grupo ICA
Sistemas y Seguridad

Informe de Ciberseguridad COVID 19

Aprovechando el Pánico del Coronavirus

19/03/20

Servicios de Ciberseguridad

Informe

Control de versiones

Versión	Responsable			Modificación
1.0	Autor:	ICA SyS Ciberseguridad	19/03/2020	Versión inicial

Contenido

1. RESUMEN EJECUTIVO

La aparición de la enfermedad por coronavirus 2019 (COVID-19), que se originó a finales de diciembre de 2019, ha traído consigo el caos en muchos sectores económicos: finanzas, industria y salud, por nombrar algunos. Además, este caos también ha originado una nueva amenaza de ciberseguridad, desencadenando la creación de campañas de phishing con la temática del COVID-19 y la creación de dominios relacionados con él.

La amenaza técnica inminente que rodea al COVID-19 parece estar, en la mayoría de los casos, relacionada con campañas de phishing en las que los atacantes indican que los archivos adjuntos contienen información sobre la actualidad del COVID-19 en el mundo.

En los últimos días se han observado una larga lista de atacantes y malware que emplean estas técnicas, incluyendo en la lista de malware Trickbot, Lokibot y el agente Tesla. Estos ataques están dirigidos a un amplio conjunto de víctimas, incluidas las de los Estados Unidos, Italia, España, Ucrania e Irán, en particular. Los actores de las amenazas también se han esforzado por ganar la confianza de las víctimas mediante el uso de marcas asociadas con los Centros para el Control y la Prevención de Enfermedades de los EE. UU. (CDC), la Organización Mundial de la Salud (OMS o WHO por sus siglas en Ingles), así como con agencias de salud específicas de cada país y empresas como FedEx.

En la sección de Anexos del presente documento se añade una lista de IOCs y Reglas Yara del actor APT36, actualmente activo.

1.1 Aspectos clave

A partir del 11 de marzo de 2020, se ha observado que el COVID-19 ha sido utilizado principalmente por los ciberdelincuentes para sus campañas de phishing. Parece bastante claro, y ya lo estamos comprobando, que a medida que se propaga y aumentan los casos de COVID-19 en el mundo, **tanto los cibercriminales como los diferentes actores en cada nación, explotan cada vez más la crisis como vector de ataque.**

Los ciberdelincuentes a menudo usan la marca de organizaciones "confiables" en estos ataques de phishing, especialmente la Organización Mundial del Salud y los Centros para el Control y la Prevención de Enfermedades de EE.UU. y otras organizaciones entorno al sector de la salud nacional, con el fin de **generar credibilidad y hacer que los usuarios abran archivos adjuntos o hagan clic en enlaces.**

El número de referencias a COVID-19 en relación con los ataques cibernéticos ha aumentado en los últimos dos meses, incluidos los señuelos de phishing específicos de cada país a medida que el virus se propaga. Probablemente, mientras dure el brote, COVID-19 continuará utilizándose como señuelo y surgirán nuevas versiones dirigidas a nuevos países.

La cantidad de dominios recientemente registrados relacionados con el coronavirus ha aumentado desde que el brote se ha generalizado, con actores de amenazas creando infraestructura para apoyar campañas maliciosas que se refieren al COVID-19. El pico inicial en los registros de dominios coincidió con un gran pico en los casos reportados de COVID-19 a mediados de febrero, un posible indicador de que **los atacantes comenzaron a darse cuenta de la utilidad de COVID-19 como vector de ataque.**

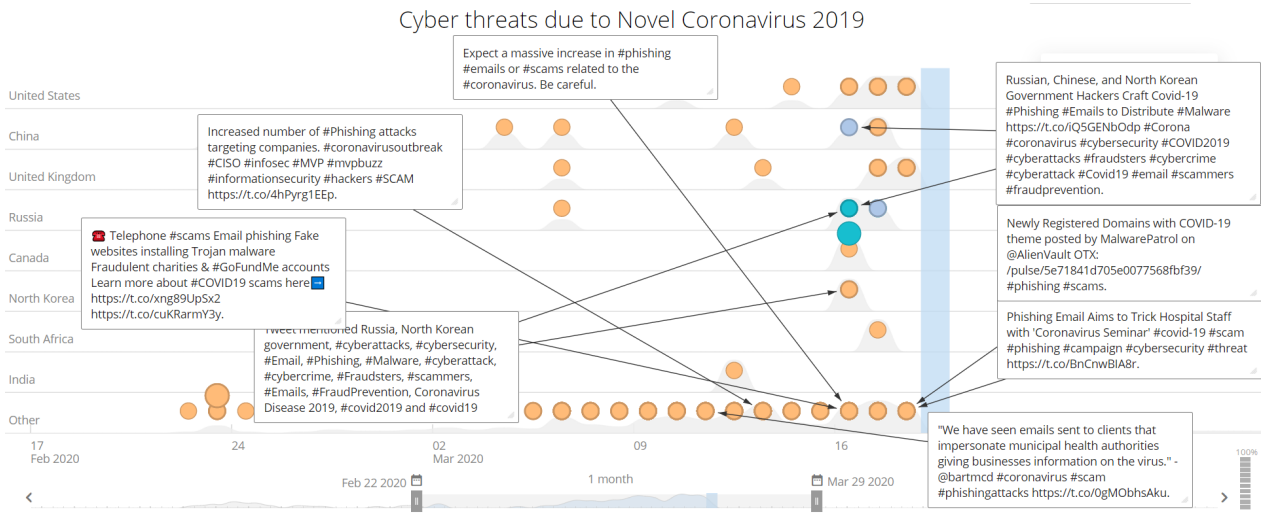
1.2 Análisis de acontecimientos

La enfermedad viral y respiratoria que se ha extendido por todo el mundo conocido como coronavirus 2019 (COVID-19), desde que fue detectado por primera vez en Wuhan, China, el 31 de diciembre de 2019 se ha extendido por todo el mundo, causando miedo y pánico a medida que avanza el brote. Hasta la fecha, más de 215.000 personas han sido infectadas en 164 países de todo el mundo y alrededor de 8.000 han muerto.

Los ciberdelincuentes y los actores de amenazas han comenzado a aprovecharse de la propagación del virus y la incertidumbre y el miedo asociados con él, desplegando campañas de phishing que utilizan COVID-19 como reclamo para que las víctimas descarguen malware o den información personal. Para comprender el uso de COVID-19 por parte de ciberdelincuentes se ha establecido una relación entre la cantidad de dominios creados asociados con el "coronavirus" en 2020 y la cantidad de referencias a ciberataques o exploits relacionados con "coronavirus" o "COVID -19".

1.3 Ciberataques que utilizan el COVID-19

En los últimos meses, se ha observado un aumento en el número de instancias que utilizan COVID-19 como vector de ataque en cualquier incidente cibernético, como se muestra en la siguiente línea de tiempo:



Fuente: Recorded Future

A partir de finales de enero de 2020, y durante el mes de Febrero se ha ido viendo un aumento de ciberataaues a medida que ha ido aumentando el número de infecciones por COVID-19, presentando picos altos en el mes actual, Marzo. A pesar de que el COVID-19 se utiliza como parte de diferentes tipos de ataques, parece claro que el preferido por los ciberatacantes es utilizarlo como señuelo en campañas de phishing.

- **Malware AZORult propagado mediante adjuntos de phishing que usaban COVID-19 como señuelo**. A principios de febrero de 2020 los investigadores de Proofpoint observaron una campaña de phishing temática de COVID-19 dirigida al sector industrial, finanzas, transporte, farmacéutica y cosmética. Estos ataques incluyeron correos electrónicos que contenían archivos adjuntos de documentos de Microsoft Office diseñados para atraer a las víctimas y explotar la vulnerabilidad de

Microsoft Office **CVE-2017-11882**, que permite a los atacantes ejecutar código arbitrario en el contexto del usuario. Los documentos maliciosos contenían lo que se supone es un aviso sobre el impacto del virus en la industria del transporte marítimo. Una vez que se abre el documento malicioso, instala el software de robo de información "AZORut". Sin embargo, esta cepa de AZORult no descargó ransomware, como lo ha hecho en ataques anteriores. Según los investigadores de Proofpoint, los correos electrónicos maliciosos se originaron en grupos de Rusia y Europa del Este.

- **CODVID-19 Phishing para distribuir Emotet en Japón**. En enero de 2020, los investigadores de IBM X-Force observaron que los cibercriminales están utilizando el coronavirus como phishing para distribuir Emotet en una campaña dirigida a Japón. Los correos electrónicos de phishing afirmaban que los documentos adjuntos de Microsoft Word contenían información y actualizaciones, pero en realidad contenían una macro maliciosa de VBA que instala un script de PowerShell, que luego descarga el troyano Emotet.
- **Kaspersky publicó un artículo sobre correos electrónicos de phishing que emulaban los CDC**, en particular de correos electrónicos que contenían los dominios cdc-gov[.] org y cdcgov[.] org. En una instancia, la URL contenida en un correo electrónico de phishing que llevaba a una página falsa de Microsoft Outlook, diseñada para convencer a las víctimas de ingresar sus credenciales. En otro caso, se pidió a las víctimas que donaran Bitcoin a los CDC para ayudar a la búsqueda de una vacuna.
- **La firma de seguridad Cofense identificó una campaña de phishing diferente, aunque más sofisticada**, utilizando el tema "COVID-19 - Now Airborne, Increase Community Transmisión" que parece originarse desde la dirección CDC-Covid19[@]cdc[.]gov. Cuando las víctimas hacen clic en la imagen incrustada, son redirigidas a una página de inicio de Microsoft Outlook, y al ingresar sus credenciales legítimas, son redirigidas nuevamente a un sitio web legítimo de CDC. El hecho de que estos correos electrónicos de phishing parezcan provenir de una dirección legítima en el dominio de los CDC se debe a que el actor de la amenaza oculta a propósito el verdadero origen del correo electrónico. El engaño se hizo posible al insertar un comando SMTP HELO que le indica al servidor de correo electrónico que trate el correo electrónico como si se hubiera originado en el dominio cdc[.]gov a pesar tener un remitente con un dominio e IP diferentes.
- **Cofense también identificó otra campaña de suplantación de identidad hacia Italia** con correos del estilo "Atención: Lista de empresas afectadas con coronavirus, 02 de marzo de 2020". Los correos electrónicos de phishing estaban dirigidos principalmente a direcciones de correo electrónico italianas y contenían documentos maliciosos de Microsoft Office con macros VBA incrustadas que se utilizaron para descartar Trickbot. El troyano bancario Trickbot se puede utilizar para robar información confidencial de las víctimas, así como para eliminar un malware adicional. El asunto del correo electrónico utilizado en esta campaña fue "Coronavirus: informazioni importanti su precauzioni", y para reforzar la credibilidad del señuelo adjunto, el supuesto autor fue "Dr. Penélope Marchetti", un representante de la OMS en ese momento.
- **El equipo de investigación de seguridad @issuemakerslab observó un documento malicioso de Microsoft Word que descargaba el malware BabyShark de Corea del**

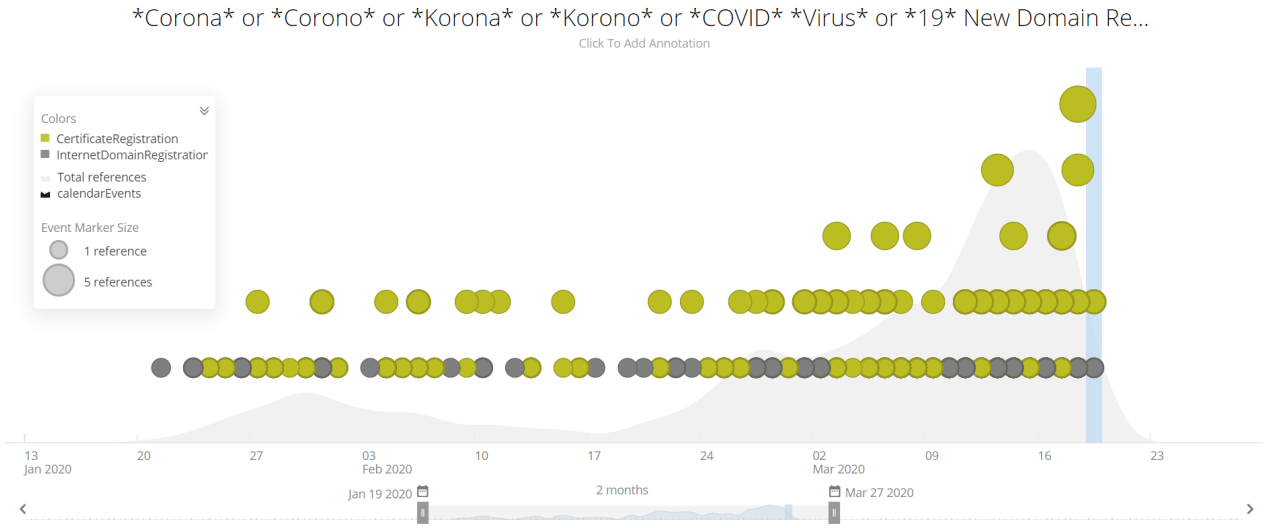
Norte que afirmaba contener información sobre la respuesta de Corea del Sur al virus COVID-19.

- **El equipo de investigación de seguridad @reddrip7 detecto una campaña que denominó "TrickyMouse" dirigida a Ucrania.** Detectaron un archivo adjunto malicioso de un documento de Word llamado "KOPOHaaipyCHa iHcÞeK4ifi COVID-19.doc" que contenía una puerta trasera C#. Los investigadores sospechan este malware está relacionado con la APT de Hades. Debido a la presencia de la cadena "TrickyMouse" en el malware, la han denominado a la campaña "TrickyMouse". El documento utiliza la marca registrada de la OMS y el Centro de Salud Pública del Ministerio de Salud de Ucrania como señuelo y se utilizó para atacar a Ucrania.
- **También @reddrip7 identificó una campaña de phishing temática de COVID-19 que utilizó un documento señuelo que contenía Nanocore RAT dirigido a la empresa de fabricación de productos químicos de Corea del Sur**, Dongwoo Fine-Chem Corporation.
- **Otra campaña utilizó la marca registrada FedEx en un ataque de phishing**, con el objetivo de proporcionar a las víctimas información sobre las operaciones globales de FedEx mientras continúa el brote de COVID-19. Los correos contenian un archivo adjunto titulado "Customer Advisory.PDF. exe" que, al abrirse, infectaba a la víctima con el software Lokibot.
- **Lokibot se distribuyó adicionalmente en una campaña de phishing que usó COVID-19 como señuelo, reclamando ser enviado por el Ministerio de Salud en la República Popular de China**. Los correos electrónicos afirmaban contener información sobre las regulaciones de emergencia que rodean al virus con la línea de asunto "Ordenanza de Regulación de Emergencia" (sic), y tenían un archivo adjunto RAR de Windows con la extensión .arj. Una vez abierto, el archivo malicioso adjunto infecta a la víctima con Lokibot, contactando de inmediato con una dirección IP maliciosa y exponiendo las credenciales del usuario.
- **También el troyano bancario Grandoreiro** se distribuía a través de sitios que utilizan la epidemia de coronavirus como señuelo. El usuario de Twitter @JAMESWT_MHT compartió una instancia del troyano utilizado como parte de esta campaña. Los sitios web muestran información sobre el coronavirus con un video incrustado, a través del cual, y una vez que el usuario hace clic, se descarga el ejecutable Grandoreiro. **Según el usuario de Twitter @ESETresearch, el malware está actualmente dirigido a usuarios en Brasil, México y España**.

Además, el coronavirus ha sido "*weaponizado*" como una forma de difundir spyware por el gobierno iraní. El Ministerio de Salud de Irán envió un mensaje a las víctimas aconsejándoles que descarguen una aplicación específica para monitorizar los posibles síntomas de COVID- 19. Esta aplicación era, en realidad, spyware. La aplicación maliciosa de Android, llamada ac19.apk, es una recopilación de servicios de localización de víctimas y monitorización de la actividad física de un usuario (como caminar o sentarse), ostensiblemente para determinar a dónde va el usuario y cuándo. La aplicación se distribuye en un sitio web creado por el gobierno iraní, https://ac19[.]ir/

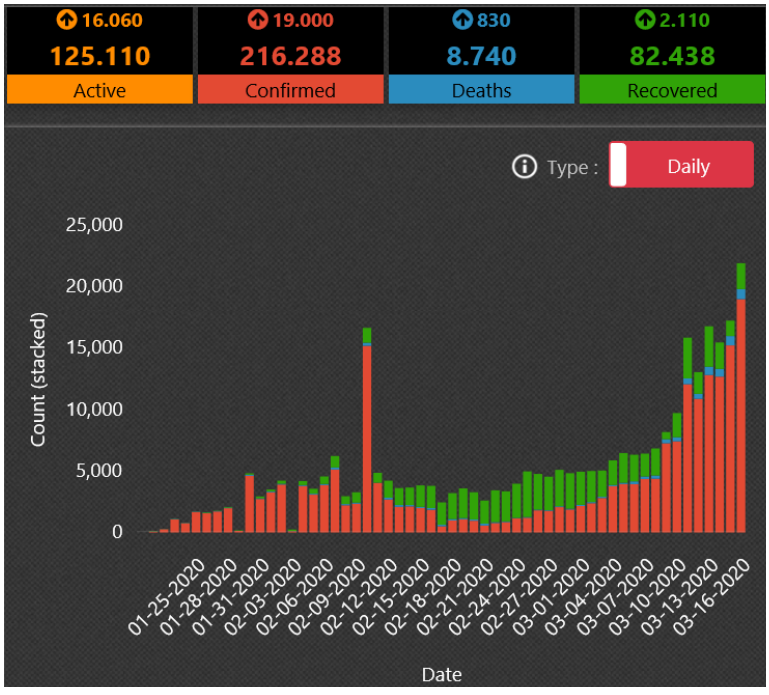
1.4 Registro de dominios

A partir de mediados de Enero de 2020, el número de registros de dominio en relación al COVID-19 comenzó a aumentar, mostrando un pico adicional a partir de Marzo, como se muestra en la imagen.



Fuente: Recorded Future

Este pico coincide con el pico más grande de un solo día en el número de casos COVID-19, como se ve en el cuadro a continuación y la siguiente evolución:



Fuente: UNIVERSITY of VIRGINIA

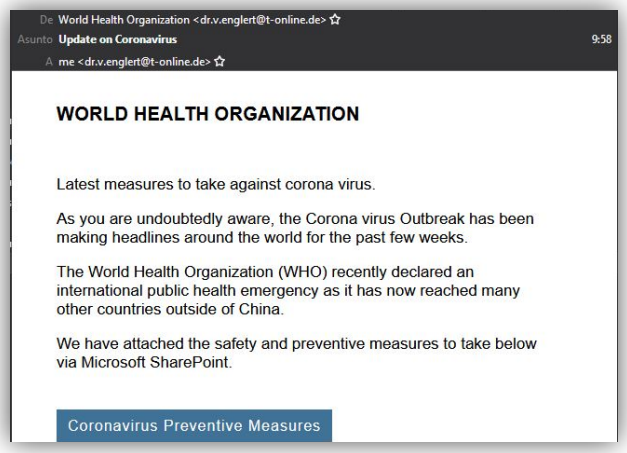
No es posible confiar en que el aumento de registros de dominio a mediados de febrero con el aumento de casos durante ese período de tiempo tenga una relación causa - efecto. Sin embargo, por otro lado, posiblemente indica que los ciberdelincuentes y otros

actores de amenazas dirigieron sus miradas a la evolución del brote como objetivo de mecanismo de propagación de malware.

1.5 Phishing

Atendiendo a la actividad de ciberdelincuentes y otros actores de amenazas que hacen referencia al COVID-19, principalmente se observan ataques de phishing diseñados para obtener información personal de las víctimas o para lanzar malware para la infección. Debido a que estos ataques se aprovechan del miedo y a menudo utilizan un sentido de urgencia para que la víctima haga clic, se recomienda tomar las siguientes precauciones:

- Ser especialmente cauteloso con cualquier comunicación por correo electrónico o de otro tipo que pretenda provenir de los CDC, de la OMS o de cualquier entidad de salud nacional, incluso si parece provenir de una dirección legítima en los dominios oficiales. En muchas ocasiones los correos de phishing utilizan la marca de estas dos organizaciones como parte del señuelo. Además, esta tendencia continuará a medida que el brote siga propagándose por el mundo. Los actores de amenazas incorporan una URL con sitios web legítimos como texto de tinta, mientras que la tinta subyacente es maliciosa. La Comisión de Comercio de Federa de EE. UU. Ha sugerido que las partes interesadas visiten los sitios web conocidos de la OMS y los CDC directamente para obtener información actualizada y ser cautelosos acerca de cualquier correo electrónico que pretenda ser de esas entidades. A menos que su organización esté en el campo de la atención médica, es muy diferente que estas agencias le envíen correos electrónicos sobre COVID-1 9. También tenga en cuenta que los CDC, la OMS y otras organizaciones no aceptan pagos de criptomonedas, por lo que cualquier solicitud de este tipo debe considerarse maliciosos.



Fuente: twitter

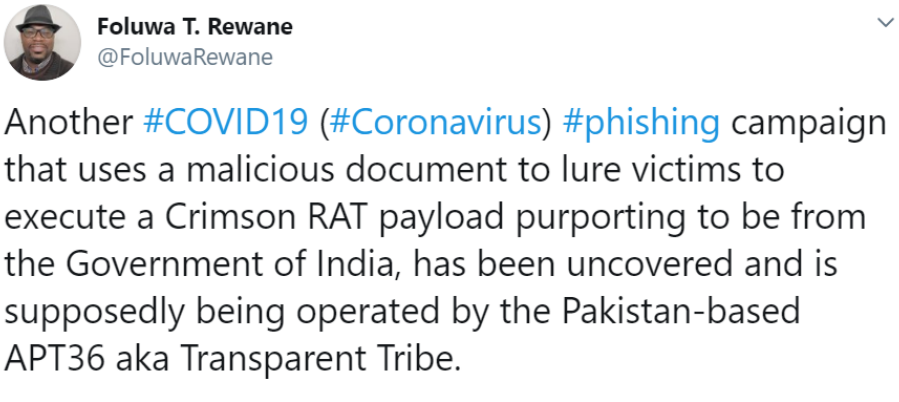
- Si bien muchas organizaciones legítimas enviarán correos electrónicos con respecto a las precauciones que están tomando para minimizar la amenaza de COVID-19, el uso de la marca corporativa legítima se ha utilizado para enviar material a las víctimas. Los correos electrónicos maliciosos a menudo usan el lenguaje creando un sentido de urgencia (aunque a menudo con mala gramática

u ortografía), o archivos adjuntos o enlaces que se dice que contienen información adicional en lugar de ser informativos. Los usuarios deben evitar abrir archivos adjuntos, pero es aconsejable tratar todos los correos electrónicos relacionados con el brote de COVID-19 con precaución.

- Al igual que con todos los ataques de phishing, se recomienda que los usuarios deshabiliten las macros en Microsoft Office para cualquier usuario que no lo requiera. Muchos de los archivos adjuntos málicos observados por los analistas del futuro registrado en asociación con COVID-19 utilizaron macros VBA como una parte inicial de la infección de las víctimas. Las macros de VBA siguen siendo mecanismos de infección populares para documentos maliciosos que se utilizan como phishing, y los analistas evalúan con gran confianza que esta tendencia continuará.

Fuente: CCN-CERT

- Recientemente se han observado referencias a una campaña de phishing del grupo de ciberdelincuentes APT36 que aprovecha la preocupación del coronavirus para difundir un troyano de acceso remoto RAT. En el correo adjuntan un supuesto documento con recomendaciones.



Fuente: twitter

2. RECOMENDACIONES ICA SISTEMAS Y SEGURIDAD

2.1 Recomendaciones de ICA Sistemas y Seguridad

Además de las campañas internacionales, este tipo de campañas de phishing en nuestro país pueden venir en forma de diferentes suplantaciones de organismos dedicados a la sanidad y pueden distribuirse por diferentes vías como WhatsApp, no solo por correo electrónico.

Recomendamos a los usuarios que verifiquen la legitimidad de la URL antes de hacer clic en un enlace enviado por correo electrónico, estén atentos a los archivos adjuntos sospechosos y eviten habilitar macros en documentos no confiables para evitar ataques de phishing.

En referencia a esto, y además de la expansión de ransomware, phishing y malware relacionado con COVID-19 hay un aumento continuo en la desinformación relacionada con el brote. En respuesta a la difusión de información falsa o engañosa, las redes sociales y las compañías de tecnología Reddit, Google, Facebook, Twitter, LinkedIn, Microsoft y YouTube anunciaron el 16 de marzo que trabajarían para combatir la propagación de información fraudulenta sobre el virus y coordinar con entidades gubernamentales en relación con sus esfuerzos.

Sin embargo, esta desinformación relacionada con el COVID-19 se está propagando muy rápidamente a través de otros medios como WhatsApp, correo electrónico, mensajería instantánea incluido Facebook, YouTube y mensajes de texto de servicio de mensajes cortos (SMS) a nivel mundial. Estos mensajes pretenden originarse en una fuente confiable pero contienen información engañosa sobre medicamentos, transmisión de enfermedades, tratamiento, libertad de movimiento, limitación de transporte, cuarentenas u otra información vital relevante para la propagación, diagnóstico, respuesta o tratamiento de la enfermedad. Estos mensajes se propagan rápidamente en formato de texto y audio de momento en España, Francia, Bélgica, Alemania, Polonia, los Estados Unidos y Portugal. **En este sentido se recomienda verificar y contrastar las fuentes de información vital, aunque parezcan fiables a simple vista.**

2.2 Referencias

El **Centro Criptológico Nacional** presenta un documento en el que aborda unas recomendaciones básicas ante las campañas de malware y de desinformación que aprovechan la pandemia del coronavirus.

https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/196-ciberconsejos-cibercovid19/file

Del mismo modo, a través de Twitter ha creado un hilo bajo el hastagh: **#NoTeinfectesConElMail**, que irá actualizando a medida vayan apareciendo nuevas campañas.

Además, el CCN-CERT también pone en marcha iniciativas para implantar un teletrabajo seguro, con la publicación (18/03/2020) de unas buenas prácticas para situaciones de teletrabajo que se une al documento sobre Acceso Remoto Seguro que desarrolló la semana pasada.

https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4691-ccn-cert-bp-18-recomendaciones-de-seguridad-para-situaciones-de-teletrabajo-y-refuerzo-en-vigilancia-1/file.html

https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/abstract/191-abstract-politica-de-acceso-remoto-seguro/file

3. APÉNDICE A

3.1 Indicadores de Compromiso IOCs

3.1.1 Agent Tesla

hxxps://healing-yui223.com/cd[.]php
hxxps://www.schooluniformtrading[.]com[.]au/cdcgov/files/
hxxps://onthefx[.]com/cd[.]php
hxxps://urbanandruraldesign[.]com[.]au/cdcgov/files
hxxps://gocycle[.]com[.]au/cdcgov/files/
150[.]95[.]52[.]104
118[.]127[.]3[.]247
153[.]120[.]181[.]196
112[.]140[.]180[.]26
13[.]239[.]26[.]132
SAFETY PRECAUTIONS.rar
SAFETY PRECAUTIONS.exe
05adf4a08f16776ee0b1c271713a7880 Ef07feae7c00a550f97ed4824862c459
Postmaster[@]mallinckrodt[.]xyz
brentpaul403[@]yandex[.]ru

3.1.2 Emotet

8C809B4AC6D95CE85A0F04CD04B7A7EA 586FB4A6FFDFEB423F1F1782AAA9BB9F
8800EBD065B52468FA778B4527437F5A 379959D80D0BFC45AAB6437474D1F727
hxxp://109.236.109.159:8080/vnx8v
hxxp://85.96.49.152/6oU9ipBIjTSU1
hxxp://186.10.98.177/faHtH2y
hxxp://erasmus-plius.tomasjs.com/wp-admin/KfesPCcG/
hxxp://easytogets.com/xfxvqq/UXbKAbm/
hxxp://drhuzaifa.com/wp-includes/2i48k7-evv28gw-205510/
hxxp://dewarejeki.info/wp-includes/up58jauc-pum2w-630352/
hxxp://dewakartu.info/wp-includes/BRVMFYvIR/

3.1.3 CDC-Related

cdc-gov.org
Cdcgov.org
CDC-Covid19[@]cdc[.]gov

3.1.4 Trickbot

hxxps://185[.]234.73.125/wMB03o/Wx9u79.php
23[.]19.227.235
45[.]128.134.14
hxxps://45.128.134.14/C821al/vc2Tmy.php?
insiderppe[.]cloudapp.net
F21678535239.doc
F21678535350.doc
3461B78384C000E3396589280A34D871C1DE3AE266334412202D4A6A85D02439

8eb57a3b520881b1f3fd0073491da6c50b7284dd8e66099c172d80ba33a5032f

3.1.5 Lokibot

Customer Advisory.PDF.exe
906EFF4AC2F5244A59CC5E318469F2894F8CED406F1E0E48E964F90D1FF9FD88
kbfvzoboss.bid/alien/fre.php
198.23.200[.]241
hxxp://198.23.200[.]241/~power13/.xoiaspxo/fre.php

3.1.6 TrickyMouse

1db31ada5f1ac2411ef33790244343946b741cd603745257a4612c5d2e6a4052
9aea43b22f214228caf4fc714f426c0a140b7dd70b010bf3778cd1c0ec440851
1545401f661f9326f5c604e1a025e811079ba4eace9d3830a05c5e4aa666803e
62dd16724874e0b05257118fb06427a6aeb839602bce52e6a139dc379f538bed
09400e30105b10cd484a2159e8496accd779045ac6775b351b80949a54e772df
5b12f8d817b5f98eb51ef675d5f31d3d1e34bf06befba424f08a5b28ce98d45a
3b701eac4e3a73aec109120c97102c17edf88a20d1883dd5eef6db60d52b8d92
2dfb086bc73c259cac18a9cb1f9dbbc8 6c73d338ec64e0e44bd54ea61b6988b2
Коронавірусна інфекція COVID-19.rar
Коронавірусна інфекція COVID-19.doc
cloud-security.ggpht[.]ml
cloud-security.ggpht[.]ml
123.161.61[.]55
145.239.23[.]7
192.35.177[.]64

3.1.7 CovidLock

coronavirusapp[.]site
dating4sex[.]us
dating4free[.]us
perfectdating[.]us
redditdating[.]us
69a6b43b5f63030938c578eec05993eb
c844992d3f4eecb5369533ff96d7de6a05b19fe5f5809ceb1546a3f801654890
phc859mgge638@inbox.ru

3.2 Dominios registrados

coronavirusoutbreakmap[.]com
www.coronavirusoutbreakmap[.]com
corona-virus[.]healthcare
coronavirusprotectionmasks[.]org
www[.]coronavirusprotectionmasks[.]org
coronavirus[.]1point3acres[.]com
coronavirus[.]dev
wuhancoronavirus[.]blogspot[.]com
coronavirusdata[.]org
www[.]coronavirusdata[.]org
coronamap[.]live
coronamap[.]site
coronatoken[.]org
bestcoronavirusprotect[.]tk
coronavirusnigeria[.]ng4n[.]com
corona[.]yagi[.]news
info-coronavirus[.]be
www[.]info-coronavirus[.]be
coronavirusnews[.]world
coronavirus[.]app
endcoronavirus[.]org
coronavirus-reports[.]com
coronavirus-map[.]com
www[.]endcoronavirus[.]org
coronavirusreport[.]buzz
www[.]coronavirusreport[.]buzz
coronavirusupdates[.]eu
coronavirus-monitor[.]ru
coronavirus123[.]com
coronavirusstatus[.]space
coronaviruszone[.]com
coronavirusofficialnews[.]com
flashnewscoronavirus[.]blogspot[.]com
coronatracker[.]com
survivecoronavirus[.]org
corona[.]help
coronaboard-env[.]csgy3mxprm[.]eu-west-1[.]elasticbeanstalk[.]com
coronavirusinformationforus[.]blogspot[.]com
www[.]coronatracker[.]com
blogcoronacl[.]canalcero[.]digital
virus-corona[.]org
coronavirusupdates[.]online

coronavirus[.]zone
coronavirusthermometer[.]com
coronavirusawerness[.]blogspot[.]com
corona[.]kpwashingtonresearch[.]org
coronaviruses[.]com[.]au
mycoronavirus[.]world
coronavirus-in[.]space
coronawatch[.]eu
coronavirus[.]cms[.]am
www[.]coronawatch[.]eu
trackcorona[.]net
coronavirustechhandbook[.]com
coronavirus[.]tghn[.]org
coronawatch[.]now[.]sh
trackcorona[.]live
coronavirusupdate[.]tk
corona[.]kompa[.]ai
whereisthecoronavirus[.]com
thecoronaviruslive[.]info
wuhan-virus-coronavirus-advice[.]blogspot[.]com
coronastats[.]net
coronalive[.]just-shared[.]top
coronavirus19news[.]com
coronavirus[.]page
coronavirusdefense[.]com
www[.]thecoronaviruslive[.]info
coronavirusaware[.]xyz
coronavirus[.]koudaitour[.]com
coronavirusabc[.]com
www[.]trackcorona[.]live
corona-nearby[.]com
coronabye[.]com
trackcoronavirus[.]com
preventcoronaviruses[.]blogspot[.]com
www[.]coronavirusabc[.]com
vaccine-coronavirus[.]com
coronavirus-realtime[.]com
whatcoronavirus[.]com
corona[.]sums[.]ac[.]ir

3.3 YARA Rule APT36's CrimsonRAT

```
rule APT_PK_APT36_CrimsonRAT {
meta:
description = "Tracking of APT36 / Transparent Tribe Crimson RAT"
author = "GLES, Recorded Future, Insikt Group"
reference = "https://s.tencent.com/research/report/669.html"
date = "2019-08-07"
hash1 = "52d8aeed7f179a9936766ecca2ad9863eb25ac744c5740a047de1192caccca11"
hash2 = "3e3f7b53d719f3d2397817cb7b93ecb288f84e0e7aa11d190d4a8dd5416025e1"
strings:
$sp1 = "SystemProcess_CheckParentProcess" fullword ascii
$sp2 = "SystemProcess_Protect" fullword ascii
$down1 = "DownloadingDownloadJobs1" fullword ascii
$down2 = "DownloadingUpdate" fullword ascii
$get3 = "GetUpdateRequest" fullword ascii
$get4 = "GetRandomFilename" fullword ascii
$get5 = "GetDeleteRequest" fullword ascii
$get6 = "GetSerial" fullword ascii
$get7 = "GetRandomNum" fullword ascii
$get9 = "GetLocalIPAddress" fullword ascii
$get10 = "GEtRoad" fullword ascii
$break2 = "BreakJsonByCustomTask11" fullword ascii
$break3 = "BreakJsonByCustomTCP11" fullword ascii
$break4 = "BreakJsonByCustomTask1" fullword ascii
$break5 = "BreakJsonByCustomTask22" fullword ascii
$break6 = "BreakJsonByCustomTCP22" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize &lt; 100KB and pe.imphash() ==
"f34d5f2d4577ed6d9ceec516c1f5a744"
and ( all of ($sp*) or ( all of ($get*) and all of ($down*) and all of ($break*)))
}
```

---------- Fin del documento ----------