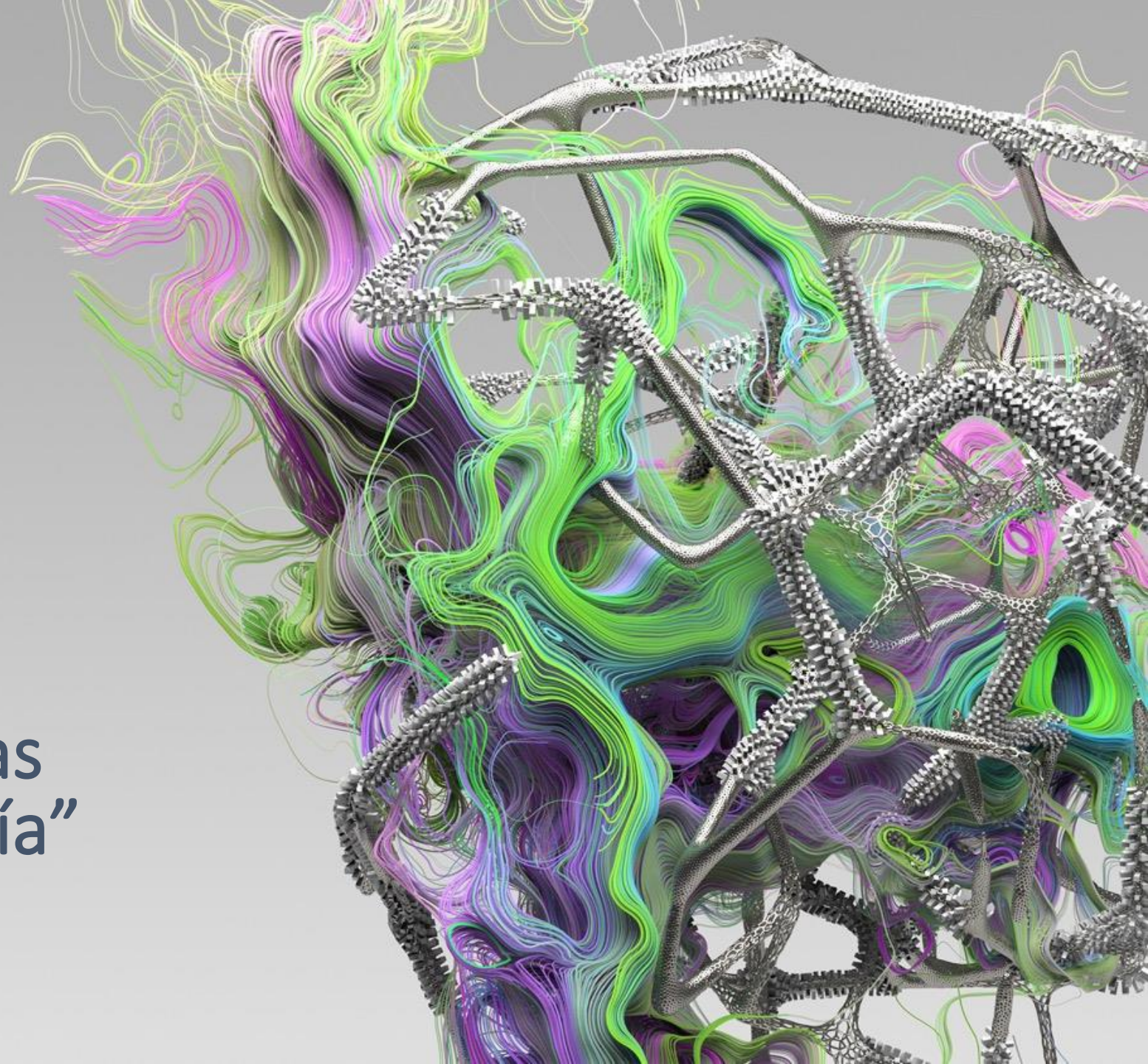


“Mis Servicios para las amenazas del día a día”

EDSI Trend Argentina – Agosto 2022

Un ejemplo práctico

Extensión de DDJJ, ganancias y bienes personales

- ¿Que sucedería si un contador es víctima de un ataque a su notebook que contiene la información de sus clientes?
- ¿Que sucedería si el contador de una empresa tuviera su dispositivo o su usuario comprometido?
- ¿Que sucedería si el CFO fuera víctima de una estafa monetaria?

B.E.C (Business Email Compromise)

- Esquema de factura falsa
- Fraude al director general
- Compromiso de cuenta
- Suplantación de abogados
- Robo de datos

Muestra de BEC

From: Wilson Ceo <wilson_ceo@company.com> Sent: 2016/7/27 (週三) 上午 04:59
To: Sandra_Finance@company.com
Cc:
Subject: URGENT

Necesito un pago de U$D22,110 durante el transcurso de la mañana, hazme saber si estas disponible ahora, así puedo enviarte los detalles. Debemos regularizar esto hoy.

Saludos
Wilson

Enviado desde mi iPhone

Encabezado

Comportamiento

Contenido

Intención

Intención del atacante

Llamado a la Acción

Implicación Financiera

Contenido del Correo

Necesito un pago de U$D22,110 durante el transcurso de la mañana, hazme saber si estas disponible ahora, así puedo enviarte los detalles. Debemos regularizar esto hoy.

Urgencia

Saludos
Wilson

Enviado desde mi iPhone

¿Qué podríamos verificar?

1) Brindar especial atención cuando se solicita que el movimiento de fondos se realice hacia una cuenta bancaria nueva o diferente a la que se venía utilizando.

2) Revisar que el dominio al que se esté respondiendo un correo con esta solicitud sea el correcto.

3) Reconfirmar de forma telefónica con la supuesta persona que está solicitando la transferencia.

Comportamiento del Hacker

Mail Header

Received: from p3plwbeout05-06.prod.phx3.secureserver.net (p3plsmtp05-06-02.prod.phx3.secureserver.net [97.74.135.51]) (using TLSv1.2 with cipher DHE-RSA-AES128-SHA (128/128 bits)) (No client certificate requested) by itf-01.company.com (Postfix) with ESMTPS id E0B9815FC65 for <Sandra_Finance@company.com>; Mon, 1 Aug 2016 05:47:42 +0000 (UTC)

Received: from localhost ([97.74.135.4]) by p3plwb[illegible] id Rhni1t[illegible]01hniYP; Sun, 25 Jul 2016 20:17:32 -

X-CMAE: v=2.1 cv=L/aTQoj8 c=1 sm=1 tr=0 p=i-petxfovf8[illegible]/YOLsA:10 a=9cW_t1CCXrUA:10 a=s5jvgZ67dGcA:10 a=WJA2BgnzfmMA:10 a=A7pwO9xP048A:10 a=IkcTkHD0fZMA:10 a=7z1cN_iqozsA:10 a=XRiNTI-inqA6s2tnS[illegible]JA:9 a=H8oodQkAz7yfcEeC:21 a=QEXdDO2ut3YA:10 a=_W_S_7VecoQA:10

Message-Id: <08924520399f2e65d9e0753294fa8fa4@email05.secureserver.net>

User-Agent: Workspace Webmail 6.4.2

X-Domain: entraser.com

X-SID: Rhni1t00205rkER01

Received: (qmail 15064 invoked by uid 99); 1 Aug 2016 05:47[illegible]

Content-Transfer-Encoding: quoted-printable

De: "Wilson Ceo" <wilson_ceo@compony.com>

Para: Sandra_Finance@company.com

Content-Type: text/[illegible]; charset="utf-8"

X-Sender: amina@entraser.com

Responder-a: "Wilson Ceo" <emailpresident2@gmail.com>

Date: Sun, 31 Jul 2016 22:47:40 -0700

Proveedor de correo inseguro !

! **Falsificado De: dominio**

Respuesta a un servicio gratuito !

Phishing

- Usa como vector principal el correo electrónico.
- Puede llevar a URLs falsas donde el usuario ingresa credenciales tanto corporativas como personales
- Tiene como objetivo el robo de datos sensibles o el compromiso de cuentas de correo para descarga de malware

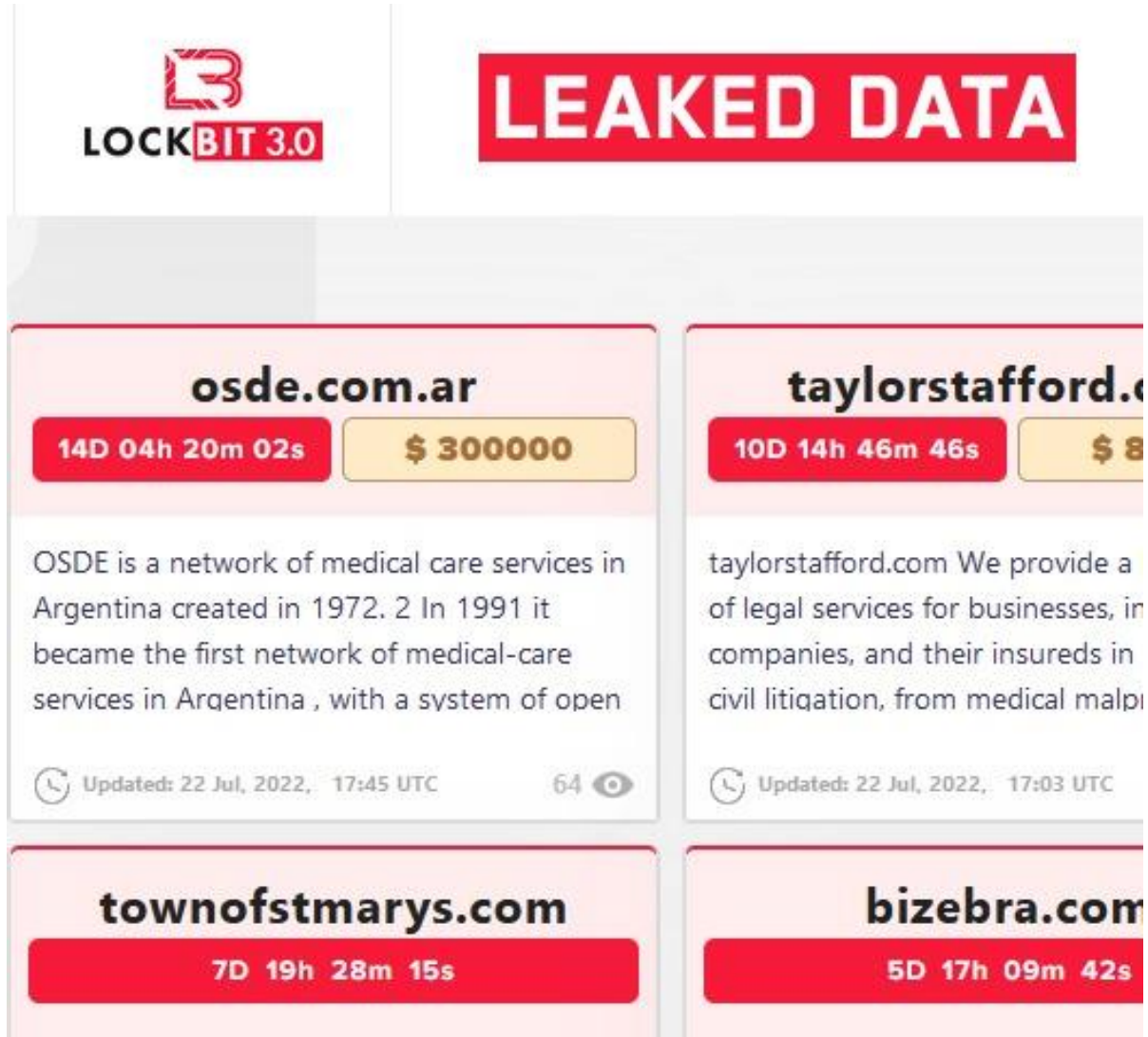

Acción requerida
Equipo de netflix <[redacted]@getticket.solutions>
Responder a: [redacted]@getticket.solutions
Para: [redacted]
7 de abril de 2019, 2:56
Acción requerida
Equipo de netflix <[redacted]@getticket.solutions>
Responder a: [redacted]@getticket.solutions
Para: [redacted]
Hemos notado alguna actividad inusual en su cuenta.
Su cuenta está bloqueada y pendiente de verificación.
Utilice el siguiente enlace para actualizar.
ACTUALIZAR
Equipo de netflix
15 Shenstone Rd, Brisbane, 4001
Unsubscribe - Unsubscribe Preferences


Netflix Argentina: Ve programa
https://www.netflix.com/ar/
Primeros pasos
Leads My Open Lead
Información del sitio para www.netflix.com
Conexión
Conexión segura
Bloqueo de contenido
Estándar
Se detectó contenido bloqueable en este sitio.
Rastreadores
Cookies
Bloqueo de cookies de rastreo
Desactivar el bloqueo para este sitio
Informar sobre un problema
Permisos
No ha dado permisos especiales a este sitio.
Eliminar las cookies y los datos del sitio...
Iniciar sesión
Tu
storia, ahora.
DIS
ANCELA CUANDO QUIERAS.
PROBAR AHORA

Ransomware

- Los emails de phishing a menudo contienen ransomware
- Encripta archivos que se consideran importantes para el negocio o los individuos.
- Genera interrupciones en la continuidad del negocio


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy

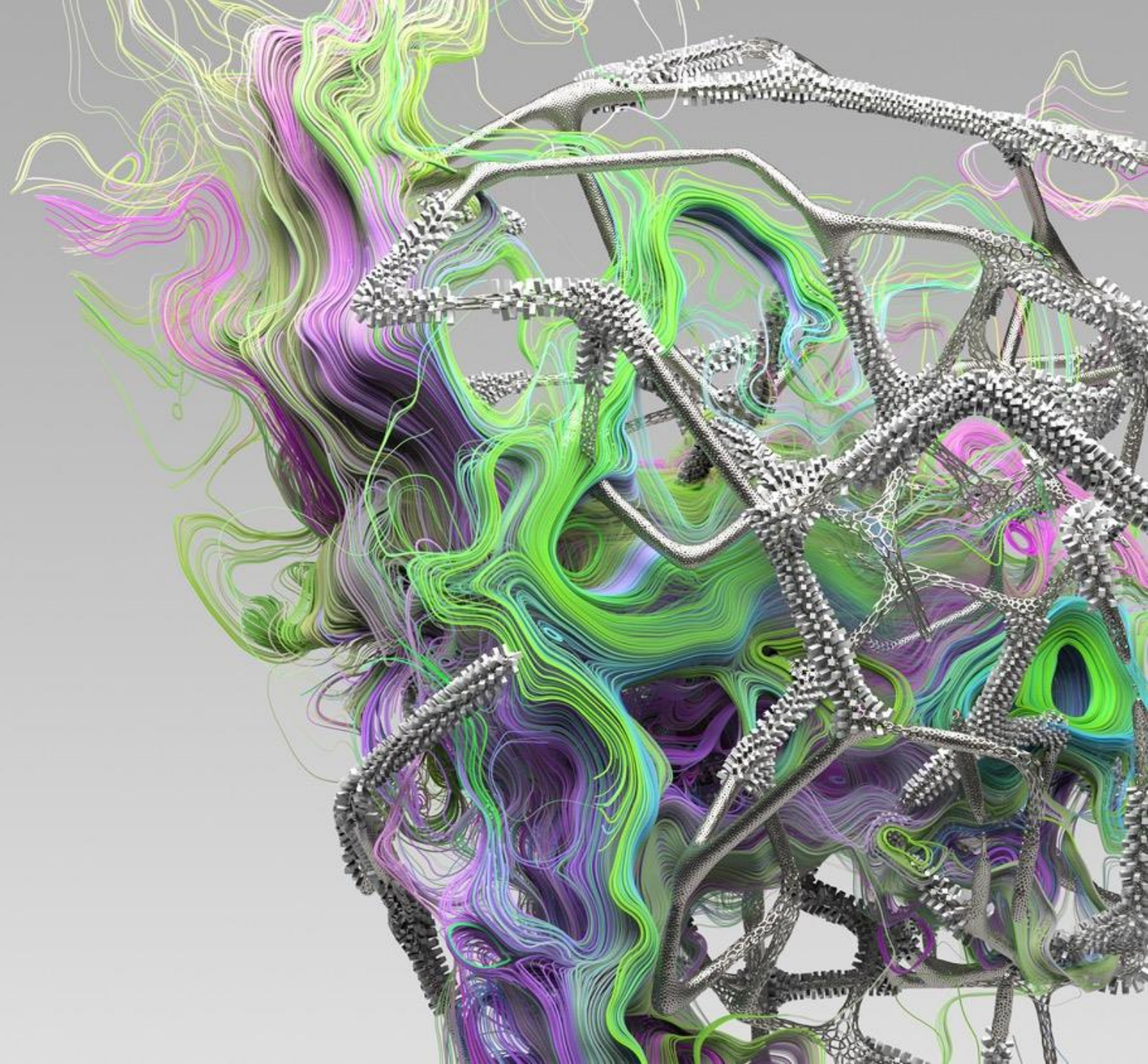

LOCKBIT 3.0
LEAKED DATA
osde.com.ar
14D 04h 20m 02s
$ 300000
OSDE is a network of medical care services in Argentina created in 1972. 2 In 1991 it became the first network of medical-care services in Argentina , with a system of open
Updated: 22 Jul, 2022, 17:45 UTC
64
taylorstafford.
10D 14h 46m 46s
$ 8
taylorstafford.com We provide a
of legal services for businesses, in
companies, and their insureds in
civil litigation, from medical malpr
Updated: 22 Jul, 2022, 17:03 UTC
townofstmarys.com
7D 19h 28m 15s
bizebra.com
5D 17h 09m 42s

¿Como protegernos del ransomware?

- Mantener actualizados nuestros sistemas operativos y aplicaciones
- Utilizar software de antivirus en nuestros dispositivos
- No descargar archivos que no sean de sitios seguros
- Ante la duda, consultar a un especialista

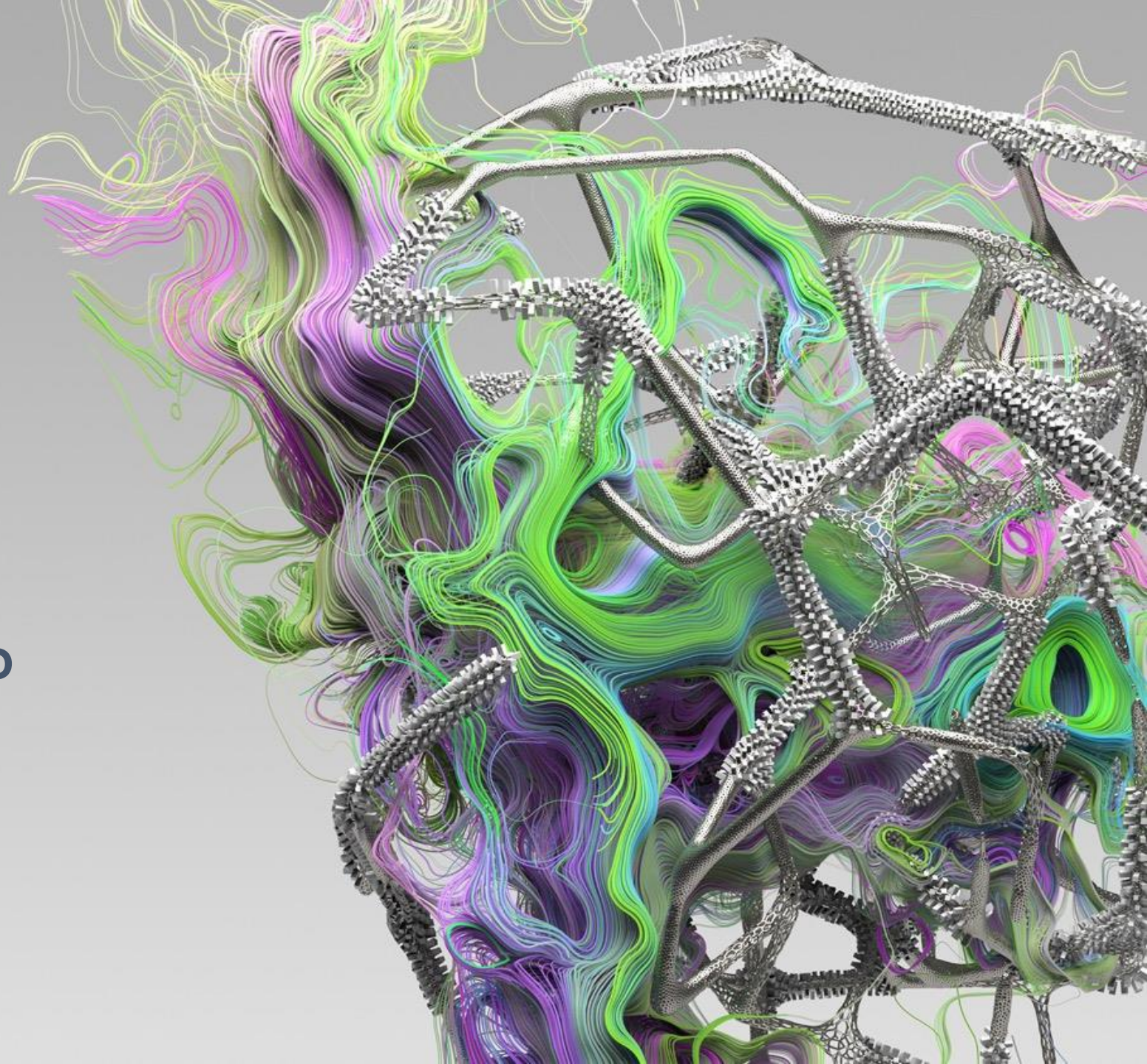
Herramientas útiles

- https://global.sitesafety.trendmicro.com/
- https://www.virustotal.com/gui/home/upload
- https://www.trendmicro.com/es_es/forHome/products/housecall.html



julianm@edsitrend.com

TREND MICRO™



¿Preguntas? ¿Dudas?

TREND MICRO™

¡Gracias!