@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. 104 – 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.

28/05/2021

- Los ciberdelincuentes de SolarWinds se centran en los *think tanks* con la nueva puerta trasera "NativeZone".
  https://thehackernews.com/2021/05/solarwinds-hackers-target-think-tanks.html
- La policía británica encuentra una mina de bitcoin que utiliza electricidad robada en West Midlands.
  https://www.theguardian.com/technology/2021/may/28/police-find-bitcoin-mine-using-stolen-electricity-west-midlands?CMP=fb_a-technology_b-gdntech
- Los ciberespías chinos atacan a las organizaciones de EE.UU. y la UE con nuevos programas maliciosos.
  https://www.bleepingcomputer.com/news/security/chinese-cyberspies-are-targeting-us-eu-orgs-with-new-malware/
- México bloquea los sitios de la lotería nacional tras la amenaza de DDoS por *ransomware*.
  https://www.bleepingcomputer.com/news/security/mexico-walls-off-national-lottery-sites-after-ransomware-ddos-threat/

29/05/2021

- Un ataque “phishing” informa por correo que “su paquete de Walmart no fue entregado”.
  https://www.bleepingcomputer.com/news/security/beware-walmart-phishing-attack-says-your-package-was-not-delivered/

30/05/2021

- Interpol intercepta 83 millones de dólares en la lucha contra la ciberdelincuencia financiera.
  https://securityaffairs.co/wordpress/118414/cyber-crime/interpol-financial-cyber-crimes.html
- APT: Un grupo con base en China ataca las VPNs de Pulse Secure.
  https://www.ehackingnews.com/2021/05/apt-china-based-threat-group-attacks.html
- Kaspersky ha detectado un nuevo método de ciberataque a los datos de las empresas.
  https://www.ehackingnews.com/2021/05/kaspersky-detected-new-method-of-cyber.html

31/05/2021

- El gigante del sector alimenticio JBS Foods cierra la producción tras un ciberataque.
  https://www.bleepingcomputer.com/news/security/food-giant-jbs-foods-shuts-down-production-after-cyberattack/
  https://www.zdnet.com/article/jbs-usa-cyber-attack-affecting-north-american-and-australian-systems/
- La Agencia Sueca de Salud cierra SmiNet tras los intentos de hackeo.
  https://securityaffairs.co/wordpress/118440/hacking/swedish-health-agency-cyberattacks.html

- Los autores divulgan a los medios de comunicación los datos de los pacientes que robaron en los hospitales de Nueva Zelanda.
https://www.ehackingnews.com/2021/05/threat-actors-release-patient-data.html

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

- **Cuál es la app de mensajería que mejor cuida nuestra privacidad: ¿Whatsapp, Telegram o Signal?**
https://cybersonthestorm.com/eludiendo-al-hermano-mayor/
- La lentitud de los desencriptadores de las bandas de ransomware hace que las víctimas busquen alternativas
https://www.bleepingcomputer.com/news/security/ransomware-gangs-slow-decryptors-prompt-victims-to-seek-alternatives/
- Los ciberdelincuentes de SolarWinds han vuelto con una nueva campaña masiva, asegura Microsoft.
https://arstechnica.com/gadgets/2021/05/microsoft-says-solarwinds-hackers-targeted-us-agencies-in-a-new-campaign/
https://www.securityweek.com/cisa-fbi-alert-350-organizations-targeted-attack-abusing-email-marketing-service
- Los investigadores demuestran dos nuevos trucos para modificar documentos PDF certificados.
https://thehackernews.com/2021/05/researchers-demonstrate-2-new-hacks-to.html
- El nuevo *ransomware* Epsilon Red captura servidores Microsoft Exchange sin parchear.
https://www.securityweek.com/cybercriminals-target-companies-new-epsilon-red-ransomware

NOTAS DE INTERÉS

- La Unión Europea abandona WhatsApp y se pasa a Signal para tener más seguridad.
https://www.elespanol.com/omicrono/software/20210526/union-europea-abandona-whatsapp-signal-tener-seguridad/584192025_0.html
- Los investigadores encuentran cuatro nuevas herramientas de malware creadas para atacar los dispositivos VPN de Pulse Secure.
https://www.zdnet.com/article/researchers-find-four-new-malware-tools-created-to-exploit-pulse-secure-vpn-appliances/
https://thehackernews.com/2021/05/chinese-cyber-espionage-hackers.html
- Los hackers se aprovechan de la vuelta a las oficinas después del COVID.
https://threatpost.com/hackers-exploit-covid-office/166550/
- Los dispositivos de Amazon pronto compartirán automáticamente su Internet con los vecinos.
https://arstechnica.com/gadgets/2021/05/amazon-devices-will-soon-automatically-share-your-internet-with-neighbors/
- Un nuevo defecto en los PLC de Siemens podría permitir a los hackers ejecutar código malicioso de forma remota.
https://thehackernews.com/2021/05/a-new-bug-in-siemens-plcs-could-let.html

ACTUALIZACIONES DE SEGURIDAD

- SonicWall insta a los clientes a *parchear* "inmediatamente" el fallo de NSM On-Prem.
https://www.bleepingcomputer.com/news/security/sonicwall-urges-customers-to-immediately-patch-nsm-on-prem-bug/