@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. 93/2021

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.

20/04/2021

- Cientos de redes habrían sido *hackeadas* en el ataque a la cadena de suministro de Codecov. https://www.bleepingcomputer.com/news/security/hundreds-of-networks-reportedly-hacked-in-codecov-supply-chain-attack/
- Más de 120 servidores de anuncios infectados se centran en millones de usuarios de Internet. https://thehackernews.com/2021/04/120-compromised-ad-servers-target.html
- El gobierno de Biden presenta un plan para defender el sector eléctrico de los ciberataques. https://www.cyberscoop.com/biden-administration-energy-department-defense-cyberattacks/
- Un atacante afirma haber hackeado Domino's. https://www.infosecurity-magazine.com/news/threat-actor-claims-to-have-hacked/

21/04/2021

- Facebook tiene una nueva megafiltración en sus manos. https://arstechnica.com/gadgets/2021/04/tool-links-email-addresses-to-facebook-accounts-at-scale/
- Una novedosa campaña con RATs basada en correo electrónico, tiene como objetivo a los clientes de Bloomberg. https://threatpost.com/email-campaign-targets-bloomberg-clients/165514/
- Filtración de datos en el mayor proveedor de energía de Nueva Inglaterra, EE.UU. https://www.infosecurity-magazine.com/news/eversource-data-breach/
- Linux rechaza a la Universidad de Minnesota por enviar parches con errores. https://www.neowin.net/news/linux-bans-university-of-minnesota-for-sending-buggy-patches-in-the-name-of-research/

22/04/2021

- Facebook descubre que funcionarios del gobierno palestino han sido atacados con malware. https://www.zdnet.com/article/facebook-uncovers-palestinian-government-officials-targeted-with-malware/
- Ciberdelincuentes utilizan Telegram para controlar el malware ToxicEye. https://thehackernews.com/2021/04/cybercriminals-using-telegram-messenger.html
- **Una banda ransomware intenta extorsionar a Apple y amenaza con vender planos robados.** https://thehackernews.com/2021/04/hackers-threaten-to-leak-stolen-apple.html https://www.theguardian.com/technology/2021/apr/22/ransomware-hackers-steal-plans-upcoming-apple-products

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

- Los piratas informáticos norcoreanos adaptan el skimming de la web para robar Bitcoin.

https://www.bleepingcomputer.com/news/security/north-korean-hackers-adapt-web-skimming-for-stealing-bitcoin/

- Hackeando una máquina de rayos X con WHIDelite y EvilCrowRF.
https://securityaffairs.co/wordpress/117053/hacking/hacking-x-ray-machine.html
- La APT Iron Tiger actualiza su kit de herramientas con el malware mejorado SysUpdate.
https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html
- Pink, malware de WhatsApp, responde automáticamente los mensajes de Signal y Telegram.
https://www.bleepingcomputer.com/news/security/whatsapp-pink-malware-can-now-auto-reply-to-your-signal-telegram-texts/

NOTAS DE INTERÉS

- El día cero de Pulse Secure VPN fue utilizado para hackear empresas de defensa y organizaciones gubernamentales. CISA solicita su mitigación a organismos del estado.
https://www.bleepingcomputer.com/news/security/pulse-secure-vpn-zero-day-used-to-hack-defense-firms-govt-orgs/
https://www.cisa.gov/pulse-connect-secure-mitigations
- Los códigos QR ofrecen vías fáciles de ciberataque a medida que aumenta su uso.
https://threatpost.com/qr-codes-cyberattack-usage-spikes/165526/
- **Cómo las operaciones cibernéticas aumentan el riesgo de una guerra nuclear accidental**.
https://www.defenseone.com/ideas/2021/04/how-cyber-ops-increase-risk-accidental-nuclear-war/173523/
- Signal denuncia a la empresa de seguridad Cellebrite por supuestos agujeros de seguridad.
https://www.bbc.com/news/technology-56846357

ACTUALIZACIONES DE SEGURIDAD

- Microsoft corrige parcialmente una vulnerabilidad de Windows 7 y Server 2008.
https://www.bleepingcomputer.com/news/security/microsoft-partially-fixes-windows-7-server-2008-vulnerability/
- Mozilla corrige el fallo de Firefox que permitía falsificar el “candado” del navegador HTTPS.
https://threatpost.com/mozilla-fixes-firefox-flaw/165501/
https://us-cert.cisa.gov/ncas/current-activity/2021/04/20/mozilla-releases-security-update-firefox-firefox-esr-and
- El fabricante de hardware de seguridad SonicWall insta a sus clientes a parchear un conjunto de tres vulnerabilidades de día cero.
https://www.bleepingcomputer.com/news/security/sonicwall-warns-customers-to-patch-3-zero-days-exploited-in-the-wild/
- Oracle publica la actualización de parches críticos de abril de 2021.
https://us-cert.cisa.gov/ncas/current-activity/2021/04/20/oracle-releases-april-2021-critical-patch-update
- Google publica una actualización de Chrome que parchea siete vulnerabilidades de seguridad.
https://www.zdnet.com/article/google-issues-chrome-update-to-patch-seven-security-vulnerabilities/
- VMware difunde una actualización de seguridad.
https://us-cert.cisa.gov/ncas/current-activity/2021/04/20/vmware-releases-security-update