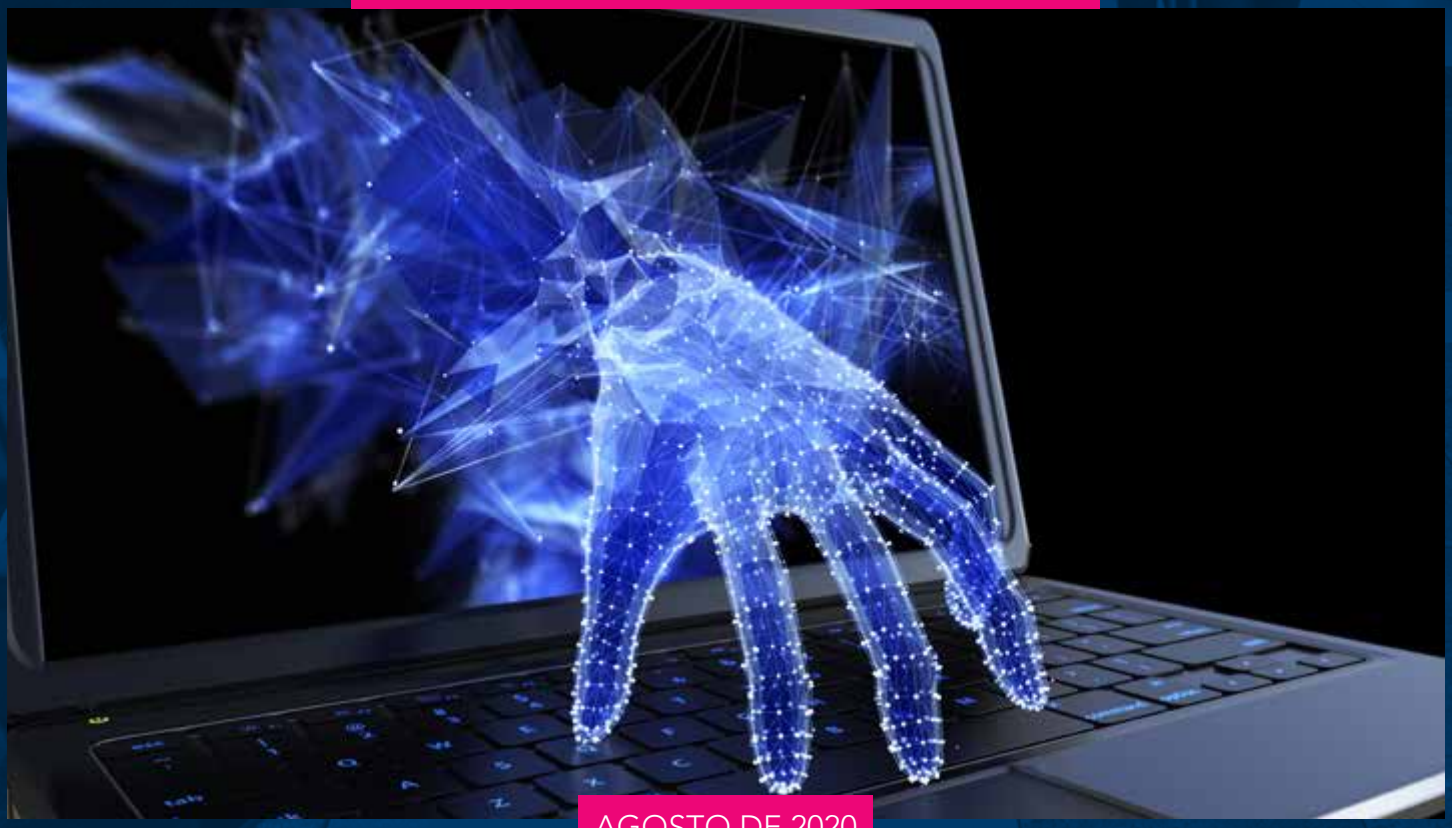
INTERPOL

CIBERDELINCUENCIA:

EFECTOS DE LA COVID-19



AGOSTO DE 2020

Secretaría General de INTERPOL
200, quai Charles de Gaulle
69006 Lyon
Francia

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

ÍNDICE

INTRODUCCIÓN

La pandemia sin precedentes de coronavirus está afectando profundamente al panorama mundial de las ciberamenazas. En todas partes, las fuerzas del orden están siendo sometidas a una presión considerable debido al agravamiento de la crisis sanitaria en el mundo y al fuerte aumento de la actividad delictiva en la red asociada a la COVID-19. Según la información facilitada por uno de los socios de INTERPOL del sector privado, entre enero y el 24 de abril de 2020 se detectaron 907 000 correos basura, 737 incidentes de tipo malware, y 48 000 URL maliciosas, todos ellos relacionados con la COVID-19[1].

Los ciberdelincuentes están cambiando de objetivo, para maximizar el alcance del daño y los ingresos económicos, y, en vez de lanzar sus ataques contra particulares y pequeñas empresas, empiezan a centrarse en las grandes empresas, gobiernos, e infraestructuras esenciales, que juegan un papel fundamental en la respuesta al brote. Al mismo tiempo, debido a la repentina –pero necesaria– instauración del teletrabajo a escala mundial, los diversos organismos han tenido que implementar rápidamente aplicaciones, redes y sistemas remotos. Como consecuencia, los delincuentes aprovechan el aumento de las fallas de seguridad derivadas del teletrabajo para robar datos, lucrarse y causar problemas.

En vista de estos hechos, la Dirección de Ciberdelincuencia de INTERPOL ha aprovechado su exclusivo acceso a datos de los 194 países miembros y de sus socios privados para elaborar el presente Informe de evaluación global sobre los delitos cibernéticos relacionados con la COVID-19, con el que pretende ofrecer una visión completa del panorama de la ciberdelincuencia durante la pandemia. El informe está basado en los datos recogidos de países miembros y socios privados de INTERPOL en el marco de la encuesta mundial de INTERPOL sobre ciberdelincuencia realizada de abril a mayo de 2020. En total, 48 de los 194 países miembros han respondido a la encuesta y 4 de los 13 socios privados han facilitado sus datos para el informe.

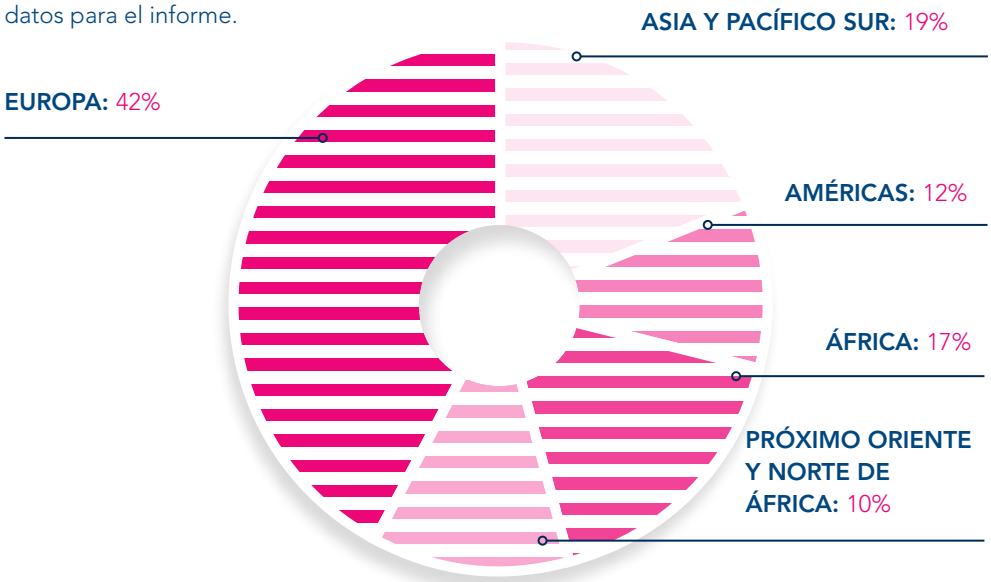


Fig. 1 Encuesta mundial de INTERPOL sobre ciberdelincuencia
Distribución por regiones de los países que han respondido

[1] Trend Micro, consultado el 27 de mayo de 2020 en: https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

El análisis resultante se ha completado con la información dada por los socios del sector privado y los Grupos de Trabajo Regionales de INTERPOL sobre Ciberdelincuencia. Asimismo, el presente documento incluye la información y análisis generados por la unidad de INTERPOL de respuesta a ciberamenazas y su Centro de Intercambio de Información sobre la Ciberdelincuencia, radicado en Singapur e integrado por un equipo formado por agentes policiales y especialistas del sector privado. A continuación figuran las constataciones principales sobre el panorama de la ciberdelincuencia en relación con la pandemia de COVID-19.

- **Las estafas por Internet y el phishing**
  Los autores de las amenazas han visto en la pandemia una oportunidad para aumentar las probabilidades de éxito de sus ataques y han aprovechado la ocasión para revisar sus sistemas habituales de estafas por Internet y phishing. Ahora envían a sus víctimas unos correos electrónicos de phishing sobre la COVID-19, a menudo haciéndose pasar por autoridades gubernamentales y sanitarias, en los que les incitan a facilitar sus datos personales y a descargarse contenidos maliciosos.

- **Los malwares disruptivos (ransomware y DDoS)**
  Alentados por la probabilidad de causar graves problemas y obtener sustanciosas ganancias, los ciberdelincuentes han multiplicado el número de ataques de malware disruptivos contra las infraestructuras esenciales y sanitarias. Los ataques de tipo ransomware o DDoS pueden provocar interrupciones frecuentes o la interrupción total de la actividad comercial, así como la pérdida temporal o permanente de información esencial.

- **Los malware de recolección de datos**
  En el ámbito de la ciberdelincuencia también están en auge los ataques de malware para recolectar datos, como los troyanos de acceso a distancia, los ladrones de información, los spyware (programas espía) o los troyanos bancarios, entre otros. Los autores de las amenazas utilizan información relacionada con la COVID-19 como señuelo para infiltrarse en los sistemas e infectar redes, sustraer datos, desviar fondos y crear botnets.

- **Dominios malignos**
  Se ha producido un aumento considerable del número de ciberdelincuentes que, aprovechando el incremento de la demanda de productos médicos e información sobre la COVID-19, registran nombres de dominio que contienen palabras clave relacionadas con la pandemia, como "coronavirus" o "COVID". Se trata de sitios web fraudulentos que esconden una amplia variedad de actividades malignas, por ejemplo, servidores C2, difusión de malware y phishing.

- **Desinformación**
  Asistimos a una amplificación de la desinformación y noticias falsas que se propagan rápidamente entre la población. Alimentadas por la incertidumbre de la situación socioeconómica en el mundo, la información no contrastada, las amenazas mal entendidas, y las teorías de la conspiración han fomentado la ansiedad de los ciudadanos y, en algunos casos, facilitado la ejecución de ciberataques.

EVOLUCIÓN DE LAS TENDENCIAS Y AMENAZAS EN MATERIA DE CIBERDELINCUENCIA DURANTE LA COVID-19

Tendencias de la ciberdelincuencia por regiones

Si bien durante la pandemia de COVID-19 la ciberdelincuencia se ha multiplicado por todo el mundo, las tendencias delictivas varían de una región a otra. A continuación se presenta por regiones el panorama de las ciberamenazas en el contexto de la COVID-19.

ÁFRICA

- Los países miembros de África que han respondido a la encuesta han destacado que, desde el inicio de la pandemia, se ha producido un aumento de los pagos por medios electrónicos, sin efectivo, lo que ha incrementado la exposición de las personas a los ataques cibernéticos.
- La mayoría de organismos y empresas han aplicado una política de teletrabajo, si bien las vulnerabilidades de estos acuerdos han provocado una ola de ataques de phishing sobre la temática adecuada, extorsiones sexuales, y estafas con organizaciones de caridad falsas.
- Se ha producido un aumento del número de noticias falsas sobre la COVID-19 que circulan en los medios sociales.
- El número de actuaciones emprendidas por las alianzas público-privadas para combatir la ciberdelincuencia ha sido relativamente bajo, lo que ha contribuido a una subida de los delitos cibernéticos sin resolver.

AMÉRICAS

- Los países que han respondido a la encuesta han informado del fuerte aumento de casos de phishing y de campañas de estafas en relación con la COVID-19 que aprovechan la crisis del coronavirus y el consiguiente confinamiento.
- Como muchas empresas de la región de las Américas han introducido el teletrabajo, los ciberdelincuentes se centran cada vez más en los empleados para conseguir un acceso remoto a las redes corporativas y hacerse con su control, con miras a robar información confidencial.
- Actualmente, las medianas empresas de algunos países de esta región están siendo víctimas de una campaña de ransomware, perpetrada principalmente por medio del malware Lockbit.
- Los delincuentes están intensificando el uso de los medios sociales para la explotación sexual de menores a través de Internet. En concreto, los malhechores que se mueven dentro de las redes de explotación sexual de menores en Internet están aprovechando el confinamiento mundial para localizar y contactar con sus víctimas en los medios sociales. Al mismo tiempo, se ha intensificado el intercambio de imágenes de explotación sexual de menores.

ASIA Y PACÍFICO SUR

- En la región de Asia y Pacífico Sur las tendencias predominantes son las campañas de estafas y phishing relacionadas con la COVID-19, así como la venta ilegal en línea de productos médicos, medicamentos, y equipos de protección individual falsos.
- Los ciberdelincuentes están aprovechando las fallas de seguridad de las aplicaciones para teleconferencias.
- La mayoría de los países de esta región que han participado en la encuesta han informado de la circulación de noticias falsas y de la desinformación en relación con la COVID-19.
- Uno de los principales problemas destacados en esta región ha sido la falta de higiene y sensibilización en materia de seguridad cibernética.

EUROPA

- Dos tercios de los países miembros de Europa han informado del considerable aumento de dominios maliciosos registrados con las palabras clave "COVID" o "corona" para sacar partido del número creciente de personas que buscan información en Internet sobre la COVID-19.
- Los ciberdelincuentes están aprovechando la pandemia para lanzar ataques de ransomware contra las infraestructuras esenciales e instituciones sanitarias encargadas de hacer frente a la COVID-19.
- Cada vez hay más casos de clonación de sitios web gubernamentales para robar datos confidenciales de usuarios y después utilizarlos en otros ciberataques.
- Los organismos encargados de la aplicación de la ley europeos han registrado una proliferación de las campañas de phishing.

PRÓXIMO ORIENTE Y NORTE DE ÁFRICA

- Esta región ha destacado la intensificación del uso de los medios sociales para propagar noticias falsas relacionadas con la COVID-19.
- Las plataformas de medios sociales se utilizan a menudo para la venta ilegal de productos farmacéuticos y de parafarmacia relacionados con el coronavirus.
- Se ha detectado un aumento de los registros de dominios maliciosos que afirman ofrecer estadísticas sobre la COVID-19.
- Se ha detectado un aumento del número de casos de estafas por Internet y phishing vinculados a la pandemia de COVID-19.

PRINCIPALES CIBERAMENAZAS RELACIONADAS CON LA COVID-19

Sobre la base del exhaustivo análisis de los datos facilitados por los países miembros, los socios privados, y el Centro de Intercambio de Información sobre la Ciberdelincuencia, a continuación se presentan las principales ciberamenazas identificadas en relación con la pandemia de COVID-19.

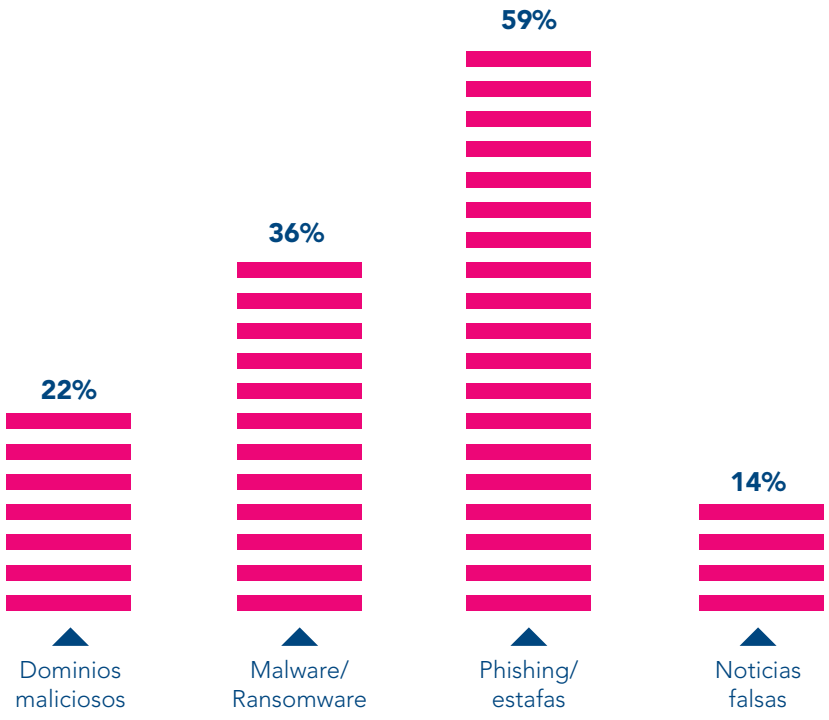


Fig. 2 Proporción de las principales ciberamenazas relacionadas con la COVID-19 calculada a partir de la información dada por los países miembros

Estafas por Internet y phishing

En torno a dos tercios de los países miembros que han respondido a la encuesta han informado de la proliferación del uso de temáticas relacionadas con la COVID-19 en delitos de phishing y estafas por Internet desde el brote de la pandemia. Trend Micro, uno de los socios privados de INTERPOL, ha detectado 907 000 mensajes relacionados con la COVID-19 desde enero de 2020[2]. Los ciberdelincuentes han aprovechado la recesión económica y la ansiedad que padecen las personas para perfeccionar sus tácticas de ingeniería social, utilizando la COVID-19 como eje de sus ataques. En concreto, muchos de los grupos delictivos organizados han cambiado sus métodos para explotar en beneficio propio la información sobre la pandemia y la escasez de suministros, recurriendo también a la promoción de medicamentos falsos, paquetes fiscales, y prestaciones de urgencia.

[2] Trend Micro, consultado el 19 de abril de 2020: https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

Un amplio porcentaje de los casos denunciados ante las autoridades policiales han sido incidentes en los que los autores de las amenazas enviaban correos de tipo phishing relacionados con la COVID-19 para solicitar credenciales y contraseñas de usuarios. A menudo, este tipo de correos suplantan la identidad de autoridades gubernamentales y sanitarias legítimas y simulan dar información y recomendaciones relacionadas con la pandemia. Además de esta relación directa con noticias sobre la pandemia, Kaspersky, socio privado de INTERPOL, ha señalado la actividad de delincuentes que ofrecen a sus víctimas una bonificación fiscal a causa de la COVID-19 para persuadirlas de que naveguen por sitios web fraudulentos que recopilan la información financiera y fiscal de los incautos usuarios.

Así pues, los correos de tipo phishing supuestamente enviados por los Ministerios de la Salud o la Organización Mundial de la Salud contienen archivos adjuntos infectados, que aprovechan las vulnerabilidades para ejecutar códigos maliciosos. Los países miembros y los socios privados de INTERPOL han detectado que los correos de tipo phishing hacen un uso generalizado de programas maliciosos como Emotet, Trickbot, y Cerberus, específicamente diseñados para el robo de información.

Según la información facilitada por los socios privados, las estafas a empresas por correo electrónico mediante suplantación de identidad (BEC) siguen siendo la opción preferida de muchos de los autores de las amenazas. Para perpetrar sus ataques, han adaptado sus métodos al actual contexto de COVID19 y ahora, por ejemplo, usan direcciones de correo electrónico de proveedores y clientes o direcciones que son casi idénticas. La extrema necesidad de suministros y productos sanitarios esenciales ofrece a los delincuentes una ocasión ideal para obtener datos o desviar millones de dólares hacia cuentas ilegales.

De acuerdo con la información facilitada por los países miembros y socios privados, estos son los principales temas relacionados con la COVID-19 utilizados en los correos de tipo phishing:

- correos electrónicos procedentes de autoridades sanitarias nacionales o mundiales;
- normas estatales e iniciativas de apoyo económico;
- solicitudes de pago y devoluciones de dinero falsas;
- ofertas de vacunas y productos médicos;
- aplicaciones de rastreo de COVID-19 para teléfonos móviles;
- ofertas de inversión y de compra de acciones;
- peticiones de donaciones y de organizaciones de caridad relacionadas con la COVID-19.

De manera general, con la COVID-19 y el consiguiente confinamiento los correos de tipo phishing relacionados con el coronavirus han ido cobrando fuerza, prevaliéndose del miedo, embaucando a las personas más vulnerables y aprovechando la inestabilidad en el lugar de trabajo.

MALWARE DISRUPTIVO (RANSOMWARE Y DDOS)

El malware ha adaptado su configuración al brote del coronavirus y en la actualidad asistimos a una proliferación del número de ataques contra un mayor abanico de objetivos. Sobre la

base del análisis del Centro de Intercambio de Información sobre la Ciberdelincuencia y su apoyo a los países miembros, las campañas de malware disruptivos están cambiando de objetivo principal; ahora, en vez de atacar a particulares y pequeñas empresas, se concentran en los organismos gubernamentales y el sector sanitario, a los que se les puede exigir el pago de cuantías más elevadas.

Varios países miembros han denunciado haber sufrido ataques de malware contra infraestructuras esenciales de organismos gubernamentales, hospitales y centros médicos, que están desbordados por la crisis sanitaria. Estos ataques de ransomware o denegación de servicio (DDoS) pretenden impedir el acceso a los datos o perturbar el funcionamiento del sistema, agravando una situación ya de por sí muy difícil.

Según el Centro de Intercambio de Información sobre la Ciberdelincuencia, los ataques con ransomware perpetrados por distintos grupos delictivos, que en meses anteriores se habían mantenido relativamente latentes, alcanzaron su punto álgido en las dos primeras semanas de abril de 2020; ello significa que puede que a día de hoy todavía existan organismos que están infectados, pero cuyo ransomware no ha sido activado. Las investigaciones de las fuerzas del orden apuntan a que los atacantes llevan a cabo primero una minuciosa inspección de las redes de las entidades que se han fijado como objetivo para poder estimar con bastante exactitud la cantidad máxima que pueden solicitar como rescate. Cuando se activa el ransomware en un sitio estratégico de la red para que cause la máxima perturbación en el proceso de trabajo, dichas entidades se suelen ver obligadas a pagar el rescate. Estos ataques pueden combinarse con la extracción de información confidencial, que luego puede servir para ejercer más presión sobre el pago.

Las principales familias de ransomware detectadas recientemente por los socios privados de INTERPOL son CERBER, NetWalker, y Ryuk, las cuales están en continua evolución para maximizar el daño que pueden provocar con un único ataque y las ganancias de los delincuentes.

Al igual que ha sucedido con las campañas de ransomware, se han multiplicado las denuncias recibidas en el Centro de Intercambio de Información sobre la Ciberdelincuencia sobre ataques de DDoS, cuya finalidad es perturbar el funcionamiento de distintos organismos y servicios esenciales. En este caso, los ciberdelincuentes sobrecargan los portales de servicio en línea con más tráfico del que el servidor o la red pueden soportar y amenazan con cerrar los sitios web objetivo, a menos que reciban una transferencia de fondos en sus cuentas.

Los ataques con ransomware y DDoS pueden tener distintos resultados, como, por ejemplo, la perturbación de la actividad, el bloqueo de sistemas esenciales y la pérdida de datos, lo que puede provocar pérdidas económicas como consecuencia del tiempo de inactividad y de la restauración de los sistemas y archivos.

DOMINIOS MALICIOSOS

Más de un tercio de los países miembros están controlando el número creciente de nuevos registros de dominio con las palabras clave "COVID" o "Corona". Al igual que sucede con las campañas de tipo phishing relacionadas con la COVID-19, un alto porcentaje de los dominios que afirman ofrecer información actualizada, sistemas de rastreo o estadísticas sobre la

COVID-19 se utilizan para perpetrar una amplia variedad de actividades malintencionadas, aprovechando la sed de información de las personas durante la pandemia. A finales de marzo de 2020, se detectaron 116 357 nuevos registros de dominio sobre la COVID, de los cuales 2 022 fueron identificados como maliciosos y 40 261 como de "alto riesgo"[3]. En junio de 2020, el Grupo Especial Mundial dedicado a los Dominios Maliciosos de la Dirección de Ciberdelincuencia de INTERPOL identificó y analizó 200 000 dominios maliciosos de los que habían sido víctimas más de 80 países miembros.

Los nuevos registros de dominios maliciosos bien almacenan datos que capturan malware, bien han sido diseñados para obtener información de identificación personal, y abordan a sus víctimas con campañas de mensajes no deseados orquestadas a través de correos electrónicos, mensajes de texto, o llamadas no solicitadas. Entre febrero y marzo de 2020, Palo Alto Networks, uno de los socios privados de INTERPOL, detectó que los registros maliciosos –malware y phishing incluidos– habían aumentado un 569 %, mientras que los registros de alto riesgo –que engloban estafas, minado no autorizado de monedas, y dominios sobre los que existen pruebas de asociación con URL maliciosas– han subido un 788 %. El incremento de registros es consecutivo al pico que alcanzó el interés de los usuarios por cuestiones relacionadas con la COVID-19, identificado por Google Trends unos días después[4].

La información adicional facilitada por los organismos encargados de la aplicación de la ley precisa que algunos de los sitios web maliciosos habían sido creados con el fin de simular ser servicios públicos oficiales, como portales gubernamentales, empresas de telecomunicaciones, bancos, autoridades nacionales fiscales y aduanas, entre otros. Esta tendencia fue desvelada por un país miembro que puso en marcha una iniciativa nacional para prestar ayuda económica rápida a autónomos y pequeñas empresas. Para poder percibirla, los empresarios debían presentar su solicitud en un sitio web gubernamental oficial. Los autores de amenazas se apresuraron a replicar estos sitios web y diseñaron una aplicación falsa para recopilar los datos de usuario personales que enviaban los solicitantes.

Otra tendencia que suscita preocupación es el número creciente de sitios web fraudulentos, que aprovechan el reciente aumento de la demanda de mascarillas quirúrgicas, equipos de protección individual, kits de detección del coronavirus, y ventiladores médicos para comerciar ilegalmente con estos productos esenciales. Los propietarios de estos sitios web utilizan estrategias distintas, como copiar un sitio web legítimo, vender artículos no autorizados o falsificados, o cobrar por artículos que luego no entregan. Además, existe el problema adicional que supone la transferencia a cuentas extranjeras de los fondos abonados por las víctimas de la venta ilegal, ya que dificulta la atribución del delito y la recuperación de las pérdidas económicas.

MALWARE DE RECOLECCIÓN DE DATOS

La encuesta mundial sobre ciberdelincuencia reveló una concentración considerable del uso de malware de recolección de datos con información relacionada con la COVID-19 como señuelo. Los autores de las amenazas engañaban a los usuarios para que ejecutaran algún tipo de malware, como troyanos de acceso a distancia, ladrones de información, spyware (programas espía)[5]

[4] Palo Alto Networks, consultado el 24 de abril de 2020: https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/

[5] Group IB, consultado el 26 de abril de 2020: https://www.group-ib.com/media/covid-phishing-campaings/

y troyanos bancarios, y así infectar las redes, recopilar datos, desviar sumas de dinero y crear botnets. Las campañas de phishing sobre la COVID-19 han facilitado en gran medida la instalación de archivos ejecutables maliciosos. Se ha observado asimismo que el malware se instala a través de enlaces incrustados en mapas interactivos de coronavirus, aplicaciones temáticas y sitios web fraudulentos.

Uno de los ejemplos más destacados de malware de recolección de datos señalados por nuestros socios del sector privado es Emotet, cuya propagación ha aumentado considerablemente desde el principio de la pandemia. Los investigadores de IBM X-Force detectaron que los ciberdelincuentes estaban haciendo un uso intensivo del troyano Emotet en Japón, haciéndose pasar por proveedores de servicios de asistencia a personas discapacitadas[6]. En sus correos electrónicos de phishing, los autores de las amenazas animaban a sus víctimas a abrir archivos adjuntos que, supuestamente, contenían medidas para prevenir la COVID-19, pero que en realidad infectaban sus ordenadores con Emotet. Muchas personas fueron víctimas de este engaño, ya que parecía que los mensajes habían sido enviados desde la dirección de correo oficial del proveedor de servicio, cuya dirección y número de teléfono aparentaban ser legítimos. Mientras examinaban este mismo caso, los investigadores de Kaspersky especializados en estas amenazas descubrieron que el troyano Emotet suele enviarse dentro de un archivo adjunto al correo electrónico en formato .pdf, .mp4, y .docx, que afirma contener información útil sobre el coronavirus, como pueden ser las últimas novedades, medidas de protección, y métodos de detección del virus[7]. Este tipo de ataques han sido especialmente eficaces porque los ciberdelincuentes han elegido el momento adecuado para propagar el malware, cuando la gente se sentía ansiosa e insegura. Como resultado, en los últimos meses se ha producido el robo de una cantidad considerable de datos personales. El 13 % de los organismos de todo el mundo se han visto afectadas por Emotet, que en enero de 2020 pasó a encabezar la lista de familias de malware de recolección de datos más destacadas[8].

Trickbot es otro malware de recolección de datos que, a raíz de la pandemia, se ha propagado considerablemente. Según un estudio reciente elaborado por Microsoft, Trickbot ha sido identificado como el malware más prolífico utilizado en combinación con engaños relacionados con la COVID-19[9]. Al parecer, desde que comenzó la pandemia su relación con correos electrónicos de tipo phishing es mayor que la de ningún otro programa malicioso. Las víctimas también lo recibían en forma de archivo adjunto en mensajes enviados por organizaciones sin ánimo de lucro falsas que ofrecían test de COVID19 gratuitos.

6 IBM, consultado el 24 de abril de 2020: https://exchange.xforce.ibmcloud.com/collection/18f373debc38779065a26f1958dc260b

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

8 Check Point Technologies, consultado el 6 de julio de 2020: 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

DESINFORMACIÓN

A mediados de febrero de 2020, la Organización Mundial de la Salud (OMS) advirtió de que la COVID19 venía acompañada de una "infodemia" de desinformación. El organismo de la ONU alertó del grave riesgo que entraña la desinformación sobre la pandemia, una práctica casi igual de peligrosa que el propio virus[10].

Según un informe mundial del Reuters Institute, los temas relacionados con la COVID-19 más comunes que han aparecido en la ola de noticias falsas y desinformación son los siguientes[11]:

- actuación de las autoridades públicas;
- contagio de la población;
- noticias sobre cuestiones médicas generales;
- figuras destacadas;
- teorías de la conspiración;
- transmisión del virus;
- preparación pública;
- desarrollo de la vacuna.

El 27 % de los países que han contestado a la encuesta mundial sobre ciberdelincuencia han confirmado la circulación de información falsa sobre la COVID-19 entre su población y el 21 % ha manifestado una preocupación creciente ante esta tendencia. En el periodo de un mes, un país miembro informó de 290 publicaciones y, en la mayoría de los casos, esas publicaciones ocultaban malware.

La información se ha difundido principalmente a través de los medios sociales (WhatsApp, Facebook, o Twitter, entre otros) y contenía afirmaciones, rumores y especulaciones falsos sobre la cambiante situación de la COVID-19. Algunos de los organismos encargados de la aplicación de la ley que han respondido a la encuesta precisaron que, en sus países, la desinformación estaba vinculada al comercio ilegal de productos médicos fraudulentos.

Algunos países miembros han manifestado su preocupación por el hecho de que la desinformación estaba propagando entre la población el pánico y los desórdenes sociales, ya de por sí exacerbados por la pandemia. Las autoridades policiales denunciaron casos de información falsa divulgada en Internet sobre el número de personas contagiadas y la emergencia ocasionada por el virus en zonas no afectadas por él.

[10] OMS, consultado el 21 de mayo de 2020: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf

[11] Reuters Institute, consultado el 22 de mayo de 2020 en: https://reutersinstitute.politics.ox.ac.uk/research

También ha habido casos de desinformación relacionados con estafas a través de mensajes de texto que ofrecían servicios y productos que parecían demasiado buenos para ser verdad, por ejemplo, alimentos gratuitos, ventajas especiales, o grandes descuentos en supermercados. Los organismos encargados de la aplicación de la ley creen que la mayoría de los mensajes se difundieron entre la población para provocar reuniones masivas de personas y aprovechar esa coyuntura.

Fig. 3: Alerta publicada por la OMS en la que advierte a la población de las noticias falsas sobre la COVID-19 difundidas por WhatsApp[12]

RESPUESTA DE INTERPOL

Ante los rápidos cambios registrados en el ámbito de la ciberdelincuencia durante la pandemia de COVID-19, INTERPOL está elaborando y dirigiendo la respuesta de las fuerzas del orden de todo el mundo a los consecuentes delitos cibernéticos. La Dirección de Ciberdelincuencia de INTERPOL ha estado trabajando en distintos escenarios con los países miembros, los socios del sector privado, y la comunidad especializada en ciberseguridad de todo el mundo.

A fin de ayudar a sus países miembros a prevenir y combatir la ciberdelincuencia durante la pandemia, INTERPOL ha adoptado las siguientes medidas, algunas de las cuales siguen vigentes:

- Organización de reuniones virtuales urgentes con diversas partes interesadas para prestar servicios adaptados a las necesidades de los países miembros, con el fin de prevenir, detectar e investigar la ciberdelincuencia relacionada con la COVID-19. En el marco de esta iniciativa se han celebrado reuniones estratégicas con los Jefes de las Unidades de Ciberdelincuencia nacionales y regionales y con el Grupo Mundial de INTERPOL de Especialistas en Ciberdelincuencia[13].

[12] OMS, consultado el 21 de mayo de 2020 en: https://www.who.int/india/emergencies/coronavirus-disease-(covid-19)/fake-news-alert

[13] El Grupo Mundial de INTERPOL de Especialistas en Ciberdelincuencia es una red integrada por personas especializadas en esta materia procedentes de países miembros, empresas del sector privado, organismos públicos, y el mundo académico. Dentro de ella intercambian información y buenas prácticas y se encargan de asesorar a la Secretaría General de INTERPOL respecto de la elaboración de políticas y la aplicación de proyectos en el ámbito cibernético.

- INTERPOL también participa activamente en debates multilaterales estratégicos organizados por el Foro Económico Mundial[14] para formar coaliciones y una alianza contra la ciberdelincuencia. También es miembro del Consejo asesor del Centro para la Ciberseguridad del Foro Económico Mundial.

- Publicación de **notificaciones moradas de INTERPOL**[15] para informar a la comunidad policial de las ciberamenazas emergentes y de alto riesgo. Estas alertas mundiales, comunicadas a través de la red protegida de INTERPOL, han tratado sobre los siguientes delitos[16]:

  - **Ataques de ransomware contra infraestructuras esenciales y hospitales:** El Centro de Intercambio de Información sobre la Ciberdelincuencia de INTERPOL ha detectado intentos de infectar organismos e infraestructuras esenciales en materia de asistencia contra la COVID-19 y de ejecutar ataques de ransomware contra ellas.

  - **Uso y propagación de troyanos bancarios:** Un troyano bancario ha aprovechado las fallas de un servicio nacional para suplantar a esta entidad y enviar mensajes de texto relacionados con la COVID-19 para propiciar la descarga de un enlace malicioso incrustado.

  - **Envío de dispositivos USB maliciosos:** El Centro de Intercambio de Información sobre la Ciberdelincuencia ha recopilado información sobre los nuevos vectores de ataque de un grupo de ciberdelincuentes, que se ha dedicado a enviar como "obsequio" unos USB maliciosos a empresas a fin de acceder a sus redes y robarles información confidencial.

  - **Uso y propagación de un malware de tipo troyano:** Este software malicioso, llamado "Coronavirus", inutiliza los discos sobrescribiendo el registro de arranque principal.

- Creación de un **Grupo Especial Mundial dedicado a los Dominios Maliciosos.** Este grupo está compuesto por funcionarios de las fuerzas del orden especializados en ciberdelincuencia, especialistas de nuestros socios del sector privado y funcionarios policiales nacionales. Su finalidad es perseguir e identificar a los autores de amenazas y las infraestructuras más comunes que están detrás de los dominios maliciosos, a fin de interrumpir su actividad y mitigar este tipo de amenazas.

  A fecha de junio de 2020, el Grupo Especial había identificado y analizado en torno a 200 000 dominios maliciosos. A partir de los resultados obtenidos, la Dirección de Ciberdelincuencia difundió unos informes sobre ciberdelincuencia con datos pertinentes para los más de 80 países miembros afectados por estas amenazas.

  - Dirección de una **campaña mundial de sensibilización sobre las ciberamenazas vinculadas a la COVID-19, #WashYourCyberHands**. Esta campaña fue lanzada en mayo de 2020 con la colaboración de los países miembros y 23 socios externos,

[14] Foro Económico Mundial, consultado el 14 de julio de 2020: 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 publica notificaciones moradas para que los países miembros soliciten o faciliten información sobre modus operandi, objetos, dispositivos y métodos de ocultación utilizados por los delincuentes.

[16] Los detalles de las notificaciones moradas se han eliminado debido a las operaciones contra la ciberdelincuencia de INTERPOL actualmente en curso.

con la finalidad de alertar al público sobre las principales amenazas relacionadas con la pandemia de coronavirus y de promover una buena "higiene" cibernética. Esta campaña tiene por objetivo garantizar la seguridad de la población frente a los ciberdelincuentes que tratan de aprovechar el brote de la enfermedad para robar datos, provocar perturbaciones o estafar, y ha ayudado a la labor llevada a cabo por las fuerzas del orden nacionales contra la creciente cantidad de ciberamenazas relacionadas con la COVID-19. Los materiales visuales y las publicaciones en medios sociales creados por INTERPOL y sus colaboradores llegaron a unos 7,5 millones de usuarios en línea. Solo en Twitter (@INTERPOL_Cyber), la etiqueta de la campaña, **#WashYourCyberHands**, fue mencionada unas 10 000 veces.

PRIORIDADES Y RECOMENDACIONES

A fin de garantizar la máxima eficacia del apoyo y los servicios ofrecidos por INTERPOL a sus países miembros para mitigar las ciberamenazas relacionadas con la COVID-19, se han identificado las siguientes prioridades y recomendaciones.

- **Favorecer el rápido intercambio de información.** Al disponer de la información más reciente sobre los nuevos ciberataques identificados, la Dirección de Ciberdelincuencia puede anticipar con exactitud las tendencias emergentes y comunicar los modus operandi de los delincuentes a través de la red mundial de INTERPOL, favoreciendo así la sensibilización y prevención. Esta práctica es especialmente útil en los casos de ataques de ransomware contra los gobiernos, las infraestructuras esenciales y el sector sanitario, porque pueden suponer un gran peligro para la seguridad pública y ocasionarle un daño grave. El hecho de recibir rápidamente la información pertinente permite a INTERPOL ayudar a sus países miembros con la elaboración y aplicación de una respuesta efectiva.
- **Mejorar la colaboración policial y la cooperación entre los países miembros.** Habida cuenta de la evolución de las ciberamenazas transnacionales derivadas de la COVID-19, INTERPOL quiere destacar la importancia de la colaboración entre las autoridades policiales nacionales y la rápida respuesta a las solicitudes de información formuladas por otros países. La cooperación y el intercambio de información son especialmente importantes para combatir las siguientes ciberamenazas:
  - ataques de ransomware contra infraestructuras esenciales, indicadores de compromiso, direcciones bitcóin;
  - casos relacionados con la estafa de pago por anticipado y la estafa BEC;
  - propagación de malware a través de aplicaciones no gubernamentales de rastreo de contactos;
  - información detallada en torno a campañas que aprovechan un alto volumen de dominios maliciosos.

- **Usar la Plataforma Colaborativa de INTERPOL sobre Ciberdelincuencia[17].** La plataforma ha sido diseñada para intercambiar información y coordinar operaciones, de manera que los países miembros dispongan de una solución segura para participar en equipos especiales conjuntos integrados por partes interesadas de distintos países a fin de combatir la ciberdelincuencia. Facilita la comunicación directa entre los equipos operativos de los países miembros y con INTERPOL, favoreciendo así un intercambio efectivo de información sobre ciberdelincuencia que permitirá formular una rápida respuesta operativa a estas perturbaciones.

- **Aplicar medidas de prevención y sensibilizar a la población.** La evolución prevista de las ciberamenazas relacionadas con la COVID-19 indica que continuarán planteando problemas de índole legal y operativa a los organismos encargados de la aplicación de la ley de todo el mundo. Para poder mitigarlos es fundamental favorecer la prevención tratando de instruir en la materia a la población y de ofrecerle los recursos oportunos para garantizar su seguridad en la red. Así pues, se anima a los países miembros a usar las plataformas de medios sociales para difundir entre la población los mensajes clave de la campaña mundial de INTERPOL, #WashYourCyberHands, y a lanzar campañas de sensibilización similares a escala nacional.

- **Mejorar la capacidad de investigación de delitos cibernéticos.** Ante la constante evolución de las ciberamenazas, ya sea en relación directa o indirecta con la pandemia, es especialmente importante que los organismos encargados de la aplicación de la ley dispongan de capacidades y tecnologías especializadas. INTERPOL ha reconocido la importancia de perfeccionar la experiencia de sus países miembros durante la crisis mundial, por eso ha creado la **Academia Mundial Virtual**, una plataforma desde la que ofrece una amplia variedad de cursos dirigidos a las fuerzas del orden. La Dirección de Ciberdelincuencia de INTERPOL organiza cursos en línea y seminarios web para mejorar las capacidades de los países miembros con miras a hacer frente a las ciberamenazas emergentes, así como para que puedan investigar satisfactoriamente los delitos cibernéticos durante la crisis mundial y después de ella.

- **Reforzar las alianzas público-privadas.** Desde que comenzó la pandemia de COVID-19, las alianzas público-privadas han sido un elemento clave para contrarrestar las ciberamenazas emergentes. Las empresas del sector privado pueden ser un valioso aliado para los organismos encargados de la aplicación de la ley ya que intercambian información y experiencia sobre las últimas tendencias y prestan asistencia técnica.
  A este respecto, desde enero de 2020 la Dirección de Ciberdelincuencia de INTERPOL ha ido acumulando información y datos sobre las ciberamenazas relacionadas con la COVID-19 facilitados por los países miembros, los socios privados de INTERPOL, los equipos nacionales de respuesta a emergencias informáticas, y la Corporación para la Asignación de Nombres y Números en Internet (ICANN), pero también por grupos de intercambio de información en línea, como Slack. La variada cartera de socios alimentó las series de datos, cuya utilidad quedó demostrada al ofrecer la ayuda necesaria y oportuna a los países miembros.

[17] La Plataforma Colaborativa de INTERPOL sobre Ciberdelincuencia está dentro de la sección de Ciberdelincuencia del Centro Global de Conocimiento de INTERPOL y utiliza la tecnología de la Plataforma Colaborativa Segura.

INTERPOL reconoce la eficacia de estas colaboraciones y quiere crear una base de datos alimentada por todas las partes interesadas, las cuales también tendrán acceso a ella, para formular la solución más efectiva contra las ciberamenazas.
Por último, el hecho de que las fuerzas del orden y el sector privado estrechen su relación forja un sentimiento de responsabilidad compartida en la lucha contra las ciberamenazas relacionadas con la COVID-19, y permite una respuesta rápida y adaptada a los delitos cibernéticos emergentes.

- **Crear y aplicar estrategias nacionales contra la ciberdelincuencia.** En la última encuesta de INTERPOL se ha observado que 30 países miembros carecían de una estrategia nacional contra la ciberdelincuencia para responder a la pandemia de COVID-19. Este hallazgo pone de relieve la necesidad de crear este tipo de estrategia para reforzar la resistencia de los servicios e infraestructuras nacionales, lo que ayudará a los países a contrarrestar las ciberamenazas de manera eficaz y a proteger a la población de las violaciones de seguridad de datos durante la crisis mundial y después de ella.

PREVISIONES A CORTO PLAZO

Tras analizar las aportaciones de los organismos encargados de la aplicación de la ley y de las empresas del sector privado, parece probable aventurar que el panorama de las ciberamenazas continuará deteriorándose. La Dirección de Ciberdelincuencia de INTERPOL ha hecho las siguientes previsiones en las que se destaca cuáles son los ámbitos de preocupación más probables.

- La COVID-19 sigue siendo una realidad a escala mundial, con lo que es altamente probable que la ciberdelincuencia siga aumentando próximamente. Es muy posible que, movidos por las vulnerabilidades asociadas al teletrabajo y la posibilidad de obtener una mayor ganancia económica, los ciberdelincuentes consoliden su actividad y conciban unos modus operandi más avanzados y complejos.
- Lo más probable es que los ciberdelincuentes continúen aprovechando las vulnerabilidades asociadas a las políticas de teletrabajo y traten de robar los datos de acceso de los empleados a través de software y herramientas ofimáticas esenciales. Los datos de carácter personal robados también pueden usarse para perpetrar otros ataques cibernéticos.
- Otro de los factores que favorece la generalización de la ciberdelincuencia son los efectos que el confinamiento impuesto por causa de la pandemia están teniendo en otros ámbitos delictivos, lo que hace que los malhechores busquen fuentes de ingresos alternativas. Así, es probable que algunos delincuentes aprovechen los mercados de la red oscura para ofrecer "ciberdelitos como servicio" para facilitar la entrada a estos delitos.
- Es probable que, para aprovechar el pánico generado por la pandemia, los autores de amenazas continúen propagando estafas por Internet y campañas de tipo phishing relacionadas con el coronavirus. Asimismo, también es posible que aumenten las estafas BEC, como consecuencia de la recesión económica y los cambios que se han producido en el panorama empresarial, lo que generará nuevas oportunidades para la comisión de delitos.

- Además, una vez que el tratamiento o la vacuna contra la COVID-19 estén disponibles, es muy probable que se produzca un repunte del phishing en relación con estos productos médicos, así como de las intrusiones en la red y de los ciberataques para robar datos.
- Es probable que los ataques de ransomware dirigidos contra el sector sanitario y las cadenas de suministro relacionadas se intensifiquen, empujados por la diversificación de los vectores de ataque.
- Se prevé que los autores de amenazas traten de hacerse con la información personal de los particulares, haciéndose pasar por proveedores de contenidos digitales y aprovechándose de ellos.
- Incluso cuando los casos de coronavirus hayan disminuido, los ciberdelincuentes seguramente adaptarán sus estafas para sacar partido de la situación posterior a la pandemia y aprovecharse del mayor número posible de víctimas.

CONCLUSIÓN

Los ciberdelincuentes están creando nuevos ataques e intensificando su ejecución a un ritmo alarmante, aprovechándose del miedo y la incertidumbre provocados por la inestabilidad de la situación socioeconómica a escala mundial. Al mismo tiempo, las medidas de confinamiento impuestas en el mundo han propiciado una mayor dependencia de la conectividad y las infraestructuras digitales, lo que aumenta las oportunidades de llevar a cabo intrusiones y ataques cibernéticos.

Sin embargo, a pesar de este panorama, INTERPOL ha adoptado una postura proactiva y está tomando todas las medidas pertinentes para respaldar a los países miembros en una crisis sin precedentes. Asimismo, se está preparando para las amenazas que se prevén después de la COVID-19. La pandemia ha dado lugar a ocasiones decisivas para reflexionar sobre las capacidades disponibles actualmente y los recursos para mejorarlas a fin de lograr una mejor preparación y resistencia ante cualquier crisis futura.

Por último, la pandemia mundial ha demostrado la importancia de una respuesta global sustentada en la colaboración y coordinación. La prioridad más urgente para combatir el recrudecimiento de las ciberamenazas es seguir potenciando la cooperación policial internacional en el ámbito de las operaciones y mejorar el intercambio de información sobre ciberdelitos con distintos socios del ecosistema mundial de la ciberseguridad.

La Dirección de Ciberdelincuencia de INTERPOL está concentrada en los principales pilares de la respuesta a las ciberamenazas, las operaciones contra la ciberdelincuencia y el desarrollo de capacidades de lucha contra la ciberdelincuencia, y continuará haciendo todo lo posible para disminuir los efectos de la ciberdelincuencia a escala mundial y proteger a la población para que pueda vivir en un mundo más seguro.

INTERPOL

ACERCA DE INTERPOL

INTERPOL es la organización policial internacional más grande del mundo. Nuestra función consiste en prestar ayuda a los organismos encargados de la aplicación de la ley de nuestros 194 países miembros para combatir todas las formas de delincuencia transnacional. Trabajamos para ayudar a las policías de todo el planeta a hacer frente a los crecientes desafíos que plantea la delincuencia en el siglo XXI, proporcionándoles una infraestructura de apoyo técnico y operativo dotada de alta tecnología. Nuestros servicios incluyen formación específica, apoyo especializado en materia de investigaciones, bases de datos especializadas y canales de comunicación policial protegida.

NUESTRA META: UNA "MAYOR COMUNICACIÓN POLICIAL PARA UN MUNDO MÁS SEGURO"

Nuestra meta es lograr un mundo en el que todos los profesionales de los organismos encargados de la aplicación de la ley sean capaces, a través de INTERPOL, de transmitir, intercambiar y consultar de forma segura información policial vital cuando y donde lo necesiten, garantizando así la seguridad de los ciudadanos de todo el planeta. Proporcionamos y promovemos constantemente soluciones avanzadas e innovadoras para hacer frente a los desafíos que se plantean a escala mundial en el ámbito policial y de la seguridad.