@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. 70/2021

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.

19/01/2021

- El FBI investiga la pista de la mujer que robó la portátil de Pelosi para venderla a Rusia.
https://www.forbes.com/sites/roberthart/2021/01/18/fbi-investigating-tip-off-that-woman-stole-pelosis-laptop-to-sell-to-russia/

- Los foros IObit fueron hackeados para difundir ransomware entre sus miembros.
https://www.bleepingcomputer.com/news/security/iobit-forums-hacked-to-spread-ransomware-to-its-members/

- El wiki OpenWRT informa de una violación de datos después de que un hacker accediera a la cuenta de administrador.
https://www.helpnetsecurity.com/2021/01/19/openwrt-data-breach/

- La nueva *botnet* FreakOut tiene como objetivo los sistemas Linux que ejecutan soft sin parches.
https://betanews.com/2021/01/19/freakout-malware-targets-linux/

20/01/2021

- Trump decreta que los proveedores en la nube americanos deben mantener registros de los clientes extranjeros.
https://www.zdnet.com/article/trump-decrees-american-cloud-providers-need-to-maintain-records-on-foreign-clients/

- Hacker publica 1,4 millones de registros de usuarios de Pixlr gratis en un foro.
https://www.bleepingcomputer.com/news/security/hacker-posts-14-million-pixlr-user-records-for-free-on-forum/

- Se filtró una BD robada que contiene las direcciones de correo electrónico, nombres y contraseñas de más de 77 millones de registros de usuarios del servicio Nitro PDF.
https://www.bleepingcomputer.com/news/security/hacker-leaks-full-database-of-77-million-nitro-pdf-user-records/

- La empresa de seguridad Malwarebytes fue infectada por los mismos hackers de SolarWinds.
https://www.engadget.com/solarwinds-hackers-targeted-malwarebytes-110537912.html

21/01/2021

- Se detectó un exploit automatizado para una vulnerabilidad crítica de SAP SolMan.
https://www.zdnet.com/article/automated-exploit-of-critical-sap-solman-vulnerability-detected-in-the-wild/

- El malware de criptominería MrbMiner está vinculado a una empresa de software iraní.
https://thehackernews.com/2021/01/mrbminer-crypto-mining-malware-links-to.html

- Microsoft está implementando un monitor de contraseñas y otras características nuevas.

https://www.bleepingcomputer.com/news/security/windows-remote-desktop-servers-now-used-to-amplify-ddos-attacks/

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

- Fue descubierta una cuarta cepa del malware en el incidente de SolarWinds.
https://www.zdnet.com/article/fourth-malware-strain-discovered-in-solarwinds-incident/
https://thehackernews.com/2021/01/researchers-discover-raindrop-4th.html

- Repensar la seguridad de la IoT: No se trata solo de los dispositivos.
https://www.darkreading.com/iot/rethinking-iot-security-its-not-about-the-devices/a/d-id/1339867

NOTAS DE INTERÉS

- El Plan Nacional de Ciberseguridad de los EE.UU. promete salvaguardar el sector marítimo.
https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/us-national-cybersecurity-plan-safeguard-maritime-sector/

- Microsoft Defender está incrementando su respuesta a los ataques de malware al cambiar una configuración de teclas.
https://www.zdnet.com/article/microsoft-defender-is-boosting-its-response-to-malware-attacks-by-changing-a-key-setting/

- **Brave se convierte en el primer navegador en añadir soporte nativo para el protocolo IPFS.**
https://www.zdnet.com/article/brave-becomes-first-browser-to-add-native-support-for-the-ipfs-protocol/

- Errores en Signal, Facebook y aplicaciones de chat de Google permiten a los atacantes espiar a los usuarios (algunas ya han sido corregidas en actualizaciones).
https://thehackernews.com/2021/01/google-discloses-flaws-in-signal-fb.html

ACTUALIZACIONES DE SEGURIDAD

- Se pide a los administradores de red que apliquen las últimas actualizaciones de Dnsmasq para prevenir los nuevos ataques DNSpooq.
https://thehackernews.com/2021/01/a-set-of-severe-flaws-affect-popular.html
https://us-cert.cisa.gov/ics/advisories/icsa-21-019-01

- Google ha publicado Chrome 88 el 19 de enero de 2021.
https://www.bleepingcomputer.com/news/google/google-chrome-88-released-rip-flash-player-and-ftp-support/

- FireEye publica una herramienta de auditoría de redes basada en técnicas utilizadas por los hackers de SolarWinds.
https://www.zdnet.com/article/fireeye-releases-tool-for-auditing-networks-for-techniques-used-by-solarwinds-hackers/

- Cisco corrige fallos críticos en SD-WAN, gestor de licencias en la nube.
https://www.bleepingcomputer.com/news/security/cisco-fixes-critical-pre-auth-bugs-in-sd-wan-cloud-license-manager/

- VLC Media Player 3.0.12 soluciona múltiples errores de ejecución remota de código.
https://www.bleepingcomputer.com/news/security/cisco-fixes-critical-pre-auth-bugs-in-sd-wan-cloud-license-manager/