@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. 101 – 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.

18/05/2021

- Los piratas informáticos están mejorando su nivel y atrapando a la sanidad con la guardia baja.
https://www.helpnetsecurity.com/2021/05/18/hackers-attacking-healthcare/
- En el primer trimestre de 2021 se registraron 2.9 millones de ataques DDoS.
https://www.infosecurity-magazine.com/news/q1-2021-sees-millions-ddos-attacks/
- Aplicaciones de Stalkerware repletas de defectos de seguridad.
https://threatpost.com/stalkerware-apps-security-bugs/166274/
https://thehackernews.com/2021/05/experts-reveal-over-150-ways-to-steal.html

19/05/2021

- Los hospitales neozelandeses, infectados por un *ransomware*, cancelan algunas cirugías.
https://www.theregister.com/2021/05/19/new_zealand_hospitals_taken_down/
- Estados Unidos presenta proyectos de ley para proteger las infraestructuras críticas de los ciberataques.
https://www.bleepingcomputer.com/news/security/us-introduces-bills-to-secure-critical-infrastructure-from-cyber-attacks/
- En 2021 más de 290 empresas fueron afectadas por seis grupos de *ransomware*.
https://www.zdnet.com/article/more-than-290-enterprises-hit-by-6-ransomware-groups-in-2021/
- El *ransomware Qlocker* se desactiva tras extorsionar a cientos de usuarios de QNAP.
https://www.bleepingcomputer.com/news/security/qlocker-ransomware-shuts-down-after-extorting-hundreds-of-qnap-users/
- El jefe de software de Apple admite que las Mac tienen una cantidad inaceptable de malware.
https://www.cnbc.com/2021/05/19/apples-head-of-software-says-current-level-of-mac-malware-is-not-acceptable.html

20/05/2021

- Las aplicaciones de Android exponen los datos de millones de usuarios por fallas en la autenticación en la nube.
https://www.zdnet.com/article/cloud-services-used-by-android-apps-exposed-data-of-millions-of-users/
- El ransomware Conti ofrece al Sistema de Salud de Irlanda un desencriptador gratuito, pero sigue comercializando los datos obtenidos.
https://www.bleepingcomputer.com/news/security/conti-ransomware-gives-hse-ireland-free-decryptor-still-selling-data/
- *Spamers* inundan el sitio de Python (PyPI) con enlaces de películas piratas y paquetes falsos.
https://www.bleepingcomputer.com/news/security/spammers-flood-pypi-with-pirated-movie-links-and-bogus-packages/

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

- El ransomware *MountLocker* utiliza la API de Windows para propagarse por las redes.
https://www.bleepingcomputer.com/news/security/mountlocker-ransomware-uses-windows-api-to-worm-through-networks/
- El software antivirus, explicado.
https://www.zdnet.com/article/antivirus-software-explained/
- SANS Institute: Concurso Forense Mayo 2021. Respuestas y análisis
https://isc.sans.edu/forums/diary/May+2021+Forensic+Contest+Answers+and+Analysis/27430/
- Se publica un *exploit* de *PoC* de Windows para un *RCE* anómalo.
https://threatpost.com/windows-exploit-wormable-rce/166289/
- Los ciberdelincuentes de Keksec estrenan la red de *bots Simps* para ataques DDoS, en juegos.
https://threatpost.com/keksec-simps-botnet-gaming-ddos/166306/
- *DarkSide*: Buenas prácticas para evitar que los ataques de *ransomware* afecten a la empresa.
https://us-cert.cisa.gov/ncas/alerts/aa21-131a

NOTAS DE INTERÉS

- Setenta (70) bancos europeos y sudamericanos atacados por el malware bancario *Bizarro*.
https://thehackernews.com/2021/05/70-european-and-south-american-banks.html
- Se han perdido más de 80 millones de dólares en estafas de inversión en criptomonedas desde octubre.
https://www.bleepingcomputer.com/news/cryptocurrency/over-80-million-lost-to-cryptocurrency-investment-scams-since-october/
- Cómo Apple dio al gobierno chino acceso a los datos de iCloud y a las aplicaciones codificadas.
https://thehackernews.com/2021/05/how-apple-gave-chinese-government.html
- Estafadores se hacen pasar por servicios de comida para robar datos de los clientes.
https://threatpost.com/scammers-meal-kit-services-customer-data/166282/
- Ha sido rastreada la *botnet* hasta la computadora de la planta de agua de Florida que fue *hackeada*.
https://www.cyberscoop.com/oldsmar-water-plant-botnet-dragos/
- En 9 meses la banda *ransomware DarkSide* extorsionó por 90 millones de dólares.
https://thehackernews.com/2021/05/darkside-ransomware-gang-extorted-90.html
- Los *hackers* buscan dispositivos vulnerables a los pocos minutos de revelarse la falla.
https://www.bleepingcomputer.com/news/security/hackers-scan-for-vulnerable-devices-minutes-after-bug-disclosure/
- “Recicle su teléfono, pero tal vez, claro, no el número”.
https://krebsonsecurity.com/2021/05/recycle-your-phone-sure-but-maybe-not-your-number/

ACTUALIZACIONES DE SEGURIDAD

- Actualizaciones de seguridad de Android de mayo solucionan “días cero”.
https://www.bleepingcomputer.com/news/security/may-android-security-updates-patch-4-zero-days-exploited-in-the-wild/

Fe de erratas: en el boletín número 100 las fechas correctas son 14/05/2021 y 15/05/2021