@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. 137 – 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.

## Noticias de ciberseguridad entre el 14/10/21 y el 20/10/21

- Los piratas informáticos afirman haber robado 60 GB de datos de la empresa Acer.
  https://www.securityweek.com/hackers-claim-have-stolen-60-gb-data-acer
  https://securityaffairs.co/wordpress/123339/data-breach/acer-suffered-second-security-breach.html
- Accenture confirma la filtración de datos tras el ataque de ransomware de agosto.
  https://www.bleepingcomputer.com/news/security/accenture-confirms-data-breach-after-august-ransomware-attack/
- El gigante brasileño de los seguros Porto Seguro sufre un ciberataque.
  https://www.zdnet.com/article/brazilian-insurance-giant-porto-seguro-hit-by-cyberattack/
- La cadena de televisión Sinclair en EE.UU. es afectada por ataque ransomware el fin de semana.
  https://www.bleepingcomputer.com/news/security/sinclair-tv-stations-crippled-by-weekend-ransomware-attack/
- Acer ha sido hackeado dos veces en una semana por el mismo "actor de amenazas".
  https://www.bleepingcomputer.com/news/security/acer-hacked-twice-in-a-week-by-the-same-threat-actor/
- La empresa de servicios al cliente Atento, en Brasil, sufre un ciberataque.
  https://www.zdnet.com/article/customer-services-firm-atento-hit-by-cyberattack/

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

- VirusTotal comparte datos sobre la actividad de los grupos ransomware.
  https://www.darkreading.com/threat-intelligence/virustotal-shares-data-on-ransomware-activity
- Google envió 50.000 avisos de ataques patrocinados por el Estado en 2021.
  https://www.bleepingcomputer.com/news/security/google-sent-50-000-warnings-of-state-sponsored-attacks-in-2021/
- Un grupo respaldado por un Estado nacional, utiliza un nuevo conjunto de herramientas para atacar a sus víctimas en el sur de Asia.
  https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/harvester-new-apt-attacks-asia
- El PIN de la tarjeta pueden descubrirse aun cuando se tape el teclado del cajero automático.
  https://www.bleepingcomputer.com/news/security/credit-card-pins-can-be-guessed-even-when-covering-the-atm-pad/
- El TA505, vinculado a Rusia, se centra en instituciones financieras en una campaña de *malspam*.
  https://securityaffairs.co/wordpress/123441/breaking-news/ta505-mirrorblast-malspam-campaign.html
  https://threatpost.com/ta505-retooled-flawedgrace-rat/175559/
- La evolución del cibercrimen de habla rusa entre el 2016 y el 2021.

https://securelist.com/russian-speaking-cybercrime-evolution-2016-2021/104656/

- La nueva variante de la botnet PurpleFox utiliza WebSockets para la comunicación C2. https://www.bleepingcomputer.com/news/security/new-purplefox-botnet-variant-uses-websockets-for-c2-communication/

## NOTAS DE INTERÉS

- La red de bots MyKings sigue activa y ganando grandes cantidades de dinero. https://www.bleepingcomputer.com/news/security/mykings-botnet-still-active-and-making-massive-amounts-of-money/
- La red de bots FreakOut convierte los DVR en máquinas de *criptominado* de Monero. https://threatpost.com/freakout-botnet-dvrs-monero-cryptominers/175467/
- Nuevo ransomware Yanluowang es utilizado en ataques dirigidos a empresas. https://www.bleepingcomputer.com/news/security/new-yanluowang-ransomware-used-in-targeted-enterprise-attacks/
- Moscú incorpora el sistema de pago por reconocimiento facial a más de 240 estaciones del subterráneo. https://www.theverge.com/2021/10/15/22728667/russia-face-pay-system-moscow-metro-privacy
- La CISA, el FBI y la NSA advierten que Las instalaciones de agua y aguas residuales de EE.UU. son objeto de ciberataques. https://www.darkreading.com/attacks-breaches/cisa-fbi-nsa-us-water-and-wastewater-facilities-targeted-in-cyberattacks
- Resumen de la semana: Reforzar la seguridad del firmware, Publicación del informe XDR. https://www.helpnetsecurity.com/2021/10/17/week-in-review-strengthening-firmware-security-help-net-security-xdr-report-released/
- El ransomware REvil se desconecta de nuevo tras el control de los sitios de Tor. https://www.bleepingcomputer.com/news/security/revil-ransomware-shuts-down-again-after-tor-sites-were-hijacked/
- Han encontrado muchos parecidos entre el nuevo ransomware Karma y las variantes de Nemty. https://securityaffairs.co/wordpress/123568/malware/karma-ransomware-nemty-similarities.html
- Expertos en ciberseguridad advierten de un aumento de las actividades del grupo de hackers Lyceum en Túnez. https://thehackernews.com/2021/10/cybersecurity-experts-warn-of-rise-in.html
- Una mala configuración de un proveedor de VPN expone a un millón de usuarios. https://www.infosecurity-magazine.com/news/vpn-provider-misconfiguration-users/
- Otra empresa de ciberseguridad con sede en Israel, Valence, sale del anonimato con un desarrollo para enfrentar riesgos de conectividad de aplicaciones empresariales. https://www.securityweek.com/valence-emerges-stealth-address-business-app-connectivity-risks

## ACTUALIZACIONES DE SEGURIDAD

- Intel y VMware se unen a los martes de parches. https://www.securityweek.com/intel-vmware-join-patch-tuesday-parade
- Oracle publica la actualización de parches críticos de octubre de 2021. https://us-cert.cisa.gov/ncas/current-activity/2021/10/19/oracle-releases-october-2021-critical-patch-update