INTERPOL

CYBERCRIME:

COVID-19 IMPACT

AUGUST 2020

INTERPOL General Secretariat
200, quai Charles de Gaulle
69006 Lyon
France

Web: www.interpol.int
E-mail: info@INTERPOL.int

CONTENTS

INTRODUCTION

The unprecedented coronavirus pandemic is profoundly affecting the global cyberthreat landscape. Compounding a global health crisis with a sharp increase in cybercriminal activities related to COVID-19 is putting significant strain on law enforcement communities worldwide. According to one of INTERPOL's private sector partners, 907,000 spam messages, 737 incidents related to malware and 48,000 malicious URLs — all related to COVID-19 were detected between January and 24 April, 2020[1].

To maximise damage and financial gain, cybercriminals are shifting their targets from individuals and small businesses to major corporations, governments and critical infrastructure, which play a crucial role in responding to the outbreak. Concurrently, due to the sudden, and necessary, global shift to teleworking, organizations have had to rapidly deploy remote systems, networks and applications. As a result, criminals are taking advantage of the increased security vulnerabilities arising from remote working to steal data, generate profits and cause disruption.

In light of these events, INTERPOL's Cybercrime Directorate produced this Global Assessment Report on COVID-19 related Cybercrime based on its unique access to data from 194 member countries and private partners to provide a comprehensive overview of the cybercrime landscape amid the pandemic. The report is based on data collected from member countries and INTERPOL private partners as part of the INTERPOL Global Cybercrime Survey conducted from April to May 2020. In total, 48 out of 194 member countries responded to the Survey and 4 out of 13 private partners contributed their data to the report.

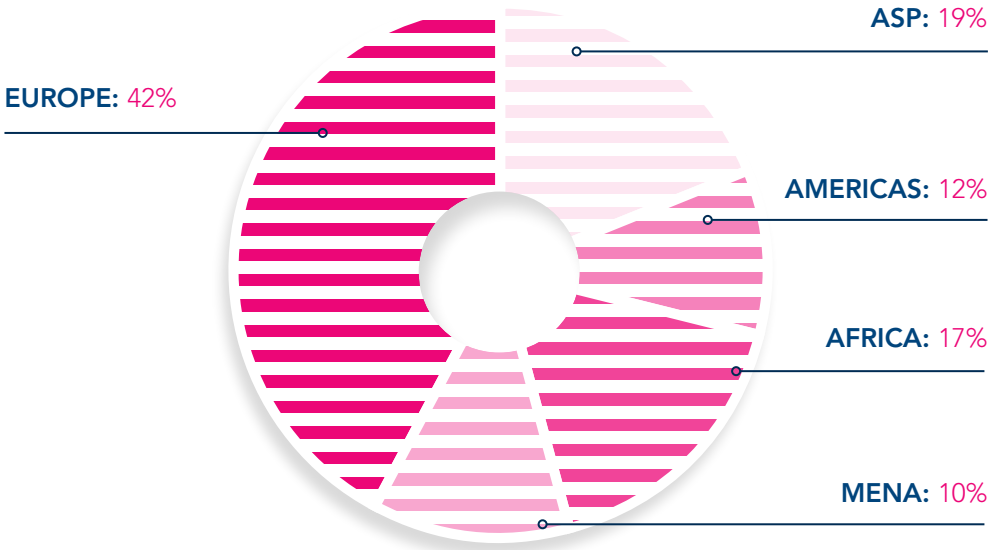

Fig 1. INTERPOL Global Cybercrime Surveys:
Breakdown of the Respondents By Region

[1] https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

The resulting analysis was supplemented by information provided by private sector partners and the INTERPOL Regional Working Groups on Cybercrime. This report also incorporates information and analysis generated by the INTERPOL Cybercrime Threat Response (CTR) unit and its Cyber Fusion Centre (CFC) – a team of law enforcement and private sector experts based in Singapore. The key findings on the cybercrime landscape in relation to the COVID-19 pandemic are as follows:

- **Online Scams and Phishing**
  Seizing the pandemic as an opportunity to give their attacks a better chance of success, threat actors have revised their usual online scams and phishing schemes. By deploying COVID-19 themed phishing emails, often impersonating government and health authorities, cybercriminals entice victims into providing their personal data and downloading malicious content.

- **Disruptive Malware (Ransomware and DDoS)**
  Cybercriminals are increasingly using disruptive malware against critical infrastructure and healthcare institutions, due to the potential for high impact and financial benefit. Such ransomware or DDoS attacks can result in regular disruptions or a total shutdown of business operations as well as a temporary or permanent loss of critical information.

- **Data Harvesting Malware**
  The deployment of data harvesting malware such as Remote Access Trojan, info stealers, spyware and banking Trojans by cybercriminals is also on the rise. Using COVID-19 related information as a lure, threat actors infiltrate systems to compromise networks, steal data, divert money and build botnets.

- **Malicious Domains**
  Taking advantage of the increased demand for medical supplies and information on COVID-19, there has been a significant increase of cybercriminals registering domain names that contain related keywords, such as "coronavirus" or "COVID". These fraudulent websites underpin a wide variety of malicious activities including C2 servers, malware deployment and phishing.

- **Misinformation**
  An increasing amount of misinformation and fake news is spreading rapidly among the public. Fueled by the uncertain social and economic situation in the world, unverified information, inadequately understood threats, and conspiracy theories have contributed to anxiety in communities and in some cases facilitated the execution of cyberattacks.

EVOLUTION OF CYBERCRIME TRENDS AND THREATS AMID

Regional Cybercrime Trends

While cybercrime has spiked across the globe during the COVID-19 pandemic, crime trends vary from region to region. Below is an overview of the COVID-19 cyberthreat landscape from a regional perspective.

AFRICA

- Respondents from African member countries highlighted the increased use of electronic or cashless payments from the onset of the pandemic making the public more exposed to cyberattacks.
- With most organizations and companies enforcing a working from home (WFH) policy, the vulnerabilities of these arrangements have led to a surge in appropriately themed phishing, sextortion and charity scams.
- The circulation of fake news related to COVID-19 in social media has increased.
- There has been relatively low Public-Private Partnership activity in tackling cybercrime, contributing to an increase in unresolved cybercrimes.

AMERICAS

- A sharp increase in COVID-19 themed phishing and fraud campaigns that leverage the coronavirus crisis and the subsequent lockdown were reported by respondents.
- As many companies in the Americas implemented teleworking, cybercriminals are increasingly targeting employees in order to gain control through remote access to corporate networks with a view to stealing sensitive information.
- A ransomware campaign carried out mainly through LOCKBIT malware is currently affecting medium-sized companies in some countries within this region.
- Social media is increasingly used by criminals for online child sexual exploitation. Specifically, offenders within online child abuse networks are locating and contacting their victims on social media taking advantage of the global lockdown. At the same time, the trade in child sexual exploitation images has intensified.

ASIA AND SOUTH PACIFIC (ASP)

- Major regional trends in ASP include COVID-19 related fraud and phishing campaigns as well as the illegal online sale of fake medical supplies, drugs and personal protective equipment.

- Cybercriminals are exploiting security vulnerabilities of teleconference tools.
- Circulation of fake news and misinformation related to COVID-19 has been reported by most ASP member countries that participated in the survey.
- The lack of cybersecurity awareness and 'hygiene' was named among the main challenges in this region.

EUROPE

- Two-thirds of member countries from Europe reported a significant increase in the malicious domains registered with the key words 'COVID' or 'Corona' aiming to take advantage of the growing number of people searching for information about COVID-19 online.
- Cybercriminals are taking advantage of the pandemic to deploy ransomware against critical infrastructure and healthcare institutions responsible for COVID-19 response.
- Cloning of official government websites is increasingly occurring to steal sensitive user data, which can later be used in further cyberattacks.
- Widespread phishing campaigns are being registered by European law enforcement agencies.

MIDDLE EAST AND NORTH AFRICA (MENA)

- This region highlighted the growing use of social media to proliferate fake news related to COVID-19.
- Social media platforms are frequently being used for the illicit sale of pharmaceutical and para-pharmaceutical products related to the coronavirus.
- Increase in registration of malicious domains that claim to provide COVID-19 statistics.
- Increasing number of phishing and online fraud linked to the COVID-19 pandemic.

KEY COVID-19 CYBERTHREATS

Based on the comprehensive analysis of data received from member countries, private partners and the CFC, the following cyberthreats have been identified as main threats in relation to the COVID-19 pandemic.

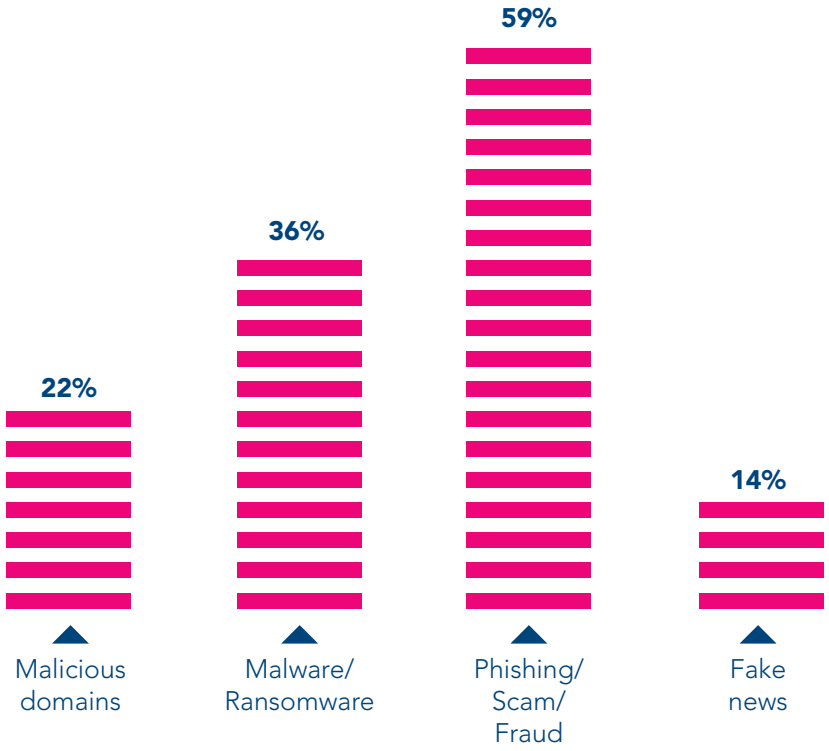

Fig. 2 Distribution of the key COVID-19 inflicted cyberthreats based on member countries' feedback

Online Fraud and Phishing

Around two-thirds of member countries who responded to the survey reported a significant use of COVID-19 themes for phishing and online fraud since the outbreak. Since January 2020, one of INTERPOL's private partners, Trend Micro, detected 907,000 messages linked to COVID-19[2]. Taking advantage of the economic downturn and people's anxiety during the pandemic, cybercriminals have enhanced their social engineering tactics by using COVID-19 as a basis in their attacks. Specifically, many existing organized crime groups have changed their tactics to exploit pandemic updates and supply shortages as well as advertising fake medications, fiscal packages, and emergency benefits.

A large proportion of incidents reported to law enforcement authorities involved

[2] https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

threat actors deploying COVID-19 themed phishing emails to solicit user credentials and passwords. These emails often impersonate official government and healthcare authorities claiming to provide information and recommendations regarding the pandemic. Beyond these direct associations to news about the pandemic, INTERPOL partner Kaspersky highlighted threat actors using a COVID-19 tax rebate to lure recipients into browsing a fraudulent website that collects financial and tax information from unsuspecting users.

Phishing emails supposedly sent from Ministries of Health or the World Health Organization contained malicious attachments, which exploit vulnerabilities to run malicious code. Malware such as Emotet, Trickbot and Cerberus, designed specifically for information theft, was registered by both member countries and INTERPOL private partners as being widely used in phishing emails.

Information provided by private partners indicates that Business Email Compromise (BEC) continues to be the scheme-of-choice for many threat actors. Tactics have been adapted to the current COVID-19 context – spoofing supplier and client email addresses, or using nearly identical email addresses – to conduct attacks. The extreme need for essential supplies and healthcare products provides an ideal scenario for criminals to harvest details or divert millions of dollars of procurement funds into criminal accounts.

According to information provided by member countries and private partners, the top COVID-19 phishing themes include:

- Emails from national or global health authorities;
- Government orders and financial support initiatives;
- Fake payment requests and money reimbursements;
- Offers of vaccine and medical supplies;
- COVID-19 tracking apps for mobile phones;
- Investments and stock offers;
- COVID-19 related charity and donation requests.

Overall, with COVID-19 and the subsequent lockdown, coronavirus-themed phishing lures are gaining momentum, leveraging fear, hooking vulnerable people and taking advantage of workplace disruption.

DISRUPTIVE MALWARE (RANSOMWARE AND DDOS)

Adjusted to the coronavirus outbreak, malware attacks are increasing in quantity and evolving in choice of targets. Based on the CFC's analysis and its support to member countries, the major focus of the disruptive malware campaigns has shifted from

individuals and small businesses to government agencies and the healthcare sector, where higher financial demands can be made.

Several member countries reported malware attacks against critical infrastructure of government organizations, hospitals and medical centres, which are overwhelmed with the health crisis. Such ransomware or DDoS attacks intend to make data inaccessible or disrupt the system, exacerbating an already dire situation.

According to the CFC, in the first two weeks of April 2020, there was a spike in ransomware attacks by multiple threat groups that had been relatively dormant for the past few months. This implies that there may still be organizations that have been infected but where the ransomware has not yet been activated. Law enforcement investigations indicate that after thorough reconnaissance of the networks of targeted organizations, the attackers estimated quite accurately the maximum amount of ransom they could demand. When the ransomware is deployed on strategic locations in the network which maximizes disruption of the business process, organizations are often coerced into paying the ransom. Such attacks can be combined with the exfiltration of sensitive information, which may later be used for additional pressure for payment.

The top ransomware families recently detected by INTERPOL private partners are CERBER, NetWalker and Ryuk. These are constantly evolving to maximize the potential damage of a single attack as well as the financial profit for its perpetrators.

Similar to ransomware campaigns, the DDoS attacks reported to the CFC have grown in size, aiming to disrupt the operation of various organizations and critical services. By overcharging online service portals with more traffic than the server or network can handle, cybercriminals threaten to take down the targeted websites unless a money transfer is made to their accounts.

The eventual impact of ransomware and DDoS attacks varies and may include disruption of operations, locking of critical systems and loss of data that will inflict financial losses due to the downtime and restoration of systems and files.

MALICIOUS DOMAINS

More than a third of the member countries are monitoring a growing influx of newly registered domains (NRDs) with "COVID" or "Corona" key words. Similar to COVID-19 themed phishing campaigns, a high percentage of domains that claim to provide COVID-19 updates, tracking systems or statistics are used for a wide variety of malicious activities exploiting the public's thirst for information during the pandemic. As of the end of March 2020, 116,357 COVID-19 NRDs were detected, out of which 2,022 were identified as malicious and 40,261 as "high-risk"[3]. In June 2020,

[3] https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/

INTERPOL Cybercrime Directorate's Global Malicious Domain Taskforce identified and analysed 200,000 malicious domains affecting more than 80 member countries.

The newly registered malicious domains either host data harvesting malware or are constructed to obtain personally identifiable information, approaching victims via spam campaigns through emails, SMS or cold calls. From February to March 2020, Palo Alto Networks, one of INTERPOL's private partners, detected a 569 per cent growth in malicious registrations, including malware and phishing; and a 788 per cent growth in high-risk registrations, including scams, unauthorized coin mining, and domains that have evidence of association with malicious URLs. The hike in registrations followed the peak of user interest in COVID-19 related topics caught in Google Trends with a few days of delay[4].

Further feedback received from law enforcement agencies highlighted that certain malicious websites have been created to mimic official public services including government portals, telecommunication companies, banks, national tax and customs authorities, etc. The trend was showcased by a member country through the exploitation of the national initiative to provide rapid financial support for the self-employed and small businesses. To receive the assistance, businesses were required to apply via an official government website. The threat actors quickly copied these websites and deployed a fake app to harvest personal user data received from the applicants.

Another area of concern is the increasing number of fraudulent websites, which exploited the recent surge in demand for surgical masks, personal protective equipment, coronavirus test kits and medical ventilators to host illicit trade in these key supplies. The tactics of the websites' owners differ and include copying a legitimate site, selling unlicensed items or counterfeit goods or taking payment for the items without delivering them. Moreover, there exists a challenge when the money paid by the victims of illegal trade is sent to overseas bank accounts, which creates difficulties in both the crime attribution and recovery of financial loss.

DATA HARVESTING MALWARE

The Global Cybercrime Survey highlighted a significant concentration in the use of data harvesting malware with COVID-19 related information as a lure. Threat actors deceive users to execute malware such as remote access Trojans, info stealers, spyware[5] and banking Trojans to compromise networks, harvest data, divert money and build botnets. This delivery of malicious executables is extensively facilitated through COVID-19 phishing campaigns. Alternatively, it has been observed that the malware is delivered through embedded links in interactive coronavirus maps, thematic applications and fraudulent websites.

4 https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/

5 https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/

One of the most distinctive examples of data harvesting malware indicated by private partners is Emotet. Its proliferation has significantly increased since the beginning of the pandemic. Researchers from IBM X-Force researchers detected an Emotet Trojan in Japan, which was widely used by cybercriminals who impersonated disability welfare service providers[6]. In their phishing emails, threat actors enticed victims to open attachments which claimed to contain COVID-19 prevention measures, but were infected with Emotet. Many people fell for this as the messages seemed to come from the official email of the service provider and appeared to have a legitimate address and phone number. Investigating the same case, Kaspersky threat researchers discovered that the Emotet Trojan is usually sent in .pdf, .mp4, and .docx formats as an attachment to emails that claim to contain useful information on coronavirus including its latest updates, protection measures and detection methods[7]. These attacks have proven to be particularly successful as cybercriminals chose the right moment to spread the malware at a time when people feel anxious and insecure. As a result, a significant amount of personal data has been stolen in recent months. Impacting 13 per cent of organizations globally, Emotet occupied the first place in the list of the most prominent data harvesting malware families in January 2020[8].

Trickbot is another example of data harvesting malware that has significantly intensified due to the pandemic. According to a recent study conducted by Microsoft, Trickbot is identified as the most prolific malware that was used in combination with COVID-19 lures[9]. This malware is reported to be linked to more phishing emails than any other since the beginning of the pandemic. It was also delivered to victims as an attachment in emails from a fake non-profit offering free COVID-19 tests.

6 https://exchange.xforce.ibmcloud.com/collection/18f373debc38779065a26f1958dc260b

7 https://www.techrepublic.com/article/hackers-using-coronavirus-scare-to-spread-emotet-malware-in-japan/

8 https://blog.checkpoint.com/2020/02/13/january-2020s-most-wanted-malware-coronavirus-themed-spam-spreads-malicious-emotet-malware/

9 https://twitter.com/MsftSecIntel/status/1251181180281450498

MISINFORMATION

In mid-February 2020, the World Health Organization (WHO) announced that COVID-19 was accompanied by an 'infodemic' of misinformation. The UN agency warned that misinformation about the pandemic presented a serious risk that is similarly dangerous as the virus itself[10].

According to a global study conducted by Reuters Institute, the following were identified as the most common COVID-19 related topics appearing in the surge of fake news and misinformation[11]:

- Public authority action;
- Community spread;
- General medical news;
- Prominent actors;
- Conspiracy theories;
- Virus transmission;
- Public preparedness;
- Vaccine development;

27 per cent of participating countries in the Global Cybercrime Survey confirmed the circulation of false information related to COVID-19 among their communities and 21 per cent expressed a growing concern in this trend. Within a one-month period, one member country reported 290 postings and in most cases, these postings contained concealed malware.

The information was mainly shared through social media (WhatsApp, Facebook, Twitter, etc.) and contained false claims, rumours and speculation on the continuously evolving COVID-19 situation. Some law enforcement authorities that participated in the survey reported that misinformation in their countries was linked to the illegal trade of fraudulent medical commodities.

Some member countries expressed concerns that misinformation was propagating communal panic and social disorder that had already been exacerbated due to the pandemic. Law enforcement authorities reported cases of false information disseminated online relating to the number of infected individuals and emergence of the virus in unaffected areas.

10 https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf

11 https://reutersinstitute.politics.ox.ac.uk/research

Other cases of misinformation involved scams via mobile text-messages containing 'too good to be true' offers such as free food, special benefits, or large discounts in supermarkets. Law enforcement agencies believe most of these messages were circulated in communities with the aim to create and exploit mass gatherings of people.

Fig. 3: Alert released by WHO warning public about fake news on COVID 19 circulating via WhatsApp[12]

INTERPOL RESPONSE

In response to the rapidly changing cybercrime landscape during the COVID-19 pandemic, INTERPOL is developing and leading the global law enforcement response against related cyberthreats. Its Cybercrime Directorate has been working with member countries, private sector partners and cybersecurity communities across the globe on multiple streams.

To support its member countries to prevent and counter cybercrime during the pandemic, INTERPOL has and/or continues to:

- Organize emergency virtual meetings with a variety of stakeholders to provide tailored services to member countries for the prevention, detection and investigation of COVID-19 related cybercrime. This effort includes strategic meetings of the Heads of National and Regional Cybercrime Units and the INTERPOL Global Cybercrime Expert Group[13].

12 https://www.who.int/india/emergencies/coronavirus-disease-(covid-19)/fake-news-alert

13 INTERPOL Global Cybercrime Expert Group is a network of cybercrime experts from member countries, private industry, public sector and academia to share information and good practices as well as to advise INTERPOL General Secretariat in policy formulation and project implementation in the field of cyber.

- INTERPOL is also actively engaging in the multilateral strategic discussions led by World Economic Forum[14] to build partnerships and an alliance against cybercrime. It is also part of the Advisory Board of World Economic Forum's Centre for Cybersecurity.
- Publish **INTERPOL Purple Notices**[15] to inform the law enforcement community of emerging and high-risk cyberthreats. These global alerts, sent through the INTERPOL secured network, include the following[16]:
  - **Ransomware attacks against critical infrastructure and hospitals:** INTERPOL's CFC has detected attempts to compromise and execute ransomware against key organizations and infrastructures required to assist in the response of COVID-19.
  - **Use and dissemination of a banking Trojan:** A banking Trojan has taken advantage of the vulnerability of a national service to impersonate the entity and send SMS using the lure of COVID-19 related content to download the embedded malicious link.
  - **Mailing of malicious USB devices:** The CFC has collected information on the new attack vector of a cybercriminal group, mailing malicious USB devices as part of 'gifts' in order to get access to business networks and steal sensitive information.
  - **Use and dissemination of a malicious software Trojan:** The malware called "Coronavirus" makes disks unusable by overwriting the master boot record.
- Convened a **Global Malicious Domain Taskforce.** Comprising cybercrime intelligence officers, experts from private sector partners and national law enforcement officials, the objective of the taskforce was to identify and target the threat actors and common infrastructure behind malicious domains, in order to disrupt and mitigate this type of threat.
  By June 2020, the Taskforce had identified and analyzed about 200,000 malicious domains. Based on the findings, Cybercrime Directorate disseminated Cyber Activity Reports containing relevant data to more than 80 member countries that were affected.
  - Lead a **Global Awareness Campaign on COVID-19 Cyberthreats #WashYourCyberHands**, Launched in May 2020, with member countries

[14] https://www.weforum.org/agenda/2019/11/why-public-private-partnerships-are-critical-for-global-cybersecurity/; https://www.weforum.org/agenda/2020/01/partnerships-are-our-best-weapon-in-the-fight-against-cybercrime-heres-why/

[15] INTERPOL publishes Purple Notices to member countries to seek or provide information on modus operandi, objects, devices and concealment methods used by criminals.

[16] The details of Purple Notices have been redacted due to ongoing INTERPOL's cybercrime operations.

and 23 external partners to alert the public to key cyberthreats linked to the coronavirus pandemic, and to promote good cyber "hygiene." Aimed to keep communities safe from cybercriminals seeking to exploit the outbreak to steal data, cause disruption or commit frauds, the campaign supported national law enforcement prevention efforts against the growing cyberthreats related to COVID-19. The visual materials and social media posts of the campaign developed by INTEPROL and its partners reached some 7.5 million users online. On Twitter (@INTERPOL_Cyber) alone, the campaign's hashtag of #WashYourCyberHands was mentioned about 10,000 times.

PRIORITIES AND RECOMMENDATIONS

To ensure INTERPOL's support and services to its member countries continue to be as effective as possible in mitigating COVID-19 related cyberthreats, the following priorities and recommendations have been identified.

- **Allow timely information sharing.** Up-to-date information on newly identified cyberattacks enables the Cybercrime Directorate to accurately project emerging trends and share criminal *modi operandi* via the INTERPOL global network to promote awareness and prevention. This particularly concerns cases of ransomware attacks against governments, critical infrastructure and the healthcare sector that may cause a major risk and harm to public safety and security. Receiving timely and relevant information allows INTERPOL to support member countries in formulating and executing an effective response.

- **Enhance Police Collaboration and Cooperation among member countries.** Given the evolution of transnational cyberthreats due to COVID-19, INTERPOL highlights the importance of collaboration among national law enforcement authorities and the timely response to requests for information that they receive from other countries. Cooperation and information exchange is particularly critical in order to address the following cyberthreats:

  - Ransomware attacks against critical infrastructure, Indicator of Compromise, Bitcoin addresses;
  - Cases related to Advance Payment Fraud (APF) and BEC;
  - Malware spreading via non-governmental contact tracing applications;
  - Details around campaigns leveraging high volume of malicious domains.

- **Utilize the INTERPOL Cybercrime Collaborative Platform**[17]. Designed for knowledge exchange and operational coordination, the platform provides a secure solution for member counties to engage in multi-stakeholder and multi-jurisdictional joint task forces to combat crimes against computer systems. This facilitates direct communications between operational teams in the member countries and with INTERPOL for the effective sharing of cybercrime information to develop timely operational response for disruption.

- **Implement Prevention Measures and Raise Awareness.** The evolution of COVID-19 related cyberthreats is projected to continue posing legal and operational difficulties for law enforcement agencies worldwide. To mitigate these challenges, prevention through educating and empowering the public to be safe on the Internet is vital. Member countries are encouraged to share the key messages of INTERPOL's global #WashYourCyberHands campaign within their communities through social media platforms and to launch similar awareness campaigns at the national level.

- **Enhance Cybercrime Investigative Capabilities.** As cyberthreats continue to evolve, either directly or indirectly in relation to the pandemic, it is especially important for law enforcement agencies to be equipped with specialized technologies and capabilities. Acknowledging the significance of elevating the level of expertise of its member countries during the global crisis, INTERPOL launched its **Virtual Global Academy** to provide a wide range of online training opportunities for law enforcement. The INTERPOL Cybercrime Directorate is hosting online training courses and webinars to enhance member countries' capabilities to face the emerging cyberthreats, and successfully investigate cybercrime cases in the time of the global crisis and beyond.

- **Strengthen Public-Private Partnerships (PPP).** Since the onset of the COVID-19 pandemic, PPP have been key to successfully mitigating emerging cyberthreats. By sharing intelligence and expertise on recent trends as well as providing technical assistance, private sector companies can serve as valuable partners for law enforcement agencies.
  In this regard, since January 2020, the INTERPOL Cybercrime Directorate has aggregated data and information on COVID-19 cyberthreats from member countries, INTERPOL private partners, National Computer Emergency Response Teams (CERTs) and the Internet Corporation for Assigned Names and Numbers (ICANN) and online information sharing groups such as Slack. The diverse portfolio of these partners enriched the dataset and proved its usefulness in providing necessary and timely assistance to member

[17] INTERPOL Cybercrime Collaborative Platform is hosted within the Cybercrime Pavilion of INTERPOL's Global Knowledge Hub powered by Secure Collaborative Platform technology.

countries. Recognizing these positive collaborations, INTERPOL aims to develop a database that all stakeholders can contribute to and access in developing the most effective cybercrime threat response.
Ultimately, building a strong relationship between law enforcement and private industry forges a sense of shared responsibility in the fight against COVID-19 cyberthreats and enables timely and targeted response to emerging cyberthreats.

- **Develop and implement National Cybercrime Strategies.** INTERPOL's recent survey identified the absence of a National Cybercrime Strategy (NCS) in in response to COVID-19 pandemic in 30 member countries. The finding underscores the necessity of establishing a NCS to build resilience of national infrastructure and services which can help countries counter cyberthreats effectively and protect communities from data breaches during the global crisis and beyond.

SHORT-TERM PROJECTIONS

Based on the analysis of the feedback from law enforcement agencies and private sector entities, the cyberthreat landscape is likely to continue to deteriorate. The following projections by the INTERPOL Cybercrime Directorate highlight what are likely be the primary areas of concern.

- As COVID-19 continues to persist globally, a further increase in cybercrime is highly likely in the near future. Attracted by the vulnerability related to WFH and the potential for increased financial benefit, cybercriminals are highly likely to build up their activities and develop more advanced and sophisticated modi operandi.
- The vulnerabilities related to WFH policies will most likely be further exploited by cybercriminals targeting employees' credentials through essential office tools and software. The stolen personal data may also be exploited for additional cyberattacks
- Another driver of the further expansion of the cybercrime scale is the impact the coronavirus-related lockdowns are having on other crimes areas, resulting in criminals searching for alternative revenue streams. As such, some criminals will likely take advantage of Darknet markets to offer 'Cybercrime-as-a-Service' for easy entry.
- Leveraging panic amidst the pandemic, threat actors are likely to continue proliferating coronavirus-themed online scams and phishing campaigns. BEC schemes will also likely surge due to the economic downturn and shift in the business landscape, generating new opportunities for criminal activities.

- In addition, when COVID-19 vaccination or medication is available, it is highly probable that there will be another spike in phishing related to these medical products as well as network intrusion and cyberattacks to steal data.
- Ransomware attacks targeting the healthcare sector and associated supply chains are likely to continue at a more rapid pace, accelerated by a diversification in attack vectors.
- Threat actors are expected to target the Personal Identifiable Information of individuals through the spoofing and exploitation of digital content providers.
- Even when cases of the coronavirus have declined, cybercriminals will most certainly adapt their fraud schemes to exploit the post-pandemic situation and the largest possible number of victims.

CONCLUSION

Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation around the world. At the same time, the higher dependency on connectivity and digital infrastructure due to the global lockdown increases the opportunities for cyber intrusion and attacks.

Despite this outlook, INTERPOL is taking proactive steps and all relevant measures to support member countries in an unprecedented crisis. It is also preparing for the post COVID-19 threat landscape. The pandemic has created pivotal opportunities to reflect on current capabilities and resources for improvement to achieve better preparedness and resilience for any future shocks.

Finally, the global pandemic has proved the importance of a global response in a collaborative and coordinated manner. The most urgent priority to address these growing cyberthreats is to further enhance international police cooperation for operational activities and to improve cybercrime information exchange with diverse partners within the global ecosystem of cybersecurity.

Focusing on the core pillars of the cybercrime threat response, cybercrime operations and cyber capabilities development, the INTERPOL Cybercrime Directorate will continue to strive to reduce the global impact of cybercrime and protect communities for a safer world.

INTERPOL

ABOUT INTERPOL

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

OUR VISION:
CONNECTING POLICE FOR A SAFER WORLD

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