@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. 102 – 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.

21/05/2021

- "Socios" de DarkSide reclaman el depósito de bitcoins de la banda en un foro de hacker. https://www.bleepingcomputer.com/news/security/darkside-affiliates-claim-gangs-bitcoin-deposit-on-hacker-forum/
- Microsoft advierte de un malware que roba datos y se hace pasar por un ransomware. https://thehackernews.com/2021/05/microsoft-warns-of-data-stealing.html
- Una campaña de correo electrónico difunde el falso ransomware StrRAT. https://threatpost.com/email-campaign-fake-ransomware-rat/166378/
- La filtración de datos de Air India afecta a 4,5 millones de pasajeros. https://thehackernews.com/2021/05/indias-flag-carrier-airline-air-india.html

22/05/2021

- Piratas informáticos extranjeros han vulnerado las agencias federales rusas, según la NKTsKI. https://securityaffairs.co/wordpress/118169/intelligence/fsb-says-russian-agencies-hacked.html
- El FBI informa que el ransomware Conti ha afectado a 16 servicios de salud y emergencias de Estados Unidos. https://thehackernews.com/2021/05/fbi-warns-conti-ransomware-hit-16-us.html
- La plataforma japonesa de comercio electrónico Mercari sufre una gran filtración de datos. https://www.ehackingnews.com/2021/05/japanese-e-commerce-platform-mercari.html

23/05/2021

- Un ataque de malware afectó al Departamento de Salud de Alaska. https://securityaffairs.co/wordpress/118184/cyber-crime/alaska-health-department-malware.html

24/05/2021

- El gobierno indonesio bloquea el acceso al foro de hacking RaidForums tras filtración de datos. https://www.bleepingcomputer.com/news/security/indonesian-govt-blocks-access-to-raidforums-hacking-forum-after-data-leak/
- Investigadores vinculan a Corea del Norte con los ataques de CryptoCore a las bolsas de criptomonedas. https://thehackernews.com/2021/05/researchers-link-cryptocore-attacks-on.html

25/05/2021

- **Los piratas informáticos iraníes Agrius han atacado a Israel a partir de diciembre de 2020.** https://www.zdnet.com/article/iranian-hacking-group-agrius-pretends-to-encrypt-files-for-a-ransom-destroys-it-instead/
https://threatpost.com/agrius-wiper-attacks-israeli-targets/166474/

- Bose admite un ataque de ransomware: se ha accedido a los datos de los empleados.
https://www.cyberscoop.com/bose-ransomware-hack-letter/

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

- Las debilidades de miles de millones de dispositivos Wi-Fi permiten a los piratas informáticos eludir los firewalls.
https://arstechnica.com/gadgets/2021/05/farewell-to-firewalls-wi-fi-bugs-open-network-devices-to-remote-hacks/

- El malware bancario Bizarro se ha centrado en 70 bancos de Europa y Sudamérica.
https://www.bleepingcomputer.com/news/security/bizarro-banking-malware-targets-70-banks-in-europe-and-south-america/

- Se revelan detalles sobre los fallos críticos que afectan al software de monitoreo Nagios IT.
https://thehackernews.com/2021/05/details-disclosed-on-critical-flaws.html
https://securityaffairs.co/wordpress/118207/hacking/nagios-it-monitoring-flaws.html

NOTAS DE INTERÉS

- Principales retos de seguridad en las aplicaciones: los malos bots, las APIs rotas y los ataques a la cadena de suministro.
https://www.helpnetsecurity.com/2021/05/21/top-application-security-challenges/

- El gigante estadounidense de los seguros CNA Financial pagó un rescate de 40 millones de dólares para recuperar el control de sus sistemas: informe.
https://www.zdnet.com/article/us-insurance-giant-cna-financial-paid-40-million-ransom-to-wrestle-back-control-of-systems/

- Los intentos de robo de credenciales a nivel mundial alcanzaron los 193.000 millones en 2020.
https://www.infosecurity-magazine.com/news/global-credential-stuffing-193/

- Microsoft: nueva herramienta de código abierto ayuda a probar defensas contra los ataques de los ciberdelincuentes.
https://www.zdnet.com/article/microsoft-this-new-open-source-tool-helps-you-test-your-defences-again-hacker-attacks/

- La vulnerabilidad HTTP de Windows también afecta a los servidores WinRM.
https://www.bleepingcomputer.com/news/security/wormable-windows-http-vulnerability-also-affects-winrm-servers/

- Ha sido detectado un *malware* que utiliza un día cero de macOS para hacer capturas de pantalla
https://techcrunch.com/2021/05/24/malware-xcsset-macos/

- Nuevos errores de Bluetooth permiten a los atacantes hacerse pasar por dispositivos legítimos.
https://thehackernews.com/2021/05/new-bluetooth-flaws-let-attackers.html

ACTUALIZACIONES DE SEGURIDAD

- Microsoft difunde la primera compilación de Windows 10 *Build* 21387, **sin Internet Explorer**.
https://betanews.com/2021/05/21/windows-10-build-21387-kills-internet-explorer/

- Apple corrige tres días cero, uno de ellos explotado por el malware XCSSET para macOS.
https://www.bleepingcomputer.com/news/security/apple-fixes-three-zero-days-one-abused-by-xcsset-macos-malware/

- **VMware ha emitido un aviso de seguridad crítico.**
https://www.vmware.com/security/advisories/VMSA-2021-0010.html