@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. 96/2021

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.

30/04/2021

- SAP admite "miles" de exportaciones ilegales de software a Irán.
  https://www.zdnet.com/article/sap-admits-to-thousands-of-illegal-software-exports-to-iran/
- **Microsoft alerta sobre un defecto denominado "BadAlloc" que afecta a una amplia gama de dispositivos IoT y OT.**
  https://thehackernews.com/2021/04/microsoft-finds-badalloc-flaws.html
  https://threatpost.com/microsoft-warns-25-critical-iot-industrial-devices/165752/
- La bolsa de criptomonedas Hotbit cerró después de que los hackers atacaran los portafolios.
  https://www.bleepingcomputer.com/news/security/hotbit-cryptocurrency-exchange-down-after-hackers-targeted-wallets/
- Los hackers aprovechan el fallo de día cero de SonicWall en los ataques del ransomware FiveHands.
  https://thehackernews.com/2021/04/hackers-exploit-sonicwall-zero-day-bug.html
- Presuntos hackers estatales chinos atacan a diseñador de submarinos rusos.
  https://www.bleepingcomputer.com/news/security/suspected-chinese-state-hackers-target-russian-submarine-designer/
  https://thehackernews.com/2021/05/new-chinese-malware-targeted-russias.html

01/05/2021

- China denuncia a 33 apps por recopilar más datos de los usuarios de lo que se considera imprescindible.
  https://www.zdnet.com/article/china-calls-out-33-apps-for-collecting-more-user-data-than-necessary/
- La Banca di Credito Cooperativo sufre un importante ciberataque.
  https://www.ehackingnews.com/2021/05/banca-di-credito-cooperativo-bank.html
- Kaspersky descubrió que Purple Lambert forma parte de la CIA.
  https://www.ehackingnews.com/2021/05/kaspersky-discovered-purple-lambert-to.html

02/05/2021

- El proveedor de hosting en la nube, Swiss Cloud, sufrió un ataque de ransomware.
  https://securityaffairs.co/wordpress/117433/cyber-crime/swiss-cloud-ransomware-attack.html

03/05/2021

- Investigadores descubren una operación de ransomware patrocinada por el Estado iraní.
  https://thehackernews.com/2021/05/researchers-uncover-iranian-state.html
- Se ha detectado una variante del malware Buer basada en Rust.
  https://thehackernews.com/2021/05/a-new-buer-malware-variant-has-been.html

- Los estafadores de Magecart atacan los sistemas de entrega en línea de los restaurantes.
https://www.cyberscoop.com/magecart-hack-delivery-pandemic/

- Ola de ciberataques en Israel del ransomware N3TW0RM.
https://www.bleepingcomputer.com/news/security/n3tw0rm-ransomware-emerges-in-wave-of-cyberattacks-in-israel/

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

- La comunidad PHP elude su tercer ataque a la cadena de suministro en tres años.
https://nakedsecurity.sophos.com/2021/04/30/php-community-sidesteps-its-third-supply-chain-attack-in-three-years/

- Python también se ve perjudicado por una vulnerabilidad crítica de validación de direcciones IP.
https://www.bleepingcomputer.com/news/security/python-also-impacted-by-critical-ip-address-validation-vulnerability/

- Hackear un modelo Teslal X con un dron DJI Mavic 2 equipado con un dispositivo WIFI.
https://securityaffairs.co/wordpress/117441/hacking/tesla-model-x-hacking.html

- La NSA publica orientaciones sobre la seguridad de la conectividad TI-OT.
https://www.securityweek.com/nsa-issues-guidance-securing-it-ot-connectivity
https://media.defense.gov/2021/Apr/29/2002630479/-1/-1/1/CSA_STOP-MCA-AGAINST-OT_UOO13672321.PDF

NOTAS DE INTERÉS

- El número de teléfono móvil del primer ministro británico ha estados accesible públicamente en Internet desde hace quince años.
https://www.infosecurity-magazine.com/news/british-prime-ministers-cell-phone/

- El malware de espionaje PortDoor está dirigido al sector de la defensa ruso.
https://threatpost.com/portdoor-espionage-malware-takes-aim-at-russian-defense-sector/165770/

- Más agencias estadounidenses posiblemente hackeadas, esta vez con exploits de Pulse Secure.
https://arstechnica.com/gadgets/2021/04/more-us-agencies-potentially-hacked-this-time-with-pulse-secure-exploits/

- Golpe de realidad del ransomware: el 92% de los que pagan no recuperan sus datos.
https://www.forbes.com/sites/daveywinder/2021/05/02/ransomware-reality-shock-92-who-pay-dont-get-their-data-back/

- Se publica un exploit PoC (proof-of-concept) del *bug* de Microsoft Exchange descubierto por la NSA.
https://www.bleepingcomputer.com/news/security/poc-exploit-released-for-microsoft-exchange-bug-dicovered-by-nsa/

ACTUALIZACIONES DE SEGURIDAD

- El servidor de DNS BIND de ISC con tres vulnerabilidades corregidas.
https://exchange.xforce.ibmcloud.com/collection/171428fe292b2364ea998578e8bfeff9
https://kb.isc.org/docs/cve-2021-25214
https://kb.isc.org/docs/cve-2021-25215
https://kb.isc.org/docs/cve-2021-25216

- Samba ha publicado un aviso de seguridad que soluciona una vulnerabilidad.
https://www.samba.org/samba/security/CVE-2021-20254.html