



Reprogramando el cerebro contra los ciberataques

2017 @juancrui



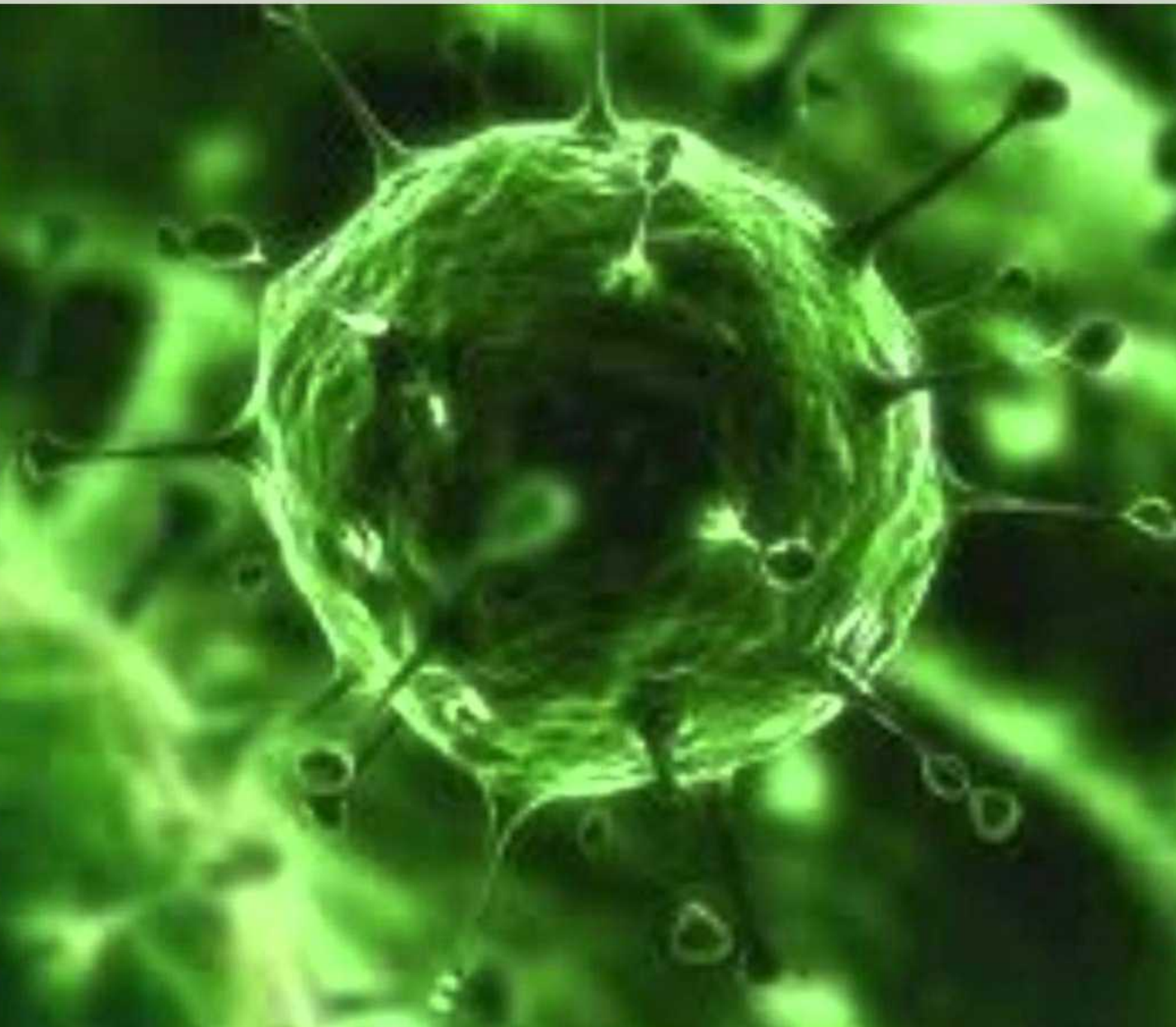
Reprogramando el cerebro contra los ciberataques

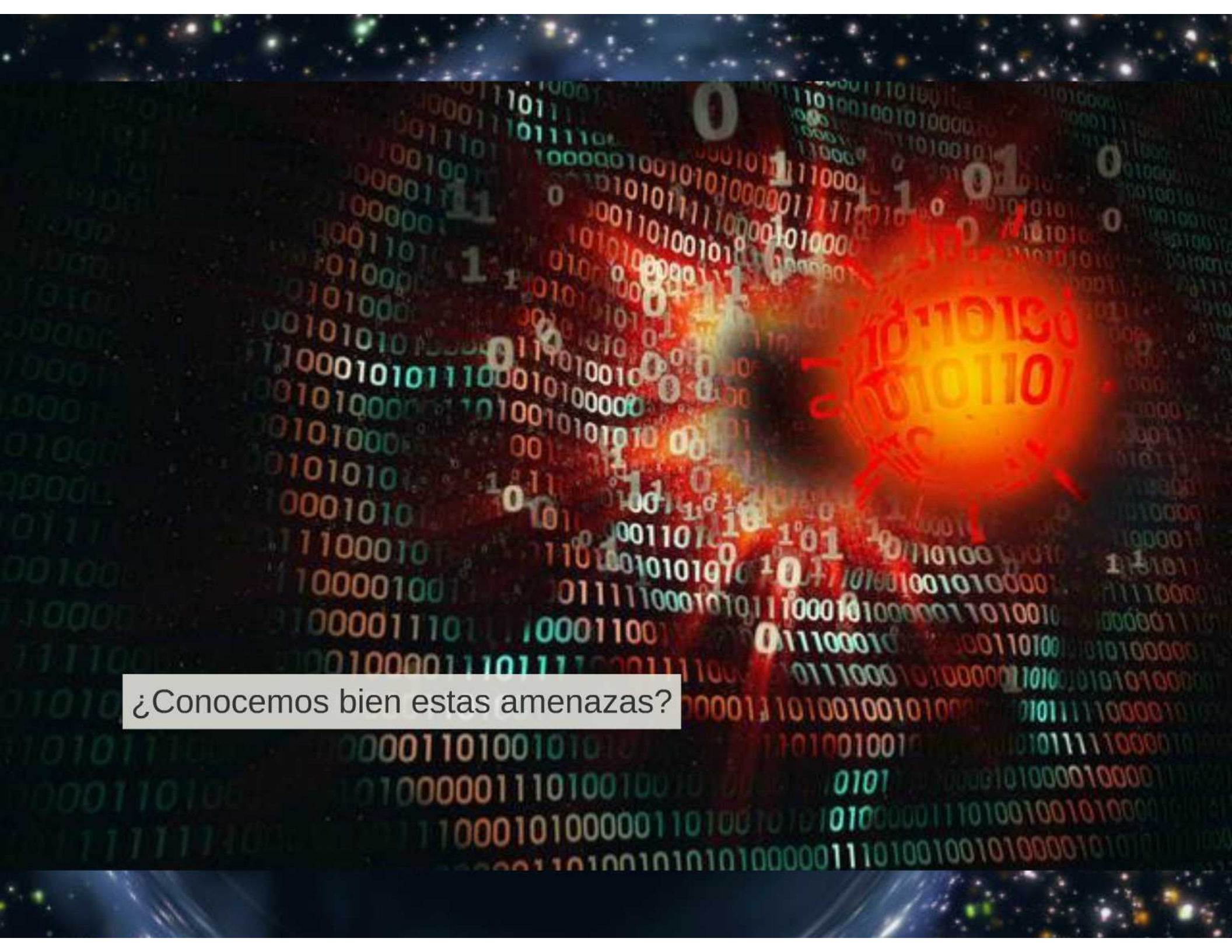
2017 @juancrui



¿Sabemos adaptarnos a la nueva realidad?

¿Sabemos defendernos a las nuevas amenazas?



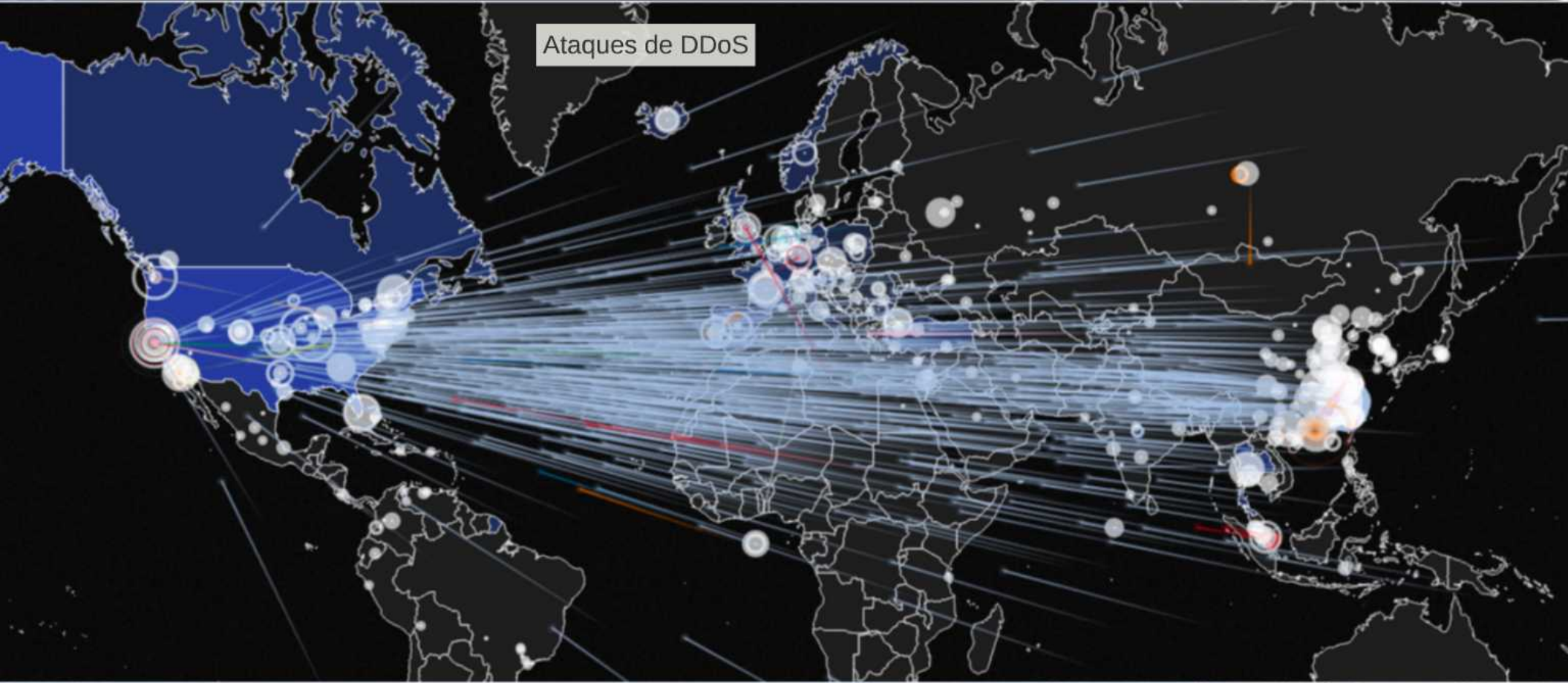


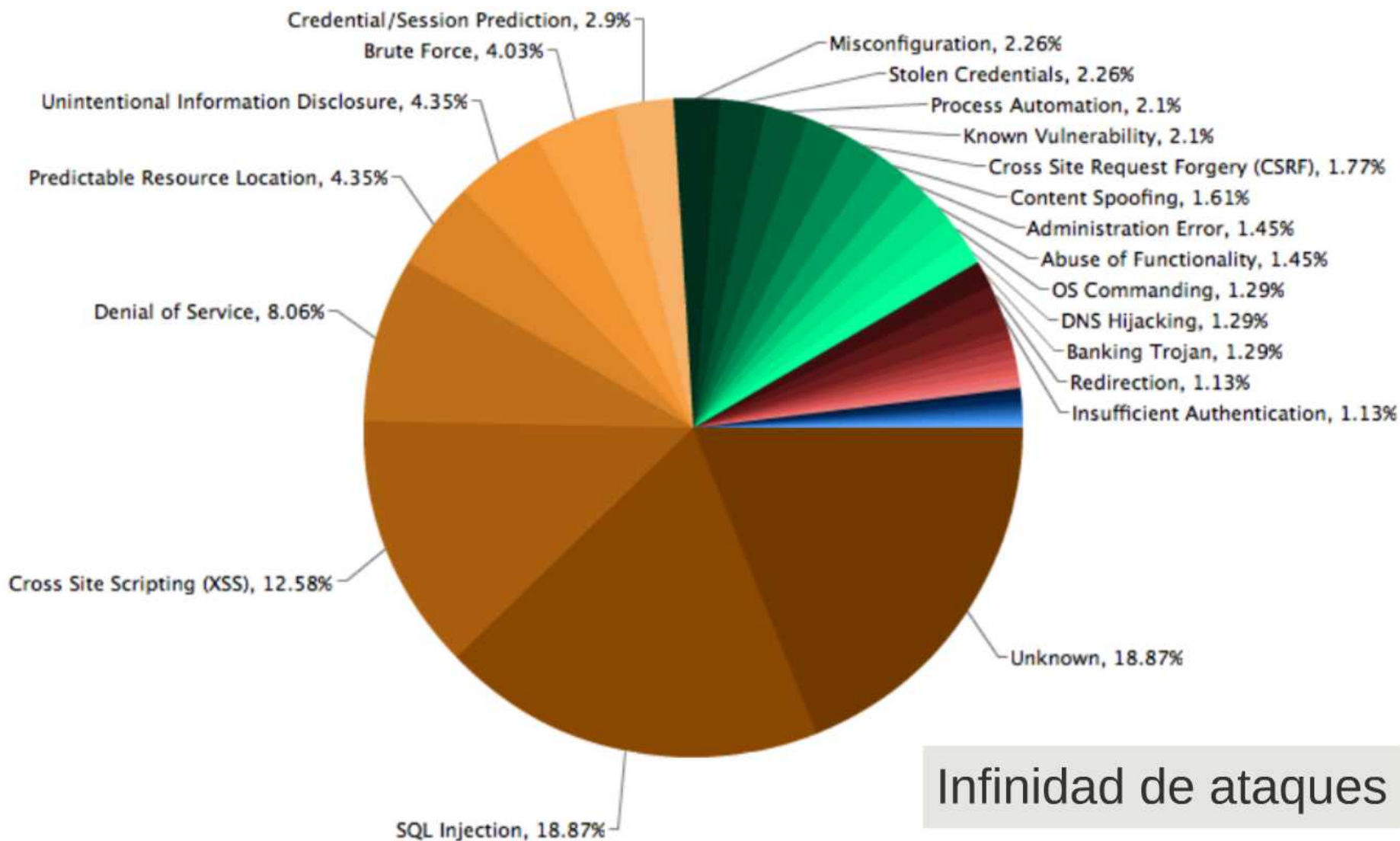
¿Conocemos bien estas amenazas?

Botnets



Ataques de DDoS





Infinidad de ataques

spyware

spam

v
i
r
u
s

a
t
t
a
c
k

p
h
i
s
h
i
n
g



data

security

malware

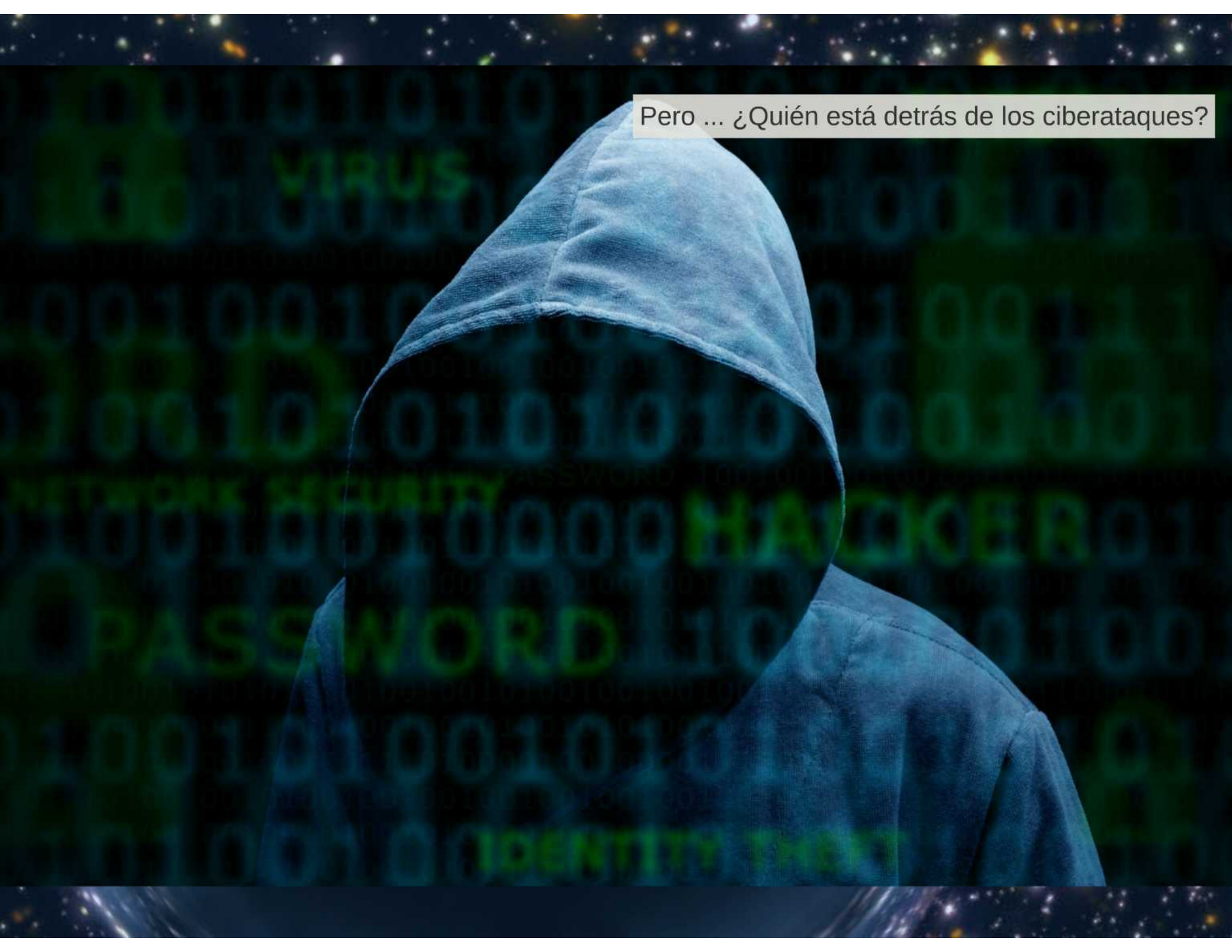
virus alert!

virus detected



t
r
o
j
a
n

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





```

0100111 00011101010010 01010 101010 10101001 10001 100101010
00010 101 1011 10011 101 101 1 1 1010100010010101010 01010100
0000101 0101 1 101 101 1010101 10 1 101001 101 1 101 10

0010100100101010 10101 101 101 1 101 10101 1010101010101 1 1
1111100000 1 101 1 1101 100111010 1 101010101010
0101010101010 101010101 11 1 111111111 00000 1

1111111110 10101010101 0101010110101 1 1010101010 1101010
01010100101 010100101010100 011010101010 101011 111 111 1
0000 11 1 1 1 101 1 1010101 101 1 1 1 1 11010101101 1 1 1 010101
0101010010101010101
0100101010

01010100101 1 1 1010 1 1 1001 1 1010101 100101010
010101001 1 10 10 10 101 101 01 01 101010100101010101 1 1 01 101

010100101 101 10 101 01 101010 1 01101 10 11 1 1 01 1 101010 11 001
0100101010 101 10 11 1 1 1 11 0101101 1 1 10101 1 101010101 0

0101010 101 1 111 1001 1 1 1 0101 1 1 1 011 11 1 1 1 010101010101
01010101010101111 1000000000000111111111 11111100000
01010 1 01 101 01 01 01 01 10 10 01 100101011 1 1 101 1 101010101
010101001010101010101010101010 1 1010 1 1 1011010 1 1010101010

```







MR. ROBOT



VIRUS

INTRUDER

CRACKER

SOFTWARE

PASSWORD

IDENTITY

CODE

UNSAFE

HACKER

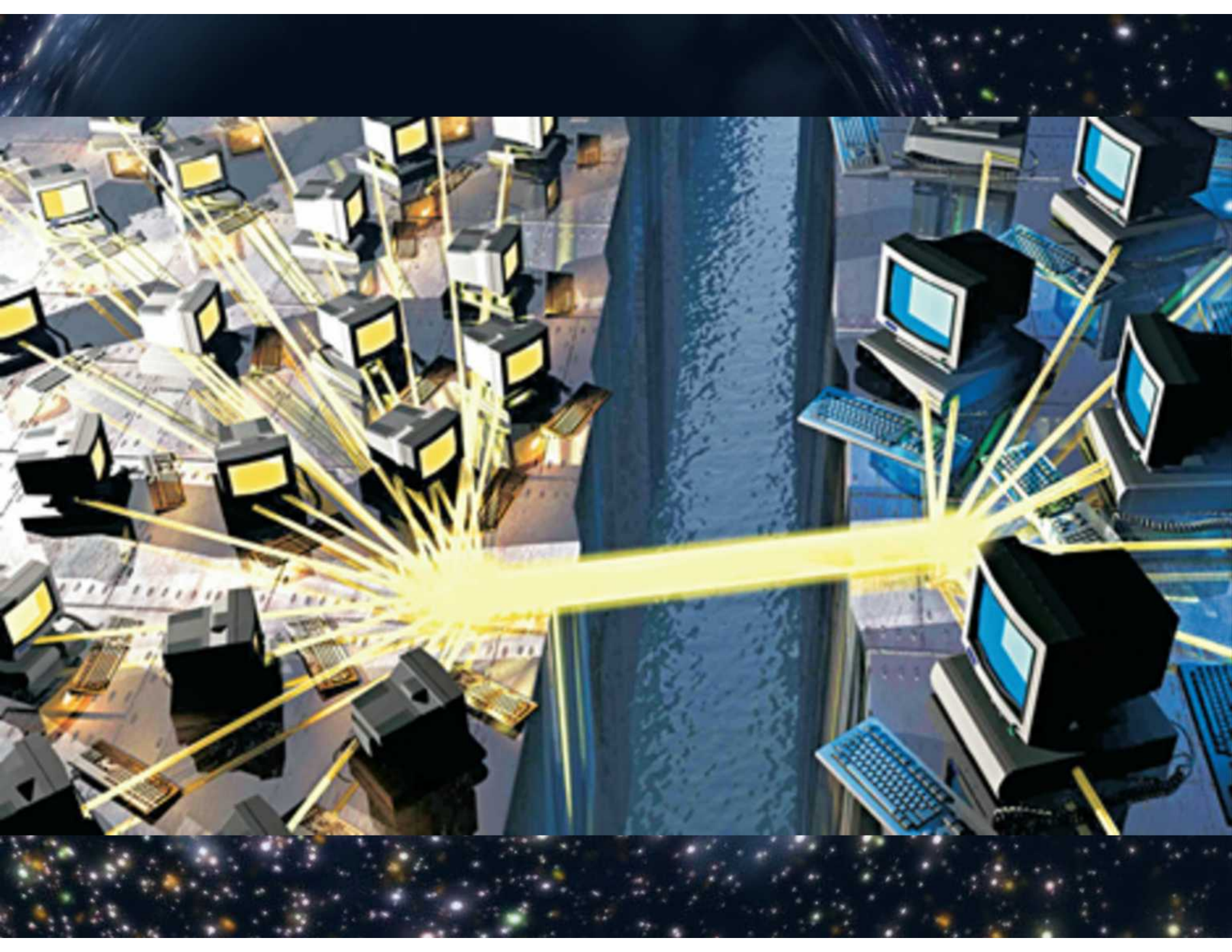
BREFT





Estados









CyberCaliphate

you isis



U.S. Central Command

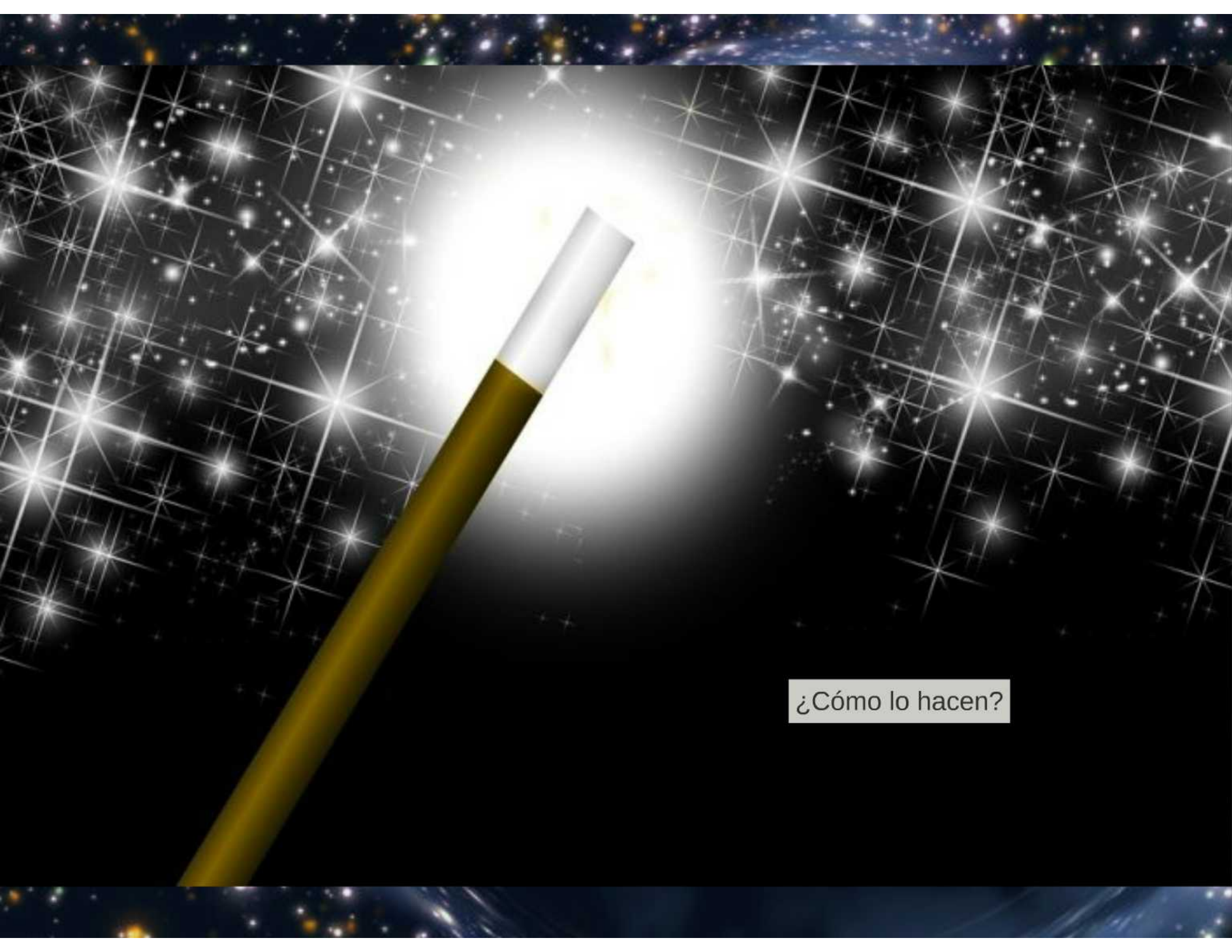
TWEETS	FOLLOWING	FOLLOWERS	FAVORITES
3,676	1,268	109K	30



 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	213,300 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	255.94
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 market	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	MSS15-034 Microsoft IIS Remote Code Execution	308.53	65,778.11
1day	*NEW* ring0 LPE Exploit CVE-2015-0067	48.17	10,269.84
hd	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



Hackers claim to hack NSA's Equation Group and selling its hacking tools and exploits online!

Recent prices from the black market

1BTC

Price

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

Ooops, your files have been What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are inaccessible because they have been encrypted. Maybe you are busy 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 anymore. We will have free events for users who are so poor that they cannot pay.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <Bitcoin>. Please check the current price of Bitcoin and how much you need to pay. And send the correct amount to the address provided in this message. After your payment, click <Check Payment>.



Payment will be raised on
5/19/2017 23:37:34
Time Left
02:23:30:20

Your files will be lost on
5/19/2017 23:37:34
Time Left
05:23:30:20

About Jacon
How to buy bitcoin?
[Contact Us](#)

¿Cómo puedo protegerme?





Copias de seguridad

Upgrading Windows

Your PC will restart several times. Sit back and relax.



Copying files

Installing features and drivers 12%

Configuring settings



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 (recomendado)
- Ocultar las extensiones de archivo para tipos de archivo conocidos
- Ocultar unidades vacías en la carpeta Equipo
- Restaurar ventanas de carpetas anteriores al iniciar sesión
- 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

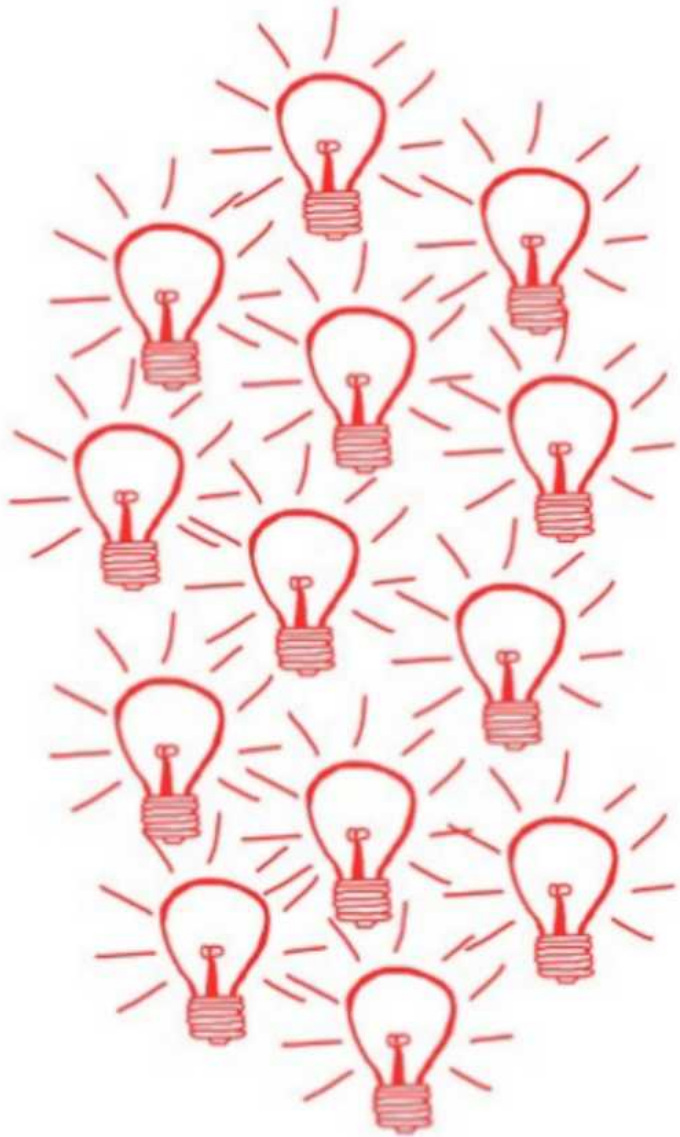
Configuración avanzada:

- 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 cifrados
 - Mostrar controladores de vista previa en el panel de vista
 - Mostrar descripción emergente para los elementos de carpeta

Restaurar valores predeterminados

Aceptar Cancelar Aplicar

Implementar soluciones propietarias



=



Nombre	Ext	Tamaño	Fecha
<DIR>			18/05/2017 13:12
<DIR>			15/07/2016 12:46
dsit		26,0 Kb	24/08/2016 13:34
psit		95,9 Kb	11/07/2016 12:59
psit		29,9 Kb	29/03/2016 10:46
psit		52,3 Kb	17/05/2016 12:26
psit		43,2 Kb	29/03/2016 10:46
psit		80,7 Kb	18/04/2016 12:39

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 árbol directorio Cancelar Opciones >>

providencia donado.psit - Adobe Acrobat Reader DC

Inicio Herramientas recsegconcert.pdf providencia donad... *

83,5%



JUZGADO DE INSTRUCCIÓN 6 RUBÍ
 Pero Esmendia, 15
 08191 Rubí Barcelona

PREVIAS1330/2009 P2

PROVIDENCIA 3.2.2016 SEÑALAMIENTO VOLCADO DE DATOS

Plantilla.dsit - Word Juan Carlos Ruloba Castilla

Archivo Inicio Insertar Diseño Formato Referencias Correspondencia Revisar Vista Complementos PDF PDF Architect Qué des

Cambria (Titul) - 26 - A⁺ A⁻ Aa -

AaBbCc 1.1. A: 1.1.1.

Normal Subtítulo Título 1 Edición

Portapap... Fuente Párrafo Estilos

DATOS ANÁLISIS DE LA INFORMACIÓN

Página 3 de 4 343 palabras Español (España) 100%

THE STRUCTURE OF A BOTNET

BOTMASTER

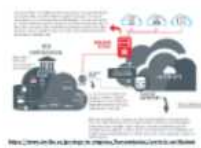


Bloquear el tráfico a dominios y servidores C2 mediante IDS/IPS

**C&C-SERVERS
(COMMAND & CONTROL)**



**INFECTED COMPUTERS
(ZOMBIES)**



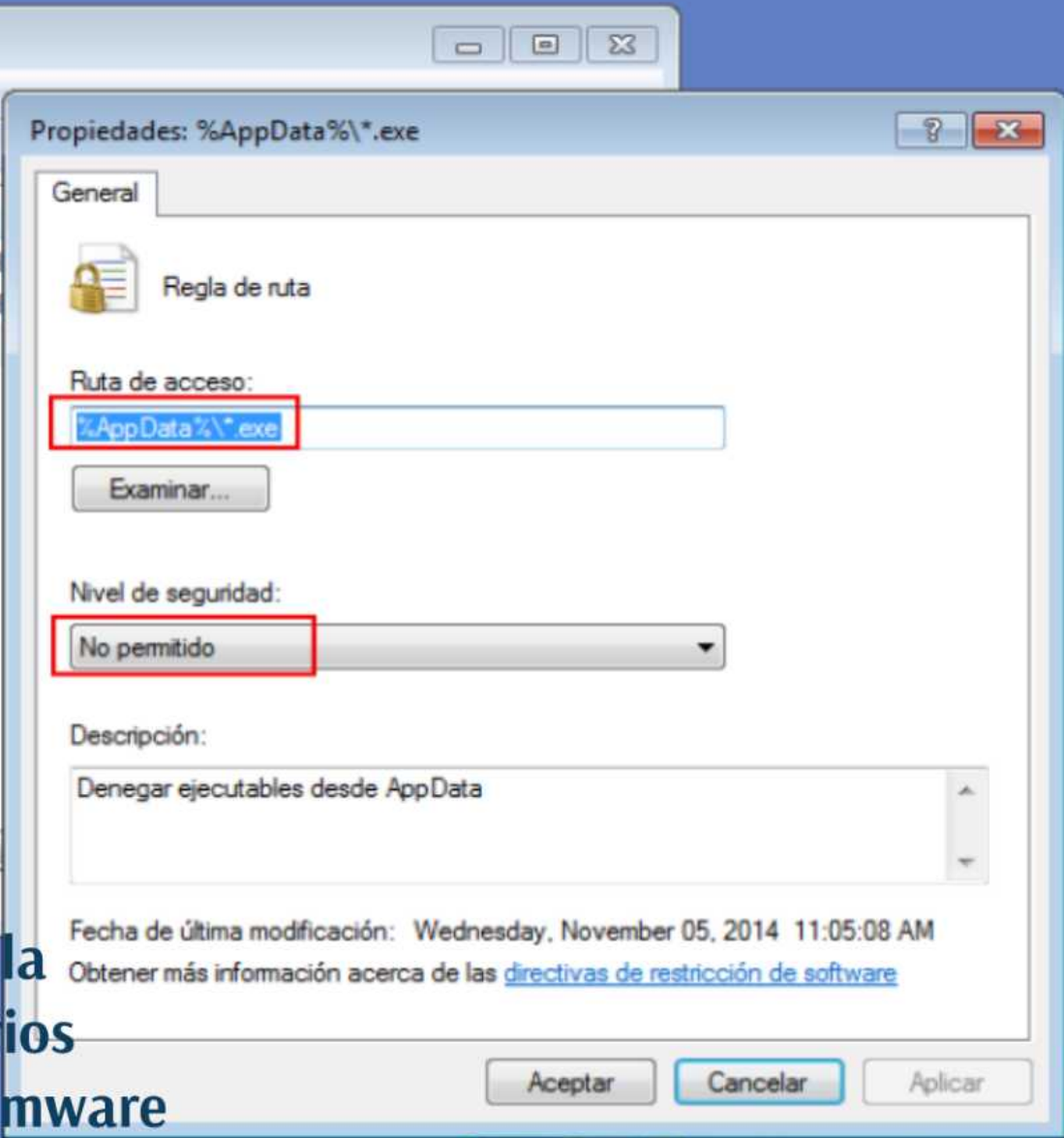
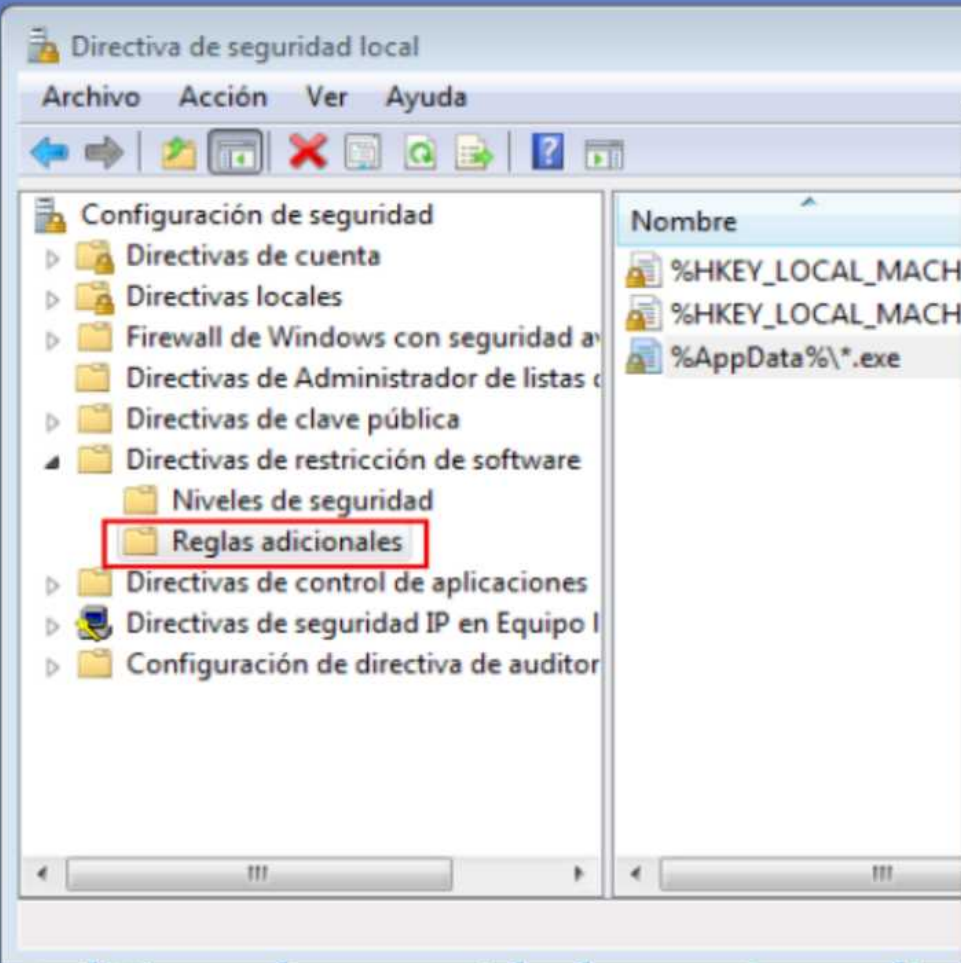
Las autoridades en colaboración con equipos de seguridad han incautado este servidor malicioso, pero es necesario que los dispositivos que controla sean desinfectados, en caso contrario los cibercriminales podrían reactivar la botnet desde otro punto. Para ello informan a las entidades competentes sobre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



La dirección IP pública se asocia al router y puede cambiar. La usan todos los dispositivos de tu red para conectarse a internet.

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

The public beta is available for testing [HERE](#).

CryptoPrevent v8.0

CryptoPrevent+ Malware Protection System and Anti-Virus Supplement

Apply Protection Custom Settings Updates Email History About Get Premium!

Choose a Protection Plan:

- None
- Minimal
- Default
- Maximum
- Use Custom Settings

For advanced configuration, you may customize all protection settings on the next tab.

Enable Active Protection:

- Use Custom Settings
- Prevent File Types (on demand)
- Folder Watch (real-time)

CryptoPrevent QuickAccess:

- Enable / Start with Windows

Apply Custom Settings

CryptoPrevent v8.0

CryptoPrevent+ Malware Protection System and Anti-Virus Supplement

Apply Protection Custom Settings Updates Email History About Get Premium!

Minimum Plan Default Plan Maximum Plan Prevent File Types Folder Watch

CryptoPrevent creates these 'Software Restriction Policy' rules when this Protection Plan is chosen. After a PC restart, rules are enforced by Windows to prevent programs from starting.

Protected Areas:

- %appdata%
- %appdata%*
- %localappdata%
- Recycle Bin

Prevent Program Naming Exploits:

- Double File Extensions
- RLO (Right-to-Left Override)

Extensions:

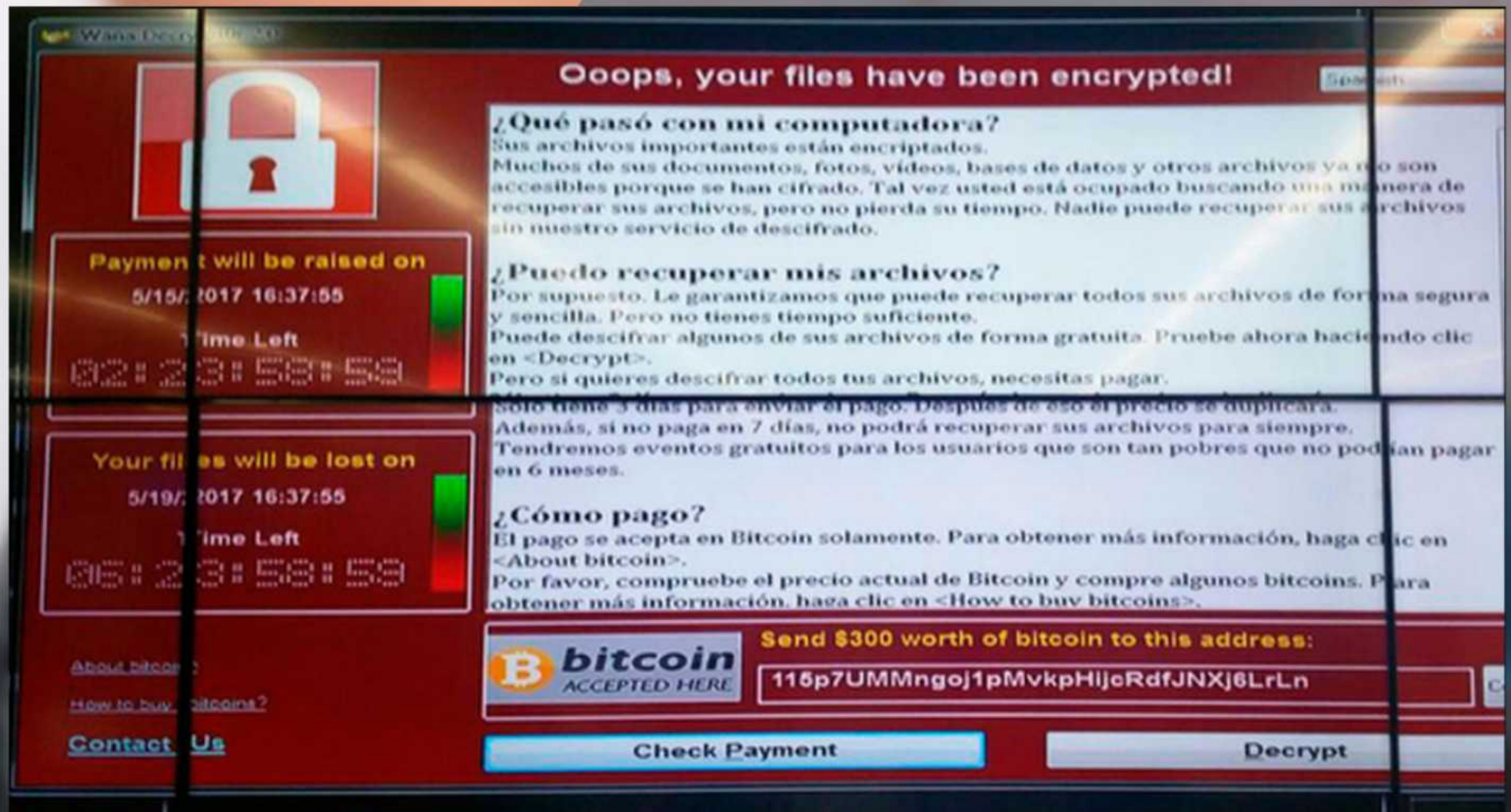
Executable files that appear to have a double (or fake) file extension will be blocked. Select the file extensions in the list to the right to include that file type in this block policy.

[Learn More \(web search\)](#)

Effective Software Restriction Policies: ---
Definitions Loaded: ---

Apply Custom Settings

¿Qué debo hacer ante un ataque?



Ooops, your files have been encrypted!

¿Qué pasó con mi computadora?
Sus archivos importantes están encriptados. Muchos de sus documentos, fotos, videos, bases de datos y otros archivos ya no son accesibles porque se han cifrado. Tal vez usted está ocupado buscando una manera de recuperar sus archivos, pero no pierda su tiempo. Nadie puede recuperar sus archivos sin nuestro servicio de descifrado.

¿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.

¿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>.

Payment will be raised on
5/15/2017 16:37:55
Time Left

Your files will be lost on
5/19/2017 16:37:55
Time Left

Send \$300 worth of bitcoin to this address:
115p7UMMngoJ1pMvKpHljcRdfJNXj6LrLn

Check Payment **Decrypt**

bitcoin ACCEPTED HERE

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

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

personal files are

ted.

encrypted with

can decrypt your

within provided
for them.

Your

Your documents, photo
strongest encryption a

on k
you pay a

ed only
time

Favorece el crimen y no te asegura librarte de la amenaza





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



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



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



Cuponespago - Consiga tu Ukash online a través de su Internet Bank o utilizando tu tarjeta de crédito.



El mensaje tiene un componente de Ingeniería Social

SALVAR VOLATILES

Filter: http.request Expression... Clear Apply Save

	Dst	Port	Host	Info
2-01 16:17:10	198.46.86.158	80	www.tripmegamart.com	GET /js/typeahead.js HTTP/1.1
2-01 16:17:11	198.46.86.158	80	www.tripmegamart.com	GET /js/scripts.js HTTP/1.1
2-01 16:17:11	198.46.86.158	80	www.tripmegamart.com	GET /js/hotel.js HTTP/1.1
2-01 16:17:11	198.46.86.158	80	www.tripmegamart.com	GET /js/flight.js HTTP/1.1
2-01 16:17:13	178.62.90.65	80	img.oduvanchiksawa.biz	GET /adverting/?id=5345896&keyword=7990adf7e882b1d8598511f94c69306e&uy...
2016-02-01 16:17:14	178.62.90.65	80	img.oduvanchiksawa.biz	GET /adverting/images/7.jpg HTTP/1.1
2016-02-01 16:17:14	192.241.243.53	80	pon.dedulkasanya.biz	GET /57198smack/hardcover-dimpling?707=daydreams&4772=undecideds&9524=...
2016-02-01 16:17:15	192.241.243.53	80	pon.dedulkasanya.biz	GET /campsite70862/totems 558?vends=615&indeterminable-sloping=e525f6w...
2016-02-01 16:17:16	192.241.243.53	80	pon.dedulkasanya.biz	GET /enema-49674754=impeached&patienter admiring=92e8pkm7dn2886c7i26&5...
2016-02-01 16:17:16	178.62.189.175	580	178.62.189.175	POST /imageserver/autogetting.php HTTP/1.1 (application/octet-stream)
2016-02-01 16:17:16	178.62.189.175	580	178.62.189.175	GET /imageserver/autoget/get.php?f=locker HTTP/1.1
2016-02-01 16:17:16	178.62.189.175	580	178.62.189.175	POST /imageserver/autogetting.php HTTP/1.1 (application/octet-stream)
2016-02-01 16:17:16	178.62.189.175	580	178.62.189.175	GET /imageserver/autoget/get.php?f=pony HTTP/1.1
2016-02-01 16:17:30	178.62.189.175	80	178.62.189.175	POST /myadvert/autoget.php HTTP/1.0
2016-02-01 16:17:30	178.62.189.175	80	178.62.189.175	POST /imageserver/autogetting.php HTTP/1.1 (application/octet-stream)
2016-02-01 16:17:35	37.140.192.170	80	sushi-panda.com	POST /components/com_content/views/categories/tmpl/dbconnect.php HTTP/...
2016-02-01 16:17:55	37.140.192.170	80	sushi-panda.com	POST /components/com_content/views/categories/tmpl/dbconnect.php HTTP/...

A file downloader (pony?) before the TeslaCrypt callback traffic.

Process Explorer - Sysinternals.com

Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
System Idle Process	0	95.26	0 K	24 K		
System	4	0.21	184 K	1,664 K		
Interrupts	n/a	0.22	0 K	0 K	Hardware Interrupts and DPCs	
smss.exe	404		596 K	460 K		
csrss.exe	552	< 0.01	2,472 K	2,336 K		
wininit.exe	624		1,636 K	360 K		
services.exe	680		6,720 K	6,076 K		
svchost.exe	828		5,744 K	5,516 K	Host Process for Windows S...	Microsoft Corporation
explorer.exe	3104	0.03	88,424 K	85,188 K	Windows Explorer	Microsoft Corporation
Process Explorer Po...	7832	< 0.01	37,960 K	1,992 K	Process Explorer Portable (P...	PortableApps.com
procexp.exe	7984		2,404 K	7,504 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64...	7840	0.41	15,292 K	28,200 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...
WmiPrivSE.exe	7812		3,220 K	6,592 K		
svchost.exe	904	< 0.01	5,196 K	5,332 K	Host Process for Windows S...	Microsoft Corporation
MaMpEng.exe	964	0.05	80,024 K	64,300 K	Antimalware Service Execut...	Microsoft Corporation
atiesnox.exe	844		1,760 K	684 K	AMD External Events Servic...	AMD
atiecbox.exe	1512		2,768 K	1,048 K		
svchost.exe	980		21,372 K	12,628 K	Host Process for Windows S...	Microsoft Corporation
audiodg.exe	4948		18,704 K	14,396 K		
svchost.exe	1060	< 0.01	156,408 K	148,924 K	Host Process for Windows S...	Microsoft Corporation
WUDFHost.exe	2616		2,372 K	3,744 K		
dwm.exe	340	0.09	46,228 K	43,472 K	Desktop Window Manager	Microsoft Corporation
svchost.exe	1104	< 0.01	30,468 K	25,480 K	Host Process for Windows S...	Microsoft Corporation
UnsignedThemesSvc.exe	1140		1,816 K	544 K	Unsigned Themes Service	The Within Network, LLC
svchost.exe	1252	< 0.01	10,648 K	11,592 K	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1424	< 0.01	18,384 K	10,264 K	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe	1588		6,628 K	3,748 K	Spooler SubSystem App	Microsoft Corporation
svchost.exe	1620		21,372 K	11,648 K	Host Process for Windows S...	Microsoft Corporation
amsvc.exe	1740		1,232 K	500 K	Adobe Acrobat Update Servi...	Adobe Systems Incorporated
svchost.exe	1788	< 0.01	47,928 K	132,220 K	Host Process for Windows S...	Microsoft Corporation

CPU Usage: 4.74% Commit Charge: 48.27% Processes: 75 Physical Usage: 71.66%

Adquirir las evidencias volatiles

Inicio y recuperación

Inicio del sistema

Sistema operativo predeterminado:

Windows 7

Mostrar la lista de sistemas operativos por 30

Mostrar opciones de recuperación por 30

Error del sistema

Grabar un evento en el registro del sistema

Reiniciar automáticamente

Escribir información de depuración

Volcado de memoria del kernel

(ninguno)

Volcado de memoria pequeño (128 KB)

Volcado de memoria del kernel

Volcado de memoria completa

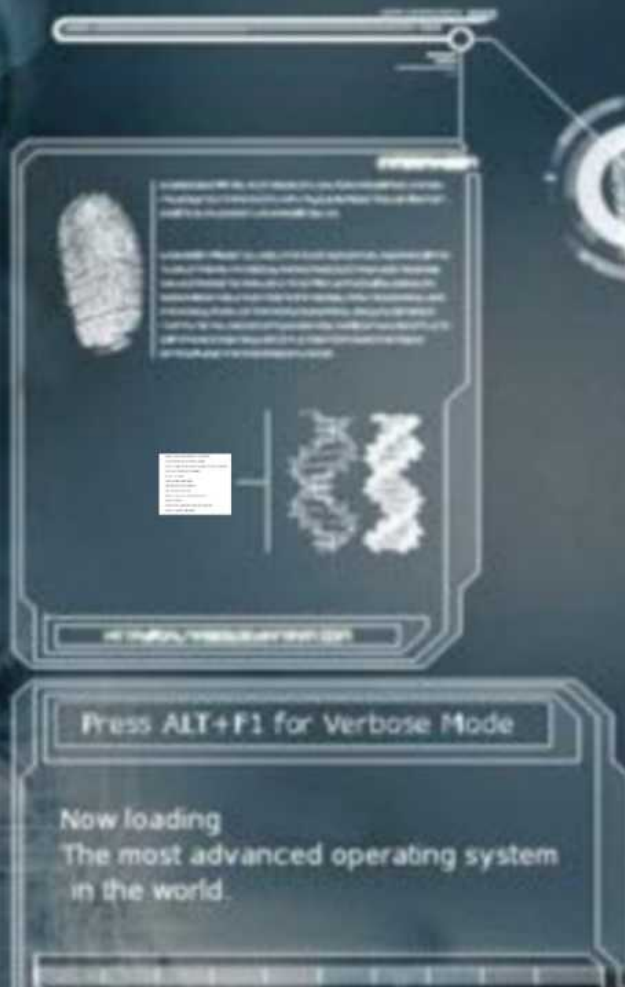
Sobrescribir cualquier archivo existente

CLONAR



Hacer una copia forensic de los almacenamiento de los equipos

ANÁLISIS FORENSE



Habr  que encargar un an lisis 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



Procesos Escaneo de seguridad

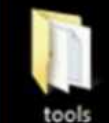
Nombre de la imagen	Seguridad	CPU	CPU Avg	PID	Uso de RAM ...	Tamaño MV	Descubierto	Parámetros
services.exe	Comprobar	0	0,00	1352	4.672	4.336	28/05/2017	
AdjustService.exe *32	Comprobar	0	0,00	3316	7.272	12.084	28/05/2017	
Agent.exe *32	Comprobar	0	0,00	3280	14.784	39.076	28/05/2017	
TodoBackupService...	Comprobar	0	0,00	7816	7.744	39.744	28/05/2017	
TrayNotify.exe *32	Comprobar	0	0,00	21376	1.048	2.132	28/05/2017	
AppleMobileDeviceServic...	Comprobar	0	0,01	2664	6.964	8.288	28/05/2017	
armsvc.exe *32	Comprobar	0	0,00	2668	200	1.272	28/05/2017	
avp.exe *32	Comprobar	0.2	0,47	2716	208.536	668.444	28/05/2017	
avpui.exe *32	Comprobar	0	0,00	11216	2.156	81.288	28/05/2017	
bcveserv.exe *32	Comprobar	0	0,00	2756	640	1.344	28/05/2017	
bcvetray.exe *32	Comprobar	0	0,00	15888	1.272	1.176	28/05/2017	
BCWipeSvc.exe *32	Comprobar	0	0,00	2292	672	2.172	28/05/2017	
BCWipeTM.exe *32	Comprobar	0	0,00	2608	156	2.944	28/05/2017	
BCWipeTM.exe *32	Comprobar	0	0,00	2600	232	2.340	28/05/2017	
CudaDriveService...	Comprobar	0	0,00	3092	344	12.540	28/05/2017	
dirmngr.exe *32	Comprobar	0	0,00	3252	656	1.804	28/05/2017	
GamingApp_Servi...	Comprobar	0	0,00	3328	1.120	11.568	28/05/2017	
igfxCUIService.ex...	Comprobar	0	0,00	1772	1.976	2.124	28/05/2017	
IPROSetMonitor.ex...	Comprobar	0	0,00	3380	296	1.764	28/05/2017	
ksde.exe *32	Comprobar	0	0,00	6136	2.128	28.024	28/05/2017	
ksdeui.exe *32	Comprobar	0	0,00	6592	3.032	7.000	28/05/2017	
mbae-svc.exe *32	Comprobar	0	0,00	3528	12.388	10.764	28/05/2017	
mbae64.exe	Comprobar	0	0,00	3968	1.332	1.836	28/05/2017	
conhost.exe	Comprobar	0	0,00	4528	752	1.356	28/05/2017	
mDNSResponder.e...	Comprobar	0	0,00	2524	3.292	2.380	28/05/2017	
NvDisplay.Conta...	Comprobar	0	0,00	1504	5.140	5.140	28/05/2017	
nvxdsync.exe	Comprobar	0	0,00	4560	9.752	9.724	28/05/2017	-first
nvtray.exe	Comprobar	0	0,00	11064	4.268	2.620	28/05/2017	-user_has_logged_in 1"
NvStreamNetwork...	Comprobar	0	0,00	4876	5.664	11.440	28/05/2017	
NvStreamServic...	Comprobar	0	0,00	3768	1.684	5.312	28/05/2017	
NvStreamUserAge...	Comprobar	0	0,01	8212	8.312	25.816	28/05/2017	serviceapp
conhost.exe	Comprobar	0	0,00	8232	1.028	1.580	28/05/2017	
OfficeClickToRun.exe	Comprobar	0	0,00	25768	34.004	43.396	28/05/2017	/service
AppVShNotify.exe	Comprobar	0	0,00	21808	256	1.840	28/05/2017	
Plex Update Service.exe ...	Comprobar	0	0,00	3932	180	1.852	28/05/2017	

Detalles del proceso

- Prioridad del proceso ▶
- Afinidad del proceso ▶
- Terminar proceso Ctrl+E
- Terminar árbol de procesos**
- Reiniciar proceso Ctrl+R
- Suspender proceso
- Tipo de inicio ▶
- Detalles del archivo
- Explorar directorio de archivos
- Busqueda de información de archivo
- Comprobar archivo
- Búsqueda en Google

Identificar y eliminar procesos

Obtener muestras de documentos cifrados



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\nsuiche>THANK
```

```
C:\Windows\system32\cmd.exe - tools\wanakiwi.exe
File c:\Python27\tcl\tc18.5\nsgs\be.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\bg.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\bn.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\bn_in.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\ca.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\cs.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\da.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\de.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\de_at.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\de_be.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\el.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\en_au.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\en_be.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\en_bv.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\en_ca.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\en_gb.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\en_hk.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\en_ie.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\en_in.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\en_nz.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\en_ph.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\en_sg.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\en_zh.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\en_zu.nsg.WNCRY -- OK
File c:\Python27\tcl\tc18.5\nsgs\eo.nsg.WNCRY --
```

Time Left
06:23:5

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)

C:\Python26\tcl\tc18.5\nsgs\en_ie.msg

C:\Python26\tcl\tc18.5\nsgs\en_in.msg

C:\Python26\tcl\tc18.5\nsgs\en_nz.msg

C:\Python26\tcl\tc18.5\nsgs\en_ph.msg

Copy to clipboard

Close

Copy

rypt

Obtener muestras del malware

ff0x2f4b8ea
ac0x7ed49aa60
52 MALWARE 50x
76f0xe46682690x
e0x8648c64a0xf2
0xee242d560x6
x5f3667fb0x
0/8200



- ◆ 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 respuesta 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

Malware Removal Self-Help Guides

Sign in to follow this Followers 54

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.

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.eszjuzuan (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.prsvsmst (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 doleblc

0 replies 214 views Metallica May 18

Removal instructions for Smart System Care

By Metallica, May 17 pup.optional.smartssystemcare (855)-332-0124 (and 4 more)

0 replies 318 views Metallica May 17



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 will...

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://ilcfbbdpbjdnkanagkdbmcbihfmkmg/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

LATEST GUIDES

- [MyLuckySurfing.com](#)
- [3Spiral Wave Tab - New Tab Extension](#)
- [Adylkuzz, msiexec.exe, & wuuser.exe Miner](#)
- [Browser Health Info Chrome Extension](#)
- [MyLuckySearching.com](#)
- [System Health Checker Chrome Extension](#)
- [Smart System Care](#)





Ransomware

How to remove Mordor ransomware (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 [...]

 **17.8k Likes**  **4.1k Followers**

HELPING PEOPLE SINCE 2010
MalwareTips has been around since 2010, and we pride ourselves on offering detailed, clear, and easy to understand guides that anyone can use to remove malware for free.

BE PART OF OUR COMMUNITY!
Our community has more than 37.000 registered members, and we'd love to have you as a member!

Join us and take part in our unbiased discussions among people of all different backgrounds about security and technology .

[REGISTER NOW \(IT'S FREE\)](#)

TIP: WHAT IS "MALWARE"?
Malware - short for malicious software - is an umbrella term that refers to any software

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

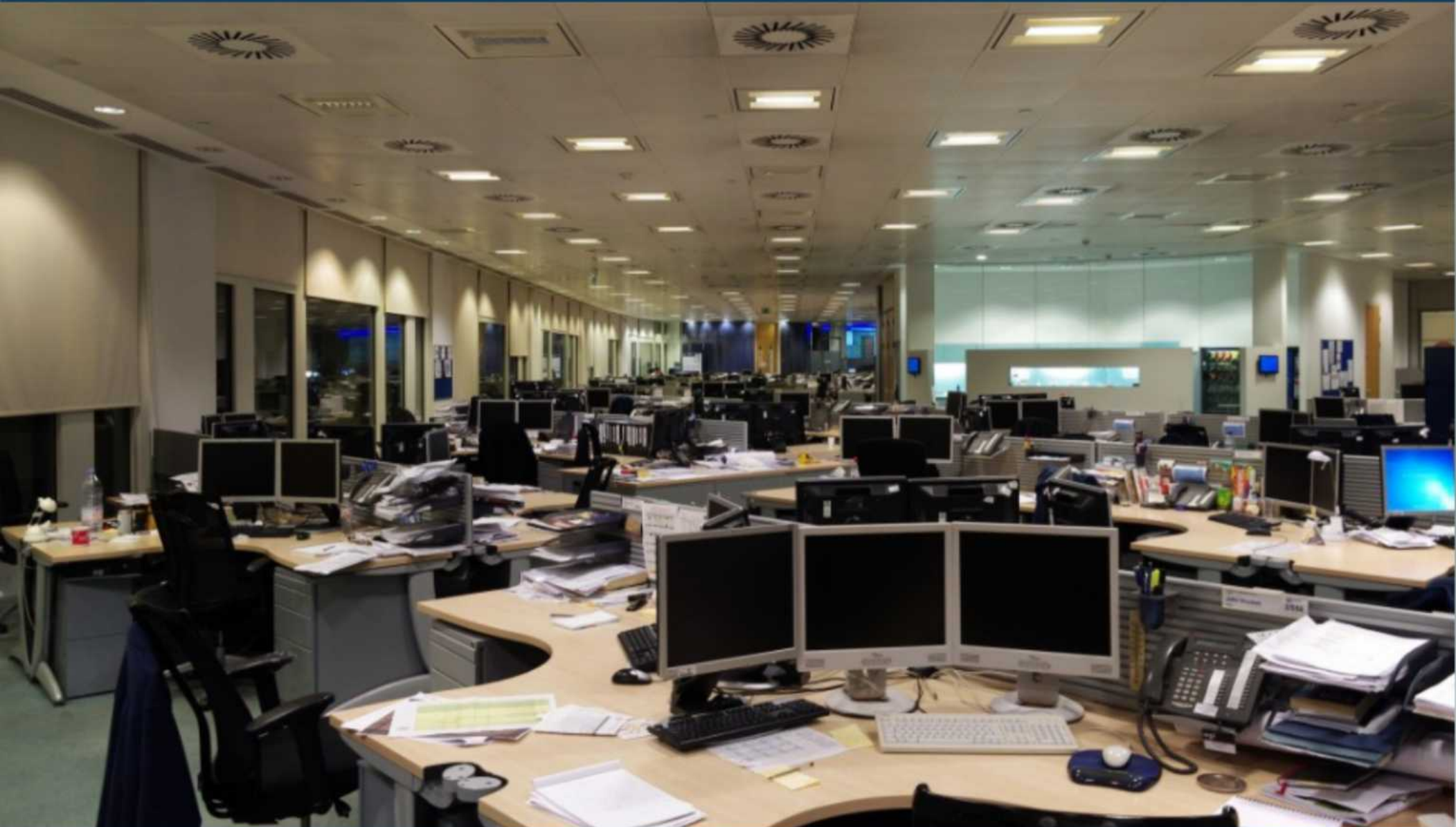
Country ▼

Number of Workstations

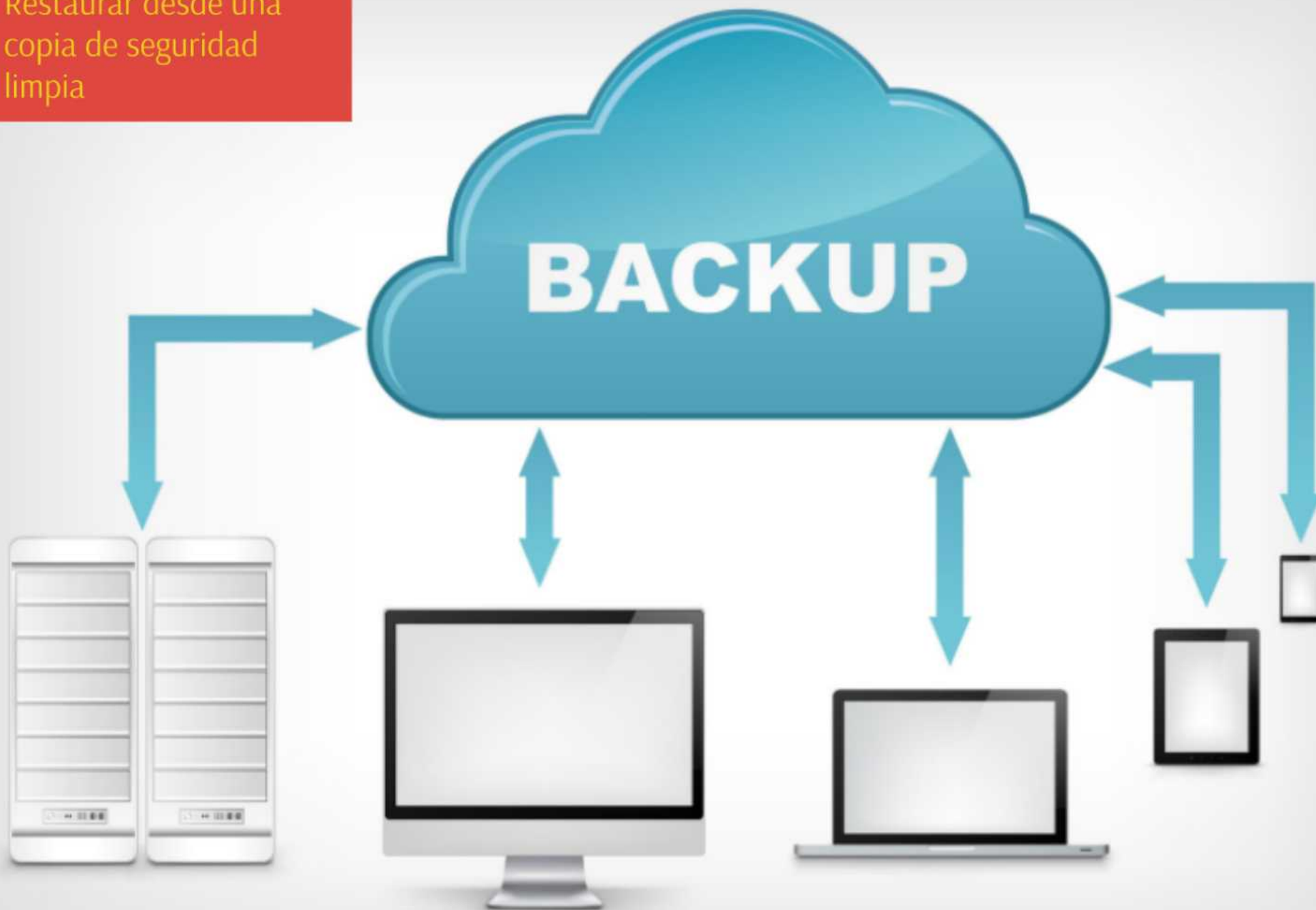
I explicitly consent to the collection and processing of my personal data as inserted in the registration form above, by AO Kaspersky Lab, to contact me and provide me with information on Kaspersky Lab's products and services including personalised promotional offers and premium assets like white papers, 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



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:





- Open in Word
- Open in Word Online


- Download
- Share
- Embed

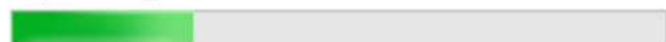
- Rename
- Delete
- Move to
- Copy to
- Version history
- Properties

- Clear selection

Ventana principal del Panel de control

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 disponible

[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 mis archivos](#)

- [Restaurar los archivos de todos los usuarios](#)
- [Selecciona otra copia de seguridad de la que restaurar archivos](#)

Vea también

[Seguridad y mantenimiento](#)

[Historial de archivos](#)

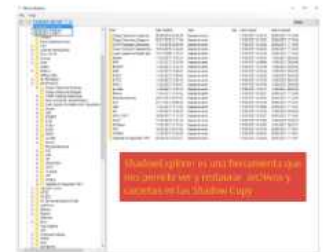


The screenshot shows the Windows File Explorer interface with two property windows open. The left window is for 'Disco local (C:)' and the right is for 'Nuevo vol (D:)'. Both windows show the 'Versiones anteriores' (Previous Versions) tab, which lists shadow copies of the folders. The C: drive shows a shadow copy from 26/05/2017 23:57, while the D: drive shows a shadow copy from 14/05/2017 13:41.

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

Nombre	Fecha de modifica...
hoy (1)	
Nuevo vol (D:)	28/05/2017 14:55
al principio de esta semana (2)	
Copia de seguridad de D:	26/05/2017 23:52
Nuevo vol (D:)	22/05/2017 23:52
al principio de este mes (1)	
Nuevo vol (D:)	14/05/2017 13:41

VSS (Volume Shadow Copy Service) o servicio de instantáneas de volúmenes, permite recuperar archivos o versiones anteriores desde esas copias.



D: 14/05/2017 13:41:29

Details

- 14/05/2017 13:41:29
- 22/05/2017 23:52:48
- 28/05/2017 14:55:17
- Avatares
- Cartas participacion tipo
- Curti
- 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



Oleada de Ransomware

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

[Más información](#)



Oleada de ransomware

Consulta nuestro aviso

ÚLTIMA HORA

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://twitter.com/juancrui)



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

¡Actualiza tu mente sino quieres perder esta guerra!

