@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. 144 – 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.

Noticias de ciberseguridad entre el 01/12/21 y el 07/12/21

- Empresa de pruebas de ADN informa una filtración de datos que afecta a 2,1 millones de personas.
  https://www.bleepingcomputer.com/news/security/dna-testing-firm-discloses-data-breach-affecting-21-million-people/
- Finlandia se enfrenta a una oleada de mensajes de texto que difunden *flubots*.
  https://threatpost.com/finland-flubot-text-messages/176649/
- Planned Parenthood LA: ataque ransomware vulnera los datos médicos de 400.000 pacientes.
  https://www.zdnet.com/article/planned-parenthood-la-announces-ransomware-incident-healthcare-info-of-400000-patients-leaked/
- Un grupo de amenazas ataca de nuevo al proveedor de plataformas en la nube, Zoho.
  https://threatpost.com/threat-group-takes-aim-again-at-cloud-platform-provider-zoho/176732/
- Roban 200 millones de dólares en tokens de criptodivisas de la plataforma BitMart.
  https://thehackernews.com/2021/12/hackers-steal-200-million-worth-of.html
- Cientos de supermercados SPAR de GB, cierran y cambian a efectivo tras el ciberataque.
  https://www.infosecurity-magazine.com/news/cyberattack-closes-uk-convenience/

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

- La red de bots EwDoor afecta los dispositivos de borde de red de AT&T en empresas estadounidenses.
  https://arstechnica.com/information-technology/2021/12/thousands-of-att-customers-in-the-us-infected-by-new-data-stealing-malware/
- La herramienta de VirusTotal Collections ayuda a mantener ordenadas las listas de IoC.
  https://www.virustotal.com/gui/collection/malpedia_win_gandcrab
- Utilizan cada vez más la técnica de inyección de templates RTF en los ataques de phishing.
  https://thehackernews.com/2021/12/hackers-increasingly-using-rtf-template.html
- La sigilosa banda "WIRTE" tiene como objetivo los gobiernos de Oriente Medio.
  https://threatpost.com/wirte-middle-eastern-governments/176688/
- Los satélites de EE.UU. son atacados todos los días, según un general de la Fuerza Espacial.
  https://www.thedrive.com/the-war-zone/43328/u-s-satellites-are-being-attacked-everyday-according-to-space-force-general
- Advierten a los usuarios iraníes de la difusión de campañas de phishing por SMS.
  https://thehackernews.com/2021/12/researchers-warn-iranian-users-of.html
- Nueve routers WiFi utilizados por millones de personas resultaron vulnerables a 226 fallas.
  https://www.bleepingcomputer.com/news/security/nine-wifi-routers-used-by-millions-were-vulnerable-to-226-flaws/

- ¿Quién es el intermediario de acceso a la red "Babam"?
https://krebsonsecurity.com/2021/12/who-is-the-network-access-broker-babam/
- Catorce nuevos ataques XS-Leaks (Cross-Site Leaks) afectan a todos los navegadores actuales.
https://thehackernews.com/2021/12/14-new-xs-leaks-cross-site-leaks.html
- El grupo NICKEL se centra en las organizaciones gubernamentales de América Latina y Europa.
https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/

NOTAS DE INTERÉS

- La operación del ransomware Yanluowang evoluciona con afiliados experimentados.
https://www.bleepingcomputer.com/news/security/yanluowang-ransomware-operation-matures-with-experienced-affiliates/
- Los hackers podrían robar datos encriptados ahora y descifrarlos con ordenadores cuánticos más adelante, advierten los analistas.
https://www.zdnet.com/article/chinese-hackers-could-steal-data-now-and-crack-it-with-quantum-computers-later-warns-report/
- Teléfonos de empleados del Depto. de Estado de EE.UU. fueron *hackeados* con un programa espía de NSO.
https://securityaffairs.co/wordpress/125260/hacking/nso-group-spyware-us-officials.html/
- EE.UU. emite una directiva de ciberseguridad para las aerolíneas y los ferrocarriles.
https://www.infosecurity-magazine.com/news/cybersecurity-directive-airlines/
- FBI: Un grupo de ransomware cubano atacó a 49 organizaciones de infraestructuras críticas.
https://www.zdnet.com/article/fbi-cuba-ransomware-hit-49-critical-infrastructure-organizations/
- El jefe del Cibercomando reconoce acciones militares de EE.UU. contra grupos de ransomware.
https://www.cyberscoop.com/naksone-cyber-command-ransomware/
- Francia advierte de que los ciberespías de Nobelium atacan a las organizaciones francesas.
https://www.bleepingcomputer.com/news/security/france-warns-of-nobelium-cyberspies-attacking-french-orgs/
- Los “actores” rusos del ataque a SolarWinds, afectan a empresas y gobiernos de todo el mundo.
https://www.darkreading.com/threat-intelligence/russian-actors-hit-global-business-government-targets
- Los clústeres de la nube de Apache Kafka exponen datos sensibles de grandes empresas.
https://threatpost.com/apache-kafka-cloud-clusters-expose-data/176778/
- Un grupo que se hace pasar por el gobierno iraní roba la información de las tarjetas de crédito y crea una red de bots.
https://www.zdnet.com/article/hackers-pretending-to-be-iranian-govt-use-sms-messages-to-steal-credit-card-info-create-botnet/
- Microsoft interviene 42 dominios web maliciosos utilizados por hackers chinos.
https://thehackernews.com/2021/12/microsoft-seizes-42-malicious-web.html

ACTUALIZACIONES DE SEGURIDAD

- Se han corregido errores críticos que afectan a 150 modelos de impresoras HP.
https://www.zdnet.com/article/printing-shellz-critical-bugs-impacting-150-hp-printers-patched/
https://thehackernews.com/2021/11/critical-wormable-security-flaw-found.html
- Mozilla *parchea* un fallo criptográfico crítico.
https://nakedsecurity.sophos.com/2021/12/03/mozilla-patches-exploitable-bigsig-cryptographic-bug/
https://thehackernews.com/2021/12/critical-bug-in-mozillas-nss-crypto.html