INTERPOL

ASEAN CYBERTHREAT ASSESSMENT 2020

KEY INSIGHTS FROM

THE ASEAN CYBERCRIME OPERATIONS DESK

Page intentionally left blank

CONTENTS

Page intentionally left blank

FOREWORD

In our profoundly interconnected world, the impact of cybercrime can be far-reaching and devastating to its victims. The borderless nature of cybercrime means that cybercriminals are agile, exploiting new technologies as well as connecting and cooperating amongst themselves in ways we have never imagined before. To address these challenges in preventing, detecting and investigating cybercrime globally, law enforcement agencies must adapt to this ever-changing criminal environment in order to protect communities and ensure a safer digital world.

Driven by the increasing use of digital technologies, INTERPOL member countries in the Association of Southeast Asian Nations (ASEAN) are rapidly transforming into digital economies. With more businesses shifting to digitalization, more individuals are performing daily transactions online in ASEAN countries. Consequently, securing cyberspace has become a high priority for all law enforcement organizations in the region.

In July 2018, the INTERPOL Cybercrime Directorate – with support from the Singapore Government and the Japan-ASEAN Integration Fund (JAIF) 2.0 – created the ASEAN Cybercrime Operations Desk (hereafter, the ASEAN Desk) to address growing cyberthreats across the region. Through the ASEAN Desk, INTERPOL delivers policing capabilities to tackle cybercrime using intelligence development, investigative support and operational coordination.

Under the mandate of reducing the global impact of cybercrime and protecting communities for a safer world, INTERPOL Cybercrime Directorate's core activity is to collect, store, process, analyse, evaluate and disseminate cyber intelligence to better support member countries in understanding cyberthreats nationally, regionally and globally.

As part of these efforts, I am proud to present the first edition of the ASEAN Cyberthreat Assessment 2020 produced by the ASEAN Desk. This report provides analyses and insights on the latest cyberthreat landscape faced by the member countries in the ASEAN region. With the aim of protecting digital economies and communities in ASEAN, the report also highlights strategies and the way forward in the region.

While the persistence of cyberthreats such as ransomware, banking malware and botnets are highlighted, a new type of cybercrime − cryptojacking − is analysed in the report. Indeed, as soon as it was captured on our radar, the ASEAN Desk was able to lead on-the-ground action against cybercriminals committing this type of crime by developing a plan for multi-jurisdictional operations and coordinating joint actions against cryptojacking.

The Cybercrime Directorate aims to deliver more operational activities by coordinating cyber operations in five regions − Africa, the Americas, Asia, Europe, and the Middle East and North Africa (MENA) replicating the ASEAN Desk framework. The increased and enhanced operational support will better support member countries, reflecting the unique challenges and needs within the respective regions.

In addition to operational delivery, we also focus on capability development. We aim to place the human aspect at the heart of our work, providing and developing the relevant skills and technology to allow for better outcomes. This has been fulfilled by the ASEAN Cyber Capacity Development Project (ACCDP) for member countries in the ASEAN region, as we strengthen their abilities to combat cybercrime and boost cooperation in cybercrime matters between countries, and regional and international partners.

I hope this report will help to provide a better understanding of the regional cyberthreat landscape to devise a prioritized and targeted response to cybercrime threats.

Craig Jones
Director, Cybercrime Directorate
INTERPOL

ABBREVIATIONS AND ACRONYMS

ACCDP	ASEAN Cyber Capacity Development Project
AJOC	ASEAN Joint Operation against Cybercrime
ASEAN	Association of Southeast Asian Nations
ASEAN Desk	INTERPOL ASEAN Cybercrime Operations Desk
BEC	Business E-mail Compromise
CERTs	Computer Emergency Response Teams
CII	Critical Information Infrastructure
CnC	Command and Control server
CARs	Cyber Activity Reports
DDoS	Distributed Denial-of-Service
DNS	Domain Name System
EU	European Union
FBI	Federal Bureau of Investigation
HTTPS	Hypertext Transfer Protocol Secure
IGCI	INTERPOL Global Complex for Innovation
IP	Internet Protocol
IRC	Internet Relay Chat
JAIF	Japan-ASEAN Integration Fund
OSINT	Open-Source Intelligence
P2P	Peer-to-Peer
PoS	Point-of-Sale
PPP	Public Private Partnerships
RATs	Remote Access Tools
SMEs	Small and Medium-sized Enterprises
SSL	Secure Sockets Layer

EXECUTIVE SUMMARY

A robust cybersecurity ecosystem is critical for countries to maintain confidence in the use of electronic communications and services, given the continuous rise in the scale and complexity of cybercrime. To make well-informed policies that support such an ecosystem, leaders need to have an understanding of the current cyberthreat landscape.

In 2019, we faced a challenging and evolving cyberthreat landscape. Threat actors continued to improve their cyberweapons, adopted new attack methods, and tailored their attacks to emerging technologies. Belonging to one of the fastest-growing digital economies in the world, member countries in the ASEAN region experienced a significant amount of cybercrime, ranging from massive data breaches, crippling ransomware attacks and the meteoric rise in cryptojacking.

With data drawn from INTERPOL's private partners and research conducted by the ASEAN Desk, this report provides a comprehensive overview of the cyberthreat trends in ASEAN countries. The report has identified the following as some of the prominent cyberthreats in 2019:

- BOTNETS. In the first half of 2019, there was an increase in botnet detections and hosting of CnC servers in the ASEAN region, which accounted for **7 per cent of botnet detections and 1.8 per cent of CnC servers worldwide**. The majority of botnets still target the financial sector and its customers, with the aim of gaining remote access to victims' computers - either to steal personal data such as banking credentials or to install and spread other malicious malwares.
- PHISHING CAMPAIGN increasing in both quantity and sophistication. We saw a more advanced exploitation of social engineering techniques worldwide with e-mail remaining the top vector for phishing (96 per cent)[1]. According to a report, Southeast Asia remains a target for cybercriminals attempting to infect networks and devices through the simple but effective trick of phishing.
- BUSINESS E-MAIL COMPROMISE campaigns have proven to be low-cost, low-risk but high-rate of return to cybercriminals. Data drawn from our private partners showed that member countries in ASEAN faced more than 5 per cent of the global BEC attacks. In the first half of 2019, it was detected that Singapore and Malaysia recorded the highest BEC attacks (54 per cent and 20 per cent of the total attacks in the ASEAN region, respectively).
- BANKING MALWARE. The first half of 2019 saw a 50 per cent increase in attacks compared to 2018. The shift of prominent malware families, such as the Emotet16 banking Trojan, from banking credential theft to the distribution business, marks a significant phenomenon observed in 2019.
- RANSOMWARE continues to grow and morph due to the increasing popularity of cryptocurrencies. We observed the emergence of numerous variants after 2013. After the shift to crypto-ransomware, ransomware continued to evolve, adding features such as countdown timers, ransom amounts that increase over time, and infection routines that enable it to spread across networks and servers. Cerber, as an evolved ransomware technology, topped the number of detected ransomwares in ASEAN countries. WannaCry, which ranks second in the ASEAN region but first globally, remains a threat following its rapid propagation in 2017.
- CRYPTOJACKING emerged as a new threat, with the growing use of cryptocurrencies and the ability to harness the computer power of unknown users' systems to perform cryptojacking, putting businesses and individual users across the globe are at risk. It was observed that cybercriminals have been exploiting vulnerabilities in cybersecurity protection and in technologies to launch cryptojacking campaigns globally, which includes ASEAN countries.

Under the mandate of reducing the global impact of cybercrime and protecting communities for a safer world, the INTERPOL Regional Cybercrime Strategy for ASEAN sets out INTERPOL's key priorities and principles in combatting cybercrime in ASEAN countries. The Strategy, delivered through the ASEAN Desk and ACCDP, is underpinned by the following four pillars: enhancing cybercrime intelligence for effective responses to cybercrime; strengthening cooperation for joint operations against cybercrime; developing regional capacity and capabilities to combat cybercrime; and promoting good cyber-hygiene for a safer cyberspace. These pillars shape the way forward for the ASEAN Desk to effectively coordinate the joint actions against cyberthreats in the ASEAN region.

[1] Verizon 2018 Data Breach Investigation Report https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf)

ACKNOWLEDGMENT

Under the supervision of James Tan, Acting Assistant Director (Strategy and Capabilities Development) concurrent Head of ASEAN Cybercrime Operations Desk, this report was written by Wei XianTee, Specialized Officer; Wookyung Jung, Policy Analyst; and Alyssa Ann Radlett, Project Manager.

The report also benefited from the contributions of member countries in the ASEAN region; INTERPOL Cybercrime Directorate's private partners; and a former colleague, Beatriz de Oliveira da Silveira.

1. INTRODUCTION: METHODOLOGY

The Internet has created borderless societies worldwide, providing unprecedented opportunities to generate wealth and stimulate economies. Countries across the world seek to benefit from new technologies to boost economic growth and facilitate access to information and services. In 2019, more than half the world's citizens were connected to the Internet (4.437 billion users)[2] and used it services, such as e-mail, online banking, e-commerce and social networks to conduct much of their day-to-day life. The Internet will become more pervasive in our everyday life. According to one study, it is projected that the total installed base of Internet of Things (IoT) connected devices will reach 75.44 billion[3] worldwide by 2025.

The ASEAN region has a total population of about 659 million— over 100 million more than the European Union (EU)—and is the world's third most populous region. It has a combined GDP of more than USD 2.7 trillion[4] and is the world's seventh largest market, which is predicted to exceed USD 4 trillion by 2022. In addition, its digital economy has the potential to add another USD 1 trillion to its GDP over the next 10 years.

On the cusp of digital transformation, ASEAN is pushing for new infrastructure and technology advancements to boost its economic capabilities.

This increasing reliance upon the Internet, however, has created a number of cyberthreats that can cause immense damage, impede trust and resilience in the digital economy, and prevent the region from realizing its full digital potential. Criminal networks also operate across the world, coordinating complex attacks against their targets in a matter of minutes. Statistics on threats to computer networks are sobering and reflect the shift from the relatively innocuous spam of yesteryear to the more malicious threats today.

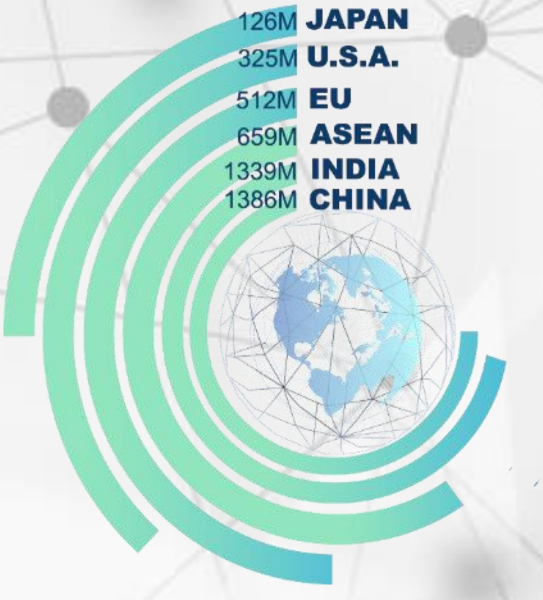


Figure 1: Population

Increasingly frequent, sophisticated and damaging cyberattacks are occurring on a global scale affecting critical information infrastructure (CII), such as in the financial and energy sectors. Take, for example, the impact of the "WannaCry" global ransomware cyberattack,[5] not only governments, businesses, and private citizens, but also on critical infrastructure such as the National Health Service in the United Kingdom, which struggled to function after it was infected.

A robust cybersecurity ecosystem is critical for countries to maintain confidence in the use of electronic communications and services, given the continuous rise in the scale and complexity of cybercrime. To make well-informed policies that support such an ecosystem, leaders will need to have an understanding of the current cyberthreat landscape.

> "The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency."

In 2019, we faced a challenging and evolving cyberthreat landscape. Threat actors continued to improve their cyberweapons, adopted new attack methods, and tailored their attacks to emerging technologies. Belonging to one of the fastest-growing digital economies in the world, member countries in the ASEAN region experienced a significant amount of cybercrime, ranging from massive data breaches, crippling ransomware attacks and the meteoric rise in cryptojacking.

[2] The State of Digital in April 2019 (www.wearesocial.com).

[3] Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (www.statista.com).

[4] GDP (Current) USD - The World Bank.

[5] "What is WannaCry ransomware?" (https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20).

While threat actors were trying hard to keep a low profile with their malicious activities, they could not avoid detection by the various stakeholders in partnership with INTERPOL. Indeed, we observed that public and private organizations are under constant attack from the ever-growing number of malwares spreading at higher rates than ever.

In this inaugural **ASEAN Cyberthreat Assessment 2020**, we provide our analyses and insights on the current cyberthreats faced by member countries in the ASEAN region. From massive data breaches and crippling ransomware attacks to a meteoric rise in cryptojacking, there is no shortage in disruption caused to the member countries in the ASEAN region.

With data drawn from INTERPOL's private partners and the research conducted by the ASEAN Desk, we will provide a comprehensive analysis of the trends observed in botnet, phishing campaigns, banking malware, cryptojacking, ransomware, and business e-mail compromise fraud.

We will conclude with a review of the predictions and recommendations on joint collaboration initiatives to tackle cybercrime effectively at a regional and global level.

2. ASEAN KEY DIGITAL FIGURES: 2019

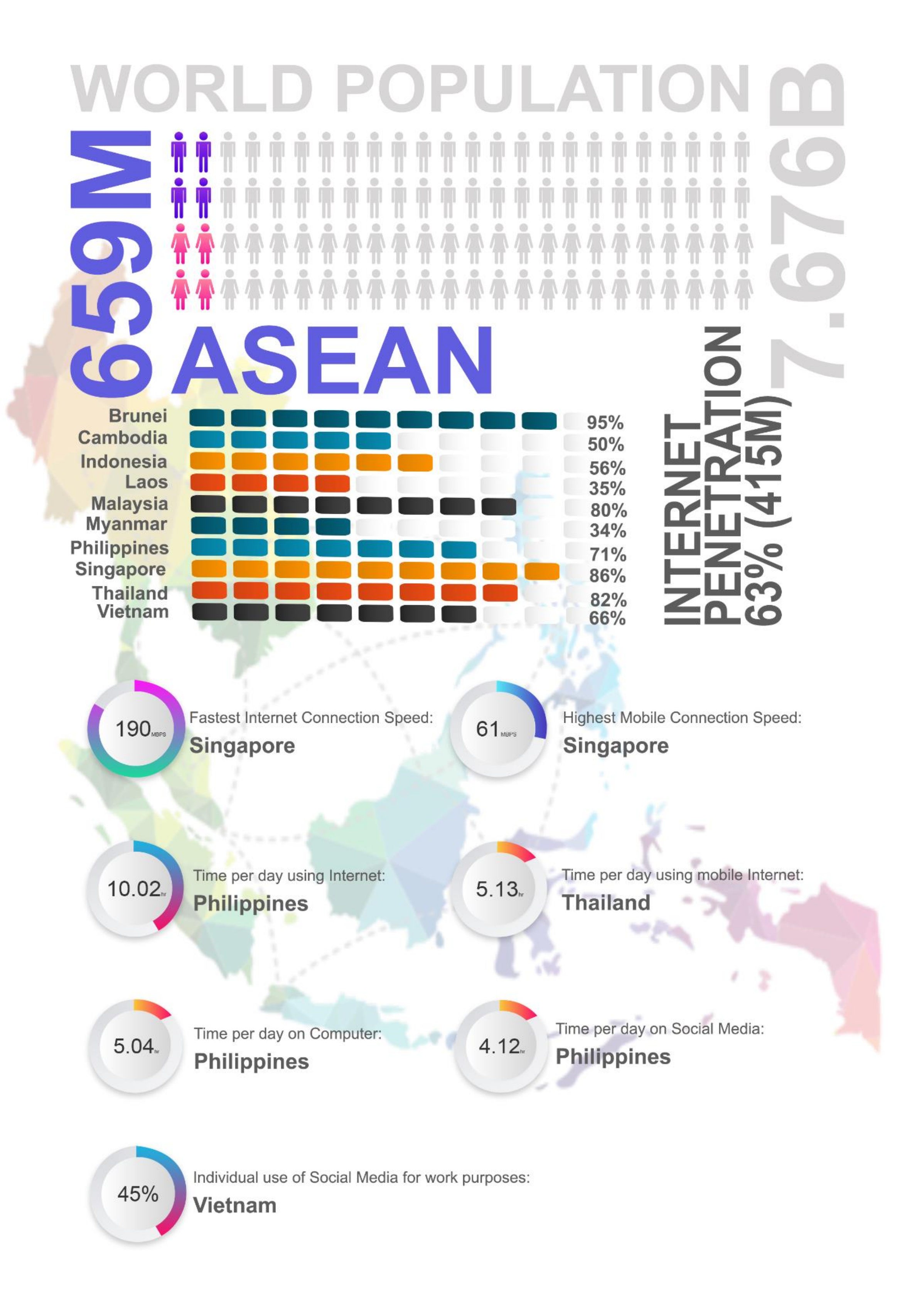
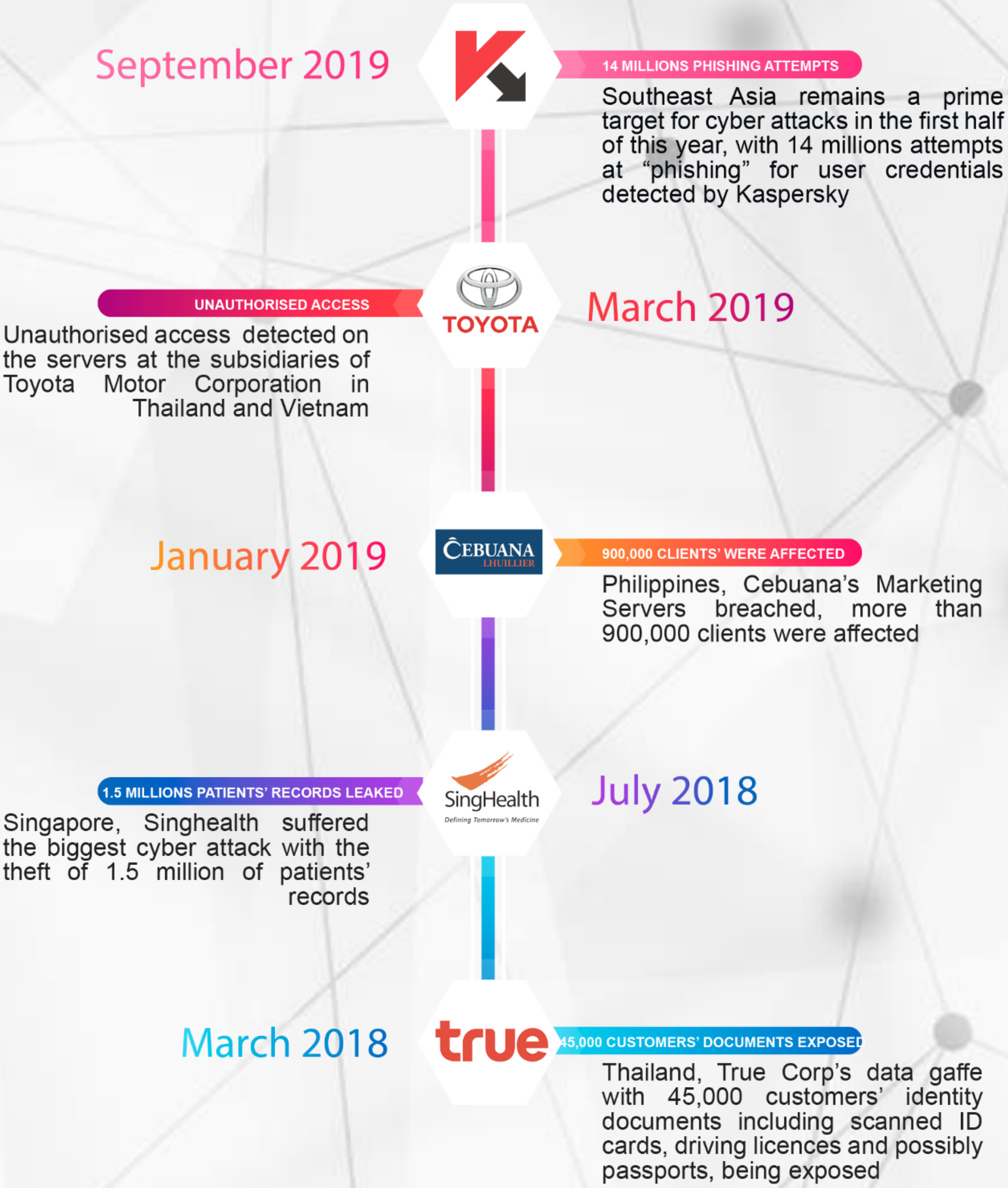


Figure 2: Digital ASEAN, WeAreSocial

3. MAJOR CYBERINCIDENTS: 2018-2019

Cyberattacks and data breaches have been ranked fourth and fifth in the recently released global risk report by the World Economic Forum (2019). The cost of cybercrime to businesses over the next five years is expected to be USD 8 trillion.[6] Here are some of the most serious data breach incidents in the ASEAN region throughout 2018 and 2019:



September 2019

14 MILLIONS PHISHING ATTEMPTS

Southeast Asia remains a prime target for cyber attacks in the first half of this year, with 14 millions attempts at “phishing” for user credentials detected by Kaspersky

March 2019

UNAUTHORISED ACCESS

Unauthorised access detected on the servers at the subsidiaries of Toyota Motor Corporation in Thailand and Vietnam

January 2019

900,000 CLIENTS' WERE AFFECTED

Philippines, Cebuana's Marketing Servers breached, more than 900,000 clients were affected

July 2018

1.5 MILLIONS PATIENTS' RECORDS LEAKED

Singapore, Singhealth suffered the biggest cyber attack with the theft of 1.5 million of patients' records

March 2018

45,000 CUSTOMERS' DOCUMENTS EXPOSED

Thailand, True Corp's data gaffe with 45,000 customers' identity documents including scanned ID cards, driving licences and possibly passports, being exposed

Figure 3: Major Cyberincidents in the ASEAN region, 2018-2019

[6] World Economic Forum 2019 Global Risk Report (http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf).

No country or organization in the ASEAN region is spared the threat of fast-evolving cybercrime. Given their position among the fastest-growing digital economies in the world, member countries in ASEAN have become a prime target for cyber-attacks.

According to research and several reports, malicious e-mail remains a weapon of choice for a wide range of cyberattacks. Spam e-mails account for **85 per cent**[7] of all e-mail sent. E-mail is also the top vector for both malware distribution (**92.4 per cent**) and phishing attacks (**96 per cent**).[8] Ransomware continues to plague businesses and consumers, with indiscriminate campaigns pushing out significant volumes of malicious e-mail.

Given that the majority of cybercrime impacts home users and small and medium-sized enterprises (SMEs), a set of preventive advice for users would raise awareness and empower them to protect themselves against malicious software and threat actors.

[7] Talos Intelligence data (www.talosintelligence.com).

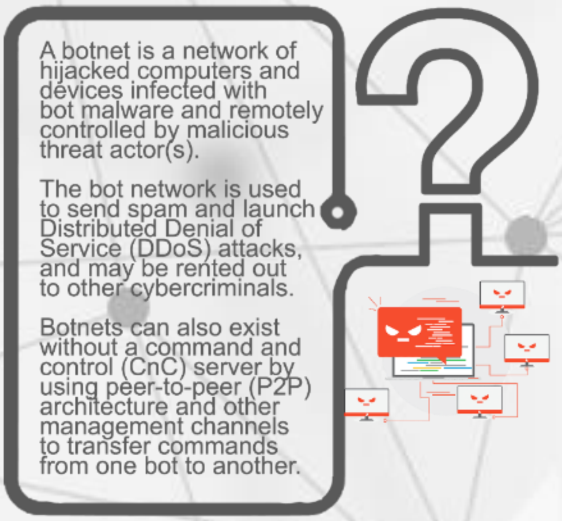
[8] Verizon 2018 Data Breach Investigation Report (https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf).

INSIGHT INTO CYBERTHREATS TRENDS IN 2019

The member countries in the ASEAN region faced numerous cyberthreats in 2019, including botnets, phishing campaigns, banking malware, ransomware, business e-mail compromise and cryptojacking.

With data drawn from INTERPOL's private partners, and the research conducted by the ASEAN Desk, this part will shed light on the threats, trends and underlying motivations of cybercrime.

4.1 Botnets



A botnet is a network of hijacked computers and devices infected with bot malware and remotely controlled by malicious threat actor(s).

The bot network is used to send spam and launch Distributed Denial of Service (DDoS) attacks, and may be rented out to other cybercriminals.

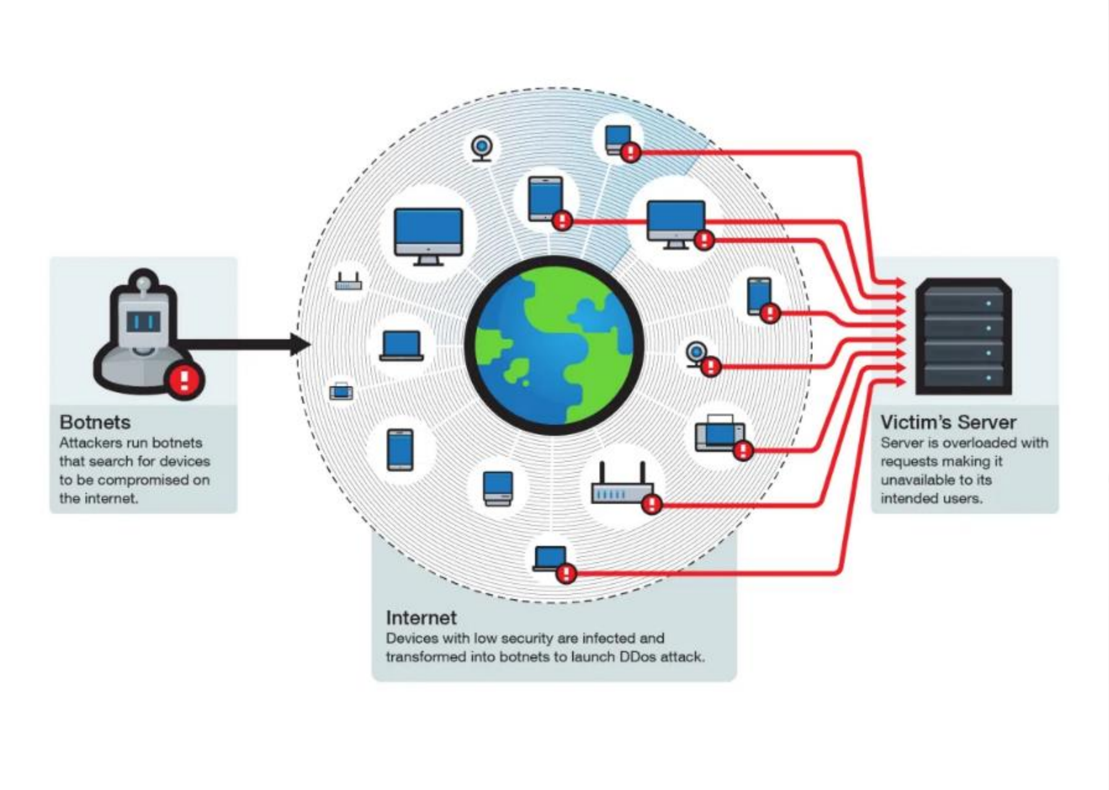
Botnets can also exist without a command and control (CnC) server by using peer-to-peer (P2P) architecture and other management channels to transfer commands from one bot to another.

Botnets have continued to evolve over the years. Their most common features now include varied CnC models:

- **Centralized or distributed;**
- **Varied attack types, such as spam, DDoS, data theft;**
- **Increase in communication protocols used: IRC, HTTPS;**
- **Effective use of evasion techniques, such as SSL, VoIP tunnelling;**
- **Versatile rallying mechanisms: hard-coded IP address, distributed DNS service.**

In 2016, a service provider, StarHub, encountered two waves of DDoS attacks that brought down Internet surfing on its broadband network. Subsequent investigations revealed that subscribers' bug-infected machines were turned into zombie machines that repeatedly sent queries to StarHub's Domain Name System (DNS), ultimately overwhelming it.

In addition to CIIs, botnets have also been used to target Points-of-Sale (PoS) and other payment systems in cases such as Operation Black Atlas,[9] causing massive financial losses. Botnets have been increasingly refined to exploit vulnerabilities, with more sophisticated versions being generated and distributed every few hours. These have been used for crimes against citizens, financial institutions, and the Internet itself – intercepting and redirecting traffic.



Botnets
Attackers run botnets that search for devices to be compromised on the internet.

Internet
Devices with low security are infected and transformed into botnets to launch DDos attack.

Victim's Server
Server is overloaded with requests making it unavailable to its intended users.

Figure 4: How a Botnet works, Trend Micro

[9] Operation Black Atlas (https://blog.trendmicro.com/trendlabs-security-intelligence/operation-black-atlas-endangers-in-store-card-payments-and-smbs-worldwide-switches-between-blackpos-and-other-tools/).

In the first half of 2019, there was an increase in botnet detections and hosting of CnC servers in the ASEAN region, which accounted for **7 per cent of botnet detections and 1.8 per cent of CnC servers worldwide**. In particular, Thailand had the highest number of botnet detections and hosted the highest number of CnC servers, followed by Malaysia, Philippines, Singapore and Indonesia.

According to our research, the top five dominant botnet threats detected in the ASEAN region were:

1. **Andromeda.Botnet**
2. **Conficker.Botnet**
3. **Necurs.Botnet**
4. **Sality.Botnet**
5. **Gozi.Botnet**

The Andromeda botnet, is the most recurrent botnet across all member countries in the ASEAN region. It has left many machines infected, despite being seized in a global operation in 2017. It is the highest detected botnet threat in the region. It is known for malicious e-mail attachments that deliver various malware modules, such as a keylogging capability.

Botnet families of Conficker and Sality appeared in 2008 and 2010, respectively. These attacks allowed infected machines to be controlled remotely.

Ramnit and Sality both have the capability of modifying legitimate files.

Necurs and Gozi botnets launched geotargeted cyberattacks circulating malicious e-mails.

In addition, the number of unique attacks on users linked to cryptocurrency services (exchanges, cryptocurrency wallets, etc.) has increased. Cybercriminals have been actively trying to monetise interest in cryptocurrencies and obtain data from victims to steal funds. The majority of botnet detections on users of cryptocurrency services featured Ramnit Banker.

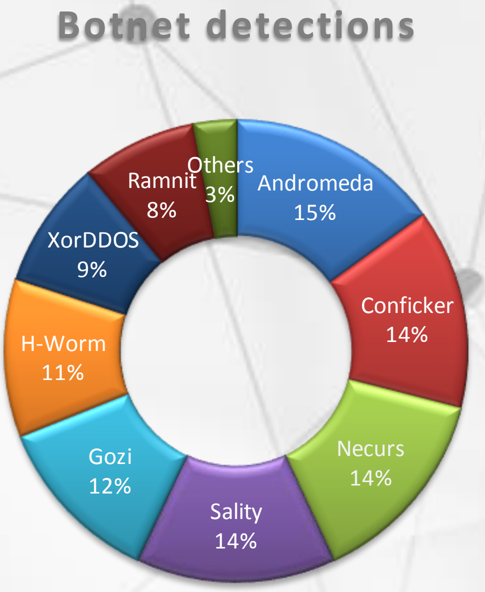


Figure 5: Botnet detections in the ASEAN region, 2019

The disruption of critical infrastructure services can have serious implications on national security. For private businesses, it will not only cause a loss of revenue, but will also have a long-term impact on the consumers' confidence and the reputation of the services provided.

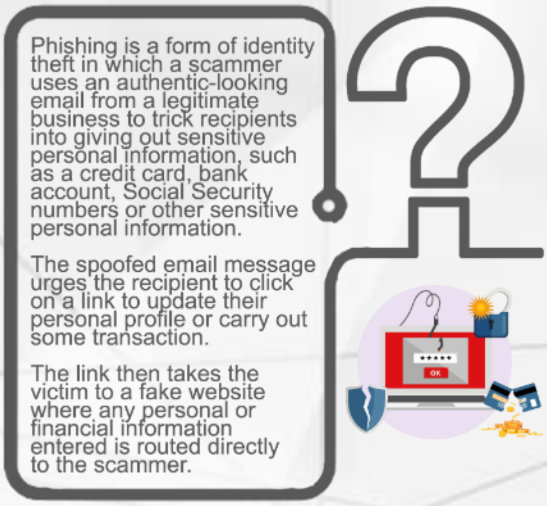
Our analysis identified the following botnet trends:

The majority of botnets still target the financial sector and its customers, with the aim of gaining remote access to victims' computers – either to steal personal data such as banking credentials or to install and spread other malicious malwares.

Given the increasing popularity of blockchain and the introduction of new cryptocurrencies, the number of attacks on users of cryptocurrency services will grow significantly. It is expected that more bots will deploy injection attacks against such resources.

New target masks are proliferating as well. Cybercriminals are adding brand new targets and modifying old masks to cover more websites where user data or money can be stolen.

4.2 Phishing campaigns



Phishing is a form of identity theft in which a scammer uses an authentic-looking email from a legitimate business to trick recipients into giving out sensitive personal information, such as a credit card, bank account, Social Security numbers or other sensitive personal information.

The spoofed email message urges the recipient to click on a link to update their personal profile or carry out some transaction.

The link then takes the victim to a fake website where any personal or financial information entered is routed directly to the scammer.

It is reported that spam e-mails accounted for 85 per cent[10] of all e-mails sent and that e-mail was the top vector for phishing (96 per cent).[11]

Phishing campaigns are increasing in quantity, sophistication, and are becoming more advanced in their exploitation of social engineering techniques worldwide. Every year, more and more attacks affect the world's largest organizations - with more than 1,000 phishing attacks[12] a month.

While some large organizations have implemented measures and educated employees in protecting themselves from phishing campaigns, individuals are nevertheless being targeted and falling victim to malicious threat actor(s).

Around **1.5m**[13] **new phishing sites** are created each month. The average lifetime of a phishing site is five days. Anti-phishing filters receive information about a new threat very quickly and so phishers constantly have to register new sites that imitate the official sites of various credible organizations. The most popular phishing targets are financial institutions, e-mail services and Internet service providers.

TrendMicro data[14] shows credential phishing is continually on the rise with a 59 per cent increase in worldwide detections in the first half of 2019. The top targeted brand is Microsoft (e.g. Office 365 credentials). Webmail (e.g. Gmail and Yahoo) are also popular targets as users' online transactions are often linked to webmail accounts.

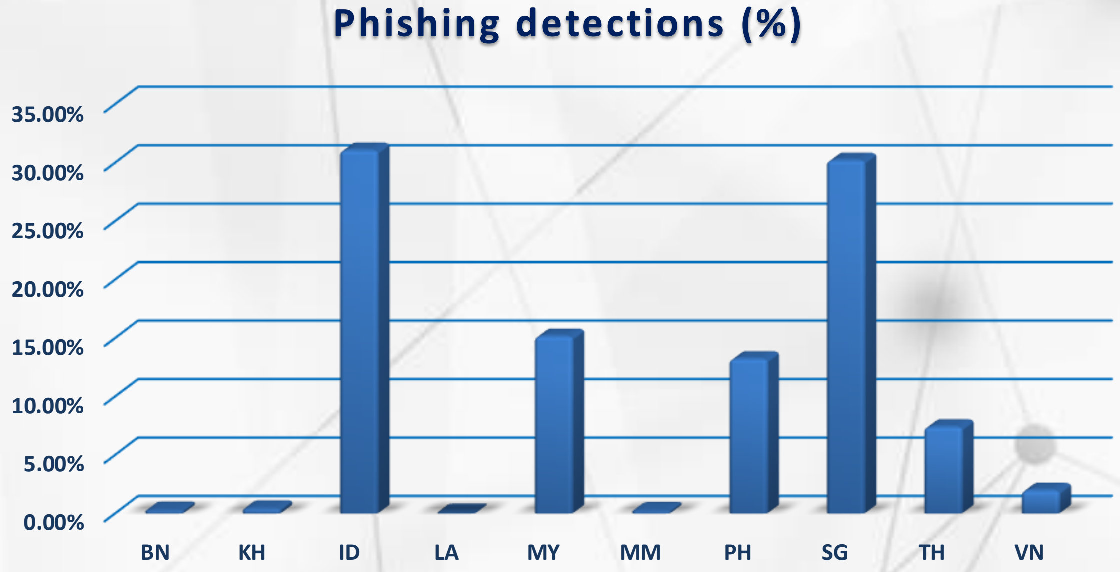


Figure 6: Phishing detections in ASEAN countries in 2019

[10] Talos Intelligence data (www.talosintelligence.com).

[11] Verizon 2018 Data Breach Investigation Report (https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf).

[12] 2018 Phishing Trends & Intelligence Report (https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report_2018-digital.pdf).

[13] 2019 Phishing Statistics (https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html).

[14] Trend Micro data (https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/the-rising-tide-of-credential-phishing).

According to Vade Secure, other top targeted service providers in the ASEAN region include PayPal; Netflix; Facebook; Dropbox and Apple, with numerous attempts recorded in Indonesia, Singapore, Malaysia and the Philippines.

Improving awareness is key to combatting cybercrime, according to a recent report from one of INTERPOL's partners – Kaspersky – which detected 14 million phishing attempts against Internet users in Southeast Asia in the first six months of 2019.

According to the report, Southeast Asia remains a target for cybercriminals attempting to infect networks and devices through the simplest yet still most effective trick of phishing.

Data shared by our partners revealed that attempts to direct users to phishing websites during the first half of 2019 was highest in **Indonesia (31.07 per cent)**, **Singapore (30.21 per cent)**, **Malaysia (15.16 per cent)**, **Philippines (13.23 per cent)** and **Thailand (7.41 per cent)**.

Despite the changing demographics in the ASEAN region, a significant amount of the population still falls prey to phishing attacks.

Kaspersky's data show that the **Philippines (17 per cent), Malaysia (16 per cent) and Indonesia (14 per cent) face the highest number of phishing victims in the ASEAN region.**

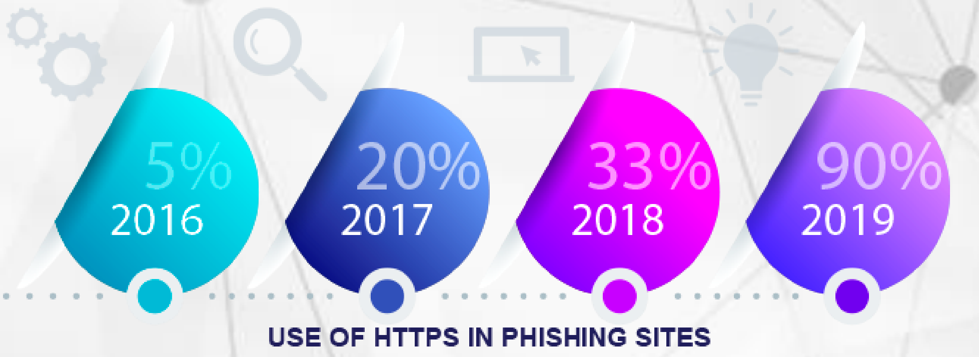


Figure 7: Use of HTTPS on phishing sites

Our analysis identified the following phishing campaign trends:

It is expected that phishing campaigns will continue to rise, given that companies are increasingly conducting their business online and relying heavily on technology for communication, and cybercriminals can easily access ready-to-deploy phishing kits.

Nearly 90 per cent of data breaches in 2019 involved phishing, causing significant financial losses to organizations recovering from the breaches.

Another aspect of the problem is that phishing sites are continuously evolving. In the past, a good way to defeat cybercriminals was to make sure you were visiting a HTTPS site. Not anymore. In 2016, only one in every 20 phishing sites had an HTTPS certificate. That number quadrupled in 2017, with 20 per cent of phishing sites having an HTTPS address. That number continues to rise with more than half of phishing sites using SSL certificates in the first quarter of 2019.

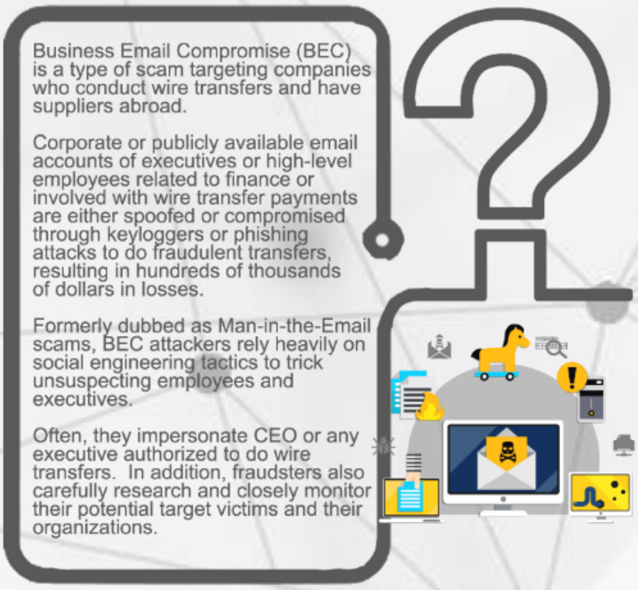
Phishing campaigns are also conducted as a launch pad for other scam activities for monetary gain by malicious threat actors, with the use of Remote Access Trojan (RAT) malware.

4.3 Business e-mail compromise

It was discussed in the previous section that phishing campaigns are increasingly served as a launch pad by malicious threat actors, with the use of RAT malware. This is often conducted during the preparation phase of business e-mail compromise (BEC) campaigns.

BEC campaigns have proven to be low-cost, low-risk but high rate of return for malicious threat actors and syndicates.

In 2018, the Federal Bureau of Investigation (FBI) reported that **companies all around the world lost USD 12 billion owing to business e-mail compromise**. The trend shows the amount of losses will continue to increase significantly over the next few years owing to the fact that more and more SMEs are going through a digital transformation. However, many organizations neglect to implement measures to protect against the emerging cyberthreats.

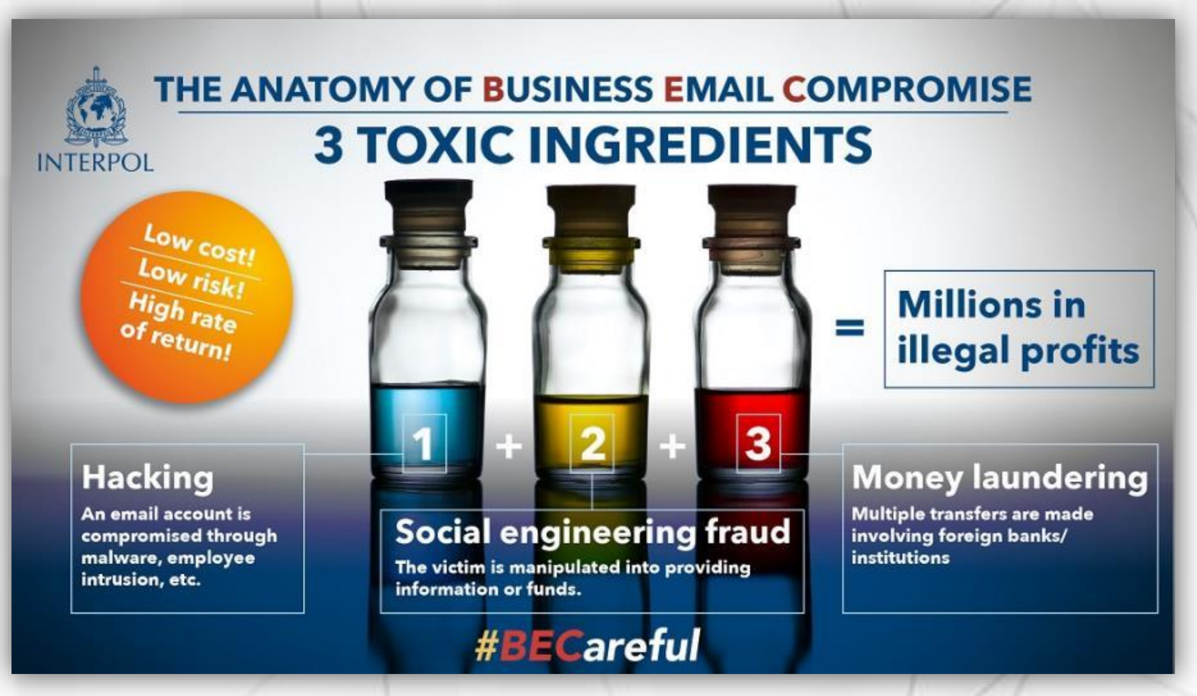


Business Email Compromise (BEC) is a type of scam targeting companies who conduct wire transfers and have suppliers abroad.

Corporate or publicly available email accounts of executives or high-level employees related to finance or involved with wire transfer payments are either spoofed or compromised through keyloggers or phishing attacks to do fraudulent transfers, resulting in hundreds of thousands of dollars in losses.

Formerly dubbed as Man-in-the-Email scams, BEC attackers rely heavily on social engineering tactics to trick unsuspecting employees and executives.

Often, they impersonate CEO or any executive authorized to do wire transfers. In addition, fraudsters also carefully research and closely monitor their potential target victims and their organizations.



THE ANATOMY OF BUSINESS EMAIL COMPROMISE

3 TOXIC INGREDIENTS

Hacking
An email account is compromised through malware, employee intrusion, etc.

Social engineering fraud
The victim is manipulated into providing information or funds.

Money laundering
Multiple transfers are made involving foreign banks/ institutions

#BECareful

Data obtained from our private partners showed that member countries in the **ASEAN region faced more than five per cent of the global BEC attacks**. While this figure does not indicate whether those BEC attacks were successful, most of the successful attacks were often not reported as the business entities were concerned that reporting might damage their reputations.

In the first half of 2019, Singapore and Malaysia recorded the highest BEC attacks among the 10 member countries in the ASEAN region, with 54 per cent and 20 per cent respectively.

With Singapore having the highest GDP in the region and also hosting many large business organizations, it attracts more attention of BEC attackers who target the private entities to yield large returns, even with fewer successful attacks.

On average, a successful BEC attack can net the attackers about USD 130,500 in returns.

According to FinCEN's[15] findings, manufacturing and construction were the most targeted sectors for BEC due to the high number of these businesses conducting regular transactions with foreign suppliers, – who often require wire transfer payments.

> Attacks that capitalize on the human desire to respond to urgent requests from authority are on the rise," such as Business Email Compromise (BEC) and phishing, with phishing URL detections increase by 269 percent from 2017
>
> Trend Micro

With under-reporting of such BEC attacks in the ASEAN region, it is difficult to have a clear picture of actual damages and to mount an effective and coordinated course of action against the attackers. As such, it is essential for law enforcement agencies in the region to share more detailed information on the attacks to further analyse trends and easily identify the perpetrators.

Traditionally, law enforcement organizations investigating BEC cases by following money trails is only effective to the extent of apprehending the money mules – leaving the BEC attackers at the top of the chain to continue their campaigns in the region.

Our analysis identified the following Business E-mail Compromise (BEC) scam trends:

BEC scams are not going away anytime soon. For a relatively low-tech type of financial fraud, it has proved to be a high-yield and lucrative enterprise for scammers.

Four popular e-mail services – Gmail, AOL, Yahoo! Mail, and Hotmail – are among the top 10 most abused domains for BEC scams, with Gmail and AOL bearing the brunt.

Once transferred, the defrauded money is commonly laundered through bank accounts in China.

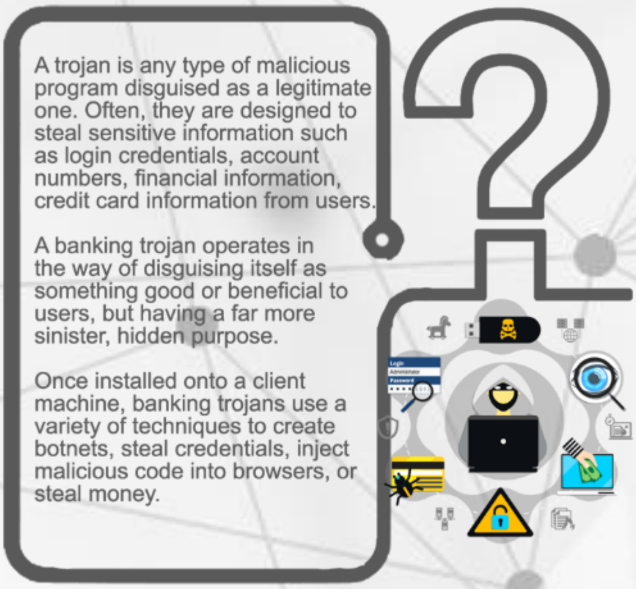
Cybercriminals who have been known for orchestrating lottery scams, romance scams and inheritance scams, now appear to be expanding their business by branching out to BEC scams.

Attackers have switched to using a targeted e-mail strategy instead of the "spray and pray" style, which proved to be more effective in convincing victims to fall into the trap.

[15] FinCEN Financial Trend Analysis (https://www.fincen.gov/sites/default/files/shared/FinCEN_Financial_Trend_Analysis_FINAL_508.pdf).

4.4 Banking malware

Compared to 2018, the first half of 2019 saw a **50 per cent increase in attacks by banking malware, especially mobile banking malware.**



A trojan is any type of malicious program disguised as a legitimate one. Often, they are designed to steal sensitive information such as login credentials, account numbers, financial information, credit card information from users.

A banking trojan operates in the way of disguising itself as something good or beneficial to users, but having a far more sinister, hidden purpose.

Once installed onto a client machine, banking trojans use a variety of techniques to create botnets, steal credentials, inject malicious code into browsers, or steal money.

Coupled with more sophisticated and effective phishing attacks, it has managed to lure online banking and banking application users to click on malicious web links which infect their mobile phones with banking malware.

The shift of prominent malware families, such as the Emotet16 banking Trojan, from banking credential theft to the distribution business, marks a significant phenomenon observed in 2019.

Malware families previously known for their single and well-functioning utility are now expanding their operations and offering upgraded capabilities.

Furthermore, new malware families are often released with more than one significant goal or attack vector. Hybrid malware that encompasses a few and often entirely different functions is a great way for cybercriminals to increase the probability of their malicious operations yielding profits.

For instance, a ransom demand is deployed together with collecting user credentials, or harvesting sensitive information for future phishing attacks. Another example is a botnet that can perform cryptocurrency mining using the bot network's CPU resources and, in parallel, utilize the same bots to distribute e-mail spam. These functions, do not have to be carried out by the same malware, though. Often, two malware developers join forces in a single campaign involving different malware strains, either to ensure revenue and success or to achieve multiple goals.

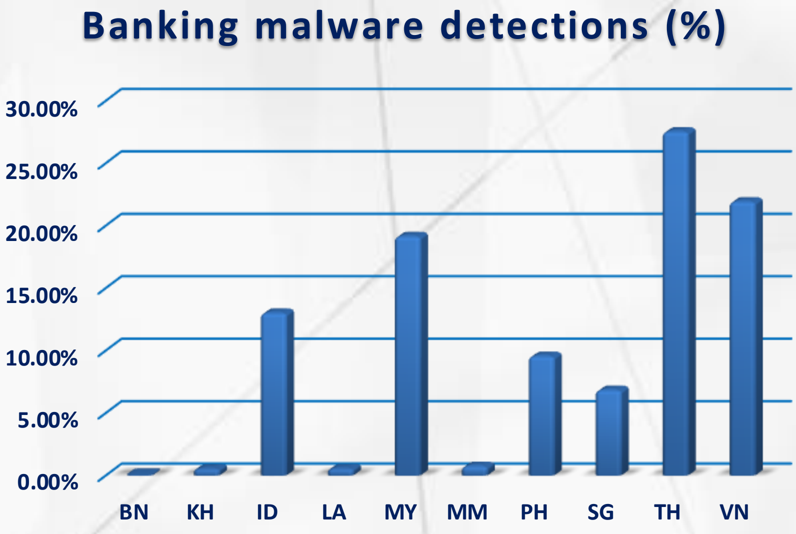


Figure 8: Banking malware detections in ASEAN countries in 2019

LokiBot is one of the top detected banking malware, targeting banking customers in the ASEAN region. It is usually delivered through spam e-mail campaigns with attachments containing the subject line, "Request for quotation".

Another banking malware variant at the top of the list targeting the region is Ramnit. It incorporates lateral movement capabilities, steals web session information, and enables the attackers to steal account credentials for all services used by the victim, including bank accounts, and corporate and social network accounts.

Other banking malwares detected in the ASEAN region are Zbot, Fareit and Emotet.

Emotet is an advanced, self-propagating and modular Trojan. Emotet functions as a banking Trojan, and is currently used to spread other malware or malicious campaigns. It uses multiple methods and persistence techniques to avoid detection. Emotet can also be spread through phishing e-mails.

With the increasing trend of banking malware, a new *mobile* banking malware trend is also entering the market.

Google Play unknowingly harbours many fake mobile applications (hereafter, "apps") posing as legitimate apps offered by real banks. Their legitimate appearance makes it extremely difficult for customers to differentiate between real and fake apps. Users are lured to download fake apps that steal their bank account and credit card information.

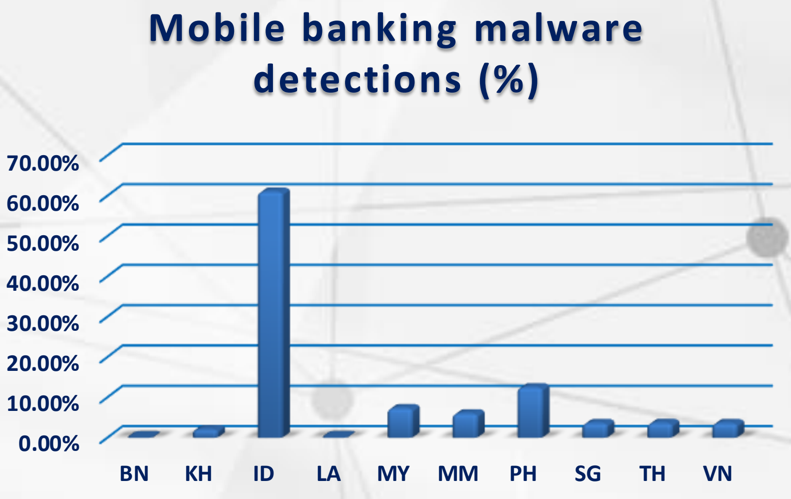


Figure 9: Mobile banking malware detections in ASEAN countries in 2019

The high incidence of mobile banking malware detections is attributable to the rapid growth of financial technology and digital banking in the region.

KPMG forecasts that the number of mobile banking users will reach 1.8 billion[16] by end of 2019 with the ASEAN region being a main driver of this development.

The top banking Trojans in **the ASEAN region are** XLoader and FakeSpy – with XLoader available in 27 languages including English, Chinese, Filipino, Malay, and Vietnamese.

Indonesia has been a key target as the country has seen exponential growth in digital banking usage and penetration. The most prevalent detected threats in Indonesia are mobile ransomware, cryptomining and mobile banking Trojans.

Mobile banking Trojans were also detected in Myanmar, the Philippines and Cambodia.

Our analysis identified the following banking malware or banking Trojan trends:

There will be more instances of hybrid malware, which demonstrate a small number of often unique functions, serving as an effective method for an attacker to guarantee illicit profits.

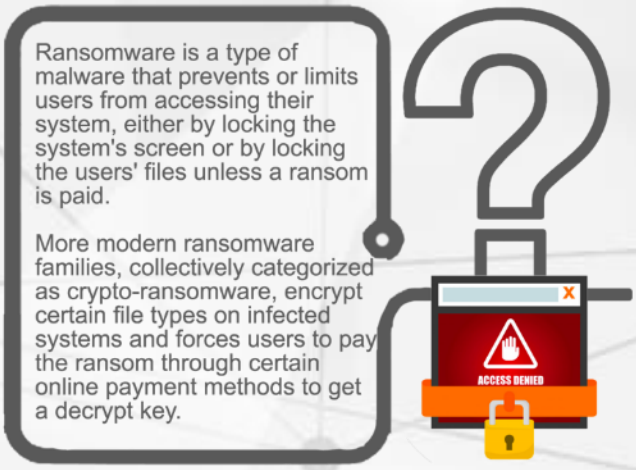
Cybercriminals have been employing techniques and methods from the general cyberthreat to the mobile platform, which includes using evasion techniques such as delayed execution to avoid sandboxes, using transparent icons with empty application labels, encrypting malicious payloads, and disabling anti-malware protection.

To avoid detection by cybersecurity vendors, cybercriminals have also included the capabilities of checking the number of running processes on the affected machine; if it detects an environment with limited processes, the malware will not proceed with its routine as it assumes that it is running in a virtual environment.

[16] Mobile Banking Users to Double by 2019 (https://home.kpmg/sg/en/home/media/press-releases/2015/09/mobile-banking-users-to-double-by-2019.html).

4.5 Ransomware

The history of ransomware starts in 1989, when malware was distributed via floppy disks. Since the Internet was not being targeted, the infection was quite limited.



Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid.

More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.

Due to the increasing popularity of cryptocurrencies, there were a lot of ransomware variants after 2013. Their development was much faster than iPhones. There were at least two to three major types of ransomware in a year, whereas Apple only launched one new iPhone annually.

In 2017, the world was surprised by the WannaCry incident because it spread to over 150 member countries during the weekend after it broke out.

This incident therefore reinforces the need to maintain vigilance of the Internet in order to remain effective in the fight against cybercrime.

After the shift to crypto-ransomware, extortion malware has continued to evolve, adding features such as countdown timers, ransom amounts that increase over time, and infection routines, which enable viruses to spread across networks and servers. The latest developments show how threat actors are experimenting with new features, such as offering alternative payment platforms to make ransom payments easier, routines that threaten to cause potentially crippling damage to non-paying victims, or new distribution methods.

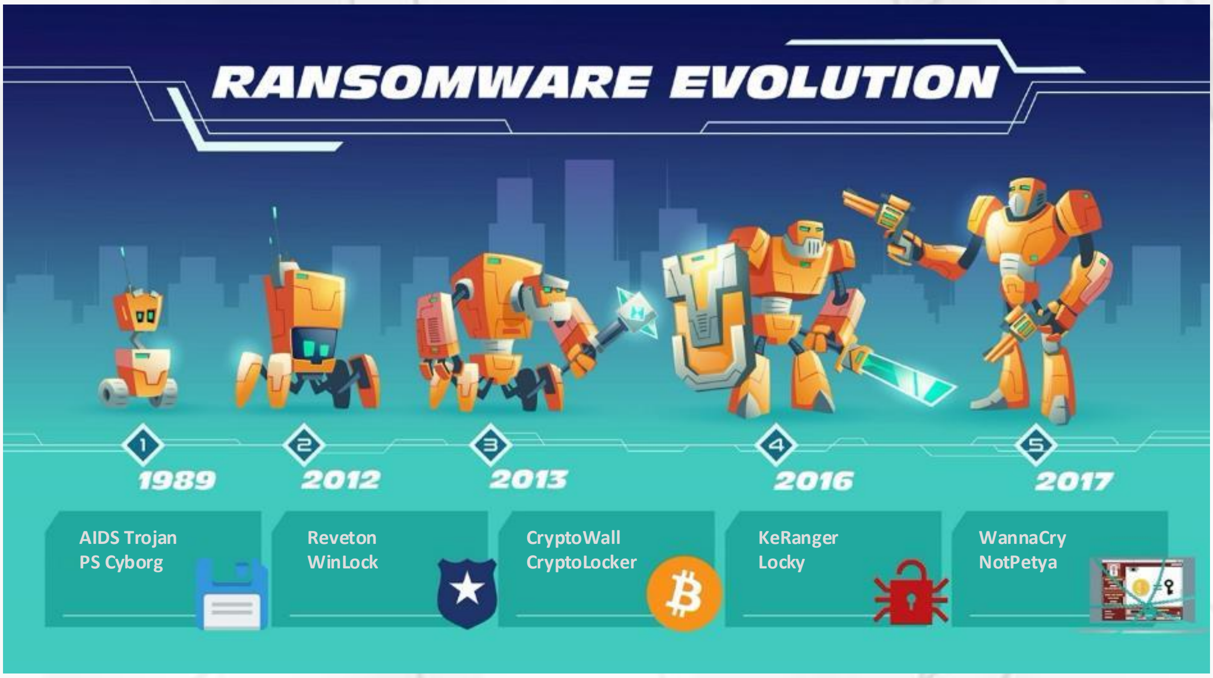


Figure 10: The evolution of ransomware

A report from the Cyber Risk Management Project, a Singapore-based initiative by organizations from the public and private sector, estimated that a major cyberattack demanding ransom payments from victims could cost USD193 billion and affect more than 600,000 businesses worldwide.

Apart from ransom payments, other costs accrue - including cyber-incident response, damage control and mitigation, business interruption, lost revenue and reduced productivity.

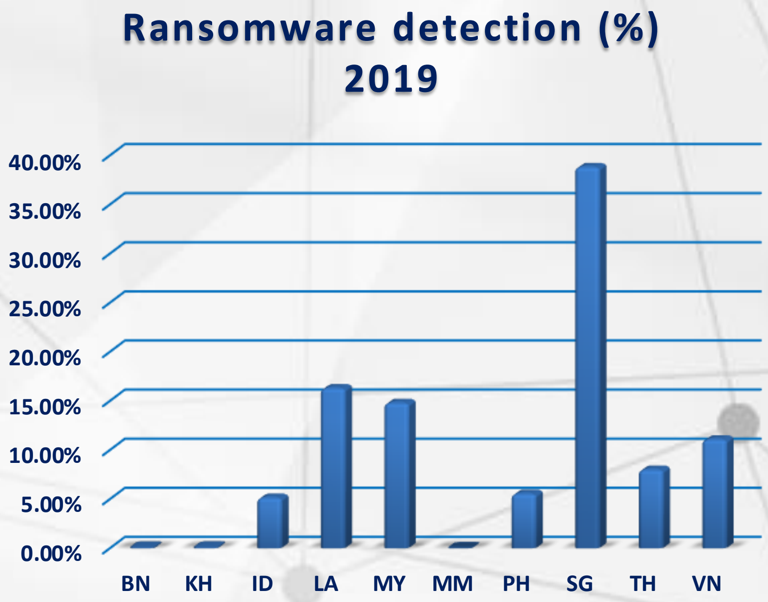


Figure 11: Ransomware detections in ASEAN countries in 2019

Singapore, being a financial services hub, experienced the highest percentage of ransomware detections in the ASEAN region in 2019, as attackers focus on following the money.

Our research shows (below) the top five ransomware families detected in the ASEAN region:

1. **Cerber (17 per cent)**
2. **WannaCry (14 per cent)**
3. **GandCrab (14 per cent)**
4. **Stop (10 per cent)**
5. **Locky (8 per cent)**

Cerber, as evolved ransomware technology, topped the number of detected ransomwares in the region.

WannaCry ranks second in the ASEAN region but first globally and continues to pose a threat after its rapid spread in 2017. Many WannaCry detections are on systems running Microsoft Windows 7, confirming that security gaps and vulnerabilities still exist despite patches being applied in 2017. Windows 7 is set to end its support in January 2020.

GandCrab sits third in the highest number of detections in the ASEAN region for the first half of 2019. In July 2019, the creators announced the ransomware would be shut down.

Our analysis identified the following ransomware trends:

In the recent trend, ransomware attacks have been targeting healthcare, education, transport and manufacturing sectors in the ASEAN region.

With the globalization of infrastructures and the increasing number of connected and centralized controls, the vulnerability to attack has increased.

Based on the latest trends, the ransomware threat will continue to grow in scale and evolve into different variants for a targeted approach.

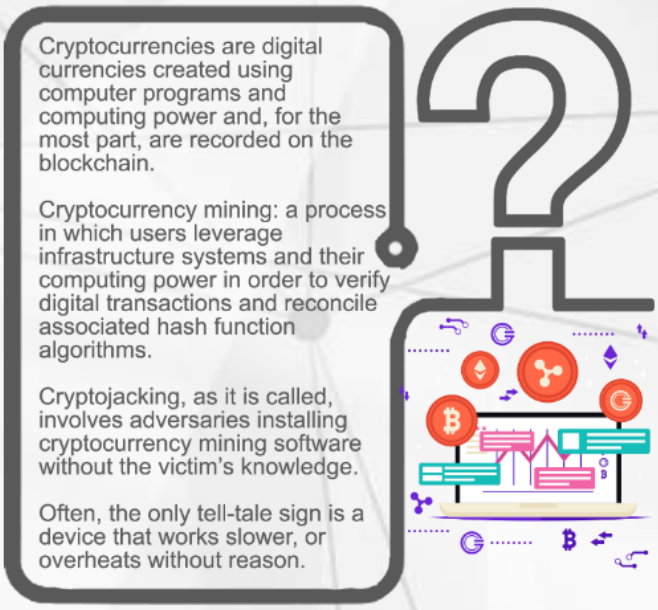
Threat actors will improve their ability to craft socially-engineered attacks against employees through their open source intelligence (OSINT) gathering, and improving their obfuscation of the malware to ensure that it cannot be detected by today’s security solutions.

Threat actors will also look to diversify targets in different industries that have critical business systems to be compromised, such as energy, critical infrastructure and distribution industries.

4.6 Cryptojacking

Cyberattacks have been evolving over the past few years, with cybercriminals employing new ideas with new technologies.

Cybercriminals have launched a new phase in achieving their main objective of financial gain. With the growing use of cryptocurrencies and the ability to harness the computer power of unknown users' systems to perform cryptojacking, businesses and individual users across the globe are at risk.



Cryptocurrencies are digital currencies created using computer programs and computing power and, for the most part, are recorded on the blockchain.

Cryptocurrency mining: a process in which users leverage infrastructure systems and their computing power in order to verify digital transactions and reconcile associated hash function algorithms.

Cryptojacking, as it is called, involves adversaries installing cryptocurrency mining software without the victim's knowledge.

Often, the only tell-tale sign is a device that works slower, or overheats without reason.

Cryptojacking surged to its peak in late 2017, when more than eight million cryptojacking activities were blocked by Symantec[17]. While this figure dropped slightly in 2018, it remains at an elevated level.

It was observed that cybercriminals have been launching their cryptojacking campaigns in the ASEAN region due to the absence of cybersecurity protection and the presence of vulnerabilities in technologies such as MikroTik routers.

As demand exceeded supplies, the value of the Bitcoin increased over several months – peaking at USD 12,000 in late June 2018 – tripling its value compared to the start of the year. With this increase came the prevalence of cryptomining in the region.

The top targeted cryptocurrency is Monero (XMR), with detections of activities in Indonesia, Philippines, Thailand and Vietnam.

Our analysis identified the following cryptojacking trends:

Cryptojacking is far from dropping off cybercriminals' radar.

Lower barriers to entry plus increasing values of cryptocurrencies, combined with the ability to stay under the radar, make cryptojacking a dream target for cybercriminals.

Coinminers' malware can run on victims' computers without them immediately being aware of their computing power being hijacked. This is one of the major appeals of cryptojacking for cybercriminals: it is a less disruptive way for the cyberthreat actors to make money compared to other cyberthreat activities.

[17] Cryptojacking: A Modern Cash Cow (https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-cryptojacking-modern-cash-cow-en.pdf).

5. INTERPOL REGIONAL CYBERCRIME STRATEGY FOR ASEAN

As underlined in the Introduction, the ASEAN region is the fastest-growing digital market in the world, with 125,000 new users accessing the Internet every day. As ASEAN seeks to fully unlock the benefits of the Fourth Industrial Revolution, digital technologies and human lifestyle factors are integrated and converging. It is projected that regional GDP will increase by USD 1 trillion over the next ten years.

Meanwhile, the impact of cybercrime is expected to increase exponentially, as cybercriminals are becoming more sophisticated, taking advantage of the borderless playing field in the digital world and the inefficiencies in law enforcement structure to tackle cybercrime.

Under the mandate of reducing the global impact of cybercrime and protecting communities for a safer world, the INTERPOL Regional Cybercrime Strategy for ASEAN (hereafter, Strategy) sets out INTERPOL's key priorities and principles in combating cybercrime in ASEAN countries. The Strategy, delivered through the ASEAN Desk and ACCDP, is underpinned by the following four pillars.

Pillar 3:
Developing regional capacity and capabilities to combat cybercrime

Pillar 4:
Promoting good cyber hygiene for a safer cyberspace

Pillar 1:
Enhancing cybercrime intelligence for effective responses

Pillar 2:
Strengthening cooperation for joint operations against cybercrime

- PILLAR I -

ENHANCING CYBERCRIME INTELLIGENCE FOR EFFECTIVE RESPONSES

The nature of cybercrime evolves rapidly, not to mention the scale and complexity in which they are perpetrated. Timely and accurate intelligence is the cornerstone of any effective law enforcement response.

In July 2018, the INTERPOL Cybercrime Directorate established the ASEAN Desk in the INTERPOL Global Complex for Innovation (IGCI), Singapore, to drive intelligence-led operations against cybercrime in the ASEAN region. As part of its mandate under the ASEAN Joint Operation against Cybercrime (AJOC), the ASEAN Desk leverages on the capabilities of the INTERPOL Cyber Fusion Centre and public private partnerships (PPP) to provide ASEAN countries with cybercrime intelligence at the strategic, operational and tactical levels.

At the strategic level, this report serves as an additional source of strategic intelligence for ASEAN's consideration during the formulation of policies pertaining to cybercrime. This report also serves as a basis for the ASEAN Desk to determine its operational priorities in year 2020.

At the operational and tactical level, the ASEAN Desk disseminated Cyber Activity Reports (CARs) to ASEAN from July 2018 to the end of 2019, providing operational and tactical intelligence on cyberthreats pertaining to malware infections, Business E-mail Compromise (BEC) frauds, cryptojacking campaigns, and web skimming attacks.

- PILLAR II -

STRENGTHENING COOPERATION FOR JOINT OPERATIONS AGAINST CYBERCRIME

The borderless nature of cybercrime, coupled with jurisdictional limits of traditional law-enforcement approaches, present immense challenges to cybercrime investigations and related operations. The ASEAN Desk aims to address these challenges through strengthening both intra-regional and inter-regional law enforcement cooperation. In addition, ASEAN countries benefit from INTERPOL's PPP, as private partners can be brought in to provide expertise on specific topics in joint operations coordinated by the ASEAN Desk.

In June 2019, the ASEAN Desk organised Operation Goldfish (Alpha), a three-day operational meeting in Singapore, to address the cyberthreat to ASEAN posed by a global cryptojacking campaign targeting routers. The meeting brought together representatives from law enforcement, Computer Emergency Response Teams (CERTs) and INTERPOL's private partners to formulate a joint operational plan to reduce the impact of cryptojacking and protect communities in the ASEAN region. The concept, which focused on prevention and mitigation efforts in ASEAN countries, was conceived during the meeting. At the end of the three-month joint operation, the ASEAN region saw a 76.6 per cent decrease in compromised routers (from22,063 to 5,167).

ASEAN Cybercrime Operations Desk:

In support of the efforts by member countries in the ASEAN region to combat cybercrime more effectively, INTERPOL launched the ASEAN Cybercrime Operations Desk in July 2018 to drive intelligence-led and coordinated actions against cybercrime through the implementation of a harmonized regional coordination framework. With cybercrime a growing threat across the region, the ASEAN Desk assists law enforcement agencies in the region to enhance their ability to combat cybercrime through intelligence development, investigative support and operational coordination. By turning information gathered from member countries and private partners into actionable intelligence, the project helps better position police in Southeast Asia to face the latest cyberthreats. When investigations lead to on-the-ground action against cybercriminals, the ASEAN Desk develops plans for multi-jurisdictional operations and coordinates joint actions against cybercrime.

- PILLAR III -

DEVELOPING REGIONAL CAPACITY AND CAPABILITIES TO COMBAT CYBERCRIME

With the cybercriminals' ever-evolving creativity, and the emergence of new cyberattack methodologies, it is critical for law enforcement agencies to keep pace and be prepared. Initiated in 2016, the ACCDP is a multiphase project that strengthens the capacity and capabilities of ASEAN countries to combat cybercrime effective and efficiently. The ACCDP also fosters regional strategic discussion, identifies trends and provides a foundation for improved information exchange.

From 2016 to 2019, the ACCDP coordinated 15 training sessions and related meetings, bringing together more than 350 participants from ASEAN countries and more than 50 trainers and expert speakers from all over the world. Practical training made up an important part of the project and covered topics including digital forensics, malware analysis, cyber investigations and the Darknet. As a result, participants improved their capabilities in data extraction and interpretation as well as cybersecurity and online investigations.

As part of ACCDP, ten National Cyber Reviews (NCRs) were carried out on ASEAN countries, providing a comprehensive assessment of each country's capability to prevent, detect and investigate cybercrime. Following the review, a tailored report was produced for each country, outlining recommendations for enhancing the existing institutional, operational, legal and technical frameworks.

- PILLAR IV -

PROMOTING GOOD CYBER HYGIENE FOR A SAFER CYBERSPACE

Given the exponential increase in the number of cybercrimes, enforcement by itself is an inadequate solution; prevention is the key. The ASEAN Desk seeks to promote good cyber hygiene in ASEAN countries, empowering the communities to stay safe and prevent themselves from becoming victims of cybercrime.

As part of Operation Goldfish (Alpha) coordinated by ASEAN Desk, the National Cyber Security Center of Myanmar formulated a set of good cyber hygiene guidelines to address the threat of cryptojacking. Supporting the operation, one of the INTERPOL's private partners, TrendMicro, also developed a set of technical advice to inform the public on how to patch the vulnerability and prevent their routers from future malware infections.

6. THE WAY FORWARD: ACTIONS AGAINST CYBERTHREATS IN THE ASEAN REGION

In this report, we have explored various types of cyberthreat trends that are affecting ASEAN countries. A critical issue surrounding these cyberthreats is that many syndicates are engaging the services of individuals or groups - which now operate a "fee for service" crime model, charging anywhere from USD40 to generate 20,000 spam e-mails or USD10,000 to develop crimeware.

Furthermore, it is evident that cybercriminals are using the dark Web as a secured space to operate anonymously and without regulation. There are significantly fewer barriers compared to the open web, and there is more to gain by stealing digital goods –employee login credentials, corporate data, source codes, credit cards, and other corporate assets – than by dealing in traditional prohibited goods, such as firearms and drugs.

Common cyberstrategies focus mainly on reactive measures in preventing cyberattacks such as ransomware, phishing, DDoS, and malware attacks. However, due to the fact that cybercriminals primarily operate, sell and share knowledge on the dark Web, law enforcement agencies and corporate cybersecurity teams must widen their focus and be proactive in collecting and analysing external threat intelligence, seeking out threats before they manifest into attacks.

In this context, and looking ahead, the ASEAN Desk will focus on meaningful operational delivery in line with its Strategy, as detailed below.

- **ENHANCING CYBERCRIME INTELLIGENCE FOR EFFECTIVE RESPONSES TO CYBERCRIME**
  Benefiting from the Project Gateway framework that enables the INTERPOL Cybercrime Directorate to have data-sharing agreements with private entities, the ASEAN Desk will further develop its understanding of the cybercrime landscape to better assist ASEAN countries. The Cyber Analytical Platform to be launched in the coming months will also enhance its cyber intelligence capability to provide more accurate and timely intelligence and analysis.

- **STRENGTHENING COOPERATION FOR JOINT OPERATIONS AGAINST CYBERCRIME**
  In close cooperation with private partners and CERT communities, the ASEAN Desk will conduct and coordinate more operational activities in 2020 reflecting the unique challenges and needs within the ASEAN region.

- **DEVELOPING REGIONAL CAPACITY AND CAPABILITIES TO COMBAT CYBERCRIME**
  Maximising the expertise of our private partners, we will continue to support member countries in ASEAN in terms of cyber skills, technology and capabilities development. The ACCDP has initiated its second phase which aims to develop a cybercrime strategy guidebook; create e-learning modules for first responders; and deliver specialised cybercrime trainings for law enforcement and judicial authorities.

- **PROMOTING GOOD CYBER HYGIENE FOR A SAFER CYBERSPACE**
  Building on the experiences in running the global BEC awareness campaign, the ASEAN Desk will support the next global awareness campaign in 2020 to reduce the impact of cybercrime in the region through awareness raising and preventive measures.

In today’s highly digitalised world, the sooner countries are aware of a threat, the sooner they can take steps to mitigate the risk and neutralise the cyberthreats coming in their direction.

To this end, collective efforts from law enforcement agencies need to be enhanced, particularly in the sharing of intelligence and the formulation of a joint operation framework to effectively tackle cybercrime. The ASEAN Desk stands ready to support member countries in ASEAN in reducing the global impact of cybercrime and protecting communities for a safer world.

ABOUT INTERPOL

INTERPOL is the world's largest international police organization. Its role is to assist law enforcement agencies in the Organization's 194 member countries to combat all forms of transnational crime. It works to help police across the world to meet the growing challenges of crime in the 21st century by providing a high-tech infrastructure of technical and operational support. The Organization's services include targeted training, expert investigative support, specialized databases and secure police communications channels

INTERPOL's VISION: "CONNECTING POLICE FOR A SAFER WORLD"

INTERPOL's vision is that of a world where each and every law enforcement professional will be able to use the Organization to securely communicate, share and access vital police information whenever and wherever needed, to ensure the safety of the world's citizens. INTERPOL constantly provides and promotes innovative and cutting-edge solutions to global challenges in policing and security

INTERPOL

INTERPOL Global Complex for Innovation
18 Napier Road
Singapore 258510

Twitter: @INTERPOL_Cyber
YouTube: INTERPOLHQ

www.interpol.int