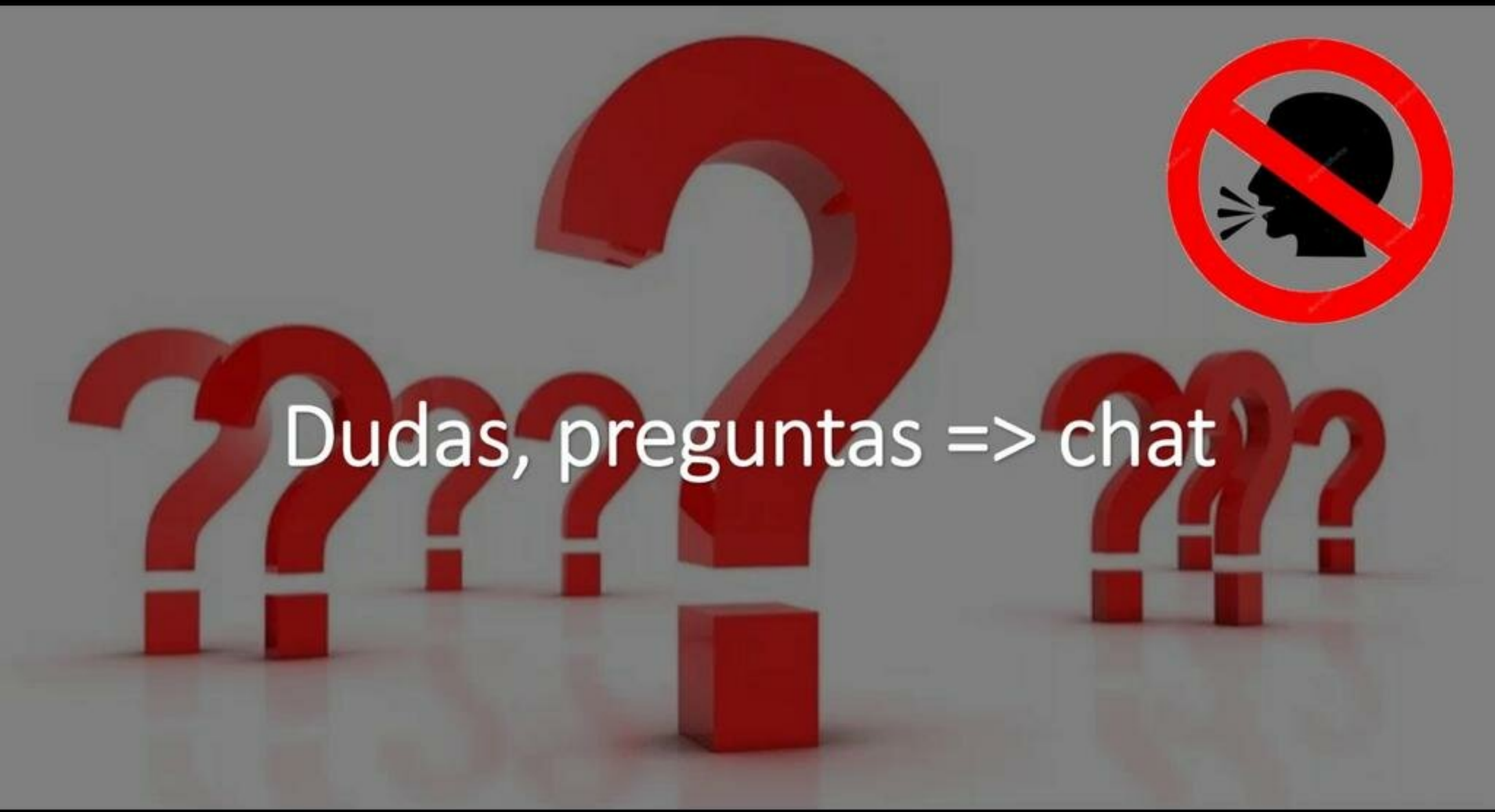
Webinar gratuito
Ciberseguridad empresarial: amenazas cotidianas y cómo prevenirlas

Transformación digital en PYMES

Oficinas de Transformación Digital

COLEGIO OFICIAL DE INGENIEROS INDUSTRIALES DEL PRINCIPADO DE ASTURIAS

EWALA


Dudas, preguntas => chat

Ponentes

Rubén Fernández Álvarez

Responsable Co-fundador y CEO en Ewala IT Services

Facundo David Gallo

Co-fundador y CSO (gerente de seguridad) en Ewala IT Services.

Webinar: Ciberseguridad empresarial: amenazas cotidianas y cómo prevenirlas

Programa:

- **Introducción: qué es la ciberseguridad y su importancia en el proceso de digitalización.**
- **Riesgos más comunes y sus posibles repercusiones en la actividad de la empresa.**
- **Ejemplos de riesgos de ciberseguridad.**
- **Consecuencia de los ataques de ciberseguridad: datos reales de fugas de datos producidas, ataques recibidos, actividad paralizada y otras consideraciones relevantes sobre el normal funcionamiento interrumpido de la empresa.**
- **Conclusiones.**


Página web
www.coiias.es
Redes sociales
www.linkedin.com/in/coiias/
Twitter/Fb/Instragram: @coiias
Correo electrónico
coiias@coiias.es

Contacto

EWALA

COLEGIO OFICIAL DE
INGENIEROS INDUSTRIALES
DEL PRINCIPADO DE ASTURIAS

Transformación digital en **PYMES**

Oficinas de Transformación Digital

Ingeniería Industrial. Pasado, presente y futuro.

Gracias por la atención.

Autoguardado · Seminario - Guardado en Este PC · Buscar · Facundo David Gallo

Archivo Inicio Insertar Diseño Transiciones Animaciones Presentación con diapositivas Revisar Vista Ayuda · Compartir · Comentarios

Pegar · Portapapeles · Nueva diapositiva · Volver a usar las diapositivas · Diseño · Restablecer · Sección · Diapositivas · Fuente · Párrafo · Formas · Organizar · Estilos rápidos · Relleno de forma · Contorno de forma · Efectos de forma · Dibujo · Buscar · Reemplazar · Seleccionar · Edición · Dictar · Voz · Ideas de diseño · Diseñador

1 2 3 4 5 6 7

Ciberseguridad empresarial: amenazas cotidianas y cómo prevenirlas

15 de junio de 2021

Organiza:

Colegio Oficial de Ingenieros Industriales del Principado de Asturias

Colabora:

11:08
15/06/2021

Diapositiva 1 de 25 · Español (España) · Notas · 91 %

iberseguridad empresarial: amenazas cotidianas y cómo prevenirlas

15 de junio de 2021

ganiza:

Colegio Oficial de
Ingenieros Industriales
del Principado de Asturias

Colabora:

Qué es Ewala

- Start up asturiana.
- Líneas de negocio:
  - Consultoría de ciberseguridad para empresas.
  - Desarrollo de productos de seguridad propios.
- Objetivos:
  - Protección del sistema productivo.
  - Divulgación científica y concienciación del usuario.
  - Aportar valor a nuestra sociedad:
    - Creación de empleo.
    - Exportación.

énes somos?

Rubén Fernández

dador y CEO en Ewala IT Services.

os de experiencia profesional:

os en banca

os en distribución comercial

o en el sector tecnológico

Licenciado en Economía por la Universidad

MBA por el IUDE

Especialista universitario en comercio exteri
UNED

énes somos ?

Facundo Gallo

dador y CSO (gerente de seguridad)
la IT Services.

os en ciberseguridad.

miento de Barcelona, CESICAT, Guardia
Policía Nacional, Centro de Regulación
ca...)

Doctorando en Criminología (línea de investigación: Cibercrimen) (UGR-presente).

Máster Universitario en Divulgación Científica (VIU-CS 2019).

Máster Universitario en Seguridad de la Información y de las Comunicaciones (UOC-2017).

Ingeniero en Tecnologías de la Información (UW-2015

CISM (Certified Information Security Manager)

ITIL (Certified IT Service Management)

:ales como la vida misma

s reales como la vida misma

os escenarios y dos actores: un atacante (Menganito) y una víctima (Fulanito):

Menganito

Fulanito

nominador común: la red IT empresarial.

Router

Firewall

Red Interna

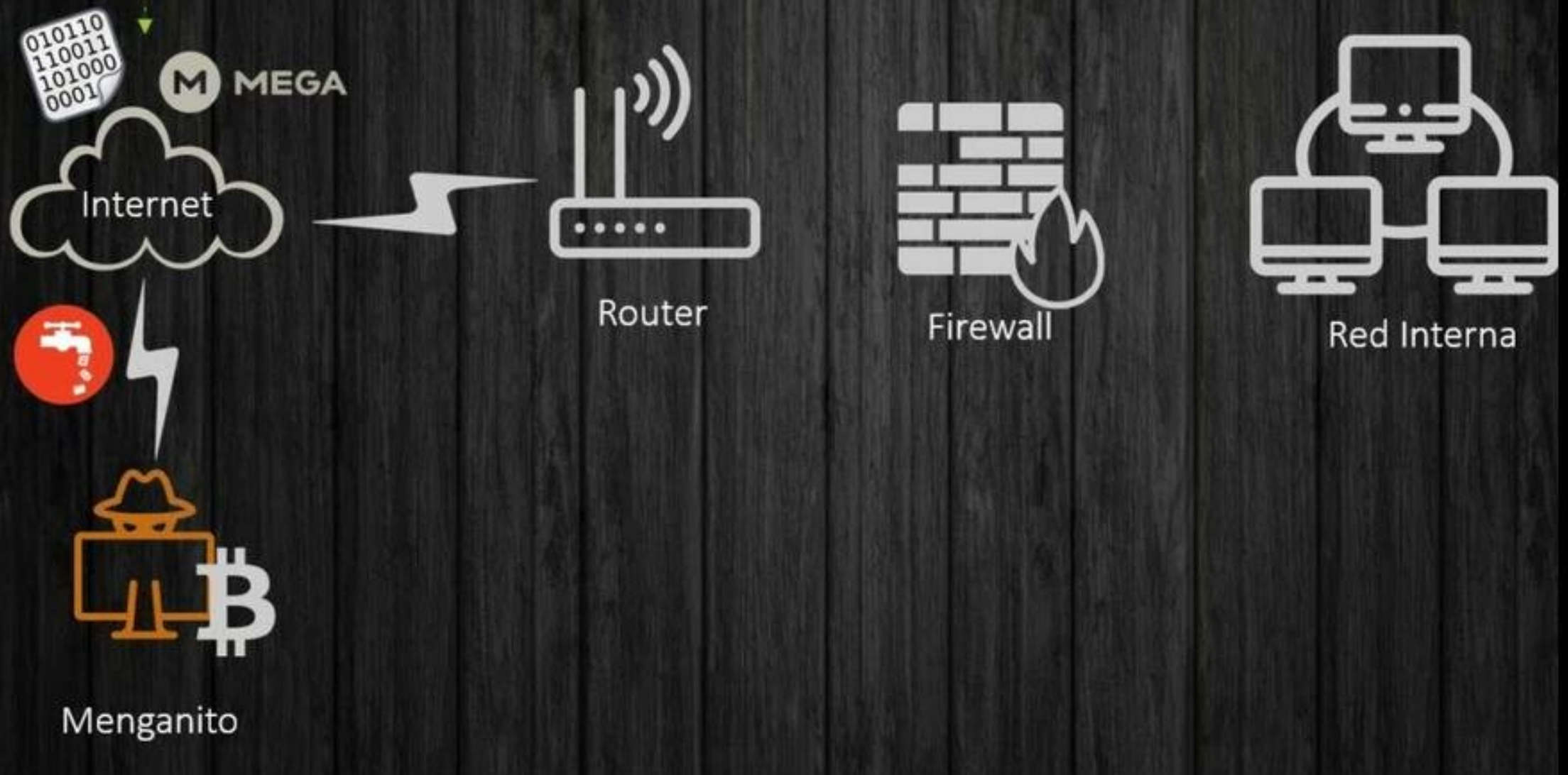
nario I

Fuga de Información (in)vuluntaria

ıario Fulanito comparte datos con otro compañero mediante Mega, Wetransfer o
amador y sube su código en Pastebin.

tenido de Fulanito se indexó o estaba mal securizado ¡Y esto Menganito lo sabe!

anito descarga los datos **sensibles**, y piensa venderlos o extorsionar a la empresa (pedi



ío I

Fuga de Información (in)vuluntaria: Posibles soluciones

io I Fuga de Información (in)vuluntaria: Posibles soluciones

e información

ación de un DLP (Data Loss Prevention) o un NGFW (Next Generation Firewall) son una
iva, pues ayudan a monitorizar y detectar los casos de fuga antes de que se produzcan.

s donde la información ya se encuentra en el mercado negro o bajo dominio público, la
ntelligence especializadas en Data Leak te permiten realizar detecciones tempranas, se
ntos fugados, contraseñas, usuarios, cuentas bancarias.

ón del uso de filesharing (aplicaciones públicas para compartir ficheros)

ación de un NGFW con capacidad de control de aplicaciones te permitirá determinar q
a de aplicaciones web deben bloquearse por defecto.

io II

El viejo truco que nunca falla

nario II

El viejo truco que nunca falla

ario Menganito ha fijado su objetivo en una empresa particular, en nuestro caso prác
ar a un empleado de la misma (Fulanito).

anito sabe que vulnerar un usuario interno es tener la llave del reino en sus manos.

Menganito envía un correo phishing, malware adjunto, BadUSB...

Pero... ¿Cómo consigue Menganito llegar hasta Fulanito?

Mediante una combinación de técnicas: ingeniería social e investig

Veamos un ejemplo...

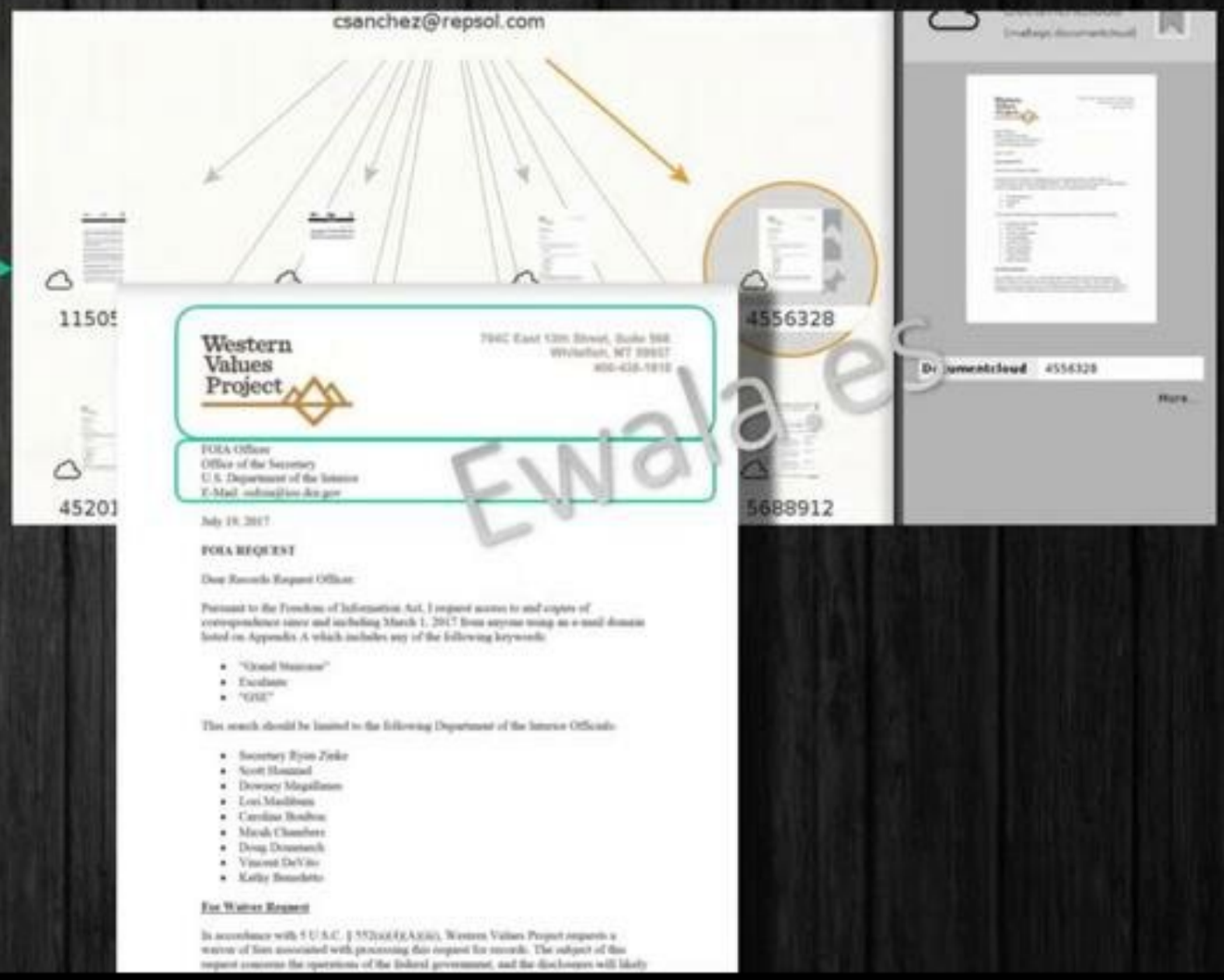
Escenario II

El viejo truco que nunca falla

Menganito realiza una recopilación de contactos de la empresa Repsol.

```
[*] Target: repsol.com

        Searching 0 results.
        Searching 100 results.
        Searching 200 results.
[*] Searching Google.

[*] No IPs found.

[*] Emails found: 20
---------------------
atencion.gas.gyp@repsol.com
cert@repsol.com
cireyg@repsol.com
cristian.ariel@servexternos.repsol.com
csanchez@repsol.com
dmarotol@repsol.com
erecruiting@repsol.com
especialidades@repsol.com
icharroaldefr@repsol.com
infous@repsol.com
jciordiar@repsol.com
last@repsol.com
prensa@repsol.com
protecciondedatos@repsol.com
rgpd.crc@repsol.com
saceess@repsol.com
sacgas@repsol.com
saclubes@repsol.com
sacportal@repsol.com
sacrq@repsol.com

[*] Hosts found: 9
---------------------
253drca.repsol.com
253dwww.repsol.com
altarepsolmas.repsol.com:195.76.35.226
chemicalsonline.repsol.com:161.71.42.70
proyectocanarias.repsol.com:104.83.25.221
rca.repsol.com:195.55.119.212
servexternos.repsol.com
www.quimica.repsol.com:195.76.35.226
www.repsol.com:104.83.25.221
```

Menganito fija un objetivo concreto y busca información sobre el mismo.



scenario II

El viejo truco que nunca falla

Menganito crea un correo fraudulento:

Para: csanchez@repsol.com

wvp_foia_doi request

To Whom IT May Concern,

Please, download and review the attached document, otherwise we will proceed to unsubscribe you as a collaborator

Regards.

Mark Stanley

FOIA Officer

Office of the Secretary

osfoia@ios.doi.gov

Western Values Project

8.62 KB 1 archivo adjuntado 1 imagen incrustada *Ocultar*

screen_shot_2018-11-26_at_12.05.49_pm.png

wvp_foia_doi_VIRUS.pdf

nario II El viejo truco que nunca falla

to ha aceptado el mail que envía Menganito y descarga su fichero adjunto en format
:ado la confianza de Fulanito.

nario II El viejo truco que nunca falla

l fichero adjunto contiene un malware que bien podría:

Propagarse por la red encriptando la información,
Conectarse a un panel de control remoto para ejecutar código malicioso desde internet.

Y ahora que está Menganito dentro y ha logrado persistencia...
¿Qué más podría hacer?

Por ejemplo, atacar los equipos de seguridad perimetral dejando a la empresa desprotegida ante ataques externos.

io II El viejo truco que nunca falla: Posibles soluciones

ón de ransomware

ar las nuevas tecnologías de antivirus (EDR) permiten detectar amenazas del tip
ortamiento del software gracias al uso de Inteligencia Artificial, entre otros facto
rimos de la vigilancia en dispositivos móviles, tendremos que optar por una solu

edida preventiva es la implantación de servicios SOC (Security Operations Center
izar sin interrupciones el tráfico de red y el comportamiento de los usuarios.

ción y remediación de ransomware

ar sistemas de backup y planes de recuperación ante desastres, así como tambié
identes.

ón de conexiones remotas (command and control)

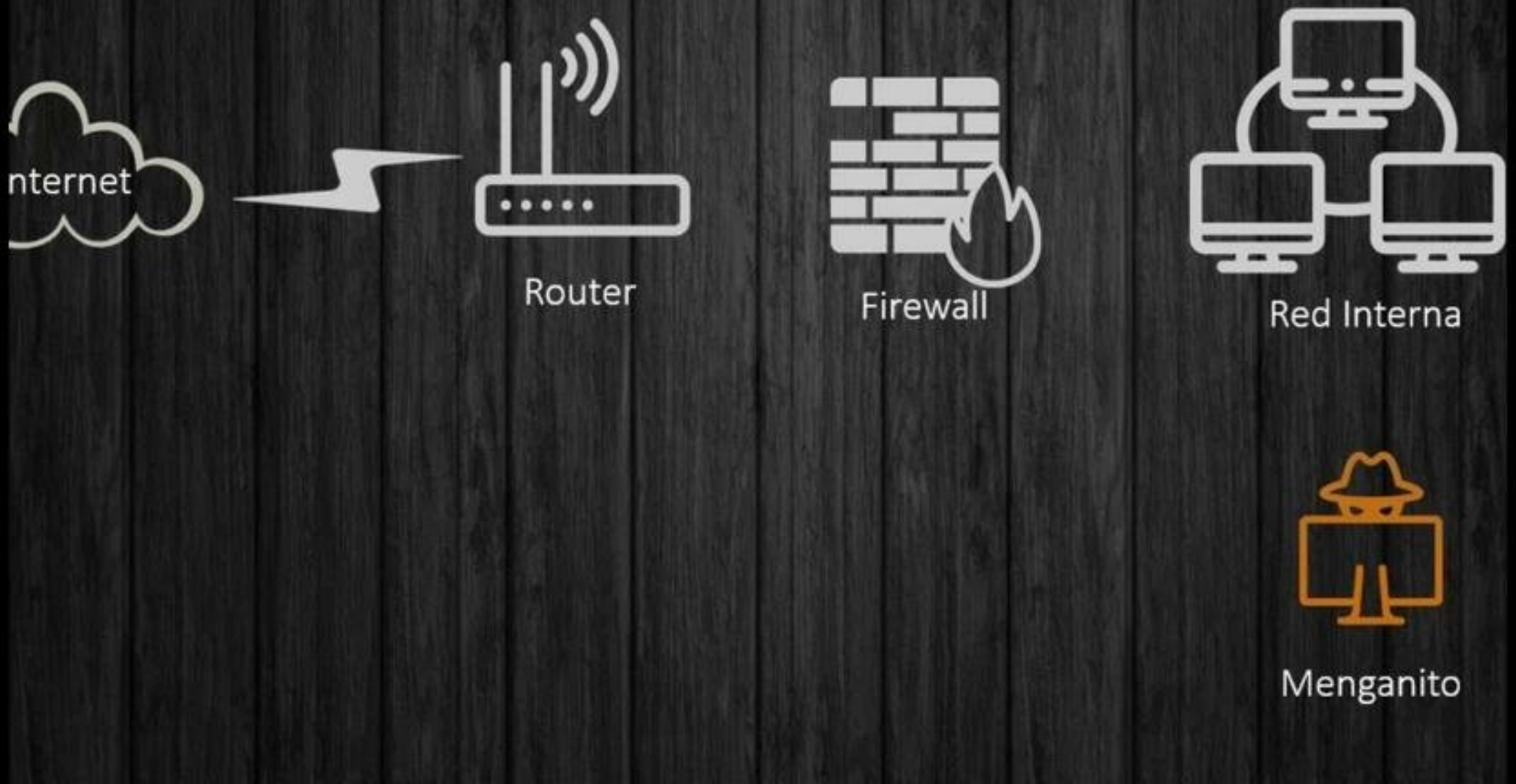
ión de un NGFW con capacidad IPS o sistema de seguridad a nivel de DNS.

ıo III

Infiltrado o empleado descontento (Insider)

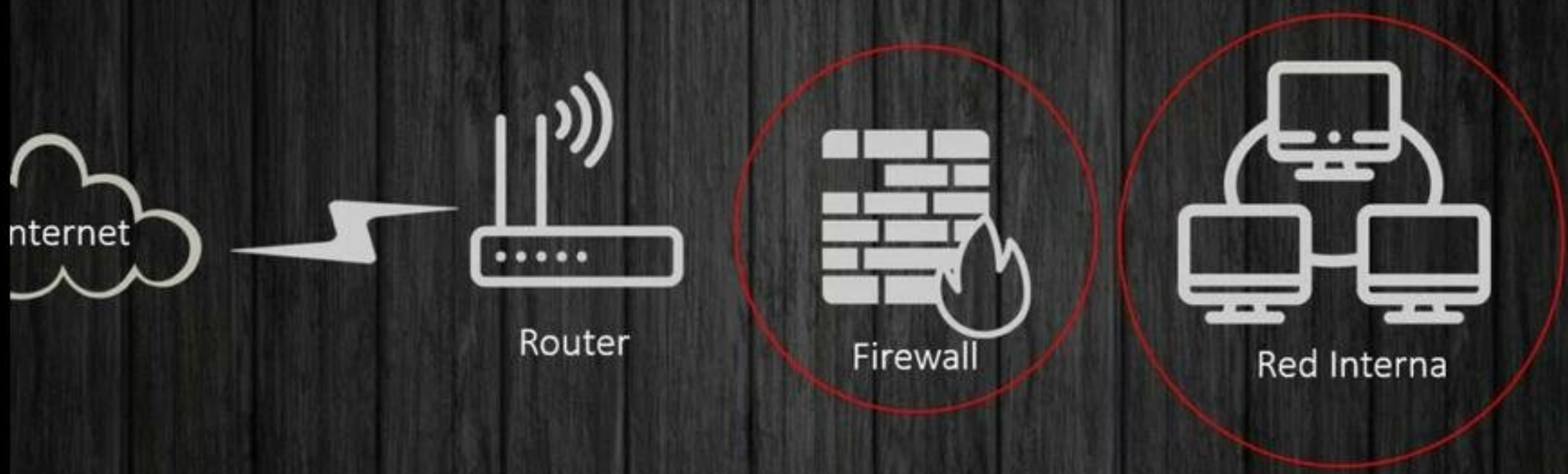
io III Infiltrado o empleado descontento (Insider)

hora es un **infiltrado**, y como empleado cuenta con claras **ventajas tácticas**:
uario avanzado puede ser conocedor de la infraestructura
mo mínimo, con permisos de usuario y acceso a diversas salas con distintos pun



ıo III Infiltrado o empleado descontento (Insider)

ıor norma general, ejecutará un reconocimiento de activos y esto le llevará a conocer
s de la red de usuarios e infraestructura de comunicaciones.



a con suficientes permisos, intentará escalar privilegios para la
e código malicioso.

Menganito

¡o III

Infiltrado o empleado descontento (Insider)

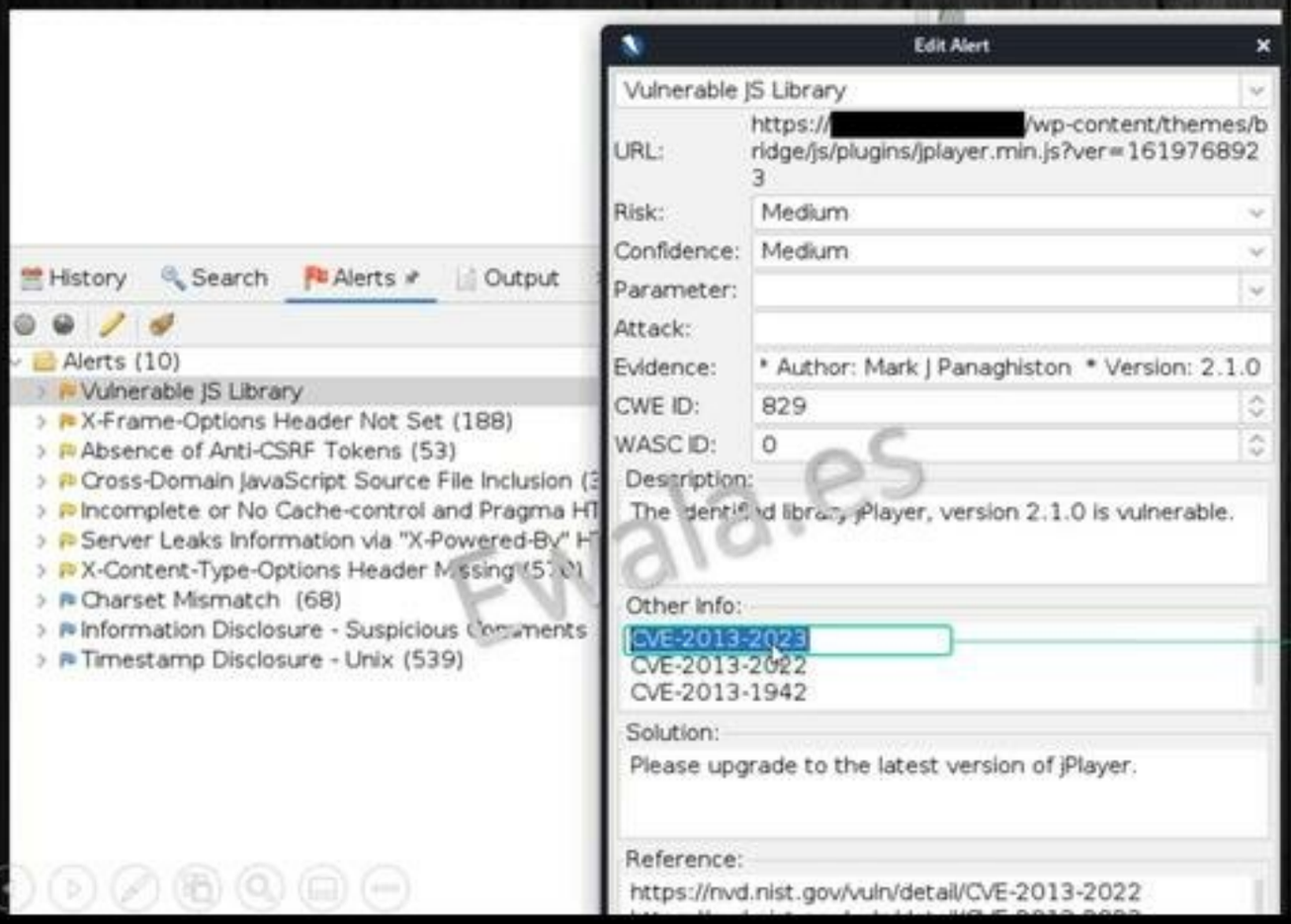
ıo III Infiltrado o empleado descontento (Insider)

ıocimiento de activos, Menganito descubre un servidor web que aloja la aplic
abe que desde una situación interna las reglas de seguridad pueden ser más
de configuración:

Escenario III

Infiltrado o empleado descontento (Insider)

Tras el reconocimiento de activos, Menganito descubre un servidor web que aloja la aplicación principal de la compañía. Sabe que desde una situación interna las reglas de seguridad pueden ser más permisivas y decide buscar fallos de configuración:



Encuentra una vulnerabilidad explotable.

CVE-2013-2023 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

Cross-site scripting (XSS) vulnerability in actionscript/Jplayer.as in the Flash SWF component (jplayer.swf) in jPlayer before 2.3.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, possibly related to incomplete blacklists, a different vulnerability than CVE-2013-1942 and CVE-2013-2022.

¡o III Infiltrado o empleado descontento (Insider)

, y aprovechando su momento estelar, Menganito puede buscar información se
erior extorsión o venta en el mercado negro.

ıo III Infiltrado o empleado descontento (Insider): Posibles soluciones

ario III Infiltrado o empleado descontento (Insider): Posibles soluciones

ección contra vulnerabilidades

izar análisis de vulnerabilidad contra los activos de la organización te permitirán cor
us activos; tendrás de esta manera un punto de partida para mejorar tu posición de
nte de un usuario mal intencionado que busque descubrir brechas explotables de s

izar un análisis detallado de las configuraciones de los activos según recomendacior
dening) es también una buena práctica de cara a securizar equipos críticos.

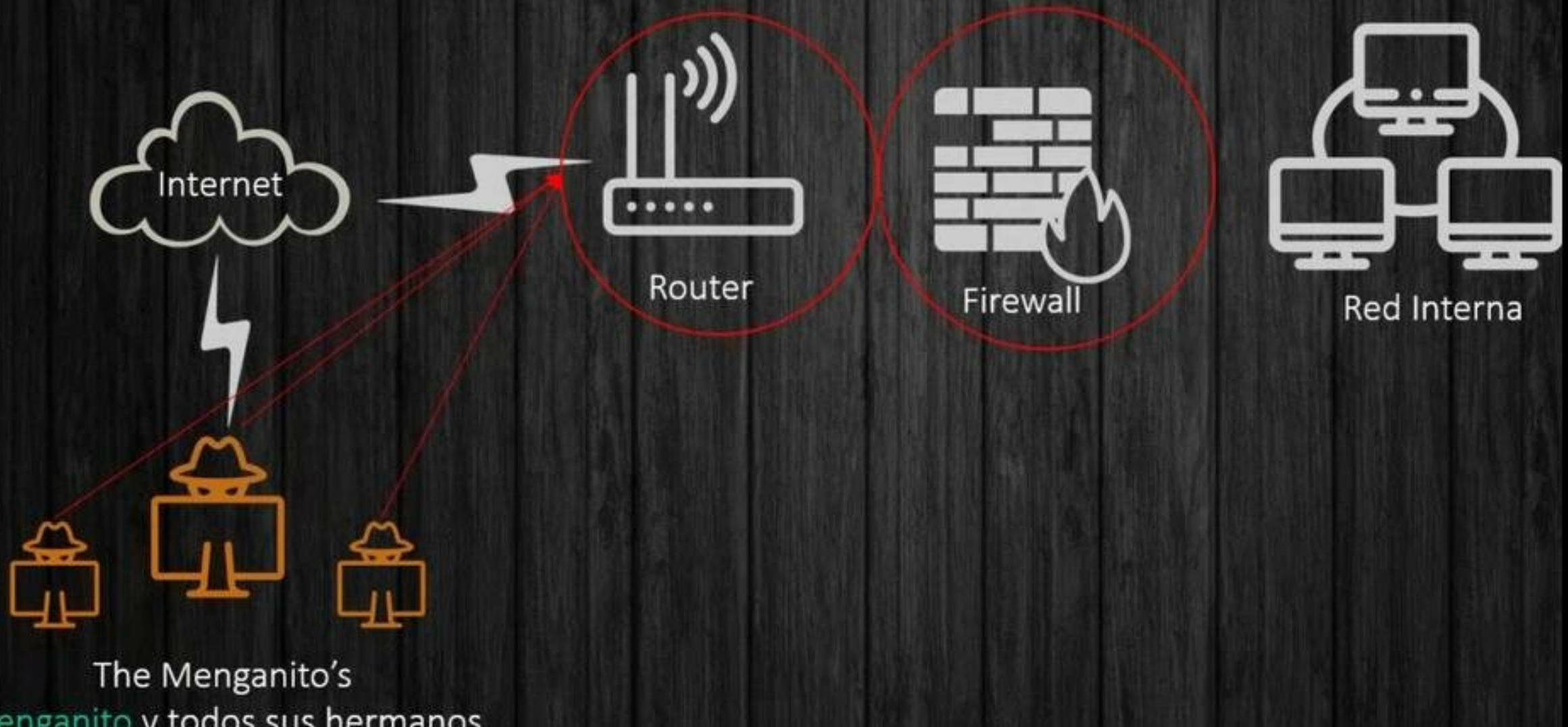
io IV Ataque en manada (denegación de servicio)

Escenario IV

Ataque en manada (denegación de servicio)

Para este último escenario, Menganito no está solo y une fuerzas con otros colaboradores.

¿Objetivo? Saturar la red de la empresa, **interrumpiendo sus operaciones y repercutiendo imagen pública**.



ıo IV Ataque en manada (denegación de servicio)

ual de ataques distribuidos
s).

Escenario IV

Ataque en manada (denegación de servicio)

Ejemplo visual de ataques distribuidos (coordinados).

Estadísticas en tiempo real.

¡o IV Ataque en manada (denegación de servicio): Posibles soluciones

rio IV Ataque en manada (denegación de servicio): Posibles soluciones

ción contra ataques volumétricos

ewalls empresariales no suelen ser tu aliado más eficiente en este tipo de casos, l
étricos" han de detenerse antes de llegar a la red corporativa, conviene entonces
dad a las aplicaciones de nube que se encargan de absorber el tráfico maliciosos

n de ataques y consecuencias inmediat

geniería Social). Distribución de malware e impacto financiero (timo del CEO).

ormación (Data Leak). Daño reputacional y aumento de la exposición ante amena

le información (Ransomware). Daño reputacional y pago de rescate (no recome
copias de seguridad.

o. Daño reputacional e impacto en las operaciones en caso de tiendas e-commer

ıfraestructura (Denegaciones de Servicio y otros vectores). Daño reputacional e
ones.

ɔs de números

os de números

tomamos como referencia el total de las detecciones año a año se observa u
% en 2020, siendo agosto el mes con más cantidad de detecciones" (ESET)

os de números

*tomamos como referencia el total de las detecciones año a año se observa un **crecir*
% en 2020, siendo agosto el mes con más cantidad de detecciones" (ESET)

*Incorporamos a nuestra base de datos de K-ront3 entre **100-200 Gb de datos fugados a***
medio para una empresa que sufre una brecha de datos ha vuelto a subir: ahora (202
dólares (3,52 millones de euros)" (IBM)

e: "*En el 2020, el coste de **remediación** supuso para las empresas españolas un desemb*
*...) El coste medio para aquellas organizaciones que pagan el **rescate** es de 1.448.458 U*

b: "*En un período de 17 meses se han detectado cerca de **2,5 billones de ataques web,***
perante" (Akamai)

de servicio: "*La frecuencia global de ataques DDoS creció un 39% entre 2018 y 2019.*
*cimiento asombroso del **776% en ataques entre 100 Gbps y 400 Gbps**.*" (Netscout)

es aprendidas: 4 reglas de oro.

prendidas: 4 reglas de oro.

il de toda cadena de seguridad es el propio ser humano.

prendidas: 4 reglas de oro.

il de toda cadena de seguridad es el propio ser humano.

ı hogar empieza más allá de la puerta de tu casa. Vigila que no haya
e atento a toda noticia de vulnerabilidades reportadas por tus proveedore

ngas un rifle de asalto, si no hay formación ni concienciación colectiva, y
á tan efectivo como un tirachinas. Tu firewall no te salvará por el mero he

ión a internet, vigila tu perímetro, pero también refuerza tus escudos i
nosas, porque nunca se sabe donde puede estar operando Menganito en

Muchas gracias

Contacto:

634 651 312

info@ewala.es

www.ewala.es

CATÁLOGO DE EMPRESAS Y SOLUCIONES DE CIBERSEGURIDAD
EMPRESA REGISTRADA
incibe_

Industria 4.0
ASTURIAS