INTERPOL

ASEAN CYBERTHREAT ASSESSMENT 2021

KEY CYBERTHREAT TRENDS OUTLOOK FROM THE ASEAN CYBERCRIME OPERATIONS DESK

This page intentionally left blank

CONTENTS

LEGAL DISCLAIMER

This page intentionally left blank

FOREWORD

Today, technology — especially the Internet — is intrinsic to our daily lives; we use it to control critical infrastructures, conduct financial transactions, manage travel networks, communicate with one another, shop, and entertain ourselves.

Without it, governments and business would have to profoundly change how they operate, and our daily lives would be unrecognisable.

Before 2020, many countries were still in the process of transforming into digital economies and becoming smart nations.

The COVID-19 pandemic has accelerated the digital transformation and is forcing both public and private sectors into digitalization, changing the ways that we work, learn, shop, and bank.

By accelerating digital transformation, it has also given cybercriminals new opportunities to attack the computer networks and systems of individuals, businesses and even global organizations. Digital and physical vulnerabilities may increase in the hardware and software environments due to rise in connectivity between businesses and their employees, working and connecting from home, giving the cybercriminal larger attack surfaces to target.

Cybercrime today is not the same as yesterday, and it will also not be the same as tomorrow. There will always be new hybrids of cybercrime methodologies emerging.

Indeed, the lines between physical and online worlds have blurred, creating an environment in which they are almost inseparable.

When securing a city, a hospital, or a bank, we can no longer only talk about controlling the movement of people in, out and around them. Criminals are able to enter unseen and undetected, or lock you out of your systems or networks never leaving the safety of their own home or country.

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 second edition of the ASEAN Cyberthreat Assessment produced by the ASEAN Cybercrime Operations Desk, or in short, the ASEAN Desk. This report provides analysis and insights on the latest cyberthreat landscape faced by ASEAN member countries. With the aim of protecting digital economies and communities in ASEAN, the report also highlights strategies and the proposed way forward for law enforcement communities in the region.

In addition to cyberthreats such as ransomware, phishing and Remote Access Trojan malware, different types of cyber frauds are highlighted in this report as the latter, in particular, presents a persistent problem to the ASEAN region. 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 actions and coordinating a joint operation codenamed Killer Bee.

With a good understanding of the unique challenges and needs of ASEAN, the increased operational support and sharing of proactive intelligence by the ASEAN Desk will better support member countries in the region.

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 of Cybercrime
INTERPOL

ABBREVIATIONS AND ACRONYMS

AAR	After-Action Review
ACCDP	ASEAN Cyber Capacity Development Project
ACTA	ASEAN Cyberthreat Assessment
AJOC	ASEAN Joint Operations against Cybercrime
AMS	ASEAN Member States
ASEAN	Association of Southeast Asian Nations
ASEAN Desk	INTERPOL ASEAN Cybercrime Operations Desk
ASEC	ASEAN Secretariat
BEC	Business E-mail Compromise
CaaS	Crimeware-as-a-Service
CARs	Cyber Activity Reports
CERTs	Computer Emergency Response Teams
CII	Critical Information Infrastructure
CnC/C2	Command-and-Control server
DDoS	Distributed Denial-of-Service
DNS	Domain Name System
EU	European Union
FBI	Federal Bureau of Investigation
HTTPS	Hypertext Transfer Protocol Secure
IC3	Internet Crime Complaint Center
IGCI	INTERPOL Global Complex for Innovation
IoT	Internet of Things
IP	Internet Protocol
IRC	Internet Relay Chat
ITRC	Identity Theft Resource Center
JAIF	Japan-ASEAN Integration Fund
OSINT	Open-Source Intelligence
P2P	Peer-to-peer
PhaaS	Phishing-as-a-Service
POS	Point-of-sale
PPP	Public private partnership
RaaS	Ransomware-as-a-Service
RAT	Remote access tool
SMEs	Small and medium-sized enterprises
SSL	Secure Sockets Layer
STPs	Standard tactical plans

ACKNOWLEDGEMENT

This assessment report has been written by the ASEAN Desk within the framework of INTERPOL's ASEAN Joint Operations against Cybercrime (AJOC) funded by the Japan-ASEAN Integration Fund 2.0, through the ASEAN Secretariat (ASEC) with the Ministry of Home Affairs of Singapore as the project proponent.

James Tan

Head of the ASEAN Cybercrime Operations Desk

TEE Wei Xian

Specialized Officer

Adam Parsons

Cybercrime Intelligence Officer

Alyssa Radlett

Project Manager, ASEAN Joint Operations against Cybercrime

This report provides INTERPOL member countries with an indication of the cyberthreat landscape in the ASEAN region.

This report is the result of the assessment of the information made available to INTERPOL by the relevant member countries and by INTERPOL's Project Gateway partners which include the Cyber Defense Institute, Group-IB, Kaspersky, and Trend Micro.

EXECUTIVE SUMMARY

The globalized world, with growing economies and fast-evolving technology, poses an increasing threat to a multitude of actors – governments, businesses, and citizens. Today, anyone is a potential victim of cybercrime.

Cybercriminals use globalized Information Communication Technology to commit cybercrime, unrestrained by geographical boundaries and causing an enormous impact on the global economy. Cybersecurity experts project the total net cost of cybercrime to grow by 15 per cent per year over the next five years, reaching USD 10.5 trillion annually by 2025, up from USD 3 trillion in 2015.[1]

A report published by the International Monetary Fund stated that cyber risks are the "new threat to financial stability" and called for help to develop cybersecurity capacity in low-income countries.[2]

Cybercrime has become a multi-billion-dollar industry, and the profits are appealing to traditional crime syndicates interested in diversifying their criminal activities by including use of the virtual ecosystem for communication and money exchange, but also for committing cybercrime.

One increasingly prevalent transnational cybercrime which does not require any sophisticated technical skill, but which causes victims huge monetary loss, is Business E-mail Compromise (BEC).

In the United States of America alone, almost half of the reported losses received by the FBI's Internet Crime Complaint Center (IC3) in 2019 – an estimated USD 1.77 billion – were generated by BEC.[3]

In 2020, the COVID-19 pandemic did not only accelerate the digital transformation of countries, but also created a surge in malicious cybercrime. Capitalizing on the coronavirus to steal personal information and credentials, cybercriminals gained access to networks which they then exploited for financial gain.

Cybercriminals have also taken advantage of the fact that more people accessed the Internet with mobile devices (that are often left unprotected) to enable remote working, shopping and transactions in the wake of COVID-19. This made users vulnerable to becoming targeted because attackers were taking a more customized approach and targeting specific geographical areas, industries and businesses and were also taking advantage of the desire for more COVID-related information.

Notwithstanding the impact that the COVID-19 pandemic has had on our cyberthreat landscape, the volume of cybercrime has always shown an upward trend and will continue to rise exponentially in the future. This is due to a range of drivers, but is also facilitated through Crimeware-as-a-Service (CaaS) that puts cybercriminal tools and services in the hands of a wider range of threat actors – even the non-technical, and as such, anyone can become a cybercriminal with minimal investment.

Cybercriminals are in fact more organized than many would expect as they share resources and expertise to their advantage. In order to counter cybercriminals more effectively both today and in the future, the public and private sectors need to work together closely to share information and expertise to counter the increasing threats posed by cybercrime and, as such, INTERPOL strives to connect the dots and facilitate collaboration between law enforcement agencies and the private sector by sharing proactive intelligence and expertise.

The ability to access information causes a redistribution of power from the powerless to the powerful. It is therefore crucial for law enforcement agencies to stay ahead of criminals by understanding new trends and responding with innovative solutions.

---

1 Globenewswire (https://www.globenewswire.com/news-release/2020/11/18/2129432/0/en/Cybercrime-To-Cost-The-World-10-5-Trillion-Annually-By-2025.html)

2 IMF (https://blogs.imf.org/2020/12/07/cyber-risk-is-the-new-threat-to-financial-stability/)

3 FBI (https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120)

With data drawn from INTERPOL's member countries and private partners, and research conducted by the ASEAN Desk, this report provides a comprehensive analysis of the cyberthreat landscape in the ASEAN region. This report has identified the following as some of the more prominent cyberthreats in 2020 and beyond:

- **Business E-mail Compromise** campaigns continue to top the chart with businesses suffering major losses, as it is a high-return investment at a low cost and risk. Data drawn from our private partners show that the use of information stealers has been declining over the last couple of years, but comparatively, the use of Remote Access Trojans has been growing. This shift suggests, among other reasons, that the cybercriminals behind BEC are becoming more sophisticated, technically proficient and able to leverage different types of tools to achieve their aims.

- **Phishing**. Cybercriminals are exploiting the widespread use of global communications on COVID-19-related information to deceive unsuspecting victims. Malware, spyware and Trojans have been found to be embedded in interactive COVID-19 maps and websites. There was a rise in the number of spam e-mails which deceive users into clicking on links that download malware onto their computers or mobile devices.

- **Ransomware.** The number of cybercriminals targeting hospitals, medical centres and public institutions for ransomware attacks increased rapidly. Cybercriminals believe that there will be a higher success rate given the current medical crisis in many countries. Other critical infrastructures, including the energy sector, are not spared.

- **E-commerce data interception** poses an emerging and imminent threat to online shoppers and can easily obtain various different commodities, which lowers consumer confidence in the security of online payments. Different kinds of malware, such as JS-sniffers in the underground forum, not only enable cybercriminals to launch malicious campaigns against e-commerce platforms with ease, but evolving functionalities also make it even more challenging to detect and investigate.

- **Crimeware-as-a-Service** (CaaS) is any computer program or set of programs designed to facilitate illegal activity online. Spyware, phishing kits, browser hijackers, keyloggers and more, are all available to attackers through CaaS.

- **Cyber scams.** Cybercriminals have been capitalizing on people's anxiety and countries' economic recessions brought about by the pandemic. With the increase in online transactions and as more people have to work from home, cybercriminals have revised their online scams and phishing schemes with phishing e-mails about COVID-19, some of which even impersonate government and health authorities to lure victims into providing their personal information and downloading malicious content.

- **Cryptojacking** continues to be used by cybercriminals. The price increase in cryptocurrency, coupled with the ubiquitous increase in the number of Internet of Things (IoT) devices, provide cybercriminals with a greater attack surface from which to launch their cryptojacking campaigns. They exploit the increasing number of vulnerabilities with evolved tactics and advanced mining malware to achieve maximum illicit gains.

With a mandate to reduce the global impact of cybercrime, protect communities and connect police for a safer world, INTERPOL's Regional Cybercrime Strategy for ASEAN sets out the Organization's key priorities and principles in combating cybercrime in ASEAN countries. The Strategy, delivered through the ASEAN Desk and the ASEAN Cyber Capacity Development Project (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 joint action against cyberthreats in the ASEAN region.

1. Current developments in Southeast Asia

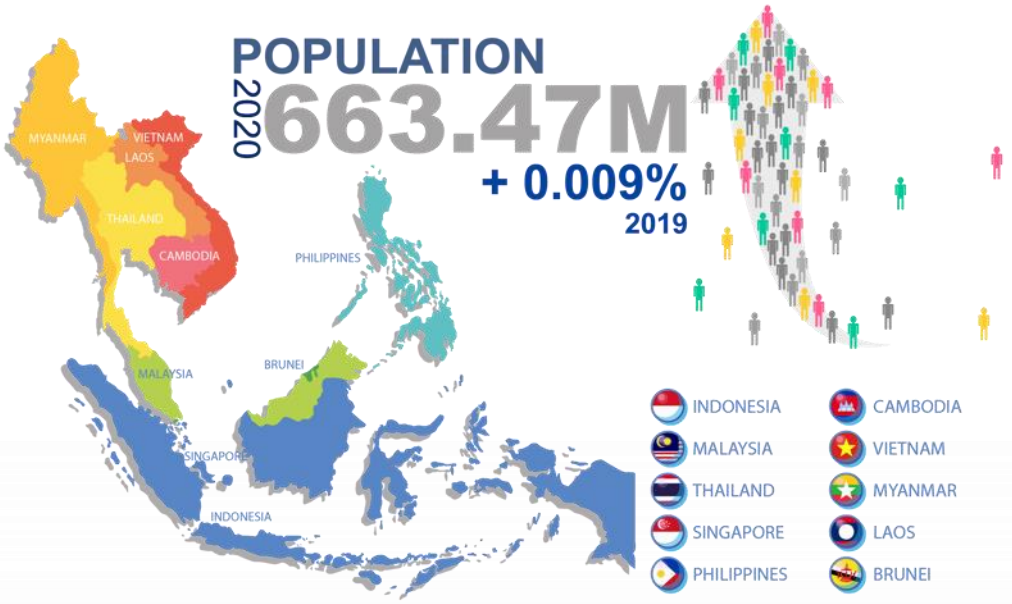

Figure 1: Population *(millions)*

The ASEAN region, home to abundant natural resources, is one of the world's largest producers of agricultural goods. Today, the region is a thriving hub for global manufacturing and trade. Notwithstanding income inequality, citizens of ASEAN member countries have generally become more affluent with rising GDP[4] in each country over the last two decades with combined regional GDP more than quintupled, from USD 613.551 billion in 2000 up to USD 3.11 trillion in 2020.

The agricultural, industrial, manufacturing, export and service sectors are the main contributors to the rising GDP. However, with ASEAN focusing on economic initiatives driven by digital technology and innovation-related industries, the electronics and technology sectors (industrial robots, cloud computing, big data analytics, Software-as-a-Service (SaaS), social media applications, and the Internet of Things, etc.) are also emerging as strong contributors. Digital technology will continue to expand as economies mature.

With a combined GDP of more than USD 3.11 trillion, the ASEAN region is the world's seventh largest market. It is predicted that the region's combined GDP will exceed USD 4 trillion by 2022. The ASEAN region has a total population of 663.47 million, which makes it the world's third most populous market.

Figure *2*: GDP, current *(billions)*

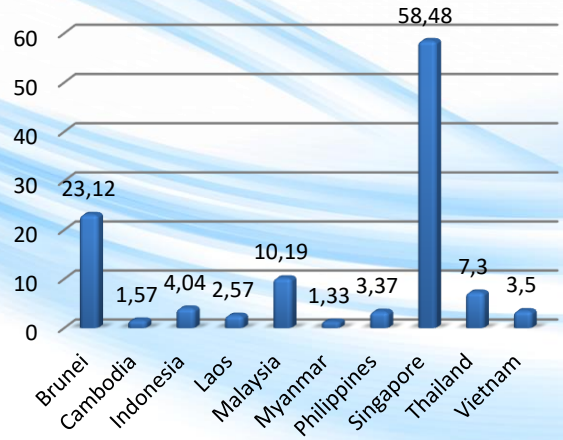

Figure *3*: GDP per capita, USD *(thousands)*

[4] GDP (current) in USD. Source: International Monetary Fund.

Internet penetration in Southeast Asia is relatively high compared to global rates.

According to the 2020 Global Digital Report,[5] the average Internet penetration rate in Southeast Asia is about 66 per cent. It has been growing rapidly over the past few years and shows no signs of slowing down. At the higher end of the spectrum, the Internet penetration rate is 95 per cent in Brunei; 88 per cent in Singapore; 83 per cent in Malaysia; 75 per cent in Thailand; 70 per cent in Vietnam; 67 per cent in the Philippines; and 64 per cent in Indonesia. At the lower end of the spectrum, in Laos and Myanmar, the penetration rate is 43 per cent and 41 per cent respectively.

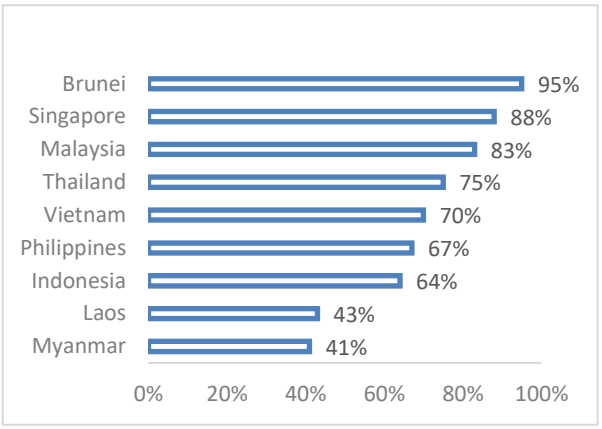

Figure *4*: Internet penetration (%)

Indonesia and Cambodia have the highest absolute growth in the region, each with a 17 per cent and 15 per cent increase in users. Users in the Philippines and Thailand spent the most amount of time per day on the Internet: between nine and 10 hours.

On a separate note, average social media penetration in Southeast Asia is about 63 per cent.

With the ASEAN region seeing exponential growth in the digital technology sector, particularly financial technology and e-commerce, there is an increasing demand for Internet and broadband services. In terms of the competitive landscape, the region is considered to be one of the most competitive markets in the world, where global investors predominate.

However, this increasing reliance on the Internet has created a large number of security threats that can cause immense damage. It impedes trust and resilience in the digital economy, which will prevent the region from realizing its full digital potential if nothing is done. Criminal networks 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 more malicious threats today.

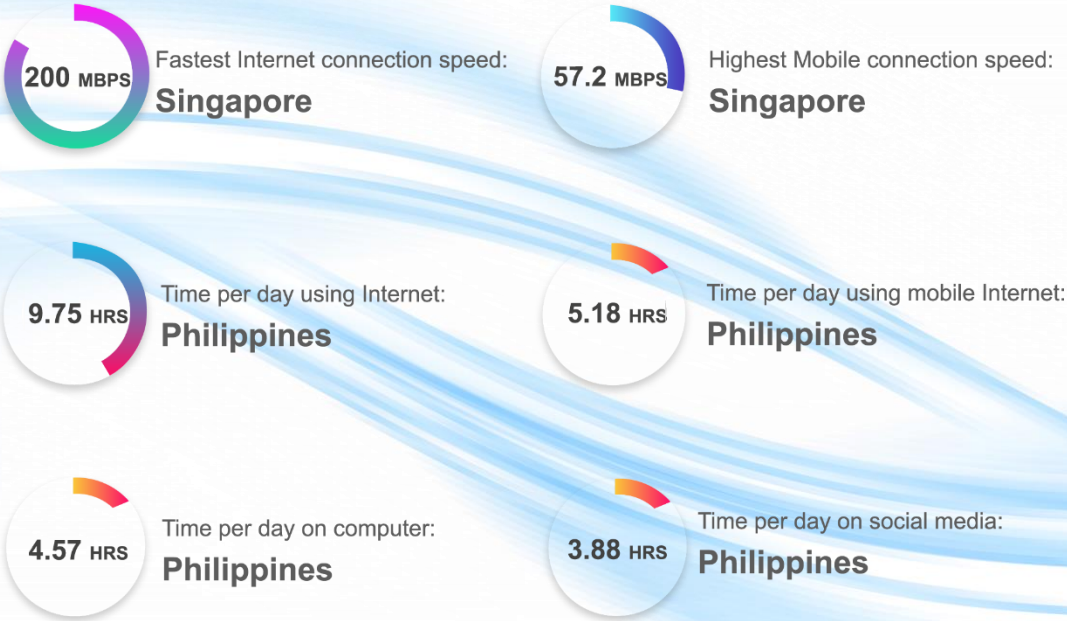

Figure *5*: Internet speed, time using the Internet

[5] 2020 Digital Global Report (www.wearesocial.com).

2. Significant Cyber Incidents in 2020

The year 2020 was both challenging and unpredictable. It was a year when society restructured people's daily lives, work, shopping and schooling. The COVID-19 pandemic has led governments and businesses to speed up digital transformation. Although this transition has its benefits and will bring immense potential in the long run, cybercriminals are quick to exploit the situation to their advantage.

The year 2020 was also yet another wake-up call for many to invest in securing their cyberspace. While many businesses are being heavily impacted by the pandemic, cyber incidents also lead to huge financial losses due to the loss of business activity and the hefty fines imposed by government regulatory bodies for failing to protect data, which may put companies out of business. Even so, cyberattacks have resulted in negative impacts on individuals and even nations, ranging from threats to life, depression, regulatory fines or disruption to daily activities. Cyberattacks and data breaches have been ranked among the critical risks to economic development. On average, the cost of a data breach is USD 3.86 million, and the average time to identify and contain a breach is about 280 days.[6]

Ransomware continues to plague businesses and consumers, with indiscriminate campaigns pushing out significant volumes of malicious e-mails.

In the past, cybercriminals have targeted various industries, especially the oil, energy, and e-commerce sectors, from which they have gained huge financial benefits. In 2020, the healthcare industry became the main focus, with cybercriminals targeting system vulnerabilities in hospitals, healthcare centres, vaccine manufacturers and laboratories for which they demanded a ransom.

It is undeniable that cyberattacks against critical infrastructure are becoming one of the fastest-growing forms of cybercrime with the globalization of infrastructures and the increasing number of connected and centralized control systems.

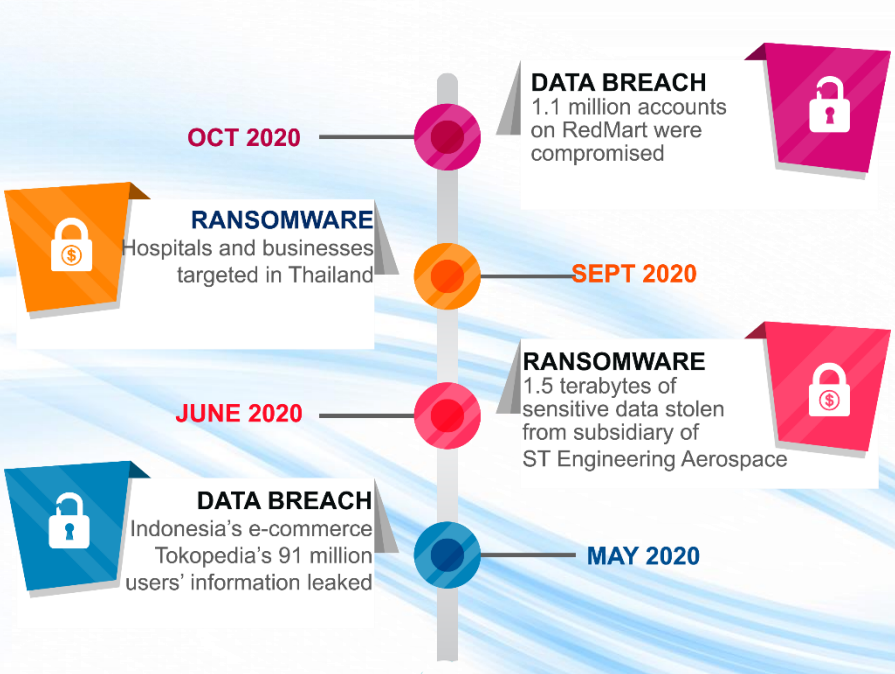

Figure *6*: Major known cyber incidents in 2020

The impact of cyberattacks on critical infrastructure does not only cause loss to the nation's economy; it actually erodes public confidence in critical services as well as in the government.

Cyberattacks also cause disruption to national or global economic systems and stability, thus presenting one of the most serious national security challenges.

Some of the most serious data breach incidents which occurred in the ASEAN region in 2020 are shown in Figure 6.

Besides the cyberattacks and data breaches, there is also an increase in COVID-19-related online fraud, including the sale of medical equipment and personal protective equipment.

Compared with 2019, there is a marked increase in the number of online scammers who are impersonating government officials from the Ministry of Health and other agencies, chiefs of police and other notable officials to obtain people's confidential details by fraudulent means.

6 IBM (https://www.ibm.com/sg-en/security/data-breach).

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, ASEAN member countries have become a prime target for cyberattacks.

3. INSIGHT INTO CYBERTHREAT TRENDS: 2020

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

The ASEAN Desk identified some of the prominent cyberthreats in 2020 and the continuing trends facing ASEAN member countries.

Business E-mail Compromise (BEC)

BEC is a type of scam which targets companies that conduct wire transfers and have suppliers in a foreign country or countries. Corporate or publicly available e-mail accounts of executives, or high-level employees involved in finance, or those involved in wire transfer payments, are either spoofed or compromised through keyloggers or phishing attacks to carry out fraudulent transfers, which result in hundreds of thousands of dollars in losses.

Phishing

Phishing is a form of identity theft in which a scammer uses an authentic-looking e-mail from a legitimate business to trick recipients into giving out sensitive personal information, such as a credit card, bank account, or Social Security number(s). The spoofed e-mail urges recipients to click on a link to update their personal profiles or carry out some transactions. The link then takes the victims to a fake website where any personal or financial information entered is routed directly to the scammer.

Ransomware

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, encrypts certain file types on infected systems and forces users to pay the ransom through certain online payment methods to obtain a decryption key.

E-commerce data interception

E-commerce data interception is a type of malware designed to steal customer payment data from online stores.

The online equivalent of a credit card skimmer targeting ATM cash machines, a JS-sniffer typically comes in the form of malicious codes that cybercriminals inject into websites to capture users' data, such as payment card numbers, names, addresses, and passwords.

Crimeware-as-a-Service

Crimeware-as-a-service, or CaaS, is any computer program or set of programs that are designed to facilitate illegal activity online. Spyware, phishing kits, browser hijackers, keyloggers and more are all available to attackers through CaaS.

Cyber fraud

Cyber fraud is the most common and threatening form of fraud which is perpetrated internationally. Cyber fraud can be considered as any fraudulent crime which is conducted via a computer or computer data.

3.1 Business E-mail Compromise

Business E-mail Compromise (BEC) is a classic example of a cybercrime which does not require any sophisticated technical skill to cause victims huge monetary loss. There are several ways to orchestrate BEC, but they usually involve the following:

- intelligence gathering;
- unauthorized access to e-mail accounts of a company or its executives;
- leveraging information obtained from e-mails to launch skilful social engineering attacks;
- document forgery;
- complex money-laundering services.

There are many variants of BEC and there is no unique name for this type of crime, which is also commonly referred to as “business e-mail scams”; “business e-mail fraud”; or simply “e-mail fraud”. Note that these names do not address the e-mail compromise that enables the fraud.

As more businesses go online, cybercriminals have more opportunities to launch BEC attacks and other forms of cybercrime. Cybercriminals are also adept at changing their social engineering schemes to reflect current events. As business enterprises are the primary targets for such scams, they need to be vigilant and to take precautionary measures to guard against BEC attacks.

Cybercriminals typically target specific individuals or departments within an organization. E-mail addresses are often spoofed or taken over through other methods such as malware. E-mails which appear to be from a senior individual within the company, or from a customer or supplier, are then sent to an employee asking him or her to transfer funds to a given bank account.

The threat posed to the ASEAN region is not only financial, but also involves the potential loss of confidential or customer information and the resultant reputational damage that can follow.

Figure 7: Five types of BEC (illustration by Trend Micro)

While the industrial, manufacturing, oil and energy, and export sectors are the main GDP contributors in ASEAN, this also make businesses in the region the prime target for BEC.

According to the 2019 FBI Internet Crime Report,[7] losses from BEC have risen rapidly in recent years, causing a staggering USD 1.7 billion in cybercrime-related financial losses in the US in 2019. This amount is nearly four times as much as the losses generated by any other category of cybercrime and 37 per cent higher than the previous year.

There are varying estimates as to the cost to businesses and individuals. One estimate puts the cost to small and medium-sized businesses at between USD 50 000 and USD 100 000.

In most instances, as part of BEC, businesses and individuals' machines are infected with information stealers or Remote Access Tools (RATs).

While cybercriminals still prefer to use information-stealing malware for carrying out fraudulent e-mail attacks, the shift towards RATs is now visible.

RATs allow cybercriminals to examine local files, acquire log-in credentials and other personal information, or use the connection to download viruses that could unwittingly spread to other machines. A RAT paired with an information stealer such as a keylogger, for instance, allows cybercriminals to easily acquire log-in information for bank and credit card accounts.

As part of the social engineering process, the whole purpose of information stealers or RATs in BEC, is to enable cybercriminals to acquire details of the company's business processes and its communications with counterparts in order to issue instructions, or divert funds away from the legitimate business purpose.

The common strains of information-stealing malware used in BEC campaigns are: AgentTesla; AzoRult; KeyBase; LokiBot; Pony; PredatorPain; and Zeus.

The RATs used in BEC scams are formed by: NetWire; DarkComet; NanoCore; LuminosityLink; Remcos; ImminentMonitor; NJRat; Quasar; Adwind; and Hworm.

Business E-mail Compromise has a huge financial impact on businesses. The reported losses from BEC attacks are much higher than for any other category of cybercrime. Furthermore, there are signs that attackers are, once again, focusing their efforts on ransomware.

The trend of BEC campaigns is expected to increase exponentially as more and more businesses undergo digital transformation. More business information is being shared online in an effort to expand business opportunities; however, this also draws attention and enables cybercriminals to be more effective in orchestrating their BEC attacks.

Cybercriminals are shifting their attention and focusing on cyberattacks that require log-in credentials and passwords to gain access to corporate networks for BEC fraud. These attacks require less effort and are largely automated, with a low risk of detection and being caught whilst having much higher returns compared to taking over an individual's account.

The use of information stealers has been declining over the past few years, but the use of RATs has been growing. This shift also shows that the cybercriminals behind BEC fraud are becoming more sophisticated and highly technical in leveraging the tools that help to accomplish fraud.

INTERPOL analysis identified above BEC trends

[7] Internet Crime Report (www.ic3.gov).

3.2 Phishing

Phishing is not a new cyberthreat, nor is it decreasing. Instead, it is considered the most prevalent cyberthreat for stealing credentials and has been pivoting towards other forms of cybercrime, such as data breach.

It is reported that the total number of phishing sites detected in the second quarter of 2020 was 146 994.[8] It was found that SaaS and webmail sites remained the biggest targets for phishing, with more than 35 per cent of all attacks. Attacks targeting the social media sector increased by 20 per cent in the second quarter over the first quarter, and were primarily driven by attacks targeted against Facebook and WhatsApp.

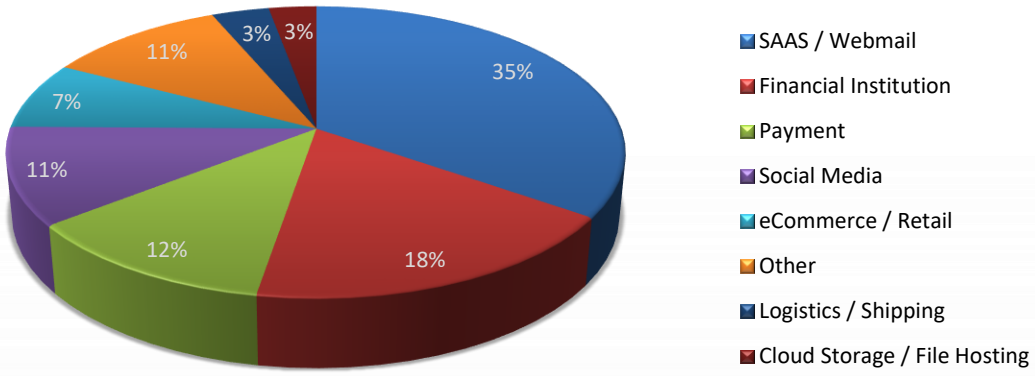

Figure *8*: Most targeted industries, second quarter of 2020 (APWG Phishing Activity Trends Report)

In terms of brands, ASEAN banks and Facebook were the most targeted. Both brands accounted for 42.3 per cent of the global figure.

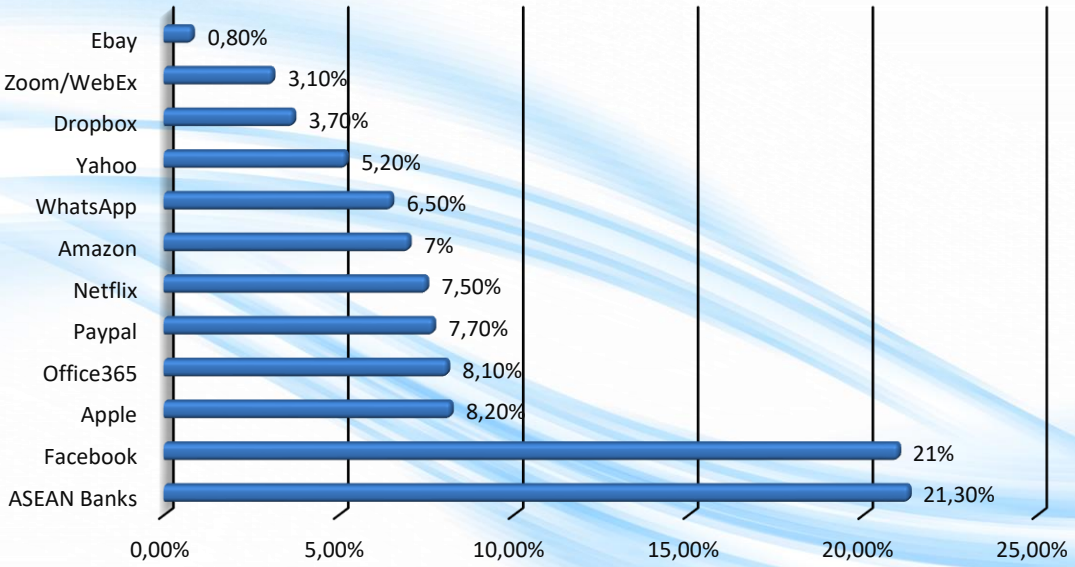

Figure *9*: Brands most targeted by phishing attacks (Trend Micro 2020)

Phishing attacks in the ASEAN region show no signs of slowing down or decreasing. From January to June 2020, Kaspersky alone blocked more than 1.6 million attempts to transfer users to phishing pages via links. In the first half of 2020, Kaspersky foiled the most phishing attempts in the region against SMBs in Indonesia, Malaysia, and Vietnam. Singapore experienced the lowest toll of phishing e-mails in the region, but still witnessed an increase of 60.5 per cent, compared with the same period in 2019.

8 Phishing Activity Trends Report (www.apwg.org).

Kaspersky's data show that Indonesia accounted for 749 915; followed by Vietnam (737 152); Thailand (478 795); Malaysia (442 439); the Philippines (200 312); and Singapore (145 004). While Singapore had the least number of attacks, the number of cases had risen by 60.5 per cent.

The proliferation of phishing attacks can be attributed to the relative ease with which an individual can engage in phishing. Phishing-as-a-Service (PhaaS) has made the use of phishing as a tool relatively easy. A phishing kit can be purchased for as little as USD 20 on the Dark market.

Once the purchase is made, the authors of the phishing kits provide online tutorials to demonstrate how to use the kits. The after-sales service even includes the provision of updates for the kits to ensure that the phishing e-mails evade detection and are blocked by Internet security solutions on the market. As a result, relatively low-skilled threat actors can launch phishing attacks in as many technical aspects such as coding and hosting, and anti-detection tools and services can likewise be purchased or added on.

The problem is further compounded by the COVID-19 pandemic. The increase in the number of individuals working remotely and spending more leisure time at home offers a wider attack surface for threat actors to exploit. In April 2020, Zoom announced that it had surpassed 300 million meeting participants daily.[9] Apart from work, individuals in ASEAN also spent more leisure time online during the pandemic.

The GlobalWebIndex's special coronavirus study[10] revealed that the Philippines has seen the greatest number of people reporting an increase in the amount of time spent on social media platforms. Around 64 per cent of the Filipinos who participated in the survey reported an increase in their "social time", compared with the global average of 47 per cent.

According to Trend Micro's endpoint detections, ASEAN accounted for 3.7 per cent of global malicious URL in relation to the COVID-19 pandemic, equivalent to 80 000 phishing attacks during the first nine months of 2020. Singapore was among the top seven countries.

There are significant challenges in dealing with phishing. While the general advice to the community is to remain vigilant and not to open suspicious e-mails and attachments, the problem will not disappear and is expected to get worse with the increase in the scale of the dissemination and sophistication of social engineering methods. As phishing is often viewed as a low-level crime, it may not be considered a top priority for many law-enforcement agencies in the region. This allows the threat actors to evolve and become more sophisticated over time.

A domain can be purchased for free or for as little as a few cents. E-mails can then be sent and victim credentials compromised within minutes. Therefore, the timeframe within which law enforcement can take action is extremely limited. When registering a domain, there are few challenges to staying anonymous with both the use of privacy protection services and lack of know-your-customer checks at most domain registrars, all of which provide cover for threat actors.

INTERPOL analysis identified above phishing trends

9 90-day security plan progress report (www.blog.zoom.us).

10 GlobalWebIndex special coronavirus study (www.globalwebindex.com).

3.3 Ransomware

Ransomware is a significant threat in the ASEAN region. According to statistics provided by Kaspersky, there were about 2.7 million ransomware detections in ASEAN during the first three quarters of 2020. Among the ten ASEAN member countries, Indonesia suffered the most with 1.3 million counts, accounting for almost half of the entire detections in the region.

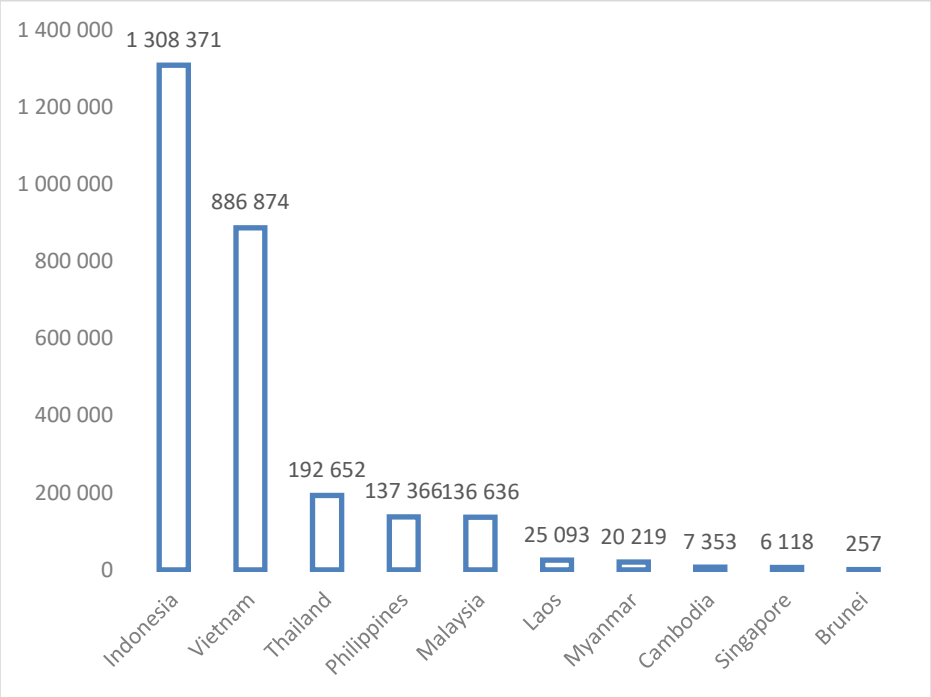

Figure 10: Ransomware detections in ASEAN countries from January to September 2020 (Source: Kaspersky)

According to a study conducted by the Identity Theft Resource Center (ITRC), the average ransomware payouts for all businesses have grown from less than USD 10 000 in the third quarter of 2018 to more than USD 178 000 per event by the end of the second quarter of 2020[11]. Large enterprises are making average ransomware payments of over USD 1 million. The sheer amount of returns is the main reason why the trend in ransomware is continuously on the rise.

According to Group-IB's conservative estimates, the total financial damage from ransomware operations amounted to over USD 1 billion (USD 1 005 186 000), but the actual damage is likely to be much higher. It is also believed that the actual situation is worse as many individuals and businesses are unwilling to report cases to the police, with Group-IB estimating that only 2.5 per cent of ransomware incidents are made public.

The reasons for not reporting a ransomware attack can be the result of the lack of quantifiable value that an individual places in the data that have been encrypted, that may extend to a far more serious and worrying idea that businesses may not want their customers to know that their data have been compromised. Victims often remain silent about incidents and pay ransoms quietly, while attackers do not always publish data from compromised networks.

Further reports from Group-IB revealed that the top five most frequently attacked industries included manufacturing, retail, government agencies, healthcare, and construction. From similar reports, it is observed that other critical infrastructures, including energy sectors, are not spared.

Particularly in 2020 during the COVID-19 pandemic, it has been observed that hospitals, medical centres and public institutions targeted by cybercriminals for ransomware attacks increased rapidly. Cybercriminals believe these institutions are more likely to pay the ransom because they are overwhelmed by the health crisis and cannot afford to be locked out of their systems. Within the ASEAN region, hospitals in Indonesia and Thailand have fallen victims.

[11] Identity Theft Resource Center. (https://www.idtheftcenter.org/2021-predictions-government-support-for-identity-crime-victims-is-out-and-stealing-passwords-is-in/).

The amount of ransom demanded by the threat actors varies greatly and this can be attributed to two tactics used to distribute ransomware. The first is the spray-and-pray tactic where malware is distributed via mail spam or fake malicious advertisements, targeting anyone unfortunate enough to become a victim. The second tactic is the targeted tactic where the threat actors select their targets before actively looking for ways to infiltrate their network. Once the network has been mapped, the threat actors proceed to encrypt the data. The latter requires far more time and resources to carry out, and consequently, the amount of ransom demanded is higher.

The challenges of addressing ransomware attacks are numerous. Given the organized and now experienced nature of the attackers, the techniques and tactics used to avoid identification have advanced. While an attacker can make multiple attempts to infiltrate a network, it only takes a single mistake by a user – such as opening an e-mail attachment – for an attack to be successful.

The organized schemes used by attackers prove how much information cybercriminals have about companies' financial situations. Ransomware demands are carefully calibrated to appear as more financially viable options than the cost of restoring backups and the reputational damage to the company.

According to research conducted by Group-IB, Maze and REvil are considered to have the largest appetite: the operators of these two strains are believed to be behind more than half of all successful attacks. Ryuk, NetWalker, and DoppelPaymer come second.

To compound the problem of ransomware, the "name and shame" tactic is used against infected companies. Hackers publicize corporate data for non-paying companies and even auction them for a higher profit. The Maze ransomware group is the only known group to use the "name and shame" tactic. However, it can be assumed that it is only a matter of time before this tactic becomes more widespread and targets businesses that operate in the ASEAN region.

Kaspersky has detected the above-mentioned ransomware targeting various industries in the ASEAN region:

Ransomware family	Target country	Target sector
Maze	Singapore	Aerospace
	Thailand	State enterprise
	Thailand	Beverage company
	Vietnam	Manufacturing and trading (steel)
REvil	Indonesia	Palm products and others
	Singapore	Engineering
Ragnar	Singapore	Aerospace
NetWalker	Malaysia	IT services
	Thailand	Hotels and accommodation

Figure 11: Ransomware attacks in ASEAN countries (Kaspersky)

Cybercriminals have displayed no discretion in their targets, with hospitals being specifically targeted at the height of the COVID-19 pandemic. With early detections, INTERPOL issued a purple notice to its 194 member countries to warn of this heightened threat.

As ransomware continues to produce substantial profit for cybercriminals, it remains a significant threat to both the ASEAN region and the rest of the world. Cybercriminals are becoming increasingly organized, and scouting and collating intelligence to decide who to attack.

Although the figures for targeted ransomware families are relatively low in the ASEAN region, the threat has the potential to increase in the future.

The "Ransomware-as-a-Service" (RaaS) model will lower the barrier of entry and will attract a lot of potential cybercriminals into hacking as a means of making money quickly.

INTERPOL analysis identified the above-mentioned ransomware trends

3.4 E-Commerce data interception

According to INTERPOL's private partner, Group-IB, the carding market grew by 116 per cent, from USD 880 million in 2019 to USD 1.9 billion in 2020. The quick growth applies to both textual data (bank card numbers, expiration dates, holder names, addresses, Card Verification Values (CVVs)) and dumps (magnetic stripe data). The amount of textual data offered for sale increased by 133 per cent, from 12.5 million to 28.3 million cards, while dumps surged by 55 per cent, from 41 million to 63.7 million. The maximum price for card textual data is USD 150 and USD 500 for a dump.[12]

Conventionally, dumps are mainly obtained by infecting computers with connected Point-of-Sale (PoS) terminals with special Trojans, thereby collecting data from random-access memory. However, with more businesses pivoting their retail shops to e-commerce platforms, there has been an alternative opportunity for cybercriminals to steal large amounts of payment data, including credit card information.

	2019			2020		
	Textual details	Dumps	TOTAL	Textual details	Dumps	TOTAL
Total amount	$12 540 190	$31 212 941	$43 754 131	$28 296 585	$70 381 942	$ 98 678 527
Market size	$179 159 552	$700 520 520	$879 680 072	$361 684 617	$1 540 043 892	$1 901 728 509
Minimum price	$ 0.7	$0.5		$0.1	$0.25	
Maximum price	$150	$500		$150	$500	
Average price	$14.29	$22.44		$12.78	$21.88	
Median	$13	$12		$12	$17	

Figure 12: Carding market overview (Group-IB)

[12] High-tech crime trends for 2020 and 2021 (www.group-ib.com).

Cybercriminal groups engaging in JavaScript (JS) card sniffing attacks have slowly spread their operations to target additional platforms besides the Magento-based stores, which were initially targeted between 2015 and 2016.

With carding information sales proving a lucrative business for cybercriminals, JS-sniffers (once considered a threat for Magento) now represent a threat to all online store platforms, including self-hosted solutions or cloud-based commercial SaaS platforms.

With the price of payment card details obtained from online stores being similar to that obtained from traditional ATM skimming, cyberattacks on online stores are expected to grow.

Our research shows that the number of JS-sniffer families has grown exponentially, targeting various e-commerce shops running on Content Management Systems (CMSs), such as Magento, OpenCart, WordPress, osCommerce, Bigcommerce and Shopify.

The threat has also evolved to include various functionalities, such as stealing payment and personal information from websites that use a variety of different payment processing systems, encrypting stolen information, avoiding detection, automatically infecting a target again, and carrying out targeted phishing attacks.

According to Group-IB, the number of JS-sniffer families has more than doubled: in 2020, there were at least 96 new families in less than 18 months, up from 38 families in March 2019. Furthermore, records show that nearly 460 000 bank cards were compromised by JS-sniffers in 2019.

The COVID-19 pandemic has propelled e-commerce growth in the ASEAN region as well as globally, as customers turn to online platforms to shop amid movement restrictions, pushing more and more businesses online. Inevitably, this has also created great opportunities for cybercriminals who are pushing the limits to maximize the sniffing of credit card information from e-commerce websites.

Our research shows some of the JS-sniffer families that have been detected (see below) and this list continues to grow:

1. **UltraRank**
2. **GetBilling**
3. **TokenLogin**
4. **FakeLogistics**
5. **WebRank**
6. **CoffeMokko**
7. **ReactGet**
8. **ImageID**
9. **Inter**

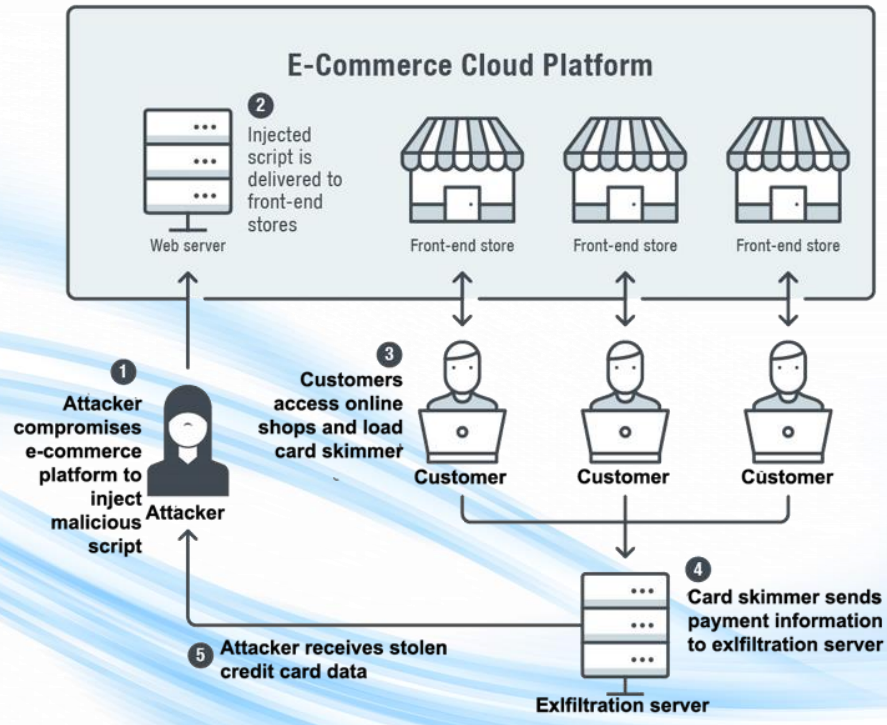

Figure 13: JS-sniffer attack illustration (Trend Micro)

Southeast Asia's online market worth is expected to reach USD 300 billion[13] by 2025, due to increasing disposable income, young Internet consumers, and a high rate of mobile Internet penetration. Thailand's e-commerce market value is expected to surge to USD 13 billion by 2025. There is no doubt that this region will be a choice target for cybercriminals.

13 Thailand Business News (www.thailand-business-news.com).

Under Operation Night Fury, INTERPOL's ASEAN Desk coordinated a cyber operation against a strain of malware targeting e-commerce websites. The Operation identified hundreds of compromised websites in affected countries and the Desk brought the threats to member countries' attention and offered support with national investigations. In particular, the intelligence detected Command-and-Control (C2) servers and located infected websites in six countries in the ASEAN region.

At the request of the Indonesian National Police, the ASEAN Desk provided technical and operational support which resulted in the arrest of three individuals suspected of commanding the C2 servers in the country.

INTERPOL analysis identified the above-mentioned JS-sniffer trends

JS-sniffers, which attack online stores and steal payment data and users' credentials, pose a growing threat.

The ease with which cybercriminals obtain JS-sniffer variants in underground forums, facilitates the launch of malicious campaigns against e-commerce platforms. The evolving functionalities make it even more challenging for law-enforcement agencies to investigate. Likewise, e-commerce users fail to detect the attacks and fail to prevent themselves from becoming victims.

This is a typical transnational form of cyberthreat which requires cooperation from multiple stakeholders to allow for intelligence sharing of early detection and prevention.

3.5 Crimeware-as-a-Service

The Crimeware-as-a-Service (CaaS) model has always been on the radar of cybersecurity experts, as well as law-enforcement communities.

Given the lucrative returns, it comes as no surprise that many cybercriminals venture into this enterprise model, adjusting their technology stacks to service clients with crimeware in the hope of increasing their revenue.

Online reports from cybersecurity websites show that crimeware, stolen data, and other saleable items on the Dark Web are increasingly sold as a service. This situation creates greater accessibility to various forms of advanced tools for cybercriminals to launch their malicious campaigns depending on their needs, the target users and organizations.

CaaS has lowered the entry barrier for new and less technologically proficient cybercriminals, facilitating the flurry of malicious activities and enabling threat actors to carry out sophisticated attacks without the need for advanced technical skills. The availability of a wide range of CaaS in cybercrime Dark Web forums and marketplaces are broadly advertised as a cheap solution. They are also offered as an optimum option for advanced attackers who wish to conduct hit-and-run campaigns.

Another factor that attracts cybercriminals to CaaS is that stolen credit card information can be used to conduct forward campaigns.

The CaaS model makes attribution difficult due to the means and infrastructures being shared among multiple bad actors or syndicate groups. The perilous aspect of the CaaS model is its role as an enabler for increasingly sophisticated attacks that are fuelling the rapid development of new advanced threats.

With the combination of various attack services, cybercriminals can also effectively challenge law enforcement's capabilities and capacities to investigate and attribute the attacks to specific actors and syndicates.

CaaS is a demand-driven market. The prices of services and products reflect the levels of complexity of the resources involved and are influenced by the availability of the means in the underground ecosystem.

Cybercrime product or service	Price (in US Dollars)
SMS spoofing	20/month
Phishing kit	20-200
Custom spyware	200
Hacker-for-hire	200+
Malware exploit kit	200-700
Blackhole exploit kit	700/month or 1 500/year
Zero-day Adobe exploit	30 000
Zero-day iOS exploit	250 000
Phishing kit	20-200

Figure 14 : Cybercrime products/ services price list (www.cyren.com)

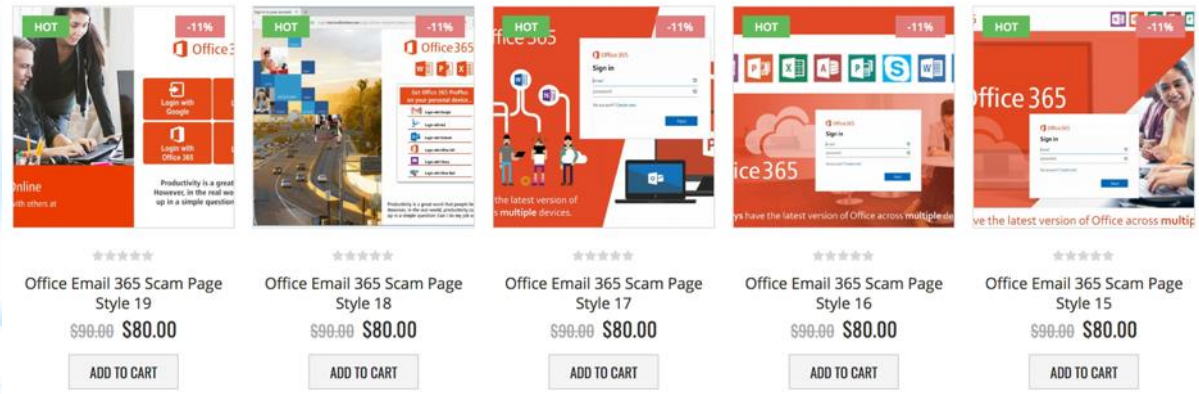

Figure 15. Price of Phishing-as-a-Service targeting Office365 (www.cyren.com)

Phishing-as-a-Service (PhaaS), a type of CaaS, offers automated and long-lasting phishing attacks without costing much to deploy numerous phishing campaigns, in just a few clicks.

When processing a payment in Bitcoin for botnet services, thousands of infected machines worldwide would be launching Distributed Denial-of-Service (DDoS) attacks on the designated targets, with the desired network capacity and timeframe of the attack.

The observed increase in ransomware attacks is partly due to ready-made Ransomware-as-a-Service (RaaS), which makes it easy to launch multiple campaigns without coding efforts. With RaaS, users can manage their campaigns from an online portal, which comes with an after-sales support service. The cost of subscribing to such a service is relatively low, with some service providers taking a cut of between 20 and 40 per cent of the ransom collected.

It is alarming that CaaS is categorized according to specific target industries, such as a strain of banking malware known as Vawtrak[14] which targets the financial industry, compromising commonly used URLs by injecting them with malicious codes. This allows hackers to steal online banking credentials entered on the bank's website.

14 Vawtrak – International Crimeware-as-a-Service (www.sophos.com).

According to research, Vawtrak represents 11 per cent of all malware, replacing Zeus as the leading banking malware botnet. Vawtrak operators set up the botnet to deliver Crimeware-as-a-Service, rather than following a more traditional kit-selling model used by older families, such as Zeus or SpyEye.

With the increase in CaaS offers in cybercrime and hacking forums, especially those hosted on the Darknet, it is crucial to monitor such platforms to identify new threats early and share information rapidly in order to detect and limit the dangers caused by cyberattacks.

INTERPOL analysis identified the above-mentioned CaaS trends

The fundamental issue surrounding the various types of cyberthreat, is that many cybercriminals are enlisting individuals or groups who charge a fee for providing the services, which can range widely from as little as USD 20 for generating thousands of spam e-mails to about USD 10 000 for developing crimeware.

With the proliferation of CaaS at affordable rates, more cybercriminals are expected to take up the offer, which will result in an increase in cyberattacks. More often than not, such services are hosted in countries with poor or no legislative framework against such activities or cybercrime, thereby creating a huge challenge for law-enforcement agencies in effectively taking down services and investigating the users.

3.6 Cyber fraud

The COVID-19 pandemic has accelerated digital transformation, forcing countries and businesses to push for digitalization efforts, and changing the way in which people work, learn, shop and bank. Notably, governments have set out various restrictions requiring organizations and staff to work from home for indefinite periods to curb the spread of the virus.

With more people working and shopping from home, there has been an increase in the volume and frequency of online transactions. Cybercriminals see this as an opportunity to make money and force their way into cyberspace through scams or fraudulent schemes.

The COVID-19 pandemic has severely affected businesses and the economy in general. Millions of people around the world have lost their jobs during the crisis. Heavy debts and financial constraints have left many people desperate for help.

It has been observed that cybercriminals are taking advantage of the economic downturn and people's anxiety by tweaking their social engineering tactics to include COVID-19-related themes. According to our findings, key COVID-19-inflicted cyberthreats are phishing/scam/fraud at 59 per cent, malware/ransomware at 36 per cent, malicious domains at 22 per cent, and fake news at 14 per cent.

Cybercriminals have revised their usual online scams and phishing schemes. By deploying COVID-19-themed phishing e-mails, cybercriminals impersonate government and health authorities and entice victims into providing their personal data and downloading malicious content. Around two thirds of INTERPOL's member countries which responded to the global cybercrime survey reported a significant use of COVID-19 themes for phishing and online fraud since the outbreak.

In Malaysia, a total of 7 765 incidents were reported to CyberSecurity Malaysia in the first eight months of 2020, with fraud topping the list at 5 697 cases compared with 4 671 incidents for the same period in 2019.

A study by Telenor Group also revealed that of the 400 Internet users aged 18-65+ interviewed in Malaysia:

- 9 in 10 were aware of Internet scams;
- 4 in 10 had been victims;
- 9 in 10 scam victims had lost money;
- 1 in 5 had fallen victim to Internet scam auctions.

Figure 16: Malaysia's public bank scam alert notice

Between January and October 2020, Malaysia experienced a surge in a particular scam – the "Macau Scam" – with 5 218 cases, which amounted to over 256 million Malaysian Ringgits (MYR) in losses.

What is the Macau Scam?

"The Macau Scam has been categorised as a telecommunication fraud … whereby the perpetrators use local and international lines mainly from Hong Kong to trick victims into handing them a large sum of money."[15]

In Indonesia, online fraud made up the second largest category of cases filed in police reports between January and September 2020. It contributed to more than a quarter of all cybercrime cases in that period, according to data from the National Police's Criminal Investigation Agency (Bareskrim).

From January to June 2020, the Singapore Police Force handled a further 4 226 scam cases, and 82 million Singapore dollars (SGD) were lost by victims through the top ten scam categories compared to 2019.

15 Commercial Crime Investigation Department (JSJK) of the Royal Malaysian Police (PDRM).

The top four categories of scams were e-commerce scams and social media impersonation ruses, followed by loan and banking-related phishing scams. Other common types of scam were credit-for-sex scams, investment scams, Internet love scams and cases where criminals impersonated government officials from China. Scammers also tapped technology and used Photoshop, bots and fake reviews to make their ruses seem as real as possible to their targets.

According to the police, the sharp increase in online scams was due to an increase in online transactions during the COVID-19 pandemic. Many of the e-commerce scams took place on digital platforms, such as Carousell, Shopee, Facebook and Lazada, and dubious transactions often involved electronics and gaming paraphernalia. Cybercrime involving social media impersonation was also an area of concern, as the number of such scams soared from 83 in in the first half of 2019 to 1 175 for the same period in 2020.

In Thailand, it was reported that an estimated 8.4 million workers may lose their jobs due to the COVID-19 pandemic. Desperation to earn an income in times of crisis perhaps led victims to fall prey to recruitment scams, with a rise in online recruitment offers promising jobs abroad that never materialize. Many of them would typically appear on the social media platform Facebook, and Line – a popular chat app.

In the Philippines, a huge increase in online scams was also recorded. There were 869 cases reported within a six-month period, which is an increase of 37.3 per cent compared to the same period for 2019. Identity theft also increased by 21.47 per cent with 362 cases.

As surgical masks and medical supplies are currently in high demand, some social media accounts and e-mail addresses claiming to sell such items have sprung up online. However, instead of receiving the promised masks and supplies, victims have seen their money end up in the hands of the cybercriminals involved in the scam.

In response to the rapidly changing cybercrime landscape during the COVID-19 pandemic, the global law-enforcement and cybersecurity communities have formed an alliance to protect the public.

Harnessing the expertise of this alliance, INTERPOL launched a global awareness campaign to keep communities safe from cybercriminals seeking to exploit the pandemic to steal data, commit online fraud or simply disrupt the virtual world.

The main message of the campaign, which focuses on alerting the public to key cyberthreats linked to the COVID-19 pandemic, is to #WashYourCyberHands and promote good cyber hygiene.

Cyber scams have long existed and have been growing exponentially in recent years as they offer lucrative revenue for cybercriminals. Scam campaigns are often coordinated by large syndicates with structured networks made up of administrators, operators and money mules, and a global money laundering network.

As more people have a digital footprint and share more information about themselves on social media platforms, this also enables cybercriminals to effectively socially engineer scam tactics against individuals or organizations.

INTERPOL analysis identified the above-mentioned cyber fraud trends

3.7 Cryptojacking

In the previous ASEAN Cyberthreat Assessment 2020, it was analysed that cybercriminals had leveraged the latest technological developments by reaching their main objective of achieving financial gain with little or zero risk of detection. The cryptojacking trend is amplified with cybercriminals targeting victims in the ASEAN region where information technology infrastructures offer a healthy supply of bandwidth.

Lower entry barriers combined with increasing values and the ability to stay under the radar, made cryptojacking an ideal target for cybercriminals.

CoinMiner malware can run on victims' computers without the victims' immediate knowledge. This is one of the major appeals of cryptojacking for cybercriminals. Cybercriminals consider the attack as a less disruptive way of making money, compared with other types of cyberthreat.

Amid the COVID-19 pandemic, there is an exponential growth of cryptojacking attempts in the ASEAN region. The growth in cryptojacking could be partly attributed to more people working from home. Compared with computers for professional use, personal computers have security features that are less likely to be kept up-to-date.

Although INTERPOL's ASEAN Desk coordinated an operation in June 2019 to mitigate cryptojacking campaigns in the ASEAN region targeting the vulnerabilities of MikroTik routers, the elimination of cyberthreats is far from over, as cybercriminals continue to target other types of devices.

Figure 17: Image from Trend Micro

This calls for continued collaboration and joint action between law-enforcement agencies and national CERTs to thwart emerging cyberthreats, as cybercriminals continue to conduct malicious activities. The key is to be proactive in the fight against cybercrime, as cybercriminals will keep turning to new technologies and will keep developing new methodologies.

Cryptojacking is not a new threat, but a highly evolving one.

The price increase in cryptocurrency, coupled with the ubiquitous increase in the number of IoT devices, provides cybercriminals with a greater attack surface from which to launch their cryptojacking campaigns. Cybercriminals exploit the increasing number of vulnerabilities with evolved tactics and advanced mining malware to achieve maximum illicit gains.

INTERPOL analysis identified the above-mentioned cryptojacking trends

4. Ways forward for proactive actions against evolving cyberthreats in ASEAN

While we have discussed the various types of cyberthreats and trends that pose risks to ASEAN, there should also be a greater awareness and understanding of the threats that the region will need to react to.

Common cyber strategies focus on reactive measures to prevent 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 need to be proactive in collecting and analysing external threat intelligence, seeking out cyberthreats before they manifest into attacks.

Intelligence gathering is a vital piece of the puzzle in which INTERPOL provides support to its member countries to effectively curb the effects of evolving cyberthreats through the establishment of capabilities like the ASEAN Desk. The ASEAN Desk gathers intelligence on cyberthreats and coordinates joint operations with the involvement of private and public entities. Knowing how the threat actors will attack and when they plan to do so, is crucial to thwarting a cyberattack at the start of the cyber kill chain.

In today's increasingly digitized world, the sooner countries are aware of a threat, the sooner they can take steps to mitigate the risks and neutralize the cyberthreats coming their way.

Additionally, law-enforcement agencies need to enhance their collective efforts in the sharing of intelligence and the formulation of a joint operational framework in order to be effective in combating cybercrime in the ASEAN region.

Whilst the law-enforcement agencies in the ASEAN region have established good relationships and bilateral cooperation arrangements for tackling traditional types of crime, there is an absence of an operational framework with INTERPOL to deal with cybercrime.

To enhance the effectiveness of intra- and interregional joint operations, the ASEAN Desk has established an operational framework known as the **Joint Operational Framework for Improving Coordinated Action against Cybercrime in ASEAN**.

The Framework will guide INTERPOL-led operations with the law-enforcement community in ASEAN, setting out how joint operations are formulated, coordinated and communicated to ensure the effective and timely exchange of information. Specifically, the Framework calls for effective cooperation between law-enforcement communities, other international/intergovernmental organizations, and the private sector.

With the development of new policies and legislative framework in ASEAN countries, the Framework will be a living document and as such, will adopt new changes to retain its relevance in line with prevailing regional and international norms.

5. ASEAN Joint Operations on Cybercrime annual planning cycle

To achieve its intended purpose, the Framework proposes a four-phase ASEAN Joint Operations against Cybercrime (AJOC) annual planning cycle, to be adopted by the ASEAN Desk in promoting a coherent and methodological approach to improve proactive coordinated operations against cybercrime in the region.

Figure 18: AJOC annual planning cycle

Phase I – Collect and analyse

The first phase focuses on an in-depth analysis of information pertaining to the prevalent cyberthreats, malicious infrastructures and threat actors that operate in/against the community in the ASEAN region. Leveraging on intelligence from law-enforcement communities, the extensive data-sharing agreements with INTERPOL's Project Gateway partners and academia, the ASEAN Desk will publish the ASEAN Cyberthreat Assessment (ACTA) during the first quarter of each year to help the ASEAN law-enforcement community to develop a deeper appreciation of its cyberthreat landscape.

Phase II – Prioritize and strategize

The ACTA published during Phase I of the Cycle will serve as a reference document to help ASEAN member countries to develop or update their respective cybercrime strategies, and steer regional prioritization of operational efforts with INTERPOL for the year. Recognizing the diversity in the ASEAN region, with each member country having its own unique challenges, the ASEAN Desk (with the relevant NCB's authorization) will involve each member country's Head of Cybercrime during this phase to explore both intra- and interregional collaboration opportunities. By the end of this phase, a regional roadmap on an agreed joint strategy with clear operational outcomes for the year will be ready for promulgation.

Phase III – Operationalize

The ASEAN Desk will develop the respective Standard Tactical Plans (STPs) to operationalize the strategy agreed upon in Phase II. STPs provide a clear set of objectives, roles and responsibilities, and an operational concept to deal with the specific cyberthreats. Each STP typically includes detailed plans on the following: (1) planning and analysis; (2) organization; (3) tactics; and (4) evaluation. STPs will be shared with participating countries for endorsement.

The participating cybercrime units will then be committed to the actions outlined in the STPs and will provide full support to achieve the agreed operational aims and objectives. Following endorsement, operations will be coordinated by the ASEAN Desk and carried out by designated investigators in accordance with the timeline specified in the STPs. Data relating to the operations are received by INTERPOL through its secure I-24/7 communications system or Cyber Collaboration Platform - Operation, for analysis.

Upon receiving the operation-related information, nominated Points-of-Contact from each member country will maintain effective communication with the ASEAN Desk for information exchange, as per the designated objectives and timeframe of the operation. Facilitating the preservation and disclosure of Internet records will be on a voluntary, not mandatory, basis and will be encouraged for all cybercrime investigation courses, given that electronic evidence is volatile. Member countries are strongly encouraged, within the limits of their respective laws and policies, to share updates on investigations and specific intelligence that may help other members of their operation to make progress with their own investigations. As far as possible, the PoCs will facilitate the sharing of information with other national agencies such as Computer Emergency Response Teams (CERTs), central banks, etc., depending on the needs of each operation.

Phase IV – Evaluate

In Phase IV, an After-Action Review (AAR) will be conducted to identify lessons learnt from the operations. Based on reviews and new information arising from the operations, the ASEAN Desk will recommend adjustments for future joint operations. Intelligence collected during Phase III will also be evaluated to enhance regional understanding of prevalent cyberthreats and to contribute to the development of the next ACTA.

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