RESPUESTA DEL GOBIERNO

(184) PREGUNTA ESCRITA CONGRESO

184/9592 **16/04/2020** **21975**

AUTOR/A: UTRILLA CANO, Julio (GVOX); FERNÁNDEZ-ROCA SUÁREZ, Carlos Hugo (GVOX)

RESPUESTA:

El Centro Criptológico Nacional Computer Emergency Response Team (CCN-CERT) es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia (CNI). Este servicio se creó en el año 2006 como Equipos de Respuesta ante Emergencias Informáticas (CERT) Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002, de 6 de mayo, reguladora del CNI, el Real Decreto 421/2004, de 12 de marzo, de regulación del CCN y en el Real Decreto 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el Real Decreto 951/2015, de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional, que coopere y ayude a responder de forma rápida y eficiente a los ciberataques, y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4.f) de la Ley 11/2002 y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticasy procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de

operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el Centro Nacional de Protección de las Infraestructuras Críticas (CNPIC).

El Centro Criptológico Nacional realiza un seguimiento, con visión global, sobre los elemento s*hacktivistas* más significativos. Dicho seguimiento tiene por objeto evitar posibles ciberataques a organismos públicos.

En caso necesario, el CCN emite las alertas correspondientes a los organismos públicos.

En el informe de Amenazas CCN-CERT IA-04/20 "Hacktivismo y Ciberyihadismo" se identifica como ciberincidente el compromiso de las cuentas de correo del Poder Judicial. Por este motivo, el CCN proporcionó el soporte necesario a los usuarios afectados para solucionar dicho compromiso.

Con el fin de evitar este tipo de incidentes y la suplantación de identidades de los usuarios, así como para reducir la superficie de exposición ante posibles ciberataques, el Centro Criptológico Nacional ha puesto a disposición de todos los organismos públicos, y en especial de aquellos del sector salud, una serie de servicios que permiten conocer si una organización ha sufrido una brecha de seguridad y si sus contraseñas han sido comprometidas.

Durante el mes de marzo, el Centro Criptológico Nacional detectó un incremento del 70% en el número de campañas de phishing en organismos públicos. Este tipo de campañas usa la ingeniería social para adquirir fraudulentamente información personal de los usuarios. Mediante correos electrónicos que aparentan ser fiables, y que suelen derivar en páginas web falsas, intentan engañar a los usuarios u organismos para infectar sus sistemas a través de un archivo adjunto o un enlace dañino. No obstante, el CCN-CERT detectó este incremento únicamente en el mes de marzo; pues en abril, el volumen de este tipo de campañas ha disminuido hasta alcanzar un nivel similar al del año anterior.

El CCN-CERT solo detecta los ciberataques dirigidos a organismos públicos. El Centro Criptológico Nacional no dispone de la cifra relativa al aumento de delitos cibernéticos.

Durante el estado de alarma, el Centro Criptológico Nacional ha reforzado todas sus capacidades para la defensa del ciberespacio español y, en especial, del sector público y de los sectores estratégicos, con prioridad absoluta en el de la salud. El Equipo de Respuesta a Incidentes está brindando apoyo y colaboración a todas las organizaciones ante cualquier emergencia que puedan sufrir. Todo ello, con el firme

propósito de mantener su papel como centro de alerta y respuesta nacional, que coopera y ayuda a responder de forma rápida y eficiente a los ciberataques.

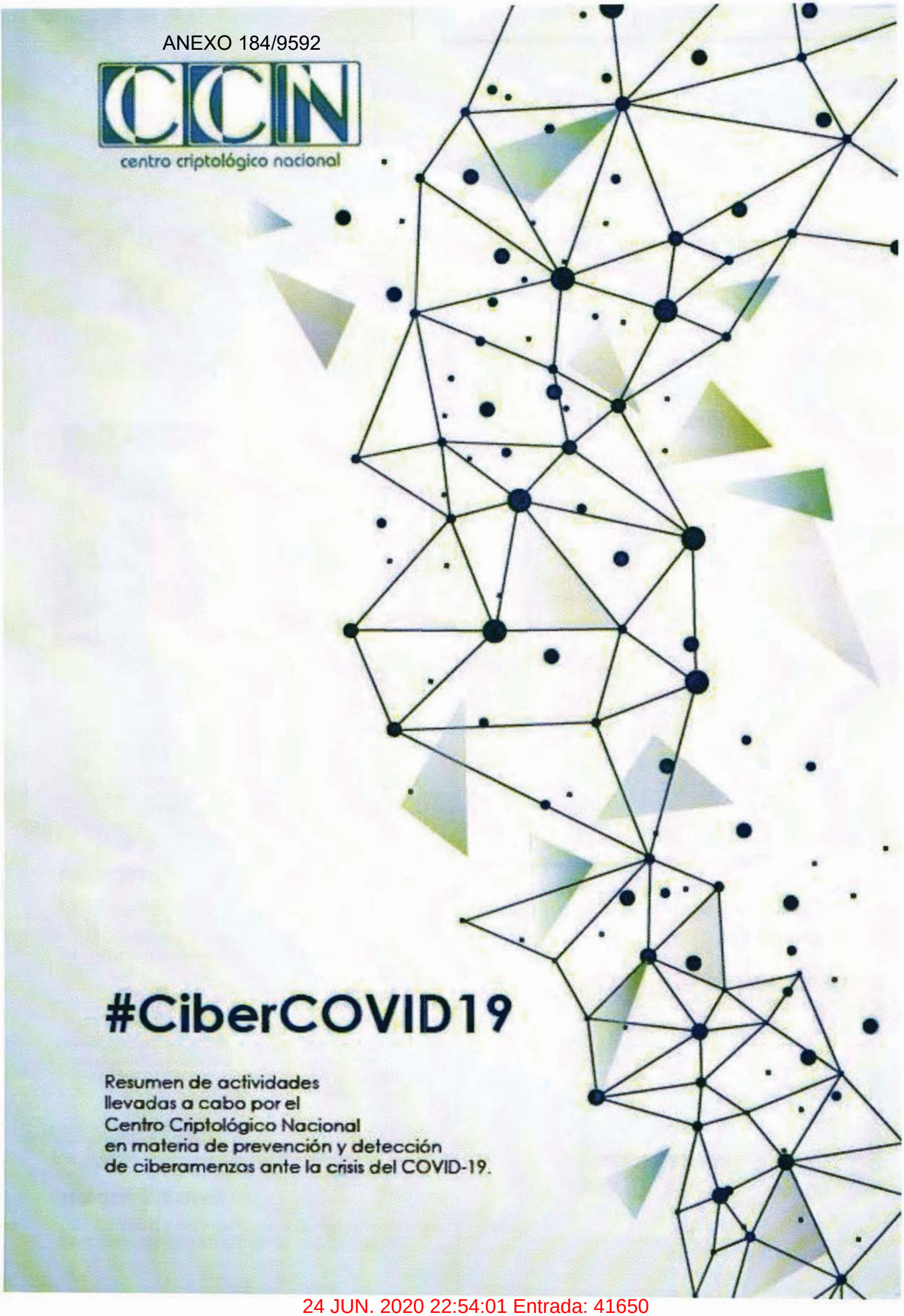
Para conocer las acciones llevadas a cabo por este organismo durante el Estado de Alarma, se ajunta en **anexo** el resumen de actividades del Centro Criptológico Nacional en materia de prevención, detección y respuesta de ciberamenazas ante la crisis del COVID-19.

La pandemia del COVID-19 ha generado una mayor concienciación de la importancia que tiene la ciberseguridad en un escenario como el actual, en el que numerosas organizaciones, institucionesy profesionales desarrollan el grueso de su actividad profesional de forma remota. La generalización del teletrabajo ha supuesto un aumento de la superficie de exposición. Ello ha conllevado, de un lado, a impulsar la coordinación con los distintos responsables de seguridad de organismos públicos, en especial de los del sector salud, y, de otro, a incrementar los recursos dirigidos a mejorar las capacidades de defensa de los organismos públicos.

Madrid, 24 de junio de 2020

ANEXO 184/9592

CCN
centro criptológico nacional



#CiberCOVID19

Resumen de actividades
llevadas a cabo por el
Centro Criptológico Nacional
en materia de prevención y detección
de ciberamenzas ante la crisis del COVID-19.

Prevención

Actividades para fomentar el uso seguro de la tecnología ante la pandemia del COVID-19.

Aspectos clave impulsados por el CCN

Iniciativa

#CiberCOVID19

Creación del hashtag para informar de campañas de ransomware.

Concienciación

35

infografías elaboradas con recomendaciones de seguridad.

Formación

13

actividades de formación a distancia impulsadas por el CCN.

Colaboración

34

empresas ofrecen sus servicios a la Administración.

Campaña de concienciación

Recomendaciones de seguridad ante las campañas de malware, phishing y desinformación bajo el hashtag #CiberCOVID19 y #NoTeInfectesConElMail.

6

infografías con buenas prácticas para prevenir posibles ataques.

29

consejos para concienciar en el buen uso de la tecnología.

Informes de seguridad. Cooperación público-privada.

Ante la generalización del teletrabajo, el CCN elabora documentación con pautas de seguridad para garantizar la seguridad de las organizaciones.

4

Informes elaborados con pautas de seguridad para situaciones de teletrabajo.

34

empresas, coordinadas por el CCN, ofrecen sus servicios a la Administración.

Coordinadas por el CCN-CERT, diferentes empresas que operan en nuestro país en el sector de la ciberseguridad, deciden ofrecer de manera altruista algunos servicios y soluciones para diferentes organizaciones, principalmente del sector público. Los informes del CCN recogen el alcance y el público objetivo al que estas empresas brindan sus productos y servicios.

"El CCN-CERT fortalece la ciberseguridad nacional ante la crisis del COVID-19"

Formación

Ante la crisis generada por el COVID-19 y la importancia que tiene la ciberseguridad en estos momentos, el Centro Criptológico Nacional ha desarrollado nuevas actividades formativas disponibles para todos los usuarios en la página web del CCN-CERT.

1

nuevo curso online sobre principios y recomendaciones básicas de ciberseguridad.

12

sesiones de formación en directo y a distancia para impulsar el teletrabajo seguro

Las sesiones de formación a distancia se realizan a través de VANESA, solución desarrollada por el CCN-CERT para facilitar la tarea de formación y sensibilización con toda su comunidad de referencia.

Sensibilización

El CCN ha recopilado toda su actividad relacionada con el #CiberCOVID19 en www.ccn-cert.cni.es/cibercovid19

Detección

Actividades de detección de las compañas de malware que emplean temáticas relacionadas con lo pandemia del COVID-19.

Actividades destacadas

Dominios

80k

nombres de sitios web detectados que hacen referencia al COVID-19.

Informes

10

Informes de análisis de código dañino con temática COVID-19-

Recopilación

3

listas negras publicados con indicadores de compromiso.

Vulnerabilidades

11

alertas publicadas sobre riesgos y vulnerabilidades en servicios externos.

Sistema de Alerta Temprana

El CCN-CERT está trabajando a través del Sistema de Alerta Temprana, que permite la actuación antes de que se produzca un incidente o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance.

Este sistema de vigilancia facilita la detección rápida de incidentes y anomalías en la Administración y en las empresas de interés estratégico que dispongan de este servicio.

En la tercera semana de marzo, el número de incidentes de phishing en organismos públicos aumentá un 75% con respecto a semanas anteriores. No obstante, esta situación solo se dio a finales del mes indicado.

Dominios

El CCN-CERT está brindando apoyo y colaboración a todas las organizaciones ante cualquier emergencia que puedan sufrir. Todo ello, con el firme propósito de mantener su papel como centro de alerta y respuesta nacional ante posibles incidentes.

80k

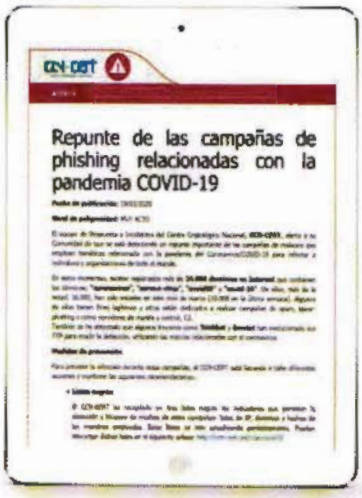
nombres de sitios web detectados que hacen referencia al COVID-19

57k

dominios, de los 80.000 detectados, se crearon en el mes de marzo.

También se ha detectado que algunos troyanos como **Trickbot** y **Emotet** -programas que aparentemente realizan una función útil para quien lo ejecuta, pero que en realidad realiza una acción que el usuario desconoce, generalmente dañina - han evolucionado sus tácticas, técnicas y procedimientos para evadir la detección, utilizando las noticias relacionadas con el coronavirus.

"Repunte de campañas de phishing relacionadas con la pandemia del COVID-19"



Listas negras, informes y vulnerabilidades

De todos los dominios detectadas, algunos de ellos tienen fines legítimos y otros están dedicados a realizar campañas de spam o phishing, entre otros acciones. Para frenar estas campañas y reducir el impacto en organizaciones e instituciones, el CCN-CERT ha recopilado en tres listas los indicadores de compromiso que permiten la detección y bloqueo de estas campañas.

10

informes de análisis de código dañino que hacen uso de la temática del COVID-19

11

alertas y avisos publicodas sobre riesgos y vulnerabilidades en servicias externos.

3

listas negras publicadas con indicadores de compromiso.

Asimismo, el Centro Criptológico Nacional está alertanda de vulnerabilidades en sistemas aperativos, navegadores y servicios de ciberseguridad, para urgir a usuarios y administradores la implementación de parches de seguridad con el fin de evitar la exposición a ataques externos.

Respuesta

Actividades de respuesta e intercambio de información sobre las campañas de malware relacionadas el COVID-19.

Actividades destacadas

Análisis

264

investigacianes sobre amenazas que utilizan la narrativa del COVID-19.

Soluciones

2

soluciones del CCN para responder a ciberataques desplegados en la red.

Coordinación nacional

44

CERTS nacionales, en contacto para fomentar el intercambio.

Seguridad ampliada

125

representantes de CC.AA. y servicios de salud, en un mismo grupo de trabajo.

Análisis e investigación de campañas

A través de REYES, herramienta desarrollada por el CCN-CERT para el intercambio y análisis de información sobre ciberamenazas, se han realizado 264 investigaciones sobre amenazas que utilizan la narrativa del COVID-19. De manera extraordinaria, se está facilitando el acceso a esta solución a los organismos pertenecientes a la comunidad de referencia del CCN para que dispongan de información actualizada sobre indicadores de compromiso y brechas de seguridad.

Asimismo, con el objetivo de reducir la superficie de exposición, se han activado, para Comunidades Autónomas y para el sector salud, dos plataformas (Trillion y HIBP) que permiten conocer si una organización ha sufrido una brecha de seguridad, así como la posible exposición de credenciales robadas.

264

investigaciones sobre amenazas que utilizan la narrativa del COVID-19.

+23k

elementos de información recopiladas sobre campañas motivadas COVID-19.

Impulso al despliegue de soluciones para responder a ciberataques

MicroCLAUDIA: centro de vocunación que, mediante el despliegue de "vacunas" permite prevenir la infección de equipos informáticos. Esta solución está orientada a complementar y ampliar las funcionalidades de los antivirus para evitar que el código dañino más, como el ransomware, se ejecute en sus entornos.

CLAUDIA: solución del CCN-CERT que permite tener una visión más completa de lo que ocurre en los ordenadores de una organización. Su objetivo principal es la detección de código dañino completo y de Amenazas Persistentes Amenazas (APT).

2

soluciones del CCN para mejorar la seguridad del trabajo en remoto.

"Comunidad y confianza, bases de nuestra ciberseguridad"

Coordinación nacional y grupos de intercambio

El CCN y la Secretaría General de Administración Digital han activado el Grupo de trabajo de Seguridad Ampliado, compuesto por 125 representantes de departamentos de seguridad de Comunidades y Ciudades Autónomas, servicios de salud de CC.AA. y el Ministerio de Sanidad, con el objetivo de refarzar la seguridad del sector sanitario. Este grupo constituye el principal instrumento de coordinación.

125

representantes de CC.AA. y servicios de salud, en un misma grupo de trabajo

6

grupos de intercambio de información en los que participa el CCN.

44

CERTS nacionales, en contacto para fomentar el intercambio.

Asimismo, el CCN está participando de forma activa en seis grupos de intercambio de información, nacionales e internacianales, para optimizar la cooperación frente a posibles problemas de seguridad informática.

El foro CSRIT.ES compuesto por 44 equipos de respuesta a incidentes de seguridad (CERT) públicos y privados que actúan en el territorio español, dispone de un canal de comunicación en el que se está promoviendo el intercambio de información sobre amenazas relacionadas con el COVID-19.