@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. 152 – 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 26/2/22 y el 3/2/22

- Puerto Rico sufrió un gran ciberataque.
  https://securityaffairs.co/wordpress/127265/hacking/puerto-rico-suffered-cyberattack.html
- Un contratista taiwanés de Apple y Tesla afectado por el ransomware Conti.
  https://www.bleepingcomputer.com/news/security/taiwanese-apple-and-tesla-contractor-hit-by-conti-ransomware/
- Un servidor de AWS no seguro expuso 3TB en registros de empleados de un aeropuerto.
  https://www.zdnet.com/article/unsecured-aws-server-exposed-airport-employee-records-3tb-in-data/
- **Shell obligada a redirigir sus suministros tras ciberataque a 2 compañías petroleras alemanas.**
  https://www.zdnet.com/article/shell-forced-re-route-oil-supplies-after-cyberattack-on-german-companies/
  https://www.zdnet.com/article/cyberattack-affecting-belgian-port-operations/

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

- El gobierno alemán advierte de la presencia de hackers de APT27 en las redes empresariales.
  https://www.bleepingcomputer.com/news/security/german-govt-warns-of-apt27-hackers-backdooring-business-networks/
- El troyano bancario Chaes piratea Chrome con extensiones maliciosas.
  https://www.bleepingcomputer.com/news/security/chaes-banking-trojan-hijacks-chrome-with-malicious-extensions/
- QNAP señala de que el ransomware DeadBolt afecta dispositivos NAS con conexión a Internet.
  https://thehackernews.com/2022/01/qnap-warns-of-deadbolt-ransomware.html
- El ransomware BlackCat se centra en organizaciones estadounidenses y europeas de venta al por menor, construcción y transporte.
  https://www.zdnet.com/article/blackcat-ransomware-targeting-us-european-retail-construction-and-transportation-orgs/
- **Ataques DDoS: Definición, ejemplos y técnicas.**
  https://www.csoonline.com/article/3648530/ddos-attacks-definition-examples-and-techniques.html
- APT iraní MuddyWater se enfoca en usuarios turcos a través de PDFs y ejecutables maliciosos.
  http://blog.talosintelligence.com/2022/01/iranian-apt-muddywater-targets-turkey.html
- Nueva y potente variante de Oski 'Mars Stealer' se apodera de las 2FAs y las criptomonedas.
  https://www.bleepingcomputer.com/news/security/powerful-new-oski-variant-mars-stealer-grabbing-2fas-and-crypto/
- El malware para Mac que se extiende desde hace unos 14 meses instala un backdoor en los sistemas infectados.
  https://arstechnica.com/information-technology/2022/02/mac-malware-spreading-for-14-months-is-growing-increasingly-aggressive/

NOTAS DE INTERÉS

- **Las distribuciones de Linux tienen un error en el PwnKit, que permite acceder al root.**
https://securityaffairs.co/wordpress/127199/security/linux-cve-2021-4034-bug.html
https://github.com/PeterGottesman/pwnkit-exploit
- Hackers norcoreanos utilizan el servicio de actualización de Windows para infectar computadoras con malware.
https://thehackernews.com/2022/01/north-korean-hackers-using-windows.html
- EE.UU. prohíbe al gigante de las telecomunicaciones China Unicom por motivos de espionaje.
https://www.bbc.com/news/business-60164747
- **Dispositivos de diplomáticos finlandeses fueron infectados con el programa espía Pegasus.**
https://securityaffairs.co/wordpress/127334/breaking-news/pegasus-spyware-finnish-diplomats.html
- Criptoagilidad: La solución a lo inevitable.
https://www.darkreading.com/vulnerabilities-threats/crypto-agility-solving-for-the-inevitable
- Quedaron expuestos 277.000 routers a ataques “Eternal Silence” a través de UPnP.
https://www.bleepingcomputer.com/news/security/277-000-routers-exposed-to-eternal-silence-attacks-via-upnp/
- CISA añade 8 nuevas vulnerabilidades a su Catálogo de Vulnerabilidades Conocidas y Explotadas.
https://securityaffairs.co/wordpress/127448/security/8-flaws-known-exploited-vulnerabilities-catalog.html
- Los hackers rusos de "Gamaredon" utilizan 8 nuevas *cargas útiles* de malware en sus ataques.
https://www.bleepingcomputer.com/news/security/russian-gamaredon-hackers-use-8-new-malware-payloads-in-attacks/
- Las nuevas vulnerabilidades de SureMDM podrían exponer a las empresas a ataques a la cadena de suministro.
https://thehackernews.com/2022/01/new-suremdm-vulnerabilities-could.html
- **Vulnerabilidad de gravedad crítica en la plataforma Samba podría permitir a los atacantes obtener la ejecución remota de código con privilegios de *root* en los servidores.**
https://threatpost.com/samba-fruit-bug-rce-root-access/178141/
- Fueron robados 324 millones de dólares de la plataforma blockchain Wormhole.
https://www.zdnet.com/article/324-million-in-ether-stolen-from-blockchain-platform-wormhole/
- Se descubren fallos críticos en los routers de la serie RV de Cisco Small Business.
https://thehackernews.com/2022/02/critical-flaws-discovered-in-cisco.html
- Nuevo malware de hackers estatales chinos les ayudó a no ser detectados durante 250 días.
https://www.bleepingcomputer.com/news/security/state-hackers-new-malware-helped-them-stay-undetected-for-250-day/

ACTUALIZACIONES DE SEGURIDAD

- Apple corrige dos errores de seguridad de día cero, uno de ellos explotado activamente.
https://threatpost.com/apple-zero-day-security-exploited/178040/
- Fue descubierta y parcheada una vulnerabilidad de Linux de hace doce años.
https://www.schneier.com/blog/archives/2022/01/twelve-year-old-linux-vulnerability-discovered-and-patched.html
- Un error del antivirus ESET permitía a los atacantes obtener privilegios de SISTEMA de Windows.
https://www.bleepingcomputer.com/news/microsoft/eset-antivirus-bug-let-attackers-gain-windows-system-privileges/