@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. 120 – 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.

23/07/2021

- **Akamai afirma que no hubo ciberataque en la interrupción generalizada de Internet.**
  https://www.cyberscoop.com/akamai-outage-cyberattack-dns/
- Saudi Aramco confirma la filtración de datos tras el pedido de rescate cibernético de 50 millones de dólares.
  https://arstechnica.com/information-technology/2021/07/saudi-aramco-confirms-data-leak-after-50-million-cyber-ransom-demand/
- El malware para macOS *XCSSET* ahora afecta a Google Chrome y al software de Telegram.
  https://thehackernews.com/2021/07/nasty-macos-malware-xcsset-now-targets.html
- Falsos instaladores de Windows 11 se utilizan ahora para infectar con malware.
  https://www.bleepingcomputer.com/news/security/fake-windows-11-installers-now-used-to-infect-you-with-malware/
- Kaseya comenta que ya tiene la clave de descifrado de REvil y que funciona.
  https://www.zdnet.com/article/kaseya-says-it-has-now-got-the-revil-ransomware-decryption-key-and-it-works/

24/07/2021

- Computadoras japonesas afectadas por un malware ante los Juegos Olímpicos de Tokio 2021.
  https://securityaffairs.co/wordpress/120513/malware/2021-tokyo-olympics-wiper.html
- La policía holandesa detiene a 2 *hackers* vinculados a la red de ciberdelincuencia "Fraud Family".
  https://thehackernews.com/2021/07/dutch-police-arrest-two-hackers-tied-to.html

25/07/2021

- **Kaspersky advierte de los peligros potenciales de la descarga de Windows 11**
  https://betanews.com/2021/07/25/kaspersky-warns-about-the-potential-dangers-of-downloading-windows-11/
- Un autor de amenazas ofrece la base de datos secreta de Clubhouse que contiene 3.8 mil millones de números de teléfono.
  https://securityaffairs.co/wordpress/120553/hacking/threat-actor-offers-clubhouse-secret-database-containing-3-8b-phone-numbers.html
- THORChain sufre otro gran *hackeo* por un total de 8 millones de dólares.
  https://www.ehackingnews.com/2021/07/thorchain-suffers-another-major-hack.html

26/07/2021

- El director de WhatsApp asegura que los funcionarios del gobierno y los aliados de EE.UU. son el objetivo del programa espía Pegasus.
  https://www.zdnet.com/article/whatsapp-chief-says-government-officials-us-allies-targeted-by-nso-groups-pegasus-spyware/

- El Departamento de Oportunidades Económicas (DEO) de Florida, EE.UU., revela una filtración de datos que afecta a 58.000 cuentas.
https://www.darkreading.com/attacks-breaches/florida-deo-discloses-data-breach-affecting-58-000-accounts

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

- El nuevo ataque PetitPotam permite tomar el control de los dominios de Windows.
https://www.bleepingcomputer.com/news/microsoft/new-petitpotam-attack-allows-take-over-of-windows-domains/
- **Un explosivo informe sobre software espía de NSO muestra los límites de la seguridad de iOS y Android.**
https://arstechnica.com/information-technology/2021/07/an-explosive-spyware-report-shows-limits-of-ios-android-security/
- Microsoft alerta sobre el malware LemonDuck dirigido a sistemas Windows y Linux.
https://www.microsoft.com/security/blog/2021/07/22/when-coin-miners-evolve-part-1-exposing-lemonduck-and-lemoncat-modern-mining-malware-infrastructure/
- Los autores de malware utilizan lenguajes de programación "exóticos".
https://threatpost.com/malware-makers-using-exotic-programming-languages/168117/
- Signal corrige un error que enviaba imágenes aleatorias a contactos equivocados.
https://www.bleepingcomputer.com/news/security/signal-fixes-bug-that-sent-random-images-to-wrong-contacts/

NOTAS DE INTERÉS

- El phishing supera la seguridad del correo electrónico con las páginas de Milanote.
https://threatpost.com/phish-email-security-milanote/168021/
- Incluso después del cierre de Emotet, los documentos de Office representan el 43% de todas las descargas de malware.
https://www.zdnet.com/article/even-after-emotet-takedown-office-docs-deliver-43-of-all-malware-downloads-now/
- Atacantes implementan criptomineros en clústeres Kubernetes a través de Argo Workflows.
https://www.bleepingcomputer.com/news/security/attackers-deploy-cryptominers-on-kubernetes-clusters-via-argo-workflows/
- El pago medio por ransomware disminuyó un 38% en el segundo trimestre de 2021, según un nuevo informe de Coveware.
https://www.cyberscoop.com/average-ransomware-payment-decline-2021/
- Seguridad: la adopción de 2FA es increíblemente baja entre los usuarios de Twitter.
https://betanews.com/2021/07/23/security-2fa-adoption-is-incredibly-low-with-twitter-users/
- **Incorporaron un malware en las "neuronas" de una IA y funciona de forma asombrosa.**
https://www.ehackingnews.com/2021/07/researchers-embedded-malware-into-ais.html
- **Y otra vez el ganador es: Signal!**
https://cybersonthestorm.com/y-otra-vez-el-ganador-es-signal/

ACTUALIZACIONES DE SEGURIDAD

- **Apple repara vulnerabilidad de día cero en iOS, iPadOS y macOS bajo ataque activo.**
https://www.theregister.com/2021/07/27/apple_patches_zeroday/