@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. 66/2021

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.

05/01/2021

- ElectroRAT drena fondos de billeteras de criptomonedas por miles de dólares.
https://arstechnica.com/information-technology/2021/01/cryptocurrency-stealer-for-windows-macos-and-linux-went-undetected-for-a-year/

- Los sitios del gobierno indio han filtrado los resultados de la prueba de COVID-19 de pacientes.
https://www.bleepingcomputer.com/news/security/indian-government-sites-leaking-patient-covid-19-test-results/

- El API de conversión de voz a texto de Google puede ayudar a los atacantes a evitar fácilmente Google reCAPTCHA.
https://thehackernews.com/2021/01/google-speech-to-text-api-can-help.html

- Un hacker publica, gratuitamente, los datos de 10.000 cuentas de American Express en México.
https://www.bleepingcomputer.com/news/security/hacker-posts-data-of-10-000-american-express-accounts-for-free/

- Agencias del gobierno de EE.UU. informan que los hackers del estado ruso probablemente están detrás del pirateo a SolarWinds.
https://www.darkreading.com/risk/fbi-cisa-nsa-and-odni-cite-russia-in-joint-statement-on-serious-solarwinds-attacks/d/d-id/1339829

06/01/2021

- **WhatsApp eliminará su cuenta si no está de acuerdo en compartir datos con Facebook.**
https://thehackernews.com/2021/01/whatsapp-will-delete-your-account-if.html

- Los *hackers* de SolarWinds tuvieron acceso a más de 3.000 cuentas de correo electrónico del Departamento de Justicia de EE.UU.
https://www.bleepingcomputer.com/news/security/solarwinds-hackers-had-access-to-over-3-000-us-doj-email-accounts/

- Nissan está investigando la posible exposición de códigos fuente.
https://www.cyberscoop.com/nissan-source-code-leak-exposure-investigation/

07/01/2021

- La empresa de software JetBrains niega ser el punto de origen del *hackeo* a SolarWinds.
https://www.zdnet.com/article/jetbrains-denies-being-the-origin-point-of-the-solarwinds-hack/
https://www.theregister.com/2021/01/07/jetbrains_solarwinds_accusation/

- *Hackers* norcoreanos usan el troyano RokRat en sus campañas contra el sur.
https://www.zdnet.com/article/north-korean-hackers-launch-rokrat-trojan-in-campaigns-against-the-south/

- Múltiples autores de malware Linux están usando el *cifrador* y cargador de memoria "Ezuri" para hacer que su código sea indetectable para los productos antivirus.
https://www.bleepingcomputer.com/news/security/linux-malware-authors-use-ezuri-golang-crypter-for-zero-detection/

- Año nuevo, nuevo ransomware: Babuk Locker afecta a las grandes corporaciones.
https://threatpost.com/ransomware-babuk-locker-large-corporations/162836/

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

- La NSA acaba de desclasificar y publicar una versión redactada de Criptoanálisis Militar, Parte III, de Lambros D. Callimahos, octubre de 1977.
https://www.schneier.com/blog/archives/2021/01/military-cryptanalytics-part-iii.html

- Un nuevo ransomware llamado Babuk Locker se centra en víctimas corporativas, en ataques operados por humanos, primero del 2021.
https://www.bleepingcomputer.com/news/security/babuk-locker-is-the-first-new-enterprise-ransomware-of-2021/

NOTAS DE INTERÉS

- El ransomware Ryuk es la principal amenaza para el sector de la salud.
https://www.bleepingcomputer.com/news/security/ryuk-ransomware-is-the-top-threat-for-the-healthcare-sector/

- Un ataque a la cadena de suministro de software por un ATP de Corea del Norte tiene como objetivo a los inversores en acciones.
https://www.bleepingcomputer.com/news/security/north-korean-software-supply-chain-attack-targets-stock-investors/

- Una función de Telegram expone la dirección exacta del usuario a los hackers.
https://arstechnica.com/information-technology/2021/01/telegram-feature-exposes-your-precise-address-to-hackers/

- Mozilla Firefox está desactivando la tecla de retroceso para evitar la pérdida de datos.
https://www.bleepingcomputer.com/news/software/mozilla-firefox-disabling-backspace-key-to-prevent-data-loss/

ACTUALIZACIONES DE SEGURIDAD

- Un proveedor de telefonía móvil italiano (Vodafone) ofrece reemplazar las tarjetas SIM después de una masiva brecha de datos.
https://www.zdnet.com/article/italian-mobile-operator-offers-to-replace-sim-cards-after-massive-data-breach/

- Google advierte de un error crítico de ejecución del código remoto de Android.
https://threatpost.com/google-warns-of-critical-android-remote-code-execution-bug/162756/
https://source.android.com/security/bulletin/2021-01-01

- CISA actualiza la directiva de emergencia 21-01 con orientación complementaria y de alerta de actividades sobre riesgos en SolarWinds Orion.
https://us-cert.cisa.gov/ncas/current-activity/2021/01/06/cisa-updates-emergency-directive-21-01-supplemental-guidance-and