@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. 185 – 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 23/09/22 y el 29/09/22

- **Masivo hackeo al EMCO de Chile y temor por la filtración de información.**
  https://www.infobae.com/america/america-latina/2022/09/23/temor-en-chile-por-la-informacion-que-podria-filtrarse-tras-el-hackeo-a-sus-fuerzas-armadas/
- Una sofisticada campaña de ciberataques furtivos está dirigida a contratistas militares de EE.UU.
  https://www.darkreading.com/attacks-breaches/sophisticated-cyberattack-campaign-targets-defense-contractors

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

- La NSA revela el "libro de estrategias de los hackers" para los ataques de OT.
  https://www.infosecurity-magazine.com/news/nsa-reveals-hackers-playbook-for/
  https://media.defense.gov/2022/Sep/22/2003083007/-1/-1/0/CSA_ICS_Know_the_Opponent_.PDF
- Se descubre una operación multimillonaria de fraude con tarjetas de crédito.
  https://www.bleepingcomputer.com/news/security/multi-million-dollar-credit-card-fraud-operation-uncovered/
- Servidores Microsoft SQL hackeados en los ataques de ransomware de TargetCompany (o Fargo).
  https://www.bleepingcomputer.com/news/security/microsoft-sql-servers-hacked-in-targetcompany-ransomware-attacks/
- **Cómo se esconde el malware en las imágenes y qué se puede hacer al respecto.**
  https://gizmodo.com/malware-images-virus-photos-pictures-how-block-antiviru-1849572516
- Utilizan los archivos de PowerPoint para distribuir malware con el movimiento del mouse.
  https://www.bleepingcomputer.com/news/security/hackers-use-powerpoint-files-for-mouseover-malware-delivery/
- Tres tipos de rutas de ataque en entornos de Microsoft Active Directory.
  https://www.helpnetsecurity.com/2022/09/28/3-types-attack-paths-microsoft-active-directory-environments/
- Se filtró el generador de LockBit 3.0 utilizado por la banda ransomware 'Bl00dy' en sus ataques.
  https://www.bleepingcomputer.com/news/security/leaked-lockbit-30-builder-used-by-bl00dy-ransomware-gang-in-attacks/
- Diferencias en la seguridad/privacidad de las aplicaciones Android según el país.
  https://www.schneier.com/blog/archives/2022/09/differences-in-app-security-privacy-based-on-country.html
- **Un malware nunca visto antes, Chaos, ha infectado cientos de dispositivos Linux y Windows.**
  https://arstechnica.com/information-technology/2022/09/never-before-seen-malware-has-infected-hundreds-of-linux-and-windows-devices/
- **Las más relevantes Iniciativas gubernamentales en ciberseguridad de distintos países en 2022.**
  https://www.csoonline.com/article/3674954/23-notable-government-cybersecurity-initiatives-in-2022.html
- Los hackers brasileños de Prilex reaparecen con un sofisticado malware para puntos de venta.
  https://thehackernews.com/2022/09/brazilian-prilex-hackers-resurfaced.html

NOTAS DE INTERÉS

- Utilizan aplicaciones OAuth maliciosas para apoderarse de los servidores de correo electrónico.
https://www.darkreading.com/application-security/cyberattackers-compromise-microsoft-exchange-servers-malicious-oauth-apps
- **Acusan a Meta de infringir la ley al rastrear en forma secreta a los usuarios de iPhone.**
https://www.theregister.com/2022/09/23/meta_app_tracking/
- En la India, aplicaciones falsas de incentivos bancarios se centran en usuarios de Android, contienen malware para robo de información.
https://thehackernews.com/2022/09/fake-indian-banking-rewards-apps.html
- El grupo de cibermercenarios Void Balaur continúa con sus campañas de hackeo por encargo.
https://www.infosecurity-magazine.com/news/void-balaur-expand-hack-for-hire/
- **Se filtran los datos de más de 300.000 reservistas rusos, según Anonymous.**
https://www.infosecurity-magazine.com/news/russian-reservists-leaked-anonymous/
- El grupo "Metador" lleva meses afectando las redes de proveedores de servicios de Internet.
https://www.bleepingcomputer.com/news/security/new-hacking-group-metador-lurking-in-isp-networks-for-months/
- Los grupos ransomware adoptan la metodología de destrucción de datos.
https://www.infosecurity-magazine.com/news/ransomware-affiliates-adopt-data/
- Los autores del ransomware BlackCat han sido descubiertos mejorando su arsenal de malware.
https://thehackernews.com/2022/09/blackcat-ransomware-attackers-spotted.html
- Rusia planea "ciberataques masivos" contra infraestructuras críticas, advierte Ucrania.
https://arstechnica.com/information-technology/2022/09/ukraine-warns-russia-plans-massive-cyberattacks-on-its-power-grids/
- El responsable de la filtración de datos de Optus publica 10.200 registros de clientes en plan de extorsión.
https://thehackernews.com/2022/09/hacker-behind-optus-breach-releases.html
- Los ciberpiratas están probando una nueva forma destructiva de hacer más efectivos los ataques ransomware.
https://www.zdnet.com/article/hackers-are-testing-a-destructive-new-way-to-make-ransomware-attacks-more-effective/
- Los actores de la amenaza utilizan Quantum Builder para distribuir el malware Agent Tesla.
https://securityaffairs.co/wordpress/136370/uncategorized/quantum-builder-agent-tesla-rat.html
- **Los errores en el stacking VLAN de Ethernet permiten a los hackers lanzar ataques DoS y MiTM.**
https://www.bleepingcomputer.com/news/security/ethernet-vlan-stacking-flaws-let-hackers-launch-dos-mitm-attacks/
- Los hackers utilizan Telegram y Signal para ayudar a los manifestantes en Irán.
https://www.infosecurity-magazine.com/news/hackers-assist-protestors-in-iran/

ACTUALIZACIONES DE SEGURIDAD

- El Consorcio de Sistemas de Internet (ISC) ha corregido seis vulnerabilidades explotables de forma remota en el software BIND DNS.
https://securityaffairs.co/wordpress/136164/security/bind-dns-software-flaws-2.html
- WhatsApp revela una vulnerabilidad crítica en versiones antiguas de la app.
https://www.theverge.com/2022/9/27/23374468/whatsapp-bug-video-call-vulnerability-cve