@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. 122 – 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.

30/07/2021

- Un nuevo malware de fraude bancario llamado Vultur infecta miles de dispositivos.
  https://arstechnica.com/gadgets/2021/07/new-bank-fraud-malware-called-vultur-infects-thousands-of-devices/
  https://securityaffairs.co/wordpress/120696/malware/android-banking-trojan-vultur.html
- **La semana del ransomware al 30 de julio de 2021. Más de 1.000 millones de euros ahorrados.**
  https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-july-30th-2021-1-billion-saved/

31/07/2021

- **La banda de ransomware BlackMatter resurge de las cenizas con DarkSide y REvil.**
  https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-gang-rises-from-the-ashes-of-darkside-revil/
- Se multiplican por siete el número de anuncios en la Dark Web que brindan acceso a redes corporativas.
  https://www.ehackingnews.com/2021/07/seven-fold-surge-in-dark-web-ads.html

01/08/2021

- Hacker utiliza phishing para acceder a cuentas de PayPal.
  https://www.ehackingnews.com/2021/08/hacker-uses-credential-phishing-to-gain.html
- **Podcast diario de seguridad de redes de SANS (Stormcast) del domingo 1 de agosto de 2021.**
  https://isc.sans.edu/podcastdetail.html?id=7610

02/08/2021

- **Zoom paga una demanda colectiva en Estados Unidos por 86 millones de dólares.**
  https://www.zdnet.com/article/zoom-to-pay-85m-settlement-to-set-aside-privacy-violation-and-zoombombing-allegations/
- **La Agencia Espacial Europea pone en órbita un satélite pirateable.**
  https://www.schneier.com/blog/archives/2021/08/the-european-space-agency-launches-hackable-satellite.html
- Falsas posiciones de buques de guerra, incluido un portaaviones británico.
  https://www.bbc.com/news/technology-58027363
- Grupos ransomware dificultan la vacunación de Covid-19 en Italia.
  https://gizmodo.com/the-situation-is-very-serious-ransomware-hackers-hobbl-1847407195

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

- Descubren varios servidores C2 vinculados al malware WellMess.
  https://thehackernews.com/2021/07/experts-uncover-several-c-servers.html

- **Se han encontrado varias bibliotecas de Python malintencionadas en el repositorio PyPI.**
https://thehackernews.com/2021/07/several-malicious-typosquatted-python.html
https://www.bleepingcomputer.com/news/security/pypi-packages-caught-stealing-credit-card-numbers-discord-tokens/
https://www.theregister.com/2021/08/02/in_brief_security/

- El fallo eBPF de Linux consigue privilegios de root en Ubuntu. Se publica el exploit.
https://www.bleepingcomputer.com/news/security/linux-ebpf-bug-gets-root-privileges-on-ubuntu-exploit-released/

- Con la ayuda de Google, un sitio web hecho pasar por Brave.com introduce malware.
https://arstechnica.com/gadgets/2021/07/with-help-from-google-impersonated-brave-com-website-pushes-malware/

- El malware Solarmarker InfoStealer vuelve a aparecer en la red.
https://thehackernews.com/2021/08/solarmarker-infostealer-malware-once.html

- **Múltiples errores de día cero en un sistema popular de tubos neumáticos para hospitales.**
https://www.darkreading.com/vulnerabilities---threats/multiple-zero-day-flaws-discovered-in-popular-hospital-pneumatic-tube-system/d/d-id/1341584
https://thehackernews.com/2021/08/pwnedpiper-pts-security-flaws-threaten.html

NOTAS DE INTERÉS

- Un nuevo *"wiper"* malware estaba detrás del reciente ciberataque al sistema ferroviario iraní.
https://thehackernews.com/2021/07/a-new-wiper-malware-was-behind-recent.html
https://threatpost.com/novel-meteor-wiper-used-in-attack-that-crippled-iranian-train-system/168262/

- La NSA advierte que las redes públicas son focos de ciberdelincuentes.
https://threatpost.com/nsa-warns-public-networks-are-hacker-hotbeds/168268/

- El NIST pide ayuda para desarrollar un marco que gestione los riesgos de la IA.
https://www.zdnet.com/article/nist-calls-for-help-in-developing-ai-risk-management-framework/

- **Los "*hackers*" de SolarWinds vulneraron 27 fiscalías estatales en EE.UU.**
https://securityaffairs.co/wordpress/120704/cyber-warfare-2/solarwinds-hackers-breached-state-attorneys-offices.html
https://www.securityweek.com/justice-department-says-russians-hacked-federal-prosecutors

- La protección contra bots ya está disponible de forma general en Azure Web Application Firewall.
https://www.bleepingcomputer.com/news/security/bot-protection-now-generally-available-in-azure-web-application-firewall/

- **CISA presenta una plataforma de divulgación de vulnerabilidades federales en Estados Unidos.**
https://www.helpnetsecurity.com/2021/08/02/us-federal-vulnerability-disclosure/

ACTUALIZACIONES DE SEGURIDAD

- Google bloqueará los inicios de sesión en dispositivos Android antiguos a partir de septiembre.
https://www.bleepingcomputer.com/news/google/google-to-block-logins-on-old-android-devices-starting-september/

- **El repositorio de paquetes PyPI de Python repara un fallo crítico en la cadena de suministro.**
https://thehackernews.com/2021/08/pypi-python-package-repository-patches.html