ENJOY SAFER TECHNOLOGY™

Evolución y estado actual del ransomware

Josep Albors
Responsable de investigación y concienciación
ESET España


RANSOM!
Your file have been encrypted


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
Spanish
¿Puedo recuperar mis archivos?
Por supuesto. Le garantizamos que puede recuperar todos sus archivos de forma segura y sencilla. Pero no tienes tiempo suficiente.
Puede descifrar algunos de sus archivos de forma gratuita. Pruebe ahora haciendo clic en <Decrypt>.
Pero si quieres descifrar todos tus archivos, necesitas pagar.
Sólo tiene 3 días para enviar el pago. Después de eso el precio se duplicará.
Además, si no paga en 7 días, no podrá recuperar sus archivos para siempre.
Tendremos eventos gratuitos para los usuarios que son tan pobres que no podían pagar en 6 meses.
¿Cómo pago?
El pago se acepta en Bitcoin solamente. Para obtener más información, haga clic en <About bitcoin>.
Por favor, compruebe el precio actual de Bitcoin y compre algunos bitcoins. Para obtener más información, haga clic en <How to buy bitcoins>.
Y envíe la cantidad correcta a la dirección especificada en esta ventana.
Después de su pago, haga clic en <Check Payment>. Mejor hora para consultar: 9:00 am - 11:00 am GMT de lunes a viernes.
Una vez comprobado el pago, puede comenzar a descifrar sus archivos inmediatamente.
Contacto
Payment will be raised on
5/17/2017 20:33:49
Time Left
02:23:58:19
Your files will be lost on
5/21/2017 20:33:49
Time Left
06:23:58:19
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt
Papelera de reciclaje
s.wnry
00000000.eky
wcry
t.wnry
00000000.res
msg
taskdl
@Please_R...
b.wnry
taskse
@WanaDec...
c.wnry
u.wnry
r.wnry
00000000.pky
3221149481...
8:35 p. m.
14/5/2017

Un ataque ransomware a un hospital en Alemania pudo ser el causante de la muerte de una paciente

18 Septiembre 2020

21 Comentarios

Muere una mujer durante un ataque de 'ransomware' a un hospital de Dusseldorf (Alemania)

MADRID, 18 Sep. (Portaltic/EP) -

Un **ataque de 'ransomware' al Hospital Universitario de Dusseldorf** (Alemania) colapsó este martes el servicio de urgencias del centro, que tuvo que cerrar temporalmente la sala de urgencias y, como resultado de ello, **una paciente gravemente enferma falleció mientras era trasladada a otro hospital**.

El colapso informático del hospital tuvo lugar debido a un **ataque de 'ransomware' dirigido originalmente contra los ordenadores de la Universidad de Dusseldorf**, pero en su lugar afectó también a los equipos de la clínica, encriptando 30 de sus servidores, como ha informado el portal local RTL.

Este fallo en los equipos del hospital **redujo la cantidad de pacientes que habitualmente se atiende en el centro**, pasando de 1.000 a 550 personas, y también la de operaciones, que de entre 120 y 70 pasó a menos de 15, según aseguraron fuentes de la clínica a la agencia DPA.

Como resultado del colapso, **una paciente gravemente enferma tuvo que ser trasladada al cercano hospital de Wuppertal** en ambulancia. Aunque se trata de un trayecto de apenas 25 minutos, la mujer falleció. Se trata de la **primera muerte registrada debida a un ciberataque.**

La policía de Dusseldorf contactó con los cibercriminales a través de la nota que acompañaba al 'ransomware', informándoles de que su ataque había colapsado el hospital, y estos **retiraron la extorsión** y ofrecieron el código para desencriptar los equipos afectados.

ÚLTIMAS NOTICIAS / PORTALTIC »

Qué son y cómo se pueden evitar los ataques 'shoulder surfing'

Denuncian a Facebook por acceder sin permiso a la cámara de los usuarios de Instagram

Muere una mujer durante un ataque de 'ransomware' a un hospital de Dusseldorf (Alemania)

Más leídas ofrecido por cellnex

1 Qué son y cómo se pueden evitar los ataques 'shoulder surfing'

2 Sony lo vuelve a hacer: la mejor cancelación de ruido y diseño con sus WH-1000XM4

3 Microsoft prueba en su aplicación 'Tu Teléfono' una opción para enviar enlaces, imágenes y notas del móvil al PC


Cambio de modelo

Maze Ransomware

(Noviembre 2019)

Primera fase

Explotación / Infección

Segunda fase

Reconocimiento

Robo de información

Cifrado

Tercera fase

Filtración de datos

Emotet

Email

Emotet

Robo información

Ransomware

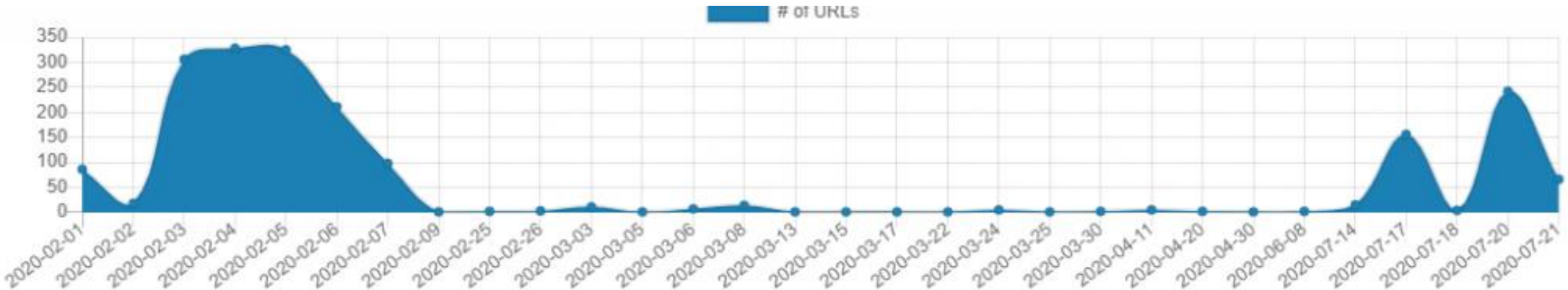
Filtración

Emotet Payload

Trickbot/Qbot

Ryuk/Conti

Conti Leak Site



MAZE Main Archive Press Release Tor Mirror

Search

New Clients

Toledo Public Schools - 2% published
Rx Technology - 2% published
Ghantoo Group - 2% published
Guillevin International Co. - 2% published
Clayton Industries - 2% published
Clark County School District - 2% published
JX Enterprises, Inc - 2% published
Groupe Interway - 2% published
Artech Information Systems LLC
BRUSCHI S.P.A. - 2% published

Represented here companies do not wish to cooperate with us, and trying to hide our successful attack on their resources. Wait for their databases and private papers here. Follow the news!
P.S. We have the second domain: newsmaze.top.

To contact us use the feedback form of our news website.

Toledo Public Schools - 2% published NEW

https://tps.org/

Article about Toledo Public Schools have been locked

Cryptoransomware

admin , 686 Read More >

Rx Technology - 2% published NEW

https://www.rx-tech.com/

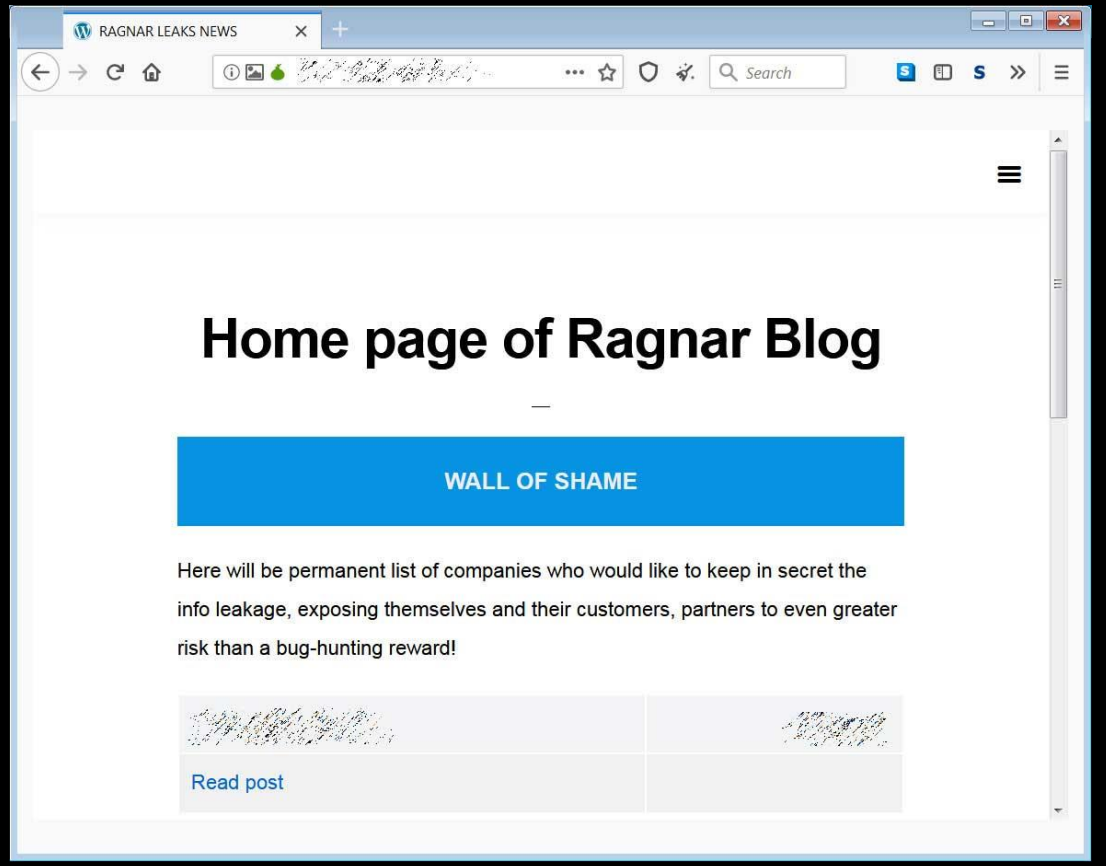
Article about Rx Technology have been locked

Cryptoransomware

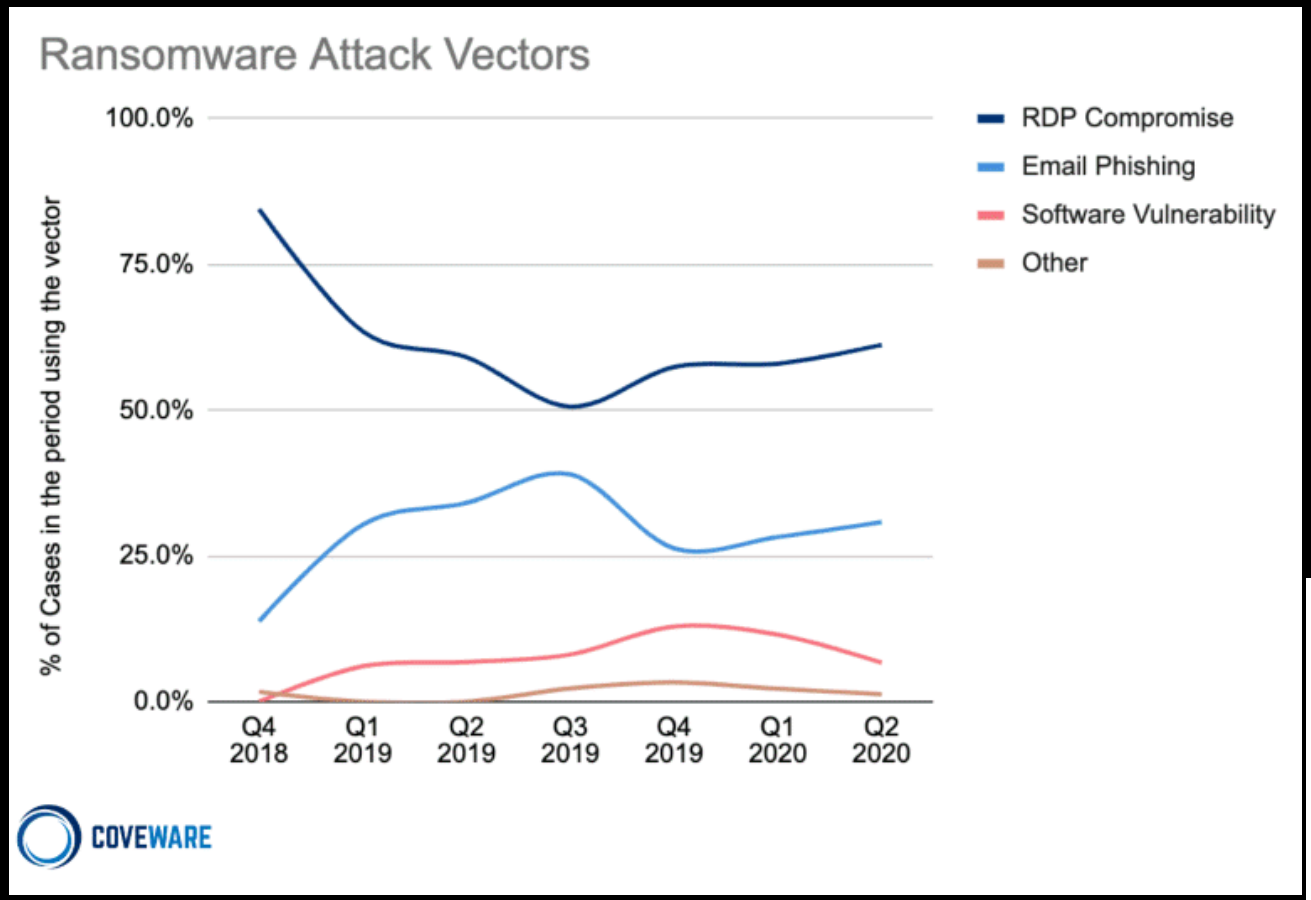
admin , 656 Read More >

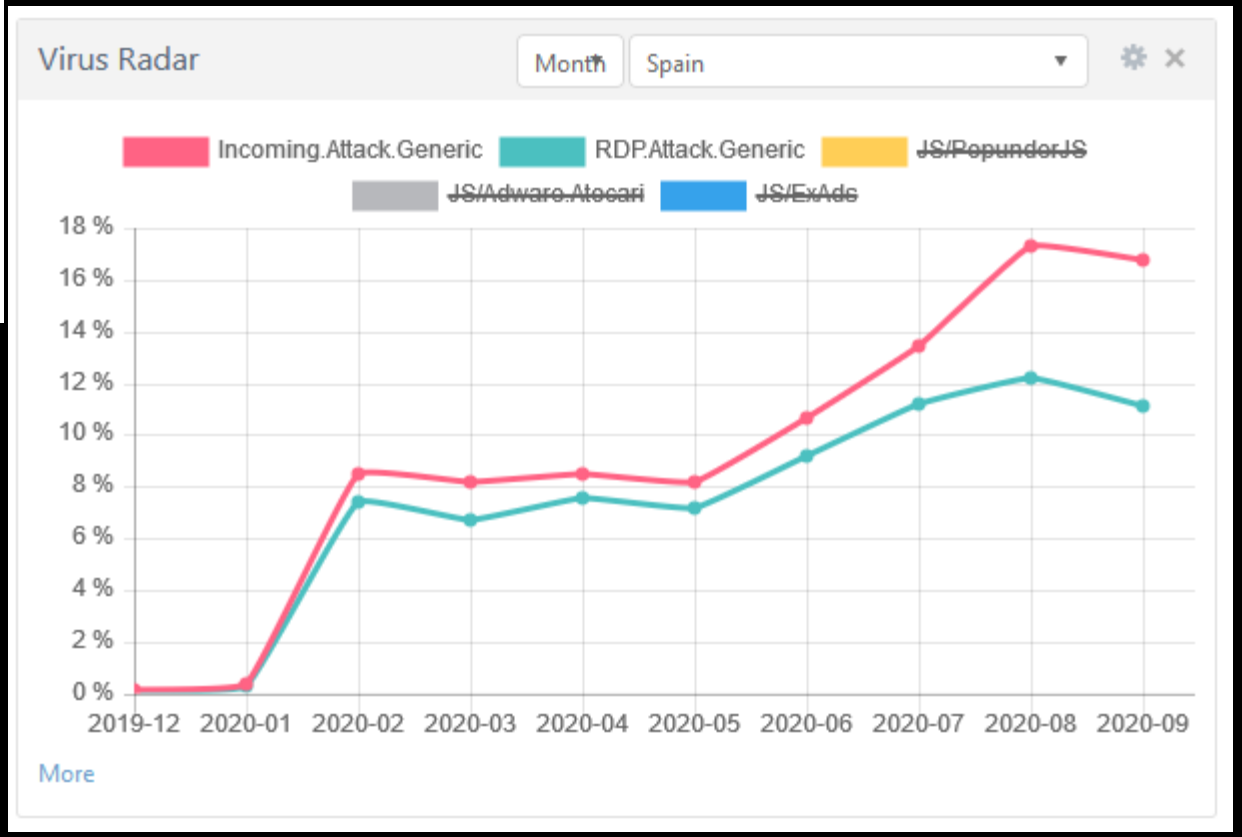
Full dump

METROPOLITAN HEALTH CORPORATE (PTY) LTD - Full dump (100%)
U.S. Auto Parts Network, Inc. - Full dump (100%)
X-FAB Silicon Foundries - Full dump (100%)
Phillips Law Firm, Inc. - Full dump (100%)
Atlanta Computer Group, Inc. - Full dump (100%)
MI Metals Inc
Tri-Boro Construction Supplies
Ptarmigan Media - Full dump (100%)
Engineering Consultants Group - Full dump (100%)
Bennett Automotive Group - Full dump (100%)



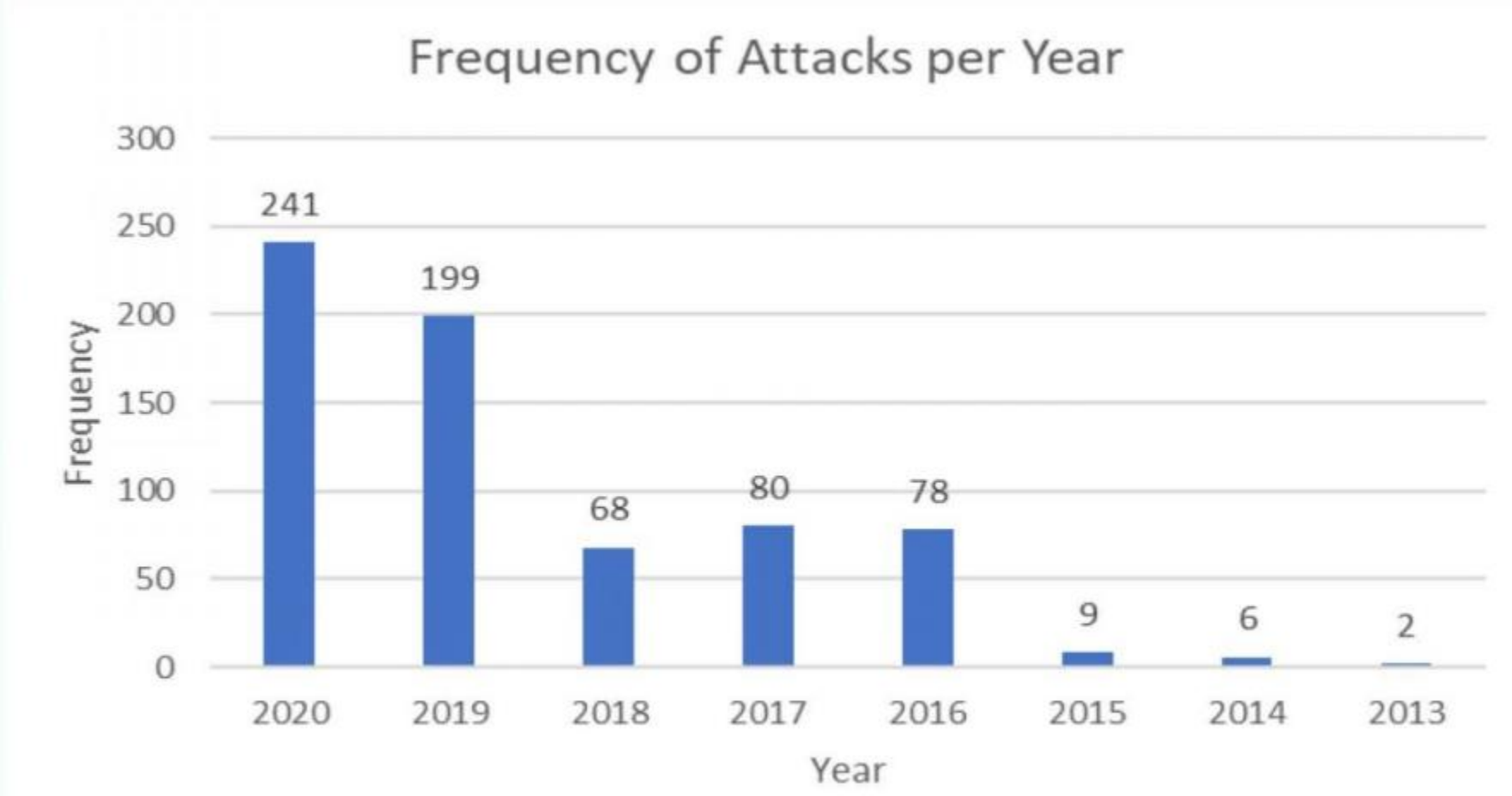

Vectores de ataque


Ransomware Attack Vectors
100.0%
75.0%
50.0%
25.0%
0.0%
% of Cases in the period using the vector
Q4 2018
Q1 2019
Q2 2019
Q3 2019
Q4 2019
Q1 2020
Q2 2020
RDP Compromise
Email Phishing
Software Vulnerability
Other
COVEWARE

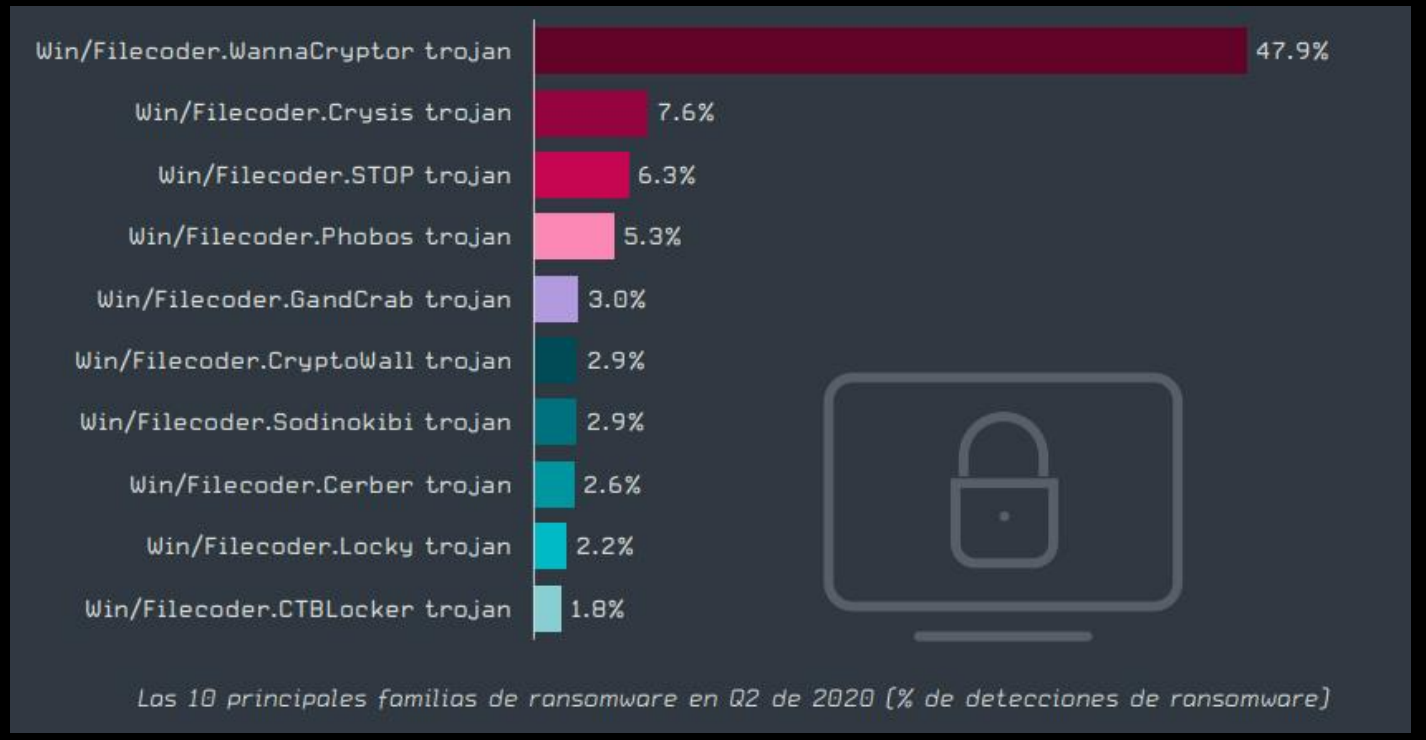

Virus Radar
Month
Spain
Incoming.Attack.Generic
RDP.Attack.Generic
JS/PopunderJS
JS/Adware.Atocari
JS/ExAds
18 %
16 %
14 %
12 %
10 %
8 %
6 %
4 %
2 %
0 %
2019-12
2020-01
2020-02
2020-03
2020-04
2020-05
2020-06
2020-07
2020-08
2020-09
More


VPN

Ataques dirigidos

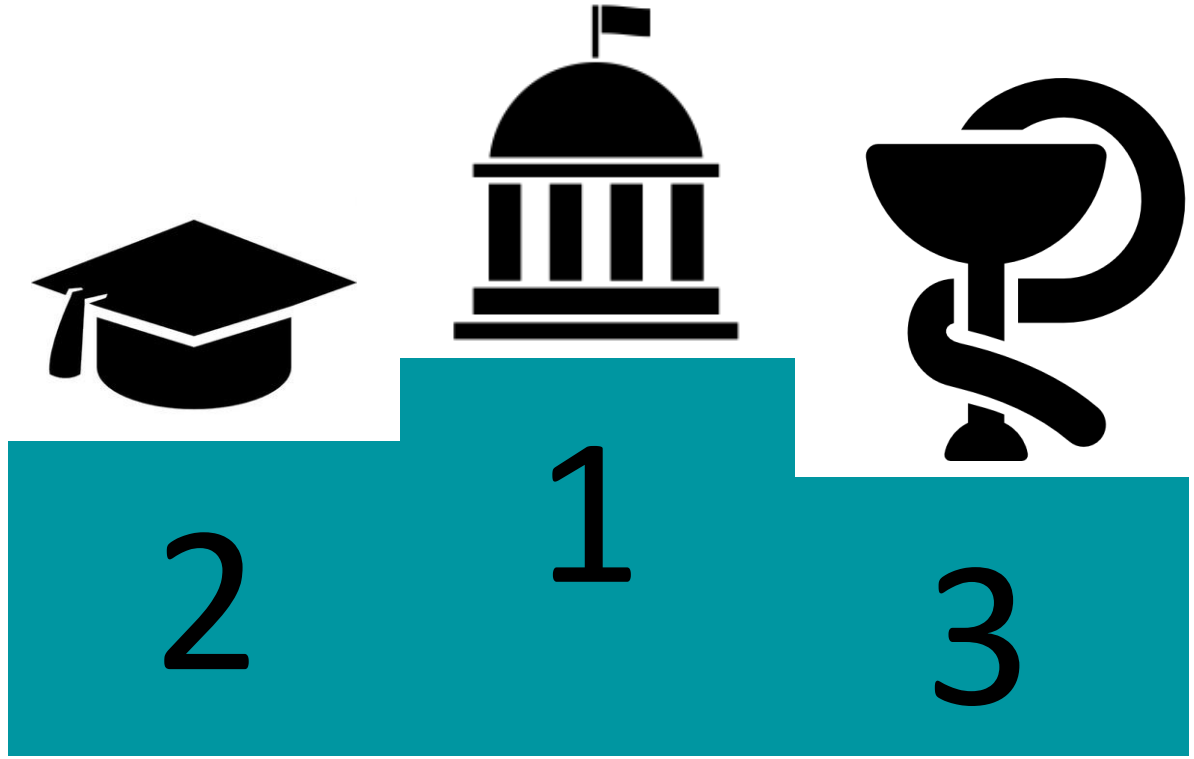

Frequency of Attacks per Year
300
250
200
150
100
50
0
Frequency
241
199
68
80
78
9
6
2
2020
2019
2018
2017
2016
2015
2014
2013
Year

Top 10 Most Commonly Used Strains	Frequency
Maze	57
WannaCry	33
Ryuk	33
Revil/sodinokibi	33
Samsam	13
DoppelPaymer	12
NetWalker	11
BitPaymer	8
CryptoLocker	7
CryptoWall	5
Grand Total	**212**



Las 10 principales familias de ransomware en Q2 de 2020 (% de detecciones de ransomware)

CI Sector	Frequency
Government Facilities	199
Education Facilities Subsector	106
Healthcare and Public Health	106
Critical Manufacturing	48
Emergency Services	61
Information Technology	42
Communications	36
Transportation Systems	35
Commercial Facilities	27
Financial Services	20
Energy	23
Food and Agriculture	15
Water and Wastewater Systems	5
Chemical	7
Defense Industrial Base	4
Nuclear Reactors, Materials, and Waste	1
Grand Total	**735**



La policía detecta un ciberataque al sistema informático de los hospitales

Los autores querían secuestrar la información colándose en correos electrónicos enviados a sanitarios y pedir un rescate para recuperarla

Un miembro de la Unidad Militar de Emergencias ante la puerta de Urgencias del hospital San Juan de Dios, en la localidad sevillana de Bormujos. En vídeo, declaraciones del director adjunto operativo de la Policía Nacional.
PACO PUENTES / VÍDEO: QUALITY

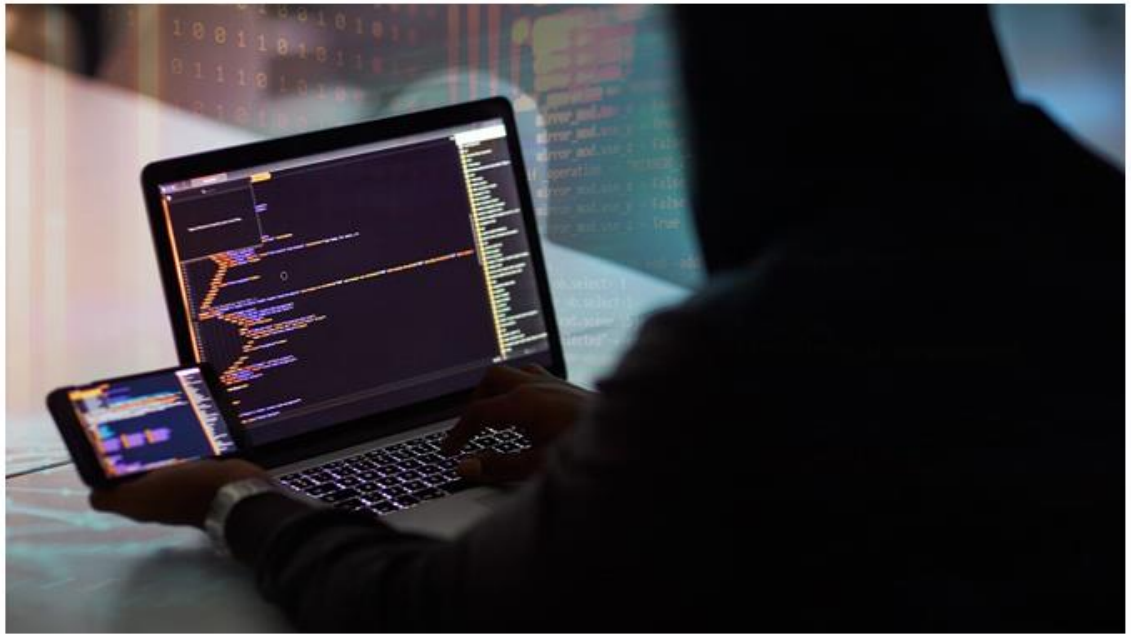
El hospital Moisès Broggi, víctima de un ataque informático en plena pandemia

Piratas informáticos rusos han pedido un rescate para liberar los servidores del hospital de Sant Joan Despí (Barcelona), que se ha negado a pagar

Exterior del hospital Moisès Broggi, situado en Sant Joan Despí (Barcelona).

Mapfre trata de frenar los efectos de un ataque de ransomware

Seguridad 18 AGO 2020



La aseguradora ha tenido que desplegar su plan de contingencia de negocio para repeler un ataque de ransomware, del que informó el pasado domingo. De momento, no ha informado del cierre de la incidencia.

SegurCaixa Adeslas activa su plan de contingencia por un ataque de ransomware

Javier Mira, presidente SegurCaixa Adeslas - SEGURCAIXA ADESLAS - Archivo

MADRID, 10 Sep. (EUROPA PRESS) -

ÚLTIMAS NOTICIAS / ECONOMÍA »

La negociación de la prórroga de los ERTE encara su semana decisiva

Planas informa al Congreso sobre las negociaciones de la futura PAC

El Gobierno prevé aprobar el martes la regulación del teletrabajo

Lo más leído

1 Emmy 2020: Lista completa de ganadores

2 El Gobierno catalán recomienda no viajar a Madrid y controlará la llegada

Garmin admite un ciberataque por «ransomware» que dejó inactivos a sus usuarios durante cinco días

- La compañía estadounidense asegura que no se han robado datos ni ha habido accesos no autorizados

AFP

LO MÁS LEÍDO EN ABC

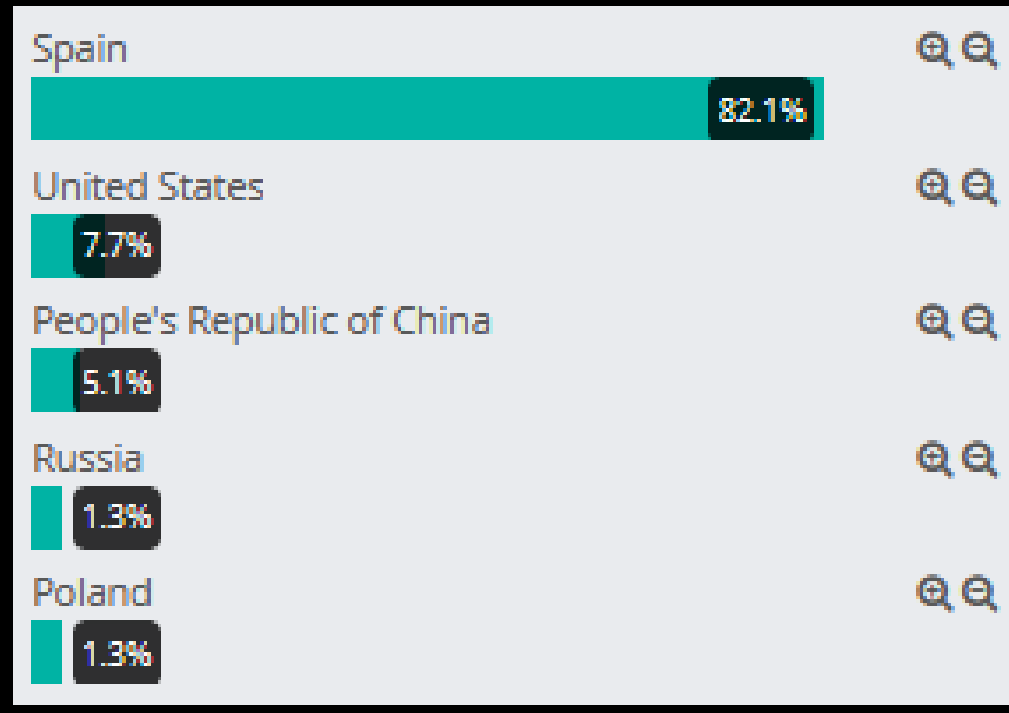
Tecnología | ABC

1 «Compañías farmacéuticas están siendo atacadas con ataques muy avanzados»

2 Trucos para mejorar la privacidad en iOS 14

3 iOS 14: todas las novedades que llegan al iPhone

4 Por qué deberías esperar antes de actualizar el iPhone a iOS 14



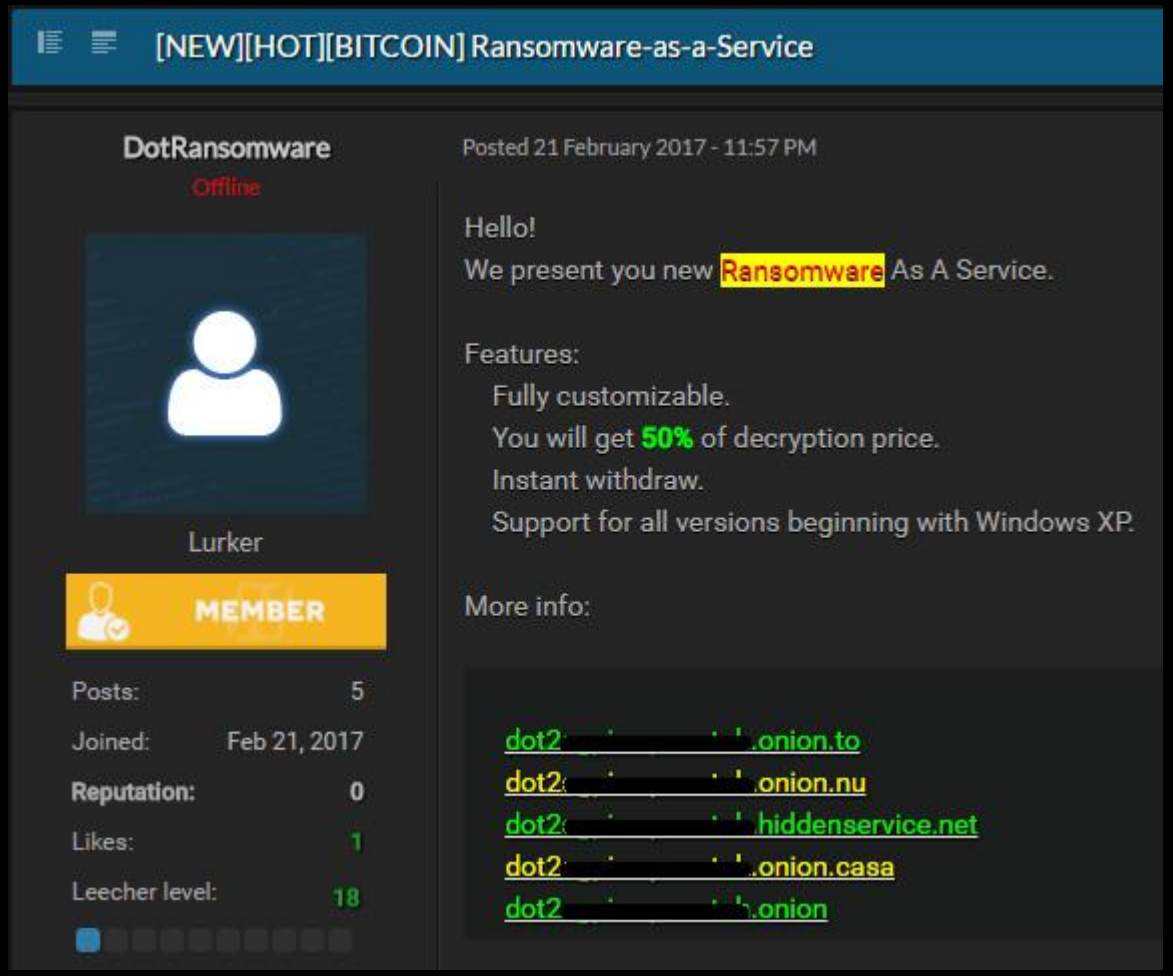
YOUR FILES ARE ENCRYPTED

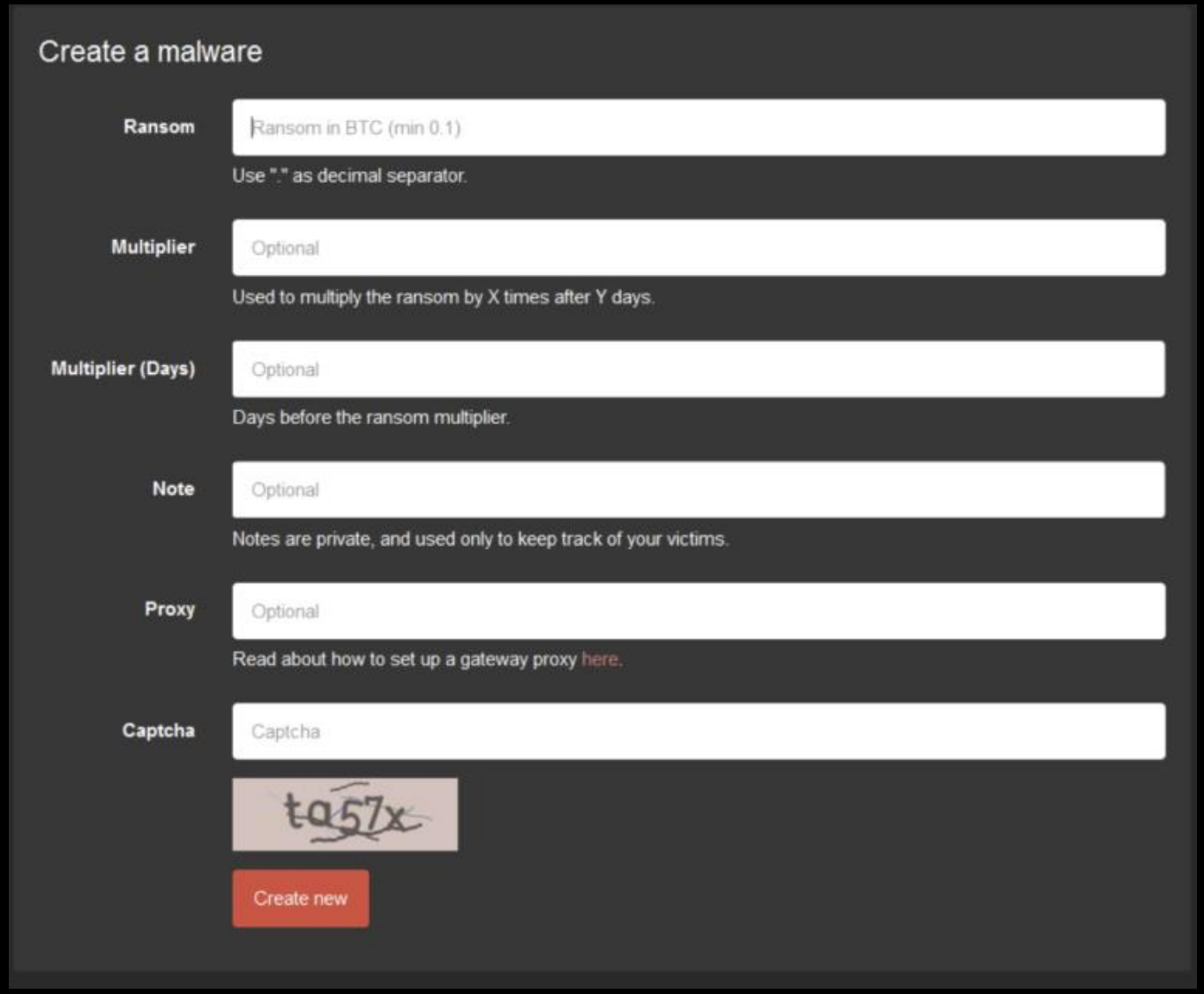
Your photos, documents and other important files have been encrypted with unique key, generated for this computer.

NEXT

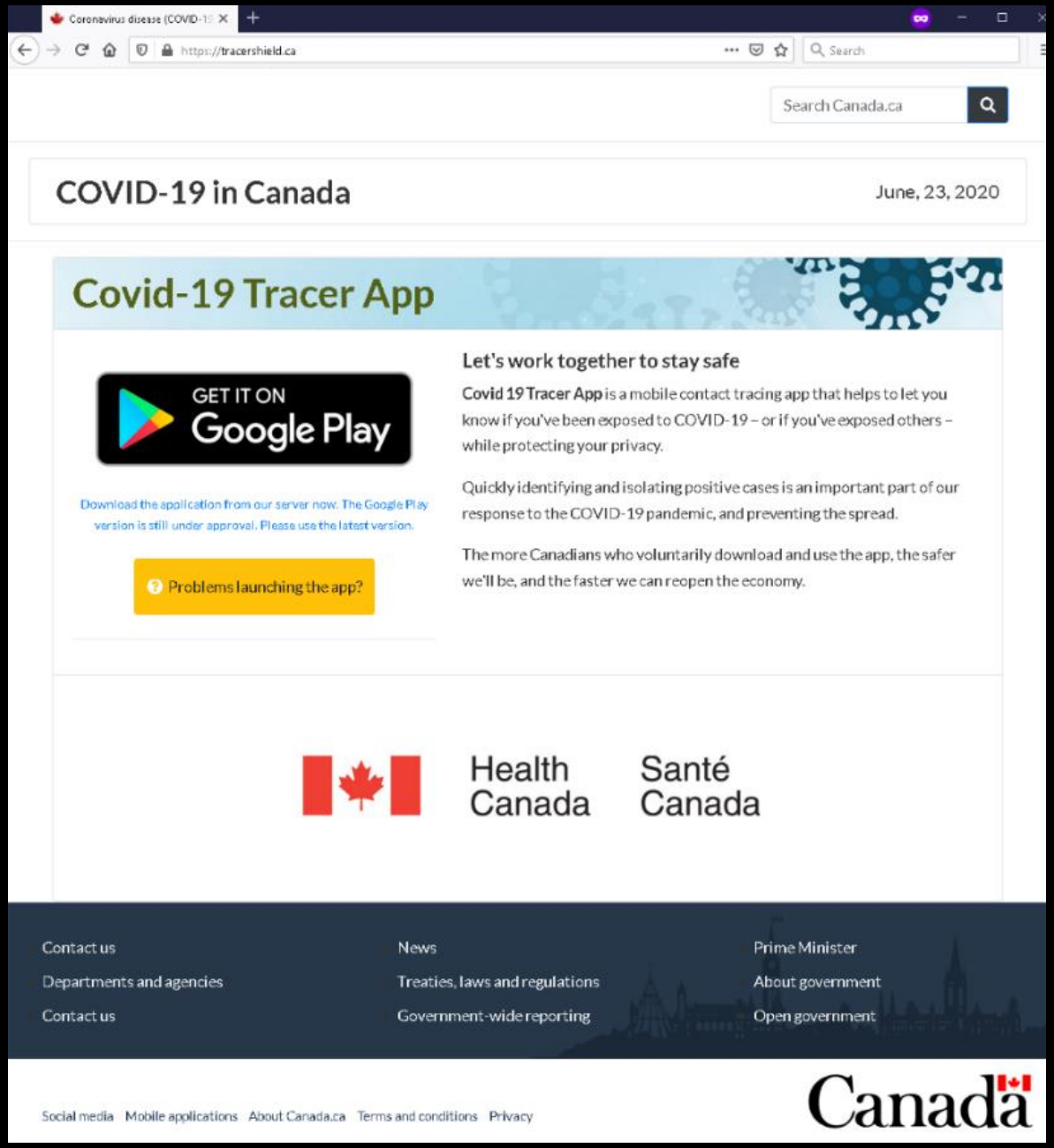

LEAK

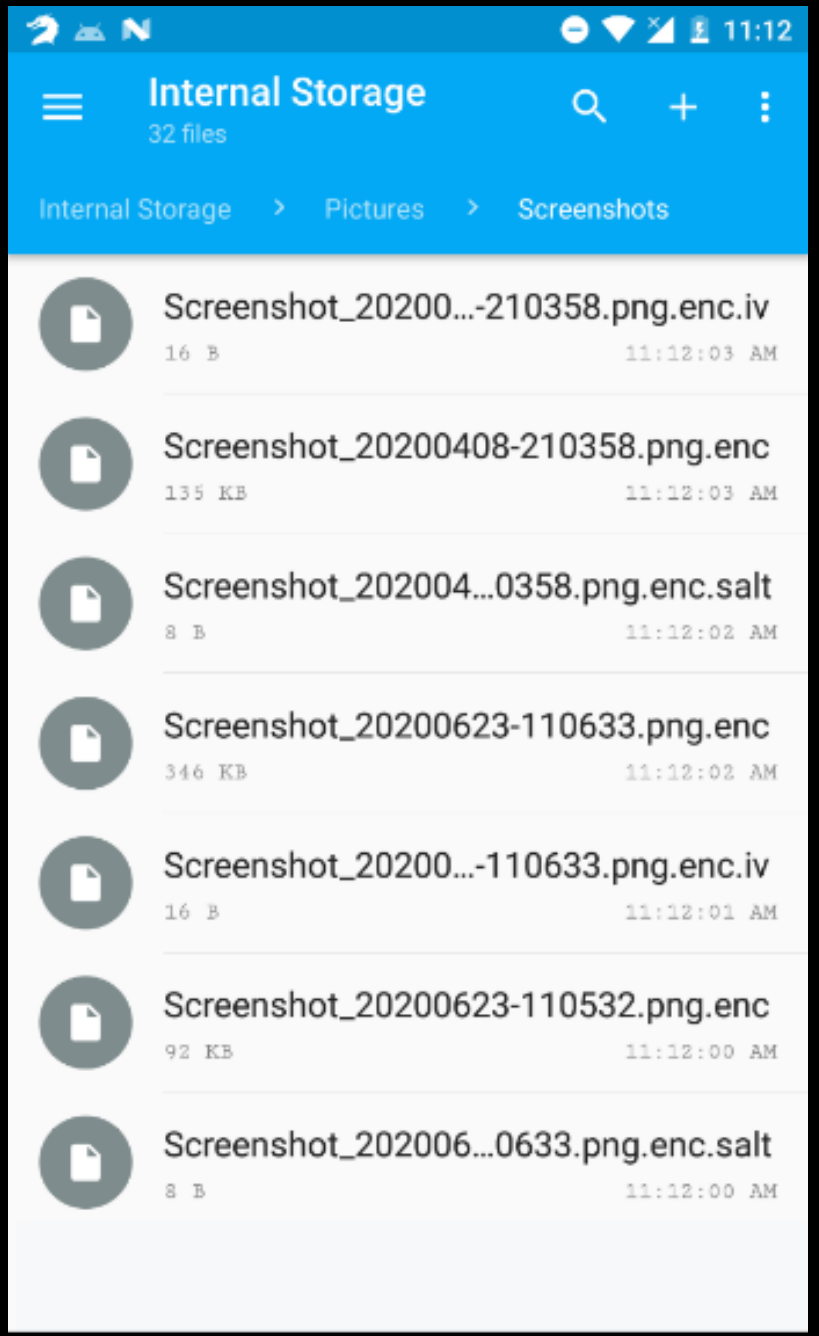

Ransomware como servicio

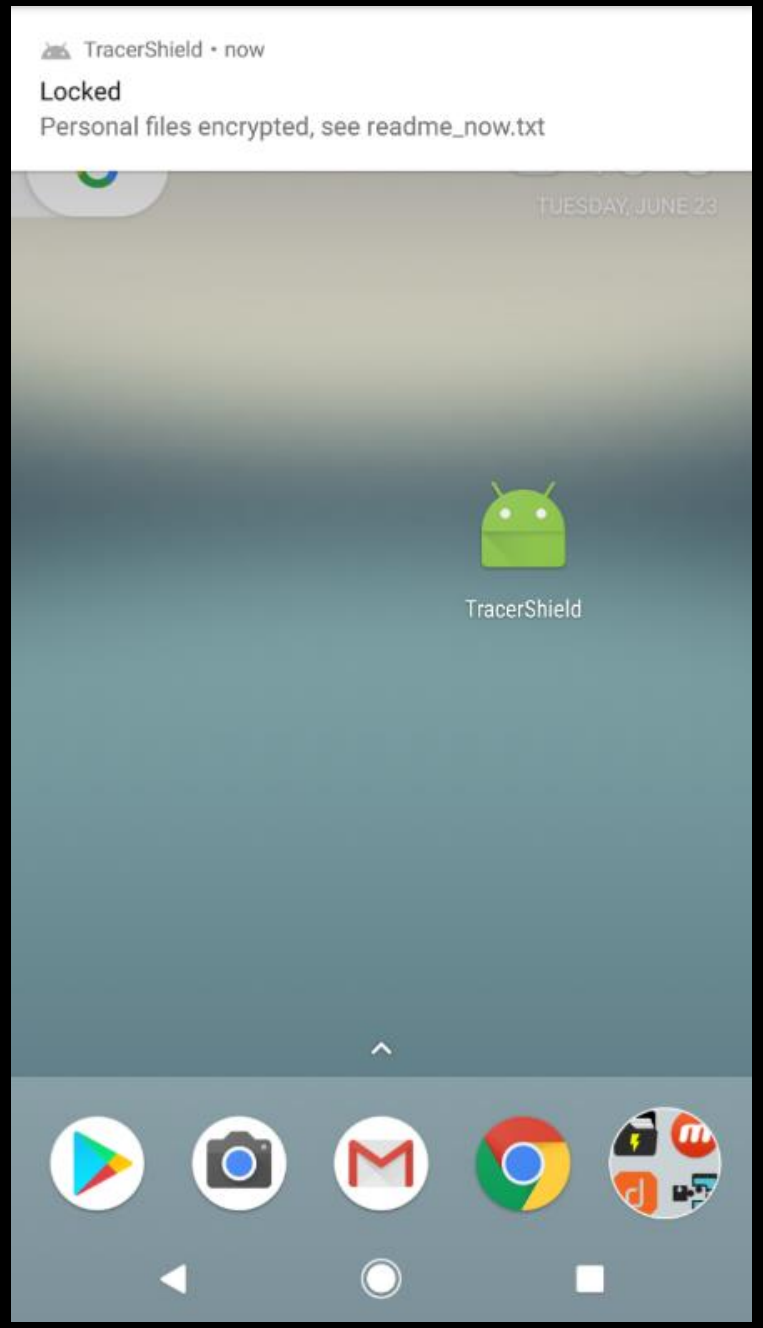

[NEW][HOT][BITCOIN] Ransomware-as-a-Service
DotRansomware
Offline
Lurker
MEMBER
Posts: 5
Joined: Feb 21, 2017
Reputation: 0
Likes: 1
Leecher level: 18
Posted 21 February 2017 - 11:57 PM
Hello!
We present you new Ransomware As A Service.
Features:
Fully customizable.
You will get 50% of decryption price.
Instant withdraw.
Support for all versions beginning with Windows XP.
More info:
dot2 .onion.to
dot2 .onion.nu
dot2 .hiddenservice.net
dot2 .onion.casa
dot2 .onion

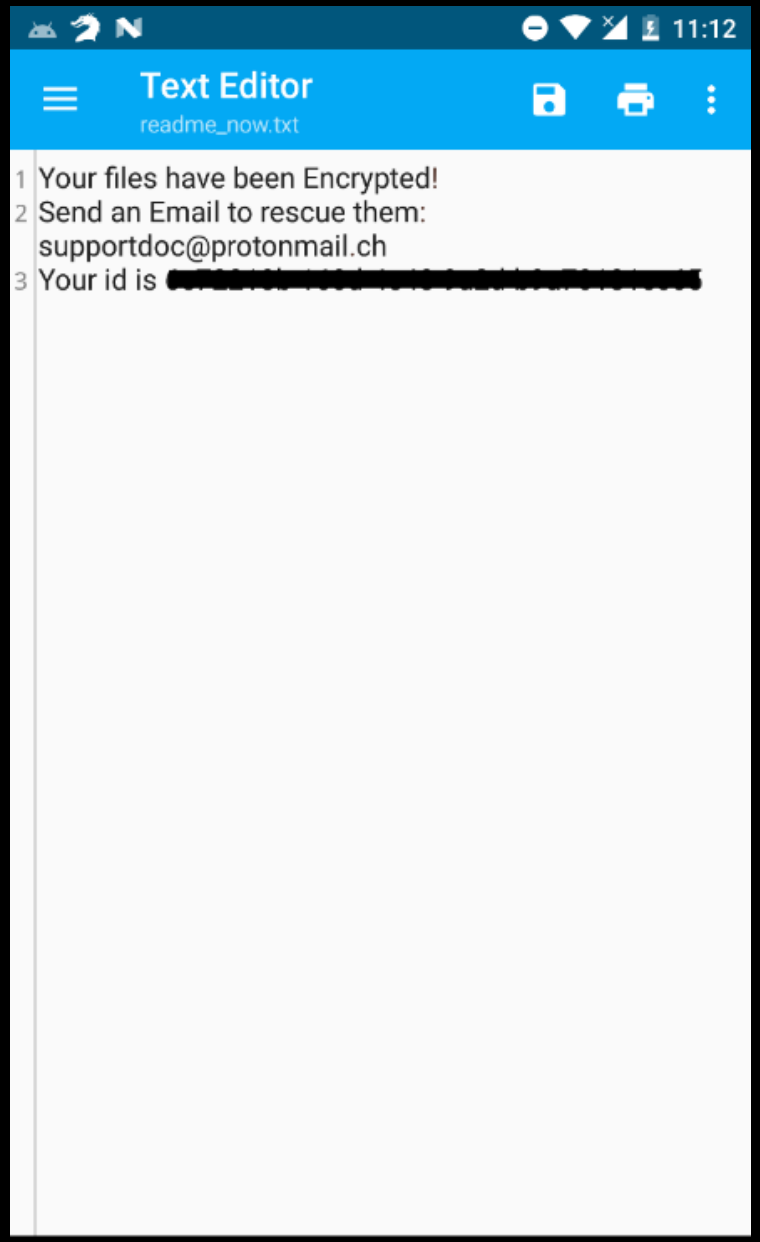

Create a malware
Ransom
Ransom in BTC (min 0.1)
Use "." as decimal separator.
Multiplier
Optional
Used to multiply the ransom by X times after Y days.
Multiplier (Days)
Optional
Days before the ransom multiplier.
Note
Optional
Notes are private, and used only to keep track of your victims.
Proxy
Optional
Read about how to set up a gateway proxy here.
Captcha
Captcha
ta57x
Create new


Ransomware en Android


Coronavirus disease (COVID-19
https://tracershield.ca
Search
Search Canada.ca
COVID-19 in Canada
June, 23, 2020
Covid-19 Tracer App
GET IT ON Google Play
Download the application from our server now. The Google Play version is still under approval. Please use the latest version.
Problems launching the app?
Let's work together to stay safe
Covid 19 Tracer App is a mobile contact tracing app that helps to let you know if you've been exposed to COVID-19 – or if you've exposed others – while protecting your privacy.
Quickly identifying and isolating positive cases is an important part of our response to the COVID-19 pandemic, and preventing the spread.
The more Canadians who voluntarily download and use the app, the safer we'll be, and the faster we can reopen the economy.
Health Canada
Santé Canada
Contact us
Departments and agencies
Contact us
News
Treaties, laws and regulations
Government-wide reporting
Prime Minister
About government
Open government
Social media
Mobile applications
About Canada.ca
Terms and conditions
Privacy
Canada


11:12
Internal Storage
32 files
Internal Storage
Pictures
Screenshots
Screenshot_20200...-210358.png.enc.iv
16 B
11:12:03 AM
Screenshot_20200408-210358.png.enc
135 KB
11:12:03 AM
Screenshot_202004...0358.png.enc.salt
8 B
11:12:02 AM
Screenshot_20200623-110633.png.enc
346 KB
11:12:02 AM
Screenshot_20200...-110633.png.enc.iv
16 B
11:12:01 AM
Screenshot_20200623-110532.png.enc
92 KB
11:12:00 AM
Screenshot_202006...0633.png.enc.salt
8 B
11:12:00 AM



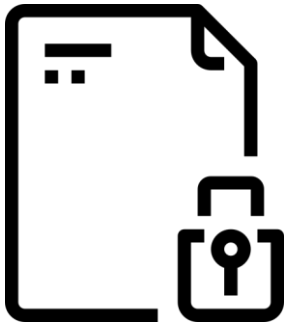


welivesecurity


Conclusion

Soluciones

Solución esencial pero parcial



Cifrado de la información

Monitorización de la red

ENJOY SAFER TECHNOLOGY™

Gracias por la atención

@JosepAlbors