@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. 79/2021

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.

26/02/2021

- Un laboratorio de la Universidad de Oxford, vinculado a la investigación sobre el COVID-19, es objetivo de los piratas informáticos.
  https://www.zdnet.com/article/oxford-university-biochemical-lab-involved-in-covid-19-research-targeted-by-hackers/
- Lazarus ataca a las empresas de defensa con el malware ThreatNeedle.
  https://threatpost.com/lazarus-targets-defense-threatneedle-malware/164321/
- Una extensión malintencionada de Firefox permitió a hackers apropiarse de cuentas de Gmail.
  https://www.bleepingcomputer.com/news/security/malicious-firefox-extension-allowed-hackers-to-hijack-gmail-accounts/

27/02/2021

- La banda “Hotarus Corp” hackeó el Ministerio de Finanzas de Ecuador y el Banco Pichincha.
  https://securityaffairs.co/wordpress/115079/malware/hotarus-corp-hacked-ecuador-entities.html

28/02/2021

- La empresa de telecomunicaciones estadounidense T-Mobile confirma la filtración de datos y los ataques de intercambio de tarjetas SIM.
  https://www.ehackingnews.com/2021/02/american-telecommunications-firm-t.html
- La bolsa de criptomonedas Cryptopia, con sede en Nueva Zelanda, ha sido hackeada de nuevo.
  https://securityaffairs.co/wordpress/115099/hacking/cryptopia-hacked-twice.html

01/03/2021

- Tether se enfrenta a un rescate de 500 Bitcoin: “No vamos a pagar”.
  https://www.zdnet.com/article/tether-faces-500-bitcoin-ransom-we-are-not-paying/
- Hackers chinos atacaron la red eléctrica de la India en medio de tensiones geopolíticas.
  https://thehackernews.com/2021/03/chinese-hackers-targeted-indias-power.html
- Hackers rusos sabotean las infraestructuras críticas de Estados Unidos.
  https://www.ehackingnews.com/2021/03/russian-hackers-sabotaging-critical-us.html
- Algunos de los ataques ransomware recientes: empresas de transporte, fabricante de barcos, redes sociales y empresas multinacionales de la alimentación-
  https://www.bleepingcomputer.com/news/security/nsw-transport-agency-extorted-by-ransomware-gang-after-accellion-attack/
  https://www.bleepingcomputer.com/news/security/worlds-leading-dairy-group-lactalis-hit-by-cyberattack/
  https://www.securityweek.com/boat-building-giant-beneteau-says-cyberattack-disrupted-production
  https://www.cnet.com/news/social-network-gab-hacked-hit-with-500000-ransom-demand/

https://www.securityweek.com/asian-food-distribution-giant-jfc-international-hit-ransomware

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

- Amazon rechaza las afirmaciones de que las "aptitudes" de Alexa pueden eludir el proceso de control de seguridad.
https://threatpost.com/amazon-dismisses-claims-alexa-skills-can-bypass-security-vetting/164316/
- Correo que simula ser una actualización de la versión de Outlook.
https://isc.sans.edu/forums/diary/Pretending+to+be+an+Outlook+Version+Update/27144/
- Desarrolladores vs. Seguridad: ¿Quién es responsable de la seguridad de las aplicaciones?
https://securityintelligence.com/articles/application-security-developers-who-is-responsible/
- Evolución del malware en los teléfonos móviles durante el 2020.
https://securelist.com/mobile-malware-evolution-2020/101029/

NOTAS DE INTERÉS

- La NSA y Microsoft promueven el enfoque “Zero Trust” en ciberseguridad.
https://www.bleepingcomputer.com/news/security/nsa-microsoft-promote-a-zero-trust-approach-to-cybersecurity/
- El malware escrito en Go es ahora común y ha sido adoptado tanto por APTs como por grupos de delincuencia electrónica.
https://www.zdnet.com/article/go-malware-is-now-common-having-been-adopted-by-both-apts-and-e-crime-groups/
- Microsoft comparte una herramienta para buscar riesgos de filtraciones en el software SolarWinds.
https://www.cyberscoop.com/microsoft-solarwinds-breach-compromise-open-source-codeql/
- La NSA publica documento orientativo sobre la adopción de la seguridad de "confianza cero".
https://www.securityweek.com/nsa-publishes-guidance-adoption-zero-trust-security
https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF
- Cómo buscan trabajo los delincuentes en la Dark Web.
https://www.darkreading.com/theedge/how-criminals-job-hunt-on-the-dark-web---/b/d-id/1340265
- X-Force ha identificado una nueva campaña de usurpación utilizada por ciberdelincuentes para atacar el sector financiero y de seguros
https://exchange.xforce.ibmcloud.com/collection/bc3c49c7e92d518a3a85daa9e4cdcbc9

ACTUALIZACIONES DE SEGURIDAD

- Una vulnerabilidad crítica podría ser explotada por atacantes remotos a los PLC de Rockwell Automation.
https://securityaffairs.co/wordpress/115085/ics-scada/rockwell-automation-software-flaw.html
- Microsoft corrige el error de corrupción de unidades bajo Windows 10.
https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-windows-10-drive-corruption-bug-what-you-need-to-know/
- Cisco publica parches de seguridad para solucionar fallos críticos que afectan a sus productos.
https://thehackernews.com/2021/02/cisco-releases-security-patches-for.html