@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. 159 – 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 18/3/22 y el 24/3/22

- Hackers brasileños afirman haber accedido a TransUnion South Africa con la contraseña "Password".
  https://www.bleepingcomputer.com/news/security/hackers-claim-to-breach-transunion-south-africa-with-password-password/
- La filtración de datos de un servicio odontológico podría afectar a un millón de personas de Texas.
  https://www.infosecurity-magazine.com/news/dental-care-data-breach-may-impact/
- **El principal productor de carne ruso sufre un ataque de encriptado con Windows BitLocker.**
  https://www.bleepingcomputer.com/news/security/top-russian-meat-producer-hit-with-windows-bitlocker-encryption-attack/
- El servicio postal público de Grecia está fuera de servicio debido a un ataque de ransomware.
  https://www.bleepingcomputer.com/news/security/greeces-public-postal-service-offline-due-to-ransomware-attack/
- **Microsoft confirma que fue hackeado por el grupo extorsivo Lapsus$.**
  https://thehackernews.com/2022/03/microsoft-and-okta-confirm-breach-by.html

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

- Google ha aportado un análisis de las operaciones de un ciberdelincuente apodado "Exotic Lily", que parece ser intermediario de acceso inicial para las bandas de ransomware Conti y Diavol.
  https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/
- Un análisis de dos ataques ransomware ha encontrado similitudes en tácticas, técnicas y procedimientos (TTP) entre BlackCat y BlackMatter, indicando fuerte relación entre los 2 grupos.
  https://thehackernews.com/2022/03/experts-find-some-affiliates-of.html
- La APT de habla rusa que está detrás de los ataques NotPetya y del derribo de la red eléctrica ucraniana podría estar preparando otros ataques, por ejemplo a *routers* ASUS.
  https://threatpost.com/sandworm-asus-routers-cyclops-blink-botnet/178986/
- Un kit de herramientas de phishing permite a cualquiera crear ventanas falsas usando Chrome.
  https://www.bleepingcomputer.com/news/security/new-phishing-toolkit-lets-anyone-create-fake-chrome-browser-windows/
- Un nuevo *backdoor* se enfoca en entidades francesas a través de un instalador de paquetes de código abierto.
  https://thehackernews.com/2022/03/new-backdoor-targets-french-entities.html
- Más código fuente del ransomware Conti filtrado por venganza en Twitter.
  https://www.bleepingcomputer.com/news/security/more-conti-ransomware-source-code-leaked-on-twitter-out-of-revenge/

- **Okta, proveedor líder de servicios de autenticación y soluciones de gestión de identidad y acceso (IAM), informa que está analizando la violación de datos del grupo Lapsus$.**
  https://www.bleepingcomputer.com/news/security/okta-investigating-claims-of-customer-data-breach-from-lapsus-group/
  https://www.theverge.com/2022/3/23/22993731/lapsus-hacking-group-teenager-mastermind
- Deadbolt, el ransomware que va directamente por las copias de seguridad.
  https://nakedsecurity.sophos.com/2022/03/23/serious-security-deadbolt-the-ransomware-that-goes-straight-for-for-your-backups/
- **FBI: El ransomware afectó a 649 organizaciones de infraestructuras críticas en 2021.**
  https://www.bleepingcomputer.com/news/security/fbi-ransomware-hit-649-critical-infrastructure-orgs-in-2021/

NOTAS DE INTERÉS

- El desarrollador detrás del popular paquete NPM "node-ipc" subió una versión destructiva para protestar por la invasión rusa de Ucrania.
  https://securityaffairs.co/wordpress/129174/hacking/node-ipc-npm-package-sabotage.html
  https://arstechnica.com/information-technology/2022/03/sabotage-code-added-to-popular-npm-package-wiped-files-in-russia-and-belarus/
- **El ransomware Avoslocker se centra en las infraestructuras críticas de Estados Unidos.**
  https://www.bleepingcomputer.com/news/security/fbi-avoslocker-ransomware-targets-us-critical-infrastructure/
  https://www.infosecurity-magazine.com/news/avoslocker-strikes-critical/
- La estafa criptográfica 'CryptoRom' se aprovecha de las funciones del iPhone para atacar a los usuarios de móviles.
  https://thehackernews.com/2022/03/cryptorom-crypto-scam-abusing-iphone.html
- El sospechoso resurgimiento de DarkHotel APT tiene por objetivo los hoteles chinos de lujo.
  https://www.zdnet.com/article/suspected-darkhotel-apt-resurgence-targets-luxury-chinese-hotels/
- Gimmick es un implante para macOS recientemente descubierto y desarrollado por la APT Storm Cloud, vinculada a China.
  https://securityaffairs.co/wordpress/129402/malware/gimmick-implant-targets-macos.html
- El backdoor Serpent se introduce en las empresas mediante un instalador Chocolatey.
  https://threatpost.com/serpent-backdoor-chocolatey-installer/179027/
- Cientos de modelos de impresoras HP son vulnerables, otra vez, a la ejecución remota de código.
  https://www.bleepingcomputer.com/news/security/hundreds-of-hp-printer-models-vulnerable-to-remote-code-execution/
- **Una red de bots controlan miles de routers MikroTik y se usan en las campañas de Glupteba y TrickBot.**
  https://thehackernews.com/2022/03/over-200000-microtik-routers-worldwide.html
- La APT china "Mustang Panda" ha sido descubierta utilizando el nuevo malware "Hodur".
  https://thehackernews.com/2022/03/chinese-mustang-panda-hackers-spotted.html
- El programa espía Vidar ahora se esconde en los archivos de ayuda de Microsoft
  https://www.zdnet.com/article/vidar-spyware-is-now-hidden-in-microsoft-help-files/

ACTUALIZACIONES DE SEGURIDAD

- Microsoft soluciona el problema de Bluetooth, que causa los pantallazos azules de Windows.
  https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-bluetooth-issue-causing-windows-blue-screens/