Subsecretaría de Ciberdefensa

Boletín de Noticias de Ciberseguridad

Informe sobre incidentes y ciberamenazas Nro. 98/2021

Este boletín periódico es un resumen seleccionado de las últimas vulnerabilidades, incidentes de seguridad e informes recopilados de fuentes internacionales conocidas dedicadas a la seguridad informática. Está destinado a las áreas de ciberseguridad de la Defensa como información de interés general para su difusión.

07/04/2021

- Un nuevo *rootkit* sigiloso se infiltró en las redes de organizaciones de alto perfil de Asia y Africa.
  https://thehackernews.com/2021/05/new-stealthy-rootkit-infiltrated.html
  https://www.zdnet.com/article/new-moriya-rootkit-stealthily-backdoors-windows-systems/

- Advertencia de ciberseguridad en USA y UK, los piratas informáticos rusos están apuntando a por lo menos 11 vulnerabilidades que ya deben ser corregidas.
  https://www.zdnet.com/article/cybersecurity-warning-russian-hackers-are-targeting-these-vulnerabilities-so-patch-now/
  https://securityaffairs.co/wordpress/117667/apt/apt29-changes-ttps.html

- El resumen semanal del ransomware al 7 de mayo de 2021.
  https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-may-7th-2021-attacking-healthcare/

08/05/2021

- **Un ciberataque interrumpe el oleoducto Colonial, en EE.UU., el mayor proveedor de combustible en ese país pues transporta 100 millones de galones al día.**
  https://www.cyberscoop.com/gas-pipeline-cyberattack-ransomware-colonial/
  https://threatpost.com/pipeline-crippled-ransomware/165963/
  https://twitter.com/CISAgov/status/1391124273155219459

09/05/2021

- Un error de inyección SQL en el plugin antispam de WordPress expone los datos de los usuarios.
  https://securityaffairs.co/wordpress/117721/security/anti-spam-wordpress-plugin-flaw.html

10/05/2021

- Ataque de ransomware a oleoducto: EE.UU. aplica normas de **emergencia** para mantener el flujo de combustible.
  https://www.zdnet.com/article/pipeline-ransomware-attack-us-invokes-emergency-transport-rules-to-keep-fuel-flowing/
  https://www.bleepingcomputer.com/news/security/us-declares-state-of-emergency-after-ransomware-hits-largest-pipeline/

- El grupo de piratas informáticos Lemon Duck usa las vulnerabilidades de Microsoft Exchange Server en nuevos ataques
  https://www.zdnet.com/article/lemon-duck-hacking-group-adopts-microsoft-exchange-server-vulnerabilities-in-new-attacks/

- La ciudad de Tulsa, es la última ciudad estadounidense afectada por un ataque de ransomware.
  https://securityaffairs.co/wordpress/117756/cyber-crime/city-of-tulsa.html

- Estados Unidos y Australia advierten un aumento de los ataques del ransomware Avaddon.

https://www.bleepingcomputer.com/news/security/us-and-australia-warn-of-escalating-avaddon-ransomware-attacks/

- La universidad tecnológica más antigua de EE.UU. cancela exámenes tras ciberataque.
https://www.infosecurity-magazine.com/news/university-cancels-exams-after/

TRABAJOS, ESTUDIOS Y ANÁLISIS ABOCADOS A LAS TEMÁTICAS DE LA CIBERSEGURIDAD

- Microsoft detectó una campaña de amenaza al correo electrónico empresarial (BEC) a gran escala que se centró en más de 120 organizaciones.
https://www.bleepingcomputer.com/news/security/microsoft-business-email-compromise-attack-targeted-dozens-of-orgs/
- Medidas de seguridad añadidas y cambios en el protocolo TLS 1.3.
https://blog.devgenius.io/added-security-measures-and-changes-in-tls-1-3-fd93bbfecb8f
- Documento recién desclasificado por la NSA sobre criptografía en los años 70.
https://www.schneier.com/blog/archives/2021/05/newly-unclassified-nsa-document-on-cryptography-in-the-1970s.html
- Más del 25% de los enlaces de salida de Tor espiaban las actividades de los usuarios en la "web oscura".
https://thehackernews.com/2021/05/over-25-of-tor-exit-relays-are-spying.html

NOTAS DE INTERÉS

- El ransomware Cuba se asocia con Hancitor para los ataques impulsados por el spam.
https://www.bleepingcomputer.com/news/security/cuba-ransomware-partners-with-hancitor-for-spam-fueled-attacks/
- DefakeHop: Un método de detección de deepfakes que aborda la detección y el reconocimiento de amenazas.
https://www.helpnetsecurity.com/2021/05/07/defakehop-deepfake-detection-method/
- La última defensa contra las estafas bancarias: Tu voz.
https://www.zdnet.com/article/the-latest-defence-against-banking-scams-your-voice/
- WhatsApp restringirá sus funciones si te niegas a compartir datos con Facebook.
https://www.bleepingcomputer.com/news/technology/whatsapp-to-restrict-features-if-you-refuse-facebook-data-sharing/
- Informe de análisis de malware de CISA da detalles técnicos del ransomware FiveHands.
https://securityaffairs.co/wordpress/117729/malware/fivehands-ransomware-cisa-mar.html
- Los expertos sugieren que el plan de la aseguradora francesa AXA de evitar el pago del ransomware sentará un precedente.
https://www.cyberscoop.com/axa-ransomware-cyber-insurance-policies/

ACTUALIZACIONES DE SEGURIDAD

- Cisco publica soluciones a las vulnerabilidades de seguridad del software SD-WAN e HyperFlex.
https://www.zdnet.com/article/cisco-publishes-solutions-to-sd-wan-and-hyperflex-software-security-vulnerabilities/
- Cuatro importantes actualizaciones de privacidad y seguridad de Google que debes saber.
https://thehackernews.com/2021/05/4-major-privacy-and-security-updates.html