@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. 82/2021

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.

09/03/2021

- Aplicaciones maliciosas disponibles en Google Play dejaron entrar troyanos bancarios en los dispositivos de los usuarios
  https://www.zdnet.com/article/malicious-apps-on-google-play-dropped-banking-trojans-on-user-devices/
  https://thehackernews.com/2021/03/9-android-apps-on-google-play-caught.html
- Los piratas informáticos que atacan Microsoft Exchange, también han vulnerado a la autoridad bancaria europea.
  https://thehackernews.com/2021/03/microsoft-exchange-hackers-also.html
- El malware de criptomonedas UnityMiner piratea los dispositivos de almacenamiento de QNAP.
  https://www.zdnet.com/article/unityminer-cryptocurrency-malware-hijacks-qnap-storage-devices/
- GitHub corrige un error que hace que los usuarios se registren en otras cuentas.
  https://www.bleepingcomputer.com/news/security/github-fixes-bug-causing-users-to-log-into-other-accounts/

10/03/2021

- Los delincuentes del FIN8 vuelven con una versión más potente del malware BADHATCH para PoS (*Punto de venta, por sus siglas en inglés*).
  https://thehackernews.com/2021/03/fin8-hackers-return-with-more-powerful.html
- El ransomware Ryuk afecta a 700 oficinas de agencias laborales (SEPE) del gobierno español.
  https://www.bleepingcomputer.com/news/security/ryuk-ransomware-hits-700-spanish-government-labor-agency-offices/
- Piratas informáticos acceden a miles de cámaras de seguridad de empresas, cárceles y hospitales.
  https://arstechnica.com/information-technology/2021/03/hackers-access-security-cameras-inside-cloudflare-jails-and-hospitals/
  https://www.zdnet.com/article/verkada-disables-accounts-after-reports-its-security-cameras-were-breached/
- **Microsoft publica actualizaciones para Windows 10 y ya hay problemas.**
  https://betanews.com/2021/03/10/microsoft-releases-kb5000802-and-kb5000808-updates-for-windows-10/
- Investigadores revelan un nuevo malware para Linux vinculado a piratas informáticos chinos.
  https://thehackernews.com/2021/03/researchers-unveil-new-linux-malware.html

11/03/2021

- GitHub informó a sus clientes de un fallo de seguridad "potencialmente grave".
  https://www.ehackingnews.com/2021/03/github-informed-clients-of-potentially.html

- El Parlamento de Noruega fue afectado por el malware de Microsoft Exchange.
https://www.theregister.com/2021/03/11/stortinget_attack/
- El RAT NanoCore sortea las defensas del correo electrónico con la táctica .ZIPX
https://threatpost.com/nanocore-rat-email-defenses-zipx/164701/
- El desarrollador de 7-Zip publica la primera versión oficial para Linux.
https://www.bleepingcomputer.com/news/software/7-zip-developer-releases-the-first-official-linux-version/

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

- Últimos avisos sobre sistemas industriales del ICS-CERT de EE.UU..
https://us-cert.cisa.gov/ics/advisories
- RedXOR, un nuevo y potente backdoor de Linux en el arsenal de Winnti APT.
https://securityaffairs.co/wordpress/115491/apt/redxor-backdoor-winnti-apt.html

NOTAS DE INTERÉS

- El backdoor SUPERNOVA que surgió tras el hackeo de SolarWinds, está probablemente vinculado a autores chinos.
https://securityaffairs.co/wordpress/115415/malware/supernova-chinese-hackers.html
- DARPA acelera el proyecto de encriptación FHE (Full Homomorphic Encryption) con Intel.
https://www.infosecurity-magazine.com/news/darpa-rampsup-fhe-encryption/
- Las vulnerabilidades del MS Exchange Server existentes se aprovechan de manera masiva.
https://www.kaspersky.com/blog/exchange-vulnerabilities/38964/
https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/
https://www.cyberscoop.com/microsoft-exchange-china-exploitation-eset/
https://www.zdnet.com/article/microsoft-exchange-server-cybersecurity-warning-apply-patches-now-because-more-hacking-groups-are-trying-to-exploit-the-vulnerabilities/
- La Fundación Linux y sus socios han creado un nuevo software para firmas criptográficas gratuitas con el fin de mejorar la seguridad de los programas de código abierto.
https://www.zdnet.com/article/linux-foundation-announces-new-open-source-software-signing-service/
- El Reino Unido introducirá nuevas leyes y un código de prácticas para la policía que quiera rastrear los mensajes de los teléfonos móviles.
https://www.theregister.com/2021/03/11/mobile_phone_extraction_law_proposals/

ACTUALIZACIONES DE SEGURIDAD

- Apple publica un parche para el defecto que permite el hackeo remoto y que afecta a miles de millones de sus dispositivos.
https://thehackernews.com/2021/03/apple-issues-patch-for-remote-hacking.html
- Martes de actualizaciones de Microsoft - Marzo 2021 y notas relacionadas.
https://msrc.microsoft.com/update-guide/releaseNote/2021-Mar
https://exchange.xforce.ibmcloud.com/collection/c82f6a928a7278759e5eec21b3ecc742
- F5 publica parches para casi dos docenas de vulnerabilidades, algunas críticas.
https://www.cyberscoop.com/f5-critical-vulnerabilities-rce-patches/
- SAP elimina un fallo crítico de RCE en su software de producción.
https://threatpost.com/sap-critical-rce-flaw-manufacturing/164666/