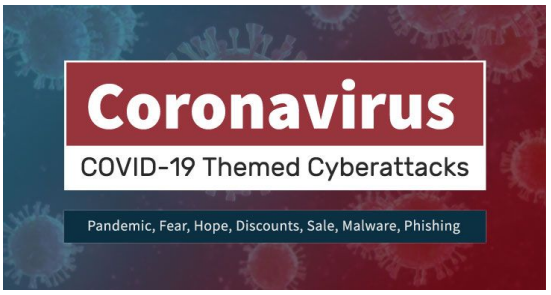
**BOLETÍN DE ALERTA**

**Boletín Nro.**: 2020-09
**Fecha de publicación**: 30/03/2020
**Tema**: COVID-19 en el mundo digital, la mayor amenaza actual en Ciberseguridad
Ciberdelincuentes se aprovechan del temor al coronavirus para infectar con malware y/o robar información a sus víctimas.

## Descripción




COVID-19 no solo representa una amenaza física, sino también virtual. COVID-19 está dando tanto que hablar en el mundo, se ha disparado el número de noticias y memes relativos al mismo, hasta el punto que recibimos decenas e incluso centenas de WhatsApps diarios con esta temática, la sociedad está tan pendiente de contar con información actualizada sobre esta enfermedad, que abren de forma compulsiva en su computadora, notebook o teléfono móvil cualquier mensaje, email, audio o archivo que reciben sobre el coronavirus, en redes sociales, correos electrónicos, etc.

El crecimiento masivo de la difusión de todo lo relacionado al coronavirus, se ha convertido en la mayor amenaza de ataque cibernético de los últimos tiempos y ha hecho que la enfermedad se haya convertido en la "puerta de entrada" perfecta de muchos ciberdelincuentes, el camuflaje ideal para infectar con algún malware o robar información. Hemos observado campañas que, a través de diversas técnicas éstos buscan engañar a sus víctimas con diversos fines. Los ataques están cada vez más preparados para vulnerar la seguridad.

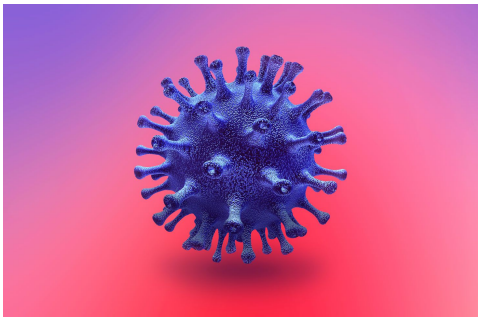
Inicialmente, estábamos viendo alrededor de una campaña por día en todo el mundo; ahora estamos observando tres o cuatro por día. Este aumento destaca cuán atractivas pueden ser las noticias globales para los ciberdelincuentes.

Desde el CERT-PY hemos recopilado información sobre las distintas campañas de actividades cibernéticas maliciosas hasta la fecha, que utilizan el temor al COVID-19 en Paraguay y en el mundo, para tratar de convencer a las víctimas. De esté modo se podrá extremar las

precauciones y los cuidados; así también alertar a los empleados de la organización para tomar las medidas en las cuestiones laborales y personales.

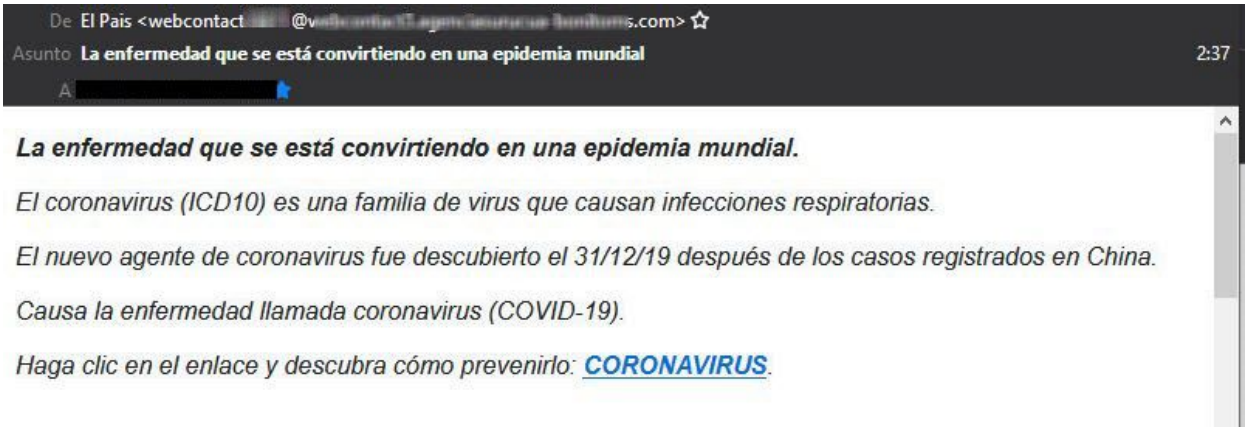
## Múltiples campañas de ataques con COVID-19 "Coronavirus" en el mundo

### A. Campañas de phishing



Aprovechando el temor público generalizado sobre el COVID-19 "Coronavirus", los phishers han comenzado a usar este tema como un anzuelo, y se han incrementado los correos electrónicos maliciosos relacionados, con el asunto "*Atención coronavirus*", o conteniendo información sobre el *"Avance del virus a nivel mundial"*, o *"Últimos casos detectados en el Paraguay"*, o *"Vacuna contra el virus"*, entre otras informaciones. Cuando el usuario accede a la información o descarga el programa para visualizar el contenido, automáticamente se descarga el malware que controla su dispositivo. Ejemplos:

- que dirigen a una página web infectada. Un caso, en la que el malware llamado Remcos RAT infecta el dispositivo de la víctima, a través de un supuesto archivo PDF denominado "*Medidas de seguridad ante el Coronavirus*". Sin embargo, al abrir el archivo se ejecuta el malware.
- que instalan un malware a través de un archivo adjunto de Microsoft Office,
- dependiendo de la creatividad del delincuentes otros miles de ejemplos más.


De El Pais <webcontact[redacted]s.com>
Asunto **La enfermedad que se está convirtiendo en una epidemia mundial** 2:37
A [redacted]

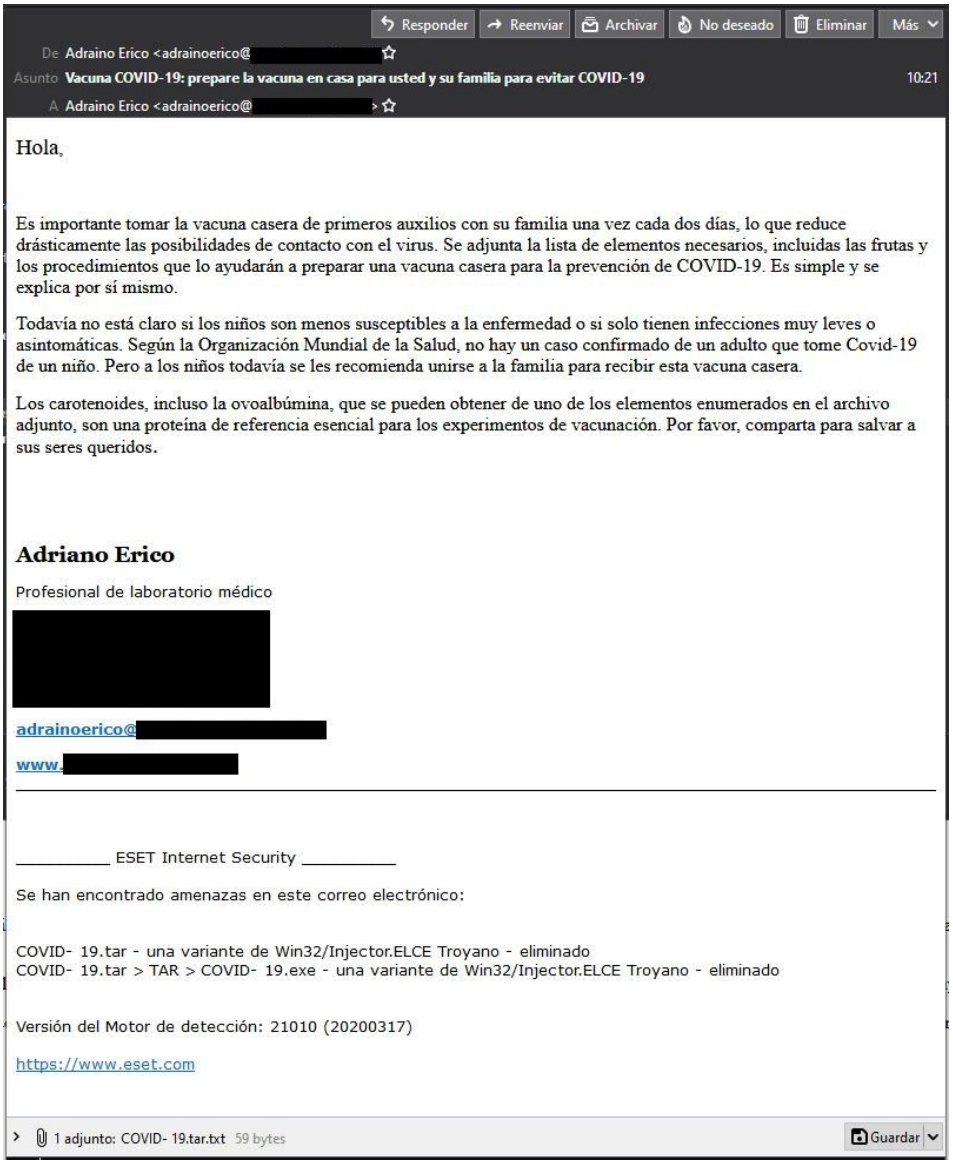
***La enfermedad que se está convirtiendo en una epidemia mundial.***

*El coronavirus (ICD10) es una familia de virus que causan infecciones respiratorias.*

*El nuevo agente de coronavirus fue descubierto el 31/12/19 después de los casos registrados en China.*

*Causa la enfermedad llamada coronavirus (COVID-19).*

*Haga clic en el enlace y descubra cómo prevenirlo: **CORONAVIRUS**.*



Responder | Reenviar | Archivar | No deseado | Eliminar | Más

De Adraino Erico <adrainoerico@[redacted]

Asunto **Vacuna COVID-19: prepare la vacuna en casa para usted y su familia para evitar COVID-19** 10:21

A Adraino Erico <adrainoerico@[redacted]>

Hola,

Es importante tomar la vacuna casera de primeros auxilios con su familia una vez cada dos días, lo que reduce drásticamente las posibilidades de contacto con el virus. Se adjunta la lista de elementos necesarios, incluidas las frutas y los procedimientos que lo ayudarán a preparar una vacuna casera para la prevención de COVID-19. Es simple y se explica por sí mismo.

Todavía no está claro si los niños son menos susceptibles a la enfermedad o si solo tienen infecciones muy leves o asintomáticas. Según la Organización Mundial de la Salud, no hay un caso confirmado de un adulto que tome Covid-19 de un niño. Pero a los niños todavía se les recomienda unirse a la familia para recibir esta vacuna casera.

Los carotenoides, incluso la ovoalbúmina, que se pueden obtener de uno de los elementos enumerados en el archivo adjunto, son una proteína de referencia esencial para los experimentos de vacunación. Por favor, comparta para salvar a sus seres queridos.

**Adriano Erico**

Profesional de laboratorio médico

[redacted]

adrainoerico@[redacted]

www.[redacted]

_____ ESET Internet Security _____

Se han encontrado amenazas en este correo electrónico:

COVID- 19.tar - una variante de Win32/Injector.ELCE Troyano - eliminado
COVID- 19.tar > TAR > COVID- 19.exe - una variante de Win32/Injector.ELCE Troyano - eliminado

Versión del Motor de detección: 21010 (20200317)

https://www.eset.com

1 adjunto: COVID- 19.tar.txt 59 bytes | Guardar

NETFLIX

Netflix contra coronavirus
¡En esta cuarentena, obtén una cuenta gratis!
netflix-usa.net

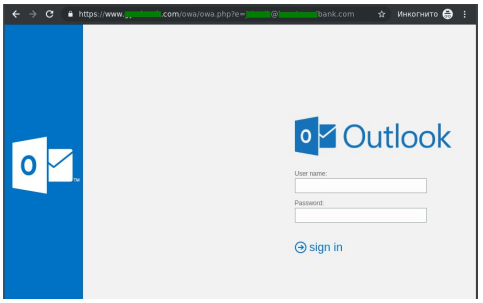
Debido a la pandemia de CoronaVirus en todo el mundo, Netflix está dando algunos pases gratis para su plataforma durante el período de aislamiento. ¡Ejecútelo en el sitio porque terminará rápido!

https://netflix-usa.net/[illegible]
-aislamiento[illegible] 7:39

En el caso de esta otra campaña de phishing, los cibercriminales detrás de la misma suplantan la identidad de Netflix para ofrecer el beneficio de una cuenta gratuita dada la situación provocada por la pandemia

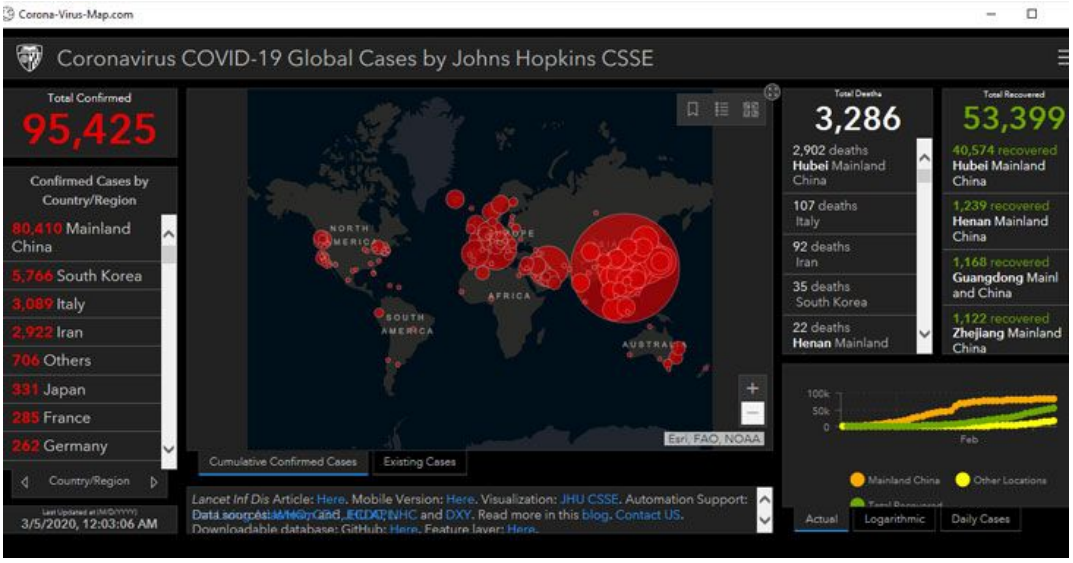
### a. Campañas inusuales dirigidas a personal de infraestructuras críticas, en este caso el personal médico

Los correos parecían anunciar un seminario sobre el coronavirus y contenían un enlace de registro. Pero ese enlace dirigía a una página de phishing disfrazada como la aplicación web del Outlook de Microsoft, donde los atacantes recopilan credenciales de inicio de sesión. Todavía se desconoce dónde y cómo usarán estos datos los cibercriminales.




### b. Malware que infecta las PCs para robar contraseñas: Coronavirus Map

En este caso, un mapa de infecciones que supuestamente muestra información variada sobre la propagación del COVID-19, pero realmente lo que intenta es forzar a los usuarios a descargar una aplicación maliciosa que compromete el dispositivo; que es similar a la fuente legítima en línea de la Universidad Johns Hopkins, para visualizar y rastrear los casos de coronavirus en tiempo real.



## B. Ransomware

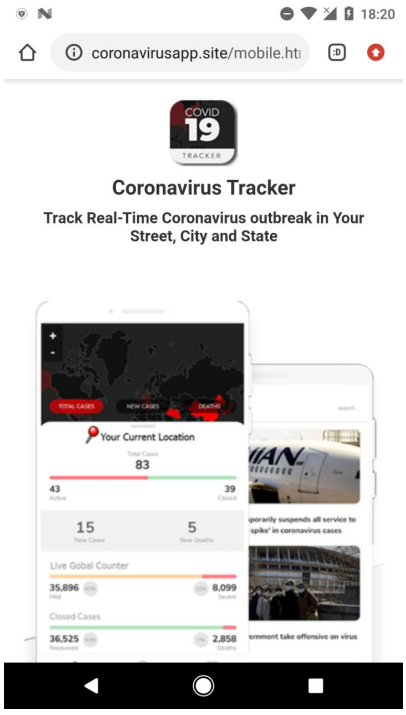
A medida que los hospitales de todo el mundo luchan para responder a la crisis de COVID-19, el ransomware presenta un grave riesgo para su capacidad de proporcionar atención urgente a los enfermos críticos. Aumentan las campañas dirigidas este sector que incluyen correos electrónicos que ofrecen curas o vacunas contra el coronavirus a cambio de pagos, y otros. Ejemplos:

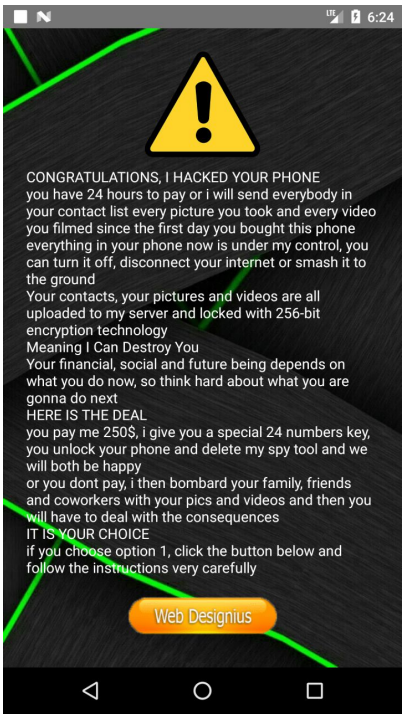
**a.** Una banda de ciberdelincuentes utilizó el **ransomware Maze** para atacar los sistemas informáticos de Hammersmith Medicines Research (HMR), publicando detalles personales de miles de ex pacientes después de que la compañía se negara a pagar un rescate. Los datos publicados incluyen datos sensibles sobre los voluntarios de las pruebas médicas como documentos de identidad, pasaportes, antecedentes médicos y detalles de las pruebas. En este caso fueron capaces de restaurar rápidamente sus sistemas a partir de copias de seguridad. En 2019, al menos 764 proveedores de atención médica se vieron afectados por el ransomware. Sin una pandemia global, un ataque de ransomware en un centro de cuidados críticos puede causar un grave peligro para los pacientes. Con COVID-19, un ataque de ransomware en un hospital abrumado podría inclinar la balanza y provocar una pérdida de vidas.

**b.** Ciberdelincuentes realizaron un ataque con ransomware a uno de los principales centros de pruebas COVID-19 en la República Checa, el Hospital Universitario de Brno. Aunque el hospital restauró rápidamente los servicios con la ayuda de la policía checa y el centro de respuestas de incidentes cibernéticos del gobierno, ese ataque y otros en los últimos tiempos han despertado preocupaciones entre los profesionales de seguridad, de que los ciberdelincuentes se dirigirán a organizaciones de atención médica y obstaculizarían las respuestas de emergencia pandémica COVID-19.

**c.** Se descubrió que una aplicación de Android falsa de seguimiento de Coronavirus en tiempo real, llamada **COVID19 Tracker**, abusó de los permisos de los usuarios

para cambiar la contraseña de la pantalla de bloqueo del teléfono e instalar el CovidLock ransomware a cambio de un rescate de U$S100 bitcoin.




### d. Ataques de Denegación de Servicios

El Departamento de Salud y Servicios Sociales de los Estados Unidos (HHS por sus siglas en inglés) aparentemente también sufrió un ataque cibernético la noche del domingo 13 de marzo. Bloomberg lo ha denominado un ataque masivo de DDoS destinado a sabotear el funcionamiento normal de los servidores del HHS, "debilitando la respuesta a la pandemia de coronavirus". Dirigido a las organizaciones que más se esfuerzan por contrarrestar el coronavirus, este ataque puede causar mucho más daño del habitual.

## C. Lista actualizada de dominios, IPs, hashes e IOCs de sitios dañinos

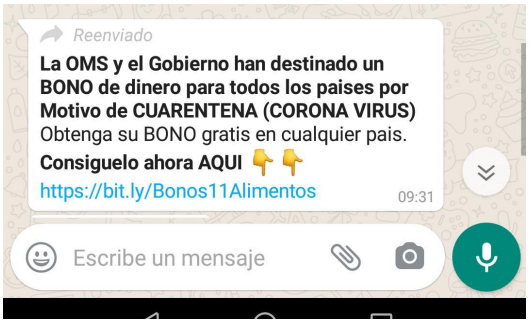
- Dominios registrados
- https://pastebin.com/YFai7KHA
- CCN-CERT de España

## D. Descuentos COVID-19: herramientas de explotación para la venta

Las ofertas especiales de diferentes delincuentes que promocionan sus “productos'” generalmente malware malicioso o herramientas de explotación, se están vendiendo a través de la Dark Web bajo ofertas especiales con “COVID-19” o “coronavirus” como códigos de descuento, dirigidos a aspirantes a ciberdelincuentes.

## E. Fake news en redes sociales

Están proliferando de forma alarmante las fake news o noticias falsas y falsos testimonios de supuestos profesionales del sector salud, o las organizaciones que apoyan con actividades varias a las respuestas ante la pandemia, muchas personas con malas intenciones que aprovechan la histeria colectiva para viralizarlas.



## F. Alertas de Ciberseguridad en organizaciones locales:

Muchas organizaciones locales han lanzado avisos y alertas sobre estas amenazas existentes. A continuación algunos ejemplos:

## Recomendaciones

### A. A usuarios

En caso de sospechas de dispositivo infectado, realiza estos pasos:

- Actualiza la base de datos de conocimientos del software antivirus y ejecuta un análisis. Las compañías de antivirus, actualizan periódicamente esas bases de datos para reconocer archivos maliciosos.
- Mantén siempre actualizado el sistema operativo y el antivirus, de este modo reducís el riesgo de ser infectado, ya que tu sistema no estaría vulnerable.
- Si sospechas infección con el malware "Coronavirus Map", seguí estos consejos de la Guía de Eliminación del Malware Coronavirus Map

En caso de sospechas de suplantación de identidad o phishing, presta atención a los detalles:

- Evita acceder a enlaces sospechosos o desconocidos, prometiendo contenido exclusivo sobre COVID-19, y usa el antivirus para los archivos que necesites descargar.
- Verifica la autenticidad de la dirección de correo electrónico del remitente, los dominios mal escritos, y otras señales.
- Revisa la extensión del archivo descargado. Documentos y archivos de video no corresponden al formato .exe o .lnk.

- Comprobá la URL del enlace con etiquetas engañosas. Si revisas el enlace sin hacer clic en él, verás que la dirección verdadera a la que conduce es diferente a la descripción del enlace.
- No contestes en ningún caso a estos correos.
- Observa el diseño de la página de phishing, que no es completamente igual a los sitios reales.
- Tene cuidado al cargar datos personales en sitios web. No te apresures ni te sientas bajo presión. Los cibercriminales utilizan emergencias como el COVID-19 para que la gente tome decisiones rápidas. Tómate tu tiempo cuando alguien te pida información personal.
- Utiliza fuentes confiables, como sitios web legítimos del gobierno, para obtener información actualizada y basada en hechos sobre COVID-19.
- No descargues aplicaciones de fuentes no oficiales, para conocer el alcance internacional del COVID-19
- Realiza siempre copias de seguridad de tus archivos y/o sistemas más importantes.

En caso de sospechas de noticias falsas o fake news:

- Consulta siempre en las fuentes oficiales, en este caso los sitios web oficiales del Gobierno.
- No reenvíes mensajes en WhatsApp que no lo hayas comprobado previamente.
- No descargues archivos desconocidos, ya que podrían contener un malware.

Mantente siempre informado acerca de los cuidados de ciberseguridad que debes considerar.

## B. A administradores de sistemas:

Evita tener funcionarios desprevenidos. Impulsa campañas de concienciación a los usuarios de los sistemas acerca de los peligros y los cuidados a tener en cuenta sobre los sistemas que se administran y en general, y la responsabilidad que recae en los usuarios que usan una cuenta de correo institucional y que también podría aplicar al uso con las cuentas personales.

En servidores de correo electrónico:

- Comprueba la configuración del servidor de correo y especialmente en los correos entrantes.
- Utiliza soluciones de seguridad.

En los servicios más importantes de su organización:

- Mantén copias de seguridad para poder reestablecer los servicios en caso de pérdidas o en este caso ransomware.
- Asegurate de que las tecnologías de acceso remoto estén instaladas y configuradas correctamente, incluido el uso de autenticación de múltiples factores.
- Controla de que las personas eviten el uso de dispositivos personales no autorizados para el trabajo y/o asegurarse de que "*los dispositivos personales deberán tener el mismo nivel de seguridad que un dispositivo propiedad de la organización, y también deberá tener en cuenta las implicaciones de privacidad de los dispositivos propiedad de los empleados que se conectan".*

La transición generalizada al trabajo remoto significa que ciberdelincuentes tendrían una gama más amplia de objetivos, por lo que recomendamos revisar la Guía de Consideraciones de Ciberseguridad para trabajos remotos.

Por todo lo mencionado anteriormente, a medida que las personas continúen preocupándose por protegerse de este virus, es posible que veamos más y más malware oculto en documentos falsos sobre la propagación del coronavirus. No debemos caer en la trampa de estos cibercriminales, convirtiéndonos en amplificadores de sus mentiras ni de su malware. Cuando recibamos mensajes relativos al coronavirus, solo debemos confiar en fuentes oficiales. Y si son mensajes con archivos descargables, es mejor desconfiar de ellos, incluso si conocemos al remitente, ya que podría tratarse de una campaña de Spoofing.

Si fuiste víctima o si algún usuario de tu organización fue víctima de algunas de estas campañas, reporta el caso a abuse@cert.gov.py para un análisis técnico, indicando los siguientes datos:

- una descripción del mismo,
- logs, captura de pantalla con explicaciones, captura de tráficos, archivos, etc.
- cualquier dato que pueda ayudar a investigar el incidente, según sea el caso.

## Referencias e información adicional

https://www.welivesecurity.com/la-es/2020/03/18/crecen-campanas-malware-aprovechar-temor-covid-19/
https://www.pandasecurity.com/spain/mediacenter/mobile-news/coronavirus-llega-mundo-digital/https://latam.kaspersky.com/blog/coronavirus-phishing/17066/
https://blog.segu-info.com.ar/2020/03/el-ransomware-afecta-hospitales-que.html
https://blog.segu-info.com.ar/2020/03/lista-de-ataques-y-dominios-daninos-por.html
https://www.computerweekly.com/news/252480238/Coronavirus-now-possibly-largest-ever-cyber-security-threat