Mes: Junio 2026

Resumen mensual

Malware

Malware en Linux mediante rootkit eBPF y robo masivo de credenciales

Resumen: Se ha detectado una campaña que distribuye malware en Linux a través de paquetes npm comprometidos, incluyendo un rootkit basado en eBPF para ocultar actividad. La amenaza roba credenciales de navegadores, tokens de desarrollo (GitHub, Docker, VPN) y datos de herramientas colaborativas, afectando especialmente a entornos de desarrollo y CI/CD.

¿Cómo protegerse?

✅ Auditar dependencias y paquetes de repositorios externos antes de su uso.
✅ Monitorizar comportamientos anómalos en procesos y módulos del kernel.
✅ Proteger credenciales y tokens con rotación y almacenamiento seguro.

Link: https://bitlifemedia.com/2026/06/descubren-un-malware-para-linux-que-roba-credenciales-y-se-oculta-con-un-rootkit-ebpf/

Ataque a la cadena de suministro npm dirigido a entornos cloud y CI/CD

Resumen: Una campaña denominada “Miasma” comprometió más de 30 paquetes npm legítimos de Red Hat para distribuir malware que roba credenciales cloud (AWS, Azure, GCP), secretos de Kubernetes y tokens de desarrollo. El ataque explotó pipelines CI/CD mediante tokens comprometidos, permitiendo acceso a infraestructuras críticas.

¿Cómo protegerse?

✅ Implementar controles de seguridad en pipelines CI/CD y tokens OIDC.
✅ Limitar permisos y aplicar principio de mínimo privilegio en cloud.
✅ Monitorizar accesos a gestores de secretos y actividad anómala en builds.

Link: https://blog.elhacker.net/2026/06/paquetes-npm-de-red-hat-comprometidos.html

Extensión maliciosa de Edge utilizada para desplegar ransomware (Edgecution)

Resumen: Investigadores han detectado una campaña que utiliza una extensión maliciosa de Microsoft Edge denominada “Edgecution” para escapar del sandbox del navegador e instalar un backdoor en Python. Este malware permite ejecutar código en el sistema, robar información y servir como punto de acceso inicial para ransomware mediante técnicas de ingeniería social.

¿Cómo protegerse?

✅ Restringir la instalación de extensiones y aplicar políticas de navegador.
✅ Monitorizar ejecución de procesos anómalos y uso de Native Messaging.
✅ Implementar controles EDR para detectar comportamientos de sandbox escape.

Link: https://www.anavem.com/en/news/cybersecurity/malicious-edge-extension-deploys-ransomware-via-sandbox-escape

Phishing

Campaña de phishing en WhatsApp vinculada a NSO Group y ataques de un solo clic

Resumen: WhatsApp ha desarticulado en junio una campaña de phishing asociada a NSO Group que utilizaba enlaces maliciosos para redirigir a páginas falsas y comprometer dispositivos mediante ataques de “un solo clic”. Estos ataques permiten la infección sin interacción adicional del usuario, aprovechando vulnerabilidades del navegador.

¿Cómo protegerse?

✅ Evitar hacer clic en enlaces recibidos por mensajería sin verificar.
✅ Mantener navegadores y dispositivos actualizados.
✅ Utilizar soluciones de seguridad móvil con capacidad anti-phishing.

Link: https://www.europapress.es/portaltic/ciberseguridad/noticia-whatsapp-pide-declarar-nso-group-desacato-frenar-nueva-campana-phishing-20260609123143.html

Campaña de phishing en WhatsApp que distribuye malware mediante archivos adjuntos

Resumen: Una campaña detectada en junio utiliza mensajes de WhatsApp con archivos adjuntos que simulan documentos financieros para engañar a los usuarios y hacerles ejecutar código malicioso. Este ataque se propaga a través de contactos comprometidos y permite a los atacantes tomar el control completo del equipo.

¿Cómo protegerse?

✅ No abrir archivos adjuntos inesperados, incluso si provienen de contactos conocidos.
✅ Verificar el contexto de los mensajes antes de interactuar con ellos.
✅ Aplicar controles de seguridad en endpoints para bloquear scripts maliciosos.

Link: https://www.notimerica.com/ciencia-tecnologia/noticia-portaltic-campana-maliciosa-mas-reciente-whatsapp-usa-lista-contactos-distribuir-programa-gestion-remota-20260623162859.html

Campaña de phishing sofisticado dirigida a viajeros mediante suplantación de hoteles

Resumen: Investigadores han identificado en junio una campaña de phishing que suplanta hoteles reales mediante mensajes personalizados en WhatsApp. Los atacantes utilizan datos reales de reservas para engañar a las víctimas y redirigirlas a páginas fraudulentas donde introducen sus datos bancarios.

¿Cómo protegerse?

✅ Verificar siempre comunicaciones con hoteles a través de canales oficiales.
✅ No introducir datos bancarios en enlaces recibidos por mensajería.
✅ Activar alertas de movimientos y pagos en cuentas bancarias.

Link: https://www.revistaciberseguridad.com/2026/06/la-sofisticada-estafa-por-whatsapp-que-suplanta-a-tu-hotel-usando-tus-datos-reales/

Brechas de seguridad

Brecha de seguridad en KDDI expone millones de credenciales de correo

Resumen: La empresa japonesa KDDI ha confirmado una brecha de seguridad que podría haber expuesto hasta 14,22 millones de cuentas de correo electrónico y contraseñas. El incidente se originó en vulnerabilidades de software de terceros integrados en sistemas de ISP, permitiendo accesos no autorizados y filtración de datos de usuarios.

¿Cómo protegerse?

✅ Cambiar contraseñas y activar autenticación multifactor en servicios críticos.
✅ Monitorizar accesos sospechosos en cuentas de correo y servicios asociados.
✅ Evaluar la seguridad de proveedores y software de terceros.

Link: https://thecyberexpress.com/kddi-data-breach-14-million-email-leak-2026/

Brecha de seguridad en Kodak compromete millones de registros corporativos

Resumen: Kodak ha confirmado una intrusión atribuida al grupo ShinyHunters que ha comprometido más de 2 millones de registros de clientes y datos internos. El incidente se produjo mediante acceso no autorizado a sistemas corporativos, lo que ha generado riesgos reputacionales y de exposición de información sensible.

¿Cómo protegerse?

✅ Monitorizar accesos a sistemas críticos y detectar exfiltración de datos.
✅ Segmentar redes y limitar accesos según el principio de mínimo privilegio.
✅ Implementar auditorías de seguridad periódicas en sistemas internos.

Link: https://www.cpomagazine.com/cyber-security/kodak-confirms-data-breach-linked-to-shinyhunters-hacking-group/

Brecha de seguridad en Tata Electronics expone datos de Apple y Tesla

Resumen: Tata Electronics ha sufrido un incidente de ciberseguridad en el que un grupo de ransomware afirma haber filtrado más de 200.000 archivos (~630GB) con datos internos, incluidos documentos relacionados con Apple y Tesla. El ataque pone de relieve los riesgos en la cadena de suministro tecnológica.

¿Cómo protegerse?

✅ Evaluar riesgos de terceros y proveedores en la cadena de suministro.
✅ Cifrar datos sensibles y controlar accesos a información crítica.
✅ Implementar monitorización continua y respuesta ante incidentes.

Link: https://gulfnews.com/technology/tata-electronics-breach-how-serious-is-the-alleged-apple-tesla-data-leak-1.500583341

CVEs

Vulnerabilidad crítica en Linux KVM permite escape de máquina virtual

Resumen: e ha identificado una vulnerabilidad en el kernel Linux (KVM/arm64) que permite a un atacante escapar de una máquina virtual y ejecutar código en el host con privilegios root. La publicación de un exploit funcional ha incrementado el riesgo para entornos cloud que utilizan virtualización.
Gravedad: 🔥 Crítica (9.0+/10) – Riesgo elevado en infraestructuras cloud y entornos virtualizados.
Ejemplo real: Un atacante compromete una máquina virtual en un proveedor cloud y, mediante el exploit, obtiene control total del servidor físico subyacente.

✅ **Solución:** Actualizar el kernel Linux a versiones parcheadas y reforzar el aislamiento entre máquinas virtuales.

Link: https://es-us.noticias.yahoo.com/falla-itscape-liberan-exploit-escape-182703942.html

Vulnerabilidad crítica en Cisco Unified CM explotada activamente

Resumen: Se ha detectado la explotación activa de una vulnerabilidad en Cisco Unified Communications Manager que permite a atacantes remotos no autenticados realizar SSRF, escribir archivos en el sistema y escalar privilegios a root. La existencia de PoC públicos ha facilitado su explotación en entornos reales.
Gravedad: 🔥 Crítica (9.8/10) – Alto impacto en sistemas de comunicaciones empresariales.
Ejemplo real: Un atacante accede a un servidor de comunicaciones corporativas expuesto y ejecuta código remoto para comprometer llamadas, datos y credenciales internas.

✅ **Solución:** Aplicar los parches oficiales de Cisco y deshabilitar servicios innecesarios como WebDialer.

Link: https://www.securityweek.com/hackers-exploiting-cisco-unified-cm-vulnerability/

Vulnerabilidad en plugin WordPress expone credenciales sin autenticación

Resumen: Una vulnerabilidad en el plugin Gravity SMTP permite acceder sin autenticación a información sensible como claves API, tokens OAuth y configuraciones completas del sistema.
Gravedad: 🔥 Alta (5.3/10) – Riesgo significativo por explotación masiva y exposición de credenciales.
Ejemplo real: Un atacante lanza una petición HTTP a un endpoint expuesto y obtiene credenciales que le permiten enviar correos en nombre del sitio, facilitando ataques de phishing.

✅ **Solución:** Actualizar el plugin a la versión parcheada y revisar/rotar todas las credenciales expuestas.

Link: https://thenextweb.com/news/gravity-smtp-wordpress-plugin-vulnerability-cve-2026-4020-api-keys-exploit