@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. 180 – Año 2022

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 22/08/22 y el 28/08/22

- El operador de gas natural griego sufre una filtración de datos relacionada con el ransomware.
https://www.bleepingcomputer.com/news/security/greek-natural-gas-operator-suffers-ransomware-related-data-breach/
- El Center Hospitalier Sud Francilien (CHSF), a 28 km del centro de París, sufrió un ciberataque el domingo, provocando la derivación de los pacientes a otros establecimientos.
https://www.bleepingcomputer.com/news/security/french-hospital-hit-by-10m-ransomware-attack-sends-patients-elsewhere/
- Saquearon cajeros automáticos de Bitcoin, creando cuentas de administrador falsas.
https://nakedsecurity.sophos.com/2022/08/23/bitcoin-atms-leeched-by-attackers-who-created-fake-admin-accounts/
- Ataque ransomware Quantum afecta una agencia gubernamental en la República Dominicana.
https://www.bleepingcomputer.com/news/security/quantum-ransomware-attack-disrupts-govt-agency-in-dominican-republic/

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

- Resumen de vulnerabilidades para la semana del 15 de agosto de 2022.
https://www.cisa.gov/uscert/ncas/bulletins/sb22-234
- **Un archivo ZIP encriptado puede tener dos contraseñas correctas. Aquí está la razón.**
https://www.bleepingcomputer.com/news/security/an-encrypted-zip-file-can-have-two-correct-passwords-heres-why/
- Actores de amenazas que aprovechan múltiples CVEs contra Zimbra Collaboration Suite.
https://www.cisa.gov/uscert/ncas/alerts/aa22-228a
- Google: Hackers iraníes utilizan nueva herramienta para robar el correo electrónico de personas.
https://www.techrepublic.com/article/iranian-cyberespionage-group-extracts-emails-using-hyperscrape/
- **Nuevo tipo de ataque a redes aisladas (air gap) utiliza un canal de ultrasonido encubierto para extraer datos (Gairoscope).**
https://thehackernews.com/2022/08/new-air-gap-attack-uses-mems-gyroscope.html
- Bug en los firewalls de Palo Alto Networks bajo ataque activo, provoca la advertencia de CISA.
https://threatpost.com/firewall-bug-under-active-attack-cisa-warning/180467/
- Actualización del malware XCSSET. Los atacantes de macOS se preparan para seguir sin Python.
https://www.sentinelone.com/blog/xcsset-malware-update-macos-threat-actors-prepare-for-life-without-python/
- Vulnerabilidades antiguas y poco conocidas a las que generalmente se les ataca cuando se realizan actividades de escaneo de OT.
https://www.securityweek.com/old-inconspicuous-vulnerabilities-commonly-targeted-ot-scanning-activity

- Casi 3 años después, el CISO de SolarWinds comparte 3 lecciones del célebre ataque. https://www.darkreading.com/edge-articles/3-years-later-solarwinds-ciso-shares-3-lessons-from-the-infamous-attack
- Herramienta de benchmark 3DMark falsa y que distribuye malware de robo de información. https://www.bleepingcomputer.com/news/security/pirated-3dmark-benchmark-tool-delivering-info-stealer-malware/
- Advierten de un ataque AiTM dirigido a los usuarios de Google G-Suite Enterprise. https://thehackernews.com/2022/08/researchers-warn-of-aitm-attack.html
- WannaCry explicado: Una tormenta de ransomware perfecta. https://www.csoonline.com/article/3227906/wannacry-explained-a-perfect-ransomware-storm.html
- Hackers utilizan páginas de protección DDoS falsas para distribuir malware. https://thehackernews.com/2022/08/hackers-using-fake-ddos-protection.html
- **Preparación de las infraestructuras críticas para la criptografía poscuántica.** https://www.cisa.gov/uscert/ncas/current-activity/2022/08/24/preparing-critical-infrastructure-post-quantum-cryptography
- Microsoft: Lo más destacado de la seguridad en Black Hat USA 2022. https://www.microsoft.com/security/blog/2022/08/25/microsoft-security-highlights-from-black-hat-usa-2022/

NOTAS DE INTERÉS

- El CEO de la empresa israelí de programas espía Pegasus, NSO, abandona su cargo. https://www.theguardian.com/world/2022/aug/22/nso-group-ceo-shalev-hulio-step-down-israel-pegasus-spyware
- El NIST se pronuncia sobre los riesgos de la IA. https://www.darkreading.com/edge/nist-weighs-in-on-ai-risk
- **Google neutraliza el mayor ataque DDoS HTTPS registrado hasta la fecha.** https://unaaldia.hispasec.com/2022/08/google-neutraliza-el-mayor-ataque-ddos-https-registrado-hasta-la-fecha.html
- El malware RAT Escanor se instala a través de documentos de Microsoft Office y PDF. https://www.infosecurity-magazine.com/news/escanor-rat-malware-microsoft-pdf/
- **El bug DirtyCred del Kernel de Linux, de 8 años de antigüedad, es desagradable como DirtyPipe.** https://securityaffairs.co/wordpress/134719/security/linux-dirtycred-flaw.html
- VMware Carbon Black provoca fallos BSOD en Windows. https://www.bleepingcomputer.com/news/security/vmware-carbon-black-causing-bsod-crashes-on-windows/
- El sector sanitario de EE.UU. ha filtrado más de 342 millones de registros desde 2009. https://www.infosecurity-magazine.com/news/us-healthcare-breach-342m-records/
- La Unión Europea esboza una respuesta cibernética crítica a la guerra de Ucrania. https://www.infosecurity-magazine.com/news/eu-critical-cyber-response-ukraine/

ACTUALIZACIONES DE SEGURIDAD

- GitLab publica un parche para un fallo crítico en su software comunitario y empresarial. https://thehackernews.com/2022/08/gitlab-issues-patch-for-critical-flaw.html
- Mozilla emite actualizaciones de seguridad para Firefox, Firefox ESR y Thunderbird. https://www.cisa.gov/uscert/ncas/current-activity/2022/08/23/mozilla-releases-security-updates-firefox-firefox-esr-and