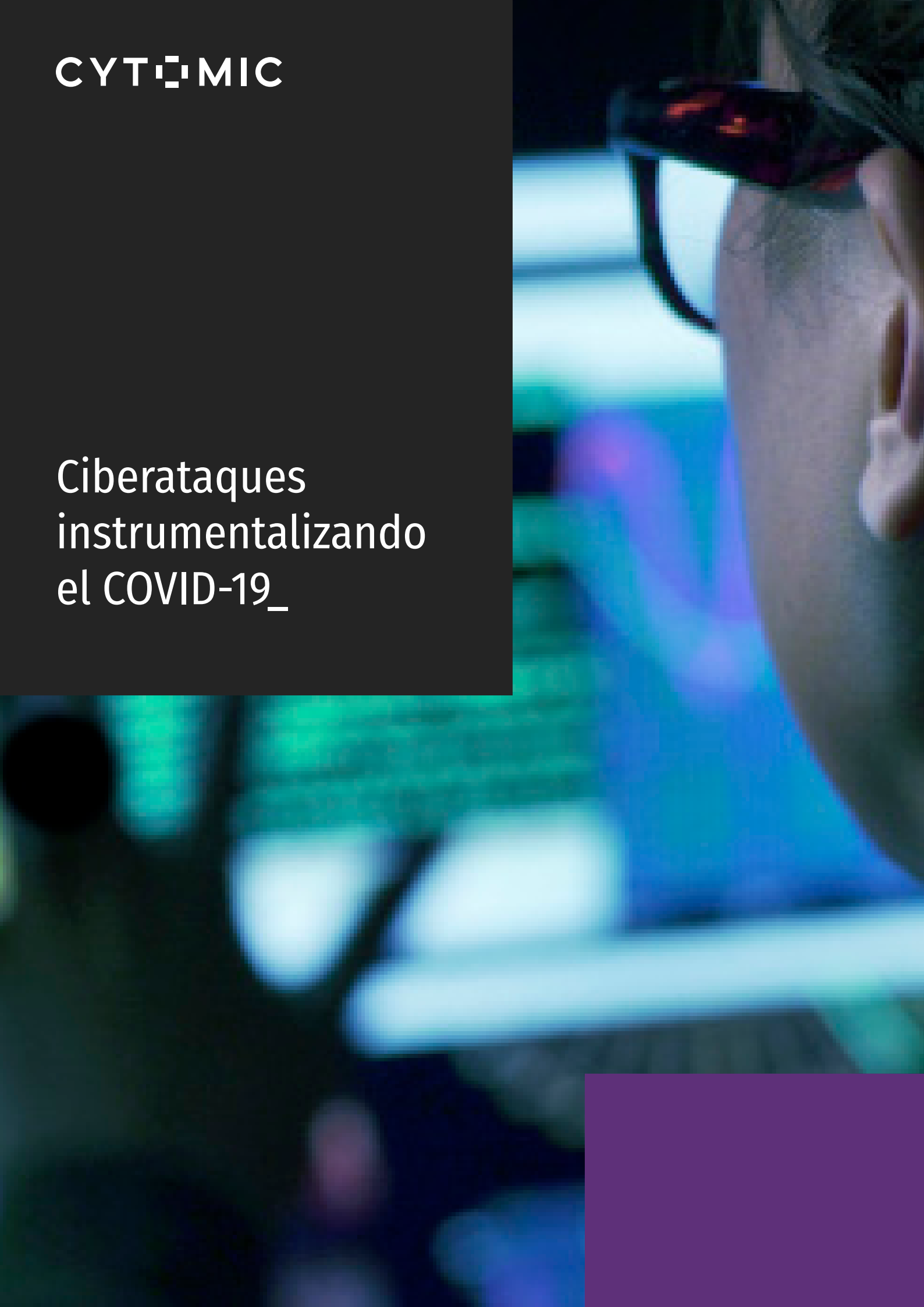
CYTOMIC

Ciberataques instrumentalizando el COVID-19_



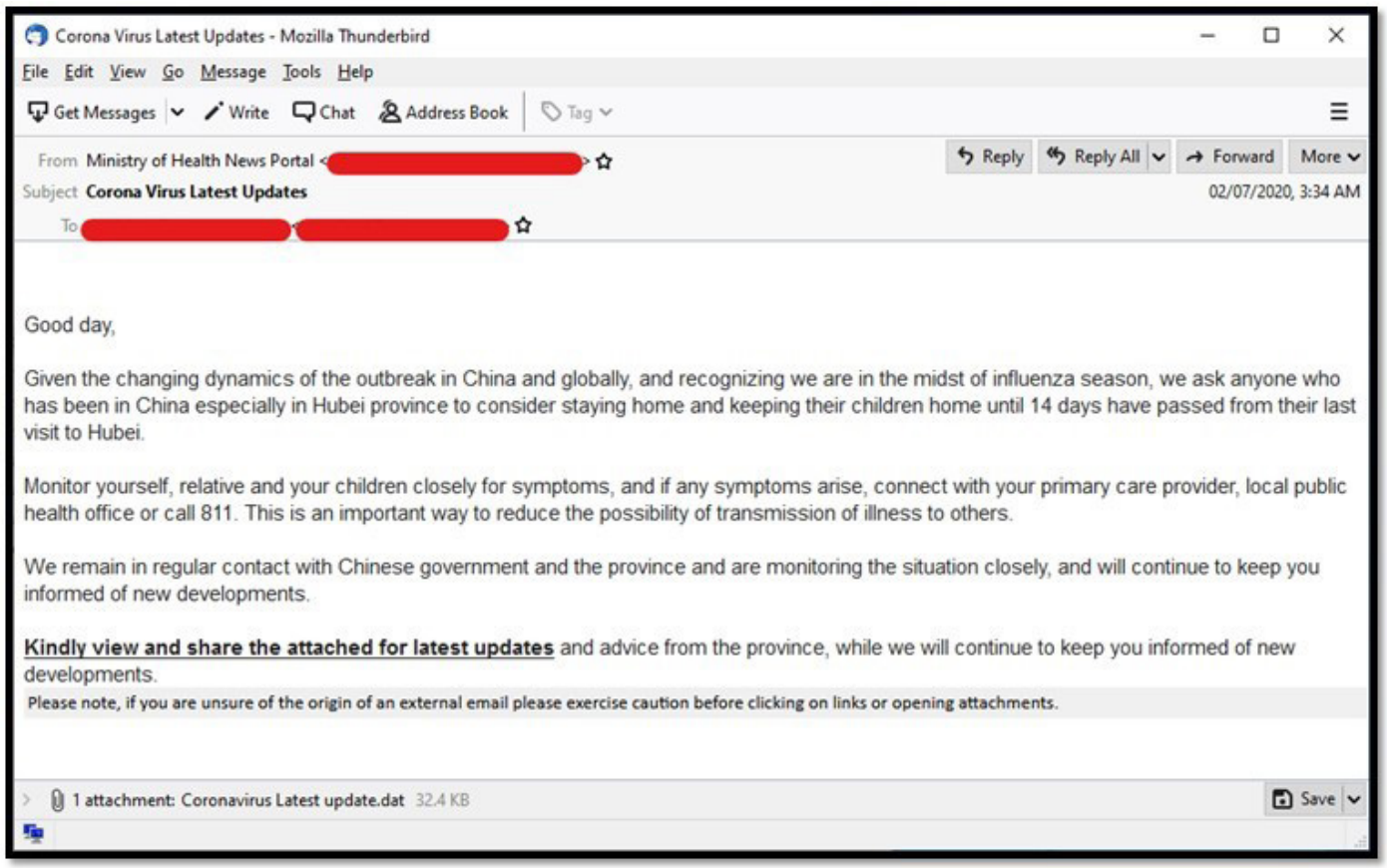
Campañas de ciber ataques instrumentalizando el COVID-19 con impacto mundial_

La enfermedad por coronavirus (COVID-19) se está utilizando como gancho de campañas maliciosas, con estrategias de ingeniería social, que incluyen correo electrónico no deseado (SPAM), malware, ransomware y dominios maliciosos. A medida que el número de afectados continúa aumentando en miles, las campañas que utilizan la enfermedad como señuelo también aumentan. Los investigadores Cytomic buscan periódicamente muestras en campañas maliciosas relacionadas con el coronavirus.

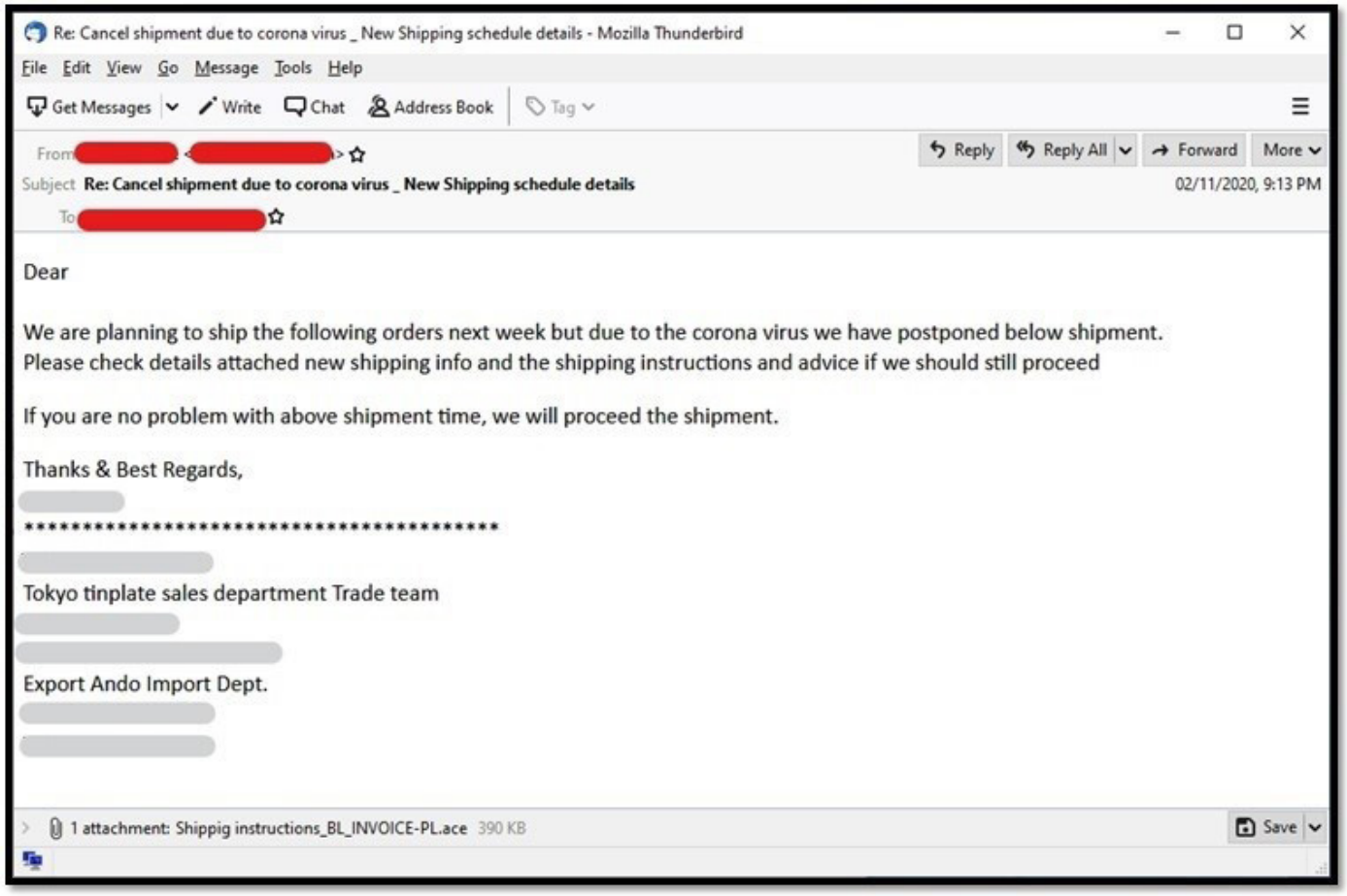
Spam relativo al CoronaVirus_

Los investigadores de Cytomic han detectado correo electrónico enviadas y recibidas de todo el mundo, incluidos países como Estados Unidos, Japón, Rusia y China. Muchos de los correos electrónicos, supuestamente de organizaciones oficiales, contienen actualizaciones y recomendaciones relacionadas con la enfermedad. Como la mayoría de los ataques de correo electrónico no deseado, también incluyen archivos adjuntos maliciosos.

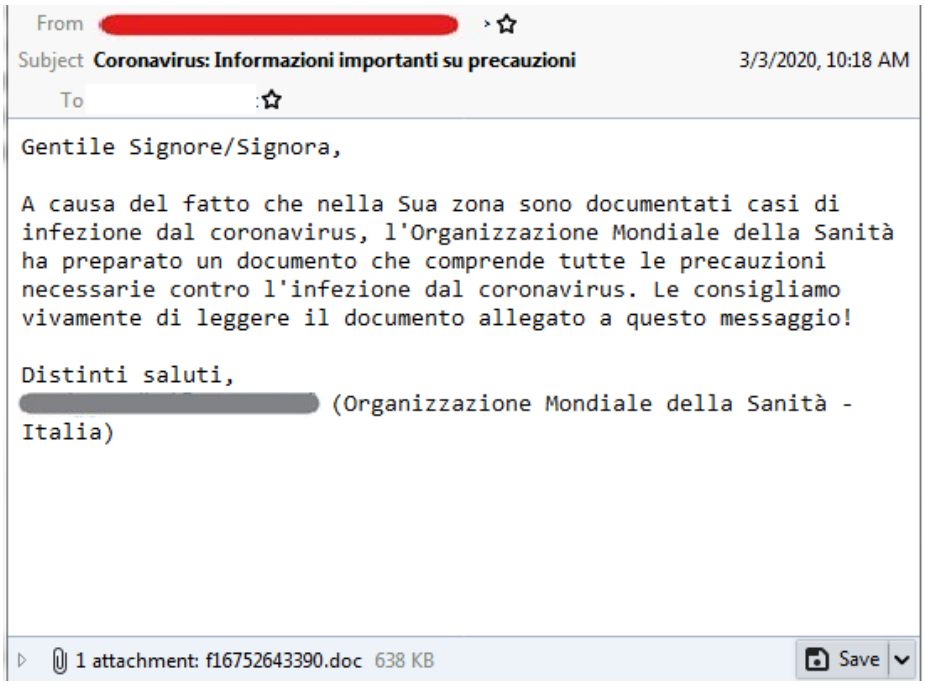
Un ejemplo, es el spam con "**Últimas actualizaciones del Corona Virus**", cuyo remitente era Ministerio de Salud. Contiene recomendaciones sobre cómo prevenir la infección y viene con un archivo adjunto que supuestamente contiene las últimas actualizaciones de COVID-19, pero en realidad llevaba un malware.



Otros correos, usados en estas campañas, están relacionados con transacciones de envío, ya sea aplazamiento debido a la propagación de la enfermedad o actualizaciones de los envíos.



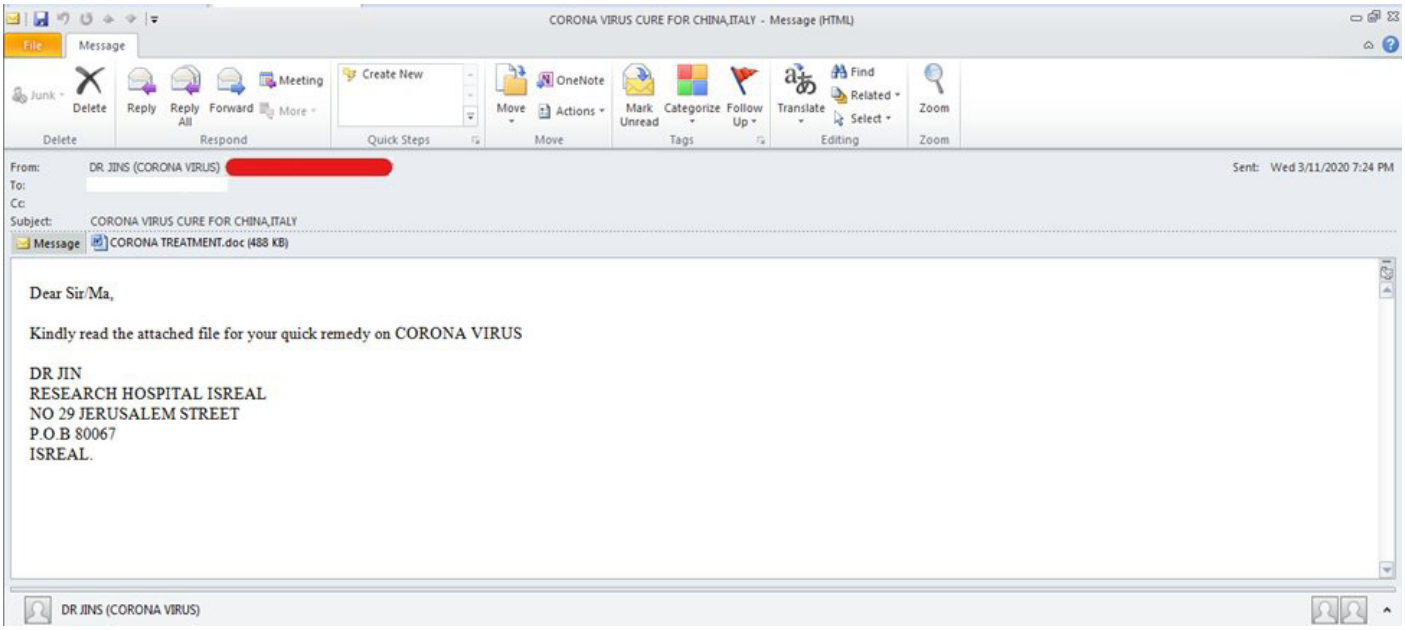
El siguiente correo electrónico en italiano hace referencia a información importante sobre el virus:



Mientras que el siguiente en portugués notifica sobre una supuesta vacuna para COVID-19.

Correo no deseado relacionado con COVID-19 en portugués

Se han detectado correos de spam que mencionaba una cura para el coronavirus en el asunto como reclamo para descargar el archivo adjunto malicioso. En algunas ocasiones este adjunto malicioso es HawkEye Reborn , una variante del troyano HawkEye que roba información.



Spam de correo electrónico de coronavirus HawkEye Reborn

Indicadores de compromiso del adjunto malicioso

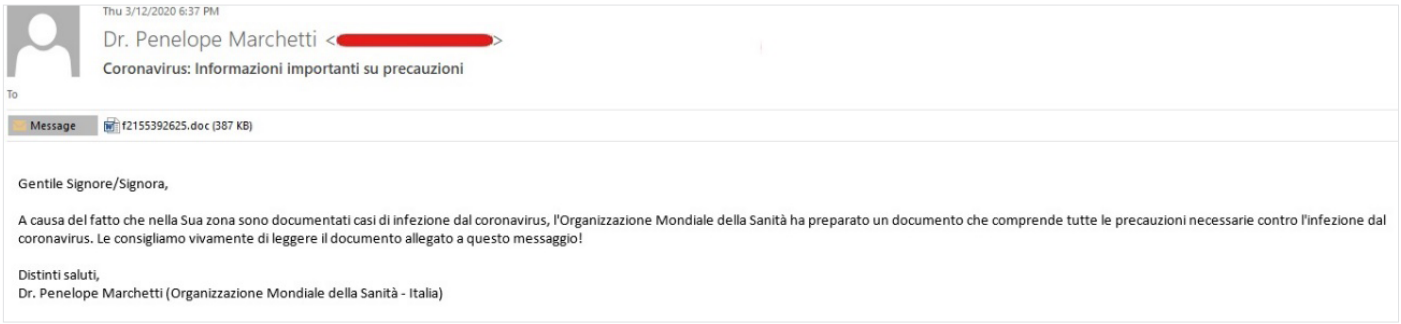
SHA-256
b9e5849d3ad904d0a8532a886bd3630c4eec3a6faf0cc68658f5ee4a5e803be

Correo electrónico italiano no deseado conectado a una URL relacionada con COVID-19

Los Indicadores de compromiso en este caso son:

SHA-256
6cc5e1e72411c4f4b2033ddafe61fdb567cb0e17ba7a3247acd60cbd4bc57bfb
7c12951672fb903f520136d191f3537bc74f832c5fc573909df4c7fa85c15105

Otro caso de spam, dirigido a usuarios italianos, país gravemente afectado por la pandemia, incluye tanto el asunto como el cuerpo del correo electrónico el texto “Coronavirus: información importante sobre precauciones”. En el cuerpo del correo electrónico, el remitente afirma que el archivo adjunto es un documento preparado por la Organización Mundial de la Salud (OMS) y recomienda encarecidamente a los lectores que descarguen el archivo comprometido adjunto de Microsoft Word. El archivo malicioso contiene un troyano.



Muestra de spam dirigido a usuarios en Italia

Al abrir el documento, se presenta el siguiente mensaje que atraen a los usuarios para habilitar el contenido macro:

Muestra de archivo adjunto

Indicadores de compromiso

SHA-256
dd6cf8e8a31f67101f974151333be2f0d674e170edd624ef9b850e3ee8698fa2

Malware & Ransomware CoronaVirus_

Los laboratorios de Cytomic, gracias al servicio Zero-Trust application service han conseguido identificar y bloquear los siguiente ejecutables maliciosos relativos a estas campañas:

Nombre del archivo	SHA 256
CORONA VIRUS AFFECTED CREW AND VESSEL.xlsm	ab533d6ca0c2be8860a0f7fbfc7820ffd 595edc63e540ff4c5991808da6a257d
	17161e0ab3907f637c2202a384de67fca 49171c79b1b24db7c78a4680637e3d5
	315e297ac510f3f2a60176f9c12fcf9 2681bbad758135767ba805cdea830b9ee
CoronaVirusSafetyMeasures_pdf.exe	c9c0180eba2a712f1aba1303b90cbf12c11 17451ce13b68715931abc437b10cd
	29367502e16bf1e2b788705014d0142 d8bcb7fcc6a47d56fb82d7e333454e923
LIST OF CORONA VIRUS VICTIM.exe	3f40d4a0d0fe1eea58fa1c71308431b5c2c e6e381cacc7291e501f4eed57bfd2
POEA HEALTH ADVISORY re-2020 Novel Corona Virus.pdf.exe	3e6166a6961bc7c23d316ea9bca87d82 87a4044865c3e73064054e805ef5ca1a
POEA Advisories re-2020 Novel Corona Virus.2.pdf.exe	b78a3d21325d3db7470fbf1a6d254e23d34 9531fca4d7f458b33ca93c91e61cd

Otros investigadores están viendo que los cibercriminales aprovechan los mapas de monitorización del coronavirus online, suplantándolos con sitios web falsos que promueven la descarga e instalación de malware. A continuación tenemos los hashes de estas aplicaciones maliciosas:

SHA 256
2b35aa9c70ef66197abfb9bc409952897f9f70818633ab43da85b3825b256307
0b3e7faa3ad28853bb2b2ef188b310a67663a96544076cd71c32ac088f9af74d
13c0165703482dd521e1c1185838a6a12ed5e980e7951a130444cf2feed1102e
fda64c0ac9be3d10c28035d12ac0f63d85bb0733e78fe634a51474c83d0a0df8
126569286f8a4caeeaba372c0bdba93a9b0639beaad9c250b8223f8ecc1e8040

Una nueva variante de ransomware CoronaVirus se propagaba a través de un sitio falso de optimización de sistema. Las víctimas, sin saberlo, descargan el archivo WSGSetup.exe del sitio falso. Dicho archivo actúa como un descargador de dos tipos de malware: el ransomware CoronaVirus y el troyano robo de contraseñas llamado Kpot.

Esta campaña sigue la tendencia de los recientes ataques de ransomware que van más allá del cifrado de datos y también roban información.

Además, se tiene constancia de otro ransomware móvil llamado CovidLock proviene de una aplicación maliciosa de Android que supuestamente ayuda a rastrear casos de COVID-19. El ransomware bloquea los teléfonos de las víctimas, que tienen 48 horas para pagar US $ 100 en bitcoins para recuperar el acceso a sus teléfonos. Las amenazas incluyen la eliminación de datos almacenados en el teléfono y la filtración de detalles de la cuenta de redes sociales.

Dominios relativos a campañas CoronaVirus_

También se ha observado un aumento notable en los nombres de dominio que usan la palabra «corona". A continuación, enumeramos algunos dominios como maliciosos:

- acccorona [.] com
- alphacoronavirusvaccine [.] com
- anticoronaproducts [.] com
- beatingcorona [.] com
- beatingcoronavirus [.] com
- bestcorona [.] com
- betacoronavirusvaccine [.] com
- buycoronavirusfacemasks [.] com
- byebyecoronavirus [.] com
- cdc-coronavirus [.] com
- combatcorona [.] com
- contra-coronavirus [.] com
- corona-blindado [.] com
- corona-crisis [.] com
- corona-emergencia [.] com
- corona explicada [.] com
- corona-iran [.] com
- corona-ratgeber [.] com
- coronadatabase [.] com
- coronadeathpool [.] com
- coronadetect [.] com
- coronadetection [.] com

Como funcionan estos ataques_

La realidad es que todos estos ataques utilizan un vector de infección que podríamos considerar "tradicional" y que tenemos sumamente cubierto en nuestras soluciones Endpoint Cytomic.Los mecanismos de detección y bloque más efectivos en estos casos son:

- El servicio que clasifica todo binario, permitiendo su ejecución solo si es verificado por nuestro sistema de Inteligencia Artificial en la nube, el **Servicio gestionado Zero-Trust Application.**
- Las tecnologías de detección en el endpoint, especialmente la detección de **Indicadores de Ataque (IOA) por comportamiento y contexto.**

De lo que estamos viendo en nuestros laboratorios, el ciclo del ataque más habitual es email/spam utilizando técnicas de ingeniería social y que contiene un dropper que descarga un binario en esta ubicación C:\Users\user\AppData\Local\Temp\qeSw.exe y con hash 258ED03A6E4D9012F8102C635A5E3DCD. En las soluciones Cytomic la detección del dropper es un Trj/GdSda.A.

Este binario se encarga de cifrar la maquina (proceso: vssadmin.exe) y eliminar las shadow Copies invocando al proceso conhost.exe

Fuentes oficial de IoCs_

El Centro Criptográfico Nacional (https://www.ccn.cni.es/index.php/es/) mantiene un listado exhaustivo de Indicadores de Compromiso (IoCs) a nivel de hashes, IPs y Dominios.

La información es accesible aquí: https://loreto.ccn-cert.cni.es/index.php/s/oDcNr5Jqqpd5cjn

Como defenderte contra estas y otras ciber amenazas_

Las soluciones avanzadas de endpoint de Cytomic, gracias al **Servicio gestionado Zero-Trust Application** que clasifica de todos los binarios antes de su ejecución y bloquea aquellos maliciosos, son sin duda un gran aliado en estas y muchas otras campañas.

Este servicio habilita un mecanísmo altamente eficiente y desatendido de detección y bloqueo de malware y ransomware, antes incluso de darle oportunidad a ejecutarse, independientemente de si son variantes nuevas o nuevos dominios de descarga, como en el caso de las variantes de malware COVID-19.

Las tecnologías endpoint de detección de **Indicadores de Ataque (IOA) por comportamiento y contexto** detectan y bloquean comportamientos inusuales en los dispositivos protegidos, como la descarga desde un word de un ejecutable o el acceso a una URL desconocida o maliciosas, bloqueando inmediatamente en intento de compromiso, denegando la ejecución y la conexión.

Más información en_
cytomic.ai

Contactanos en_
sales.hq@cytomicmodel.com
+34 900 840 407