

ACTIVIDADES PREITINERARIO #INCLUDE 2025 / 2026



ÍNDICE

ACTIVIDADES GENERALES	3
INICIAL.....	3
BUSCA 5 NOTICIAS DISTINTAS EN MEDIOS DE PRENSA RELACIONADAS CON LA CIBERSEGURIDAD..... 3	
NUEVA CAMPAÑA DE MALWARE LAZARUS CONTRA EL SOFTWARE LEGÍTIMO.	3
NUEVA ESTAFA SUPLANTANDO A IBERDROLA.....	6
LA WEB DEL SERVICIO DE INTELIGENCIA MILITAR BELGA SUFRE UN CIBERATQUE DE UN GRUPO DE HACKERS PRORRUSO.	9
SPYWARE DE LANDFALL APROVECHA UNA VULNERABILIDAD EN SMARTPHONES.12	
LOS CIBERATAQUES AUMENTAN HASTA EL 67% EN EL BLACK FRIDAY.	15

ACTIVIDADES GENERALES

INICIAL

BUSCA 5 NOTICIAS DISTINTAS EN MEDIOS DE PRENSA RELACIONADAS CON LA CIBERSEGURIDAD.

NUEVA CAMPAÑA DE MALWARE LAZARUS CONTRA EL SOFTWARE LEGÍTIMO.

REVISTA BYTE

¡Alerta! Nueva campaña de malware Lazarus contra el software legítimo.

El Equipo de Investigación y Análisis de Kaspersky (GReAT) ha desvelado una nueva campaña del grupo Lazarus. La investigación, presentada en el Security Analyst Summit (SAS), revela que esta sofisticada campaña APT de distribuye a través de malware y software legítimo.



Lazarus contra el software legítimo

Los ciberatacantes exhibieron un alto grado de sofisticación, empleando técnicas de evasión avanzadas y malware para mantener bajo control a la víctima. Utilizaron la herramienta conocida como LPEClient, previamente utilizada para atacar a víctimas en el sector de defensa, ingeniería nuclear y criptomonedas.

Este malware desempeña un papel crucial al iniciar la infección y perfilando a la víctima, alineándose con las tácticas del grupo Lazarus, como se vio en un ataque previo contra la cadena de suministro 3CX.

Kaspersky descubre una peligrosa campaña de Lazarus que explota software legítimo

Lazarus intentó en varias ocasiones comprometer al proveedor de software, posiblemente con el objetivo de robar código fuente crítico o interrumpir la cadena de suministro.

EUROPA PRESS

Lazarus lanza una nueva campaña maliciosa distribuida a través de software de certificación legítimo.

El Equipo de Investigación y Análisis de Kaspersky (GReAT) ha identificado varios actores maliciosos que empleaban un sistema diseñado para cifrar la comunicación web a través de certificados digitales para acceder a los datos de las víctimas.

europapress.es/portaltic/ciberseguridad/noticia-lazaurs-lanza-nueva-campana-maliciosa-distribuida-traves-

Buscar



PORTALTIC

Para ello, este grupo cibercriminal empleó LPEClient, una herramienta conocida por la elaboración de perfiles de víctimas y por distribuir carga útil maliciosa que ya se había registrado en anteriores ataques **en el sector de la defensa y las criptomonedas**.

Kaspersky ha revelado que descubrió la campaña maliciosa del grupo de ciberdelincuentes norcoreanos en julio de 2023, cuando detectó una serie de ataques a varias víctimas poseedoras de este 'software' de certificación legítimo.

Si bien se desconoce la manera en que los atacantes se aprovecharon de este 'software' para distribuir el 'malware', advirtió **carga maliciosa de SIGNBT** acompañado de un código shell, responsable de iniciar un archivo ejecutable de Windows directamente en la memoria.

Con ello, Lazarus podía distribuir carga maliciosa con cada inicio del sistema o realizar cargas laterales en archivos legítimos ejecutables, "lo que garantiza aún más un mecanismo de persistencia resistente", según el equipo de analistas.

IT DIGITAL SECURITY

La campaña de ciberataques Lazarus que sigue explotando software legítimo.

Mediante sofisticadas técnicas de amenaza persistente avanzada, el malware se integró en un software legítimo, precisamente de seguridad y diseñado para encriptar las comunicaciones web.

itdigilalsecurity.es/vulnerabilidades/2023/11/la-campana-de-ciberataques-lazarus-que-sigue-explotando-software-legitimo

X Post

in Compartir

Seguridad

Ciberseguridad

Ciberamenazas

Vulnerabilidades

Kaspersky

Ciberseguridad

SUSCRÍBETE A NUESTRA NEWSLETTER

ME APUNTO



Este es un ejemplo de por qué todos los actores de la ciberseguridad siguen incidiendo en la necesidad de llevar a cabo las actualizaciones, no solo de los sistemas operativos sino de todos los elementos de software de los equipos. El Equipo de Investigación y Análisis de Kaspersky (GReAT) detectó a mediados de julio una nueva campaña de ciberataques de Lazarus.

La campaña tuvo como objetivo multitud de organizaciones de todo el mundo que utilizaban un software de seguridad legítimo, no revelado por Kaspersky, especializado en la encriptación de comunicaciones web con certificados digitales. Pese a que se comunicó las vulnerabilidades a la compañía responsable del software y ésta lo parcheó, algunas organizaciones no actualizaron su aplicación y el malware pudo continuar con su actividad.

El ataque fue de alta sofisticación, una amenaza persistente avanzada (APT) que además incorporaba novedosas técnicas de evasión y que partió de la herramienta LPEClient, ya utilizada anteriormente por Lazarus. Cuando en principio el problema estaba resuelto, Kaspersky Endpoint Security identificó la amenaza y paralizó nuevos ataques en empresas que utilizaban la versión sin parchear.

Seongsu Park, investigador principal de seguridad del Equipo de Análisis e Investigación Global (GReAT) de Kaspersky, avisa de que “el grupo Lazarus es persistente, tiene una motivación inquebrantable y muestra capacidades avanzadas. Opera a escala global, dirigiéndose contra una amplia gama de sectores de distintas formas. Es una amenaza en evolución constante que debe mantenernos siempre alerta”.

NUEVA ESTAFA SUSTITUYENDO A IBERDROLA.

EL MUNDO

Alertan de correos fraudulentos que suplantan a Iberdrola para robar datos bancarios.

Los correos utilizan como gancho una cuantía desorbitada en la factura, con importes que van desde los 424,81 euros hasta los 98.589,64 euros, para generar alarma en el destinatario y provocar que pulse un enlace con un archivo adjunto.



[elmundo.es/economia/2025/11/05/690b477afc6c8341718b45a3.html](https://www.elmundo.es/economia/2025/11/05/690b477afc6c8341718b45a3.html)



Alertan de correos fraudulentos que suplantan a Iberdrola para robar datos bancarios



Imagen de archivo de la Policía Nacional, Unidad de Delitos Ciberneticos. ALBERTO VERA

Efe

León

Actualizado Miércoles, 5 noviembre 2025 - 13:47

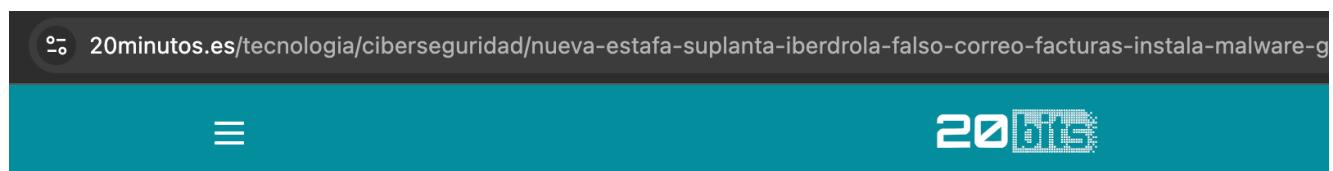
El Instituto Nacional de Ciberseguridad (INCIBE), a través de su Oficina de Seguridad del Internauta (OSI), ha emitido este miércoles una alerta de importancia alta por una campaña de *phishing* que suplanta a la compañía eléctrica Iberdrola con el **pretexto del envío de una factura**, y que tiene como objetivo la distribución del *malware* bancario Grandoreiro, también conocido como Zbot.

El ataque se realiza mediante correos electrónicos fraudulentos que simulan ser notificaciones legítimas de Iberdrola, en los que se informa al usuario de que su factura de electricidad está disponible para su consulta. El mensaje incluye un enlace que supuestamente dirige al Área Cliente, pero que en realidad **descarga un archivo con extensión .iso** que contiene el código malicioso.

20MINUTOS

Alertan de la nueva estafa de phishing suplantando a Iberdrola: un falso correo con facturas instala el temido malware Grandoreiro.

Dicho fraude se distribuye mediante correos electrónicos fraudulentos que simulan ser una notificación mensual para informar al cliente de que su factura ya está disponible para su consulta, teniendo en cuenta que el mensaje va acompañado de un resumen del gasto mensual, un supuesto número de contrato y la dirección de correo electrónico de la víctima. Además, el mensaje incluye un enlace que supuestamente dirige al Área de Cliente, pero que en realidad descarga un archivo con extensión .iso que contiene el malware Grandoreiro.



Dicho fraude se distribuye mediante **correos electrónicos fraudulentos que simulan ser una notificación mensual** para informar al cliente de que su factura ya está disponible para su consulta, teniendo en cuenta que el mensaje va acompañado de un resumen del gasto mensual, un supuesto número de contrato y la dirección de correo electrónico de la víctima. Además, el mensaje incluye un enlace que supuestamente dirige al Área Cliente, pero que en realidad descarga un **archivo con extensión .iso que contiene el malware Grandoreiro**.

Según informa el INCIBE, para generar sensación alarmista, **los correos emplean como gancho una cuantía del gasto desorbitada** —que van desde los 424,81 euros hasta los 98.589,64 euros—, de esta manera, provoca al usuario que pulse en el enlace para ver de dónde procede el importe.

EL CONFIDENCIAL

Alerta del INCIBE por esta nueva campaña que suplanta a Iberdrola: cómo protegerte ante ella.

El Instituto Nacional de Ciberseguridad (INCIBE) ha emitido una alerta urgente por una nueva campaña de phishing que suplanta a Iberdrola mediante correos electrónicos fraudulentos. Estos mensajes, que imitan el logotipo y diseño oficial de la compañía, informan al usuario de una supuesta factura pendiente con un importe elevado. El objetivo de los ciberdelincuentes es que la víctima descargue un archivo malicioso con el que podrían robar contraseñas y acceder a cuentas bancarias.

elconfidencial.com/espana/2025-11-10/alerta-incibe-nueva-campana-phising-suplanta-iberdrola_4244680/

Cómo funciona el engaño



El **correo parece auténtico**, pero el remitente **no pertenece a Iberdrola**. En el mensaje se incluye un enlace que dirige a una **falsa área de clientes**. Al hacer clic, se descarga un archivo comprimido en formato **.iso**, que contiene un programa malicioso identificado como **Zbot o Grandoreiro**. Una vez ejecutado, **este malware puede robar credenciales, datos financieros e incluso propagarse a otros dispositivos** conectados a la red.



elconfidencial.com/espana/2025-11-10/alerta-incibe-nueva-campana-phising-suplanta-iberdrola_4244680/

Qué hacer si recibes el correo



El **INCIBE recomienda comprobar siempre el remitente** antes de abrir cualquier mensaje sobre facturas pendientes. Si el correo resulta sospechoso, **no pinches en los enlaces, márcalo como spam y elimínalo por completo**. Además, **Iberdrola recuerda** que las facturas se pueden consultar directamente desde su **página web oficial** o llamando a su **teléfono de atención al cliente**, sin utilizar enlaces externos.

Si descargaste el archivo pero **no lo ejecutaste, elimínalo y vacía la papelera**. En caso de haberlo abierto, **desconecta el dispositivo de internet, realiza un análisis con un antivirus actualizado** y, si es necesario, **restaura el sistema** para eliminar la infección. El **INCIBE aconseja conservar pruebas**, como capturas de pantalla o el correo, y **denunciar el intento de fraude** ante las autoridades. Ante cualquier duda, contacta con los **canales oficiales de Iberdrola** o con la **línea gratuita de ayuda en ciberseguridad** del INCIBE.

LA WEB DEL SERVICIO DE INTELIGENCIA MILITAR BELGA SUFRE UN CIBERATAQUE DE UN GRUPO DE HACKERS PRORRUSO.

TELEPRENSA

El ministerio de Defensa Belga ha informado de que la web de servicio de inteligencia y seguridad belga (SGRS) sufrió un ciberataque del grupo de hackers prorruso NoName057.

El ataque informático de denegación de servicio distribuido (DDoS) dirigido contra las páginas web del SGRS ya fue reivindicado por sus autores a través de la red Telegram.

teleprensa.com/articulo/internacional/web-servicio-inteligencia-militar-belga-sufre-ciberataque-grupo-hackers-prorruso/2025



CANTORIA 19.5 °C



PRIMER PERIÓDICO DIGITAL DE ALMERÍA

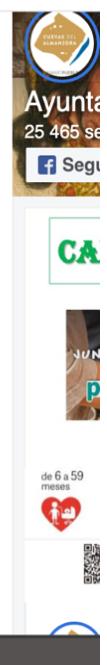
La web del servicio de inteligencia militar belga sufre el ciberataque de un grupo de 'hackers' prorruso

Fuentes del Ministerio consultadas por la RTBF también confirman el ciberataque pero matizan que "no hubo intrusión en el sitio y nada indica que se accediera a informaciones sensibles o que se hayan difundido datos". La acción del grupo prorruso dejó las páginas web del servicio de inteligencia momentáneamente inoperativas, pero el servicio ya se ha recuperado.

En su reivindicación, los 'hackers' justifican el ataque como advertencia al ministro de Defensa, el ultranacionalista flamenco Theo Francken, quien en una entrevista reciente a la revista 'Humo' afirmó que si Rusia atacaba Bruselas entonces la OTAN "arrasaría" Moscú.

"Aconsejamos al ministro belga que haga ese tipo de declaraciones", avisan los autores del ciberataque en el mensaje difundido el jueves pasadas las 18:00 horas en la red social.

Este suceso se suma a la serie de avistamientos de drones que a lo largo de esta semana ha obligado a Bélgica a suspender el tráfico aéreo en varias ocasiones, debido a la presencia de aparatos no autorizados en las cercanías de los aeropuertos de Bruselas y de Lieja, así como de tres bases militares.



ESCUDO DIGITAL

Los hacktivistas prorrusos NoName057 lanzan un ciberataque contra la inteligencia militar belga.

El Ministerio de Defensa belga ha informado de que la web de servicio de inteligencia y seguridad militar belga (SGRS, por sus siglas en francés) ha sufrido un ciberataque del grupo de hacktivistas prorrusos NoName057.

 escudodigital.com/ciberseguridad/los-hacktivistas-prorrusos-nomname057-lanzan-un-ciberataque-contra-la-inteligencia-militar-belga/

Escudo digital

En su reivindicación, los hackers justifican el ataque como advertencia al ministro de Defensa, el ultranacionalista flamenco **Theo Francken**, quien en una entrevista reciente a la revista '*Humo*' afirmó que **si Rusia atacaba Bruselas entonces la OTAN "arrasaría" Moscú**.

"Aconsejamos al ministro belga que no haga ese tipo de declaraciones", avisan los autores del ciberataque en el mensaje difundido el jueves pasadas las 18:00 horas en la red social.

Este suceso se suma a la serie de **avistamientos de drones** que a lo largo de esta semana ha obligado a Bélgica a suspender el tráfico aéreo en varias ocasiones, debido a la presencia de aparatos no autorizados en las cercanías de los aeropuertos de Bruselas y de Lieja, así como de tres bases militares.



Bélgica ordena derribar los drones que violen su espacio aéreo

Javier Rubio Monte

El Gobierno no ha apuntado oficialmente a ningún responsable por las incursiones de drones, pero fuentes de los servicios de inteligencia citados por la prensa apuntan a un "actor estatal" tercero y el propio Francken aseguró tras los incidentes que no era obra de un aficionado, sino que se trataba de **acciones coordinadas**.

INFOBAE

Hackers prorrusos atacaron a la inteligencia militar de Bélgica y amenazaron a un ministro por sus comentarios sobre Moscú.

Bruselas confirmó que la página web de SGRS fue blanco de un ataque DDoS reivindicado por el grupo NoName057.

The screenshot shows a news article from Infobae.com. At the top, there are navigation icons (back, forward, search) and the URL "infobae.com/america/mundo/2025/11/07/hackers-prorrusos-atacaron-a-la-inteligencia-militar-de-belgica-y-ame". Below the header, there are links for Argentina, Colombia, España, México, Perú, and Estados Unidos. The main text discusses a DDoS attack on the Belgian military intelligence website by the group NoName057, with quotes from the Belgian government and the attackers' justification.

Según la cadena pública VRT, el ataque, de tipo **denegación de servicio distribuido (DDoS)**, fue reivindicado el mismo jueves por los autores a través de su canal en la red social Telegram. El Ministerio precisó que el ataque afectó temporalmente el funcionamiento del sitio web, pero que “**no hubo intrusión en el sitio y nada indica que se accediera a informaciones sensibles o que se hayan difundido datos**”. Informaron que el portal ya fue restablecido y opera con normalidad.

En su comunicado, los **atacantes justificaron la acción como una advertencia al ministro de Defensa Theo Francken**, quien recientemente declaró en una entrevista que, en caso de un ataque ruso contra Bruselas, la OTAN “arrasaría” a Moscú.

SPYWARE DE LANDFALL APROVECHA UNA VULNERABILIDAD EN SMARTPHONES.

XTechAI

El spyware Landfall: un ataque encubierto contra los Samsung Galaxy.

Se trata de un spyware el cual logró explotar un fallo de seguridad en estos dispositivos para extraer datos sensibles de usuarios sin su conocimiento.

The screenshot shows a web browser window with the URL consultoriainformatica.net/el-spyware-landfall-un-ataque-encubierto-contra-los-samsung-galaxy-que-duro-meses/. The page header includes the XTechAI logo and navigation links for Servicios, Casos de Éxito, Blog, and Alianzas. The main content discusses the evolution of cyber threats, specifically the Landfall spyware that exploited a vulnerability in Samsung Galaxy devices to steal sensitive user data without their knowledge.

Las amenazas ciberneticas están en constante evolución, y en los últimos meses, un nuevo caso ha puesto en alerta a los usuarios de Samsung Galaxy. Se trata del 'spyware' conocido como **Landfall**, el cual logró explotar un fallo de seguridad en estos dispositivos para extraer datos sensibles de usuarios sin su conocimiento. Este incidente ha suscitado preocupaciones sobre la seguridad de los smartphones y la privacidad de los datos personales.

¿Qué es el 'spyware' Landfall?

Landfall es un tipo de software malicioso diseñado para espionar y robar información de los dispositivos infectados. A través de técnicas sofisticadas, este 'spyware' consigue acceder a datos críticos, como registros de llamadas, mensajes de texto, datos de ubicación y, en algunos casos, incluso información bancaria. La aparición de Landfall revela la creciente complejidad y peligrosidad de las amenazas ciberneticas actuales.

DEVEL

Samsung corrige falla Zero-Click explotada para desplegar el spyware Landfall a través de WhatsApp.

El fallo, identificado como CVE – 2025 – 21042 (CVSS 8.8), afectaba a la biblioteca `libimagecodec.quram.so` y permitía ejecución remota de código sin interacción del usuario.



CÓMO FUNCIONÓ EL ATAQUE: IMÁGENES MANIPULADAS ENVIADAS POR WHATSAPP

El vector: archivos DNG modificados

La campaña utilizó imágenes maliciosas en formato DNG (Digital Negative) enviadas a través de WhatsApp. Estas imágenes contenían, incrustado al final del archivo, un ZIP oculto con librerías diseñadas para explotar la vulnerabilidad y desplegar el spyware sin que la víctima tocara nada.

Entre los archivos analizados se encontraron nombres como:

- “WhatsApp Image 2025-02-10 at 4.54.17 PM.jpeg”
- “IMG-20240723-WA0000.jpg”

Esto confirma actividad maliciosa desde julio de 2024, más de seis meses antes de que el fallo fuera documentado.

CADENA DE EXPLOTACIÓN ZERO-CLICK

Una vez que WhatsApp procesaba la imagen, el fallo en `libimagecodec.quram.so` permitía:

1. Extraer la librería maliciosa oculta en el ZIP.
2. Ejecutar código remoto para desplegar LANDFALL.
3. Cargar un segundo módulo que altera la política de SELinux, dándole al spyware permisos elevados y permanencia en el dispositivo.

INFOSERTEC

Alerta el spyware Landfall comprometió teléfonos Samsung Galaxy por más de un año vía WhatsApp.

Un sofisticado spyware explota una vulnerabilidad de día cero en la biblioteca de procesamiento de imágenes de Android a través de imágenes enviadas por WhatsApp.

← → C  infosertecla.com/2025/11/10/alerta-el-spyware-landfall-comprometio-telefonos-samsung-galaxy-por-mas-de-un-ano-via-whatsapp/

Alerta el Spyware LandFall comprometió teléfonos Samsung Galaxy por más de un año vía WhatsApp

Un informe de la firma de ciberseguridad Palo Alto Networks (Unidad 42) reveló la existencia de un *spyware* altamente sofisticado, denominado **LandFall**, que estuvo activo en dispositivos Samsung Galaxy por más de un año, afectando a usuarios en Turquía, Marruecos, Irán e Irak desde al menos julio de 2024.

El método de infección de LandFall fue particularmente insidioso: se propagó a través de **imágenes enviadas por WhatsApp**. Esto significaba que el ataque se ejecutaba sin requerir ninguna acción por parte del usuario, como descargar un archivo o hacer clic en un enlace malicioso.

Vulnerabilidad y Consecuencias

El *spyware* explotó una vulnerabilidad de día cero (identificada como **CVE-2025-21042**) en la biblioteca de procesamiento de imágenes de Android específica de Samsung, lo que permitió a los atacantes ejecutar código arbitrario en el dispositivo. Una vez instalado, LandFall otorgó un acceso prácticamente ilimitado al atacante, incluyendo:

LOS CIBERATAQUES AUMENTAN HASTA EL 67% EN EL BLACK FRIDAY.

PRESSDIGITAL

Los ciberataques en el comercio digital aumentan un 67% durante las campañas de ofertas de Black Friday, CyberMonday y Navidad.

Esto está relacionado con el aumento de las compras por internet, pues el comercio electrónico aumentó un 15% durante el primer semestre de 2025 en tasa interanual.

pressdigital.es/articulo/economia/2025-11-07/5659051-ciberataques-aumentan-hasta-67-black-friday-afectan-sobre-todo-pymes

Así, el director de operaciones de Factum, David López, ha concluido que "complementar la capacitación con sistemas de detección y respuesta 24/7 puede marcar la diferencia entre una interrupción mínima y un colapso de la actividad, salvaguardando no solo la operativa sino también la reputación de las pymes en plena campaña de ventas".

Estas son, precisamente, las más vulnerables, por la poca formación en ciberseguridad que el informe destaca, con un 55% de pymes que declaran no saber cómo protegerse frente a un ciberataque, mientras que tres de cada diez creen que no sobrevivirían a un ataque serio.

En este sentido, la compañía de ciberseguridad ha instado a las empresas a reforzar la seguridad -- auditorías internas, copias de seguridad o seguridad en las transacciones online--, para evitar un daño económico que puede provocar el cierre de los negocios.



■ El Gol
estabili
próxim

A Y E ECONOMÍA REAL

Los expertos avisan de que los momentos de compras masivas a través del comercio online aumentan significativamente el riesgo de sufrir un ciberataque para las pymes.

El comercio electrónico es un sector que ha experimentado un aumento interanual del 15% en sus ventas y del 8% en sus pedidos. Y las pymes españolas lideran un importante incremento en pedidos internacionales (125%).

The screenshot shows a news article from the website autonomosyemprendedor.es. The URL in the address bar is: autonomosyemprendedor.es/articulo/ciberseguridad/expertos-alertan-ciberataques-pymes-aumentan-67-black-friday-. The page features a dark header with the letters 'AyE' in white. The main text discusses the increased risk of cyber attacks during Black Friday, quoting experts from Cylum and Factum.

Pero las diferentes campañas encadenadas son un arma de doble filo, según los expertos de Cylum y Factum, dado que **los ciberataques aumentan un 67% durante esta campaña**, en la que miles de datos de millones de consumidores están en la red para adquirir productos y servicios.

1. [Tres de cada diez pymes no podrán sobrevivir a un ciberataque](#)
2. [El 55% de las pymes afirman no saber cómo protegerse de un ciberataque](#)

Tres de cada diez pymes no podrán sobrevivir a un ciberataque

Según recordaron desde Cylum, las pequeñas y medianas empresas **pueden sufrir importantes dificultades a nivel económico y de reputación** por los daños derivados de ciberataques.



Así deben actuar los autónomos en las primeras 72 horas tras un ciberataque para evitar sanciones

En particular, tres de cada diez pymes reconocen que no podrán sobrevivir a un ciberataque serio. Por tanto, los profesionales del sector recomiendan **realizar**

PERIÓDICO PUBLICIDAD

Con la inminente llegada de miles de ofertas por el Black Friday, el CyberMonday y la campaña de compras de Navidad, los comercios se preparan para dar el empujón final a las ventas del año.

El último tramo del año, con diferentes campañas de venta encadenadas es un arma de doble filo, pues se produce un aumento muy significativo de las ventas vía e-commerce.

 periodicopublicidad.com/articulo/estudios/ciberataques-aumentan-67-black-friday-cybermonday-navidad/20251106105504165214.html



CAMPAÑAS ▾ TEMÁTICAS ▾ ENTREVISTAS NEGOCIOS ▾ EVENTOS ▾ TENDENCIAS OPINIÓN ▾ CLUB EXPERTOS ▾

Como explican los profesionales de **Cylum**, la unidad de ciberseguridad como servicio de Factum para pequeñas y medianas empresas, esto es particularmente preocupante y no tomar precauciones puede salir muy caro a nivel económico, reputacional y, en ocasiones, puede implicar el cierre de un negocio. Concretamente 3 de cada 10 pymes reconocen que no podrían sobrevivir a un ciberataque serio.

Por eso, **Cylum insta a reforzar la seguridad de sus plataformas digitales para proteger sus tiendas online durante campañas críticas.**

Para sus expertos en el área de protección de la pyme, resulta esencial realizar auditorías previas de seguridad, que permitan anticiparse a posibles vulnerabilidades antes de los picos de tráfico.

Otra medida fundamental es **la protección de la información y de los sistemas de pago**, con la implantación de copias de seguridad cifradas e inmutables, verificadas regularmente, para reducir el tiempo de recuperación en caso de incidente. Además, se debe garantizar la seguridad de las transacciones online mediante protocolos cifrados, cumplimiento de PCI-DSS y autenticación multifactor en accesos administrativos minimiza el riesgo de fraudes en momentos de alta demanda.

LO MÁS V



NEGO
Fall
ever



NEGO
Chei
desc
Cent
Sam



SPOTS
No
mon



DISEÑ
Truec