INTERPOL

# Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19

4 de agosto de 2020

Los ataques han cambiado de objetivo, pasando de centrarse en los particulares a dirigirse contra las administraciones y las infraestructuras sanitarias esenciales

Una evaluación de INTERPOL sobre las repercusiones de la COVID-19 en la ciberdelincuencia ha puesto de manifiesto un cambio sustancial en los objetivos de los ataques, que antes eran particulares y pequeñas empresas y ahora tienden a ser grandes multinacionales, administraciones estatales e infraestructuras esenciales.

Ahora que las organizaciones y las empresas están desplegando rápidamente redes y sistemas a distancia para que el personal pueda trabajar desde sus hogares, los delincuentes se aprovechan del aumento de las vulnerabilidades en materia de seguridad para robar datos, obtener beneficios y ocasionar disfunciones.

En solo un cuatrimestre (entre enero y abril), uno de los socios de INTERPOL del sector privado detectó 907 000 correos basura, 737 incidentes de tipo malware, y 48 000 URL maliciosas, todos ellos relacionados con la COVID-19.

*e intensificando su ejecución a un ritmo alarmante, aprovechándose del miedo y la incertidumbre provocados por la inestabilidad de la situación socioeconómica generada por la COVID-19"*

**Jürgen Stock, Secretario General de INTERPOL**

"La dependencia cada vez mayor de Internet por parte de los ciudadanos en todo el mundo también brinda nuevas oportunidades, ya que muchas empresas y particulares no están velando por que sus ciberdefensas estén actualizadas".

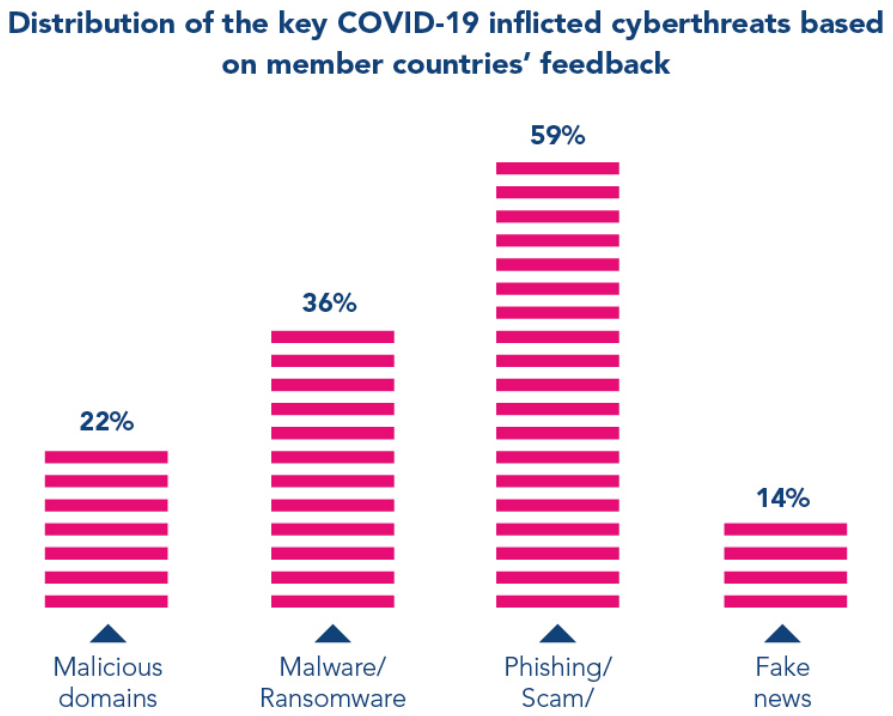
"Una vez más, en las conclusiones del informe se destaca la necesidad de una cooperación más estrecha entre los sectores público y privado si queremos atajar con eficacia el peligro que la COVID 19 también plantea a nuestra salud cibernética", concluyó el jefe de INTERPOL.

Entre las constataciones principales que pone de relieve la evaluación de INTERPOL sobre el panorama de la ciberdelincuencia en relación con la pandemia de COVID-19 cabe señalar:

- **Las estafas por Internet y el phishing -** Los autores de las amenazas han revisado sus métodos habituales en materia de estafas por Internet y phishing. Ahora, los ciberdelincuentes, a menudo haciéndose pasar por autoridades gubernamentales y sanitarias, envían a sus víctimas correos electrónicos de phishing sobre la COVID-19 en los que las incitan a facilitar datos personales y a descargar contenidos maliciosos. Unos dos tercios de los países miembros que respondieron a la encuesta mundial sobre ciberdelincuencia informaron de la proliferación del uso de temáticas relacionadas con la COVID-19 en los delitos de phishing y las estafas por Internet desde el brote de la pandemia.
- **Malware disruptivos (ransomware y DDoS) -** Alentados por la probabilidad de causar graves problemas y obtener sustanciosas ganancias, los ciberdelincuentes están multiplicando el número de ataques con malware disruptivos contra las infraestructuras esenciales y las instituciones sanitarias.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.Las investigaciones de las fuerzas del orden muestran que la mayoría de los atacantes calculaban con bastante exactitud la cantidad máxima que podían solicitar como rescate a las organizaciones víctimas de sus ataques.
- **Malware destinados a la obtención de datos -** En el ámbito de la ciberdelincuencia también están en

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 como “coronavirus” o “COVID”. Se trata de sitios web fraudulentos que sustentan una amplia variedad de actividades malignas, por ejemplo, servidores C2, difusión de malware y phishing.Entre febrero y marzo de 2020, un socio del sector privado detectó y comunicó a INTERPOL que los registros maliciosos —malware y phishing incluidos— habían aumentado un 569 %, mientras que los registros de alto riesgo habían subido un 788 %.
- **Desinformación -** Asistimos a una amplificación de la desinformación y las noticias falsas que se propagan rápidamente entre los ciudadanos. La información no contrastada, las amenazas mal entendidas y las teorías de la conspiración han fomentado la ansiedad de la población y, en algunos casos, facilitado la ejecución de ciberataques.Cerca del 30 % de los países que contestaron a la encuesta mundial sobre ciberdelincuencia confirmaron la circulación de información falsa sobre la COVID-19. En el plazo de un mes, un país informó de 290 publicaciones, la mayoría de las cuales ocultaba malware. También se comunicaron casos de desinformación vinculada al comercio ilegal de productos médicos fraudulentos.Otros casos de desinformación guardaban relación con estafas a través de mensajes de texto que presentaban ofertas demasiado buenas para ser ciertas, por ejemplo, alimentos gratuitos, ventajas especiales, o grandes descuentos en supermercados.



# Previsiones

Entre las principales preocupaciones de cara al futuro señaladas en el informe de INTERPOL figuran las siguientes:

- Es altamente probable que la ciberdelincuencia siga aumentando a corto plazo. Debido a las vulnerabilidades asociadas al teletrabajo y la posibilidad de obtener mayores ganancias, los ciberdelincuentes seguirán ampliando sus actividades y concebirán unos modus operandi más avanzados y complejos.
- Es probable que, para aprovechar la preocupación de la ciudadanía por la pandemia, los autores de amenazas continúen propagando estafas por Internet y campañas de tipo phishing relacionadas con el coronavirus.
- También es posible que aumenten las estafas a empresas por e-mail mediante suplantación de identidad, 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.
- Una vez que se disponga de vacunas contra la COVID-19, 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 sustraer datos.

## DOCUMENTOS CONEXOS

| | | | | | | |
|---|---|---|---|---|---|---|
| PDF | Ciberdelincuencia: efectos de la COVID-19 | 4.06MB | EN | FR | ES | AR |

## VÉASE TAMBIÉN

Ciberdelincuencia

Ciberamenazas relacionadas con la COVID-19

# Noticias conexas

## INTERPOL launches initiative to fight cybercrime in Africa

12 de mayo de 2021


## Estafas con vacunas por Internet: INTERPOL y la Oficina de Investigaciones de Seguridad Nacional de Estados Unidos publican una alerta

24 de marzo de 2021


## INTERPOL describe en un informe las principales ciberamenazas en el Sudeste Asiático

22 de enero de 2021

## INTERPOL y la OCDE determinan nuevos ámbitos para intensificar la cooperación

14 de diciembre de 2020

## Tres personas detenidas a raíz de una investigación en la que INTERPOL, Group-IB y las Fuerzas Policiales de Nigeria desmantelan un prolífico grupo...

25 de noviembre de 2020