 2.0 ransomware gang published details of Thailand's airline company Bangkok Airways to its blog on the dark web after they have breached the airline's network. The actors claimed to have stolen over 200 GB of data and eventually deployed ransomware to its computers. Public reporting suggests that Bangkok Airways refused to pay the ransom demanded by the ransomware gang which likely led to the release of its data. An investigation conducted by Bangkok Airways confirmed that personal data were accessed by the threat actors. This includes passenger name, family name, nationality, gender, phone number, email, address, contact information, passport information, historical travel information, partial credit card information, and special meal information.



Fig. 1: Bangkok Airways listed in LockBit 2.0 portal

A month before the ransomware attack on Bangkok Airways, on 20 July, GreyInt discovered a threat actor "babam" in a Russian-language hacking forum auctioning credentials, in the form of username and password, to a Cisco AnyConnect VPN network of an unnamed Thai Airline company. The post suggests the airline company has a revenue of USD 854 million. In addition, this post was given the 'thumbs up' by forum member LockBitSupp – an account used by LockBit 2.0 ransomware gang.

Using the details posted by the actor, GreyInt discovered that Bangkok Airways was listed as having the same amount of revenue mentioned by the actor. GreyInt also discovered a login portal to access Bangkok Airways internal network. The URI and the login interface suggest that Bangkok Airways was using Cisco AnyConnect VPN to access its private network. It is not known how the actor was able to obtain the credentials however, it is possible that the credential was used to login into Bangkok Airways via the VPN portal to access the airline's internal resources.

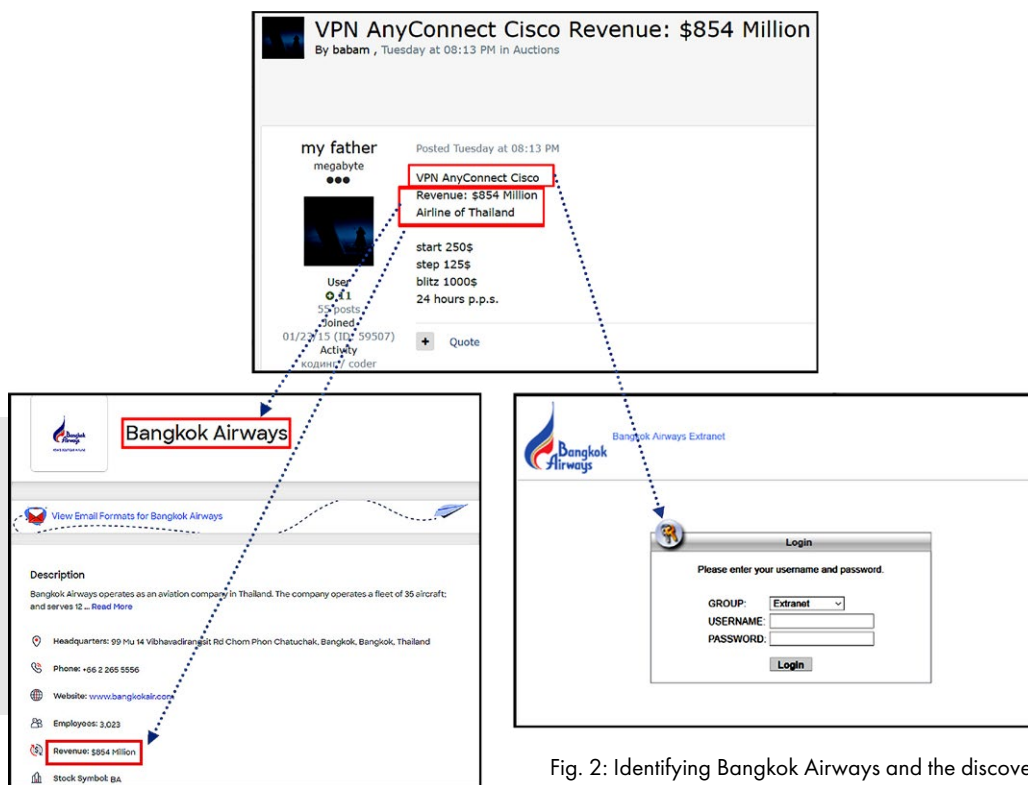


Fig. 2: Identifying Bangkok Airways and the discovery of a login portal using Cisco AnyConnect



Fig. 3: LockBitSupp giving a 'like' to babam's post

While there are no incident reports publicly published mentioning how LockBit 2.0 actors were able to breach Bangkok Airways network, GreyInt assesses with low confidence that LockBit 2.0 had bought the advertised compromised credentials, either directly with babam or through an access broker, and used them to gain initial access to Bangkok Airways network before deploying their tools and eventually detonating its ransomware.



OUTLOOK AND **CONCLUSION**

Ransomware will continue to be a pressing and urgent issue for many companies and organisations worldwide. The profitability yielded from ransomware attacks have risen from hundreds to millions of dollars and this will only attract more financially motivated actors to either develop their own version of ransomware or become an affiliate to them. While some ransomware groups have their operations 'shut down' due to supposedly international and political pressures from authorities and governments, it has been observed that new ones will be created or rebranded with different names.

GreyInt assesses that ransomware actors will likely increase their efforts in operational security given reports of actors associated directly with or affiliates to ransomware groups arrested by authorities. Additionally, ransomware actors will likely be quick in adopting new techniques such as leveraging on newly publicly published exploits and vulnerabilities to conduct their operations.

It is imperative for organisations to be resilient and prepare for ransomware attacks. Unlike other forms of cyber attacks, ransomware attacks can cause reputational damage, impacts confidentiality and affects the availability of an organisation's business. Mature organisations should also consider adopting an intelligence-led security operations model to ensure proactive research to identify new threats and be situationally aware of the cyber events happening in the region and globally.

GreyInt predicts that 2022 will be a testing year for organisations given the increase of ransomware groups in 2021. While BHG groups historically prefers to target large organisations with millions of profitable revenues, GreyInt has observed the same groups targeting smaller companies with less than a million in revenue. This suggests that ransomware groups no longer discriminate smaller organisations and will attack regardless of its size. Needless to say, no organisations is safe from ransomware attacks.

REFERENCES

1. <https://www.taiwannews.com.tw/en/news/4155964>
2. <https://www.merdeka.com/teknologi/data-internal-pertamina-bocor-dibobol-hacker.html>
3. <https://www.sangfor.com/en/info-center/blog-center/cyber-security/axa-insurance-ransomware-attack-hits-4-asian-countries>
4. <https://techcrunch.com/2021/06/03/fujifilm-becomes-the-latest-victim-of-a-network-crippling-ransomware-attack/>
5. <https://www.rnz.co.nz/news/national/445735/waikato-dhb-ransomware-attack-documents-released-online>
6. <https://www.straitstimes.com/tech/tech-news/nearly-73500-patients-data-affected-in-ransomware-attack-on-eye-clinic-in-spore>
7. <https://www.zdnet.com/article/bangkok-airways-apologizes-for-passport-info-breach-as-lockbit-ransomware-group-threatens-release-of-more-data/>
8. <https://news.abplive.com/tamil-nadu/tamil-nadu-public-department-attacked-by-ransomware-suspect-demands-1-950-usd-in-cryptocurrency-1482904>
9. <https://www.thestar.com.my/tech/tech-news/2021/09/20/web-hosting-service-exabytes-hit-by-ransomware-attack-still-restoring-services>
10. <https://cnnphilippines.com/business/2021/11/24/NPC-SnR-breach-report-submission.html>
11. <https://www.zdnet.com/article/queensland-government-energy-generator-hit-by-ransomware/>

**References provided above are for page 7 as shown in the report.*

CONTACT DETAILS



About Greyint

Grey Intelligence (GreyInt) is a Singapore-based cyber threat intelligence company founded in 2016 and officially established in 2019. Our mission is to provide clients an enhanced visibility into the cyber threat activities in Asia-Pacific with a deeper focus on Southeast Asia. We provide actionable intel through threat alerts derived from open source intelligence (OSINT), deep and dark web intelligence (DDWINT), social media intelligence (SOCMINT) and cyber human intelligence (Cyber-HUMINT). We pride ourselves as a company with enhanced bird's eye view into the underground hacking communities, especially in Southeast Asia. Having experienced threat intelligence analysts and researchers based in Singapore, as well as neighboring countries throughout the region, helped us in achieving our mission in the past three years, and led to the creation of this report.

EMAIL : contact@greyint.com

TELEGRAM : [@greyint](https://www.instagram.com/greyint)

WEBSITE : greyint.com

LINKEDIN : <https://www.linkedin.com/company/greyint>

DISCLAIMER:

The "Ransomware Threat Landscape Report for Asia Pacific – 2022" publication reviews the ransomware events in Asia Pacific for 2021. The enclosed facts, statistics and analyses are based on information available at the time of publication. The contents of this publication are provided on an "as is" basis without warranties of any kind. To the fullest extent permitted by law, GreyInt does not warrant and hereby disclaims any warranty as to the accuracy, correctness, reliability, timeliness, noninfringement, title, merchantability or fitness for any particular purpose of the contents of this publication. GreyInt shall also not be liable for any damage or loss of any kind caused as a result (direct or indirect) of the use of the publication, including but not limited to any damage or loss suffered as a result of reliance on the contents contained in the publication. GreyInt also reserves the right to refine its analyses as the threat situation evolves, and/or as further information is made available.