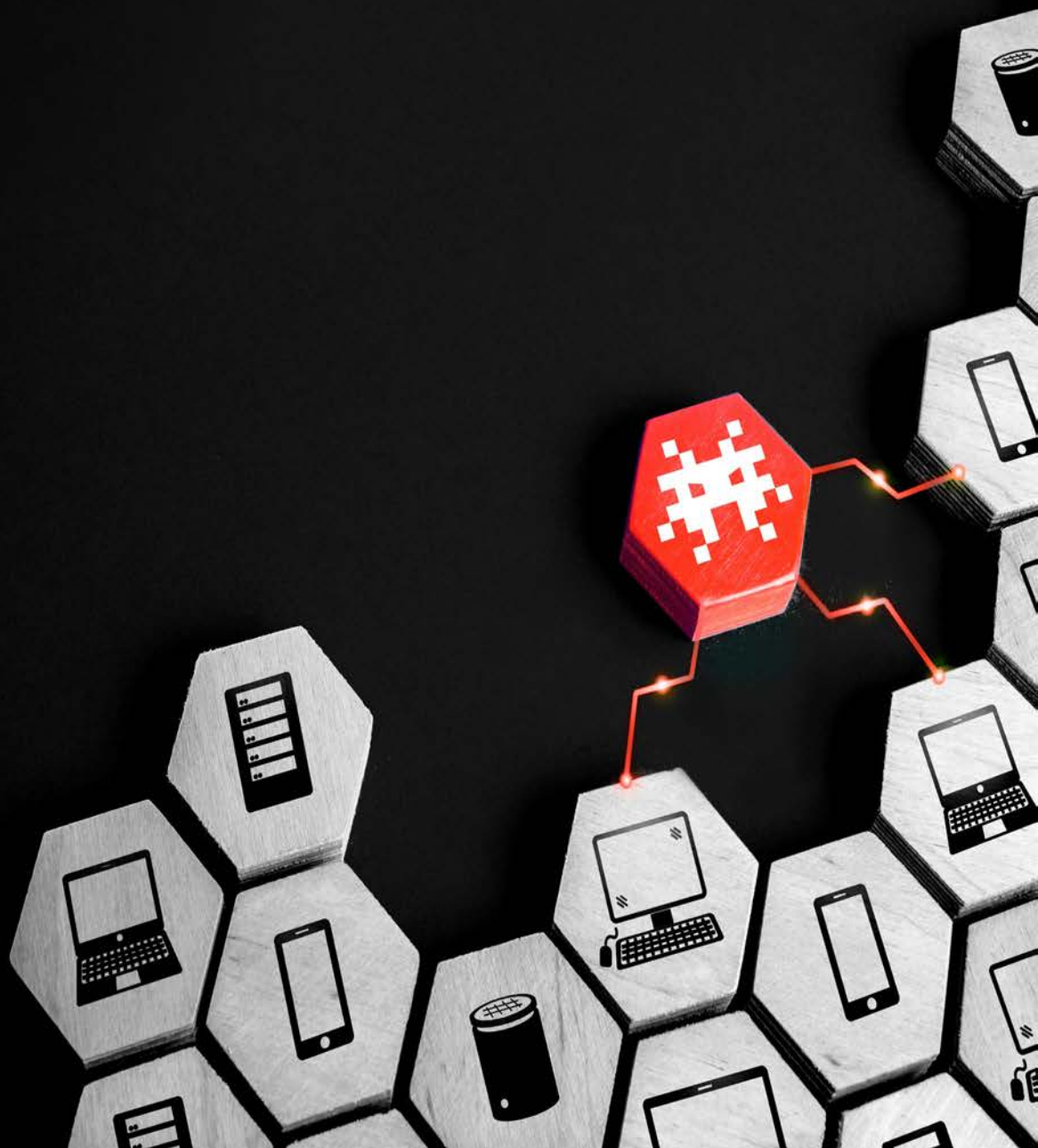
CYBER THREAT LANDSCAPE REPORT 2021

A SPOTLIGHT ON SOUTHEAST ASIA FROM 2019 TO 2020



GreyInt

GreyInt

GREYINT CYBER THREAT LANDSCAPE REPORT 2021

TABLE OF CONTENT


Providing
" Providing clients an enhanced visibility into the cyber threat activities in Asia-Pacific with a deeper focus on Southeast Asia. "

FOREWORD

We are happy to issue GreyInt's first Cyber Threat Landscape report, titled *Cyber Threat Landscape 2021 – Spotlight on Southeast Asia*, which aims to provide situational awareness of the cyber incidents, events and activities surrounding the region from 2019 to 2020. This report highlights significant threats, sectors targeted, hacking groups observed in Southeast Asia (SEA), and advanced persistent threat actors with possible interest in the region.

As a brief background, Grey Intelligence (GreyInt) is a Singapore-based cyber threat intelligence company 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 two years, and led to the creation of this report.

To this day, the region continues to be active in the cyber realm. Majority of the activities highlighted in this report were derived from direct observation, monitoring and research into the underground hacking and cybercriminal communities located in the surface, deep, and dark web, as well as information received from peers in various industries. This report details activities observed by three main groups of threat actors, mainly **hacktivists**, **cybercriminals**, and **advanced persistent threat actors (APTs)**.

HACKTIVISTS

CYBERCRIMINALS

APTs

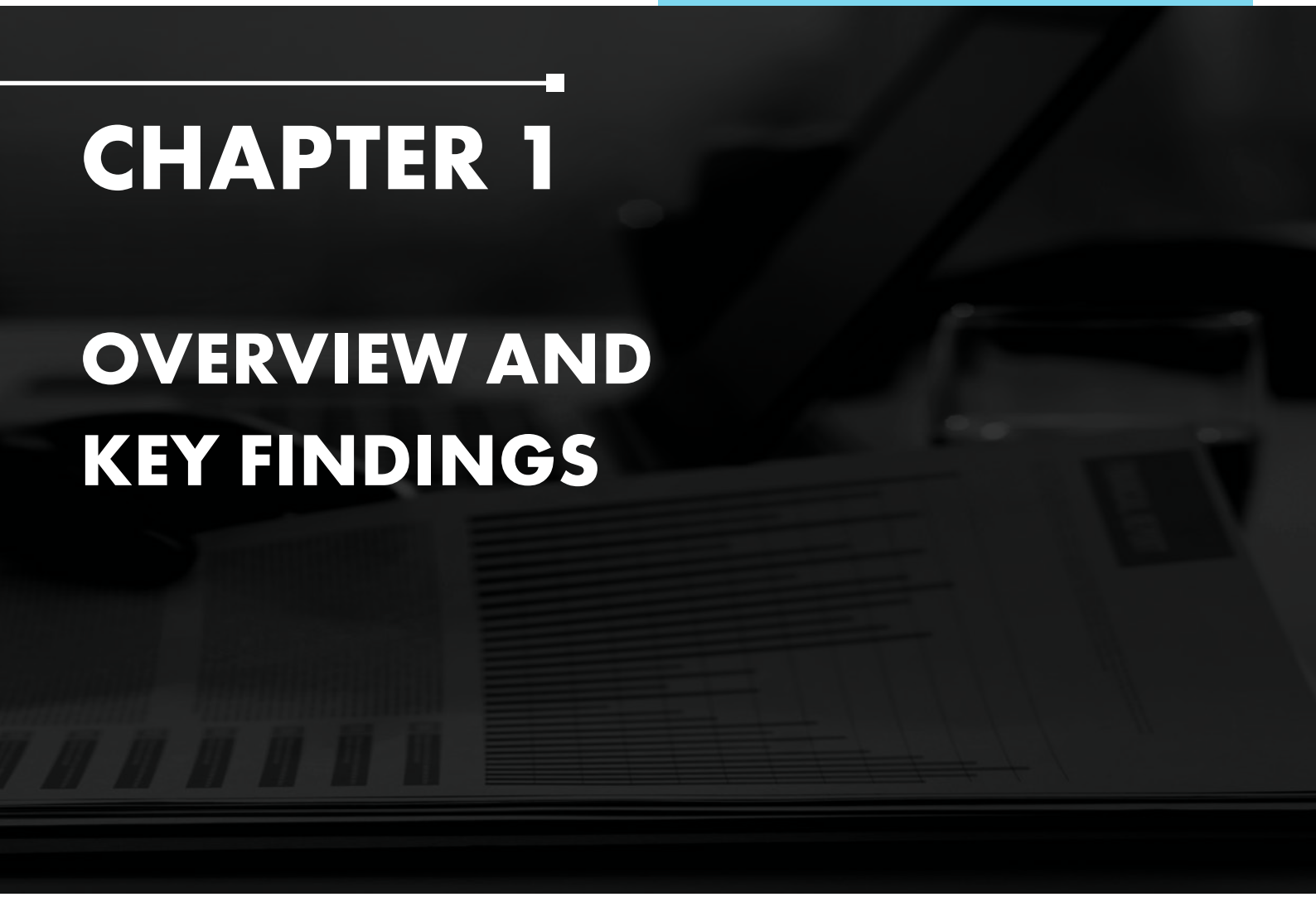
We observed that political issues remain the basis for a majority of hacktivist activities. Issues, such as the enactment of a contentious law in Indonesia, or illegal trespass of maritime boundaries, became the cornerstone for hacktivists to conduct cyberattacks to voice their unhappiness and discontentment to the rest of the world. These would likely continue in the coming year, as hacktivists often find ways to ensure they are heard.

Financially motivated cybercriminals continue to thrive in the deep and dark web forums, as they find multiple avenues to ensure continuity in their monetisation tactics. While global cybercriminals evolve their methodology and modus operandi, especially in the wake of the pandemic in 2020, we did not observe similar developments within the Southeast Asia region. Nevertheless, this group of threat actors continue to pose a threat to organisations within the region.

APT threat actors, mainly from East Asia, have taken an interest in the region in the last few years. Strategic issues, such as the Belt Road Initiative (BRI), were part of the motivation in some of the attacks observed and reported publicly. Being one of the fastest growing regions globally, it is not surprising that APT actors that act in interest of the state would be interested to steal and spy on the developments in various countries within the region.

Despite being a relatively young organisation, we are grateful and proud to produce actionable intelligence and alerts to our customers. As part of our outreach efforts, we actively engage various countries' computer emergency response teams (CERTs) to share and alert them on threats that may impact the country. As we move forward, we continue to improve our processes to ensure that valuable and actionable intel would be delivered to our customers as timely as possible. We hope that you would have a lovely read ahead of you.

HAPPY READING!

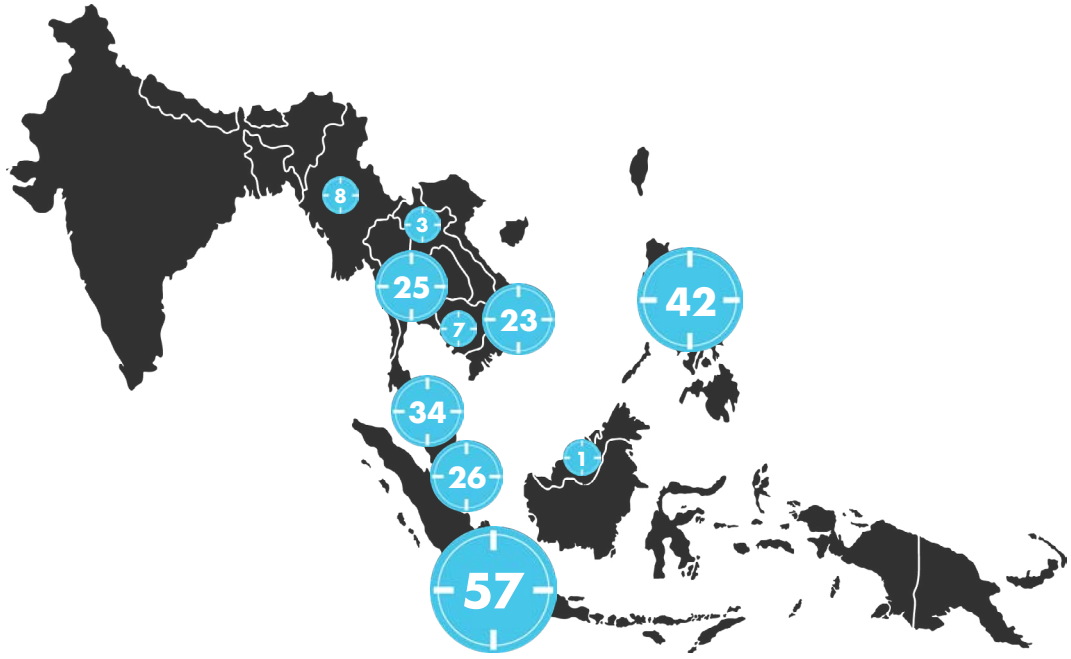


CHAPTER 1

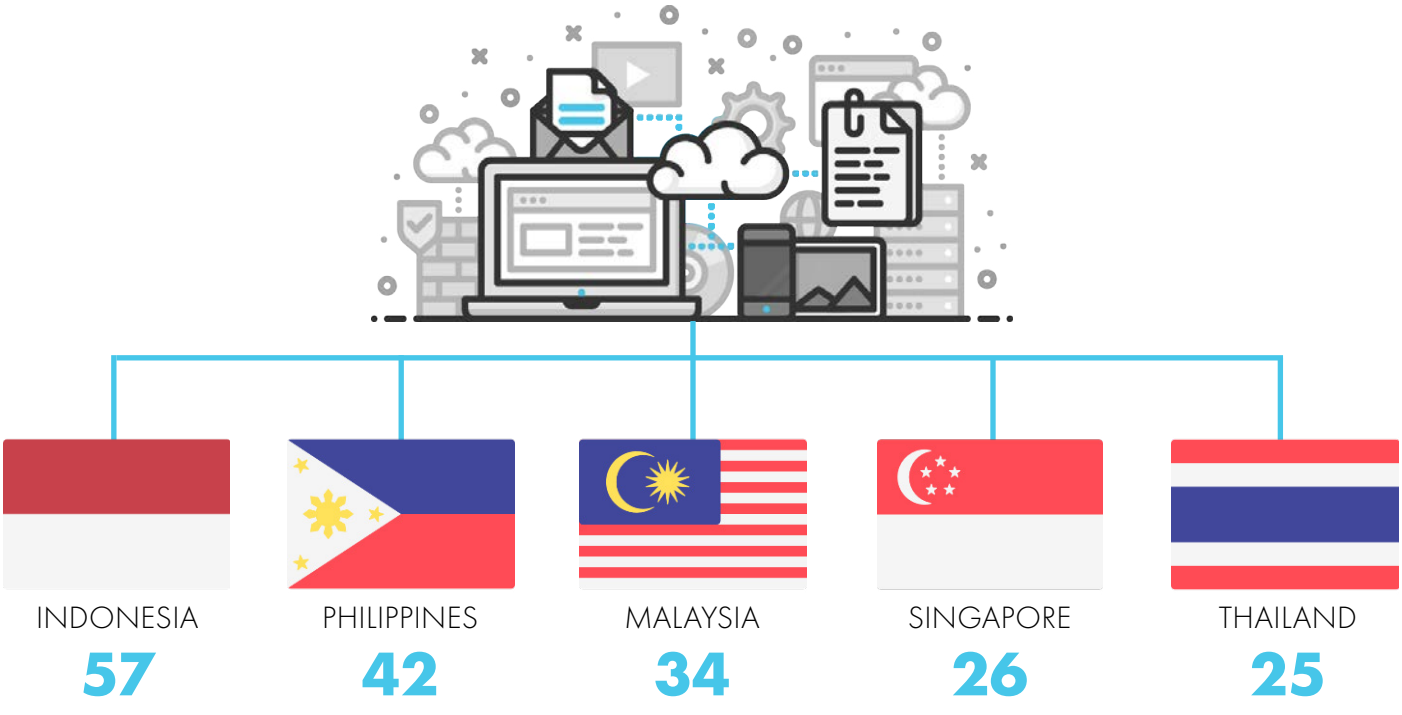
OVERVIEW AND KEY FINDINGS

OVERVIEW AND KEY FINDINGS

In the last two years, GreyInt published more than 500 tactical intelligence reports concerning incidents and malicious activities observed in Asia Pacific. Almost one in two tactical reports published concerned cyber activities observed in Southeast Asia (SEA).

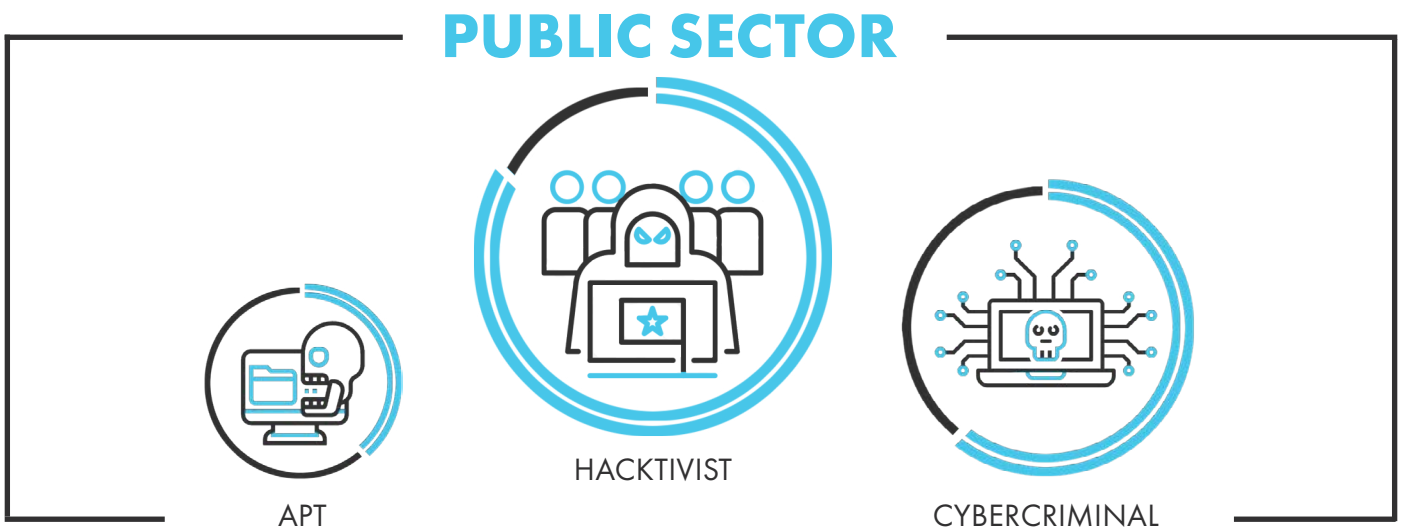


The five countries highlighted here had some of the highest cyber threat activities that GreyInt observed from 2019 to 2020. Every activity observed was alerted in the form of a contextualized tactical report. It is important to note that the numbers and ranking here are not indicative of the country's current state of cybersecurity.
More details on significant activities observed in each country are highlighted in Chapter 3.



TOP 3 SECTORS IMPACTED

Over the last two years, GreyInt observed various sectors being targeted by three main threat actor groups, which consisted of hacktivists, cybercriminals, and advanced persistent threat (APT) actors. Among them, three sectors stood out as being the most impacted, mainly the public, education, and financial sectors. These sectors made up more than 75 per cent of all the sectors combined.

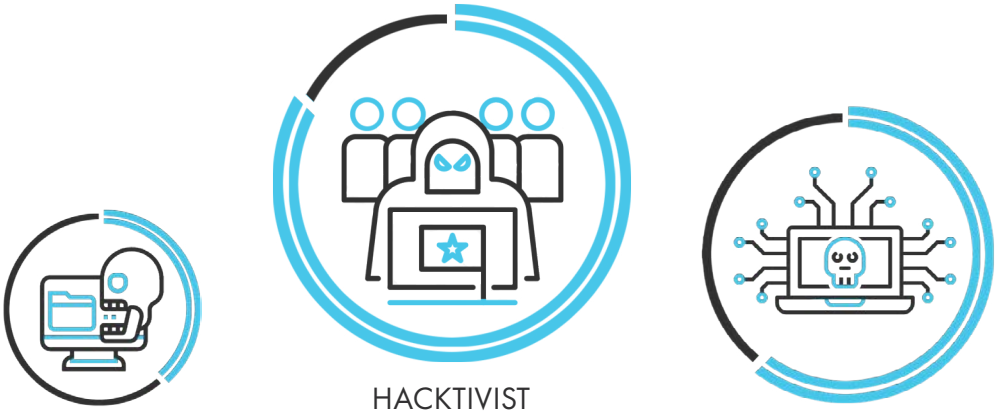


The public sector in SEA was observed to be the most targeted sector, accounting for more than 40 per cent of the activities observed. Majority of the attacks were observed to be conducted by hacktivists. Government websites, particularly from Indonesia, Malaysia, and the Philippines, were compromised with web defacement attacks and data leaks. The hacktivist operations were mostly driven by political issues and disagreement towards government policies.

Second to the hacktivists were financially motivated cybercriminals. Attacks ranged from infecting government websites with ransomware, advertising compromised government networks to selling personally identifiable information (PIIs) belonging to government employees via underground forums. Government websites across SEA were also targeted by cybercriminals such as Emotet to host malicious documents and payloads.

APT actors were mostly observed demonstrating interests in government organisations based in Vietnam, Cambodia and Malaysia. The documents used as lures or decoys suggest interest in specific agencies likely aimed to gather strategic intelligence.

EDUCATION SECTOR

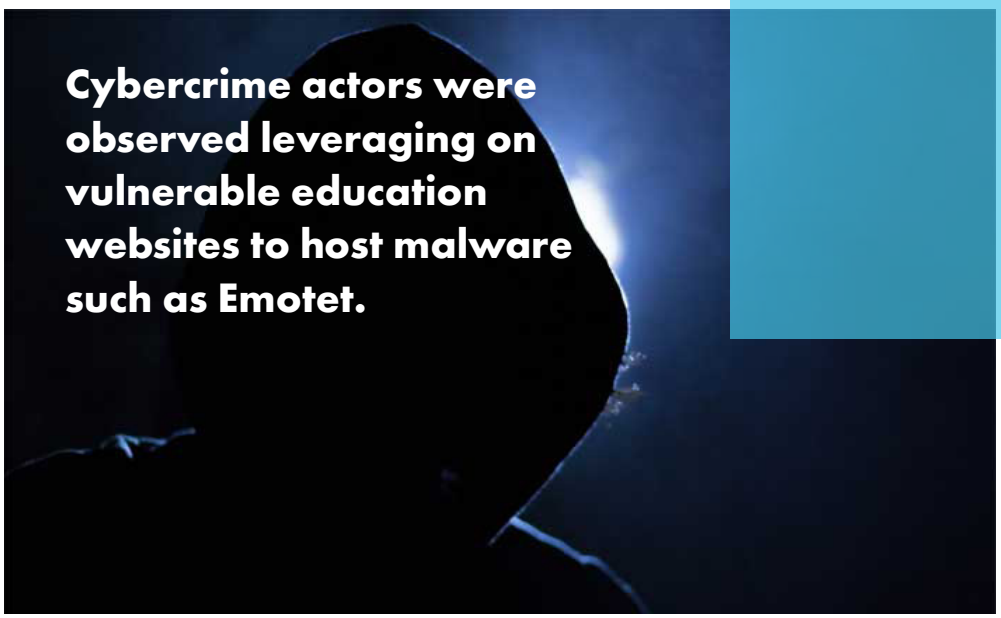


The education sector was observed to be the second most targeted sector in SEA, amounting to about 20 per cent of the attacks observed. Similar to the public sector, hacktivists were observed to be the top threat actor to schools and universities.

Websites associated with the education sector such as colleges and universities were specifically targeted by hacktivists in SEA though with different motivations. Hacktivists from Indonesia were found targeting Malaysian universities driven by political or territorial issues. Hacktivists from the Philippines and Indonesia targeted their local education institutions to expose vulnerabilities with the intent to provide security awareness and enhance their underground presence and credibility. However, the method used could potentially affect the confidentiality of the institutions' data, and be constituted as a crime.

Cybercrime actors were observed leveraging on vulnerable education websites to host malware such as Emotet. In addition, threat actors exfiltrated data associated with students and teachers, with the intention to either expose, or sell in criminal markets and forums. Actors in this category were also discovered selling access to compromised education institutions' websites.

The education sector was least affected by APT actors. In late-2020, a Middle East-based group targeted education institutions worldwide including a Singapore university to steal credentials.



FINANCIAL SECTOR

The financial sector completes the top three targeted sectors in SEA, with financially motivated cybercriminals being the primary actor targeting this sector.

Cybercrime actors conducted DDoS-for-ransom threats against multiple financial institutions in SEA. Actors were also observed selling databases allegedly stolen from banks through their compromised websites. These databases were put up for sale in underground criminal forums and markets. Webshell access and credentials belonging to banks based in Indonesia were also offered for sale.

As part of their campaigns, hacktivists would include prominent banks as part of their target lists. In a hacking operation organised by Indonesian hacktivists in 2019, a Malaysian bank was listed as a DDoS target. Fortunately, the bank's security infrastructure was able to fend off the attack. Hacktivists based in the Philippines were also observed targeting local organisations providing financial services. In one instance, a hacktivist group claimed to have compromised a loan and savings services company. The group posted screenshots of its access and documents obtained from the company as proof of access in its social media accounts.

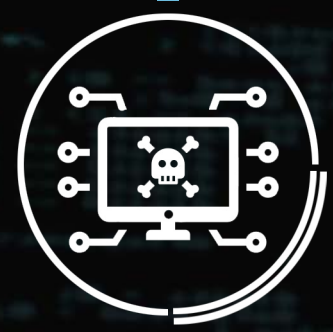
While not observed directly, APT groups have conducted campaigns against financial institutions in the region. In 2019, a Russian-speaking APT group, known as Silence APT, conducted reconnaissance campaigns aimed at banks located in various countries, including Malaysia and Singapore. In the last two years, GreyInt observed documents leveraging lures containing references or themes associated with financial institutions, which suggested possible interest in the sector. However, it was unclear if financial institutions were the target of these documents.

TOP 3 THREATS OBSERVED

DATA LEAK ATTACK

A data leak is the intentional release of private and confidential data by threat actors to the public internet. Hacktivists utilised this tactic to expose the confidentiality of targeted organisations either for a political cause or to embarrass them for their lack of security. Cybercriminals also use this tactic for financial purposes, such as leaking a portion of stolen data in criminal forums or websites as samples for interested buyers, or to threaten victims into paying a ransom or risk having all of its data leaked.

GreyInt identified confidential and private data, such as PIIs, financial, government, military, and sensitive company information from organisations in SEA, leaked by threat actors.



MALWARE/RANSOMWARE

A malware is a program designed to cause damage to a computer system. Depending on the motivation of the developers, these malware could be designed to steal, corrupt or encrypt information in the infected system. Malware is typically delivered to a user via phishing emails or from clicking on malicious links when browsing suspicious or infected websites. However, the rise of ransomware, particularly ransomware operators that were involved in Big Game Hunting (BGH), changed the way malware is being delivered to a system. By penetrating into company networks and manually searching for valuable assets within the network to install ransomware, this technique did not require much user interaction.

In addition to malware campaigns delivered via phishing emails, GreyInt observed multiple SEA organisations targeted with ransomware operators involved in the BGH business.

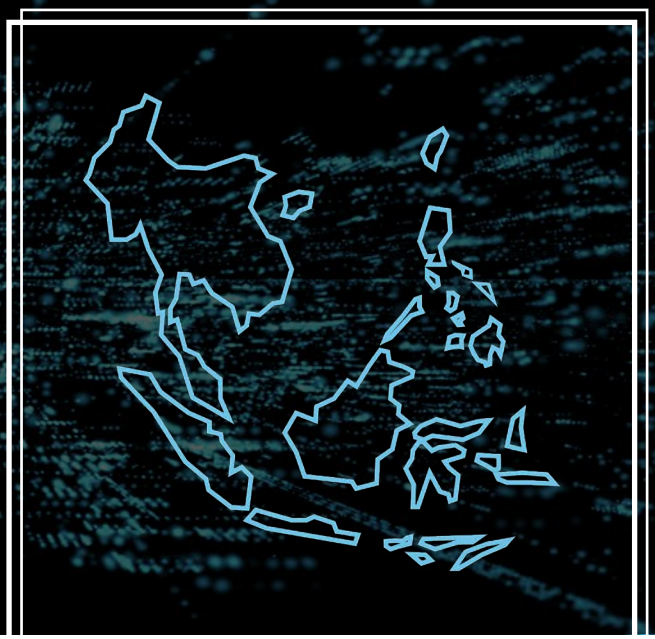
WEBSITE COMPROMISE/UNAUTHORIZED ACCESS

An attacker could gain access to a website's contents, or the web server through an exploitation of a vulnerability. Affected information could include credentials, user information, and databases, which could contain sensitive data.

GreyInt observed SEA-based hacktivists utilising this tactic to deface a website's content, delete, or download databases to leak to the public. Cybercriminals were also observed offering access to compromised websites, including those from the public sector, and advertising them on criminal forums.

ACTIVE HACKTIVIST GROUPS IN SOUTHEAST ASIA

Throughout the year 2019 and 2020, GreyInt monitored hacking operations conducted by multiple groups based in SEA. This section highlights some of the key hacking groups identified, and their associated activities and capabilities.



PHANTOM TROUPE

PHILIPPINES

Phantom Troupe is a hacking group consisting of members believed to be located in the Philippines. The group was first observed in early August 2020, and compromised multiple prominent websites mostly based in the Philippines. These websites included education institutions, governments, and military organisations. The group demonstrated capabilities such as exploiting web application vulnerabilities, injecting unauthorised content, and data exfiltration. Phantom Troupe has yet to display any activities that were either financially or politically motivated, despite being active in the Philippines underground hacking community.

1945VN

VIETNAM

1945VN is a hacking group consisting of members believed to be located in Vietnam, and has been operating since at least 2017. The group conducted primarily website defacement attacks, and denial of service attacks against a variety of targets including private sectors, government organisations, education, and financial institutions. The group was also recently observed exfiltrating databases and leaking them on social media. According to defacement messages left on compromised websites, the group has 14 members: ROX3T5, 0c34n, Shuu, JookerMoon, Snake2K1, j4pa0, binpc, Moewut, zFap, CP04042K, J4cki3, PassDDoS, lulzkid and LHL69.

TYPICAL IDIOT SECURITY

INDONESIA

Typical Idiot Security is an Indonesian hacking group which existed since at least June 2018. The group has been active in breaching websites both in-country and foreign, and has demonstrated capabilities in addition to defacing websites. In July and August 2019, the group hijacked multiple Google Togo subdomains and some major websites using the .SLK top level domain via DNS Hijacking technique. In January 2020, one of the hacking group's founders was arrested by local authorities after breaching into the Jakarta State Court's website. It was reported that Typical Idiot Security has compromised over 3800 websites and were also involved in carding related activities. GreyInt did not observe any activity on the group's social media accounts since January 2020 suggesting a halt on their hacking activities after the arrest.

MALAYSIAGOV

MALAYSIA

MalaysiaGov is believed to be a Malaysia-based hacking group and has been active in compromising websites since at least 2016. The group has compromised over 700 websites of both Malaysian and foreign including governments, education institutions and private organizations in various sectors. Though the group does not engage in financially-motivated hacking, one of its members has been discovered operating a Telegram channel where activities such as spamming, carding and databases obtained from hacking were advertised.

UNION OF UNDERGROUND MYANMAR HACKERS (UGMH)

MYANMAR

The Union of UnderGround Myanmar Hackers (UGMH) is a representative of hackers and hacking groups based out of Myanmar and has been active since 2015. The UGMH has also conducted politically-motivated hacktivist operations against Bangladesh (#Op_Bangli) and Thailand (#OpThai) targeting both public and private sector websites with defacement and data leak attacks. In March 2019, members of the hacking group demonstrated their capability by gaining access into a South Asia-based military organization website and posted screenshots of their access to it social media accounts. In September 2020, a ransomware binary masquerading as a PDF document was discovered. This ransomware was submitted to a public malware repository from a Thai-owned IP address. An indicator identified during analysis suggested the ransomware was likely developed by members of UGMH.

ACTIVE APT GROUPS WITH INTERESTS IN SOUTHEAST ASIA

Throughout the year 2019 and 2020, GreyInt identified indicators associated with APT groups reportedly linked to nation states. These indicators were observed leveraging themes, contents, decoys, domains, and infrastructures containing references to entities in SEA. It is important to note that these indicators are not evident of APTs directly targeting SEA entities. However, the use of SEA-reference signified potential interest in organisations operating within the region.

MUSTANG PANDA *AKA BRONZE PRESIDENT, TEMP HEX, HONEYMYTE*

EAST ASIA

POSSIBLE INTEREST: MYANMAR, VIETNAM

Mustang Panda is an East Asia-based cyber espionage group that has been active since 2014. The group targeted multiple countries, including those in Asia Pacific, to gather intelligence. Tools and malware used by Mustang Panda included Cobalt Strike, PlugX and Poison Ivy. Throughout 2019 and 2020, GreyInt identified malicious documents used as lures and decoys using references and themes associated with public sectors in Myanmar and Vietnam suggesting interest in the two countries.

OCEAN LOTUS *AKA APT32, APT-C-00, OCEAN BUFFALO, SECTORF01*

SOUTHEAST ASIA

POSSIBLE INTEREST: CAMBODIA

Ocean Lotus is a SEA-based cyber espionage group that has been reportedly active since at least 2014. The group was known to target multiple countries in SEA with interests in various sectors, including government, telecommunications, defense, financial and manufacturing, amongst others. Tools used by Ocean Lotus included Cobalt Strike, Mimikatz, Quasar RAT and KerrDown. Throughout 2019 and 2020, GreyInt identified multiple documents using themes associated with entities from both public and private sectors in Cambodia, suggesting a deep interest in the country.

SIDEWINDER *AKA RATTLESNAKE, T-APT-04, APT-C-17*

SOUTH ASIA

POSSIBLE INTEREST: MYANMAR

SideWinder is a South Asia-based cyber espionage group that has been reportedly active since at least 2012. The group was observed targeting military and government organisations based in Pakistan and China. Some of the key techniques used by SideWinder included the exploitation of an Equation Editor vulnerability (CVE-2017-11882), the use of DLL Sideloading attack, and the registration of domains mimicking targeted organisations. In November 2020, GreyInt identified a domain attempting to impersonate a Myanmar embassy based in China and Singapore. The attempt to impersonate a domain associated with the embassy suggested potential interest in entities within Myanmar government.

SILENT LIBRARIAN *AKA COBALT DICKENS, TA407*

MIDDLE EAST

POSSIBLE INTEREST: SINGAPORE

Silent Librarian is a Middle East-based cyber espionage group that was widely reported to target education institutions worldwide, including universities in Israel, US, UK, Australia, China and Japan. According to the US Treasury Department, the group exfiltrated over 31TB of data associated with academic research and projects. Silent Librarian heavily used spear phishing technique and cloned universities' web portals, in an attempt to lure users into providing credentials. In October 2020, GreyInt identified two phishing websites and domains impersonating a Singapore-based university with an intent to steal username and password.

KIMSUKY *AKA VELVET CHOLLIMA, THALLIUM, BLACK BANSHEE*

EAST ASIA

POSSIBLE INTEREST: MALAYSIA

Kimsuky is an East Asia-based cyber espionage group that has been reportedly active since at least 2013. The group was observed conducting campaigns against entities in the education, energy and government sectors in South Korea. Public reports indicated Kimsuky's use of tools such as Mimikatz, Gh0st RAT and BabyShark malware. In October 2020, GreyInt identified a decoy PDF document used in a campaign by the group. The contents of the PDF document referenced a financial company and a bank based in Malaysia, suggesting potential interests in financial institutions based in Malaysia.

VICIOUS PANDA

EAST ASIA

POSSIBLE INTEREST: MALAYSIA

Vicious Panda is an East Asia-based cyber espionage group that was first seen by security firms in 2015. The group targeted government organisations in Belarus, Mongolia, Russia and Ukraine. Vicious Panda utilised tools such as the Royal Road RTF Weaponizer and Byeby RAT, and exploited Microsoft Office vulnerabilities such as CVE-2012-0158, CVE-2014-1761, CVE-2017-11882 or CVE-2018-0802. In April 2020, GreyInt identified two weaponized RTF documents with contents referencing government entities in Malaysia, including the use of the Malay language. The two documents were observed using a command and control domain attributed to Vicious Panda in past campaigns.

CHAPTER 2

TRENDS OBSERVED

SOCIAL MEDIA

THE PLATFORM USED BY SOUTHEAST ASIA-BASED ACTORS

Unlike many threat actors outside of Asia Pacific, GreyInt observed an increasing amount of reliance on social media platforms, particularly Facebook, leveraged by threat actors in South Asia and Southeast Asia (SEA) to facilitate cybercrime, or organize hacktivist-related operations.

Throughout 2019 and 2020, GreyInt observed significant activities in which Facebook was leveraged as the preferred platform for SEA-based actors to advertise hacked materials such as illegally obtained databases, credentials, financial data, and the sale of unauthorised access to networks or websites exploited. Hacktivist campaigns, such as Operation Thailand and Operation GayangMalaysia, were organised through Facebook pages and groups, though actors based out of Indonesia were also observed organizing hacktivist operations using Instagram and Telegram.

Furthermore, the use of Facebook by SEA-based actors far outweighed the use of forums and markets located over the TOR network (dark web). Till date, GreyInt observed minimal reliance on the dark web by SEA-based actors. For most, criminal forums in the deep web were utilised to advertise hacked proceeds for financial profit. One example would be an Indonesia-based actor who developed ransomware and used private Facebook groups to advertise its tools. This actor would demonstrate the ransomware's capability by targeting prominent government websites, infect them, and share screenshots of its success as evidence to these private Facebook groups. In addition to using Facebook, the actor was also active in deep web criminal forums, where he advertised his ransomware tools.

GreyInt assessed that the use of social media, particularly Facebook, would continue to be a key platform for SEA-based actors to conduct, organize or facilitate cybercriminal and hacktivist operations.

EMOTET: A ONCE PERSISTENT THREAT TO SOUTHEAST ASIA

Throughout 2019 to the end of 2020, GreyInt observed continuous compromise of prominent websites in both public and private sectors based in SEA. These websites were compromised by Emotet operators to host malicious binaries, such as Emotet's payloads and malicious documents. Some of the websites were observed being leveraged for payload retrieval, which would be downloaded when malicious documents received by a victim via phishing email were opened.

Emotet is a malware first reported by security firms in 2014. The malware evolved from what was once a banking trojan, to a distributor of other malware including ransomware. In 2019, Emotet was observed deploying the information stealer, TrickBot, and subsequently, Ryuk ransomware. This combination was dubbed the 'Triple Threat' and infected many organisations worldwide, encrypting important files and demanding millions of dollars in exchange for the decryption keys.

Towards the end of 2020, malicious Emotet emails were observed delivered to multiple companies across SEA. This included companies in Myanmar, Thailand and Singapore. An email was also found delivered to a government agency based in East Asia.

Research into the compromised websites revealed that the majority of the websites were running on outdated and unpatched versions of WordPress. This allowed Emotet operators to automate its 'search, exploit and upload' attack leveraging on known web application vulnerabilities associated with WordPress.

On 27 January 2021, Europol released a public statement that the organisation, together with authorities from the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada and Ukraine, managed to disrupt Emotet's operations by taking down its massive network of botnets. This takedown would likely see a drastic fall in Emotet infections in the coming months. It is important to note that a similar operation was conducted by Europol against the Andromeda botnet back in 2017. However, the malware was still observed infecting systems in 2020. According to the Center for Internet Security, Andromeda was still seen as the top 10 malware in 2019.

As the takedown was conducted against Emotet's infrastructure and there were no reports of its operators and developers being arrested during the operation as opposed to the eventual arrest of the mastermind behind Andromeda in 2017, GreyInt assessed that Emotet could make a comeback with better operational security and capabilities in the near future.

TIMELINE OF EMOTET ACTIVITIES IMPACTING SEA FROM 2019 - 2020

2019

MARCH 19

Public sector websites from Indonesia, Thailand and the Philippines compromised to host Emotet binaries.

APRIL 19

Public sector websites from Indonesia and Kenya compromised to host Emotet binaries.

2020

DECEMBER 19 - JANUARY 20

Public sector websites from Indonesia, Thailand and the Philippines compromised to host Emotet binaries.

JULY 20

Public and private sector websites from Indonesia, Vietnam, Thailand and Mongolia compromised to host Emotet binaries.

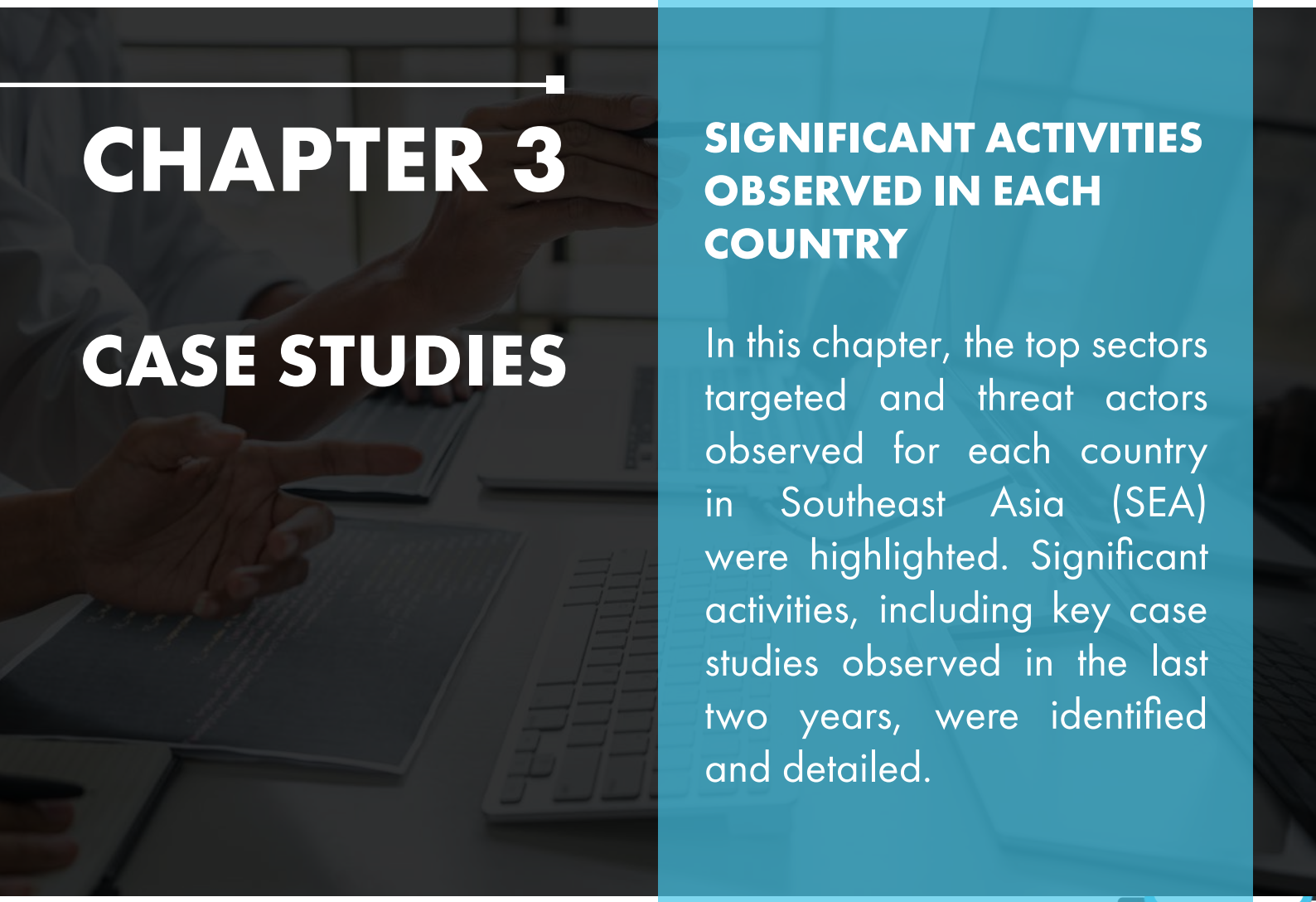
AUGUST 20

Public sector websites from Indonesia, Pakistan, Malaysia and Maldives compromised to host Emotet binaries.

OCTOBER 20

Emotet phishing emails sent to medical device manufacturing company in Thailand and a government agency based in East Asia identified.

2021



CHAPTER 3

CASE STUDIES

SIGNIFICANT ACTIVITIES OBSERVED IN EACH COUNTRY

In this chapter, the top sectors targeted and threat actors observed for each country in Southeast Asia (SEA) were highlighted. Significant activities, including key case studies observed in the last two years, were identified and detailed.

SINGAPORE

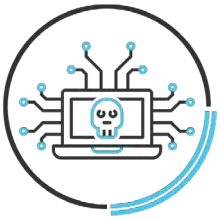
TOP 3 TARGETED SECTORS

CONSTRUCTION

LOGISTICS

EDUCATION

TOP ACTOR OBSERVED



CYBERCRIMINAL

2019

APRIL 19

- IP address belonging to a Singaporean company targeted by hacktivists based in Southeast Asia.

2020

FEBRUARY 20

- An education institution targeted by Covid-19-themed phishing email observed delivering HawkEye malware.

JUNE 20

- Singapore General Election-themed document identified delivering Raccoon info-stealing malware.
- Domain masquerading as a healthcare organization discovered hosting ransomware samples.

AUGUST 20

- Singapore-based pharmaceutical company received extortion threats from cybercriminals.

SEPTEMBER 20

- Email addresses and passwords associated with users in the education and government sector advertised in cybercriminal forum.
- Phishing emails posing as Singapore-based postal company observed targeting Singaporeans to steal financial data.
- Databases containing PIIs belonging to companies based in Singapore advertised in cybercriminal forum.

OCTOBER - DECEMBER 20

- Universities targeted by Middle East APT group aimed to steal credentials.

2021

SINGAPORE SELECTED CASE STUDIES

APRIL 2019

IP address belonging to a Singaporean company targeted by hacktivist groups based in Indonesia.

Threat actor classification: ***Hacktivist***

IIn April 2019, GreyInt identified hackers based in SEA sharing images calling for an attack against specific IP addresses, one of which belonged to a Singaporean logistic company. According to a Facebook post written in the Indonesian language, an individual accused Singapore and Vietnam of conducting denial of service attack on Indonesia's election commission (KPU) website during the 2019 Indonesian general election. One of the images that invited hackers to target Singapore and Vietnam was shared by over 11,000 users. Another image was also shared on Instagram calling for hackers to conduct a synchronized attack against the IP addresses over a four-day period.

JULY 2020

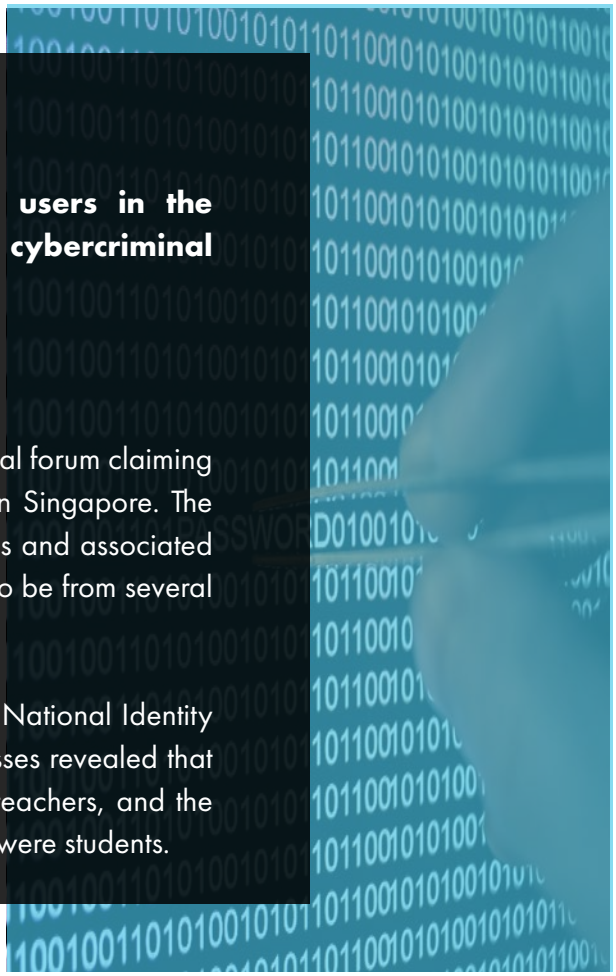
Singapore General Election-themed document identified delivering Raccoon info-stealing malware.

Threat actor classification: ***Cybercriminal***

In July 2020, GreyInt identified a malicious document named "Election Results.xlsm" in a malware repository. The content of the spreadsheet contained an image of members from a Singapore's political party with the title "The PAP WON ONCE AGAIN", likely referencing the general election that happened in the same month. The document was observed delivering an information-stealing malware known as Raccoon.

According to public reports, Raccoon emerged as Malware as a Service (MaaS) in April 2019. The malware is capable of stealing login credentials, credit card information, cryptocurrency wallets, and browser information.

SINGAPORE SELECTED CASE STUDIES



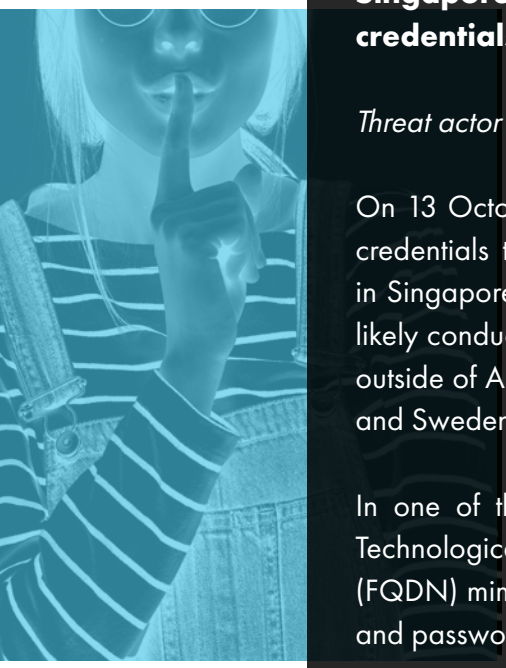
SEPTEMBER 2020

Email addresses and passwords associated with users in the education and government sector advertised in cybercriminal forum.

Threat actor classification: ***Cybercriminal***

In September 2020, GreyInt discovered a post in a cybercriminal forum claiming to possess a database belonging to an education institution in Singapore. The post claimed to have at least 18,000 rows of e-mail addresses and associated passwords. One in 20 of the e-mail addresses were identified to be from several government and educational institutions.

Some of the email addresses were found using the Singapore National Identity number as their passwords. Our research into the email addresses revealed that the majority of the users from the domain moe.edu[.]sg were teachers, and the majority of the users from the domain [school domain].edu[.]sg were students.



OCTOBER 2020

Singapore Universities targeted by Silent Librarian aimed to steal credentials.

Threat actor classification: ***APT***

On 13 October 2020, GreyInt identified a phishing campaign aimed at stealing login credentials targeted at multiple education institutions worldwide including universities in Singapore, Hong Kong, Australia and China. The credential phishing campaign was likely conducted by a threat actor known as Silent Librarian. Other education institutions outside of Asia Pacific targeted were from the US, UK, Canada, Germany, Netherlands and Sweden.

In one of the phishing URLs identified, the website was found using the Nanyang Technological University logo. The website was hosted on a fully qualified domain name (FQDN) mimicking the Singapore-based university, and attempted to obtain usernames and passwords.

MALAYSIA

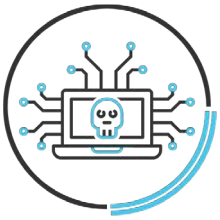
TOP 3 TARGETED SECTORS

PUBLIC SECTOR

EDUCATION

FINANCIAL

TOP ACTORS OBSERVED



CYBERCRIMINAL

HACKTIVIST

2019

APRIL 19

- Hacktivist operation targeting Malaysia organized after Belawan waters incident.

AUGUST 19

- *Malaysian websites including public sector's targeted by hacktivists in Operation Malingsial.*

OCTOBER 19

- Postal delivery service company in Malaysia likely hit by GlobeImposter ransomware.

2020

MARCH 20

- Financial institutions including a Malaysian investment bank targeted by hacking group 1945VN.

APRIL 20

- Weaponized documents linked to Vicious Panda likely used against entities in Malaysia.

JULY 20

- Hacker based in Venezuela selling access to a compromised Malaysian public sector website.

AUGUST 20

- Military documents associated with Royal Malaysia Navy leaked on dark web.
- Public sector websites observed hosting Emotet's payloads.

SEPTEMBER - OCTOBER 20

- Malaysian companies Hit by Egregor, Ragnarok and Netwalker ransomware.

2021

MALAYSIA SELECTED CASE STUDIES

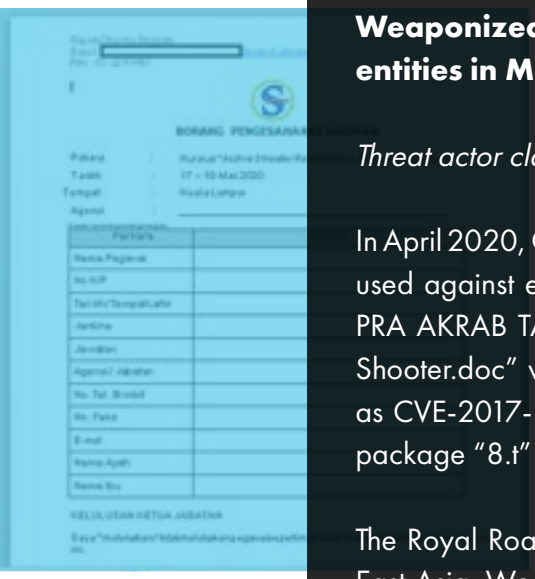
APRIL 2019

Hacktivist operation targeting Malaysia organised after Belawan waters incident.

Threat actor classification: ***Hacktivist***

In mid-April 2019, GreyInt observed multiple Malaysian websites targeted by hacktivists in a campaign dubbed Operation Gayang Malaysia (#Op_GayangMalaysia). The operation began after news of a Malaysian patrol boat and helicopter were found trespassing Indonesian territory to intercept the impounding of Malaysian-flagged illegal fishing vessels on Belawan waters. An image organizing an attack against a Malaysian government website was also shared among the hacking groups.

Websites from sectors such as financial, government and media were amongst those targeted by hacktivists. Some of the attacked websites were defaced with political statements, protesting the trespass.



APRIL 2020

Weaponized documents linked to Vicious Panda likely used against entities in Malaysia.

Threat actor classification: ***APT***

In April 2020, GreyInt identified two malicious documents written in Malay language likely used against entities in Malaysia. The two documents "TENTATIF KURSUS PROGRAM PRA AKRAB TAHAP 1.doc" and "Borang Pengesahan Kehadiran Peserta NCIS Active Shooter.doc" were observed exploiting Equation Editor vulnerabilities (publicly tracked as CVE-2017-11882 and CVE-2018-0802) and dropped indicators, including the OLE package "8.t" - an indication of the use of the tool known as "Royal Road" weaponizer.

The Royal Road weaponizer tool was reportedly shared among threat actors based in East Asia. We also observed that the command and control (C2) domain contacted by the two documents was used in a campaign dubbed "Vicious Panda".

MALAYSIA SELECTED CASE STUDIES

SEPTEMBER - OCTOBER 2020

Malaysian companies hit by Egregor, Ragnarok and Netwalker ransomware.

Threat actor classification: ***Cybercriminal***

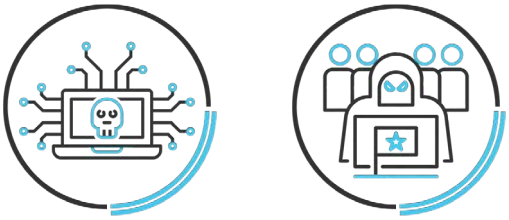
From September to October 2020, GreyInt discovered multiple Malaysian companies affected by ransomware, including Egregor, Ragnarok and Netwalker. These companies were from various sectors such as IT, technology, retail and manufacturing. Data samples from these companies were posted on the ransomware's blog site hosted in the dark web and those that did not pay the ransom had the entire stolen data leaked to the public. Some of the data leaked included confidential documents such as passport scans, client information, financial data and personally identifiable information (PII) such as full name, email address, contact number, physical address and national identity numbers.

PHILIPPINES

TOP 3 TARGETED SECTORS

PUBLIC SECTOR (MILITARY) | EDUCATION | FINANCIAL

TOP ACTORS OBSERVED



CYBERCRIMINAL | HACKTIVIST

2019

APRIL 19

- Databases allegedly from public sector, education institutions and military exposed by hacktivist.
- Hacker gains unauthorized access to a Philippine airline's web server.

MAY 19

- *Hacktivist identified organizing campaign to target Philippines' Commission on Elections (COMELEC) website.*

2020

JANUARY 20

- Philippine public sector websites breached by hackers from the Middle East to protest against the assassination of General Qassem Soleimani.
- 60GB database allegedly exfiltrated from a public sector website advertised for sale.

APRIL 20

- Hackers with ties to Communist Party initiated Operation Juliet and leaked over 15K personal information of Filipinos.

JULY 20

- Information system belonging to a Philippine provincial prison compromised by hackers and leaked screenshots of inmates data.
- Venezuelan hacker claimed to sell access to a Philippine public sector website.

AUGUST - SEPTEMBER 20

- New hacking group targeted education institutions and government websites.

OCTOBER 20

- Philippine company allegedly hit by Ragnarok ransomware.

2021

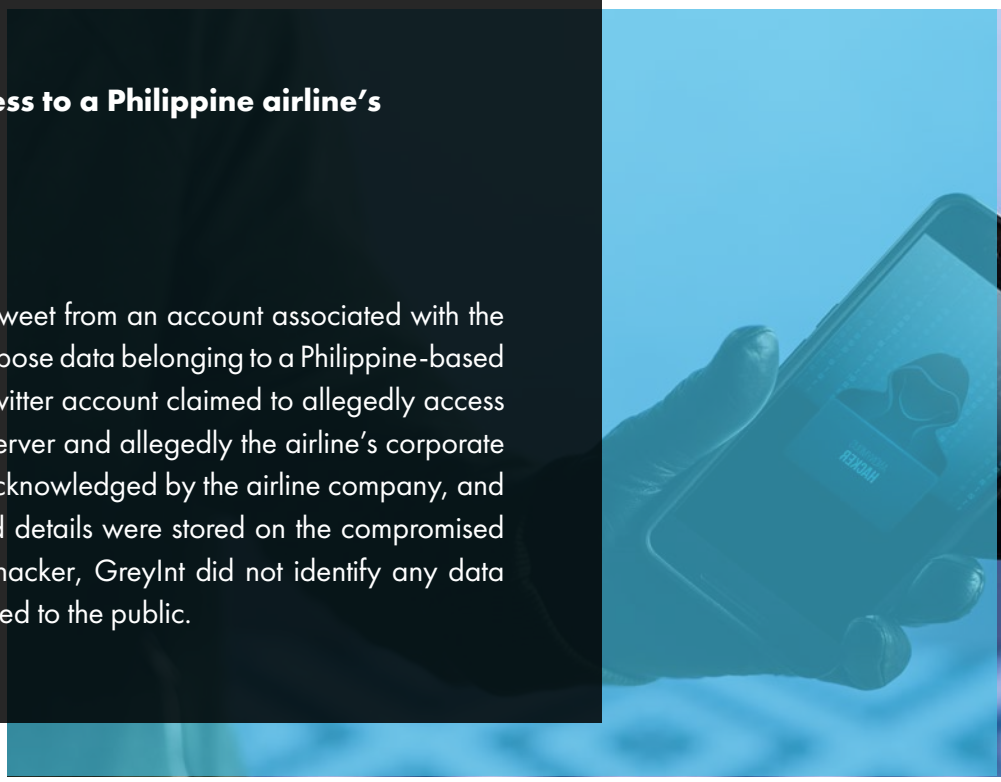
PHILIPPINES SELECTED CASE STUDIES

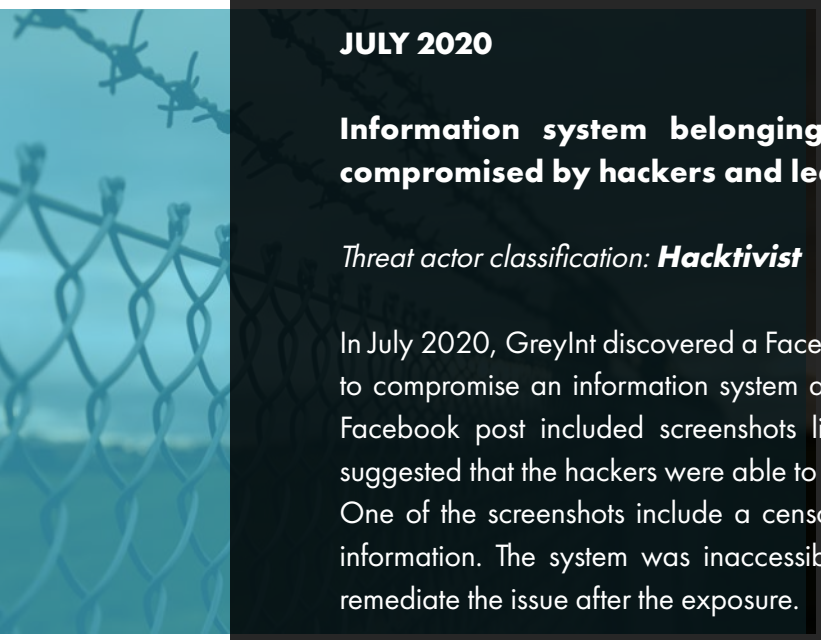
APRIL 2019

Hacker gained unauthorised access to a Philippine airline's web server.

Threat actor classification: ***Hacktivist***

In late-April 2019, GreyInt identified a tweet from an account associated with the hacking collective LulzSec planning to expose data belonging to a Philippine-based airline company. The actor behind the Twitter account claimed to allegedly access the contents of the airline's application server and allegedly the airline's corporate network. The unauthorised access was acknowledged by the airline company, and the company assured that no credit card details were stored on the compromised server. Despite the threat made by the hacker, GreyInt did not identify any data associated with the airline company leaked to the public.





JULY 2020

Information system belonging to a Philippine provincial prison compromised by hackers and leaked screenshots of inmates data.

Threat actor classification: ***Hacktivist***

In July 2020, GreyInt discovered a Facebook post from a local hacking group claiming to compromise an information system associated with a Philippine-based prison. The Facebook post included screenshots likely taken from the system. The screenshots suggested that the hackers were able to view, edit and delete information of detainees. One of the screenshots include a censored mugshot of a detainee and his personal information. The system was inaccessible the next day, likely being taken down to remediate the issue after the exposure.

PHILIPPINES SELECTED CASE STUDIES

OCTOBER 2020

Philippine company allegedly hit by Ragnarok ransomware.

Threat actor classification: ***Cybercriminal***

In late-September 2020, GreyInt discovered two Philippine education institutions likely hit by Ragnarok ransomware. Sample data allegedly belonging to the two institutions were posted on Ragnarok's blog accessible via the Tor network. Sample data posted included bank accounts, financial check-up forms, client information, employees and students' information including name, education, phone number, amongst others.

INDONESIA

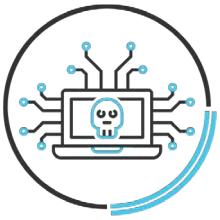
TOP 3 TARGETED SECTORS

PUBLIC SECTOR

FINANCIAL

EDUCATION

TOP ACTORS OBSERVED



CYBERCRIMINAL

HACKTIVIST

2019

AUGUST 19

- Public sector website compromised and infected with "Shutdown57" ransomware.
- *Web application vulnerability on an Indonesian Bank shared by hacker in a private Facebook group.*

DECEMBER 19

- Platform developed to trade hacked data shared in private Facebook groups.

2020

MARCH 20

- Foreign hacking group based in South Asia claimed to have breached a website associated with Indonesian military.

JUNE 20

- Actor claimed to possess COVID-19 database of Indonesian patients offered for sale in criminal forum.

AUGUST 20

- Variant of Hidden Tear ransomware used by hacker to infect a public sector website.

SEPTEMBER 20

- Hacker advertises access to an Indonesian Bank and shares screenshots as proof in private Facebook group.
- REvil threatens to release data belonging to an Indonesian company from the agriculture sector unless ransom is paid.
- Hacker deploys ransomware known as RedSkull on public sector website to demonstrate capabilities.

OCTOBER 20

- Public sector websites targeted by hacktivists to protest against the Omnibus Law.

2021

INDONESIA SELECTED CASE STUDIES

AUGUST 2020

Variant of Hidden Tear ransomware used by hacker to infect a public sector website.

Threat actor classification: ***Cybercriminal***

In mid-August 2020, GreyInt identified a threat actor sharing a screenshot of a compromised public sector website in a private Facebook group. The screenshot suggested that the public sector website ending with "go.id" was replaced with a ransom note. The note states that the files on the website were encrypted and a ransom would need to be paid to a bitcoin address in order to get the decryption key to unlock the files.

GreyInt research into the actor revealed that the actor was likely based in Indonesia. The actor developed multiple ransomware variants, and advertised them on his blog site. The actor also had a presence in a cybercriminal forum, which he leveraged to sell ransomware building tools.

SEPTEMBER 2020

Hacker advertised access to an Indonesian bank and shared screenshots as proof in private Facebook group.

Threat actor classification: ***Cybercriminal***

In early September 2020, GreyInt discovered a threat actor advertising backdoor access to an Indonesian bank in a private Facebook group. The actor posted screenshots of the alleged access as proof in the private group consisting mainly Indonesian users. One of the screenshots suggested that a webshell was uploaded into the bank's website revealing its contents. The actor also claimed to have access to a retail company, and showed proof of his hack, including the exfiltration of a database by uploading his hacking process to YouTube.

INDONESIA SELECTED CASE STUDIES

OCTOBER 2020

Public sector websites targeted by hacktivists to protest against the Omnibus Law.

Threat actor classification: ***Hacktivist***

In early October 2020, GreyInt identified over 60 Indonesian websites, mostly government related, compromised and defaced by local hacktivists. The links to these defaced websites were shared in multiple private Facebook groups dominated by Indonesian-speaking users. According to the Facebook posts and comments, the defacement attacks were conducted to protest against the Omnibus Law (also known as Job Creation Law) that saw several public protests since it was passed.

The Omnibus Law was designed to strengthen the national economy through the improvement of investment ecosystem and competitiveness, particularly in the midst of global uncertainty and economic slowdown. The Law (or Bill), which President Jokowi vowed to initiate reform to boost investments and create more jobs, was passed in Parliament on 5 October.

The passing of the Law was followed by multiple street protests by Indonesians, including labour unions which raised concerns over how it could affect the country's environment, human rights and labourers. Comments made on social media revealed that many Indonesians were worried that the law would reduce the salary, cut down contracts, and make Indonesians harder to get jobs.

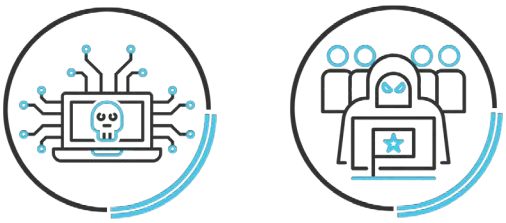
This sense of insecurity and concerns by Indonesians likely drove the hacktivists into targeting public sector websites as a form of protest.

VIETNAM

TOP 3 TARGETED SECTORS

PUBLIC SECTOR | EDUCATION | FINANCIAL

TOP ACTORS OBSERVED



CYBERCRIMINAL | HACKTIVIST

2019

MARCH 19

- Phishing emails delivering GandCrab ransomware target Vietnamese users.

NOVEMBER 19

- 2 million records of customer information associated with a Vietnamese bank advertised in criminal forum.

2020

JANUARY 20

- Credentials associated with a public sector entity and an education institution leaked on criminal forum.
- Public sector websites breached by Iranian hacktivist in protest against the assassination of Iranian General.

FEBRUARY 20

- Hackers posted screenshots of user details after breaching a Vietnam-based e-commerce and entertainment website.

MARCH - APRIL 20

- East Asia-based APT groups likely targeting Vietnam using Covid-19 lure.

APRIL 20

- Hacking group breached Vietnamese gaming site and leaked database on Facebook.

JULY 20

- Venezuelan hacker claims to sell access to a public sector website.

AUGUST 20

- Vietnam-based steel sheet manufacturing company hit by Maze ransomware.

OCTOBER 20

- Customer records of Vietnam-based car manufacturing company leaked on criminal forum.

2021

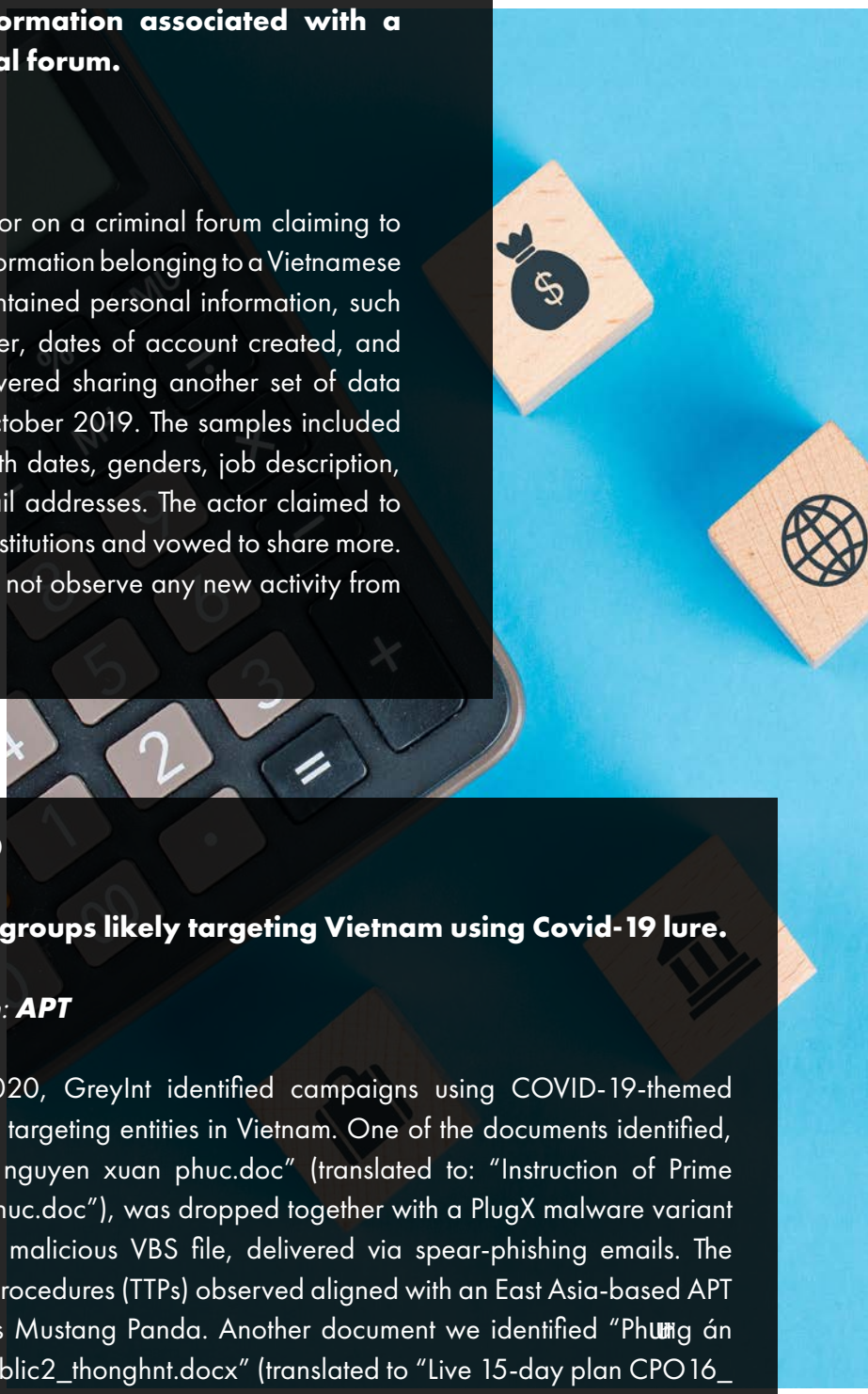
VIETNAM SELECTED CASE STUDIES

NOVEMBER 2019

Two million records of customer information associated with a Vietnamese bank advertised in criminal forum.

Threat actor classification: ***Cybercriminal***

In November 2019, GreyInt identified an actor on a criminal forum claiming to possess over two million records of customer information belonging to a Vietnamese commercial bank. Sample records posted contained personal information, such as account numbers, names of account holder, dates of account created, and account balances. The actor was also discovered sharing another set of data from the same commercial bank earlier in October 2019. The samples included PIIs such as customer names, ID numbers, birth dates, genders, job description, contact numbers, home addresses, and e-mail addresses. The actor claimed to have more databases belonging to financial institutions and vowed to share more. However, since November 2019, GreyInt did not observe any new activity from the actor.



MARCH - APRIL 2020

East Asia-based APT groups likely targeting Vietnam using Covid-19 lure.

Threat actor classification: ***APT***

In March and April 2020, GreyInt identified campaigns using COVID-19-themed documents as lures likely targeting entities in Vietnam. One of the documents identified, "Chi Thi cua thu tuong nguyen xuan phuc.doc" (translated to: "Instruction of Prime Minister Nguyen Xuan Phuc.doc"), was dropped together with a PlugX malware variant from the execution of a malicious VBS file, delivered via spear-phishing emails. The tactics, techniques, and procedures (TTPs) observed aligned with an East Asia-based APT group publicly known as Mustang Panda. Another document we identified "Phương án trực 15 ngày BĐCP16_public2_thonghnt.docx" (translated to "Live 15-day plan CPO16_public2_thonghnt.docx") was likely impersonating the Central Post Office of Vietnam. The document exploited the CVE-2017-0199 vulnerability and dropped artefacts which were previously observed in campaigns conducted by an East Asia-based APT group publicly known as Goblin Panda. Both APT groups have historically targeted government entities in SEA.

VIETNAM SELECTED CASE STUDIES

FEBRUARY 2020

Hackers posted screenshots of user details after breaching a Vietnam-based e-commerce and entertainment website.

Threat actor classification: ***Hacktivist***

In February 2020, GreyInt found an image posted on the Facebook page owned by a Vietnam-based hacking group. The image was revealed to be a screenshot of user details possibly associated with an e-commerce website of a major entertainment company. User details included name, gender, login name, personal email address, company email address, among others - all in cleartext.

The Vietnam-based hacking group has been operating since at least 2017, conducting mainly website defacement as well as denial of service attacks against their targets which included government organisations, education institutions and banks.

THAILAND

TOP 3 TARGETED SECTORS

PUBLIC SECTOR EDUCATION FINANCIAL

TOP ACTORS OBSERVED

CYBERCRIMINAL NATION STATE

2019

JULY 19

- Public sector websites targeted by foreign hacktivists during Burmese Martyrs Day.

2020

JANUARY 20

- *Threat actor 'White System' compromised and infected public sector website with ransomware.*

JUNE 20

- Power authority organization allegedly hit by Maze ransomware.

JULY 20

- Venezuelan hacker claims to sell access to a public sector website.

AUGUST 20

- Threat actor selling access to a corporate network belonging to an organization from the media industry.

SEPTEMBER 20

- Ransomware likely developed by foreign hackers in Southeast Asia possibly used against Thailand users.
- Millions of PII associated with companies in the Food and Beverages industry leaked and offered for sale on criminal forum.

SEPTEMBER - OCTOBER 20

- Multiple Thai companies allegedly hit by Netwalker and Ragnarok ransomware.

NOVEMBER 20

- Threat actor claims to sell access and databases associated with websites from the public sector.

2021

THAILAND SELECTED CASE STUDIES

SEPTEMBER 2020

Ransomware likely developed by Southeast Asian hackers possibly used against Thailand users.

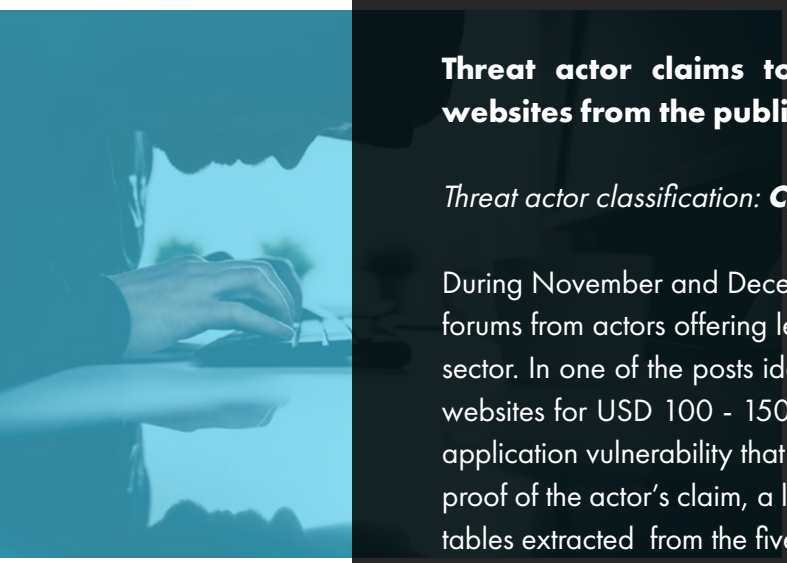
Threat actor classification: ***Hacktivist***

In late August 2020, GreyInt discovered a ransomware binary, named "salary.exe", using a Adobe PDF icon in an attempt to impersonate a PDF document. The ransomware when executed on a system will encrypt files such as documents and images. These encrypted files were given the .UGMH extension. A text file "Pwned.txt" would then appear on the desktop which reads "Your country is weak, your system is like a poor cheese, lot of holes, lot of vulnerabilities. You will never see your files again and we will public it to everyone. Fear us!! We are UGMH".

The contents of the text file indicated that the hackers were likely not financially motivated as there were no demands of ransom or contact provided to negotiate the process of getting the decryption key to unlock the encrypted files.

GreyInt assessed the term UGMH was likely a reference to a hacktivist group based in SEA. UGMH has also conducted politically-motivated hacktivist operations against Bangladesh (#Op_Bangli) and Thailand (#OpThai) targeting both public and private sector websites with mainly defacement attacks. Previously, in late August 2019, UGMH announced Operation Thailand 2019 (#OpThailand2019) and attacked 30 Thai websites from the public sector.

The UGMH extension ransomware sample submission to a public malware scanning service on 25 August 2020 from Thailand aligns with the anniversary of #OpThailand2019 conducted by UGMH. GreyInt assessed that hackers from UGMH possibly developed a ransomware and used it to target entities in Thailand.



NOVEMBER 2020

Threat actor claims to sell access and databases associated with websites from the public sector.

Threat actor classification: ***Cybercriminal***

During November and December 2020, GreyInt discovered multiple posts on criminal forums from actors offering leaked data, credentials and network access to Thai public sector. In one of the posts identified, an actor was offering access to five public sector websites for USD 100 - 150 per website. The actor claimed to know of a critical web application vulnerability that could allow access to the web servers when exploited. As proof of the actor's claim, a link to a text-sharing site showing a list of internal database tables extracted from the five websites was posted on the forum. Other similar postings identified by GreyInt include offering access, data and/or credentials to a travel company, an e-commerce organisation and a media conglomerate.

MYANMAR

TOP 2 TARGETED SECTORS

PUBLIC SECTOR TECHNOLOGY

TOP ACTORS OBSERVED

HACKTIVIST NATION STATE

2019

MARCH 19

- Public sector websites targeted by South Asia-based hacktivists.

2020

SEPTEMBER 19 - MAY 20

- Public sector likely targeted by East Asia-based APT delivering PlugX.

OCTOBER 20

- Screenshots of personal information allegedly from online portal associated with the public sector shared by hackers on Facebook.

NOVEMBER 20

- Domain created to mimic embassy suggests potential targeting against entities in Myanmar.

2021

MYANMAR SELECTED CASE STUDIES

MARCH 2019

Public sector websites targeted by South Asia-based hacktivists

Threat actor classification: ***Hacktivist***

In late March 2019, GreyInt observed multiple websites ending with the domain ".mm" defaced by South Asia-based hackers. A total of 11 websites – seven of which belonging to the Myanmar's public sector were targeted by a hacktivist group calling itself "Cyber71". The attack was conducted as a protest towards the Burmese government's stand and handling on the Rohingya issue which has raised concerns by the United Nations and Human Rights Watch groups.

SEPTEMBER 2019 AND MAY 2020

Public sector likely targeted by East Asia-based APT delivering PlugX

Threat actor classification: ***APT***

In September 2019 and May 2020, GreyInt identified two documents, written in the Burmese language used as decoy in campaigns using TTPs aligned with an East Asia-based APT group known as Mustang Panda. One of the decoy documents impersonated the Myanmar Department of Urban and Housing Development (DUHD) and the other contained a symbol of a political organisation based in Myanmar.

Though it was not known who were targeted during the campaigns conducted by Mustang Panda, the use of political-themed decoy documents in the Burmese language suggested interest in entities based in Myanmar.

MYANMAR SELECTED CASE STUDIES

NOVEMBER 2020

Domain created to mimic embassy suggests potential targeting against entities in Myanmar by South Asia-based APT.

Threat actor classification: ***APT***

In mid-November 2020, GreyInt identified a domain impersonating the Myanmar embassy based in China and Singapore. The domain was using an IP address which resolved to domains impersonating other government entities based in South Asia. A malicious document utilising one of the domains as its command and control (C2) server was demonstrating TTPs observed used by a South Asia-based APT known as SideWinder. The creation of a domain impersonating a Myanmar embassy suggested the actor's possible interest in the country's foreign affairs.

SideWinder is an APT actor that has been observed targeting government and military entities based in South Asia and East Asia.

CAMBODIA

TOP TARGETED SECTOR

PUBLIC SECTOR

TOP ACTOR OBSERVED

NATION STATE

2019

MAY 19

- Three Cambodian government-themed document attributed to Ocean Lotus identified.

SEPTEMBER 19

- Khmer-language document leveraged by Ocean Lotus suggested interest in Cambodia's civil affairs.

2020

OCTOBER 20

- Ocean Lotus's decoy documents shows possible targeting of Cambodia's public and tourism sector.

NOVEMBER 20

- Executable file pretending to be a document with military-themed filename likely aimed at Ministers conference hosted by Cambodia.

2021

CAMBODIA SELECTED CASE STUDIES

2019 - 2020

Ocean Lotus Observed Targeting Entities in Cambodia.

Threat actor classification: ***APT***

Since April 2019, GreyInt identified multiple malicious documents in Khmer-language using themes and contents that suggested interest in entities within the public sector based in Cambodia. These malicious documents were attributed to Ocean Lotus with moderate confidence based on the TTPs demonstrated during the execution of the malicious documents. This includes the use of artefacts and C2 servers previously leveraged by the APT group, which were also reported by other security researchers.

In one of the artefacts GreyInt discovered, it was an executable masquerading as a Word document. This executable displayed a decoy document "9_Programme_SOMCA-Japan_FINAL.docx" when executed.

The decoy document "9_Programme_SOMCA-Japan_FINAL.docx" was likely referring to the Ninth ASEAN Ministers Responsible for Culture and Arts (AMCA) Meeting and the AMCA Meetings with Dialogue Partners, including the ASEAN Plus Three, China, Japan and the Republic of Korea that was held on 22 October via video conference. The meeting was hosted by Cambodia.

GreyInt assesses the malicious executable was likely intended for the host or the participants of the conference.

From 2019 to 2020, GreyInt did not observe much activities in Brunei and Laos compared to other countries mentioned in this section. The case studies here highlight the significant activity GreyInt identified in the two countries.

LAOS

SEPTEMBER 2020

Pubic sector website compromised to host Crimson RAT.

Threat actor classification: ***APT / Cybercriminal***

In early September 2020, GreyInt identified an email using a financial-themed subject sent to an engineering company in South Korea. The attachment, when executed, was observed retrieving a Crimson RAT sample from a website associated with Laos public sector, ending with "gov[.]la".

Crimson RAT is a remote administration tool and was reported to be utilised mainly by South Asia-based APT known as Transparent Tribe (aka Mythic Leopard, APT36). This APT group has primarily targeted neighboring governments and military personnel based in South Asia. However, the use of financial-themed subject and filename suggests criminal intent rather than cyberespionage.

BRUNEI

DECEMBER 2019

Public sector website leveraged by cybercriminals to deliver Emotet payloads.

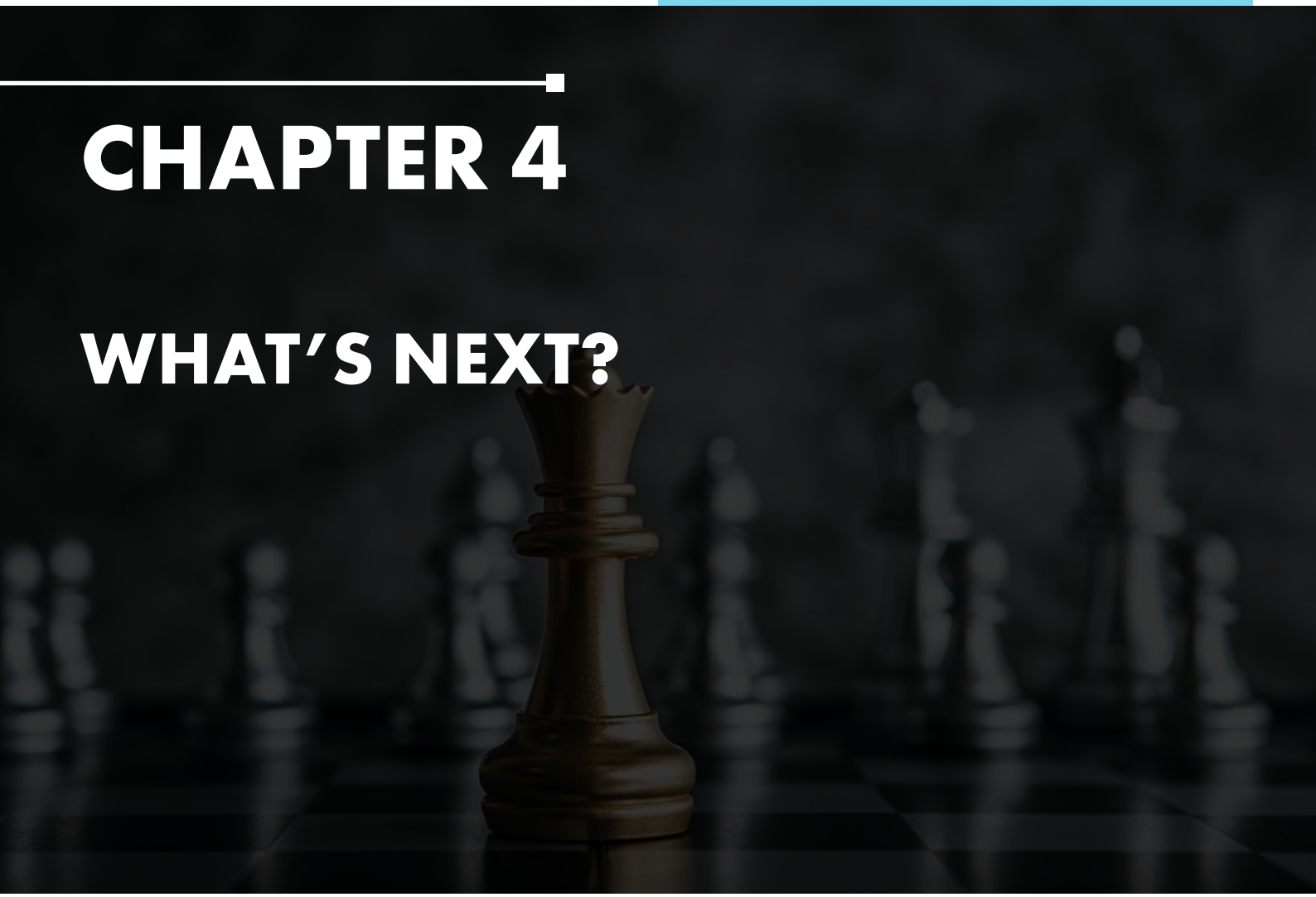
Threat actor classification: ***Cybercriminal***

In late-December 2019, GreyInt identified multiple malicious documents that when opened, spawned a PowerShell to retrieve Emotet payloads from a Bruneian public sector website. The website was discovered to be hosting several Emotet payloads and malicious Word documents.

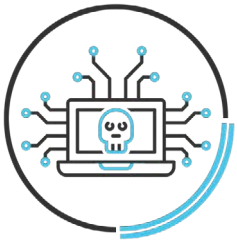
The public sector website was likely compromised by Emotet operators and used it to store its malicious payloads and documents.

CHAPTER 4

WHAT'S NEXT?

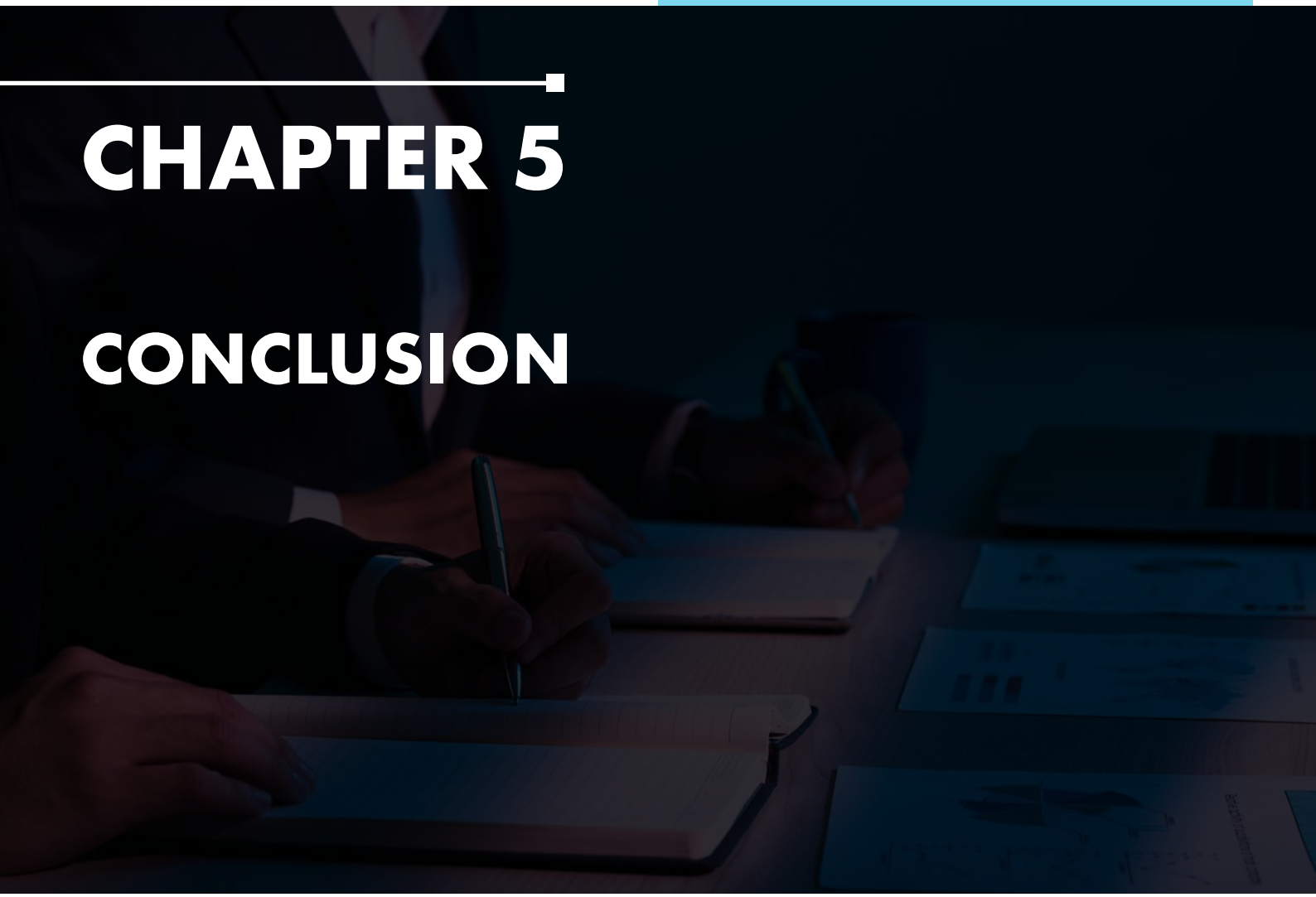


Hacktivism will continue to be active in Southeast Asia (SEA) particularly in Philippines, Indonesia and Myanmar, where operations organised by hacking groups were mostly driven by political issues and discontentment against authorities. Public sectors such as government organisations will continue to be the primary target as compared to organisations in other sectors. Techniques used in hacktivist operations will continue to be mainly website defacements, data leaks and denial of service attacks. However, recent observation highlighted the use of non-financially motivated ransomware likely used in hacktivist operations. It is worth noting that the use of non-financially motivated ransomware was also observed used by hacktivists in South Asia to target prominent websites in politically-motivated operations.



Cybercrime in SEA will likely rise in months to come as operations such as malicious spam emails attached with information stealing malware, ransomware attacks, data leaks and selling of unauthorised access to corporate and government networks have significantly spiked in 2020 as compared to 2019. The rise of Big Game Hunting (BGH) and human operated ransomware were observed increasingly targeting organisations in SEA as compared to previous years, when ransomware were mostly delivered via malicious spam emails from opportunistic cybercriminals. Cybercriminals were also observed exploiting vulnerable government and corporate websites across SEA, and advertising access on Facebook and criminal forums for profit. SEA-based hackers have also leveraged, and will continue to exploit, vulnerable e-commerce websites. The financial data obtained from exfiltrated databases would continue to be used to conduct carding-related activities, and advertise on social media, or communication platforms such as Telegram.

Advanced persistent threat (APT) actors targeting SEA will remain active, with government and multinational corporations (MNCs) likely being the primary targets of cyberespionage campaigns. The initial attack vectors observed by APT actors showing interest in SEA were not as sophisticated as those adopted by cybercriminals observed targeting SEA organisations. APT actors with interest in SEA continue to rely on traditional, yet effective, social engineering tactics, such as spear-phishing emails to deliver weaponized documents, malicious .EXE files using PDF/Word icon, or APK files, hoping that the targeted person would execute, download, and install them. The weaponized documents attached in spear phishing emails could leverage on malicious macros, or known vulnerabilities, such as CVE-2017-11882 and CVE-2018-0802, of which patches are readily available. Organisations with proper patch management framework and employee security training programs would be able to decrease the risks of being vulnerable to such initial attack vectors.



CHAPTER 5

CONCLUSION

Financially motivated cybercrime actors will continue to be a top threat to organisations in this region. Hacktivism, driven by political issues and territorial conflict, would come in second. Nation state actors, while not significantly active in this region, will continue to target government and government-linked organisations, likely for strategic intelligence.

Majority of the compromises and breaches highlighted in this report showed that most attacks against organisations were not highly sophisticated, which incorporated publicly available exploits of known, and sometimes old vulnerabilities to compromise public facing servers and websites, rather than utilising zero-day attacks. Organisations that have a mature patch management program, conduct regular security assessments, and incorporate cybersecurity trainings for employees would significantly reduce the risk of being vulnerable to many of the common initial attack vectors.

The rise in actors publishing stolen data observed against organisations in this region suggests that this technique will continue to be leveraged moving forward. Organisations could incorporate threat simulation plans using data leak as a scenario, and observe the various teams' preparedness, including senior management, in handling such incidents.

CONTACT DETAILS

EMAIL	:	**contact@greyint.com**
TELEGRAM	:	**@greyint**
WEBSITE	:	**greyint.com**
LINKEDIN	:	**https://www.linkedin.com/company/greyint**
RESPONSIBLE DISCLOSURE	:	**https://greyint.com/responsible-disclosure/**