@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. 73/2021

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.

29/01/2021

- Ayer por la tarde se informó de un grave error utilizado contra Libgcrypt 1.9.0.
  https://lists.gnupg.org/pipermail/gnupg-announce/2021q1/000455.html
  https://www.theregister.com/2021/01/29/severe_libgcrypt_bug/
- Una red de bots de Twitter ha atacado al gobierno belga por prohibir el 5G de Huawei.
  https://www.zdnet.com/article/a-network-of-twitter-bots-has-attacked-the-belgian-governments-huawei-5g-ban/
- La filtración en UScellular permitió a cibercriminales acceder a nros. de teléfono de los clientes.
  https://www.securityweek.com/uscellular-breach-allowed-hackers-port-customer-phone-numbers
- Un defecto del plugin Pop-Up Builder de WordPress afecta a 200.000 sitios web.
  https://threatpost.com/wordpress-pop-up-builder-plugin-flaw-plagues-200k-sites/163500/
- Los piratas ransomware Fonix se retiran y hacen pública la clave maestra de descifrado.
  https://www.zdnet.com/article/fonixcrypter-ransomware-gang-releases-master-decryption-key/

30/01/2021

- El UK Research and Innovation (UKRI) sufre un ataque ransomware.
  https://securityaffairs.co/wordpress/114026/hacking/ukri-ransomware-attack.html

31/01/2021

- Perl.com, el sitio oficial del lenguaje de programación Perl fue pirateado.
  https://www.ehackingnews.com/2021/01/perlcom-official-site-for-perl.html
- El servicio antispam SpamCop de Cisco sufre una interrupción al expirar su dominio.
  https://www.bleepingcomputer.com/news/security/spamcop-anti-spam-service-suffers-an-outage-after-its-domain-expired/
- El malware 'Android Worm' se propaga a través de la lista de contactos de WhatsApp.
  https://www.ehackingnews.com/2021/01/android-worm-malware-is-spreading-via.html

01/02/2021

- La empresa de seguridad NCC Group dice que detectó una utilización "indiscriminada" de un misterioso “día cero” de SonicWall.
  https://www.zdnet.com/article/sonicwall-zero-day-exploited-in-the-wild/
- Un grupo de ciberdelincuentes insertó un malware en el emulador NoxPlayer de Android.
  https://thehackernews.com/2021/02/a-new-software-supplychain-attack.html
- La empresa multinacional de servicios informáticos Serco se ve afectada por un ransomware.
  https://www.infosecurity-magazine.com/news/global-government-outsourcer-serco/

- Una intrusión de datos deja al descubierto 1,6 millones de solicitudes de desempleo en Washington.
https://www.bleepingcomputer.com/news/security/data-breach-exposes-16-million-washington-unemployment-claims/

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

- Vovalex es probablemente el primer ransomware escrito en D.
https://www.bleepingcomputer.com/news/security/vovalex-is-likely-the-first-ransomware-written-in-d/
- Apple iOS 14 frustra los ataques de iMessage con el sistema BlastDoor.
https://threatpost.com/apple-ios-imessage-blastdoor/163479/
- Nuevo malware de criptojacking centrado en los servidores Apache, Oracle y Redis.
https://thehackernews.com/2021/02/new-cryptojacking-malware-targeting.html
- Operación NightScout: El ataque se dirige a la cadena de suministro de juegos en línea en Asia.
https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/

NOTAS DE INTERÉS

- El grupo de piratas informáticos de Hezbollah tiene como objetivo las telecomunicaciones, el almacenamiento y los proveedores de servicios de Internet de todo el mundo.
https://thehackernews.com/2021/01/hezbollah-hacker-group-targeted.html
- El ataque a SolarWinds no es un caso aislado, sino un momento de reflexión para la industria de la seguridad, dice el ejecutivo de Microsoft.
https://www.zdnet.com/article/solarwinds-attack-is-not-an-outlier-but-a-moment-of-reckoning-for-security-industry-says-microsoft-exec/
- Google implementa *mitigaciones* en Chrome contra el nuevo ataque NAT *Slipstreaming*.
https://www.zdnet.com/article/google-deploys-new-chrome-mitigations-against-new-nat-slipstreaming-attack/
- Incluyen a hackers en los juegos de guerra de la OTAN.
https://www.schneier.com/blog/archives/2021/01/including-hackers-in-nato-wargames.html
- Expertos explican cómo burlar la reciente mejora del Gran Firewall de China.
https://securityaffairs.co/wordpress/114053/digital-id/chinas-great-firewall-bypass.html

ACTUALIZACIONES DE SEGURIDAD

- La vulnerabilidad de día cero de Windows Installer recibe un “microparche” gratuito.
https://www.bleepingcomputer.com/news/security/windows-installer-zero-day-vulnerability-gets-free-micropatch/
- Se ha publicado la versión 3.4.3 de Wireshark (analizador de protocolos).
https://isc.sans.edu/forums/diary/Wireshark+343+Released/27048/
- Los desarrolladores de Libgcrypt publican una actualización urgente para hacer frente a una grave vulnerabilidad.
https://www.zdnet.com/article/libgcrypt-developers-release-urgent-update-to-tackle-severe-vulnerability/