@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. 113 – 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.

29/06/2021

- **Los datos de 700 millones de usuarios de LinkedIn están a la venta en la "*dark web*".**
  https://threatpost.com/data-700m-linkedin-users-cyber-underground/167362/
  https://www.reddit.com/r/sysadmin/comments/oa7e0l/linkedin_breach_reportedly_exposes_data_of_92_of/
- Hackers rusos tuvieron acceso durante meses al banco central de Dinamarca.
  https://www.bleepingcomputer.com/news/security/russian-hackers-had-months-long-access-to-denmarks-central-bank/
- La Casa Blanca estudia tomar medidas contra los pagos secretos de ransomware y perseguir a los delincuentes informáticos.
  https://www.cyberscoop.com/biden-ransomware-cryptocurrency-neuberger/

30/06/2021

- **CERT Nacional de la República Argentina (CERT.AR) informa que se ha manifestado una variante del ransomware DarkRadiation.**
  https://www.trendmicro.com/en_us/research/21/f/bash-ransomware-darkradiation-targets-red-hat--and-debian-based-linux-distributions.html
  https://github.com/willshiao/node-bash-obfuscate
- La Policía británica advierte de las estafas de WhatsApp a propósito del Día de las Redes Sociales
  https://nakedsecurity.sophos.com/2021/06/30/police-warn-of-whatsapp-scams-in-time-for-social-media-day/
- Grupos de amenaza se centran en empresas de aviación mediante campañas de *spear phishing*.
  https://www.ehackingnews.com/2021/06/threat-actors-target-aviation-firms-via.html
- La policía colombiana detiene al sospechoso del malware Gozi tras 8 años prófugo.
  https://nakedsecurity.sophos.com/2021/06/30/colombian-police-arrest-gozi-malware-suspect-after-8-years-at-large/

01/07/2021

- Un grupo de *hackers* chinos se hace pasar por el presidente afgano para infiltrarse en organismos gubernamentales.
  https://www.zdnet.com/article/chinese-hacking-group-impersonates-afghan-president-to-infiltrate-government-agencies/
  https://threatpost.com/dropbox-malware-ongoing-spearphishing-cyberespionage/167402/
- NSA: Los hackers rusos de la GRU utilizan Kubernetes para realizar ataques de fuerza bruta.
  https://www.bleepingcomputer.com/news/security/nsa-russian-gru-hackers-use-kubernetes-to-run-brute-force-attacks/
- Los datos hackeados de 69.000 usuarios de LimeVPN están a la venta en la Dark Web
  https://threatpost.com/hacked-data-limevpn-dark-web/167492/

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

- El sitio Halo de desarrollo de Microsoft fue pirateado mediante el secuestro de dependencias. https://www.bleepingcomputer.com/news/security/microsofts-halo-dev-site-breached-using-dependency-hijacking/
- Guía de seguridad de la información para nuevos empleados. https://www.kaspersky.com/blog/security-awareness-basic-instruction/40416/
- **La herramienta CSET de CISA que se enfoca en ayudar ante la amenaza del ransomware.** https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat
- Microsoft encuentra nuevas vulnerabilidades en el firmware de NETGEAR que podrían llevar al robo de identidad y a comprometer todo el sistema. https://www.microsoft.com/security/blog/2021/06/30/microsoft-finds-new-netgear-firmware-vulnerabilities-that-could-lead-to-identity-theft-and-full-system-compromise/
- El creador del ransomware Babuk aparece misteriosamente en VirusTotal. https://threatpost.com/babuk-ransomware-builder-virustotal/167481/

NOTAS DE INTERÉS

- La mafia del siglo XXI: las empresas criminales en el corazón del ransomware. https://cybernews.com/security/xxi-century-mafia-criminal-enterprises-at-the-heart-of-ransomware/
- El malware de *día cero* alcanzó un máximo histórico del 74% en el primer trimestre de 2021. https://www.helpnetsecurity.com/2021/06/29/zero-day-malware-q1-2021/
- Google Play Store requiere que los desarrolladores de aplicaciones verifiquen su dirección y usen doble factor de autenticación (2FA). https://thehackernews.com/2021/06/google-now-requires-app-developers-to.html https://www.theverge.com/2021/6/29/22555281/google-play-developer-information-verification-two-factor-authentication-2fa-scams
- Un nuevo ransomware pone de manifiesto la adopción generalizada del lenguaje Golang por parte de los ciberatacantes. https://www.zdnet.com/article/this-new-malware-highlights-widespread-adoption-of-golang-language-by-cyberattackers/
- **El desencriptador del ransomware Lorenz recupera archivos de víctimas de forma gratuita.** https://www.bleepingcomputer.com/news/security/lorenz-ransomware-decryptor-recovers-victims-files-for-free/
- GitHub presenta "Copilot", una herramienta de terminación de código potenciada por la IA. https://thehackernews.com/2021/06/github-launches-copilot-ai-powered-code.html
- Las TI, la sanidad y el sector manufacturero son los que más ataques de phishing sufren. https://www.zdnet.com/article/it-healthcare-and-manufacturing-facing-most-phishing-attacks-report/
- La cifra de población mundial con 5G crece a razón de 1 millón de personas al día. https://www.zdnet.com/article/global-5g-population-growing-at-1m-a-day-ericsson/

ACTUALIZACIONES DE SEGURIDAD

- La actualización de emergencia de Windows 10 KB5004760 soluciona el problema de apertura de PDFs. https://support.microsoft.com/es-es/topic/29-de-junio-de-2021-kb5004760-compilaciones-del-sistema-operativo-19041-1082-19042-1082-y-19043-1082-fuera-de-banda-9508f7a2-0713-432f-b06c-1ae6d802a2f7