

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

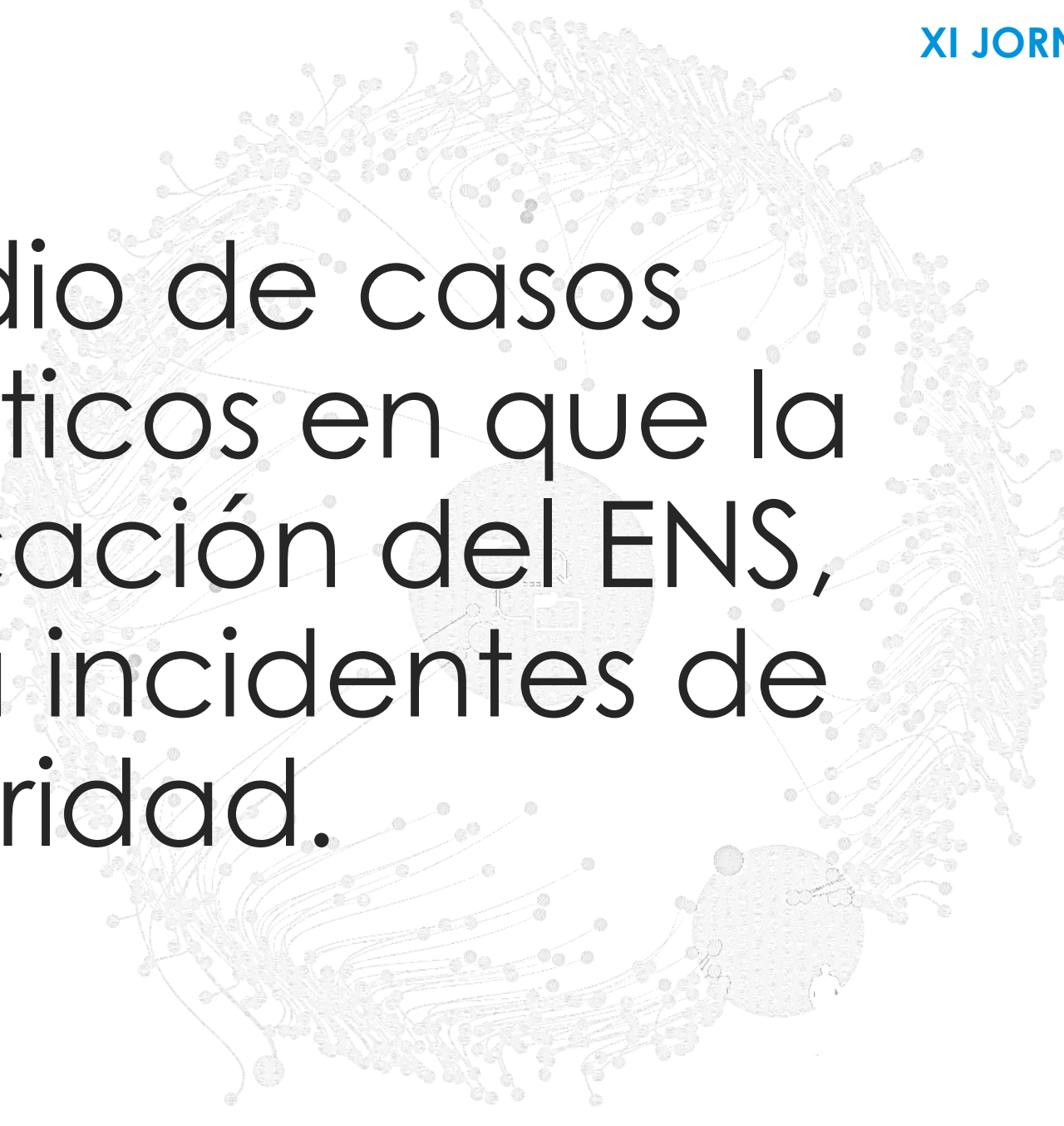
Cine, cine, cine,
mas cine por favor...



- Antonio Grimaltos Vidal
- Confederación Hidrográfica del Júcar
- Antonio.Grimaltos@chj.es

Índice

1. **Introducción**
2. **Cine club, cine, cine, mas cine por favor...**
3. **El reto de compartir.**
4. **Epilogo.**



Estudio de casos
prácticos en que la
aplicación del ENS,
evita incidentes de
seguridad.

Esquema Nacional de Seguridad

¿Para qué?, ¿Realmente sirve?

Son las preguntas que intentaremos responder...

Un poco de cine...

Películas que NO nos gustaría ver:



Un poco de cine...

Películas que NO nos gustaría ver:

- Struts, el octavo pasajero.



Un poco de cine...

Películas que NO nos gustaría ver:

- Struts, el octavo pasajero.
- Bienvenido Mr. Ransomware

Un poco de cine...

Películas que NO nos gustaría ver:

- Struts, el octavo pasajero.
- Bienvenido Mr. Ransomware
- Far From Love Story

Un poco de cine...

Películas que NO nos gustaría ver:

- Struts, el octavo pasajero.
- Bienvenido Mr. Ransomware
- Far From Love Story
- Sonrisas y lagrimas (WannaCry Story)

Un poco de cine...

Películas que NO nos gustaría ver:

- Struts, el octavo pasajero.
- Bienvenido Mr. Ransomware
- Far From Love Story
- Sonrisas y lagrimas (WannaCry Story)
- El Cartero con Malware siempre llama 2 veces

Un poco de cine...

Películas que NO nos gustaría ver:

- Struts, el octavo pasajero.
- Bienvenido Mr. Ransomware
- Far From Love Story
- Sonrisas y lagrimas (WannaCry Story)

Forma, reza, ama (a los usuarios)

Un poco de cine...

Películas que NO nos gustaría ver:

- Struts, **el octavo pasajero.**
- **Bienvenido Mr. Ransomware**
- Far From **Love Story**
- **Sonrisas y lagrimas** (WannaCry Story)
- **Forma, reza, ama** (a los usuarios)
- **Quien/a quien engaño a Bad Rabbit**

Nuestra película favorita...

El hombre tranquilo



Struts, el octavo pasajero.

Artículo 20. Integridad y actualización del sistema.

1. Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.
2. **Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.**

Struts, el octavo pasajero.

4.3.4 Mantenimiento [op.exp.4]

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

- A. Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas.
- B. Se efectuará un **seguimiento continuo de los anuncios de defectos**.
- C. Se dispondrá de un **procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones**. La **priorización** tendrá en cuenta la **variación del riesgo** en función de la aplicación o no de la actualización.

Struts, el octavo pasajero.

De: CCN-CERT [<mailto:no-reply@ccn-cert.cni.es>]
Enviado el: viernes, 10 de marzo de 2017 14:57
Para: Grimaltos Vidal, Antonio
Asunto: [CCN-CERT Alerta] Vulnerabilidad Crítica en Apache



ALERTAS

Vulnerabilidad Crítica en Apache

10/03/2017

El Equipo de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, alerta de la existencia de una vulnerabilidad Crítica (CVE-2017-5638). Los atacantes podrían obtener acceso de lectura, escritura y ejecución, de forma remota, al árbol de directorios de Apache.

El software afectado es el siguiente: Struts 2.3.5 - Struts 2.3.31, Struts 2.5 - Struts 2.5.10

Se recomienda actualizar la versión de Struts a las versiones 2.3.32 o 2.5.10.1

Más información:

<https://cwiki.apache.org/confluence/display/WW/S2-045>

Atentamente,

Equipo CCN-CERT

Struts, el octavo pasajero.



vi. 10/03/2017 15:00

Grimaltos Vidal, Antonio

RV: [CCN-CERT Alerta] Vulnerabilidad Crítica en Apache

Para Informática, Incidencias; [REDACTED]

Por favor decidme si necesitáis actualizar el apache en algún servidor.

De: CCN-CERT [<mailto:no-reply@ccn-cert.cni.es>]

Enviado el: viernes, 10 de marzo de 2017 14:57

Para: Grimaltos Vidal, Antonio

Asunto: [CCN-CERT Alerta] Vulnerabilidad Crítica en Apache



ALERTAS

Vulnerabilidad Crítica en Apache

10/03/2017

El Equipo de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, alerta de la existencia de una vulnerabilidad Crítica (CVE-2017-5638). Los atacantes podrían obtener acceso de lectura, escritura y ejecución, de forma remota, al árbol de directorios de Apache.

Struts, el octavo pasajero.

vi. 10/03/2017 15:11

Re: [CCN-C] ma. 14/03/2017 10:01

Para Grimaltos Vidal, Ant Informática, Incidencias

RE: [CCN-CERT Alerta] Vulnerabilidad Crítica en Apache

Buenas tardes.

Si, el apache lo teni

Supongo que habrá

Buenos días

Han hablado F con el personal c, según le ha comentado B usan como entorno de desarrollo el Netbeans (Java) y directamente el C++ en los servidores.

No obstante, han quedado en que actualizarán el Apache en los servidores (), pero después del episodio actual de lluvias. Se les ha comentado que antes de actualizarlos, nos manden un correo informándonos y así se realizará un snapshot de

Con el fin de mejorar el soporte ofrecido y de acuerdo con el correo remitido en su día y las instrucciones recibidas del Servicio de Informática, se hace necesaria la apertura de una incidencia a través de la herramienta Service Manager accesible mediante el siguiente enlace <http://informatica-incidencias.chj.es:8080/webtier-9.20/ess.do>

Un saludo

Struts, el octavo pasajero.

De: CCN-CERT [<mailto:no-reply@ccn-cert.cni.es>]
Enviado el: lunes, 13 de marzo de 2017 15:28
Para: SI_Proyectos
Asunto: [CCN-CERT Alerta] Vulnerabilidad Crítica en Apache (continuación)



ma. 14/03/2017 13:15

Antonino Daviu, Francisco

RE: [CCN-CERT Alerta] Vulnerabilidad Crítica en Apache

Para: SAIH; [\[redacted\]](#) Informática, Incidencias; [\[redacted\]](#)
CC: Grimaltos Vidal, Antonio; [\[redacted\]](#)

Buenos días,

El Struts se puede instalar como librerías dentro de un tomcat en del directorio /WEB-INF/lib, de hecho esta es la configuración que tienen en @Firma y que es la que ha sufrido el ataque.

En el nodo visaih, como mínimo, existen dos desplegables dentro del tomcat que hacen uso de librerías struts:

```
root@visaih64:/opt/apache-tomcat# find . -name *struts*  
./webapps/saihq/WEB-INF/lib/struts-menu-2.4.3.jar  
./webapps/chj/WEB-INF/lib/struts-menu-2.4.3.jar
```

Necesitamos que reviséis si estas librerías están afectadas por la vulnerabilidad y, en su caso, si las aplicaciones desplegadas hacen uso de ellas.

Gracias.

Struts, el octavo pasajero.



Información al Ciudadano

⊕ **Informática, Incidencias**

16/03/2017

RE: Problemas de acceso a [REDACTED]

Gracias por la información. Esta mañana nos han empezado a llamar a nosotros.

Hay problemas de disponibilidad del servicio [REDACTED]. Ya hemos mandado un correo informativo a los usuarios de [REDACTED]

Un saludo.

De: Informática, Incidencias

Enviado el: miércoles, 15 de marzo de 2017 18:54

Para: Información al Ciudadano

CC: Informática

Asunto: Problemas de acceso a [REDACTED]

Buenas tardes

Varios usuarios

Lo que hacemos en la vida tiene su eco en la eternidad.

Máximo Décimo Meridio.

Gladiator

Struts, el octavo pasajero.

Lecciones aprendidas....

Fundamental... Procedimiento de gestión de la vulnerabilidad y parcheado



Bienvenido, Mr. Ransomware

5.4.1 Perímetro seguro [mp.com.1]

Categoría BÁSICA

Se dispondrá un sistema cortafuegos que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho cortafuegos que sólo dejara transitar los flujos previamente autorizados.

Categoría ALTA

- a) El sistema de cortafuegos constará de dos o más equipos de diferente fabricante dispuestos en cascada.**
- b) Se dispondrán sistemas redundantes.**

Bienvenido, Mr. Ransomware

4.6.1 Detección de intrusión [op.mon.1

Categoría ALTA

**Se dispondrán de herramientas de
detección o de prevención de intrusión.**

Procedimiento de gestión de incidentes

Bienvenido, Mr. Ransomware

lu. 27/03/2017 10:05

Incidente #525535: [SAT-INET] Detectada posible infección por parte de Ransomware (CryptoWall) - CHJUCAR

Nuevo caso en

Despliegue Editar Dividir Unir

Metadatos del caso

Incidente #525535

Asunto: [SAT-INET] Detectada posible infección por parte de Ransomware (CryptoWall) - CHJUCAR

Propietario: satinet_chjucar_user (User SATINET_CHJUCAR)

Visibilidad: no value

Peligrosidad: Muy alto

Estado: resuelto

Descripción: Incidente

• 10.31.48.151

Reportes de Incidentes

(No hay Reportes de Incidentes activos)
(No hay Reportes de Incidentes inactivos)

Investigaciones

(No hay Investigaciones activos)
(No hay Investigaciones inactivos)

URL: <https://lucia.ccn-cert.cni.es/Ticket/Display.html?id=525535>

Atentamente,
Equipo SAT-INET CCN-CERT
Centro Criptológico Nacional



Bienvenido, Mr. Ransomware

lu. 27/03/2017 10:05

Incidente #525535: [SAT-INET] Detectada posible infección por parte de Ransomware (CryptoWall) - CHJUCAR

Nuevo caso en

^ Fechas

Creado: Lun Mar 27 10:05:05 2017

Comienzo: No establecido

Comenzado: Lun Mar 27 10:05:05 2017

Último Contacto: No establecido

Fecha Límite: Mar Jul 25 10:05:06 2017

Cerrado: Mar Mar 28 10:34:15 2017

Actualizado: Mar Mar 28 10:34:15 2017 por RT_System



^ Historial

Mar Mar 28 10:33:00 2017

satinet_chjucar_user (User SATINET_CHJUCAR) - Comentarios añadidos

siguiendo EL PROCEDIMIENTO HABITUAL, se bloquean las IP en los firewalls.

Bienvenido, Mr. Ransomware



Dashboard ACC **Monitor** Policies Objects Network Device

Logs (addr.src in 10.31.48.151)

	Fecha de registro	Tipo	Nombre	Origen	Destino	Alcance	Acción	Gravedad
	03/27 09:09:12	spyware	CryptoWall.Gen Command and Control Traffic	inside	outside	10.31.48.151	reset-server	critical
	03/27 09:09:12	spyware	CryptoWall.Gen Command and Control Traffic	inside	outside	10.31.48.151	reset-server	critical
	03/27 09:09:12	spyware	CryptoWall.Gen Command and Control Traffic	inside	outside	10.31.48.151	reset-server	critical
	03/27 09:08:56	spyware	CryptoWall.Gen Command and Control Traffic	inside	outside	10.31.48.151	reset-server	critical
	03/27 09:07:59	spyware	CryptoWall.Gen Command and Control Traffic	inside	outside	10.31.48.151	reset-server	critical
	03/27 09:07:59	spyware	CryptoWall.Gen Command and Control Traffic	inside	outside	10.31.48.151	reset-server	critical
	03/27 09:07:56	spyware	CryptoWall.Gen Command and Control Traffic	inside	outside	10.31.48.151	reset-server	critical
	03/27 09:07:54	spyware	CryptoWall.Gen Command and Control Traffic	inside	outside	10.31.48.151	reset-server	critical
	03/27 09:07:49	spyware	CryptoWall.Gen Command and Control Traffic	inside	outside	10.31.48.151	reset-server	critical
	03/27 09:07:48	spyware	CryptoWall.Gen Command and Control Traffic	inside	outside	10.31.48.151	reset-server	critical
	03/27 09:07:48	spyware	CryptoWall.Gen Command and Control Traffic	inside	outside	10.31.48.151	reset-server	critical
	03/27 09:07:48	spyware	CryptoWall.Gen Command and Control Traffic	inside	outside	10.31.48.151	reset-server	critical

Bienvenido, Mr. Ransomware



ma. 28/03/2017 14:02

at_infsis02

Incidencia SD48318 / IM35587 Incidente LUCIA #525535 [SAT-INET] equipo MACHIRIVELLASM - Detectada posible infección por parte de Ransomware (CryptoWall) - CHJUCAR

Para Grimaltos Vidal, Antonio

CC **Informática, Incidencias**

Respondió a este mensaje el 28/03/2017 14:20.

Buenos Días:

Tras la llamada de Antonio Grimaltos se llama a la usuaria pero lo coge una compañera. Se le indica que hay que apagar el ordenador, me conecto en remoto, le cierro todo lo que tenia abierto y lo apago.

Se le quita el cable de red también por si volvieran a encenderlo. Se informa a la usuaria de la alerta de Virus, y que le avisaremos cuando sepamos algo. La usuaria me indica que ha conectado su movil al pc para cargar.

Se desconecta el equipo de la red. Se avisa a la usuaria, se baja el equipo al despacho y de deja apagado.

La usuaria tenía previsto el cambio de equipo el Martes 28/03/2017, por lo que se le prepara el equipo nuevo, SIN COPIAR NINGUN DATO, hasta que Antonio Grimaltos decida que hacer con los datos del antiguo disco duro. Se clona el disco duro del equipo antiguo para pruebas, comprobaciones, y para el caso de que el cryptowall encripte los datos.

Se comprueba en el PaloAlto que ha bloqueado los intentos de conexión desde el equipo MACHIRIVELLASM (10.31.48.151) hacia las IPs indicadas en la incidencia, al detectar el tráfico como amenaza: **CryptoWall.Gen Command And Control Traffic**

Se bloquean las IPs indicadas en los Firewalls externo e interno, para que sean bloqueadas las conexiones entrantes/salientes como los objetos:

Incidente_Lucia_525535_1	108.167.160.63
Incidente_Lucia_525535_2	64.50.163.44
Incidente_Lucia_525535_3	217.107.34.123

Bienvenido, Mr. Ransomware



ma. 28/03/2017 14:20

Amenazas Críticas

PA1-CHJ : V

Hora de recepción
2017/09/20 10:00

Lecciones aprendidas....

Usa tus recursos, programamos el firewall, para que nos avisase en caso de alerta crítica, y añadimos en el procedimiento que esas alertas se revisarán, todas, sin excepción

Enviado el: martes, 28 de marzo de 2017 14:02

Para: Grimaltos Vidal, Antonio

CC: Informática, Incidencias

Asunto: Incidencia SD48318 / IM35587 Incidente LUCIA #525535 [SAT-INET] equipo [REDACTED] - Detectada posible infección por parte de Ransomware (CryptoWall) - CHJUCAR

Buenos Días:

Tras la llamada de Antonio Grimaltos se llama a la usuaria pero lo coge una compañera. Se le indica que hay que apagar el ordenador, me conecto en remoto, le cierro todo lo que tenía abierto y lo apago.



Far From Love Story

- **Artículo 24. Incidentes *de seguridad*.**
 1. Se establecerá un sistema de detección y reacción frente a código dañino
 2. Se registrarán los incidentes de seguridad que se produzcan y las acciones de tratamiento que se sigan. Estos registros se emplearán para la mejora continua de la seguridad del sistema.

Far From Love Story

- **4.3.7 Gestión de incidencias [op.exp.7]**
 - Procedimiento de gestión de incidentes. Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, ...

Far From Love Story

Vier
desc
hay



vi. 17/03/2017 17:09

Leal García, José Manuel

Bull

Para Grimaltos Vidal, Antonio

ción que

901 116119 Te pondrán con el que está de guardia

Hoy me he dado un baño en la maso

Saludos

Correo raro

Ya me dices algo

Dich
en p
dich



Una primera valoración

Far From Love Story

Binarios Análisis Búsqueda Avanzada Configuración Monitorización Estadísticas  MARTA ® Innotec System S.L. Usuario: agrimaltos					
Fecha	MDS	Nombre Fichero	Tipo Fichero	Etiquetas	Acciones
14-09-2017	5c2d34322ff78d7f42b058faaec7baa	FACV00000-478.xls	Composite Document File V2 Document		  
13-09-2017	1f7740b2dbfb240c4c12b7a435deb35f	SikreDokumenter.doc	Composite Document File V2 Document		  
07-09-2017	3520b18d56244e96fa234975d855fa7b	keygen.exe	PE32 executable (GUI) Intel 80386, for MS...		  
02-05-2017	1d02f7dcc1216c04462afa8a793e493b	troyano_pcbellus.exe	PE32 executable (DLL) (GUI) Intel 80386, f...	CH01	  
19-04-2017	46965cfa8c1fe4f14dd5b99f4bf80500	577395.doc	Composite Document File V2 Document	CH01	  
07-04-2017	423670d769803ab76d1ab18e96267599	report Informacion comercial-94885.pdf	PDF document, version 1.4	CH01	  
04-04-2017	53c6c41356d532fe8056ab2906d129	Lightshot.exe	PE32 executable (GUI) Intel 80386, for MS...	CH01	  
28-03-2017	67f29f617af9fcd7c8a54c1f75b85e96	sweetimsetup.exe	PE32 executable (GUI) Intel 80386, for MS...	CH01	  
18-03-2017	9971ea1bba599ee3272b2b1c32423a7c	far_from_love.mp3	Audio file with ID3 version 2.3.0	CH01	  
15-03-2017	ce9da5b8c7d790f88e9b0839706bce97	owa[1]	HTML document, ASCII text, with very long...	CH01	  

Far From Love Story

● Análisis del Binario far_from_love.mp3 con MD5: 9971ea1bba599ee3272b2b1c32423a7c

General Informe Reglas Etiquetas Evidencias Strings Red Registro Ficheros Procesos Servicios Hooks Pers

DNS TCP / UDP HTTP ICMP IRC SMTP Geolocaliz.

☐ Dominio	IP		
☒ go.microsoft.com	23.217.171.33	Externa	
☐ obsp.omniroot.com	93.184.220.20	Externa	
☐ obsp.msocsp.com	198.41.214.186	Externa	
☐ icanhazip.com Simulación Humana	64.182.208.184	Externa	
☐ ieonline.microsoft.com	204.79.197.200	Externa	

Google Maps

Datos de mapas ©2017 Google Términos de uso Informar de un error de Maps

Far From Love Story

● Análisis del Binario far_from_love.mp3 con MD5: 9971ea1bba599ee3272b2b1c32423a7c

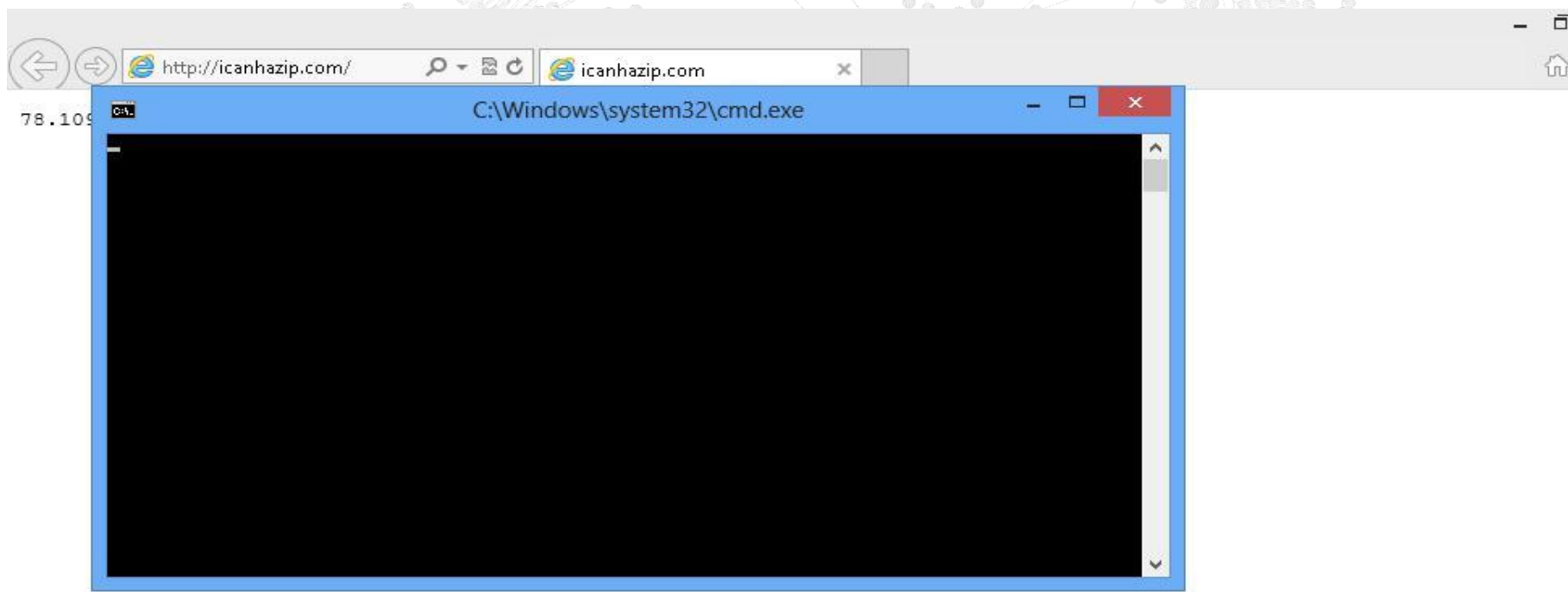
General Informe Reglas Etiquetas Evidencias Strings Red Registro **Ficheros** Procesos Servicios Hooks Pers

Abiertos Leídos **Escritos** Eliminados Ejecutados Movidos Copiados

Nombre del Fichero	Ruta Completa	MD5	Tamaño	Estado
KERNELBASE.dll.mui	C:\Windows\system32\en-US\KERNELBASE.dll.mui			✓

Mostrando del 1 al 1. Total: 1 15 por página

Far From Love Story



Far From Love Story

🔴 Análisis del Binario far_from_love.mp3 con MD5: 9971ea1bba599ee3272b2b1c32423a7c

General Informe Reglas Etiquetas Evidencias Strings Red **Registro** Ficheros Procesos Servicios Hooks Pers →

Abiertas Leídas Escritas Eliminadas

Path	Status
HKEY_CURRENT_USER\	✓
Software\Policies\Microsoft\Windows\System\	✗
Software\Microsoft\Command Processor\	✓
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts\	✓
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups\	✓
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\AppCertDlls\	✗
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SafeBoot\Option\	✗
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\	✓
HKEY_CURRENT_USER\ware\Policies\Microsoft\Windows\Safer\CodeIdentifiers\	✗
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\AppCompatibility\	✗
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppCompat\	✗
HKEY_CURRENT_USER\ware\Microsoft\Windows NT\CurrentVersion\	✓
AppCompatFlags\Layers\	✗
Custom\cmd.exe\	✗
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\	✓

⏪ ⏩ | Página 1 de 2 | 🔍 ↻

Mostrando del 1 al 15. Total: 18 15 ▼ por página

Far From Love Story



at_infsis01

Informática, Incidencias; Grimaltos Vidal, Antonio

1

19/03/2017

RV: NO ABRIR ARCHIVO ADJUNTO AL CORREO DE Migu

Respondió a este mensaje el 19/03/2017 20:26.
Mensaje enviado con importancia Alta.



SearchCorreo.xlsx
Archivo .xlsx

Buenos días

A petición de Antonio se ha borrado de todos los buzones los mensajes enviados por [redacted] con el .mp3. que tengan el asunto "BalduqueFiuokm j zff de dddzfgx,,rma"

Para realizar esta acción ha sido necesario agregar al grupo AdministradoresCHU el rol Mailbox Import-Export que no tenía por defecto.

Previamente se ha sacado un listado de los usuarios que lo tenían en sus buzones (adjunto listado)

Hay algunos buzones con una determinada propiedad "SingleItemRecoveryEnabled" que permite desde el servidor recuperar los mensajes una vez borrados.

En mi caso, se han borrado los mensajes que tenía con ese asunto, sin embargo al hacer la query continua indicando que están porque tengo habilitada la propiedad indicada.

Cualquier cosa me preguntais.

Far From Love Story

Responder

Responder a todos

Reenviar



NO ABRIR ARCHIVO ADJUNTO AL CORREO DE

Grimaltos Vidal, Antonio

Para: [chj](#)

CC: [Informática, Incidencias](#)

domingo, 19 de marzo de 2017 12:43

• Mensaje enviado con importancia Alta.

El pasado día 17 de marzo sobre las 17:30 de la tarde, recibimos todos incluso algunos por duplicado un correo que en principio proviene de una dirección de correo legítimo de la CHJ.

Dicho correo llevaba un archivo adjunto far_from_love.mp3, en principio un archivo de audio inofensivo, **dicho archivo se adjuntó sin conocimiento del usuario.**

NO LO ABRAIS, CONTIENE UN ARCHIVO CON CODIGO MALICIOSO. SI POR CASCUALIDAD ALGUIEN LO HA ABIERTO, QUE SE PONGA EN CONTACTO CON EL SERVICIO DE INFORMATICA Y LO COMUNIQUE.

BORRAD EL CORREO Y VACIAD LA PAPELERA DEL CORREO.

Antonio grimaltos Vidal
Jefe de seccion de sistemas informáticos.
Responsable de Seguridad



Sonrisas y Lagrimas. WannaCry.

Artículo 20. Integridad y actualización del sistema.

1. ... /...
2. Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

Sonrisas y Lagrimas. WannaCry.

4.3.4 Mantenimiento [op.exp.4]

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

- A.... /...
- B. Se efectuará un seguimiento continuo de los anuncios de defectos.
- C. Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.

Sonrisas y Lagrimas. WannaCry.



at_infsis02

SI_Proyectos; Informática, Incidencias

15/03/2017

[SEGURIDAD-ACTUALIZACIONES-AVISO]: Parches de Seguridad Microsoft Marzo 2017 (incluidos los no liberados en Febrero 2017)



Mensaje enviado con importancia Alta.



mi. 15/03/2017 8:32

at_infsis02

[SEGURIDAD-ACTUALIZACIONES-AVISO]: Parches de Seguridad Microsoft Marzo 2017 (incluidos los no liberados en Febrero 2017)

Para SI_Proyectos

CC Informática, Incidencias



Mensaje enviado con importancia Alta.

Buenos Días:

Como siempre, el segundo martes de cada mes, Microsoft ha liberado parches de seguridad, incluidos los que no distribuyó en Febrero 2017 por problemas de última hora.

Entre los parches liberados se encuentra 12 parches para vulnerabilidades 0-days ya publicadas, entre ellas, la de 0-day SMB, CVE-2017-0016 relativa a la SD47213 / IM34767.

- SMB-related denial-of-service (DoS) flaw in Windows (CVE-2017-0016), a Windows kernel privilege escalation (CVE-2017-0050)
- Remote code execution bug in a graphics component (CVE-2017-0014)

Sonrisas y Lagrimas. WannaCry.



at_infsis02

SI_Proyectos; Informática, Incidencias ▾

15/03/2017

RV: [SEGURIDAD-ACTUALIZACIONES-AVISO]: Parches de Seguridad Microsoft Marzo 2017 (incluidos los no liberados en Febrero 2017)



De: Grimaltos Vidal, Antonio

Enviado el: miércoles, 15 de marzo de 2017 8:34

Para: at_infsis02

Asunto: RE: [SEGURIDAD-ACTUALIZACIONES-AVISO]: Parches de Seguridad Microsoft Marzo 2017 (incluidos los no liberados en Febrero 2017)

Pues programado I hacedlo cuanto antes



Lo habíamos aprendido en Struts, el octavo pasajero

Enviado desde mi dispositivo Samsung

Buenos Días:

Como siempre, el segundo martes de cada mes, Microsoft ha liberado parches de seguridad, incluidos los que no distribuyó en Febrero 2017 por problemas de última hora.

Sonrisas y Lagrimas. WannaCry.



at_infsis09

[Redacted]

⊕ Informática, Incidencias; ⊕ SI_Proyectos ▾

15/03/2017

Actualización de Servidores de prueba de la CHJ MIÉRCOLES 22 DE MARZO

Buenos días,

El miércoles que viene esta planificado a partir de las 15:30 la actualización de los servidores de prueba.

Os mando correo para que lo envíes a la casa avisando de esta actuación a los informáticos de las aéreas.

Con el fin de mejorar el soporte ofrecido y de acuerdo con el correo remitido en su día y las instrucciones recibidas del Servicio de Informática, se hace necesaria la apertura de una incidencia a través de la herramienta Service Manager accesible mediante el siguiente enlace <http://informatica-incidencias.chj.es:8080/webtier-9.20/ess.do>

Un saludo

Sonrisas y Lagrimas. WannaCry.

 Informática, Incidencias | **[Redacted]** CHJDesarrollo; OPHAdminInfor; **[Redacted]** SI_Proyectos; + 1 22/03/2017

RE: Actualización de Servidores de prueba de la CHJ MIÉRCOLES 22 DE MARZO

Buenas tardes,

Ha finalizado correctamente la actualización de los servidores de prueba

Con el fin de mejorar el soporte ofrecido y de acuerdo con el correo remitido en su día y las instrucciones recibidas del Servicio de Informática, se hace necesaria la apertura de una incidencia a través de la herramienta Service Manager accesible mediante el siguiente enlace <http://informatica-incidencias.chj.es:8080/webtier-9.20/ess.do>

Un saludo

Asistencia Técnica Informática - ATOS
Confederación Hidrográfica del Júcar
Tel: 96 393 88 15

De: Molinero Collada, María Rosario
Enviado el: lunes, 20 de marzo de 2017 10:06
Para: CHJDesarrollo; OPHAdminInfor; **[Redacted]**
CC: SI_Proyectos; Informática, Incidencias
Asunto: Actualización de Servidores de prueba de la CHJ MIÉRCOLES 22 DE MARZO

El próximo 23 de Marzo , a partir de las 15:00 h se van a instalar las actualizaciones críticas y de seguridad de los siguientes servidores de la CHJ considerados como de prueba.
Es posible que en algún caso haya que reiniciar el servidor.

Sonrisas y Lagrimas. WannaCry.



Informática, Incidencias

[Redacted] CHJDesarrollo; OPHAdminInfor; [Redacted] SI_Proyectos; + 1

29/03/2017

RE: Actualización de Servidores de la CHJ.

Buenas tardes,

Han terminado las tareas de actualización de los servidores correctamente.

Con el fin de mejorar el soporte ofrecido y de acuerdo con el correo remitido en su día y las instrucciones recibidas del Servicio de Informática, se hace necesaria la apertura de una incidencia a través de la herramienta Service Manager accesible mediante el siguiente enlace <http://informatica-incidencias.chj.es:8080/webtier-9.20/ess.do>

Un saludo

Asistencia
Confederación
Tel: 96 35

45 días después.....

De: [Redacted]

Enviado el: jueves, 23 de marzo de 2017 12:20

Para: CHJDesarrollo; OPHAdminInfor; Sanchis Pastor, Emilio Luis; Barragán Benítez, Francisca

CC: SI_Proyectos; Informática, Incidencias

Asunto: Actualización de Servidores de la CHJ.

Dentro de las tareas de actualizaciones críticas y de seguridad que va liberando Microsoft, os informamos que este próximo **miércoles 29 de Marzo** a partir de las 15:00 horas empezaremos la actualización **del resto de servidores de la CHJ que no se actualizaron el día 22 de Marzo.**

Son los siguientes:

Sonrisas y Lagrimas. WannaCry.

CCN-CERT [no-reply@ccn-cert.cni.es]

Acciones

Para: SI_Proyectos

Bandeja de entrada

viernes, 12 de mayo de 2017 13:33

- Renviaste este mensaje el 12/05/2017 13:35.

ccn-cert
centro criptológico nacional



ALERTAS

Ataque masivo de ransomware que afecta a un elevado número de organizaciones españolas

Publicado el:
12/05/2017

Se ha alertado de un ataque masivo de ransomware a varias organizaciones que afecta a sistemas Windows cifrando todos sus archivos y los de las unidades de red a las que estén conectadas, e infectando al resto de sistemas Windows que haya en esa misma red.

El ransomware, una versión de WannaCry, infecta la máquina cifrando todos sus archivos y, utilizando una vulnerabilidad de ejecución de comandos remota a través de SMB, se distribuye al resto de máquinas Windows que haya en esa misma red.

Los sistemas afectados son:
Microsoft Windows Vista SP2
Windows Server 2008 SP2 and R2 SP1
Windows 7

Sonrisas y Lagrimas. WannaCry.

Responder Responder a todos Reenviar

Información y recomendaciones eventos de seguridad de este fin de semana

Leal García, José Manuel

Para: chj; aatt

domingo, 14 de mayo de 2017 20:59

Buenas tardes,
El viernes a última hora se detectó un software malicioso que cifra los archivos y pide un rescate a los usuarios de red que tenga conexión. El ransomware, utilizado para la explotación de vulnerabilidades de compartición de archivos.

El parche / solución se instaló en la mayoría de los equipos el 12 de marzo (hace más de un mes y medio). Esto es así, porque, el software que se ejecuta en los equipos y servidores necesita ser probado con anterioridad y el proceso de verificación y prueba de los parches no es rápido ni trivial.

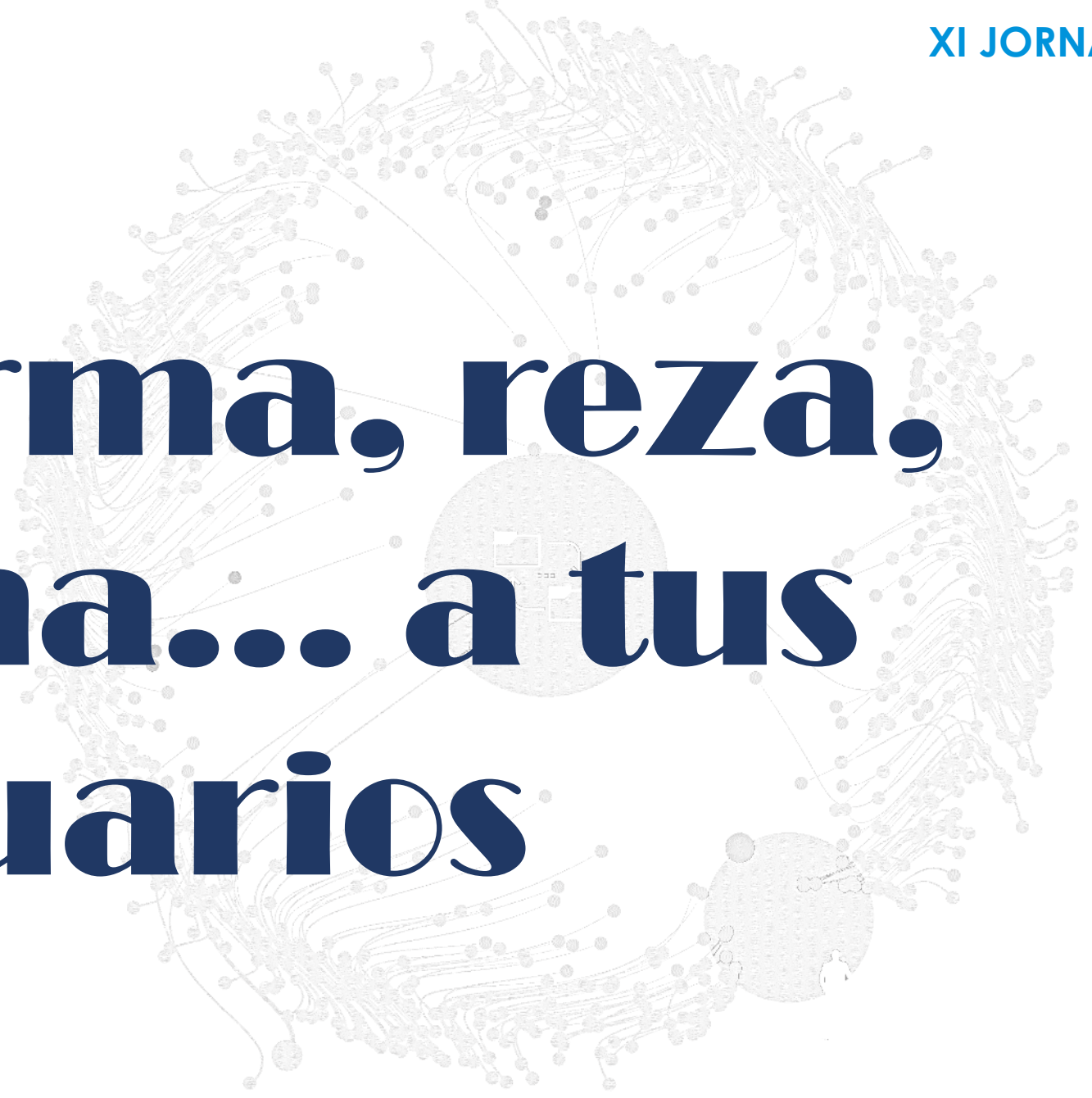
Ante cualquier duda o problema, no hacer nada y contactar inmediatamente con el 8815, o con Antonio Grimaltos (responsable de seguridad de la CHJ)

Esperamos que esta información os haya tranquilizado y aclarado alguna que otra duda.

Lecciones aprendidas....

Cuenta con tus usuarios, informales y hazles sentir parte de el Sistema de Gestión de la Seguridad de la Información





**Forma, reza,
ama... a tus
usuarios**

Forma, reza, ama... (a los usuarios)

Artículo 5. *La seguridad como un proceso integral.*

1. La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.
2. Se prestará la **máxima atención** a la **concienciación** de las **personas que intervienen en el proceso** y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

Forma, reza, ama... (a los usuarios)

5.2.3 Concienciación [mp.per.3].

Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.

En particular, se recordará regularmente:

- a) La normativa de seguridad relativa al buen uso de los sistemas.
- b) La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
- c) El procedimiento de reporte de incidentes de seguridad, sean reales o falsas alarmas.

Forma, reza, ama... (a los usuarios)

¿Que ha pasado? entre:

----- Mensaje original -----

De: [REDACTED]
Fecha: 20/03/2017 7:00 (GMT+01:00)
Para: "Grimaltos Vidal, Antonio" <Antonio.Grimaltos@chj.es>
Cc: "Informática, Incidencias" <informatica@chj.es>
Asunto: Re: **NO ABRIR ARCHIVO ADJUNTO** AL CORREO DE Miguel Angel Martinez Martinez

Buenos días,
Al recibir el correo opté por la apertura del mismo, llegando a descargar el audio. [REDACTED]
Como me recomendáis que proceda

De: Grimaltos Vidal, Antonio
Enviado: domingo, 19 de marzo de 2017 12:43
Para: chj
CC: Informática, Incidencias
Asunto: **NO ABRIR ARCHIVO ADJUNTO** AL CORREO DE Miguel Angel Martinez Martinez

Buenos días:

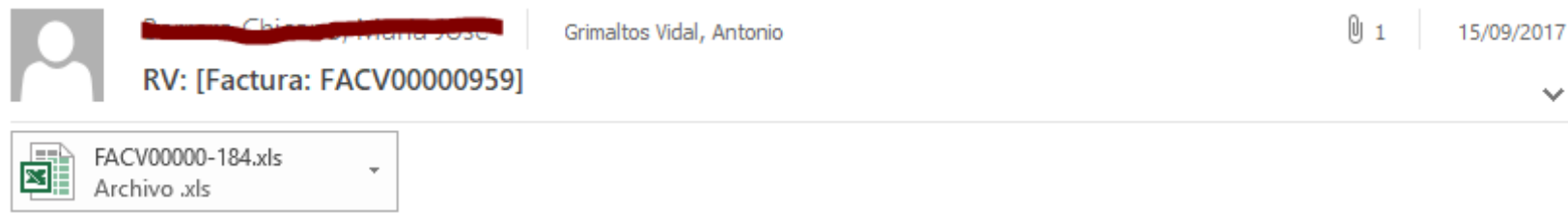
El pasado día 17 de marzo sobre las 17:30 de la tarde, recibimos todos incluso algunos por ducplicado un correo que en principio proviene de una direccion de correo legítimo de la CHJ.

Dicho correo llevaba un **archivo adjunto** far_from_love.mp3, en principio un **archivo** de audio inofensivo, dicho **archivo** se adjuntó sin conocimiento del usuario.

NO LO ABRAIS, CONTIENE UN **ARCHIVO** CON CODIGO MALICIOSO. SI POR CACSUALIDAD ALGUIEN LO HA ABIERTO, QUE SE PONGA EN CONTACTO CON EL SERVICIO DE INFORMATICA Y LO COMUNIQUE.

Forma, reza, ama... (a los usuarios)

Y esto:



Hola Antonio,
te paso el correo sospechoso, muchas gracias.
Saludos

[Redacted signature]

De: lourditaspimpinela@mi.madridtel.es [mailto:lourditaspimpinela@mi.madridtel.es]

Enviado el: jueves, 14 de septiembre de 2017 13:11

Para: [Redacted email address]

Asunto: [Factura: FACV00000959]

Estimados Sres

Les remitimos la factura adjunta al correo.

Reciban un cordial saludo

:ne de una direccion de

nocimiento del usuario.

NO LO ABRAIS, CONTIENE UN **ARCHIVO** CON CODIGO MALICIOSO. SI POR CACSUALIDAD ALGUIEN LO HA ABIERTO, QUE SE PONGA EN CONTACTO CON EL SERVICIO DE INFORMATICA Y LO COMUNIQUE.

Forma, reza, ama... (a los usuarios)



 **[Redacted Name]** | Grimaltos Vidal, Antonio | 1 | 14/09/2017
RV: [Factura: FACV00000870]

 FACV00000-722.xls
Archivo .xls

Antonio, me ha entr
podría ser bueno (fa
acabo de enviar.

 **[Redacted Name]** | Grimaltos Vidal, Antonio | 1 | 14/09/2017
RV: [Factura: FACV00000647]

 FACV00000-883.xls
Archivo .xls

Antonio, me ha entrado este correo con factura adjunta. Lo cierto es que esta vez el CC si es trabajador de la casa por lo que sí podría ser bueno (facturas de locomoción, tal vez) pero te lo envío por la similitud con los maliciosos y con otro que te voy a enviar a continuación en el que en CC está el Jefe de Personal.

Forma, reza, ama... (a los usuarios)



NORMAS DE USO SEGURO

BUENAS PRACTICAS EN EL USO DE RECURSOS INFORMÁTICOS DE LA CHJ

Los sistemas de información son un activo valioso para la CHJ, y sus usuarios deberán utilizarlos de forma segura y responsable. Será responsabilidad de cada empleado siempre que haga uso de dichos sistemas actuar evitando abusar de los mismos y emplearlos de forma que se mantenga el buen nombre y la reputación de la CHJ.

En este sentido, todo trabajador, en el ejercicio de sus funciones, deberá observar las directrices para su adecuado uso que detallan en los siguientes apartados.

VI. PROPIEDAD INTELECTUAL.

Respecto a los programas utilizados en la CHJ, se establece lo siguiente:

- Tal y como se ha indicado en el punto 4.1.2 *Sistemas de información*, para utilizar programas informáticos protegidos por la propiedad intelectual, la CHJ debe disponer de la correspondiente licencia.
- Los programas informáticos propiedad de la CHJ están protegidos por la propiedad intelectual, por lo que está estrictamente prohibida su reproducción, modificación, cesión o comunicación sin la debida autorización.
- Queda estrictamente prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier otro tipo de obra o invención protegida por la propiedad intelectual sin previa autorización.

VII. TRASLADO O RETIRADA DE MATERIAL

En cuanto al traslado o retirada del material de la CHJ, las indicaciones a seguir se indican a continuación:

- Los desplazamientos de activos hardware, software o información, recogidos dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) fuera de las instalaciones de la CHJ, deberán ser previamente autorizados por el Responsable de Seguridad de la información
- La autorización deberá solicitarse a través del gestor de incidencias, y toda salida deberá ser consignada en un registro de salida de material.
- El registro de salida de material se almacenará en el gestor documental de la CHJ y se comprobará periódicamente para garantizar el retorno de los activos.

2. Comunicaciones seguras.

I. COMUNICACIONES MÓVILES

El uso responsable y seguro de las comunicaciones móviles se establece en una serie de normas desarrolladas en el *Procedimiento de Usuarios y Contraseñas*. En dicho procedimiento, se establecen las medidas de seguridad necesarias para garantizar un acceso seguro y proteger aquellos activos de la CHJ pertenecientes al alcance del Sistema de Gestión de Seguridad de la Información (SGSI).

II. CORREO ELECTRÓNICO

Para un uso adecuado del correo electrónico corporativo se deben seguir las siguientes indicaciones:

- La configuración de las cuentas de correo (posibilidades de envío y recepción, tamaño máximo permitido, etc.) se establecerá para cada usuario en función de sus necesidades de trabajo. Cualquier modificación sobre estas configuraciones deberá solicitarse al responsable pertinente.

Forma, reza, ama... (a los usuarios)

Normativa de uso seguro de los recursos informáticos de la CHJ

Noviembre 2017

Forma, reza, ama... (a los usuarios)

El arte del engaño

Phising

Ingeniería social

Refinada al aroma de APT

Es fácil hacer el mal si sabes como hacerlo

Forma, reza, ama... (a los usuarios)

De todas formas queda mucho camino...:



GestionIncidencias

Grimaltos Vidal, Antonio

15/09/2017

Aviso de registro de nueva interacción SD52582

Se han quitado los saltos de línea adicionales de este mensaje.

Contacto: Grimaltos Vidal, Antonio

Su petición ha sido registrada con los siguientes datos:

Nº Interacción: SD52582

Fecha de creación: 15/09/2017 09:39:14

Descripción breve: **[Redacted]** ha abierto Factura

Servicio: Incidentes de Seguridad

Para consultar el estado de su petición, o para cualquier otra cuestión relacionada, puede ponerse en contacto con Asistencia Técnica informática de la CHJ, indicando el número de interacción que le ha sido asignado.

También puede consultar el estado de la petición a través de la siguiente web:

<http://informatica-incidencias.chj.es:8080/webtier-9.20/ess.do>



A quien Engaño Bad Rabbit.

Artículo 36. *Capacidad de respuesta a incidentes de seguridad de la información.*

El Centro Criptológico Nacional (CCN) articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (Centro Criptológico Nacional-Computer Emergency Reaction Team), que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN.

Las Administraciones Públicas notificarán al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados en relación con la categorización de sistemas recogida en el Anexo I del presente real decreto.

A quien Engaño Bad Rabbit.

4.3.7 Gestión de incidentes [op.exp.7].

Categoría MEDIA

Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, incluyendo:

- a) Procedimiento de reporte de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación.
- b) Procedimiento de toma de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.
- c) Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.

d) Procedimientos para informar a las partes interesadas, internas y externas.

A quien Engaño Bad Rabbit.



John Kelly

@mrjohnkelly73 · 24 oct.

11 5

@GossiTheDog Looks like a fake flash installer as the initial vector



Jiri Kropac @jiriavirlab

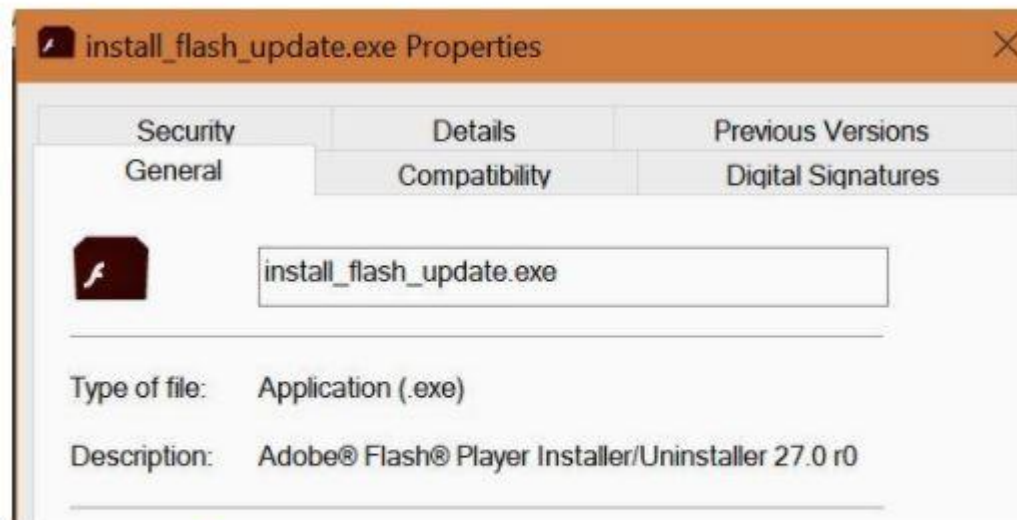
#ESET confirms Discoder/#Petya/#BadRabbit campaign live today, incorporating #Mimikatz distributed via fake flash. More info soon.



Lorenzo Franceschi-Bicchierai

@lorenzoFB · 24 oct.

A new ransomware called Bad Rabbit (variant of Petya) is spreading through Ukraine and Russia
motherboard.vice.com/en_us/article/...



Kevin Beaumont @GossiTheDog · 24 oct.

This is the #BadRabbit dropper - but it has creds to spread around by looks of it.

82 50

A quien Engaño Bad Rabbit.



Sobre 'Bad Rabbit'

Tiene similitudes con WannaCry y Petya, aunque es seguro que no alcanzará el nivel de propagación de estos.

Hasta ahora se ha distribuido a través de páginas web comprometidas, que solicitan al usuario instalar una falsa actualización de Flash Player. Una vez instalado en los equipos pide un rescate para recuperar el acceso a los datos.

La forma de operar es similar a la de otros de tipos de ransomware: encripta el contenido del equipo y exige un pago, en este caso de 0.05 bitcoins (unos 240€), a cambio de poder volver a tener acceso a la información.

Lo que hace que este malware sea más peligroso que los típicos ataques de ransomware que se distribuyen de manera similar, es su capacidad de propagación a través de la red interna de la empresa.



El 24 de octubre apareció el ransomware
principalmente a usuarios

A quien Engaño Bad Rabbit.



PRODUCTS & SERVICES

COMPANY

INSIGHTS

PARTNERS

BLOG

GET A DEMO



Oct
24
2017

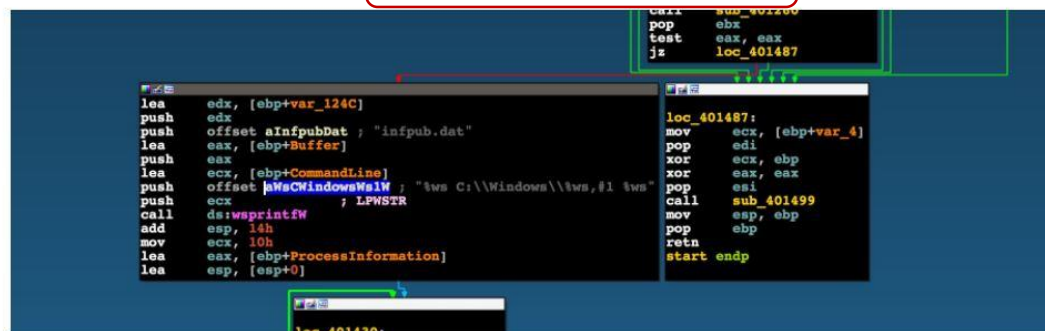
Subscribe to receive weekly
blog updates

Email Address

☐ Cybereason Blog

SUBSCRIBE

Cybereason researcher discovers vaccine for Bad Rabbit ransomware



POST BY: LITAL ASHER-DOTAN

Cybereason researcher [Amit Serper](#) has developed a vaccine to prevent the Bad Rabbit data-encrypting malware from infecting machines.

Bad Rabbit, which spread across Europe on Tuesday, targets enterprise networks by employing similar methods that [NotPetya](#) used to infect computers around the globe in June. Bad Rabbit's full impact is still unknown. So far, the attack has affected airports, news agencies and train stations in the Ukraine, Russia, Turkey and Germany, according to [media reports](#).

Here's the encryption screen:

```

Oops! Your files have been encrypted.

If you see this text, your files are no longer accessible.
You might have been looking for a way to recover your files.
Don't waste your time. No one will be able to recover them without our
decryption service.

```

A quien Engaño Bad Rabbit.

Vacuna BadRabbit que creamos en la CHJ

Copia 2 ficheros de solo lectura desde el directorio \\chj.es [buscar host]\NETLOGON\BadRabbit en el directorio C:\Windows indicado para evitar la ejecución del Malware, ya que al ser de solo lectura, no puede sobrescribirlos, y no prosigue la ejecución del malware (al igual que Petya)

C:\windows\infpub.dat [buscar host] y C:\Windows\cscc.dat [buscar host]

Se han seguido las indicaciones de este artículo, y la GPO creada anteriormente para la vacuna contra Petya

<https://www.cybereason.com/blog/cybereason-researcher-discovers-vaccine-for-badrabbit-ransomware>

Se adjunta correo electrónico donde se explica que se ha creado la GPO Vacuna BadRabbit para evitar el contagio.

Se comprueba en los equipos cuya IP se indica, que los ficheros indicados ubicados en C:\Windows son los mismos que en \\chj.es [buscar host]\netlogon, son de solo lectura, y están vacíos.

.../...

¿Qué Falta...?

A quien Engaño Bad Rabbit.

Incid

3) ANÁLISIS DEL EVENTO

Los payloads relacionados con MALWARE-OTHER Win.Ransomware.BadRabbit propagation via SMB2 transfer attempt son:

... BadRabbit\csc.dat [buscar host] ...

... BadRabbit\inpub.dat [buscar host] ...

Se han detectado comunicaciones SMB sospechosas, donde se encuentran los patrones inpub.dat [buscar host] y csc.dat [buscar host], los cuales podrían estar relacionados con el ransomware BadRabbit [1, 2].

Este ransomware tiene la capacidad de propagarse vía SMB como un gusano escaneando la red en busca de componentes SMB abiertos:

- admin
- atsvc
- browser
- eventlog
- lsarpc
- netlogon
- ntsvcs
- spoolss
- samr
- srsvcs
- scerpc
- svcctl
- wkssvc

Ejecuta Mimikatz en el equipo comprometido para recolectar credenciales, incluyendo también una lista de nombres de usuario y contraseñas, para lograr la propagación.

Cuando se encuentran las credenciales funcionales, se descarga el archivo inpub.dat [buscar host] en el directorio de Windows y se ejecuta a través de SCManager y rundll.exe [buscar host].

Más información:

[1] - <https://www.virustotal.com/en/file/579fd8a0385482fb4c789561a30b09f25671e86422f40ef5cca2036b28f99648/analysis/> [buscar "www.virustotal.com"]

[2] - <https://www.welivesecurity.com/la-es/2017/10/25/bad-rabbit-not-petya-de-vuelta/> [buscar "www.welivesecurity.com"]

A quien Engaño Bad Rabbit.

[Historial](#)[Mostrar todo el texto citado](#) — [Mostrar cabeceras completas](#)

#

Mar Oct 31 16:37:33 2017

satinet_chjucar_user (User SATINET_CHJUCAR) - Comentarios añadidos

[Responder](#) [Comentario](#)

Este tráfico debe corresponderse a la GPO Vacuna BadRabbit que copia 2 ficheros de solo lectura desde el directorio \\chj.es [buscar host]\NETLOGON\BadRabbit en el directorio C:\Windows indicado para evitar la ejecución del Malware, ya que al ser de solo lectura, no puede sobrescribirlos, y no prosigue la ejecución del malware (al igual que Petya)

[Descargar \(sin título\)](#)[con cabeceras](#)[text/plain 1KiB](#)

C:\windows\infpub.dat [buscar host] y C:\Windows\cscc.dat [buscar host]

Se han seguido las indicaciones de este artículo, y la GPO creada anteriormente para la vacuna contra Petya

<https://www.cybereason.com/blog/cybereason-researcher-discovers-vaccine-for-badrabbit-ransomware> [buscar "www.cybereason.com"]

Se adjunta correo electrónico donde se explica que se ha creado la GPO Vacuna BadRabbit para evitar el contagio.

Se comprueba en los equipos cuya IP se indica, que los ficheros indicados ubicados en C:\Windows son los mismos que en \\chj.es [buscar host]\netlogon, son de solo lectura, y están vacíos.

Quedamos a la espera de que nos indiquéis si deseáis algún análisis/investigación adicional, o si el CCN-CERT desea alguna ampliación de información, o si podemos proceder al cierre de la incidencia.

Atentamente,

Asunto: RV Ataque de nuevo malware BadRabbit en Europa del Este y Rusia.msg [buscar host]

[Descargar RV Ataque de nuevo malware BadRabbit en Europa del Este y Rusia.msg](#)

El cuerpo del mensaje no se muestra porque no es texto plano.

[application/octet-stream 128KiB](#)

Mar Oct 31 11:35:46 2017

inet_oper2 (SAT-INET CCN-CERT) - Caso creado

[Responder](#) [Comentario](#)

Asunto: [SAT-INET] Detectado posible infección por BadRabbit - CHJUCAR

Fecha: Tue, 31 Oct 2017 11:35:46 +0100

Para: incidentes@ccn-cert.cni.es [buscar email][Investigar a] [buscar "ccn-cert.cni.es"]

Desde: sat-inet@ccn-cert.cni.es [buscar email][Investigar a] [buscar "ccn-cert.cni.es"]

A quien Engaño Bad Rabbit.

Vacuna Bad Rabbit. Esperemos que os sirva.

Grimaltos Vidal, Antonio

Para: ccn@cni.es
Cc: info@ccn-cni.es

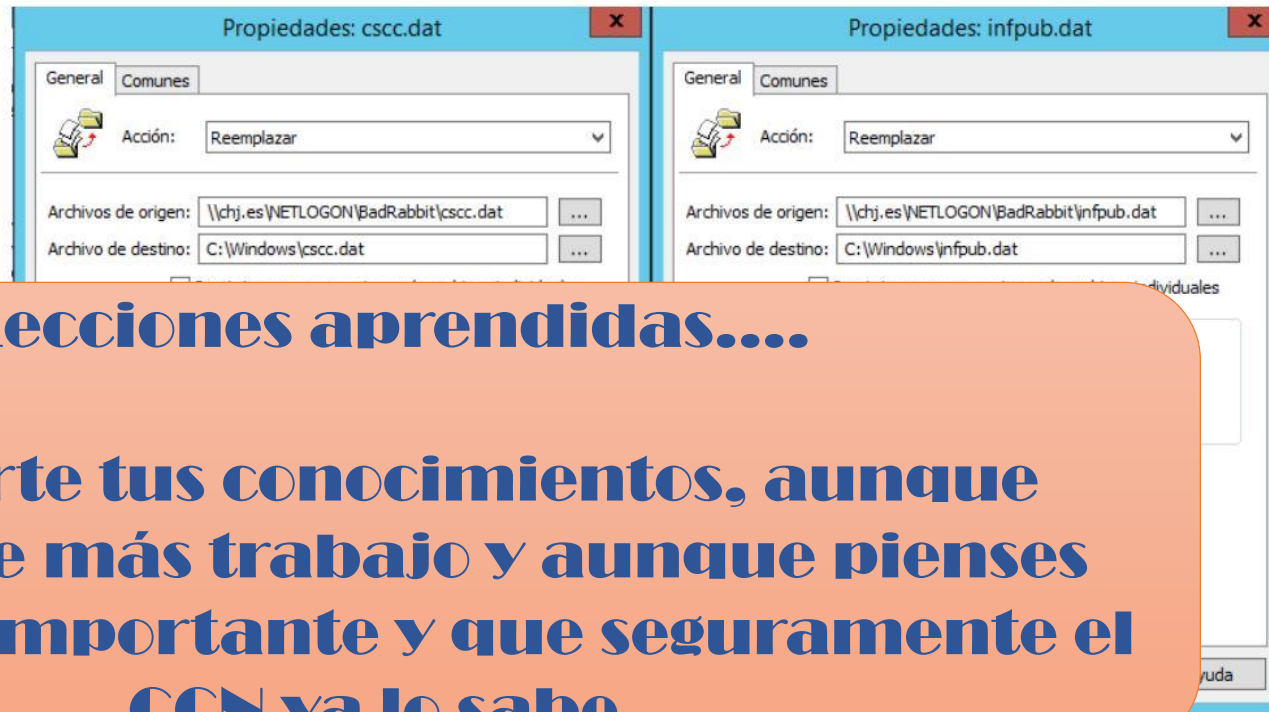
Elementos enviados

Se parece mucho a lo que hemos hecho con otros Ransomware:

Bloqueado el acceso a la IP 185.149.120.3/32

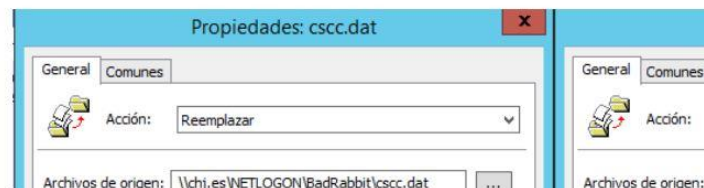
Se ha creado una GPO Vacuna BadRabbit que crear 2 ficheros de solo lectura en el directorio indicado para evitar

C:\windows\inpub.dat y C:\Windows\cscc.dat



Lecciones aprendidas....

Comparte tus conocimientos, aunque signifique más trabajo y aunque pienses que no es importante y que seguramente el CCN ya lo sabe.



la GPO Vacuna BadRabbit copia 2 ficheros de solo lectura desde el directorio [\\chj.es\NETLOGON\BadRabbit](https://chj.es/NETLOGON/BadRabbit) en el directorio C:\Windows indicado para evitar la ejecución del Malware, ya que al ser de solo lectura, no puede sobrescribirlos, y no prosigue la ejecución del malware (al igual que Petya)

C:\windows\inpub.dat y C:\Windows\cscc.dat

Se han seguido las indicaciones de este artículo, y la GPO creada anteriormente para la vacuna contra Petya

<https://www.cybereason.com/blog/cybereason-researcher-discovers-vaccine-for-badrabbit-ransomware>

www.ccn-cert.cni.es





Hacer que continúe aportando ese nivel de Seguridad y que seamos capaces de adaptarlo a los nuevos ataques y a las nuevas tecnologías que surgen



Hacer que continúe aportando ese nivel de Seguridad y que seamos capaces de adaptarlo a los nuevos ataques y a las nuevas tecnologías que surgen

Es nacional, es de toda una nación y debemos abordar este reto entre todos, ya que mejorar este esquema.

Mejorar la seguridad del conjunto y nos permitirá reducir el esfuerzo individual



Hacer que continúe aportando ese nivel de Seguridad y que seamos capaces de adaptarlo a los nuevos ataques y a las nuevas tecnologías que surgen

Es nacional, es de toda una nación y debemos abordar este reto entre todos, ya que mejorar este esquema, mejorar la seguridad del conjunto, nos permitirá reducir el esfuerzo individual

Esquema: Es la expresión gráfica del subrayado que contiene de forma sintetizada las ideas principales, las ideas secundarias y los detalles del texto.



Hacer que continúe aportando ese nivel de Seguridad y que seamos capaces de adaptarlo a los nuevos ataques y a las nuevas tecnologías que surgen

Es nacional, es de toda una nación y debemos abordar este reto entre todos, ya que mejorar este esquema, Mejorar la seguridad del conjunto, nos permitirá reducir el esfuerzo individual

Intuitivo
Esquema: Es la expresión gráfica del subrayado que contiene de forma sintetizada las ideas principales, las ideas secundarias y los detalles del texto.

Sencillo



Hacer que continúe aportando ese nivel de Seguridad y que seamos capaces de adaptarlo a los nuevos ataques y a las nuevas tecnologías que surgen

Es nacional, es de toda una nación y debemos abordar este reto entre todos, ya que mejorar este esquema. Mejorar la seguridad del conjunto, nos permitirá reducir el esfuerzo individual

Que siga siendo como un esquema,
fácil de entender y sencillo de aplicar

- https://es.wikipedia.org/wiki/Esquema_Nacional_de_Seguridad
- <https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330>
- <https://www.boe.es/buscar/act.php?id=BOE-A-2007-12352>
- <https://www.boe.es/buscar/doc.php?id=BOE-A-2015-10565>
- <https://www.ccn-cert.cni.es/ens.html>
- <http://boe.es/boe/dias/2015/10/02/pdfs/BOE-A-2015-10566.pdf>
- <https://www.ccn-cert.cni.es/publico/ens/ens/index.html>
- Antonio.Grimaltos@chj.es

➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

➤ Síguenos en

