Edición 11 Julio 2025

CIBER E-DEA

Boletín de Seguridad

e-dea NETWORKS | CYBER SECURITY

Great Place To Work. Certificada NOV 2024 - NOV 2025 COL
icontec ISO 9001 CO-SC-CER890596
icontec ISO 45001 CO-ST-CER890599
icontec ISO / IEC 27001 CO-SI-2001607
IQNET CERTIFIED MANAGEMENT SYSTEM

Los hackers utilizan repositorios de GitHub para alojar malware

El uso de plataformas de desarrollo colaborativo, como GitHub, ha aumentado considerablemente en los últimos años. Sin embargo, este crecimiento también ha sido aprovechado por actores maliciosos que emplean estos repositorios para distribuir malware y llevar a cabo ataques cibernéticos

Técnicas de ocultamiento en GitHub

Los atacantes han desarrollado diversas estrategias para utilizar GitHub como un medio de distribución de malware. Algunas de estas técnicas incluyen:

- **Alojamiento de scripts maliciosos: Los hackers suben archivos que contienen scripts o binarios maliciosos a repositorios públicos o privados de GitHub, disfrazándolos con nombres aparentemente benignos.**
- **Uso de dependencias y librerías: Al incluir código malicioso dentro de dependencias o librerías utilizadas comúnmente en proyectos legítimos, los atacantes logran infiltrarse en sistemas sin levantar sospechas.**
- **Páginas web falsas: Algunos actores crean páginas web que simulan ser sitios oficiales o herramientas populares, redirigiendo a las víctimas a descargar el malware alojado en GitHub.**

Estrategias recomendadas para mitigar riesgos

A fin de protegerse contra la amenaza representada por el uso indebido de repositorios en línea, se sugieren las siguientes prácticas:

- **Análisis estático y dinámico: Implementar herramientas que analicen automáticamente el código antes de integrarlo a proyectos existentes.**
- **Auditoría regular del software utilizado: Realizar revisiones periódicas sobre las dependencias utilizadas para asegurar su legitimidad.**
- **Cultura organizacional proactiva: Fomentar una cultura donde se priorice la seguridad desde las primeras etapas del ciclo de desarrollo (DevSecOps).**

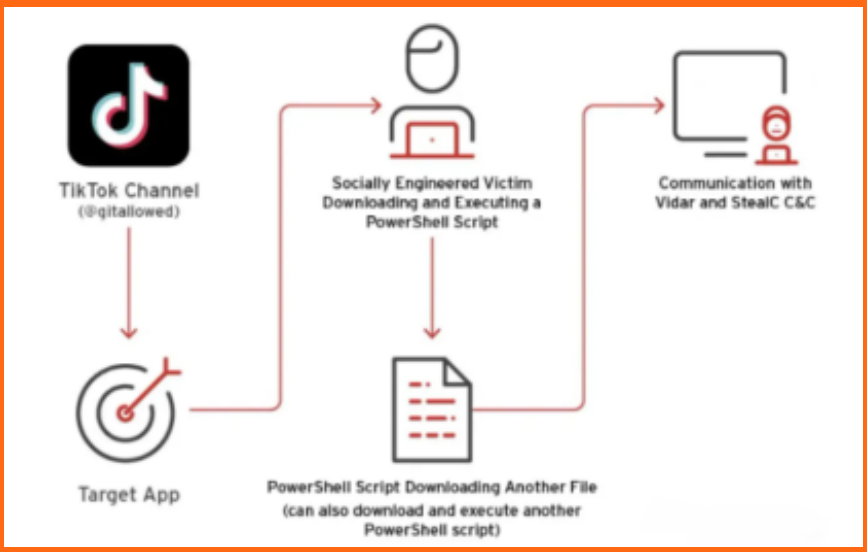
Más información

TikTok y malware: peligrosa combinación

Los atacantes están utilizando TikTok de para propagar software malicioso, engañando a los usuarios con videos que aparentan ser tutoriales útiles.

Estos clips, que muchas veces parecen generados con inteligencia artificial, inducen a las personas a ejecutar comandos que instalan malware como Vidar y StealC, diseñados para robar información personal y financiera..

¿Cómo funciona?



Los videos muestran supuestos “trucos” para activar Windows, desbloquear funciones premium en aplicaciones como CapCut o Spotify, o mejorar el rendimiento del sistema.

Uno de estos videos, por ejemplo, que promete “mejorar Spotify al instante”, ya acumula cerca de medio millón de visualizaciones, más de 20.000 "me gusta" y cientos de comentarios.

Recomendaciones

- Nunca ejecutes comandos de PowerShell que veas en redes sociales, especialmente si provienen de fuentes no verificadas.
- Desconfía de tutoriales que prometen desbloquear funciones premium o activar software de forma gratuita.
- Mantén actualizado tu antivirus y sistema operativo.
- Activa la autenticación en dos pasos en todas tus cuentas.
- Reporta contenido sospechoso en TikTok para ayudar a frenar su propagación.

Más información

Computación cuántica: un llamado a la acción para los profesionales de la seguridad

La computación cuántica promete transformar las industrias, pero también representa un serio riesgo para la ciberseguridad. Su capacidad para romper los sistemas de cifrado actuales podría comprometer la privacidad de millones de usuarios y la seguridad de datos sensibles.

Esta falta de preparación se debe a la creencia de que el riesgo aún está lejano o a una comprensión limitada del impacto real que puede tener.
El Instituto Nacional de Estándares y Tecnología (NIST) ya ha empezado a publicar estándares criptográficos poscuánticos, pero solo el 7% de los encuestados afirma comprenderlos bien, lo que revela una brecha importante de conocimiento técnico. Al mismo tiempo, el 55% de las organizaciones aún no ha tomado ninguna medida concreta, a pesar de que el 57% reconoce los riesgos y el 46% el potencial innovador de esta tecnología.

El Instituto Nacional de Estándares y Tecnología (NIST) ya ha empezado a publicar estándares criptográficos poscuánticos, pero solo el 7% de los encuestados afirma comprenderlos bien, lo que revela una brecha importante de conocimiento técnico. Al mismo tiempo, el 55% de las organizaciones aún no ha tomado ninguna medida concreta, a pesar de que el 57% reconoce los riesgos y el 46% el potencial innovador de esta tecnología.

Ante esta situación, se plantea un llamado urgente a las siguientes acciones:

1. Educación: formar a los responsables de la toma de decisiones mediante programas, talleres y simulaciones.
2. Evaluación de vulnerabilidades: identificar sistemas críticos y datos sensibles para priorizar su protección.
3. Cifrado resistente a la computación cuántica: migrar a nuevos algoritmos seguros compatibles con los estándares del NIST.
4. Modernización tecnológica: reforzar infraestructuras digitales mediante controles, actualizaciones, auditorías y sistemas de detección.

Además, se destaca el papel clave de la inteligencia artificial como aliada en la mitigación de riesgos cuánticos. La IA puede anticipar amenazas, automatizar respuestas a incidentes y adaptarse continuamente a nuevas vulnerabilidades.

De esta manera se puede determinar que la era cuántica representa tanto una amenaza como una oportunidad. Prepararse implica actuar ahora: educar, adaptar infraestructuras, adoptar nuevos estándares criptográficos y presupuestar inversiones sostenidas en seguridad

Actualización de Emergencia Corrige Fallo Crítico en Máquinas Virtuales

Microsoft lanzó la actualización KB5064489 para resolver un grave error que impedía el arranque de máquinas virtuales con VBS habilitado y Secure Boot desactivado. Este fallo, introducido con las actualizaciones del Patch Tuesday de julio, afecta a Windows 11 24H2 y Windows Server 2025.

¿Qué estaba pasando?

Las VMs (especialmente en Azure versión 8.0 y en hipervisores locales) simplemente no iniciaban si el host ofrecía VBS y la VM no tenía Trusted Launch activado. El problema se originó por un fallo en la inicialización segura del kernel.

¿Quiénes son afectados?

Microsoft indicó que las configuraciones más afectadas fueron aquellas que combinan:
Windows Server 2025 o Windows 11 24H2.
Máquinas virtuales con VBS activado (esto puede habilitarse de forma predeterminada en muchas imágenes).
VMs que usan configuración "Standard" sin Trusted Launch habilitado.
Infraestructura Azure corriendo en plataforma v8.0 o superior.
Algunos hipervisores locales (ej. Windows Server 2016 con Hyper-V) también pueden verse afectados si se usan imágenes nuevas de Windows Server 2025 con VBS activado.

Solución

Microsoft ha lanzado la actualización KB5064489 como una solución fuera de banda (es decir, no incluida en las actualizaciones regulares). Se recomienda instalar esta actualización y evitar temporalmente la instalación de la acumulativa KB5062553, ya que podría causar problemas. Además, Microsoft ha actualizado las imágenes de instalación de Windows Server 2025 para prevenir que estas fallas se presenten en nuevas implementaciones del sistema.

Más información

Vulnerabilidades destacadas

CVE-2025-25257

FortiWeb

Versiones afectadas
7.0.0 a 7.6.3

Es una vulnerabilidad que permite a los atacantes ejecutar comandos SQL dañinos sin iniciar sesión. Mediante el envío de solicitudes web especiales, pueden tomar el control total del sistema, incluso como root, instalar shells web, robar datos o comprometer completamente el dispositivo.

CVE-2025-6558

Google

Versiones afectadas
138.0.7204.157

Es una vulnerabilidad que permite a un atacante remoto eludir la zona protegida del navegador y potencialmente ejecutar código arbitrario aprovechando una validación de entrada insuficiente al procesar una página HTML especialmente diseñada

CVE-2025-20309

Cisco

Versiones afectadas
15.0.1.13010-1 a 15.0.1.13017-1

Es una vulnerabilidad que permitir que un atacante remoto no autenticado inicie sesión en un dispositivo afectado utilizando la cuenta raíz, que tiene credenciales estáticas predeterminadas que no se pueden modificar ni eliminar. Esta vulnerabilidad se debe a la presencia de credenciales de usuario estáticas para la cuenta raíz, reservadas para su uso durante el desarrollo.

Ciber incidentes en Colombia y en el mundo

Alerta de phishing con Bre-B y el avance del ransomware con IA

La noticia de Impacto TIC alerta sobre una nueva campaña de phishing que utiliza el nombre "BRE-B" para engañar a usuarios en Colombia, suplantando entidades legítimas como la Registraduría Nacional. Los atacantes buscan robar credenciales y datos personales mediante correos falsos con enlaces maliciosos. Además, se advierte sobre el avance del ransomware potenciado por inteligencia artificial (IA), lo que permite ataques más personalizados, automatizados y difíciles de detectar, aumentando significativamente los riesgos para empresas y usuarios. La nota enfatiza la necesidad de reforzar medidas de ciberseguridad y concienciación digital.

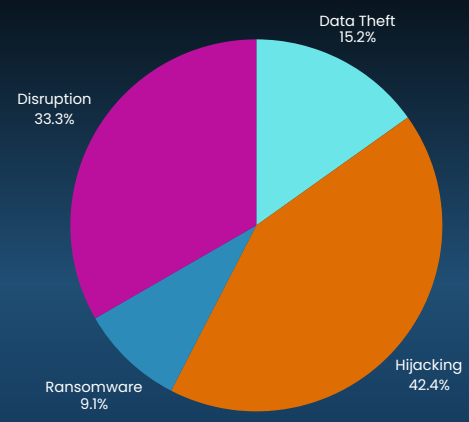
Tipo de incidente: Phishing (Suplantación de identidad)

Más información

El mundo

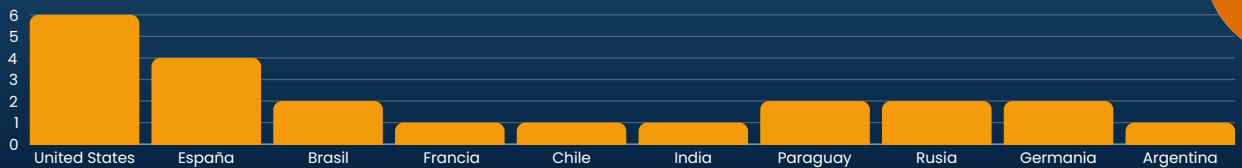
19
Ciber incidentes

TIPO DE INCIDENTE



SECTORES AFECTADOS

PAISES ATACADOS



Más información

CYBER SECURITY

e-dea NETWORKS

CIBER E-DEA

Boletín de Seguridad

E-dea Networks

@e_deanetworks

E-dea Networks

Csirt E-dea

e-dea.co