@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. 131 – 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.

07/09/21

- Hackean el servidor Confluence del proyecto Jenkins para minar Monero.
https://www.bleepingcomputer.com/news/security/jenkins-projects-confluence-server-hacked-to-mine-monero/
- **Un hacker afirma haber robado información de 7 millones de israelíes.**
https://www.jpost.com/israel-news/hacker-claims-to-have-stolen-information-of-7-million-israelis-678905
- La Universidad de Howard informa de un ataque de ransomware y cierra las clases este martes.
https://www.zdnet.com/article/howard-university-announces-ransomware-attack-shuts-down-classes-on-tuesday/
- Ciberataque a la Universidad de Washington DC.
https://www.infosecurity-magazine.com/news/cyberattack-on-washington-dc/

08/09/21

- Los atacantes de BladeHawk espían a los kurdos con falsas aplicaciones para Android.
https://www.zdnet.com/article/bladehawk-attackers-spy-on-kurds-with-fake-android-apps/
- Intrusos filtran las contraseñas de 500.000 cuentas VPN de Fortinet.
https://www.bleepingcomputer.com/news/security/hackers-leak-passwords-for-500-000-fortinet-vpn-accounts/
- ANZ de Nueva Zelanda vuelve a estar *en línea* tras la interrupción por un ataque DDoS.
https://www.zdnet.com/article/anz-new-zealand-back-online-after-outage-from-ddos-attack/

09/09/21

- Yandex lucha contra el mayor ataque DDoS de la historia de Internet en Rusia.
https://www.bleepingcomputer.com/news/security/yandex-is-battling-the-largest-ddos-in-russian-internet-history/
https://www.bleepingcomputer.com/news/security/new-m-ris-botnet-breaks-ddos-record-with-218-million-rps-attack/
- Las computadoras de Naciones Unidas fueron pirateadas por hackers a principios de este año.
https://time.com/6096271/united-nations-hack/
- **La Guardia Nacional de Virginia confirma que el ciberataque afectó a las cuentas de correo electrónico de las Fuerzas**
https://www.zdnet.com/article/virginia-national-guard-confirms-cyberattack-hit-virginia-defense-force-email-accounts/

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

- Los servidores del ransomware REvil vuelven a estar en línea misteriosamente.

https://www.bleepingcomputer.com/news/security/revil-ransomwares-servers-mysteriously-come-back-online/

- Error de suplantación de identidad pone en alerta a la ciberseguridad de los pasaportes digitales del Reino Unido.
https://threatpost.com/spoofing-bug-cybersecurity-vaccine-passports/169287/

- GitHub encuentra 7 vulnerabilidades de ejecución de código en 'tar' y npm CLI.
https://www.bleepingcomputer.com/news/security/github-finds-7-code-execution-vulnerabilities-in-tar-and-npm-cli/

NOTAS DE INTERÉS

- ProtonMail, un servicio de e-mail encriptado, informó que la orden del tribunal suizo no dejó otra opción que la de registrar la dirección IP de un activista.
https://www.cyberscoop.com/protonmail-swiss-court-ip-france/

- McDonald's filtra la contraseña de la base de datos del Monopoly VIP a los ganadores del juego.
https://www.bleepingcomputer.com/news/security/mcdonalds-leaks-password-for-monopoly-vip-database-to-winners/

- El mercado de la computación en nube alcanzará los 1,25 billones de dólares en 2028.
https://www.helpnetsecurity.com/2021/09/08/cloud-computing-market-2028/

- **Nuevo ataque de día 0 dirigido a usuarios de Windows en documentos de Microsoft Office.**
https://thehackernews.com/2021/09/new-0-day-attack-targeting-windows.html
https://www.helpnetsecurity.com/2021/09/08/cve-2021-40444/

- La ciberdelincuencia rusa continúa pero disminuyen ataques a empresas respaldadas por el gobierno.
https://www.cyberscoop.com/crowdstrike-russia-wizard-spider/

- OpenSSL 3.0: Un nuevo módulo FIPS, nuevos algoritmos, compatibilidad con Linux Kernel TLS y mucho más.
https://www.helpnetsecurity.com/2021/09/09/openssl-3-0/

- La *puerta trasera* SideWalk está relacionada con el grupo de espionaje "Grayfly" vinculado a China.
https://threatpost.com/sidewalk-backdoor-china-espionage-grayfly/169310/

ACTUALIZACIONES DE SEGURIDAD

- Zoho soluciona un error crítico de ADSelfService Plus que es explotado activamente.
https://www.bleepingcomputer.com/news/security/zoho-patches-actively-exploited-critical-adselfservice-plus-bug/
https://thehackernews.com/2021/09/cisa-warns-of-actively-exploited-zoho.html

- Dell presenta un conjunto de nuevas herramientas de seguridad de datos para resolver los problemas de latencia.
https://www.zdnet.com/article/dell-rolls-out-a-set-of-new-data-security-tools-to-address-latency-and-scale-issues/

- Microsoft corrige el error que permite a los *hackers* tomar el control de los contenedores de Azure.
https://www.bleepingcomputer.com/news/security/microsoft-fixes-bug-letting-hackers-take-over-azure-containers/