@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. 145 – 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.

Noticias de ciberseguridad entre el 08/12/21 y el 14/12/21

- Un malware para Android infectó más de 300.000 dispositivos con troyanos bancarios.
  https://www.techrepublic.com/article/android-malware-infected-more-than-300000-devices-with-banking-trojans/
- El proveedor de electricidad australiano "CS Energy" es víctima de un ransomware.
  https://www.securityweek.com/australian-electricity-provider-cs-energy-hit-ransomware
- Cibercriminales roban datos de investigación de la empresa sueca Volvo Cars.
  https://www.securityweek.com/hackers-steal-research-data-swedens-volvo-cars
- La empresa de logística internacional Hellmann se esfuerza para recuperarse de un ciberataque.
  https://www.securityweek.com/logistics-firm-hellmann-scrambling-recover-cyberattack
- Los piratas informáticos atacan al Primer Ministro de la India.
  https://www.infosecurity-magazine.com/news/hackers-target-indias-prime/
- El Ministerio de Salud brasileño sufre el segundo ciberataque en menos de una semana.
  https://www.zdnet.com/article/brazilian-ministry-of-health-hit-by-second-cyberattack-in-less-than-a-week/
- El multimillonario proveedor de gas natural Superior Plus es víctima de un ransomware.
  https://www.zdnet.com/article/billion-dollar-natural-gas-supplier-superior-plus-hit-with-ransomware/

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

- CISA publica una guía sobre protección de cuentas en medios sociales.
  https://www.cisa.gov/uscert/ncas/current-activity/2021/12/09/cisa-releases-guidance-protecting-organization-run-social-media
- La red de bots Dark Mirai ataca al RCE en el popular router TP-Link.
  https://www.bleepingcomputer.com/news/security/dark-mirai-botnet-targeting-rce-on-popular-tp-link-router/
- **Vulnerabilidad de día cero en la biblioteca Java Log4j (actualizar Apache).**
  https://exchange.xforce.ibmcloud.com/collection/4daa3df4f73a51590efced7fb90bc949
  https://thehackernews.com/2021/12/extremely-critical-log4j-vulnerability.html
  https://nakedsecurity.sophos.com/2021/12/13/log4shell-explained-how-it-works-why-you-need-to-know-and-how-to-fix-it/
  https://securityaffairs.co/wordpress/125562/malware/linux-botnets-log4shell-flaw.html
  https://logging.apache.org/log4j/2.x/security.html
  https://www.techrepublic.com/article/how-to-test-if-your-linux-server-is-vulnerable-to-log4j/
  https://securityaffairs.co/wordpress/125630/malware/khonsari-ransomware-log4shell.html
- Microsoft detalla los bloques de construcción del ampliamente activo troyano bancario Qakbot.
  https://thehackernews.com/2021/12/microsoft-details-building-blocks-of.html
- **Explicación de las pruebas de penetración: Cómo los hackers éticos simulan los ataques.**
  https://www.csoonline.com/article/3643032/penetration-testing-explained-how-ethical-hackers-simulate-attacks.html
- CISA añade al catálogo trece vulnerabilidades conocidas y explotadas.

https://www.cisa.gov/uscert/ncas/current-activity/2021/12/10/cisa-adds-thirteen-known-exploited-vulnerabilities-catalog

- ¿Son legales las VPN? ¿Puedes tener problemas por usar una VPN?
  https://www.privacyaffairs.com/are-vpns-legal/
- **El malware Anubis para Android vuelve a atacar a 394 aplicaciones financieras.**
  https://www.bleepingcomputer.com/news/security/anubis-android-malware-returns-to-target-394-financial-apps/

NOTAS DE INTERÉS

- Se ha descubierto múltiples vulnerabilidades en un paquete de software de código abierto para centros de llamadas, GOautodial, con más de 50000 instalaciones en todo el mundo.
  https://www.infosecurity-magazine.com/news/vulnerabilities-found-in-goautodial/
- Emotet se apoya en TrickBot en su " Regreso de los Muertos".
  https://thehackernews.com/2021/12/140000-reasons-why-emotet-is.html
- Se descubre un error de autorización de la API GraphQL en una importante plataforma financiera B2B.
  https://www.zdnet.com/article/graphql-api-authorization-vulnerability-found-in-large-b2b-financial-technology-platform/
- Más de 300.000 dispositivos MikroTik son vulnerables a ataques remotos.
  https://thehackernews.com/2021/12/over-300000-mikrotik-devices-found.html
- La mitad de los sitios web siguen utilizando claves criptográficas heredadas.
  https://www.infosecurity-magazine.com/news/half-of-websites-still-using/
- Paquetes PyPI maliciosos con más de 10.000 descargas desactivadas.
  https://www.bleepingcomputer.com/news/security/malicious-pypi-packages-with-over-10-000-downloads-taken-down/
- El ransomware BlackCat, un malware muy sofisticado escrito en Rust.
  https://securityaffairs.co/wordpress/125459/cyber-crime/blackcat-ransomware.html
- Los atacantes pueden conseguir el root colapsando el AccountsService de Ubuntu.
  https://www.bleepingcomputer.com/news/security/attackers-can-get-root-by-crashing-ubuntu-s-accountsservice/
- La actualización del controlador de Dell permite aún ataques a nivel del Kernel de Windows.
  https://www.bleepingcomputer.com/news/security/dell-driver-fix-still-allows-windows-kernel-level-attacks/

ACTUALIZACIONES DE SEGURIDAD

- Google parchea graves vulnerabilidades en Chrome.
  https://www.securityweek.com/google-patches-serious-use-after-free-vulnerabilities-chrome
- Las actualizaciones de seguridad de Android resuelve 46 vulnerabilidades.
  https://www.securityweek.com/android-security-updates-patch-46-vulnerabilities
- La actualización de Firefox trae un nuevo tipo de “caja de arena” (*sandbox*) de seguridad.
  https://nakedsecurity.sophos.com/2021/12/07/firefox-update-brings-a-whole-new-sort-of-security-sandbox/
- Kali Linux 2021.4 fue liberado.
  https://www.helpnetsecurity.com/2021/12/09/kali-linux-2021-4-released/
- Apple corrige 42 fallos de seguridad en la última actualización de iOS.
  https://www.securityweek.com/apple-patches-42-security-flaws-latest-ios-refresh
- Martes de parches de Microsoft, diciembre de 2021
  https://www.zdnet.com/article/microsoft-december-2021-patch-tuesday-zero-day-exploited-to-spread-emotet-malware/