¡Bienvenidos!

Empezamos en unos minutos.

Con nosotros hoy

Alma Hernández
Key Account Manager
@KIPPEO

Jérémie Andrillon
Head of Engineering
@ThalesGroup

Frédéric Costé
Managing Director
@KIPPEO

THALES

COVID-19 : Cibersegurídad en tiempos de crisis

El agravamiento de la crisis de COVID-19 implica un aumento en el número de actores de amenazas que utilizan trampas vinculadas a esta noticia para comprometer a sus víctimas.

Desde campañas de phishing de cibercriminales que buscan robar dinero hasta grupos respaldados por gobiernos están intentando sacar partido de la preocupación desatada por el COVID-19 para infectar a sus blancos.

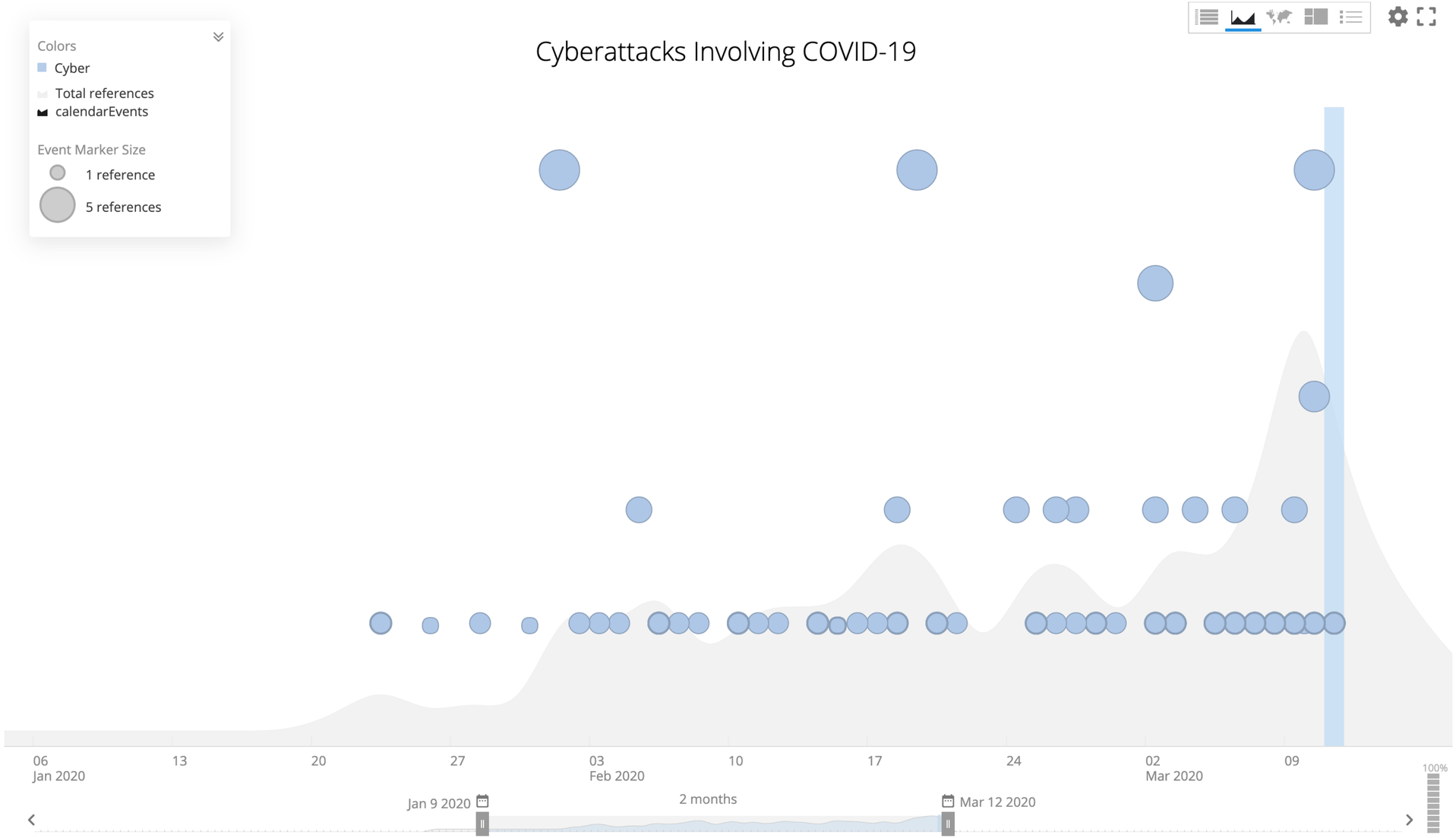
A nivel mundial, el 50% de los nombres de dominio creados desde diciembre y vinculados al tema de COVID-19 o Coronavirus pueden conducir a la inyección de software malicioso.

THALES

Agenda

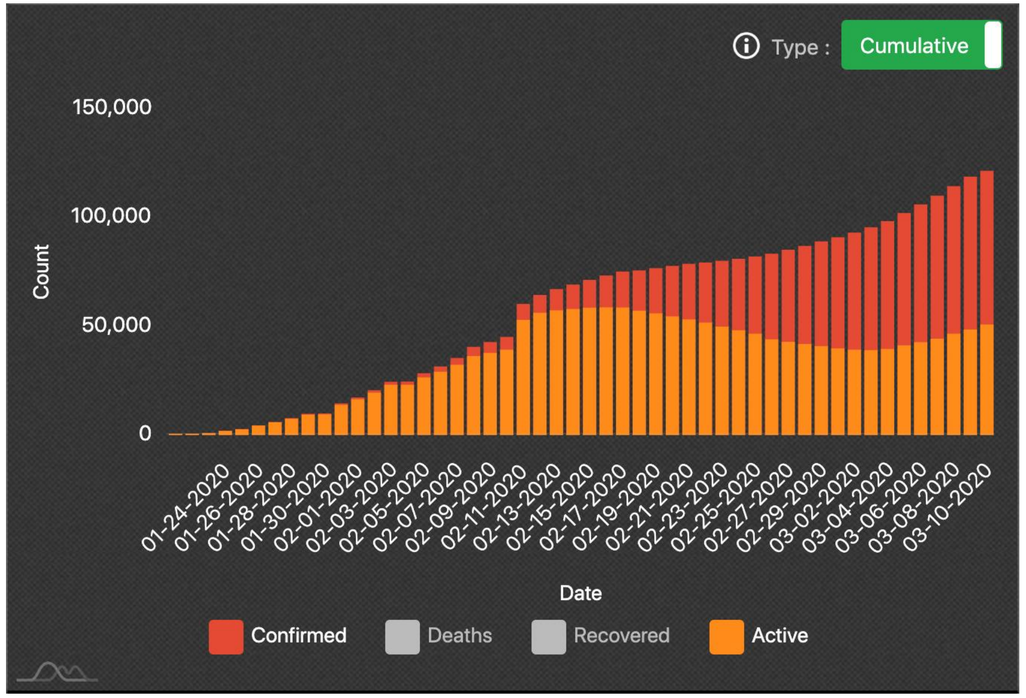
- Crisis del CODID-19 y ciberamenazas
- Metodología de defensa
- Recomendaciones : Gobierno del riesgo cibernético
- Recomendaciones : Controles de seguridad
- Preguntas y respuestas.

COVID-19 y ciberataques

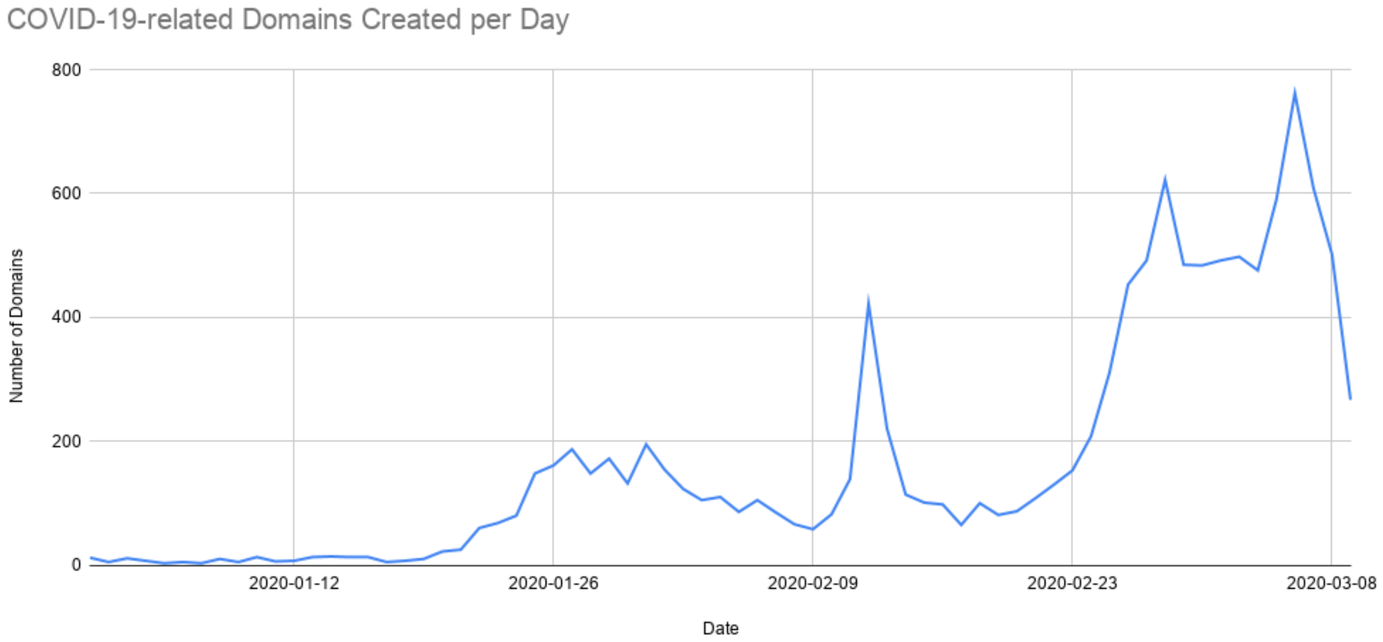


THALES

COVID-19 y dominios sospechosos 1/2



Graph showing number of COVID-19 cases per day over time.



COVID-19 y dominios sospechosos 2/2

coronavirusoutbreakmap[.]com

bestcoronavirusprotect[.]tk

corona-virus[.]healthcare

www.coronavirusoutbreakmap[.]com

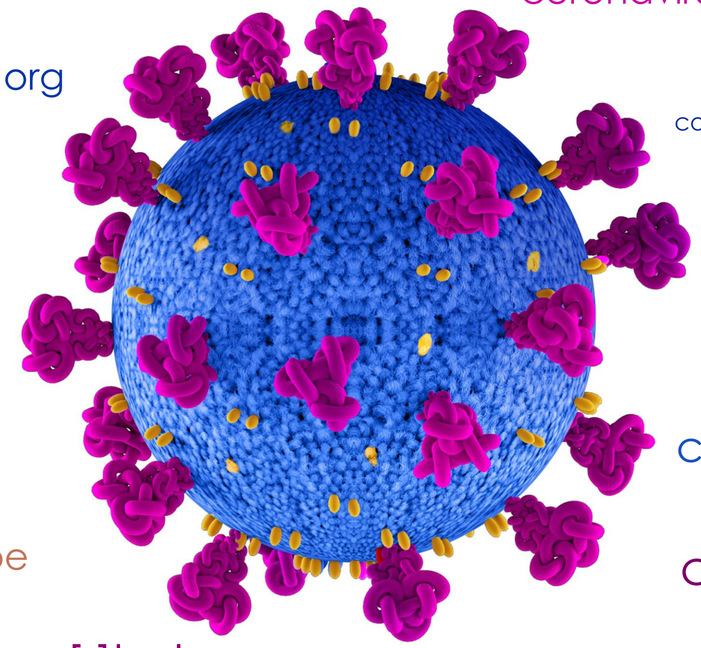
coronavirusprotectionmasks[.]org

www[.]coronavirusdata[.]org

coronavirus-map[.]com

www[.]coronavirusprotectionmasks[.]org

coronamap[.]site



coronavirusnews[.]world

survivecoronavirus[.]org

info-coronavirus[.]be

coronavirusdata[.]org

wuhancoronavirus[.]blogspot[.]com

corona[.]yagi[.]news

coronavirus[.]dev

coronatoken[.]org

www[.]info-coronavirus[.]be

coronavirusnigeria[.]ng4n[.]com

corona[.]help

stopcorona[.]org

coronavirus[.]1point3acres[.]com

coronavirusecuador[.]com

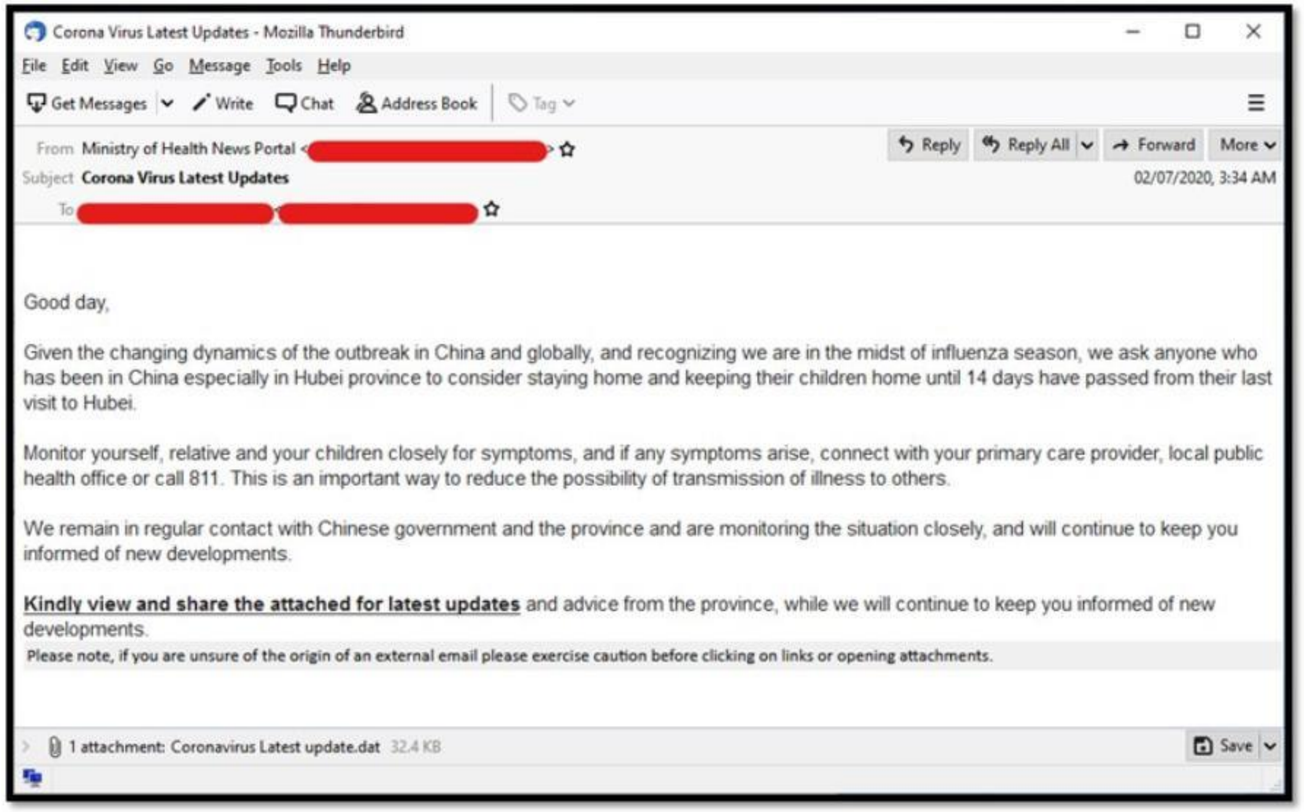
coronavirus[.]app

coronamap[.]live

vaccine-coronavirus[.]com

THALES

Campañas de Phishing 1/2



Campañas de Phishing 2/2

From: Ministerio de Salud <comunicados@minsalud.gov.co>
Sent: Thursday, March 5, 2020 10:43:34 AM
Subject: Detectamos en su sector la presencia de COVID-19 (Corona virus) intentamos comunicarnos via telefonica con usted .

La salud es de todos | Minsalud

Estimado ciudadano

Hemos intentado comunicarnos via telefonica con usted en el dia de hoy pero ha sido imposible , se trata de un tema muy delicado el cual le relatamos a continuación .

Detectamos en su sector la presencia de COVID-19 (Corona virus) es por eso que como medida preventiva hemos adjuntado los sitios en los cuales no le recomendamos visitar , ya que estos se encuentran a pocos metros de su residencia .

Adjuntamos un archivo pdf este se encuentra con una clave es : salud

Le recomendamos leer rapidamente esta informacion adjuntada recuerde que la salud es de todos

Línea de orientación sobre el nuevo CORONAVIRUS COVID-19: En Bogotá: +57(1) 330 5041 Resto del país: 018000955590

FALSO

+34 632 [redacted]
en línea

ALERTA POR CORONAVIRUS
Mensaje **urgente** del Ministerio de Sanidad:

http://www.[redacted]coronavirus.es

Rogamos colaboración ciudadana y máxima difusión de este mensaje
¡Compártelo en tus grupos de WhatsApp y en tus Redes Sociales!
¡¡PUEDES SALVAR VIDAS!!

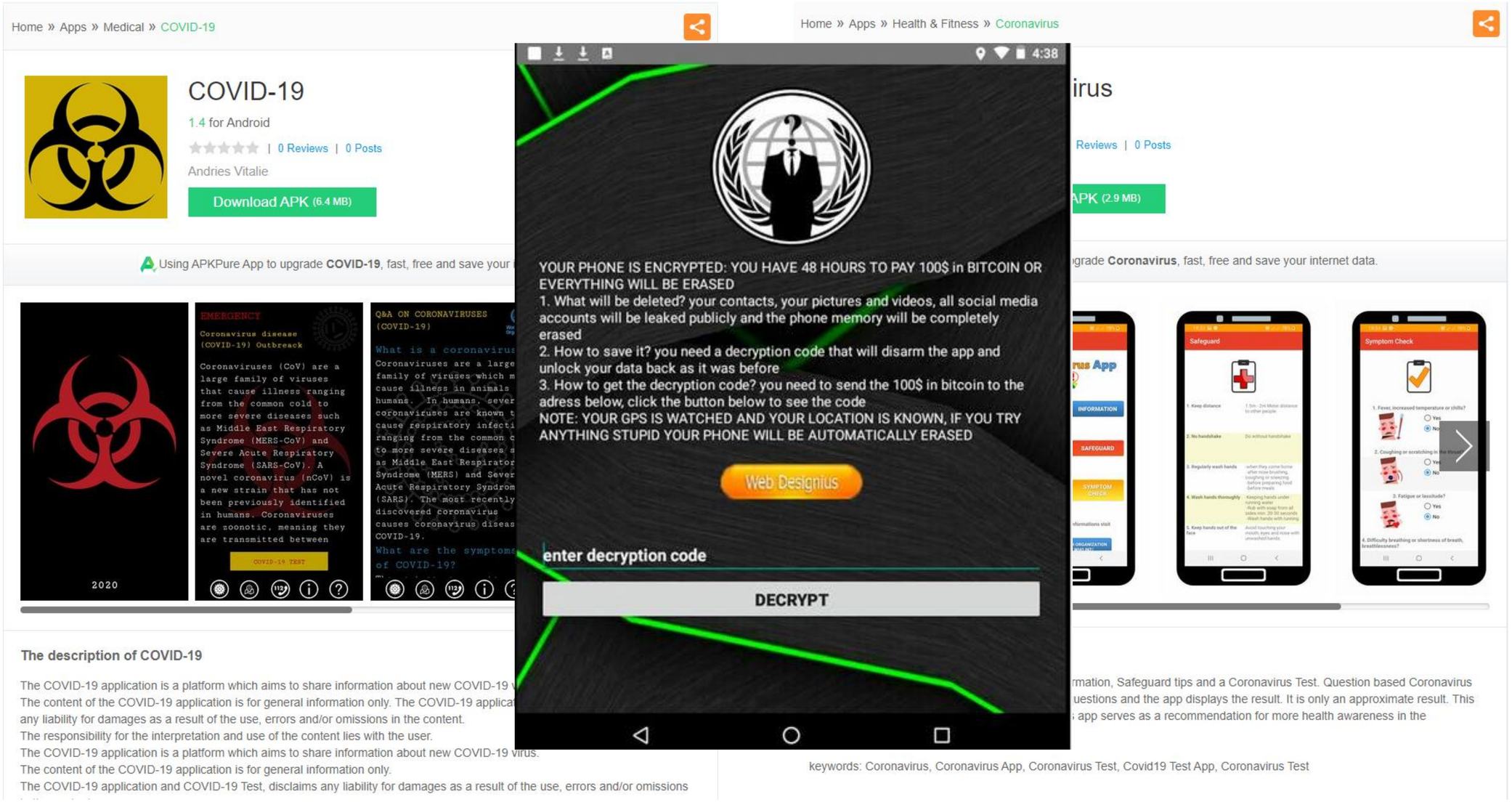
Es muy importante que siga las medidas de protección recomendadas:

DEPARTAMENTO DE DELITOS TELEMÁTICOS
UNIDAD CENTRAL OPERATIVA

#NiCaso

THALES

Aplicaciones móviles apócrifas?



COVID-19 : Metodología de defensa

- Favorecer canales confiables para obtener información.
- Restringir el número de canales y protegerse contra el sensacionalismo.
- Verificar información que se considere poco probable.
- Concientizar a sus teletrabajadores sobre las recomendaciones de Agencias Nacionales de Ciberseguridad.
- Contra las campañas de los principales atacantes, dar prioridad a la inteligencia de amenazas cibernéticas.
- Combinar herramientas de detección con inteligencia de amenazas cibernéticas para proteger sus sistemas.

THALES

Recomendaciones : Gobierno del ciber-riesgo

THALES

Ciber Riesgo

De acuerdo con el *NIST, se define el riesgo cibernético como el riesgo de pérdida financiera, interrupción operativa o daño, debido a la falla de las tecnologías digitales empleadas para funciones informativas y/o operativas introducidas a un sistema por medios electrónicos sin acceso autorizado, para el uso, divulgación, interrupción, modificación o destrucción de los sistemas.

**NIST: The National Institute of Standards and Frameworks.*

THALES

Riesgos relacionados con el Home Office 1/2

RIESGOS

El lugar de conexión del trabajador nómada puede presentar diferentes niveles de seguridad según el entorno. Esto depende no solo de la protección física y lógica del lugar (control de acceso mediante gafete, vigilancia), sino también de si las instalaciones se comparten o no entre varias organizaciones.

Uno de los casos más delicados es cuando el usuario trabaja desde un espacio completamente abierto al público (cafetería, biblioteca, etc.).

Del mismo modo, el hogar desde el que un usuario trabaja a distancia debe considerarse como un lugar no seguro, ya que es muy difícil evaluar el entorno desde el punto de vista de la seguridad.

Por lo tanto, la característica principal del nomadismo es el grado de exposición de la información, debido a la ubicación del usuario en lugares sin los medios de protección física que generalmente se implementan en las instalaciones de la organización.

THALES

Riesgos relacionados con el Home Office 2/2

RIESGOS

Este es el caso, por ejemplo:

- Cuando uno trabaja en el hotel durante un viaje de negocios
- Durante el viaje al trabajo, en los transportes públicos
- Cuando uno trabaja en salas de espera o en cualquier otro lugar público
- Cuando uno se conecta desde un espacio de trabajo compartido

En todos estos lugares de trabajo no controlados por la organización, se intensifican los siguientes riesgos:

- Pérdida o robo de equipos
- Situaciones de peligro del equipo, por ejemplo, durante una ausencia temporal del usuario
- Alteración de la información contenida en el equipo robado, perdido o prestado
- Acceso ilegítimo al SI de la organización
- Intercepción o incluso alteración de la información (pérdida de confidencialidad y / o integridad)

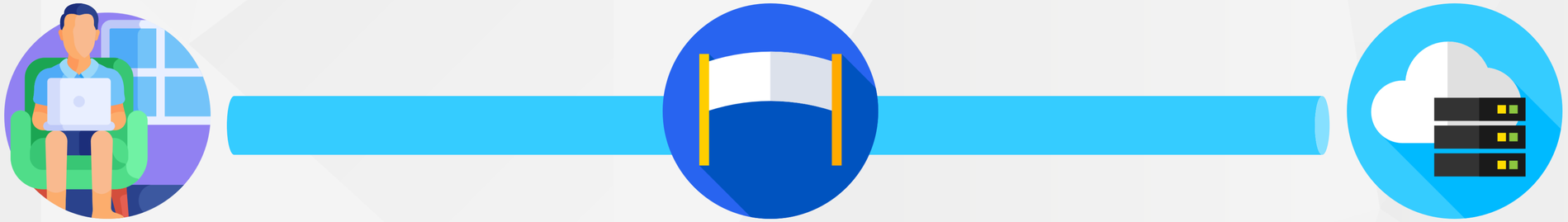
THALES

El riesgo cibernético en el gobierno corporativo

- ¿Cuáles son los principales activos críticos? ¿Están protegidos y cómo?
- ¿Cuál es la exposición de la empresa al riesgo cibernético y cuál es el nivel aceptable?
- ¿Qué controles existen para monitorear redes, aplicaciones en los dispositivos fijos y móviles de la compañía?
- ¿Quién es responsable de su protección?
- ¿La empresa cuenta con personal capacitado y con experiencia en prevención de riesgos cibernéticos?
- ¿Son suficientes los recursos asignados a la ciberseguridad?
- ¿Está la compañía preparada para un incidente mayor?

THALES

Arquitectura de nomadismo digital



Usuario
y su equipo
de acceso

Pasarela
de interconexión

Recursos accesibles
en el SI de la organización

THALES

kippeo.com/guia-recomendaciones-sobre-el-nomadismo-digital/

KIPPEO
GET STARTED IN HOLISTIC SECURITY

Home Servicios Nosotros Blog Contacto LLÁMANOS

GUÍA: RECOMENDACIONES SOBRE EL NOMADISMO DIGITAL

BUSCAR

Search Here

RECIBE UNA ASESORÍA SIN COSTO

Email*

Nombre*

Escríbenos

THALES

Recomendaciones : controles de seguridad

Cifrado
de disco duro

Bloqueo
de puertos USB

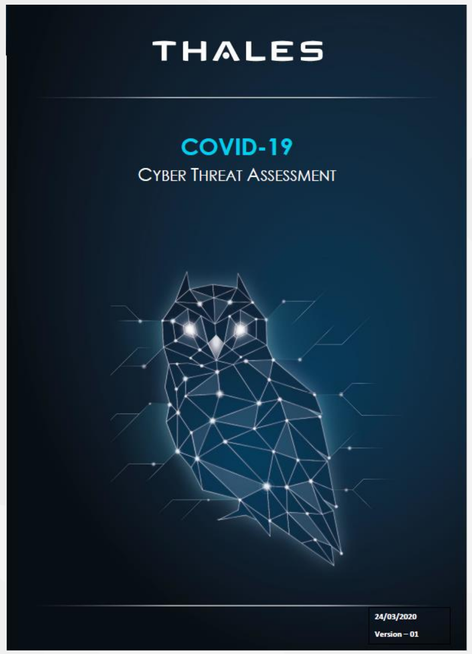
Uso
de VPN

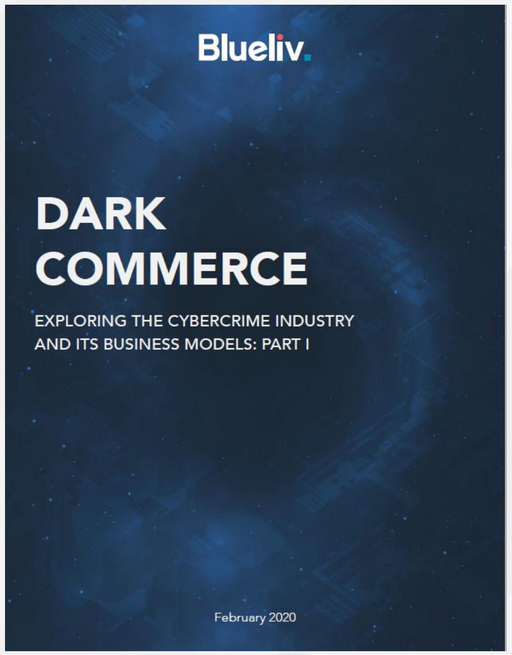
Herramientas
de comunicación
segura

Concientización
de los
teletrabajadores

THALES

Lecturas recomendadas





THALES

Preguntas & Respuestas

THALES

GRACIAS

Quédate @127.0.0.1
No seas 255.255.255.255

THALES