@mindefarg
argentina.gob.ar/defensa
Ministerio de Defensa
Argentina
Edificio Libertador
Azopardo 250 (CABA)
(54 11) 4346-8836/9

Subsecretaría de Ciberdefensa

Boletín de Noticias de Ciberseguridad

Informe sobre incidentes y ciberamenazas Nro. 126 – Año 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.

13/08/2021

- Sitios de WordPress fueron utilizados en la campaña de Spear-Phishing de Aggah.
  https://threatpost.com/aggah-wordpress-spearphishing/168657/
- Un error en el software de gestión de gimnasios permite a piratas informáticos borrar el historial de ejercicios.
  https://www.bleepingcomputer.com/news/security/bugs-in-gym-management-software-let-hackers-wipe-fitness-history/
- Tribunal de Dallas, EE.UU., pierde 8 TB de datos de casos criminales.
  https://www.infosecurity-magazine.com/news/dallas-loses-8tb-of-criminal-case/
- Windows 365 expone las credenciales de Microsoft Azure en texto plano.
  https://www.bleepingcomputer.com/news/microsoft/windows-365-exposes-microsoft-azure-credentials-in-plaintext/

14/08/2021

- Se advierte a los brokers estadounidenses de los persistentes ataques de phishing.
  https://www.bleepingcomputer.com/news/security/us-brokers-warned-of-ongoing-phishing-attacks-impersonating-finra/
- "DeepBlueMagic": un ransomware recién descubierto con un modus operandi único.
  https://www.ehackingnews.com/2021/08/deepbluemagic-newly-discovered.html

15/08/2021

- Un bug de Ford expuso los registros de clientes y empleados en los sistemas internos.
  https://www.bleepingcomputer.com/news/security/ford-bug-exposed-customer-and-employee-records-from-internal-systems/
- Un hacker afirma haber robado los datos de 100 millones de clientes de T-mobile en Alemania.
  https://www.theverge.com/2021/8/15/22626270/t-mobile-investigating-report-customer-data-breach

16/08/2021

- Variante de AdLoad elude las defensas de seguridad de Apple para atacar los sistemas macOS.
  https://thehackernews.com/2021/08/new-adload-variant-bypasses-apples.html
  https://www.zdnet.com/article/researchers-discover-new-adload-malware-campaigns-against-macs-and-apple-products/
- **Lista secreta de vigilancia de terroristas con 2 millones de registros expuestos en línea.**
  https://www.bleepingcomputer.com/news/security/secret-terrorist-watchlist-with-2-million-records-exposed-online/
- El ransomware Hive ataca al Memorial Health System y roba los datos de los pacientes.
  https://www.bleepingcomputer.com/news/security/hive-ransomware-attacks-memorial-health-system-steals-patient-data/

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

- Hackers son descubiertos utilizando código Morse en ataques de phishing para evadir detección.
https://thehackernews.com/2021/08/hackers-spotted-using-morse-code-in.html
- El ransomware SynAck libera las claves de descifrado tras el cambio de marca de El_Cometa.
https://www.bleepingcomputer.com/news/security/synack-ransomware-releases-decryption-keys-after-el-cometa-rebrand/
- **Los atacantes pueden aprovechar los firewalls y las zonas intermedias para amplificar los ataques DDoS.**
https://thehackernews.com/2021/08/attackers-can-weaponize-firewalls-and.html
- Un desarrollador de malware infecta su propio PC y los datos terminaron en una plataforma de inteligencia de cibercrimen.
https://www.bleepingcomputer.com/news/security/malware-dev-infects-own-pc-and-data-ends-up-on-intel-platform/

NOTAS DE INTERÉS

- Los hospitales siguen sin estar protegidos contra las peligrosas vulnerabilidades.
https://www.helpnetsecurity.com/2021/08/13/hospitals-vulnerabilities/
- La actualización KB5005033 de *PrintNightmare* está causando problemas de rendimiento en Windows 10.
https://betanews.com/2021/08/12/printnightmare-fixing-kb5005033-update-is-causing-performance-issues-in-windows-10/
- Bandas de ransomware que explotan las vulnerabilidades de Windows Print Spooler.
https://thehackernews.com/2021/08/ransomware-gangs-exploiting-windows.html
- Los hackers buscan activamente servidores Microsoft Exchange sin parches.
https://thehackernews.com/2021/08/hackers-actively-searching-for.html
- Los ciberatacantes adoptan los CAPTCHA para ocultar el phishing y el malware.
https://threatpost.com/cyberattackers-captchas-phishing-malware/168684/
- Facebook agrega el cifrado de extremo a extremo para las llamadas de audio y vídeo en Messenger.
https://thehackernews.com/2021/08/facebook-adds-end-to-end-encryption-for.html
- Una herramienta de código abierto puede extraer las credenciales de Microsoft Azure de Windows 365 en texto plano.
https://betanews.com/2021/08/14/open-source-tool-can-pull-microsoft-azure-credentials-from-windows-365-in-plain-text/
- **Un anuncio de trabajo publicado por el Ministerio de Defensa del Reino Unido reveló la existencia de un escuadrón secreto de hacking.**
https://securityaffairs.co/wordpress/121172/cyber-warfare-2/uk-ministry-of-defence-secret-hacking-squad.html
- Fueron afectados 65 distribuidores por graves vulnerabilidades en los chips de Realtek.
https://www.helpnetsecurity.com/2021/08/16/realtek-rtl819xd-vulnerability/
- Los recientes ataques a Irán fueron orquestados por el grupo Indra.
https://securityaffairs.co/wordpress/121190/hacking/eindra-group-attacks-iran.html