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.

Prevention

Activities to promote the secure use of technology in response to the COVID-19 pandemic.

Key aspects promoted by the CCN

Initiative	Awareness-raising	Training	Collaboration
#CiberCOVID19	31	13	32
Creation of the hashtag to inform about ransomware campaigns.	infographics prepared with security recommendations.	distance training activities promoted by the CCN.	companies offer their services to the Administration.

Awareness-raising campaign

Security recommendations against malware, phishing and disinformation campaigns under the hashtag #CiberCOVID19 and #NoTeInfectesConElMail.

6
infographics with best practices to prevent possible attacks.

25
tips to raise awareness on the proper use of technology.

Security reports. Public-private cooperation.

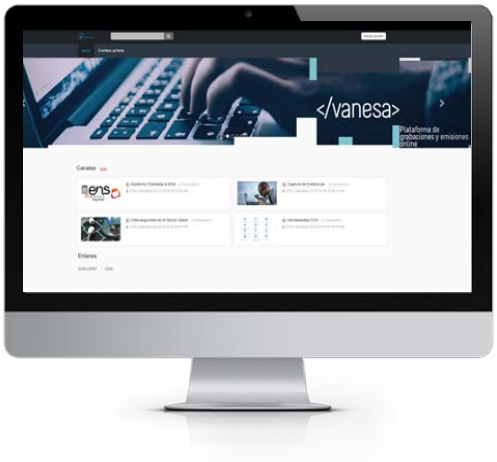
Given the generalisation of teleworking, the CCN prepares documentation with security guidelines to ensure the security of organizsations.

4
Reports elabored with security guidelines for teleworking situations.

32
companies, coordinated by the CCN, offer their services to the Administration.

Coordinated by the CCN-CERT, different companies that operate in our country in the cybersecurity sector, decided to altruistically offer some services and solutions to different organisations, mainly public entities. The CCN reports include the scope and target audience to which these companies offer their products and services.

"CCN-CERT strengthens national cybersecurity in response to the COVID-19 crisis"



Training

In view of the crisis generated by the COVID-19 and the importance of cybersecurity at this time, the National Cryptologic Centre has developed new training activities available to all the users on the CCN-CERT website.

1
new online course on basic cybersecurity principles and recommendations

12
live and distance training sessions to promote secure teleworking

The distance training sessions are carried out through VANESA, a solution developed by the CCN-CERT to facilitate the task of training and awareness-raising with all its community of reference.

Awareness-raising

The CCN has collected all its activity related to #CiberCOVID19 at www.ccn-cert.cni.es/cibercovid19

Detection

Detection activities of malware campaigns that use thematics related to the COVID-19 pandemic.

Highlighted activities

Early Warning

75%

increase of phishing incidents in public bodies.

Domains

80k

names of detected websites that refer to COVID-19.

Compilation

3

published blacklists with indicators of commitment.

Vulnerabilities

10

alerts published on risks and vulnerabilities in external services.

Early Warning System

The CCN-CERT is operating through the Early Warning System, which allows to take action before an incident occurs or, at least, to detect it at an early stage in order to reduce its impact and scope. This surveillance system facilitates the swift detection of incidents and anomalies in the Administration and in companies of strategic interest that have this service.

Through this system, a surge of phishing campaigns related to the COVID-19 pandemic has been detected. Infected files or links to harmful websites are attached to e-mails. Identities of government agencies, financial institutions, service providers and health institutions are being supplanted.

75%

increase of phishing incidents in public bodies

Domains

The CCN-CERT is providing support and collaboration to all organizations in any emergency they may suffer. All this, with the firm purpose of maintaining its role as a national alert and response centre for possible incidents.

80k

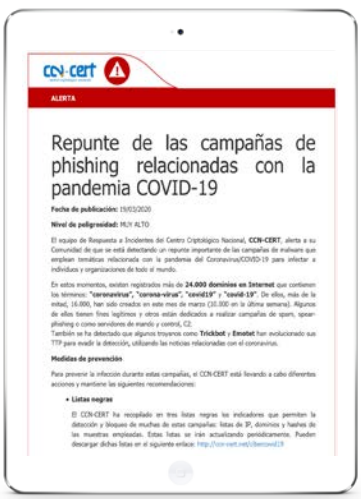
names of detected websites referring to COVID-19

57k

domains, of the 80,000 detected, were created in March.

It has also been detected that some Trojans such as **Trickbot and Emotet -** programs that apparently perform a useful function for the user, but in reality carry out an action that the user is unaware of, generally harmful - have evolved their tactics, techniques and procedures to evade detection, using the news related to the coronavirus.

"Surge in phishing campaigns related to the COVID-19 pandemic"


ccn-cert

ALERTA

Repunte de las campañas de phishing relacionadas con la pandemia COVID-19

Blacklists, reports and vulnerabilities

Of all the domains detected, some of them have legitimate purposes and others are dedicated to spam or phishing campaigns, among other actions. In order to stop these campaigns and reduce the impact on organizations and institutions, the CCN-CERT has compiled in three lists the indicators of commitment that allow the detection and blocking of these campaigns.

10

Malware analysis reports that make use of the COVID-19 theme

10

alerts and notices published on risks and vulnerabilities in external services.

3

published blacklists with indicators of commitment.

http://ccn-cert.net/cibercovid19

The National Cryptologic Centre is also warning of vulnerabilities in operating systems, browsers and cybersecurity services, in order to urge users and administrators to implement security patches to avoid exposure to external attacks.

Answer

Activities of response and exchange of information on malware campaigns related to COVID-19.

Highlighted activities

Analysis

264

investigations on threats that use and take advantage of COVID-19

Solutions

2

CCN solutions to improve the security of remote work.

National coordination

44

national CERTS, in contact to promote the exchange.

Exchange groups

6

information exchange groups in which the CCN participates.

Campaign analysis and research

Through REYES, a tool developed by the CCN-CERT for the exchange and analysis of information on cyberthreats, 264 investigations have been carried out on threats using the COVID-19 narrative. In an extraordinary way, access to this solution is being facilitated to the agencies that belong to the CCN reference community so that they have updated information on commitment indicators and security breaches.

In addition, with the aim of reducing the exposure area, two platforms (Trillion and HIBP) have been activated for Autonomous Communities and the health sector, which make it possible to find out if an organisation has suffered a security breach, as well as the possible exposure of stolen credentials.

264

investigations on threats that use and take advantage of COVID-19

+23k

information elements collected on COVID-19 motivated campaigns.

Solutions to improve security

EMMA: CCN solution that allows surveillance beyond remote access, by establishing a secure and verified connection in a robust way (with two-factor authentication) between the user and the systems.

MicroCLAUDIA: a tool that, by deploying "vaccines" like Emotet-Stopper, allows the prevention of computer equipment infection. This solution is designed to complement and extend the functionalities of anti-viruses in organisms that do not have sufficient capacity to prevent malware, such as ransomware, from being executed in their environments.

2

CCN solutions to improve remote work security

"Community and trust, bases of our cybersecurity"

National coordination and exchange groups

The CSRIT.ES forum is an independent platform composed of those public and private security incident response teams (CERTs) whose scope of action is within the Spanish territory.
Currently, this forum is composed of 44 national CERTS.
CSIRT.ES has a communication channel that is promoting the exchange of information on threats related to COVID-19

44

national CERTS, in contact to promote the exchange.

6

information exchange groups in which the CCN participates.

The National Cryptologic Centre is also actively participating in six information exchange groups, both national and international, to optimise the cooperation in the face on potential computer security problems.