Mes: Mayo 2026

Resumen mensual

Malware

Malware basado en rootkits y robo de credenciales en la nube

Resumen: Se han identificado nuevas amenazas avanzadas como rootkits para Linux con capacidades P2P y campañas de robo de credenciales en entornos cloud. Estas herramientas permiten a los atacantes mantener persistencia, moverse lateralmente y exfiltrar información crítica sin depender de infraestructuras tradicionales de control.

¿Cómo protegerse?

✅ Monitorizar comportamiento anómalo en sistemas (procesos, conexiones P2P).
✅ Auditar módulos críticos de sistema y bibliotecas cargadas.
✅ Implementar detección avanzada en entornos cloud y endpoints.

Link: https://gbhackers.com/orbit-rootkit-targets-linux/

Malware basado en campaña de robo de credenciales en la nube (PCPJack)

Resumen: Se ha identificado una campaña activa de malware denominada PCPJack, diseñada para robar credenciales en entornos cloud. Este malware sustituye a otras herramientas maliciosas previamente instaladas en sistemas comprometidos para quedarse como única amenaza y maximizar la exfiltración de información sensible, especialmente en servicios de productividad y desarrollo.

¿Cómo protegerse?

✅ Monitorizar accesos a servicios cloud y detectar comportamientos anómalos.
✅ Revisar regularmente credenciales expuestas o reutilizadas.
✅ Implementar controles de acceso robustos y autenticación multifactor.

Link: https://thehackernews.com/2026/05/pcpjack-credential-stealer-exploits-5.html

Ciberespionaje encubierto como ataque de ransomware tipo “Chaos”

Resumen: Se ha descubierto una campaña de ciberespionaje atribuida al grupo APT MuddyWater en la que los atacantes simulan un ataque de ransomware (aparentando pertenecer al grupo “Chaos”) para ocultar operaciones de robo de información.

¿Cómo protegerse?

✅ Realizar una segmentación de red evitando la propagación del malware.
✅ Monitorizar accesos remotos sospechosos.
✅ Implementar controles de identidad robustos y revisar accesos privilegiados.

Link: https://securityaffairs.com/191765/breaking-news/iranian-cyber-espionage-disguised-as-a-chaos-ransomware-attack.html

Phishing

Microsoft alerta de una campaña masiva de phishing

Resumen: Microsoft detalló una campaña de phishing a gran escala que emplea una cadena multietapa con señuelos corporativos (p. ej., “código de conducta”) para llevar a las víctimas a un flujo Adversary-in-the-Middle (AiTM).

¿Cómo protegerse?

✅ Priorizar métodos MFA resistentes al phishing y reforzar políticas de acceso.
✅ Monitorizar anomalías de sesión y activar alertas de riesgo de inicio de sesión.
✅ Aplicar al correo protección anti-phishing, análisis de URLs y bloqueo de redirección.

Link: https://www.microsoft.com/en-us/security/blog/2026/05/04/breaking-the-code-multi-stage-code-of-conduct-phishing-campaign-leads-to-aitm-token-compromise/

Phishing que suplanta a la AEAT para exigir pagos en criptomonedas

Resumen: La Agencia Tributaria (AEAT) informó de un nuevo caso de phishing en el que se suplanta a la AEAT/Ministerio de Hacienda para presionar a la víctima a realizar un pago en criptomonedas bajo el pretexto de una supuesta regularización o reclamación fiscal.

¿Cómo protegerse?

✅ Desconfiar de cualquier comunicación que solicite pagos en criptomonedas.
✅ Acceder a enlaces usando la sede electrónica desde marcadores verificados.
✅ Reportar cualquier intento sospechoso a los responsables de seguridad o IT.

Link: https://www3.agenciatributaria.gob.es/Sede/condiciones-uso-sede-electronica/aviso-seguridad/novedades/2026/2026/mayo/20/nuevo-phishing-suplantacion-aeat-objetivo-criptomonedas.html

Falsa reparación de correo en Microsoft Teams

Resumen: Se difundió el análisis de una campaña donde los atacantes usan Microsoft Teams como canal de ingeniería social: contactan a empleados con un pretexto creíble para lograr que la víctima ejecute acciones que terminan en instalación de código malicioso o compromiso de credenciales.

¿Cómo protegerse?

✅ Restringir comunicaciones externas en Teams y aplicar controles de seguridad.
✅ Establecer un procedimiento ante estas incidencias.
✅ Monitorizar ejecución de herramientas remotas y correlacionar eventos.

Link: https://ciberprisma.org/2026/05/04/ciberdelincuentes-usan-microsoft-teams-para-distribuir-malware-con-falsa-herramienta-de-reparacion-de-correo/

Brechas de seguridad

Brecha en plataforma educativa Canvas expone datos de usuarios

Resumen: La empresa Instructure, responsable de la plataforma educativa Canvas, confirmó una brecha de seguridad tras un ciberataque vinculado al grupo ShinyHunters. Los atacantes lograron acceder a datos personales de usuarios, incluyendo información de registro y uso de la plataforma.

¿Cómo protegerse?

✅ Evitar reutilizar credenciales en distintos servicios.
✅ Activar la verificación de dos pasos siempre que esté disponible.
✅ Cambiar contraseñas si reutilizan datos filtrados en otros servicios.

Link: https://www.secure.com/news/instructure-canvas-data-breach-shinyhunters

Brecha en Santalucía expone datos personales de asegurados

Resumen: La aseguradora Santalucía notificó un ciberataque que permitió el acceso no autorizado a datos personales de clientes. Entre la información comprometida se encuentran nombres, direcciones, teléfonos, emails y DNI asociados a pólizas.

¿Cómo protegerse?

✅ Extremar la precaución ante llamadas, SMS o correos que soliciten información personal.
✅ Formar empleados para detectar intentos de suplantación basados en datos reales.
✅ Aplicar controles de seguridad sobre datos personales (cifrado, accesos restringidos).

Link: https://www.escudodigital.com/ciberseguridad/seguros-santalucia-brecha-datos.html

Filtración en 7-Eleven expone datos personales de 185.000 personas

Resumen: Se confirmó una brecha de seguridad en la cadena 7-Eleven que expuso datos personales de aproximadamente 185.000 personas, incluyendo nombres, direcciones, teléfonos y fechas de nacimiento. El incidente fue atribuido al grupo ShinyHunters, que publicó los datos tras un intento fallido de extorsión.

¿Cómo protegerse?

✅ Vigilar posibles intentos de fraude o suplantación a través de emails, SMS o llamadas.
✅ Monitorizar exposiciones de datos y posibles fugas.
✅ Disponer de un plan de respuesta a incidentes con protocoles claros de comunicación y mitigación.

Link: https://www.helpnetsecurity.com/2026/05/26/7-eleven-data-breach-shinyhunters/

CVEs

Vulnerabilidad crítica en Microsoft Outlook

Resumen: Microsoft ha publicado una actualización de seguridad para corregir una vulnerabilidad que permite la ejecución remota de código a través de correos electrónicos especialmente manipulados. La vulnerabilidad puede explotarse sin interacción del usuario en algunas configuraciones.
Gravedad: 🔥 Crítica (9.8/10) – Riesgo elevado para organizaciones que utilizan Outlook como principal cliente de correo.
Ejemplo real: Empleados que reciben correos aparentemente legítimos y cuya visualización en el panel de vista previa activa el exploit sin necesidad de abrir adjuntos.

✅ **Solución:** Aplicar los parches de seguridad de Microsoft y deshabilitar el panel de vista previa en entornos de riesgo hasta actualizar.

Link: https://msrc.microsoft.com/update-guide/

Vulnerabilidad en servidores Apache HTTP Server

Resumen: Se ha identificado una vulnerabilidad en Apache HTTP Server que permite ataques de denegación de servicio (DoS) mediante peticiones manipuladas que agotan los recursos del servidor.
Gravedad: 🔥 Alta (8.2/10) – Puede provocar interrupciones en servicios web públicos y aplicaciones críticas.
Ejemplo real: PYMEs con páginas web corporativas alojadas en Apache que pueden sufrir caídas del servicio ante ataques automatizados.

✅ **Solución:** Actualizar Apache a la última versión disponible y configurar límites de peticiones para mitigar ataques de saturación.

Link: https://httpd.apache.org/security/

Vulnerabilidad en dispositivos Fortinet VPN

Resumen: Una vulnerabilidad en dispositivos Fortinet VPN permite a atacantes no autenticados acceder a información sensible o comprometer credenciales mediante explotación remota.
Gravedad: 🔥 Crítica (9.3/10) – Alto impacto en organizaciones que utilizan VPN para acceso remoto.
Ejemplo real: Empresas que utilizan VPN para teletrabajo pueden ver comprometido el acceso a su red si no aplican parches.

✅ **Solución:** Actualizar firmware de los dispositivos Fortinet y revisar accesos remotos en busca de actividad sospechosa.

Link: https://www.fortiguard.com/psirt