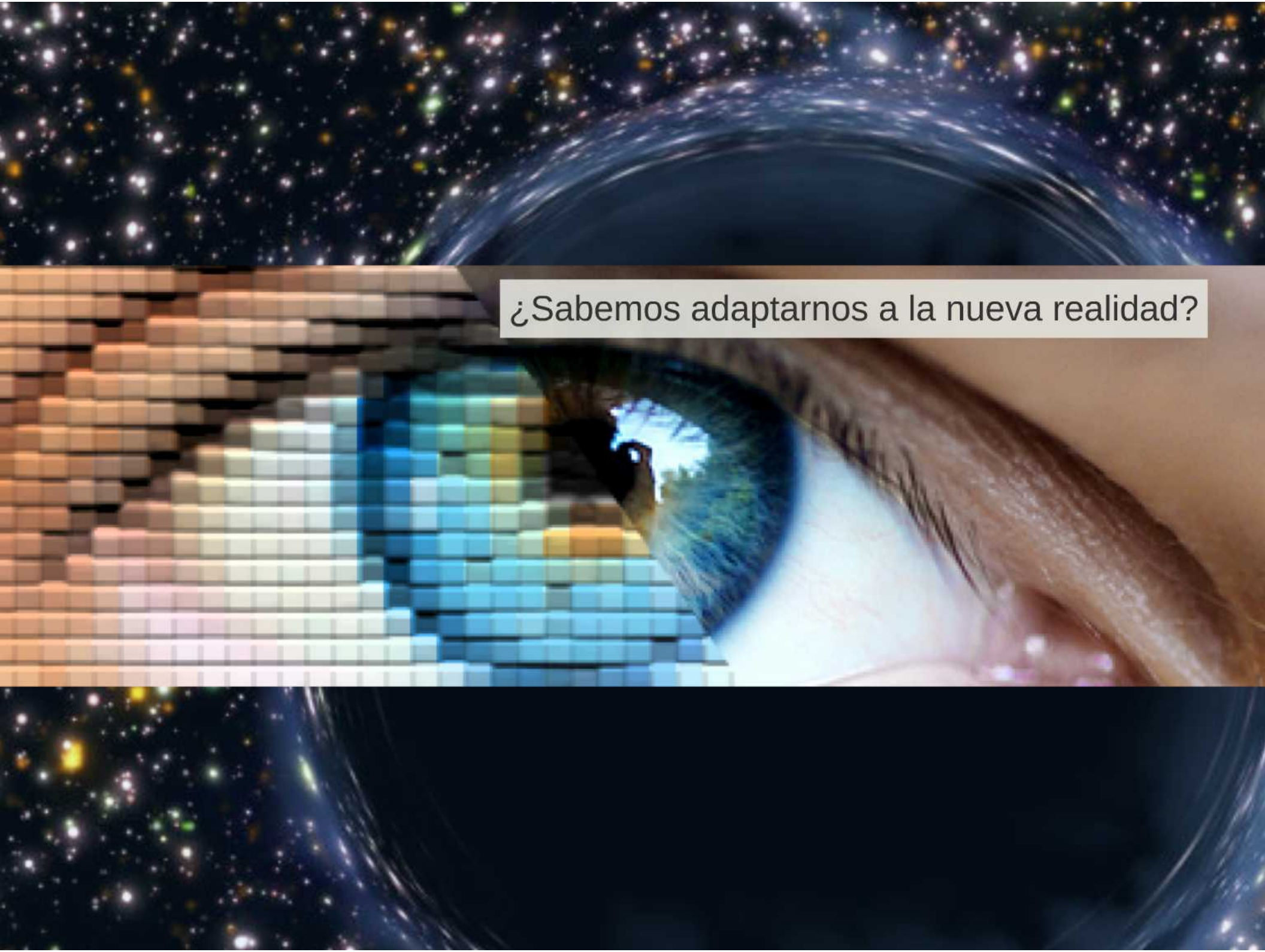
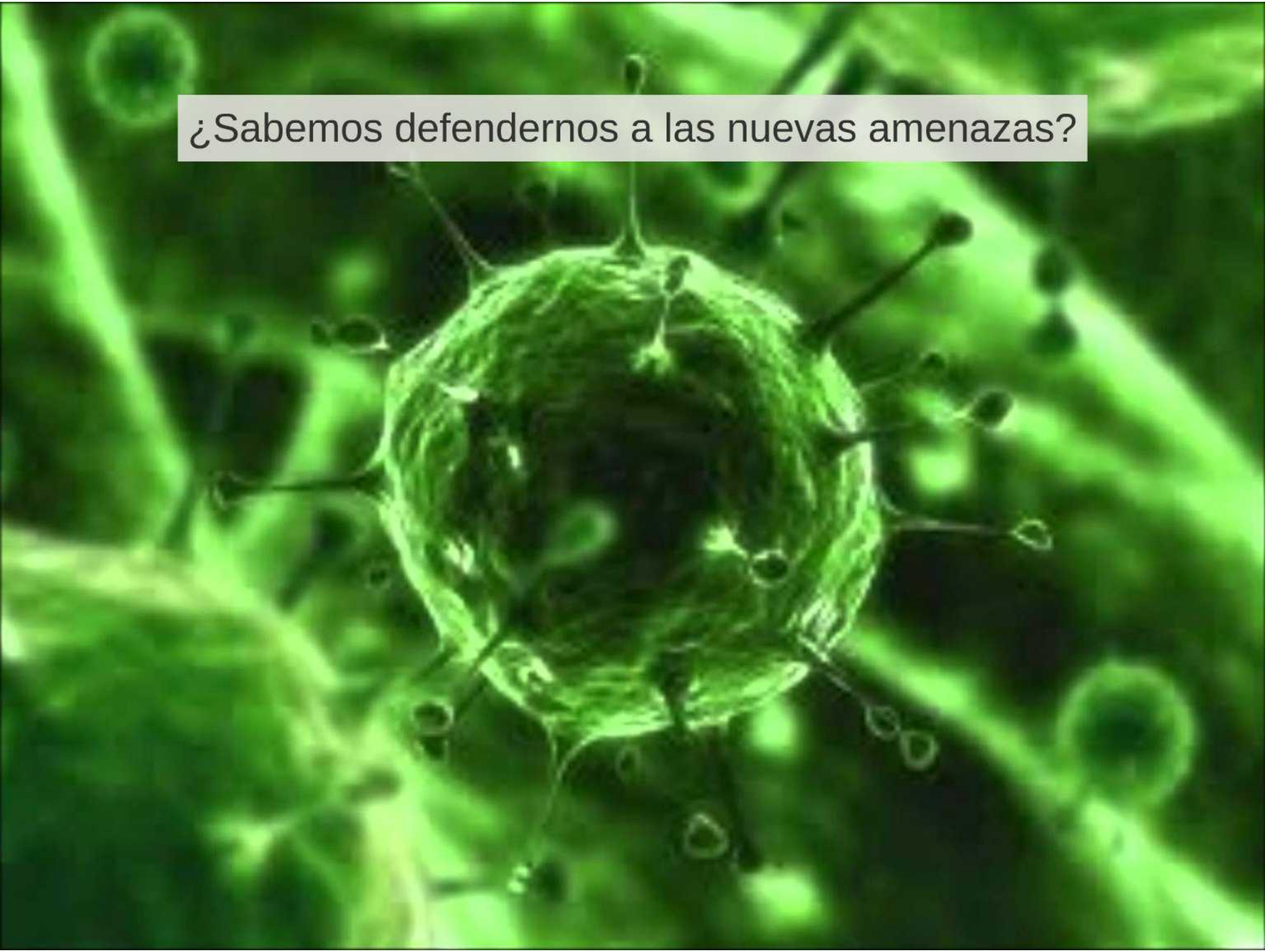
Reprogramando el cerebro contra los ciberataques

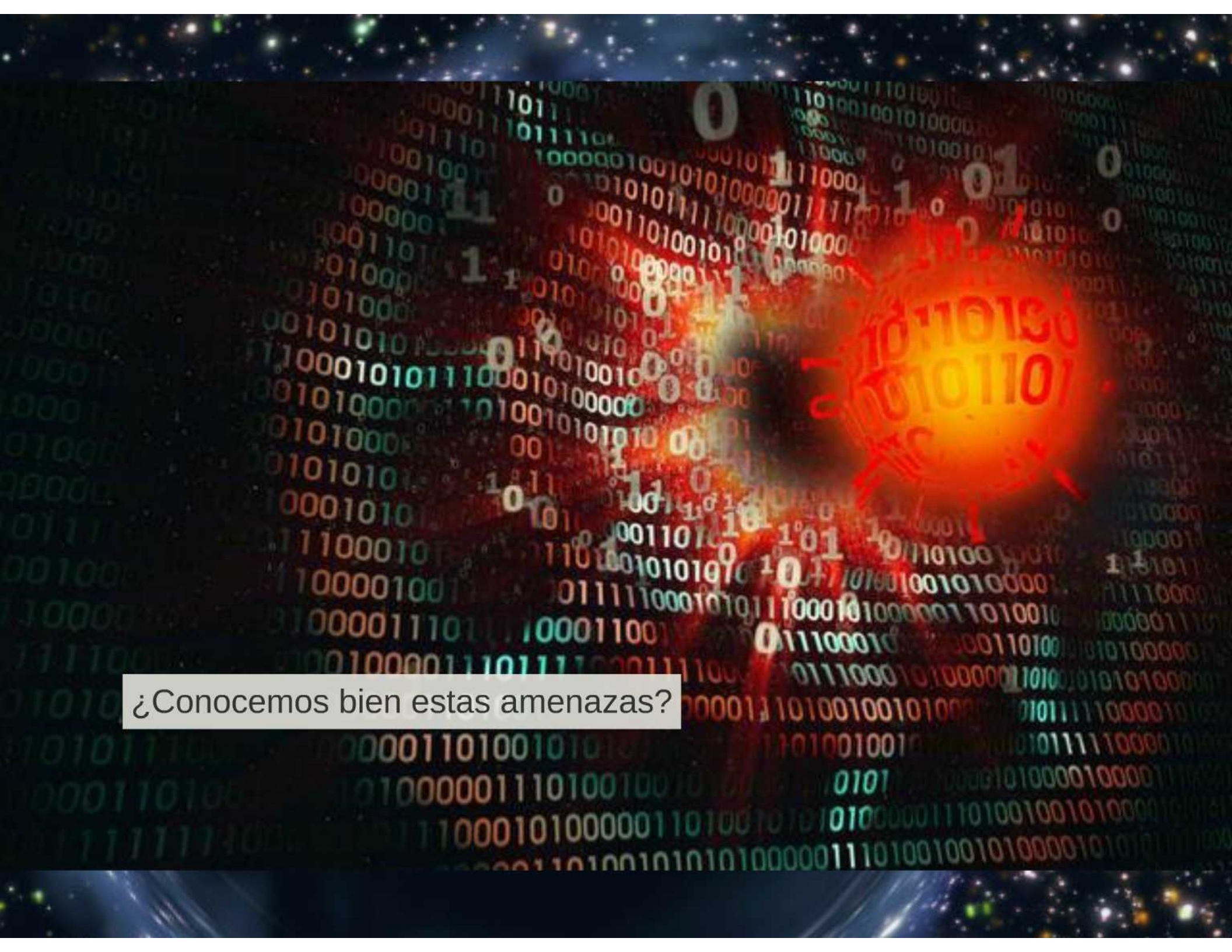
2017 @juancrui

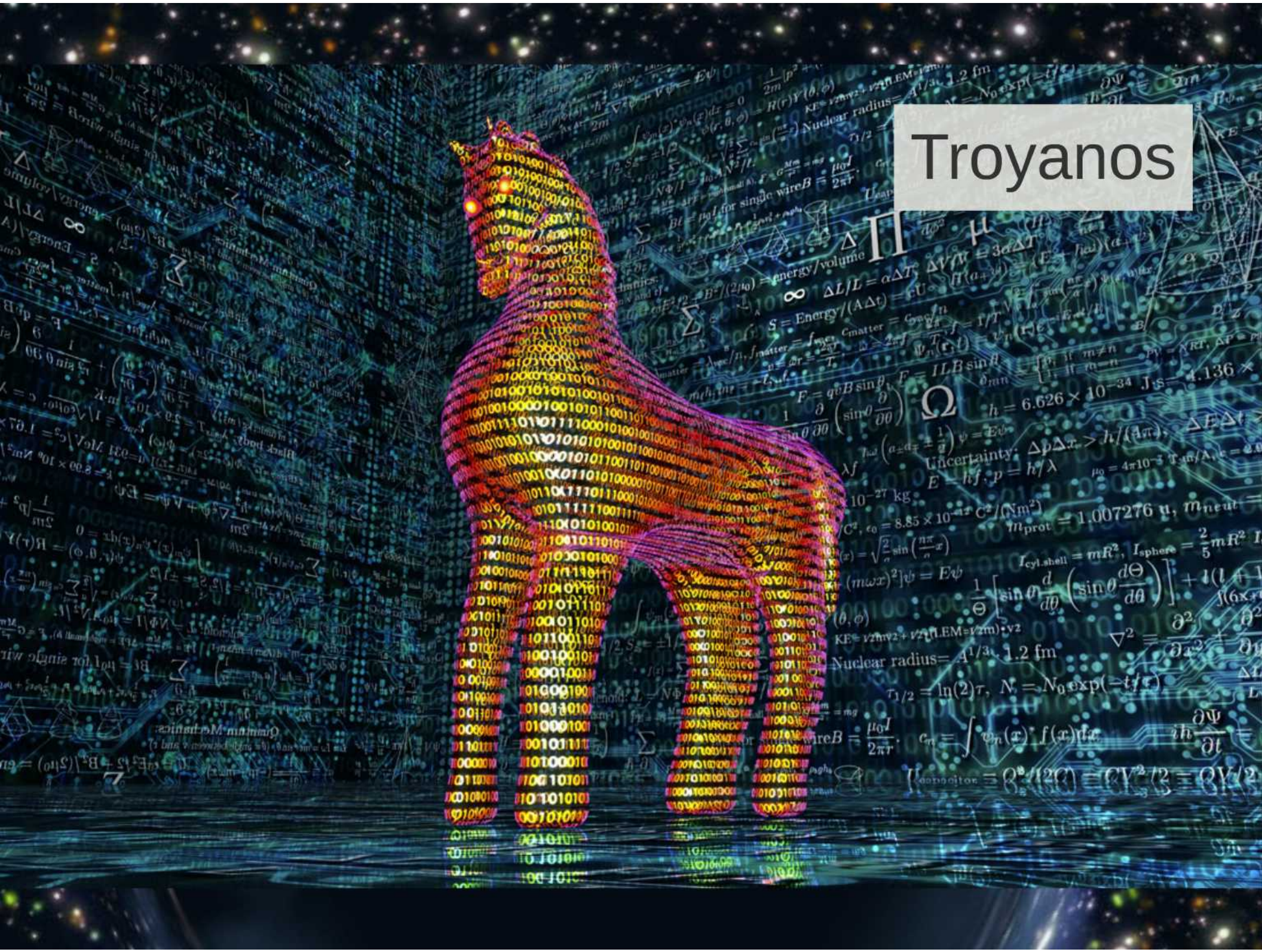
Reprogramando el cerebro contra los ciberataques

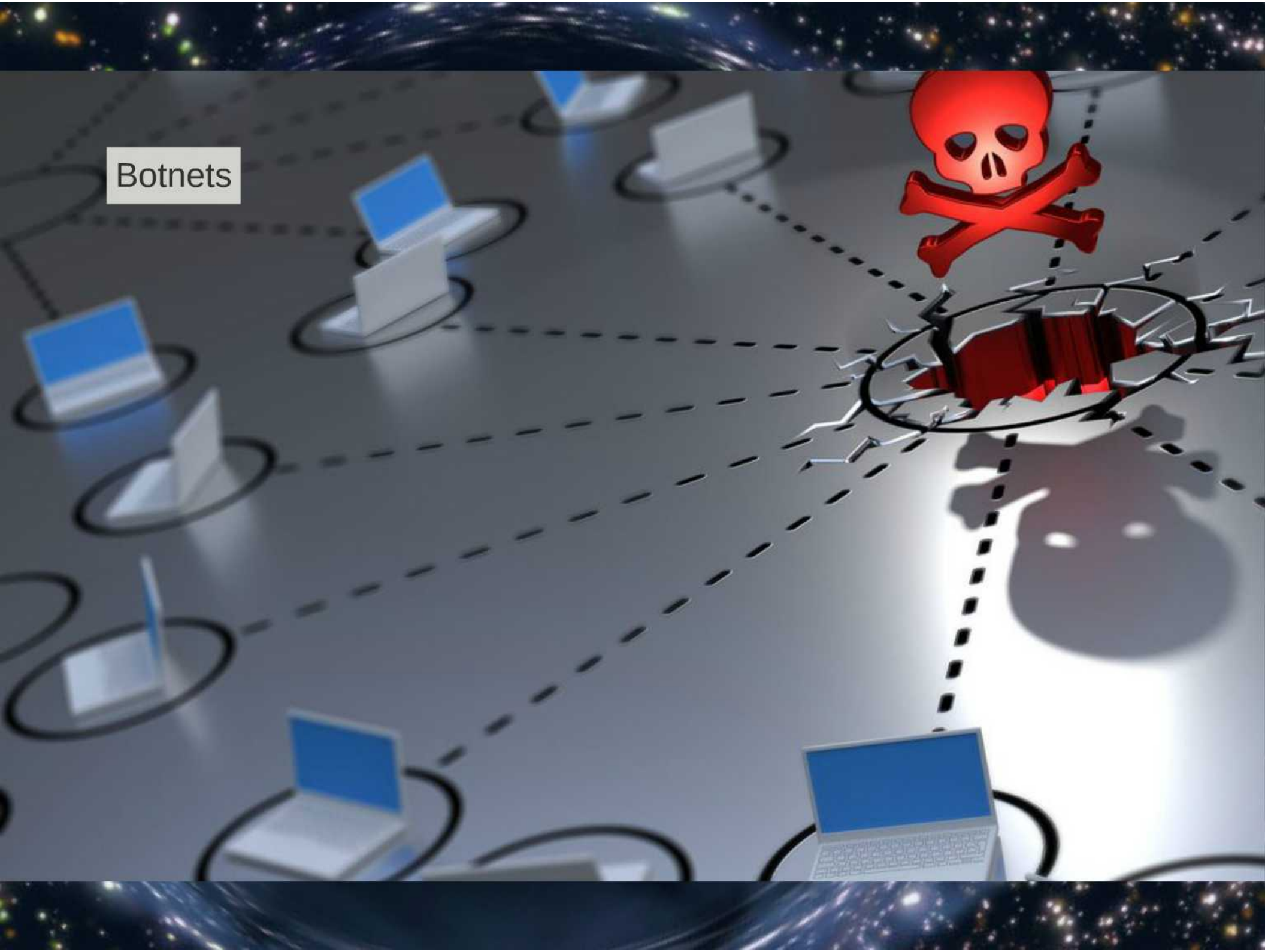
2017 @juancrui

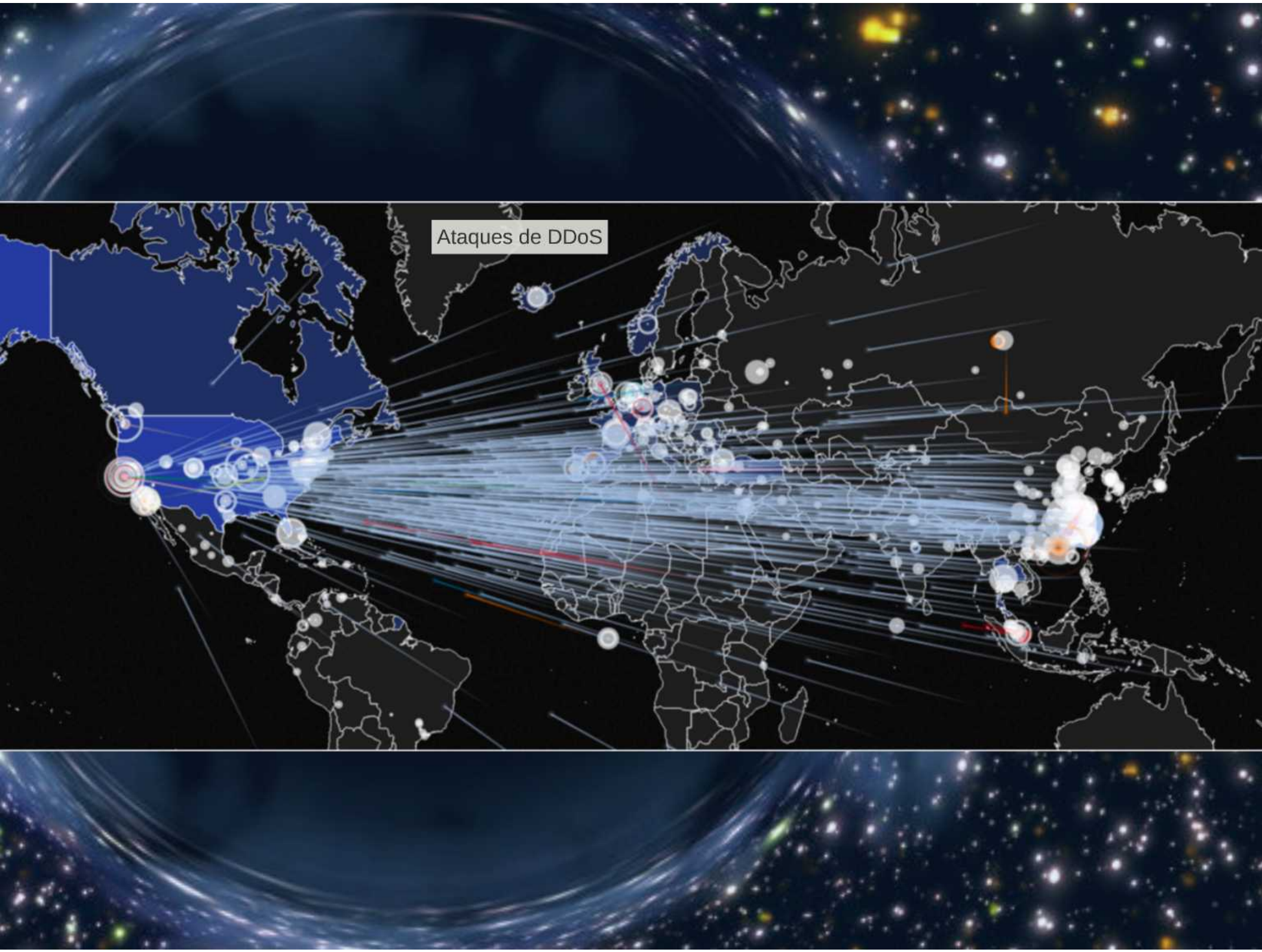

¿Sabemos adaptarnos a la nueva realidad?

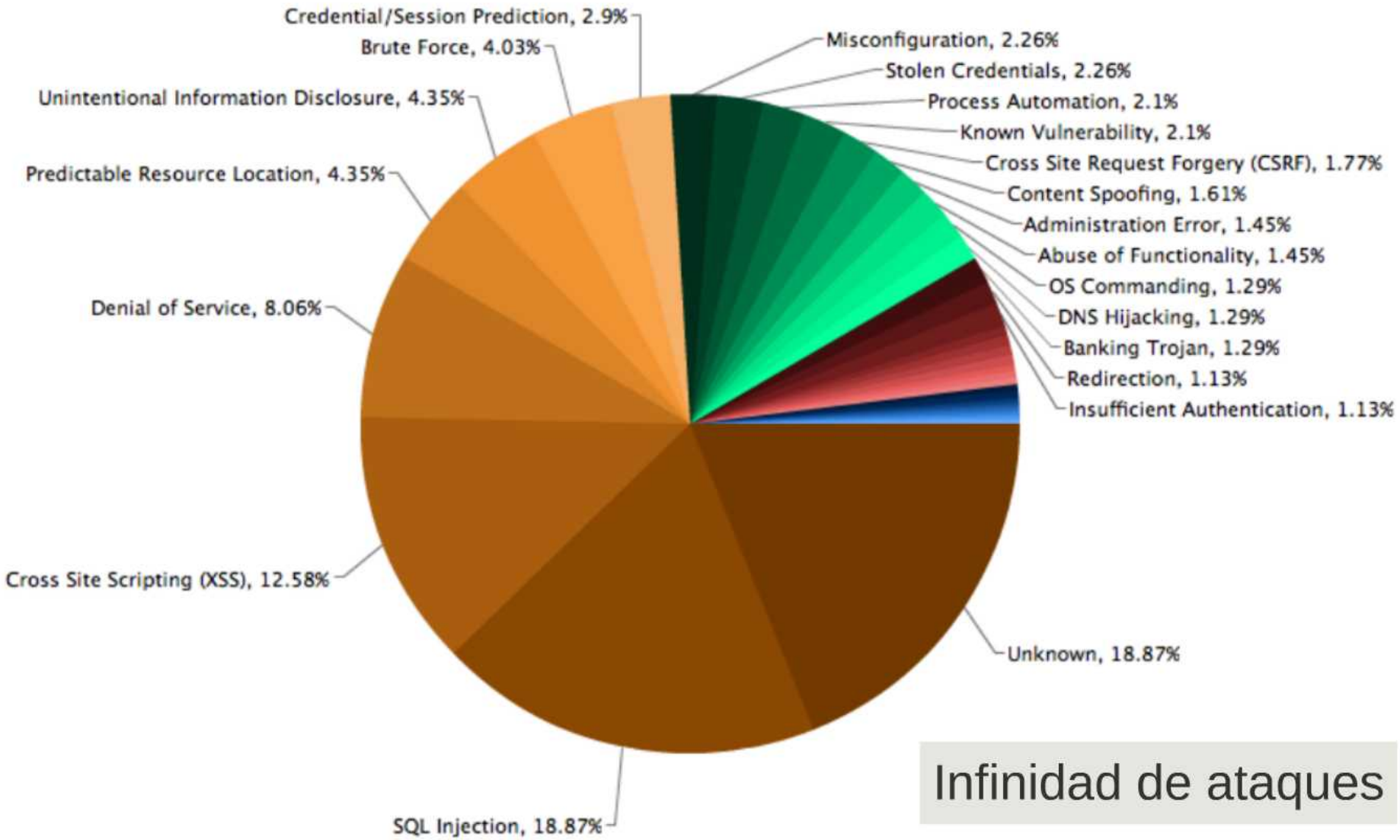

¿Sabemos defendernos a las nuevas amenazas?


¿Conocemos bien estas amenazas?


Troyanos

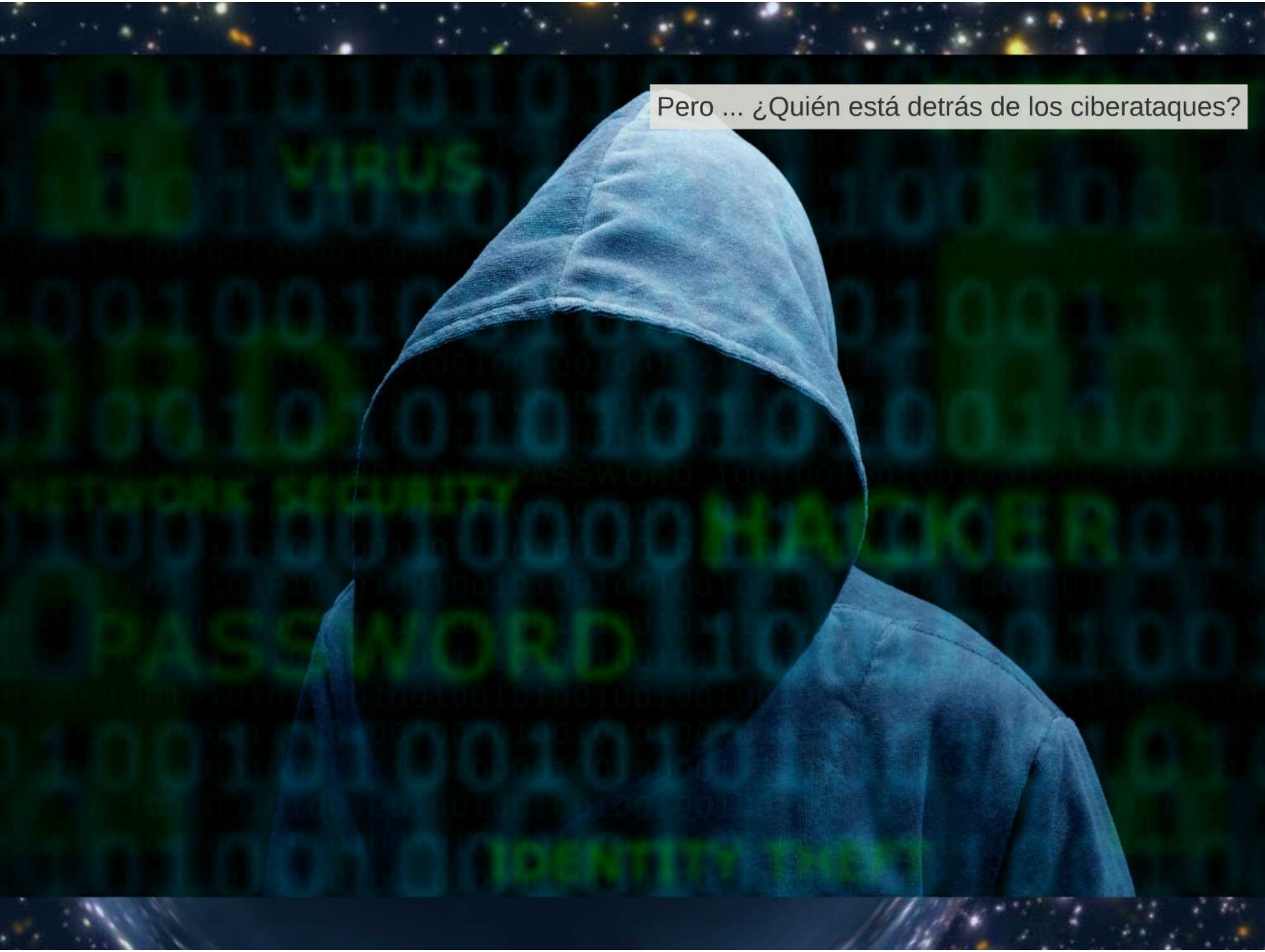

Botnets

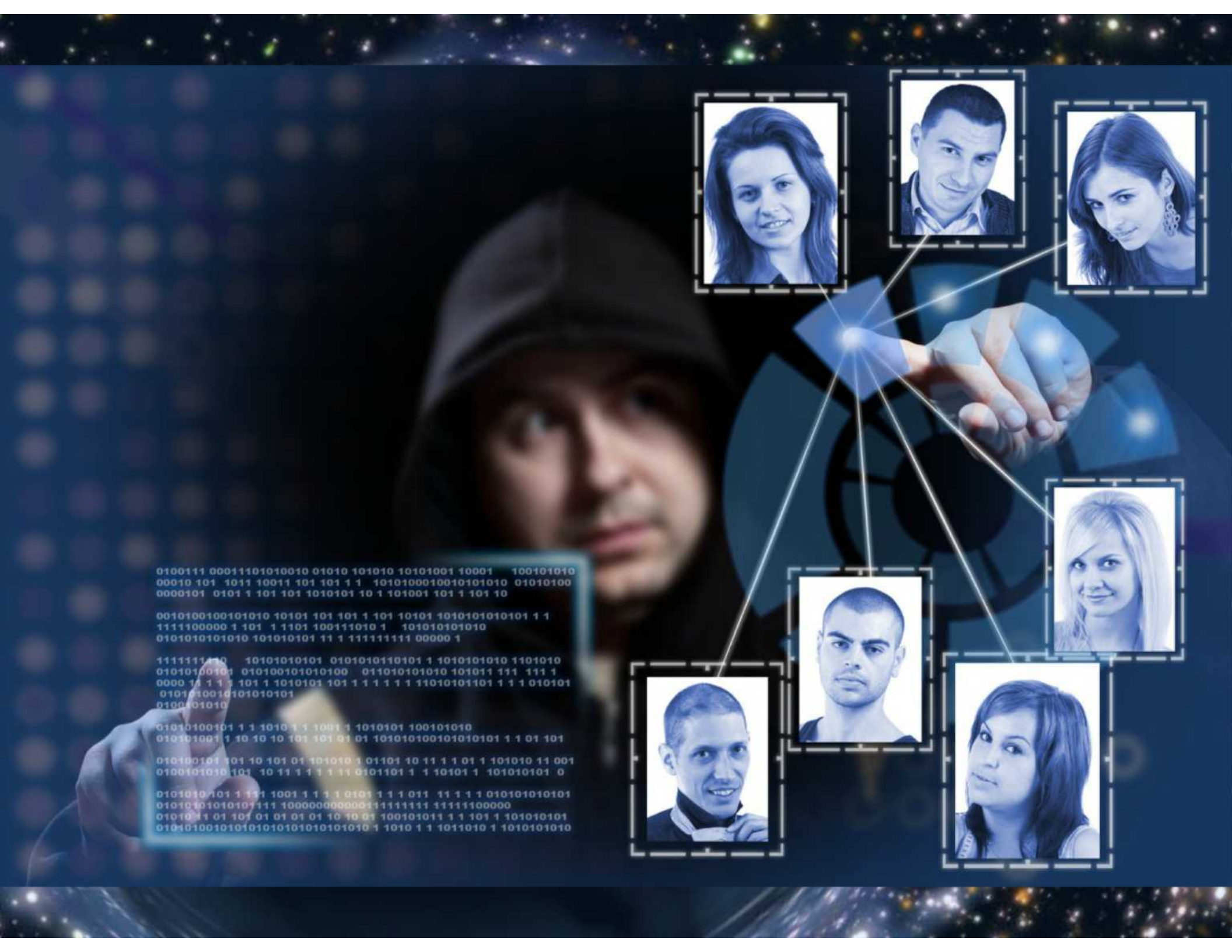

Ataques de DDoS



Infinidad de ataques


spyware
spam
virus
attack
phishing
trojan
data
security
malware
virus alert!
virus detected

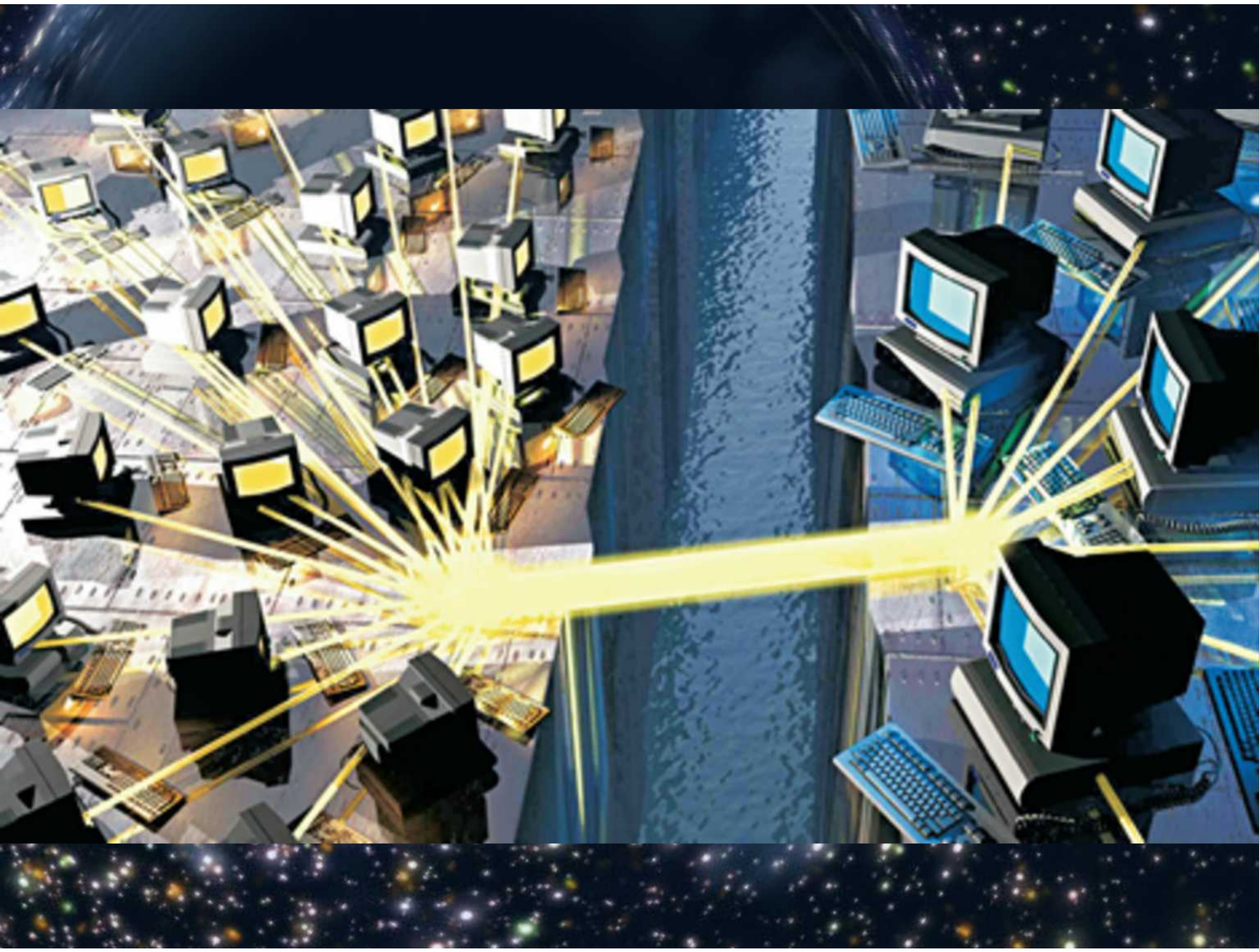

Pero ... ¿Quién está detrás de los ciberataques?




MR.ROBOT


VIRUS
INTRUDER
CRACKER
SPYWARE
PASSWORD
IDENTITY
UNSAFE
CODE
HACKER


Estados




Say it
CLEARER
Use it
HOPE
BY BHINDA JATT

CyberCaliphate

you isis

U.S. Central Command

TWEETS 3,676 | FOLLOWING 1,268 | FOLLOWERS 109K | FAVORITES 30

Follow

Tweets | Tweets & replies | Photos & videos

Who to follow · Refresh · View all


¿Cómo lo hacen?

¿De dónde se obtienen las vulnerabilidades?

- Underground Market
- Zero-Day
- Publicaciones
- Agencias de Inteligencia

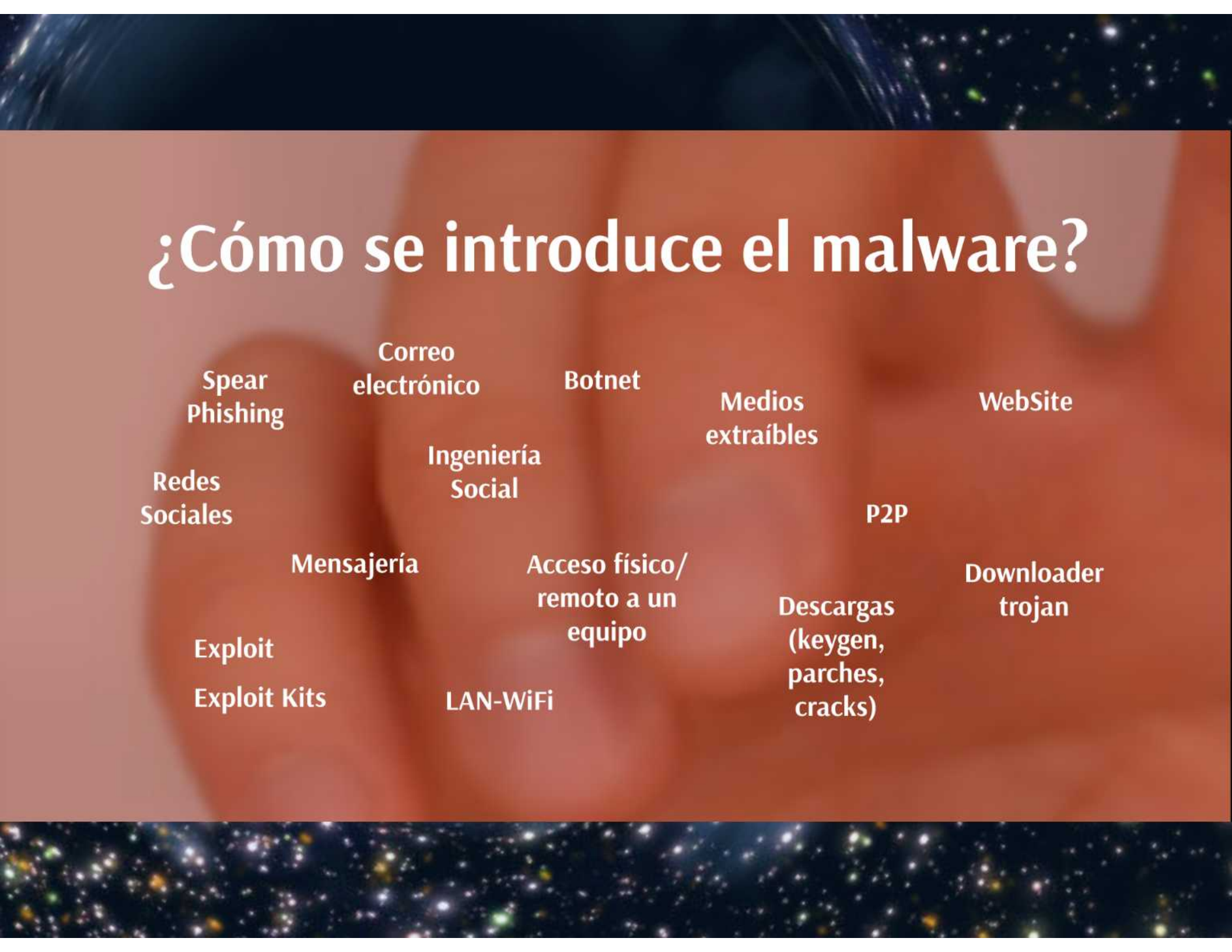
Recent prices from the black market		Price	
		1BTC	213,200 EUR
N	**SERVICES**	**BTC**	**EUR**
50.000	Root shell	1,85	394,62
45.000	Wordpress admin passwords	1,50	319,80
50.000	SSH sniffer logs	1,20	255,84
1.000	Linux botnet	2,00	426,40
1.103.504	FTP/SSH passwords	3,00	639,60
N	**SERVICES**	**BTC**	**EUR**
1	Start your own maket	33,48	7.137,00
1	Virtual credit card + bank account	0,01	2,69
1	Unlimited REAL code signing	4,20	895,44
TYPE	**KIT**	**BTC**	**EUR**
spam	Wordpress Comment Spammer + Exploit	2,50	533,00
malware	Bitcoin Ransomware	0,21	44,77
malware	Tomcat Worm	7,40	1.578,67
malware	The real GovRAT	4,50	959,40
TYPE	**EXPLOIT**	**BTC**	**EUR**
1day	MS15-034 Microsoft IIS Remote Code Execution	308,53	65.778,11
1day	*NEW* ring0 LPE Exploit CVE-2015-0057	48,17	10.269,84
fud	Adobe Flash < 16.0.0.296 (CVE-2015-0313)	2,50	533,00
0day	Internet Explorer <= 11	35,00	7.462,00
0day	Android WebView 0day RCE	36,50	7.781,80
0day	Linux <= 3.13.0-48 Kernel Panic	2,00	426,40

Figure 2 - Listing and average prices for black markets

Recent prices from the black market		Price	
		1BTC	213,200 EUR
N	**SERVICES**	**BTC**	**EUR**
50.000	Root shell	1,85	394,62
45.000	Wordpress admin passwords	1,50	319,80
50.000	SSH sniffer logs	1,20	255,84
1.000	Linux botnet	2,00	426,40
1.103.504	FTP/SSH passwords	3,00	639,60
N	**SERVICES**	**BTC**	**EUR**
1	Start your own maket	33,48	7.137,00
1	Virtual credit card + bank account	0,01	2,69
1	Unlimited REAL code signing	4,20	895,44
TYPE	**KIT**	**BTC**	**EUR**
spam	Wordpress Comment Spammer + Exploit	2,50	533,00
malware	Bitcoin Ransomware	0,21	44,77
malware	Tomcat Worm	7,40	1.578,67
malware	The real GovRAT	4,50	959,40
TYPE	**EXPLOIT**	**BTC**	**EUR**
1day	MS15-034 Microsoft IIS Remote Code Execution	308,53	65.778,11
1day	*NEW* ring0 LPE Exploit CVE-2015-0057	48,17	10.269,84
fud	Adobe Flash < 16.0.0.296 (CVE-2015-0313)	2,50	533,00
0day	Internet Explorer <= 11	35,00	7.462,00
0day	Android WebView 0day RCE	36,50	7.781,80
0day	Linux <= 3.13.0-48 Kernel Panic	2,00	426,40

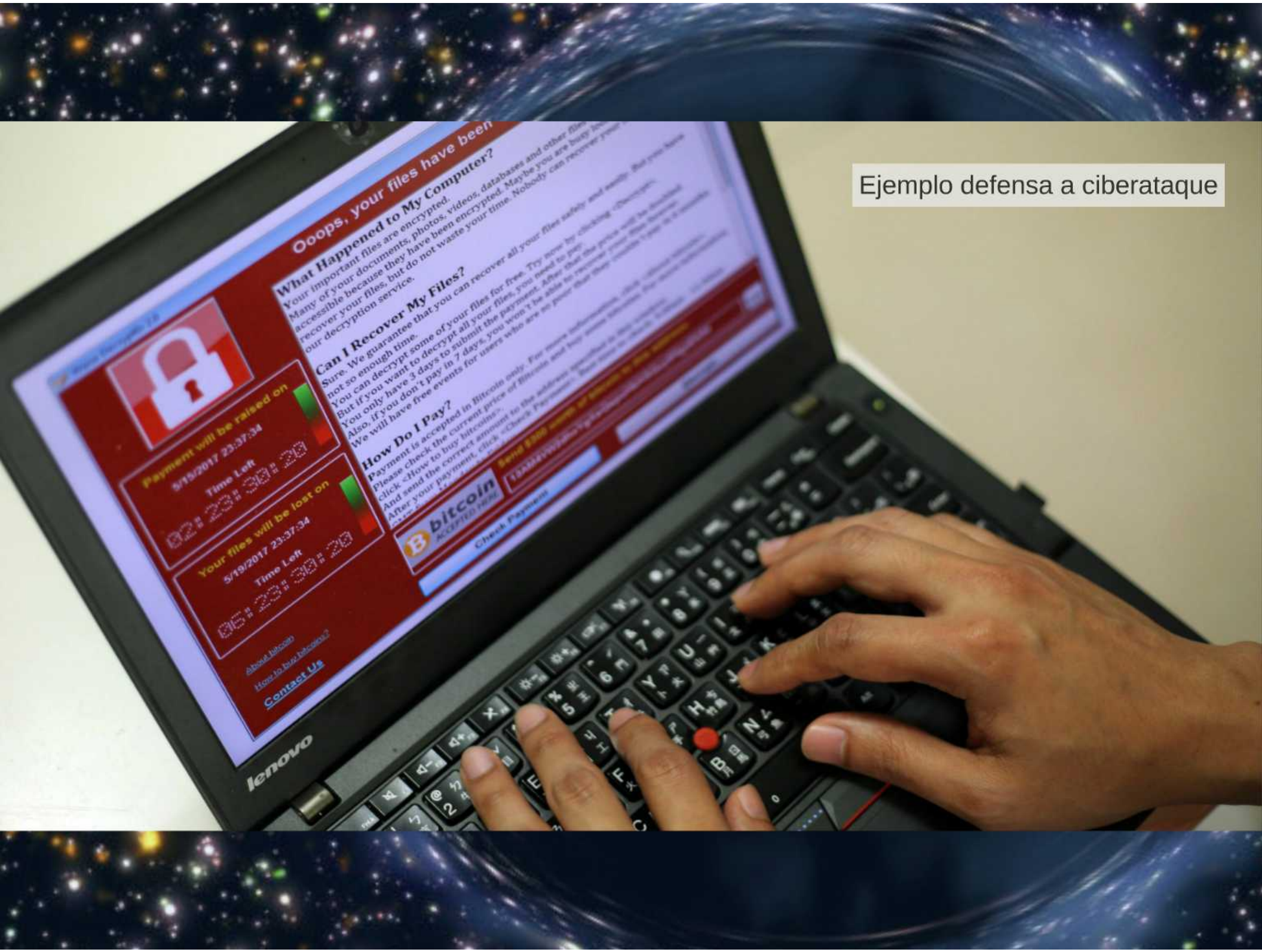
Figure 2 – Listing and average prices for black markets

¿Cómo se introduce el malware?



Ingeniería Social

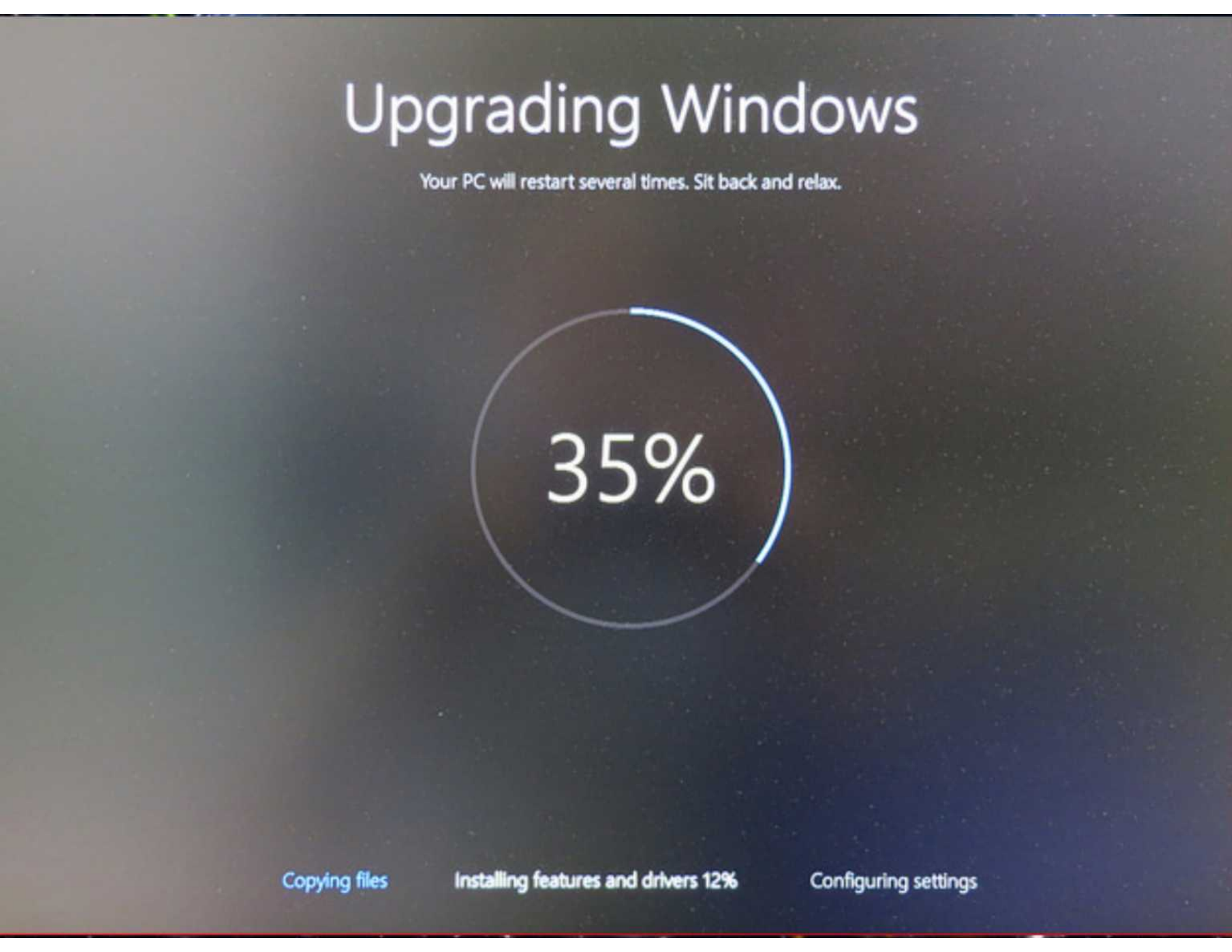
Es el conjunto de técnicas psicológicas y habilidades sociales utilizadas para la obtención de información o realización de una acción por parte de un tercero, sin que éste sea consciente de que lo que realmente está realizando.



Ejemplo defensa a ciberataque

¿Cómo puedo protegerme?

Copias de seguridad


Upgrading Windows
Your PC will restart several times. Sit back and relax.
35%
Copying files
Installing features and drivers 12%
Configuring settings


Reporting & Dashboard
Discovery
Spyware Blocking/ Removal
Host Intrusion Prevention
Inventory
Cloud Services Appliance
Endpoint Security Management
Patch Management
Audit & Compliance Enforcement
Application Blocking
Antivirus Auditing and Enforcement
Connection Control Management
Antivirus Add-On
Network Access Control Add-On


Training


Virtualización

Elegir la cuenta que desee cambiar

SATURNO
Administrador
Protegida por contraseña

juancrui
Administrador
Protegida por contraseña

SIT1
Usuario estándar
Protegida por contraseña

Invitado
La cuenta de invitado está desactivada

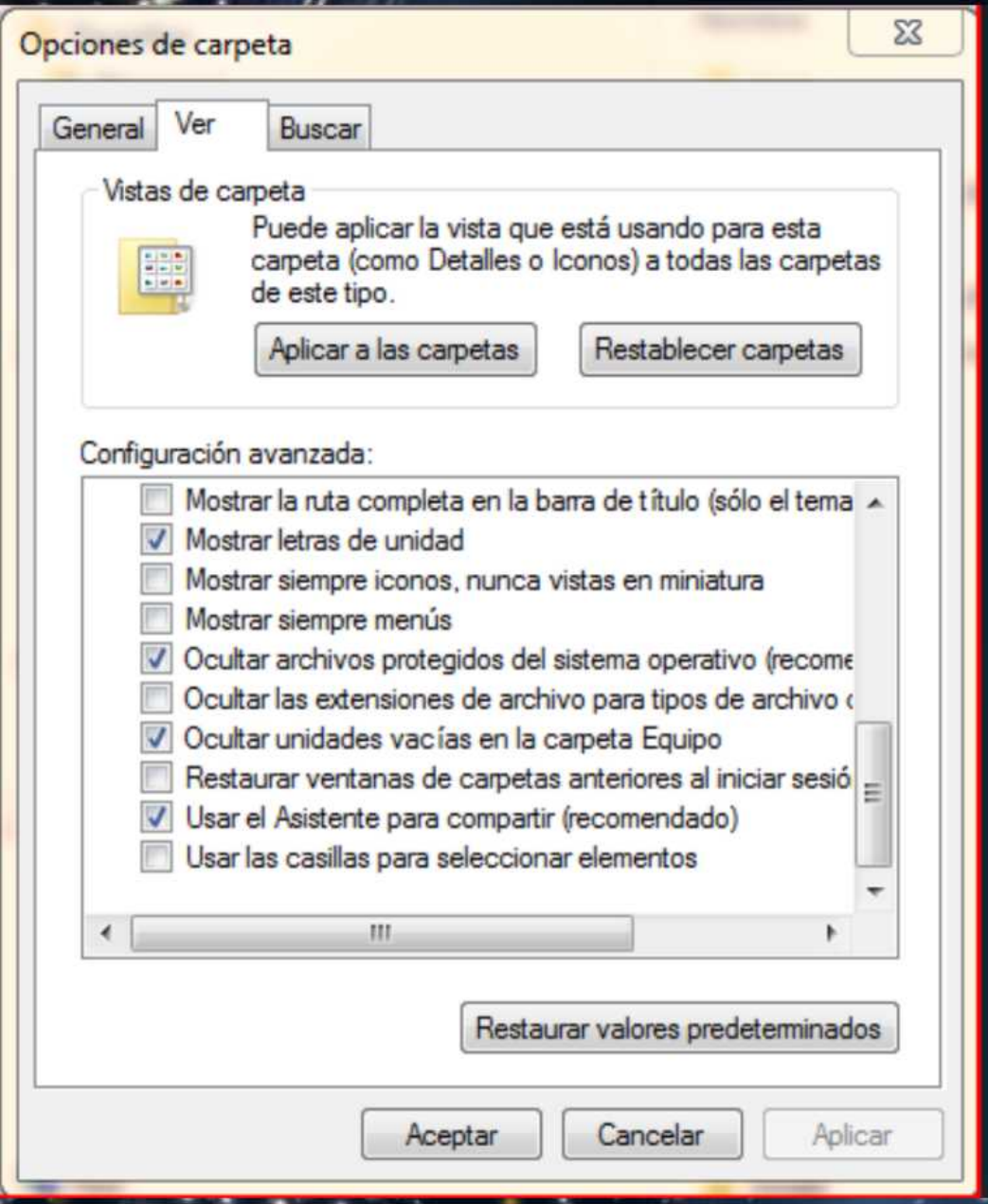
Crear una nueva cuenta

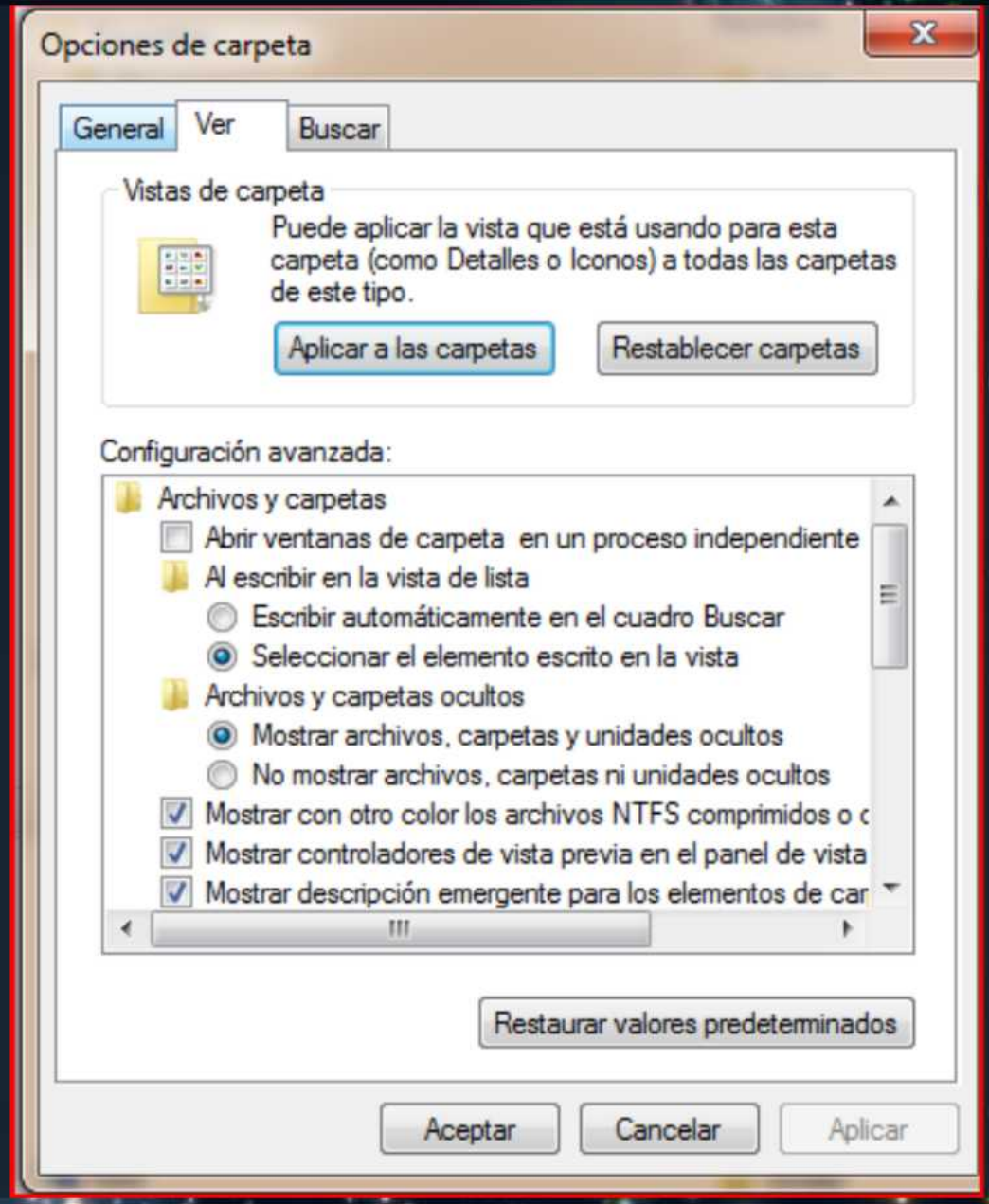
¿Qué es una cuenta de usuario?

Acciones adicionales que se pueden realizar

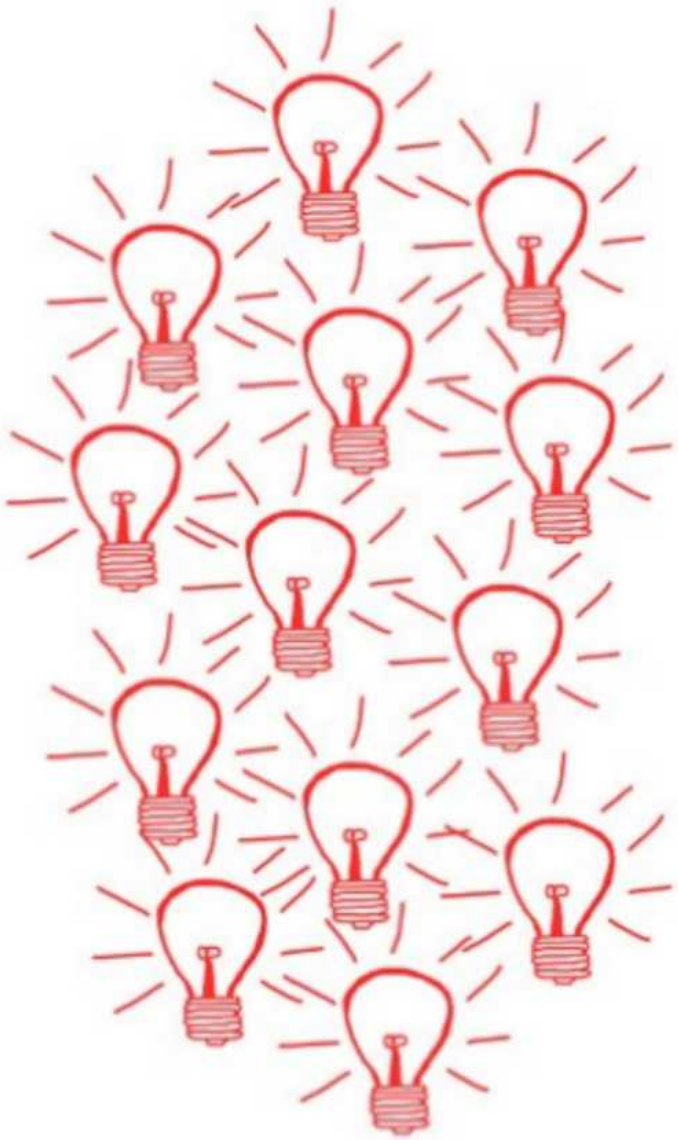
Configurar Control parental

Ir a la página principal de Cuentas de usuario

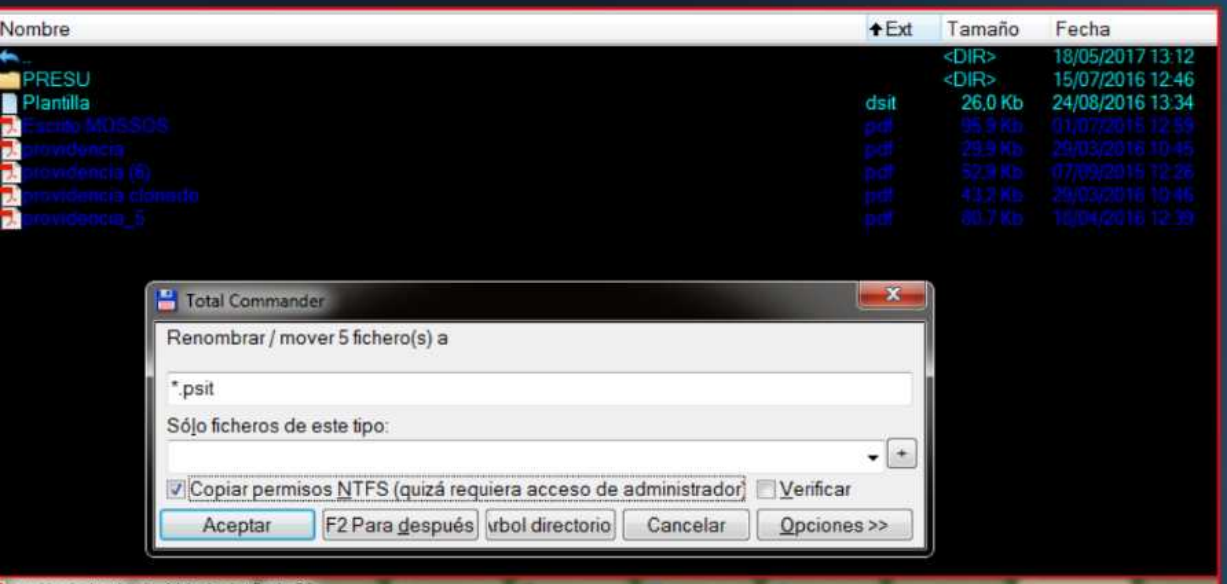

Opciones de carpeta
General
Ver
Buscar
Vistas de carpeta
Puede aplicar la vista que está usando para esta carpeta (como Detalles o Iconos) a todas las carpetas de este tipo.
Aplicar a las carpetas
Restablecer carpetas
Configuración avanzada:
Mostrar la ruta completa en la barra de título (sólo el tema
Mostrar letras de unidad
Mostrar siempre iconos, nunca vistas en miniatura
Mostrar siempre menús
Ocultar archivos protegidos del sistema operativo (recome
Ocultar las extensiones de archivo para tipos de archivo c
Ocultar unidades vacías en la carpeta Equipo
Restaurar ventanas de carpetas anteriores al iniciar sesió
Usar el Asistente para compartir (recomendado)
Usar las casillas para seleccionar elementos
Restaurar valores predeterminados
Aceptar
Cancelar
Aplicar

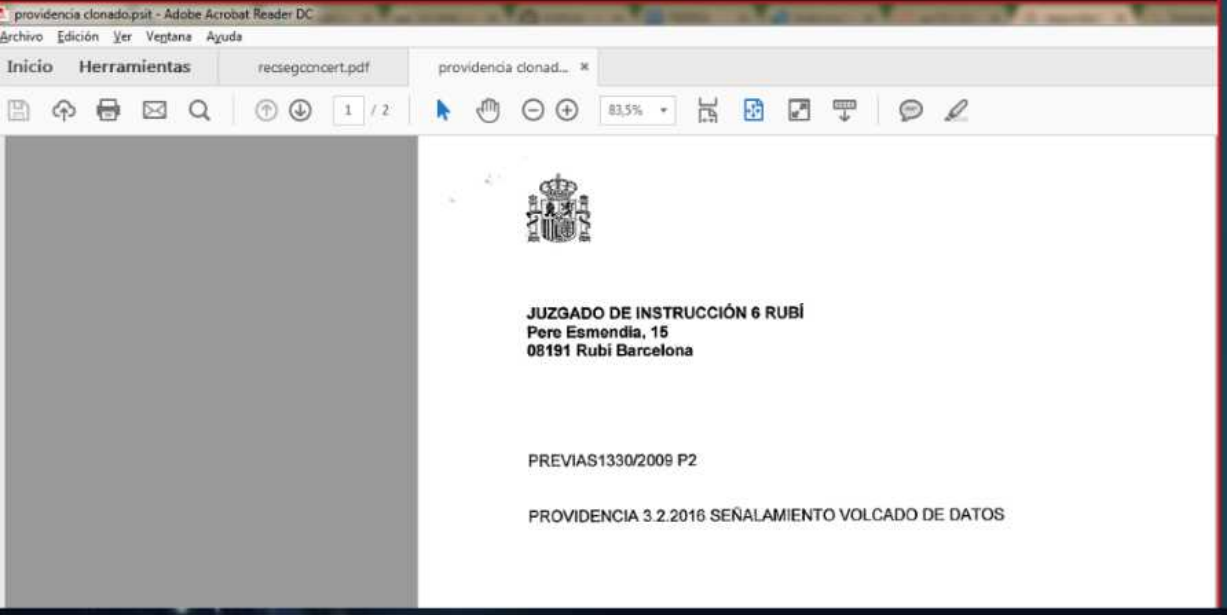

Opciones de carpeta
General
Ver
Buscar
Vistas de carpeta
Puede aplicar la vista que está usando para esta carpeta (como Detalles o Iconos) a todas las carpetas de este tipo.
Aplicar a las carpetas
Restablecer carpetas
Configuración avanzada:
Archivos y carpetas
Abrir ventanas de carpeta en un proceso independiente
Al escribir en la vista de lista
Escribir automáticamente en el cuadro Buscar
Seleccionar el elemento escrito en la vista
Archivos y carpetas ocultos
Mostrar archivos, carpetas y unidades ocultos
No mostrar archivos, carpetas ni unidades ocultos
Mostrar con otro color los archivos NTFS comprimidos o c
Mostrar controladores de vista previa en el panel de vista
Mostrar descripción emergente para los elementos de car
Restaurar valores predeterminados
Aceptar
Cancelar
Aplicar

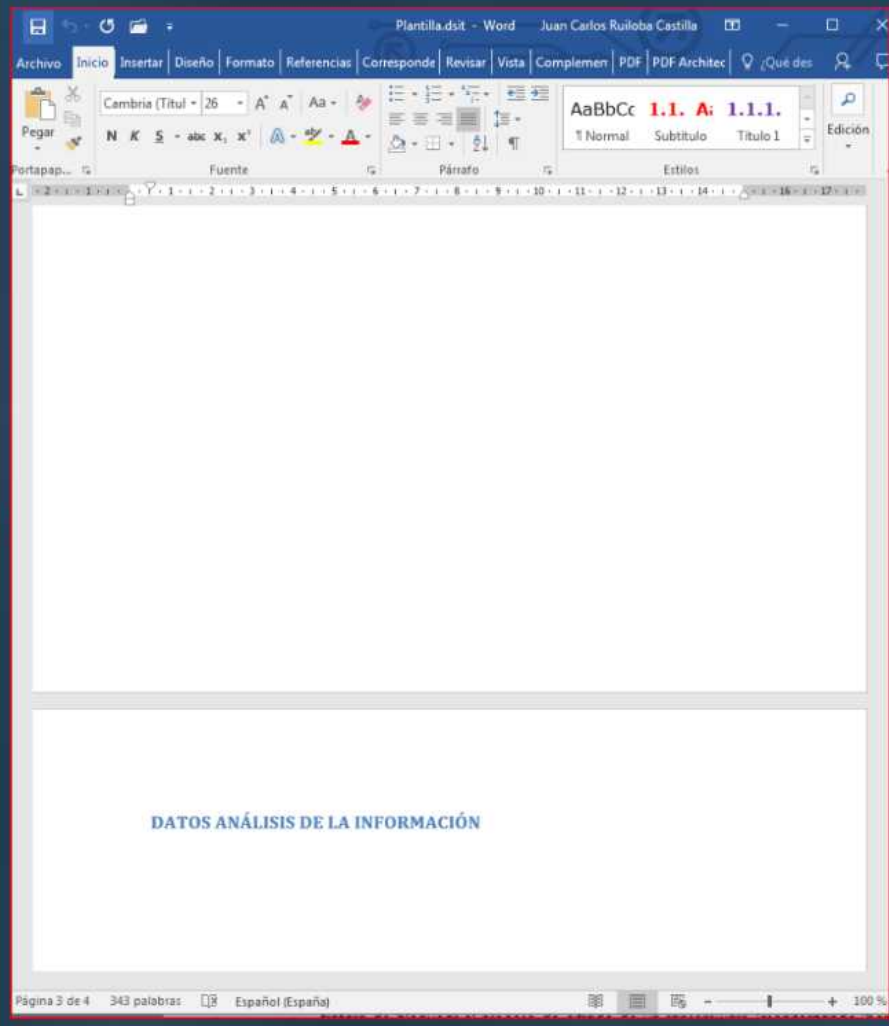
Implementar soluciones propietarias



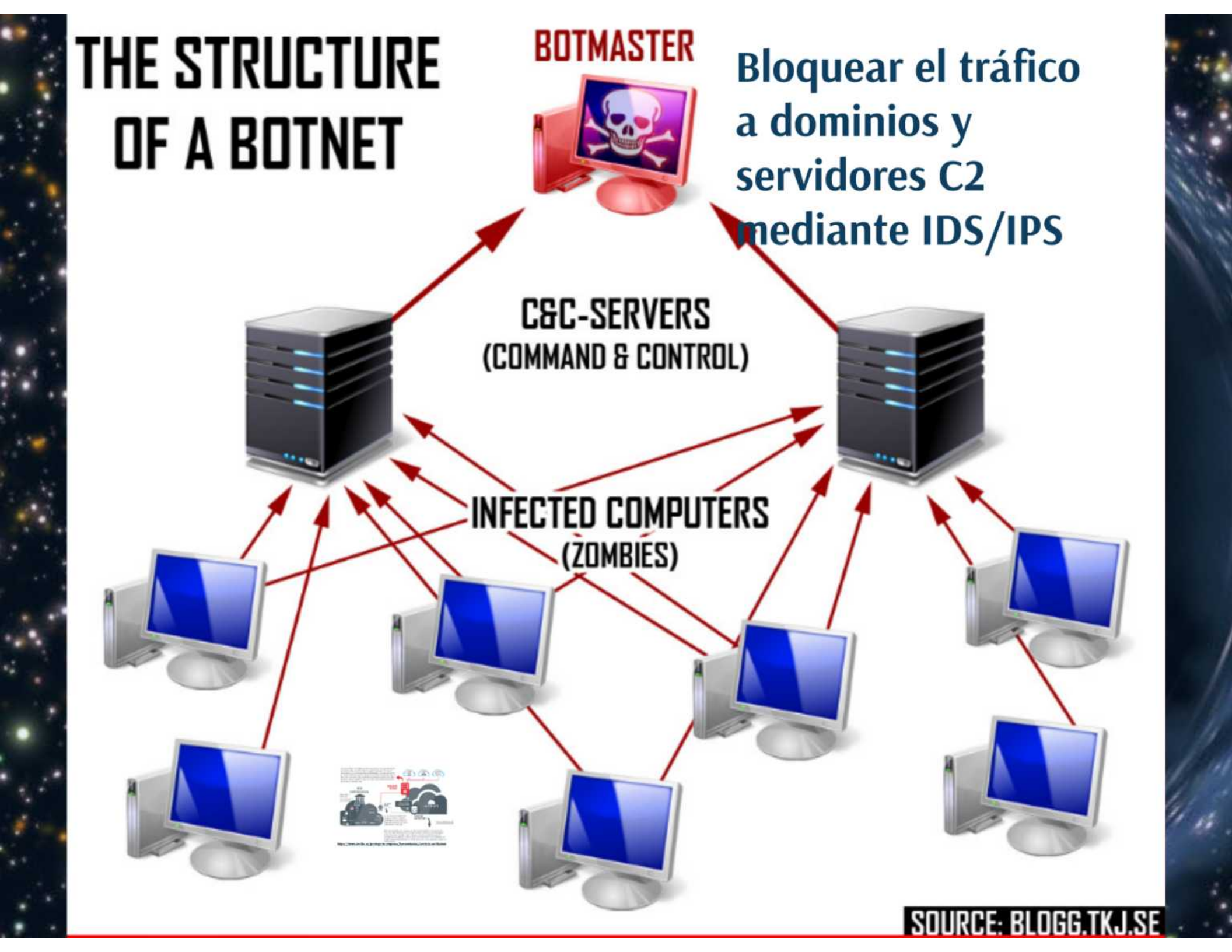
=


Nombre
Ext
Tamaño
Fecha
<DIR> 18/05/2017 13:12
PRESU <DIR> 15/07/2016 12:46
Plantilla dsit 26,0 Kb 24/08/2016 13:34
Total Commander
Renombrar / mover 5 fichero(s) a
*.psit
Sólo ficheros de este tipo:
Copiar permisos NTFS (quizá requiera acceso de administrador)
Verificar
Aceptar
F2 Para después
Arbol directorio
Cancelar
Opciones >>


providencia clonado.psit - Adobe Acrobat Reader DC
Archivo Edición Ver Ventana Ayuda
Inicio Herramientas
providencia clonad...
JUZGADO DE INSTRUCCIÓN 6 RUBÍ
Pere Esmendia, 15
08191 Rubí Barcelona
PREVIAS1330/2009 P2
PROVIDENCIA 3.2.2016 SEÑALAMIENTO VOLCADO DE DATOS


Plantilla.dsit - Word
Juan Carlos Ruiloba Castilla
Archivo Inicio Insertar Diseño Formato Referencias Corresponde Revisar Vista Complemen PDF PDF Architec
DATOS ANÁLISIS DE LA INFORMACIÓN
Página 3 de 4
343 palabras
Español (España)

THE STRUCTURE OF A BOTNET

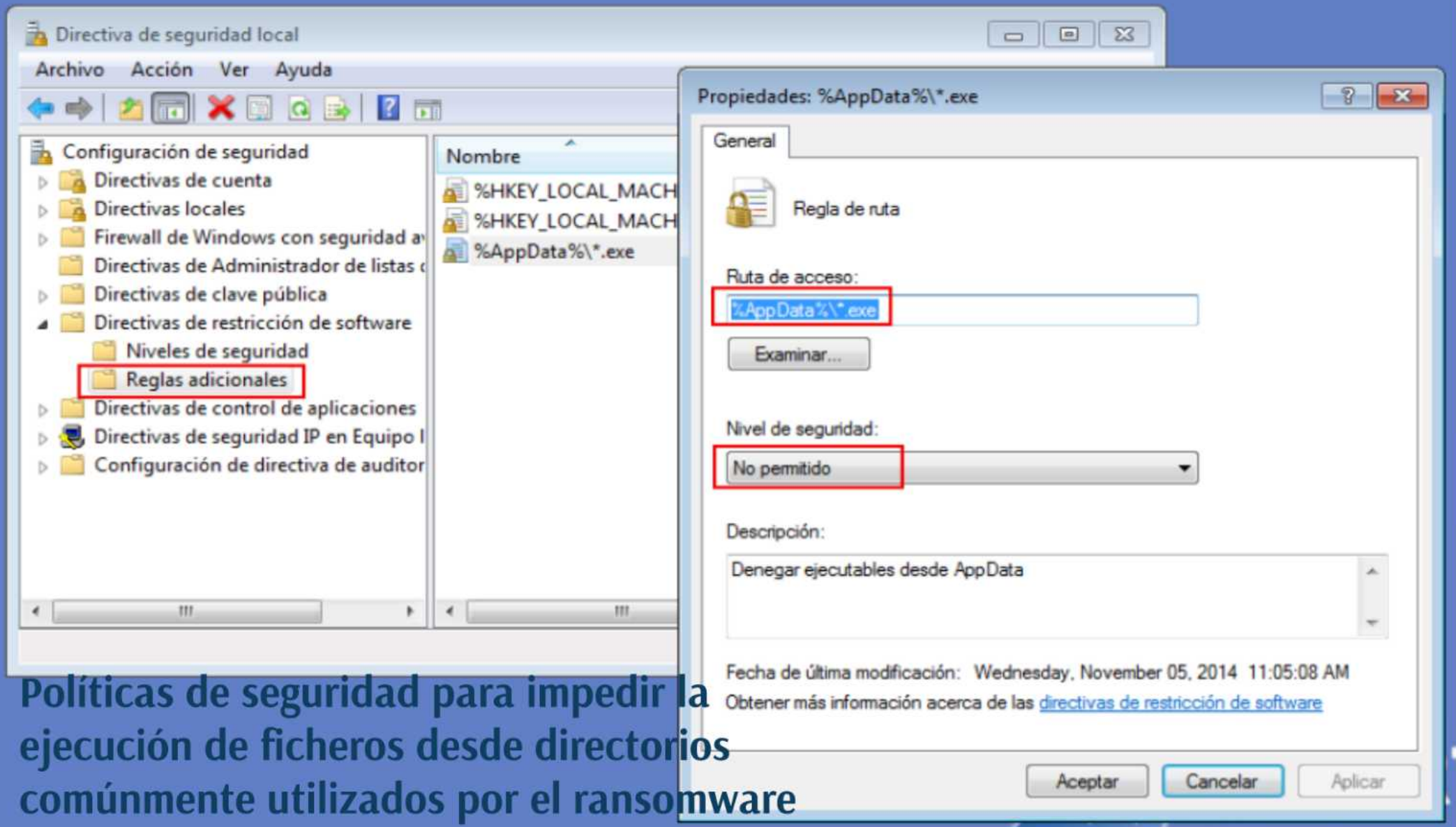


Bloquear el tráfico a dominios y servidores C2 mediante IDS/IPS

Las autoridades en colaboración con equipos de seguridad han incautado este servidor malicioso, pero es necesario que los dispositivos que controla sean desinfectados, en caso contrario los cibercriminales podrían reactivar la botnet desde otro punto. Para ello informan a las entidades competentes sobre las miles de direcciones IP públicas que se están conectando al servidor malicioso en tiempo real.

El Servicio Antibotnet chequea tu dirección IP pública contra nuestra base de datos de direcciones IP para saber si desde tu red hay alguna conexión con el servidor malicioso que controla la botnet, pero no accedemos ni podemos saber cuál de tus dispositivos es el afectado. En ningún caso monitorizamos el tráfico de tu red, ni accedemos a datos en tu ordenador.

https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antibotnet



Políticas de seguridad para impedir la ejecución de ficheros desde directorios comúnmente utilizados por el ransomware

https://www.foolishit.com/cryptoprevent-malware-prevention/v8-teaser/

Firefox | Inves | Logins | Enlaces | Traductor | DFIR | Tecno | Legal | Soft | Publicar | Cursos | Info | eCommerce | Ataqu

d7II: PC Tech Productivity Software | CryptoPrevent: Malware Prevention | Other Software | News & Info | Store

The public beta is available for testing HERE.

¿Qué debo hacer ante un ataque?


NO TOCAR
Actuar según el Plan de actuación o contactar con un experto

PREPARACIÓN PLAN RESPUESTA A INCIDENTES

1) Quién realiza la gestión de los incidentes

2) Dónde está la documentación sobre la tecnología y Sistemas de Información.

3) Con quién se ha de contactar en caso de incidencia

4) Clasificación del incidente

5) Escalación del incidente a experto en caso de que sea necesario


NO PAGAR
Favorece el crimen y no te asegura librarte de la amenaza

GOBIERNO DE ESPAÑA

CUERPO NACIONAL DE POLICÍA

BRIGADA DE INVESTIGACIÓN TECNOLÓGICA

NO CREER

Atención!

Fue detectado un caso de actividad ilegal. El sistema operativo fue bloqueado por violación de las leyes de España! Fue detectada la siguiente infracción:

Desde su dirección IP bajo el número "[redacted]" fue efectuado un acceso a páginas de internet que contienen pornografía, pornografía infantil, zoofilia, asimismo como violencia sobre los menores. En su ordenador asimismo fueron encontrados archivos de vídeo que contienen pornografía, elementos de violencia y pornografía infantil. Desde el correo electrónico asimismo se realizaba envío de spam con subtexto de terrorismo. El bloqueo del ordenador se realiza para suprimir la posibilidad de acciones ilegales por su parte.

Your details: IP:[redacted] Location: [redacted] ISP: [redacted]

Para quitar el bloqueo del ordenador, usted debe pagar una multa de 100 euro.

Realizar el pago a través de Ukash:

Para ello, por favor introduzca el código recibido (en caso de necesidad junto con la contraseña) en la línea del pago, y posteriormente pulse OK (si usted tiene varios códigos, introdúzcalos uno detrás de otro, y después pulse OK).

Si el sistema le genera un error, usted deberá enviar el código al correo electrónico deposito@cyber-police.net.

Ukash Donde conseguir Ukash?

Puedes adquirir Ukash en cientos de miles de establecimientos en todo el mundo, en línea, a partir de carteras, en quioscos y cajeros. A continuación encontrarás dónde puedes adquirir Ukash en tu país.

cajamar — **Cajamar** - A partir de ahora esta disponible Ukash en todos los cajeros de Cajamar.

CAIXAGALICIA — **Caixa Galicia** - A partir de ahora Ukash esta disponible en todos los cajeros de Caixa Galicia.

Telefónica — **Telefonica** - Ahora, Ukash esta disponible en las 80.000 cabinas de Telefonica.

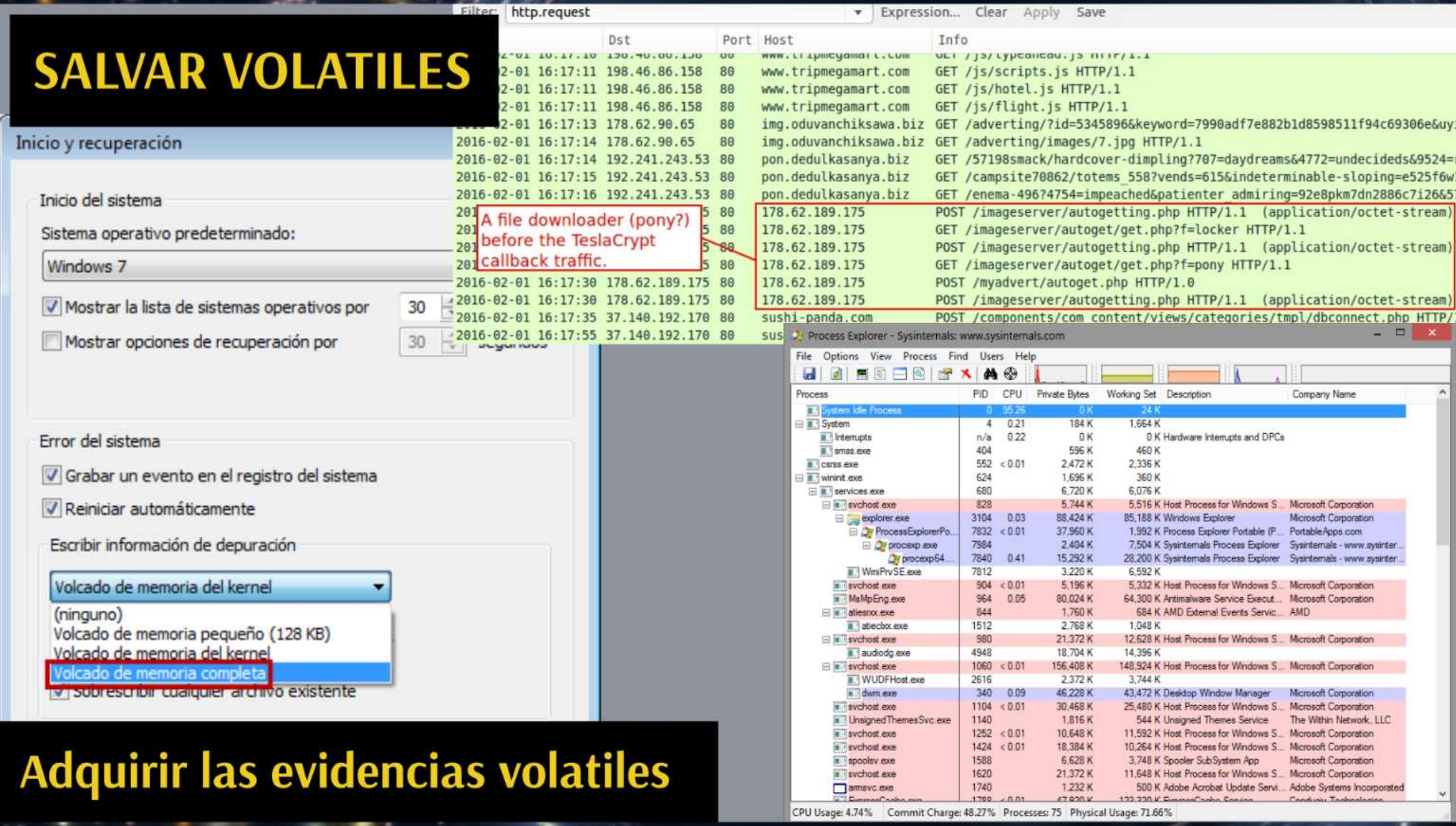
Cuponesprepago - Consiga tu Ukash online a traves de su Internet Bank o utilizando tu tarjeta de credito.

epoy · CORREOS · TELECOR · canalrecargas · MundiRecargas · REPSOL

OK

El mensaje tiene un componente de Ingeniería Social

SALVAR VOLATILES



Adquirir las evidencias volatiles


CLONAR
TABLEAU
Forensic Duplicator
Hacer una copia forensic de los almacenamiento de los equipos


ANÁLISIS FORENSE
Press ALT+F1 for Verbose Mode
Now loading
The most advanced operating system
in the world.
Habrá que encargar un análisis forense para tener respuestas

¿Cómo se ha introducido? Vector de infección

¿Cuál es el paciente cero? Primer equipo

¿Cómo ha superado las medidas de seguridad? Exploit utilizado

¿Qué hace el malware en el equipo?

¿Cómo se propaga?

¿Cómo secuestra el equipo?

¿Qué tipo de cifrado se utiliza?

¿Qué documentos afecta?

¿Cómo se comunican los extorsionadores?

¿Cómo se ofusca?

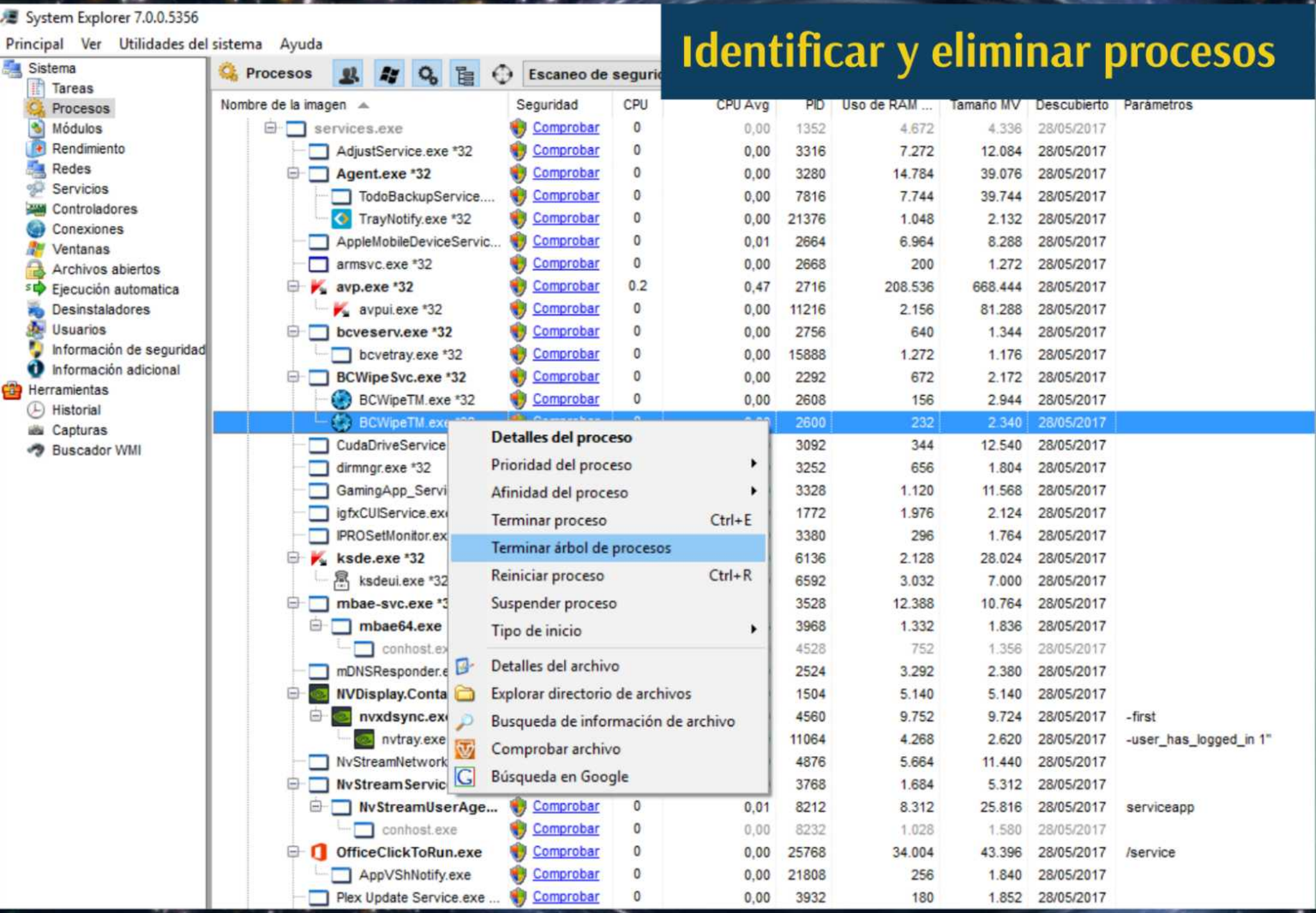
¿Cómo evade la ingeniería inversa del malware?

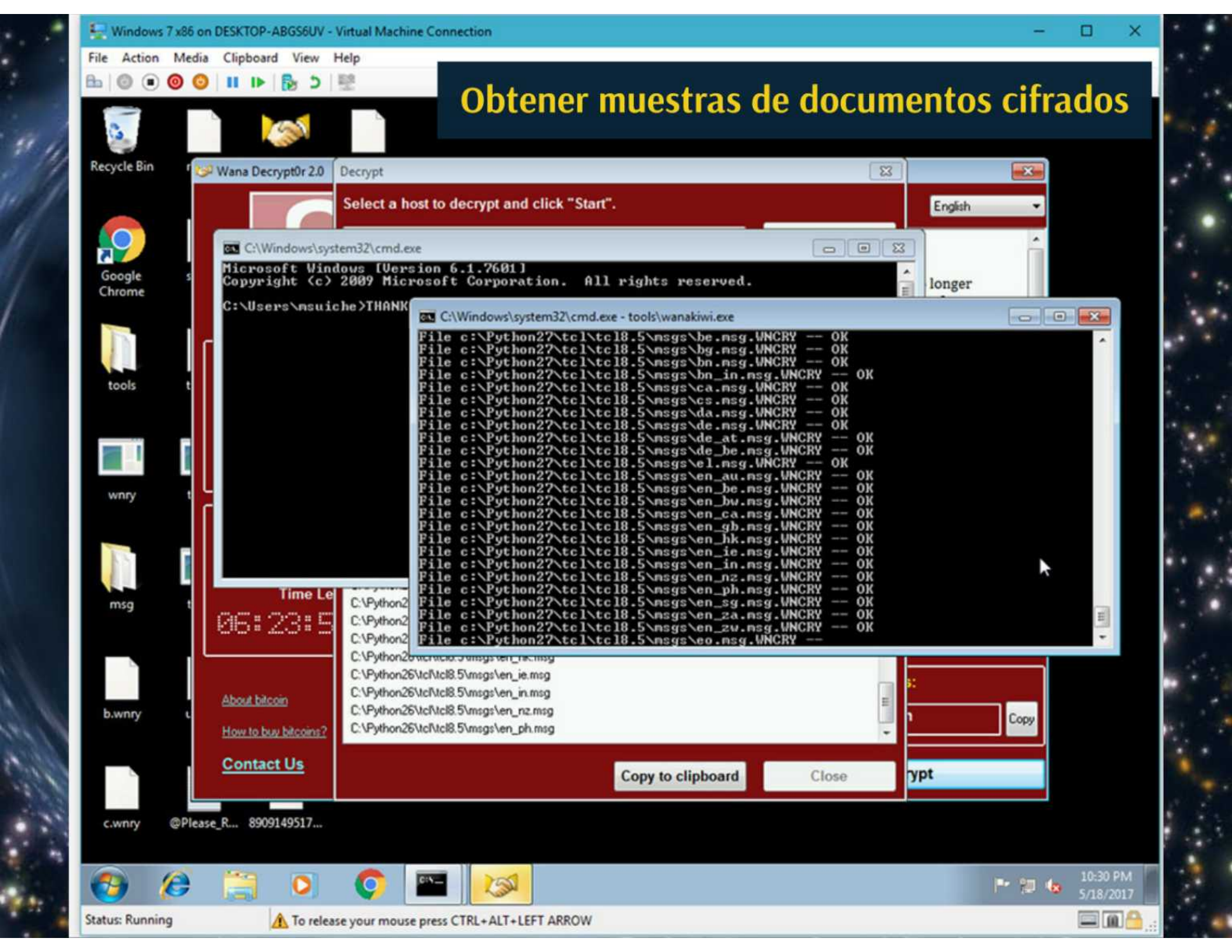
¿Cómo se controla a distancia?

CONTENER, LIMPIAR y RECUPERAR

Eliminar el malware de los equipos comprometidos

Identificar y eliminar procesos




Windows 7 x86 on DESKTOP-ABGS6UV - Virtual Machine Connection
File Action Media Clipboard View Help
Obtener muestras de documentos cifrados
Recycle Bin
Google Chrome
tools
wnry
msg
b.wnry
c.wnry
@Please_R...
8909149517...
Wana Decrypt0r 2.0
Decrypt
Select a host to decrypt and click "Start".
English
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\msuiche>THANK
longer
C:\Windows\system32\cmd.exe - tools\wanakiwi.exe
File c:\Python27\tcl\tcl8.5\msgs\be.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\bg.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\bn.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\bn_in.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\ca.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\cs.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\da.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\de.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\de_at.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\de_be.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\el.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_au.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_be.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_bw.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_ca.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_gb.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_hk.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_ie.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_in.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_nz.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_ph.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_sg.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_za.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_zw.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\eo.msg.WNCRY --
Time Le
About bitcoin
How to buy bitcoins?
Contact Us
C:\Python26\tcl\tcl8.5\msgs\en_ie.msg
C:\Python26\tcl\tcl8.5\msgs\en_in.msg
C:\Python26\tcl\tcl8.5\msgs\en_nz.msg
C:\Python26\tcl\tcl8.5\msgs\en_ph.msg
Copy to clipboard
Close
Copy
10:30 PM
5/18/2017
Status: Running
To release your mouse press CTRL+ALT+LEFT ARROW

Obtener muestras del malware

- Puede que te soliciten una cifra mayor una vez hayas pagado.
- Pagar **fomenta el negocio de los ciberdelincuentes**.

¿Qué tengo que hacer?

Contacta con nuestro centro de respuesta a incidentes, CERTSI. Te ayudaremos a mitigar los efectos del incidente y te indicaremos cómo actuar. Disponemos de un servicio de análisis y descifrado de ficheros afectados por **algunos tipos de ransomware en determinadas condiciones**.

- Para poder identificar el tipo de ransomware y si los datos son recuperables, puedes utilizar la dirección de correo incidencias@certsi.es
- Para reportar un incidente adjunta:
  - **dos o tres ficheros cifrados** con extensión original .doc o .xls y un tamaño superior a 1 MB
  - **el fichero en el que se indica cómo realizar el pago** para recuperar la información, normalmente es un fichero .txt o .html.

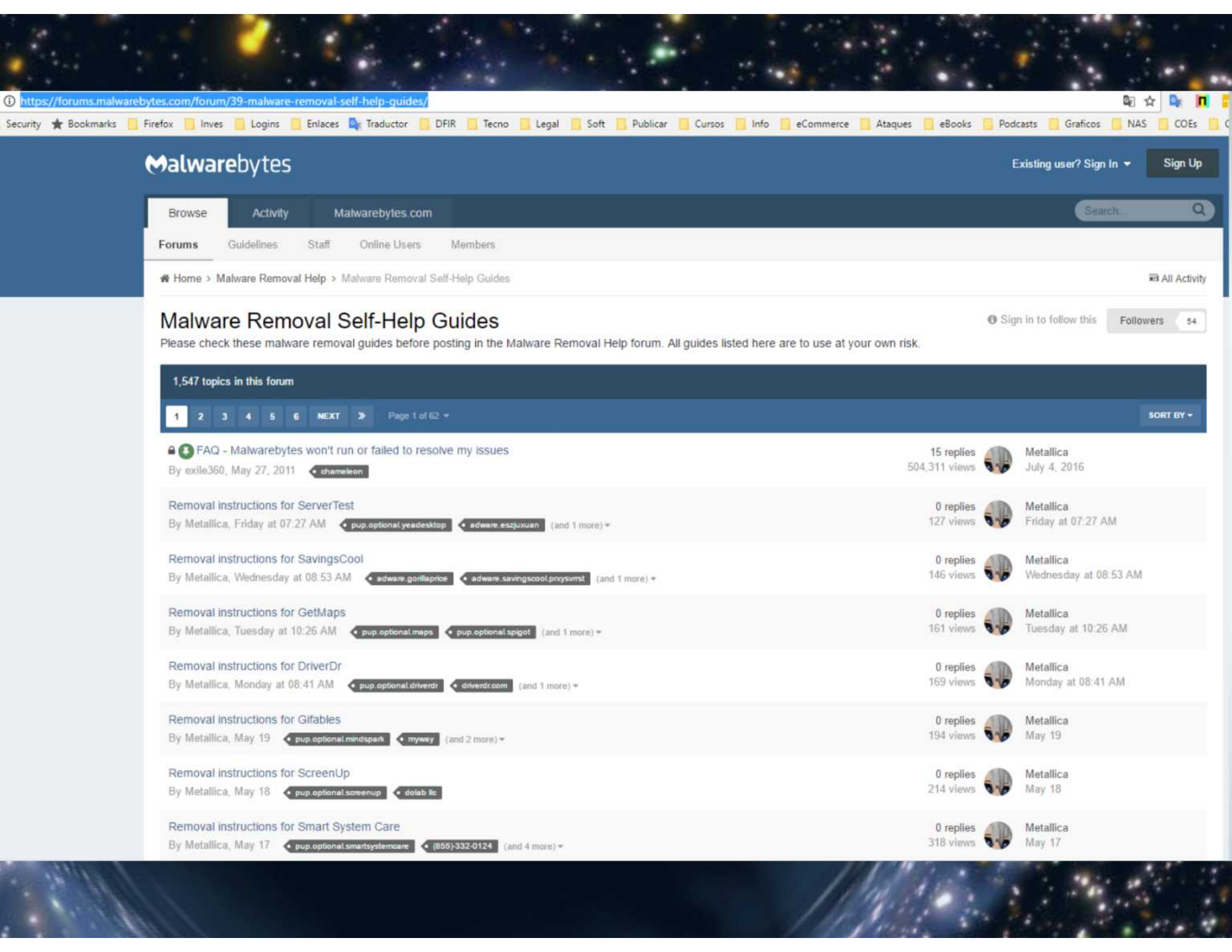
De esta manera podremos darte una repuesta mucho más ágil. Si desconoces como hacerlo, no te preocupes, podemos darte algunas pautas.

Debido a que la prestación de este servicio de análisis y descifrado se realiza en colaboración con una entidad externa a INCIBE, y a pesar de tener acuerdo de confidencialidad con la misma, es recomendable que los ficheros que nos envíe no contengan información privada o confidencial, ya que serán compartidos con la citada entidad para su análisis.

También puedes denunciar el incidente para que se investigue el origen del delito así también podrás colaborar a que se pueda mitigar este ataque a otras empresas y capturar al ciberdelincuente:

- Guardia civil – Grupo de delitos telemáticos
- Policía nacional – Brigada de Investigación Tecnológica (BIT)

Reemplazar las máquinas sería la opción más recomendable, reiniciarlas en segundo lugar y, como última alternativa, limpiarlas


https://forums.malwarebytes.com/forum/39-malware-removal-self-help-guides/
Security Bookmarks Firefox Inves Logins Enlaces Traductor DFIR Tecno Legal Soft Publicar Cursos Info eCommerce Ataques eBooks Podcasts Graficos NAS COEs
Malwarebytes
Existing user? Sign In
Sign Up
Browse
Activity
Malwarebytes.com
Search...
Forums
Guidelines
Staff
Online Users
Members
Home > Malware Removal Help > Malware Removal Self-Help Guides
All Activity
Malware Removal Self-Help Guides
Please check these malware removal guides before posting in the Malware Removal Help forum. All guides listed here are to use at your own risk.
Sign in to follow this
Followers 54
1,547 topics in this forum
1 2 3 4 5 6 NEXT
Page 1 of 62
SORT BY
FAQ - Malwarebytes won't run or failed to resolve my issues
By exile360, May 27, 2011
chameleon
15 replies
504,311 views
Metallica
July 4, 2016
Removal instructions for ServerTest
By Metallica, Friday at 07:27 AM
pup.optional.yeadesktop
adware.eszjuxuan
(and 1 more)
0 replies
127 views
Metallica
Friday at 07:27 AM
Removal instructions for SavingsCool
By Metallica, Wednesday at 08:53 AM
adware.gorillaprice
adware.savingscool.proxysvmst
(and 1 more)
0 replies
146 views
Metallica
Wednesday at 08:53 AM
Removal instructions for GetMaps
By Metallica, Tuesday at 10:26 AM
pup.optional.maps
pup.optional.spigot
(and 1 more)
0 replies
161 views
Metallica
Tuesday at 10:26 AM
Removal instructions for DriverDr
By Metallica, Monday at 08:41 AM
pup.optional.driverdr
driverdr.com
(and 1 more)
0 replies
169 views
Metallica
Monday at 08:41 AM
Removal instructions for Gifables
By Metallica, May 19
pup.optional.mindspark
myway
(and 2 more)
0 replies
194 views
Metallica
May 19
Removal instructions for ScreenUp
By Metallica, May 18
pup.optional.screenup
dolab llc
0 replies
214 views
Metallica
May 18
Removal instructions for Smart System Care
By Metallica, May 17
pup.optional.smartsystemcare
(855)-332-0124
(and 4 more)
0 replies
318 views
Metallica
May 17

https://www.bleepingcomputer.com/virus-removal/

Security Bookmarks Firefox Inves Logins Enlaces Traductor DFIR Tecno Legal Soft Publicar Cursos Info eCommerce Ataques eBooks Podcasts Graficos NAS COE

BLEEPINGCOMPUTER

Search Site LOGIN SIGN UP

NEWS DOWNLOADS VIRUS REMOVAL GUIDES TUTORIALS DEALS FORUMS MORE

Home › Virus, Spyware, Malware, & PUP Removal Guides

REMOVAL GUIDES

Sort By : Date Added

1 2 3 4 5 › »

Remove the MyLuckySurfing.com Home Page

MyLuckySurfing.com is a potentially unwanted program that changes the home page of your installed browsers. When this program is installed, it will change the browser's settings so that they automatically open the myluckysurfing.com as their home page and use it for searches. This causes your browser to automatically open myluckysurfing.com when the browser opens. Furthermore, when a user searches from the address bar, it wil...

LAWRENCE ABRAMS • LAST MODIFIED ON MAY 22, 2017

Remove the 3Spiral Wave Tab - New Tab Chrome Extension

3Spiral Wave Tab - New Tab is a Google Chrome extension that changes the page shown when you click on the New Tab button in Google Chrome. The new tab page that is displayed will have an address of chrome-extension://ilcfbbdpbjdjnkanagkbdbmcblhfmkmg/newtab.html and will contain a search form that displays results from Google, your weather, and a variety of links to various sites....

LAWRENCE ABRAMS • LAST MODIFIED ON MAY 22, 2017

SEARCH GUIDES

Search

LATEST GUIDES

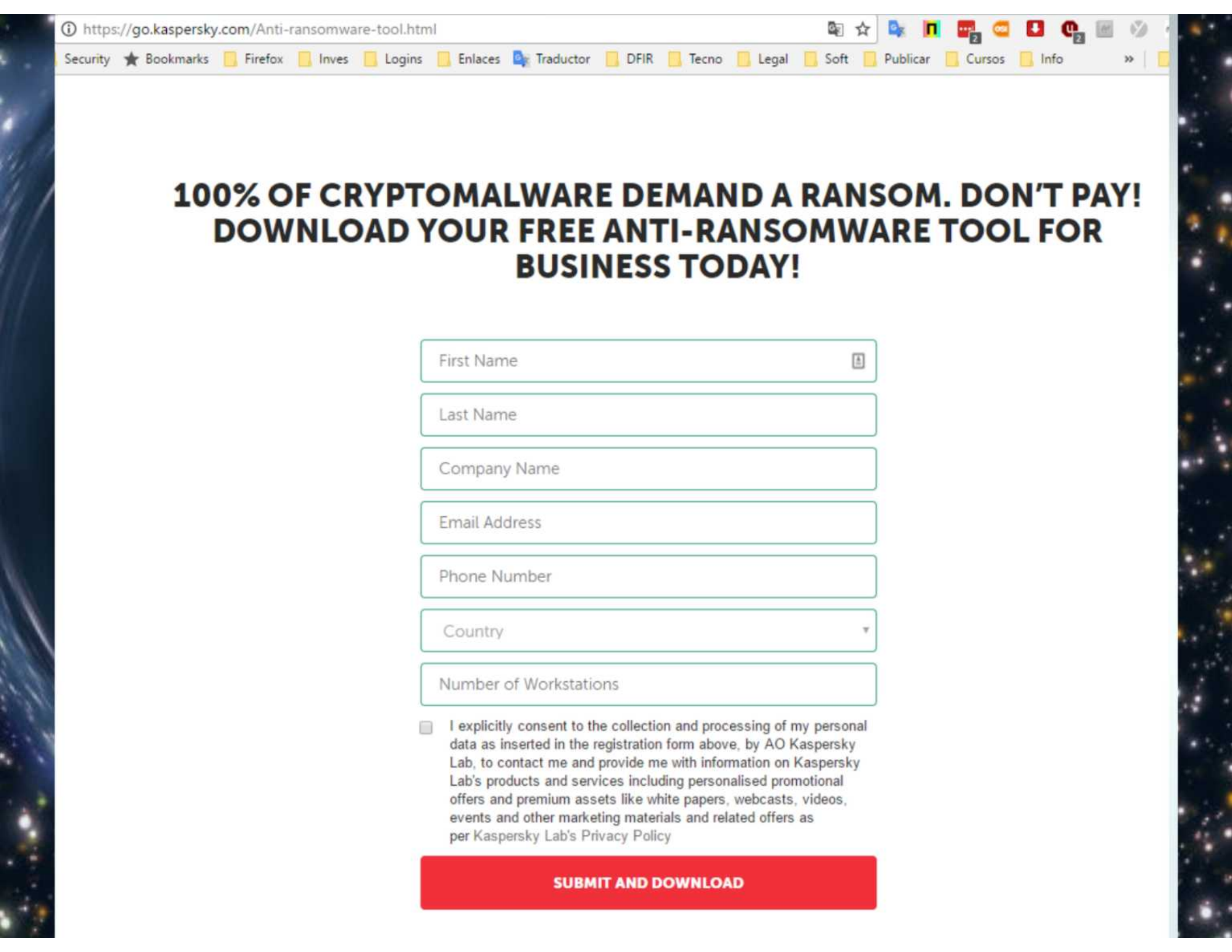
- MyLuckySurfing.com
- 3Spiral Wave Tab - New Tab Extension
- Adylkuzz, msiexev.exe, & wuauser.exe Miner
- Browser Health Info Chrome Extension
- MyLuckySearching.com
- System Health Checker Chrome Extension
- Smart System Care

Ransomware

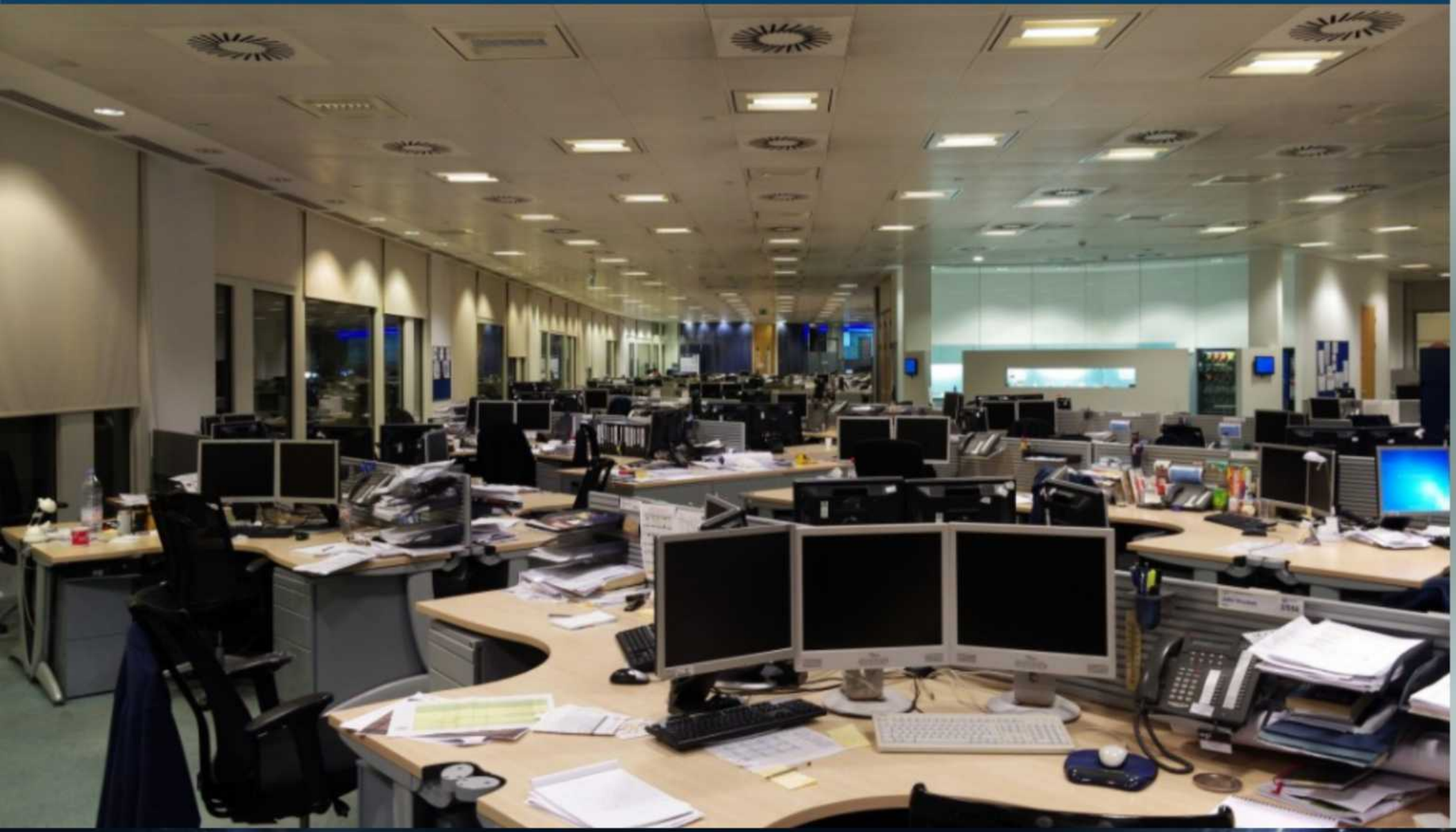
How to remove Mordor ransowmare (Virus Removal Guide)

BY STELIAN PILICI ON MAY 17, 2017

Mordor is a file-encrypting ransomware, which will encrypt the personal documents found on victim's computer using RSA-2048 key (AES CBC 256-bit encryption algorithm), appending the .mordor extension to encrypted files. The Mordor ransomware then displays a message which offers to decrypt the data if a payment of $100, or approximately 0.07 Bitcoins is made. We [...]


https://go.kaspersky.com/Anti-ransomware-tool.html
Security
Bookmarks
Firefox
Inves
Logins
Enlaces
Traductor
DFIR
Tecno
Legal
Soft
Publicar
Cursos
Info
100% OF CRYPTOMALWARE DEMAND A RANSOM. DON'T PAY!
DOWNLOAD YOUR FREE ANTI-RANSOMWARE TOOL FOR BUSINESS TODAY!
First Name
Last Name
Company Name
Email Address
Phone Number
Country
Number of Workstations
I explicitly consent to the collection and processing of my personal data as inserted in the registration form above, by AO Kaspersky Lab, to contact me and provide me with information on Kaspersky Lab's products and services including personalised promotional offers and premium assets like white papers, webcasts, videos, events and other marketing materials and related offers as per Kaspersky Lab's Privacy Policy
SUBMIT AND DOWNLOAD

Actuar en todos los equipos, no solo los que presentan síntomas



Restaurar desde una copia de seguridad limpia

Microsoft

Buscar en

Office Productos Plantillas **Soporte**

Aplicaciones Instalar Cuenta Aprendizaje Administración

Para documentos de Microsoft Office estos pueden estar salvaguardados en OneDrive donde podemos encontrar el historial de versiones

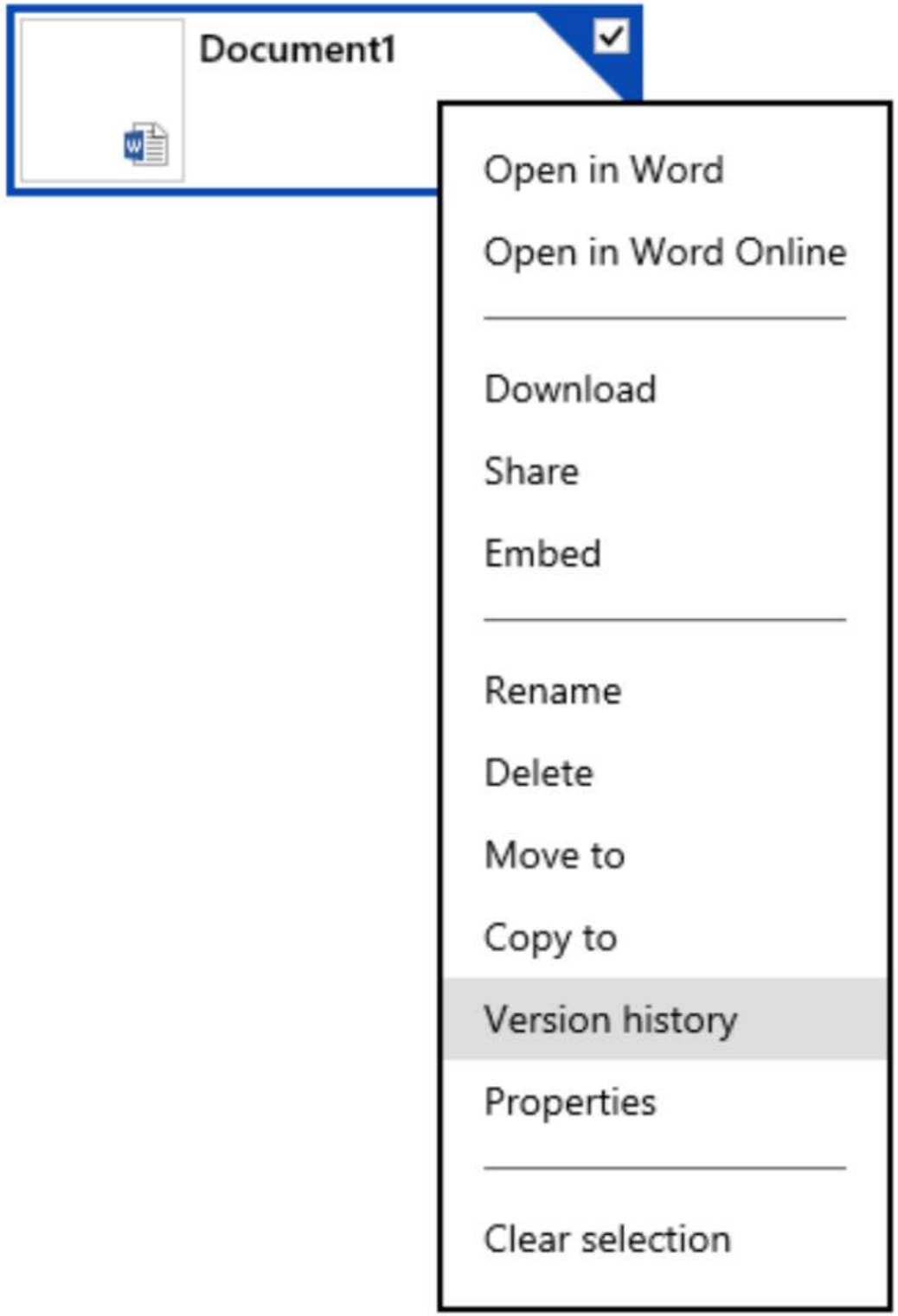
Seguridad de archivos de OneDrive

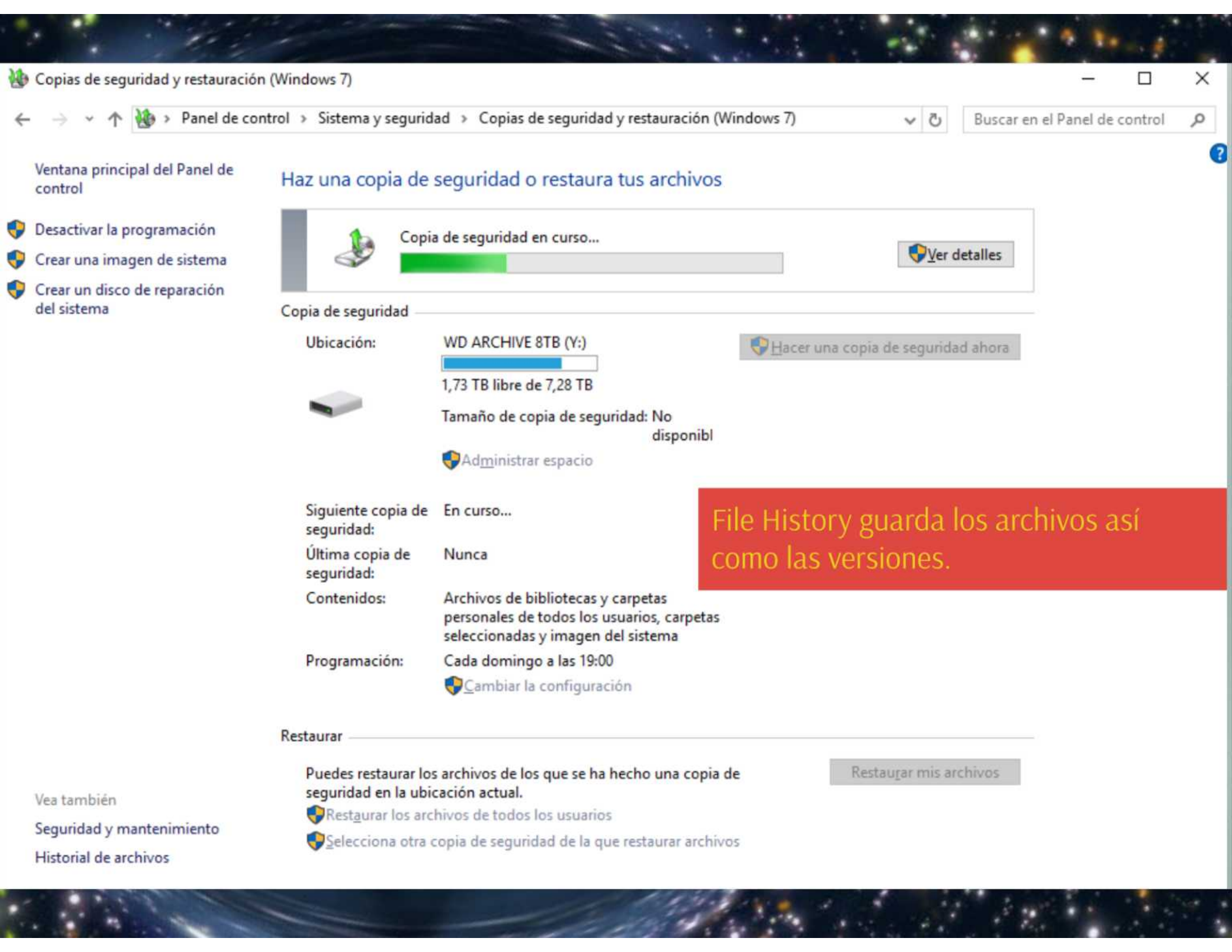
Se aplica a: OneDrive

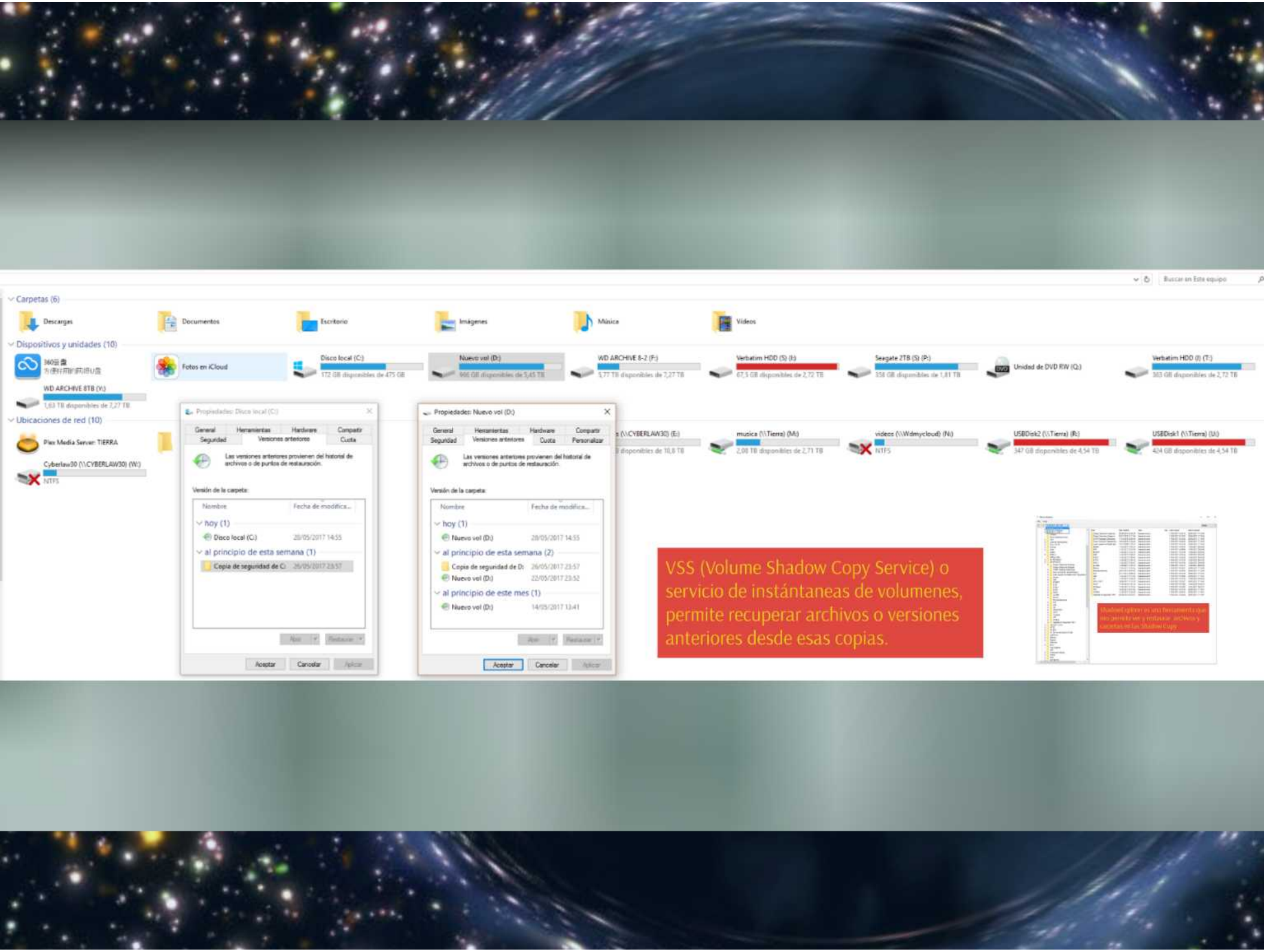
IMPORTANTE: Este artículo se ha traducido con traducción automática; vea la declinación de responsabilidades. Para su referencia, puede encontrar la versión en inglés de este artículo aquí.

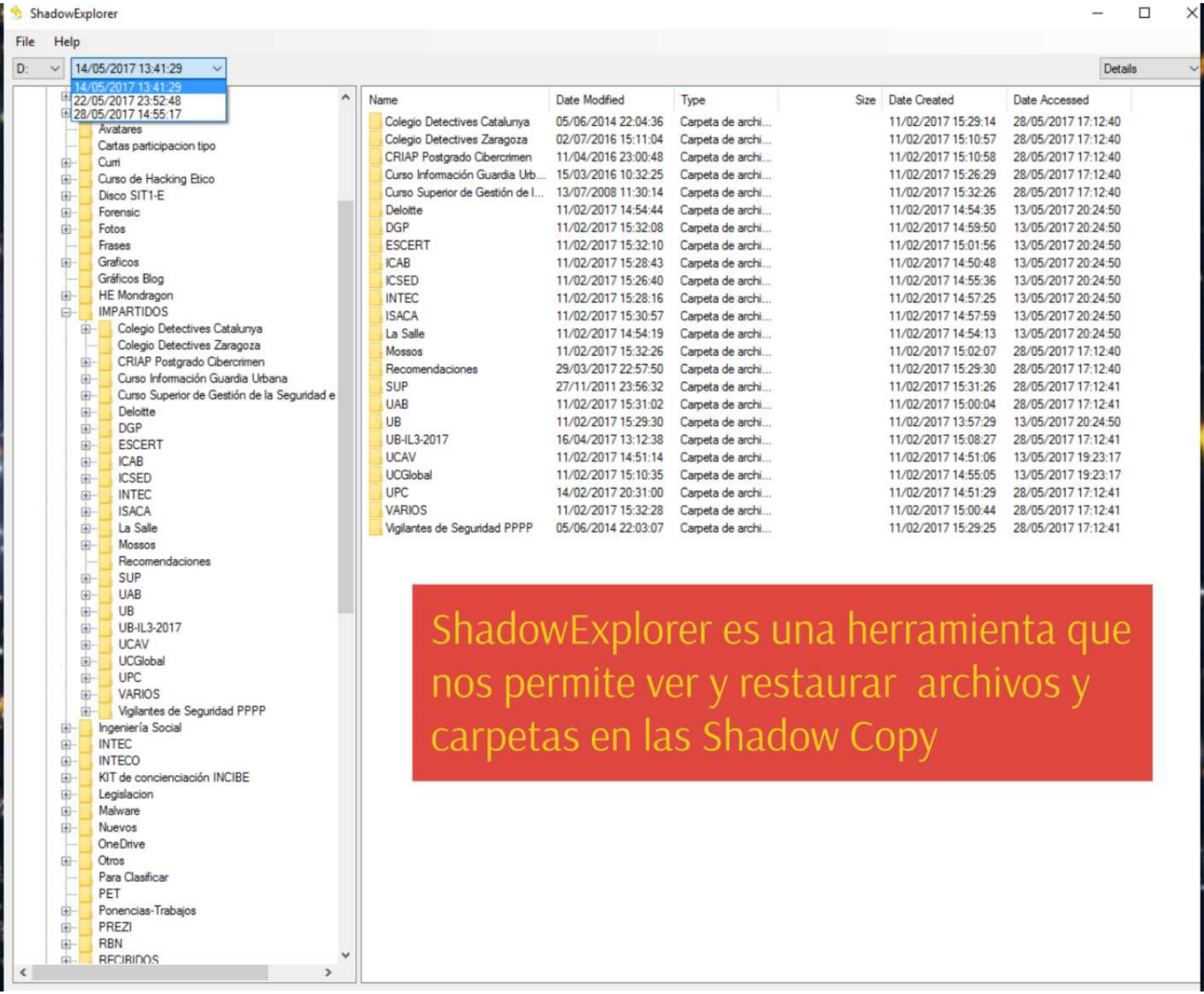
Hay varias maneras que tratamos de proteger los archivos en OneDrive. No se comparten los archivos con otras personas a menos que guarde en la carpeta pública o elija compartirlos. Para ayudar a proteger los archivos de OneDrive de error de hardware, se guardan varias copias de cada archivo en servidores y unidades diferentes.

A continuación se incluyen algunas otras cosas que puedes hacer para proteger tus archivos en OneDrive:


Document1
Open in Word
Open in Word Online
Download
Share
Embed
Rename
Delete
Move to
Copy to
Version history
Properties
Clear selection


Copias de seguridad y restauración (Windows 7)
Panel de control › Sistema y seguridad › Copias de seguridad y restauración (Windows 7)
Buscar en el Panel de control
Ventana principal del Panel de control
Desactivar la programación
Crear una imagen de sistema
Crear un disco de reparación del sistema
Haz una copia de seguridad o restaura tus archivos
Copia de seguridad en curso...
Ver detalles
Copia de seguridad
Ubicación:
WD ARCHIVE 8TB (Y:)
1,73 TB libre de 7,28 TB
Tamaño de copia de seguridad: No disponibl
Administrar espacio
Hacer una copia de seguridad ahora
Siguiente copia de seguridad:
En curso...
Última copia de seguridad:
Nunca
Contenidos:
Archivos de bibliotecas y carpetas personales de todos los usuarios, carpetas seleccionadas y imagen del sistema
Programación:
Cada domingo a las 19:00
Cambiar la configuración
File History guarda los archivos así como las versiones.
Restaurar
Puedes restaurar los archivos de los que se ha hecho una copia de seguridad en la ubicación actual.
Restaurar los archivos de todos los usuarios
Selecciona otra copia de seguridad de la que restaurar archivos
Restaurar mis archivos
Vea también
Seguridad y mantenimiento
Historial de archivos


Carpetas (6)
Descargas
Documentos
Escritorio
Imágenes
Música
Vídeos
Dispositivos y unidades (10)
Fotos en iCloud
Disco local (C:)
Nuevo vol (D:)
WD ARCHIVE 8-2 (F:)
Verbatim HDD (S) (I:)
Seagate 2TB (S) (P:)
Unidad de DVD RW (Q:)
Verbatim HDD (J) (T:)
WD ARCHIVE 8TB (V:)
Ubicaciones de red (10)
Plex Media Server: TIERRA
Cyberlaw30 (\\CYBERLAW30) (W:)
musica (\\Tierra) (M:)
videos (\\Wdmycloud) (N:)
USBDisk2 (\\Tierra) (R:)
USBDisk1 (\\Tierra) (U:)
Propiedades: Disco local (C:)
Propiedades: Nuevo vol (D:)
General
Seguridad
Versiones anteriores
Hardware
Compartir
Cuota
Personalizar
Las versiones anteriores provienen del historial de archivos o de puntos de restauración.
Versión de la carpeta:
Nombre
Fecha de modifica...
hoy (1)
Disco local (C:)
28/05/2017 14:55
al principio de esta semana (1)
Copia de seguridad de C:
26/05/2017 23:57
al principio de esta semana (2)
Copia de seguridad de D:
Nuevo vol (D:)
22/05/2017 23:52
al principio de este mes (1)
14/05/2017 13:41
Abrir
Restaurar
Aceptar
Cancelar
Aplicar
VSS (Volume Shadow Copy Service) o servicio de instántaneas de volumenes, permite recuperar archivos o versiones anteriores desde esas copias.


ShadowExplorer
File
Help
D:
14/05/2017 13:41:29
14/05/2017 13:41:29
22/05/2017 23:52:48
28/05/2017 14:55:17
Details
Avatares
Cartas participacion tipo
Curri
Curso de Hacking Etico
Disco SIT1-E
Forensic
Fotos
Frases
Graficos
Gráficos Blog
HE Mondragon
IMPARTIDOS
Colegio Detectives Catalunya
Colegio Detectives Zaragoza
CRIAP Postgrado Cibercrimen
Curso Información Guardia Urbana
Curso Superior de Gestión de la Seguridad e
Deloitte
DGP
ESCERT
ICAB
ICSED
INTEC
ISACA
La Salle
Mossos
Recomendaciones
SUP
UAB
UB
UB-IL3-2017
UCAV
UCGlobal
UPC
VARIOS
Vigilantes de Seguridad PPPP
Ingeniería Social
INTEC
INTECO
KIT de concienciación INCIBE
Legislacion
Malware
Nuevos
OneDrive
Otros
Para Clasificar
PET
Ponencias-Trabajos
PREZI
RBN
RECIBIDOS
Name
Date Modified
Type
Size
Date Created
Date Accessed
Colegio Detectives Catalunya 05/06/2014 22:04:36 Carpeta de archi... 11/02/2017 15:29:14 28/05/2017 17:12:40
Colegio Detectives Zaragoza 02/07/2016 15:11:04 Carpeta de archi... 11/02/2017 15:10:57 28/05/2017 17:12:40
CRIAP Postgrado Cibercrimen 11/04/2016 23:00:48 Carpeta de archi... 11/02/2017 15:10:58 28/05/2017 17:12:40
Curso Información Guardia Urb... 15/03/2016 10:32:25 Carpeta de archi... 11/02/2017 15:26:29 28/05/2017 17:12:40
Curso Superior de Gestión de l... 13/07/2008 11:30:14 Carpeta de archi... 11/02/2017 15:32:26 28/05/2017 17:12:40
Deloitte 11/02/2017 14:54:44 Carpeta de archi... 11/02/2017 14:54:35 13/05/2017 20:24:50
DGP 11/02/2017 15:32:08 Carpeta de archi... 11/02/2017 14:59:50 13/05/2017 20:24:50
ESCERT 11/02/2017 15:32:10 Carpeta de archi... 11/02/2017 15:01:56 13/05/2017 20:24:50
ICAB 11/02/2017 15:28:43 Carpeta de archi... 11/02/2017 14:50:48 13/05/2017 20:24:50
ICSED 11/02/2017 15:26:40 Carpeta de archi... 11/02/2017 14:55:36 13/05/2017 20:24:50
INTEC 11/02/2017 15:28:16 Carpeta de archi... 11/02/2017 14:57:25 13/05/2017 20:24:50
ISACA 11/02/2017 15:30:57 Carpeta de archi... 11/02/2017 14:57:59 13/05/2017 20:24:50
La Salle 11/02/2017 14:54:19 Carpeta de archi... 11/02/2017 14:54:13 13/05/2017 20:24:50
Mossos 11/02/2017 15:32:26 Carpeta de archi... 11/02/2017 15:02:07 28/05/2017 17:12:40
Recomendaciones 29/03/2017 22:57:50 Carpeta de archi... 11/02/2017 15:29:30 28/05/2017 17:12:40
SUP 27/11/2011 23:56:32 Carpeta de archi... 11/02/2017 15:31:26 28/05/2017 17:12:41
UAB 11/02/2017 15:31:02 Carpeta de archi... 11/02/2017 15:00:04 28/05/2017 17:12:41
UB 11/02/2017 15:29:30 Carpeta de archi... 11/02/2017 13:57:29 13/05/2017 20:24:50
UB-IL3-2017 16/04/2017 13:12:38 Carpeta de archi... 11/02/2017 15:08:27 28/05/2017 17:12:41
UCAV 11/02/2017 14:51:14 Carpeta de archi... 11/02/2017 14:51:06 13/05/2017 19:23:17
UCGlobal 11/02/2017 15:10:35 Carpeta de archi... 11/02/2017 14:55:05 13/05/2017 19:23:17
UPC 14/02/2017 20:31:00 Carpeta de archi... 11/02/2017 14:51:29 28/05/2017 17:12:41
VARIOS 11/02/2017 15:32:28 Carpeta de archi... 11/02/2017 15:00:44 28/05/2017 17:12:41
Vigilantes de Seguridad PPPP 05/06/2014 22:03:07 Carpeta de archi... 11/02/2017 15:29:25 28/05/2017 17:12:41
ShadowExplorer es una herramienta que nos permite ver y restaurar archivos y carpetas en las Shadow Copy

COMUNICAR y DENUNCIAR

certsi_
CERT DE SEGURIDAD E INDUSTRIA

ncuesta de valoración | Mapa web

es ▾ | Sobre CERTSI ▾

Oleada de Ransomware

Consulta nuestros avisos para tener la última hora acerca de la oleada de ransomware.

Más información

Reporte de incidentes

Avisos

- Ejecución de código remota en Samba
  24/05/2017
- Múltiples vulnerabilidades en Digium Asterisk
  23/05/2017
- Múltiples vulnerabilidades en Cisco Integrated Management Controller
  23/05/2017

Ver más

Avisos SCI

- Múltiples vulnerabilidades en Allen-Bradley MicroLogix 1100 y 1400 de Rockwell Automation
  24/05/2017
- Múltiples vulnerabilidades en dispositivos OnCell de Moxa
  24/05/2017
- Salto de directorio en productos de la serie PG 85 de Miele Professional
  19/05/2017

Notificar el incidente a los CERT's y a las FFCCSE

Recomendaciones INCIBE

- Aislar todos los equipos de la red.
- Aislar la comunicación a los puertos 137 y 138 UDP y puertos 139 y 445 TCP.
- Parchear la máquina si fuera vulnerable con el parche de Microsoft MS17-010 (https://technet.microsoft.com/en-us/library/security/ms17-010.aspx)
- En el caso de que no sea posible actualizar el equipo, se recomienda deshabilitar SMBv1 desde las «Características de Windows» en el «Panel de Control».
- Bloquear las conexiones salientes a través de los puertos 137,139, 445 y para evitar que se propague.
- Actualizar el fichero de firmas del antivirus instalado y pasarlo para eliminar el malware.
- En el caso de que se tengan copias de seguridad, se deben restaurar. En el caso de que no existan se recomienda contactar con el servicio antiransomware de INCIBE.

Juan Carlos Ruiloba

CEO / CTO Scientific Intelligence Team 1, S.L.

juancrui@sit1.es

www.sit1.es

@juancrui

https://www.linkedin.com/in/juancrui/

¡Actualiza tu mente sino quieres perder esta guerra!