Mes: Marzo 2026

Resumen mensual

Malware

Malware distribuido desde GitHub afecta a empresas españolas

Resumen: Investigadores y medios especializados alertaron de campañas activas del infostealer BoryptGrab, un malware diseñado para robar credenciales y datos corporativos, distribuido desde más de 100 repositorios públicos de GitHub. INCIBE-CERT incluyó esta amenaza entre las campañas relevantes con impacto potencial en empresas españolas, especialmente en entornos de desarrollo y TI.

¿Cómo protegerse?

- ✅ Restringir descargas de código desde repositorios públicos no verificados.
- ✅ Integrar análisis de seguridad en pipelines CI/CD.
- ✅ Supervisar tráfico saliente y posibles exfiltraciones.
- ✅ Concienciar a desarrolladores sobre riesgos de dependencias externas.

Link: https://www.ciberext.es/noticias-de-ciberseguridad-malware-en-github-backdoor-irani-que-evade-edr-brecha-masiva-en-plataforma-de-ia-y-nuevas-vulnerabilidades-criticas-en-routers

Malware como fase inicial de campañas de ransomware en España (Qilin, Akira)

Resumen: Europa Press y ESET señalaron que familias de malware utilizadas por grupos como Qilin y Akira siguen siendo la fase inicial de campañas de ransomware en España. Estas cargas permiten reconocimiento, robo de credenciales y movimiento lateral antes del cifrado.

¿Cómo protegerse?

- ✅ Monitorizar ejecución de herramientas de pos-explotación.
- ✅ Aplicar segmentación de red.
- ✅ Vigilar creación anómala de servicios y tareas programadas.
- ✅ Probar periódicamente procesos de detección temprana.

Link: https://www.europapress.es/portaltic/ciberseguridad/noticia-espana-cierra-2025-segundo-pais-mundo-mas-afectado-ransomware-20260122142548.html

El malware de robo de información LummaStealer vuelve a operar a gran escala tras su desmantelamiento

Resumen: Tras su caida durante una operación internacional que consiguió desmantelar su infraestructura operativa, han vuelto a detectarse casos del programa malicioso LummaStealer, dedicado al robo de información. Esto sugiere el regreso del actor de amenaza y supone un riesgo para la actividad empresarial.

¿Cómo protegerse?

- ✅ Evita guardar información sensible en tu navegador para impedir su extracción.
- ✅ No descargues aplicaciones desde fuentes no oficiales.
- ✅ No concedas accesos innecesarios a tus datos ni a las funciones del dispositivo.

Link: https://www.20minutos.es/tecnologia/ciberseguridad/ciberataques-espana-crecen-estas-amenazas-peligros-mas-comunes_6941867_0.html

Phishing

Campaña de phishing que suplanta “Mi Carpeta Ciudadana”

Resumen: La Guardia Civil y el Instituto Nacional de Ciberseguridad (INCIBE) advierten de una campaña masiva de suplantación de identidad. Su objetivo es incitar a las víctimas a clicar en un correo que suplanta la apariencia de la Agencia Tributaria para obtener credenciales de acceso, lo que les permitiría acceder a datos sensibles como los encontrados en la declaración de la Renta de los ciudadanos afectados.

¿Cómo protegerse?

- ✅ Desconfiar de correos que prometen ingresos o devoluciones.
- ✅ Verificar siempre dominios oficiales .gob.es.
- ✅ No introducir datos bancarios desde enlaces recibidos.
- ✅ Reportar el incidente al 017 o INCIBE-CERT.

Link: https://www.abc.es/tecnologia/guardia-civil-alerta-campana-phishing-notificaciones-falsas-20260204120919-nt.html

INCIBE activa protocolo rojo por phishing masivo de suplantación institucional

Resumen: INCIBE activó en marzo un protocolo de alerta máxima ante una campaña de phishing altamente sofisticada que utiliza lenguaje legal, referencias normativas reales y datos personalizados para robar DNI, cuentas bancarias y credenciales a ciudadanos españoles. La campaña fue catalogada como amenaza activa a nivel nacional.

¿Cómo protegerse?

- ✅ No facilitar nunca DNI, contraseñas o códigos por email.
- ✅ Revisar cuidadosamente el remitente y el dominio.
- ✅ Activar alertas de movimientos en cuentas bancarias.
- ✅ Cambiar credenciales inmediatamente si se ha interactuado.

Link: https://www.moncloa.com/2026/03/06/incibe-phishing-suplantacion-3364525/

Campaña de smishing y phishing dirigida a viajeros en aeropuertos españoles

Resumen: INCIBE emitió un aviso urgente por una campaña de smishing y phishing que afecta a viajeros en aeropuertos españoles. Los mensajes simulan incidencias con equipajes o tasas aduaneras pendientes y conducen a pasarelas falsas para robar datos de tarjetas y credenciales bancarias.

¿Cómo protegerse?

- ✅ Desconfiar de SMS sobre incidencias de vuelo o equipaje.
- ✅ No introducir datos de pago desde enlaces recibidos por mensaje.
- ✅ Verificar siempre con la aerolínea por canales oficiales.
- ✅ Eliminar el mensaje y bloquear al remitente.

Link: https://www.moncloa.com/2026/03/09/incibe-ciberestafa-aeropuertos-3364712/

Brechas de seguridad

Ransomware paraliza los sistemas del Puerto de Vigo

Resumen: Un ataque de ransomware afectó a los sistemas digitales del Puerto de Vigo, obligando a operar temporalmente con procedimientos manuales. Aunque la actividad portuaria no se detuvo totalmente, la gestión logística y la coordinación digital se vieron seriamente impactadas. El incidente evidencia el riesgo creciente del ransomware sobre infraestructuras críticas en España.

¿Cómo protegerse?

- ✅ Mantener copias de seguridad offline periódicamente probadas.
- ✅ Segmentar redes IT y OT para reducir movimientos laterales.
- ✅ Disponer de planes de respuesta y continuidad debidamente probados.

Link: https://www.integrity360.com/es/cyber-news-roundup-march-27th-2026

Cecotec: sanción AEPD por brecha de datos y respuesta tardía

Resumen: La AEPD impuso una sanción de 1,09 millones de euros a Cecotec Innovaciones S.L.U. por incumplimientos RGPD relacionados con una brecha de seguridad y su gestión.
El caso se originó tras detectarse una base de datos atribuida a la compañía en la dark web, y la investigación puso el foco en medidas insuficientes y en una respuesta tardía ante el aviso. Entre los factores señalados figura la existencia de una plataforma antigua, accesible y con software desactualizado, que mantenía datos personales sin protección adecuada.

¿Cómo protegerse?

- ✅ Retirar sistemas legacy expuestos y sin mantenimiento.
- ✅ Cifrar datos sensibles en reposo y tránsito.
- ✅ Activar respuesta inmediata ante alertas externas verificadas.

Link: https://bitlifemedia.com/2026/03/multa-millonaria-a-cecotec-por-una-brecha-de-datos-cuando-el-problema-no-es-el-ciberataque-sino-la-gestion/

Filtración de datos de altos cargos y fuerzas de seguridad (caso “doxing” en marzo)

Resumen: En marzo se investigó la publicación de datos personales de altos cargos y personal de seguridad del Estado (incluida la dirección del CNI), difundidos mediante prácticas de doxing. La información filtrada afectó a perfiles sensibles y activó actuaciones de investigación por parte de unidades especializadas. Aunque no es una “empresa”, sí es un caso concreto de exposición de datos con impacto directo en España.

¿Cómo protegerse?

- ✅ Minimizar datos públicos y revisar huella digital.
- ✅ Aplicar controles de acceso y monitorización continua.
- ✅ Activar procedimientos rápidos de retirada de contenidos.

Link: https://theobjective.com/espana/2026-03-29/cni-caza-hacker-filtrando-datos-policias-fiscales/

CVEs

Vulnerabilidad en Fortinet FortiClient EMS (SQLi explotada activamente)

Resumen: La vulnerabilidad CVE-2026-21643 afecta a FortiClient EMS y se describe como inyección SQL explotable remotamente, con impacto crítico.
La fuente indica que estaba siendo explotada activamente en ataques, especialmente contra instancias expuestas a Internet.
Gravedad: 🔥 Crítica (9.1/10) – Riesgo alto por tratarse de un servidor de gestión centralizada de endpoints.
Ejemplo real: Una organización usa FortiClient EMS para desplegar políticas a endpoints; si la consola está expuesta y sin parche, un atacante podría explotar la SQLi y obtener control del servidor de gestión, afectando a inventario, políticas y telemetría de endpoints.

✅ **Solución:** Actualizar FortiClient EMS a una versión corregida.

Link: https://blog.elhacker.net/2026/03/vulnerabilidad-critica-en-fortinet.html

Vulnerabilidad en Microsoft Devices Pricing Program (RCE)

Resumen: En el Patch Tuesday de marzo de 2026, INCIBE-CERT recoge una vulnerabilidad crítica CVE-2026-21536 de ejecución remota de código en Microsoft Devices Pricing Program. El aviso de INCIBE-CERT indica que se trata de la vulnerabilidad crítica destacada del ciclo y que Microsoft aplicó corrección/mitigación en el servicio.
Gravedad: 🔥 Crítica (9.8/10) – Riesgo para usuarios que usen dicho producto.
Ejemplo real: Un servicio Microsoft expuesto podría ejecutar código remoto.

✅ **Solución:** Aplicar de manera urgente las actualizaciones de seguridad lanzadas por Microsoft.

Link: https://www.incibe.es/incibe-cert/alerta-temprana/avisos/actualizaciones-de-seguridad-de-microsoft-de-marzo-de-2026

Vulnerabilidad en Umami Software (SQLi crítica coordinada por INCIBE)

Resumen: INCIBE coordinó la publicación de una SQLi crítica en la aplicación web de Umami Software, identificada como CVE-2026-4317. La vulnerabilidad permite a un atacante autenticado ejecutar comandos SQL arbitrarios mediante manipulación de parámetros, comprometiendo datos en base de datos. El aviso incluye versión afectada (3.0.2) y versión corregida (3.0.3).
Gravedad: 🔥 Crítica (9.3/10) – Riesgo para usuarios que utilizan dicho software.
Ejemplo real: Un atacante autenticado podría extraer datos de la base.

✅ **Solución:** Actualizar urgentemente el software Umami a la versión 3.0.3.

Link: https://www.incibe.es/incibe-cert/alerta-temprana/avisos/inyeccion-sql-en-la-aplicacion-de-umami-software